

Bare Metal Server

User Guide

Issue 02
Date 2023-07-05



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 Common Operations.....	1
2 Instance.....	4
2.1 Creating a BMS.....	4
2.1.1 Introduction.....	4
2.1.2 Creating a Common BMS.....	4
2.1.3 Creating a BMS Supporting Quick Provisioning.....	13
2.1.4 Creating a Dedicated BMS.....	13
2.1.5 Creating a BMS from a Private Image.....	15
2.2 Viewing BMS Information.....	15
2.2.1 Viewing BMS Creation Statuses.....	15
2.2.2 Viewing BMS Details.....	16
2.3 Logging In to a Linux BMS.....	17
2.3.1 Linux BMS Login Methods.....	17
2.3.2 Remotely Logging In to a BMS.....	18
2.3.3 Logging In to a BMS Using an SSH Key Pair.....	19
2.3.4 Logging In to a BMS Using an SSH Password.....	21
2.4 Logging In to a Windows BMS.....	22
2.4.1 Windows BMS Login Methods.....	22
2.4.2 Logging In to a BMS Remotely Using MSTSC.....	22
2.5 Managing BMSs.....	23
2.5.1 Changing the Name of a BMS.....	23
2.5.2 Stopping a BMS.....	24
2.5.3 Restarting a BMS.....	25
2.5.4 Reinstalling the OS.....	25
2.5.5 Rebuilding a BMS.....	27
2.5.6 Backing Up a BMS.....	29
2.5.7 Releasing a BMS.....	30
2.6 User Data and Metadata.....	30
2.6.1 Injecting User Data.....	30
2.6.2 Retrieving Metadata.....	38
3 Image.....	45
3.1 Private Image Overview.....	45

3.2 Creating a Private Image from a BMS.....	45
3.3 Creating a Private Image from an External Image File.....	46
4 Disk.....	49
4.1 Disk Types.....	49
4.2 Attaching Data Disks.....	51
4.3 Initializing Data Disks.....	52
4.3.1 Introduction to Data Disk Initialization Scenarios and Partition Styles.....	52
4.3.2 Initializing a Windows Data Disk (Windows Server 2016).....	54
4.3.3 Initializing a Linux Data Disk (fdisk).....	65
4.3.4 Initializing a Linux Data Disk (parted).....	70
4.3.5 Initializing a Windows Data Disk Greater Than 2 TB (Windows Server 2012).....	75
4.3.6 Initializing a Linux Data Disk Greater Than 2 TB (parted).....	83
4.4 Detaching a Disk.....	88
4.5 Expanding Disk Capacity.....	89
5 Key Pair and Password.....	90
5.1 Using an SSH Key Pair.....	90
5.2 Obtaining the Password of a Windows BMS.....	95
5.3 Deleting the Password of a Windows BMS.....	96
6 Network.....	98
6.1 EIP.....	98
6.1.1 Overview.....	98
6.1.2 Binding an EIP to a BMS.....	99
6.1.3 Unbinding an EIP from a BMS.....	100
6.2 VPC.....	100
6.2.1 Overview.....	100
6.2.2 Binding a Virtual IP Address to a BMS.....	104
6.2.3 Setting the Source/Destination Check for a NIC.....	105
6.2.4 Enabling IPv4/IPv6 Dual Stack.....	106
7 Security.....	109
7.1 Security Group.....	109
7.1.1 Adding Security Group Rules.....	109
7.1.2 Security Group Configuration Examples.....	110
7.1.3 Changing a Security Group.....	112
8 Resources and Tags.....	114
8.1 Tag.....	114
8.1.1 Overview.....	114
8.1.2 Adding Tags.....	115
8.1.3 Searching for Resources by Tag.....	116
8.1.4 Deleting Tags.....	117
8.2 Resource Location.....	117

8.3 Adjusting Resource Quotas.....	119
9 Server Monitoring.....	120
9.1 Overview.....	120
9.2 Monitored Metrics (with Agent Installed).....	121

1 Common Operations

When using BMSs, you may encounter various problems, such as remotely logging in to a BMS, expanding disk capacity, and reinstalling the OS. This section provides navigation to common operations to help you with these problems.

Create and Manage a BMS

General Operations

Perform the following steps to use a BMS:

1. Create a BMS by following the instructions in [Creating a Common BMS](#).
If the BMS quota is insufficient, you can apply to increase the quota by following the instructions in [Adjusting Resource Quotas](#).
2. Log in to the BMS. The login mode varies depending on the BMS OS.
 - Linux BMS: [Remotely Logging In to a BMS](#), [Logging In to a BMS Using an SSH Key Pair](#), or [Logging In to a BMS Using an SSH Password](#)
 - Windows BMS: [Logging In to a BMS Remotely Using MSTSC](#)
3. Stop the BMS by following the instructions in [Stopping a BMS](#).
4. Delete the BMS by following the instructions in [Releasing a BMS](#).

Billing Management

You can renew your yearly/monthly BMS in the following ways:

- [Manual Renewal](#)
- [Auto Renewal](#)

Configuration Change

If the BMS OS cannot meet your requirements, you can reinstall or change the OS by following the instructions in [Reinstalling the OS](#).

Refined BMS Control and Management

You can control and manage your BMS in a refined way using the following methods:

- [Injecting User Data](#)

- [Retrieving Metadata](#)

BMS Security and Reliability Configuration

You can improve the security and reliability of your BMS using the following methods:

- [Backing Up a BMS](#)

Create and Manage Private Images

By using private images, you can quickly deploy the service environment.

You can create a private BMS image in the following ways:

- [Creating a Private Image from a BMS](#)
- [Creating a Private Image from an External Image File](#)

You can perform the following operations on private images:

- [Share images](#) with other tenants.
- [Export images](#) to your OBS bucket.

Create and Manage Disks

General Operations

To use a disk as a data disk, perform the following steps:

1. Create a disk in any of the following ways:
 - [Purchasing an EVS Disk](#)
2. [Attach the disk to a BMS.](#)
3. [Initialize the disk.](#)
4. [Detach the disk from the BMS.](#)
5. [Delete the disk.](#)

Configuration Changes

If the capacity of an existing system disk or data disk cannot meet requirements, you can expand the disk capacity. For details, see [Expanding the Capacity of an EVS Disk](#). After the disk capacity has been expanded, the additional disk space needs to be allocated to an existing partition or a new partition.

Create and Use a Key Pair

To use a key pair, perform the following steps:

1. [Create](#) or [import](#) a key pair.
2. When creating a BMS, bind the key pair to the BMS.
3. [Log in to the BMS using the key pair.](#)
4. [Delete the key pair.](#)

Create and Manage a BMS Network

Security Group

To use a security group, perform the following steps:

1. [Create a security group.](#)
2. [Add a security group rule.](#)
3. When creating a BMS, add it to the security group.
4. [Delete the security group rule.](#)
5. [Delete the security group.](#)

EIP

To use an EIP, perform the following steps:

1. [Bind an EIP to a BMS.](#)
2. [Unbind the EIP from the BMS.](#)

VPC

You can bind an extra IP address (virtual or floating IP address) to a NIC to enable flexible network functions. You can also enable the source/destination check function of the NIC to prevent packet spoofing and improve security.

- [Binding a Virtual IP Address to a BMS](#)
- [Setting the Source/Destination Check for a NIC](#)

Tags

You can use tags to identify various resources to improve the efficiency in classifying, querying, and managing resources. To use a tag, perform the following steps:

1. [Add a tag.](#)
2. [Query resources by tag.](#)
3. [Delete a tag.](#)

Monitor a BMS

To meet the basic monitoring and O&M requirements for servers, **Server Monitoring** monitors more than 40 metrics, such as CPU, memory, disk, and network. You need to install Agent on the BMS to implement the monitoring. For details, see [Overview](#).

For all the supported BMS metrics, see [Monitored Metrics \(with Agent Installed\)](#).

2 Instance

2.1 Creating a BMS

2.1.1 Introduction

You can:

- Create a common BMS meeting your basic requirements as instructed in [Creating a Common BMS](#).
- Create a BMS that can be quickly provisioned. For details, see [Creating a BMS Supporting Quick Provisioning](#).
- Create a BMS in a DeC if you have high requirements for security compliance. For details, see [Creating a Dedicated BMS](#).
- Create a private image containing a required OS and applications and use it to create a BMS. For details, see [Creating a BMS from a Private Image](#).

2.1.2 Creating a Common BMS

Scenarios

This section describes how to create a BMS to deploy your services.

Prerequisites

- You have completed [Preparations](#).
- To inject user data, you have prepared [user data scripts](#).
- You have enabled Dedicated Cloud (DeC).
For details, see [Creating a Dedicated BMS](#).

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.

3. Click **Buy BMS**.


The page for you to purchase a BMS is displayed.

4. In the **Current Configuration** area on the right pane, confirm the billing mode. Currently, only the **Yearly/Monthly** billing mode is supported.

 **NOTE**

Yearly/Monthly is a prepaid billing mode in which your BMS is billed based on the service duration. This cost-effective mode is ideal when the duration of BMS usage is predictable.

5. Confirm **Region**.

If the region is incorrect, click  in the upper left corner of the page to correct it.

6. Select an AZ.

An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network.

- It is recommended that you create BMSs in different AZs to ensure high availability of applications running on the BMSs.
- To lower the network delay, create BMSs in the same AZ.

7. Select a flavor.

Flavor contains the CPU, memory, local disks, and extended configuration of the BMS. After you select a flavor, the name and use scenarios of the flavor are displayed under the flavor list.

Extended Configuration provides the NIC information of the selected flavor. For example, 2 x 2*10GE indicates that the BMS has two 10GE NICs, each with two ports. One NIC is used for the BMS to connect to a VPC and the other is used for the BMS to communicate with other BMSs in a high-speed network.

 **NOTE**

- Configuration in the flavor, such as the CPU, memory, and local disks, cannot be changed.
- The bandwidth of different BMS flavors varies. Choose a flavor that meets your requirements.
- Some flavors support quick BMS provisioning. If you select a flavor of this type, parameter **System Disk** is displayed under **Disk**. The OS will be installed on the EVS disk attached to the BMS.

8. Set **Image**.

- Public Image

A public image is a standard OS image provided by the system and is available to all users. It contains an OS and pre-installed public applications, such as the SDI iNIC driver, bms-network-config (a network configuration program), and Cloud-Init (an initialization tool). If you need other applications or software, configure them on the new BMSs.

- Private Image

A private image is created from an external image file or a BMS and is available only to the user who created it. It contains an OS, preinstalled public applications, and the user's private applications.

- Shared Image

A shared image is a private image shared by another public cloud user with you.

9. Set **Disk**.

Disks are classified as EVS disks and DSS disks based on whether the disks use dedicated storage resources. DSS disks provide dedicated storage resources.

- If you have applied for a storage pool on the DSS console and have obtained the pool, click the **DSS** tab and create disks in the storage pool.
- If you have not obtained a dedicated storage pool, click the **EVS** tab and create EVS disks that use public storage resources.

NOTE

- When you use DSS resources to create a disk, the disk type must be the same as that of the requested storage pool. For example, both are of the high I/O type.
- For details about different disk types, see [Disk Types](#).

A BMS has one system disk and one or more data disks. You can add multiple data disks for a BMS and customize the system disk size.

- System disk

If you select a flavor that supports quick provisioning, parameter **System Disk** is available. You can set the system disk type and size as needed.

- Data disk

You can add multiple data disks for a BMS and enable sharing for each data disk.

- Currently, BMSs only support SCSI disks.
- **Share**: indicates that the EVS disk can be shared. A shared disk can be attached to multiple BMSs simultaneously.

NOTE

- After a system disk is detached from a BMS charged in yearly/monthly mode, the disk can only be used as a system disk and can only be attached to this BMS.
- If you detach a non-shared data disk purchased when you buy a BMS charged in yearly/monthly mode and want to attach it again, you can only attach it to the original BMS as a data disk.
- The non-shared data disk purchased when you buy a BMS charged in yearly/monthly mode does not support separate renewal, unsubscription, automatic service renewal, conversion to pay-per-use payment, or release.

10. Configure automatic backup.

After automatic backup is enabled, the system automatically backs up the BMS based on the preset backup policy.

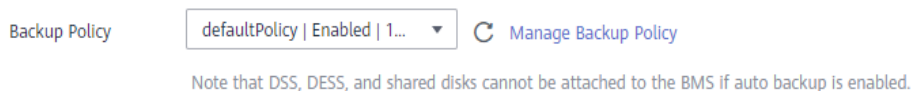
NOTE

The automatic backup function applies only to BMSs that support quick provisioning. To enable this function, you must select a flavor that supports quick provisioning in [step 7](#).

- a. Select **Enable auto backup**.
- b. Configure **Backup Policy**.

In the drop-down list, select a backup policy. Alternatively, you can click **Manage Backup Policy** and set the backup policy on the Cloud Server Backup Service (CSBS) page. If you have not created any backup policy but select **Enable auto backup**, the system will use the default backup policy shown in [Figure 2-1](#).

Figure 2-1 Default backup policy



For details about CSBS, see [Cloud Backup and Recovery Overview](#).

11. Set network parameters, including **VPC**, **NIC**, and **Security Group**.

When you use VPC for the first time, the system automatically creates a VPC for you, including the security group and NIC. The default subnet segment is 192.168.1.0/24 and the subnet gateway is 192.168.1.1. Dynamic Host Configuration Protocol (DHCP) is enabled for the subnet.

Table 2-1 Network parameters

Parameter	Description
VPC	You can select an existing VPC or create one.
NIC	<p>Includes primary and extension NICs. You can add an extension NIC for a BMS and specify IP addresses for the primary and extension NICs.</p> <p>CAUTION</p> <ul style="list-style-type: none">• The primary NIC cannot be deleted because it is used to provide the default route.• If you choose to assign an IP address automatically, 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.• If a fixed IP address is assigned to a NIC, you cannot create BMSs in a batch.

Parameter	Description
Security Group	<p>Security groups are used to control access to BMSs. You can define different access control rules for a security group, and these rules take effect for all BMSs added to this security group.</p> <p>When creating a BMS, you can select only one security group. After a BMS is created, you can associate it with multiple security groups. For details, see Changing a Security Group.</p> <p>Security group rules determine BMS access and usage. For instructions about how to configure a security group rule, see Adding Security Group Rules. Enable the following common protocols and ports as needed:</p> <ul style="list-style-type: none">● Port 80: used to view web pages by default through HTTP.● Port 443: used to view web pages through HTTPS.● ICMP: pings BMSs to check their communication statuses.● Port 22: reserved for logging in to a Linux BMS using SSH.● Port 3389: reserved for logging in to a Windows BMS using SSH. <p>NOTE</p> <p>Before initializing a BMS, ensure that security group rules in the outbound direction meet the following requirements:</p> <ul style="list-style-type: none">● Protocol: TCP● Port Range: 80● Remote End: 169.254.0.0/16 <p>If you use the default outbound security group rule, the preceding requirements are met, and the BMS can be initialized. The default outbound security group rule is as follows:</p> <ul style="list-style-type: none">● Protocol: Any● Port Range: Any● Remote End: 0.0.0.0/16

Parameter	Description
EIP	<p>An EIP is a static public IP address bound to a BMS in a VPC. Using the EIP, the BMS can access the Internet.</p> <p>You can select one of the following three options for EIP as needed:</p> <ul style="list-style-type: none">● Automatically assign: The system automatically assigns an EIP with a dedicated bandwidth to the BMS. The bandwidth is configurable.● Use existing: An existing EIP is assigned to the BMS.● Not required: The BMS cannot communicate with the Internet and can only be used to deploy services or clusters in a private network. <p>NOTE If you select Use existing, you can create only one BMS at a time.</p>
Specifications	<p>This parameter is available when you select Automatically assign for EIP.</p> <ul style="list-style-type: none">● Dynamic BGP: When changes occur on a network using dynamic BGP, network configurations can be promptly adjusted using the specified routing protocol, ensuring network stability and optimal user experience.● Static BGP: When changes occur on a network using static BGP, carriers cannot adjust network configurations in real time to ensure optimal user experience.
Bandwidth Type	<p>This parameter is mandatory when EIP is set to Automatically assign.</p> <ul style="list-style-type: none">● Dedicated: The bandwidth can be used by only one EIP.● Shared: The bandwidth can be used by multiple EIPs. <p>NOTE</p> <ul style="list-style-type: none">● A bandwidth can be shared between a limited number of EIPs. If the number of EIPs cannot meet service requirements, switch to a higher shared bandwidth or apply to expand the EIP quota of the existing bandwidth.● EIPs that are charged yearly/monthly do not support shared bandwidths.● When a shared bandwidth that is charged yearly/monthly expires, the system automatically deletes the bandwidth and creates an exclusive bandwidth charged by traffic for the EIPs sharing the deleted bandwidth.

Parameter	Description
Billed By	This parameter is available when you select Automatically assign for EIP. <ul style="list-style-type: none">• Bandwidth: You specify a maximum bandwidth and pay for the time you use the bandwidth.• Traffic: You are charged based on the actual traffic you have used.
Bandwidth	This parameter is available when you select Automatically assign for EIP. Specifies the bandwidth size in Mbit/s.

12. Set the BMS login mode.

Key pair is recommended because it features higher security than **Password**. If you select **Password**, ensure that the password meets complexity requirements described in [Table 2-2](#) to prevent malicious attacks.

– Key pair

A key pair is used for BMS login authentication. You can select an existing key pair, or click **Create Key Pair** to create one.

NOTE

If you use an existing key pair, ensure that you have one.

– Password

In this mode, the initial password is used for authentication. You can log in to the BMS using the username and its initial password.

If the BMS runs Linux, you can use username **root** and its initial password to log in to the BMS. If the BMS runs Windows, you can use username **Administrator** and its initial password to log in to the BMS. The passwords must meet the requirements described in [Table 2-2](#).

Table 2-2 Password requirements

Parameter	Requirements	Example Value
Password	<ul style="list-style-type: none">• Consists of 8 to 26 characters.• Must contain at least three of the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters !@\$%^&*_+=[]{};,:/?• Cannot contain the username or the username spelled backwards.• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows BMSs.)	Test12\$@

13. Configure **Enterprise Project**.

This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager.

An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project. The default project is **default**.

Select an enterprise project from the drop-down list. For details about enterprise projects, see [Enterprise Management User Guide](#).

14. (Optional) Configure **Advanced Settings**.

To use functions listed in **Advanced Settings**, click **Configure now**. Otherwise, click **Do not configure**.

- **Agency**

An agency provides BMSs with temporary security credentials for accessing other cloud services. The agency is created by the tenant administrator on the IAM console.

If you have created an agency in IAM, you can select the agency from the drop-down list. If you have no agency, click **Create Agency** to create one. Currently, agencies are mainly used for server monitoring. For more information, see [Overview](#).

15. Set **BMS Name**.

The name can be customized but can contain only letters, digits, underscores (_), hyphens (-), and periods (.).

If you purchase multiple BMSs at a time, suffixes will be added to the BMSs in sequence, such as **bms-0001**, **bms-0002**, ... If you purchase multiple BMSs again, the values in the new BMS names increase from the existing maximum

value. For example, the existing BMS with the maximum number in name is **bms-0010**. If you enter **bms**, the names of the new BMSs will be **bms-0011**, **bms-0012**, When the value reaches 9999, it will start from 0001 again.

16. Set **Required Duration** and **Quantity**.

- **Required Duration**: Set the service duration if you select the **Yearly/Monthly** billing mode. The service duration ranges from one month to one year.

 **NOTE**

BMSs charged in yearly/monthly mode cannot be deleted. They support only resource unsubscription. If you no longer need a BMS, you can unsubscribe from it using either of the following methods:

- Locate the row that contains the BMS, click **More** in the **Operation** column, and select **Unsubscribe** from the drop-down list. On the **Unsubscribe** page, select a reason and click **Confirm**.
 - Choose **Billing Center > Orders > Unsubscriptions**. Locate the row that contains the BMS and click **Unsubscribe from Resource** in the **Operation** column.
- **Quantity**: You can purchase BMSs of the remaining quota at a time.

 **NOTE**

If you manually set an IP address when configuring **NIC** or **High-Speed NIC** or select **Use existing** when configuring **EIP**, you can create only one BMS at a time.

17. Click **Buy Now**. If you have any question about the price, click **Pricing details**.

Confirm the BMS information and click **Pay Now**.

18. Pay the fees as prompted and click **OK**.

The BMS console is displayed.

19. Wait for the system to create your requested BMSs.

The BMS status changes to **Running** after about 30 minutes. If you select a flavor that supports quick provisioning, you can obtain a BMS within about five minutes.

 **NOTE**

You can view the BMS creation status. For details, see [Viewing BMS Creation Statuses](#).

Follow-up Operations

- After the BMS is created, you can view its details, such as name/ID, disks, and private IP address. For details, see [Viewing BMS Details](#).
- After logging in to the BMS, you can install software or deploy services as needed. The login mode varies depending on the BMS OS. For details, see [Linux BMS Login Methods](#) or [Windows BMS Login Methods](#).
- If you have created data disks when creating the BMS, you must format partitions of the data disks. For details, see [Introduction to Data Disk Initialization Scenarios and Partition Styles](#).
- Change the validity period of the password to prevent any inconvenience caused by password expiration. For detailed operations, see [How Do I Set the Password Validity Period?](#)

- Currently, Windows Server 2012 BMSs have the same security identifier (SID), which is used to identify users, groups, and computer accounts. In cluster deployment scenarios, change the SIDs of BMSs by following the instructions in [How Do I Change the SID of a Windows Server 2012 BMS?](#) to ensure that each BMS has a unique SID.

2.1.3 Creating a BMS Supporting Quick Provisioning

Scenarios

When you create a common BMS (that is, a BMS booted from a local disk), its OS needs to be downloaded from the cloud and it also takes some time to install the OS. When you create a BMS that uses an EVS as its system disk, the OS has been installed on the disk and does not need to be downloaded or installed. In this way, the BMS can be provisioned within a short time when you apply for it.

BMSs supporting quick provisioning have the following advantages over other BMSs:

- BMSs booted from EVS disks can be provisioned within about 5 minutes.
- CSBS backups ensure data security.
- BMS rebuilding upon faults is supported, enabling quick service recovery.
- An image of a BMS can be exported to apply configurations of the BMS to other BMSs, eliminating the need to repeatedly configure BMSs.

On the page for creating a BMS, select a flavor that supports quick BMS provisioning, set the system disk type and capacity, and configure other required parameters.

Procedure

You can create a BMS supporting quick provisioning by following the instructions in [Creating a Common BMS](#).

When creating the BMS, pay attention to the following:

- **Flavor:** Select **physical.s4.medium**, **physical.s4.large**, **physical.s4.xlarge**, **physical.s4.2xlarge**, or **physical.s4.3xlarge**. For more information about flavors, see [Instance Family](#).
- **Image:** Not all public images can be used to create BMSs supporting quick provisioning.
- **Disk:** Set the system disk type and size.
- **Auto Backup:** You are advised to select **Enable auto backup** and set **Backup Policy** to ensure data security.

2.1.4 Creating a Dedicated BMS

Scenarios

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 in either of the following ways:

- [Create a BMS on the DeC Console](#)
- [Create a BMS on the Cloud Server Console](#)

Before creating a BMS in a DeC, you must apply for a dedicated BMS resource pool.

Prerequisites

You have enabled DeC.

Apply for a Dedicated BMS Pool

1. Log in to the management console.
2. Click the region name in the upper left corner and select the region where DeC resides from the drop-down list.
3. Choose **Service List > Dedicated Cloud > Dedicated Bare Metal Server**.
The **Dedicated Bare Metal Server** page is displayed.
4. In the upper right corner, click **Apply for Resources**.
5. Select a flavor based on your service requirements and set the quantity and usage duration.
6. Click **Next**. After confirming that the configurations are correct, click **Submit**.
Message **Request submitted successfully**. is displayed. The application will be reviewed by the O&M personnel. After the application is approved, you can choose **Fees > My Orders** and pay the order.
7. After paying the order, you can view information about the resource pool on the **Dedicated Bare Metal Server** page, such as **Resource Pool Type**, **CPU Allocation Rate**, and **Memory Allocation Rate**.

Method 1: Create a Dedicated BMS on the DeC Console

1. Log in to the management console.
2. Click the region name in the upper left corner and select the region where DeC resides from the drop-down list.
3. Choose **Service List > Dedicated Cloud > Dedicated Bare Metal Server**.
The **Dedicated Bare Metal Server** page is displayed.
4. In the upper right corner of the page, click **Provision BMS in DeC**.
The page for creating a BMS is displayed.
5. Set the parameters as prompted. These parameters are the same as those for creating a common BMS. For details, see [Creating a Common BMS](#).
After the BMS is created, the number of BMSs on the **Dedicated Bare Metal Server** page becomes **1**, and **CPU Allocation Rate** and **Memory Allocation Rate** increase.

Method 2: Create a Dedicated BMS on the Cloud Server Console

1. Log in to the management console.
2. Click the region name in the upper left corner and select the region where DeC resides from the drop-down list.

3. Choose **Service List > Computing > Bare Metal Server**.
The Cloud Server Console is displayed.
4. On the BMS page, click **Provision BMS in DeC** in the upper right corner.
The page for creating a BMS is displayed.
5. Set the parameters as prompted. These parameters are the same as those for creating a common BMS. For details, see [Creating a Common BMS](#).
After the BMS is displayed, click the **BMS Resource Pool** tab in the **Resource Usage Details** area on the **Dashboard** page. The number of BMSs is **1**, and **CPU Allocation Rate** and **Memory Allocation Rate** increase.

2.1.5 Creating a BMS from a Private Image

Scenarios

If you want to create a BMS that has the same OS and applications as an existing BMS, you can create a private image using the existing BMS and then create a BMS using the private image. This frees you from repeatedly configuring BMSs and improves efficiency.

Background

You can create a private image using either of the following methods:

- [Creating a Private Image from a BMS](#)
- [Creating a Private Image from an External Image File](#)

Procedure

Create a BMS by following the instructions in [Creating a Common BMS](#).

Note for setting the parameters:

- **Region:** Select the region where the private image is located.
- **Flavor:** OSs supported by different BMS flavors vary. For details, see [OSs Supported by Different Types of BMSs](#). Select a flavor based on the private image OS.
- **Image:** Select **Private image** or **Shared image** and select the required image from the drop-down list.
- **Disk:** If the selected flavor supports quick provisioning, you are advised to increase **System Disk** by 2 GB or more.

2.2 Viewing BMS Information

2.2.1 Viewing BMS Creation Statuses

Scenarios

After clicking **Submit** to request a BMS, you can query the task status in the **Task Status** area. A task involves several sub-tasks, such as creating a BMS resource, binding an EIP, and attaching an EVS disk.

The task status may be either **Creating** or **Failed**:

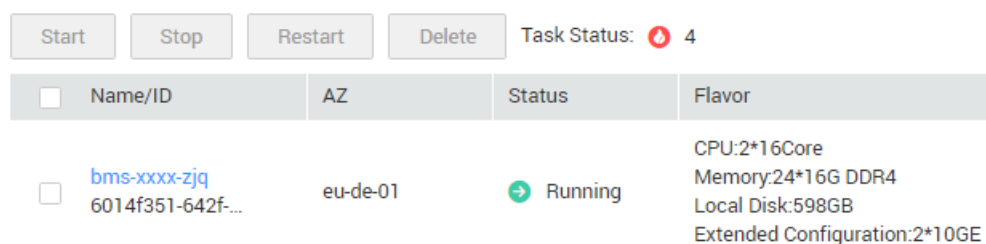
- **Processing**: The system is processing the task.
- **Failed**: The system has failed to process the task. The system rolls back the failed task and displays an error code, for example, **(BMS.3033) Failed to create system disk**.

This section describes how to query BMS application processing status and the information displayed in the **Task Status** area.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. **Task Status** is displayed on the right of common operations, such as **Start**, **Stop**, **Restart**, and **Delete**. After you purchase a BMS, the **Task Status** area will show the task processing status.

Figure 2-2 BMS application status



<input type="checkbox"/>	Name/ID	AZ	Status	Flavor
<input type="checkbox"/>	bms-xxxx-zjq 6014f351-642f...	eu-de-01	➔ Running	CPU:2*16Core Memory:24*16G DDR4 Local Disk:598GB Extended Configuration:2*10GE

4. Click the number displayed in the **Task Status** area to view details about the BMS application processing status. The tasks in **Processing** and **Failed** statuses are displayed.

NOTE

If **Failed** is displayed for a task in the **Task Status** area, but the BMS list contains the BMS, handle this issue by following the instructions in [Why Is the BMS Creation Task Displayed as Failed But the BMS List Shows the BMS?](#)

2.2.2 Viewing BMS Details

Scenarios

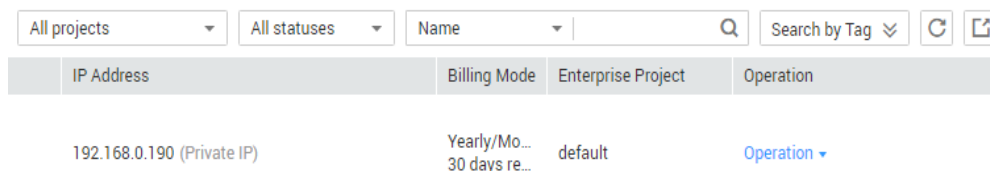
After you obtain a BMS, you can view and manage your BMS on the management console. This section describes how to query detailed information about a BMS, such as the BMS name/ID, disks, NICs, and EIP.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
On the BMS list page, you can view your BMS and its flavor, image, and private IP address.

- In the upper right corner of the BMS list, query BMSs by specifying the project, status, name, BMS ID, flavor, and private IP address. Alternatively, click **Search by Tag** above the upper right corner of the BMS list and search for a BMS by tag key and value.

Figure 2-3 Searching BMSs



- Click the name of the queried BMS.
The page showing details of the BMS is displayed.
- View the BMS details, such as name, status, flavor, and VPC. You can also click the **Disks**, **NICs**, **Security Groups**, **EIPs**, **Tag**, and **Monitoring** tabs to attach EVS disks to or detach EVS disks from the BMS, change the security group, bind an EIP to or unbind an EIP from the BMS, and create agencies.

NOTE

The BMS monitoring data and charts are not displayed on the BMS details page. You need to view them on the Cloud Eye console. The prerequisite is that Agent has been installed on your BMS. For details, see [Overview](#).

2.3 Logging In to a Linux BMS

2.3.1 Linux BMS Login Methods

Choose an appropriate method to log in to a Linux BMS based on the BMS network configuration and your on-premise OS.

Table 2-3 Linux BMS login methods

Access to the Internet	On-premise OS	Login Method
Yes/No	Windows or Linux	Remotely Logging In to a BMS
Yes	Windows	Use a remote login tool, such as PuTTY. <ul style="list-style-type: none"> For how to log in to a BMS using an SSH key pair, see Logging In to a BMS Using an SSH Key Pair. For how to log in to a BMS using an SSH password, see Logging In to a BMS Using an SSH Password.

Access to the Internet	On-premise OS	Login Method
Yes	Linux	Run commands. <ul style="list-style-type: none">For how to log in to a BMS using an SSH key pair, see Logging In to a BMS Using an SSH Key Pair.For how to log in to a BMS using an SSH password, see Logging In to a BMS Using an SSH Password.

