

ALIBABA CLOUD

阿里云

专有云企业版

无影
产品简介

产品版本：V3.14.0

文档版本：20210618

 阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.什么是阿里云无影	06
2.阿里云无影产品优势	08
3.产品功能	09
3.1. 零终端	09
3.1.1. 什么是零终端	09
3.1.2. 零终端的优势	10
3.1.3. 零终端的功能	11
3.1.4. 外设支持	12
3.1.5. 零终端规格	14
3.1.5.1. 零终端基础版规格	14
3.1.5.2. 零终端C-key规格	15
3.2. ASP协议	16
3.2.1. 什么是ASP协议	16
3.2.2. ASP协议的特性	17
3.2.3. ASP协议的性能	18
3.3. 轻空间	19
3.3.1. 什么是轻空间	19
3.3.2. 轻空间优势	19
3.3.3. 轻空间架构	19
3.3.4. 核心功能	20
3.3.5. 文档协作	22
3.4. 云管控	23
3.4.1. 什么是云管控	23
3.4.2. 云管控优势	24
3.4.3. 云管控架构	24
3.4.4. 核心功能	25

3.5. 云应用	27
3.6. 云桌面	29
3.7. 云资源	32
4.架构介绍	34
4.1. 系统架构	34
4.2. 安全架构	35
5.应用场景	37
6.基本概念	38

1.什么是阿里云无影

本文为您介绍阿里云无影产品的定义以及构成。

阿里云无影是一款面向数字经济时代的生产力工具，基于流式传输服务和容器化架构，可实现随时随地云上办公、海量算力触手可得、海量应用一网打尽，依托阿里云专有云打造云管端一体化安全防护体系，全面保障企业业务和数据安全，拥有超越PC的便捷、流畅、安全、高效体验。

概述

阿里云无影为您提供长在云上的“超级电脑”，将“云电脑”的主机、CPU、硬盘等硬件设施都集中在云端的数据中心。只需要将超轻量级终端连接到电视机、屏幕等主流显示设备上，就可以进入专属云电脑，访问各种应用和文件。

无影产品所属“云电脑”不但具备传统电脑的所有能力，而且能够完成传统电脑做不到的工作，例如动画渲染、制图设计、软件研发等对计算性能要求非常高的工作场景。

说明

主要服务于企业办公市场，在办公网络环境下，使用体验非常流畅。

结构

阿里云无影由如下几个部分构成：



- 终端：支持超轻量零终端，同时提供SDK用于生态扩展。
- 零终端：阿里云自主研发超轻量级终端设备，支持自主协议，主要用于连接用户终端外设和服务接入。

- 外设与企业IT设施：支持主流外设与IT环境。
- 轻空间：提供给终端办公用户的一个智能办公空间。
- 云流自适应流媒体技术：就是自主研发的ASP协议，是阿里云无影产品中自主研发的面向应用流的新型端云协同协议，用于终端与云端交互。
- 云应用：部署在云平台的各操作系统平台的应用。
- 云管控：面向客户运维管理人员一站式控制台，可对云桌面、云资源及零终端进行安全有效的管控。
- 专有云平台：基于飞天技术的阿里云专有云。
- 云安全：依托阿里云强大安全能力打造的端到端安全。

2. 阿里云无影产品优势

以阿里云计算服务为依托，阿里巴巴集团在办公领域沉淀服务为基础，为政府及企业级用户完成云上办公的办公体验升级。阿里云无影产品服务价值体现在如下几个方面。

自主研发

- 自主研发终端方案
- 自主研发可控流化协议
- 自主研发云端方案

产品安全

- 终端安全：终端采用自研系统，避免病毒和木马侵害。
- 外设安全：终端外设端口的使用支持灵活管控。
- 数据安全：用户数据均在云端，终端上不留业务数据，保证数据不泄露、不丢失。
- 行为安全：通过云管控平台全链路监控数据流转，保证用户行为可追溯。
- 环境安全：采用阿里云专有云安全基础设施，支持配置安全组规则、云盾防DDOS系统、多用户隔离、防密码破解等安全措施。

高效运维

- 集中式管理：软件、桌面、云资源、用户、终端和外设在管控平台中心化部署、发放和授权，大幅提升管理设备的效率。
- 资源利用高：充沛的算力资源，根据应用即时按需调度，轻松满足日常办公或大型软件研发等不同需求。
- 迁移便捷：用户所有数据保存到云端，终端上无数据，支持随时迁移。
- 平台易使用：云管控运维工具高效、可靠、简单、易用，无学习成本。
- 容灾备份：环境和数据具备多份副本，单份损坏可在短时间内快速恢复。
- 云主机简化运维：软件升级、系统打补丁都在云上完成，配合分时、迁移设置，对用户无感。主机数据与计算分离，若主机运维操作故障，无需担心主机数据丢失。

便捷接入与云平台办公高效协同

- 灵活接入：零终端接入方式，满足固定场所或移动场所办公的需求。
- 办公新体验：轻空间将场景所需应用集中编排，即点即用，带来创新办公体验。
- 卡片终端随身携带：超轻量卡片式终端，可以随身携带。通过高速网络接入服务，支持随时随地高效办公。
- 工具丰富：支持云桌面、企业OA、钉钉等多种办公工具。

云端一体方案降低成本

- 降低终端成本：零终端超低成本，硬件简单，超过5年的超长使用周期。
- 减少运维投入：大幅减少运维人力支出及安全管控方案采购需求。

3. 产品功能

3.1. 零终端

3.1.1. 什么是零终端

通过本文您可以了解零终端的概念以及作用机制。

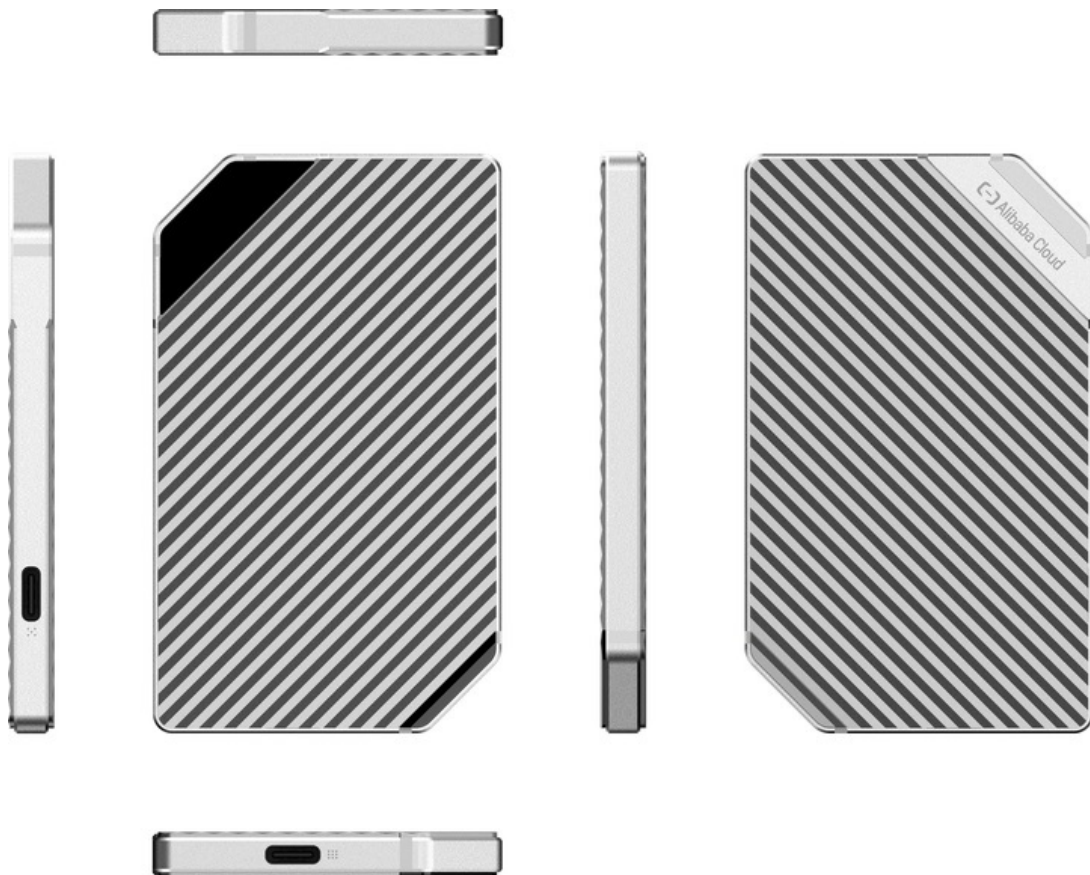
零终端是阿里云无影产品中的用户使用的超轻量级终端设备。零终端基于阿里云自研的Streaming Docker方案及自适应流化协议，将从网络接收到的加密数据流，在本地进行解密及解码，并通过零终端连接的显示设备将图像输出给用户。

