

裸金属服务器

产品介绍

文档版本 15
发布日期 2022-11-15



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。

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 什么是裸金属服务器	1
2 裸金属服务器的优势	4
3 使用场景	5
4 实例	6
4.1 实例家族	6
4.2 x86 V4 实例（CPU 采用 Intel Broadwell 架构）	6
4.3 x86 V5 实例（CPU 采用 Intel Skylake 架构）	9
4.4 x86 V6 实例（CPU 采用 Intel Cascade Lake 架构）	12
4.5 鲲鹏 V1 实例	13
4.6 实例生命周期	14
5 镜像	16
5.1 镜像概述	16
5.2 裸金属服务器类型与支持的操作系统版本	18
6 云硬盘	23
7 网络	25
8 安全	28
8.1 责任共担	28
8.2 身份认证与访问控制	29
8.3 数据保护技术	31
8.4 审计与日志	32
8.5 监控安全风险	32
8.6 认证证书	32
9 计费	34
9.1 计费说明	34
10 BMS 权限管理	36
11 区域和可用区	39
12 裸金属服务器与其他服务的关系	41
13 支持列表和使用限制	43

14 修订记录..... 45

1 什么是裸金属服务器

裸金属服务器介绍

裸金属服务（Bare Metal Server，BMS）是一款兼具弹性云服务器和物理机性能的计算类服务，为您和您的企业提供专属的云上物理服务器，为核心数据库、关键应用系统、高性能计算、大数据等业务提供卓越的计算性能以及数据安全。租户可灵活申请，按需使用。

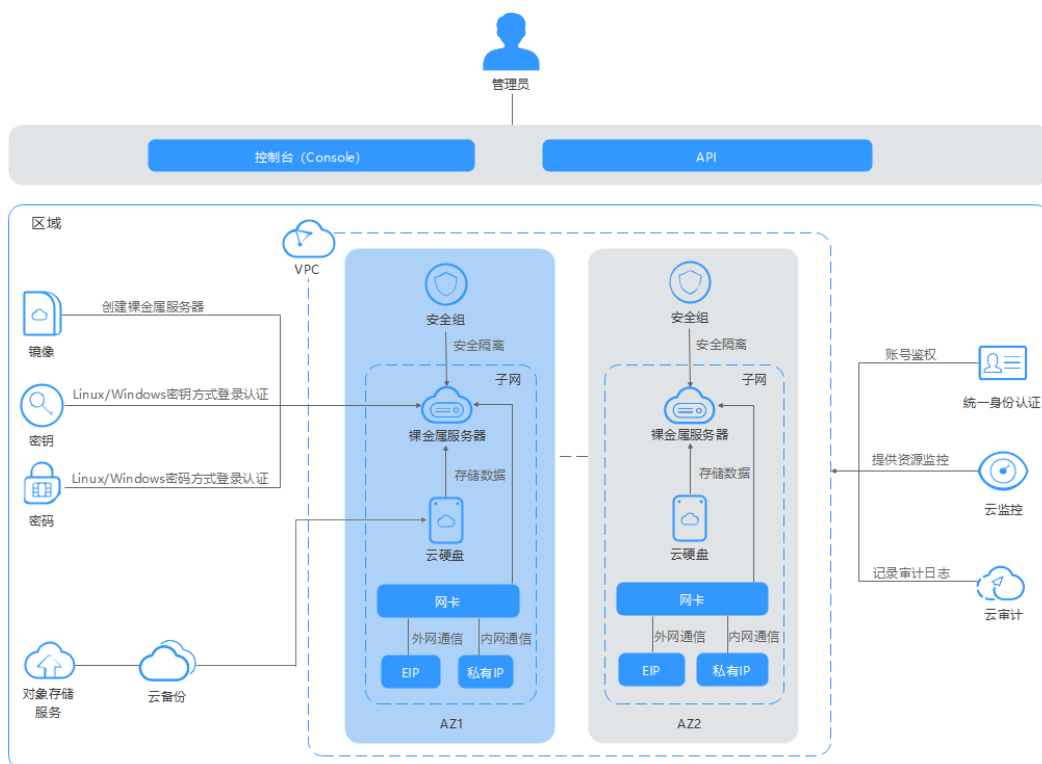
裸金属服务器的开通是自助完成的，您只需要指定具体的服务器类型、镜像、所需要的网络配置等，即可在30min内获得所需的裸金属服务器。服务器供应、运维工作交由华为云，您可以专注于业务创新。

产品架构

通过和其他服务组合，裸金属服务器可以实现计算、存储、网络、镜像安装等功能：

- 裸金属服务器在不同可用区中部署（可用区之间通过内网连接），部分可用区发生故障后不会影响同一区域内的其他可用区。
- 可以通过虚拟私有云（Virtual Private Cloud，VPC）建立专属的网络环境，设置子网、安全组，并通过弹性公网IP实现外网链接（需带宽支持）。
- 通过镜像服务，可以对裸金属服务器安装镜像，也可以通过私有镜像批量创建裸金属服务器，实现快速的业务部署。
- 通过云硬盘服务实现数据存储，并通过云硬盘备份服务实现数据的备份和恢复。
- 云监控是保持裸金属服务器可靠性、可用性和性能的重要部分，通过云监控，用户可以观察裸金属服务器资源。
- 云备份提供对云硬盘和裸金属服务器的备份保护服务，支持基于快照技术的备份服务，并支持利用备份数据恢复服务器和磁盘的数据。

图 1-1 BMS 产品架构



裸金属服务器与物理机、虚拟机的功能对比

裸金属服务器与物理机、虚拟机的对比如表1-1所示。其中，Y表示支持，N表示不支持，N/A表示不涉及。

说明

无特性损失、无性能损失：裸金属服务器具备物理机的一切特性和优势，您的应用可以直接访问裸金属服务器的处理器和内存，无任何虚拟化开销。

表 1-1 特性对比

功能分类	功能	裸金属服务器	物理机	虚拟机
下发方式	自动化发放	Y	N	Y
计算	无特性损失	Y	Y	N
	无性能损失	Y	Y	N
	资源无争抢	Y	Y	N
存储	拥有本地存储	Y	Y	N
	使用云硬盘（系统盘）启动	Y	N	Y
	使用镜像，免操作系统安装	Y	N	Y

功能分类	功能	裸金属服务器	物理机	虚拟机
网络	使用虚拟私有云网络	Y	N	Y
	物理机集群和虚拟机集群之间通过VPC通信	Y	N	Y
管控	远程登录等用户体验和虚拟机一致	Y	N	Y
	支持监控以及关键操作审计	Y	N	Y

常用概念

- 云上的物理计算资源，即运行在华为云数据中心的裸金属服务器，请查看[实例](#)。
- 描述裸金属服务器所在的数据中心，请查看[区域和可用区](#)。
- 裸金属服务器由不同的CPU、内存、存储和网络等组成，请查看[实例类型](#)。
- 裸金属服务器运行环境的模板，其中包含了特定的操作系统和一些预装的应用软件，请查看[镜像](#)。
- 裸金属服务器网络类型及各自使用场景，请查看[网络](#)。
- 实例对内和对外的服务地址，即私有IP地址和[弹性公网IP地址](#)。

访问方式

公有云提供了Web化的服务管理系统（即管理控制台）和基于HTTPS请求的API（Application Programming Interface）管理方式。

- API方式
如果用户需要将云平台上的裸金属服务器集成到第三方系统，用于二次开发，请使用API方式访问裸金属服务器。
- 管理控制台方式
其他相关操作，请使用管理控制台方式访问裸金属服务器。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“计算 > 裸金属服务器”。
如果未注册，请参见[准备工作](#)。

2 裸金属服务器的优势

安全可靠

裸金属服务器是用户专属的计算资源，支持VPC、安全组隔离；支持主机安全相关组件集成；基于擎天架构的裸金属服务器支持云磁盘作为系统盘和数据盘，支持硬盘备份恢复能力；支持对接专属存储，满足企业数据安全和监管的业务安全和可靠性诉求。

性能卓越

裸金属服务器继承物理服务器特征，无虚拟化开销和性能损失，100%释放算力资源。结合华为自研擎天软硬协同架构，支持高带宽、低时延云存储、云网络访问性能；满足企业数据库、大数据、容器、HPC、AI等关键业务部署密度和性能诉求。

敏捷的部署效率

裸金属服务器基于擎天加速硬件支持云磁盘作为系统盘快速发放；分钟级资源发放，基于统一console控制台、开放API和SDK，支持自助式资源生命周期管理和运维。

云服务和解决方案快速集成

裸金属服务器基于统一的VPC模型，支持公有云云服务的快速集成；帮助企业客户实现数据库、大数据、容器、HPC、AI等关键业务云化解决方案集成和加速业务云化上线效率。

