

Bare Metal Server

Service Overview

Issue	15
Date	2022-11-15



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

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

For vulnerability information, enterprise customers can visit the following web page:

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

Contents

1 What Is BMS?	1
2 BMS Advantages	5
3 Application Scenarios	6
4 Instance	7
4.1 Instance Family.....	7
4.2 x86 V4 BMS with Intel Broadwell CPU.....	7
4.3 x86 V5 BMS with Intel Skylake CPU.....	11
4.4 x86 V6 BMS with Intel Cascade Lake CPU.....	14
4.5 Kunpeng V1 BMS.....	15
4.6 Lifecycle.....	16
5 Image	19
5.1 Overview.....	19
5.2 OSs Supported by Different Types of BMSs.....	21
6 EVS Disk	26
7 Network	28
8 Security	33
8.1 Shared Responsibilities.....	33
8.2 Identity Authentication and Access Control.....	34
8.3 Data Protection.....	37
8.4 Auditing and Logging.....	37
8.5 Risk Control.....	37
8.6 Certificates.....	38
9 Billing	40
9.1 Billing.....	40
10 Permissions	42
11 Region and AZ	45
12 Related Services	47
13 Features and Constraints	49

14 Change History..... 51

1 What Is BMS?

Overview

Bare Metal Server (BMS) features both the scalability of Elastic Cloud Server (ECS) and high performance of physical servers. It provides dedicated servers on the cloud, delivering the performance and security required by core databases, critical applications, high-performance computing (HPC), and big data.

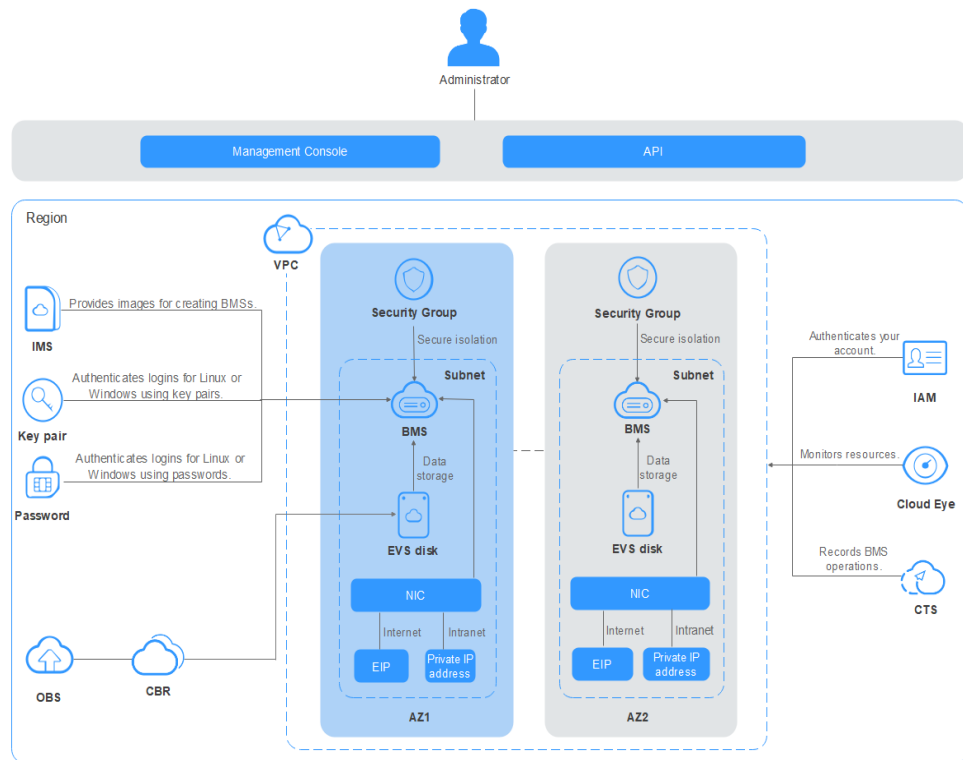
The BMS self-service feature allows you to apply for and use a BMS on demand. To apply for a BMS, you need to specify the server type, image, required network, and other configurations. You can obtain the BMS you require within 30 minutes.

System Architecture

BMS works with other cloud services to provide computing, storage, network, and image functions.

- BMSs are deployed in multiple availability zones (AZs) connected with each other through an internal network. If an AZ becomes faulty, other AZs in the same region will not be affected.
- Virtual Private Cloud (VPC) allows you to create a dedicated network for BMSs and configure subnets and security groups. BMSs in a VPC can communicate with the external network through EIPs (bandwidth support required).
- Image Management Service (IMS) allows you to install OSs on BMSs or create BMSs using private images for rapid service deployment.
- Elastic Volume Service (EVS) provides storage and Volume Backup Service (VBS) provides data backup and restoration.
- Cloud Eye is a key measure to monitor BMS performance, reliability, and availability. Using Cloud Eye, you can monitor BMS in real time.
- Cloud Backup and Recovery (CBR) backs up data for EVS disks and BMSs, and uses snapshot backups to restore the EVS disks and BMSs.

Figure 1-1 System architecture



BMSs, Physical Servers, and ECSs

Table 1-1 compares BMSs, physical servers, and ECSs. Y indicates supported and N indicates unsupported.

NOTE

BMSs have all the features and advantages of physical servers. Your applications can access the physical CPU and memory without any virtualization overhead.

Table 1-1 Comparison between BMSs, physical servers, and ECSs

Category	Function	BMS	Physical Server	ECS
Provisioning	Automatic provisioning	Y	N	Y
Compute	No feature loss	Y	Y	N
	No performance loss	Y	Y	N
	Exclusive resources	Y	Y	N
Storage	Local storage	Y	Y	N

Category	Function	BMS	Physical Server	ECS
	Booting from an EVS disk (system disk)	Y	N	Y
	Using an image (free from OS installation)	Y	N	Y
Network	VPC	Y	N	Y
	Communication between physical servers and VMs through a VPC	Y	N	Y
Management and control	Consistent remote login experience as VMs	Y	N	Y
	Monitoring and auditing of key operations	Y	N	Y

Related Concepts

- [Instance Family](#)
- [Region and AZ](#)
- [BMS Types](#)
- [Image](#)
- [BMS Networks](#)
- [EIP](#)

Access Methods

The public cloud provides a web-based service management system (management console). You can access BMS through the management console or HTTPS APIs. The two access methods differ as follows:

- API
If you want to integrate BMS into a third-party system for secondary development, use APIs to access the BMS service.
- Management console

For all other purposes, use the management console. Log in to the management console and choose **Compute > Bare Metal Server** on the homepage.

If you do not have an account, sign up to create one as instructed in [Making Preparations](#).

2 BMS Advantages

High Security and Reliability

BMS allows you to use dedicated computing resources, add servers to VPCs and security groups for network isolation, and integrate related components for server security. The BMSs running on the QingTian architecture can use EVS disks as system and data disks, which can be backed up for restoration. BMS can interconnect with dedicated storage to ensure the data security and reliability required by enterprise services.

High Performance

BMS has no virtualization overhead, allowing dedicated computing resources for service running. Running on QingTian, a hardware-software synergy architecture developed by Huawei, BMS can use high-bandwidth, low-latency storage and networks on the cloud, meeting the deployment density and performance requirements of critical services such as enterprise databases, big data, containers, HPC, and AI.

Quick Provisioning and Unified O&M

Hardware-based acceleration provided by the QingTian architecture enables EVS disks to be used as system disks. The required BMSs can be provisioned within minutes after you submit an order. You can manage your BMSs throughout their lifecycle from the management console or using open APIs with SDKs.

Quick Integration of Cloud Services and Solutions

Based on the unified VPC model, cloud services and solutions (such as database, big data, container, HPC, and AI solutions) can be quickly integrated to run on BMSs. This accelerates cloud transformation.

3 Application Scenarios

Database

Mission-critical database services of governments and financial institutions must be deployed on physical servers with dedicated resources, isolated networks, and guaranteed performance. The BMS service properly meets these database service requirements by providing high-performance servers dedicated for individual users.

Big Data

For Internet services involving big data storage and analysis, the BMS service provides both local storage and compute-storage decoupling backed by OBS.

