# 采购需求

## 一、用户需求书

### （一）项目背景

医院于2000成立开始就致力于医联信息化建设，至今已经建成了HIS、PACS、LIS、A、EMR等应用系统。根据《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》要求，医院须加大信息化投资力度，进一步升级改造原有的信息系统，建设医院管理信息系统（HMIS）、医院资源管理信息系统（HRP）、临床信息系统（CIS）及建立基于电子病历的医院信息平台等临床及运营信息系统，建设信息集成平台及临床数据中心，达到国家医疗健康信息区域卫生　信息互联互通互级四级甲等及电子病历五级要求。通过建设信息系统，在进一步规范医院医疗业务发展的基础上，提升医院的医疗服务能力、运营管理能力，提高患者满意度，充分发挥医院信息系统在促进医院业务发展、降低医院运营成本、提升医疗服务能力方面的重要作用。

如何充分利用影像数据，病历数据、检验检查结果、诊疗费用等在内的各种数据，搭建合理先进的数据服务平台，为广大患者、医务人员、科研人员及决策者提供服务和协助，成为未来信息化工作的重要方向。为了解决上述的问题，需要在医院现有信息系统的建设成果的基础上建立信息集成平台及全院数据中心，对医院各应用系统数据进行采集和清洗，实现系统数据互联互通，为医院的运营、管理、绩效、临床等各方面提供重大帮助，进一步提高整个医院的工作效率、医院整体信息化水平和医疗服务质量。

项目以需求为向导医院信息系统互联互通成熟度标准、电子病历系统功能应用水平分级评价方法及标准等相关的标准规范，开展信息集成及临床数据中心建设，达到互联互通四级甲评审要求。

#### 1、信息集成平台

采购成熟的企业服务总线系统，实施基于主数据管理的业务应用，指导医院业务厂商改造医院原各应用系统，开发各应用系统接口，实现基于标准协议的医院各系统互联互通，建设运行监控平台、服务管理平台、统一用户管理、统一工作门户、统一

消息平台等应用系统平台，医院各信息系统达到《医院信息互联互通标准化成熟度测评》四级甲等标准要求，通过医院信息互联互通标准化成熟度四级甲等测评。

**2、临床数据中心**

临床数据中心平台立足于医院已有的信息系统，将封闭在多套孤立信息系统中的医疗数据释放出来，实现了物理集中；然后通过对数据的离散化处理，转变成各种有价值的信息，以帮助医院实现持续的质量改进和服务创新。由于信息更完整，使用更方便，各类用户的工作效率得以提升，决策判断的依据更加充分，服务响应更加及时，对促进公立医院的管理制度转型和服务创新，开展各项惠民服务，破解群众“看病难，看病贵”的难题，都具有非常重要的意义。同时，通过全院数据中心平台建设，可大幅提高惠州第六人民医院整体信息化水平，实现医院信息化建设的跨越式发展。

**3、运营数据中心**

运营数据中心（ODR）汇集来自 HIS 等业务系统中与运营管理主题有关数据，在此基础上构建运营数据仓库；通过 OLAP 分析，实现关键业绩指标(KPI)展示、决策驾驶舱(DSS)中动态仪表盘、决策预警雷达等功能，为医院决策者提供全方位的经营管理决策警示和支持。

**4、基于数据中心的应用系统建设**

1.临床类应用

建设患者 360 视图功能模块，基于临床数据中心，按照患者为核心的起始维度，依靠患者主索引 (EMPI),把患者当前和历史的全部门急诊就诊记录、门急诊病历、住院病史、影像检查、检验结果、心电图及扫描文档等信息进行整合及展示。

2.管理类应用

通过开发全院 360 管理决策驾驶舱、科室主任管理视图、门诊业务管理、医疗质量管理门户等功能，建立以人员、业务、疾病为基础的应用系统，为医院管理、运营管理、医疗服务提供技术支撑，建立全面、直观、灵活的数据展示功能等。

## （二）具体功能需求

### 1、信息集成平台需求

1.企业服务总线功能需求

▲（1）信息集成平台基于 HL7 等标准，参照 IHE(Integrating the Healthcare Enterprise 集成医疗企业)技术框架和体系结构，采用 SOA 和信息集成技术将各种医疗信息（文字、视频、检验数据等）进行松耦合集成，通过互联互通的方式实现临床工作模式与工作流程的优化。

（2）采用企业级服务总线（ESB）技术，通过松耦合模式，将业务逻辑和应用逻辑、数据逻辑分离。服务总线遵循 SOA 设计原则和技术标准，支持数据的自动采集、传输、标准化转换、存储、共享，提供可靠的数据或消息传输，支持标准消息中间件。

（3）基于主流成熟的企业服务总线服务产品，支持按服务分组，相互组之间不会受影响（需提供产品的登记证书复印件）。

（4）支持多种数据通信模式，包括同步、异步、点对点、发布/订阅等。

（5）支持通过适配器的方式将中间件和数据库连接，适配器包括但不限于 SQL Server、 Oracle、SAP，同时还可支持外部扩展。

（6）支持多种消息格式（CSV、XLS、XLSX）转换为 XML 消息格式

▲（7）支持最新 Web Services 标准，包括 SOAP 1.1/1.2.WSDL 1.1.MTOM/XOP、WS-I Basic Profile 1.1 等，支持 Web Services 自有的安全性 WS-Security 和寻址功能 WS-Addressing，实现 Web Services 同步和异步调用。

（8）支持 Minimal Lower Layer Protocol (MLLP) 传输协议，连接各类医疗设备。

（9）支持灵活开放的协议，包括但不限于 JSON、MLLP、HTTP/HTTPS、FTP/File、Socket、SMTP、SOAP/HTTP、SOAP/JMS，具备协议相互的转换能力。

（10）支持集群功能，队列管理器之间能够共享负载，实现自动负载均衡。

（11）支持标准接入规范，基于统一描述、发现和集成标准，进行关键业务活动服务注册，方便第三方供应商基于该统一架构进行平台接入。

（12)支持 ESB 事件驱动模型构建,支持业务规则引擎场景设置和自定义应用场景。可以实现不同协议的动态路由，且路由规则通过配置方式实现。

（13）企业服务总线产品需要内置医疗行业 HL7 系列适配器。

（14）具有较高的并发处理性能，包括 Web Service/http 调用等。

（15）系统采用多层架构的体系结构，应充分考虑到系统今后纵向和横向的平滑扩展能力。企业服务总线服务需要支持 3 个及以上故障转移架构能力。

（16）支持界面化配置管理企业服务总线内服务创建配置以及相关订阅方权限分配，并能跟踪每一次调用记录，同时能够通过配置界面干预服务转发重发功能。

（17）参考互联互通服务接入标准，采用统一接入方式，简化接入开发工作，简化第三方接入开发量。

（18）根据医院需求，建立相应的接口定义及使用规范，至少包括如下类型的接口定义和使用规范：病人基本信息、检查电子申请、检验电子申请、手术电子申请、输血电子申请、费用确认、危急值确认、主数据（包括员工、科室、病区、检验项目、检查项目、收费项目、医嘱项目、药品、诊断 ICD、手术 ICD、耗材等）。

（19）系统需要高度的安全性和可靠性保证

（20）系统配置易用性需要考虑，院方可以通过简单的系统配置操作完成后期新增服务的发布订阅配置。

（21）集成互联互通标准服务，实现互联互通评审的所有审查点，包括但不限于日志查询，重发跟踪，日常服务调用统计等功能

（22）提供账号维护、服务维护、订阅信息管理、配置管理、日志查询、统计分析、性能监控等功能。

（23）企业服务总线产品支持与公有云的集成，以方便未来业务扩展。

2.运行监控平台

（1）系统要求开发直观、友好的图形用户界面，直观展示平台运行指标及状态参数。

（2）界面可监控当天服务调用得情况、告警信息、异常信息、异常消息及异常处理等，接入服务、接入系统、服务调用、消费系统和数据备份等统计信息。

（3）支持在一个界面中显示集成平台服务器、数据库及具体服务的运行状态信息。

（4）支持提供服务调用日志、服务器和数据库日志。

（5）提供队列、服务器、数据库、告警规则、告警短信等配置功能。

（6）提供服务调用各种指标的统计报表。

3.服务管理平台

（1）支持界面化管理企业服务总线内服务的增删改及启用配置，相关订阅方权限

分配功能，服务分类管理。

（2）能跟踪每一次调用记录，同时能够通过配置界面干预服务转发重发功能。

（3）可以通过配置的方式实现服务的定义，根据医院的需求做相应的适配性修改，至少包括如下类型的接口定义和使用规范：病人基本信息、检查电子申请、检验电子申请、手术电子申请、输血电子申请、费用确认、危急值确认、主数据（包括员工、科室、病区、检验项目、检查项目、收费项目、医嘱项目、药品、诊断 ICD、手术 ICD、耗材等），主数据要根据医院需求，遵循国家、地区、行业及医院相关标准。

（4）系统配置易用性需要考虑，院方可以通过简单的系统配置操作完成后期新增服务的发布订阅配置。

（5）集成互联互通标准服务，实现互联互通评审的所有审查点，包括但不限于日志查询，重发跟踪，日常服务调用统计等功能

（6）系统要求提供模拟测试环境，新增加或修改的配置，须给测试环境测试通过后，才能发布到工程环境使用。

4.统一用户管理

（1）统一用户服务为全院各应用系统提供统一用户管理、统一认证管理和统一授权管理。

▲（2）统一用户管理系统需要支持 LDAP 协议，为医院各应用系统提供统一的、高可靠性和安全的用户管理服务，它集中存放以前分散在各应用系统的用户信息和组织机构信息，并按照管理流程，实现信息在各系统之间的流转和同步，并为各系统提供人员创建、调动、注销和密码同步等功能。

（3）单点登录（SSO）功能：统一身份与权限管理平台实现对医院各信息系统进行统一管理，各应用系统不再独立管理用户信息和授权信息。每个用户可以在单一点只需输入一次用户名和密码，就可以按系统设置的权限范围，访问所有被授权访问的系统，而无需二次输入用户名和密码。

（4）统一授权管理服务按照基于角色的访问控制模型，与信息系统应用成为一种松耦合的工作模式，为各类信息系统应用集成提供基础。

（5）实现完善的用户信息管理功能，能实现各系统用户帐号的对应关系管理，并集中存放分散在各系统的人员信息。

（6）提供用户创建功能，并与各系统接口，自动创建各系统用户帐号。

（7）提供用户注销的功能，并与各系统接口，自动注销各系统用户帐号。

（8）用户信息修改，提供修改用户信息的界面和访问接口，保证修改后的用户信息在各系统中保持一致。

（9）用户管理系统应具备高性能和可靠性，系统应能通过增加对等的人员管理服务器来均衡负载，以提升性能和可靠性，并增强数据安全性。

（10）系统应能通过权限设置和委托，实现分级管理功能，以方便管理部门（如医务处、护理部和人事处等）或各临床科室管理各自的用户信息。

（11）系统应提供完善的日志处理功能，对所有重要操作都应记录日志，并提供灵活的查询界面和接口。日志不能随意删除和修改。

（12）系统应提供完善的错误、警告、性能日志和事件，管理员并能通过 Windows 事件查看器和性能检测器查看，并能和系统管理和监控系统集成，以实现集中的监控和告警。

