第1包

“\*”号为关键技术指标，不满足投标将被拒绝

1. 基本要求

\*(1) 投标人IDC中心需提供300M独享IDC带宽。

\*(2) 投标人提供上联核心网络设备须具备双路热备冗余。

\*(3) 投标人提供北京地区12个标准机柜，每个机柜供电≥10A。

\*(4) 提供光明日报社至IDC机房一条裸光纤连接。

(5) 带宽质量优异，具有较好的与基础运营商的网络连通速度，无瓶颈。

(6) 服务期限1年。

1. 技术要求
   1. 机房要求
      1. 机房地理位置及环境优越，距离光明日报社机房不超过20公里，须提供具体百度地图中查询地址；
      2. 拥有先进的IDC机房设施及充足的带宽资源；
      3. 机房整体承重大于750公斤/平米，局部承重不低于800公斤/平米；
      4. 有防静电设施或设备；
      5. 具备基础运营商机房环境标准，或通过国际认证的Tier3以上IDC机房标准；
      6. 具有单独的货梯，以保证客户设备的运输与安全；
   2. 网络要求
      1. 要求网络结构安全冗余：设备冗余、链路冗余、端口冗余、路由冗余；
      2. 接入网络不多于三跳至基础运营商核心网络，99.9%的网络连通性保证；
      3. 可根据需求对网络进行路由优化；
   3. 机柜要求
      1. 提供不低于42U的标准机柜，可上标准服务器导轨及按需求提供机柜托盘；
      2. 每个机柜至少10个托盘，且能按需提供；
      3. 机柜具有独享封闭机笼或独立门锁；
   4. 配电要求
      1. 每机柜双路UPS供电，总容量大于等于20A；
      2. 机房供给双路独立的高压供电电源；
      3. 备用应急电源采用柴油发电机组，保证后备供电时间不低于8小时；
      4. 双路UPS部署，后备时间满负载不低于30分钟；
      5. 保证可用性99.99%以上的持续供电率；
   5. 空调要求
      1. 温度需保持在21℃-26℃，湿度需保持在30-70%，温度、湿度符合国家计算机场地技术标准，设备具备根据要求提高标准的能力；
      2. 自动温湿度监控，自动报警；
      3. 具备大容量的空调系统，N+1配置，保证所有机柜的通风散热要求；
   6. 消防要求
      1. 有烟雾感应探测器及温度感应探测器；
      2. 有火灾智能预警系统；
      3. 具备环保高效的管道式气体灭火系统；
   7. 安全服务要求
      1. 监控系统7×24小时进行全方位机房监控、录像；监控历史数据保留至少3个月；
      2. 防止任何无关人员进入，保证机房空间的私密性；
   8. 监控要求
      1. 有集中监控系统，可对机房内的温度、湿度、电力等情况进行全面检测；
      2. 对网络连接状况实时监测及告警；
      3. 对机房网络和点对点专线进行7×24小时的监控与服务；
      4. 提供7×24小时的安全管理与视频监控服务，视频资料至少保存3个月；
   9. 故障处理要求
      1. 明确故障响应和故障解决的时间。如果服务出现故障，在规定的故障解决时间内解决故障，并向客户提交事故报告；
      2. 对电力供应及网络连接等发生的意外情况紧急寻呼告警，并以最快速度排除故障；
      3. 提供7×24小时的客户服务。
   10. 搬迁要求

投标方需提供机房搬迁过程中涉及的实施方案、技术服务、网络资源及所有必须的设备、工具等。为尽可能减少甲方业务中断所造成的经济损失，投标方需在新的机房环境提供过渡期间使用的网络环境和设备环境，并提供过渡期间的所有技术服务。

