中数国科云桌面
技术白皮书

2023 年 8 月

目 录

1. 背景介绍

企业信息化建设过程中，到目前为止国内客户几乎还是采用传统 PC 的办公模式，越来越多的企业在 PC 的生命周期中出现了诸如运维工作量大、数据安全无法保障等一系列问题。

“瘦终端+云桌面”是快速兴起的技术潮流，通过将用户桌面在数据中心集中化运行和管理，极大地降低了运维难度并提高了数据的安全性，同时实现了用户桌面在各种终端上的任意切换。越来越多的企业开始接受桌面虚拟化技术来实现企业的桌面基础架构。它通过桌面虚拟化技术在一台性能强大的服务器上虚拟出若干台虚拟机，用户或管理员可以在该虚拟机中安装操作系统、应用程序等，管理员可以根据需要将一台或多台虚拟机分配给一个或多个用户，而用户桌面上不再需要部署性能强大的 PC，而只要部署一台安全、易管理的云计算终端就可以连接到数据中心的虚拟机并使用该虚拟机，通过网络把服务器端的虚拟主机传输到客户端并展现给最终用户。

通过“瘦终端+云桌面”的方式，中数国科桌面云平台为用户提供一站式的桌面虚拟化解决方案，大大简化了桌面的部署和管理。通过节省操作费用和提高灵活性来降低桌面管理成本，同时提供给最终用户熟悉的 PC 使用体验，企业级别的桌面可靠性，数据保护和灾难恢复能力。

因此，顺应市场潮流，中数国科推出桌面云解决方案，对 IT 桌面基础架构进行变革，通过丰富、完善的云桌面技术，提升企业在数据安全建设、终端用户体验、业务连续性等方面的价值，让企业充分享受虚拟化技术所带来的优质体验。

2. 传统桌面办公面临的挑战

2.1. 桌面运维复杂化

传统办公模式将员工的工作环境绑定于 PC 上，当个人电脑出现故障后，需要 IT 维护人员亲临现场，对电脑进行系统修复和重新配置，而在整个 PC 生命周期中，如此繁琐的工作是非常多的，使得 IT 管理员的工作量巨大；加上复杂的桌面运维工作比较消耗时间，往往导致响应能力不足，影响员工的工作效率。

同时，企业中 PC 一般每 3 到 4 年就需要更新替换，也即是说，复杂的桌面

运维工作，每过三四年时间，这样的过程还要继续重复。因此，在 IT 应用环境日益复杂、人员有限的情况下，如何保证服务质量，如何摆脱“救火队”的角色，而给各部门提供高效的IT服务以及良好体验已然成为IT部门致力于发展的目标。

2.2. 总体拥有成本高

虽然 PC 采购成本相对较低，但是无法抵消高昂的管理和支持成本。目前，PC 的管理工作主要包括对操作系统环境、应用的安装配置和更新、桌面日常维护等，且随着应用的增多，维护成本呈不断上升增长趋势。

另外，随着企业中传统 PC 的不断增加，耗电量、制冷、空间等问题已经逐渐凸显出来。以耗电量为例，假设员工使用的是一台普通 PC，一般工作状态下功率为 200W 左右，液晶显示器大概 50 瓦左右，按照一天开机时间为 9 小时，一年工作时间为 264 天，那么该普通 PC 一年的耗电量大概是 250W×9h×264 = 594KW。如果算上空调、空间等因素，运营成本是非常高昂的。

2.3. 数据安全保障难

传统 PC 模式下，PC 数量众多并且核心数据都存储于本地，随着系统安全隐患日益增多，PC 往往成为数据安全风险集中爆发的地方。再者，传统 PC 模式难以对移动存储等进行限制，难以防止数据外泄。加上近年来主动及被动的安全泄漏事件日益上升，而这种安全事件对企业形象和核心竞争力的影响是巨大的，如何有效解决终端主动及被动数据泄漏事件等安全问题一直困扰着 IT 部门。

企业中的开发部门由于其业务特殊性，对开发环境和文档管理环境的安全性要求非常高。为了支撑业务的飞速拓展，在开发项目中往往还会牵涉到很多第三方公司和外包项目，甚至于开发人员需要在任意地点进行办公，这对开发系统的安全构成了极大的挑战。因此，需要有一套安全的桌面开发环境，能够让开发项目的员工及外包员工在受控的办公桌面环境下，进行相关应用的开发和调试，同时能有效保护应用代码及企业数据的安全。

2.4. 办公地点固定化

随着移动互联网的技术潮流，企业的办公环境也不再局限于固定工位，而是

需要能够随时随地访问统一的桌面、应用和数据，通过为员工打造桌面随身行的办公平台，可以更好地提升工作效率。但是，传统 PC 办公方式将办公位置固定化，无法实现桌面环境与用户绑定（随身桌面），影响用户体验和工作效率。因此，如何满足随时随地桌面、应用的接入，并兼容各类终端设备，从而实现移动化价值，是信息化建设的趋势。

