

云桌面

产品介绍

文档版本 08
发布日期 2024-10-16



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 什么是云桌面?	1
2 产品优势	2
3 应用场景	3
4 业务流程	4
5 相关概念	6
6 支持列表	9
7 安全	11
7.1 责任共担	11
7.2 身份认证与访问控制	12
7.3 数据保护技术	13
7.3.1 Hypervisor 安全	13
7.3.2 主机安全	14
7.4 审计与日志	15
7.5 监控安全风险	16
7.6 故障恢复	16
7.7 认证证书	16
7.8 许可证类型	18
8 权限管理	19
8.1 权限和授权项	19
9 约束与限制	37
10 套餐与计费	40
11 云桌面与其他服务的关系	43
A 修订记录	45

1 什么是云桌面?

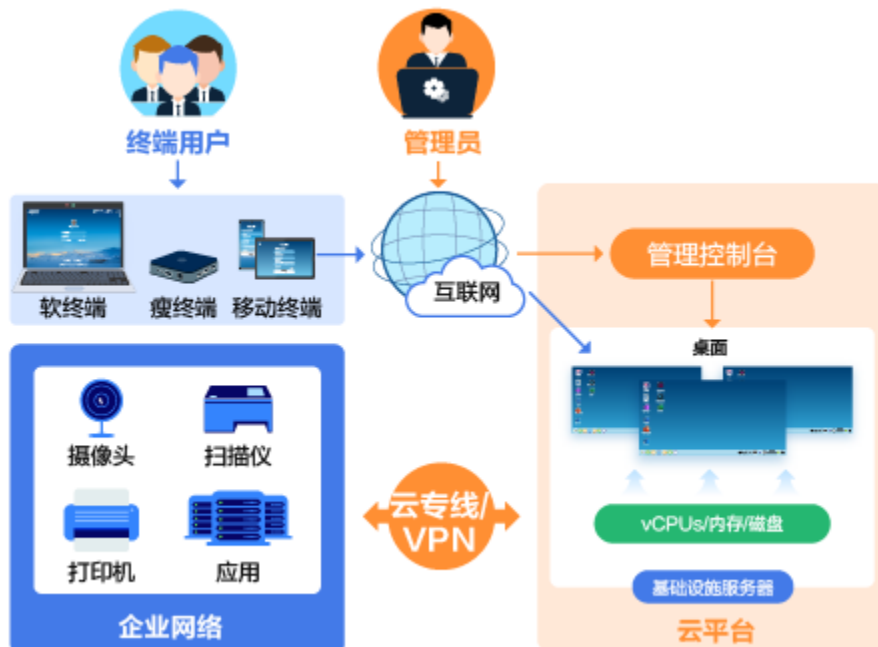
云桌面简介

华为云桌面是一种基于云计算（包括边缘计算）的桌面服务。与传统PC和VDI不同，企业无需投入大量的资金和花费数天的部署时间，即可快速构建桌面办公环境。云桌面支持多种登录方式，可让您灵活存取文件及使用应用，实现移动办公。

基本原理

终端用户通过终端设备登录由管理员在云平台的管理控制台中购买的桌面，实现办公需求。并且可以通过云专线/VPN的方式使用存储于企业网络中的网络应用。云桌面的基本原理，如图1-1所示。

图 1-1 云桌面基本原理示意图



2 产品优势

云桌面采用即开即用式桌面发放形式，支持多种终端无缝登录，能快速为您提供可靠、安全、灵活、高效的办公环境。

体验流畅

自研HDP高清传输协议，真彩无损显示，高清流畅体验，桌面操控延时无感知。

弹性高效

按需扩缩，按需购买使用；资源集中管理，桌面部署快速。

安全可靠

端到端安全防护，数据不落地。安全策略强管控，芯片级安全加密存储。

生态开放

开放云桌面API和SDK，免底层技术自研、零起点办公生态上云。

3 应用场景

传统PC和VDI需要大量的资金投入，而且部署和管理工作通常都比较复杂和困难。云桌面无需前期投资，亦无需对基础设施进行持续管理，您只需支付一定的费用，便可享受一套完整的云桌面计算服务，包括计算、持久性存储，还能够让您以简单、经济实惠的方式为您的用户提供安全且具有丰富访问选项的桌面体验。

云桌面可广泛应用于公共事业、电信、能源、金融、交通、医疗、教育、广电、媒资、制造业等主流行业，适用于多种的场景，如普通办公、安全办公、分支机构、公用终端（呼叫中心、营业厅、培训教室等）。

移动办公场景

可以通过移动设备随时随地登录云桌面进行办公，适用于经常出差和工作地点不固定的员工办公。

短期使用场景

云桌面和必要的应用系统服务可以配置给企业的短期雇员，在短期雇员离开后，可以终止服务。

安全 OA 场景

云桌面可以为企业提供符合企业安全标准的办公方案，有效管控员工访问物理设备的权限，数据不存储在本地，有效提高了企业数据的安全性。

分支机构场景

在公司分支机构或外部的员工可以通过登录云桌面来访问公司总部的应用，数据不会存储在本地，适用于公司分支机构的员工和公司外部员工办公。

4 业务流程

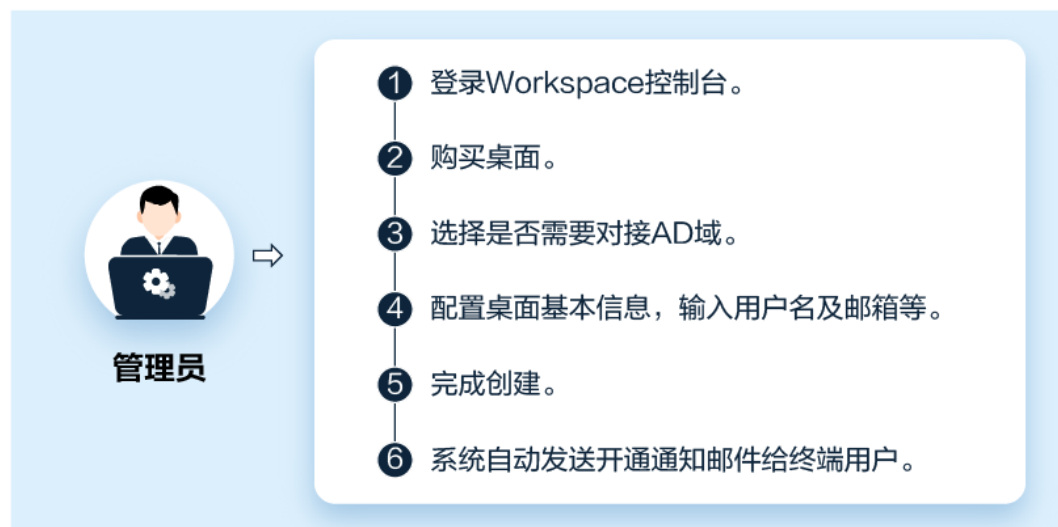
为终端用户发放桌面的用户为管理员，其具体操作流程如[图4-1](#)所示。

最终使用桌面的用户为终端用户，其具体操作流程如[图4-2](#)所示。

管理员业务流程

管理员通过云桌面控制台购买桌面，购买过程中支持选择是否对接AD域，并为具体用户分配桌面，购买成功后，系统自动推送桌面开通信息给终端用户。

图 4-1 管理员操作流程



终端用户业务流程

终端用户可使用多种终端设备登录并使用桌面，如[图4-2](#)所示。

图 4-2 终端用户操作流程



5 相关概念

桌面

桌面是指安装了桌面代理软件，可以与桌面管理组件进行交互的虚拟计算机系统。云桌面将所有桌面在数据中心进行托管并统一管理，终端用户可通过软终端、瘦终端、移动终端的方式登录桌面，获得完整PC桌面的使用体验。

您可以为每个终端用户购买专属桌面，使其各自独享一个桌面。

桌面池

桌面池是一批同规格镜像桌面集合，它能为管理员提供该项目下一批桌面的统一管理和运维的能力。桌面池包含动态池、静态池两种类型。

- 动态池是指M:N的池类型的桌面组，该桌面池内的虚拟机与对应的虚拟机用户一直没有固定的分配绑定关系；虚拟机用户每次通过客户端登录该桌面池时，workspace会动态的从该桌面池中随机分配一台空闲的虚拟机给该用户使用。
- 静态池是指1:1的池类型的桌面组。该桌面池内的虚拟机与对应的虚拟机用户最初没有固定的分配绑定关系，当该池内某个虚拟机第一次登录使用时，这个虚拟机与用户的分配绑定关系就固定下来了，后续该用户登录该桌面组，都会分配同一台虚拟机供其使用的，此虚拟机不会再分配给其他用户使用。

用户

根据用户权限区分为终端用户和管理员。终端用户即最终使用桌面的用户，具有登录、使用桌面的权限。管理员即租户，即为最终使用桌面的用户分配桌面的用户，具有购买桌面、删除桌面、设置策略、管理用户等权限。

