**一、项目整体采购需求**

* 1. **项目名称**

2021年政务云租用服务项目

* 1. **项目概述**

党中央、国务院高度重视电子政务发展，目前政务云已成为国家实施网络强国战略、国家大数据战略、“互联网+”行动计划的重要支撑。

乐山市政务云（一期）已经建成，目前已经承载了多个部门业务系统，集约化建设取得一定成效。但是随着全市数字政府的深入发展，上云业务应用不断增多，现有政务云资源分配使用率不断攀升，已无法满足各部门对计算能力、存储能力的需求，急需扩充云资源以满足各部门的需要。

为更好的提升云服务商服务水平，本次拟采购3家政务云服务商作为我市政务云服务商，为我市各部门提供更优质实惠的云服务，满足各部门的个性化需求，建立支撑乐山市各政府部门非涉密电子政务系统运行使用的政务云平台，逐步实现各部门在互联网、政务外网、非涉密业务专网上运行的应用迁移；构建稳定可靠的云安全体系和政务数据灾备体系；完善云计算数据中心公共服务支撑能力；强化数据资源分析处理能力，推动跨部门信息共享和业务协同。

* 1. **项目采购服务内容**

1、基础设施资源服务：包括计算资源服务、存储资源服务、网络资源服务和机房资源服务。

2、支撑软件资源服务：提供相应的应用支撑软件服务需求。

3、信息安全技术服务：按照国家信息安全等级保护三级要求建立政务云平台和租户层的安全服务。

4、应用迁移服务：配合提供业务迁移服务包括迁移设计服务、数据迁移服务、业务系统迁移服务。

5、服务的实施：包括基础设施服务实施、支撑软件服务实施、信息安全服务实施、运行保障服务实施。

6、运行保障服务：提供政务云平台的资源监测、资源配置、资源优化、服务监控、事件处理、运维流程、日常巡检、灾备管理、应急预案管理、服务质量监督和报告等服务。

7、提供健全配套制度标准，可提供政务云管理办法、运维制度、应急预案等。

8、提供的政务云平台应具有兼容性，应用软件在政务云平台之间可实现跨平台的兼容部署和调度能力。

* 1. **项目总体技术要求**
		1. **系统架构**

乐山市政务云系统总体架构，由1个云服务门户、N个云服务提供商、N个云应用服务商组成，简称“1+N+N”模式。如下图所示：



为方便采购人行使监管职能及各部门使用，采购人将构建连接多个云服务商的统一的安全监管平台，实现云平台资源使用情况的实时监控。

云平台总体架构分为基础设施资源服务、应用支撑服务、信息安全保障体系、运维保障服务体系以及安全可靠云管理系统。如下图所示：



（1）基础设施平台

基础设施服务层包含国产化服务器、存储、网络等设备，提供可扩展的计算、存储和网络安全服务，支撑业务快速部署，主要提供云主机、块存储、VPC、云备份服务等。

（2）应用支撑平台

应用支撑服务层按需提供公共软件服务，包括但不限于国产化操作系统、数据库、中间件、微服务等服务。

（3）信息安全保障体系

基于国产化软硬件产品，建设安全、合规的信息安全保障体系，主要包括：安全计算环境、安全网络环境、安全管理以及安全服务等。

（4）运维保障服务体系

为保障乐山市政务云服务的稳定高效运行，除了信息安全保障体系之外还需要一个良好的运维体系，提供资源管理、调度管理、监控管理等运维功能，实现全市安全可靠统一的资源运维监控管理。

（5）安全可靠云管理系统

基于安全可靠云建设云管理系统，实现统一运营与统一运维，用户可通过自助门户实现资源申请、发放以及资源管理等，通过运维门户实现资源监控，故障处理等。

* + 1. **总体技术要求**

以下各条为基本要求，供应商可进行优化，具体投标方案中的功能、性能可优于本方案；应答说明中标“★”的项为实质性要求部分，必须满足。

（1）▲云服务商必须**承诺提供**的主机房位于乐山市范围内的确定位置，至少具备两大运营商网络直接接入能力。

（2）云服务商必须**承诺提供**异地灾备机房环境，为关键业务提供异地灾备服务。

（3）▲云服务商提供的云管理平台软件应为国产。（提供云平台厂商对投标供应商的云平台使用授权证明，并加盖投标供应商公章）。

（4）本次建设所提供的软硬件设备不能有授权及用户数的限制，影响未来扩展。

* 1. **具体技术要求**

云服务商必须**承诺**未来提供的云资源软硬件设备在功能和性能上均相当于或者优于本次投标产品。所有云资源软件系统必须为稳定可靠版本。若云服务商提供的设备不满足以上条件，采购人有权责令云服务商进行整改，如云服务商拒绝整改，采购人有权取消合同，由此造成的一切责任和后果由云服务商承担。

政务云平台必须采用私有云模式搭建。

**注：参数和服务要求有明确要求提供证明材料的须按要求提供，无明确要求的可以直接响应。**

**标注“★”的条款为本项目的实质性条款，供应商须全部满足，不响应或不满足作无效响应处理。**

**二、第1包：通用政务云服务采购项目**

**A.采购内容**

**（一）政务云平台服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目名称 | 服务内容 | 数量 |
| 1 | 云服务基础支撑 |
| 1.1 | 机房环境 | （机房环境技术服务具体内容要求详见“包1政务云平台服务技术要求”中“1.1.机房环境”） | 1项 |
| 1.2 | 传输链路 | （传输链路技术服务具体内容详见“包1政务云平台服务技术要求”中“1.2.传输链路”） | 1项 |
| 1.3 | 计算资源池 | （计算资源池技术服务具体内容详见“包1政务云平台服务技术要求”中“1.3.计算资源池”）或相当于同等或更优算力的其它计算资源解决方案 | 1项 |
| 1.4 | 存储资源池 | （存储资源池技术服务具体内容详见“包1政务云平台服务技术要求”中“1.4.存储资源池”）或相当于同等或更优算力的其它计算资源解决方案 | 1套 |
| 1.5 | 网络资源池 | （网络资源池技术服务具体内容详见“包1政务云平台服务技术要求”中“1.5.网络资源池”）或相当于同等或更优算力的其它计算资源解决方案 | 1项 |
| 2 | 云平台 |
| 2.1 | 云管理平台 | （云管理平台技术服务具体内容详见“包1政务云平台服务技术要求”中“2.1.云管理平台”） | 1项 |
| 2.2 | 容灾备份系统 | （容灾备份技术服务具体内容详见“包1政务云平台服务技术要求”中“2.2.容灾备份系统”）或相当于同等或更优算力的其它计算资源解决方案 | 1项 |
| 2.3 | 主机托管 | （主机托管技术服务具体内容详见“包1政务云平台服务技术要求”中“2.3.主机托管”） | 1套 |
| 3 | 安全等保要求 |  |
| 3.1 | 边界保护能力要求 | （边界保护技术服务具体内容详见“包1政务云平台服务技术要求”中“3.1.边界保护能力要求”） | 1项 |
| 3.2 | 链路保护能力要求 | （链路保护技术服务具体内容详见“包1政务云平台服务技术要求”中“3.2.链路保护能力要求”） | 1项 |
| 3.3 | 威胁检测能力要求 | （威胁检测技术服务具体内容详见“包1政务云平台服务技术要求”中“3.3.威胁检测能力要求”） | 1项 |
| 3.4 | 安全审计能力要求 | （安全审计技术服务具体内容详见“包1政务云平台服务技术要求”中“3.4.安全审计能力要求”） | 1项 |
| 3.5 | 安全管理能力要求 | （安全管理技术服务具体内容详见“包1政务云平台服务技术要求”中“3.5.安全管理能力要求”） | 1项 |

**（二）政务云平台服务技术要求**

**标注“★”的条款为本项目的实质性条款，供应商须全部满足，不响应或不满足作无效响应处理。**

**1.云服务基础支撑**

**1.1.机房环境**

▲（1）云服务商平台机房在乐山市范围内，具备独立的政务云服务器、存储设备空间，**提供**机房产权证明或长期租赁协议。

▲（2）云服务商提供的机房面积不得低于300㎡，并具备后期扩展能力。

▲（3）云服务商**提供**的机房应不少于25个42U标准服务器机柜的空间，每机柜提供不间断供电，机房空间和供电在满足本期建设规模基础上，具备适应业务发展的扩展能力。

▲（4）云服务商需**提供**机房同地点处不少于150平方米的办公场地和会议场所，满足日常运维值班，设备安装调试，后期业务系统迁移等工作需要。

▲（5）云服务商**提供**的机房应具独立的机房监控中心，并配置不少5㎡的运维监控大屏。

▲（6）提供较高性能的安防、环境监控、灭火系统等基础设施服务，机房抗震烈度达7度或以上，备火灾自动报警及管道式气体灭火系统。

▲（7）机房具备动力环境自动监控的能力，能实现对机房供配电、UPS、精密空调、漏水监测、机房温湿度的监测和预警能力。

（8）机柜区域配备专用门禁和24小时监控系统，视频监控画面可远程调用，监控录像保存时间不小于**3**个月。

▲（9）云服务商**提供**的机房应具备双路市电接入并配备独立变压器，为保障电力稳定持续供应应同时配备双路柴油发电机和双路UPS备用电池。

▲（10）云服务商必须保证机房可持续获得电力供应，每年持续电力供应时间在99.99%以上，以确保电子政务应用系统可持续工作，满足采购人对于政务信息化工作的高要求。

▲（11）机房内应具备冗余、高效的下送风精密空调系统，保障机房温湿度环境。

▲（12）机房需获得等保三级测评，**提供证明**。

▲（13）以上要求为机房服务的基本要求，应按照GB50174-2017《数据中心设计规范》B级以上标准进行建设，满足安全可靠、节能环保、扩展灵活等建设原则，应保证**提供**不间断的云服务，可用性应在99.99%以上。

**1.2.传输链路**

▲（1）具备独立的运营商线路接入机房。

▲（2）具备至少3家运营商接入机房内的出口互联网链路，可**提供**运营商传输设备的不间断供电服务，链路带宽不低于200M。

▲（3）具备至少 2 家运营商接入机房内的出口电子政务外网链路，可**提供** 运营商传输设备的不间断供电服务，主链路带宽不低于 1G、备链路带宽不低于500M。

**1.3.计算资源池**

1.3.1.基本要求

（1）云服务商须**承诺**未来**提供**的硬件设备，在功能和性能上必须相当于或者优于本次投标产品的配置要求；云服务商平台应至少划分为互联网业务区和非互联网业务区，两个区域之间应进行隔离防护；互联网业务区和非互联网业务区内部计算资源池统一为高性能计算区。

（2）资源负载率应保持在85%以下。

（3）高性能计算区，用4路14核或以上配置；

（4）计算节点和存储节点必须与交换设备实现双连接接入。

1.3.2.设备技术要求

（1）高性能计算节点

| 用途：高性能计算（承载高性能计算节点） |
| --- |
| 指标项 | 指标要求（除特别说明外，以下为单台设备的参考配置要求） |
| 服务器密度 | 每机箱≥16半宽或半高服务器节点，或者≥8台全宽或全高服务器节点； |
| 散热模块 | 机箱可支持≥10个热插拔冗余风扇；本次风扇满配； |
| 电源模块 | 每机箱配置≥6个热插拔电源模块，支持N+1, N+N等多种冗余方式，电源模块需采用高能效设计，电源额定功率≥2000W； |
| I/O插槽 | 提供≥4个I/O模块插槽，支持GE交换、10GE交换、40GE、FC交换、FCoE交换，交换模块已成熟商用； |
| 以太网交换机模块 | 配置2个10Gb以太网交换机模块，单台交换模块≥16个10Gb对外上联端口，本次配置≥8个10Gb多模光模块及光纤跳线；  |
| FC交换模块 | 配置2个8GB FC交换模块，单台交换模块≥8个8GB FC对外上联端口，本次配置≥16个8GB FC光模块及光纤跳线； |
| 机箱管理模块 | 内置2个机箱管理模块，提供远程仿真图形界面管理，支持远程状态监控，故障告警，电源能耗控制，微码更新，机箱与计算节点批量初始化配置，网络与交换机管理，资产管理等功能； |

（2）高性能计算节点

| 用途：高性能计算刀片服务器（虚拟化计算资源池） |
| --- |
| 指标项 | 指标要求（除特别说明外，以下为单台设备的参考配置要求） |
| CPU | 配置不低于2.2GHz/14-core处理器； |
| 内存配置数量 | ≥512GB DDR4 内存； |
| 硬盘 | 至少2\*600GB 10K RPM SAS硬盘、支持断电保护； |
| RAID卡 | 支持RAID0/1； |
| HBA卡 | 配置2\*8G FC HBA扣卡和2\*10GE端口扩展卡； |
| 兼容性 | 必须和高性能计算节点兼容； |

**1.4.存储资源池**

1.4.1.基本要求

（1）云服务商须**承诺**未来提供的硬件设备，在功能和性能上必须相当于或者优于本次投标产品的配置要求；

（2）存储池的设计为FC-SAN或分布式存储。

（3）FC-SAN存储：设计为高端集中式存储池，用来承载对IOPS要求较高的业务数据。

（4）FC-SAN为了实现数据的集中存储、以及充分利用虚拟架构中虚拟机可动态在线从一台物理服务器迁移到另一台物理服务器上的特性等。FC-SAN建议使用双控且双控支持A/A模式工作，防止单个控制器或光纤链路失效。

（5）存储要求采用大于或等于8个 16GB FC，提供大于或等于256GB 的存储缓存吞吐量，充分保证了未来各级政务业务系统的 I/O 需求。

（6）计算节点和存储节点必须与交换设备实现双连接接入。

（7）资源负载率应保持在85%以下。

1.4.2.设备技术要求

FC-SAN存储

| 用途：FC-SAN存储 |
| --- |
| 指标项 | 指标要求（除特别说明外，以下为单台设备的参考配置要求） |
| 数量 | 不少于1套 |
| 体系架构 | 实配SAN和NAS统一存储，配置NAS协议（包括NFS和CIFS）、IP SAN和FC SAN协议 |
| 控制器 | 至少2个控制器，双控之间（含SAN和NAS）采用PCI-E互联，最大可扩展为8个控制器 |
| 缓存 | 每量不小于128GB；  |
| 接口 | 至少提供16个16Gb光纤接口和8个GE接口； |
| 存储模式、容量 | ≥25\*600GB 10K RPM SAS硬盘单元(2.5")、≥200\*1200GB 10K PRM SAS硬盘单元(2.5")和≥33\*4000GB 7.2K RPM NL SAS硬盘单元(3.5")，最大支持磁盘插槽个数≥1200 |
| 在线扩容方式 | 支持不中断业务在线扩容 |
| 软件功能 | 配置存储软件基础包、快照，远程复制，智能数据迁移，智能异构虚拟化使用许可 |

**1.5.网络资源池**

1.5.1.基本要求

网络服务要求能实现动态的网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接。

依照电子政务外网的安全域划分，云服务商平台主要划分为公用网络区和互联网区。其中公用网络区主要是政务部门系统内和系统间的互访，互联网用户不能直接访问这个区域的数据和信息系统；互联网区部署政务部门的WEB服务器，完成政务信息互联网发布和数据填报。

各安全域内从网络服务、数据应用业务的独立性、各业务的互访关系及业务的安全隔离需求综合考虑，将管理数据、网络数据、存储数据进行的存储、传输和交互进行有效隔离。

市级部门的业务通过逻辑隔离划分不同的安全域，市级部门访问或管理业务系统可通过VPN等多种方式实现。

1. 互联网区与公用网络区出口边界应通过访问控制设备建立边界。
2. 平台内网络至少划分为业务网、存储网、管理网等，业务网络至少具备10G网络通讯能力，存储网络至少具备10G通讯能力，管理网络至少具备1G网络通讯能力。
3. 平台核心交换机至少配置1台数据中心级高性能模块化交换机，具备网络虚拟化集群部署能力。若部署接入交换机也需具备虚拟化部署能力。

1.5.2.设备技术要求

（1）核心层交换机：配置数量：1台；

①性能要求:交换容量≥180Tbps;

②包转发率≥110000Mpps；

③配置要求: 主控引擎与交换网板硬件分离,主控板故障或者更换不影响整机转发性能；

④配置主控引擎≥2；

⑤交换网槽位数≥4；

⑥交换网满配，满足所有槽位线速转发；

⑦整机业务板槽位数≥8；

⑧提供48端口千兆电接口，24个万兆以太网光接口；

⑨配置冗余交流电源，16颗万兆多模光模块，配置MPLS功能；

⑩整机要求：Clos架构、信元交换，要求单条流可以负载分担到多块交换网，提高交换网利用效率，设备支持严格前后风道,便于机房散热统一规划；

⑪风扇框冗余设计，要求风扇框个数≥3,任意风扇框故障或者不在位不能造成业务中断；

⑫具备基本网络功能、openflow1.3、IPv6网络功能、虚拟化功能。

⑬支持跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现；

⑭支持集群或堆叠支持带外管理方式（主控板上提供专用GE端口用于集群或堆叠协议报文传送），实现数据、控制、管理平面分离。

⑮数据中心特性：支持FCoE、VxLAN功能，支持N:1虚拟化后再进行1：N虚拟化；

⑯线卡前面板开孔进风，加快光模块散热，延长光模块寿命; 支持RIP V1、V2, OSPF, IS-IS，BGP，支持RIPng、OSPFv3、IS-ISv6、BGP4+，支持MPLS TE。