第2包

“\*”号为关键技术指标，不满足投标将被拒绝

|  |  |  |
| --- | --- | --- |
| 项目 | 序号 | 招标要求 |
| 云平台  基本要求 | 1 | 有详细的云平台各项服务价格统计，且客户可根据需求自由选择服务项目 |
| 2 | 服务级别；协议承诺级别达99.95% |
| 3 | 可对所有宕机时间都提供SLA；机房维护时间，受攻击等在保障范围内 |
| 4 | 服务类型：提供基于虚机托管的基础架构即服务（IaaS）与应用托管的平台即服务（PaaS），用户不需维护底层基础架构，只需应用开发，支持软件即服务（SaaS） |
| 5 | \*机房标准： T4标准机房，数据中心内万兆互联 |
| 6 | 要求异地容灾，异地机房数据中心间有专线数据同步，数据中心间必须有专线连接，具有异地容灾能力，提供高可靠高可用服务。云服务商必须获得国家相关主管部门合法的运营资质 |
| 7 | \*互联网接入：要求多运营商接入，确保全国用户访问畅通；离主干网跳数不超过2个 |
| 8 | 兼容性：认知服务 API 跨编程语言、跨硬件设备、跨软件平台 高扩展性：平滑升降级，同时支持自动化扩展缩放 架构灵活：可根据需要选择认知服务的不同 API 或者自定义 API 服务 快速搭建解决方案 支持快速部署上线 灵活弹性的成本控制 |
| 9 | 技术支持：提供免费技术支持服务，免费版本升级和专业的24x7x365售后服务专线支持等。提供丰富的在线文档和社区资源。提供明确的具有财务保障的服务级别协议 |
| IaaS  虚拟机  技术要求 | 1 | 具备提供身份标识与访问控制机制，能与企业内部身份管理机制集成，并能与第三方平台实现联合身份关联验证机制  提供针对应用架构层级的负载均衡机制，如面向Internet的负载均衡和非面向Internet的内部层级负载均衡机制，并支持TCP和UDP的协议  入侵检测和防护系统、拒绝服务攻击防护、定期渗透测试帮助识别内部和外部的潜在威胁并加以预防，具备流量清洗机制 |
| 2 | \*操作系统和数据库：提供正版Windows Server 2012/2012 R2、 2008/2008 R2, Ubuntu，CentOS，SUSE, SQL Server 2014/2012 SP1等  提供在线升级和版本切换 |
| 3 | 虚机管理工具支持：支持网站界面、脚本工具和REST API等三种途径管理配置虚机 |
| 4 | 多种资源配置支持：提供多种CPU、内存、带宽等资源的组合，支持内存密集型的资源配置，CPU核数支持1～8个，内存支持高达56GB；  支持磁盘条带化横向扩展，提供可并能在线添加或分离数据磁盘。虚拟机磁盘提供99.9%可用性。支持SSD存储 |
| 5 | 操作系统映像管理：允许用户自定义映像和上传自己的操作系统映像 |
| 6 | \*迁移支持：支持虚拟机在用户数据中心和公有云平台之间的迁移，不绑定云平台，并提供官方迁移工具 |
| 7 | 虚机功能支持：可以实现物理机的全部功能，虚机具有自己的资源（内存、CPU、网卡、存储），可以分配单独的IP地址等 |
| 8 | 监控管理：云平台提供内置性能监控功能，对资源中CPU、网络、磁盘使用率等指标进行实时数据统计，并提供丰富的扩展接口，实现服务级别的监控和预警 |
| 9 | 自动缩放支持：应提供虚机横向缩放和纵向缩放功能，并可根据计划时间和虚机CPU指标等参数进行自动缩放控制 |
| 10 | 为计算节点提供内置可用性集、负载均衡和故障恢复 |
| IaaS  虚拟网络  技术要求 | 1 | 网络功能支持：提供公共DNS服务，可选择自建的DNS服务器；允许虚机有独立的局域网IP地址和对外的公共IP地址；允许端口转发端点和自定义的负载均衡监控情况探测；支持虚机对虚机间所有基于IP的协议。配置固定公网IP地址，不受虚拟机关机影响。支持虚拟机按照实际使用时间收费，支持按照分钟收费 |
| 2 | VPN支持：支持Site-to-Site, Point-to-Point, Point-to-Site和VNET-to-VNET的VPN打通，提供对常用的VPN设备品牌如Cisco、Juniper、F5等的支持 |
| 3 | DNS支持：提供DNS服务，虚拟网络提供99.9%可用性，VPN网关提供99.9%可用性 |
| IaaS  存储  技术要求 | 1 | 虚拟网络支持：允许用户为单个应用服务的基础设施建立一个虚拟私有网络，同一个账号可以创建多个虚拟网络。支持与本地网络打通，架设混合云。单台虚拟机网络连接不少于100Mbps，配置越高则网络带宽越高  虚拟网络支持：允许用户为单个应用服务的基础设施建立一个虚拟私有网络，支持虚拟子网划分，同一个账号可以创建多个虚拟网络。支持与本地网络连接，架设混合云  网络隔离功能：用网络隔离来防止部署之间不必要的通信，通过访问控制阻止未授权的用户访问系统。  网络访问控制：按需制定全局安全策略，控制云端服务器访问Internet，  提供CDN服务 |
| 2 | 冗余备份支持：支持云平台多份数据冗余，且有异地备份机制，支持故障转移 |