由于零终端仅负责接收并处理网络下发的视频数据，使得零终端的安全性、稳定性以及在降低方案成本上相比传统PC有大幅提升。

零终端基础版



零终端C-key



3.1.2. 零终端的优势

本文从零终端的使用、运维、管控、安全以及成本五个方面为您展现其优势。

使用简单

- 管理员云端一键配置即可使用。
- 支持外设重定向。

运维简单

- 设备固件问题可通过硬件“reset”按键一键修复。
- 硬件简单，稳定性高。

管理简单

- 云端管控策略可定制。
- 支持对终端外设类型进行灵活管控。

安全

- 自研系统封闭，无病毒木马威胁。
- 系统升级，保障设备系统始终运行在最新的版本并及时修复各种安全隐患。

低成本

超低成本接入设备。

3.1.3. 零终端的功能

本文以图表的方式为您展示零终端基础版和零终端C-key产品功能。

零终端基础版



功能	描述
网络支持	支持有线网络和无线网络接入。
蓝牙支持	支持蓝牙输入设备和蓝牙音频设备。
外设支持	支持USB存储设备、USB打印机等通用外设。
显示	支持1080P 60FPS显示输出。
ASP客户端	负责流化视频的解码及客户端操作的重定向。
设备管控	支持外设管控、设备禁用。
系统升级	支持通过网络进行终端的固件升级。
恢复出厂	支持一键恢复出厂状态。

零终端C-key



功能	描述
网络支持	支持无线网络接入。
蓝牙支持	支持蓝牙输入设备和蓝牙音频设备。
外设支持	支持USB Type-C存储设备等通用外设。
显示	支持1080P 60FPS显示输出。
ASP客户端	负责流化视频的解码及客户端操作的重定向。
设备管控	支持外设管控、设备禁用。
系统升级	支持通过网络进行终端的固件升级。
指纹认证	支持一体式指纹认证，一次按压即可完成开机和认证双重功能。

3.1.4. 外设支持

本文主要展现了终端优良的外设兼容性，外设与VM之间的数据实现高效稳定传输的技术保障。

外设兼容性

目前兼容外设类型：

鼠标	键盘	USB 存储	耳机	MIC	打印机	扫描仪	手写板	Ukey	指纹仪	条码枪
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

② 说明

- Y表示零终端支持该设备。
- N表示零终端不支持该设备。

阿里云无影产品支持市场上绝大部分主流厂家的产品和型号。以下设备型号均已通过测试验证：

- 打印机型号如奔图 P3305DN、得实AR460、HP LaserJet 1020 plus。
- 打印扫描一体机如MP236、奔图PDN7105。
- 扫描仪如Epson V19。
- 主流的移动存储设备。

技术保障

● USB重定向

对主流的外设，在无法支持设备重定向时，采用USB重定向进行设备挂载。目前支持如下外设类型：

- i. U盘
- ii. 打印机
- iii. 扫描仪
- iv. 高拍仪
- v. Camera
- vi. 手写板
- vii. Ukey
- viii. 指纹仪
- ix. 条码枪

② 说明

U盘、打印机和扫描仪外设的优先级若支持设备重定向，则优先使用设备重定向。

● 设备重定向

在Linux容器环境下或在Windows多用户环境下外设通过设备重定向方案，支持多种类型的打印机、扫描仪等外设类型。例如：

- 在linux容器环境下外设使用需求通过设备重定向方案，支持HP、Cannon打印机。
- 在windows多用户环境下的使用需求通过设备重定向方案，支持HP、Cannon打印机。

3.1.5. 零终端规格

通过零终端基础版和零终端C-key的零部件规格，可以了解零终端的基本能力和性能。

3.1.5.1. 零终端基础版规格

本文为您介绍零终端基础版的零部件规格。

零终端基础版的规格

下表详细介绍说明零终端基础版的规格参数。

类别	子类	规格
芯片组	SOC	ARMv8芯片（4核A55）
存储	内存	DDR4 2GB
	存储	eMMC 4GB
网络和无线连接	有线网络	10M、100M、1000M（RJ-45接口带指示灯）
	无线网络	• 802.11 a @2.4/5G • 802.11 b @2.4/5G • 802.11 g @2.4/5G • 802.11 n @2.4/5G • 802.11 ac @2.4/5G
	Wi-Fi天线	MIMO
	蓝牙	5.0
显示	HDMI 2.X母头	1个
	VGA母头	1个
	耳麦接口	3.5mm耳机座

类别 音频	子类	规格
	mic in接口	3.5mm接口
	speaker接口	• 立体声 • 3.5mm立体声接口
USB	USB 2.0	2个
	USB 3.0	2个
电源	电源接口	直径5.5mm
	电源	AC/DC 12V
电子机械按键	1个电源开关	微动开关
	1个reset按键	长按恢复出厂设置
指示灯	电源按键指示灯	橙白双色
	“X”形指示灯	橙色单色
安装方式	无	• 平放/立放桌面 • 显示器背挂防盗扣 • 兼容VESA显示器背挂标准（75mm和100mm）

3.1.5.2. 零终端C-key规格

本文为您介绍零终端C-key的零部件规格。

零终端C-key采用一体式指纹认证，大面积异性玻璃盖板模组方案，一次按压即可完成开机和认证双重功能，从开机到登录仅需5秒。

零终端C-key的规格

下表详细说明零终端C-key的规格参数。

类别	子类	规格
芯片	SOC	1.5GHz（四核）
存储	内存	DDR4 2GB
	存储	64GB
无线连接	无线网络	• 802.11 a • 802.11 b • 802.11 g • 802.11 n • 802.11 ac
	Wi-Fi天线	2.4G/5G MIMO
	蓝牙	5.0
拓展接口	USB	Type-C
显示	DP1.2	Type-C
电源	PD2.0	Type-C

3.2. ASP协议

本文介绍了阿里云无影ASP协议的含义、特性、技术特点和性能。

3.2.1. 什么是ASP协议

通过本文可以了解ASP协议的定义及其作用。

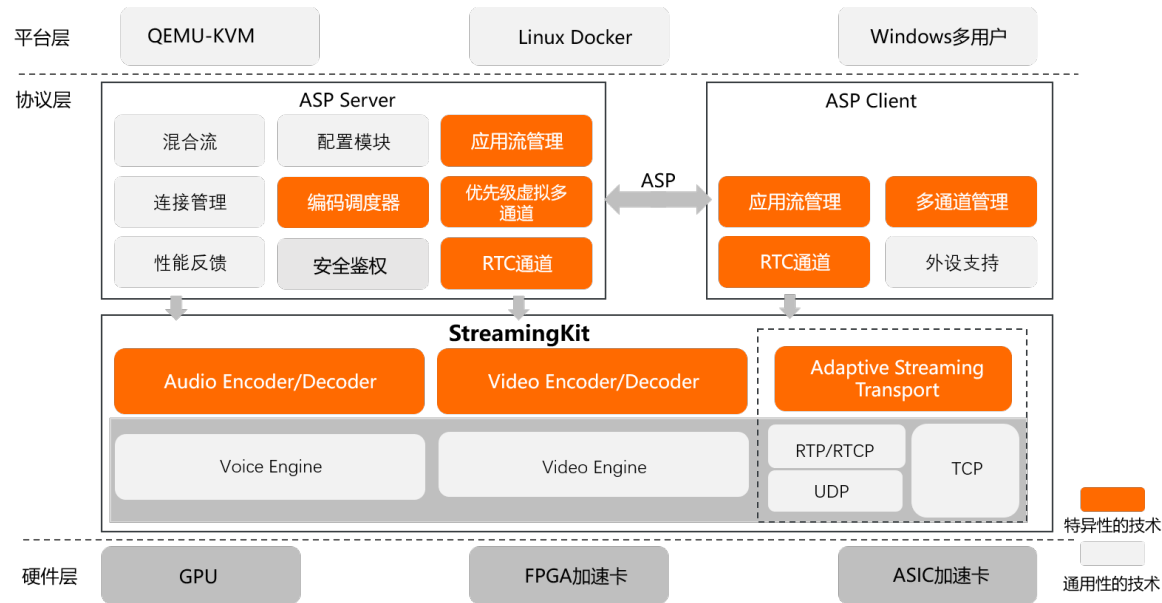
ASP（Adaptive Streaming Protocol）是阿里云自主研发的面向应用流的一种新型端云协同协议，旨在为无影产品提供端云一体的协议支撑，为终端用户提供低时延高画质的实时交互体验。通过ASP协议用户在不同服务器和客户端配置需求中、不同的工作场景下以及不同的网络条件时均能得到最佳的用户体验。

