

ZHENG FU CAI GOU

上海市徐汇区卫生健康委员会 2025 年  
卫健分支节点云建设（二期）政府采购

招

标

文

件

招标编号：徐采中招 2025-161

招标单位：上海市徐汇区政府采购中心

二〇二五年十月

2025年10月15日

## 第一部分 投标邀请

根据《中华人民共和国政府采购法》之规定，上海市徐汇区政府采购中心受委托，对上海市徐汇区卫生健康委员会 2025 年卫健分支节点云建设（二期）政府采购项目进行国内公开招投标采购，特邀请合格的供应商前来投标。

### 一、合格的投标人必须具备以下条件：

- 1、具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商，同时经信用信息查询未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；
- 2、具有工信部颁发的《基础电信业务经营许可证》或《增值电信业务经营许可证》；
- 3、本项目**不允许**联合投标。

### 二、项目概况：

1、项目名称：上海市徐汇区卫生健康委员会 2025 年卫健分支节点云建设（二期）政府采购项目

2、招标编号：（代理机构内部项目编号：徐采中招 2025-161）

3、预算编号：0425-000171493、K00004084

### 4、项目主要内容及要求：

采购内容：云服务商提供完整的云服务，包含云平台服务、基础安全服务、国密安全服务、集成服务、配套物理空间服务及运维服务，资源池需通过等保三级及密评相关测评。具体服务要求等详见招标文件第三部分。

5、服务地址：徐汇区卫健委指定地点。

6、项目服务期限：详见招标文件第三部分。

7、采购项目需要落实的政府采购政策情况：根据上海市财政局沪财库[2009]19号“关于落实政府采购优先购买福利企业产品和服务的通知”要求，本项目在同等条件下优先采购福利企业的产品和服务。同时项目采购应当符合采购价格低于市场平均价格、采购质量优良和服务良好的要求。本项目面向所有企业采购，对小型和微型企业投标人产品的价格给予 10% 的扣除，用扣除后的价格参与评审。其要求标准详见《政府采购促进中小企业发展管理办法》（财库[2020]46号）中相关规定。

### 三、招标文件的获取

1、合格的供应商可于 2025-10-16 本公告发布之日起至 2025-10-25 截止，登录“上海政府采购网”（<http://www.zfcg.sh.gov.cn>）在网上招标系统中获取招标文件。

采购文件上午获取时间：00:00:00~12:00:00

采购文件下午获取时间：12:00:00~23:59:59

2、凡愿参加投标的合格供应商可在上述规定的时间内下载（获取）招标文件并按照招标文件要求参加投标。

注：投标人须保证报名及获得招标文件需提交的资料和所填写内容真实、完整、有效、一致，如因投标人递交虚假材料或填写信息错误导致的与本项目有关的任何损失由投标人承担。

#### 四、投标截止时间及开标时间：

1、投标截止时间：2025-11-6 9:30，迟到或不符合规定的投标文件恕不接受。

2、开标时间：2025-11-6 9:30。

#### 五、投标地点和开标地点

1、投标地点：上海政府采购网（政府采购云平台）<http://www.zfcg.sh.gov.cn>；根据上海市财政局相关规定，本项目招投标相关活动在上海市政府采购云平台（网址：[www.zfcg.sh.gov.cn](http://www.zfcg.sh.gov.cn)）进行。政府采购云平台是由市财政局建设和维护。投标人应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。投标人在政府采购云平台的有关操作方法可以参照政府采购云平台中相关专栏的有关内容和操作要求办理。

2、开标地点：上海政府采购网（政府采购云平台）<http://www.zfcg.sh.gov.cn>；本项目实行网上远程开标，按有关规定在开标时间内无法签到、解密的供应商将被取消投标资格，不纳入评审范围。响应投标的供应商请在开标时间开始后持投标时所使用的数字证书（CA证书）参加远程开标。

#### 3、开标所需携带其他材料：

本项目实行网上远程开标，按有关规定在开标时间内无法签到、解密的供应商将被取消投标资格，不纳入评审范围。响应投标的供应商请在开标时间开始后持投标时所使用的数字证书（CA证书）参加远程开标。

#### 六、发布公告的媒介：

以上信息若有变更我们会通过“上海政府采购网”通知，请供应商关注。

#### 七、注意事项：

(1)投标单位对招标文件有疑问的可在2025年10月21日上午12点整前以书面传真的形式向徐汇区政府采购中心提出，由采购中心负责统一解答。采购中心将于2025年10月21日下午17点前通过“上海政府采购网”(<http://www.zfcg.sh.gov.cn>)公开发布。

(2)本项目采购预算为44070000元人民币，报价超过采购预算的投标不予接受。

(3) 投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在电子采购平台上的签收情况，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

## 八、联系方式

采购人：上海市徐汇区城市网格化综合 管理中心 采购代理机构：上海市徐汇区政府采购中心

地址：南宁路 969 号

地址：南宁路 969 号

联系人：高卉

联系人：曾妮

电话：24092222\*2511

电话：24092222\*2586

## 第二部分 投标人须知

### 一、总则

#### 1、概述

1. 1 本招标文件适用于本投标邀请中所述系统及相关服务的招标投标。
1. 2 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其他依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。
1. 3 根据上海市财政局相关规定，本项目招投标相关活动在上海市政府采购云平台（网址：[www.zfcg.sh.gov.cn](http://www.zfcg.sh.gov.cn)）进行。

#### 2、定义：

- 2.1 “招标人”指组织本次招标的上海市徐汇区政府采购中心和采购人。
- 2.2 “采购人”指上海市徐汇区城市网格化综合管理中心。
- 2.3 “招标项目”指本招标文件中第三部分所述相关系统及相关服务，本项目属于软件和信息技术服务业。
- 2.4 “潜在投标人”指符合招标文件规定的合格供应商。
- 2.5 “投标人”指按规定获取招标文件，并按照招标文件要求提交投标文件的供应商。
- 2.6 “上海市政府采购云平台”系指上海市政府采购信息管理平台的门户网站上海政府采购网（[www.zfcg.sh.gov.cn](http://www.zfcg.sh.gov.cn)），是由市财政局建设和维护。

#### 3、合格投标人的条件

3.1 具有本项目生产、供应或实施能力，符合、承认并承诺履行本文件各项规定的国内法人和其他组织均可参加投标。

3.2 投标人应遵守有关的国家法律、法规和条例，具备《中华人民共和国政府采购法》和本文件中规定的条件：

(1) 具有《中华人民共和国营业执照》、《税务登记证》，根据《上海市政府采购供应商登记及诚信管理办法》要求登记入库，在近三年内无行贿犯罪记录，未被政府采购监督管理部门禁止参加政府采购活动的供应商；同时经信用信息查询未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

(2) 具有工信部颁发的《基础电信业务经营许可证》或《增值电信业务经营许可证》；  
(3) 本项目不允许联合投标。

3.3 只有在法律上和财务上独立运作并独立于采购中心的供应商才能参加投标。

3.4 如投标人代表不是法定代表人，须持有《法定代表人授权委托书》（统一格式）。

#### 4. 投标费用

**4.1** 投标人应承担所有与准备和参加投标有关的费用，采购中心和采购人在任何情况下均无义务和责任承担这些费用。

**4.2** 本次招标工作由徐汇区政府采购中心自行组织实施，不收取任何中介费用。

## 二、招标文件

### 5.招标文件的构成

**5.1** 招标文件是阐明招标的项目范围、投标文件的编写、递交、招标投标程序、评标原则、中标条件和相关的协议条款的文件。招标文件由以下六部分内容组成：

第一部分 投标邀请（招标公告）；

第二部分 投标人须知；

第三部分 招标项目需求；

第四部分 合同参考范本；

第五部分 投标文件格式；

第六部分 评标办法

**5.2** 投标人应详细阅读招标文件的全部内容。如果投标人没有按照招标文件要求提交全部资料或者没有对招标文件在各方面的要求都做出实质性响应，可能导致其投标被拒绝。

### 6.招标文件的澄清

**6.1** 任何通过电子采购平台获取了招标文件的潜在投标人，均可要求对招标文件进行澄清。澄清要求应于投标邀请函所述日期前，按投标邀请书中的联系地址以书面形式（包括书面材料、信函、传真等，下同）送达采购中心，采购中心将通过“上海政府采购网”（<http://www.zfcg.sh.gov.cn>）公开发布相关答复。

**6.2** 采购中心将视情况确定是否有必要召开标前会（现场踏勘）。召开标前会（现场踏勘）的，所有投标人应根据招标文件或者招标人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

### 7.招标文件的修改

**7.1** 在投标截止期 15 日以前任何时候，采购中心无论出于何种原因，均可对招标文件用补充文件的方式进行修改。

**7.2** 对招标文件的修改，将通过“上海政府采购网”（<http://www.zfcg.sh.gov.cn>）公开发。补充文件将作为招标文件的组成部分，对所有获取了招标文件的潜在投标人均具有约束力。

**7.3** 为使投标人有足够的时间按招标文件的修改要求考虑修正投标文件，采购中心可酌情推迟投标的截止日期和开标日期，并将具体变更情况通知上述每一投标人。

### 8.通知

**8.1** 对与本项目有关的通知，采购中心将通过“上海政府采购网”（<http://www.zfcg.sh.gov.cn>）公开发。

8.2 招标文件的澄清、答复、修改或补充都应由采购中心以澄清或修改公告形式发布，除此以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，招标人不承担任何责任。

### 三、投标文件

#### 9.投标文件的语言和计量单位

9.1 投标人提交的以及投标人与采购中心就有关投标的所有来往函电均应使用中文简化字。

9.2 投标人所提供的技术文件和资料，包括图纸中的说明，应使用中文简化字。所使用的计量单位，应使用国家法定计量单位。

#### 10.投标文件的组成及相关要求

10.1 投标文件由商务响应文件、技术响应文件两部份构成。

10.2 商务响应文件、技术响应文件所应包含的内容如下：

##### 10.2.1 商务响应文件：

- (1) 投标函；
- (2) 投标报价明细表；
- (3) 法定代表人证明书和法人代表委托书；
- (4) 主要产品厂商授权证明；
- (5) 主要产品检测报告（复印件加盖单位公章）；
- (6) 投标单位基本情况表及声明；
- (7) 供应商行贿犯罪记录承诺书；
- (8) 中小企业声明函；
- (9) 近三年同类型项目成功案例介绍及最终用户的有效联系方式，附相关采购合同复印件加盖单位公章；
- (10) 资格证明文件，包括：投标单位营业执照、税务登记证（复印件加盖单位公章）；工信部颁发的《基础电信业务经营许可证》或《增值电信业务经营许可证》（复印件加盖单位公章）；投标人信用信息查询记录，投标人应当通过“信用中国”网站（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）查询投标人主体信用记录（查询截止时点为 2025 年 11 月 5 日），并对查询的信用详情截屏打印并加盖单位公章；投标单位财务状况及税收、社会保障资金缴纳情况声明函。资格证明文件不满足招标要求的，将作为无效投标处理。

- (11) 投标产品中属于国家强制性认证的，应提供相应认证证书等相关资料，并提供副本等明细材料以便于评标查阅；（复印件加盖单位公章）；

##### 10.2.2 技术响应文件：

- (1) 产品选型及说明一览表；
- (2) 产品规格、技术参数偏离表；

- (3) 拟从事本项目人员及其技术资格一览表；
- (4) 卫健分支节点云服务方案 提供详细的卫健分支节点云建设扩容设计方案，包括但不限于网络、安全等设计内容，实现云服务整体需求和服务指标。具体包括针对性的云平台建设方案、软硬件服务（包含所选用产品的数量、型号、详细技术参数指标等）、集成服务（包括整体硬件配置方案、机柜上架方案、网络规划方案和安全方案等）、配套物理空间服务、运维服务等，并满足相应的性能需求和服务指标等。
- (5) 项目实施计划 请投标单位自报项目实施周期，并根据项目实施具体情况制作详细实施周期及针对性施工组织方案、施工管理人员的资质（包括项目经理相关资质证书）、项目组成员工作内容与职责、项目组人员表(列表说明姓名、年龄、性别、学历、职称、从事本分系统工作年限、主要业绩)等项目质量、安全、工期保障措施，以确保项目优质按期安全完工；
- (6) 投标产品的说明书、产品厂家彩页性能介绍样本（catalog）等技术文件；
- (7) 售后服务承诺（保修期内售后服务的内容、期限、响应时间、应急保障措施等）及培训等相关伴随服务实施方案；
- (8) 规章制度一览表；
- (9) 投标人认为需要提供的其它说明和资料。

**10.3** 上述文件中凡招标文件提供格式文本的以及要求“加盖单位公章”的材料须上传原件彩色扫描件。

**10.4** 如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供，否则视作投标人放弃潜在中标资格，并且招标人将对该投标人进行调查，发现有欺诈行为的按有关规定进行处理。

**10.5** 本项目不接受纸质投标文件。

## 11. 投标内容填写说明

**11.1** 获取了招标文件的潜在投标人应认真阅读招标文件的所有内容，按照招标文件和电子采购平台电子招投标系统要求的格式填写相关内容。

**11.2** 投标人必须保证投标文件所提供的全部资料真实可靠，并接受采购中心对其中任何资料进一步审查的要求。

**11.3** 开标一览表要求按格式统一填写，不得自行增减内容。

**11.4** 投标文件须对招标文件中的内容做出实质性和完整的响应，否则其投标将被拒绝。如果投标文件填报的内容资料不详，或没有提供招标文件中所要求的全部资料及数据，包括但不限于**第 10 条（投标文件的组成及相关要求）**规定的内容，将可能导致投标被拒绝。

## 12. 投标报价

**12.1** 所有投标报价均以人民币元为计算单位。投标价格应该已经扣除所有同业折扣以及现金折扣，应为考虑所有优惠后的最有竞争性价格，不得再以其他形式进行标后优惠，否则视为不诚信行为记入供应商诚信记录。投标报价应已经包含了购买相关服务的费用和所需

缴纳的所有税费，并包含了完成全部服务内容所需的一切费用。

**12.2** 投标人提供的相关系统及服务，应当符合国家有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

**12.3** 投标人应按照招标文件中提供的投标文件格式完整地填写开标一览表、报价明细表和报价构成表等，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

**12.4** 除招标文件说明并允许外，投标的每一种服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价将可能导致投标被拒绝。

**12.5** 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均将予以拒绝。

### **13. 投标保证金**

本项目不收取投标保证金。

### **14. 投标文件的有效期**

**14.1** 自开标日起 90 天内，投标文件应保持有效。有效期短于该规定期限的投标，将被拒绝。

**14.2** 在特殊情况下，采购中心可与投标人协商延长投标文件的有效期。这种要求和答复都应以书面形式进行。此时，按本须知规定的投标保证金的有效期也相应延长。投标人可以拒绝接受延期要求而不会被没收保证金。同意延长有效期的投标人除按照采购中心要求修改投标文件有效期外，不能修改投标文件的其他内容。

### **15. 投标文件的签署及其他规定**

**15.1** 组成投标文件的各项文件均应遵守本条。

**15.2** 投标文件中凡招标文件要求签署、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签署和加盖公章。投标人应写明全称。如果是由法定代表人授权代表签署投标文件，则必须按招标文件提供的格式出具《法定代表人授权书》并将其附在投标文件中。投标文件若有修改错漏之处，须加盖投标人公章或者由法定代表人或法定代表人授权代表签字或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

**15.3** 投标人应按招标文件和电子采购平台电子招投标系统规定的内容、格式和顺序编制投标文件。凡招标文件提供有相应格式的，投标文件均应完整的按照招标文件提供的格式打印、填写并按要求在电子采购平台电子招投标系统上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

**15.4** 用于网上招投标系统上传的扫描件等有关文件应确保清晰、可辨，投标人上传文件的电子数据量不应过大，因数据量过大导致无法正常投标、开标的，投标人将自行承担其责任后果，招标人不承担任何责任。

## **四、投标文件的递交和解密（开标）**

### **16. 投标文件的递交和解密**

**16.1** 投标单位在制作投标文件后应在上传投标文件截止时间之前在上海政府采购网上将电子投标文件加密上传。

**16.2** 举行开标会时，各投标供应商须带好本单位的 CA 证书及可以无线上网的笔记本电脑，按照规定的开标时间和地点到场后登陆上海政府采购网集中解密。按有关规定当场无法解密的供应商将被取消投标资格，不纳入评审范围。

**16.3** 在投标文件解密之后，投标人不得撤回投标。投标后撤回投标文件的行为将被记录在案，投标人今后参与同类政府采购项目的机会可能会受到影响。

## 17. 投标截止时间

**17.1** 投标文件须按照招标文件规定的投标时间、地点解密。

**17.2** 采购中心推迟投标截止时间时，将通过“上海政府采购网”（<http://www.zfcg.sh.gov.cn>）公开发布。在这种情况下，采购中心和投标人的权利及义务将受到新的截止期的约束。

## 五、评标

### 18. 评标

**18.1** 采购中心根据有关法律法规和本招标文件的规定，结合本招标项目的特点组建评标委员会，对具备实质性响应的投标文件进行评估和比较。评标委员会由采购人代表和上海市政府采购评审专家组成，其中专家的人数不少于评标委员会成员总数的三分之二。

### 18.2 评标原则

- (1) 评标应严格按照招标文件的要求和条件进行；
- (2) 评标委员会只对实质上响应招标文件的投标进行评价和比较；
- (3) 评标委员会分别对每包进行独立评标，每包只限确定一家供应商为中标单位，但一家供应商可以中一包或多包；
- (4) 评标委员会在评标时除考虑投标报价因素外，同时还根据各项技术和服务因素对投标人和投标服务进行综合评价。

**18.3 评标办法：**本项目采用综合评分法，各评标因素所占权重见第六部分评标办法。

## 19. 对投标文件的初审

**19.1** 开标后，采购中心将组织对投标文件进行资格性检查，依据法律法规和招标文件的规定，对投标文件中的资格证明、投标保证金等进行审查，以确定投标供应商是否具备投标资格。

**19.2** 在详细评标之前，评标委员会对通过资格性检查的投标文件进行符合性检查，依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

(1) 实质上响应的投标是指与招标文件的全部条款、条件和规格相符，没有重大偏离或保留。

(2) 重大偏离或保留系指投标人货物的质量、数量和交货期限等明显不能满足招标文

件的要求，或者实质上与招标文件不一致，而且限制了采购中心的权利或投标人的义务，纠正这些偏离或保留将对其他实质上响应要求的投标人的竞争地位产生不公正的影响。

(3) 重大偏离不允许在开标后修正，但采购中心将允许修正投标中不构成重大偏离的地方，这些修正不会对其他实质上响应招标文件要求的投标人的竞争地位产生不公正的影响。

(4) 如果实质上没有响应招标文件的要求，评标委员会将予以拒绝，投标人不得再对投标文件进行任何修正从而使其投标成为实质上响应的投标。

19.3 初审中，投标文件中如果有下列计算或表达上的错误或矛盾，将按以下原则或方法进行修正；其他错误或矛盾将按不利于出错投标人的原则进行修正：

(1) 开标一览表内容与报价明细表及投标文件其他部分内容不一致的，以开标一览表内容为准。

(2) 如果以文字表示的数据与数字表示的有差别，以文字为准修正数字。如果大小写金额不一致的，以大写金额为准。

(3) 单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

(4) 修正后的结果应对投标人具有约束力，投标人不同意以上修正，其投标将被拒绝。

19.4 评标委员会对投标文件的判定，只依据投标文件内容本身，不依据任何外来证明。

## 20. 投标的澄清

20.1 评标委员会有权要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容等作必要的澄清、说明或者补正。投标人必须按照评标委员会通知的澄清内容和时间做出澄清。必要时评标委员会可要求投标人就澄清的问题作书面答复，该答复经投标人的法定代表人或投标人代表的签字认可，将作为投标文件内容的一部分。澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

20.2 如评委会一致认为某个投标人的报价明显不合理，有降低质量、不能诚信履行的可能时，评标委员会有权通知投标人限期进行解释。若该投标人未在规定期限内做出解释，或作出的解释不合理，经评标委员会取得一致意见后，可拒绝该投标。

## 21. 评标过程保密

21.1 开标之后，直到授予投标人合同止，凡是属于审查、澄清、评价和比较投标的有关资料以及授标意向等，均不向投标人或其他与评标无关的人员透露。

21.2 在评标期间，投标人企图影响采购中心或评标委员会的任何活动，将导致投标被拒绝，并由其承担相应的法律责任。

## 六、授予合同

### 22. 合同授予标准

22.1 买方将把合同授予符合招标文件的要求，并能圆满地履行合同的，对买方最为有利的

得分最高的投标方。

**22.2 最低报价不是被授予合同的保证。**

**23. 买方接受和拒绝任何或所有投标的权利**

买方保留在授标之前任何时候接受或拒绝任何投标，以及宣布招标程序无效或拒绝所有投标的权利，对于受影响的投标人不承担任何责任，也无义务向受影响的投标人解释采取这一行动的理由。

**24. 采购中心宣布废标的权利**

**24.1** 出现下列情况之一时，采购中心有权宣布废标，并将理由通知所有投标人：

- (1) 符合专业条件的投标人或者对招标文件作实质性响应的投标人不足三家的；
- (2) 出现影响采购公正的违法、违规行为的；
- (3) 投标人的报价均超过了采购预算，采购人不能支付的；
- (4) 因重大变故，采购任务取消的。

**24.2** 有下列情况之一的投标文件，将做无效投标处理：

- (1) 投标文件无法按规定解密；
- (2) 不具备招标文件中规定的资格要求的；
- (3) 投标报价不按招标文件规定的计价办法投报或超过招标文件规定的预算金额或投标最高限价；
- (4) 投标文件未按招标文件要求签署、盖章的；
- (5) 未按规定格式填写,内容不全或字迹模糊,辨认不清；
- (6) 经行贿犯罪档案查询，被政府采购监督管理部门禁止参加政府采购活动的；
- (7) 经信用信息查询，投标供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；
- (8) 不同投标人的投标文件出现了评标委员会认为不应当雷同的情况；
- (9) 投标人递交两份或多份内容不同的投标文件，按招标文件规定提交备选投标方案的除外；
- (10) 投标文件未对招标文件作出完全的、实质性响应,导致投标无效；
- (11) 投标文件含有采购人不能接受的附加条件的；
- (12) 单位负责人或法定代表人为同一人，或者存在直接控股、管理关系的不同供应商，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效；
- (13) 因不可抗力造成投标文件遗失或损坏的。

**25. 中标通知**

**25.1** 评标结束后，采购中心将向中标单位签发《中标通知书》，《中标通知书》一经发出即

发生法律效力。

**25.2** 采购中心同时通过指定网络发布评标结果公告。采购中心对未中标的投标人不作未中标原因的解释，不退还投标文件。

**25.3** 中标通知书是合同的组成部分。

## **26. 签定合同**

**26.1** 中标人应按采购中心规定的时间、地点与采购人签定中标合同。中标人不得再与采购人签署订立背离合同实质性内容的其它协议或声明，否则按开标后撤回投标处理。

**26.2** 中标人应按照招标文件、投标文件及评标过程中有关的澄清文件的内容与采购人签订合同。

**26.3** 投标人一旦中标，签订合同后，未经监管部门书面同意不得转包，否则将被视为中标后撤回投标处理。

## **27. 履约保证金**

**27.1** 中标人在总合同签定后十五（15）天内，应按照合同条款的规定，按照招标文件中提供的履约保证金格式向买方提交履约保证金。

**27.2** 如果中标人没有按照投标人须知第 26 条、第 27.1 条规定执行，买方将有充分理由取消原中标决定并没收其投标保证金。在此情况下，买方可将该标授予下一个综合评标得分最好的投标人，或重新招标。

## **28. 腐败和欺诈**

**28.1** “腐败行为”是指提供、给予、接受或索取任何有价值的东西来影响采购人员在采购过程或合同实施过程中行为；“欺诈行为”是指为了影响采购过程或合同实施过程而谎报事实，损害采购人的利益，包括投标人之间串通投标（递交投标书之前或之后），人为地使投标丧失竞争性，损害采购人从自由公开竞争中所能获得的权益。

**28.2** 如果买方认为所建议的中标人在本合同的竞争中有腐败和/或欺诈行为，则将拒绝该授标建议。

## **七、中标服务费**

### **29. 中标服务费**

**29.1** 本次招标不收取中标服务费，请投标人在测算投标报价时充分考虑这一因素。

## **八、询问和质疑**

### **30 询问和质疑**

**30.1** 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

**30.2** 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，

对招标文件的质疑，应当在其收到或下载招标文件之日起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。投标人提出质疑应当坚持依法依规、诚实信用原则，并应在法定质疑期内一次性提出针对同一采购程序环节的质疑。

