云化数据中心 CloudDC

产品介绍

文档版本 01

发布日期 2025-10-24

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2025。 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


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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

 版权所有 © 华为云计算技术有限公司

1 什么是云化数据中心

什么是云化数据中心（CloudDC）

云化数据中心 (CloudDC)是一种满足传统DC客户云化转型诉求的产品，支持将客户持有服务器设备部署至华为云机房，通过外溢华为云的基础设施管理、云化网络、裸机纳管、确定性运维等能力，帮助客户DC快速云化转型。

为什么选择云化数据中心（CloudDC）

- IDC一站式算网存云化：云化数据中心为客户提供多种组件组合方式，为不同云化阶段的客户提供解决方案。
- 全栈AI基础设施使能：云化数据中心针对AI基础设施独有的复杂软件栈、高耗能等特点，可基于客户的AI服务器提供基础设施、云原生软件栈、基础设施调优等一站式的AI基础设施构建能力。
- 全球布局的安全合规云化DC：云化数据中心依托华为云全球存算网基础设施能力，在全球范围内提供稳定、安全的数据中心运行环境。
- 免运维的基础设施管理体验：云化数据中心外溢华为云确定性运维能力，为客户提供数据中心基建、机房环境、计算、存储、网络等基础设施运维能力，使客户可聚焦业务管理，不必关心基础设施底层实现。

产品功能

iRack

iRack为客户提供智能机柜，华为云通过将全球华为云数据中心的资源整合，为客户提供高可靠的机柜基础设施，免除在数据中心建设中的选址、基建、机房风火水电的投入，快速上线业务。

客户可通过CloudDC的控制台实时查询机柜的分布、数量与运行状态。

iMetal

iMetal是对客户资产服务器的纳管，纳管之后客户可以直接在iMetal界面上查看服务器的基础信息，并对服务器进行OS安装。iMetal服务对于周边的依赖，主要有2部分：

- CloudDCN：iMetal纳管必须要搭配CloudDCN，通过CloudDCN控制网络，创建VPC和CloudDCN子网。CloudDCN提供API接口供iMetal调用，创建网络服务。
- 华为云数据中心运维平台：iMetal服务器的基础信息，存在于CMDB中；iMetal通过将华为云数据中心的CMDB重新组织以适合客户理解的维度呈现至CloudDC控制台。