用户组

用户组是多个用户的集合，通过将用户分配到不同的组中，可以方便的管理和控制资源的访问。用户组还可以拥有自己的权限和设置，从而控制组内用户的行为。

策略

策略分为协议策略和接入策略。

协议策略是为桌面配置的一组关于USB重定向、文件重定向读写权限、剪切板读写权限、水印、客户端自动重连间隔、画面显示等的安全规则集合，用于控制用户终端与云桌面之间的数据传输和外设接入权限。

接入策略是为桌面配置的一组关于接入方式使用的规则，用于控制用户使用互联网接入地址还是云专线接入地址访问云桌面。

优先级

优先级是云桌面服务判定桌面策略执行先后顺序或者作用权重的依据。优先级由正整数表示，数值越小，优先级越高。

软终端

软终端（Software Client）是指在本地图PC上安装云桌面的客户端，使用户能通过该PC接入桌面，该PC即称为软终端。

瘦终端

瘦终端（Thin Client）是基于PC工业标准设计的小型行业专用商用PC，使用专业嵌入式处理器、小型本地闪存、精简版操作系统，用于接入桌面。瘦终端将鼠标、键盘等输入传送到后台服务器处理，服务器再把处理结果返回给瘦终端连接的显示器显示。不同型号的瘦终端有不同的性能、外设接口、操作界面，可以灵活满足普通办公、高安全、高性能图形设计等使用场景。

移动终端

移动终端是指在移动设备上安装云桌面的客户端，使用户能通过该移动设备接入桌面，该移动设备即称为移动终端。当前仅支持Android智能设备。

AD 管理服务器

活动目录（Active Directory），简称AD。AD管理服务器即部署了AD服务的基础架构组件，它可以提供一系列集中组织管理和访问网络资源的目录服务功能。云桌面支持对接您自己的AD服务器，实现对云桌面的鉴权和认证。

区域和可用区

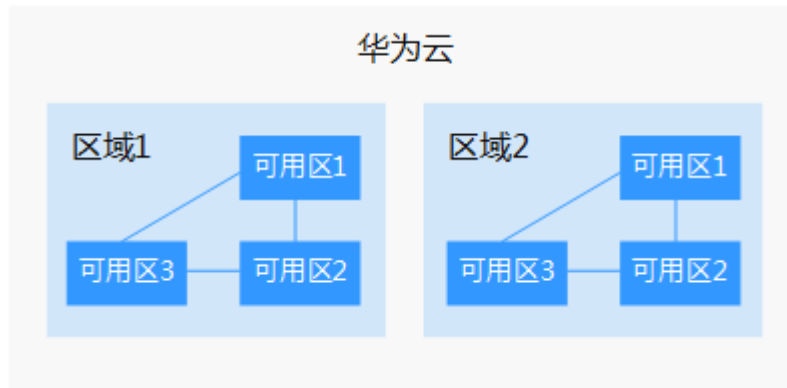
华为云用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区购买桌面。

区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

[图5-1](#)阐明了区域和可用区之间的关系。

图 5-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

项目

区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中购买资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

多因素认证

多因素认证是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，终端用户登录桌面时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。

虚拟 MFA

虚拟Multi-Factor Authentication (MFA) 是能产生6位数字认证码的虚拟设备，遵循基于时间的一次性密码（TOTP）标准。云桌面使用的虚拟MFA是基于软件的虚拟MFA应用程序，可以在移动硬件设备（包括智能手机）上运行，非常方便，虚拟MFA是多因素认证方式中的一种。

6 支持列表

操作系统支持列表

支持购买如[表6-1](#)中所示操作系统的桌面。

表 6-1 操作系统支持说明

操作系统版本	操作系统类型	说明
Windows Server 2016	64位	云桌面目前支持、麒麟操作系统Windows操作系统的普通桌面。后续云桌面将持续为您提供更多操作系统桌面版本，丰富办公环境。镜像语言支持“西班牙语”和“法语”。 云桌面不提供默认镜像，需要用户参考《管理员用户指南》的“ 制作Windows普通桌面私有镜像 ”章节制作私有镜像。
Windows Server 2019	64位	
Windows 10	64位	

软终端支持列表

支持通过如[表6-2](#)中所示版本软终端登录桌面。客户端软件包可从[华为云桌面客户端下载页面](#)获取。

表 6-2 软终端支持说明

终端设备操作系统	说明
Windows 10	支持Windows 10操作系统的PC，通过安装的客户端登录桌面。
macOS 10.14~12.4 (64位)	支持macOS (64位，版本10.14到12.4) 的PC，通过安装的客户端登录桌面。

瘦终端支持列表

支持通过云桌面适配瘦终端登录桌面，例如，可使用[表6-3](#)中所示瘦终端型号接入云桌面。

表 6-3 瘦终端支持说明

瘦终端型号	说明
HT3300	该TC操作系统为UOS，支持通过安装的客户端（华为云办公）登录桌面。
HT1100	该TC操作系统为Android，支持通过安装的云桌面客户端登录桌面。

移动终端支持列表

支持如[表6-4](#)所示操作系统的移动终端设备登录桌面。客户端软件包可从[华为云桌面客户端下载页面](#)通过浏览器扫描二维码获取。

表 6-4 移动终端支持说明

移动终端操作系统版本	说明
Android 6.0以上	支持安装了Android 6.0以上版本操作系统的移动终端设备，通过安装的客户端（华为云办公）登录桌面。

7 安全

- 7.1 责任共担
- 7.2 身份认证与访问控制
- 7.3 数据保护技术
- 7.4 审计与日志
- 7.5 监控安全风险
- 7.6 故障恢复
- 7.7 认证证书
- 7.8 许可证类型

7.1 责任共担

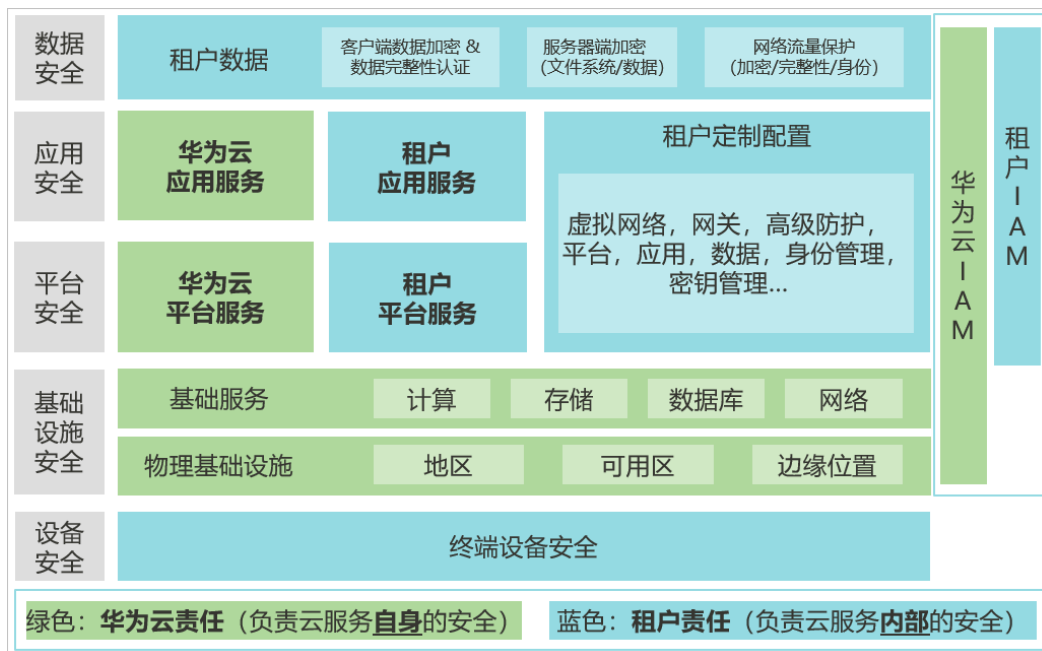
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图7-1所示。

- 华为云：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- 租户：负责云服务内部的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 7-1 华为云安全责任共担模型



7.2 身份认证与访问控制

IAM 身份认证

Workspace支持通过IAM进行精细的权限管理，实现用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制资源的访问。

您可以在账号中创建IAM用户，并授权控制他们对资源的访问范围。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。

- 权限管理简介，请参见[权限管理](#)。
- 授权使用Workspace，请参见[创建用户并授权使用Workspace](#)。
- 自定义策略，请参见[Workspace自定义策略](#)。
- 策略及授权项详情，请参见[策略及授权项说明](#)。

项目与企业项目

Workspace支持通过项目及企业项目对资源进行分组、管理和隔离，实现按照企业、部门或者项目组等不同组织对资源的管理和访问控制。

- 项目
IAM中的项目用于将资源进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。一个账户中可以创建多个项目。
- 企业项目
企业管理中的企业项目是对多个资源进行分组和管理，不同区域的资源可以划分到一个企业项目中。企业可以根据不同的部门或项目组，将相关的资源放置在相同的企业项目内进行管理，并支持资源在企业项目之间迁移。
- 项目和企业项目的区别