Container

Containers enable elastic load balancing for Internet services. BMSs provide more agile container deployment with higher density and lower resource overhead than VMs. Cloud native technologies reduce the cost of cloud transformation.

HPC/AI

In high-performance computing (HPC) such as supercomputing, DNA sequencing, and AI, a large amount of data needs to be processed. The BMS service meets the requirements of HPC services for high computing performance, high stability, and high real-time performance of servers.

4 Instance

4.1 Instance Family

Overview

An instance is a purchased BMS. Different instance types provide varied computing capabilities, storage space, and network performance. You can select a type that meets your service requirements. After you purchase a BMS, you can perform operations such as starting, stopping, and in-band monitoring.

BMS Types

A BMS has x86 or Kunpeng CPUs. Huawei-developed high-performance physical servers with exclusive optimization algorithms provide a reliable hardware environment for all the BMSs.

- [x86 V4 BMS with Intel Broadwell CPU](#) (no more provisioning)
- [x86 V5 BMS with Intel Skylake CPU](#) (no more provisioning)
- [x86 V6 BMS with Intel Cascade Lake CPU](#)
- [Kunpeng V1 BMS with Kunpeng 920 CPU](#)

Remarks

- If a BMS uses local disks, its system disk is configured as RAID 1 and cannot be changed. The data disks are configured as RAID 0. To change the RAID configuration of data disks, contact the operation administrator.

4.2 x86 V4 BMS with Intel Broadwell CPU

 CAUTION

x86 V4 BMSs will no longer be provisioned.

- **General-purpose**
This BMS type provides general compute, storage, and network specifications and is ideal for systems that have general requirements for performance but require dedicated resources and isolated networks, such as databases, core ERP systems, and financial systems.

Table 4-1 General-purpose BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.s3.large	2 x 10 Core Intel Xeon E5-2618L V4 (2.20 GHz)	DDR4 RAM (128 GB)	2 x 600GB SAS System Disk RAID1	2 x 2-port 10GE + SDI
physical.s3.xlarge	2 x 14 Core Intel Xeon E5-2658 V4 (2.30 GHz)	DDR4 RAM (256 GB)	2 x 600GB SAS System Disk RAID1	2 x 2-port 10GE + SDI
physical.s3.2xlarge	2 x 10 Core Intel Xeon E5-2618L V4 (2.20 GHz)	DDR4 RAM (192 GB)	2 x 600GB SAS System Disk RAID1	2 x 2-port 10GE + SDI

- **Disk-intensive**
This BMS type uses local disks as both the system disk and data disks, and is ideal for scenarios that have large data volumes and require high computing performance, stability, and real-time performance, such as big data and distributed cache.

Table 4-2 Disk-intensive BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.d1.large	2 x 10 Core Intel Xeon E5-2618L V4 (2.20 GHz)	DDR4 RAM (128 GB)	2 x 600GB SAS System Disk RAID 1 + 8 x 4TB SATA	2 x 2-port 10GE

- **Memory-optimized**
This BMS type provides ultra-large memory of more than 1 TB and is ideal for scenarios such as in-memory databases, SAP HANA, and HPC fat nodes.

Table 4-3 Memory-optimized BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.m2.small	4 x 24 Core Xeon E7-8890 V4 (2.20 GHz)	DIMM RAM (1024 GB)	2 x 600GB SAS System Disk RAID1 + 7 x 1.8TB SAS HDD RAID5 + 2 x 1.6TB NVMe SSD	2 x 2-port 10GE + 16G FC + SDI
physical.m2.medium	4 x 24 Core Xeon E7-8890 V4 (2.20 GHz)	DIMM RAM (2048 GB)	2 x 600GB SAS System Disk RAID1	2 x 2-port 10GE + SDI
physical.m2.large	4 x 24 Core Xeon E7-8890 V4 (2.20 GHz)	DIMM RAM (3072 GB)	2 x 600GB SAS System Disk RAID1 + 14 x 1.8TB SAS HDD + 4 x 400GB SAS SSD + 2 x 1600GB NVMe SSD	2 x 2-port 10GE + SDI
physical.m2.xlarge	4 x 24 Core Xeon E7-8890 V4 (2.20 GHz)	DIMM RAM (4096 GB)	2 x 600GB SAS System Disk RAID1 + 14 x 1.8TB SAS HDD + 4 x 400GB SAS SSD + 2 x 1600GB NVMe SSD	2 x 2-port 10GE + SDI

- I/O-optimized
This BMS type uses SSD disks as both the system disk and data disks. It is ideal for high-performance big data, databases, and other scenarios that require high storage I/O performance.

Table 4-4 I/O-optimized BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.io1.large	2 x 10 Core E5 2618L V4 (2.20 GHz)	DDR4 RAM (256 GB)	2 x 800GB SAS SSD System Disk RAID1 + 4 x 3.2TB NVMe SSD	2 x 2-port 10GE

- GPU-accelerated

This BMS type includes computing-accelerated BMSs (P series) and graphics-accelerated BMSs (G series). It provides outstanding floating-point computing performance and is ideal for scenarios that require real-time, highly concurrent massive computing, such as deep learning, scientific computing, CAE, 3D animation rendering, and CAD.

Table 4-5 GPU-accelerated BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.p1.large	2 x 14 Core Intel Xeon E5-2690 V4 (2.60 GHz)	DDR4 RAM (512 GB)	2 x 600GB SAS HDD System Disk RAID1+ 6 x 800GB NVMe SSD Disk	NIC: 1 x 100G IB + 2 x 10GE + SDI GPU: 8 x Tesla P100 GPU memory: 16 GB
physical.p2.large	2 x 14 Core Intel Xeon E5-2690 V4 (2.60 GHz)	DDR4 RAM (512 GB)	2 x 600GB SAS HDD + 6 x 800GB NVMe SSD	NIC: 1 x 100G IB + 2 x 10GE + SDI GPU: 8 x Tesla V100 GPU memory: 16 GB
physical.g1.small	2 x 14 Core Intel Xeon E5-2690 V4 (2.60 GHz)	DDR4 RAM (256 GB)	2 x 600GB SAS + 960GB SSD	NIC: 3 x 2-port 10GE GPU: 1 x M60

4.3 x86 V5 BMS with Intel Skylake CPU

 CAUTION

x86 V5 BMSs will no longer be provisioned.

- General-purpose

This BMS type provides general compute, storage, and network specifications and supports attachment of EVS disks. It is ideal for systems that have general requirements for performance but require dedicated resources and isolated networks, such as databases, core ERP systems, and financial systems.

Table 4-6 General-purpose BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.s4.medium	2 x 10 Core Intel Xeon Silver 4114 V5 (2.20 GHz)	DDR4 RAM (128 GB)	None	2 x 2-port 10GE + SDI
physical.s4.large	2 x 10 Core Intel Xeon Silver 4114 V5 (2.20 GHz)	DDR4 RAM (192 GB)	None	2 x 2-port 10GE + SDI
physical.s4.xlarge	2 x 14 Core Intel Xeon Gold 5120 V5 (2.20 GHz)	DDR4 RAM (192 GB)	None	2 x 2-port 10GE + SDI
physical.s4.2xlarge	2 x 14 Core Intel Xeon Gold 5120 V5 (2.20 GHz)	DDR4 RAM (384 GB)	None	2 x 2-port 10GE + SDI
physical.s4.3xlarge	2 x 22 Core Intel Xeon Gold 6161 V5 (2.20 GHz)	DDR4 RAM (384 GB)	None	2 x 2-port 10GE + SDI

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.o3.small	2 x 4 Core Intel Skylake Xeon Gold 5122 V5 (3.60 GHz)	DDR4 RAM (192 GB)	None	2 x 2-port 10GE + SDI

- Disk-intensive

This BMS type uses local disks as both the system disk and data disks, and is ideal for scenarios that have large data volumes and require high computing performance, stability, and real-time performance, such as big data and distributed cache.