版权所有 © 华为云计算技术有限公司

CloudDCN云化网络

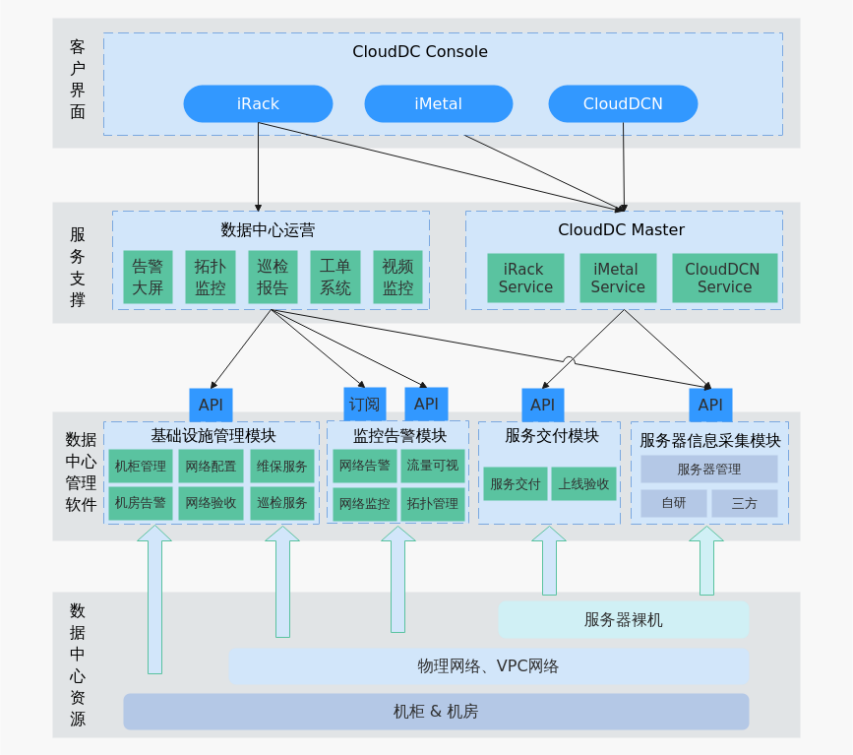
CloudDCN为CloudDC提供网络服务能力：

- VPC网络连通：提供CloudDC专区与华为公有云之间的网关。
- AI参数面网络：为CloudDC专区AI集群建设提供参数面网络。

产品架构

CloudDC通过外溢华为云数据中心能力，对客户提供数据中心管理服务，主要分为四个层次，如图1-1。

图 1-1 CloudDC 产品架构



数据中心资源

华为云数据中心通过将机房/机柜资源、物理网络/VPC网络资源、客户部署的裸机资源整合，为客户提供IT基础设施服务。

数据中心管理软件

- 基础设施管理模块：复用华为云数据中心现有能力，为客户提供机房、机柜、网络资源的建设、管理服务。
- 监控告警模块：复用华为云数据中心现有能力，为客户提供网络基础设施的流量监控与拓扑管理，辅助基础设施运维。
- 服务交付模块：复用华为云数据中心现有能力，对客户资产的第三方服务器进行工程实施，交付上线。
- 服务器信息采集模块：复用华为云数据中心现有能力，对服务器的运行状态进行管理。

版权所有 © 华为云计算技术有限公司

服务支撑

- 数据中心运营：整合华为云数据中心底层基础设施管理模块信息呈现，并提供CloudDC运维能力。
- CloudDC Master：由iRack Service、iMetal Service、CloudDCN Service构成，为CloudDC控制台提供接口调用服务。

CloudDC 控制台（Console）

客户界面CloudDC通过整合iRack、iMetal、CloudDCN为客户提供统一的操作管理界面，客户可以通过界面对CloudDC进行状态管理、资源管理和运维操作。

访问方式

公有云提供了Web化的服务管理平台，即管理控制台管理方式。

可使用管理控制台方式访问云化数据中心（CloudDC）Console控制台。

如果用户已注册公有云，可直接登录管理控制台，从主页选择“CloudDC”。如果未注册，请参见**注册华为账号并开通华为云**。

版权所有 © 华为云计算技术有限公司

2 产品优势

IDC 一站式算网存云化

- 平滑云化：利旧资产，平滑切换入云，云化改造周期缩短三分之一。
- 服务化管理：计算、网络、存储服务化使用，按需组合。
- 无缝协同：与公有云服务同机房部署，低时延访问公有云服务。

全栈 AI 基础设施使能

- 全栈方案：一站式AI基础设施部署，高效云边协同。
- AI最佳底座：智能机柜与200G服务化网络提供最佳AI基础设施运行环境。
- 持续优化：丰富AI基础设施调优经验，万卡线性度>90%。

全球布局的安全合规云化 DC

- 广泛覆盖：全球14+国家/地区，23+可用区广泛覆盖。
- 极致可靠：Tier3+高标准建设机房，全流程数据中心建设认证评价体系。
- 安全可信：一个中心+七层防线，公有云等同的纵深防御体系。

免运维的基础设施管理体验

- 专业专注：170+全球服务中心，30年ToB服务经验。
- 化繁为简：卸载繁杂基础设施管理任务，7*24小时代维守护。
- 全景洞悉：数据中心运行状态全景数字化可视。

版权所有 © 华为云计算技术有限公司

3 应用场景

3.1 DC 云化

场景描述

通过纳管用户自有资产，并低时延的连通至华为公有云服务，实现数据中心基础设施云化管理、CloudDC专区业务与华为公有云弹性协同，灵活应对业务高峰。

版权所有 © 华为云计算技术有限公司

场景价值

- 低时延：CloudDC专区与华为公有云服务同机房部署，享有华为公有云等同时延，就近访问云服务。
- 高弹性：统一调度CloudDC专区与华为公有云算力资源，业务秒级弹性上云。
- 易管理：数据中心基础设施、服务器算力资源、网络资源、容器资源华为云统一管理。

