|  |
| --- |
| 2025年度西宁市市场监督管理大数据监管服务中心政采招标技术参数 |
| **一、云业务** |
| **序号** | **名称** | **设备规格** | **数量** | **单位** | **备注** |
| 1 | 云主机（租用） | 1、主机配置：vCPU≥ 64 核、内存≥ 256G、超高IO磁盘≥6200G、高IO磁盘空间≥12000GB的主机1台，vCPU≥ 4 核、内存≥ 8G、高IO磁盘空间≥ 540GB的主机4台，vCPU≥ 4 核、内存≥ 32G、高IO磁盘空间≥ 2040GB的主机1台，vCPU≥8 核、内存≥ 64G、磁盘空间≥ 2040GB的主机1台，vCPU≥8 核、内存≥ 64G、磁盘空间≥ 540GB的主机1台； | 1 | 套 |  |
| 2、云主机基于 OpenStack 云平台，不可为私有标准，基于原生OpenStack 开发的管理平台向上层提供 API 接口及说明文档，对主机、存储、网络、负载均衡器、防火墙、弹性 IP 等功能提供 API 级别的支持；API 与其它主流云计算平台兼容,或具备适配能力，要求提供不低于符合国家三级等级保护要求的云平台服务能力，通过可信云认证，提供相关证明材料； |
| 3、可为互联网安全访问（如客户信息安全、传输安全）等提供端口策略控制；云主机可用性不低于 99.95%，自动检测云服务器故障，自动启用故障转移。 |
|  | 4、API 调用 支持控制台或者通过 API 调用方式对云主机进行包括创建、查询、销毁云主机实例等相关管理和操作，支持云主机实例分钟级快速发放； |
| 5、提供常见的主流操作系统公共镜像，支持主流的 Windows 和 Linux 操作系统。Windows镜像包括 2012DataCenter 中/英/64 位、2012Standard 中/英/64 位，包含正版的 License 授权，Linux 支持 CentOS6.4/64 位、CentOS6.6/64 位、CentOS7.1/64位 Ubuntu14.04/64 位"； |
| 6、支持绑定浮动私有 IP 地址，为网卡提供第二个 IP 地址，实现更灵活的网络功能，比如 HA双机热备时的浮动 IP。支持多网卡，可为云主机配置 1 张主网卡以及最多 11 张从网卡；可以设置不同的 IP 地址； |
| 7、可提供负载均衡能力； |
| 8、支持云硬盘的创建/删除、批量创建/批量删除、查看、挂载、卸载，支持对可用状态数据盘以及系统盘进行扩容，支持共享云硬盘，可以创建共享云硬盘，最多同时挂载到 16 台云主机上，支持对云硬盘读速率、读操作速率、写速率、写操作速率的监控；支持普通 IO、高 IO、超高 IO 三种类型的云硬盘，单盘最大支持 32T 容量，超高 IO 单盘最大吞吐量达到 350MBps，最大 IOPS 达到 20000，时延低至 2ms（8k 数据库测试结果）； |
| 9、三副本冗余，数据持久性达 99.99999%，支持云硬盘备份，可以手动执行备份，也可以通过设置备份策略进行自动备份； |
| 10、支持密码和证书两种登录方式， 其中 Windows 云主机仅支持密码登录方式，支持多种登录云主机方式，包括 VNC 登录，SSH 方式登录（Linux 云主机 ），MSTSC 方式登录（Windows 云主机）； |
| 11、支持重装云主机操作系统、支持重置云主机密码、支持云主机多维度状态监控和告警； |
| 12、云机房有自建机房，且要求机房在青海省境内（须提供产权证明）； |
| 13、提供独立的公网 IP 资源，包括公网IP 地址与公网出口带宽服务。可以与弹性云主机、虚拟 IP、弹性负载均衡、 NAT 网关等资源灵活地绑定及解绑。 |
| 2 | 云下一代防火墙（租用） | 1、要求吞吐≥1Gbps，最大并发连接数不少于5万，每秒新建连接数不少于2W，产品可在虚拟机上实现快速灵活的部署专业防护，为虚拟网络或应用提供专业的边界网络安全防护功能； | 1 | 套 |  |
| 2、支持对4000+ 种应用的控制，包括200+移动应用（需提供产品页面截图）；支持应用过滤器便于配置和维护，至少支持6个维度进行过滤，包括：名称、类别、子类、应用技术、风险界别、特性；其中应用技术至少包括：基于浏览器、客户端服务器、网络协议、点对点；风险级别包括：1、2、3、4、5总共5个等级；特性包括：能够传输文件、已被大规模使用、大量消耗带宽、易逃逸、易被滥用、被其它应用使用、存在已知漏洞、被恶意软件利用（需提供产品页面截图）；支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip、P2P下载、视频、网络游戏等）限制新建连接、并发连接（需提供产品页面截图）； |