Table 4-7 Disk-intensive BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.d2.tiny	2 x 10 Core Intel Xeon Silver 4114 V5 (2.20 GHz)	DDR4 RAM (128 GB)	2 x 600GB SAS System Disk RAID1 + 12 x 1.8TB SAS	2 x 2-port 10GE
physical.d2.large	2 x 12 Core Intel Xeon Gold 5118 V5 (2.30 GHz)	DDR4 RAM (192 GB)	2 x 600GB SAS System Disk RAID1 + 12 x 10TB SATA	2 x 2-port 10GE
physical.d2.xmedium	2 x 18 Intel Xeon Gold 6151 V5 (3.00 GHz)	DDR4 RAM (384 GB)	2 x 600GB SAS RAID1 + 24 x 1.8TB SAS	2 x 2-port 10GE

- I/O-optimized

This BMS type uses SSD disks as both the system disk and data disks. It is ideal for high-performance big data, databases, and other scenarios that require high storage I/O performance.

Table 4-8 I/O-optimized BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.io2.xlarge	2 x 22 Core Intel Xeon Gold 6161 V5 (2.20 GHz)	DDR4 RAM (384 GB)	2 x 800GB SSD RAID1 + 10 x 800GB SSD	2 x 2-port 10GE

- High-performance computing
This BMS type uses InfiniBand NICs and provides a large number of CPU cores, large memory size, and high throughput. It is ideal for high-performance computing.

Table 4-9 High-performance computing BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.h2.large	2 x 18 Core Intel Xeon Gold 6151 V5 (3.00 GHz)	DDR4 RAM (192 GB)	1 x 1.6TB NVMe SSD	1 x 100G IB + 2 x 10GE + SDI
physical.hc2.xlarge	2 x 18 Core Intel Xeon Gold 6151 V5 (3.00 GHz)	DDR4 RAM (384 GB)	None	2 x 2-port 10GE + SDI

- GPU-accelerated
This BMS type provides powerful floating-point computing and is ideal for real-time, highly concurrent massive computing scenarios, such as deep learning, scientific computing, CAE, 3D animation rendering, and CAD.

Table 4-10 GPU-accelerated BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.p3.large	2 x 18 Core Intel Skylake 6151 V5 (3.00 GHz)	DDR4 RAM (512 GB)	2 x 1.2TB RAID 1 + 6 x 800GB NVMe SSD	NIC: 1 x 100G IB + 2 x 10GE + SDI GPU: 8 x Tesla V100 GPU memory: 32 GB

4.4 x86 V6 BMS with Intel Cascade Lake CPU

- General-purpose
This BMS type provides general compute, storage, and network specifications and supports attachment of EVS disks. It is ideal for systems that have general requirements for performance but require dedicated resources and isolated networks, such as databases, ERP systems, containers, and big data computing.

Table 4-11 General-purpose BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.c6s.3xlarge	2 x 26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	DDR4 RAM (384 GB)	None	SDI 3.0 (40 GE)
physical.c6sd.3xlarge	2 x 26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	DDR4 RAM (384 GB)	4 x 3.2TB NVMe SSD	SDI 3.0 (40 GE)
physical.c6sd.6xlarge	2 x 26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	DDR4 RAM (768 GB)	4 x 3.2TB NVMe SSD	SDI 3.0 (40 GE)

- High-performance computing
This BMS type meets the requirements of multi-core, high-frequency, and low-latency HPC.

Table 4-12 High-performance computing BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.h6.xlarge	2 x 22 Core Intel Cascade Lake 6266 V6 (3.00 GHz)	DDR4 RAM (192 GB)	None	100G Mellanox IB (RDMA) + SDI 3.0 (40 GE)

- GPU-accelerated

This BMS type uses NVIDIA T4 GPU and meets the requirements of AI inference and graphics acceleration services.

Table 4-13 GPU-accelerated BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration
physical.pi6.3xlarge.6	2 x 26 Core Intel Cascade Lake 6278 V6 (2.60 GHz)	DDR4 RAM (448 GB)	2 x 480GB SATA SSD + 1.6TB NVMe SSD	NIC: 2 x 10GE (IN200) + 2 x 25GE (IN200) GPU: 6 x NVIDIA T4

4.5 Kunpeng V1 BMS

Kunpeng BMSs use Kunpeng 920 processors to offer powerful computing and high-performance networks, meeting the requirements of governments and Internet enterprises for cost-effective, secure, reliable cloud services.

Table 4-14 Kunpeng BMS specifications

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration	QingTian Architecture
physical.k1.2xlarge	2 x 64 Core Kunpeng 920-6426 (2.60 GHz)	256 DDR4 RAM (GB)	960 GB SAS SSD	2 x 25GE + 2 x 25GE	No

Flavor Name/ID	CPU	Memory	Local Disk	Extended Configuration	QingTian Architecture
physical.k s1ne.2xlarge	2 x 64 Core Kunpeng 920-6426 (2.60 GHz)	256 DDR4 RAM (GB)	None	SDI 3.0 (40 GE)	Yes
physical.k s1ne.4xlarge	2 x 64 Core Kunpeng 920-6426 (2.60 GHz)	512 DDR4 RAM (GB)	2 x 3.2TB NVMe SSD	SDI 3.0 (40 GE)	Yes
physical.k s1ne.8xlarge	2 x 64 Core Kunpeng 920-6426 (2.60 GHz)	1024 DDR4 RAM (GB)	2 x 3.2TB NVMe SSD	SDI 3.0 (40 GE)	Yes
physical.k h1ne.2xlarge	2 x 64 Core Kunpeng 920-6426 (2.60 GHz)	256 DDR4 RAM (GB)	960 GB SAS SSD	1 x 100G RDMA(Mellanox)+ SDI 3.0 (40 GE)	Yes

4.6 Lifecycle

The lifecycle of a BMS contains all states from its creation to deletion.

Figure 4-1 BMS states

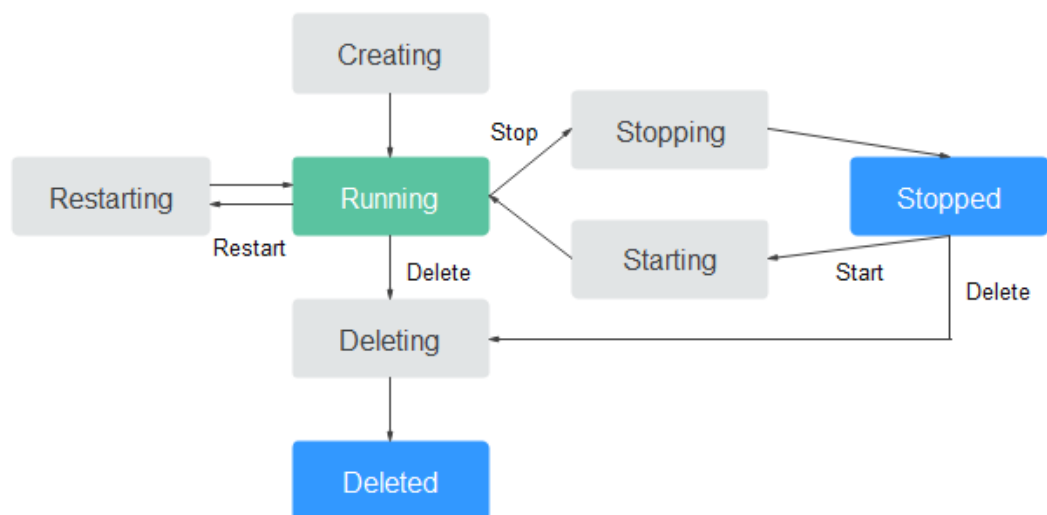


Table 4-15 BMS states

State	Attribute	Description	API Status
Creating	Intermediate state	A BMS is in this state after you request for the BMS and before it enters the running state. If a BMS remains in this state for a long time, exceptions will occur. Contact the operation administrator to handle the exceptions.	BUILD/ BUILDING
Starting	Intermediate state	It is an intermediate state between Stopped and Running . If a BMS remains in this state for a long time, exceptions will occur. Contact the operation administrator to handle the exceptions.	SHUTOFF
Running	Stable state	A BMS is in this state when it is running properly. A BMS in this state can be used normally.	ACTIVE
Stopping	Intermediate state	It is an intermediate state between Running and Stopped . If a BMS remains in this state for a long time, exceptions will occur. Contact the operation administrator to handle the exceptions.	ACTIVE
Stopped	Stable state	A BMS is in this state after it is stopped successfully. A BMS in this state cannot be used.	SHUTOFF
Restarting	Intermediate state	A BMS is in this state when it is being restarted. If a BMS remains in this state for a long time, exceptions will occur. Contact the operation administrator to handle the exceptions.	REBOOT
Forcibly restarting	Intermediate state	A BMS is in this state when it is being forcibly restarted.	HARD_REBOOT
Deleting	Intermediate state	A BMS is in this state when it is being deleted. If a BMS remains in this state for a long time, exceptions will occur. Contact the operation administrator to handle the exceptions.	ACTIVE/ SHUTOFF/ REBOOT/ HARD_REBOOT/ ERROR