30.3 质疑函应明确阐述招标文件、招标过程或中标结果中使自己合法权益受到损害的实质性内容，具体、明确的质疑事项和与质疑事项相关的请求，提供相关事实依据、必要的法律依据和证据及其来源或线索，以便于有关单位调查、答复和处理。

30.4 招标人将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人和其他有关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

30.5 对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的，招标人将通知提出询问或质疑的投标人，并在原招标公告发布媒体上发布变更公告。

30.6 投标人提起询问和质疑，应当按照《徐汇区政府采购中心质疑答复处理规程》的规定办理。质疑函应当由质疑供应商法定代表人签字并加盖公章。质疑函应当按照财政部制定的范本填写，范本格式可通过中国政府采购网 (<http://www.ccgp.gov.cn>) 右侧的“下载专区”下载。质疑供应商委托代理人办理质疑事务的，应当向徐汇区政府采购中心或徐汇区卫生事业管理发展中心提交供应商法定代表人签署的授权委托书和身份证明。质疑函的递交可以采取邮寄、快递或当面递交形式。涉及采购需求技术内容的质疑，请向徐汇区卫生事业管理发展中心提出，联系人：施骥达，联系电话：54012832，通讯地址：三江路 89 号 519 室；其余质疑内容请向徐汇区政府采购中心提出，接收质疑函的联系人：柳老师，联系电话：021-24092222\*2591，通讯地址：上海市南宁路 969 号。

## 九、保密和披露

### 31. 保密和披露

31.1 投标人自领取招标文件之日起，须承诺承担本招标项目下保密义务，不得将因本次招标获得的信息向第三人外传。

31.2 采购中心有权将投标人提供的所有资料向其他政府部门或有关的非政府机构负责评审标书的人员或与评标有关的人员披露。

31.3 采购中心有权在认为适当时，或在任何第三人提出要求（书面或其他方式）时，无须事先征求中标人同意而披露关于已订立合同的资料、中标人的名称及地址、中标货物的有关信息以及合同条款等。

### 第三部分 招标技术需求

#### 一、项目概况

以“泛在智能、集约高效、绿色低碳”为核理念，聚焦大模型开发与AI技术应用，依托“通用计算+智能计算”双引擎，将为医疗数据治理等提供强大算力，推动卫健行业大模型创新。

#### 二、项目内容

以云资源底座为基础，支撑区内算力资源持续高速发展，赋能各类数字转型场景，并提供区内核心应用系统部署及全面的安全能力。本次通过采购信息化服务的方式为区内数字化转型提供坚实的基础。

本次项目配套环境规划部署在三江路 89 号机房，按电子政务网络安全要求，本次卫健分支节点划分在政务外网区，用于为区内政务外网侧医疗卫生业务提供云资源部署环境。120 天内提供完整服务。

整体信息化服务需求如下：

序号	服务项	服务内容	服务期限
1	上海市徐汇区卫生健康委员会 2025 年卫健分支节点云建设项目（二期）	满足区域内三甲及社区医院大模型应用等需求，云服务商提供完整的云服务，包含云平台服务、基础安全服务、国密安全服务、集成服务、配套物理空间服务及运维服务，资源池需通过等保三级及密评相关测评。	3 年

#### 三、项目要求

##### 3.1 总体服务要求

本期项目基于卫健分支节点一期项目进行扩容，提供国产化资源池及智算服务，并满足等保三 2.0 及国密测评要求。本次项目将采用统一的资源池化技术，实现计算资源池、存储资源池等能力，支持一键式基于资源池快速分配业务应用所需的资源，避免传统架构下的物理资源分布及繁琐的部署过程。云平台具备便捷的横向扩展能力，同时，云平台提供支持多租户能力，以实现在一个云平台构建多个管理独立、资源及网络完全隔离的虚拟专有云，以支持多业务系统独立部署或开发测试隔离的需求。

本次项目配套环境规划部署在三江路 89 号机房，按照电子政务网络安全要求，本次卫健分支节点扩容划分在政务外网区，用于为区内政务外网侧医疗卫生业务提供云资源部署环境。

本次卫健分支节点云建设项目扩容所涉及的硬件与软件均以三年租赁的服务方式提供（从整体部署安装完毕、正常运行起算）。所涉及的各组件满足国家安全可控政策。本次提供卫健分支节点扩容国产化专区服务资源需不少于 190 核 CPU、1800G 内存，40TB 的全闪存储和 120TB 的对象存储资源，同时，提供智算服务，提供不少于 128 GPU 卡，单卡 F16 算力不低于 280TFlops，总算力不低于 30PFlops (FP16)、并提供不少于 80TB AI 存储资源及 400G 高速集群网络及配套物理空间的资源。

本次项目提供的云平台能力应包括：云服务器、云硬盘、对象存储、弹性伸缩服务、镜像服务、私有网络、智算服务、SDN 网管平台、云解析、云堡垒机、主机安全、数据安全审计、高级威胁检测系统、云平台国密套件、密钥管理服务、安全运营中心、Web 应用防火墙、云监控、运营平台、运维平台等服务。

上述资源需提供配套的云平台服务，且需满足如下总体设计要求：

- **高安全性：**投标人所投云平台服务应经过国家信息安全测评，并获得信息安全服务资质证书；所提供的云平台服务应符合工信部信息技术服务标准，并获得符合性证书。
- **高性能性：**所提供的云平台服务需采用经过大规模商用实践检验的架构方案和软硬件产品选型；云平台应具备自动部署能力，支持快速部署。
- **高可用性：**投标人及原厂商须保证项目整体方案内软硬件的兼容性。所提供的云平台服务应支持主流厂商多样化服务器（包括国产化 X86 架构和国产化 ARM 架构）、网络设备、安全设备的统一管理；应具备支持多中心多活的能力，并从硬件设备冗余、链路冗余等方面充分保证整体系统的可用性；云平台所提供的软件产品之间应为松耦合关联、无依赖关系，单组件部署时不会影响其他组件的运行。
- **高扩展性：**所提供的云平台服务应具备支持大规模服务器的纳管能力，可支持单数据中心不少于 1 千台物理服务器；应支持平滑升级，升级过程对所提供的云服务、云上资源及应用均无影响，并承诺服务期内 3 至 6 个月发布一次小版本、1 至 2 年发布一次大版本；需支持纳管徐汇区已有的裸金属服务器。
- **高可管理性：**所提供的云平台服务需具备运维和运营能力，并支持在徐汇区级云管理平台进行统一资源查看。

卫健分支节点云建设项目需在约定服务期内，提供云平台服务、基础安全服务、国密安全服务、集成服务、配套物理空间服务及运维服务，并满足相关功能、配置、数量和性能要求。

### 3.2 云平台服务要求

卫健分支节点云建设项目需提供云平台服务能力，包括但不限于：云主机服务、弹性伸缩服务、镜像服务、云硬盘服务、对象存储服务、虚拟私有云服务、弹性负载均衡服务、弹性 IP 配置服务、云解析服务、NAT 网关服务、智算服务、专线支持服务、云运维服务、云运营服务。

云平台要具备如下能力：

#### 3.2.1 云主机服务能力

需在不超分的情况下提供国产化专区服务资源不少于 190 核 CPU、1800G 内存，并配套相应的云主机服务，可根据业务需要支持随时创建或释放任意多台云主机。云主机服务需提供且不限于以下能力：

功能名称	功能需求说明
技术先进性	原厂商应具备专有云虚拟化等核心技术的自主知识产权。
自主可控	云主机管理系统是原厂商自主研发并自主可控，不采用不具有自主可控能力的 OpenStack 架构。
云主机管理	可创建、删除、启动、关闭、查看（含批量）云主机。
规格调整	可根据业务需要调整云主机配置和规格，支持升级、降级 vCPU 和内存。
挂载/卸载磁盘	云主机创建成功后，可根据要求，将已有云硬盘挂载给云主机，或创建新的磁盘，然后再挂载至云主机。同时，也可将磁盘从云主机中卸载。虚拟云主机可支持最大挂载 20 个云硬盘。
挂载/卸载网卡	当业务需要多个网卡时，可在创建云主机时进行挂载，也可在创建完成后进行挂载。同样，也可将已经挂载在云主机中的网卡卸载。

功能名称	功能需求说明
标签管理	为云主机添加标签，可方便用户识别和管理拥有的云主机资源。用户可在创建云主机时添加标签，也可在云主机创建完成后添加标签。
反亲和性	反亲和性指的是同一组云主机尽量分散地创建在不同的宿主机上，提高业务的可靠性。
用户数据注入	在创建云主机时，应提供用户初始化的能力。
密码和密钥对	云主机登录时需要进行身份验证，可以通过密码、密钥对来完成。用户可以对密码进行重置。
配置、更改安全组	安全组创建后，用户可在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云主机出入方向网络流量进行访问控制，当云主机加入该安全组后，即受到这些访问规则的保护。
冷/热迁移	支持云主机冷/热迁移，支持对批量云主机进行热迁移操作。
宕机疏散	当承载云主机的节点发生宕机时，平台应有将该节点上的云主机自动疏散至其它节点的能力，疏散完成后，云主机可正常登录。
救援模式	支持通过云主机控制台一键进入救援模式，通过自动加载的方式，解决当引导文件丢失、系统关键文件缺失等原因导致的系统无法启动的问题。

### 3.2.2 弹性伸缩服务能力

需提供弹性伸缩服务，可在区云的使用过程中，根据业务需求通过策略自动调整其业务资源。弹性伸缩服务需提供且不限于以下能力：

功能名称	功能需求说明
伸缩组生命周期管理	支持创建、修改、删除、启停、查询伸缩组。
设置最大、最小、期望实例数	支持设置伸缩组最大实例数和最小实例数，保证伸缩组在任何情况下，实例数均不会超过最大实例数和最小实例数的范围，同时可以使伸缩组的实例数始终自动保持和期望实例数相同。

功能名称	功能需求说明
搭配负载均衡	支持为伸缩组设置自动绑定的负载均衡监听器。
设置多 AZ	支持为伸缩组设置分属多个 AZ, 使伸缩过程中将虚拟机实例平均分配至不同 AZ, 保证伸缩组中部署应用的容灾能力。
设置多子网	支持为伸缩组设置多个子网, 为虚拟机绑定多块网卡。
健康检查	支持设置伸缩组健康检查周期、健康检查方式和健康状况检查宽限期。
伸缩活动日志	查询伸缩组伸缩活动日志, 支持查看伸缩组历史伸缩活动信息, 支持按时间范围筛选。
查看伸缩组监控数据	支持查看伸缩组内实例的监控数据: 实例数、CPU 利用率、内存利用率、带内网络流入流出速率、磁盘读写速率、磁盘读写操作速率。
资源标签	资源标签, 通过标签的形式将自定义数据分配给每个伸缩组内的虚拟机, 可以对组内的虚拟机进行组织和管理。
设置实例保护	当伸缩组发生自动缩容活动时, 设置了实例保护的实例将不会被移除伸缩组。
伸缩配置生命周期管理	支持创建、查询、删除(包括批量删除)伸缩配置。
拷贝伸缩配置	根据现有伸缩配置拷贝并修改生成新的伸缩配置。
设置自动绑定公网地址	为扩容出的虚拟机实例自动绑定公网 IP。
伸缩策略生命周期管理	创建、修改、删除、启停、查询伸缩策略, 批量启用、停用、删除伸缩策略。
伸缩策略类型	支持三种伸缩策略类型: 定时, 周期, 告警。
支持通过多种监控指标触发	告警策略支持通过多种监控指标触发: CPU 利用率、内存利用率、带内网络流入流出速率。

功能名称	功能需求说明
伸缩策略动作定义	伸缩策略支持定义触发动作，可设置增加、减少。
手动触发伸缩策略	支持手动触发执行伸缩策略。

### 3.2.3 镜像服务能力

需提供镜像服务，提供且不限于以下能力：

功能名称	功能需求说明
查询镜像列表	根据不同条件查询镜像列表信息。
更新镜像	更新镜像相关属性值。
镜像生成	可通过云主机、云主机备份、云硬盘及外部镜像文件制作镜像。
镜像导出	用户可将自己的私有镜像导出到指定的对象存储中，也可将自己的私有镜像导出到本地。
私有镜像	租户可基于弹性云服务器或外部镜像文件创建个人镜像，包括操作系统、预装的公共应用、用户的私有应用及用户的业务数据等，仅租户自己可见。
私有镜像共享	支持将私有镜像共享给其他用户使用。
公共镜像	包含常见的操作系统，能够提供简单方便的镜像自助管理功能，对所有用户可见。
自定义镜像上传	支持上传自定义的镜像。
查询镜像配额	查询租户在当前可用区的私有镜像的配额数量。
国产操作系统支持	支持银河麒麟、统信 UOS 等国产操作系统。

### 3.2.4 云硬盘服务能力

全闪存储需在保证三副本架构的前提下，提供 40TiB 的可用存储空间，并配套相应的云硬盘服务，需提供且不限于以下能力：

功能名称	功能需求说明

功能名称	功能需求说明
云硬盘管理	<p>支持创建、删除、查看、挂载、卸载；支持数据盘在线扩容；</p> <p>支持基于已有云硬盘创建云硬盘快照/备份，支持通过云硬盘快照/备份回滚源云硬盘，支持通过云硬盘快照/备份创建新云硬盘；云硬盘快照/备份的后端数据存储池应不同于云硬盘本身的后端数据存储池；</p> <p>根据不同的后端存储介质（如 SATA 与 SSD 盘混合、纯 SSD 盘），云硬盘服务应具备提供多种不同性能规格的云硬盘类型的能力。</p>
云硬盘 QoS	<p>支持 QoS，针对不同云硬盘介质及容量自动限制 iops 与带宽吞吐能力，并支持黑白名单能力。</p>
云硬盘跨介质升级	<p>支持调整云硬盘类型，业务无需中断，支持租户自主调整，支持运营管理员代租户调整。</p>
云硬盘集群扩容	<p>支持存储集群（仓库）的横向扩容能力，扩容期间对原有云硬盘无任何性能影响。扩容后支持新创建云硬盘成功落入新存储仓库。</p>
云硬盘专用存储集群	<p>支持某一个存储集群（仓库）指定给一个租户（用户）使用的能力，实现业务独占物理存储集群的能力。</p>
多故障域	<p>支持多个独立的存储仓库，每一个仓库为独立故障域，单一存储仓库出现灾难性故障时，不能对其它存储仓库有任何影响。</p>
存储集群的自动流控 QoS 能力	<p>存储池（仓库）自带 iops/带宽多个维度的流控策略，自动监测整个存储池的 iops 与流量情况；当触发集群流控值时，存储控制器能自动下发流控策略降低云硬盘的访问速度。</p>
快照功能	<p>支持在线的快照创建能力，云硬盘无需卸载或云主机关机，实现业务不中断的快照备份创建；</p> <p>支持租户针对云硬盘创建快照；支持运营管理员为租户的某块云硬盘创建快照；支持选定某一快照，创建基于该快照数据的新的数据盘；</p>

功能名称	功能需求说明
	支持通过系统盘快照创建新的自定义镜像； 快照的使用不依赖源盘存在，当源盘被彻底删除后快照仍可正常恢复出新的云硬盘。

### 3.2.5. 对象存储服务能力

需在保证三副本架构的前提下，提供不少于 120TB 的对象存储空间，并配套相应的对象存储服务。对象存储服务需提供且不限于以下能力：

功能名称	功能需求说明
对象存储服务	支持多重冗余分布式架构，避免单点故障隐患； 支持数据 SSL 加密传输，控制每个单独文件的读写权限，并支持数据完整性校验；支持服务端加密； 提供界面、命令行、API 等多种途径对存储对象进行批量操作； 支持文件追加上传、断点续传下载； 支持存储桶的创建、列表、查看、删除，单租户最大可创建 200 个存储桶； 支持对象的上传、列举、删除；支持通过桶策略、对象策略、acl 规则等方式对存储桶和对象的访问权限进行管理；支持多版本控制； 支持日志管理、支持生命周期管理； 支持云监控上展示流量统计和请求次数等指标。

### 3.2.6. 虚拟私有云服务能力

需提供虚拟私有云服务 VPC (Virtual Private Cloud, VPC) 服务，用于支持用户自定义私有网络、实现用户资源网络隔离。虚拟私有云服务需提供且不限于以下能力：

功能名称	功能需求说明
私有网络	支持创建私有网络、修改私有网络基本信息、删除私有网络和导出私有网络列表。VPC 支持扩展多个外部网段，每个 VPC 不低于

功能名称	功能需求说明
	5 个。
子网	子网是虚拟私有云下管理云资源的网络平面，云资源都部署在子网内。应支持为虚拟私有云创建新的子网、修改子网网络信息和删除子网。
路由表	路由表中定义路由规则，路由规则用于将目标网段的流量路由至指定的目的地。支持添加自定义路由规则，将指定目标网段的流量路由至指定目的地。应提供管理路由表的功能：如添加自定义路由、查询路由、修改路由和删除路由。
安全组	<p>提供管理安全组和安全组规则的功能：创建安全组、删除安全组、添加安全组规则、快速添加多条安全组规则、复制安全组规则、修改安全组规则、删除安全组规则、查看弹性云主机的安全组、变更弹性云主机的安全组、云资源加入/移出安全组等，并支持批量导入导出安全组规则。</p> <p>支持安全组在多个 VPC、多个 AZ 间复用，安全组支持 IP 列表/端口列表。</p>
网络 ACL (虚拟防火墙服务)	网络 ACL 是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。需支持提供管理网络 ACL 和网络 ACL 规则的功能并支持批量导入导出规则。
对等连接	<p>对等连接是指两个 VPC 之间的网络连接。需支持用户使用私有 IP 地址在两个 VPC 之间进行通信，就像两个 VPC 在同一个网络中一样。同一区域内，用户可在自己的 VPC 之间创建对等连接，也可在自己的 VPC 与其他帐户的 VPC 之间创建对等连接；</p> <p>需可以创建同一账户或不同账户下的对等连接，查看、修改、删除对等连接，查看和删除对等连接路由等；</p>

功能名称	功能需求说明
	同时需支持跨可用区的对等连接。

### 3.2.7. 弹性负载均衡服务能力

需提供弹性负载均衡服务，用于实现应用流量均衡、消除服务单点故障、提升服务可用性。弹性负载均衡服务需提供且不限于以下能力：

功能名称	功能需求说明
支持公网和私网负载均衡	公网负载均衡器可通过公网 IP 对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端云主机进行处理。 私网负载均衡器通过私网 IP 对外提供服务，将来自同一个 VPC 的客户端请求按照指定的负载均衡策略分发到后端进行处理。
支持轮询/最少连接/源 IP 分发策略	负载均衡应支持轮询、最小连接、加权轮询、加权最小连接和源 IP 等算法。
支持四层 (TCP/UDP) 和七层负载均衡 (HTTP/HTTPS)	四层负载均衡：支持 TCP 和 UDP 协议，监听器收到访问请求后，将请求直接转发给后端服务器； 七层负载均衡：支持 HTTP 和 HTTPS 协议，监听器收到访问请求后，需要识别并通过 HTTP/HTTPS 协议报文头中的相关字段，进行数据的转发。七层负载均衡应支持加密传输、基于 Cookie 的会话保持等高级功能。
支持会话保持	会话保持功能应可以识别客户端与服务器之间交互过程的关联性，在作负载均衡的同时，还保证一系列相关联的访问请求会保持分配到同一台服务器上。
支持按域名和 URL 转发	通过添加转发策略支持自行设定的域名和 URL，将来自不同域名或者不同 URL 的请求转发到不同的后端服务器组处理。 需支持协议类型为 HTTP、HTTPS 的监听器。
支持访问控制	支持通过添加白名单的方式控制访问负载均衡的监听器的 IP，能够设置允许特定 IP 访问，而其他 IP 不许访问。

功能名称	功能需求说明
支持后端服务器为基础 网络	负载均衡支持基础网络的后端服务器。
支持双向认证	支持对通信双方的身份都做认证，以确保业务的安全性。除了配置服务器的证书之外，还需要配置客户端的证书，以实现通信双方的双向认证功能。
支持按监听器粒度监控 相关指标	云平台提供的云监控服务，可以对弹性负载均衡器的运行状态进行日常监控。用户可以通过管理控制台，直观地查看弹性负载均衡器的各项监控指标。
HTTP 重定向到 HTTPS	支持将 HTTP 访问重定向至 HTTPS，客户端 HTTP 的访问请求，后端服务器返回 HTTPS 的响应。
负载均衡器管理	创建、修改、启停、删除、查看负载均衡器。
监听器管理	创建、修改、删除、查看。
后端服务器管理	添加、修改、删除、查看后端服务器，允许添加 IP 地址。
健康检查管理	通过健康检查来判断后端服务器是否可用。 对于四层（TCP）和七层（HTTP/HTTPS）监听器，用户可以配置 TCP 健康检查；四层（UDP）监听器默认配置 UDP 健康检查； 对于四层（TCP）和七层（HTTP/HTTPS）监听器，用户可以配置 HTTP 健康检查；添加、关闭健康检查，支持端口、检查周期、超时时间、检查路径、最大重试次数等配置。
证书管理	支持两种类型的证书，服务器证书和 CA 证书； 支持创建、更换证书，查看证书关联的监听器等；负载均衡监听器支持 SNI 多个 SSL 证书。
标签管理	通过云资源标签，快速查找具有某标签的云资源，可对这些资源标签统一进行检视、修改、删除等操作，方便用户对云资源的管理。 支持为负载均衡器、监听器等添加标签，修改和删除标签。

### 3.2.8. 弹性 IP 配置服务能力

需提供弹性 IP 配置服务, 提供且不限于以下能力:

功能名称	功能需求说明
绑定/解绑到云主机	绑定到云主机, 实现云主机连接公网或政务外网, 并支持解绑。
绑定/解绑到裸金属	绑定到裸金属, 实现裸金属连接公网或政务外网, 并支持解绑。
绑定/解绑到 NAT 网关	绑定到 NAT 网关, NAT 网关通过与弹性 IP 绑定, 可以使多个云主机(弹性云主机、裸金属服务器、云桌面等)共享弹性 IP 访问公网或政务外网, 并支持解绑。
上下行带宽配置	支持配置上下行带宽限制。

### 3.2.9. 云解析服务能力

需提供云解析服务, 提供稳定、高效、安全灵活的 DNS 解析以及流量调度能力。云解析服务需提供且不限于以下能力:

功能名称	功能需求说明
内网域名 解析	内网域名 支持创建在关联 VPC 内生效的内网域名, 并为域名提供内网 DNS 解析服务, 提供创建、修改、删除、查看内网域名等基本操作。
	关联 / 解关联 VPC 支持为内网域名关联或者解关联 VPC。
	记录集 记录集是一组资源记录, 用于定义域名的解析类型以及解析值; 支持为内网域名添加 A、CNAME、MX、AAAA、TXT、PTR 等类型的记录集, 还支持修改、删除以及查看记录集。
	泛解析 支持为内网域名的所有子域名添加记录集, 为所有子域名提供解

功能名称		功能需求说明
		析服务。
	TTL	支持设置解析记录在本地 DNS 服务器的缓存时间。
	批操作	支持批量删除域名列表中的内网域名。
反向解析	反向解析	支持通过弹性 IP 获取该 IP 地址指定域名的反向解析服务, 提供创建、修改以及删除反向解析。
	TTL	支持设置解析记录在本地 DNS 服务器的缓存时间。
权限	权限管理	用户可使用统一身份认证服务 IAM 对其所拥有的云解析服务进行权限管理, 可基于组织划分、职能划分设置不同的访问权限。
资源管理	配额调整	支持限定各类资源的配额、防止资源滥用。可对用户的资源数量和容量做限制, 包括用户最多可以创建多少公网域名、内网域名、记录集或者反向解析;  如当前资源配额无法满足业务需要, 支持用户申请扩大配额。

### 3.2.10. NAT 网关服务能力

需提供 NAT 网关服务, 提供网络地址转换能力。NAT 网关服务需提供且不限于以下能力:

功能名称		功能需求说明
	SNAT	支持 SNAT, 支持多个云主机通过同一公网 IP 主动访问公网。
	DNAT	支持 DNAT, 支持绑定到 NAT 网关, NAT 网关通过与弹性公网 IP 绑定, 可使多个云主机 (弹性云主机、裸金属服务器等) 共享弹性公网 IP。
	流量告警	可以设置自定义流量告警, 当指标超过一定阈值时自动告警, 告警消息通过电子邮件、短信等方式发出, 帮助用户提前预警风险。

