InCloud Access V6.10

技术白皮书

济南浪潮数据技术有限公司

2024 年 4 月

目录

1 前言

文档用途

本文档用于描述 InCloud Access 产品功能特色、技术原理、规格参数及适用场景。

适用范围

本文档为公司内部、外部了解 InCloud Access 技术实现的参考文档。

读者对象

本文档提供给以下相关人员使用：

- 客户代表
- 产品经理
- 售前工程师
- 系统维护工程师
- 研发工程师

安全声明

公司产品不会主动获取或使用用户的个人数据，仅在您同意使用特定功能或服务时，在业务运营或故障定位的过程中可能会获取或使用用户的某些个人数据（如告警邮件接收地址、IP 地址），公司产品在涉及个人数据的收集、存储、使用、传输、删除等全生命周期的处理活动中，已在产品功能上部署了必要的安全保护措施，同时，您也有义务根据所适用国家或地区的法律法规制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

浪潮高度重视产品数据安全，公司产品在涉及系统运行和安全数据的全生命周期处理活动中，已严格按照相关法律法规及监管要求，在产品功能上部署了必要的安全保护措施。作为系统运行和安全数据处理者，您有义务根据所适用国家或地区的法律法规制定必要的数据安全政策并采取足够的措施以确保系统运行和安全数据受到充分的保护。

浪潮将一如既往的严密关注产品与解决方案的安全性，为客户提供更满意的服务。浪潮已全面建立产品安全漏洞应急和处理机制，确保第一时间处理产品安全问题。若您在本产品使用过程中发现任何安全问题，或者寻求有关产品安全漏洞的必要

支持，请直接联系浪潮客户服务人员。

修订记录

修订时间	修订人	修订内容
2024.4	PM	第一次正式发布。

2 产品概述

国内客户在企业信息化建设过程中几乎还是采用传统 PC 的办公模式，越来越多的企业在 PC 的使用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。据 IDC 的统计，企业在 PC 硬件上每投资 10 元，就需要为后续的运维支出 30 元（整整 3 倍），而从业务价值的角度来说，桌面运维对组织业务发展并不创造直接的价值，没有带来生产力的提升，在这方面的投入越大、浪费就越多。

在日常的办公领域，越来越多的企业体验到了桌面云或虚拟桌面的魅力。桌面云是指将桌面与 PC 分离开，所有桌面在数据中心进行集中化保存和管理，并虚拟交付到终端用户的一种方式，这是目前将 Windows 桌面交付到办公场所、分支机构的最佳方式，其提供了任意时间、任意地点、任意终端的接入，有利于业务的快速拓展。桌面云因为和传统 PC 桌面用户的使用习惯一致因而受到了企业客户的青睐。

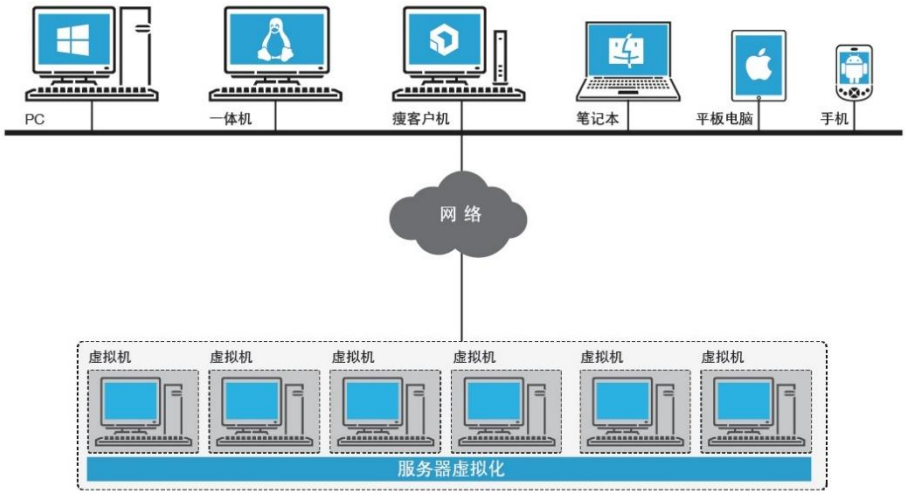


图 1 桌面云示意图

“瘦终端+桌面云”作为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。根据《2012 年中国虚拟化市场研究报告》，以往客户对虚拟化的采购比例为“服务器虚拟化占比 73%，桌面虚拟化占比 18%”；而未来客户对虚拟化的采购比例将变成“服务器虚拟化 20%，桌面虚拟化 70%”。也即是说，在整个虚拟化市场领域里，客户对服务器虚拟化的投资占比在逐渐降低，而对桌面虚拟化的投资占比在快速提升。另外，Gartner 也预测未来 30%以上的大中型企业将部署“瘦终端+桌面云”方案。

2.1 产品定位

InCloud Access 采用业界先进的架构设计理念和技术架构，驱动产品在可靠性、稳定性、性能、易用性等方面的全面提升。InCloud Access 不仅提供基于虚拟化技术的云主机、云硬盘等资源类型服务，同时提供基于容器的各类应用服务，以更好的匹配企业级业务的多样性，在提供相关服务的基础上，为了保障业务的高效稳定运行，也提供配套的智能化监控运维、服务治理能力。通过统一的运营运维门户，保证一致性的用户体验。

2.2 产品简介

浪潮桌面云正在成为被广泛使用的技术，虚拟化技术实现桌面云核心技术的支撑。通过它帮助企业以更低成本，实现更灵活、稳定和高效的 IT 系统。目前虚拟化技术主要包含：服务器虚拟化，应用虚拟化和桌面虚拟化技术。服务器虚拟化技术在 2007 年开始被广泛接受并采用，目前已经成为一种成熟的满足企业应用的主流技术。而虚拟桌面技术被逐步接受，尤其是和虚拟应用的结合，使得桌面虚拟化技术能被更广泛地使用帮助企业以更低成本、更好地实现桌面管理。

虚拟桌面是一个企业级的，通过一定手段实现的可远程访问、调度和管理的桌面的操作系统，其可以是运行在服务器上的虚拟操作系统，也可以是直接安装、运行在数据中心内的物理 PC（工作站，刀片 PC）上的操作系统。目前桌面虚拟化技术融合了应用虚拟化技术，在虚拟桌面模式下，每个人独享的远程操作系统，并利用内含的应用虚拟化技术，实现更灵活，高效的管理和应用。将桌面操作系统虚拟化带来很多好处，包括：

灵活办公

在传统桌面环境下，用户只能通过单一的专用设备访问其个性化桌面，这极大的限制了用户办公地点的灵活性。采用桌面云，由于数据和桌面都集中运行和保存在数据中心，用户可以随时随地，通过网络，访问到被授权的桌面与应用，终端设备支持更广泛，可以通过 PC，瘦客户端、甚至是手机来访问传统 PC 上才能使用到的各种 Windows 应用。应用运行不中断，实现无缝切换办公地点。

资源按需分配，更高利用率

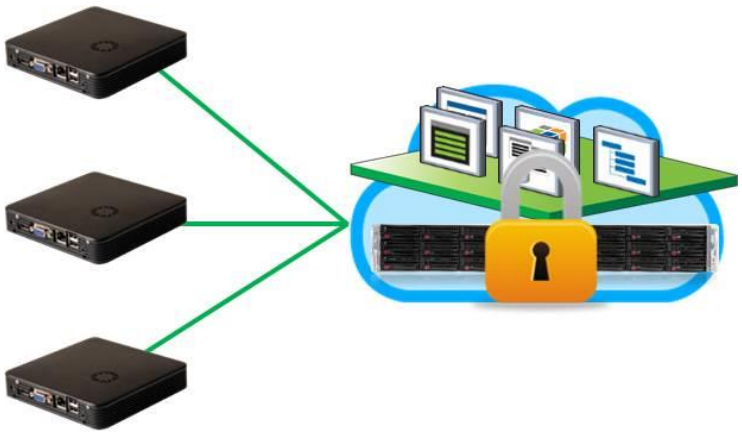
在桌面云环境下，所有资源都集中在数据中心，可实现资源的集中管控，弹性调度。资源的集中共享，提高了资源利用率。传统 PC 的 CPU 平均利用率为 5%～20%，桌面云环境下，云数据中心的 CPU 利用率可控制在 60%左右，整体资源利用率提高。桌面分享服务器硬件，配置资源可以按照用户需求动态调整。

故障时间短，系统可用性高

传统桌面环境下，所有的业务和应用都在本地 PC 上进行处理，稳定性仅 99.5%，年宕机时间约 21 个小时。在桌面云中，所有的业务和应用都在数据中心进行处理，

专业的服务器和强大的机房保障系统能确保业务年度平均可用度达 99.9%，充分保障业务的连续性。各类应用的稳定运行，有效降低了办公环境的管理维护成本。

数据不落地，信息更安全



在传统桌面环境下，由于用户数据都保存在本地 PC，因此，内部泄密途径众多，且容易受到各种网络攻击，从而导致数据丢失。而在桌面云环境下，终端与数据分离，数据不传输到终端，仅传输加密的屏幕图像。本地终端只是显示设备，无本地存储，所有的桌面数据都是集中存储在企业数据中心，无需担心企业的敏感数据资产遭到泄露。除此之外，瘦客户机的认证接入、加密传输等安全机制，保证了桌面云系统的安全可靠。

高效运维

传统桌面系统故障率高，据统计，平均每 200 台 PC 机就需要一名专职 IT 人员进行管理维护，且每台 PC 维护流程（故障申报—>安排人员维护—>故障定位—>进行维护）需要 2～4 个小时。

桌面云不需要前端维护，强大的一键式维护工具让自助维护更加方便，提高了企业运营效率。使用桌面云后，每位 IT 人员可管理超过 2000 台虚拟桌面，维护效率提高 10 倍以上。

应用管理更简单，管理员在服务器进行统一管理，无需特定的补丁与应用的分发软件，统一进行安装和升级，维护桌面的费用大大降低。

节能减排，降低 TCO

通过部署节能、无噪的瘦客户机，有效解决密集办公环境的温度和噪音问题。瘦客户机让办公室噪音从 50 分贝降低到 10 分贝，办公环境变得更加安静。瘦客户机和液晶显示器的总功耗大约 20W 左右，终端低能耗可以有效减少降温费用。

资源自动管控

白天可自动监控资源负载情况，保证物理服务器负载均衡；夜间可根据虚拟机资源占用情况，关闭不使用的物理服务器，节能降耗。这些技术降低了 IT 系统的 TCO。

2.3 产品架构

2.3.1 整体架构

传统 PC 的众多弊端是由“终端分散化”所引起的，为了降低综合维护成本，提升信息安全管理水平，“云端集中化”模式应运而生。通过桌面云技术将办公桌面集中部署在服务器上，使得不同设备可以随意访问，并且实现桌面维护简单化、业务数据集中化。

浪潮 InCloud Access 产品提供了一套高性价比的智能桌面云解决方案，产品从层次上可以分为硬件资源层、虚拟化层、桌面云层、桌面协议层、终端接入层。系统架构如下图所示：

浪潮 InCloud Access 的系统架构图如图 1 所示：

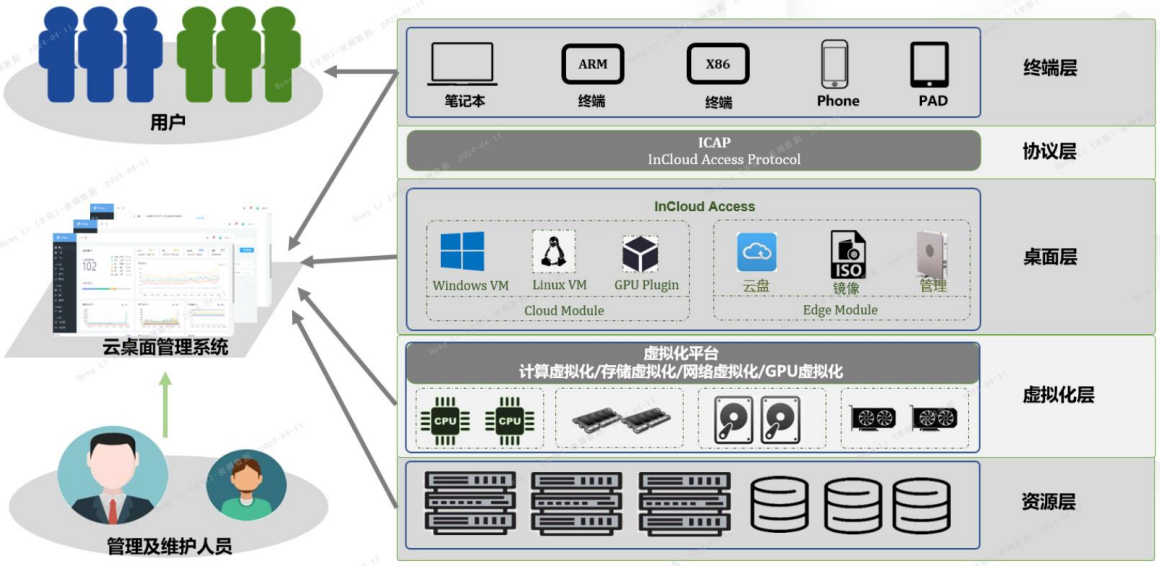


图 1 InCloud Access 系统架构图

硬件资源层：通过 X86 服务器的 CPU、内存、磁盘、显卡，提供桌面云系统所需要的底层硬件资源池。

虚拟化层：通过浪潮虚拟化平台完成对硬件资源的虚拟化，括：

- 计算虚拟化是桌面云系统的关键组件，负责将服务器的 CPU、内存、磁盘、I/O 等硬件资源转换成可以动态管理的“资源池”，让一台服务器变成几台甚至上百台虚拟服务器（虚拟机），从而提升服务器资源利用率，并实现高可靠服务器集群环境。计算虚拟化组件部署在操作系统内核内部，因而可以很容易控制云平台所有虚机的虚拟化进程，可以利用整个计算系统的性能、可扩展性和安全优势。可以实现对服务器物理资源的池化，将 CPU、MEM、HDD 等物理资源转化为一组可统一管理、调度和分配的逻辑资源池，在此基础上在物理服务器节点上构建多个相互隔离、同时运行、内核交互的虚机工作环境。

- 存储虚拟化可以根据用户需求、现有 it 系统情况进行灵活选择：

  - 本地存储方案：利用服务器的本地存储，当前计算节点的桌面数据存储在本地磁盘。

  - 分布式存储方案：通过部署分布式存储，通过将存储服务器所有磁盘虚拟化为一个存储资源池，用于存储用户个性化数据。

  - 集中存储方案：在一些现有集中式存储的环境，如 NAS 存储，可以充分

利用该存储，继续用于存储用户个性化数据。

- 超融合存储：可以采用超融合存储，利用桌面服务器的本地存储，本着资源集约化、最大程度利用的前提条件，基本的设计思路是桌面服务器本地存储通过虚拟化后，将服务器的所有磁盘虚拟化为一个存储资源池，虚拟化后的存储资源将用于保存用户数据数据、日志文件和虚拟镜像文件等。

桌面云层：InCloud Access 产品核心层次，用于管理桌面云及提供云终端接入服务，并提供身份验证、桌面发布、桌面管控、应用发布、终端管控、桌面数据库等关键组件，主要功能如下：

- 支持桌面管理，包括新建、删除、关机、开机、重启、挂起和规格调整等。
- 支持虚拟桌面链接克隆，同时支持将含有个性化修改的用户桌面制作成镜像，并通过该镜像创建新的桌面。
- 提供内置管理员和桌面用户管理功能，无需依赖第三方身份系统，能够实现帐号集中管理，包括帐号创建、修改和删除等操作。
- 支持系统监控、告警和日志管理，可实时了解主机和桌面的资源使用情况，并可审计管理员的操作，避免安全风险。

桌面协议层：ICAP 高性能桌面传输协议，支持场景化压缩编码技术，包括 H.264、H.265，桌面通过 ICAP 进行网络传输，智能云终端本地解码后呈现在本地显示器：

- 画面智能侦测（自然和非自然图像），静态场景下带宽低至 0
- 支持多通道传输，提高传输效率
- 桌面流化 VBR（动态比特率）传输，支持文本、音视频、3D 建模、云游戏
- 加密传输，提高安全性和数据保护

- 支持 H.264、H.265 硬件编码加速，提高单机桌面并发数

- 支持多种格式、多种播放器的超高清视频播放 4K/8K@60FPS，和云游戏场景（不依赖于瘦终端）

终端接入层：包括软终端、智能终端（X86/ARM 架构）。

2.3.2 系统组件

InCloud Access 的具体组件结构从物理部署结构上可以分为 3 个大部分：

终端部分、管理平台部分和云桌面所在的物理机设备部分。

终端部分

终端为用户提供了在各个操作系统上远程访问其拥有的云桌面的方法。终端使用远程访问协议，在终端设备获取虚拟机的桌面访问。

终端主要包含各种硬件设备终端：瘦终端/胖终端、软终端（windows/linux/mac）以及移动终端（android/ios）；终端通过其内置的应用：lander+InCloud Access-player 来进行业务操作：

- Lander 是终端上的主要应用。安装在接入终端 TC/SC 中的 ICAP 协议客户端，用于发起连接虚拟桌面请求，接收并处理 ICAP 协议服务端的请求和响应消息。

- InCloud Access -player 是 spice-client 的二次开发。

InCloud Access 管理平台部分

InCloud Access 管理平台是一个基于 Web 的网页系统。该部分主要包含 InCloud Access 管理平台的各个组件，是云桌面生态系统的核心和调度中心，是云桌面系统的子系统间通信的重要枢纽。

- web: 管理平台的管理页面，可视化的管理 InCloud Access 的各种配置与服务。

- portal：基于浏览器的简单用户客户端。

- grafana: 监控图表。

- cm: 终端接入网关。
- api: 管理平台的后端 API 服务。
- taskflow：长任务/异步任务等管理。
- vnc: 提供 noVNC 服务。
- prometheus：监控数据。
- auth-center: license 校验。
- message：websocket 消息转发。
- upgrade：在线升级。
- mysql: 业务数据库。
- redis: 热点数据和临时数据库。

云桌面宿主机部分

云桌面宿主机部分主要包含云桌面运行环境和协议：

- ICAP-mgr: 一个 agent 程序，用来和 InCloud Access 管控通信。
- 虚拟化控制平台，比如 openstack 等。
- qemu-kvm: 虚拟化核心组件，可以创建出 vm；vm 内有以下组件：
  - cloud-init 实现对 vm 的初始化操作，比如修改计算机名等。
  - qga: 支持在物理机层面给虚拟机内发命令，比如：获取 vm 内的网络信息等。
  - helper：InCloud Access 在 vm 内的 agent，实现一些定制化功能，比如修改壁纸等。
  - ICAP -agent：是对 spice-agent 的二次开发。
- ICAP -server: 对 spice-server 的二次开发产品。

InCloud Access 桌面云产品分成终端组件、核心组件、扩展组件、桌面组件、虚拟化组件等大的功能组件。系统组件如下图所示：

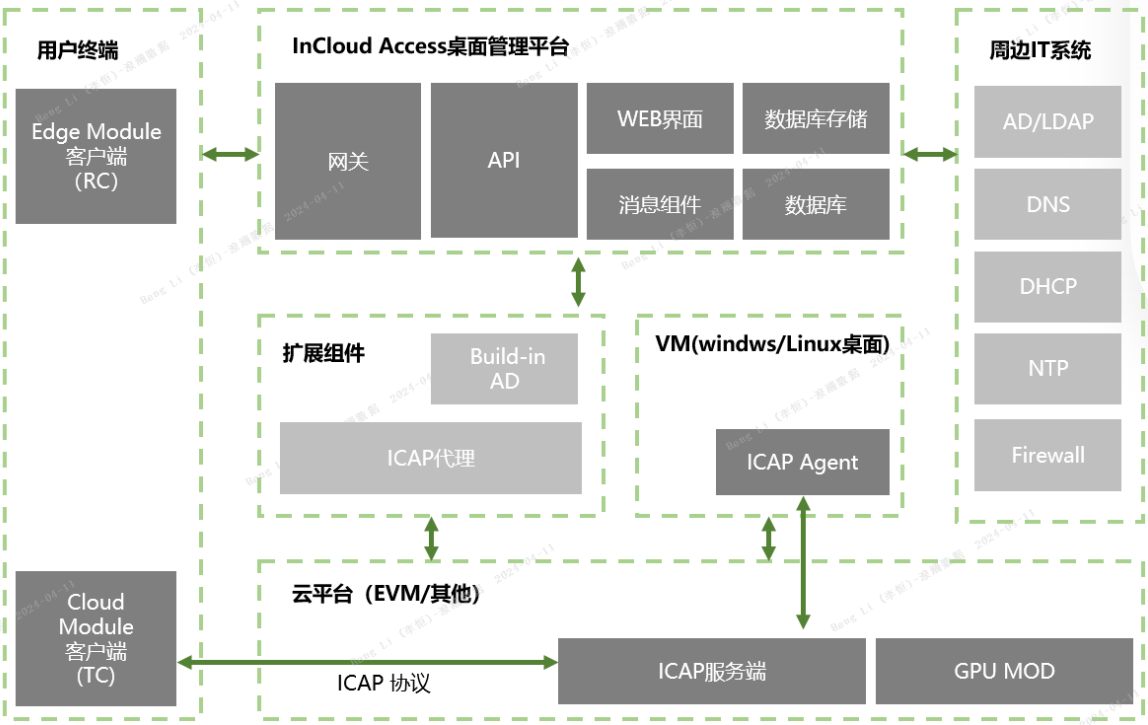


图 2 InCloud Access 组件逻辑关系

各组件功能描述如下：

表 1 系统组件说明

组件	子组件	功能简介
核心组件	API 组件	核心组件，控制整个应用的业务处理。实现了桌面的生命周期与电源管理、桌面与用户的关系管理、用户和用户组管理、终端管理、策略管理、管理员管理、license 控制以及其他设置等。
	网关&终端管理	是终端和桌面连接的管理者。该组件是 API 和终端的中间件，处理终端和 API 之间的通讯。同时，实现对终端的管理能力，简化终端运维工作，支持丰富的终端策略。
	监控	负责对系统、桌面运行情况进行监控。

	WEB GUI	InCloud Access 应用的 WEB dashboard， 可视化的管理 InCloud Acces 的各种配置与服务。具体包括： ---具备强大的桌面管理功能，支持桌面的生命周期管理，开机/关机/挂起/恢复/重启/启用/禁用/删除；支持显示桌面的名称/状态/关联信息/IP/设备/创建日期；支持桌面的设备管理，GPU 设备挂载/移除；支持桌面的设备管理，数据盘挂载/移除；支持指定桌面的显示名称编辑；支持指定桌面策略配置，支持相同桌面池下不同桌面的差异化策略配置；支持桌面与用户自动关联，桌面池与用户组关联时，用户组下用户登录终端时，自动为其创建桌面并关联；支持桌面与用户关联的指定与解除；支持桌面远程协助，管理员可在不影响用户登录的同时远程协助用户操作云桌面；支持修改云桌面计算机名。 ---支持终端的生命周期管理，开机（部分型号）/关机/重启/删除；支持终端的自动纳管，终端连接管控平台自动纳入默认终端组管控；支持显示终端的序列号/型号/最后登录用户/IP/连接记录；支持显示指定终端上已连接的设备，支持设置指定设备的策略权限控制；支持终端生命周期管理/移动的批量操作；支持终端组下终端检索；支持 PC 客户端、手机/平板客户端的管控平台便捷下载。 ---支持配置全局的 UI 个性化设置，包括浏览器标题、图标、登录页 LOGO、首页 LOGO。支持受管控平台管控的终端策略配置终端登录的 UI LOGO。支持配置终端登录的 UI LOGO。 ---概况页面可对管控平台中的云桌面、用户及终端资源进行实时统一监控和总览。支持丰富的系统告警功能，可通过手机、邮箱接收告警信息。
	消息组件	负责系统通讯管理，负责与页面、IaaS 控制器、API 组件间的消息通知。
	数据存储组件	后端数据存储组件，主要用于做终端策略等消息的下发。

	数据库组件	InCloud Acces 系统的数据库，原生可信赖的稳定与高效，存储应用的所有业务相关数据。
桌面协议	ICAP 协议	ICAP 是实现通过客户端 TC 远程访问虚拟桌面的接入协议。支持 H.264/265 以及硬件加速处理，支持 GPU 桌面显示的高性能协议。
	ICAP 服务端	安装在阿里云平台中的 ICAP 协议服务端，是用于处理来自 ICAP 协议客户端的键盘鼠标，音频的输入与输出，USB 外设输入与输出等请求和响应消息。
	GPU MOD	配合 ICAP 实现普通桌面加速、以及 MXGPU 等 GPU 桌面的功能模块
桌面云组件	ICAP Agent/Driver/Tools	安装在虚拟桌面中的 ICAP 协议客户端,区别 Windows 和 Linux 虚拟桌面，是用于处理来自 ICAP 协议服务端的交互请求以及配置信息。
客户端组件	InCloud Access客户端	安装在接入终端 TC/SC 中的 ICAP 协议客户端，用于发起连接虚拟桌面请求，接收并处理 ICAP 协议服务端的请求和响应消息。包括： - TC 全称 Thin Client，虚拟桌面接入终端 - SC 全称 Software Client，非 TC 设备上的虚拟桌面接入终端软件
扩展组件	Build-in AD	实现 windows 虚拟机的注册表、组策略等管控，实现批量安装软件、补丁升级、其他任何 windows 设置
	ICAP Proxy	在特殊网络环境下，集中代理分布的协议端口
虚拟化组件	ICS 虚拟化	负责将服务器的 CPU、内存、磁盘、I/O 等硬件资源通过虚拟化技术转化成可以动态管理的“资源池”，可以兼容第三方基于 QEMU-KVM 虚拟化平台

2.3.3 服务器硬件

浪潮 InCloudAccess 系统可部署于标准的 x86 设备，广泛支持主流厂家硬件，根据需求灵活配置，无须与平台软件进行绑定，提供充分的用户选择空间。

X86 服务器：提供桌面云所需的计算资源，主要包括 CPU 资源和内存资源，支持主流厂商的服务器硬件设备，如通用 X86 服务器、国产 X86/ARM 服务器等。在一体机和超融合架构下，X86 服务器同时提供平台所需的存储资源，以满足各类不同场景的实际需求。

集中存储：在 SAN 架构下，计算资源与存储资源分离，InCloud Access 支持各类存储设备，如磁盘阵列、存储服务器等，支持 SDS/FC SAN/NAS 等存储。

分布式存储：以 X86 服务器为主，在超融合场景下，存储资源主要使用服务器本地硬盘，通过文件系统，将不同服务器上的存储资源整合成逻辑资源池，支持分布式存储，通过两副本或三副本，大幅提高系统可用性。

2.3.4 智能云终端

智能云终端是指连接到 InCloud Access 管理平台中，使用管理员创建的桌面云的终端设备。云计算中，业务的使用和展现通过终端实现。终端根据架构及最终展现形式主要有如下两种类型：

瘦客户端

瘦客户端 TC（Thin Client）是一种终端设备，用于将用户接入数据中心，并处理桌面云协议。它通过网络连接使用 InCloud Access 管理平台中的桌面云资源，无硬盘、光驱。TC 体积小巧，耗电低，使用寿命长。瘦客户端通常需要安装基于 Linux 的操作系统，因此也称为 Linux 客户端。

瘦客户端根据架构又可以分为 ARM 终端和 X86 终端两种。

软终端

软客户端（Software Client）是指安装在 PC 或者移动设备上（包括便携笔记本、上网本、平板电脑、智能手机等）的软件客户端，需要单独安装。用户通过软终端使用 InCloud Access 管理平台中的桌面云资源。InCloud Access 产品配套软终端支持 Win7/Win10/Win11/Android 等系统。

3 功能及实现原理

3.1 桌面协议

3.1.1 模块设计

从大的层面上说，InCloud Access 云桌面产品分为管理平台和协议管理 2 个部分。

管理平台起始于管理界面和终端界面，结束于云桌面的生命周期管理；而协议管理起始于终端连接上云桌面，结束于断开连接。

这两个部分是可以看做是互相不影响的 2 个管理层面，也可以是这个产品互相依赖的组成部分。

3.1.1.1 管理平台的实现

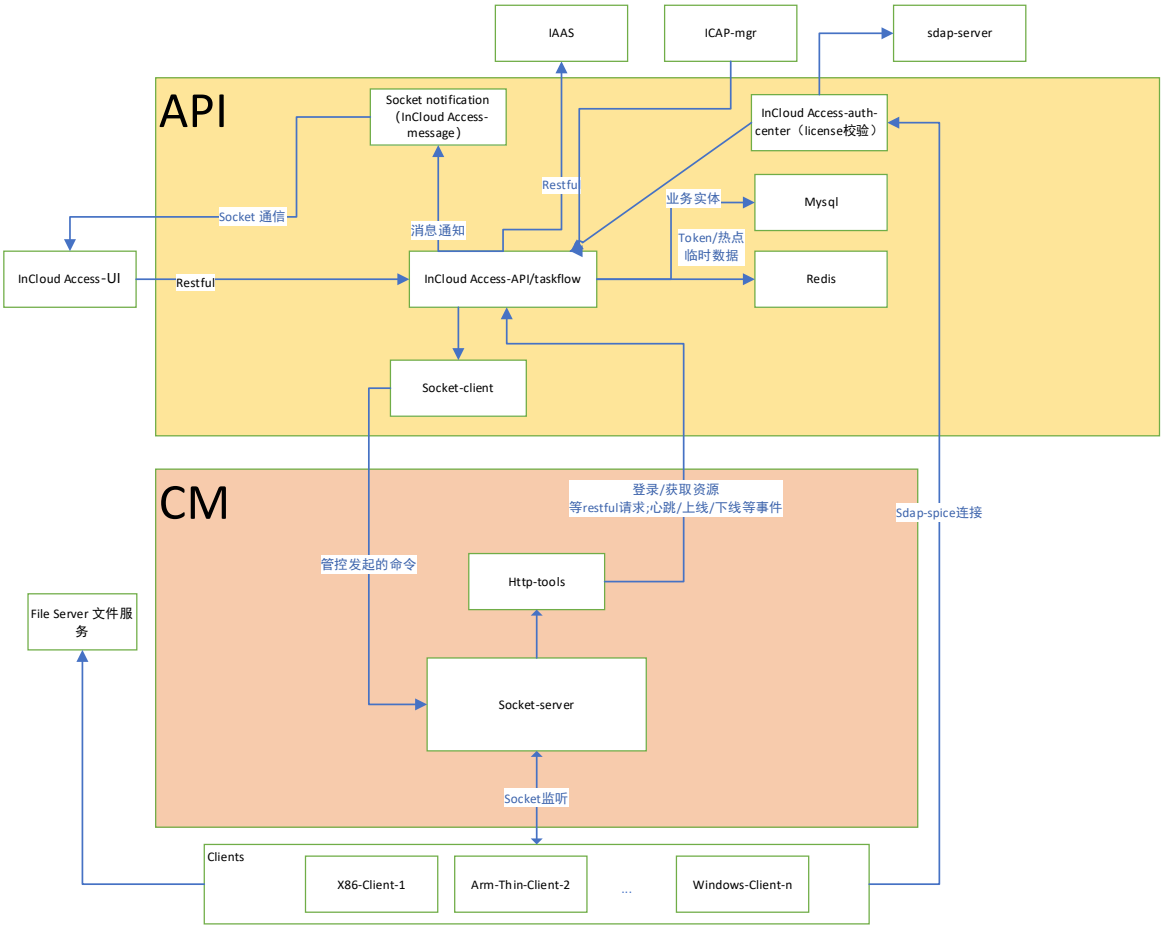


图 1 管理平台的组件结构

图 1 主要描述了管理平台的组件之间数据流转的示意图，可以看到主要有以下几个线路：

1. 管理页面调用线路 1：UI 通过 restful 接口调用 API 组件，API 收到请求之后，进行业务处理，如果业务没有涉及到虚拟化底层，那么直接走 mysql/redis 这样的存储；处理结果通过 message 给前端通知。
2. 管理页面调用线路 2：如果线路 1 出现有需要处理虚拟机底层数据（比如调用 openstack 接口创建 vm），那么除了需要数据库之外，还需要调用 IAAS 接口。
3. 管理页面调用线路 3：如果 1 线路出现有长时间处理的任务或者需要异步操作，此时需要 taskflow 来处理，处理结果通过 message 通知给页面。
4. 管理页面调用线路 4：如果 1 线路请求的对象是终端，那么 API 需要发消息给 CM，CM 转给终端
5. ICAP -mgr 上报信息线路：ICAP -server 定时上报云桌面的内存、CPU、磁盘使用率等信息给管控 API，管控 API 入库。
6. auth-center 校验 license 线路：云桌面开机时会启动 ICAP -server，ICAP -server 向 auth-center 发起 license 校验。
7. 终端业务线路：终端发起请求到达网关 CM，cm 是一个 socket server， cm 根据业务内容向管控 API 发起请求，API 之后的路线参考管理页面调用线路 1/2/3。
8. 终端连接云桌面线路：终端通过 API 得到 spice 地址之后，终端通过内置的 player 连接 spice 地址
9. 终端获取升级文件线路：终端在网关连通之后，会向文件服务器发起请求，获取升级包以及自定义 logo 等。

