技术白皮书

威讯云桌面系统

7.0

福建升腾资讯有限公司
www.centerm.com

文档版本 01
发布日期 2022-05-30

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或 WeixunSphere 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，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。

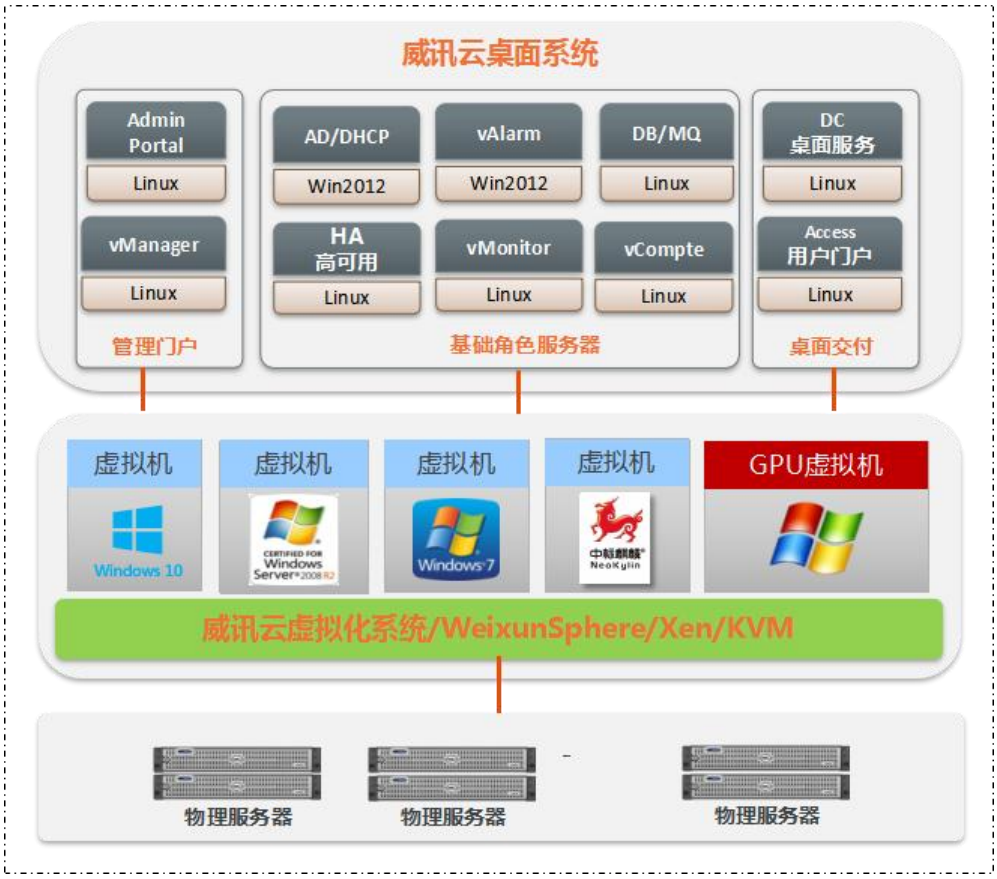


图 威讯云桌面系统组成意图

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。
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。
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，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。
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。
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。
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	
远程维护	支持采用远程方式对云桌面进行远程协助，远程协助基于WEB页面，无需额外安装客户端；通过WEB方式远程管理，支持对物理资源管理、虚拟主机管理，支持虚拟桌面接入控制功能。
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。
系统升级	支持系统补丁上传和自动升级，无需手动更新。
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。

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	● 主流 X86 服务器，支持 Intel 及 AMD CPU ● 国产化服务器支持：海光、鲲鹏服务器
虚拟化平台支持	● 威讯云虚拟化系统、WeixunSphere、XenServer、KVM、品高等等
桌面系统支持	● 支持 Windows 系统，如：Windows7、Windows10、Windows Server2008、2012 等 ● 支持常见国产 Linux 系统，如：中标麒麟、银河麒麟、UOS 等
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

