TaiShan 200 Server (Model 2280)

User Guide

Issue 16

Date 2024-10-18

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/ecolumnsweb/en/warranty-policy

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

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices.* For details about this document, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Huawei Enterprise End User License Agreement

This agreement is the end user license agreement between you (an individual, company, or any other entity) and Huawei for the use of the Huawei Software. Your use of the Huawei Software will be deemed as your acceptance of the terms mentioned in this agreement. For details about this agreement, visit the following web page:
https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

About This Document

Purpose

This document describes the appearance, structure, components, and specifications of the 2280 balanced model of the TaiShan 200 server (TS200-2280 for short), and provides guidance for installing, cabling, powering on, powering off, configuring, and troubleshooting the server and installing an OS.

Intended Audience

This document is intended for:

- Enterprise administrators
- Enterprise end users

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Date	Description
16	2024-10-18	Added temperature and humidity specifications. For details, see **3.2 Environmental Specifications**.
15	2024-07-15	• Added the restrictions on riser cards for the SP686C RAID controller card. For details, see **2.7 Riser Cards and PCIe Slots**. • Added the description of 900 W AC Titanium PSUs' output power. For details, see **3.4 PSU Specifications**. • Added the port description. For details, see **3.1 Technical Specifications**.
14	2024-04-09	• Optimized the "Maintenance and Warranty" section. • Optimized the "Logging In to the Server Using the Independent Remote Console" section.
13	2023-08-11	Added the configuration of the 8 x 2.5-inch SAS/SATA drives in pass-through mode.
12	2023-07-12	Added the configuration of 24 x 2.5-inch drives in RAID pass-through mode.
11	2021-05-31	This issue is the eleventh official release.
10	2021-01-12	Added the 1711 iBMC card information.
09	2020-08-14	Added the 8 x 2.5-inch drive configuration.
08	2020-06-29	Added the "Powered by Kunpeng" label on the front panel.
07	2020-04-15	• Updated the memory specifications of servers powered by Kunpeng 920 5220 or 3210 processors. • Updated the L3 cache capacity of servers powered by Kunpeng 920 5220 or 3210 processors.
06	2020-03-03	Modified the power consumption description.

Issue	Date	Description
05	2020-01-16	• Added information about servers powered by Kunpeng 920 5220 or 3210 processors. • Added information about the WebUIs of iBMC V561 and later versions.
04	2019-12-17	Added the 24 x 2.5-inch SAS/SATA pass-through drive configuration.
03	2019-11-14	• Changed the product name. • Added the FlexIO card with four 25GE optical ports.
02	2019-07-01	Added some server models.
01	2019-06-15	This issue is the first official release.

Contents

1 Overview

The TaiShan 200 servers powered by Huawei Kunpeng 920 processors are dedicated for data centers. The 2280 balanced model (TS200-2280, marked as K22R-02 on the nameplate) is a 2U 2-socket rack server.

It features high-performance computing, large-capacity storage, low power consumption, easy management, and easy deployment, and is ideal for Internet, distributed storage, cloud computing, big data, and enterprise services.

Figure 1-1 shows the appearance of a server with 12 drives.

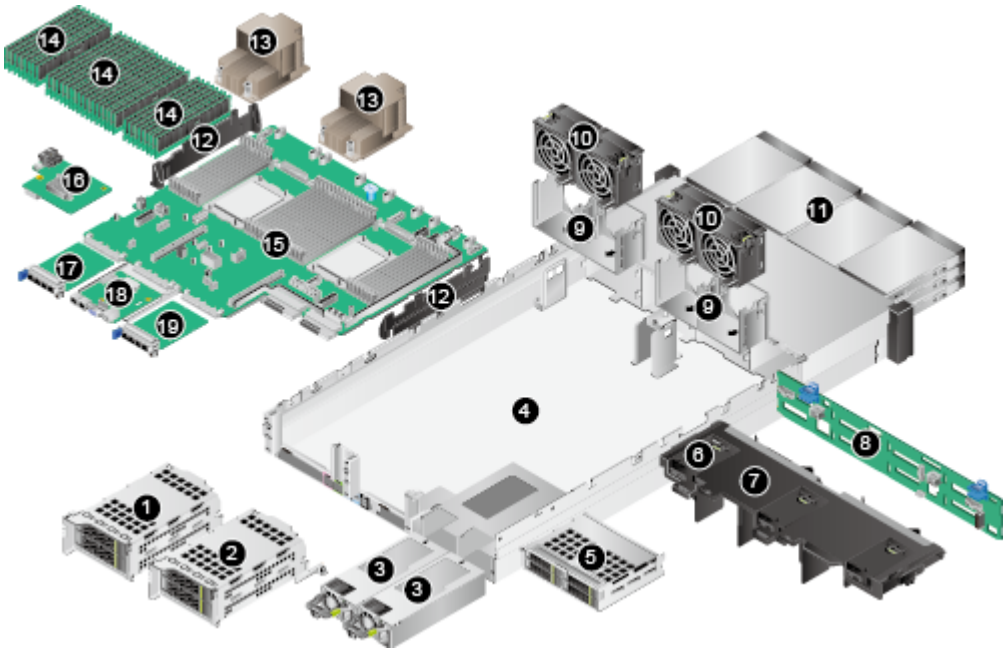
Figure 1-1 Appearance

1.1 Physical Structure

The physical structure of the TS200-2280 server varies depending on the CPU and drive configurations. This chapter uses a server with 12 drives as an example to describe the physical structure of the server with different processors.

When configured with Kunpeng 920 7260 or 5250 processors, the server provides 32 DIMM slots. **Figure 1-2** shows the components of the server.

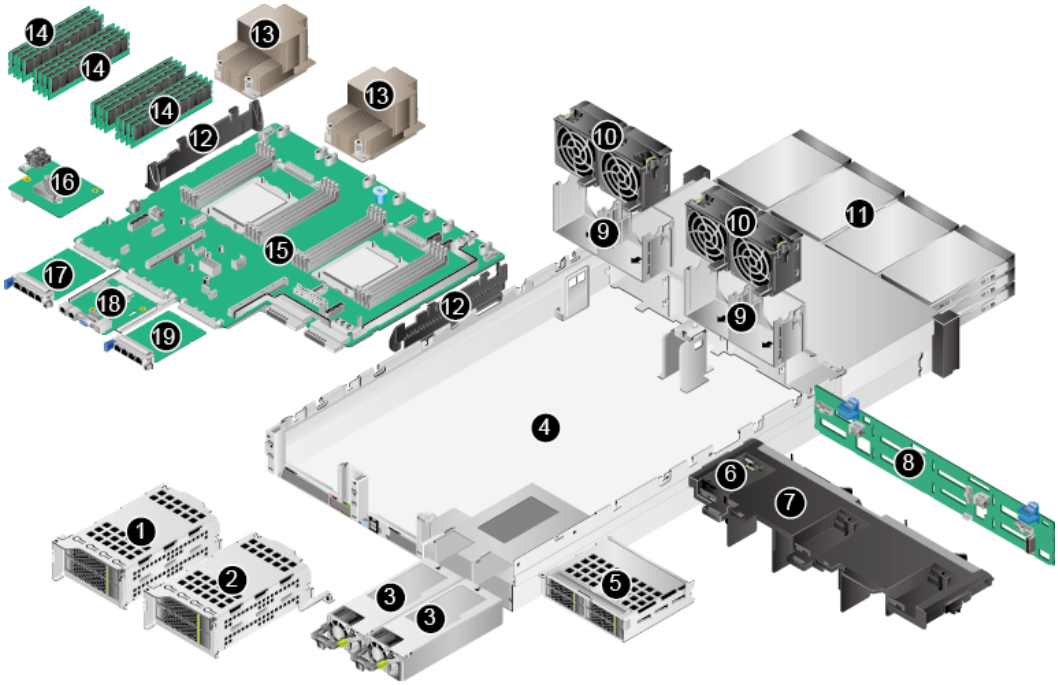
Figure 1-2 Components of the server powered by Kunpeng 920 7260 or 5250 processors



1	I/O module 1	2	I/O module 2
3	Power supply unit (PSU)	4	Chassis
5	I/O module 3	6	Supercapacitor holder
7	Air duct	8	Front-drive backplane
9	Fan module bracket	10	Fan module
11	Front drive	12	Cable organizer
13	Heat sink	14	DIMM
15	Mainboard	16	RAID controller card
17	FlexIO card 1 (connected to CPU 1)	18	iBMC card
19	FlexIO card 2 (connected to CPU 2)	-	-

When configured with Kunpeng 920 5220 or 3210 processors, the server provides 16 DIMM slots. **Figure 1-3** shows the components of the server.

Figure 1-3 Components of the server powered by Kunpeng 920 5220 or 3210 processors



1	I/O module 1	2	I/O module 2
3	Power supply unit (PSU)	4	Chassis
5	I/O module 3	6	Supercapacitor holder
7	Air duct	8	Front-drive backplane
9	Fan module bracket	10	Fan module
11	Front drive	12	Cable organizer
13	Heat sink	14	DIMM
15	Mainboard	16	RAID controller card
17	FlexIO card 1 (connected to CPU 1)	18	iBMC card
19	FlexIO card 2 (connected to CPU 2)	-	-

NOTE

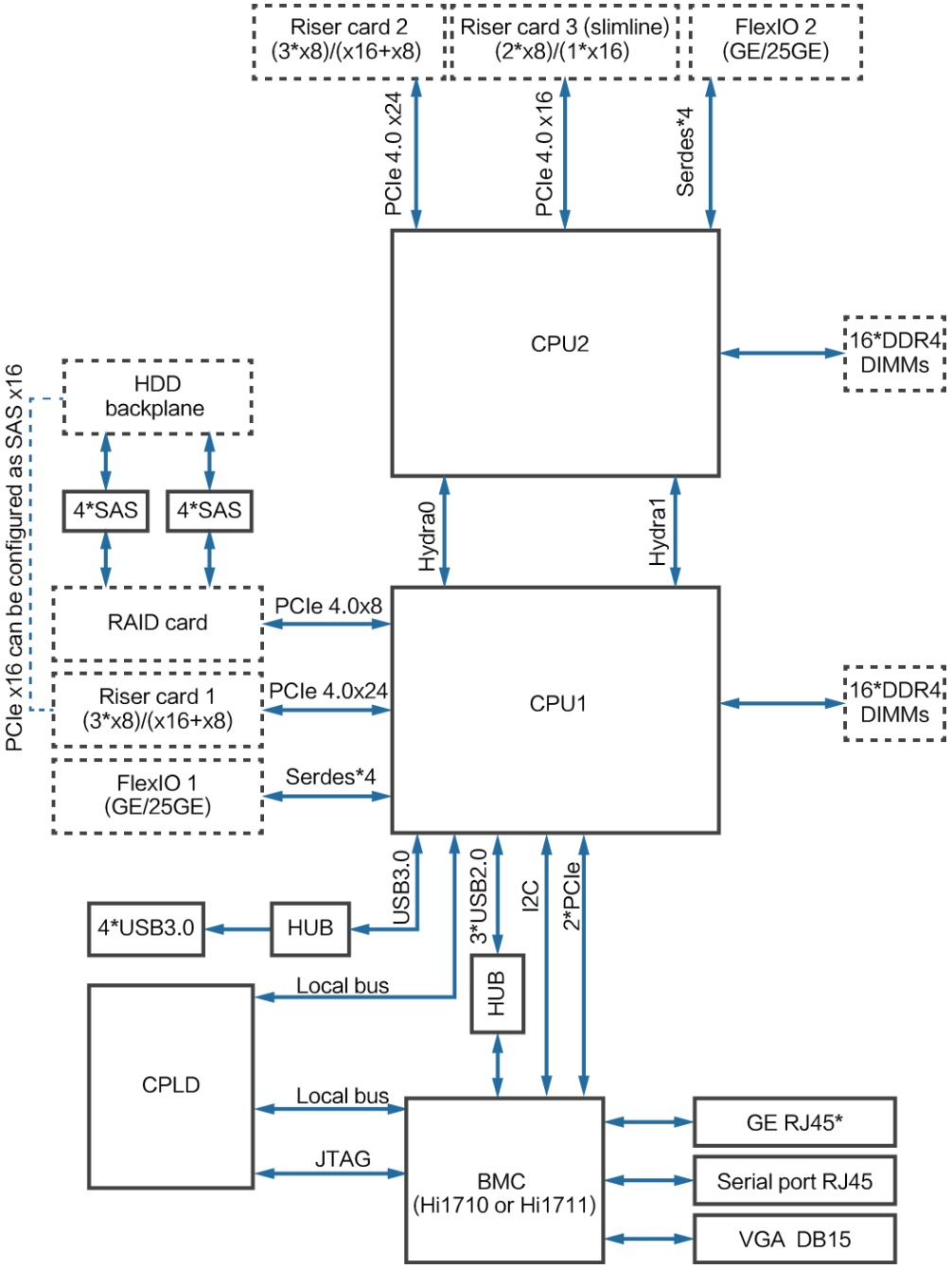
- I/O modules 1, 2, and 3 can be drive modules or riser modules. The preceding figures are for reference only.
- Processors are integrated on the mainboard and cannot be replaced independently.
- For details about the spare parts, use **Computing Product Spare Parts Checker**.

1.2 Logical Structure

The server supports the Hi1710 or Hi1711 iBMC card, which provides ports such as the VGA port, management network port, and commissioning serial port. This document uses the Hi1710 card as an example.

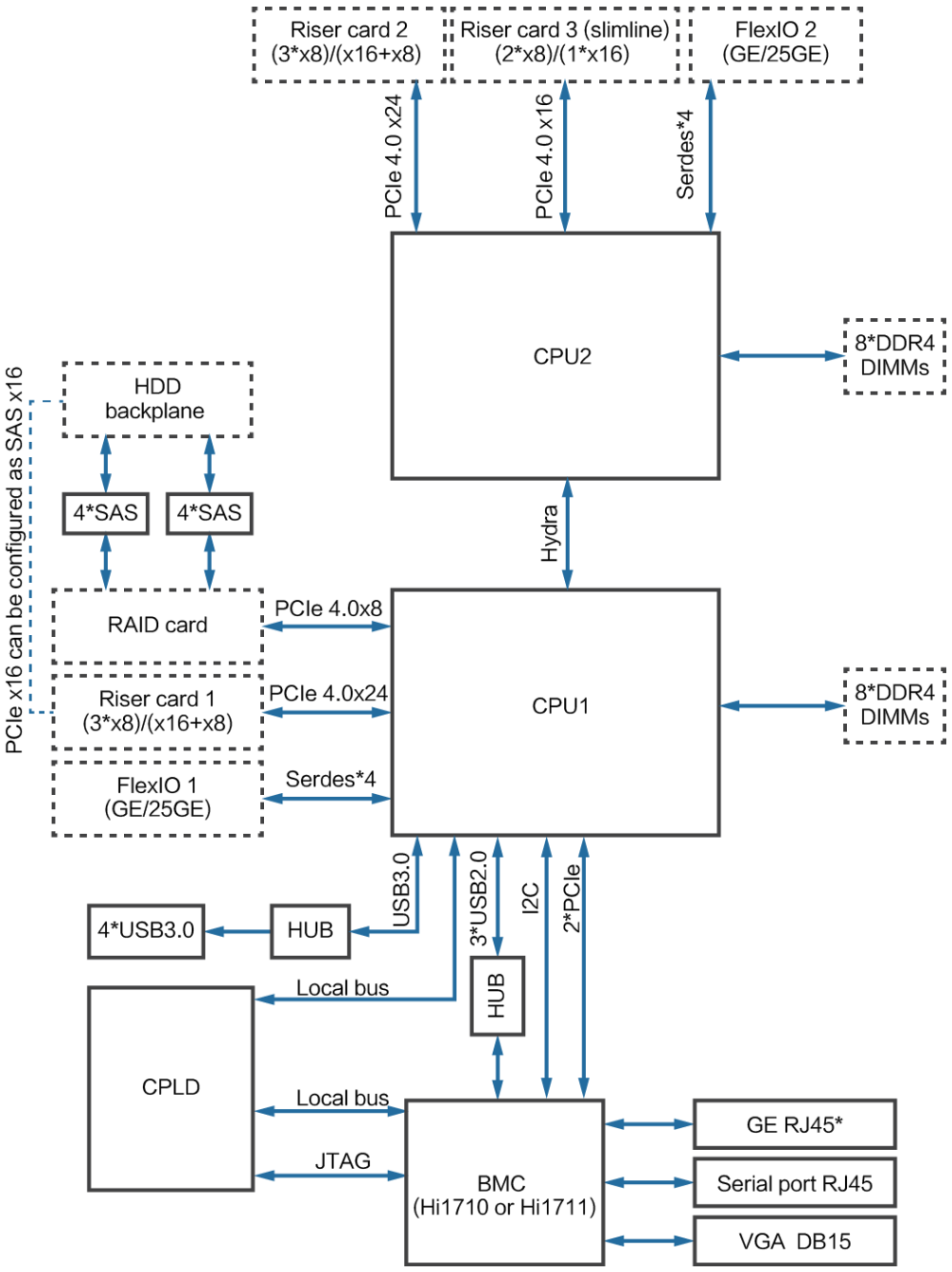
- Figure 1-4 shows the logical structure of the server equipped with Kunpeng 920 7260 or 5250 processors.

Figure 1-4 Logical structure of the server equipped with Kunpeng 920 7260 or 5250 processors



  - The server supports two Huawei Kunpeng 920 7260 or 5250 processors. Each processor can have up to 16 DDR4 DIMMs.
  - CPU 1 and CPU 2 are interconnected through two Hydra buses, both of which provide x8 bandwidth. The maximum transmission rate of a single lane is 30 Gbit/s.
  - The Ethernet FlexIO cards can have four GE or 25GE ports, and are connected to CPUs through high-speed SerDes interfaces.
  - The screw-in RAID controller card connects to CPU 1 through PCIe buses, and to the drive backplanes through SAS signal cables. The server supports flexible drive configurations, depending on the drive backplanes used.
- **Figure 1-5** shows the logical structure of the server equipped with Kunpeng 920 5220 or 3210 processors.