State	Attribute	Description	API Status
Deleted	Intermediate state	A BMS is in this state after it is deleted successfully. A BMS in this state cannot be used and will be removed from the system in a short time.	DELETED
Faulty	Stable state	A BMS is in this state when an exception occurs on it. A BMS in this state cannot be used. Contact the operation administrator to rectify the fault.	ERROR
Rebuilding	Intermediate state	A BMS is in this state when it is being rebuilt.	SHUTOFF
Reinstalling OS	Intermediate state	A BMS is in this state when its OS is being reinstalled.	SHUTOFF
Reinstalling OS failed	Stable state	An exception occurred when the BMS OS was being reinstalled and the reinstallation failed. A BMS in this state cannot be used. Contact the operation administrator to rectify the fault.	SHUTOFF

5 Image

5.1 Overview

What Is an Image?

An image is a template of the BMS running environment. It contains an OS and runtime environment, and some pre-installed applications. An image file is equivalent to a copy file that contains all data in the system disk.

Image Types

Images can be classified into public images, private images, and shared images.

Table 5-1 Image types

Image Type	Description
Public image	A public image is provided by the cloud platform and is available to all users. It contains an OS and preinstalled public applications.
Private image	A private image is created by a user and is available only to the user who created it. It contains an OS, pre-installed public applications, and the user's private applications. Using a private image to create BMSs frees you from repeatedly configuring BMSs.
Shared image	A shared image is a private image other users share with you.

Public Images

Public images are provided by Huawei Cloud. These images are available to all users, compatible with BMSs and most mainstream OSs, and are pre-installed with necessary plug-ins. Public images available to you vary depending on the BMS flavor you selected. For details, see [OSs Supported by Different Types of BMSs](#).

Characteristics

- OS types: Linux and Windows OSs that are updated and maintained periodically
- Pre-installed software: plug-ins that BMS storage, networks, and basic functions depend on

⚠ CAUTION

These plug-ins are necessary for BMSs to run properly. Do not delete or modify any of them. Otherwise, basic BMS functions will be affected.

Table 5-2 Pre-installed software

Software	Description
Cloud-Init	Cloud-Init is an open-source cloud initialization program, which initializes specific configurations, such as the host name, key, and user data, of a newly created BMS.
One-click password reset plug-in	BMS provides the one-click password resetting function. If you lose your BMS password or it expires, the password reset plug-in enables you to set a new password on the management console.
bms-network-config	This plug-in is used to automatically configure BMS networks during BMS provisioning and restore the BMS network when the network is interrupted due to faults. The plug-in is stored in the <code>/opt/huawei</code> directory. Do not delete or modify it.
SDI iNIC frontend driver plug-in	This plug-in is installed in the image so that EVS disks can be attached to BMSs. In this way, BMSs can be booted from EVS disks, facilitating quick BMS provisioning.

- Compatibility: compatible with server hardware
- Security: highly stable and licensed
- Restrictions: no restrictions on usage

Private Images

A private image contains an OS, preinstalled public applications, and a user's private applications. You can use a private image to create BMSs without having to repeatedly configure them.

Characteristics

- Compatibility: Private images can be used to deploy servers that are of the same model as the source BMS and may fail to deploy servers of other models.

- Functions: You can create and delete private images, as well as create BMSs and reinstall the BMS OS using private images. You can also perform the following operations:
 - [Share images](#) with other tenants.
 - [Replicate images](#) across regions.
 - [Export images](#) to your OBS bucket.
- Restrictions: You can create a maximum of 50 private images.
- Pricing: You will be charged for storing private images. For more information, see [Pricing Details](#).

Shared Images

A shared image is a private image other users share with you.

Application Scenarios

- Deploying software environments in a batch
Prepare a BMS with an OS, the partition arrangement you prefer, and software installed to create a private image. You can use the image to create batch clones of your custom BMS.
- Backing up a BMS
Create an image from a BMS to back up the BMS. If the software of the BMS becomes faulty, you can use the image to restore the BMS.

5.2 OSs Supported by Different Types of BMSs

The following tables list the 64-bit OSs supported by different BMS types.

- [Table 5-3](#) lists the OSs supported by x86 V4 BMSs with Intel Broadwell CPU.
- [Table 5-4](#) lists the OSs supported by x86 V5 BMSs with Intel Skylake CPU.
- [Table 5-5](#) lists the OSs supported by x86 V6 BMSs with Intel Cascade Lake CPU.
- [Table 5-6](#) lists the OSs supported by BMSs with Kunpeng CPU.

NOTE

- It is recommended that you use the official OS release versions. Do not tailor or customize the release versions, or problems may occur.
- OS vendors do not always update OS release versions regularly. Some versions are no longer maintained, and these deprecated versions no longer receive security patches. Ensure that you read the update notifications from OS vendors and update your OS so that it runs properly.
- For CentOS 7.4 or earlier, BMS extension NICs cannot be pinged due to known kernel issues. So, you are advised to use CentOS 7.5 or later. For details, see [How Do I Handle the Failure to Ping a CentOS 7 Extension NIC?](#)

Table 5-3 OSs supported by BMSs with x86 V4 CPU

BMS Type	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
Disk-intensive physical.d1.large	Windows Server 2012 R2/2016 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
General-purpose physical.s3.large physical.s3.xlarge physical.s3.2xlarge	Windows Server 2012 R2/2016 Standard	CentOS 6.7/6.8/6.9/7.2/7.3/7.4/7.5/7.6	Red Hat 6.7/6.8/6.9/6.10/7.2/7.3/7.4/7.5	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
Memory-optimized physical.m2.small physical.m2.medium physical.m2.large physical.m2.xlarge	-	CentOS 7.2	-	-	-	-	-
I/O-optimized physical.io1.large	Windows Server 2012 R2/2016 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

BMS Type	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
GPU-accelerated physical.p1.large physical.p2.large physical.g1.small	-	CentOS 7.4/7.5/7.6	-	-	Ubuntu 16.04 LTS	-	EulerOS 2.3

Table 5-4 OSs supported by BMSs with x86 V5 CPU

BMS Type	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
Disk-intensive physical.d2.large physical.d2.tiny physical.d2.xmedium	Windows Server 2012 R2/2016 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 2.3
General-purpose physical.s4.medium physical.s4.large physical.s4.xlarge physical.s4.2xlarge physical.s4.3xlarge	Windows Server 2012 R2/2016 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

BMS Type	Windows	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
I/O-optimized physical.io 2.xlarge	Windows Server 2012 R2/2016 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
High-performance computing physical.h 2.large	-	CentOS 6.9/7.3/7.4/7.5/7.6	-	SUSE Linux Enterprise 11.SP4	Ubuntu 16.04 LTS	-	EulerOS 2.3
High-performance computing physical.h c2.xlarge	Windows Server 2012 R2/2016 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-accelerated physical.p 3.large	-	-	-	-	-	-	EulerOS 2.3

Table 5-5 OSs supported by BMSs with x86 V6 CPU

BMS Type	CentOS	Red Hat	SUSE	Ubuntu	Oracle Linux	EulerOS
General-purpose physical.s6.xlarge physical.c6s.3xlarge physical.c6sd.3xlarge physical.c6sd.6xlarge	CentOS 7.6/7.8/7.9/8.2	Red Hat 7.6	SUSE Linux Enterprise 15.SP2	Ubuntu 18.04.3 LTS	Oracle Linux7.6	EulerOS 2.5
High-performance computing physical.h6.large	CentOS 7.6/7.8/7.9	-	-	-	-	-
GPU-accelerated physical.pi6.3xlarge.6	CentOS 7.6	-	-	-	-	-

Table 5-6 OSs supported by BMSs with Kunpeng CPU

BMS Type	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 EVS Disk

What Is Elastic Volume Service (EVS)?