关键组件

- 智能机柜（iRack）：提供风冷智能机柜服务。
- 机房服务（确定性运维）：提供协维、维保、安全改造、工程交付等专业服务。
- 三方裸机纳管（iMetal）：提供用户自有服务器纳管服务，以裸金属方式发放资源。
- 网络服务（CloudDCN）：提供CloudDC专区网络建设、CloudDC专区与华为公有云VPC连通服务。

搭配使用

- 分布式云原生 UCS
- 云容器引擎 CCE
- 云容器实例 CCI
- Huawei Cloud EulerOS

3.2 全栈 AI

场景描述

通过纳管客户自有的AI设备，结合华为公有云算网存的全栈AI基础设施交付模式，帮助客户快速实现AI资产投入业务运行。

版权所有 © 华为云计算技术有限公司

场景价值

- 高密度：智能机柜，适配不同AI设备的能耗要求，PUE1.1。
- 高性能：200G服务化参数面网络，按需分配，灵活组网，微秒级时延。
- 自优化：拓扑感知的AI容器，资源分配率与通信效率双提升。

关键组件

- 智能机柜（iRack）：提供智能机柜服务。
- 机房服务（确定性运维）：提供AI基础设施建设的咨询、实施、代维、调优服务。
- 云化AI网络(MatrixLink)：提供大规模、高效率、高可靠的AI网络。
- AI容器（CCE）：提供全局统一调度的AI容器运行环境。

搭配使用

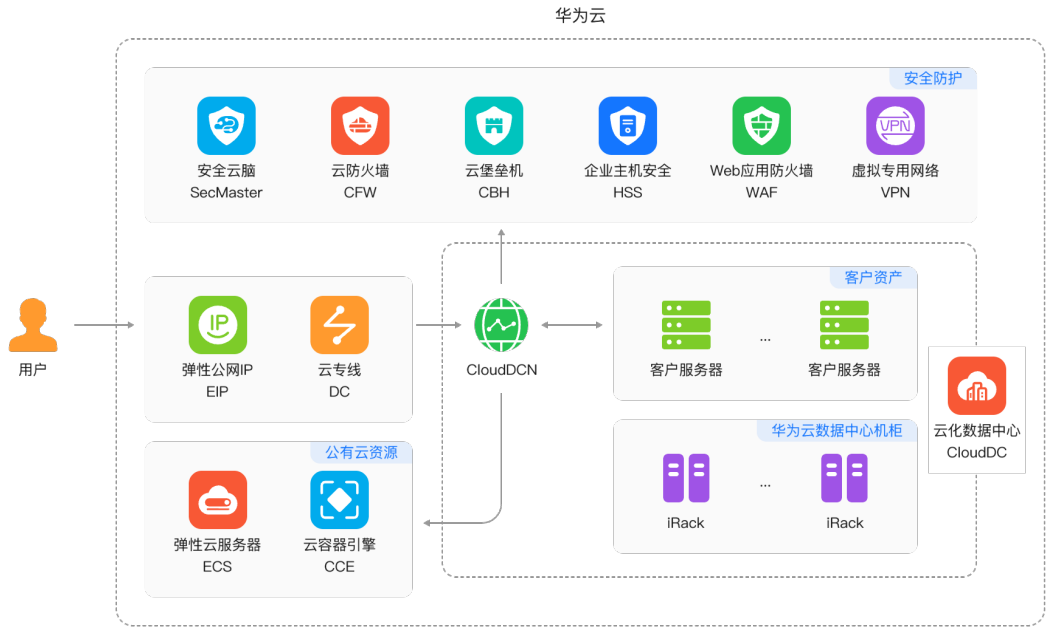
- 云容器引擎 CCE
- 分布式云原生 UCS

3.3 中资出海

场景描述

通过将客户资产部署至华为云全球广泛覆盖的数据中心中，帮助客户快速在海外构建IT基础设施能力。

版权所有 © 华为云计算技术有限公司



场景价值

- 广覆盖：全球14+国家/地区，23+可用区广泛覆盖，业务购买可用，无需选址基建。
- 高可靠：多AZ高可靠设计，法规遵从的云化DC，快速满足行业规范与法规要求。
- 强安全：复用华为云1+7纵深防御体系，使出海离散站点具备大型数据中心等同防护能力。