3 使用场景

数据库场景

政企、金融关键的数据库业务必须通过资源专享、网络隔离、性能有保障的物理服务器承载。裸金属服务器为用户提供独享的高性能物理服务器，满足业务需求。

大数据场景

互联网大数据相关业务，包含大数据存储、分析等典型业务。支持裸金属本地存储和结合OBS服务的存算分离方案。

容器场景

互联网弹性业务负载。相比虚拟机，裸金属容器提供更高的部署密度、更低的资源开销、更加敏捷的部署效率。基于云原生技术帮助客户实现降低云化成本目标。

高性能计算/AI 场景

超算、基因测序、人工智能等高性能计算场景，处理的数据量大，裸金属服务器满足业务对服务器的高计算性能、高稳定性、高实时性的诉求。

4 实例

4.1 实例家族

实例概述

实例即您创建的一台裸金属服务器。不同实例类型提供不同的计算能力、存储空间、网络性能，您可以基于业务需求选择不同类型的实例。当华为云向您交付一个实例时，您将获得这台服务器完整的控制权限，包括开机、关机、带内管理等。

实例类型

裸金属服务器按着CPU体系架构，分为x86和鲲鹏实例，物理资源池配备华为自研高性能物理服务器，搭配独家调优算法，为您提供可靠的硬件环境。您可以根据业务需求选购不同配置的裸金属服务器。

- [x86 V4实例（CPU采用Intel Broadwell架构）](#)（停止扩容）
- [x86 V5实例（CPU采用Intel Skylake架构）](#)（停止扩容）
- [x86 V6实例（CPU采用Intel Cascade Lake架构）](#)
- [鲲鹏 V1实例（CPU采用Huawei Kunpeng 920架构）](#)

其他说明

- 基于本地盘的裸金属服务器，系统盘默认RAID 1，数据盘默认直通盘。如果需要更改数据盘RAID配置，可以联系运营管理员变更。系统盘RAID不支持变配。

4.2 x86 V4 实例（CPU 采用 Intel Broadwell 架构）

注意

x86 V4实例已停止扩容。

- 通用型

提供均衡的计算、存储以及网络配置，满足资源专享、网络隔离、性能有基本要求的业务场景，如数据库、核心ERP系统、金融系统等。

表 4-1 通用型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.s3.large	2*10 Core Intel Xeon E5-2618L V4 (2.20 GHz)	128 DDR4 RAM (GB)	2*600GB SAS System Disk RAID 1	2 x 2*10GE + SDI卡
physical.s3.xlarge	2*14 Core Intel Xeon E5-2658 V4 (2.30 GHz)	256 DDR4 RAM (GB)	2*600GB SAS System Disk RAID 1	2 x 2*10GE + SDI卡
physical.s3.2xlarge	2*10 Core Intel Xeon E5-2618L V4 (2.20 GHz)	192 DDR4 RAM (GB)	2*600GB SAS System Disk RAID 1	2 x 2*10GE + SDI卡

- 本地存储型

系统盘和数据盘均使用本地磁盘，针对数据量大，对计算性能、稳定性、实时性等要求很高的业务场景，如大数据、分布式缓存等。

表 4-2 本地存储型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.d1.large	2*10 Core Intel Xeon E5-2618L V4 (2.20 GHz)	128 DDR4 RAM (GB)	2*600GB SAS System Disk RAID 1 + 8*4TB SATA	2 x 2*10GE

- 内存优化型

提供1TB以上超大内存，适用于内存数据库、SAP HANA和HPC胖节点等场景。

表 4-3 内存优化型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.m2.small	4*24 Core Xeon E7-8890 V4 (2.20 GHz)	1024 DIMM RAM (GB)	2*600GB SAS System Disk RAID 1 + 7*1.8TB SAS HDD RAID 5 + 2*1.6TB NVMe SSD Card	2 x 2*10GE + 16G FC + SDI卡

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.m2.medium	4*24 Core Xeon E7-8890 V4 (2.20 GHz)	2048 DIMM RAM (GB)	2*600GB SAS System Disk RAID 1	2 x 2*10GE + SDI卡
physical.m2.large	4*24 Core Xeon E7-8890 V4 (2.20 GHz)	3072 DIMM RAM (GB)	2*600GB SAS System Disk RAID 1 + 14*1.8TB SAS HDD + 4*400GB SAS SSD + 2*1600GB NVMe SSD	2 x 2*10GE + SDI卡
physical.m2.xlarge	4*24 Core Xeon E7-8890 V4 (2.20 GHz)	4096 DIMM RAM (GB)	2*600GB SAS System Disk RAID 1 + 14*1.8TB SAS HDD + 4*400GB SAS SSD + 2*1600GB NVMe SSD	2 x 2*10GE + SDI卡

- IO优化型

系统盘和数据盘均使用SSD。适用于高性能大数据、数据库等存储IO性能要求高的场景。

表 4-4 IO 优化型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.io1.large	2*10 Core E5 2618L V4 (2.20 GHz)	256 DDR4 RAM (GB)	2*800GB SAS SSD System Disk RAID 1 + 4*3.2TB NVMe SSD	2 x 2*10GE

- GPU加速型

GPU加速型实例包括计算加速型（P系列）和图形加速型（G系列），提供优秀的浮点计算能力，从容应对高实时、高并发的大量计算场景。特别适合于深度学习、科学计算、CAE、3D动画渲染、CAD等应用。

表 4-5 GPU 加速型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.p1.large	2*14 Core Intel Xeon E5-2690 V4 (2.60 GHz)	512 DDR4 RAM (GB)	2*600GB SAS HDD System Disk RAID 1+ 6*800GB NVMe SSD Disk	NIC: 1*100G IB + 2*10GE + SDI卡 GPU: 8*Tesla P100 显存: 16G
physical.p2.large	2*14 Core Intel Xeon E5-2690 V4 (2.60 GHz)	512 DDR4 RAM (GB)	2*600GB SAS HDD + 6*800GB NVMe SSD	NIC: 1*100G IB + 2*10GE + SDI卡 GPU: 8*Tesla V100 显存: 16G
physical.g1.small	2*14 Core Intel Xeon E5-2690 V4 (2.60 GHz)	256 DDR4 RAM (GB)	2*600GB SAS + 960GB SSD	NIC: 3 x 2*10GE GPU: 1*M60

4.3 x86 V5 实例（CPU 采用 Intel Skylake 架构）

注意

x86 V5实例已停止扩容。

- 通用型

提供均衡的计算、存储以及网络配置，支持挂载可弹性扩展的云硬盘，满足资源专享、网络隔离、性能有基本要求的业务场景，如数据库、核心ERP系统、金融系统等。

表 4-6 通用型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.s4.medium	2*10 Core Intel Xeon Silver 4114 V5 (2.20 GHz)	128 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.s4.large	2*10 Core Intel Xeon Silver 4114 V5 (2.20 GHz)	192 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡
physical.s4.xlarge	2*14 Core Intel Xeon Gold 5120 V5 (2.20 GHz)	192 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡
physical.s4.2xlarge	2*14 Core Intel Xeon Gold 5120 V5 (2.20 GHz)	384 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡
physical.s4.3xlarge	2*22 Core Intel Xeon Gold 6161 V5 (2.20 GHz)	384 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡
physical.o3.small	2*4 Core Intel Skylake Xeon Gold 5122 V5 (3.60 GHz)	192 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡

- 本地存储型

系统盘和数据盘均使用本地磁盘，针对数据量大，对计算性能、稳定性、实时性等要求很高的业务场景，如大数据、分布式缓存等。

表 4-7 本地存储型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.d2.tiny	2*10 Core Intel Xeon Silver 4114 V5 (2.20 GHz)	128 DDR4 RAM (GB)	2*600GB SAS System Disk RAID 1 + 12*1.8TB SAS	2 x 2*10GE
physical.d2.large	2*12 Core Intel Xeon Gold 5118 V5 (2.30 GHz)	192 DDR4 RAM (GB)	2*600GB SAS System Disk RAID 1 + 12*10TB SATA	2 x 2*10GE

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.d2.x medium	2*18 Intel Xeon Gold 6151 V5 (3.00 GHz)	384 DDR4 RAM (GB)	2*600GB SAS RAID 1 + 24*1.8TB SAS	2 x 2*10GE

- IO优化型

系统盘和数据盘均使用SSD。适用于高性能大数据、数据库等存储IO性能要求高的场景。

表 4-8 IO 优化型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.io2.x large	2*22 Core Intel Xeon Gold 6161 V5 (2.20 GHz)	384 DDR4 RAM (GB)	2*800GB SSD RAID 1 + 10 * 800GB SSD	2 x 2*10GE