（13）系统应提供完善的日志处理功能，对所有重要操作都应记录日志，并提供灵活的查询界面和接口。日志不能随意删除和修改。

（14）对于 B/S 应用下的 Form 认证场景，系统应采用 SSL 加密协议，以避免密码探测，提供用户会话(Session)有效期管理。

（15）授权管理系统应采用基于角色的访问控制，用户所能访问的权限就由该用户所拥有的所有角色的功能集合的并集决定。

5.统一工作门户

（1）将医院相关系统都整合到统一的门户中，用户可以通过统一门户，查看平时重要的通知、日程、管理、报表等信息。

（2）同时可以无须再次输入用户名密码，直接登陆其他业务系统。

（3）统一门户针对每个角色的不同，为领导、医生、护士等不同角色定制不同的门户模版，使用户在门户中可以查看自己角色最关心的信息。

（4）用户可以根据自己的需求，对门户中的模块进行自定义。

（5）如果一个用户拥有多个角色（不如即是领导，又是医生），他也可以在多个角色中进行切换，使其能更好的进行日常工作。

（6）通过自动化部署发布脚本，可以自动发布并更新应用程序。

（7）提供应用系统接入规范，包括认证、消息和界面集成方案。

6.互联互通四甲标准测评

在本项目的实施过程中，需完成和医院现有的业务系统（HIS、EMR、LIS、PACS 等）业务系统对接，项目的建设方案需具备对业务系统进行数据分析能力。按照国家卫计委的互联互通标准化测评的四级甲等要求对本项目的建设内容进行建设和改造，协助医院完成测评材料、实验室及现场测评相关工作。互联互通相关系统对接费用、互联互通四甲标准测评费用等含在投标总价中。

▲投标人所投产品可兼容医院现有的信息系统（HIS 系统）和电子病历系统（EMR 系统）。（投标人需提供承诺函，格式自拟）

**2、数据中心需求**

1.数据中心基础架构

（1）临床数据中心实现所有临床诊疗数据的整合与集中展现，包括但不限于院内各临床信息系统(如就诊、住院、医嘱、病历、病案、护理文书、药敏、检查、检验等)所集成的患者所有重要的临床数据。

（2）建设运营数据中心（ODR），包括但不限于除临床信息系统外的其它数据源，（如预约、挂号、费用信息、医保信息、人事等）。

（3）数据中心建设包括数据对象、对象之间的关联关系、数据标准和业务数据的映射关系等，逐步形成医院运营数据集规范、数据获取规范、数据对外发布规范等。

（4）在确保对生产系统的资源和运行没有影响前提下，全院所有临床数据要以实时或近实时的方式，通过对原始数据的抽取、清洗、转换处理后集中存储，所产生的元数据支持灵活的查询利用需求。抽取的数据不能仅仅是对业务系统表的复制，必须按照国际、国内标准转换后存储，保证数据中心不依赖于业务系统。

（5）对历史临床数据进行抽取、清洗、转换，按标准化格式存储。描述数据渐变过程追踪和管理过程，确保数据的准确性。

▲（6）要求该平台软件是基于国际先进的医疗信息汇集（Data Aggregation）技术，对于采集的数据加以解析处理，形成最小的、可复用的数据元素，以提高数据利用的效率。

（7）具有内置的数据分析路径，可以根据医院关注的主题按医院的习惯层层分解，而无需定制。

（8）通过配置验证规则，自动验证 CDR 中的数据的准确性，如对比记录条数、对

比汇总金额等方法，确保 CDR 中的数据准确及时的反映了业务系统中的数据。

（9）临床数据中心应具有高度的可扩展性，支撑医院业务向区域的延伸，满足跟各级各类区域卫生信息服务平台的接口整合和数据共享，支持双向转诊、远程会诊等业务。

（10）提供临床数据的统一展现，按权限为系统管理员和用户提供不同级别不同层次的临床数据中心数据汇总展示，便于各类用户能够快速获取诸如医嘱、病历文书、检查报告、检验报告等各类临床数据概略信息。

（11）数据中心所使用的数据库产品必须是当前成熟的关系型数据库产品，并且数据库需内置 ETL 工具模块、联机分析 OLAP 功能模块、联机交易处理 OLTP 功能模块、报表服务，无需额外购买。

2.主数据管理

▲（1）在集成平台上构建医院主数据管理数据库，集中统一的管理全院主数据，通过对平台相关的各业务系统提供主数据服务，实现主数据的同步和匹配，包括但不限于术语、人员、科室、检查检验项目、药品、耗材、诊断 ICD、手术 ICD 等。

（2）遵循主数据的国际标准（如 ICD10）、国家标准（如患者的部分基本信息）、行业标准（卫计委定义的相关值域）、医院标准。主数据可由平台管理者进行注册、维护等。

（3）基于医院临床应用，实现临床诊断，手术的二级编码管理，并通过院内管理流程通过审核与国际标准 ICD10.ICD9 等进行对应。

（4）全体工作人员（包括本院和非本院）和科室数据管理：建立医院统一的组织机构架构，包括业务科室、护理单元、职能部门、后勤部门等。

（5）支持从医院现有业务系统同步人员、科室、病区、药品、材料等相关信息，建立与主数据同步的对应管理。供应商提供主数据梳理服务，实现对大历史患者信息自动化归并等服务。

3.患者主索引

（1）患者主索引（EMPI），用于患者基本信息索引的创建、搜索和维护，可对患者有效地进行管理。

（2）通过建设主索引来自动或手动匹配、合并患者信息，利用主索引可获得完整的患者视图。

（3）EMPI 为每个患者创建一个唯一标识，并与所有相关系统医疗记录的标识之间建立映射。

（4）根据索引规则，对院内各类信息系统中的患者信息进行索引重建，使历史记录可以进行关联。

（5）通过给定规则，实现相似患者汇总页面，方便医院手工合并、分拆患者主索引。

（6）EMPI 提供给其它应用程序订阅或调用等服务。

▲（7）患者主索引（EMPI）匹配算法应符合 IHE-PIX、IHE-PDQ 集成规范，患者主索引提供符合 HL7 标准的对外服务接口。

（8）主索引建设部分应包括但不限于：患者信息管理，患者疑似信息管理，匹配算法引擎，操作记录审计等内容，主索引系统业务记录发生的变化都需要记录操作日志，并能实现分拆。

**3、基于数据中心的应用系统**

1.临床类应用

（1）患者 360 视图

▲①在临床数据中心的基础上，按照患者为核心的起始维度，依靠患者主索引 (EMPI)，把患者当前和既往的全部门急诊就诊记录、门急诊病历、住院病史、影像检查、检验结果、心电图及扫描文档等信息进行整合。

②建立患者 360 视图，临床人员可通过一个视图快速浏览患者的全部信息。

③支持按照时间轴查看患者在指定期间内的门诊、住院、体检等所有信息。

④患者 360 视图提供简单的集成接口，方便第三方应用系统调用，并且可以配置不同的默认视图，为不同角色的用户提供不同的默认界面。

⑤提供时间轴管理，支持关键指标时间轴汇总展示。

⑥支持行业主流移动设备展现

2.管理类应用

（1）全院 360 管理决策驾驶舱

①基于临床数据中心（CDR）及运营数据中心（ODR）开展 OLAP 分析，实现关键业绩指标(KPI)展示、决策驾驶舱(DSS)中动态仪表盘、决策预警雷达等功能，为医院决

策者提供全方位的决策警示和支持。

②充分整合现有运营数据：通过数据平台整合医院现有的各类信息数据，将数据物理集中到统一的数据仓库环境；

③数据仓库标准化：为医院建立规范、完整、高效、可持续发展的运营数据仓库核心模型、ODS 和多维分析模型，标准数据集符合国家卫计委、江苏省的相关标准；

④展现形式丰富细致：为医院提供自主分析、数据查询、报表分析、多维分析、数据挖掘等多种信息分拆手段；

⑤展现运营数据全面准确：从财务状况、人员绩效、医疗质量、医院未来发展趋势和能力等全方位、多角度提供领导决策分析；

⑥统一的门户：提供完整的数据门户，用户通过数据门户的定制化功能，可将各类数据使用、数据分析和业务应用功能整合在统一的环境中。

⑦提供完整的医院管理指标概述，概述中含有各类指标横向、纵向、基值对比，然后根据管理专题或者单指标进行钻取，实现院级、科室组、科室、医疗组、医生、患者的多层级数据查看及原因分析，也可以从病种、手术、医嘱、药品等方面查看各类指标的对比情况。

⑧数据分析对象包括：门诊、住院实时数据监测、管理专题--门诊专题、住院专题、标准专题--收入专题、医疗服务、工作效率、医疗质量、患者安全、合理用药、医院管理专题--医保控费、门诊就诊时间、大处方、高值耗材。

⑨支持行业主流移动设备展现。

（2）科室主任管理视图

科室主任视图帮助科室负责人对科室从宏观到微观的数据、信息、资源的全面统计，自动产生报表，实现科学决策。它覆盖科室院各个部分、各个方面的信息，包括业务量、收入及各级明细、各类统计信息、药品信息、医疗工作质量及效益等。

查询统计方法灵活、简便，采用数据和图像结合显示，使得信息更直观、一目了然。门诊收入、住院收入、全院收入既可以按科室查询也可以按医师开单量查询，支持多个维度。

门诊就诊量、日出入院量、在院病人情况、床位占用等动态数据情况的查询让管理者达到更有效的管理决策效果。

①医疗服务统计

主要对科室发展情况、资源利用、医疗护理质量、科室工作效率、科室经济效益等方面的数据进行整合、统计分析并提供准确、可靠的统计数据，为科室负责人提供所需要的各种报表。

1） 门诊病人统计数据；急诊医疗统计数据；住院病人统计数据；

2） 门急诊日报表、月报表、季报表、半年报表和年报表；

3） 病房日报表、月报表、季报表、半年报表和年报表；病人分类报表；

4） 对上级部门的报表；医疗工作月报表；住院病人分类报表；

5） 损伤和中毒小计的外部原因分类表卫生行政主管部门规定的其他法定报表；

6） 门诊工作情况；病房(病区)工作情况(含病房床位周转情况、床位使用率等)；

7） 出院病人分病种统计及其他分类统计；手术与麻醉情况；

②综合查询与分析

1）科室财务管理分析、统计、收支执行情况和科室核算分配信息；

2）医疗、护理管理质量和分析信息；

3）人事管理：科室各类卫生技术人员和其他技术人员总额、比例、分布、使用情况；

4）科室设置、重点学科、医疗水平有关决策信息；

5）门诊挂号统计、收费分项结算、科室核算信息及门诊月报；

6）住院收费分项核算、科室月核算、患者费用查询、病人分类统计信息；

7）科室工作指标、医保费用统计信息；

8）科研管理统计，全部课题或分类统计课题的汇总等；

③支持行业主流移动设备展现

（3）门诊业务管理

门诊业务管理系统基于全院数据中心，以图形化方式展示门诊业务统计数据，实时监测门诊各诊区或窗口业务环节的滞留病人数量以及平均（或最长）候诊时间，以便及时干预，消除门诊流程中的瓶颈。此外，提供患者投诉管理，跟患者满意度管理和医德医风管理系统进行整合，改善病人服务。支持行业主流移动设备展现