总而言之，新型办公模式衍生出“简化管理、数据安全、移动办公”三大需求，为了应对桌面运维的挑战，并更好满足客户需求，“瘦终端+云桌面”替换传统 PC 势在必行。

3. 桌面云产品简介

3.1. 产品概述

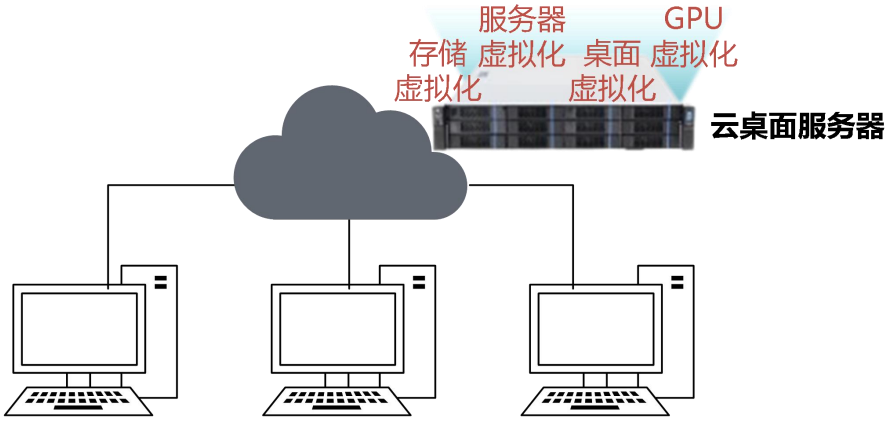
通过虚拟化技术，中数国科云桌面将桌面、应用和数据从传统 PC 本地转移到数据中心进行集中管理。在数据中心，我们采用桌面云一体机，利用超融合技术将服务器的 CPU、内存和存储资源根据用户需求虚拟化为独立的桌面虚拟机。通过桌面交付协议，操作系统界面以图像形式传送给用户的接入设备，构建了与传统 PC 相似的桌面环境。由于数据集中存储在后端服务器，终端设备无需保存数据，因此实现了较高的数据安全性。此外，由于桌面统一运行在后端，可以通过统一界面进行维护，提高了管理和维护的效率。用户只需具备网络连接，便可随时随地通过各种终端设备登录云桌面进行办公。

3.2. 平台架构

企事业单位中，不同员工对桌面的需求是不一样的，有些需要简易、标准化的桌面，有些需要高性能、个性化的桌面，有些可能仅需通过访问个别应用程序进行移动办公。利用中数国科桌面交付技术可以满足多种类型的桌面，实现具备灵活性、安全性、可扩展性的一站式桌面云解决方案

中数国科整体桌面云方案是由云终端、虚拟桌面控制器、服务器存储设备等组成，实现将企业员工的办公桌面统一部署于服务器上，员工的个人数据也集中存储，然后通过网络将个人桌面系统快速交付给员工，员工可以通过各种不同类型的终端设备如瘦客户机、笔记本、手机及平板等随时随地接入办公，打造一种

新型的桌面办公模式。



3.3. 平台组件

中数国科桌面云平台以独享桌面的形式，将桌面作为一种按需服务随时随地交付给任何用户，利用独特的桌面传输协议，可以快速而安全地向企业内的所有用户交付整个桌面，不管他们是固定办公员工，还是移动办公员工。平台核心组件如下：

虚拟机管理平台：构建硬件资源可动态调度的服务器集群环境，通过虚拟机可承载 Windows 和 Linux 桌面操作系统和应用，实现桌面池的统一管理和性能监控。独有的集群架构，可以登陆到任意一台服务器对整个集群进行管理，从而保证了管理平台的高可用性。

虚拟桌面控制器：内置服务提供集中式的桌面用户认证，自动化的桌面管理，进行创建、更新、还原虚拟桌面等操作。在不依赖于虚拟机的网络情况下将虚拟桌面安全，快速，可靠地交付。

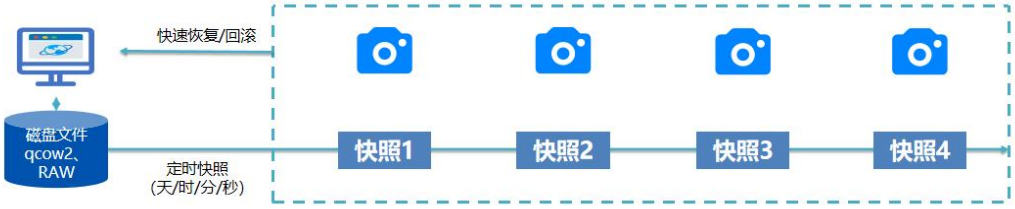
云终端：无论是体积小巧，功率低的瘦客户机，还是 PC 机，笔记本，智能终端，都能作为云终端的软件载体，随时随地连接到虚拟桌面进行办公应用。