| 3、支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换；为解决公网IP地址资源问题，支持NAT的端口扩展技术，实现单个公网IP的无限地址转换（需提供产品页面截图）；支持NAT地址可用性探测； |
| 4、支持防火墙策略命中数统计功能，便于管理员维护防火墙策略（需提供产品页面截图）；支持策略冗余检测，对策略重复检查； |
| 5、支持静态路由、等价路由、策略路由，以及RIPv1/v2等动态IPv4路由协议（非透传）（需提供产品页面截图）；策略路由支持基于指定IP地址、指定应用协议、指定时间表生效（需提供产品页面截图）； |
| 6、支持QoS管道策略实际流量情况监控，支持子管道叠加情况监控（需提供产品页面截图）；支持链路状态监控，可查看指定应用/应用组详情，支持选择多条链路进行对比分析（需提供产品页面截图）；支持通过netflow v9进行流量信息采集和外发； |
| 7、支持Qos流量管理，可根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan等信息划分管道，支持对多层级管道进行最大带宽限制、最小带宽保证、每IP或每用户的最大带宽限制和最小带宽保证 （需提供产品页面截图）； |
| 8、支持基于流、低延时、高并发、高性能的病毒过滤，支持加密流量开启病毒过滤功能，实时病毒连接阻断，病毒事件记录，支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描，支持超过 1000多万的病毒特征库，病毒库可以在线更新、本地更新（需提供产品页面截图）；支持对压缩文件类型的病毒检测，必须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型； |
| 9、支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测和防御，具备9000种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询，并支持网络实时更新（需提供产品页面截图）；内置知识库，详细描述攻击特征及解决方案 （需提供产品页面截图）支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法（需提供产品页面截图）； |
| 10、本次配置基础功能授权及配套弹性云主机； |
| 3 | 云堡垒机（租用） | 1、支持在IPV4,IPV6，IPV4与IPV6网络环境下部署；支持物理旁路，逻辑串联模式，无需镜像、无需改造现有网络结构； | 1 | 套 |  |
| 2、支持分权分域，支持用户管理，包括添加、删除、启用、禁用、移动、修改功能；支持用户组管理，包括添加、删除、修改功能；支持用户帐号的批量导入导出功能；支持批量修改用户帐号属性；支持设置密码策略，策略包括：最小密码长度（强制最小8位）、密码复杂度（小写字母，大写字母，数字，特殊字符）、不允许密码与用户一致设置，不允许密码与用户逆序，密码周期（过期前提醒）、历史密码对比；支持用户账号有效期配置，提供产品配置截图； |
| 3、支持AD域用户抽取，从AD域抽取组织机构和用户帐号，方便快速建立组织机构和用户帐号； |
| 4、支持资源管理与授权，支持资源管理功能，包括添加、删除、启用、禁用、移动、修改功能；支持资源组管理功能，包括添加、删除、修改功能；支持资源（包括服务和资源帐号）批量导入导出功能；要求内置常见资源分类和资源系统类型； |
| 5、支持资源自动发现，支持资源自动发现和添加，便于快速添加资源； |
| 6、支持数据库审计，支持的数据库类型包括：Oracle（支持ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担；支持Oracle、Postgresql、Sybase、MySQL、SQL server数据库下行返回行数记录；支持在Oracle数据库运维，运维人员对变量进行绑定，执行SQL后，堡垒机系统可审计对应SQL中唯一标识符的具体值，协助审计员分析安全事件；支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句关键字定位审计回放； |