3.1.1.2 协议管理的实现

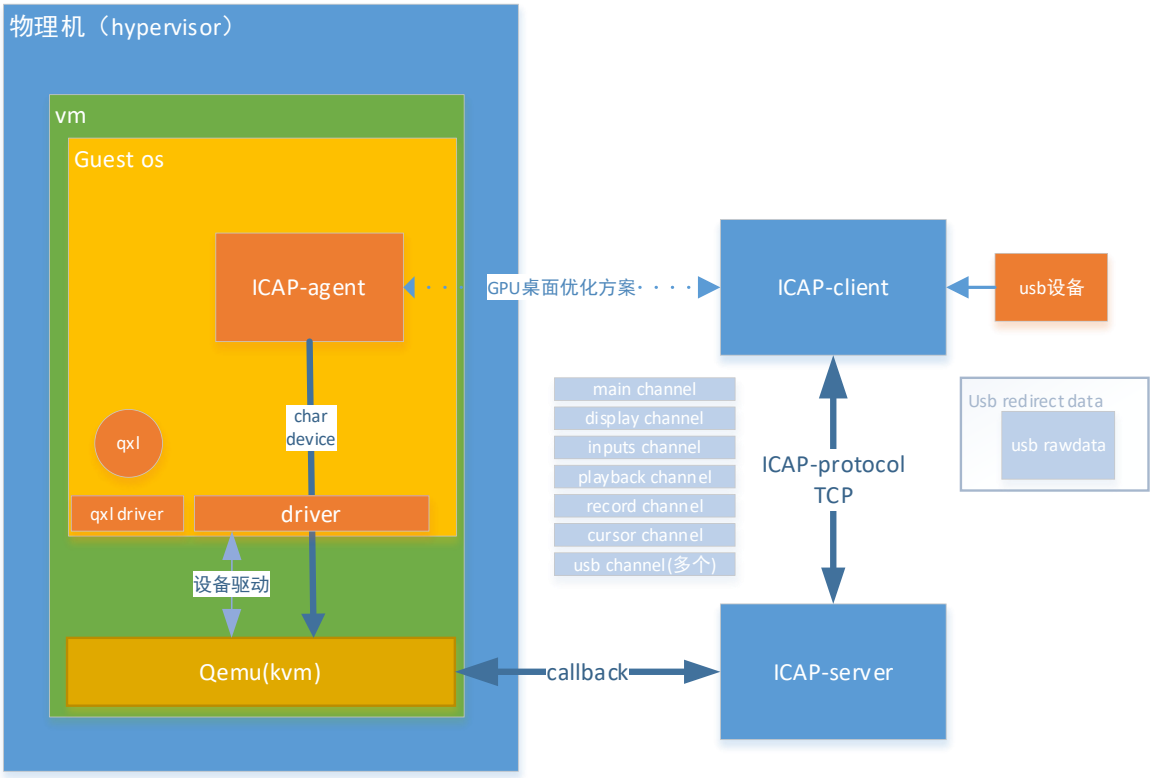


图 2 spice 组件结构

组件职责

ICAP（InCloud Access Protocol）组件是浪潮科技自主研发的高效桌面传输协议，主要包含 ICAP-server，ICAP-client 和 ICAP-agent。其中：

1. ICAP -server 部署在物理上，是 qemu-kvm 的一个外部库，随 vm 启动而运行，vm 关机而销毁。ICAP -server 会在 qemu-kvm 内注册各种 callback 函数，从而实现其机制。ICAP -server 会暴露相应的 ip:port 来作为 ICAP 协议数据传输通道。

   - 是一个类库，有多个 so 文件组成，被 qemu-kvm 进程调用。
   - 提供与 qemu-kvm 定好的接口，在进程启动时，注册到 qemu-kvm 进程中。
   - 将 qemu-kvm 提供的数据编码为 ICAP -protocol 数据格式。
   - 解码从 ICAP -client 传过来的输入操作。

2. ICAP -client 就是 InCloud Access-player。player 连接 ICAP -server 暴露的 ip:port 成功之后，即可接受 ICAP -server 的 spice 协议数据包，ICAP -client 在终端上对协议包进行解包渲染，展示在终端的屏幕上。

   - 监听客户端设备的键鼠、usb 外设（摄像头、usb 存储、打印机等）等各种输入设备的输入数据；进行数据编码；转成 spice-protocol 标准协议数据，通过 TCP 连接传给 qemukvm 进程；qemu-kvm 通过提前注册好的 callback hook 接口，处理相应的数据。

   - 接收经过 ICAP -server 压缩编码通过 qemu-kvm 进程发出的数据，根据 ICAP -protocol 协议标准，解码数据，并进行相应的输出（声音播放；画面渲染等）。

3. ICAP -agent 部署在云桌面内部，可以调用操作系统提供的接口和一些设备提供的接口（比如 nvdia GPU 显卡）实现云桌面的一些功能，比如打印机，比如 GPU 桌面等。

   - GPU 桌面的显示画面数据捕捉；并且把捕捉数据进行压缩编码后通过 qemu-kvm 转给 ICAP-server。

   - 处理一些剪切板操作和文件传输等。

3.1.2 云桌面协议介绍

3.1.2.1 ICA

ICA（Citrix Independent Computing Architecture）是 Citrix 公司开发远程协议架构，Citrix 在 1989 年成立时,就一直拥有这个当前仍然保密的协议。ICA 协议是基于 TCP/IP，与平台无关（Windows、Linux 甚至是 DOS 都可运行），共定义了 32 个虚拟通道（虚 拟通道可以简单理解为缓存，类似于 USB 的端点），其中 16 个是系统通道，用于传输 视频、音频、剪贴板、磁盘、打印和外设，还有 16 个客户自定义通道，像有的高拍仪等外设产品就可以用这些通道。ICA 的特点是远程图像传输采用的是矢量数据处理方式，即把图形数据分为位图、文字、图形命令，再通过压缩算法传输至终端，再渲染显示，因此 ICA 性能上比较突出的特点是较低的带宽占用，在弱网高

延迟、高抖动）的情况下也能正常使用。ICA 不仅支持 Citrix 自家的虚拟化平台 XenServer，还支持 vSphere 和 Hyper-V。

3.1.2.2 RDP

RDP（Remote Desktop Protocol）是微软的远程桌面协议，是微软公司操作系统标配的软件，RDP 传输的也是位图数据，只是经过压缩，因此也需要较大的带宽。微软本来有能力把 RDP 做得相关完善，但微软一直不待见 RDP。从 RDP 协议 7 版本之后，微软终于实现了 RemoteFx 技术，不仅实现了 USB 设备映射，也实现多媒体播放重定向，即将码流压缩后传到终端上，然后用终端的 CPU 来解码播放。

3.1.2.3 SPICE

SPICE（Simple Protocol for Independent Computing Environments）是一款开源虚拟桌面协议，该协议是 Redhat（红帽）公司研发的，该协议来源是由 Qumranet 公司 开发的一款开源网络协议，经过几年的社区开发，SPICE 协议不断成熟。SPICE 协议对于视频具有一定的优越性，其主要原因还是对于显示信息的压缩处理由 KVM 完成，避免了 GuestOS 内由于视频压缩对于 CPU 的过量消耗。SPICE 协议采用无损压缩，所以清晰度较高，缺点是带宽较高，消耗的资源较大。

3.1.2.4 PCoIP

PCoIP（PC-over-IP）是由 VMware 与 Teradici 共同开发的协议，以改进自己的 VDI 解决方案 VMware View。PCoIP 和硬件结合紧密，数据的编码和解码，图形的处理可以 通过专门的硬件来完成，让 CPU 有精力来做其他的事情，也有专门集成了 PCoIP 显示芯片的显示器。PCoIP 是基于 UDP 协议的，UDP 传输不可靠，但是 UDP 没有 TCP 的三次握手复杂的校验和数据恢复，传输速度快，适合多媒体的传输，同时由于传输的是位图数据，体验仍然不如基于 TCP 协议的 ICA。PCoIP 的缺点是带宽占用相对较高，原生 PCoIP 协议没有串并口等外设的重定向能力，但一些 TC 厂商通过额外的端口重定向插件弥补了其这方面功能的不足。目前 Vmware 正在研发自己的

3.1.2.5 ICAP 高效桌面传输协议

浪潮自主研发了高效的 ICAP（InCloud Access Protocol）桌面传输协议，使用流化技术传输云桌面。InCloud Access 对桌面内容进行编码，把桌面的视频流下载到客户端播放，因此视频码率不会因正在运行的程序的不同而变化，支持场景化压缩编码技术，支持 H.264、H.265 编码，云桌面通过 InCloud Access 协议进行桌面画

面传输，智能云终端本地解码后呈现在本地显示器。

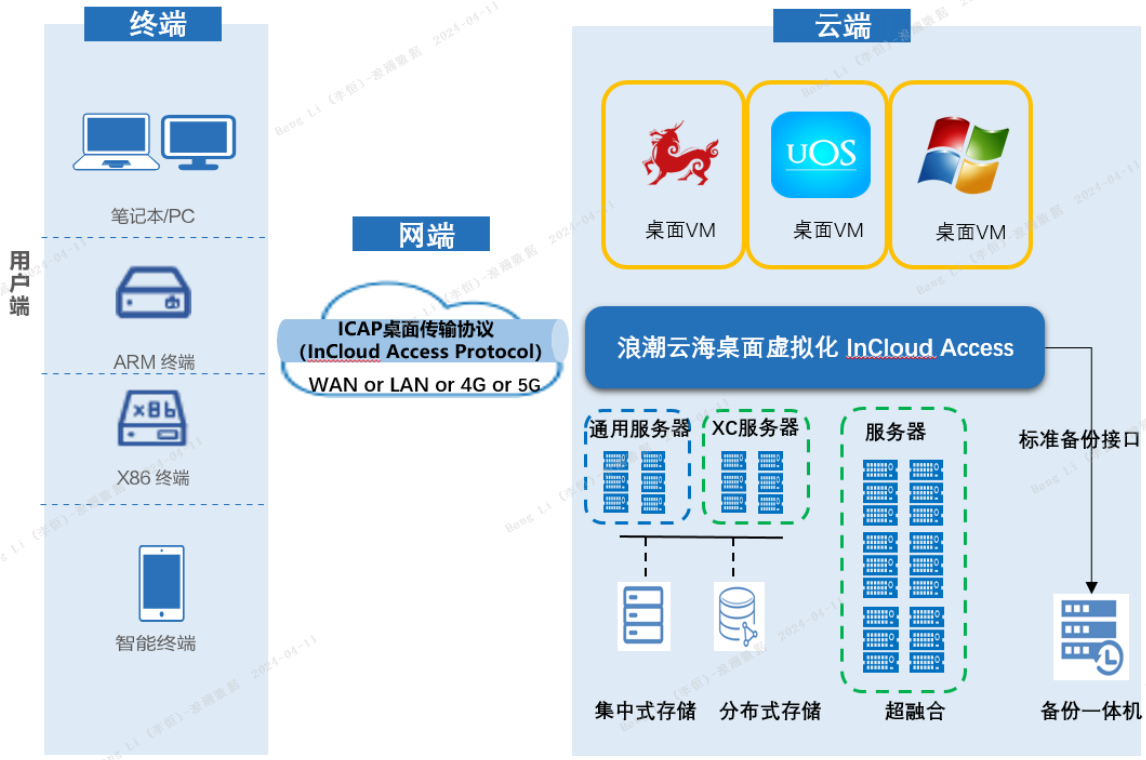


图 3 终端数据传输过程

其特性如下：

- 画面智能侦测（自然和非自然图像），某些场景下带宽低至几 KB
- 支持多通道传输，提高传输效率
- 桌面流化 VBR（动态比特率）传输，支持文本、音视频、3D 建模、云游戏
- 加密传输，提高安全性和数据保护
- 支持 H.264、H.265 硬件编码加速，提高单机桌面并发数
- 支持多种格式、多种播放器的超高清视频播放 4K/8K@60FPS，和云游戏场景，并且不依赖于瘦终端的能力

InCloud Access 传输协议采用分布式处理架构，每台服务器独立完成所承载云桌面的显示图像编码，消除了传统集中式云桌面接入网关的性能瓶颈和高可用架构缺陷。

3.1.3 InCloud Access 协议主要功能

3.1.3.1 普通桌面显示技术

显示流程

云桌面要实现远程屏幕显示，首先实现虚拟机截图，再对截图进行去重压缩等处理，然后发送至终端。虚拟机截图的方案常见的有两种,一种是应用层调用系统的截图 API 进行截图，这种截图方案性能消耗大、效率比较低，该方案目前用于 VNC、Teamview 等远程工具，不适合云桌面场景。另一种方案是封装虚拟的显卡驱动，在虚拟显卡驱动层拦截绘图命令，该方案效率非常高，且性能消耗小，在 QEMU 架构中，直接可以通过 QXL 设备发送给 Host 机处理。

VDI 普通桌面画面展示流程如下：

gust-os ---> qxl ---> driver ---> qemu-kvm -->InCloud Access-server(buffer) --> InCloud Access -client

普通桌面的画面通过 qxl 显卡设备把相应的 io 指令通过 driver 传到 qemu-kvm 层，被 InCloud Access -server 识别到，spice-server 缓存一定数量的帧画面，使用 H.264 或者 H.265 格式进行压缩编码转成 InCloud Access -protocol 数据，通过 display-channel 把数据转给 InCloud Access -client。InCloud Access client 获取到数据进行解码，渲染到客户端的显示器上。

压缩技术的好坏直接影响了终端用户的使用体验。InCloud Access 传输协议支持 H.264/H.265 编码压缩方式，用以满足复杂的业务场景及带宽需求。通常的 H.264 编码方式适用于局域网/专线环境，H.265 编码方式适用于互联网/VPN 环境。

3.1.3.2 GPU 桌面显示技术

显示流程

gust-os ---> nvdia gpu ram ---> InCloud Access -agent---> qemu-kvm --> InCloud Access -server(buffer) --> InCloud Access -client

由于 GPU 桌面的显卡设备不再是虚拟的 qxl，而是 nvdia 等 GPU 设备，此设备的画面显示数据不再通过 qemu-kvm 模拟设备处理，而是直接通过 nvdia 设备驱动进入

GPU 设备的 ram 空间。InCloud Access -agent 通过 nvdia 接口抓取 ram 内的显示数据，然后进行压缩（直接使用 GPU 卡进行压缩）并编码再转给 InCloud Access -server.。此时 InCloud Access -server 再把该数据当成普通桌面的画面数据一样进行传输。

InCloud Access 产品支持 GPU Passthrough、AMD MxGPU、NVIDIA VGPU 等主要的 GPU 方案。在项目中可以根据用户需求灵活选择。

与此同时，InCloud Access 采用先进的 CPU+GPU 异构双算力架构，一方面采用全规格 GPU 桌面，在客户端提供高性能 vGPU 架构，支持多种主流 GPU，满足客户设计渲染需求；另一方面，在服务端将云桌面图像编解码压力给到 GPU，有效释放 CPU 性能，提升计算效率。可为企业打造专业、可靠、高性能的云图形工作站，可完美支撑中大型 2D/3D 设计、超高清视频、云游戏等高端场景。

GPU Passthrough

GPU Pass-through，即 GPU 透传模式，就是将主机的多块物理 GPU 按照一比一的比例分配给此主机上运行的云桌面。此模式下，物理 GPU 被指派给每个云桌面用户。该方式避免了 GPU 共享模式带来的抽象层开销，最大限度提升虚拟化 GPU 性能体验。

如下图所示：

图 8 InCloud Access 直通模式示意图

InCloud Access 基于 GPU Pass-through 可搭配 NVIDIA GeForce GTX 1050 或其他规格显卡，实现云端计算资源与后台 GPU 资源的一对一映射绑定，支持创建高性能虚拟工作站，提供简单安装和操作，保障关键数据安全以及卓越的性能表现，以满足用户 IT 建设及使用需求。

在此架构下，我们可以使云计算技术拥有比拟传统 PC 甚至工作站 GPU 显卡的特性，支持 3D 图形显示处理、视频编解码、图形处理硬解码等。用于满足大型游戏、

AutoCAD、Solidworks、ArcGIS、Revit、Maya、CATIA 等场景的 2D/3D 高端使用需求，及视频监控相关业务系统多路视频播放的使用需求。

对比传统 GPU 软件虚拟化：

传统虚拟化桌面由于是在物理 GPU 层上端做了资源池化，然后将池化后的资源通过软件算法及协议分配给多个用户进行使用，很容易受限于算法质量，导致虚拟化层显卡资源效率低下，同时还会大概率出现资源分配不均等，小部分用户占用大量资源的情况。

InCloud Access GPU Pass-through 方案，搭配 4U 服务器，单服务器最多可提供 8 个高性能（性能参数 8C 16G 1T 2G 显存）的 GPU 直通云桌面，完美解决以上问题，我们将物理显卡直接映射到对应的云桌面，独立调用，资源独占，越底层的协议意味着越高效。每块显卡资源由单一桌面调用，可以开启显卡的所有物理属性及软件 API 特性。支持 OpenGL、DirectX®、 OpenCL 等所有核心协议。支持客户视频监控业务的多路视频码流硬解码，降低 CPU 资源消耗，保障前段显示流畅无卡顿。即使在处理 CAD 图纸、GIS 地图、3D 建模的软件需求时，也可做到性能游刃有余，满足客户高性能业务需求。

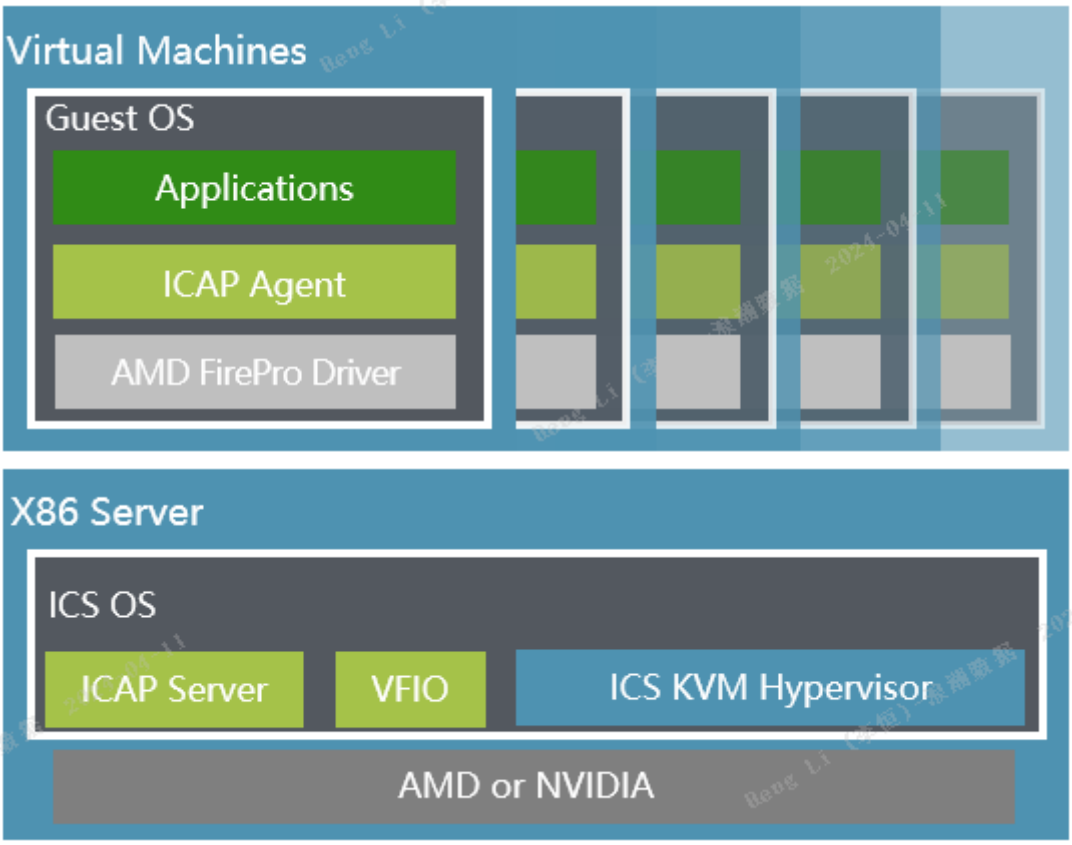


图 9 InCloud Access GPU Passthrough 架构示意图

适用场景：

用于满足大型游戏、AutoCAD、Soildworks、ArcGIS、Revit、Maya、CATIA 等场景的 2D/3D 高端使用需求。

NVIDIA Vgpu

InCloud Access 支持由 NVIDIA 虚拟 GPU 助力的 VDI 环境，虚拟 GPU 软件与管理程序一同安装在虚拟层。通过虚拟 GPU 软件创建虚拟 GPU，使每台虚拟机能够共享安装在服务器上的物理 GPU。NVIDIA 虚拟化软件包含每台虚拟机的图形驱动程序。Quadro vDWS 包含强大的 Quadro 驱动程序。由于通常由 CPU 完成的工作转移到了 GPU，因此用户获得更好的体验，并且现在可以在虚拟化和云环境中支持严苛的工程和创意应用程序。

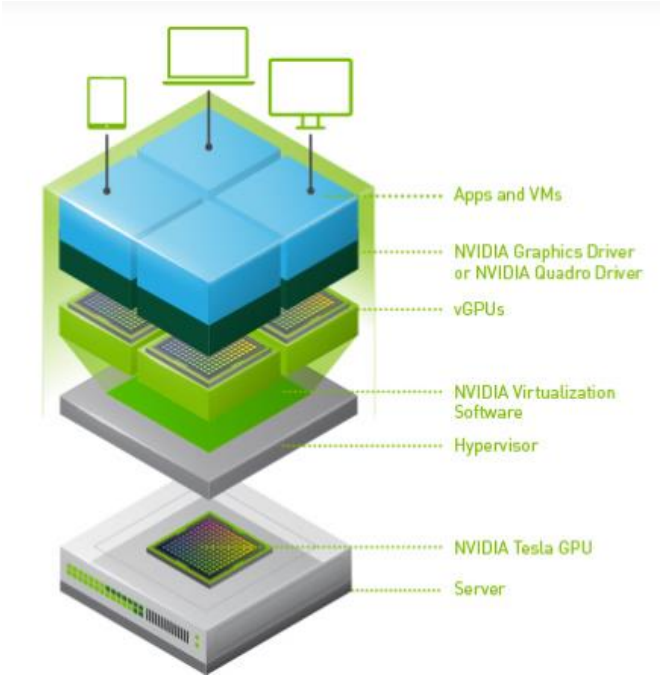


图 10 NVIDIA vGPU 架构示意图

vGPU 引入了内存管理单元处理虚拟机地址空间与物理地址空间之间的地址转换。更高级的 vGPU 还包括了足够多的独立输入缓存用于接收来自不同虚拟机的输入流，允许每台虚拟机都有自己的 vGPU。

vGPU 和 GPU 共享以及 GPU 直通模式相比，各有特点，vGPU 像虚拟化其他系统组件那样虚拟化 GPU 具有独特的优势：vGPU 与 GPU 共享不同，vGPU 没有额外的抽象层或者 API 转换，因此延迟更低；vGPU 与 GPU 直通模式不同，vGPU 能够同时在多个虚拟机之间共享一个 GPU。

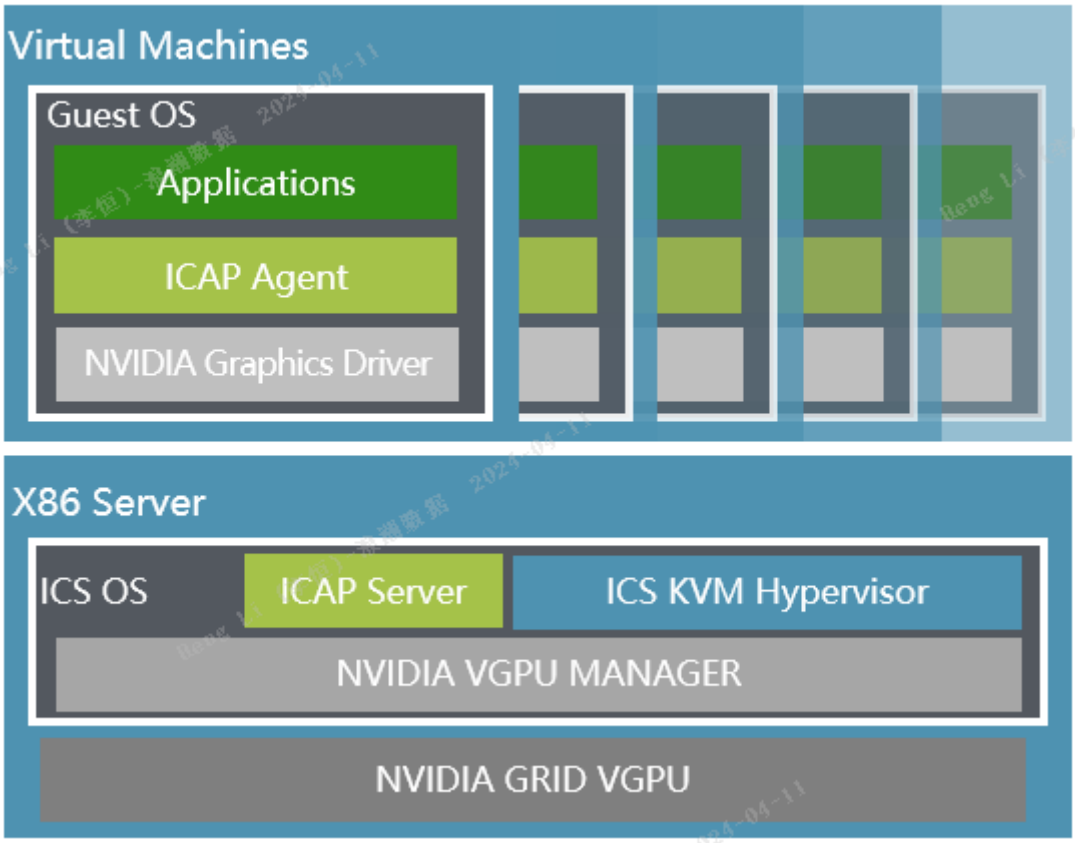


图 11 InCloud Access vGPU 架构示意图

适用场景：

InCloud Access 基于 vGPU 的 GPU 解决方案用于满足游戏、AutoCAD、Solidworks、ArcGIS、Revit、Maya、CATIA 等场景的 2D/3D 中端使用需求。

AMD MxGPU

在虚拟化生态系统当中，如 CPU、网络控制器和存储设备等关键部件都被硬件虚拟化，以提供最佳用户体验。AMD MxGPU 技术第一次将虚拟化行业标准引入 GPU 硬件，实现 GPU 硬件虚拟化。

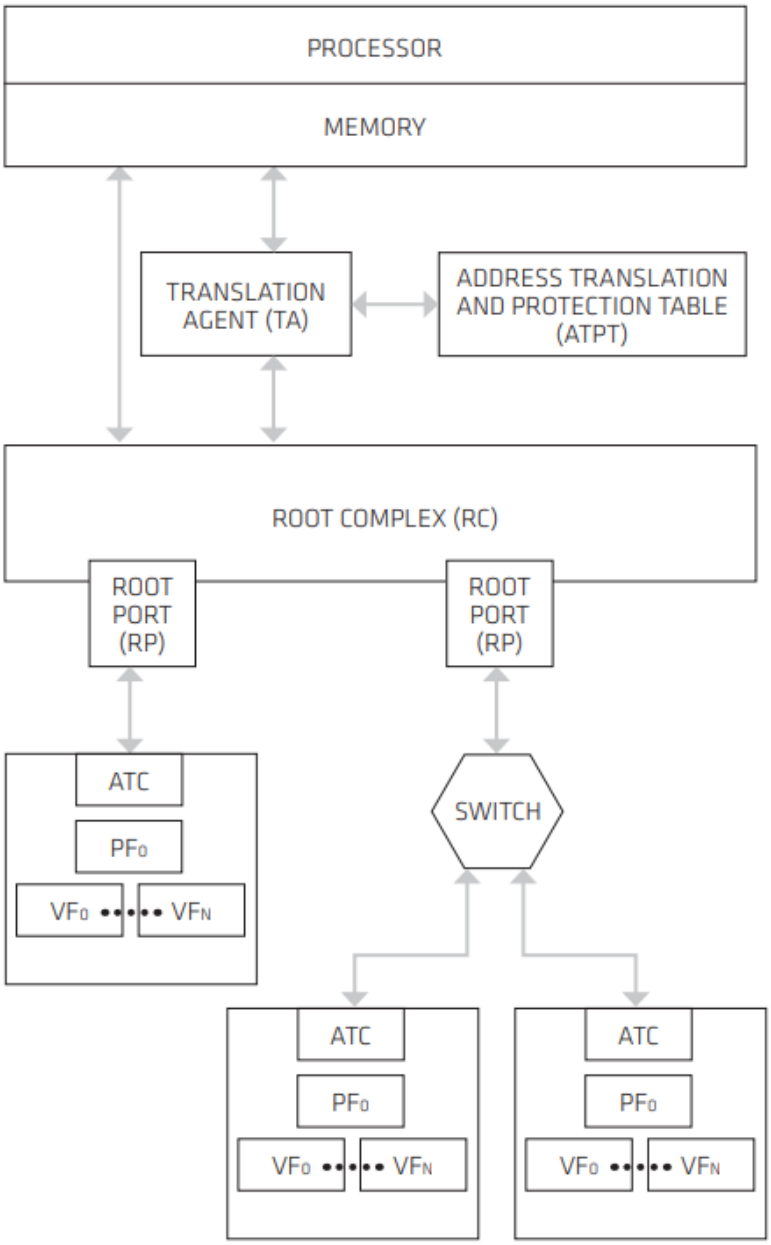


图 12 MxGPU SR-IOV 架构示意图

MxGPU 通过底层控制 GPU 调度，为用户提供可预测的服务质量，这意味着跨越虚拟机的稳定性能和安全性能。InCloud Access 基于 MxGPU 的 GPU 解决方案完全基于 SR－IOV 标准，提供一致的、可预测的性能：

为用户提供 GPU 硬件调度逻辑和高精密服务质量。

通过硬件强制隔离内存逻辑，防止一个虚拟机访问另一个虚拟机数据，从而保护虚拟机应用程序数据以及数据完整性。

将 GPU 所有图形功能暴露给应用程序，不仅允许完全虚拟化支持 DirectX 和

OpenGL 等图形 API，也允许其支持如 OpenCL 等 GPU 计算 API。

GPU 硬件虚拟化面向计算、渲染中载应用，一般的 3D 图形处理，让多个 VM 共享一个虚拟化的 GPU，针对有大量绘图需求的企业，高密度并发，降低 GPU 用户的成本。GPU 虚拟化将一块物理显卡虚拟化为多个虚拟显卡，每个 VM 绑定一个 vGPU，支持多 VM 共享单 GPU 的图形加速能力，满足 3D 应用的图形渲染需求。

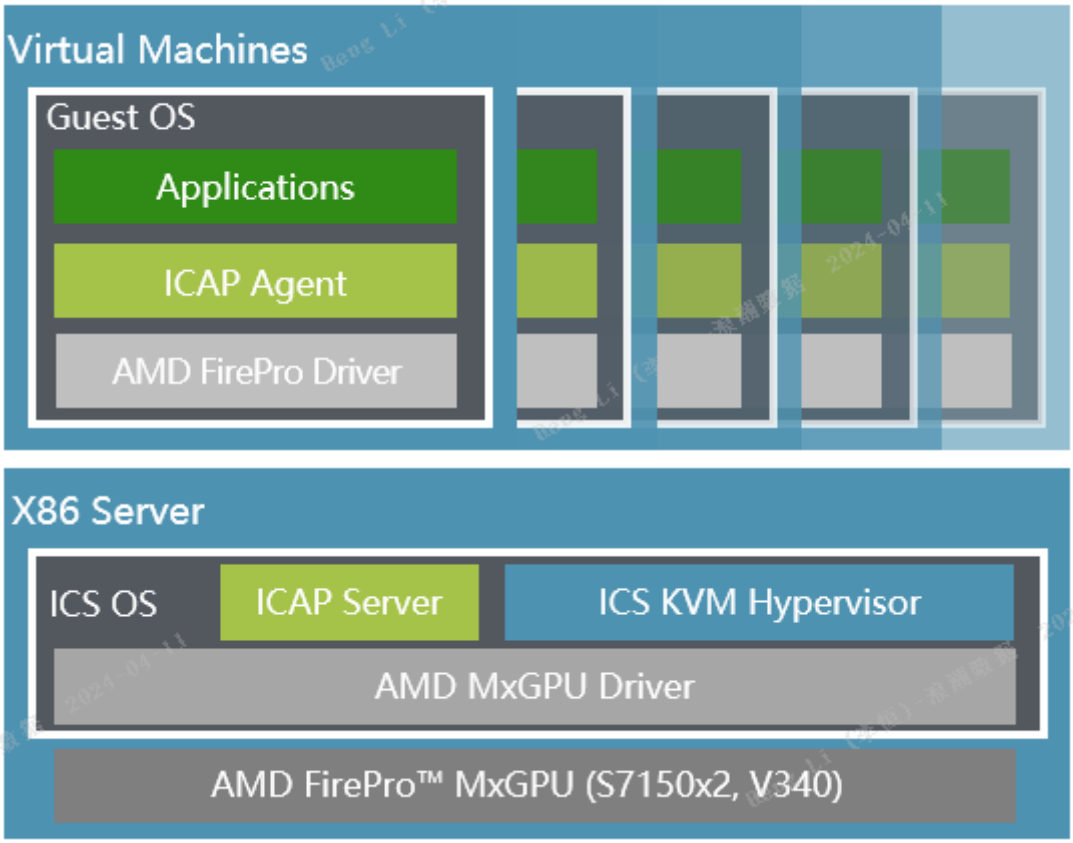


图 13 InCloud Access MxGPU 架构示意图

适用场景：

InCloud Access 基于 MxGPU 的 GPU 解决方案用于满足游戏、AutoCAD、Solidworks、ArcGIS、Revit、Maya、CATIA 等场景的 2D/3D 中端使用需求。

3.1.3.3 音频技术

在 InCloud Access 中，QEMU 模拟一个音频设备给虚拟机，虚拟机直接使用标准的音频驱动即可，音频 APP 调用系统音频处理接口（录音、播放），虚拟声卡设备进行交互。

音频 APP 调用系统音频播放接口播放音频数据时，音频驱动将收到音频子系统发

送过来的音频数据，并将音频数据发送给音频设备，音频设备再把音频数据推送给云桌面的服务端，服务端对音频数据进行压缩处理后传输到云桌面客户端，云桌面客户端进行解码并进行放音。

音频 APP 调用系统音频录音接口获取录音数据时，云桌面客户端读取本地系统录音数据，编码后并传输到云桌面服务器端，云桌面服务器端对录音数据进行解码后，并把数据推送给音频设备。

InCloud Access 协议音质具有高音质、时延低的优势，能够提供更加清晰的声音，准确还原声音细节。通过对浪潮云桌面协议 InCloud Access 的双向语音优化，实现 VOIP 数据流的带内传输。用户只需在瘦客户机上连接耳麦即可使用，并能保证高质量、低延时的语音传输，通话质量清晰、无卡顿。

3.1.3.4 视频技术

InCloud Access 云桌面采用 InCloud Access 协议，开创性的使用流化技术传输虚拟桌面。云桌面视频播放场景，由于视频帧率比较高、变化区域比较大，需要消耗的带宽也比较大，普通图形处理流程无法满足视频场景，故需要对视频场景做进一步优化。虚拟机内部播放视频时直接解码并显示视频画面，云桌面服务端画面智能侦测，图片与视频分别处理，对视频区域的图形进行重新视频编码处理，然后将视频编码数据传输到客户端进行解码播放显示。

由于云桌面软件对桌面内容进行编码，把桌面的视频流下载到客户端播放，因此视频码率不会因正在运行的程序的不同而变化，1080P 分辨率时仅占用带宽约 4Mbps（最低可低至 3Mbps），网络流量恒定。瘦客户机只需要播放视频，功能简单。虚拟桌面播放高清视频时不需要做视频内容的重定向，减轻了传输网络的负担。

