技术白皮书

威讯云桌面系统

福建升腾资讯有限公司
www.centerm.com

文档版本 01
发布日期 2020-08-14

升腾威讯 CentermWeixun
做 更 好 用 的 桌 面 云

1 产品概述

1.1 产品简介

完全自主研发的桌面虚拟化软件，通过构建统一的桌面云平台，实现对桌面云系统的统一管理和交付，帮助客户将办公从传统的 PC 模式向云办公演进。威讯云桌面系统兼容多个虚拟化平台，具备自动化监控和告警功能，同时实现对计算、存储、网络资源的集中共享、统一调度和灵活扩展，解决了传统 PC 办公模式给客户带来的如：办公效率低、运维管理难、信息安全弱、资源浪费和运行成本高等诸多问题，通过可将虚拟化技术从数据中心延伸到终端设备，降低 IT 日常运维开销。

1.2 产品组成

威讯云桌面方案产品组成主要包括如下内容：

- **计算主机：**基于威讯云虚拟化系统用来运行虚拟桌面的主机。
- **网络：**用来把整个环境联系在一起。它包括物理网络连接和逻辑网络；逻辑上可以划分为存储网络、管理网络和业务网络等。
- **威讯云虚拟化系统：**采用银河麒麟系统分布式高可用架构，实现去中心化设计，通过虚拟化技术，将计算、存储、网络融合到同一套物理服务器上，多套物理服务器通过网络实现统一管理、统一资源调度，实现资源的汇聚管理。采用 SSD 加速、内存加速，精简置备满足用户高性能体验。平台支持按需扩容，即插即用，降低后台数据成本的同时帮助用户实现 IT 基础架构平滑稳定演进。
- **威讯云桌面系统：**通过构建统一的桌面云平台，实现对桌面云系统的统一管理和交付，帮助客户将办公从传统的 PC 模式向云办公演进。除了支持自研的威讯云虚拟化系统外，还支持市场上主流的一些虚拟化平台，比如：XenServer、KVM 等等。
- **威讯云客户端：**提供跨平台的桌面接入能力，涵盖 Windows、Linux、Android 和 IOS 主流平台，兼容银河麒麟、统信等主流国产操作系统，满足用户多场景下的接入需求，同时针对键鼠交互和触摸交互 2 种交互模型进行了特定的优化，以确保不

