ICS 35.240.99
CCS L60

T/GYJS

团　　体　　标　　准

T/GYJS 013—2025

区域医疗混合云异构多云纳管技术规范

Technical Specification for Regional Medical Hybrid Cloud Heterogeneous Multi-Cloud Management

2026－01－28 发布　　2026－02－01 实施

广东省云计算应用协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由暨南大学附属顺德医院提出。

本文件由广东省云计算应用协会归口。

本文件起草单位：暨南大学附属顺德医院、广东慧云科技股份有限公司、佛山市顺德区中西医结合医院、广东医科大学顺德妇女儿童医院、广州市番禺区卫生健康局、顺德区第三人民医院、佛山市顺德区第四人民医院（佛山市顺德区伍仲珮纪念医院）、中山大学附属第三医院肇庆医院、广州市弘宇科技有限公司、中山大学附属第三医院、中山大学孙逸仙纪念医院、中山大学肿瘤防治中心、北京志凌海纳科技股份有限公司、南方医科大学珠江医院、广东省第一荣军优抚医院、中山大学附属口腔医院、南方医科大学附属第三医院、广州医科大学附属妇女儿童医疗中心、广州医科大学附属第二医院、广州医科大学附属第五医院、广州市第一人民医院、中山市人民医院、中国医学科学院阜外医院深圳医院、深圳市第三人民医院、深圳市第四人民医院、深圳大学附属华南医院、粤北人民医院、连州市医疗总院、广州开发区医院、深圳市南山区人民医院、广州医科大学附属番禺中心医院、广州市番禺区中医院、广州市番禺健康管理中心（广州市番禺区康复医院）、番禺区医疗卫生集团、深圳市南山区医疗集团总部、深圳市龙岗区人民医院、深圳市坪山区人民医院、深圳市龙华区妇幼保健院、深圳市龙岗区第五医院、广州市南沙区东涌镇东涌社区卫生服务中心、广州市南沙区大岗镇灵山社区卫生服务中心、广州市南沙区东涌镇鱼窝头社区卫生服务中心、广州市南沙区珠江街道社区卫生服务中心、中山大学国家超级计算广州中心、国家超级计算长沙中心、中国电信股份有限公司广州分公司、中国移动通信集团广东有限公司广州分公司、中国联合网络通信有限公司广州分公司、广东省通信产业服务有限公司、广东安家医健科技有限公司、联通（广东）产业互联网有限公司、深圳市棒可可科技有限公司、广东飞和信息科技有限公司、暨南大学、西安电子科技大学、中南大学、湖南大学、广东药科大学、广东工业大学、广东技术师范大学、西安邮电大学、西华大学、上海电力大学。

本文件主要起草人：刘化龙、陈玉兵、吴庆斌、林汉辉、苏榕彬、王健英、郑华国、李世君、谭建皓、力竟成、林志辉、李国练、廖颖研、张晓东、吴向群、任忠敏、邹志武、陈智斌、龙运艺、张家庆、高峰、查正清、宗慧、郭华星、黄幸青、欧阳杰、任英华、张泽彬、陈汉威、徐飞、王逸欣、李贵华、练剑锋、吴庆军、杨川川、李鹏、何颖新、王文辉、鲁俊杰、苏悦洪、谢显荣、罗雪琼、刘斌、魏严冬、卢思远、白思韵、冯蔚学、李博孜、梁润锦、邓意恒、岳浩、李轩豪、廖茂成、李正文、周日文、吴冠雄、潘贵青、邓亚萍、陈景良、陈桂能、陈志福、张浩然、蔡永铭、王永祥、蔡勇、杨进、王铿、宋京、赵伍杰、洪永发、刘可儿、梁高翔、黄礼强、宁丽萍、何旭宇、黄玉辉、郑东生、刘志全、苗银宾、雷前、唐卓、曾安、潘丹、杨腾飞、周望、王亮亮、张嘉鹏、林舒源、杨宝瑶、苗美霞、刘玉娟、庾燕莉。

引　言

随着云计算技术在医疗行业的广泛应用，区域医疗混合云环境日益复杂，多云并存成为常态。为实现区域医疗信息化的高质量发展，提升医疗云平台的管理效率、资源利用率、数据安全性和业务连续性，相关医疗领域专家会同信息化专业人士经过充分交流制定本标准的必要性及可行性，旨在为区域医疗混合云环境中的多云纳管提供统一的技术指导，确保不同云平台之间的互操作性、兼容性和安全性，推动医疗信息化的创新与发展。

区域医疗混合云异构多云纳管技术规范

1 范围

本文件适用于地市级及以上卫生健康行政部门牵头建设的区域医疗混合云环境下的多云纳管，包括但不限于公有云、私有云、信创云、区域行业云等多种云平台的统一管理。适用于各级医疗机构、医疗信息化服务提供商、云服务提供商以及相关监管部门的云平台管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20988-2025 网络安全技术 信息系统灾难恢复规范
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 31168-2023 信息安全技术 云计算服务安全能力要求
GB/T 39725-2020 信息安全技术 健康医疗数据安全指南
GB/T 43206-2023 信息安全技术 信息系统密码应用测评要求
GM/T 0002-2012 SM4分组密码算法
GM/T 0030-2014 服务器密码机技术规范
JR/T 0208-2021 金融信息系统多活技术规范
WS 445-2014 电子病历基本数据集
WS/T 447-2014 基于电子病历的医院信息平台技术规范
YD/T 3890-2021 基于云计算的多云管理平台技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

资源池 Resource Pool

将不同云平台的同构或异构物理资源通过抽象、去耦合后形成的逻辑集合，含多平台CPU、内存、存储等资源的集合，对外提供统一计量、统一服务目录、统一生命周期管理的资源供给单元。

3.2

池化粒度 Pool Granularity

资源池的最小可分配单元规格，应与医疗机构业务负载模型匹配，支持vCPU、GPU、FPGA、裸金属、块存储、对象存储、文件存储、VPC子网、浮动EIP、负载均衡实例等多维度粒度。

