**信息容灾机房租赁项目（2022年）需求**

# 项目名称及项目概况

**1.1 项目名称：信息容灾机房租赁项目（2022年）。**

**1.2 项目概况：**

广东省人民医院由于院内机房空间不足，资源紧张，需要租用运营商机房空间及硬件资源作为容灾数据中心建设容灾系统，以满足信息系统快速发展的需求。2021年通过租赁中国移动广东分公司的机房资源，完成了容灾数据中心建设，实现医院HIS、LIS系统的异地容灾，提升核心系统的数据安全及可靠性。

为进一步提升医院核心业务系统的可靠性和可持续发展，继续缓解医院机房资源紧张的困境，拟继续租用运营商机房空间及硬件资源建设容灾数据中心，建设核心业务系统的容灾系统，并提供互联网医院、影像中心等业务系统对计算能力、存储资源的需求。

# 采购清单

项目采购服务清单如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 分项 | 配置描述 | 数量 | 租用期 |
| 1 | 容灾系统 | 详见3.1 容灾系统需求 | 1套 | 2年 |
| 2 | 灾备机房资源 | 详见3.2 灾备机房资源需求 | 1套 | 2年 |
| 3 | 云主机资源 | 详见3.3 云主机资源需求 | 1套 | 2年 |
| 5 | 光纤线路 | 详见3.4 光纤线路需求 | 4条 | 2年 |

# 技术参数要求

* 1. 容灾系统需求

国家标准《信息系统灾难恢复规范》（GB/T20988-2007）规定了六个级别的容灾，下表分别针对每个级别的内容要求给出了相应的应对措施。

|  |  |  |
| --- | --- | --- |
| 级别 | 内容 | 措施 |
| Level 6 | 数据零丢失和远程集群支持 | 实现远程数据实时备份，实现零丢失；应用软件可以实现无缝切换；远程集群系统的实时监控和自动切换能力。 |
| Level 5 | 实时数据传输及完整设备支持 | 实现远程数据复制技术；备用网络也具备自动或集中切换能力。 |
| Level 4 | 电子传输及完整设备支持 | 配置所需要的全部数据和通讯线路及网络设备，并处于就绪状态；7\*24 运行；更高的技术支持和运维管理。 |
| Level 3 | 电子传输和部分设备支持 | 配置部分数据通信线路和网络设备；每天实现多次的数据电子传输；备用场地配置专职的运行管理人员。 |
| Level 2 | 备用场地支持 | 预定时间调配数据通信线路和网络设备；备用场地管理制度；设备及网络紧急供货协议 |
| Level 1 | 基本支持 | 每周至少做一次完全数据备份；  制定介质存取/验证和转储的管理制度；完整测试和演练的灾难恢复计划。 |

容灾系统应遵循科学先进、实用高效、安全可靠、节能环保的理念，按国家标准《信息系统灾难恢复规范》（GB/T20988-2007）关于灾备系统能力的6级标准，结合广东省人民医院HIS、LIS系统的实际业务情况，要求容灾系统数据零丢失，实现数据层和应用层容灾的手动或自动切换，生产中心和容灾中心应具备对称的基础设施和网络设备，保障数据管理层面、应用程序层面、访问通道层面都能够平滑切换。

### 3.1.1 容灾系统范围

**1、新一代HIS系统**

新HIS系统由5台高性能数据库服务器、近100台虚拟机,通过F5负载均衡设备实现七层负载均衡分发。

**数据库配置情况：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用 | 系统情况 | 存储空间 | 数据库 |
| 1 | HIS系统数据库(主库，3台) | 服务器配置：华为 5885H V5  4 \* Intel Xeon Platinum 8280，内存1024G | 截止2022年9月30日数据量为4TB（每月增加300GB） | Oracle 19.12 |
| 2 | HIS系统数据库（DG库， 2台） | 服务器配置：华为 5885H V5  4\*Intel Xeon Platinum 8280，内存1024G | 截止2022年9月30日数据量为4TB（每月增加300GB） | Oracle 19.12 |

**应用服务器（虚拟化）配置情况：**

|  |  |  |  |
| --- | --- | --- | --- |
| **应用类型** | 数量 | 配置 | 应用 |
| **IIH 基础架构** | 30台 | CentOS 7.2  CPU 4核心，内存8GB | RocketMQ、  FastDFS  redis  codis  zookeeper  nginx  Jetty |
| **IIH中间件** | 11台 | CentOS 7.2  CPU 8核心，内存16GB |
| **第三方访问/平台对接中间件** | 4台 | CentOS 7.2  CPU 8核心，内存16GB |
| **XAP/报表中间件** | 4台 | CentOS 7.2  CPU 8核心，内存16GB |
| **运维平台\资源服务器** | 3台 | CentOS 7.2  CPU 8核心，内存16GB |