（2）接入交换机和委办局接入汇聚交换机：配置数量：8台；

①性能要求：交换容量≥1.28Tbps，包转发率≥950Mpps；

②端口要求: ≥32个10GE电接口，≥16个10GE光接口，≥4个40GE 光接口，8颗万兆多模光模块；

③设备功能要求：为了提高设备可靠性，支持并配置电源1+1备份和风扇框1+1备份，支持前后、后前风道，本次配置后前风道，便于机房统一规划设计散热；

④支持跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现；

⑤数据中心特性：支持与核心交换机配套，通过纵向虚拟化技术，作为远程板卡，提供10GE SFP+端口接入，可支持本地转发。

**2.云平台**

**2.1.云管理平台**

**2.1.1.云管理平台软件要求**

云管理平台软件需满足以下需求：

| 指标项 | 指标要求 |
| --- | --- |
| 成熟度需求 | 为保证平台的稳定性，云管理平台软件需自主可控，采用OpenStack技术架构，具备内核级开发能力，**并提供证明材料**； |
| 云管理平台高可用性 | 云管理平台服务应该保证高可用性，所有云平台内的提供管理能力的服务或者组件都应该使用集群或者高可靠的方式进行部署，并且针对所有关键管理数据进行定期备份，防止重要数据丢失，并可以用这些数据快速恢复业务，同时可以对管理系统进行平滑的扩容； |
| 资源管理界面 | 云管理面向租户提供服务Portal，租户登录时支持双因素认证保证安全性。租户通过服务Portal申请需要的各项云服务； |
| 大屏展示能力 | 提供大屏展示能力。支持用户自定义大屏的展示内容以及布局，支持用户定义多种不同的大屏展示内容，每个大屏都支持容量、性能、资源统计、告警等的自定义展示，且可以定义每个内容的不同呈现形式（例如柱状图、饼图、仪表盘等等）**提供截图证明**； |
| 统一的告警管理 | 云管理平台可以统一管理系统中物理设备（服务器、存储、网络设备）和虚拟资源的告警，并支持告警的清除、指派、调整级别、设置告警提示音等；支持告警转发能力，系统可以按照管理员指定的规则，将不同类型的告警通过短信或者邮件发送给不同的用户或者用户组进行处理，**提供截图证明**； |
| 报表管理 | 系统支持基础的容量、资源使用、设备、告警统计报表，并支持报表的自定义呈现，管理员可以对已有的指标进行交叉组合、过滤来进行自助式的业务分析，并生成最终报表，也可以配置定期生成指定报表并发送到指定用户/用户组； |
| 服务自定义 | 管理员可以灵活的定义已有服务，配置用户申请服务时需要输入的参数，例如管理员可以指定用户申请虚拟机时是自己指定虚拟机规格还是只能使用固定规格，配置好后可以发布为一个新的服务让用户申请。新的服务发布时可以分别指定用户申请、修改、删除这个服务时是否需要审批，需要被谁审批;支持管理员自定义可以线下实施的任何业务**，提供统一的申请、审批、计量、开通能力,提供截图证明；** |
| 虚拟数据中心（VDC）管理能力 | 提供虚拟数据中心（VDC）管理能力，并支持在VDC下再划分多级子VDC，以匹配业主的组织/租户体系进行管理。每个VDC都可以分配多个数据中心的资源，管理云可以对每个VDC（组织）可以使用的资源做配额限制； |
| 用户的性能、告警管理能力 | 支持用户的性能、告警管理能力。用户可以通过统一管理平台查看自己资源的性能统计情况以及资源性能的TOP分析报表；并且用户可以针对自己的组织设置配额阈值和性能阈值规则，可以配置在资源分配率和资源使用率达到设置值时通过短信和邮件的方式发送告警给用户，**提供截图证明**； |
| 虚拟机热迁移 | 当虚拟机所在的硬件设备维护升级时能够实时的迁移到其它硬件设备上运行，而虚拟机中的服务不应停止；而当原硬件设备维护升级结束后也可以将虚拟机从其他硬件中迁移回来，在迁移过程中服务正常运转。 |
| 云主机服务 | 提供云主机服务，用户可以通过自己的账号登录管理平台来申请云主机资源，并且定义自己的虚拟机规格（包括CPU、内存、磁盘、网卡）；申请到云主机后，用户可以通过管理平台对虚拟机执行开机、关机、重启、删除、远程登录、快照、克隆、重置密码等操作，也可以根据虚拟机名称、IP、ID、运行状态以及自定义标签等快速查找、过滤虚拟机，**提供截图证明**； |
| 虚拟私有云（VPC）服务 | 提供虚拟私有云（VPC）服务，用户可以通过虚拟私有云自由的创建自己的虚拟网络。用户可以自行创建自己要的多个网段，指定每个要创建的网络的网段、掩码、DNS等，也可以指定这个网络内的路由规则以及NAT规则，**提供截图证明**。 |
| 云硬盘服务 | 提供云硬盘服务，用户可以通过管理平台为虚拟机申请磁盘，用户可以将申请到的磁盘空间分配给一台或者多台虚拟机/物理机使用，在操作系统支持的情况下，可以对已经在使用的云硬盘进行在线/离线扩容（提供支持在线扩容的操作系统清单），**提供截图证明**； |
| 备份服务 | 提供备份服务能力，用户可以通过管理平台申请对自己的部分或全部虚拟机或者虚拟机的磁盘做备份，用户可以自行设置备份策略，包括备份周期、执行时间点、备份时保留的副本数目（或者每个副本保留多长时间）、全备/增备策略，将数据备份到其它机房的备份周期等；同时，用户也可以选择特定的备份策略进行手动备份；用户可以通过管理平台管理备份数据，包括删除特定备份数据、恢复指定时间点的备份数据等，**提供截图证明；** |
| 支持镜像服务能力 | 提供镜像服务能力，允许管理员可以通过管理平台上传镜像，这些镜像可以被所有用户同时使用，也可以支持用户通过管理平台自行创建并共享自己的镜像，这些镜像可以被创建者以及被共享的用户使用，用户可以通过管理平台导入常见格式的镜像， 用户可以查看已经上传的所有镜像，包括镜像名称、OS类型、镜像大小等； |
| 授权 | 提供不少于64颗CPU云管理平台软件授权许可 |

**2.1.2.云管理平台硬件要求**

云服务商平台至少配置3台服务器用于云平台基础管理和配置1台服务器用于云服务扩展管理，须保证各功能节点的高可用性。

云平台基础管理服务器参考参数要求如下：

| 用途：云平台基础管理 |
| --- |
| 指标项 | 指标要求（除特别说明外，以下为单台设备的参考配置要求） |
| 数量 | 根据需求配置，至少3台； |
| CPU | 至少配置2.2GHz/14-core处理器； |
| 内存配置数量 | ≥448GB DDR4 内存； |
| 硬盘 | 配置至少2\*600GB 10K SAS硬盘、2\*1200GB 10K SAS硬盘、5\*4000GB 7.2K SATA硬盘、2\*800GB读写混合型固态硬盘、1\*1600GB-NVMe PCIe-读写混合型-固态硬盘 |
| RAID卡 | 支持RAID0,1,5,6,10,50,60-12Gb/s-1GB Cache |
| 网络接口 | 至少4\*10GE光口(含光模块)、2\*1GE电口  |
| 电源和风扇 | 配置冗余电源和风扇； |

**2.2.容灾备份系统**

2.2.1.基本要求

（1）乐山市政务云平台为各委办局用户应用虚拟机提供本地备份服务，各委办局单位可以申请备份服务，将业务主机的卷备份到本地的备份存储中，保障核心业务数据的安全保护。保障当业务主机出现故障时，数据不丢失，并且可以通过备份数据恢复，提高业务的高可靠。

（2）云服务商需完成备份系统建设，完成搭建工作并提供相应服务。

（3）云服务商提供备份一体机。

2.2.2.设备技术要求

备份一体机

| 用途：备份一体机  |
| --- |
| 指标项 | 指标要求（除特别说明外，以下为单台设备的配置要求） |
| 基本功能 | 实现MYSQL数据库、SQL数据库和ORACLE数据库的备份与恢复； |
| 容量 | 100T容量 |
| 处理器 | 两颗Intel Xeon处理器； |
| 缓存要求 | 配置128GB高速缓存 |
| 接口 | 自带2个Intel千兆以太网接口及2个光纤接口； |

**2.3.主机托管**

云服务商平台须至少提供25个42U标准服务器机柜用于物理设备托管服务。

**3.安全等保要求**

云服务商平台应具备必要的边界防护、链路保护、威胁检测、安全审计及平台安全管理等安全服务能力，云服务商提供电子政务云平台应满足国标GB/T 31168-2014《信息安全技术云计算服务安全能力要求》，实现信息安全等级保护第三级的防护要求，达到为政府部门提供云计算服务的基本安全能力。各委办局单位按照自身业务等保需求，自行完成等级保护测评。

**3.1.边界防护能力要求**

云服务商平台须具备边界防护能力，须提供针对DDOS攻击流量的检测及清洗、访问流量的访问控制、入侵防御、网络恶意代码防范、web应用攻击防御等安全保护能力。

云服务商平台须提供包括不限于抗DDOS流量清洗系统、互联网边界防火墙、省政务外网边界防火墙、WEB应用安全网关系统（WAF）等安全系统作为边界防护能力的服务工具，且服务工具必须为国产。工具技术要求如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 工具名称 | 技术要求 |
|  | 抗DDOS流量清洗系统 | 须提供不少于4个万兆光口，不少于7个接口扩展插槽，抗64字节小包抗攻击能力须不低于20Gbps。须具备流量型攻击和应用层 DDoS 攻击防护能力，有效保护整个政务云内部网络应用免受各种 DDOS 攻击。须支持智能特征提取功能、通过主机活跃性和通信模式分析异常流量功能、智能协议解析功能，以上功能须**提供证明材料**。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
|  | 互联网边界防火墙 | 须提供不少于8个万兆光口，性能须不低于120Gbps，并发连接数不低于1500万；须具备访问控制、入侵防御、病毒防御、流量控制等功能，须保证IPS特征库、病毒库不少于三年的实时性。须支持TCP连接阻断功能、基于网络数据流的网络病毒检测功能、对网络入侵事件进行风险评估功能，以上功能须提供国家相关机构证明材料。须具备《国家信息安全测评信息技术产品安全测评证书》（EAL4+或以上级别），提供证明材料。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
|  | 政务外网边界防火墙 | 须提供不少于6个千兆电口，不少于4个万兆光口，网络层吞吐量不少于4G，并发连接数不少于220万；须支持下一代防火墙访问控制、入侵防御、上网行为及URL分类管理、流控和IPSec VPN模块；须保证IPS特征库、病毒库不少于三年的实时性。须支持TCP连接阻断功能、基于网络数据流的网络病毒检测功能、对网络入侵事件进行风险评估功能，以上功能须提供国家相关机构证明材料；须具备《国家信息安全测评信息技术产品安全测评证书》（EAL4+或以上级别），**提供证明材料**。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
|  | Web应用安全网关（WAF） | 须提供不少于6个千兆电口，不少于4个千兆光口，不少于2个万兆光口，性能须不低于20G，最大并发HTTP连接数不低于1000万；须保证特征库不少于三年的实时性；须具备包括但不限于HTTP/HTTPS 应用防护、Web 请求信息限制、Web 敏感信息防护、Cookie 防篡改、网页防篡改、Web应用防护事件库升级等功能。须支持检测恶意HTTP请求的功能、主动识别网页爬虫的防护功能、网页防篡改功能，**以上功能须提供国家相关机构证明材料。**★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |

**3.2.链路保护能力要求**

云服务商平台须具备链路保护能力，提供等针对链路高可用性、链路高利用性保护等安全防护能力。

云服务商平台须提供包括不限于链路负载均衡系统等安全系统作为链路高可用性保护能力的服务工具，且服务工具必须为国产，**提供公安部颁发的《计算机信息系统安全专用产品销售许可证》。**工具技术要求如下：

链路负载均衡系统

|  |  |  |
| --- | --- | --- |
| 序号 | 工具名称 | 技术要求 |
| 1 | 链路负载均衡系统 | 性能须不少于40Gbps，须提供不少于4个千兆电口，4个千兆光口、8个万兆光口，冗余电源；须提供包括不限于服务器负载均衡，多链路负载均衡，全局负载均衡，内容交换，应用系统加速，TCP 单边加速，商业智能分析功能及缓存、压缩、SSL卸载、TCP连接复用等优化特性等功能；须具备链路负载均衡功能，可实现多条运营商链路的负载均衡，保证链路的高可用性，不需要额外的授权；须具备主主（AA）、主备（AS）工作模式，IP地址可在设备间漂移，根据设备状态将流量牵引到主设备；须具备V4/V6双栈，支持V4/V6地址转换,支持前缀地址转换，IVI，地址池，IPv4和IPv6混合环境下的四层服务器负载，链路负载，健康检查功能；须具备DNSv6，支持基于IPV6地址的七层内容交换（URL负载、HTTP头擦除、重定向信息改写等）功能。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |

**3.3.威胁检测能力要求**

云服务商平台须具备威胁检测能力，提供针对传统已知入侵威胁的检测、未知威胁的检测、异常流量分析检测、系统脆弱性检测等安全检测能力。

云服务商平台须提供包括不限于入侵检测系统、漏洞扫描系统等安全系统作为威胁检测能力的服务工具，且服务工具必须为国产。工具技术要求如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 工具名称 | 技术要求 |
| 1 | 入侵检测系统 | 为保证检测性能，须提供包括检测引擎及数据分析中心的分体式入侵检测系统。检测引擎须提供不少于6个电口，须具备IDS,APT静态检测,流量监控分析功能，性能不低于2Gbps，最大并发链接数不低于200万；数据分析中心须提供不少于6个电口，数据存储量不少于3T。检测功能可使用期限须不少于3年。须支持网络设备上提取流量攻击报文特征的功能、安全事件实时确认功能、IP地址快速定位功能、计算机网络入侵定位功能，以上功能须提供国家相关机构证明材料。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
| 2 | 漏洞扫描系统 | 须提供不少于6个千兆电口，1TB硬盘、双电源；最大并发扫描任务数不少于40,可扫描总数量不少于200个无限制范围的IP地址，须提供不少于3年的最新漏洞库。支持云平台扫描功能，覆盖OpenStack 、KVM、Vmware、Xen等主流的云计算平台。须支持对计算机信息系统综合风险计算功能、基于异常度量的宏观网络安全状态进行评估，以上功能须提供国家相关机构证明材料。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |

**3.4.安全审计能力要求**

云服务商平台须具备安全审计能力，提供针对网络行为的安全审计，包括不限于数据库操作行为审计、网络行为审计、运维行为审计、日志审计等安全审计能力。

云服务商平台须提供包括不限于数据库审计系统、运维审计系统、网络行为审计系统等安全系统作为边界防护能力的服务工具，且服务工具必须为国产。工具技术要求如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 工具名称 | 技术要求 |
| 1 | 数据库审计系统 | 须提供不少于6个千兆电口，不少于1个接口扩展插槽，数据存储量不少于4T，支持raid1;须可对不少于23个数据库进行审计,须具备Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、国产数据库、人大金仓、达梦、南大通用、神通数据库的审计能力。须具备基于被审计对象的报文过滤功能、数据库错误信息提取功能、数据库响应时间测算功能，以上功能须提供证明材料。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
| 2 | 运维审计系统 | 须提供不少于6个千兆电口，一个接口扩展插槽，数据存储量不少于2T，可管控资源数量无限制。须具备基于角色管理的安全审计功能，具备基于回显的审计功能，能够通过回显解析telnet协议。以上功能须提供证明材料。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
| 3 | 网络行为审计系统 | 须提供不少于12个千兆电口，不少于12个千兆光口，不少于8个万兆光口，性能须不低于80Gbps，每秒新建连接数不低于50万，每秒最大并发连接数不低于1000万；须具备对网络社区、P2P/IM 带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别，同时对内网用户所有的上网行为进行记录，留存相关日志的功能。须支持智能协议解析功能、基于流量特征的P2P应用识别功能、广域网P2P流量监控功能，以上功能须提供证明材料。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |

**3.5.安全管理能力要求**

云服务商平台须具备云平台安全管理能力，提供针对云平台网络、系统等的安全管理，包括不限于云平台资产管理、云平台设备性能监控、云平台安全事件管理、云平台日志管理及审计、脆弱性管理等安全管理能力。

云服务商平台须提供包括不限于安全管理平台等安全系统作为安全管理能力的服务工具，且服务工具必须为国产。工具技术要求如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 工具名称 | 技术要求 |
| 1 | 安全管理平台 | 须为软件形态，基于大数据技术，须具备日志管理及审计、系统平台框架、资产管理、安全事件管理、安全事件关联分析、脆弱性管理、风险评估、报表、响应管理、权限管理、知识管理、系统管理、网络拓扑、机架拓扑，对网络设备、安全设备、主机服务器的可用性与性能监控等功能；提供的可管理设备数须不少于100；须支持标准日志范式化功能，在日志采集时采用基于通用范化标签语言的安全信息管理技术、海量日志关联分析功能、针对网络安全事件的可视化定位分析功能、基于规则的安全事件关联分析功能，以上功能须提供证明材料。 |