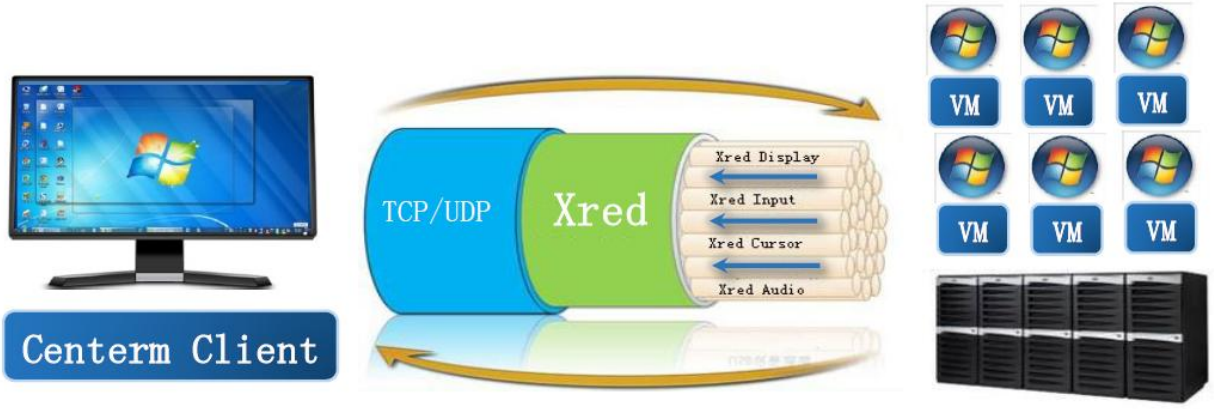


图 Xred 协议

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

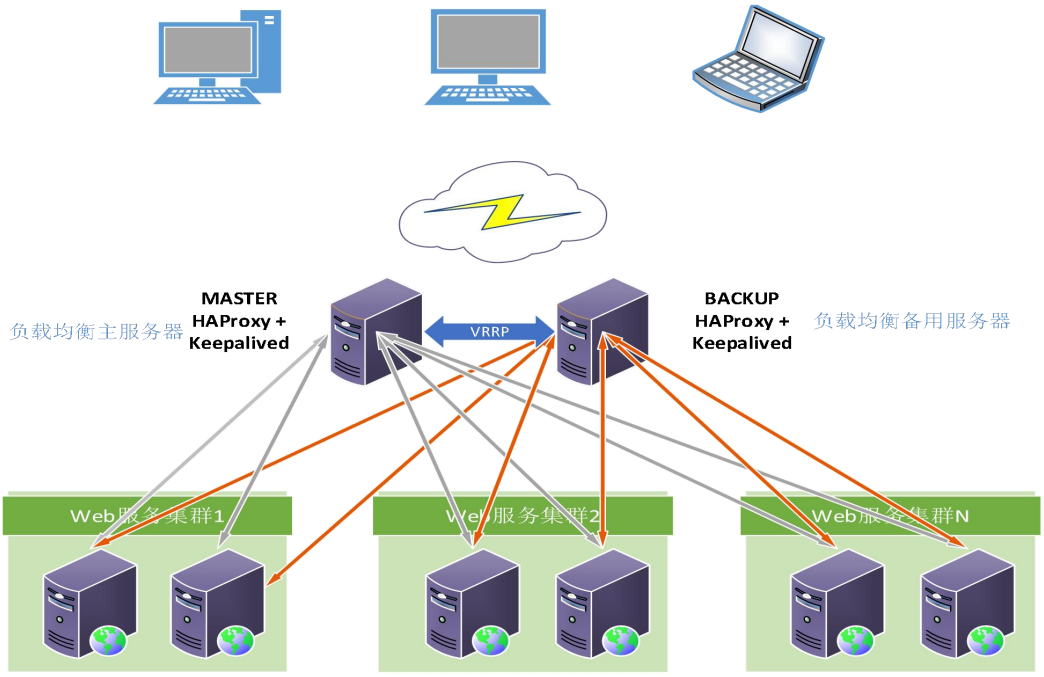


图 基础架构服务 HA 结构

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。

- 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

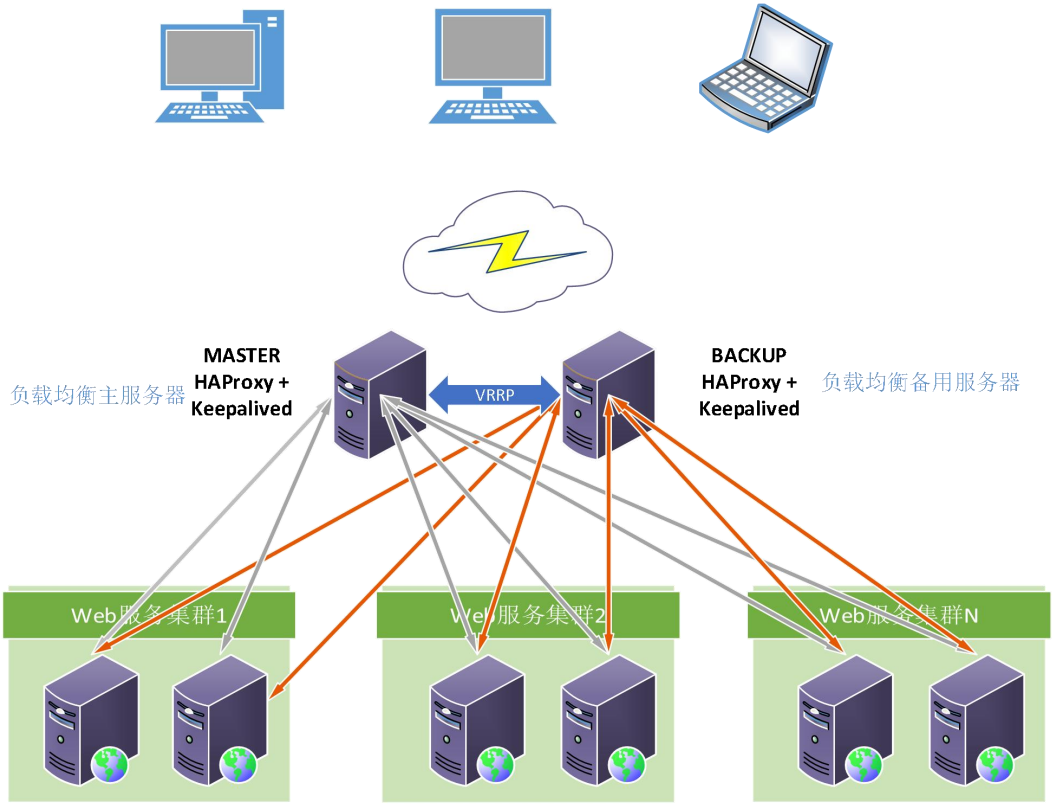
图 统一管理平台

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。

5 角色服务说明

5.1 高可用服务