同场景下的用户体验。

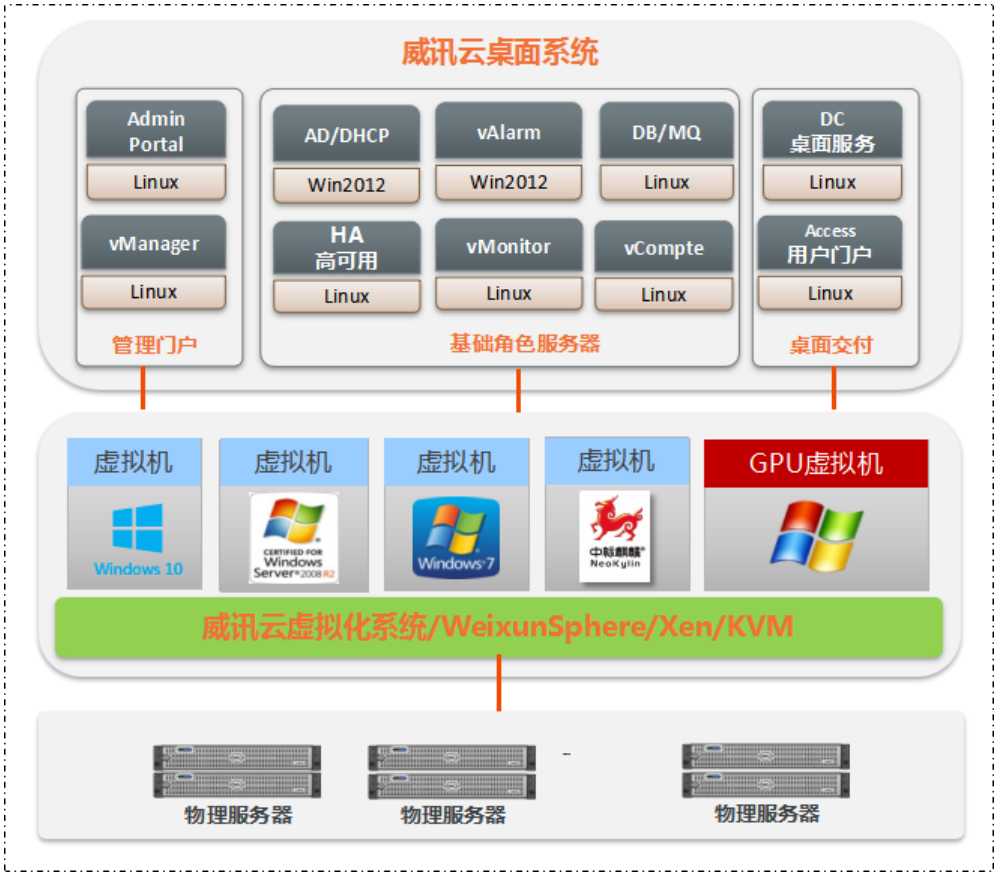

图 威讯云桌面系统组成意图

2 主要功能

为不同用户提供最佳的云桌面	
共享桌面	采用多会话技术，交付一个桌面，供多个用户同时使用。
静态池桌面	为用户提供重启还原系统、保存用户数据的标准化云桌面。
随机池桌面	为用户提供重启还原系统和用户数据的标准化云桌面。
标准桌面	为用户提供专用、重启用系统和用户数据不还原的云桌面。
GPU桌面	采用GPU虚拟化技术，交付有GPU资源的桌面。
VIP桌面	支持对桌面设置VIP属性，平台会优先保障VIP桌面的计算资源和实施监控VIP桌面的健康状态。
云电脑	基于CVDI技术，交付本地终端桌面。充分利用终端本地的性能，确保用户体验与传统PC一致。
云应用	采用应用虚拟化技术，无需为用户发布桌面，即可使用云端上的应用。
端到端的安全控制	
回收站机制	桌面删除后自动进入回收站，可从回收站恢复被删除的桌面，避免误操作导致数据难以恢复。
统一管理	采用 B/S 架构，通过浏览器可实现对云桌面终端的统一管理，可一列表形式实时显示当前在线的云桌面终端，云桌面管理服务器的负载情况,云桌面终端的使用活跃度、闲置率等； 平台对软硬件实行统一管理，支持多数据中心资源调度,管理员可通过设置终端准入策略设置终端的接入许可,同时可查看接入的终端 IP、MAC 地址、接入/断开时间、接入时长等；
终端准入	终端用户绑定、终端型号、接入时间等多种终端准入策略，确保桌面只能被可信的终端登录，保障接入端的安全，为确保数据传输安全，自研的高性能传输协议实现协议通道加密机制,防止用户传输数

	据的监听窃取,保障用户数据的安全，云桌面客户端支持设置免密登录,使用国密算法防止密码泄露,保证用户密码安全，对 USB 等存储外设进行权限管控,防止数据恶意访问或私自拷贝，对登录用户、登录时间、登录终端进行严格规定,以防非法用户或在非办公时间登录桌面。
多因素接入认证	微信二维码扫码登录、用户账号密码、图片验证码、Radius动态口令、UKey等多因素接入认证，防止用户密码泄露导致桌面被恶意连接。
丰富的外设接入策略	支持为用户或用户组配置云桌面的外设接入策略，只有授权的用户才能在云桌面中使用终端本地的USB、磁盘、剪切板、打印机、串并口、摄像头、扫描仪、音频设备等外设重定向，支持直通打印功能，同时可以针对USB设备配置黑、白名单控制。
桌面安全水印	提高员工安全意识，方便泄密追溯，在桌面屏幕上显示安全水印，支持水印内容、用户名、桌面IP等信息展示。
三员分立	系统强制存在系统管理员、安全管理员和安全审计员三个默认账号和三类默认角色。管理员间的权限应相互制约、互相监督，避免由于权限过于集中带来的安全风险。
分权分域	针对不同管理员，分配不同的桌面组、用户组等管理对象，并对桌面组实行资源配额制，实现系统分权分域管理。
用户管理	支持创建单一用户或批量导入用户，支持管理员启用或禁用用户，支持对用户的密码进行重置，支持创建用户组,支持将用户加入或移出到不同的用户组，支持设置是否允许终端启用命令行和启用密码
日志审计	记录管理员和普通用户在门户中的操作事件，支持事后审计和导出。
传输协议加密	使用标准的高性能加密传输，通过SSL技术确保桌面协议传输过程的安全性。
协议支持	支持可选云桌面远程连接协议类型：Xred协议、spice 协议、rdp 协议；
集中存储	用户云桌面数据集中存储在数据中心，通过RAID机制及可选的备份