3.3

弹性伸缩 Elastic Scaling

依据预定义策略或实时指标自动横向扩展（Scale-out/in）或纵向扩展（Scale-up/down）资源实例数量或规格，以满足业务负载变化并控制成本。

3.4

同城双活 Same-city Active-Active

在≤100km地理距离内建设两个物理隔离的可用区（AZ），网络往返时延≤5ms，数据实时同步，任一可用区故障时业务可切换，RPO（恢复时间目标）≤15min，RTO（数据丢失容忍点）≤15min。

3.5

多云纳管 Multi-cloud Management

通过统一的管理系统对两个及以上不同云服务提供商的云计算资源（涵盖计算资源、存储资源、网络资源、数据库资源等）进行集中整合、管理、监控、调度和优化的操作方式。

3.6

异地灾备 Off-site Disaster Recovery

在≥300km、不同地震带、不同电网节点的城市建立灾备中心，网络往返时延5－30ms；数据异步复制，故障时可切换，RPO≤15min，RTO≤30min。

3.7

医疗业务分级 Medical Business Classification

a） A 级：7×24 核心业务（HIS、EMR 在线服务）；
b） B 级：4×24 准实时业务（PACS 影像调阅）；
c） C 级：可延后业务（科研大数据、运营分析）。

4 参考模型

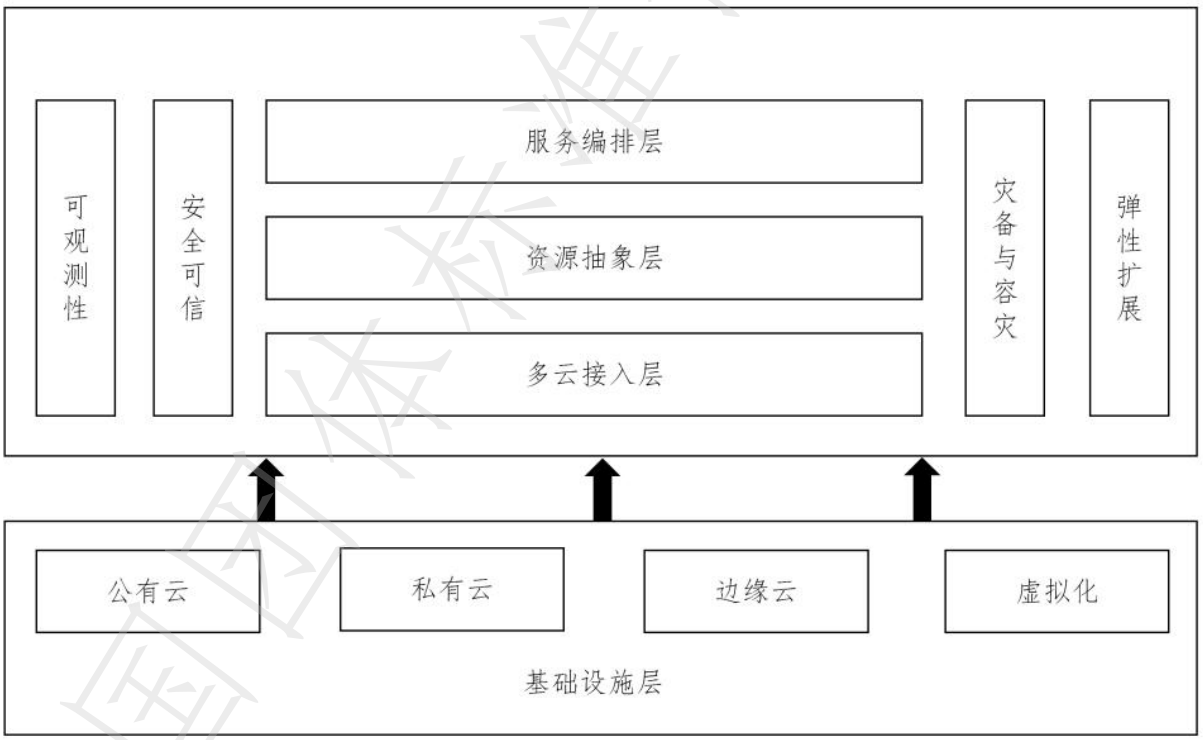

图1 区域医疗混合云异构多云纳管技术参考模型

4.1 架构设计原则

4.1.1 异构兼容性

支持主流公有云、私有云及边缘云的统一纳管，通过标准化接口屏蔽底层差异。

采用分层架构设计（基础设施层、资源抽象层、服务编排层），实现跨云资源池的透明化访问。同时，具备可观测性和合规性，满足审计链和数据跨云所需。

4.1.2 安全可信

基于国密算法（SM2/SM4）构建端到端加密通道，满足GB/T 39725-2020要求，算法实现须通过商用密码产品认证 GM/T 0002-2012。

实施零信任核心架构原则，动态验证云服务商接口的合规性，防止未授权访问。

4.2 核心组件模型

a) 多云接入层：提供标准化 API 网关，支持 RESTful、gRPC 协议，兼容 OpenAPI 3.0 规范，实现多云资源统一接入。集成多因素认证（MFA）与证书管理体系（PKI），确保接入身份合法性。标准化 API 网关具备安全防护能力，对可疑攻击来源进行限速。支持接口版本升级，支持向后兼容接口设计；
b) 资源抽象层：构建虚拟资源池，将计算（CPU/GPU）、存储（分布式块存储/对象存储）、网络（SDN/VPC）资源抽象为标准化服务单元。支持动态资源映射，实现跨云资源配额灵活调配；
c) 服务编排层：基于 Kubernetes 构建多云容器编排平台，支持跨集群应用部署与流量治理。提供可视化编排工具，支持医疗业务场景的微服务链式编排。

