招 标 文 件

招标编号：ZHBRJ202201-43

项目名称：采购云平台软件及服务

招标内容：云平台软件 计算资源服务节点规划 存储设备规划 网络设备安全服务 多云管理平台

湖北日报传媒集团招标采购部

2022 年 9 月

投标邀请函

请合格的投标人就采购云平台软件及服务项目提交密封投标文件。

投标人可在2022年9月16日—9月22时间内，上午9:00至11:00时，下午2：30时至4:00(北京时间)到本部领取招标文件，或在湖北日报客户端、荆楚网客户端、http://www.cnhubei.com下载招标文件。

所有投标书应于2022年9月29日下午17：00前送达本部，逾期将不予接受。

在招标期间，投标人可提供相关产品进行测试。联系人：张先生，联系电话：13908628692。

开标一览表请单独封装在一个投标信封内，并注明“开标一览表”字样，放在投标文件正本中。

地址:武汉市武昌区东湖路181号楚天传媒大厦

联系人:胡先生

电话：027-88568112　15972202401

湖北日报传媒集团招标采购部

2022年9月14日

第一章 投标人须知附表

序号	名称	内容规定
1	招标人	招 标 人：湖北日报传媒集团招标采购部 地　　址：武汉市武昌区东湖路 181 号楚天传媒大厦 邮　　编：430077
2	项目名称	采购云平台软件及服务
3	投标人报名时间	2022 年 9 月 16 日至 2022 年 9 月 22 日 16 时 00 分止
4	投标截止时间	2022 年 9 月 29 日下午 17 时 00 分
5	递交投标文件地点	楚天传媒大厦附楼 B0132 室
6	投标文件份数	一正一副，并提交投标文件电子档（相关文件及资料不予退还)
7	评标小组	不少于 5 人，且为奇数
8	中标通知	招标人将直接联系中标人并发放中标通知书
9	解释权	构成本招标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；除招标文件中有特别规定外，仅适用于招标投标阶段的规定，按招标公告（投标邀请书）、投标人须知、评标办法、投标文件格式的先后顺序解释；同一组成文件中就同一事项的规定或约定不一致的，以编排顺序在后者为准；按本款前述规定仍不能形成结论的，由招标人负责解释。

第二章　投标人须知

一、项目介绍

1、项目名称：采购云平台软件及服务

2、招标单位：湖北日报传媒集团招标采购部

3、招标方式：公开招标

4、招标内容：云平台软件 计算资源服务节点规划 存储设备规划 网络设备安全服务 多云管理平台

二、合格投标人条件

1、资格要求：依法依规登记设立，具有独立法人资格，并符合本招标文件资质能力要求的投标人；

2、信誉要求：遵守国家法律法规，诚实守信，信用中国近两年无市场不良行为记录。

3、参与本次招标投标活动的各方应对招标文件和投标文件中的商业和技术秘密保密，否则应承担相应的法律责任，并赔偿招标人因此遭受的损失。

4、参与本次招标投标活动的各方，若有拉拢、腐蚀等贿赂招标方工作人员行为的，不论年限过去多久，招标方有权通过法律途径起诉索赔，并取消投标方参与今后招标方采购项目的资格。

5、投标人具有对所提供产品的维护能力。

三、招标文件说明

1、投标人应仔细阅读招标文件中的所有内容，按照招标文件及要求编制投标文件，并保证投标文件的正确性和真实性。

2、投标人获取招标文件后，应仔细检查招标文件中的所有内容，如有疑问，应及时向招标人提出。

3、不按招标文件的要求提供的投标文件将被拒绝。

4、招标文件发出后，投标截止时间之前，招标人如对招标文件进行补充和修改，将发布澄清公告。澄清公告与招标文件表述不一致的，以澄清公告为准。

四、投标文件要求

（一）投标人应按招标文件要求的格式制作投标文件，装订成册。投标文件应包括下列部分：

1、投标函（按附件 1 格式）；

2、投标保证书（按附件 2 格式）；

3、法定代表人身份证明；

4、如投标人代表不是法定代表人，须在投标文件中提供《法定代表人授权委托书》（按附件 3 格式）；

5、投标人具备实施该项目所必需专业技术能力的证明材料以及相关资质（正本必须提供加盖公章的彩色影印件），包括但不限于以下材料：

（1）法人或者其他组织的营业执照等证明文件，自然人的身份证明；

（2）采购活动前 3 年内在经营活动中没有重大违法记录的书面声明；

（3）提供原厂商针对本项目授权和服务承诺函；

（4）投标人提供 CCRC 信息系统安全集成或安全运维资质证书；

（5）投标人具备 ISO20000 IT 信息技术管理体系认证证书；

（6）投标人具备 ISO9001 质量管理体系认证证书；

（7）投标人具备 ISO/IEC 27001 信息安全管理体系认证证书；

（8）投标人提供 ITSS 认证运行维护成熟度证书；

（9）具备法律、法规规定的其他条件的证明材料；

（10）投标人认为需提供的其它相关资格证明材料。

6、厂商相关资质：

（1）计算机信息系统安全专用产品销售许可证，提供证书文件复印件并加盖原厂公章有效；

（2）所投产品《计算机软件著作权登记证书》；

（3）产品应用案例，提供所投同类型产品近三年相关案例，提供合同关键页，内容清晰可见。

（4）所投产品其他证书或资质，提供有效证明材料。

7、投标报价

（1）投标报价应包括招标文件及所注明的全部内容以及为完成上述内容所必须的部署、运输、安装、调试、税金等全部费用；一经中标，合同金额在合同期限内不做调整。

（2）投标人未计入或计算的招标范围内的设备及配件将被视为已包含在其投标报价中，投标人没有填写单价或合价的项目，招标人将拒绝承认和接受投标报价中未列出的任何费用，并认为这些项目的费用已经包括在报价单的其它单价或总价之中。

（3）投标方在运输和安装所需要的设备工具及人员的食宿由投标方自行解决，招标方可为投标方提供必要的帮助。

（4）当单价与数量的乘积和总价不一致时，以单价为准。除非评标小组认为有明显的的小数点错误，此时则以总价为准，并修改单价。

8、其他

投标文件均需打印或用不褪色的书写工具书写，投标文件任何行间插字、涂改和增删，必须由投标人盖章确认方为有效。

投标文件一式二份（**正本壹份，副本壹份**）正本和副本如有不一致处，以正本为准。同一数字的表达不一致时，以大写为准。

投标文件装袋后应进行密封、封口应粘贴封口条，加盖投标人单位公章和法定代表人印章。如果投标文件没有按上述要求密封，招标人将不承担投标文件提前开封的责任。

投标有效期为提交投标文件截止之日起 60 天。在此期限内，凡符合招标公告和招标文件的投标文件均保持有效。

（二）投标人出现以下情况之一，其投标文件作废：

1、投标文件中有弄虚作假的内容。

2、投标文件不满足招标文件要求。

3、投标文件附有招标人不能接受的条件。

4、投标有效期不足。

5、按照相关法律法规，应视为废标的情形。

五、采购货物需求、技术规格及相关要求

序号	名称	数量	单位	要求	服务
（一） 云平台软件					
1	云平台软件	2	套	含云平台基础软件、运营平台、运维平台、SDN 及满足需求规模的授权	
2	虚拟化授权			足量授权	