EVS offers scalable block storage for BMSs. EVS disks feature high reliability, high performance, and rich specifications, and are ideal for distributed file systems, development and test environments, data warehouse applications, and high-performance computing (HPC) scenarios.

Unlike traditional servers that can only use local disks, BMSs can use EVS disks that are not constrained by capacity. Shared EVS disks allow concurrent reads and writes by multiple BMSs, enabling you to deploy core applications in clusters.

EVS Disk Types

BMSs support the following types of EVS disks:

- **Common I/O (previous generation):** This EVS disk type delivers a maximum of 2200 IOPS. It is ideal for application scenarios that require large capacity, medium read/write speed, and fewer transactions, such as enterprise applications and small-scale testing.
- **High I/O:** This EVS disk type delivers a maximum of 5,000 IOPS and a minimum of 1 ms read/write latency. It is designed to meet the needs of mainstream high-performance, high-reliability application scenarios, such as enterprise applications, large-scale development and testing, and web server logs.
- **Ultra-high I/O:** This EVS disk type delivers a maximum of 33,000 IOPS and a minimum of 1 ms read/write latency. It is excellent for ultra-high I/O, ultra-high bandwidth, and read/write-intensive application scenarios, such as distributed file systems in HPC or NoSQL/RDS in I/O-intensive scenarios.
- **General purpose SSD:** This EVS disk type delivers a maximum of 20,000 IOPS and a minimum of 1 ms read/write latency. It is designed to meet the needs of mainstream high-performance, low-latency, interactive application scenarios, such as enterprise office applications, large-scale development and testing, transcoding, web server logs, and containers.
- **Extreme SSD:** This EVS disk type delivers up to 128,000 IOPS and sub-millisecond read latencies. With RDMA integrated with low-latency congestion control algorithms, this disk type is suitable for application scenarios that require ultra-high bandwidth and ultra-low latency.

NOTICE

EVS disks cannot be attached to `physical.d2.large` (disk-intensive) or `physical.io2.xlarge` (I/O-optimized) because they are mainly used for big data.

EVS Disk Performance

The key indicators of EVS disk performance include read/write latency, IOPS, and throughput.

- IOPS: number of read/write operations performed by an EVS disk per second
- Throughput: amount of data successfully transmitted by an EVS disk per second, that is, the amount of data read from and written into an EVS disk
- Read/write latency: minimum interval between two consecutive read/write operations of an EVS disk

For more details, see [Disk Types and Performance](#).

EVS Disk Device Types

BMS supports only Small Computer System Interface (SCSI) EVS disks.

On the management console, you can create EVS disks with **Device Type** set to **SCSI**. The EVS disks support transparent SCSI command transmission, allowing BMS OSs to directly access underlying storage media. The EVS disks support basic read/write SCSI commands and advanced SCSI commands.

NOTE

BMS public image OSs are preinstalled with the driver required to use SCSI disks, so you do not need to install the driver. To know how to install the driver, see [Installing the SDI Card Driver](#) in *Bare Metal Server Private Image Creation Guide*.

7 Network

BMS network types include:

- VPC
- High-speed network, enhanced high-speed network
- IB network
- User-defined VLAN

Table 7-1 BMS network types

Network	Network Feature	x86 V4 BMS	x86 V5 BMS	x86 V6 BMS	Kunpeng BMS
VPC	Supported	Yes	Yes	Yes	Yes
	Bandwidth	10 GE	10 GE	40 GE	40 GE
	Number of NICs	2	2	32	32
High-speed network	Supported	Yes	Yes	No	No
	Bandwidth	Share the bandwidth with VPCs.	Share the bandwidth with VPCs.	N/A	N/A
Enhanced high-speed network	Supported	Yes	Yes	No	No
	Bandwidth	10 GE	10 GE	N/A	N/A
IB network	Supported	Yes. (Only specific BMSs support IB networks.)	Yes. (Only specific BMSs support IB networks.)	Yes. (Only specific BMSs support IB networks.)	Yes. (Only specific BMSs support IB networks.)

Network	Network Feature	x86 V4 BMS	x86 V5 BMS	x86 V6 BMS	Kunpeng BMS
	Bandwidth	100 GE	100 GE	100 GE	100 GE
User-defined Network	Supported	Yes. User-defined networks depend on enhanced high-speed networks and dedicated gateways.	Yes. User-defined networks depend on enhanced high-speed networks and dedicated gateways.	No	No

BMS provides five types of networks: VPC, high-speed network, enhanced high-speed network, user-defined VLAN, and IB network. They are isolated from each other.

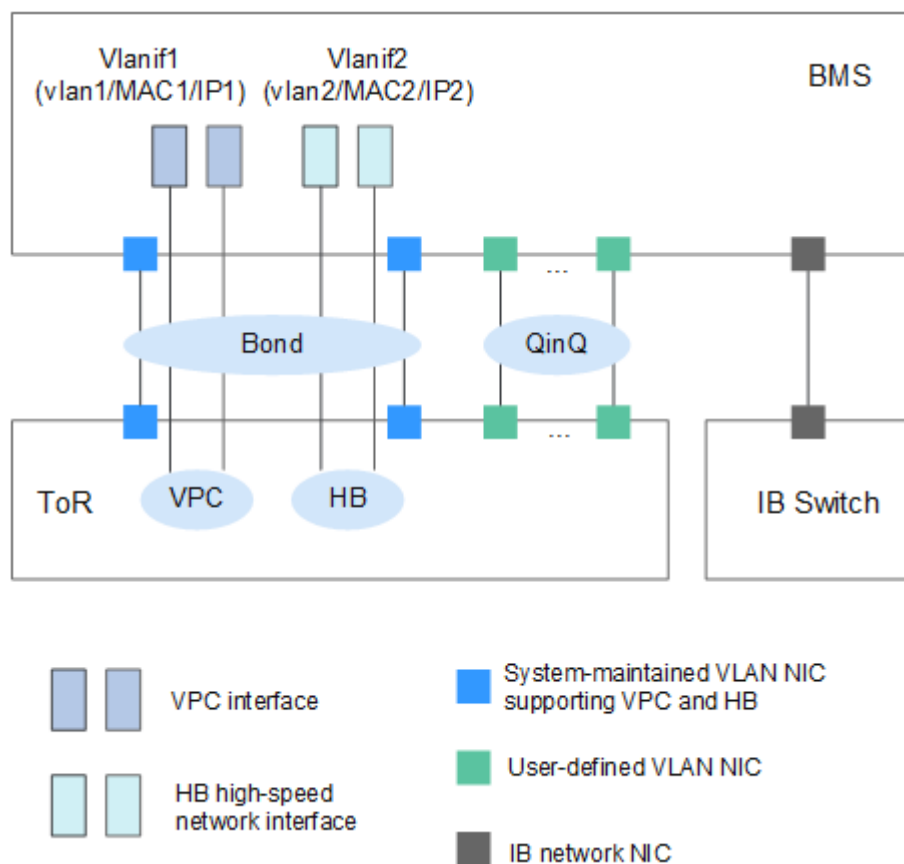
x86 V4/V5 BMS:

VPC and high-speed network interfaces are VLAN sub-interfaces created after system maintenance VLAN NICs are bonded. You can manage and configure NICs of user-defined VLANs and IB networks.

x86 V6/Kunpeng BMS:

The QingTian architecture improves the network performance and VPC NIC bonding provides high reliability.

Figure 7-1 BMS networks



NOTE

- In the preceding figure, ToR indicates the cabling mode in the server cabinet. The access switch is placed on top of the rack and the server is placed beneath it. HB indicates a high-speed network. QinQ indicates an 802.1Q tunnel.
- VPC and high-speed network interfaces are generated by the system and cannot be changed. They are configured in the same NIC bond.
- BMSs can communicate with ECSs through VPCs or IB networks (if any).
- Only VPC supports security groups, EIPs, and ELB.
- For a high-speed network and user-defined VLAN, BMSs in the same network communicate with each other only through layer-2 connections.

VPC

A VPC is a logically isolated, configurable, and manageable virtual network. It helps improve the security of cloud resources and simplifies network deployment. You can create security groups and VPNs, configure IP address ranges, and specify bandwidth sizes in your VPC. With a VPC, you can easily manage and configure internal networks and change network configurations. You can also customize access rules to control BMS access within a security group and across different security groups to enhance BMS security.

