|  |
| --- |
| **温州市洞头区政府采购**  **竞争性磋商文件**  **（线上电子招投标）**  **项目名称：洞头区政务云平台租赁**  **采购编号：DTCG20240918114**  **采购人：温州市洞头区大数据管理中心**  **采购代理机构：温州华晟招标代理有限公司**  **二○二四年九月** |

磋商文件目录

关于洞头区政务云平台租赁的竞争性磋商公告

第一部分、投标邀请函（投标须知前附表）

第二部分、采购内容及要求

第三部分、供应商须知

一、说明

二、竞争性磋商文件

三、磋商响应文件

四、磋商响应文件递交

五、开标和评审

六、授予合同

第四部分、政府采购政策功能相关说明

第五部分、合同格式（参考格式）

第六部分、附件--磋商响应文件格式

一、资格文件格式

附件一、投标供应商参与政府采购活动投标资格声明函

二、报价文件格式

附件二、开标一览表

三、商务技术文件格式

附件三、投标函

附件四、法定代表人授权书

附件五、法定代表人诚信投标承诺书

附件六、投标供应商业绩

附件七、偏离表

附件八、项目服务人员汇总表

附件九、拟派项目人员情况表

第七部分、评标办法

**★注：磋商文件中有的条款及要求以加粗、加下划线或符号\*、▲、★、●的形式强调，这些特别强调的条款及内容有些是重要条款，供应商对重要条款的响应程度将作为评审工作的主要依据之一。**

**温州华晟招标代理有限公司关于洞头区政务云平台租赁的竞争性磋商采购公告**

项目概况

洞头区政务云平台租赁采购项目的潜在供应商应在政采云平台（www.zcygov.cn）获取（下载）采购文件，并于2024年9月29日15:00（北京时间）前提交（上传）响应文件。

**一、项目基本情况**

项目编号：DTCG20240918114

项目名称：洞头区政务云平台租赁

采购方式：竞争性磋商

预算金额（元）：1700000

最高限价（元）：990000、710000

采购需求：

标项一:

标项名称: 洞头区政务云（公有云）

数量：1

预算金额（元）：990000

单位：项

简要规格描述：见磋商文件

备注：\

标项二:

标项名称: 洞头区政务云（私有云）

数量：1

预算金额（元）：710000

单位：项

简要规格描述：见磋商文件

备注：\

合同履约期限：标项1、2，见磋商文件要求。

本项目（否）接受联合体投标。

**二、申请人的资格要求：**

1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）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.落实政府采购政策需满足的资格要求：标项1，2:无

3.本项目的特定资格要求：标项1，2: 供应商须具有增值电信业务经营资质（提供增值电信业务经营许可证）运营商或其分支机构（提供有效授权或证明文件）

**三、获取（下载）采购文件**

时间：/至2024年9月29日，每天上午00:00至12:00，下午12:00至23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

地点（网址）：政采云平台（www.zcygov.cn）

方式：潜在供应商自公告发布之日起至响应文件递交截止时间前通过账号登录政采云平台获取磋商文件，具体如下：项目采购--获取采购文件菜单，点击【申请获取采购文件】，填写获取采购文件的申请信息，提交后点击【下载采购文件】即可获取磋商文件；（备注：1、本项目磋商文件不收取工本费；仅需浏览磋商文件的供应商可点击“游客，浏览采购文件”直接下载磋商文件浏览。2、潜在供应商应当按照公告规定的方式获取磋商文件，未按照公告规定的方式获取磋商文件的，针对磋商文件的质疑不予受理。）

售价（元）：0

**四、响应文件提交（上传）**

截止时间：2024年9月29日15:00（北京时间）

地点（网址）：政府采购云平台在线投标，投标供应商无须前往评审现场。

**五、响应文件开启**

开启时间：2024年9月29日15:00（北京时间）

地点（网址）：温州市洞头区政务服务中心2楼

**六、公告期限**

自本公告发布之日起3个工作日。

**七、其他补充事宜**

1.《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 （浙财采监（2022）3号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）已分别于2022年1月29日和2022年2月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

2.根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表:鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。注意：需在线质疑后才可在线投诉，并电话告知相关采购人、代理机构、财政部门。  
 3.其他事项：1、质疑投诉：供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起7个工作日内，对采购文件需求的以书面形式向采购人提出质疑，对其他内容的以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。2、在线投标响应（电子投标）说明：1.本项目通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应（电子投标），供应商应先安装“政采云电子交易客户端”，并按照本磋商文件和“政府采购云平台”的要求，通过“政采云电子交易客户端”编制并加密磋商响应文件。供应商未按规定加密的磋商响应文件，“政府采购云平台”将予以拒收。 “政采云电子交易客户端”请自行前往“浙江政府采购网-下载专区-电子交易客户端”进行下载；电子投标具体操作流程详见《供应商-政府采购项目电子交易操作指南》（https：//help.zcygov.cn/web/site\_2/2018/12-28/2573.html）；通过“政府采购云平台”参与在线投标时如遇平台技术问题详询400-881-7190。 2.为确保网上操作合法、有效和安全，投标供应商应当在响应文件递交截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用CA电子签章。使用“政采云电子交易客户端”需要提前申领CA数字证书，申领流程请自行前往“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”进行查阅； 3.投标供应商应当在响应文件递交截止时间前，将生成的“电子加密磋商响应文件”上传递交至“政府采购云平台”。响应文件递交截止时间以后上传递交的磋商响应文件将被“政府采购云平台”拒收。 4.通过“政府采购云平台”成功上传递交的“电子加密磋商响应文件”无法按时解密的，其磋商响应文件按拒收处理。

**八、凡对本次招标提出询问、质疑、投诉，请按以下方式联系**

1.采购人信息

名 称：温州市洞头区大数据管理中心

地址：温州市洞头区新城大道68号电信大楼2楼大数据管理中心

传真：/

项目联系人（询问）：颜先生

项目联系方式（询问）：13968908099

质疑联系人：陈先生

质疑联系方式：13867752220

2.采购代理机构信息

名 称：温州华晟招标代理有限公司

地　址：乐清市双雁路508号三楼

传真：\

项目联系人（询问）：张先生

项目联系方式（询问）：15868575066

质疑联系人：金先生

质疑联系方式：13868320918

3. 同级政府采购监管管理部门

名 称：温州市洞头区财政局政府采购监管科

地址：浙江省温州市洞头区腾飞路79号财政大楼

传真：0577-63387900

联系人：许先生

监督投诉电话：0577-63387968

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线400-881-7190获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

第一部分 磋商邀请函（供应商须知前附表）

|  |  |  |
| --- | --- | --- |
| 序号 | 内容 | 说明与要求 |
| 1 | 项目名称 | 洞头区政务云平台租赁 |
| 2 | 项目编号 | DTCG20240918114 |
| 3 | 资金来源 | 财政性资金 |
| 4 | 采购预算 | 标项一99万元，标项二71万元。 |
| 5 | 采购方式 | 竞争性磋商 |
| 6 | 采购人 | 名称：温州市洞头区大数据管理中心  地址：温州市洞头区新城大道68号电信大楼2楼大数据管理中心  联系人：颜先生  联系电话：13968908099 |
| 7 | 采购代理机构 | 名称：温州华晟招标代理有限公司  联系人：张先生  联系电话：15868575066 |
| 8 | 招标内容 | 具体内容见竞争性磋商文件。 |
| 9 | 评标办法 | 综合评分法 |
| 10 | 供应商资格要求 | 具体要求见磋商采购公告。 |
| 11 | 是否接受联合体投标 | 不接受  □接受 |
| 12 | 踏勘现场 | 不组织  □组织 |
| 13 | 是否允许递交备选投标方案 | 不允许  □允许 |
| 14 | 投标货币 | 人民币 |
| 15 | 投标语言 | 中文 |
| 16 | **磋商响应文件的形式** | **投标供应商应准备电子磋商响应文件**  **电子磋商响应文件是指通过“政采云电子交易客户端”完成磋商响应文件编制后生成并加密的数据电文形式的电子加密磋商响应文件。** |
| 17 | **磋商响应文件的编制** | **供应商应先安装“政采云电子交易客户端”，并按照本磋商文件和“政府采购云平台”的要求，通过“政采云电子交易客户端”编制并加密磋商响应文件。** |
| 18 | **磋商响应文件份数** | “电子加密磋商响应文件”：在线上传递交，一份。 |
| 19 | **投标有效期** | **提交磋商响应文件截止时间起90天内。** |
| 20 | **磋商响应文件的签章** | **磋商响应文件中所涉及的公章均采用CA电子签章。** |
| 21 | 投标样品 | 不需要  □需要 |
| 22 | 保证金 | 无 |
| 23 | 履约担保 | 不需要  □需要 合同签订后成交供应商应提供合同总金额1%的履约保证金至采购人指定账户（可采用银行转账或银行保函或保险保函）。 |
| 24 | 竞争性磋商文件获取方式 | 见公告具体说明。 |
| 25 | **响应文件递交截止时间**  **投标地点** | **2024年9月29日下午15：00分截止(北京时间)。**  **政府采购云平台在线投标，投标供应商无须前往评审现场递交响应文件。** |
| 26 | **磋商开始时间**  **开标地点** | **磋商开始时间：2024年9月29日下午15：00分 (北京时间)**  **开标地点：温州市洞头区政务服务中心2楼** |
| 27 | **磋商响应文件上传和递交** | **本项目通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应（电子投标），投标供应商应当在响应文件递交截止时间前，将生成的“电子加密磋商响应文件”上传递交至“政府采购云平台”。**  **“电子加密磋商响应文件”的上传、递交：**  **a.投标供应商应在响应文件递交截止时间前将“电子加密磋商响应文件”成功上传递交至“政府采购云平台”，否则投标无效。**  **b.“电子加密磋商响应文件”成功上传递交后，供应商可自行打印磋商响应文件接收回执。** |
| 28 | **电子加密磋商响应文件的解密和异常情况处理** | **1、开标后，采购组织机构将向各投标供应商发出“电子加密磋商响应文件”的解密通知，各投标供应商代表应当在接到解密通知后30分钟内自行完成“电子加密磋商响应文件”的在线解密。**  **2、通过“政府采购云平台”成功上传递交的“电子加密磋商响应文件”无法按时解密的，其磋商响应文件按拒收处理。** |
| 29 | 磋商小组的组建 | 磋商小组构成：由采购人代表以及有关技术、经济等方面的专家组成，成员为3人及以上单数，其中技术、经济类专家不得少于总人数的2/3；评标专家确定方式：按相关规定从专家库中抽取。 |
| 30 | 政府采购  扶持政策 | 本项目对符合财政扶持政策的小微企业（或监狱企业或残疾人福利性单位）给予评标价格优惠。供应商企业属于以上多种性质的，不重复享受扶持政策。 |
| 31 | 供应商  信用查询 | 1、投标供应商信用信息查询的查询渠道：“信用中国”(www.creditchina.gov.cn)；“中国政府采购网”（www.ccgp.gov.cn）；  2、供应商信用信息查询截止时点：公告发布之日至磋商响应文件递交截止时间前。  3、供应商信用信息查询记录和证据留存的具体方式：网页截图打印；  4、信用信息的使用规则：对列入失信被执行人、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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，其投标做无效投标处理。 |
| 32 | 合同备案 | 1、成交供应商须在发出成交通知书之日起30日历天内与采购人签订合同。  2、成交供应商与采购人签订合同后，2日历天内将合同原件交温州华晟招标代理有限公司备案。  3、本项目政府采购合同按规定在浙江政府采购网予以公告。 |
| 33 | 合同履约管理 | 合同签订后，采购人依法加强对合同履约进行管理，并在成交单位供货、项目验收等重要关节，如实填写《合同验收报告》，并及时向同级财政部门报告验收过程中遇到的问题。 |
| 34 | 免责声明 | 1、供应商自行承担投标过程中产生的费用。无论何种因素导致采购项目延期开标、废标（流标）、投标供应商未中标、项目终止采购的，采购人与采购代理机构均不承担供应商投标费用。  2、投标供应商在投标、合同履行过程中必须做好安全保障工作，不因项目实施而危及自身及第三方人员、财产安全。若发生任何安全事故，由成交供应商自行承担一切责任并赔偿损失。 |
| 35 | 质疑 | 供应商认为磋商文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑，逾期采购代理机构可不予受理及答复。供应商须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。在线提起质疑的须上传质疑函扫描件。 |
| 36 | 解释权 | 构成本磋商文件的各个组成文件应互为解释，互为说明；如有不明确或不一致，构成合同文件组成内容的，以合同文件约定内容为准，且以专用合同条款约定的合同文件优先顺序解释；仅适用于采购阶段的约定，按采购公告、供应商须知、评标办法、磋商响应文件格式的先后顺序解释；同一文件中就同一事项的约定不一致的，以逻辑顺序在后者为准；同一文件不同版本之间有不一致的，以形成时间在后者为准。按本款前述约定仍不能形成结论的，由采购人负责解释。 |
| 37 | **注意事项** | **1.请务必确保磋商响应文件制作客户端为最新版本，旧版本可能导致磋商响应文件解密失败。**  **2.请务必确保磋商响应文件制作时所用的 CA 锁与磋商响应文件解密时的 CA 锁为同一把，否则可能导致磋商响应文件解密失败。** |

第二部分 采购内容及要求

**一、采购总说明**

经批准，温州市洞头区大数据管理中心对所需的洞头区政务云平台租赁进行竞争性磋商采购。本次招标的资金已经落实。我们热情欢迎有关公司（企业）前来投标。

**二、项目总则**

1、采购的服务所涉及的产品标准、规范，验收标准、规范，应符合国家有关条例及规范，如有新的标准应采纳新标准，如是国外相应标准应征得采购人认可。

本次招标采购为[洞头区政务云服务](https://www.zcygov.cn/proj-procurement/project-result-detail/5ee80cd0c504722a?utm=web-bid-inviting-front.6a89804f.0.0.b0bc53800b8911ec9f4db3814ed08c6a" \t "https://www.zcygov.cn/bid-inviting/purchaseFileMake/_blank)，投标供应商应根据磋商文件所提出的技术规格和服务要求，综合考虑，选择具有最佳性能价格比的服务前来投标。希望投标供应商以精良的设备、优良的服务和优惠的价格，充分显示你们的竞争实力。

**▲投标供应商必须根据自己的技术及商务和报价优势对标项全部内容进行投标，不得只投标项部分内容。**

**三、采购内容及具体要求**

**标项一：洞头区政务云（公有云）**

**（一）采购内容**

根据温州市政府《关于推进政府大数据平台建设的实施意见》相关要求，温州市洞头区大数据管理中心组织进行洞头区政务云采购，洞头区政务云（公有云）是洞头区政务云平台建设的重要组成部分，主要为全区各政务部门提供高性能云主机、云存储、云应用、云安全、异地备份等基础设施资源共享服务，为各政务部门间数据交换、共享、应用等提供基础平台支撑。

本项目采用企业建设和运维、政府按需购买服务方式进行，通过明确各项服务内容的采购单价和计价规则，对经准确登记云资源进行计费并支付费用。

本项目服务对象是洞头区党政机关、财政全额保障事业单位，服务对象根据政务云实际需求提出申请政务云服务相关需求内容，区大数据中心根据各服务对象实际政务云使用量进行服务费用结算。

服务内容包括：

1、基本云服务：包括政务专用要求、政务云平台带宽、服务区域划分、安全等级、服务支撑等；

2、基础设施服务（IaaS）：包括云平台机房环境及相关物理硬件要求、云平台软件、云平台架构、计算服务、存储服务、网络服务等；

3、平台服务（PaaS）：包括云数据库、高性能数据库、大数据服务等；

4、云安全服务：包括云备份、异地备份、自主云安全服务等；

5、云平台监管及审计：包括云管平台、运行监测系统等；

6、技术支持服务：包括应用迁移咨询服务、其他技术服务、培训服务等。

**（二）服务交付期**

本项目在合同签订后7天内提供本地化的云主机、云存储、云负载均衡、云数据库、互联网出口、政务外网互联链路等服务。同时原有在网系统需在20个自然天内完成迁移。如若未按规定执行，采购人上报采购监管部门后有权取消其中标资格，并重新组织招标或将合同授予第二候选人。

**（三）基本云服务**

投标供应商提供的云服务需要满足以下基本条件：

（1）政务专用要求

要求提供的云平台为洞头区政务外网用户专用，洞头区各级党政机关、事业单位申请使用政务云服务的应由采购方或采购方指定的部门统一受理、审核。未经采购方或采购方指定的部门审核同意，云服务提供商不得擅自对外提供或开放任何政务云服务。

（2）政务云平台带宽

要求提供的政务云平台与市本级以及12个区县政务外网的专用互联光纤带宽不小于1G，以满足网络互访的要求，并提供高可靠的双物理路由保护措施。

要求提供的政务云平台和互联网独享出口总带宽不少于2G,可扩充到20G。▲投标供应商必须承诺其提供的IDC机房接受其他运营商的网络接入。

（3）服务区域划分

本次采购要求提供包括政务云政务外网资源共享专网、政务外网公共服务专网等不同网络环境，同时提供满足不同安全级别、不同业务及不同业务专网的需要，并提供应用测试区域等环境。

（4）安全等级

要求政务云平台应能满足信息系统三级（含）以上安全等级保护要求，须通过信息系统三级（及以上）安全等级测评，并按相关标准定期复测。要求对于核心业务应能实现应用级容灾保护，非关键性业务实现数据级容灾保护。

（5）服务支撑

为保证政务云稳定可靠运行，供应商须提供且不低于下列服务支撑要求：

1、**▲**要求本期至少4人次常驻机房服务，提供7\*24小时运行值班监控服务，同时要求指定一名专职人员负责协调处理各类有关业务，并配备服务终端两台。运维人员必须具备2年以上云平台维护经验，并需提供相关资质证明，相关人员资质及技术能力须由采购方认可。

2、要求组建本地专业政务云维护团队，人员组成必须包含网络、数据库、信息安全、IT管理等领域专业人员组成，并需提供人员相关资质证明，相关人员资质及技术能力须由采购方认可。

3、对使用单位政务应用上云做好培训指导。要求定期举办现场或网络视频培训，免费提供仿真测试环境，供各级部门应用系统正式部署上云前的测试，通过测试优化云资源使用方案，测试时间内不得收费，测试完成后迁移到正式环境。

4、要求协助采购方组织并推荐应用系统功能、性能、安全测试服务。严格按照云平台管理办法对新上云及重大升级后的系统进行入口管理。免费协助采购方进行新开发应用系统部署，并协助完成相关使用单位原有应用系统迁移到政务云平台。

5、要求交付云服务时提供详细的云服务租用清单，并定期（一般按月）提供云服务使用量报表和政务云平台运维日志（包含各类云服务总体的运维工作日志，云安全服务的管理、升级与配置记录，以及采购人认为需要掌握和调用的其他信息）。

6、要求云服务商协助各使用单位开展云平台应急演练；每月对云上政务系统开展安全漏洞扫描工作，并出具相关报告；积极配合测评公司落实业务系统等保测评工作。对上云的政务系统提供备份策略，做好数据备份。

7、要求云服务商每季度至少组织一次对各上云应用系统云资源使用情况的评估并出具报告。云资源部署或扩容调整一个月后，云服务商对云资源利用情况进行评估，对存在云资源过度申请的，须告知采购方进行核查。

8、具备督促检查使用单位落实云资源安全措施能力，对存在的安全风险，云服务商应及时通知使用单位，使用单位通过云管系统对落实情况一一进行回复登记，安全风险整改落实情况定期报采购方；负责定期向各使用单位提供系统安全漏洞月报；在重保和安全专项检查期间定期提供专项安全风险报告。

9、要求云服务商在评估验证的基础上，为使用单位推荐系统及数据备份服务、安全服务等。

10、云服务商负责云平台的整体平台安全，承担平台问题导致的安全责任。

**（四）基础设施服务（IaaS）**

（1）云平台机房环境及相关物理硬件要求

1、云平台数据中心机房标准

要求机房符合国际标准的数据中心机房，A级以上，能够365天全天候稳定提供优质的电力、空调、消防、监控、机架、空气清风系统等服务，政务云专用机房面积不小于300平方，且为完全独立空间，配套独立门禁,非经授权外人不能进入。保证7\*24小时电力供应，供电保障系统需配置保障油机1500KWA或更高的规格,并实现油机1+1备份、不间断电源系统需配置400KVA（1+1）或更高的UPS规格，机房基础安全设施需配置管网式气体消防、早期烟雾告警、门禁系统等系统。

2、物理服务器

物理服务器数量不少于150台 ，主要用于承载业务系统的云主机服务。服务器不低于如下配置：2路INTEL XeonE5-2650V2 CPU（核数8核，主频2.6GHz），内存≥128G，双电源。要求可根据用户使用情况进行扩展，不会导致业务中断。云平台单集群支持不少于5000台物理服务器。

3、物理存储设备

物理存储容量不少于 1 PB，要求可根据用户使用情况进行扩展，扩展过程中不会导致业务中断。云存储采用分布式文件系统。

4、物理网络

为保证网络高可靠性、高可用性、高扩展性、冗余性，要求采用双核心和接入两层扁平化的组网架构，分别构建独立的业务网、管理网、存储网，核心接入之间万兆捆绑互联；所有服务器分别双归属接入业务网、管理网、存储网。

要求保证产品成熟可靠。适应40GE和100GE以太网标准，并且充分满足数据中心级的应用及发展需求，核心层设备应采用具有新一代交换架构的产品。

要求满足今后5年内洞头各地各部门（单位）对政务云平台中业务应用网络带宽、业务平稳、持续不间断运行等应用需要。

（2）云平台软件

供应商的云平台软件需要基于成熟、大规模商用、安全的云平台，有成功应用案例。

1、云平台自主知识产权

云平台软件，必须提供原厂知识产权证明，并能够不依赖于第三方，具备对全部软件代码的自主研发、升级、及时的bug修复能力。

2、大数据服务能力

云平台需具备分布式大数据服务能力，提供成熟的大规模数据处理平台案例。提供统一的数据开发平台，云平台集成统一的大数据运维管理。

3、云平台安全合规

云平台需通过工信部可信云认证。

4、云平台案例

要求云平台已商业化运行，经过了市场的有效检验。要求提供所投标的云平台在政府领域使用案例3个（含）以上，提供用户合同扫描件，合同必须包括用户购买云平台的详细情况。

5、与现有云平台的兼容性

云平台要求与现有市政务云（公有云）平台全面兼容，新老平台可整体进行整合。如与现平台采用不同的技术路线，则要求能在业务不中断的情况下实现所有云资源的整体迁移。

（3）云平台架构

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 标准规范 | 采用统一管理集群资源，统一管理集群内的CPU、内存、磁盘和网络资源使得这些关键资源可以被高效地使用。 |
| 具备分布式系统底层服务、分布式文件系统、任务调度、集群监控和部署能力并提供技术白皮佐证。 |
| 根据应用对资源进行全局的调度，提高资源的利用率。 |
| 采用自动故障切换提高系统整体的可用性。 |
| 采用统一的安全措施，保证用户数据的安全性。 |
| 采用统一运维的方式，提高系统的安全并降低成本。 |
| 扩展规模 | 支持在线集群扩容和应用服务的在线升级。 |
| 单个集群最大规模可达到5000台物理服务器并行作业。 |
| 资源管理 | 提供计算存储设备，网络设备和安全设备等物理设备的管理功能。 |
| 提供虚拟化后的“分布式计算资源池”、“网络资源池”和“存储资源池”的管理功能。 |
| 提供对网络资源的管理功能，包括：IP地址资源和带宽资源的管理。 |
| 提供资源协同能力，包括资源的注册、创建、销毁、回收、状态同步、分布式锁服务，支持分布式共识协议。 |
| 提供集群并行作业能力，实现资源的高可用和集群的负载均衡能力。 |
| 远程过程调用 | 提供可靠高效的进程间远程调用服务，支持通讯信道的数据压缩和一致性校验。 |
| 分布协同服务 | 分布协同服务提供分布式系统基本的命名服务、状态同步服务和分布式锁服务。支持基于Paxos的分布式共识协议。 |
| 虚拟化功能 | 支持并配置计算资源虚拟化，形成“分布式计算资源池”。硬件采用标准X86服务器，不使用IP SAN和FC SAN等专用存储作为存储资源。 |
| 支持并配置计算设备“一虚多”，同一台物理主机上同时支持多种操作系统，或是相同操作系统的不同版本。分区与分区之间相互独立，互不影响。 |
| 支持并配置资源的动态调配与弹性可伸缩，资源池具备各级资源的按需获取功能，提高资源消费者的可用性、容错与扩展能力。 |
| 分布式文件系统 | 云平台操作系统支持分布式文件系统，支持存储资源虚拟化,形成“存储资源池”。 |
| 数据存储在不同机架的多个节点上，集群中的节点出现硬件、软件故障,集群系统能够自动进行数据的备份和迁移,保证数据的高可用性在并提供技术白皮书佐证。 |
| 支持IO优先级控制和QoS保证。 |
| 支持增量扩容和自动数据平衡能力，允许用户定制数据分布策略。 |
| 具备高可扩展性，可支持上亿个文件和100PB以上量级的文件存储；支持不重启系统，增加物理服务器后自动扩容。 |
| 在不依赖RAID卡和NAS等特殊硬件设备的条件下，提供高可用性和高可靠性。 |
| 支持SATA磁盘块存储和SSD高性能块存储两种分布式存储规格。 |
| 普通分布式存储吞吐大于等80M/s，高性能分布式存储吞吐大于等于280M/s，随机IOPS大于等于20000。 |
| 采用多管理节点设计，为避免集群单点故障，分布式文件系统必须支持多Master设计，至少有3个及以上的存储Master控制节点。 |
| 分布式文件系统上创建出的单个存储盘，能够被多个虚机同时挂载，实现共享存储功能。 |
| 任务调度 | 提供一个数据驱动的多级流水线并行计算框架，兼容业界主流的多种编程模型。 |
| 提供并行任务调度能力，且具备高可扩展性，最高可支持十万以上级的并行任务调度。 |
| 实现自动检测故障和系统热点，重试失败任务，保证作业稳定可靠运行完成。 |

