**广东省妇幼保健院信息系统容灾备份体系建设项目用户需求书**

# 需求背景

## 医院测评评级背景

《信息安全等级保护》医疗行业是重点对象，需确保并落实数据安全保障各方面的要求。其中根据国家数据安全等保2.0要求，需要对所有的业务系统及数据进行完整的容灾备份，保障数据的安全可靠。要求：本地备份与恢复+异地数据备份存储+业务高可用+定时恢复演练。

《国家医疗健康信息医院信息互联互通标准化成熟度测评方案（2020年版）》中的附件1、医院信息互联互通标准化成熟度测评指标体系的基础设施建设情况 “4.1.2.3医院信息平台具有存储灾备能力的等级要求”中提出“RTO≤24h,RPO≤24h,为四级乙等；RTO≤4h,RPO≤6h，为四级甲等；RTO≤0.25h,RPO≤0.25h，为五级乙等”。

《电子病历系统应用水平分级评价标准（试行）》5级09.04.5要求：（1）对于重点系统具备完整的灾难恢复保障体系，每年至少完成一次应急演练（2）每季度至少进行一次数据恢复验证，保障备份数据的可用性（3）对于重点系统数据与系统的恢复时间不大于2小时，数据丢失时间不超过1天

《电子病历基本规范2017》第十九条规定：门(急)诊电子病历由医疗机构保管的，保存时间自患者最后一次就诊之日起不少于15年;住院电子病历保存时间自患者最后一次出院之日起不少于30年。

《电子病历基本规范(试行)》第十六条第一项规定：具备保障电子病历数据安全的制度和措施，有数据备份机制，有条件的医疗机构应当建立信息系统灾备体系。应当能够落实系统出现故障时的应急预案，确保电子病历业务的连续性。

《医学影像诊断中心管理规范 (试行)》规定：影像资料保存10年以上，至少3年在线，可供快速调阅、浏览和诊断使用。按照卫生计生行政部门有关要求及时上传影像资料数据信息。

## 医疗数据安全背景

随着信息化建设不断发展，我院现有卫健专网、互联网、政务外网、省医保专网等多种网络接入，面对当前层出不穷的新型攻击，医院网络安全环境日趋严峻。广东省内医疗体系均出现过多起非结构化数据因感染勒索病毒导致电子文件全部被非法加密锁定导致不可用的安全事件。

目前广东省妇幼保健院经过多年信息化建设，随着多院区多机房建成使用，其中包括大量核心业务系统，其数据库类型主要为Oracle、SQL Server和电子档案及影像文件数据量有近200TB实现本地备份，随着数据量不断增加和行业监管关于要求保障数据安全及建设异地备份系统。

因数据安全问题十分严峻，迫切需要更加有效的数据备份系统来进行增加的数据扩容保障，并在异地院区信息化机房建立异地灾备；在灾难事故发生时，可以在相对较小的代价，应对广泛的各类事故和灾难，在整体上保障并提升系统的可用性及数据安全性。

## 机房搬迁及数据迁移背景

随着我院信息化的不断发展，业务负荷的不断增加，服务器超出正常负载能力，已考虑我院未来规划做机房搬迁，将机房现有的IT设备，搬迁或迁移至新机房托管，搬迁期间保障数据不丢失，不影响后续业务运行。

一旦搬迁及迁移期间核心业务系统层面故障，数据丢失误删除等逻辑性故障，将会导致与其相关的业务均无法开展，更有可能会出现整体IT医疗系统的全面崩溃，所有业务均无法开展，甚至会造成毁灭性的业务数据永久性丢失。

数据备份、业务容灾是机房搬迁过程中最重要的保障环节。机房搬迁过程中一定要保证服务器和其他相关设备搬迁到新机房后可正常的启动，即使在业务系统服务器不能正常重启的情况下，也需要建立一套快速恢复的容灾备份措施。机房搬迁过程中保障方式是利用大容量的备份服务器进行重要数据的备份，同时采用虚拟化计算资源池搭建核心业务1：1容灾保证，搬迁过程中服务器发生故障无法正常运行，非核心业务通过备份的数据进行恢复，核心业务通过1：1应急容灾切换保障。

因此搬迁期间需要考虑数据的有效性、安全性、完整性。建设满足现在我院医疗单位业务迁移和搬迁保障需求，提供一种智能的、一体化的、适应各种应用场景的业务迁移和搬迁场景的容灾备份保障方案。

# 项目需求

## “容灾机房”建设需求：

灾备机房是我院实现业务连续性的重要数据中心机房，需要具有数据备份和灾难恢复所需的网络通信、网络安全、计算算力等资源。

**番禺院区与越秀院区网络建设需求：**

应根据当前医院网络情况进行全面的规划设计，采用全冗余架构和SDN技术、裸纤等技术对两院区网络进行融合，实现万兆主干，千兆到桌面的目标，在一套管控平台上对院区网络和数据中心网络进行业务配置与管理运维，对端对端的网络业务进行部署配置，可适应业务系统的频繁调整，同时在性能上应至少能够满足未来5~10年的业务发展需求。

