中国医学科学院肿瘤医院

安全桌面

技术需求

**信息中心/计算机室**

**2017年8月**

目录

[中国医学科学院肿瘤医院 1](#_Toc491932239)

[安全桌面 1](#_Toc491932240)

[技术需求 1](#_Toc491932241)

[一、 项目概述 3](#_Toc491932242)

[二、 技术要求 3](#_Toc491932243)

[2.1系统配置 3](#_Toc491932244)

[2.2详细要求 3](#_Toc491932245)

[2.2.1桌面云一体机 3](#_Toc491932246)

[2.2.2瘦终端 9](#_Toc491932247)

[2.2.3运行环境控制软件 10](#_Toc491932248)

[三、 服务 10](#_Toc491932249)

# 项目概述

我院目前已经建成使用的信息系统数量众多，各系统的开发厂商都不尽相同。系统在运行过程中，需要大量的运维工作。在处理故障问题时，目前各厂家的运维方式包括：到场处理、电话处理与远程接入处理。

目前的主要问题是远程接入处理这种方式。运维人员会用一台终端将我院内网与互联进行连接，从而达到远程接入管理方式。这存在以下几点问题：

1. 破坏内网隔离环境，增加入侵风险；
2. 运维人员使用的终端不受管理，容易造成信息泄漏；
3. 运维终端环境没有保障，增加病毒传播可能性。

针对以上问题，现计划建设统一的接入平台，解决因私联内、外网导致边界不清的问题；提供受控的安全运维桌面供运维人员使用，全面防护运维环境。从而实现对远程接入方式的统一管理。

# 技术要求

## 2.1系统配置

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 配置描述 | 数量 |
| 1 | 桌面云一体机 | 支持发布专有桌面、还原桌面、池化桌面、共享桌面、远程应用至少5种桌面资源，千兆网口6个、冗余双电源。15个以上并发授权. 实现桌面云一体机的系统部署与管理。 | 2台 |
| 2 | 瘦终端 | ARM四核1.6Ghz、内存1G、存储4G、USB接口6个、1个VGA/HDMI、1个以太网口、1对音频口。 | 5台 |
| 3 | 运行环境控制软件 | 针对全系统环境（系统文件、应用软件、文档等）的运行权限进行管理，保持桌面环境可信，操作动作可信。 | 1套 |