- 高性能计算型

主要使用在受计算限制的高性能处理器的应用程序上。它需要更多处理器核数、大量的内存和高吞吐量的存储系统。该规格使用V5 CPU服务器，并结合IB网卡，适用于HPC高性能计算等场景。

表 4-9 高性能计算型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.h2.la rge	2*18 Core Intel Xeon Gold 6151 V5 (3.00 GHz)	192 DDR4 RAM (GB)	1*1.6TB NVMe SSD Disk	1*100G IB + 2*10GE + SDI 卡
physical.hc2. xlarge	2*18 Core Intel Xeon Gold 6151 V5 (3.00 GHz)	384 DDR4 RAM (GB)	无	2 x 2*10GE + SDI卡

- GPU加速型

提供优秀的浮点计算能力，从容应对高实时、高并发的大量计算场景。特别适合于深度学习、科学计算、CAE、3D动画渲染、CAD等应用。

表 4-10 GPU 加速型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.p3.large	2*18 Core Intel Skylake 6151 V5 (3.00 GHz)	512 DDR4 RAM (GB)	2*1.2TB RAID 1 + 6*800GB NVMe SSD	NIC: 1*100G IB + 2*10GE + SDI卡 GPU: 8*Tesla V100 显存: 32G

4.4 x86 V6 实例（CPU 采用 Intel Cascade Lake 架构）

- 通用型

提供均衡的计算、存储以及网络配置，支持挂载可弹性扩展的云硬盘，满足资源专享、网络隔离、性能有基本要求的业务场景，如数据库、企业ERP系统、容器、大数据计算等。

表 4-11 通用型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.c6s.3xlarge	2*26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	384 DDR4 RAM (GB)	无	SDI 3.0 (40GE)
physical.c6sd.3xlarge	2*26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	384 DDR4 RAM (GB)	4*3.2TB NVMe SSD	SDI 3.0 (40GE)
physical.c6sd.6xlarge	2*26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	768 DDR4 RAM (GB)	4*3.2TB NVMe SSD	SDI 3.0 (40GE)

- 高性能计算型

采用Intel Cascade Lake CPU，满足多核高主频、低时延HPC的业务场景。

表 4-12 高性能计算型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.h6.xlarge	2*22 Core Intel Cascade Lake 6266 V6 (3.00 GHz)	192 DDR4 RAM (GB)	无	100Ge RDMA(Mellanox)+ SDI 3.0 (40GE)

- GPU加速型

采用Intel Cascade Lake CPU、NVIDIA T4，满足AI推理和图形图像加速业务场景。

表 4-13 GPU 加速型规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置
physical.pi6.3xlarge.6	2*26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	448 DDR4 RAM (GB)	2*480GB SATA SSD + 1.6TB NVMe SSD	NIC: 2*10GE(IN200) + 2*25GE(IN200) GPU: 6*NVIDIA T4

4.5 鲲鹏 V1 实例

鲲鹏型裸金属实例搭载鲲鹏920处理器，提供强劲鲲鹏算力和高性能网络，更好满足政府、互联网等各类企业对云上业务高性价比、安全可靠等诉求。

表 4-14 鲲鹏实例规格详情

规格名称/ID	CPU	内存	本地磁盘	扩展配置	是否基于擎天架构
physical.k1.2xlarge	2*64 Core Kunpeng 920-6426 (2.60 GHz)	256 DDR4 RAM (GB)	960GB SAS SSD	2*25GE + 2*25GE	否
physical.k1.ne.2xlarge	2*64 Core Kunpeng 920-6426 (2.60 GHz)	256 DDR4 RAM (GB)	无	SDI 3.0 (40GE)	是
physical.k1.ne.4xlarge	2*64 Core Kunpeng 920-6426 (2.60 GHz)	512 DDR4 RAM (GB)	2*3.2TB NVMe SSD	SDI 3.0 (40GE)	是

规格名称/ID	CPU	内存	本地磁盘	扩展配置	是否基于擎天架构
physical.k s1ne.8xlarge	2*64 Core Kunpeng 920-6426 (2.60 GHz)	1024 DDR4 RAM (GB)	2*3.2TB NVMe SSD	SDI 3.0 (40GE)	是
physical.k h1ne.2xlarge	2*64 Core Kunpeng 920-6426 (2.60 GHz)	256 DDR4 RAM (GB)	960GB SAS SSD	1*100G RDMA(Mellanox)+ SDI 3.0 (40GE)	是

4.6 实例生命周期

生命周期是指一台裸金属服务器实例从创建到删除所经历的所有状态，本章节简单描述各个状态的详情，以及状态之间的转换。

图 4-1 裸金属服务器状态转换

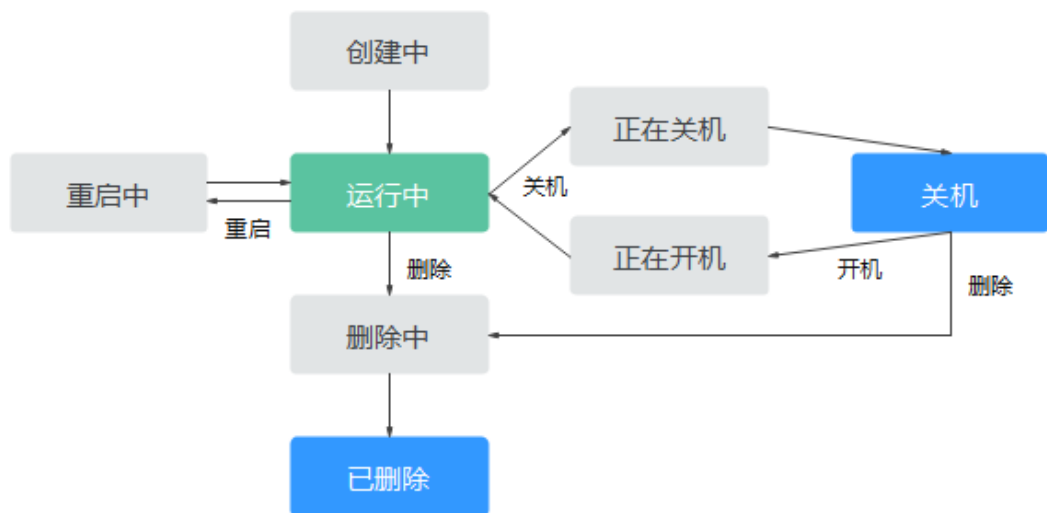


表 4-15 裸金属服务器状态说明

状态	状态属性	说明	API对应的状态
创建中	中间状态	创建裸金属服务器后，裸金属服务器状态进入运行中之前的状态。 如果长时间处于该状态，则说明出现异常，需要联系运营管理员处理。	BUILD/ BUILDING
正在开机	中间状态	裸金属服务器从关机到运行中的中间状态。 如果长时间处于该状态，则说明出现异常，需要联系运营管理员处理。	SHUTOFF

状态	状态属性	说明	API对应的状态
运行中	稳定状态	裸金属服务器正常运行中的状态。 在这个状态的服务器可以运行您的业务。	ACTIVE
正在关机	中间状态	裸金属服务器从运行中到关机的中间状态。 如果长时间处于该状态，则说明出现异常，需要联系运营管理员处理。	ACTIVE
关机	稳定状态	裸金属服务器被正常停止。 在这个状态下的服务器，不能对外提供业务。	SHUTOFF
重启中	中间状态	裸金属服务器正在进行重启操作。 如果长时间处于该状态，则说明出现异常，需要联系运营管理员处理。	REBOOT
强制重启中	中间状态	裸金属服务器正在进行强制重启操作。	HARD_REBOOT
删除中	中间状态	裸金属服务器处于正在被删除的状态。 如果长时间处于该状态，则说明出现异常，需要联系运营管理员处理。	ACTIVE/ SHUTOFF/ REBOOT/ HARD_REBOOT/ ERROR
已删除	中间状态	裸金属服务器已被正常删除。在该状态下的服务器，不能对外提供业务，并在短时间内从系统中彻底清除。	DELETED
故障	稳定状态	裸金属服务器处于异常状态。 在这个状态下的服务器，不能对外提供业务，需要联系运营管理员进行处理。	ERROR
重建中	中间状态	裸金属服务器接收到重建请求，处于重建的过程中。	SHUTOFF
重装操作系统中	中间状态	裸金属服务器接收到重装操作系统请求，处于重装操作系统的过程中。	SHUTOFF
重装操作系统失败	稳定状态	接收到重装操作系统请求，进行重装的过程中发生异常，导致重装失败。 在这个状态下的服务器，不能对外提供业务，需要联系运营管理员进行处理。	SHUTOFF