**越秀院区网络安全建设需求：**

整体网络安全防护建设需要满足《网络安全等级保护技术2.0版本》和《医疗行业信息安全技术健康医疗数据安全指南》等相关法律法规，在越秀院区的网络防护体系上进行完善。需分别在数据中心、外联区及互联网区部署防火墙实现安全区域划分；部署日志审计、上网行为管理等设备，便于信息追踪、风险防范和审计取证；在老院区部署态势感知系统探针，数据上传至态势感知分析平台，实现主动威胁识别；对终端杀毒系统及服务器虚拟化安全系统进行扩容。

**越秀院区计算、存储资源建设需求：**

越秀院区新建灾备系统必须与现有业务应用系统完全兼容，最大限度保护现有信息化投资。现有业务系统基础设施FCSAN架构部分包括HIS系统数据库主备服务器、服务器虚拟化集群及存储阵列，服务器虚拟化承载医院除HIS外LIS、EMR、PACS等大部分业务系统。

越秀院区灾备架构基础设施应满足HIS系统及绝大部分虚拟机的在线容灾支撑需求，如采用传统物理机方式部署，存在单点故障，新建灾备系统需合理考虑架构冗余，采用3节点超融合集群，实现关键业务系统的异地容灾，初期目标应实现核心数据库的实时复制，即RPO<1秒，RTO<10分钟；应用服务器通过一定的技术手段实现RPO<1秒，RTO<15分钟的目标。

**越秀院区数据安全建设需求：**

数据安全是越秀院区灾备一体化项目的基本需求，在项目建设整个生命周期中，需要确保数据的安全性不受影响。现有院区数据中心架构复杂，涵盖数据库高可用集群、服务器虚拟化、超融合集群等基础设施，承载医院HIS、EMR、LIS、PACS等数十个业务系统，对应的物理服务器及虚拟机达到一百余台。在方案设计时应谨慎周密，确保现有系统容灾到新建灾备数据中心后数据百分百安全，还要考虑清楚同步过程中数据增量问题，以及出现异常问题后的保障机制。

## “容灾计算资源池”建设需求：

为了保证主中心业务平台容灾接管需求，至少提供144物理核、3TB内存、480TB裸硬盘存储空间来满足容灾接管业务运行的需求，并且需要保证容灾接管平台接管业务后相关业务的高可用性和数据安全性，需要提供计算虚拟化、网络虚拟化来保证接管业务平台的高可用性，需要提供存储虚拟化，包括快存储、文件存储、对象存储等，来满足不同业务的接管需求，同时，需有云管平台、租户、裸金属管理等，来满足平台分权管理与隔离的需求。

考虑未来国产化需求，虚拟化平台须支持 ARM、X86 和 Mips 等 CPU 架构体系，同一管理平台下可同时支持接管理 ARM、X86 和 Mips 等异构计算资源。提供至少3种国产化芯片互认证证书。

## “数据备份与恢复”需求：

番禺本地数据中心建设有本地备份，但现有的备份平台已投产使用近三年，其软件架构已做迭代升级，并需要适应未来建设的灾备集中统一式管理平台，迫切需要对本地备份软件系统进行升级改造。

并根据等保三级“8.1.4.9 数据备份恢复”建设指导意见，利用越秀院区机房作为异地备份机房，并将番禺院区重要数据和系统备份到越秀机房，保障基础数据安全。

本院已在之前上架部署完成了业务数据本地备份机制，保障了部分核心业务的安全运行。但由于业务数据量的剧增，目前本地容灾设备容量、软件版本已无法满足正常的业务需求。

目前情况统计如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **位置** | **备份相关设备** | **关键数据备份** | **生产数据量** | **目标规划备份设施容量** | **备注** |
| 番禺院区 | **已建1台备份一体机** | File、DB、VM、OS  物理机41台  虚拟机77台 | 200T | 50T可用备份空间  200T磁带空间 | 原已有备份设备从原有30T扩容至50T及升级备份系统架构 |
| 越秀院区 | **规划1台备份一体机** | - | - | 150T可用备份空间 | 新建设 |

**番禺院区备份设施扩容升级需求：**

对原有已部署的备份一体机上扩容全新原厂硬盘，扩容至50TB可用容量软件授权许可。扩容完成之后，需确保对系统稳定性、性能无影响。原有备份数据零丢失，停机时间控制在1小时以内。

对原有已部署的备份一体机需免费升级为最新备份架构版本，免费开发对接新购置灾备一体机平台，实现数据复制到备份中心，进行统一存储，作为异地数据中心的数据备份副本存放。提供备份集中管理，并支持远程复制策略的统一管理。

**越秀院区备份设施功能建设需求：**

文件系统保护：支持Windows、Linux等平台下的文件系统定时备份与恢复。

操作系统保护：支持对Windows和Linux平台进行定时备份与恢复。

数据库保护：支持对Oracle、SQL Server、MySQL等主流数据库以及人大金仓、南大通用、达梦数据库等国产数据库进行定时备份与恢复。

虚拟化平台保护：支持对VMware、Hyper-V、Huawei FusionCompute、H3C CAS、深信服等主流虚拟机进行备份与恢复。

NAS存储数据保护：支持对于NAS存储中的数据进行定时备份与恢复。

数据离线归档：针对已完成备份任务，提供定时数据离线归档任务，可根据实际需求自定义归档策略，将备份数据归档到磁带设备中，实现离线备份。

数据传输与加密：支持提供AES256、SM4多种高级加密算法，在数据传输和存储过程中，对于所有备份任务所产生的备份数据进行加密处理，确保备份数据安全。高级加密标准算法能避免数据泄露等安全问题，备份数据在传输和存储过程中将被加密，即使有人通过抓包等方式在数据传输过程中恶意截获备份数据，也将无法解析备份数据。如果有人试图通过插拔磁盘解密磁盘中的备份数据，当进行磁盘数据读取时，将无法解析磁盘中的数据。因而通过传输和存储加密，能够避免企业因为数据丢失或泄露所导致的业务损失等问题。