InCloud Access 能够完美支持 720P（1280×720）、1080P 分辨率（1920×1080）、4K（4096×3112）、8K（7680 × 4320）高清视频播放，不限定播放器及视频文件格式，并且播放高清视频不依赖终端能力。

InCloud Access 还可借助 GPU 硬件加速方案或 GPU Passthrough 方案，支持诸如客户视频监控业务的多路视频码流硬解码，降低 CPU 资源消耗，保障前段显示流畅无卡顿。

3.1.3.5 外设重定向技术

现在市面上的外设各式各样，特别是 USB 外设，一种接口能兼容众多的外设，这也是 USB 协议的优势。如果从外设提供的功能来分，则种类繁多，如：U 盘、移动硬

盘、摄像头、智能卡读卡器、UKey、加密狗、打印机、扫描仪、高拍仪、USB 耳机等。外设重定向的定义就是将外设与虚拟机的通信，通过一个重定向通道进行连接，使得外设在虚拟机使用跟在物理机使用达到一样效果。

InCloud Access 通过深度融合在虚拟化底层去做外设映射,即不需改变和依赖虚拟机操作系统,保留了和 PC 一样的总线通道,这样可以完全消除总线和设备驱动的对接问题，兼容性极大提升，让用户可以像在 PC 一样使用各种外设。

对于云桌面场景来说，利用外设重定向技术来实现通用 USB 外设重定向的过程相对来说比较复杂。这里用一个 U 盘在 ARM 客户端的使用做具体描述。过程如下：

InCloud Access-client --> usb 数据打包成 useb-redirect 协议数据-->qemu-kvm--> InCloud Access -server--->driver(gustos)

1. ARM（如 A2001）盒子的安卓系统接收到一个 U 盘插入的事件后，系统会通知到桌面终端。
2. 客户端收到消息后，接下来就开始获取 U 盘的信息，包括 VID（Vendor ID，供应商识别码）和 PID（Product ID，产品识别码），配置信息等等。客户端在收到 U 盘插入的消息，然后就 Reset U 盘了。
3. 客户端获取到 U 盘的一些信息后，就给虚拟机发送一个 U 盘插入的事件。客户端通过 USB 重定向通道通知虚拟平台 HCI 的虚拟 USB 主控制器，虚拟机收到事件后创建一个虚拟机设备，然后虚拟主控器就将事件告诉虚拟机。
4. 虚拟机收到有 U 盘插入的事件之后，就通过 USB 映射通道向客户端发送命令，获取 U 盘的信息，获取 U 盘基本信息完成后，就在虚拟机里面给 U 盘找到匹配的驱动。这个过程跟物理 PC 是一样的。
5. 虚拟机找到匹配的驱动后就关联起来，用户就可以在虚拟机对 U 盘进行读写操作，就像在物理机使用 U 盘一样了。
6. 用户在虚拟机读写 U 盘的操作，都会变成命令通过 USB 重定向通道发送给 VDI
7. 客户端解释这些命令，然后转换为 ioctl 系统读写 U 盘，再将读写的结果通过 USB 重定向通道传回 Windows 虚拟机。使用结束、或者中途拔出 U 盘，ARM 盒子就会收到一个热拔出事件，然后这个消息也会传递到虚拟机，虚拟机就会取消跟

驱动的关联，这个跟 PC 上使用的是一样的。然后 ARM 盒子也将取消 usbfs 驱动与 U 盘的关联，这时候 USB 重定向通道也就释放了。

8. USB 外设策略配置

9. 通过 USB 设备的管理界面可以创建各种重定向相关的策略配置，并能有针对性地应用这些策略配置，目前支持的重定向策略简要描述如下。

表 1 USB 策略

策略分类	策略名称	策略选项
设备权限	允许 USB 存储器	如 U 盘、共享桌面 USB 设备。 决定是否允许 USB 存储类设备（U 盘）的映射。 可选项 1：只读模式：允许读 USB 存储器数据，不允许向 USB 存储器写数据。。 可选项 2：读写模式：允许虚拟桌面与 USB 存储器双向读写数据。
	允许 USB 打印机	决定是否允许 USB 打印机的映射。 可选项：启用、禁用，默认选项：开启。
	USB 智能卡	如 Ukey。 决定是否允许 USB 智能卡的映射。 可选项：启用、禁用，默认选项：开启。
	USB 音频设备	如麦克风、耳机。 决定是否允许 USB 音频设备的映射。 可选项：启用、禁用，默认选项：开启。
	USB 视频设备	如摄像头。 决定是否允许 USB 视频设备的映射。 可选项：启用、禁用，默认选项：开启。

	其它 USB 设备	如手机、Hub 集线器、串口转 USB。 决定是否允许如上以外的 USB 设备的映射。
设备优化规则		当用户插入 USB 设备时，主机设备会依次根据每条策略规则对其进行检查，直至找到一个匹配项。任何设备的第一个匹配项都被视为最终选择。 设备策略规则的格式为 Allow:或者 Deny:后接一组以空格分隔的 tag=value 表达式。
USB 外设黑白名单	新增外设权限	在已经设置的设备访问权限之外如果需要设置排除在设备权限管控之外的设备。 通过例外设备的 VID、PID 和描述信息添加设备。

10. 不同终端设备的重定向规则

表 2 不同终端的设备重定向规则

型号	HID 设备-键盘鼠标	HID 设备-磁性手写笔，游戏手柄	其他 usb 设备	重定向方式
S1000-W /S1000-M/S1000-L	默认不重定向 默认使用客户端鼠标	默认不重定向	默认不重定向	USB 设备菜单中勾选
A3000/A3001/A3002	默认不重定向 默认使用客户端鼠标	默认重定向	默认重定向	USB 设备菜单中勾选
x2000/A2001	默认不重定向	默认重定向	默认重定向	USB 设备菜单中勾选

	默认使用客户端鼠标			

11. USB 设备菜单中的设备列表受 InCloud Access 管理平台桌面策略中的 USB 策略控制。如果某款 USB 设备无法使用，特别是一些多功能设备，可能存在策略冲突，而导致某些功能无法使用，请联系管理员配置相应策略。

3.1.4 InCloud Access 协议关键技术

3.1.4.1 H.264/H.265 编码精细控制

InCloud Access 从两个维度提供了有关协议方面的控制：InCloud Access 管理平台可以集中配置协议参数，并下发到各个终端上；终端侧可以独立配置协议控制，如果和管理平台配置参数冲突，那么优先选择本地，同时我们可以做到更为细颗粒的协议参数控制。

普通桌面和 GPU 桌面

支持协议传输画面视频质量的自定义设置，包括视频编码方式：H.264/H.265/自适应；编码格式的类型及数值的精细控制。

普通桌面协议参数说明见表 3，GPU 桌面协议参数说明见表 4。

表 3 普通桌面协议参数设置说明

参数名称	设置说明
编码方式	采用的编码协议。 —自适应：根据终端类型自动选择适应的编码协议，终端类型为 A2000、A3000 和 AX2000 时协议为 H.265，其他终端使用 H.264 协议。 —H.264：使用 H.264 编码协议，普通办公场景选择 H.264 协议即可。 —H.265：使用 H.265 编码协议，适用于工业设计和高清视频播放等对画面质量要求高的场景。如果普通桌面要使用 H.265 协议，请使用 GPU 硬编环

	境，如 P2000 显卡，并且只有当终端类型为 A2000 或者 A3000 时才可使用 H.265 编码协议，其他类型的终端不支持 H.265 协议。
编码格式	画面编码格式及参数设置。 —CRF：CRF 是恒定质量的编码方式，通过设置参数值来定义视频质量，参数值越小视频质量越高，同时视频文件越大。 —VBR：VBR 动态编码方式，可设置视频的比特率范围，以适应不同的视频质量。 —CRB：CBR 是恒定码率的编码方式，与 CRF 相反，视频比特率保持的恒定值，视频质量变化较为明显，适用于视频质量变化范围小的场景。 —QP：QP 为恒定码率的编码方式，通过设置参数值来定义视频质量，参数值越低视频质量越高，同时视频文件越大。
视频帧率	配置显卡每秒编码次数。高的帧率可增加画面流畅度，但同时会增加显卡和客户端的负载。

图 14 协议传输设置-普通桌面

表 4 GPU 桌面协议参数设置说明

参数名称	设置说明
编码方式	采用的编码协议。 —自适应：根据终端类型自动选择适应的编码协议，终端类型为 A2000 或者 A3000 时协议为 H.265，其他终端使用 H.264 协议。 —H.264：使用 H.264 编码协议，普通办公场景选择 H.264 协议即可。 —H.265：使用 H.265 编码协议，适用于工业设计和高清视频播放等对画面质量要求高的场景。只有当终端类型为 A2000 或者 A3000 时才可使用 H.265 编码协议，其他类型的终端不支持 H.265 协议。

色彩格式	采用的色彩编码格式。YUV 是一种颜色编码方法，通过亮度信息（Y）与色彩信息（UV）定义画面质量。 —YUV444：保留了完整的色彩信息，同时占用的网络带宽相对较高。A2000、A2001、A3000 和 A3001 终端不支持 YUV444 色彩编码格式。AX2000 终端选择 H.265 编码方式时不支持 YUV444 色彩编码格式。 —YUV420：移除了一半的水平和垂直色彩信息，以便降低带宽的使用。
编码格式	画面编码格式及参数设置。 —CRF：CRF 是恒定质量的编码方式，通过设置参数值来定义视频质量，参数值越小视频质量越高，同时视频文件越大。 —VBR：VBR 动态编码方式，可设置视频的比特率范围，以适应不同的视频质量。 —CRB：CBR 是恒定码率的编码方式，与 CRF 相反，视频比特率保持的恒定值，视频质量变化较为明显，适用于视频质量变化范围小的场景。 —QP：QP 为恒定码率的编码方式，通过设置参数值来定义视频质量，参数值越低视频质量越高，同时视频文件越大。
视频帧率	配置显卡每秒编码次数。高的帧率可增加画面流畅度，但同时会增加显卡和客户端的负载。

图 15 协议传输设置-GPU 桌面

3.1.4.2 支持 H.265 编码

目前业界主流云桌面采用 H.264 编码，InCloud Access 在支持 H.264 编码基础上，前瞻性的支持 H.265 编码。H.265 又称之为 HEVC（高效率视频编码）或者 MPEG-H Part 2，是由 ISO/IEC MPEG 和 ITU-T 组织联合成立的 JCT-VC（Joint Collaborative Team on Video Coding）定义和发布的。从最初 2013 第一个版本到 2017 年经过了几年的发展，目前逐步成为主流的视频编码技术，可以支持 4K/8K 等超高清的图像编码。

采用 H.265 编码相比 H.264 编码，在画质提升、带宽消耗、存储需求等方面，有较大提升。同时，配合 InCloudAccess 特有的硬件编码技术，在更进一步降低服务器 CPU 压力的同时，提高用户体验。

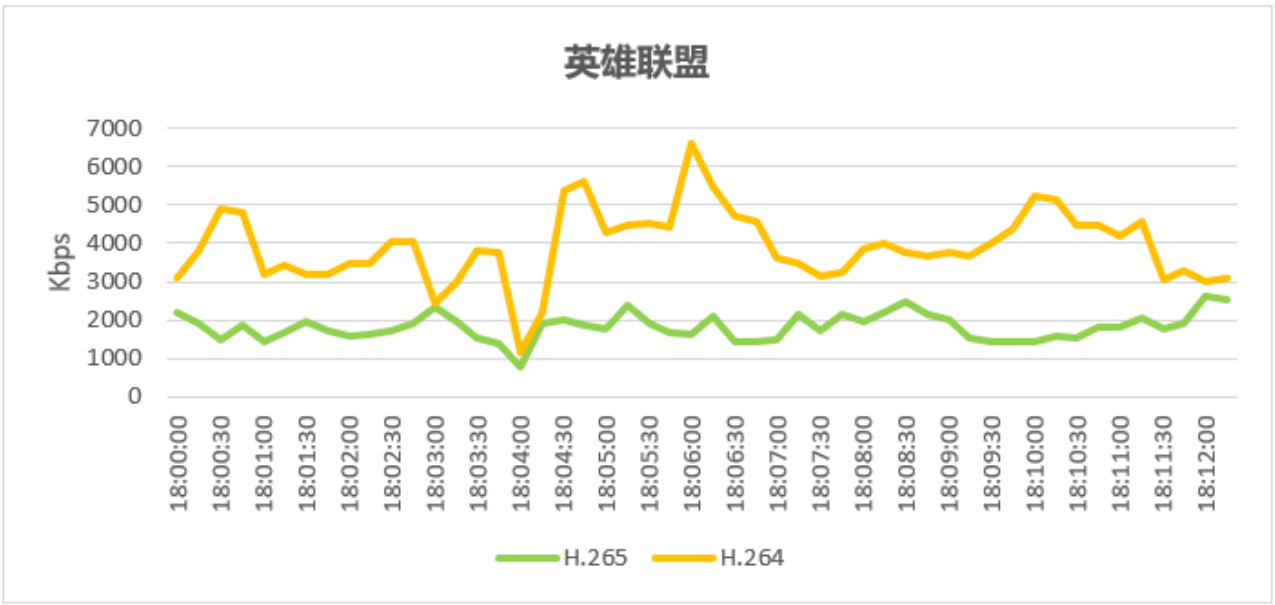
InCloud Access 是业内首个为普通 OA 桌面实现桌面图像硬件编码加速和采用 H.265 编码的云桌面传输协议。

互联网部署环境下，InCloud Access 云桌面借助于自研高效桌面传输协议 InCloud Access 和 H.265 编码，则可节省超过 30-40%的带宽资源，降低互联网带宽消耗和成本，同时，桌面体验保持良好。

图 16 H.265 vs H.264 对比

浪潮桌面云平台 InCloud Access 基于 H.265 编码的流化桌面传输技术，在不降低用户体验情况下，大幅降低超高清视频播放等高端场景对传输带宽的需求。可以在 4K/8K 视频场景中，为用户提供良好的视觉体验，同时，浪潮把 GPU 编码技术引入云桌面产品，采用 CPU+GPU 的融合架构。大幅降低对 CPU 资源的消耗，可以增加单台服务器承载桌面的并发能力。

游戏场景英雄联盟及 1080P 高清视频播放：



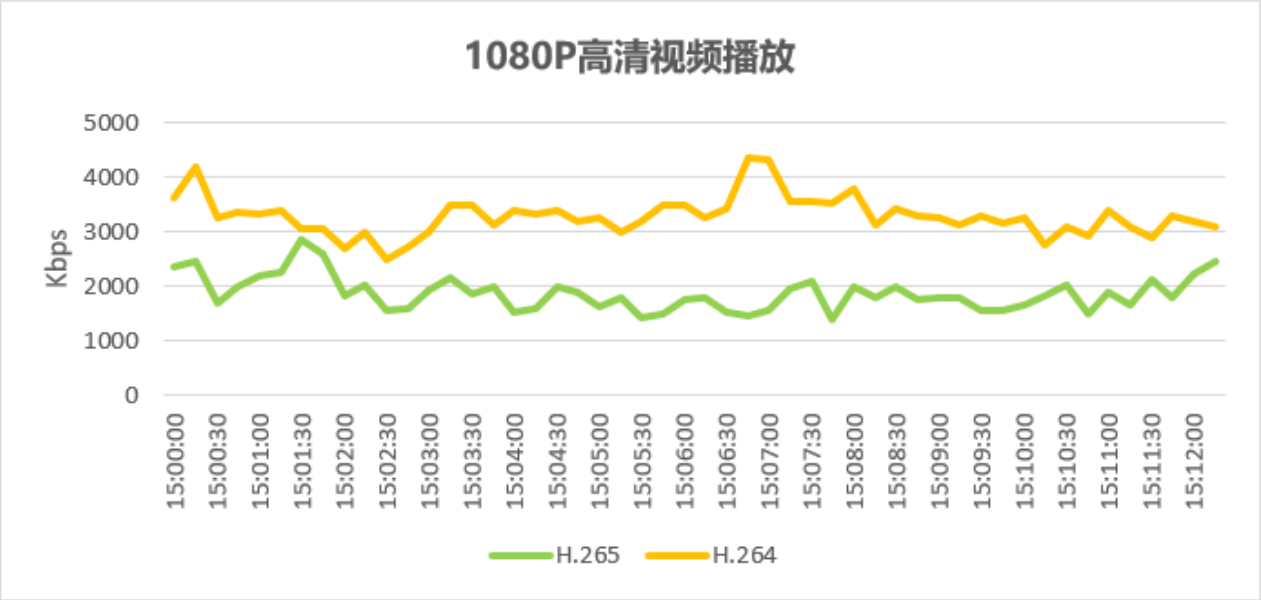


图 17 采用 H.265 编码对宽带资源需求大幅降低

3.1.4.3 通道化传输，互不干涉

图 18 多通道传输

InCloud Access 协议的 Client 端与 Server 端同时提供专用通道以支持各类外设，每个通道类型专用于一种特殊数据类型传输。它将数据逻辑分离，通过添加一个新的虚拟通道来完成客户端的新设备的加入。每个通道中的内容都可以通过相应的图形命令数据流或代理命令数据流进行传输

客户端将每个通道实现为一个单独的线程，每个通道就是客户端与服务端一个的网络连接。客户端启动后会首先与服务器建立连接，连接建立之后，客户端首先向服务器发送查询命令，请求服务器支持的 Channel 类型，然后客户端对所有支持的 Channel 一一创建对应的 Channel 类实例，每个实例都会开启自己的工作线程并向服务端发起连接请求，从而建立网络连接。InCloud Access 协议通过多通道技术与客

户端进行不同资源数据传输，提高了资源通道传输控制的灵活性和针对不同资源通道管理的能力，能够兼容各种常见外设，并且定制化开发能力很强。

3.1.4.4 硬件加速技术

InCloud Access 采用独特的硬件加速技术，支持单机高并发，降低系统造价，提高性价比。InCloud Access 将云桌面图像编码的负载从 CPU 卸载到 GPU 上，可以有效释放 30%左右的 CPU 性能，增加服务器承载桌面数量的同时，提升最终用户使用体验。

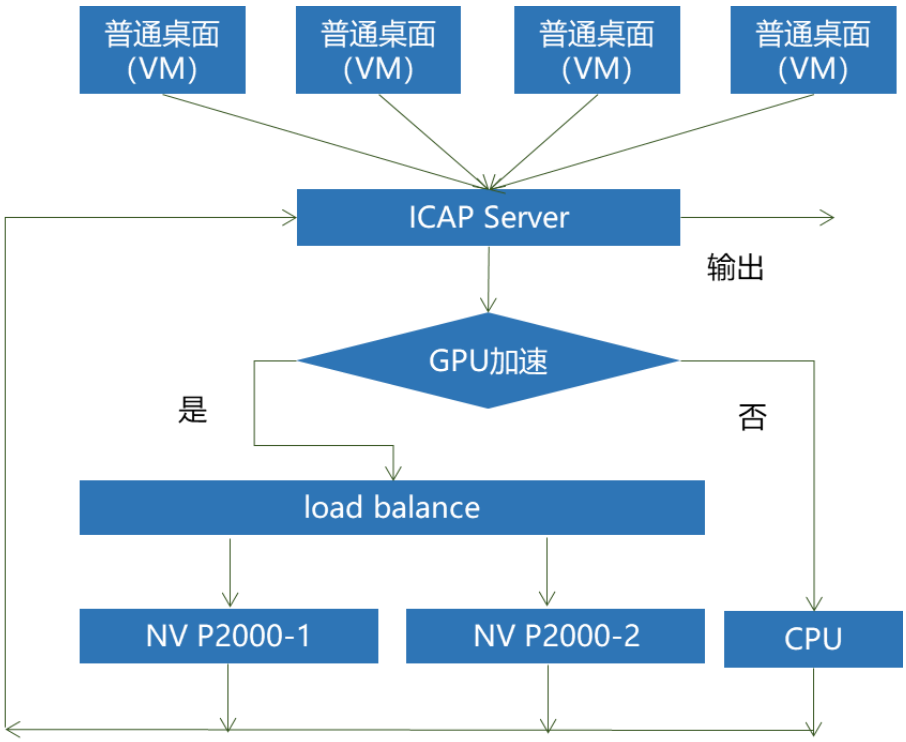


图 19 GPU 硬件加速原理图

浪潮把 GPU 编码技术引入 InCloud Access 产品，服务器采用 CPU+GPU 的组合，CPU 负责支撑用户桌面上面的应用程序，GPU 负责视频编码，这样才能达到最佳的资源利用效果。InCloud Access 的 GPU 编码功能遵循以下几个原则：

- 尽可能地将任务并行化，同时在 CPU 和 GPU 上并行地处理。
- 因为 GPU 与计算机主存的交换速度很慢，因此要尽量减少 GPU 与主存的数据交换，将数据尽可能地留在 GPU 中进行计算而不是反复读写。
- 尽可能地将编码任务交给 GPU 来做，减轻 CPU 的计算量。

InCloud Access通过GPU辅助编码技术能够在各种场景下为每个用户提供1080P的桌面分辨率，重度高清图像应用场景时，云桌面系统支持的桌面数不变，用户体验不下降。

表 5 GPU 加速测试数据

测试场景	无显卡加速模式 CPU 利用率	显卡加速模式 CPU 利用率
播放视频	11% ~ 13%	6% ~ 8%
播放视频 + CPU 加压	31% ~ 34%	25% ~ 28%
视频帧率	配置显卡每秒编码次数。高的帧率可增加画面流畅度，但同时会增加显卡和客户端的负载。	

3.1.5 InCloud Access 协议性能

3.1.5.1 云桌面网络流量构成

云桌面的网络流量构成主要包括以下几部分：

- 云桌面远程桌面访问流量

云桌面远程桌面访问流量是指客户端到云桌面间的流量。

云桌面远程访问协议一般主要传输的是虚拟桌面的图像信息，图像信息主要包括桌面图像的像素点编码以及图像变化的变化量编码信息。云桌面远程桌面访问流量与远程桌面传输协议有关。

- 虚拟机访问业务系统流量

传统终端的访问模式有 B/S 和 C/S 模式，不同的业务场景要求终端侧网络带宽情形不同。如文档处理类用户，主要的网络流量来自邮件、办公 OA 系统，发生在虚拟机与邮件系统或办公 OA 系统之间;软件开发类用户主要的网络流量可能是虚拟机与软件版本控制服务器之间的流量，或虚拟机之间的软件传输;系统维护类用户的主要流量是虚拟机与运维管理系统间的访问流量，如实时的监控数据、日志数据等。云

桌面与业务系统的流量应根据云桌面业务的类型特别考虑。

- 虚拟机访问互联网流量

云桌面用户访问互联网时与目前 PC 终端用户的需求很相似。在特殊的任务场景中，一般的工作终端允许用户访问互联网资源，如信息检索、新闻浏览、即时消息、网络视频、P2P 下载等，这些互联网访问会带来巨大的网络压力。以前，这些网络流量是各分散用户 PC 终端通过企业统一的互联网出口实现进出的。云桌面将用户的互联网流量直接汇聚到云桌面平台交换机，通过云桌面系统所在的数据中心互联网出口汇聚交换。

- 虚拟机间相互访问流量

虚拟机间相互访问流量反映到云桌面网络中，可能是一台服务器内部虚拟网络的流量，也可能是服务器间、虚拟机间的流量。这种流量一般是用户以 P2P 方式互相访问或传递文件。

3.1.5.2 影响云桌面网络带宽占用的因素

影响云桌面的网络带宽的因素如下：

- 桌面传输协议

桌面传输协议，指的是一组特殊的数据传输规则，可以使云桌面和客户端之间的数据有序并高效传输，从而达到“丰富而流畅”的用户体验。云桌面和客户端之间传输的数据包括视频、音频、图像、键盘鼠标输入以及其它外设输入。云桌面传输协议是影响网络带宽占用至关重要的因素。

- 使用场景

云桌面所占用的网络带宽会根据业务场景的不同而有所变化：营业厅场景以 Web 查询、操作处理为主；会议演示场景以 PPT 播放为主；客服场景，客服话音打包在远程桌面数据分组中传输，带宽及网络质量必须满足话音通信要求；GPU 场景下，播放 4K/8K 视频时对网络带宽的要求更高。另外，部分外部设备访问带宽需求较大，如打印机，打印数据传输要从数据中心发回本地打印机，带宽占用较大。

- 桌面分辨率

云桌面的分辨率对带宽占用也有一定的影响。

- 云桌面配置

不同的云桌面配置，如普通云桌面和 GPU 云桌面，所占用的网络带宽会有区别。

3.1.5.3 InCloud Access 云桌面在不同场景下的带宽占用

InCloud Access 基于 InCloud Access 协议，大幅降低了视频播放、PPT 播放之列的场景流量，在低带宽占用下能保证视频流畅播放，对于普通办公场景，带宽占用更低，具体如下表所示：

表 6 InCloud Access 云桌面在不同场景下的带宽占用情况

桌面类型	分辨率	编码帧率	最高带宽（KB/S）	最低带宽（KB/S）	平均带宽（KB/S）
普通桌面 Win 10 4C8G	1080P	10fps	1634.35	204.42	783.10
		20fps	2614.86	253.27	1088.32
		30fps	2925.86	249.29	1066.18
	1280*720	10fps	1279.97	130.1	567.57
		20fps	1823.58	179.66	795.56
		30fps	2190	108.4	820.87
	2560*1440	10fps	2530.35	213.5	1137.31
		20fps	2548.54	311.79	1202.04
		30fps	2346	250.11	1133.86
vGPU 桌面 win 10 4C8G	1080P	15 fps	2014.53	329.50	1023.96
		30 fps	2045.24	172.41	1029.46
		45 fps	2003.46	307.50	1037.44

		60 fps	2087.82	219.89	1041.16
	1280*720	15 fps	918.29	99.64	445.27
		30 fps	888.55	143.66	441.98
		45 fps	955.26	97.76	478.34
		60 fps	889.33	119.79	470.08
	2560*1440	15 fps	3960.61	136.30	1751.53
		30 fps	3671.90	120.71	1784.99
		45 fps	3706.91	312.83	1741.65
		60 fps	3639.75	395.52	1787.21

基于自研的 InCloud Access 及智能灵活的桌面策略控制，InCloud Access 高性能云桌面能大幅缩减云桌面图像传输时的流量，有效降低带宽压力，提升用户使用体验，保证用户能获得极致流畅的视频和办公体验。

3.2 安全性

3.2.1 传统桌面安全之痛

1. 终端分散，容易泄密

传统 PC 桌面办公分散，任何一台 PC 都可能是泄密点。为防范泄密，对于像多办公楼、多分支机构的企业，在物理安全上需要再各门岗设置安全岗来检查出入的存储设备介质；在各 PC 端安装安全机箱、数据防泄密软件等。这种方式维护人力多且成本高昂。

2. 多网多终端，管理困难

多网络物理隔离。在移动化办公的趋势下，企业网中也引入了大量的接入终端，管理异常困难，密码记忆不易。一些高安全行业的桌面存在多台电脑及终端的情形，例如一台互联网电脑、一套行业专网电脑、一套办公专网电脑，这些导致现有信息化建设模式变得复杂。

3. 终端安全软件不堪重负

为了保护终端安全，需在 PC 上安装各种安全软件，如防病毒、防木马、个人防火墙、进程保护、桌面管理与监控、USB KEY、终端加密软件、数据防泄密、防非法外联、多因素认证等，电脑不堪重负。众多的软件也带来了大量维护困难。如果电脑崩溃，终端恢复和重装系统的时间耗费也很长。

3.2.2 云桌面安全威胁分析

云桌面作为一种新的计算资源提供方式，用户在享受它带来的高安全、便捷性、低成本等优越性的同时，也对其自身的安全性存在疑虑。云桌面除了需应对传统数据中心的安全威胁，同时页面临着云计算带来的新的安全威胁与挑战：

1. 终端安全风险

- 在云桌面下，虽然用户数据并不会存放在云终端（如瘦客户端 TC），但是也需要防止客户端上被安装恶意软件，如截获键盘操作的木马软件，可能导致登录密码被窃取。

- 云桌面支持多种类型终端接入是云桌面的一个重要特点，因云终端不存放数据，对接入终端的管控在管理上会弱化。需要考虑如何不合规或恶意终端接入云桌面环境导致信息泄密的风险。

- 用户可移动接入带来便利的同时，也会引入一定的安全风险。用户的认证口令信息通过云终端进行传递认证，如果用户密码泄露，非法用户可以利用网络从任意一个云终端接入，因此需要支持比密码更安全的身份认证机制。

2. 网络安全风险

- 传统网络安全威胁仍然存在。云桌面下，用户的所有操作、界面交互都是通过网络进行。同时云桌面接入入口多、分布广，在可连接的地方都可以进行接入，具有遭受网络攻击的风险。

- 云桌面终端与数据中心的数据传输过程中的私密性与完整性威胁。一些敏感信息如密码，可能被窃取；界面交互信息可能被截获，进行协议解析后可能恢复一些重要信息。

3. 虚拟化技术带来的安全风险与挑战

- Hypervisor 的安全威胁

Hypervisor 为虚拟化的核心，可以捕获 CPU 指令，为指令访问硬件控制器和外设充当中介，协调所有的资源分配。而桌面虚拟化通常采用裸金属架构，Hypervisor 运行在比操作系统特权还高的最高优先级上。一旦 Hypersvior 被攻击破解，在 Hypervisor 上的所有虚拟机将无任何安全保障，直接处于攻击之下。

- 资源共享风险

多用户共享计算资源带来的风险。在虚拟化中，逻辑隔离代替物理隔离，隔离措施不当可能会造成数据泄露、病毒攻击扩散。

- 虚拟机间的恶意网络流量可能逃过审计

在同一台物理主机的虚拟机间的通信，如果同在一个虚拟局域网中，可能直接在物理主机中完成通信，导致现有网络监控审计系统无法审计虚拟机间流量。

4. 数据安全

- 数据集中存储在数据中心，如何防范管理员查看、窃取用户数据。
- 云桌面环境中，用户依旧可以使用 U 盘等存储介质，且使用云桌面协议进行数据传输，外部设备难以审计和控制，主动泄密的通道和风险依旧存在。
- 用户桌面虚拟机中的重要数据通过云桌面终端、网络、拍照等方式泄露。
- 物理磁盘更换带来的数据泄露风险。

5. 运维安全

数据集中在数据中心,对管理员的安全要求尤为重要。管理员的身份认证、权限管理、审计等都是很大的挑战。

因此，如何保障用户数据和资源的机密性、完整性和可用性成为云计算系统亟需解决的课题。本章将在分析云计算带来的安全风险和威胁的基础上，介绍了 InCloud Access 针对这些风险和威胁所采取的应对策略及措施，旨在为用户提供安全可信的云桌面解决方案。

3.2.3 InCloud Access 安全架构

inCloud Access 构建了端、网、云、管四维安全防护体系，保障数据安全、系统稳定、桌面可靠。

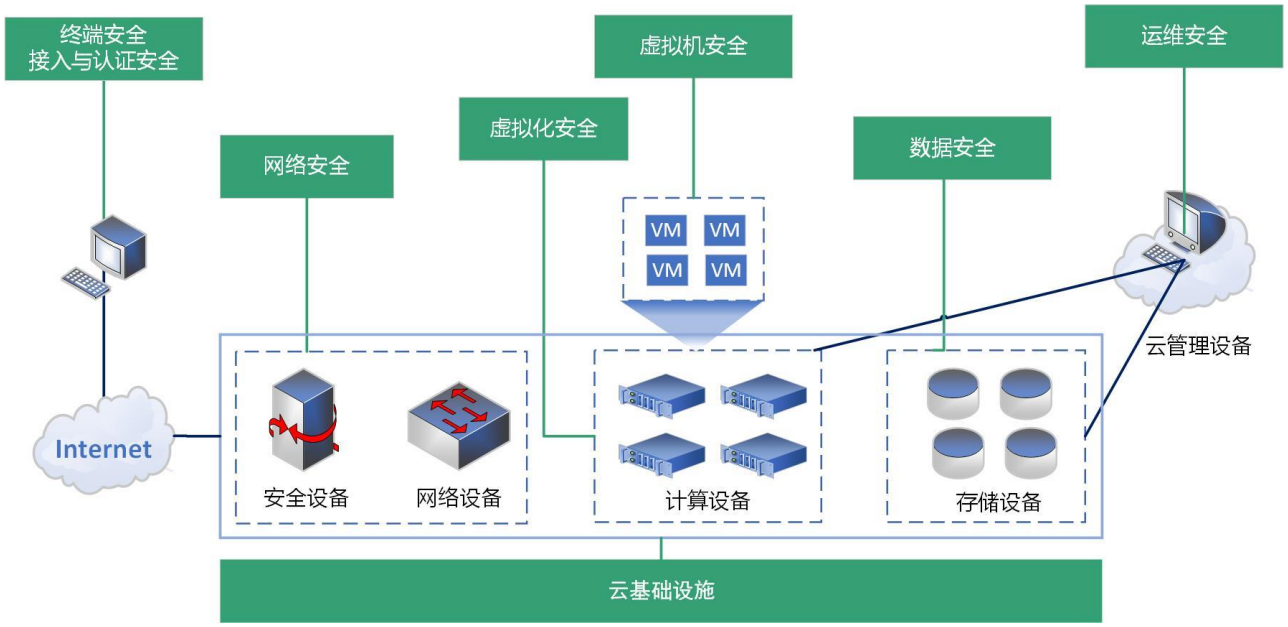


图 1 InCloud Access 安全解决方案框架

各维度简要介绍如下：

- 终端接入及认证安全：

包括终端自身安全，接入认证安全，外设管控以及相关安全策略配置，对所接入云平台的终端和外设进行合法性校验。

- 网络安全

主要围绕网络隔离与行为管控来构建整个云桌面的网络安全体系，包含分布式防火墙，双网隔离，安全域划分，VPN 隧道技术等方面。

- 数据安全

通过双向拷贝限制，屏幕水印，快照和灾备，数据加密传输等措施，保障用户数据免受侵害。

- 虚拟化安全

包含计算，存储，网络虚拟化安全，资源隔离，以及虚拟机内部安全。

- 运维管理安全

包括日志管理，管理员分权分域，自服务及工单可追溯管理、统计报表中心运维与审计等方面。

3.2.4 终端安全

3.2.4.1 瘦终端系统安全

瘦终端从硬件和软件设计上，采用了多种安全机制，有效防止病毒入侵。InCloud Access 所提供的安全机制如下：

- BIOS 安全
- OS 安全

BIOS 安全

BIOS 仅从内置存储引导，并且仅保留从内置存储引导的方式，没有保留其他的引导方式如 USB 引导、PXE 引导等，保证 InCloud Access 云终端不会引导其他第三