概述

ASP协议在TCP/UDP网络协议上运行，借助于当前高效的编解码技术，将云上的图形化交互界面进行编码，以视频流（Streaming）的方式推送到客户端，客户端执行解码并显示图形化界面。ASP协议通过虚拟传输通道技术，将客户端侧的鼠标、键盘等外设事件重定向到服务端，从而实现端和云的交互事件输入。

基本原理

ASP工作原理图如下所示：



3.2.2. ASP协议的特性

本文主要介绍了ASP协议面向应用流、自适应性、虚拟多通道优先级、I/O外设兼容性以及终端交互多样性的技术优势以及低时延高画质的性能优势。

低时延高画质

ASP协议利用高效的帧间压缩技术(如H.264/HEVC)，将图形化界面以视频流方式推送到客户端，高效的压缩比可以在带宽有限条件下传输质量更高的视频流，既能降低网络传输时延，又能保证画面的高画质。

云上编码器充分利用GPU、FPGA、ASIC等编码专用芯片，既能节省了云上计算资源，又能降低了编码时延，从而提升用户的实时交互体验。

面向应用流

和传统的远程桌面传输协议不同的是，ASP协议是面向应用级的协议，通过云上构建轻量级的应用运行环境，将单个应用的图形化界面，推流传输至客户端。其中云桌面只是ASP协议的一个特例。

以往一台服务器只需支持数十个云桌面同时运行，而对于云应用来说，同样一台服务器可能需要同时支持几百个应用同时运行，对时延、系统I/O、资源调度和图形实时交互方面提出了更高的要求。

- 基于此ASP协议引入编码异构调度技术，对编码资源进行合理分配和调度，支持高并发的编码请求。
- ASP协议还引入端云协同的应用管理机制，实时同步端和云侧的应用状态、窗口状态、层叠区域和交互事件，特别是对多窗口支持，提供和原生应用接近的交互体验。

自适应性

- **场景自适应**
针对不同的场景，如普通办公、视频播放、3D动画等，根据场景的特点自动选择最优的流化路径。
- **网络自适应**

支持TCP/UDP网络协议，针对不同的网络条件，自动检测网络带宽条件，根据自动检测结果，适时调整网络拥塞算法，在弱网情况下尽可能保障用户体验。

● 配置自适应

根据服务器与客户端之间不同的配置，如是否支持GPU、是否支持编码加速卡、终端设备的视频解码能力等，自动选择最优的编解码格式和渲染路径。

虚拟多通道优先级

ASP协议支持多个虚拟通道，比如显示通道、鼠标、键盘、光标、音视频通道、USB外设通道。ASP协议根据当前网络状况、网络上的各种流量优先级，对每个通道占用的带宽、优先级进行统一分配和调度，将数据和控制命令分离，确保流畅的交互体验和关键数据的实时传输。

I/O 外设兼容性

多虚拟通道支持不同类型的外设，能支持多个外设从终端侧接入并支持同时在不同操作系统上工作，带宽分配和优先级上遵循ASP协议的调度策略。

终端交互多样性

面向用户实时交互的场景，支持终端侧接入多种交互方式，如键盘、鼠标、游戏手柄、3D手势等。

3.2.3. ASP协议的性能

本文从多个维度展现ASP协议性能的优越性。

背景信息

VMAF是一种基于机器学习的模型设计能真实反映人对视频质量感知情况的指标。VMAF分值越高代表用户体验越好。

FPS是测量用于保存、显示动态视频的信息数量。每秒钟帧数越多，所显示的动作就会越流畅。

常见媒体的FPS帧率：

- 电影：24FPS
- 电视（PAL）：25FPS
- 电视（NTSC）：30FPS
- CRT显示器：75Hz以上
- 液晶显示器：一般为60Hz

性能指标

指标项	指标值说明
端到端时延	平均时延70ms - 打开文件夹、拖动窗口、点击打开文件等文件相关操作时延在50ms以内 - 页面浏览、滚动页面、刷新等web浏览器操作时延在60ms以内 - 视频播放的操作时延在45ms以内
平均带宽	小于2M

指标项	指标值说明
FPS	60
VMAF	大于95

3.3. 轻空间

3.3.1. 什么是轻空间

本文为您介绍轻空间的基本概念。

轻空间是在云端运行面向办公人员的一个智能办公空间，集成办公协作、文档管理、跨系统应用、云桌面等服务。保障了办公数据在云端的安全且易于管理，便利了应用服务的使用，从而实现高效办公。

3.3.2. 轻空间优势

下表为您列出轻空间与传统PC的对比，更清晰地展现轻空间的优势。

对比项	轻空间	传统PC
功能及体验	- 操作便捷，无需关注系统。 - 支持跨OS的应用使用，无需对应用进行下载安装。 - 依托阿里办公生态优势，集成协作办公服务，提高办公效率。 - 支持多端数据访问和办公协作。	传统OS体验，支持本地应用和本地数据存储。
安全	数据均在云端且进行容灾处理，保证不泄露、不丢失。	数据在本地，不易进行安全数据管理。
运维	资源在云端，运维成本低。	需要进行线下运维，投入成本较高。
可扩展性	使用资源可根据岗位和场景动态扩展。	若资源不足，需要更换设备，并迁移数据。

3.3.3. 轻空间架构

本文为您介绍轻空间的架构。



轻空间由以下6个部分构成：

- 工作台：协作办公的集成桌面模式。
- 应用中心：支持跨系统的云应用访问，受云管控的整体管控。
- 云桌面：支持桌面访问服务。
- 文件中心：所有用户文件数据的存储及管理。
- 空间管理：支持用户自主运维和个性化定义。
- 零终端：支持零终端基础版和零终端C-key的访问。

多端：支持PC软终端、移动端的访问。

3.3.4. 核心功能

本文为您介绍构成轻空间各部分的核心功能。

工作台

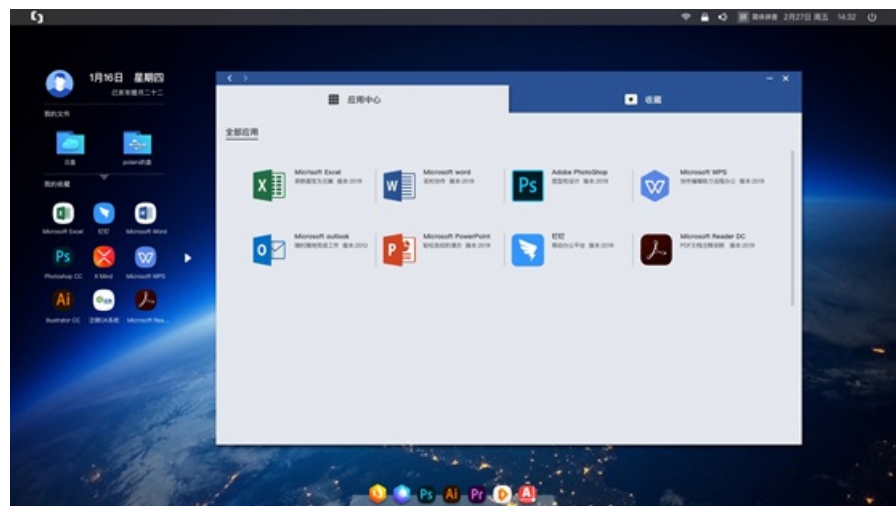
卡片组支持根据场景定义快捷协作办公的功能组合，可以定义多卡片组。

默认卡片组：由天气卡、常用应用卡、个人活动卡、最近文件卡、常用链接卡、语雀卡组成。

- 天气卡：显示当下城市的现实时天气信息。
- 常用应用卡：通过记录应用服务使用的累计时长，显示经常使用的应用。
- 个人活动卡：按照个人活动时间线显示用户操作应用服务的行为活动。
- 最近文件卡：支持用户快速访问最近访问过的文件。
- 常用链接卡：通过文档链接或路径被打开的频率高低，显示经常被打开的链接。
- 语雀卡：是快速记录笔记的入口，可以直接在此窗口进行录入信息。