序号	名称	数量	单位	要求	服务
3	云存储软件			足量授权	
（二）计算资源服务节点规划					
4	云平台控制节点服务器	6	台		
5	云平台网络服务器	4	台		
6	安全资源池服务器(含管控节点)	6	台		
7	计算节点服务器(含负载均衡)	10	台		
（三）存储设备规划					
8	NAS 存储	2	套	每套可用空间不少于 100T(分布式存储需采用三副本技术)	
9	集中式块存储	2	套	每套可用空间不少于 50T	
（四）网络设备					
10	核心交换机	4	台		
11	业务交换机	4	台		
	存储交换机	4	台		

序号	名称	数量	单位	要求	服务
	综合接入交换机	4	台		
	带外管理汇聚交换机	4	台		
	带外管理接入交换机	4	台		
（五）容灾备份管理服务					
12	备份软件	50	T		
（六）安全服务					
13	安全管理平台	2	套		
14	主机安全（虚拟机）	100	点		
15	主机安全（平台物理服务器）	32	点		
16	云堡垒机	100	资产		
17	数据库审计	10	实例		
18	云安全中心	2	套		
19	云防火墙	6	套	每套性能不低于 1Gbps	
20	云 WAF	6	套	每套性能不低于 1Gbps	
21	日志审计	100	资产计入		
（七）多云管理平台					

序号	名称	数量	单位	要求	服务
22	基础平台	1	套		
23	纳管节点授权	28	节点	包含 18 个 VMWare 虚拟化节点	
24	纳管公有云资源授权	≥20	个		
（八）服务要求					
25	集成服务	1	套		
26	驻场服务	12	人*月		
27	年服务费	3	年	另承诺三年后云平台及相关软件的年度服务费用	
项目工期	合同签订之日起 45 个工作日				
服务期	采购人初验合格正式投入使用之日起 3 年				

（一） 建设内容

目前集团及二级单位部分业务部署在不同的公有云、私有云资源上，数据和业务尚未互通形成信息孤岛，对提供的服务也不能实现计量计费。本项目以集约建设、资源共享、业务联动、综合利用为目标，运用云技术构建云虚拟化基础设施，为湖北日报信息化工程中的各类业务应用提供支撑服务，同时纳管现有 Vmware 集群，实现全集团硬件资源集约化和统一管理，对二级单位提供云服务，消除信息孤岛。

（1） 建设湖北日报云底座基础设施，构建统一的网络、计算、存储资源池；云平台采用存算分离架构，解耦计算、存储、网络、安全等模块。

（2） 依据现有主备机房，构建云平台容灾体系；

（3） 纳管现有 Vmware 集群和公有云服务；

（4） 为平台和租户应用提供安全功能，以满足等保三级要求；

（二） 技术服务要求

1 总体要求

1．架构要求：

云平台服务商需按照湖北日报对云平台的多中心部署要求,利用主机房与后备机房组成的双数据中心特点，以“一朵云，双资源池”“存算分离”的形式构建底层网络和云平台各类资源，实现资源和数据的相互备份容灾，提供基础架构的规划和落地部署技术方案,并配合湖北日报落地实施,提供相应技术支持服务。

设计方案要求采用双 Region 部署，每个数据中心部署各自 Region。不同 Region 有各自的一组管控节点，避免单点故障；同时，两 Region 可互为备份。双数据中心统一管理，统一运营，对外呈现逻辑一朵云。

2．自主可控要求：

1） 本次建设全栈云平台需具备“一云多芯”能力，支持在单一集群内扩展包括鲲鹏、飞腾、海光等计算资源池（单 AZ 多资源池，一个资源池一个架构）。

2） 支持国产化及信创设备资源池；

3．安全要求：

云平台服务商需提供等保三级服务支持,能够支撑甲方通过等保三级认证，实现安全合规要求。

4．灾备要求：

主备数据中心管控节点及资源池可以实现互备。

2 云平台要求

项目名称	技术参数	证明材料要求
技术路线	采用业界先进的技术路线，基于先进的云原生理念设计，可支持容器、虚拟化、数据库、中间件等各类云产品进行云原生统一调度与分配，减少技术复杂度，提升运维效率。	
组网方式	云平台网络独立建网，上行到主机房的中心网络交换机互联，实现与现有网络的互通。现有网络已通过防火墙与互联网联通，并已准备了云平台网络所需防火墙。	
容灾要求	云平台的 SDN 节点、管理节点应考虑一侧机房设施故障情况下，顺利切换到对端机房的具体技术方案。	
无感知业务升级	本次建设全栈云平台需基于虚拟化技术栈构建，平台各组件服务采用分布式架构，可以进行在线版本升级，业务无感知，不同版本之间可以相互兼容。	
	采用基于 KVM 技术架构需支持 KVM 和 Qemu 热升级。	
硬件兼容性	本次建设全栈云平台软件不与硬件绑定，服务器设备除了支持 X86 芯片以外，还需至少支持鲲鹏、海光、飞腾三家芯片，并提供兼容设备列表，网络设备支持两家及以上。同时，计算、存储资源扩容时，云平台软件须支持异构品牌物理设备。	提供使用自主可控CPU的国产服务器的兼容性认证材料。
	本次建设全栈云平台软件的存储服务能力支持多品牌硬件设备的纳管和部署，包括但不限于集中式块存储，对象存储与文件存储。	提供至少四家主流分布式存储的兼容性认证证书。
	服务器、存储、网络等硬件设备的兼容性列表	提供清单并加盖公章
性能损耗	产品厂商提供体现 CPU、内存虚拟化损耗率的证明材料。	提供截图并加盖公章

3 计算服务要求

计算资源池主要提供计算能力，是 IAAS（基础设施即服务）建设的核心。由于信息化业务快速发展的特点，计算资源池建设中需要充分体现动态化、弹性

化的特征，做到能够根据业务部门实际需要，动态分配计算资源，并需要提供弹性计算资源的管理工具，从而实现计算资源的可视化管理。

项目名称	技术参数	证明材料要求
基本服务要求	支持用户通过云平台管理界面对虚拟机的生命周期管理，包括开机、关机、重启、暂停、恢复、克隆、删除、远程登录、重置密码、重置系统等。操作方式支持通过WEB 页面或 API 的方式	
	虚拟机服务需提供虚拟机实例、镜像、快照、安全组、弹性网卡、弹性 IP、秘钥/密码、自定义标签、主机组等服务能力及相关管理能力	
	计算资源池管理。可查询、添加、修改、移除资源池。可查看资源池详情，包括：资源池概览信息、性能监控、历史曲线、主机列表、可用分区、主机组、主机 HA 、虚拟数据中心列表、外部网络、云主机列表、任务信息、操作日志、资源审计等信息。	
弹性伸缩	支持弹性伸缩功能，用户可通过定义弹性伸缩策略，在业务需求增长时自动增加计算资源（虚拟机）以保证计算能力；支持在业务需求下降时，自动减少计算资源以节省成本，基于负载均衡和健康检查机制，可同时适用于请求量波动和业务量稳定的业务场景。	
镜像	支持镜像生命周期管理，包括创建、上传、下载、URL 镜像、修改、删除以及通过镜像批量创建云主机等。	

4 存储服务要求

项目名称		技术参数	证明材料要求
云硬盘	服务描述	为云服务器提供块级存储设备，相当于一台物理机的硬盘。云硬盘是独立的资源，它的生命周期独立于云主机，可以被挂载到任何云主机上，也可以从云主机卸载，然后挂接到其他云主机。用户通过自服务界面可对云硬盘进行创建、删除、快照、备份、恢复、扩容等操作	