方的系统，第三方也无法访问 InCloud Access 云终端内置存储的内容。从硬件级别保证了云终端的安全。

OS 安全

瘦终端是一个精简的、封闭的定制化 Android/Linux 操作系统，系统设计全面考虑了安全性问题，主要包括以下内容：

1. 禁止直接访问内置存储

InCloud Access 云终端在操作系统本地没有暴露内置存储访问接口，用户只能通过系统提供的程序间接访问，这样能有效的避免系统文件被破坏。

2. 禁止任意安装程序

Android/Linux 操作系统的云终端在本地不提供安装软件的接口，用户或者其他第三方人员，无法自行安装任何软件。

3. 网络端口限制

为防止恶意入侵，云终端在本地只开放必须的端口，用于云平台管理云终端，其他端口均被限制对外开放。

4. 无需病毒防护

从病毒的传播途径看，主要为通过存储类设备传播和通过网络传播。对于云终端没有病毒所需要的传播途径及运行环境，完全阻断了病毒传播方式。

3.2.4.2 特定终端接入

账号接入唯一性

应用场景：在信息安全要求高的场合，只允许特定用户从固定地点的终端登录包含敏感信息的虚拟桌面，以避免敏感信息在其它地方被查看。

通过在终端 MAC 地址与域用户、域用户组之间建立 VIP 绑定关系（1 对 1 绑定），实现指定域用户/域用户组成员从固定的终端接入桌面。VIP 绑定的用户，仅可通过该终端登录，无法使用其他终端登录。

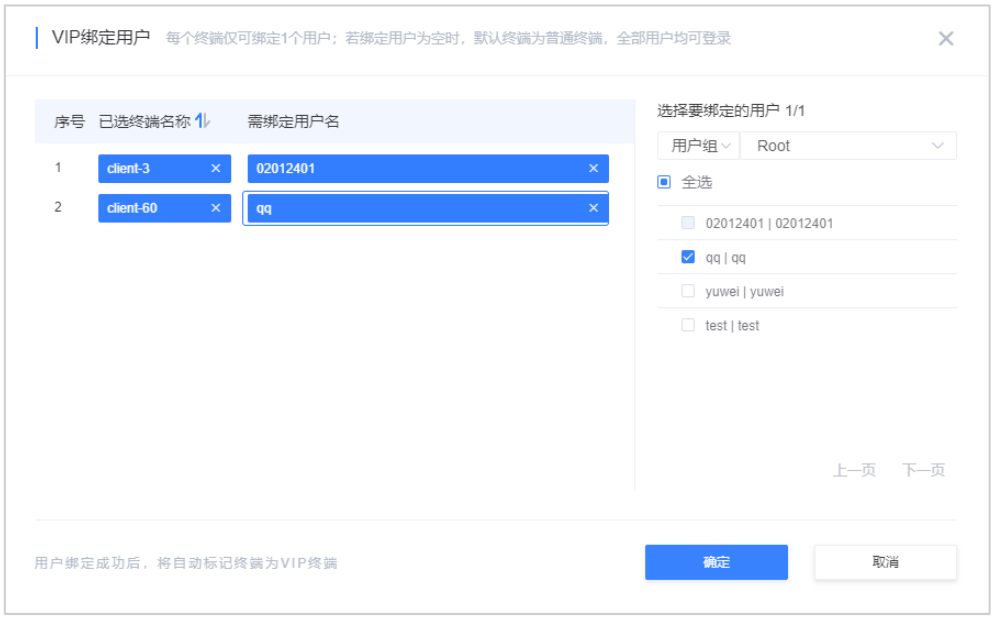


图 2 VIP 绑定用户

登录会话的有效性

为了防止用户离开终端后，账号被盗用，管理员可以在 InCloud Access 管控平台的用户策略管理中配置会话无操作时的超时时间.用户登录认证成功后,如果长时间无桌面会话或没有操作，将主动注销该会话，防止他人盗用该终端。

还可以配置连接在线状态的云桌面时，需正在连接使用的用户确认。开启该策略后，开启后，正在使用的终端用户确认后才能在新终端连接云桌面。

图 3 会话有效性和唯一性

3.2.4.3 接入协议安全

1. 桌面数据不落地

云桌面将桌面数据集中存储，用户终端与数据分离，用户终端无任何存储数据，

实现数据不落地。通过云计算技术，在数据中心运行用户云桌面虚拟机，通过专用传输协议传输屏幕、鼠标、键盘、外设等信息。以此构建一个基于数据不落地的终端桌面环境，这样就从根本上解决了传统 PC 桌面数据泄露的问题。

2. HTTPS 加密保护

支持配置 HTTPS 访问，加密用户访问数据，强化网站用户侧可信展示程度，防劫持、防篡改、防监听。对接国际，国内最值得信赖的第三方数字证书颁发机构(CA)，确保数字证书认证可信力和加密强度，保障用户服务，并支持配置自签名证书，支持更换证书，或导入其他证书，以确保只有经过授权的用户能够访问。

3. 数据传输安全

为了保护用户云桌面的数据传输安全，云桌面终端做了以下处理：

- 终端和服务端的数据传输支持采用 SSL 加密。
- 云桌面的图片数据仅用终端显示，不会写入终端磁盘。云桌面关闭时，内存中显示的图片数据全部释放。

3.2.4.4 接入与认证安全

InCloud Access 支持多种认证方式按需组合，包括本地认证、第三方结合认证（AD/LDAP）、Ukey 等，满足不同级别的接入安全需求。

图 3 认证管理

此外，为提高登录安全性，系统提供了防暴力破解登录功能。当选择“账号密码认证”时，可配置密码输入错误时启用随机图形校验码，以确认用户身份。

3.2.4.5 多种接入及认证策略

InCloud Access 针对用户名和密码认证有相关的策略控制，管理员可以针对不同的场景设置不同的密码策略。密码策略包含密码安全策略、用户密码策略、终端登

录安全及用户自服务管控策略。

密码安全策略

密码策略定义了管理员和用户的密码复杂度，合理的设置密码策略可以保证用户帐号的安全性，避免非法用户操作。包括密码长度、复杂度、找回密码方式等。

图 4 密码安全策略

用户密码策略

- 允许用户修改密码：可禁用该配置项，防止用户修改密码。
- 由系统添加的用户，首次登录时须强制修改密码：开启后，管理员所创建的用户在首次登录时，系统会弹出修改密码提示框强制用户修改密码。
- 距上次修改密码超过 X 天，则用户登录时强制修改密码：默认间隔天数为 30 天。开启时，从上次修改时间算起，每超过 X 天，客户端将提示用户强制修改密码。

- 距上次登录超过 X 天，则自动禁用该用户默认间隔天数为 30 天。开启时，从用户上次登录（用户退出终端时间）超过 X 天，且用户当前处于离线状态，将自动禁用该用户。该策略项为一级策略，仅全局可配置。

图 5 用户策略中对密码的管控

终端登录安全

- 终端设置安全密码

开启并设置了终端管理员密码后，进入终端系统设置（如 IP 地址、接入网关等）需要密码认证。

- 离线终端定时清理

开启“终端清理”并设置时间后，在指定的时长内离线终端未“在线”则被自动

删除。

- 终端自定义登录安全

开启“终端自定义登录安全”后，允许用户在登录终端时记住密码和自动登录。关闭后，终端不支持记住密码和自动登录。

- 锁定登录输入框

开启时，终端登录页账号密码输入框被锁定，无法输入。

若终端已存在记住的账号/密码，那么锁定后信息仍然存在，只是无法修改，用户可直接点击登录按钮登录。

- 密码/验证码输入限制

设置密码/验证码限制规则，可设置连续输入错误次数及终端和用户锁定时长。

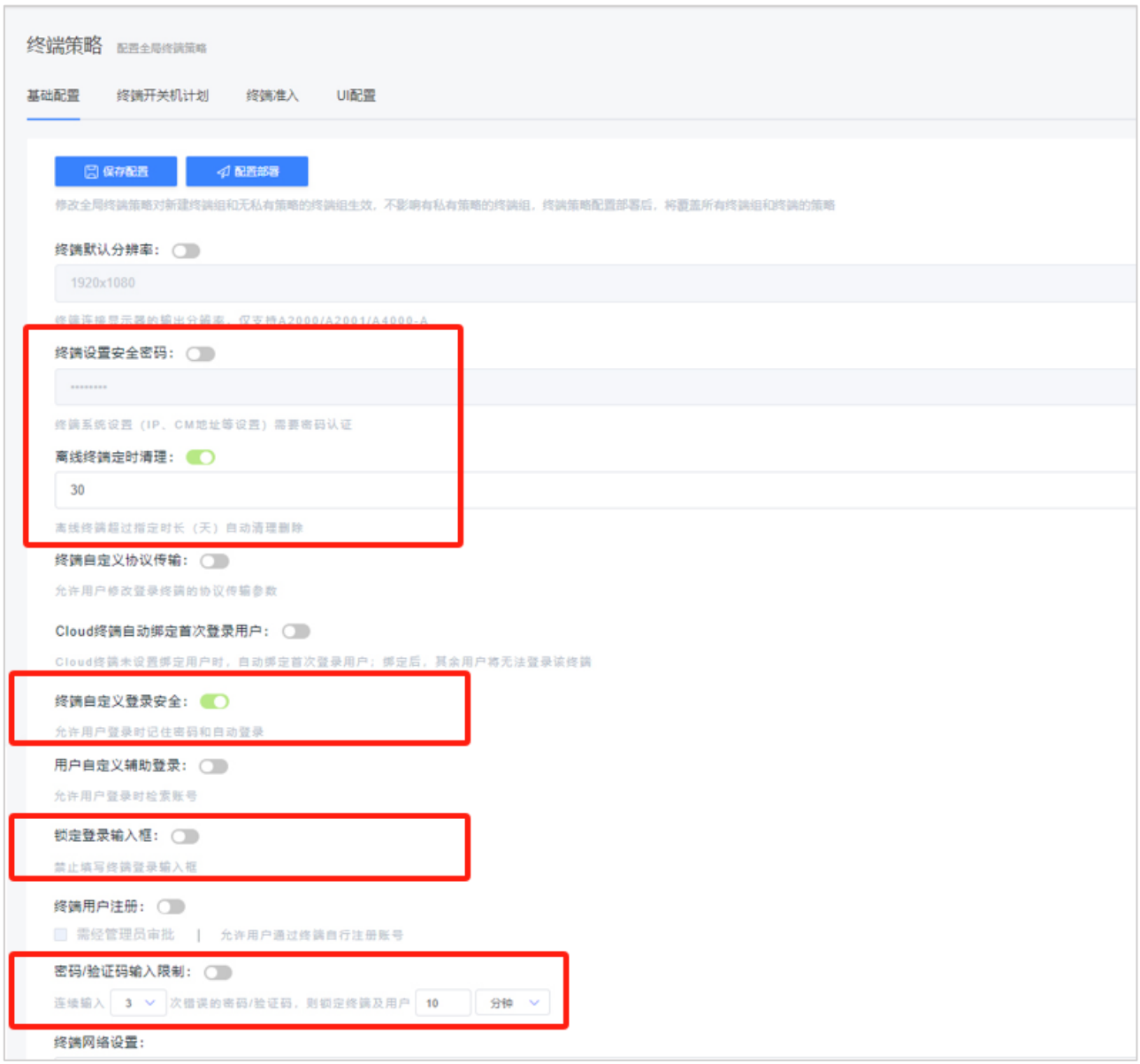


图 6 终端策略中的安全登录配置

用户终端自服务管控

- 终端用户注册

开启时，终端显示“用户注册”按钮，用户可于终端进行自助注册流程，同时设置”需经管理员审批”配置项：勾选时，用户注册完成后，需等待管理员进行审批，待审批通过后，用户列表新增该用户数据，用户方可正常登录。

- 允许用户自行获取桌面

开启时，用户才可自助申请和获取桌面。同时设置“需经管理员审批”复选框。

勾选时，用户不可在终端资源列表页直接获取桌面，需通过管理员审批方可获得。

图 7 用户及终端策略中的自服务管控

3.2.4.6 USB 设备管控

InCloud Access 由后台统一管控 USB 设备的使用，USB 设备的访问权限配置包括：USB 设备配置开关、功能设置、外设黑白名单及设备优化规则：

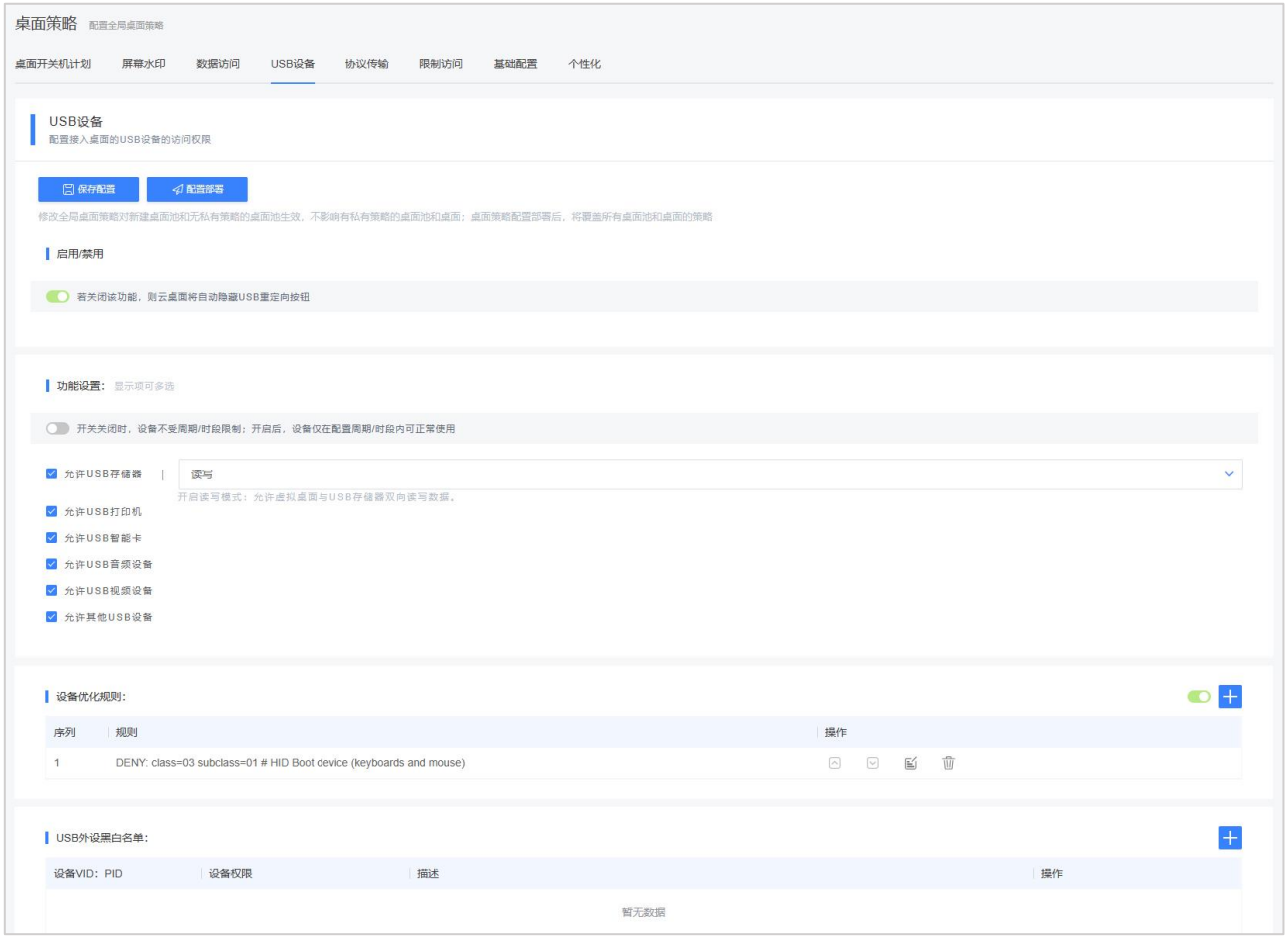


图 8 USB 管控

- USB 设备配置开关

开启时，可配置下方 USB 设备相关设置。此时客户端 USB 重定向功能可正常使用。

关闭时，不可配置下方 USB 设备相关设置。此时云桌面将自动隐藏 USB 重定向按钮，所有 USB 设备都无法重定向到桌面内。

- 功能设置

可配置：生效周期/生效时段、设备权限。

生效周期/生效时段：可配置 USB 设备定时可用。

开关开启时，USB 设备仅在配置周期/时段内可正常使用。开启开关，将自动打开设置弹窗，即可编辑生效周期和时段。

图 9 编辑 USB 设备生效周期/时段

设备权限：功能设置中的设备权限是指对某一类型设备的权限管理。

可设置的设备包括如下类型，可多选：

- USB 存储器（如 U 盘、共享桌面 USB 设备），并可设置读写/只读

  开启只读模式：允许读 USB 存储器数据，不允许向 USB 存储器写数据。

  开启读写模式：允许虚拟桌面与 USB 存储器双向读写数据。

- USB 打印机（如打印机）
- USB 智能卡（如 UKey）
- USB 音频设置（如麦克风、耳机）

- USB 视频设备（如摄像头）
- 其他 USB 设备（如手机、Hub 集线器、串口转 USB）

- 设备优化规则

设备优化规则针对 USB 设备定义了详细的“允许”或者“禁止”细则。系统默认增加了一条规则(DENY: class=03 subclass=01 #HID Boot device(keyboards and mice))。

当用户插入 USB 设备时，主机设备会依次根据每条策略规则对其进行检查，直至找到一个匹配项。任何设备的第一个匹配项都被视为最终选择。如果第一个匹配项是一条“Allow”规则，则该设备会远程连接到云桌面中，如果第一条匹配项是“Deny”规则，则该设备只能连接本地桌面，如果未找到匹配项，则使用默认规则。

提示

通过设备优化细则设置了 USB 设备直通后，如果通过软终端登录云桌面，请在软终端中通过 USB 设备重定向增加该 USB 设备。

设备策略规则的格式为 Allow:或者 Deny:后接一组以空格分隔的 tag=value 表达式，支持以下标记：

- VID - 设备描述符中的供应商 ID，如 0733
- PID - 设备描述符中的产品 ID，如 0430
- REL - 设备描述符中的版本 ID
- Class - 设备描述符或接口描述符中的类
- SubClass - 备描述符或者接口描述符中的子类
- Port - 设备描述符或接口描述符中的协议

创建策略规则时，请注意以下事项：

- 规则不区分大小写
- 规则的末尾可能带有由 # 引入的可选注释
- 空白注释行和纯注释行会被忽略

- 标记必须使用匹配运算符=。例如 VID=1230。

- USB 外设黑白名单

在已经设置的设备访问权限之外如果需要设置排除在设备权限管控之外的设备，则可以添加 USB 设备黑白名单。

图 10 USB 外设黑白名单

在“USB 外设黑白名单”后单击新增设备，设置例外设备的 VID、PID 和描述信息添加设备。并设置该设备的设备权限，也可增加描述信息。

3.2.4.7 实时终端操作日志

实时详细地记录所有终端的操作日志，通过日志管理可审计终端用户的操作，避免安全风险。

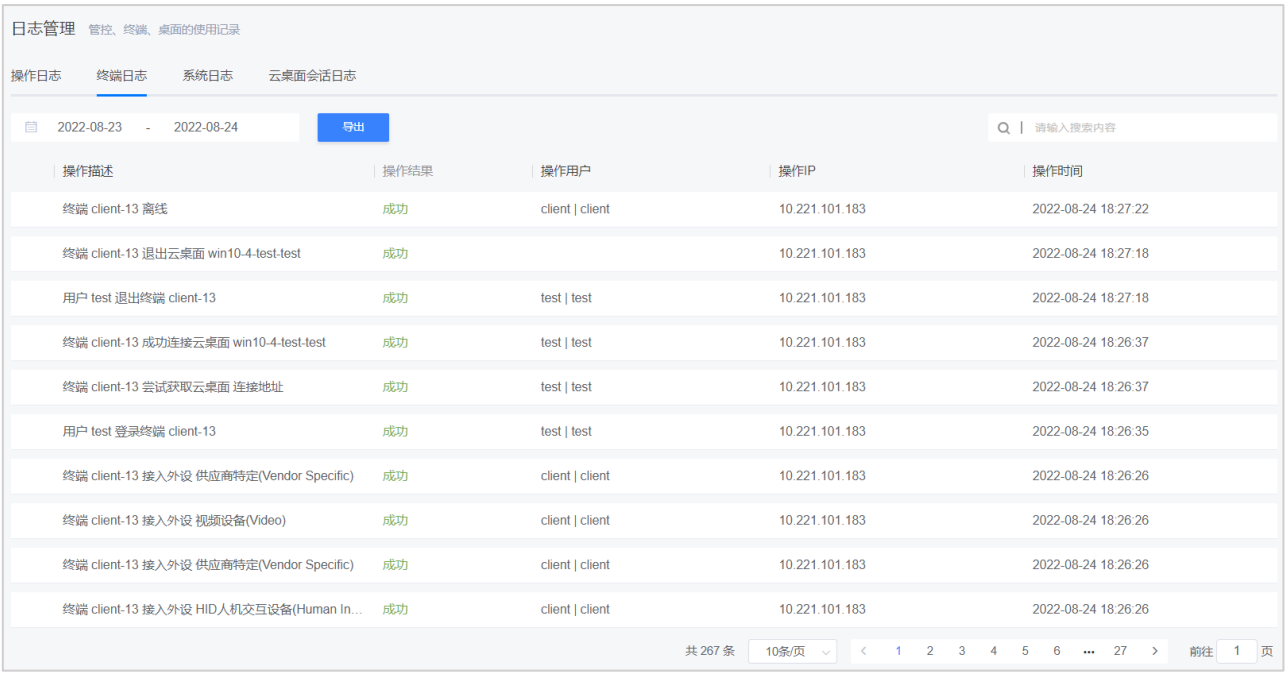


图 11 终端日志

3.2.4.8 NTP 授时服务

对于瘦客户端,其时间存在很多不确定性，比如客户端是否通外网，客户端不定时关机断电等。都会影响客户端时间的正确性。而错误的客户端时间可能造成 SSL 证书的验证问题以及出现问题时排查日志困难（因为时间对不上）。

为了解决以上问题，可以使用 InCloud Access server 作为时间服务器的同步目标，每次开机时都进行时间同步，如此来保证客户端和服务端的时间一致。

InCloud Access 采用 ntpd 服务作为客户端时间同步服务，因为 ntpd 的服务每个客户端都有，不会出现需要改配置安装并带来风险的情况。

1. 在 InCloud Access-server 机器安装 chrony；
2. 客户端安装 ntpd(A3000 等 linux 系统已经具备)；
3. 客户端网关接口通过之后将网关 ip 写入配置；如果网关不通，外网正常则使用外网 NTP 服务器。

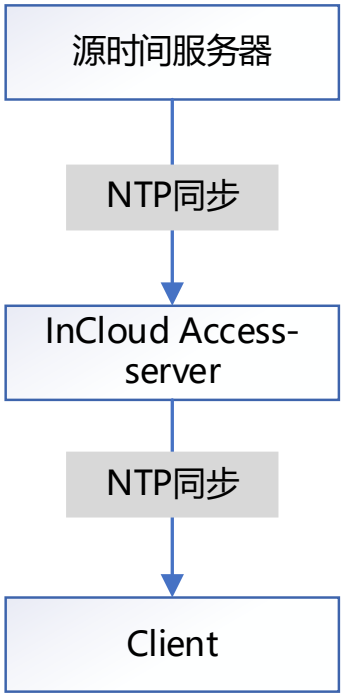


图 12 NTP 时间同步机制

3.2.5 网络安全

3.2.5.1 网络传输安全

为了防止云桌面数据在传输过程中被嗅探、复制、窃取、伪造、截断，InCloud Access 传输安全从以下几个方面保障数据安全的完整性、机密性和有效性。

- 用户接入、管理员接入均采用 HTTPS，传输通道采用 SSL 加密；
- 接入终端与虚拟机之间传输通道使用加密协议（SSL/TLS）对传输的数据进行加密。通过在传输层上应用加密，可以保护数据的机密性，防止在网络传输过程中被窃听或篡改。加密传输可以有效地防止攻击者获取敏感信息，并提供更安全的远程访问体验。
- 密码传输与存储采用 MD5 、RSA 算法加密。

3.2.5.2 网络隔离安全

双网物理隔离

通过为 InCloud Access 云桌面服务器的不同网卡配置连接不同的网络，每张网

卡单独负责局域内网或因特网，再配

存储/业务/管理网络平面隔离

为避免共用网口带来的网络性能问题与网络鲁棒性问题。InCloud Access 云桌面提供存储/业务/管理网络隔离服务，存储数据、业务数据与管理数据通过不同网口传输。不仅避免了不同业务使用同一个网口可能造成的网络拥塞，也摒除了一个网口故障导致业务通信与管理通信皆中断的可能性。

IaaS 层安全组

InCloud Access 云平台为虚拟机提供三层网络安全组控制，三层网络包括：扁平网络、公有网络、VPC 网络。扁平网络可给云主机分配私有网络地址，同时虚拟机可通过分布式弹性 IP 访问公有网络。VPC 网络是一块可由租户自定义的网络空间，其目的是让租户在云平台上构建出一个隔离的、可自行管理配置及策略的虚拟网络环境，从而进一步提升租户在云环境中的资源安全性。VPC 网络和服务由 VPC 路由器提供，一个 VPC 路由器下可提供多个相互隔离的 VPC 网络。安全组实质是一个分布式防火墙，专注东西向流量管控，为虚拟网卡提供防护。按照指定的安全规则对进出网卡的 TCP/UDP/ICMP 等数据包进行有效过滤。

VPC 集成防火墙

云平台支持对 VPC 路由器配置防火墙，主要用于 VPC 网络环境下的南北向流量管控。VPC 防火墙创建后，系统为 VPC 路由器自动配置入方向规则集，用户可灵活配置出方向规则集。VPC 路由器的每个接口方向允许应用一个规则集，通过对 VPC 路由器接口处的南北向流量进行过滤，可有效保护整个 VPC 的通信安全以及 VPC 路由器安全。与作用于云主机虚拟网卡、侧重于保护 VPC 内部东西向通信安全的安全组相辅相成。

3.2.6 虚拟化平台安全

3.2.6.1 云平台服务监控接口

主要通过监控系统以及通知系统提供监控报警功能，监控系统对时序化数据和事件进行监控，通知系统推送报警消息至指定的接收端。

通过监控系统提供包括系统性能、资源用量在内的监控数据指标，以大屏监控/仪表盘/可视化图表/横幅提示等形式，让用户全面了解云平台资源使用情况、系统运

行状态以及健康度。用户还可自定义报警器以及接收端，实现细粒度灵活监控，及时发现并诊断相关问题。

3.2.6.2 运维报警机制

管理节点监控

在多管理节点物理机高可用场景下，可直观查看每个管理节点的健康状态。

监控报警

监控报警支持对时序化数据（如资源负载数据和资源容量数据）以及系统中发生的预定义事件进行监控，并通过通知服务（SNS）推送报警消息至指定的通知对象。

一键巡检

一键巡检支持对关键资源和服务进行全方位一键式健康检查，并根据巡检结果为巡检资源和服务进行健康评分，同时提供巡检建议和巡检报告，助力高效运维，确保云平台资源和服务处于最佳状态。一键巡检适用于需要对云平台进行集中高效运维场景。

一键巡检提供平台、计算、网络、存储、全局设置五大类别巡检项，支持对管理节点、物理机和云主机、镜像服务器和主存储、物理/虚拟网络和网卡、许可证等云平台关键资源和服务进行巡检：

- 平台：检测云平台基础服务和运行状态。
- 计算：检测云平台物理计算资源和虚拟化计算资源使用状况和运行状态。
- 网络：检测云平台物理网络和虚拟化网络配置和状态。
- 存储：检测云平台物理存储资源使用状况和运行状态。
- 全局设置：检测云平台全局性重要资源的配置情况。

3.2.6.3 集群部署高可用

系统将一组服务器主机合并为一个具有共享资源池的集群，并持续对集群内所有的服务器主机与虚拟机运行状况进行检测，一旦某台服务器发生故障，系统会持续进行检测，确定此服务器宕机后，会立即在集群内另一台服务器上重启所有受影响的

虚拟机，保证业务的连续性。系统虚拟机高可用方案不需要专门的备用硬件，也不需要集成其他软件，就可以将停机时间和 IT 服务中断时间降到最低程度。同时避免单一操作系统或特定于应用程序的故障切换解决方案带来的成本和复杂性

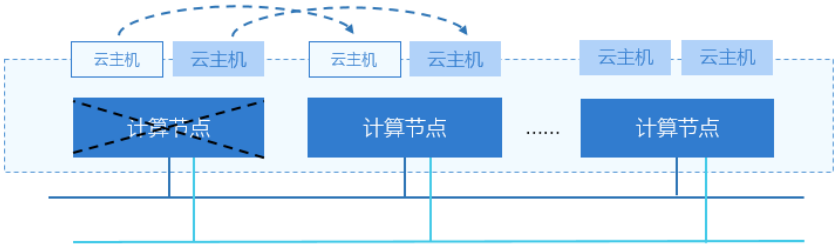


图 14 集群部署

虚拟机高可用设计如下：

1. 添加物理机时，在连接物理机的过程中，管理节点会通过 KVM agent 抓取物理机的所有 IP 地址。

2. 管理节点周期性的发送 ping 命令到物理机的 agent

3. ping 命令发送失败，或物理机未在指定时间内响应 ping 命令，则认定物理机可能宕机，物理机探测器启动。

4. 当发现疑似宕机的物理机时，管理节点查找该物理机所在集群的主存储的存储网络 IP。

5. 管理节点对疑似宕机物理机进行检测

（1）管理节点在指定时间内，使用存储网络 IP 周期性的使用 nmap 扫描物理机端口，如果某次扫描成功，则认为物理机仍然工作，不执行 VM HA 动作。

（2）管理节点通知集群内监控的物理机通过存储网络 IP 使用 nmap 扫描疑似宕机物理机。如果某次扫描成功，则认为该物理机仍然工作，不执行 VM HA 动作。

（3）如果上述检查全部失败，则认为物理机宕机，VM HA 启动。管理节点会选择健康的物理机，启动宕机物理机上所有设置了高可用的 VM。

3.2.7 数据安全

3.2.7.1 数据云端存储不落地

VDI 架构特性是本地不留存用户数据，从根本保障用户核心数据安全。云桌面环境下，终端与数据分离，本地终端只是显示设备，无本地存储，所有的桌面数据都是集中存储在企业数据中心，无需担心企业的智力资产泄露。

3.2.7.2 桌面快照

在虚拟机的运行状态下，不中断用户的业务，实现虚拟机内存和磁盘状态的备份，同时，通过该备份文件，可以方便地恢复虚拟机，保证恢复后的虚拟机状态与快照点完全一致，包括：打开了哪些应用程序、窗口，编写一半的文档等，都能如实还原。主要用户场景为：创建快照和还原快照。用户通过创建快照可以实时保存虚拟机的状态，包括虚拟机的内存、磁盘等数据信息。创建快照后，会生成一个内存快照文件和存储快照卷。当虚拟机发生故障，或者用户想恢复到之前做快照时刻的虚拟机状态，可以选择相应的内存快照文件和存储快照卷来进行快照还原。快照还原后，虚拟机恢复到快照时间点的状态。

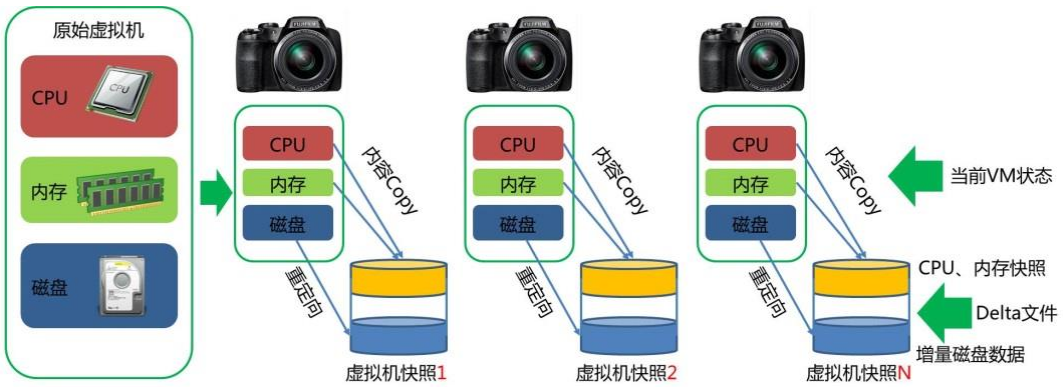


图 15 InCloud Access 桌面快照示意图

3.2.7.3 数据多副本

在有分布式存储或超融合存储情况下，可以通过数据副本技术保证数据安全：底层管理的副本对云桌面服务是透明的，上层无法感知副本的存在。磁盘管理、副本分布由存储虚拟化服务负责；在没有故障等异常情况下，文件副本数据是始终一致的，不存在所谓主副本和备副本之分；如果云桌面对数据 A 进行修改，如写入一段数据，这段数据会被同时写到副本。如果是从数据 A 读取一段数据，则只会从其中一个副

本读取；支持主动式/触发式副本修复，在副本修复期间云桌面服务不受影响。

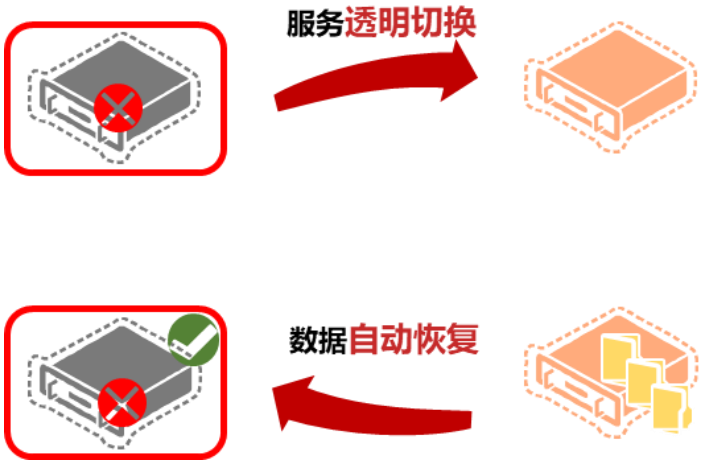


图 16 InCloud Access 数据副本示意图

3.2.7.4 屏幕水印

在 helper 中实现屏幕水印，包括如下功能：

1. 可以根据 InCloud Access 中屏幕水印的配置，更新显示的屏幕水印样式、内容。
2. 水印悬浮在桌面顶层，屏幕截图时，水印会出现在截图中。
3. 系统启动后，自动按照配置信息，显示、隐藏水印。

