|  |  |
| --- | --- |
| 服务器 | 一、硬件要求： 1、单台硬件配置要求：CPU配置不低于2颗intel(R) Xeon(R) Gold 6326 ，内存容量1T，系统空间≥2块240GB SATA SSD、缓存空间≥2块1.92T-SSD-新（混合型）、存储空间≥6块8T SATA，配置4千兆电口+2万兆光口； 2、要求预装服务器虚拟化软件，确保设备上架时的便捷性； 3、要求桌面云一体机可以组成HA集群环境，支持虚拟机热迁移技术，可在桌面业务不中断的情况将虚拟机运行位置更改至其他虚拟机节点，保障业务连续性； 4、支持与现有市场上的支持Intel VT processors技术的主流X86服务器共同组建桌面云集群； 5、为了保证能够快速平滑扩容，要求集群中服务器的添加支持热添加，在添加过程中不影响运行中的虚拟机； 6、支持在线的虚拟机热迁移动能，实现虚拟机在集群之内的不同物理机上热迁移，保障业务连续性。  二、存储虚拟化软件要求： 1、本项目要求所提供的存储虚拟化授权无容量限制，满足桌面云数据存储空间的扩容需求； 2、支持SSD缓存加速，采用SSD+HDD混合模式，SSD用于缓存热点数据，HDD用于存储个人数据，SSD缓存命中率不低于50%，确保最优用户体验； 3、支持故障自动切换，硬盘故障，存储则会被重新指向另外一台服务器上可用的数据副本，实现毫秒级切换，对用户来讲基本是无感知的；主机或者网络故障，虚拟桌面可以快速切换到另一台服务器拉起，平均切换时间最多为5分钟；  4、支持UPS QoS（UPS联动），为尽可能保障数据中心断电场景下的业务，可在市电断电时通过UPS临时供应电量，当UPS电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机。（需提供产品功能截图，并加盖投标人公章）  5、支持数据冗余副本技术，每份数据同时写入多台服务器，每次数据变化时自动实时同步，确保磁盘或服务器故障，数据不丢失；  6、为避免主机假死导致系列问题发生，支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险。（需提供产品功能截图，并加盖投标人公章）；  7、提供基于PowerShell的CLI命令行功能，通过PowerShell脚本可简化用户运维操作。（提供产品功能截图或命令行说明手册，并加盖投标人公章）  8、支持全局热备盘技术，管理员可配置在集群中保留多块磁盘作为热备盘，分布在不同主机上，当任何一台主机的任意一块硬盘出现故障后，会自动选择其中1块热备盘进行替换和重建； 9、支持主机和磁盘故障后不停机替换；  10、当扫描到物理主机的内存条出现ECC CE和UE错误时，能够将对应内存空间进行隔离并定位故障内存的槽位，减少硬件问题对业务的影响。（需提供产品功能截图，并加盖投标人公章）。  三、虚拟化管理接入授权： 1、支持PC、笔记本电脑（含Windows操作系统和MAC笔记本）、瘦终端（含ARM和X86）、iPad、iPhone、Android移动终端等设备接入访问虚拟桌面；本次提供10个接入授权； 2、支持管理员可自定义设置加速应用进程、降速应用进程，以及算法推荐的优化项，对已运行应用的CPU和内存进行实时优化，有效提高虚拟机资源利用率；（提供功能界面截图并加盖投标人公章） 3、支持虚拟机扩容审批功能，用户虚拟机配置变更申请提交完成后，需要管理员进行审核；（提供功能界面截图并加盖投标人公章） 4、支持对个人磁盘加密，保障个人稳私安全；（提供功能界面截图并加盖投标人公章） 5、支持在桌面云管理组件中内置应用控制技术，实现基于黑名单或白名单策略的桌面应用管控，当启用应用控制时，桌面虚拟机将无法运行黑名单列表中的应用程序或无法运行除操作系统必要程序与列表中之外的任何应用程序，并且内置的应用程序规则至少200条； 7、支持虚拟机回收站功能，避免误操作导致虚拟机数据丢失，当虚拟机删除后，会自动进入回收站，支持恢复到原位置，可设置回收站自动清理时长； 8、为了提高平台安全性，平台需内置防火墙，包括设置过滤规则、NAT设置、访问监控、防DOS攻击、QOS上传下载规则等； 9、支持客户端准入检测，可根据用户接入的终端类型、操作系统版本、接入IP和时间、软件安装情况等条件设置接入访问策略，如客户端不满足安全检测要求则不允许接入； 10、支持在控制台查看用户虚拟机的CPU、内存、磁盘的详细情况，且CPU、内存支持正反排序，磁盘支持按比例的大小进行正序和反序排序。  四、安全杀毒软件要求：  配置10个虚拟机安全软件授权，同时应满足以下需求：   1. 云安全中心需集成于虚拟化平台中，一体化方式交付，无需第三方平台承载，平台必须能够提供虚拟主机安全防护安全能力,并对检测到的恶意活动可采取分布式防火墙隔离虚拟机、为虚拟机拍摄快照等防护手段（需提供产品界面截图，并加盖投标人公章） 2. 要求配置按CPU颗数的安全虚拟化授权，授权可随虚拟机数量增加而弹性扩展。 3. 支持虚拟化平台自动安装安全组件进行虚拟主机防护（需提供产品功能截图，并加盖投标人公章） 4. 可通过至少4个以上杀毒引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率，并提供一键威胁处置 5. 提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品功能截图，并加盖投标人公章） 6. 支持对Windows终端的漏洞情况进行扫描，用户查看漏洞具体情况及KB号，支持一键批量修复并显示具体修复情况 7. 支持防暴力破解，统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置，支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史。 |