4.3 典型应用场景模型

4.3.1 灾备与容灾

采用双活数据中心架构，通过异步复制技术实现应用与数据同步机制。

支持跨云数据一致性校验，确保医疗影像、电子病历等关键数据完整性。

4.3.2 弹性扩展

基于AI预测算法预判资源需求，动态扩展工作节点应对峰值负载。

实施细粒度资源回收策略，空闲资源自动释放率≥95%。

5 通则技术

5.1 多云接入技术

多云接入技术是区域医疗混合云实现异构资源统一管理的核心能力，需满足跨云平台、跨地域的资源调度与数据交互需求，同时确保高可用性、安全性和可扩展性。

5.1.1 标准化 API

技术要求需通过统一接口规范，消除不同云平台间的技术差异，实现跨云服务的无缝集成与自动化管理。要求如下：

a) 接口设计规范
   1) 兼容 RESTful 与 gRPC 两种风格，不同场景按需选型；
   2) 路径设计遵循资源导向原则；
   3) 采用 JSON 作为标准数据交换格式；
   4) 响应状态码遵循 HTTP 标准。
b) 数据模型标准化
   1) 定义跨云通用资源模型，映射不同云平台的专属属性；
   2) 支持扩展字段，允许云平台保留特有参数，同时确保核心字段兼容性。
c) 版本控制与兼容性
   1) 接口版本通过 URL 路径或请求头标识，禁止破坏性变更；
   2) 提供旧版本接口的长期维护（至少 12 个月），支持平滑迁移至新版本。
d) 文档与工具链
   1) 生成交互式 API 文档，支持在线调试与代码生成，单规格文档生成时间≤3s，并发≥50个，95%内的请求延迟≤500ms；
   2) 提供 API 测试工具，验证接口功能与性能。

5.1.2 多种认证机制

5.1.2.1 背景与目标

多云环境下的医疗数据管理，需要保障数据的安全性、隐私性，确保不同云平台间的资源有效协同。在此背景下，区域医疗系统应采用多种认证机制，实现身份互认互通。要求如下：

a) 提供统一的认证机制框架，混合云异构多云纳管下对医疗系统进行有效身份验证和访问控制；
b) 提供多种认证机制的互操作性和灵活扩展，便于根据实际需求进行调整和优化；
c) 提供明确的认证标准和流程规范，保障医疗数据的安全访问和合规性要求。

5.1.2.2 认证机制的设计原则

在设计区域医疗混合云异构多云纳管技术框架时。认证机制的设计原则应符合以下要求：

a) 安全性：确保各云平台和医疗系统中用户、设备、应用等实体的身份真实可靠；
b) 兼容性与可扩展性：支持多种认证协议和方式，同时具有良好的兼容性和可扩展性；
c) 简单性与高效性：提供简洁、易用的认证机制，在高负载场景下及时响应请求；
d) 隔离性与合规性：认证框架满足数据隔离和合规性要求，确保数据访问符合相应的法律和行业标准。

5.1.2.3 多种认证机制结合的架构设计

在区域医疗混合云异构多云纳管技术框架中，应建立统一身份认证与访问控制机制，支持基于OAuth 2.0、 SAML 2.0、设备、多因素（MFA）以及角色基础访问控制（RBAC）等多种认证方式，实现支持不同认证模型的集成与无缝协作。

5.1.2.4 认证机制的集成与协同

认证机制的集成是确保不同平台、服务、设备能够无缝协同工作的重要保障。以下是几种常见的认证集成方式：

a) 单点登录（SSO）是多云和混合云环境中常见的认证需求。通过 SSO，用户只需一次身份验证，即可访问不同云平台和系统，减少登录的复杂性；
b) 联邦身份管理（FIM）是将多个不同云平台和企业系统中的身份和认证进行统一管理的机制，通过 FIM，区域医疗系统可以跨云环境统一身份验证，实现更加灵活的访问控制和权限管理。

5.1.2.5 认证框架实施的合规性与安全性要求

认证机制必须符合国家和地区的法律法规及行业标准。要求如下：

a) 数据保护与隐私：确保符合《中华人民共和国个人信息保护法》《个人健康医疗信息保护法》等法规，保障患者隐私；
b) 合规性认证：医疗云系统必须满足认证要求，确保数据的合法性和安全性；
c) 访问控制安全：基于角色的权限分配模式，最小权限原则，管理员双因素认证，敏感操作两次确认，操作日志全留存。

5.2 资源管理技术

5.2.1 资源池化

a) 异构纳管：支持多种主流云资源统一抽象；CPU 架构差异（x86、ARM、C86、LoongArch）对应用程序代码透明；检测时应提供统一的持续集成与持续发布体系，根据不同 CPU 架构生成相应的容器或虚拟机镜像；标记 CPU 架构的容器或模板镜像导入相应的计算资源池；
b) 池化建模：建立“地域-可用区-资源池-集群-节点”五级模型；模型元数据包含性能等级（Gold/Silver/Bronze）、安全域、灾备域、成本标签、国产化标签；
c) 统一计量：池内资源须秒级采集并归一化为标准计量单元（SCU：Standard Capacity Unit），1 SCU = 1vCPU • 4GiB • 1000 IOPS • 1Gbps；支持按需、预留、竞价多模式计价；
d) 多租户隔离：资源池须支持物理/逻辑两种隔离级别；医疗敏感业务（HIS/PACS）默认物理独占池，科研等非敏业务可共享逻辑池；池间网络采用下一代防火墙和微分段隔离；
e) 池化安全：池化层内置国密算法（SM4/SM3）对元数据及控制面报文加密；支持远程证明+可信启动，确保节点固件、OS、虚拟化层完整性。

5.2.2 弹性伸缩

a) 伸缩维度：同时支持横向（实例数量）与纵向（实例规格）伸缩；单实例规格调整中断时间≤30s；单集群横向伸缩速度≥100 节点，且集群就绪状态达成时间 5min；
b) 策略模型：内置≥3 种预设策略（性能优先、成本优先、信创优先等），支持自定义策略（指标阈值+时间窗口+步长+冷却期）；指标范围涵盖 CPU、内存、GPU 利用率、PACS 存储水位、门诊并发量、HL7 消息队列深度；
c) 预测式伸缩：集成时序预测算法（Prophet/LSTM），基于门诊排班、检查预约、节假日等特征，提前 1-4h 完成资源预热；连续 30d，日均门诊量预测误差≤15%，且峰值时段预测准确率≥85%；
d) 信创混合伸缩：当业务标签为“信创”时，优先在 C86/ARM/LoongArch 池扩容；若信创池资源不足，可跨池借用 x86 资源，但需在 24h 内回迁；
e) 成本治理：伸缩过程实时输出“成本-性能”权衡曲线；支持设置成本上限，超支时自动回缩并发出审计告警；
f) 伸缩安全：伸缩前自动创建快照/备份；节点下线前执行数据擦除。