**（三）云服务目录报价要求**

1、云服务目录报价包括按照“GB 50174-2017”B级及以上机房要求的空间、消防、制冷、供电、监控等相应服务环境支撑费用。

2、云服务目录报价包括满足本期项目采购文件和服务期内国家相关法规文件所提出的网络、安全、备份、服务、运维等要求费用。

3、云服务商平台软件应具备灵活可靠的计费计量功能，并开放接口。云租赁服务商应该按市场情况，本次建设情况，提供如下格式的云资源单元报价表。

★4、下表**为**单项最高限价，**报价上浮**为无效投标。

★5、云服务目录单元报价限价表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 服务目录 | 明 细 | 配置规格 | 计量 单位 | 云服务目录报价（元） | 云服务目录最高限价（元） |
| 计算和存储服务 | 物理内存（通用性） | 物理内存≥448GB DDR4，频率最高达2933MT/s | GB·月 | P1 | 29 |
| 物理内存（高性能） | 物理内存DDR4，频率最高达4266MT/s | GB·月 | P2 | 32 |
| 虚拟CPU（通用型） | 物理CPU为英特尔至强金牌5120(2.2GHz/14-core/19.25MB/105W)处理器（虚拟配比不超过1:4） | 核·月 | P3 | 22 |
| 虚拟CPU（高性能） | 物理CPU频率不低于2.6GHz（虚拟配比不超过1:4） | 核·月 | P4 | 24.5 |
| SAS块存储 | 存储池应为FC-SAN存储，≥10K RPM SAS硬盘单元(2.5")、≥7.2K RPM NL SAS硬盘单元(3.5") | TB·月 | P5 | 462 |
| 设备托管 | 设备托管 | 不少于25个42U机柜 | U·月 | P6 | 360 |
| 42U机柜·月 | P7 | 4100 |
| 总计 |  |  | P8 | 5029.5 |

注：P8= P1+P2+P3+P4+P5+P6+P7

**B、服务要求**

**（一）项目总体服务要求**

1、成交的云服务商运营主体应当接受安全监管中心监管，接受采购人的服务考核。

2、云服务商必须**承诺**配合云平台上云单位业务应用及其数据迁移上云的工作。

3、云服务商须**承诺**在服务期结束后，配合各使用单位迁移应用系统，并**提供服务退出承诺书原件**。

4、云服务商必须**承诺**提供给云服务商的数据、设备等资源，以及云计算平台上政务系统运行过程中收集、产生、存储的数据和文档等数据资源均属政府所有。云服务商必须保障各政府部门对这些资源的访问、利用、支配。未经政府授权，不得访问、修改、披露、利用、转让、销毁数据。

5、云资源实际使用量由采购人组织专家团队核定。

6、云服务商的软硬件设备授权数、用户数不足时须主动扩展，不能因授权不足影响租户使用。

**（二）项目运维服务要求**

**1、运维总体要求**

（1）云服务商平台提供的服务应满足《信息安全技术云计算服务安全能力要求》（GBT 31168-2014）、《信息安全技术 云计算服务安全指南》（GBT 31167-2014）、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14号）及国家主管部门发布的其他标准规范要求。

（2）云服务商提供的服务总体应满足业务需求，确保云平台安全、稳定、可靠运行。

**2、运维团队要求**

云服务商需提供素质高、专业性强、经验丰富、稳定的运维团队，主要负责整个电子政务云平台的软硬件和网络运维。云服务商需建设有严格的、有组织有纪律的管理运维流程，并指派专职接口人，团队需要7\*24在岗及时响应故障请求，负责电子政务云平台的故障受理、处理、跟踪、结果汇报工作。

云服务商提供的运维团队成员须具备相应的资质，且需将运维团队的组织架构及人员名单报采购人同意和备案。

云服务商须提交《政务云平台应急预案》和培训，且每年应至少进行一次应急演练。

**3、响应要求**

云服务商须提供7\*24不间断技术服务支持时间。且应在1小时内解决出现的故障问题。

**4、保密要求**

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

**5、运维考核**

为了保证云服务商提供的服务具备可靠性、稳定性，降低云平台对电子政务业务系统的影响和风险，必须符合运维服务考核标准与事故处理办法。云服务商每月向采购人提交《运维服务报告》，采购人按照《运维服务考核标准及办法》进行考核。

对运维服务不合格的云服务商采购人将采取服务费用扣除方式进行惩处（具体细节合同再行约定）。

运维服务考核标准及办法

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 考核内容 | 费用扣除标准 | 核验方式 |
| 运维制 度 | 未建立完善的年度运维方案和应急预案，责任未明确到公司领导，发生重大变故时未及时更新方案并报采购人。 | 1000元/条 | 查验文件 |
| 未组建专业运维团队，未明确运维团队负责人，运维团队中无虚拟化工程师、运维工程师，有成员不具备政务云平台运维基本资质，有成员均未与运维公司就该项目签订专门的保密协议。 | 查验文件 |
| 运维团队未每月召开至少一次运维服务工作专题会议。 | 查验会议记录 |
| 未每年进行一次应急演练。 | 现场查验 |
| 信息报 送 | 运维服务期间**每月、年**向采购人报送政务云运维信息和上云系统使用情况。报送信息应反映各单位上云系统运维管理情况和CPU、内存、磁盘等资源的实际使用率。 | 3000元/次（未报送） |  |
| 运维事 件 | 三级故障（低）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、因服务商问题，导致云平台客户业务中断数量大于1个，少于5个；二、云平台1、云平台服务少于20%不可用三、基础设施1、网络性能下降小于50%2、核心设备出现故障 | 一次扣2000元 | 日志记录监管记录用户考评 |
| 二级故障（中）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、因服务商问题，导致政务互联网、政务外网或者专网客户业务中断数量超过5个二、云平台1、云平台服务超20%少于50%不可用三、基础设施1、部分设备断电2、网络性能下降50%或者部分网络中断 | 一次扣6000元 | 日志记录监管记录用户考评 |
| 一级故障（高）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、政务互联网、政务外网或者专网业务全部中断二、云平台1、云平台服务超50%不可用三、基础设施1、单机房完全断电(UPS供电正常不计为故障）2、政务互联网、政务外网或者专网全网中断； | 一次扣20000元 | 日志记录监管记录用户考评 |

以上考核细则将按照符合国家相关法律法规和符合项目实际需要的原则，进行不定期的修订完善，若有修订按修订后细则执行。

在政务云平台运维服务中，若对运维职责范围内的工作有任何异议，以服从采购人安排为先，事后双方再协商解决。

**C、商务要求**

**1、报价要求：**

本项目对云服务商服务目录总报价进行了最高限价。云服务商应科学合理地对每项云资源目录服务单元进行同比例下浮报价。

 **报价包含但不限于：**满足本期项目采购文件和服务期内国家相关法规文件所提出的网络、安全、备份、服务、运维等要求费用**、**及**场地费、链路费、人工费、资料费、利润、税金等**所有相关费用。

**2、项目实施要求**

**1)项目实施与管理**

**云服务商应制定详细的项目运维计划，并提供项目运维人员保障方案。**

**2)技术文档要求**

所有设备具备全套中文（或英文）技术文档手册、资料；投标方应提供与设备相关的所有技术文档和资料，并且均应以磁介质（或光盘）或纸张为载体。

**3、合同服务期限和地点**

服务期限：本项目服务期为1年度。

 履约地点：乐山市范围内

**4、付款方式**

**①乙方收取的服务费包含但不限于：平台软件硬件系统费用、场地费、链路费、人工费、资料费、利润、税金等。**

②云资源服务费按采购单价和实际分配资源量进行付费，结算方式:**签定合同后30个工作日内，甲方向乙方预付预算金额的10%(成交人为小微企业的，预付预算金额的30%），余下款项分两次支付，签订合同并提供服务后6个月内，第一次支付服务期起算日起至服务期满六个月后所产生的服务费用的70%；第二次在服务期结束后，根据服务考核情况支付尾款。**若验收时云服务商有不影响功能使用要求的负偏离，在结算时按合同约定扣款。甲方付款前，乙方应先向甲方开具等额增值税普票。

③上述款项的支付时间具体以财政部门将资金划拨到甲方账户时为准，且在到账后30个工作日内支付，乙方理解并同意。

**三、第2包：视频政务云服务采购项目**

**A.采购内容**

**（一）政务云平台服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目名称** | **服务内容** | **数量** |
| 1 | 机房环境 | （机房技术服务标准要求详见“包2政务云平台服务技术要求”中“1.1.机房环境”） | 1项 |
| 2 | 计算资源池 | （计算资源池技术服务要求详见“包2政务云平台服务技术要求”中“1.2. 计算资源池”） | 1项 |
| 3 | 存储资源池 | （存储资源池技术服务要求详见“包2政务云平台服务技术要求”中“1.3. 存储资源池”） | 1项 |
| 4 | 视频资源池 | （视频资源池技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.4. 视频资源池”） | 1项 |
| 5 | 网络资源池 | （网络资源池技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.5. 网络资源池”） | 1项 |
| 6 | 安全资源池 | （安全资源池技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.6. 安全资源池”） | 1项 |
| 7 | 虚拟私有云 | （虚拟私有云技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.7. 虚拟私有云”） | 1项 |
| 8 | 容灾备份 | （容灾备份技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.8. 容灾备份”） | 1项 |
| 9 | 云管理平台 | （云管平台技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.9. 云管理平台”） | 1项 |
| 10 | 传输链路 | （传输链路技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.10. 传输链路”） | 1项 |
| 11 | 云主机托管 | （云主机托管技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.11. 云主机托管”） | 1项 |
| 12 | 基础软件 | （云主机托管技术服务要求具体内容要求详见“包2政务云平台服务技术要求”中“1.12. 基础软件服务”） | 1项 |

（**二**）**政务云平台服务技术要求**

**标注“★”的条款为本项目的实质性条款，供应商须全部满足，不响应或不满足作无效响应处理。**

**1.1机房环境**

（1）机房应具备环境智能监控，实现对设备电流量、UPS、精密空调、机房漏水、温度、湿度等的监控。机柜区域须配备专用门禁和24小时视频监控系统，视频监控画面可远程调用至安全监管中心，云服务商必须无条件开放接口或者提供监控服务，监控录像保存时间不少于3个月。

（2）云服务商必须保证主机房设备（包括采购人托管设备）可持续获得电力供应（配备柴油发电机和UPS备用电池），每年持续电力供应时间在99.99%以上，以确保电子政务应用系统可持续工作，满足采购人对于信息化政务工作的要求。

（3）机房应按照GB50174-2017《数据中心设计规范》B级及以上级标准进行建设，云服务可用性应在99.99%以上。主机房整体面积≥150㎡（至少容纳25个42U标准服务器机柜），机房同地点处办公场地面积≥150㎡，其中机房监控室面积≥50㎡（配置不少5㎡的运维监控大屏）。机房、办公场地和机房监控室应具备拓展性。

**1.2计算资源池**

1、基本要求

（1）互联网服务区和政务服务区计算资源池划分为通用性能计算区和高性能计算区，两类计算区使用不同配置的服务器进行承载。

（2）云服务商需将服务器按照两类计算区划分的原则，将不同用途的服务器进行划分并进行上架，测试，安装操作系统和虚拟化软件，连接到虚拟化存储池，创建虚拟文件系统，并将虚拟化服务器纳入云管理平台，包括安装和配置虚拟网络、配置虚拟交换机、配置虚拟机模板、安装操作系统及常用工具、安装常用的中间件模板、安装常用的数据库系统模板系统、配置虚拟机安全策略、日志监控、配置集群、配置自动迁移策略、配置资源池等工作。

（3）计算节点和存储节点必须与交换设备实现双连接接入。

（4）资源负载率应保持在75%以下。

2、设备要求

以下为单台设备的配置要求，云服务商可自行选型，但设备性能参数不得低于以下性能参数。

（1）表1--通用性能计算服务器配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| CPU | 配置2颗INTEL Gold -5118系列及以上CPU（**每颗**≥12 核） |
| 内存 | ≥768GB DDR4内存 |
| 硬盘 | 至少SAS 10K 600G \*2硬盘支持断电保护 |
| RAID卡 | 八通道高性能 RAID卡 原厂LSI 9361-8i-2G缓存（超级电容）；提供掉电保护功能 |
| 网络接口 | Intel原厂I350双口千兆网卡\*2（电口），Intel原厂82599双口万兆网卡\*2（光口），配置4个万兆光模块（多模） |
| 电源和风扇 | 配置冗余电源和风扇 |

（2）表2--高性能计算服务器配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| CPU | 配置4颗INTEL\_GOLD-6132 系列及以上CPU（**每颗**≥14 核） |
| 内存 | ≥1024 GB DDR4 内存 |
| 硬盘 | SAS 10K 600G \*2 Raid1 |
| RAID卡 | RAID:八通道 SAS 高性能RAID-9361（1G缓存)+缓存断电保护模块（超级电容）\*1 ；提供掉电保护功能 |
| 网络接口 | Intel原厂I350双口千兆网卡\*2（电口），Intel原厂82599双口万兆网卡\*2（光口），配置4个万兆光模块（多模） |
| HBA卡 | 光纤通道HBA卡,FC 16GB,单端口,LC接口\*2 |
| 电源和风扇 | 2+2冗余电源；冗余风扇，机架安装导轨 |

（3）表3--数据库服务器配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| CPU | 配置4颗INTEL Gold-6132系列及以上CPU（**每颗**≥14 核） |
| 内存 | ≥512GB DDR4 内存 |
| 硬盘 | 至少2\*1200GB 10K RPM SAS硬盘，支持断电保护 |
| RAID卡 | 支持 RAID0/RAID1/RAID5/RAID10/RAID6，Raid 卡缓存≥1G；提供掉电保护功能 |
| 网络接口 | 至少2\*10GE光口；2\*1GbE电口 |
| FC接口 | 至少2\*16GB FC 接口 |
| 电源和风扇 | 配置冗余电源和风扇 |

**1.3存储资源池**

1、基本要求

存储池的设计分为两类：分布式存储、FC-SAN存储。

（1）分布式存储用来承载如虚拟机系统、虚拟机镜像、ISO、虚拟机的模板文件、非结构化数据、大文件等。

（2）FC-SAN存储用来承载对IOPS要求较高的业务数据，支持SSD、SAS、SATA三种存储介质，并根据业务场景提供适合的IO性能。要求采用大于或等于8个16GB FC，提供大于或等于128GB的存储缓存吞吐量并具备扩展能力，保证各级政务业务系统的 I/O 需求。

（3）服务期间磁盘故障更换时，云服务商应首先向采购人提出故障磁盘消磁处理申请，经采购人书面同意后对故障磁盘应做消磁处理。服务期满后，存储系统及介质的处置，云服务商亦需经过采购人书面同意。

2、设备要求

以下为单台设备的配置要求，云服务商可自行选型，但设备性能参数不得低于以下性能参数。

（1）表4-- 分布式存储器配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| CPU | 配置2颗INTEL Silver4114系列及以上CPU（**每颗**≥10核） |
| 内存 | ≥128GB |
| 硬盘 | ≥SSD 480G\*2|SAS 10K 600G \*2|SAS 1.8T \*10 |
| RAID卡 | 支持RAID 0/1，直通 |
| 网络接口 | ≥Intel原厂I350双口千兆网卡\*1（电口），Intel原厂82599双口万兆网卡\*1，配2个模块（多模） |
| 电源和风扇 | 配置冗余电源和风扇 |

(2)表5--FC-SAN存储配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| 控制器 | 采用SAN和NAS统一集成的多控制器架构，统一管理；（具备FC/IP SAN和NAS融合组网能力）；控制器扩展能力≥8；配置≥2个控制器；控制器冗余设计（PCI-E、Rapid-IO、IB或FC互联），支持在线更换控制器；在线升级存储系统，无须停机，控制器故障自动切换和自动重建功能 |
| 缓存 | 双控配置高速缓存≥256GB（缓存不包含SSD磁盘、PCI-E SSD、闪存、压缩或重删缓存和NAS控制器缓存） |
| 端口 | 每控制器可扩展≥3个主机扩展卡（非板载）；配置≥8个1Gb iSCSI主机端口和≥8个8Gb FC主机接口，支持16Gb FC，10Gb iSCSI/FCoE，10GbE/1GbE NAS等接口。 |
| 硬盘 | 支持10000转高性能磁盘、SSD固态硬盘，同时支持2.5、3.5寸SAS硬盘，支持硬盘混插技术。支持热备盘或者热备空间两种热备技术。 |
| 功能要求 | 配置快照、克隆、自动精简、本地复制、卷镜像、卷备份，以上几个功能配置全容量许可，后续扩容无需额外购买许可；配置QoS功能，支持单卷的IOPS、Bandwidth的限制设定；配置性能监控功能，可以定制历史运行数据的图形化报表；支持SSD缓存加速功能；支持自动分层功能：可实现四层数据分层；支持存储虚拟化功能，可以整合异构厂商的存储阵列，通过虚拟化功能将存储资源统一管理和分配；支持存储双活：支持基于阵列的双活功能，切换过程无需人工干预，支持3DC远程复制组网模式；配置云备份特性，支持存储数据直接备份到公有云和私有云，支持Amazon S3、IBM SoftLayer、OpenStack Swift、Aliyun OSS 等对接能力，无须单独配置备份软件 |
| 兼容性要求 | 支持Windows、Linux、VMware、UNIX (HP-UX、AIX、Solaris等)；获得VAAI/VASA/SRM/vMSC认证，提供vmware官网认证截图和链接；获得OpenStack Cinder兼容性认证，支持Openstack的Queens版本，提供OpenStack官方官网截图及链接；获得SMI-S v1.6或以上版本的CTP认证并提供截图证明 |

**1.4视频资源**

视频云存储用来存储视频和图片等非结构化数据，这类数据规模大、保存时间长，并要求随时调用。面对这样的需求，传统的SAN或NAS在容量和性能的扩展上会存在瓶颈。视频云存储可以突破这些性能瓶颈，并且可以实现性能与容量的线性扩展。

设备要求

以下为单台设备的配置要求，云服务商可自行选型，但设备性能参数不得低于以下性能参数。

表6--视频云存储配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| CPU | 配置2颗INTEL Gold -5218系列及以上CPU（**每颗**≥12 核） |
| 内存 | ≥256GB DDR4内存。 |
| 硬盘 | 2\*600GB 10K 2.5寸硬盘，1\*480GB SSD，35\*6TB SATA硬盘。 |
| 接口 | 4个万兆网络接口（含多模光模块），2个千兆主机接口。 |
| 体系架构 | 采用全分布式对称架构，元数据节点和数据节点融合部署，可实现业务不中断情况下扩充容量和性能。 |
| 存储服务 | 同一系统中并发提供文件、块、对象、HDFS四种存储服务，满足文件共享、云计算、大数据等业务访问，存储系统同时支持并配置Swift、S3、iSCSI、CIFS、NFS、FTP、HDFS、OpenStack Swift等协议，支持HDFS API。 |