关键组件

- 智能机柜（iRack）：提供风冷智能机柜服务。
- 机房服务（确定性运维）：提供中资出海咨询、部署、代维服务。
- 数据中心管理平台(DCOS)：提供远程离散站点统一管理、运维、工单平台。

搭配使用

- 安全云脑 SecMaster
- 云防火墙 CFW
- 云堡垒机 CBH
- 企业主机安全 HSS
- Web应用防火墙 WAF
- 虚拟专用网络 VPN

版权所有 © 华为云计算技术有限公司

4 产品功能

本页面介绍了CloudDC服务支持的主要功能。关于各功能支持的地域（Region）信息，可通过控制台查询详情。

购买 iRack 机柜

您可以通过管理控制台购买iRack机柜，快速获取高可靠的数据中心运行环境，免除传统数据中心选址、基建、风火水电改造、运维运营等长周期投入。有关更多信息，请参阅**购买iRack机柜**。

管理 iRack 机柜

您可以通过控制台查看iMetal服务器所属的iRack机柜信息，支持按iRack机柜查看iMetal服务器信息，也支持导入和导出iRack机柜信息。有关更多信息，请参阅**管理iRack机柜**。

管理机房

您可以通过控制台查看iMetal服务器的部署机房信息，支持按机房查看iMetal服务器信息，也支持将所有机房数据以.xlsx文件的形式导出至本地。有关更多信息，请参阅**管理机房**。

创建 iMetal 服务器

您可以通过管理控制台创建iMetal服务器，将已有的服务器资产纳管并连通到华为公有云，实现低时延访问公有云服务，并在业务波峰时弹性扩展至公有云，增强业务弹性。有关更多信息，请参阅**创建iMetal服务器**。

查看 iMetal 服务器

您可以通过管理控制台查看iMetal服务器的状态及详细信息，也可以导出全部或者指定iMetal服务器信息。有关更多信息，请参阅**查看iMetal服务器**。

登录 iMetal 服务器

您可以选择合适的方法登录iMetal服务器：Windows：使用管理控制台的“远程登录”，登录凭证方式为密码；Linux&Windows：使用SSH等远程连接工具，登录凭证方式为密码。有关更多信息，请参阅**登录iMetal服务器**。

版权所有 © 华为云计算技术有限公司

管理 iMetal 服务器

您可以通过管理控制台管理iMetal服务器，包括重置密码、开机、关机、重启、导出日志等操作。有关更多信息，请参阅**管理iMetal服务器**。

操作系统管理

您可以通过管理控制台为iMetal服务器安装或卸载操作系统。

安装操作系统：为iMetal服务器安装镜像、网络以及设置远程登录密码。有关更多信息，请参阅**安装iMetal服务器操作系统**。

卸载操作系统：当iMetal服务器操作系统无法正常运行时，您可以通过卸载并重新安装iMetal服务器操作系统的方式进行修复。有关更多信息，请参阅**卸载iMetal服务器操作系统**。

监控 iMetal 服务器

iMetal服务器支持带外监控。您可以通过带外监控数据获取服务器的健康状态以及运行信息等，及时发现并定位故障。有关更多信息，请参阅**监控iMetal服务器**。

审计 iMetal 服务器

通过云审计服务，您可以审计iMetal服务器的关键操作，查看审计日志。有关更多信息，请参阅**使用CTS审计iMetal服务器**。

CloudDCN 子网

您可以将自有的物理服务器（iMetal服务器）接入到云上的私有网络中，通过CloudDCN子网，您可以快速为iMetal服务器构建隔离，私密、高性能的虚拟网络环境。有关更多信息，请参阅**CloudDCN子网**。

CloudDCN 专用网络 ACL

CloudDCN专用网络ACL是一个子网级别的可选安全防护层，您可以在CloudDCN专用网络ACL中设置入方向和出方向规则，并将CloudDCN专用网络ACL绑定至CloudDCN子网，可以精准控制出入CloudDCN子网的流量。有关更多信息，请参阅**CloudDCN专用网络ACL**。