功能名称	功能需求说明
管理	NAT 网关、SNAT 规则 DNAT 规则管理, 包含创建、查看、修改、删除等。
批量操作	支持批量操作。
高可用	单个 NAT 网关支持绑定多个 EIP 时, 可以设定备份 EIP, 实现主备 EIP 的自动探测和切换。

### 3.2.11. 智算服务

提供基于高规格智算云算力集群硬件和智算云管理软件, 通过 RDMA 网络优化, 满足大模型训练、推理及业务场景的多层级需求, 为智算业务提供高效、弹性的基础资源服务, 并通过算力平台整合算力资源, 实现集中化调度与动态分配策略提升资源利用率, 本期提供不少于 128 GPU 卡, 单卡 F16 算力不低于 280TFlops, 总算力不低于 30PFlops (FP16)、并提供不少于 80TB AI 存储资源及 400G 高速集群网络的资源。

#### 1、算力基础平台

功能名称	功能需求说明
计算虚拟化	支持虚拟机规格的在线调整, 包括 CPU、内存等资源, 不用重启即可生效。
	支持对虚拟机打一致性快照, 当发生故障时保障业务能够快速恢复到快照时间点状态。
	支持将主机的 GPU 设备、SSD 设备直通给虚拟机, 提升虚拟机的整体性能。
	支持虚拟机启动阶段的负载均衡策略, 虚拟机启动时根据集群内主机的实时 CPU、内存负载情况动态选择运行的主机。
	支持通过文件夹对虚拟机进行分组, 不同类型的虚拟机实现逻辑分组管理, 方便运维, 文件夹深度最多可以支持 5 层, 并可以对分组虚拟机批量进行关闭、启动、重启、迁移等操作。
	支持在 ARM 场景下导出 OVF 模板。

	<p>支持动态电源管理 (DPM) , 系统可根据集群的负载情况, 自动上下电主机, 优化数据中心的能耗, 达到节能减排的目的。</p>
	<p>使用块存储场景下, 虚拟机支持在线导出 OVF 格式模板, 用于虚拟机本地备份或者导入其他平台。</p>
	<p>使用块存储场景下, 支持对虚拟机进行克隆、开机状态下导出为模板。</p>
	<p>支持在线和离线迁移带快照的虚拟机。</p>
存储虚拟化	<p>每个虚拟机拥有独立的存储 LUN, 可以支持将 VM 的快照, 克隆, 复制的能力卸载到存储, 以节省主机资源开销。</p>
	<p>虚拟化平台使用存储设备时, 须支持本地硬盘、IP-SAN、NAS 等不同类型的存储设备, 无需限制虚拟交换模式。</p>
	<p>为提升数据安全性, 对接远端存储时, 要求指定对接存储时的 CHAP 信息, 支持配置对接存储的存储 IP 以及端口号</p>
	<p>支持只迁移虚拟机存储, 在迁移设置可指定磁盘的目的配置模式并指定迁移速率控制。</p>
网络虚拟化	<p>支持对接硬 SDN 能力。</p>
	<p>支持配置虚拟交换机, 可通过设置安全组、微分段、DHCP 隔离、广播抑制等能力保障虚拟机网络安全。</p>
	<p>支持虚拟交换机级别的用户态交换技术 (OVS+DPDK) , 可实现高性能网络转发, 提高数据处理性能和吞吐量, 提高数据平面应用程序的工作效率。</p>
	<p>虚拟交换机采用主从 VLAN 实现相同端口组的虚拟机网络设备之间的相互通信或隔离, 以满足减少 VLAN ID 大量消耗和降低网络维护难度的诉求 (MUX VLAN) 。</p>
	<p>虚拟机主动链路故障检测 (包括链路状态、丢包率) , 提升虚拟化网络监测效率。</p>
	<p>在管理网络平面和业务网络平面共用物理网卡时, 支持设置两个网络平面之间带宽的比例, 当物理网卡总带宽不足时, 保障平台管理功能的稳定性。</p>

模型使能	提供模型导入、查询、修改、删除的能力，兼容主流的大语言模型、embedding 模型，包括：Qwen-14B、Qwen-72B、Qwen2-72B、ChatGLM3-6B、LLaMA3 8B、LLaMA3 70B、bge-zh-large-v1.5，bge-reranker-large，Qwen2.5 全系列，Qwen2.5-VL 多模态系列，DeepSeek-R1/V3 671B 满血量化版。
	支持模型多版本能力，支持 Checkpoints 归档为模型新版本。
	支持模型回收站和软删除能力，提供一键恢复已删除模型及其版本。
	支持部分模型的量化权重转换，具体范围请参考用户指南。
	支持模型微调训练任务，提供全参和 LoRA 两种模型微调方式，支持基于 MindIE 和 MindSpeed-LLM 提供 NPU 芯片平台的推理和训练的加速能力。
	支持 TP、PP 等训练策略配置，支持训练超参数自定义配置。
	支持模型权重格式转换，支持训练时自动将 safetensors 格式的权重转换为按照 Megatron 分布式训练策略拆分后的 mcore 格式，也支持在 Checkpoints 归档时将训练后的 Megatron mcore 格式的权重转换为 safetensors 格式。
	支持单机多卡分布式推理服务部署，提供统一网关提供多模型的统一访问入口，支持 SK 认证。
	支持多实例推理服务部署和多推理实例负载均衡。
	支持 MoE 模型大规模专家并行推理服务部署。
	支持多模态大模型的推理服务部署。
	通过自定义镜像支持 LLM、CV、OCR、ASR 等模型推理服务。
	支持使用第三方评测数据集和自定义评测数据集对大模型进行性能和精度评测。
	支持对评测结果进行可视化分析和导出下载。
	支持基于 Jupyter Notebook 开发环境提供模型开发能力，支持 Notebook 的检索、创建、删除、启动和停止，在 Notebook 内，支持 Python 代码的编辑和运行。

	模型工程开放模型实例查询、模型推理、文本向量化（embedding）、文本的重排序（rerank）等北向 API。
弹性容器引擎服务	支持一个平台提供容器和虚拟机双栈管理，包括容器集群、容器镜像、应用模板、应用实例的可视化管理。
	为防止多次升级影响业务，支持跨社区版本升级 K8S 集群，升级过程中不重启业务 Pod，以保证客户业务不中断。
	支持通过 WebCLI 访问 K8S 集群，WebCLI 支持上传 yaml 文件。
	支持通过节点池管理 K8S 工作节点，可通过节点池伸缩工作节点、可批量设置节点标签和注解。
	支持可视化管理应用模板，支持 Helm Chart 应用模板的上传、导出、编辑、删除、历史版本跟踪，可通过 Helm 命令行查询、拉取应用模板。
	支持监控 K8S 集群、节点、应用实例、工作负载性能，提供图形化的指标监控，包括但不限于 CPU、内存、磁盘使用率、磁盘 I/O 写入写出、网络流速等。
	容器引擎（CRI 容器运行时）支持 docker 和 containerd 两种。
	支持基于 yaml 和向导式两种方式创建 K8S 资源。
	支持集群纳管裸机节点。
运营服务能力	提供按多级 VDC（最大 5 级 VDC）管理、资源集、用户组等方式的组织模型管理能力。
	支持对用户按云服务权限进行独立授权，不同用户具有不同的云服务管理权限需求。
	支持服务白名单能力，可以指定服务对组织的可见度设置。
	提供配额管理能力，支持对 VDC、资源集使用的资源做配额限制，包括但不限于虚拟机、裸金属、云硬盘、对象桶、文件共享等服务。
	提供计量报表能力，支持按照 VDC、资源集维度对 VDC/资源集下的云服务资源进行计量统计，并支持按不同维度（VDC、资源集）、不同时间范围、不同云服务类型进行计量报表导出。

	提供流程审批能力，支持管理员预置审批模型，审批模型中可以指定单人审批或者多人会签。租户基于审批模型可以自助创建审批订单，审批订单由审批人审批完成后方可进行资源申请。
运维服务能力	平台或软件支持对存储、交换机、服务器、超融合、虚拟化资源的统一管理，无需多个软件界面分散管理，管理能力包括设备基本信息查询、配置信息查询、历史性能信息、资源利用率查询、设备告警信息查询等。
	提供了虚拟机视角的 IO 路径全链路故障诊断：一个界面展示虚拟盘、虚拟机、主机、交换机、存储设备的 IO 路径级的拓扑信息。
	提供了包含虚拟机、主机、LUN、存储等对象实例的多维度的关联对象分析，快速定位问题。
	支持通过设置快照策略任务对虚拟机进行定时快照，满足日常运维管理诉求。运维人员可设置不同的虚拟机快照策略，可按天、周、月设置执行计划。
	支持用户针对指定的虚拟机配置检查策略，达到策略定义的阈值后自动扩容虚拟机的 CPU 或者内存。过程中虚拟机正常运行不需要重启。
	支持批量对多个虚拟机的 CPU、内存、磁盘硬件参数做变更配置，提升运维效率。
	支持大屏展示，预置超过 3 种大屏；预置超过 20 种图表控件，可支持用户自定义大屏内容。
	支持报表统计，支持周期性自动生成报表，预置容量、资源性能，告警等 30 多种典型业务场景的报表。支持用户自定义报表统计内容。

## 2. 算力调度平台

功能名称	功能需求说明
异构计算架构	为方便用户进行算子开发，应支持算子开发语言，语言原生支持类 C、C++ 进行开发。

	为方便用户基于系统快速开展业务，应提供算子库，算子库支撑多种类别的算子，基础算子不低于 500 个，融合算子不低于 50 个。
框架	支持 Pytorch 不低于 2.4 版本、支持 Python 3.11。 支持使用图模式进行开发，支持离线场景导图、模型编译时间优化、集合通信算子入图功能。
大模型加速库	为方便用户对大模型的研究，应提供大模型开箱即用能力，支持不低于 80 个主流大模型。
应用使能	需提供对接上层调度平台的相关组件，组件应支持资源监测、亲和性调度、故障调度、设备发现功能。 为方便定位定界设备故障，需提供故障诊断工具，工具支持提供日志清洗和故障诊断功能，支持分析故障根因节点以及故障事件。
工具能力	为便于调试算子、模型的精度和性能，支持基于命令行的算子、训练、推理开发工具。 为便于开发者进行算子开发、训练开发、推理开发，提供开发工具，工具支持在 windows 安装部署。 支持模型精度异常可定位功能。 支持训练/微调不中断在线采集 profiling 功能。 支持自动分析模型性能瓶颈功能。 支持模型性能数据可视化功能。 支持算子性能瓶颈分析和可视化。
集群稳定性	支持断点续训和故障检测功能。
集群线性度	支持大模型训练千卡集群线性度 95%以上。
推理引擎	支持自研推理服务化框架等。 支持接口对接社区大语言模型 vLLM、TGI、Triton 等服务化框架。 提供推理运行时组件，支持 ONNX、PyTorch、MindSpore 等框架训练模型平滑迁移，提供一站式调试调优工具，快速界定精度问题及性能瓶颈；支持自定义优化 PASS 及 Plugin，

	提供 Transformer 类高性能算子以及同学、融合、稀疏、量化等算子；支持用户注册自定义算子后基于 RT 框架调用。
	支持多机推理能力。
	支持 PD 分离部署能力。
	支持服务快速部署、服务监控、故障重调度。

### 3、SDN 网管平台

功能名称	功能需求说明
网络数字地图	提供开放的数据采集框架，支持收集域控制器、三方系统、设备配置和表项等，作为运维系统的统一数据底座。
	支持三级网络拓扑，三级网络拓扑分别为：多地多 DC 层级拓扑、单 DC 层级拓扑和单 Region 拓扑。支持呈现拓扑的流量路况，支持查询拓扑的统计信息，且支持在未开启 LLDP 场景下通过 AI 拓扑还原技术还原设备间链路信息，补齐网络拓扑。
	支持展示业务实际部署网络位置；支持呈现业务网络互访关系。
AI 业务发放与网络加速	支持路径还原，输入两个 VM 的 IP，通过仿真还原出两个 VM 之间互通的流量路径（包括云内虚拟网络）。支持业务网络互视，基于业务互访关系对，一键映射网络路径，支持网络路径叠加告警、带宽使用率、时延等路况信息，加速故障定位定界。
	支持 AI 场景 ZTP 零配置开局，即插即用，实现端到端自动化部署。
	AI 场景业务发放：支持提供多租业务自动化发放，使能 AI 多租户安全隔离。
可靠性	支持基于 NSLB 全网负载均衡算法的 AI 网络加速。
	支持业务回滚、租户回滚、全网回滚三级回滚实现网络业务的快速恢复。
	支持故障 1-3-5，对于典型故障，支持智能推荐和评估修复方案，选定方案后自动下发修复方案，完成故障修复闭环。
开放性	南向支持开放可编程框架（AOC），支持三方设备快速适配。
	南向支持 SNMP、Netconf、Openflow(1.3/1.4)、OVSDB、JSON-RPC、

	sflow 等标准协议。
	北向支持 Restful、Restconf、Webservice、Syslog 等接口。
业务链	支持 IETF 标准的服务链 (SFC) 模型。
运维与故障定位	支持从应用到逻辑、逻辑到物理拓扑的映射关系展示。
	网络检测工具：路径探测、环路智能检测、连通性检测。
	运维工具：南北向一致性对账、应急预案、意图验证、替换/故障影响性分析、一键全网检测。
网络安全	支持基于角色的访问控制。
	本地 / 远端认证 (Radius、AD、LDAP)。
安全控制	支持基于角色的访问控制，实现多租户间的隔离和多用户账户和权限的管理。
	支持基于密码的本地认证，及 Radius、LDAP 等安全用户认证。
	支持修改已有用户的密码，支持新增用户。
意图理解仿真	支持基于智能机器人，自动识别意图，智能推荐逻辑网络方案，免业务编排。
	支持多云多 DC 场景逻辑网络设计，无需下发配置至设备即可进行业务编排以及仿真评估。
	支持多云多 DC 场景配置变更前在线仿真：结合设备已有配置和新增配置评估逻辑资源占用及业务连通性。

### 3.2.12. 专线支持服务能力

需提供专线支持服务，用于建立徐汇区城运中心与卫健委分支节点云建设项目机房之间的专属网络连接通道。专线支持服务需提供且不限于以下能力：

功能名称	功能需求说明
物理专线	连接徐汇区城运中心与卫健委分支节点云建设项目所租用机房之间的物理线路连接，在用户的数据中心和云专线网络接入点间建立网络连接。支持添加、查看、修改、删除。

功能名称	功能需求说明
网络地址转换 (NAT)	网络地址转换是对专线两端 IP 冲突问题的一种解决方案。用户可在专线网关上配置网络地址转换规则，网络地址转换 (NAT) 包含 IP 转换和 IP 端口转换两种。
专线共享	支持多个租户共享专线并支持用户自助化。
专线接入安全防护	具备专线链路上的安全防护措施。

### 3.2.13. 云运维服务能力

需提供云运维服务，提供且不限于以下能力：

功能名称	功能需求说明
监控和告警	<p>租户端支持监控面板和监控图表的能力，并支持将实例监控指标进行明细视图和聚合视图的展示；支持针对实例分组绑定告警策略，并支持针对平台事件和产品事件进行跟踪和告警；</p> <p>租户端支持配置告警触发条件、自定义指标阈值和告警信息接口回调；并支持告警的屏蔽、收敛、处理以及模拟告警；</p> <p>租户端/管理端支持监控的自定义 Dashboard 展示。平台运维系统可以自定义新建图标，监控目标产品的指标信息；</p> <p>管理端监控可针对告警级别进行分类，告警级别需支持严重、重要、次要和警告，并支持按照告警级别，归属产品，恢复状态，触发时间段等对告警信息进行查询；监控指标数据和告警数据最长需支持 365 天，同时指标数据需支持定期归档备份；</p> <p>管理端监控需支持和现有的邮件服务器、短信网关或第三方系统进行对接，同时也支持现有系统上报指标和事件数据到云内的监控系统；</p> <p>管理端监控可新建告警策略，告警策略的触发条件中支持配置静态阈值和动态阈值，并支持配置持续时间；支持告警屏蔽，告警屏蔽需支持屏蔽时间段的选择。</p>

功能名称	功能需求说明
日志、巡检和报表	<p>日志平台支持云平台内置组件相关日志的收集和分析，支持收集文本文件、JSON 格式的数据；支持对数据进行过滤、分组，并支持图表下钻；支持日志告警检测和告警消息发送；</p> <p>支持巡检平台，可自定义巡检项，巡检类型支持设置为安全、性能、可用性、可靠性和水位，支持导出巡检报告至表格，并可配置巡检频率；</p> <p>支持报表平台，支持自定义报表生成时间，报表周期支持设置日报、周报和月报，默认报表需支持性能、容量、资源和告警数据统计报表。</p>
运维工具	<p>支持对物理机和虚拟机进行密码入库功能，支持临时密码、长期密码和密钥免密登录，其中临时密码支持重置周期和更换周期的设置，并支持对密码复杂度进行设置；</p> <p>支持 NTP 管理功能，可修改上级时钟源 IP 地址，支持修改上级时钟源地址后，自动轮询重启 NTP 服务器，并支持查看 NTP 服务器的状态和告警历史；</p> <p>支持软件源管理，可通过 rsync、自定义脚本或者手动上传的方式进行数据源设置，并支持以分钟级自动定时同步软件源。</p>
自动化部署和运维	<p>支持对物理服务器进行部署和管理，可对物理服务器进行自动化的安装，部署，开关机，带外账号重置，带外密码导出等功能；并支持操作系统和 raid 字典的管理；</p> <p>支持对网络设备进行管理，可展示网络设备的品牌、型号、状态等信息，支持网络设备之间的信息比较，支持 IDC 机位管理，显示可用区、机架号、已占用机位和剩余机位数等信息；支持网络质量管理，可展示 IDC 出口质量和 LAN 质量；</p> <p>支持业务 CMDB 功能，支持全局搜索，业务管理，模型管理，同步任务管理，数据校验等功能；</p> <p>支持资源交付功能，支持资源的申领、交付和撤销功能，并支持在资源申领环节中嵌入审批流程；</p>

功能名称	功能需求说明
	<p>支持作业工具和包管理，可实现作业的编排和支持定时任务；包发布需支持程序包、配置文件和脚本文件；</p> <p>支持多可用区、多组件的白屏化变化、升级，支持变更过程管控（暂停/继续/重试/跳过/终止），支持变更历史记录和回溯，并支持以下特性：</p> <p>（1）原子操作白屏化管理：能白屏化对原子操作进行增删改查，原子操作可实现变更的自动化、白屏化执行，覆盖部署、变更、升级、扩容等场景。</p> <p>（2）编排&amp;执行能力：能基于原子操作编排部署、变更、回滚、升级、扩容流程，支持原子操作/应用的串并行执行、分组分阶段执行，支持执行过程暂停、继续、重试、跳过、终止等能力，执行过程支持详细日志输出。</p>
API 管理	<p>提供统一的 API 接口在线管理能力，支持云平台所有 API 的在线调用和调试；</p> <p>提供白屏化 API 调用代码生成的能力，代码语言至少包括 java、python、PHP、Node.js、GO 五种常用开发语言。</p>

### 3. 2. 14. 云运营服务能力

需提供云运营服务，提供且不限于以下能力：

功能名称	功能需求说明
客户管理	<p>支持批量创建主账号，并对主账号进行创建子账号、IP 访问限制、锁定、解锁等操作；</p> <p>支持资质审核功能，由管理端审核租户端创建的主账号；支持创建和编辑租户类别，并对租户账号进行分类；</p> <p>支持通过白名单的方式限制某个/某些账号可以/不能访问某类资源，支持通过白名单的方式限制某个/某些账号可以/不能访问某个地域或可用区。</p>

功能名称	功能需求说明
计量	<p>支持查询用量明细，可按照产品、APPID、UIN、实例 ID，时间范围筛选用量明细列表，并支持导出用量明细；</p> <p>针对云产品有默认配额管理，同时支持针对单个租户进行配额管理。</p>
消息管理	<p>系统消息至少可支持通过邮件、短信、站内信或者语音消息查询，并支持客户的自定义渠道对接消息；</p> <p>支持消息模板功能，并支持消息模板的查看、编辑、删除和提交审核功能；</p> <p>消息一级分类至少包含产品消息、安全消息、财务消息和运维消息，并支持用户自定义二级分类。</p>
产品管理	<p>支持运营人员为不同租户设置不同的控制台产品菜单，便于产品的灰度发布。</p>
资源管理	<p>支持租户内设置项目，项目内可以管理资源、人员权限和产品配额；资源实例可以在不同项目之间转入和转出；租户内一个用户可以管理多个项目，项目产品配额用尽后，不允许再新增或转入资源实例。</p>
应用帐号接入	<p>支持将云平台作为统一认证的服务端，通过界面化的配置，应用可复用云平台的帐号登录认证体系，实现用户登录到专有云之后，即可免密访问第三方应用的效果。</p>
运营数据中台	<p>支持云平台自身的数据采集和处理，天然集成云平台 API，支持数据展开、数据映射、自定义数据处理等能力；</p> <p>支持实时数据查询，提供类 SQL 的查询语言 FQL，快速上手支持数据计算，数据预测等高级能力。</p>

功能名称	功能需求说明
可视化中台	支持低代码的灵活配置，支持 10 多种组件覆盖布局、图表、展示、选择器，可自由式拖拽布局，实时预览； 支持数据下钻，多组件数据联动依赖等页面交互配置。
资源容量平台	支持在资源容量平台上查看云服务器，云硬盘，负载均衡等常见资源的容量已使用和总体情况； 支持查看对应产品的容量在某一段时间内的使用趋势。

### 3.3 基础安全服务要求

本次卫健分支节点云建设项目扩容所需的安全服务包括但不限于：堡垒机服务、主机安全防护服务、数据安全审计服务、高级威胁检测服务、密钥管理服务、云平台管控面国密合规服务、Web 应用防火墙服务、安全运营中心服务。本次提供的云安全服务须与提供的云平台服务进行统一运维和运营。

#### 3.3.1. 云堡垒机服务能力

功能名称	功能需求说明
用户管理	支持设置运维用户的有效期，不在有效期内的运维用户无法登录堡垒机； 支持对用户进行分组； 开启 OTP 作为多因子认证时，用户首次登录会自动提示进行 OTP 绑定； 提供小程序进行 OTP 验证，无需单独下载 APP。也可以使用 Google Authenticator 进行验证； 用户可使用短信进行双因子认证； 管理员创建运维用户之后，用户可通过短信验证码自助完成激活，无需管理员分配默认口令； 当运维人员忘记密码时，支持用户通过短信+邮件方式自主重置登录密码。

资产管理	<p>支持的资产协议类型：SSH、SFTP、RDP、MySQL、MariaDB；</p> <p>支持手动和自动同步云租户的云主机和云数据库资产信息；</p> <p>支持手动添加主机和数据库资产纳入堡垒机进行管理；</p> <p>支持对资产进行分组；</p> <p>支持将一个账号批量添加到多台主机；</p> <p>提高设备的安全性，不采用标准的协议端口，平台支持协议服务端口号变更。</p>
权限管理	<p>可基于用户、用户组、资产、资产组、账号、访问操作权限、高危命令权限设置多对多的访问授权关系；</p> <p>针对 Linux 主机，支持对 RZ/SZ 命令、文件上传/下载操作进行控制；</p> <p>针对 Windows 主机，支持对剪切板上行/下行、文件上传/下载操作进行控制；</p> <p>支持根据资产维度查看拥有该资产访问权限的账号；</p> <p>支持根据用户维度查看当前用户拥有的访问权限；</p> <p>支持根据配置的高危命令拦截 Linux 运维操作指令；</p> <p>支持单独展示命令拦截风险事件，使管理员可以快速掌握运维安全风险。</p>
资产运维	<p>运维人员可将经常访问的资产添加到快速访问列表；</p> <p>支持将主机账号信息录入系统后，可以单点登录目标资源，无需分发账号口令；</p> <p>支持通过 web 页面调用 Xshell、SecureCRT、MSTSC、iTerm、Terminal（Mac 自带程序）等工具连接服务器，不改变用户的操作习惯；</p> <p>支持通过访问串直接在客户端访问 Linux 主机、数据库，无需打开堡垒机 Web 页面；</p> <p>支持通过浏览器访问 Linux 主机，无需客户端。</p>

审计管理	针对图形会话，支持审计录像及回放，还原用户的真实操作；
	针对字符会话，可以审计到所有交互内容，可以还原操作过程的命令输入，支持审计录像及回放；
	可根据字符命令定位到运维会话；
	针对文件传输会话，支持对用户文件传输操作（上传、下载）进行详细记录；
	针对数据库会话，支持解析 SQL 语句文本、并进行提取，完整记录用户执行的 SQL 语句；