| 7、支持RDP、VNC图形操作行为的审计，图形回放形式还原真实操作过程；支持RDP、VNC图形操作过程中键盘输入操作记录和鼠标点击行为记录，并支持开启或关闭键盘输入审计功能；支持对剪贴板拷贝文件记录文件名、拷贝文本进行字符记录，并支持通过搜索字符信息关键字定位审计回放； |
| 8、支持审计查询和报表，自定义审计查询条件，包括：时间范围、用户与用户IP、资源IP、资源服务、命令关键字条件；审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS\_C\_5601\_1987,Shift\_JIS,Window-874)，由审计管理员自主选择；提供用户统计报表和系统运行报表，支持Word，Excel，PDF，HTML方式导出； |
| 9、支持运维人员通过IE（9-11版本）、谷歌浏览器、Firefox浏览器单点登录资源，无需安装Java控件；同事支持C/S运维客户端功能，用于运维人员通过运维客户端登录进行运维操作，整个运维过程不依赖任何Active或Java控件；为运维用户提供 SSH/RDP CLI工具直连模式，通过认证后进行资源的访问。支持SecureCRT，Mstsc工具；提供产品配置截图 |
| 10、支持二次审批，支持根据需求对特殊指令操作进行二次审批功能，运维人员操作过程中触发命令策略，需要得到审批员的审批后才能继续执行后续操作；可设置审批规则与资源角色关联，对运维人员访问资源制定登录审批策略，需要得到审批员的审批后才能继续执行后续操作； |
| 11、本次配置≥20个资产授权及配套弹性云主机； |
| 4 | 云WAF（租用） | 1、通过多维度防御策略，为网站拦截SQL 注入、XSS 跨站、命令& 代码注入、敏感文件访问、恶意爬虫等Web 类型的攻击，保障您的业务安全稳定运行； | 1 | 套 |  |
| 2、支持常见Web 攻击进行检测，包括但不限于SQL 注入、XSS跨站攻击、命令注入、代码注入、敏感文件访问等。能通过预置的信誉库，防护恶意扫描爬虫等攻击。支持第三方漏洞攻击等威胁检测和拦截； |
| 3、支持策略事件集中配置，支持记录、阻断两种模式，支持误报屏蔽策略； |
| 4、支持精确识别，支持语义分析+正则双引擎，支持常见编码还原； |
| 5、支持流量及事件统计：可实时查看访问次数、安全事件的数量与类型，可查看详细的事件信息，支撑事件溯源； |
| 6、当第三方 Web 框架、插件爆出高危漏洞，业务无法快速升级修复，Web 应用防火墙会第一时间升级预置防护规则，保障业务安全稳定； |
| 7、支持黑白名单配置，可自定义防护域名、黑白名单类型支持IP、URL、referer、useragent，提供产品配置截图； |
| 8、支持攻击日志告警及处置，告警类型包含请求方法、访问URL、客户端IP、攻击类型、地区、请求时间等，提供产品界面截图； |
| 9、支持业务访问带宽、流量、访问趋势图、访问状态分布、访问URL排行、源站延时趋势等信息集中展示，支持WEB攻击趋势、CC攻击拦截、攻击来源、攻击类型、攻击IP排行、攻击记录集中展示； |
| 10、本次配置≥一个域名包可支持10个子域名防护，200MB防护带宽； |
| 5 | 云日志审计（租用） | 1、支持拓扑管理，并能够支持拓扑维度展示整体安全、事件分布、告警分布等； | 1 | 套 |  |
| 2、支持对IP对象的自动发现功能，支持IPv6，对自动发现的设备可以转资产或删除； |
| 3、支持从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段； |
| 4、支持完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间的占用；可通过自定义聚合规则修改日志的聚合归并逻辑规则，提高日志分析效率； |
| 5、支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计（需提供产品功能截图证明）； |
| 6、支持挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统支持GUI方式的关联规则设置功能； |