Figure 1-5 Logical structure of the server with Kunpeng 920 5220 or 3210 processors



- The server supports two Huawei Kunpeng 920 5220 or 3210 processors. Each processor can have up to 8 DDR4 DIMMs.
- CPU 1 and CPU 2 are interconnected through one Hydra bus, which provides x8 bandwidth. The maximum transmission rate of a single lane is 30 Gbit/s.
- The Ethernet FlexIO cards can have four GE or 25GE ports, and are connected to CPUs through high-speed SerDes interfaces.
- The screw-in RAID controller card connects to CPU 1 through PCIe buses, and to the drive backplanes through SAS signal cables. The server

supports flexible drive configurations, depending on the drive backplanes used.

2 Components

2.1 Components on the Front Panel

NOTE

For details about the drive numbers and types of the TS200-2280 server, see **2.6.1 Drive Numbers**.

- **Figure 2-1** shows the components on the front panel of a server with 12 x 3.5-inch drives.

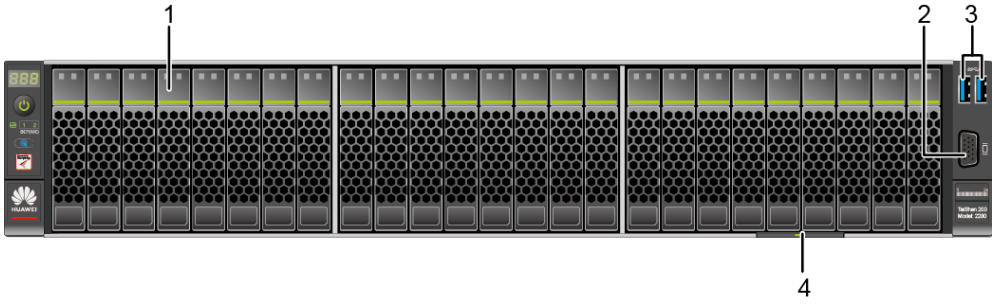
Figure 2-1 Components on the front panel of a server with 12 x 3.5-inch drives

1	Drive	2	VGA port

3	USB 3.0 port	4	Label plate with an SN label

- **Figure 2-2** shows the components on the front panel of a server with 25 x 2.5-inch drives.

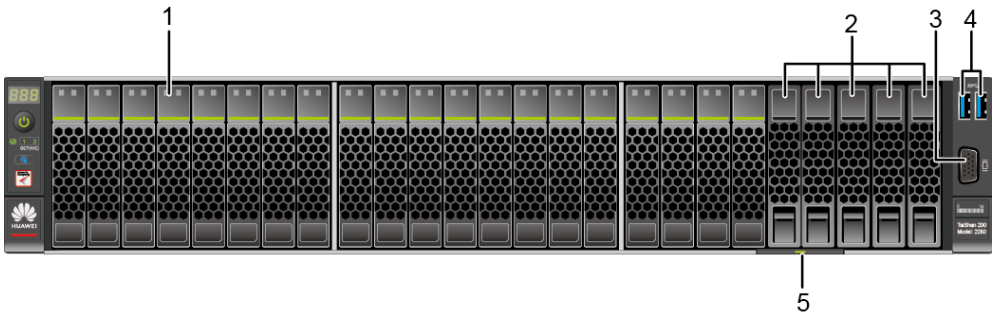
Figure 2-2 Components on the front panel of a server with 25 x 2.5-inch drives



1	Drive	2	VGA port
3	USB 3.0 port	4	Label plate with an SN label

- **Figure 2-3** shows the components on the front panel of a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives.

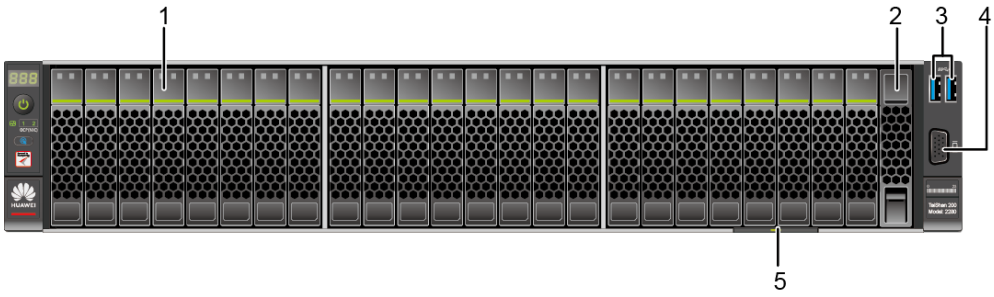
Figure 2-3 Components on the front panel of a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives



1	Drive	2	Filler panel
3	VGA port	4	USB 3.0 port
5	Label plate with an SN label	-	-

- **Figure 2-4** shows the components on the front panel of a server with 24 x 2.5-inch drives.

Figure 2-4 Components on the front panel of a server with 24 x 2.5-inch drives



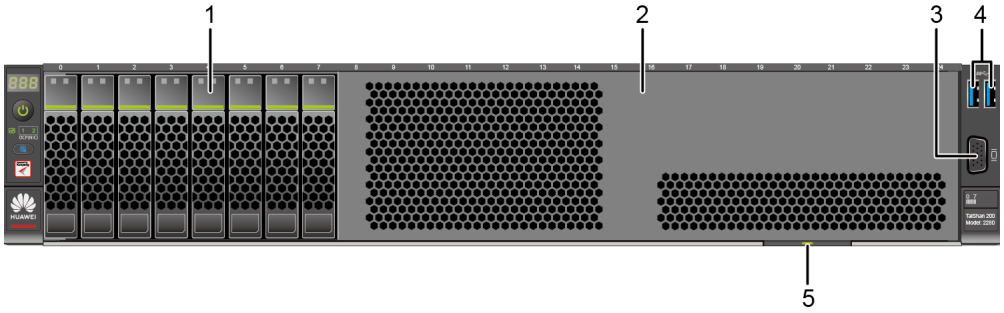
1	Drive	2	Filler panel
3	USB 3.0 port	4	VGA port
5	Label plate with an SN label	-	-

NOTE

Servers powered by Kunpeng 920 5220 or 3210 processors do not support the 24 x 2.5-inch SAS/SATA drive pass-through configuration.

- Figure 2-5 shows the components on the front panel of a server with 8 x 2.5-inch drives.

Figure 2-5 Components on the front panel of a server with 8 x 2.5-inch drives



1	Drive	2	Filler panel
3	VGA port	4	USB 3.0 port
5	Label plate with an SN label	-	-

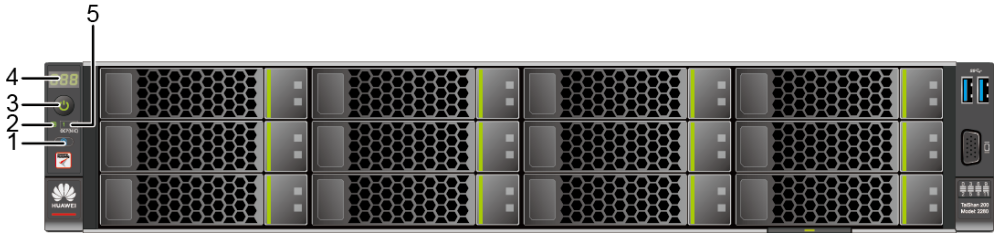
Table 2-1 Ports on the front panel

Port	Type	Description
USB port	USB 3.0	The USB ports allow USB devices to be connected to the server. **NOTE** • Before connecting an external USB device, check that the USB device functions properly. A server may operate improperly if an abnormal USB device is connected. • If an external USB device is used, the maximum length of the extension cable is 1 m. • If USB devices, including USB flash drives and portable drives, are not detected, contact Huawei technical support.
VGA port	DB15	The VGA port is connected to a terminal, such as a monitor or physical KVM. **NOTE** The VGA port on the front panel does not have cable screws, and the VGA cable is easy to disconnect. Therefore, you are advised to use the VGA port on the rear panel.

2.2 Indicators and Buttons on the Front Panel

- Figure 2-6 shows the indicators and buttons on the front panel of a server with 12 x 3.5-inch drives.

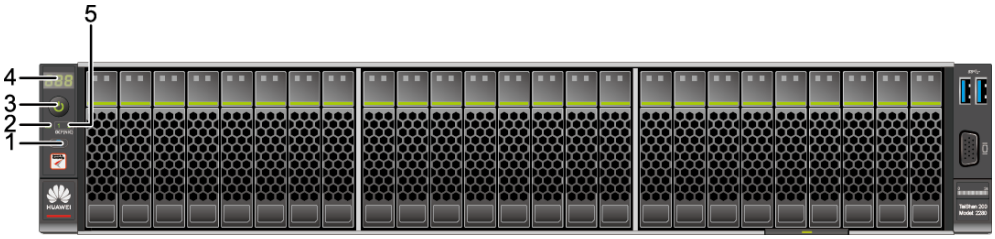
  Figure 2-6 Indicators and buttons on the front panel of a server with 12 x 3.5-inch drives

1	UID button/indicator	2	Health indicator
3	Power button/ indicator	4	Fault diagnostic LED
5	FlexIO card presence indicators (1 and 2)	-	-

- Figure 2-7 shows the indicators and buttons on the front panel of a server with 25 x 2.5-inch drives.

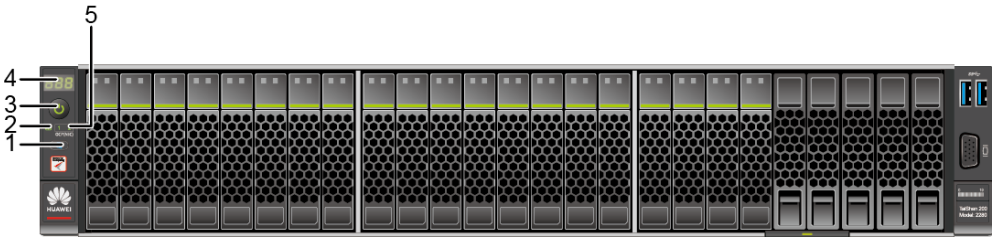
Figure 2-7 Indicators and buttons on the front panel of a server with 25 x 2.5-inch drives



1	UID button/indicator	2	Health indicator
3	Power button/ indicator	4	Fault diagnostic LED
5	FlexIO card presence indicators (1 and 2)	-	-

- Figure 2-8 shows the indicators and buttons on the front panel of a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives.

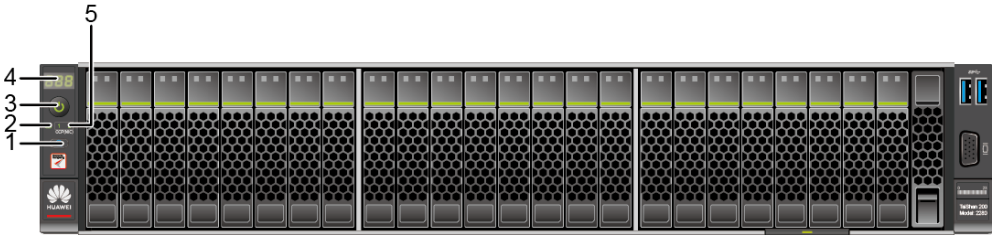
Figure 2-8 Indicators and buttons on the front panel of a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives



1	UID button/indicator	2	Health indicator
3	Power button/ indicator	4	Fault diagnostic LED
5	FlexIO card presence indicators (1 and 2)	-	-

- Figure 2-9 shows the indicators and buttons on the front panel of a server with 24 x 2.5-inch drives.

Figure 2-9 Indicators and buttons on the front panel of a server with 24 x 2.5-inch drives



1	UID button/indicator	2	Health indicator
3	Power button/ indicator	4	Fault diagnostic LED

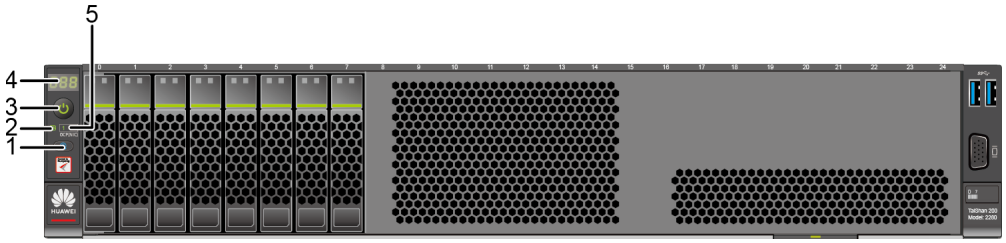
5	FlexIO card presence indicators (1 and 2)	-	-

NOTE

Servers powered by Kunpeng 920 5220 or 3210 processors do not support the 24 x 2.5-inch SAS/SATA drive pass-through configuration.

- Figure 2-10 shows the indicators and buttons on the front panel of a server with 8 x 2.5-inch drives.

Figure 2-10 Indicators and buttons on the front panel of a server with 8 x 2.5-inch drives



1	UID button/indicator	2	Health indicator
3	Power button/ indicator	4	Fault diagnostic LED
5	FlexIO card presence indicators (1 and 2)	-	-

Table 2-2 Indicators and buttons on the front panel

Silkscreen	Indicator/ Button	State Description
888	Fault diagnostic LED	• ---: The server is operating properly. • Error code: A server component is faulty. For details about error code, see **TaiShan Rack Server iBMC Alarm Handling**.

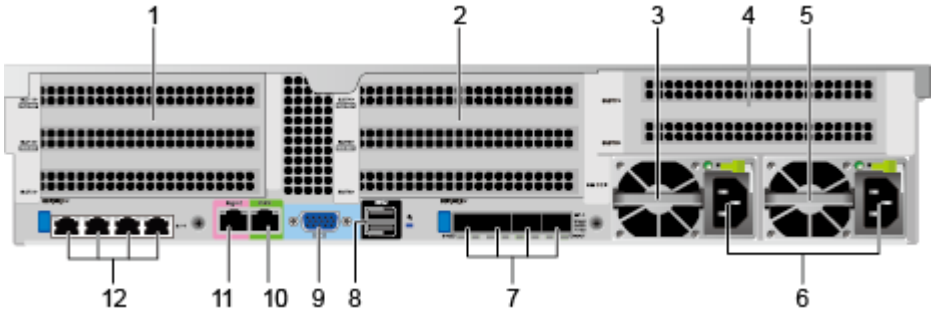
Silkscreen	Indicator/ Button	State Description
	Power button/ indicator	Power indicator ● Steady yellow: The server is in the standby state. ● Steady green: The server is properly powered on. ● Blinking yellow: The iBMC is starting. ● Off: The server is not powered on. Power indicator ● When the server is powered on, you can press this button to shut down the OS. ● When the server is powered on, you can hold down this button for 6 seconds to force the server to power off. ● When the server is in the standby state, you can press this button to start the server.
	UID button/ indicator	The UID button/indicator helps locate a device. UID indicator: ● Off: The server is not being located. ● Blinking blue (for 255 seconds): The server has been located and is differentiated from other servers that have also been located. ● Steady blue: The server is being located. **NOTE** ● After the iBMC is initialized, the UID indicator restores to the default Off state. You can press the UID button to relocate the server. ● The blinking continues for 255 seconds for each setting on the iBMC. After 255 seconds, the indicator is off. UID button: ● You can turn on, turn off, or blink the UID indicator by pressing the UID button on the panel or by using the iBMC CLI or WebUI. ● You can press this button to turn on or off the UID indicator. ● You can press and hold down this button for about 5 seconds to reset the iBMC.
	Health indicator	● Steady green: The server is operating properly. ● Blinking red at 1 Hz: A major alarm has been generated on the server. ● Blinking red at 5 Hz: A critical alarm has been generated on the server.

Silkscreen	Indicator/ Button	State Description
	FlexIO card presence indicators (1 and 2)	• 1 indicates FlexIO card 1, and 2 indicates FlexIO card 2. • Steady green: The FlexIO card is installed and is identified. • Off: The FlexIO card is not installed or is faulty.

2.3 Components on the Rear Panel

Figure 2-11 shows the components on the rear panel of the TS200-2280 server.

Figure 2-11 Components on the rear panel



1	I/O module 1	2	I/O module 2
3	PSU 1	4	I/O module 3
5	PSU 2	6	PSU socket
7	FlexIO card 2 (connected to CPU 2)	8	USB 3.0 port
9	VGA port	10	Serial port
11	Management network port	12	FlexIO card 1 (connected to CPU 1)

NOTE

- The preceding figure is for reference only.
- FlexIO cards 1 and 2 are not hot-swappable. If you need to replace them, power off the server first.