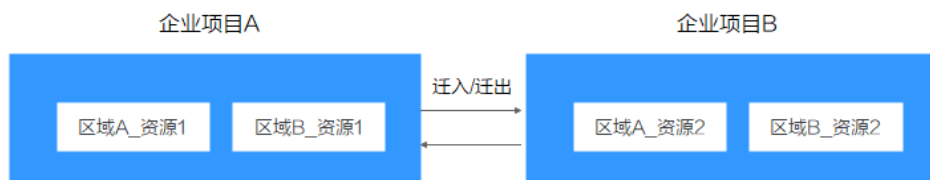
- IAM项目

IAM项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。



- 企业项目

企业项目是IAM项目的升级版，是针对企业不同项目间资源的分组和管理。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。如果您开通了企业管理，将不能创建新的IAM项目（只能管理已有项目）。未来IAM项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。



项目和企业项目都可以授权给一个或者多个用户组进行管理，管理企业项目的用户归属于用户组。通过给用户组授予策略，用户组中的用户就能在所属项目/企业项目中获得策略中定义的权限。

关于如何创建项目、企业项目，以及如何授权，请参阅[企业项目](#)。

访问控制

- 虚拟私有云

虚拟私有云（Virtual Private Cloud，以下简称VPC）为Workspace构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为Workspace构建一个逻辑上完全隔离的专有区域。您还可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。同时，您可以自定义安全组内与组间云桌面的访问规则，加强Workspace的安全保护。

- 安全组

安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的Workspace提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当Workspace加入该安全组后，即受到这些访问规则的保护。

7.3 数据保护技术

7.3.1 Hypervisor 安全

什么是Hypervisor

Hypervisor能实现同一物理机上不同虚拟机之间的资源隔离，避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响。用户使用虚拟机

时，仅能访问属于自己的虚拟机的资源（如硬件、软件和数据），不能访问其他虚拟机的资源，保证虚拟机隔离安全。

CPU隔离

x86架构为了保护指令的运行，提供了指令的4个不同特权级别，术语称为Ring，优先级从高到低依次为：

- Ring 0：被用于运行操作系统内核。
- Ring 1：用于操作系统服务。
- Ring 2：用于特权代码（具有I/O访问权限的用户程序）。
- Ring 3：用于应用程序。

各个级别对可以运行的指令进行限制：

- Hypervisor运行在Ring0。
- 虚拟机操作系统运行在Ring 1，有效地防止了虚拟机Guest OS直接执行所有特权指令。
- 应用程序运行在Ring 3上，保证了操作系统与应用程序之间的隔离。

CPU硬件辅助虚拟化的引入进一步实现了Hypervisor和虚拟机操作系统运行模式的深度隔离。

内存隔离

Hypervisor通过内存虚拟化技术来实现不同虚拟机之间的内存隔离。内存虚拟化技术在传统OS两层地址映射（“虚拟地址”到“机器地址”）的基础上，引入三层地址映射：虚拟机负责将“Guest虚拟地址”映射为“Guest物理地址”，然后Hypervisor负责将“虚拟机物理地址”映射成“机器地址”，再交由物理处理器来执行，保证了虚拟机无法直接接触实际的机器地址，只能访问Hypervisor分配给它的物理内存。

I/O隔离

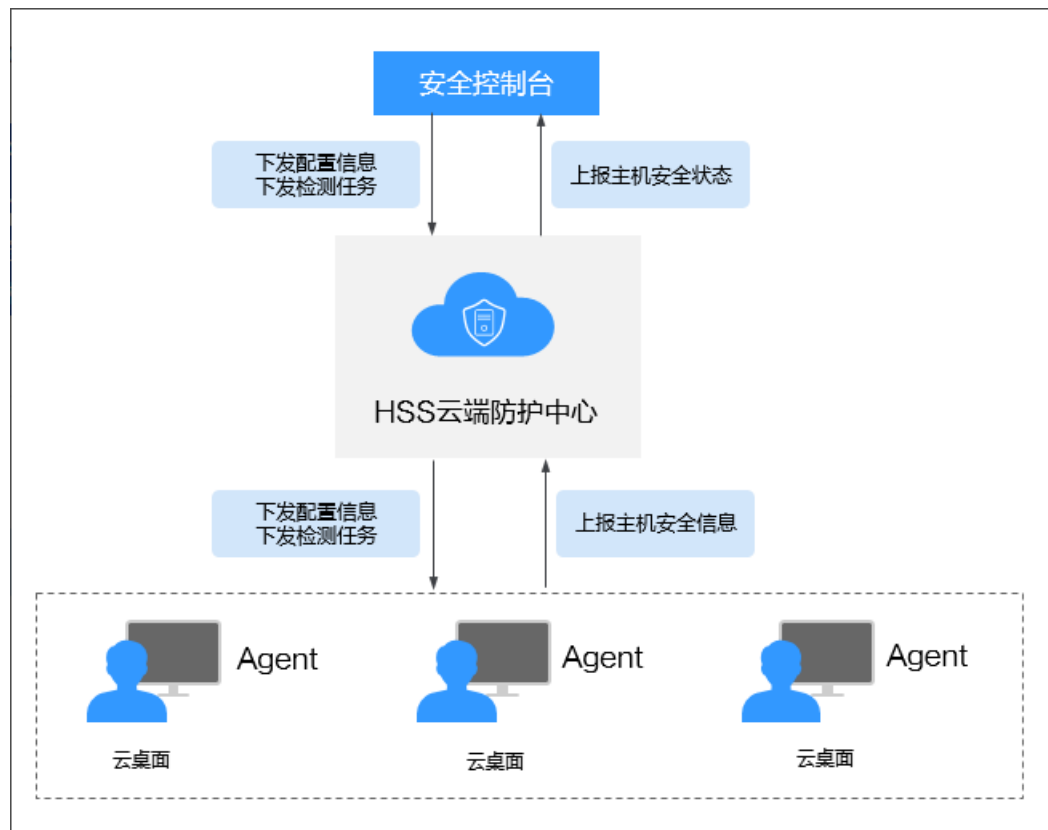
Hypervisor采用分离设备模型实现I/O的虚拟化。前端负责将虚拟机的I/O请求传递到Hypervisor中的后端，后端解析I/O请求并提交给相应的设备完成I/O操作。Hypervisor保证虚拟机只能访问分配给它的I/O资源。

7.3.2 主机安全

主机安全服务（Host Security Service，HSS）是提升服务器整体安全性的服务，为用户提供资产管理、漏洞管理、入侵检测、基线检查等功能，降低服务器被入侵的风险。

在云桌面中安装Agent后，云桌面受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

图 7-2 HSS 功能原理



主机安全服务的组件功能及工作流程说明如下：

- 安全控制台：
可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
- HSS云端防护中心：
 - 接收您在控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent。
 - 接收Agent上报的主机信息，分析主机中存在的安全风险和异常信息，将分析后的信息以检测报告的形式呈现在控制台界面。
- HSS客户端：
 - 接收HSS云端防护中心转发的检测任务。
 - 按检测任务要求扫描云桌面，并将事件扫描信息上报给HSS云端防护中心。

您在使用主机安全服务前，需要先在云服务器上安装客户端。更多信息，请参考[主机安全](#)。

7.4 审计与日志

云审计服务（Cloud Trace Service, CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。用户开通云审计服务并创建和配置追踪器后，CTS可记录Workspace的管理事件用于审计。

CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。

7.5 监控安全风险

云桌面（Workspace）提供基于云监控服务CES的资源 and 操作监控能力，帮助用户对每个云桌面实例进行自动实时监控、告警和通知操作。用户可以实时掌握实例的资源占用、接入网络、接入统计、异常事件等监控等关键信息。

关于云桌面支持的监控指标，以及如何创建监控告警规则等内容，请参见[告警监控及Workspace支持的CES基础监控指标](#)。

7.6 故障恢复

当云桌面或磁盘出现故障或者人为错误导致数据误删时，可以自助快速恢复数据，具体参考如下：

- 云桌面可以通过云备份实现故障恢复：详情参考[数据备份与恢复](#)。
- 云桌面可以通过桌面快照实现故障恢复：详情参考[桌面快照管理](#)。

7.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行[申请下载](#)合规资质证书。

图 7-3 合规证书下载

合规证书下载

请输入关键词搜索

BS 10012:2017
BS 10012为个人信息管理体系提供了一个符合欧盟GDPR原则的最佳实践框架。它概述了组织在收集、存储、处理、保留或处理与个人相关的个人记录时需要考虑的核心需求。保留或处理与个人相关的个人记录时需要考虑的核心需求。

CSA STAR认证
CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。

ISO 20000-1:2018
ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的IT服务来满足客户和业务的需求。

SOC 1 类型II 报告 2022.04.01-2023.03.31
华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。

