临夏州中医医院云运维服务项目参数要求

一、总体要求

应支持基于业界主流的微服务架构体系进行开发和建设，运维人应具有丰富的云平台运维管理和底层问题解决经验，确保能够解决、修复所使用的软件中的问题。

二、基础服务：

1、应提供业务系统所需的整体计算能力和业务承载能力保障。

2、云平台可靠性服务：应支持在容错、容灾、故障、攻击等场景下，通过冗余、高可用集群、应用与底层设备松耦合等特性来体现，从硬件设备冗余、链路冗余、应用容错等方面充分保证整体系统的可用性，来实现系统在故障或攻击时服务的正常使用或服务降级时的核心服务确保一定的服务能力。应能够快速恢复故障应用系统，确保业务的连续性。

3、云平台建设服务：应支持对云平台上业务系统的整体建设，对各个业务系统模块建设资源应支持具体动态调整、弹性扩容、网络支持动/静态 BGP 接入、支持 x86 及异构算力等保证业务平稳健康运行满足业务需求，对业务建设发展过程中资源调整应提供增扩容的技术支持。应提供计算、存储、网络、安全、容器、数据库、中间件、大数据、人工智能、物联网等多种服务，满足当前及未来业务的扩展。

4、平台高可用性服务：云平台业务系统建设过程中所需的中间件支持，应提供稳定的消息队列服务支撑、稳定的高速缓存存储能力支撑、大数据量写入存储能力支持、大数据量日志的数据搜索引擎能力支撑等。

5 云平台服务系统持续集成与持续发布，应支持为整个业务系统敏捷版本发布提供稳定的持续集成与发布能力，提供无故障感知的服务升级能力，提供服务升级灰度发布以及滚动升级能力。

三、安全服务：

1、应支持为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。VPC 丰富的功能应支持灵活管理云上网络，包括创建子网、设置安全组和网络 ACL、管理路由表、申请弹性公网 IP 和带宽等。通过链路冗余，分布式网关集群，多 AZ 部署等多种技术，保障网络的安全、稳定、高可用。

2、安全组：安全组是一个逻辑上的分组，应支持为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，应支持

在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

3、Web 应用防火墙（WAF），应支持对网站业务流量进行全方位检测和防护；HTTP(S)请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定；提供精准高效的威胁检测、针对业界爆发的高危 web 漏洞，应提供快速分析漏洞、向引擎下发漏洞防御规则的支持，保障 0day 漏洞及时在 waf 打上虚拟补丁，用户无感知；应支持通过 Web 应用防火墙服务配置地理位置访问控制规则。可针对指定国家、省份的来源 IP 自定义访问控制；提供简洁友好的控制界面，实时查看攻击信息和事件日志。

4、DDoS 高防，以应对 DDoS 攻击挑战，应支持提供毫秒级攻击响应、多维度行为分析及机器学习、防御策略自动调优、精确识别各种复杂 DDoS 攻击，以保护业务连续性。抵御大流量 DDoS 攻击，避免服务器被攻击后导致业务瘫痪。

5、企业主机安全，应提升主机整体安全性的服务，提供资产管理、漏洞管理支持检测系统和软件漏洞、Web-CMS 漏洞，识别潜在风险。入侵检测、基线检查等功能，降低主机安全风险；检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性；对运行中的程序进行检测，识别出其中的后门、木马、蠕虫和病毒等恶意程序，帮助用户识别出系统存在的安全风险。

6、云堡垒机，应支持对云上服务器的操作运维审计；提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计；提供可视化运维行为监控，及时预警发现违规操作；实时记录管理员的资源管理、用户管理和策略管理等所有行为日志，以便监控和审计。

7、数据库安全服务，审计数据库操作行为；基于机器学习机制和大数据分析技术，应提供数据库审计，SQL 注入攻击检测，风险操作识别等功能；应提供旁路模式数据库审计功能，对风险行为进行实时告警。应支持对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

8、安全态势感知，应支持统一的威胁检测和风险处置平台；应支持检测出 8 大

类的云上安全风险，包括 DDoS 攻击、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，呈现全局安全攻击态势。

9、云审计，应支持对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等，记录审计日志、审计日志查询、审计日志转储、事件文件加密。

10、云监控，应支持一个针对弹性云服务器、带宽等资源的立体化监控平台。资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

11、云日志，应支持日志收集、实时查询、存储等功能，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，提供实时、高效、安全的日志处理能力，快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

四、云平台日常运维服务：

1、专门的运维团队，应支持全时段运维服务，制定科学的管理制度、服务流程、质量管控策略等，形成稳定高效的服务管控体系，做到管理规范、流程合理、职责明确、服务高效。

2、监控服务：云平台基础资源的实时监控与告警，应包括云主机计算资源、内存资源、存储资源等维度的实时监控与分析，对日常业务运行提供业务异常监控，对日常网络带宽提供预警监控，对以上所有监控维度的实时监控与实时告警能力支撑。

3、云平台故障处理服务：应支持根据业务运行需要，对云平台各组件、各项参数进行针对性的调优，如调整资源虚拟化比例、虚拟 CPU 类型与型号、服务线程数量，对业务运行过程中的故障进行分析监测，故障解决，提供 7x24 的检测与处理能力。

4、云平台容量规划与调整服务。应支持对业务需求统计分析，对云平台进行容量规划，包括计算能力、存储容量、网络 IP 地址空间等；实施网络隔离，保障网络安全。