3.4. 平台特性

3.4.1. 云桌面快照

当云桌面磁盘数据被误操作删除时，利用之前创建的快照，可以快速而准确地回滚到任一快照时的数据状态。例如：

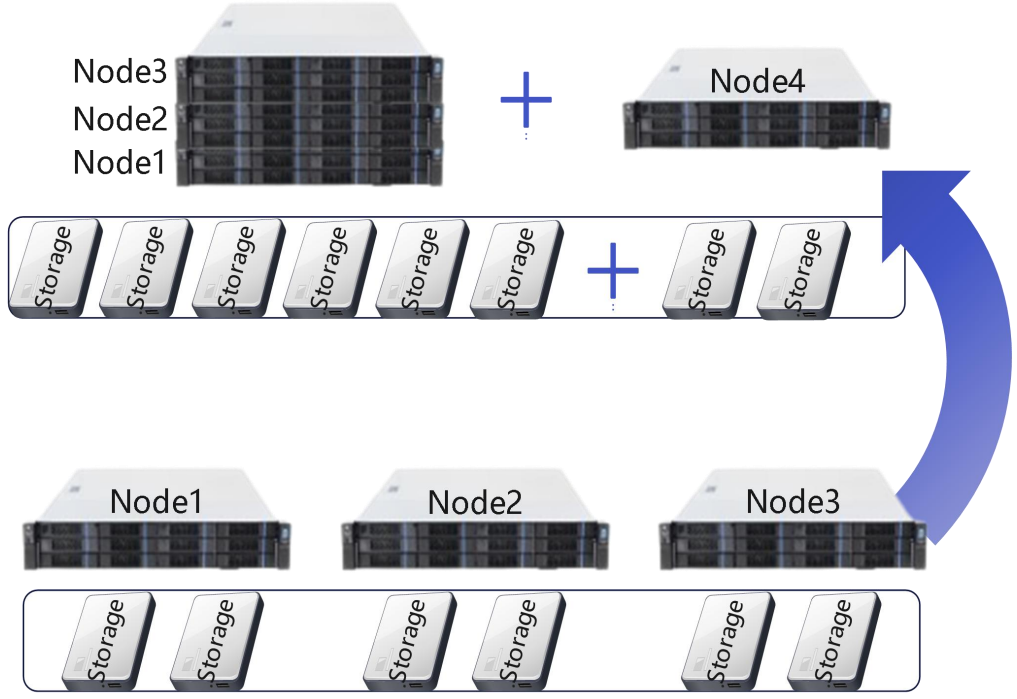
- 云桌面变更失败；
- 误删除操作；
- 遭受病毒攻击等；



3.4.2. 云桌面资源灵活扩展

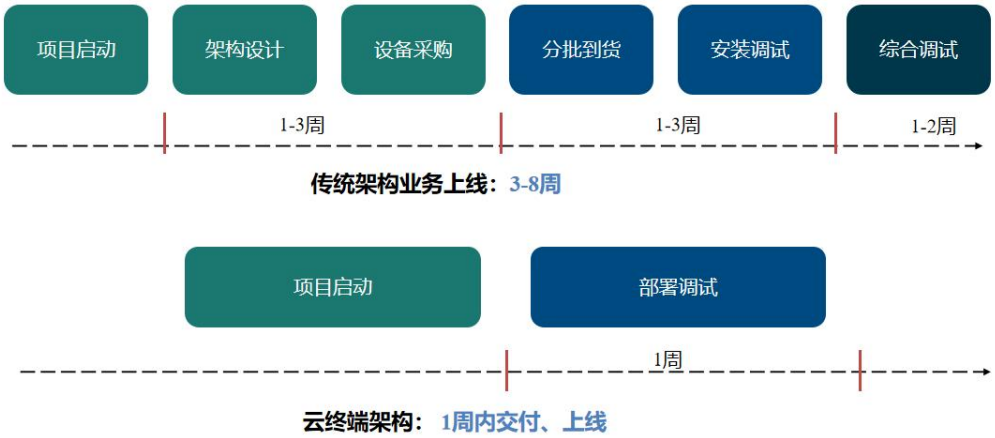
云桌面服务器部署基于超融合部署架构，有效保留了该架构的弹性拓展能力使得企业可以根据实际需求灵活地调整资源，快速适应业务变化，提高资源利用率，降低成本，并实现更加高效的 IT 运维管理。