### 3.3.2. 主机安全防护服务能力

需提供主机安全防护服务，帮助服务器构建安全防护体系。主机安全防护服务需提供且不限于以下能力：

功能名称	功能需求说明
资产管理	<p>支持资产概况、主机概况趋势图、主机标签 TOP5、资源监控概览、账号 TOP5、端口 TOP5、进程 TOP5、软件应用 TOP5、数据库 TOP5、web 应用 TOP5、Web 服务 TOP5、Web 框架 TOP5、Web 站点 TOP5；</p> <p>支持展示所有服务器信息，包括所属的操作系统、防护状态；</p> <p>支持展示资产指纹分类列表，包括各资产指纹项及其对应服务器数量，展示该指纹详情。资产指纹信息包含：资源监控、账号、端口、进程、软件应用、Web 应用、Web 服务、Web 框架、Web 站点。</p>
文件查杀	<p>支持显示所有机器扫描出来的木马文件，并可以查看木马所在的机器，可以对木马进行删除，隔离操作；</p> <p>支持 webshell 查杀：提供常用的 Web 网站类脚本木马后门检测，包含 ASP/PHP/JSP/Python 脚本语言；</p> <p>支持二进制病毒木马检测：提供对二进制可执行类的病毒木马检测，包括 exe、dll、bin 类型文件，并告警用户。</p>
密码破解	<p>支持对暴力破解行为进行审计，审计记录包含破解状态、服务器、来源 IP、来源地、登录用户名、攻击时间、尝试次数信息；</p> <p>支持根据来源 IP 加白名单配置以避免误阻断；</p>

功能名称	功能需求说明
	支持联动网络入侵防护系统，进行阻断攻击源。
高危命令	支持实时监控被审计规则判断为危险的操作，并提供默认规则配置，以及支持用户自定义规则配置； 显示登录用户下发的高危命令记录，可根据日期、APPID、登录用户、高危命令查询记录。
漏洞管理	支持提供系统级漏洞和常用组件类型的漏洞检测，并显示检测结果和导出检测结果，提供修复方案； 支持提供常用 Web 类型的漏洞检测，并显示检测结果和导出检测结果，提供修复方案； 支持提供应急漏洞检测，并显示检测结果和导出检测结果，提供修复方案。
基线管理	检测口令脆弱性，支持 Linux 系统、Windows 系统、MySQL、Tomcat、Rsync 等弱口令检测； 提供 CIS 基线标准，展示不同基线策略下的检测服务器、检测项、基线通过率、基线检测项 TOP5 和服务器风险 TOP5 检测结果信息，支持一键检测和定期检测； 提供等保二级、三级的基线标准检测，展示不同基线策略下的检测服务器、检测项、基线通过率、基线检测项 TOP5 和服务器风险 TOP5 检测结果信息，支持一键检测和定期检测； 支持自定义配置选择等保合规、未授权访问、弱口令、远程代码执行、其他、云安全标准。
系统适配	支持国产化操作系统，包括麒麟：V10, V10 SP1 (64bit)、UOS: 20 (64bit) 等； 支持 Linux 操作系统，包括：CentOS:6, 7, 8 (64 bit)、Ubuntu:9.10 – 20.10 (64 bit)、Debian:6, 7, 8, 9, 10, 11 (64 bit)、RHEL: 6, 7 (64 bit) 支持 Windows 操作系统，包括：Windows server 2012, 2016, 2019、Windows server 2008 R2、Windows server 2003 (limited support)。

功能名称	功能需求说明
安全能力	<p>支持至少每月远程更新能力；</p> <p>TAV 病毒库：支持按月更新，查杀引擎获得国际权威评测 VB100、AVC 认证；</p> <p>漏洞库：支持 10 万+漏洞规则检测，默认开启 3000+热点漏洞检测，根据用户需求开启漏洞规则，新增漏洞按月更新；</p> <p>基线库：支持 3000+基线检测，满足等保及 CIS 标准基线，新增基线支持按月更新。</p>

### 3.3.3. 数据安全审计服务能力

功能名称	功能需求说明
agent 管理	<p>支持手动安装 agent 至数据库服务器或者应用服务器中进行审计；</p> <p>当 Agent 有新版本时，可以在线直接升级，无需用户介入操作；</p> <p>可以实时监控 Agent 的 CPU 使用率、内存使用率、运行状态（运行中、离线、过载停止、手动停止等）。</p>
资产管理	<p>支持一键同步云平台的数据资产信息，无需手动添加；</p> <p>支持主流的云数据库和自建数据库、大数据组件，其中至少包括：</p> <ul style="list-style-type: none"> <li>&gt;云数据库：MySQL、PostgreSQL、SQL Server、MariaDB，NOSQL 数据库 Redis、MongoDB；</li> <li>&gt;自建数据库：MySQL、PostgreSQL、SQL Server、Oracle、MariaDB、Redis、MongoDB、Hbase、Hive；</li> <li>&gt;大数据组件：Hbase、Hive。</li> </ul>
数据库审计	<p>支持数据库操作请求、数据库操作响应实时动态审计，包括对原始 SQL 语句、包长度、操作时间、客户端 IP 地址、端口、数据库用户、数据库表等数据库操作请求信息审计；</p> <p>支持对 SQL 语句执行时间、影响行数、SQL 语句执行返回码等数据库操作响应信息的审计；</p>

	<p>具有高效的快速检索查询功能，支持采用部分匹配模糊查询方式检索审计日志；</p> <p>支持基于风险等级、用户名、命中规则、Session ID、模糊查询、客户端 IP、数据库 IP、数据库端口、数据库名称的审计查询；</p> <p>支持从审计日志、审计会话、审计风险的维度分别进行查询分析，可从审计会话定位到会话中的语句列表。</p>
审计规则	<p>支持按照操作时间、客户端 IP、数据库 IP、数据库名、数据库端口、数据库用户名、表名、操作类型、操作语句、影响行数、执行时间，进行审计规则的设置；</p> <p>支持设置白名单规则，对特定的操作予以放行；</p> <p>内置丰富的审计规则，覆盖违规操作、数据泄露、注入攻击、漏洞攻击等；</p> <p>支持规则快捷配置，可以针对单个资产或所有资产，快捷启用规则配置；</p> <p>应至少提供常见配置、宽松配置和严格配置三个快捷配置组。</p>
审计报表	<p>支持创建单次报表、周期报表，周期报表支持以日、周、月进行设置；</p> <p>支持创建综合分析报告和等保参考报表；</p> <p>支持报表在线查看，并且支持下载报表。</p>
告警设置	<p>支持多种告警方式，包括邮件、短信、站内信；</p> <p>告警内容包括：审计风险告警、Agent 掉线告警、行为规则告警、性能超限告警（QPS、存储超过规格限制）。</p>

### 3.3.4. 高级威胁检测服务能力

需提供高级威胁检测服务，识别网络攻击及高级威胁，并对事件告警原始流量进行留存、方便事后追溯。高级威胁检测服务需提供且不限于以下能力：

功能名称	功能需求说明

功能名称	功能需求说明
密码安全检测	<p>支持按照时间范围展示弱密码、空密码和明文密码的告警数量趋势图；</p> <p>支持对弱密码、空密码和明文密码的敏感内容进行数据脱敏；</p> <p>支持配置弱密码检测模式：一种是规则模式（通过密码类型和密码长度来检测）；另一种是字典模式（即弱密码库），每次新增上限是 100 个，每次导入上限是 1000 个。</p>
勒索病毒检测	<p>支持按照时间范围、资产 IP 和攻击阶段进行搜索，展示内容包括：攻击阶段分布图、资产 IP TOP10 和勒索病毒告警统计列表；</p> <p>支持按照时间范围、资产 IP 和操作类型进行搜索，展示内容包括：SMB 行为的 RENAME/DELETE/READ/WRITE 操作频次图、SMB 行为的 RENAME/DELETE 操作资产 TOP10、低版本 SMB 资产 IP 列表、对外开放 445 端口的资产 IP 列表和 SMB 行为统计列表。</p>
组件安全检测	<p>支持按照时间范围、源 IP、目的 IP、事件名称、CVE 编号或组件名称进行搜索，展示内容包括：告警组件类型分布、组件告警趋势、攻击视角和资产视角；</p> <p>支持下载 PCAP 文件；</p> <p>支持导出组件告警信息。</p>
数据泄漏检测	<p>支持按照时间范围或授权状态进行搜索，展示内容包括：事件趋势、接口 TOP5、请求源 TOP5、泄露事件接口列表和泄露事件请求源列表；</p> <p>支持授权关键词配置；</p> <p>支持数据脱敏功能的开启和关闭。</p>
登录行为分析	<p>支持按照时间范围、IP 地址、账号或协议进行搜索，展示内容包括登录来源统计、登录行为趋势、登录类型分布、爆破账号登录统计、爆破行为统计；支持白名单管理。</p>

功能名称	功能需求说明
邮件安全分析	支持按照时间范围、发件人、收件人、邮件主题或邮件内容进行搜索，展示内容包括：恶意邮件趋势、来源国家统计、发件人统计、收件人统计、钓鱼邮件、邮件伪造、恶意邮件附件和邮件附件类型分布； 支持白名单管理。
域名解析分析	支持按照时间范围、IP 或者域名进行搜索，展示内容包括：DNS 解析类型分析、DNS 解析错误类型分析、DNS 服务器解析列表和动态域名流量分析列表； 支持白名单管理。
高级分析事件	支持对手动添加的资产进行高级风险分析； 支持告警资产的搜索、忽略和查看分析。
资产发现	支持在流量中自动发现资产的功能、支持资产的批量注册； 支持 DHCP 网段配置，指定网段不在资产发现的扫描范围。
SSL/TLS 解密管理	支持 SSL/TLS 卸载解密，用户可导入证书并添加目的 IP 及端口的过滤策略，对 HTTPS 流量解密。
抓包任务	支持根据源 IP、目的 IP、源端口、目的端口、协议建立的全包抓取任务； 支持下载 PCAP 包进行分析。
数据接入	支持流量 Flow 日志采样输出； 支持 HTTP Payload 存储和报文载荷存储配置（仅在流量解析配置页面中，流量日志输出选中 Flow 和 HTTP 字段时，才可进行 HTTP payload 存储和报文载荷存储配置）。

### 3.3.5. Web 应用防火墙服务能力

需提供 Web 应用防火墙服务 (Web Application Firewall, WAF)，用于应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫等网站及 Web 业务安全防护问题。Web 应用防火墙服务需提供且不限于以下能力：

功能名称	功能需求说明

功能名称	功能需求说明
Web 攻击防护	可防御 SQL 注入、命令注入攻击、XSS 跨站脚本攻击、WebShell 木马上传、文件包含、路径穿越类攻击及其他常见 Web 服务器漏洞等攻击。
规则引擎	<p>支持提供基于安全 Web 威胁和情报积累的专家规则集，防护 OWASP TOP10 攻击。可防护 Web 攻击包括：SQL 注入、XSS 攻击、恶意扫描、命令注入攻击、Web 应用漏洞、Webshell 上传、不合规协议、木马后门等通用 Web 攻击；</p> <p>支持规则等级划分，可根据实际业务需要进行规则防护等级设置，并支持对规则集规则或单条规则进行开关设置，可以对预设的规则进行禁用操作，同时提供基于指定域名 URL 和规则 ID 白名单处置策略，进行误报处理。</p>
敏感数据防泄漏	<p>支持自定义的信息泄露防护规则，针对检测到的数据窃取行为，自动启用数据替换策略，将攻击响应传输中的敏感数据，如电话号码，ID 身份证号进行替换隐藏，防止黑客获取业务数据；</p> <p>支持防敏感信息泄露，可匹配手机号、身份证、银行卡号的敏感信息及通过响应码、关键字自定义敏感信息，防护动作支持观察、阻断、全替换、仅显示前 4 位、仅显示后 4 位；</p> <p>支持防信息泄漏支持匹配条件为响应码支持观察。</p>
自定义精准防护	<p>支持精细化基于 IP, URL 路径, Referer, POST, UA 参数的自定义防御规则设置 Web 攻击防护措施，且不限制自定义防御规则数；</p> <p>支持地理区域封禁，对国内大区，省份或国外访问进行黑名单封禁。</p>
CC 防护	<p>支持针对特定请求路径访问频率的识别及控制；</p> <p>支持触发条件开启“封禁访问”或“人机识别”策略模式；</p> <p>支持基于 session 的 CC 防护设置，有效解决因使用相同 IP 出口而导致的误拦截问题；</p> <p>支持自定义惩罚时长最短 1 分钟，最长一周。</p>
IP 管理	<p>支持 IP 黑白名单添加，可将一个或多个 IP 加入黑/白名单，实现精准的访问控制；黑白名单模块支持 IPV6 地址的添加；</p> <p>支持查询 IP 状态信息；</p> <p>支持查询某个 IP 的封堵状态，是否在 IP 黑白名单中，是否触</p>

功能名称	功能需求说明
	触发了 CC 规则、触发自定义人机识别等。
兼容性	支持 HTTP 1.2 及 TLS 1.0/1.1/1.2；支持 HTTP 2.0； 支持 Websocket 协议； 支持 HTTP 和 HTTPS 非标端口； 支持泛域名格式。
日志服务	支持展示指定时间的防护业务网站域名受到的攻击次数、时间、来源、攻击类型、对应的规则 ID 等信息； 支持攻击日志分页显示和导出。
接入防护方式	支持通过 CNAME 接入 Web 应用防火墙，隐藏用户真实源站，将可信流量回源，覆盖云和非云上用户； Web 应用防火墙服务开通后，无需进行业务变更即可完成防护接入，一键绑定云负载均衡（外网 7 层 CLB）实现网站旁路检测和威胁清洗，同时提供一键 bypass 功能，实现业务转发和安全防护分离，稳定可靠。

### 3.3.6. 安全运营中心服务能力

需提供安全运营中心服务，提供一体化安全运营能力、提升安全运营效率。安全运营中心服务需提供且不限于以下能力：

功能名称	功能需求说明
监测中心	支持仪表盘功能，包括今日新增风险资产、今日新增安全告警、今日新增安全事件、今日新增脆弱性、近 30 日新增工单、近 30 日新增调查任务的统计和可视化展示，提供环比昨日的统计及 30 天日均数的统计； 提供今日 TOP 50 风险资产、今日 TOP 50 脆弱性、今日 TOP 50 安全告警、今日 TOP 50 安全事件的统计和列表展示； 支持按照攻击链阶段对安全告警进行分类展示，支持通过可视化地图对安全告警攻击源进行统计和展示； 支持提供系统整体安全态势，包括综合态势大屏，攻击态势大屏，威胁大屏，脆弱性态势大屏，流量态势大屏，资产态势大屏。

功能名称	功能需求说明
	屏，租户安全运营大屏。
告警与事件	<p>支持将采集到的多源数据过滤、归一化及富化后进行统一呈现和展示，包括安全事件名称、事件源 IP、事件目的 IP、事件数据源的统一展示；</p> <p>支持对安全事件直接创建调查任务；</p> <p>支持安全告警的告警名称、受影响资产、源 IP、目的 IP、告警评分及告警状态的分析与展示；支持对安全告警的详情进行详细分析与展示，包括告警攻击链还原。</p>
资产中心	<p>支持对用户环境中的各个资产实现列表管理，包含列表呈现各个资产基本信息，例如资产名称、资产 IP、资产来源、资产分组、该资产近 90 天安全告警数、该资产近 90 天安全事件数、该资产近 90 天脆弱性数等展示；</p> <p>支持选取资产列表中的相关资产以 Excel 表格的形式进行导出；</p> <p>针对单个资产的详细信息，支持提供详细直观的可视化展示，包含该资产的详细信息、安全告警、安全事件及脆弱性的展示；</p> <p>支持自定义资产字段（每类最多 10 个字段，总共最多 60 个字段），用于资产信息的扩展，字段属性包括字符串、IP、整型、长整型、浮点和时间；</p> <p>支持通过高级威胁检测系统探针自动发现用户网络环境中的相关资产，实现网络环境中资产在安全运营中心的自动发现。</p>
漏洞管理	<p>支持漏洞的检索查询，可按漏洞名称、类型、风险等级、IP 地址、漏洞状态、来源、资产分组进行检索；</p> <p>支持漏洞的导入、导出及新建。</p>
调查中心	<p>支持提供图形化交互的威胁调查功能，可根据调查需求，选择相应的安全事件及安全告警进行调查分析，可将调查结果直接导出，作为威胁调查的结果呈现与留存存档；</p>

功能名称	功能需求说明
	支持对平台中的数据根据用户需求进行大数据检索，可根据需要对平台中存储的数据进行按需检索，进行安全威胁的调查与分析。
响应中心	<p>支持针对平台分析出的安全告警及资产脆弱性，通过响应中心通报工单平台进行下发。将不同的安全告警、事件及脆弱性按需下发给相应责任人进行处置，实现安全运营的分级响应与处置；</p> <p>通报工单平台支持工单的下发与工单签收，可选择相应的安全告警与脆弱性下发给特定责任人进行响应和处置；</p> <p>支持联动网络入侵防护系统，支持自定义阻断策略，对告警和事件中的源 IP、目的 IP 或 IP 对进行精准的流量封堵，从而形成响应联动；支持阻断白名单的配置。</p>
数据源接入	<p>支持近 300 种主流网络设备、安全设备、主机系统、数据库等主流产品的数据归一化解析能力，支持对个性化日志进行自定义解析模板配置；</p> <p>支持自定义日志源类型及其子类型；</p> <p>支持正则库的创建和批量导入，以便于解析策略的配置；</p> <p>支持自定义解析策略和策略组管理，支持对日志样本进行二次解析，简化正则表达式的编写难度；</p> <p>支持日志接入方式为 kafka、nsq、mysql 和 elasticsearch 的预处理配置。</p>

### 3.3.7. 大模型安全防护服务

通过体系化网络安全建设，实现算力基础设施防护，包含建设大数据日志审计、XDR 扩展检测与响应、数据库审计、终端 DLP 数据防泄露能力。

功能名称	功能需求说明
大数据日志审计	<ol style="list-style-type: none"> <li>提供日志全域采集包含算力集群内主机运行日志、网络设备日志、数据库操作日志、终端操作日志；</li> <li>提供智能关联分析通过机器学习算法识别日志中的异常关联，定位潜在威胁链条；</li> </ol>

	3. 合规溯源留存不少于 6 月日志信息及查询功能。
XDR 扩展检测与响应	1、提供多源威胁数据分析能力，对集群服务器、AI 存储、网络等安全态势进行分析形成威胁视图； 2、提供高级威胁精准检测，通过 AI 算法关联分析多场景数据，对各类攻击链进行识别； 3、提供自动化应急响应，发现威胁后无需人工干预即可触发联动防御，快速阻断威胁扩散至整个算力集群。
数据库审计	提供针对大模型全维度访问监控，记录所有针对数据库的操作行为，精准识别操作主体、操作内容、操作时间； 提供异常行为告警，通过建立基线，识别异常操作，实时触发告警并阻断高危操作； 提供合规审计留存，按照《个人信息保护法》《医疗数据安全指南》要求，留存数据库操作审计日志至少 1 年，支持按时间、操作类型、账号等维度快速检索。
终端 DLP 数据防泄露	提供针对大模型训练过程中的敏感数据识别，通过内容识别、标签识别，精准定位终端存储或处理的医疗敏感数据、AI 核心数据； 提供数据传输管控，阻断未授权的数据外发渠道，如禁止通过 U 盘、移动硬盘拷贝敏感数据，限制通过邮件、即时通讯工具外发 AI 模型文件或批量患者数据，仅允许经审批的合规传输； 提供操作行为记录，留存终端敏感数据的操作日志，一旦发生数据泄露事件，可快速追溯操作主体与过程，同时通过行为分析识别潜在泄漏风险，提前干预防范。

### 3.3.8. 算力平台安全服务

本次卫健分支节点云建设项目需配套完善的安全能力建设，按照信息安全等级保护三级认证的相关安全要求，对平台及硬件设备实施安全加固。需配备的相关安全能力如下：

安全能力	功能简述	防护对应
网络边界防护	基础防火墙功能、应用识别控制、应用层防	通信传输、边界防护、访

安全能力	功能简述	防护对应
	护、资产风险识别等	问控制、恶意代码防范
	敏感数据保护、高级威胁防御、僵尸网络防护、客户端防护等	入侵防范
	集中账号管理、集中访问控制、集中安全审计等	身份鉴别、访问控制、系统管理、安全管理
	通过扫描检测指定系统或应用的安全脆弱性，发现潜在的安全漏洞	网站安全
日志审计	资产异构日志高效采集、统一管理、集中存储、统计分析，安全事件事后取证	安全审计、入侵防范、审计管理、集中管控
数据审计	数据库操作行为记录、数据库操作实时审计、数据库操作实时监控、事故追根溯源、提高资产安全	安全审计
主机安全及终端防病毒	提供终端查杀病毒、软件管理、漏洞补丁、统一升级管理等功能；	恶意代码防范

### 1、网络边界防护

功能名称	功能要求说明
规格	开启入侵防御及网络防病毒功能后，满足全威胁吞吐量 2G
NAT 功能	支持源地址转换 SNAT，目的地址转换 DNAT 和双向 NAT 等功能，支持一对一、一对多、多对一等形式的 NAT。
	支持各种应用协议的 NAT 穿越，实现 SQLNET、TFTP、RTSP、PPTP、FTP、H.323、SIP 等多种 NAT ALG 功能。
访问控制	支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。
应用控制	支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。
DDoS 防护	支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
防病毒	支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。

	<p>支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。</p> <p>支持勒索病毒检测与防御功能，保障勒索病毒的防御效果。</p>
入侵防御	预定义漏洞特征数量超过 9000 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。
	支持僵尸主机检测功能，产品预定义特征库超过 110 万种，可识别主机的异常外联行为。
Web 应用防御	支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁。
	支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。
账号安全	支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。
蜜罐联动	支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP。
策略生命周期管理	产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。
双因素认证	产品支持管理员双因素认证功能，用户通过用户名/密码和 Key 等不同方式登录产品管理界面。

## 2、日志审计

功能名称	功能要求说明
规格	支持 20 个资产数接入。
日志采集	支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 720 种日志对象的日志数据采集。
	支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka 等多种方式完成日志收集。
	内置大量日志处理模型，自动解析主流网络设备、安全设备和

	<p>中间件的日志数据，标准化自动识别系统类型至少达到 200 种。</p> <p>支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。</p>
日志传输与存储转发	<p>支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。</p> <p>支持 TLS 加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。</p>
日志检索	<p>支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件。</p>
日志分析	<p>支持网站攻击、漏洞利用、C&amp;C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上，支持自定义关联分析规则。</p>
资产管理	<p>支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义资产标签、属性。</p>

### 3、安全运维

功能名称	功能要求说明
规格	支持 20 个资产数接入。
支持协议	<p>字符协议：SSHv1、SSHv2、TELNET。</p> <p>图形协议：RDP、VNC。</p> <p>文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板。</p>
用户管理	<p>支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登录认证方式、设定用户有效期。</p> <p>用户登录认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD 域认证、Radius 认证等认证方式；</p>

功能名称	功能要求说明
资源管理	并支持各种认证方式和静态口令组合认证。
	内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴。
	支持对用户指定限制登录 IP、登录时间段（可循环，如每周一到周五 9:00-17:00 时）等规则，以确保可信用户登录系统。
	支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求。
运维授权	支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源。
	支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口。
	支持 RDP 安全模式（RDP、NLA、TLS、ANY）设置，以适应 RDP-Tcp 属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合 FIPS 标准等加密级别。
改密计划	支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。
	支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问。
	支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。
运维方式	支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式。
	支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容。
审计日志	支持 web 页面直接发起运维，无须安装任何控件，并同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP 等客户端工具实现单点登录，不改变运维人员操作习惯。

功能名称	功能要求说明
	址、资源地址、协议、开始时间等，并可以实时阻断。
	图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放。

#### 4、数据审计

功能指标	指标要求
规格	支持审计 100M 数据库流量。
部署模式	工作模式：数据库审计产品可以旁路镜像模式部署，不影响数据库性能和网络架构；支持多点联合部署；支持集中管理，可集中管理多台审计设备审计事件的存储、分析，实现统一配置、统一报表、统一查询。
部署管理	采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。
审计功能	<p>支持主流数据库 Oracle (Tdata)、SQL-Server、DB2、MySQL (Tdsql)、Informix、Sybase、Postgresql、Cache、MongoDB、K-DB，虚谷。</p> <p>支持同时审计多种数据库及跨多种数据库平台操作。</p> <p>支持 HTTP 请求审计，可指定 GET、POST、URL、响应码进行精细审计。</p> <p>支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。</p>
统计功能	<p>支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况。</p> <p>支持以源 IP、业务主机、操作类型、SQL 模板、数据库用户为维度的数据库行为排行。</p> <p>精细化日志秒级查询； 通过 SQL 串模式抽取保障磁盘 IO 的读写性能； 分离式存储 SQL 语句保障数据审计速度快。</p>
数据库安全	<p>内置大量 SQL 安全规则</p> <p>包括如下：导出方式窃取、备份方式窃取、导出可执行程序、</p>