5.2.3 性能指标

根据资源池关键场景性能要求，池化资源发现延迟应小于10s，弹性扩容生效时间应小于60s，纵向热升级中断时间应小于30s，多池并发伸缩成功率应大于99%，具体指标应符合表1。

表1 资源池关键场景性能指标

序号	指标项	目标值	测试条件
1	池化资源发现延迟	≤10s	新增 100 节点，90th 百分位延迟
2	弹性扩容生效时间	≤60s	CPU＞80%触发，实例 Ready
3	纵向热升级中断时间	≤30s	2vCPU→4vCPU，业务保持
4	多池并发伸缩成功率	≥99%	同时操作 5 个资源池，1000 次/池

5.3 服务编排技术

5.3.1 容器化

采用Kubernetes联邦集群管理多云容器，支持跨云服务发现与负载均衡。提供医疗专用镜像仓库，内置HIPAA合规镜像扫描工具,漏洞检测覆盖率≥99%。医疗专用镜像仓库支持镜像版本追溯与回滚机制，镜像需记录版本变更日志，支持30d内任意版本一键回滚。

5.3.2 微服务支持

基于Service Mesh实现微服务治理，支持灰度发布、熔断降级等策略。提供医疗业务模板库，预置电子病历共享、远程会诊等典型场景的服务链配置。

5.3.3 容器网络安全

对于区域医疗混合云，容器平台横向访问的网络安全需重视。采用下一代防火墙和统一态势感知实现容器边界的网络安全预警和阻断。

5.4 运维监控技术

5.4.1 智能化运维

区域医疗混合云统一管控平台实现对各个医疗云节点通过网络进行运维和管理，包括对各个医疗云节点的基础设施（交换机、物理机等）进行管控和运维、各类云资源及云服务的监控、监控报警、异常监测、故障监测、日志收集和上报等，以及中心到区域云节点的集中管控通道的安全、高可用等。

5.4.1.1 基础设施状态监控

a) 物理机监控：提供资源整体运行状态、电源状态、CPU 状态及性能、内存状态及性能、硬盘状态、文件系统空间、I/O 读写情况、网络状态及网络流量情况、资源事件、服务进程的监控；
b) 虚拟机监控：对虚拟机管理器进行全方位监控，涵盖其资源调度策略、自身资源占用、托管虚拟机的运行位置，以及相关关键服务进程的状态；
c) 存储类监控：提供资源数据存储介质空间情况、读写速率情况、资源事件、控制器状态、电源状态、存储介质状态、读写命中率情况的监控；
d) 网络类监控：提供资源的健康情况、网络流量情况、配置变动、链路情况、操作事件的监控。

5.4.1.2 云资源监控

a) 资源监控：对计算、存储及网络资源的分配与超配状态进行实时监控，其中网络监控包括 IP 地址分配状态；
b) 监控核心维度包括：服务运行状态，以及资源（CPU、内存、存储空间）、运行状态（主要进程）、连接（会话、网络）与可观测性（存储 I/O、日志、事件）等关键指标；
c) 应用能力类型监控：提供健康状态、页面可用性、API 可用性、整体可用性、性能表现、资源使用、访问情况、事务执行、进程状态、会话连接、日志与告警信息、浏览器端接入监测、移动端接入监测以及后端程序处理运行情况。

5.4.1.2.1 监控管理

a) 监控数据采集应支持对云资源性能、告警及配置等监控数据进行采集与管理。应满足以下要求：
   1) 采集模型定义与数据获取：应支持定义采集模型，明确被管对象的类型、指标属性及采集方式；基于采集模型获取数据，包括访问配置管理、数据采集与数据订阅。访问配置管理对访问资源的参数进行统一管理与合规性校验；数据采集按模型执行并校验参数，支持操作扩展与向后兼容；数据订阅通过规则管理采集行为，实现定时获取与分发；
   2) 资源自动发现与变更管理：应能自动发现平台新增或置备的资源，并完成其采集配置；当资源被删除或配置发生变更时，应能自动调整相应的采集管理策略；
   3) 数据归一化与采集机制：应支持对采集自异构系统的相同含义指标，按统一格式进行归一化处理；并支持集中式或分布式采集机制；
   4) 数据共享：应支持在监控管理各子模块间共享数据。
b) 监控平台性能应对云平台采集的性能指标数据进行处理、分析与呈现，并向云服务提供方与消费方提供监控与分析结果。具体要求如下：
   1) 指标采集与数据验证：应制定性能指标的采集策略，明确指标项、采集频率及时间间隔；并应对所采集数据的准确性进行验证；
   2) 数据处理与分析呈现：当原始数据为性能指标构成基础时，应通过关联、计算或聚合等方式，生成管理所需的有效指标；并应以恰当方式，向提供方与消费方呈现当前及历史数据，同时提供统计分析报告；
   3) 数据共享与开放接口：应支持向其他管理域共享性能数据；宜提供开放接口，供消费方获取其所属资源的性能数据。