2.3.2 Remotely Logging In to a BMS

Scenarios

If common remote connection software (such as PuTTY) is unavailable, you can use the remote login function on the management console to log in to a BMS.

Constraints

- Only Linux BMSs support remote login.
- Only the user who creates a BMS or users with the Tenant Administrator or Server Administrator role can log in to the BMS remotely.
- When you log in to a BMS remotely, shortcut keys such as Ctrl and Alt are not well supported. For example, if you enter **Alt + ASCII code**, multiple special characters are displayed.
- Before exiting the management console, log out of the OS.

Prerequisites

- The BMS must be in **Running** state.
- You have set a login password when creating the BMS. If you did not set a password or forget the password, you can contact the administrator to reset the password.
- If you selected the key pair login mode when creating the BMS, log in to the BMS by following the instructions in [SSH Key Pair](#) and set a password for the BMS. The detailed operations are as follows:

Log in to the BMS using the key pair, switch to user **root**, and run the **passwd** command to set a password for user **root**.

Figure 2-4 Setting a password for user **root**

```
[root@serverc28ef36e-08ef-4d94-8921-155fa4d4332b ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@serverc28ef36e-08ef-4d94-8921-155fa4d4332b ~]#
```


Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the target BMS and click **Remote Login** in the **Operation** column.

After about one minute, the login page is displayed. Press **Enter** and enter username **root** and password to log in.

NOTE

- If you do not log in within 10 minutes after obtaining the remote login link, it will become invalid.
- If you do not perform any operation on the remote login page within 10 minutes, you need to obtain the link again.
- If the login page does not respond after you press **Enter**, a possible cause is that remote login is not configured for the BMS image. You can resolve the issue by following the instructions in [What Do I Do If the Login Page Does Not Respond?](#)
- If the BMS console is displayed improperly (such as broken lines and garbled characters) after you remotely log in to it, see [What Do I Do If the BMS Console Is Displayed Improperly After I Remotely Log In to a BMS?](#)
- If numbers are not properly displayed after you enter them using the numeric keypad for remote login, see [What Do I Do If the Numeric Keypad Does Not Work During Remote Login?](#)

2.3.3 Logging In to a BMS Using an SSH Key Pair

Scenarios

This section describes how to log in to a Linux BMS using an SSH key pair from a Windows or Linux PC.

Prerequisites

- The BMS must be in **Running** state.
- You have obtained the private key file used during BMS creation.
- You have bound an EIP to the BMS. For details, see [Binding an EIP to a BMS](#).
- You have configured the inbound rules of the security group. For details, see [Adding Security Group Rules](#).
- The network connection between the login tool (such as PuTTY) and the target BMS is normal. For example, the default port 22 is not blocked by the firewall.

Logging In to the Linux BMS from a Windows PC

You can use the following methods to log in to a Linux BMS from a local PC running Windows:

Method 1: Use PuTTY to log in to the BMS.

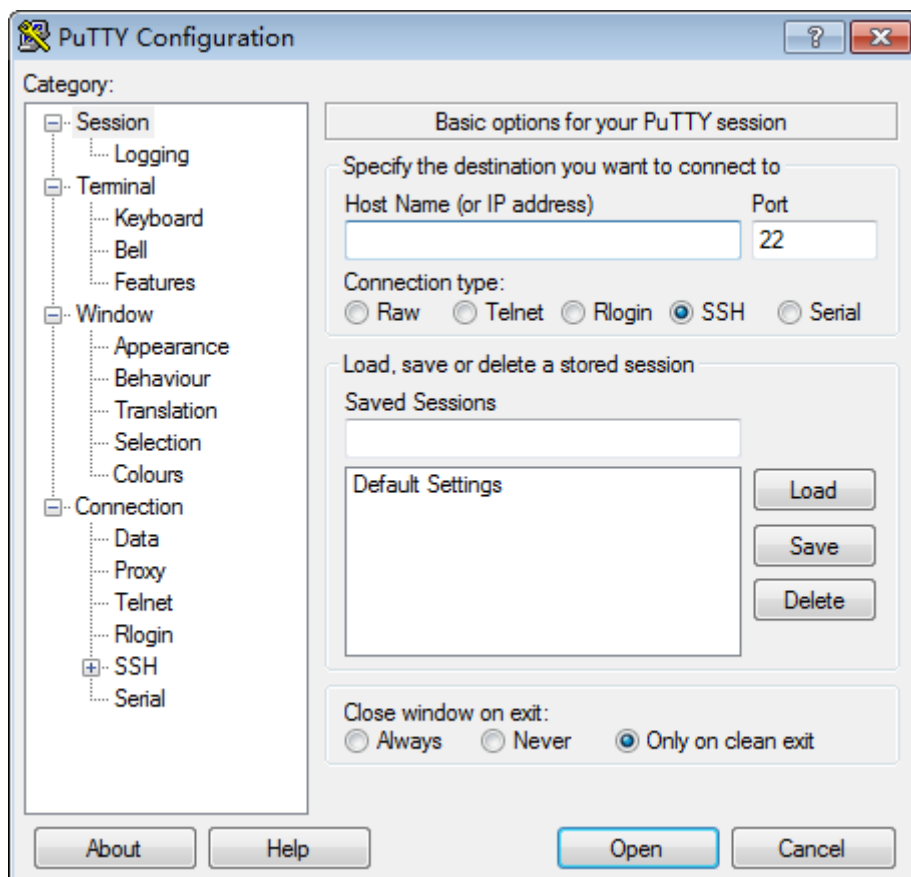
Before logging in to the BMS using PuTTY, ensure that the private key file has been converted to .ppk format.

1. Check whether the private key file has been converted to **.ppk** format.
 - If yes, go to step 7.
 - If no, go to step 2.
2. Visit the following website and download PuTTY and PuTTYgen:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

 **NOTE**

- PuTTYgen is a private key generator, which is used to create a key pair that consists of a public key and a private key for PuTTY.
3. Run PuTTYgen.
 4. In the **Actions** area, click **Load** and import the private key file that you stored when creating the BMS.
Ensure that the private key file is in the format of **All files (*.*)**.
 5. Click **Save private key**.
 6. Save the converted private key, for example, **kp-123.ppk**, to your local PC.
 7. Double-click **PuTTY.EXE**. The **PuTTY Configuration** page is displayed.

Figure 2-5 PuTTY Configuration



8. Choose **Connection > Data**. Enter the image username **root** in **Auto-login username**.
9. Choose **Connection > SSH > Auth**. In the last configuration item **Private key file for authentication**, click **Browse** and select the .ppk private key in step 6.

10. Choose **Session** and enter the EIP of the BMS in the box under **Host Name (or IP address)**.
11. Click **Open**.
Log in to the BMS.

Method 2: Use Xshell to log in to the BMS.

1. Start the Xshell tool.
2. Run the following command to remotely log in to the BMS through SSH:
ssh Username@EIP
Example:
ssh root@192.168.0.1
3. (Optional) If the system displays the **SSH Security Warning** dialog box, click **Accept & Save**.
4. Select **Public Key** and click **Browse** beside the user key text box.
5. In the user key dialog box, click **Import**.
6. Select the locally stored key file and click **Open**.
7. Click **OK** to log in to the BMS.

Logging In to the Linux BMS from a Linux PC

Perform the following operations to log in to a Linux BMS from a local PC running Linux: The following procedure uses private key file **KeyPair-ee55.pem** as an example to describe how to log in to the BMS.

1. On the Linux CLI, run the following command to change operation permissions:

```
chmod 400 /path/KeyPair-ee55
```

NOTE

In the preceding command, *path* refers to the path under which the key file is stored.

2. Run the following command to log in to the BMS:

```
ssh -i /path/KeyPair-ee55 root@EIP of the BMS
```

NOTE

- In the preceding command, *path* refers to the path under which the key file is stored.
- In the preceding command, **root** is the username of the BMS image.

2.3.4 Logging In to a BMS Using an SSH Password

Scenarios

This section describes how to log in to a Linux BMS using an SSH password from a Windows or Linux PC.

Prerequisites

- The BMS must be in **Running** state.

- You have bound an EIP to the BMS. For details, see [Binding an EIP to a BMS](#).
- You have configured the inbound rules of the security group. For details, see [Adding Security Group Rules](#).
- The network connection between the login tool (such as PuTTY) and the target BMS is normal. For example, the default port 22 is not blocked by the firewall.

 **NOTE**

If you want to use a password to log in a Linux BMS, log in to the BMS remotely by following the instructions in [Remotely Logging In to a BMS](#) and enable the SSH password login mode. For details, see [How Do I Set SSH Configuration Items?](#)

Log In to a BMS from a Windows PC

You can use the following methods to log in to a Linux BMS from a local PC running Windows (for example, use PuTTY):

 **NOTE**

Download PuTTY from <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

1. Run PuTTY.
2. In the navigation pane on the left, choose **Session**, enter the EIP of the BMS in the text box under **Host Name (or IP address)**, and select **SSH** for **Connection type**.
3. Choose **Windows > Translation** and select **UTF-8** from the **Received data assumed to be in which character set:** drop-down list box.
4. Click **Open**.
5. Enter username **root** and the password you set to log in to the BMS.

Log In to a BMS from a Linux PC

To log in to a Linux BMS from a Linux PC, run the following command:

```
ssh EIP of the BMS
```

2.4 Logging In to a Windows BMS

2.4.1 Windows BMS Login Methods

Currently, you can only log in to a Windows BMS remotely by running MSTSC on your local PC. An EIP must be bound to the BMS.

2.4.2 Logging In to a BMS Remotely Using MSTSC

Scenarios

This section describes how to log in to a Windows BMS using MSTSC (a remote login tool) from your local PC.

Prerequisites

- The BMS must be in **Running** state.
- If a Windows BMS uses the key pair authentication mode, you have obtained the password for logging in to the BMS. For details, see [Obtaining the Password of a Windows BMS](#).
- You have bound an EIP to the BMS. For details, see [Binding an EIP to a BMS](#).
- You have configured the inbound rules of the security group. For details, see [Adding Security Group Rules](#).
- The network connection between the login tool and the target BMS is normal. For example, the default port 3389 is not blocked by the firewall.

Procedure

The following procedure describes how to log in to a Windows BMS using **mstsc.exe**.

1. On the local PC, click **Start**.
2. In the **Search programs and files** text box, enter **mstsc.exe**.
3. Enter the EIP and username of the Windows BMS, click **Connect**, enter the password as prompted, and click **OK**.

2.5 Managing BMSs

2.5.1 Changing the Name of a BMS



Scenarios

To make it easy for you to identify and manage each BMS, Huawei Cloud allows you to set BMS names and change the names at any time. The new name of a BMS takes effect after the BMS is restarted.

Constraints

The names of Windows BMSs cannot be changed.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click the name of the BMS whose name is to be changed.
4. Click  next to **Name**, enter a new name that meets requirements, and click  to save the change.
The BMS name can contain only letters, digits, hyphens (-), underscores (_), and periods (.).
5. Log in to the BMS OS and run the following command to enable automatic hostname synchronization:

```
sed -i 's/auto_synchronize_hostname.*/auto_synchronize_hostname = True/g' `find / -name bms-network-config.conf`
```

Check that automatic synchronization is enabled.

```
cat `find / -name bms-network-config.conf`
```

```
[NETWORK_CONFIG]
enable_bms_network = True
enable_bms_udev_rules = False
bsdtdar_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtdar.exe
mtu_use_dhcp_config = True
is_distributed_bms = False

[METADATA]
enable_preserve_hostname = False
auto_synchronize_hostname = True

[IB]
enable_ib = True

[ROCE]
enable_roce = True
```

NOTE

If the value of `auto_synchronize_hostname` is `False`, after the BMS is restarted, the hostname will be automatically changed to that set during BMS creation.

6. Log in to the management console again. Locate the row that contains the BMS, click **More** in the **Operation** column, and select **Restart**.
After about 10 minutes, verify that the BMS is restarted and its hostname is automatically updated.

2.5.2 Stopping a BMS

Scenarios

You can stop BMSs in **Running** state.

Stopping a BMS charged in yearly/monthly mode does not affect the BMS fees. If other service products, such as EVS disks, EIPs, and bandwidths are bound to the BMS, these products are billed using their own billing mode (yearly/monthly or pay-per-use).

NOTE

- If you choose to forcibly stop a BMS, services running on the BMS will be stopped. Before performing this operation, ensure that you have saved files on the BMS.
- You can stop a BMS only on the management console and cannot run **shutdown** to stop it. It is because that the **shutdown** and other commands attempting to stop a BMS will be regarded as unexpected operations and will not take effect.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the target BMS, click **More** in the **Operation** column, and select **Stop** from the drop-down list. To stop multiple BMSs, select them and click **Stop** at the top of the BMS list.

4. In the displayed dialog box, click **Yes**.

After a BMS is stopped, its status becomes **Stopped**.

You can perform the following operations only when the BMS is stopped:

- [Detaching the System Disk](#)
- [Creating an Image](#)
- [Rebuilding a BMS](#)

2.5.3 Restarting a BMS

Scenarios

You can restart BMSs on the console. Only BMSs in running state can be restarted.

NOTE

Restarting a BMS will interrupt your services. Exercise caution when performing this operation.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the target BMS, click **More** in the **Operation** column, and select **Restart** from the drop-down list. To restart multiple BMSs, select them and click **Restart** at the top of the BMS list.
4. In the displayed dialog box, click **Yes**.

2.5.4 Reinstalling the OS

Scenarios

If the OS of a BMS fails to start, suffer from viruses, or requires optimization, reinstall the OS.

The original image is used to reinstall the BMS OS. BMSs provisioned on local disks and quickly provisioned BMSs both support OS reinstallation.

After the OS is reinstalled:

- The system disk type of the quickly provisioned BMS does not change.
- The IP address and MAC address of the BMS do not change.

Precautions

Reinstalling the OS is a mission-critical operation. Before performing this operation, read the following precautions carefully:

- To reinstall the OS, you must stop the BMS, which will interrupt your services.
- Reinstalling the OS clears the data in all partitions of the system disk. Back up data before performing this operation.

- Do not power off or restart the BMS during the OS reinstallation. Otherwise, the reinstallation may fail.
- After the OS is reinstalled, custom configurations, such as DNS and hostname of the original OS will be reset. You must reconfigure the OS.

Constraints

- The reinstalled OS must be the same as the original OS.
- During the OS reinstallation, the system disk capacity of a BMS provisioned using a local disk is not displayed.
- If the EVS disk where the BMS OS is installed is deleted during the OS reinstallation, the reinstallation will fail.
- During the OS reinstallation, you cannot inject user data.
- The OS of a BMS in maintenance state cannot be reinstalled.

Prerequisites

- The BMS must be in **Stopped** or **Reinstalling OS failed** state.
- If the boot device of the BMS is the EVS disk, the EVS disk quota must be greater than 0.
- If it is a quick-provisioning BMS, ensure that the BMS has a system disk.
- If the BMS is created using a private image, ensure that the image is still available.
- The OS reinstallation depends on the bms-network-config and Cloud-Init plug-ins in the BMS image.
 - If the BMS is created using a public image, ensure that the image has the bms-network-config and Cloud-Init plug-ins.
 - If the BMS is created using a private image, check whether bms-network-config and Cloud-Init are installed by following the instructions in [Bare Metal Server Private Image Creation Guide](#).

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row containing the target BMS, click **More** in the **Operation** column, and select **Reinstall OS** from the drop-down list.
The **Reinstall OS** dialog box is displayed.

Figure 2-6 Reinstalling the BMS OS

Reinstall OS ×

Reinstalling the OS is to use the original image of a BMS to install the BMS again. This operation does not incur extra fees.

1. OS reinstallation will delete system disk data, including data on the system partition and other partitions. Back up your system disk data before performing this operation.
2. After the OS reinstallation on a BMS is successful, the BMS will be automatically started.
3. To reset the BMS password, you must install a plug-in on the BMS after it is created. [Click here for more details.](#)
4. After the OS is reinstalled, customized configurations (such as DNS and hostname) will be reset.

Image CentOS 7.2 64bit for BareMetal
 OS Bit64-bit

Login Mode Key pair Password

The private key is required for you to log in to the BMS. It is important that this key not be lost.

Key Pair --Select-- C Create Key Pair

OK Cancel

4. Set **Login Mode**.
 - **Key pair**: You can select an existing key pair or click **Create Key Pair** and create a private key used to log in to the BMS.
 - **Password**: You can set the initial password for logging in to the BMS OS. The new password must meet the password complexity requirements listed in [Table 2-6](#).
5. Click **OK**.
6. On the **BMS OS Reinstallation** page, confirm the OS configuration and click **Submit**.

After the application is submitted, the BMS status changes to **Reinstalling OS**. The reinstallation is complete when the BMS status changes to **Running**. After the OS is reinstalled, the BMS will start automatically.

NOTE

Do not perform any operation on the temporary BMS during the reinstallation process.

2.5.5 Rebuilding a BMS

Scenarios

If a BMS cannot work properly due to hardware or SDI card damage, you can rebuild it. This section describes how to rebuild a BMS.

NOTE

A BMS cannot be rebuilt automatically. You need to contact the operation administrator to rebuild it.

Notes

- Currently, only BMSs that are quickly provisioned can be rebuilt.
- After a BMS is rebuilt, it will start automatically.

- If the BMS uses an IB NIC, record the IP address of the IB NIC rebuilding the BMS.
- If the BMS uses a QinQ network, record the IP address of the QinQ network before rebuilding the BMS.

Constraints

- A BMS can only be rebuilt in the same POD.
- A BMS to be rebuilt must use an EVS disk as its system disk.
- Data on local disks cannot be migrated after a BMS is rebuilt.

Prerequisites

- The BMS to be rebuilt must be stopped.
- The BMS to be rebuilt must have a system disk.

Procedure

1. If your BMS uses a QinQ network, delete configurations of the original QinQ network before rebuilding the BMS. For example, if eth3 and eth5 form port group bond1 for the QinQ network, delete the following configuration files:

```
rm /etc/udev/rules.d/80-persistent-net.rules
rm /etc/sysconfig/network-scripts/ifcfg-eth3
rm /etc/sysconfig/network-scripts/ifcfg-eth5
rm /etc/sysconfig/network-scripts/ifcfg-bond1
```

2. Contact the operation administrator and apply for rebuilding the BMS.
 - If your BMS uses the IB network and the IB NIC IP address assignment mode is DHCP, the IP address of the BMS will change after it is rebuilt. Therefore, if your service heavily depends on the IP address, you need to reconfigure the IP address of the IB network using the static configuration method. The operations describe how to set the IP address of the IB NIC to the original IP address.

- i. Log in to the BMS OS.

- ii. Create the `/etc/sysconfig/network-scripts/ifcfg-ib0` configuration file. The following uses CentOS as an example. Set `IPADDR` to the IP address of the BMS before it is rebuilt.

```
#/etc/sysconfig/network-scripts/ifcfg-ib0
DEVICE=ib0
ONBOOT=yes
BOOTPROTO=none
IPADDR=172.31.0.254
NETWORK=172.31.0.0
BROADCAST=172.31.0.255
NETMASK=255.255.255.0
```

- iii. Change the value of `enable_ib` in the `bms-network-config.conf` file to **False**.

```
sed -i 's/enable_ib.*/enable_ib = False/g' `find / -name bms-
network-config.conf
```

Check that the value has been changed.

```
cat `find / -name bms-network-config.conf
```

Figure 2-7 Checking the value of enable_ib

```
[NETWORK_CONFIG]
enable_bms_network = True
enable_bms_udev_rules = False
bsdtar_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtar.exe
mtu_use_dhcp_config = True

[METADATA]
enable_preserve_hostname = False

[IB]
enable_ib = False
```

- iv. Save the configuration and exit. Then restart the NIC.

```
ifdown ib0
```

```
ifup ib0
```

- v. Run the following command to check whether the configured IP address takes effect:

```
ifconfig ib0
```

2.5.6 Backing Up a BMS

Scenarios

To ensure data security, you can back up all EVS system and data disks of a BMS. This backup mode prevents data inconsistency caused by the difference in the backup creation time. The Cloud Server Backup Service (CSBS) offers the backup service for BMSs. It works based on the consistent snapshot technology for Elastic Volume Service (EVS) disks. With CSBS, you can use backup data to restore BMS data, ensuring data security and correctness.

Constraints

- BMS backups cannot be used to create images.
- BMSs with shared EVS disks cannot be backed up.
- When the BMS is restored using backup, the BMS will automatically stop, which will interrupt tenant services. After the BMS is stopped, it is locked for a specified time period during which tenants cannot perform operations on the BMS.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the target BMS, click **More** in the **Operation** column, and select **Create Backup**.
The **Create CSBS Backup** page is displayed.
4. Perform the following operations as prompted:
 - Select a BMS: By default, the BMS to be backed up is selected in the BMS list. Retain the default.
 - Configure the backup: Select **Auto Backup** and select a backup policy.

 NOTE

After the selected BMS is associated with the backup policy, the BMS will be automatically backed up based on the backup policy.

If the selected BMS has been associated with other policy, it will be disassociated from the original policy automatically and then associated with the new policy.

You can also select **back up now**. The selected BMS will be backed up immediately.

For more information, see [Cloud Backup and Recovery Getting Started](#).

2.5.7 Releasing a BMS

Scenarios

You can delete BMSs you no longer need. Once the status of a BMS becomes **Deleted**, no fees will be incurred for the BMS.

After a BMS is deleted, it is still displayed in the BMS list for a short period of time, after which it will be deleted from the BMS list. Tags and disks of the BMS will be disassociated from the BMS, and data on the disks will be deleted.

 NOTE

You can manually release a BMS billed in yearly/monthly mode after the validity period ends. If you do not renew the BMS, it will be released automatically. Before the BMS expires, you can apply for unsubscription to release the BMS in advance.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the target BMS, click **More** in the **Operation** column, and select **Unsubscribe** from the drop-down list.
4. On the **Unsubscribe** page, select a reason and click **Confirm**.
5. In the displayed dialog box, click **Yes**.

2.6 User Data and Metadata

2.6.1 Injecting User Data

Application Scenarios

You can inject user data to configure BMSs.

- Use scripts to simplify BMS configuration.
- Use scripts to initialize BMS OSs.
- Upload scripts to BMSs at creation time.
- Use scripts for other purposes.

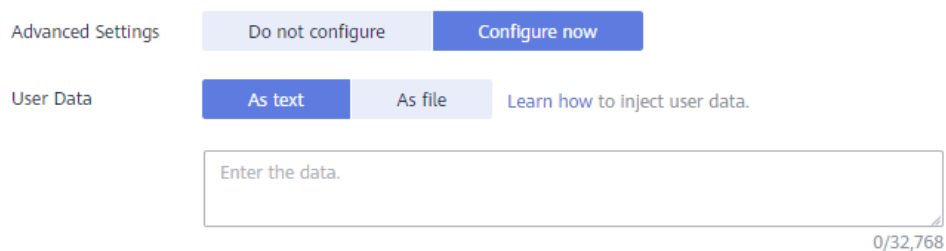
Constraints

- Linux:
 - The image that is used to create BMSs must have Cloud-Init installed.
 - The user data to be injected must be less than or equal to 32 KB.
 - User data uploaded as text can contain only ASCII characters. User data uploaded as a file can contain any characters, and the file size must be less than or equal to 32 KB.
 - The image that is used to create BMSs must be a public image, a private image created based on a public image, or a private image with Cloud-Init installed.
 - The script format must comply with user data script specifications for Linux BMSs.
 - DHCP must be enabled for the VPC, and port 80 must be enabled for the security group in the outbound direction.
 - If password login is used, user data injection will be unavailable.
- Windows:
 - The image that is used to create BMSs must have Cloudbase-Init installed.
 - The user data to be injected must be less than or equal to 32 KB.
 - User data uploaded as text can contain only ASCII characters. User data uploaded as a file can contain any characters, and the file size must be less than or equal to 32 KB.
 - The image that is used to create BMSs must be a public image, a private image created based on a public image, or a private image with Cloudbase-Init installed.
 - DHCP must be enabled for the VPC, and port 80 must be enabled for the security group in the outbound direction.

Procedure

1. Create a user data script. The format must comply with user data script specifications. For details, see [Helpful Links](#).
2. When creating a BMS, set **Advanced Settings** to **Configure now**, and paste the content of the user data script to the **User Data** text box or upload the user data file.

Figure 2-8 Injecting user data



3. The created BMS automatically runs Cloud-Init or Cloudbase-Init to read the user data script upon startup.

User Data Scripts of Linux BMSs

User data scripts of Linux BMSs are customized by using the open-source Cloud-Init architecture. This architecture uses BMS metadata as the data source for automatically configuring the BMSs. The script types are compatible with open-source Cloud-Init. For details about Cloud-Init, see <http://cloudinit.readthedocs.io/en/latest/topics/format.html>.

- Script execution time: A user data script is executed after the time when the status of the target BMS changes to **Running** and before the time when `/etc/init` is executed.

 **NOTE**

By default, the scripts are executed as user **root**.

- Script type: user-data scripts and Cloud-Config data scripts

Table 2-4 Linux BMS script types

-	User-Data Script	Cloud-Config Data
Description	Scripts, such as Shell and Python scripts, are used for custom configurations.	Methods pre-defined in Cloud-Init, such as the Yum source and SSH key, are used for configuring certain BMS applications.
Format	A script must be started with #! , for example, #!/bin/bash and #!/usr/bin/env python . When the BMS is started for the first time, the script will be executed at the rc.local-like level, indicating a low priority in the boot sequence.	The first line must be #cloud-config , and no space is allowed in front of it.
Constraint	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.
Frequency	The script is executed only once when the BMS is started for the first time.	The execution frequency varies depending on the applications installed on the BMS.

- How can I view the user data injected into a Linux BMS?
 - a. Log in to the BMS.
 - b. Run the following command to view the user data as user **root**:
curl http://169.254.169.254/openstack/latest/user_data

- Examples

This section describes how to inject scripts in different formats into Linux BMSs and view script execution results.

Example 1: Inject a User-Data script.

When creating a BMS, set **User Data** to **As Text** and enter the user data script content.

```
#!/bin/bash
echo "Hello, the time is now $(date -R)" | tee /root/output.txt
```

After the BMS is created, start it and run the **cat [file]** command to check the script execution result.

```
[root@XXXXXXXX ~]# cat /root/output.txt
Hello, the time is now Mon, 16 Jul 2016 16:03:18+0800
```

Example 2: Inject a Cloud-Config Data script.

When creating a BMS, set **User Data** to **As Text** and enter the user data script content.

```
#cloud-config
bootcmd:
- echo 192.168.1.130 us.archive.ubuntu.com >> /etc/hosts
```

After the BMS is created, start it and run the **cat /etc/hosts** command to check the script execution result.

Figure 2-9 Viewing the execution result

```
localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.130 us.archive.ubuntu.com
```

User Data Scripts of Windows BMSs

User data scripts of Windows BMSs are customized by using the open-source Cloudbase-Init architecture. This architecture uses BMS metadata as the data source for initializing and automatically configuring the BMSs. The script types are compatible with open-source Cloudbase-Init. For details about Cloudbase-Init, see <https://cloudbase-init.readthedocs.io/en/latest/userdata.html>.

- Script type: batch-processing program scripts and PowerShell scripts

Table 2-5 Windows BMS script types

-	Batch-Processing Program Script	PowerShell Script
For mat	The script must be started with rem cmd , which is the first line of the script. No space is allowed at the beginning of the first line.	The script must be started with #ps1 , which is the first line of the script. No space is allowed at the beginning of the first line.
Con strai nt	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.

- How can I view the user data injected into a Windows BMS?
 - a. Log in to the BMS.
 - b. Enter the following URL in the address box of a browser and view the injected user data:

http://169.254.169.254/openstack/latest/user_data

- Examples

This section describes how to inject scripts in different formats into Windows BMSs and view script execution results.

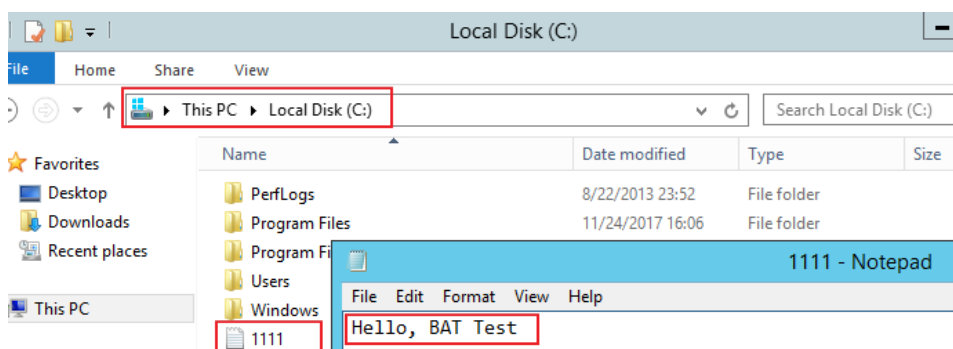
Example 1: Inject a batch-processing program script.

When creating a BMS, set **User Data** to **As Text** and enter the user data script content.

```
rem cmd
echo "Hello, BAT Test" > C:\1111.txt
```

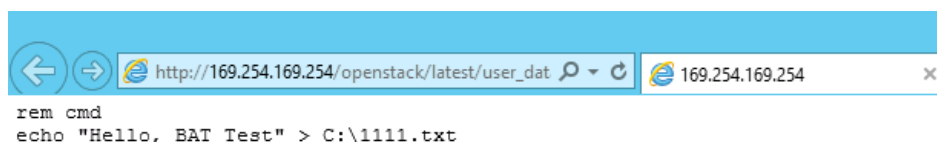
After the BMS is created, start it and check the script execution result. In this example, a text file named **1111** is added to disk C:\.

Figure 2-10 Text file 1111.txt



To view the user data injected into the Windows BMS, log in at http://169.254.169.254/openstack/latest/user_data.

Figure 2-11 Viewing user data in 1111.txt

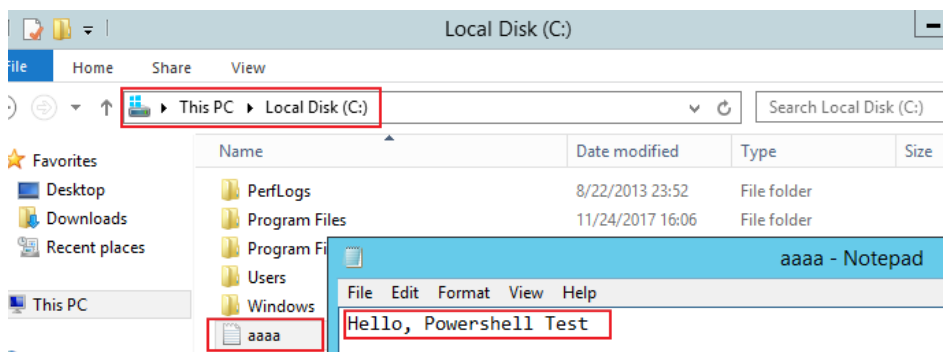


Example 2: Inject a PowerShell script.

