第五章　采购需求

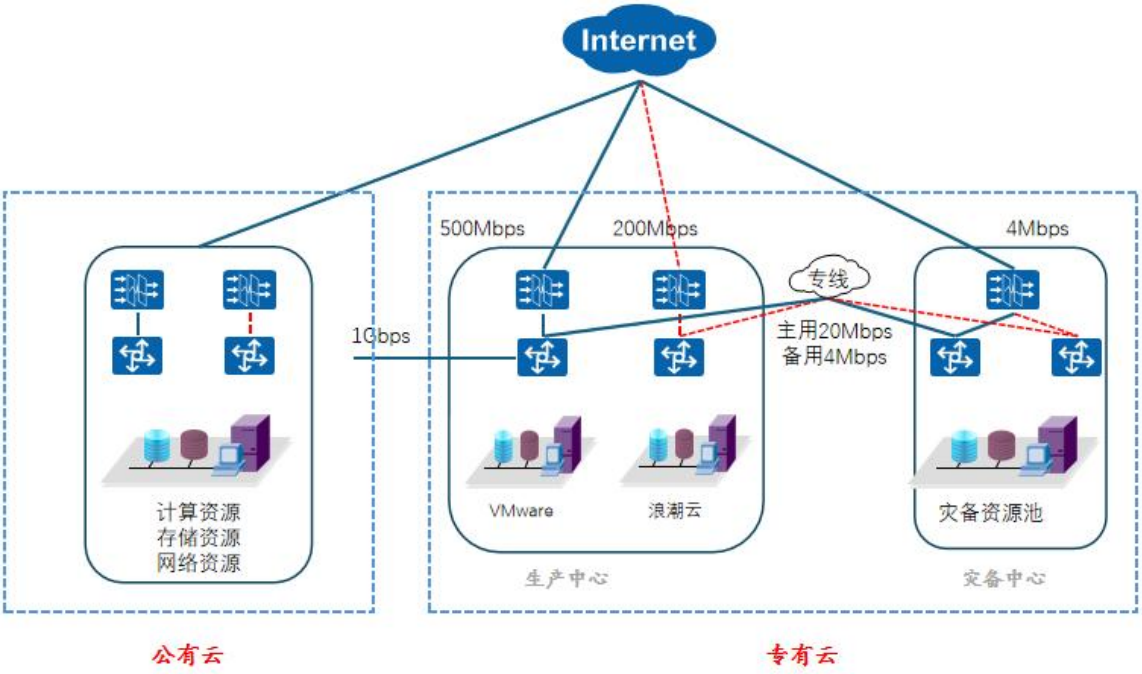
项目概述

一、背景介绍

中国工程科技知识中心（含国际工程科技知识中心，以下统一简称“知识中心”）是经国家批准建设的国家工程科技领域公益性、开放式的知识资源集成和服务平台，旨在积极发挥中国工程院学科分布优势和工程科技领域的示范引领作用，发挥院士群体智慧，与国内信息技术领先企事业单位、权威数据服务机构等共同形成知识服务协同创新体系，支撑国家战略决策和高端智库建设，推进我国数字中国建设。

知识中心主要包括基础设施体系、资源体系、技术产品体系、以及平台系统体系等。基础设施运维服务主要是构建基于云的计算、存储和网络运行环境，目前知识中心形成了由专有云、公有

云组成的混合云架构基础设施体系。



公有云由知识中心项目通过采购第三方服务商的云服务实现，主要承载业务弹性伸缩需求较高或高并发、业务需敏捷开发、互联网数据采集等服务，为面向国内外用户的公益性平台系统提供支撑。

专有云由知识中心项目自建，主要承载数据资源长期存储、数据安全性要求较高、业务对云计算资源定制需求较高、为院核心业务系统提供支撑。专有云设有生产中心、灾备中心双节点。生产中心部署了韦睿(VMware)软件和浪潮云虚拟化资源池，配备双互联网出口，通过专线对接灾备中心，完成数据同步。灾备中心搭建独立灾备资源池，支持对重要数据的异地灾备。