- 不停机在线增加节点；
- 不停机在线扩展容量；
- 按需动态分配资源，实现资源灵活配置和分配；



3.4.3. 快速部署

快速交付、简单高效。



3.5. 平台优势

集中管理统一运维：

- 通过 Web 图形化界面统一运维管理集中到数据中心的所有桌面。
- 利用虚拟化模板克隆、复制等技术快速创建桌面，提高效率。

安全可控：

- 基于超融合架构，支持多种快照、复制、HA、备份等策略，数据随时安全可控，业务零中断。
- 终端设备可选择性映射、可选择开放粘贴板复制方向和复制内容（文字/文件）。

移动桌面：

- 只要满足网络可达的前提，用户可以使用云终端、PC 和 PAD 等设备接入虚拟桌面，实现随时随地办公的无缝衔接。
- 移动桌面，数据集中存储，终端零数据，多种备份策略，避免有意、无意删除系统或破坏数据。

降低企业 TCO：

- 统一管理简化运维方式，节省人力成本；低功率瘦终端降低电力成本。
- 硬件生命周期较长，降低整体折旧成本，且可实现按需拓展。

3.6. 方案价值

完善的全系列云方案：涵盖瘦终端、虚拟桌面控制器、虚拟机管理软件三大环节，方案最全面，兼容性最好，性价比最高，为 IT 提供了一种更加精简和安全的方法来管理用户和提供可按需访问的敏捷桌面服务。

卓越的用户体验：针对各种应用场景进行性能调优，高效传输协议 SRAP 提升 6 倍以上的速度，将访问带宽降至最低，达到与传统 PC 一致的访问体验。并且利用瘦终端架构内置的高清视频协议处理器可流畅播放 1080P 高清视频。

更全面的安全保护机制：高达 8 种身份认证方式自由组合以保障用户接入安全，全方位的加密算法保障传输安全，灵活访问控制进行集中鉴权，数据存储加密保障个人数据安全，最终实现端到端桌面云安全保护。

集中式 WEB 管理模式：整套方案的搭建仅需两大组件，相对业界其他厂商其部署组件最少，并可提供集中式、单一化的远程运维模式，提高了虚拟桌面部署的易用性和可维护性。

4. 平台亮点解析

4.1. 绝佳的用户体验

4.1.1. 高清视频体验

桌面云方案允许在虚拟桌面中查看或编辑图像和多媒体信息，且可以支持 1980*1200 分辨率和 32 位彩色桌面显示。另外，传统桌面虚拟化方案在播放高清视频时主要采用服务器解码和播放，然后将变化中的图像按帧传输给前端显示设备，但这种方式对服务器性能要求高，且非常占用带宽资源，往往效果不好。而中数国科提出音视频重定向技术，将 1080P 高清视频流在服务器上进行编码和压缩，然后直接传输到前端设备，利用基于高清视频处理器和本地解码技术流畅地播放高清视频，给客户带来极佳的视频观看体验。

4.1.2. 单点登录技术

客户有可能使用多个虚拟应用程序或 Windows 虚拟桌面，而每套应用系统

或桌面系统都会有单独的身份认证措施，一般情况下是需要多次认证才能正常办公，这种工作非常繁琐且容易出错，影响工作效率。为了提升终端用户的满意度，引入单点登录技术，在通过严格认证之后，无需再次进行虚拟应用和虚拟桌面的认证，采用“一键化”模式开启桌面和应用的操作界面。目前支持 BS 类型的远程应用和 Windows 虚拟桌面的单点登录功能，实现多系统和多桌面整合，避免用户重复输入账号或口令的繁琐操作，提升员工工作效率和操作满意度。同时，对已经开启了单点登录的虚拟应用程序，用户可在登录成功后在个人设置中对这些应用进行单点登录帐号、密码自设定，所设置的数据将以加密的方式进行传递，并对管理员不可见，保证用户帐号的安全性。

4.1.3. 自动化桌面部署

在 DHCP 环境下，用户使用瘦终端，可在无人指导的情况下，快速接入云桌面，实现即插即用的终端操作体验。另外，相对传统 PC 上线前需要经过硬件采购、系统安装、桌面运维等一系列的繁琐、复杂的过程，在部署好桌面云平台之后，管理员可以通过虚拟机模板来快速、自动地为新用户派生虚拟桌面，同时管理员不仅可在控制台查看用户虚拟机的 CPU、内存、磁盘的详细情况，还可以对用户虚拟机进行开机、关机、挂起、重启等电源级别操作。当用户虚拟机出现故障后，管理员既可以通过新的虚拟机模板进行快速替换，也可以在控制台远程接入用户虚拟桌面，协助处理系统故障问题。