	策略，避免重要数据因异常故障丢失。
网络隔离	生产、管理、存储三网隔离，不同角色仅能访问特定网络资源。
桌面备份	管理员和桌面用户都可以对桌面进行快照备份，实现桌面异常故障快速恢复。
统一的镜像管理	
快速的业务更新	通过更新单一的镜像，实现批量桌面中的系统更新。
“热”更新	管理员通过镜像更新桌面业务时不会中断云桌面的当前使用，用户下次开机时可获取更新。
灰度更新	镜像完成编辑后，实现在某些桌面上先应用新的镜像，等验证通过后应用到全部关联桌面。
镜像跨集群	将桌面管理的成本节约优势扩展到镜像管理。采用WeixunSphere+NAS方案时，一个镜像可在多个集群中使用。
云电脑和VDI融合桌面	云电脑桌面为技术型用户交付正常办公云桌面的同时，还可通过同一镜像交付“漫游”桌面，满足不同场合相同桌面办公的需求。
高效的资源复用策略	
空闲桌面自动关闭	自动检测处于开机但长时间没有连接的桌面，并自动关闭这类桌面，以释放计算资源给其他用户使用。
活跃桌面定时启动	上班前预启动前一个工作日处于活跃状态的桌面，避免上班高峰期批量启动桌面导致存储IO风暴。
故障桌面定时重启	定时重启故障状态的桌面，以便桌面恢复到初始状态。
智能启动预留桌面	随机池桌面组，会自动根据当前桌面连接情况，预启动一批桌面，减少这类桌面的连接时间，提高用户体验。
空闲桌面智能挂起	桌面处于连接状态，但长时间无人操作时，能够智能挂起该桌面，以释放计算资源给其他用户使用。当用户下一次连接时，能够恢复桌面之前的状态。
磁盘链接克隆	桌面系统盘基于同一个母镜像文件链接克隆创建，采用链接克隆技术，降低存储成本60%。

虚拟机迁移	支持虚拟机热迁移，主机存在性能不足时，可以把虚拟机从负载高的主机迁移到负载较小的主机上。
桌面/云应用负载均衡	基于会话并发的负载均衡策略，自动把用户新连接的会话创建在空闲的桌面和云服务器上，支持客户端设置应用桌面快捷键。
IP配置工具	支持对云桌面系统进行IP修改，以适应客户现场IP环境变更。
多重运维保障	
自助维护	用户门户自助维护功能（远程连接、快照、电源操作、服务状态检测等），快速检测和解决桌面连接异常类问题，当云桌面用户使用异常时,支持向管理员发起远程协助。
远程连接/桌面重影	在用户确认后，远程连接到用户桌面会话，进行远程桌面运维。
监控与告警	实时监控系统运行状态，针对异常情况进行邮件等多手段告警。
系统HA	系统支持多节点高可用部署模式，一个节点异常，集群还能正常提供服务； 支持虚拟机高可用功能,典型硬件故障下虚拟机自动恢复时间小于 5 分钟； 全系统意外断电,在恢复供电后,系统能够自动恢复到断电前状态； 支持后端服务(数据库、调度器和 API 等)负载均衡及高可用,单一控制节点 down 机不影响平台访问，保障平台高可用性； 支持网络高可用性,当主网卡出现故障时,可立即切换至备用网卡进行服务，保障业务连续性。
系统升级	支持系统补丁上传和自动升级，无需手动更新。
可维护性	系统支持提供日志管理服务,支持查看管理员操作日志、用户操作日志及错误日志，方便问题排查跟踪，支持通过云桌面管理端下发云桌面客户端升级包批量升级云桌面客户端；
会话管理	远程管理桌面会话，可对会话进行断开、注销等操作。
系统健康报告	实时生成和导出系统健康报告。