5 镜像

5.1 镜像概述

什么是镜像

镜像是裸金属服务器运行环境的模板，模板中包含了特定的操作系统和运行时环境，有时也额外包括了一些预装的应用软件。镜像文件相当于副本文件，该副本文件包含了系统盘中的所有数据。

镜像类型

根据镜像来源可以划分为公共镜像、私有镜像和共享镜像。

表 5-1 镜像类型列表

镜像类型	说明
公共镜像	常见的标准操作系统镜像，所有用户可见，包括操作系统以及预装的公共应用或服务。
私有镜像	包含操作系统、预装的公共应用以及用户的私有应用，仅用户个人可见。选择私有镜像创建裸金属服务器，可以节省您重复配置裸金属服务器的时间。
共享镜像	由其他用户共享的私有镜像。

公共镜像

公共镜像是由华为云官方提供的镜像，适配了裸金属服务器兼容性并安装了必要的初始化插件，所有用户均可使用，涵盖大部分主流操作系统。裸金属服务器规格不同，可供选择的镜像会有所不同（参见[裸金属服务器类型与支持的操作系统版本](#)）。

公共镜像特点

- 操作系统类型：包含基于Linux或者Windows的系统，并定期更新维护。

- 软件支持：集成了一些裸金属服务器的存储、网络以及用户基本功能正常使用所依赖的相关插件。

⚠ 注意

这些插件为裸金属服务器功能保障的基本插件，请勿做删除或者修改操作，否则会影响您的基本功能使用。

表 5-2 软件支持

软件	描述
Cloud-init	Cloud-init是开源的云初始化程序，能够对新创建裸金属服务器中指定的自定义信息（主机名、密钥和用户数据等）进行初始化配置。
一键式重置密码插件	裸金属服务器提供了一键式重置密码功能，当系统密码丢失或过期时，如果您的裸金属服务器提前安装了密码重置插件，可以在控制台页面设置新密码。
bms-network-config网络配置插件	网络初始化插件主要用于裸金属服务器下发过程网络的自动化配置以及用户误操作导致网络中断场景下裸金属服务器网络恢复。 该插件位于“/opt/huawei”目录下，请勿删除和改动。
SDI卡前端驱动插件	镜像中安装SDI卡前端驱动插件，使裸金属服务器能够支持挂载云硬盘，并且支持从云硬盘启动，实现快速发放能力。

- 兼容适配：对服务器硬件做了兼容适配。
- 安全性：公共镜像具有高度稳定性，并且为正版授权。
- 限制：暂无使用限制。

私有镜像

包含操作系统、预装的公共应用以及用户的私有应用。选择私有镜像创建裸金属服务器，可以节省您重复配置裸金属服务器的时间。

私有镜像特点

- 兼容适配：只适配了用于导出镜像的同型号服务器，不能保证能正确部署其他型号的裸金属服务器。
- 功能支持：支持用户自由创建和删除私有镜像，并使用私有镜像部署和重装服务器。私有镜像还支持以下操作：
 - 不同账号之间[共享镜像](#)。
 - 不同区域之间[复制镜像](#)。
 - [导出镜像](#)至个人OBS桶。
- 限制：每个用户最多创建50个私有镜像。
- 费用：私有镜像会收取一定的存储费用。详细计费标准可参考[镜像的计费标准](#)。

共享镜像

由其他用户共享的私有镜像。

镜像应用场景

- 批量部署软件环境
将已经部署好的裸金属服务器的操作系统、分区和软件等信息打包，用以制作私有镜像，然后使用该镜像批量创建裸金属服务器实例，新实例将拥有一样的环境信息，从而达到批量部署的目的。
- 服务器运行环境备份
对一台裸金属服务器实例制作镜像以备份环境。当该实例的软件环境出现故障而无法正常运行时，可以使用镜像恢复。

5.2 裸金属服务器类型与支持的操作系统版本

裸金属服务器不同规格操作系统兼容性列表如下所示。操作系统版本均为64bit。

- 使用X86 V4版本（CPU采用Intel Broadwell架构）的服务器请参考[表5-3](#)。
- 使用X86 V5版本（CPU采用Intel Skylake架构）的服务器请参考[表5-4](#)。
- 使用X86 V6版本（CPU采用Intel Cascade Lake架构）的服务器请参考[表5-5](#)。
- 使用鲲鹏CPU的服务器请参考[表5-6](#)。

📖 说明

- 建议您使用操作系统官方发行版本进行系统构建，避免对发行版本进行裁剪及高度定制，以减少问题发生概率。
- 操作系统发行版本由操作系统厂商进行不定期版本更迭，部分系统版本厂商已停止维护，不再发布问题修复及安全补丁，建议及时关注厂商公告进行系统升级更新，保证您系统的健壮性。
- CentOS 7.4及以下版本的7系列操作系统，因已知的内核问题会导致无法ping通裸金属服务器扩展网卡网关，涉及扩展网卡相关业务建议使用CentOS 7.5及以上系统版本，具体请参考[如何处理CentOS 7系列扩展网卡无法ping通的问题？](#)

表 5-3 裸金属服务器兼容性列表 (V4)

类型	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
本地存储型 d1 physical.d1. large	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.7/6.8/6.9/6.10/7.2/7.3/7.4/7.5/7.6	Red Hat 6.7/6.8/6.9/7.2/7.3/7.4/7.5	SUSE Linux Enterprise 11.SP4 / 12.SP1 / 12.SP2 / 12.SP3	Ubuntu 14.04.5 LTS Ubuntu 16.04 LTS	Oracle Linux 6.9/7.4	EulerOS 2.2/2.3
通用型规格 s3 physical.s3. large physical.s3. xlarge physical.s3. 2xlarge	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.7/6.8/6.9/6.10/7.2/7.3/7.4/7.5/7.6	Red Hat 6.7/6.8/6.9/6.10/7.2/7.3/7.4/7.5	SUSE Linux Enterprise 11.SP4 / 12.SP1 / 12.SP2 / 12.SP3	Ubuntu 14.04.5 LTS Ubuntu 16.04 LTS	Oracle Linux 6.9/7.4	EulerOS 2.2/2.3
内存优化型 规格m2 physical.m 2.small physical.m 2.medium physical.m2.l arge physical.m 2.xlarge	-	CentOS 7.2	-	-	-	-	-
IO优化型规格 io1 physical.io1 .large	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.7/6.8/6.9/7.2/7.3/7.4/7.5/7.6	Red Hat 6.7/6.8/6.9/7.2/7.3/7.4/7.5	SUSE Linux Enterprise 11.SP4 / 12.SP1 / 12.SP2 / 12.SP3	Ubuntu 14.04.5 LTS Ubuntu 16.04 LTS	Oracle Linux 6.9/7.4	EulerOS 2.2/2.3

类型	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
GPU加速型 规格 physical.p1. large physical.p2. large physical.g1. small	-	CentOS 7.4/7.5/ 7.6	-	-	Ubuntu 16.04 LTS	-	EulerOS 2.3

表 5-4 裸金属服务器兼容性列表 (V5)

类型	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
本地存储型 d2 physical.d2.l arge physical.d2. tiny physical.d2. xmedium	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.7/6.8/ 6.9/7.2/ 7.3/7.4/ 7.5/7.6	Red Hat 6.7/6.8 /6.9/7. 2/7.3/ 7.4/7.5	SUSE Linux Enterp rise 11.SP4 / 12.SP1 / 12.SP2 / 12.SP3	Ubuntu 14.04. 5 LTS Ubuntu 16.04 LTS	Oracle Linux 6.9/7. 4	EulerOS 2.3
通用型规格 s4 physical.s4. medium physical.s4.l arge physical.s4.x large physical.s4. 2xlarge physical.s4. 3xlarge	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.9/7.3/ 7.4/7.5/ 7.6	Red Hat /6. 9/7.3/ 7.4/7.5	SUSE Linux Enterp rise 11.SP4 / 12.SP2 / 12.SP3	Ubuntu 14.04. 5 LTS Ubuntu 16.04 LTS	Oracle Linux 6.9/7. 4	EulerOS 2.3