4.1.4. 高效 VDX 协议

VDX(Virtual Desktop eXtend, 虚拟桌面扩展协议)是面向 VDI 架构定制化桌面访问而专门打造的的一种优化连接协议，旨在克服现有桌面访问协议(RDP/ICA/PCoIP/SPICE etc.)在虚拟桌面架构环境下，与传统 PC 桌面功能缺失与体验差距的弱点，包括视频多媒体流畅度及外设支持等方面。目前主流桌面访问协议都是在 VDI 架构诞生之前而设计的，并没有考虑周全 VDI 桌面访问过程中所特有的场景需求，而 VDX 协议则是专门为 VDI 架构量身打造，解决了视频多媒体播放和多种外设支持等重点问题，并学习和借鉴了 RDP 和 SPICE 开放协议的优点，整合成为一种更加适合 VDI 部署的协议，提供更优化的带宽，更好的

用户体验，更加类似于传统 PC 的外设支持。

具体特性如下：

1、高效的视频识别及编码效率。要想达到流畅的视频效果，同时能够承载更高的虚拟化密度，那么必须采用高效的编码算法。VDX 协议通过优化 MJPEG 编码中的耗时部分，能够显著的提示算法的效率，从而得到流程的视频体验。

2、动态的视频帧率调整。在 VDX 协议中将会一直探测网络时延和带宽情况，同时客户端将发送视频播放的情况的反馈，于是根据不同的播放情况和网络情况调整对视频的编码帧率，从而更适应网络带宽，得到更流畅的视频体验。

3、高性能的图片压缩算法。在虚拟化的协议中，无论是 RDP、ICA 还是 PCoIP 等，都无可避免的需要传输一些图片，而对图片格式的选择将无疑产生重要的影响。大部分的图像选择 bmp 或者 jpeg 的格式进行传输，VDX 协议借鉴了 JPEG2000 标准中的算法，在原有 JPEG 的基础上提升 30%以上的压缩率，同时支持有损和无损压缩算法，并且能够对图片进行渐进传输，同时能够在图像和视频压缩直接平滑的进行切换，减少因切换不同压缩算法切换导致的图像抖动。

4、图像缓存。对于操作一些渲染操作比较多的动作来说，例如 photoshop 等画图软件时，由于产生了大量的渲染命令，如果客户端瞬间渲染不过来的话，那么就会发生卡顿的现象，这种情况下，VDX 利用缓存技术，对每一个位图区域进行缓存，如果某个区域发生变化，仅更新该区域，剩余区域直接从缓存中读取，同时删除原有的渲染命令，在图像合成后再进行显示，通过该缓存技术，将大大提升在复杂操作情况下的性能。

4.1.5. PC 一致的使用习惯

在用户从 PC 模式切换到云桌面模式时，势必会存在使用习惯的不一致问题，针对用户在实际使用过程中可能出现的常规操作，做了大量的使用体验改进工作。

允许修改登录用户密码：

在企业的客户中用户可以修改自己登陆虚拟桌面的密码，用户可以是本地域帐号和域里面的用户，从而更好地保障用户个人桌面的安全性。

用户关机/停止/启动自己的虚拟机：

对于一部分用户来说，如果虚拟机出现蓝屏或卡死等异常现象，无法登录到

管理控制台，则无法对属于自己的虚拟机进行杀掉重启或者关机，导致需要管理员的参与，给管理带来不便。传统 PC 模式下的关机重启操作，也可以在客户端上完成，用户可以自由地控制自己的虚拟机运行状态。

云桌面可看到系统开机画面：

用户在启动或者重启虚拟桌面时，可以看到整个操作系统的开机画面，可以进入安全模式来进行操作，跟使用 PC 的开机体验完全一致。

云桌面开机自动连接：

云桌面可以选择开启开机自动连接，从而不需要重复输入账号密码，直接打开云终端，即可自动进入云桌面。

4.2. 便捷的平台管理

4.2.1. 智能的云终端设计

从云终端的软件设计上讲，之所以称之为智能云终端。因为其除了具备传统 PC 主机的硬件接口外，还独创性地加入了用户体验状态指示灯。能够会对用户在使用云桌面时，面临的各种硬件或网络问题，进行智能的报警，从而帮助用户了解云桌面的运行状况，当有故障发生时，能够轻松地排障，或者清晰地向管理员反馈故障现场，帮助管理员快速定位问题并及时恢复业务。

通过状态指示灯的闪烁，暗，亮等不同的状态，能够区分不同情况下影响服务质量的状况，用户只需根据指示灯的状态，就能轻松判断故障的原因。

4.2.2. 一体化的桌面部署

平台组件在同一台服务器上，即只需要对一台服务器操作，即可完成服务器虚拟化，桌面虚拟化平台部署，所有的桌面新建，更新，还原等操作，部署时间与传统虚拟化厂商平台相比，减少了安装步骤。

同时，平台内置本地域服务器，可以不需要安装 AD 域的情况下，轻松实现用户的授权和管理工作。

4.2.3. 统一的云终端管理

采用“云终端+云桌面”的部署模式，除了对于虚拟桌面的统一部署和管理

之外，针对企业级用户推出的一套云终端管理系统，它为 IT 管理人员提供易用的组织管理、控制和云终端设备的 OS 镜像、软件分发、补丁更新及运行状态监控，可支持上万数量级的运行软件的终端设备，无论是瘦客户机，还是运行软件的 PC 机。