		申请云硬盘服务时用户可以配置需要申请的磁盘名称，创建磁盘的数量，磁盘类型	
	资源池管理	云管理平台管理存储资源时可以根据 SSD/SAS 配置不同的存储资源池，用户申请存储资源时可根据需要选择对应的资源池，达到云存储规格分级管理与使用的需要，不同资源池提供独立的资源规格和计费策略。	
		支持不同性能层次或厂家的存储后端资源进行 SLA 标识，用户可以通过自助管理界面创建不同 SLA 规格的云硬盘	
		支持 SAS、SSD 等不同存储在同一存储资源池内混合部署；	
	生命周期管理	云硬盘生命周期管理，包括创建、删除、挂载、卸载、快照、备份、扩展、编辑名称等功能。	
		云硬盘能够提供在线添加（挂载）、在线卸载、在线扩容功能	
		云盘支持以系统盘或数据盘的方式挂载到云服务器实例中。	
		支持云硬盘扩容，支持在 OS 支持的情况下，在线/离线扩容云硬盘，提供支持在线扩容的操作系统清单	
		支持云硬盘的管理，用户可以查看系统中已有的硬盘列表。可以查看磁盘名称、状态、容量、挂载到的服务器、创建时间等基本信息；可以通过磁盘名称或者磁盘是否挂载等条件搜索目标磁盘/磁盘组	
		支持云硬盘回收站功能，能够快速恢复软删除的云硬盘，避免误操作；支持逾期自动删除回收站内的云硬盘	
	备份和快照	支持快照服务，支持即时快照和快照策略两种方式；用户可以通过管理平台为自己的虚拟机磁盘创建快照，并自助完成快照恢复； 支持增量快照； 支持快照链； 支持快照回收站； 支持用户自助删除无需使用的磁盘快照	
		支持定时快照。用户可以指定周期、	

		时间节点自动进行云硬盘快照。支持设置最大快照保留数量，仅保留最近的快照。	
文件存储服务	文件存储服务	支持并配置客户端连接负载均衡软件,负载策略支持 CPU 占用率。	
		支持自动精简配置，可按需 动态分配存储空间，保证存储资源的最大化利用。	
		支持文件系统的总带宽可随容量扩展而增长，适合高带宽型应用。同时保障数据的高持久度，满足业务增长需求。	
		支持在服务界面选择共享文件系统，挂载给虚拟机。	
对象存储服务		对接浪潮 AS13000，作为云平台对象存储服务的资源池。	提供相关证明材料

5 网络服务要求

建设畅达的网络是湖北日报云底座发挥整体效益的基础承载，该云底座将作为湖北日报未来应用的基础承载平台，因此本期项目在网络整体架构设计时，不仅需要满足云底座本期需求，还需要考虑网络的可拓展性，能够在后期对网络功能指标及性能指标进行按需拓展。具体存在如下需求：

（1）云底座网络需要具备快速收敛、高转发性能、易维护、易管理和节能环保等特性，即需要简化网络架构，降低网络复杂度。

（2）云底座网络需要具备高可靠性、高可用性。网络设计能有效的避免单点故障，在设备的选择和关键设备的互联时，应提供充分的关键设备冗余、重要业务模块冗余和链路冗余。

（3）云底座网络架构和设备选型方面需要具备高可扩展性，不仅满足当前需要，也能满足未来业务扩展需求。

（4）满足安全隔离的需求，实现各租户之间网络层面的隔离。

（5）支持网络虚拟化，减少设备节点，简化配置。

项目名称	技术参数	证明材料要求
VPC 服务	专有网络服务（VPC）必须是基于软件定义的虚拟网络（SDN）技术，为用户在专有云环境中构	

	建出一个完全隔离的、自我掌控的虚拟网络，包括选择自由 IP 地址范围、划分网段、配置路由表和网关等	
	实现二层网络隔离，并且可以将虚拟机、虚拟负载均衡等云服务部署在一个 VPC 内	
	支持多租户、各个 VPC 之间是安全逻辑隔离的；支持自定义多个互相隔离的网络地址段，且允许 IP 地址重合	
	支持创建三层网络，支持公有网络、私有网络、系统网络，用户能够将指定用途网络创建在指定网络类型中。	
	虚拟路由应可实现和物理交换机建立邻接关系，从而联通物理网络和虚拟网络。	
	虚拟网络支持 DHCP 协议，为虚拟网络中的云服务器实例配置 DNS 服务器 IP 地址和域名。	
	支持网络拓扑图可视化，通过图形化界面，查看网络拓扑结构。	
IPv6	支持开启 IPV6，支持双栈	
	可以创建 IPv4/IPv6 双栈虚拟网卡	
安全组	支持安全组服务，可以对进出虚拟机端口的网络报文进行限制的安全过滤规则。关联虚拟机端口与安全组后，该安全组的规则会对进出该虚拟机端口的网络报文进行过滤，只有规则允许的报文才能通过。	
	支持创建和管理安全组； 提供安全组的创建、修改、删除等功能	
	安全组内支持对 TCP、UDP、ICMP 等协议的自定义配置，可以指定当前安全组出/入方向上过滤的对象,过滤对象可以为 IP 段(可以指定 TCP/UDP 的源/目的 IP 及端口）或者其他安全组	
	安全组可以过滤虚拟机实例出入口的流量，控制的规则可以由租户自定义。	
	可以将 VPC 内的虚拟机加入一个安全组，然后设定不同安全组间的访问规则。同一个安全组内的地址之间的访问不受限制，默认组间是禁止访问的	
虚拟 IP	支持虚拟 IP，支持增删改查，支持绑定/解绑云服务器，支持绑定/解绑 EIP。通过虚拟 IP 功能支持多云主机的构建高可用集群，	
网络 ACL	支持网络 ACL 管理，支持网络 ACL 规则管理。	
	网络 ACL 要求基于 IP 协议、服务端口和源或目的 IP 地址，允许或拒绝流量。	
权限管理	支持权限管理，使用统一身份认证服务 IAM 对所拥有的专有网络进行精细的权限管理，以满足企	

	业基于组织划分、职能划分设置不同的访问权限。	
网络路由服务	支持根据业务需求配置虚拟路由器的路由规则，支持默认路由表和自定义路由表，支持系统路由和自定义路由。	
负载均衡服务	负载均衡服务：对多台云服务器进行流量分发的网络服务。支持多种流量分发策略，满足海量访问请求，提升业务系统的高可用。负载均衡均以软件方式实现。	
	支持用户通过云平台申请负载均衡服务，支持指定负载均衡集群中 Server 使用的服务器 IP 地址（Server IP）池，支持用户指定及系统自动分配等多种方式配置集群的虚服务 IP（VSIP），并且支持为负载均衡器绑定弹性 IP/公网 IP 以便提供对外服务	
	支持负载均衡实例管理，支持创建、查询、修改、删除、启动、停止负载均衡服务。	
	支持后端云服务器管理，支持向负载均衡实例添加和移除后端服务器。	
	支持对后端云服务器进行权值配置。	
	支持多协议，支持 4 层、7 层负载均衡，支持 TCP、UDP、HTTP、HTTPS 负载均衡。	
	提供用户自服务门户，用户可自行创建负载均衡实例，并对其进行配置。	
	支持私网负载均衡和公网负载均衡，公网负载均衡需要绑定弹性公网 IP，对公网进行负载均衡服务。	
	支持高可用，负载均衡实例节点故障后，自动将虚拟 IP 飘移到备实例节点对外提供服务。	
	支持接入虚拟网络，实现将访问负载均衡虚拟 IP 的流量转发到虚拟网络中。	
数据转发	支持基于 IP、协议、端口等规则进行转发，支持基于 HTTP Header、Host、Cookie 等多种规则进行转发，实现基于业务的灵活调度。	
	负载均衡流程分发策略管理，支持加权轮询、加权最小连接数、源 IP 等策略。（支持多种负载均衡调度算法：随机、轮询、基于 IP 的哈希算法、最少连接等。）	
	支持域名/URL 的转发策略，针对 HTTP 和 HTTPS 协议服务，根据域名或 URL 进行流量转发。	
监听器	支持监听器管理，支持添加、修改、删除、启动、停止监听器，支持添加和删除云服务器至监听器。	
	附加 HTTP HEADER，可附加客户端 IP 和端口、SLB	