**2、LIS检验信息系统**

检验系统数据库使用两台高性能服务器安装linux7.2操作系统，部署Oracle 高可用架构，数据库版本Oracle11.2.0.4。应用服务器由2台高性能服务器部署MSCS群集，存储分别划分了10T/3TB空间用于存放检验报告、应用数据。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用 | 系统情况 | 存储空间 | 数据库 |
| 1 | LIS系统数据库 | 两台联想SR950，四路Intel(R) Xeon(R) Gold 5118，512GB内存 | 3T | 安装RHEL 6.5操作系统，部署Oracle 高可用方式，Oracle11.2.0.4 |
| 2 | 应用服务器 | 两台HP388 gen 9，2颗E5-2630，256GB内存 | 0.5T | Windws server 2012R2  sqlserver 2008R2sp3 |

### 3.1.2 容灾系统要求

* + - 1. 基础设施和网络要求

建设满足当前新HIS、LIS系统运行所需软硬件容灾环境，实现数据层和应用层容灾的手动或自动切换，生产中心和容灾中心应具备对称的基础设施和网络设备，保障数据层面、应用程序层面、访问通道层面都能够平滑切换；要求提供独立的网络环境。



* + - 1. 容灾系统的设备清单

建设满足当前新HIS、LIS系统运行所需软硬件容灾环境，当业务系统架构发生变化时，容灾环境需做同步调整。容灾系统的设备清单，包括但不限于如下列表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 归属 | 配置 | 数量 | 单位 |
| 1 | HIS数据库容灾服务器 | CPU:4\*18C 内存：512GB HBA：2\*16G单口 网络4\*10G，网络电口4\*1G 硬盘3\*960GB SSD | 3 | 台 |
| 2 | HIS数据库延时服务器 | CPU:4\*18C 内存：512GB HBA：2\*16G单口 网络4\*10G，4\*1G 硬盘2\*300GB | 1 | 台 |
| 3 | HIS应用服务器集群 | CPU:4\*18C 内存：512GB HBA：2\*8G单口 网络2\*10G，4\*1G 硬盘2\*300GB | 9 | 台 |
| 4 | 应用服务器集群 | CPU:2\*8C，64G内存，2\*600G。20片刀片合共2个刀箱，每个刀箱共享两个8\*8G HBA口，两个8\*10G网络光口 | 20 | 组 |
| 5 | LIS数据库容灾服务器 | CPU:2\*8C 内存：256GB HBA：2\*8G单口 网络2\*10G，4\*1G 硬盘2\*600GB | 2 | 台 |
| 6 | 存储 | 双控制器，支持San copy、MirrorView，支持Fast Cache、Fast VP，8\*1.6T SSD，12\*900GB，5个200G CACHE SSD，30\*4TB NLS，25\*1200GB，共120TB可用存储空间。 | 1 | 台 |
| 7 | 负载均衡器 | LTM license，2口万兆、8口千兆 | 4 | 台 |
| 8 | 48口万兆交换机 | 48口万兆交换机 | 2 | 台 |
| 9 | 带外管理服务器 | 4C，16G内存，网络电口4\*1G，600G硬盘\*2 | 1 | 台 |
| 10 | 带外管理交换机 | 48口百兆交换机 | 1 | 台 |
| 11 | 光纤交换机 | 8GB SAN光纤交换机 | 2 | 台 |

* + - 1. RPO/RTO指标要求

| 项目 | 指标 |
| --- | --- |
| 容灾恢复需要时间（RTO，Recovery Time Objective） | 小于15分钟 |
| 容灾保护需要时间（RPO，Recovery Point Objective） | 小于1分钟 |

* + - 1. 应用容灾需求

要求生产中心和容灾中心支持应用主备容灾，通过全局负载均衡设备可以将外部对系统的访问流量导向双数据中心。并采用自主知识产权的容灾服务平台进行容灾策略调整和监控。

应用容灾应满足应用程序版本一致性的要求。应用程序的版本决定了处理算法的不同，如果出现生产、容灾中心应用陈旭版本不一致将可能导致系统运行故障，甚至会导致数据损失等严重后果。因此，需要保持生产中心、容灾中心应用程序版本的一致性。

