## 吉林省农业科学院官网上云服务项目

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **主要功能配置及技术参数要求** | **指标项** | **指标要求** | **数量** | **数量单位** |
| 1 | 云服务器 | 13台：2vCPUs| 4GB系统盘SATA 40GB数据盘SATA 40GB2台：4vCPUs| 8GB系统盘SATA 40GB数据盘SATA 40GB | 可用性 | 云服务器采用全冗余架构，无单点故障，平均可用性不低于99.9%。 | 15 | 个 |
| 数据可销毁性 | 服务提供商在用户要求删除数据或设备被弃置、转售前必须将其所有数据彻底删除，确保这些数据无法被复原，需提供最高级别的数据销毁，应包括但不限于数据覆写、硬盘消磁、硬盘分解等常见销毁手段。 |
| 数据可迁移性 | 用户能够自主控制数据的迁移；云服务商保证用户启用或弃用相关云服务时，数据能自主迁入和迁出。 |
| 数据私密性 | 云服务商应支持用户通过各种加密或隔离手段保证使用同一物理资源池的用户数据互不可见。不同用户的云主机至少要通过网络隔离的方式，保证同一云数据中心的用户数据互不可见，互不可访问。 |
| 数据知情权 | 按用户要求提供数据存储、备份的物理位置，并及时通知用户直接或间接使用了用户数据的事件以及实体信息。 |
| 数据可审查性 | 用户在必要的条件下由于合规或是安全取证调查等原因需要服务提供相关的信息：如关键组件的运行日志。数据的处置需遵守国家相应的法律法规，配合政府监管部门的监管审查。除以上情况外，服务上不应在未获得用户书面授权的情况下，删除用户数据，或将用户数据、个人信息等泄露给任何第三方。 |
| 宿主机硬件规格 | CPU主频性能不低于2.2GHz；内存最高支持768GB；数据盘存储容量不低于1200GB， IOPS SATA 最小 500/ 最大 2200/ 突发 2200 30 分钟；本机网卡不少于4个，网卡网速不低于1G。 |
| 故障迁移 | 具备HA功能，当某台物理机发生故障时，其上的云主机可以自动迁移到其它物理机上。 |
| 易用性 | 用户可通过云服务门户100%自助实现：购买、开通、释放云主机。  |
| 创建、管理、调整安放云主机的网络空间地址以及相应的NAT、路由、VPN等网络服务。 |
| 管理云主机的启动、关闭、重启，管理为云主机以及附属的外部存储快照的创建、销毁、恢复。 |
| 管理云主机安全组创建、释放、调整。 |
| 可通过可视化报表查看云主机的资源利用状况。 |
| 可通过可视化报表查看云主机存在的安全风险。 |
| 能够通过设置特定阈值自动触发警报，至少邮件和短信通知云主机存在重要问题（如：资源利用率长期过高、正在经受攻击、账户余额不足以自动续费等）。 |
| 根据用户的需求动态的创建、分配、释放、调整所用的计算、存储、数据盘、网络带宽等资源。 当云主机现有配置不满足要求时，用户可自主进行云主机配置快速升级，可升级配置包括： CPU、内存、数据盘大小和性能规格、网络带宽和网络位置等。 |
| 平台运维 | 7×24小时运行值班监控，应急支持。 |
| 2 | 共享带宽 | 30T | 网络服务 | 提供Region级别的带宽复用共享能力，不区分弹性公网IP类型及绑定实例类型，随时从共享带宽中增加或移出按需计费的弹性公网IP。 | 1 | 个 |
| 3 | 服务器安全 | 基于大数据威胁情报保障服务器安全，通过实时监控和批量修复漏洞、深度查杀网站后门、审计登录日志和定期安全基线巡检，维护服务器运行环境纯净，避免服务器数据泄露。 | 安全防护服务 |  全面细致的风险分析报告：自动化细粒度风险分析,包括如弱密码。 软件漏洞、web网站风险等等,定期报送安全专家将可视化报告。 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。 自内而外的监测防护：从服务器内部进行安全的监控与分析。 最高程度发现问题并第一时间对入侵进行响应与告警。 风险检测能力：扫描超过20000个漏洞，并且给出明确的漏洞验证处理方法。 实时分析发现反弹Shell；实时监控暴力破解行为，迅速通知并阻断恶意IP。 多维度Webshell检测，最大程度发现Webshell威胁。 | 15 | 套 |