SOC 1 类型II 报告 2022.10.01-2023.09.30
华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为 2022.10.01-2023.09.30。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。

SOC 2 类型II 报告 2022.04.01-2023.03.31
华为云每年滚动发布两期SOC2报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 2报告着重于组织的内部运作与合规，包括安全性、可用性、进程完整性、保密性、隐私性五大控制属性。

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看[资源中心](#)。

图 7-4 资源中心

资源中心

白皮书资源

隐私遵从性白皮书 | 行业规范遵从性白皮书 | 指南和最佳实践

尼日利亚NDPR遵从性指南
本白皮书基于尼日利亚NDPR合规要求，分享华为云隐私保护的经验和实践，以及如何助力您满足尼日利亚NDPR合规要求。

阿根廷PDPL遵从性指南
本白皮书基于阿根廷PDPL及第47号决议的合规要求，分享华为云隐私保护的经验和实践，以及如何助力您满足PDPL和第47号决议的合规要求。

巴西LGPD遵从性指南
本白皮书基于巴西LGPD合规要求，分享华为云在隐私保护领域的经验和实践，以及如何助力您满足巴西LGPD合规要求。

智利共和国PDPL遵从性指南
本白皮书基于智利共和国PDPL合规要求，分享华为云隐私保护的经验和实践，以及如何助力客户满足智利共和国PDPL合规要求。

7.8 许可证类型

使用自带许可证（BYOL）

什么是BYOL

BYOL（Bring Your Own License）是指用户自带许可证，即用户使用已有操作系统的授权许可，无需重新申请新的许可证。

使用BYOL

对于自带许可证的用户，需自行管理云桌面许可证。如果您已有相应操作系统的授权许可证，可直接使用已有许可证。

支持使用自带许可证（BYOL）的操作系统有：

- Windows

相关操作场景

系统不支持动态修改许可证类型。云桌面可以在如下场景使用自带许可证（BYOL）：

- 创建云桌面
云桌面创建完成后，用户不能动态修改该云桌面的许可证类型。如需修改，请重装或切换云桌面的操作系统。
- 重装云桌面的操作系统
重装操作系统时，用户可以选择该云桌面的许可证类型。
- 切换云桌面的操作系统
切换操作系统时，用户可以选择该云桌面的许可证类型。

8 权限管理

8.1 权限和授权项

8.1 权限和授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，租户管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。
- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。
- IAM项目（Project）/企业项目（Enterprise Project）：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。关于IAM项目与企业项目的区别，详情请参见：[IAM与企业管理的区别](#)。

授权项（Action）	对应API接口	授权项说明	IAM项目（Project）	企业项目（Enterprise Project）
workspace:desktops:create	POST /v2/{project_id}/desktops	创建桌面	√	√
workspace:desktops:update	PUT /v2/{project_id}/desktops/{desktop_id}	更新桌面信息	√	√
workspace:desktops:delete	DELETE /v2/{project_id}/desktops/{desktop_id}	删除桌面	√	√

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:desktops:get	GET /v2/{project_id}/desktops/{desktop_id}	查询桌面详情	√	√
workspace:desktops:list	GET /v2/{project_id}/desktops	查询桌面列表	√	√
workspace:desktops:listDetail	GET /v2/{project_id}/desktops/detail	查询桌面详情列表	√	√
workspace:desktops:batchDelete	POST /v2/{project_id}/desktops/batch-delete	批量删除桌面	√	√
workspace:desktops:operate	POST /v2/{project_id}/desktops/action	操作桌面 (开关机、重启、休眠)	√	√
workspace:desktops:reboot	POST /v2/{project_id}/desktops/reboot	重启桌面	√	√
workspace:desktops:start	POST /v2/{project_id}/desktops/start	启动桌面	√	√
workspace:desktops:stop	POST /v2/{project_id}/desktops/stop	关闭桌面	√	√
workspace:desktops:getLastDeleteTime	GET /v2/{project_id}/desktops/last-desktop-delete-time	查询租户最后一台计算机的删除时间	√	x
workspace:desktops:resize	POST /v2/{project_id}/desktops/resize	变更规格	√	√
workspace:desktops:rebuild	POST /v2/{project_id}/desktops/rebuild	重建桌面	√	√
workspace:desktops:getActions	GET /v2/{project_id}/desktops/{desktop_id}/actions	查询桌面开关机信息	√	√
workspace:desktops:getMonitor	GET /v2/{project_id}/desktop-monitor/{desktop_id}	查询桌面监控信息	√	√
workspace:desktops:createConsole	GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	获取远程登录控制台地址	√	√
workspace:desktops:updateSids	PUT /v2/{project_id}/desktops/sids	更新桌面SID	√	√

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:desktops:rejoinDomain	POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	重新加入AD域	√	√
workspace:desktops:createImage	POST /v2/{project_id}/desktops/desktop-to-image	桌面转镜像	√	x
workspace:desktops:export	GET /v2/{project_id}/desktops/export	导出桌面列表	√	√
workspace:desktops:detach	POST /v2/{project_id}/desktops/detach	解绑用户	√	√
workspace:desktops:attach	POST /v2/{project_id}/desktops/attach	分配用户	√	√
workspace:desktops:getSysprepVersion	GET /v2/{project_id}/desktops/{desktop_id}/sysprep	查询Sysprep版本信息	√	x
workspace:desktops:getConnectStatus	GET /v2/{project_id}/connections/status	查询桌面登录状态统计数据	√	x
workspace:agencies:create	POST /v2/{project_id}/agencies	创建委托	√	x
workspace:agencies:get	GET /v2/{project_id}/agencies	查询委托	√	x
workspace:desktops:verifyDesktopName	POST /v2/{project_id}/verification/desktop-name	校验桌面名称	√	x
workspace:desktops:getAdStatus	GET /v2/{project_id}/ad/status	查询AD网络状态	√	x
workspace:desktopPools:create	POST /v2/{project_id}/desktop-pools	创建桌面池	√	√
workspace:desktopPools:update	PUT /v2/{project_id}/desktop-pools/{pool_id}	修改桌面池属性	√	√
workspace:desktopPools:delete	DELETE /v2/{project_id}/desktop-pools/{pool_id}	删除桌面池	√	√

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:desktopPools:get	GET /v2/{project_id}/desktop-pools/{pool_id}	查询桌面池详情	√	√
workspace:desktopPools:list	GET /v2/{project_id}/desktop-pools	查询桌面池列表	√	√
workspace:desktopPools:expand	POST /v2/{project_id}/desktop-pools/{pool_id}/expand	扩容桌面池	√	√
workspace:desktopPools:resize	POST /v2/{project_id}/desktop-pools/{pool_id}/resize	桌面池变更规格	√	√
workspace:desktopPools:rebuild	POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	桌面池重建系统盘	√	√
workspace:desktopPools:batchAddVolumes	POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	桌面池批量添加磁盘	√	√
workspace:desktopPools:batchDeleteVolumes	POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	桌面池批量删除磁盘	√	√
workspace:desktopPools:batchExpandVolumes	POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	桌面池批量扩容磁盘	√	√
workspace:desktopPools:operate	POST /v2/{project_id}/desktop-pools/{pool_id}/action	操作桌面池	√	√
workspace:desktopPools:authorizeUsers	POST /v2/{project_id}/desktop-pools/{pool_id}/users	桌面池授权用户、用户组	√	√
workspace:desktopPools:listUsers	GET /v2/{project_id}/desktop-pools/{pool_id}/users	查询桌面池授权的用户、用户组	√	√
workspace:desktopops:tag	POST /v2/{project_id}/desktops/{desktop_id}/tags	创建桌面标签	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:desktops:listTags	GET /v2/{project_id}/desktops/{desktop_id}/tags	查询桌面标签	√	x
workspace:desktops:untag	DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	删除桌面标签	√	x
workspace:desktops:listProjectTags	GET /v2/{project_id}/desktops/tags	查询项目标签	√	x
workspace:desktops:operateTags	POST /v2/{project_id}/desktops/{desktop_id}/tags/action	批量添加删除标签	√	x
workspace:desktops:listByTags	POST /v2/{project_id}/desktops/resource_instances/action	使用标签过滤桌面	√	x
workspace:jobs:list	POST /v2/{project_id}/workspace-jobs	查询任务列表	√	x
workspace:jobs:get	GET /v2/{project_id}/workspace-jobs/{job_id}	查询任务详情	√	x
workspace:jobs:listSubJobs	GET /v2/{project_id}/workspace-sub-jobs	查询子任务列表	√	x
workspace:jobs:retry	POST /v2/{project_id}/workspace-jobs/{job_id}/actions	重试任务	√	x
workspace:jobs:deleteSubJobRecords	POST /v2/{project_id}/workspace-sub-jobs/batch-delete	删除子任务记录	√	x
workspace:networks:createNat	POST /v2/{project_id}/internet	开通NAT网关上网功能	√	√
workspace:networks:listNats	GET /v2/{project_id}/internet	查询NAT网关上网功能	√	√
workspace:networks:createEips	POST /v2/{project_id}/eips	创建EIP	√	√