When creating a BMS, set **User Data** to **As Text** and enter the user data script content.

```
#ps1
echo "Hello, Powershell Test" > C:\aaaa.txt
```

After the BMS is created, start it and check the script execution result. In this example, a text file named **aaaa** is added to disk C:\.

Figure 2-12 Text file aaaa.txt

To view the user data injected into the Windows BMS, log in at http://169.254.169.254/openstack/latest/user_data.

Figure 2-13 Viewing user data in aaaa.txt

Case 1

This case illustrates how to inject user data so as to simplify BMS configuration.

In this example, vim is configured to enable syntax highlighting, display line numbers, and set the tab stop to 4. Configuration file `.vimrc` is created and injected into the `/root/.vimrc` directory during BMS creation. After the BMS is created, vim is automatically configured based on your requirements. This helps to improve BMS configuration efficiency, especially when you are creating BMSs in a batch.

The script is as follows:

```
#cloud-config
write_files:
- path: /root/.vimrc
  content: |
    syntax on
    set tabstop=4
    set number
```

Case 2

This case illustrates how to inject user data so as to reset the password for logging in to a Linux BMS.

In this example, the password of user `root` will be reset to `"*****"`.

NOTE

The new password must meet the password complexity requirements listed in [Table 2-6](#).

Table 2-6 Password requirements

Parameter	Requirements	Example Value
Password	<ul style="list-style-type: none">• Consists of 8 to 26 characters.• Must contain at least three of the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters !@\$%^_+=[]{};.,/?• Cannot contain the username or the username spelled backwards.• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows BMSs.)	Test12\$@

The script is as follows (retain the indentation in the following script):

```
#cloud-config
chpasswd:
  list: |
    root:*****
  expire: False
```

After the BMS is created, you can use the new password to log in to it. To ensure system security, change the password of user **root** after logging in to the BMS for the first time.

Case 3

This case illustrates how to inject user data so as to create a user on a Windows BMS and set a password for the user.

In this example, the user's username is **abc**, its password is *********, and the user is added to the **administrators** user group.

NOTE

The new password must meet the password complexity requirements listed in [Table 2-7](#).

Table 2-7 Password requirements

Parameter	Requirements	Example Value
Password	<ul style="list-style-type: none">• Consists of 8 to 26 characters.• Must contain at least three of the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters !@\$%^_+=[]{};.,/?• Cannot contain the username or the username spelled backwards.• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows BMSs.)	Test12\$@

The script is as follows:

```
rem cmd
net user abc ***** /add
net localgroup administrators abc /add
```

After the BMS is created, you can use its username and password to log in to it.

Case 4

This case illustrates how to inject user data so as to update system software packages for a Linux BMS and enable the HTTPd service. After the user data is injected, you can use the HTTPd service.

The script is as follows:

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Case 5

This case illustrates how to inject user data so as to assign the user **root** permission for remotely logging in to a Linux BMS. After injecting the file, you can log in to the BMS as user **root** in SSH key authentication mode.

The script is as follows:

```
#cloud-config
disable_root: false
runcmd:
- sed -i 's/^PermitRootLogin.*$/PermitRootLogin without-password/' /etc/ssh/sshd_config
- sed -i '/^KexAlgorithms.*$/d' /etc/ssh/sshd_config
- service sshd restart
```

Helpful Links

For more information about user data injection cases, visit the official Cloud-init/Cloudbase-init website:

- <https://cloudinit.readthedocs.io/en/latest/>
- <https://cloudbase-init.readthedocs.io/en/latest/>

2.6.2 Retrieving Metadata

Introduction

The BMS metadata includes BMS basic information on the cloud platform, such as the BMS ID, hostname, and network information. The BMS metadata can be retrieved using compatible OpenStack and EC2 APIs listed in [Table 2-8](#).

Table 2-8 BMS metadata types

Metadata Type	Metadata Item	Description
OpenStack type	/meta_data.json	This interface is used to query BMS metadata. For the key fields in the BMS metadata, see Table 2-9 .
	/password	This interface is used to query the BMS password. If a key pair is selected during the creation of a Windows BMS, Cloudbase-Init is used to save the ciphertext password when the BMS is initialized.
	/user_data	This interface is used to query BMS user data. This metadata allows you to specify scripts and configuration files for initializing BMSs. For details, see Injecting User Data . For password-authenticated Linux BMSs, save the password injection script.
	/network_data.json	This interface is used to query network information of a BMS.
	/securitykey	This interface is used to obtain temporary security credentials: Access Key ID (AK) and Secret Access Key (SK). Before obtaining temporary AK/SK on a BMS, you need to create an agency for BMS on IAM and assign required resource permissions to BMS.

Metadata Type	Metadata Item	Description
EC2 type	/meta-data/ hostname	This interface is used to query the host name of a BMS. To remove the suffix .novalocal from a BMS, see: Is the BMS Host Name with Suffix novalocal Normal?
	/meta-data/ instance-type	This interface is used to query the flavor name of a BMS.
	/meta-data/local- ipv4	This interface is used to query the fixed IP address of a BMS. If there are multiple NICs, only the IP address of the primary NIC is displayed.
	/meta-data/ placement/ availability-zone	This interface is used to query AZ information about a BMS.
	/meta-data/public- ipv4	This interface is used to query the EIP of a BMS. If there are multiple NICs, only the EIP of the primary NIC is displayed.
	/meta-data/public- keys/0/openssh-key	This interface is used to query the public key of a BMS.
	/user-data	This interface is used to query BMS user data.
	/meta-data/ security-groups	This interface is used to query the name of the security group of the BMS.

Table 2-9 Metadata key fields

Parameter	Type	Description
uuid	String	Specifies the BMS ID.
availability_zone	String	Specifies the AZ where the BMS is located.
meta	Dict	Specifies the metadata information, including the image name, image ID, and VPC ID.

Parameter	Type	Description
hostname	String	Specifies the hostname of the BMS. To remove the suffix .novalocal from a BMS, see: Is the BMS Host Name with Suffix novalocal Normal?
vpc_id	String	Specifies the ID of the VPC where the BMS is located.

The following describes the URI and methods of using the supported BMS metadata.

Prerequisites

- You have logged in to the BMS.
- Security group rules in the outbound direction meet the following requirements:
 - Protocol: TCP
 - Port Range: 80
 - Remote End: 169.254.0.0/16

NOTE

If you use the default security group rules in the outbound direction, the preceding requirements are met, and the metadata can be accessed. The default outbound security group rule is as follows:

- Protocol: Any
- Port Range: Any
- Remote End: 0.0.0.0/16

Metadata (OpenStack Metadata API)

This interface is used to query BMS metadata.

- URI
`/169.254.169.254/openstack/latest/meta_data.json`
- Method
Supports GET requests.
- Example

The following describes how to use the cURL tool to query the BMS metadata:

curl http://169.254.169.254/openstack/latest/meta_data.json

```
{
  "random_seed": "rEocCViRS+dNwlYdGlxJHUp+00poeUsAdBFkbPbYQTmpNwpoEb43k9z+96TyrekNKS
+iLYDdRNy4kKGoNPEVBCC05Hg1TcDbLAPfJwgJS1okqEtlcofUhKmlL3K0fto
+5KXEDU3GNuGwyZXjdVb9HQWU+E1jztAJjqsahnU+g/tawABTVySLBKlAT8fMGax1mTGgArucn/
WzDcy19DGioKPE7F8lLtSQ4Ww3VClK5VYB/h0x+4r7IVHrPmYX/
bi1Yhm3Dc4rRYNaTjdOV5gUOsbo3oAeQkmKwQ/
NO0N8qw5Ya4l8ZUW4tMav4mOsRySOOB35v0bvalc6p
```

```
+50DTbWNeX5A2MLiEhTP3vsPrmvk4LRF7CLz2J2TGIM14OoVBw7LARwmv9cz532zHki/c8tlhRzLmOTXh/  
wL36zFW10DeuReUGmxth7lGNmRMQKV6+mil78jm/KMPpgAdK3vwYF/  
GcelOFJD2HghMUUCeMbwYnvijLTejuBpwhJMNIHA/NvIExJDxqBCoss/Jfe+yCmUFyxovJ  
+L8oNkTzkmtCNzw3Ra0hiKchGhqK3BleToV/kVx5DdF081xrEA  
+qyoM6CVyfJtEoz1zLRyoo9bJ65Eg6Jd8dj1UCVsDqRY1plJgzE/  
Mzsw6AaaCVhaMJL7u7YmVdyKzA6z65Xtvujz0Vo=",  
  "uuid": "ca9e8b7c-f2be-4b6d-a639-f10b4d994d04",  
  "availability_zone": "lt-test-1c",  
  "hostname": "bms-ddd4-l00349281.novalocal",  
  "launch_index": 0,  
  "meta": {  
    "metering.image_id": "3a64bd37-955e-40cd-ab9e-129db56bc05d",  
    "metering.imagetype": "gold",  
    "metering.resourcespeccode": "physical.s3.small",  
    "metering.cloudServiceType": "service.type.ec2",  
    "image_name": "CentOS 7.6 64bit",  
    "os_bit": "64",  
    "vpc_id": "3b6c201f-aeb3-4bce-b841-64756e66cb49",  
    "metering.resourcetype": "1",  
    "cascaded.instance_extrainfo": "pcibridge:2",  
    "os_type": "Linux",  
    "charging_mode": "0"  
  },  
  "project_id": "6e8b0c94265645f39c5abbe63c4113c6",  
  "name": "ecs-ddd4-l00349281"  
}
```

User Data (OpenStack Metadata API)

This interface is used to query BMS user data. The value is configured when you create a BMS. It cannot be changed after the configuration.

- URI
/169.254.169.254/openstack/latest/user_data
- Method
Supports GET requests.
- Example

curl http://169.254.169.254/openstack/latest/user_data

```
ICAgICAgDQoiQSBjbG91ZCBkb2VzIG5vdCBrbm93IHdoeSBpdCBtb3ZlcyBpbjBqdXN0IHN1Y2ggYSBkaXJlY  
3Rpb24gYW5kIGF0IHN1Y2ggYSBzcGVlZC4uLkI0IGZlZWxzIGFuIGltcHVsc2lubi4uLnRoaXMgaXMgdGhlIH  
BsYWNIHRvIGdvlG5vdy4gQnV0IHRoZSBza3kga25vd3MgdGhllHJlYXNvbnMgYW5kIHRoZSBwYXR0ZXJl  
cyBiZWhpbmQgYWx5IGNsbnV0IHRoZSBza3kga25vd3MgdGhllHJlYXNvbnMgYW5kIHRoZSBwYXR0ZXJl  
Vyc2VsZiBoaWdoIGVub3VnaCB0byBzZWUgYmV5b25kIGhvcml6b25zLilINCg0KLlVpY2hhcmQmFjaA=  
=
```

NOTE

If user data is not injected during BMS creation, the query result is 404.

Figure 2-14 404 Not Found

```
[root@pythonsdktempest--server-1519783681 ~]# curl http://169.254.169.254/openstack/latest/user_data  
<html>  
<head>  
<title>404 Not Found</title>  
</head>  
<body>  
<h1>404 Not Found</h1>  
The resource could not be found.<br /><br />  
</body>  
</html>
```

Network Data (OpenStack Metadata API)

This interface is used to query network information of a BMS.

- URI
/openstack/latest/network_data.json
- Method
Supports GET requests.

- Example

curl http://169.254.169.254/openstack/latest/network_data.json

```
{
  "services": [
    {
      "type": "dns",
      "address": "100.125.1.250"
    },
    {
      "type": "dns",
      "address": "100.125.21.250"
    }
  ],
  "networks": [
    {
      "network_id": "67dc10ce-441f-4592-9a80-cc709f6436e7",
      "type": "ipv4_dhcp",
      "link": "tap68a9272d-71",
      "id": "network0"
    }
  ],
  "links": [
    {
      "type": "cascading",
      "vif_id": "68a9272d-7152-4ae7-a138-3ef53af669e7",
      "ethernet_mac_address": "fa:16:3e:f7:c1:47",
      "id": "tap68a9272d-71",
      "mtu": null
    }
  ]
}
```

Security Key (OpenStack Metadata API)

This interface is used to obtain temporary security credentials: Access Key ID (AK) and Secret Access Key (SK).

NOTE

- To obtain temporary AK/SK on a BMS, you need to create an agency for BMS on IAM and assign required resource permissions to BMS. For details, see [Identity and Access Management User Guide](#).
- The temporary AK/SK pair expires an hour later but is updated 10 minutes ahead of the expiration time. During the 10 minutes, both the new and old temporary AK/SK pairs can be used.
- When using temporary AK/SK, add '**X-Security-Token:securitytoken**' in the message header. **securitytoken** is the value returned when a call is made to the API.

- URI
/openstack/latest/securitykey
- Method
Supports GET requests.

- Example

curl http://169.254.169.254/openstack/latest/securitykey

User Data (EC2 Compatible API)

This interface is used to query BMS user data. The value is configured when you create a BMS. It cannot be changed after the configuration.

- URI
/169.254.169.254/latest/user-data
- Method
Supports GET requests.
- Example

curl http://169.254.169.254/latest/user-data

```
ICAgICAgDQoiQSBjbG91ZCBkb2VzIG5vdCBrbm93IHdoeSBpdCBtb3ZlcyBpbjBqdXN0IHN1Y2ggYSBkaXJlY  
3Rpb24gYW5kIGF0IHN1Y2ggYSBzcGVlZC4uLkI0IGZlZWxzIGFuIGltcHVsc2lubi4uLnRoZXN0IGF0IHN1Y2ggYSBkaXJlY  
BsYWNlIHJlIGVlIG5vdy4gQnV0IHRob290ZSBza3kga25vd3MgdGhllHJlYXNvbnMgYW5kIHRob290ZSBwYXR0ZXJl  
cyBiZWwhpbmQgYWxsIGNsbnV0IGVlIG5vdy4gQnV0IHRob290ZSBza3kga25vd3MgdGhllHJlYXNvbnMgYW5kIHRob290ZSBwYXR0ZXJl  
Vyc2VsZiBoaWdoIGVub3VnaCB0byBzZWUgYmV5b25kIGhvcml6b25zLiINCg0KLVJpY2hhcmQgQmFjaA=  
=
```

Hostname (EC2 Compatible API)

This interface is used to query the name of the host accommodating a BMS. The **.novalocal** suffix will be added later.

- URI
/169.254.169.254/latest/meta-data/hostname
- Method
Supports GET requests.
- Example

curl http://169.254.169.254/latest/meta-data/hostname

```
bms-test.novalocal
```

Instance Type (EC2 Compatible API)

This interface is used to query the flavor name of a BMS.

- URI
/169.254.169.254/latest/meta-data/instance-type
- Method
Supports GET requests.
- Example

curl http://169.254.169.254/latest/meta-data/instance-type

```
physical.o2.medium
```

Local IPv4 (EC2 Compatible API)

This interface is used to query the fixed IP address of a BMS. If there are multiple NICs, only the IP address of the primary NIC is displayed.

- URI
/169.254.169.254/latest/meta-data/local-ipv4

- Method
Supports GET requests.
- Example
curl http://169.254.169.254/latest/meta-data/local-ipv4
192.1.1.2

Availability Zone (EC2 Compatible API)

This interface is used to query AZ information about a BMS.

- URI
/169.254.169.254/latest/meta-data/placement/availability-zone
- Method
Supports GET requests.
- Example
curl http://169.254.169.254/latest/meta-data/placement/availability-zone
az1.dc1

Public IPv4 (EC2 Compatible API)

This interface is used to query the EIP of a BMS. If there are multiple NICs, only the EIP of the primary NIC is displayed.

- URI
/169.254.169.254/latest/meta-data/public-ipv4
- Method
Supports GET requests.
- Example
curl http://169.254.169.254/latest/meta-data/public-ipv4
46.1.1.2

Public Keys (EC2 Compatible API)

This interface is used to query the public key of a BMS.

- URI
/169.254.169.254/latest/meta-data/public-keys/0/openssh-key
- Method
Supports GET requests.
- Example
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADI5Fw5k8Fgzajn1zJwLoV3+wMP+6CyvsSilc/
hioggSnYu/AD0Yqm8vVO0kWLun1rFbdO+QUZKyVr/OPUjQSw4SRh4qsTKf/+eFoWTjplFvd1WCBZzS/
WRenxlwR00KkczHSJro763+wYcwKieb4eKRxaQoQvoFgVjLBULXAJH4eKoKTVNtMXAvPP9aMy2SLgsJNt
Mb9ArfziAiblQynq7UIflnN3VclzPeiWrqtzjyOp6CPUXnL0lVPTvbLe8sUteBsJZwLL6K4i
+Y0lf3ryqnmQgC21yW4Dzu+kwk8FVT2MgWkCwiZd8gQ/+uJzrJFyMFUOBkiOBfuUENIUhAB
Generated-by-Nova

3 Image

3.1 Private Image Overview

A private image is an image available only to the user who created it. It contains an OS, preinstalled public applications, and a user's private applications. You can create a private image in the following ways:

- [Creating a Private Image from a BMS](#)
- [Creating a Private Image from an External Image File](#)

After a private image is created successfully, the image status becomes **Normal**. You can use the image to create BMSs or share the image with other tenants. You can also replicate the image to your other regions. The following figure shows how to use private images.

3.2 Creating a Private Image from a BMS

Scenarios

You can create a private image from a BMS and copy the system disk data of the BMS to the private image. The system disk contains an OS and pre-installed applications for running services.

Constraints

- Currently, only a BMS that supports quick provisioning (the OS is installed on an EVS disk) can be used to create a private image.
- Data disks of a BMS cannot be exported as images.
- The BMS must be stopped.
- This operation depends on the bms-network-config and Cloud-Init plug-ins in the BMS image.

NOTE

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 the BMS is created using a public image, the image has the bms-network-config and Cloud-Init plug-ins by default.
- If the BMS is created using a private image, check whether bms-network-config and Cloud-Init are installed by following the instructions in [Bare Metal Server Private Image Creation Guide](#).

Precautions

- Delete sensitive data from the BMS before using it to creating a private image to prevent data leak.
- Delete residual files from the OS. For details, see [Deleting Files](#).
- During the image creation process, do not change the BMS status. Otherwise, the image will fail to be created.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the target BMS, click **More** in the **Operation** column, and select **Stop** from the drop-down list.
Only a BMS in stopped state can be used to create a private image.
4. After the BMS status changes to **Stopped**, click **More** in the **Operation** column and select **Create Image**.
The page for creating an image is displayed.
5. Enter the image name, select an enterprise project, set a tag, and enter description as needed.
Click **Next**.
6. On the displayed **Details** page, confirm the configuration and click **Submit**.
7. Return to the image list. If the status of the private image changes to **Normal**, the private image is created successfully.

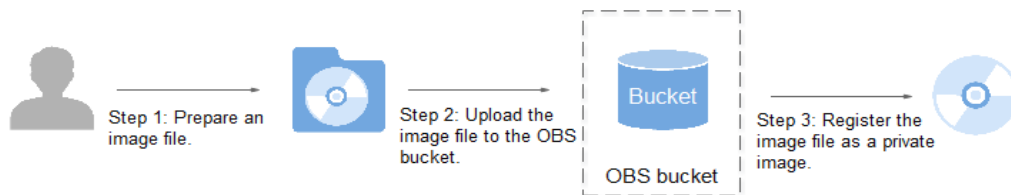
Follow-up Operations

If you want to create BMSs using the private image, see [Creating a BMS Using a Private Image](#). On the page for creating BMSs, select the private image you have created.

3.3 Creating a Private Image from an External Image File

Scenarios

You can create and register a private image using an external image file. [Figure 3-1](#) shows the procedure.

Figure 3-1 Creating a private image from an external image file

The procedure contains the following steps:

1. Prepare an image file. For details, see [Bare Metal Server Private Image Creation Guide](#).
2. Upload the image file to your OBS bucket. For details, see [Upload an External Image File](#).
3. On the management console, select the uploaded image file and register it as a private image. For details, see [Register a Private Image](#).

Constraints

You can import an image file in VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format to create a private image.

NOTE

Images of other formats must be converted using the image conversion tool before they can be used on BMSs. For details about how to convert the image format, see [Image Management Service Best Practices](#).

Upload an External Image File

Use OBS Browser+ to upload external image files..

When uploading the external image file, you must select an OBS bucket with standard storage.

Register a Private Image

1. Log in to the management console.
2. Under **Computing**, click **Image Management Service**.
The IMS console is displayed.
3. Click **Create Image** in the upper right corner.
4. Configure the following information:

Image Type and Source

- **Type:** Select **System disk image**.
- **Source:** Select **Image file**.

In the bucket list, select the bucket that stores the image file and select the image file.

Image Information

- **Function:** Select **BMS system disk image**.

Ensure that you have completed initialization configuration on the image file by following the instructions in [Bare Metal Server Private Image Creation Guide](#).

- **OS:** (Optional) Select the OS of the image file.
To ensure that the image can be created and used properly, select the OS consistent with that of the image file.
 - **System Disk (GB):** Set the system disk size. You are advised to set the value to the image system disk size plus 2 GB.
 - **Name:** Enter a name for the image to be created. The value can contain only letters, digits, spaces, hyphens (-), underscores (_), and periods (.), and cannot start or end with a space.
 - **Enterprise Project:** Select an enterprise project from the drop-down list. This parameter is available only when you have enabled the enterprise project function, or your account is an enterprise account. To enable this function, contact your customer manager.
 - **Description:** (Optional) Enter description of the image.
5. Click **Next**.
On the displayed **Details** page, confirm the configuration and click **Submit**.
 6. Return to the image list. If the status of the private image changes to **Normal**, the private image is registered successfully.

 **NOTE**

The time required for registering a private image varies depending on the size of the image file.

Follow-up Operations

You can use the private image to create a BMS by following the instructions in [Creating a BMS Using a Private Image](#).

4 Disk

4.1 Disk Types

Huawei Cloud provides various storage products for your BMSs, including block storage based on the distributed storage architecture, dedicated storage based on Huawei enterprise storage architecture, and local disks.

- Block storage refers to EVS disks, which are block-based storage products and adopt a three-copy distributed mechanism. EVS disks provide high reliability, performance, and scalability. You can create or release them at any time.
- Dedicated Distributed Storage Service (DSS) provides dedicated physical storage resources and adopts a three-copy distributed mechanism similar to block storage. It provides high availability and durability, and stable and low latency using multiple technologies, such as data redundancy and cache acceleration.
- Local disks include NVMe SSDs, SATA disks, and others. They provide a low latency, high throughput, and high cost-effectiveness and are applicable to scenarios that have large volumes of data and require high storage I/O performance and real-time performance.

Because local disks of a single physical server may encounter a single point of failure (SPOF), you are advised to configure data redundancy at the application layer to ensure data availability.

Table 4-1 Comparison of storage products

Storage Product	Storage Type	Typical Application Scenarios	Process
Block storage	Shared storage pools	<ul style="list-style-type: none"> • Enterprise daily work • Development and testing • Enterprise applications, including SAP, Microsoft Exchange, and Microsoft SharePoint • Distributed file systems • Various databases, including MongoDB, Oracle, SQL Server, MySQL, and PostgreSQL 	Create a disk and then attach the disk to the BMS.
DSS	Physically isolated storage pools and dedicated resources	<ul style="list-style-type: none"> • Hybrid load: DSS supports hybrid deployment of HPC, database, email, OA, and web applications. • High-performance computing • OLAP applications 	<p>DSS can be used with BMSs in DeCs or those not in DeCs.</p> <ul style="list-style-type: none"> • DeC scenario: Enable DeC, apply for a storage pool, create a disk in the storage pool, and attach the disk to the BMS. • Non-DeC scenario: Apply for a storage pool, create a disk in the storage pool, and attach the disk to the BMS.
Local disks	Local disks of servers	<ul style="list-style-type: none"> • Big data • Distributed cache 	Create a BMS and use its local disks directly.

4.2 Attaching Data Disks

Scenarios

If the existing disks of a BMS fail to meet service requirements, for example, due to insufficient disk space or poor disk performance, you can attach more available disks to the BMS, or create more disks and attach them to the BMS.

Constraints

- The disk and the target BMS must be located in the same AZ.
- The BMS must be in **Running** or **Stopped** state.
- **Device Type** of the EVS disk must be **SCSI**.
- A non-shared EVS disk must be in **Available** state.
A shared EVS disk must be in **In-use** or **Available** state.
- BMSs using some flavors or images cannot have EVS disks attached because the servers do not have SDI iNICs or for other reasons.
- Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. For details, see [How Do I View My Quotas?](#)

Prerequisites


Disks are available.

For details about how to create disks, see "Creating an EVS Disk" in *Elastic Volume Service User Guide*.

NOTE

If DSS is used, see Dedicated Distributed Storage Service Getting Started.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the upper right corner of the BMS list, enter the name, private IP address, ID, or flavor of a BMS and click  to search for the desired BMS.
4. Click the name of the target BMS.
The page showing details of the BMS is displayed.
5. Click the **Disks** tab. Then, click **Attach Disk**.
The **Attach Disk** dialog box is displayed.
6. Select the disk type and target disk, and set the mount point as prompted.

 NOTE

If no EVS disks are available, click **Create Disk** in the lower part of the list.

7. Click **OK**.

After the disk is attached, you can view the information about it on the **Disks** tab.

Follow-up Operations

If the attached disk is newly created, the disk can be used only after it is initialized (formatted). For details about how to initialize data disks, see [Initializing Data Disks](#).

 NOTE

After the BMS is restarted, the drive letter of the EVS disk may change. For the mapping between the EVS disk device and drive letter, see [How Do I Obtain the Drive Letter of an EVS Disk?](#)

4.3 Initializing Data Disks

4.3.1 Introduction to Data Disk Initialization Scenarios and Partition Styles

Scenarios

After a disk is attached to a BMS, you need to log in to the BMS to initialize (format) the disk before you can use the disk properly.

- System disk
A system disk does not need to be initialized because it is automatically created and initialized during the BMS creation. The default disk partition style is master boot record (MBR).
- Data disk
 - If a data disk is created during the BMS creation, it will be automatically attached to the BMS.
 - If a data disk is created explicitly, you need to manually attach the data disk to the BMS.

In both cases, the data disk can only be used after it is initialized. Choose a proper disk partition style based on your service plans.

Disk Partition Style

[Table 4-2](#) lists the common disk partition styles. For Linux OSs, different disk partition styles require different partitioning tools.

Table 4-2 Disk partition styles

Disk Partition Style	Maximum Disk Capacity Supported	Maximum Number of Partitions Supported	Linux Partitioning Tool
Master Boot Record (MBR)	2 TB	<ul style="list-style-type: none">• 4 primary partitions• 3 primary partitions and 1 extended partition <p>With the MBR partition style, primary partitions and an extended partition can be included, where the extended partition can contain several logical partitions. For example, if 6 partitions need to be created, you can create the partitions in the following two ways:</p> <ul style="list-style-type: none">• 3 primary partitions and 1 extended partition, with the extended partition containing 3 logical partitions• 1 primary partition and 1 extended partition, with the extended partition containing 5 logical partitions	<ul style="list-style-type: none">• fdisk• parted
GUID Partition Table (GPT)	18 EB 1 EB = 1048576 TB	Unlimited Disk partitions allocated using GPT are not categorized.	parted

 **CAUTION**

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Currently, an EVS data disk supports up to 32 TB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB.

If you change the disk partition style after the disk has been used, the original data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Partitioning Operation Guide

For a disk with less than 2 TB capacity, see one of the following topics:

- [Initializing a Windows Data Disk \(Windows Server 2016\)](#)
- [Initializing a Linux Data Disk \(fdisk\)](#)
- [Initializing a Linux Data Disk \(parted\)](#)

For a disk with greater than 2 TB capacity, see one of the following topics:

- [Initializing a Windows Data Disk Greater Than 2 TB \(Windows Server 2012\)](#)
- [Initializing a Linux Data Disk Greater Than 2 TB \(parted\)](#)

4.3.2 Initializing a Windows Data Disk (Windows Server 2016)

Scenarios

This section uses Windows Server 2016 Standard 64bit to describe how to initialize a data disk attached to a BMS running Windows.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB. For details about disk partition styles, see [Introduction to Data Disk Initialization Scenarios and Partition Styles](#).

The method for initializing a disk varies depending on the OSs running on the BMS. This document is for reference only. For detailed operations and differences, see the product documents of the OSs running on the corresponding BMSs.

⚠ CAUTION

When using an EVS disk for the first time, if you have not initialized the disk, including creating partitions and file systems, the additional capacity added to the disk in a later expansion operation may not be normally used.

Prerequisites

- You have logged in to the BMS.
- A data disk has been attached to the BMS and has not been initialized.

Procedure

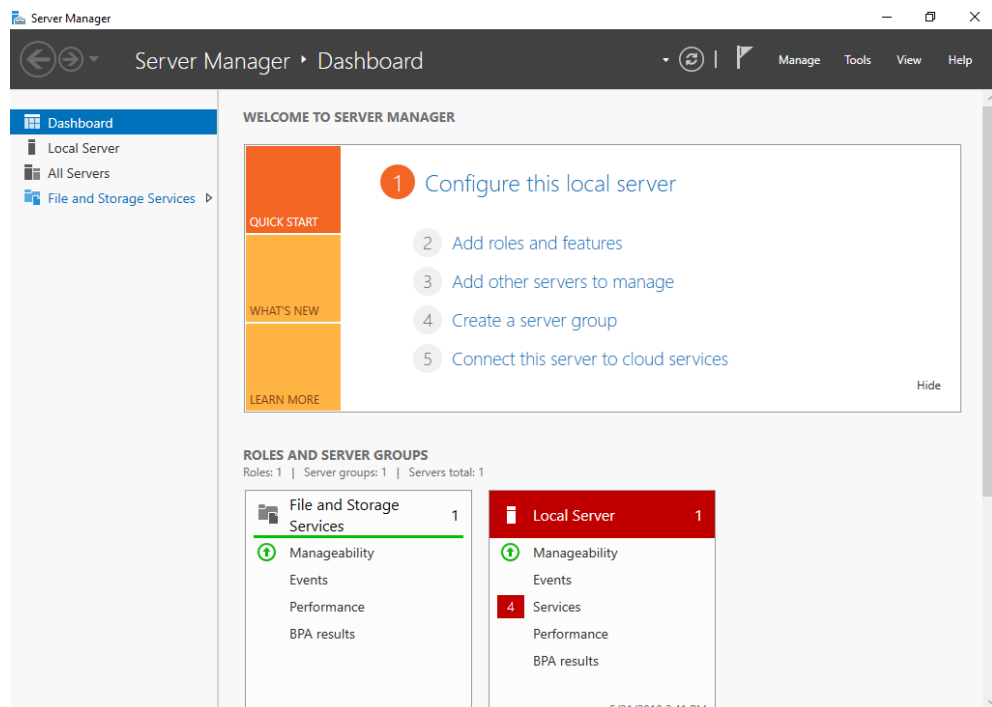
Step 1 On the BMS desktop, click the start icon in the lower left corner.

The **Windows Server** window is displayed.

Step 2 Click **Server Manager**.