* + - 1. 数据容灾需求

数据容灾对象包含：主机（含虚拟机）、数据库、非结构化存储、网络存储等。正常情况下生产中心为主（读写）、容灾中心为备（只读），前端应用都连接到生产中心进行生产。

当生产中心工作正常，容灾中心发生故障时，生产中心不受影响，待容灾中心恢复后可自动同步，并追平生产中心的变化数据。

当生产中心发生故障停止工作后，容灾中心能通过便捷的操作方式快速切换为生产模式，接续生产。

当生产中心故障恢复后，进入数据恢复模式，此时仍然由容灾中心负责生产，数据将同步回生产中心。

生产中心完成数据同步后，能通过便捷的方式将业务切回生产中心。

* + - 1. 机房环境需求

要求提供高等级数据中心机房，生产中心与容灾中心在同一城市，距离不少于15公里。要求为用户提供可围栏的独立区域、独立机柜建立容灾中心，必须满足如下条件：

* 满足乙级建筑
* 抗震烈度：8度
* 一类市电引入
* 110kv变电站
* 数据机房承重能力：1000KG/平方米
* 电力机房承重能力：1600KG/平方米
* UPS采用2(N+1)的备份模式

要求提供双路由的传输专线构建生产中心与容灾中心的传输专网，网络传输带宽不小于1000Mbps，时延不超过50ms。

* + - 1. 安全要求

容灾系统涉及用户核心业务系统的患者数据，要求容灾中心符合网络等级保护2.0的三级认证，有完善的容灾机房管理制度，提供相关安全设备等。

* 1. 灾备机房资源需求

### 灾备机房资源需求

灾备机房的资源，主要为用户提供影像中心、测试环境计算及存储资源，基本要求如下：

| **序号** | **指标项** | **指标要求** |
| --- | --- | --- |
| 1 | 未虚拟化前计算资源要求 | 448个CPU核、1280GB或以上内存 |
| 2 | 虚拟化存储资源 | 200TB可用存储空间 |
| 3 | 影像中心的存储资源 | 400TB可用存储空间 |
| 4 | 网络资源 | 机房具有独立的核心交换机，防火墙，负载均衡设备等 |
| 5 | 虚拟化软件 | 提供兼容医院在用的VMware虚拟化环境，由用户根据需求对虚拟化资源进行分配和部署。 |