| 7、支持显示审计事件分类统计列表，按照审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度进行展现（需提供产品功能截图证明）； |
| 8、支持审计对象的定义，包括：审计目标对象、审计行为对象、审计行为执行者对象、审计来源对象、审计时间段对象等（需提供产品功能截图证明）； |
| 9、支持HTTP网页标题、BBS、威胁情报、DGA、搜索关键词的网络会话分类展现（需提供产品功能截图证明）；支持DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现（需提供产品功能截图证明）；支持TLS会话、数据库会话、邮件会话、FTP会话、Telnet会话，即时通讯会话的展现（需提供产品功能截图证明）； |
| 10、本次配置日志审计授权及配套弹性云主机； |
| 6 | 云数据库安全（租用） | 1、支持敏感数据发现：包括PCI、HIPAA、SOX、GDPR 等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据，可以一键自动生成脱敏规则和审计规则； | 1 | 套 |  |
| 2、支持合规审计：支持数据库活动监控，可提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访问时间、请求的数据库、原SQL 语句、操作、 成功与否、耗时和返回内容等，协助用户溯源到攻击者； |
| 3、支持实时告警：支持通过操作类型、操作对象、风险等级等多种元素细粒度定义要求监控的风险操作行为，当系统资源（CPU、内存和磁盘）占用率达到设置的告警阈值时立即告警； |
| 4、支持审计时长、语句总量、风险总量、风险分布、会话统计、SQL分布等多维度的快速分析，支持根据时间、数据库用户、客户端等多角度进行分析，提供时间、风险等级、数据用户、客户端IP、数据库IP、操作类型、规则等多维度线索分析； |
| 5、支持用户行为发现审计：可关联应用层和数据库层的访问操作，提供内置或自定义隐私数据保护规则，防止审计日志中的隐私数据（例如，账号密码）在控制台上以明文显示； |
| 6、支持精细化报表：提供客户端和数据库用户会话分析报表、提供风险分布情况分析报表、提供满足数据安全标准（例如Sarbanes-Oxley）的合规报告等功能； |
| 7、支持审计规则配置，包括审计范围、SQL注入、风险操作、隐私数据保护，可根据实例情况进行具体配置，提供配置界面截图； |
| 8、支持审计报表导出，报表内容包括名称、关联数据库、报表类型、生成时间、格式、状态、操作等； |
| 9、支持告警通知，支持邮件告警、告警风险等级、系统资源告警，支持自动备份、手动备份； |
| 10、本次配置≥2个数据库实例授权； |
| 7 | 服务器安全卫士（租用） | 1、支持主流Linux（64位）和windows server（64位）服务器；支持安全报告，服务器端安全监测和防护，监测数据由专业安全团队以报告的形式定期发送给客户； | 1 | 套 |  |
| 2、支持所有安全风险、安全加固、漏洞修复等都具有详细的视图与可落地的操作指令； |
| 3、支持自动化细粒度风险分析，涵盖弱口令检测、软件漏洞检测、防暴力破解、异常登录、web后门监测诊断、shell检测等多维度； |
| 4、支持资产清点，自动清点主机内部资产如进程、端口、账号、应用等，实时掌握主机内部资产变化，为安全分析提供数据基础； |
| 5、支持对入侵等高危情况进行实时邮件通知； |
| 6、支持安全审计，操作审计，实时操作命令记录，实时发现危险操作，支持审计规则自定义，支持审计日志导出； |
| 7、本地提权，支持实时进程提权监测，支持进程提权过程详细记录； |
| 8、支持合规基线，结合基线内容，可快速进行企业内部风险自测，发现问题并及时修复，可根据业务组、主机自行定义基线标准； |
| 9、支持病毒查杀、自动处理、杀毒引擎设置，支持病毒隔离、阻断、删除，支持病毒告警功能； |
| 10、本次配置≥11台服务器授权； |