系统采用 keepalived+HAProxy 的高可用方案。



高可用方案结构图

在 web 前端部署 1 台 HAProxy 作为负载均衡服务器。对于不同的业务请求，HAProxy 将请求重定向到不同的 web 服务集群；对于相同的业务情况，HAProxy 根据负载均衡算法将请求重定向到同一个 web 服务集群的不同 web 服务器中。

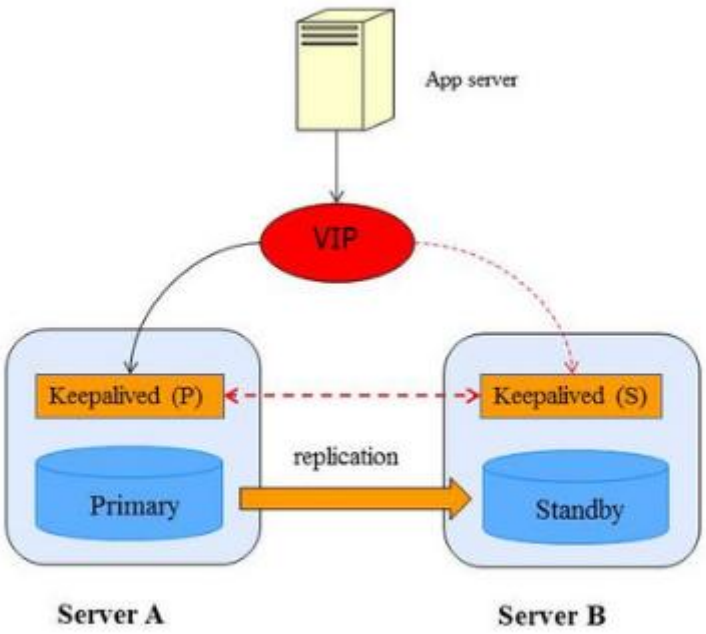
为了保障负载均衡服务器的高可用，防止负载均衡服务器异常后，造成整个系统无法使用，建立一台备用的负载均衡服务器。主备负载均衡服务器上的 HAProxy 需要完全一致。主备负载均衡服务器通过 keepalived 实现故障切换。Keepalived 会对外提供一个虚拟 IP，客户端访问的是这个虚拟 IP，而不是负载均衡服务器的 IP。当主服务器上的 keepalived