云应用

云应用是指运行在云端的应用，无需安装直接使用。云应用受云管控平台的管理，可对应用进行控制和升级管理。支持跨系统环境的云应用，同时支持网页应用。



应用中心：展示所有云管控平台中管理的应用，您可以直接使用该应用。也可以添加到收藏或者添加到应用站台中以便快捷使用。应用可以打开云盘中的文件，在应用中创建或编辑的文件也可以直接保存在云盘中。

云桌面

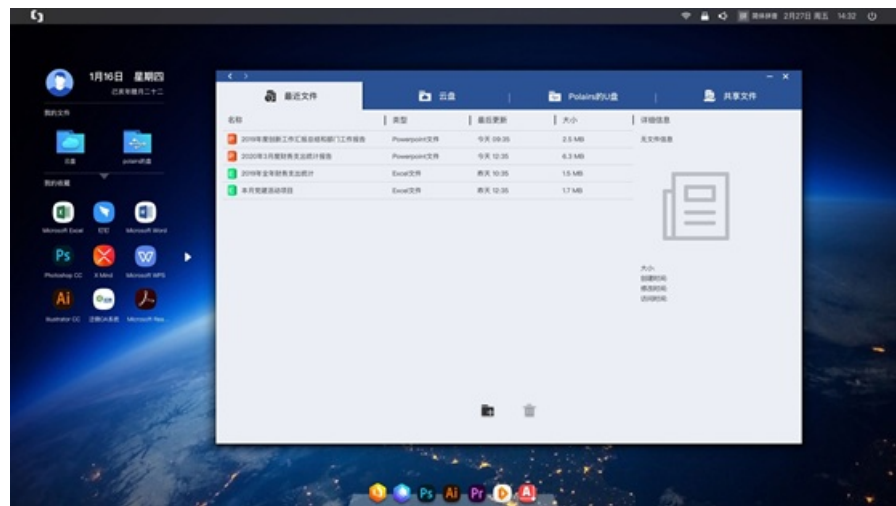
云桌面是指运行在云端的桌面系统，包括UOS桌面和Windows桌面。

云桌面受云管控平台的管理，可以定义您所需要的类型和规格。

云桌面列表：可选择所需的云桌面规格。

文件中心

文件中心对您的文件数据进行统一存储及管理，可管理云盘和外部存储设备。云盘为您分配云端存储空间，数据默认保存在云盘中。

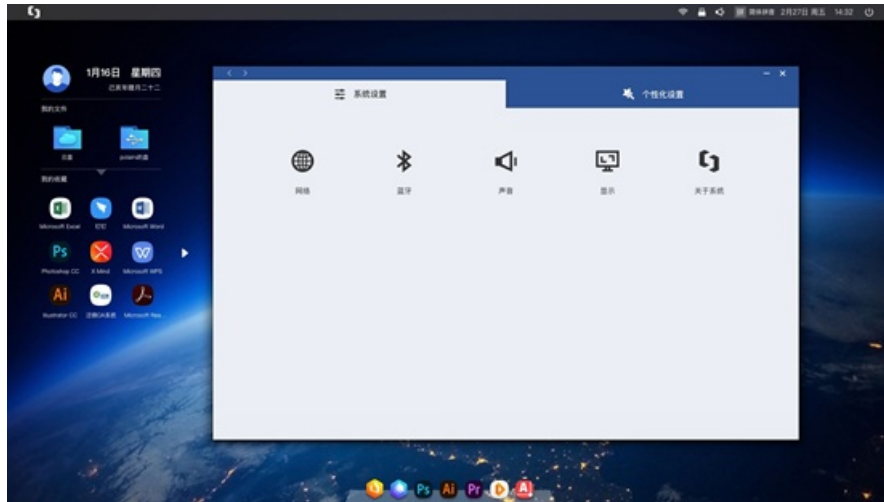


支持如下能力：

- 文件存储：文件存储在云端，且进行容灾备份。
- 文件目录树：基于目录树结构读取文件数据。
- 文件处理：包括文件打开、文件重命名、文件复制、文件删除、移动文件等。
- 文件上传/下载：支持文件从外部存储器上传到云盘中，或从云盘中下载到外部存储器中（是否可下载受云管控平台管控）。

- 最近文件列表：读取最近访问过的文件。
- 动态扩展：在用户空间不足时，支持动态扩展。

空间管理



目前为您提供自有空间的系统设置和个性化设置：

- **系统设置**
针对网络、蓝牙、声音和显示进行设置。
- **个性化设置**
支持对默认输入法和快捷键的设置。

多端

目前支持零终端版本，很快将会为您提供PC软终端版本和移动版本。

3.3.5. 文档协作

本文主要展示了阿里云无影产品中的文档协作新场景的安全与便捷。

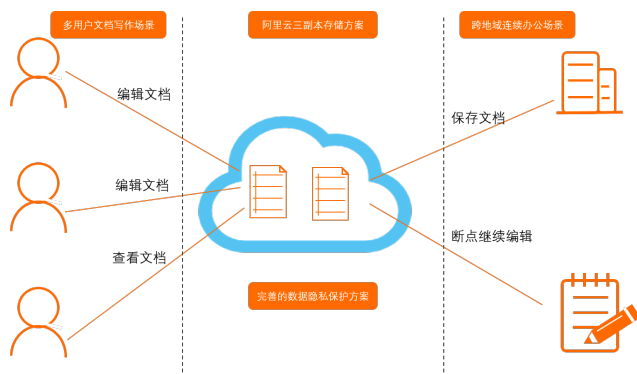
场景简述

多用户协作场景

针对于办公场景中，若存在一份文档内容需要多位成员一起参与完成，需要提供一个多个用户同时打开编辑或查看文档的解决方案。阿里云无影产品打造了云钉一体办公方案，可以复用钉钉自带的多用户同时在线编辑或查看文档的能力。

跨地域连续办公场景

针对于跨场地办公的场景中，若文档责任人在编写文档过程中需要出差，在A地存在未编辑完成的文档，需要在B地支持继续编辑。阿里云无影产品中会根据应用自带的自动保存机制来保存文档，支持断点继续编辑的能力。



核心方案

阿里云三副本存储方案

阿里云提供一个扁平的线性存储空间，在内部会对线性地址进行切片，一个分片称为一个Chunk。对于每一个Chunk，阿里云会复制出三份副本，并将这些副本按照一定的策略存放在集群中的不同节点上，保证数据的可靠性。

对云盘上的数据而言，无论是新增、修改还是删除数据，所有用户层的读写操作都会同步到底层的三份副本上。这种三副本模式，能够保障您数据的可靠性和一致性。详细内容请参考[云服务器 ECS > 块存储 > 块存储介绍 > 云盘三副本技术](#)。

完善的数据隐私保护方案

- 读写稳定

在同一可用区中，您的业务数据以多副本的形式分布存储在块存储集群中，保证读写过程中的数据稳定性，实现了99.9999999%的数据可靠性保证。

- 数据擦除机制

您删除的数据不会被其他用户通过任何途径访问，存储系统中已删除的数据一定会被完全擦除。主要通过以下机制保证数据擦除的完整性：

- 云盘底层基于顺序追加写来实现，充分了利用物理盘顺序写的高带宽、低时延特性。基于追加写的特性，一切删除或者覆盖写操作形成的物理磁盘上的遗留数据，会从底层物理磁盘上强制永久删除。
- 当释放云盘时，存储系统立即销毁元数据，与此同时该云盘对应的物理存储空间会被回收，以确保无法继续访问数据。

- 数据加密

对于数据敏感型应用，建议您加密存储设备。用户云盘加密采用行业标准的AES-256算法，利用密钥加密云盘以及云盘快照。从云应用或云桌面实例传输到云盘的数据会被自动加密，并在读取数据时自动解密。详细内容可以参考[云服务器 ECS > 块存储 > 块存储介绍 > 块存储概述](#)。

