项目需求

注：

1、如本章内容与其他章节有冲突，以本章内容为准。

2、如本章内容与国家法律法规相冲突的，以相关法律法规为准。

3、如本章内容与国家、地方强制标准相冲突的，以强制标准为准。

一、采购人提出的服务需求

（一）项目基本情况、项目背景、采购内容

随着医院医疗信息化的快速发展，需新增采购基础计算、存储资源承载医院信息系统。考虑传统物理服务器在整个系统健壮性、安全性、冗余性表现较低，运维压力大且数据安全无法保证，云计算技术发展日益成熟，根据对系统的调研，本次采取购买云计算服务的方式部署医院信息系统。根据《网络安全法》及等保2.0相关要求，支撑医院正常运营的各项业务应用需要满足《网络安全等级保护基本要求》中的等保三级的要求,同时要满足医院互联互通评级和电子病历等级评审中相关的机房、硬件、网络和安全等方面要求。

试用期：合同签订后30个工作日内完成云计算服务交付，提供不少于1个月的试用期，试用期满后方可组织项目验收，试用期未达要求，甲方有权无条件作废合同。

服务期：合同签订后30个工作日内完成云计算服务交付，提供不少于1个月的试用期，试用期未达要求，采购人有权无条件结束合同,

试用期结束20个工作日内组织验收，服务期自验收合格日起3年，合同一年一签。

本项目服务期限为三年，根据财购【2018】215号文件，本项目3年期满后，在原合同价格不变、服务对象认定服务良好以上情况下，可一年一签续签采购服务合同，签续期限不得超过3年。

（二）技术方案或服务内容、范围

1、设计原则

（1）标准行业统一

医院信息化系统云服务平台建设过程中必须贯彻使用行业统一的规范体系和中台服务，依托行业统一的技术体系和安徽省指导意见构建我院全新的医疗信息化系统。

（2）业务高可用部署

根据成本风险平衡原则以及运行管理要求，核心业务系统采用“一主一备”布局模式，实现应用级高可用。若系统或应用故障造成业务中断，备用系统可自动在分钟级内切接管并恢复业务，切换时间小于2分钟。

（3）安全保障有力

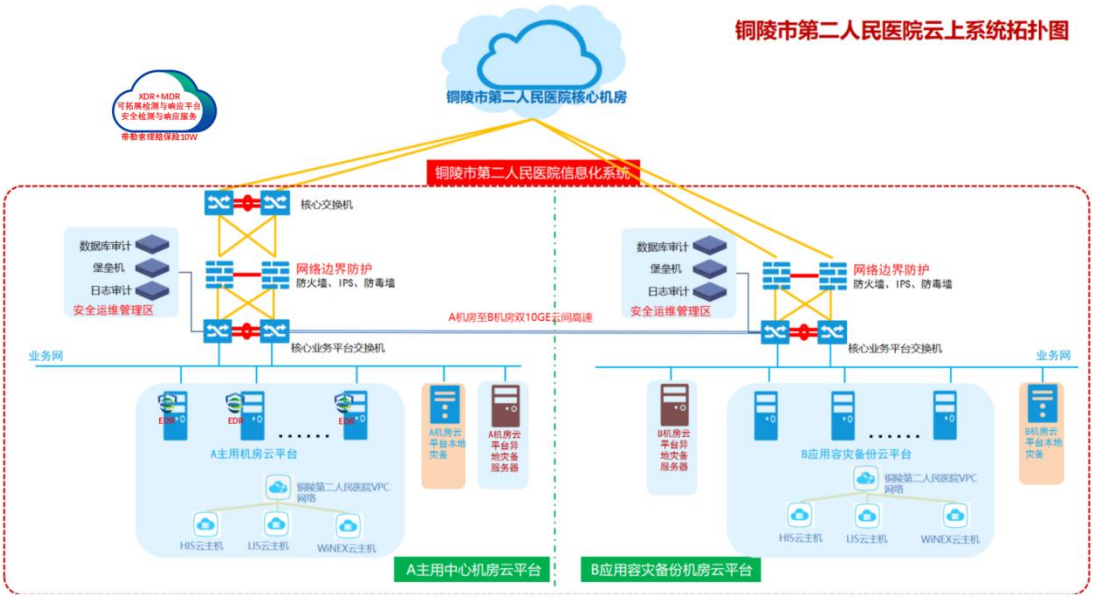
按照满足等级保护2.0三级要求建设，如下一代防火墙、入侵防御、云主机安全服务、杀毒软件等。