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:networks:listEips	GET /v2/{project_id}/eips	查询EIP列表	√	√
workspace:networks:bindEips	POST /v2/{project_id}/eips/binding	绑定EIP	√	√
workspace:networks:unbindEips	POST /v2/{project_id}/eips/unbinding	解绑EIP	√	√
workspace:networks:getEipQuota	GET /v2/{project_id}/eips/quotas	查询EIP配额	√	√
workspace:networks:listVpcs	GET /v2/{project_id}/vpcs	查询查询vpc	√	√
workspace:networks:listSubnets	GET /v2/{project_id}/subnets	查询子网列表	√	√
workspace:networks:listSecurityGroups	GET /v2/{project_id}/security-groups	查询安全组列表	√	√
workspace:networks:getAvailableIp	GET /v2/{project_id}/subnets/{subnet_id}/available-ip	根据子网id查询该子网下可用的ip	√	√
workspace:orders:create	POST /v2/{project_id}/periodic/subscribe/order	包周期下单	√	√
workspace:orders:change	POST /v2/{project_id}/periodic/{desktop_id}/change/order	创建变更订单	√	√
workspace:renderDesktops:create	POST /v2/{project_id}/render-desktops	创建渲染桌面	√	√
workspace:renderDesktops:delete	DELETE /v2/{project_id}/render-desktops	删除渲染桌面	√	√
workspace:renderDesktops:list	GET /v2/{project_id}/render-desktops	查询渲染桌面列表	√	√
workspace:renderDesktops:action	POST /v2/{project_id}/render-desktops/action	操作渲染桌面	√	√