## “备份数据离线归档”需求：

备份数据是勒索病毒防护的最后一道防线，并对所有关键数据进行定期离线归档备份。在数据长期保存方面，应与备份系统同步建设归档存储设备，可满足备份数据的可离线归档，应支持的归档存储设备包括：光盘库、磁带库等设备。在原始备份数据丢失或遭到破坏的情况下，利用磁带库数据把原始备份数据恢复出来，使业务数据能够恢复系统能够正常工作。以下是磁带库建设需求：

1．需求大存储容量。由于磁带库中可存放多盘磁带，因此磁带库的在线容量为n倍的单盘磁带容量。本次至少需要200T物理磁带存储空间。同时需求对一个或多个备份作业其数据量大于单盘磁带容量的情况来说，能够实现自动换带，不需要系统管理员来人工更换磁带；同时磁带库的大容量加上磁带的轮换使用，使用户在几个月甚至一年内不需要打开磁带库的门来更换磁带。

2．需求速度快。至少需要配备LOT 7磁带，因此数据备份、恢复、查询速度相应提高了数倍。提高磁带库的可用性。

3.全自动操作。结合专业备份软件，通过高级备份功能，把电子病历、PACS 影像等数据备份到本地备份系统内置空间后，定期统一归档一份到磁带库中，实现数据的异地归档保留，可实现异地保护及恢复数据，充分满足现有法规要求。

4.备份数据更安全。由于磁带库有机械锁和软件锁双重保护，使不相关的人员根本无法接触到磁带，从而确保备份磁带的安全性。同时由于减少了人工磁带管理工作，避免了磁带搞混、丢失或错误处理。

## “主机容灾”需求：

我院信息化业务运行除HIS等核心数据库外，还需要依靠大量外围设备作为服务支撑。其中涉及41+台物理机，77+台虚拟机。一提供非结构化数据做支撑，主要涉及FTP、附件、文档等数据。二提供应用环境，主要涉及中间件服务支撑，业务软件安装在不同的存储设备中，安装环境架构复杂、文件多、目录结构深、海量小文件多。三提供轻量级数据库环境，超声、电生理、手术麻醉、病理、固定资产管理、财务管理等均需要独立数据库。

主机容灾备份需求：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **位置** | **相关设备** | **关键数据备份** | **生产数据量** | **目标规划设施容量** | **备注** |
| 番禺院区 | **-** | File、DB、VM、OS  物理机40台  虚拟机76台 | 37T | - | 两地带宽10G |
| 越秀院区 | **规划1台CDP一体机** | - | - | 60T（可用空间） | 新建设 |

1.基于整机完整性实时的数据备份，可以保证应用服务器任意时刻I/O级别的数据安全，数据恢复后可立即作为第二生产中心应急使用，支持基于P2P、P2V、V2V、V2P的应急、恢复，从应用程序服务的角度，提供磁盘镜像、数据副本、IO日志、远程复制以及自动化数据恢复等全面的数据恢复功能，帮助信息科管理人员达到异构环境中的业务保护需求，并为实现业务连续性提供可靠方案。

2.可以对所有的业务系统进行保护，建立相应的磁盘备份任务，设置备份策略、备份计划，根据不同数据安全需求制定不同作业计划；在制定了实时或定时备份任务后，会在在指定时间发起备份命令，将生产数据压缩加密，将数据传给数据备份设备。

3.直接式数据恢复，实现服务器操作系统、应用软件、数据库、文件的一键式快速恢复，大幅减少业务中断时间，保障业务连续性。同时恢复时自动识别目标硬件/虚拟化平台的PCI设备，并虚拟化此PCI硬件，动态注入对应的驱动到操作系统中，让操作系统能在新的硬件配置上正常启动。

4.当生产中心业务系统因为各种灾难导致出现宕机、数据丢失、文件破坏，造成业务中断时，本地灾备系统可即时启动接管功能，可以将故障系统在数分钟内通过内置虚拟机应急接管功能即时恢复至故障前状态，最大限度地保障业务连续性，减少数据丢失。

## “数据库容灾”需求：

我院除HIS、EMR有采用双服务器双活存储组建数据库集群（如Oracle RAC）方式，虽然能够一定程度上抵御硬件故障，但以下几个问题无法有效应对：

1.防范一些大型灾难故障，比如停电、着火等。

2.防范逻辑错误，一旦数据库内部发生故障，利用数据库日志或备份点恢复数据。

考虑到HIS、EMR等是医院最核心、实时性最高的业务系统，因此在有集群等高可用的基础上，HIS和EMR应配有独立完整数据的应急服务器作为备用容灾节点，其余的ODS、CDR、LIS、PACS等核心系统同样需要相关容灾措施建设。对不同业务进行规范统一的容灾同步集中式管理，现有数据库“容灾”需求：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **位置** | **相关设备** | **关键数据** | **生产数据量** | **规划设施容量** | **备注** |
| 番禺院区 | **-** | HIS数据库  EMR数据库  集成平台ODS库  集成平台CDR库  临床工作站库  LIS数据库  PACS数据库  统一授权管理库  ESB服务总线库 | 30T | - | 两地带宽10G |
| 越秀院区 | **规划3台超融合一体机**  **规划1套数据库同步软件** | 建设不少于9台数据库虚拟机  建设1台数据库同步管理平台 | - | 30T | 新建设 |