（4）计算服务

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 基本功能 | ★云主机CPU核数可选范围1-32核， 128G内存、8TB数据盘。（提供截图证明） |
| ★互联网出口独享带宽可选范围2-100Mb。（提供截图证明） |
| 虚拟主机支持主流的WINDOWS、LINUX等操作系统，兼容常见的操作系统。 |
| 扩展功能 | 按需开通。根据用户的需求动态的创建和分配计算、存储、网络带宽等资源；用户可以在线按时长购买云主机，并支持任意时刻的续费管理。 |
| 云主机创建。创建后，云主机已包含有操作系统，可立即使用，从创建到启动在5分钟以内。 |
| 云主机升级。当云主机现有配置不满足要求时，用户可自主进行云主机配置快速升级，可升级配置包括：CPU，内存，网络带宽等；配置升级生效时间在10分钟以内。 |
| 云主机克隆。指创建一台跟现有云主机一模一样的机器，根据云主机数据盘的大小整个克隆过程一般在15分钟以内。 |
| 云主机迁移。云平台根据物理主机负载情况综合调度，将云主机在不停机状态下从一台物理主机迁移到另外一台物理主机；在线迁移时，云主机应用完全不中断，用户完全无感知。 |
| 管理功能 | 提供用户自服务门户和API接口，用户可自行创建不同规格的虚拟主机，自定义CPU、内存、网络、磁盘等属性。 |
| 提供虚拟主机的动态升级、快照备份、性能监测分析、异常告警、日志管理等功能。 |
| 提供快照和自定义镜像能力，支持对运行或停止状态的虚拟主机生成快照，应提供分钟级别快照回滚功能。 |
| 可靠性 | 数据备份。云主机数据在云计算平台有三份（含）以上数据拷贝，单份数据损坏对云主机使用没任何影响，且一份数据损坏后，后台系统会自动拷贝，使数据始终保证三重备份。 |
| 磁盘快照。需要提供云主机任一时刻的磁盘快照功能，含快照制作，快照回滚，快照恢复等。 |
| 故障恢复。云主机发生故障后，切换恢复时间在30分钟以内。 |
| 虚拟主机服务采用全冗余架构，无单点故障，平均可用性不低于99.9%。 |
| 安全性 | 防ARP欺骗，防DDos攻击，提供流量清洗服务。 |
| 用户可自助开通防火墙，并定义防火墙规则。 |
| 网络隔离。支持两块网卡，不同网卡连接不同网络安全域。 |

（5）存储服务

|  |  |
| --- | --- |
| **1、存储功能要求** | |
| 指标项 | 规格要求 |
| 基本功能 | 支持海量存储，文件数量无限制，容量按用户需求扩展。 |
| 采用分布式存储，一份数据在不同的物理服务器上存三份备份。 |
| 采用分布式存储系统，支持大规模强结构化数据存储，如SQL关系性数据库，单库容量可达1TB。 |
| 采用分布式存储系统，支持大规模结构、半结构化数据存储，如NOSQL数据库,单表支持的存储空间可达100TB。 |
| 扩展功能 | 提供存储对象的读、写、删除、拷贝、查找等基本功能。 |
| 支持大存储对象的分片并发上传和下载，支持断点续传。 |
| 提供易用的用户Web控制台文件管理界面，与更多第三方工具、插件，满足各种应用需求。 |
| 提供完整的API接口、SDK开发包、文档说明。 |
| 存储管理 | 支持将数据以对象方式进行存储，用户可以通过调用API以对象为单位操纵存储的数据，实现在任何应用、任何时间、任何地点上传和下载数据，也可以通过用户Web控制台对数据进行简单的管理。 |
| 大文件支持 | 支持并配置分段上传大文件，单个分段最大5GB，最大分段数≥5000段。支持断点续传。 |
| 安全性 | 具备完善的多用户隔离机制，保障用户数据的私密性。 |
| 云服务端提供加密用户身份验证，提供签名权限控制与防盗链功能。 |
| **2、数据盘（含SSD数据盘和高效数据盘）** | |
| 指标项 | 规格要求 |
| SSD云盘 | 采用SSD盘做为存储机制，提供稳定的高随机I/O。 |
| 采用分布式三副本机制，99.9999999%数据可靠性。 |
| 高性能存储，最高提供2万的随机读写IOPS、256MB/s的吞吐能力。 |
| 单独挂载:SSD云盘支持挂载到相同区内的任意ECS实例上。 |
| 高效云盘 | 采用固态硬盘与机械硬盘的混合基质作为存储机制。 |
| 采用分布式三副本机制，99.9999999%数据可靠性。 |
| 单独挂载:高效云盘支持挂载到相同区内的任意ECS实例上。 |
| 最高提供3000的随机读写IOPS、80MB/s的吞吐能力。 |

（6）网络服务

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 安全稳定 | 采用分布式结构，具有高度的冗余和可靠性，可根据系统负载弹性扩容。 |
| 透明接入 | 提供4层和7层的负载均衡；Web和中间件服务器，无需更改配置即可透明接入。 |
| 健康检查 | 可以按照指定规则进行健康检查，自动隔离异常状态云主机，并迅速将服务切换，服务切换时间秒级。 |
| 会话保持 | 可以将用户和后台服务器绑定到同一会话，确保会话不中断。其中4层负载均衡可以设置连接持久时间。 |
| 权重转发 | ★可根据后台云服务器的性能设置不同的转发权重，权重支持轮询，最小连接数转发等方式。（提供截图证明） |
| 易用简单 | 提供API或控制台调用方式，可以随时开启，关闭负载均衡，立即生效，灵活简单。 |
| 按需计费 | 支持按流量、使用时间进行计费。 |

**（五）平台服务（PaaS）**

（1）云数据库

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 基本功能 | 基于高效的调度、备份、HA控制、在线迁移以及监控系统，为用户提供为专业的云数据库服务。 |
| 支持关系型数据库的基本功能，并进行优化服务。 |
| ★云平台提供MsSqlserver、Mysql主流关系型数据库服务；云主机上可安装Oracle数据库。（提供截图证明） |
| 单数据库实例内存可达24G，IOPS可达12000次，并发连接数可达2000。 |
| MsSqlserver单数据库实例可创建的数据库数量达20个，用户数达20个。 |
| Mysql单数据库实例可创建的数据库数量达200个，用户数达50个。 |
| 每份数据都保留两份并可实时切换。 |
| 支持数据库在线升级、云内动态迁移、故障自动切换，实现业务秒级无缝切换，不中断用户服务。 |
| 自动多重备份数据库，支持从备份文件创建临时实例，支持从备份文件恢复到实例，可下载备份文件。 |
| 扩展功能 | 按需开通，即开即用，按需计费，为用户提供方便的Web管理界面。 |
| 随着用户数和访问量的变化，可以弹性的调整数据库的规格，包含内存、连接数、IOPS、存储容量等，调整时服务不间断。 |
| 提供数据导入、导出工具，方便用户进行数据迁移。 |
| 提供完整的API接口、SDK开发包、文档说明。 |
| 提供日志记录功能，包括错误日志、操作日志、访问日志等，可追查访问来源以及进行多维度的统计分析。 |
| 安全性 | 支持IP授权访问。 |
| 云服务端提供加密用户身份验证，提供不同的访问权限控制。 |
| 提供数据库存储加密服务。 |

（2）高性能数据库

供应商的高性能数据库平台软件需要兼容基于成熟、大规模商用、安全的云平台，有成功应用案例，主要为Oracle、MySQL等数据库提供专用、高性能、高可靠、高扩展的数据库云平台。同时，考虑到后期平台的扩展性和可持续性要求，对国产化软硬件等方面均需具备兼容性。本项目对高性能数据库平台的总体要求如下所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 指标项 | | | 规格要求 |
| 整体要求 | 数据库支持 | ★支持多种数据库，包括但不限于Oracle、MySQL，PostgreSQL等（提供截图或证明）。 | |
| 支持3种以上国产数据库，如达梦、Gbase。 | |
| 网络协议 | 支持基于NVMe Over Fabrics的RDMA协议，并能运行在Mellanox Infiniband和Intel OPA上。 | |
| 内部互联网络能够支持Mellanox Infiniband网络和ROCE网络。 | |
| 存储软件要求 | 存储资源管理 | ★支持对存储卷的快照、克隆、自动精简配置、Qos等功能。（提供截图证明） | |
| 分布式存储支持一键更换存储磁盘功能；存储日志一键收集功能；存储软件一键扩容功能。 | |
| 功能要求 | 分布式存储可实现数据副本保护，支持两、三副本冗余保护，任意一个存储节点离线维护，而不影响存储层服务和上层数据库平台的正常运行。 | |
| 云平台可同时为多个异构数据库系统提供存储服务。 | |
| 支持在一套云平台内，同时部署多套、异构数据库系统，可以通过CPU核绑定、内存预分配、IO直通、独立运行操作系统等隔离方式，为不同数据库运行提供基础环境，确保数据库性能及稳定性。 | |
| 缓存管理 | ★支持SSD/PCIe闪存卡盘作为永久非易失读、写缓存使用，同时缓存管理机制应当智能化，能够根据数据访问特征进行自动的优化调整，并且支持热插拔。  （请提供具体的实现方式、架构说明）。 | |
| 支持缓存部件在线迁移更换，能够在线完成寿命到期的SSD的在线更换。 | |
| 支持自动/手动Flush数据刷新模式，刷新频率及速度可自定义设置。 | |
| 支持缓存中划分LUN用于全闪空间。 | |
| 支持缓存读写缓存空间的在线调整，部件在线迁移，能够在线完成。 | |
| ★支持多种缓存模式，支持Writeback和Writethrough、RAW三种缓存模式，并能支持三种缓存模式的在线转换（提供截图证明）。 | |
| 管理平台要求 | 数据库管理 | 支持云平台的告警监控，包含但不限于CPU、内存、硬盘、闪存、容量、网络、存储软件等。 | |
| 支持云平台各节点性能监控，包含但不限于CPU、内存、磁盘使用率、IOPS、MBPS，Cache命中率、链路等。 | |
| 支持数据库告警监控，包含但不限于数据库状态、日志、空间等。 | |
| ★支持数据库集群管理，包括集群启停、相关参数设置、ocr增加和删除、vote迁移、监听启停等（提供截图证明）。 | |
| 支持数据库管理，包括启停、创建、删除，相关参数查看与修改，redo的增加和删除。 | |
| 支持数据库表空间管理，包括增加、删除及数据库文件的增加和扩展。 | |
| 支持ASM管理，包括磁盘组的创建和删除、mount和unmount、兼容性参数修改、重平衡等。 | |
| 可追踪监控SQL语句运行效率，并能查看SQL的执行计划。 | |
| 支持Oracle、MySQL等多种数据库数据库按照模板创建，混合部署 | |
| 节点管理 | 支持逻辑卷挂载权限控制。 | |
| 高级管理 | 全局拓扑图管理  展示计算层、网络层、存储层全局拓扑；  展示节点、交换机状态；  展示端口状态、展示lvvote卷状态；  支持单数据中心、多数据中心拓扑图显示。 | |
| 容灾演练  支持在拓扑图上进行节点重启、端口disable、enable等容灾演练操作。 | |
| 仲裁管理  支持展示集群内所有仲裁盘的状态图。 | |
| IO优先访问  支持展示ASM IO优先读取的拓扑展示，包括即ASM实例优先读取哪些节点上的数据。  支持计算节点到存储节点IO链路延时曲线显示。 | |
| 系统监控 | 支持告警发送、事件处理、规则定义及汇总报表。 | |
| 管理软件必须实现完整的集中化监控管理，即通过统一的管理软件和界面实现对硬件、操作系统、交换网络、数据库、分布式存储软件的状态和性能进行监控和管理。 | |
| 系统配置 | ★管理界面支持基于角色的用户权限管理（提供截图证明）。 | |

（3）大数据服务

1、离线大数据平台

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 总体描述 | 离线大数据平台采用分布式计算框架提供大规模数据存储与计算，提供快速、完全托管的 GB/TB/PB 级数据仓库服务。 |
| 数据存储 | 与云平台采用相同的分布式文件管理系统。 |
| 支持结构化及非结构化存储。 |
| 数据装载 | 具备完善的数据装载机制，支持高并发、高吞吐量的大规模数据上传下载，可以与虚拟主机服务、关系型数据库服务和对象存储服务实现数据同步；数据装载具有线性扩展能力。 |
| 双数据通道，批量、历史数据通道和实时、增量数据通道，支持全量和增量的源数据抽取方式；实时增量数据通道支持多种数据传输插件。 |
| 自带数据装载工具支持与第三方插件对接，包括Fluentd、Logstash、OGG等。 |
| SQL查询 | 提供基于SQL的数据处理模式，支持UDF和存储过程，支持窗口函数等高级数据分析功能。 |
| 支持标准的SQL语法，同时兼容Hive SQL语法；支持Java/Python UDF，以及支持窗口函数等高级数据分析功能。 |
| 分布式计算 | 支持MapReduce类型的分布式计算任务；支持DAG模式的作业处理方式。 |
| 作业优先级 | 支持作业优先级设置功能，可支持9级优先级设置，在作业任务资源分配优先级上进行细粒度控制。 |
| 图编程 | 支持的Graph图编程功能，支持面向迭代的图计算处理框架。 |
| 机器学习算法 | 支持分布式的集群学习算法库，包括逻辑回归、随机森林、GBRT、决策树、线性支持向量机、朴素贝叶斯、GBDT等算法。 |
| 多租户 | 支持多租户，支持用户空间保护与跨用户空间访问授权。支持项目空间级别的安全配置，项目拥有者可以定制适合自己的外部账号支持和鉴权模型。 |
| 安全性 | 具备完善的用户和权限认证机制，支持ACL和Policy授权机制。 |
| 具备完善的用户空间隔离机制，提供多级安全沙箱防护及监控能力，保障用户数据的私密性。 |
| 为提升安全性，对数据的访问必须通过统一访问和授权入口，且底层文件形态对用户不可见。 |
| 支持多粒度的数据授权访问，可针对单表或某一字段指定授权。 |
| 提供用户操作审计功能。 |
| 高可用性 | 大数据计算平台底层采用分布式文件系统，数据存储可达到三副本可靠性；数据可靠性不低于99.99%。 |
| 采用全冗余架构，无单点故障；服务可用性不低于99.9%。 |
| 扩展性 | 支持将数据以结构化的二维表的形式处理，二维表支持分区。 |
| 数据管理 | 支持列存储结构，支持数据压缩存储，最大可压缩5倍。 |

2、大数据开发套件服务

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 数据集成基础模块 | 项目新建时，支持开发项目、测试项目、预发项目、生产项目，分别用做开发环境、测试环境、预发环境、生产环境；支持不同的环境采用不同的计算引擎，保障环境之间的独立性和隔离性，并支持指定不同项目之间的发布关系。 |
| 安全性要求 | 具备完善的权限认证与隔离机制，保障用户数据的私密性。 |

**（六）云安全服务**

（1）安全目标

1、明确安全工作界面、维护责任界面

明确定义政务云安全工作中的关键角色及其安全工作任务；规划设计政务云信息安全管理组织架构，细化各岗位的工作职责。全面梳理各个关键角色的安全工作内容及责任划分，细化事前、事中、事后各项安全工作的分工和各角色之间的责任边界。

2、建立全面的安全监测机制

内部对云计算平台、网络设备、安全设备、应用软件等进行多层次的动态事件监控；外部实施全网全方位的网络安全监测，实现安全事件的统一收集和处理，用于预警、分析和追查。实现尽早预测安全威胁、及时发现安全事件；进而快速做好防护应对，全面掌控政务云的安全现状。

3、综合运用各种安全保障技术解决实际问题

根据应用的实际安全需求制定切实可行的安全防护策略。将传统安全保障措施与先进安全技术相结合，科学解决云计算应用和互联网发展带来的网络安全风险与隐患，保障云平台安全和各种具体应用场景下的安全，有效提高抵御和防范风险能力。

（2）云备份

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 备份兼容性 | 支持LAN、LAN-free等多种备份方式。 |
| 备份方式 | 备份系统为专用基于Linux的64位嵌入式系统，减少病毒感染几率，确保系统稳定。 |
| 备份安全性 | 产品可实现对物理机环境以及虚拟机环境的的一体化保护（一个备份模块，无需单独配置其他备份模块），实现对机房重要系统的统一备份与管理。 |
| 同步备份 | 产品能实现对应用服务器的一体化备份，实现对服务器上隐藏分区、操作系统分区、数据分区等所有分区一体化直接实时备份成虚拟化磁盘镜像格式(无需第三方工具转换)；千兆网环境初始化备份，任何类型应用和数据都能保持速度不低于60MB/s；基于磁盘卷变化增量复制，复制系统卷分区大小，属性，权限，加密等要必须完全一致。 |
| 采用块级复制技术，支持数据的增量备份，系统能实现将包括系统、应用以及数据在内的整机直接实时备份成虚拟化磁盘镜像格式，可实现数据的秒级同步。 |
| 支持对备份数据的快照功能，支持保留不同时间版本的备份数据。 |
| 支持对备份数据的安全删除策略设置，支持对备份数据集阀值设置。 |
| 支持平台内源生的OVS虚拟网络；支持平台与不同的OVS虚拟网络间互相联通，提升平台与不同网络间的互联互通。 |
| 支持对同步时间段设置，可以设定只允许在某个时间段进行同步。 |
| 支持对快照时间段进行设置，可设定只允许在某个时间段进行快照。 |
| 支持将本地备份数据可远程复制到异地，当本地发生场地灾难时，依旧可以通过异地的备份数据进行恢复。 |
| 支持断点续传特性，当远程复制过程中出现中断时，恢复正常后可基于上一次断点处进行续传。 |
| 支持流量限速及固定时段暂停传输，当远程复制链路资源比较紧张时，可通过流量限速和在固定时段内暂停远程复制以减小对正常业务的影响。 |
| 支持整机备份、数据库单独备份等多种备份功能，整机备份支持全盘备份与增量备份，数据库备份支持全备份、增量备份以及差异备份等多种模式。 |
| 支持备份数据的远程挂载，备份的格式文件中任何时间点的硬盘分区远程挂载任意设备上，从而实现小文件和单个库文件的恢复。挂载分区属性大小等与原机保持完全一致。直接通过文件拷贝的方式即可实现对单个文件的颗粒级恢复。 |
| 支持各种单机环境、主备集群、RAC集群的应急接管，支持本地磁盘、共享磁盘、多路径软件环境。 |
| 业务恢复 | 支持对备份业务系统的分区恢复功能，可直接进行系统分区或者数据分区的单个分区的数据恢复。 |
| 提供对备份业务系统的整机恢复功能，可直接实现操作系统、应用环境以及生产数据的一体化整体恢复。 |
| 支持1对多温热灾备，单平台可实现不低于20:1的主机在线容灾规模；支持业务主机分钟级的容灾恢复能力。（提供实现业务快速恢复相关证明文件）。 |
| 支持主机的平台解耦后，构建成独立的VM系统文件；支持解耦后的VM文件，可耦合到不同的云平台上，便于在不同云平台间的统一灾备。 |
| 产品支持对不同品牌不同型号不同配置服务器的本地/远程恢复功能，可直接将故障生产系统整机本地/远程恢复到不同品牌不同型号不同配置的服务器上，恢复包括操作系统、应用环境以及生产数据等所有数据，恢复完成之后，开机即可用。 |
| 能模拟采购人任何基于X86架构的应用环境，一键可仿真原应用生产环境（系统+数据）。可同时启动多个时间版本，整个测试过程对平台作业和生产业务无任何影响。可对测试过程进行手动/自动的流程化记录保存，包括截图、日志等形式，对测试进行全流程管理。支持用户同一套业务包含多台主机的整套环境的模拟；不接受手动搭建、配置任何模块。 |
| GIS分级管理。支持基于地图，多系统集中管控，实时信息采集和展示，提供精准区域故障报警功能及系统资源分布情况信息。 |
| 业务预警 | 要求存储管理、存储快照复制管理、备份管理、远程复制管理、用户及权限管理等均在一个管理界面内，中文界面，基于WEB管理模式，易于管理与维护。 |
| 能够监测被保护服务器的CPU/内存/网络/IO等性能，对数据库/中间件等其他应用能够监控运行状况；能够模拟用户访问方式对各种应用服务提供运行安全监控，支持用户自定义数据库、应用监控脚本的运行。并提供基于事件的统计报表、生成图表，提供邮件、短信等通知手段。对备份系统各种状况进行统计和报警，并提供各种统计报表。 |

（3）异地备份

供应商需为云平台的数据提供异地备份节点，备份节点和本地节点的距离要求大于60公里。

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 备份方式 | 备份系统为专用基于Linux的64位嵌入式系统，减少病毒感染几率，确保系统稳定。 |
| 备份安全性 | 产品可实现对物理机环境以及虚拟机环境的的一体化保护（一个备份模块，无需单独配置其他备份模块），实现对机房重要系统的统一备份与管理。 |
| 同步备份 | 产品能实现对应用服务器的一体化备份，实现对服务器上隐藏分区、操作系统分区、数据分区等所有分区一体化直接实时备份成虚拟化磁盘镜像格式(无需第三方工具转换)。 |
| 采用块级复制技术，支持数据的增量备份，系统能实现将包括系统、应用以及数据在内的整机直接实时备份成虚拟化磁盘镜像格式。 |
| 支持对备份数据的安全删除策略设置，支持对备份数据集阀值设置； |
| 支持平台内源生的OVS虚拟网络；支持平台与不同的OVS虚拟网络间互相联通，提升平台与不同网络间的互联互通。 |
| 支持将本地备份数据可远程复制到异地，当本地发生场地灾难时，依旧可以通过异地的备份数据进行恢复。 |
| ★支持断点续传特性，当远程复制过程中出现中断时，恢复正常后可基于上一次断点处进行续传。（提供截图证明） |
| 支持流量限速及固定时段暂停传输，当远程复制链路资源比较紧张时，可通过流量限速和在固定时段内暂停远程复制以减小对正常业务的影响。 |
| 支持备份数据的远程挂载，备份的格式文件中任何时间点的硬盘分区远程挂载任意设备上，从而实现小文件和单个库文件的恢复。挂载分区属性大小等与原机保持完全一致。直接通过文件拷贝的方式即可实现对单个文件的颗粒级恢复。 |
| 业务恢复 | 支持对备份业务系统的分区恢复功能，可直接进行系统分区或者数据分区的单个分区的数据恢复。 |
| 提供对备份业务系统的整机恢复功能，可直接实现操作系统、应用环境以及生产数据的一体化整体恢复。 |
| 支持主机的平台解耦后，构建成独立的VM系统文件；支持解耦后的VM文件，可耦合到不同的云平台上，便于在不同云平台间的统一灾备。 |
| 产品支持对不同品牌不同型号不同配置服务器的本地/远程恢复功能，可直接将故障生产系统整机本地/远程恢复到不同品牌不同型号不同配置的服务器上，恢复包括操作系统、应用环境以及生产数据等所有数据，恢复完成之后，开机即可用。 |

（4）自主云安全服务

除基础共性服务全覆盖外，通过建设云安全资源池，落实安全服务目录化，云上用户可根据需要，构建自己的安全防护体系。满足云上用户对安全的各种需要，覆盖从远程接入、边界防护、入侵防护、病毒过滤、终端防护、堡垒机、数据库审计等全面的安全能力。

1、统一基础云安全服务

（1）漏洞扫描服务要求

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 漏洞扫描管理 | 1）提供采用SMB、SSH、Telnet、RDP、SNMP等协议对Windows、Linux系统进行登录授权扫描；厂商漏洞特征库不少于53000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容；主流的应用服务WWW、FTP、DNS、SMTP等等。  2）支持云平台扫描，漏洞覆盖OpenStack、Kvm、VMware、Xen等主流的云计算平台；支持对各种网络主机、操作系统、网络设备(如交换机、路由器、防火墙等)、常用软件以及应用系统的识别和漏洞扫描。  支持识别国内外主流Web应用防火墙品牌。  3）支持常见Web漏洞类型的扫描，包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL跳转、文件包含、反序列化漏洞、文件上传、CSRF跨站请求伪造、信息泄露等。支持OWASP TOP10等主流安全漏洞。  4）支持Oracle、Mysql、SQLServer、DB2、informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描。  5）支持在线查看报告和离线导出报告，报告导出可将弱口令隐藏不以明文的形式展现至报告。 |
| 扫描策略管理 | 1）数据库扫描的漏洞库数量大于3000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD等国际、国内漏洞库标准兼容。  2）用户可自定义扫描端口范围、端口扫描策略等扫描选项。  3）数据库扫描支持的检测类型大于10种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL注入、危险程序、安全信息查看等。 |
| 漏洞库 | 数据库扫描的漏洞库数量大于3000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD等国际、国内漏洞库标准兼容。 |
| 服务要求 | 每月进行一次全面漏洞扫描，并向政务云平台租户提供漏洞分析报告和修复建议。网络安保重点时期可根据采购方要求，适当增加扫描频次和范围。 |

（2）入侵防御服务要求

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 入侵防护功能 | 系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、web序列化、webshell等主流防护类型。 |
| 预置防护模板，可基于常见场景进行一键式的安全加固；支持基于常见协议进行异常检查，包括但不限于：HTTP、DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：url长度、请求头长度、目录长度、host字段、version字段，支持针对每协议设置处置动作和事件等级。 |
| 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能。 |
| 支持日志聚合，可按照源IP、目的IP、防护规则和源目IP等维度进行聚合，方便管理员快速进行攻击事件统计和回溯。 |
| 支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户。 |
| 服务要求 | 部署在政务云平台边界，对全流量进行清洗分析，含运维管理服务，安排专人定期巡检和分析日志，及时向政务云平台采购方和租户通报入侵防御重要安全风险事件，并协助租户按需完成策略调整与优化。 |

（3）防DDoS攻击服务要求

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 技术参数 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。 |
| 支持云内访问控制，配置云内区域只允许指定的IP地址或IP范围对外进行访问，防止内部伪造源IP对外DoS攻击的情况。 |
| 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为。 |
| 服务要求 | 部署在政务云平台边界，对全流量进行清洗分析，含运维管理服务，安排专人定期巡检和分析日志，及时向政务云平台采购方和租户通报重要安全风险事件。 |