5.4.1.2.2 统计分析

应通过对性能与告警指标数据进行多维度统计分析，并支持按云资源类型、时间及租户等条件进行统计，以获取云资源的运行情况和变化趋势。

5.4.1.3 告警管理

告警管理功能应能对平台产生的告警信息进行分析、处理和展示。具体要求包括：
a) 应制定告警策略，明确指标阈值、告警分类与分级规则；
b) 宜支持针对同一指标，为服务提供方与消费方设置不同的告警策略；
c) 告警信息需包含标题、来源、发生时间、描述和级别等关键内容，并支持基于时间或资源等维度定义告警间的关联规则；

d) 宜支持通过短信、邮件、界面等多种方式通知告警，并提供开放接口供消费方获取其资源告信息；
e) 应支持告警信息的查询功能。

5.4.2 自动化流程

自动化流程设计目标在于构建一个统一、智能、高效、可靠的可视化、自动化运维监控中枢，实现对异构混合云资源（包括本地数据中心、多个公有云、私有云）的管理。要求如下：

a) 提供全局统一的监控视角，消除因云平台差异带来的“监控孤岛”；
b) 降低 MTTR（平均修复时间）、提升 MTBF（平均故障间隔）为核心目标，将人工干预降至最低；
c) 提供统一的全局仪表盘，可自定义并综合展示跨云资源的健康状态、容量趋势、性能瓶颈及成本分析；
d) 告警系统支持多级阈值设定（警告、严重），并支持动态基线告警，能够根据历史数据自动学习并识别异常波动；
e) 内置或集成自动化运维引擎，能够接收监控告警事件作为触发条件，自动执行预定义的修复脚本或流程；
f) 提供低代码/可视化的流程编排界面，支持灵活定义自动化处理流程；
g) 支持跨云平台的批量资源巡检、配置下发、补丁更新等操作；
h) 定期自动检查安全组规则、存储策略等配置是否符合基线要求，发现违规自动修正或告警。

5.5 安全审计技术

5.5.1 日志管理

a) 应详细记录设备连接、报警触发、非法访问尝试，以及对患者信息等敏感数据的关键操作事件，并关联至操作用户、目标系统及核心数据标识；
b) 日志内容应包括事件发生的时间、IP 地址、涉及的设备或用户信息等；
c) 保留不少于 6 个月，定期进行加密备份，并采用校验技术保障日志完整性；
d) 应支持日志导出和打印，导出格式需满足司法取证及第三方审计工具要求；
e) 应支持对公有云、私有云及边缘节点的操作记录，支持虚拟机、容器、服务、API 网关、数据库等运行日志的统一收集、标准化与关联分析；
f) 应支持对日志存储及展示中的敏感字段实施动态屏蔽或脱敏，采用基于正则表达式与令牌化相结合的脱敏；
g) 宜支持基于角色的细粒度日志访问控制策略。

5.5.2 安全审计

a) 应支持敏感数据操作审计，记录敏感数据访问行为并生成日志，对异常敏感数据操作行为支持告警；
b) 应支持异常用户识别，识别异常用户并告警；
c) 应支持业务审计、运维审计，并生成审计报告；
d) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
e) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
f) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
g) 应对审计进程进行保护，防止未经授权的中断；
h) 应对云服务商及客户执行的远程特权命令，网络策略的变更等进行专项审计；
i) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计；
j) 应实现网络边界及重要节点的用户行为审计，对远程访问及互联网访问行为单独分析。

5.6 容灾双活技术

5.6.1 高可用性

5.6.1.1 多活架构

应基于混合云与多云环境构建跨地域/跨平台的多活服务能力。满足以下医疗核心业务连续性要求：

a) 部署模式：支持业务系统在异构云平台间实现多活部署，具备跨可用区、跨地域的流量分发与负载均衡能力；
b) 数据同步：建立实时/准实时的数据双向同步机制，确保关键业务数据在多地副本的一致性，同步延迟应低于业务容忍阈值；
c) 故障隔离：当单一云平台或可用区故障时，自动将流量切换至健康节点，切换过程需保证业务无感知，且具备人工干预接口；
d) 医疗场景适配：针对急诊、挂号等强连续性业务，设计业务层无状态化及会话保持机制，避免服务切换导致诊疗中断。

5.6.1.2 业务连续性

应建立覆盖业务全链路的连续性保障体系。要求如下：

a) 指标定义：明确核心医疗业务系统的 RTO 和 RPO；非核心系统按业务等级制定差异化指标；
b) 健康监测：实现对应用服务、中间件、云资源的多维度健康状态秒级监控，异常事件触发自动告警及预案执行；
c) 容灾合规：符合医疗卫生信息系统灾难恢复相关规范和政策要求，重点保障电子病历、医保结算等强监管业务的高可用性。

5.6.2 灾备建设

5.6.2.1 同城双活技术要求

a) 双活架构：采用“Active-Active”模式，双区同时承载业务；数据库使用分布式一致性协议（Raft/Paxos）或共享存储双写，保证单区故障数据零丢失；验证时应断开任一可用区（AZ）上行链路，验证业务会话不中断、数据零丢失；
b) 网络层：双活 AZ 间部署≥2 条不同路由的波分专线，单链路带宽≥100 Gbps，时延≤2ms，丢包率≤0.01%；网络虚拟化启用 SR-IOV+DPDK 加速；验证时应使用 RFC 2544 吞吐量与延迟测试仪，持续 24h 监控；
c) 存储层：采用伸展集群（Stretch Cluster）或分布式块存储，双写副本≥2+2，强同步写成功才返回 ACK；支持秒级一致性快照；验证时应模拟单 AZ 存储节点掉电，验证 IO 暂停时间＜1s，数据无分歧；
d) 数据库层：医疗核心库须支持分布式事务，提交协议满足“过半写成功”；提供全球事务号（GTN）保证跨 AZ 读一致性；验证时应使用 JMeter 模拟 10k TPS 混合事务，注入 AZ 隔离，验证事务无回滚、无脏读；
e) 负载均衡与流量调度：基于 Anycast+BGP 的 GSLB，健康探测间隔≤1s；流量可自动降级到存活 AZ，切换时间＜30s；验证时应关闭主 AZ 出口交换机，观察 DNS 解析变化及业务恢复时间；
f) 故障演练：每季度至少一次真实“拔网线”演练，覆盖存储、网络、电力三大场景；演练报告需包含 RPO、RTO、回切时间；验证时应提供演练报告及监控系统原始日志。