功能指标	指标要求
	备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等。
	支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断。
风险分析	支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模板为条件的数据库风险查询。

### 5、主机安全及终端防病毒

技术指标	技术规格要求
客户端授权	服务器客户端授权≥20 套。
安全管理	采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能。
	支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell 后门、高危漏洞及其各自影响的终端数量。
	提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。
	支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。

	支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录。
威胁检测	支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户。
	具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种。
	支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz 的自启动，可以防止黑客攻击。
	支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具。
	支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截。
	支持基于异常行为 AI 的实时监测，实现文件秒级动态备份，发生勒索事件时，支持自动删除原始文件夹中被加密的文件夹并隔离文件；支持文件恢复密码保护，用户下发文件恢复操作时需要经过认证校验，确保文件恢复操作的合法性；支持备份区的文件大小限制管理，即当勒索发生时备份的单个文件大小限制，以及备份区总空间大小。
	支持流行 Windows 高危漏洞的轻补丁免疫防御，支持 Windows

	补丁批量一键修复。
威胁狩猎	支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况。
Webshell 防护	支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离。
远程登录保护	支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵。 支持 Linux 服务器 SSH 远程登录保护，可开启 SSH 远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单。
内存马检测	支持内存马检测功能，在检测到进程被注入和进程新建时，主动调用内存马检测引擎进行相关进程扫描检测，检测到内存马后产生告警并可提供举证信息（进程信息、检测时间等）。
网端联动	本次所投防火墙检测到某主机有僵木蠕毒的 C2 通信时，支持手动或自动化将恶意域名信息下发到本产品做 C2 通信的封锁拦截，实现精准防控，且防火墙的此事件不再重复告警。 支持与本次所投防火墙进行安全联动，管理员可以在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。 支持管理员在本次所投防火墙管理界面下发一键隔离指令，对

	终端恶意文件进行隔离，防止病毒进一步扩散。
	支持为本次所投防火墙提供溯源举证功能，即本产品检测到僵尸木蠕毒的恶意域名访问时，会共享事件信息给防火墙，包含事件相关的文件、进程、域名连接、注册表修改操作等关键项，并且可以在防火墙侧进行威胁事件的溯源分析。支持对根据回溯出的风险项一键根除，清除后进程无法被创建、运行。

### 3. 4. 国密安全服务要求

本次卫健分支节点云建设项目扩容所需的国密安全服务要求提供云平台管控面国密合规服务能力和密钥管理服务能力，同时可以提供平台应用侧密码服务。本次提供的国密安全服务须与提供的云平台服务进行统一运维和运营。

#### 3. 4. 1 云平台管控面国密合规服务能力

功能名称	功能需求说明
合规性	专有云平台应使用国产密码算法，使用国家密码管理局认可的商用密码产品；
	专有云平台满足等保三级系统商用密码应用安全性评估的合规要求；
传输通道安全	网络 VPN 通道支持基于国产密码算法的传输通道加密；
	云平台支持通过基于国产密码算法的 HTTPS 访问管理页面或控制台；
身份鉴别	网络 VPN 通道，支持通过合规密码产品（如 OTPServer 或数字证书等）实现用户身份真实性鉴别；
	云平台支持通过合规密码产品（如 OTPServer 或数字证书等）实现用户身份真实性鉴别；
重要数据安全	云平台支持用户鉴别信息、个人敏感信息的信元传输加密及完整性保护，密码算法采用国产密码算法；
	云平台支持用户鉴别信息、个人敏感信息的存储加密及完整性保护，密码算法采用国产密码算法；

	云平台支持平台日志、审计日志数据的完整性保护方案，密码算法采用国产密码算法；
	云平台支持集中存储服务器日志、网络设备日志，并支持日志数据的完整性保护，密码算法采用国产密码算法；
	云平台支持对云网关访问控制策略、云平台访问控制策略的完整性保护，密码算法采用国产密码算法；
	云平台支持对网络设备访问控制策略的集中管理并进行完整性保护，密码算法采用国产密码算法；
高可用部署	密码应用方案支持高可用部署，提供多地域、多可用区容灾能力；
密码组件隔离	支持租户层业务密码支撑组件与云平台管控层密码支撑组件部署物理隔离。
方案兼容性	云平台支持基于系统密码模块的国产商用密码算法加密、基于软件密码模块的国产商用密码算法加密、国际通用密码算法加密三种配置方案；
	方案支持国产化环境部署。

### 3.4.2 密钥管理服务能力

功能名称	功能需求说明
主密钥创建	产品需支持创建主密钥 CMK，且支持创建对称加解密密钥以及非对称加解密密钥（支持 SM2/RSA_2048 加密算法），也支持创建用途为非对称签名验签的主密钥（支持 SM2/RSA_2048/ECC 加密算法）
外部密钥导入（BYOK）	产品需支持用户导入自有密钥，通过 KMS 生成一个密钥材料为空的 CMK，并将自己的材料导入用户主密钥中，形成一个外部密钥 CMK，再由 KMS 系统进行该密钥的分发管理
密钥启禁用和轮换	产品需支持启用 / 禁用密钥，可进行批量操作，并支持设置轮换策略
配额管理	产品需支持按照租户 APPID 维度显示和配置租户可以管理的密钥个数

权限控制	产品需与鉴权模块集成。如果需要对主密钥的生命周期进行直接控制，或者想让其他账户使用它，可以创建并管理自己的主密钥。这些密钥均由 KMS 托管管控，通过身份管理和策略管理控制哪些账户，哪些角色可以访问或管理敏感密钥
日志审计	产品需与云平台审计系统集成。启用云平台审计后，向 KMS 发出的每个请求都会记录在日志文件中，该文件会被传送到启用云平台审计时指定的文件夹中。记录的信息包括用户、时间、日期、API 操作和所用密钥（如果相关）的详细信息
敏感数据加密	产品加密接口 (Encrypt) 用于加密最多为 4KB 的任意数据，可用于加密数据库密码，RSA Key，或其它较小的敏感信息。实际应用中主要用来保护服务器硬盘上敏感数据的安全（小于 4KB），如密钥、证书、配置文件等
信封加密	产品需对海量数据的高性能加解密方案。对于较大的文件或者对性能敏感的数据加密，使用 GenerateDataKey 接口生成 AES 数据加密密钥 DEK，只需要传输数据加密密钥 DEK 到 KMS 服务端（通过 CMK 进行加解密），所有的业务数据都是采用高效的本地对称加密处理
硬件安全	KMS 服务密钥生成、存储与云平台分离，底层采用合规化的硬件安全模块 HSM 支持，确保密钥在整个生命周期的安全性
国密认证	产品底层 HSM（硬件密码机）支持由国家密码局签发的商用密码产品型号证书

### 3.4.3 算力平台密码服务

本次卫健分支节点云建设项目需配套完善的密码能力建设，按照信息安全技术信息系统密码应用基本要求，对平台及硬件设备实施密码改造加固。需配备的相关密码能力如下：

组件名称	组件用途	组件功能要求
安全认证网关组件	在通信网络中融合身份认证、访问控制等安全手段，构建安全传输通道，为用户提供安全接入服务	支持单端口服务同时采用国密和国际证书双证书策略；支持 SSL 通道加速功能，支持 WEB 缓存、

		连接复用、异步 I/O、Cache、HTTP 压缩等多种模式。
签名验签组件	基于数字签名、验证签名技术，使用证书为系统提供应用级数字签名、验证签名等服务。	支持 SM2、RSA 签名验签算法；支持采用账户/口令或者数字证书的方式进行接口级别的应用系统身份鉴别，确保密码设备不会被非法调用。
加解密组件	该服务包括对称密码运算和杂凑密码运算，用于应用系统服务端的海量数据、高并发的密码运算业务请求。	支持 SM1、SM2、SM4、SM9、DES/3DES、AES、RSA、ECDSA 算法等国内和国际主流密码算法；
时间戳组件	基于公钥密码基础设施应用技术，为信息系统提供精准、安全和可信时间认证服务。	同时支持对关键操作的日志记录进行审计验证。
密钥管理组件	根据密码接入规范和标准管理协议，为信息系统提供密钥生成、存储、更新、注销、归档、恢复、销毁等密钥生命周期管理和服务。	支持密钥状态轮转，支持密钥定时或者手动翻新，翻新密钥名称不变。数字证书、密钥用户和访问口令等方式对客户端进行身份认证。
动态令牌组件	基于动态令牌的方式，实现客户端与服务端间的身份鉴别。	支持时间口令，以用户登录时间作为随机因素，保证时间同步；支持计数器口令，客户端计算口令时，客户端计数器进行加一操作，服务端验证口令时，计数器同样进行加一，并进行口令验证，验证通过后加一。

数据库加密组件	提供字段级的透明加密服务，确保数据加密存储的机密性和完整性。	支持应用免改造的国密算法透明加密； 支持对历史数据的自动转加密，适用于已有数据的生产环境。
协同签名组件	基于 SM2 算法的协同签名技术实现移动终端的数字签名、身份鉴别等。	对应的移动终端密码模块具备基于 Andriod、iOS 等终端操作系统的国密认证证书。支持管理员对设备和密钥强制解绑。
电子签章组件	为租户提供电子印章管理、电子签章/验章等服务，实现电子公文流转。	支持上传 PDF 文件或选用模板发起签署、支持指定签署位置、支持单页签章、多页签章、骑缝章、关键字签章、支持单页签章、多页签章、骑缝章、关键字签章。
文件加解密组件	该服务基于文件加密技术，对非结构化文件提供加密服务，保障用户数据安全。	支持多操作系统和 NAS 文件加密支持；支持国密 SM4 对称算法；支持国际算法 AES 算法，支持 AES-128，AES-192 和 AES-256；支持服务器弹性扩展。

### 3.5 性能要求

卫健分支节点云建设的云扩容服务需保证集成调优后满足以下性能要求：

#### (1) 整体性能要求

- 单 AZ 能纳管的物理节点最大规模  $\geq 10000$ ；
- 单台云主机创建耗时  $\leq 60s$ ；
- CVM 热迁移业务中断时长  $\leq 500ms$ ；
- 故障迁移（宿主机宕机） $\leq 150s$ ；
- 云硬盘单盘创建耗时  $\leq 10s$ ；

- 云硬盘单盘快照创建耗时≤1分钟

## (2) SSD 云硬盘性能要求

- 访问时延小于 3ms;
- 磁盘大小 10GB-16TB;
- 数据可用性 99.99%;
- 单盘最大吞吐 260MB/s;
- 单盘 IOPS≥26000

为保证卫健分支节点云建设项目扩容整体性能和对未来徐汇区医疗卫生信息化系统的承载能力，投标人提供的设备应包含以下类型，且不低于以下配置要求。所提供的硬件设备需兼容主流云厂商云平台。服务期内需提供配套硬件维护服务，保证硬件可用性。

### 3.5.1 平台管理服务器 1

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片，不少于 2 颗 CPU，每颗 CPU 物理核数≥48 核、每颗 CPU 主频≥2.6GHz
内存要求	内存总容量≥768GB，单条内存容量=64G。
硬盘要求	1 块 SATA SSD 480G，市场主流品牌，企业级 SATA SSD 硬盘 4 块 NVMe SSD 6.4T，DWPD≥3，市场主流品牌，企业级 NVMe SSD 硬盘 8 块 SATA HDD 16T，市场主流品牌，企业级 SATA HDD 硬盘 配置 HBA 卡，8 块 HDD 必须为直通模式
网卡要求	25GE：双端口 25G 光口普通网卡； 支持 PXE、支持 DPDK 应用，支持 SRIOV 技术；
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI)；预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能； 独立管理口 100%兼容千兆或百兆交换网络，通过管理口实现远程开关机、重启、网络安装操作系统等操作

远程管理功能	配置远程管理卡，具有单独的管理网口，可不依赖主机操作系统进行远程操作
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警

### 3.5.2 平台管理服务器 2

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片，不少于 2 颗 CPU，每颗 CPU 物理核数 $\geq 48$ 核、每颗 CPU 主频 $\geq 2.6$ GHz
内存要求	内存总容量 $\geq 512$ GB，单条内存容量 = 32G。
硬盘要求	1 块 SATA SSD 480G，市场主流品牌，企业级 SATA SSD 硬盘 4 块 NVMe SSD 3.84T，DWPD $\geq 1$ ，市场主流品牌，企业级 NVMe SSD 硬盘
网卡要求	25GE：双端口 25G 光口普通网卡； 支持 PXE、支持 DPDK 应用，支持 SRIOV 技术；
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI)；预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能； 独立管理口 100% 兼容千兆或百兆交换网络，通过管理口实现远程开关机、重启、网络安装操作系统等操作。
远程管理功能	配置远程管理卡，具有单独的管理网口，可不依赖主机操作系统进行远程操作。
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警。

### 3.5.3 云计算服务器

指标项	技术要求
服务器类型	机架式、高度 2U

CPU 要求	国产 ARM 架构芯片，不少于 2 颗 CPU，每颗 CPU 物理核数 $\geq 48$ 核、每颗 CPU 主频 $\geq 2.6$ GHz
内存要求	内存总容量 $\geq 1024$ GB，单条内存容量 $= 64$ G。
硬盘要求	1 块 SATA SSD 480G，市场主流品牌，企业级 SATA SSD 硬盘
网卡要求	25GE：双端口 25G 光口普通网卡； 支持 PXE、支持 DPDK 应用，支持 SRIOV 技术；
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI)；预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能； 独立管理口 100% 兼容千兆或百兆交换网络，通过管理口实现远程开关机、重启、网络安装操作系统等操作。
远程管理功能	配置远程管理卡，具有单独的管理网口，可不依赖主机操作系统进行远程操作。
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警。

### 3.5.4 智算服务器

指标项	技术要求
计算能力	配置 4 颗 ARM 架构通用计算处理器
	CPU 主频 $\geq 2.6$ GHz， $\geq 48$ 核
	单颗 AI 处理器 FP16 算力 $\geq 280$ TFLOPS，FP32 算力 $\geq 75$ TFLOPS
	单颗 AI 处理器提供不低于 64GB HBM，速度不低于 1600GB/S
通信能力	支持 AI 处理器直出 200G 网口
	AI 处理器间支持 8 卡 fullmesh 全互联
	AI 处理器间互联带宽最大不低于 380GB/s
设计规格	不超过 4U 空间提供 2.24P FLOPS FP16、0.60P PFLOPS FP32 稠密算力
	可以扩展服务器同品牌 NVMe SSD
基础能力	内存配置容量： $\geq 1024$ GB

	<p>支持以下内存保护技术：</p> <ul style="list-style-type: none"> <li>● ECC</li> <li>● SEC/DED</li> <li>● SDDC</li> <li>● Patrol scrubbing, 提供证明材料。</li> </ul> <p>Raid 卡采用国产自主可控芯片</p> <p>支持 8200GE 光口</p> <p>整机最大功耗不高于 6kW</p> <p>采用国产自主可控电源管理芯片</p> <p>整机满配电源模块数量不高于 4 个</p> <p>满配冗余热插拔电源, 输出功率小于 5.2KW 支持 2+2 冗余, 输出功率大于 5.2KW 支持 3+1 冗余</p>
--	---

### 3. 5. 5 全闪存储服务器

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片, 不少于 2 颗 CPU, 每颗 CPU 物理核数 $\geq 48$ 核、每颗 CPU 主频 $\geq 2.6$ GHz
内存要求	内存总容量 $\geq 128$ GB, 单条内存容量 $= 32$ G。
硬盘要求	1 块 SATA SSD 480G, 市场主流品牌, 企业级 SATA SSD 硬盘 12 块 NVMe SSD 3.84T, DWPD $\geq 1$ , 市场主流品牌, 企业级 NVMe SSD 硬盘
网卡要求	25GE: 双端口 25G 光口普通网卡; 支持 PXE、支持 DPDK 应用, 支持 SRIOV 技术;
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI); 预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能; 独立管理口 100% 兼容千兆或百兆交换网络, 通过管理口实现远程开关机、重启、网络安装操作系统等操作
远程管理功能	配置远程管理卡, 具有单独的管理网口, 可不依赖主机操作系统进行远程操作

硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警
--------	---

### 3. 5. 6 混闪存储服务器

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片, 不少于 2 颗 CPU, 每颗 CPU 物理核数 $\geq 32$ 核、每颗 CPU 主频 $\geq 2.6$ GHz
内存要求	内存总容量 $\geq 384$ GB, 单条内存容量 = 32G。
硬盘要求	1 块 SATA SSD 480G, 市场主流品牌, 企业级 SATA SSD 硬盘 2 块 NVMe SSD 6.4T, DWPD $\geq 3$ , 市场主流品牌, 企业级 NVMe SSD 硬盘 10 块 SATA HDD 16T, 市场主流品牌, 企业级 SATA HDD 硬盘 配置 HBA 卡, 10 块 HDD 必须为直通模式
网卡要求	25GE: 双端口 25G 光口普通网卡; 支持 PXE、支持 DPDK 应用, 支持 SRIOV 技术;
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI); 预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能; 独立管理口 100% 兼容千兆或百兆交换网络, 通过管理口实现远程开关机、重启、网络安装操作系统等操作
远程管理功能	配置远程管理卡, 具有单独的管理网口, 可不依赖主机操作系统进行远程操作
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警

### 3. 5. 7 算力平台服务器

指标项	技术要求
服务器类型	机架式、高度 2U

CPU 要求	国产 ARM 架构芯片, 不少于 2 颗 CPU, 每颗 CPU 物理核数 $\geq 64$ 核、每颗 CPU 主频 $\geq 2.6$ GHz
内存要求	支持内存类型: ECC DDR4 RDIMM/LRDIMM 内存插槽, 本次配置 512GB 内存
硬盘要求	配置 $\geq 2$ 块 960 SAS SSD 系统盘 配置 1 块独立磁盘阵列卡, 缓存 $\geq 2$ G, 支持 RAID 0/1/10/6/5/50/60, 配置超级电容保护; 支持 iBMC 带外管理
网卡要求	25GE: 双端口 25G 光口普通网卡; 支持 PXE、支持 DPDK 应用, 支持 SRIOV 技术;
电源要求	220VAC/240HVDC 交直流兼容电源 2
管理要求	集成系统管理支持: 电源启动和关闭、风扇监视和控制、电源监控、温度监控、本地固件更新、错误日志; 具有图形管理界面及其他高级管理功能; 管理带宽 GE

### 3.5.8 AI 存储服务器

指标项	技术要求
管理节点 CPU 要求	采用国产 CPU, 单框总核心数 $\geq 192$ 核。集群总核心数 $\geq 3072$ 核 (16 框)
内存要求	单存储节点 (控) 内存 $\geq 512$ GB 单框设备内存 $\geq 1024$ GB 硬件设备包括保电内存、BBU, 文件数据在断电后数据能够继续保存。
AI 加速存储要求	采用 NVME SSD 机型, 每框 (2U) 设备可放置 $>= 36$ 块 SSD 盘。 单节点配置 CPU 数量 $\geq 2$ 颗, 单节点 CPU 内核总数 $\geq 96$ 核 单框支持 $\geq 825$ GE TCP 业务网络, $\geq 20100$ GE RoCE 存储网络, 本次配置 825GE TCP 业务网络, 16100 GE RoCE 存储网络 提供统一交付的文件存储集群 1、具备大规模横向扩展能力, 单集群规模最大可扩展至 $\geq 32$ 节点 (控)。 2、支持卡在线扩展, 业务不中断, 可以灵活扩容计算 (存储、计算、网络同时增加, 可在线增加网络平面)

	<p>支持超高性能密度， 单台设备读带宽不低于 160 GB/s。</p> <p>单节点（控）读带宽不低于 80GB/s， 写带宽不低于 25GB/s；</p> <p>支持横向扩展能力，新增节点带来的集群性能提升不低于单节点性能的 85%</p>
	<p>支持超高性能密度， 单台设备读 IOPS 不低于 360 万。</p> <p>单节点（控）8K IO 随机读 IOPS 不低于 180 万， 8K IO 随机写 IOPS 不低于 32.5 万；</p> <p>支持横向扩展能力，新增节点带来的集群性能提升不低于单节点性能的 85%</p>

### 3.5.9 网关服务器

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片，不少于 2 颗 CPU，每颗 CPU 物理核数 $\geq$ 64 核、每颗 CPU 主频 $\geq$ 2.6GHz
内存要求	内存总容量 $\geq$ 512GB，单条内存容量=32G。
硬盘要求	6 块 SATA SSD 480G，市场主流品牌，企业级 SATA SSD 硬盘 配置 HBA 卡，6 块 SSD 必须为直通模式
网卡要求	100GE：双端口 100G 光口普通网卡 支持 PXE、支持 DPDK 应用，支持 SRIOV 技术
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI)；预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能； 独立管理口 100%兼容千兆或百兆交换网络，通过管理口实现远程开关机、重启、网络安装操作系统等操作
远程管理功能	配置远程管理卡，具有单独的管理网口，可不依赖主机操作系统进行远程操作
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊

	断报警
--	-----

### 3.5.10 安全服务器

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片，不少于 2 颗 CPU，每颗 CPU 物理核数 $\geq 32$ 核、每颗 CPU 主频 $\geq 2.6$ GHz
内存要求	内存总容量 $\geq 384$ GB，单条内存容量 = 32G。
硬盘要求	1 块 SATA SSD 480G，市场主流品牌，企业级 SATA SSD 硬盘 12 块 SATA HDD 16T，市场主流品牌，企业级 SATA HDD 硬盘 配置 HBA 卡，12 块 HDD 必须为直通模式
网卡要求	25GE：双端口 25G 光口普通网卡； 支持 PXE、支持 DPDK 应用，支持 SRIOV 技术；
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI)；预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能； 独立管理口 100% 兼容千兆或百兆交换网络，通过管理口实现远程开关机、重启、网络安装操作系统等操作
远程管理功能	配置远程管理卡，具有单独的管理网口，可不依赖主机操作系统进行远程操作
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警

### 3.5.11 安全探针服务器

指标项	技术要求
服务器类型	机架式、高度 2U
CPU 要求	国产 ARM 架构芯片，不少于 2 颗 CPU，每颗 CPU 物理核数 $\geq 48$ 核、每颗 CPU 主频 $\geq 2.6$ GHz

内存要求	内存总容量 $\geq 384\text{GB}$ , 单条内存容量=32G。
硬盘要求	1 块 SATA SSD 480G, 市场主流品牌, 企业级 SATA SSD 硬盘
网卡要求	2 块 10GE (电口): 2 块双端口 10G 电口普通网卡 2 块 10GE (光口): 2 块双端口 10G 光口普通网卡 支持 PXE、支持 DPDK 应用, 支持 SRIOV 技术
电源要求	220VAC/240HVDC 交直流兼容电源 2
出厂配置	必须提供服务器出厂设置定制服务 (CFI); 预装 BIOS/BMC 版本与云平台兼容
管理维护功能	提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能; 独立管理口 100%兼容千兆或百兆交换网络, 通过管理口实现远程开关机、重启、网络安装操作系统等操作
远程管理功能	配置远程管理卡, 具有单独的管理网口, 可不依赖主机操作系统进行远程操作
硬件诊断功能	能够对主机 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断报警

### 3. 5. 12 云加密机服务器

指标项	技术要求
设备类型	2U 标准设备, 8 核 CPU, 内存 16G, RJ45 网口 2 个, SFP28 光网口 2 个, 密码卡 1 块;
对接要求	支持与云平台密钥管理系统 KMS 的集成对接, 提供密钥管理系统 KMS 的密钥生成与存储等功能, 满足密钥管理系统产品对接需求;
性能要求	SM2 生成 $\geq 100000$ 对/秒 SM2 签名 $\geq 100000$ 次/秒 SM2 验签 $\geq 20000$ 次/秒 SM4 加解密 $\geq 1000$ Mbps

### 3. 5. 13 SSL VPN 网关服务器

指标项	技术要求

功能要求	产品符合 GM/T 0024、GM/T 0025 规范要求，支持国产密码标准 SSLv1.1 协议；
	至少提供 4 个网络端口，2 个千兆电口，2 个万兆光口（光口可支持 10GE 或者 25GE）；
	支持基于国产密码算法的 SSL 卸载、国密双证双向 HTTPS 应用交付功能；
	支持一个地址端口上 RSA 与 SM2 同时自适应；支持 IP 协议与 TCP/UDP/ICMP 协议的加密传输；
	支持国际通用密码算法 SSLv3/TLS 1.0/1.1/1.2/1.3 认证模式；
合规证书	具备国家密码管理局的商用密码产品认证证书，符合 GM/T 0028 安全等级第二级要求。