	ID、监听协议以及监听端口等信息	
	支持 TCP/HTTP/HTTPS 三种监听模式	
健康检查	支持基于 ICMP 的健康检查机制，向后端服务器组发送 ICMP 请求，查看是否收到应答。 支持基于 TCP 监听的健康检查机制，向后端云服务器实例发送 TCP SYN 数据包，查看是否能接受到 SYN+ACK 数据包。	
	支持基于 HTTP/HTTPS 监听的健康检查机制，向后端云服务器实例的指定端口发送 HTTP HEAD 请求，查看返回的 HTTP 状态码。	
	支持基于 UDP 监听的健康检查机制，向后端云服务器实例发送 UDP 探测报文，查看是否接受到 ICMP 报错信息。	
会话保持	支持会话保持，保证在会话的生命周期内，同一条会话的请求被转发到同一台后端服务器上。	
	支持会话保持，针对 7 层（HTTP 协议）服务，实现基于 cookie 的会话保持。针对 4 层（TCP 协议）服务，实现基于源 IP 地址的会话保持。	
	支持 TLS 安全策略，可接入证书管理服务，在负载均衡实例中对 HTTPS 流量进行验证，降低后端服务器的开销。	
	支持证书管理，针对 HTTPS 协议服务，支持服务器证书管理。支持创建、修改、删除 CA 证书	
	HTTPS 证书双向认证	
	HTTP 重定向 HTTPS	
	支持权限管理，使用统一身份认证服务 IAM 对所拥有的负载均衡进行精细的权限管理，以满足企业基于组织划分、职能划分设置不同的访问权限。	
全局负载均衡	支持基于 DNS 和 IP 地址的全局负载均衡，实现互联网流量的接入并在云内进行转发，如将两个负载均衡实例的虚拟 IP 添加到 DNS 服务器中，实现多负载均衡实例的高可用。	
弹性 IP（EIP）	可提供独立的公网 IP 资源，包括公网 IP 地址与公网出口带宽服务。支持弹性公网 IP 网段动态发布	
	可灵活与云服务器、负载均衡、裸金属等云产品进行绑定、解绑，灵活使用，实时生效。	
	支持修改带宽，实时生效。	
	提供用户自服务门户，用户可自行创建弹性公网 IP，并对其进行配置。支持批量购买，支持指定 EIP 地址池申请，支持指定 IP 申请 EIP	

	支持权限管理，使用统一身份认证服务 IAM 对所拥有的弹性公网 IP 进行精细的权限管理，以满足企业基于组织划分、职能划分设置不同的访问权限。	
对等连接	提供的跨 VPC 网络的数据互联服务，实现相同或不同账号的 VPC 互联，支持本端 VPC 和对端 VPC 的 IPv6 子网间的对等连接	
	应支持多个独立地址段的专有网络（地址不重叠）可以做一对一互通的对等连接设置。支持子网级别的网络互通。	
	支持对等连接配置管理，包括创建、查看、修改、删除、配置路由等操作。	
	支持同账号对等连接配置，支持跨账号对等连接配置。	
云专线	通过物理专线实现企业数据中心与专属云的专属连接	
	应支持静态路由模式对接用户 IDC 网络设备。	
	应支持不同规格的专线接口类型，如支持 GE 接口、10GE 接口。	
	支持云专线配置管理，包括创建、查看、修改、删除等操作。	
	支持通过云管理平台配置二层桥接服务让云平台内虚拟机和云外虚拟机使用同一个网段的 IP 地址。	
NAT 网关	为专有网络 VPC 提供 Internet 通信服务，通过自定义 SNAT、DNAT 功能灵活使用网络资源 无	
	支持 NAT 网关配置管理，支持配置 SNAT 和 DNAT 规则	
	支持 NAT 网关绑定多个 EIP，形成地址池	
	NAT 网关支持绑定虚拟网络，实现云服务器实例与 NAT 网关的接入。	
DNS	支持内网 DNS	
VPN	支持 IPSec VPN，用户可以自己申请、选择 VPN 服务的配置参数	
	支持用户选择要互通的本端网络以及远端子网	

6 备份服务要求

充分利用湖北日报主备双数据中心，实现新建云平台的容灾备份。

项目名称	技术参数	证明材料要求
客户端兼容性	支持 x86 平台 windows、linux 操作系统备份，包括 Windows 2003、Windows 2008、Windows 2012、 Windows 2016、CentOS、Redhat、Ubuntu、Suse、银河麒麟、中标麒麟等。 支持任意中间件和应用程序。 支持任意数据库，包括主流的数据库 Oracle，Mysql，SqlServer，sybase，达梦等 支持 Linux 多路径存储、多 PV 线性 LVM、动态盘、跨区卷动态盘等复杂存储结构备份。 支持主流文件系统，包括 NTFS、FAT32、EXT2、EXT3、EXT4、XFS、ZFS、ReiserFS、BTRFS 等。	
虚拟机备份	采用业务整机备份技术进行备份，支持磁盘或者分区的块级备份，不采用文件级备份技术进行备份。 精简复制，智能分析磁盘的数据使用情况，只备份有效的数据块，自动忽略空闲块。备份数据大小应约等于磁盘的实际使用空间大小。通过精简复制，可以显著节省备份时间和备份的存储空间。 支持在不停机的状态下，进行数据备份。 备份数据以虚拟机镜像格式存储，支持国内主流云厂商采用的 qcow2 格式，备份数据可以被主流云计算平台直接读取并拉起虚拟机，具有和云平台兼容扩展的能力。 支持限定备份带宽。	
云硬盘备份与恢复	原云平台原设备恢复。 原平台异机恢复。 异地恢复。 支持全量、增量备份与恢复，增量备份恢复时传输的数据为增量的数据。	
恢复	支持挂载恢复，可支持磁盘、分区、卷多个级别的挂载恢复，从而提供从磁盘、分区、卷到文件级别的恢复颗粒度。 可通过恢复镜像进行恢复，支持跨平台恢复。 支持多颗粒度恢复，可以一次性恢复所有磁盘、分区、卷数据， 支持 LVM、软 RAID 恢复。	
预警方式	支持日志告警、控制台告警、邮件告警等多种告警手段。 受限于实施的环境的多样性，需要可以自定义选择告警方式，支持将特定故障类型和告警方式进	

	行关联设置，自定义告警模式。	
备份恢复	具有良好的操作体验，可以整体设置备份策略、整体执行全量备份、增量备份等操作。	
备份存储介质	使用现有浪潮 AS13000 对象存储的存储资源。	提供相关证明材料