2、云安全服务资源池

（1）云下一代防火墙（传统防火墙、防病毒网关）

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 技术参数 | 1）★支持标准IPsec VPN和快速IPsec VPN，标准IPsec VPN认证方式包括数字证书和预共享密钥；同品牌设备快速IPsec VPN对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址。（提供功能截图）  2）★应用特征不少于5000个，移动应用不少于450个；支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等10大类；支持给每个应用自定义标签；支持根据标签选择一类应用做控制。（提供功能截图）  支持源地址转换、目的地址转换、双向NAT等地址转换。  3）自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名。  4）支持PING、TCP、DNS方式进行接口、域名、IP地址连通性和时延探测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示的名单。 |
| 服务要求 | 在政务云边界部署，支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；能够实时监控并显示全网安全设备最近发生的50次有效安全事件，并可以根据时间、类型、ip、设备名称等条件查询历史有效事件日志；支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限。 |

（2）云WAF

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 技术参数 | 1）能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为。  2）支持第三方组件漏洞防护，包括WEB容器漏洞（Nginx、IIS、Tomcat等WEB服务器漏洞）、开源CMS漏洞（Kuwebs、phpcms、TRS WCM、JBR-CMS、DeDeCMS内容管理系统漏洞）、WEB服务器插件漏洞；支持抵御SQL注入、XSS、系统命令等注入型攻击。  3）支内置主流Webshell特征库，对上传内容进行检查，防止恶意Weshell上传。  4）支持网站自学习建模功能，能通过自学习形成网站URL树；通过自学习能生成安全防护策略，发现参数的名称、类型、匹配频率。  5）支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站，可配置攻击者识别策略和算法、锁定时间，展示攻击者发生的时间和攻击者所在的地理位置，支持配置将攻击者直接加入网络黑名单；支持上传文件类型识别，防止文件后缀名修改绕过。  6）★支持对CC攻击进行检测防护，可基于URL、请求头字段、目标IP、请求方法等多种组合条件进行检测；检测对象支持IP或IP+URL算法，IP可支持X\_Forwarded-For字段解析，并支持自定义检测字段功能；支持基于地理位置的识别，可设置不同地理区域的检测算法。（提供功能截图）  7）按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域IP的访问。  8）按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域IP的访问。  9）支持对网站黑链进行检测。  10）根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率。 |
| 服务要求 | 部署在政务云平台边界，可根据需要对流量进行清洗分析，含运维管理服务，安排专人定期巡检和分析日志，及时向政务云平台采购方和租户通报重要安全风险事件，并协助租户按需完成策略调整与优化。 |

（3）云数据库审计

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 基本要求 | 1）支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、MariaDB等主流数据库审计；支持PostgreSQL、GuassDB、HANA、Teradata、Cache、人大金仓、达梦、Redis审计。 2）支持MongoDB、Hbase、Hive、Impala、Elastic Search、HDFS、Canssandra非关系型数据库审计。 3）★支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单（提供功能截图）。 |
| 详细要求 | 1. ★内置安全特征库不少于900条，如SQL注入、缓冲区溢出（提供功能截图）。   2）支持主流业务协议HTTP、HTTPS、Telnet、FTP的审计。 3）支持用户界面告警、SNMP、邮件、短信、钉钉、SYSLOG方式告警。 4）支持报表页面信息钻取。 5）支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询。 |
| 服务要求 | 含运维管理服务，安排专人定期进行日志分析，并定期向租户提供专项分析报表。 |

（4）云VPN 安全接入

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 基本要求 | 1）支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务。 2）支持用户名密码认证、IP+MAC绑定认证、支持自定义广告，实现首次URL重定向。 |
| 详细要求 | 1）支持针对跨运营商访问业务实现链路加速优化，消除丢包和延迟业务体验慢情况 2）具有20多个大类、超过850条应用识别规则，并支持应用协议识别库实时更新。 3）通过平台对VPN策略编辑、部署和维护；支持离线配置；新策略支持即时下发和定时下发两种模式；可在线禁用、中断用户联接；策略数据库支持定时自动备份。 4）不依赖于第三方的基于动态IP寻址的VPN组网技术（非DDNS方式，提供自主知识产权证明） 5）支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，[M7.1版本差异化优势，目前已知厂商中没有能支持的。可控性很强。GOOGLE Chrome最新版本，在不翻墙情况下，国内其他厂商没有支持的。]Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。 6）可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果。 7）支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统 。 8）支持针对移动APP的VPN安全代码的自动封装，实现APP应用的双区域隔离。 |
| 服务要求 | 含运维管理服务，包括用户管理和技术支撑服务等。 |

（5）云运维审计（堡垒机）

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 身份认证及访问授权 | 1）支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。  2）★支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机（提供功能截图）。  3）混合云管理：可以通过socks5/http/ssh等代理协议连接管理异地云资源区中私有网络的云主机。  4）客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力；  支持对堡垒主机的配置行为进行审计记录。  5）★可以使用SSH-agent-forwarding登录到ssh服务器，用于登录堡垒机和登录ssh主机使用相同私钥的场景（提供功能截图）；  支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备。 |
| 访问控制及异常告警 | 1）管理员对运维工单进行审核之后以邮件方式通知给运维人员；如果允许，则运维人员才可访问；否则就无法访问。  2）运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。 |
| 服务要求 | 含运维管理服务，含用户VPN接入服务；安排专人定期进行运行监控，支持电话、网上值班等响应方式。 |

（6）云日志审计

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 数据采集 | 设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等；支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]。 |
| 监控功能 | 1）支持通过在目标主机上安装agent程序，监控目标主机的CPU利用率、内存使用率、磁盘使用率、流量等信息。  2）支持对操作系统（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）进行性能监控。 |
| 服务要求 | 含运维管理服务，安排专人定期进行日志分析，并定期向租户提供专项分析报表。 |

（7）云主机安全（EDR）

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 基本要求 | 1）支持Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、win xp 、win 7、win 8、win 10、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、Ubuntu 14 +、华为鲲鹏、中标麒麟、银河麒麟、凝思等操作系统。 2）Apache 2.0-2.4、IIS6、IIS7、IIS8、IIS10、Java系列(JBoss、Tomcat、Weblogic、Websphere)等。 3）MSSQL，Oracle、Sybase、Informix、DB2、MySQL等关系型数据库；Mongodb、Cassandra等非关系型数据库。 |
| 核心功能 | 1）支持防端口扫描，防违规外联，锁定恶意的端口扫描及外联行为，并记录告警。  2）★违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。（提供功能截图）。  3）支持网站防护，包括SQL注入、XSS、Web应用及容器漏洞防护、访问控制、屏蔽扫描器等。  4）支持智能检测防御CC攻击，并可进行高、中、低三档设置。  5）内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。  6）★支持流量画像，支持全网流量可视化；支持威胁横向扩散路径可视化与一键阻断；支持违规外联路径可视化与一键阻断。（提供功能截图）。  7）管理中心可作为补丁服务器，支持管理中心可上网和不可上网2种情况。提供离线补丁下载器，按需智能获取内网所需补丁。  8）支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux等）、数据库漏洞（Mysql等）、Web容器漏洞（Tomcat、Apache、Ngnix等）、其他组件漏洞。  9）移动存储介质管理。  10）防病毒模块，支持文件实时监控，在进程启动、文件创建、存储介质连接时自动触发。可保护系统指定文件不被恶意篡改或执行。可防止指定命令被恶意利用，损害主机。（支持对顽固流行病毒进行智能拦截。  11）提供专门的勒索风险评估功能。提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。支持白名单设置。  12）文件推送、屏幕水印、告警功能、升级系统 。  13）支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据。  14）可视化功能 能展示各个服务器或主机节点的信息，运行状态、活动规律、行为变化趋势和详细资料，以及历史行为数据查询、全局安全态势等。 |
| 服务要求 | 1）安全事件：提供重大事件应急响应预案。  2）应急响应：对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知用户，并提供专应急预案、处置工具或专杀工具。  3）技术支持：支持7x24小时威胁溯源服务。 |

**（七）云平台监管及审计**

（1）云管平台

云供应商须为招标方提供专用的云管平台，云管平台按照政务云云管平台统一标准规范建设，须与政务云其他云管平台整合统一使用。支持通过机关内部最多跑一次网办平台受理、审核用户的需求，相关数据录入云管平台，云供应商进行处理；管理政务用户云资源，实时监控云资源运行状况。运管平台须具备如下功能：

| 指标项 | 规格要求 |
| --- | --- |
| 审核管理需求 | 单位管理；用户管理；系统管理；申请审批流程；邮件、手机、短消息。 |
| 管理员需求 | 开通管理、登录管理、日志管理、统计报表、用户管理、云主机管理、系统重装、快照管理、系统镜像管理、安全组管理、工单管理、 计费管理、产品管理、云主机迁移、负载均衡管理、云数据库管理、 事件历史管理。 |
| 使用单位用户需求 | 用户管理、 手机绑定、 日志管理、 云主机管理、安全组管理、 工单管理、 快照管理、监控管理、告警管理、事件历史管理、安全漏洞管理；月度账单确认；云资源利用率报告确认。 |
| 运维人员需求 | 监控管理、告警管理、故障管理、云主机管理、云主机迁移、变更管理、事件历史管理、安全漏洞管理。 |
| 资源管理需求 | 云产品物理资源管理、云产品逻辑资源管理、云产品虚拟资源管理、 资源利用统计、月度账单、云资源利用率、安全漏洞整改情况。 |
| 监控需求 | 日志管理、统计报表、监控管理、事件历史管理。 |
| 查询需求 | 按部门查询；按时间段查询；按资源分类查询；按资源利用率查询。 |

（2）运行监测系统

运行监测系统包括：日志采集监测、日志采集统计、日志查询统计、监测预警等功能，并产生日常运行日志、系统资源占用情况、用户数、操作日志等。具体要求见下表：

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 运行监测系统 | 提供日志管理、统计报表、监控管理、事件历史管理等运行监测功能。 |
| 实现维护事件提醒自动化：通过对云计算平台资源的实时监控,自动在第一时间将异常事件通知相关责任人。 |
| 实现系统健康检测自动化,定期自动地对云计算平台资源和应用系统进行健康巡检。 |
| 实现维护报告生成自动化,定期自动的对系统做日志的收集分析,记录系统运行状况，并通过阶段性的监控、分析和总结,定时提供云计算平台运维的可用性、性能、系统资源利用状况分析报告。 |

**（八）云技术支持服务**

（1）应用迁移咨询服务

投标供应商应制定云平台应用开发及迁移部署规范、关系型数据库使用规范、政务云安全防护体系等规范标准，协助各级部门进行云应用开发，配合做好所有业务应用系统的部署、运行和安全保障。

投标供应商应承诺在项目服务期内，针对上云的业务应用提供架构设计咨询，对采购人指定的云业务系统进行统筹规划，指导业务系统的原软件开发商进行代码修改和系统部署，在系统迁移部署提供非代码级别的迁移支持服务。

投标供应商应配合采购人对现业务系统进行调查摸底，根据实际情况配合制定迁移方案，配合各业务部门做好应用迁移工作，确保平稳过渡、顺利迁移。

具体服务要求如下：

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 政务整体云架构设计规划 | 提供政务整体IT架构云化解决方案，包括现有业务应用的梳理、云架构的设计以及上云的策略等。 |
| 业务应用上云架构设计 | 提供对单个业务应用的上云架构设计，包括架构设计、改造方案和云资源需求评估等。 |
| 软件设计及开发技术咨询 | 提供基于云计算平台的软件设计与开发咨询与技术指导。 |
| 开发测试环境 | 免费提供仿真的开发与测试环境，供应用系统上线前的开发与测试。测试时间一般为7-30天，测试时间内不得收费。 |
| 测试 | 协助用户完成应用系统的功能、性能、安全等测试，测试未通过则禁止应用系统上线运行。 |
| 安全咨询 | 提供基于云计算平台的业务应用和政务整体IT规划的安全方面咨询服务。 |
| 业务应用上云分析诊断 | 提供业务应用上云的方法指导，并提供相关上云指导手册，对上云过程中的技术问题提供支持。 |

（2）其他技术服务

投标供应商应提供灾难时数据恢复服务和容灾系统规划服务；提供虚拟机(含操作系统)、存储(含数据库)和网络服务的监控、配置、管理和优化服务；提供故障警告、日志采集、计量统计的功能；提供专家级系统安全和网络安全优化；建设一套规范的资源使用与管理制度；需在项目建设实施期间以及日后维护过程中全部提供原厂服务。

投标供应商保证在云平台出现故障和缺陷时,或接到采购人提出的技术服务要求后 1 小时内作出响应。

投标供应商应负责云平台整体运维服务,包括IDC 基础运维、云平台运维等,并提供具体的服务方案。

（3）培训服务

投标供应商应根据本项目的特点制定培训方案，应提供培训，使招标方相关人员在培训后能够独立的使用系统，而不必依赖投标供应商现场指导。培训课程应安排在整个项目计划的合适时间段内，培训的内容至少应涵盖政务云平台日常使用所需功能。培训应分为使用及管理培训（针对技术管理人员）和业务开发培训（针对业务开发人员），中标人负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表。

**（九）商务条款**

**1、付款方式：**

▲合同签订后，服务提供方按实际需求提供服务（招标前未支付的服务费用均按照此次招标结果计费支付），同时，需提供各使用单位实际使用的服务项目（产品类型）、数量的服务费用清单，并经过使用单位确认后由采购人结算服务费用。合同期内一次性支付费用清单内的服务费，经双方确认并签订支付协议，成交供应商出具发票后7个工作日内支付服务费。

2、服务期限：所有政务云服务计费方式均按照此次结果执行，直至出现新的政务云招标结果为止。

**3、本项目为单价合同，具体服务金额按照实际使用情况对照此次单价和统一折扣率计算并支付。**

**4、报价说明**

1）鉴于各使用单位应用系统数量为动态数值，故本项目不能确定各项服务总量，本次招标采购的是云主机等资源每月租赁费的单价（不足1月按实际产生天数计费，每日租赁费=月租赁费/30）。

2）本次投标品目采购人已设单价最高限价，投标供应商在采购人设定的最高限价的基础上根据企业自身实力及市场行情自行填报折扣率，▲**不同投标品目要求填报统一的折扣率（即所有投标品目的折扣率均相同），否则其报价无效并作无效标处理**。

**3）本项目按各单价最高限价×最高限价的统一折扣率×各部门各实际服务数量进行结算。各单价最高限价详见下表：**

**洞头区政务云（公有云）服务内容清单和最高限价**

单位：(元/月)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务类型 | **计费项** | **规格说明** | | **说明** | **最高限价** | **备注** |
| **一、基础设施服务（IaaS)** | | | | | |  |  |
| 1 | 计算服务 | 增强型云主机 | 一核 | 1GB | CPU主频≥2.3GHz；以上云主机价格包含操作系统正版授权；40G系统盘（SATA），linux系统盘40G，Windows系统盘40G；不含数据盘的价格 | 35 | CPU主频≥2.3GHz；以上云主机价格包含操作系统正版授权；linux系统盘不低于20G，Windows系统盘不低于40G；不含数据盘的价格 |
| 2GB | 64 |
| 4GB | 160 |
| 8GB | 294 |
| 两核 | 2GB | 178 |
| 4GB | 238 |
| 8GB | 352 |
| 16GB | 525 |
| 四核 | 4GB | 350 |
| 8GB | 470 |
| 16GB | 700 |
| 32GB | 1040 |
| 八核 | 8GB | 660 |
| 16GB | 880 |
| 32GB | 1315 |
| 64GB | 1960 |
| 十六核 | 16GB | 1300 |
| 32GB | 1745 |
| 64GB | 2620 |
| 128GB | 3840 |
| 三十二核 | 64GB | 3490 |
| 128GB | 5200 |
| 2 | 存储服务 | 云主机数据盘 | SSD数据盘 | 100GB | 需挂载在云主机上使用，需以100G为单位订购 | 70 | 挂载在云主机上，可单独也可组合使用 |
| 高效数据盘 | 100GB | 需挂载在云主机上使用，需以100G为单位订购 | 41 |
| 云存储 | 每TeraByte (TB)字节 | 1T | 对象存储OSS，需以1T为单位订购 | 181 |  |
| 3 | 网络服务 | 共享互联网出口带宽 | 共享带宽 | 500 Mbps | 云平台共享互联网出口；提供配套的IP地址 | 6856 |  |
| 1000 Mbps | 13711 |  |
| 每增加100Mbps | 1644 |  |
| 独享互联网出口带宽 | 独享带宽 | 10M |  | 363 |  |
| 20M | 727 |  |
| 50M | 1091 |  |
| 100M | 2182 |  |
| 200M | 3819 |  |
| 云负载均衡 | 以1个实例为单位 | 实例 | 提供4层和7层负载均衡。支持包括全局负载均衡和服务器负载均衡的功能；支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、UDP强行负载等算法。 | 639 | 支持包括全局负载均衡和服务器负载均衡的功能；支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、UDP强行负载等算法。 |
| **二、平台服务（PaaS）** | | | | | |  |  |
| 1 | 数据库服务 | 云数据库 | My SQL数据库服务（最大连接数） | 60 | 约占用内存240MB | 27 |  |
| 150 | 约占用内存600MB | 67 |  |
| 300 | 约占用内存1200MB | 127 |  |
| 600 | 约占用内存2400MB | 247 |  |
| 1500 | 约占用内存6000MB | 620 |  |
| 2000 | 约占用内存12000MB | 1102 |  |
| 2000 | 约占用内存24000MB | 2029 |  |
| 2000 | 约占用内存48000MB | 3940 |  |
| MS SQL Server数据库服务（最大连接数） | 100 | 约占用内存1000MB | 91 |  |
| 200 | 约占用内存2000MB | 183 |  |
| 400 | 约占用内存4000MB | 365 |  |
| 600 | 约占用内存6000MB | 550 |  |
| 800 | 约占用内存8000MB | 732 |  |
| 1200 | 约占用内存12000MB | 1097 |  |
| 2000 | 约占用内存24000MB | 1736 |  |
| 2000 | 约占用内存48000MB | 3292 |  |
| 高性能数据库 | 2C8G |  | 352 |  |
| 4C16G |  | 700 |  |
| 4C32G |  | 1040 |  |
| 8C32G |  | 1315 |  |
| 8C64G |  | 1960 |  |
| 8C128G |  | 3970 |  |
| 16C64G |  | 2620 |  |
| 16C128G |  | 4357 |  |
| 16C256G |  | 7957 |  |
| 32C128G |  | 5230 |  |
| 32C256G |  | 8830 |  |
| 32C512G |  | 16030 |  |
| 数据库存储（以100GB为单价） | 100GB | SSD存储，以100GB为单价 | 70 |  |
| 100GB | SAS存储 | 41 |  |
| 2 | 大数据服务 | 大数据服务 | 大数据存储 | 大数据存储 | 不高于10G，以占用存储空间1GB位单价，1GB | 101 | 大数据存储空间 |
| 不高于100G时，以占用存储空间1GB位单价，1GB | 43 |  |
| 不高于1T，100G-1000G部分以占用存储空间1GB位单价，1GB | 17 |  |
| 高于1T，以占用存储空间1GB位单价，1GB | 1 |  |
| 计算单元（CU） | 1CU=1核4G（50个CU为一组，按组提供服务） | 148 | 50个CU为一组，按组提供服务 |
| 大数据ETL | 以导入数据1GB为步长增加1GB | 9 |  |
| **三、云安全服务** | | | | | |  | |
| 1 | 自主云安全服务 | 自主云安全服务 | WAF | 25M | 1个一级域名和10个二级域名（流量上限为25M） | 702 | 防护流量25Mbps，HTTP最大新建连接数3000，HTTP最大并发连接数30000 |
| 50M | 2个一级域名和20个二级域名（流量上限为50M） | 1163 | 防护流量50Mbps，HTTP最大并发连接数50000，HTTP最大新建数5000 |
| 100M | 4个一级域名和40个二级域名（流量上限为100M） | 1888 | 防护流量100Mbps、HTTP最大并发数180000、HTTP最大新建数10000 |
| 200M | 8个一级域名和80个二级域名（流量上限为200M） | 3097 | 防护流量200Mbps、HTTP最大并发数300000、HTTP最大新建数30000 |
| 500M |  | 4687 | 防护流量500Mbps、HTTP最大并发数500000、HTTP最大新建数40000 |
| 防火墙 | 25M吞吐量 |  | 703 | 应用层性能支持：200M、500M和1000M；支持静态路由，ECMP等价路由，支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议，支持多播路由协议，支持路由异常告警功能；提供基本的安全防御；含预警及报表服务。 |
| 50M吞吐量 |  | 757 |
| 100M吞吐量 |  | 909 |
| 200M吞吐量 |  | 2410 |
| 500M吞吐量 |  | 4638 |
| 1000M吞吐量 |  | 8639 |

**标项二：洞头区政务云（私有云）**

**（一）采购内容**

根据温州市政府《关于推进政府大数据平台建设的实施意见》相关要求，温州市洞头区大数据管理中心组织进行洞头区政务云采购。其中，洞头区政务云（私有云）主要为全区各政务部门提供高性能云主机、云计算、云应用、云安全、异地备份等基础设施资源共享服务，为各政务部门私有业务系统上云提供基础平台支撑。

本项目采用企业建设和运维、政府按需购买服务方式进行，通过明确各项服务内容的采购单价和计价规则，对经准确登记云资源进行计费并支付费用。

采购的服务内容主要包括：

1、云基础服务：包括云主机（含安全管理模块EDR）、高性能云主机(含安全管理模块EDR）、云主机数据盘、共享互联网出口带宽、云存储、云数据库、云负载均衡等。

2、云应用服务：包括云管理服务、云备份、云网盘等。

3、云安全服务：包括统一基础云安全服务、共享云安全服务、自主云安全服务（独立虚拟设备）。

4、大数据服务：大数据计算服务、数据治理服务、数据集成服务等。

5、云基础设施服务：包括IDC托管服务。

6、云管系统：满足租户对订购的云资源清单、性能、运行状态查询导出功能，具备与内跑平台资源开通流程进行对接。

7、异地备份：对现有云资源和数据库重要数据进行异地备份。

**（二）服务交付期**

▲本项目在收到成交通知书后按各条实际需求审核完成后7天内提供本地化的高性能云主机、云主机、云存储、云负载均衡、云数据库、互联网出口、政务外网互联链路等服务。如若未按规定执行，采购人上报采购监管部门后有权取消其中标资格，并重新组织招标或将合同授予第二候选人。

**（三）云服务基本要求**

投标供应商提供的云服务需要满足以下基本条件：

**（1）政务专用要求**

要求提供的云平台为洞头区政务外网用户专用，洞头区各级党政机关、事业单位申请使用政务云服务的应由采购方或采购方指定的部门统一受理、审核。未经采购方或采购方指定的部门审核同意，云服务提供商不得擅自对外提供或开放任何政务云服务。

**（2）机房地点要求**

要求提供云服务的机房地点必须在温州市范围内。

**（3）政务云平台的带宽基本要求**

要求提供的政务云平台与市本级以及12个区县政务外网的专用互联光纤带宽不小于1G，以满足网络互访的要求，并提供高可靠的双物理路由保护措施。

要求提供的政务云平台和互联网独享出口总带宽不少于2G，可扩充到20G。

**（4）服务区域划分要求**

本次采购要求提供包括政务云政务外网资源共享专网、政务外网公共服务专网等不同网络环境，同时提供满足对不同安全级别、不同业务及不同业务专网的需要，并提供应用测试区域等环境。支持虚拟专有域功能（VPC），能够划分隔离的区域为特定的用户提供云服务，区域内的资源与别的用户完全隔离，完全为该用户使用。各局办可通过专线方式接入私有云平台，实现与原有业务专网互通，IP地址自定义划分，与云上其他局办业务隔离。

**（5）安全等级要求**

要求对于核心业务应能实现应用级容灾保护，非关键性业务实现数据级容灾保护。

**（6）服务支撑要求**

为保证政务云稳定可靠运行，供应商须提供且不低于下列服务支撑要求：

1、要求本期至少4人次常驻机房服务，提供7\*24小时运行值班监控服务；同时要求指定一名专职人员负责协调处理各类有关业务，并配备服务终端两台。相关人员必须具备2年以上网络及云平台维护经验，并需提供相关资质证明，相关人员资质及技术能力须由采购方认可。

2、要求组建本地专业政务云维护团队，人员组成必须包含网络、数据库、信息安全、IT管理等领域专业人员组成，并需提供人员相关资质证明，相关人员资质及技术能力须由采购方认可。

3、要求定期举办现场或网络视频培训，免费提供仿真的开发与测试环境，供各级部门应用系统上线前的开发与测试，测试时间内不得收费。

4、要求对应用系统上线、迁移、测试进行规划、设计，协助采购方制定建设方案，协助采购方完成相应应用系统的功能、性能、安全等测试，测试未通过严禁系统上线。免费协助采购方进行新开发应用系统部署，并协助完成相关原有应用系统迁移到政务云平台。

5、要求交付云服务时提供详细的云服务租用清单，并定期（一般按月）提供云服务使用量报表和政务云平台运维日志（包含各类云服务总体的运维工作日志，云安全服务的管理、升级与配置记录，以及采购人认为需要掌握的其他信息）。

6、要求云服务商协助局办单位开展每年不少于1次的云平台应急演练；每月对云上政务系统开展安全漏洞扫描工作，并出具相关报告；积极配合测评公司落实租户业务系统等保测评工作。对上云的政务系统要求定制快照备份策略，做好数据备份。

**（7）安全要求**

要求云服务商保证政务云平台的整体安全，如果云平台出现安全问题，由云服务商承担相应的安全责任。

**（四）政务云平台要求**

**（1）云平台机房环境及相关物理硬件要求**

1、云平台数据中心机房标准要求

要求机房符合国际标准的数据中心机房，能够稳定的365天全天候的提供优质的电力、空调、消防、监控、机架、空气清风系统等服务，保证7\*24小时电力供应，供电保障系统需配置保障油机1500KWA或更高的规格，并实现油机1+1备份、不间断电源系统需配置400KVA（1+1）或更高的UPS规格，机房基础安全设施需配置管网式气体消防、早期烟雾告警、门禁系统等系统。

2、物理服务器要求

物理服务器数量不少于180台，主要用于承载业务系统的ECS云主机服务（不包括RDS、对象存储等云产品）。服务器不低于如下配置：2路INTEL XeonE5-2650V2 CPU（核数8核，主频2.6GHz），内存≥128G，双电源。要求可根据用户使用情况进行扩展，不会导致业务中断。云平台单集群支持不少于5000台物理服务器。