### 3.5.14 核心交换机

指标项	技术要求
硬件架构	机框高度≤6U；配置独立的交换网板，控制引擎和交换网板硬件相互独立；机框采用正交 CLOS 架构，交换网板槽位与业务槽位互相垂直，机框采用无中板架构，机框严格前后风道设计； 主控板 1+1 冗余，交换网板 5+1 冗余，业务板槽位数≥4； 电源支持冗余
性能指标	交换容量≥387Tbps；包转发率≥115200Mpps； 支持单槽位 36 口 100G 单板线速
板卡配置	支持 10G/40G/100G/400G 全系列线卡； 单板最大 10G 端口数≥48；单板最大 40G 端口数≥36；单板最大 100G 端口数≥36
实配需求	实配 2 张主控板；实配 6 张交换网板； 实配 2 张 100G QSFP28 端口板卡，实配每张板卡的 100G 端口≥36； 按照实际需求配置光模块
二层功能	支持端口聚合，802.3ad，支持二、三层聚合
三层功能	支持 IPv4 静态路由、RIP、OSPF、ISIS、BGP； 支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+；

	支持 IP 报文分片和重组
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备； 支持跨框链路聚合 (DRNI/M-LAG)； 支持 BFD for DRNI/M-LAG
镜像	支持 BFD for DRNI/M-LAG；支持流镜像
流量调度	支持 ACL、CAR、Remark 等动作；支持 Diff-serv/QoS；支持 PQ、WFQ、PQ+WFQ 等队列调度方式；支持基于端口和 VLAN 的 ACL
可靠性	支持微分段；支持 BFD FOR VRRP 功能；硬件 BFD 3.3ms 最小间隔，收敛时间小于 10ms；支持电源、风扇模块在线热拔插
智能无损	支持 RDMA、RoCE v2、PFC、ECN 等无损以太网特性； 支持 PFC 死锁预防，PFC 死锁检测
VxLAN	支持 VXLAN over IPv6；支持 IPv6 VXLAN over IPv4； 支持 VxLAN OAM: VxLAN ping, VxLAN tracert；支持 BGP EVPN 协议
管理和监控	支持 SNMP V1/V2/V3、Telnet、RMON、SSH2.0 功能； 支持 AAA/Radius 认证；支持 TACACS，支持命令行认证； 支持 NetStream 流量统计功能；支持 sflow 流量统计分析功能； 支持配置回滚

### 3.5.15 业务网交换机

指标项	指标要求
转发性能	交换容量 $\geq 8\text{Tbps}$ 。
	包转发率 $\geq 2400\text{Mpps}$ 。
硬件规格	电源模块槽位 $\geq 2$ 个，电源 1+1 备份。
	风扇模块槽位 $\geq 5$ 个，风扇模块 4+1 备份。
	CPU (处理器)、LSW (转发芯片) 均为国产自研芯片。
端口配置要求	下行接口：25GE 光接口 $\geq 48$ 个。
	上行接口：100 GE 光接口 $\geq 8$ 个。
二层功能	支持 Access、Trunk 和 Hybrid 三种模式。

	支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术。 支持动态 MAC、静态 MAC 和黑洞 MAC 表项。
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议。
	支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。
	支持 IPv6 ND、PMTU 发现。
QoS	支持 PQ、DRR、PQ+DRR 等队列调度方式。
	支持 WRED、尾丢弃等拥塞避免机制。
	支持 MAC 漂移联动端口 error-down。
可靠性	支持硬件 BFD (Bidirectional Forwarding Detection) 3.3ms 检测间隔。
	支持 VRRP、VRRP 负载分担、BFD for VRRP 。
DC 特性	支持 Vxlan, 且支持 EVPN VxLAN, 支持 VxLAN 网络与 VLAN 网络互通。
安全性	支持防止 DOS、arp 攻击和 ICMP 攻击。
	支持 IP、MAC、端口和 VLAN 的组合绑定。
	支持端口隔离。
超融合以太网特性	支持 AI ECN。
	支持 ECN Overlay。
配置和维护	支持 Telemetry。
	支持 ERSPAN 增强。
	支持 SNMP V1/V2/V3、Telnet、RMON、SSH。
	支持配置回滚。
流量分析	支持 Netstream。

### 3.5.16 样本面交换机

指标项	指标要求
转发性能	交换容量 $\geq 8\text{Tbps}$ 。
	包转发率 $\geq 2400\text{Mpps}$ 。
硬件规格	电源模块槽位 $\geq 2$ 个, 电源 1+1 备份。
	风扇模块槽位 $\geq 5$ 个。

	CPU（处理器）、LSW（转发芯片）均为国产自研芯片。
端口配置要求	100GE QSFP28 光接口 $\geqslant$ 32 个（兼容 40GE）。
二层功能	支持 Access、Trunk 和 Hybrid 三种模式。
	支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术。
	支持动态 MAC、静态 MAC 和黑洞 MAC 表项。
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议。
	支持 IPv6 ND、PMTU 发现。
QoS	支持 PQ、DRR、PQ+DRR 等队列调度方式。
	支持 MAC 漂移联动端口 error-down。
可靠性	支持 BFD (Bidirectional Forwarding Detection) 3.3ms 检测间隔。
	支持 VRRP、VRRP 负载分担、BFD for VRRP。
DC 特性	支持 Vxlan, 且支持 EVPN VxLAN, 支持 VxLAN 网络与 VLAN 网络互通。
安全性	支持 MacSec 国密算法。
	支持防止 DOS、arp 攻击和 ICMP 攻击。
	支持 IP、MAC、端口和 VLAN 的组合绑定。
	支持端口隔离。
超融合以太网特性	支持 AI ECN。
	支持 ECN Overlay。
配置和维护	支持 Telemetry。
	支持 ERSPAN 增强。
流量分析	支持 Netstream。

### 3.5.17 管理面交换机

指标项	指标要求
转发性能	交换容量 $\geqslant$ 758Gbps。
	包转发率 $\geqslant$ 252Mpps。
硬件规格	高度 $\leqslant$ 1U, 固定接口交换机。

	电源 1+1 备份。
端口配置要求	SFP+接口 $\geq 4$ 个。
	BASE-T 接口 $\geq 48$ 个。
二层功能	支持 Access、Trunk 和 Hybrid 三种模式。
	支持 QinQ。
	支持 ERPS 以太环保护协议 (G.8032)。
	支持动态 MAC、静态 MAC 和黑洞 MAC 表项。
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议。
	支持 RIPng、OSPFv3、IS-ISv6、BGP4+等 IPv6 动态路由协议。
	支持 IPv6 ND、PMTU 发现。
QoS	支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 调度方式。
	支持双向端口限速。
	支持流量整形。
虚拟化技术	支持集群或堆叠多虚一技术，实现单一界面管理多台设备。
安全性	支持防止 Ddos、arp 攻击和 ICMP 攻击。
	支持 IP、MAC、端口和 VLAN 的组合绑定。
	支持 802.1X 认证。
	支持端口隔离。
	支持 RMON。
配置和维护	支持 Telemetry。
	支持 SNMP V1/V2/V3、Telnet、RMON、SSH。
	支持基于命令行的配置回滚。
流量分析	支持 Netstream。

## 3.5.18 100G 光口交换机

指标项	技术要求
国产化	采用国产化 CPU 和国产化转发芯片
交换容量	交换容量 $\geq 6.4$ Tbps
转发性能	转发性能 $\geq 2000$ Mpps

缓存	整机缓存 $\geq 36M$
硬件规格	高度 1U; 支持可插拔冗余电源和风扇; 支持前后、后前风道
端口配置要求	实配 100GE 光接口 $\geq 32$ 个, 100GE 端口支持自适应为 40G; 支持 1 个带外管理口
二层功能	支持 802.1Q (VLAN), 数目不小于 4k; 支持 QinQ; 支持 MAC Flapping
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议; 支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议; 支持 IGMP V1/V2/V3, 支持 IGMP Proxy; 支持 PIM-DM、PIM-SM、MSDP、MBGP 、Any-RP; 支持 IP 报文分片和重组
虚拟化	支持集群或堆叠多虚一技术, 实现单一界面管理多台设备; 支持跨框链路聚合 (M-LAG)
镜像	支持本地端口镜像和远程端口镜; 支持流镜像
QoS	支持 SP、WRR、WFQ、SP+WRR、SP+WFQ 调度方式; 支持 ACL、CAR、优先级重新标记等; 支持 L2~L4 协议包过滤功能和流分类; 支持流量整形
可靠性	支持 VRRP; 支持 STP/RSTP/MSTP; 兼容 PVST 协议, 支持跨厂商生成树互通; 支持硬件 BFD (最小 3.3ms 发包间隔); 支持 BFD for BGP/IS-IS/OSPF/静态路由
安全特性	支持 IP、MAC、端口、VLAN 的组合绑定; 支持风暴抑制, 包括广播抑制、未知单播抑制和组播抑制; 支持防 ARP 攻击、DOS 攻击、ICMP 防攻击; 支持 AAA、Radius 和 TACACS 认证
VxLAN	支持 VxLAN over IPv6; 支持 IPv6 VxLAN over IPv4; 支持 VxLAN OAM: VxLAN ping, VxLAN tracert; 支持 BGP EVPN 协议
配置和维护	支持 Telemetry 可视化功能; 支持系统日志和用户操作日志, 支持分级告警; 支持 SNMP、Telnet、RMON、SSH;

	支持配置回滚；支持缓存的微突发检测
--	-------------------

## 3.5.19 25G 光口交换机

指标项	技术要求
国产化	采用国产化 CPU 和国产化转发芯片
交换容量	交换容量 $\geq 4.8\text{Tbps}$
转发性能	转发性能 $\geq 1600\text{Mpps}$
缓存	整机缓存 $\geq 36\text{M}$
硬件规格	高度 1U；支持可插拔冗余电源和风扇；支持前后、后前风道
端口配置要求	实配 100GE 光接口 $\geq 6$ 个，100GE 端口支持自适应为 40G； 实配 25GE 光接口端口数量 $\geq 48$ 个； 支持 1 个带外管理口
二层功能	支持 802.1Q (VLAN)，数目不小于 4k； 支持 QinQ；支持 MAC Flapping
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议； 支持 RIPng、OSPFv3、IS-ISv6、BGP4+ 等 IPv6 动态路由协议； 支持 IGMP V1/V2/V3，支持 IGMP Proxy； 支持 PIM-DM、PIM-SM、MSDP、MBGP、Any-RP； 支持 IP 报文分片和重组
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备； 支持跨框链路聚合 (M-LAG)
镜像	支持本地端口镜像和远程端口镜；支持流镜像
QoS	支持 WRR、WFQ、SP+WRR、SP+WFQ 调度方式； 支持 ACL、CAR、优先级重新标记等； 支持 L2~L4 协议包过滤功能和流分类；支持流量整形
可靠性	支持 VRRP；支持 STP/RSTP/MSTP； 兼容 PVST 协议，支持跨厂商生成树互通；支持硬件 BFD (最小 3.3ms 发包间隔)；支持 BFD for BGP/IS-IS/OSPF/静态路由
安全特性	支持 IP、MAC、端口、VLAN 的组合绑定；

	支持风暴抑制，包括广播抑制、未知单播抑制和组播抑制；支持防 ARP 攻击、DOS 攻击、ICMP 防攻击；支持 AAA、Radius 和 TACACS 认证
VxLAN	支持 VxLAN over IPv6；支持 IPv6 VxLAN over IPv4； 支持 VxLAN OAM: VxLAN ping, VxLAN tracert；支持 BGP EVPN 协议
配置和维护	支持 Telemetry 可视化功能； 支持系统日志和用户操作日志，支持分级告警； 支持 SNMP、Telnet、RMON、SSH； 支持配置回滚；支持缓存的微突发检测

### 3. 5. 20 10G 光口交换机

指标项	技术要求
国产化	采用国产化 CPU 和国产化转发芯片
交换容量	交换容量 $\geq 4.8\text{Tbps}$
转发性能	转发性能 $\geq 1600\text{Mpps}$
缓存	整机缓存 $\geq 36\text{M}$
硬件规格	高度 1U；支持可插拔冗余电源和风扇；支持前后、后前风道
端口配置要求	实配 100GE 光接口 $\geq 6$ 个，100GE 端口支持自适应为 40G； 实配 10GE 光接口端口数量 $\geq 48$ 个； 支持 1 个带外管理口
二层功能	支持 802.1Q (VLAN)，数目不小于 4k； 支持 QinQ；支持 MAC Flapping
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议； 支持 RIPng、OSPFv3、IS-ISv6、BGP4+ 等 IPv6 动态路由协议； 支持 IGMP V1/V2/V3，支持 IGMP Proxy； 支持 PIM-DM、PIM-SM、MSDP、MBGP 、Any-RP； 支持 IP 报文分片和重组
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备； 支持跨框链路聚合 (M-LAG)
镜像	支持本地端口镜像和远程端口镜；支持流镜像

QoS	支持 WRR、WFQ、SP+WRR、SP+WFQ 调度方式； 支持 ACL、CAR、优先级重新标记等； 支持 L2~L4 协议包过滤功能和流分类；支持流量整形
可靠性	支持 VRRP；支持 STP/RSTP/MSTP； 兼容 PVST 协议，支持跨厂商生成树互通；支持硬件 BFD（最小 3.3ms 发包间隔）；支持 BFD for BGP/IS-IS/OSPF/静态路由
安全特性	支持 IP、MAC、端口、VLAN 的组合绑定； 支持风暴抑制，包括广播抑制、未知单播抑制和组播抑制；支持防 ARP 攻击、DOS 攻击、ICMP 防攻击；支持 AAA、Radius 和 TACACS 认证
VxLAN	支持 VxLAN over IPv6；支持 IPv6 VxLAN over IPv4； 支持 VxLAN OAM：VxLAN ping, VxLAN tracert；支持 BGP EVPN 协议
配置和维护	支持 Telemetry 可视化功能； 支持系统日志和用户操作日志，支持分级告警； 支持 SNMP、Telnet、RMON、SSH； 支持配置回滚；支持缓存的微突发检测

### 3.5.21 千兆交换机

指标项	技术要求
国产化	采用国产化 CPU 和国产化转发芯片
交换容量	交换容量≥600Gbps
转发性能	转发性能≥140Mpps
硬件规格	高度 1U，固定接口交换机； 支持双电源，双风扇框；支持前后风道
端口配置要求	实配 10GE 光接口≥4 个；实配 1GE 电口≥48 个； 支持 1 个带外管理口
二层功能	支持 802.1Q (VLAN)，数目不小于 4k； 支持 QinQ；支持 MAC Flapping
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议； 支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议；

	支持 IGMP V1/V2/V3, 支持 IGMP Proxy; 支持 PIM-DM、PIM-SM、MSDP、MBGP、Any-RP
虚拟化	支持集群或堆叠多虚一技术, 实现单一界面管理多台设备; 支持跨框链路聚合 (M-LAG)
镜像	支持本地端口镜像和远程端口镜; 支持流镜像
QoS	支持 SP、WFQ、SP+WFQ 调度方式; 支持 ACL、CAR、优先级重新标记等; 支持 L2~L4 协议包过滤功能和流分类
可靠性	支持 VRRP; 支持 STP/RSTP/MSTP; 支持 BFD for BGP/IS-IS/OSPF/静态路由
安全特性	支持 IP、MAC、端口、VLAN 的组合绑定; 支持 OSPF、RIPv2 报文的明文及 MD5 密文认证; 支持防 ARP 攻击、DOS 攻击、ICMP 防攻击; 支持 AAA、Radius 和 TACACS 认证
配置和维护	支持 Syslog, 系统日志, 分级告警, 调试信息输出; 支持 SNMP、Telnet、RMON、SSH; 支持零配置 Auto-config; 支持 SFlow; 支持 Telemetry 可视化; 支持 NTP

### 3. 5. 22 400G 参数面接入/汇聚交换机

指标项	技术要求
转发性能	交换容量 $\geq 25.6\text{Tbps}$ ,
	包转发率 $\geq 8000\text{Mpps}$
硬件规格	高度 $\leq 1\text{U}$ , 固定接口交换机
	电源模块槽位 $\geq 2$ 个, 电源 1+1 备份;
	风扇模块槽位 $\geq 6$ 个
	设备整机缓存 $\geq 128\text{M}$
	CPU、转发芯片均为国产芯片
端口配置要求	400GE QSFP-DD 光接口 $\geq 32$ 个 (兼容 200GE/100GE/40GE) 实配 32 个 400 光模块

二层功能	支持 Access、Trunk 和 Hybrid 三种模式
	支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术。
	支持动态 MAC、静态 MAC 和黑洞 MAC 表项
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议
	支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议
	支持 IPv6 ND、PMTU 发现
QoS	支持 PQ、DRR、PQ+DRR 等队列调度方式
	支持 WRED、尾丢弃等拥塞避免机制
	支持 MAC 漂移联动端口 error-down。
可靠性	支持 BFD (Bidirectional Forwarding Detection) 3.3ms 检测间隔
	支持数据面故障快速自愈 DPFR
	支持 VRRP、VRRP 负载分担、BFD for VRRP
DC 特性	支持 Vxlan, 且支持 EVPN VxLAN, 支持 VxLAN 网络与 VLAN 网络互通
	支持 VxLAN over IPv6、IPv6 VXLAN over IPv4。
安全性	支持防止 DOS、arp 攻击和 ICMP 攻击
	支持 IP、MAC、端口和 VLAN 的组合绑定
	支持端口隔离
组播	支持组播流量抑制
	支持 IGMP Snooping
超融合以太网特性	支持 RDMA, RoCEv2, DCB。
	支持 AI ECN。
	支持 NSLB 功能。
配置和维护	支持 Telemetry
	支持 ERSPAN 增强。

### 3.5.23 AI 存储交换机

指标项	技术要求
转发性能	交换容量 $\geq 8\text{Tbps}$ ,
	包转发率 $\geq 2400\text{Mpps}$

硬件规格	电源模块槽位 $\geq 2$ 个, 电源 1+1 备份;
	风扇模块槽位 $\geq 5$ 个。
	CPU (处理器)、LSW (转发芯片) 均为国产自研芯片。
端口配置要求	100GE QSFP28 光接口 $\geq 32$ 个 (兼容 40GE)
二层功能	支持 Access、Trunk 和 Hybrid 三种模式
	支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术。
	支持动态 MAC、静态 MAC 和黑洞 MAC 表项
三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议
	支持 IPv6 ND、PMTU 发现
QoS	支持 PQ、DRR、PQ+DRR 等队列调度方式
	支持 MAC 漂移联动端口 error-down。
可靠性	支持 BFD (Bidirectional Forwarding Detection) 3.3ms 检测间隔
	支持 VRRP、VRRP 负载分担、BFD for VRRP
DC 特性	支持 Vxlan, 且支持 EVPN VxLAN, 支持 VxLAN 网络与 VLAN 网络互通
安全性	支持 MacSec 国密算法
	支持防止 DOS、arp 攻击和 ICMP 攻击
	支持 IP、MAC、端口和 VLAN 的组合绑定
	支持端口隔离
超融合以太网特性	支持 AI ECN。
	支持 ECN Overlay。
配置和维护	支持 Telemetry
	支持 ERSPAN 增强。
流量分析	支持 Netstream

### 3.5.24 防火墙 1

指标项	技术要求
硬件特性	设备高度 1U, 端口形态: $\geq 8$ 个 10GE 接口, 接口扩展槽位 $\geq 1$
	采用多核架构
	具备可插拔冗余电源模块

性能指标	防火墙吞吐量（大包） $\geq 35\text{Gbps}$
	并发连接数 $\geq 1000$ 万
	每秒新建连接数 $\geq 40$ 万
升级服务	具备入侵防御、防病毒、应用识别和 web 应用防护等能力
部署模式	实现路由模式、透明（网桥）模式、混合模式。
路由实现	支持静态路由、策略路由，以及 RIP、OSPF 等动态路由协议
	支持 IPv4/IPv6 双协议栈，并支持 IPv6 数据报文转发、静态路由、动态路由及组播路由等功能
	支持 IPv6 路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由等
NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，支持多种应用协议的 NAT ALG 功能。
	NAT 地址池支持动态探测和可用地址分配
系统冗余性	支持两台设备之间主主或主备冗余方式。
	支持链路探测及路由联动。
	支持虚拟防火墙功能
防护功能	支持 APT 攻击防范功能。支持 HTTP、HTTPS、DNS 等应用层 Flood 攻击，包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood 等常见 DDoS 攻击的检测防御。
设备管理	提供命令行和图形化用户接口（GUI）。

### 3. 5. 25 防火墙 2

指标项	技术要求
硬件特性	设备高度 1U，端口形态：配置 1GE（光口或电口） $\geq 4$ 个，10GE 光口 $\geq 2$ 个
	采用多核架构
	具备可插拔冗余电源模块
性能指标	防火墙吞吐量（大包） $\geq 15\text{Gbps}$
	并发连接数 $\geq 500$ 万
	每秒新建连接数 $\geq 10$ 万

升级服务	具备入侵防御、防病毒、应用识别和 web 应用防护等能力
部署模式	实现路由模式、透明（网桥）模式、混合模式。
路由实现	支持静态路由、策略路由，以及 RIP、OSPF 等动态路由协议
	支持 IPv4/IPv6 双协议栈，并支持 IPv6 数据报文转发、静态路由、动态路由及组播路由等功能
	支持 IPv6 路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由等
NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，支持多种应用协议的 NAT ALG 功能。
	NAT 地址池支持动态探测和可用地址分配
系统冗余性	支持两台设备之间主主或主备冗余方式。
	支持链路探测及路由联动。
	支持虚拟防火墙功能
防护功能	支持 APT 攻击防范功能。支持 HTTP、HTTPS、DNS 等应用层 Flood 攻击，包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood 等常见 DDoS 攻击的检测防御。
设备管理	提供命令行和图形化用户接口（GUI）。

### 3.5.26 服务器密码机

指标项	技术要求
安全特性	支持对称密钥加解密功能，可提供基于 SM1、SM4、SM7、DES/3DES、AES 等算法的加解密功能，算法模式支持 ECB/CBC/OFB/CFB/CTR/XTS/GCM/CCM 等。
	支持消息摘要功能，可提供基于 SM3、SHA-1、SHA-2、SHA-3 等算法的杂凑运算功能。
	支持基于 SM2、RSA 等算法的非对称密钥加解密功能、签名验签功能。
	256 位 SM2 密钥对生成（对/秒） $\geq 130000$ ； 256 位 SM2 签名/验签（次/秒） $\geq 130000/35000$ ； 256 位 SM2 加密/解密（次/秒） $\geq 10000/40000$ 。

	内置自签 CA 功能，支持为连接客户端签发国密数字证书。同时支持第三方证书管理。
设备功能	设备管理：设备支持 B/S 和命令界面对设备进行管理。支持 B/S 基于控件的远程管理，B/S 管理支持国密 SSL 通道；在 SSH 管理界面可以开启或关闭密码设备的 SSH 服务，以及选择使用普通 SSH 服务或国密 SSH 服务。
	具有用户管理功能，对访问用户分级管理，使用智能密码钥匙作为管理介质提高密码设备自身的安全性；按照超级管理员、审计员、操作员进行管理。
产品资质	具备《商用密码产品认证证书》，且符合 GM/T 0028《密码模块安全技术要求》第二级要求。

### 3.5.27 安全认证网关

指标项	技术要求
	RSA-2048 每秒新建连接数 $\geq 36000$ ； SM2 每秒新建连接数 $\geq 38000$ ； RSA-2048 并发连接数 $\geq 700000$ ； SM2 并发连接数 $\geq 820000$ ； RSA-2048 并发用户数 $\geq 680000$ ； SM2 并发用户数 $\geq 660000$ ； RSA-2048 吞吐率 $\geq 9400\text{Mbps}$ ； SM2 吞吐率 $\geq 8900 \text{ Mbps}$ 。
安全特性	支持协同签名、协同解密功能。
	支持所有密码运算与密钥管理均通过硬件密码模块实现。
	支持国密双证书体系，支持以标准 PKCS10、PKCS7、自定义数字信封机制导入加密密钥对及数字证书，能够与第三方 CA、行业自建 CA 无缝对接，并内置自签证书系统。

产品资质	具备《商用密码产品认证证书》，且符合 GM/T 0028《密码模块安全技术要求》第二级要求。
------	--

### 3.6 集成服务要求

投标人应根据机房的基础环境及条件提供详细的卫健分支节点云建设项目扩容设计方案，包含硬件设备配置方案、机柜上架方案、网络规划方案和安全方案，具体方案设计需满足以下要求：