弹性网卡和辅助弹性网卡

弹性网卡即虚拟网卡，在您创建iMetal服务器时，随iMetal服务器会默认创建弹性网卡。您无法解除弹性网卡和iMetal服务器的绑定关系。

辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，您可以通过创建辅助弹性网卡，使单个iMetal服务器挂载更多网卡，实现灵活、高可用的网络方案配置。

有关更多信息，请参阅**弹性网卡和辅助弹性网卡**。

版权所有 © 华为云计算技术有限公司

5 实例规格

5.1 iRack 机柜

CloudDC解决方案面向不同业务场景，提供多种类型的iRack机柜。

表 5-1 支持机柜规格

机柜参数	规格
机柜尺寸	600mm(宽度)*1200mm(深度)*2200mm(高度)
机柜高度	47U
额定功率	不同区域和机房支持的机柜功率不同，请以控制台界面支持规格为准。
散热技术	风冷机柜/液冷机柜

5.2 CloudDCN 云化网络

CloudDC解决方案面向不同业务场景，提供多种规格的CloudDCN云化网络。

表 5-2 支持网络规格

网络参数	CloudDCN通用网络	CloudDCN智算网络
网卡规格	不同区域和机房支持的网卡规格不同，请以控制台界面支持规格为准。	200G

版权所有 © 华为云计算技术有限公司

6 安全

6.1 责任共担

华为云秉承“将公司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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图6-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

版权所有 © 华为云计算技术有限公司

图 6-1 华为云安全责任共担模型

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图6-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

6.2 身份认证与访问控制

身份认证

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助用户安全地控制云服务和资源的访问权限。

CloudDC支持通过IAM权限策略进行访问控制。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。

版权所有 © 华为云计算技术有限公司

管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予CloudDC所需的权限，组内用户自动继承用户组的所有权限。

- IAM的详细介绍，请参见**IAM功能介绍**。
- CloudDC所需的权限，请参见**权限管理**。

访问控制

CloudDC通过网络ACL对整个CloudDCN子网进行防护。网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。

华为云提供了管理网络ACL和网络ACL规则的功能：创建网络ACL、查看网络ACL、修改网络ACL、删除网络ACL、开启/关闭网络ACL、关联/解除子网和网络ACL、添加网络ACL规则、修改网络ACL规则、修改网络ACL规则生效顺序、开启/关闭网络ACL规则、删除网络ACL规则等。

用户可以通过与子网关联的出方向/入方向规则控制出入子网的数据流。

6.3 审计与日志

审计

云审计服务，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后，CTS可记录CloudDC的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。
- CloudDC支持审计的操作事件，请参见**表6-1**。

说明

镜像服务（IMS）支持的相关审计操作，请参见**IMS支持审计的关键操作列表**。

表 6-1 CloudDC 服务支持审计的操作

支持的服务	操作名称	资源类型
CTS	更新iRack实例	irack
CTS	创建iRack资源标签	irack
CTS	删除iRack资源标签	irack
CTS	修改机房IDC描述	idcs
CTS	安装imetal资源操作系统	imetal
CTS	切换imetal资源操作系统	imetal
CTS	卸载imetal资源操作系统	imetal
CTS	创建imetal资源标签	imetal
CTS	删除imetal资源标签	imetal

版权所有 © 华为云计算技术有限公司

支持的服务	操作名称	资源类型
CTS	更改imetal ip	imetal
CTS	日志下载导出	imetal
CTS	重置密码	imetal
CTS	开关机、重启	imetal

日志

CloudDC支持上报iMetal服务器的BMC事件和告警到CloudDC控制台，同时支持通过CloudDC控制台导出iMetal服务器的BMC硬件日志，用于协助服务器的日常运维及问题诊断。