1.容灾中心需建设在异地越秀院区机房，当生产中心业务系统因为各种灾难导致服务器、存储设备、交换机等其他设备损坏业务系统无法访问时，容灾中心完全独立的1：1数据库系统能够在5-10分钟内完成整个业务数据库系统，包括数据库启动停止的一键式接管，同时还要自动配置好相应的网络环境，确保用户能够直接访问容灾中心的业务数据库系统，从而实现数据库业务的快速恢复。

2生产系统和容灾系统之间形成可以相互切换，相互恢复的容灾关系，生产系统出现异常或计划内维护时，生产系统可以简单的切换至容灾系统，容灾系统替代生产系统提供服务；生产系统硬设备复原之后，容灾系统初始化后可以回切至生产系统。

3.容灾系统需具历史状态回退。对于业务系统因为中病毒／人为误删／误改导致的数据丢失可以在容灾系统中找回历史状态时间点，可对整个容灾系统回退到指定时间点，因逻辑性故障导致业务中断问题。

4.建设后容灾数据库为可读模式，后续我院查询业务转移至容灾库进行。

## “数据防勒索”需求：

考虑数据灾备方案的同时，亦需要考虑数据存放安全问题。当其对文件、数据加密和修改时，往往是无法恢复，只能就范或舍弃数据，导致医院损失重大。容灾端数据库作为最后一道防线，其底层数据文件需要保障完整可用。否则整个容灾系统形同虚设。

容灾端数据库系统需要采用独特的底层白名单技术，对文档、数据库文件进行主动防护，确保只有被允许的合法操作才能被执行，一切未被允许的操作都被禁止，避免勒索病毒对文件的加密和修改。即使业务系统未及时安装补丁，也可防止漏洞被利用进行勒索加密。这样即使有新的勒索病毒出现，容灾端数据库也可以全面无忧的防范新病毒的攻击，从根本上避免勒索病毒加密。

1、容灾数据库文件保护

容灾端数据库防勒索需求要提供数据库文件自动保护机制，将数据库各格式的文件加入保护列表，在保护列表的文件只有经过授权的应用程序才能进行更新，如Oracle文件只能被Oracle写入更新。数据库保护是防勒索保护中的重要内容，针对数据保护，容灾端数据库防勒索内置数据库文件保护引擎，使数据库文件免受勒索病毒的加密和删除，目前支持Oracle、Sql Server、Mysql、DB2等主流数据库。

2、数据库主机保护

目前容灾环境是数据库主机提供服务。数据库主机作为容灾应用程序、数据库程序运行的载体，部署完成投入使用后仅运行特定的应用程序，除了程序升级外，不需要安装新的应用程序。针对此种使用场景，容灾端数据库匹配设置堡垒模式，在堡垒模式下，禁止任何新的程序在数据库主机上运行，包括勒索软件、已知勒索病毒、未知勒索病毒、挖矿病毒等。

## “灾备集中管控运营管理”需求：

业务连续性管理对于医院是最核心的容灾建设目标，本次项目我院要建成以RTO为目标的容灾运营管理体系。具体实现以容灾集中管控平台为中心，能够将本院涉及业务系统相关的灾备技术实进行现统一集中管理，实现以下核心功能目标：

1.为保证相关容灾备份设施建成后，有相应的闭环管控，实现灾备集中、高效管控，减少灾难发生时人工处置时间，提高灾备RTO。灾备集中管控中心需要支持但不限于本期建设的备份系统、CDP主机容灾系统、数据库容灾同步系统。同时需支持开发对接第三方灾备管控，如原生数据库容灾技术纳管（Oracle DataGuard、SqlServer alwayson、MySQL Replication、DB2 Hadr、Redis 主从集群、MongoDB 主从、达梦数据守护集群、Informix HDR）、虚拟化平台Vmware纳管、Veeam备份纳管、NetBackup备份纳管等。由投标人承诺解决，并在标书中提供承诺函。

2． 对灾备资源进行实时运行状态监控、告警；

3． 根据本院业务流程进行容灾资源的灵活编排，以满足不同场景、不同业务、不同层次的容灾预案管理需求；

4． 在不影响业务的情况下能够安全高效地进行容灾演练，制定规范的演练流程、根据应对不同灾难风险随时开展桌面演练，检验容灾系统的可用性、完整性、可靠性、RTO目标；

5． 在业务发生故障时能够一键进行容灾切换，将故障业务快速切换至备机继续提供相应服务，实现自动化、流程化、高效地灾难故障应急响应，保障业务的连续性；

6． 通过容灾集中管控平台提供容灾集中监控大屏、容灾应急切换指挥大屏让容灾应急管理指挥状态可视、过程可见、高效指挥。

## “灾备预案编排”服务需求：

**服务简介**

含10人天现场，提供资产梳理、脚本编写、预案编排、计划演练保障等服务。

**服务内容**

容灾编排是灾难恢复计划的核心部分，涉及到在灾难发生时如何快速、有效地恢复业务系统。为了实现这个目标，供应商应提供“灾备预案编排”服务，例如备份策略、数据复制、恢复流程、人员培训等。帮助管理人员更好地了解恢复流程和备份策略，从而优化灾难恢复计划。此外，还需要对相关人员进行培训，以确保我院相关人员具备必要的技能和知识，从而在灾难发生时能够有效地执行恢复流程。