**1.5网络资源池**

1、功能要求

（1）网络服务要求能实现动态的网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接。

（2）依照电子政务外网的安全域划分，云平台主要划分为政务服务区和互联网服务区。政务服务区主要是政务部门系统内和系统间的互访，互联网用户不能直接访问这个区域的数据和信息系统。互联网服务区部署政务部门的Web服务器，完成政务信息互联网发布和数据填报。

（3）云平台的计算平面、存储平面及应用服务网络整体设计和设备配置上均按照双备份要求设计。在网络连接上消除单点故障，提供设备的故障切换。关键网络设备之间的物理链路采用双路冗余连接，可靠性要求高于99.99%。

（4）从网络服务、数据应用业务的独立性、各业务的互访关系及业务的安全隔离需求综合考虑，将管理数据、网络数据、存储数据进行的存储、传输和交互进行有效隔离。

（5）提供电子政务外网接入访问服务，带宽不低于2Gbps,提供政务外网出口流量的实时监控，带宽根据实际需求进行动态扩展。(实际平均使用带宽/出口带宽≤0.6)

（6）云平台内部业务网带宽不少于10Gbps。FC-SAN存储网带宽不少于16Gbps。其他网络带宽不少于1Gbps。虚拟主机虚拟网卡支持带宽不低于1Gb/s。

（7）市级部门的业务通过逻辑隔离划分为不同的安全域，市级部门访问或管理业务系统可通过VPN等多种方式实现。

（8）互联网服务区与政务服务区之间通过安全数据交换系统进行数据交换。

（9）互联网服务区与政务服务区出口边界应通过访问控制设备建立边界。

（10）云服务商须为租户提供电子政务外网IP地址规划。

2、设备要求

云平台至少配置2台核心交换机、7台服务器业务接入交换机。

以下为单台设备的配置要求，云服务商可自行选型，但设备性能参数不得低于以下性能参数。

1. 表7--核心交换机配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| 核心交换机 | 1、多插槽严格前后通风散热的横式插槽机箱，业务板卡槽位数≥8个，交换矩阵板卡槽位≥6个，交换容量≥700Tbps，包转发性能≥140000Mpps，模块化冗余电源、模块化冗余风扇；支持在双机智能堆叠或者虚拟化模式下跨设备链路聚合；要求端口芯片级别缓存，每10G端口≥1.5MB；每插槽带宽≥2.6Tbps，提供工信部进网证书复印件；2、IPv4：支持静态路由，RIP V2，OSPF V2，ISIS,BGP,PBR，路由表≥64K；IPv6：支持静态路由，OSPF V3，ISIS,BGPv6，PBR；支持BFD （支持BGP,ISIS,OSPF,RIP,VRRP,PIM等)。3、支持与下连交换机的一体化管理，通过直连，可将下联交换机作为远程板卡来使用，降低管理复杂度,单台支持远程板卡≥64；可扩展支持MPLS-VPN，MPLS TE的硬件包转发；Layer-3 VPNs VRF数量≥4000。4、支持VxLAN L2/L3 gateway；单台支持虚拟为≥8台虚拟交换机，每个虚拟交换机拥有独立的配置和管理界面以及独立的管理IP地址；支持对交换机操作系统每个进程的故障隔离，系统进程可进行状态化或无状态化重启，不影响其他进程；必须支持模块化软件，即业务特性可根据命令控制来决定是否装入内存-RAM运行 (如BGP，OSPF 等)； |

1. 表8--服务器业务接入交换机配置要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| 接入交换机 | 1. 端口：≥48个10Gbps SFP+端口，≥6个QSFP28端口（支持作为40G或拆分为10G端口使用），≥1\*10/100/1000M电口，≥1个USB口2、交换容量≥23Tbps,三层包转发率≥1200Mpps，缓存≥16M3、端口到端口转发延迟平均≤1us，同时低时延转发模式下依然能够支持访问控制列表以及QoS等关键功能4、支持跨机箱的链路的端口捆绑, 且两台设备支持独立的控制平面，非堆叠设备，提供**有资质的检测机构**出具的测试报告

5、支持SDN,Openflow；支持VXLAN Routing and Bridging，支持Segment Routing；支持动态路由协议，RIP，EIGRP，OSPF，BGP等，路由表≥24K，支持组播，支持PIMv26、支持按需装载功能特性，例如OSPF，BGP等，可单个重启该进程，提供**有资质的检测机构**出具的测试报告7、电源：支持交流或直流电源，同一机箱支持交、直流电源混合，实现1：1冗余；风扇：支持可热插拔的冗余的风扇模块，支持严格前后送风，或者反方向的后向前送风，符合机房冷热风道设计要求 |

**1.6安全资源池**

1、平台安全要求

云服务商提供的云平台应满足国标GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》，实现信息安全等级保护第三级的防护要求，达到为政府部门提供云计算服务的基本安全能力。

云平台防护的边界是电子政务外网和互联网的出口。

云平台必须配置必要的运维审计设备，保证对所有运维操作的可溯源。

云平台安全由云服务商提供。

（1）表10--云平台安全基础设备配置要求

|  |  |
| --- | --- |
| 名称 | 性能和参数（以下表格内容为推荐配置，云服务商可根据三级等保要求自行选型） |
| 出口防火墙 | ≥4个万兆光口，≥4个SFP，≥4个GE。支持可选≥2个扩展槽。整机吞吐量≥40Gbps，启用IPS模块吞吐量≥18Gbps，启用防病毒模块吞吐量≥10Gbps。配置IPS，AV，QOS功能模块，支持链路负载均衡功能。配置SSL VPN功能，**支持license升级1年，**默认带10个并发授权。**★**提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
| 抗DDOS | 抗攻击能力不低于1.6Gbps。支持2对bypass，不低于4个10/100/1000M 电口。支持对流量型攻击、应用层攻击进行清洗、普通常见攻击的清洗，支持智能UDP防护，智能HTTP-CC防护、DNS防护。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
| 安全数据交换 | 标配内外网各≥2个GE业务接口，≥1个HA接口、≥1个管理接口。吞吐量不低于1000Mbps，通道数无限制。配置定制访问、文件交换、数据库同步、数据库访问、安全浏览、FTP访问、邮件传输等。支持主备部署，配置冗余电源。 |
| 运维审计系统（堡垒机） | 支持虚拟机环境中部署，使用虚拟机镜像模式部署。支持ISO和qcow2格式镜像方式部署，可根据具体要求进行修改。产品可管理设备数及用户数可分别进行设置，可满足最大可管理设备数授权100个，而运维用户数不少于50个。产品性能方面，图形和字符并发性能根据硬件配置的提升可以增加。支持手机短信、动态令牌、USBKey即动态口令卡等多因子认证，满足采用动态口令卡方式，标配5个口令卡。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |
| 安全审计 | 支持在硬件服务器或虚拟机环境中部署。日志审计对象授权标配100个，日志处理性能无限制。支持SNMP Trap、Syslog、FTP等多种方式完成日志收集功能。具备日志收集与分析IPV6功能。★提供由中国信息安全认证中心颁发的信息安全产品认证证书 |

（2）表11--云平台安全防护措施

|  |  |  |
| --- | --- | --- |
| 安全 类别 | 安全项 | 具体措施（以下表格内容为推荐措施，云服务商可根据三级等保要求自行采取措施） |
| 网络安全 | 网络结构安全 | 全冗余网络架构、不同安全等级的网络域划分、合理的路由及网段规划。 |
| 网络设备防护 | 网络设备加固，包括密码复杂度限制、登录地址限制、管理通道加密、双因子身份鉴别等。 |
| 访问控制 | 访问权限及访问规则管理，基于防火墙的系统隔离与访问控制。 |
| 网络安全审计 | 网络流量中操作行为监视及记录，危险事件分析及告警。 |
| 网络防病毒 | 网络边界部署防病毒网关，安装国产网络版杀毒软件，病毒库及时更新。 |
| 边界入侵防御 | 及时发现或阻断网络违规行为和未授权的网络访问。 |
| 可信接入 | 接入终端管理、终端授权认证、非法终端网络阻断、IP与MAC地址绑定。 |
| 主机安全 | 身份鉴别 | 口令复杂度限制、登录失败次数限制、管理通道加密、用户权限控制。 |
| 访问控制 | 资源访问权限控制、特权用户管理、、默认用户及多余账户锁定。 |
| 安全审计 | 操作系统及各种软硬件系统日志抓取及分析，针对安全事件、危险行为、重要系统命令使用进行告警。 |
| 资源控制 | 设定终端接入方式、网络地址范围等条件限制终端登录、限制单个用户对系统资源的最大使用限度。 |
| 恶意代码防范 | 主机安装防病毒软件。 |
| 存储安全 | 身份鉴别 | 设备访问控制。 |
| 存储系统安全 | 存储设备及系统冗余保护、细粒度存储空间访问授权、存储设备级数据加密。 |
| 存储访问控制 | 存储卷访问控制策略、存储交换机访问控制策略。 |
| 数据冗余保护 | 多种数据冗余机制，包括Raid，多副本，冗余纠删码。 |

2、租户安全

云服务商必须为租户提供虚拟web防火墙、虚拟防火墙、虚拟IDS、防病毒、日志审计、数据库审计、运维审计、应用负载均衡服务等安全服务以供租户选择，租户可通过云管平台按需选择安全服务内容。

（1）虚拟防火墙：支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制。支持IPv6安全控制策略设置。支持针对策略中的源、目的地址进行并发限制，可以针对单IP(或地址范围)进行并发控制。支持针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制。支持根据连接数对IP进行实时排行，支持基于IP、用户、协议、连接数、应用等方式统计会话。支持基于策略的入侵检测与防护、网络防病毒功能。

（2）虚拟web防火墙: IPV6安全策略防护和IPV6协议下邻居指定。能识别和阻断SQL注入攻击,Cookie 注入攻击，命令注入攻击，支持爬虫防护、扫描防护，支持文件上传、下载过滤，支持LDAP、XPATH、struct2/xworks检测和防护。应能识别阻断跨站脚本(XSS)注入式攻击，应能识别和阻断应用层拒绝服务攻击，非法上传阻断，包括WebShell攻击防护。应能识别和阻断敏感信息泄露、恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、缓冲区溢出攻击。能够针对基于HTTP/HTTPS协议的蠕虫攻击、木马后门、间谍软件、灰色软件、网络钓鱼、漏洞扫描等行为进行检测与防护。

（3）虚拟IDS：入侵检测系统具备实时发现网络攻击企图、攻击行为的入侵检测能力。通过网络数据监听及多样的告警机制帮助用户及时发现安全威胁事件的发生并采取相应措施。可对常见的端口扫描攻击、木马后门、蠕虫、拒绝服务攻击、缓冲溢出攻击、邮件服务器攻击、SQL注入攻击、CGI访问攻击、IIS服务器攻击、P2P、IM、网络游戏以及其他违规行为进行实时检测告警。

（4）防病毒：能够对已知、未知病毒、木马、恶意程序等进行检测、清除。具备公有云检测能力，并且公有云特征存储超过10亿。具备内部私有云建设能力，确保无法连接公有云时仍具备云查能力。具备压缩包查杀功能，支持25种解压缩格式，涵盖压缩包、安装包、文档格式解析能力。具备系统文件监控能力，能够监控计算机系统所有活跃文件的安全性。勒索病毒防护，能够对勒索病毒进行监控，拦截以及恢复受损文件。

（5）日志审计：无需另外安装软件组件，管理中心即可通过多种方式完成日志收集功能。可灵活定制不支持的数据源采集，而无须改动代码。具备日志范式化功能，实现对异构日志格式的统一化。支持对无用日志的自动过滤，减少垃圾数据数量。具有基于规则的安全事件关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息。支持按照天、月度、季度、年度等时间周期生成报表，并支持邮件自动投递。

（6）数据库审计：能够监视并记录对数据库服务器的各类操作行为，通过对数据的分析，实时地、智能地解析对数据库服务器的各种操作，并记入审计数据库中以便日后进行查询、分析、过滤，实现对目标数据库系统的用户操作的监控和审计。支持Oracle、MySQL、SQLServer等主流数据库的审计和保护功能。

（7）运维审计：支持针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计，记录会话、命令执行时间、会话协议、服务端IP、端口、客户端IP、操作命令、返回信息、运维、审批、资源账号等信息；支持针对RDP等图形终端操作的连接情况进行记录及审计，记录会话、命令执行时间、会话协议、服务端IP、客户端IP、端口、运维用户、资源账号等信息。

（8）应用负载均衡服务：通过设置虚拟服务地址，将添加的云主机虚拟成一个高性能、高可用的应用服务池，并根据转发规则，将来自客户端的请求分发给云服务器池中的云主机。负载均衡默认检查云服务器池中的云主机的健康状态，自动隔离异常状态的云主机，消除单台云主机的单点故障，提高了应用的整体服务能力。此外，负载均衡还具备抗DDoS攻击的能力，增强了应用服务的防护能力。

表12--租户安全服务目录

|  |  |
| --- | --- |
| 云安全服务 | 虚拟web防火墙 |
| 虚拟防火墙 |
| 虚拟IDS |
| 防病毒 |
| 日志审计 |
| 数据库审计 |
| 运维审计 |
| 应用负载均衡服务 |

**1.7虚拟私有云**

云计算数据中心支持虚拟私有云，支持在一个云数据中心中灵活设定多个虚拟私有云，配合网络的VPN技术或VXLAN技术，达到端到端的隔离效果。

用户可以在控制台创建私有网络，创建时需要同步创建初始子网，以方便向私有网络内添加云服务资源。新建私有网络要求用户指定私有网络和子网的CIDR网段，前期建设时需要为私有网络和子网留出足够的IP资源以防业务扩容导致网络资源不足。（提供截图证明）

**1.8容灾备份**

1、基本要求

为保证数据安全，云服务商须设计详细的容灾备份方案，制定可行的备份和恢复策略。满足业务系统虚拟主机镜像备份需求。提供虚拟主机备份恢复能力，支持基于磁盘的备份与恢复。

（1）数据级灾备：云服务商须具备数据级灾备环境，对租户业务系统数据提供数据级灾备。

（2）云服务商须为部门业务系统提供快照功能。

（3）云服务商与租户自主商定其业务系统的灾备方式。

（4）云服务商须承诺保证数据的安全性，未经政府授权，不得访问、修改、披露、利用、转让、销毁。

 （5）云服务商须为所有上云系统免费制作镜像备份，通过镜像可在三分钟内恢复业务系统。

2、其他要求

（1）支持Oracle、Oracle RAC、SQLserver、DB2、MySQL及国产主流数据库的备份，配置过程完全通过图形化界面，无需手工配置脚本文件。

（2）支持VMware、Hyper-V、KVM等多种虚拟化平台的无代理备份。

（3）支持全局重复数据删除，可以大幅度减少备份数据量。

（4）可以直接支持SAP、Lotus、Exchange等应用系统，轻松完成对应用数据的备份和恢复。

（5）支持针对对象存储产品进行备份。

（6）实现业务信息系统的整体备份，包括应用程序和数据资源。

（7）支持在线备份，能够保障数据的一致性和完整性，实现数据近零丢失。

（8）通过增量备份的方式降低容灾对存储和网络资源的需求。

（9）备份数据即时可用，可利用整机备份的数据即时恢复业务。

（10）在生产数据中心网络、应用系统、数据库、存储等不同环节故障时提供应用服务接管和恢复能力。

（11）支持不同品牌、不同型号的物理服务器或虚拟机恢复。

 表13--备份一体机配置要求

| 指标项 | 指标要求（以下表格内容为推荐配置，云服务商可根据灾备要求自行选型） |
| --- | --- |
| 基本功能 | 实现MYSQL数据库、SQL数据库和ORACLE数据库的备份与恢复。 |
| 裸容量 | **≥**80T。 |
| 处理器 | **≥**两颗Intel Xeon处理器。每颗≥10核。 |
| 缓存要求 | **≥**配置128GB高速缓存。 |
| 接口 | **≥**配置2个千兆接口及2个万兆接口。 |