3、物理存储设备要求

物理存储初期容量不少于1 PB，要求可根据用户使用情况进行扩展，扩展过程中不会导致业务中断。云存储采用分布式文件系统。

4、物理网络要求

为保证网络高可靠性、高可用性、高扩展性、冗余性，要求采用双核心和接入两层扁平化的组网架构，分别构建独立的业务网、管理网、存储网，核心接入之间万兆捆绑互联；所有服务器分别双归属接入业务网、管理网、存储网。

要求保证产品成熟可靠。为了适应云计算中心出现的40GE和100GE以太网标准，并且充分满足数据中心级的应用及发展需求，核心层设备应采用具有新一代交换架构的产品。

要求满足今后5年内洞头各地各部门（单位）对政务云平台中业务应用网络带宽、业务平稳、持续不间断运行等应用需要。

**（2）云平台软件要求**

供应商的云平台软件需要基于成熟、大规模商用、安全的云平台，有成功应用案例。

基本要求：

1、云平台自主知识产权

云平台软件，必须提供原厂知识产权证明，并能够不依赖于第三方，具备对全部软件代码的自主研发、升级、及时的bug修复能力。

2、大数据服务能力

云平台需具备分布式大数据服务能力，提供成熟大规模数据处理平台案例。提供统一的数据开发平台，云平台集成统一的大数据运维管理。

3、云平台安全合规

云平台需通过工信部可信云认证。

4、与现有云平台的兼容性

新的云平台要求与现有市政务云（私有云）平台全面兼容，如与现平台采用不同的技术路线，则要求能在业务不中断的情况下实现所有云资源的整体迁移。

**（3）云平台架构要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 标准规范 | 采用统一管理集群资源，统一管理集群内的CPU、内存、磁盘和网络资源使得这些关键资源可以被高效地使用。 |  |
| 具备分布式系统底层服务、分布式文件系统、任务调度、集群监控和部署能力并提供技术白皮佐证。 |  |
| 根据应用对资源进行全局的调度，提高资源的利用率。 |  |
| 采用自动故障切换提高系统整体的可用性。 |  |
| 采用统一的安全措施，保证用户数据的安全性。 |  |
| 采用统一运维的方式，提高系统的安全并降低成本。 |  |
| 扩展规模 | 支持在线集群扩容和应用服务的在线升级。 |  |
| 单个集群最大规模可达到5000台物理服务器并行作业。 |  |
| 资源管理 | 提供计算存储设备，网络设备和安全设备等物理设备的管理功能。 |  |
| 提供虚拟化后的“分布式计算资源池”、“网络资源池”和“存储资源池”的管理功能。 |  |
| 提供对网络资源的管理功能，包括：IP地址资源和带宽资源的管理。 |  |
| 提供资源协同能力，包括资源的注册、创建、销毁、回收、状态同步、分布式锁服务，支持分布式共识协议。 |  |
| 提供集群并行作业能力，实现资源的高可用和集群的负载均衡能力。 |  |
| 远程过程调用 | 提供可靠高效的进程间远程调用服务，支持通讯信道的数据压缩和一致性校验。 |  |
| 虚拟化功能 | 支持并配置计算资源虚拟化，形成“分布式计算资源池”。硬件采用标准X86服务器，不使用IP SAN和FC SAN等专用存储作为存储资源。 |  |
| 支持并配置计算设备“一虚多”，同一台物理主机上同时支持多种操作系统，或是相同操作系统的不同版本。分区与分区之间相互独立，互不影响。 |  |
| 支持并配置资源的动态调配与弹性可伸缩，资源池具备各级资源的按需获取功能，提高资源消费者的可用性、容错与扩展能力。 |  |
| 分布式文件系统 | 云平台操作系统支持分布式文件系统，支持存储资源虚拟化,形成“存储资源池”。 |  |
| 数据存储在不同机架的多个节点上，集群中的节点出现硬件、软件故障,集群系统能够自动进行数据的备份和迁移,保证数据的高可用性在并提供技术白皮书佐证。 |  |
| 支持IO优先级控制和QoS保证； |  |
| 支持增量扩容和自动数据平衡能力，允许用户定制数据分布策略； |  |
| 具备高可扩展性，可支持上亿个文件和100PB以上量级的文件存储；支持不重启系统，增加物理服务器后自动扩容； |  |
| 在不依赖RAID卡和NAS等特殊硬件设备的条件下，提供高可用性和高可靠性； |  |
| 支持SATA磁盘块存储和SSD高性能块存储两种分布式存储规格。 |  |
| 普通分布式存储吞吐大于等80M/s，高性能分布式存储吞吐大于等于280M/s，随机IOPS大于等于20000。 |  |
| 采用多管理节点设计，为避免集群单点故障，分布式文件系统必须支持多Master设计，至少有3个及以上的存储Master控制节点。 |  |
| 分布式文件系统上创建出的单个存储盘，能够被多个虚机同时挂载，实现共享存储功能。 |  |
| 任务调度 | 提供并行任务调度能力，且具备高可扩展性，最高可支持十万以上级的并行任务调度。 |  |
| 实现自动检测故障和系统热点，重试失败任务，保证作业稳定可靠运行完成。 |  |

**（五）采购服务内容要求**

**1、云基础服务要求**

**（1）云主机要求（含安全管理模块EDR）**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 基本功能 | 云主机CPU核数可选范围1-16核， 64G内存、8TB数据盘。 |  |
| 互联网出口独享带宽可选范围2-100Mb。 |  |
| 虚拟主机支持主流的WINDOWS、LINUX等操作系统，兼容常见的操作系统 |  |
| 支持SATA磁盘块存储和SSD高性能块存储两种分布式存储规格。 |  |
| 扩展功能 | 按需开通。根据用户的需求动态的创建和分配计算、存储、网络带宽等资源；用户可以在线按时长购买云主机，并支持任意时刻的续费管理。 |  |
| 云主机创建。创建后，云主机已包含有操作系统，可立即使用，从创建到启动在5分钟以内。 |  |
| 云主机升级。当云主机现有配置不满足要求时，用户可自主进行云主机配置快速升级，可升级配置包括：CPU，内存，网络带宽等；配置升级生效时间在10分钟以内。 |  |
| 云主机克隆。指创建一台跟现有云主机一模一样的机器，根据云主机数据盘的大小整个克隆过程一般在15分钟以内。 |  |
| 云主机迁移。云平台根据物理主机负载情况综合调度，将云主机在不停机状态下从一台物理主机迁移到另外一台物理主机；在线迁移时，云主机应用完全不中断，用户完全无感知。 |  |
| 管理功能 | 提供用户自服务门户和API接口，用户可自行创建不同规格的虚拟主机，自定义CPU、内存、网络、磁盘等属性。 |  |
| 提供虚拟主机的动态升级、快照备份、性能监测分析、异常告警、日志管理等功能。 |  |
| 提供快照和自定义镜像能力，支持对运行或停止状态的虚拟主机生成快照，应提供分钟级别快照回滚功能。 |  |
| 可靠性 | 数据备份。云主机数据在云计算平台有三份（含）以上数据拷贝，单份数据损坏对云主机使用没任何影响，且一份数据损坏后，后台系统会自动拷贝，使数据始终保证三重备份。 |  |
| 磁盘快照。需要提供云主机任一时刻的磁盘快照功能，含快照制作，快照回滚，快照恢复等。 |  |
| 故障恢复。云主机发生故障后，切换恢复时间在30分钟以内。 |  |
| 虚拟主机服务采用全冗余架构，无单点故障，平均可用性不低于99.9%。 |  |
| 安全性 | 防ARP欺骗，防DDos攻击，提供流量清洗服务 |  |
| 用户可自助开通安全组，并定义安全组规则。 |  |

**（2）高性能云主机要求（含安全管理模块EDR）**

|  |  |  |
| --- | --- | --- |
| 指标项 | 指标要求 | 备注 |
| 设备商资质 | 提供中国信息安全认证中心《信息安全应急处理服务资质（一级）》和《信息系统安全集成服务资质（一级）》认证证书 |  |
| 投标品牌 | 国产自主品牌，非OEM机型，投标机型能够在中国官方网站下载到完整的中文资料，包含产品彩页、规格白皮书、兼容性列表、用户指南、安装升级指南等 |  |
| 可提供与服务器同品牌的交换机、存储等基础设施 |  |
| 产品资质 | 提供中国环境标志产品认证证书，提供证明材料 |  |
| 可管理性 | ★具备带外故障检测功能，不依赖于OS，对CPU故障；I2C和 IPMB总线故障；内存故障；PCIe设备故障；硬盘故障，系统宕机等进行分析和定位，提供白皮书或官网证明材料 |  |
| ★支持最后一屏、中文BIOS界面功能，提供官方截图证明 |  |
| ★支持使用客户端证书和证书密码的双因素认证方式登录单板管理系统，提供白皮书或官网证明材料 |  |
| ★支持黑匣子功能，支持linux系统内核panic时的内核栈信息记录和导出，便于记录的系统故障数据，方便问题定位，提供白皮书或官网证明材料 |  |
| 安全特性 | 为保障数据安全，服务器管理系统配置国产自研管理芯片，提供对应证明材料 |  |
| 体系架构 | 实配SAN与NAS统一存储，配置NAS协议（包括NFS和CIFS）、IP SAN和FC SAN协议，不需额外配置NAS网关，存储操作界面同时支持块存储和文件存储功能（须提供相关截图证明） |  |
| 控制器扩展能力 | 支持控制器扩展，最大支持≥8控； |  |
| 控制器配置 | 配置双Active-Active控制器； |  |
| 控制器处理器 | 采用多核处理器，配置控制器处理器总物理核心数≥96核 |  |
| 存储缓存容量 | 系统内总一级缓存容量配置≥512GB，且任意控制器一级缓存容量≥256GB（不含任何性能加速模块、FlashCache、PAM卡，SSD Cache、SCM等）  控制器缓存均具备断电保护功能， 在出现电源故障时，可提供充足的电源，将高速缓存内容转储至非易失性内部存储设备上（非通用服务器架构） |  |
| 后端磁盘通道 | 配置后端磁盘通道带宽≥192Gbps |  |
| 配置硬盘 | 配置≥8个3.84TB 企业级双端口TLC SAS SSD硬盘（非单端口），配置≥31个2.4TB 10K SAS硬盘 |  |
| Gartner魔力四象限 | 投标存储厂商（不含OEM原厂商）近四年（2017~2020年）入选Gartner通用磁盘阵列存储魔力四象限领导者象限； |  |
| 中国区销售排名 | 投标存储厂商（不含OEM原厂商）连续四年国内企业存储市场收入排名前五（2017至2020年）的专业存储厂商 |  |

**（3）安全管理模块EDR要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 技术参数 | 备注 |
| 产品资质 | ★具由列入《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》且认证检测范围包含网络安全专用产品的机构出具的安全认证合格或安全检测符合要求的有效证明文件。 |  |
| ★具备中国国家版权局颁布的《计算机软件著作权证书》 |  |
| ★通过IPv6论坛IPv6 Ready Logo委员会认证并获得认证证书，提供证书扫描件 |  |
| 软件要求在中华人民共和国境内开发，具备自主知识产权，提供软件著作权登记证书扫描件； |  |
| 基本要求 | 支持通过云安全管理平台自动化部署管理端，防护端通过软件代理的方式部署在主机上； |  |
| 支持的操作系统：Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、win xp 、win 7、win 8、win 10、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、Ubuntu 14 +等； |  |
| 性能监控 | 支持对防护资产的CPU使用率、内存使用率、磁盘使用情况、网络上下行流量进行性能监控，并支持对性能监控项设置阈值，达到阈值后告警；支持对CPU、内存达到一定阈值时客户端进行熔断。 |  |
| 高级威胁防护模块 | 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露 |  |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为 |  |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为 |  |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为 |  |
| 可对渗透的收尾阶段的数据清除行为进行识别和阻断 |  |
| 功能要求 | 支持占用系统资源低，网络版杀毒软件的客户端程序在监控状态占用系统资源CPU不高于3%，内存占用不超过30MB； |  |
| 提供包括Web安装在内的多种安装方式，以适应大型网络的安装部署工作，而且要求采用Web安装过程中，可以不需要客户端进行任何干预； |  |
| 提供基于Web的B/S移动管理架构，管理员可以在网内任意一台计算机上通过web方式随时随地登录控制台实现全网管理，而勿须在实现该功能的客户机上安装特定的管理组件； |  |
| 支持文件实时监控，在进程启动、文件创建、存储介质连接时自动触发； |  |
| 支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并且将修复前的病毒文件进行备份； |  |
| 提供专门的勒索风险评估功能。包括弱口令检测、系统漏洞检测、恶意进程检测、高危端口检测等能力； |  |
| 提供专门的挖矿实时防御工具，并提供功能开关； |  |
| 支持强力查杀，对于无法普通隔离的病毒文件强制停止进程并隔离或动态移除到删除队列； |  |
| 支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用； |  |
| 支持查杀映像劫持类型的病毒； |  |
| 支持对压缩文件、打包文件查、杀毒（默认支持9层压缩扫描，可根据客户需求增加扫描层数）； |  |
| 支持查杀各类Office文档中的宏病毒、夹带型木马； |  |
| 支持在线、离线病毒库升级； |  |
| 支持管理员通过控制台，集中地实现所有节点上防毒软件的监控、配置、查询等管理工作，包括Windows、Linux、虚拟化、移动端等系统上的防病毒软件。 |  |
| 安全防护模块 | 支持防端口扫描，防违规外联，锁定恶意的端口扫描及外联行为，并记录告警 |  |
| 违规外联支持黑、白名单双模式，白名单模式下可选择断开互联网模式，一键添加三类私有地址；黑名单模式可自定义IP，支持黑名单告警和阻断； |  |
| 支持网站防护，包括SQL注入、XSS、Web应用漏洞防护、访问控制、屏蔽扫描器等 |  |
| 支持智能检测防御CC攻击，并可进行高、中、低三档设置。 |  |
| 内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制 |  |
| 支持流量画像，支持全网流量可视化、应用级流量可视化；支持威胁横向扩散路径可视化与一键阻断；支持违规外联路径可视化与一键阻断 |  |
| 支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置。 |  |
| 文件推送 | 支持下发文件、安装应用程序、远程执行命令 |  |
| 告警功能 | 告警类型包括：高级威胁、系统防护、网络防护、Web应用防护。 |  |

**（4）云数据库要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 基本功能 | 基于高效的调度、备份、HA控制、在线迁移以及监控系统，为用户提供为专业的云数据库服务。 |  |
| 支持关系型数据库的基本功能，并进行优化服务。 |  |
| 云平台提供MsSqlserver、Mysql主流关系型数据库服务；云主机上可安装Oracle数据库。 |  |
| 单数据库实例内存可达24G，IOPS可达12000次，并发连接数可达2000。 |  |
| MsSqlserver单数据库实例可创建的数据库数量达20个，用户数达20个。 |  |
| Mysql单数据库实例可创建的数据库数量达200个，用户数达50个。 |  |
| 每份数据都保留两份并可实时切换。 |  |
| 支持数据库在线升级、云内动态迁移、故障自动切换，实现业务秒级无缝切换，不中断用户服务。 |  |
| 自动多重备份数据库，支持从备份文件创建临时实例，支持从备份文件恢复到实例，可下载备份文件， |  |
| 扩展功能 | 按需开通，即开即用，按需计费，为用户提供方便的Web管理界面。 |  |
| 随着用户数和访问量的变化，可以弹性的调整数据库的规格，包含内存、连接数、IOPS、存储容量等，调整时服务不间断。 |  |
| 提供数据导入、导出工具，方便用户进行数据迁移。 |  |
| 提供完整的API接口、SDK开发包、文档说明。 |  |
| 提供日志记录功能，包括错误日志、操作日志、访问日志等，可追查访问来源以及进行多维度的统计分析。 |  |
| 安全性 | 支持IP授权访问。 |  |
| 云服务端提供加密用户身份验证，提供不同的访问权限控制。 |  |
| 提供数据库存储加密服务。 |  |

**（5）云存储（对象存储）要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 基本功能 | 支持海量存储，文件数量无限制，容量按用户需求扩展。 |  |
| 采用分布式存储，一份数据在不同的物理服务器上存三份备份。 |  |
| 采用分布式存储系统，支持大规模强结构化数据存储，如SQL关系性数据库，单库容量可达1TB。 |  |
| 采用分布式存储系统，支持大规模结构、半结构化数据存储，如NOSQL数据库,单表支持的存储空间可达100TB。 |  |
| 扩展功能 | 提供存储对象的读、写、删除、拷贝、查找等基本功能。 |  |
| 支持大存储对象的分片并发上传和下载，支持断点续传。 |  |
| 提供易用的用户Web控制台文件管理界面，与更多第三方工具、插件，满足各种应用需求。 |  |
| 提供完整的API接口、SDK开发包、文档说明。 |  |
| 存储管理 | 支持将数据以对象方式进行存储，用户可以通过调用API以对象为单位操纵存储的数据，实现在任何应用、任何时间、任何地点上传和下载数据，也可以通过用户Web控制台对数据进行简单的管理。 |  |
| 大文件支持 | 支持并配置分段上传大文件，单个分段最大5GB，最大分段数≥5000段。支持断点续传。 |  |
| 安全性 | 具备完善的多用户隔离机制，保障用户数据的私密性。 |  |
| 云服务端提供加密用户身份验证，提供签名权限控制与防盗链功能。 |  |

**（6）共享互联网出口**

服务提供商必须保证政务云互联网出口不出现流量拥塞，在出口流量峰值达到90%时应立即安排出口带宽扩容。

**（7）云负载均衡要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 安全稳定 | 采用分布式结构，具有高度的冗余和可靠性，可根据系统负载弹性扩容。 |  |
| 透明接入 | 提供4层和7层的负载均衡；Web和中间件服务器，无需更改配置即可透明接入 |  |
| 健康检查 | 可以按照指定规则进行健康检查，自动隔离异常状态云主机，并迅速将服务切换，服务切换时间秒级。 |  |
| 会话保持 | 可以将用户和后台服务器绑定到同一会话，确保会话不中断。其中4层负载均衡可以设置连接持久时间。 |  |
| 权重转发 | 可根据后台云服务器的性能设置不同的转发权重，权重支持轮询，最小连接数转发等方式。 |  |
| 易用简单 | 提供API或控制台调用方式，可以随时开启，关闭负载均衡，立即生效，灵活简单。 |  |
| 按需计费 | 支持按流量、使用时间进行计费。 |  |

**2、云应用服务要求**

**（1）云管理服务要求**

采购人将集中受理、审核政务用户的需求，并统一发布给云供应商；并集中管理政务用户云资源，实时监控云资源运行状况。云供应商应为采购人提供专用的综合管理平台，需求见下表：

|  |  |  |
| --- | --- | --- |
| 功能项 | 规格要求 | 备注 |
| 审核管理需求 | 单位管理  用户管理  系统管理  申请审批流程  邮件、手机、短消息 |  |
| 管理员需求 | 开通管理：  登录管理：  日志管理：  统计报表：  用户管理：  云主机管理：  系统重装：  快照管理：  系统镜像管理：  安全组管理：  工单管理：  计费管理：  产品管理：  云主机迁移：  负载均衡管理：  云数据库管理：  事件历史管理： |  |
| 普通用户需求 | 用户管理：  手机绑定：  日志管理：  云主机管理：  安全组管理：  工单管理：  快照管理：  监控管理：  告警管理：  事件历史管理： |  |
| 运维人员需求 | 监控管理：  告警管理：  故障管理：  云主机管理：  云主机迁移：  变更管理：  事件历史管理： |  |
| 资源管理需求 | 云产品物理资源管理：  云产品逻辑资源管理：  云产品虚拟资源管理：  资源利用统计 |  |
| 监控需求 | 日志管理：  统计报表：  监控管理：  事件历史管理： |  |

**（2）数据交换服务要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 架构部署 | ★采用分布式云架构设计，支持云上进行部署，支持单机部署模式和集群部署模式； |  |
| 资源目录管理 | 支持对资源目录的审核、编目、发布，支持目录分类，支持资源检索，使用用户可以快速定位资源； |  |
| 支持流程化的资源申请，提供流程审批功能； |  |
| 提供信息资源目录驱动数据资源交换的功能； |  |
| 提供数据资源标准管理及展示功能； |  |
| 适配多种数据资源 | 适配各种主流数据库（Oracle、MySQL、DB2等）； |  |
| 适配大数据平台,包括Spark、ODPS、ADS等； |  |
| 适配主流的公文类型、二进制等格式文件； |  |
| 适配Restful、WebService方式的API； |  |
| 支持各种异构数据资源间的交换； |  |
| 数据变化捕获 | 支持通过日志解析的模式获取增量数据； |  |
| 支持通过触发器的模式获取增量数据； |  |
| 支持通过时间戳的模式获取增量数据； |  |
| 基础交换功能 | 支持直接交换、安全交换（在大数据平台下，实现数据交换可用不可见）、共享交换（在大数据平台下，实现数据交换不搬家）、API服务等多种数据交换方式； |  |
| 支持实时、准实时、周期性定时批量、全量等多种交换频率； |  |
| 支持多表的关联后的数据交换； |  |
| 支持数据路由功能，可将数据按条件分发给多个数据需方； |  |
| 支持数据过滤功能，可设置数据过滤条件，可使用该功能实现数据脱敏交换； |  |
| 易用性 | 安装部署应简单，对于数据交换节点的部署，需做到可配置化、一键式部署； |  |
| 支持数据交换任务的全配置化管理，配置应简单化、人性化； |  |
| 支持Web页面的数据交换管理。方便运维人员通过图、表的形式直观的了解数据交换的情况，并进行数据交换任务的管理； |  |
| 高性能 | 平台应具备分布式横向平滑扩展能力，线性的提升数据交换性能； |  |
| 平台应具有对数据压缩传输能力，提供数据的传输性能； |  |
| 平台应具有分布式负载均衡功能，多进程、多线程同步处理提供性能； |  |
| 高可靠 | 支持高可用部署，提供单节点容错机制，在出现单节点故障时，数据交换工作仍可正常运行； |  |
| 支持自动断点继传，在网络故障和服务器故障修复后，可自动重启中断的交换任务，从故障点自动继传数据； |  |
| 开放性 | 产品功能模块化,可插拔;用户流程可配置； |  |
| 提供全套 API 支持二次开发； |  |
| 授权合规 | 采用的数据共享交换软件产品应具备国家颁发的相关软件著作权证书。 |  |

**（3）云备份服务要求（数据库备份与恢复）**

1）备份软件具备计算机信息系统安全专用产品销售许可证。

2）要求采用B/S的管理和使用架构，备份管理、恢复管理、远程复制管理、用户及权限管理等均在一个管理界面内，中文界面，基于WEB管理模式，易于管理与维护。

3）支持多任务的时间计划，具有独立的存储空间（与云平台存储相隔离）。

4）支持对SQL Server、Oracle、Sybase、Exchange Server、Lotus Domino、DB2、MySQL、AD等主流应用进行在线备份保护。

5）具备管理员和审计管理员双管理员角色，同时和业务系统嵌入后，保持和备份系统的权限独立。审计管理员则可以进行备份内容审计、备份系统安全性审计和备份行为审计，以保证备份的安全性。

6）支持Oracle数据库任意时间点恢复功能，在Oracle（支持单机、双机和RAC架构）数据库恢复时，可以将数据库恢复至备份数据保留周期内任意一秒钟，所有操作包括时间的指定均图形化实现，无需任何的人工脚本干预，在无需专业人员操作的情况下，大幅提高数据恢复的时间精度，降低数据丢失量。

7）支持异地备份数据的安全管理机制，异地备份存储系统需要得到本地授权许可后，才可以浏览、恢复本地传输过去的备份数据，最大限度避免备份数据的泄密可能。

**（4）云网盘服务要求**

1）云网盘产品要求为国内知名品牌，非OEM产品，系统管理可以通过登录Web，统一管理集群系统、云共享服务（包括创建用户组织、自定义文档库、权限管理、访问控制、安全访问管理控制等、访问日志）。

2）可以通过登陆Web了解整个集群的运转绩效，要求包括在线人数监控、文件分类数量统计、文件操作变化统计，可以提供实时、每日、每月及年度的报表。

3）支持PC客户端、移动客户端（Android、IOS）、Web访问，可以基于文档所有者对指定文档配置指定范围可发现，对于访问者，可以通过全文检索找到可以发现的共享文档进行下载使用。

4）支持基于云存储的全文检索，当用户想找某个文档资料，希望找到某个关键词相近的文档，输入关键词，获取全文检索的结果。

5）采用灵活的组织架构，既可以构建符合企业分层管理的用户结构，也可以构建灵活的多用户组织单元。

**3、云安全服务要求**

**（1）统一基础云安全服务要求**

1）漏洞扫描

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 漏洞扫描 | 提供网站漏洞扫描系统，可扫描的漏洞类型包括OWASP、WASC、CNVD等。支持恶意篡改检测，支持Web2.0、AJAX、各种脚本语言、PHP、ASP、.NET 和 Java 等环境，支持复杂字符编码、chunk,gzip,deflate等压缩方式、多种认证方式（Basic、NTLM、Cookie、SSL 等），支持代理、HTTPS 、DNS绑定扫描等。  仪表盘功能，直观展示最近10天整体风险等级、最近10天扫描站点列表、最近30天危险站点TOP10等内容  能够扫描主流虚拟机管理系统的安全漏洞，如：VMWare ESX/ESXi，要求能够扫描大于300条相关漏洞，并提供详细的漏洞列表  漏洞知识库漏洞信息大于15000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准  系统内置Exploit DB漏洞、Metasploit漏洞、Exploit Pack漏洞检测模板 |  |
| 服务要求 | 每月进行一次全面漏洞扫描，并向政务云平台租户提供漏洞分析报告和修复建议。网络安保重点时期可根据采购方要求，适当增加扫描频次和范围。 |  |

2）入侵防御

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 入侵防御 | 防护对象 支持以下两种防护对象：自定义防护对象 默认防护对象  引流支持以下两种方式：策略路由引流 BGP引流  防御模式 防御模式支持以下几种方式：自动 手动 不防御  白名单支持以下几种方式：全局白名单 防护对象白名单  黑名单 黑名单支持以下几种方式：全局黑名单 接口板黑名单 防护对象黑名单 |  |
| 回注支持以下几种方式：二层回注 静态路由回注 策略路由回注 GRE回注 MPLS LSP回注 MPLS VPN回注 |  |
| 基于接口的防御策略 支持的基于接口的防御类型包括以下几种攻击：SYN Flood SYN-ACK Flood ACK Flood RST Flood TCP-abnormal Flood TCP Fragment Flood UDP Flood UDP Fragment Flood ICMP Flood DNS Request Flood DNS Reply Flood HTTP Flood SIP Flood |  |
| 服务要求 | 部署在政务云平台边界，对全流量进行清洗分析，含运维管理服务，安排专人定期巡检和分析日志，及时向政务云平台采购方和租户通报入侵防御重要安全风险事件，并协助租户按需完成策略调整与优化。 |  |