（4）医疗质量管理门户

①提供 2016 版卫计委医政司要求的医疗质量管理的全部指标体系及三级综合医院评审标准的相关指标。

②要能对医疗质量监测指标进行监控，不仅可以得到的指标计算值，而是能够实时看到正在发生的具体情况，并能够接受医务部门的反馈或干预信息。

③关键事件动态监测：包括全部手术、有创操作、全部微生物检验结果、危重抢救病例。

④关键节点动态监测：包括入院记录、首次病程录、日常病程记录、交接班记录、手术记录、会诊记录、出院记录、体温单、护理记录、入院评估单、健康教育单。患者入院须知、手术病人接送护理记录单、临时医嘱单等。

⑤关键环节过程审核：对特殊的医疗行为应先由相关和质量控制科审核方可进行。可对需要审核的时间条件进行定义，出现需要审核的环节时系统提示相关人员进行审核。

⑥质量指标综合查询：综合查询各考核对象、各时间段的各项质量指标评估和监测结果。

⑦质量指标超限预警：对各种超过标准限制的质量指标给予预警。

⑧质量指标结构分析：根据不同质量指标的评估结果和给出的各种条件生成报表，并能根据报表数据情况生成各种表示结构与比例的饼图。

⑨质量指标对比分析：根据不同对象评估的结果和给出的各种条件生成下列报表，并能根据报表数据情况生成各种表示结构与比例的直方图。

⑩质量指标趋势分析：根据不同时间评估的结果和给出的各种条件生成下列报表，并能根据报表数据情况生成各种表示结构与比例的直方图或线性图。

⑪针对质量控制的数据，须根据业务需求提供业务数据补录功能，确保数据的完整性及有效性。针对临床数据中心不具有的数据，提供数据录入界面进行人工录入。

⑫支持行业主流移动设备展现。

**4、非功能需求**

1.服务器操作系统技术要求

本项目中信息集成平台与临床数据中心的底层操作系统应兼容目前市场上主流的X86服务器，支持最多将64台物理主机配置为单一群集，支持群集中构建的虚拟机可以在群集内实现实时迁移、故障转移等功能。投标人需在技术方案中阐述所使用的操作系统产品名称及主要功能描述，并且所使用的操作系统需要和医院现有技术路线保持连续性。

2.数据中心底层数据库技术要求

▲全院数据中心底层所使用的数据库产品必须是关系型数据库产品。

本项目中使用的数据库产品需内置 ETL 工具模块、联机分析 OLAP 功能模块、联机交易处理 OLTP 功能模块及报表服务，并非通过若干产品模块或组件组合而成，并且在采购数据库产品后，无需额外购买其它功能模块或组件。投标人需在技术方案中阐述所使用的数据库产品名称及主要功能描述。

3.信息安全要求

项目建设要符合《卫生行业信息安全等级保护工作的指导意见》及《信息安全等级保护管理办法》等信息安全相关标准规范要求，系统信息安全等级保护达到信息安全等级三级测评标准关于医院核心软件系统的要求。

4.运行安全环境要求

4.1 安全软件要求

根据国家网络安全法及等级保护对公民个人敏感信息保护的要求和 IT 风险管理风险评估及处置建议，必须完善对信息集成平台应用内嵌特权账号及密码的管理机制，包括：

（1）建立应用内嵌特权账号与密码的集中管理（包括存放、修改、保存），并对保存特权账号与密码的文件设定严格的访问控制；

（2）建立完善的应用内嵌特权账号与密码的申请、审批、发放及回收的机制，提供有效的过程记录。确保特权账号使用的可追溯性，及密码的保密性/安全性；

（3）在系统层面按照相关规范的密码策略要求定期更新特权账号的密码；

（4）建立面向操作系统特权用户的权限细粒度管控机制，实现对高风险特权和高危命令的管控;

4.2 软件兼容性

▲投标方所采用的应用内嵌特权管理系统，需与应用内嵌特权管理系统厂家完成直联直通、无缝对接等兼容性工作，包括 API、SDK、源代码、配置文件、脚本等各种方式对接，并保证整个信息集成平台在上线之后的安全运行。要求投标方需提供应用内嵌特权管理系统供应商与投标方联合出具可与本次信息集成平台直联直通、无缝对接的承诺函（双方均需加盖公司公章，且日期为项目实施阶段）。

4.3 安全软件功能要求

| 功能名称 | 指标 | 具体参数和要求 |
| --- | --- | --- |
| 账号密码管理 | 密码管理平台 | 1.提供特权账号安全管理平台，管理和使用数据中心的特权账号，通过该平台，用户可以申请/获取密码，审核密码申请，权限管理，审计/监视活动等等。<br>2.密码管理平台应支持双机热备的高可用（HA）模式，一旦主平台停止服务，业务可以实时切换到备平台，不影响业务的连续性。**（提供截图证明及部署方案）**<br>3.密码管理平台应支持并配置异地容灾（DR）的高可靠性设计，一旦主数据中心停止服务，业务可以自动切换到异地，不影响业务的连续性。**（提供截图证明及部署方案）** |
| | ▲账号自动发现 | 能对 Windows、UNIX、 Linux、AIX、SSH-KEY、硬编码等账号凭证进行扫描；支持自动发现云平台新建 VM 账号或新增账号，并能自动托管**（提供截图证明）** |
| | 对密码设置访问权限 | 数据中心的管理员根据不同的特权用户配置不同的访问权限，为每个用户提供可以访问的设备和设备上的系统身份。 |
| | 密码版本 | 保留所有特权账号密码历史版本,以应对任何可能的系统恢复。 |
| | 密码使用申请 | 用户可以自助申请所需账号，经审批通过后，获得该账号的密码使用权限。 |
| | 密码管理 | 管理员可以进行用户账号密码管理。 |
| | 密码定期修改 | 支持手动触发更改、定期自动更改、一次性密码触发更改、密码申请使用到期触发更改密码重置工作。 |
| | 强密码 | 密码单一性，确保不同的设备/系统不同的账号都有完全不同的独一无二的密码。 |
| | 密码策略 | 支持根据所托管的不同设备/系统制定不同密码策略，在制定策略后，自动生成符合密码强度和复杂度要求的密码。 |
| | 广泛的系统支持性 | 1.操作系统：支持 Windows（本地及域账号）、Linux、Unix、Aix、AS/400、ZSeries (OS/390)、Mainframe 等等<br>2.数据库：支持 ORACLE、SQL SERVER、DB2、SYBASE、MySQL 等等<br>3.虚拟化：支持 VMWARE、ORACLE 虚拟化等<br>4.网络设备：支持交换机、路由器、负载均衡等网络设 |

| | | |
|---|---|---|
| | | 备特权账号的管控，包括 SSH 或 TELNET 工具或 WEB 页面控制台访问网络设备的管控。应支持的厂家不限于 CISCO、华为、H3C、juniper、绿盟、array、hillstone 等等<br>5.安全设备：支持防火墙、IPS、IDS、VPN、防病毒、终端准入等，包括 SSH 或 TELNET 工具或 WEB 页面控制台访问网络设备的管控。应支持的厂家不限于 CISCO、华为、H3C、juniper、绿盟、array、hillstone 等等<br>6.工控设备：支持智能电表、集中控制、工控交换机、工控网闸、工控安全、电力功能监控等等<br>7.中间件：支持 WEBSHPERE、WEBLOGIC、TOMCAT、TUEXDO、Jboss 等中间件连接池账号及 Web Console 控制台的管控<br>8.应用账号：支持应用系统源码、配置文件（包括 txt、ini 等）、API 接口账号、服务账号、计划任务、B/S 应用、C/S 应用等<br>9.业务前台管理账号：支持核心业务系统前台的管理账号、批量数据下载账号、用户管理账号、公众平台管理账号等<br>10.云技术的支持，需支持主流云，如阿里云、亚马逊云、微软云等，提供云市场的公网链接及截图。**（需提供截图证明）** |
| | 密码检查 | 定期检查密码一致性，并为不一致的情况提供处理机制。 |
| | 一次性密码 | 当密码使用完之后，特权账号管理系统进行重置。使得下一次用户申请的密码和前一次密码不同。系统中能够指定密码重置时间窗口。**（提供截图证明）** |
| | 排他密码 | 支持排他性密码策略，一个密码在同一时刻只能被某一个用户使用，在该用户使用此密码期间，其他用户不能使用该密码。 |
| | 支持密码关联 | 能够自动同步 Windows 服务,Windows 计划任务,IIS 应用程序池等所用登录账号。 |
| | 密码分段 | 支持所托管设备/系统的密码分段查看功能，两人各查看密码其中一半，合并一起就是完整密码。 |
| | 密码信封管理 | 能导出密码明文用以物理信封保存。 |
| | 提供统一的访问密码的界面 | 系统提供 web 门户访问方式，且采用 SSL 加密。 |
| | 密码的获取 | 只有相应权限的人才能获得对应密码，或通过产品修改 |

| | | |
|---|---|---|
| | 和授权 | 密码：<br>1.可自定义 IP 区域限制用户获取密码<br>2.可自定义用户分组，分级授权<br>3.可自定义时间段限制用户获取密码<br>4.可以通过支持密码获取的申请和审批流程加强安全性和可管理性 |
| | 密码批量导入 | 支持操作系统类账号、数据库类账号、中间件管理类型账号、网络设备类型账号、特权账号管理系统本身账号执行批量编辑操作。 |
| 权限管理 | 角色授权 | 细化角色，对于账号管理平台，应至少能包含：平台管理员、运维账号管理员、运维账号使用者、审计员这四类角色。平台管理员有管理整个平台服务和配置的权限，运维账号管理员有管理系统账号及密码配置的权限，运维账号使用者可以登录受管系统，审计员可以定制查看审计报表。 |
| | 访问控制 | 1.建立受管系统登录连接时先要进行身份验证、实时鉴权，鉴权过程包括时间、IP 地址等属性验证；<br>2.访问锁定，用户登录平台时口令输入多次错误则锁定，避免用户密码被暴力破解。可以配置输入失败的次数和锁定时间。 |
| | 临时访问 | 用户如需临时登录某受管系统时，系统管理员可赋予其访问权限，临时允许登录时间段可进行限定设置。 |
| | 登录审批 | 1.可对指定的系统运维账号配置登录审批，即无论什么用户要使用该账号登录受管系统，均要通过审核后才能登录系统，并可限定登录时间段；<br>2.支持多种审批方式，包括平台审批、邮件审批、短信验证码审批 |
| | 跨部门分治 | 具有区域的概念，区域内的管理员只能管理其所在区域内的其他用户 |
| | UNIX 和 Linux 权限管理 | 可以将 UNIX/Linux 中的任何 UID 的权限赋予一般用户，比如将 root 的部分命令执行权限赋予普通用户（**提供截图证明**） |
| | Windows 权限管理 | 1.可以将 Windows 中原本需要管理员权限的命令赋予给普通用户；<br>2.也可以规定不允许 administrators 组用户执行某些命令；<br>3.Windows 平台权限分配时，可以具体细化到 MMC 控制台中的权限。比如，在 Services.msc 中，可以不同用户对 |