| 3 | 提供多种存储类型服务，类型包括非结构化的二进制和文本数据存储，消息队列传递存储，非关系结构化数据存储 |
| 4 | 提供多种访问数据方式：支持通过RESTful访问协议，存储客户端和驱动器的方式，有相应的SDK调用机制，存储可直接支持SMB/CIFS文件协议，实现多虚拟机实例共享挂载存储 |
| 5 | 支持内置CDN节点分发 |
| 6 | 提供具有安全性的存储服务调用方式 |
| 7 | 提供可调颗粒度的监控，收集存储服务的入口/出口、可用性、延迟及成功百分比等数据的度量值 |
| 8 | 提供日志记录，可以查询读、写和删除存储数据的操作日志 |
| PaaS  技术要求 | 1 | 提供安全访问存储服务的密钥机制 |
| 2 | PaaS平台应支持语言：.NET, Java, PHP, Python, Node.js，有相应的开发SDK |
| 3 | 网站服务：提供网站应用一键式开发部署功能，选择拓展选项，上传代码和数据库即可完成服务搭建；支持多种部署方式，可使用现有常用开发工具，或者直接从支持 Git、GitHub、TFS 等源代码管理部署现有网站；提供内置的自动缩放功能；支持.NET, Java, PHP, Python主流开发语言和框架；提供内置的监控和警报机制 |
| 4 | 数据库服务：提供内置的成熟的数据库服务，不需要用户单独运维管理操作系统层；支持多种规模的数据库大小，提供灵活内置的可管理性，内置高可用并且支持大规模横向拓展 |
| 5 | 服务总线：提供应用程序之间的消息传递基础设施 |
| 6 | 支持PaaS和IaaS的混合模式 |
| 7 | 活动目录：提供云应用程序的标识管理和访问控制功能的服务，提供本地的身份认证体系集成 |
| 8 | 云服务框架：提供一种不需要单独维护操作系统和中间件层的云服务框架，通过上传配置应用信息和服务框架配置文件，即可使用应用的持续可用性和弹性伸缩 |
| 云平台管理  技术要求 | 1 | 媒体服务： 实现视频自动转解码，并根据访问请求实现弹性伸缩 |
| 2 | 提供API、SDK等接口，可以与第三方管理软件结合或二次开发 |
| 3 | 提供自动化作业，支持周期性的计划程序执行 |
| 4 | 提供操作日志记录，支持对单个账号内的所有历史操作记录查询 |
| 5 | 提供灵活科学的账号管理分配机制，允许多个管理员共享一个资源账号，允许同一个企业账号下拥有多个子资源账号 |
| 6 | 管理员可查看单个账号和企业总账号的历史资源消耗清单和余额信息，提供邮件提醒 |
| 云平台安全 | 1 | 支持双中心提供高可用性和异地容灾 |
| 2 | 24 小时监视物理安全性： 采取物理措施构造、管理和监视数据中心，防止未经授权访问数据和服务以及防范一些环境风险。要求具备入侵检测和防护系统、拒绝服务攻击防护、定期渗透测试和法医式工具帮助识别云平台内部和外部的潜在威胁并加以预防，具备预测全球性安全风险能力 |
| 3 | 入侵检测和 DDoS： 入侵检测和防护系统、拒绝服务攻击防护、定期渗透测试和法医式工具帮助识别云平台内部和外部的潜在威胁并加以预防 |
| 4 | 运营和支持人员仅在获得授权的情况下才能访问数据。授予权限时，应管理和记录其访问情况。数据中心对存储数据的系统访问通过锁箱流程进行严格控制。未经许可不得复制、移动、转移、引用等 |
| 5 | 要求通信加密： 提供内置的 SSL 和 TLS 加密方法使用户可以加密部署内、部署之间、从公有云到本地数据中心以及从公有云到管理员和用户的通信 |
| 6 | 数据加密： 应提供包括 AES-256 在内的各种加密功能；  规范性：基于ISO/IEC 27001:2005 审核和认证，通过可信云服务认证，SSAE 16/ISAE3402,CSA CCM，PCI DSS，工信部云安全认证，完全符合国际和国内安全标准；  付费模式：支持按年付费，默认提供云平台全部现有功能服务，按照各项功能使用量计费  每年为客户免费提供云平台使用培训，并且培训课程不少于八次  提供上门售后服务  24x7x365售后服务专线提供免费技术支持服务，提供丰富的在线文档和社区资源 |

|  |
| --- |
| **采购列表** |

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务描述 | 单位 | 具体配置 |
| 1 | 虚拟机-通用计算-基本级别 | 台 | 4个内核，7GB RAM， 500GB附加磁盘（含正版WINDOWS2012服务器操作系统）40台 |
| 2 | 虚拟机-通用计算-标准级别 | 台 | 8个内核，14 GB RAM，500GB附加磁盘（含正版Linux服务器操作系统）40台 |
| 3 | 虚拟机-通用计算-高级级别 | 台 | 16个内核，32 GB RAM，500GB附加磁盘（含正版Linux服务器操作系统）15台 |
| 4 | 数据存储 | T | 40T存储量 |
| 5 | 传输 | T | 传入每月可提供20T  所有云服务需提供400GB带宽 |
| 以上资源使用周期365天 | | | |