3）防DDOS攻击

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 防DDOS | 在网络边界部署。 |  |
| 支持支持10G的清理能力，可以准确识别正常流量，清洗各类异常流量，包括流量型攻击、应用层攻击、扫描窥探型攻击及畸形包攻击。 |  |
| 单台设备同时支持检测与清洗功能。 |  |
| 服务要求 | 部署在政务云平台边界，对全流量进行清洗分析，含运维管理服务，安排专人定期巡检和分析日志，及时向政务云平台采购方和租户通报重要安全风险事件。 |  |

**（2）共享云安全服务要求**

1）云杀毒

1. 在云主机上部署主机保护系统，实现恶意代码检测、web信誉评估、入侵检测和防火墙功能。
2. 在虚拟化环境中在尚无原厂补丁的情况下，要通过虚拟补丁功能及时防御通过漏洞入侵系统等措施实现安全加固；
3. 提供自动扫描功能，针对服务器弱点、漏洞进行安全检测并自动形成防护，产品必须能够防御应用层攻击、SQL Injection 及Cross-site跨网站程序代码改写的攻击。
4. 所有产品必须是自主开发，拥有自主知识产权，必须具有产品销售许可证和著作权证明。

2）SSL VPN

三层吞吐量6G，应用吞吐量2G，最大并发会话数200W，2U设备，最大14个GE电口，最高8个SFP接口，1个SLOT插槽,1管理接口，1个RJ45，2个USB口，同时含IPSEC和SLL VPN功能。

服务要求：含并发用户许可授权，含运维管理服务，包括用户管理和技术支撑服务等。

3）运维审计服务

|  |  |  |
| --- | --- | --- |
| 项目 | 技术要求 | 备注 |
| 主体功能要求 | 支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录 IP 范围等 |  |
| 须内嵌认证引擎，除用户名/密码认证方式外，能够提供动态令牌、USBkey 等认证方式 |  |
| 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能，自动修改windows服务器密码无需在目标服务器上安装agent、开启telnet服务等 |  |
| 支持完善的自动改密策略，包括改密前发送密码、改密后发送密码、密码文件加密、密码传输加密、密码强度控制、自动密码恢复等。发送方式包括邮件、FTP、SFTP等 |  |
| 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志，支持以首页中的设备为基准，支持直接查询该主账号有权限运维的所有设备。 |  |
| 支持SSH、Telnet、远程桌面，VNC、FTP/SFTP、数据库、Http/HTTPS等协议和应用的运维，要能支持B/S和C/S两种运维方式，支持SSH密钥批量登录、批量命令执行等。 |  |
| 支持对运维过程审计录像，并支持远程桌面磁盘映射、复制粘贴、Linux的xmodel等文件传输的原文件记录。 |  |
| 支持批量导入/导出/修改用户帐号信息和目标设备信息 |  |
| 支持自动填写特权密码，从普通管理模式进入到特权模式 |  |
| 用户登录后可在首页分组显示该用户有权限管理的目标设备，设备分组可按最近访问、最常访问、访问策略、按照个性化配置中的分类等分组显示可登录的设备；并可按全部/工单相关来查询设备 |  |
| 访问策略支持设备视图和用户视图，管理员可以对运维权限一目了然，视图可以按照xls格式导出，方便管理员管理 |  |
| 服务要求 | 含管理对象授权许可，含运维管理服务，含用户VPN接入服务；安排专人定期进行运行监控，支持电话、网上值班等响应方式。 |  |

4）日志审计

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全综合审计服务。 |  |
| 使用方式 | Windows云主机通过部署轻量Agent程序进行数据采集、Linux云主机配置syslog进行数据采集，从而实现综合日志审计效果 |  |
| 主要功能要求 | 支持Syslog、SNMP Trap、FTP、代理(Agent)等方式收集日志 |  |
| 支持目前主流的安全设备、操作系统、应用系统等日志收集 |  |
| 支持对收集到的日志进行解析，解析规则可以根据客户要求定制扩展 |  |
| 支持按认证操作、授权操作、账号操作、访问控制、配置变更、攻击威胁等纬度进行报表统计 |  |
| 服务要求 | 含运维管理服务，安排专人定期进行日志分析，并定期向租户提供专项分析报表。 |  |

5）Web应用防火墙

标准2U设备，双冗余电源，1个HA口，1个RJ-45 Console口，1个10/100/1000 Base-T带外管理口，4个网络接口板扩展槽位，可选配WAF-NIM-L通用接口板，默认含3个接口（含1个HA接口）永久使用授权），2个USB口；2个万兆SFP+ 接口，万兆多模光模块；网络层吞吐量≥8G ；应用层吞吐量≥4G；最大HTTP并发连接数≥200万；每秒新建HTTP连接数不少于2.5万；

|  |  |  |
| --- | --- | --- |
| 项目 | 技术要求 | 备注 |
| 基础防护 | Web服务器/插件防护 |  |
| HTTP访问控制 |  |
| 爬虫防护 |  |
| Web通用防护 |  |
| 文件非法上传防护 |  |
| 非法下载限制 |  |
| 信息泄露防护 |  |
| Webshell防护 |  |
| 高级防护 | 盗链防护 |  |
| 跨站请求伪造防护 |  |
| 扫描防护 |  |
| Cookie安全 |  |
| 内容过滤 |  |
| 敏感信息过滤 |  |
| 暴力破解防护 |  |
| XML防护 |  |
| 智能引擎检测 |  |
| 服务要求 | 部署在政务云平台边界，可根据需要对流量进行清洗分析，含运维管理服务，安排专人定期巡检和分析日志，及时向政务云平台采购方和租户通报重要安全风险事件，并协助租户按需完成策略调整与优化。 |  |

**（3）自主云安全服务要求**

以下安全服务要求提供独立虚拟安全设备，能够根据用户要求，提供自服务管理界面。

1）自主云安全产品整体服务要求

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全防护服务 |  |
| 交付方式 | ★资源池必须具备安全需求弹性扩展，安全灵活部署。按需交付。安全功能以基于不同安全需求以安全服务包的形式交付。（需提供产品功能截图） |  |
| 角色授权及使用方式 | 支持三权分立安全原则，可实现虚拟防火墙、虚拟IPS、虚拟化web应用防火墙、网页防篡改、云堡垒机、云数据库审计、云日志审计、云主机防御（东西向流量隔离、防病毒）等所有安全产品的角色统一授权，授权粒度精细到每一个安全产品的每一个角色，同时可以给用户批量授权，如一次性给用户A授权堡垒机的运维管理员角色，给用户B授权堡垒机的审计管理员角色（须提供相关截图证明） |  |
| 支持用户认证统一，被授权的用户可以通过登录到云安全管理平台单点登录到各个安全产品，包括虚拟防火墙、虚拟IPS、虚拟化web应用防火墙、网页防篡改、云堡垒机、云数据库审计、云日志审计、云主机防御（东西向流量隔离、防病毒）等所有安全产品。（须提供相关截图证明） |  |
| 资产管理 | 支持通过管理平台统一添加资产自动同步到相关安全产品，添加主机资产自动同步到堡垒机、主机扫描，添加网站资产自动同步到网站扫务等，无需到不同的安全产品模块逐一添加 。 |  |
| 运维态势 | 支持管理员通过可视化大屏获取整个安全资源池的物理节点总数量和物理节点在线／离线数量，虚拟机总数量和虚拟机在线／离线数量信息，且包含安全资源池总CPU、内存、磁盘使用率，CPU、内存、磁盘占用趋势，网络总流入流出速率趋势等信息。 |  |
| 许可管理 | 支持许可自动化导入激活安全产品，云安全管理平台会根据开通安全产品的规格、数量、时间周期等信息自动导入许可到安全产品，实现安全产品自动化激活，包括虚拟防火墙、虚拟IPS、虚拟化web应用防火墙、网页防篡改、云堡垒机、云数据库审计、云日志审计、云主机防御（东西向流量隔离、防病毒）等所有安全产品许可的自动化导入激活。 |  |
| 产品资质 | ★要求安全管理平台具备CSA云安全star-cstr证书（提供证书扫描件） |  |
| 技术支撑 | ★提供原厂商常驻浙江省内不少于5个CISP-CSE云安全工程师（须提供在本单位2024年1月1日至今任意一月缴费情况（个人参保证明以已到账为准、单位参保证明以养老保险参保为准）的社会险参保证明），以便提供快速的售后服务 |  |
| ★提供原厂商常驻浙江省内不少于5个CISP-BDSA（大数据安全分析师）工程师（须提供在本单位2024年1月1日至今任意一月缴费情况（个人参保证明以已到账为准、单位参保证明以养老保险参保为准）的社会险参保证明），以便提供快速的售后服务 |  |

2）云Web应用防火墙服务要求

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全防护服务。 |  |
| 使用方式 | 云租户通过登录云安全管理平台，单点登录到WEB应用防火墙服务模块，对网站进行安全防护配置管理 |  |
| 主要功能要求 | 支持对SQL注入、XSS、命令注入、webshell等OWAP10的攻击防护 |  |
| 支持对服务器返回的内容包括身份证信息、银行卡号、手机号等敏感信息进行隐藏 |  |
| 支持网站自学习建模功能，能通过自学习形成网站URL树、生成安全防护策略、发现参数的名称、类型、匹配频率；可配置匹配到自学习特征后放行，匹配不到自学习特征直接阻断请求； |  |
| 支持对访问流程的校验  可配置页面合规页面流程  可配置页面思考时间  违反合规的访问直接被拦截并产生告警日志（需提供第三方测评机构（公安部三所、国家保密局、ISCCC其中一家）的检测报告） |  |
| ★按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP的访问  （需提供第三方测评机构（公安部三所、国家保密局、ISCCC其中一家）的检测报告） |  |
| 支持CC攻击防护：  支持多种算法检测方法，对指定URL访问速率、对指定URL访问集中度检测  检测对象支持IP或IP+URL算法；  支持挑战模式，客户端访问时WAF发起302重定向与js挑战验证是真实客户还是CC工具发起的访问  支持学习业务流量模型，在业务流量异常时开启CC防护，并支持启动配置阈值（需提供第三方测评机构（公安部三所、国家保密局、ISCCC其中一家）的检测报告） |  |
| 规格 | 保护站点授权2个，防护流量20Mbps |  |
| 保护站点授权4个，防护流量50Mbps |  |
| 保护站点授权8个，防护流量100Mbps |  |
| 保护站定授权16个，防护流量200Mbps |  |
| 保护站定授权32个，防护流量1Gbps |  |

3）SSL VPN服务要求

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全防护服务 |  |
| 使用方式 | 云租户通过登录云安全管理平台，单点登录到SSL VPN服务模块，对SSL VPN配置管理 |  |
| 主要功能要求 | 支持site to site 和远程接入VPN方式,支持主模式，野蛮模式，野蛮模式支持FQDN、USER-FQDN和通配符设置 |  |
| 支持VPN零配置上线、VPN批量下发 |  |
| 支持专有SSL VPN客户端，客户端支持Windows 32位/64系统，支持开源的SSL VPN客户端系统包括IOS 安卓 linux（须提供相关截图证明） |  |
| 规格 | 20个并发用户 |  |
| 50个并发用户 |  |
| 100个并发用户 |  |

4）运维审计（云堡垒机）服务要求

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全运维审计服务。 |  |
| 使用方式 | 云租户通过登录云安全管理平台，单点登录到运维审计服务模块，对云主机、业务系统进行统一运维管理 |  |
| 主要功能要求 | ★支持oracle、mysql、sqlserver数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机。（须提供相关截图证明） |  |
| 支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权（须提供相关截图证明） |  |
| ★导出的设备信息文件加密存储，解密时须由2个管理员同时解密才能查看到设备信息文件内容（须提供相关截图证明） |  |
| 在不依赖于应用发布的条件下，支持通过堡垒机页面直接调用本地windows的plsql、sqlplus、sqlwb、ssms、mysql.exe等数据库客户端工具（须提供相关截图证明） |  |
| ★支持保存RDP传输的原始文件（提供第三方权威机构检测报告证明及功能截图） |  |
| 支持可管理SSH、RDP、SFTP、FTP、TELNET、web类的服务器，以及可管理其他远程工具或自定义的应用客户端 |  |
| 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细审计日志 |  |
| 支持文件传输协议控制、命令控制、访问控制的三种安全策略 |  |
| 支持自动化运维功能，可将结果通过邮件通知管理员；可对linux/windows云主机进行自动改密 |  |
| 规格 | 10个管理对象 |  |
| 20个管理对象 |  |
| 50个管理对象 |  |

5）网页防篡改服务要求

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全防护服务 |  |
| 使用方式 | 云租户通过登录云安全管理平台，单点登录网页防篡改服务模块，进行中心端的统一运维管理。同时网站所在虚拟机上需安装轻量Agent程序，实现网页防篡改效果 |  |
| 主要功能要求 | 支持windows、linux等主流操作系统的文件和目录的保护：支持各类网页文件的保护，支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码 |  |
| 支持一键启停文件保护：一键启停所有监控端对文件保护，不必登录WEB服务器进行停启 |  |
| 篡改规则：支持基于目录、进程、文件、文件类型等进行设置篡改规则，支持正则表达式策略 |  |
| 支持模板配置：支持在同一种操作系统下，网站路径相同，可通过规则模板，用模板统一将规则下发到各监控端，无需对监控端进行一一配置 |  |
| Docker容器：防护端agent兼容docker容器环境的部署 |  |
| 规格 | 每台web云主机一套 |  |

6）云防火墙(IPS\防病毒网关\内容过滤)服务要求

|  |  |  |
| --- | --- | --- |
| 项目 | 要求 | 备注 |
| 服务形态 | 承载于云安全资源池内，以软件形态提供云上安全防护服务 |  |
| 使用方式 | 云租户通过登录云安全管理平台，单点登录云防火墙服务模块，进行安全运维管理。 |  |
| 主要功能要求 | 支持访问控制功能: 基于用户、应用、时间、地址、服务等方式进行网络访问控制 |  |
| 支持攻击源地图实时展示，支持攻击源、攻击目的、攻击事件统计功能 |  |
| ★支持入侵防御的功能：IPS特征库数量不少于2000多条，支持事件集自定义自动和手动两种更新，支持应急事件及时更新（提供产品截图或官方技术说明文档） |  |
| 支持防病毒功能:支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀、病毒库自动更新、虚拟脱壳、自定义查杀文件大小 |  |
| 规格 | 防护流量100Mbps |  |
| 防护流量200Mbps |  |
| 防护流量500Mbps |  |
| 防护流量1Gbps |  |

**4、大数据服务要求**

**（1）大数据计算服务要求**

1）分布式系统，主要提供结构化数据的存储和计算，采用抽象的作业处理框架为不同用户对各种数据处理任务提供统一的编程接口和界面。

2）采用分布式架构，规模可以根据需要平行扩展。

3）自动存储容错机制，保障数据高可靠性。

4）所有计算在沙箱中运行，保障数据高安全性。

5）以RESTful API的方式提供服务。

6）支持高并发、高吞吐量的数据上传下载。

7）支持离线计算、机器学习两类模型及计算服务。

8）支持基于SQL、Mapreduce、Graph、MPI等多种编程模型的数据处理方式。

9）支持多租户，多个用户可以协同分析数据。

10）支持基于ACL和policy的用户权限管理，可以配置灵活的数据访问控制策略，防止数据越权访问。

**（2）数据治理服务**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 高度集成 | 所有数据治理工作可以在一个平台内完成，用户不再需要关注系统，而只需要关注数据本身。在这个统一的平台上，用户可以进行设计、集成、加工、分析、质量监控、可视化、运维等全生命周期的管理，不同角色的用户登录同一系统进行数据治理不同环节的操作，从而实现用户之间良好的分工协作，为高效、开放的数据治理提供了保障。 |  |
| 安全隔离 | 提供了多租户逻辑隔离的软硬件资源共享机制，提供了租户内的不同部门和用户的数据安全管控体系 |  |
| 不同租户之间的逻辑隔离，一个租户对应一系列的软硬件资源，互不影响，数据层面完全隔离不能互通。用户登录系统后位于某个租户空间，无法查看和操作其它租户空间的数据和代码。 |  |
| 同一租户内部的不同项目空间之间相互隔离，需要由数据的拥有者进行授权才能互通。 |  |
| 在同一项目空间内部，不同的用户具有不同的角色，不同角色对数据的访问权限不同，可以基于独立的表来设置角色对该表的访问权限，也可以设置表和用户的安全等级来控制不同用户对该表的访问。 |  |
| 超大规模 | 基于阿里海量存储和计算引擎 ODPS ，支持 PB 级别的数据治理和管控，支持全天候的自动化作业调度计算，并且系统能够横向扩展和自动伸缩，从而能够适应不同用户不同场景下的数据治理需求。 |  |
| 高可用性和高安全性 | 支持多租户的使用场景，同时满足多用户协同、数据共享、数据保密和安全需求。 |  |
| 多级用户管理机制，数据与运维独立，保证用户数据安全。 |  |
| 易用性与人性化 | 图形化的 运维 管理平台，可以全局、租户等多视角观察数据质量情况。 |  |
| 多种图形化展示分析工具，从多方面分析数据分布情况，以形象生动的图形展示数据血缘关系。 |  |
| 自动化的元数据提取机制，尽可能减轻运维人员的工作负担，由系统自动、动态的捕获元数据的变化。 |  |
| 丰富的数据标准模板数据，参考国标和行业标准，预先设置好多个数据标准模板，方便用户根据自身需求进行选择，并可以根据需要自定义模板。 |  |
| 安装部署 简单，仅需简单的几步操作，用户就可以搭建出数据治理平台 |  |

**（3）数据集成服务**

|  |  |  |
| --- | --- | --- |
| 指标项 | 规格要求 | 备注 |
| 分布式架构 | 采用分布式架构，支持单节点和集群方式部署，作业会被 拆解成多个任务同时在多个作业节点上运行，支持横向扩展，线性 提升处理性能。 |  |
| 多源异构数据转换 | 支持 主流数据库和大数据平台，如Oracle、MySQL、SQL Server、Db2、Sybase、PostgreSQL、Teradata、MongoDB、华为 LibrA、达梦、GBase、PPAS、Kafka、HDFS、HBase、Hive等； |  |
| 支持 RDS、DRDS 、MaxCompute、AnalyticDB、DataHub、OTS、OSS等 组件的数据互通； |  |
| 支持文件搬移与文件解析，FileServer 协议支持 SFTP、SMB、FTP、 FTP、OSS等，文件解析支持诸如xml、txt、csv 和 Excel等格式，支持zip包。 |  |
| 非侵入式数据增量获取 | 不仅支持数据库表全量（ Full Load ）交换复制和基于时间戳的数据库表增量同步，同时支持非侵入式（Non-intrusive）增量（日志或 CDC 方式）数据同步。数据库日志扫描、CDC 的非侵入式数据增量获取技术，用户无需在应用系统数据库端部署任何“代理（ Agent ）”程序，对应用系统的运行影响为零“ Zero-Footprint ”。 |  |
| 自动建表 | 传统方式，当目的数据库未创建数据表时需要手工执行 SQL 语句去创建目的表，效率低而且容易出错；DataBridge 支持异构数据库之间 Web 页面自动建表，字段类型自动匹配，无需手工执行操作过程。 |  |
| 数据统计 | 数据统计功能可以方便用户查看转换运行条数信息。 |  |
| 通过搜索功能，用户可以选择搜索条件（转换名称 / 数据源名称 / 表名）后输入搜索内容并设置时间区间，也可以查看某个时间段的全部转换运行信息。如需导出，单击“导出数据”可将查询结果导出成 csv 文件。 |  |
| 数据对账 | 数据对账用于查询数据源中某张表的总数据，需要在作业管理“统计” 中进行配置。如需导出，单击“导出数据”可将查询结果导出成 csv 文件。 |  |
| 该功能需要先在作业中配置，统计数据保存插件上游有任意个 ODPS 统计和表条数统计插件，即为数据对账管理列表中的的 step 列。 |  |
| 完全基于 B/S 用户界面、简单易用 | 屏蔽了复杂的数据操作过程，无需高级 DBA 或技术人员提供咨询或编写不透明的定制脚本代码，通过简单的界面操作，就可实现大部分数据转换整合的应用场景。同时可以根据业务需要周期性对作业进行自动调度，无需人工干预，任务执行情况可通过日志和图表进行查询。 |  |
| 多租户管理 | 支持创建不同租户，用户加入租户以后，可以创建只属于该租户下的数据源、转换和作业等信息。在数据层面，多租户之间数据严格隔离，租户内的用户数据共享。租户内的每个用户都拥有独立的角色和权限，可以独立配置。租户内不同角色的用户，拥有操作租户资源的不同权限。 |  |
| 高性能 高可靠 | 基于分布式任务的技术架构，多线程并行流式处理，单节点数据传输 性能可达60M B /s 以上 ，单节点TPS最高可达 3 0 万，并可以通过增加作业节点提升整体处理性能。管控 节点及作业节点均为多节点部署，单点故障的情况下，对整体集群不产生任何影响。任务断点续传和自动回滚功能，有效保证了整体作业的高可靠。 |  |

**5、云基础设施服务要求**

（1）IDC机房

供应商提供的政务云专用机房面积不小于300平方，且为完全独立空间、独立门禁，不得同时提供其他非电子政务类云托管业务，要求机房托管业务获得国内信息安全管理体系认证。机房供电保障系统需配置保障油机1500KWA或更高的规格，并实现油机1+1备份、不间断电源系统需配置400KVA（1+1）或更高的UPS规格，机房基础安全设施需配置管网式气体消防、早期烟雾告警、门禁系统等系统。

（2）网络支撑

投标供应商应具有对全市党政单位、企事业单位、乡镇、行政村（社区）等接入单位的完整网络覆盖能力。网络线路要求自用户提出需求起７个工作日完成施工，若无法竣工，采购人有权选择使用其他电信运营商提供的网络。

▲投标供应商必须承诺其提供的IDC机房接受其他电信运营商的网络接入。

**6、云管系统要求**

满足租户对订购的云资源清单、性能、运行状态查询导出功能，具备与内跑平台资源开通流程进行对接。

|  |  |  |
| --- | --- | --- |
| 功能项 | 要求 | 备注 |
| 系统管理 | 组织管理，角色管理，人员管理，界面管理 |  |
| 账单管理 | 账单查询，账单统计，账单导出。账单确认 |  |
| 实例查询 | 云应用服务，云安全服务--统一基础安全服务，云安全服务--自主安全服务 |  |
| 首页优化 | 首页展示，模块互换，费用展示，资源使用 |  |
| 任务订单 | 工作台，任务列表 |  |

**7、异地备份服务要求**

|  |  |  |
| --- | --- | --- |
| 指标项 | 要求 | 备注 |
| 远程复制 | 支持catalog、备份集等备份数据的异地容灾，即通过异地存储的备份数据，对本地、异地中备份服务器、存储服务器、代理端等设备，实现在本机或异机上进行恢复 |  |
| 支持备份任务执行时，采用接龙式的点到点复制方式，实现备份集在存储服务器中的多份同步复制，避免源端服务器在备份集进行1对多并发复制时造成的占用多倍传输资源。 |  |
| 数据加密 | 支持AES、Blowfish等加密算法。对于AES加密需要支持选择不同密钥长度，以便用户根据源端计算资源情况选择合适的数据加密处理。 |  |
| 云端存储 | 基于对象存储技术，支持采用D2C方式，把本地数据备份到云平台，实现本地与云端数据的协同保护。 |  |

**（六）云技术支持服务要求**

（1）应用迁移咨询服务

投标供应商应制定云平台应用开发及迁移部署规范、关系型数据库使用规范、政务云安全防护体系等规范标准，协助各级部门进行云应用开发，配合做好所有业务应用系统的部署、运行和安全保障。

投标供应商应承诺在项目服务期内，针对上云的业务应用提供架构设计咨询，对采购人指定的云业务系统进行统筹规划，指导业务系统的原软件开发商进行代码修改和系统部署，在系统迁移部署提供非代码级别的迁移支持服务。

投标供应商应配合采购人对现业务系统进行调查摸底，根据实际情况配合制定迁移方案，配合各业务部门做好应用迁移工作，确保平稳过渡、顺利迁移。

具体服务要求如下：

|  |  |  |
| --- | --- | --- |
| 指标项 | 服务要求 | 备注 |
| 政务整体云架构设计规划 | 提供政务整体IT架构云化解决方案，包括现有业务应用的梳理、云架构的设计以及上云的策略等。 |  |
| 业务应用上云架构设计 | 提供对单个业务应用的上云架构设计，包括架构设计、改造方案和云资源需求评估等。 |  |
| 软件设计及开发技术咨询 | 提供基于云计算平台的软件设计与开发咨询与技术指导 |  |
| 开发测试环境 | 免费提供仿真的开发与测试环境，供应用系统上线前的开发与测试。测试时间一般为7-30天，测试时间内不得收费。 |  |
| 测试 | 协助用户完成应用系统的功能、性能、安全等测试，测试未通过则禁止应用系统上线运行。 |  |
| 安全咨询 | 提供基于云计算平台的业务应用和政务整体IT规划的安全方面咨询服务 |  |
| 业务应用上云分析诊断 | 提供业务应用上云的方法指导，并提供相关上云指导手册，对上云过程中的技术问题提供支持。 |  |

（2）其他技术服务

投标供应商应提供灾难时数据恢复服务和容灾系统规划服务；提供虚拟机(含操作系统)、存储(含数据库)和网络服务的监控、配置、管理和优化服务；提供故障警告、日志采集、计量统计的功能；提供专家级系统安全和网络安全优化；建设一套规范的资源使用与管理制度；需在项目建设实施期间以及日后维护过程中全部提供原厂服务。