For more information, see [Virtual Private Cloud Service Overview](#).

High-Speed Network

A high-speed network is an internal network between BMSs. It provides high bandwidth for connecting BMSs in the same AZ. If you want to deploy services that require high throughput and low latency, you can create high-speed networks. Currently, the BMS service supports high-speed networks with a maximum bandwidth of 10 Gbit/s.

Enhanced high-speed networks use upgraded hardware and software and provide performance superior to high-speed networks.

Enhanced high-speed networks have the following advantages:

- The bandwidth is 10 Gbit/s or higher.
- The number of network planes can be customized and a maximum of 4,000 subnets are supported.

User-defined VLAN

You can use the 10GE Ethernet NICs that are not being used by the system to configure a user-defined VLAN. The QinQ technology is used to isolate networks and provide additional physical planes and bandwidths. You can create VLANs to isolate network traffic. User-defined VLAN NICs are in pairs. You can configure NIC bonding to achieve high availability. User-defined VLANs in different AZs cannot communicate with each other.

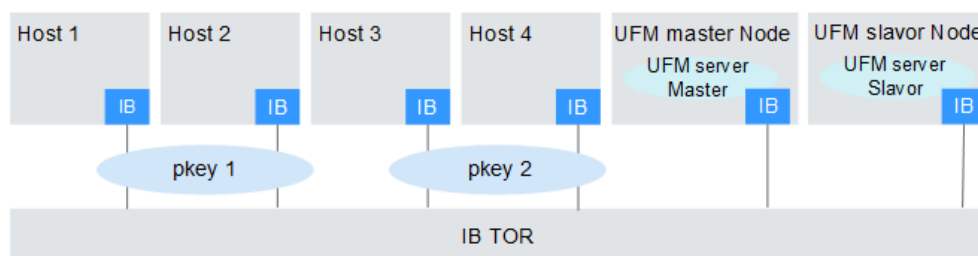
NOTE

QinQ is a layer 2 tunnel protocol based on IEEE 802.1Q encapsulation. It adds a public VLAN tag to a frame with a private VLAN tag and allows the frame with double VLAN tags to be transmitted over the service provider's backbone network based on the public VLAN tag. This provides a layer 2 VPN tunnel for customers.

IB Network

An IB network features low latency and high bandwidth and is used in a number of High Performance Computing (HPC) projects. It uses the 100 Gbit/s Mellanox IB NIC, dedicated IB switch, and controller software UFM to ensure network communication and management, and uses the Partition Key to isolate IB networks of different tenants (similar to VLANs in an Ethernet).

Figure 7-2 IB network isolation



 **NOTE**

Unified Fabric Manager (UFM) is the IB switch controller of an IB network based on OpenSM software and provides northbound interfaces. It is deployed in active/standby mode.

8 Security

8.1 Shared Responsibilities

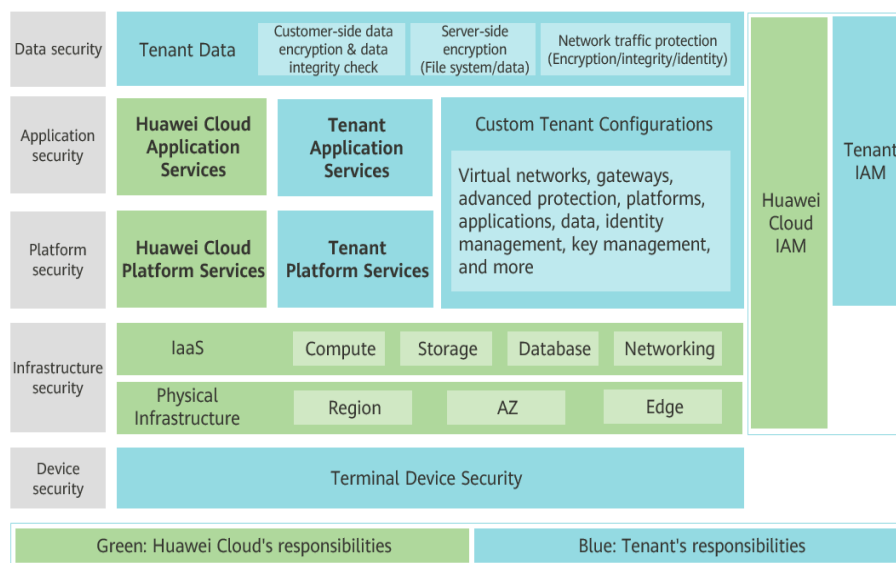
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 8-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud:** Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant:** Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 8-1 Huawei Cloud shared security responsibility model



8.2 Identity Authentication and Access Control

Identity and Access Management (IAM) provides functions such as user identity authentication, permission assignment, and access control. You can use IAM to securely control user access to your BMSs. IAM permissions define which actions on your cloud resources are allowed or denied. After creating an IAM user, add it to a user group and grant the permissions required by BMS to the user group. Then, all users in this group will be automatically granted with these permissions.

Account Security

If you are an enterprise administrator, you can use IAM to create a user and grant permissions to the user. Enterprise employees can use the user account to access the system, and you do not need to share your account password or key pair with them. This helps you manage resources efficiently. You can also configure account security policies to protect these user accounts and reduce security risks for your enterprise information.

Fine-Grained Authorization

You can grant refined permissions to employee accounts to ensure that cloud services are properly used. For details, see [BMS Permissions Policies and Supported Actions](#).

Security Group

A security group is a virtual firewall that detects status and filters data packets. It is an important network isolation method used for access control of ECSs, BMSs, load balancers, and databases.

You can configure security group rules to allow instances in a security group to access the public or private network.

- A security group is a logical group. You can add BMSs that have the same security protection requirements within a region to the same security group.
- By default, BMSs in the same security group can communicate with each other through an internal network, whereas BMSs in different security groups cannot.
- You can modify a security group rule at any time, and the modification takes effect immediately.

Default Security Group

When you create a BMS in a region, the system will create a default security group if there is no security group in the region.

The default security group rule allows all outgoing data packets and blocks incoming data packets. BMSs in this security group can access each other already. You do not need to add additional rules.

Figure 8-2 Default security group

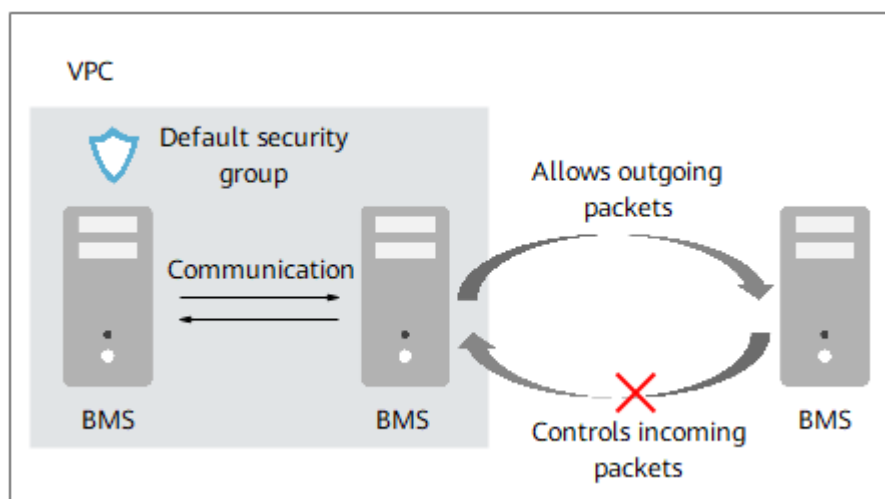


Table 8-1 describes the rules of the default security group (**Sys-default**).

Table 8-1 Rules in the default security group

Direction	Priority	Action	Protocol	Port/Range	Source/Destination	Description
Outbound	100	Allow	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	100	Allow	All	All	Source: Current security group name	Allows communications among BMSs within the same security group on any port.

Direction	Priority	Action	Protocol	Port/Range	Source/Destination	Description
Inbound	100	Allow	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux BMSs over SSH.
Inbound	100	Allow	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows BMSs over RDP.