3.2.2 灾备机房资源清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **配置** | **数量** |
| 1 | IDC标准机柜 | 42U标准机柜及配套围闭、空调、3KW双路UPS电源、消防、门禁、安防、PDU插座 | ≥6个 |
| 2 | 服务器 | 单台：2U 机架式服务器，2\*12核/24\*32GB内存/2\*480GB | ≥14台 |
| 2\*480GB SSD硬盘(系统盘)/2\*960GB SSD硬盘（数据盘），实配≥1块RAID卡，支持raid1/5/10 |
| 1\*双端口GE电口网卡/2\*双端口10GE光口网卡/交流双冗余电源/含操作系统, |
| 前面板上配备有液晶屏，可显示默认或定制信息。如果系统发生故障，该液晶屏上将显示关于故障的代码，具备远程管理网卡IPMI网卡，允许用户独立于操作系统状态之外（免代理安装方式）远程访问、监控、维修、修复和升级服务器。 |
| 租赁期内提供7x24h，当日4小时上门原厂硬件售后服务,提供故障硬盘免返还服务 |
| 3 | 虚拟化存储 | 单台：机架式均衡型存储服务器，2颗12核CPU /Intel，缓存≥384GB内存 | ≥1台 |
| 2\*480GB SSD硬盘（系统盘），2\*960GB SSD硬盘，22\*1.2TB SAS硬盘(数据盘） |
| 2块万兆双口光网卡，1\*2口GE以太网口,具备远程管理网卡IPMI网卡，支持raid1/5/10,电源冗余,含操作系统 |
| 每个硬盘框高度2U/2.5寸硬盘25盘位,每个硬盘框高度4U/3.5寸硬盘24盘位 |
| 块基础软件包授权许可(含磁盘存储软件)/含负载均衡功能、自动精简配置、存储分层管理、自动数据迁移、在线重复数据删除、智能数据压缩、数据加密功能、快照、克隆、同步远程复制、异步远程复制、NDMP功能； |
| 块存储升级统一存储基础软件包授权(含磁盘存储软件)/含单机监控管理软件、单机性能优化软件；文件系统协议(含磁盘存储软件)/含文件系统协议软件 |
| 4 | 影像中心存储 | 企业级存储 | ≥1台 |
| 实用存储容量400TB，块存储，具备双控双电，双控制器，支持San copy、MirrorView，支持Fast Cache、Fast VP，135个4TB NLS 硬盘。 |
| 5 | 核心交换机 | 单台：框式三层交换机，交流冗余电源，冗余主控板，可用业务槽位≥2，交换容量≥3Tbps，包转发率≥2000Mpps | ≥1台 |
| 24端口千兆以太网光接口模块(SFP+,LC)\*1 48端口万兆以太网光接口模块(SFP+,LC)\*1 |
| 支持Access、Trunk、Hybrid方式等、支持MPLS基本功能 支持基于MAC的动态VLAN分配、支持基于端口和VLAN的MAC地址学习限制 支持STP(IEEE 802.1d)，RSTP(IEEE 802.1w)和MSTP(IEEE 802.1s)等 支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议 支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议 |
| 6 | 接入交换机 | 单台：数据中心接入交换机，单台配置48个10GE光口，6个40GE光口（支持拆分为10GE端口） | ≥2台 |
| 支持支持智能表项技术，整机路由、ARP表项及MAC地址表可调，整机最大路由地址表≥120K，最大ARP地址表≥120K，最大MAC地址表≥280K |
| 可靠性保障，支持前后风道、模块化风扇冗余配置、模块化双电源、带外网管、链路端口聚合、STP/RSTP/MSTP协议； |
| 7 | 带外管理交换机 | 单台：三层交换机，配置交流冗余电源，支持48个10/100/1000BASE-T电口,4个10G/1G BASE-X SFP+端口 | ≥1台 |
| 遵循 IEEE 802.1d 标准，支持 4K 个 VLAN，支持STP/MSTP/RSTP，支持IPV4/IPv6协议 |
| 8 | 防火墙 | 单台：主机交流型基本配置（含主机/主控\*1/网板\*3/交流电源\*2,4个业务槽位），防火墙业务板\*2，32端口万兆以太网光接口模块(SFP+,LC)\*1 | ≥2台 |
| 支持IPSec VPN、SSL VPN、 L2TP VPN、MPLS VPN、GRE等 支持IPv4：静态路由、RIP、OSPF、BGP、IS-IS等 支持IPv6：RIPng、OSPFv3、BGP4+、IPv6 IS-IS、IPv6RD、ACL6等 支持透明、路由、混合部署模式，提供访问控制、用户识别、应用识别、入侵防御、防病毒、APT防御等功能。 |
| 9 | 虚拟化软件 | VMware vSphere 企业增强版，带虚拟化网络管理功能（NSX）、虚拟化存储管理功能（VSAN）。 | ≥1套 |
| 基本要求 支持部署于X86架构服务器，虚拟化软件部署无需绑定服务器操作系统 |
| 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。 |
| 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IP地址、MAC地址等。 |
| 能够提供性能监控功能，可以对资源中的CPU、网络、磁盘使用率等指标进行实时统计，并能反映目前物理机、虚拟机的资源瓶颈。 |
| 支持虚拟机HA保护，在物理硬件故障的条件下，选择资源池中的其他健康物理主机重新部署虚拟机，并在原有数据不丢失的条件下，尽快恢复虚拟机业务。 |
| 支持现有市场上的主流x86服务器，具有双方认可的官方服务器硬件兼容性列表，包括华为、HP、DELL、Cisco、NEC以及国内自主品牌服务器等。 |
| 兼容现有市场上主流的存储阵列产品，具有双方认可的官方存储阵列兼容性列表，存储阵列类型包括SAN、NAS和iSCSI等，存储阵列品牌包括华为、EMC、IBM、HP、HDS、NetApp、Dell等。 |

* + 1. 灾备机房位置要求

| 指标项 | 指标要求 |
| --- | --- |
| 位置 | 数据中心附近400米内无任何产生腐蚀性气体、粉尘、噪音、强震动的厂矿企业和易燃易爆危险品或化学品的生产存放单位，800米内无铁路或高速公路。不属于地震断层附近、有滑坡危险区域和有可能发生洪水区域。数据中心位置不在建筑物的顶层或地下室，以及用水设备的下层或隔壁。 |