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。

5.2 数据库服务

数据库服务采用开源数据库 postgres，为平台提供数据存储服务，是非常重要的底层服务，不能出现异常。否则系统大部分功能都会出现问题。

数据库服务高可用方案采用：Keepalived+异步流复制的 postgres HA 的方案。



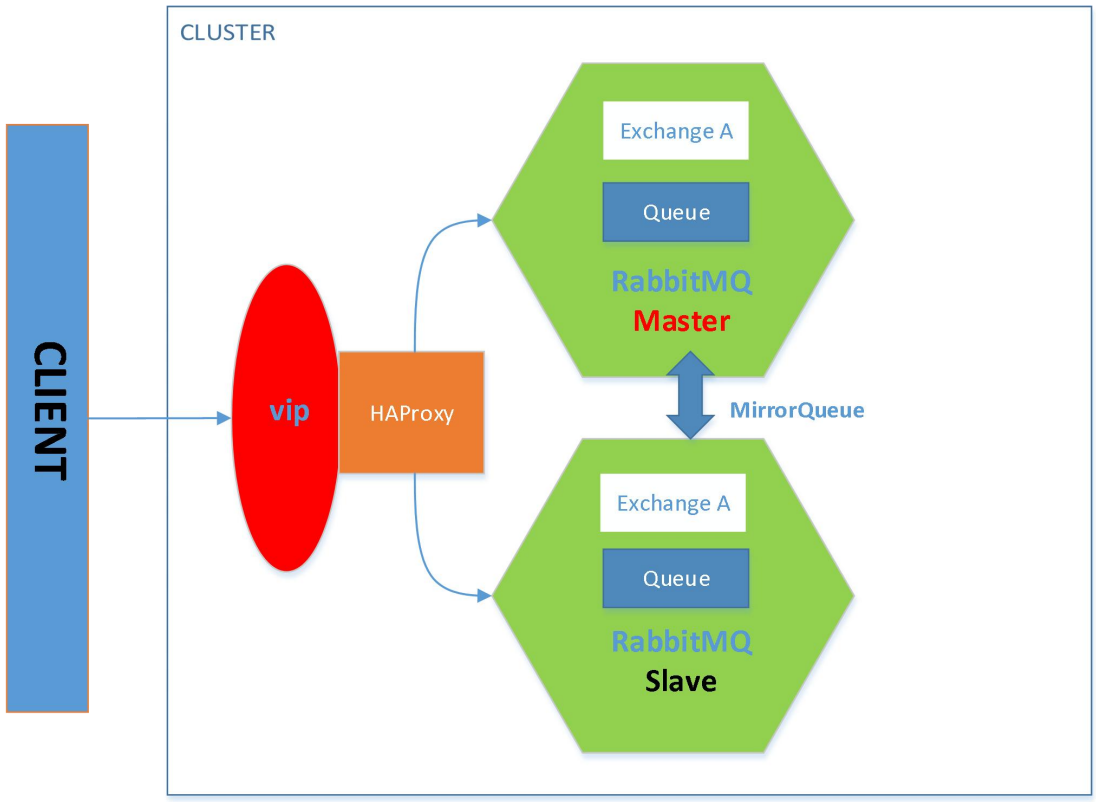
“Keepalived+异步流同步”部署结构图

1. VIP 是数据库集群统一对外提供数据库服务的地址；
2. Keepalived 集群负责对数据库状态健康情况进行监控和故障切换；
3. 数据库 A + B 做主备关系，两台服务器之间做异步流同步，进行数据备份；

5.3 消息队列服务

采用 RabbitMQ 作为企业版消息队列服务。消息队列主要用在服务内部进行异步方法的处理，是非常重要的底层服务，不能出现异常。否则系统大部分功能都会出现问题。

RabbitMQ 消息队列利用 Erlang 的分布式特性进行集群的构建，各 RabbitMQ 服务为对等节点，通过镜像队列的方式，进行消息队列的结构复制和同步。Master-Slave 机制，保证了每时每刻由主节点 Master 负责进行消息处理，当 Master 宕机，则会有一个 Slave 自动升级为 Master，保证了服务的高可用。通过 HAProxy，构建负载均衡器 LB，来完成消息队列的负载均衡，客户端只需访问 VIP 即可。