7 运营运维要求

项目名称	技术参数	证明材料要求
整体要求	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。	
	云管理面向租户提供自服务 Portal，租户登录时支持双因素认证保证安全性。租户通过自服务 Portal 申请需要的各项云服务。面向管理员提供云运营管理和云运维能力，运营管理实现对云服务的管理功能，运维管理实现对云的监控功能。	
	服务集中监控：监管云资源的配置和使用是否合理，避免资源浪费；以及监管云服务的可用性、可靠性和性能等服务质量是否满足业务的要求。	
	统一运营管理：服务目录管理、计量计费管理、订单管理、运营统计分析等。	
	云服务门户：云服务门户主要包括云服务子门户、云运维子门户、云管理子门户和云监控子门户。云服务子门户主要是提供给各个云平台的用户使用，可通过该门户完成各种资源的申请和管理操作；云运维子门户主要是服务于运维管理人员，通过该门户实现对与运维管理有关的所有功能模块的操作；云监控子门户基于数据实时渲染等各种技术，实现云数据的图形可视化、场景化以及实时交互，让各级管理人员、用户更加方便地进行数据的个性化管理与使用。云管理子门户主要服务于运营管理组织及人员，通过该门户实	

	现对所有运营管理功能模块的操作。	
云运营管理	支持一朵云上创建多个运营单位，每个运营单位有独立的组织架构。	
	运营单位间组织、用户、资源等默认隔离，互不可见。	
	1、支持查看 VPC 网络拓扑和在 VPC 下管理网络、路由器、防火墙、安全组、弹性 IP、负载均衡器、 VPN 等。 2、支持设置或修改定时备份策略、备份副本个数。 3、支持根据提供的编排模板和资源唯一标识，对原有编排模板中的资源进行修改。 4、支持根据资源唯一标识查询原有资源编排模板。	
	支持定义资源模板，包括所需云计算资源的集合及资源间的依赖关系、资源配置细节等。	
	支持通过编排引擎自动完成所有资源的创建和配置，以实现自动化部署、运维。	
	支持云虚拟机、对象存储等多个云服务组件。	
	支持多级组织创建及管理，不同组织之间资源默认隔离，每个组织可以对应多个账号，实现跨区域资源管理。异地备调节点的组织、账号信息将通过中心节点同步，组织架构、账号信息由中心节点统一管理。	
	支持提供在组织下创建及管理资源集的功能，资源集是资源实例的集合，可包含混合云的资源实例。	
	提供登录策略的创建及管理功能，支持单点登录，控制用户登录地址、登录时间、认证方式等。	
	支持与企业已有的用户系统对接，支持组织和用户信息的同步和导入，并支持统一登录认证。	
	支持限制每个组织所能使用的云资源，以及能浏览到的云资源。	
	支持通过组织维度、资源集维度对资源实例数量进行统计包括。	
监控管理	支持从数据中心物理位置为维度层层钻取查看各资源间的拓扑关系，如机房到机柜、机柜关联的设备（物理服务器、存储设备、交换机、路由器等）、以及物理机上运行的虚拟机、虚拟机承	

	载的业务系统。	
	具备对各类业务监控进行接入的能力，包括对用户业务所在服务器运行状态的监控，服务进程监控，业务特性监控以及业务拓扑展示，可将整个业务的逻辑拓扑进行直观展示以及实时监控。	
	支持平台服务能力集中监控，提供监控数据图表，比如某一段时间内的虚拟机在线数、平台的低负载率、以及平台的可用性等	
	统计报表，支持统计平台中所包含的物理机资源、虚拟机、存储资源、网络资源等资源信息；统计各类资源的用户使用量、每类资源的使用情况，如基础云平台、业务系统的 CPU、内存、存储、IP 的资源总量及占用量	
	支持云报分析，按月统计各资源池资源容量情况、资源开通情况、以及资源使用率情况等，并支持报表导出。	
访问控制	支持用户管理，可以创建多个子账户，支持账户的查看、修改、删除等操作。	
	支持子账户权限的添加、移除、查看等操作。	
	支持创建用户组，并为用户组添加多个子账户，支持用户组的查看、修改、删除等操作。	
	支持为用户组授权，用户组内所有子用户都具有相同权限。	
	支持预定义和自定义的权限策略，控制用户对计算资源、存储资源、网络资源等的访问。	
	支持集中控制用户及其密钥，在云账号下创建并管理用户及其访问密钥，并可以为用户绑定/解绑多因素认证设备。	
	支持集中控制用户的访问权限，为每个用户或用户组绑定一个或多个授权策略，限制用户对指定资源的操作权限。	
	支持集中控制用户的资源访问方式，要求用户必须使用安全信道（如 SSL）、指定时间范围、以及在指定源 IP 条件下才能操作指定的云资源。	
	支持用户单点登录。	
组织管理	支持多级组织。	
	支持组织与租户关联，每级组织均可关联租户，组织与租户为 1:1 关系。	
管理员用户	每级组织均可创建多个管理员用户，每个管理员用户可授予一个或多个角色。	
	管理员用户可对租户下的资源进行管理。	
角色管理	支持系统默认角色和自定义角色。	
	支持角色切换，一个用户如果绑定多个角色，支持用户自行切换角色。	

	角色分为全局角色和部门角色，全局角色生效范围为所有部门，部门角色生效范围为所在部门及子部门。	
租户管理	管理员可创建多个租户，每个租户可自主管理和部署名下的资源；	
	支持租户生命周期管理，包括创建、关闭、恢复、注销等；	
	租户间资源默认隔离；	
用户管理	支持租户创建用户，并按需分配用户的资源访问权限；	提供截图证明
	支持分配用户特定资源的访问权限；	
	支持通过配置，允许用户跨租户访问资源；	
	支持用户的生命周期管理；	
	支持用户的访问凭证 AK、SK 管理；	
用户组管理	支持用户组的生命周期管理，支持组成员管理，支持用户组授权	
角色&权限管理	支持角色的增删改查管理；	提供截图证明
	支持角色授权管理，不同的角色可绑定不同的权限策略；	
	支持用户与角色、权限的绑定、解绑等；	
标签管理	支持在租户范围内创建标签并为资源打标，支持根据标签统计、导出资源；	
资源组	支持租户范围内对资源进行分组管理；支持资源添加、移除，支持资源组访问权限配置，支持资源组数据统计展示	
库存管理	支持云平台的计算、存储、网络等资源的总量及使用量以饼图、折线图等进行展示；支持配置库存阈值、告警通知	
操作审计	支持记录用户的操作行为，包括操作名称、操作描述、所属模块、操作类型、资源类型、资源 ID、操作内容、操作结果、操作用户、用户身份、操作时间等，并可通过资源类型、操作类型、操作用户、资源 ID 等进行过滤。	
认证登录	支持多因素认证虚拟 MFA，支持双因子认证密码+验证码，支持邮箱验证码和短信验证码	
登录策略配置	支持设定用户可访问平台的时间范围，支持设定访问云平台的客户端 IP 地址范围，支持设定用户尝试登录的次数与锁定时间，支持配置用户密码有效期，支持配置用户登录会话超时时间，支持配置同一用户同时在线客户端数量；	
配额管理	支持为租户预置资源额度，租户可在配额度内自行创建资源；	
	支持租户配额的实时查看与调整；	
	支持配额阈值告警	