* + 1. 灾备机房标准

灾备机房应满足网络等级保护2.0标准的三级认证，以及《电子信息系统机房设计规范》中国家A级机房标准，并满足下述要求：

| 指标项 | 指标要求 |
| --- | --- |
| 产权要求 | 供应商所提供数据中心产权应归属供应商自身所有 |
| 认证要求 | 数据中心应通过ISO 27001信息安全管理体系认证 |
| 承重要求 | 机柜区域不小于1000kg/m²，电力电池区域的承重能力不小于1600kg/m² |
| 净空层高要求 | ≥3.0米 |
| 电梯要求 | 数据中心具有完备的客梯和货梯，其中货梯载重量≥2.0吨 |
| 防水要求 | 具有地湿报警器，24小时全天候监控，适时报警 |
| 防雷要求 | 需满足国家A级机房标准以及《建筑物防雷设计规范》GB50057和《建筑物电子信息系统防雷技术规范》GB50343的有关规定 |
| 综合布线要求 | 按照现行国家标准《综合布线系统工程设计规范》GB50311-2016的规定执行，机房布局采用下送风、上走线的方式。强电、弱电分走不同的桥架，减少相互之间的干扰。所有设备与网络配线柜之间互联以及网络配线柜之间互联的尾纤、双绞线等由成交供应商提供，并按采购人要求进行布线实施。 |
| 供电要求 | 数据中心所在园区具有专用变电站，提供7x24小时不间断供电，双路独立市电接入，油机满足数据中心整体功率要求，并采用冗余配置。UPS输出功率满足整体功率要求，电池满载备用时间满足至少30分钟要求；数据中心内电源列头柜和服务器机架为双路UPS电源输入；标准机柜和非标准机柜应能根据采购人设备需求进行供电改造。 |
| 制冷能力要求 | 采用数据中心专用空调，下送风方式，可精确控制各空间的温度及湿度，并配有冗余空调设备。新风系统高压输入洁净的新鲜空气，保证数据中心常年恒温恒湿，满足数据中心温度常年在21-25 摄氏度之间，相对湿度常年在40%-60%之间 |
| 消防要求 | 数据中心能够满足国家消防有关规定和数据机房建筑的特殊功能和技术要求，通过消防验收。采用高灵敏度的烟雾探测系统，能在第一时间发现火灾隐患，具备自动灭火系统在不停电的情况下实施灭火。机房墙壁、门、天花板采用防火建材；具备完备的安全走火通道和逃生门，并严格按照规范布置相关的安全指示。 |
| 安防要求 | 数据中心提供7x24小时的安保服务，机楼外围设置有专用安保执勤。机房门采用门禁卡、授权密码等方式控制人员出入，确保非授权人不得进入设备运行区域。 |
| 防静电及电磁防护要求 | 参考《税务系统信息安全等级保护基本要求》中第三级安全技术要求的物理安全技术要求中的相关规定，以及国家A级机房标准的要求 |
| 其它 | 数据中心需完全满足防虫、防鼠要求。机房需满足洁净度要求，在静态条件下测试，每升空气中大于或等于0.5μm的尘粒数应少于15000粒 |

* + 1. 机架服务需求

| 指标项 | 指标要求 |
| --- | --- |
| 机架要求 | 占用≥6个标准机架，总功耗≥18kw |
| 标准机柜及电源分配单元（PDU）要求 | 标准19英寸机柜，机柜承重托盘保证每机柜至少2块，PDU质量可靠，每机柜需提供双路电源，C13、C19或国标口电源插座、或接线柱接驳，每机柜不少于20位接入，并配备足够挡板。非标准机柜根据实际情况和采购人的要求进行改造。 |
| 预留空间要求 | 须围闭6个或以上的机架，作为采购人未来新增设备所用，供应商应在方案中阐明所额外预留的空间大小、位置等情况。 |
| 围蔽要求 | 要求具备空调、电源、消防、门禁、安防等基础设施，本项目提供的资源是医院重要信息化机房，需进行单独隔离，防止围蔽外人员触碰设备及机柜，围蔽区域设置门禁系统，门禁系统的权限根据用户要求配置。 |

* 1. 云主机资源需求
     1. **云主机资源的基本要求**

提供用户在用的互联网医院运行环境所需的云主机资源，互联网出口带宽及安全防护环境等相关资源。

* + 1. **云主机资源清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用分类 | 云产品名称 | 云产品类型 | 数量 |
| 1 | 数据库服务器1 | 云主机 | 通用型，16核，128G内存，高性能存储≥40G，2T存储，Windows Server 2019 DataCenter 64位 | 1台 |
| 2 | 数据库服务器2 | 云主机 | 通用型，16核，128G内存，高性能存储≥40G，2T存储，Windows Server 2019 DataCenter 64位 | 1台 |
| 3 | 代理服务器 | 云主机 | 通用型，4核，8G内存，高性能存储≥40G，500G存储，CentOS 7.6 64位，外网ip | 1台 |
| 4 | 应用服务器 | 云主机 | 通用型，8核，64G内存，高性能存储≥40G，500G存储，Windows Server 2019 DataCenter 64位，外网IP | 1台 |
| 5 | 应用服务器 | 云主机 | 通用型，8核，64G内存，高性能存储≥40G，500G存储，Windows Server 2019 DataCenter 64位 | 1台 |