良好的用户体验	
可视化部署	基于引导式的可视化工具部署，只需配置IP、账号、密码等即可完成云桌面系统部署。
远胜于本地安装的应用	虚拟应用可提供与本地安装应用相同的外观和用户体验，同时可统一管理。
任何终端接入支持	自研的Xred协议允许桌面接入时不受接入终端系统类型的限制。
随时随地移动办公	可通过安卓、iOS等手机、平板设备移动设备，登录办公桌面
个性化定制	根据客户自定义的logo和名称，切换产品名称和logo，满足快速个性化定制。
大数据展示平台	虚拟化系统的大数据监控和展示，能够清晰展示系统健康状态、资源和用户使用情况、异常告警情况等等。
高可扩展性	
异构平台支持	虚拟化系统支持：威讯云虚拟化系统、WeixunSphere、XenServer、KVM、品高等等。可同时管理不同的虚拟化系统。
主机可扩展	支持主机可扩展，满足未来云桌面规模的扩展需求
管理节点可扩展	根据云桌面用户数量的增长，通过管理节点分布式平滑扩展，可轻松支持10000以上的用户规模。
存储可扩展	支持存储可扩展。根据存储增长需求，可实现存储在线平滑扩容。
客户端服务	
多平台兼容	支持Windows、Linux、银河麒麟、统信等主流国产操作系统，支持PC 机、笔记本、瘦客户机(X86、ARM、飞腾、龙芯)多终端接入。
云服务	支持客户端配置多个云中心服务,对云中心进行管理，可新增、删除和编辑云中心；
网络检测	支持使用网络质量进行检测,包括丢包率、平均延时、网络速率、网络延迟等。
客户端服务	

计算虚拟化	虚拟机是对真实计算环境的抽象和模拟，VMM 需要为每个虚拟机分配一套数据结构来管理它们状态，包括虚拟处理器的全套寄存器，物理内存的使用情况，虚拟设备的状态等等。VMM 调度虚拟机时，将其部分状态恢复到主机系统中。并非所有的状态都需要恢复，例如主机 CR3 寄存器中存放的是 VMM 设置的页表物理地址，而不是 Guest OS 设置的值。主机处理器直接运行 Guest OS 的机器指令，由于 Guest OS运行在低特权级别，当访问主机系统的特权状态（如写 GDT寄存器）时，权限不足导致主机处理器产生异常，将运行权自动交还给 VMM。此外，外部中断的到来也会导致 VMM 的运行。
存储虚拟化	威讯云超融合系统的存储虚拟化，通过分布式存储方式实现对分布在不同物理设备的存储设备和数据进行聚合实现统一的交付。简单来说，数据就近存储，将数据分散在多个存储节点上，各个节点通过网络相连，实现了对存储资源的重复利用，降低了单点瓶颈提升整体的性能。
网络虚拟化	网络虚拟化将网络控制与物理网络拓扑分离，从而摆脱硬件对网络架构的限制。将网络设备上的控制权分离出来，由集中的控制器管理，无须依赖底层网络设备，屏蔽了底层网络设备的差异。用户可以自定义任何想实现的网络路由和传输规则策略，从而更加灵活和智能。
分布式资源调度	所有的调度采用异步调度和无锁结构，使得在分布式环境中，各资源调度能够实现极大的性能提升。
异构服务器支持	通过虚拟化技术，实现对不同CPU指令集的屏蔽，使不同CPU在虚拟化层上工作在同类型的CPU指令集上。通过虚拟化层的屏蔽，使不同类型的CPU能够纳管到同一个资源池中，实现对异构资源池资源统一管理
智能缓存算法	ssd cache 采用读写缓存机制，能够将热点数据缓存在存储上。使得存储在提供高性能IO的同时又能够有效降低存储的成本
分布式数据一致性	在大规模的数据中心上，硬件的故障是频繁且正常的事件，因此对于数据的安全和可靠性不能只是由硬件来决定。分布式环境上，通