RabbitMQ 高可用部署结构图

5.4 AD 域控

AD 域控在我们平台中，提供以下主要功能：

- 提供给平台的账号的认证、存储和计算机管理；
- 提供用户配置信息和策略的漫游；

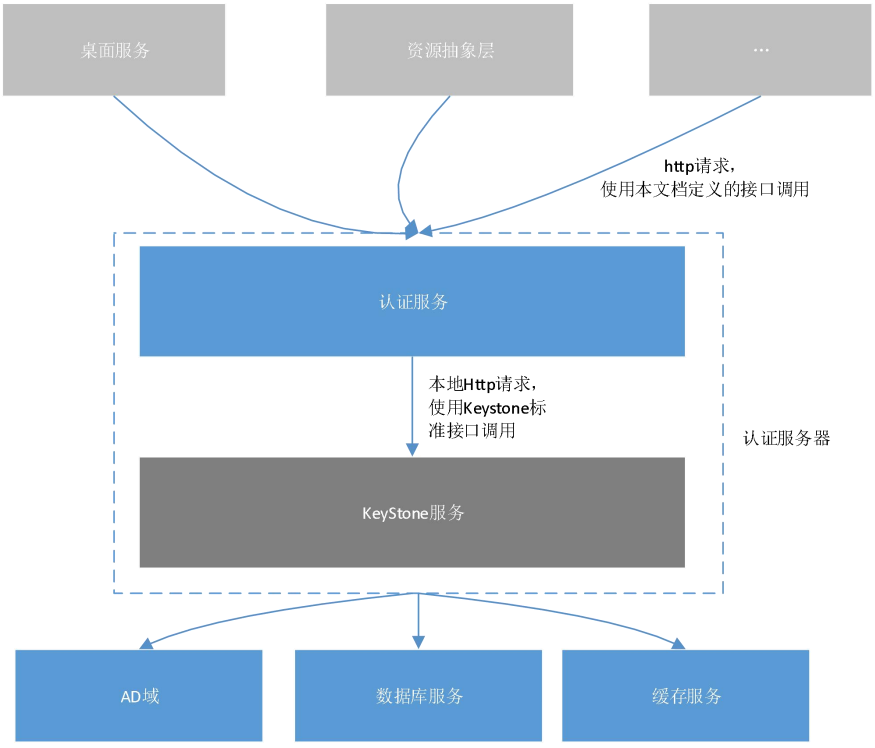
- 提供 DNS、DHCP 服务

5.5 认证服务

认证服务，目前对接的是 AD。提供以下功能：

- 提供服务之间的安全通信认证，避免服务接口被第三方恶意攻击；
- 提供管理员 portal 和用户 portal 的登录认证和鉴权；
- 登录桌面时，提供用户登录身份信息的申请和认证；
- 分布式服务信息的存储和注册；

如下的结构：

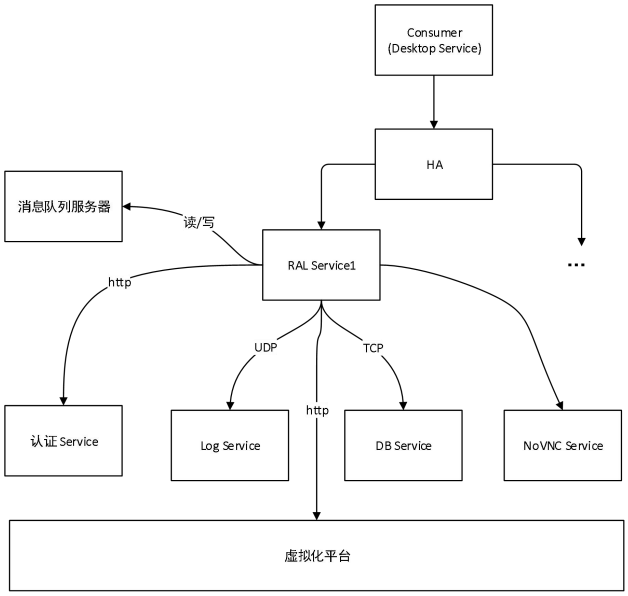


认证服务和 KeyStone 服务部署在同一台服务器上，由认证服务负责对外提供接口。服务本身是无状态的，即使某个节点异常，高可用服务也可以转发到正常的服务节点上。因此可以通过部署多个节点，来保证服务的高可用和负载均衡。