二、需求概述

为保证知识中心相关平台系统健康、稳定运行，本次拟采购包括公有云运维服务、专有云运维服务，需求概述如下：

（一）公有云运维服务

基础设施云服务。满足知识中心业务应用对计算环境、存储环境、网络环境的需求，为相关业务提供稳定可靠的基础云服务。

应用云服务。根据知识中心实际需要，提供类似于云邮箱、短信通知、云视频等应用层服务。

云安全服务。提高公有云服务的安全保障能力，满足高安全等级系统运行的需要。

其他服务。包括跨云业务迁移技术服务、统一网元管理、上云技术服务及公有云账户服务等。

（二）专有云运维服务

基础设施服务。提供支撑客户业务系统、服务器、网络设备稳定在线运转的底层基础设施服务，核心服务包含机柜租赁、网络出口租赁、专线租赁等机房场地租赁服务。

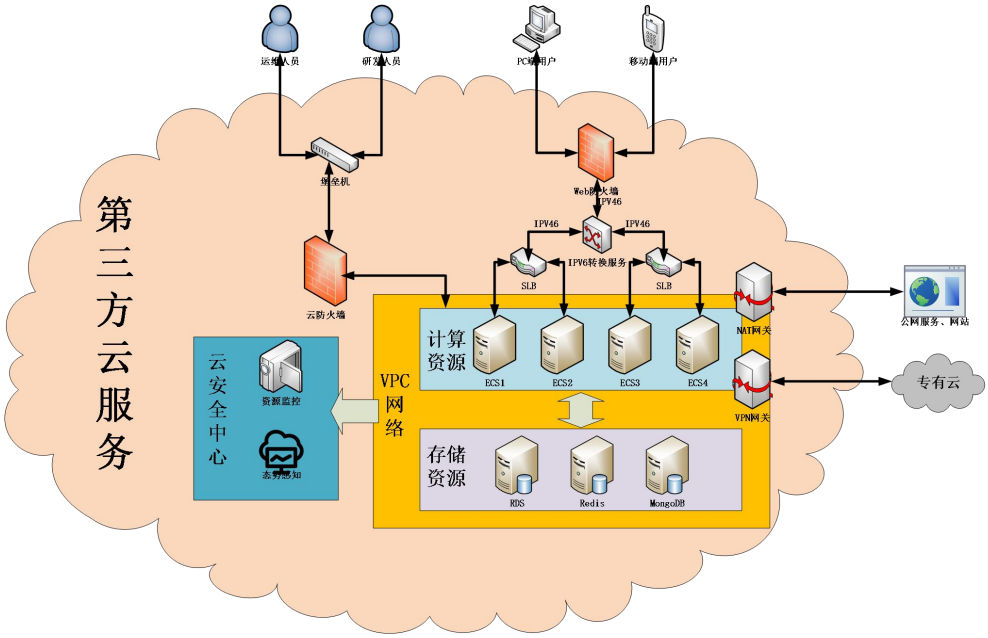
运维驻场服务。主要包括定期巡检维保服务、重大节假日保障服务、软硬件环境替换改造服务、等保合规安全保障服务等。

公有云服务需求

一、概述

1. 背景介绍

中国工程科技知识中心目前使用阿里云作为公有云服务环境，网络部署结构如下图所示。



截止到 2025 年 12 月底，采购人使用 200 台云主机、20 台关系型数据库、10 台负载均衡设备，基本保证了知识中心相关应用系统的健康运行，大致使用情况如下。

1.使用 200 个云主机实例，约 2000 核心 CPU、6000GB 内存、100TB 硬盘存储、200MB 独享带宽。

2.使用 20 个关系型数据库（MySQL）存储实例，共计 140 核心 CPU、196GB 内存、29000GB 存储空间。

3.使用 4 个 Redis 存储实例，共计 256G 存储空间。

4.使用 2 个 MongoDB 存储实例，共计 12 核心 CPU、24GB 内存、4000GB 存储空间。

5.使用约 450TB 对象存储空间。

6.按照网络安全等级保护的有关要求，使用了相关云安全服务中心、堡垒机、防火墙（含应用防火墙）等安全服务。

2. 需求概述

为保证知识中心相关业务系统健康、稳定运行，拟继续采购以下公有云服务：

（1）**基础设施云服务**。满足知识中心业务应用对计算环境、存储环境、网络环境的需求，为相关业务提供稳定可靠的基础云服务。

（2）**应用云服务**。根据知识中心实际需要，提供类似于云邮箱、短信通知、云视频等应用层服务。

（3）**云安全服务**。提高公有云服务的安全保障能力，满足高安全等级系统运行的需要。

（4）**其他服务。**包括跨云业务迁移技术服务、统一网元管理、上云技术服务及公有云账户服务等。

二、技术需求

1．基础设施云服务

表 1 基础设施云服务需求

序号	服务类型	服务能力描述	数量
Case1	虚拟化服务器实例	虚拟化服务器	110 台
Case2	对象存储服务	云存储服务	300T
Case3	关系型数据库服务	关系型数据库	16 个
Case4	非关系数据库服务	非关系数据库	-
Case5	网络服务	弹性组网、流量加速等组网能力	-

虚拟化服务器实例

虚拟化服务器实例需求详见表 2，共 1080 核 vCPU，3760GB 内存，约 90TB 存储空间。

表 2 虚拟化服务器实例需求

序号	处理器（核心数）	内存（GB）	存储容量（GB）	独享带宽（MB）	数量（台）

序号	处理器（核心数）	内存（GB）	存储容量（GB）	独享带宽（MB）	数量（台）
Case1-1	2	4	500	4	20
Case1-2	4	8	500	0	20
Case1-3	8	16	500	0	20
Case1-4	8	32	500	0	20
Case1-5	16	64	1000	0	20
Case1-6	32	128	1000	0	10