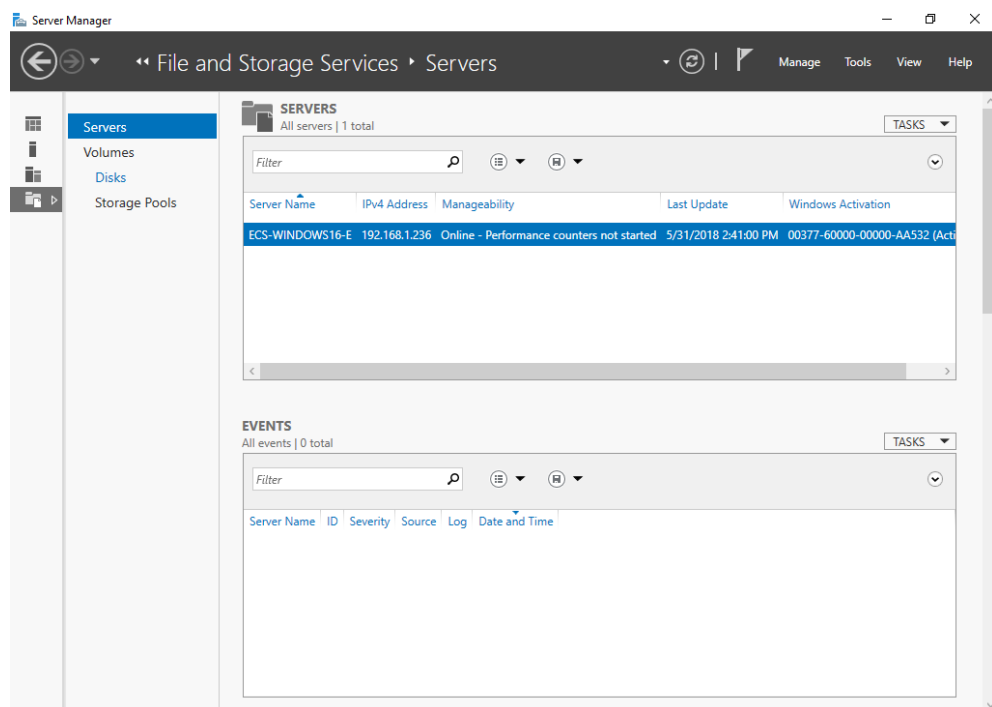
The **Server Manager** window is displayed.

Figure 4-1 Server Manager



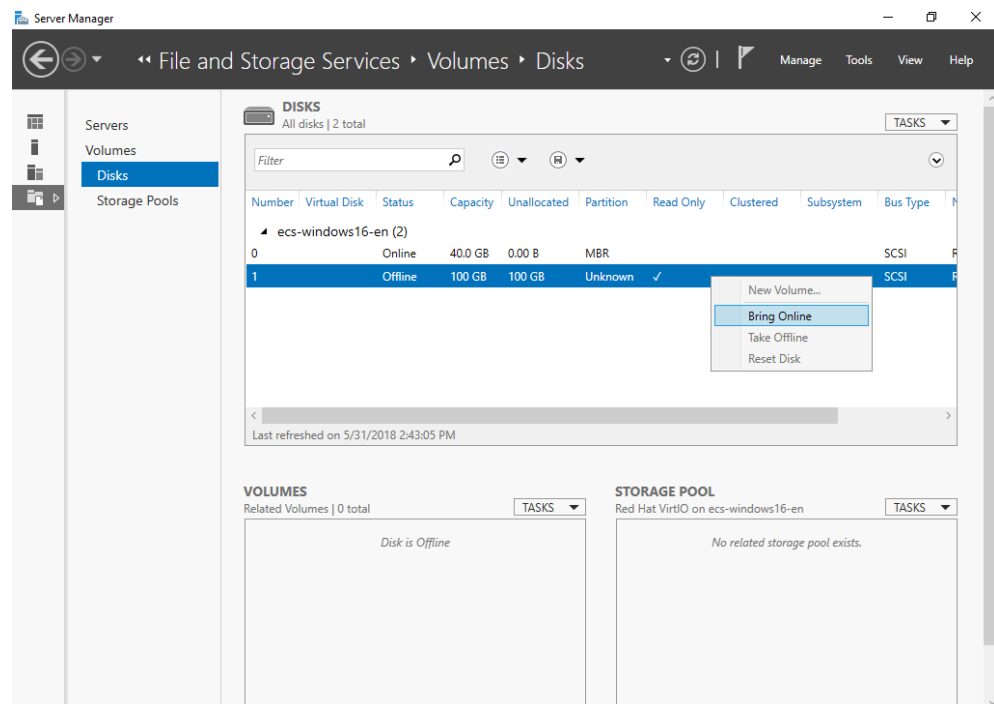
Step 3 In the navigation tree on the left, choose **File and Storage Services**.
The **Servers** page is displayed.

Figure 4-2 Servers



Step 4 In the navigation pane, choose **Disks**.
The **Disks** page is displayed.

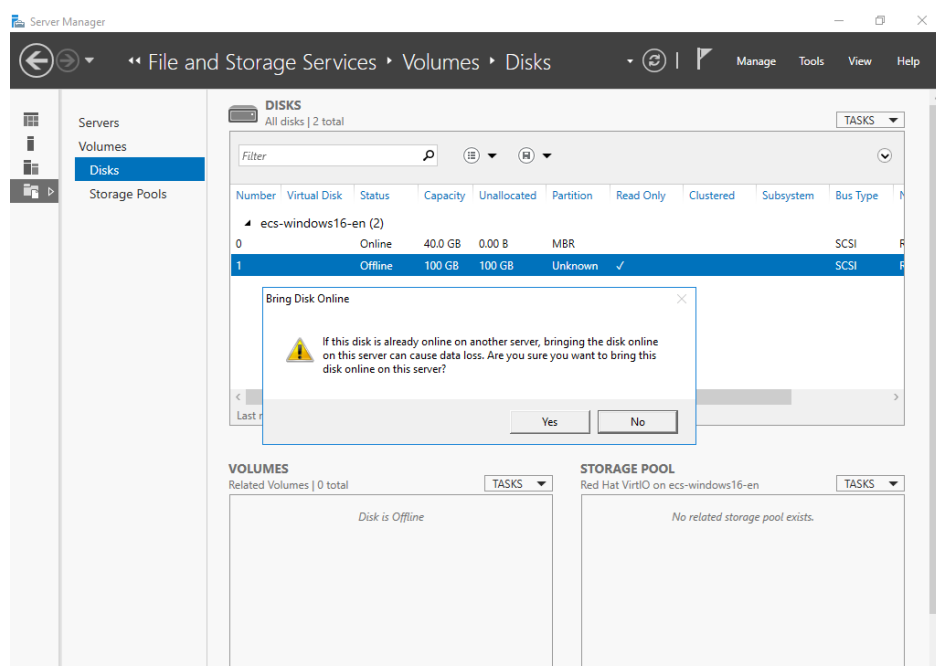
Figure 4-3 Disks



Step 5 Disks are listed in the right pane. If the new disk is in the offline state, bring it online before initialize it.

1. Right-click the new disk and choose **Bring Online** from the shortcut menu. The **Bring Disk Online** dialog box is displayed.

Figure 4-4 Bring Disk Online



2. Click **Yes** to confirm the operation.


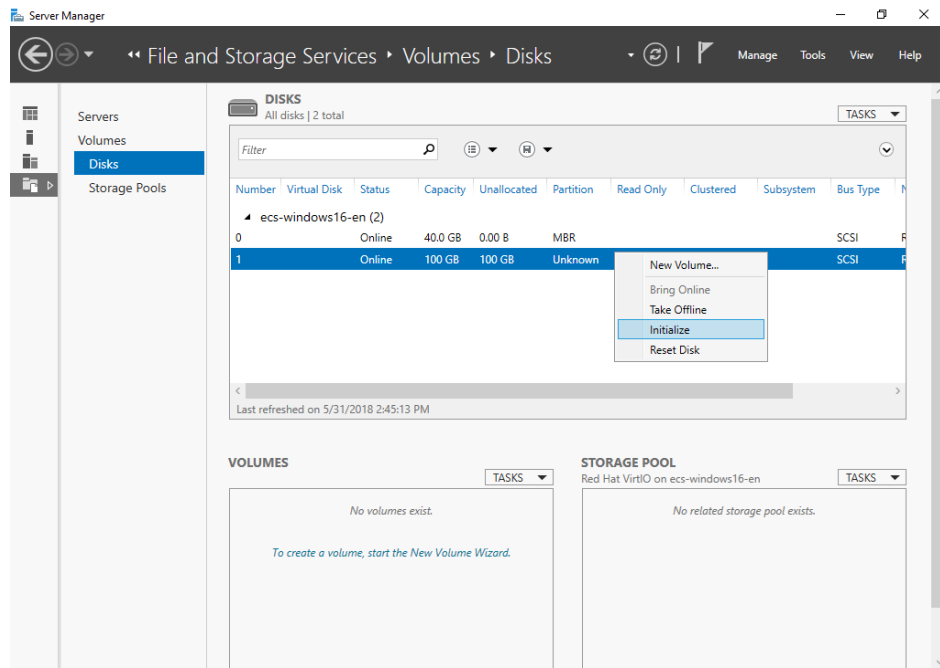
3. Click  in the upper area of the page to refresh the disk information. When the disk status changes from **Offline** to **Online**, the disk has been brought online.

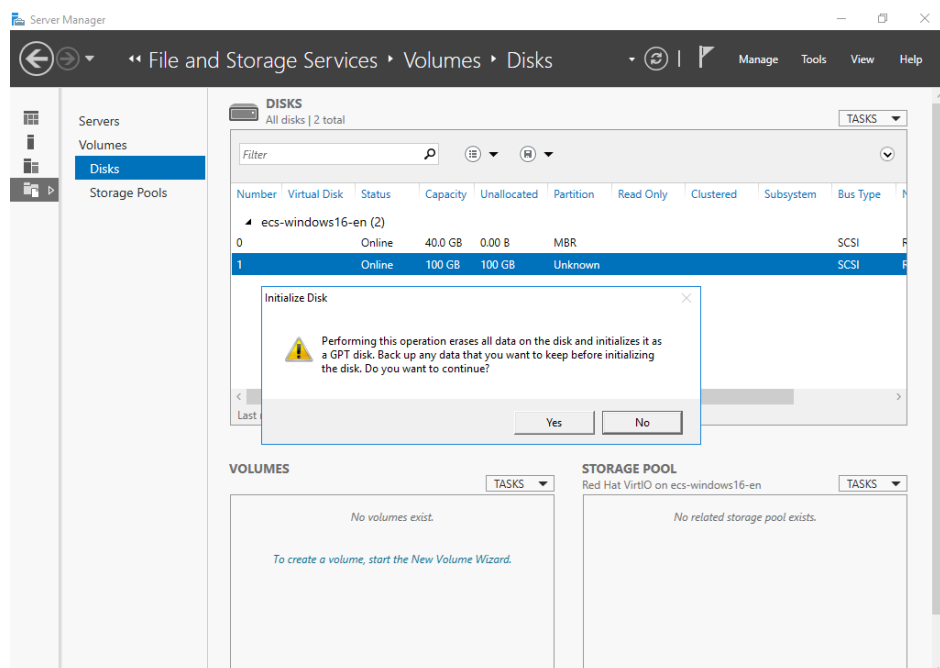
Figure 4-5 Bring online succeeded



Step 6 After the disk has been brought online, initialize the disk.

1. Right-click the new disk and choose **Initialize** from the shortcut menu. The **Initialize Disk** dialog box is displayed.

Figure 4-6 Initialize Disk (Windows 2016)




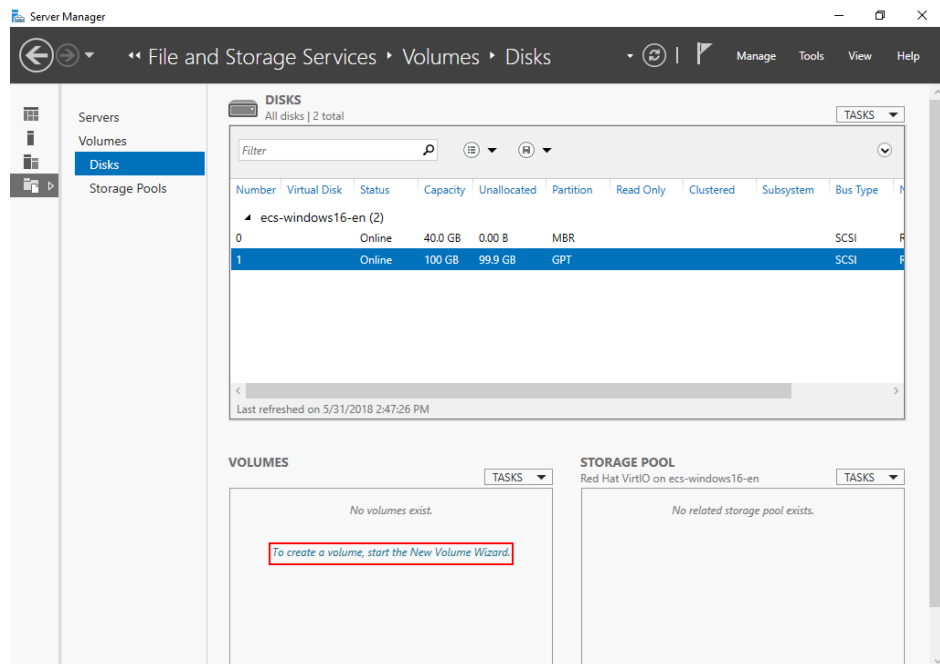
2. Click **Yes** to confirm the operation.
3. Click  in the upper area of the page to refresh the disk information. When the disk partition changes from **Unknown** to **GPT**, the initialization is complete.

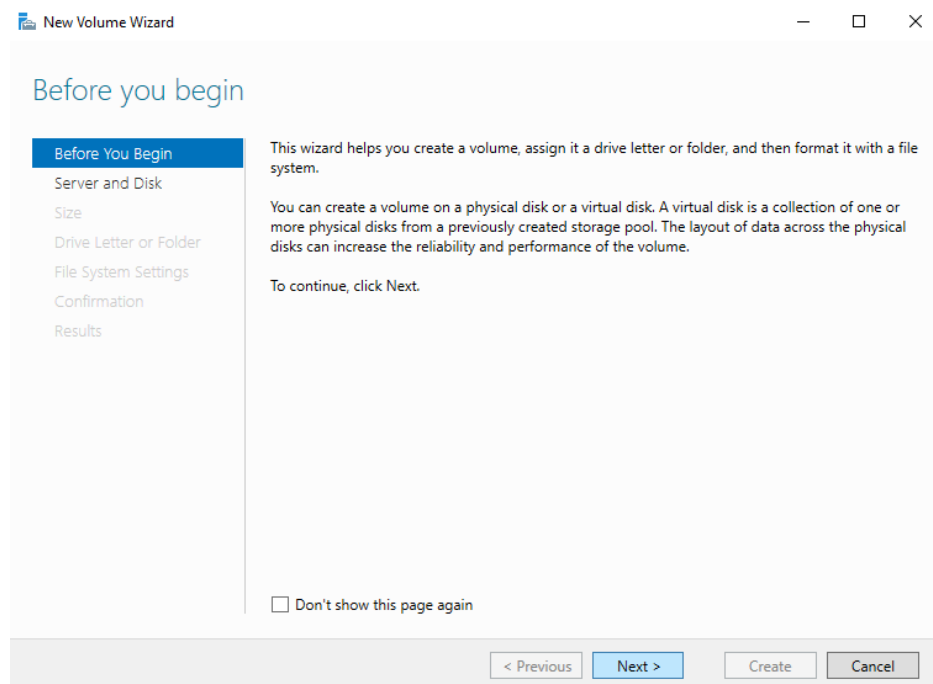
Figure 4-7 Completing initialization



Step 7 In the lower left area of the page, click **To create a volume, start the New Volume Wizard.** to create a new volume.

The **New Volume Wizard** window is displayed.

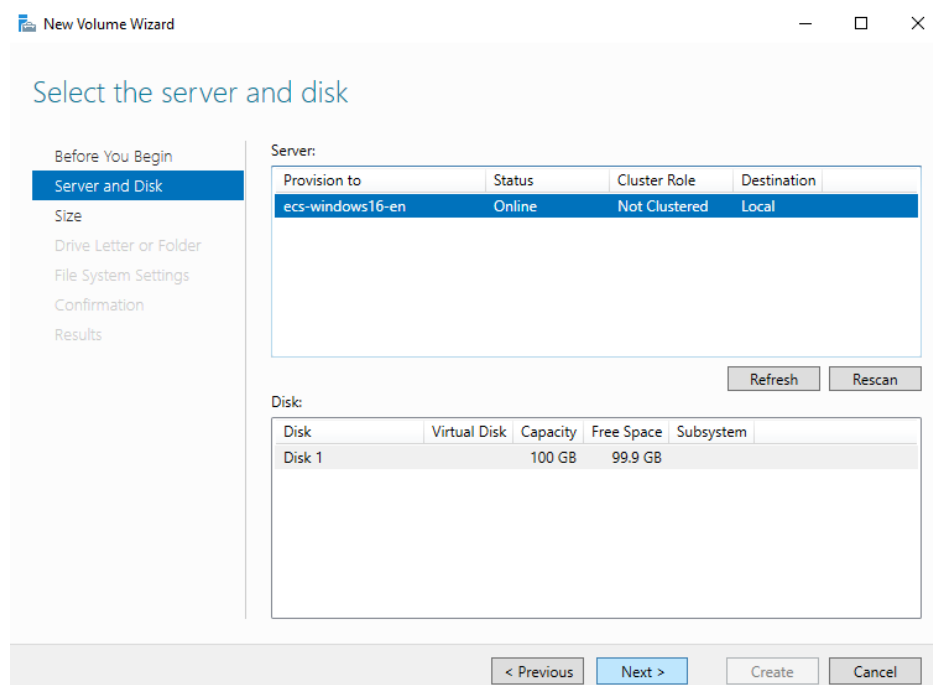
Figure 4-8 New Volume Wizard



Step 8 Follow the prompts and click **Next**.

The **Select the server and disk** page is displayed.

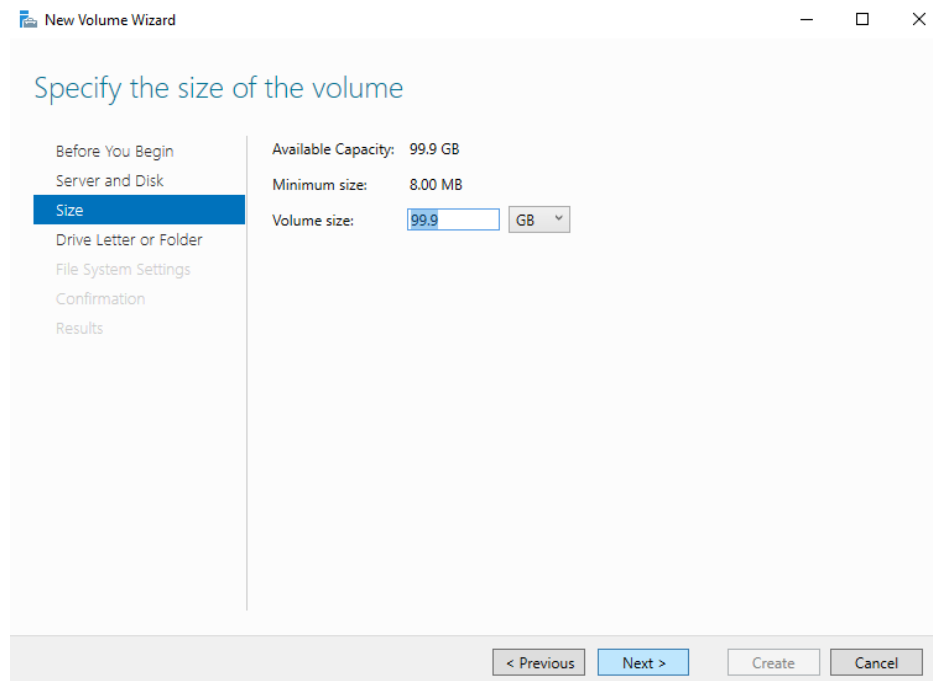
Figure 4-9 Select the server and disk



Step 9 Select the server and disk, and then click **Next**. The system selects the server to which the disk is attached by default. You can specify the server based on your requirements. In this example, the default setting is used.

The **Specify the size of the volume** page is displayed.

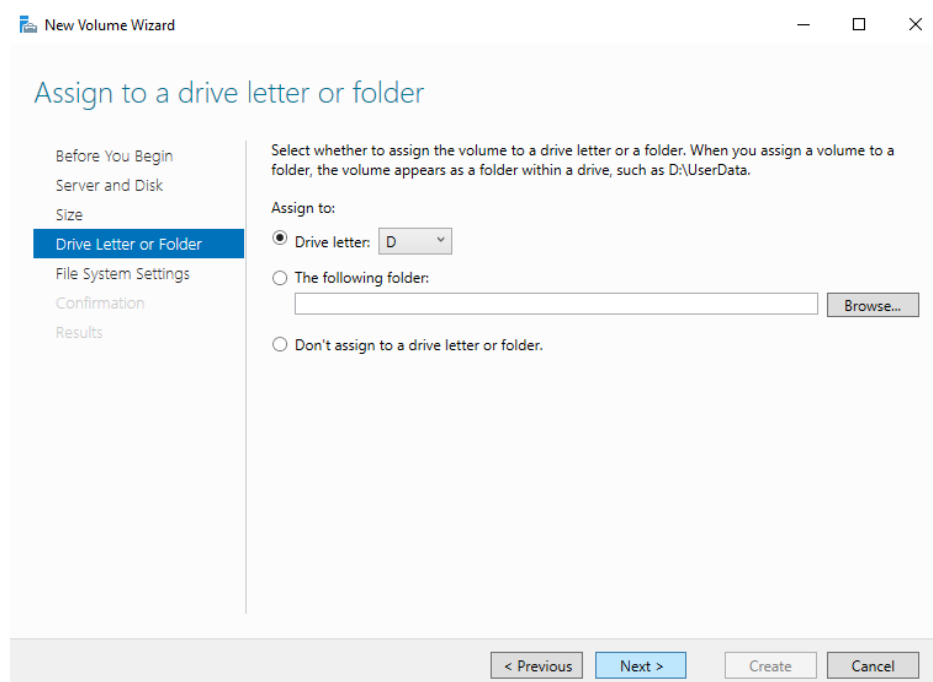
Figure 4-10 Specify Volume Size (Windows 2016)



Step 10 Specify the volume size and click **Next**. The system selects the maximum volume size by default. You can specify the volume size as required. In this example, the default setting is used.

The **Assign to a drive letter or folder** page is displayed.

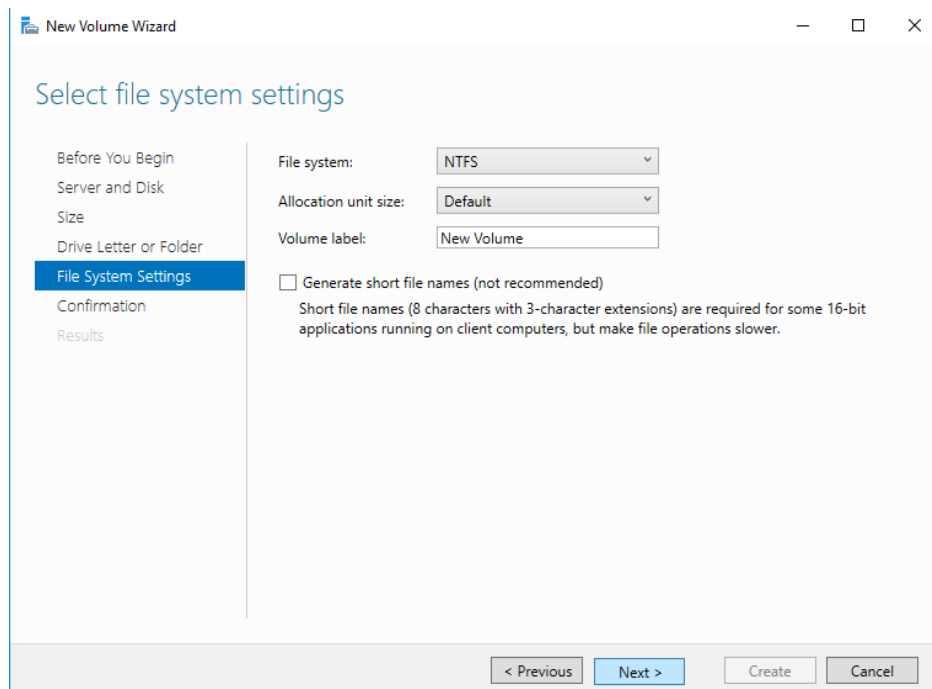
Figure 4-11 Assign to a drive letter or folder



Step 11 Assign the volume to a drive letter or folder and click **Next**. The system assigns the volume to drive letter D by default. In this example, the default setting is used.

The **Select file system settings** page is displayed.

Figure 4-12 Select file system settings



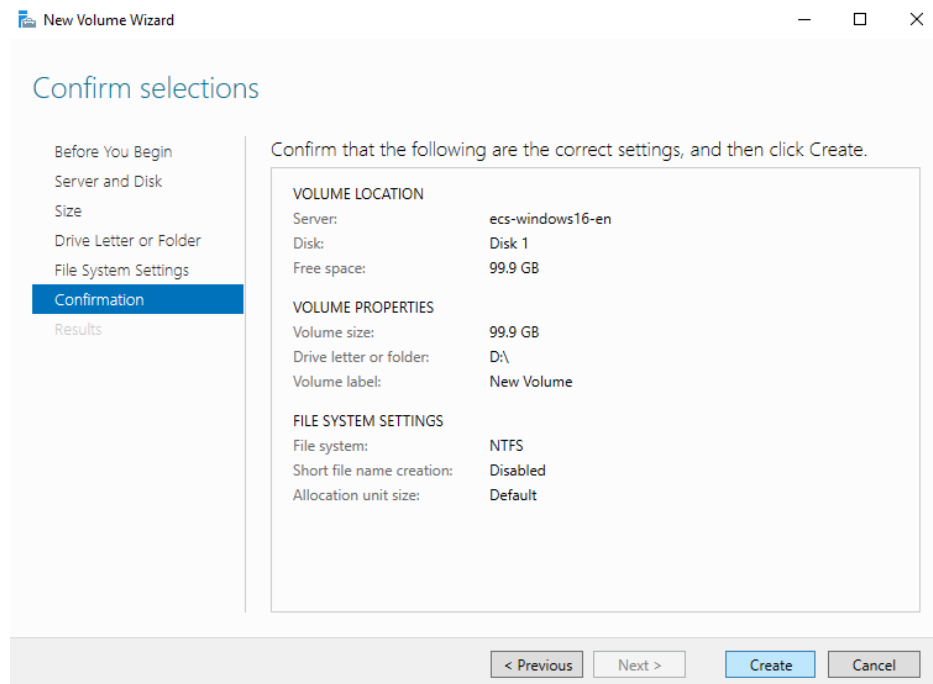
Step 12 Specify file system settings and click **Next**. The system selects the NTFS file system by default. You can specify the file system type based on the actual condition. In this example, the default setting is used.

NOTE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

The **Confirm selections** page is displayed.

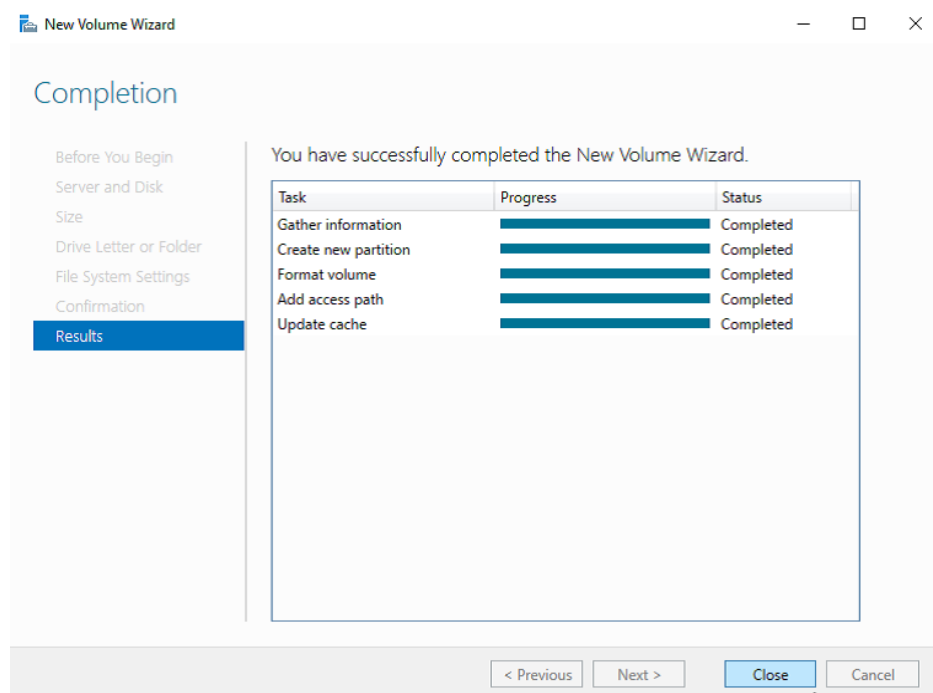
Figure 4-13 Confirm selections



Step 13 Confirm the volume location, volume properties, and file system settings. Then, click **Create** to create a volume.

If the page shown in [Figure 4-14](#) is displayed, the volume is successfully created.

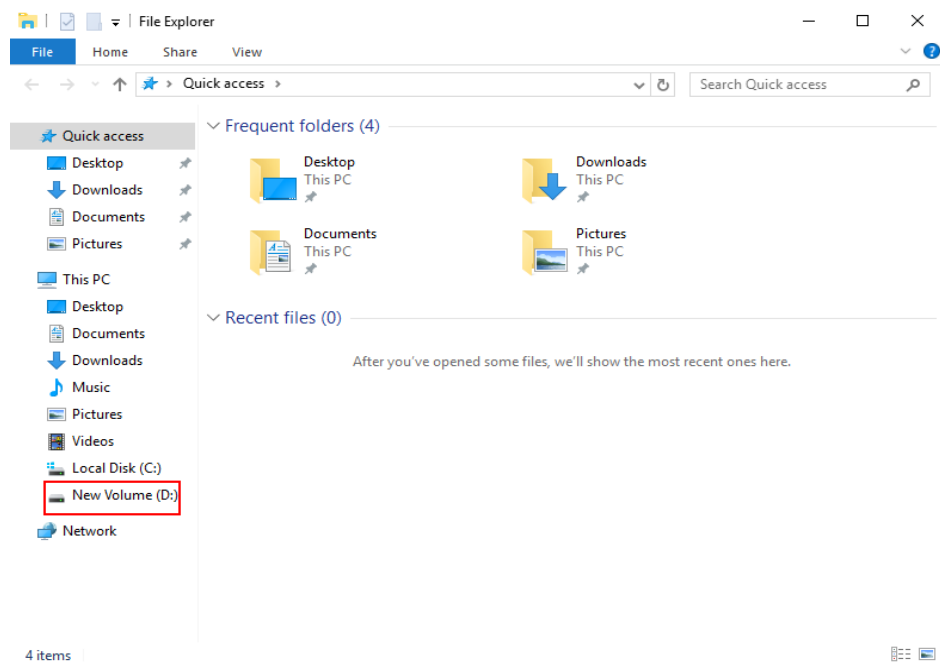
Figure 4-14 Completion



Step 14 After the volume is created, click  and check whether a new volume appears in File Explorer. In this example, New Volume (D:) is the new volume.