5.6 RAL 服务

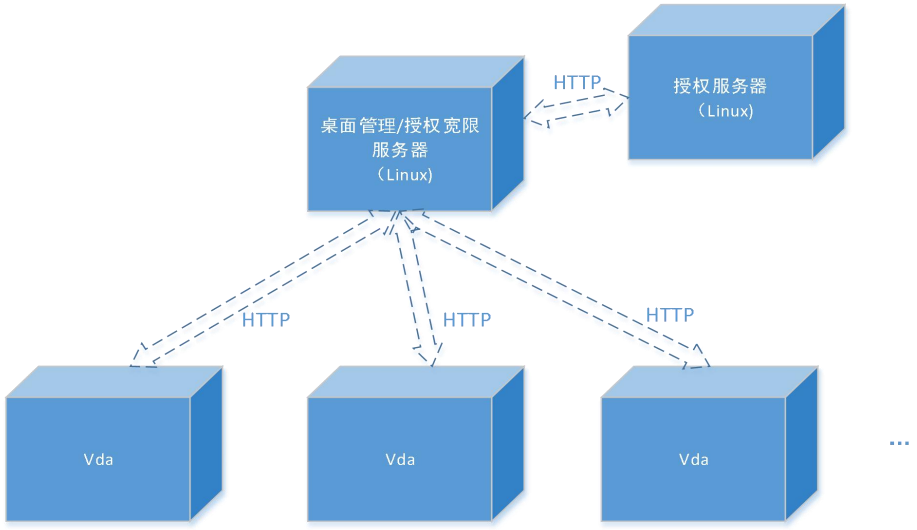
RAL 服务提供的是虚拟化底层的资源抽象服务，直接负责与虚拟化底层进行交互。同时，屏蔽掉各个虚拟化底层的差异，对外暴露同一套虚拟化底层的调用接口。这样，后续平台要新增一个虚拟化平台后，只需要 RAL 服务与该平台对接即可，其他服务无需做任何修改。

目前，RAL 服务已经支持与 WeixunSphere、HCI、bingo、xen 等平台的对接。RAL 服务在整个平台的结构如下：



5.7 授权服务

授权服务提供用户登录桌面授权数量的控制。当前平台的授权控制按照并发的用户数量进行控制。授权服务在整个平台的结构如下：



考虑到授权信息的唯一性，授权的注册码跟着安装授权服务的设备走。没有对授权服务器进行高可用设计。授权服务器异常后，我们有 30 天的授权容错期，因此，并不会因为授权服务的异常，导致平台不可用。

5.8 日志服务

日志服务采用 linux 本身的 syslog 日志机制进行维护和管理的，每个自研的角色服务运行时的日志，除了在各自服务本地保存一份副本外，都会统一上传到日志服务器。目前日志服务没有做高可用，主要原因是考虑到即使这个服务异常，不会导致日志的丢失和其他服务的运行问题。