	常采用多个副本来确保数据完整性。分布式数据一致性就是用于保证多个副本的数据一致性。
存储精简置备	精简置备是一种高效的存储容量分配和管理的技术，通过技术手段实现在小的存储上，分配出大的空间，如分配了4GB的空间，实际写入的数据量只有100M，传统存储上，需要使用4GB的空间，而采用精简置备系统只占用100M的空间，同时随着业务的扩展自动实现实际物理空间的数据分配
多副本技术	crush算法会根据机架->主机的分布关系，以及副本数量，选择不同机架不同主机上的不同磁盘。实现数据的多副本写入。
在线容量扩容技术	通过扩大磁盘、主机、机架的数量，实现在CRUSH所选择的目标设备扩大，从而实现，数据可以分布到更多的设备上。从而达到实时在线容量扩容的技术。通过数据平衡技术，在新设备接入后，系统会自动调度实现数据上的均衡。

3 指标参数

3.1 支持指标

表 1　平台支持指标表

参数	指标
服务器支持	● 支持通用 X86 平台和国产飞腾、鲲鹏、海光、兆芯平台的混合管理
虚拟化平台支持	● 威讯云虚拟化系统、WeixunSphere、XenServer、KVM、品高，支持银河麒麟服务器操作系统（国防版）V10 等
桌面系统支持	● 支持 Windows 系统，如：Windows7、Windows10、Windows Server2008、2012 等 ● 支持国产 Linux 系统，如：UOS 桌面操作系统（军用版）V20、银河麒麟桌面操作系统（国防版）V10 等 ● 桌面操作系统与云桌面系统兼容
存储类型支持	支持包括本地存储、iSCSI、FC 和 NFS 等
终端系统支持	支持主流的终端操作系统，包括：Windows、Linux、iOS、安卓 ，支持常见国产 Linux 系统，如：中标麒麟、银河麒麟、UOS 等
网络支持	企业内网、互联网

3.2 管理规模指标

表 2　管理规模支持指标表

参数	参数值	备注
集群数量	32	每个数据中心支持的最大集群数量
虚拟机数量	10000	单平台支持的最大虚拟机数量

3.3 可靠性指标

表 3　可靠性指标表

参数	指标
系统可用度	≥99.9%
系统掉电恢复时间	≤20 分钟

4 产品特点及关键技术

4.1 丰富的桌面类型

威讯云桌面系统提供标准桌面、随机池、静态池、GPU 桌面、共享桌面、云电脑和云应用等多种类型的应用。管理员可根据将应用场景将桌面划分不同组，同组桌面采用同一镜像，系统镜像与用户数据分离。

标准桌面：根据镜像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，并可拥有完全独立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。

池桌面：支持系统重启还原，数据盘重启不还原。支持将用户的所有配置文件和个人文件夹全部重定向到数据盘，在桌面重启后，用户设置信息及数据可以全部保留。因此，在用户系统盘更新或切换后，用户的原有数据不会受到任何影响。池桌面下的用户支持统一更新，管理员只需通过 web 直接打开母镜像，进行升级更新操作，完成镜像编辑后，可将更新后的镜像一键推送给桌面组下面的所有用户，用户重启后即可使用升级桌面系统。静态池类型的桌面，用户和桌面一一绑定，桌面重启后绑定关系不丢失。随机池桌面，桌面重启后绑定关系丢失，用户下一次连接桌面，系统将自动选择一个空闲的桌面。

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虚拟机，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。

GPU 桌面：提供有 GPU 资源的桌面，可以是标准桌面模式，也可以是池桌面模式。

云应用：利用应用虚拟化和服务器会话共享等技术，为用户提供云应用交付模式。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。