* + 1. **云安全集成产品清单**

通过部署云安全平台，配套形成智慧云安全防护能力，对云主机进行安全防护。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 产品规格 | 数量（台） | 备注 |
| 1 | 态势感知 | 态势感知产品可通过采集系统的网络安全数据信息，对所有安全数据进行统一处理分析，实现对网络攻击行为、安全威胁事件、日志、流量等网络安全问题的发现和告警 | 5 | 支持至少5个授权管理，可根据具体业务情况提升配额满足需求 |
| 支持态势总览、资产管理、告警管理、弱点分析、日志库，警规则设置、日报/周报设置等 |
| 服务可用性不能低于99.00% |
| 2 | 云主机安全 | 云主机安全产品提供云主机安全保护功能，对每一台需防护的服务器，全面保障安全 | 5 | 支持至少5个云主机实例，可根据具体业务情况提升配额满足需求 |
| 支持云主机系统基线统一配置检查、自动化系统病毒检测、网站后门检测、系统口令暴力破解防护、反弹shell检测、主机异地登录提醒等 |
| 服务可用性不低于99.00% |
| 3 | Web应用防护 | web应用防护产品可应对Web应用中的各类攻击，充分保障Web应用安全 | 2 | 支持至少2个站点，100M防护带宽，可根据具体业务情况提升配额满足需求 |
| 支持防SQL注入攻击、防XSS 跨站脚本攻击、防CSRF攻击、HTTP 异常检测、缓冲区溢出检测、黑白名单管理 |
| 服务可用性不能低于99.00% |
| 4 | 云堡垒机 | 云堡垒机产品提供云资源安全管理平台，能对云上资产实现自动化运维功能，包括事前规划、事中控制和事后审计 | 1 | 支持至少20个资产管理，可根据具体业务情况提升配额满足需求 |
| 支持身份管理、角色分权、集中管控、资源改密、全程审计、命令控制、工单申请、报表分析 |
| 服务可用性不能低于99.00% |
| 5 | 数据库审计 | 数据库审计产品能够监控数据库，可用于审计移动云平台中的云数据库、自建数据库，提高数据安全等级和合规能力。 | 1 | 支持至少5个数据库实例，可根据具体业务情况提升配额满足需求 |
| 支持操作审计、多维度线索分析、操作行为检索、多样化审计报表 |
| 服务可用性不能低于99.95% |
| 6 | 日志审计 | 日志审计系统可以针对大量分散的异构日志进行集中采集、统一管理、存储、统计分析，协助医院满足等保合规要求、高效统一管理资产日志并为安全事件的事后取证提供依据。 | 1 | 支持至少10个数据源数量，可根据具体业务情况提升配额满足需求 |
| 支持日志统计展示、日志管理、事件管理 |
| 服务可用性不能低于99.00% |
| 7 | 安全中心 | 安全中心产品需对所有资产实现实时监控，让云上所有服务器的漏洞、威胁与攻击等情况一目了然，能够对资产进行统一的安全管控，满足网络安全等级保护制度对云主机的漏洞扫描、基线检查等监管合规要求 | 1 | 支持至少5个实例，可根据具体业务情况提升配额满足需求 |
| 支持安全总览、防暴力破解和动态蜜罐、自定义检测策略和周期检测基线配置、一键扫描发现漏洞、检测服务器弱口令、威胁检测 |
| 服务可用性不能低于99.95% |
| 8 | 云日志 | 提供用户级别的云日志产品，将数据以端-端的方式提供面向业务的运维日志分析与价值呈现，帮助用户利用实时日志进行线上业务维护 | 1 | 支持至少5个日志源数量，可根据具体业务情况提升配额满足需求 |
| 支持实时采集、查询分析、日志转储、关键字告警 |
| 服务可用性不能低于99.95% |
| 9 | 云审计 | 提供云审计产品，能够记录从页面控制台发起的资源操作请求，并且会记录每次请求资源操作的结果，并供查询、审计和回溯使用，同时支持将操作事件转存至高可靠、低成本的存储 | 1 | 支持至少7天内事件的存储和检索，可根据具体业务情况提升配额满足需求 |
| 支持事件追踪、事件列表展示、事件文件生成，对于需要长期存储的数据，支持转存至对象存储 |
| 服务可用性不能低于99.95% |
| 10 | 云监控 | 提供对云资源进行监控和告警的云监控服务，能够直观展示云主机、云硬盘、云存储等云资源的使用情况、性能和运行状况，以及针对指标设置告警 | 1 | 支持至少5个实例的监控，可根据具体业务情况提升配额满足需求 |
| 支持自定义监控，监控指标包括：计算资源监控、网络资源监控、数据库监控、拨测监控，并支持告警服务 |
| 服务可用性不能低于99.95% |
| 11 | 云防火墙 | 提供云防火墙产品，支持自定义防火墙规则，通过定义规则，允许或禁止流量通过。 | 1 | 支持至少1个私有网络的防护，可根据具体业务情况提升配额满足需求 |
| 支持二层逻辑隔离、公网地址和私网地址的转换 |
| 12 | 抗DDoS | 提供不低于5Gbps流量的DDoS(分布式拒绝服务)攻击防护安全产品，能够检测DDoS攻击和通过流量清洗设备对DDoS 攻击流量进行过滤 | 1 | 支持至少5Gbps流量防护攻击，可根据具体业务情况提升配额满足需求 |
| 支持异常流量检测与清洗、攻击防护、数据展示、黑洞策略 |