（1） ★CPU 采用 X86 架构，主频不低于 3.2GHz，全核睿频不低于 3.6GHz，单核最大睿频不低于 3.9GHz。

（2） 内存容量支持 4G/8G/16G/32G/64G/128G 等主流配置。

（3） 网络带宽支持 1M 到 100M 动态可设，可选支持 BGP。云主机网络资源要求支持按照使用流量计费或按照固定带宽计费。

（4） 为保证业务稳定性，云主机实例不允许采用共享性、抢占式实例。

（5） #支持按策略定时自动创建快照，并按照设定的保留时长自动删除。

（6） #创建快照极速可用，回滚云盘时性能无损。

（7） #应用一致性快照，保证数据库数据的可恢复性。

（8） △支持镜像构建能力，自动化构建镜像。

（9） △支持镜像检测能力，自动检测镜像缺陷。

对象存储服务实例

对象存储服务实例需求详见表 3。

对象存储服务实例应支持云对象存储服务，云对象存储应支持标准存储（文件访问次数较多，每月在 1 次以上）、低频存储（访问次数较少）、归档存储（档案、操作日志、备份等）等不同存储方式。标准存储容量不低于 50TB，低频存储容量不低于 50TB，归档存储容量不低于 200TB。

表 3 对象存储服务实例需求

序号	存储类型	存储容量（TB）
Case3-1	标准存储	≥50
Case3-2	低频存储	≥50
Case3-3	归档存储	≥200

（1） ★本次采购标准存储/低频存储/归档存储实例规格必须均采用同城冗余存储（多 AZ），提供更高的可用性保障。

（2） #支持为存储空间创建多个接入点 Access Point，并对不同的接入点配置不同的访问控制权限及网络控制策略。通过在不同业务场景使用不同的接入点进行访问，降低大规模的共享数据集数据访问管理的复杂度。

（3） #提供文件元数据索引能力。支持利用文件的元数据自定义索引的条件，从而快速获取期望文件列表。

（4） #支持将标准存储、低频存储和归档存储的本地冗余类型转换为同城冗余类型，以实现单 AZ 向多 AZ 的容灾升级。

（5） △支持数据复制时间控制 RTC，具备在 10 分钟内复制 99.99%的对象的能力。

关系数据库服务实例

关系数据库服务实例需求详见表 4。

关系数据库服务实例需求为 96 核 vCPU，192GB 内存，18TB 存储空间。

表 4 关系数据库服务实例需求

序号	数据库类型	处理器（核心数）	内存（GB）	存储容量（GB）	数量（台）
Case4-1	RDS 数据库	4	8	1000	8
Case4-2	RDS 数据库	8	16	1000	6
Case4-3	RDS 数据库	8	16	2000	2

（1） 关系数据库采用一主一备高可用，X86 架构，支持自动故障切换，支持增加只读实例扩展读能力。存储采用高性能本地盘，I/O 延时可低至微秒级，支持扩容至 15TB。

（2） ★高可用版应部署在 2 个不同可用区，SLA 不低于 99.99%。

（3） #支持全密态数据库、设置 SSL 加密。设置透明数据加密 TDE、云盘加密。

（4） #支持 serverless，RDS MySQL Serverless 实例不采用固定规格，实例的计算资源会在指定的范围内根据业务负载自动弹性伸缩，存储资源也根据数据量自动扩容。

（5） 关系数据库服务支持 MYSQL、MariaDB、PostgreSQL、MicrosoftSQLServer 等数据库引擎。

（6） 支持提供通过页面实时管理数据库会话，支持通过页面结束数据库会话，支持下发数据库限流指令。

非关系数据库服务实例

非关系数据库服务实例需求详见表 5。

非关系数据库服务实例应支持 Redis 数据库、MongoDB 数据库、数据库备份及数据管理等实例。

表 5 非关系数据库服务实例需求

序号	数据库类型	处理器（核心数）	内存（GB）	存储容量（GB）	数量（台）
Case5-1	Redis 数据库	-	≥256	-	2
Case5-2	MongoDB 数据库	64	128	≥10000	1
Case5-3	数据库备份	-	-	-	4
Case5-4	数据管理	-	-	-	2

（1） ★Redis 数据库采用云原生部署模式，集群架构，高可用类型（双可用区）。内存存储容量不小于 256GB，兼容 Redis5.0/6.0/7.0 及以上版本，连接模式采用代理模式，分片规格不低于 4GB；采购数量 2 个。

（2） ★MongoDB 数据库采用 64 核 128G 独享性实例，支持 MongoDB7.0 及以上版本，三节点，三个节点跨可用区部署，支持机房级别同城容灾切换，存储空间不低于 10000GB，存储类型采用 SSD 盘,最大 IOPS 不低于 5 万,最大吞吐量不低于 350MB/s。