智能化管理：

- 终端设备的自动发现；
- 设备的自动更新和升级；
- 终端设置的自适应管理；
- 终端设备远程开机，关闭，重启；

增强安全设计：

- 通讯加密，基于 HTTPS 的镜像更新升级；
- 系统权限分组管理，避免重复配置；
- 设备执行功能授权委托管理；
- 密码统一下发管理；

精确状态监控：

- 细粒度的资产报表；
- 实时的设备运行状态监控；
- 全面的操作日志审计；

高效扩展：

- 可以同时支持上千台云终端设备，最多可达 10 万台基于组的配置文件管理和分发，实现大规模终端设备的快速部署和更新；
- 基于 MAC 地址或其他分配规则，实现配置文件的快速推送和执行；

4.2.4. 跨地域集中管理

对于全国各地的分支机构人员，分布范围较散且每个分支机构人数也不多，一般不会单独配置 IT 管理员，而这个时候总部管理员便难以对其桌面系统进行高效管理和维护。因此，分支机构使用分布式部署集中管理的瘦客户机+虚拟桌面进行接入，快捷高效，无需管理员过多干预，后续运维工作统一在数据中心完成，如果分支机构新增人员可直接配发瘦客户机，管理员在 10 分钟以内便可以

实现桌面环境的部署。

由于分支机构采用广域网线路进行互联，带宽资源有限，通过桌面云分布式部署集中管理模式避免传输大量的非业务数据在广域网上传输，对互联网带宽占用少，同时保障分支机构的用户体验。对于极小的分支，或者零散的人员，可采用互联网 VPN 形式接入到总部的虚拟桌面平台，通过高效传输协议 VDX，能够保证在窄带宽情况下，虚拟桌面的正常访问和应用，从而达到统一接入的效果。

4.3. 灵活的平台设计

4.3.1. 全面的终端支持

对于云终端的类型，除了瘦客户机之外，传统的 PC 机，笔记本电脑，移动终端等，均可作为桌面云客户端的载体。

旧 PC 改造：

对于性能较低的 PC，在其 windows 操作系统上运行客户端，即可连接到高性能桌面。

4.3.2. 完善的外设重定向

对于企业用户来说，经常会使用到各种外设，例如 U 盘、UKey、打印机等。虚拟化平台，对外设的支持有 2 种形式，并且 2 种形式均支持外设的热插拔：

1. 支持把插在服务器上的 USB 外设进行透传到虚拟机；
2. 把终端上接入的外设进行重定向到虚拟机。

平台从虚拟化的底层就对上层的外设提供了支持，因此不需要在终端或者虚拟机里面安装任何驱动程序，从而能够最大程度的兼容各种外设。

对于并口/串口设备的支持，仅需要将其转接为 USB 口，从而可以按照 USB 设备的方式来进行使用，同样不需要安装任何额外的驱动，无论是从用户使用体验还是从兼容性方面都做到了最佳。

4.3.3. 精细的 USB 权限控制

在桌面控制平台上，可以控制用户是否有权限使用 USB，并可以区分使用哪种类型的 USB（打印机、大容量存储设备等），每种类型可以单独控制。

4.3.4. 广泛终端支持

用户可以通过任意终端设备来访问属于自己的个人虚拟桌面，而且可以实现终端迁移功能，在多个终端间切换，不会影响原先的桌面操作行为，真正做到桌面随身行。目前支持 PC、笔记本、瘦终端、iPad、手机或智能终端等设备接入访问虚拟桌面；支持 Windows 7（32 位和 64 位）、Windows XP（32 位）、Windows 8（32 位和 64 位）等客户端操作系统。

4.3.5. 丰富的桌面类型

不同的场景、不同的岗位上的员工需要不同类型的桌面，通过交付技术提供多种不同类型的虚拟桌面，来满足用户多样化的桌面需求，具体如下：

共享桌面：利用服务器操作系统的多用户会话共享功能，允许多个用户同时远程连接到同一个操作系统，并为每个用户提供不同的桌面，用户可拥有自己的桌面配置和个人数据，并共享同一套完整的桌面系统；标准化的桌面办公环境，可以提供一组核心应用，适用于不需要个性化安装软件或无自主桌面控制权限的任务型员工，比如办事大厅、职能办公、生产线、培训中心等。

远程应用：利用服务器操作系统的用户会话共享和应用程序多实例功能，允许多个用户同时远程连接到同一个应用程序，用户可拥有自己的应用配置和个人数据，并共享同一套应用程序；特定的应用程序交付，适合于应用数量较少，日常办公时仅需操作某几类软件，或需要移动办公的员工，如营业厅、生产线、销售部门及管理层移动办公等。