* 1. 光纤线路需求

### 3.4.1 光纤线路基本要求

根据业务需要，容灾中心在进行选址时需要考虑2对光纤线路，即生产中心与容灾机房、灾备机房的互联线路，双路由；生产中心与容灾机房、灾备机房的光纤线路速率不低于1000Mbps。互联网云主机需提供200M的出口带宽，详见下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 分类 | 产品名称 | 起止点 | 规格 | 数量（条） |
| 光纤专线 | 容灾机房专线 | 容灾机房到用户生产中心机房 | 每条专线传输带宽不小于1000Mbps，时延不超过50ms；光纤专线可复用，正常情况下可提供不小于2000M的传输带宽。 | 2 |
| 影像中心存储专线 | 灾备机房到用户生产中心机房 | 1000Mbps | 1 |
| 云主机专线 | 云主机互联网专线 | 200Mbps | 1 |

### 3.4.2 光纤线路服务需求

使用两条上下行对等千兆光纤线路连接用户中心机房与运营商机房，要求两条光纤异路由。传输设备采用冗余的物理光纤资源和光传输设备，实现线路级和设备级的双重冗余备份，确保网络可用率达到99.9%。

为保证专线安全可靠，应采用环网保护，设备应具备关键板卡热备份或冗余配置，最大限度地支持系统的正常运行。网络能够根据未来业务的增长和变化，随时可以平滑地扩充和升级至10Gb，最大程度的减少对网络架构和现有设备的调整，不影响现有的业务运行。

# 项目工期及交付方式

供应商需在合同签订后，并在用户2021年信息容灾机房租赁项目合同结束之后的三个月内，完成该项目采购清单的建设内容，并交付给用户使用。

本项目租赁期限为2年，以用户确认交付内容的日期，作为租赁结算的起始时间。

# 项目实施要求

1. **实施方案**

本建设项目，需要提供一份详细的设计和实施方案，根据技术参数要求，完成容灾系统、灾备机房设备、云主机等设备的安装部署，要求实施方案符合实际建设需求，确保项目可按时和按质量交付。

1. **实施要求**

用户已在2021年信息容灾机房租赁项目中完成了容灾系统、灾备机房设备租赁、云主机等建设内容，要求该项目的承建商能无缝对接原项目的建设内容，完成数据迁移部署等工作。

1. **建立重大事件应急机制和管理流程**

承诺在发生重大事件时，由供应商项目经理亲自牵头处理，调动供应商一切可调用资源，尽一切努力恢复用户的业务，并协助消除影响。对整个项目进行监督和管理，为实现工期的缩短，提供合理性建议。

1. **突发应急培训**

定期对项目工程人员开展正确应对和处理突发事件的技能培训，培训内容包括容灾系统、灾备机房设备管理、云资源、线路等相关内容。

1. **岗位人员留守**

在节假日期间，如春节、国庆节等，供应商仍保留部分工作人员候命，以应付突发任务的需求，并把名单及联系方式发给用户，办好相关紧急出入手续和保证时刻联系。

1. **跨地域联动协调**

为满足工期的需要，与多方协商简化各种手续，尽量缩短中间流程，供应商承诺储备一些备件做为应对突发任务时的借调用，尽量缩短突发任务完成的时间。

针对项目过程中，有可能出现的突发事件，供应商将根据突发事件处理办法，在最短时间内处理完相关问题。

# 保修服务要求

1. **质保要求**

在租用期内提供硬件和软件7\*24 小时原厂保修服务。

1. **备件更换**

本项目的容灾系统、灾备机房设备、云主机及光纤线路等，在使用过程中发现设备质量问题，投标人需在服务响应时间要求内免费更换。

1. **驻场人员要求**

在合同期内， 供应商提供两名驻场人员，要求计算机相关专业大学本科学历或以上，熟悉Oracal、SQLserver、VMware、网络、机房管理等相关经验，在供应商单位工作1年或以上，工作时间严格按照用户单位要求，并提供7\*24小时响应，节假日安排值班。驻场人员不得随意更换，如必须更换，供应商需提前1个月提交书面申请，征得用户同意之后才能更换。