在资产梳理方面，供应商在前期现场参与调研了解的业务系统，包括系统架构、数据存储、备份策略等，并对现有的IT资产进行全面的盘点和记录。确保在灾难发生时，能够快速定位并恢复关键资产。

在脚本编写方面，供应商根据业务恢复流程编写详细的脚本，包括业务恢复预案脚本等。这些脚本会在灾难发生时自动执行，从而快速恢复业务系统。

在预案编排方面，供应商制定详细的灾难恢复预案，包括恢复流程、恢复点目标、恢复时间目标等。确保预案的合理性和可操作性，以确保在灾难发生时能够快速执行预案。

在计划演练保障方面，供应商提供定期的计划演练服务，以确保恢复流程的顺畅和有效。在每次演练后提供详细的报告和分析，以便了解演练结果和改进方案。

综上所述，供应商需提供容灾编排服务，确保在灾难发生时能够快速、有效地恢复业务系统。

## “数据迁移”服务需求：

**服务简介**

提供所有需迁移的核心数据库的迁移工作，工作内容包括：项目系统调研，制定数据库迁移方案，操作系统参数优化，数据库软件安装，模拟迁移及正式迁移和迁移后的保障工作。

**服务内容**

此次数据迁移服务，涉及番禺院区业务及应用系统，从旧物理服务器上迁移到新生产虚拟化系统上。同时,还需要在系统迁移后，对访问系统的客户端进行调试，确保各个客户端能够正常访问系统。

“数据迁移”服务要求，对迁移到新主机上的数据及环境进行可用性测试，功能性测试、集成测试，性能测试、稳定性测试，并对有问题的地方进行初步优化，进行模拟的切换测试，保证数据顺利割接。

1) 测试脚本撰写、测试用例、测试数据、测试报告：迁移实施方、应用开发商应一起对被迁移的应用系统创建测试用例和测试脚本，选择合适的测试数据和测试样例，确认迁移数据在系统迁移到云平台环境后的有效性，进行有计划的测试。迁移实施方应和应用系统开发商执行测试脚本，并在测试结果基础上生成报告

2) 功能性测试：功能性测试对云平台的业务应用系统进行功能性测试，并与原服务器进行对比，确保应用系统在平台迁移后所有功能工作正常，可采用手工测试或者自动化测试工具。对于迁移后应用系统，重点测试新环境下对应用业务的影响，可不过多的进行业务逻辑性测试。对于新的业务系统，需要进行完整的业务逻辑性测试。

3) 性能测试：在测试云平台的性能测试中，主要采用压力软件在压力机上对应用系统进行压力测试，或者采用人工脚本进行压力性测试，从而衡量应用系统对主机的资源消耗及由此产生的对物理机的资源消耗从而更好的掌握应用系统的性能需求，验证云平台是否能满足业务系统的性能需求。性能测试可在验证环境平台进行，如测试云平台条件满足也在进行相关测试。

4) 稳定性测试：在稳定性测试中，可以利用一些压力工具软件(如Loadrunner等)进行压力测试，在一定周期内测试系统的稳定性，以保证应用系统在割接后能稳定运行。稳定性测试可在验证环境平台进行，如测试云平台条件满足也在进行相关测试。

5) 系统优化：对测试过程中发现的系统问题，进行系统优化，达到比较优化的运行状态。一些小的可使系统更优化的调整或配置可由操作员决定，每个参数调整需进行详细记录，大的调整或者重新配置需提交项目组进行审议后再决定；

6) 系统调优中，建议考虑如下因素：在系统优化中，应从全局出发，进行通盘考虑；从整体考虑资源组的资源保留情况，整体考虑资源组内的虚拟机的资源保留和竞争情况；充分利用性能测试结果，找出系统性能的短板，从物理基础架构和虚拟基础架构两个层次进行调优；

7) 模拟迁移,使用新数据进行一次模拟的迁移演练，预估整个切换所需要的时间，排除切换过程中可能存在问题，对于不满足要求的部分重新修改方案或调优一直到满足预定要求为止。

8) 回退方案：整个迁移过程都不改动原生产系统上的数据和硬件架构，迁移出现意外故障的时候可以迅速切换回原生产数据库继续运行。

## “容灾数据库优化”需求：

**服务简介**

提供数据库监控工具，针对数据库实现智能监控、容量预测和性能分析能力，支持资产发现、监控告警、智能巡检、容量分析、性能诊断、SQL审核等数据库日常运维场景。

**服务内容**

结合日常检查、容灾库巡检、灾难演练和客户重大事件，提供容灾数据库优化评估服务，并给出数据库系统性能调优工作方案。针对当前数据库运行情况以及收集的性能信息提出系统各项性能参数配置合理调优或硬件扩容建议，经商讨评估后，对数据库系统各项性能参数配置进行合理调优。