（4）数据备份

为保障医疗数据的安全，所有业务系统数据库和应用程序需要备份到集中备份系统中。数据备份策略可根据数据的变化频率和数据量大小随时调整。在发生数据被破坏或丢失时，可通过备份系统恢复需要的数据。并每日将完整备份传输至甲方指定位置。

2、云计算服务方案设计

本次为医院上云的各业务系统提供云资源服务，包括计算、网络和存储资源；同时为保障业务连续性，核心业务系统需提供系统级高可用保护，对于同一个系统，需要在云平台上部署两台云主机，并通过高可用软件实现系统高可用，当云主机出现系统级故障时，业务可自动切换到备用云主机运行，从而快速恢复业务运行。系统所用数据库为Microsoft SQL Server 2008或以上版本。



总体技术架构图

2.1云计算服务

云计算平台分为物理层和虚拟化层，物理层提供硬件资源，采用X86服务架构,支持未来部署ARM服务器；虚拟化层基于硬件来构建池化的虚拟资源，包括服务器虚拟化、存储虚拟化、网络虚拟化和监控/运维系统等。云平台满足等保2.0三级要求，保障平台的安全性。通过配置选型高可靠、性能卓越的服务器以及资源的HA集群设计，提供高性能、可靠的计算资源池，云资源池内资源可根据需要由用户自行调整。

云计算平台通过云计算软件抽象出来各类云计算的服务，来满足不同业务场景的需要。基于这些服务可以无需关注底层平台的复杂性，直接调用各类计算资源，同时规避维护的困难性。这些云服务既涵盖了传统IOE提供的计算和存储能力，同时也包含了传统IOE架构难以满足的大规模数据处理能力。

云计算平台底层采用标准的x86服务器，通过部署云计算软件，将各个产品按照集群进行整合，对外提供统一的服务。云平台的分布式调度系统采用有向无环图的方式调度。通过分布式调度系统进行计算及存储资源的分配与调度，构建了一个安全的、可支撑海量计算与存储资源需求、且一定程度兼容现有应用运行环境的云平台。

针对HIS、手麻和PACS等核心业务系统（见详细清单说明），每个系统开通两个云主机，并实现应用级的高可用，当某个核心系统的其中一台云主机故障时，另一台云主机可自动接管并恢复业务。

2.2网络服务需求：根据组网需求，并综合考虑安全、性能、以及效率等因素，计划采用如下解决方案：

铜陵市第二人民医院到云中心机房云平台双路由电路(光缆线路不同路由)、确保网络带宽及安全。

2.3 IDC机房托管服务

IDC机房满足消防、UPS、油机、精密空调、动环监控等保障。

防雷接地系统配置机楼防雷、市电引入防雷、UPS电源防雷三级防雷，大楼及机房接地。

机房需具有火警探测器、烟雾报警器的自动报警，具有气体灭火系统等完善的消防报警系统。

机房的主要出入口、设备通道设置远程监控，并对监视情况进行显示、录像、查看及回放等操作，对机房安全进行监控。

机房拥有专业机房运维团队，负责机房关键基础设施（包括供配电系统和机房空调系统）的运行管理、日常维护和安全保卫，提供日常设备巡检与24小时现场支持服务（包括人员和设备进出）等。

2.4运维保障服务

针对机房基础设施、支撑网络及云平台的建设与运维，需要达到高可用、稳定、安全的目标，提供全面的保障及运维服务，运维管理对象包括：机房、物理设备、虚拟设备、云管理平台、运维管理平台等承诺对外提供的各种服务。