实现方案

每次虚拟机在开机时，InCloud Access 给 helper 发送 HTTP 请求，helper 在接收请求后根据 header 中的信息获取 IP 及水印设置参数，加密存储在本地。

helper 后台进程固定频率读取水印配置，根据配置显示、隐藏水印。

1. 修改 Helper 与 InCloud Access 握手接口：接口`http://${虚拟机 ip}:10090/agent/update`修改为 http://${虚拟机 ip}:10090/agent/init。
2. 新的接口添加水印启停、设置参数。
3. 每次接受到参数后，将参数与 helper 本地 config 文件中的参数对比，有变化则更新 helper 本地 config。

4. 本地存储的参数信息采用 AES 加密后存储，防止用户手动修改水印信息。

5. helper 后台线程，1 分钟读取一次水印配置，根据配置检测水印状态，开启、关闭水印，防止用户手动关闭水印进程。

如果配置为【开启水印】，而未检测到水印的进程，说明水印未开启，则开启水印；

如果配置为【关闭水印】，而检测到水印进程存在，说明水印已开启，则关闭水印。

配置方法

水印就是在载体信息内容上加上的标识,水印分为内部水印和外部水印。

内部水印可用于截屏，推荐使用 Windows 10 系统（也可支持 Linux 桌面，如 uos 20 及麒麟 v10），外部水印可用于拍照，推荐使用 Windows 7 系统。

管理平台预置了五种水印样式效，可以直接选择并使用，也可自定义水印效果。选择自定义的水印效果后，可设置水印内容或者自定义水印内容，并可设置水印效果。

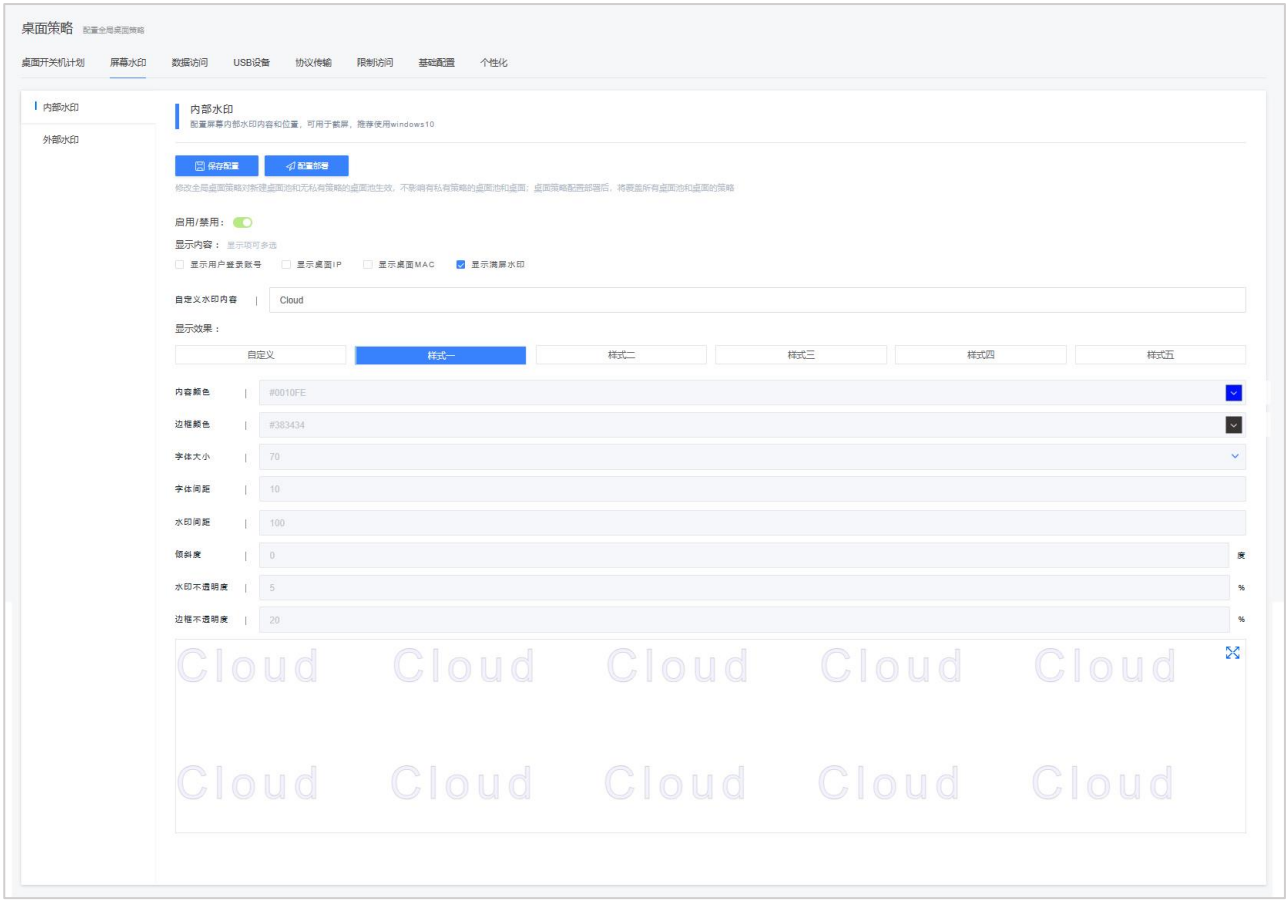


图 17 屏幕水印

3.2.7.5 双向拷贝限制

InCloud Access 支持配置通过 WinClient 或者 MacClient 软终端登录桌面后，桌面数据与本地数据的访问权限。包括：可设置 PC 剪切板权限、PC 文件拖拽权限和 PC 内置磁盘权限。

- 允许 PC 文件拖拽

开关默认开启。开关开启时，允许本地磁盘文件通过拖拽方式拷贝至云桌面。

- 允许 PC 剪切板

图 18 允许 PC 剪切板配置

开关开启时，开启本地至云桌面的复制权限。

可选择如下三种复制权限：

1. 双向：允许桌面数据与本地磁盘数据双向拷贝，包括云桌面到本地磁盘数据以及本地磁盘数据到云桌面的拷贝和剪切。
2. 桌面至本地：仅允许桌面数据拷贝至本地。
3. 本地至桌面：仅允许本地数据拷贝至桌面。

- 重定向磁盘访问

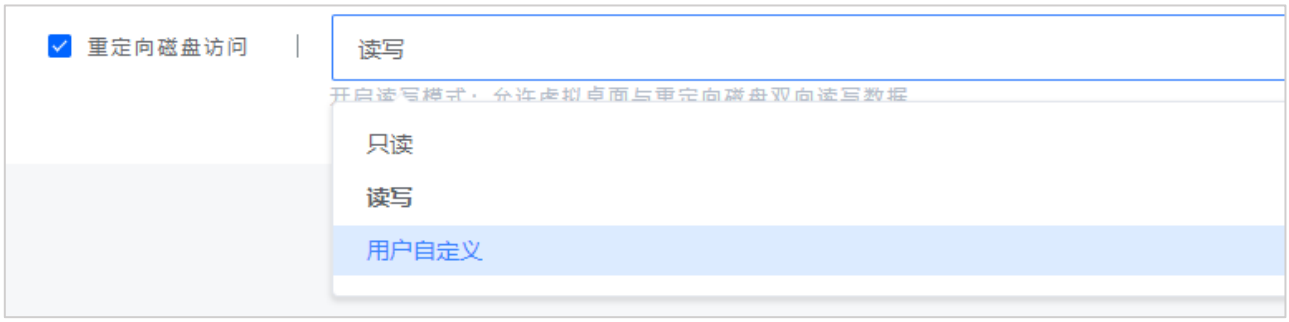


图 19 重定向磁盘访问配置

开关开启时，可开启读写模式：允许虚拟桌面与重定向磁盘之间读写数据，且终端云桌面内显示“磁盘重定向“功能按钮。

可选择如下三种读写权限。

4. 只读：云桌面仅可对重定向磁盘进行数据读取，不可对重定向磁盘中的数据新增、编辑保存、删除、粘贴（不可将桌面内数据复制粘贴进入重定向磁盘，但是重定向磁盘中数据可以复制粘贴到桌面）。

5. 读写：用户可读取重定向磁盘/目录中的数据，也可对该部分数据进行增、删、改（增、删、改时会导致本地磁盘内的数据同步发生变更）。

6. 用户自定义：终端云桌面重定向配置窗口中用户可行修改其读写权限。

3.2.8 运维安全

3.2.8.1 权限分级管理

通过对管理员区分权限和区域，限制管理员对系统的访问范围，保证系统的安全。

服务端支持管理角色分权，系统更安全，工作更高效。InCloud Access 管理平台采用【超级管理台 admin 与三员管理】并存的方案。

系统提供三种管理角色：系统管理员、子管理员和租户。系统管理员负责服务器及系统日常维护与管理，拥有最高级资产统计分析权限。子管理员由系统管理员创建，拥有租户分配与管理权限，拥有管辖范围内所有租户的资产统计分析权限。租户可自行按需注册，也可由管理员手动创建，其可归属系统管理员直接管辖，也可由子管理员管理。租户可随时随地访问服务端管理国产终端，租户间共享服务资源，数据完全隔离。

图 20 管理员管理

平台预置【系统管理员】【保密管理员】【安全审计员】账号，以实现三员分立管理。

表 1 预置管理员权限说明

预置管理员名称	描述
系统管理员	可向下创建子管理员和区域，子管理员无法向下创建。
	子管理员所产生的日志可由【上级系统管理员】和【安全审计员】查看。
	仅可查看角色，但是无法新建、编辑、删除。
	创建管理员时，无法选择【系统管理员】【保密管理员】【安全审计员】这三个角色
	可查看自身和下级所生成的日志。
安全保密管理员	可创建角色，角色中无法勾选日志、管理员、角色、区域的功能权限。
	仅可查看【安全审计员】和【普通用户】所生成的日志。
安全审计员	仅可查看【系统管理员】和【保密管理员】所生成的日志。
	无区域限制，无需切换区域即可查看所有管理员和用户的日志。

管理员的权限通过所属角色来控制。通过为不同的管理员分配不同的权限，保证系统安全性并提升运维效率。

平台除 admin 外，还预置了六个角色：三个三员角色——系统管理员、保密管理员、安全审计员，及三个非三员角色——高级管理员、一级管理员、普通管理员。

表 2 预置角色权限说明

角色名称		描述
超级管理员		能够对系统内所有业务进行管理的管理员。
三员角色	系统管理员	能够对普通用户、系统配置进行日常运维的管理员。

	安全保密管理员	能够对角色、日志进行查看维护的管理员。
	安全审计员	能够对系统管理员和安全保密管理员的操作日志进行查看并导出的管理员。
非三员角色	高级管理员	能够对系统内主要业务进行管理的管理员。
	普通管理员	能够对云桌面和用户进行管理，分配和维护的管理员。
	一线管理员	能够对普通用户使用的云桌面进行简单维护的管理员。

admin 不可在页面修改、删除三员角色，但可通过配置文件修改三员管理员所查看的日志类型，修改后需重启服务)；admin 可在页面修改、删除非三员角色。

三个非三员角色无日志及管理员、角色、区域权限，其产生的日志可由预置【系统管理员】和【安全审计员】查看。

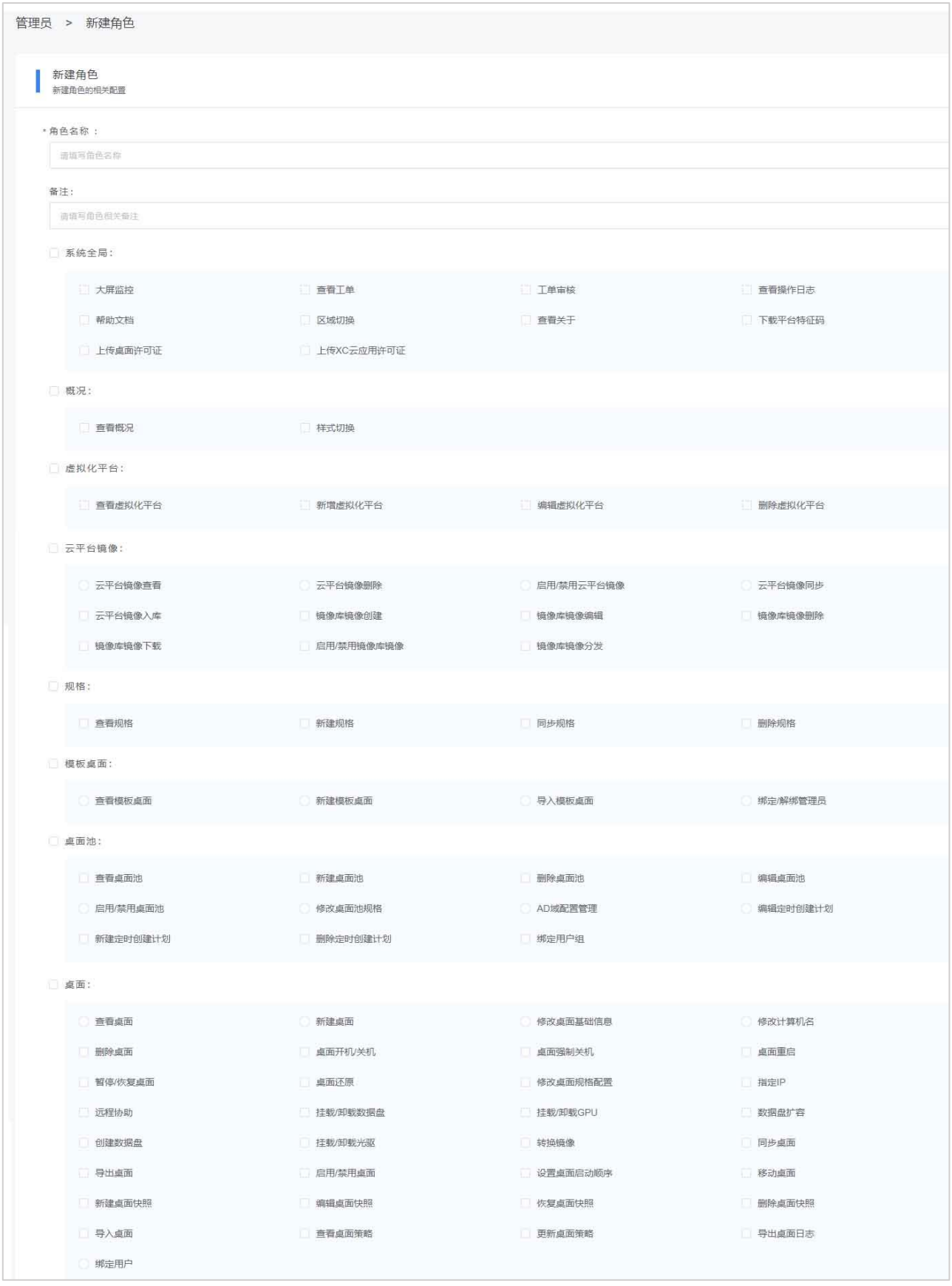

管理员 > 新建角色
新建角色
新建角色的相关配置
* 角色名称：
请填写角色名称
备注：
请填写角色相关备注
系统全局：
大屏监控
查看工单
工单审核
查看操作日志
帮助文档
区域切换
查看关于
下载平台特征码
上传桌面许可证
上传XC云应用许可证
概况：
查看概况
样式切换
虚拟化平台：
查看虚拟化平台
新增虚拟化平台
编辑虚拟化平台
删除虚拟化平台
云平台镜像：
云平台镜像查看
云平台镜像删除
启用/禁用云平台镜像
云平台镜像同步
云平台镜像入库
镜像库镜像创建
镜像库镜像编辑
镜像库镜像删除
镜像库镜像下载
启用/禁用镜像库镜像
镜像库镜像分发
规格：
查看规格
新建规格
同步规格
删除规格
模板桌面：
查看模板桌面
新建模板桌面
导入模板桌面
绑定/解绑管理员
桌面池：
查看桌面池
新建桌面池
删除桌面池
编辑桌面池
启用/禁用桌面池
修改桌面池规格
AD域配置管理
编辑定时创建计划
新建定时创建计划
删除定时创建计划
绑定用户组
桌面：
查看桌面
新建桌面
修改桌面基础信息
修改计算机名
删除桌面
桌面开机/关机
桌面强制关机
桌面重启
暂停/恢复桌面
桌面还原
修改桌面规格配置
指定IP
远程协助
挂载/卸载数据盘
挂载/卸载GPU
数据盘扩容
创建数据盘
挂载/卸载光驱
转换镜像
同步桌面
导出桌面
启用/禁用桌面
设置桌面启动顺序
移动桌面
新建桌面快照
编辑桌面快照
恢复桌面快照
删除桌面快照
导入桌面
查看桌面策略
更新桌面策略
导出桌面日志
绑定用户

图 21 角色配置

3.2.8.2 多区域架构

服务端支持部署在公有云服务器上，区域是一组虚拟化平台、云桌面、用户等资源的组合，是组合内资源管理的边界。每个区域都有对应的区域管理员，系统管理员默认为所有区域的区域管理员，可自定义区域的其他区域管理员。

有远程统一管控云终端的单位可以通过多租户申请注册的方式，在公有云平台上申请租户管理资源，远程管理终端。每个租户申请通过授权后，随时随地通过浏览器访问公有云服务端，输入租户账号密码登录，即可管理相关资源。所有租户共用相同的系统组件，使用相同的管理功能，但各租户间数据完全隔离，每个租户都是完全独立管理各自其下的区域。

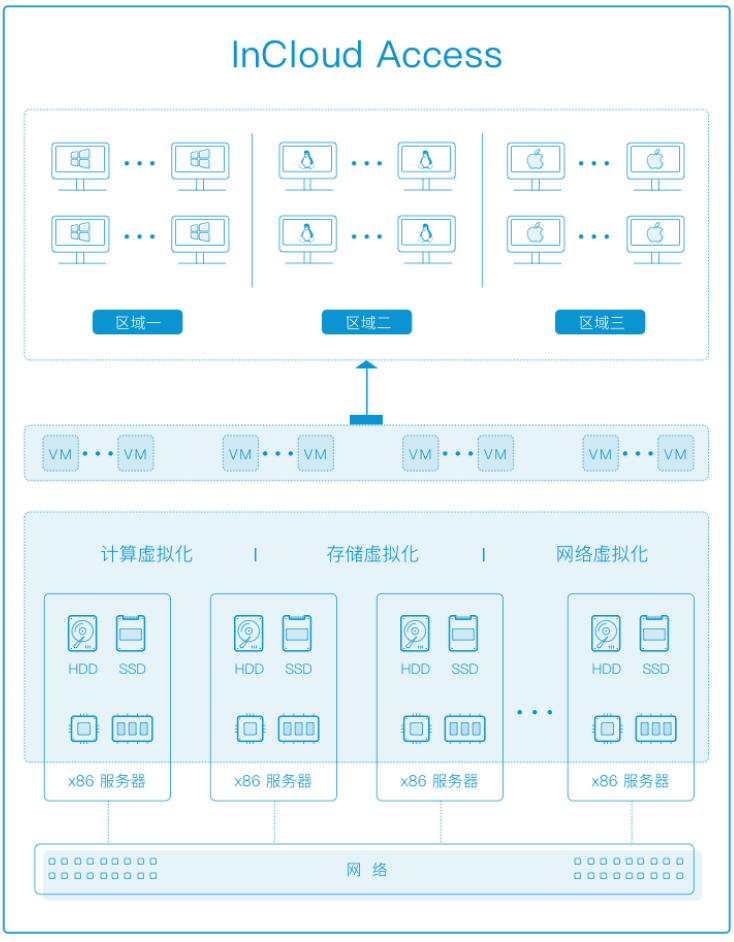


图 22 多区域架构

如果管理员同时管理多个区域，可切换不同的域进行资源管理。

单击右上角用户名前面的“全部区域”，可展示当前管理员的区域范围，选中需要管理的区域即可。

图 23 管理员切换区域

3.2.8.3 运维日志管理

日志分类

日志审计是支撑管理模块的核心功能，是信息安全管理的重要组成部分，它可以帮助企业识别和分析系统中发生的事件，以及识别和解决可能存在的安全漏洞。此外，日志审计还可以帮助企业发现潜在的安全威胁，从而防止安全事件的发生。因此，日志审计是企业信息安全管理的重要组成部分，因此加强日志审计功能的实施至关重要。管理员可查询管控、终端、桌面的使用记录，并可根据查询条件过滤日志。通过日志管理可审计管理员及终端用户的操作，避免安全风险。

- 操作日志记录了管理员在 InCloud Access 管理平台中的相关操作。
- 终端日志记录了终端用户的相关操作。
- 系统日志记录了系统服务组件的日志信息。
- 云桌面会话日志记录了终端用户登录云桌面的会话历史信息。

图 24 系统日志

日志导出

当系统中日志记录较多，在界面上不便于查看时可将日志导出为文件进行查看，也可将日志过滤后导出为文件进行备份以便审计。

3.2.8.4 用户自助运维

InCloud Access 云终端提供用户自助服务，在无需管理员帮助下，也可自助维护办公电脑。传统 PC 需要 IT 管理员到工位进行维护，耗时耗力。产品为用户提供了简易自助维护功能，如：创建快照（创建桌面 C 盘文件副本）、快照还原（病毒感染、蓝屏等情况下，可基于 C 盘快照副本，一键恢复数据）、切换办公模式（还原模式：终端关机自动清除数据，用于无需保存个人数据的特殊场景；不还原模式：保存用户自定义数据）等。用户自助服务确保在不影响用户原有办公习惯基础上，提高办公效率，有效减少业务中断时间。

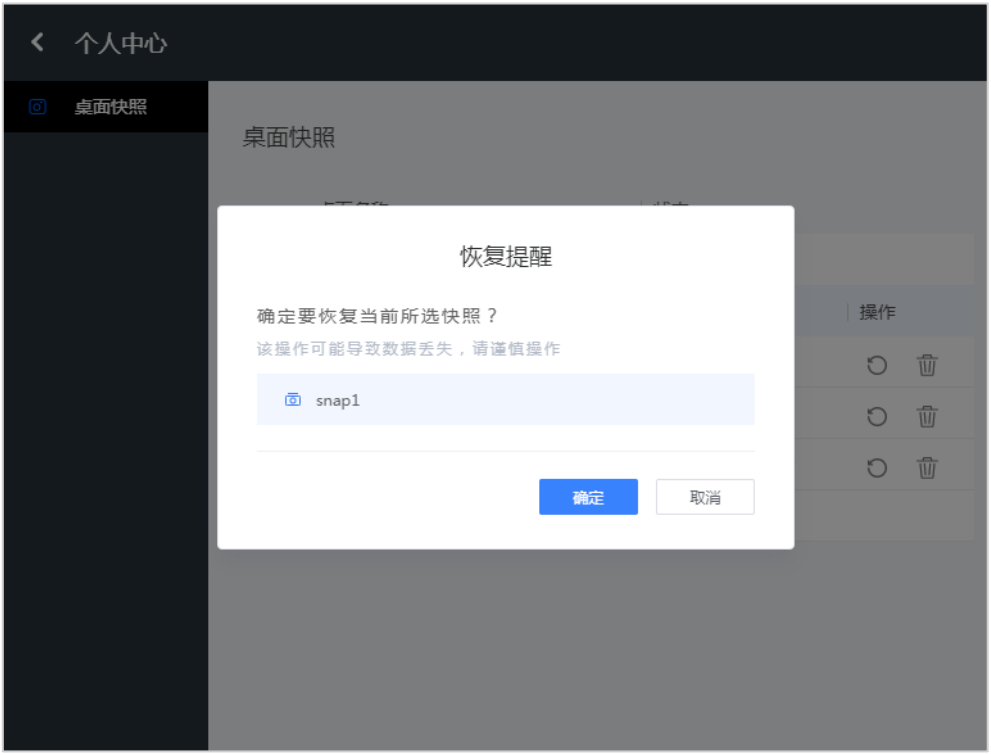


图 25 恢复快照

3.2.8.5 远程协助

InCloud Access 远程协助基于底层虚拟化云平台功能实现，无需在云桌面内安装 TeamView、向日葵等基于外网服务器和防火墙穿透技术的第三方远程协助工具软

件，消除了第三方工具漏洞的安全隐患和内外网络物理隔离环境下的远程协助难题。

图 26 InCloud Access 远程协助

3.2.8.6 系统访问许可

系统可配置特定的 IP 地址设备登录 InCloud Access 管理平台。配置后，若某管理员的 IP 不在该访问范围内，则将自动掉线，且该 IP 地址无法再访问此链接。

图 27 访问许可

3.3 可靠性

3.3.1 平台高可用

3.3.1.1 计算高可用

系统将一组硬件服务器虚拟化为一个逻辑资源池，并以集群进行划分管理。云平台持续对集群内所有物理主机与云主机运行状况进行检测。一旦某台物理机发生故障，云平台管理节点会持续进行检测，确定此物理机宕机后，会立即在集群内另一台物理机上重启所有受影响的云主机，保障业务连续性。云平台计算高可用无需专门的备用硬件或集成其它软件，就可将停机时间和 IT 服务中断时间降至最低程度，并且避免了因特定操作系统或特定应用程序做故障切换带来的成本和复杂性。

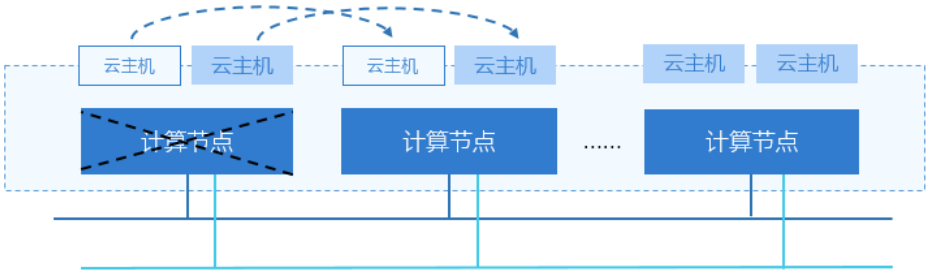


图 1 集群计算高可用

3.3.1.2 存储高可用

分布式存储

这里主要介绍自研分布式存储的高可用性。

存储虚拟化是通过软件定义的方式，基于 X86 服务器平台提供文件、块、对象三种服务类型的存储。解决了传统存储容量和性能难以扩展、硬件绑定、设备单点故障、信息孤岛、接口单一、管理复杂等一系列问题。其主要特点：

- 分布式存储，随需而用

存储虚拟化将 HDD、SSD 等硬件存储介质通过分布式技术组织成各类型大规模存储资源池，为上层应用和客户端提供业界标准协议接口，消除传统数据中心多类型存储系统烟囱式构建形成资源孤岛、硬件资源利用不均问题。

- 统一存储服务

提供 POSIX、NFS、CIFS、FTP、iSCSI、S3 等标准协议接口，以卓越性能、大规模横向扩展能力为用户提供结构化数据、半结构化数据和非结构化数据统一存储资源，广泛应用于媒资生产、云计算、视频监控等多业务场景。

- 弹性高效

存储虚拟化采用全分布式全对等架构，支持通过横向扩展硬件节点线性增加整系统容量与性能，资源供给可预期，无需复杂的资源需求规划。系统可轻松扩展至数千节点及 EB 级容量，满足您的云业务规模扩张。提供自动负载均衡策略，数据与元数据均匀分布于各节点，消除元数据访问瓶颈，保障规模扩展场景下的系统性能。

- 丰富特性

存储虚拟化分别提供满足应用场景需求的丰富企业级特性。远程复制、EC、副本等数据保护机制保障数据安全。精简配置、分层存储等更合理的利用存储资源。多租户功建立存储资源的灵活、有效分配策略。

- 多副本

存储虚拟化提供副本机制，相当于 RAID1，同一数据存储于多个存储节点上，主要用于实现高可用及数据的自我修复。写数据时，首先对数据加锁，然后对多个存储节点同时写，最后解锁。写过程中，单节点故障导致副本数据不一致，可自动修复。读数据时，可根据读策略选择从哪个存储节点读数据，一般选择优先读本地，可提高读性能。AFR 副本数越多，数据的可靠性越高。

双副本卷的数据至少会在不同的 pack 上被存储两份，具体采取存储几份的冗余数据则可以在创建副本卷时予以设定。副本卷可以有效得预防存储块损坏可能引发

的数据丢失的风险。

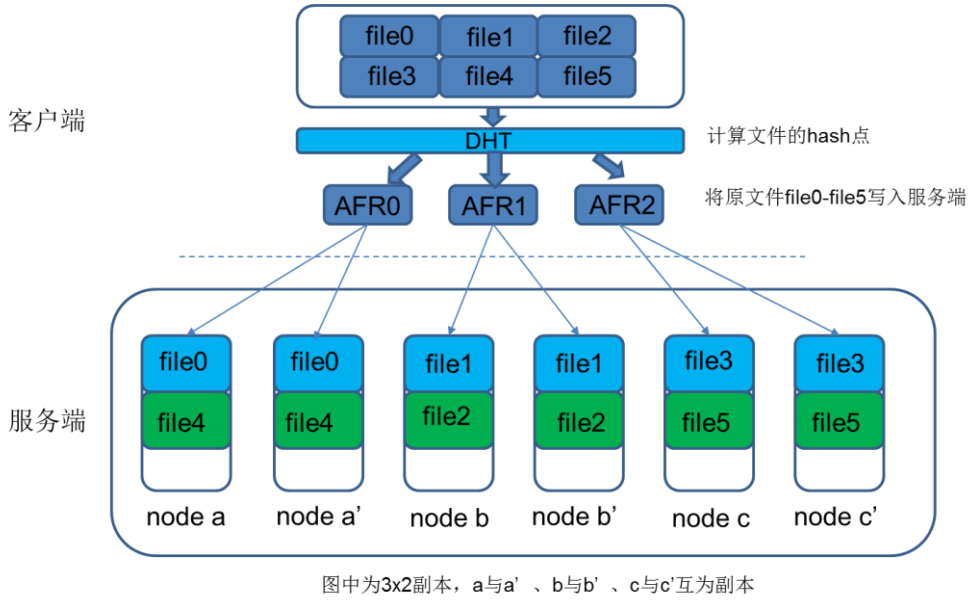


图 2 存储多副本

上图为 3*2 副本，客户端的 file0~file5 经过 DHT 层后，决定文件的 hash 点，即数据即将落在哪个存储节点上。经过 AFR 层后，在 client 端将文件分别写入互为副本的 2 个服务端的存储节点上。

SSD 缓存加速

在每台虚拟桌面服务器上都采用 SSD+HDD 的部署方式，通过热点数据精准抓取技术和冗余数据快速淘汰技术，可以让用户以较低的成本获得非常高的 IO 性能。

缓存算法优化，虚拟桌面所请求的数据、绝大部分情况下都会直接读取到 SSD 硬盘，缓存命中率高达 60%以上，从而使得存储的响应速度大幅提升，明显提升整体存储的 IOPS 性能，从而使得多并发使用时操作体验更好，也有效解决了开机风暴的问题。

相比直接分配物理存储资源，可以显著提高存储空间利用率，明显降低存储成本。

3.3.1.3 网络高可用

虚拟网络高可用

扁平网络通过网桥连接到服务器 Bond 口，高可用依赖于服务器网卡。

VPC 网络采用定制的路由器镜像创建一台云主机作为 VPC 路由器，三层流量均经过 VPC 路由器进行转发。一旦 VPC 路由器所在物理机宕机，数分钟之后会在其他正常节点重新启动，保证业务连续性。不同租户使用不同的 VPC 路由器，即使有物理机宕机，也仅影响其上运行 VPC 路由器的租户数分钟，对其他租户无任何影响，缩小故障影响范围。

VPC 路由器双机主备

VPC 路由器支持双机主备模式，可在创建 VPC 路由器时按需选择。主备路由器会不断进行心跳检测，若主路由器发生故障，备路由器将提升为主路由器，所有流量秒级进行切换，最大程度保障业务连续性。

3.3.1.4 业务高可用

调度策略

云主机调度策略可为云主机分配物理机资源编排策略，用于保障业务高性能和高可用。

双机热备

对于需要实时在线的业务系统，支持通过镜像/快照等技术，部署主备业务系统，在主业务系统故障时，实现秒级故障切换。

3.3.1.5 系统配置备份与恢复

在系统维护过程中，适当合理的备份与恢复操作可保证数据可靠性和业务连续性。

备份原则

系统维护工程师或技术支持工程师在对系统进行重大操作（如升级、重大数据调整等）前，为了保证 InCloud Access 中各部件在出现异常或未达到预期结果时可以及时进行数据恢复，将对业务的影响降到最低，需对数据进行备份。

针对数据的备份通过系统提供的自动备份功能来实现，当系统部件故障无法通过常规方法修复时，利用备份数据快速恢复系统部件和业务。

InCloud Access 管理平台支持对用户的桌面数据及配置信息进行备份，以便在系统故障时恢复至之前的状态。

系统备份

可对如下信息进行备份：

1. 桌面池、桌面相关信息
2. 本地用户、AD/LDAP 用户
3. 终端组、终端
4. 桌面池与用户组的关联关系
5. 桌面与用户的关联关系
6. 系统配置的相关信息

系统提供三种备份方式：备份当前配置至本地、自动备份计划及异地备份。

- 备份当前配置：单击“下载当前配置”，可将当前系统配置信息下载至本地。

- 自动备份计划：为提高系统安全性，可开启自动备份计划功能，设置自动备份的周期、时间点及本地备份路径后，系统会在设置的周期和时间点自动备份系统配置至指定路径，保留四个最近的历史记录，并在历史备份中展示。