主要针对以下展开：存储空间分配和发展，表格和索引空间分配和增长规律，CPU负载分配和增长规律，内存负载分配和使用规律，连接资源变化分析，更新变化规律，进程使用分配以及增长规律等等主要数据库系统资源的检查和规划。

结合当前数据库系统的最新补丁情况、生产库补丁情况，从而提供容灾数据库最安全可靠，适合的补丁安装服务以及相关现场支持服务。明确升级需要的条件、升级时间、业务停止时间、升级技术、风险、数据一致性、回退措施等，协助用户选择最适合的容灾库升级方案。

提供专业数据库运维监控工具，实时监控容灾数据库运行状态，提前感知运行风险，智能定位问题，并利用工具箱快速解决故障。可通过告警平台，实现主动运维服务，有效保障容灾数据库系统的持续稳定运行。

利用专业数据库运维监控工具可有效提升对容灾数据中心的自动化运维水平，实现对容灾数据中心的主动运维服务。主要功能包括：

（1）容灾数据库智能化监控和巡检。

（2）容灾数据中心一体化监控。

（3）利用告警平台实现告警订阅、工单管理等。

（4）大屏展示，可自主定制运维视图，实现运行状态可视化。

## “容灾库特权账号管理”服务需求：

**服务简介**

提供容灾数据库账户检测功能，定时从权限、状态、最近登录时间等维度检测数据库内用户，并根据内置规则，统计整、异常用户数量并给出不同风险等级分类，对容灾数据库内用户情况做清晰明确。

针对容灾侧操作系统账户支持修改密码操作，方便用户统一管理账户。

针对容灾数据库账户支持修改密码和锁定操作，方便用户统一管理账户。

**服务内容**

按照安全监管要求，提供容灾端数据库账户的创建、修订、赋权等操作，并提供容灾端主机账户、数据库账户的批量改密操作。日常使用容灾端数据库的过程中，涉及开发、测试、运维、应用等人员，因各种需求在容灾端数据库内新建数据库用户。针对此场景，统计异常用户数量并给出不同风险等级分类，对大权限账户、过期状态账户态和长时间未登录账户等进行安全检测，并给出检测报告。

供应商需要新建、修改现有数据库用户权限以及其他数据库变更工作时，有义务根据实际场景要求，在数据库中做相应的权限新建、授权和收回等调整。

## “操作系统及数据库”正版化需求：

**服务简介**

本次容灾建设所涉及相关的商业化操作系统、数据库软件等保证均为正版，以确保容灾数据库的数据的安全性、可靠性和稳定性，避免因为使用盗版软件而带来的法律风险。

**服务内容**

涉及商业化操作系统、数据库软件等，选用官方授权和正式发行的操作系统，以确保系统的稳定性和安全性。应从官方渠道购买操作系统，并确保使用的版本是正版。

确保操作系统软件的来源合法和合规。供应商采购操作系统时应选择官方认可的渠道，并遵守相关法律法规和许可协议。

实施严格的安全策略，包括更新和补丁程序，以保护操作系统免受漏洞和病毒的攻击。正版操作系统通常提供官方的安全更新和补丁程序，应被及时应用。

采用官方授权和正式发行的容灾数据库软件，以确保数据的完整性和可靠性。容灾数据库应使用与主数据库相同的正版软件，以避免潜在的漏洞和安全风险。

确保数据库软件的来源合法和合规。供应商采购数据库软件时应选择官方认可的渠道，并遵守相关法律法规和许可协议。

建立完善的服务支持体系。选择提供正版操作系统和数据库服务的供应商应能够提供及时的故障排除和技术支持，以确保系统的稳定运行。

遵循法律和道德规范。使用非正版操作系统和数据库不仅违反法律规定，还会对软件开发商和其他合法使用者造成经济和法律风险。在任何情况下，供应商都应坚持使用正版软件，维护良好的行业生态。

## 灾备服务要求：

**1.“每月灾备巡检”服务需求：**

**服务简介**

每月提供灾备产品的现场巡检服务，保障系统的正常稳定运行，交付产品巡检报告，包含产品硬件巡检；

**服务内容**

提供每月一次现场灾备相关设施例行检查服务，内容涉及到容灾系统、备份系统、灾备网络、容灾应用、容灾数据库的方方面面，主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。巡检工作由现场检查和页面日志分析构成，提供一份内容详尽的灾备巡检报告。

通过巡检可以了解灾备系统运行情况、解决灾备系统使用中存在的问题、进行灾备系统健康检查、收集灾备系统性能信息等，并按照出具灾备系统检查报告，指出灾备系统运行隐患，提出对策建议并在用户的认可下实施，并出具故障修复报告。

**2.“每季度备份恢复校验”服务需求：**

**服务简介**

每季度提供原厂工程师现场数据恢复演练1次服务，交付季度数据恢复报告

**服务内容**

提供数据备份恢复验证，技术服务团队需精通灾备技术，能快速恢复各种灾难性故障。熟悉我院的备份机制和模式，利用备份机制实现快速故障恢复。

数据恢复测试服务主要是为了验证日常备份数据的有效性，实现流畅的恢复流程，把握准确的恢复时间，并以此为依据来重新评估调整备份系统的备份策略和数据恢复测试流程。

**3.“每年灾备演练”服务需求：**

**服务简介**

每季度提供原厂工程师现场容灾切换演练1次服务，交付年度容灾演练报告

**服务内容**

提供容灾演练，演练之前预留故障模拟时间。待正式切换开始后，进行应急响应、应急容灾切换等各项工作，并做好时间记录，按演练步骤逐个填写演练记录表。

应急系统演练主要包括应急切换决策流程、切换前消息发布、切换指标的达标情况、切换之后的业务测试、应急回切时间、应急回切后数据一致性测试、应急回切后正式业务完成性测试、自动化平台等内容，演练完成需要提供数据库容灾演练报告。