Table 2-3 Ports on the rear panel

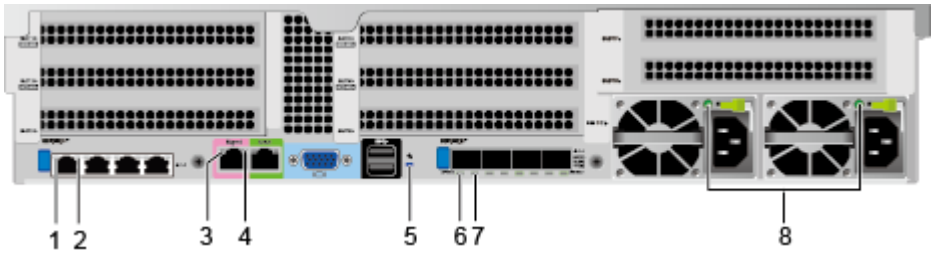
Port	Type	Quantity	Description
VGA port	DB15	1	The VGA port is connected to a display terminal, such as a monitor or a physical KVM.
USB port	USB 3.0	2	The USB ports allow USB devices to be connected to the server. **NOTE** • Before connecting an external USB device, check that the USB device functions properly. A server may operate improperly if an abnormal USB device is connected. • If an external USB device is used, the maximum length of the extension cable is 1 m. • If USB devices, including USB flash drives and portable drives, are not detected, contact Huawei technical support.
Management network port	RJ45	1	This 1000 Mbit/s Ethernet port is used for server management. It supports 10/100/1000 Mbit/s auto-negotiation.
Serial port	RJ45	1	The serial port is used as the system serial port by default. You can set it as the iBMC serial port using CLI commands. It is used mainly for debugging.
GE electrical port	RJ45	4/8	• Each FlexIO card provides four GE electrical ports. Two FlexIO cards provide up to eight GE electrical ports. • The server provides a 1000 Mbit/s Ethernet port and supports 10/100/1000 Mbit/s auto-negotiation.
25GE optical port	SFP28	4	A FlexIO card provides a maximum of four 25GE optical ports. **NOTE** The 25GE optical ports support auto-negotiation to 10GE, and optical modules of different rates are required.

Port	Type	Quantity	Description
PSU socket	-	1/2	• Determine the number of PSUs based on actual requirements, but ensure that the rated power of the PSUs is greater than that of the server. • You are advised to configure two PSUs to ensure reliable device operating. When one PSU is used, **Predicted PSU Status** or **Power Supply Settings** cannot be set to **Active/Standby** on the iBMC WebUI.

2.4 Indicators on the Rear Panel

Figure 2-12 shows the indicators on the rear panel of the TS200-2280 server.

Figure 2-12 Indicators on the rear panel



1	FlexIO card indicator	2	FlexIO card indicator
3	Management network port data transmission status indicator	4	Management network port connection status indicator
5	UID indicator	6	FlexIO card indicator
7	FlexIO card indicator	8	PSU indicator

For details about the FlexIO card indicators, see **2.5 FlexIO Cards**.

Table 2-4 Indicators on the rear panel

Indicator		State Description
Management network port	Data transmission status indicator	• Blinking yellow: Data is being transmitted. • Off: No data is being transmitted.

Indicator		State Description
	Connection status indicator	• Steady green: The network port is properly connected. • Off: The network is not connected.
UID indicator		The UID indicator helps locate a device. • Off: The server is not being located. • Blinking blue (for 255 seconds): The server has been located and is differentiated from other servers that have also been located. • Steady blue: The server is being located. **NOTE** • After the iBMC is initialized, the UID indicator restores to the default Off state. You can press the UID button to relocate the server. • The blinking continues for 255 seconds for each setting on the iBMC. After 255 seconds, the indicator is off.
25GE optical port	Transmission rate indicator	• Steady green: The data transmission rate is 25 Gbit/s. • Steady yellow: The data transmission rate is 10 Gbit/s. • Off: The network is not connected.
	Connection status indicator/Data transmission status indicator	• Steady green: The network port is properly connected. • Blinking green: Data is being transmitted. • Off: The network is not connected.

Indicator	State Description
PSU indicator	• Steady green: The power input and output are normal. • Steady orange: The input is normal, but no power is output due to overheat protection, overcurrent protection, short circuit protection, output overvoltage protection, or some component failures. • Blinking green at 1 Hz: – The input is normal and the server is in the standby state. – The input is overvoltage or undervoltage. For details, see **TaiShan Servers Troubleshooting**. • Blinking green at 4 Hz: The PSU firmware is being upgraded online. • Off: There is no power input.

2.5 FlexIO Cards

For details about FlexIO cards supported by the server, use the **Computing Product Compatibility Checker**. For details about the specifications and features of each FlexIO card, see their white paper.

Figure 2-13 TM210 with four GE electrical ports

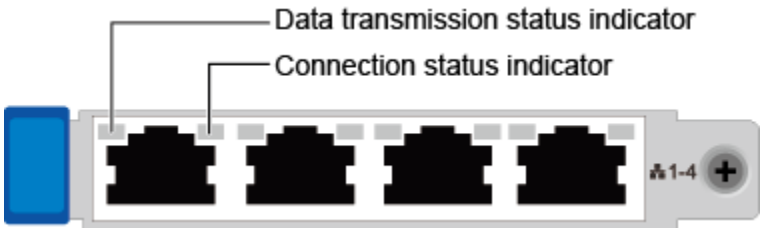


Figure 2-14 TM280 with four 25GE optical ports

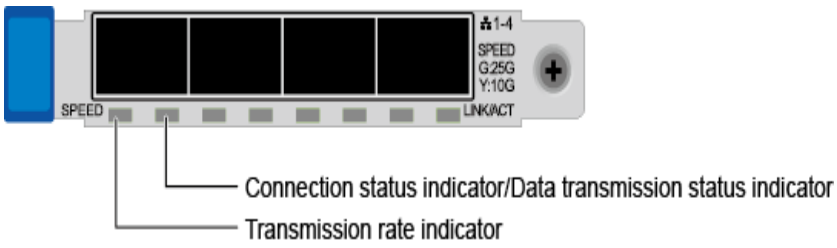


Table 2-5 FlexIO card indicators

NIC Type	Indicator	State Description
FlexIO card with four GE electrical ports	Data transmission status indicator	• Steady yellow: The network port is in active status. • Blinking yellow: Data is being transmitted. • Off: No data is being transmitted.
	Connection status indicator	• Steady green: The network port is properly connected. • Off: The network port is not connected.
FlexIO card with four 25GE optical ports	Transmission rate indicator	• Steady green: The data transmission rate is 25 Gbit/s. • Steady yellow: The data transmission rate is 10 Gbit/s. • Off: The network port is not connected.
	Connection status indicator/Data transmission status indicator	• Steady green: The network port is properly connected. • Blinking green: Data is being transmitted. • Off: The network port is not connected.

2.6 Drive Numbers and Indicators

2.6.1 Drive Numbers

- **Figure 2-15** shows the drive numbers of a server with the 12 x 3.5-inch drive expander configuration.

Figure 2-15 Drive numbers of a server with the 12 x 3.5-inch drive expander configuration

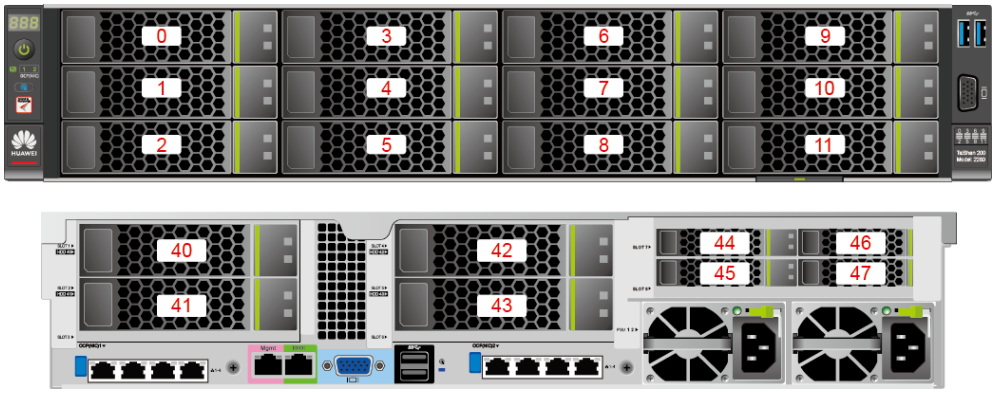
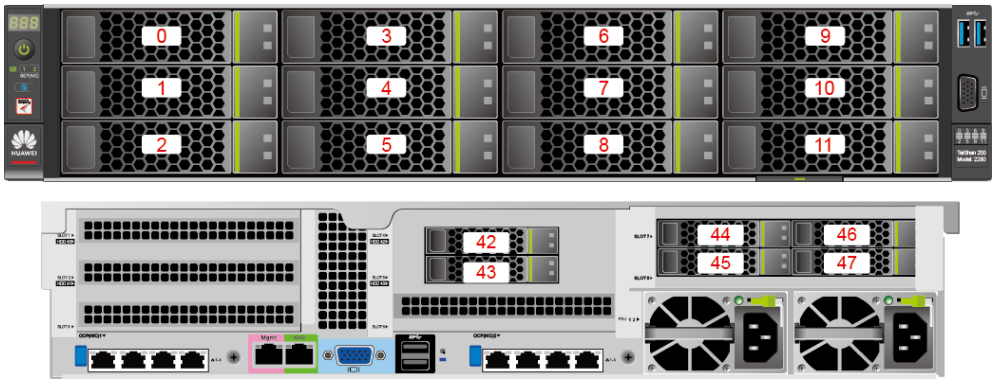


Table 2-6 Drive numbers of a server with the 12 x 3.5-inch drive expander configuration

Physical Drive Number	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
40	Disk40	12
41	Disk41	13
42	Disk42	14
43	Disk43	15

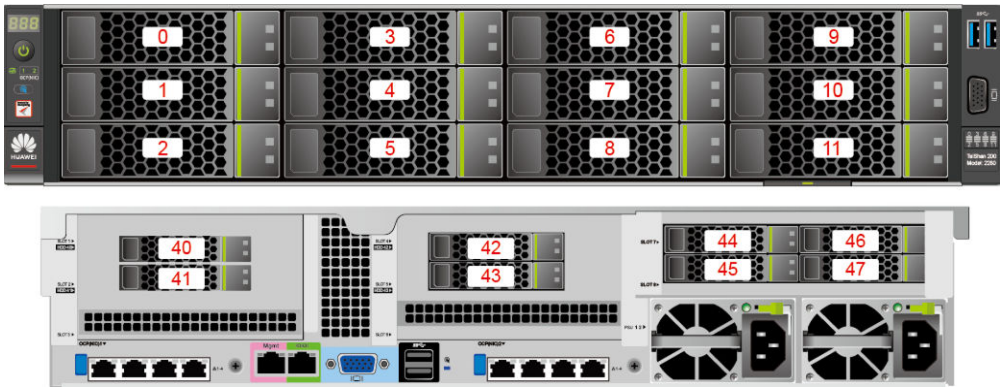
- **Figure 2-16** shows the drive numbers of a server with the 12 x 3.5-inch drive pass-through configuration.

Figure 2-16 Drive numbers of a server with the 12 x 3.5-inch drive pass-through configuration



- **Figure 2-17** shows the drive numbers of a server with the 12 x 3.5-inch drive RAID pass-through configuration.

Figure 2-17 Drive numbers of a server with the 12 x 3.5-inch drive RAID pass-through configuration



- **Figure 2-18** shows the drive numbers of a server with the 25 x 2.5-inch drive expander configuration.

Figure 2-18 Drive numbers of a server with the 25 x 2.5-inch drive expander configuration

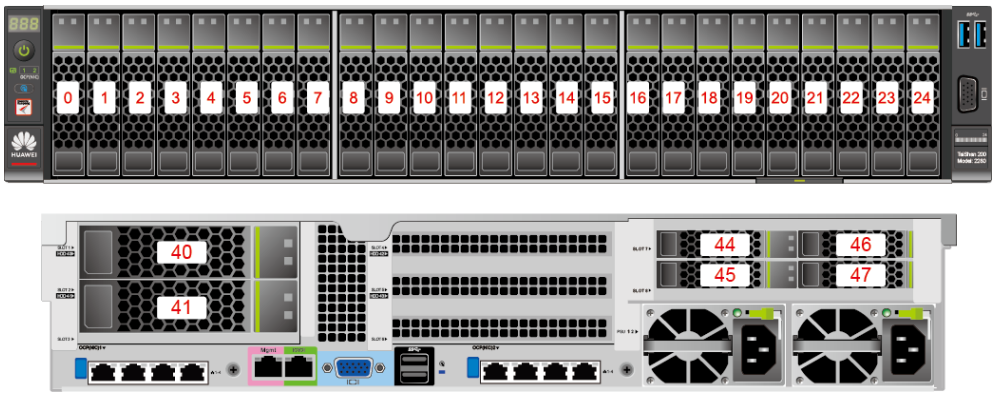
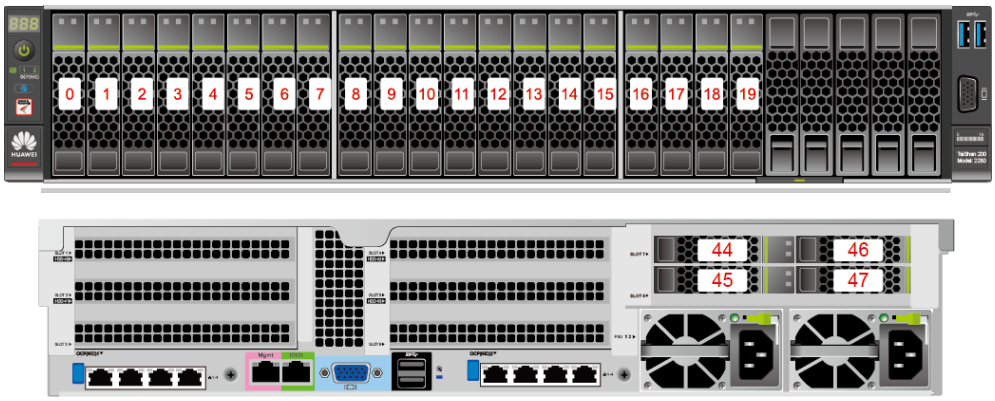


Table 2-7 Drive numbers of a server with the 25 x 2.5-inch drive expander configuration

Physical Drive Number	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
40	Disk40	25
41	Disk41	26

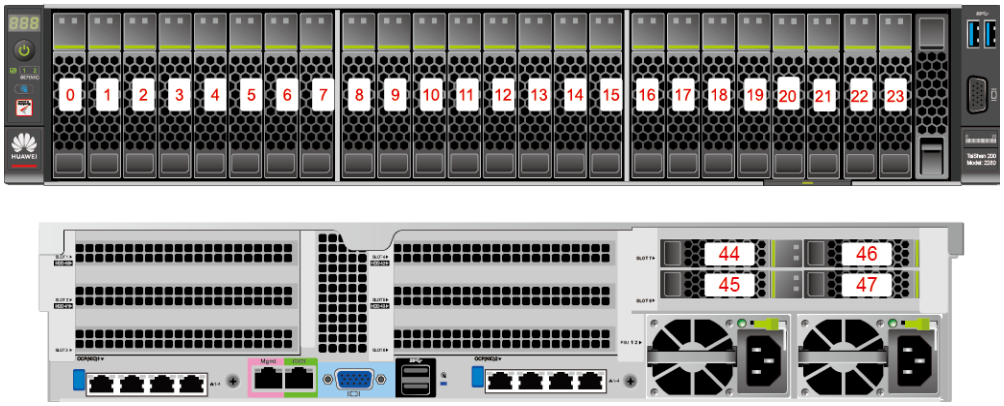
- **Figure 2-19** shows the drive numbers of a server equipped with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives.

Figure 2-19 Drive numbers of a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives



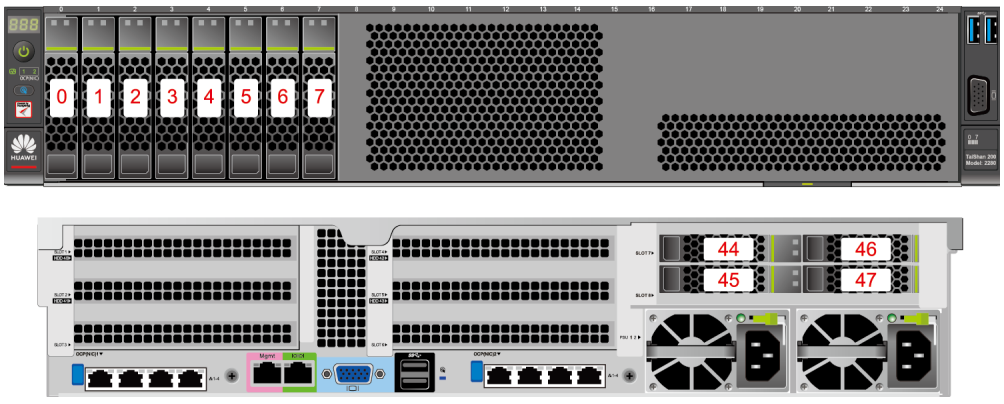
- **Figure 2-20** shows the drive numbers of a server with the 24 x 2.5-inch drive pass-through configuration.

Figure 2-20 Drive numbers of a server with the 24 x 2.5-inch drive pass-through configuration



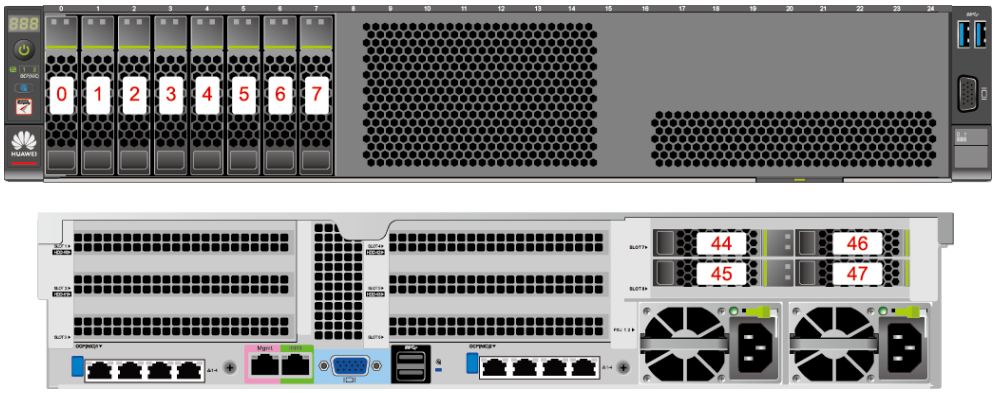
- **Figure 2-21** shows the drive numbers of a server with the 8 x 2.5-inch drive RAID pass-through configuration.