投标供应商保证在云平台出现故障和缺陷时，或接到采购人提出的技术服务要求后1小时内作出响应。

投标供应商应负责云平台整体运维服务，包括IDC 基础运维、云平台运维等,并提供具体的服务方案。

（3）培训要求

投标供应商应根据本项目的特点制定培训方案，应提供培训，使采购人相关人员在培训后能够独立的使用系统，而不必依赖投标供应商现场指导。培训课程应安排在整个项目计划的合适时间段内，培训的内容至少应涵盖政务云平台日常使用所需功能。培训应分为使用及管理培训（针对技术管理人员）和业务开发培训（针对业务开发人员），成交供应商负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表。

**（七）测评要求**

投标供应商所投的软件及硬件部分必须满足基本要求，如果采购人对中标后产品功能存在有疑议，可邀请第三方测评中心对投标方所投软件、硬件进行测试。如果无法满足标书要求的，以虚假应标处理，采购人有权终止合同，并保留追究投标方违约责任的权力。测评所产生的费用由投标供应商承担，并赔偿因项目延误造成的一切损失。

**（八）服务退出和考核**

|  |  |  |
| --- | --- | --- |
| 服务内容 | 服务描述 | 备注 |
| 资源可用性 | 云服务商初期建设应具备一定的规模，以适应业务需求。 |  |
| 需根据政务云使用现状，适时启动扩容，确保云资源的实时可用，即资源使用率不超过70%。 |  |
| 资源可用性业务可用性 | 本指标定义为云服务商应承诺在合同期内每年用户云服务业务可用时间的概率，即每年实际可用时间/(实际可用时间+不可用时间)。 |  |
| 云主机：大于等于99.9%。（每年不可用时间小于8.8小时） |  |
| 云存储：大于等于99.9%。（每年不可用时间小于8.8小时） |  |
| 云数据库：大于等于99.95%。（每年不可用时间小于4.4小时） |  |
| 数据存储持久性 | 本指标定义为云服务商承诺在合同期内数据保存不丢的概率，即每年完好数据/(完好数据+丢失数据)。 |  |
| 云主机：大于99.999%。 |  |
| 云存储可用性：大于等于99.99999999%。 |  |
| 云数据库可用性：大于等于99.9999%。 |  |
| 运营能力 | 对用户开通的服务进行计量计费，按月、季度、年向用户提供完整的记账单。 |  |
| 运维保障能力 | 7\*24小时运行值班监控，专门配属具备云平台维护经验的运维人员，提供专门的支持电话、微信、QQ号等值班方式。 |  |
| 业务和维护响应时间不超过15分钟。 |  |
| 云主机创建时间不超过5分钟。 |  |
| 云主机升级。当云主机现有配置不满足要求时，可进行云主机配置快速升级，可升级配置包括：CPU，内存，网络带宽等；配置升级生效时间不超过10分钟。 |  |
| 云主机克隆。指创建一台跟现有云主机一模一样的机器，根据云主机数据盘的大小整个克隆过程一般不超过30分钟。 |  |
| 故障恢复。云主机发生故障后，切换恢复时间不超过30分钟。 |  |
| 服务赔偿和退出 | 本指标定义为云服务商承诺用户业务某项指标没有达到服务协议中承诺的要求，则会提供的具体赔偿方式。要求云服务承诺对不可用时间、数据丢失等进行赔偿。 |  |
| 云主机：针对不可用时间给予不超过百倍时间赔偿。 |  |
| 云存储：针对不可用时间给予不超过十倍时间赔偿。 |  |
| 云数据库：针对不可用时间给予不超过百倍时间赔偿。 |  |
| 服务退出，如果服务期内单项服务故障总时长超过48小时，或云服务故障，数据丢失，酿成重大事故（正常工作日系统终端24小时以上或社会影响重大）的采购方有权终止合同。 |  |

**（九）商务条款**

**1、付款方式：**

▲合同签订后，服务提供方按实际需求提供服务（招标前未支付的服务费用均按照此次招标结果计费支付），同时，需提供各使用单位实际使用的服务项目（产品类型）、数量的服务费用清单，并经过使用单位确认后由采购人结算服务费用。合同期内一次性支付费用清单内的服务费，经双方确认并签订支付协议，成交供应商出具发票后7个工作日内支付服务费。

2、服务期限：所有政务云服务计费方式均按照此次结果执行，直至出现新的政务云招标结果为止。

**3、本项目为单价合同，具体服务金额按照实际使用情况对照此次单价和统一折扣率计算并支付。**

**4、报价说明**

1）鉴于各使用单位应用系统数量为动态数值，故本项目不能确定各项服务总量，本次招标采购的是云主机等资源每月租赁费的单价（不足1月按实际产生天数计费，每日租赁费=月租赁费/30）。

2）本次投标品目采购人已设单价最高限价，投标供应商在采购人设定的最高限价的基础上根据企业自身实力及市场行情自行填报折扣率，▲**不同投标品目要求填报统一的折扣率（即所有投标品目的折扣率均相同），否则其报价无效并作无效标处理**。

**3）本项目按各单价最高限价×最高限价的统一折扣率×各部门各实际服务数量进行结算。各单价最高限价详见下表：**

**[洞头区政务云（私有云）服务](https://www.zcygov.cn/proj-procurement/project-result-detail/5ee955ecdf4d3b97" \t "https://www.zcygov.cn/bid-inviting/purchaseFileMake/_blank)内容清单和最高限价**

单位：(元/月)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务类型 | **计费项** | **规格说明** | | **说明** | **最高限价** | **备注** |
| **一、基础服务（IaaS)** | | | | | | | |
| 1 | 计算服务 | 增强型云主机 | 一核 | 1GB | CPU主频≥2.3GHz；以上云主机价格包含操作系统正版授权；40G系统盘（SATA），linux系统盘40G，Windows系统盘40G；不含数据盘的价格 | 35 | 需额外订购云主机数据盘进行搭配使用 |
| 2GB | 64 |
| 4GB | 160 |
| 8GB | 294 |
| 两核 | 2GB | 178 |
| 4GB | 238 |
| 8GB | 352 |
| 16GB | 525 |
| 四核 | 4GB | 350 |
| 8GB | 470 |
| 16GB | 700 |
| 32GB | 1040 |
| 八核 | 8GB | 660 |
| 16GB | 880 |
| 32GB | 1315 |
| 64GB | 1960 |
| 十六核 | 16GB | 1300 |
| 32GB | 1745 |
| 64GB | 2620 |
| 128GB | 3840 |
| 三十二核 | 64GB | 3490 |
| 128GB | 5200 |
| 2 | 存储服务 | 云主机数据盘 | SSD数据盘 | 100GB | 需挂载在云主机上使用，需以100G为单位订购 | 70 | 需以100G为单位订购 |
| 高效数据盘 | 100GB | 需挂载在云主机上使用，需以100G为单位订购 | 41 | 需以100G为单位订购 |
| 云存储 | 每TeraByte (TB)字节 | 1T | 对象存储OSS，需以1T为单位订购 | 181 | 需以1T为单位订购 |
| NAS存储 | 以100GB为单价 | 100GB | 可提供常见标准接口协议提供存储服务，需以100G为单位订购 | 23 | 需以100G为单位订购 |
| 3 | 网络服务 | 共享互联网出口带宽 | 共享带宽 | 500 Mbps | 云平台共享互联网出口；提供配套的IP地址 | 6856 |  |
| 1000 Mbps | 13711 |
| 每增加100Mbps | 1644 |
| 独享互联网出口带宽 | 独享带宽 | 10M |  | 363 |  |
| 20M | 727 |
| 50M | 1091 |
| 100M | 2182 |
| 200M | 3819 |
| 云负载均衡 | 以1个实例为单位 | 实例 | 提供4层和7层负载均衡。支持包括全局负载均衡和服务器负载均衡的功能；支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、UDP强行负载等算法。 | 639 | 提供4层和7层负载均衡 |
| **二、平台**即**服务（PaaS）** | | | | | | | |
| 1 | 云数据库 | 云数据库 | My SQL数据库服务（最大连接数） | 60 | 约占用内存240MB | 27 | 不含“数据库存储”，需额外订购“数据库存储”，数据库存储单价为76.5元/100G/月，数据库存储需以100G为单位订购。 |
| 150 | 约占用内存600MB | 67 |
| 300 | 约占用内存1200MB | 127 |
| 600 | 约占用内存2400MB | 247 |
| 1500 | 约占用内存6000MB | 620 |
| 2000 | 约占用内存12000MB | 1102 |
| 2000 | 约占用内存24000MB | 2029 |
| 2000 | 约占用内存48000MB | 3940 |
| MS SQL Server数据库服务（最大连接数） | 100 | 约占用内存1000MB | 91 |
| 200 | 约占用内存2000MB | 183 |
| 400 | 约占用内存4000MB | 365 |
| 600 | 约占用内存6000MB | 550 |
| 800 | 约占用内存8000MB | 732 |
| 1200 | 约占用内存12000MB | 1097 |
| 2000 | 约占用内存24000MB | 1736 |
| 2000 | 约占用内存48000MB | 3292 |
| 数据库存储（以100GB为单价） | 100GB | SSD存储，以100GB为单价 | 70 | 与数据库搭配使用，需以100G为单位订购 |
| **三、云安全服务** | | | | | | | |
| 1 | 自主云安全服务 | 自主云安全服务 | WAF | 25M | 1个一级域名和10个二级域名（流量上限为25M） | 702 | 1个一级域名和10个二级域名（流量上限为25M） |
| 50M | 2个一级域名和20个二级域名（流量上限为50M） | 1163 | 2个一级域名和20个二级域名（流量上限为50M） |
| 100M | 4个一级域名和40个二级域名（流量上限为100M） | 1888 | 4个一级域名和40个二级域名（流量上限为100M） |
| 200M | 8个一级域名和80个二级域名（流量上限为200M） | 3097 | 8个一级域名和80个二级域名（流量上限为200M） |
| 500M |  | 4687 |  |
| 2 | 网页防篡改 | 防篡改防护服务（1个网站） |  | 355 |  |
| 3 | 主机防护 （EDR） | 1台服务器 | 单价\*数量计算总价 | 120元/台 | 单价\*数量计算总价 |
| 10台服务器 | 94元/台 |
| 50台服务器 | 84元/台 |
| 200台服务器 | 75元/台 |
| 300台以上 | 65元/台 |
| 4 | 防火墙 | 100M吞吐量 |  | 535 |  |
| 200M吞吐量 |  | 825 |  |
| 500M吞吐量 |  | 1379 |  |
| 1000M吞吐量 |  | 2110 |  |
| 5 | 入侵防护/入侵监测 | 500M吞吐量 |  | 450 |  |
| 1G吞吐量 |  | 800 |  |
| 2G吞吐量 |  | 1500 |  |

第三部分 供应商须知

一、说明

1、本次采购工作是按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购竞争性磋商采购方式管理暂行办法》、并参照《浙江省财政厅、省监察厅关于进一步规范政府采购活动的若干意见》及相关法律规章组织和实施。

2、投标供应商根据自身情况可选择标项进行投标，也可以同时对多个标项进行投标，但必须对所投标项中全部采购内容进行投标，不允许仅对所投标项中部分内容进行投标，否则按无效投标处理。

3、无论投标过程中的作法和结果如何，供应商自行承担采购活动中所发生的全部费用。采购人有权选择成交供应商的供货及服务范围。

4、**本项目采用竞争性磋商采购方式进行采购，在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。已提交磋商响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。**

5、知识产权

5.1投标供应商应保证，采购人在中华人民共和国使用货物和服务的任何一部分时，免受第三方提出侵犯其专利权、商标权或其它知识产权的起诉。

5.2投标供应商应对采购人在使用该产品时所涉及到的专利权负责，不损害采购人的利益。

5.3报价应包括所有应支付的对专利权和版权、设计或其他知识产权而需要向其他方支付的版税。

5.4投标供应商提供得货物或服务中如使用其他公司的相关专利，应在标书中出示相关授权，如未出示但使用了其他公司的专利，导致供应商中标而引起相关诉讼，由投标供应商承担。

6、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。如在评标过程（或标后质疑投诉期内）中发现供应商间存在上述关系，存在上述关系的全部供应商均做无效投标（无效中标）处理。

除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

7、本项目投标供应商如涉及分公司的，负责人等同于法定代表人（磋商文件以下同）。

**8、根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号），本项目所属行业为信息传输业，投标供应商属于磋商文件中明确的行业所对应的小微企业享受价格优惠折扣，否则不享受。**

9、为使投标供应商对本项目情况有所了解，投标供应商可自行到采购人实地进行现场勘察，以便获取由投标供应商自行负责编制响应文件和签订合同所需的一切资料并充分理解了为之所承担的风险、义务和责任。

10、安全生产

在招标及合同执行过程中，投标供应商应承担由于其行为所造成的人身伤害、财产损失或损坏的责任，无论何种原因所造成，采购人均不负责。

11、**法定代表人（负责人）授权书中法定代表人（负责人）必须签字或盖章，否则做无效投标处理。**

**12、本项目磋商文件如有补充、更正均见浙江政府采购网（http://zfcg.czt.zj.gov.cn/）。供应商须在投标截止前自行查看是否有补充、更正文件，并按补充、更正文件要求投标，否则责任自负。**

**13、供应商如果获取磋商文件后不来参与本次投标要在响应文件递交截止前给予书面告知及其理由，否则采购组织机构将该情况报同级财政部门，并视情况将其列入不良供应商名单。**

**14、成交供应商必须是已申请加入浙江省政府采购供应商库的，未申请加入的请到浙江省政府采购网申请加入：http://zfcg.czt.zj.gov.cn/。**

**15、本项目采用在线投标响应方式，执行《浙江省财政厅关于印发浙江省政府采购项目电子交易管理暂行办法的通知》（浙财采监〔2019〕10 号）等相关规定。**

16、为支持和促进中小企业发展，进一步发挥政府采购政策功能，温州市财政局出台了《温州市财政局关于温州市政府采购支持中小企业信用融资的通知》（温财采〔2020〕3号），供应商若有融资意向，可直接登录http://jinrong.zcygov.cn，查看信用融资政策文件及各相关银行服务方案，也可直接向各银行咨询相关业务。

二、竞争性磋商文件

1、竞争性磋商文件

1.1 磋商文件发放

投标供应商网上自行下载磋商文件。

1.2 竞争性磋商文件约束力

▲供应商一旦获取了本竞争性磋商文件并参加磋商采购，即被认为接受了本竞争性磋商文件中所有条款和规定。

1.3 竞争性磋商文件的组成

竞争性磋商文件由竞争性磋商文件总目录所列内容及补充资料等组成。

2、竞争性磋商文件的澄清

供应商对竞争性磋商文件如有疑点要求澄清，或认为有必要与采购人进行技术交流，可用书面形式（包括信函、传真，下同）通知采购代理机构，但通知不得迟于规定的质疑时间前使采购代理机构收到，采购代理机构将用书面形式予以答复。如有必要，可将不说明来源的答复书面发给各有关供应商并予以公告。任何口头答复均不作为报价依据。

3、竞争性磋商文件的修改

3.1 在响应文件递交截止时间前，采购人有权澄清或者修改磋商文件，并以书面形式（补充、更正文件）通知供应商。补充、更正文件作为磋商文件的组成部分，对所有供应商均有约束力。

3.2 澄清或者修改的内容可能影响响应文件编制的，采购人或者采购代理机构在响应文件递交截止时间至少5个工作日前，以书面形式通知所有获取磋商文件的潜在供应商；不足5个工作日的，采购人或者采购代理机构顺延提交响应文件的截止时间。

3.3 补充、更正文件在浙江政府采购网（http://www.zjzfcg.gov.cn/）予以公告公布。

三、磋商响应文件

1、磋商响应文件

1.1 供应商应仔细阅读竞争性磋商文件中的所有内容，按照竞争性磋商文件要求，详细编制磋商响应文件。并对竞争性磋商文件的要求做出实质性响应。实质性响应的磋商响应文件应该是与竞争性磋商文件要求没有重大偏离。未实质性响应的磋商响应文件将被拒绝，但允许在基本满足采购技术要求的前提下出现的微小差异。

1.2 供应商必须按竞争性磋商文件的要求提供相关技术参数、资料，包括采用的计量单位，并保证磋商响应文件的正确性和真实性。磋商响应文件全部内容应保持一致，否则可能导致对其不利评定甚至被拒绝。技术和商务如有偏离均应填写偏离表。

1.3 供应商应仔细阅读竞争性磋商文件中的所有内容，按照竞争性磋商文件要求，详细编制磋商响应文件，所有文件资料必须是针对本次采购。不按竞争性磋商文件的要求提供的磋商响应文件可能导致被拒绝。

2、磋商响应文件的组成

▲**磋商响应文件由资格文件、报价文件、商务技术文件组成。**

**2.1 资格文件组成**

|  |  |
| --- | --- |
| 序号 | 内容（**以下1-3项内容投标供应商必须提供，否则不能通过资格审查的，责任自负。**） |
| 1 | 投标供应商的营业执照、税务登记证（如为多证合一仅需提供营业执照，扫描件加盖有效公章）。 |
| 2 | 投标供应商参与政府采购活动投标资格声明函（附件一） |
| 3 | 投标供应商特定资格条件证明：供应商须具有增值电信业务经营资质（提供增值电信业务经营许可证）运营商或其分支机构（提供有效授权或证明文件） |

**2.2 报价文件组成**

|  |  |
| --- | --- |
| 序号 | 内容（▲**序号2项投标供应商必须提供，否则不能通过符合性审查的，责任自负**。） |
| 1 | 报价文件封面（格式自拟） |
| 2 | 开标一览表（附件二） |
| 3 | 1、投标供应商享受小微企业价格折扣应提供以下证明材料（放在报价文件中，不提供的不享受价格折扣）：  （1）《中小企业声明函》（加盖供应商公章，格式见磋商文件第四部分附件1）。  2、投标供应商享受监狱企业价格折扣应提供以下证明材料（放在报价文件中，不提供的不享受价格折扣）：  （1）监狱企业参加政府采购活动时，应当提供由省级及以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件（加盖投标供应商公章）。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策。  3、投标供应商享受残疾人福利性单位价格折扣应提供以下证明材料（放在报价文件中，不提供的不享受价格折扣）：  （1）残疾人福利性单位声明函（加盖投标供应商公章，格式见磋商文件第四部分附件2）。在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。  说明：供应商企业属于以上多种性质的，不重复享受扶持政策。 |

**2.3 商务技术文件组成**

|  |  |
| --- | --- |
| 序号 | 内容（**投标供应商应提供相关内容，否则不能通过符合性审查的，责任自负**。） |
| 1 | 商务技术文件封面（格式自拟） |
| 2 | 投标函（附件三） |
| 3 | 供应商法定代表人授权书（附件四），如为法定代表人参与的只须提供法定代表人身份证扫描件。 |
| 4 | 法定代表人诚信投标承诺书（附件五） |
| 5 | 供应商相关资质、资信或信用证书、荣誉证书、获奖证书等（如有则提供，扫描件加盖有效公章） |
| 6 | 投标供应商业绩（附件六，如有则提供） |
| 7 | 商务偏离表（附件七（一））、技术偏离表（附件七（二）） |
| 8 | 云平台资质（具体要求见各标项评分项） |
| 9 | 云平台技术方案（具体要求见各标项评分项） |
| 10 | 云平台安全方案（具体要求见各标项评分项） |
| 11 | 技术服务能力（具体要求见各标项评分项） |
| 12 | 机房要求（具体要求见各标项评分项） |
| 13 | 技术服务方案（具体要求见各标项评分项） |
| 14 | 项目服务人员汇总表（附件八，具体要求见各标项评分项） |
| 15 | 拟派项目人员情况表（附件九，具体要求见各标项评分项） |
| 16 | 根据磋商文件中的采购内容与技术要求、评标细则，需要提供的其它文件和资料。 |
| 17 | 其它供应商须说明的资料（如有则提供） |
| 18 | 供应商针对评分细则，编制目录索引，注明评标细则项目所在响应文件页码。 |

3、采购内容填写说明

3.1 磋商响应文件格式

供应商应按照磋商文件第三部分第三条第2款所列出的内容及格式逐一按顺序组成磋商响应文件。

4、投标报价

4.1供应商应按磋商文件中《开标一览表》填写投标报价。

4.2项目执行过程中，如成交供应商不能全量提供所需资源，或所提供的资源基础平台（含新增）发生重大变更的，成交供应商需及时通知采购人，双方就相关问题进行协商。

4.3投标价必须包括完成租赁项目所需的租赁费用、人员支出费用、必要设备及工具、维护服务、器材、管理费用、税费、利润、招标代理费、完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定及合同包含的所有风险、责任等各项全部费用并承担一切风险责任。

4.4供应商应考虑企业自身实力、经验及项目实施过程中的各种因素，根据采购说明，详细说明所能提供的各项具体服务内容，自主确定投标价。投标供应商应在各自技术和商务占优势的基础上并充分考虑本项目的重要性，提供对采购人最优惠的报价。

4.5**投标供应商在投标价中应充分考虑项目期间成本投入的市场风险、政策性调整及调查期间的不可预见因素，今后不再作调整，采购人要求变动的内容除外。供应商在最终报价中应充分考虑所有可能发生的费用，否则采购人将视报价中已包括所有费用。供应商须注意报价风险。**

**供应商对在合同执行中，除上述费用及磋商文件规定的由成交供应商负责的工作范围以外需要采购人协调或提供便利的工作应当在响应文件中说明。**

填写报价表格时，各项费用应如实填写。

5、采购人要求分类报价是为了方便评审，但在任何情况下不限制采购人以其认为最合适的条款签订合同的权利。

6、保证金

无

7、磋商响应文件的有效期

7.1 自响应文件递交截止时间起90天内，磋商响应文件应保持有效。有效期短于这个规定期限的磋商响应文件将被拒绝。

7.2 在特殊情况下，采购人可与供应商协商延长磋商响应文件的有效期，这种要求和答复均应以书面形式进行。

7.3 供应商可拒绝接受延期要求，同意延长有效期的供应商不能修改磋商响应文件。

8、磋商响应文件的编制

**8.1 本项目通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应（电子投标）。供应商应通过“政采云电子交易客户端”，并按照本磋商文件和“政府采购云平台”的要求编制并加密磋商响应文件。**

**8.2 投标供应商应当按照本章节“磋商响应文件组成”规定的内容及顺序在“政采云电子交易客户端”编制磋商响应文件。**

**8.3 本文件《第六部分 磋商响应文件格式》中有提供格式的，投标供应商参照格式进行编制（格式中要求提供相关证明材料的还需后附相关证明材料）；本文件《第六部分 磋商响应文件格式》未提供格式的，请各投标单位自行拟定格式。**

**8.4 《磋商响应文件》内容不完整、编排混乱导致《磋商响应文件》被误读、漏读或者查找不到相关内容的，相关责任由投标供应商自负。**

**8.5 《磋商响应文件》因字迹潦草或表达不清所引起的后果由投标供应商负责。**

**8.6 投标供应商没有按照本章节“磋商响应文件组成”要求提供全部资料，或者没有仔细阅读磋商文件，或者没有对磋商文件在各方面的要求作出实质性响应，由此造成的一切后果由投标供应商自行承担。**

**9、磋商响应文件的签章**

**9.1 《磋商响应文件》的签章：见《第一部分 磋商邀请函（供应商须知前附表）》；**

**9.2 根据磋商文件要求在磋商响应文件相应位置由投标供应商法定代表人或授权代表签字（或盖章），需要加盖投标供应商公章的采用CA电子签章。**

**9.3 CA电子签章操作指南详见《供应商-政府采购项目电子交易操作指南》（https://help.zcygov.cn/web/site\_2/2018/12-28/2573.html）。**

**10、磋商响应文件的形式**

**10.1 磋商响应文件的形式：见《第一部分 磋商邀请函（供应商须知前附表）》；**

**10.2 “电子加密磋商响应文件”：“电子加密磋商响应文件”是指通过“政采云电子交易客户端”完成磋商响应文件编制后生成并加密的数据电文形式的磋商响应文件。**

**10.3磋商响应文件的份数**

**磋商响应文件的份数：见《第一部分 磋商邀请函（供应商须知前附表）》。**

四、磋商响应文件递交

**1、磋商响应文件的上传和递交**

**“磋商响应文件”的上传、递交：见《第一部分 磋商邀请函（供应商须知前附表）》。**

**2、“电子加密磋商响应文件”解密和异常情况处理**

**“电子加密磋商响应文件”解密：见《第一部分 磋商邀请函（供应商须知前附表）》。**

**3、磋商响应文件的补充、修改或撤回**

**3.1 供应商应当在响应文件递交截止时间前完成磋商响应文件的上传、递交，并可以补充、修改或者撤回磋商响应文件。补充或者修改磋商响应文件的，应当先行撤回原文件，补充、修改后重新上传、递交。响应文件递交截止时间前未完成上传、递交的，视为撤回磋商响应文件。响应文件递交截止时间后递交的磋商响应文件，“政府采购云平台”将予以拒收。**

**3.2 响应文件递交截止时间后，投标供应商不得撤回、修改《磋商响应文件》。**

**4、磋商响应文件的备选方案**

**投标供应商不得递交任何的投标备选（替代）方案，否则其磋商响应文件将作无效标处理。**

五、开标和评审

1、开标

1.1 **采购代理机构按磋商文件规定的时间、地点通过“政府采购云平台”组织开标、开启磋商响应文件，所有供应商均应当准时在线参加。投标供应商因未在线参加开标而导致磋商响应文件无法按时解密等一切后果由供应商自己承担**。

**在线开评标进行时，供应商投标代表需自行关注平台提示信息，期间有发出“询标/澄清函”、“多轮报价函”等相关线上函件时，因供应商自身原因逾期/错过回复时间，由此造成的后果由供应商自行承担。**

1.2 开标流程

（1）向各投标供应商发出电子加密磋商响应文件【开始解密】通知，由供应商按磋商文件规定的时间内自行进行磋商响应文件解密。**投标供应商在规定的时间内无法完成已递交的“电子加密磋商响应文件”解密的，其磋商响应文件按拒收处理。**

（2）磋商响应文件解密结束，磋商小组在对磋商响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对磋商响应文件中含义不明确、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出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出磋商响应文件的范围或者改变磋商响应文件的实质性内容。

（3）磋商小组所有成员应当集中与单一供应商分别进行磋商。在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组通知所有参加磋商的供应商。供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交磋商响应文件，并由其法定代表人或授权代表签字（或盖章）并加盖公章。**如竞争性磋商文件所列采购内容明确不需要修改的或供应商磋商响应文件清楚明确不需要澄清的，可以不进行磋商，直接要求供应商进行最终报价。**