**1.9云管理平台**

1、软件要求

云服务商需采用稳定可靠的云管理平台软件，完成搭建并提供服务，云管理平台软件需满足以下性能要求：

表14--云管理平台软件性能要求

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 扩展需求 | 云管理平台除能满足目前设备资源使用以及业务支撑需求，还需支持兼容平台现有硬件设备及未来在线扩展的需求。 |
| 接口需求 | 为满足采购人通过云监管平台实施统一管理的需要，云服务商必须无条件提供接口定制化开发服务，参与云监管平台与云服务商平台间监管接口规范的制定、开发、配合适配和联调等工作。 |
| 应用自动部署 | 云管理平台软件应为稳定可靠的最新商用版本并保证版本升级方便。另外，云管理平台软件需要提供应用自动化部署功能，方便用户通过自助界面进行使用。 |
| 需提供本地化支持 | 为保证云管理平台软件的实施质量和服务质量，云管理平台软件供应商需在项目实施过程及后期维护过程中全部提供本地技术支持和服务。 |
| 产品成熟度需求 | 云管理平台软件需自主可控并采用Openstack架构。 |
| 服务器动态扩展需求 | 云管理平台软件无需单独授权，当整个政务云平台的资源不足时，新的物理服务器资源可以自动被识别到并加入到平台的资源池中，而整个过程不应停止原有服务，且不对原有服务造成影响。 |
| 使用量可计量计费需求 | 云管理平台软件需对用户使用的资源如虚拟机、存储、IP、负载均衡、虚拟网络等资源的使用做到精细化管理并提供统计分析功能，根据用户需要提供资源计量报告。 |
| 软、硬件资源池化需求 | 云管理平台软件可以将现有的物理软、硬件资源进行资源池化。能够根据用户需求动态提供虚拟化的资源（虚拟机、存储、IP、负载均衡、虚拟网络等）。 |
| 虚拟机热迁移 | 当虚拟机所在硬件设备维护升级时能够实时的迁移到其它硬件设备上运行，而虚拟机中的服务不应停止。当原硬件设备维护升级结束后也可以将虚拟机从其他硬件中迁移回来，在迁移过程中服务正常运转。 |
| 虚拟机高可用 | 云管理平台软件应能够提供虚拟机冗余机制，当应用配置了高可用之后，应用虚拟机或虚拟机所在的物理机出现宕机情况时，云管理平台软件应支持自动切换至另外的其他虚拟机或物理机上，保证应用可用性，同时不应对虚拟机CPU数量做出限制。 |
| 故障自动迁移 | 平台所有的服务器都是以节点形式存在，一旦某节点出现硬件故障，云管理平台可以自动把运行在其中的应用自动在另外一个可用节点上启动。如果目标节点上也突然出现问题，应该可以自动寻找下一可用节点，直到服务被启动。理论上是只要不是所有的节点都损坏，系统可以自动保持应用的可用性。 |
| 按照策略调整运行资源 | 能够提供多种管理策略，帮助使用部门更容易调整资源配置和应用系统的运行位置。能够使服务器、存储等设备在故障修复、例行维修、迁移运行环境和节电休眠时能够更方便地进行调配。 |
| 资源自助管理界面 | 云管理面向租户提供自服务Portal。租户通过自服务Portal申请需要的各项云服务。申请过程支持多级流程审批，审批流程可个性化配置。 |
| 负载均衡服务 | 弹性负载均衡器是在Hypervisor上以虚机的方式实现的负载均衡功能，支持第4到7层的负载均衡，支持web服务、中间件、数据库以及其它互联网服务，可以实时测量服务器利用率和连接负载，在此基础上高效地分配统一应用业务负载，提供全面的可视性并有效地管理应用性能、安全性和服务交付。 |
| 虚拟私有云 | 云管理平台支持虚拟私有云功能，用户可以完全掌控自己的虚拟网络，包括申请弹性带宽/IP、创建子网、配置DHCP、设置安全组等。 |

云管理平台应向安全监管平台提供如下格式的接口以便安全监管平台对云平台进行监管：

接口支持Http、HTTPS、JDBC、SYSLOG 等业界标准协议。

对外提供RESTful 接口能力，支持分布式全文检索系统接口。

接口返回格式支持JSON。

数据开放方式包括：主动请求、被动接收、发布定阅等方式。

数据范围、接口使用方式等提供详细的说明描述文档。

2、硬件要求

云服务商应配置至少2台服务器用于云管理平台软件部署，必须保证各功能节点高可用性（资源负载率70%以下），云管理服务器参数要求如下。

以下为单台设备的配置要求，云服务商可自行选型，但设备性能参数不得低于以下性能参数。

表15--云管理平台服务器性能要求

|  |  |
| --- | --- |
| 指标项 | 指标要求（设备性能参数要求） |
| CPU | ≥2颗INTEL Gold 5118 CPU系列及以上CPU（≥12 核） |
| 内存数量 | ≥768G 内存 |
| 硬盘 | ≥SSD 960GB \*12，2\*600GB SAS硬盘； |
| RAID卡 | 八通道高性能 RAID卡，支持RAID 0/1 |
| 网络接口 | 至少Intel原厂I350双口千兆网卡（电口）\* 2，Intel 原厂82599 双口万兆网卡\*2，配置4个万兆光模块（多模） |
| 电源和风扇 | 配置冗余电源和风扇 |

**1.10传输链路**

云服务商提供冗余1Gbps连接电子政务外网的线路和2条不同运营商互联网接入线路，互联网出口总带宽支持2Gbps，并具备拓展能力。

**1.11主机托管**

云服务商平台须能提供标准42U服务器机柜用于物理设备托管服务。用户托管设备需纳入云管理平台进行统一监控和管理，托管设备的运维管理由云服务商负责。

基础软件

**1.12基础软件服务**

云服务商免费提供不限数量的开源Linux操作系统和MariaDB数据库等基础软件。

**（三）云服务目录报价要求**

1、云服务目录报价包括按照“GB 50174-2017”B级及以上机房要求的空间、消防、制冷、供电、监控等相应服务环境支撑费用。

2、云服务目录报价包括满足本期项目招标文件和服务期内国家相关法规文件所提出的网络、安全、备份、服务、运维等要求费用。

3、云服务商平台软件应具备灵活可靠的计费计量功能，并开放接口。云租赁服务商应该按市场情况，本次建设情况，提供如下格式的云资源单元报价表。

★4、**下表为单项最高限价，报价上浮为无效投标**

★5、云服务目录单元报价限价表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **明 细** | **计量单位** | **产品简介** | **报价品目代码** | **云服务目录最高限价（元）** |
| X86云服务器 | 物理内存（通用性） | GB·月 | ≥768 GB DDR4 内存，频率最高可达2933MT/s | P1 | 29 |
| 物理内存（高性能） | GB·月 | 物理内存DDR4，频率最高达4266MT/s | P2 | 32 |
| 虚拟CPU（通用性） | 核·月 | 配置INTEL Gold -5118系列及以上CPU（≥12 核,≥2.3GHz）（虚拟配比不超过1:4） | P3 | 22  |
| 虚拟CPU（高性能） | 核·月 | 配置INTEL\_GOLD-6132 系列及以上CPU（≥14 核，≥2.6GHz）（虚拟配比不超过1:4） | P4 | 24.5 |
| X86存储 | FC存储（SAS块存储） | TB·月 | 用来承载对IOPS要求较高的业务数据，支持SSD、SAS、SATA三种存储介质，并根据业务场景提供适合的IO性能。 | P5 | 462 |
| FC存储（SSD块存储) | TB·月 | P6 | 1175 |
| 分布式存储 | TB·月 | 承载如虚拟机系统、虚拟机镜像、ISO、虚拟机的模板文件、非结构化数据、大文件等 | P7 | 166 |
| 视频云存储 | TB·月 | 用来存储视频和图片等非结构化数据，这类数据规模大、保存时间长，并要求随时调用。面对这样的需求，传统的SAN或NAS在容量和性能的扩展上会存在瓶颈。视频云存储可以突破这些性能瓶颈，并且可以实现性能与容量的线性扩展 | P8 | 39  |
| 云备份服务 | TB·月 | 按照视频存储计费 | P9 | 39 |
| 托管 | 设备托管 | U·月 | 云服务商平台须能提供标准42U服务器机柜用于物理设备托管服务。用户托管设备需纳入云管理平台进行统一监控和管理，托管设备的运维管理由云服务商负责 | P10 | 360 |
| 42U机柜·月 | P11 | 4100 |
| 安全 | 等保二套餐 | 套/月 | 包含：虚拟防火墙（100M)、虚拟web防火墙（100M)、云主机安全(5节点）、日志审计(500G)、云堡垒机（5节点） | P12 | 3000.00  |
| 等保三套餐 | 套/月 | 包含：虚拟防火墙（100M)、虚拟web防火墙（100M)、主主机安全（5节点）、日志审计(500G)、数据库审计(2实例）、专业渗透测试服务（每月一次）、云堡垒机（5节点） | P13 | 7260.00  |
| GPU物理主机 | G1-T4\*8 | 台·月 | 机型：G1；GPU（NVIDIA Tesla T4）：8颗；CPU：24C；内存：384G；硬盘：7.2T，适用于深度学习推理、视频解析 | P14 | 15,020.83  |
| G2-V100\*4 | 台·月 | 机型：G2；GPU（NVIDIA Tesla V100）：4颗；CPU：24C；内存：192G；硬盘：7.2T，适用于深度学习、科学计算、高性能计算、图形渲染、视频解析 | P15 | 20,687.50  |
| 总计 | P16 | 52355.83 |

注：P16= P1+P2+P3+P4+P5+…+P15

**B、服务要求**

**（一）项目总体服务要求**

1、成交的云服务商运营主体应当接受安全监管中心监管，接受采购人的服务考核。

2、供应商必须承诺中标后30日内所提供的云中心机房在乐山本地部署，并具备服务能力。

3、云服务商必须搭建自己的运管平台，可实现云平台资源的网上申请、网上审批、网上核算，形成对自身云平台的计算资源、存储资源、网络资源、安全资源的监控和管理，并形成可视化展示。云管平台必须能基于 OpenStack 实现与云服务门户的对接，并接入到云管理中心。

4、云服务商必须承诺配合云平台上云单位业务应用及其数据迁移上云的工作。

5、云服务商须承诺在服务期结束后，配合各使用单位迁移应用系统，并提供**服务退出承诺书**原件。

6、云服务商必须承诺提供给云服务商的数据、设备等资源，以及云计算平台上政务系统运行过程中收集、产生、存储的数据和文档等数据资源均属政府所有。云服务商必须保障各政府部门对这些资源的访问、利用、支配。未经政府授权，不得访问、修改、披露、利用、转让、销毁数据。

7、云资源实际使用量由采购人组织专家团队核定。

8、云服务商的响应文件中必须明确设备品牌并详细列出功能参数。

9、云服务商的软硬件设备授权数、用户数不足时须主动扩展，不能因授权不足影响租户使用。

1. 云服务商必须按照采购人的要求，提供详细的建设实施方案。

**（二）项目运维服务要求**

1、运维总体要求

云服务商平台提供的服务应满足《信息安全技术 云计算服务安全能力要求》（GBT 31168-2014）、《信息安全技术 云计算服务安全指南》（GBT 31167-2014）、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14号）及国家主管部门发布的其他标准规范要求。

云服务商提供的服务总体应满足业务需求，确保云平台安全、稳定、可靠运行。

2、运维团队要求

云服务商需提供素质高、专业性强、经验丰富、稳定的运维团队，明确运维团队负责人，主要负责整个电子政务云平台的软硬件和网络运维，团队包括虚拟化工程师、网络工程师。云服务商需建设有严格的、有组织有纪律的管理运维流程，并指派专职接口人，团队需要7\*24在岗及时响应故障请求，负责电子政务云平台的故障受理、处理、跟踪、结果汇报等工作。

云服务商提供的运维团队成员须具备相应的资质，且需将运维团队的组织架构及人员名单报采购人同意和备案。

云服务商须提交《政务云平台应急预案》，须对运维人员进行培训，且每年应至少进行一次应急演练。

3、响应要求

云服务商须提供7\*24不间断技术服务支持时间。出现故障时 ，云服务商应启用相关备用设施设备， 确保系统正常运行。故障应在 60 分钟内排除。

4、保密要求

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

5、运维考核

为了保证云服务商提供的服务具备可靠性、稳定性，降低云平台对电子政务业务系统的影响和风险，必须符合运维服务考核标准与事故处理办法。云服务商每月向采购人提交《运维服务报告》，采购人按照《运维服务考核标准及办法》进行考核。

对运维服务不合格的云服务商采购人将采取服务费用扣除方式进行惩处（具体细节合同再行约定）。

运维服务考核标准及办法

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 考核内容 | 费用扣除标准 | 核验方式 |
| 运维制度 | 未建立完善的年度运维方案和应急预案，责任未明确到公司领导，发生重大变故时未及时更新方案并报采购人。 | 1000元/条 | 查验文件 |
| 未组建专业运维团队，未明确运维团队负责人，运维团队中无虚拟化工程师、运维工程师，有成员不具备政务云平台运维基本资质，有成员均未与运维公司就该项目签订专门的保密协议。 | 查验文件 |
| 运维团队未每月召开至少一次运维服务工作专题会议。 | 查验会议记录 |
| 未每年进行一次应急演练。 | 现场查验 |
| 信息报送 | 运维服务期间**每月、年**向采购人报送政务云运维信息和上云系统使用情况。报送信息应反映各单位上云系统运维管理情况和CPU、内存、磁盘等资源的实际使用率。 | 3000元/次（未报送） |  |
| 运维事件 | 三级故障（低）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、因服务商问题，导致云平台客户业务中断数量大于1个，少于5个；二、云平台1、云平台服务少于20%不可用三、基础设施1、网络性能下降小于50%2、核心设备出现故障 | 一次扣2000元 | 日志记录监管记录用户考评 |
| 二级故障（中）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、因服务商问题，导致政务互联网、政务外网或者专网客户业务中断数量超过5个二、云平台1、云平台服务超20%少于50%不可用三、基础设施1、部分设备断电2、网络性能下降50%或者部分网络中断 | 一次扣6000元 | 日志记录监管记录用户考评 |
| 一级故障（高）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、政务互联网、政务外网或者专网业务全部中断二、云平台1、云平台服务超50%不可用三、基础设施1、单机房完全断电(UPS供电正常不计为故障）2、政务互联网、政务外网或者专网全网中断； | 一次扣20000元 | 日志记录监管记录用户考评 |

以上考核细则将按照符合国家相关法律法规和符合项目实际需要的原则，进行不定期的修订完善，若有修订按修订后细则执行。

在政务云平台运维服务中，若对运维职责范围内的工作有任何异议，以服从采购人安排为先，事后双方再协商解决。

**C.商务要求**

**1、报价要求： 报价包含但不限于：**满足本期项目采购文件和服务期内国家相关法规文件所提出的网络、安全、备份、服务、运维等要求费用**、**及**场地费、链路费、人工费、资料费、利润、税金等**所有相关费用。

**2、项目实施要求**

**1)项目实施与管理**

云服务商应制定详细的项目运维计划，并提供项目运维人员保障方案。

**2)技术文档要求**

所有设备具备全套中文（或英文）技术文档手册、资料；投标方应提供与设备相关的所有技术文档和资料，并且均应以磁介质（或光盘）或纸张为载体。

**3、合同服务期限和地点**

服务期限：本项目服务期为1年度。

 履约地点：乐山市范围内

**4、付款方式**

**①乙方收取的服务费包含但不限于：平台软件硬件系统费用、场地费、链路费、人工费、资料费、利润、税金等。**

②云资源服务费按采购单价和实际分配资源量进行付费，结算方式:**签定合同后30个工作日内，甲方向乙方预付预算金额的10%(成交人为小微企业的，预付预算金额的30%），余下款项分两次支付，签订合同并提供服务后6个月内，第一次支付服务期起算日起至服务期满六个月后所产生的服务费用的70%；第二次在服务期结束后，根据服务考核情况支付尾款。**若验收时云服务商有不影响功能使用要求的负偏离，在结算时按合同约定扣款。甲方付款前，乙方应先向甲方开具等额增值税普票。

③上述款项的支付时间具体以财政部门将资金划拨到甲方账户时为准，且在到账后30个工作日内支付，乙方理解并同意。

**5、违约责任**

（1）甲乙（采购人与成交供应商，下同）双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。任何一方违约给对方造成的直接损失均负有赔偿责任，对方均有权视情况要求对方继续履行合同或提出解除合同；

（2）如因乙方在履行过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任；

如因乙方在提供服务过程中出现违规、违约等情形，有投诉或举报或验收时发现违规收费的，经核实属实的，扣减当季结算费用的1%，且甲方有权单方终止合同。

**6、争议解决办法**

1）甲乙双方就本协议所产生的任何争议都应该进行友好协商，协商解决不成的，任何一方均可向项目所在地有管辖权的人民法院提起诉讼；

2）诉讼费应由败诉方承担；

3）在诉讼期间，除正在进行诉讼的部分外，合同其他部分继续执行**。**

**四.第3包：算力政务云服务采购项目**

**A.采购内容**

**（一）**政务云平台服务清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目名称** | **服务内容** | **数量** |
| 1 | 机房环境 | （机房环境技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.1.机房环境”） | 1项 |
| 2 | 计算资源池 | （计算资源池技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.2. 计算资源池”） | 1项 |
| 3 | 存储资源池 | （存储资源池技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.3. 存储资源池”） | 1项 |
| 4 | 算法资源池 | （算法资源池技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.4. 算法资源池”） | 1项 |
| 5 | 网络资源池 | （网络资源池技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.5. 网络资源池”） | 1项 |
| 6 | 安全资源池 | （安全资源池技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.6. 安全资源池”） | 1项 |
| 7 | 虚拟私有云 | （虚拟是由云技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.7. 虚拟私有云”） | 1项 |
| 8 | 容灾备份 | （容灾备份技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.8. 容灾备份”） | 1项 |
| 9 | 云管理平台 | （云管理平台技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.9. 云管理平台”） | 1项 |
| 10 | 传输链路 | （传输链路具体内容要求详见“包3政务云平台服务技术要求”中“1.10. 传输链路”） | 1项 |
| 11 | 主机托管 | （主机托管技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.11. 主机托管”） | 1项 |
| 12 | 基础软件 | （技术软件服务技术服务要求具体内容要求详见“包3政务云平台服务技术要求”中“1.12. 基础出软件”） | 1项 |

**（二）政务云平台服务技术要求**

**标注“★”的条款为本项目的实质性条款，供应商须全部满足，不响应或不满足作无效响应处理。**

★云服务商必须承诺未来提供的云资源软硬件设备在功能和性能上均相当于或者优于本次投标产品。所有云资源软件系统必须为稳定可靠版本。若云服务商提供的设备不满足以上条件，采购人有权责令云服务商进行整改，如云服务商拒绝整改，采购人有权取消合同，由此造成的一切责任和后果由云服务商承担。

★政务云平台必须采用私有云模式搭建。

**1.1机房环境**

★（1）机房应具备环境智能监控，实现对设备电流量、UPS、精密空调、机房漏水、温度、湿度等的监控。机柜区域须配备专用门禁和24小时视频监控系统，视频监控画面可远程调用至安全监管中心，云服务商必须无条件开放接口或者提供监控服务，监控录像保存时间不少于3个月。