Figure 2-21 Drive numbers of a server with the 8 x 2.5-inch drive RAID pass-through configuration



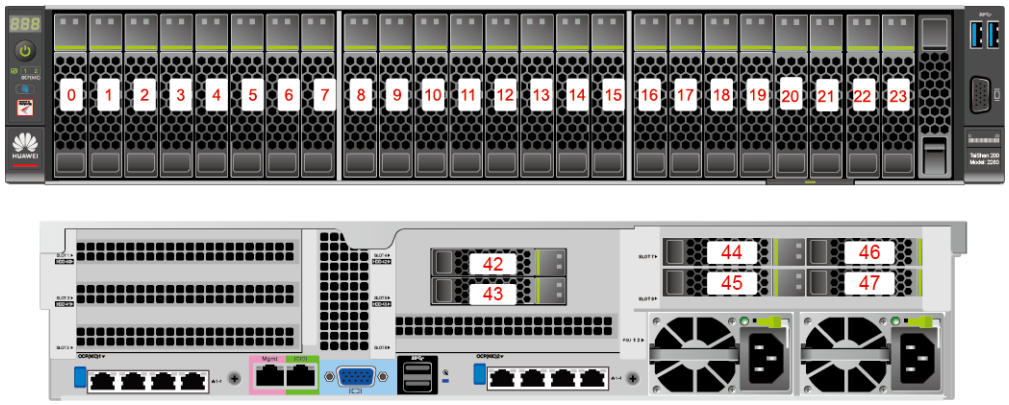
- **Figure 2-22** shows the drive numbers of a server with the 8 x 2.5-inch drive pass-through configuration.

Figure 2-22 Drive numbers of a server with the 8 x 2.5-inch drive pass-through configuration



- Figure 2-23 shows the drive numbers of a server with the 24 x 2.5-inch drive RAID pass-through configuration.

Figure 2-23 Drive numbers of a server with the 24 x 2.5-inch drive RAID pass-through configuration



2.6.2 Drive Configurations

Table 2-8 Drive configurations

Configuration	Maximum Front Drives	Maximum Rear Drives	Drive Management Mode
25 x 2.5-inch drive expander configuration[1]	25 (SAS/SATA drives)	• I/O module 1: 2 (SAS/SATA drives) • I/O module 3[2]: 4 (NVMe drives)	One RAID controller card[6]
12 x 3.5-inch drive expander configuration[1]	12 (SAS/SATA drives)	• I/O module 1: 2 (SAS/SATA drives) • I/O module 2: 2 (SAS/SATA drives) • I/O module 3[2]: 4 (NVMe drives)	RAID controller card[11]

Configuration	Maximum Front Drives	Maximum Rear Drives	Drive Management Mode
12 x 3.5-inch drive pass-through configuration[1, 3]	12 (SAS/SATA drives)	• I/O module 2: 2 (SAS/SATA drives) • I/O module 3[2]: 4 (NVMe drives)	CPU over SAS
12 x 3.5-inch drive RAID pass-through configuration[1]	12 (SAS/SATA drives)	• I/O module 1: 2 (SAS/SATA drives) • I/O module 2: 2 (SAS/SATA drives) • I/O module 3: 4 (NVMe drives)	One PCIe plug-in RAID controller card[7]
8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives[1]	20 • Slots 0 to 7 support only SAS/SATA drives. • Slots 8 to 19 support only NVMe drives.[4]	I/O module 3[2]: 4 (NVMe drives)	One RAID controller card[8]
24 x 2.5-inch drive pass-through configuration[1, 5]	24 (SAS/SATA drives)	I/O module 3[2]: 4 (NVMe drives)	CPU over SAS
8 x 2.5-inch drive RAID pass-through configuration[1]	8 (SAS/SATA drives)	I/O module 3[2]: 4 (NVMe drives)	One RAID controller card[6]
24 x 2.5-inch drive RAID pass-through configuration[9]	24 (SAS/SATA drives)	• I/O module 2: 2 (SAS/SATA drives) • I/O module 3[2]: 4 (NVMe drives)	One PCIe plug-in RAID controller card[10]
8 x 2.5-inch drive pass-through configuration[1]	8 (SAS/SATA drives)	I/O module 3[2]: 4 (NVMe drives)	CPU over SAS

Configuration	Maximum Front Drives	Maximum Rear Drives	Drive Management Mode
• [1]: A server with 24 x 2.5-inch drive pass-through configuration, 8 x 2.5-inch drive pass-through configuration, 25 x 2.5-inch drive expander configuration, or 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drive configuration supports only 2.5-inch front drives. A server with 12 x 3.5-inch drive RAID pass-through configuration, 12 x 3.5-inch drive expander configuration, or 12 x 3.5-inch drive pass-through configuration supports only 3.5-inch front drives. • [2]: I/O module 3 supports 2.5-inch NVMe drives through the PCIe signals directly from CPU 2. I/O modules 1 and 2 support 2.5-inch and 3.5-inch drives. • [3]: CPU over SAS pass-through requires a SAS riser card. By default, it is installed in I/O module 2. • [4]: The NVMe drives in slots 8 to 19 of a server equipped with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives support PCIe 4.0. • [5]: A server powered by Kunpeng 920 5220 or 3210 processors does not support the 24 x 2.5-inch SAS/SATA drive pass-through configuration. • [6]: The server supports PCIe plug-in and screw-in RAID controller cards. It is recommended that the PCIe plug-in RAID controller card be installed in slot 3. • [7]: The PCIe plug-in RAID controller card can be installed in slot 3. • [8]: The server supports screw-in and PCIe plug-in RAID controller cards. Slot 8 is recommended for a PCIe plug-in RAID controller card (slot 7 recommended for an SP686C RAID controller card). If a PCIe plug-in RAID controller card is installed, one IO3 slot is occupied. In this case, IO3 does not support NVMe drives. • [9]: This configuration requires the riser module shown in **Figure 2-27**. • [10]: The PCIe plug-in RAID controller card is installed in slot 2. • [11]: The server supports two PCIe plug-in RAID controller cards. If the server is managed by only one RAID controller card, it can be a PCIe plug-in RAID controller card or a screw-in RAID controller card. If it is a PCIe plug-in RAID controller card, install it in slot 3.			

2.6.3 SAS/SATA Drive Indicators

Figure 2-24 SAS/SATA drive indicators

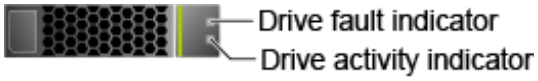


Table 2-9 Drive indicators

Drive Activity Indicator (Green Indicator)	Drive Fault Indicator (Yellow Indicator)	Description
Steady on	Off	The drive is in position.
Blinking at 4 Hz	Off	Data is being read or written properly, or data on the primary drive is being rebuilt.
Steady on	Blinking at 1 Hz	The drive is being located by the RAID controller card.
Blinking at 1 Hz	Blinking at 1 Hz	The data on the secondary drive is being rebuilt.
Off	Steady on	A member drive in the RAID array is removed.
Steady on	Steady on	A member drive in the RAID array is faulty.

2.6.4 NVMe Drive Indicators

Figure 2-25 NVMe drive indicators

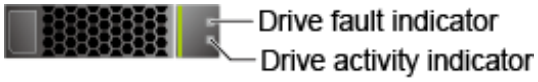


Table 2-10 NVMe drive indicators

Drive Activity Indicator (Green Indicator)	Drive Fault Indicator (Yellow Indicator)	State Description
Off	Off	The NVMe drive is not detected.
Steady green	Off	The NVMe drive is detected and is working properly.
Blinking green at 2 Hz	Off	Data is being read from or written to the NVMe drive.
Off	Blinking yellow at 2 Hz	The NVMe drive is being located or hot-swapped.
Off	Blinking yellow at 0.5 Hz	The NVMe drive completes the hot removal process and is removable.
Steady green or off	Steady yellow	The NVMe drive is faulty.

NOTE

The indicator status of some NVMe drive models during hot swap is different from that listed in Table 2-10. The differences include but are not limited to the following:

- When a drive is being hot swapped, the green indicator blinks at 2 Hz and the yellow indicator also blinks at 2 Hz.
- When the hot swap process is complete and the drive is removable, the green indicator is steady on and the yellow indicator blinks at 0.5 Hz.

2.6.5 RAID Levels

Table 2-11 lists the performance of different RAID levels, the minimum number of drives required, and the drive utilization.

Table 2-11 RAID levels

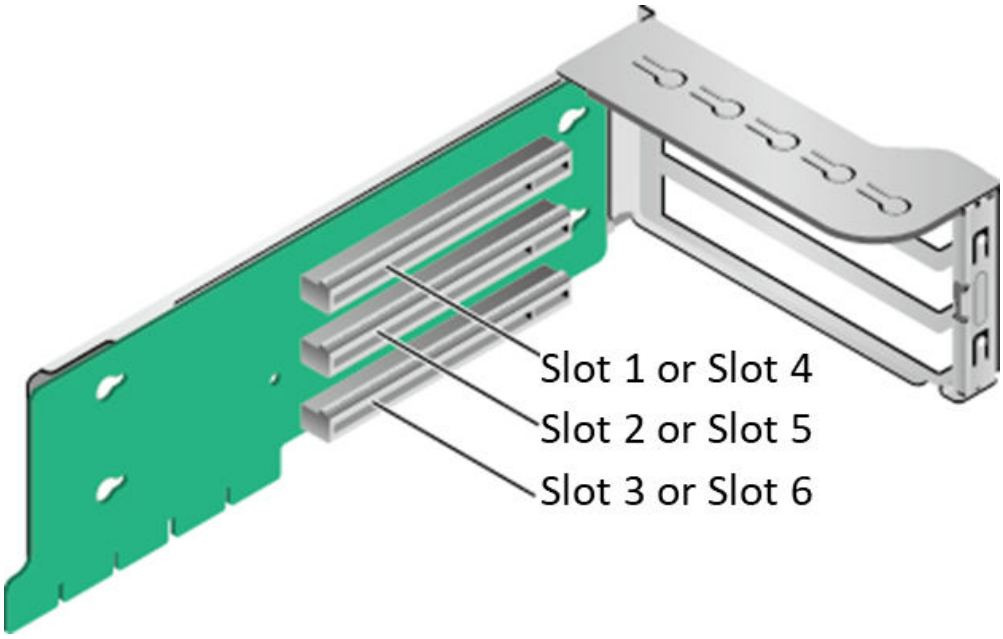
RAID Level	Reliability	Read Performance	Write Performance	Drive Usage
RAID 0	Low	High	High	100%
RAID 1	High	High	Medium	50%
RAID 5	Relatively high	High	Medium	(N – 1)/N
RAID 6	Relatively high	High	Medium	(N – 2)/N
RAID 10	High	High	Medium	50%
RAID 50	High	High	Relatively high	(N – M)/N
RAID 60	High	High	Relatively high	(N – M x 2)/N
Note: N indicates the number of member drives in the RAID array, and M indicates the number of spans in the RAID array.				

2.7 Riser Cards and PCIe Slots

Figure 2-26, Figure 2-27, Figure 2-28, Figure 2-30, and Figure 2-31 show the riser cards supported by I/O modules 1 and 2.

- The riser card shown in Figure 2-26 can be installed in I/O module 1 or 2. If installed in I/O module 1, the riser card uses PCIe slots 1 to 3. If installed in I/O module 2, the riser card uses PCIe slots 4 to 6.

Figure 2-26 3x8 riser card (board No.: BC82PRUA)

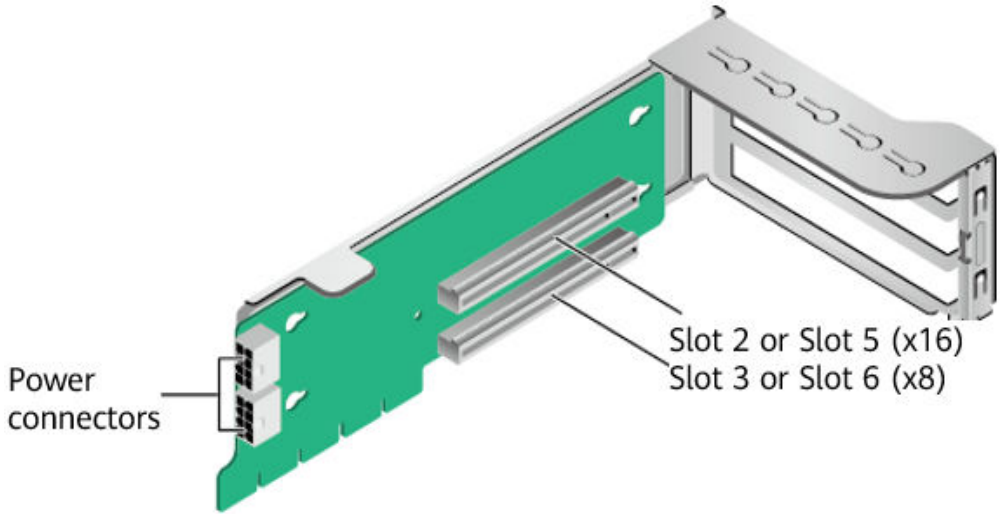


- The riser card shown in **Figure 2-27** supports full-height full-length dual-width GPUs and SDI cards. It uses PCIe slots 2 and 3 when the riser card is installed in I/O module 1 and PCIe slots 5 and 6 when installed in I/O module 2.

  NOTE

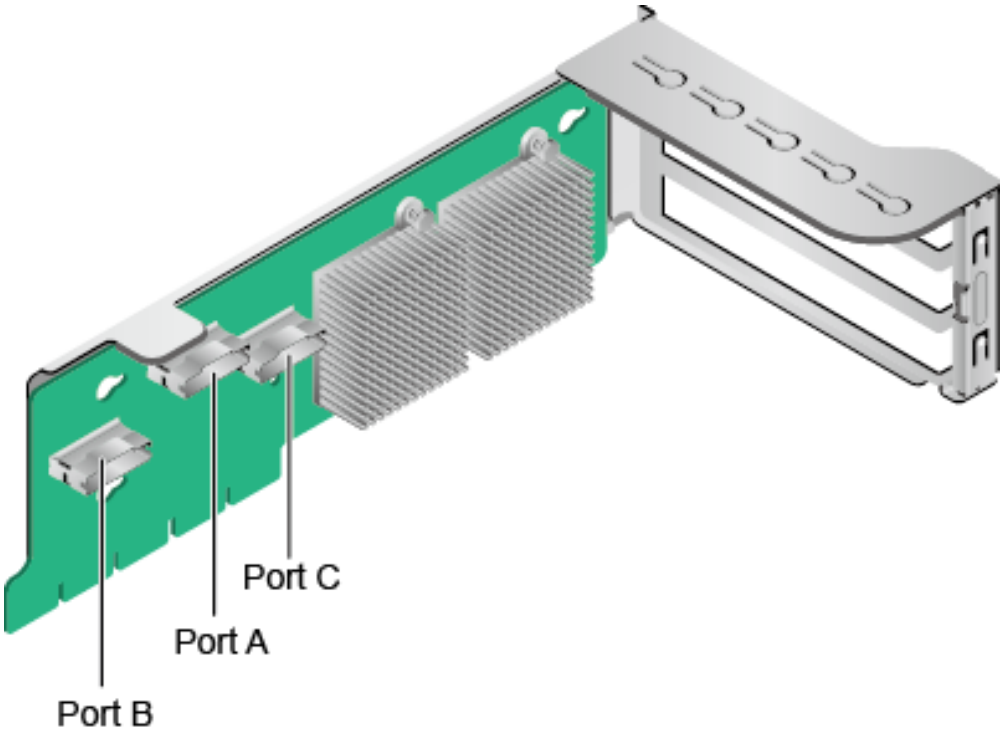
  - Use the GPU power cable delivered with the server. Do not use any other power cable.
  - Only slots 2 and 5 support full-height full-length dual-width GPUs.

Figure 2-27 1x8 + 1x16 riser card (board No.: BC82PRUB)



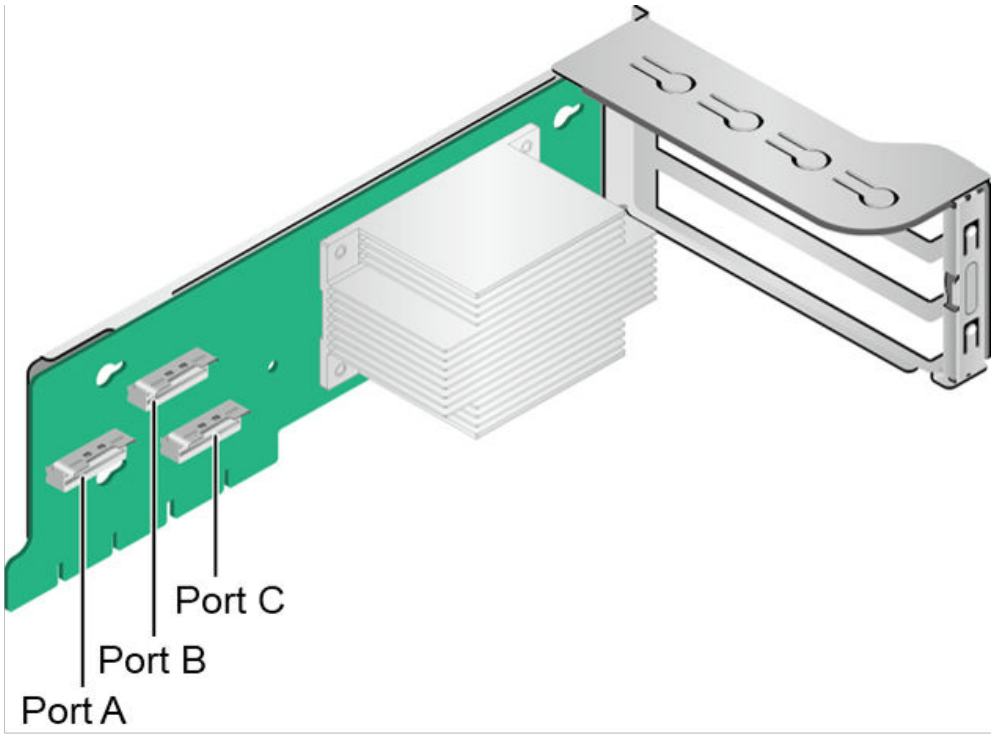
- For a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives and the 03029TDE drive backplane, I/O modules 1 and 2 must be equipped with dedicated NVMe riser cards. See **Figure 2-28**. Port A, port B, and port C are Slimline cable connectors.