（3） 数据库备份实例备份数据源支持MySQL、PostgreSQL、MongoDB、Redis、Oracle 等主流数据库。每月备份数据量约1600GB，采用逻辑备份,采购数据库备份实例数 4 个。

（4） 数据管理：采购实例数 2 个，提供细粒度权限管控、灵活可定义的设计规范、审批流程构建专属数据库 DevOps 方案。

（5） △Redis 数据库兼容 4.0/5.0/6.0/7.0 版本。

（6） △Redis 数据库数据库代理（proxy）支持热 key 缓存。

（7） MongoDB 数据库应支持实例会话管理，可查看会话列表，具体操作，执行耗时等信息，可对会话进行批量 kill 操作。支持 IP 白名单设置，支持提供灵活的安全访问管理能力。

（8） 数据库备份实例支持秒级恢复、恢复演练等能力，保证数据高可用、高安全。

（9） 数据库备份实例支持通过重复数据删除技术,降低备份数据的存储成本；支持通过存储快照和克隆技术，使得备份数据秒级可用。

（10） 数据管理实例支持查看 SQL 窗口中所有操作行为，包括登录信息、操作信息、SQL 语句详情、影响行数、耗时等。

（11） 数据管理实例支持对高危 SQL 操作（如 DDL、批量变更等）进行权限审批与管控，经审批通过后可在受控范围内执行不受常规规则限制的 SQL 操作。

网络服务

网络服务实例需求详见表 6。

网络服务应包含主机负载均衡、弹性公网 IP、NAT 网关、网络 VPC、网络 CDN、边缘安全加速、专线接入、VPN 网关等产品。

表 6 网络服务实例需求

序号	服务类型	服务能力描述	数量
Case6-1	主机负载均衡	对云上流量按需分发	≥10 个
Case6-2	弹性公网 IP	为云资源提供互联网访问能力	≥100MB 带宽
Case6-3	NAT 网关	网络地址转换	2 个
Case6-4	网络 VPC	构建逻辑隔离的网络环境	1 套
Case6-5	网络 CDN	弹性内容分发	200TB
Case6-6	专线接入	连接数据中心与云上的网络服务	10GE
Case6-7	边缘安全加速	提供动静态加速、TCP/UDP 四层加速	1 个
Case6-8	VPN 网关	基于加密隧道实现云下与 VPC 安全互联	≥20Mbps

（1） ★主机负载均衡服务实例数量不低于 10 个，独享性实例、可用区数量不低于 3 个，总带宽峰值不低于 2000Mbps，日常带宽/峰值带宽的比例不低于 30%。

（2） 弹性公网 IP 服务应提供互联网链路带宽服务、互联网 IP 地址租用服务，支持配合应用开发厂商提供网络策略配置，带宽不低于 100Mbps。

（3） ★2 个 NAT 网关实例数量，按照峰值带宽计费方式，总峰值带宽不低于 30Mbps，日常带宽/峰值带宽的比例不低于 30%。

（4） 网络 VPC 服务应支持针对相对独立的业务系统通过 VPC 部署业务。支持实现不同业务虚拟主机的网络隔离，不同业务之间云主机内网默认不可相互访问，且同一用户的不同云主机之间可以通过配置安全组策略等方式，实现内网不可互访。

（5） ★边缘安全加速服务实例规格类型包含支持 HTTPS 请求数、WAF 请求数、拦截流量等，支持版本管理、等候室，支持 Bots 机器流量防护，年度支持流量不低于 3000GB。

（6） 专线接入要求配合完成知识中心另外在北京市建设的专有云环境（专有云）到公有云之间专线开通工作，包括但不限于公有云接入端口协调、所在机房纤芯资源配置等，专线接入独享 10GE 端口。潜在供应商应在投标文件中提供专线部署的方案建议，提出专线接入的物理端子位置建议。其中，从公有云接入物理端子至公有云所在机房区域的光交箱之间的光纤跳纤，由供应商负责完成（采用 2 芯光缆）；由公有云所在机房的指定光交箱端子至专有云机房之间的光缆铺设/租赁/光模块，由采购人通过其他项目完成。

（7） ★VPN 网关采用国密型公网双隧道，提供 IPsec-VPN，不低于 20Mbps。

（8） 主机负载均衡服务支持通过设置虚拟服务地址，将客户端请求分发到后端多台云服务器，提升应用的服务能力和可用性。支持四层（TCP、UDP）、七层（HTTP、HTTPS）协议。