3.4. 云管控

3.4.1. 什么是云管控

本文为您介绍云管控的概念和作用。

云管控是为阿里云无影产品管理运维人员提供的一站式控制台。是无影产品的“中枢管理站”，可实现云应用发放管理、云桌面管理、用户管理、相关云资源管理、终端管理、系统运维管理、策略管理等简单、高效的管理运维。



3.4.2. 云管控优势

本文为您介绍云管控平台产品三大核心优势：简单、高效、低成本。

简单

- 对管理运维涉及的云桌面、云应用、资源、用户、终端、系统、策略进行一站式统一入口管控。
- 对云桌面管理和云应用管理等操作进行封装简化和可视化，使得无影运维管控更简单。

高效

在无影的业务场景中，不同业务在不同时间段对于并发用户规模以及用户使用资源要求不同，例如，视频图像类、3D设计软件类、普通Office办公等。云管控可以实现自动化弹性调度。

- 弹性扩张：自动添加资源。
- 弹性收缩：自动释放资源。
- 弹性自愈：资源健康状态自诊断，自动释放不健康的资源并创建新的资源。

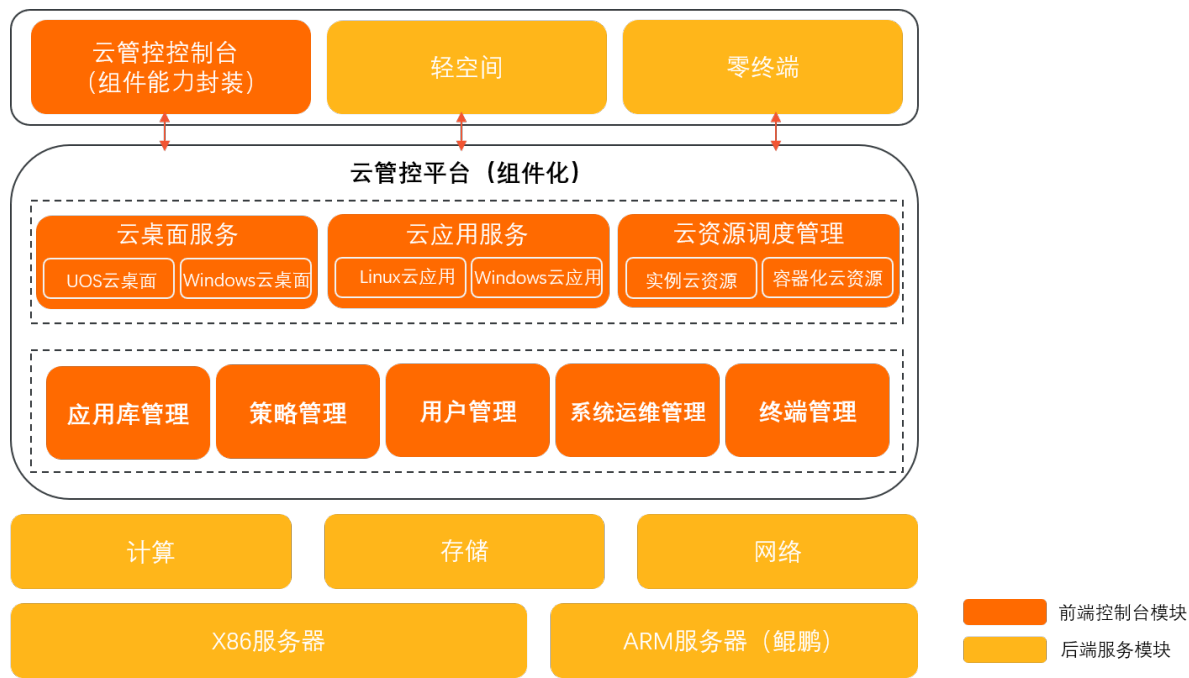
低成本

- Linux云应用支持以应用为单位进行容器化，并对用户进行分配。
- Windows云应用支持应用组维度进行实例虚拟化，并支持多用户模式，最大程度上提高资源利用率。

3.4.3. 云管控架构

本文为您介绍云管控的架构。

云管控产品架构包含后端服务模块和前端控制台模块。云管控服务和基础云设施、虚拟机或容器、终端实现交互管控，发挥中枢管理作用。云管控平台支持组件化统一管控，根据您的业务需求，提供不同的组件化组合。



3.4.4. 核心功能

本文为您介绍云管控服务的主要功能。

云应用管理

实现终端轻空间云应用中心的应用发放和管理。

- 云应用发放：提供默认的应用库，支持您根据业务需求，自定义集成应用进行发放，包含创建应用组或单应用、授权用户、网络授权和发布。

说明

在应用组详情页面中支持应用组实例镜像的停止与更新操作。

- 云应用管理：
 - Windows云应用：提供对云应用的各项管理操作，包括创建、删除应用组，修改应用组用户授权、网络权限，应用组内新增、删除、更新应用，切换镜像等。
 - Linux云应用：提供对Linux云应用的各项管理操作，包括上架、下架应用，修改应用用户授权、批量授权等。

云桌面管理

实现终端云桌面的发放和管理，支持不同平台、不同规格、不同类型的云桌面。

- 云桌面发放：提供创建桌面组、授权用户和发布桌面组。

说明

在桌面组详情页面中支持桌面组实例镜像的停止与更新操作。

- 云桌面管理：提供对云桌面的各项管理操作，包括创建、删除桌面组，修改桌面组规格、用户授权、网络权限，桌面组内新增、删除、更新桌面，镜像切换，关闭、启动、重启桌面，桌面备份和恢复等。

云资源管理

提供无影业务相关的各项云资源的一站式管理，包含镜像、虚拟机、容器、存储、网络资源等。

- 镜像：提供公共镜像和自定义镜像功能，支持创建与删除自定义镜像、查询镜像相关实例。
- 虚拟机：提供针对无影业务涉及虚拟机资源的管理操作，包括实例创建、升降配、编辑、备份、启动、关闭、重启、删除和回收站，支持修改单虚拟机磁盘存储、网络权限等。
- 容器：提供针对无影业务涉及Docker容器资源的管理操作，包括创建实例、创建模板，编辑实例、编辑模板，备份实例，支持修改Linux应用存储卷的存储等。
- 存储：包含虚拟机系统盘、数据盘、云盘和存储卷的管理，其中云盘的数量和容量支持修改，存储卷的容量也支持修改。
- 网络权限：支持配置内外网不同网络权限和安全组，通过不同的安全组规则管控虚拟机网络的出入权限。

用户管理

提供无影业务的用户管理，包含用户组织管理、用户外设管控。

- 用户组织管理：支持用户组织、用户组、用户管理功能。
- 用户外设管控：以用户为单位，管控用户的外设权限。

说明

支持外设包含但不限于：USB输入设备、USB存储设备、打印机、扫描仪、蓝牙等。

终端管理

提供无影业务的终端管理，包含终端管控、终端状态统计。

- 终端管控：包含不仅限于某些设备的禁用设置。
- 终端状态统计：支持按照设备SN和设备型号查询对应的设备状态和信息，包括联网状态、规格、最后登录用户、激活时间、终端IP。

系统运维管理

包含无影业务涉及的云资源、云桌面、云应用的各项运维。无影产品涉及的资源的性能监控，云桌面、云应用的异常告警等。

- 云资源运维：提供虚拟机性能、存储资源监控分析和异常告警，集成在Apsara Uni-manager运营控制台，由Apsara Uni-manager运营控制台统一提供。

说明

物理机（集群、主机等）的运维监控，集成在Apsara Uni-manager运维控制台，由Apsara Uni-manager运维控制台统一提供。

- 云桌面异常监控告警：支持对云桌面异常连接时长的告警，监控用户在UOS上安装的应用，告警规则自定义配置。
- 云应用异常监控告警：支持对云应用异常连接时长的告警，告警规则自定义配置。

- 管理员操作日志：集成在Apsara Uni-manager运营控制台，由Apsara Uni-manager运营控制台统一提供，支持安全审计员角色查询和日志导出。
- 用户行为日志：支持终端用户行为日志的查询和导出。