Figure 2-28 Riser card for 12 x NVMe (board No.: BC82PRUD)



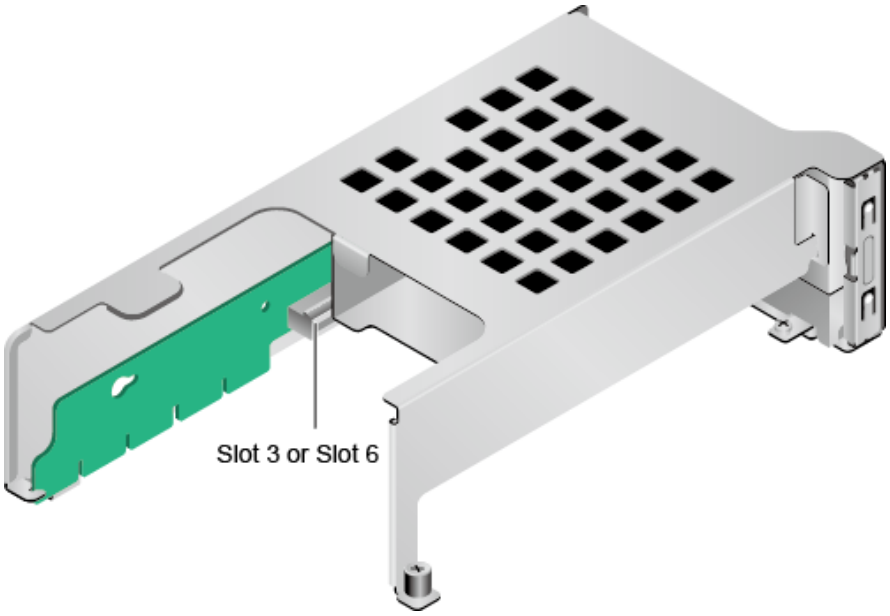
- For a server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drives and the 03028GDX drive backplane, I/O modules 1 and 2 must be equipped with dedicated NVMe riser cards. See **Figure 2-29**. Port A, port B, and port C are Slimline cable connectors.

Figure 2-29 Riser card for 12 x NVMe (board No.: BC13PRTJA)



- When configured with 2 x 2.5-inch rear drives, both I/O modules 1 and 2 support x16 riser cards. See **Figure 2-30**. If installed in I/O module 1, the riser card uses PCIe slot 3. If installed in I/O module 2, the riser card uses PCIe slot 6.

  Figure 2-30 1x16 riser card (board No.: BC82PRUC)

  NOTE

  If the server is equipped with an SP686C RAID controller card, the card cannot be installed in slot 3 or 6 of a 2 x 2.5-inch rear drive module.

- The SAS riser card shown in **Figure 2-31** can be installed in I/O module 1 or 2. By default, it is installed in I/O module 2. When installed in I/O module 1, it occupies PCIe slots 1 to 3 and only slot 3 (x8) is available. When installed in I/O module 2, it occupies PCIe slots 4 to 6 and only slot 6 (x8) is available.

Figure 2-31 SAS riser card (board No.: BC82PRNE)

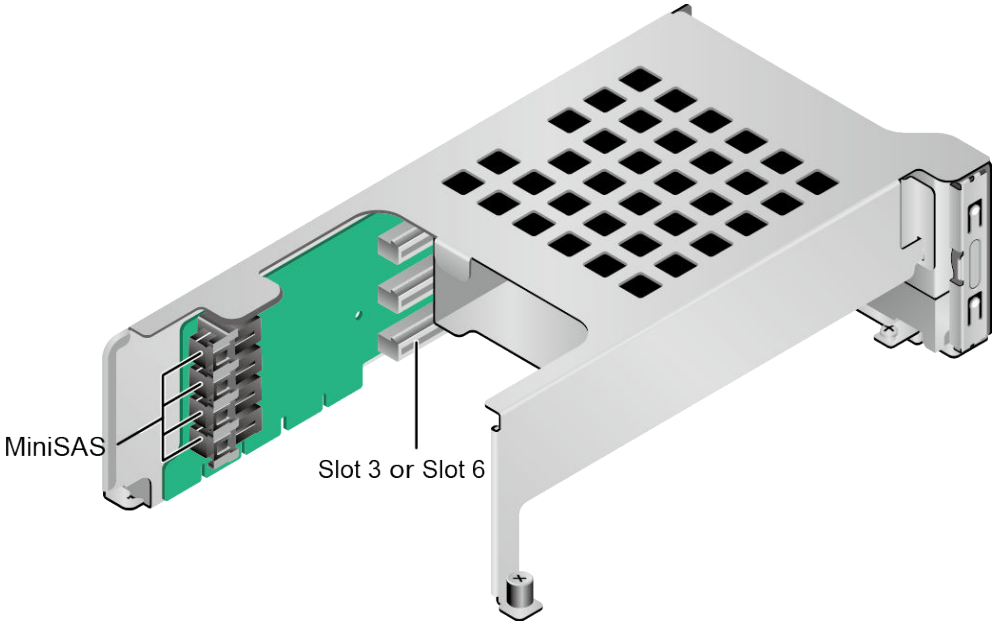
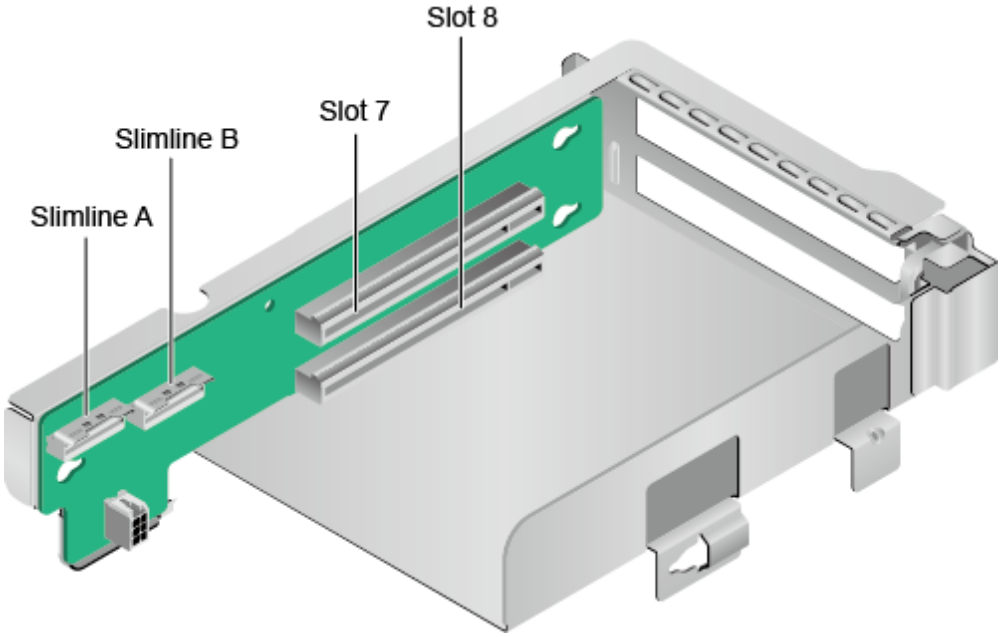


Figure 2-32 and **Figure 2-33** show the riser cards supported by I/O module 3.

- When installed in I/O module 3, the riser card shown in **Figure 2-32** uses PCIe slots 7 and 8.

Figure 2-32 2x8 riser card (board No.: BC82PRUF)



- When installed in I/O module 3, the riser card shown in **Figure 2-33** uses PCIe slot 8.

Figure 2-33 1x16 riser card (board No.: BC82PRUG)

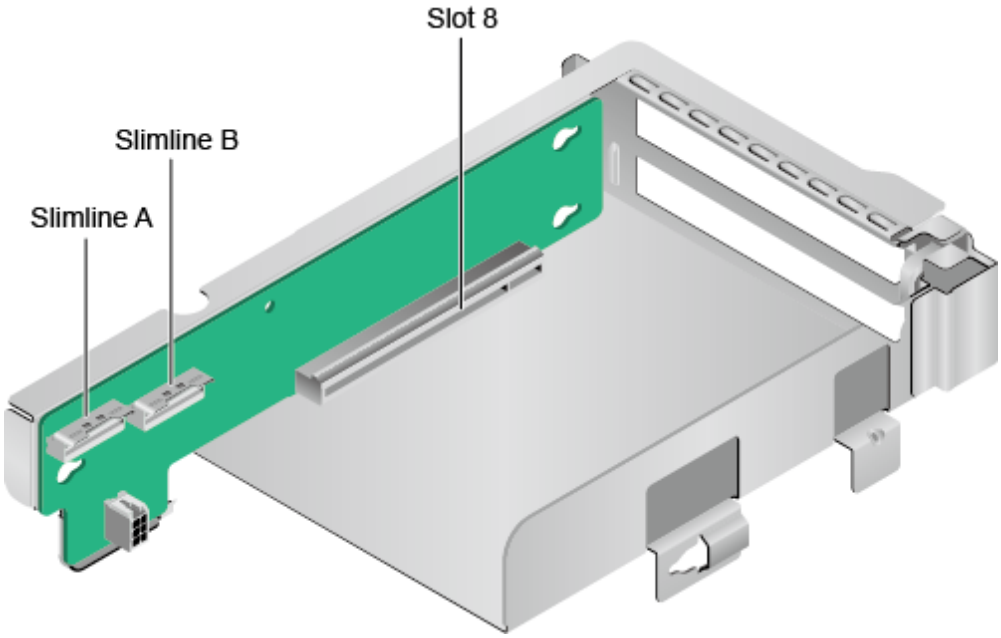
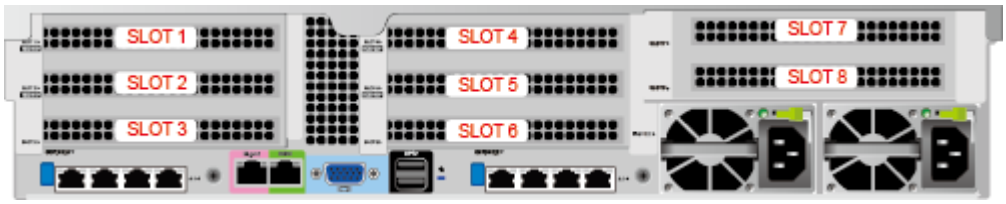


Figure 2-34 shows the rear PCIe slots of the TS200-2280 server.

Figure 2-34 PCIe slots



I/O module 1 provides slots 1 to 3, I/O module 2 provides slots 4 to 6, and I/O module 3 provides slots 7 and 8.

- If I/O module 1 uses a 2-slot PCIe riser module, slot 1 is unavailable.
- If I/O module 2 uses a 2-slot PCIe riser module, slot 4 is unavailable.
- If I/O module 3 uses a 1-slot PCIe riser module, slot 7 is unavailable.

Table 2-12 PCIe slots

PCIe Slot	CPU	PCIe Standard	Connector Width	Bus Width	Port Number in the BIOS	ROOT PORT (B/D/F)	Device (B/D/F)	Slot Size
Slot 1	CPU 1	PCIe 4.0	x16	2-slot PCIe riser module: N/A	-	-	-	Full-height full-length
				3-slot PCIe riser module: x8	Port 0	00/00/0		
				SAS PCIe riser module: N/A	-	-		
Slot 2	CPU 1	PCIe 4.0	x16	2-slot PCIe riser module: x16	Port 0	00/00/0	-	Full-height full-length
				3-slot PCIe riser module: x8	Port 4	00/04/0		
				SAS PCIe riser module: N/A	-	-		
Slot 3	CPU 1	PCIe 4.0	x16	1-slot PCIe riser module: x16	Port 0	00/00/0	-	Full-height half-length
				2-slot PCIe riser module: x8	Port 12	00/0C/0		
				3-slot PCIe riser module: x8	Port 12	00/0C/0		
				SAS PCIe riser module: x8	Port 12	00/0C/0		
Slot 4	CPU 2	PCIe 4.0	x16	2-slot PCIe riser module: N/A	-	-	-	Full-height full-length
				3-slot PCIe riser module: x8	Port 0	80/00/0		
				SAS PCIe riser module: N/A	-	-		
Slot 5	CPU 2	PCIe 4.0	x16	2-slot PCIe riser module: x16	Port 0	80/00/0	-	Full-height full-length
				3-slot PCIe riser module: x8	Port 4	80/04/0		
				SAS PCIe riser module: N/A	-	-		

PCIe Slot	CPU	PCIe Standard	Connector Width	Bus Width	Port Number in the BIOS	ROOT PORT (B/D/F)	Device (B/D/F)	Slot Size
Slot 6	CPU 2	PCIe 4.0	x16	1-slot PCIe riser module: x16	Port 0	80/00/0	-	Full-height half-length
				2-slot PCIe riser module: x8	Port 16	80/10/0		
				3-slot PCIe riser module: x8	Port 16	80/10/0		
				SAS PCIe riser module: x8	Port 16	80/10/0		
Slot 7	CPU 2	PCIe 4.0	x16	1-slot PCIe riser module: N/A	-	-	-	Full-height half-length
				2-slot PCIe riser module: x8	Port 8	80/08/0		
Slot 8	CPU 2	PCIe 4.0	x16	1-slot PCIe riser module: x16	Port 8	80/08/0	-	Full-height half-length
				2-slot PCIe riser module: x8	Port 12	80/0C/0		
RAID controller card	CPU 1	PCIe 4.0	x8	x8	Port 8	00/08/0	-	-
FlexIO card 1	CPU 1	-	x4	x4	-	7C/00/0	7D/00/x	-
FlexIO card 2	CPU 2	-	x4	x4	-	BC/00/0	BD/00/x	-

PCIe Slot	CPU	PCIe Standard	Connector Width	Bus Width	Port Number in the BIOS	ROOT PORT (B/D/F)	Device (B/D/F)	Slot Size

NOTE

- A PCIe slot that supports a full-height full-length PCIe card also supports a full-height half-length or half-height half-length PCIe card. A PCIe slot that supports a full-height half-length PCIe card also supports a half-height half-length PCIe card.
- A PCIe slot that supports a PCIe x16 card also supports a PCIe x8, x4, or x2 card. A PCIe slot that supports a PCIe x8 card also supports a PCIe x4 or x2 card.
- All slots support PCIe cards of up to 75 W. The power of a PCIe card depends on its model. For details about supported PCIe cards, use the **Computing Product Compatibility Checker**. For PCIe cards not listed on the Computing Product Compatibility Checker, contact the local Huawei sales personnel to submit a compatibility test application.
- When two 2.5-inch drives are installed in I/O module 1 or 2, this module also supports a PCIe x16 riser card in slot 3 or 6.
- B/D/F indicates Bus/Device/Function Number.
- ROOT PORT (B/D/F) indicates the B/D/F of a CPU internal PCIe root port. Device (B/D/F) indicates the B/D/F (displayed on the OS) of an onboard or external PCIe port.
- This table lists the default B/D/F information. The values may be different if: (1) The server is not fully configured with PCIe devices; (2) The PCIe cards in full configuration are of a different model or installed in different slots; (3) A PCIe card with a PCI bridge is configured.

3 Product Specifications

Use the **Computing Product Compatibility Checker** to learn details about the product specifications.

3.1 Technical Specifications

NOTE

The original CPU models Kunpeng 920 6426/4826/3226 are renamed to Kunpeng 920 7260/5250/3210.

Table 3-1 Technical specifications

Item	Specifications
Form factor	2U rack server
Processor	• Kunpeng 920 7260 processor: 2 x 64 cores @ 2.6 GHz • Kunpeng 920 5250 processor: 2 x 48 cores @ 2.6 GHz • Kunpeng 920 5220 processor: 2 x 32 cores @ 2.6 GHz • Kunpeng 920 3210 processor: 2 x 24 cores @ 2.6 GHz
Cache	Each core integrates a 64 KB L1 instruction cache, a 64 KB L1 data cache, and a 512 KB L2 cache. The L3 cache is 24 MB to 64 MB (1 MB/core).

Item	Specifications
Memory	• When the server is equipped with Kunpeng 920 7260 or Kunpeng 920 5250 processors, it supports up to 32 DDR4 RDIMM slots. • When the server is equipped with Kunpeng 920 5220 or 3210 processors, it supports up to 16 DDR4 RDIMM slots. • Maximum memory speed: 2933 MT/s • Capacity of a single DIMM: 16 GB, 32 GB, 64 GB, or 128 GB **NOTE** A server cannot be configured with DIMMs of different specifications (capacity, bit width, rank, or height). DIMMs of a server must have the same part number (P/N).
Storage	SAS, SATA, and NVMe drives: • For detailed configurations, see **2.6.2 Drive Configurations**. • Drives are hot-swappable. RAID controller cards: • Use the **Computing Product Compatibility Checker** to obtain information about the supported RAID controller cards. • The RAID controller cards support a supercapacitor for power failure protection, RAID level migration, disk roaming, self-diagnosis, and web-based remote configuration. For details about the RAID controller cards, see **RAID Controller Card User Guide (Kunpeng Processors)**.
FlexIO card	One or two FlexIO cards. A FlexIO card provides the following network ports: • Four GE electrical ports, supporting PXE • Four 25GE/10GE optical ports, supporting PXE **NOTE** Different optical modules can be used for auto-negotiation between 25GE and 10GE.