独享桌面：基于服务器虚拟化提供的可远程访问的桌面，即服务器可以根据模板自动为每用户分配一个虚拟机（安装 Windows 7、Windows 10 等桌面操作系统，并且每个独享桌面相互隔离），用户远程访问自己的虚拟机，并可拥有独立、完全的桌面使用和控制权限。适用于有系统个性化需求、对性能要求高的桌面用户，当然部署独享桌面对服务器和存储资源的要求比较高。

无论企业内的各种用户应用场景以及用户的需求如何多样化，通过交付技术，总能找出一种适合的技术来满足各种场景和用户的需求。IT 部门能够交付各种虚拟桌面每种桌面都经过专门定制，可满足每位用户的性能、安全性和灵活性要求。

4.3.6. 外设的总线映射技术

桌面云方案允许将外设连接到终端上，外设驱动安装于服务器上，然后可以如本地桌面一样使用各种外设，尽管虚拟桌面是在服务器上运行的。通过总线映射技术在终端连接外设的接口如 USB 或串口与服务器上的虚拟桌面构建一条专有的隧道，用于传输各种外设的控制指令，可以支持包括手写板、打印机映射、USB-key 等常见总线办公设备，并且保持会话间的隔离。

4.3.7. 智能开关机

智能开关机能够真正实现对用户虚拟桌面开、关机进行自动控制。即使瘦终端已经关闭，用户可能会忘记关闭位于服务器上的虚拟机，此时便可以实现对虚拟机的自动关闭功能，从而可以节省服务器的硬件资源。同时，通过软件内置的定时开机功能，可以指定在任意时间开启个人的虚拟机，且开机时可将用户虚拟机自动调度至资源充足的服务器上，一方面通过此技术可以避免 IO 风暴，加快系统登录时间，另一方面，通过自动化技术来简化用户访问虚拟桌面的操作步骤，让用户体验到简约、便捷的桌面操作。

4.4. 从云到端的安全设计

4.4.1. 平台安全

虚拟化基础架构的安全性关系到整个虚拟桌面访问的稳定性和数据安全性，本方案首先通过高可用性设计满足业务稳定性需求，然后再通过虚拟机隔离、数据盘加密控制、管理员权限细化等安全机制保证用户数据的安全。

从整体认证架构上讲，通过 SSL 加密通讯，嵌入到显示协议中，以保证整个平台的安全性，防止中间人攻击(MITM)。即使用户在登陆过程中遭遇中间人截持，由于其无法同时完成认证，最终会显示登陆失败，进行无法进入整个虚拟化平台。

从虚拟机的安全性来讲，在云桌面内，每用户独占一个虚拟机，通过底层机制实现 CPU 调度、内存、网络访问、磁盘 IO、存储空间的隔离，用户虚拟机的故障和安全问题不会影响到其他用户，保证虚拟机之间的隔离安全；每用户都会

分配个人数据盘来存放文档，当用户迁移至虚拟桌面的使用模式后，所有数据都集中存储于数据中心。因此，通过为个人数据盘进行加密存储，让其他用户包括管理员都无法访问，可以保证用户个人稳私安全；

从虚拟机的管理安全性来讲，不同管理员角色，授予合适的管辖权限范围，并保存操作日志。支持分级管理权限，包括上级管理员有权操作下级管理员的配置行为，相反则无权；支持上级管理员将虚拟桌面资源授权给下级管理员。

通过终端安全、传输安全、平台安全三大层次、多方位安全机制，可以完善保障用户接入安全、数据安全、管理安全、虚拟化安全、基础设施安全等多个建设环节，轻松应对虚拟桌面在建设过程中所面临的安全威胁及挑战。

4.4.2. 传输安全

从服务器到终端通过网络传输的，并不是真实的用户数据，而是云桌面内的图像信息，这些图像信息在传输过程中，已经基于 SSL 加密处理，一般情况下无法简单破解。与此同时，由于传输的是图像，所以即使能够截获，也无法得到原始的用户数据，最大程度上保障了数据的安全性。

通过 VLAN 隔离，并内置企业级防火墙模块进行状态化 ACL 访问控制，管理员登录时采用 HTTPS 加密传输、用户访问虚拟桌面采用传输加密等手段，保证业务运行和维护安全。

终端到虚拟桌面之间仅传输图像变化和指令信息，不直接传输实际数据，也即是说，“瘦终端+云桌面”让数据不落地，保障传输安全性；

可对传输加密通道进行基于 IP、服务的访问控制策略，减少异常流量的传输，且支持同一传输通道不同会话的隔离控制，包括存储会话、虚拟打印会话、总线映射会话等等，从而提升传输通道的灵活度；

通过对终端到虚拟桌面进行全程流量加密，杜绝中间人攻击行为，目前支持 AES、DES、3DES、MD5、SHA、DH、RSA 等算法，并且支持扩展国密办 SCB2（SM1）等其他加密算法，确保通信的安全性；