For more information, see [Security Group Overview](#).

Key Pair Authentication

- What is a key pair?

A key pair, or SSH key pair, is an authentication method used when you remotely log in to Linux instances. A key pair is generated using an encryption algorithm. It contains a public key, and a private key reserved for you. The public key is used to encrypt data (for example, a password), and the private key is used to decrypt the data.

Huawei Cloud stores the public key, and you need to store the private key. Do not share your private key with anyone. Keep your private key secure.

- Advantages

A key pair is more secure and easier to use than username/password in authentication.

Table 8-2 Comparison between the key pair and username/password

Item	Key pair	Username and Password
Security	<ul style="list-style-type: none">• More secure than username/password and free from brute-force attacks• Cannot be derived from the public key	Less secure
Easy to use	Simultaneous login to a large number of Linux instances, simplifying management	Login to only one Linux instance at one time, giving no chance of batch maintenance

- Constraints
 - Only Linux instances support the key pair method.

- Only RSA key pairs are supported. RSA keys are typically 1024, 2048, or 4096 bits long.
- A Linux instance can have only one key pair. If a key pair has been bound to your BMS and you bind a new key pair to the BMS, the new key pair will replace the original one.
- Generation
 - Create a key pair on the management console.
 - 📖 **NOTE**
 - When a key pair is generated, download and properly keep it.
 - Use PuTTYgen to create a key pair and import the key pair into Huawei Cloud.

Helpful Links

[Using an SSH Key Pair](#)

8.3 Data Protection

BMS takes different measures to ensure data security and reliability.

- BMSs offer physical server-level performance and isolation. They provide dedicated computing resources without any loss due to virtualization. Such BMSs can ensure the security of data stored on them.
- If a BMS uses local disks, RAID can be used to improve fault tolerance and ensure data security.
- You can boot BMSs without local disks from Elastic Volume Service (EVS) disks and provision the BMSs within minutes. Cloud Server Backup Service (CSBS) provides the backup service for BMSs. It works based on the consistent snapshot technology for EVS disks. With CSBS, you can use backup data to restore BMS, ensuring data security and correctness.

8.4 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records for security analysis, audit compliance, resource tracking, and fault locating.

After CTS is enabled, it can record BMS operations.

- If you want to enable and configure CTS, refer to [CTS Getting Started](#).

8.5 Risk Control

Server Monitoring

Server monitoring provided by Cloud Eye includes basic monitoring and OS monitoring. Basic monitoring refers to monitoring of server metrics automatically

reported (BMS does not support basic monitoring). OS monitoring provides system-wide, active monitoring for BMSs, on which Agent is installed. Agent uses less than 50 MB of memory and 1.5% of CPU resources.

To meet the basic monitoring and O&M requirements for servers, more than 40 metrics (such as CPU, memory, disk, and network) will be monitored.

- [Cloud Eye Functions](#)
- [Monitored Metrics](#)

Mission-Critical Operation Protection

BMS provides protection against mission-critical operations. If you want to perform a mission-critical operation on the management console, you must enter a credential that can prove your identity. You can perform the operation only after passing the identity authentication. For account security, you are advised to enable operation protection. The setting will take effect for both the account and users under the account.

8.6 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

Figure 8-3 Downloading compliance certificates

Download Compliance Certificates

Please enter a keyword to search

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

ENS

Mandatory law for companies in the public sector and their technology suppliers

Download

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the Level 3 (highest) certification of MTCS.

Download

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

ISO 27001:2022

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Download

ISO 27017:2015

ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 8-4 Resource center

Resource Center

White Papers

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

9 Billing

9.1 Billing

Billing Items

The billing items include BMS, EVS disk (optional), and EIP (optional). For details, see [Table 9-1](#).

Table 9-1 BMS billing

Billing Item	Description
BMS	Pricing for the BMS is based on the specifications you choose, including CPU, memory, local disks, and extended configurations. For details, see BMS Pricing Details .
(Optional) EVS disk	EVS disks that you create when you create a BMS are billed in the same manner as the BMS, but those you later attached to a BMS are billed independently (pay-per-use or yearly/monthly). For details, see EVS Pricing Details .
(Optional) EIP	You can bind an EIP to a BMS and pay for the EIP by bandwidth or traffic. For details, see EIP Pricing Details .

Billing Modes

BMSs are billed on a yearly/monthly basis and cannot be billed on a pay-per-use basis. You can buy 10 months and get two free. If you intend to use BMSs for a long term, you can save more by specifying a longer duration.

Billing Involved in Specifications Changes

If you require additional storage space, you can either expand the capacity of EVS disks that are attached to a BMS or attach more EVS disks to the BMS. The

additional storage space will be billed on a pay-per-use or yearly/monthly basis depending on the billing modes you specified for the EVS disks.

FAQ

- [Where Can I Query the BMS Price?](#)
- [What Are Pre-payment and Post-payment? How Do I Choose Between Them?](#)
- [What Is the Impact on Billing if I Unsubscribe from a BMS?](#)
- [How Do I Set Automatic Renewal for BMSs Billed on a Yearly/Monthly Basis?](#)
- [When Will a BMS Be Released After It Expires?](#)

10 Permissions

Background

If you need to assign different permissions to personnel in your enterprise to access your BMSs, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your Huawei Cloud resources.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. For example, if you want some software developers in your enterprise to use BMSs but do not want them to delete BMSs or perform any other high-risk operations, you can create IAM users and grant permission to use BMSs but not permission to delete them.

If your Huawei Cloud account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

For more information, see [IAM Service Overview](#).

BMS Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

BMS is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, ap-southeast-2) in the specified regions (for example, AP-Bangkok), the users only have permissions for BMSs in the selected projects. If you set **Scope** to **All resources**, users have permissions for BMSs in all region-specific projects. When accessing BMSs, the users need to switch to the authorized region.

You can grant user permissions by using roles and policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Huawei Cloud services

depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.

- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage BMSs of a certain type. A majority of fine-grained policies contain permissions for specific APIs. For the API actions supported by BMS, see [Permissions and Supported Actions](#).

Table 10-1 lists all the system-defined permissions for BMS.

Table 10-1 System-defined permissions for BMS

Role/Policy Name	Description	Type
BMS FullAccess	Administrator permissions for BMS. Users with these permissions can perform all operations on BMSs.	System-defined policy
BMS CommonOperations	Common user permissions for BMS. Users with these permissions can start, stop, restart, and query BMSs.	System-defined policy
BMS ReadOnlyAccess	Read-only permissions for BMS. Users with these permissions can only view BMS data.	System-defined policy

Table 10-2 lists the common operations supported by system-defined permissions for BMS.

Table 10-2 Common operations supported by system-defined permissions

Operation	BMS FullAccess	BMS CommonOperations	BMS ReadOnlyAccess
Creating BMSs	√	x	x
Querying BMSs	√	√	√
Querying BMS details	√	√	√
Changing the name of a BMS	√	x	x
Starting a BMS	√	√	x
Stopping a BMS	√	√	x

Operation	BMS FullAccess	BMS CommonOperations	BMS ReadOnlyAccess
Restarting a BMS	√	√	x
Attaching a data disk to a BMS	√	√	x
Detaching a data disk from a BMS	√	√	x
Reinstalling a BMS OS	√	x	x
Resetting a BMS password with a few clicks	√	x	x

Helpful Links

- [IAM Service Overview](#)
- [Permissions Policies and Supported Actions](#)

11 Region and AZ

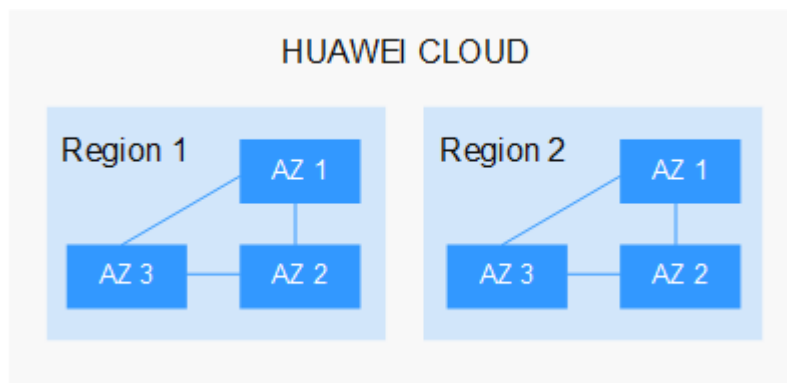
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 11-1 shows the relationship between regions and AZs.