应用库管理

支持云桌面服务和云应用服务涉及的应用的管理维护，包含：应用上传、更新、删除。

策略管理

提供显示策略、定时策略、剪切板策略配置。

3.5. 云应用

本文主要介绍阿里云无影产品中基于应用虚拟化实现Linux云应用和Windows云应用的发放与管控。

背景信息

传统的云桌面，将个人PC主机或者操作系统的桌面在云端虚拟化。阿里云无影产品是以应用为粒度进行虚拟化，直接提供应用给用户使用。

- 基于容器虚拟化，实现Linux云应用的发放与管控。
- 基于VM虚拟化，实现Windows云应用的发放与管控，并且Windows云应用支持共享模式。

应用虚拟化

应用虚拟化是将应用程序与操作系统解耦合，为应用程序提供了一个虚拟的运行环境。在这个环境中，不仅包括应用程序的可执行文件，还包括它所需要的运行时环境。

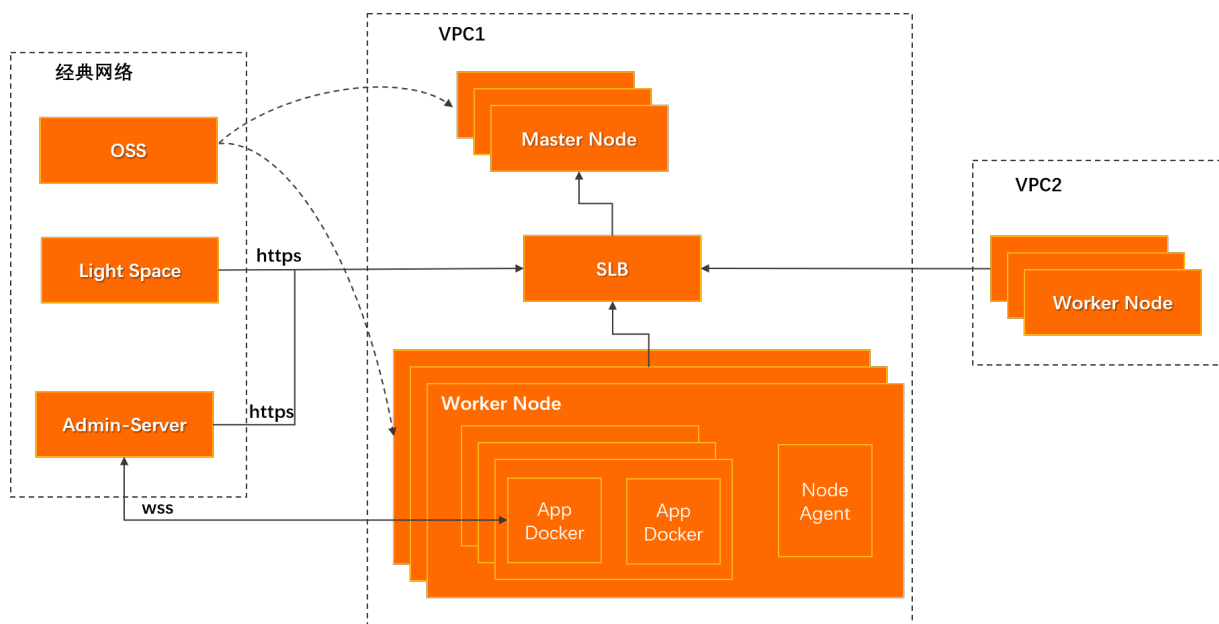
应用虚拟化是把应用对低层的系统和硬件的依赖抽象出来，以解决应用版本不兼容的问题。

容器虚拟化

解决方案

容器应用实现架构图，如下图所示。

核心要点说明



• Admin-Server

提供容器服务的管控能力，将业务模型转换为技术模型，为容器服务输入模型参数，主要职责有容器镜像管理、应用管理、集群管理、容器实例管理、控制器管理等。

• Lightspace

容器服务使用者，提供对零终端的接口，基于Admin-Server的模型从容器服务中获取相应的实例分发给零终端。

• OSS

容器服务本身部署带来的文件托管服务。

• Master Node

容器服务管控节点，在不同ECS节点上部署来做到高可用。以阿里云SLB提供API-server的负载均衡能力，K8s本身选举机制保障Scheduler的高可用。

- 当前版本只支持ECS作为Worker Node，在创建节点实例时，下发初始化脚本，安装部署K8s环境并加入集群。

实现技术

• 调度策略

◦ 默认调度策略

- 节点预选：磁盘、内存、存储卷是否支持挂载等条件是否满足
- 节点评分：基于资源空闲情况、资源分布情况等条件综合评分，选取评分最高者（资源总量-（已分配+当前request））/资源总量