Item	Specifications
PCIe slot	• A maximum of nine PCIe 4.0 slots, among which one is a PCIe slot dedicated for a screw-in RAID controller card, and the other eight are for PCIe cards. The specifications of PCIe 4.0 slots are as follows: I/O modules 1 and 2 provide the following PCIe slots: – Two standard full-height full-length PCIe 4.0 x16 slots (width: PCIe 4.0 x8) and one standard full-height half-length PCIe 4.0 x16 slot (width: PCIe 4.0 x8) – One standard full-height full-length PCIe 4.0 x16 slot and one standard full-height half-length PCIe 4.0 x16 slot (width: PCIe 4.0 x8) I/O module 3 provides the following PCIe slots: – Two standard full-height half-length PCIe 4.0 x16 slots (width: PCIe 4.0 x8) – One standard full-height half-length PCIe 4.0 x16 slot • The PCIe expansion slots fully support Huawei proprietary PCIe SSD cards, which bolster I/O performance for applications such as search, cache, and download. • The PCIe slots support Huawei-developed Atlas 300 AI accelerator cards to implement fast and efficient processing and reasoning, and image identification and processing.
Port	• Two USB 3.0 ports and one DB15 VGA port on the front panel • Two USB 3.0 ports, one DB15 VGA port, one RJ45 serial port, and one RJ45 management network port on the rear panel **NOTE** If the VGA port is connected to a physical KVM device, insert the KVM device after the server is powered on.
Fan module	Four hot-swappable fan modules, providing protection against single-fan failure **NOTE** All the fan modules on a server must have the same part number (P/N code).
System management	The iBMC supports Intelligent Platform Management Interface (IPMI), Serial over LAN (SOL), KVM over IP, and virtual media, and provides one 10/100/1000 Mbit/s RJ45 management network port.
Security	• Administrator password • Front bezel (optional) **NOTE** The front bezel is installed on the front panel and comes with a security lock to prevent unauthorized operations on drives.

Item	Specifications
Video card	An SM750 video chip with 32 MB display memory is integrated on the mainboard. The maximum display resolution is 1920 x 1200 at 60 Hz with 16 M colors. **NOTE** • The integrated video card can provide the maximum display resolution (1920 x 1200) only after the video card driver matching the operating system version is installed. Otherwise, only the default resolution supported by the operating system is provided. • If both the front and rear VGA ports of a device are connected to a monitor, the front VGA port is used by default.

3.2 Environmental Specifications

Table 3-2 Environmental specifications

Item	Specifications
Temperature	• Operating temperature: 5°C to 40°C (41°F to 104°F) (ASHRAE Classes A2 and A3 compliant) • Storage temperature (within 24 hours): –40°C to +65°C (–40°F to +149°F) • Storage temperature (within 3 months): –30°C to +60°C (–22°F to +140°F) • Storage temperature (within 6 months): –15°C to +45°C (5°F to 113°F) • Storage temperature (within 1 year): –10°C to +35°C (14°F to 95°F) • Maximum temperature change rate: 20°C (36°F) per hour, 5°C (9°F) per 15 minutes **NOTE** The operating temperature limitation varies depending on the server configuration. For details, see **Table 3-3**.
Relative humidity (RH, non-condensing)	• Operating humidity: 8% to 90% • Storage humidity (within 96 hours): 8% to 95% (40°C) • Storage humidity (within 3 months): 8% to 85% • Storage humidity (within 6 months): 8% to 80% • Storage humidity (within 1 year): 20% to 75% • Maximum humidity change rate: 20%/h
Air volume	≥ 204 CFM

Item	Specifications
Altitude	≤ 3050 m (10,000 ft.) **NOTE** • ASHRAE Class A1 and A2 compliant: For altitudes above 900 m (2952.72 ft.), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 300 m (984.24 ft.) in altitude. • ASHRAE Class A3 compliant: For altitudes above 900 m (2952.72 ft.), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 175 m (574.15 ft.) in altitude. • ASHRAE Class A4 compliant: For altitudes above 900 m (2952.72 ft.), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 125 m (410.10 ft) in altitude.
Corrosive gaseous contaminant	Maximum corrosion product thickness growth rate: • Copper corrosion rate test: 300 Å/month (meeting level G1 requirements of the ANSI/ISA-71.04-2013 standard on gaseous corrosion) • Silver corrosion rate test: 200 Å/month
Particle contaminant	• The equipment room environment meets the requirements of ISO 14644-1 Class 8. • There is no explosive, conductive, magnetic, or corrosive dust in the equipment room. **NOTE** It is recommended that the particulate pollutants in the equipment room be monitored by a professional organization.
Acoustic noise	The declared A-weighted sound power levels (LWAd) and declared average bystander position A-weighted sound pressure levels (LpAm) listed are measured at 23°C (73.4°F) in accordance with ISO 7779 (ECMA 74) and declared in accordance with ISO 9296 (ECMA 109). • Idle: – LWAd: 5.64 Bels – LpAm: 41 dBA • Operating: – LWAd: 6.24 Bels – LpAm: 46.6 dBA **NOTE** Actual sound levels generated during operation vary depending on server configuration, load, and ambient temperature.

Table 3-3 Operating temperature limitations

Model	Max. 30°C (86°F)	Max. 35°C (95°F) (ASHRAE Class A2 Compliant)	Max. 40°C (104°F) (ASHRAE Class A3 Compliant)
12 x 3.5-inch drive EXP configuration	All options supported	Some rear NVMe drives are not supported. **NOTE** The NVMe drives not supported are: 2.5''-ES3600P V6-3200GB PCIE 16GT/s, 2.5''-ES3500P V6-7680GB PCIe 16GT/s, 2.5''-PM1733-3840GB PCIe 16GT/s, 2.5''-PM1733-7680GB PCIe 16GT/s, 2.5''-ES3500P V6-3840GB-NVMe 16GT/s, and 2.5''-PM1733-1920GB PCIe 16GT/s.	Options not supported: • 64-core CPUs • PCIe SSD cards • Passive GPU cards (including DMINI cards) • Rear drives
12 x 3.5-inch drive pass-through configuration			
12 x 3.5-inch drive RAID pass-through configuration			
25 x 2.5-inch drive EXP configuration		All options supported	
24 x 2.5-inch drive pass-through configuration			
8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe drive configuration			Not supported
8 x 2.5-inch drive configuration			Supported

Model	Max. 30°C (86°F)	Max. 35°C (95°F) (ASHRAE Class A2 Compliant)	Max. 40°C (104°F) (ASHRAE Class A3 Compliant)
24 x 2.5-inch drive RAID pass-through configuration	All options supported	All options supported	• Does not support 64-core CPUs. • Does not support PCIe SSD cards. • Does not support passive cooling GPUs (including DMINI cards). • Does not support rear drives.
NOTE • When a single fan fails, the highest operating temperature is 5°C (9°F) lower than the rated value. • When powered by Kunpeng 920 5220 or 3210 processors, the server does not support 24 x 2.5-inch SAS/SATA pass-through drive configuration.			

NOTE

SSDs and HDDs (including NL-SAS, SAS, and SATA) cannot be preserved for a long time in the power-off state. Data may be lost or faults may occur if the preservation duration exceeds the specified maximum duration. When drives are preserved under the specified storage temperature and humidity, the following preservation time is recommended:

- Maximum preservation duration of SSDs:
  - 12 months in power-off state without data stored
  - 3 months in power-off state with data stored
- Maximum preservation duration of HDDs:
  - 6 months in unpacked/packed and powered-off state
- The maximum preservation duration is determined according to the preservation specifications provided by drive vendors. For details, see the manuals provided by drive vendors.

3.3 Physical Specifications

Physical Specifications

Table 3-4 Physical specifications

Item	Specifications
Dimensions (H x W x D)	Chassis with 3.5-inch drives: 86.1 mm (2U) x 447 mm x 790 mm (3.39 in. x 17.60 in. x 31.10 in.) Chassis with 2.5-inch drives: 86.1 mm (2U) x 447 mm x 790 mm (3.39 in. x 17.60 in. x 31.10 in.)

Item	Specifications
Installation space	Requirements for cabinet installation (cabinet compliant with the IEC 297 standard): • Cabinet width: 482.6 mm (19 in.) • Cabinet depth: ≥ 1000 mm (39.37 in.) Requirements for guide rail installation: • L-shaped guide rails: apply only to Huawei cabinets. • Adjustable guide rails: apply to a cabinet with a distance of 543.5 mm to 848.5 mm (21.40 in. to 33.41 in.) between the front and rear mounting bars.
Weight in full configuration	Net weight: • Server with 12 x 3.5-inch front drives + 4 x 3.5-inch rear drives + 4 x 2.5-inch rear drives: 32 kg (70.55 lb) • Server with 25 x 2.5-inch front drives + 2 x 3.5-inch rear drives + 4 x 2.5-inch rear drives: 27 kg (59.52 lb) • Server with 8 x 2.5-inch SAS/SATA + 12 x 2.5-inch NVMe front drives + 4 x 2.5-inch rear drives: 26 kg (57.32 lb) • Server with 24 x 2.5-inch front drives + 4 x 2.5-inch rear drives: 27 kg (59.52 lb) • Server with 8 x 2.5-inch front drives + 4 x 2.5-inch rear drives: 19 kg (41.89 lb) Packaging materials: 5 kg (11.03 lb)
Power consumption	The power consumption parameters vary according to server configurations (including the ErP standard configuration of the European Union). Use the **Computing Product Power Calculator** to obtain the specific power consumption details.

3.4 PSU Specifications

- The PSUs are hot-swappable and work in 1+1 redundant mode.
- For details about supported PSUs, use the **Computing Product Compatibility Checker**.
- The recommended current specifications for an external power circuit breaker connected to the server are as follows:
  - AC power supply: 32 A
  - DC power supply: 63 A
- A server must use PSUs of the same model.
- The PSUs are protected against short circuit. Double-pole fuse is provided for the PSUs with dual input live wires.
- If the input voltage ranges from 200 V to 220 V AC, the output power of the 2000 W AC Platinum PSUs decreases to 1800 W.

- If the input voltage ranges from 100 V to 127 V AC, the output power of the 900 W AC Titanium PSUs decreases to 450 W.

4 Software and Hardware Compatibility

For details about the operating systems and hardware supported by the server, use the **Computing Product Compatibility Checker**.

NOTICE

Do not use incompatible components. Otherwise, the server may fail to work properly. The technical support and warranty do not cover faults caused by incompatible components.

5 Installation and Configuration

5.1 Tool Preparations

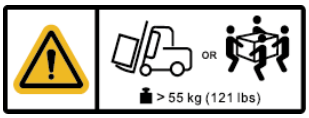
Prepare the following tools:

- ESD wrist strap or ESD gloves
- M3 Phillips screwdriver
- Protective gloves
- ESD bag
- Flat-head screwdriver

5.2 Safety Labels on Devices

Table 5-1 Safety labels

Label	Meaning	Description
	Warning	Indicates that wrong operations may cause device damage or human injury.
	External grounding	Indicates grounding of external devices. One end of the ground cable must connect to the device, and the other end to a ground point. This ensures normal running of the devices and the safety of the operator.
	Internal grounding	Indicates grounding of internal devices. The two ends of the ground cable are connected to different components of the same device. This ensures normal running of the devices and the safety of the operator.
	ESD	Indicates a static sensitive area. Do not touch the device with your hands. When operating the device within this area, take electrostatic discharge (ESD)-preventive measures. For example, wear an ESD wrist strap.
	Altitude	Indicates that the device operates properly at an altitude of 2000 m or lower. The symbol applies only to CCC.
	High touch current	Indicates that the device has high touch current and must be grounded before powering it on.
	Do not touch	Indicates hazardous moving parts. Do not touch the fans when they are rotating.
	Warning	Indicates that at least two people are required for moving the device.

Label	Meaning	Description
	Warning	Indicates that at least three people are required for moving the device.
	Warning	Indicates that a pallet truck or at least four people are required for moving the device.
	No stacking	Indicates that the device cannot be stacked after unpacking. This may cause device damage.
	No handling	Indicates that the device cannot be carried by holding its handles. This may cause personal injury or damage to the device.
	Multiple inputs	Indicates that the device has multiple power inputs. Disconnect all power inputs before you power off the device.

5.3 ESD Protection

5.3.1 Operation Instructions

To minimize ESD damage, observe the following precautions:

- Lay ESD floors or ESD cushions in the entire equipment room, and use ESD chairs. Equip the equipment room with ESD clapboards, ESD screens, and ESD curtains.
- All floor-standing electric devices, metal frames, and metal chassis shells in the equipment room must be directly grounded. All electric meters and tools on a workbench must be connected to the common ground point of the workbench.
- Monitor the temperature and humidity in the equipment room. Heating decreases the indoor humidity and increases static electricity.
- Place components in ESD bags or boxes during transportation or storage.
- Wear an ESD wrist strap when installing or removing a server component. Ensure that the ground terminal of the ESD wrist strap is inserted into the ESD jack in the chassis.
- Before touching a device, ensure that you are wearing ESD clothing and ESD gloves (or a wrist strap), and remove any conductive objects (such as watches and jewelry). **Figure 5-1** shows conductive objects that must be removed before you touch a device.

Figure 5-1 Conductive objects to be removed

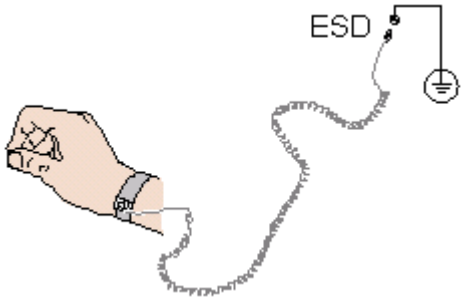
- Both ends of an ESD wrist strap must be in good contact. One end contacts your bare skin, and the other is securely inserted into the ESD jack in the chassis. For details, see **5.3.2 ESD Wrist Strap**.
- During parts replacement, keep new server components in ESD bags before installation, and place removed server components on ESD mats for temporary storage.
- Do not touch welding points, pins, or exposed circuits.

5.3.2 ESD Wrist Strap

A cabinet or chassis is properly grounded.

Step 1 Put on the ESD wrist strap. See **Figure 5-2**.

Figure 5-2 Wearing an ESD wrist strap



Step 2 Tighten the ESD wrist strap to ensure that it is in good contact with your bare skin.

Step 3 Insert the ground terminal of the ESD wrist strap into the ESD jack in a cabinet or chassis.

----End

5.4 Environmental Requirements

NOTE

- For details about the safety precautions to be observed when you install or replace servers and their parts, see **Huawei Server Safety Information**.
- This product is only suitable for installation on concrete or non-flammable surface.

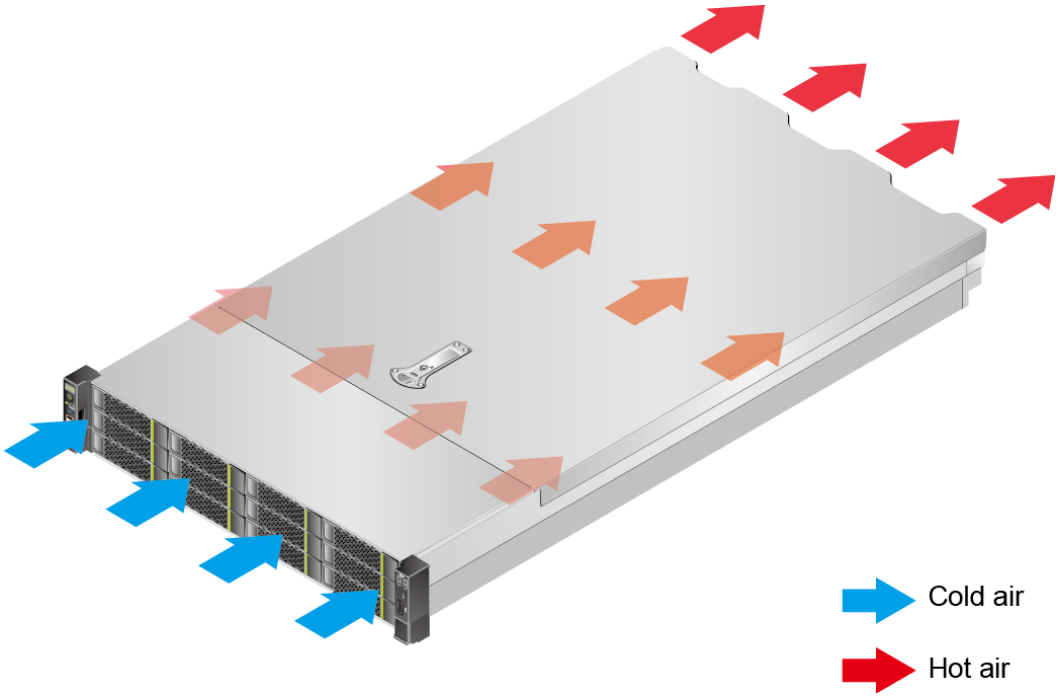
5.4.1 Space and Airflow

To allow for servicing and adequate airflow, observe the following space and airflow requirements:

- Install the server in an access-restricted area.
- Keep the area in which the server is located clean and tidy.
- To facilitate heat dissipation and maintenance, keep a clearance of 800 mm (31.50 in.) between walls and the front and rear doors of the cabinet.
- Do not block the air intake vents. Otherwise, air intaking and heat dissipation will be affected.
- The air conditioning system in the equipment room provides enough wind to ensure proper heat dissipation of all components.

The server draws in cool air from the front of the cabinet and exhausts hot air from the rear. Therefore, the front and rear of the cabinet must be well ventilated for optimal heat dissipation. **Figure 5-3** shows the direction of heat dissipation.