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:renderDesktops:create Console	GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	获取远程登录控制台地址	√	√
workspace:renderDesktops:resize	PUT /v2/{project_id}/render-desktops/resize	变更渲染桌面规格	√	√
workspace:scheduledTasks:create	POST /v2/{project_id}/scheduled-tasks	创建定时任务	√	x
workspace:scheduledTasks:list	GET /v2/{project_id}/scheduled-tasks	查询定时任务列表	√	x
workspace:scheduledTasks:update	PUT /v2/{project_id}/scheduled-tasks/{task_id}	更新定时任务	√	x
workspace:scheduledTasks:delete	DELETE /v2/{project_id}/scheduled-tasks/{task_id}	删除定时任务	√	x
workspace:scheduledTasks:get	GET /v2/{project_id}/scheduled-tasks/{task_id}	查询定时任务详情	√	x
workspace:scheduledTasks:getFuture	POST /v2/{project_id}/scheduled-tasks/future-executions	查询定时任务未来执行时间	√	x
workspace:scheduledTasks:batchDelete	POST /v2/{project_id}/scheduled-tasks/batch-delete	批量删除定时任务	√	x
workspace:scheduledTasks:listRecords	GET /v2/{project_id}/scheduled-tasks/{task_id}/records	查询定时任务执行记录	√	x
workspace:scheduledTasks:getRecord	GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	查询定时任务执行记录详情	√	x
workspace:scheduledTasks:exportRecords	POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	导出定时任务记录及执行详情	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:statistics:getRunState	GET /v2/{project_id}/desktops/statistics/run-state	运行状态统计	√	x
workspace:statistics:getLoginState	GET /v2/{project_id}/desktops/statistics/login-state	登录状态统计	√	x
workspace:statistics:getUnused	GET /v2/{project_id}/desktops/statistics/unused	查询在指定时间段未使用的桌面	√	x
workspace:statistics:getUsed	POST /v2/{project_id}/desktops/statistics/used	查询使用桌面的时长	√	x
workspace:bindingPolicies:getConfig	GET /v2/{project_id}/terminals/binding-desktops/config	查询终端与桌面绑定的开关配置信息	√	x
workspace:bindingPolicies:createConfig	POST /v2/{project_id}/terminals/binding-desktops/config	设置终端与桌面绑定的开关配置	√	x
workspace:bindingPolicies:get	GET /v2/{project_id}/terminals/binding-desktops	查询终端与桌面绑定配置列表	√	x
workspace:bindingPolicies:add	POST /v2/{project_id}/terminals/binding-desktops	增加终端与桌面绑定配置	√	x
workspace:bindingPolicies:update	PUT /v2/{project_id}/terminals/binding-desktops	修改终端与桌面绑定配置	√	x
workspace:bindingPolicies:delete	POST /v2/{project_id}/terminals/binding-desktops/batch-delete	删除终端与桌面绑定配置	√	x
workspace:bindingPolicies:getTemplate	GET /v2/{project_id}/terminals/binding-desktops/template	下载终端与桌面绑定模板	√	x
workspace:bindingPolicies:import	POST /v2/{project_id}/terminals/binding-desktops/template/import	批量导入终端与桌面绑定	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:bindingPolicies:export	GET /v2/{project_id}/terminals/binding-desktops/template/export	导出终端与桌面绑定配置excel	√	x
workspace:volumes:add	POST /v2/{project_id}/desktops/{desktop_id}/volumes	增加桌面磁盘	√	√
workspace:volumes:delete	POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	删除桌面数据盘	√	√
workspace:volumes:batchAdd	POST /v2/{project_id}/desktops/volumes	多个桌面增加桌面磁盘	√	√
workspace:volumes:batchAdd	POST /v2/{project_id}/volumes	增加桌面磁盘	√	√
workspace:volumes:expand	POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	扩容磁盘	√	√
workspace:volumes:batchExpand	POST /v2/{project_id}/volumes/expand	扩容桌面磁盘	√	√
workspace:volumes:listDssPoolsDetail	GET /v2/{project_id}/dss-pools/detail	获取专属分布式存储池详情列表	√	√
workspace:wdh:listDesktops	GET /v2/{project_id}/hosts/{host_id}/servers	查询云办公主机包含桌面信息	√	√
workspace:wdh:getType	GET /v2/{project_id}/hosts/types	查询云办公主机类型	√	√
workspace:wdh:create	POST /v2/{project_id}/hosts	购买云办公主机	√	√
workspace:wdh:get	GET /v2/{project_id}/hosts	查询云办公主机列表	√	√
workspace:wdh:update	PUT /v2/{project_id}/hosts	更新云办公主机信息	√	√
workspace:tenants:get	GET /v2/{project_id}/workspaces	查询云办公服务详情	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:tenants:open	POST /v2/{project_id}/workspaces	开通云办公服务	√	x
workspace:tenants:update	PUT /v2/{project_id}/workspaces	修改云办公服务属性	√	x
workspace:tenants:delete	DELETE /v2/{project_id}/workspaces	注销云办公服务	√	x
workspace:tenants:checkEnterpriseIds	POST /v2/{project_id}/workspaces/enterprise-ids/check	检查企业ID是否已被使用	√	x
workspace:tenants:updateEnterpriseId	PUT /v2/{project_id}/workspaces/enterprise-id	修改企业ID	√	x
workspace:tenants:getRealms	GET /v2/{project_id}/workspaces/realms	查询租户域信息	√	x
workspace:tenants:getLockStatus	GET /v2/{project_id}/workspaces/lock-status	查询云办公服务是否被锁定	√	x
workspace:tenants:unlock	PUT /v2/{project_id}/workspaces/lock-status	解除云办公服务锁定状态	√	x
workspace:tenants:getRoles	GET /v2/{project_id}/tenants/roles	查询租户角色	√	x
workspace:natMappings:getConfig	GET /v2/{project_id}/nat-mapping-configs	查询租户的NAT映射配置项	√	x
workspace:natMappings:updateConfig	PUT /v2/{project_id}/nat-mapping-configs	修改租户的NAT映射配置项	√	x
workspace:sites:get	GET /v2/{project_id}/sites	查询站点信息	√	x
workspace:sites:add	POST /v2/{project_id}/sites	新增站点	√	x
workspace:sites:delete	DELETE /v2/{project_id}/sites/{site_id}	删除站点	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:sites:updateAccessMode	PUT /v2/{project_id}/sites/{site_id}/access-mode	修改站点接入方式	√	x
workspace:sites:updateSubnets	PUT /v2/{project_id}/sites/{site_id}/subnet-ids	修改站点业务子网	√	x
workspace:privacystatements:sign	POST /v2/{project_id}/privacystatement	签署隐私声明	√	x
workspace:quotas:get	GET /v2/{project_id}/quotas	查询租户配额	√	x
workspace:authConfigs:get	GET /v2/{project_id}/auth-config/method-config	查询认证登录方式配置信息	√	x
workspace:authConfigs:update	PUT /v2/{project_id}/auth-config/method-config	更新认证策略配置信息	√	x
workspace:assistAuthConfigs:get	GET /v2/{project_id}/assist-auth-config/method-config	查询辅助认证的配置信息	√	x
workspace:assistAuthConfigs:update	PUT /v2/{project_id}/assist-auth-config/method-config	更新辅助认证配置	√	x
workspace:accessPolicies:create	POST /v2/{project_id}/access-policy	创建接入策略	√	x
workspace:accessPolicies:delete	DELETE /v2/{project_id}/access-policy	删除指定接入策略	√	x
workspace:accessPolicies:get	GET /v2/{project_id}/access-policy	查询接入策略	√	x
workspace:accessPolicies:getTarget	GET /v2/{project_id}/access-policy/{access_policy_id}/objects	查询指定接入策略的应用对象	√	x
workspace:accessPolicies:updateTarget	PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	更新指定接入策略的应用对象	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:availabilityZones:list	GET /v2/{project_id}/availability-zones	查询支持的可用分区列表	√	x
workspace:availabilityZones:getSummary	GET /v2/{project_id}/availability-zones/summary	查询可用分区列表概要	√	x
workspace:availabilityZones:get	GET /v2/{project_id}/availability-zones/detail	查询可用分区详情	√	x
workspace:connections:securityList	GET /v2/{project_id}/connections/desktops	查询连接信息	√	x
workspace:connections:securityExport	GET /v2/{project_id}/connections/desktops/export	导出连接记录	√	x
workspace:connections:securityList	GET /v2/{project_id}/desktops/connections	查询连接信息	√	x
workspace:connections:securityExport	GET /v2/{project_id}/desktops/connections/export	导出连接记录	√	x
workspace:policyGroups:create	POST /v2/{project_id}/policy-groups	新增策略组	√	x
workspace:policyGroups:delete	DELETE /v2/{project_id}/policy-groups/{policy_group_id}	删除策略组	√	x
workspace:policyGroups:update	PUT /v2/{project_id}/policy-groups/{policy_group_id}	修改策略组	√	x
workspace:policyGroups:list	GET /v2/{project_id}/policy-groups	查询策略组列表	√	x
workspace:policyGroups:get	GET /v2/{project_id}/policy-groups/{policy_group_id}	查询策略组	√	x
workspace:policyGroups:export	POST /v2/{project_id}/policy-groups/export	导出策略组	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:policy Groups:import	POST /v2/{project_id}/policy-groups/import	导入策略组	√	x
workspace:policy Groups:listPolicies	GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	查询策略组中的策略项	√	x
workspace:policy Groups:updatePolicies	PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	修改策略组中的策略项	√	x
workspace:policy Groups:listTargets	GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	查询策略组应用对象	√	x
workspace:policy Groups:updateTargets	PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	修改策略组应用对象	√	x
workspace:policy Groups:listDetail	GET /v2/{project_id}/policy-groups/detail	查询策略组详情列表	√	x
workspace:policy Groups:getQuotas	GET /v2/{project_id}/policy-groups/quotas	查询策略组上限数量	√	x
workspace:policy Groups:getMaxPriority	GET /v2/{project_id}/policy-groups/max-priority	查询策略组最大优先级	√	x
workspace:policy Groups:getOriginalPolicies	GET /v2/{project_id}/policy-groups/original-policies	查询初始策略项	√	x
workspace:policy Groups:createTemplate	POST /v2/{project_id}/policy-groups/policy-template	创建策略模板	√	x
workspace:policy Groups:updateTemplate	PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	更新策略模板	√	x
workspace:userGroups:create	POST /v2/{project_id}/groups	创建用户组	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:userGroups:list	GET /v2/{project_id}/groups	查询用户组列表	√	x
workspace:userGroups:update	PUT /v2/{project_id}/groups/{group_id}	修改用户组信息	√	x
workspace:userGroups:delete	DELETE /v2/{project_id}/groups/{group_id}	删除桌面用户组	√	x
workspace:userGroups:batchDelete	POST /v2/{project_id}/groups/batch-delete	批量删除用户组	√	x
workspace:userGroups:operate	POST /v2/{project_id}/groups/{group_id}/actions	操作用户组	√	x
workspace:userGroups:getUsers	GET /v2/{project_id}/groups/{group_id}/users	查询用户组中的用户	√	x
workspace:ous:create	POST /v2/{project_id}/ous	新增OU信息	√	x
workspace:ous:delete	DELETE /v2/{project_id}/ous/{ou_id}	删除OU信息	√	x
workspace:ous:update	PUT /v2/{project_id}/ous/{ou_id}	更新OU信息	√	x
workspace:ous:get	GET /v2/{project_id}/ous	查询OU信息	√	x
workspace:users:create	POST /v2/{project_id}/users	创建用户	√	x
workspace:users:delete	DELETE /v2/{project_id}/users/{user_id}	删除指定用户	√	x
workspace:users:update	PUT /v2/{project_id}/users/{user_id}	修改用户信息	√	x
workspace:users:list	GET /v2/{project_id}/users	查询用户列表	√	x
workspace:users:get	GET /v2/{project_id}/users/{user_id}	查询用户详情信息	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:users:operate	POST /v2/{project_id}/users/{user_id}/actions	操作用户 (锁定、解锁和重置密码)	√	x
workspace:users:resetPassword	POST /v2/{project_id}/users/password	重置用户密码	√	x
workspace:users:resendEmail	POST /v2/{project_id}/users/{user_id}/resend-email	重新发送邮件	√	x
workspace:users:batchDelete	POST /v2/{project_id}/users/batch-delete	批量删除用户	√	x
workspace:users:uploadTemplate	POST /v2/{project_id}/users/template-upload	上传用户模板文件	√	x
workspace:users:getTemplate	GET /v2/{project_id}/users/desktop-users/template	用户模板下载	√	x
workspace:users:importUser	POST /v2/{project_id}/users/desktop-users/action/import	导入用户列表	√	x
workspace:users:checkExist	POST /v2/{project_id}/users/exist	校验用户是否存在	√	x
workspace:users:listOtps	GET /v2/{project_id}/users/{user_id}/otp-devices	查询OTP设备	√	x
workspace:users:deleteOtps	DELETE /v2/{project_id}/users/{user_id}/otp-devices	解绑OTP设备	√	x
workspace:users:getImportTemplate	GET /v2/{project_id}/users/template/download	创建用户模板下载	√	x
workspace:users:import	POST /v2/{project_id}/users/import	导入用户	√	x
workspace:users:export	POST /v2/{project_id}/users/export	导出用户	√	x
workspace:users:batchCreate	POST /v2/{project_id}/users/batch-create	批量创建用户	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:users:randomPassword	GET /v2/{project_id}/users/{user_id}/random-password	给用户重置随机密码	√	x
workspace:images:list	GET /v2/{project_id}/images	查询产品镜像列表	√	√
workspace:appcenter:listApps	GET /v1/{project_id}/app-center/apps	按照名称分页查询应用	√	x
workspace:appcenter:createApp	POST /v1/{project_id}/app-center/apps	上传应用	√	x
workspace:appcenter:updateApp	PATCH /v1/{project_id}/app-center/apps/{app_id}	修改应用	√	x
workspace:appcenter:deleteApp	DELETE /v1/{project_id}/app-center/apps/{app_id}	删除应用	√	x
workspace:appcenter:installApp	POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	自动安装应用	√	x
workspace:appcenter:listAppAuthorizations	GET /v1/{project_id}/app-center/apps/{app_id}/authorizations	查询应用授权信息	√	x
workspace:appcenter:updateAppAuthorizations	POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	设置应用授权	√	x
workspace:appcenter:batchDeleteApps	POST /v1/{project_id}/app-center/apps/actions/batch-delete	批量删除应用	√	x
workspace:appcenter:batchDisableApps	POST /v1/{project_id}/app-center/apps/actions/batch-disable	批量设置应用不可见	√	x
workspace:appcenter:batchEnableApps	POST /v1/{project_id}/app-center/apps/actions/batch-enable	批量设置应用可见	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:appcenter:batchUpdateAppAuthorizations	POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	批量设置应用授权	√	x
workspace:appcenter:batchInstallApps	POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	批量自动安装应用	√	x
workspace:appcenter:listAppCatalogs	GET /v1/{project_id}/app-center/app-catalogs	查询应用分类信息	√	x
workspace:appcenter:listJobs	GET /v1/{project_id}/app-center/jobs	查询应用安装job信息	√	x
workspace:appcenter:batchDeleteJobs	POST /v1/{project_id}/app-center/jobs/actions/batch-delete	批量删除job	√	x
workspace:appcenter:retryJobs	POST /v1/{project_id}/app-center/jobs/actions/retry	重试失败job	√	x
workspace:appcenter:createAppRule	POST /v1/{project_id}/app-center/app-rules	创建应用规则	√	x
workspace:appcenter:listAppRule	GET /v1/{project_id}/app-center/app-rules	查询应用规则	√	x
workspace:appcenter:updateAppRule	PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	修改应用规则	√	x
workspace:appcenter:deleteAppRule	DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	删除应用规则	√	x
workspace:appcenter:batchDeleteAppRules	POST /v1/{project_id}/app-center/app-rules/batch-delete	批量删除应用规则	√	x
workspace:appcenter:enableRuleRestriction	POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	启用规则管控	√	x