## 2.2详细要求

★为重要指标项，其它为一般指标项。

### 2.2.1桌面云一体机

|  |  |
| --- | --- |
| **技术指标** | **具体参数** |
| **硬件规格** | ★CPU核数≥6（主频不低于2.4Ghz）、内存≥96G、千兆网口≥6个、冗余双电源。  ★本项目要求至少配备1块64G SSD硬盘、1块120G SSD硬盘和4块2T的SATA硬盘。 |
| **配置要求** | ★本项目要求提供15个VDI用户授权，支持发布专有桌面、还原桌面、池化桌面、共享桌面、远程应用至少5种桌面资源，满足不同场景的应用需求。 |
| **部署模式** | 为了简化部署环节，本项目要求桌面云控制器所有组件完全集成化，不需要过多的安装调试步骤，后台导入一个镜像就可以完成部署，提升上线效率。  ★支持双机（主备）和集群（主主）2种模式，如果选择集群模式部署，要求桌面云控制器宕机切换会话不中断。  支持分布式部署、集中管理模式，桌面云服务器部署在各个分支本地数据中心，总部通过一套集中管理平台实现对分支桌面云的统一管理，包括统一授权、统一升级、统一监控等，提供集中管理平台所需软件。  ★内置DHCP功能，部署时无需额外搭建DHCP服务器。  ★要求自带SSL VPN功能，不要借助第三方设备。 |
| **用户体验** | 支持PC、笔记本、云终端（含ARM和X86）、iPad、iPhone、Android移动终端等设备接入访问虚拟桌面。  支持Windows XP/7/10、iOS、Android、Linux等客户端操作系统。  支持Windows XP/7/10、Windows Server、Linux等虚拟桌面操作系统。  ★支持池化桌面，该模式下虚拟机不固定关联给用户，当用户需要时从桌面资源池中随机获取一个闲置虚拟机，退出后自动归还（即还原到“未关联用户状态”），其他用户仍然可以使用。  支持PC磁盘映射，即PC本地硬盘可直接映射到虚拟桌面上使用。  PC（或笔记本）接入虚拟桌面支持通过导航条或快捷键切换为窗口化模式，用户可随意改变窗口大小且分辨率会自动适应。  ★支持USB外设映射，兼容高拍仪、扫描枪、扫描仪、摄像头、密码小键盘、指纹收集器、身份证读卡器、手写板、打印机、USB-key等不同外设。  ★支持云盘存储方案，包括个人云盘和公共云盘，可设置配额和读写权限，其中个人云盘绑定用户，只允许特定用户访问，公共云盘允许所有人访问。  支持本地、AD域等多种情况下的单点登录，用户登录VDI客户端和虚拟桌面操作系统只有1次账号密码输入动作，保持和PC使用习惯一致。  ★支持联动关机，用户可以跟使用PC一样，打开操作系统“开始”菜单、点击“关机”按钮，云终端和操作系统将会一体化关闭，没有多余的操作步骤。  支持显示虚拟机开关机画面；支持分辨率自适应和更改分辨率，操作时要求与PC一样，即在桌面右键点击“个性化分辨率”进行设置。  支持桌面会话保持功能，在多桌面切换、更换不同终端接入、临时性网络中断（自动重连）等情况下，用户重新登录后不会影响原先的桌面操作行为。  客户端连接虚拟桌面无需依赖虚拟机IP，具体表现为禁用虚机网卡或者随意更改IP，桌面会话不会中断，VDC可以正常下发策略，用户可以正常办公和播放视频，避免因误操作而导致业务中断。  ★支持视频重定向，视频文件不在服务器解码，直接重定向到终端本地解码，提升播放体验，能够兼容Media Player等。  ★针对广域网接入虚拟桌面的场景可配置缓存级别、有损压缩比率、启用帧控等策略，降低流量、提升体验。 |
| **运维功能** | 支持模板链接克隆，克隆时可指定虚拟机数量、运行位置、存储位置、网口信息、磁盘大小，本项目要求100个虚拟机派时间不超过5分钟。  支持在原磁盘上扩容或添加新的磁盘，扩大磁盘容量。  支持模板升级，可以统一安装所需要升级的软件/补丁，一键更新到对应的虚拟机，满足标准化场景的软件和补丁更新需求。  ★支持软件分发，通过创建软件库并关联给虚拟机，实现应用软件、驱动程序的增量式更新，不需要在每个虚拟机执行安装过程，整个分发过程秒级完成，且分发后不会覆盖原虚拟机的个性化配置和自主安装的软件，本项目要求支持应用软件、USB打印机和网络打印机驱动、网页快捷方式和页面控件、办公文件的分发。  支持批量完成如下配置：创建用户、删除用户、禁止/踢除用户、关联虚拟机、导入导出用户、用户分组。  支持删除用户时，可选择是否删除关联的虚拟机，如果不删除，虚拟机处于闲置状态，可重新关联给其他用户。  支持虚拟机自由分组、支持修改计算机名称、支持虚拟机名称搜索。  支持批量删除虚拟机、批量设置虚拟机IP地址、批量关联/解关联虚拟机用户。  支持开机状态下编辑虚拟机配置，重启生效。  ★支持外置数据中心报表功能  支持升级前和升级后的健康检查，确保升级不出问题。 |
| **安全管理** | ★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。  ★支持USB黑白名单技术，能够精准识别每一款不同类型的外设（包括高拍仪、摄像头、USB光驱、认证key等），并设置放通或者限制策略，提高管控粒度和安全性。  ★支持多种认证方式随需组合，包括本地账号密码、usb-key认证、短信认证、硬件特征绑定、动态口令、ldap认证、raduis认证、AD域认证等多种方式，满足不同级别用户的安全接入需求。  ★支持设置首次登录强制修改密码、定时修改密码、图形校验码和软键盘等密码安全策略，以保障认证密码安全性，避免越权访问行为。  ★支持不同用户通过不同地址接入虚拟桌面，适用于互联网访问场景，可以指定特定账号在外网访问桌面云，而其他用户只能在内网访问。  ★支持U盘、PC本地桌面到虚拟桌面这2种情况的双向拷贝管控，可控制U盘的只读和读写权限，可控制本地桌面和虚拟桌面双向拷贝、单向拷贝。  ★支持录屏审计，提供用户的所有桌面操作行为审计（录像），帮助管理人员查看内部操作人员是否符合操作规范性，以及既定的规则要求，适用于对敏感岗位进行责任认定和授权管理。  支持虚拟机快照技术，当数据误删或系统故障时可实现回滚，快照只保存增量数据，节省存储空间。  ★桌面云控制器内置防火墙，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。（提供功能截图）  兼容国内外多款虚拟化防病毒软件，防止虚拟机中毒。 |
| **其他要求** | 为确保身份认证、传输加密、存储加密、加密算法等技术的高安全性，本项目要求桌面云厂商具备国家级别的商用密码产品生产资格和信息安全服务资格，投标时需提供相关的资质证书（至少2种）。  本项目要求所投桌面云产品厂商具备CMMI5证书，确保桌面云软件开发成熟度。  ★桌面云平台包含桌面云终端、桌面云控制器、桌面云服务器、服务器虚拟化、存储虚拟化总共5个重要组件，为保障产品兼容性，避免售后服务互相推诿，本项目要求以上组件统一品牌。  为证明本次采购桌面云产品的稳定性，需提供所投产品案例合同复印件，要求一次性采购规模高于1000用户的合同2份、一次性采购规模高于2000用户的合同2份，并且还需要提供所投产品用户盖章使用报告5份。  ★本项目要求所有组件提供3年原厂服务，并且所投桌面云产品厂商在本省有分公司/办事处，投标时提供售后服务ISO9001资质证书。 |
| **功能支持** | 支持服务器端口汇聚技术（管理口、业务口、存储口），将多个网络端口聚合起来，提高网络带宽和容错能力。  支持虚拟机集中备份与恢复，可按需选择多个虚拟机或全部虚拟机备份至外置服务器（NAS、FTP、CIFS等），支持设置备份策略，实现全自动化备份。  支持自动/手动将配置文件备份到FTP服务器。  虚拟机损坏无法启动时，支持将虚拟机磁盘挂载到新虚拟机上，用户可登录新虚拟机将磁盘内容备份出来。  支持数据冗余副本技术（双副本、三副本），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。 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60%，确保最优用户体验。  支持磁盘故障自动重建技术、支持磁盘横向/纵向扩展。  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，约3-5分钟。  ★支持主机和磁盘故障后不停机替换。  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。 |