| 4 | 日志审计 | 通过主被动结合的方式，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储。 | 安全防护服务 | 提供全局监视仪表板，可展示不同设备类型、不同安全区域的实时日志流曲线、统计图，以及网络整体运行态势、待处理告警信息等。对于目前暂不支持的审计数据源，需要提供方便灵活的扩展机制。系统对收集的各种日志进行范式化处理，将各种不同表达方式的日志转换成统一的描述形式。系统在安全审计员进行日常审计时，可将审计过程中选择的条件组合保存为策略。系统提供的混合检索技术属于交互式分析技术，提供基于范式化后的格式数据内容的实时关联分析和统计报表以及全文搜索能力。 | 1 | 套 |
| 5 | 云堡垒机 | 实现云上服务器的操作运维审计和账号权限管理。支持20资产和10并发。 | 安全防护服务 |  字符协议：SSHv1、SSHv2、TELNET。 图形协议：RDP、VNC。 文件传输协议：FTP、SFTP。 数据库访问：Oracle、SQL Server、DB2、Sybase、Informix、Teradata、MySQL、PostgreSQL。支持TELNET、SSH协议使用SecureCRT工具批量登录目标资源。支持对目标设备自动定期修改密码，特别是数据库协议（包括Oracle、SQL Server、DB2、Sybase、Informix、MySQL、PostgreSQL）。 | 1 | 套 |
| 6 | 云下一代防火墙 | 高可用性 (HA)、入侵防御 (IPS)、病毒过滤 (AV)、服务质量保证 (QoS) | 安全防护服务 | 支持在 VMware、KVM、XEN、Hyper-V等主流虚拟化平台上运行，可串联或单臂连接到虚拟网络中（如：虚拟应用服务器前端的网关，或者是VPC网络的边界网关），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 |
| 7 | 数据库安全 | 提供数据脱敏、数据库审计、敏感数据发现和防注入攻击等功能的，保障云上数据库安全的数据库安全防护服务。 | 安全防护服务 | 提供数据库审计、数据脱敏、细粒度权限控制、防SQL注入、数据库异常及脱库检测等能力，端到端保证数据库安全。 | 1 | 套 |
| 8 | 防病毒系统 | 具备反病毒技术、查杀性能、易用的操作界面，符合国内企业用户的安全习惯。 | 安全防护服务 | 边界防护：支持从文件落点进行监控；策略查杀：强制终端进行不可取消的病毒查杀策略；后台鉴定：支持收集无法鉴别的极特殊样本并由专业分析师确定样本属性后进行反馈；实时监控：可自定义设置系统监控及威胁处理方式；主动防御：只能判定风险等级并进行拦截。 | 1 | 套 |
| 9 | 态势感知 | 利用大数据分析技术，对攻击事件、威胁告警和攻击源头进行分类统计和聚合分析，呈现安全攻击态势。 | 安全防护服务 | 能够检测操作系统、中间件、弱密码、主机、数据库、账号配置存在的风险，也能够检查云产品上身份认证、访问控制、日志审计、数据安全、基础防护五方面的配置，并提供修复建议。 | 15 | 套 |
| 10 | 数据迁移上云 |  | 数据迁移服务 | 支持服务器工作负载初始复制迁移阶段：分别进行试点实施和批量实施工作；支持服务器工作负载最终同步迁移阶段：分别进行试点实施和批量实施工作。支持迁移后目标云主机系统和应用验证。支持迁移后目标云主机正式上线运行。 | 1 | 套 |