工作内容包括：

1) 提供7\*24小时，本项目涉及的主机、存储，网络、安全设备、虚拟化平台的日常监控，故障响应。

2) 提供本项目涉及的主机、存储，网络、安全设备、虚拟化平台等软硬件日常运维工作，包括但限于版本优化，软硬件日常巡检，软硬件故障处理，架构优化，安全加固，日常分析，配合完成业务迁移上云等日常工作。

3) 定期向院方汇报灾备机房设备运行状况，提交巡检记录单等。

1. **灾备机房维护人员要求**

供应商应有专门的维护团队，对本项目租赁机房涉及的主机、存储，网络、安全设备、虚拟化平台等软硬件进行日常运维工作，包括但限于版本优化，软硬件日常巡检，软硬件故障处理，架构优化，安全加固，日常分析，配合完成业务迁移上云等日常工作。

须提供不少于6人的固定团队，指定项目经理，提供团队人员名单，与驻场人员共同维护、监控该项目内容。定期向院方汇报租赁机房设备运行状况，提交巡检记录单等。

1. **服务方式**

以现场服务为主，其它电话、邮件指导、远程维护、技术交流方式不限。

1. **服务响应时间**

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **关键控制点** | **衡量内容** | **目标** |
| 服务响应时间 | 现场响应能力 | 工作时间 | 7x24 |
| 紧急故障（系统瘫痪） | 响应时间 | 即时响应 |
| 严重故障（系统性能受损） | 响应时间 | <=10分钟 |
| 一般故障（系统运行正常） | 响应时间 | <=30分钟 |
| 服务周期 | 硬件故障恢复 | 工作时间 | 7x24 |
| 紧急故障（系统瘫痪） | 硬件故障恢复周期 | <=30分钟  超过1小时提供配件备机 |
| 严重故障（系统性能受损） | 硬件故障恢复周期 | <=2小时 |
| 一般故障（系统运行正常） | 硬件故障恢复周期 | <=24小时 |

1. **培训**

供应商应为院方进行容灾系统等相关方面知识培训，包括使用培训和维护培训。

供应商应提出详细的培训计划，提供培训教材。技术培训的内容必须覆盖产品的安装、日常操作和管理维护，以及基本的故障诊断与排错，并保证培训效果。

1. **合同付款方式**

用户将按如下方式向供应商支付合同费用：

1. 合同签订后，用户在收到供应商开具相应金额正式发票后，向供应商支付合同总金额的20%。
2. 供应商在完成项目采购清单的建设内容，并交付给用户使用，经用户签名确认后，收到供应商开具相应金额正式发票后，向供应商支付合同总金额的20%。
3. 项目租用期为两年，从正式租赁时间开始计算，用户在收到供应商开具相应金额正式发票后，每半年向供应商支付合同总金额的15%，最后一次需完成项目验收后才能办理支付。
4. **履约保证金要求**

(一)乙方在签订合同后十个工作日内，应按照招标文件中提供的履约保证金保函格式或甲方可以接受的其它形式向甲方提交履约保证金（合同金额的5%），如现金支付履约保证金的，甲方在项目验收通过后无息退还。如发生违约可从履约保证金中扣除，于质保期满或合同中止后结算。

(二) 若采用银行保函格式提交履约保证金，则银行保函的有效期限应至少保持到合同期满/项目验收；如果项目延期，乙方有责任第一时间办理银行保函延期手续，保证银行保函的有效期限直至项目完成。

(三) 如果乙方没有按招标文件规定签订采购合同并提交履约保证金，则视为乙方自动放弃中标资格，甲方有权没收乙方的投标保证金。

(四) 在乙方按合同要求全部完成规定的本项目建设内容并提请甲方归还履约保证金后，甲方将把履约保证金无息全额退还给乙方；若乙方在完成项目建设内容后没有主动提请甲方归还履约保证金，则从质保期满之日起、三年诉讼时效期满后，视为乙方放弃要求退还履约保证金权利，甲方有权不予退还履约保证金。

(五) 如在质保期内，软硬件及/或服务出现任何缺陷，则应在该等缺陷完全修补并达到本合同要求后，甲方才有义务支付本款对应的价款。同时，甲方有权从履约保证金中扣除乙方按照本合同应当承担的任何赔偿金额。

(六) 如乙方未严格履行本合同义务，在不影响甲方任何其他权利或补救的前提下，甲方有权扣留或推迟支付任何到期款项，直至乙方履行义务或以甲方满意的方式进行补救。

1. **保密要求**

供应商严格遵守国家的经济、技术工作保密规定和人的保密工作条例，对项目实施期间在用户了解的各种情况、获取的全部信息资料等严格保密，不得泄露。对人有特殊保密要求的资料或要求特定人员接触的情况，如果供应商不具备相关条件，则提出具体的技术要求，委托人办理。