### 2.2.2瘦终端

|  |  |
| --- | --- |
| **技术指标** | **具体参数** |
| **数量要求** | ★本项目要求配备5台云终端，与桌面云软件、服务器同一品牌。 |
| **硬件规格** | ★ARM架构，CPU≥四核1.6Ghz、内存≥1G、存储≥4G、USB≥4个、1个VGA或HDMI、1个以太网口、1对音频口。 |
| **其他要求** | 采用嵌入式操作系统，比如Android、Linux。  云终端权限管理：支持配置是否允许显示本地桌面和是否允许安装应用、支持开启“修改云终端配置和登录信息需要密码”功能、支持配置是否允许新的云终端接入或者接入需要密码。  云终端易用性管理：支持配置自定义开机画面、支持云终端分组管理、支持配置云终端定时开关机计划、支持开启“云终端加电自启”功能、支持配置是否自动下载并安装更新、支持批量移动/删除/关闭云终端、支持配置是否允许自动登录和保存密码。  通过CCC产品质量管理认证、节能环保认证。 |

### 2.2.3运行环境控制软件

|  |  |  |
| --- | --- | --- |
| **功能分类** | **技术指标** | **详细描述** |
| **安全功能** | **程序白名单生成方式** | ★支持MD5等hash算法或数字签名 |
| **可执行文件支持** | ★支持对PE等格式的可执行文件运行控制  ★非程序白名单中的可执行程序不能被系统运行 |
| **支持操作系统** | 支持WindowsXP、Windows7、Windows8、Windows10  支持Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016等  支持中标麒麟、Ubuntu Kylin、Suse、Redhat等 |
| **程序白名单自身安全** | 程序白名单本身采用数字签名保护机制，防止被篡改 |
| **管理** | **审计** | ★要记录对可执行程序的控制结果，包括被允许执行或被拦截不被执行的可执行程序文件名、结果、调用进程、时间等  所有对程序白名单的管理维护操作都要被系统审计，并保存日志记录 |
| **配置能力** | 支持管理人员对程序白名单的增删查改 |
| **第三方认证鉴定** | **防病毒功能** | 提供计算机病毒防治产品检验中心提供的产品检验报告、并判定为合格品 |

# 服务

提供原厂三年免费服务，包括软件升级，硬件质保，现场技术支持服务，永久电话支持服务。