| | | |
|---|---|---|
| | | 不同的服务器具有不同的管理员权限。 |
| | 提权模式要求 | 任何提权模式可以限定到访问时间，提权的命令以及参数。 |
| | 提权命令保护 | 提权命令可以通过 HASH 值来进行保护，避免提权命令被恶意修改。 |
| | 提权审计记录 | 每一次提权都会具有审计记录。 |
| 特权操作监控与审计 | 特权会话实时监控 | 支持远程对正在进行的特权会话进行基于权限策略的实时监控：即操作人在 A 终端上进行操作，审计人可在 B 终端上观看操作过程，可以观看，也可以控制干预，终止会话 |
| | 用户管理记录 | 支持对用户登入登出受管系统信息、用户角色及权限分配、账号分配、用户身份认证方式等进行详细记录。 |
| | 密码管理记录 | 对人为的或自动的密码使用、变更、查看、打印、密码一致性检查等操作进行详细记录。 |
| | 特权操作记录 | 对所有使用特权账号进行登入登出、操作行为进行详细的记录，包括文本和视频记录：<br>1.支持以文本形式和视频形式对 WINDOWS、LINUX、UNIX、AIX 系统的操作行为识别和记录；<br>2.支持对数据库操作行为协议审计，包括操作脚本中 SQL 命令的识别和记录；支持所识别的行为、命令与对应的操作视频记录的关联。**（提供截图证明）** |
| | SSH Key 的管理与审计 | 支持定期轮换受保护的 SSH 密钥，确保受保护的私钥和分布在目标系统的公钥保持同步。**（提供截图证明）** |
| | 审计功能 | 1.审计管理员可以随时检查密码管理和特权操作的文本和视频记录；<br>2.支持灵活的搜索功能，包括基于 IP、用户、命令等的搜索；<br>3.支持多条件组合搜索。 |
| | 审计记录防篡改 | 所有审计记录在规定的时限内不可删除。 |
| | 特权账号的统计/审阅报告 | 1.能够对已管理的特权账号等系统账号生成使用状态统计报告，提供审阅支持；<br>2.支持自定义报表内容。 |
| | 特权威胁分析 | 1.应允许在持续和历史的活动中检测和识别异常<br>2.在异常发生时应提供实时警报<br>3.应提供对当前威胁级别的意义，基于：实时检测、事件的相关性、等级的严重性 |

| | | |
|---|---|---|
| | | 4.不需要使用签名，沙箱或其他方法等（识别）攻击的知识库<br>应能适应随时间变化的用户行为主动学习 |
| 单点登录工具支持 | 单点登录 | 支持单点登录功能，并提供相应工具进行运维、管理、开发等操作。 |
| | RDP | 支持通过 RDP 登录 Windows 系统。 |
| | Telnet | 支持通过 Telnet 登录目标系统，如 AIX。 |
| | SSH | 支持通过 SSH 登录目标系统，如 Linux/Unix。 |
| | FTP | 支持 FTP 文件传输。 |
| | Oracle PLSQL Developer | 支持通过 PLSQL 连接 Oracle 数据库。 |
| | Sql*Plus | 支持通过 Sql*Plus 连接数据库。 |
| | Xmanager | 支持通过 XShell 登录目标系统，如 AIX。 |
| 数据库安全运维 | 动态数据库遮罩与脱敏 | 动态拦截 SQL 指令，并依设定的遮罩策略识别规则而修改调整 SQL 指令，不需变更数据库实际数据内容 |
| | | 可依据「数据库、数据表、字段名称」定义数据自动遮蔽脱敏规则，并可使用数据库所支持的内建函数，定制【数据遮蔽脱敏】的规则 |
| | | 遮蔽所采用的字符，支持中英文各种标准字符，例如：英文的（*/星号字符）、（O/大写字母）、（X/大写字母）、空白字符等等，中文的（〇/符号字符）、（＃/符号字符）、（＊/符号字符）、（密/中文标准字符）等等 |
| | | 可对英文及数字的主键值数据（例：身份证号）进行脱敏，并使应用程序的主键关联查询仍维持正常，不会因主键脱敏后查不到数据 |
| | | 提供【中英文编码】的遮蔽脱敏功能，支持 BIG5 与 Unicode 编码,不会因为不字符编码长度不同而导致遮蔽后中文乱码 |
| | | 可根据【数据库用户、连接数据库的应用程序名城、主机名称、时间、SQL 命令关键字】多重条件组合，来定义不同的动态遮蔽脱敏策略 |
| | 数据库访问的管控功能 | 可根据【数据库访问端口、数据库名称、数据库用户、来源主机名称、来源应用程序名称、SQL 命令所含特殊关键字】等参数多重条件组合，来决定所需要【套用】的动态遮蔽管控规则 |
| | | 可实时管控特定的数据库用户能否执行特定的SQL命令， |

| | | |
|---|---|---|
| | | 例如：SELECT、INSERT、UPDATE、DELETE、CREATE TABLE、DROP TABLE 等等 |
| | 数据库存取审计日志功能 | 可记录完整日志【原始 SQL 命令】与动态调整【遮蔽变更后】的 SQL 命令内容 |
| | | 审计日志内容包含：日期、时间、来源主机名称、数据库用户、应用程序名称、原始 SQL 命令、应用的规则名称 |
| | 支持的数据库 | 1.Oracle 8i （含）以上版本<br>2.Microsoft SQL Server 2005（含）以上版本<br>3.DB2 v9（含）以上版本<br>4.Informix<br>5.Sybase ASE/IQ<br>6.Teradata<br>7.MySql<br>8.Hive<br>9.JDBC/ODBC |
| 应用内嵌账号管理 | 静态密码管理 | 支持通过修改源代码的方式，使得应用程序中的静态密码可以定期修改；应用程序使用系统提供的 API 进行动态密码获取。 |
| | 动态管理中间件数据库连接池密码 | 支持应用是基于中间件（Weblogic、Websphere、Tomcat、Jboss、Spring）数据库连接池功能的，则可以在不修改代码情况下，定期自动变更管理数据库连接池的密码，并不需重启中间件。**（提供截图证明）** |
| | 中间件 Web Console 密码管理 | 对中间件（Weblogic、Websphere）Web Console 密码进行统一管理，定期自动变更密码，支持单节点以及多节点群集部署结构，支持各种中间件运维条件场景（如命令行、图形化、管理工具）。密码变更后不影响各种运维场景、运行中的 app 且无需重启中间件**（提供截图证明）** |
| | 稳定性 | 在系统本身出现宕机，或者网络不通畅情况下，应用程序依旧正常工作 |
| | 多平台支持性 | 相应的 API 必须支持多种平台，包括：Windows，Linux，AIX，HPUX，Solaris。 |
| | 多语言支持性 | 相应的 API 必须支持不同开发语言.Net（C＃/ VB。NET），Java，C，C++，VBScript，命令行，等类似的语言。 |
| | 业务连续性 | 应用程序不受本系统故障的影响，当密码存储的服务器出现故障时，应用程序依旧正常运作。 |

| | | |
|---|---|---|
| | 应用程序的多种验证方式 | 支持限定登录用户名/密码，程序执行目录，OS 用户，程序的 hash 值等。 |
| 产品安全性 | 身份认证 | 支持 LDAP、Radius、RSA 等多种身份认证方式 ，且支持如 AD+动态口令的双因素认证 |
| | 数据安全 | 1.要为密码和审计记录提供专门的安全存储，此服务器为专门服务器，没有其他任何第三方程序；<br>2.存储密码的服务器，必须经过安全加固，需架设防火墙，对远程访问只能开放有限的端口；<br>3.产品所需数据库能够自动管理，不依赖任何 DBA 的介入，以防止 DBA 对数据库的审计信息进行篡改；<br>4.产品具有独立的数据备份与恢复软件，不依赖于第三方数据库产品；<br>5.所有密码信息应以加密形式保存,加密后的密码只可以被自身应用访问，无法被其它文件系统明文查看；<br>6.每个客户都具有唯一的加密密钥；<br>7.密码只存储在系统中，不能以邮件等其它方式对外发送。 |
| | 应用安全 | 1.存储密码的服务器，必须经过安全加固，需架设防火墙，对远程访问只能开放有限的端口；<br>2.密码的传输应使用安全的加密协议；<br>3.用户账号初次登陆必须强制修改密码；<br>4.对同一用户账号错误尝试超过阈值次数后，该账号被锁，需管理员账号解锁；<br>5.以 Web 方式访问系统,须 SSL 加密；<br>6.用户账号可设置有效期，失效账号不再对系统具有访问权限；<br>6.服务器间组件通信所使用的密码须定期自动修改，以确保安全。 |
| 产品成熟度要求 | 自主知识产权要求 | 具有中华人民共和国版权局颁发的《计算机软件著作权登记证书》（提供证书扫描件） |
| | ▲公安部销售许可 | 具有中华人民共和国公安部颁发的《销售许可证》（提供证书扫描件） |
| | ▲ IT 产品信息安全认证证书 | 具备中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，并符合 ISCCC 《特权帐户管理产品安全技术要求》**（提供证书扫描件）** |
| | 系统集成性要求 | 具有文档详尽，并且正式的 API SDK 包，能够支持与其他系统进行整合，例如 Syslog、ArcSight 等 SIEM 应用 |

## 5、配套硬件需求

1.采购清单：

| 序号 | 产品 | 单位 | 数量 |
|---|---|---|---|
| 1 | 高性能超融合服务器 | 台 | 3 |
| 2 | 常规超融合服务器 | 台 | 4 |
| 3 | 服务器虚拟化软件 | 套 | 14 |
| 4 | 存储虚拟化软件 | 套 | 14 |
| 5 | 网络虚拟化软件 | 套 | 14 |
| 6 | 虚拟下一代防火墙软件 | 套 | 1 |
| 7 | 负载均衡 | 台 | 2 |
| 8 | 业务交换机 | 台 | 2 |
| 9 | 存储交换机 | 台 | 4 |
| 10 | 分布式存储 | 套 | 1 |