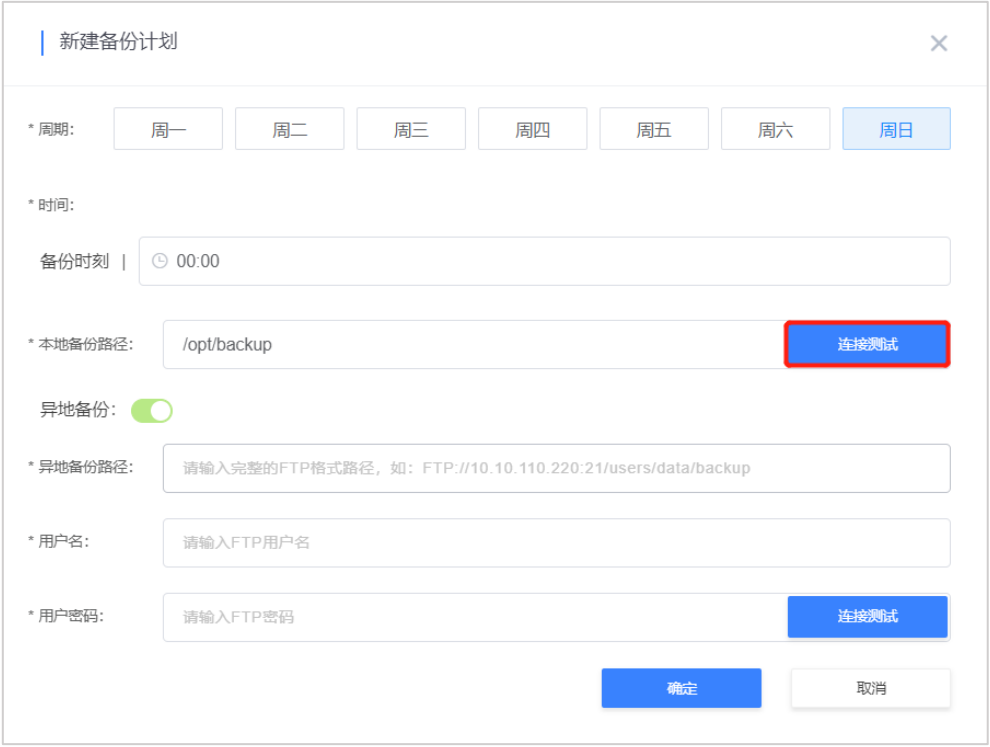


图 3 新建自动备份计划

- 异地备份：开启异地备份后，设置备份路径、用户名和用户密码即可将备份数据放置异地服务器，支持 ftp 方式。

系统还原

对系统进行备份后，可将已备份的文件进行还原。

可选择以下两种方式进行系统还原：（1）选择本地备份文件；（2）选择历史备份记录。

3.3.2 虚拟机高可用

虚拟机高可用设计如下：

1. 添加物理机时，在连接物理机的过程中，管理节点会通过 KVM agent 抓取物理机的所有 IP 地址。
2. 管理节点周期性的发送 ping 命令到物理机的 agent
3. ping 命令发送失败，或物理机未在指定时间内响应 ping 命令，则认定物理机可能宕机，物理机探测器启动。

4. 当发现疑似宕机的物理机时，管理节点查找该物理机所在集群的主存储的存储网络 IP。

5. 管理节点对疑似宕机物理机进行检测

（1）管理节点在指定时间内，使用存储网络 IP 周期性的使用 nmap 扫描物理机端口，如果某次扫描成功，则认为物理机仍然工作，不执行 VM HA 动作。

（2）管理节点通知集群内监控的物理机通过存储网络 IP 使用 nmap 扫描疑似宕机物理机。如果某次扫描成功，则认为该物理机仍然工作，不执行 VM HA 动作。

（3）如果上述检查全部失败，则认为物理机宕机，VM HA 启动。管理节点会选择健康的物理机，启动宕机物理机上所有设置了高可用的 VM。

3.3.3 服务器硬件可靠性

3.3.3.1 内存可靠性

内存错误主要包括硬件错误和软件错误，其中硬件错误是由硬件失效或是损坏造成的，器件会不断返回不正确的数据，硬件错误可以通过服务器启动时 BIOS 的内存自检发现。

内存使用中经常碰到的为软件错误，软件错误不能通过内存自检发现，只有通过一些 内存检错和纠错的算法来保护内存中的数据。服务器在内存软件错误纠正上采用内存 ECC（Error Checking and Correction）技术，采用工业标准的纠错算法，能够检测内存 2bit 错误，并修复内存单 bit 错误。

3.3.3.2 硬盘可靠性

硬件热插拔：服务器支持系统运行时的硬盘（SATA/SAS）热插拔。

硬盘 RAID：服务器支持 RAID0、1、5 等多种 RAID 方式，支持 RAID 下另加热备盘的配 置，保证了硬盘数据的高可靠性，在 RAID 组的某颗硬盘坏掉后，支持数据恢复、RAID 组恢复和在线更换硬盘。其中 RAID 卡支持电池，可以对 Cache 数据进行保护，既可以

提高对硬盘的访问性能，又可以防止意外掉点时数据的丢失。

3.3.3.3 CPU 可靠性

表 1 CPU 可靠性功能表

组件	模块名称	功能说明
CPU 核隔离技术	以再某些 CPU Core 故障情况 下关闭这些 Core 运行业务	可以在牺牲一定性能的基础上保证业务的可用性等备件充足，业务空闲时，再进行系统维护恢复系统的处理能力。
Socket 隔离	可以在从 CPU 故障情况下只启动主 CPU 运行业务	可以在牺牲一定性能的基础上保证业务的可用性等备件充足，业务空闲是在进行系统维护 恢复系统的处理能力。 带外系统通过 PECI 访问 MAC 寄存器
PECI 带外访问 MCA	提供一个与主系统解耦的 PECI 通道，用于带外访问 COU 的 MAC 寄存器。	PCH 内部出错，不能通过 ME 的 PECI 通道访问 CPU 的情况下，可以使用带外系统的 PECI 通道对 CPU 的 MAC 寄存器进行访问，最大程度上抓取故障信息用于故障定位。
IVR(core/soket 电压检测)	提供 CPU 内部集成的 IVR 模块的检测及告警。	CPU 内部模块的故障监控告警充分覆盖，可能影响系统稳定运行的风险因素可以提前识别，根据需要进行相应处理。

3.3.3.4 电源可靠性

服务器配置多组冗余电源（PSU），提供电源故障告警，支持电源冗余和热插拔，可以在一组电源故障后，系统持续运行而不影响业务；并且可以在线更换故障电源。

3.3.3.5 网卡可靠性

服务器绑定多网卡的实际意义在于当系统绑定多网卡(采用网口绑定方式)之后，不仅可以扩大服务器网络进出口宽度，而且可以实现有效负载均衡和提高容错能力，避免服务器出现传输瓶颈或是因某块网卡故障而停止服务。

聚合网口工作方式有两种方式：

1. 静态聚合静态聚合支持
2. 使用主备模式工作、使用 MAC 地址进行负载、根据 IP 地址进行负载、根据网口轮询进行负载、根据四层信息进行负载。
3. LACP 模式支持
4. 使用 MAC 地址进行负载、根据 IP 地址进行负载、根据四层信息进行负载。
5. 同时交换机上建议需要配置一样的负载均衡模式。

3.3.4 HA 部署方案

支持以虚拟机部署时进行主备切换，提高可用性。

Keepalived

keepalived 是集群管理中保证集群高可用（HA）的一个服务软件，其功能类似于 heartbeat，用于防止单点故障。

keepalived 的两大核心功能是失败切换（高可用）和健康检查。所谓的健康检查，就是采用 tcp 三次握手，icmp 请求，http 请求，udp echo 请求等方式对负载均衡器后面的实际的服务器(通常是承载真实业务的服务器)进行保活；而失败切换主要是应用于配置了主备模式的负载均衡器，利用 VRRP 维持主备负载均衡器的心跳，当主负载均衡器出现问题时，由备负载均衡器承载对应的业务，从而在最大限度上减少流量损失，并提供服务的稳定性。

部署方案

1. 将 keepalived 部署在 InCloud Access server 上，keepalived 的 VIP 机制只有 1 个 InCloud Access server 提供服务，InCloud Access server 处于主备状态

2. InCloud Access 的登录等操作会记录操作日志，对 MySQL 有写的操作

3. MySQL 的 HA 方案支持主备、主主的方式。

   - 在主备的情况下，仅对主节点进行写操作，备节点是 read-only 状态，由于 InCloud Access 的登录等会写操作日志，因此如果主节点宕机，只读的备节点是无法提供访问的

   - MySQL 主主 HA，两台 MySQL 都可以写。一个 MySQL 宕机后，另外一个仍可提供服务。由于 MySQL 内置于 InCloud Access server 虚拟机中，keepalived 的 VIP 仅落在一台服务器上，因此两台主主的 MySQL 只有一台提供服务，类似主备模式。

4. MySQL 部署成 HA 模式后，InCloud Access server 可以两种方式访问 MySQL：

   - 访问本机 MySQL：主 InCloud Access server 虚拟机宕机后，VIP 飘到另外的服务器上，不会影响服务；

   - 通过集群方式访问 MySQL：通过 VIP 访问，仅有一个 MySQL 提供服务。

部署示意图

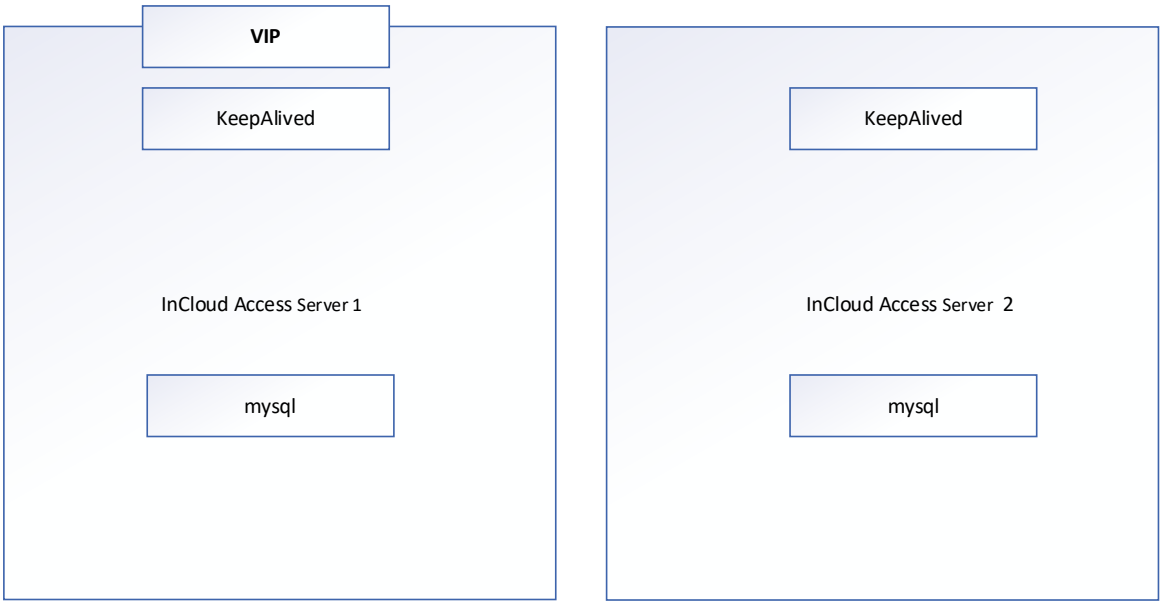


图 4 部署示意图

两台 InCloud Access server 上部署 keepalived，VIP 位于 InCloud Access

Server1 上

两个 MySQL 构建成双主的 HA，用于 VIP 的 InCloud Access 只会访问本机的 MySQL，因此 InCloud Access、MySQL 都处于主备的状态。

3.4 兼容性

3.4.1 解耦合架构

InCloud Access 云桌面管理平台采用解耦合的轻量化架构设计，专注于云桌面的深耕与优化，与云平台强强联合，为用户带来更专业的使用体验。支持与第三方基于 QEMU-KVM 的虚拟化平台进行对接，减少客户 IT 基础架构的复杂度。

在用户建设企业云的同时轻松扩展至云桌面,无需大动干戈的更换现有 IT 建设，或者被不适产品所绑架。

3.4.2 服务器硬件

InCloud Access 系统可部署于标准的 x86 设备，广泛支持主流厂家硬件，根据需求灵活配置，无须与平台软件进行绑定，提供充分的用户选择空间。

- X86 服务器：提供云桌面所需的计算资源，主要包括 CPU 资源和内存资源，支持主流厂商的服务器硬件设备，如通用 X86 服务器、国产 X86/ARM 服务器等。在一体机和超融合架构下，X86 服务器同时提供平台所需的存储资源，以满足各类不同场景的实际需求。

- 集中存储：在 SAN 架构下，计算资源与存储资源分离，InCloud Access 支持各类存储设备，如磁盘阵列、存储服务器等，支持 SDS/FC SAN/NAS 等存储。

- 分布式存储：以 X86 服务器为主，在超融合场景下，存储资源主要使用服务器本地硬盘,通过文件系统,将不同服务器上的存储资源整合成逻辑资源池，InCloud Access 支持分布式存储，通过两副本或三副本，大幅提高系统可用性。

3.4.3 多终端与操作系统支持

支持多家国产产业芯片架构厂商提供的终端，如：兆芯、龙芯、飞腾等，并支持与之配套的国产操作系统上，单位可以根据自己的需要选择合适的终端。灵活的终端

支持技术，满足了单位多样化的办公需求。

- 服务器生态：

适配飞腾、鲲鹏、海光、兆芯等国产 CPU 服务器，如浪潮、华为、曙光、中科可控、联想、东海等品牌国产化/信创服务器。

- 操作系统生态：

适配 Windows、Linunx、统信 UOS、银河麒麟、中标麒麟、中科方德等国产化桌面操作系统。

适配麒麟服务器操作系统

- 终端生态：

适配飞腾、兆芯等国产化终端，如长城、联想等品牌国产化/信创终端。

4 用户体验

4.1 快速交付体验

4.1.1 快速上线体验

一键式安装

InCloud Access 云桌面系统支持普通安装方式和 TUI 工具安装方式，通过 TUI 工具完成安装及所有配置，安装便捷，无需登录虚拟化平台界面即可完成整套系统的安装配置。

虚拟化平台和 InCloud Access 的安装包及开局所需的内核升级包、协议安装包和驱动等都包含在一个 iso 安装包中，并提供了简单便捷的开局工具 TUI，所有的安装和配置均可通过 TUI工具完成，安装便捷，小时级别安装部署。

相比于其它云桌面解决方案，InCloud Access 云桌面解决方案具有安装便捷，部署快速的特点。InCloud Access 云桌面解决方案部署模式可以实现把部分虚拟化软件预安装到服务器上。到客户现场后，只需服务器上电，进行云桌面软件的向导式

安装，接通网络并进行相关业务配置即可进行业务发放，大幅度提高了部署效率。

多样交付方式

InCloud Access 产品提供了多种销售方式和产品交付方式，包括：

- 产品交付：纯软件交付、云桌面一体机交付（软硬一体化交付）
- 产品销售：订单模式（一次性销售）、订阅模式（按月收取服务费）
- 一体机：普通桌面一体机、3D 桌面一体机（即 GPU 桌面）、混合桌面一体机（即普通与 3D 桌面混合部署）、私有云一体机

InCloud Access 产品交付和销售的多样性，既实现了产品标准化，并可开箱即用，又适合用于不同的客户需求，满足不同客户、不同场景的多样化需求。

4.1.2 快速升级体验

InCloud Access 管控系统不重建升级

支持管控端滚动升级，将升级包上传至管理平台后即可完成升级。

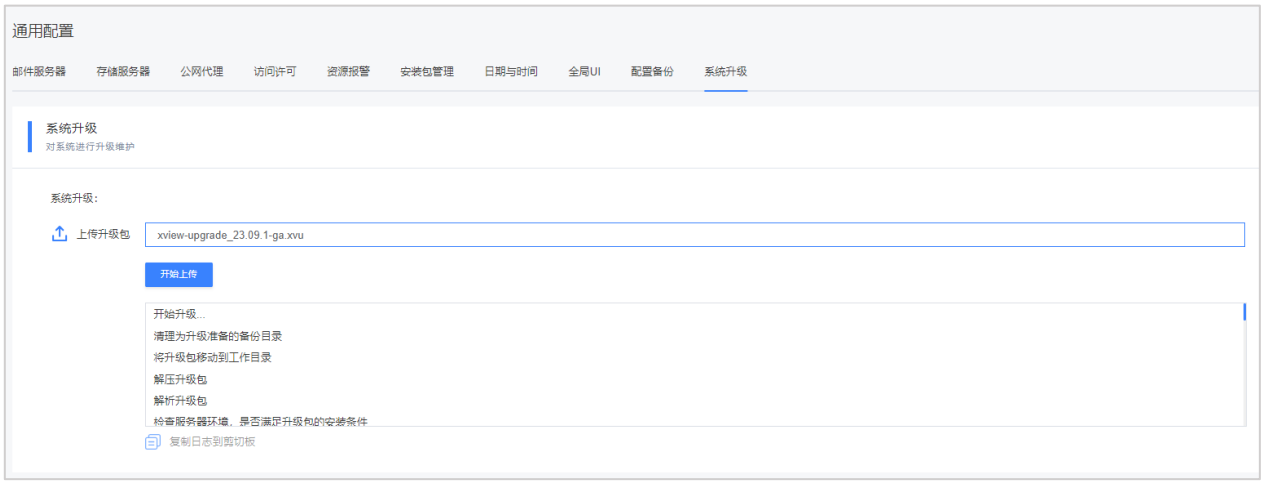


图 2 上传系统安装包升级

终端自动升级

为减轻 IT 管理员工作量，提升工作效率，服务端提供了终端客户端统一自动升级的功能。管理员只需要通过管理平台上传并发布客户端升级包，国产终端开机后，系统将自动检测版本信息，如有新版本，系统会自行下载后安装，省去了逐个升级的

繁琐操作。

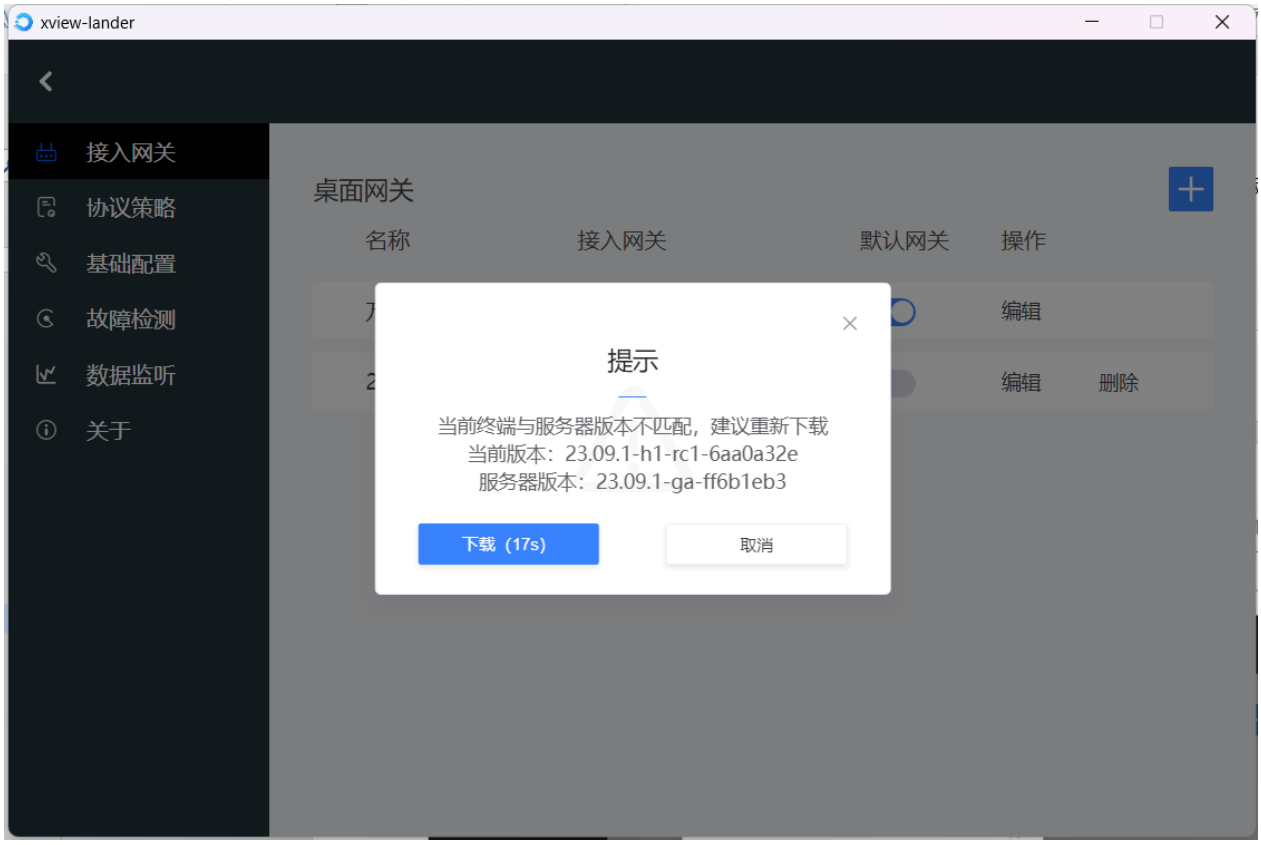


图 3 自动检测客户端版本

4.1.3 用户自助申请

作为用户，可以通过自服务申请自己所需要的云桌面，管理员审批后下发，以降低管理压力。用户可以通过申请的桌面的方式，经过管理员审批同意后，自动获取桌面。

1. 用户按需自助申请桌面；
2. 用户查看申请桌面工单状态；
3. 管理员查看用户提交的工单，并处理；
4. 用户和管理员工单状态同步。

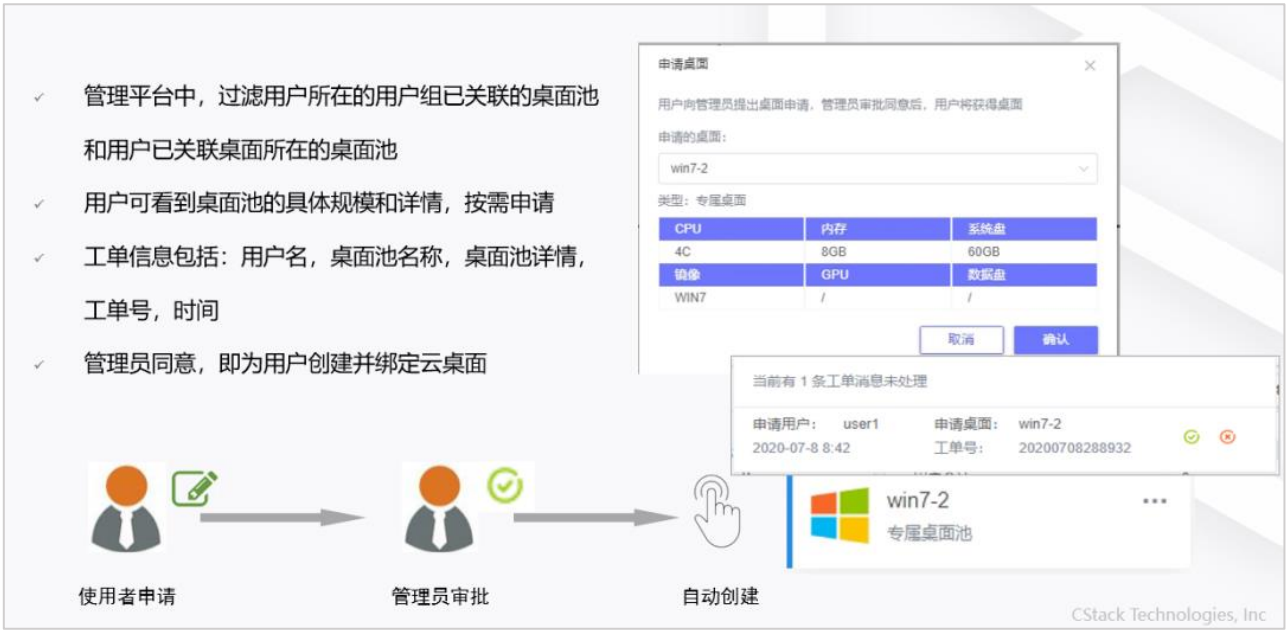


图 4 用户自助申请桌面流程

4.1.4 统一授权管理

对于规模较大的客户，云桌面服务器被划分在多个集群，甚至部署在多个地域的数据中心。为了简化授权，降低云桌面授权管理的复杂度，InCloud Access 支持统一授权管理和批量更新。

按区域配置并发数

授权并发数按区域划分，可以运用在多分支部署场景，统一管控各集群的授权。如图 5 所示。

图 5 授权按区域划分

管理员也可统一配置 XC 云应用用户并发数和 Edge 桌面接入数。

License 批量更新

当系统完成 License 授权后，出现版本升级、新增了计算节点、服务器的硬件配置信息（网卡、硬盘等信息）发生变化、项目升级和 License 已过期的情形时，则需要重新授权。

InCloud Access 支持对同一项目中的不同 InCloud Access 管控平台 license 授权统一进行批量更新。

用户可登录 InCloud Access 管控平台，下载请求码，并将管控请求码（dat 格式）进行逐一替换进行合并。

参考格式：[{"hostname": "InCloud Access", "ip": "127.0.0.1", "code": ["管控平台 1 请求码", "管控平台 2 请求码"]}]

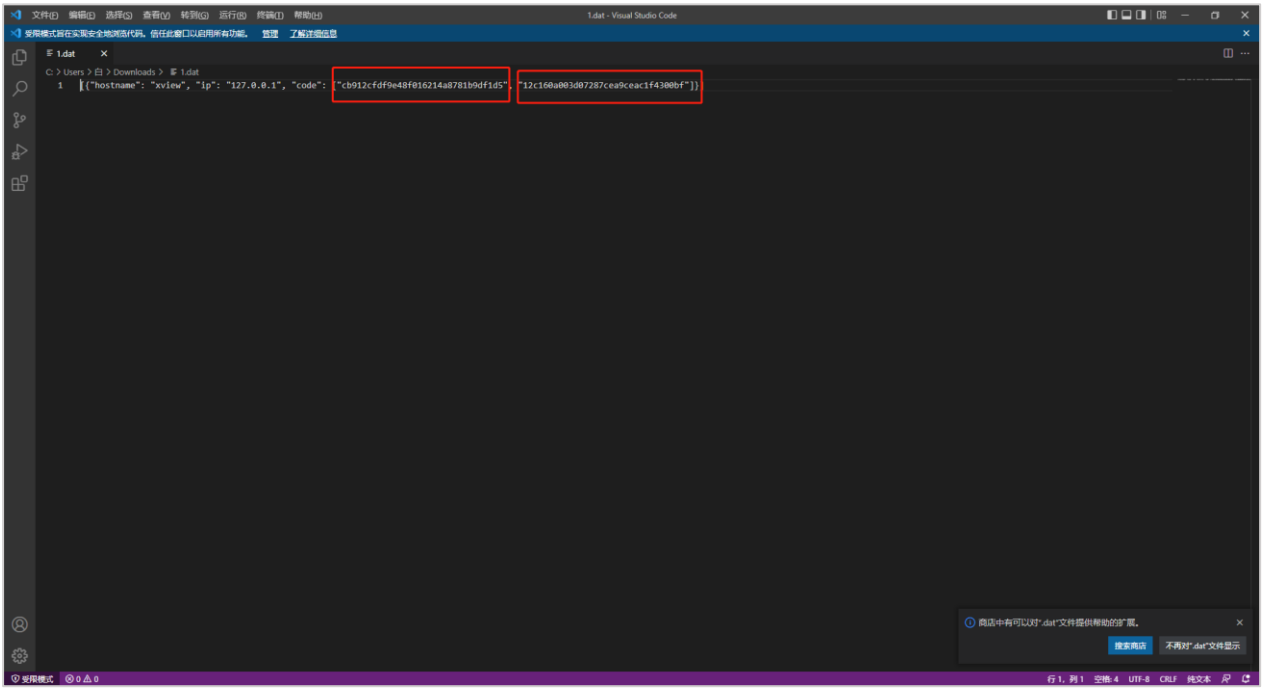


图 6 合并请求码

然后，登录界面，进入用户个人中心。配置授权信息并上传已完成合并的请求码文件。系统会自动生成新的 license 文件，请将其下载至本地。用户可将将获得的新许可证分别上传至不同的管控平台。

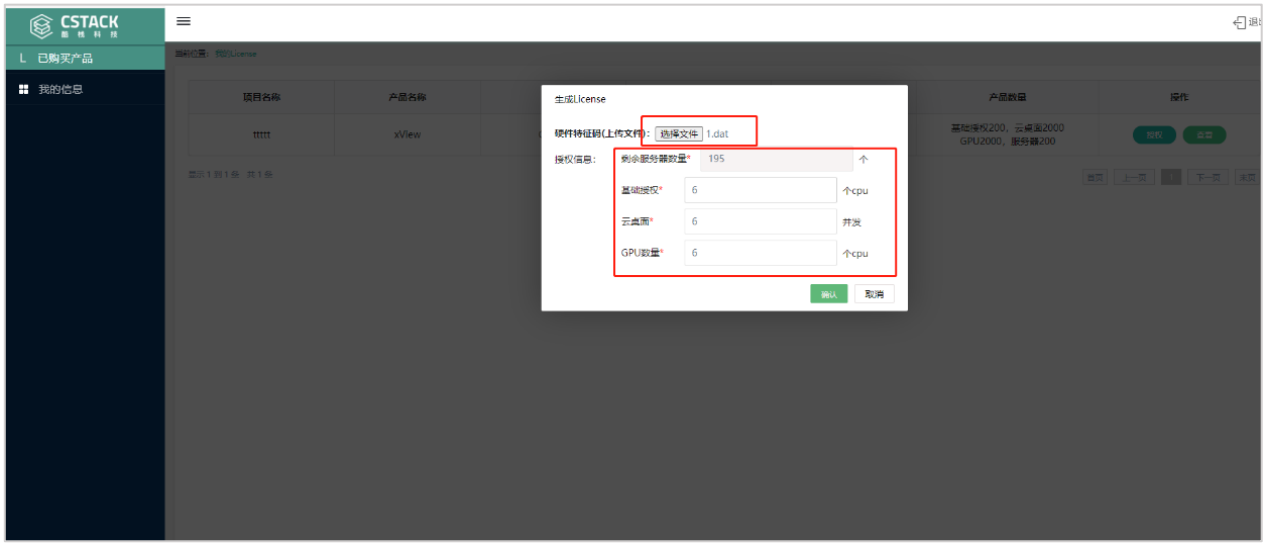


图 7 配置授权信息生成 License 文件

4.2 便捷运维管理

InCloud Access 为终端用户和运维人员提供了丰富的运维工具，帮助用户快速配置和使用云桌面客户端的同时，还可以帮助运维人员更加方便和快捷地进行日常维护，大大提高了终端用户自助能力和运维效率。

4.2.1 实时监控及巡检报告

图 5 浪潮 InCloud Access 管控平台仪表盘

InCloud Access 通过 Web 方式的图形化控制台统一管理云桌面， 仪表盘页面可对管控平台中的云桌面、用户、终端及系统资源进行实时统一监控和总览。通过形象、简洁的单一图形化 Web 控制台进行云桌面的统一管控，IT 管理员可以快速配置整个云桌面环境，降低 IT 管理复杂度与成本，并对所有关键组件(包括 CPU、内存等)提供全面、清晰的性能监控。

还可对 InCloud Access 管理平台关键资源和服务进行全方位一键式健康检查，同时提供巡检报告，助力高效运维，确保云桌面资源和服务处于最佳状态。

报告总体分为：资源使用情况/服务运行情况/Cloud 云桌面/Edge 云桌面/时间

比对/授权许可证/数据库运行情况/数据库同步情况(HA)/keepalived 运行情况(HA)/AD 域控配置情况。

4.2.2 异常桌面巡检

管控平台可自动巡检状态异常的桌面，包括：

（1）【桌面状态：错误】的桌面；

（2）桌面 IP 与管控 IP 不一致的桌面。（巡检结果仅展示有桌面 IP，且桌面 IP 和管控 IP 不一样的数据）

图 6 一键巡检

4.2.3 资源报警

可新增报警报警数据，当使用率大于等于所设定报警条件时，系统将自动发送报警邮件至指定邮箱。报警数据可修改与删除。

支持配置的报警类型：Server CPU 平均使用率（2min）或 Server 内存使用率。

支持自定义资源报警的最低触发临界值。

- Server CPU 平均使用率（2min）：当 2 分钟内 CPU 的平均使用率大于等于所设定报警条件时，系统将自动发送报警邮件至指定邮箱；
- Server 内存使用率:当 server 内存使用率大于等于所设定报警条件时，系统将自动发送报警邮件至指定邮箱。

图 7　新增报警

4.2.4 告警参考

为了保障系统的正常运行，需要在 InCloud Access 管理平台快速查看用户侧上报的告警信息。申报后管理员通过故障消息收到提示并收集用户的故障信息，便于快速定位问题，提高运维效率。

通过告警消息功能，管理员可以进行：

1. 查看告警详情。
2. 参考告警联机帮助及时清理上报的实时告警。
3. 影响业务重点关注的相关告警必须要第一时间闭环。
4. 分析历史告警，确认是否有重复告警定期上报。

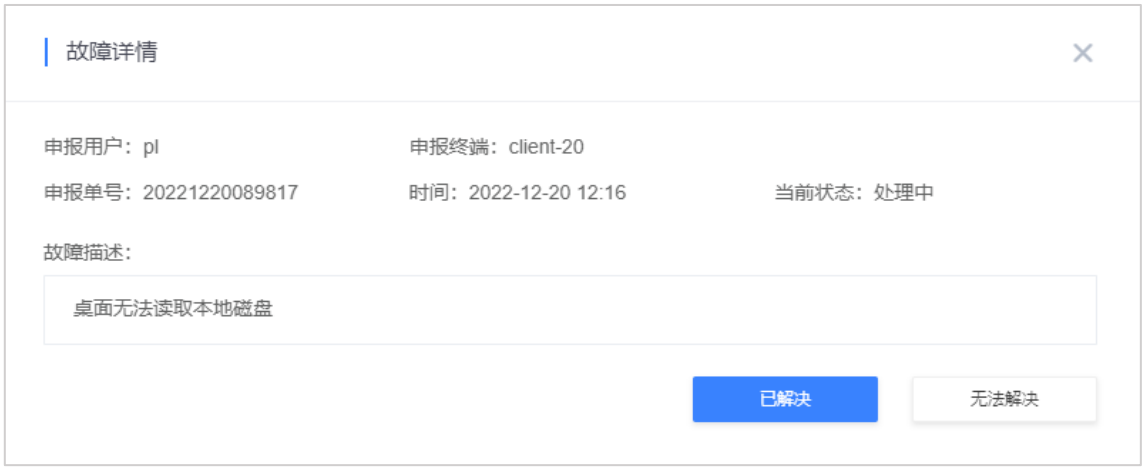


图 8 查看故障消息

4.2.5 终端网络诊断

InCloud Access 云桌面客户端提供了故障诊断工具，以应对用户无法登录虚拟桌面等常见故障。

检测项包括：安装包文件、网卡设备、网关状态、本地用户模拟登录、虚拟化平台连通性、网关服务、后台管理服务以及升级服务。

图 9 故障检测

4.2.6 终端网络数据监控

InCloud Access 云桌面可对硬终端的网络通讯情况进行监控和记录，方便运维人员排查网络问题。

监控项包括：30 分钟内终端的 CPU 使用率、内存使用率、磁盘使用率、网络吞吐、最高上行速率、最低上行速率、最高下行速率、最低下行速率、平均上行速率、平均下行速率、发包数量及收包数量。