Figure 5-3 Direction of heat dissipation



5.4.2 Temperature and Humidity

To ensure secure and reliable server running, install or position the server in a well-ventilated, climate-controlled environment.

- Use temperature control devices all year long in any climates.
- In dry and humid areas, maintain the ambient humidity within range with humidifiers and dehumidifiers.

Table 5-2 Temperature and humidity requirements in the equipment room

Item	Description
Temperature	5°C to 40°C (41°F to 104°F)
Humidity	8% RH to 90% RH (non-condensing)

5.4.3 Cabinet

- A general 19-inch cabinet with a depth of more than 1000 mm (39.37 in.) which complies with the International Electrotechnical Commission 297 (IEC 297) standard
- Air filters installed on cabinet doors
- AC power supply from the rear of the cabinet

5.5 Unpacking the Chassis

Step 1 Check that the packaging is in good condition.

NOTE

If there is damage (for example, if the package is soaked or deformed, or the seals or pressure-sensitive adhesive tapes are not intact), submit the *Cargo Problem Feedback Form*.

Step 2 Use a box cutter to cut the pressure-sensitive adhesive tape and open the packing case.

CAUTION

Exercise caution with the box cutter to avoid injury to your hands or damage to devices.

Step 3 Check the contents against **Table 5-3** to ensure that nothing is missing. Check that they are free from oxidation, corrosion, and damage.

Table 5-3 Packing list

No.	Description
1	Documentation bag that contains a warranty card, and a Quick Start guide
2	Guide rails
3	A TaiShan rack server

----End

5.6 Installing Optional Hardware Parts

Before installing and configuring the server, install all optional hardware parts, such as extra drives and PCIe cards. For details about how to install the optional parts of the server, see **TaiShan 200 Server Maintenance and Service Guide (Model 2280)**.

5.7 Installing a Server on Guide Rails

5.7.1 Installing a Server on L-shaped Guide Rails

L-shaped guide rails are only for Huawei racks.

The servers are stackable when L-shaped guide rails are used.

Step 1 Install the floating nuts.

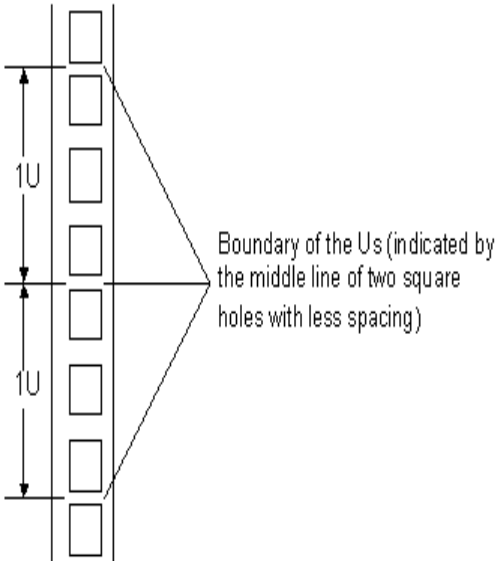
1. Determine the installation positions of the floating nuts according to the cabinet device installation plan.

   NOTE

   Floating nuts are used to tighten screws.

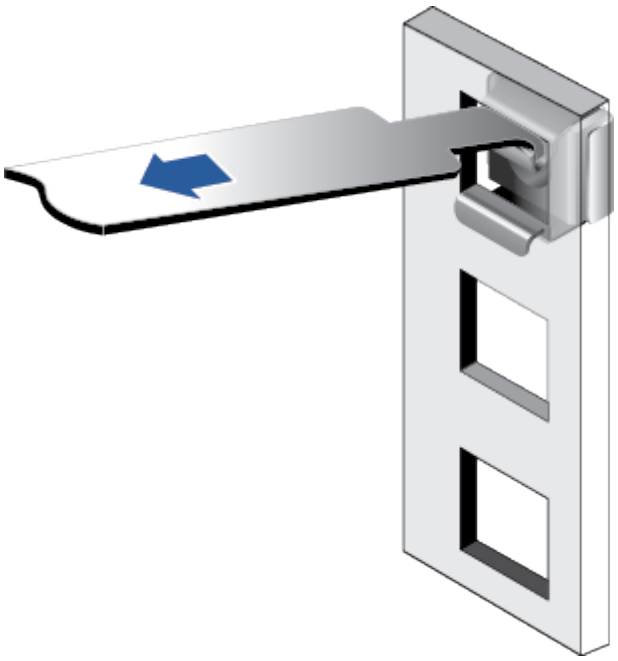
   The boundary between Us is used as the reference for calculating device installation space, as shown in **Figure 5-4**.

   Figure 5-4 Boundary between Us

2. Fasten the lower end of a floating nut to the target square hole in a mounting bar at the front of the rack.
3. Use a floating nut hook to pull the upper end of the floating nut, and fasten it to the mounting bar on the front of the cabinet. See **Figure 5-5**.

Figure 5-5 Installing a floating nut

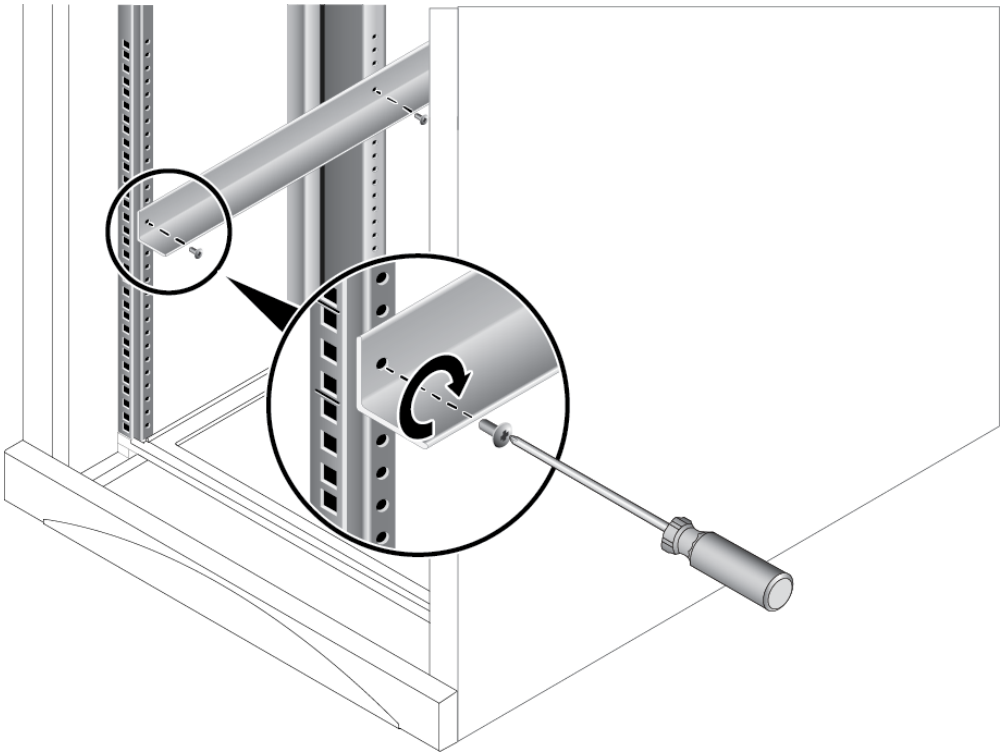


4. Install a floating nut to the other front mounting bar in the same way.

Step 2 Install the L-shaped guide rails.

1. Place a guide rail horizontally in the planned position, and keep the guide rail in close contact with mounting bars.
2. Tighten the screws on the guide rail clockwise. See **Figure 5-6**.

Figure 5-6 Installing an L-shaped guide rail

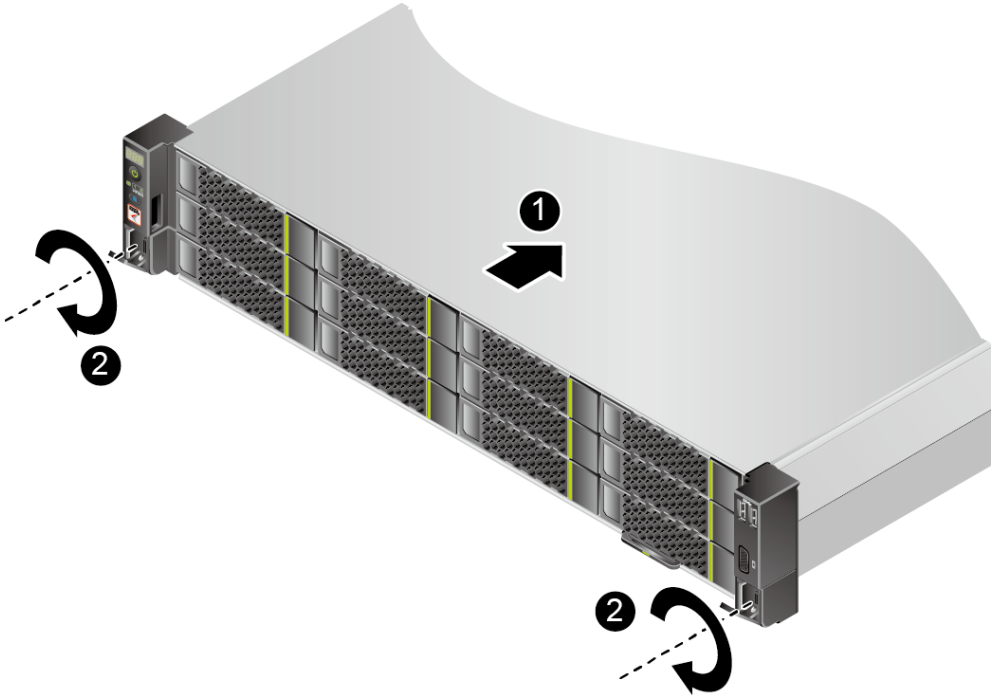


3. Install the other guide rail in the same way.

Step 3 Install the server.

1. Lift the server. This task requires at least two people.
2. Place the server on the guide rails and slide it into the cabinet. See (1) in **Figure 5-7**.

Figure 5-7 Installing the server



3. When the two mounting ears of the server come into contact with the mounting bars on the cabinet, tighten their captive screws clockwise to secure the server. See (2) in **Figure 5-7**.

Step 4 Connect the power cables, network cables, VGA cables, and USB devices as required, and power on the server.

----End

5.7.2 Installing a Server on Adjustable Guide Rails

Adjustable guide rails are for a cabinet with a depth of 543.5 mm to 848.5 mm (21.40 in. to 33.41 in.) between the front and rear mounting bars.

The servers are stackable onto adjustable guide rails.

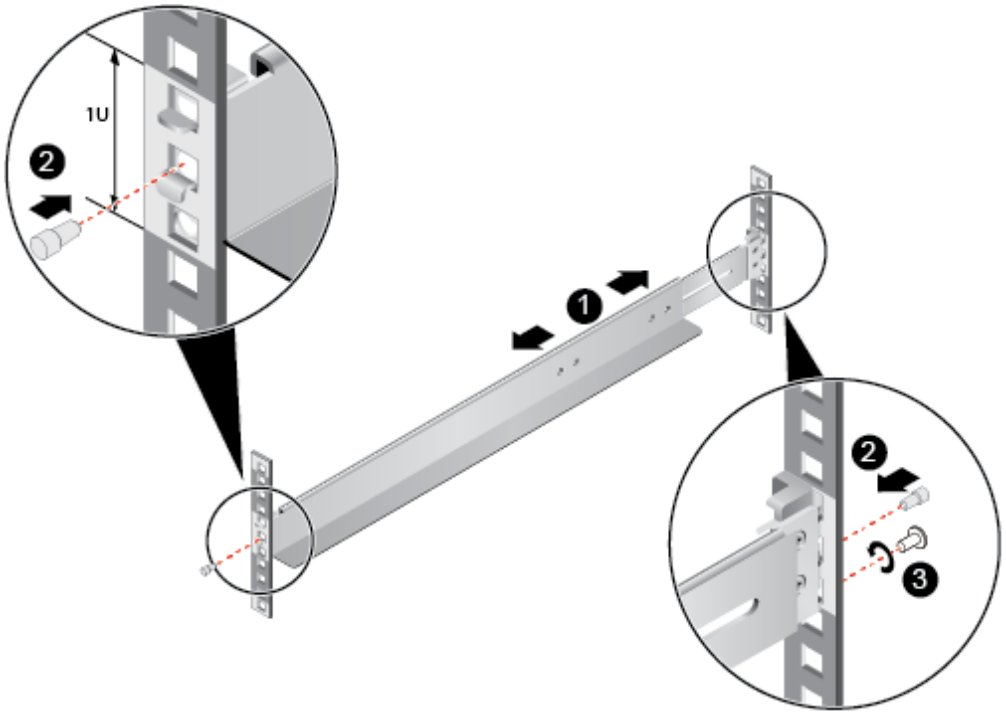
Step 1 Install the adjustable guide rails.

1. Position a guide rail horizontally, keeping it in contact with the mounting bar in the cabinet and hook the guide rail. See (1) in **Figure 5-8**.

NOTE

The distance between the three holes in each mounting bar for the guide rail must be within 1U.

Figure 5-8 Installing an adjustable guide rail



2. Fill the second square holes at the front and rear of the guide rail with the plugs to secure the guide rail. See (2) in **Figure 5-8**.
3. (Optional) Install an M6 screw in the square hole underneath at the rear of the guide rail to secure the guide rail. See (3) in **Figure 5-8**.

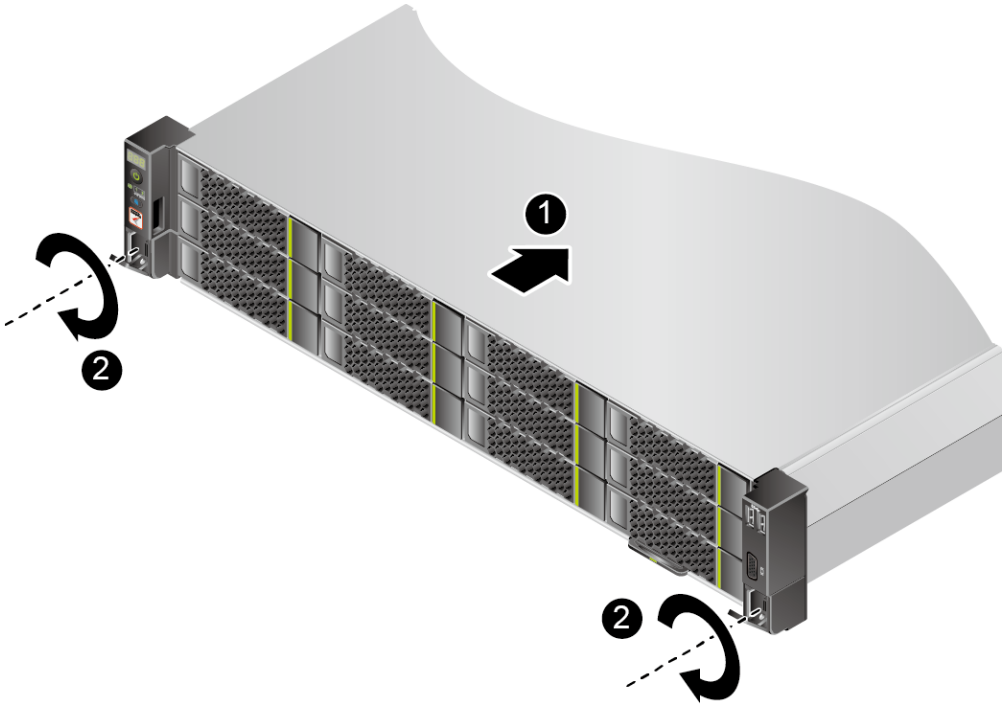
   NOTE

   Although the adjustable guide rails do not need screws for installation, we recommend you use M6 screws at the rear end to make the server more shockproof and secure.
4. Install the other guide rail in the same way.

Step 2 Install the server.

1. Lift the server. This task requires at least two people.
2. Place the server on the guide rails and slide it into the cabinet. See (1) in **Figure 5-9**.

Figure 5-9 Installing the server



3. When the two mounting ears of the server come into contact with the mounting bars on the cabinet, tighten their captive screws clockwise to secure the server. See (2) in **Figure 5-9**.

Step 3 Connect the power cables, network cables, VGA cables, and USB devices as required, and power on the server.

----End

5.8 Connecting External Cables

5.8.1 Cabling Overview

Basic Guidelines

NOTICE

To ensure optimal heat dissipation, do not block the air exhaust vents of PSUs.

- Lay out and bind cables of different types (such as power and signal cables) separately. Cables of the same type must be routed in the same direction. Route cables near each other in crossover mode. Ensure that the distance between power cables and signal cables is greater than or equal to 30 mm (1.18 in.) when you route the cables in parallel.
- If you cannot identify cables by their labels, attach an engineering label to each cable.

- Protect cables from burrs, heat sinks, and active accessories, which may damage the insulation layers of cables.
- Ensure that the length of cable ties for binding cables is appropriate. Do not connect two or more cable ties together for binding cables. After binding cables properly, trim off the excess lengths of the cable ties and ensure that the cuts are neat and smooth.
- Ensure that cables are properly routed, supported, or fixed within the cable troughs inside the cabinet to prevent loose connections and cable damage.
- Coil any surplus lengths of cables and bind them to proper positions inside the cabinet.
- Route cables straightly and bind them neatly. The bending radius of a cable varies depending on the position where the cable is bent.
  - If you need to bend a cable in its middle, the bending radius must be at least twice the diameter of the cable.
  - If you need to bend a cable at the output terminal of a connector, the bending radius must be at least five times the cable diameter, and the cable must be bound before bending.
- Do not use cable ties at a place where the cables are bent. Otherwise, the cables may break.