在租用云平台服务期间，云服务商需提供全程的运维服务。运维服务自签订的合同生效之日起，至合同失效之日止。

在运维服务期间，云服务商应提供保障专有云平台正常运行的所有技术服务和支持，服务内容包括：不限定时间技术服务、现场支持技术服务、故障排除、定期巡检服务、技术升级服务、接口服务、相关规范标准或业务变更后的修改服务等。双方因合同终止等原因终止购买服务时，云服务商应协助用户进行云平台上所运行的应用系统及数据的迁移工作。

在服务期间，云服务商需安排不少于5名技术服务人员组建成运维服务团队，团队成员根据职责的不同，需由项目经理、技术负责人等

人员组成，团队成员保证24小时通讯畅通。为保证服务响应及时性，服务团队内的所有成员须常驻项目所在地。云服务商需提供运维服务方案，包括服务方式、服务范围、故障响应、应急保障及技术力量保障等方面的内容。运维服务期间内需保证 7*24 小时服务，在接到用户故障报告后响应时间不超过 0.5 小时，修复时间不超过6小时，以保证用户的正常使用。遇系统出现故障或意外情况导致系统不能正常运行时，应针对不同响应级别的即时响应进行应急处置。

同时，本项目服务周期为3年，服务期满云服务商应无条件配合采购人做好所有数据及业务的迁移工作。

3、业务需求：

云计算服务能力需求：根据业务系统架构、系统使用人数等综合评估，医院信息化系统能力需求满足380核vCPU、1100G内存、40T普通存储空间、IDC机房托管服务、灾备服务、云上安全服务，并满足后期按需调整云计算数量和规格，具备提供高性能物理服务器的能力,同时对院内现存若干台服务器托管运行，确保我院所有业务互联互通，整个系统正常运行，各客户端均可正常使用，整个项目所涉及的硬件与软件必须有合法授权，详见服务内容。

3、服务内容：

服务名称	服务说明	技术参数
云计算服务	CPU:380核； 内存:1100G；	（1）支持自定义报警器内容。支持常见的虚拟资源和物理资源报警，包括但不限于CPU、内存、网卡和

	云盘：40T	磁盘等资源。支持自定义报警条件和报警间隔时间。
		（2）☆云平台支持对云主机整个生命周期的管控。包括创建云主机，启动云主机，停止云主机，删除云主机，彻底删除云主机，在线克隆云主机，重置云主机。（需提供截图证明）
		（3）云平台支持扁平网络和VPC网络。
		（4）☆能够接管已有的VMware VCenter环境，同时接管KVM、VMWare两套虚拟化环境。（需提供截图证明）
		（5）云平台支持USB设备透传到云主机。
		（6）☆云平台为国产自研产品，需提供软件著作权证书复印件或扫描件。
		（7）支持云主机使用多个弹性IP。
		（8）支持自定义云主机MAC地址，支持创建过程中和创建之后指定云主机MAC地址。
		（9）云平台支持配置二层网络MTU大小。
		（10）☆云平台支持黑洞路由。云平台支持设置黑洞路由，防止内网流量意外走到公网，导致流量泄露和带宽被消耗。（需提供截图证明）
		（11）☆云平台须支持IP-SAN/FC-SAN 透传，将物理LUN直接透传给云主机使用，实现更好的性能和存储特性支持（需提供截图证明）
		（12）☆新增云主机与原物理服务器满足内网1000M互通，需求提供实现方案及承诺，否则视为不满足。
		（13）云平台所使用服务器、普通存储等设备均采用X86架构，支持线性扩容；宿主机单台配置要求不低于2*Intel Xeon Gold 5115处理器，256G内存，10GE*2。
		（14）☆所有资源API开放，提供开发手册、REST API、Java SDK, Python SDK，提供承诺函。
		（15）☆须支持配置IPv6、IPv4或双栈网络，根据需求选择地址类型（需提供截图证明）
		（16）支持通过Access Key授权云平台API调用。第三方用户可以在云平台获取Access Key来访问云资源，支持配置Access Key ID和Access Key Secret