★（2）云服务商必须保证主机房设备（包括采购人托管设备）可持续获得电力供应（配备柴油发电机和UPS备用电池），每年持续电力供应时间在99.99%以上，以确保电子政务应用系统可持续工作，满足采购人对于信息化政务工作的要求。

（3）机房应按照GB50174-2017《数据中心设计规范》B级及以上级标准进行建设，云服务可用性应在99.99%以上。主机房整体面积≥150㎡（至少容纳25个47U标准服务器机柜），机房同地点处办公场地面积≥150㎡，其中机房监控室面积≥50㎡（配置不少5㎡的运维监控大屏）。机房、办公场地和机房监控室应具备拓展性。

**1.2计算资源池**

1、基础要求

（1）互联网服务区和政务服务区计算资源池需包含x86计算资源、ARM计算资源。

（2）云服务商需将服务器上架，测试，安装操作系统和虚拟化软件，连接到虚拟化存储池，创建虚拟文件系统，并将虚拟化服务器纳入云管理平台，包括安装和配置虚拟网络、配置虚拟交换机、配置虚拟机模板、安装操作系统及常用工具、安装常用的中间件模板、安装常用的数据库系统模板系统、配置虚拟机安全策略、日志监控、配置集群、配置自动迁移策略、配置资源池等工作。

★（3）计算节点和存储节点必须与交换设备实现双连接接入。

★（4）资源负载率应保持在75%以下。

2、云主机服务应具有以下功能

（1）单个云主机在创建时支持设置多个网卡，并且可以设置不同的IP地址。

（2）具备云主机生命周期管理，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。

▲（3）添加共享盘：支持创建共享盘，默认支持将共享盘挂载给最大16个ECS。**（提供产品彩页或者功能截图，并加盖投标人公章）**

▲（4）支持整机备份，一个云主机一个备份文件，支持基于多云硬盘一致性快照技术的数据保护，可以将备份数据恢复到初始主机。**（提供产品彩页或者功能截图，并加盖投标人公章）**

▲（5）云主机批量网络规划能力，可以指定虚拟机私有IP地址，并且批量创建时，可以指定连续的IP地址**（提供产品彩页或者功能截图，并加盖投标人公章）**

**1.3存储资源池**

存储池的设计包括块存储、对象存储、文件存储、云备份等服务；

云硬盘服务应具有以下功能

▲（1）云硬盘在线扩容，无需关机。**（提供产品彩页或者功能截图，并加盖投标人公章）**

（2）云硬盘备份支持自动备份策略。

（3）弹性扩展：云硬盘支持按需扩容，最小扩容步长为1GB，单个块存储可在卸载后扩容，单个云硬盘可由10 GB扩展至32 TB，满足业务增长对数据存储空间的需求。

（4）3副本冗余：数据持久性高达99.99999%

（5）安全可靠：系统盘和数据盘均支持数据加密，保护数据安全。云硬盘支持备份、快照等数据备份保护功能，为存储在云硬盘中的数据提供 可靠保障，防止应用异常、黑客攻击等情况造成的数据错误。

弹性文件服务应具有以下功能：

（1）支持客户的多个VPC虚机共享同一文件系统。

（2）弹性扩展：弹性文件服务可以根据用户的使用需求，在不中断应用的情况下，增加或者缩减文件系统的容量。一键式操作，轻松完成用户的容量定制。

（3）业务无中断：采用横向扩展分布式存储体系架构，扩容和减容时支持不停机情况下的数据自动迁移和均衡

（4）高性能、高可靠性：性能随容量增加而线性提升，同时通过采用纠删码技术进行数据冗余存储，保障数据的高持久度，满足业务增长需求。

对象存储服务应具有以下功能

▲（1）提供POSIX文件语义桶和客户端，可提供高性能、追加写、修改写、文件截断等功能。**（提供产品彩页或者功能截图，并加盖投标人公章）**

（2）对象存储提供日志记录功能，方便追查访问来源以及进行多维度的统计分析。用户开启一个桶的日志记录功能后，OBS会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶（即目标桶）中。

（3）提供RESTful接口，支持http和https协议访问。提供用户自服务门户和API接口，用户可自行完成数据的上传下载和管理。

（4）支持用户、用户组、桶访问权限，支持桶和对象的ACL（支持租户、匿名用户、日志管理用户等读写权限，并且支持Policy策略，进行复杂的权限设置，如：对象前缀后缀，各自操作的权限均可设置）

★服务期间磁盘故障更换时，云服务商应首先向采购人提出故障磁盘消磁处理申请，经采购人书面同意后对故障磁盘应做消磁处理。服务期满后，存储系统及介质的处置，云服务商亦需经过采购人书面同意。

**1.4算法资源池**

多场景应用使用全球先进算法为多种高频场景：人脸识别、车牌识别、防汛点位监测预警、森林防火预警监测、地址灾害预警监测、区域车辆闯入预警、区域人员闯入预警、人群集聚预警、占用消防通道预警、船舶违停预警、交通拥堵预警等关联视频结构化分析为场景应用提供基础数据支持。

视频结构化算法应用中台支持算法仓：

人脸识别算法、人体识别算法、车辆识别算法、非机动车辆识别算法、物体识别算法、内涝积水检测识别算法、违停识别算法、区域人员闯入识别算法、区域车辆闯入识别算法、河道船舶违停识别算法、人群聚集识别算法、口罩识别算法、打架闹事识别算法、交通拥堵识别算法、消防通道占用识别算法、占道经营识别算法、垃圾堆放识别算法、疫情管控、医闹人员管控、黄牛人员管控、邪教人员管控、六类人员管控、独居老人智慧养老、河道水域水位检测、河道违停、堆放大量可燃物检测、外来入侵检测、水污染检测、安全工地检测、生态环境污染检测、渣土车滴漏、高空抛物、乱堆垃圾、垃圾外溢、井盖确实、牛皮癣广告、乱发传单等算法。

算法中台软件功能：

1、提供基于Linux运行环境的应用系统，支持不少于90路前端的综合应用中台解析比对授权；

2、支持对实时视频流进行人员、车辆、场景应用等活动目标的特征属性信息结构化提取，并按人脸、人体、车辆和非机动车展示抓拍照；支持算法支持：内涝积水检测预警算法、车辆灾情发生点及时间检测预警算法、船舶河道占用违停检测算法、人群集聚算法、消防通道占用检测算法等。

3、系统应能根据视频内人脸两眼间距像素数进行人脸图片选优，误选率应＜5%,漏选率＜1%。

4、支持对水平转动角不超过±75°、俯仰角不超过±45°及两眼瞳间距不大于15像素点的视频或图片进行人脸分析功能；

5、支持分析路人的年龄、年龄段，种族属性，性别，是否戴口罩，是否戴眼镜，是否有刘海，是否维族人；支持检出性别、上身颜色、上身款式、下身颜色、下身款式、有无帽子、是否戴黑镜、是否戴口罩等结构化信息；

6、支持对视频中车辆自动捕获、跟踪和抓拍的功能。可以提取视频中的车辆数据，包括车牌、车型、颜色、方向等特征属性信息。

7、以脸搜脸首位命中率不低于98%。；

8、系统应具备动态布控功能。在布控库规模为100万、动态布控的非黑名单误报率≤2%条件下，布控的黑名单漏报率应＜4%，准确率应＞96%。

9、支持告警记录功能，包括：告警记录保存；告警记录导出；告警记录级联推送；按照不同告警相似度查看告警记录；按照告警记录关联布控人员详情；按照告警记录关联抓拍人员详情；按照告警记录关联现场照片；

10、支持报警规则设置功能：可设置弹窗提醒、声音提醒、报警类型和报警颜色。具有抓捕类、监控类和提示类三种布控结果的处置类型；

11、系统应具备宏观数据分析功能。应支持实时更新抓拍照片数量、汇聚档案数量、区域内风险人群的统计数据及人员的位置信息。

13、支持档案汇聚功能。支持8000万底库照片实时汇聚档案功能。

14、支持根据人脸相似度对人脸照片进行人脸归档功能，在8000万实名档案规模下，归档准确率应＞99.9%，召回率＞99.9%。

15、档案查询能力：支持查询360天档案数据，查询结果返回平均时间≤2秒。

16、支持通过监控模块监控整个平台运行状态，可在界面上显示服务器ID，IP，CPU占用，内存占用，磁盘占用百分比等监控信息；

17、支持记录日志权限授予、用户刷脸登录、用户对摄像头操作、人像检索、人像库图片操作等事件形成日志；系统日志具有防篡改功能，且可锁定，无法被删除。

18、**上述17项**指标要求须提供具有资质的检测机构出具的检测报告复印件并加盖**投标人公章**予以证明，未提供证明视为负偏离。

调度算法仓

|  |  |  |
| --- | --- | --- |
| 算法类型 | 算法名称 | 说明 |
| 人物算法 | 人群聚集算法 | 检测指定区域内人数大于指定人数且持续时间超过指定时间 |
| 快速移动算法 | 检测移动速度超过指定阈值的人 |
| 打架算法 | 检测双人靠近，有身体接触的挥拳打架 |
| 打电话算法 | 检测单手拿手机在耳朵旁打电话 |
| 打标语算法 | 检测双手上举10秒以上，且手未被标语遮挡的行为 |
| 偷拍检测算法 | 检测举手机的人 |
| 绊线数人数算法 | 划线且指定绊线方向，统计越过线的人数 |
| 物品算法 | 物品遗留算法 | 检测物品的主人离开物品一段距离，并持续一段时间 |
| 垃圾检测算法 | 检测丢垃圾的行为 |
| 积水检测算法 | 检测影响行人、机动车正常交通的路面积水 |
| 船舶违停检测算法 | 检测特定两点位的船舶 |
| 动作算法 | 车辆违停算法 | 检测指定区域车辆静止时间超过指定时间 |
| 骑车未戴头盔算法 | 检测没有佩戴头盔的骑车人 |
| 区域入侵算法 | 检测进入指定区域的人 |
| 持刀检测算法 | 检测持刀的人，当前版本检测明显的菜刀和水果刀 |
| 徘徊检测算法 | 检测停留时间超过指定时间的人 |
| 摔倒检测算法 | 检测处于摔倒的状态的人员 |
| 绊线入侵算法 | 检测越过指定线的人 |
| 人群逆流算法 | 指定正方向，检测和正方向相反的人 |
| 态势算法 | 区域人数统计算法 | 指定区域内实时的人数统计 |
| 敏感区域出现幼儿算法 | 指定区域内出现幼儿 |
| 人员配备不合规算法 | 指定区域内幼儿/成人比例超过了7:1 |

**1.5网络资源池**

（1）网络服务要求能实现动态的网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接。

（2）依照电子政务外网的安全域划分，云平台主要划分为政务服务区和互联网服务区。政务服务区主要是政务部门系统内和系统间的互访，互联网用户不能直接访问这个区域的数据和信息系统。互联网服务区部署政务部门的Web服务器，完成政务信息互联网发布和数据填报。

（3）云平台的计算平面、存储平面及应用服务网络整体设计和设备配置上均按照双备份要求设计。在网络连接上消除单点故障，提供设备的故障切换。关键网络设备之间的物理链路采用双路冗余连接，可靠性要求高于99.99%。

（4）从网络服务、数据应用业务的独立性、各业务的互访关系及业务的安全隔离需求综合考虑，将管理数据、网络数据、存储数据进行的存储、传输和交互进行有效隔离。

（5）提供电子政务外网接入访问服务，带宽不低于2Gbps,提供政务外网出口流量的实时监控，带宽根据实际需求进行动态扩展。(实际平均使用带宽/出口带宽≤0.6)

★（6）云平台内部业务网带宽不少于10Gbps。虚拟主机虚拟网卡支持带宽不低于1Gb/s。

（7）市级部门的业务通过逻辑隔离划分为不同的安全域，市级部门访问或管理业务系统可通过VPN等多种方式实现。

（8）互联网服务区与政务服务区之间通过安全数据交换系统进行数据交换。

（9）互联网服务区与政务服务区出口边界应通过访问控制设备建立边界。

（10）云服务商须为租户提供电子政务外网IP地址规划。

**1.6安全资源池**

1、平台安全要求

★云服务商提供的云平台应满足国标GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》，实现信息安全等级保护第三级的防护要求，达到为政府部门提供云计算服务的基本安全能力。

云平台防护的边界是电子政务外网和互联网的出口。

云平台必须配置必要的运维审计设备，保证对所有运维操作的可溯源。

★云平台安全由云服务商提供。

表8--云平台安全防护措施

|  |  |
| --- | --- |
| 指标项 | 指标能力 |
| 基本能力 | 提供符合安全等保三级的云平台安全基础设施服务。服务项目含流量监测与清洗、边界防火墙、入侵检测、SSL VPN运维通道、漏洞扫描、日志审计、网络防毒、运维审计、主机安全、补丁服务器和安全威胁分析等能力。安装国产网络版杀毒软件，病毒库及时更新。 |
| 安全流程 | 提供漏洞扫描管理和事件响应流程，应急预案。 |

2、租户安全

云服务商必须为租户提供态势感知、主机安全、漏洞扫描、云堡垒机、数据库安全、Web应用防火墙、容器安全等安全服务以供租户选择，租户可通过云管平台按需选择安全服务内容。

|  |  |  |
| --- | --- | --- |
| 安全中心-主机安全 | 支持可扩展性 | 支持多公有云、私有云与本地数据中心混合部署，既支持物理机也支持虚拟机。 |
| 支持高可用性 | 服务节点支持集群部署，服务客户端性能消耗低（1%），不影响主机上的业务。 |
| 主机资产管理 | 资产管理：支持收集并展示账号、开放端口、进程、Web目录、软件等主机资产信息，帮助用户进行监控和管理 |
| 支持双因子认证 | ▲双因子认证：支持结合短信/邮箱验证码，对云服务器登录行为进行二次认证，极大地增强云服务器账户安全性**（提供产品彩页或者功能截图，并加盖投标人公章）** |
| 账户暴力破解防护 | 账户暴力破解防护：检测账户遭受的口令破解攻击，对识别出的攻击源IP封锁24小时，禁止其再次登录，防止主机因账户破解被入侵  |
| 异地登录检测 | 检测主机异地登录行为并进行告警  |
| 网站后门检测 | 检测云服务器上Web目录中的文件，判断是否为 WebShell木马文件 |
| 恶意程序检测  | 恶意程序检测 （病毒云查杀）：使用三重检测算法：恶意程序库（查杀已知恶意程序）+图像指纹算法（基于AI查杀变种）+病毒云查杀（多款杀毒引擎查杀未知病毒），对运行的进程进行检测，识别出其中的病毒、木马、后门、蠕虫和挖矿软件等，并提供一键隔离查杀能力。 |
| 关键文件变更检测  | ▲关键文件变更检测 ：对于系统关键文件（例如：ls、ps、login、top等）进行监控，一旦文件被修改就进行告警，提醒用户关键文件存在被篡改的可能**（提供产品彩页或者功能截图，并加盖投标人公章）** |
| 网页防篡改 | 使用第三代网页防篡改技术，内核级事件触发技术，锁定用户目录下的文件后，有效阻止非法篡改行为。 |
| 篡改监测自动恢复技术，在主机本地和远端服务器上实时备份已授权的用户所修改的文件，保证备份资源的时效性。当企业主机安全服务检测到非法篡改行为时，将使用备份文件主动恢复被篡改的网页。 |
| 基线检查  | 口令复杂度策略检测 ：检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性  |
| 弱口令检测：使用最新的常见弱口令字典，对系统帐户进行口令扫描，检测出其中的弱口令，提示用户修改，可防止帐户口令被轻易猜解。 |
| 风险账号检测：检测系统中是否存在黑客的影子账号，克隆账号等风险账号  |
| 配置检测 ：对常见的Tomcat配置、Nginx配置、SSH登录配置进行检查，帮助用户识别不安全的配置项，支持的应用有SSH、RDP、SMB、MYSQL、MSSQL、MongoDB、Redis、Oracle、DB2、GaussDB、Postgres、Telnet。 |
| 安全中心-漏洞扫描★提供由中国信息安全认证中心颁发的信息安全产品认证证书 | 提供云化漏洞扫描 | 提供云化漏洞扫描功能，支持集群扩展、支持同时对多个站点进行扫描； |
| 主机漏洞扫描 | 支持操作系统漏洞检测与管理，包括主流Window与Linux系统 |
| 支持软件漏洞检测与管理，例如：SSH、OpenSSL、Apache、Mysql等存在的漏洞 |
| 支持Web-CMS漏洞检测与管理：通过对Web目录和文件进行检测，识别出Web-CMS漏洞，提升Web服务安全性 |
| 支持主机等保合规扫描，呈现主机配置是否满足等保的合规要求； |
| 网站漏洞扫描 | 提供网站漏洞扫描能力，可扫描的漏洞类型包括Owasp、WASC等，支持Web2.0、AJAX、各种脚本语言、PHP、ASP、.NET和Java环境，支持多种认证方式（Cookie、Password等），支持代理、HTTPS扫描；提供WEB漏洞修复建议，支持下载报告； |
| 支持扫描规则云端自动更新，全网生效，及时涵盖最新爆发的漏洞 |
| 支持HTTPS网站扫描。 |
| ▲支持对Web页面中恶意链接的扫描能力；（提供控制台截图并加盖投标人公章） |
| 支持网站目录结构发现能力，扫描之后可呈现出网站目录结构 |
| 提供漏洞扫描任务管理能力，提供同时对多个站点进行扫描的能力，支持定时扫描，自定义扫描深度；支持智能调速，可通过动态监控网络时延，调整发送攻击报文的频率，最小程度影响用户站点服务； |
| Web应用防火墙★提供由中国信息安全认证中心颁发的信息安全产品认证证书 | Web基础防护 | 针对OWASP top攻击进行安全防护，包括XSS、SQL注入、命令注入、CSRF、代码注入、远程溢出攻击、Webshell检测（上传木马）等；支持CC防御、数据防爬虫、自定义防护策略等；使用双引擎，语义分析+规则防护，误报率更低； |
| 支持多种注入攻击防护（包括SQL注入、命令注入、LDAP注入攻击防护、跨站脚本攻击防护(XSS)、XML/Xpath注入攻击、命令/代码注入） |
| 支持目录攻击防护（支持对目录的访问控制，支持路径遍历攻击防护） |
| 支持恶意扫描防护（支持防爬虫、防扫描工具恶意扫描、防应用扫描） |
| 支持多维度CC防御 | ▲支持基于IP/Cookie/Referer的多维度CC防御，支持人机验证；支持用户自定义拦截页面；支持CSRF防盗链场景**（提供控制台截图并加盖投标人公章）** |
| 泛域名防护 | ▲支持对泛域名（\*.abc.com类）防护，其中\*可以是任意字符串**（提供控制台截图并加盖投标人公章）** |
| 安全可视化 | 支持实时查看攻击信息和事件日志，实时查看访问次数、安全事件的数量与类型、详细的日志信息 |
| 支持集中配置策略，快速下发，快速生效 |
| 精准访问防护 | 基于丰富的字段和逻辑条件组合，精确自定义访问控制策略。字段条件包括IP、URL、Referer、User Agent、Params、Header等HTTP常见参数，可组合包含、不包含、等于、不等于、前缀为、前缀不为等逻辑条件，设置阻断或放行策略。 |
| 扫描器爬虫防护 | 支持自定义扫描器与爬虫规则，用于阻断非授权的网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。 |
| 网站防爬虫 | 动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。 |
| 防逃逸 | ▲支持防逃逸，至少支持对web攻击的url\_encode，Unicode编码，xml编码，C-OCT编码，十六进制编码，html转义编码，base64编码，大小写混淆，javascript、shell、php等拼接混淆编码的还原能力**（提供控制台截图并加盖投标人公章）** |
| 黑白名单设置 | 支持添加始终拦截与始终放行的黑白名单IP，增加防御准确性。 |
| 地理位置封禁 | 能够基于IP的地理位置来源如海外国家、国内省份，设置访问、阻断的策略，快速实现海外IP访问的封禁场景。 |
| 网页防篡改 | 支持静态文件的防篡改，保证返回给客户正常页面内容，并随机检测网页是否被篡改。 |
| 误报屏蔽 | 针对特定请求忽略某些攻击检测规则，用于处理误报事件。 |
| 隐私屏蔽 | 支持用户自定义隐私屏蔽策略，对隐私参数进行匿名化处理，当隐私数据（如用户名、密码）出现在攻击负载中，也不会被平台侧记录，最大化保障用户隐私；  |
| 防敏感信息泄露 | 防止在页面中泄露用户的敏感信息，例如：用户的身份证号码、手机号码、电子邮箱等。 |
| 支持PCI DSS合规配置 | ▲支持PCI DSS合规配置，在域名级别实现对TLS版本、SSL Ciphers加密套件的自定义配置**（提供控制台截图并加盖投标人公章）** |
| 支持虚拟补丁一键下发 | 针对业界爆发的高危web漏洞，提供快速分析漏洞、向引擎下发漏洞防御规则的支持，保障0day漏洞及时在waf打上虚拟补丁，客户无感知； |
| HTTPS防护 | 支持HTTPS业务的防护，支持源站为HTTP通过WAF以HTTPS发布业务的防护 |
| 重定向 | 支持http到https的相同域名的重定向 |
| 非标准端口 | 除标准的80，443端口外，还支持以169个非标准端口对外发布服务 |