- If New Volume (D:) appears, the disk is successfully initialized and no further action is required.

Figure 4-15 File Explorer




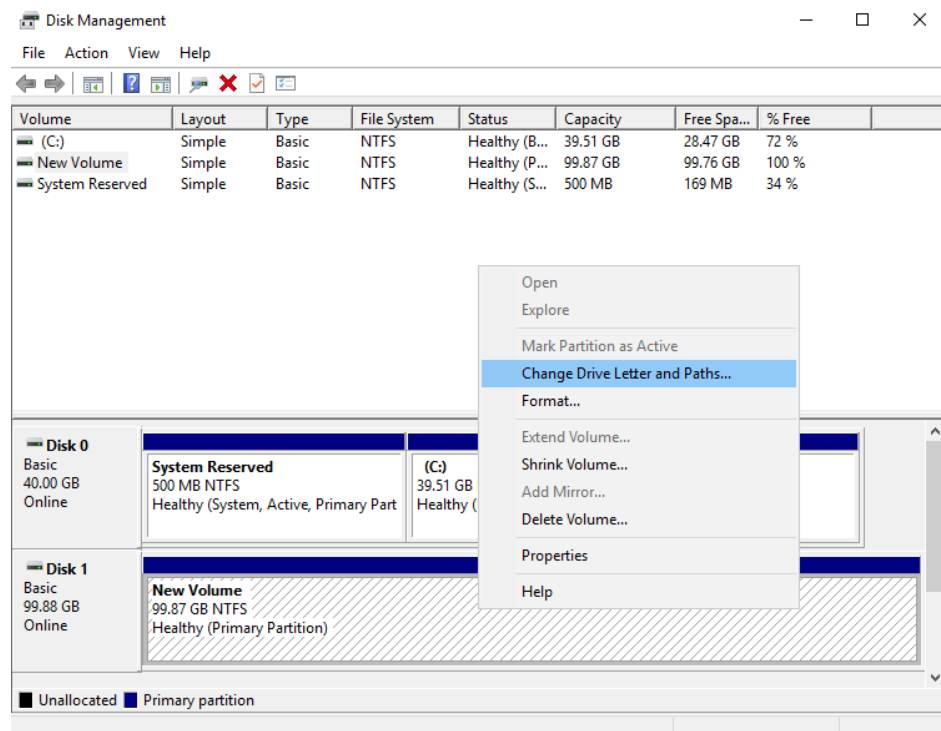
- If New Volume (D:) does not appear, perform the following operations to assign the volume to another drive letter or folder:
 - a. Click , enter **cmd**, and press **Enter**.
The **Administrator: Command Prompt** window is displayed.
 - b. Run the **diskmgmt** command.
The **Disk Management** page is displayed.

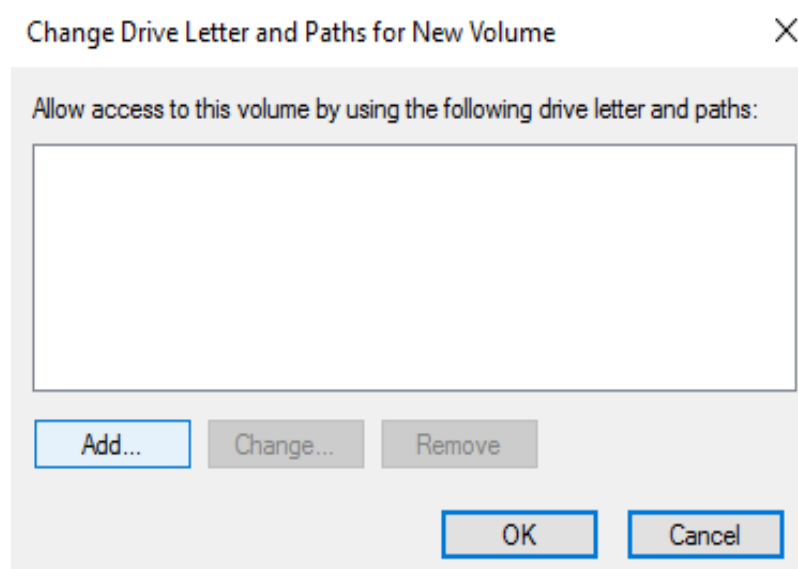
Figure 4-16 Disk Management (Windows 2016)



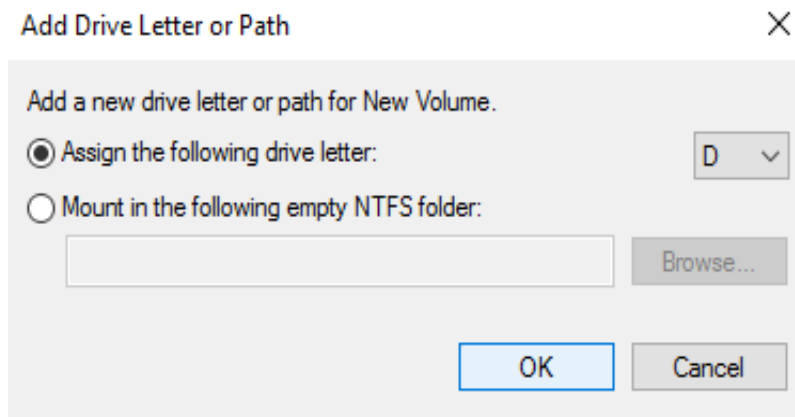
- c. In the right pane of **Disk 1**, right-click and choose **Change Drive Letter and Paths**.

The **Change Drive Letter and Paths for New Volume** dialog box is displayed.

Figure 4-17 Change Drive Letter and Paths for New Volume



- d. Click **Add**.
The **Add Drive Letter or Path** dialog box is displayed.

Figure 4-18 Add Drive Letter or Path

- e. Select **Assign the following drive letter** to re-assign the volume to a drive letter. Then, click **OK**. Drive letter D is used in this example. After assigning the drive letter, you can view New Volume (D:) in File Explorer.

 **NOTE**

The drive letter selected here must be the same as that set in [Step 11](#).

----End

4.3.3 Initializing a Linux Data Disk (fdisk)

Scenarios

This section uses CentOS 7.0 64-bit as an example.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB. In Linux OSs, if the GPT partition style is used, the fdisk partitioning tool cannot be used. The parted partitioning tool must be used. For details about disk partition styles, see [Introduction to Data Disk Initialization Scenarios and Partition Styles](#).

The method for initializing a disk varies depending on the OSs running on the BMS. This document is for reference only. For detailed operations and differences, see the product documents of the OSs running on the corresponding BMSs.

 **CAUTION**

When using an EVS disk for the first time, if you have not initialized the disk, including creating partitions and file systems, the additional capacity added to the disk in a later expansion operation may not be normally used.

Prerequisites

- You have logged in to the BMS.
- A data disk has been attached to the BMS and has not been initialized.

Create Partitions and Attach a Disk

The following example shows how to use `fdisk` to create a primary partition on a data disk that has been attached to the BMS. The default partitioning style is MBR and the default file system format is **ext4**. Mount the file system to `/mnt/sdc`, and configure automatic mounting upon system start.

Step 1 Run the following command to query information about the added data disk:

fdisk -l

Information similar to the following is displayed:

```
[root@bms-b656 test]# fdisk -l

Disk /dev/sda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000cc4ad

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1 *        2048       2050047    1024000   83  Linux
/dev/xvda2          2050048     22530047    10240000   83  Linux
/dev/xvda3          22530048     24578047     1024000   83  Linux
/dev/xvda4          24578048     83886079    29654016    5  Extended
/dev/xvda5          24580096     26628095     1024000   82  Linux swap / Solaris

Disk /dev/sdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

The command output shows that the BMS has two disks, system disk `/dev/sda` and data disk `/dev/sdb`.

Step 2 Run the following command to use `fdisk` to perform the partitioning operations for the added data disk:

fdisk Newly added data disk

For example, run the following command to use `fdisk` to perform the partitioning operations for the `/dev/sdb` data disk:

fdisk /dev/sdb

Information similar to the following is displayed:

```
[root@ecs-b656 test]# fdisk /dev/sdb
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0xb00005bd.
Command (m for help):
```

Step 3 Enter **n** and press **Enter** to create a new partition.

Information similar to the following is displayed:

```
Command (m for help): n
Partition type:
 p primary (0 primary, 0 extended, 4 free)
 e extended
```

There are two types of disk partitions:

- Choosing **p** creates a primary partition.
- Choosing **e** creates an extended partition.

Step 4 Recreate the partition with the same partition type as before. In this example a primary partition is used. Therefore, enter **p** and press **Enter** to create a primary partition.

Information similar to the following is displayed:

```
Select (default p): p
Partition number (1-4, default 1):
```

Partition number indicates the serial number of the primary partition. The value can be **1** to **4**.

Step 5 Enter the same partition number as the partition had before and press **Enter**. Primary partition number **1** is used in this example.

Information similar to the following is displayed:

```
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
```

First sector indicates the start cylinder number. The value can be **2048** to **20971519**, and the default value is **2048**.

Step 6 Ensure that you enter the same first cylinder as the partition had before. In this example, we previously noted down **2048**, so we type in **2048** here and press **Enter**.

Information similar to the following is displayed:

```
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
```

Last sector indicates the end cylinder number. The value can be **2048** to **20971519**, and the default value is **20971519**.

Step 7 In this example, select the default end cylinder number **20971519** and press **Enter**.

Information similar to the following is displayed:

```
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set
Command (m for help):
```

A primary partition has been created for a 10-GB data disk.

Step 8 Enter **p** and press **Enter** to view the details about the created partition.

Information similar to the following is displayed:

```
Command (m for help): p

Disk /dev/sdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xb00005bd
```

Device	Boot	Start	End	Blocks	Id	System
--------	------	-------	-----	--------	----	--------

```
/dev/sdb1      2048  20971519  10484736  83  Linux
```

Command (m for help):

Details about the `/dev/sdb1` partition are displayed.

Step 9 Enter **w** and press **Enter** to write the partition result into the partition table.

Information similar to the following is displayed:

```
Command (m for help): w
```

```
The partition table has been altered!
```

```
Calling ioctl() to re-read partition table.  
Syncing disks.
```

The partition is successfully created.

NOTE

In case that you want to discard the changes made before, you can exit `fdisk` by entering **q**.

Step 10 Run the following command to synchronize the new partition table to the OS:

```
partprobe
```

Step 11 Run the following command to set the format for the file system of the newly created partition:

```
mkfs -t File system format /dev/sdb1
```

For example, run the following command to set the **ext4** file system for the `/dev/sdb1` partition:

```
mkfs -t ext4 /dev/sdb1
```

Information similar to the following is displayed:

```
[root@bms-b656 test]# mkfs -t ext4 /dev/sdb1  
mke2fs 1.42.9 (28-Dec-2013)  
Filesystem label=  
OS type: Linux  
Block size=4096 (log=2)  
Fragment size=4096 (log=2)  
Stride=0 blocks, Stripe width=0 blocks  
655360 inodes, 2621184 blocks  
131059 blocks (5.00%) reserved for the super user  
First data block=0  
Maximum filesystem blocks=2151677952  
80 block groups  
32768 blocks per group, 32768 fragments per group  
8192 inodes per group  
Superblock backups stored on blocks:  
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632  
  
Allocating group tables: done  
Writing inode tables: done  
Creating journal (32768 blocks): done  
Writing superblocks and filesystem accounting information: done
```

The formatting takes a period of time. Observe the system running status and do not exit.

NOTE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Run the following command to create a mount point:

```
mkdir Mount point
```

For example, run the following command to create the **/mnt/sdc** mount point:

```
mkdir /mnt/sdc
```

Step 13 Run the following command to mount the new partition on the mount point created in [Step 12](#):

```
mount /dev/sdb1 Mount point
```

For example, run the following command to mount the newly created partition on **/mnt/sdc**:

```
mount /dev/sdb1 /mnt/sdc
```

Step 14 Run the following command to view the mount result:

```
df -TH
```

Information similar to the following is displayed:

```
[root@bms-b656 test]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda2      xfs       11G   7.4G 3.2G  71% /
devtmpfs        devtmpfs  4.1G   0    4.1G   0% /dev
tmpfs           tmpfs     4.1G   82k  4.1G   1% /dev/shm
tmpfs           tmpfs     4.1G   9.2M  4.1G   1% /run
tmpfs           tmpfs     4.1G   0    4.1G   0% /sys/fs/cgroup
/dev/sda3       xfs       1.1G   39M   1.1G   4% /home
/dev/sda1       xfs       1.1G  131M  915M  13% /boot
/dev/sdb1       ext4      11G   38M   9.9G   1% /mnt/sdc
```

The newly created **/dev/sdb1** is mounted on **/mnt/sdc**.

----End

Set Automatic Disk Attachment Upon BMS Start

To automatically attach a disk when a BMS starts, you should not specify its partition, for example **/dev/sdb1**, in **/etc/fstab**. This is because the sequence of cloud devices may change during the server start or stop process, for example, from **/dev/sdb** to **/dev/sdc**. You are advised to use the universally unique identifier (UUID) in **/etc/fstab** to automatically attach a disk at system start.

NOTE

The universally unique identifier (UUID) is the unique character string for disk partitions in a Linux system.

Step 1 Run the following command to query the partition UUID:

```
blkid Disk partition
```

For example, run the following command to query the UUID of **/dev/sdb1**:

```
blkid /dev/sdb1
```

Information similar to the following is displayed:

```
[root@bms-b656 test]# blkid /dev/sdb1
/dev/sdb1: UUID="1851e23f-1c57-40ab-86bb-5fc5fc606ffa" TYPE="ext4"
```

The UUID of `/dev/sdb1` is displayed.

Step 2 Run the following command to open the `fstab` file using the vi editor:

```
vi /etc/fstab
```

Step 3 Press `i` to enter the editing mode.

Step 4 Move the cursor to the end of the file and press `Enter`. Then add the following information:

```
UUID=1851e23f-1c57-40ab-86bb-5fc5fc606ffa /mnt/sdc ext4 defaults 0 2
```

Step 5 Press `Esc`, enter `:wq`, and press `Enter`.

The system saves the configurations and exits the vi editor.

----End

4.3.4 Initializing a Linux Data Disk (parted)

Scenarios

This section uses CentOS 7.0 64-bit as an example to describe how to initialize a data disk attached to a BMS running Linux and use parted to partition the data disk.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB. In Linux OSs, if the GPT partition style is used, the fdisk partitioning tool cannot be used. The parted partitioning tool must be used. For details about disk partition styles, see [Introduction to Data Disk Initialization Scenarios and Partition Styles](#).

The method for initializing a disk varies depending on the OSs running on the BMS. This document is for reference only. For detailed operations and differences, see the product documents of the OSs running on the corresponding BMSs.

CAUTION

When using an EVS disk for the first time, if you have not initialized the disk, including creating partitions and file systems, the additional capacity added to the disk in a later expansion operation may not be normally used.

Prerequisites

- You have logged in to the BMS.
- A data disk has been attached to the BMS and has not been initialized.

Creating Partitions and Attaching a Disk

The following example shows how to use parted to create a partition on a new data disk that has been attached to the BMS. The default partitioning style is GPT and the default file system format is `ext4`. Mount the file system to `/mnt/sdc`, and configure automatic mounting upon system start.

Step 1 Run the following command to query information about the added data disk:

lsblk

Information similar to the following is displayed:

```
[root@bms-centos-70 linux]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 202:0 0 40G 0 disk
├─sda1 202:1 0 4G 0 part [SWAP]
└─sda2 202:2 0 36G 0 part /
sdb 202:16 0 10G 0 disk
```

The command output shows that the BMS has two disks, system disk **/dev/sda** and data disk **/dev/sdb**.

Step 2 Run the following command to enter parted to partition the added data disk:

parted *Added data disk*

For example, run the following command to use fdisk to perform the partitioning operations for the **/dev/sdb** data disk:

parted /dev/sdb

Information similar to the following is displayed:

```
[root@bms-centos-70 linux]# parted /dev/sdb
GNU Parted 3.1
Using /dev/sdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
```

Step 3 Enter **p** and press **Enter** to view the current disk partition style.

Information similar to the following is displayed:

```
(parted) p
Error: /dev/sdb: unrecognised disk label
Model: Xen Virtual Block Device (xvd)
Disk /dev/sdb: 10.7GB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
```

In the command output, the **Partition Table** value is **unknown**, indicating that the disk partition style is unknown.

Step 4 Run the following command to set the disk partition style:

mklabel *Disk partition style*

For example, run the following command to set the partition style to GPT: (Disk partition styles include MBR and GPT.)

mklabel gpt

CAUTION

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the original data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 5 Enter **p** and press **Enter** to view the disk partition style.

Information similar to the following is displayed:

```
(parted) mklabel gpt
(parted) p
Model: Xen Virtual Block Device (xvd)
Disk /dev/sdb: 20971520s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number Start End Size File system Name Flags
```

Step 6 Enter **unit s** and press **Enter** to set the measurement unit of the disk to sector numbers.

Step 7 Enter **mkpart opt 2048s 100%** and press **Enter**.

In this example, one partition is created for the added data disk. Variable *2048s* indicates the disk start capacity, and variable *100%* indicates the disk end capacity. The two values are used for reference only. You can determine the number of partitions and the partition capacity based on your service requirements.

Information similar to the following is displayed:

```
(parted) mkpart opt 2048s 100%
Warning: The resulting partition is not properly aligned for best performance.
Ignore/Cancel? Ignore
```

If the preceding warning message is displayed, enter **Ignore** to ignore the performance warning.

Step 8 Enter **p** and press **Enter** to view the details about the created partition.

Information similar to the following is displayed:

```
(parted) p
Model: Xen Virtual Block Device (xvd)
Disk /dev/sdb: 20971520s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number Start End Size File system Name Flags
1 2048s 20969471s 20967424s opt
```

Details about the **/dev/sdb1** partition are displayed.

Step 9 Enter **q** and press **Enter** to exit parted.

Step 10 Run the following command to view the disk partition information:

lsblk

Information similar to the following is displayed:

```
[root@bms-centos-70 linux]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda  202:0  0  40G  0 disk
├─sda1 202:1  0   4G  0 part [SWAP]
├─sda2 202:2  0  36G  0 part /
sdb  202:16 0 100G  0 disk
├─sdb1 202:17 0 100G  0 part
```

In the command output, **/dev/sdb1** is the partition you created.

Step 11 Run the following command to set the format for the file system of the newly created partition:

```
mkfs -t File system format /dev/sdb1
```

For example, run the following command to set the **ext4** file system for the **/dev/xvdb1** partition:

```
mkfs -t ext4 /dev/sdb1
```

Information similar to the following is displayed:

```
[root@bms-centos-70 linux]# mkfs -t ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2620928 blocks
131046 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677925
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

The formatting takes a period of time. Observe the system running status and do not exit.

NOTE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Run the following command to create a mount point:

```
mkdir Mount point
```

For example, run the following command to create the **/mnt/sdc** mount point:

```
mkdir /mnt/sdc
```

Step 13 Run the following command to mount the new partition on the created mount point:

```
mount /dev/sdb1 Mount point
```

For example, run the following command to mount the newly created partition on **/mnt/sdc**:

```
mount /dev/sdb1 /mnt/sdc
```

Step 14 Run the following command to view the mount result:

```
df -TH
```

Information similar to the following is displayed:

```
[root@bms-centos-70 linux]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/sda2       xfs       39G   4.0G  35G   11% /
devtmpfs        devtmpfs  946M   0  946M   0% /dev
tmpfs           tmpfs     954M   0  954M   0% /dev/shm
tmpfs           tmpfs     954M   9.1M  945M   1% /run
tmpfs           tmpfs     954M   0  954M   0% /sys/fs/cgroup
/dev/sdb1       ext4      11G   38M  101G   1% /mnt/sdc
```

The newly created **/dev/sdb1** is mounted on **/mnt/sdc**.

----End

Set Automatic Disk Attachment Upon BMS Start

To automatically attach a disk when a BMS starts, you should not specify its partition, for example **/dev/sdb1**, in **/etc/fstab**. This is because the sequence of cloud devices may change during the server start or stop process, for example, from **/dev/sdb** to **/dev/sdc**. You are advised to use the universally unique identifier (UUID) in **/etc/fstab** to automatically attach a disk at system start.

NOTE

The universally unique identifier (UUID) is the unique character string for disk partitions in a Linux system.

Step 1 Run the following command to query the partition UUID:

```
blkid Disk partition
```

For example, run the following command to query the UUID of **/dev/sdb1**:

```
blkid /dev/sdb1
```

Information similar to the following is displayed:

```
[root@bms-b656 test]# blkid /dev/sdb1
/dev/sdb1: UUID="1851e23f-1c57-40ab-86bb-5fc5fc606ffa" TYPE="ext4"
```

The UUID of **/dev/sdb1** is displayed.

Step 2 Run the following command to open the **fstab** file using the vi editor:

```
vi /etc/fstab
```

Step 3 Press **i** to enter the editing mode.

Step 4 Move the cursor to the end of the file and press **Enter**. Then add the following information:

```
UUID=1851e23f-1c57-40ab-86bb-5fc5fc606ffa /mnt/sdc ext4 defaults 0 2
```

Step 5 Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

----End

4.3.5 Initializing a Windows Data Disk Greater Than 2 TB (Windows Server 2012)

Scenarios

This section uses Windows Server 2012 R2 Standard 64bit to describe how to initialize a data disk whose capacity is greater than 2 TB. In the following operations, the capacity of the example disk is 3 TB.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB. For details about disk partition styles, see [Introduction to Data Disk Initialization Scenarios and Partition Styles](#).

The method for initializing a disk varies depending on the OSs running on the BMS. This document is for reference only. For detailed operations and differences, see the product documents of the OSs running on the corresponding BMSs.

CAUTION

When using an EVS disk for the first time, if you have not initialized the disk, including creating partitions and file systems, the additional capacity added to the disk in a later expansion operation may not be normally used.

Prerequisites

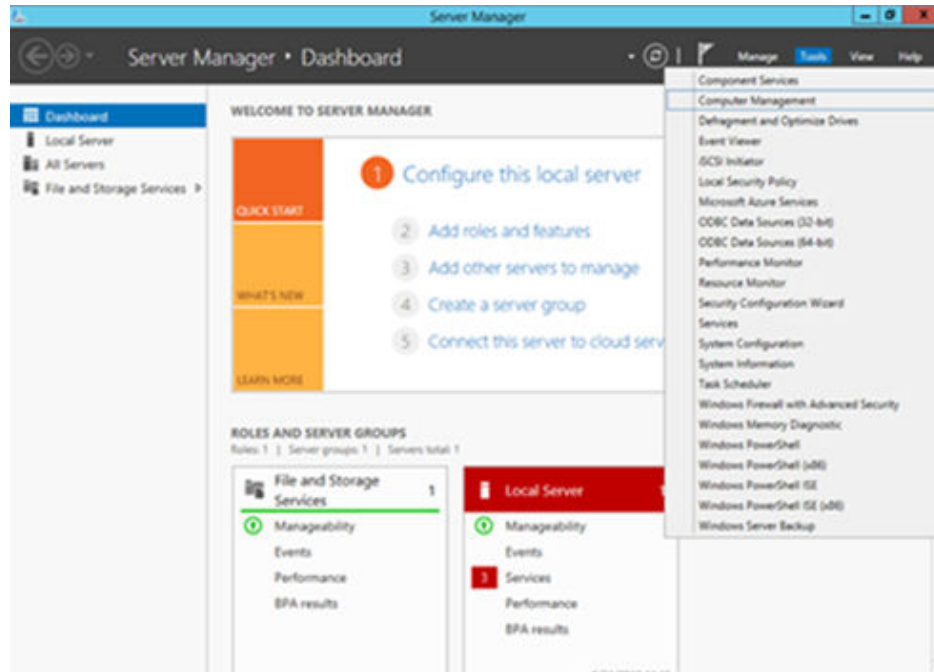
- You have logged in to the BMS.
- A data disk has been attached to the BMS and has not been initialized.

Procedure

Step 1 On the BMS desktop, click  in the lower left corner.

The **Server Manager** window is displayed.

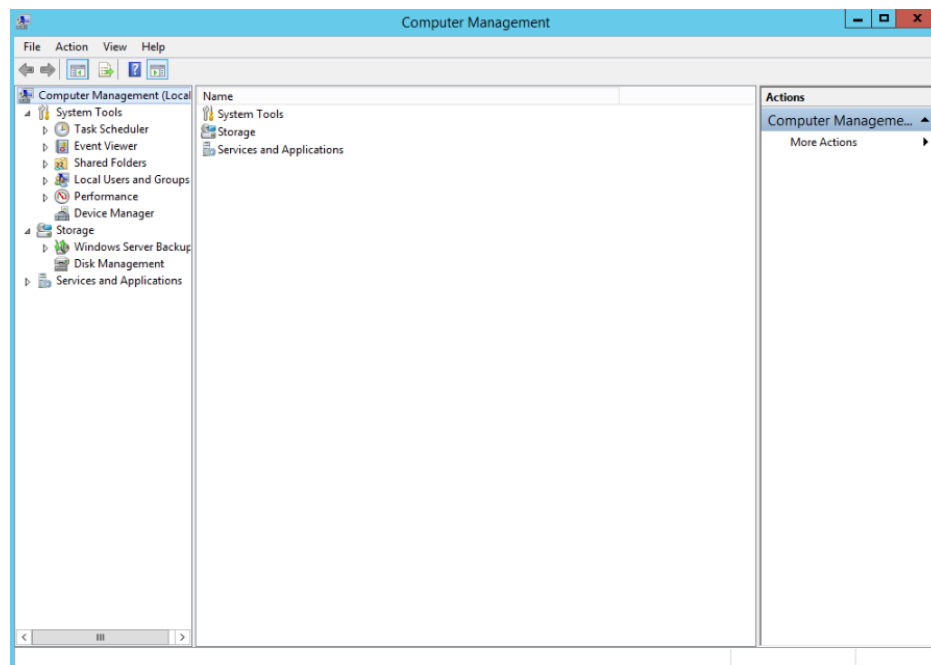
Figure 4-19 Server Manager (Windows 2012)



Step 2 In the upper right corner of the **Server Manager** page, choose **Tools > Computer Management**.

The **Computer Management** page is displayed.

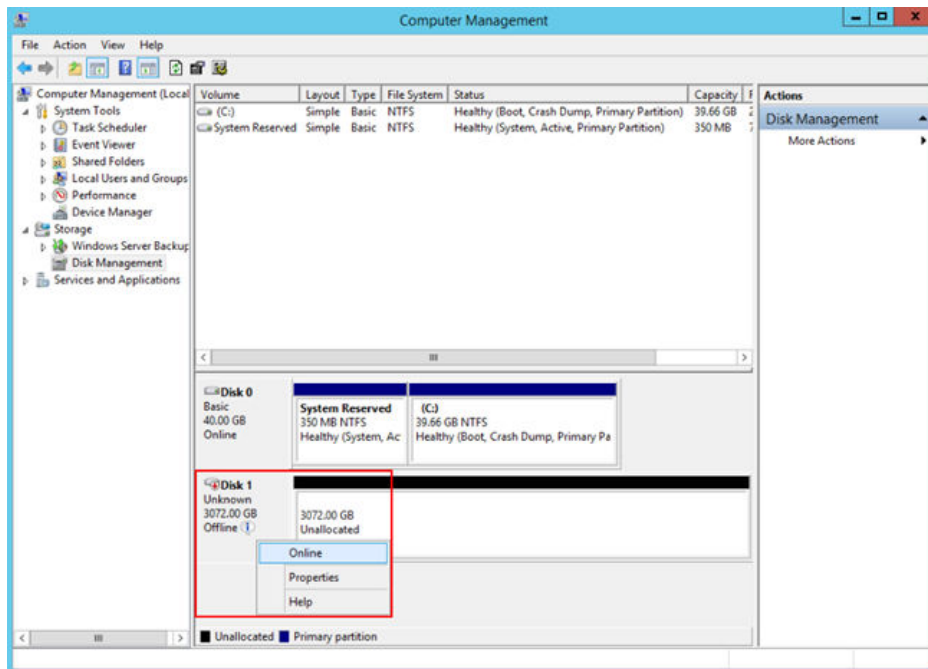
Figure 4-20 Computer Management



Step 3 Choose **Storage > Disk Management**.

The disk list is displayed.

Figure 4-21 Disk list

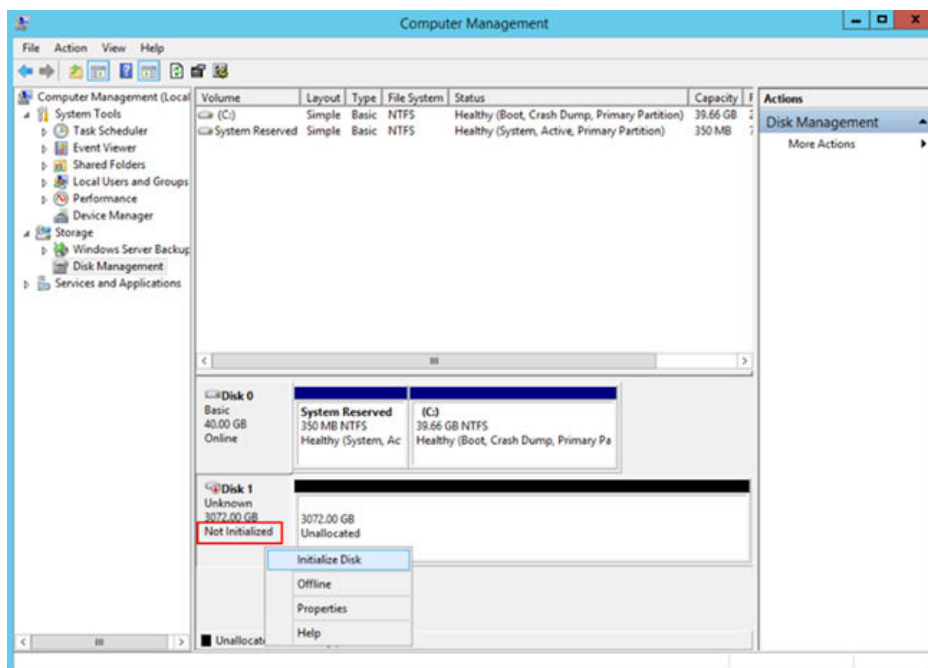


Step 4 Disks are listed in the right pane. If the new disk is in the offline state, bring it online before initialize it.

In the **Disk 1** area, right-click and choose **Online** from the shortcut menu.

When the Disk 1 status changes from **Offline** to **Not Initialized**, the disk has been brought online.