2.主要产品设备技术规格、参数及要求

2.1 超融合服务器 1

| 序号 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|
| 1 | 要求标准 2U 机架式设备，标准 X86 架构； | | |
| 2 | 处理器：要求配置 2 颗多核处理器，至少为 Intel Xeon GOLD 6132 V5 系列处理器；单颗 CPU 计算核心数≥14 个，单颗 CPU 主频≥2.6GHz； | | |
| 3 | 内存：至少配置 256G DDR4 内存； | | |
| 4 | 存储：至少配置 1 块 128G 系统盘，4 块 960G 企业级 SSD 数据盘； | | |
| 5 | 网络：配置至少 6 个 GE 电口及 2 个 10GE 光口； | | |
| 6 | 电源：要求冗余电源配置； | | |

2.2 超融合服务器 2

| 序号 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|
| 1 | 要求标准 2U 机架式设备，标准 X86 架构； | | |
| 2 | 处理器：要求配置 2 颗多核处理器，至少为 Intel Xeon GOLD 5118 V5 系列处理器；单颗 CPU 计算核心数≥12 个，单颗 CPU 主频≥2.3GHz； | | |
| 3 | 内存：至少配置 256G DDR4 内存； | | |

| | | | |
|---|---|---|---|
| 4 | 存储：至少配置 1 块 128G 系统盘，2 块 960G 企业级 SSD 缓存盘，4 块 2T 企业级 SATA 硬盘； | | |
| 5 | 网络：配置至少 6 个 GE 电口及 2 个 10GE 光口； | | |
| 6 | 电源：要求冗余电源配置； | | |

2.3 服务器虚拟化软件：

| 序号 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|
| 1 | 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 MAC 地址等 | | |
| 2 | 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加 CPU 和内存资源，确保业务持续高效运行 | | |
| 3 | 虚拟化内核基于开源软件 KVM 底层开发 | | |
| 4 | 支持配置内存回收机制，实现虚拟化平台内存资源的动态复用，保障虚拟机的性能。 | | |
| 5 | 支持虚拟机的无代理备份，能提供至少 100 个虚拟机的高性能备份功能，提供无备份容量上限，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 6 | 支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预，减少运维工作量。 | | |
| 7 | 支持 IO 重试，当存储出现故障，导致虚拟机无法读取存储数据时，自动挂起虚拟机，避免业务故障。 | | |
| 8 | 每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括 Windows、 Linux，并且支持国产操作系统包括：红旗 linux、中标麒麟、中标普华、深度 linux 等。 | | |
| 9 | 支持在线的带存储的虚拟机迁移功能，可以在不停机状态下和非共享存储的环境中，实现虚拟机在集群内的不同物理机上迁移，保障业务连续性。 | | |
| 10 | 支持虚拟机跨集群的虚拟机迁移，支持在不停机的状态下跨集群迁移。 | | |
| 11 | 支持虚拟机的 HA 功能。当物理服务器发生故障时，该物理服务器上的所有虚拟机，可以在集群之内的其它物理服务器上重新启动，保障业务连续性。 | | |

| | | | |
|---|---|---|---|
| 12 | 支持无代理跨物理主机的虚拟机 USB 映射，需要使用 USB KEY 时，无需再虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的 USB 资源，对于业务的自适应能力、使用便捷性更佳。 | | |
| 13 | 支持纳管第三方主流虚拟化平台，提供对 Vmware 平台上的虚拟机进行管理。(提供产品功能界面截图)<br>支持在本地管理平台实现对 VMware vCenter 中的虚拟机备份，并能够在超融合的平台实现 VMware 虚拟机的启动恢复；(提供产品功能界面截图)<br>支持双向迁移，可将 VMware 虚拟机在运行状态下迁移到超融合平台上，也可将超融合平台上的虚拟机在运行状态下迁移到 VMware vCenter 的集群中，迁移最后阶段业务会中断,可选择自动或手动拉起。(提供产品功能界面截图) | 是 | ▲ |
| 14 | 采用分布式管理架构，去中心化，管理平台不依赖于某一个虚拟机或物理机部署，采用分布式架构保障平台更可靠 | | |
| 15 | 虚拟化管理平台具备监控功能，对资源池中 CPU、网络、磁盘使用率等指标进行实时的数据统计。 | | |
| 16 | 支持对平台虚拟机的精细化权限管理，可根据单个虚拟机开关机、打开控制台、删除等操作设定不同的权限，管理员也可以根据用户需求合理分配权限。 | | |
| 17 | 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。 | | |
| 18 | 支持创建虚拟机的时候批量指定 IP 地址和虚拟机的 hostname，支持编辑已经创建的虚拟机的 IP 地址和 hostname。 | | |
| 19 | 支持在管理界面提供基础的命令行功能，通过命令行可以进行基础的排障操作。 | | |
| 20 | 虚拟化的管理平台、可以支持扩展同一品牌的网络功能虚拟化、虚拟应用防火墙、虚拟应用负载均衡等功能组件的，并支持统一管理，以保障平台的扩展性和兼容性（需提供通过序列号方式扩展产品功能的截图，并加盖厂商公章） | 是 | ▲ |

2.4 存储虚拟化软件：

| 序号 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用 License 激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 2 | 采用分布式架构设计，由多台物理服务器组成分布式存储集群，通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out 架构），扩容过程保证业务零中断。 | | |
| 3 | 支持磁盘坏道检测功能，虚拟存储集群可以对数据盘进行坏道检测，发现坏道后可自动从另外一个副本读取数据，并对坏道数据进行修复。 | | |
| 4 | 支持标准的 iSCSI 协议，允许外部物理主机或应用通过标准的 iSCSI 接口访问虚拟存储，实现 Server SAN 和 IP SAN 的融合，能够使存储资源的利用率发挥到最大价值。在 iSCSI 接入场景下支持内部负载均衡和高可用。 | | |
| 5 | 支持多副本冗余功能，支持 2 个或以上副本，副本互斥地保存在集群的不同节点，当 1 个或多个主机或者磁盘故障，确保数据依旧正常访问。 | | |
| 6 | 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达 30min/TB 以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 7 | 支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 8 | 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中 IO 性能占用导致对业务的性能造成影响。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 9 | 在可视化的 WEB 管理平台上，可以查看虚拟分布式存储对应的容量大小、容量使用率、实时的 IOPS 读写次数、IOPS 读写数据量等信息，方便为 IT 管理做为有效的决策依据。 | | |
| 10 | 支持数据写入优化机制，将高速 SSD 作为写缓存，数据先写到 SSD，再回写到机械硬盘，提升写 IO 性能。 | | |
| 11 | 支持数据分层，提供好的读写性能，并支持对重要虚拟机提供性能保护。 | | |
| 12 | 支持内存读缓存功能，可以利用物理节点的内存作为读缓存，以提高读性能，实现内存、SSD、HDD 三级存储分层。 | | |
| 13 | 支持条带化功能，实现分布式 raid0 的性能提升效果，并且支持以虚拟磁盘为单位设置不同的条带数（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |

| | | | |
|---|---|---|---|
| 14 | 支持磁盘亚健康监测，包括 PCIE SSD 寿命告警、硬盘卡、慢的检测和告警、IO 错误告警、RAID 卡错误告警等。 | | |
| 15 | 分布式存储能够提供超高性能，能够提供百万级 IOPS 和 12GB/s 以上的带宽能力。 | | |
| 16 | 支持存储分卷功能，以物理主机为单位划分为不同的存储卷，如高性能卷，大容量卷，全闪存卷等，可使对存储性能和容量要求不同的业务运行在不同的存储卷上。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 17 | 为了便于部署关键业务系统，虚拟存储可支持 Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度。 | | |
| 18 | 本次配置持续数据 CDP 软件，配置 15 个虚拟机数据保护授权。并满足以下技术要求：<br>1.持续数据保护 CDP 软件模块需采用无代理的方案，避免对虚拟机的稳定性和性能产生影响。<br>2.持续数据保护 CDP 软件模块，能够动态的开启和关闭，比如能够提供对正在运行的虚拟机，在不需要重启或中断业务的情况下，就可以开启 CDP。<br>3.CDP 提供与虚拟机故障隔离能力，支持 CDP 模块故障时，虚拟机仍然能够正常实现数据读写。<br>4.支持快速浏览指定 CDP 备份内的文件，可快速的从 CDP 备份中找回数据文件，查看虚拟机文件目录的操作可做安全审计（需提供产品功能截图，并加盖厂商公章）。 | 是 | ▲ |
| 19 | | | |

2.5 网络虚拟化软件：

| 序号 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|
| 1 | 提供大屏展示功能，可直观看到当前整个数据中心业务状态。 | | |
| 2 | 支持对 oracle、sqlserver、Weblogic 数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析。 | | |
| 3 | 主动探测业务系统，实时监控业务可用性，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障。 | | |
| 4 | 提供虚拟机报表功能,可以导出 TOPN 的虚拟机进行 1 年以内的性能分析与趋势分析报表。 | | |
| 5 | 支持部署虚拟分布式交换机、虚拟路由器、分布式防火墙 | | |
| 6 | 分布式防火墙能够基于虚拟机进行 3-4 层安全防护，以虚拟机为单位的安全策略部署,即使改变虚拟机的 IP 地址信息,安全策略依然生效。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |

| | | | |
|---|---|---|---|
| 7 | 分布式防火墙提供实时拦截日志显示，以及支持“数据直通 ByPass”功能，方便出现问题快速定位问题。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 8 | 通过 License 激活的方式，实现网络虚拟化功能（分布式虚拟交换机、虚拟路由器、虚拟应用防火墙、虚拟应用负载均衡），支持 Vxlan 网络和现有的 Vlan 网络对接，实现虚拟化平台与原有网络的兼容性。 | | |
| 9 | 本次配置虚拟路由器，虚拟路由器支持 HA 功能，当虚拟路由器运行的主机出现故障时，可以实现故障自动恢复，保障业务的高可靠性。 | | |
| 10 | 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 | | |
| 11 | 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。 | | |
| 12 | 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，并且能够排查到 acl 策略配置错误等层面，方便快速排查问题保障业务的高连续性。 | | |

2.6 虚拟下一代防火墙软件：

| 序号 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|
| 1 | 支持 DDoS 攻击防护、Web 应用安全防护、入侵防护功能、支持 URL 过滤和文件过滤功能、僵尸主机检测、病毒防护、网页篡改防护等功能，保障业务的高安全性 | | |
| 2 | 具备独立的 Web 应用防护规则库，Web 应用防护规则总数在 3000 条以上 | | |
| 3 | 具备独立的僵尸主机识别特征库，恶意软件识别特征总数在 50 万条以上 | | |
| 4 | 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 5 | 支持对被防护网站是否被挂黑链进行检测； | | |
| 6 | 具备对常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能，全面保障业务的安全。 | | |

| | | | |
|---|---|---|---|
| 7 | 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则，能够及时的进行安全防护，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 8 | 支持 B/S 服务漏洞扫描功能,可扫描 WEB 网站是否存在 SQL 注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 9 | 提供安全报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，可以查看到有效攻击行为次数和攻击趋势 | | |
| 10 | 为保障应用防火墙软件功能的领先性，云平台厂商要求为公安部第二代防火墙（GA / T 1177-2014）标准的制定单位之一,符合国家信息安全规范要求； | 是 | ▲ |