5.9 计算服务

计算服务，主要与 RAL 服务进行交互，负责：

- 集群、网络、存储管理；
- 虚拟机、镜像、主机的生命周期的管理；
- 虚拟机、主机的电源管理；

5.10 桌面服务

桌面服务，主要与计算服务、认证服务进行交互，负责：

- 桌面和桌面组的发布、桌面策略的调度；
- 桌面生命周期的管理（桌面创建、分配、删除等）和电源操作；
- 与 VDA 服务的通信，桌面内部信息的管理等；

5.11 交付服务

交付服务，主要与桌面服务、认证服务进行交互，负责：

- 桌面用户登录时，用户分配桌面资源的展示；
- 负责桌面用户登录；

5.12 管理服务

管理服务，主要与桌面服务、计算服务、认证服务、RAL 进行交互，负责：

- 用户角色、权限的管理；
- 管理员操作日志的收集和存储；

5.13 监控服务

监控服务，主要与桌面服务、计算服务、RAL、管理服务进行交互，负责：

- 桌面用户登录和使用情况的收集和统计；
- 虚拟机、主机等 CPU、内存、网络等使用情况的收集和统计；
- 角色服务的状态监控；

5.14 告警服务

告警服务，主要与告警服务、管理服务进行交互，负责：

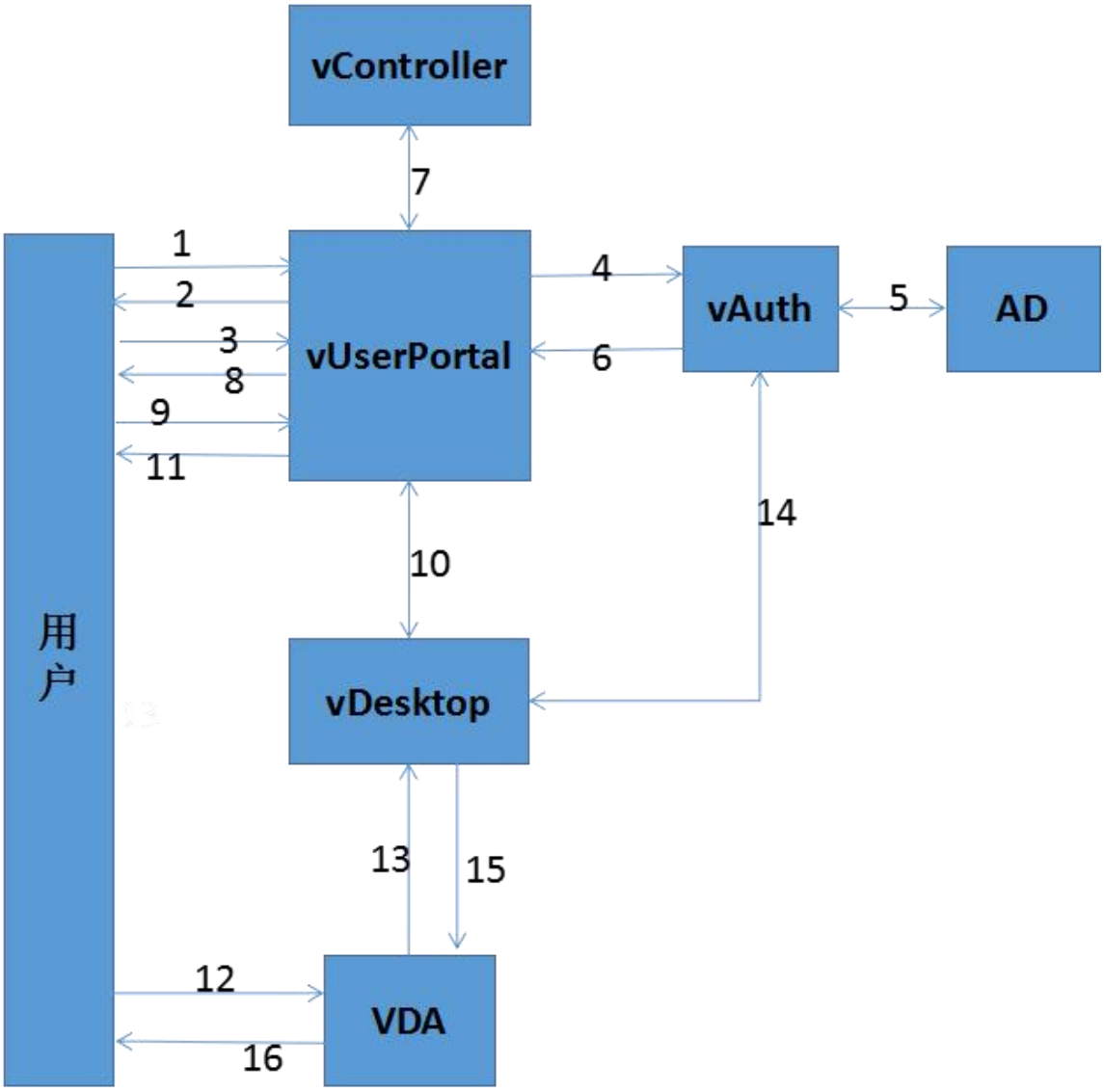
- 告警策略的配置和管理；
- 告警策略的调度和告警的触发；
- 告警的邮件通知等；

5.15 管理员 portal

管理员 portal，主要与管理服务、桌面服务、计算服务、监控服务进行交互，负责提供后台管理界面给管理员。通过管理员 portal，管理员可以运维整个虚拟化环境。