（4）磋商结束后，磋商小组应当要求所有实质性响应的投标供应商在规定时间内提交最终报价。投标供应商未在规定时间提交最终报价的按无效投标处理。

（5）开启所有实质性响应的投标供应商的最终报价。

（6）评审结束后，公布采购结果。

**特别说明：如遇“政府采购云平台”电子化开标或评审程序调整的，按调整后程序执行。**

2、评审

2.1 评审由采购人依法组建的磋商小组负责，并独立履行下列职责：

1）审查磋商响应文件是否符合竞争性磋商文件要求，并作出评价；

2）要求供应商对磋商响应文件有关事项作出解释或者澄清；

3）按照竞争性磋商文件确定的评审办法对供应商进行排序，推荐候选供应商，将综合得分第一的供应商向采购人推荐其为成交供应商；

4）向采购代理机构或者有关部门报告非法干预评审工作的行为。

2.2 评审应当遵循下列工作程序：

1）磋商响应文件初审。初审分为资格性检查和符合性检查。

（1）资格性检查。依据法律法规和竞争性磋商文件的规定，对磋商响应文件中的资格证明等进行审查，以确定供应商是否具备参与磋商资格。

（2）符合性检查。依据竞争性磋商文件的规定，从磋商响应文件的有效性、完整性和对竞争性磋商文件的响应程度进行审查，以确定是否对竞争性磋商文件的实质性要求作出响应。

2）澄清有关问题。对磋商响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，磋商小组可以要求供应商对磋商响应文件中含义不明确、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出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出磋商响应文件的范围或者改变磋商响应文件的实质性内容。

3）比较与评价。按竞争性磋商文件中规定的评审方法和标准，对资格性检查和符合性检查合格的磋商响应文件进行商务和技术评估，综合比较与评价。

2.3 ▲**供应商存在下列情况之一的，磋商响应文件按无效处理：**

**1）磋商响应文件未按磋商文件要求签署或CA电子签章的；**

**2）不具备磋商文件中规定的资格要求的；**

**3）最终报价超过磋商文件中规定的预算金额或者最高限价的；**

**4）响应文件含有采购人不能接受的附加条件的（包括磋商文件中明确要求不得偏离的招标要求，存在负偏离的）；**

**5）对关键条文的偏离、保留或反对，例如关于付款方式、服务期（完工期）、免费质保期、适用法律法规、标准、税费等其他内容；**

**6）存在串标或弄虚作假情况的；**

**7）参与本项目的不同供应商单位负责人为同一人或者存在直接控股、管理关系的；**

**8）在竞争性磋商文件未做任何调整的情况下，参与磋商的供应商最终报价超过其磋商响应文件中报价的；**

**9）未在规定时间提交最终报价的；**

**10）法律、法规和磋商文件规定的其他无效情形（或出现重大偏差）。**

2.4 ▲**磋商小组发现磋商响应文件有下列情形之一的属于重大偏差(磋商小组按少数服从多数原则认定),按照无效投标处理**：

**1）未按磋商文件要求编制或字迹模糊、辨认不清的磋商响应文件；**

**2）除2.3条款以外，出现其它明显不符合采购要求的磋商响应文件；**

**3）除2.3条款以外，出现其它不符合磋商文件中规定的实质性要求的磋商响应文件，是否为偏离实质性要求由磋商小组认定。**

2.5 ▲**磋商小组认为供应商的最终报价明显低于其他有效供应商的最终报价，有可能影响采购质量或者不能诚信履约的，评审时应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应当将其作为无效投标处理**。

2.6 磋商小组在评标中，不得改变磋商文件中规定的评标标准、方法和中标条件。

2.7 评标时如遇到磋商文件未规定的特殊情况，由磋商小组按少数服从多数原则集体决定处理。

2.8 磋商小组对未中标的供应商不作解释。

3、磋商响应文件的澄清

3.1 为有利于对磋商响应文件的比较和评议，必要时磋商小组可要求投标供应商对磋商响应文件相关事宜进行澄清。磋商小组将通过“政府采购云平台”在线询标的形式要求投标供应商在规定的时间内作出必要的澄清、说明，供投标供应商澄清、说明时间不少于30分钟，投标供应商未在规定的时间内作出必要的澄清、说明将导致对其不利的评定。

3.2 投标供应商的澄清、说明应当通过“政府采购云平台”在线答复形式提交，并加盖公章。投标供应商的澄清、说明不得超出磋商响应文件的范围或者改变磋商响应文件的实质性内容。

4、响应文件递交截止时或评审过程中有效投标供应商不足三家的，不予开标或评标（在评审过程中以下情况除外：符合《财政部关于政府采购竞争性磋商采购方式管理暂行办法有关问题的补充通知》（财库【2015】124号文件）的规定，采用竞争性磋商采购方式采购的政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有2家的，竞争性磋商采购活动可以继续进行。）

5、评审原则

磋商小组按照竞争性磋商文件的要求和条件对磋商响应文件进行评估，综合比较与评价。

5.1 磋商小组负责审查磋商响应文件是否符合竞争性磋商文件的要求，并作出评价。磋商小组认为必要时，可向供应商进行询标澄清。

5.2 磋商小组将综合分析合格供应商的各项指标，而不是以单项指标的优劣评选出成交的供应商。

5.3 磋商小组对合格供应商的磋商响应文件和最终报价进行综合评定。如竞争性磋商文件所列采购内容明确不需要修改的或供应商磋商响应文件清楚明确不需要澄清的，可以不进行磋商环节，直接要求供应商进行最终报价，进行综合评分。在竞争性磋商文件未做任何调整的情况下，参与磋商的供应商如有出现最终磋商报价超过磋商响应文件中报价的，则该供应商的报价按无效投标处理。

5.4本次评审采用综合评分法，磋商小组根据竞争性磋商文件制定的评审办法对供应商进行评审排序，将综合得分第一的供应商向采购人推荐其为成交供应商。

6、有下列情形之一的，视为供应商相互串通投标：

6.1 不同供应商的磋商响应文件由同一单位或者个人编制；

6.2 不同供应商委托同一单位或者个人办理投标事宜；

6.3 不同供应商的磋商响应文件载明的项目管理成员为同一人；

6.4 不同供应商的磋商响应文件异常一致或者投标报价呈规律性差异；

6.5 不同供应商的磋商响应文件相互混装；

7、经磋商小组认定供应商进行串通投标的，磋商小组可以对相关供应商做出无效投标处理，并上报政府采购管理部门进行进一步处理。

**8、可中止电子交易活动的情形**

**采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购组织机构可中止电子交易活动：**

**1）电子交易平台发生故障而无法登录访问的；**

**2）电子交易平台应用或数据库出现错误，不能进行正常操作的；**

**3）电子交易平台发现严重安全漏洞，有潜在泄密危险的；**

**4）病毒发作导致不能进行正常操作的；**

**5）其他无法保证电子交易的公平、公正和安全的情况。**

**出现前款规定情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新采购。**

六、授予合同

1、决标

磋商结束后，磋商小组按照竞争性磋商文件确定的评审办法，确定成交供应商。

**采购人将把成交通知书授予最佳报价者，但最低报价不是成交的唯一保证。**

2、成交通知书

2.1 评审结束后，采购代理机构在浙江政府采购网公告采购结果，同时发出成交通知书，成交公告期限为1个工作日。

2.2 成交通知书对采购人和成交供应商具有法律约束力。成交通知书发出后，采购人改变成交结果或者成交供应商放弃成交资格的，应当承担法律责任。

2.3 成交无效

1）发现成交供应商资格无效或成交供应商放弃成交或拒绝与采购人签订合同的,按相关规定执行。

2）有《中华人民共和国政府采购法实施条例》第七十一条、第七十二条、第七十三条、第七十四条规定的违法行为之一，由政府采购监管部门依法处理。

3、磋商小组对未成交的供应商不作落标原因解释。

4、签订合同

4.1 成交供应商须主动联系采购人或采购代理机构领取成交通知书。成交供应商应当在成交通知书发出之日起30日内与采购人签订合同。成交供应商未经采购人许可，在规定时间内未到采购人处与采购人签订合同，则视为拒签合同。

4.2 磋商文件、成交供应商的磋商响应文件及投标修改文件、评标过程中有关澄清文件及经双方签字的询标纪要（承诺）和成交通知书均作为合同附件。

4.3 拒签合同的责任

成交供应商接到成交通知书后，在规定时间内（30日历天）借故否认已经承诺的条件而拒签合同，以违约处理，并赔偿采购人由此造成的直接经济损失；采购人重新组织采购的，所需费用由原成交供应商承担。

5、招标代理服务费

中标后，各标项成交供应商需向招标代理机构支付招标代理服务费（标项1:16500元，标项2:11500元），招标代理服务费包含在报价中，但不在报价表中单列。

第四部分 政府采购政策功能相关说明

一、小、微企业（含监狱企业、残疾人福利性单位）扶持政策说明

1、文件依据

（1）关于印发《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46号）

（2）浙江省省财政厅《关于开展政府采购供应商网上注册登记和诚信管理工作的通知》（浙财采监〔2010〕8号）

（3）《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）

（4）财政部、司法部《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）

（5）《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）

2、在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策：

（一）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（二）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（三）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

3、投标供应商享受小微企业价格折扣应提供以下证明材料（放在报价文件中，不提供的不享受价格折扣）：

（1）《中小企业声明函》（加盖投标供应商公章，格式见附件1）；

4、投标供应商享受监狱企业价格折扣应提供以下证明材料（放在报价文件中，不提供的不享受价格折扣）：

（1）监狱企业参加政府采购活动时，应当提供由省级及以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件（加盖投标供应商公章）。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策。

5、投标供应商享受残疾人福利性单位价格折扣应提供以下证明材料（放在报价文件中，不提供的不享受价格折扣）：

（1）残疾人福利性单位声明函（加盖投标供应商公章，格式见附件2）。在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。

附件1：

中小企业声明函（服务类）

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（采购文件中明确的所属行业）；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1，属于（中型企业、小型企业、微型企业）；

2. （标的名称） ，属于（采购文件中明确的所属行业）；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：

说明：

1、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。

2、如中标，将在中标公告中将此中小企业声明函予以公示，接受社会监督。

附件2

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位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（盖章）：                  
日期：

说明：

1、如中标，将在成交公告中将此残疾人福利性单位声明函予以公示，接受社会监督；

2、供应商提供的《残疾人福利性单位声明函》与事实不符的，依照《政府采购法》第七十七条第一款的规定追究法律责任。

第五部分 合同格式（参考格式）

项目编号：

政府采购合同

项目名称:

标项名称:

采购人（全称）:

供应商（全称）:

签订日期:

签订地点:

采购人（全称，以下简称甲方）：

地址：

法定代表人：

供应商（全称，以下简称乙方）：

地址：

法定代表人：

为了保护甲、乙双方合法权益，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》、《政府购买服务管理办法》及其他有关法律、《浙江省财政厅关于进一步加强和规范政府购买服务管理的通知》（浙财综〔2021〕19号）等有关规定，为保证政府采购服务质量，明确双方的权利义务，经甲乙双方协商，本着平等互利和诚实信用的原则，双方一致同意，签订本合同。

1. 服务项目内容

1.1甲方通过 竞争性磋商 方式确定由乙方提供以下服务：洞头区政务云平台租赁。

1.2 服务内容及数量（可另附明细附件）：详见磋商文件的采购内容及要求部分和响应文件的相应内容。

1.3 服务地点：

1.4服务期限：所有政务云服务计费方式均按照此次结果执行，直至出现新的政务云招标结果为止。

**1.5本项目为单价合同，具体服务金额按照实际使用情况对照此次单价和统一折扣率计算并支付。**

1.6售后服务

详见磋商文件及响应文件承诺。

2. 服务项目质量标准和要求（可另附明细附件)

见磋商文件 。

3. 合同金额及报价明细

3.1本项目单价最高限价的统一折扣率为 %。

**3.2本项目按各单价最高限价×最高限价的统一折扣率×各部门各实际服务数量进行结算。各单价最高限价详见磋商文件。**

3.3鉴于各使用单位应用系统数量为动态数值，故本项目不能确定各项服务总量，本次招标采购的是云主机等资源每月租赁费的单价（不足1月按实际产生天数计费，每日租赁费=月租赁费/30）。

3.4合同服务费用应包括履约验收产生的检验（监测）费、劳务报酬等费用；

3.5乙方开户名称：

开户银行：

银行帐号：

4. 付款方式，甲方以下述第4.4项方式支付合同款项。

4.1一次性付款：

乙方履约完毕后且甲方按照本合同第5条规定验收合格后， 日内一次性支付全部服务费。

4.2分期支付：

（1）按年/按季度/按月支付等额的服务费；

（2）本合同签订后 日内，甲方向乙方支付 元（或服务费总额的 %)；在交付服务成果并经验收合格后，支付服务费 元（或服务费总额的 %)。

4.3按本合同项下的项目进度支付服务费（应根据项目特点具体约定,以下阶段支付仅为参考）：

（1）乙方服务人员到达服务地点并提交服务实施方案后 日内，甲方将总服务费的 %支付给乙方；

（2）第二次付款为总服务费的 %,甲方在乙方提交服务阶段报告及其它文件,且该报告及相关文件符合本合同要求并经甲方验收后 日内付给乙方；

（3）最后一次付款为总服务费的 %，甲方应在乙方完全履行合同，递交服务总报告及相关文件资料并经甲方验收完毕日内付给乙方。

4.4其他付款：▲合同签订后，乙方按实际需求提供服务（招标前未支付的服务费用均按照此次招标结果计费支付），同时，需提供各使用单位实际使用的服务项目（产品类型）、数量的服务费用清单，并经过使用单位确认后由甲方结算服务费用。合同期内一次性支付费用清单内的服务费，经双方确认并签订支付协议，乙方出具发票后7个工作日内支付服务费。

5. 验收程序、方法及标准

5.1本项目验收按照《温州市政府采购履约验收办法》（温财采〔2020〕6号）文件执行。

5.2验收程序，可按照简易程序验收（ ）或一般程序验收（ ）进行验收。

5.3验收方法，可按照一次性验收（ ）、分段验收（ ）或分期验收（ ）进行验收。

5.4验收标准（可另附明细附件)：

6. 履约保证金

无

7. 资质保证及使用规则

7.1甲方保证各使用单位提供信息与文件的真实、完整、准确、合法、有效，并承担相应的法律责任。

7.2各使用单位使用本服务开展互联网信息服务等相关业务的，应保证于本合同签订时及本合同有效期内持续具备开展该业务所需的全部资质及/或履行相关手续，并应根据乙方要求签订相关安全责任协议书并严格遵守在该等文件中的承诺。

7.3各使用单位应按照本合同约定向乙方提交上述资质证明文件、资料的原件，并提交复印件并加盖甲方公章，供乙方留存。各使用单位保证所提供资料的真实、完整、准确、合法、有效。

7.4在本合同有效期内，如甲方上述主体资格、资质证明文件所记载内容出现变更，甲方应在完成变更后尽快向乙方提供最新的文件。

7.5各使用单位使用本合同项下云业务服务从事非经营性互联网信息服务的，须严格遵循《非经营性互联网备案管理办法》等规定。承诺并确认：各使用单位及其最终用户所提交的所有备案信息真实、完整、合法、有效，当提供的备案信息发生变化时应及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，导致服务被行业主管部门关闭，乙方不承担任何责任。

7.6如各使用单位违反在本合同及附件中任一项保证的，包括但不限于在本合同签订时不具备开展业务所需的全部资质许可、履行相关手续，或在本合同有效期内丧失全部或部分资质许可的，如被政府管理部门暂停或关闭服务，使用单位应当承担违约责任，并赔偿乙方的相应损失，乙方不承担任何责任。

7.7各使用单位承诺，不得通过转让、出售、无偿使用或其他任何方式许可甲方之外的任何第三人使用本合同项下云业务服务。否则，乙方有权终止本合同，并追究甲方相应责任。

7.8各使用单位负责其服务的账号和密码的保密和使用安全，如因各使用单位原因导致账号或密码泄露或为他人获取的，各使用单位自行承担损失和责任。各使用单位发现其账号或密码被他人非法使用或有使用异常的情况的，应及时根据乙方公布的处理方式通知乙方，并有权通知乙方采取措施暂停该账号的登录和使用。乙方在收到甲方要求采取措施暂停其账号登录和使用的通知后，应当要求各使用单位提供并核实与其注册身份信息相一致的个人或单位有效身份信息。乙方核实各使用单位所提供的个人或单位有效身份信息与所注册的身份信息相一致的，应当及时采取措施暂停各使用单位账号的登录和使用。各使用单位没有提供其个人或单位有效身份证件或者各使用单位提供的个人或单位有效身份证件与所注册的身份信息不一致的，乙方有权拒绝各使用单位前述请求，由此造成的损失由各使用单位自行承担。

8.甲方的权利和义务

8.1甲方的权利

（1）甲方有权随时向乙方了解项目进度，并要求乙方提供项目相关资料。

（2）甲方有权对项目资金使用情况进行监督、检查，并要求乙方提供相关资料。

（3）甲方有权按照本合同约定或有关法律法规、政府管理的相关职能规定，对本项目进行监督和检查，有权要求乙方按照监督检查情况制定相应措施并加以整改。甲方不因行使该监督和检查权而承担任何责任，也不因此减轻或免除乙方根据本合同约定或相关法律法规规定应承担的任何义务或责任。

（4）甲方有权在乙方履行合同过程中出现损害或可能损害公共利益、公共安全情形时终止本合同。

（5）甲方有权根据国家政策或法律法规的变动对服务项目的需求标准和质量要求作出相应变动或者取消项目。

（6）甲方有权将乙方履行合同情况及不符合相关法律法规的规定情况，向相关部门报告并纳入不良信用记录、年检（报）、评估、执法等监管体系中。

（7）在本合同有效期内，甲方对由乙方分配的IP地址具有使用权，且不可以任何方式转由他人使用。甲方不得私自使用乙方未分配给甲方的IP地址。甲方不再使用本服务时，则相关IP地址使用权由乙方收回。

（8）其他

8.2甲方的义务

（1）甲方应及时向乙方提供与履行本合同相关的所有必须的文件、资料。

（2）甲方应为乙方履行本合同过程中与相关政府部门及其他第三方的沟通、协调提供必要的协助。

（3）甲方应按照合同约定支付服务费用。

（4）甲方使用本合同项下云业务服务的，必须遵守《中华人民共和国电信条例》、《中华人民共和国计算机信息网络国际联网暂行规定》和其他有关法律、法规或相关规定，不得存在任何违法违规行为，不得侵犯乙方以及任何第三方的合法权益。

1、除遵从本合同其他条款及附件要求外，甲方使用本服务所发布、传输或存储的信息内容不得存在以下任一情形，且不得为他人发布、传输或存储该类信息内容提供任何便利（包括但不限于设置URL、链接等）：

1）违反国家规定的政治宣传和/或新闻信息；涉及国家秘密和/或安全的信息。

2）涉及封建迷信、淫秽色情、赌博、暴力、恐怖的信息内容和教唆犯罪的内容。

3）违反国家民族政策和宗教政策的信息内容。

4）博彩有奖、赌博游戏、“私服”、“外挂”等非法互联网出版活动。

5）侮辱或者诽谤他人，侵害他人所有权或知识产权等合法权益。

6）其它有损于社会秩序、社会治安、社会公共道德，违反法律法规强制性规定，或侵害他人合法权益的信息内容。

2、甲方不得有任何危害或可能危害云业务服务相关平台及网络安全和信息安全的行为，包括但不限于：

1）对云业务服务相关平台的功能或者存储、处理、传输的数据和应用程序进行删除或者修改。

2）利用网络及系统从事窃取或者破坏他人信息、损害他人合法权益的活动。

3）故意制作、复制、传播计算机病毒或者以其他方式攻击他人服务。

4）进行钓鱼、黑客、网络诈骗等非法行为，网站或空间中含有或涉嫌散播病毒、木马、恶意代码等，或通过虚拟主机对其他网站、主机进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DOS等。

5）危害电信网络安全和信息安全的其他行为。

3、若甲方存在上述1～2条约定的任一情形的，乙方有权按相关规定暂停或终止提供云业务服务，保存有关记录，并向政府主管部门报告，由此引起的一切后果和责任由甲方负责。同时，乙方有权终止本合同，并不承担任何责任。

（5）本服务使用过程中，对于甲方自行提供并使用的软件，甲方应保证该等软件的合法性和不侵权。如任何第三方主张甲方所使用软件侵犯其所有权或者知识产权等合法权益，甲方应负责解决，并赔偿乙方就此而承担的一切费用和损失。

（6）甲方承担自身服务、业务平台所引起的一切后果。如因甲方使用云业务服务中所涉行为或内容不合法或侵权而导致乙方承担责任或对乙方造成损失的，甲方应负责解决，并赔偿乙方由此遭受的全部损失；同时乙方有权终止本合同。

（7）对于甲方使用云业务服务过程中所涉自身信息和资料、数据（包括但不限于商业机密等）、最终用户及其他相关主体的信息和资料、数据等，甲方负责保密，并自行承担由此产生的一切后果和责任。

（8）其他

9.乙方的权利和义务

9.1乙方的权利

（1）乙方有权按照本合同约定向甲方收取服务费用。

（2）乙方有权自甲方处获得与提供本合同项下服务相关的所有必须的文件、资料。

（3）其他

9.2乙方的义务

（1）乙方应配备具有相应资质、特定经验的工作人员负责项目实施，按照本合同约定的标准、要求和时间完成项目。

（2）乙方不得以任何理由将本合同项下的服务项目转包给第三方承担。

（3）乙方应全面履行本项目实施过程中的相关安全管理职责，因乙方未尽到管理职责发生安全事故的，由乙方承担相应的法律责任。

（4）乙方承诺根据本合同提供的服务及相关的软件和技术资料，均已取得有关知识产权的权利人的合法授权。如发生涉及到专利权、著作权、商标权等争议，乙方负责处理并承担由此引起的全部法律及经济责任。

（5）乙方应接受并配合甲方或甲方组织的对本合同履行情况的监督与检查，对于甲方指出的问题，应及时作出合理解释或予以纠正。

（6）乙方应对项目资金进行规范的财务管理和会计核算，加强自身监督，确保资金规范管理和使用。

（7）乙方应建立健全财务管理与报告制度，按要求向甲方提供资金的使用情况、项目执行情况、成果总结等材料，并配合甲方及甲方组织的监督检查或绩效评价。

（8）乙方应根据甲方要求，无条件接受和配合甲方或甲方委托的会计师事务所进行的与本合同相关的审计。乙方应保存与本合同相关的记录和账目，保存期限为本合同履行完毕或终止后15年。经提前通知，甲方或甲方委托的会计师事务所有权检查并复制上述记录和账目。

（9）项目交付后，乙方应无条件返还甲方向其提供的文件、资料并向甲方移交项目资料，同时乙方应当自留一份完整的项目档案并予以妥善保存。

（10）乙方负责按照本合同约定的条件提供云业务服务及相关的支撑服务。

（11）乙方将消除甲方非人为操作所出现的云计算资源、云存储资源、互联网接入故障，但因甲方原因和/或不可抗力以及非乙方控制范围之内的事项除外。

（12）其他

10. 违约责任

10.1甲方无正当理由拒绝接收服务，到期拒付服务费的，甲方向乙方偿付本合同总服务费1%的违约金。甲方逾期付款的，则每日按逾期金额的0.1‰向乙方偿付违约金。

10.2乙方提供的服务不符合本项目相关文件和本合同规定的，甲方有权拒收，并且乙方须向甲方支付本合同总服务费20%的违约金。

10.3乙方未能按照本合同约定时间提供服务或完成约定的项目服务内容的，从逾期之日起每日按本合同总服务费0.5‰的数额向甲方支付违约金；逾期15日以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

10.4未经甲方同意，乙方不得擅自将本合同服务转包第三方承担。如擅自转包，则乙方应支付给甲方本合同总服务费20%的违约金。

10.5双方应共同遵守本合同条款及相应附件规定，如一方违约给对方造成损失的，违约方应赔偿守约方的损失。

10.6鉴于计算机、互联网的特殊性，下述情况不属于乙方违约：

1）乙方在进行服务器配置、维护时，需要短时间中断服务；

2）由于Internet上的通路阻塞造成甲方网站访问速度下降。

10.7如果因乙方自身及其控制范围内原因造成甲方不能按约定正常使用本服务的，包括云计算资源、云存储资源、互联网接入故障，乙方以小时为单位向甲方赔偿，即连续达1小时不能正常提供服务的，延长一小时的服务期（以此类推）。如果因乙方原因造成甲方连续72小时不能按约定正常使用服务的，甲方有权终止云业务服务，并要求乙方进行赔偿。

10.8无论本合同其他条款是否有相反约定，乙方对因本合同项下违约行为而导致的甲方可得利益损失、商业信誉损失以及数据丢失或损坏等其他损失不承担责任。

10.9其他违约责任按《中华人民共和国民法典》处理。

11. 知识产权归属

12. 保密条款

12.1乙方应遵守国家有关保密的法律法规和行业规定，并对甲方提供的资料负有保密义务。未经甲方同意，不得将承接政府公共服务项目获得的政府、公民个人等各种信息和资料提供给其他单位和个人。如发生以上情况，甲方有权索赔。

12.2甲方有义务保护乙方的知识产权，未经乙方同意，不得将乙方交付的具有知识产权性质的成果文件、资料向第三方转让或用于本合同以外的项目。如发生以上情况，乙方有权索赔，但甲方依据相关法定职责对外公开的除外。

12.3未经对方书面许可，任何一方不得向第三方提供或者披露因本合同的签订和履行而得知的与对方业务有关的资料和信息，法律另有规定或本合同另有约定的除外。乙方向其关联公司提供或披露与甲方业务有关的资料和信息的，不受此限。

12.4保密责任不因本合同的无效、提前终止、解除或不具操作性而失效。

12.5 数据私密性、数据知情权和数据可审查性

（1）乙方承诺各使用单位的数据互相隔离，不可互访。

（2）乙方不会删除各使用单位数据，也不会将各使用单位数据、个人信息等泄露给任何第三方，除非政府监管部门监管审计需要。各使用单位所有数据不会存在国外数据中心或用于国外业务或数据分析。