5.6.2.2 异地灾备技术要求

a) 灾备模式：采用“两地三中心”架构：生产中心、同城双活、异地灾备；异地为“Active-Standby”模式，日常只读验证；验证时应查看拓扑图及设备上架照片；异地中心提供只读查询截图；
b) 距离与风险域：异地中心与生产中心直线距离≥300km，处于不同地震带、不同流域、不同省级电网；避免同光缆路由；验证时需提供地震局与电网公司证明文件；光缆路由 RTT 测试；
c) 复制策略：异步复制，延迟≤15min；对象存储：近实时（≤1min）事件触发+定时差异合并；块存储：快照链每日 0、6、12、18 点各执行一次快照，保留 7d；验证时应模拟主中心断网，检查异地最新事务号与主中心差值≤15min；
d) 网络链路：主备中心间≥2 条不同运营 10Gb 专线，启用 FEC 及丢包重传；链路利用率＞70%时自动扩容；验证时应通过 7×24h NetFlow 统计，提供月度峰值报表；

e） 数据完整性校验：每日自动校验块级 checksum 与对象级 Hash（SM3），差异告警≤1min；每月全量恢复演练，随机抽样 5%对象做 bit-level 比对；验证时需提供校验日志与演练报告；比对成功率=100%；

f） 一键切换：提供“一键式”灾备切换脚本，RTO≤5min；切换范围包括 DNS、VIP、数据库角色、存储挂载、Kubernetes 集群；支持灰度回切；验证时应通过真实演练进行验证，注入主中心整体断电，测量业务恢复时间；回切过程业务中断＜30s；

g） 灾备容量：异地中心 CPU 与内存容量≥生产中心 50%，存储容量≥生产中心 120%；支持快速扩容至 100%；验证时需提供资源池实时截图及扩容测试记录。

5.6.2.3 灾备等级与业务映射

根据业务连续性要求，不同等级的灾备保护策略与恢复目标存在明确差异，具体业务等级与对应的灾备要求应符合表2。

表2 业务灾备等级与要求

序号	业务等级	同城双活	异地灾备	RPO 目标	RTO 目标
1	A 级	必选	必选	0	＜30s
2	B 级	必选	可选	≤1min	≤5min
3	C 级	可选	可选	≤15min	≤30min

5.6.2.4 指标与验证

a） 年度真实切换演练次数≥2次（含1次同城、1次异地）；

b） 演练报告需在48h内提交协会备案，包含RPO、RTO、回切时间、问题清单及改进计划；

c） 第三方评测：每三年通过国家级灾备评测机构现场评测，获得“增强级”及以上证书。

6 关键要求

区域医疗混合异构多云纳管架构的关键技术要求如下。

6.1 统一纳管

需支撑多云环境的资源管理、服务编排和智能运维。

6.1.1 资源管理

应实现对异构多云资源的统一抽象化、池化与自动化调度，在不影响在运业务下接入纳管。

应统一纳管平台应具备全面的资源管理能力，实现多租户、多业务、跨地域、跨云平台的资源集中调度、隔离管理与灵活扩展，支持云适配器版本监测与API演进适配。

6.1.1.1 多租户管理

应实现租户逻辑隔离与权限分级控制，支持基于组织结构的资源分配，确保各租户资源物理上隔离、逻辑上独立，具备租户间策略隔离与数据访问控制能力，并支持租户资源的按需弹性伸缩与动态调整。

6.1.1.2 统一资源池

a） 异构云资源纳管：支持纳管主流私有云及边缘节点资源，形成跨云资源目录。资源抽象层需屏蔽底层差异，提供统一的虚拟机、容器、存储、网络资源服务模型；

b） 资源画像与拓扑：自动生成资源拓扑视图，标识资源位置、健康状态及依赖关系。支持资源标签化管理，实现医疗业务与资源的智能绑定；

c） 支持将不同厂商、不同形态的资源统一纳入资源池，按需供给；

d) 支持计算、存储、网络、安全等资源的池化管理，具备资源注册、发现、状态监控、生命周期管理等功能；
e) 实现跨云平台资源抽象与标准化封装，屏蔽底层差异，提升平台兼容性与可移植性；
f) 提供资源池的可视化拓扑视图、容量分析和使用统计，便于管理者进行容量规划与优化；
g) 支持资源池的热扩容、故障自动恢复与资源健康检测，确保平台稳定运行。

6.1.1.3 动态分配与调度

a) 智能调度策略：基于医疗业务 SLA 要求，支持权重调度、故障域隔离、成本优化（竞价实例策略）等模式。敏感医疗数据资源调度需强制满足本地化策略；
b) 弹性过程需确保医疗业务连续性，缩容前执行服务无损迁移；
c) 平台应具备智能资源调度能力，根据业务需求、资源负载、使用策略等进行动态资源分配；
d) 支持基于策略的调度机制，实现跨资源池的最优资源利用。当策略冲突时，优先级顺序为：合规＞安全＞业务 SLA＞成本；
e) 提供资源调度日志与策略审计功能，确保资源调度过程透明、可回溯；
f) 可集成 AI 智能调度算法，结合历史数据与预测模型，优化资源配置与性能表现；
g) 支持容器资源调度与混合部署，提升对云原生应用的支持能力。

6.1.2 智能运维

统一纳管平台应具备全栈的运维监控能力，涵盖基础资源、平台组件、业务系统的运行状态监测与智能分析，实现“可视、可管、可控、可预警”的运维目标，包括故障原因分析、自动化修复策略、智能决策支持、具备AIOps能力、资源预测与弹性扩缩容建议、智能巡检与自动诊断工具、运维报告、健康评分生成、告警驱动的自动化执行及闭环工单系统联动，提升故障处理效率。

6.2 数据管理

区域医疗混合云异构多云纳管须具备高效、安全、灵活的数据管理能力，涵盖数据的存储方式、安全保护机制及共享交互手段。

6.2.1 数据存储

必须构建跨异构存储资源的统一纳管体系，全面覆盖数据创建、传输、存储、归档及销毁全生命周期，确保满足高可用性（年度可用率不低于99.95%）、数据持久性（年度丢失概率低于1×10^{-9}）、安全合规性及多云调度能力。