类型	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
IO优化型规格io2 physical.io2.xlarge	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.9/7.3/7.4/7.5/7.6	Red Hat 6.9/7.3/7.4/7.5	SUSE Linux Enterprise 11.SP4 / 12.SP2 / 12.SP3	Ubuntu 16.04 LTS	Oracle Linux 6.9/7.4	EulerOS 2.3
高性能计算型规格h2 physical.h2.large	-	CentOS 6.9/7.3/7.4/7.5/7.6	-	SUSE Linux Enterprise 11.SP4	Ubuntu 16.04 LTS	-	EulerOS 2.3
高性能计算型规格hc2 physical.hc2.xlarge	Windows Server 2012 R2 Standard Windows Server 2016 Standard	CentOS 6.9/7.3/7.4/7.5/7.6	Red Hat 6.9/7.3/7.4/7.5	SUSE Linux Enterprise 11.SP4 / 12.SP2 / 12.SP3	Ubuntu 14.04.5 LTS Ubuntu 16.04 LTS	Oracle Linux 6.9/7.4	EulerOS 2.3
GPU加速型规格p3 physical.p3.large	-	-	-	-	-	-	EulerOS 2.3

表 5-5 裸金属服务器兼容性列表（V6）

类型	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
通用型规格 s6/c6 physical.s6.x large physical.c6s. 3xlarge physical.c6s d.3xlarge physical.c6s d.6xlarge	CentOS 7.6/7.8/7 .9/8.2	Red Hat 7.6	SUSE Linux Enterpris e 15.SP2	Ubuntu 18.04.3 LTS	Oracle Linux7.6	EulerOS 2.5
高性能计算 型规格h6 physical.h6.l arge	CentOS 7.6/7.8/7 .9	-	-	-	-	-
GPU加速型 规格pi6 physical.pi6. 3xlarge.6	CentOS 7.6	-	-	-	-	-

表 5-6 裸金属服务器兼容性列表（鲲鹏）

类型	CentOS	HCE	EulerOS
physical.ks1ne.2xlarge physical.ks1ne.4xlarge physical.ks1ne.8xlarge	CentOS 7.6	Huawei Cloud EulerOS 2.0	EulerOS 2.8
physical.kd1ne.2xlarge physical.kd1ne.4xlarge	CentOS 7.6	Huawei Cloud EulerOS 2.0	EulerOS 2.8
physical.kat1.6xlarge	-	-	EulerOS 2.8
physical.ks1.2xlarge	CentOS 7.6	-	-

6 云硬盘

什么是云硬盘

云硬盘（Elastic Volume Service, EVS）可以为裸金属服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，满足不同场景的业务需求，适用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。

裸金属服务器支持挂载云硬盘，解决了传统物理服务器受限于本地硬盘容量的问题。支持共享云硬盘，由多台服务器并发读写访问，满足您企业核心系统集群部署的需求。

云硬盘类型

裸金属服务器使用的云硬盘类型有如下几种：

- 普通IO（上一代产品）：该类型云硬盘的最大IOPS为2200，适用于大容量、读写速率中等、事务性处理较少的应用场景，例如企业的日常办公应用或者小型测试等。
- 高IO：该类型云硬盘的最大IOPS可达5000，最低读写时延为1ms，适用于主流的高性能、高可靠应用场景，例如企业应用、大型开发测试以及Web服务器日志等。
- 超高IO：该类型云硬盘的最大IOPS可达33000，最低读写时延为1ms，适用于超高IO，超大带宽的读写密集型应用场景，例如高性能计算应用场景，用来部署分布式文件系统，或者I/O密集型应用场景，用来部署各类NoSQL/关系型数据库。
- 通用型SSD：该类型云硬盘的最大IOPS可达20000，最低读写时延为1ms，适用于各种主流的高性能、低延迟交互应用场景，例如企业办公、大型开发测试、转码类业务、Web服务器日志以及容器等高性能系统盘。
- 极速型SSD：该类型云硬盘的最大IOPS可达128000，最低读写时延为亚毫秒级，采用了结合全新低时延拥塞控制算法的RDMA技术，适用于需要超大带宽和超低时延的应用场景。

须知

当前physical.d2.large和physical.io2.xlarge规格为本地存储型（大数据）机型，不支持挂载云硬盘。

云硬盘性能

云硬盘性能的主要指标有IO读写时延、IOPS和吞吐量。

- IOPS：云硬盘每秒进行读写的操作次数。
- 吞吐量：云硬盘每秒成功传送的数据量，即读取和写入的数据量。
- IO读写时延：云硬盘连续两次进行读写操作所需要的最小时间间隔。

云硬盘性能指标的详细介绍请参见《[云硬盘产品介绍](#)》。

云硬盘的磁盘模式

裸金属服务器当前仅支持SCSI（小型计算机系统接口，Small Computer System Interface）磁盘模式的云硬盘。

您可以通过管理控制台创建SCSI类型的云硬盘，该类型的云硬盘支持SCSI指令透传，允许裸金属服务器操作系统直接访问底层存储介质。除了简单的SCSI读写命令，SCSI类型的云硬盘还可以支持更高级的SCSI命令。

说明

裸金属服务器公共镜像的操作系统中已经预安装了使用SCSI类型云硬盘所需的驱动，无需再安装。您也可以参考《裸金属服务器私有镜像制作指南》的“[安装SDI卡驱动](#)”章节了解驱动安装的操作。

7 网络

裸金属服务器目前支持以下网络类型：

- 虚拟私有云（VPC）
- 高速网络与增强高速网络
- IB网络
- 自定义VLAN网络

表 7-1 裸金属网络类型与实例映射关系

维度	子项	V4实例	V5实例	V6实例	鲲鹏实例
VPC	特性	支持	支持	支持	支持
	典型带宽	10GE	10GE	40GE	40GE
	网卡数	2	2	32	32
高速网络	特性	支持	支持	不支持	不支持
	典型带宽	VPC共用物理带宽	VPC共用物理带宽	NA	NA
增强高速网络	特性	支持	支持	不支持	不支持
	典型带宽	10GE	10GE	NA	NA
IB网络	特定实例支持	特定实例支持	特定实例支持	特定实例支持	特定实例支持
	典型带宽	100GE	100GE	100GE	100GE
自定义网络	-	依赖增强高速网络；依赖于专属网关设备。	依赖增强高速网络；依赖于专属网关设备。	不支持	不支持

裸金属服务有五种网络类型，分别是虚拟私有云、高速网络、增强高速网络、自定义VLAN网络和IB网络，不同网络之间相互隔离不互通。

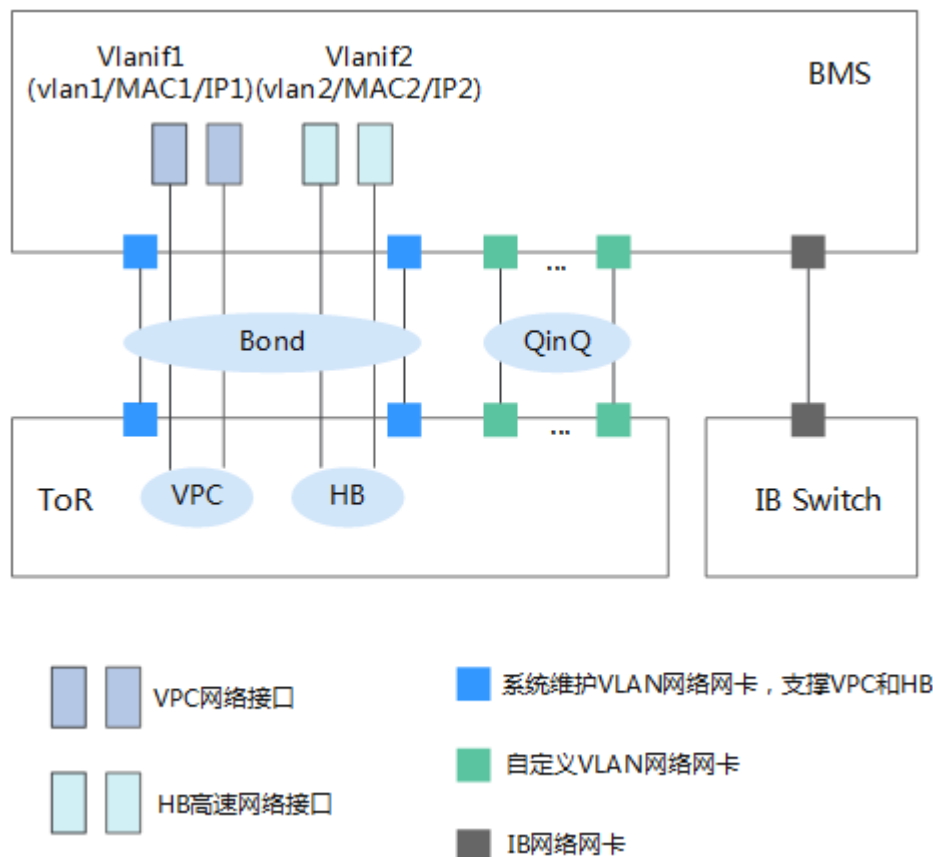
V4/V5实例:

VPC网络接口和高速网络接口是基于系统维护VLAN网卡组建bond后创建的VLAN子接口。自定义VLAN网络网卡和IB网络网卡由用户进行管理配置。

V6/鲲鹏实例:

基于擎天架构，网络性能大幅提升，VPC网卡组bond提供高可靠性。

图 7-1 裸金属服务网络



说明

- 图中的ToR表示服务器机柜的布线方式，接入交换机放在机架顶部，服务器放在下方。HB表示高速网络。QinQ表示802.1Q隧道。
- VPC网络接口和HB高速网络接口由系统生成，租户不可修改。这两个网络接口属于同一个网卡Bond。
- 弹性云服务器和裸金属服务器之间可以通过虚拟私有云通信，也可以通过IB网络通信（如果存在）。
- 只有虚拟私有云支持安全组、弹性公网IP和弹性负载均衡能力。
- 对于高速网络和自定义VLAN网络，同一网络中的裸金属服务器实例之间仅提供L2连接。

虚拟私有云

虚拟私有云（Virtual Private Cloud, VPC），为裸金属服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。您可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。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，用户可以自定义安全组内与组间的访问规则，加强裸金属服务器的安全保护。

更多信息，请参见《[虚拟私有云产品介绍](#)》。

高速网络

裸金属服务器的内部网络，为同一可用区内的裸金属服务器之间提供高带宽的网络。如果您需要部署高吞吐量或要求低时延的服务，可以创建高速网络。目前，裸金属服务支持的高速网络带宽的最大值为10Gbps。

增强高速网络基于上一代高速网络进行了软硬件的优化升级，为租户提供更强大的网络功能。

相比上一代高速网络，增强高速网络具有如下优势：

- 带宽提升至10GE及以上。
- 租户自定义网络平面数量，最多支持4K个子网。

自定义 VLAN 网络

未被系统默认使用的以太网卡（10GE，在裸金属服务器规格中定义）可用于自定义VLAN网络，物理上采用QinQ技术实现用户的网络隔离，提供额外的物理平面和网络带宽，用户能够自由划分所需的VLAN子网来分隔流量。自定义VLAN网络的网卡是成对出现的，用户可以通过配置bond实现高可用。自定义VLAN网络当前不支持跨AZ互通。

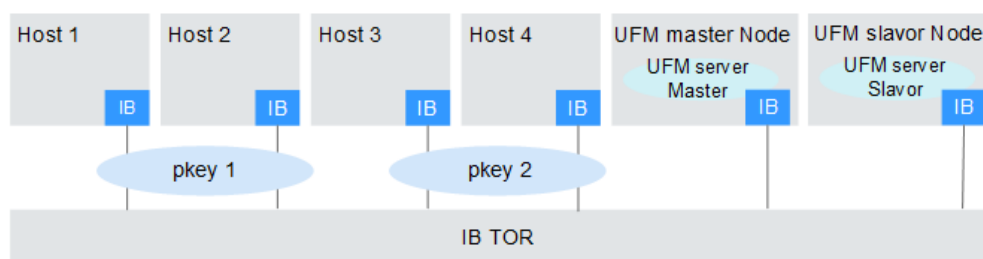
说明

QinQ：一种基于802.1Q封装的二层隧道协议，它将用户私网VLAN TAG封装在公网VLAN TAG中，报文带着两层TAG穿越服务商的骨干网络，从而为用户提供二层VPN隧道。

IB 网络

IB网络因其低延迟、高带宽的网络特性被用于很多高性能计算（High Performance Computing, HPC）项目，IB网络采用了100G Mellanox IB网卡，通过专用IB交换机和控制器软件UFM实现网络通信和管理。IB网络通过Partition Key实现网络隔离，不同租户的IB网络可通过不同的Partition Key来隔离，类似于以太网的vlan。

图 7-2 IB 网络隔离方式



说明

UFM（Unified Fabric Manager）是IB网络上IB交换机控制器，基于OpenSM软件，提供北向服务接口。UFM采用主备部署方式。

8 安全

8.1 责任共担

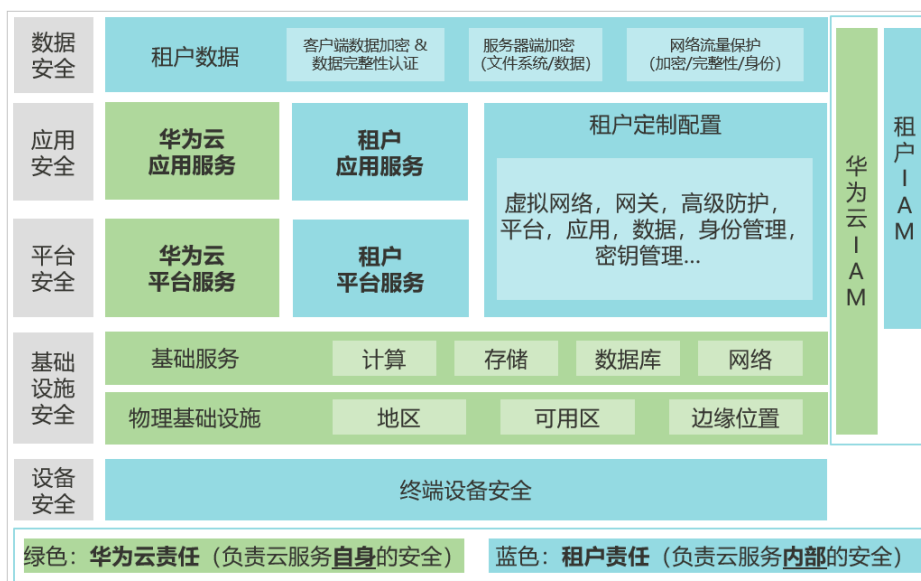
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1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 8-1 华为云安全责任共担模型



8.2 身份认证与访问控制

统一身份认证 (Identity and Access Management, IAM) 提供用户身份认证、权限分配、访问控制等功能, 您可以使用 IAM 安全地控制用户对您裸金属服务器资源的访问。裸金属服务器支持通过 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。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 BMS 所需的权限, 组内用户自动继承用户组的所有权限。

账户安全性

如果您是企业管理员, 企业中有不同的员工需要使用您在云上购买的资源, 为了避免您将自己账号的密码/访问密钥共享给员工, 建议您使用 IAM 创建用户并授予对应权限, 员工可以使用新创建的用户账号访问系统, 帮助您高效的管理资源。您还可以设置账号安全策略确保这些用户账号的安全, 从而降低您的企业信息安全风险。

细粒度授权

您可以对员工的用户账号授予精细的操作权限, 确保云服务被合理使用。BMS 所需的权限请参见 [BMS 权限管理](#)。

安全组

安全组是一种虚拟防火墙, 具备状态检测和数据包过滤功能, 用于设置弹性云服务器、裸金属服务器、负载均衡、数据库等实例的网络访问控制, 是重要的网络安全隔离手段。

您可以通过配置安全组规则, 允许安全组内的实例对公网或私网的访问。

- 安全组是一个逻辑上的分组, 您可以将同一区域内具有相同安全保护需求的裸金属服务器加入到同一个安全组内。
- 同一安全组内的 BMS 实例之间默认内网网络互通, 不同安全组内的实例之间默认内网不通。

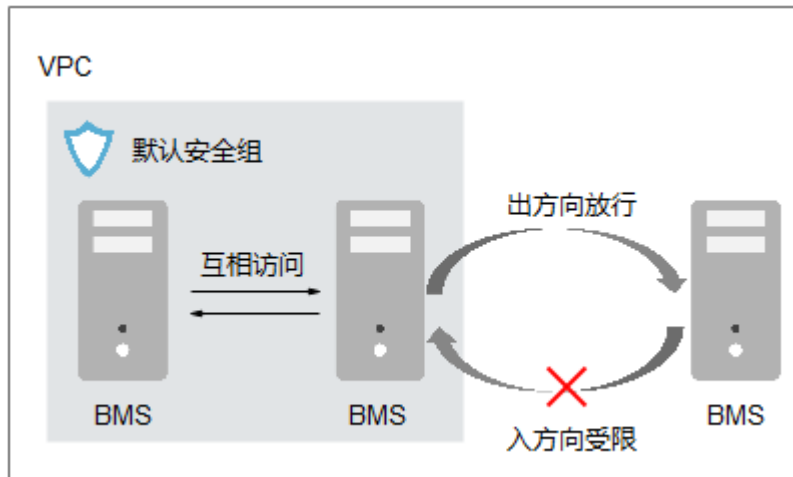
- 您可以随时修改安全组的规则，新规则立即生效。

默认安全组

在一个区域创建BMS实例时，如果当前账号在这个区域尚未创建安全组，系统会为您创建一个默认安全组。

安全组的默认规则是在出方向上的数据报文全部放行，入方向访问受限，安全组内的裸金属服务器无需添加规则即可互相访问，如图 默认安全组所示。

图 8-2 默认安全组



默认安全组Sys-default规则如表8-1所示：

表 8-1 默认安全组规则

方向	优先级	策略	协议	端口范围	目的地址/源地址	说明
出方向	100	允许	全部	全部	目的地址： 0.0.0.0/0	允许所有出站流量的数据报文通过。
入方向	100	允许	全部	全部	源地址：当前 安全组名称	允许同样使用当前安全组的裸金属服务器之间通过任意端口和规则互访。
入方向	100	允许	TCP	22	源地址： 0.0.0.0/0	允许所有IP地址通过SSH远程连接到Linux裸金属服务器。
入方向	100	允许	TCP	3389	源地址： 0.0.0.0/0	允许所有IP地址通过RDP远程连接到Windows裸金属服务器。