4.2 高效、安全的桌面连接协议

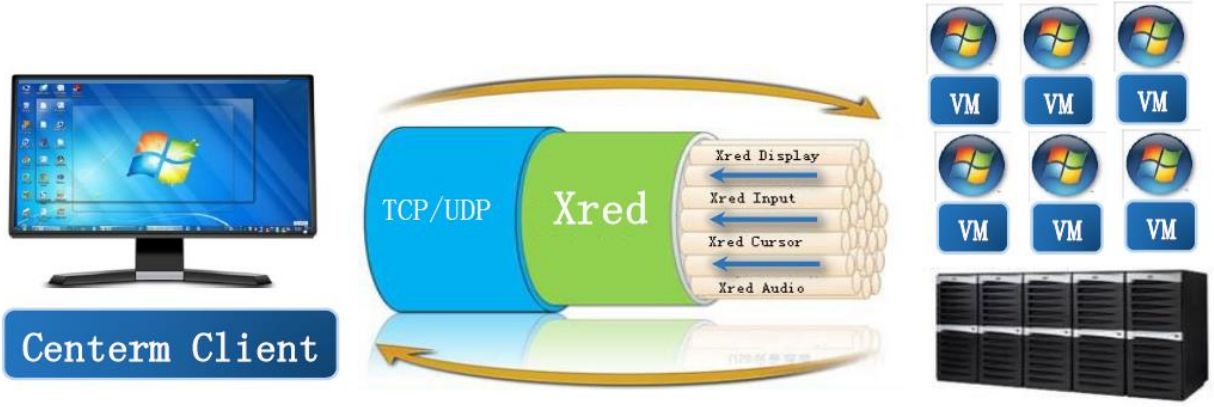

图 Xred 协议

桌面连接协议是影响虚拟桌面用户体验的关键，Xred 协议作为威讯云全自助研发的桌面连接协议，它提供了高分辨率会话、多媒体流远程处理、多显示支持、动态对象压缩和缓存、USB 重定向、视频重定向、驱动器映射等功能。Xred 协议在丢包和延迟都比较高的网络环境下依然能够正常使用，最大程度保障用户桌面体验。除了上述功能外，Xred 协议还存在以下几个特点：

- **安全：**将应用程序的执行和显示从逻辑上分开，只在网络上传输经过加密的键盘、鼠标以及屏幕更新的信息。

- **集中化的应用程序和客户管理：**借助 Xred 能够使企业克服应用软件的管理、访问、性能以及安全方面的问题，IT 部门能够更好地交付最高级别的服务，并在满足最终用户不断发展的需求的同时，进一步简化桌面管理、降低运营成本和提高总体桌面安全性。

- **平台无关性的支持：**本身具有平台独立的特性，可以运行在各类的虚拟化平台之上，比如威讯服务器虚拟化系统、KVM、Hyper-V、XenServer、vSphere 等。