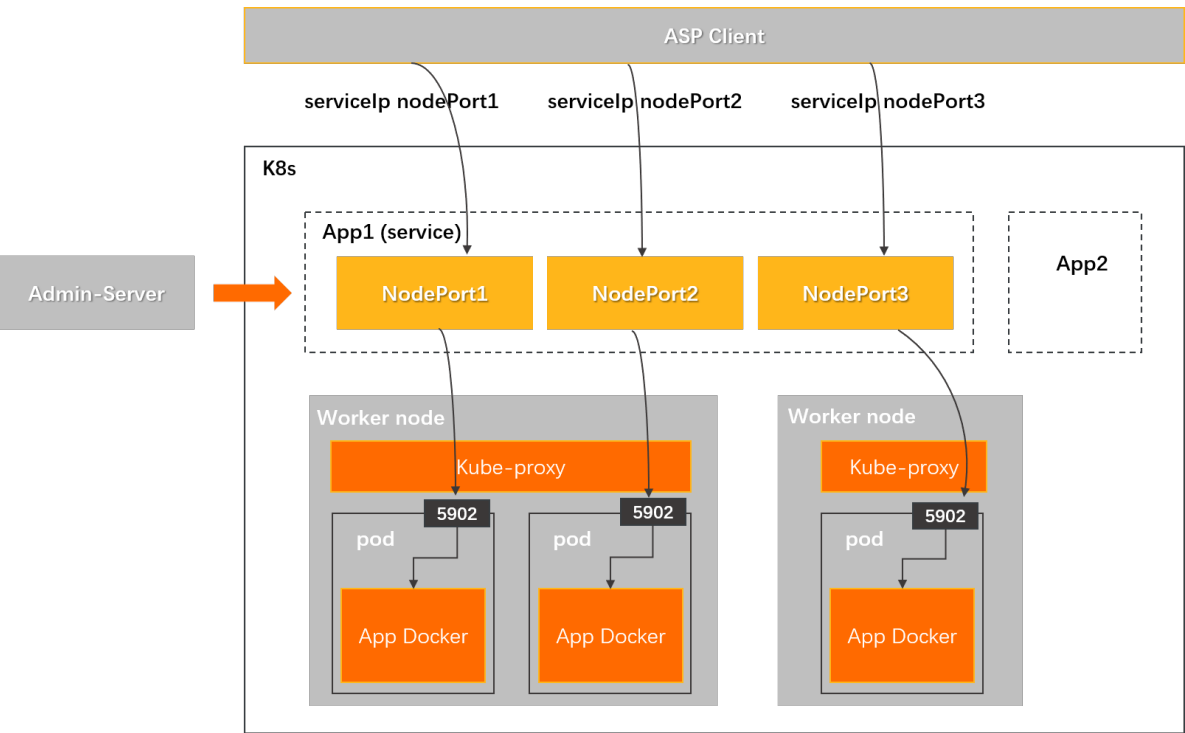
◦ 节点亲和性策略

预先将所有工作节点规划为多个分组，并配置好节点与应用的分配策略，在创建容器阶段通过NodeSelector机制，使能节点亲和性策略。

• 容器编排

采用statefulset控制器，通过原生机制保障容器高可用，在容器异常退出后会自动恢复Pod名称、网络、存储等。

● 网络



● 存储卷

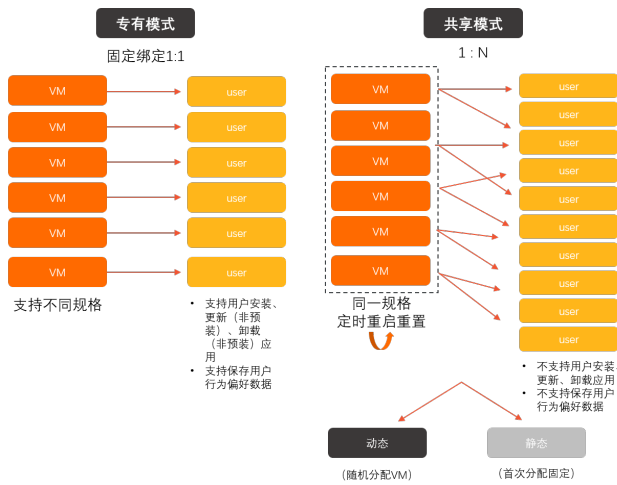
存储类型OSS

天然支持高可用，有完善的控件、权限验证机制。

3.6. 云桌面

本文主要介绍说明了阿里云无影产品中云桌面实现发放、管控的原理与机制。

基本概念



单用户：一个VM虚拟机同一时刻只能供一个用户使用。

多用户：一个VM虚拟机同一时刻可以供多个用户共享同时使用。

专有模式：一个VM虚拟机和用户绑定锁定，无论用户是否连接，虚拟机只能给该用户使用。

共享模式：VM虚拟机和用户之间无固定绑定关系，同一时刻一个虚拟机给多个用户同时使用，VM虚拟机支持定时重启重置，VM虚拟机可再随机分配给其他用户使用。

场景	专有模式	共享模式
应用场景	• VIP用户 • 研发类型桌面	• 客服 • 办事大厅 • 呼叫中心等
VM: 用户	1 : 1	1 : N
VM和用户绑定关系	绑定	动态不绑定

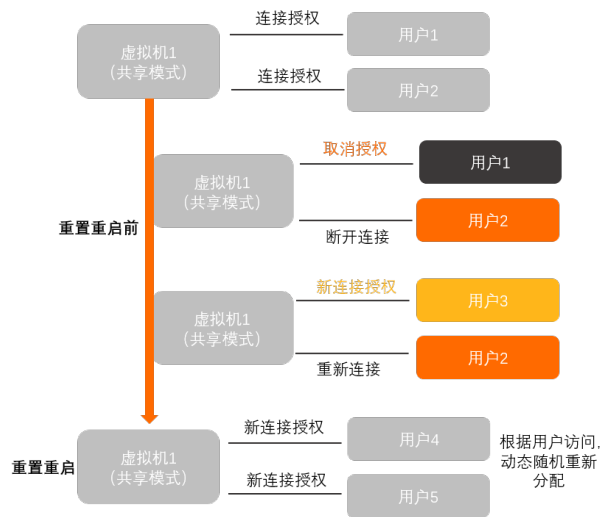
核心原理与机制

• VM多用户重启重置分配机制

共享模式存在重启重置机制。

- 重启重置后，VM会根据用户的访问，动态重新随机分配。

- 重启重置前，存在如下三种情况：
 - 用户一直没有断开连接：用户一直获得授权。
 - 用户断开连接后，但未取消授权，又重新连接：分配给用户之前的VM，保证使用体验的延续性（下图示意用户2）。
 - 用户取消授权：资源释放，可分配给其他用户建立授权（下图示意用户1、用户3）。



根据定时策略或管理员手动发起重启，同一桌面组下的VM的状态可能不同步，部分重启完成，部分重启中。此时如果端上有用户来访问，重启机制如下：

- a. 优先给出同一桌面组下可用的VM。
- b. 如果都不可用，返回对应的状态结果，端上给出提示。

● 用户安装、下载、卸载应用权限要求

场景	专有模式	共享模式
办公用户应用/应用插件安装	支持	不支持
办公用户应用更新（应用包、应用内推送）	预装应用，不支持 非预装应用，支持	均不支持
办公用户应用卸载（预装、非预装）	预装应用，不支持 非预装应用，支持	均不支持

② 说明

专有模式下不支持用户更新、卸载（预装应用）的原因：

- 降低管理员对应用组或桌面组内应用管理的复杂度。
- 避免引起应用版权纠纷。

● 用户数据保存机制

场景	专有模式	共享模式
用户使用生成的文件数据	单独网盘绑定用户，不影响	单独网盘绑定用户，不影响
用户系统应用设置数据、应用安装数据	- 保存 - 快照用于异常恢复	- 重启重置，不保存 - 不需要快照处理异常恢复
VM重启重置机制	不提供	VM重启后重置初始化 仅后台配置定时重启，不支持用户重启

- 用户数据
 - 文档类数据。
 - 应用内行为设置数据，如输入法皮肤设置等。
 - 应用内记录数据，如聊天记录，文件记录，浏览器收藏等。
- 共享模式重启重置对应的数据回收机制
 - 和用户分配机制关联。
 - 重启重置后，用户数据输出后不保存。
 - 重启重置前，存在如下三种情况：
 - 用户一直没有断开连接
用户一直获得授权，数据保存。
 - 用户断开连接后，但未取消授权，又重新连接
分配给用户之前的VM，保证使用体验的延续性，数据保存。
 - 用户取消授权
资源释放，该用户数据在重启前保存，重启后初始化。可分配给其他用户建立授权，建立新的用户目录。
- VM多用户最大连接数支持管控可配
 - 多用户的VM配置先以ECS实例最大数配置。
 - VM最大连接数在创建桌面组发布时可配置。

3.7. 云资源

本文主要介绍了无影产品对于云资源的弹性使用和应用级迁移与调度。

资源弹性使用

传统的云端虚拟机，资源都是提前分配且独占的，即使虚拟机没有在使用时，资源仍然占用不会释放，造成资源浪费。通过资源弹性使用的方式分配给应用虚拟化环境的资源，都属于共享的资源。

- 办公桌面可以根据用户不同的工作场景选用不同模式。
- 应用可以根据用户需要，动态使用更多的资源。当用户操作减少负载降低时，可以实时减少资源的占用。

阿里云无影产品根据用户可能使用客服、办事大厅或呼叫中心等对计算资源要求不高的业务，给出多用户共享桌面的方案。在使用共享桌面进行办公时，在同一时刻一个虚拟机资源可以给多个用户同时使用。从而减少虚拟机资源的占用，将更多的计算资源给专有桌面的用户使用，实现虚拟机粒度的资源弹性使用。

阿里云无影产品基于容器化技术，可以以0.1vcpu为粒度对资源进行分配。云应用资源调整可以在毫秒级完成，可以支撑应用平滑运行，用户不会感受到任何差异。被释放的云资源可以其他云上业务使用。

应用级迁移与调度

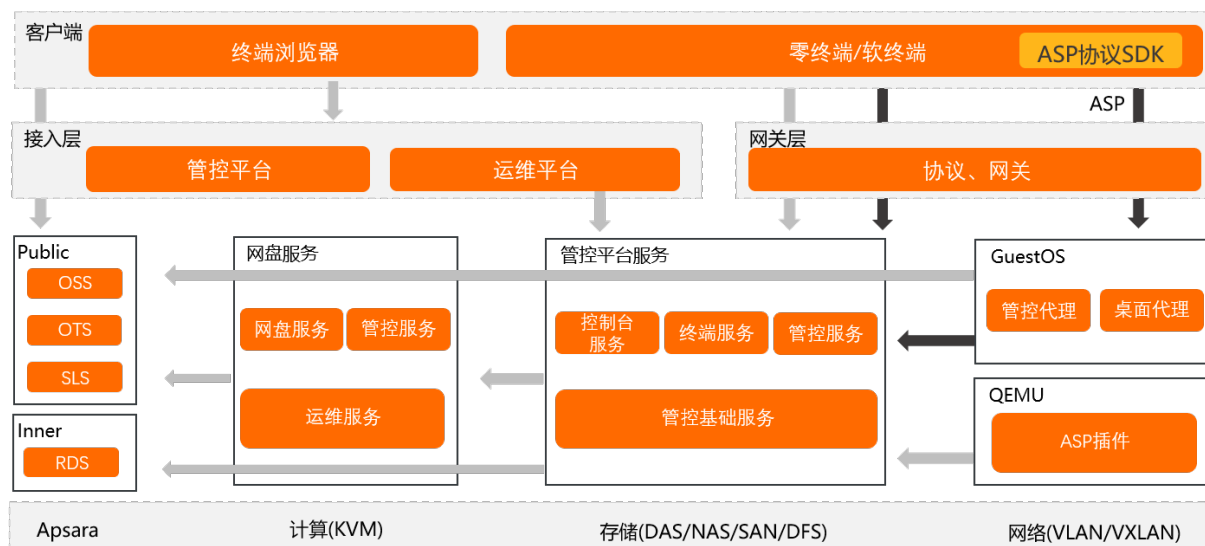
传统的云端虚拟机，很难做到热迁移，或者会将虚拟主机操作系统处于一个暂停的状态才能做迁移。在云端应用程序，相对于虚拟主机和操作系统而言，体量更小，粒度更细，热迁移的难度大大减低。