- 从资源规划合理性角度，要求在技术架构合理的情况下，满足等保和国密的要求前提，复用一期已建设的相关能力；
- 网络规划须采用容灾架构：内部网络链路和设备须采取冗余架构，配套的网络设备（如交换机、路由器等）以及配套的防火墙等安全设备，均需要满足冗余架构；
- 通过云平台软件 SDN 技术实现网络虚拟化，构建网络资源池；
- 核心交换机支持在线扩容至支撑部署 1000 台服务器以上的能力，LEAF 节点统一下联 25G 光口，上联 100G 光口，LEAF 到 SPINE 的收敛比不高于 3:1，LEAF 交换机应不少于 48 个端口，每对 LEAF 节点支持最多接入 45 台服务器，服务器与 LEAF 交换机之间通过双网卡绑定，逻辑层隔离平台管理和租户业务网络平台，不同平面间设置不同网络策略；
- 智算服务采用 RDMA 网络实现支撑 16 个节点的技能，LEAF 到 SPINE 采用 400G 光口提供上下行。
- 本次扩容提供的资源所涉及的安全架构须与已建的政务外网区安全技术架构保持一致，以确保卫健分支节点云建设项目安全架构的稳定性；
- 出云数据流须通过物理防火墙进行隔离；
- 支持服务器管理和业务网络间的有效隔离，满足合规性要求并通过等保三级安全相关检测。

中标人应根据采购方实际环境进行方案调整，完成软硬件及相关基础设施环境的安装、部署、调优，确保达到云服务、网络和安全等方面的指标要求。安装部署完成后需进行软硬件调优测试，测试范围包括功能测试和高可用测试，其中功能测试需确保所提供的云服务的所有功能均可用，高可用测试包括云产品单集群级别高可用测试和链路高可用测试。调优测试需提供云产品原厂标准测试用例，测试完成后需输出测试报告。

### 3.7 配套物理空间服务要求

投标人需为智算服务提供配套物理空间服务,在三江路 89 号 3 楼 145 平米已完成基础装修的智算机房环境内, 提供机柜及配套资源服务满足智算服务器运行物理环境。

提供不少于 20 个 14kw, 6 个 5kw, 单柜空间不少于 42U IT 模块机柜及配套资源服务, 并配置空调系统满足机柜内服务器稳定运行。

服务提供的资源应同时符合《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019) 中的物理和环境三级、GM/T0054-2018《信息系统密码应用基本要求》对于的物理与环境密评要求, 并通过等保三级及密评第三方测试。

机房应配置冗余或并行的电力电缆线路, 为计算机系统供电; 机房须采用市电与 UPS 组成的双路供电系统, 并确保为机柜负载提供不少于 15 分钟的 UPS 后备供电保障。

提供机柜环境监控, 对机柜运行环境、温湿度、用电情况、电池运行情况等进行管理监控。

服务所提供的硬件需采用国内一线品牌, 保障配套物理空间的运行稳定可靠。

### 3.8 运维服务要求

#### 3.8.1 服务要求

(1) 云服务商提供的卫健分节点云平台整体可靠性应不低于 99.975%, 数据可靠性应不低于 99.9999%。

(2) 网络故障处理要求: 在处理发生的各类软硬件、通信线路等故障时, 应确保业务正常稳定运行, 云服务商需每月给甲方提供本次服务中涉及的网络运行报告和故障报告, 处理的故障等级故障响应及时率不小于 99.9%, 故障修复及时率不小于 99.9%。

(3) 云平台故障处理要求: 处理卫健分节点云平台发生的各类软硬件等故障, 确保上层业务系统能够正常稳定运行, 云服务商需每月给甲方提供本次服务中涉及的云平台运行报告和故障报告, 处理的故障等级故障响应及时率不小于 99.9%, 故障修复及时率不小于 99.9%。

(4) 迁移及升级割接: 如涉及开展业务系统迁移割接和卫健分节点云平台软硬件升级割接; 云服务商在升级前制定完善的操作实施方案并出具迁移及升级责任承诺书, 在方案

中尽量降低对上层业务系统的影响；对于可能影响上层业务系统的各类操作，应全面评估操作影响，提前至少 72 小时（重大自然灾害除外）通知采购人做好相关准备工作，征得采购人同意方可实施。在采购人同意后方可执行操作，并提供应急响应方案。

#### （5）服务时间及响应

投标人需按各分项服务指标要求、提供服务响应。提供 7×24 响应的二线技术服务需满足以下要求：

系统临时出现的使用、操作或其他非故障的简单问题，需及时提供线上指导，一般 2 小时内提供解决方案；

遇到电话无法解决的故障时，一般 4 小时内到达用户现场，并在 8 小时之内提供解决方案（特大故障除外）。

中标人应在项目服务期内提供维护服务范围内的系统维护服务，根据系统故障级别提供不同处理方式：

- 1 级故障：系统宕机，业务停止。处理方式：中标人在接到故障通知后，应立即响应，1 小时内前往现场，4 小时内提供解决方案。硬件设备出现故障时，应进行紧急备件更换，保证采购方业务的正常运行。
- 2 级故障：系统可工作，但部分功能失效。处理方式：中标人在接到故障通知后，半小时内响应，3 小时内前往现场，24 小时内提供解决方案。
- 3 级故障：系统可运行，但出现系统报错或出现问题。处理方式：中标人在接到故障通知后，1 小时内响应，3 个工作日内提供解决方案。

（6）提供节假日保障要求：重大节假日期间进行卫健分节点云平台运行和信息安全的重点保障。

（7）特殊保障实施前，要求制定详细的《应急保障预案与计划》，保障结束后提供《应急保障服务总结报告》。

#### 3.8.2 服务团队要求

云服务商应为本项目组建专业的技术服务团队，包含项目经理 1 人，二线服务团队不少于 5 人。

##### （1）项目经理要求：

项目经理对服务项目过程实行全面管理，执行检查控制协调项目的各项工作。

项目经理需具有 PMP 等主流项目管理认证相关证书。

应从事大型网络、云、机房维护等相关工作至少 5 年以上实际经验，从事项目经理或项目负责人至少 5 年以上实际经验。

具备强烈的责任心和认真负责的工作态度。

需提供人员社保证明和无违法犯罪记录证明。

(2) 本次服务所提供的二线服务团队要求：

二线服务团队为现场运维管理、现场故障处置提供远程技术支撑服务，针对电子卫健分节点云平台异常业务量运营问题诊断，提供针对异常业务流量的数据分析，需提供类似项目异常业务流量分析截图，能针对政务外网区业务流量特征提供因子分析，具备对异常业务流量事件严重度评估能力，优化规划策略。通过热线电话、电子邮件和即时通讯等技术支持方式，提供 7\*24 小时电话响应服务。

服务人员中至少 1 名需具备专家级云计算认证资格（提供相关认证互联网专家证书或类似相应能力证书）。

服务人员中至少 1 名需具备网络认证工程师资格（提供相关认证证书或类似相应能力证书）。

服务人员中至少 1 名需具备数据分析师（CDA-Level 2）资质证明（提供相关认证互联网专家证书或类似相应能力证书）。

服务人员中至少 1 名需具备信息安全认证工程师资格。

服务人员中至少 1 名需具备云计算安全认证工程师资格。

从事网络、云、机房维护等相关工作至少 5 年以上实际经验。

### 3.8.3 服务满意度调查要求

本服务项目的实施，要求服务请求响应率达到 100%，故障处理解决率 95%以上，服务满意度调查达到 90%以上，所有服务请求响应要求在 2-5 分钟以内。

要求每年度随机抽取 100 起针对资源服务、事件处置、工单服务、巡检服务、应急保障服务等工作，实施售后服务满意度问卷调查统计工作，统计满意度数据要求达到 90%（含）

以上。

如达不到以上满意度要求，用户方有权终止合同。

### 3.9. 验收要求

服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。服务提供方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此服务提供方应当配合。

如果属于服务提供方原因致使系统未能通过验收，服务提供方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由服务提供方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

## 四、其他要求

1) 投标报价要求：本项目服务期限为合同签订后 3 年。投标报价应包括为提供本项目规定的全部管理、服务所发生的一切费用等。各投标人应根据招标内容结合自己的服务管理经验、水平和市场风险测算确定服务细目报价并进行汇总。

2) 投标人应根据招标文件要求以及自身经验能力，提供针对本项目指定的相关技术文件等，包括但不限于投标人对采购项目总体需求的理解以及相应的服务理念和方案（包括对采购项目服务内容的理解以及投标人完成采购项目的具体实施计划、服务流程、方法，人力、物力、技术力量的投入，提供详细的卫健分支节点云建设扩容设计方案，包括但不限于网络、安全等设计内容，实现云服务整体需求和服务指标。具体包括针对性的云平台建设方案、软硬件服务（包含所选用产品的数量、型号、详细技术参数指标等）、集成服务（包括设备配置方案、机柜上架方案、网络规划方案和安全方案等）、配套物理空间服务、运维服务，并满足相应的性能需求和服务指标等。

3) 投标方应进一步了解招标项目内容、范围。如有疑问，提出答疑，放弃了解或询问

不清的，视为确认标准、范围、内容所有条件，一旦中标，不得以不了解或不完全了解采购方的需求而提出额外费用，对此采购方一律不予考虑。

4) 投标方应为本项目组配一支有能力的服务团队。项目经理和有关负责人须具有类似项目的工作、管理经验，并且有检查机制。

5) 投标方需在投标文件中提供应急预案及相关保障措施、针对性方案等各项相关保障服务方案。

6) 投标方应加强内部管理控制，针对招标项目，制定相应管理、工作流程、服务方案、人员培训、巡查监督、考核奖惩等制度，建立健全各项管理机制，确保管理运作正常，良好有效无事故。如遇管理、协调、责任不到位，发生各类事故，应追究相关人员责任。

7) 本项目合同不得转让。

8) 中标单位与采购人应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，采购人应当按照沪财采〔2024〕22号《关于进一步加强本市政府采购履约验收管理有关事项的通知》及《徐汇区政府采购货物、服务项目合同履约验收管理办法》等相关规定进行验收管理和支付相应合同价款，中标单位有义务参加并协助采购人验收，提供相关技术资料、合格证明等文件或材料，并对自己生产或销售的货物质量或提供的服务负责。验收书要求可参考附件。

9) 如中标供应商实际供货产品与投标产品不一致，送货服务承诺无法完成，产品质量、服务被使用方有效投诉，经查实中标供应商要承担相应违约责任，并将按《徐汇区政府采购供应商诚信档案管理（暂行）办法》规定进行相应记载和处理，同时保留向市、区政府采购管理机构通报的权利。

## 第四部分 合同条款及格式

包1合同模板：

# 合同通用条款及专用条款

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同主体：

甲方： [合同中心-采购单位名称]

乙方： [合同中心-供应商名称]

地址： [合同中心-采购单位所在地]

地址： [合同中心-供应商所在地]

电话： [合同中心-采购单位联系人电话]

电话： [合同中心-供应商联系人电话]

联系人： [合同中心-采购单位联系人]

联系人： [合同中心-供应商联系人]

开户银行： [合同中心-供应商银行名称]

账号： [合同中心-供应商银行账号]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》及其他有关法律法规之规定，本合同当事人遵循平等、自愿、公平和诚实信用原则，在本项目经过政府采购的基础上，经协商一致，同意按下述条款和条件签署本合同：

## 一、定义

本合同中的下列词语应按以下内容进行解释：

1.1 “甲方”系指与乙方签署线上合同的采购人，本合同项下甲方的权利和义务在线下合同中由甲方（项目责任单位）和丙方（资金支付单位）共同承接，在线下合同中甲方和丙方根据条款约定分别享有和承担各自的权利和义务，具体事项由线下合同予以规定和明确。

1.2 “乙方”系指根据合同约定履行合同项下义务的中标(成交)供应商。

## 二、合同主要要素

### 2.1 项目服务内容及范围

乙方根据本合同的规定执行及完成合同文件所说明的本项目实施内容。乙方所提供的软、硬件及其各部分组成来源应符合国家的有关规定，信息系统的配置、功能、规格、等级、版本、数量、价格和交付日期等详见合同文件。

2.2 合同金额(含税): 人民币 【合同中心-合同总价】(大写: 【合同中心-合同总价大写】)

2.3 合同期限: 合同签订之日起 【合同中心-合同有效期】 个月(含试运行期    个月)。

2.4 质量保证期: 自本项目通过最终验收之日起, 硬件(含介质保留服务) 3 年质量保证期、成品软件 3 年质量保证期, 系统整体 1 年质量保证期, 乙方在质量保证期内提供免费的软件升级与现场维护服务。

2.5 其它:

## 三、合同文件的组成和解释顺序

3.1 本合同执行中双方共同签署的补充与修正文件及双方确认的明确双方权利、义务的会谈纪要;

3.2 本合同书;

3.3 本项目中标或成交通知书;

3.4 乙方的本项目投标文件或响应文件;

3.5 本项目招标文件或采购文件中的合同条款;

3.6 本项目招标文件或采购文件中的采购需求；

3.7 其他合同文件（需列明）： 。

上述文件互相补充和解释，如有不明确或不一致之处，按照上述文件次序在先者为准。同一层次合同文件有矛盾的，以时间较后的为准。

#### **四、服务质量、权利瑕疵担保及验收**

##### **4.1 服务质量标准和要求**

4.1.1 采购文件规定的规范及要求明确的，乙方所提供的软、硬件质量要求应当符合采购文件规定的规范及要求，且应不低于国家强制性标准。

4.1.2 采购文件规定的规范及要求不明确的，乙方所提供的软、硬件标准及质量要求应按照最新的国家、地方标准或行业标准或企业标准确定，均有标准的以高者（严格者）为准。没有国家、地方标准、行业标准或企业标准的，按照通常标准或者符合合同目的的特定标准确定。

4.1.3 乙方所提供的软、硬件还应符合上海市之有关规定。

4.1.4 乙方应建立和完善履行合同的内部质量保证体系，并依照甲方要求提供其相关内部规章制度，便于甲方的监督检查。

4.1.5 乙方应保证履行合同的人员数量和素质、软件和硬件设备的配置、场地、环境和设施等符合其在投标文件（响应文件）中所作的响应及承诺，并应接受甲方的监督检查。

##### **4.2 权利瑕疵担保**

4.2.1 乙方保证对其提供的产品及服务享有合法的权利，甲方接受乙方服务不会因此而侵犯任何人的合法权益。

4.2.2 乙方保证对其交付的软、硬件享有合法的权利，保证其在提供服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等，甲方接受乙方服务不会因此而存在合同外义务的负担。

4.2.3 乙方保证其所交付的软件系统没有侵犯任何第三人的知识产权和商业秘密等权利。如甲方使用该系统构成上述侵权的，则由乙方承担全部责任，甲方并有权解除本合同，并要求乙方返还甲方已支付的费用并赔偿其全部损失。

#### 4.3 验收

4.3.1 甲方有权在其认为必要时，对乙方是否能够按照合同约定提供服务进行履约检查，以确保乙方所提供的服务能够依约满足甲方的项目需求，但不得因履约检查妨碍乙方的正常工作，乙方应予积极配合。

4.3.2 乙方应在合同期满前\_\_\_\_个工作日内，以书面方式通知甲方并提供完整的竣工资料。乙方应配合开展验收前置审核工作。验收前置审核通过后\_\_\_\_个工作日，甲方应安排交付验收。乙方在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

4.3.3 乙方应按照合同及其附件所约定的内容进行交付，如果本合同约定甲方可以使用或拥有某软件源代码的，乙方应同时交付软件的源代码并不做任何的权利保留。所交付的文档与文件应当是可供人阅读的书面和电子文档。

4.3.4 甲方在领受竣工资料后，应当在\_\_\_\_个工作日内向乙方出具书面文件，以确认其初步达到符合本合同所约定的任务、需求

和功能。如有缺陷，应向乙方出具书面报告，陈述需要改进的缺陷。乙方应立即改进此项缺陷，并再次进行检测和评估。期间乙方需承担由自身原因造成修改的费用。三方将重复 4.3.2、4.3.4 项程序直至甲方验收通过或甲方依法或依约终止本合同为止。

4.3.5 如果属于甲方原因致使信息系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。乙方不得就此向甲方主张额外的费用。

4.3.6 甲方根据项目的技术规格要求和质量标准，对项目开展验收，签署验收意见。

## 五、费用支付

### 5.1 合同金额

本合同项目服务费用金额见 2.2，乙方完成及达到本合同文件规定的要求与标准的与本服务项目有关的所有费用（包括应承担的各项税负）均包含在合同金额中，甲方不再另行支付任何费用。

### 5.2 付款方式

本合同总金额为人民币 \_\_\_\_\_ (大写: \_\_\_\_\_)，此费用为本合同约定的全部费用。

采用以下方式付款：

a. 第一笔合同款金额：人民币 \_\_\_\_\_ (大写: \_\_\_\_\_)。付款条件：合同签订生效后，甲方收到乙方开具的等额发票后的 10 个工作日内。

b. 第二笔合同款金额：人民币 \_\_\_\_\_ (大写: \_\_\_\_\_)。付款条件： \_\_\_\_\_ 且甲方收到乙方开具的等额发票后的 10 个工作日内。

乙方应当及时向甲方开具与付款金额等额的合法有效的增值税

普通发票。因乙方未及时开具发票导致甲方延迟付款的，甲方不承担违约责任。

### 5.3 税费

与合同有关的一切税费，均已包含在上述合同金额中。

## 六、双方权利义务

### 6.1 甲方的权利和义务

6.1.1 甲方有权向乙方询问工作进展情况及相关的内容，有权检查和监督服务工作的质量、管理等情况，有权要求乙方以书面形式就前述内容进行汇报。

6.1.2 甲方有权对乙方服务过程中出现的具体问题提出建议和意见，有权通知乙方对违反合同规定的行为及时纠正，并按本合同有关规定给予处理。

6.1.3 因乙方违反合同规定给甲方或相关方造成损失时，甲方有权要求乙方赔偿经济损失。

6.1.4 当甲方认定项目服务专业人员不按项目服务合同履行其职责，或专业能力、管理能力、责任心较差，不能有效与甲方配合并履行其项目服务义务，或与第三人串通给甲方造成经济损失的，甲方有权要求乙方更换项目服务专业人员，如对甲方造成实际损失的，甲方有权终止合同并要求乙方承担相应的赔偿责任。

6.1.5 甲方有权同意或不同意乙方因自身工作需要而更换合同约定的主要工作小组成员的要求。

6.1.6 甲方有权根据《徐汇区政务信息化项目建设全过程管理办法》(徐数〔2025〕18号)，开展项目验收前置审核、验收审价，并根据审价金额支付尾款。

6.1.7 甲方应根据本合同约定及时向乙方支付合同款项。

6.1.8 甲方应当在合同履约中,督促、协调与本项目服务有关的第三人(与合同履行有关的相关单位)协同乙方办理有关服务事项。

6.1.9 甲方应按照合同文件明确的要求向乙方提供相应的工作环境。

## 6.2 乙方的权利和义务

6.2.1 乙方有权在履行合同期限内取得按合同约定应有的报酬。

6.2.2 乙方在项目服务过程中,如甲方提供的资料不明确时可向甲方提出书面报告。

6.2.3 乙方有权在合同履行期间得到甲方必要的支持,有权拒绝执行任何不符合有关法律、法规规定的要求。

6.2.4 乙方应向甲方提供与本项目服务有关的资料,包括项目服务单位、人员的资质证书及承担本合同业务的专业人员名单、项目服务工作计划等,并按合同约定的范围、时间、工作依据、工作标准等,出具内容齐全、规范、准确的相关报告等。

6.2.5 乙方应提交所提供硬件设备的技术文件并将其包装好随同设备一起发运,包括相应的每一套设备和仪器的中文技术文件,例如:产品目录、图纸、操作手册、使用说明、维护手册和/或服务指南。

6.2.6 乙方还应提供下列服务:

(1) 硬件设备的现场移动、安装、调试及技术支持;

(2) 提供系统集成和维修所需的专用工具和辅助材料;

(3) 按照合同文件工作与管理要求负责对项目进度的安排、现

场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患；

（4）在质量保证期内对交付的信息系统实施运行监督、维护、维修；

（5）乙方应根据项目实施的计划、进度和甲方的合理要求，及时安排对甲方的相关人员进行培训。培训目标为使受训者能够独立、熟练地完成操作，实现依据本合同所规定的信息系统的目标和功能。

6.2.7 交付的信息系统中，不得含有未经甲方许可的可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任或刑事责任。

6.2.8 乙方所提供的软件，包括受甲方委托所开发的软件，如果需要经国家有关部门登记、备案、审批或许可的，乙方应当保证所提供的软件已经完成上述手续。

6.2.9 乙方交付的软、硬件产品发生缺陷且在约定的时间内未能弥补缺陷，甲方可采取必要的补救措施，但其风险和费用将由乙方承担。

6.2.10 乙方应严格遵守国家、地方的法律、法规的规定，保证在合法且不侵犯他人利益的原则下进行项目服务活动，并对其所进行的服务活动负责。

6.2.11 乙方应对履行本合同所规定的服务以及在履行中因自己违约而给甲方造成的损失承担责任并应当向甲方进行赔偿。但下列情况不视为乙方违约：

（1）非乙方的行为、过失、违约或失职造成的损失或伤害；

(2) 不可抗力造成的损失。

6.2.12 乙方必须为本项目涉及的各种资料、数据和收据等保密。未经甲方书面同意，乙方及乙方员工不得泄露、遗失、复印与本合同规定业务活动有关的一切资料和内容。所有甲方或第三人(与合同业务有关相关单位)提供的与本合同规定业务活动有关的一切资料，在合同结束后均应归还。

6.2.13 乙方在本合同履行期间均不能直接或间接从事与本合同中活动相冲突的商业或职业活动，不得以任何理由向甲方任何工作人员行贿或有类似的行为。

## 七、保密及廉洁条款

### 7.1 保密

7.1.1 双方在履行本合同过程中，所提供之接触、知悉的对方相关仍处于不为公众所知悉或尚未主动对外公开的信息(包括但不限于有关人员、技术、经营、管理等各方面的各类信息)，均为本条款项下双方所应恪守保密义务所针对的对象，即使该等信息未能在本保密条款的约定中穷尽。

7.1.2 在合同中专辟本保密条款，视为双方已就相关需保密信息采取了必要、适当的保密措施。在履行本合同的过程中，除须配合司法调查的情形外，在未征得对方书面同意之前，双方均负有保密义务，不得向第三方泄露、披露、透露或促使第三方获得前述应当保密的信息。

7.1.3 违反保密义务的，视为严重的根本违约行为，除应按合同约定承担有关违约责任外，还应当承担由此导致的行政乃至刑事责任，并应承担损失赔偿责任。

7.1.4 保密的内容包括但不限于书面、电子数据等承载保密信息的各种形式。

7.1.5 前述保密义务条款为独立条款，不因本协议的解除、终止而失效。

## 7.2 廉洁

7.2.1 乙方应当守法诚信，保证服务能力及服务质量，不得与甲方恶意串通操纵政府采购活动。

7.2.2 甲方不得接受乙方组织的宴请、旅游、娱乐，不得收受礼品、现金、有价证券等，乙方亦不得向甲方提供或报销前述费用以及其他应当由个人承担的费用。若甲方工作人员要求乙方给予其任何形式的不正当利益，或发现甲方工作人员违反前述原则的行为，乙方应当及时向甲方举报，并提供相关证据，甲方经查实后作出处理，并为乙方保密。

7.2.3 乙方承诺并且确认，违背本条款的廉洁及诚信义务，将被视为严重的根本违约行为，应按合同约定承担相应的违约责任，并对造成的损失承担赔偿责任。

## 八、知识产权及所有权归属

### 8.1 知识产权

8.1.1 在项目期间内，乙方根据本合同要求提交的项目文件及服务成果（包括但不限于甲方委托开发的软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料，以及阶段性、过程性成果等相关资料）的知识产权，归甲方所有并使用，乙方就此不做任何的权利保留。乙方向甲方交付使用的信息系统已享有知识产权的，甲方可在合同文件明确的范围内自主使用。