- **协议无关性的支持：** 协议工作于标准的网络协议 TCP/IP 之上，通过标准的通信协议以及无线通信协议都可以进行接入工作。

4.3 基础架构高可用

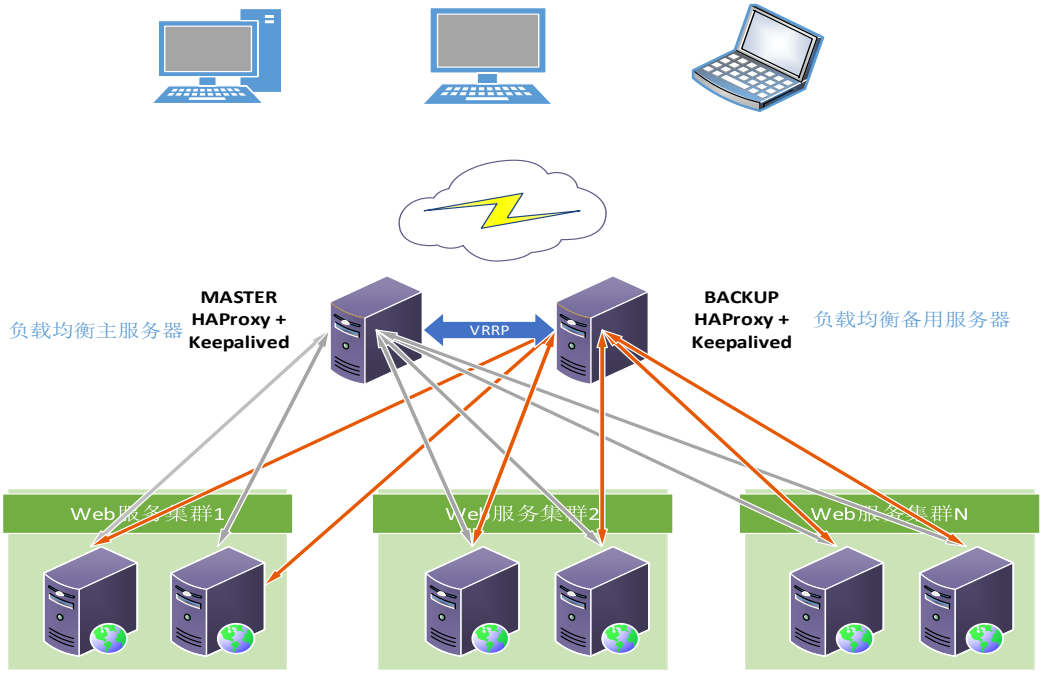

图 基础架构服务 HA 结构

为了保障负载均衡服务器的高可用，防止负载均衡服务器异常后，造成整个系统无法使用，建立一台备用的负载均衡服务器。主备负载均衡服务器上的 HAProxy 需要完全一致。主备负载均衡服务器通过 Keepalived 实现故障切换。Keepalived 会对外提供一个虚拟 IP，客户端访问的是这个虚拟 IP，而不是负载均衡服务器的 IP。当主服务器上的 Keepalived 检测到 HAProxy 没有正常工作时，将结束自身进程。这时，备用服务器上的 Keepalived 检测到主服务器上的 Keepalived 没有正常工作，将接管主服务器的工作，对外提供服务。

4.4 细粒度的外设控制

图 外设管理

通过智能扩展协议软件（SEP）提供的设备映射和多媒体重定向技术，支持将连接在终端上的外设通过协议通道映射到桌面内部，桌面可以直接使用这些外设。外设控制策略支持配置：USB 设备、磁盘、剪切板、打印机、串并口、摄像头、扫描仪等设备是否启用重定向。同时，能够针对 USB 类型的设备等配置详细的准入黑白名单。

4.5 网络分域安全隔离

- 虚拟化层安全隔离

虚拟化层为虚拟机提供独立的运行环境，提供虚拟机间的 CPU 指令隔离、内存隔离、网络隔离等防护机制；屏蔽硬件平台的动态性、分布性、差异性等，为每个用户提供相互独立、隔离的计算机环境，同时方便整个系统的软、硬件资源的高效、动态管理与维护。

- 网络隔离

依据数据流量的不同用途，可以把系统网络划分为管理网络、业务网络、存储网络，可实现各网络平面的逻辑隔离，确保各个平面网络流量互相不干扰，保证系统可靠性与安全性，支持在云桌面管理端设置网络端口映射，提供 vlan、vxlan、flat、local、gre 等虚拟化网络

- 网络支持

虚拟网络支持二层和三层组播协议,且支持在带宽占用 70%的情况下,丢包率小于 10e-7。

- 安全域隔离

不同部门的虚拟机可以利用 VLAN 实现逻辑隔离；不同的业务可以按照不同等级划分为不同的安全域，可以通过 VLAN 实现不同安全域的逻辑隔离。

4.6 统一资源管理

图 统一管理平台

平台采用 B/S 架构，提供可视化的管理门户，系统管理员通过浏览器访问管理门户，可以直观的管理、监控和维护整个虚拟机平台的资源，包括所有数据中心及其集群、服务器、存储、磁盘、网络和虚拟机等。