图 10 数据监控

4.2.7 终端故障检测

InCloud Access 提供故障诊断工具，以应对用户无法登录虚拟桌面等常见故障。提供故障信息收集机制，能够对系统、网络、外设兼容等报错信息进行归档收集，便于维护分析。包含升级前后的检查。

图 11 终端故障检测

终端检测项：安装包文件、网卡设备、网关状态、本地用户模拟登录、云桌面宿主机连通性、网关服务、后台管理服务、升级服务。

1. 查看关键文件是否缺失
2. 检查如 InCloud Access-player 等文件是否缺失。
3. 网卡设备的状态以及网关连通性检测
4. 使用 internet-available 检测，这个库检测因特网连接状态原理，是检测 dns 连接状态。
5. CM 网关检测
6. 查询当前网关是否连接成功。
7. 后台管理服务检测
8. 查询 api 和 taskflow 服务状态。
9. CM 网关服务检测
10. 查询当前终端 online 接口是否成功。
11. 升级服务检测
12. 同 3。
13. 本地用户模拟登录
14. 模拟用户登录过程，创建用户 --> 登录用户 --> 删除测试用户。
15. 云桌面宿主机连通性检测

查询当前环境所有管理物理机连通性。

4.2.8 最近任务与事件的便捷提示

系统可对最近任务及事件进行通知。

下图为删除桌面池的提示及删除桌面成功的通知。

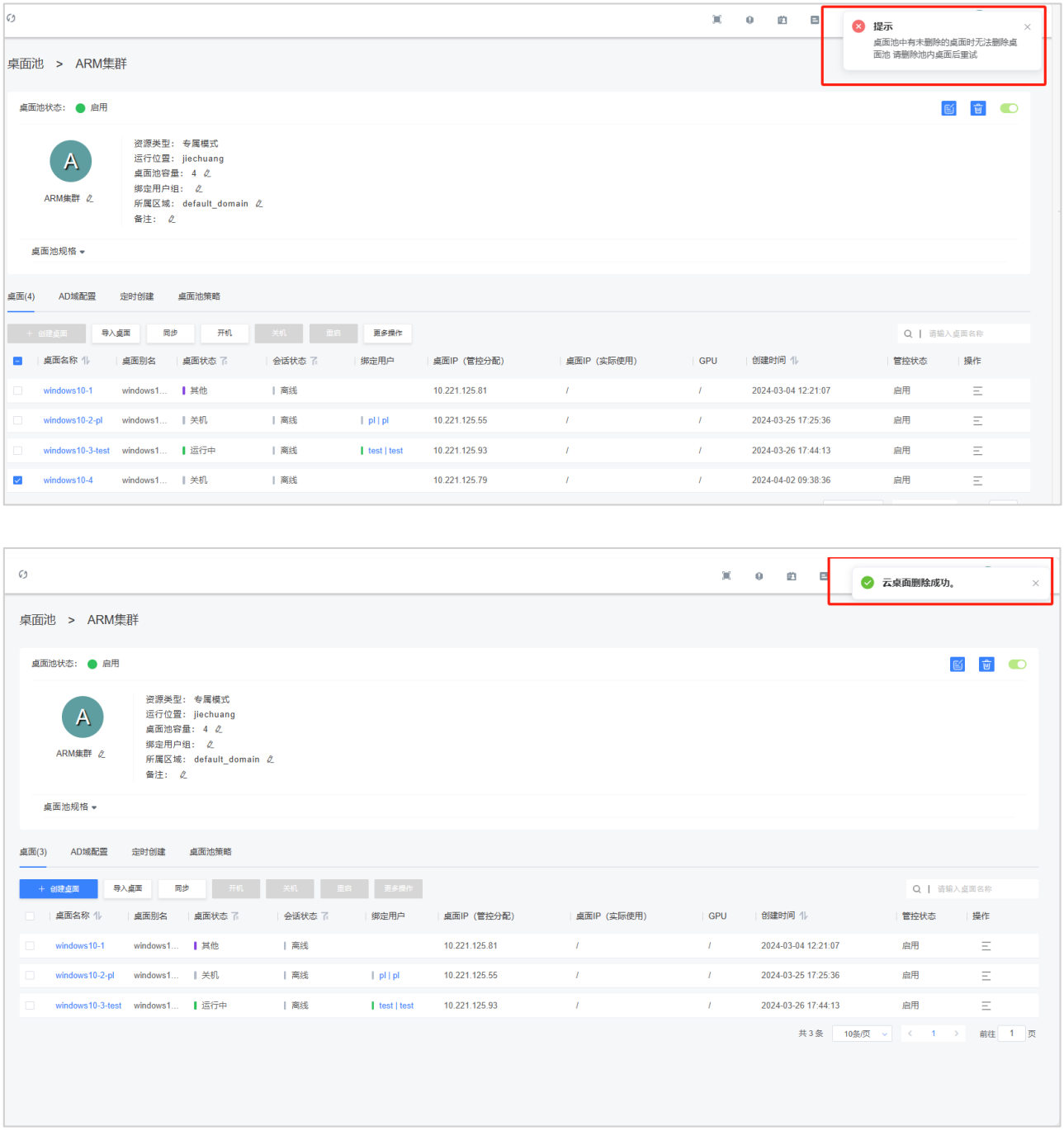


图 12 最近事件便捷提示

4.3 本地 PC 一致的桌面体验

4.3.1 支持通过浏览器连接云桌面

InCloud Access 支持使用浏览器访问普通云桌面，在支持 native 的平台引导使用 native 终端，在 MacOS IOS 等设备也可以进行云桌面的简单访问与操作。

在浏览器中输入 http:// InCloud Access Server 的 IP 地址:443 进入 web 终端登录页面，输入终端用户的用户名和密码，并选中“我已阅读并同意《用户使用协议》”即可登录。

用户有多个可用云桌面资源时，可在多个浏览器页面中同时连接多个云桌面。

图 13 Web 端登录页面

图 14 浏览器查看云桌面详细信息

4.3.2 云桌面与本地数据传输

通过终端连接云桌面时，可通过文件拖曳、剪贴板粘贴、USB 设备及本地磁盘重定向实现云桌面数据与本地 PC 数据的双向传输。

文件拖曳及剪贴板粘贴

说明

仅支持 WinClient/MacClient 软终端。

- 文件拖曳：终端用户通过软终端连接云桌面后，本地磁盘文件可通过直接拖拽的方式拷贝至云桌面。

说明

桌面策略中已同时开启“允许 PC 剪切板”和“允许 PC文件拖拽”。

- 剪贴板粘贴：终端用户通过软终端连接云桌面后，可通过复制粘贴的方式在本地磁盘和云桌面之间单向/双向传输数据。

USB 设备重定向

USB 设备连接至本地 PC 后，通过终端连接云桌面时，可将 USB 设备重定向至云桌面。USB 设备可同时选择多个。

本地磁盘重定向

终端用户通过软终端连接云桌面时，可将本地 PC 的磁盘以盘符的形式重定向进入桌面里。

4.3.3 支持双屏显示

通过 X2000 终端及软终端连接云桌面后，支持配置云桌面双屏显示。

应用场景及双屏模式

双屏模式分为复制模式和扩展模式两种。

- 复制模式

复制模式是指两个显示器显示相同的内容，一般应用在营业厅、会议演示等场景，方便双方互动沟通。

- 扩展模式

扩展模式是指扩展整个屏幕内容的范围，即一个云桌面在两个显示器中运行不同的应用程序，并且两个显示器上显示的内容可以相互拖拽，或者同一个应用扩展到两个显示器中显示，一般应用在办公和制图等场景，方便多任务应用。

双屏连接方式

双屏连接方式如下图所示。

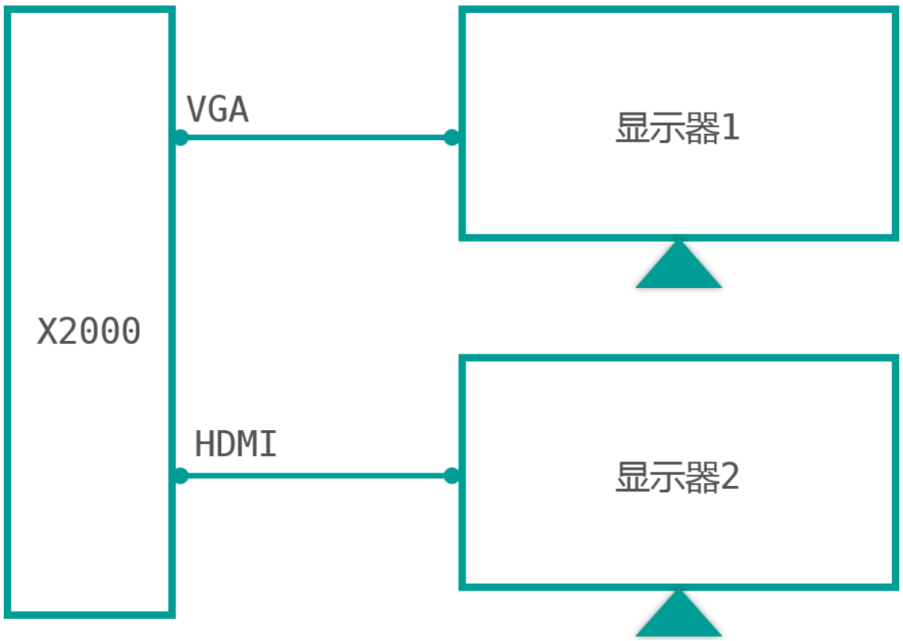


图 15 双屏连接方式

双屏配置参数如下：

图 16 设置双屏参数

- 设置双屏模式

不选中“在所有显示器显示同样的图像”代表扩展模式，选中“在所有显示器显示同样的图像”为复制模式。

- 设置主要屏幕

左上角以颜色区分两个显示器，选中后页面上方显示该显示的基本信息，单击“设为主要屏幕”可将其设置为主屏幕，也可单击“开”或者“关闭”开启或者关闭该显示器。

- 设置屏幕分辨率

可设置屏幕分辨率、刷新率和旋转。设置分辨率时，建议将两个屏幕的分辨率设置为相同的数值，如果两个屏幕的分辨率不一致，最大分辨率为两个显示器中分辨率较低的数值。

4.3.4 支持 4k 分辨率

云桌面的分辨率是在管理平台中或者终端设置的，登录云桌面后，可根据显示器的大小自定义分辨率。

4K 的名称来源于其横向解析度约为 4000 像素，分辨率有 3840x2160 和 4096×2160 像素 2 种超高分辨率规格。相比主流的 1080P 全高清分辨率，4K 显示器增加数百万个像素点，画面的精细程度及显示品质有质的飞越。

InCloud Access 云桌面支持设置 4K 分辨率。终端已连接 4K 显示器后，通过终端或者云桌面操作系统设置屏幕分辨率为 4K 即可

说明

如果云桌面未使用硬编加速，则设置 4K 分辨率时可能会有卡顿。建议为硬编加速、GPU 直通或者 vGPU 桌面设置 4K 分辨率。

4.3.5 打印机重定向

基本原理

1. InCloud Access player 和 InCloud Access agent 通过 InCloud Access 主通道进行打印机重定向信息的交互；
2. player 需要获取到打印机名称 printer_name 和 IP 地址 printer_IP；

3. player 将打印机名称传给 agent；
4. agent 负责虚机 IPP 打印机，打印机的端口为标准 TCP/IP 端口，名称为：${printer_name}(重定向)。agent 监听在 127.0.0.1:9100 端口，接受打印数据；
5. 用户在桌面内选择虚拟打印机进行打印时，agent 在 9100 端口上接收到 RAW 打印数据；
6. agent 通过 spice 通道将打印数据下发给 player；
7. player 连接 printer_IP:9100，将接收到的打印数据传给打印机。
8. LANDER 负责：
9. 用户可以在 lander 上对打印机的“名称”、"IP 地址"进行增、删、改。打印机名称/IP 地址一一对应。
10. 打印机连接端口为 9100，lander 上可选进行配置。
11. 用户在 lander 上从已经添加的打印机中可以选择某一个打印机进行重定向，也可以不选择打印机。
12. 若用户选择了某个打印机，lander 在连接桌面时，传递“该打印“机的名称、IP 地址给 player，由 player 进行重定向（lander 只传 1 个打印机的信息给 player）。
13. 若用户在 lander 里没有选择打印机，player 不进行打印机重定向。
14. PLAYER 负责：
15. Player 通过参数获取到打印机的名称、IP 地址和端口号。
16. Player 将打印机名称传给 agent，并启用打印机重定向。
17. 用户打印时，和打印机 printer_ip/printer_port 建立 socket 连接。
18. 接收 agent 下发的 raw 打印数据并发给打印机。
19. 打印完成后，agent 下发通知，player 断开和打印机的 socket 连接。

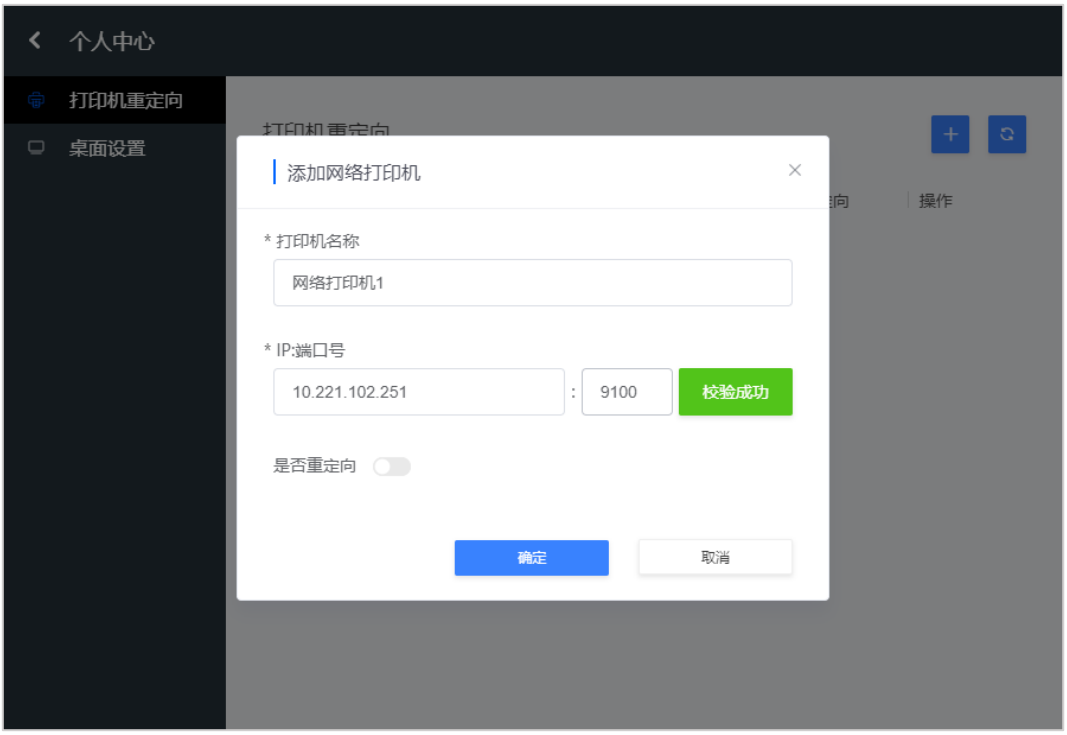


图 18 终端设置网络打印机参数

4.3.6 外设无感知重定向

云桌面中，USB 设备都可以通过客户端的 USB 接口直接映射进入虚拟机，外设的使用体验和传统 PC 一样方便，即插即用。这其中就用到了 USB 重定向技术，将客户端 USB 的数据接管后，通过网络发送至 InCloud Access InCloud Access Server，InCloud Access 会虚拟出一个 USB 设备插入虚拟机。

通过终端连接云桌面之后，在桌面顶部菜单的下拉图标中选择重定向按钮。

重定向的设置页面如下所示：

图 19 云桌面中 USB 重定向设置页面

4.4 增值桌面体验

4.4.1 丰富的云桌面类型

由于使用场景和工作岗位的不同，用户需要多种类型的云桌面，InCloud Access 提供了以下五种类型的云桌面：

专属模式：用户与桌面持久关联，并独享桌面所有资源，直至桌面与用户解绑。用户可在桌面中安装应用程序并进行个性化设置，桌面关机或者重启后系统不还原。

还原模式：用户与桌面持久关联，桌面关机后系统盘还原至初始状态。

临时模式：用户与桌面非持久关联，桌面关机后自动删除。

定时模式：用户与桌面非持久关联，桌面到期后自动删除。

池模式：用户与桌面非持久关联，桌面关机后解绑用户。在池模式下，还可配置 “关机是否自动还原至初始状态”：

- 设置为还原时，桌面关机后，自动还原至初始状态；
- 设置为不还原时，桌面关机后，不还原至初始状态，再次绑定时，保留上次操作者所存数据。

4.4.2 用户行为审计

InCloud Access 云桌面提供桌面监控功能用于事件回溯。传统办公模式下，用户日常行为无法监控，这就导致了很多无法控制的风险，包括数据泄露等，InCloud Access 云桌面为客户提供了屏幕监控功能，进行用户行为查看及事后回溯。支持管理员对用户的桌面行为进行实时视频监控录屏，支持对特定用户的桌面行为，在特定时间段，周期性（每隔几秒或几分钟可配置）的屏幕保存，系统会自动进行桌面的图片保存，实现对用户操作的监管和事后回溯。

InCloud Access 云桌面 InCloud Access 协议桌面基于 H.264 进行传输，易于对屏幕进行录像和持久保存。

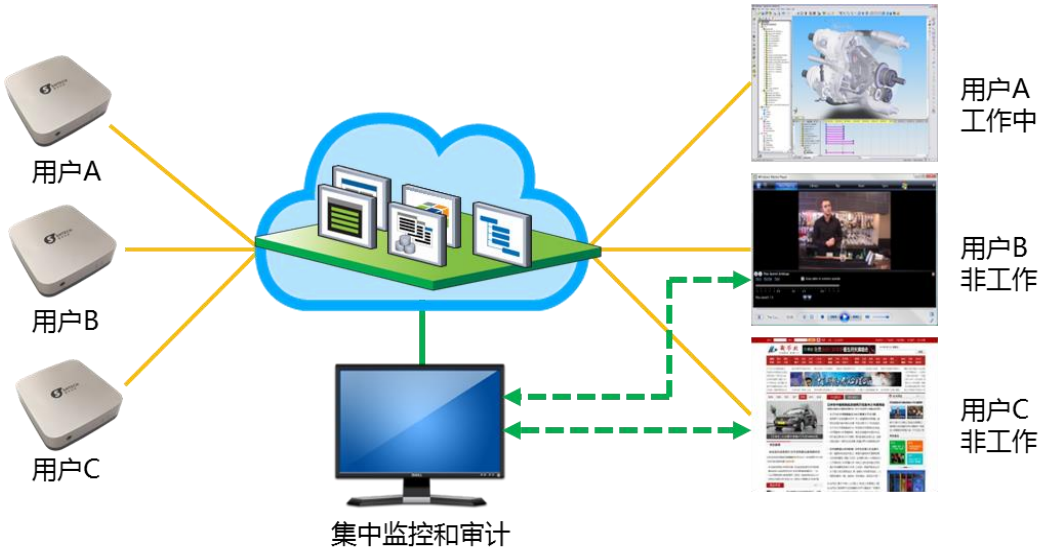


图 20 用户行为监控和审计

4.4.3 4K/8K 超高清视频体验

所谓 4K 视频通常是指的是在 16：9 的画幅下 3840×2160（4096×2160 通常用于数字电影领域）像素分辨率的视频节目，它的分辨率是高清电视的 4 倍。在此分辨率下，观众将可以看清画面中的每一个细节，每一个特写，得到一种身临其境的观感体验。而 8K 视频是 4K 视频的后续产品，电视制造商正在推动 4K 成为新的电视标准，8K 预计在 5 年后成为主流消费显示器分辨率。

因此，将云桌面与 4K/8K 视频播放场景结合起来，将云桌面应用于 4K/8K 视频播放场景，有重要的意义。同时，也对云桌面重载情况下的服务能力，提出更高的要求。主要体现在以下两点：

- 4K/8K 视频对云桌面显卡能力的需求
- 云桌面在 4K/8K 视频传输情况下的带宽控制

GPU 虚拟化技术

浪潮云海 InCloud Access 产品支持基于显卡虚拟化、显卡直通等多种云桌面 GPU 虚拟化技术，并针对具体客户云桌面使用场景和需求，采用不同的解决方案，以满足从视频播放、简单 AutoCAD 图形设计，到 CATIA、大型游戏、Revit 等中高端使用需求。

- （AMD）显卡虚拟化技术

AMD MxGPU 是一款基于硬件的 GPU 虚拟化解决方案。它基于行业标准 SR-IOV（单根 I/O 虚拟化）技术而构建，每个物理 GPU 支持多达 16 个虚拟用户远程工作（如 AMD Radeon™ Pro V340 每个显卡最多支持 32 个并发用户）。

- 显卡直通技术

GPU Pass-through 方案，即 GPU 透传或直通方案，就是将主机的多块物理 GPU 按照一比一的比例分配给此主机上运行的虚拟桌面。此模式下，物理 GPU 被指派给每个虚拟桌面用户。该方式避免了 GPU 共享模式带来的抽象层开销，最大限度的提升虚拟化 GPU 性能体验。

高性能流化桌面传输技术

H.264 是目前常见的视频编码标准之一，是一种基于块（Block）的视频编码，H.264 支持 16*16，8*8，4*4 的帧内预测块。它充分利用帧内块（Block）的空间相关性和帧间块(Block)的时空相关性来对视频进行压缩，因此可以达到比较高的压缩率。

H.265 是继 H.264 之后所制定的新的视频编码标准。H.265 标准围绕着现有的视频编码标准 H.264，保留原来某些技术的同时并加以改进。H.265 旨在在有限带宽下传输更高质量的网络视频，仅需 H.264 一半带宽即可播放相同质量的视频。H.265 标准也同时支持 4K 和 8K 视频。

InCloud Access 开创性的使用流化技术传输云桌面。该技术对云桌面内容使用 H.264/H.265 格式进行编码，码流通过网络传输，智能云终端对码流解码后呈现在显示器。

基于硬件加速技术

传统云桌面方案使用CPU做桌面音视频内容的编码,对于视频的支持效果较差，视频播放会严重影响其他用户的在线体验，同时降低单服务器的并发支持能力。

浪潮云海把 GPU 编码技术引入云桌面产品，服务器采用 CPU+GPU 的融合技术。CPU 和 GPU 各有所长，视频编解码中涉及到多种类型的操作，因此需要将 CPU 和 GPU 结合使用，CPU 负责支撑用户的桌面上面的应用程序，GPU 负责视频编码，以达到最佳的效果。InCloud Access 的 GPU 编码功能遵循以下几个原则：

- 尽可能地将任务并行化，同时在 CPU 和 GPU 上并行地处理。
- 因为 GPU 与计算机主存的交换速度很慢，因此要尽量减少 GPU 与主存的数据交换，将数据尽可能地留在 GPU 中进行计算而不是反复读写。
- 尽可能地将计算任务交给 GPU 来做，减轻 CPU 的计算量。

InCloud Access通过GPU硬件加速技术能够在各种场景下为每个用户提供1080P的桌面分辨率，尤其是多路 4K/8K 并发应用场景时，可以节省 CPU 资源以承载更多用户，并且用户体验不下降。

实际经验表明，基于 GPU 虚拟化技术、硬件加速技术的 InCloud Access 云桌面解决方案可以良好的支持 4K/8K 视频播放场景，从而体现出较高的方案价值和经济价值。

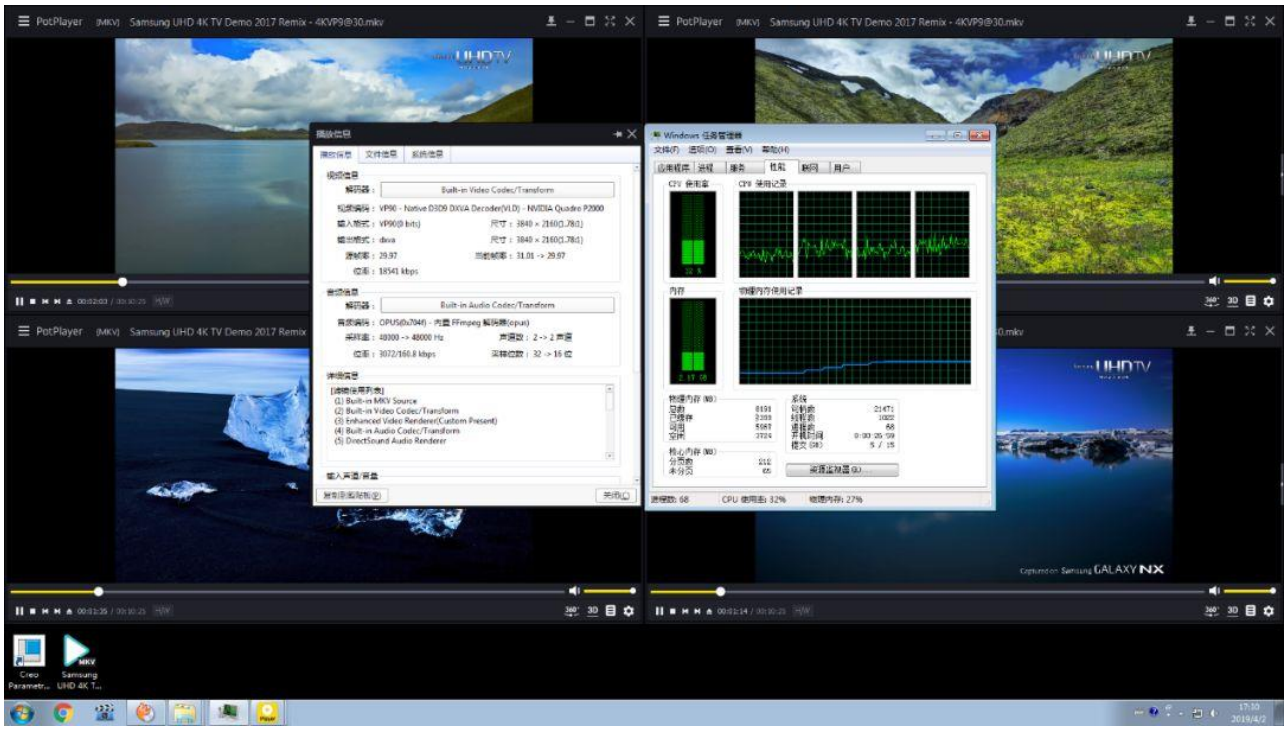


图 21 4 路 4K 视频同时播放

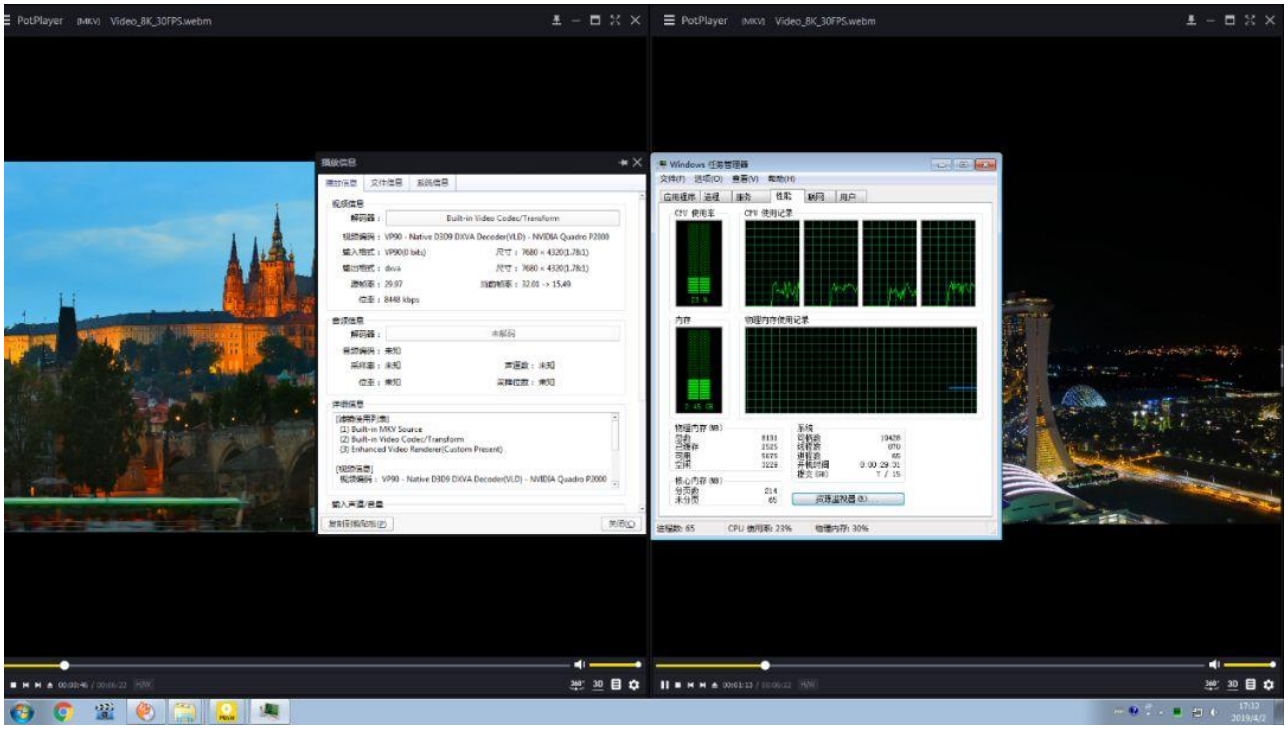


图 22 2 路 8K 视频同时播放

图 1 和图 2 表明在配置为 4C8G 云桌面坏境下，单个云桌面可以完美支持 4 路 4K 视频或 2 路 8K 视频同时播放。并且通过硬件加速技术，大幅降低对 CPU 资源的消耗。

同时，考虑到 4K/8K 视频对带宽的占用较高，尤其是在广域网环境中，给用户带来更多的带宽成本。因此，InCloud Access 产品基于 H.265 编码的流化桌面传输技术，在不降低用户体验情况下，大幅降低 4K/8K 视频等高端场景对传输带宽的需求。H.265 编码占用带宽是 H.264 编码占用带宽的 60%。

4.4.4 大型游戏及云游戏体验

随着 5G 网络时代的来临，网络延迟和带宽情况将得到极大的改善，因此，采用（VDI 模式）云桌面去承载云游戏，将云桌面与云游戏结合起来，是云桌面和云游戏未来发展的一个可行方向，主要体现在以下几点：

- 在 5G 高速网络下的多终端支持能力
- 云端的 GPU 处理能力
- 云端资源复用带来成本降低，提高业务收益

基于云桌面的云游戏，游戏的服务端运行在云端，用户终端侧采用瘦终端，游戏内容采用流化的方式下传，降低了对硬件的需求。

InCloud Access 产品不仅仅可以作为普通云桌面，通过我们对游戏的实测，也可以为用户提供一个高配置的游戏云桌面，所有游戏云端统一部署，用户可以通过瘦终端、手机、甚至电视都可以体验大型游戏。InCloud Access 采用流式传输协议，支持 H.264/H.265 编码、GPU 虚拟化/透传、硬件加速等独特技术，保障了云游戏的高画质、低延迟、操作灵活，极大的提升了游戏玩家的体验，由于游戏处理和画面渲染全部在云端完成，极大的简化了客户端的配置需求。相比其他云桌面，InCloud Access 云桌面所提供给用户的配置更高、体验更好。

所有的游戏均安装在云桌面的服务端，在云桌面上运行的云游戏支持多终端访问，用户可以通过瘦终端、软终端（PC 端以及手机端）体验游戏。云桌面服务端与终端通过有线网络、无线网络、5G 网络进行桌面、键鼠及游戏手柄信号的传输，而这些数据的传输则依赖于浪潮云海 ICAP（InCloud Access Protocol）自研高效桌面传输协议，该协议支持场景化压缩编码技术，包括 H.264、H.265，桌面通过 ICAP 协议进行网络传输，瘦终端本地解码后呈现在本地显示器，同时该协议支持画面的智能侦测，VBR 等技术，有效的解决了带宽占用和画面质量的矛盾关系。

浪潮云海云游戏桌面解决方案中提供了灵活的 GPU 方案选择，包括 AMD 的显卡虚拟化方案，GPU Pass-through 方案（即 GPU 透传或直通方案），通过上述方案，可以给不同层次的云游戏玩家提供不同的云桌面解决方案，以此满足玩家对不同游戏

配置的需求。

InCloud Access 支持 H.264 和 H.265 两种编码格式，同时支持硬件和软件编码方式。

游戏名称及流编码方式	带宽占用（谷值）	带宽占用（平均值）	带宽占用（峰值）
《尘埃 4》H.264 1080P@60FPS	5.36Mbps	14-18Mbps	32.86Mbps
《尘埃 4》H.265 1080P@60FPS	3.24Mbps	9-11Mbps	16.75Mbps
《刺客信条奥德赛》H.264 1080P@60FPS	4.78Mbps	15-17Mbps	34.57Mbps
《刺客信条奥德赛》H.265 1080P@60FPS	3.47Mbps	10-11Mbps	17.36Mbps

图 23 两款游戏在不同编码格式下的带宽占用测试情况

上表是我们对两款大型游戏采用 H.264 和 H.265 编码格式进行实际测试，其测试表明基用 H.265 编码格式优化的 InCloud Access 协议，在大型游戏高消耗情景下可以节约 40%以上的带宽，更加适合移动网络的云游戏场景，从而体现出较高的方案价值和经济价值。

目前，经过实测的游戏有《Apex 英雄》、《刺客信条奥德赛》、《尘埃 4》、《只狼》、《守望先锋》、《拳皇 14》、《英雄联盟》、《星际争霸》等，并且可以支持游戏手柄方向盘等游戏套件。

4.4.5 Cloud + Edge 双模式统一管理

基于边缘+中心混合云计算架构理念，浪潮云海研发了 InCloud Access Edge 前端云桌面产品线，实现了云+端双模式融合云桌面平台 InCloud Access ，使得两张模式云桌面的系统镜像、用户数据磁盘、用户账号认证和管理 UI 的融合和统一管理，按需交付，相较传统云桌面场景支持更优秀、丰富。

Cloud 模式将云桌面用户所需的计算、存储和 GPU 等资源全部集中在云端，并通

过局域网、5G、4G 或其他广域网方式将桌面流推送至用户设备。由此，用户便可在传统 PC、瘦客户机、手机、平板等各类终端上使用各类桌面系统和应用。

而 Edge 模式则将用户登录信息、安全策略、管理策略等与操作系统剥离并存放在云端，如此，用户便可充分利用本地的计算、存储和 GPU 资源，在弱连接甚至无连接的情况下完成办公和其他应用。Edge 模式优势在于既可实现完整、全面的管理和安全功能，亦能降低对云端服务器和网络的压力，实现成本、应用体验和管理运维之间的平衡。Edge 模式主要部署在具备本地计算和存储能力的胖终端、台式机和笔记本当中。