（3）乙方数据中心遵守国家法律合法建设，遵守中华人民共和国法律。

（4）乙方承诺各使用单位在必要的条件下，由于合规或是安全取证调查等原因，可以提供相关的信息。乙方承诺遵守国家相应的法律法规，配合政府监管部门的监管审查。提供的相关信息包括关键组件运行日志、运维人员操作记录等。

13. 争议的解决

本合同在履行过程中发生的任何争议，如双方不能通过友好协商解决，通过项目所在地有管辖权的人民法院诉讼处理。

14. 不可抗力

14.1 不可抗力是指合同双方不可预见、不可避免、不可克服的自然灾害和社会事件。

14.2 任何一方对由于不可抗力造成的部分或全部不能履行合同不承担违约责任。但迟延履行后发生不可抗力的，不能免除责任。

14.3 遇有不可抗力的一方，应在三日内将事件的情况以书面形式通知另一方，并在事件发生后十日内，向另一方提交合同不能履行或部分不能履行或需要延期履行理由的报告。

14.4如由于战争、骚乱、恐怖主义、自然灾害、国家法律法规或规章变动、网络安全、网络无法覆盖、电力故障、通信线路被人为破坏、黑客攻击、计算机病毒侵入或发作，导致协议双方或一方无法继续履行协议时，受影响方不承担违约责任，但应尽快书面通知对方，并协商适当延长协议的期限。在影响消除后，受影响方应及时通知对方，本合同继续执行。

14.5如政府管理部门提出要求的，乙方将暂停或终止提供相应服务，且不承担任何责任。

15. 服务的变更、中断

15.1乙方因技术进步或国家法律、政策变动等原因可对云业务服务的服务内容、业务功能、操作方法等做出调整，但调整时应按本合同约定提前公告甲方并提供相应解决方案。

15.2如因系统维护或升级的需要而暂停云业务服务的，乙方将尽可能事先以公告方式通知甲方等用户。

15.3乙方依据本合同约定暂停向甲方提供本合同项下云业务服务的，应当通知甲方并告知暂停期间，暂停期间届满乙方应当及时恢复对甲方的服务。其中，非乙方原因造成的服务暂停，暂停期间甲方仍需正常付费。

15.4除法定或双方另行约定外，自本合同期满或因任何原因导致本合同提前终止之日起的7日内（注：云存储服务为30日内），乙方应继续存储甲方数据。逾期乙方将不再保留甲方数据，甲方需自行承担其数据被销毁后引发的一切后果。

16. 合同的终止

16.1本合同期满，双方未续签合同的；

16.2乙方服务能力丧失，致使本合同服务无法正常提供的；

16.3在履行合同过程中，发现乙方已不符合承接主体应具备的条件，造成合同无法履行的；

16.4受国家政策或法律法规变动影响，经双方协商终止本合同的。

17. 税费发生与履行

本合同有关的一切税费均由乙方负担。

18. 其他

18.1本合同所有附件及相关购买文件均为本合同的有效组成部分，与本合同具有同等法律效力。若合同附件与本合同存在不一致的，则以本合同为准。

18.2在履行本合同过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

18.3如一方地址、电话、传真号码及乙方银行账户信息有变更，应在变更当日书面通知对方，否则，应承担相应责任。

19. 补充条款：

20. 合同生效

20.1本合同订立时间： 年 月 日

20.2本合同订立地点：

20.3本合同在甲、乙双方法人代表或其授权代表签章之日起生效。

20.4本合同一式陆份，具有同等法律效力，甲乙双方各执贰份，洞头区政务服务中心执壹份，温州华晟招标代理有限公司执壹份。

21. 合同附件（若有附件应注明附件名称）

下列文件与本合同具有同等法律效力：

1、甲方的磋商文件与招标补充文件；

2、乙方的响应文件；

3、询标纪要和承诺书；

4、成交通知书。

采购人（盖章）： 　 成交供应商（盖章）：

法定代表人（盖章或签字）： 法定代表人（盖章或签字）：

委托代理人（签字）： 委托代理人（签字）：

地址： 地址：

电话： 电话：

传真： 传真：

日期： 年 月 日 日期： 年 月 日

第六部分 附件--磋商响应文件格式

1. 资格文件格式

附件一

投标供应商参与政府采购活动投标资格声明函

|  |  |
| --- | --- |
| 项目名称 |  |
| 招标编号 |  |
| 时 间 | 磋商响应截止时间前 |
| 我单位参与本项目投标，现声明如下：  1、我单位符合政府采购法第二十二条规定。  2、根据财政部单独或与有关部门联合签署了《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库【2016】125号）、《关于对重大税收违法案件当事人实施联合惩戒措施的合作备忘录》(发改财金〔2014〕3062号)、《失信企业协同监管和联合惩戒合作备忘录》(发改财金〔2015〕2045号)、《关于对违法失信上市公司相关责任主体实施联合惩戒的合作备忘录》(发改财金〔2015〕3062号)、《关于对失信被执行人实施联合惩戒的合作备忘录》(发改财金〔2016〕141号)、《关于对安全生产领域失信生产经营单位及其有关人员开展联合惩戒的合作备忘录》(发改财金〔2016〕1001号)，依法限制相关失信主体参与政府采购活动。我单位**□**存在/**□**不存在上述文件规定依法限制参与政府采购的情况。（说明：在**□**上打**√**。）  3、我单位**□**没有被限制参加政府采购活动/**□**在参加政府采购活动前3年内因违法经营被禁止在一定期限内参加政府采购活动，但期限届满，已可以参加政府采购活动。（说明：在**□**上打**√**。）  4、我单位参与本项目政府采购活动3年内其它重大违法记录（重大违法记录，是指投标供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）情况声明：  5、我单位、法定代表人及授权代表近3年行贿犯罪记录情况声明：    6、我单位符合本项目特定资格条件： 的要求，并在响应文件中提供了相应的证明材料（磋商文件没有要求特定资格条件的，本条款空格处可以空白）  7、我单位与参加本次项目同一合同项下政府采购活动的其他供应商不存在单位负责人为同一人或者直接控股、管理关系。  8、本公司所提交的声明和陈述均是真实的、准确的。若与真实情况不符，本公司愿意承担由此而产生的一切后果。 | |
| 投标供应商（盖章）： | |
| 法定代表人或授权代表（签字或盖章）： | |
| 签署日期： | |

二、报价文件格式

附件二

开标一览表（标项一）

供应商名称： 采购编号：

|  |  |
| --- | --- |
| 标项名称 | 投标报价（最高限价的统一折扣率） |
| 洞头区政务云（公有云） | % |

▲投标报价为最高限价的统一折扣率，以百分数表示。采购人将根据公式：“最高限价×投标报价（最高限价的统一折扣率）=支付金额”核算实际支付金额。如：某产品最高限价为100元，投标报价：­­最高限价的统一折扣率为80%，则采购人实际支付金额为：最高限价100元×投标报价（最高限价的统一折扣率）80%=80（元）。以投标供应商所投最高限价的“统一折扣率”进行价格分计算。

▲投标报价（最高限价的统一折扣率）不得超过100%，否则按无效投标处理。

▲不提供此表格的将视为没有实质性响应磋商文件。

供应商全称（盖章）：

法定代表人或授权代表（签字或盖章）：

日期：

开标一览表（标项二）

供应商名称： 采购编号：

|  |  |
| --- | --- |
| 标项名称 | 投标报价（最高限价的统一折扣率） |
| 洞头区政务云（私有云） | % |

▲投标报价为最高限价的统一折扣率，以百分数表示。采购人将根据公式：“最高限价×投标报价（最高限价的统一折扣率）=支付金额”核算实际支付金额。如：某产品最高限价为100元，投标报价：­­最高限价的统一折扣率为80%，则采购人实际支付金额为：最高限价100元×投标报价（最高限价的统一折扣率）80%=80（元）。以投标供应商所投最高限价的“统一折扣率”进行价格分计算。

▲投标报价（最高限价的统一折扣率）不得超过100%，否则按无效投标处理。

▲不提供此表格的将视为没有实质性响应磋商文件。

供应商全称（盖章）：

法定代表人或授权代表（签字或盖章）：

日期：

三、商务技术文件格式

附件三

投 标 函

温州市洞头区大数据管理中心

温州华晟招标代理有限公司：

（投标供应商全称）授权 （授权代表名称） （职务、职称）为授权代表，参加贵方组织的 （招标项目名称）（括号内填招标编号）标项 招标的有关活动，并对此进行投标。为此：

1、提供磋商文件要求的全部磋商响应文件。

2、保证遵守磋商文件中的有关规定和约定。

3、保证忠实地执行双方所签的合同，并承担合同规定的责任义务。

4、我方对服务期承诺如下：▲**按采购人要求提供服务。**

5、我方已详细审查全部磋商文件，包括磋商文件补充文件（如果有的话）。我方完全理解并同意放弃对这方面有不明及误解的权力。如果磋商文件有相互矛盾之处，我方同意按采购人的理解处理。

6、愿意向贵方提供任何与该项投标有关的数据、情况和技术资料，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。

7、利益冲突：近三年内直至目前，我公司与本项目的采购人、采购代理机构没有任何的隶属关系。

8、我公司没有被财政部门限制参加政府采购活动或曾被财政部门限制参加政府采购活动但已不在限制期内。

9、磋商响应文件自提交响应文件递交截止时间起90天内有效。

10、与本采购有关的一切往来通讯请寄：

地址：

邮编： 电话： 传真：

投标供应商（盖章）：

法定代表人或授权代表（签字或盖章）：

日期：

附件四

法定代表人授权书

温州市洞头区大数据管理中心

温州华晟招标代理有限公司：

本授权委托书声明：我 （法定代表人姓名） 系 （供 应 商 名 称） 的法定代表人，现授权委托 （单 位 名 称） 的 （授权代表姓名） 为我公司法定代表人授权代表，参加贵处组织的 （招标项目名称，括号中填写项目编号） 项目标项 投标，全权处理本次招投标活动中的一切事宜，我承认授权代表全权代表我所签署的本项目的磋商响应文件的内容。

授权代表无转授权，特此授权。

授权代表： 性别 ： 年龄：

详细通讯地址： 邮政编码：

电话： 传真：

投标供应商： （盖章）

法定代表人： （签字或盖章）

授权委托日期： 年 月 日

|  |
| --- |
| 粘贴法人授权代表身份证复印影印件 |

|  |
| --- |
| 粘贴法人身份证复印影印件 |

附件五

法定代表人诚信投标承诺书

本人以企业法定代表人的身份郑重承诺：

将遵循公开、公平、公正和诚信信用的原则参加 项目（采购编号： ）标项 的投标；

一、杜绝以收取管理费等形式的一切挂靠、违法转包、分包行为；并选派有丰富经验、无不良行为记录的项目管理人员、技术人员，严格按磋商文件、磋商响应文件及合同等要求保证拟派人员的到岗率。

二、磋商响应文件所提供的一切材料都是真实、有效、合法的。

三、不与其他投标供应商相互串通投标报价，不排挤其他投标供应商的公平竞争，不损害采购人或其他投标供应商的合法权益。

四、不与采购人或采购代理机构串通投标，不损害国家利益，社会公共利益或其他人的合法权益。

五、不向采购人或者评标委员会成员行贿以牟取中标。

六、不以其他人名义投标或者以其他方式弄虚作假，骗取中标。

七、不在开标后进行虚假恶意投诉。

八、我单位没有被政府机关列入失信被执行人名单、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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的情形（《中华人民共和国政府采购法实施条例》第十九条规定的情形除外）。

本公司若有违反本承诺内容的行为，愿意承担法律责任，包括不限于：愿意接受相关行政主管部门作出的处罚；给采购人造成损失的，依法承担相应的赔偿责任。

投标供应商（盖章）

法定代表人（签字或盖章）：

承诺书签署日期：

附件六

投标供应商业绩（分标项提供）

（具体要求见评分细则，如有则提供）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 采购单位 | 项目名称 | 合同金额 | 签约日期 | 联系人 | 联系电话 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

注：1、表格可以延续。

供应商盖章：

附件七

（一）商务偏离表（分标项提供）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序 号 | 内容 | 磋商文件要求 | 响应文件响应情况 | 备 注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

供应商盖章：

（二）技术偏离表（分标项提供）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序 号 | 内容 | 磋商文件要求 | 响应文件响应情况 | 备 注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

供应商盖章：

说明：

1.如不填写，则视为完全响应磋商文件。

2.如出现偏离，投标供应商务必如实填写此表，否则存在的风险由投标供应商自行承担。

3.▲不提供此表的磋商响应文件将被视为未实质性响应磋商文件，其按无效投标处理。

4.表格可以延续。

附件八

项目服务人员汇总表（分标项提供）

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 本项目主要工作岗位 | 年龄 | 性别 | 职务 | 专业/  年限 | 职称/资格/认证 | 到现场服务起止时间 | 类似服务的经历 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

附注：1. 项目负责人、技术负责人(技术总监)、安全负责人（安全总监）以及各主要专业工种均应列入；

2. 列入本表人员如要更换，需经采购人同意，擅自更换或不到位属违约行为；

3. 职称/资格证书/认证证书、社保证明扫描件附后。

供应商全称（公章）：

日期：

附件九

拟派项目人员情况表（分标项提供）

|  |  |  |
| --- | --- | --- |
| 姓名 |  | 近年来主要工作业绩 |
| 性别 |  | 注：业绩证明应提供旁证材料  （合同及业主佐证材料） |
| 年龄 |  |
| 职称/资格证书 |  |
| 毕业时间 |  |
| 学校专业 |  |
| 联系电话 |  |
| 最近一年工作状况 |  |
| 拟在本项目中担任主要工作 |  | |

附注：1.以上人员包括项目负责人、技术负责人(技术总监)、安全负责人（安全总监）；

2.后附学历、职称/资格证书/认证证书，业绩证明旁证材料（加盖公章）。

供应商全称（公章）：

日期：

第七部分 确定成交供应商办法

根据《中华人民共和国政府采购法》等有关政府采购法规，结合本次所要采购项目的实际，按照公平、公正、科学、择优的原则选择成交单位，特制定本评审办法。

一、总则

评审工作遵循公平、公正、民主、科学的原则和诚实、信誉、效率的服务原则。本着科学、严谨的态度，认真进行评审。择优选定提供服务单位，确保服务质量、服务期(完工期)，节约投资，最大限度的保护当事人权益，严格按照竞争性磋商文件的商务、技术要求，对磋商响应文件进行综合评定，提出优选方案，编写评审报告。磋商小组必须严格遵守保密规定，不得泄漏评审的有关情况，不得索贿受贿，不得接受吃请和礼品，不得参加影响公正评审的有关活动。对未成交单位，磋商小组不作任何解释。供应商不得以任何方式干扰采购工作的进行，一经发现其磋商响应文件将被拒绝。

二、评审组织

评审工作由采购人依法组建的磋商小组负责，磋商小组由采购人代表以及评审专家库中随机抽取的有关技术、经济专家共同组成。评审全过程由采购管理部门全程监督。

三、开标程序

具体开标流程见本磋商文件第三部分相关内容描述。

四、评分细则（按标项评审）

**一、报价评分 20分**

**以供应商有效投标价中的最低价为评标基准价，得满分20分。商务报价评分结算公式为:投标报价得分=(评标基准价／投标报价)×20%×100。**

**本项目对符合磋商文件规定条件的小、微企业（或监狱企业或残疾人福利性单位）所投的价格给予10%的扣除，用扣除后的价格参与评审，如中标签订合同时以其投标价作为签订合同价。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。供应商企业属于以上多种性质的，不重复享受扶持政策。**

**二、商务技术综合评分80分**

**1、适用于标项一**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分项目 | 评分细则 | 分值 | 评分标准 |
| 1 | 投标供应商综合实力 | 综合实力 | 3分 | ①具有质量管理体系认证证书的得1分  ②具有环境管理体系认证证书的得1分  ③具有职业健康安全管理体系认证证书的得1分  备注：若分公司参与投标，总公司具有该证书均认可，相关证书需在有效期内。 |
| 2 | 云平台技术方案 | 云平台建设能力 | 3分 | 根据投标供应商提供的政务云平台在国内建设的知名度、成熟度和应用案例由评委打分，0-3分。 |
| 云平台系统架构方案 | 5分 | 根据响应文件中对政务云平台总体设计思路和技术架构的合理性、先进性打分。  应答详尽、明晰，内容完整齐全、表述准确、条理清晰，内容无前后矛盾，符合磋商文件要求，分析本项目的特点针对性强，服务响应时间及时的3-5分；  应答基本详尽、基本明晰，内容基本齐全、表述基本准确、条理基本清晰，内容前后矛盾较少，基本符合磋商文件要求，分析本项目的特点针对性一般，服务响应时间拖沓的1-3分；  应答不详尽、不明晰，内容不齐全、表述不准确、条理不清晰，内容有明显前后矛盾，不符合磋商文件要求，分析本项目的特点针对性差，服务响应时间不满意的0-1分。 |
| 技术指标需求响应程度 | 20分 | 根据响应文件对所列云平台技术需求和技术指标的符合程度评分。  1.标有“▲”且加下划线必须满足，负偏离按无效投标处理；  2.投标产品的技术参数“★”的，每负偏离1项扣2分，  扣完为止，由评委共同认定。 |
| 机房要求 | 9分 | 1.获得平台等保三级（含）以上安全等级保护要求。提供证书扫描件得3分，不满足不得分。  2.获得信息安全管理体系认证证书，认证范围必须包含云计算服务，提供证书扫描件得3分，不满足不得分。  3.提供信息技术服务管理体系认证证书得3分，不满足不得分。  备注：若分公司参与投标，授权函有相关内容授权则总公司具有该证书均认可，相关证书需在有效期内。 |
| 平台带宽与链路 | 6分 | 1.提供的政务云平台与市本级以及12个区县政务外网的专用互联光纤带宽不小于1G，以满足网络互访的要求。（满足得4分，部分满足得2分，不满足不得分）。  2.提供的政务云平台和互联网独享出口总带宽不少于2G，可扩充到20G。（满足得2分，不满足不得分）。 |
| 3 | 云平台安全方案 | 整体方案 | 5分 | 根据投标供应商提供完整技术方案，包含组网方案、维保方案，以及所提供方案的合理性、科学性和服务能力及条件综合评定打分。  应答详尽、明晰，内容完整齐全、表述准确、条理清晰，内容无前后矛盾，符合磋商文件要求，分析本项目的特点针对性强，服务响应时间及时的3-5分；  应答基本详尽、基本明晰，内容基本齐全、表述基本准确、条理基本清晰，内容前后矛盾较少，基本符合磋商文件要求，分析本项目的特点针对性一般，服务响应时间拖沓的1-3分；  应答不详尽、不明晰，内容不齐全、表述不准确、条理不清晰，内容有明显前后矛盾，不符合磋商文件要求，分析本项目的特点针对性差，服务响应时间不满意的0-1分。 |
| 云安全服务参数符合程度 | 10分 | 对投标供应商提供的云安全服务参数是否满足磋商文件要求评分。  1.标有“▲”且加下划线必须满足，负偏离按无效投标处理；  2.投标产品的技术参数“★”的，每负偏离1项扣1分，扣完为止，由评委共同认定。 |
| 4 | 云服务供应商服务能力 | 技术服务能力 | 4分 | 1.投标供应商提供的服务方案：  应答详尽、明晰，内容完整齐全、表述准确、条理清晰，内容无前后矛盾，符合磋商文件要求，分析本项目的特点针对性强，服务响应时间及时的1.5-2分；  应答基本详尽、基本明晰，内容基本齐全、表述基本准确、条理基本清晰，内容前后矛盾较少，基本符合磋商文件要求，分析本项目的特点针对性一般，服务响应时间拖沓的1-1.5分；  应答不详尽、不明晰，内容不齐全、表述不准确、条理不清晰，内容有明显前后矛盾，不符合磋商文件要求，分析本项目的特点针对性差，服务响应时间不满意的0-1分。  2.投标供应商本地化技术服务团队在云服务运营方面的实践经验：  应答详尽、明晰，内容完整齐全、表述准确、条理清晰，内容无前后矛盾，符合磋商文件要求，分析本项目的特点针对性强，团队技术强大的1.5-2分；  应答基本详尽、基本明晰，内容基本齐全、表述基本准确、条理基本清晰，内容前后矛盾较少，基本符合磋商文件要求，分析本项目的特点针对性一般，团队技术普通的1-1.5分；  应答不详尽、不明晰，内容不齐全、表述不准确、条理不清晰，内容有明显前后矛盾，不符合磋商文件要求，分析本项目的特点针对性差，服务团队不满意的0-1分。 |
| 13分 | 3.投标供应商技术服务团队组成人员在网络、数据库、信息安全领域的专业能力。 1）项目负责人（一名）同时具有信息系统项目管理师、数据库系统工程师得3分，具备一个得1分，没有不得分；  2）技术总监（一名）同时具有系统分析师、信息系统监理师得3分，具备一个得1分，没有不得分；  3）安全总监（一名）同时具有网络规划设计师、信息安全工程师得3分，具备一个得1分，没有不得分；  4）服务团队中（除项目负责人、技术总监、安全总监外）有成员持有系统集成项目管理工程师、网络工程师、软件设计师、数据库系统工程师，每提供一个得1分，满分4分。  以上人员须提供相关证书扫描件和在投标单位近三个月中任意一个月的社保证明，两者缺一不可，否则不予给分。 |
| 5 | 投标供应商业绩 | | 2分 | 投标供应商2021年1月1日以来同类项目业绩（每个得1分，最多得2分，提供合同扫描件，否则不得分）。 |

**2、适用于标项二**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评审项目** | **分值** | **评分标准** |
| 1 | 投标供应商综合实力 | 10分 | 1.具有质量管理体系认证证书的得2分；  2.具有环境管理体系认证证书的得2分；  3.具有职业健康安全管理体系认证证书（认证范围必须包含云计算服务）的得2分；  4.具有信息安全管理体系认证有效证书（认证范围必须包含云计算服务）的得2分；  5.具有信息技术服务管理体系认证证书得 2分。  备注：若分公司参与投标，总公司具有该证书均认可，相关证书需在有效期内。 |
| 2 | 投标供应商业绩 | 2分 | 投标供应商2021年1月1日以来同类项目业绩（每个得1分，最多得2分，提供合同扫描件，否则不得分）。 |
| 3 | 投标供应商的云平台资质 | 6分 | 1、投标供应商自有的云平台等级测评报告中安全保护等级为第三级及以上，满足要求得3分。（提供有效期内的相关证书扫描件加盖公章，否则不得分）。  2、投标供应商具有云管理服务评估证书（卓越级）的得3分，其他不得分。（若分公司参与投标，总公司具有该证书均认可，相关证书需在有效期内）。 |
| 4 | 云平台技术方案 | 9分 | 云平台整体方案设计：考察投标供应商对于本项目的理解是否全面，包括政务云平台总体设计思路、技术架构，以及云平台安全保障体系技术方案的可靠性、全面性、可行性。 |
| 1、政务云平台总体设计思路：  ①描述全面、可行、可靠，得2-3分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。  2、政务云平台总体技术架构：  ①描述全面、可行、可靠，得2-3分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。  3、云平台安全保障体系技术方案：  ①描述全面、可行、可靠，得2-3分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。 |
| 22分 | 根据磋商文件中云基础服务、云平台服务、云安全服务、云基础设施服务、云管系统技术参数的满足程度评分：  1.标有“▲”且加下划线必须满足，负偏离按无效投标处理；  2.投标产品的技术参数“★”的，每负偏离1项扣2分，扣完为止，由评委共同认定。 |
| 5 | 云平台安全方案 | 4分 | 根据投标供应商提供完整技术方案，包含组网方案、维保方案，以及所提供方案的合理性、科学性和服务能力及条件综合评定打分：  ①描述全面、可行、可靠，得2-4分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。 |
| 6 | 机房要求 | 4分 | 机房环境及相关物理硬件是否满足磋商文件相关技术指标要求，须提供相关证明材料：  ①描述全面、可行、可靠，得2-4分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。 |
| 7 | 服务人员要求 | 14分 | 1、投标人服务于此次项目的项目负责人（一名）具备高级信息系统项目管理师（软考）证书、一级建造师（通信与广电工程）证书、高级软件开发工程师证书的，全部具备得4分，具备一个证书得1分； 2、投标人服务于此次项目的技术负责人（一名）具备高级系统规划与管理师（软考）证书、高级软件设计师证书、信息技术应用创新专业人员证书的，全部具备得4分，具备一个证书得1分； 3、投标人服务于此次项目的安全负责人（一名）具备中级及以上网络工程师（软考）、信息安全管理（高级）证书、中级及以上信息安全工程师（软考）证书，全部具备得4分，具备一个证书得1分； 4、投标人服务于此次项目的项目组成员中有具备安全评价师证书得1分；具备信息技术应用创新专业人员证书得1分。同一个人具有多种证书的，按一种证书来计算。 (注：①以上项目负责人、技术负责人，安全负责人，不得兼任。 ②以上人员证书须提供相关证明材料（签发/颁证机构为人力资源和社会保障部（厅、局）或工业和信息化部（厅、局、教育与考试中心、电子工业标准化研究院）扫描件加盖公章，否则不得分。 ③以上人员须提供在投标单位近三个月中任意一个月的社保证明，否则不予给分。 |
| 8 | 技术服务方案 | 9分 | 根据详细的运维服务方案、运维服务报告的详细程度、服务响应时间等打分，最高得9分。  1、运维服务方案：  ①描述全面、可行、可靠，得2-3分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。  2、运维服务报告的详细程度：  ①描述全面、可行、可靠，得2-3分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。  3、服务响应时间：  ①描述全面、可行、可靠，得2-3分；  ②描述基本全面、合理，得1-2分；  ③描述简单或存在缺漏的，得0-1分；  ④无描述不得分。 |

三、说明

1、各标项每个有效投标供应商的综合得分=商务技术得分（所有磋商小组成员打分的算术平均值）＋报价得分。

2、磋商小组推荐各标项综合得分最高的供应商为成交供应商（如果得分相同则按最终磋商报价从低到高顺序依次推荐为成交候选供应商；如果综合得分相同最终磋商报价也相同，则抽签决定），并编写评审报告。

3、所有分值计算保留小数点后二位，小数点后第三位起四舍五入。

其它参见本磋商文件第三部分：“供应商须知” 中的相关内容，未尽事宜按有关法律规定处理。