授权项 (Action)	对应API接口	授权项说明	IAM项目 (Project)	企业项目 (Enterprise Project)
workspace:appcenter:disableRuleRestriction	POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	禁用规则管控	√	x
workspace:appcenter:addRestrictedRule	POST /v1/{project_id}/app-center/app-restricted-rules	增加管控规则	√	x
workspace:appcenter:listRestrictedRule	GET /v1/{project_id}/app-center/app-restricted-rules	查询管控规则列表	√	x
workspace:appcenter:deleteRestrictedRule	POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	批量删除管控规则列表	√	x
workspace:appcenter:updateTenantProfile	PATCH /v1/{project_id}/app-center/profiles	启禁用租户功能	√	x
workspace:appcenter:listTenantProfiles	GET /v1/{project_id}/app-center/profiles	查询租户功能状态	√	x
workspace:appcenter:createBucketCredential	POST /v1/{project_id}/app-center/buckets/actions/create-credential	生成OBS桶凭证信息	√	x
workspace:appcenter:createAndAuthorizeBucket	POST /v1/{project_id}/app-center/buckets	添加并授权默认OBS桶	√	x

9 约束与限制

本章节介绍云桌面服务产品功能的使用限制。

表 9-1 云桌面使用限制

场景	限制项	限制说明
购买桌面	账号	只有使用实名认证后的账号登录云桌面控制台才能购买桌面。
	是否对接AD	<ul style="list-style-type: none">购买桌面后，不支持变更是否对接AD。对接AD时，需确保云桌面所在网络与微软AD所在网络互通。
	区域	不同区域的桌面之间内网互不相通，且需分区域管理桌面。
	CPU架构	支持x86计算。
	桌面操作系统	目前支持Windows Server 2016/2019操作系统版本。云桌面将会持续增加操作系统支持范围。
	系统盘	受所选区域资源限制，系统盘大小需设置为80~1020GB。
	数据盘	受所选区域资源限制，最多只能添加10个数据盘，且每个数据盘大小需为10~1020GB之间的10的整数倍。
	网络	云桌面预留172.20.0.0/16~172.31.0.0/16网段作为内部服务运行网段，故请勿选择172开头的VPC网络，否则将无法成功购买桌面。
	分配用户	每个桌面只能属于单个用户。
登录桌面	移动终端	支持安装了Android 6.0以上版本操作系统的移动终端设备登录桌面。
	瘦终端和PC软终端	支持操作系统为Windows 10以及macOS（10.14~12.4，64位）的PC软终端，以及适配的瘦终端（UOS、Android等操作系统）登录桌面。

场景	限制项	限制说明
配置桌面	策略	<ul style="list-style-type: none"> ● 桌面策略会在用户下一次登录桌面后生效。 ● 支持从客户端到服务端或服务端到客户端的单向复制或者双向复制。 <ul style="list-style-type: none"> - 仅在客户端（TC/SC）操作系统和云桌面操作系统均为Windows时，支持富文本复制、文件复制，且最多同时可复制500个文件。 - 当客户端（TC/SC、移动客户端）操作系统或云桌面操作系统为其他时，只支持纯文本格式复制，不支持文件复制。 ● 渲染加速仅适用多媒体视频编辑场景，其它场景不建议打开。 ● 默认策略为预设好的通用策略，且不支持优先级修改。 ● 当您创建多条策略时，默认策略的优先级最低。 ● 单一区域默认的策略配额为50个。
	网络接入方式	<ul style="list-style-type: none"> ● 云桌面可同时支持互联网接入方式和专线接入方式，并且同一时间内至少保持一种接入方式处于开启状态，不可将两种接入方式同时关闭。 ● 云桌面使用172.20.0.0/16~172.31.0.0/16网段为桌面管理网卡的保留网段，使用云专线的方式与企业内网的PC进行通信时，请避免在企业内网使用此网段，以免路由冲突而导致无法互相访问。 ● 使用云专线接入方式需要创建VPC终端节点。
	配置云桌面可访问企业内网	使用防火墙时，需确保防火墙中出方向的8443端口和443端口为放通状态。
	变更规格	● 变更规格过程中，请勿对云桌面进行其他操作。
	重建系统盘	<ul style="list-style-type: none"> ● 重建系统盘前，桌面“登录状态”不为“无法连接”，且“运行状态”为“运行中”或“已停止”。 ● 重建系统盘后，原系统盘中的数据（如桌面，收藏夹等）会丢失，如果需要这些数据，请提前通知用户备份。 ● 重置系统盘时，如果该云桌面使用的私有镜像，需确保该私有镜像仍存在。
管理桌面	重发通知邮件	只在该用户绑定了桌面的情况下，可重新发送通知邮件。
	删除用户	只在该用户未绑定桌面的情况下，可删除用户。
	重置密码	已对接Windows AD域，将无法给桌面用户重置密码。
	解锁用户	已对接Windows AD域，将无法对桌面用户进行解锁。

场景	限制项	限制说明
禁用操作 (Windows 操作系统桌面)	进程和服务	<ul style="list-style-type: none"> 禁止更改系统配置中默认的服务和启动选项。 禁止结束任务管理器中“LOCAL SERVICE”、“NETWORK SERVICE”和“SYSTEM”类进程。 禁止禁用HDP类服务。 禁止卸载以下程序。 <ul style="list-style-type: none"> - Access Agent - Microsoft .NET Framework x Client Profile - Microsoft .NET Framework x Extended - Microsoft Visual C++ xxx Redistributable - xxx
	网络	<ul style="list-style-type: none"> 禁止禁用网卡、禁用或修改网络配置。 禁止执行修改路由的脚本或命令，如route DELETE*。 禁止在Windows防火墙例外选项中删除28511、28512、28521和28522端口。 禁止打开IPsec等具有禁用网络流量功能的软件或工具。
	其他	<ul style="list-style-type: none"> 禁止删除“C:\Program Files\Huawei”目录下的文件和文件夹。 禁止对桌面执行睡眠操作，桌面默认不启用睡眠操作。 禁止修改HDP客户端（Access Agent）配置文件。 禁止运行魔法兔子或Windows优化大师等软件对注册表进行清理和优化。 自定义安装具有变换功能的屏保会消耗大量系统资源，导致用户重新进入桌面时会有一定延迟，请慎重操作。
云桌面使用	云桌面访问互联网	云桌面是通过绑定数据中心的IP进行互联网访问，部分娱乐类的网站基于自身运营的需要，会对数据中心IP访问进行限制，导致的结果是云桌面无法访问相关的网站，目前识别到的有是优酷、淘宝等网站。

10 套餐与计费

计费概述

购买云桌面时，用户指定的云桌面实例规格决定了实例的主机硬件配置。云桌面实例提供丰富多样的规格，每一个实例类型提供不同的计算能力，您可以基于需要提供的服务规模而选择实例计算能力、存储空间，您可灵活地为您的使用场景选择适当的资源。

计费模式

云桌面的规格包括计算资源（vCPU、内存）和存储资源（系统盘、数据盘）。您可以根据业务中接入用户规划及云桌面使用场景规划，来决定您购买云桌面实例规格、数量及区域分布，以便为您的用户提供最优的云桌面服务。云桌面支持包年包月计费模式和按需计费模式供您灵活选择。

- **包年包月：**华为云提供包月和包年的购买模式。这种购买方式相对于按需付费则能够提供更大的折扣，对于长期使用者，推荐该方式。包年/包月计费按照订单的购买周期来进行结算。

适用场景：适合稳定长期使用云桌面资源的场景，相对于按需付费则能够提供更大的折扣。

- **按需计费：**按需申请云桌面资源使用，实例从“开通”开启计费到“删除”结束计费，按实际购买时长（精确到秒）计费即开即停，支持变更为包年/包月资源，具体详情参考云桌面《用户指南》的“桌面计费模式变更（按需转包周期）”章节。

适用场景：适合短期业务需求的场景使用，可按需开关机释放实例计算资源，节省成本。

计费规则：

按需购买的实例支持关机/休眠不计费，关机/休眠后的计费规则：

- 实例本身（vCPU，内存，镜像）不计费，其它所挂载的资源如云硬盘，公网IP或带宽则正常计费。
- 按需计费云桌面支持关机/休眠不计费，即关机/休眠期间，在保留云桌面的前提下，系统将自动回收计算资源（vCPU、内存）。此时，将不再收取计算资源相关费用，仅收取存储资源（系统盘和数据盘）费用，可以降低您的使用成本，再次