# 项目内容

## 数据备份建设内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **位置** | **产品** | **配置描述** | **数量** | **备注** |
| 番禺院区 | 备份一体机软件扩容 | 升级扩容至50T可用容量授权 | 1项 |  |
| 备份一体机硬件扩容 | 12T 7200转 高容量SATA | 4块 |  |
| 备份一体机升级 | 原有备份系统升级，实现集中管控，支持异地远程复制功能 | 1项 |  |
| 磁带机 | 驱动器LTO Ultrium 7 半高\*1  8Gbps 光纤通道，配置1条光纤线 | 1台 |  |
|  |  |  |  |
| 越秀院区 | 备份一体机软件 | 【数据备份模块】支持常规数据库等主流DB备份，支持虚拟化无代理备份，支持x86环境文件备份，支持差异/增量/全备模式，含150T可用容量无限制主机数据备份功能授权；D2D2T备份授权许可，实现将备份数据离线归档到磁带库 | 1套 |  |
| 备份一体机硬件 | 4U机架式，8000（1+1）冗余电源，一颗64位八核十六线程处理器，内存32GB，24个热插拔盘位，12块16T SATA 7200企业级硬盘，2块2400G SSD系统硬盘，提供2个千兆以太网接口，2个万兆以太网接口，2个光纤16GB FC接口。 | 1台 |  |

## 灾备一体化平台建设内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **位置** | **产品** | **配置描述** | **数量** | **备注** |
| 越秀院区 | CDP主机容灾 | 采用磁盘级I/O复制技术捕获磁盘数据块变化，将应用环境和数据整体打包备份，不区分数据库，文件，操作系统等数据类型，通过主机级数据同步，实现对整个业务环境和数据的实时备份保护。  含60T可用容量无限制主机数据实时保护功能授权；无限制节点容灾接管授权。 | 1套 | 主机容灾 |
| CDP主机容灾硬件 | 2U机架式，550（1+1）冗余电源，两颗64位十六核三十二线程处理器，内存1TB，12个热插拔盘位，8块12T SATA 7200企业级硬盘，2块240G SSD系统硬盘，提供2个千兆以太网接口，2个万兆以太网接口。 | 1台 |
| 硬盘不返服务 | 客户硬盘损坏保修期内不返还 | 3年 |  |
| 超融合一体机 | 本次采购需提供3台超融合服务器，每台服务器配置要求如下：  CPU：2路Intel gold 5318Y 2.1G 24C CPU  内存：提供≥32条32G DDR4 内存条  系统盘：提供≥2块480G 2.5 SATA SSD  缓存盘：提供≥2块1.6T NVME SSD  数据盘：提供≥10块16T HDD硬盘  阵列卡：提供1块阵列卡，支持raid1、JBOD  提供≥4口万兆光纤网卡(含模块)，≥4口千兆RJ45网卡  标配冗余电源、风扇、导轨 | 3台 | 考虑数据增长冗余 |
| 数据库容灾 | 搭建1:1的数据库容灾。支持内存、存储的数据同步复制和灾难切换基本功能，同时支持桌面演练、活动站点、误操作恢复功能。满足我院所有核心系统容灾侧数据库实例授权。 | 1套 | 数据库容灾 |
| 防勒索加固 | 防勒索系统精确识别保护文档的操作者，防止敏感信息文档被加密，保护容灾服务器的数据库文件，支持web界面策略配置及下发、设备监控、日志收集及分析功能，有效阻断已知和未知勒索软件的攻击。功能项：  1.基础功能：进程防护、诱捕、报表等  2.服务器：默认包含9台以上数据库服务器防勒索授权 | 1套 | 容灾库防勒索 |
| 灾备一体化平台 | 灾备一体化平台要求实现灾备状态可感知、灾备能力可订购、灾备演练可掌控、灾难切换可指挥，充分保证业务连续性和数据完整性，具有强兼容性，实现所有灾备资源的统一纳管。  【管控中心】对不同类型的灾备技术实现集中管控，支持灾备运行状态监控、预案编排、预案评估、容灾演练和灾难切换等功能。包含50个灾备管控资产授权。 | 1套 | 灾备集中管控 |
| 编排梳理服务 | 含10人天现场，提供资产梳理、脚本编写、预案编排、计划演练保障等服务 | 1次 |  |
| 数据迁移 | 提供核心数据库（不少于9个）的迁移工作，工作内容包括：项目系统调研，制定数据库迁移方案，操作系统参数优化，数据库软件安装，模拟迁移及正式迁移和迁移后的保障工作。 | 1次 |  |
| 产品巡检服务 | 提供所有灾备产品的巡检服务，保障系统的正常稳定运行，提供产品巡检报告 | 1年4次  共三年 |  |
| 数据恢复演练服务 | 原厂工程师现场数据恢复演练服务 | 1年4次  共三年 |  |
| 容灾演练服务 | 原厂工程师现场容灾切换演练服务 | 1年4次  共三年 |  |
| 数据库监控优化工具（含特权账号管理） | 提供专业数据库运维监控工具，实时监控容灾数据库运行状态，提前感知运行风险，智能定位问题，并利用工具箱快速解决故障。可通过告警平台，实现主动运维服务，有效保障容灾数据库系统的持续稳定运行。  通过用户权限检测工具，分析用户权限并检测存在安全风险的账户，通过批量改密工具。 | 1套 |  |
|  | 容灾机房建设服务 | 提供容灾机房搬迁服务 | 1项 |  |
| 产品维保服务 | 原厂维保服务 | 以上产品提供三年原厂服务 | 1项 | 均需提供原厂服务承诺函 |