（9） #主机负载均衡服务采用全冗余设计，无单点，根据流量负载进行弹性扩容，在流量波动情况下不中断对外服务。支持同城容灾。

（10） △主机负载均衡服务集群支持亿级并发连接，单实例最大支持100万并发。

（11） △主机负载均衡服务可根据业务的需要，随时增加或减少后端服务器的数量，扩展应用的服务能力。

（12） 弹性公网支持查看公网IP的出、入方向秒级带宽峰值、出、入方向秒级包速率、出、入方向秒级丢包速率、出、入方向新建TCP连接速率。

（13） 弹性公网IP支持BGP(多线)线路,在中国大陆地域,经白名单授权后可额外支持中国电信、中国联通、中国移动等单线线路。

（14） △支持查看出、入方向秒级带宽峰值、出、入方向秒级包速率、出、入方向秒级丢包速率、出、入方向新建TCP连接速率。

（15） 弹性公网IP支持基于地域粒度和实例粒度,分别以一元组功能（云端IP）、二元组功能（云端IP、对端IP）、五元组（云端IP、云端端口、协议、对端IP、对端端口）展示入云方向和出云方向流量的排行。

（16） NAT网关服务支持处理TCP、UDP和ICMP分片包。

（17） △NAT网关提供Session统计功能，包括并发连接数、丢弃连接数、新建连接速率/新建丢弃连接速率、并发连接水位/新建连接水位。

（18） #CDN 内容分发系统应通过公安部网络安全等保三级测评。

（19） △CDN 服务支持配置组配置，用户可以通过 api 批量对域名回源进行配置。

（20） #CDN 支持将相关参数、头部信息作为缓存的 key，当用户携带不同参数、头部信息时，可以区分进行缓存。

（21） 边缘安全加速产品提供在控制台界面实时展示的即时日志功能，无需额外存储。提供全量的回源 IP 列表，并且在用户未确认的情况下不能直接启用新上线的回源 IP。

2. 应用云服务

表 7 应用云服务实例需求

序号	服务类型	服务能力描述	数量
Case7	DNS 解析	域名解析服务	≥2 个顶级域名
Case8	云短信	验证码、通知短信	50 万条
Case9	云视频直播/点播	高清视频直播/点播服务	≥200TB/200TB
Case10	云邮箱	邮箱服务	≥50 用户
Case11	API 网关	提供服务暴露及流量管控	1 套
Case12	内容审核	基于 AI 技术的内容审核监管	1 套

DNS 解析

（1） 支持 DNS 解析服务，支持知识中心及其下属子系统的域名申请、续费与 DNS 解析。

（2） 实例规格类型为公网 DNS 解析，用于互联网域名网站解析、邮箱解析等，支持常见解析记录类型包含：A、AAAA、CNAME、MX、NS、TXT、SRV、CAA 类型记录，支持 IPv4、IPv6、域名等类型地址按轮询/权重规则解析应答；支持 DNS 攻击保护能力，攻击防御不低于每秒 1000 万次，域名数量不低于 2 个。