在桌面云接入平台上内置了企业级防火墙模块，通过灵活的 ACL 访问控制策略和 DDoS 设置，为整个平台提供状态包过滤和基本安全保护。

4.4.3. 终端安全

云终端的安全可以从硬件和软件两个层面来解析。

硬件层面上，由于云终端本身并不进行任何计算，只是对图像进行编解码的操作，所以其物理硬件上并不带硬盘，从而数据不会存储在云终端上，从根本上杜绝了数据的泄密问题。

软件层面上，通过 USB 权限控制，能够保证虚拟桌面内的数据按照管理员设定的权限来禁止、允许对应的 USB 拷贝。同时，云终端操作系统为精简加固的轻量级 Linux 操作系统，封闭的系统漏洞少，被黑客木马入侵的可能性远远小于 Windows 操作系统，从而保障了终端系统的安全。

瘦客户机无本地存储，可以说数据总是存放在最安全的地方。用户接入虚拟桌面资源时通过合法性认证、USB 灵活可控策略、应用策略化控制、还原模式等方式保证终端安全。

集成本地认证、短信认证、动态令牌、数字证书、第三方认证等身份认证机制，而且多种身份认证方式可以自由组合，以确保接入用户的身份唯一性；

基于灵活策略设置 USB 端口使用权限，比如是否允许使用 USB 设备（包括打印机、扫描仪等），还可以灵活控制 USB 硬盘的单向使用权限（比如仅允许访问终端往虚拟桌面拷贝数据，而不允许桌面到终端的数据拷贝）；

基于策略的访问控制：可以根据用户、网络、服务、设备、系统等，通过关联的策略为他们分配合适的访问权限。支持客户端安全检查功能，可以根据客户接入终端的系统版本、接入 IP，接入时间，杀毒软件的安装更新情况等，指定用户的访问控制策略；

桌面注销时还原至原始状态，该模式下，除了指定的一些目录外，用户所做的操作都会在重启后被还原。模板升级后，用户重新打开的虚拟机包含模板升级的内容，可以降低终端中毒风险。

4.5. 从点到面的稳定性设计

4.5.1. 对称式集群

传统的桌面虚拟化平台，其管理节点必须是一台单独的服务器或者虚拟机，

一旦管理平台发生故障，则会失去对整个虚拟化平台的控制，存在严重的单点故障风险。

在中数国科桌面云平台中，当服务器采用集群模式部署时，集群内每个服务器都是平等的，没有中央管理节点，每个节点的信息都会互相同步，登陆到任意一个节点都能够对整个集群做管理.从而实现管理平台的高可用。

集群内同步的是状态信息和配置文件，并不会有大流量的数据，不会因为信息的同步而造成网络堵塞。

4.5.2. 虚拟化平台高可用

集群内所有的服务器接到同一个存储设备，我们支持 iSCSI,SAN,NAS 等主流的存储系统。

1）群集监听机制：

A,B,C 三个服务器组成集群，接到同一个存储 S。A,B,C 在 S 上会有一个共享的存储块，它们会不断地去刷新各自的状态信息，同时互相会监听。

2）虚拟机加锁机制：

A,B,C 上运行的虚拟机，在正常情况下是加锁的，也就是说，只有本身才能控制自身的虚拟机。当 A 故障时，A 的状态信息将不再更新，B,C 会立刻知道这个信息，并开始对 A 上的虚拟机进行接管。此时，A 的虚拟机会全部解锁，直至 A 正常，将虚拟机重新加锁，由自己来接管。

当然，如果某台物理服务器需要维护，在无需中断服务的情况下，可将服务器之上的虚拟机动态迁移至其他服务器，管理员可以快速、完整地执行透明的运维工作。

5. 应用场景

5.1. 软件开发

需求描述：

- 防止内部人员将敏感文档外泄；
- 代码、开发文档及项目文档等自动备份；
- 快速创建标准化开发环境供研发人员使用；

对开发测试人员进行上网行为管理。

解决方案关键点：

- 集中存储，数据不落地；
- 开发桌面和上网桌面逻辑隔离，互不影响；
- 虚拟桌面模板、克隆；
- 远程应用发布上网工具、AC 做文件外发控制和审计、专用虚拟化杀毒方案。

5.2. 日常办公

需求描述：

- 总部-多分支办公场景，数据进行集中存储、集中管控；
- 需满足快速拓展的分支业务办公场景；
- 多分支机构终端的安全管控以及安全隐患问题。

解决方案关键点：

- 总部部署桌面云服务器，分支机构部署云终端，办公场景快速就位；
- 远程协助解决故障，一键还原和备份恢复；
- 数据集中存储云端、数据不落地，终端实现 0 数据，对外设进行策略控制，有效解决数据外泄。