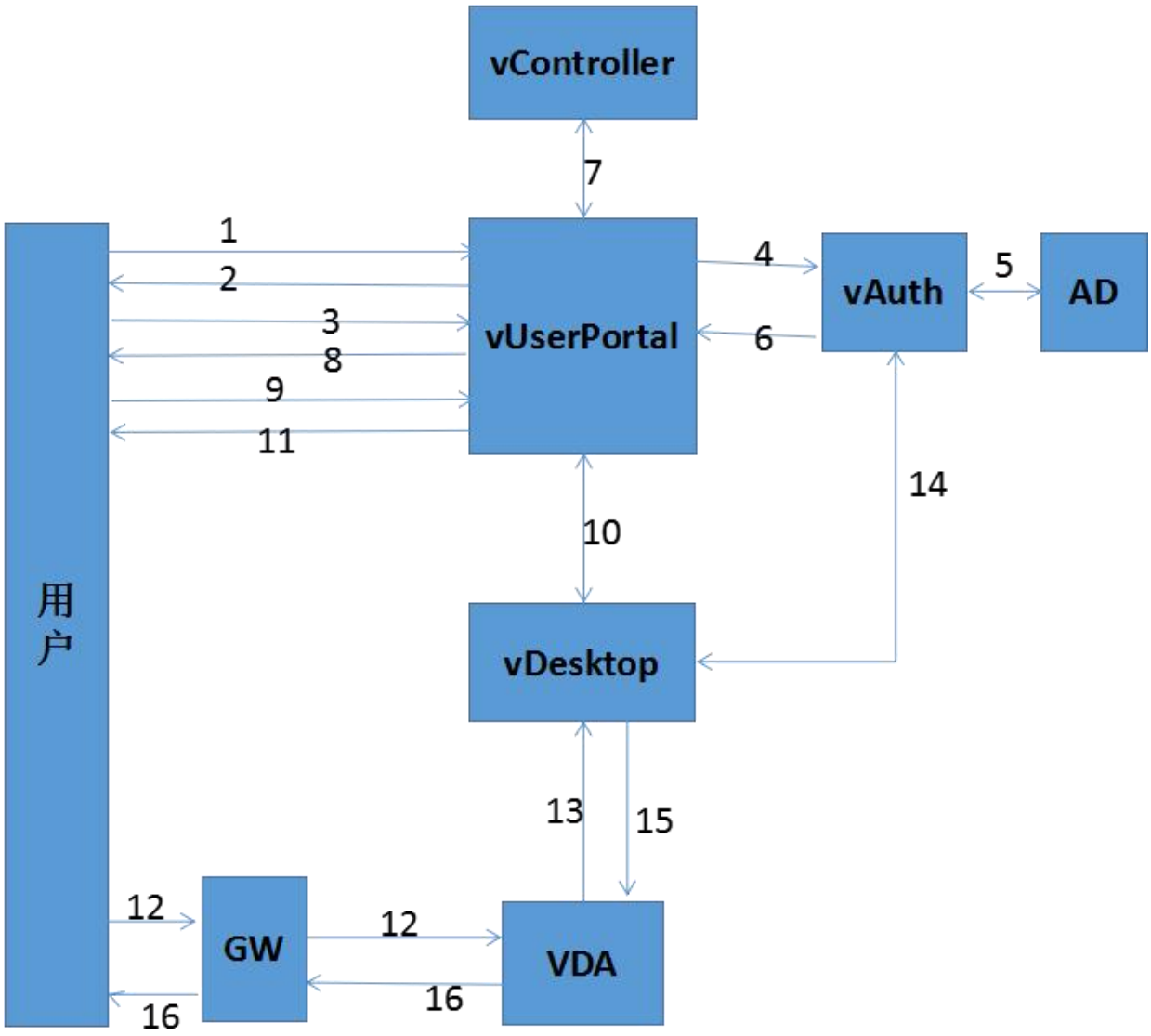
5.16 用户 portal

用户 portal，主要与交付服务、管理服务进行交互，负责提供用户分配资源的展示、桌面登录等。通过用户 portal，用户可以登录到自己的桌面。 内、外网登录流程见如下：



	内网登录流程
1	浏览器打开用户门户地址
2	返回一个登陆页面
3	输入用户名、密码，请求资源列表
4	向认证服务请求用户名、密码有效性验证
5	通过 LDAP 向 AD 认证
6	返回认证通过的 token

7	向交付服务请求该用户分配的资源列表
8	展示该用户分配的资源列表
9	点击一个桌面图标，发起连接请求
10	请求桌面连接信息
11	返回桌面连接的 ivy 文件
12	根据 ivy 文件内的桌面地址，xred 协议连接桌面
13	把 token 和桌面 id 发送给 vDesktop
14	根据 token 置换桌面用户名和密码
15	返回桌面用户名和密码
16	认证通过，用户登录桌面，进入加载配置文件、组策略



	外网登录流程
1	浏览器打开用户门户外网地址
2	返回一个登陆页面
3	输入用户名、密码，请求资源列表
4	向认证服务请求用户名、密码有效性验证
5	通过 LDAP 向 AD 认证
6	返回认证通过的 token
7	向交付服务请求该用户分配的资源列表

8	展示该用户分配的资源列表
9	点击一个桌面图标，发起连接请求
10	请求桌面连接信息
11	返回桌面连接的 ivy 文件
12	根据 ivy 文件内的桌面地址，xred 协议连接桌面
13	把 token 和桌面 id 发送给 vDesktop
14	根据 token 置换桌面用户名和密码
15	返回桌面用户名和密码
16	认证通过，用户登录桌面，进入加载配置文件、组策略