**1.7虚拟私有云**

1、基本要求

虚拟私有云（Virtual Private Cloud，VPC），为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。租户可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。租户可以通过VPC方便地管理、配置内部网络，进行安全、快捷的网络变更。同时，租户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

2、其他要求

（1）支持按需创建使用虚拟专有网络；在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。用户可以通过VPC方便地管理、配置内部网络，进行安全、快捷的网络变更。同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

（2）▲支持跨账号打通不同vpc，vpc可以子网重叠。**（提供产品彩页或者功能截图，并加盖投标人公章）**

（3）支持设置高可用的虚拟IP，且虚拟IP可绑定EIP访问公网。

**1.8容灾备份**

1、基本要求

为保证数据安全，云服务商须设计详细的容灾备份方案，制定可行的备份和恢复策略。满足业务系统虚拟主机镜像备份需求。提供虚拟主机备份恢复能力，支持基于磁盘的备份与恢复。

（1）数据级灾备：云服务商须具备数据级灾备环境，对租户业务系统数据提供数据级灾备。

（2）云服务商须为部门业务系统提供快照功能。

（3）云服务商与租户自主商定其业务系统的灾备方式。

★（4）云服务商须承诺保证数据的安全性，未经政府授权，不得访问、修改、披露、利用、转让、销毁。

 （5）云服务商须为所有上云系统免费制作镜像备份，通过镜像可在三分钟内恢复业务系统。

2、其他要求

（1）自动备份：通过备份策略周期性为云服务器/云硬盘创建自动备份

（2）手工备份：手工触发自动备份策略，为云服务器/云硬盘创建即时备份

（3）数据恢复：使用备份将云服务器/云硬盘恢复到历史时间点

（4）备份创建镜像：通过云服务器备份创建整机镜像，使用镜像发放新的云服务器

（5）快速恢复：使用云服务器备份创建镜像发放新的云服务器时，支持即时恢复，恢复时间可缩短到分钟级

**1.9云管理平台**

1、软件要求

云服务商需采用稳定可靠的云管理平台软件，完成搭建并提供服务，云管理平台软件需满足以下性能要求：

表17--云管理平台软件性能要求

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 云服务 | 提供云服务管理控制台Console，租户登录Portal门户，使用自助Portal提供的各种云服务。所有的服务都以Console或者API/SDK的形式提供。 |
| 多租户 | 云服务支持组织和个体以相互隔离的租户使用云服务，每个租户按需使用资源，不会感知其他租户的存在，多租户同时保证租户间数据的安全隔离。 |
| 按需自助服务 | 租户可以通过服务控制台查看和申请所有的云服务。 |
| 网络传输 | 云服务均提供Web Console和API SDK两种访问方式，两种方式均通过标准的HTTP进行网络传输。 |
| 弹性伸缩 | 云服务均提供从基础到高级多种规格供选择，已经申请的服务实例也方便变更规格，支持随需扩展和弹性伸缩，从而满足不同业务应用所需。 |
| 虚拟化内核 | 基于KVM虚拟化内核把计算、存储、和网络安全设备虚拟化成逻辑的虚拟资源池，通过标准API接口对接云服务层，支持虚拟化集群的大规模扩展。 |
| 租户Portal | 支持租户通过租户门户portal登录，在服务控制台创建、使用和删除云服务的资源，并且在租户门户、帮助中心查询了解相关信息。 |
| 运维管理 | 告警概况：展示云服务状态、历史告警TOP10、告警趋势主机概况：展示正常物理机数量、异常物理机数量容量概况：展示块存储资源使用趋势（呈现总量、使用量等维度的使用趋势）、云主机资源（云主机虚拟机个数、物理服务器台数趋势、vCPU个数趋势、内存大小趋势） |
| 运维监控 | 云服务级监控：展示云服务错误率、云服务QPS、云服务平均响应时长云服务级监控项趋势：展示客户端错误率趋势、服务端错误率趋势、平均响应时长趋势组件级监控：展示平均CPU使用率、平均内存使用率、平均FHCount、平均SWAP组件级监控趋势：展示CPU使用率趋势、内存使用率趋势、FHCount趋势、SWAP趋势 |
| 告警管理 | 当前告警和历史告警：呈现告警ID、告警时间、告警名称、告警状态、告警级别、所属云服务/服务/微服务、告警数据源、告警信息、告警详情等字段 |
| 资源监控 | 云主机容量：云主机资源vCPU容量（资源类型维度）、云主机资源内存容量（资源类型维度）、云主机的vCPU资源使用趋势、云主机的内存资源使用趋势、云主机的物理机资源使用趋势、云主机虚拟机资源容量（资源类型维度）、云主机虚拟机资源容量趋势块存储容量：高IO当前容量、超高IO当前容量、高IO资源使用趋势、超高IO资源使用趋势对象存储容量：对象存储当前容量、对象存储容量使用趋势 |

★云管理平台应提供不低于如下能力：

（1）云平台管理节点须支持集群部署，可平滑升级扩展。

（2）云平台须提供自服务门户，便于使用单位申请、管理云资源，通过云管理平台的资源自助式服务门户实现资源的按需获取。

（3）云平台须提供功能完整、架构完善、体系完备的服务能力。使用通用X86服务器硬件、国产ARM服务器硬件，云平台应采用Openstack架构，通过标准接口实现对底层计算、存储、网络、安全等资源进行统一管理。

（4）云平台所提供的云主机产品，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、数据盘大小等；配置升级生效时间在10分钟以内。

**1.10传输链路**

★云服务商提供2条1Gbps连接电子政务外网的不同运营商电路和2家不同运营商互联网接入出口，互联网出口总带宽不少于2Gbps，并具备拓展能力。同时，云服务商需要提供将来为同城不同云服务商之间互为备份提供对等链路和出口。

**1.11主机托管**

云服务商平台须能提供标准47U服务器机柜用于物理设备托管服务。用户托管设备需纳入云管理平台进行统一监控和管理，托管设备的运维管理由云服务商负责。

**1.12基础软件**

★云服务商免费提供不限数量的主流发行版开源Linux操作系统。

**（三）云服务目录报价要求**

1、云服务目录报价包括按照“GB 50174-2017”B级及以上机房要求的空间、消防、制冷、供电、监控等相应服务环境支撑费用。

2、云服务目录报价包括满足本期项目招标文件和服务期内国家相关法规文件所提出的网络、安全、备份、服务、运维等要求费用。

3、云服务商平台软件应具备灵活可靠的计费计量功能，并开放接口。云租赁服务商应该按市场情况，本次建设情况，提供如下格式的云资源单元报价表。

★4、**下表为单项最高限价，报价上浮为无效投标**

★5、云服务目录单元报价限价表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 服务大类 | 云服务类别 | 规格 | 量纲 | 报价品目代码 | 云服务目录最高限价（元） |
| 计算服务 | 虚拟CPU | 配置不低于2.6GHz/22Core,虚拟配比不超过1:2。 | 核/月 | P1 | 49 |
| 或者信创服务器（可提供专享云服务） |
| 内存（高性能） | DDR4 2400MHZ，最高可达4266MT/s. | GB/月 | P2 | 32 |
| 裸金属物理机 | 2\*6278 CPU，12\*16GB 内存，无硬盘，1\* SDI3.0  | 台/月 | P3 | 6000 |
| GPU物理机1 | CPU：2\*6278;内存：384GB;本地存储:2\* 480G SATA SSD+1\*1600G NVMe SSD;GPU：6\*16G-T4 GPU;网卡：2\*Hi1822; | 台/月 | P4 | 20000 |
|
|
| GPU物理机2 | CPU：2\*5118;内存：256GB：2 \*600GB硬盘：1 \* 1.2TB SAS；4 \* T4 GPU | 台/月 | P5 | 12500 |
| 视频解析算力 | 虚拟GPU、AI算力，应用解析算力资源按照单路视频结构化解析计算调度节点算力 | 路/月 | P6 | 390 |
| 存储服务 | 块存储 | SAS云硬盘，X86/信创 | TB/月 | P7 | 470 |
| 块存储 | SSD云硬盘，X86/信创 | TB/月 | P8 | 1180 |
| 文件存储 | 文件存储容量，X86/信创 | TB/月 | P9 | 230 |
|
| 对象存储 | 对象存储容量，X86/信创 | TB/月 | P10 | 110 |
| 安全服务 | 等保二套餐 | 主机安全（3节点），日志审计（20数据源），云堡垒机（3节点） | 套/月 | P11 | 3100 |
| 等保三套餐 | 虚拟web防火墙（100M），主机安全（3节点），日志审计（20数据源），数据库审计（3实例），云堡垒机（3节点） | 套/月 | P12 | 7360 |
| 托管服务 | 设备托管 | 设备托管（国家A级，国际T3+，五星级数据中心机房） | U/月 | P13 | 360 |
| 机柜托管 | 机柜托管（国家A级，国际T3+，五星级数据中心机房） | 47U机柜/月 | P14 | 5000 |
| 总计 |  | P15 | 56781 |

注：

P15=P1+P2+P3+P4+P5+P6+P7+P8+P9+P10+P11+P12+P13+P14

**B、服务要求**

**（一）项目总体服务要求**

1、成交的云服务商运营主体应当接受安全监管中心监管，接受采购人的服务考核。

2、云服务商必须搭建自己的运管平台，可实现云平台资源的网上申请、网上审批、网上核算，形成对自身云平台的计算资源、存储资源、网络资源、安全资源的监控和管理，并形成可视化展示。

3、云服务商必须承诺配合云平台上云单位业务应用及其数据迁移上云的工作。

4、云服务商须承诺在服务期结束后，配合各使用单位迁移应用系统，并提供服务退出承诺书原件。

5、云服务商必须承诺提供给云服务商的数据、设备等资源，以及云计算平台上政务系统运行过程中收集、产生、存储的数据和文档等数据资源均属政府所有。云服务商必须保障各政府部门对这些资源的访问、利用、支配。未经政府授权，不得访问、修改、披露、利用、转让、销毁数据。

6、云资源实际使用量由采购人组织专家团队核定。

7、云服务商的软硬件设备授权数、用户数不足时须主动扩展，不能因授权不足影响租户使用。

8、云服务商的主机房和异地灾备机房在正式启用之前需向采购人提供相关设备的技术文档，采购人将组织专家团队对其进行验收，验收合格方可正式启用。

9、云服务商必须按照采购人的要求，提供详细的建设实施方案。

**（二）项目运维服务要求**

1、运维总体要求

云服务商平台提供的服务应满足《信息安全技术 云计算服务安全能力要求》（GBT 31168-2014）、《信息安全技术 云计算服务安全指南》（GBT 31167-2014）、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14号）及国家主管部门发布的其他标准规范要求。

云服务商提供的服务总体应满足业务需求，确保云平台安全、稳定、可靠运行。

2、运维团队要求

云服务商需提供素质高、专业性强、经验丰富、稳定的运维团队（初期人数不低于5人，后期随政务云规模增长而增加），明确运维团队负责人，主要负责整个电子政务云平台的软硬件和网络运维，团队包括虚拟化工程师、运维工程师、网络工程师。云服务商需建设有严格的、有组织有纪律的管理运维流程，并指派专职接口人，团队需要7\*24在岗及时响应故障请求，负责电子政务云平台的故障受理、处理、跟踪、结果汇报等工作。

重要节日、重大活动、重要事件期间，云服务商须增加2名以上运维服务工程师驻场运维，确保政务云平台安全、稳定运行。

云服务商提供的运维团队成员须具备相应的资质，且需将运维团队的组织架构及人员名单报采购人同意和备案。

云服务商须提交《政务云平台应急预案》，须对运维人员进行培训，且每年应至少进行一次应急演练。

3、响应要求

云服务商须提供7\*24不间断技术服务支持时间。出现故障时 ，云服务商应启用相关备用设施设备， 确保系统正常运行。一般故障应在 30分钟内排除故障，重大故障应在 60 分钟内排除。

4、保密要求

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

5、运维考核

为了保证云服务商提供的服务具备可靠性、稳定性，降低云平台对电子政务业务系统的影响和风险，必须符合运维服务考核标准与事故处理办法。云服务商每月向采购人提交《运维服务报告》，采购人按照《运维服务考核标准及办法》进行考核。

对运维服务不合格的云服务商采购人将采取服务费用扣除方式进行惩处（具体细节合同再行约定）。

运维服务考核标准及办法

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 考核内容 | 费用扣除标准 | 核验方式 |
| 运维制度 | 未建立完善的年度运维方案和应急预案，责任未明确到公司领导，发生重大变故时未及时更新方案并报采购人。 | 1000元/条 | 查验文件 |
| 未组建专业运维团队，未明确运维团队负责人，运维团队中无虚拟化工程师、运维工程师，有成员不具备政务云平台运维基本资质，有成员均未与运维公司就该项目签订专门的保密协议。 | 查验文件 |
| 运维团队未每月召开至少一次运维服务工作专题会议。 | 查验会议记录 |
| 未每年进行一次应急演练。 | 现场查验 |
| 信息报送 | 运维服务期间**每月、年**向采购人报送政务云运维信息和上云系统使用情况。报送信息应反映各单位上云系统运维管理情况和CPU、内存、磁盘等资源的实际使用率。 | 3000元/次（未报送） |  |
| 运维事件 | 三级故障（低）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、因服务商问题，导致云平台客户业务中断数量大于1个，少于5个；二、云平台1、云平台服务少于20%不可用三、基础设施1、网络性能下降小于50%2、核心设备出现故障 | 一次扣2000元 | 日志记录监管记录用户考评 |
| 二级故障（中）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、因服务商问题，导致政务互联网、政务外网或者专网客户业务中断数量超过5个二、云平台1、云平台服务超20%少于50%不可用三、基础设施1、部分设备断电2、网络性能下降50%或者部分网络中断 | 一次扣6000元 | 日志记录监管记录用户考评 |
| 一级故障（高）出现如下故障，未在120分钟内处理完成，按照费用扣除标准进行扣款。一、生产系统1、政务互联网、政务外网或者专网业务全部中断二、云平台1、云平台服务超50%不可用三、基础设施1、单机房完全断电(UPS供电正常不计为故障）2、政务互联网、政务外网或者专网全网中断； | 一次扣20000元 | 日志记录监管记录用户考评 |