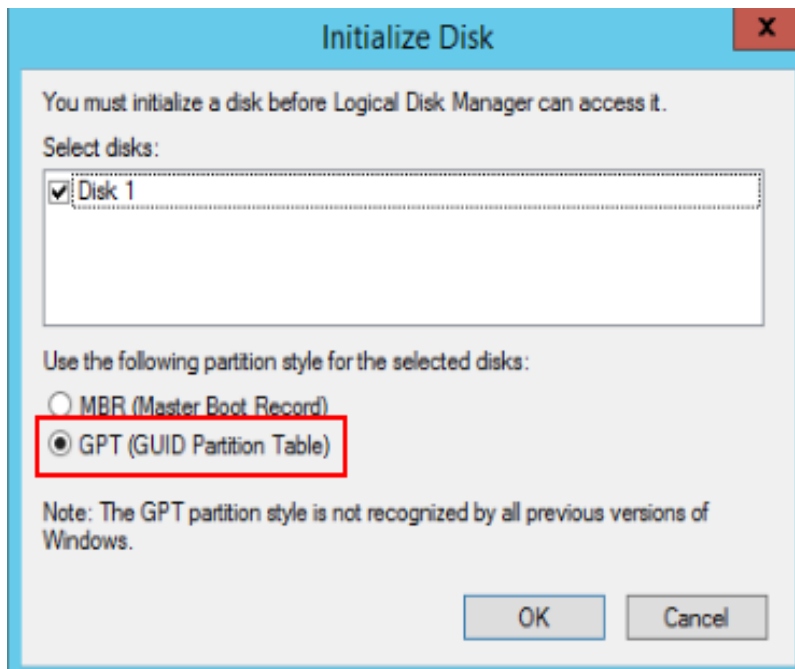
Figure 4-22 Bring online succeeded (Windows 2012)



Step 5 In the **Disk 1** area, right-click and choose **Initialize Disk** from the shortcut menu.

The **Initialize Disk** dialog box is displayed.

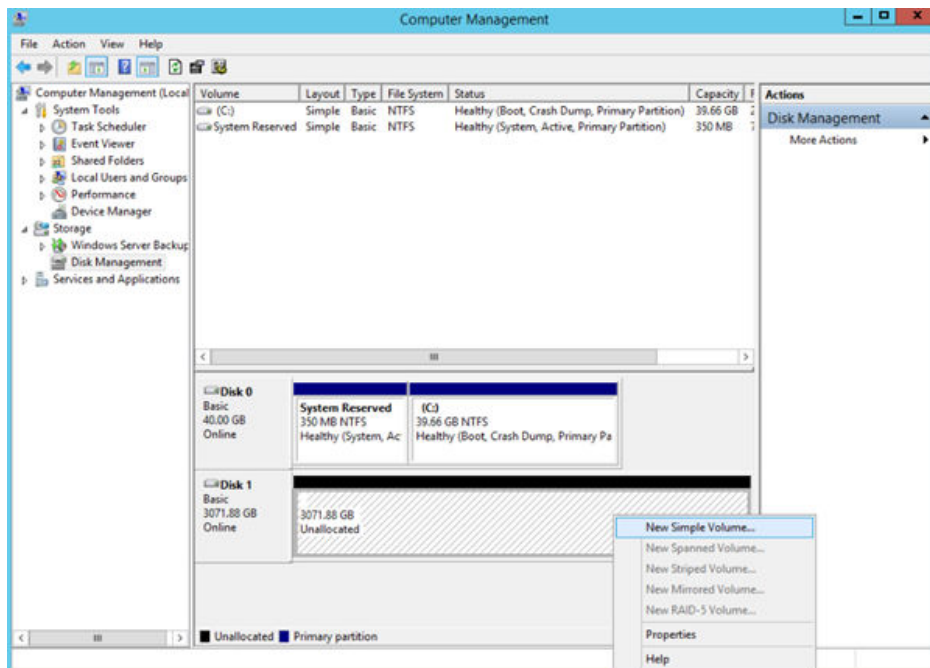
Figure 4-23 Initialize Disk (Windows 2012)



Step 6 The **Initialize Disk** dialog box displays the disk to be initialized. If the disk capacity is greater than 2 TB, select **GPT (GUID Partition Table)** and click **OK**.

The **Computer Management** page is displayed.

Figure 4-24 Computer Management (Windows 2012)



 **CAUTION**

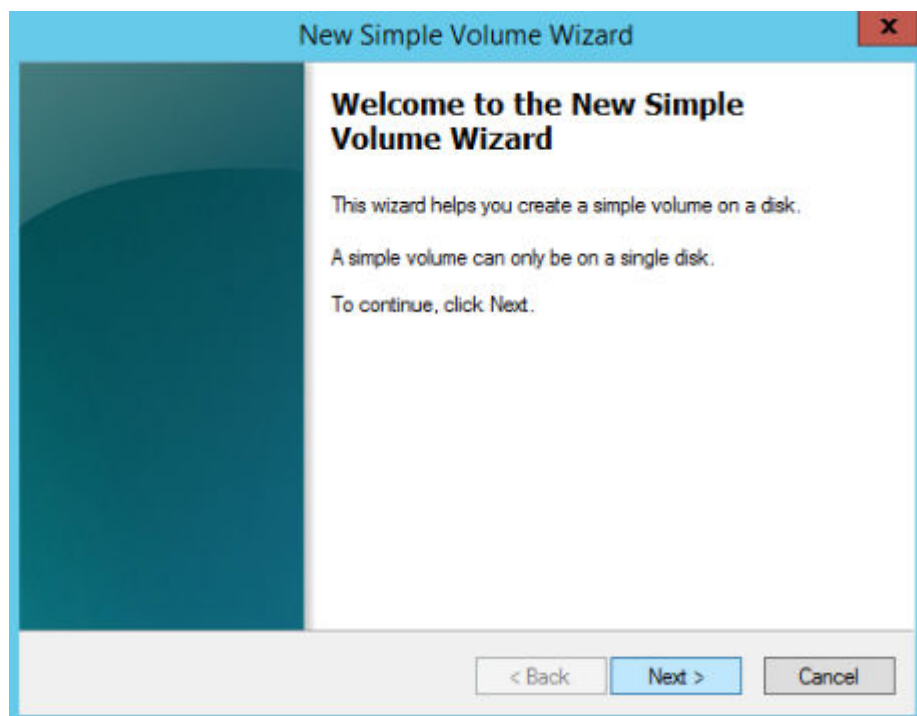
The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the original data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 7 Right-click at the unallocated disk space and choose **New Simple Volume** from the shortcut menu.

The **New Simple Volume Wizard** window is displayed.

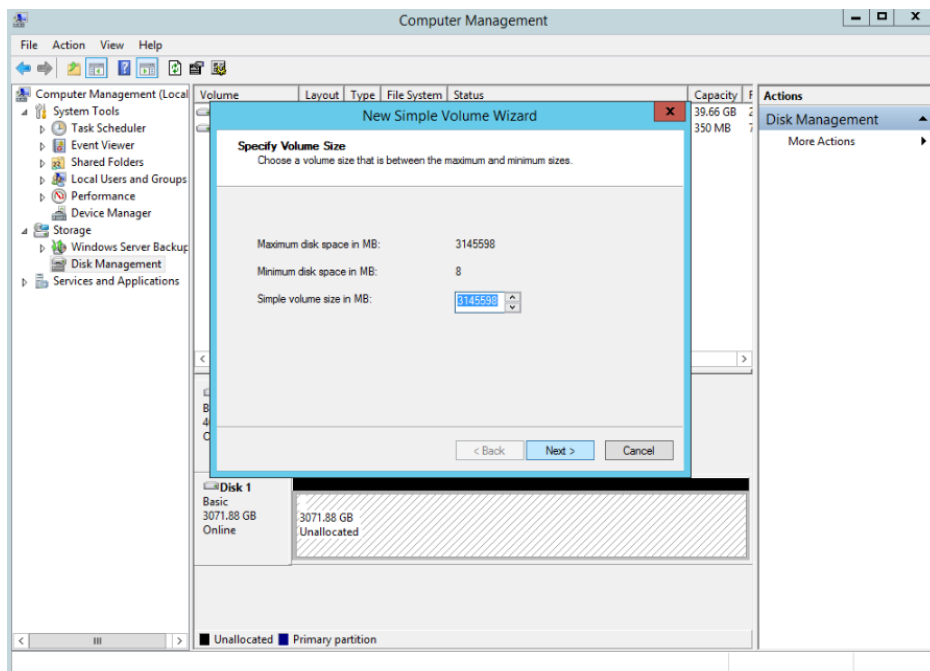
Figure 4-25 New Simple Volume Wizard (Windows 2012)



Step 8 Follow the prompts and click **Next**.

The **Specify Volume Size** page is displayed.

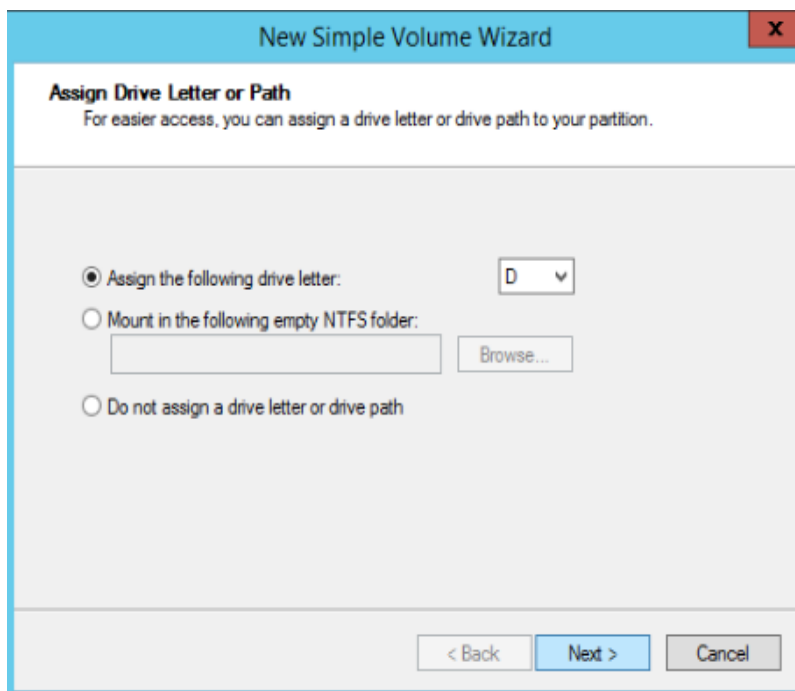
Figure 4-26 Specify Volume Size (Windows 2012)



Step 9 Specify the volume size and click **Next**. The system selects the maximum volume size by default. You can specify the volume size as required. In this example, the default setting is used.

The **Assign Drive Letter or Path** page is displayed.

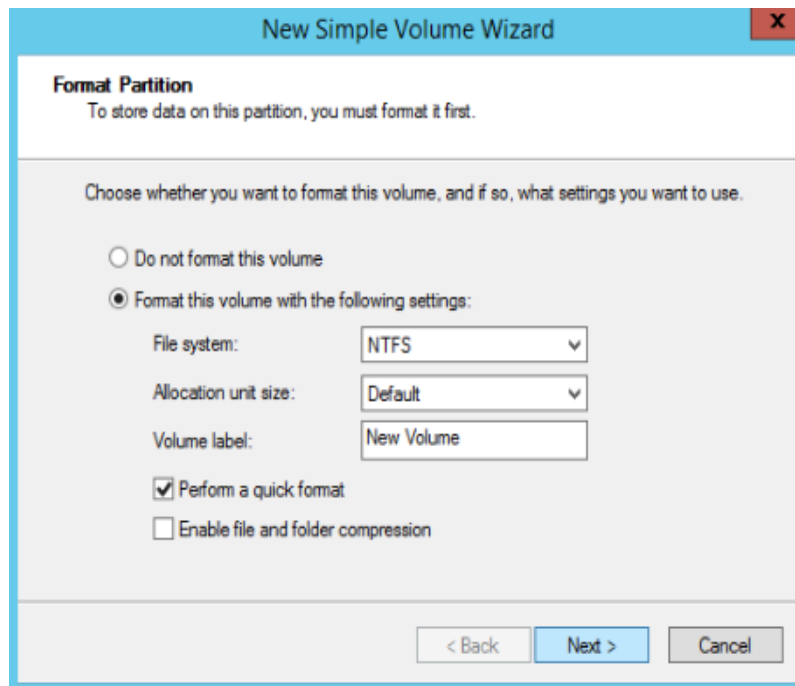
Figure 4-27 Assign Driver Letter or Path (Windows 2012)



Step 10 Assign the volume to a drive letter or folder and click **Next**. The system assigns the volume to drive letter D by default. In this example, the default setting is used.

The **Format Partition** page is displayed.

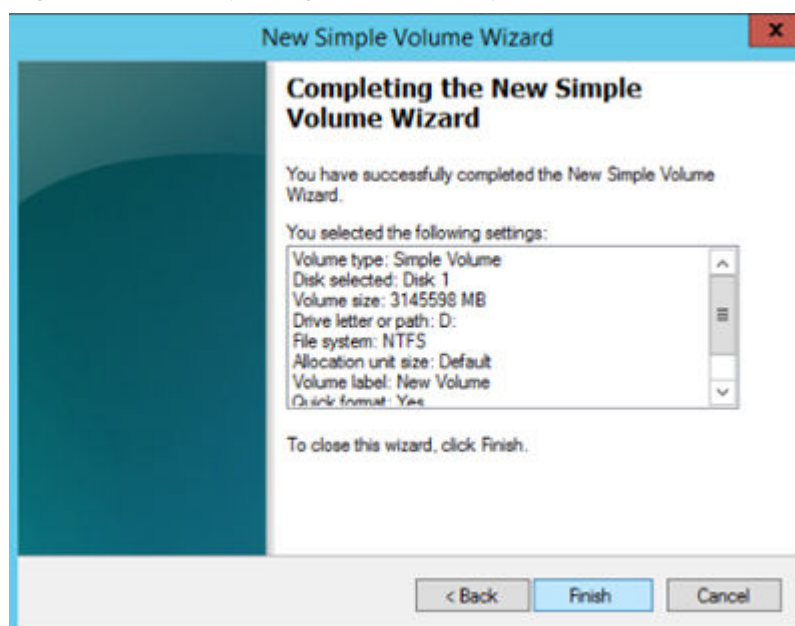
Figure 4-28 Format Partition (Windows 2012)



Step 11 Specify format settings and click **Next**. The system selects the NTFS file system by default. You can specify the file system type based on the actual condition. In this example, the default setting is used.

The **Completing the New Simple Volume Wizard** page is displayed.

Figure 4-29 Completing the New Simple Volume Wizard (Windows 2012)



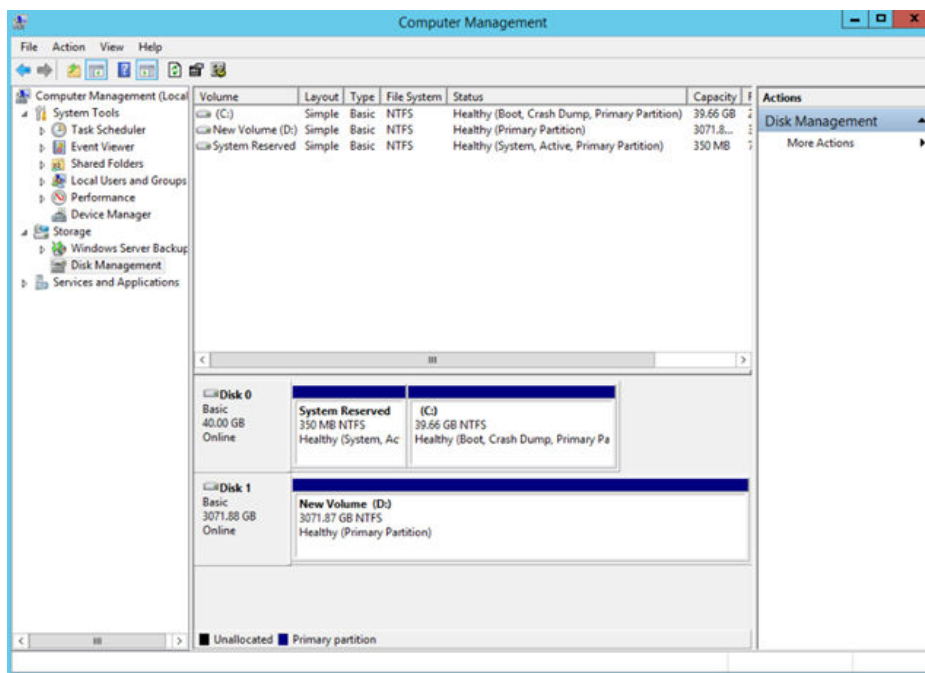
 **NOTE**

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Click **Finish**.

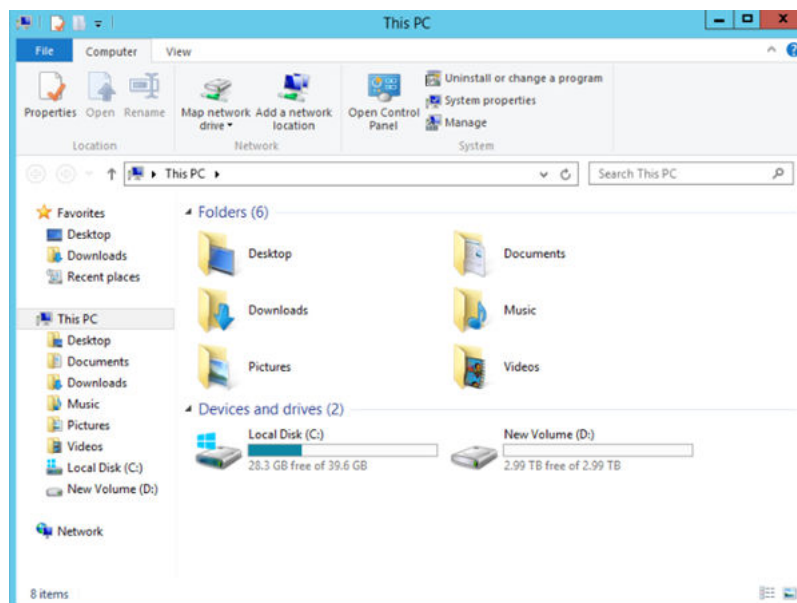
Wait for the initialization to complete. When the volume status changes to **Healthy**, the initialization has finished successfully, as shown in [Figure 4-30](#).

Figure 4-30 Disk initialization succeeded (Windows 2012)



Step 13 After the volume is created, click  and check whether a new volume appears in **This PC**. In this example, New Volume (D:) is the new volume.

If New Volume (D:) appears, the disk is successfully initialized and no further action is required.

Figure 4-31 This PC (Windows 12)

----End

4.3.6 Initializing a Linux Data Disk Greater Than 2 TB (parted)

Scenarios

This section uses CentOS 7.4 64bit to describe how to use parted to initialize a data disk whose capacity is greater than 2 TB. In the following operations, the capacity of the example disk is 3 TB.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB. In Linux OSs, if the GPT partition style is used, the fdisk partitioning tool cannot be used. The parted partitioning tool must be used. For details about disk partition styles, see [Introduction to Data Disk Initialization Scenarios and Partition Styles](#).

The method for initializing a disk varies depending on the OSs running on the BMS. This document is for reference only. For detailed operations and differences, see the product documents of the OSs running on the corresponding BMSs.

CAUTION

When using an EVS disk for the first time, if you have not initialized the disk, including creating partitions and file systems, the additional capacity added to the disk in a later expansion operation may not be normally used.

Prerequisites

- You have logged in to the BMS.
- A data disk has been attached to the BMS and has not been initialized.

Creating Partitions and Attaching a Disk

The following example shows how to use parted to create a partition on a new data disk that has been attached to the BMS. The default partitioning style is GPT and the default file system format is **ext4**. Mount the file system to **/mnt/sdc**, and configure automatic mounting upon system start.

Step 1 Run the following command to query information about the added data disk:

lsblk

Information similar to the following is displayed:

```
[root@bms-centos74 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda  253:0  0 40G  0 disk
├─vda1 253:1  0  1G  0 part /boot
├─vda2 253:2  0 39G  0 part /
└─vdb  253:16  0  3T  0 disk
```

The command output shows that the BMS has two disks, system disk **/dev/vda** and data disk **/dev/vdb**.

Step 2 Run the following command to enter parted to partition the added data disk:

parted *Added data disk*

In this example, **/dev/vdb** is the newly added data disk.

parted **/dev/vdb**

Information similar to the following is displayed:

```
[root@bms-centos74 ~]# parted /dev/vdb
GNU Parted 3.1
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

Step 3 Enter **p** and press **Enter** to view the current disk partition style.

Information similar to the following is displayed:

```
(parted) p
Error: /dev/vdb: unrecognised disk label
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 3299GB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
(parted)
```

In the command output, the **Partition Table** value is **unknown**, indicating that the disk partition style is unknown.

Step 4 Run the following command to set the disk partition style:

mklabel *Disk partition style*

The disk partition style can be MBR or GPT. If the disk capacity is greater than 2 TB, choose the GPT partition style.

mklabel **gpt**

CAUTION

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the original data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 5 Enter **p** and press **Enter** to view the disk partition style.

Information similar to the following is displayed:

```
(parted) mklabel gpt
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 3299GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
(parted)
```

Step 6 Enter **unit s** and press **Enter** to set the measurement unit of the disk to sector numbers.

Step 7 Enter **mkpart opt 2048s 100%** and press **Enter**.

In this example, one partition is created for the added data disk. Variable *2048s* indicates the disk start capacity, and variable *100%* indicates the disk end capacity. The two values are used for reference only. You can determine the number of partitions and the partition capacity based on your service requirements.

Information similar to the following is displayed:

```
(parted) mkpart opt 2048s 100%
Warning: The resulting partition is not properly aligned for best performance.
Ignore/Cancel? Cancel
```

If the preceding warning message is displayed, enter **Cancel** to stop the partitioning. Then, find the first sector with the best disk performance and use that value to partition the disk. In this example, the first sector with the best disk performance is **2048s**. Therefore, the system does not display the warning message.

Step 8 Enter **p** and press **Enter** to view the details about the created partition.

Information similar to the following is displayed:

```
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 6442450944s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
1      2048s 6442448895s 6442446848s  opt
```

Details about the **dev/vdb1** partition are displayed.

Step 9 Enter **q** and press **Enter** to exit parted.

Step 10 Run the following command to view the disk partition information:

lsblk

Information similar to the following is displayed:

```
[root@bms-centos74 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 253:0 0 40G 0 disk
├─vda1 253:1 0 1G 0 part /boot
├─vda2 253:2 0 39G 0 part /
vdb 253:16 0 3T 0 disk
├─vdb1 253:17 0 3T 0 part
```

In the command output, **/dev/vdb1** is the partition you created.

Step 11 Run the following command to set the format for the file system of the newly created partition:

mkfs -t *File system format* /dev/vdb1

For example, run the following command to set the **ext4** file system for the **/dev/vdb1** partition:

mkfs -t ext4 /dev/vdb1

Information similar to the following is displayed:

```
[root@bms-centos74 ~]# mkfs -t ext4 /dev/vdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
201326592 inodes, 805305856 blocks
40265292 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2952790016
24576 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
    102400000, 214990848, 512000000, 550731776, 644972544

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

The formatting takes a period of time. Observe the system running status and do not exit.

NOTE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Run the following command to create a mount point:

mkdir *Mount point*

For example, run the following command to create the **/mnt/sdc** mount point:

mkdir /mnt/sdc

Step 13 Run the following command to mount the new partition on the created mount point:

```
mount /dev/vdb1 Mount point
```

For example, run the following command to mount the newly created partition on **/mnt/sdc**:

```
mount /dev/vdb1 /mnt/sdc
```

Step 14 Run the following command to view the mount result:

df -TH

Information similar to the following is displayed:

```
[root@bms-centos74 ~]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/vda2       ext4      42G  1.5G  38G   4% /
devtmpfs        devtmpfs  2.0G   0  2.0G   0% /dev
tmpfs           tmpfs     2.0G   0  2.0G   0% /dev/shm
tmpfs           tmpfs     2.0G  8.9M  2.0G   1% /run
tmpfs           tmpfs     2.0G   0  2.0G   0% /sys/fs/cgroup
/dev/vda1       ext4      1.1G  153M  801M  17% /boot
tmpfs           tmpfs     398M   0  398M   0% /run/user/0
/dev/vdb1       ext4     3.3T   93M  3.1T   1% /mnt/sdc
```

In the command output, the newly created **dev/vdb1** partition has been mounted on **/mnt/sdc**.

----End

Setting Automatic Disk Mounting at System Start

To automatically attach a disk when a BMS starts, you should not specify its partition, for example **/dev/vdb1**, in **/etc/fstab**. This is because the sequence of cloud devices may change during the BMS stop and start, for example, **/dev/vdb1** may change to **/dev/vdb2**. You are advised to use the UUID in **/etc/fstab** to automatically attach a disk at system start.

 **NOTE**

The universally unique identifier (UUID) is the unique character string for disk partitions in a Linux system.

Step 1 Run the following command to query the partition UUID:

```
blkid Disk partition
```

For example, run the following command to query the UUID of **/dev/vdb1**:

```
blkid /dev/vdb1
```

Information similar to the following is displayed:

```
[root@bms-centos74 ~]# blkid /dev/vdb1
/dev/vdb1: UUID="bdd29fe6-9cee-4d4f-a553-9faad281f89b" TYPE="ext4" PARTLABEL="opt"
PARTUUID="c7122c92-ed14-430b-9ece-259920d5ee74"
```

In the command output, the UUID of **/dev/vdb1** is displayed.

Step 2 Run the following command to open the **fstab** file using the vi editor:

```
vi /etc/fstab
```

Step 3 Press **i** to enter the editing mode.

Step 4 Move the cursor to the end of the file and press **Enter**. Then add the following information:

```
UUID=bdd29fe6-9cee-4d4f-a553-9faad281f89b /mnt/sdc ext4 defaults 0 2
```

Step 5 Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

----End

4.4 Detaching a Disk

Scenarios

A disk attached to a BMS can be detached.

- A disk mounted to **/dev/sda** functions as the system disk. You can only detach the system disk from a stopped BMS.
- Disks attached to a mount point other than **/dev/sda** function as data disks and can be detached from a running or stopped BMS.

NOTE

After a BMS is restarted, the drive letter of an EVS disk attached to the BMS may change to the one different from that in the OS.

So, you are advised to use a world wide name (WWN) instead of a driver letter when you perform operations on disks. For details about the mapping between a WWN and driver letter, see [How Do I Obtain the Drive Letter of an EVS Disk?](#)

Constraints

- Detaching the system disk is a mission-critical operation. A BMS without the system disk cannot start. Exercise caution when performing this operation.
- Before detaching a data disk from a running Windows BMS, ensure that no program is reading data from or writing data to the disk. Otherwise, data will be lost.
- Before detaching a data disk from a running Linux BMS, you must log in to the BMS and run the **umount** command to cancel the association between the disk and the file system. In addition, ensure that no program is reading data from or writing data to the disk. Otherwise, detaching the disk will fail.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click the name of the BMS from which the disk is to be detached. The page showing details of the BMS is displayed.

4. Click the **Disks** tab. Locate the row containing the disk to be detached and click **Detach**.

4.5 Expanding Disk Capacity

If a disk does not have sufficient capacity, you can expand its capacity. Both the system disk and data disk can be expanded. The maximum size of a system disk is 1 TB. For details about how to expand the disk capacity, see [Expansion Overview](#) in *Elastic Volume Service User Guide*.

NOTICE

The system disk capacity of a Windows BMS that is quickly provisioned cannot be expanded. If you need to expand the capacity, contact technical support.

After the capacity expansion is successful, allocate the partition for the extended space of the DSS disk.

- For details about the follow-up operations after a system disk is expanded, see [Extending Disk Partitions and File Systems \(Windows\)](#) or [Extending Partitions and File Systems for System Disks \(Linux\)](#) in *Elastic Volume Service User Guide*.
- For details about the follow-up operations after a data disk is expanded, see [Extending Disk Partitions and File Systems \(Windows\)](#) or [Extending Partitions and File Systems for Data Disks \(Linux\)](#) in *Elastic Volume Service User Guide*.

5 Key Pair and Password

5.1 Using an SSH Key Pair

Scenarios

To ensure system security, you are advised to use the key authentication mode to authorize the user who attempts to log in to a BMS. Therefore, you must use an existing key pair or create a new one for remote login authentication.

- **Creating a Key Pair**

If no key pair is available, create one that contains a public and a private key used for login authentication. You can use either of the following methods:

- Create a key pair using the management console. After the creation, the public key is automatically stored in the system, and the private key is manually stored in a local directory. For details, see [Create a Key Pair on the Management Console](#).
- Use PuTTYgen to create a key pair, and save both the public and private keys to the local host. For details, see [Create a Key Pair Using PuTTYgen](#). After the creation, import the key pair by following the instructions provided in [Import a Key Pair](#). Then, the key pair can be used.

 **NOTE**

PuTTYgen is a tool for generating public and private keys. You can obtain the tool from <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

- **Using an existing key pair**

If a key pair is available locally, for example, generated using PuTTYgen, you can import the public key on the management console so that the system maintains the public key file. For details, see [Import a Key Pair](#).

Constraints

- SSH key pairs can only be used to log in to Linux BMSs.
- Only key pairs encrypted by Rivest–Shamir–Adleman (RSA) can be imported, and the length can be 1,024, 2,048, or 4,096 bits.

Create a Key Pair on the Management Console

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the navigation tree, choose **Key Pair**.
4. On the right side of the page, click **Create Key Pair**.
5. Enter the key name and click **OK**.
An automatically populated key name consists of **KeyPair-** and a 4-digit random number. Change it to an easy-to-remember one, for example, **KeyPair-xxxx_bms**.
6. Download the private key file. The file name is the specified key pair name with a suffix of .pem. Store the private key file securely. In the displayed dialog box, click **OK**.

 **CAUTION**

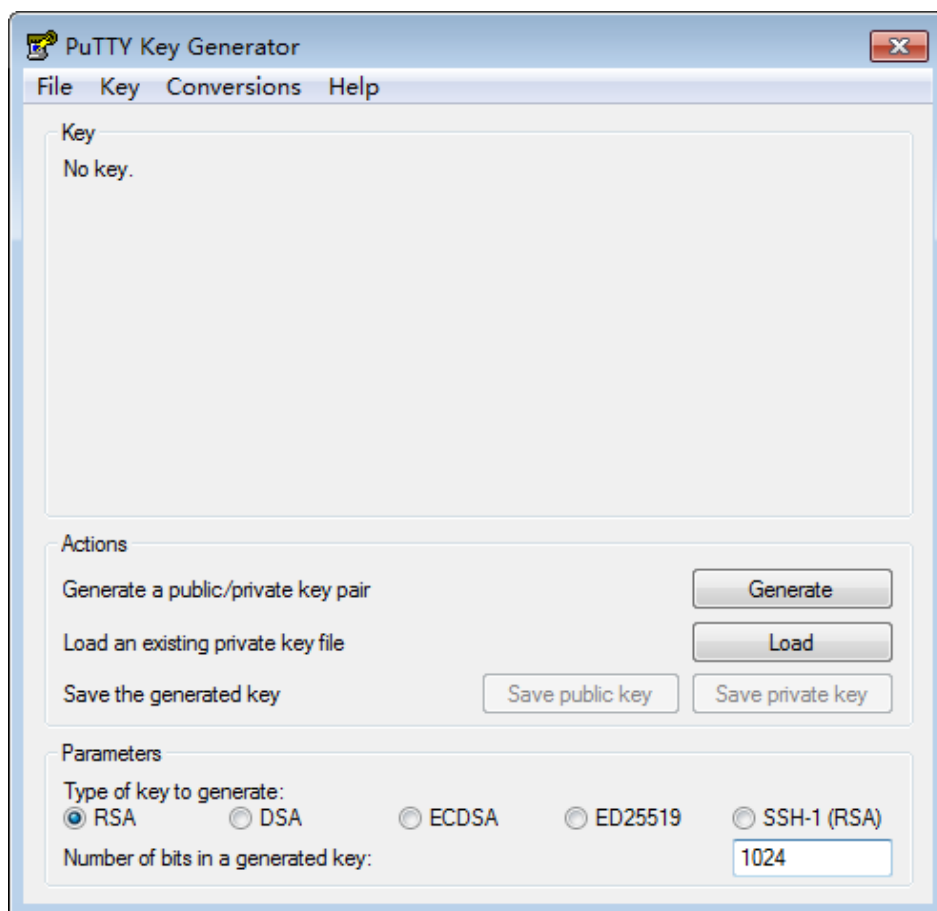
You can save the private key file only once. When you create a BMS, provide the key pair name. Each time you log in to the BMS using SSH, you need to provide the private key.