		作为用户身份标识信息，是外部程序调用API时的唯一凭证。
		（17）☆须支持基于TCP/UDP/HTTP/HTTPS协议的云路由负载均衡服务，用户创建的负载均衡器可以将公网地址的访问流量分发到一组后端的云主机上，并支持自动判断并隔离不可用的云主机，从而提高业务的服务能力和可用性。（需提供截图证明）
		（18）☆须支持对云主机、云盘以及云平台数据库进行本地备份、异地备份（需提供截图证明）
		（19）须支持共享云盘，能够把一块云盘共享给多个云主机使用（需提供截图证明）
		（20）云平台存储为分布式存储，架构为三个副本及以上数据保护。
		（21）☆提供双机冗余方式保证业务的高可用性
网络服务	内网专线服务(医院到中心机房云平台双10GE电路,光缆线路不同路由)	（1）☆电路光缆线路需要至少2条物理不同路由的线路
		（2）☆1000M电路要求裸纤
		（3）交换机配置4*10GE光口，24*GE电口。
		（4）☆交换机为主备冗余方式。
		（5）☆接入核心交换设备
		（6）☆保证院内现在已在用的外接第三方网络和接口网络的连接和通讯
灾备服务	云主机及云盘数据备份	（1）☆将云主机、云盘本地备份、异地备份（需提供截图证明）
		（2）☆支持灵活定义备份策略：包含增量及定时全量备份，备份间隔可指定小时、天、周，最小备份间隔可达到15分钟，同时须支持配置保留备份保留天数，以健康利用备份存储空间；备份任务支持网络QoS和磁盘QoS，支持备份数据网络，保证备份服务不影响正常业务服务质量（需提供截图证明）
		（3）支持从本地备份数据恢复资源时可选择新建资源以及覆盖原始资源
云安全下一代	提供边界安全防护,可为	（1）产品支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式。

防火墙服务	用户提供L2-L7层各类威胁的检测和防护,能够有效应对传统网络攻击和未知威胁攻击的网络安全产品。满足客户对安全访问,攻击防护以及应用识别和控制等需求。	（2）产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等。
		（3）产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型。
		（4）★产品内置超过4000种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。（需提供产品功能截图证明）
		（5）★产品内置不低于10800种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明）
		（6）产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。
		（7）产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。
		（8）★产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。（需提供产品功能截图证明）
云日志审计服务	云日志审计服务,协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及审计违规。	（1）支持多种类型设备的日志采集，支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于780种日志对象的日志数据采集。
		（2）支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取等多种方式完成日志收集；
		（3）★支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。（需提供截图证明）

		（4）支持拓扑管理，能够基于拓扑图的资产相关数据信息快速查看资产评分、安全事件分布、告警分布等，支持通过拓扑下钻查看对应资产的关联事件、审计事件、日志数量。
		（5）支持预置审计策略模板，包括：Windows主机类审计策略模板、Linux/Unix主机类审计策略模板、数据库系统类审计策略模板等，内置审计规则数量不少于40条。
		（6）★支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则（需提供截图证明）
		（7）★支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。（需提供截图证明）
		（8）内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持提供日报、周报、月报和自定义时间导出报表，
		（9）★支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。 （需提供截图证明）
云主机安全服务	云主机安全服务，提供虚拟化主机安全轻代理防护能力，集成防病毒、漏洞扫描、基线检查、文件实时监控、勒索病毒立体防护等功能	（1）本次投标授权许可包含server服务器端授权25个，PC端授权400个，管理中心1个；投标人免费提供设备3年质保，提供工程师安装、实施、培训服务；
		（2）三年勒索保险服务：针对勒索病毒场景，与EDR绑定一起交付客户（信息系统须已安装EDR并正常启用），当客户信息系统遭受勒索病毒攻击被加密时，根据保单约定责任范围赔偿如应急响应费用、数据修复费用、勒索损失等，共计10万保额；
		（3）产品需通过公安部检测获得网络版防病毒产品（一级品）销售许可证书；
		（4）★支持对CPU、内存、磁盘读写、网络上下行