两种模式虽然对应了不同的应用形态，但却可以在 InCloud Access 云端管理平台上的统一门户实现混合管理，让一套解决方案满足尽可能多的应用场景需求。

4.4.6 vApp 模式满足国产化需求

在很多具体业务场景中，仍有大量应用软件需要传统 Windows 环境的支持；但如此一来，政企用户又很难满足安全合规的硬性需求。

为解决这一矛盾，InCloud Access 还提供了在国产操作系统中嵌套 Windows 应用的 vApp 模式。

图 25 vApp 云应用

云应用指的是终端与服务端（云应用服务器）互动的应用，终端操作同步云端，也通过云端备份保留终端数据。

根据终端操作系统的不同，云应用分为 XC 云应用管理和 MS 云应用管理，以针对不同的应用场景。

XC 云应用：支持 A3000 系列、X2000 系列瘦客户端。

MS 云应用：支持 Web-Client。

由此，用户便可在安全合规的国产 OS 云桌面环境下继续使用运行在云端的 Windows 应用程序；业务、合规两不误。

适用场景：使用者无需关注桌面操作系统，仅按需使用应用即可；在国产化过程中，解决依赖 X86/windows 环境的应用过渡期使用的问题。

适用终端：兆芯/飞腾等国产化 CPU 终端、传统 X86 PC、windows/麒麟/UOS 等 OS 下软终端、VDI 云桌面。

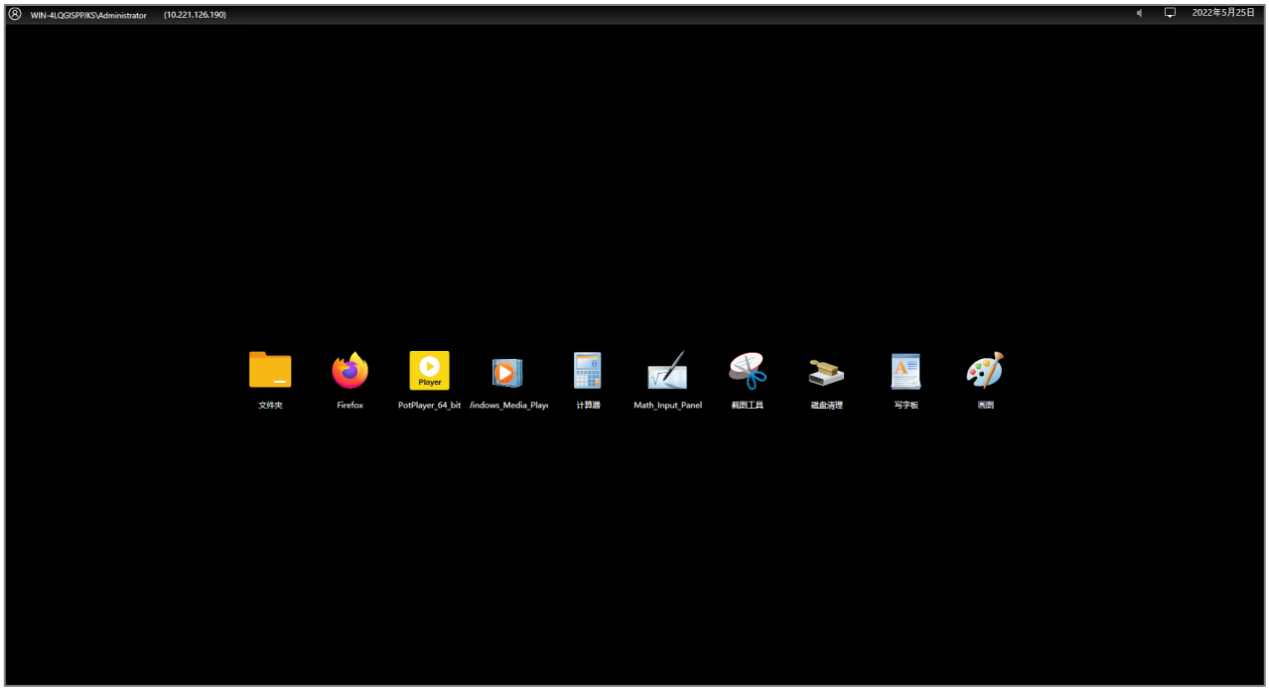


图 26 云应用界面

4.4.7 用户自助恢复快照

用户在终端可进行快照管理，如果用户误操作导致系统蓝屏、无法开机、数据丢失或者其他异常时，可通过回滚将桌面状态恢复至创建快照的时刻，减少桌面系统数据丢失，保证业务连续。

图 27 桌面快照页面

4.4.8 桌面访问限制

1. 管理员可通过策略配置限制访问时段，禁止桌面再该策略启用时间段内被访问。

   - 内容主要包含周几、时间段、是否启用。
   - 同一天不允许添加两条限制，例如：已经存在周二的限制策略，就不能再添加周二的策略，只能对其修改。
   - 最多添加 7 条策略数据。

2. 通过策略配置限制访问 ip，禁止桌面连接终端的 ip 地址在启用策略时且存在于限制 ip 范围时被访问。内容主要包括 ip 段或者单个 ip。

实现方法

在终端连接桌面时（connect-desktop），首先查询该桌面的限制访问策略数据，如果开启了相关策略，则根据时间或者 ip 进行校验，验证通过则允许连接，否则，抛出异常。

图 28 限制访问桌面策略

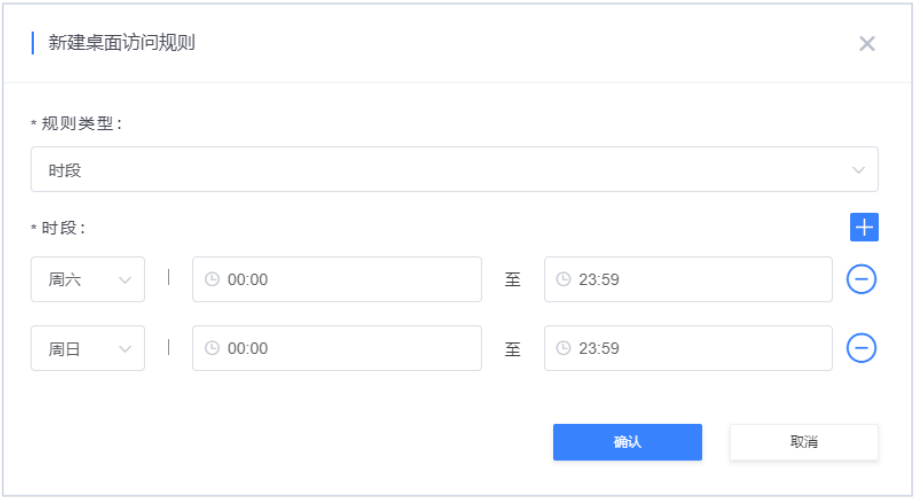


图 29 桌面访问规则配置-时段

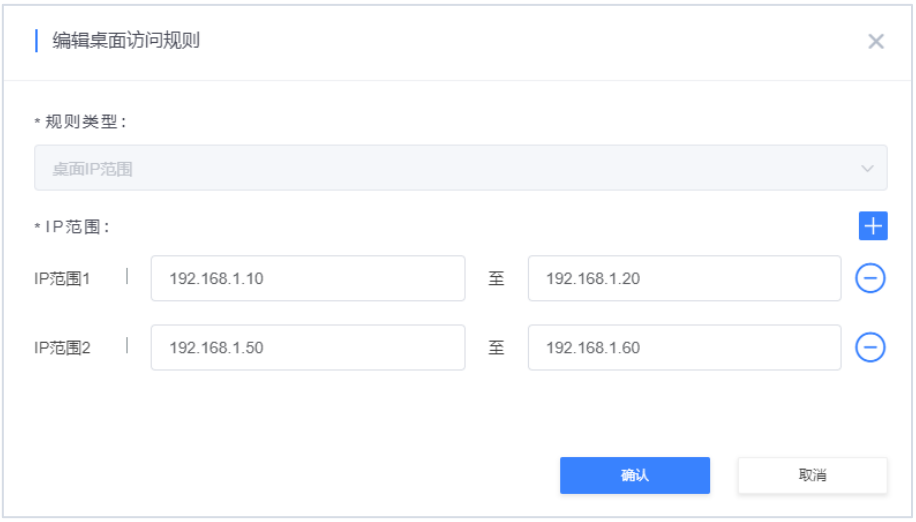


图 30 桌面访问规则配置-IP 范围

4.4.9 多元化策略管控

内置三个层级的策略管控机制，可针对全局、组及单个资源设置策略，管理员可根据实际环境和特有要求创建合理、高效、灵活的策略方案，真正实现随心所欲的管控。

- 多维度

桌面策略、用户策略和终端策略三个维度的策略管控，分别针对桌面、用户及终端进行精细策略管控。

- 多层级

内置三个层级的策略管控机制，可针对全局、组及各个资源设置策略。

- 精细粒度

满足不同桌面类型和访问方式等不同场景下的精细控制。

新建系统时，桌面策略、用户策略和终端策略均为全局策略。桌面/用户/终端添加后，可根据实际需求配置私有策略。

创建私有策略并保存配置后会立即生效，且显示“私有”标记；修改全局策略后，下发后将应用于管理平台中的所有桌面/用户/终端组和桌面/用户/终端，私有策略经配置部署后，将自动清除私有标记。

策略总览图如下所示：

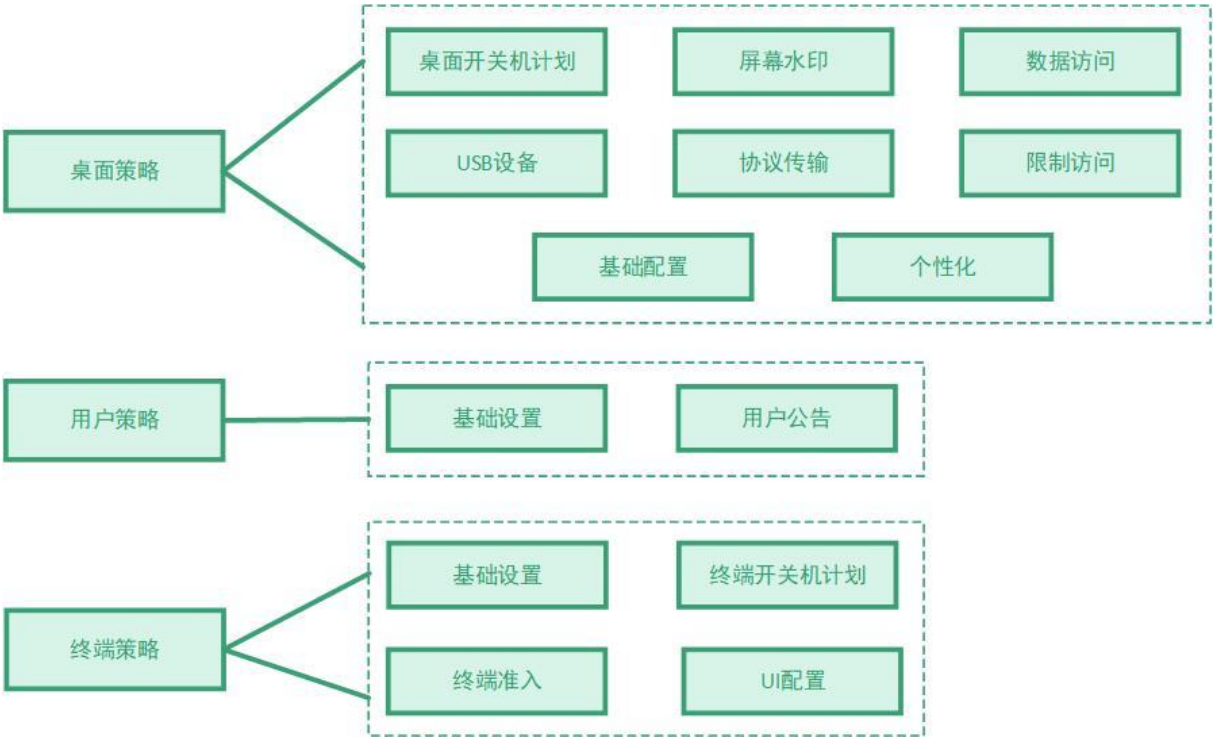


图 31 策略功能总览

4.4.10 全显卡及方案支持

目前，InCloud Access 可提供基于 GPU Passthrough、硬件 GPU 虚拟化等技术的全显卡 InCloud Access 桌面云解决方案。满足不同场景，各类用户对 GPU 的使用需求。

InCloud Access GPU 方案

- GPU 虚拟化方案—MxGPU

国内首家 AMD 认证的开源 KVM MxGPU 方案，采用 AMD 推出的业界第一款基于 SR-IOV 标准的硬件虚拟化 GPU，单卡最多可支持 32 个用户并发使用，采用纯硬件的调度方式，避免 GPU 抢占问题，使用原生 AMD 驱动，无需虚拟化软件层支持，无需软件授权费用。

- GPU 虚拟化方案—KVMGT

Intel GPU 全虚拟化技术，通过 Intel Xeon E3 系列 CPU 核显实现，无需额外配置专业 GPU，单 CPU 支持至多 4 个桌面。用于满足入门级游戏、视频编辑、媒体转码、平面设计等场景中的低端的 2D/3D 加速需求。

- GPU 虚拟化方案—Passthrough

支持市面上主流的显卡，包括 NVIDIA Quadro、GeForce GTX、Tesla Grid 系列，Intel Iris Pro 系列，AMD Firepro 系列，提供和本地图形工作站一致体验的 GPU 解决方案，用于满足大型游戏、AutoCAD、Solidworks、ArcGIS、Revit、Maya、CATIA 等场景的 2D/3D 高端使用需求。

InCloud Access GPU 虚拟化方案性能

作为考查桌面云 GPU 虚拟化性能的重要参考依据，互联网部署环境下 3D 效果的好坏和高清视频播放的流畅度与解决方案性能的优劣有着密切联系。

以下测试方案在云桌面配置规格方面，选择了三类典型带 GPU 的云桌面配置；GPU 虚拟化方案采用了 GPU Passthrough；在场景测试部分，选取了普通办公、大型游戏、高清视频播放三类常见使用场景，针对使用体验、性能指标、网络带宽等方面进行严格检测。

- 三类配置开关机用时对比

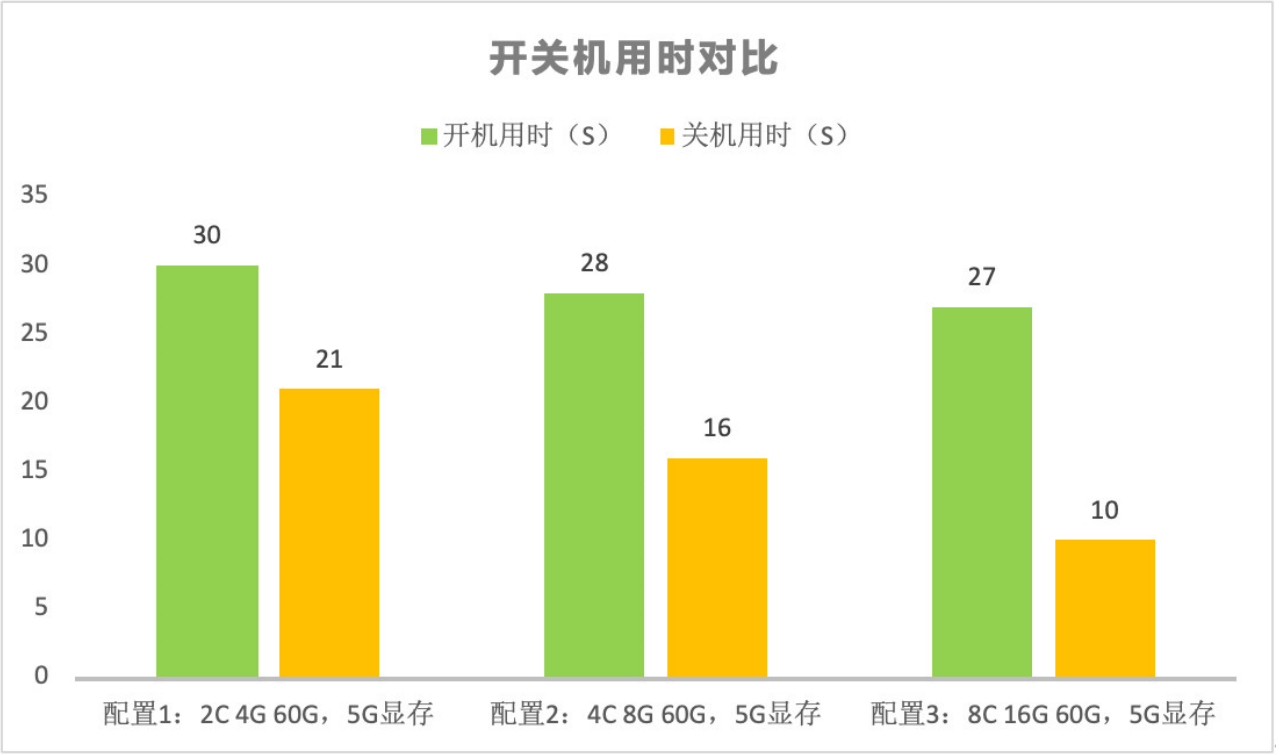


图 33 开关机用时对比

- 三类配置开机资源占用率对比

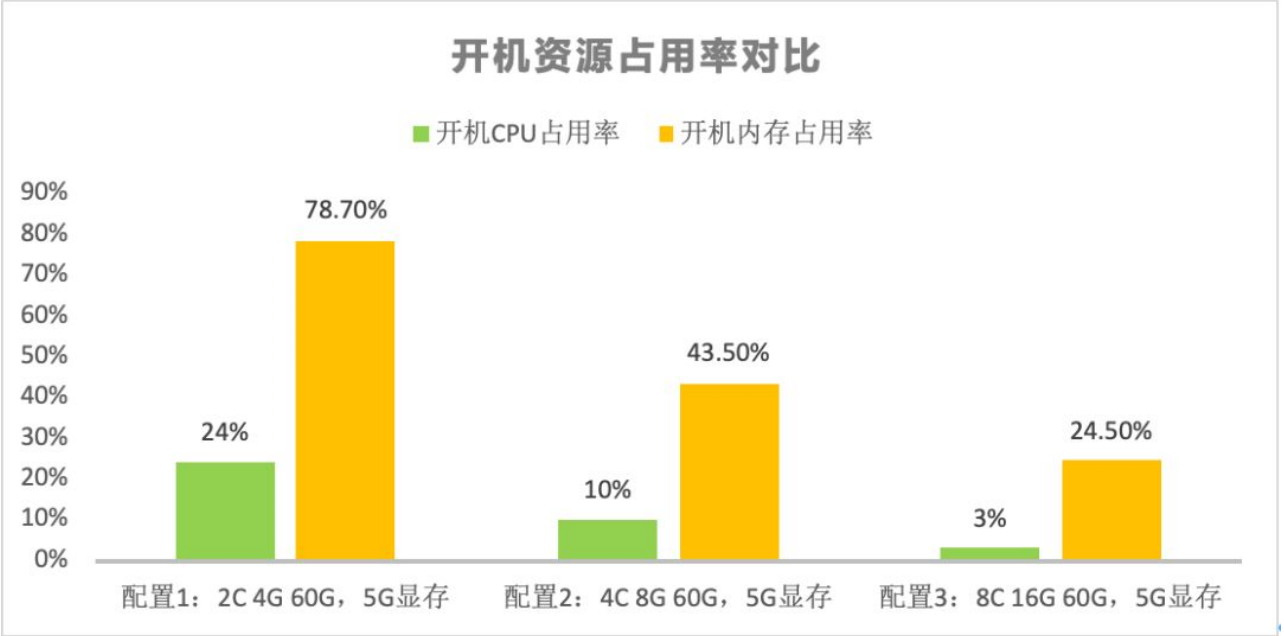


图 34 开机资源占用率对比

- 三类配置在不同应用场景下性能对比

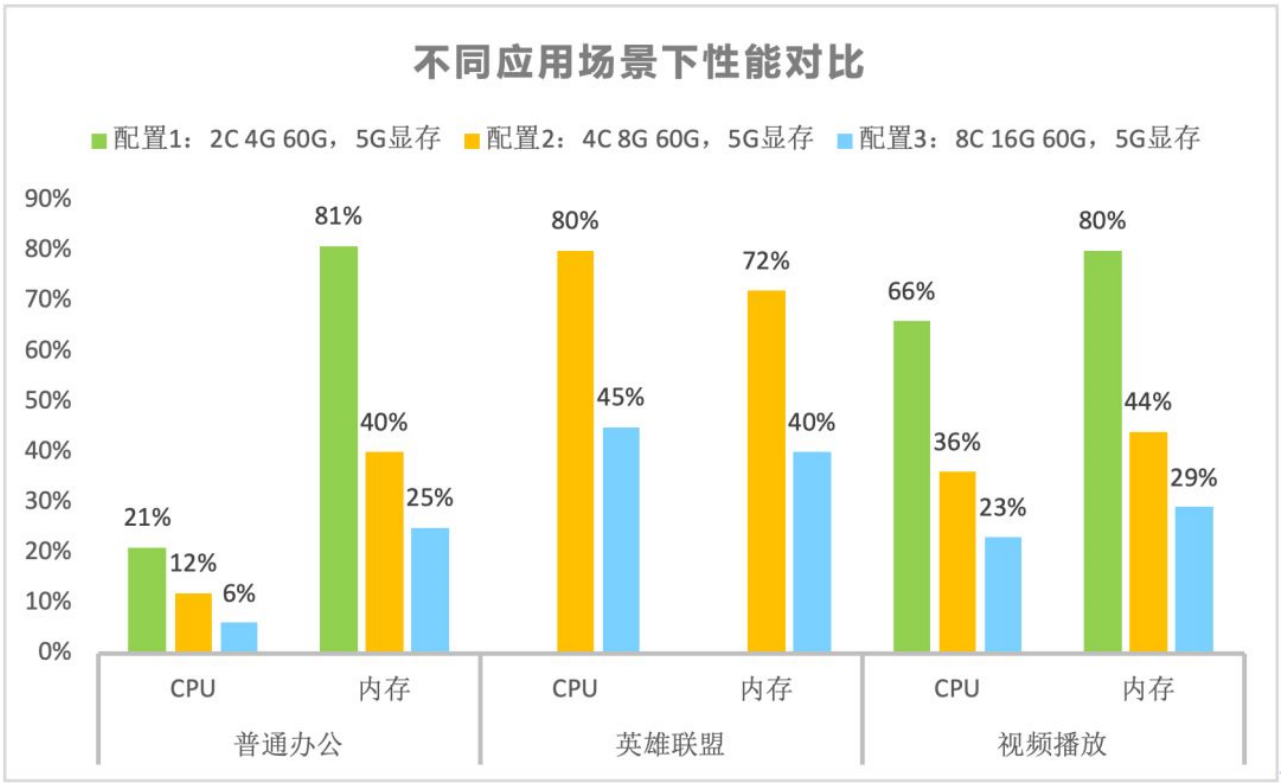


图 35 不同应用场景下性能对比

注：配置 1 因资源不足无法进入英雄联盟。

- H.264 与 H.265 协议带宽峰值对比

游戏场景：星际争霸 2

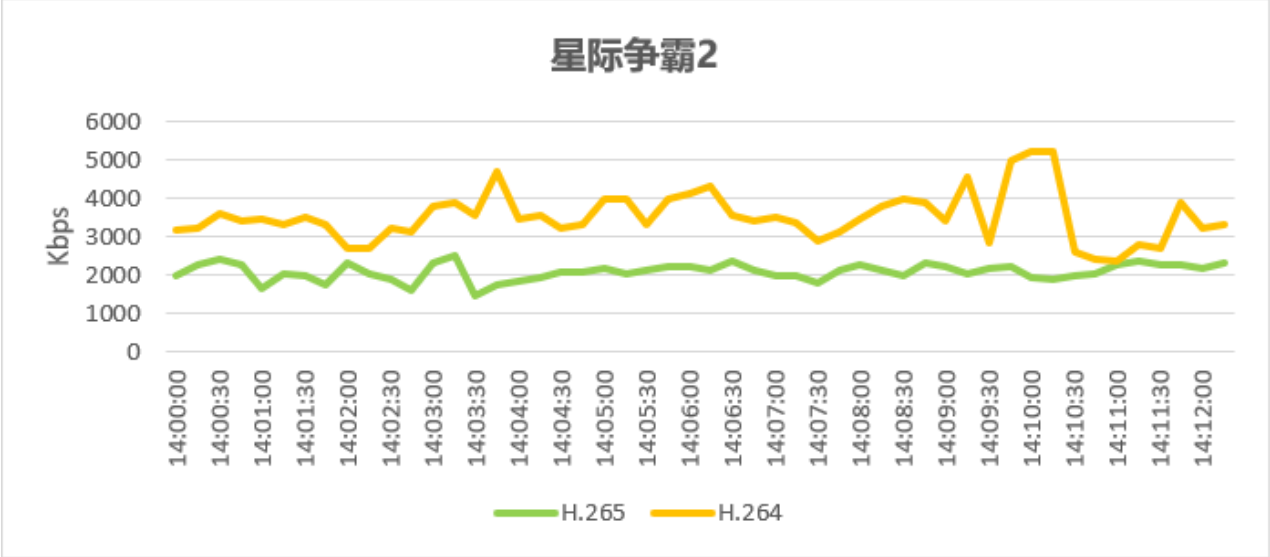


图 36 游戏场景下 H.264 与 H.265 协议带宽峰值对比

通过上述对比数据，浪潮云海 InCloud Access GPU Passthrough 解决方案在互联网环境下，支持绝大多数使用场景。可以提供与本地数据中心部署模式下一致的使用体验；常规配置可以支撑普通办公、大型游戏、高清视频播放三类使用场景的正常使用；协议对比测试结果表明：基于 H.265 优化的 ICAP 协议，在高清视频播放、大型游戏等高带消耗场景下，可节约原有带宽资源的一半，平均带宽占用约为 2Mbps。

适用场景

InCloud Access GPU 云桌面解决方案，可适用于多种高端桌面场景：

1. 支持三维设计领域的各种应用

InCloud Access 支持制造、建筑等相关行业 2D/3D 设计场景，这类场景特点是：零件众多、结构复杂，对 CPU、内存、磁盘 IO、显卡要求很高。对桌面硬件性能，特别是显卡性能，有非常高的要求。InCloud Access 在三维设计上的良好表现，其主要特点如下：

- 支持 AMD MxGPU 、NVIDIA vGPU 及 GPU Passthrough 方案，能有效支持多种场景下多类设计软件；

- 支持主流的 2D/3D 设计软件，包括：AutoCAD、PS、3DMax、Catia、SolidWorks、Revit、Pro/E、UG NX、Creo、Teamcenter、Sketchup 等；
- 采用 SSD 缓存方案使得 GB 级设计文件打开速度更快；
- GPU Passthrough 方案，使得云桌面显卡性能媲美图形工作站，保障用户 3D 图形拖拽、旋转无卡顿；
- 浪潮 GPU 云桌面可广泛适用于工业零部件设计、模具设计、发动机设计、整车设计、建筑设计等图形设计场景。

2. 支持大型游戏及云游戏

云游戏场景需要极高的 GPU 运算能力和高效的流传输协议，对网络带宽、时延、显卡、云桌面整体性能要求很高，传统的 VDI 解决方案无法支持高端云游戏场景。InCloud Access 采用流式传输技术，支持 H.264/H.265 编码、GPU 直通和硬件加速技术，保障了云游戏的高质量、低延迟交付，极大的提升了游戏玩家的体验。同时，由于游戏的计算和渲染全部在云端完成，极大的简化了客户端的配置要求，可以仅仅是 ARM 瘦终端和相关外设（键鼠、游戏手柄）就可以获取良好体验。目前已经适配的游戏包括：英雄联盟、守望先锋、冒险岛、地下城与勇士、魔兽世界、跑跑卡丁车、星际争霸 2、天胖、流放之路、天堂 2、暗黑破坏神 3、剑灵、巨商、永恒之塔、尘埃 4、Apex 英雄、刺客信条奥德赛、只狼、拳皇 14 等。

3. 支持 4K/8K 超高清视频播放

InCloud Access 支持 1080P/2K/4K/8K 高清视频播放，不限定播放器及视频文件格式，如 Media Player/Potplayer/QQ 影音等多种播放器，并且，播放高清视频不依赖终端能力。

4. 支持视频监控应用场景

在安防行业的视频监控场景，目前 InCloud Access 可以兼容大华、海康、宇视、东方网力等视频监控平台，并可以实现单桌面 9 路 1080P 监控视频的播放。InCloud Access 借助 GPU 硬件加速方案或 GPU Passthrough 方案，支持客户视频监控业务的多路视频码流硬解码，降低 CPU 资源消耗，保障前段显示流畅无卡顿。

图 37 9 路 1080P 高清视频监控效果

4.5 InCloud Access 产品价值体现

4.5.1 产品价值

数据上移，信息安全

传统桌面环境下，由于用户数据都保存在本地 PC，因此，内部泄密途径众多，且容易受到各种网络攻击，从而导致数据丢失。桌面云环境下，终端与数据分离，本地终端只是显示设备，无本地存储，所有的桌面数据都是集中存储在企业数据中心，无需担心企业的智力资产泄露。

高效维护，业务连续

传统桌面系统故障率高，据统计，平均每 200 台 PC 机就需要一名专职 IT 人员进行管理维护，且每台 PC 维护流程（故障申报—>安排人员维护—>故障定位—>进行维护）需要 2～4 个小时。桌桌面云不需要前端维护，强大的一键式维护工具让自助维护更加方便，提高了企业运营效率。使用桌面云后，每位 IT 人员可管理超过 2000 台虚拟桌面，维护效率提高 10 倍以上。 平均故障恢复时间缩减至 3

分钟，有效保障业务连续性。

应用上移，业务可靠

传统桌面环境下，所有的业务和应用都在本地 PC 上进行处理，稳定性仅99.5%，年宕机时间约 21 个小时。在桌面云中，所有的业务和应用都在数据中心进行处理，强大的机房保障系统能确保全局业务年度平均可用度达 99.9%，充分保障业务的连续性。各类应用的稳定运行，有效降低了办公环境的管理维护成本。

无缝切换，移动办公

传统桌面环境下，用户只能通过单一的专用设备访问其个性化桌面，这极大的限制了用户办公地灵活性。 采用桌面云，由于数据和桌面都集中运行和保存在数据中心，用户可以不中断应用运行，实现无缝切换办公地点。

降温去噪，绿色办公

节能、无噪的 TC 部署，有效解决密集办公环境的温度和噪音问题。TC 让办公室噪音从 50 分贝降低到 10 分贝，办公环境变得更加安静。TC 和液晶显示器的总功耗大约 20W 左右，终端低能耗可以有效减少降温费用。

资源弹性，复用共享

资源弹性桌面云环境下，所有资源都集中在数据中心，可实现资源的集中管控，弹性调度。 资源的集中共享，提高了资源利用率。传统 PC 的 CPU 平均利用率为 5%～20%，桌面云环境下，云数据中心的 CPU 利用率可控制在 60%左右，整体资源利用率提升。

安装便捷，部署快速

相比于其它桌面云解决方案，InCloud Access 桌面云解决方案具有安装便捷，部署快速的特点。InCloud Access 桌面云解决方案部署模式可以实现把部分虚拟化软件预安装到服务器上。到客户现场后，只需服务器上电，进行桌面云软件的向导式安装，接通网络并进行相关业务配置即可进行业务发放，大幅度提高了部署效率。

4.5.2 应用场景

随着服务器虚拟化技术、桌面虚拟化技术、显卡虚拟化技术的发展，桌面云已经可以覆盖现有 PC 的应用场景，InCloud Access 桌面云秉承“all in on”的理念，

采用同一套桌面云 InCloud Access 产品覆盖用户多样化使用场景，典型场景列举如下：

GPU 桌面---高端（制造）图形设计场景

常用软件： AUTOCAD、CATIA、Pro/E、CREO、TEAMCENTER 等

场景特点：设计产品结构复杂，外形要求严格、零件形状各异、内部结构复杂、组件数量巨大等；三维模型文件由多个不同类属性文件组成，结构复杂、数据量大，数据从硬盘调到内存，模型实时还原，通过 CPU 和显卡，展现近似实物的三维模型，对 CPU 和 GPU 计算、硬盘 IO 要求较高。

GPU 桌面---高端（建筑）图形设计场景

常用软件： AUTOCAD、REVIT

场景特点：三维模型以及文件结构复杂、数据量大，对 CPU、GPU 计算、硬盘 IO 要求较高；

GPU 桌面---中端（机械）图形设计场景

常用软件： AUTOCAD、SolidWorks、UG

场景特点：需要高性能的数值计算能力和图形功能，需要较大容量的内存和磁盘。

普通桌面---网络隔离场景

常用软件： 日常办公软件、图形设计软件、信息敏感类应用等

场景特点：分成物理网络隔离，即内外网各部署一套系统，终端与系统侧相互隔离；逻辑网络隔离，即内外网无需严格物理隔离，但需要保证无数据交互。

普通桌面---政企办公场景

常用软件：办公软件、企业业务软件

场景特点：政府、企业、事业单位、学校办公等日常办公场景，关注便捷运维管理、企业数据安全。

普通桌面---分支机构场景

常用软件：办公软件、企业业务软件

场景特点：零售企业、4S 店等规模小、数量多的分支机构日常办公场景，关注便捷运维管理、企业数据安全。

普通桌面---医疗卫生场景

常用软件： PACS（医学影像信息系统）、CIS（临床信息系统）、HIS（医院信息系统）、RIS（放射学信息系统）、LIS（实验室信息系统）等

场景特点：医疗系统系统建设比较完善，办公电脑通过 C/S 方式访问业务，数据集中在服务端，本地有少量个人数据；外设种类、数量众多；更加关注系统运行的稳定性和连续性。

普通桌面---公安监控场景

常用软件： 东方网力/海康/大华/宇视等视频监控系统

场景特点：信息安全高要求，多网物理隔离，兼容已建安全防护软件；单桌面通常承载多路（如 9 路）监控视频；部分监控系统需要 GPU 硬件解码能力支持。

普通桌面---呼叫中心场景

常用软件： 呼叫中心软件、avaya 语音系统

场景特点：呼叫中心语音系统分带内、带外两种，其中带内语音对桌面云要求高，桌面没有或有少量个人数据，业务数据集中在业务系统。

普通桌面---职教教学场景

常用软件：教学软件、办公软件

场景特点：承载教学软件，对系统稳定性、连续性有较高要求，对系统便捷运维管理有较高要求。