（3） #需提供增值电信业务经营许可证-互联网域名解析服务业务复印件。

（4） 支持解析到云服务器、负载均衡。

云短信

（1） 支持短信服务，支持知识中心及其下属子系统的注册、登录短信验证码以及短信通知。

（2） ★实例规格为 50 万条，可用于发送验证码、通知短信和推广短信等。

（3） 支持统一的短信发送、回复接收及转发、回执查询等基本功能，支持单发和群发短信。

（4） 兼容国内三大运营商的短信收发，具有短信量统计、短信发送状态实时监控等功能。

（5） 支持对短信送出环节进行全链路监控。

云视频直播/点播

（1） ★标准直播年流量包不低于 200TB，视频点播年流量包不低于 200TB。

（2） Web 推流 SDK 支持本地混流，如一个画面同时将屏幕分享、摄像头进行混流。

（3） 支持客户免配置转码模版,实现 B 帧和 AAC 自动转码。

（4） 支持控制台配置全链路 WebRTC 直播，并且在直播控制台可配置，和超低延时直播共用一套 SDK。

（5） 控制台支持查看推流、录制回调最多 1000 条，最近 7 天的回调记录。

云邮箱

（1） 支持云邮箱服务，具备基本的邮箱功能。

（2） ★应支持不低于 50 个用户,个人网盘容量不低于 5GB,共享网盘容量不低于 20GB。

（3） 深度集成日历、任务、云盘与即时消息，最大支持 5000 人组织架构；

（4） 丰富开放的邮箱 API 接口,支持单点登录、用户同步、AD 统一验证等企业集成需求。

API 网关

（1） ★API 网关每秒最大请求数（最大短连接）QPS 不低于 80000，SLA 不低于 99.99%，网络访问类型为公网，公网线路为 BGP（多线）。

（2） 支持 API 策略管理，包括限流、重写、Header 修改、跨域、认证、流量复制、超时和重试等功能。

（3） 支持集成容器和微服务体系，支持 K8s、Nacos、函数计算等多种服务发现方式。

（4） 支持集成日志和监控服务，可一览网关核心指标和风险指标。

（5） 支持 API 设计、开发、测试、发布及下线的全生命周期管理。

内容审核服务

（1） ★支持对图片、文本、视频等对象进行多样化场景检测，降低内容违规风险，实例规格年调用量不低于 2 亿次。

（2） 支持检测指定的文本中是否包含违规信息，包括但不限于：色情、广告、灌水、涉政、辱骂等。

（3） △内容安全文本审核，能够支持智能识别语种，支持超过 15 种主流语种，包括但不限于：汉语、英语、阿语、法语、日语、韩语、俄语等。

（4） △内容安全图片审核，支持 gif 图片检测并可设置截帧时间。

（5） 支持检测音频文件或语音流（例如直播流）中的风险或违规内容，例如垃圾信息、广告、暴恐、辱骂、色情、灌水、违禁、无意义等内容。

（6） #内容安全视频审核，支持通过接口异步检测，支持通过接口主动查询检测结果和通过 callback 方式回调检测结果。

支持 AVI、FLV、MP4、MPG、WMV、MOV、WMA、RMVB、m3u8 等格式视频。支持设置截帧频率。

（7） 支持弹性扩容，具备快速布控、快速审核的应急响应能力。

（8） #支持实时监控各服务接口 QPS 占用，支持实时监控各服务接口服务状态。

3．云安全服务

具备不低于网络安全等级保护第三级的安全防护能力，提供堡垒机、Web 防火墙、云防火墙、数据库审计、云安全中心等云安全服务，保障网络安全。

表 8 云安全服务实例需求

序号	服务类型	服务能力描述	数量
Case13	DDoS 防护	DDoS 防护服务	可接入域名数≥60 个
Case14	云防火墙	不多于 200 台云主机以及互联网边界、VPC 边界、主机边界	带宽不低于 200Mbps
Case15	Web 应用火墙	防御各类 OWASP 常见 Web 攻击并过滤海量恶意 CC 攻击	可接入域名数≥60 个
Case16	运维安全审计	统一、高效、安全的运维通道	200 台主机（线上及线下）
Case17	日志审计	日志审计服务覆盖对象存储、网络、RDS 数据库以及各类安全服	1 套

序号	服务类型	服务能力描述	数量
		务日志	
Case18	数据库审计	数据库资产安全监控保障	≥16 个数据库
Case19	SSL 证书	全站 HTTPS	10 个专业版 OV 通配符 SSL 证书
Case20	云安全中心	检测、防御、响应于一体的云安全管理平台	≥160 台云主机防护（包含弹性需求）

DDOS 防护

（1） ★保底防护带宽不低于 30GB，弹性防护带宽不低于 50GB，业务带宽不低于 100Mbps，业务 QPS 不低于 3000，防护域名数不低于 60 个，端口数不低于 60 个。

（2） #DDoS 最大防护能力不低于 1.5T。

（3） 支持智能 AI 防护。

（4） 提供 DNS 解析和 IP 指向两种接入方式。

云防火墙

（1） ★云防火墙提供跨 VPC 互访流量的访问控制、横向攻击防护、流量分析。防火墙带宽不低于 200Mbps，防火墙实例不低于 3 个，访问控制策略授权规格不低于 50000 个。

（2） #提供云厂商可信云云防火墙能力增强级检验证书。

（3） △支持一键平滑无损开关 VPC 边界防火墙，创建、开启及关闭 VPC 边界防火墙时，无需更改当前的网络拓扑，对业务无影响。

（4） 支持 AI 访问流量，包含主动外联 AI 服务、内网 AI 业务访问等。

（5） △支持资产自动同步，可设置新增资产自动保护开关，对新增资产自动添加防护，新增资产自动保护需支持按资产类型开启。支持手动同步资产。

（6） 支持策略分析服务，包含互联网边界、NAT 边界、VPC 边界等。

WEB 应用防火墙

（1） ★QPS 不低于 5000，可接入域名数不低于 60 个，具备 API 安全检测功能。

（2） #提供云厂商可信云云 WEB 防火墙能力检验证书复印件。

（3） #支持共享集群、独享 IP、智能负载均衡集群的接入和选择。

（4） #根据客户端 IP、请求 URL 及常见的请求头字段定义请求特征匹配条件，对命中匹配条件的请求执行相应处置。可以使用自定义规则拦截访问指定 URI 的请求、对包含指定 User-Agent 内容的请求进行校验等。