		流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断；（需提供相关截图证明）
		（5）★支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露；（需提供相关截图证明）
		（6）★识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为（需提供相关截图证明）
		（7）可对渗透的收尾阶段的数据清除行为进行识别和阻断；
		（8）提供专门的勒索风险评估功能，提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密，支持白名单设置；。
		（9）支持运行文件的病毒查杀;支持支持图片、视频等多媒体文件的病毒查杀;支持查杀各类Office文档中的宏病毒、夹带型木马;支持对扫描发现的网马进行自动查杀设置。
		（10）支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用；支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据；
云堡垒机服务	对日常内部运维中日常的各种误操作、恶意操作提供精细化控制和操作过程全审计，有效解决用户内部运维过程中的各种风险	（1）支持协议：字符协议：SSHv1、SSHv2、TELNET，图形协议：RDP、VNC，文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板等。
		（2）★支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（需提供产品功能截图证明）。
		（3）用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证。
		（4）内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴。
		（5）★支持运维水印、录像水印、监控水印开启（

		需提供产品功能截图证明）。
		（6）★支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作（需提供产品功能截图证明）。
		（7）支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批。
		（8）★支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人（需提供产品功能截图证明）。
		（9）支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯。
云数据库审计服务	提供SQLSERVER、Oracle数据库安装维护服务	（1）支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、达梦、人大金仓、南大通用、MongDB、K-DB、虚谷。
		（2）★精细化日志秒级查询，通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快。（需提供产品功能截图证明）
		（3）★TB级日志秒级查询、支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多SQL语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询。（需提供产品功能截图证明）

		（4）自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。
		（5）支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询。
		（6）★内置大量SQL安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp_addrolemember提权、web端sp_addrolemember提权、查询内置敏感表、篡改内置敏感表等。（需提供产品功能截图证明）
IDC机房托管服务		（1）要求IDC机房满足消防、UPS、油机、精密空调、动环监控等保障
其它服务要求		（1）★本项目提供服务内容要求必须可以通过等级保护2.0三级评测（不含评测费用，如测评不通过，后续费用由承建方承担）。
		（2）★如遇医院信息化政策调整，医院可以终止合同
		（3）★保证医院的数据安全，不外传，不泄露医院信息，否则承担相应后果；提供承诺函装订入投标文件
		（4）★合作期满后或合同中止，后期如不合作，无条件配合院方完成数据回迁，且不得复制和扣留；提供承诺函装订入投标文件

	（5）满足全院医务人员使用的物联网卡服务
	（6）★提供的云计算的主、备资源池全部部署于铜陵辖区内且部署云计算资源池的机房取得等保2.0三级测评证书；提供相关承诺函和证书装订入投标文件。

二、主要标的一览表

此表中服务公告名称、服务范围、服务要求由采购人列出，服务时间、服务标准由投标人填写，将随中标结果公告一并发布，接受社会监

督。未填写此表按无效标处理。

服务名称	铜陵市第二人民医院信息化系统云服务采购项目
服务范围	服务范围包括不限于以下内容：根据业务系统架构、系统使用人数等综合评估，医院信息化系统能力需求满足380核vCPU、1100G内存、40T普通存储空间、IDC机房托管服务、灾备服务、云上安全服务，并满足后期按需调整云计算数量和规格，具备提供高性能物理服务器的能力，同时对院内现存若干台服务器托管运行，确保我院所有业务互联互通，整个系统正常运行，各客户端均可正常使用，整个项目所涉及的硬件与软件必须有合法授权。
服务要求	满足采购人要求的项目需求内容
服务时间	
服务标准	