关于iMetal服务器日志导出的详细介绍，请参见**导出iMetal服务器的日志**。

版权所有 © 华为云计算技术有限公司

7 约束与限制

iRack 使用限制

- 不支持将客户自有的波分等传输设备部署在云化数据中心。
- 部署设备仅支持使用双电源设备或转换器。
- 裸机纳管设备需要至少有一年以上硬件维保。

iMetal 使用限制

- 不支持直接加载外接硬件设备（如USB设备、银行U key、外接硬盘、加密狗等）。
- 仅支持部署指定厂商的设备。
- 禁止升级OS自带内核版本，否则服务器硬件驱动会存在兼容性风险，影响服务器可靠性。

版权所有 © 华为云计算技术有限公司

8 与其他服务的关系

CloudDC服务与周边服务的依赖关系如图8-1所示，与其他服务的交互功能请参考表8-1。

图 8-1 CloudDC 服务与其他服务的关系

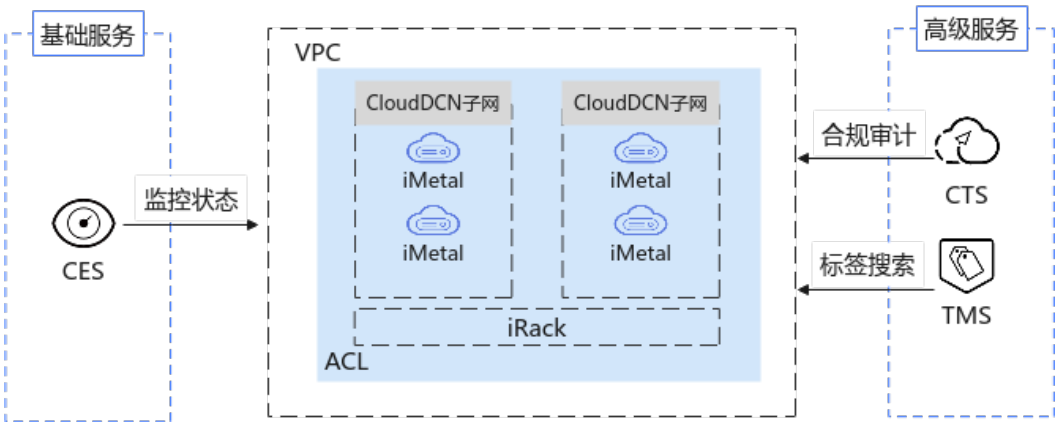


表 8-1 CloudDC 服务与其他服务的关系

服务名称	CloudDC服务与其他服务的关系	主要交互功能
虚拟私有云（Virtual Private Cloud，VPC）	为iMetal服务器提供一个逻辑上完全隔离的专有网络。用户可以通过VPC方便地管理、配置内部网络，进行安全、快捷的网络变更。同时，用户可以通过网络ACL控制访问规则，加强iMetal服务器的安全保护。	创建网络ACL 创建CloudDCN子网
云监控（Cloud Eye，CES）	当用户购买了iMetal服务器后，即可查看对应服务的实例状态。	监控iMetal服务器

版权所有 © 华为云计算技术有限公司

服务名称	CloudDC服务与其他服务的关系	主要交互功能
云日志服务（Log Tank Service，LTS）	记录与imetal服务器相关的操作事件，便于日后的查询、审计和回溯。	支持云审计的关键操作
标签管理服务（Tag Management Service，TMS）	使用标签来标识iMetal服务器，便于分类和搜索。	添加标签 使用标签检索资源

版权所有 © 华为云计算技术有限公司

9 权限管理

如果您需要对华为云上购买的云化数据中心（CloudDC）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用CloudDC服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有云化数据中心（CloudDC）的使用权限，但是不希望他们拥有退订CloudDC资源等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用CloudDC，但是不允许退订CloudDC资源的权限，控制他们对CloudDC资源的使用范围。

目前IAM支持两类授权，一类是策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 9-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
策略授权	用户-权限-授权范围	• 系统策略 • 自定义策略	为主体授予策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

版权所有 © 华为云计算技术有限公司

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	• 系统身份策略 • 自定义身份策略	• 为主体授予身份策略 • 身份策略附加至主体	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快速地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的CloudDC和华南-广州区域的CloudDC的权限，基于策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在身份策略中通过条件键“g:RequestedRegion”的配置即可达到身份策略对于授权区域的控制。将身份策略附加主体或为主体授予该身份策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，云化数据中心 (CloudDC)服务支持使用**身份策略权限管理**方式。推荐使用身份策略进行授权。策略权限管理和**身份策略权限管理**分别介绍两种模型的系统权限。