（5） △API 安全通过离线分析业务访问日志，自动检测流量中存在的所有 API，并支持根据接口特征，自动识别 API 业务用途。

（6） △检测 API 存在的未授权访问、敏感数据暴露等各类安全风险，并提供详细的风险分析及安全处置建议。

（7） △监控分析 API 的调用行为，及时发现各类异常访问或攻击行为。

运维安全审计

（1） 实例采用双引擎架构，多可用区，高稳定性保障，授权云主机数量不低于 200 台，并发不低于 100 台。

（2） 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、用户登录客户端限制等。

（3） 支持对重要命令进行实时审核：运维人员执行命令后，系统响应动作包括：指令审批、阻断会话、产生告警。

日志审计

（1） 日写入数据量不低于 50GB，存储时间不少于 6 个月。

（2） 支持分隔符、正则表达式等文件采集、支持客户端对日志进行结构化解析、支持 syslog 协议采集。

（3） 支持 Log、Metric、Trace 多类型数据接入。

（4） 支持提供采集时、写入时、写入后多阶段实时数据加工能力。

数据库审计

（1） ★支持数据库、对象存储、大数据等多类型的数据审计，满足等级保护合规要求，不低于16个数据库实例和1TB对象存储容量。

（2） 支持跨语句、跨多包的访问方式及绑定变量值的审计。

（3） 支持IP地址、数据库用户、时间、对象、应用用户、操作系统用户、客户端工具、数据库实例分组，并且分组对象可以直接在规则中引用。

（4） △支持OSS、数据库的数据泄漏监测与响应。

SSL证书服务

（1） 提供10个通配符域名OV证书。证书品牌为国产品牌，支持vTrus或CFCA。

（2） 提供域名SSL证书服务，可支持服务器、负载均衡等设备部署配置，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证信息传递的安全性。

（3） 支持包括OV、EV等多种证书类型，覆盖单域名、多域名和泛域名多种域名格式，并支持纯IP证书。

（4） 支持通过API的方式调用SSL证书管理的能力，包括证书申请、查询、吊销等。

云安全中心

（1） ★提供不低于160台云主机防护，云安全态势检测分析不低于15000次，恶意文件检测不低于10万次，不低于2400GB防勒索能力。

（2） ★提供不低于10个防篡改授权，不低于10个应用防护授权。

（3） 提供对常见Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞、应急漏洞五种漏洞类型进行扫描，并支持CVE系统漏洞的一键修复。

（4） 支持主动防御设置，包含恶意主机行为防御、防勒索、网站后门链接防御，可实现自动阻断、主动拦截。

（5） △支持自动分析资产在互联网上的暴露情况，查看资产暴露的通信链路、链路详情、弱口令和漏洞信息。

（6） #对网站目录的网站后门（Webshell）进行检测，支持文件落盘检测+周期全盘检测，支持PHP、JSP、ASP文件检测，支持静态引擎、沙箱引擎、词法引擎、机器学习引擎等多引擎检测。

（7） △对恶意进程进行识别和告警，支持多种引擎对常见病毒文件的告警和一键隔离，支持主动实时拦截已知的勒索病毒、挖矿程序等恶意病毒进程、文件。

4. 其他服务

表9 其他服务需求

序号	服务类型	服务能力描述	数量

序号	服务类型	服务能力描述	数量
Case21	业务互迁移	业务、数据迁移	-
Case22	统一网元管理	混合云网络管理	-
Case23	账户服务	账户管理服务	-
Case24	重要时期保障	云平台重保服务	-
Case25	技术支持及培训	云产品技术培训	-

业务互迁移

（1） 知识中心不同业务系统存在数据互通的需要，需要在专有云、公有云之间通过 API 接口、内部传输通道等方式进行互通，供应商应在投标文件中提供专、公有云接口、数据互通建议，并配合实施。

（2） 采购人提出数据迁移需求时，供应商应能够提供镜像、用户数据和应用的迁入和迁出的服务。包括但不限于：提供虚拟机镜像、数据和应用可以导入导出的接口或界面、操作说明，并说明可支持的虚拟化平台、镜像文件格式等；应支持线上和线下迁移。

（3） 根据业务运行的实际需要，知识中心业务系统存在从专有云搬迁到公有云、从公有云搬迁到专有云的实际需要，供应商应在投标文件中提供业务系统互迁移的方案建议，并配合实施。该工作如需费用，应包含在投标报价中。

统一网元管理

（1） 专有云相关服务和第三方服务云的相关服务需纳入部署在专有云的统一网元管理系统中进行管理，供应商需配合做

好网元统一纳管的支撑工作。该工作如需费用，应包含在投标报价中。

（2） 知识中心在专有云部署了集中终端威胁防御系统，支持操作系统的防病毒、主动防御等功能；供应商提供的云安全服务需能够提供混合云统一安全管理能力。

账户服务

（1） 支持创建主账号和子账号，同时支持主账和子账号进行关联。

（2） 支持在联时设置允许子账号继承主账号商务折扣、请求查看子账号财务信息、请求查看子账号消费信息。

重要时期保障

（1） 在重要会议、重大活动、重大节日期间，供应商应提供专项服务，保障相关云资源，以及重点网站、业务系统安全。

技术支持及培训

（1） 供应商须向采购人提供相关培训，满足采购人对云平台及其云资源、云服务进行有效管理的要求。参加培训人员由采购人根据业务使用的实际情况确定，培训人数不少于 2 人，培训时间不少于 24 小时。