Create a Key Pair Using PuTTYgen

Step 1 Obtain the public and private keys.

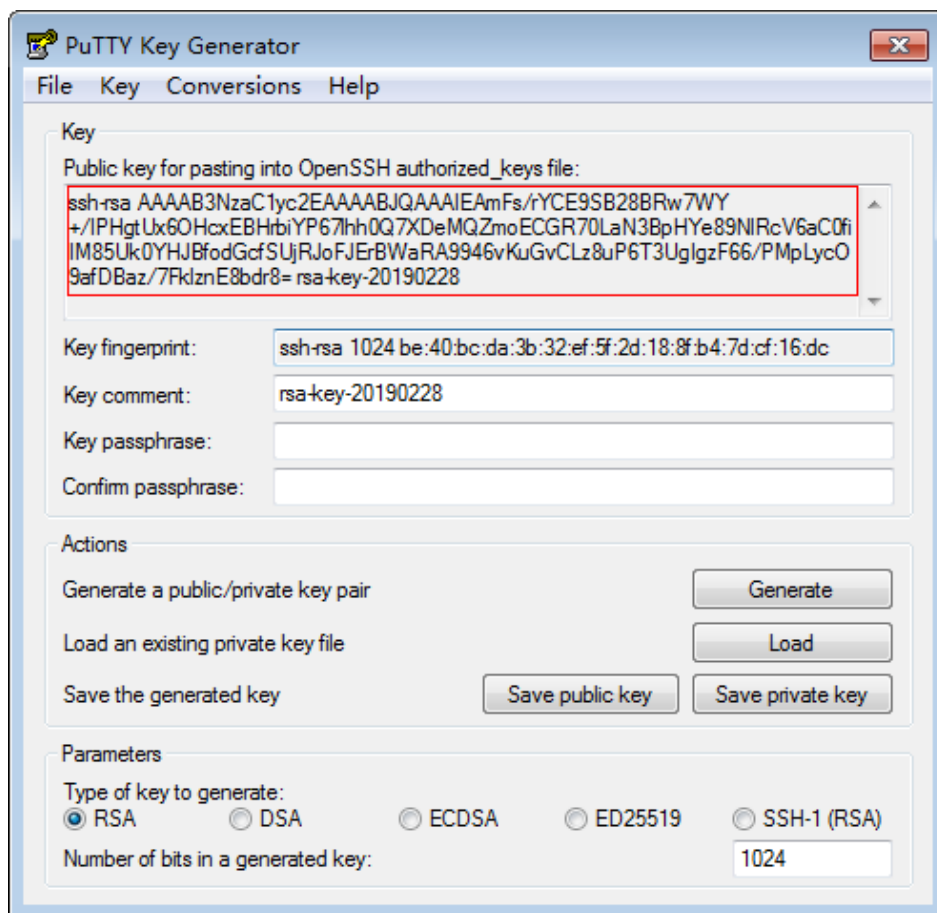
1. Double-click **puttygen.exe**. The **PuTTY Key Generator** window is displayed.

Figure 5-1 PuTTY Key Generator



2. Click **Generate**.

The key generator automatically generates a key pair that consists of a public key and a private key. The public key is that shown in the red box in [Figure 5-2](#).

Figure 5-2 Obtaining the public and private keys

Step 2 Copy the public key content to a .txt file and save the file in a local directory.

NOTE

Do not save the public key by clicking **Save public key**. Storing a public key by clicking **Save public key** of PuTTYgen will change the format of the public key content. Such a key cannot be imported to the management console.

Step 3 Save the private key file.

The format in which to save your private key varies depending on application scenarios: To ensure BMS security, you are limited to downloading the private key only once.

- Saving the private key in .ppk format
When you are required to log in to a Linux BMS using PuTTY, you must use the .ppk private key. To save the private key in .ppk format, perform the following operations:
 - a. On the **PuTTY Key Generator** page, choose **File > Save private key**.
 - b. Save the private key, for example, **kp-123.ppk**, to the local PC.
- Saving the private key in .pem format
When you are required to log in to a Linux BMS using Xshell or attempt to obtain the password for logging in to a Windows BMS, you must use the .pem private key for authentication. To save the private key in .ppk format, perform the following operations:

- a. On the **PuTTY Key Generator** page, choose **Conversions > Export OpenSSH key**.

 **CAUTION**

If you use this private file to obtain the password for logging in to a Windows BMS, when you choose **Export OpenSSH key**, do not configure **Key passphrase**. Otherwise, obtaining the password will fail.

- b. Save the private key, for example, **kp-123.pem**, in a local directory.

Step 4 After the public key file and private key file are saved, import the public key to the system by referring to [Import a Key Pair](#).

----End

Import a Key Pair

If you store a public key by clicking **Save public key** of PuTTYgen, the format of the public key content will change. Such a key cannot be imported to the management console. To resolve this issue, obtain the public key content in correct format and import the content to the management console. For details, see [What Do I Do If a Key Pair Created Using PuTTYgen Cannot Be Imported to the Management Console?](#)

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the navigation tree, choose **Key Pair**.
4. On the right side of the page, click **Import Key Pair**.
5. Use either of the following methods to import the key pair:
 - Selecting a file
 - i. On the **Import Key Pair** page of the management console, click **Select File** and select the local public key file, for example, the .txt file saved in [Step 2](#).

 **NOTE**

When importing a key pair, ensure that the public key is imported. Otherwise, importing the key pair will fail.

- ii. Click **OK**.
After the public key is imported, you can change its name.
- Copying the public key content
 - i. Copy the content of the public key in .txt file into the **Public Key Content** text box.
 - ii. Click **OK**.

Delete a Key Pair

If you no longer need a key pair, you can delete it. After a key pair is deleted, it cannot be restored. However, you can still use the private key saved locally to log in to the BMS, and the deleted key pair is still displayed in the BMS details.

NOTE

- If your key pair has been bound to a BMS and you do not unbind the key pair from the BMS before deleting the key pair, you cannot create a key pair of the same name. When you enter this name when creating or importing a key pair, the console displays an error message indicating that the key pair already exists.
- If your key pair is not bound to any BMS or has been unbound from the BMS before it is deleted, you can create a key pair of the same name.

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the navigation tree, choose **Key Pair**.
4. Locate the row that contains the target key pair and click **Delete** in the **Operation** column.

5.2 Obtaining the Password of a Windows BMS

Scenarios

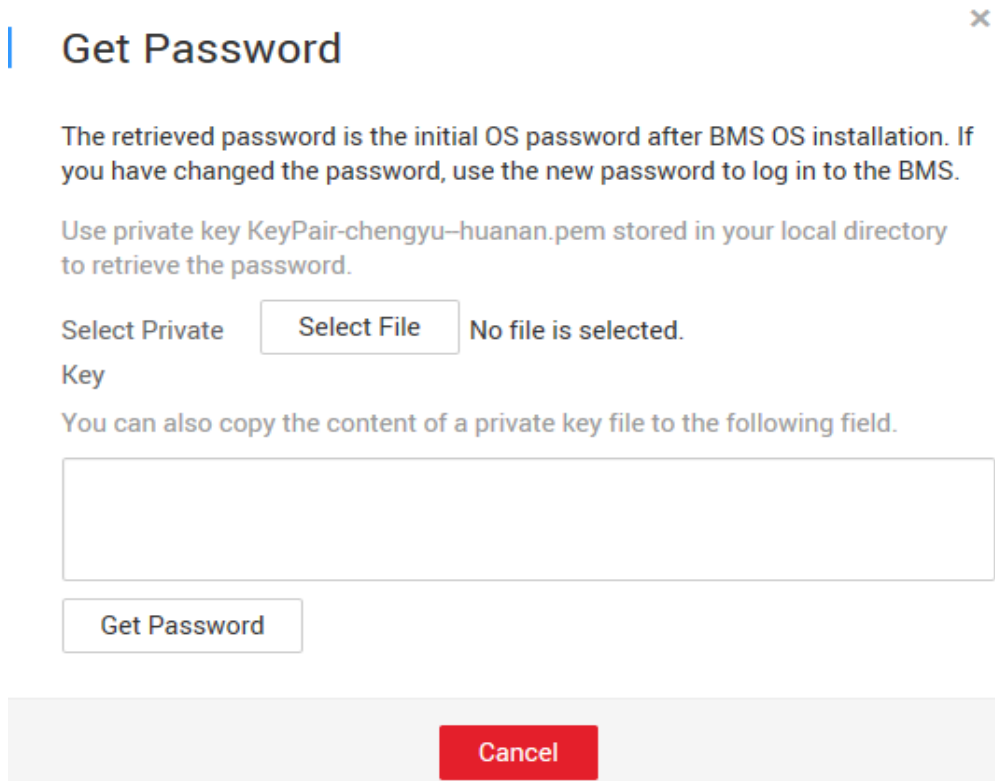
Password authentication mode is required to log in to a Windows BMS. Therefore, you must use the key file used when you created the BMS to obtain the administrator password generated when the BMS was initially installed. The administrator user is **Administrator** or the user configured using Cloudbase-Init. This password is randomly generated, offering high security.

Prerequisites

You have obtained the private key file used during BMS creation.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the row that contains the Windows BMS, click **More** in the **Operation** column, and select **Obtain Password**.

Figure 5-3 Obtaining the password

4. Use either of the following methods to obtain the password through the private key:
 - Click **Select File** and upload the private key from a local directory.
 - Copy the private key content to the text field.
5. Click **Get Password** to obtain a random password.

5.3 Deleting the Password of a Windows BMS

Scenarios

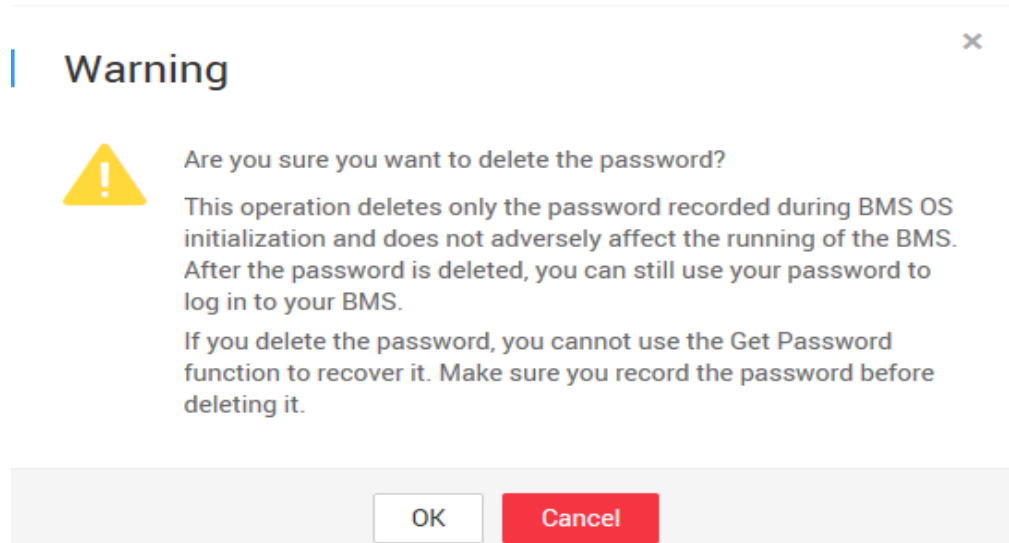
To ensure security, you are advised to delete the initial password recorded in the system.

Deleting the initial password does not affect BMS operation or login. Once deleted, the password cannot be retrieved. Before deleting a password, you are advised to record it.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Locate the target BMS in the BMS list.
4. In the **Operation** column, click **More** and select **Delete Password**.
The following dialog box is displayed.

Figure 5-4 Warning



5. Click **OK** to delete the password.

6 Network

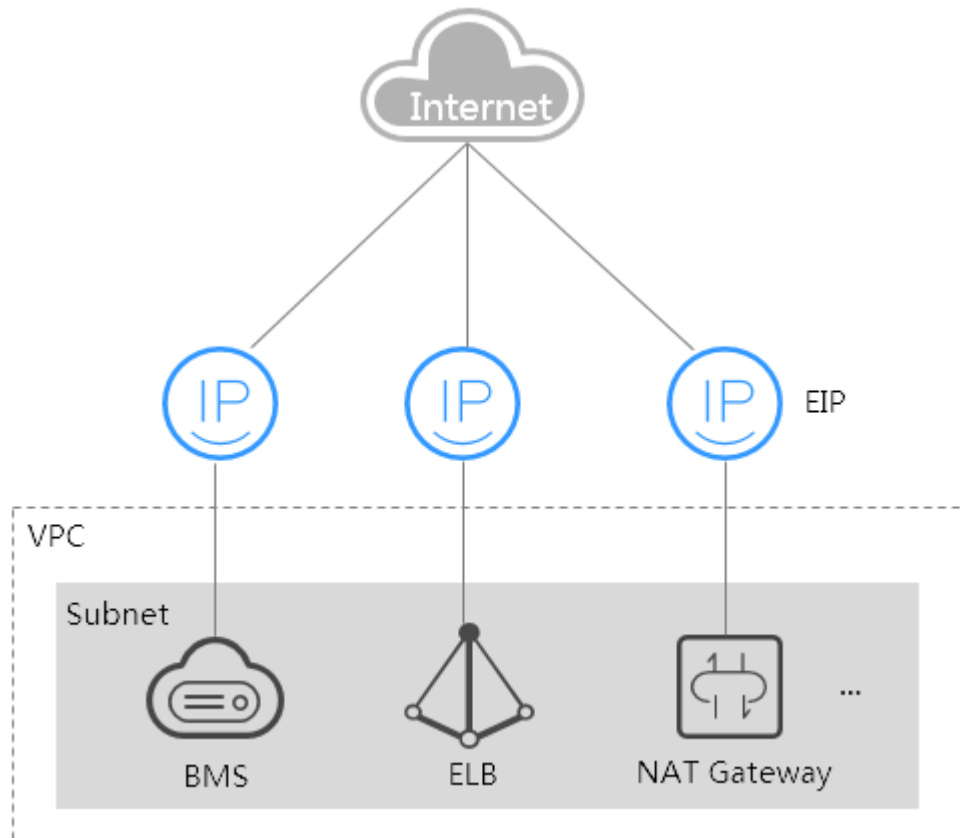
6.1 EIP

6.1.1 Overview

EIP

The Elastic IP (EIP) service provides independent public IP addresses and bandwidth for Internet access. Different from traditional static IP addresses, EIPs can be dynamically bound to or unbound from resources such as BMSs, ECSs, and NAT gateways. If a server becomes faulty, the EIP can be quickly unbound from it and bound to another healthy server to recover services.

Figure 6-1 Accessing the Internet through an EIP



Helpful Links

- [Can I Bind Multiple EIPs to a BMS?](#)
- [Will I Obtain an EIP That Has Been Released?](#)
- [What Are the Differences Between EIPs, Private IP Addresses, and Virtual IP Addresses?](#)

6.1.2 Binding an EIP to a BMS

Scenarios

To allow your BMS to communicate with the Internet, bind an EIP to the BMS.

Prerequisites

An EIP is available. For details about how to apply for an EIP, see [Assigning an EIP](#).

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.

3. Click a BMS.
The page showing details of the BMS is displayed.
4. Click the **EIPs** tab and then **Bind EIP**.
The **Bind EIP** dialog box is displayed.
5. Select the EIP to be bound and click **OK**.

 **NOTE**

Only one EIP can be bound to a NIC.

6.1.3 Unbinding an EIP from a BMS

Scenarios

This section describes how to unbind an EIP from a BMS.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click a BMS.
The page showing details of the BMS is displayed.
4. Click the **EIPs** tab. On the displayed page, locate the target EIP and click **Unbind**. In the displayed dialog box, click **Yes**.

 **NOTE**

The EIP is still billed after it is unbound. Release it if you do not need it any more.

6.2 VPC

6.2.1 Overview

VPC

A VPC provides a logically isolated network environment for BMSs. You can configure EIPs, security groups, and VPNs in a VPC and use the VPC for communication between ECSs and BMSs.

View VPC NICs

You can view the network interfaces of the VPC on the **NICs** tab page of the BMS details page. For Linux images, you can also locate the VLAN sub-interface or bond interface in the OS based on the allocated IP address.

Figure 6-2 Viewing NICs

192.168.0.48	
NIC ID	496fa0e-3d3f-4811-8a6b-b724e02716e
EIP	--
Security Group	default
Source/Destination Check	<input checked="" type="checkbox"/>
VLAN	3095
MAC Address	fa:16:3e:04:5c:8c
IPv4 Subnet ID	242ce9f6-0e7b-4466-b0a0-3f0a00f5920
Status	Activated
Subnet	asdfas (192.168.0.0/24)
Private IP Address	192.168.0.48
IPv6 Address	--
Virtual IP Address	--
Network ID	94f655de-0f6a-4eef-65e7-57aab3031db7
IPv6 Subnet ID	3e7535e1-df33-449b-980b-16db060c26c2

192.168.0.14	
NIC ID	59b0bbe-4ef3-4719-8098-57b0881372f4
EIP	--
Security Group	default
Source/Destination Check	<input checked="" type="checkbox"/>
VLAN	3029
MAC Address	fa:16:3e:04:5c:6a
IPv4 Subnet ID	242ce9f6-0e7b-4466-b0a0-3f0a00f5920
Status	Activated
Subnet	asdfas (192.168.0.0/24)
Private IP Address	192.168.0.14
IPv6 Address	--
Virtual IP Address	--
Network ID	94f655de-0f6a-4eef-65e7-57aab3031db7
IPv6 Subnet ID	3e7535e1-df33-449b-980b-16db060c26c2

172.16.20.183 High-Speed NIC	
172.16.18.188 High-Speed NIC	

Take CentOS 7.4 64-bit as an example. Log in to the OS and view the NIC configuration files **ifcfg-eth0**, **ifcfg-eth1**, **ifcfg-bond0**, **ifcfg-bond0.3029**, **ifcfg-bond0.3187**, and **ifcfg-bond0.3189** in the **/etc/sysconfig/network-scripts** directory. You need to use IP mapping to match the network.

Run the **ifconfig** command. The private IP address and MAC address of VPC NIC 1 are 192.168.0.48 and fa:16:3e:04:5c:8c. The private IP address and MAC address of VPC NIC 2 are 192.168.0.14 and fa:16:3e:04:5c:6a. eth0 and eth1 automatically form bond0, and they have the same MAC address. In addition, it can be determined that **ifcfg-eth0**, **ifcfg-eth1**, **ifcfg-bond0**, **ifcfg-bond0.3029**, **ifcfg-bond0.3187**, and **ifcfg-bond0.3189** are VPC NIC configuration files.

```
[root@bms-7e45 network-scripts]# ifconfig
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST> mtu 8888
    inet 192.168.0.48 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::f816:3eff:fe04:5c8c prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:04:5c:8c txqueuelen 1000 (Ethernet)
    RX packets 243 bytes 58662 (57.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 728 bytes 95132 (92.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bond0.3029: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 8888
    inet 192.168.0.14 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::f816:3eff:fe04:5c6a prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:04:5c:6a txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 833 (833.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1424 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bond0.3187: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 8888
    inet6 fe80::f816:3eff:fe09:47f3 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:09:47:f3 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 125 bytes 40670 (39.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bond0.3189: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 8888
    inet 172.16.16.188 netmask 255.255.255.0 broadcast 172.16.16.255
    inet6 fe80::f816:3eff:fe88:6322 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:88:63:22 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1076 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST> mtu 8888
    ether fa:16:3e:04:5c:8c txqueuelen 1000 (Ethernet)
    RX packets 110 bytes 16560 (16.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 728 bytes 95132 (92.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST> mtu 8888
    ether fa:16:3e:04:5c:8c txqueuelen 1000 (Ethernet)
    RX packets 133 bytes 42102 (41.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The following figures show the NIC and bond configuration information.

```
[root@bms-7e45 network-scripts]# cat ifcfg-eth0
USERCTL=no
MTU=8888
NM_CONTROLLED=no
BOOTPROTO=dhcp
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
MASTER=bond0
SLAVE=yes
[root@bms-7e45 network-scripts]# cat ifcfg-eth1
USERCTL=no
MTU=8888
NM_CONTROLLED=no
BOOTPROTO=dhcp
DEVICE=eth1
TYPE=Ethernet
ONBOOT=yes
MASTER=bond0
SLAVE=yes
[root@bms-7e45 network-scripts]# cat ifcfg-bond0
MACADDR=fa:16:3e:04:5c:8c
USERCTL=no
PERSISTENT_DHCLIENT=1
BONDING_MASTER=yes
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=dhcp
BONDING_OPTS="mode=1 miimon=100"
DEVICE=bond0
TYPE=Bond
[root@bms-7e45 network-scripts]# cat ifcfg-bond0.3029
MACADDR=fa:16:3e:04:5c:6a
USERCTL=no
PERSISTENT_DHCLIENT=1
PHYSDEV=bond0
VLAN=yes
NM_CONTROLLED=no
BOOTPROTO=dhcp
DEVICE=bond0.3029
TYPE=Ethernet
ONBOOT=yes
```

```
[root@bms-7e45 network-scripts]# cat ifcfg-bond0.3189
MACADDR=fa:16:3e:88:63:22
USERCTL=no
PHYSDEV=bond0
VLAN=yes
IPADDR=172.16.16.188
NM_CONTROLLED=no
NETMASK=255.255.255.0
BOOTPROTO=static
DEVICE=bond0.3189
TYPE=Ethernet
ONBOOT=yes
[root@bms-7e45 network-scripts]# cat ifcfg-bond0.3187
MACADDR=fa:16:3e:09:47:f3
USERCTL=no
PERSISTENT_DHCLIENT=1
PHYSDEV=bond0
VLAN=yes
NM_CONTROLLED=no
BOOTPROTO=dhcp
DEVICE=bond0.3187
TYPE=Ethernet
ONBOOT=yes
```

6.2.2 Binding a Virtual IP Address to a BMS

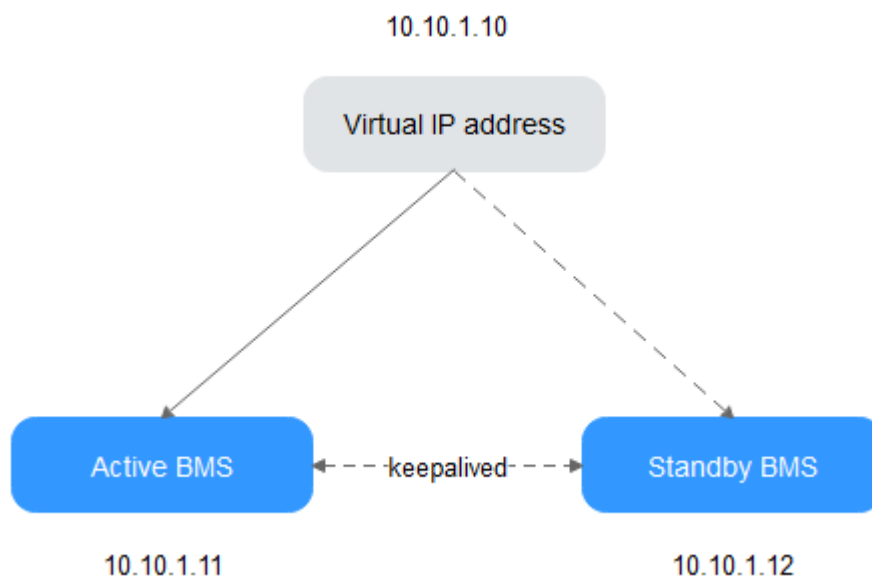
Scenarios

You can bind a virtual IP address to a BMS for connection redundancy. This section describes how to bind a virtual IP address to a BMS.

What Is a Virtual IP Address?

Virtual IP addresses, also called floating IP addresses, are used for active and standby switchover of servers to achieve high availability. If the active server is faulty and cannot provide services, the virtual IP address is dynamically switched to the standby server to provide services.

If you want to improve service high availability and avoid single points of failure, you can use BMSs that are deployed to work in the active/standby mode or one active and multiple standby modes. These BMSs use the same virtual IP address.

Figure 6-3 Networking diagram of the HA mode

- Bind two BMSs in the same subnet to the same virtual IP address.
- Configure Keepalived for the two BMSs to work in the active/standby mode. For details about Keepalived configurations, see the common configuration methods in the industry.

NOTE

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

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click the name of the BMS to which a virtual IP address needs to be bound.
The page showing details of the BMS is displayed.
4. Click the **NICs** tab. Then, click **Manage Virtual IP Address**.
The page showing details of the particular VPC is displayed.
5. On the **Virtual IP Address** tab, select a desired one or click **Assign Virtual IP Address** for a new one.
6. Click **Bind to Server** in the **Operation** column and select the target BMS and the NIC to bind the virtual IP address to the NIC.

6.2.3 Setting the Source/Destination Check for a NIC

Scenarios

After source/destination check is enabled, the system checks whether source IP addresses contained in the packets sent by BMSs are correct. If the IP addresses

are incorrect, the system does not allow the BMSs to send the packets. This mechanism prevents packet spoofing, thereby improving system security.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click the name of the target BMS.
The page showing details of the BMS is displayed.
4. Select the **NICs** tab. Expand the details of the target NIC.
5. Enable or disable **Source/Destination Check**.
By default, **Source/Destination Check** is enabled. If the BMS functions as a NAT server, router, or firewall, you must disable the source/destination check for the BMS.

6.2.4 Enabling IPv4/IPv6 Dual Stack

Scenarios

IPv4/IPv6 dual stack allows your BMSs to use both IPv4 and IPv6 addresses for private and public network communications. This section describes how to enable IPv4/IPv6 dual stack.

Notes

- Currently, you can only enable IPv6 when creating a BMS, rather than when adding a NIC. After IPv6 is enabled, it cannot be disabled.
- After IPv6 is enabled, IPv6 CIDR blocks will be automatically assigned to subnets. You are not allowed to specify a custom IPv6 CIDR block.
- After IPv4/IPv6 dual stack is enabled, a BMS has an IPv4 and an IPv6 address, and cannot use the IPv6 address alone.

Procedure

1. Enable IPv6 for a VPC subnet.
 - a. On the management console, choose **Network > Virtual Private Cloud** from the service list.
The VPC console is displayed.
 - b. Locate the target VPC and click the number of subnets.
The **Subnets** page is displayed.
 - c. Locate the target subnet and click **Enable IPv6**.
 - d. In the **Enable IPv6** dialog box, click **Yes**.

NOTE

IPv6 cannot be disabled.

2. Create a BMS and enable IPv4/IPv6 dual stack.

- Image
Select an image that supports IPv6. A public image that supports IPv6 has a tag after the image's OS version. For a private or shared image, you need to find out whether it supports IPv6.
- VPC
Select the VPC subnet for which IPv6 has been enabled.

Figure 6-4 Network configuration

The screenshot shows a network configuration interface. At the top, there is a 'VPC' dropdown menu with 'vpc-ipv6-open' selected and a 'Create VPC' button. Below this is the 'NIC' section. The 'Primary NIC' dropdown is set to 'subnet-f255(192.168.2.0/24)'. To its right is a 'User-configured IP address' field with a 'View In-Use IP Address' link. Below the 'Primary NIC' dropdown is a 'Self-assigned IPv6 address' dropdown, which is highlighted with a red box. To its right is a 'Do not configure' dropdown and a 'Manage shared bandwidth' button. At the bottom, there is a '+ Add NIC' button with the text 'You can add 1 more NICs.'

- NIC
After you select a subnet with IPv6 enabled, the **Self-assigned IPv6 address** option will be available when you configure a NIC.

NOTE

- If you select a private or shared image that does not support IPv6, **Self-assigned IPv6 address** will not take effect. That is, no IPv6 address can be found in the BMS OS even if **Self-assigned IPv6 address** is selected. Therefore, you are advised to select a public image that supports IPv6.
 - CentOS 7.3 public images do not support IPv6 address assignment to extension NICs. Therefore, you are advised to use other images.
3. After the BMS is created, log in to BMS and view the IPv6 address assigned to it.
- For example, run the **ip addr** command on a Linux BMS to query the IPv6 address.

Figure 6-5 Example command