6.2.2 数据加密

数据加密是保障区域医疗混合云数据安全的核心措施，应贯穿数据存储加密、传输加密及密钥管理全生命周期。应符合以下要求：

a) 数据存储加密
   1) 支持国产加密算法，包括 SM1/SM2/SM3/SM4，支持向客户提供非对称与对称加密服务；
   2) 核心医疗数据应采用国密算法加密存储；
   3) 加密存储需支持“透明加密”模式，加密/解密过程响应延迟增加不超过 10ms。
b) 数据传输加密
   1) 跨云数据同步、医患端数据交互需采用 TLS 1.3 协议加密传输（禁用 TLS 1.0/1.1 及 SSL 协议）；
   2) 跨机构专线传输需额外部署 IPSec VPN 加密，加密套件应选用国密算法。
c) 密钥管理
   1) 加密密钥由硬件密码机生成与存储，禁止明文存储密钥，密钥管理系统需符合 GM/T 0030-2014 要求；
   2) 密钥更换周期不超过 1 年，且需留存密钥变更日志（含变更人、时间、旧密钥销毁状态），日志留存不少于 36 个月。

6.2.3 数据安全

6.2.3.1 访问控制

访问控制是区域医疗混合云异构多云环境中保障数据安全、资源合规使用及服务有序调用的核心机制，需实现多租户隔离、敏感数据精准管控及全流程可追溯，涵盖身份认证与统一管理、权限模型设计、数据访问控制及审计与合规。

6.2.3.2 备份恢复

a) 使用云服务的医疗机构应在本地保存其业务数据的备份；
b) 云平台应提供查询医疗机构数据及其备份存储位置的能力；
c) 云存储服务应保证医疗机构数据存在若干个可用的副本，各副本之间的内容应保持一致；
d) 应提供技术手段，协助医疗机构将其业务系统及数据迁移到其他云平台或本地系统，并支持迁移过程。

6.2.4 数据共享

6.2.4.1 跨云数据交换

a) 应支持多云环境间的数据安全互通；
b) 应提供数据网关或同步平台；
c) 应支持带宽优化、差异同步、数据压缩等能力；
d) 应提供数据传输链路加密、身份认证与权限校验；
e) 应提供标准化数据交换接口。

6.2.4.2 信息互联互通

a) 应支持区域内医疗机构与卫生信息平台间的信息共享与交换；
b) 兼容国家及行业相关标准与接口；
c) 应具备接口统一管理、格式转换与映射能力；
d) 应提供目录服务、服务注册与调用功能；
e) 应支持共享行为审计、统计与监管，规范跨机构审批流程。

6.3 应用管理

6.3.1 应用开发

应用开发需兼顾“跨云一致性”与“医疗业务特殊性”，通过标准化框架确保应用在异构多云中的兼容性、安全性和可扩展性，支持为应用开发标准化框架增加快速开发工具。

6.3.1.1 标准化开发框架

标准化开发框架是区域医疗应用在异构多云环境中实现“一次开发、多端适配、跨云部署”的基础，应覆盖技术栈、接口、数据、安全、生命周期等核心维度，确保不同医疗机构、不同云平台的应用协同互通。

6.3.1.1.1 技术栈标准

a) 前端：支持跨终端适配（PC 端、移动端、大屏），推荐采用 Vue.js、React 等主流框架，应兼容医疗专用终端的操作系统（国产操作系统、Windows、Android 等）；
b) 后端：基于云原生架构，支持容器化部署和编排，推荐 Java、Python 等语言，应适配异构云平台的服务器架构（x86、ARM 等）；
c) 数据库：支持多模式数据存储，关系型数据库用于结构化数据，非关系型数据库用于非结构化数据，应兼容不同云厂商的数据库服务；
d) 中间件：应确保跨云服务调用的一致性，包括消息队列服务、Web 应用服务器、服务注册发现、服务配置中心等。

6.3.1.1.2 接口标准

应符合医疗行业互联互通规范，实现应用与云平台、应用与应用间的无缝对接。要求如下：

a) 数据交换接口：强制支持 HL7 FHIR（健康数据交换国际标准）、卫健委 WS/T 447 中的接口规范，兼容 DICOM（医学影像）、IHE（跨企业医疗集成）等协议；
b) 服务调用接口：统一采用 RESTful API 设计规范，支持 HTTPS 加密传输，接口命名、参数格式、返回码需符合行业标准；
c) 跨云适配接口：内置云平台适配层，屏蔽公有云与私有云的底层接口差异，支持接口调用的路由、负载均衡和故障转移。

6.3.1.1.3 数据模型标准

基于医疗数据的特殊性（敏感、结构化与非结构化混合），需定义统一的数据模型规范。要求如下：
a) 核心数据结构：应遵循 WS 445-2014 等国家规范，应明确患者标识、诊疗信息、药品信息等核心字段的格式、类型和约束；
b) 数据分类存储标准：区分敏感、一般医疗、运营等数据，定义不同类型数据在混合云环境中的存储策略；
c) 数据流转规则：明确数据跨云传输的格式转换、加密方式、脱敏规则及完整性校验方法；
d) 基于医疗信息的特殊性（敏感性高、结构与非结构混合），需制定统一的数据模型规范。

6.3.1.1.4 安全合规标准

嵌入医疗级安全控件。满足下列要求：
a) 身份认证：支持多因素认证，兼容医疗行业统一身份认证体系；
b) 权限控制：基于 RBAC（角色权限）模型，细化医疗角色权限（医生、护士、管理员），支持数据级权限；
c) 数据安全：强制要求传输加密（TLS 1.3）、存储加密（敏感字段加密存储），支持隐私计算技术的集成接口，实现数据“可用不可见”；
d) 审计追溯：内置日志采集组件，记录应用操作、数据访问、跨云传输等行为，日志应符合医疗行业“至少保存 6 年”的归档要求，应支持对接多云审计平台。

6.3.1.1.5 生命周期管理标准

规范应用从开发到下线的全流程，适配异构多云的部署环境。满足下列要求：
a) 环境标准化：定义开发、测试、预生产、生产环境的配置标准，支持跨云环境一键复制；
b) CI/CD 流水线：统一代码管理、构建工具、部署工具，支持跨云平台自动部署；
c) 运维监控：兼容多云监控平台，定义医疗应用核心指标的监控阈值和告警规则。