计量管理	支持多种方式的计量数据统计，多维度分析，提供计量数据接口	
	支持对上线运营的云服务进行剂量，支持按虚拟数据中心来汇总级导出计量数据，支持导出计量详细清单。	
	支持分配计算资源量，并对资源的使用量进行统计展示；	
	支持存储资源的分配、回收，并对存储资源的使用量进行统计展示；	
	支持对网络流量进行统计展示；	
	支持按照时间维度统计计量数据，包括月、天和小时；	
	支持按组织和资源集维度统计计量数据；	
	支持按组织和时间维度进行计量数据查询；	
	支持计量报表的查询结果导出。	
计费	支持多种计费模型，计费信息多维度分析。	
	不同资源类型设置不同的资源单价。也可以根据资源规格设置资源规格的单价，同时可对项目是否计费进行开启和关闭操作。	
账单管理	支持账单查询，可按照产品类型、地域、计费模式等方式查询账单数据，支持账单导出。	
	云平台可以查看 VDC 的账单和账单明细，支持按照资源类型筛选账单明细。	
	支持用户费用报表的导出。用户可以生成费用报表。	
工单	支持用户线上提交工单，工单处理、工单流转、工单超期预警、工单统计分析、自动/手动分配工单、备注、派单升级、常见问题配置等功能	
消息中心	支持站内信、邮件、短信等消息通道的消息发送，消息数据的多维度统计	
基础设施监控	支持监控资源信息维护，其中包括区域、机房、机柜、设备类型、厂商的信息等。支持以资源树的形式查看资源关系。支持单个设备的详细信息查看，包括监控详情。支持数据批量导入；支持展示服务器和交换机的监控数据；支持通过 agent 方式获取服务器数据；支持展示设备的 cpu、分区、硬盘、接口、进程、文件等监控信息；支持获取设备的监控瞬时数据与历史数据；支持对设备进行简单搜索和高级搜索；支持展示概览信息，包括已监控设备的统计、告警信息统计、基础架构快照、设备分状态统计等图表。概览页面支持用户自定义，用户可以自由配置页面中图表的位置	
	利用设备厂商的 API 接口，提供 HDS E590 存储	

	设备资源信息展示的定制服务。	

（三） 安全服务技术要求

1 安全资源池整体要求

1、为租户应用提供安全功能，以满足等保三级要求。具体模块包括：防火墙、 IPS 、主机安全、堡垒机、日志审计、数据库审计、 WAF。

2、模块数量：云防火墙 6 套、云堡垒机 100 资产、日志审计 100 个日志源、云 WAF 6 套、数据库审计 10 实例、主机安全（虚拟机）100 套。

3、云平台各节点物理服务器的安全防护套件，数量根据所投方案足量配置。

2 安全管理平台要求

项目名称	技术参数	证明材料要求
多区域支持	支持为不同区域的不同安全资源池分别设置引流交换机，实现对分布式安全资源池部署的支持。	
授权步长	为满足不同租户安全组件的实际使用需求，云安全管理平台中应能够支持扩容单步长，如堡垒机可以设置管理资产数、数据库审计可以设置数据库实例数等。运营场景下支持租户级授权，分租户导入总包授权，租户使用时从租户授权总包中扣除授权。租户间授权互不影响。	提供相关证明材料
自服务操作	为云租户提供自助服务门户，租户可以自行登录自助服务门户，在线申请安全资源；安全市场支持查看各安全组件的介绍，包括：安全组件特点、规格描述，使用场景等；	
	租户按需选购对应的安全组件，并可以自助选择部署安全组件的区域，网络，套餐，时长等信息。	
安全组件策略下发	为满足用户通过云安全管理平台统一管理各个安全组件的需求，在云安全管理界面上能够基于每个组件下发安全策略。	

工单管理	工单列表显示租户提交的安全组件防护策略，包括防护添加、删除、编辑、启停，防护操作同安全策略管理。支持自动审批，同时支持设置审批角色对工单进行审核。	
日志审计	可为云租户提供所有安全组件的统一日志管理功能,可展示日志概览及各组件的日志情况，无需登录具体的安全组件去查看。	
日志导出	支持云租户通过云安全管理平台导出安全组件所有类型或特定类型的日志。	

3 虚拟防火墙

项目名称	技术参数	证明材料要求
规格	本次投标规格：网络吞吐：≥1Gbps，最大并发连接数：≥500000，最大新建连接数：≥15000	
访问控制	所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制,并支持地理区域对象的导入以及重复策略的检查	
入侵防御	所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息。	
	所投产品的漏洞防护特征库包含高危漏洞攻击特征。	
网络协议	支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP,手动管理 VxLan 网络;支持 MAC、VNI、VTEP 静态绑定	
IPv6 支持	支持配置 IPv6 地址,并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；	

应用识别与控制	支持应用识别,应用特征库包含的应用数量（非应用协议的规则总数）大于 2800 种，可深度识别每种应用的属性,为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类	
网络攻击防护	支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施	
	支持基于安全区域的异常包攻击防御,异常包攻击类型至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等;并可在设备页面显示每种攻击类型的丢包统计结果	

4 主机安全

项目名称	技术参数	证明材料要求
操作系统支持	产品应至少支持Windows 及主流Linux 操作系统,包括 SuSE、Red Hat、Ubuntu、Debian、CentOS、麒麟操作系统等。	需提供功能截图证明
CPU 架构支持	服务器端和客户端可同时支持信创 ARM CPU 架构、X86CPU 架构部署。	需提供功能截图证明
入侵检测	支持客户端模式的按需动态部署蜜罐,支持对恶意访问进行抓包、并可下载分析。	需提供功能截图证明
	异常进程行为检测可以根据用户真实场景自定义检测规则，对进程命令行做威胁匹配。	需提供功能截图证明
	Webshell 检测支持 PHP、JSP 语义分析检测能力，降低误报率。	
客户端部署	同时支持进程方式、容器化方式部署客户端。	

合规基线	针对服务器操作系统、数据库、软件和容器的配置进行安全检测,并提供检测结果说明和加固建议，帮助用户进行系统安全加固，降低入侵风险并满足安全合规要求。	
异常登录检测	异常登录：根据客户端上传登录流水信息，以及来自用户端设置异常规则,可实现异地登录、异常时间登录、异常账号登录、异常IP登录告警。 防暴力破解：根据客户端上传登录流水信息，以及来自用户端设置异常规则，可实现检测与阻断暴力破解行为,根据算法识别暴力破解成功行为 。	

5 Web防火墙

项目名称	技术参数	证明材料要求
规格	本次提供规格：网络吞吐：≥1Gbps，每秒新建连接数：≥10000。	
双栈防护	支持全功能IPv4、IPv6双栈防护	
基础防护	支持HTTPS服务器透明防护	
	支持自定义阻断返回信息，响应码，页面标题，重定向URL	
状态监控	支持系统状态CPU，内存，硬盘使用率以实时图形化展示，并可查询历史数据	
	支持协议连接监控，可针对协议的源目的IP，端口，源目的接口，运行时间，协议状态，收发字节数展示，可针对监控协议进行阻断以及加黑操作	需提供功能截图证明
	支持防护资产安全状态展示,可针对资产的TCP， UDP,ICMP/ICMP6， RAW-IP,HTTP.DNS等进行统计，统计的数据包括检测bytes，清洗bytes以及并发连接数,新建链接数等数据,并可根据攻击次数，定义资产的今日安全等级	需提供功能截图证明
	支持系统预览,可针对资产状态,封禁状态，攻击数据以及攻击源，攻击源地域，攻击类型，被攻击目的，被攻击域名TOP展示	
	支持接口流量的收发速率实时图形化展示，并可查询历史流量数据以流量图形化展示	