# 服务要求

## 响应供应商资格要求：

1. 参加本项目的响应供应商必须是具有独立承担民事责任能力的在中华人民共和国境内注册的法人；
2. 本项目不接受联合体参与。

## 实施要求：

详细实施进度要求如下：

项目总建设周期为签订合同后 6 个自然月完成所有工作。

项目交付地点：医院指定地点。

## 服务团队要求：

要求项目团队成员具备良好的数据库技术支持能力以保障灾备系统的建设实施及顺利运行，原厂服务团队成员具体要求如下（要求提供相关证书和社保复印件备查）：

1、项目经理同时具备PMP和OCM；须具备3个以上的容灾备份相关项目经验，提供相关简历及项目合同证明。

2、实施工程师需具备Oracle OCP、MySQL OCP、CISSP、高级数据库管理工程师（工信部、职称职业鉴定），提供相关资质证明。

3、配备数据库支撑顾问2名，需具备Oracle ACE认证、PostgreSQL ACE认证，提供相关资质证明。

## 售后服务要求：

1、供应商需按照我院要求提供投标产品的实施、安装、调试、部署、派送、培训以及各设备软件之间集成、常态化配置维护等服务，确保产品可以投入正常实际使用。

2、供应商负责服务工具的系统软件升级、更新。供应商需要根据与我院的约定定期（合同签订时确认）对合同购置产品免费进行必要的软件更新（包括操作系统、备份软件等）和版本升级。当我院准备对合同产品进行升级或扩容时，供应商须提供咨询服务，并提交相关方案，并提供升级后的测试报告。

3、培训要求。为使掌握系统，熟悉基础故障的处理方法，减少系统问题的出现，保证工作正常开展；供应商提供对本项目的技术培训，采用理论培训与现场培训相结合的方式进行培训，培训时间由供应商和我院在签订合同时协商决定。

4、合同质量保证期。质保期内对医院所供货物实行包修、包换、包退、包维护保养；质保期内，如设备或零部件因非人为因素出现故障而造成短期停用时，则质保期和免费维修期相应顺延，如停用时间累积超过60天则质保期重新计算。

5、对售后服务期内供应商承诺提供免费和完善的技术支持。承诺遇到应急救灾、故障或缺陷时能迅速响应并在2小时内提供完善的解决方案，且能派足够的技术人员同时达现场协助客户并解决问题。

6、供应商为产品保修第一响应方，在保修期开始时向我院提供售后服务联系方式。联系方式包括但不限于供应商售后人员的联系方式和原厂售后联系方式。原厂商需要协助供应商为产品提供保修服务。

7、供应商提供现场7×24小时的响应。按医院通知：工作期间（正常工作日8：00-18：00）故障响应时间不超过0.5 小时，到达现场时间不超过1 小时；非工作期间（正常工作日0:00-8:00、18:00-24:00及节假日）软件故障响应时间不超过1 小时，到达现场时间不超过2 小时；并于4小时内排除故障，保证系统正常运行。

8、供应商必须做好系统环境的维护，主要防止因操作系统故障或系统配置故障影响用户正常使用。

## 培训服务要求：

（1）从合同签订开始，实施厂家相关技术人员免费对所有科室骨干进行分期、分批的各种容灾技术培训。根据不同专业、不同管理要求对科室负责人及所有上岗操作使用人员进行系统主要功能、系统操作使用方法、系统工作流程培训。通过培训，使他们较好的掌握应用软件的使用方法，熟悉系统工作流程，基本达到了操作准确、及时、迅速的要求。

（2）培训对象包括信息系统管理员、信息科管理人员、信息科运维人员(技术员)等。

（3）培训计划：包括容灾一体化系统管理员的培训、操作骨干的培训和操作人员的培训方法和内容。

## 验收要求：

（1）供应商提供详尽的系统运行方案。系统运行分为试运行、正式运行、稳定运行及系统移交等步骤。

（2）试运行期满且系统运行正常后，供应商需按合同所列标准，向院方提供完成验收报告及相关资料，包括但不限于本合同涉及的全部有关产品说明书、原厂安装手册、技术文件、资料及安装、测试、试运行合格报告等文档，汇集成册一式二套交予采购人（包括纸质版和电子版）。

（3）初次运行期内灾备安全运营技术支持工作，提交初次运行情况总结报告。

（4）院方收到供应商提交的验收报告及相关资料后 5个工作日内组织有关单位验收，并在验收后 5个自然日给予认可或提出修改意见。供应商应当按修改意见进行修改，并承担由自身原因导致再次修改的费用。