2.7 负载均衡：

| 序号 | 技术要求 | | 关键指标说明 | 主要标识指标 |
|---|---|---|---|---|
| 1 | 设备部署 | 支持串接部署方式和旁路部署方式，支持三角传输模式。 | | |
| 2 | 多合一功能集成 | 提供针对多条出口线路的链路负载均衡功能，实现 inbound 和 outbound 流量的均衡调度，以及链路之间的冗余互备。 | | |
| | | 提供针对 L4/L7 内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求。 | | |
| | | 提供针对多站点业务发布的全局负载均衡功能，通过智能 DNS 等机制实现内外网用户对多个数据中心的最优接入路径选择 | | |
| | | 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。(提供设备操作界面截图证明材料，并提供厂家授权免费开通功能声明并加盖公章) | 是 | ▲ |
| 3 | 负载均衡算法 | 支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法。 | | |
| 4 | 可编程流量控制 | 通过某种编程语言(如 lua)实现自定义的流量编排，对 TCP、SSL、HTTP 和 HTTPS 等类型的流量进行分发、修改和统计等操作。 | | |
| 5 | 链路负载 | 支持静态 IP 和 PPPOE 两种线路接入方式。 | | |
| | | 支持三明治架构，对防火墙、IPS、行为管理等网络设备进 | | |

| | | | | |
|---|---|---|---|---|
| | 均衡 | 行流量负载均衡和故障切换，使以上网络设备获得Active-Active运行的能力。 | | |
| | | 支持基于五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。 | | |
| | | 支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| | | 内置完备的IP地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能 | | |
| | | 支持基于URL的链路调度功能，内置不少于1000条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| | | 支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度。 | | |
| | | 支持基于域名的流量调度，针对特定网站选择指定的链路转发。 | | |
| | | 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。 | | |
| | | 支持DNS内网记录，包含A、AAAA、CNAME、MX和TXT等类型，可识别内网用户并对其DNS请求直接返回相应结果；<br>支持智能DNS解析功能，实现外网用户访问内网业务系统的最优路径选择。 | | |
| | | 链路健康检查与服务器健康检查联动，入站负载跟服务器负载结合的时候，如果后端服务器全挂，则入站负载时也认为该虚拟IP（此时要求入站负载的虚拟IP与虚拟服务发布的IP组相同）也离线，从而达到联动效果。 | | |
| | | 支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 | | |
| | | SLB能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备CPU、新建并发吞吐等数据上报GSLB，设备之间的联动使得GSLB能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式。 | | |
| | | 支持跨数据中心集群和跨数据中心会话保持 | | |
| | | 支持多种链路检测方法，能够通过PING、TCP、HTTP等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。 | | |

| | | | | |
|---|---|---|---|---|
| | | 支持链路负载投屏展示，能够分别基于链路监测、应用选路和 ISP 流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP 展示基于运营商分类选择链路的示意图（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 6 | 服务器负载均衡 | 支持源 IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID 等多种会话保持机制。 | | |
| | | 支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制。 | | |
| | | 支持用户自定义方式的健康检查，支持多种编程语言（如 Python、Java 等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。 | | |
| | | 支持节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。 | | |
| | | 支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规 HTTP 应用可配置基于反映 URL 失效的 HTTP 响应状态码的观测判断机制，对于复杂应用可配置基于 RST 关闭连接和零窗口等异常 TCP 传输行为的观测判断机制。 | | |
| | | 支持面向服务器健康度的弹性调控机制，可通过监控业务流中的 TCP 传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| | | 支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。 | | |
| | | 支持配置每台的服务器最大连接限制和新建连接限制，以及单个特定用户或者一个用户组中所有用户访问指定应用服务的并发连接总数限制，避免应用系统的服务器过载。 | | |
| | | 支持命令行配置，支持 Tab 键补全操作，支持界面全部模块通过命令行的模式配置，支持命令批量操作，支持配置导入导出命令行操作 | | |
| | | 对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包 | | |
| | | 服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU 温度、CPU 和内存占用率、新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、 | | |

| | | | | |
|---|---|---|---|---|
| | | 并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量； | | |
| | | 可通过读写分离等技术手段实现数据库负载均衡，至少包括 MySQL、Oracle、MSSQL 等类型的数据库。以 MySQL 为例，通过对数据库操作请求做内容解析，将其中的写操作调度到指定服务器，读操作则调度到所有节点，提高数据库资源使用率，无需在服务器上安装任何插件。 | | |
| | | 支持基于消息的长连接负载（MBLB），对于非 HTTP 协议的长连接应用，可通过分析议特征来识别消息的开始和截止，以消息为对象进行七层负载均衡，而非传统基于连接的四层负载均衡。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 7 | 资 质要求 | 设备生产商的负载均衡类产品入选 Gartner 应用交付控制器（ADC）魔力象限报告，属于国际市场认可的知名品牌 | 是 | ▲ |

## 2.8 业务交换机

| 序号 | 技术要求 | | 关键指标说明 | 主要标识指标 |
|---|---|---|---|---|
| 1 | 交换机性能 | 48 个 10/100/1000Base-T 自适应电口，4 个万兆 SFP+光口，支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；支持终端识别、终端准入、安全防护及安全画像可视；支持胖瘦一体化 | | |
| 2 | 接入方式 | 支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时在控制器平台灵活的进行切换 | | |
| 3 | 访问控制策略 | 支持基于交换机单端口、聚合口的 ACL 策略；支持基于源目 IP 地址、MAC 地址的 ACL 策略；支持基于协议（例如：OSPF、UDP、ARP），同时支持自定义协议号的 ACL 策略；支持基于时间的 ACL 策略；支持基于 802.1p、IP 及服务等级、DSCP 的优先级设置； | | |
| 4 | 流量镜像 | 支持流量端口镜像及重定向功能； | | |
| 5 | DHCP Snooping | 支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文 | | |
| 6 | 交换机零配置上线方式 | 二层广播自动发现控制器平台，配置静态 IP 地址三层发现控制器平台，DHCP Option43 方式发现控制器平台，DNS 域名发现控制器平台 | | |
| 7 | 一键替换 | 支持通过控制器平台一键替换“按钮”即可完成故障设备替换，提供平台功能截图证明并加盖厂商公章； | 是 | ▲ |

| | | | | |
|---|---|---|---|---|
| 8 | 生成树 | 支持 STP、RSTP、MSTP 协议 | | |
| 9 | 组播 | 支持 IGMP v1/v2/v3 Snooping | | |
| 10 | VLAN | 支持 4K 个 VLAN | | |
| 11 | 端口聚合 | 支持端口聚合 64 个<br>支持手工和静态 LACP | | |
| 12 | ARP | ARP 表≥1K | | |
| 13 | DHCP | 支持 DHCP Server | | |
| 14 | M-LAG | 支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面 | | |
| 15 | 三层功能 | 支持静态路由，路由表≥512 | | |
| 16 | 组播 | 组播条目≥1k，支持 IGMP Snooping V1,V2,V3 | | |
| 17 | 交换机状态显示 | 支持通过控制器平台查看交换机端口负载情况 | | |
| 18 | 网络管理 | 支持通过 APP 进行远程管理,并且可以修改交换机网络配置，提供 APP 软件功能配置截图证明并加盖厂商公章； | 是 | ▲ |

## 2.9 存储交换机

| 序号 | 技术名称 | 技术要求 | 关键指标说明 | 主要标识指标 |
|---|---|---|---|---|
| 1 | 固定端口 | 15 个万兆 SFP+光口，1 个千兆 SFP 光口，1 个千兆电口。支持全端口线速转发；交换容量：1.28Tbps/12.8Tbps，包转发率：420Mpps | | |
| 2 | 整机功耗 | 整机功耗≥300W | | |
| 3 | 冗余性 | 支持双电源模块，5 个风扇模块； | | |
| 4 | 管理端口 | 1 个 Console 口 | | |
| 5 | USB 端口 | 1 个 USB2.0 端口； | | |
| 6 | 交换机性能 | 交换性能≥2.56Tbps/40.96Tbps<br>包转发率≥1080Mpps | | |
| 7 | 接入方式 | 支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时在控制器平台灵活的进行切换 | | |

| | | | | |
|---|---|---|---|---|
| 8 | DHCP Snooping | 支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文 | | |
| 9 | 交换机零配置上线方式 | 二层广播自动发现控制器平台<br>配置静态 IP 地址三层发现控制器平台<br>DHCP Option43 方式发现控制器平台<br>DNS 域名发现控制器平台 | | |
| 10 | 一键替换 | 支持通过控制器平台一键替换“按钮”即可完成故障设备替换，提供平台功能截图证明并加盖厂商公章； | 是 | ▲ |
| 11 | M-LAG | 支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面 | | |
| 12 | 交换机状态显示 | 支持通过控制器平台查看交换机端口负载情况。 | | |
| 13 | 网络管理 | 支持通过 APP 进行远程管理，并且可以修改交换机网络配置，提供 APP 软件功能配置截图证明并加盖厂商公章；<br>支持通过控制器平台跨广域网、NAT 远程管理智能交换机。 | | |
| 14 | 交换机画像管理 | 支持通过在控制器平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息，提供功能截图证明并加盖厂商公章；<br>支持通过控制器平台图形化操作对交换机端口状态的开启与关闭，提供功能截图证明并加盖厂商公章； | 是 | ▲ |
| 15 | 运维 | 支持通过控制器平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作；<br>支持通过控制器平台查看交换机处于工作端口的最近 5 分钟、1 小时、最近 1 天、最近 1 周发送与接收的流量趋势； | | 否 |
| 16 | 智能终端类型识别 | 支持终端类型库，基于指纹自动识别 PC、路由器、监控终端设备等，提供平台终端类型识别库截图证明并加盖厂商公章；<br>支持基于终端类型自动识别结果，禁止非法终端(例如私接路由器)接入 | 是 | ▲ |

| | | | | |
|---|---|---|---|---|
| 17 | 终端安全策略 | 支持终端 IP-MAC 绑定，当 IP+MAC 不对应时，可以将终端加入黑名单实现断开终端流量<br>支持终端 IP-MAC 首次部署自动学习绑定<br>支持将交换机的端口进行端口组划分，方便配置管理<br>支持预留的特权 IP 必须由管理员审批才可以使用，同时支持 IP 白名单免审批<br>支持终端的 MAC 与交换机端口变更检测<br>支持终端发生安全策略事件后，交换机将终端加入黑名单<br>支持交换机端口终端类型变更后，通过 APP、短信告警<br>可以自定义交换机端口接入终端类型，及 MAC 黑白名单 | | |