了解更多信息，请参阅“[安全组简介](#)”。

密钥对与密码

- 什么是密钥对

密钥对，也称SSH密钥对，是区别于用户名+密码的远程登录Linux实例的认证方式。通过加密算法生成一对密钥，一个对外界公开，称为公钥，另一个由用户自己保留，称为私钥。公钥和私钥组成密钥对。密钥对的工作原理是使用公钥加密某个数据（例如一个密码），用户可以使用私钥解密数据。

华为云只会存储公钥，您需要存储私钥。拥有您的私钥的任何人都可以解密您的登录信息，因此将您的私钥保存在一个安全的位置非常重要。

- 功能优势

相比用户名+密码认证方式，密钥对在安全性和便捷性上都更具优势，如表 [密钥对与密码对比](#) 所示。

表 8-2 密钥对与密码对比

对比项	密钥对	用户名+密码
安全性	<ul style="list-style-type: none">• 安全强度远高于常规用户口令，可以杜绝暴力破解威胁。• 不可能通过公钥推导出私钥。	安全性较低。
便捷性	便于远程登录大量Linux实例，方便管理。	一次只能登录一台Linux实例，不利于批量维护。

- 使用限制

- 仅支持Linux实例。
- 仅支持的RSA密钥对，支持的长度：1024、2048和4096。
- 一台Linux实例只能拥有一个密钥对。如果您的实例已绑定密钥，绑定新的密钥会替换原来的密钥。

- 生成方式

- 通过管理控制台创建密钥对

 说明

在首次生成密钥对时，务必下载并妥善保存私钥。

- 通过PuTTYgen等工具创建密钥对，并导入华为云

相关操作

[使用SSH密钥对](#)

8.3 数据保护技术

裸金属服务器通过多种数据保护手段和特性，保障存储数据的安全可靠。

- 裸金属服务器具备物理机级的性能和隔离性，用户独占计算资源，并且无任何虚拟化开销。存储在高性能高可靠的服务器上的数据，自然也会很安全。
- 带有本地磁盘的裸金属服务器，支持本地磁盘组RAID，磁盘数据冗余存储，提升容错能力，确保数据安全。
- 无本地磁盘的裸金属服务器，支持从云硬盘启动（即系统盘为云硬盘，且称之为快速发放裸金属服务器）。云服务器备份可以对裸金属服务器提供备份保护，支持基于多块云硬盘一致性快照技术的备份服务，并支持利用备份数据恢复服务器数据，最大限度保障用户数据的安全性和正确性，确保业务安全。

8.4 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后，CTS可记录BMS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](#)。

8.5 监控安全风险

主机监控

云监控服务的主机监控分为基础监控和操作系统监控，基础监控为云服务器自动上报的监控指标（裸金属服务器不支持基础监控）。操作系统监控通过在裸金属服务器中安装Agent插件，为用户提供服务器的系统级、主动式监控服务。Agent占用的系统资源很小，CPU用率<1.5%、内存<50M。

云监控会提供CPU、内存、磁盘、网络等四十余种监控指标，满足服务器的基本监控运维需求。

- 云监控服务的详细介绍，请参见[CES功能介绍](#)。
- 裸金属服务器支持的监控指标，请参见[支持的监控指标](#)。

敏感操作保护

裸金属服务器支持敏感操作保护，在控制台进行敏感操作时，需要输入一种能证明身份的凭证，身份验证通过后方可进行相关操作。为了账号安全，建议开启操作保护功能，该功能对账号以及账号下的用户都生效。

8.6 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 8-3 合规证书下载

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 8-4 资源中心

9 计费

9.1 计费说明

计费项

计费项包括裸金属服务器、云硬盘（可选）、弹性公网IP（可选），详细说明如[表9-1](#)所示。

表 9-1 计费项说明

计费项	计费说明
裸金属服务器	对您选择的裸金属服务器规格计费（包括CPU规格、内存容量、本地磁盘和扩展配置等）。 具体请参考 裸金属服务器产品价格详情 。
云硬盘（可选）	随裸金属服务器一起创建的云硬盘，计费方式与裸金属服务器相同。单独创建的云硬盘，支持按量付费和包年包月，具体请参考 云硬盘产品价格详情 。
弹性公网IP（可选）	裸金属服务器支持绑定弹性公网IP，按带宽或流量计费，具体请参考 弹性公网IP产品价格详情 。

计费模式

裸金属服务器计费模式为包年包月付费，不支持按量付费。其中付10个月费用即可享受一年使用期。对于长期使用者，推荐包年购买。

变更配置

扩容存储空间：如果您的业务需求增大，可以通过扩容或者增加裸金属服务器挂载的云硬盘来扩展您的存储空间。这部分存储空间将按照您选择的云硬盘计费方式（按需或者包年包月）计费。

相关问题

- [在哪里查询裸金属服务器的价格?](#)
- [预付费和后付费是什么意思? 如何选择?](#)
- [裸金属服务器退订时怎么扣费?](#)
- [怎么设置“包年/包月”资源的自动续费?](#)
- [裸金属服务器到期了, 多久会释放资源?](#)

10 BMS 权限管理

背景介绍

如果您需要对华为云上购买的裸金属服务器资源，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。

通过IAM，您可以在账号中给员工创建IAM用户，并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BMS的使用权限，但是不希望他们拥有删除BMS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用BMS，但是不允许删除BMS的权限，控制他们对BMS资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用BMS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。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

BMS 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

BMS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问BMS时，需要先切换至授权区域。

根据授权精度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对BMS服务，管理员能够控制IAM用户仅能对某一类裸金属服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，BMS支持的API授权项请参见[权限及授权项说明](#)。

表1 BMS系统权限列出了BMS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 10-1 BMS 系统权限

系统角色/策略名称	描述	类别
BMS FullAccess	裸金属服务器管理员，拥有该服务下的所有权限	系统策略
BMS CommonOperations	裸金属服务器基本操作权限，包括开机、关机、重启、查询等操作	系统策略
BMS ReadOnlyAccess	裸金属服务器只读权限，拥有该权限的用户仅能查看裸金属服务器列表和详情	系统策略

表10-2列出了BMS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 10-2 常用操作与系统权限的关系

操作	BMS FullAccess	BMS CommonOperations	BMS ReadOnlyAccess
创建裸金属服务器	√	x	x
查看裸金属服务器列表	√	√	√
查询裸金属服务器详情	√	√	√
修改裸金属服务器名称	√	x	x
启动裸金属服务器	√	√	x
关闭裸金属服务器	√	√	x
重启裸金属服务器	√	√	x
裸金属服务器挂载数据卷	√	√	x

操作	BMS FullAccess	BMS CommonOperations	BMS ReadOnlyAccess
裸金属服务器卸载数据卷	√	√	x
重装裸金属服务器操作系统	√	x	x
一键重置裸金属服务器的密码	√	x	x

相关链接

- [IAM产品介绍](#)
- [权限及授权项说明](#)