| 8 | SSL VPN（租用） | 1、要求专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN、PPTP VPN、L2TP VPN；支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持Windows、IOS、Android、塞班等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入；移动端（Android、IOS）支持通过PPTP、L2TP VPN方式接入； | 1 | 套 |  |
| 2、支持国产化终端使用，包括中标麒麟、银河麒麟、深度OS等操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用（提供截图证明，或至少2家国产系统厂商与VPN产品的兼容性认证报告）； |
| 3、支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用； |
| 4、支持IPv6/IPv4协议下的网关模式、单臂模式、主备模式、集群模式的部署，支持资源访问优化，可以过滤网页广告、自动清除浏览器cookie、自动优化国外资源的访问等； |
| 5、产品应提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作； |
| 6、可针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果； |
| 7、产品应支持的密码算法包括：AES、AES192、AES256、DES、3DES、MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、DH、RSA ； |
| 8、本次配置SSL VPN授权≥10个； |
| 9 | 云互联网出口带宽（租用） | 1、支持将弹性IP添加到共享带宽: 支持20个弹性IP，支持弹性IP添加到共享带宽， 支持将不需要的弹性IP从共享带宽中移出，弹性IP移出后默认以移出前的共享带宽的带宽大小进行限速； | 1 | 套 |  |
| 2、支持流量监控：提供对共享带宽的上行流量、下行流量、上行带宽、下行带宽查询和监控。 提供对共享带宽中每个弹性IP的入网流量、出网流量、入网带宽、出网带宽的查询和监控。 监控告警: 支持对共享带宽设定告警规则，触发告警时发送邮件和短信通知； |
| 3、支持访问ipv6公网：支持IPv4/IPv6双栈云主机，可将云主机的双栈网卡加入共享带宽，访问IPv6公网并面向IPv6公网提供服务； |
| 4、本次配置互联网带宽≥100M的1条、可以开通为共享带宽供云端多个互联网 IP 使用，互联网带宽≥5M的8条； |
| 10 | 云异地备份（租用） | 需提供青海省外备份空间，备份空间合计≥12T，功能要求如下： | 1 | 套 |  |
| 1、支持文件、SQL Server、Oracle、MySQL数据库等在线备份，保障备份数据一致性； |
| 2、支持灵活的备份策略，可按分钟、小时、天、周、月自由设置计划任务； |
| 3、支持断点续传，网络中断恢复正常后可基于上一次中断处进行续传，无需用户干预； |
| 4、支持重复数据删除功能，降低上云的数据传输量，减轻带宽压力； |
| 5、支持SSL加密及AES-256位加密机制，保证数据安全性； |
| 6、支持对备份/恢复作业实现邮件告警通知。 |
| 11 | 互联网专线电路（租用） | 提供一条带宽≥200M互联网专线电路 | 1 | 条 |  |
| 12 | 安全网关（租用） | 1、电口≥6个，吞吐量≥ 300Mbps/500Mbps，并发连接数≥16万，最大用户数大≥750；2、支持DPI、DFI、节点跟踪、主动探测、加密分析等多种技术，对已经采用加密技术的P2P类应用比如BT、迅雷、Skype、eDonkey、Qvod、PPFilm、百度影音等精确识别；3、支持单条策略总控和单IP限速，可分别设置总控带宽和单IP带宽，可设置为一个具体的数值如50 kbits/s，也可设置为一个范围如10-100 kbits/s；4、支持TOP排名、流量组成、流量趋势图等网络概况呈现，支持记录微信ID、QQ号、IMEI等账号信息，支持1：1记录URL日志，并且支持按照应用协议、URL关键字、端口号、运营商等信息进行检索和查询；5、支持分析每一条会话的客户时延（设备到客户端的网络时延），服务时延（设备到服务器的网络时延），应用时延（会话上下行首包时间差），最大包长（会话上下行最大包的长度）。用于故障定位，故障定责；6、要求同时具备CNVD和CNNVD二级（含以上）认证，提供相关认证证书。 | 4 | 台 |  |