## 2.10 分布式存储

| 序号 | 技术要求 | | 关键指标说明 | 关键指标标识 |
|---|---|---|---|---|
| 1 | 基本要求 | 国内知名品牌，非 OEM 产品，非联合产品。拥有自主知识产权，能够提供分布式存储授权软件的自主知识产权证书 | | |
| | | 采用控制器集群全冗余架构设计，无独立元数据节点。性能随节点数量的增加而近线性提升。提供多控制器负载均衡及故障自动切换功能。 | | |
| | | 要求提供 SAN、NAS+Object 统一存储系统，一套系统同时支持 iSCSI、NFS、CIFS、S3、Swift 存储服务，实现统一管理。（提供公司产品彩页，并加盖公章） | | ▲ |
| | | 同时提供纠删码、副本做数据保护策略，保障数据冗余安全； | | |
| | | 支持在不停机情况下，向集群中添加存储节点，实现业务不中断情况下扩充容量和性能。集群支持节点数不少于 5000 个。 | | |
| 2 | 配置要求 | 存储节点,本次配置≥3 个存储节点;每个存储节点配置≥1 颗 8 核 CPU； | | |
| | | 高速缓存，要求至少配置单控制器≥32GB | | |
| | | 系统支持千兆、10GE、40GE 主机接口，本次要求每个存储节点配置 4 个千兆口，4 个 10GE 接口。 | | |
| | | 要求配置 6 块 480GB 企业级 SSD，15 块 4T 企业级 SATA 磁盘。提供可用空间 30TB。 | | |
| | | 支持 SSD、SAS、NL-SAS、SATA 类型硬盘混插； | | |
| 3 | 对象存储 | 支持 Amazon S3 标准接口，兼容 S3 生态体系； | | |
| | | 对象分池处理：大对象存入 EC 数据池，有效提高存储空间利用率，小对象和索引数据存入副本性能池 | | |
| | | 支持对象数据网关加密，避免数据通过其他非法途径获取，保证数据安全。 | | |
| | | 支持针对海量小文件存取优化，同时聚合小对象为大数据块整体操作，提升小文件下的空间利用率。 | | |
| | | 对象存储桶支持多版本，开启多版本后，桶中的对象都以多版本形式 | | |

| | | | | |
|---|---|---|---|---|
| | | 存储。 | | |
| | | 对象存储支持 SSL 访问加密，通过购买受信任 CA 认证中心颁发的数字证书，然后应用在对象存储，可将 HTTP 访问转换成 HTTPS，提供认证加密功能。在客户端和服务器端之间建立加密通道，保证数据在传输过程中不被窃取或篡改。 | | |
| | | 支持对象存储负载均衡，在保证对象存储高可用的同时，实现负载均衡作用。 | | |
| | | 支持对象存储整池扩容功能，避免大规模池内扩容导致海量数据重平衡 | | |
| | | 支持 bucket 的生命周期配置，用于定期清理不需要的旧对象 | | |
| | | 支持 Qos 功能，可以设置不同用户访问某个 bucket 的带宽/请求数 | | |
| | | 支持多数据中心部署，统一管理各地数据中心集群，实现数据同步存储； | | |
| | | 支持对 bucket 的 ACL 配置，控制不同用户对同一 bucket 的访问权限（提供配置截图，加盖厂家公章） | 是 | ▲ |
| 4 | 文 件 存储 | 支持支持 NFS V3.0 和 CIFS 1.0/2.0/3.0 标准接口 | | |
| | | 支持文件系统级链接克隆及独立克隆。 | | |
| | | 支持文件行为审计功能，用于记录客户如访问、创建、删除等常规文件操作行为； | | |
| | | 快照，支持目录级快照功能，可按时间点策略进行快照，支持快照数≥1024 个。支持快照重命名功能，支持删除快照链上任意快照点，支持文件数据回滚。 | | |
| | | 可实时查看访问 CIFS 共享目录的 Session 信息，并显示 CIFS 共享路径总的连接数； | | |
| 5 | 块存储 | 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，快速恢复数据的冗余度，确保用户数据的可靠性和安全性。（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| | | 支持多副本冗余功能，支持 2 个或以上副本，副本互斥地保存在集群的不同节点，当 1 个或多个主机或者磁盘故障，确保数据依旧正常访问。 | | |
| | | 提供超高性能块存储，单节点可提供至少 10 万 IOPS，集群能够提供百万级 IOPS 和 12GB/s 以上的带宽能力（要求厂家提供性能满足要求的承诺函，并提供集群的相应测试数据，加盖厂家公章） | 是 | ▲ |
| | | 支持条带化功能，实现分布式 raid0 的性能提升效果，并且支持以逻辑卷或 LUN 为单位设置不同的条带数（需提供产品功能截图，并加盖厂商公章） | 是 | ▲ |
| 6 | 高 级 功能 | 文件存储要求配置目录配额管理功能，支持容量和文件数配额。 | | |
| | | 支持一键检测功能，支持用户自行检测系统健康状态，检测包括 CPU、内存、硬盘、网口等硬件故障、告警等问题，同时支持检测各类存储服务是否正常启动。针对问题能够提出解决推荐办法。 | | |
| | | 智能缓存，通过基于 sraft 数据一致性协议实现分布式缓存，提供高性能的 I/O 读写优化。智能缓存拥有独立的可靠性机制，拥有 3 副本的容错能力。 | | |
| | | 智能分层，提供数据冷热智能分层，通过 SSD 缓存针对性提高读写性 | | |

| | | | | |
|---|---|---|---|---|
| | | 能。通过智能业务感知，分析判断数据冷热情况，从而实现热数据优先保存性能高的 SSD 中，从而实现提高存储性能。 | | |
| | | 故障自动恢复，在主机或者硬盘故障情况下，支持快速数据重建，重建速度 1TB/30min，智能感知 IO 压力，保证运行业务性能； | | |
| | | 数据自动平衡，支持数据自动和手动进行热平衡，无需中断业务，自动感知业务 IO，智能限速。支持设置平衡时间，利用空闲时间平衡数据。（要求提供界面截图并加盖公章） | 是 | ▲ |
| | | 亚健康监测，支持对硬件健康及亚健康状态的检测及管理。通过扫描硬件状态，对故障点做预警分析，同时提出解决方案建议。减少设备故障对信息系统的影响。 | | |
| | | 机械盘加速，通过给机械盘配置缓存空间，提高数据写入磁盘的速度。 | | |
| 8 | 可视化 | 智能监控平台，能够清楚展示当前存储的关键硬件和逻辑资源，包含存储池、块存储、文件存储、对象存储、服务器硬件状态，并且能够在监控视图中根据当前状态给予客户提示，以达到快速清晰告警的目的。同时为了方便客户排错，支持点击各个资源和硬件等，能够展示当前选中单元的详细信息。（要求提供界面截图并加盖公章） | 是 | ▲ |
| | | 配置界面上提供细化到每个节点的磁盘级监控，在管理界面上每个节点的磁盘与物理服务器真实盘位实现一一对应 | | |
| | | 存储拓扑，支持存储拓扑功能，展示块存储当前授权服务器和 LUN 之间的对应关系方便用户查看以及故障定位。 | | |
| 9 | 数据安全 | 文件存储，访问审计，对用户访问操作的文件动作进行全量审计，并支持审计日志导出。 | | |
| | | 用户权限管理，支持 NFS 访问用户鉴权，共享目录访问权限校验，文件修改 ACL 策略权限校验。 | | |
| | | 支持对象行为审计功能，用于记录客户如上传、下载等常规对象操作行为 | | |
| 10 | 产品资质 | 为确保软件的开发成熟度，要求分布式存储厂家具备 CMMI5 级别证书，需提供证书复印件加盖厂家公章； | | |

## 二、采购项目商务要求

1、报价要求：本项目为总价包干，投标人承诺所投价格包含了完成项目所有系统建设费用，包括项目设备采购、软件开发、安装部署涉及的所有软件、人工等费用。

2、建设要求：中标人须根据惠州第六人民医院的原信息化系统及业务需求开展，深入调研，形成需求规格说明书及项目实施方案，确保项目能满足建设工程项目建设要求，符合三级综合医院评审标准、HQMS 质量体系等相关标准规范。

3、实施要求：医院信息化工程部分描述为概要性要求，不作为最终实施和验收标准，每项系统的实施以中标方进场实施时与用户单位正式确认的用户需求确认书及中标方根据用户需求确认书提供的实施方案为准。

4、实施目的：通过本次项目建设需符合《医院信息互联互通标准化成熟度测评》四级甲等标准，确保系统能通过互联互通四级甲等测评。

5、建设内容：系统与医院现有的相关信息系统（包含但不限于 HIS 系统、PACS 系统、EMR 系统、LIS 系统、医保系统、省厅病案系统、供应室系统）对接，中标人承担第三方系统接入产生的所有费用（包括第三方系统接入平台改造等费用），实现各应用系统数据互联互通，建立临床数据中心。系统建设过程，确保不影响医院医疗业务的正常开展；系统建设须根据用户最新的业务需求及医疗政策进行调整。中标商须提供医院各信息系统现有应用系统的数据梳理及整合服务，完成基于现有的信息系统数据的临床数据中心、运营数据中心建设。

6、本次项目建设需要实现根据国家、省、市计生卫生主管部门要求，与国家、省、市相关的计生卫生信息系统及社保信息系统对接，中标人承担对接的开发工作及第三方系统的接入改造费用。

★7、服务要求：项目要求 2020 年 10 月达到医院信息系统互联互通成熟度标准四级甲等要求，参加并通过 2021 年医院信息系统互联互通成熟度标准四级甲等标准评审，2021 年通过最终验收。

8、工期要求：12 个月。

9、项目实施要求

9.1 人员组织管理

（1）中标供应商必须针对本项目专门建立一个完善和稳定的管理组织机构。稳定的项目负责人，其中必须包括一名专职负责的项目经理。

★（2）投标人若中标须承诺，在质保期内，投标人必须至少配备 1 名以上参加系统开发和熟悉本项目的技术人员，如更换技术人员，需提供不低于原技术人员同等资历的人员，并通过用户书面同意。

（3）项目实施期间，项目经理、技术负责人必须长驻惠州，接到采购人通知 2 小时内必须到达采购人现场处理问题。在系统实施期间，投标人承诺的项目经理和关键人员未经用户同意不得调整，中标供应商如中途更换项目经理，必须征得用户同意。

中标供应商必须无条件接受采购人的监督检查，并承担人员不足、不到位所导致的相关质量、进度等违约责任。

（4）对中标供应商在项目实施过程中出现资源、进度、质量协调控制不力的情况，招标方有权要求更换相关项目人员，中标供应商必须予以配合，并确保不影响项目建设的进度和质量。

（5）投标人必须在响应文件中提出项目组织方案、人员名单及沟通方案。

9.2 计划与进度要求

（1）投标人应在响应文件中必须提出详细的工作方案，明确项目开发方法、所采用的关键技术，项目管理过程，充分分析项目的可行性及存在的风险，提出完善的项目解决方案及项目计划，包括需求调研计划、软件开发计划、测试计划、部署及试运行计划、售后服务计划等，各阶段设立里程碑，经采购人审核批准后，作为项目的最终实施计划。