11 区域和可用区

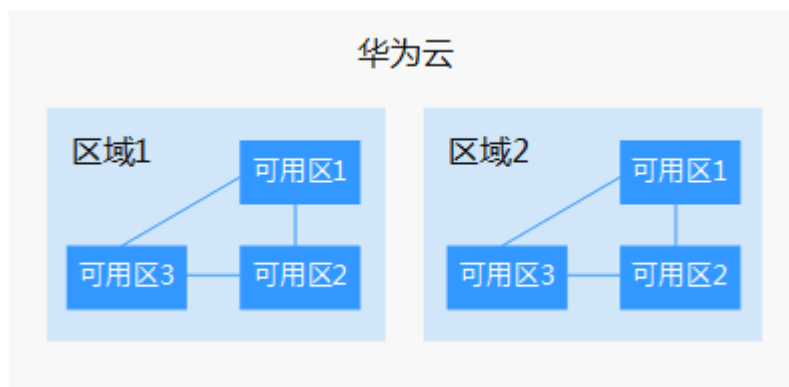
什么是区域、可用区？

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11-1阐明了区域和可用区之间的关系。

图 11-1 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：

- 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](#)。

12 裸金属服务器与其他服务的关系

裸金属服务器与其他服务的关系

表 12-1 裸金属服务器与其他服务的关系

服务名称	裸金属服务器与其他服务的关系	主要交互功能/最佳实践
镜像服务 (Image Management Service, IMS)	您可以通过镜像创建裸金属服务器，提高裸金属服务器的部署效率；也可以将裸金属服务器转换为私有镜像，供您个人使用，或者共享给他人。	<ul style="list-style-type: none">● 通过私有镜像创建裸金属服务器● 通过裸金属服务器创建私有镜像● 通过外部镜像文件创建私有镜像
虚拟私有云 (Virtual Private Cloud, VPC)	为裸金属服务器提供一个逻辑上完全隔离的专有网络，您可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。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，用户可以自定义安全组内与组间裸金属服务器的访问规则，加强裸金属服务器的安全保护。	<ul style="list-style-type: none">● 添加安全组规则● 绑定弹性公网IP至服务器
专属云 (Dedicated Cloud, DeC)	专属云中的专属资源池与公共资源池物理隔离，如果您的业务对安全合规性有较高要求，那么您可以选择将裸金属服务器创建在专属云中。创建专属裸金属服务器有两种方式： <ul style="list-style-type: none">● 在专属云控制台创建专属裸金属服务器。● 在云服务器控制台创建专属裸金属服务器。	<ul style="list-style-type: none">● 开通专属云● 创建专属裸金属服务器

服务名称	裸金属服务器与其他服务的关系	主要交互功能/最佳实践
云硬盘 (Elastic Volume Service, EVS)	可以将云硬盘挂载至裸金属服务器，并可以随时扩容云硬盘容量。	<ul style="list-style-type: none">• 挂载数据盘• 初始化数据盘• 卸载数据盘• 扩容磁盘
专属分布式 存储服务 (Dedicat ed Distributed Storage Service, DSS)	专属分布式存储服务为您提供独享的物理存储资源，通过数据冗余和缓存加速等多项技术，提供高可用性和持久性，以及稳定的低时延性能，适用于HPC、OLAP以及混合负载等应用场景。	<ul style="list-style-type: none">• 磁盘类型概述
云监控服务 (Cloud Eye)	当您申请裸金属服务器后，安装Agent插件并完成相关配置，即可在云监控服务查看裸金属服务器的监控数据，还可以获取可视化监控图表。	<ul style="list-style-type: none">• 主机监控概述• 支持的监控指标（安装Agent）
标签管理服务 (Tag Managem ent Service, TMS)	使用标签来标识裸金属服务器，便于分类和搜索。	<ul style="list-style-type: none">• 添加标签• 使用标签检索资源• 删除标签

13 支持列表和使用限制

支持列表

实例

- 支持自动化发放裸金属服务器，远程Console登录。
- 支持租户自主管理裸金属服务器生命周期：查询、启动、关机、重启、删除。
- 支持一键重置密码。
- 支持重装操作系统：裸金属服务器OS无法正常启动、操作系统中毒等场景，可以重装OS。
- 支持故障重建：由于服务器硬件损坏、SDI卡损坏等原因，导致服务器无法正常使用时，可以申请服务器重建。
- 支持备份服务器：使用云服务器备份，将裸金属服务器的配置和所包含的多个云硬盘数据备份到高可靠性等级的对象存储服务中，保障用户数据安全。
- 支持用户数据注入：通过注入脚本简化服务器配置、初始化系统等。
- 裸金属服务器支持安装大数据软件产品CDH（Cloudera's Distribution Including Apache Hadoop），并且CDH可以与已购买的华为云上的其他服务通信。
- 支持通过API管理裸金属服务器。
- 支持主机监控，可实时获取裸金属服务器的CPU、内存、磁盘I/O等监控指标数据。
- 支持标签管理服务，使用标签来标识裸金属服务器，便于分类和搜索。

磁盘

- 支持为Linux和Windows裸金属服务器挂/卸载云硬盘。
- 支持共享卷。
- 支持云硬盘动态扩容。

镜像

- 可以使用公共镜像、私有镜像、共享镜像发放裸金属服务器。
- 支持通过裸金属服务器创建私有镜像。
- 支持通过外部镜像文件创建私有镜像。
- 私有镜像还支持不同账号之间共享镜像、不同区域之间复制镜像、导出镜像至个人OBS桶。

网络

- 支持虚拟私有云、IB网络，满足多种场景的需求。
- 创建安全组并定义安全组规则，为裸金属服务器提供安全防护。
- 支持绑定弹性公网IP，满足客户互联网访问需求。
- 支持绑定多张网卡。

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）。
- 不支持带外管理，您的裸金属服务器资源统一由华为云管理和维护。
- 不支持热迁移，服务器故障后会对业务造成影响，建议您通过业务集群部署、主备部署等方式实现业务的高可用。
- 不支持创建没有操作系统的裸设备，即裸金属服务器必须自带操作系统。
- 创建后不支持更换VPC。
- 不支持二次虚拟化，即不支持安装虚拟化软件。
- 不支持自定义裸金属服务器的CPU、内存等配置，也不支持CPU、内存、本地磁盘扩容，仅云硬盘可以扩容。
- 仅支持挂载SCSI类型的云硬盘。
- 由于某些机型的服务器没有配备SDI卡，或者其他服务器本身的原因，有些规格或镜像的裸金属服务器不支持挂载云硬盘。
- 请勿删除或者修改镜像中内置的插件服务（如Cloud-Init、bms-network-config等），否则会影响您的基本功能使用。
- 在创建裸金属服务器时，如果选择自动分配IP地址，请不要在裸金属服务器发放完成后修改私有IP地址，避免和其他裸金属服务器IP冲突。
- 裸金属服务器不支持配置桥接网卡，会导致网络不通。
- 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。
- 当前仅支持从管理控制台关机裸金属服务器，不支持在单独实例OS内部使用关机命令关机裸金属服务器。
- 为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。裸金属服务器没有独立的服务配额，它的实例数、核心数和RAM容量与弹性云服务器共用一套配额，在查看配额时，需要在“弹性云服务器”栏目查看，详情请参见[查看配额](#)。

14 修订记录

版本日期	变更说明
2022-11-15	第十五次正式发布。 新增： 责任共担 身份认证与访问控制 数据保护技术 审计与日志 监控安全风险 认证证书
2022-11-09	第十四次正式发布。 修改： 云硬盘 ，补充不支持挂载云硬盘的裸金属服务器规格说明。
2022-09-20	第十次正式发布。 修改： 裸金属服务器类型与支持的操作系统版本 ，补充CentOS兼容性列表及相关说明。
2020-07-15	第九次正式发布。 <ul style="list-style-type: none">将实例规格重新划分，新增x86 V4实例（CPU采用Intel Broadwell架构）、x86 V5实例（CPU采用Intel Skylake架构）、鲲鹏 V1实例章节。裸金属服务器类型与支持的操作系统版本，新增计算优化型o3系列的操作系统兼容性列表。
2020-03-31	第八次正式发布。 新增： 计费说明

版本日期	变更说明
2020-01-20	第七次正式发布。 裸金属服务器与其他服务的关系 ，补充BMS和标签管理服务（TMS）的关系。
2019-07-30	第六次正式发布。 <ul style="list-style-type: none">• 大纲调整。• 什么是裸金属服务器，补充常用概念、访问方式。• 实例生命周期，修改生命周期表流程。
2019-05-30	第五次正式发布。 新增 裸金属服务器类型与支持的操作系统版本 章节。
2019-04-16	第四次正式发布。 <ul style="list-style-type: none">• 什么是裸金属服务器，补充内网带宽信息。• 实例家族，补充RAID配置信息和GPU实例的显存信息。
2019-03-18	第三次正式发布。 大纲调整，并新增如下章节： <ul style="list-style-type: none">• 实例生命周期• 身份认证与访问控制• 支持列表和使用限制
2018-10-31	第二次正式发布。 新增 实例家族 章节。
2018-06-30	第一次正式发布。