以上考核细则将按照符合国家相关法律法规和符合项目实际需要的原则，进行不定期的修订完善，若有修订按修订后细则执行。

在政务云平台运维服务中，若对运维职责范围内的工作有任何异议，以服从采购人安排为先，事后双方再协商解决。

**C、商务要求**

**1、报价要求：**

 **报价包含但不限于：**满足本期项目采购文件和服务期内国家相关法规文件所提出的网络、安全、备份、服务、运维等要求费用**、**及**场地费、链路费、人工费、资料费、利润、税金等**所有相关费用。

2、项目实施要求

**1)项目实施与管理**

云服务商应制定详细的项目运维计划，并提供项目运维人员保障方案。

**2)技术文档要求**

所有设备具备全套中文（或英文）技术文档手册、资料；投标方应提供与设备相关的所有技术文档和资料，并且均应以磁介质（或光盘）或纸张为载体。

**3、合同服务期限和地点**

服务期限：本项目服务期为1年度。

 履约地点：乐山市范围内

**4、项目验收标准**

本项目服务期限结束后，由采购人组织专业人员会同成交供应商严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205号)、《乐山市财政局关于进一步规范市级政府采购有关事项的通知》（乐市财政采[2020]113号）等文件要求和规定进行验收。

**5、付款方式**

**1、乙方收取的服务费包含但不限于：平台软件硬件系统费用、场地费、链路费、人工费、资料费、利润、税金等。**

2、云资源服务费按采购单价和实际分配资源量进行付费，结算方式:**签定合同后30个工作日内，甲方向乙方预付预算金额的10%(成交人为小微企业的，预付预算金额的30%），余下款项分两次支付，签订合同并提供服务后6个月内，第一次支付服务期起算日起至服务期满六个月后所产生的服务费用的70%；第二次在服务期结束后，根据服务考核情况支付尾款。**若验收时云服务商有不影响功能使用要求的负偏离，在结算时按合同约定扣款。甲方付款前，乙方应先向甲方开具等额增值税普票。

3、上述款项的支付时间具体以财政部门将资金划拨到甲方账户时为准，且在到账后30个工作日内支付，乙方理解并同意。

6、违约责任

（1）甲乙（采购人与成交供应商，下同）双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。任何一方违约给对方造成的直接损失均负有赔偿责任，对方均有权视情况要求对方继续履行合同或提出解除合同；

（2）如因乙方在履行过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任；

如因乙方在提供服务过程中出现违规、违约等情形，有投诉或举报或验收时发现违规收费的，经核实属实的，扣减当季结算费用的1%，且甲方有权单方终止合同。

7、争议解决办法

1）甲乙双方就本协议所产生的任何争议都应该进行友好协商，协商解决不成的，任何一方均可向项目所在地有管辖权的人民法院提起诉讼；

2）诉讼费应由败诉方承担；

3）在诉讼期间，除正在进行诉讼的部分外，合同其他部分继续执行。

**标注“★”的条款为本项目的实质性条款，供应商须全部满足，不响应或不满足作无效响应处理。**

**第1包：通用政务云服务采购项目**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 总评分因素及权重 | 评分标准 | 说明 |
| 1 | 报价10% | 满足招标文件要求且下浮最多的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算∶投标报价得分=（评标基准价/投标报价）×10%×100=（1-最多的下浮比例）/（1-投标下浮比例）×10%×100备注：下浮比例≦100%； | 共同评分因素 |
| 2 | 技术响应40% | 技术服务要求完全满足招标文件要求（实质性要求除外）的得40分，带▲的每有一项不满足招标文件要求的，扣1.5分，其他每有一项不满足招标要求的，扣0.1分 | 技术类评分因素 |
| 3 | 企业综合实力13% | 1. 投标人提供增值电信业务经营许可（IDC），提供得3分。
2. 投标人提供增值电信业务经营许可（ISP），提供得3分。
3. 投标人提供增值电信业务经营许可（EDI），提供得3分。
 | 共同评分因素 |
|  人员配置，项目经理：具有工信部和中国电子信息行业联合颁发的高级项目经理证书或者项目管理专业人员资格认证（PMP证书）证书的得2分；项目经理近两年有类似业绩的得2分,提供投标人为其连续缴纳 6个月以上社保证明材料及业绩证明材料（证明材料能证明项目负责人为该项目经理）,工作不足6个月的，提供入职至递交文件截止日相应月份的社保证明材料 |
| 4 | 云平台建设方案25% | 1. 投标人准确理解采购人业务需求，根据对

（1）本服务项目理解、认识,（2）对系统总体安全设计思路、（3）系统功能结构、（4）系统运行保障措施等需求分析方面.以上4项内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得10分；方案存在缺项或不符合本项目实际情况的，每有一处扣2.5分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1.5分。不提供不得分。2、对乐山市电子政务云平台方案（1）完整性、（2）架构安全性、（3）平台扩展性、（4）数据安全、（5）巡检值守等5项内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得10分；方案存在缺项或不符合本项目实际情况的，每有一处扣2分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1分。不提供不得分。3、对迁移上云时效性的承诺提供承诺在10日内完成迁移上云50套系统的，得5分；提供承诺在一个月内完成迁移上云50套系统的，得3分。不提供不得分。 | 技术类评分因素 |
| 5 | 售后服务方案10% | 投标人从对（1）售后服务质量保证及（2）售后服务的要求、（3）保障措施、（4）人员配置、（5）技术支持、（6）故障响应时间、（7）处理流程及（8）应急响应机制等方面提供详细的售后服务方案，以上,8项内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得10分；方案存在缺项或不符合本项目实际情况的，每有一处扣1.25分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的扣0.5分，不提供不得分。 | 技术类评分因素 |
| 6 | 节能环保1% | 投标产品为环境标志产品的，有一个得0.5分，最多得1分。（本项目不涉及节能产品和无线局域网产品） | 共同评分因素 |
| 7 | 少数民族地区和不发达地区1% | 投标人注册地属于少数民族地区和不发达地区，得1分。 | (少数民政地区：以投标人营业执照中住所或登记机关为少数民族地区为准，不发达地区：以投标人营业执照中住所或登记机关为原832个脱贫县域为主。不提供则不得分) |

**第2包：视频政务云服务：**

|  |  |  |  |
| --- | --- | --- | --- |
| 分类 | 评分项 | 评审标准 | 备注 |
| 报价（10分） | 10分 | 满足招标文件要求且下浮最多的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算∶投标报价得分=（评标基准价/投标报价）×10%×100=（1-最多的下浮比例）/（1-投标下浮比例）×10%×100备注：下浮比例≦100%； | 共同评分因素 |
| 商务部分（25分） | 云服务商综合实力（25分） | 投标人提供增值电信业务经营许可证得2分，未提供或不满足得0分。（提供证书复印件并加盖投标人单位公章）。 | 共同评分因素 |
| 投标人具有第三方认证机构颁发的IT服务管理体系认证证书、环境管理体系认证证书、信息安全管理体系认证证书 、云计算安全评估证书、业务连续性管理体系认证证书，以上满足全部证书得5分，每少提供一个证书扣1分，直到全部扣完为止，（提供证书复印件并加盖投标人单位公章）。 |
| 投标人提供ITSS云计算服务能力标准符合性证书（信息技术服务云计算）二级或以上的得1分，（提供证明材料并加盖投标人单位公章）。 |
| 基于云安全运营的考虑，投标人获得可信云认证：云管理服务能力评估卓越级、企业级SaaS服务（舆情分析）、混合云安全能力评估、云服务企业综合信用水平评估（AAA）、GPU云主机服务、云服务用户数据保护能力增强级（私有云平台、公有云平台）、安全运营中心解决方案、大规模容器集群性能卓越级。以上满足全部证书得9分，每少提供一个证书扣1分，直到全部扣完为止。（提供证书复印件并加盖投标人单位公章）。 |
| 投标人具有：容器镜像服务系统、数据库服务系统、大数据平台服务系统、虚拟私有网络服务系统、云运维支撑系统、云监控服务系统、大数据存储与分析服务系统、云安全管理系统等著作权证书，以上满足全部证书得8分，每少提供一个证书扣1分，直到全部扣完为止，。（提供相关证书复印件并加盖投标人单位公章）。 |
| 技术部分（63分） | 方案能力（22分） | 政务云平台建设方案方案包含但不限于（1）完整性、（2）架构安全性、（3）平台扩展性（4）数据安全、（5）巡检值守。以上5项内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得5分；方案存在缺项或不符合本项目实际情况的，每有一处扣1分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的扣0.5分，不提供不得分,本项满分5分。 | 技术类评分因素 |
| 资源池建设方案方案包含但不限于（1）计算资源池方案，（2）存储资源池方案，（3）网络资源池方案，（4）安全资源池方案，以上4项内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得8分；方案存在缺项或不符合本项目实际情况的，每有一处扣2分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1分。不提供不得分,本项满分8分。 |
| 云平台运营管理方案方案包含但不限于（1）云迁移需求，能够为业务云间迁移提供全面的支持和管理，提出完整、可行、先进、合理的跨云迁移方案，（2）应用上云需求，能够为业务上云迁移提供全面的支持和管理的上云方案，（3）云运营管理需求，能够针对资源管理制度、运维管理制度、应急响应制度、安全管理制度等规范制度方面的规范制度。以上3项内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得9分；方案存在缺项或不符合本项目实际情况的，每有一处扣3分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1.5分。不提供不得分,本项满分9分。 |
| 云管理平台能力（14分） | 1、提供云管平台厂商ITSS信息技术服务运行维护标准符合性证书（成熟度等级一级）得1分；2、提供云管平台厂商CMMI5级能力成熟度模型认证证书得2分，CMMI4级及以下能力成熟度模型认证证书得1分。3、提供云管平台厂商信息安全服务资质认证证书-信息系统安全集成一级证书得2分；4、提供云管平台厂商信息安全风险评估服务资质一级证书得2分。5、提供云管平台厂商信息安全等级保护安全建设服务机构能力评估合格证书得2分。6、提供不少于7个由公安机关认证的所建云计算中心或云平台系统通过等保三级备案证明得5分，未完全提供或不满足得0分。（提供证书复印件并加盖投标人单位公章）。 |
| 云平台测评（5分） | 投标人所具有的云平台提供《信息技术云计算参考架构》、《信息技术云资源监控指标体系》《信息技术云计算资源监控总体技术要求》、《信息技术弹性计算应用接口》、《信息技术云计算虚拟机管理通用要求》等云基准测评证书，以上证书全部提供者得5分，每少提供一个扣1分，直到该项分值扣完为止。（提供证书复印件并加盖投标人单位公章）。 |
| 服务能力（7分） | 1、投标人为本项目指定的专职项目经理具有工信部或中国电子信息行业联合会颁发的信息系统项目管理师证书或PMP证书的得1分。 |
| 2、为本项目配备10个及以上专业技术人员参与本项目实施，其中包含具备OCP数据库专家、CCIE网络认证专家、ITIL认证、VCP、AWS SAP认证、信息系统项目管理师的人员，出具专业人员证书复印件（包括专业资格证明、社保证明等）。说明：1、若同一人具备多个证书，只按一种证书计算2、为本项目配备的专业技术人员满足以上6类全部证书要求，每提供一个证书得1分，满分6分。3、项目经理及专业技术实施人员的投保单位要与投标人主体完全一致，不一致的一律不得分。  |  |
| 案例能力（15分） | 投标人或所投云管理平台厂商提供近5年来（自2016年1月1日起）实施过的类似项目案例，每提供一个类似项目案例的得3分。本项最多得15分。 |
| 注：提供合同（合同须为服务目录模式且包含服务目录内容，未含服务目录的合同一律不得分）关键页复印件并加盖投标人公章；合同签订主体要与须投标人（或所投云平台厂商）主体名称完全一致，否则一律不计入有效案例。 |
| 节能环保1% | 1分 | 投标产品为环境标志产品的，有一个得0.5分，最多得1分。（本项目不涉及节能产品和无线局域网产品） | 共同评分因素 |
| 其他 | 少数民族地区和不发达地区1分 | 投标人注册地属于少数民族地区和不发达地区，得1分。提供相关证明材料(少数民政地区：以投标人营业执照中住所或登记机关为少数民族地区为准，不发达地区：以投标人营业执照中住所或登记机关为原832个脱贫县域为主。不提供则不得分) |  |

备注：1、响应文件中要求提供的以上证明材料的复印件须加盖投标人公章；2、投标人或所投云管理平台厂商提供的证明材料必须与其主体名称完全一致，其母公司、子公司、分公司的资质证书或案例合同不参与评分；3、投标人所投云管理平台厂商相关证明材料其主体名称必须与云管理平台著作权证书主体名称一致，否则不参与评分。4、本项目所要求相关资质证明、证书的取得日期须为本项目挂网之日前。

**第3包：算力政务云服务：**

|  |  |  |  |
| --- | --- | --- | --- |
| 总评分因素及权重 | 分值 | 评分标准 | 说明 |
| 报价10% | 10分 | 满足招标文件要求且**下浮最多**的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算∶投标报价得分=（评标基准价/投标报价）×10%×100**=（1-最多的下浮比例）/（1-投标下浮比例）×10%×100**备注：下浮比例≦100%； | 共同评分因素 |
| 业绩案例8% | 8分 | 投标人或投标人所投云平台厂商近三年来（合同签订时间为2018年1月1日至今）具有类似业绩，需提供合同原件扫描件（包括合同金额、买卖双方名称及盖章、合同签订日期），每提供一个得1分，最高得8分。 | 共同评分因素 |
| 投标人或所投云平台厂商能力15% | 7分 | 投标人或投标人所投云平台厂商具有ISO 20000信息技术服务管理体系、ISO 27017信息安全管理体系云安全、ISO 27701隐私信息管理体系认证证书，满足全部3个认证的得7分，满足其中2个认证的得4分，满足其中1个认证得2分，提供有效认证证书复印件，否则不得分。 | 共同评分因素 |
| 5分 | 投标人或投标人所投云平台厂商具有ISO 22301业务连续性管理体系、ISO 29151通用个人信息保护管理体系认证证书，满足全部2个认证的得5分，满足其中1个认证的得2分，提供有效认证证书复印件，否则不得分。 | 共同评分因素 |
| 3分 | 投标人或投标人所投云平台厂商具有质量管理体系TL 9000行业标准认证证书，提供有效认证证书复印件得3分，其他不得分。 | 共同评分因素 |
| 云平台实力及安全能力11% | 4分 | 云平台相关系统获得信息系统安全等级保护备案证明3级或以上，提供3个及以上备案证明复印件得4分，提供2个备案证明复印件得3分，提供1个备案证明复印件得1分，最高得分为4分。 | 共同评分因素 |
| 4分 | 投标人或投标人所投云平台厂商实施的云计算服务平台通过中央网信办党政部门云计算服务安全评估，提供2个安全能力级别为增强级案例得4分，提供1个的得2分，最高得分4分。（需提供国家互联网信息办公室官网链接及截图证明。） | 共同评分因素 |
| 3分 | 投标人或投标人所投云平台厂商具有中国信息安全测评中心颁发的信息安全服务资质云计算安全类认证证书得3分，提供证书复印件，其他不得分。 | 共同评分因素 |
| 技术指标及要求30% | 30分 | 响应文件完全满足招标文件技术(实质性指标除外）的，得30分；对招标文件中标条款为▲重要条款，每1条不满足减**1.5分**；其他条款（非★和▲条款）每1条不满足扣0.**06分**，直到本项分值扣完即止。 | 技术类评分因素 |
| 技术方案10% | 10分 | 技术方案**包括但不限于**：（1）需求理解分析；（2）总体技术方案及架构；（3）详细设计方案；（4）安全建设方案等内容。内容齐全无缺陷、满足项目实际需求，逻辑条理清晰的得10分；方案存在缺项或不符合本项目实际情况的，每有一处扣2.5分；每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1.5分。不提供不得分。 | 技术类评分因素 |
| 项目实施及组织管理4% | 4分 | 项目实施方案**包含但不限于**：（1）时间进度安排；（2）实施保证措施。内容齐全无缺陷、满足项目实际需求，合理可行的得4分；方案存在缺项或不符合本项目实际情况的，**每有一处扣2**分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1分。不提供不得分。 | 技术类评分因素 |
| 运维服务方案6% | 6分 | 运维服务方案**包含但不限于**：（1）运维服务体系；（2）运维保障措施；（3）服务响应时间等。**内容齐全无缺陷且完全满足项目实际需求，逻辑条理清晰的得6分；方案存在缺项或不符合本项目实际情况的，每有一处扣2分，**每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1分。**不提供不得分。** | 技术类评分因素 |
| 售后服务方案4% | 4分 | 售后服务方案**包含但不限于**：（1）售后服务内容；（2）培训服务内容。内容齐全无缺陷、满足项目实际需求，逻辑条理清晰的得4分；方案存在缺项或不符合本项目实际情况的，每有一处扣2分，每项内容中阐述存在缺陷或不契合项目实际需要或不完整或虽有内容但描述简单的，扣1分。不提供不得分。 | 技术类评分因素 |
| 节能环保1% | 1分 | 投标产品为环境标志产品的，有一个得0.5分，最多得1分。（本项目不涉及节能产品和无线局域网产品） | 共同评分因素 |
| 少数民族地区和不发达地区1% | 1分 | 投标人注册地属于少数民族地区和不发达地区，得1分。提供相关证明材料(少数民政地区：以投标人营业执照中住所或登记机关为少数民族地区为准，不发达地区：以投标人营业执照中住所或登记机关为原832个脱贫县域为主。不提供则不得分) | 共同评分因素 |