（2）投标人应承诺允许项目单位的全过程监管系统的调研、设计、开发、测试、集成、诊断及解决遇到的问题等各项工作。提出在开发过程中的开发计划及详细的进度安排计划，在项目实施过程中进行追踪和控制，定时总结并提交开发进度周报。投标人必须在响应文件中提出项目的开发计划、进度安排计划、项目实施过程中的追踪和控制方案。

10、培训要求

10.1 培训资料要求

投标人在响应文件中提出全面的培训计划和课程内容安排，承诺合同签订后征得用户方同意后实施。中标供应商应承担培训所产生的所有费用。所有的培训资料必须是中文或英文书写。

10.2 培训内容及目标

本项目培训包括用户培训和系统管理员培训。投标人在响应文件必须针对不同的对象制定不同的培训计划，中标供应商则应根据实际数量分别培训，项目培训要求达到以上目标：

（1）普通用户培训目标，中标供应商完成对用户的普通用户进行技术培训，用户能够正确熟练地使用系统，培训人员为所有使用系统的用户。

（2）系统管理员培训目标，中标供应商完成对系统管理员及技术人员进行全面培训，系统管理员及技术人员熟练管理集成平台并可以实现服务的管理维护，完成集成平台日常的管理维护等工作。培训要求达到采购人能自行实施服务配置、调试及发布，具备实施接口发布、更新与维护的能力。

（3）人数要求

用户培训：惠州第六人民医院工作人员；

系统管理员：惠州第六人民医院系统管理员。

（4）时间要求

用户：不少于 10 个工作日；

系统管理员：不少于 5 个工作日。

11、验收要求

11.1 软件验收要求

（1）系统验收

对整个项目的验收包括检查整个系统是否实现了采购人在本标书中所要求的功能，采购人在本标书中所采购的第三方软件和硬件是否能符合要求并满足用户的需求，是否与中标供应商提出的解决方案中既定目标功能完全一致。

（2）文档验收

系统总体设计方案在响应文件中提出验收方案和验收文档清单（包含需求调研、系统分析、软件设计、软件开发、系统测试、实施上线、运行维护等阶段），项目完成后，采购人将根据验收方案对系统每个部分逐一进行项目用户验收。

投标人在响应文件中必须提供详细的项目验收方案。

（3）医院通过医院信息互联互通标准化成熟度四级甲等测评。

（4）验收要求

软件系统的验收属于项目的合同验收，应符合信息化项目相关验收管理办法的要求，同时应符合下列要求：

①满足合同和招标文件中列举的全部要求。

②实现合同和招标文件中列举的全部功能和非功能要求。

③达到合同和招标文件中列举的全部指标。

④文档齐全，符合合同和招标文件及相关标准要求，包括但不限于下列文档；需求说明书、概要设计说明书、详细设计说明书、数据库设计说明书、测试计划、测试报告、用户手册、项目计划书、用户培训计划、会议记录和开发进度月报等。以及满足用户使用、医院信息部门运维及二次开发、项目实施管理及档案管理部门、主管信息化部门及资金来源管理部门的验收的其它文档。

⑤验收项目包括按照合同和招标文件中所标明的软件系统，及相关的技术维护文档、培训教材、使用说明书等。

⑥如需进行验收测评，投标人需配合采购人进行验收测评。

（5）实施及验收要求

项目验收包括初验（用户验收）和终验（综合验收）。具体要求如下：

项目试运行期满，达到验收条件的，进行符合性检查，符合性检查结果作为用户验收依据。本期所有系统正式投入运一个月后进行用户验收，用户验收小组由采购人与中标供应商相关人员共同组成，验收结果双方主管人员签字认可，存档留作验收时参考。用户验收标准参照下表要求：

| | |
|---|---|
| 验收标准 | 1）所有建设项目按照合同要求全部建成，并满足使用要求； |
| | 2）各个分项工程全部初验合格； |
| | 3）软件已置于配置管理之下； |
| | 4）各种技术文档和验收资料完备，符合合同的内容； |
| | 5）系统建设和数据处理符合信息安全的要求； |
| | 6）经过相关主管部门和项目业主同意； |
| | 7）合同或合同附件规定的其他验收条件。 |

12、售后运维服务

12.1 质保期

（1）应用软件系统

项目通过最终验收后，中标供应商须提供 1 年以上的免费软件版本升级、功能更新和现场维护服务。

（2）第三方软件产品

本项目所采购的第三方系统软件均需提供原厂 1 年以上原厂上门免费维护服务。

12.2 软件服务

（1）应用软件系统售后运维服务要求

中标供应商为用户方提供 1 年的免费维护服务和技术服务支持，免费维护包括数据梳理、数据整合、系统适配、系统维护、功能完善、性能提升、故障检测、不超出系统功能范围的二次开发，并保证中标供应商所开发的软件正常运行。

（2）第三方软件产品售后运维服务要求

为本项目中第三方软件产品提供原厂 1 年以上现场免费维护服务，包括系统维护、测试、联调和安装。

（3）售后运维服务人员要求

在质保期内，投标人必须至少提供 1 名以上参加系统开发和熟悉本项目中软件的工程师驻场，接收采购人管理，提供有关软件的技术支持。配备 1 名以上参加系统开发和熟悉系统、第三方软件系统的工程师，提供有关软件的技术支持。

（4）售后运维服务方式要求所

有保修服务方式均为投标人上门保修，即由投标人派员到采购人使用现场维护。

（5）售后运维服务质量要求

本项目投入正式运行和在免费服务期内，每个月进行一次系统全面检测；出具检测报告，系统出现故障时，中标供应商全天候 24 小时服务响应，维护工程师应在接到报障后 30 分钟内到现场处理应用系统出现的故障；及时做出故障原因报告并提出有效措施加以解决。硬件故障必须在 1 小时之内解决，如在 1 小时内无法排除故障，必须提供相同的产品代替，确保不影响业务的开展。

（6）售后运维服务责任及费用

在项目验收后的免费服务期内，如因需要增加系统功能而产生的费用，双方另议；如果是软件设计漏洞或偏差，中标供应商必须免费修正。免费服务期间，中标供应商为采购人提供服务所产生的一切费用均由中标供应商承担。项目免费服务期满后，中标供应商必须承诺在法定工作时间内，可以提供免费的技术指导和咨询，如需其他技

术支持服务，则费用由双方另议。

投标人在响应文件中要求提出详细的软件售后服务方案。

13、质量管理要求

13.1 源代码风格要求

中标供应商程序开发要求严格遵照相关的国际、国内及行业标准，系统软件开发的规范化保证，要有统一的命名规范，良好的编码风格，统一的代码布局格式，详尽的程序注解等，对软件开发的各个阶段都要进行质量评审，并提供评审报告。

13.2 质量控制要求

（1）质量控制依据中标供应商要求根据 ISO9000、CMM 及项目管理成熟度模型，结合本项目的实际情况，编制详细的质量控制计划。

（2）质量监督及责任中标供应商必须接受采购人的质量监督检查，提供真实有效的相关质量活动记录、证据，无条件接受招标方提出的质量问题整改要求，承担质量责任及因质量问题导致的进度延迟责任。

（3）软件质量测试对软件的测试应贯穿于系统开发的始终，要提供详尽的测试计划、测试报告及结果分析报告。

投标人必须在响应文件中提出质量控制和保证机制。

13.3 文档管理要求

（1）文档管理内容要求中标供应商提供的文档包括需求说明书、系统概要设计说明书、系统详细设计说明书、数据库设计说明书、测试计划、测试记录、测试分析报告、系统维护手册、操作手册、系统安装手册、能够编译生成目前正在运行的应用程序的源代码以及采购人认为必要的其他文档等。

（2）其他文档要求项目管理应提交软件开发和实施计划、进度报告、培训计划、培训记录、例会记录以及采购人认为必要的其他文档。

（3）文档语言要求未经采购人另行许可的情况下，本项目所有的技术文件必须用中文书写或有完整的中文翻译。

（4）投标人必须在响应文件提出文档管理方案。

13.4 需求变更管理

（1）变更控制委员会（CCB）变更控制委员会是项目变更的提出及审核机构，要求由建设单位及承建单位的项目负责人、技术负责人及单位信息分管领导共同组成，进行严格分工，处理不同类型或重要程度不同的项目变更建议。

（2）变更控制机制项目可能会因为对项目的实施前提、项目范围、进程安排、阶段性标准、交付物、价格或付款条件等条款的变更的原因，要求进行本项目的变更。本机制的制定是为了检查所有的变更请求，决定哪些需要实施、哪些需要推延、哪些需要否决。

（3）变更过程如双方需进行项目变更，则需遵守以下申请步骤。

第一步变更申请方要求先填写《项目变更申请》。

第二步 CCB 组织就《项目变更申请》的技术可行性以及对整个项目的影响做出评估。经过批准的《项目变更申请》将转给中标供应商，未被批准的将被退还给变更申请方。

第三步成交投标方将在接到《项目变更申请》的 3 天内编写相应的《项目变更建议书》。《项目变更建议书》就《项目变更申请》中所提出的修改对整个项目的影响做出说明。

第四步 CCB 组织对《项目变更建议书》进行审核和批准，根据变更的。

第五步对于 CCB 批准通过的项目变更，中标供应商必须 3 个工作日内投入实施。

变更责任由于建议单位提出的变更累积变更所增加的工作量不超过 0.5 个人月的，中标供应商可以免费修改。累积增加工作量超过 0.5 个人月的，双方另行签订协议处理。

投标要必须在响应文件中提出详细的变更管理方案。

13.5 部署、安装调试要求

（1）投标人在响应文件中必须向采购人提供本项目采购的系统安装、部署和调试工作。若项目系统实施过程中出现不合理或不完整的问题时，投标人有责任和义务在响应文件中提出补充修改方案并征得采购人同意后付诸实施。

（2）中标供应商应首先拟出一个测试方案，具体到每一个测试步骤，与采购人讨论通过后，方可按计划进行测试。

（3）安装调试及搭建测试环境在项目单位指定的地点进行。中标供应商负责全部应用软件的安装、调试及正式运行前的测试。

14、付款方式

（1）合同生效后 10 个工作日内，采购人支付合同总额的 40%。

（2）项目设备全部到货且安装调试后，采购人支付合同总额的 20%。

（3）项目上线后 10 个工作日内，采购人支付合同总额的 20%。

（4）项目通过最终验收后 10 个工作日内，采购人支付合同总额的 15%。

（5）项目免费维保期为一年，维保期后 10 个工作日内采购人支付合同总额的 5%。

**注：招标文件中带“▲”号条款为评审时的重要评分依据，不作为报价无效条款，未响应或不满足将导致扣分。带“★”号条款为实质性响应性条款，偏离将导致废标。**