| 13 | 智慧监管用云pad服务 | 为实现便捷现场检查、开展日常市场监管任务，需提供配套智慧监管用云pad，配套智慧监管终端服务要求如下：1、需具备平板、云电脑双模式，处理器主频≥2.2GHz，屏幕≥10.95英寸，内存≥8GB，存储≥128GB，支持5G网络，支持WIFI，支持蓝牙5.0模块，支持通话功能；前后置摄像头 ≥500万像素；需预装Android 13及以上版本； 2、云电脑配置CPU≥4核，运行内存≥8G，系统盘≥80G，云电脑使用的操作系统及办公软件需完成正版化激活；3、提供≥80GB/月的移动流量； | 30 | 套 |  |
| **二、西宁市市场主体信息库及联动监管平台** |
| 序号 | 维护项目 | 维护要求 | 数量 | 单位 | 备注 |
| 1 | 基础服务 | （1）提供5\*8客服热线电话。（2）提供7\*24小时电话，现场受理市局提出的问题，利用电话、微信、QQ即时聊天工具对西宁市市场主体信息库及联动监管平台操作问题进行解答。 | 1 | 项 |  |
| 2 | 市场主体信息库与省局相关业务系统业务交换、联动保障服务 | （1）提供西宁市市场主体信息库及联动监管平台与青海省市场监管管理局相关业务平台的数据交互、业务联动技术保障，实现省、市业务上下联动、数据实时同步。（2）每日检查市场主体信息库的数据交换情况，包括与青海省市场监督管理局、西宁市大数据基础平台数据共享，对出现异常的交换进行处理保障数据正常交换。 | 1 | 项 |  |
| 3 | 日常巡检及问题反馈服务 | (1)系统相关例行性运行检查服务，定期检查相关业务系统的运行状态，并形成《日常巡检报告》；当出现异常时查找原因并解决问题。(2)接收西宁市市场主体信息库及联动监管平台软件的问题，形成《应用系统问题反馈单》反馈至公司运维项目组分析判断；针对软件缺陷类问题直接反馈公司运维项目组进行修正，涉及业务系统需求类问题反馈市局相关部门负责人。 | 1 | 项 |  |
| 4 | 系统更新服务 | 根据市局业务系统的《应用系统上线确认书》提供市本级应用系统更新、与其他应用系统的接口修改维护服务。 | 1 | 项 |  |
| **三、西宁市智慧市场监管平台** |
| 序号 | 维护项目 | 维护目标 | 数量 | 单位 | 备注 |
| 1 | 西宁市食品药品安全网络监管平台 | 食品经营监管系统、食品生产监管系统、药品经营监管系统、医疗机构监管系统、网格化监管系统、食品快检速查管理系统、食品追溯系统、价格监管等系统的运行维护服务，保证以上系统的正常运行，同时提高西宁市食品药品安全网络监管平台的整体服务水平。另根据日常维护的数据和记录，提供平台的的整体建设规划和建议，更好的为用户的信息化发展提供有力的保障。 | 1 | 套 |  |
| 2 | 西宁市食品药品远程非现场电子监管平台 | 对五区二县食品药品远程监管数据汇聚、存储、展示、分析等工作，同时需完成横纵向数据接入及共享工作，横向完成与西宁市各局委办市场监管数据的数据接入及共享，纵向完成与青海省市场监督管理局所需食品药品远程非现场电子相关数据的对接、共享，向下完成对所辖五区二县的食品药品远程非现场电子监管数据的接入工作。 | 1 | 套 |  |
| 3 | 西宁市食品药品监管大数据中心 | 全市食品药品监管领域的全量数据的运维工作，包含数据汇聚、数据开发、数据资源整合、数据资产管理与治理、应用支撑与数据服务、数据运营及安全管理等方面，最终形成不同维度的数据服务能力，为市场监管决策、精细化管理及创新应用提供支撑。 | 1 | 套 |  |
| **四、信息系统安全等级保护** |
| 序号 | 服务项目 | 服务要求 | 数量 | 单位 | 备注 |
| 1 | 系统测评服务 | 1、服务要求：提供系统等保三级测评服务。服务时间1年。（三级测评服务每年一次。） | 1 | 项 |  |
| 2、服务标准：网络安全等级保护测评要求（GB/T28448-2019） |
| 3、服务内容：等级保护测评内容包括但不限于以下内容a)安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面的安全测评；b)安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。 |