（2） 技术培训内容至少应包括：云平台所能提供相关产品功能、性能、配置介绍；云平台及其云资源、云服务、网络资源

的使用、配置、运维；云安全产品的使用、配置、运维；业务上云架构、弹性配置等。

（3） 供应商应在投标文件中提出对于培训具体内容、时间、期次、地点等详细安排。

三、项目实施相关要求

1．配合项目监理工作

（1） 根据信息化建设项目实际需要，采购人拟为本项目聘请相关咨询机构负责信息化建设的全流程监理。供应商应积极配合监理完成相关工作。

（2） 供应商应与监理机构建立合理、高效的沟通协调机制，规范项目组织间工作交流、任务传递、消息共享、问题商讨的方式方法，包括但不限于：邮件沟通机制、例会机制、专项会议机制、周报机制、月报机制、工作联系单机制及联络机制等。确保采购人业务需求、工作计划、调整方案能够顺畅地上传下达，确保重大事项及时向采购人通报和汇报。

（3） 如有需要，供应商应配合监理机构建立质量保证体系，制定项目建设质量控制方案，并督促落实各环节质量控制内容和目标。供应商应根据整个系统建设的工作计划，对阶段性工作成果进行审查和测试，并向提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个系统建设的质量。

2．迁移要求

本项目涉及的业务系统均为采购人在用系统，业务连续性是首要保障需求。如果因变更发生云服务平台或业务系统迁移。迁移过程中产生的相关费用（包括为保证系统不中断，继续在原来

的云上运行产生的费用），均由供应商承担。该工作需提供承诺函，如不需要迁移则不需提供承诺函。

服务厂商须提供完整、可落地的系统迁移实施方案。迁移方案应包含但不限于迁移范围、迁移拓扑、迁移步骤、停机窗口规划、风险识别与应急回退预案、数据校验规则、测试验证方案、人员分工、交付物清单等内容，保障业务系统、配置数据、账号权限、文档资料等完整平稳迁移，确保业务连续不中断。原运维厂商需配合新任服务商完成全流程迁移实施、联调测试、问题处置，直至迁移工作全部验收通过。

（1）迁移范围

迁移内容包括但不限于所有当前部署在“阿里云”平台上运行的相关服务、存储的相关数据，以及一切相关系统配置、安全策略、备份信息。

（2）迁移方案

云服务提供商负责云迁移调研工作，并根据调研结果编写详细的《迁移方案》，经采购人及其组织的专家评审通过后方可实施。

《迁移方案》应明确所有迁移对象及相应的迁移技术方案与实施流程（包括但不限于应用服务器、规范化数据、非规范化数据、云安全服务及配置、其他已开通的云服务及配置）。

《迁移方案》应明确以业务不中断、数据不丢失为前提，还应包含新旧云平台环境切换方案，迁移过程中可能出现的风险保障预案和异常回滚预案。

《迁移方案》应明确迁移工作的具体实施工作计划。

（3）迁移时效

在用户业务不间断（不受任何影响）的情况下，需在较短时间内快速完成迁移工作，迁移工作不得影响用户业务正常运行、数据不可丢失。

供应商要保障所有相关服务平滑迁移，且迁移后系统正常运行。

（4）迁移确认

迁移成果需由采购人指定的第三方测试单位出具测试方案，测试方案由建设单位、云服务提供商及建设单位委托的监理单位对测试方案进行确认，三方确认后开展测试工作，通过第三方机构测试后，视为交付工作完成。

（5）迁移费用

为确保迁移过程中数据不丢失、系统业务不中断，本次供应商应负责与原公有云服务商主动对接，系统迁移所需各项费用（包括但不限于供应商迁移测试阶段的云资源费用及调试费用等），由本次供应商负责解决并包含在本次投标报价中。

业务迁移过程中，为保证系统不中断，继续在阿里云运行而产生的有关费用由中标供应商承担。

供应商需对承担迁移过程中产生的费用提供承诺函并加盖供应商公章。

3．项目团队人员配置

投标人应为本项目组建不少于 4 人的项目团队，其中项目经理 1 名、技术负责人 1 名，项目经理和技术负责人均应由云服务

商原厂提供；其他人员应能够满足项目实施、迁移、运维和安全保障等工作需要。

项目经理，应具备系统分析师、信息系统项目管理师、注册信息安全管理员（CISO）、所投云服务商原厂工程师认证证书。主要负责项目总体组织、计划、质量、进度、风险及沟通协调等工作。

技术负责人应具备系统规划与管理师、信息系统项目管理师、所投云服务商原厂工程师认证证书。主要负责项目技术方案、架构设计、实施迁移、运行保障及重大技术问题处置等工作。