	支持攻击信息大屏实时展示,可通过产品自带的实时监测模块进行地图展示,包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件的动画统计	
访问控制防护	支持静态及动态 ARP 管理	
	支持 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则,过滤非法请求.支持多种 http 访问控制方法：GET、POST、DELETE、COPY、OPTIONS、LOCK、PROPFIND、HEAD、PUT、MKCOL、MOVE、PATCH、UNLOCK、PROPPATCH	需提供功能截图证明
安全防御	支持协议合规校验,可根据实际网络状况自定义协议参数合规标准，过滤非法数据	
	支持识别和阻断注入攻击,包括命令注入攻击，XPATH 注入防护,XML 注入防护,SSI 注入防护,JOSN 注入防护,LDAP 注入防护	
	支持组件漏洞防护	
	支持爬虫防护，黑链防护	
	支持盗链防护，并支持 referer 以及 referer+cookie 两种检测方式	
	支持 webshell 防护，内置 webshell 特征，针对文件上传内容进行检查，防止恶意 Webshell 上传，对已经上传的 webshell 发起请求的行为进行拦截阻断	
	支持非法文件上传下载防护,有效识别非法文件的上传下载行为。	
	支持敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护	
	支持敏感词防护,可针对检测位置进行自定义	
	支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护	
DDoS 防护	支持智能分析 DDOS 防护，内置五个防护等级，并可自定义防护等级	
	支持检测并清洗的攻击类型：IP 攻击，TCP 攻击,UDP 攻击,ICMP 攻击,DNS 攻击,HTTP 攻击	

虚拟补丁	支持虚拟补丁功能,支持导入 appscan 的扫描结果生成 WAF 的规则,对此类网站漏洞直接防护	
爬虫陷阱	支持爬虫陷阱防护	
蜜罐防护	支持蜜罐防护,内置后台蜜罐页面进行防护可以设置蜜罐的 url,蜜罐页面标题让攻击者攻击设置的 url 和页面	
智能封禁	支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间	
安全扫描	支持自定义 Web 安全扫描任务，支持手工，定期进行 Web 安全扫描	
	提供 Web 站点安全扫描功能	
外联控制	支持 URL 外联检测功能，针对特定外联 URL 进行监控或阻断	
	支持自定义 URL 过滤	
流量限速	支持流量限速功能,根据流量智能自动生成流量阈值	
	支持检测 TCP 并发链接数,TCP 新建链接数，TCP 带宽（c2s），UDP 带宽（c2s），ICMP 带宽（c2s），HTTP GET 速率，HTTP POST 速率，HTTP 其他请求速率，DNS 查询请求速率，并发 IP 数量等单用户和总量进行自定义阈值配置	

6 数据库审计

项目名称	技术参数	证明材料要求
数据库支持	支持传统的数据库：SqlServer、 MySQL、PostgreSQL、达梦等数据库的审计	
审计策略	审计策略支持 18 种以上分项响应条件，可支持数据库操作命令（包括 select、create 等 14 个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端	

	进程名、会话 ID、关键字、时间（含开始结束日期）等。	
组合审计规则	支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警。	

7 云堡垒机要求

项目名称	技术参数	证明材料
数据库	支持对 MySQL 等数据库的访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制。	
H5 运维	不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RDP、Telnet、VNC 和应用发布资源。	
批量登录	支持 SSH、RDP、TELNET、VNC 协议资源的批量登录功能，并且支持混合协议的批量登录，支持同时在一个页面运维不同协议的资源	
会话协同	支持运维过程中邀请其他用户参与、协助操作；会话协同过程中，协同者可以申请控制会话，创建者可以强制获取控制权	

8 日志审计

项目名称	技术参数	证明材料要求
日志审计管　理	支持日志审计生命周期管理，包括：日志采集、解析、转发、存储、分析、报表。需提供功能截图证明。	需提供功能截图证明
多源日志接　入	支持多源日志接入模块，可收集、解析、转发多种安全设备日志，为日志审计模块提供数据采集能力，满足等保三级要求。为后续智能安全分析模块提供高质量的原始接入数据以及安全设备产生的告警数据。 安全设备采集自定义模板：通用数据实时采集引擎支持多种数据源的的接入，包括	需提供功能截图证明

	syslog、kafka、Agent 等模式接入；通用数据解析引擎，可对接入数据做 gork、json 等归一化处理，同时支持数据拍生与增强；通用转发引擎，默认支持写入 clickhouse，同时持 kafka 转发。	

9 安全中心

项目名称	技术参数	证明材料要求
统一告警处置	提供安全告警事件统一处置与响应功能，帮助用户集中处理全网安全事件，提升安全运营效率。 精准安全告警识别：通过集成商业威胁情报能力对原始告警二次分析，富化关键信息，实现告警动态定级，降低信息过载。 一站式告警处置：客户可通过云安全中心，针对各类告警执行不同处置方案，包括忽略、误报、加白、线下处理操作等，联动 XDR 设备实现一键封禁功能，针对无法快速处置告警，可参考处置建议，灵活应变。	需提供功能截图证明
告警展示	支持来自于外部告警日志映射到统一告警处置中心，同时支持展示到安全大屏。	需提供功能截图证明
安全大屏	将安全攻防数据转化并呈现到安全大屏上，可实时展现攻击告警、漏洞、基线情况；实时展现攻击来源、攻击分布、明确攻击者来源及攻击情况，构建实时威胁感知能力。 全局安全态势总览：支持安全评分、3D 攻击炮图、Top5 被攻击资产、Top5 攻击类型、Top5 攻击地域，安全事件发展趋势，高危安全事件实时入侵监控	需提供功能截图证明

（四） 多云管服务技术要求

1、除新建云平台外，需对现有两个 VMWare 虚拟化资源池进行有效纳管；（版本 6.5 和 6.7 资源池各一套，共 18 节点）；

2、与主流公有云的对接和资源纳管；

3、为保证云平台 API 的规范性、互操作性以及被多云管理平台纳管能力，所投产品须至少提供基于 Restful API 接口标准预留接口，供多云管理平台调度对接。应至少涵盖计算资源、存储资源、网络资源、权限认证接口调用能力。

项目名称	技术参数	证明材料要求
基础要求	系统基于模块化架构，支持容器化部署；采用 B/S 应用架构，中文管理界面，人机界面友好。	需提供功能截图证明
	支持 HTTPS/SSL 加密访问。	
系统管理	权限管理：具备灵活的细粒度分级权限和逐级授权功能，角色权限可以后台自定义配置。权限配置可以实现并不限于最终用户可以对虚拟机创建，登陆操作，但无法进行重启，删除操作。系统管理员可以根据权限配置完成全部功能操作等。	需提供功能截图证明
	用户管理：支持多角色/权限用户组的数量、名称、权限定义，角色类型至少支持系统管理员、租户管理员（项目管理员）、最终用户（项目用户）。每个角色只能看到自己权限范围内的资源信息。	
	日志管理：具备完善的日志管理功能，日志种类包括但不限于系统运行日志、告警日志、用户登录及操作日志等，日志支持导出，不提供删除。	
统一门户	系统管理员门户：a.通过管理平台实现用户管理、云账号及资源管理、租户管理（项目管理）。b.通过平台进行企业工单管理、服务目录及资源管理。c.通过平台进行资源统计、容量管理及成本分析通过平台实现业务系统管理、应用管理、仓库管理及业务系统相关的集群和主机管理。	
	租户管理员（项目管理员）门户：租户管理员可以通过服务运营平台实现工单管理、订单管理、资源管理及配额管理等功能。	
	用户门户：a.用户可以通过自服务平台实现服务目录产品申请，订单及工单的自助申请，已申请订单、资源的管理；b.用户可以对应用或资源的持续交付以及生命周期的管理，支持续期或终止等功能。	
监控	提供对云平台各云资源池下虚拟机或云主机的 CPU 使用率、内存使用率、磁盘读写速度、磁盘写入速度、网络入流量、网络出流量的监控。	