8.1.2 支撑该信息系统开发和运行的第三方编制的软件的知识产权仍属于第三方。

8.1.3 乙方提供软件产品（包括软件载体和文档）和相关系统接口，仅限于甲方使用，未经乙方书面许可不能对外转让。软件不加密，不限制甲方安装次数和安装的终端数量。

8.1.4 乙方应当保证其交付给甲方的信息系统不侵犯任何第三方的合法权益。如发生第三方指控甲方实施的技术侵权的，乙方应当承担相应责任。

## 8.2 所有权

在项目期间内，乙方根据本合同要求提交的项目文件及服务成果（包括但不限于阶段性、过程性成果等相关资料）的所有权，归甲方所有，除公安机关、法院、检察院及其他相关政府部门依据相关法律法规查阅外，乙方需要查阅的，应向甲方提出申请，经甲方书面同意后可以查阅与其有关的材料（应对乙方保密的材料除外）。

## 九、违约责任

9.1 除合同规定外，如果甲方无正当理由未能按照合同规定的时间足额支付相应服务费用的，应当按照未付服务费用的万分之一（0.1‰）按日计收延迟付款滞纳金，直至足额支付服务费用时止，但延迟付款滞纳金的最高限额不超过合同价的5%。一旦达到延迟付款滞纳金的最高限额，乙方有权提前终止合同，并有权就由此造成损失向甲方主张赔偿或补偿。

9.2 乙方应根据合同文件规定的时间、内容和质量标准要求及时完成本项目软件开发及相关服务，在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的

事实，可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应根据《徐汇区政务信息化项目建设全过程管理办法》(徐数〔2025〕18号)的相关流程判定是否同意，同意延长交付时间或延期提供服务并不免除乙方责任。

除合同规定或甲方确定同意延期提供服务外，如果乙方没有按照合同规定的时间提供服务，甲方有权从服务费用中扣除误期赔偿费，赔偿费按每周赔偿延期服务的服务费用的千分之五(5‰)计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的10%。一周按七天计算，不足七天按一周计算。一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

9.3 乙方未按合同约定履行服务职责，给甲方造成损失的，乙方应按实赔偿，违约金最高为合同金额的20%。因乙方服务能力、服务质量问题导致甲方无法实现合同目的的，甲方有权单方解除合同并根据情况向乙方追回已付合同款项及追索最高为合同金额20%的违约金。

9.4 因乙方原因导致违反法律、法规和规章规定的行为的，甲方有权单方解除合同，并要求乙方按合同9.3条承担违约金并赔偿相关损失。

## 十、不可抗力

10.1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

10.2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大

变化（如突发应急事件，政府采取应急措施的），以及其它双方商定的其他事件（如黑客攻击、系统崩溃、互联网灾难等）。

10.3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知另一方，并在 15 日内将有关当局出具的不可抗力证明文件发送给另一方确认。合同双方应尽实际可能继续履行合同义务，并积极寻求采取合理的方案履行不受不可抗力影响的其他事项。合同双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

10.4 当不可抗力情形终止或消除后，受影响的一方应尽快以电话或传真通知对方，并以 EMS 证实。

10.5 受不可抗力影响方应尽一切努力减少因不可抗力而产生的损失，否则应对扩大的损失承担责任。

10.6 如不可抗力延续超过 45 日以上（含本数）时，双方应通过友好协商解决本合同的执行问题，并应尽快达成协议。

## 十一、合同终止、中止、变更

### 11.1 合同终止

#### 11.1.1 违约终止合同

11.1.1.1 在甲方针对乙方违约行为而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同：

（1）如果乙方未能在合同规定的限期或甲方同意延长的限期内提供服务。

（2）如果乙方的行为构成根本违约。

（3）如果乙方未能履行合同规定的其它任何义务。

11.1.1.2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定向有关部门举报，追究其法律责任。

### 11.1.2 破产终止合同

如果乙方破产、进入解散或清算程序，或丧失清偿能力（包括但不限于被有关部门列入执行黑名单、失信被执行人名录等情形），视为乙方已无法履行本合同项下义务，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方赔偿与补偿。该终止合同将不损害或影响甲方已经采取或将要采取的任何追究违约责任及追讨损失的行动或补救措施的权利。

### 11.1.3 不可抗力终止合同

如因发生不可抗力事件导致合同无法履行的，或延迟履行会损害国家利益和社会公共利益，或给一方或多方造成严重利益损害的，双方可协商终止本合同履行，双方互不承担违约及赔偿责任，但仍应就已履行部分进行费用结算。

## 11.2 合同中止

11.2.1 除合同继续履行将损害国家利益和社会公共利益的情形外，双方当事人不得擅自中止合同。

11.2.2 若发生不可抗力事件，但合同仍有继续履行可能的，双方当事人可协商中止履行本合同全部或部分内容。

## 11.3 合同变更

11.3.1 甲方需追加与合同标的相同服务的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同。

11.3.2 除合同规定情形外，双方不得擅自变更合同。合同继续

履行将损害国家利益和社会公共利益的，双方应当变更。有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

11.4 在本合同项下的任何权利和义务不因合同乙方发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则本合同项下的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对甲方承担连带责任。

## 十二、合同转让和分包

本合同不得转让、不得分包。

## 十三、争议解决

协议履行过程中发生争议时，双方应本着诚实信用原则，通过友好协商解决。协商仍无法解决的，向合同签订地的上海市徐汇区人民法院提起诉讼。

## 十四、其他

14.1 本合同经双方签字、盖章后生效。

14.2 本合同壹式\_\_\_\_份，甲方执\_\_\_\_份、乙方执\_\_\_\_份，一份报上海市徐汇区政府采购管理办公室备案。

14.3 本合同附件与合同具有同等效力。

以下无内容

签约各方：

甲方（盖章）： 乙方（盖章）：

法定代表人或其授权委托人（签章）： 法定代表人或其授权委托人（签章）：

日期：[合同中心-签订时间] 日期：[合同中心-签订时间]

2025年10月15日

合同签订点：网上签约



**第五部分 投标文件格式**  
**投标文件格式详见网上招投标系统相关附件**

**附件 1 投标函**

徐汇区政府采购中心:

\_\_\_\_\_ (投标人全称) 授权 \_\_\_\_\_ (投标人代表姓名)  
(职务、职称) 为我方代表, 参加贵方组织的 \_\_\_\_\_ (项目名称、项目编号、  
包号) 招标的有关活动, 并对此项目进行投标。为此:

1、我方同意在本项目招标文件中规定的开标日起 90 天内 遵守本函中的承诺且在此期限期满  
之前均具有约束力。

2、我方按招标文件规定提供交付的的系统及相关服务的投标总价为 \_\_\_\_\_ (大  
写) 元人民币。

3、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商  
应当具备的条件:

(1) 具有《中华人民共和国营业执照》、《税务登记证》, 根据《上海市政府采购供应商  
登记及诚信管理办法》要求登记入库, 在近三年内无行贿犯罪记录, 未被政府采购监督管理  
部门禁止参加政府采购活动的供应商; 同时经信用信息查询未被列入失信被执行人、重大税  
收违法案件当事人名单、政府采购严重违法失信行为记录名单;

(2) 具有工信部颁发的《基础电信业务经营许可证》或《增值电信业务经营许可证》;  
(3) 本项目不允许联合投标。

4、我方已充分考虑到投标期间网上投标会发生的故障和风险, 并对发生的任何故障和风险  
造成投标内容不一致或利益受损或投标失败, 承担全部责任。

5、我方同意网上投标内容均以网上投标系统开标时的开标记录表内容为准, 投标人的授权  
代表将在开标记录上签名以确认开标过程和结果, 如果不签字, 则由我们承担全部责任。

6、保证遵守招标文件的规定, 忠实地执行双方所签订的合同, 并承担合同规定的责任和义  
务。

7、如果在开标后规定的投标有效期内撤回投标, 我方的投标保证金可被贵方没收。

8、我方完全理解贵方不一定接受最低价的投标或收到的任何投标。

9、我方愿意向贵方提供任何与本项投标有关的数据、情况和技术资料。若贵方需要, 我方  
愿意提供我方作出的一切承诺的证明材料。

10、我方已详细审核全部投标文件, 包括投标文件修改书 (如有的话)、参考资料及有关附  
件, 确认无误。

11、我方承诺: 采购中心若需追加采购本项目招标文件所列货物及相关服务的, 在不改变合  
同其他实质性条款的前提下, 按相同或更优惠的折扣保证供货。

12、我方承诺接受招标文件中《中标合同》的全部条款且无任何异议。

13、我方将严格遵守《中华人民共和国政府采购法》的有关规定, 若有下列情形之一的, 将  
被处以采购金额 5%以上 10%以下的罚款, 列入不良行为记录名单, 在一至三年内禁止参加  
政府采购活动; 有违法所得的, 并处没收违法所得; 情节严重的, 由工商行政管理机关吊销

营业执照；构成犯罪的，依法追究刑事责任：

- (1) 提供虚假材料谋取中标、成交的；
- (2) 采取不正当手段诋毁、排挤其他供应商的；
- (3) 与采购人、其它供应商或者采购中心工作人员恶意串通的；
- (4) 向采购人、采购中心工作人员行贿或者提供其他不正当利益的；
- (5) 未经监管部门同意，在采购过程中与采购人进行协商谈判的；
- (6) 拒绝有关部门监督检查或提供虚假情况的。

与本投标有关的一切往来通讯请寄：

地址：\_\_\_\_\_

邮编：\_\_\_\_\_

电话：\_\_\_\_\_

传真：\_\_\_\_\_

投标人代表姓名：\_\_\_\_\_

投标人代表联系电话，e-mail：\_\_\_\_\_

投标人(公章)：

投标人代表(签字)：

日 期：

## 开标一览表

项目名称: \_\_\_\_\_

项目编号: \_\_\_\_\_

投标人名称: \_\_\_\_\_

上海市徐汇区政府采购中心——上海市徐汇区卫生健康委员会 2025 年卫健分支节点云建设（二期）政府采购项目包 1

项目名称	最终报价(总价、元)

注: (1) 所有价格均系用人民币表示, 单位为元, 保留到整数位。

投标人代表签字:

投标人(公章):

日期:       年       月       日

## 附件 2 投标报价明细表

填报单位 (公章):

第 页 共 页

序号	分类名称	费用 (元)	备注
1			详见明细 ( )
2			详见明细 ( )
3			详见明细 ( )
4			详见明细 ( )
5			详见明细 ( )
6	利润		详见明细 ( )
7	税费		详见明细 ( )
...	...		
<b>报价合计</b>			

注: (1) 所有价格均系用人民币表示, 单位为元, 保留到整数位。

(2) 投标人应根据分类报价费用情况编制明细费用表并随本表一起提供。

(3) 分项目明细报价合计应与开标一览表报价相等。

投标人代表签字: \_\_\_\_\_

投标人 (公章): \_\_\_\_\_

日期: \_\_\_\_\_ 年 \_\_\_\_\_ 月 \_\_\_\_\_ 日

---

### 附件3 产品选型及说明一览表

序号	产品名称	型号规格及 主要技术参数	产地	数量	性能说明	备注

注：各产品材质、详细技术参数表（请供应商也可根据自身情况调整列表予以说明），请供应商务必详细描述，如描述不清，将会影响到对投标文件的评判，请供应商充分重视。

投标人代表签字：

投标人（公章）：

日期： 年 月 日

---

附件 4 产品规格、技术参数偏离表（可根据实际情况自行设计表式填报）

序号	产品名称及规格型号	数量	产地	招标产品配置要求	投标产品对应配置	偏差	备注

说明：1、投标人必须根据技术需求表来填写本表，如投标产品实际技术规格与技术需求无偏差，在“偏离”一列填写“无”。

2、投标产品的规格、技术参数和性能与招标文件的要求如不完全一致，在“偏离”一列填写“有”，还需填写偏差说明，并注明是“正偏离”还是“负偏离”以及偏差的幅度（以百分比表示）。

投标单位（盖章）：

投标人代表签名：\_\_\_\_\_

日期：\_\_\_\_\_

---

## 附件 5 法定代表人证明书和法人代表委托书

### 法定代表人证明书

\_\_\_\_\_先生/女士现担任\_\_\_\_\_职务，负责全面工作，  
为我单位的法定代表人。

特此证明。

投标人全称: \_\_\_\_\_

公章 (盖章):

\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

### 法人代表委托书

兹委托\_\_\_\_\_先生/女士全权代理\_\_\_\_\_ (招标项目和招标  
编号) 政府采购招标项目的招标投标工作。

特此证明。

投标人法定代表人姓名 (印刷体): \_\_\_\_\_

投标人法定代表人签字、盖章: \_\_\_\_\_

公章 (盖章):

\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

#### 附件 6-1 项目服务团队人员情况一览表

填报单位:

第 页 共 页

注：

- 1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。
  - 2、**我方承诺以上人员均为本单位职工，并按时交纳四金。并提供项目组人员身份证件及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。**
  - 3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字):

填写日期：

### 附件 6-2 售后服务人员情况一览表

填报单位（公章）：

第 页 共 页

注：

- 1、在填写时，如本表格不适合投标单位的实际情况，可根据本表格格式自行制表。
  - 2、**我方承诺以上人员均为本单位职工，并按时交纳四金。**并提供项目组人员身份证件及相关资格证书、工作履历等证明材料复印件，并加盖单位公章。
  - 3、此表作为中标后服务承诺书的组成部分，项目组人员应保持稳定。

投标人（公章）：

投标人代表(签字):

填写日期:

---

### 附件 6-3 项目经理说明表

姓名		出生年月		文化程度		毕业时间	
资格证书			技术职称				
获得证书 时间			聘任时间				
从业年限			进入本公司时间				
主要工作经历: (包括起止年限、单位名称、从事的工作内容、证明人、证明人联系电话)							
2022 年以来相关项目服务情况							
序号	项目名称	参与时间	项目预算金额 (万元)	参与项目的 角色	所附证明材料 页码		
1							
2							
3							
...							

注: 我方承诺以上人员均为本单位职工, 并按时交纳四金。并提供以上人员身份证及相关学历、资格证书、工作履历、业绩证明等证明材料复印件, 并加盖单位公章。

投标人 (公章):

投标人代表(签字):

填写日期:

附件 6-4 拟从事本项目售后服务人员的详细情况表

姓名		出生年月		文化程度		毕业时间	
资格证书				技术职称			
获得证书时间				聘任时间			
从业年限				进入本公司时间			

主要工作经历: (包括起止年限、单位名称、从事的工作内容、证明人、证明人联系电话)

2022 年以来相关服务情况

序号	项目名称	参与时间	项目预算金额(万元)	参与项目的角色	所附证明材料页码
1					
2					
3					
...					

投标人(公章):

投标人代表(签字):

填写日期:

---

附件 7 规章制度一览表

序号	规章制度名称	执行起始时间	备注
1			
2			
3			
...			
...			

各规章制度的具体内容另行提供。

投标人代表签字: \_\_\_\_\_

投标人(公章): \_\_\_\_\_

日期:       年       月       日

---

附件 8 供应商行贿犯罪记录承诺书  
上海市徐汇区政府采购中心：

\_\_\_\_\_ (投标供应商全称) 现参与你单位组织的 \_\_\_\_\_ 政府采购项目，并承诺本公司根据《上海市政府采购供应商登记及诚信管理办法》已申请加入上海市政府采购供应商库，且在 3 年内无行贿犯罪行为记录。

投标供应商全称：\_\_\_\_\_

公章（盖章）：

法定代表人签字、盖章：\_\_\_\_\_

---

## 附件9 中小企业声明函（服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称），属于软件和信息技术服务行业；承接企业为（企业名称），从业人员\_\_\_\_\_人，营业收入为\_\_\_\_\_万元，资产总额为\_\_\_\_\_万元，属于（中型企业、小型企业、微型企业）；
  2. （标的名称），属于软件和信息技术服务行业；承接企业为（企业名称），从业人员\_\_\_\_\_人，营业收入为\_\_\_\_\_万元，资产总额为\_\_\_\_\_万元，属于（中型企业、小型企业、微型企业）；
- .....

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：  
日期：

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

注：各行业划型标准：

（一）农、林、牧、渔业。营业收入20000万元以下的为中小微型企业。其中，营业收入500万元及以上的为中型企业，营业收入50万元及以上的为小型企业，营业收入50万元以下的为微型企业。

（二）工业。从业人员1000人以下或营业收入40000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入300万元及以上的为小型企业；从业人员20人以下或营业收入300万元以下的为微型企业。

（三）建筑业。营业收入80000万元以下或资产总额80000万元以下的为中小微型企业。其中，营业收入6000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入300万元及以上，且资产总额300万元及以上的为小型企业；营业收入300万元以下或资产总额300万元以下的为微型企业。

（四）批发业。从业人员200人以下或营业收入40000万元以下的为中小微型企业。其中，从业人员20人及以上，且营业收入5000万元及以上的为中型企业；从业人员5人及以上，且营业收入1000万元及以上的为小型企业；从业人员5人以下或营业收入1000万元以下的为微型企业。

（五）零售业。从业人员300人以下或营业收入20000万元以下的为中小微型企业。其中，从业人员50人及以上，且营业收入500万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（六）交通运输业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入3000万元及以上的为中型企业；从业人员20人及以上，且营业收入200万元及以上的为小型企业；从业人员20人以下或营业收入200万元以下的为微型企业。

（七）仓储业。从业人员200人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（八）邮政业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（九）住宿业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元

---

及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

---

附件 10 投标人近三年来已承接的主要类似项目一览表

序号	年份	项目名称	合同金额	业主情况			项目主要内容
				单位名称	经办人	联系方式	
1							
2							
3							
4							
...							

注： 1、如在本表格不能全部填写完，可按此表格格式自行制表填写。

2、提供相应采购项目合同复印件，加盖单位公章。

投标人代表签字：\_\_\_\_\_

投标人（公章）：\_\_\_\_\_

日期： 年 月 日

---

## 附件 11 投标单位基本情况表及声明

### (一) 名称及其他资料:

- 1、单位名称:
- 2、地址:
- 3、邮编:
- 4、电话/传真:
- 5、工商注册日期:
- 6、企业类型:
- 7、注册资本:
- 8、法定代表人或执行事务负责人姓名:
- 9、人员情况

    从业人员数

    专业技术人员数

### (二) 主要财务指标 (2024 年 1 月 1 日至 2024 年 12 月 31 日) 并请如实另附单位财务状况报告, 依法缴纳税收和社会保障资金的相关材料

- ① 业务收入: \_\_\_\_\_
- ② 风险基金额: \_\_\_\_\_
- ③ 资产净值: \_\_\_\_\_

### (三) 参加政府采购活动前三年内在经营活动中没有重大违法记录的声明: (请如实填写)

上海市徐汇区政府采购中心:

按照政府采购法实施条例要求, 我单位郑重声明: 我单位参与 \_\_\_\_\_ 政府采购项目, 在参加本项目政府采购活动前三年内在经营活动中 （没有/有） 重大违法记录。特此声明。

就我方全部所知, 兹证明上述声明是真实、准确的, 并已提供了全部现有资料和数据, 我方同意根据招标方要求出示文件予以证实。

投标单位 (公章):

投标人代表(签字):

填写日期:

---

附件 12 财务状况及税收、社会保障资金缴纳情况声明函（按包件填写）

我方 （供应商名称） 参加（单位名称）组织的（项目名称）征集活动，符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1. 具有健全的财务会计制度；
2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

---

**附件****上海市徐汇区政府采购项目验收书（服务类）**

供应商：

采购单位：

采购编号	采购项目	金额（元）
项目金额合计		
验收内容		
一、规章制度	1、人员管理	
	2、设备运维	
	3、服务管理	
	4、应急管理	
	.....	
二、运行记录	1、人员上岗及培训	
	2、设备检测记录	
	3、巡更记录	
	4、内审记录	
	.....	
三、现场实地检查情况		

验收意见	验收小组意见：	
	结论：该服务采购项目验收合格（或不合格）。	
验收小组签字：		
组长： 组员：		
年 月 日		
供应商盖章：	采购单位盖章：	

备注：1、采购人须按照《徐汇区政府采购货物、服务项目合同履约验收管理办法》第三章第十条“验收的基本程序”组织验收。2、政府向社会公众提供的公共服务项目（包括：以物为对象的公共服务，如公共设施管理服务、环境服务、专业技术服务等；以人为对象的公共服务，如教育、医疗卫生和社会服务等），验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告。3、该表式仅供参考。

## 第六部分

### 上海市徐汇区卫生健康委员会 2025 年卫健分支节点云建设（二期）

#### 政府采购项目评标办法

##### 一、评标依据：

1、评标办法系本着公开、公平、公正的原则，按照《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》制定，作为本次采购招标选定中标单位的依据。本次采购招标采用“综合评分法”评标，根据评标细则规定的评分标准对所有投标单位的有效投标文件进行评议，各评标项目累计总分为 100 分。

2、评标委员会由专家和采购单位代表组成，对各投标单位的投标报价进行甄别并经算术修正后得出各投标报价的得分，最终结果取算术平均值。

**3、评标委员会依据投标文件评分结果汇总后，对各投标单位的得分按由高到低的顺序依次排列，得出相应名次，得分最高的投标单位作为本项目中标单位。如出现最高得分并列情况时，则取投标报价较低者作为中标单位，如出现最高得分并列且报价相同则由评标委员会以投票表决方式，得票最多者为中标单位。采购人授权评标委员会在投标供应商中直接确定本项目中标单位。**

##### 二、评标规则：

- (1) 参加评标的专家为上海市政府采购咨询专家库中的专家，并在评标前按规定程序产生。
- (2) 任何人不得干预评标委员会成员的评审权利，评审表要保存备查。
- (3) 评标委员会成员必须对所有投标单位作出评审。

##### 三、“综合评分法”评标细则

###### 1、报价（20 分）采用低价优先法计算

(1) 首先确定评标基准价：经评标委员会甄别确认，满足招标文件要求且投标价格最低的投标报价为评标基准价，其报价分为满分 20 分。

(2) 确定其他投标报价分：计算公式为投标报价得分=评标基准价/打分投标单位的投标报价 $\times 20\% \times 100$ 。

注：①经评标委员会评审如投标单位的服务内容不能满足招标文件要求，该投标将不列入评审范围，其报价如为最低投标报价，将不作为评标基准价。②如果评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或不能诚信履约的，将要求该投标人作书面说明并提供相关证明材料。投标人不能证明其报价合理性的，评标委员会应将其作无效投标处理。

###### 2、卫健分支节点云服务（30 分）

###### (1) 整体服务方案（6-15 分）

评审内容：投标人提供的卫健分支节点云服务方案等。评审标准：对服务方案需求理解、分析到位，平台服务、安全服务、集成服务、配套物理空间服务等服务方案完整、响应全面、可操作性强，云平台服务安全可靠、可用性高、扩展性好、整体性能强等情况进行综

---

合评审。打分区间可根据主观评判划分为（15-13 分）、（13-9 分）、（9-6 分）三档。

## （2）软硬件产品性能及质量（6-15 分）

评审内容：投标人提供的各类产品性能及质量优劣情况。评审标准：投标响应的各类产品性能好、性价比高、产品成熟可靠、品牌知名度和市场占有率高、产品选型与配置好、品牌一致性高等情况进行综合评审。打分区间可根据主观评判划分为（15-13 分）、（13-9 分）、（9-6 分）三档。

## 3、项目服务团队人员配备及管理（20 分）

### （1）项目经理（3-10 分）

评审内容：投标人提供的项目经理情况。评审标准：具有相应资质证书、类似项目服务的业绩证明材料齐全、工作经历丰富、工作能力强等情况进行综合评审。打分区间可根据主观评判划分为（10-8 分）、（8-5 分）、（5-3 分）三档。

### （2）项目团队人员配备情况及管理（3-10 分）

评审内容：投标人提供的项目团队人员配备等情况。评审标准：从事本项目二线服务团队人员的配备数量充足、类似项目服务的业绩证明材料齐全、工作经历丰富、具有相应资质证书、工作能力强等情况进行综合评审。打分区间可根据主观评判划分为（10-8 分）、（8-5 分）、（5-3 分）三档。

## 4、项目实施计划及组织管理（6-15 分）

评审内容：投标人提供的项目实施计划、项目组织管理等情况。评审标准：项目实施计划完整合理、进度安排合理满足要求、项目管理及项目相关保障措施得当有效等情况进行综合评审。打分区间可根据主观评判划分为（15-13 分）、（13-9 分）、（9-6 分）三档。

## 5、费用报价依据和合理性（2-5 分）

评审内容：投标人提供的投标报价明细情况。评审标准：投标报价依据充分准确、报价完整、清晰合理等情况进行综合评审。打分区间可根据主观评判划分为（5-4 分）、（4-3 分）、（3-2 分）三档。

## 6、综合服务能力及投标响应度（3-10 分）

评审内容：投标人综合服务能力及投标响应度。评审标准：投标人综合服务能力强、类似业绩多、相关信誉好、投标整体响应度高等情况进行综合评审。打分区间可根据主观评判划分为（10-8 分）、（8-5 分）、（5-3 分）三档。

累计最高得分 100 分。