云应用进行热迁移时，应用的运行状态不需要任何改变，应用的临时数据也不会丢失。

4.架构介绍

4.1. 系统架构

本文为您介绍阿里云无影产品的系统架构。



核心模块

- **客户端**
超轻量零终端，支持多个软终端的轻空间服务接入，同时提供ASP协议SDK用于生态扩展。
- **接入层**
 - 管控平台：交付给用户的统一管控平台。
 - 运维平台：交付给系统运维使用的统一运维平台。
- **网关层**
云桌面接入和各种系统服务的统一网关代理，用于隔离内外网，确保安全通讯。
- **云端**
 - **网盘服务**
为客户端、轻空间、Guest OS内提供虚拟网盘服务。
 - **管控平台服务**
提供标准化的功能接口，完成云桌面虚拟机管理运维功能。
 - **Guest OS**
 - 管控代理：云桌面管理服务，软件应用分发管理。
 - 桌面代理：桌面心跳检测、配置、管理、热升级、日志收集、审计等功能。
 - **QEMU**
ASP插件：云桌面连接入口。负责协议接入、授权认证、桌面信息串流等服务。

网络架构

云桌面核心协议采用自研ASP协议，协议通过Streaming流到客户端。

阿里云无影网络组成：

- 客户侧私有网络
- Guest OS虚拟网络
- 无影产品管理网络
- 无影产品运维网络

4.2. 安全架构

本文从全面的安全态势感知展现阿里云无影产品端管云一体的安全保障方案。

方案简述

通过对用户行为日志、文件或进程等实体行为日志的数据分析，发现识别安全威胁事件，并发出告警或自动处理，同时进行可视化展示，帮助管理侧了解全网安全状态、对风险的及时处置。以端到端的系统安全为根基，防控内外部的风险，保护流转在无影环境中的数据资产。结合阿里云安全容器方案，提高多租户环境安全等级。



核心模块

- **终端安全**
 - 终端安全：通过安全技术，提升终端安全能力。
 - 漏洞补丁OTA升级：零终端支持固件升级，系统出现漏洞时可通过强制升级方式更新固件。
 - 零终端禁止用户访问本地存储，禁止用户在本地安装软件，防止病毒注入。
- **接入安全**
 - 多重用户身份认证：
 - 登录轻空间以帐号密码方式进行身份验证。
 - 通过零终端C-Key指纹认证支持免密登录轻空间。

- 设备认证：系统根据终端设备的多个硬件标识，给每个终端生成唯一标识，设备接入时进行合法性校验。
- 加密传输：终端与服务端之间通过加密方式进行数据传输。

- 云端安全

- 安全管控
 - 云应用管控：轻空间云应用由管理员统一发放，终端用户无权限安装使用其他云应用，防止恶意软件入侵。
 - 外设可管控：可对USB存储设备、USB打印机、蓝牙等外设进行管控，防止数据资产泄漏。
- 实例安全
 - 实例管理、镜像管理有权限项，可与其他权限项分开授权，避免不当操作。
 - 实例上具备防病毒软件集成兼容能力，防止用户虚拟桌面遭受病毒攻击。
 - 实例被重新分配给另一用户时，用户数据清除，防止前用户数据泄露。
- 云盘安全
 - 支持用户数据加密存储。
 - 支持数据备份和恢复，故障发生时用户数据不丢失。
- 管理安全
 - 对管理员划分多个角色，不同角色之间相互制约。
 - 支持对业务管理员进行不同权限配置，保障最小可用原则。
 - 支持管理员操作日志可审计，行为可追溯。
 - 终端用户轻空间访问、云桌面、云应用使用记录可查看导出，行为可追溯。
- 云基础设施安全

基于阿里云专有云平台，保障物理环境、硬件、虚拟化层平台的安全，同时，云盾——作为专有云安全解决方案，从网络、服务器、应用、数据等多方面保护无影系统安全。

5.应用场景

阿里云无影产品为不同规模、不同行业的用户提供适合的行业解决方案。针对不同行业打造行业特性方案，包括政务、金融、教育等行业。

政务办公

政务办公场景中，政府对服务运行环境、办公数据安全、管理效率提出了更高的要求，所以针对这些行业需求，结合阿里生态办公服务，形成更安全高效的方案。

价值体现如下：

- 基于阿里云专有云企业版，具备合规安全的一整套成熟方案。
- 办公管理模式突破，形成资源 and 数据集中化管理、按需动态分配，无需过多本地管理。
- 安全管控升级，数据生产在云端，同时形成多份备份，从源头即杜绝泄露或遗失。

企业办公

在企业办公场景中，大部分公司数据管控较为松散，资产利用率不高，员工流动性较高导致运维成本过高。针对这些问题和难点，采用阿里云无影产品企业办公方案，更好地解决这些问题。

价值体现如下：

- 办公管理模式突破，资源和数据的集中化管理，按需动态分配，无需过多本地管理。
- 安全管控的升级，让数据生产在云端，同时形成多份备份，从源头即杜绝泄露或遗失。

6.基本概念

本文将对所涉及的专有名词进行解释。

名词	解释
Apsara Uni-manager运营控制台	Apsara Uni-manager运营控制台是基于阿里云专有云平台为客户定制的服务能力平台。
Apsara Uni-manager运维控制台	Apsara Uni-manager运维控制台是阿里云专有云统一的智能化运维平台。
ASP	ASP（Adaptive Streaming Protocol）是阿里云自主研发的面向应用流的一种新型端云协同协议，旨在为无影产品提供端云一体的协议支撑，为终端用户提供低时延高画质的实时交互体验。
Docker	Docker是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的容器中，然后发布到任何流行的Linux机器或Windows 机器上，也可以实现虚拟化，容器完全使用沙箱机制，相互之间不会有任何接口。
FPS	FPS（Frames Per Second）是指画面每秒传输帧数。
Kubernetes	Kubernetes是容器集群管理系统，是一个开源的平台，可以实现容器集群的自动化部署、自动扩缩容、维护等功能。
NACK	丢包重传（NACK）是避免网络错误的重要手段之一。
Pod	Pod是Kubernetes创建或部署的最小、最简单的基本单位，一个Pod代表集群上正在运行的一个进程。
StreamingDocker	零终端流媒体软件底座。
TWAIN	TWAIN（Technology Without An Interesting Name）无注册工具包协议，是一个软件和数码相机、扫描仪等图像输入设备之间的通讯标准。
URB	URB（USB Request Block）是USB设备驱动中用来描述与USB设备通信所用的基本载体和核心数据结构。

名词	解释
UOS	统一操作系统UOS是由多家国内操作系统核心企业自愿发起“UOS(unity operating system)统一操作系统筹备组”共同打造的中文国产操作系统。
UVC	UVC (USB Video Class) USB视频类，是一种为USB视频捕获设备定义的协议标准。是Microsoft与另外几家设备厂商联合推出的为USB视频捕获设备定义的协议标准，已成为USB org标准之一。
VM	虚拟机 (Virtual Machine)。
VMAF	VMAF (Video Multimethod Assessment Fusion) 由Netflix开发并开源在Github上，基本想法在于，面对不同特征的源内容、失真类型，以及扭曲程度，每个基本指标各有优劣。通过使用机器学习算法(SVM)将基本指标“融合”为一个最终指标，可以为每个基本指标分配一定的权重，这样最终得到的指标就可以保留每个基本指标的所有优势，借此可得出更精确的最终分数。
存储卷	存储卷 (Volume) 是Pod中能够被多个容器访问的共同目录。与Pod生命周期相同，但与Pod内的容器生命周期不相关，当容器终止或重启，存储卷中的数据也不会丢失。
零终端	阿里云无影产品中的自主研发超轻量级终端设备，支持ASP协议，主要用于连接用户终端外设和轻空间服务接入。
轻空间	在阿里云无影产品中提供给终端办公用户的一个智能办公空间。
云管控	阿里云无影产品中面向客户运维管理人员一站式控制台，集成在Apsara Uni-manager运营控制台中，可对轻空间、云资源及零终端进行安全有效的管控。