	支持数据库监控并图表展示。支持达梦、MySQL 等主流数据库的性能监控。	
	支持自定义各项告警规则，如 CPU 使用率、内存使用率、磁盘读写速度、磁盘写入速度、网络入流量、网络出流量，当 CPU、内存使用率等监控数据达到设定阈值时触发告警。告警方式支持邮件、短信等通知。	
资源管理及交付	云管平台须自动同步及管理虚拟化平台中各项信息变动，支持自定义同步间隔时间，支持手动即时同步。范围包括但不限于如集群状态、宿主机、子网、存储、硬盘、快照、虚拟机、模板、镜像、实例、资源目录或文件夹，内容包括但不限于数量、属性、利用率、运行状态、告警等等。具有 IP 地址管理功能，可以对租户 VPC 下虚拟机 IP 地址进行动态检测和管理。	需提供功能截图证明
	服务目录定义：提供服务目录产品定义，定义范围包括但不仅限于该虚拟机在哪个资源池、群集、存储器、网络中创建等。服务目录支持产品的上架和下架。	
自服务	提供针对用户不同业务系统的服务目录，对用户所属权限范围可见的云平台、自定义编排的 IaaS、PaaS 等服务信息展示。	
	审批流程：支持多级流程，流程配置支持后台预配置。	
	工单管理：提供图形化自定义工单类型，支持拖拽方式设计自定义表单，可以关联审批流程。	需提供功能截图证明
容量管理	资源统计：支持资源总量、使用容量、剩余容量、趋势分析，统计对象包括宿主机、存储器、虚拟机等。基于私有云环境可以在统一的界面展示云环境实际计算能力，置备率，实际使用率等。	
	统计报表：支持多维度展现资源数据，并生成报表。	
计量计费	云管平台应具备专属云计费管理功能，计费策略应支持自定义：支持资源计量计费，可配置资源计量粒度，包括但不限于 CPU、内存、存储（存储大小）操作系统，所属资源分区，支持包年包月和按量付费的方式。	
	计量计费规则设置，支持规则的添加、修改、查询、删除、启用、停用等操作功能；规则包含规则名称、计量属性、属性数量、计量单位、计量周期、计量金额等。	

	租户或项目费用统计和成本分析，支持多维度统计分析，维度类别包括不限于项目、部门、单位、系统。	
自动化运维管理	支持用户自定义 Shell，Ansible 脚本，包含但不限于创建、删除、对比、查询、版本管理、语法验证、克隆等功能。提供常用脚本配置，支持用户导入脚本进行脚本的二次编辑使用，脚本也可以发布成服务提供给普通用户申请使用	
	支持 VPC 网关模式实现穿透式作业调度，自动化管理平台只与 VPC 网关特定端口通信，确保 VPC 内原有网络安全策略不做调整；	
	内置常用运维场景，CMP 应支持预置常用运维场景和用户自定义运维场景。包括但不限于系统工具，网络工具，远程命令，软件安装等，可直接使用平台内置场景，也可以基于场景做自定义调整实现运维作业。支持操作系统安全基线检测等安全相关场景。	
	自动化作业编排可以通过平台的 Web 流程定义设计器实现自动化作业任务的顺序，并行模式的灵活组合；作业编排采用的任务活动支持动态参数化节点绑定，支持实现更具通用性的流程。	
VMWare 纳管	提供对 VMWare 虚拟化资源池及单台虚拟机的纳管功能项	需提供功能截图证明

六、开标、评标及合同授予

（一）评审

1、检查投标文件是否完整、资格证明是否齐全、有无计算上的错误。

2、同一数值的表达不一致时，以文字表达为准。如投标人不接受对其错误的修正，其投标将被拒绝。

3、对于投标文件中不构成实质性偏差的不正规、不一致、或不规则，招标人可以接受，但这种接受可能会影响投标人的综合得分。

4、开评标时，评标小组依法依规严格审查每份投标文件是否实质上响应招标文件的要求，实质上没有响应招标文件要求的投标文件将被拒绝。

（二）合同授予

1、《中标通知书》作为签订合同的依据，也是合同文件的组成部分。

2、招标人发出中标通知书之后，双方基于招标文件和投标文件订立合同。

3、在签订合同之前，招标人如发现中标人的投标文件有弄虚作假的内容，

招标人将取消其中标资格，并禁止参与招标方今后的招标采购项目。

4、正式合同文本经双方协商一致，投标人应按招标文件要求及时签字、签署日期并加盖公章后送达本部。

七、售后服务

投标人提供的售后服务包括但不限于满足招标文件的要求。

八、本招标文件未尽事宜，按国家相关法律法规规定执行。

附件 1

投 标 函

致：湖北日报传媒集团招标采购部：

_____（投标单位全称）授权_____（全权代表姓名）_____（职务）为全权代表，参加贵方组织的

_____（招标项目名称）招标的有关活动。我方已充分理解贵方本项目招标公告及招标文件的全部内容，包括补充、修改、澄清、答疑文件（如果有），我方接受招标文件的全部条款，且无任何异议。

如我方中标，我方保证按投标报价的优惠折扣签订合同，不因其他任何情况而改变折扣比率。

如我方中标，我方保证忠实地执行双方签订的合同，按贵方的委托要求按期、按质、按量履行合同义务。若在合同执行的过程中，发现货物质量、规格、性能、数量等有差异，我方一定尽快更换或退货，并承担相应的经济责任。

我方同意在本招标项目开标时间起 60 天内，遵守本投标文件的承诺，且在此期限内具有约束力。

本投标函附录是本投标函的组成部分。

在签订合同前，贵方的中标通知书连同本函及附录，对双方具有约束力。

与本投标有关的一切正式往来函件请寄：

地址：_____ 邮编：_____

电话：_____ 传真：_____

投标单位（公章）：_____

法定代表人（或授权人）签字并盖章_____

年 月 日

附件 2

投 标 保 证 书

湖北日报传媒集团招标采购部：

1、我方一定严格遵守相关法律法规参与本次项目投标。

2、若我方中标，按照贵方的招标文件，积极配合招标人签订合同，并按合同要求承担本项目的实施。

3、在正式合同订立之前，本投标书连同贵方中标通知书、以及其他文件和附件成为约束双方的合同。

4、我方对出具的业绩表、人员一览表以及反映我方实力及信誉的各种证明材料的真实性负责。如有虚假行为，无条件同意贵方取消我方的投标资格和中标资格。

5、我方同意从定标日起至双方签订的合同有效期内，严格遵守本投标书的各项承诺。本投标书始终对我方具有法律约束力。

6、我方承诺，若中标，本投标书中人员安排不做更换。

投标单位：（公章）

邮政编码：

投标单位地址：

法定代表人或其授权的代理人：（章）

联系电话：

传真号码：

日期：　　年　　月　　日

附件 3

法定代表人授权委托书

本授权书声明：注册于_____（地址）的（单位全称）的法定代表人_____（法定代表人姓名、职务）授权_____（被授权人姓名、职务）为本单位的合法代理人，并将以本单位名义处理一切与_____（招标项目名称）招标投标活动中的有关事宜，代理人（被授权人）在本项目投标及合同中所签署的一切文件和处理的一切有关事宜，我单位均予承认。

本授权书于 _____年____月____日签字生效，特此申明。

法人授权代表（被授权人）情况：

姓名：_____ 性别：_____ 年龄：_____ 职务：_____

联系地址：_____

邮编：_____ 电话：_____ 传真：

授权单位（公章）：_____

法定代表人（签字或盖章）：_____

法人授权代表（被授权人）（签字）_____

授权日期：_____

注：无投标单位公章及法定代表人签章的视为无效授权。

年 月 日