关于IAM的详细介绍，请参见**IAM产品介绍**。

身份策略权限管理

CloudDC服务支持身份策略授权。如**表9-2**所示，包括了CloudDC身份策略中的所有系统身份策略。身份策略授权场景的系统身份策略与策略授权场景的并不互通。

表 9-2 CloudDC 系统身份策略

系统身份策略名称	描述	策略类别
CloudDCFullAccessPolicy	云化数据中心服务的所有权限	系统身份策略
CloudDCReadOnlyPolicy	云化数据中心服务的只读权限	系统身份策略
CloudDCConsoleFullAccessPolicy	云化数据中心服务控制台所有权限	系统身份策略
CloudDCConsoleReadOnlyPolicy	云化数据中心服务控制台只读权限	系统身份策略

表9-3列出了云化数据中心（CloudDC）常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

版权所有 © 华为云计算技术有限公司

说明

根据IAM权限安全原则，CBC资费和OBS桶相关权限不可添加到FullAccess系统策略中，若需使用相关权限，请使用**自定义策略**添加相关权限，服务依赖权限可参见**表9-4**。

表 9-3 常用操作与系统身份策略的关系

操作	CloudDCFullAccessPolicy	CloudDCReadOnlyPolicy	CloudDCConsoleFullAccessPolicy	CloudDCConsoleReadOnlyPolicy
批量查询物理服务器	√	√	√	√
查询物理服务器信息	√	√	√	√
查询服务器硬件详细信息	√	√	√	√
查询服务器固件详细信息	√	√	√	√
修改物理服务器电源状态	√	×	√	×
导出服务器日志请求	√	×	√	×
查询日志导出状态	√	√	√	√
下载日志文件	√	×	√	×
获取console地址信息	√	×	√	×
批量创建裸机实例	√	×	√	×
批量查询裸机实例	√	√	√	√
批量删除裸机实例	√	×	√	×
创建裸机实例	√	×	√	×
删除裸机实例	√	×	√	×

版权所有 © 华为云计算技术有限公司

操作	CloudDCFullAccessPolicy	CloudDCReadOnlyPolicy	CloudDCConsoleFullAccessPolicy	CloudDCConsoleReadOnlyPolicy
修改裸机实例密码	√	×	√	×
重新安装裸机实例OS	√	×	√	×
查询裸机实例状态	√	√	√	√
修改裸机实例ip	√	×	√	×
查询资源实例列表	√	√	√	√
查询资源标签	√	√	√	√
查询项目标签	√	√	√	√
查询实例数量	√	√	√	√
批量创建资源标签	√	×	√	×
批量删除资源标签	√	×	√	×
服务器概览	√	√	√	√
服务器告警概览	√	√	√	√
服务器告警趋势	√	√	√	√
服务器告警列表	√	√	√	√
服务器事件列表	√	√	√	√
查询事件定义	√	√	√	√
更新/创建服务器维修数据	√	×	√	×
服务器维修数据查询	√	√	√	√

版权所有 © 华为云计算技术有限公司

操作	CloudDCFullAccessPolicy	CloudDCReadOnlyPolicy	CloudDCConsoleFullAccessPolicy	CloudDCConsoleReadOnlyPolicy
创建与更新备件	√	×	√	×
备件查询	√	√	√	√
修改 iRack 描述	√	×	√	×
查询 iRack 实例列表	√	√	√	√
修改 IDC 描述	√	×	√	×
查询 IDC 列表	√	√	√	√
查询机柜实例列表	√	√	√	√
查询机柜标签	√	√	√	√
查询机柜项目标签	√	√	√	√
查询机柜实例数量	√	√	√	√
批量创建机柜标签	√	×	√	×
批量删除机柜标签	√	×	√	×
校验机柜下单参数	√	×	√	×