```
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST> mtu 8888
    inet 192.168.2.106 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::f816:3eff:fed2:fa58 prefixlen 64 scopeid 0x20<link>
    inet6 2001:db8:a583:1:d865:fc53:24c4:71b3 prefixlen 64 scopeid 0x0<global>
bal>
    ether fa:16:3e:d2:fa:58 txqueuelen 1000 (Ethernet)
    RX packets 92 bytes 12013 (11.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 367 bytes 31758 (31.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bond0.2065: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 8888
    inet 192.168.0.243 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 2001:db8:a583:2:b5ef:74d4:f59f:5824 prefixlen 64 scopeid 0x0<global>
bal>
    inet6 fe80::f816:3eff:fe8a:8abe prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:8a:8a:be txqueuelen 1000 (Ethernet)
    RX packets 19 bytes 2886 (2.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 3822 (3.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST> mtu 8888
    ether fa:16:3e:d2:fa:58 txqueuelen 1000 (Ethernet)
:
_
```

7 Security

7.1 Security Group

7.1.1 Adding Security Group Rules

Scenarios

The default security group rule allows all outgoing data packets. BMSs in a security group can access each other without the need to add access rules. After a security group is created, you can create different access rules for the security group to protect the BMSs that are added to this security group.


NOTE

You can add only one security group when creating a BMS. After the BMS is created, you can modify the security group of each NIC on the BMS details page.

Suggestions

- When adding a security group rule for a BMS, grant the minimum permissions possible:
 - Enable specific ports rather than a port range, for example, port 80.
 - Be cautious to authorize source address 0.0.0.0/0 (entire network segment).
- You are not advised to use one security group to manage all applications because isolation requirements for different layers vary.
- Configuring a security group for each BMS is unnecessary. Instead, you can add BMSs with the same security protection requirements to the same security group.
- Simple security group rules are recommended. For example, if you add a BMS to multiple security groups, the BMS may comply with hundreds of security group rules, and a change to any rule may cause network disconnection for the BMS.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the BMS list, click the name of the BMS whose security group rules you want to modify.
The page showing details of the BMS is displayed.
4. Click the **Security Groups** tab and then  to view security group rules.
5. Click the security group ID.
The system automatically switches to the **Security Group** page.
6. Click **Manage Rule** in the **Operation** column. On the security group details page, add a rule.

Value **Inbound** indicates that traffic enters the security group, and value **Outbound** indicates that traffic leaves the security group.

Table 7-1 Parameter description

Parameter	Description
Protocol	Network protocol for which the security group rule takes effect. The value can be All , TCP , UDP , ICMP , or GRE .
Port	Port or port range for which the security group rule takes effect. The value ranges from 1 to 65535 .
Source	Traffic source (inbound rule). This parameter is required for an inbound rule. The value can be an IP address or a security group.
Destination	Traffic destination (outbound rule). This parameter is required for an outbound rule. The value can be an IP address or a security group.

NOTE

The default source IP address **0.0.0.0/0** indicates that all IP addresses can access BMSs in the security group.

7.1.2 Security Group Configuration Examples

Case 1: BMSs in Different Security Groups Need to Communicate with Each Other Through an Internal Network

- Scenario
Resources on a BMS in a security group need to be copied to a BMS in another security group. The two BMSs are in the same VPC. Then, you can

enable internal network communication between the two BMSs and copy resources.

- Security group configuration

In the same VPC, BMSs associated with the same security group can communicate with one another by default, and no additional configuration is required. However, BMSs in different security groups cannot communicate with each other by default. You must add security group rules to enable the BMSs to communicate with each other through an internal network.

However, BMSs in different security groups cannot communicate with each other by default. You must add security group rules to enable the BMSs to communicate with each other through an internal network.

Protocol	Direction	Port Range/ ICMP Protocol Type	Source
Protocol to be used for internal network communication. Supported values are TCP, UDP, ICMP, and All.	Inbound	Port number range or ICMP protocol type	IPv4 address, IPv4 CIDR block, or another security group ID

Case 2: Only Specified IP Addresses Can Remotely Access BMSs in a Security Group

- Scenario

To prevent BMSs from being attacked, you can change the port number for remote login and configure security group rules that allow only specified IP addresses to remotely access the BMSs.

- Security group configuration

To allow IP address **192.168.20.2** to remotely access Linux BMSs in a security group over the SSH protocol and port 22, you can configure the following security group rule.

Protocol	Direction	Port Range	Source
SSH (22)	Inbound	22	IPv4 address, IPv4 CIDR block, or another security group ID For example, 192.168.20.2

Case 3: Remotely Connecting to a Linux BMS Through SSH

- Scenario

To remotely connect to a Linux BMS through SSH, you need to add a security group rule.

 NOTE

The default security group comes with this rule. If you use the default security group, you do not need to configure the rule again.

- Security group configuration

Protocol	Direction	Port Range	Source
SSH (22)	Inbound	22	0.0.0.0/0

Case 4: Remotely Connecting to a Windows BMS Through RDP

- Scenario

To remotely connect to a Windows BMS through RDP, you need to add a security group rule.

 NOTE

The default security group comes with this rule. If you use the default security group, you do not need to configure the rule again.

- Security group configuration

Protocol	Direction	Port Range	Source
RDP (3389)	Inbound	3389	0.0.0.0/0

Case 5: Pinging a BMS from the Internet

- Scenario

To ping BMSs from each other to check connectivity, you need to add a security group rule.

- Security group configuration

Protocol	Direction	Port Range	Source
ICMP	Inbound	All	0.0.0.0/0

7.1.3 Changing a Security Group

Scenarios

This section describes how to change the security group of the BMS NIC or associate multiple security groups with the BMS.

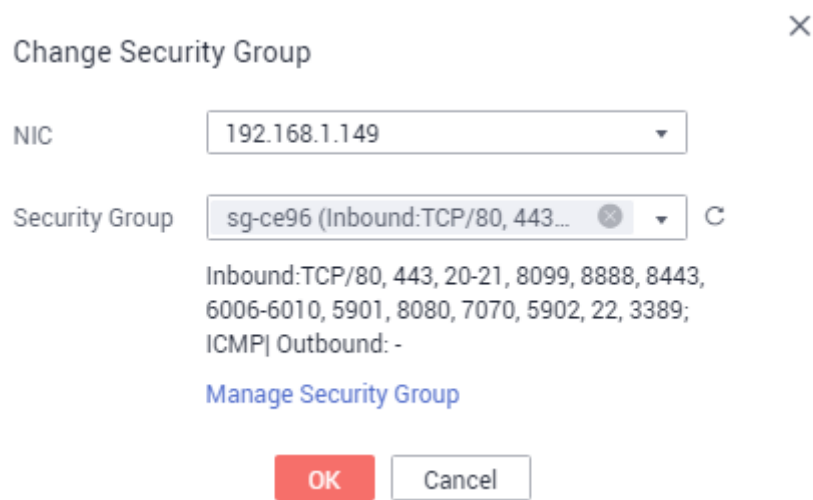
 NOTE

When multiple security groups are associated with the BMS, all the security group rules take effect.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click the name of the target BMS.
The page showing details of the BMS is displayed.
4. Click the **Security Groups** tab. Then, click **Change Security Group**.
5. In the displayed **Change Security Group** dialog box, select the target security group and click **OK**.

Figure 7-1 Changing a security group



To associate multiple security groups with the BMS, select the groups.

Result

On the BMS details page, click the **Security Groups** tab. The security group has been changed, or new security groups are contained in the list.

8 Resources and Tags

8.1 Tag

8.1.1 Overview

To facilitate your management of BMSs, disks, images, and other cloud resources, you can add a tag to each resource to allocate your own metadata to the resource. Tag Management Service (TMS) is a visualized service for fast and unified cross-region tagging and categorization of cloud services.

Basics of Tags

Tags are used to identify cloud resources. When you have many cloud resources of the same type, you can use tags to classify cloud resources by dimension (for example, use, owner, or environment).

Figure 8-1 Example tags

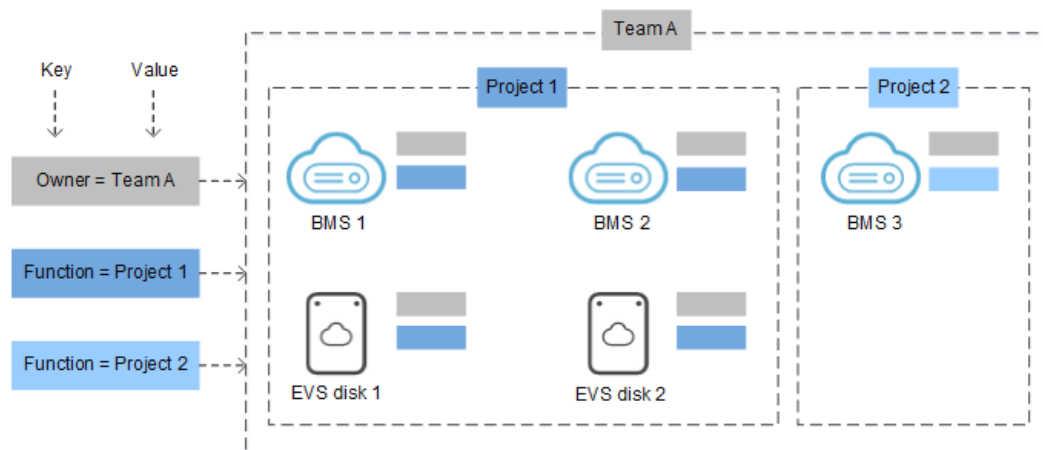


Figure 8-1 shows how tags work. In this example, you assign two tags to each cloud resource. Each tag contains a key and a value that you define. The key of one tag is **Owner**, and the key of another tag is **Use**. Each tag has a value.

You can quickly search for and filter specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier.

Tag Usage

- BMS-related services that support tags include ECS, IMS, and EVS.
- Each tag consists of a key and a value.
- A BMS can have a maximum of nine tags.
- For each resource, each tag key must be unique and can have only one tag value.
- [Table 8-1](#) provides the tag key and value requirements.

Table 8-1 Tag key and value requirements

Parameter	Requirement	Example Value
Tag key	<ul style="list-style-type: none">• Cannot be left blank.• Can only contain letters, digits, underscores (_), and hyphens (-).• Contains a maximum of 36 characters.	Organization
Tag value	<ul style="list-style-type: none">• Cannot be left blank.• Can only contain letters, digits, underscores (_), periods (.), and hyphens (-).• Contains a maximum of 43 characters.	Apache

8.1.2 Adding Tags

Tags are used to identify cloud resources, such as instances, images, and disks. If you have multiple types of cloud resources which are associated with each other, you can add tags to the resources to classify and manage them easily. For more information, see [Overview](#).

You can add tags to a BMS in either of the following ways:

- [Add Tags During BMS Creation](#)
- [Add Tags on the BMS Details Page](#)

Add Tags During BMS Creation

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. Click **Buy BMS**.

4. Configure the BMS parameters.
Select **Configure now** for **Advanced Settings** and add a tag key and tag value. For the tag key and tag value requirements, see [Table 8-1](#).

 **NOTE**

For details about other parameters, see [Creating a Common BMS](#).

Add Tags on the BMS Details Page

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the BMS list, click the name of the target BMS.
The page showing details of the BMS is displayed.
4. Click the **Tags** tab and then **Add Tag**. In the displayed dialog box, enter the tag key and tag value. For the tag key and tag value requirements, see [Table 8-1](#).
You can change the tag value after the tag is added.

Tips

If you want to add the same tag to multiple BMSs or other resources, you can create a predefined tag on the TMS console and then select the tag for the BMSs or resources. This free you from having to repeatedly enter tag keys and values. The procedure is as follows:

1. Log in to the management console.
2. In the upper right corner of the page, click the username and select **Tag Management** from the drop-down list.
3. In the navigation pane on the left, choose **Predefined Tags**. In the right pane, click **Create Tag**, and enter a key (for example **project**) and a value (for example **A**) in the displayed dialog box.
4. Choose **Service List > Computing > Bare Metal Server**. On the BMS console, click the name of the BMS to which you want to add the predefined tag.
The page showing details of the BMS is displayed.
5. Click the **Tags** tab and then **Add Tag**. In the displayed dialog box, select the predefined tag you have created.


8.1.3 Searching for Resources by Tag

After tags are added to resources, you can search for resources by tag using either of the following methods.

Filter Resources in the Resource List

On the BMS console, query BMSs by tag key and value.

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.

3. Click **Search by Tag** above the upper right corner of the BMS list to expand the search area.
4. Enter the tag of the target BMS.
Both the tag key and value are mandatory. If the tag key or value is matched, the system automatically displays the target BMSs.
5. Click  to add multiple tags.
You can add multiple tags. The system will display BMSs that have all the tags.
6. Click **Search**.
The system searches for BMSs based on the specified tag keys and values.

Filter Resources on the TMS Console

1. Log in to the management console.
2. In the upper right corner of the page, click the username and select **Tag Management** from the drop-down list.
3. On the **Resource Tags** page, set the search criteria, including **Region**, **Resource Type**, and **Resource Tag**.
4. Click **Search**.
All the resources that meet the search criteria will be displayed in the **Search Result** area.

8.1.4 Deleting Tags

If you no longer need a tag, delete it in either of the following ways:

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Bare Metal Server**.
The BMS console is displayed.
3. In the BMS list, click the name of the target BMS.
The page showing details of the BMS is displayed.
4. Click the **Tags** tab. Locate the row containing the tag to be deleted and click **Delete** in the **Operation** column. In the **Delete Tag** dialog box, click **Yes**.

8.2 Resource Location

Some resources are available in all regions around the globe, while others are only available in specified regions or AZs.

Resource	Type	Description
Account of Huawei Cloud	Global	You can use the same Huawei Cloud account across all regions.

Resource	Type	Description
Predefined tags	Global	You can use the same predefined tag in all regions.
Key pair	Global or regional	<p>A key pair you create on the management console is associated with the region where it is created.</p> <p>You can create your own RSA key pair and import it into the region where you want to use it. Therefore, you can upload a key pair to each region to use it globally.</p> <p>For details about key pairs, see Using an SSH Key Pair.</p>
Resource identifier	Regional	Each resource identifier (such as instance ID, EVS disk ID, and VPC ID) is associated with a region and can be used only in the region where the resource is created.
User-defined resource name	Regional	Each resource name (such as the security name and key pair name) is associated with a region and can be used only in the region where the resource is created. Although you can create resources with the same name in different regions, the resources are not associated with each other.
VPC	Regional	A VPC is associated with a region and can only be associated with instances in the same region.
EIP	Regional	An EIP is associated with a region and can only be associated with instances in the same region.
Security group	Regional	A security group is associated with a region and can only be allocated to instances in the same region. The security group rule cannot be used to enable communication between instances in different regions.
Image	Regional	An image is associated with a region and can only be associated with instances in the same region. The image can be a public, private, or shared image.
Instance	AZ	An instance is associated with an AZ, but the instance ID is associated with a region.
Disk	AZ	A disk is associated with an AZ and can only be attached to instances in the same AZ.
Subnet	AZ	A subnet is associated with an AZ and can only be associated with instances in the same AZ.

8.3 Adjusting Resource Quotas

What Is Quota?


Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of BMSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

NOTE

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.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.
3. Click **Increase Quota** in the upper right corner of the page.
4. On the **Create Service Ticket** page, configure parameters as required.
In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

9 Server Monitoring

9.1 Overview

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 the Cloud Eye 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, **Server Monitoring** monitors more than 40 metrics, such as CPU, memory, disk, and network.

Constraints

- Agent can only be installed on BMSs running a 64-bit Linux OS.
- Private images do not support this function.

Table 9-1 lists the Linux images that support server monitoring.

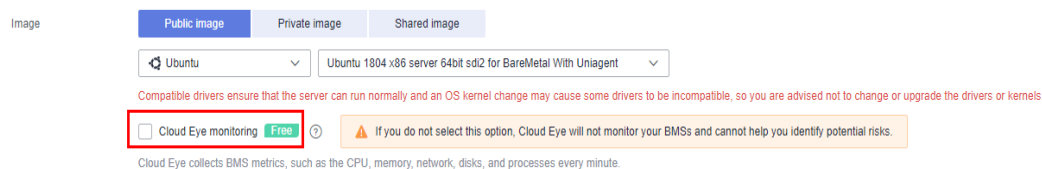
Table 9-1 Linux images that support server monitoring

OS Type (64-bit)	Version
SUSE	Enterprise11 SP4 and Enterprise12 SP1
CentOS	6.9, 7.2, 7.3, 7.4, 7.6, and 7.9
EulerOS	2.2, 2.9
Debian	8.6

Installation Methods

If you use a public image to create a BMS, you can either select **Cloud Eye** during the BMS creation (as shown in [Figure 9-1](#)) or manually install the Agent after the BMS creation. For details, see [Agent Installation and Configuration](#).

Figure 9-1 Installing the Agent during BMS creation



9.2 Monitored Metrics (with Agent Installed)

Description

This section describes monitoring metrics reported by BMS to Cloud Eye as well as their namespaces and dimensions. You can use the management console or APIs provided by Cloud Eye to query the metrics of the monitored objects and alarms generated for BMS.

NOTE

After installing the Agent on a BMS, you can view its OS monitoring metrics. Monitoring data is collected at an interval of 1 minute.

Namespace

SERVICE.BMS

Metrics

Supported BMS **OS Monitoring** metrics include CPU metrics listed in [Table 9-2](#), CPU load metrics listed in [Table 9-3](#), memory metrics listed in [Table 9-4](#), disk metrics listed in [Table 9-5](#), disk I/O metrics listed in [Table 9-6](#), file system metrics listed in [Table 9-7](#), NIC metrics listed in [Table 9-8](#), software RAID metrics listed in [Table 9-9](#), and process metrics in [Table 9-10](#).

NOTE

To monitor software RAID metrics, Agent 1.0.5 or later is required.
Currently, BMSs running the Windows OS cannot be monitored.

Table 9-2 CPU metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_usage_idle	(Agent) Idle CPU Usage	Percentage of time that CPU is idle Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) id value. Unit: percent	0-100%	BMS	1 minute
cpu_usage_other	(Agent) Other Process CPU Usage	Percentage of time that the CPU is used by other processes Formula: Other Process CPU Usage = 1 - Idle CPU Usage - Kernel Space CPU Usage - User Space CPU Usage Unit: percent	0-100%	BMS	1 minute
cpu_usage_system	(Agent) Kernel Space CPU Usage	Percentage of time that the CPU is used by kernel space Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) sy value. Unit: percent	0-100%	BMS	1 minute
cpu_usage_user	(Agent) User Space CPU Usage	Percentage of time that the CPU is used by user space Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) us value. Unit: percent	0-100%	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_usage	(Agent) CPU Usage	CPU usage of the monitored object Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) value. Unit: percent	0-100%	BMS	1 minute
cpu_usage_nice	(Agent) Nice Process CPU Usage	Percentage of time that the CPU is used by the Nice process Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) ni value. Unit: percent	0-100%	BMS	1 minute
cpu_usage_iowait	(Agent) iowait Process CPU Usage	Percentage of time during which the CPU is waiting for I/O operations to complete Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) wa value. Unit: percent	0-100%	BMS	1 minute
cpu_usage_irq	(Agent) CPU Interrupt Time	Percentage of time that the CPU is servicing interrupts Check the metric value changes in the /proc/stat file in a collection period. Run the top command to check the %Cpu(s) hi value. Unit: percent	0-100%	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_usage_softirq	(Agent) CPU Software Interrupt Time	<p>Percentage of time that the CPU is servicing software interrupts</p> <p>Check the metric value changes in the /proc/stat file in a collection period.</p> <p>Run the top command to check the %Cpu(s) value.</p> <p>Unit: percent</p>	0-100%	BMS	1 minute

Table 9-3 CPU load metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
load_average_1	(Agent) 1-Minute Load Average	<p>CPU load averaged from the last 1 minute</p> <p>Obtain its value by dividing the load1/ value in /proc/loadavg by the number of logical CPUs.</p> <p>Run the top command to check the load1 value.</p>	≥ 0	BMS	1 minute
load_average_5	(Agent) 5-Minute Load Average	<p>CPU load averaged from the last 5 minutes</p> <p>Obtain its value by dividing the load5/ value in /proc/loadavg by the number of logical CPUs.</p> <p>Run the top command to check the load5 value in the /proc/loadavg file.</p>	≥ 0	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
load_average_15	(Agent) 15-Minute Load Average	<p>CPU load averaged from the last 15 minutes</p> <p>Obtain its value by dividing the load15/ value in /proc/loadavg by the number of logical CPUs.</p> <p>Run the top command to check the load15 value in the /proc/loadavg file.</p>	≥ 0	BMS	1 minute

Table 9-4 Memory metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mem_available	(Agent) Available Memory	<p>Available memory size of the monitored object</p> <p>Obtain the MemAvailable value by checking the file /proc/meminfo. If it is not displayed in the file:</p> <p>MemAvailable = MemFree + Buffers + Cached</p> <p>Unit: GB</p>	≥ 0 GB	BMS	1 minute
mem_usedPercent	(Agent) Memory Usage	<p>Memory usage of the monitored object</p> <p>Obtain its value by checking the file /proc/meminfo. Memory Usage = (MemTotal - MemAvailable) / MemTotal</p> <p>Unit: percent</p>	0-10 0%	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mem_free	(Agent) Idle Memory	Amount of memory that is not being used Obtain its value by checking the file /proc/meminfo . Unit: GB	≥ 0 GB	BMS	1 minute
mem_buffers	(Agent) Buffer	Memory that is being used for buffers Obtain its value by checking the file /proc/meminfo . Run the top command to check the KiB Mem:buffers value. Unit: GB	≥ 0 GB	BMS	1 minute
mem_cached	(Agent) Cache	Memory that is being used for file caches Obtain its value by checking the file /proc/meminfo . Run the top command to check the KiB Swap:cached Mem value. Unit: GB	≥ 0 GB	BMS	1 minute

Table 9-5 Disk metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mountPointPrefix_disk_free	(Agent) Available Disk Space	<p>Available disk space of the monitored object</p> <p>Run the df -h command to check the data in the Avail column.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: GB</p>	≥ 0 GB	BMS	1 minute
mountPointPrefix_disk_total	(Agent) Disk Storage Capacity	<p>Disk storage capacity of the monitored object</p> <p>Run the df -h command to check the data in the Size column.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: GB</p>	≥ 0 GB	BMS	1 minute
mountPointPrefix_disk_used	(Agent) Used Disk Space	<p>Used disk space of the monitored object</p> <p>Run the df -h command to check the data in the Used column.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: GB</p>	≥ 0 GB	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mountPointPrefix_disk_usedPercent	(Agent) Disk Usage	<p>Disk usage of the monitored object. It is calculated as follows: Disk Usage = Used Disk Space/Disk Storage Capacity.</p> <p>Disk Usage = Used Disk Space/Disk Storage Capacity</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: percent</p>	0-100%	BMS	1 minute

Table 9-6 Disk I/O metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mountPointPrefix_disk_agt_read_bytes_rate	(Agent) Disks Read Rate	<p>Volume of data read from the monitored object per second</p> <p>The disk read rate is calculated by checking data changes in the sixth column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: byte/s</p>	≥ 0 bytes/s	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mountPoint Prefix _disk_ agt_read_ requests_ _rate	(Agent) Disks Read Requests	<p>Number of read requests sent to the monitored object per second</p> <p>The disk read requests are calculated by checking data changes in the fourth column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: request/s</p>	≥ 0	BMS	1 minute
mountPoint Prefix _disk_ agt_write_ bytes_ rate	(Agent) Disks Write Rate	<p>Volume of data written to the monitored object per second</p> <p>The disk write rate is calculated by checking data changes in the tenth column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: byte/s</p>	≥ 0 bytes /s	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mountPointPrefix_disk_agt_write_requests_rate	(Agent) Disks Write Requests	<p>Number of write requests sent to the monitored object per second</p> <p>The disk write requests are calculated by checking data changes in the eighth column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: request/s</p>	≥ 0	BMS	1 minute
disk_readTime	(Agent) Average Read Request Time	<p>Average amount of time that read requests have waited on the disks</p> <p>The average read request time is calculated by checking data changes in the seventh column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: ms/count</p>	≥ 0 ms/Count	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_writeTime	(Agent) Average Write Request Time	<p>Average amount of time that write requests have waited on the disks</p> <p>The average write request time is calculated by checking data changes in the eleventh column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: ms/count</p>	≥ 0 ms/Count	BMS	1 minute
disk_ioUtils	(Agent) Disk I/O Usage	<p>Disk I/O usage of the monitored object</p> <p>Check the data changes in the thirteenth column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: percent</p>	0-100%	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_queue_length	(Agent) Disk Queue Length	<p>Average number of read or write requests to be processed for the monitored disk in the monitoring period</p> <p>The average disk queue length is calculated by checking data changes in the fourteenth column of the corresponding device in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: count</p>	≥ 0	BMS	1 minute
disk_write_bytes_per_operation	(Agent) Average Disk Write Size	<p>Average number of bytes in an I/O write for the monitored disk in the monitoring period</p> <p>The average disk write size is calculated by dividing the data changes in the tenth column of the corresponding device by that of the eighth column in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: KB/op</p>	≥ 0 KB/op	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_read_bytes_per_operation	(Agent) Average Disk Read Size	<p>Average number of bytes in an I/O read for the monitored disk in the monitoring period</p> <p>The average disk read size is calculated by dividing the data changes in the sixth column of the corresponding device by that of the fourth column in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: KB/op</p>	≥ 0 KB/op	BMS	1 minute
disk_io_svc_time	(Agent) Disk I/O Service Time	<p>Average time in an I/O read or write for the monitored disk in the monitoring period</p> <p>The average disk I/O service time is calculated by dividing the data changes in the thirteenth column of the corresponding device by the sum of data changes in the fourth and eighth columns in the /proc/diskstats file in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: ms/op</p>	≥ 0 ms/op	BMS	1 minute

Table 9-7 File system metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_fs_rwstate	(Agent) File System Read/Write Status	Read and write status of the mounted file system of the monitored object Possible values are 0 (read and write) and 1 (read only). Check file system information in the fourth column in the /proc/mounts file.	0 and 1	BMS	1 minute
disk_inodes Total	(Agent) Disk inode Total	Total number of index nodes on the disk Run the df -i command to check information in the Inodes column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	≥ 0	BMS	1 minute
disk_inodes Used	(Agent) Total inode Used	Number of used index nodes on the disk Run the df -i command to check data in the IUsed column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	≥ 0	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_inodesUsedPercent	(Agent) Percentage of Total Inode Used	<p>Percentage of used inodes on the disk</p> <p>Run the df -i command to check data in the IUse% column.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <p>Unit: percent</p>	0-100%	BMS	1 minute

Table 9-8 NIC metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
net_bitRecv	(Agent) Inbound Bandwidth	<p>Number of bits received by this NIC per second</p> <p>Check metric value changes in the /proc/net/dev file in a collection period.</p> <p>Unit: bit/s</p>	≥ 0 bits/s	BMS	1 minute
net_bitSent	(Agent) Outbound Bandwidth	<p>Number of bits sent by this NIC per second</p> <p>Check metric value changes in the /proc/net/dev file in a collection period.</p> <p>Unit: bit/s</p>	≥ 0 bits/s	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
net_packet Recv	(Agent) NIC Packet Receive Rate	Number of packets received by this NIC per second Check metric value changes in the / proc/net/dev file in a collection period. Unit: count/s	≥ 0 count/s/s	BMS	1 minute
net_packet Sent	(Agent) NIC Packet Send Rate	Number of packets sent by this NIC per second Check metric value changes in the / proc/net/dev file in a collection period. Unit: count/s	≥ 0 count/s/s	BMS	1 minute
net_errin	(Agent) Receive Error Rate	Percentage of receive errors detected by this NIC per second Unit: percent	0-100 %	BMS	1 minute
net_errout	(Agent) Transmit Error Rate	Percentage of transmit errors detected by this NIC per second Check metric value changes in the / proc/net/dev file in a collection period. Unit: percent	0-100 %	BMS	1 minute
net_dropin	(Agent) Received Packet Drop Rate	Percentage of packets discarded by this NIC to the total number of packets received by the NIC per second Check metric value changes in the / proc/net/dev file in a collection period. Unit: percent	0-100 %	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
net_dropout	(Agent) Transmitted Packet Drop Rate	Percentage of packets transmitted by this NIC which were dropped per second Check metric value changes in the /proc/net/dev file in a collection period. Unit: percent	0-100 %	BMS	1 minute

Table 9-9 Software RAID metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
md1_status_device:1	(Agent) Status	Software RAID status of the monitored object. Its value is 0 if the RAID is abnormal. Run the plug-in script /usr/local/telescope/plugins/raid-monitor.sh in a collection period. Obtain its value by checking data changes in the /proc/mdstat file and run mdadm -D/dev/md0 (md0 indicates the RAID name).	0 and 1	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
md1_active_device:2	(Agent) Active Disks	Number of active disks in software RAID of the monitored object. Its value is -1 if the RAID is abnormal. Run the plug-in script <code>/usr/local/telescope/plugins/raid-monitor.sh</code> in a collection period. Obtain its value by checking data changes in the <code>/proc/mdstat</code> file and run <code>mdadm -D/dev/md0</code> (<code>md0</code> indicates the RAID name).	$\geq 0, -1$	BMS	1 minute
md1_working_device:2	(Agent) Working Disks	Number of working disks in software RAID of the monitored object. Its value is -1 if the RAID is abnormal. Run the plug-in script <code>/usr/local/telescope/plugins/raid-monitor.sh</code> in a collection period. Obtain its value by checking data changes in the <code>/proc/mdstat</code> file and run <code>mdadm -D/dev/md0</code> (<code>md0</code> indicates the RAID name).	$\geq 0, -1$	BMS	1 minute
md1_failed_device:0	(Agent) Failed Disks	Number of failed disks in software RAID of the monitored object. Its value is -1 if the RAID is abnormal. Run the plug-in script <code>/usr/local/telescope/plugins/raid-monitor.sh</code> in a collection period. Obtain its value by checking data changes in the <code>/proc/mdstat</code> file and run <code>mdadm -D/dev/md0</code> (<code>md0</code> indicates the RAID name).	$\geq 0, -1$	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
md1_spare_device:0	(Agent) Spare Disks	<p>Number of spare disks in software RAID of the monitored object. Its value is -1 if the RAID is abnormal.</p> <p>Run the plug-in script <code>/usr/local/telescope/plugins/raid-monitor.sh</code> in a collection period. Obtain its value by checking data changes in the <code>/proc/mdstat</code> file and run <code>mdadm -D/dev/md0</code> (<code>md0</code> indicates the RAID name).</p>	≥ 0, -1	BMS	1 minute

Table 9-10 Process metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
proc_pHashld_cpu	CPU Usage	<p>CPU consumed by a process. pHashld (process name and process ID) is the value of md5.</p> <p>Check the metric value changes in the <code>/proc/pid/stat</code> file.</p> <p>Unit: percent</p>	0-100 %	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
proc_pHashId_mem	Memory Usage	<p>Memory consumed by a process. pHashId (process name and process ID) is the value of md5.</p> <p>Memory Usage = $RSS \times PAGESIZE / MemTotal$</p> <ul style="list-style-type: none"> Obtain the RSS value by checking the second column of the file /proc/pid/statm. Obtain the PAGESIZE value by running the getconf PAGESIZE command. Obtain the MemTotal value by checking the file /proc/meminfo. <p>Unit: percent</p>	0-100 %	BMS	1 minute
proc_pHashId_file	Opened Files	<p>Number of files opened by a process. pHashId (process name and process ID) is the value of md5.</p> <p>Run the ls -l /proc/pid/fd command to view the number of opened files.</p>	≥ 0	BMS	1 minute
proc_running_count	(Agent) Running Processes	<p>Number of running processes</p> <p>You can obtain the status of each process by checking the Status value in the /proc/pid/status file, and then collect the total number of processes in each state.</p>	≥ 0	BMS	1 minute
proc_idle_count	(Agent) Idle Processes	<p>Number of idle processes</p> <p>You can obtain the status of each process by checking the Status value in the /proc/pid/status file, and then collect the total number of processes in each state.</p>	≥ 0	BMS	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
proc_zombie_count	(Agent) Zombie Processes	Number of zombie processes You can obtain the status of each process by checking the Status value in the /proc/pid/status file, and then collect the total number of processes in each state.	≥0	BMS	1 minute
proc_blocked_count	(Agent) Blocked Processes	Number of blocked processes You can obtain the status of each process by checking the Status value in the /proc/pid/status file, and then collect the total number of processes in each state.	≥0	BMS	1 minute
proc_sleeping_count	(Agent) Sleeping Processes	Number of sleeping processes You can obtain the status of each process by checking the Status value in the /proc/pid/status file, and then collect the total number of processes in each state.	≥0	BMS	1 minute
proc_total_count	(Agent) Total Processes	Total number of processes on the monitored object You can obtain the status of each process by checking the Status value in the /proc/pid/status file, and then collect the total number of processes in each state.	≥0	BMS	1 minute