启动时会重新申请vCPU和内存，在资源不足时会有启动失败的风险，您可以通过稍后启动或更改实例规格的方式来恢复。

- 按需计费的特殊实例不支持关机/休眠不计费。特殊实例关机/休眠后仍然正常收费，同时vCPU和内存等资源也会保留。

📖 说明

不支持关机不计费的特殊实例包括：

- 含本地盘的实例，如磁盘增强型实例、超高I/O型实例等。
- 公网/私网NAT网关根据您选择的公网NAT网关规格和使用时长计费。详细的价格说明请参考[NAT网关价格计算器](#)。
- 除特殊公共镜像，其他公共镜像为免费，如果公共镜像转为私有镜像，则会根据云市场价格收取镜像费用。
- 云桌面删除或者退订（具体操作请参考云桌面《用户指南》的“桌面退订”章节），桌面的弹性公网IP会自动解绑、弹性公网IP会继续保留并计费，请前往[弹性公网IP](#)页面手动删除。
- 应用中心中文件使用OBS存储时进行计费，详情参考 [对象存储服务 OBS](#)的计费说明。

云桌面的计费量纲

资源不同，计费单位不同。如[表10-1](#)所示，记录了云桌面相关资源的计费单位。

表 10-1 计费量纲

资源	计费单位
云桌面套餐	台/年、月、小时
云系统盘	GB/年、月、小时
云数据盘	GB/年、月、小时

云桌面的计费方式

不同区域支持的计费类型可参考[云桌面价格计算器](#)，具体请以实际购买云桌面页面显示为准。

表 10-2 云桌面计费方式

计费模式	计费方式	计费周期
包年/包月	先购买再使用，用户在购买时，系统会根据用户所选的套餐对用户云账户中的金额进行扣除。	计费周期以UTC+8时区的时间为准。计费周期的起点是资源开通的时间点（精确到秒），终点是指定使用时长后的第一个00:00:00。

计费模式	计费方式	计费周期
按需计费	先使用后扣款，后台会依据用户在区间时间段内使用时长，对用户云账户中的金额进行扣除。	以整点小时为计费周期，计费周期以UTC+8时区的时间为准。使用过程中，系统在每个整点时间（如2:00:00，3:00:00）会自动出账单核算区间时间内使用时长所需费用。

📖 说明

- 订单到期后，提供7天的宽限期，宽限期内资源依然可用。
- 宽限期后，提供15天的保留期，保留期内资源不可用，但并未删除。
- 保留期后，如果您没有续费订单，资源将自动删除。

变更配置

- 变更计费模式
支持按需变更为包年/包月。按需变更为包年/包月，会生成新的订单，用户支付订单后，包年/包月资源立即生效。具体变更操作请参见[桌面计费模式变更（按需转包周期）](#)。
- 变更桌面规格
计费周期内可通过[变更规格](#)功能，更改云桌面的vCPU和内存大小。

续费

一个计费周期到期后，用户可以选择续费，继续使用资源，也可以选择中止服务。如需续费，请参考[为包年/包月桌面续费](#)。或者参考[续费管理](#)在管理控制台[续费管理](#)页面进行续费操作。

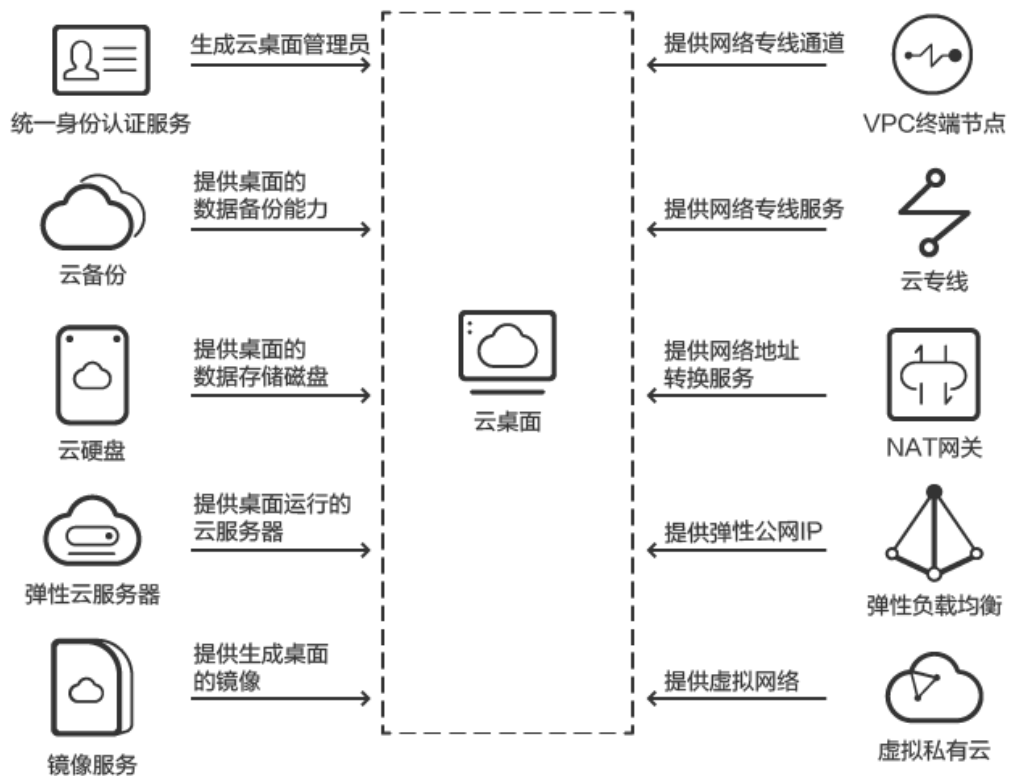
到期与欠费

欠费后，可以查看欠费详情。为防止相关资源被停止或者释放，请及时进行充值，账号将进入欠费状态，需要在约定时间内支付欠款，详细操作请参考[充值还款](#)。

11 云桌面与其他服务的关系

云桌面与周边服务的依赖关系如图11-1所示。

图 11-1 云桌面与其他服务的关系



弹性云服务器

弹性云服务器（Elastic Cloud Server, ECS）由CPU、内存、镜像、云硬盘组成，是一种可随时获取、弹性可扩展的计算服务器。为云桌面服务提供桌面运行的云服务器。

镜像服务

镜像服务（Image Management Service, IMS）提供简单方便的镜像自助管理功能。为云桌面服务提供生成桌面的镜像。

云硬盘

云硬盘（Elastic Volume Service, EVS）提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，可满足不同场景的业务需求。为云桌面提供数据存储能力。

云备份

云备份（Cloud Backup and Recovery, CBR）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。保障用户数据的安全性和正确性，确保业务安全。为云桌面服务提供数据备份能力。

弹性负载均衡

弹性负载均衡（Elastic Load Balance, ELB）通过将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。ELB是从互联网访问云桌面的入口，为云桌面服务提供弹性公网IP。

虚拟私有云

虚拟私有云（Virtual Private Cloud, VPC）提供和传统网络一样的虚拟网络以及先进的网络服务，如弹性IP、安全组和虚拟专用网。虚拟私有云在逻辑上实现网络隔离并且为云桌面提供安全、隔离的网络环境。为云桌面服务提供虚拟私有网络。

VPC 终端节点

VPC终端节点（VPC Endpoint）是将VPC私密地连接到终端节点服务（云服务、用户私有服务），使VPC中的云资源无需弹性IP就能够访问终端节点服务。本地数据中心可以通过VPN或者云专线，利用建立的终端节点通过内网访问云服务，可以提高访问效率，节约使用成本，更加便捷安全。为云桌面服务提供连接其他服务的云专线通道。

NAT 网关

NAT网关（NAT Gateway）能够为虚拟私有云内的云桌面桌面提供网络地址转换（Network Address Translation）服务，使多个云桌面桌面可以共享使用弹性IP（EIP）访问Internet。

统一身份认证服务

统一身份认证服务（Identity and Access Management, IAM）是华为云提供权限管理的基础服务，可以帮助您安全地控制云服务和资源的访问权限。管理员通过IAM创建账号后，可以精细控制云桌面相关资源的访问范围。

云专线

云专线服务（Direct Connect, DC）是一个建立连接本地数据中心和云平台的专线网络服务。该服务能够有效地降低云桌面的网络时延，让用户获得比Internet线路更好的桌面体验。

A 修订记录

发布日期	更新说明
2024-10-16	第八次正式发布。 新增： 7 安全 章节。
2024-03-19	第七次正式发布。 修改： 9 约束与限制 中云桌面支持的网段。
2024-01-03	第六次正式发布。 新增： 8.1 权限和授权项 新增应用中心细粒度权限内容。
2023-08-25	第五次正式发布。 新增： 套餐与计费章节新增计费说明。
2023-07-11	第四次正式发布。 修改： 去掉 10 套餐与计费 章节中的套餐内容。
2023-07-03	第三次正式发布。 新增： 8 权限管理 新增支持IAM细粒度鉴权。
2023-06-15	第二次正式发布。 修改： 6 支持列表 新增Windows10操作系统版本，增加Windows镜像说明。
2022-12-26	第一次正式发布。