CloudDC 控制台功能依赖的身份策略权限

表 9-4 CloudDC 控制台依赖服务的身份策略

控制台功能	依赖服务	需配置身份策略
安装OS	镜像服务 IMS	• 支持设置了CloudDCConsoleFullAccessPolicy或CloudDCConsoleReadOnlyPolicy权限的IAM用户直接使用或访问安装OS功能。

版权所有 © 华为云计算技术有限公司

控制台功能	依赖服务	需配置身份策略
CloudDCN云化网络	虚拟私有云 VPC	• 支持设置了CloudDCConsoleFullAccessPolicy或CloudDCConsoleReadOnlyPolicy权限的IAM用户直接使用或访问CloudDCN云化网络。
CloudDC资源标签信息	标签管理服务 TMS	• 支持设置了CloudDCConsoleFullAccessPolicy或CloudDCConsoleReadOnlyPolicy权限的IAM用户直接使用或访问TMS标签服务。
查询/获取监控信息	云监控服务CES	• 支持设置了CloudDCConsoleFullAccessPolicy或CloudDCConsoleReadOnlyPolicy权限的IAM用户直接访问云监控服务，查询监控数据。 **说明** 若用户需要创建告警规则、查看告警列表，自定义监控等依赖CES服务权限的功能，此时用户需要从CloudDC Console切换到CES Console。 具体CES服务的使用与权限配置，请参考**CES服务使用指导**。
支付、查看、续费，退订CloudDC资源	费用中心 CBC	• 支持授权了费用中心服务以下操作权限的IAM用户可直接使用或访问CBC计费服务，进行CloudDC资源的支付、查看、续费和退订操作。 - billing:order:pay：授予支付购买资源的权限。 - billing:order:view：授予可查看订单资源的权限。 - billing:subscription:renew：授予续费、设置自动续费、设置到期策略的权限。 - billing:subscription:unsubscribe：授予查看可退订资源，退订资源的权限。

版权所有 © 华为云计算技术有限公司

控制台功能	依赖服务	需配置身份策略
创建私有镜像	对象存储服务 OBS	• 支持授权了对象存储服务以下操作权限的IAM用户可直接使用或访问OBS对象存储服务，进行CloudDC资源创建镜像操作。 - obs:object:getObject：授予下载非指定版本对象的权限。 - obs:object:getObjectAcl：授予不指定版本获取对象的ACL的权限。 - obs:bucket:getBucketAcl：授予获取桶ACL的权限。 - obs:bucket:getBucketLocation：授予查询桶区域位置信息的权限。 - obs:bucket:listBucket：授予获取桶内对象列表的权限。 - obs:bucket:headBucket：授予获取桶元数据的权限。 - obs:bucket:listAllMybuckets：授予查询创建的桶列表的权限。

版权所有 © 华为云计算技术有限公司

10 区域和可用区

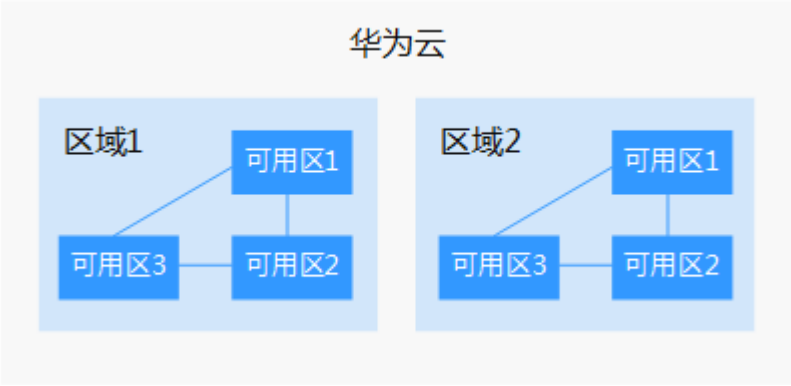
什么是区域、可用区?

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 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10-1阐明了区域和可用区之间的关系。

图 10-1 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。更多信息请参见华为云全球站点。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

版权所有 © 华为云计算技术有限公司

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

    说明

    “拉美-圣地亚哥”区域位于智利。

- 资源的价格

  不同区域的资源价格可能有差异，请参见华为云服务价格详情。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

版权所有 © 华为云计算技术有限公司