Figure 11-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see [Huawei Cloud Global Regions](#).

Selecting a Region

When selecting a region, consider the following factors:

- Location

It is recommended that you select the closest region for lower network latency and quick access.

- If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
- If your target users are in Africa, select the **AF-Johannesburg** region.
- If your target users are in Latin America, select the **LA-Santiago** region.

 **NOTE**

The **LA-Santiago** region is located in Chile.

- Resource price

Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

12 Related Services

Relationships Between BMS and Other Services

Table 12-1 Relationships between BMS and other services

Service	Relationship	Main Interactions/ Best Practices
Image Management Service (IMS)	You can quickly create BMSs using images. You can also create private images using BMSs and share them with other users.	<ul style="list-style-type: none">• Creating a BMS Using a Private Image• Creating a Private Image from a BMS• Creating a Private Image from an External Image File
Virtual Private Cloud (VPC)	You can configure a logically isolated network for your BMSs and configure security groups, VPN, IP address segments, and bandwidth. With a VPC, you can easily manage and configure internal networks and change network configurations. You can also customize access rules to control BMS access within a security group and across different security groups to enhance BMS security.	<ul style="list-style-type: none">• Adding Security Group Rules• Binding an EIP

Service	Relationship	Main Interactions/ Best Practices
Dedicated Cloud (DeC)	<p>Resources in a DeC are physically isolated from those in public resource pools. If your services have high security compliance requirements, you can create BMSs in a DeC. You can create a dedicated BMS in either of the following ways:</p> <ul style="list-style-type: none"> Method 1: Create a dedicated BMS on the DeC console. Method 2: Create a dedicated BMS on the Cloud Server Console. 	<ul style="list-style-type: none"> Enabling a DeC Creating a Dedicated BMS
Elastic Volume Service (EVS)	<p>You can attach EVS disks to a BMS and expand their capacity at any time.</p>	<ul style="list-style-type: none"> Attaching Data Disks Initializing Data Disks Detaching Data Disks Expanding Disk Capacity
Dedicated Distributed Storage Service (DSS)	<p>DSS provides you with dedicated, physical storage resources. DSS features data redundancy and cache acceleration and provides highly reliable, durable, low-latency, and stable storage resources. It provides enterprise-class performance in a wide range of scenarios, such as HPC, OLAP, and a mix of loads.</p>	<ul style="list-style-type: none"> Disk Types
Cloud Eye	<p>After you obtain a BMS and install and configure Agent on the BMS, you can view the monitoring data of the BMS in Cloud Eye.</p>	<ul style="list-style-type: none"> Server Monitoring Overview Supported Monitoring Metrics (with Agent Installed)
Tag Management Service (TMS)	<p>You can tag BMSs to classify and search them more easily.</p>	<ul style="list-style-type: none"> Adding Tags Searching for Resources by Tag Deleting Tags

13 Features and Constraints

Features

BMS

- Automatic BMS provisioning and remote login to BMSs through the management console
- Managing the lifecycle of a BMS, including querying, starting, stopping, restarting, and deleting a BMS
- One-click password reset
- Reinstalling the OS
- Rebuilding a BMS if the BMS hardware or SDI iNIC is damaged
- Using Cloud Server Backup Service (CSBS) to back up BMS configurations and EVS disk data into Object Storage Service (OBS) buckets for data security
- Injecting scripts to simplify BMS configuration and initialization
- Installation of Cloudera's Distribution Including Apache Hadoop (CDH) on BMSs, which enables communication with other services you have purchased
- Using APIs to manage BMSs
- Server monitoring, with which you can obtain the CPU, memory, and disk I/O metrics of your BMSs
- Tagging BMSs to make them easier to identify and search

Disk

- Attaching EVS disks to or detaching EVS disks from Linux or Windows BMSs
- Shared EVS disks
- Dynamic capacity expansion of EVS disks

Image

- Using a public, private, or shared image to create BMSs
- Creating a private image from a BMS
- Creating a private image from an external image file
- Sharing images, replicating images across regions, and exporting images to an OBS bucket

Network

- VPC and IB network
- Creating a security group and defining rules to protect BMS security
- Binding an EIP to a BMS to enable the BMS to access the Internet
- Attaching multiple NICs to a BMS

Constraints

- External hardware devices (such as USB devices, bank USB keys, external hard disks, and dongles) cannot be loaded.
- Out-of-band management is not supported. Your BMSs are managed and maintained by Huawei Cloud.
- Live migration is not supported. If a BMS is faulty, your services running on it may be affected. It is good practice to deploy your services in a cluster or in primary/standby mode to ensure high availability.
- You cannot create a server without an OS, that is, a BMS must have an OS.
- After a BMS is created, you cannot change its VPC.
- Virtualization software cannot be installed on a BMS.
- When you create a BMS, you can only select a flavor with specified CPU, memory, and local disks but cannot configure them separately. After a BMS is created, you can expand the capacity of attached EVS disks but cannot modify the BMS CPU, memory, or local disks.
- You can only attach EVS disks whose device type is **SCSI** to a BMS.
- You cannot attach EVS disks to BMSs of certain flavors or BMSs created from certain images because these BMSs do not have SDI iNICs or lack compatibility.
- Do not delete or modify built-in plug-ins of an image, such as Cloud-Init and bms-network-config. Otherwise, basic BMS functions may be unavailable.
- If you choose to assign an IP address automatically when you create a BMS, do not change the private IP address of the BMS after the BMS is provisioned. Otherwise, the IP address may conflict with that of another BMS.
- BMSs do not support bridge NICs because they will cause network interruptions.
- Do not upgrade the OS kernel. Otherwise, the hardware driver may become incompatible with the BMS and adversely affect the BMS reliability.
- You can stop a BMS only on the management console and cannot run **shutdown** to stop it.
- Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. The BMS service has no independent quota. It shares the number of instances, CPU cores, and memory with the ECS service. You can view BMS quota in the **Elastic Cloud Server** row. For details see [How Do I View My Quotas?](#)

14 Change History

Released On	Description
2022-11-15	<p>This issue is the fifteenth official release.</p> <p>Added the following content:</p> <ul style="list-style-type: none"> Shared Responsibilities Identity Authentication and Access Control Data Protection Auditing and Logging Risk Control Certificates
2022-11-09	<p>This issue is the fourteenth official release.</p> <p>Modified the following content:</p> <p>Gave the reason why EVS disks cannot be attached to certain BMSs in EVS Disk.</p>
2022-09-20	<p>This issue is the tenth official release.</p> <p>Modified the following content:</p> <p>Added OSs supported by BMSs and related description in OSs Supported by Different Types of BMSs.</p>
2020-07-15	<p>This issue is the ninth official release.</p> <ul style="list-style-type: none"> • Reclassified BMSs by instance type and added x86 V4 BMS with Intel Broadwell CPU, x86 V5 BMS with Intel Skylake CPU, and Kunpeng V1 BMS. • Added the OSs supported by compute-optimized o3 BMSs in OSs Supported by Different Types of BMSs.
2020-03-31	<p>This issue is the eighth official release.</p> <p>Added the following content:</p> <ul style="list-style-type: none"> Billing

Released On	Description
2020-01-20	This issue is the seventh official release. Added the relationship between BMS and TMS in Related Services .
2019-07-30	This issue is the sixth official release. <ul style="list-style-type: none"> Adjusted the outline. Added common concepts and access modes in What Is BMS? Modified the lifecycle chart in Lifecycle.
2019-05-30	This issue is the fifth official release. Added OSs Supported by Different Types of BMSs .
2019-04-16	This issue is the fourth official release. <ul style="list-style-type: none"> Added the internal network bandwidth in What Is BMS? Added the RAID configuration and graphics card memory of GPU instances in Instance Family.
2019-03-18	This issue is the third official release. Adjusted the outline and added the following sections: <ul style="list-style-type: none"> Lifecycle Identity Authentication and Access Control Features and Constraints
2018-10-31	This issue is the second official release. Added Instance Family .
2018-06-30	This issue is the first official release.