6.3.1.2 快速开发工具

快速开发工具旨在降低医疗应用开发门槛，加速区域医疗业务响应，确保快速开发的应用符合跨云规范。其要求如下：
a) 低代码/无代码开发平台
   1) 核心功能：提供可视化拖拽界面、配置化逻辑设计，支持多终端自动适配；
   2) 医疗适配：内置医疗场景模板，预配置与 HIS、LIS、PACS 等系统的集成接口；
   3) 多云部署：支持一键生成符合标准化框架的容器镜像，可直接部署至混合云环境，并自动适配目标云平台的资源调度规则。
b) 医疗专用组件库：提供可复用的医疗业务组件，减少重复开发，包括数据录入组件、影像处理组件、流程引擎组件、数据可视化组件等；
c) 集成开发环境（IDE）增强工具：针对传统编码开发的效率提升，宜采用行业插件、多云适配工具及代码生成器等赋能工具；
d) 测试自动化工具：确保快速开发的应用满足医疗级可靠性，应部署医疗数据模拟器、接口自动化测试及性能压力测试等验证机制；
e) 工具生态集成：所有快速开发工具应支持与标准化开发框架的 CI/CD 流水线、安全控件集成。

6.3.2 应用部署

为确保异构多云环境中医疗业务的连续性与稳定性。应用部署应遵循以下核心要求：

a) 一键式部署：应用部署应构建标准化的全流程机制，采用自动化编排工具实现高效调度与管理，并分别建立符合信创要求及通用技术体系的容器与虚拟机镜像仓库，确保异构多云环境下的部署一致性、安全性与可追溯性；
b) 自动化升级：利用自动化脚本或专业的软件管理工具，定时对医疗应用进行版本检测。在各云平台上部署检测代理，该代理与应用供应商的官方版本库建立安全链接，定期查询是否有新版本发布；
c) 失败与回退：基于应用版本软件管理控制工具实现自动化升级后，若出现新版本不兼容或影响业务稳定性等情况，需要支持上一个版本或指定版本回退机制，达到快速恢复升级前状态。

6.3.3 应用监控

6.3.3.1 实时性能监控

a) 应用监控范围：应覆盖所有异构云资源池、跨域网络链路及运行在多云之上的全部医疗业务应用，包括 HIS、EMR、PACS、区域健康档案平台等；
b) 应用监控指标体系：门诊挂号平均响应时间、影像调阅端到端时延、电子病历保存成功率、CDSS 推理耗时等。
c) 数据采集与传输
   1) 采集协议：支持 SNMP、JMX、Prometheus Exporter、OpenTelemetry、Syslog、WMI 等；
   2) 采集周期：资源层≤10s，平台层≤30s，应用层≤60s，关键业务指标可降至 1s；
   3) 传输要求：经 TLS1.3 加密，采用消息队列或 gRPC Stream 确保不丢失，支持断点续传。
d) 应用实时告警：应用监控采集数据对接到云监控平台，并沿用云监控平台的实时告警模块；
e) 应用可视化与报表：提供多租户 Portal，支持拓扑图、折线图、热力图、桑基图等多维可视化；支持按照医疗机构、业务域、云厂商维度钻取；自动生成日报、周报、月报；
f) 应用监控高可用：沿用云资源监控架构，实现统一监控高可用服务。

6.3.3.2 应用优化

a) 性能瓶颈定位：应利用 APM 探针、代码级诊断、调用链追踪、日志聚类分析，形成“指标-链路-日志”三维关联；支持自动标记慢 SQL、慢 API、内存泄漏、线程阻塞根因。
b) 弹性伸缩策略
   1) 水平伸缩：基于 CPU＞60%或 QPS 预测模型自动增加副本，缩容冷却时间≥300s；
   2) 垂直伸缩：针对高 I/O 数据库实例，在业务低峰期在线扩容 CPU/内存，热升级时间＜90s。
c) 多云调度：依据费用、合规、网络延迟综合评分，动态将无状态应用漂移至成本最优云。
d) 数据层优化
   1) 缓存：应针对患者主索引、药品目录等高频查询数据使用分布式缓存，命中率≥80%；
   2) 分库分表：电子病历、影像元数据按时间分片，自动归档至低频存储；
   3) 读写分离：主从延迟＜100ms，支持只读副本横向扩展。
e) 网络优化：在跨域链路启用 TCP BBR 拥塞算法；关键业务流量采用 QoS 等级 EF（Expedited Forwarding），带宽保障≥20%；对影像文件传输启用多线程断点续传+CDN 边缘缓存，降低 50%出口流量。
f) 持续优化流程
   1) 每月召开一次“性能与成本治理例会”，责任人包括信息中心、业务科室、云服务商；
   2) 建立优化知识库，沉淀 SQL 索引、代码补丁、配置模板；
   3) 对优化效果进行 A/B 验证，结果纳入年度考核。

6.4 成本管理

6.4.1 成本控制

6.4.1.1 按需付费

a) 资源动态分配：支持基于业务负载的实时资源分配与释放，按实际使用量计费（云厂商原始计量值与平台二次核算值偏差≤±3%，以平台数据为结算依据）。需提供资源使用量预测工具，避免因突发流量产生超额费用；
b) 多云统一计费接口：集成不同云服务商的计费 API，生成统一的费用报表。计费粒度应精确到分钟级，支持按项目、部门或医疗机构拆分账单；
c) 医疗场景优化：对低频访问的医疗数据自动切换至低成本存储类型。

6.4.1.2 弹性计费

a) 自动伸缩策略应支持依据预设规则自动扩容，资源增量部分自动计费，业务低谷时自动缩容，资源减量部分停止计费；需支持医疗业务优先级设置；
b) 混合云成本优化应实现自动将非敏感计算任务调度至公有云低成本区域；同时将核心业务默认调度至私有云或信创云资源池；
c) 费用告警与拦截功能应支持设置月度预算阈值，超支时自动触发告警或暂停非关键资源分配；并提供成本根因分析工具，定位异常费用来源。

6.4.1.3 资源利用优化

通过区域医疗混合云异构多云纳管技术，实现统一的资源利用率分析功能，为对接单位基础设施提供资源优化参考，降低数据中心运营成本，提高资源的利用率。