Common Methods

Route cables inside a cabinet using one of the following methods:

- Determine overhead cabling and underfloor cabling for power cables based on specific conditions of the equipment room. Specifically, take into consideration the AC power distribution frame (PDF), surge protector, and terminal block.
- Determine overhead and underfloor cabling for service data cables based on specific conditions of the equipment room.
- Place the connectors of all service data cables at the bottom of the cabinet so that the connectors are difficult to reach.

5.8.2 Connecting Cables to Mouse, Keyboard, and VGA Ports

The front and rear panels of the server have DB15 VGA ports but no standard PS/2 port for a keyboard or mouse.

You can connect a keyboard and mouse to the USB ports on the front and rear panels using either of the following methods:

- Connect the keyboard and mouse to the USB ports.
- Connect the keyboard and mouse using a USB-to-PS2 cable.

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

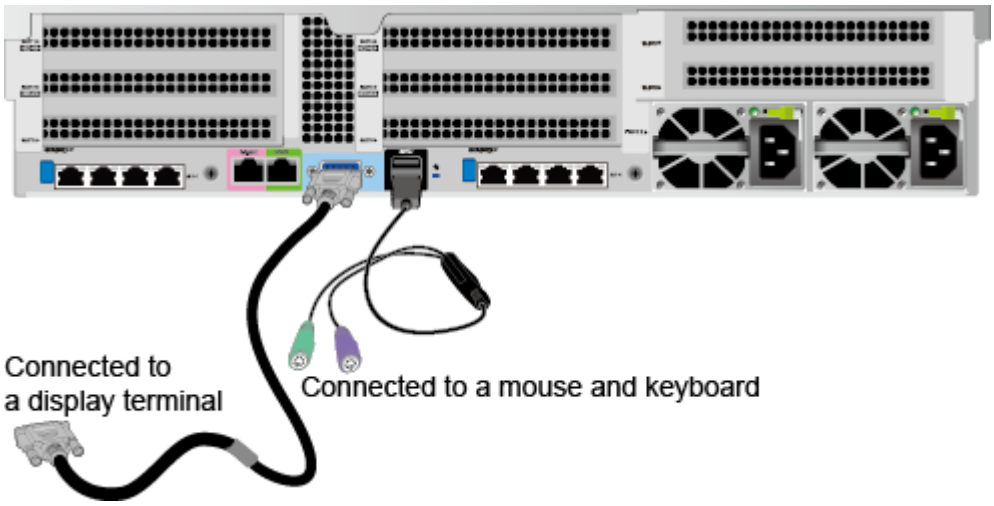
Step 2 Connect the USB connector on one end of the USB-to-PS/2 cable to a USB port on the front or rear panel of the server.

Step 3 Connect the connector on the other end to the keyboard and mouse.

Step 4 Connect the DB15 connector of the VGA cable to the VGA port on the rear panel of the server and tighten the two screws.

Step 5 Connect the other connector of the VGA cable to the VGA port on the monitor and tighten the two screws.

Figure 5-10 Connecting USB-to-PS2 and VGA cables



----End

5.8.3 Connecting a Network Cable

Before connecting or replacing a network cable, use a network cable tester to check whether the new network cable is functional.

The new and old cables must be of the same model or be compatible.

Before installing a network cable to a network port, ensure that the network cable connector is intact and the pins have no sundries or deformation.

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

Step 2 Check the model of the new network cable.

A shielded network cable is recommended. According to professional EMC test results, unshielded network cables provide poor ESD prevention, and the system may stop responding or restart when the static electricity is high.

Step 3 Number the new network cable.

- The new network cable must have the same number as the existing one to be replaced.
- Use the same type of labels for network cables. Record the name and number of the local device on one side of a label and those of the peer device on the other side. Attach a label 2 cm (0.79 in.) away from the end of a network cable.

Step 4 Route the new network cable.

Route the new network cable in the same way (underfloor or overhead) as the old one.

- Underfloor cabling is recommended because it is tidy and easy to route. Route network cables in the cabinet based on the installation requirements. You are

advised to arrange new cables in the same way as existing cables. Ensure that the cables are routed neatly without damage to the cable sheath.

- Separate network cables from power cables when routing.
- The minimum bend radius of a network cable is 4 cm (1.57 in.). Check that the cable insulation layer is intact. Ensure that cables are routed for easy maintenance and capacity expansion.
- Bind cables with ties when routing. Ensure that optical cables are routed straightly and bound neatly, and that cable ties are installed at even spacing and fastened properly.

Step 5 Remove the network cables to be replaced.

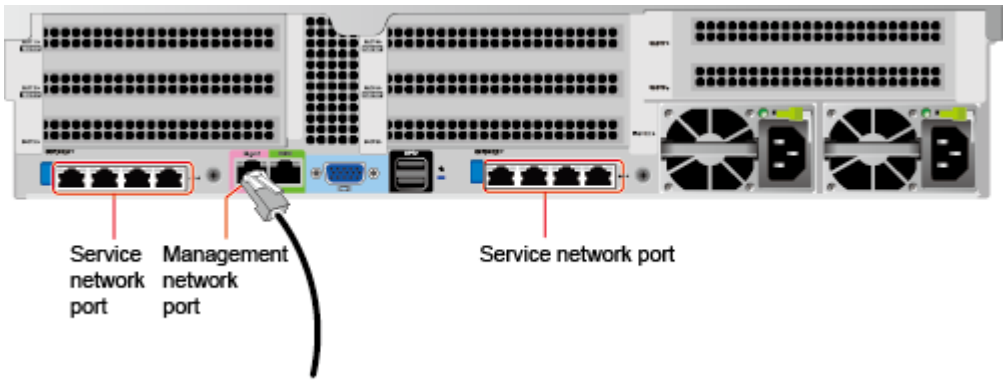
Remove the network cables from the NIC or board in the cabinet.

Step 6 Install the new network cable.

Note the following points:

- Connect the new network cable to the same port as the removed one.
- Connect the network cable to the network port securely.

Figure 5-11 Connecting a network cable



Step 7 Connect the new network cable to the peer network port.

Connect the other end of the network cable to the peer device based on the network plan.

- Connect the new network cable to the same port as the removed one.
- Connect the network cable to the network port securely.

Step 8 Check whether the new network cable is properly connected.

Power on the device, and ping the peer device connected by the new network cable. If the peer device cannot be pinged, check whether the network cable is damaged or the connectors are not securely connected.

Step 9 Bind the new network cable with other cables.

Bind the new network cable in the same way as the existing network cables. You can also remove all cable ties and bind all of the network cables again if necessary.

----End

5.8.4 Connecting a Cable to an Optical Port

You can connect an optical or SFP+ cable to an optical port. You need to first determine the type of the cable to be connected.

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

Step 2 Check the model of the new cable.

Step 3 Number the new cable.

- The new cable must have the same number as the existing one to be replaced.
- Use the same type of labels for network cables. Record the name and number of the local device on one side of a label and those of the peer device on the other side. Attach a label 2 cm (0.79 in.) away from the end of a network cable.

Step 4 Route the new cable.

Route the new network cable in the same way (underfloor or overhead) as the old one.

- Route optical or SFP+ cables in the cabinet based on the installation requirements. You are advised to arrange new cables in the same way as existing cables. Ensure that the cables are routed neatly without damage to the cable sheath.
- Separate optical or SFP+ cables from power and signal cables when routing the cables.
- Bend optical or SFP+ cables with a bending radius of at least 4 cm (1.57 in.) to prevent damage to core wires. Ensure that the cable sheath is intact. Ensure that optical or SFP+ cables are properly routed for easy maintenance and capacity expansion.
- Bind cables with ties when routing. Ensure that optical cables are routed straightly and bound neatly, and that cable ties are installed at even spacing and fastened properly.

Step 5 Connect the cables to the optical ports.

When you use an optical cable:

1. Remove the optical cable to be replaced.

   Remove the existing optical cable from the server.

2. Connect the new optical cable.

   NOTE

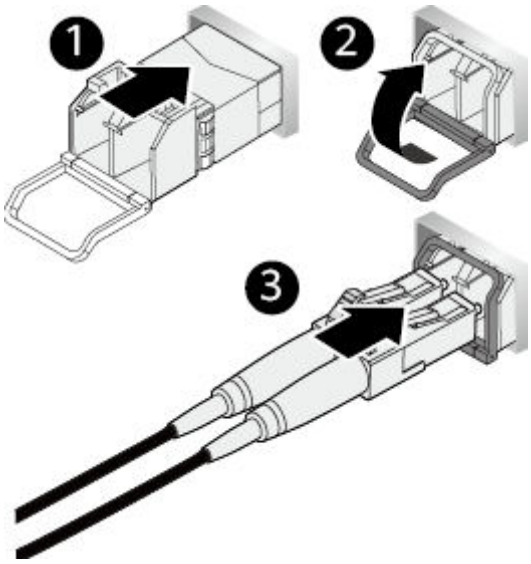
   - Connect the new optical cable to the same port as the old one.
   - Connect the optical cable to the optical module securely.

   a. Insert the optical module into the optical module port. See (1) in **Figure 5-12**.

   b. Close the latch on the optical module to secure it. See (2) in **Figure 5-12**.

   c. Insert the optical cable into the optical module. See (3) in **Figure 5-12**.

Figure 5-12 Connecting an optical cable



When you use an SFP+ cable:

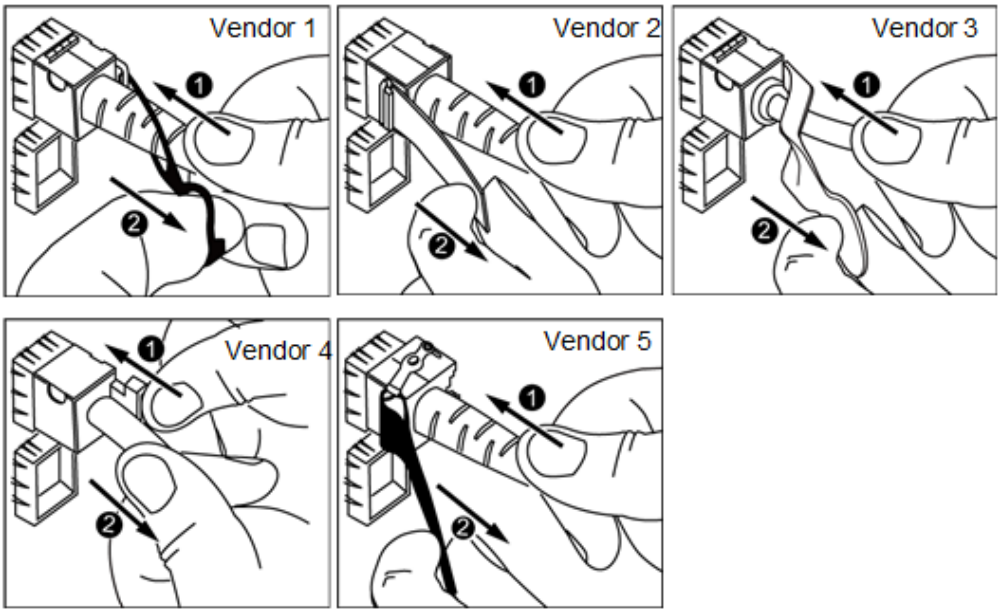
1. Remove the SFP+ cable to be replaced.

   Gently push the power connector inwards and pull the latch out to remove the cable. See **Figure 5-13**.

NOTICE

Do not directly pull out the latch.

Figure 5-13 Removing an SFP+ cable



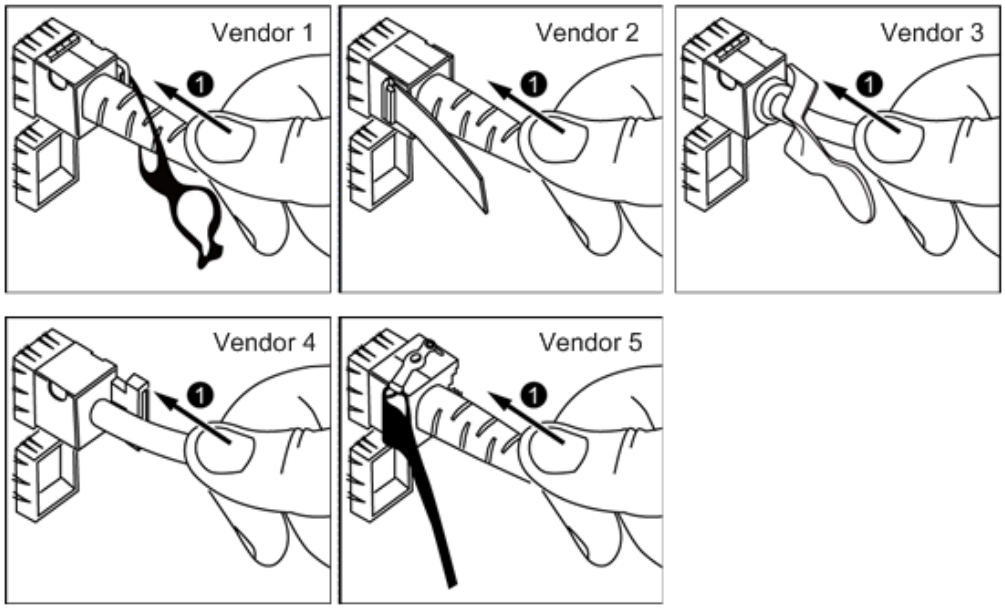
2. Connect the new SFP+ cable.

   Remove the dustproof cap from the port, and insert the cable connector into the port. See **Figure 5-14**.

NOTE

When you hear a "click" sound and the cable cannot be pulled out, the connector is secured.

Figure 5-14 Connecting an SFP+ cable



Step 6 Check whether the new cable is properly connected.

Power on the device, and ping the peer device connected by the new network cable. If the peer device cannot be pinged, check whether the network cable is damaged or the connectors are not securely connected.

Step 7 Bind the new optical cable.

Bind the new network cable in the same way as the existing network cables. You can also remove all cable ties and bind all of the optical cables again if necessary.

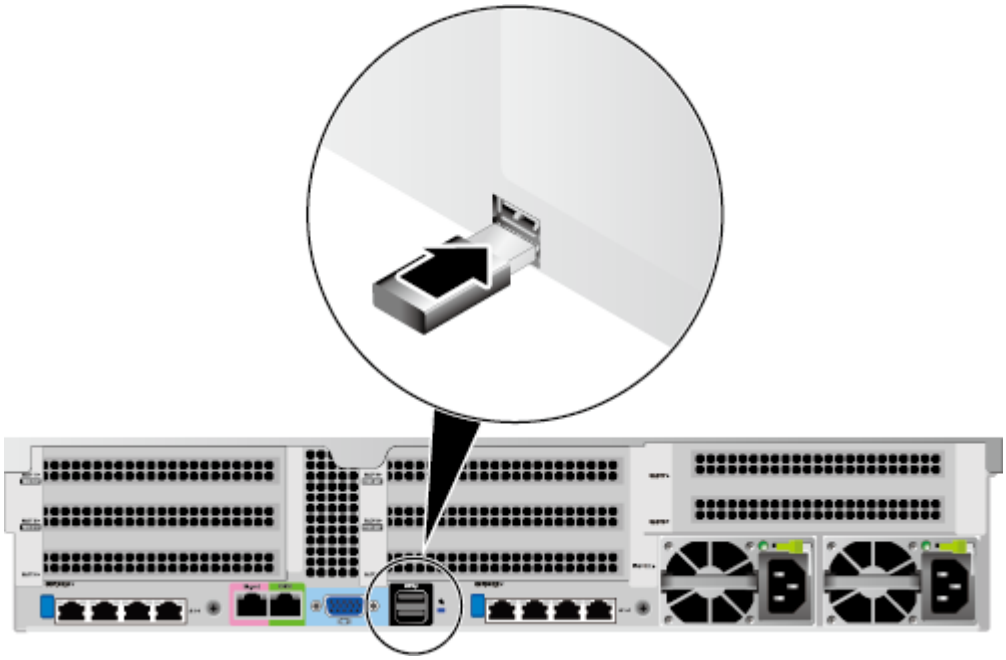
----End

5.8.5 Connecting a USB Device

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

Step 2 Connect a USB device to a USB port on the server. See **Figure 5-15**.

Figure 5-15 Connecting a USB device



----End

5.8.6 Connecting a Serial Cable

The rear panel of the server provides a standard RJ45 serial port, which works as the system serial port by default. You can set it as the iBMC serial port using the iBMC CLI.

The serial port can be used as:

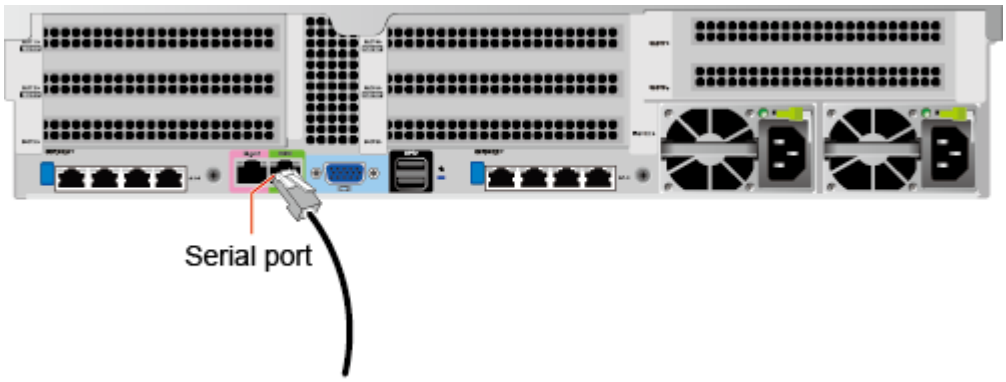
- System serial port to monitor the OS status
- iBMC serial port for debugging and fault locating

Procedure

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

Step 2 Connect a serial cable. See **Figure 5-16**.

Figure 5-16 Connecting a serial cable



----End

5.8.7 Connecting a Power Cable

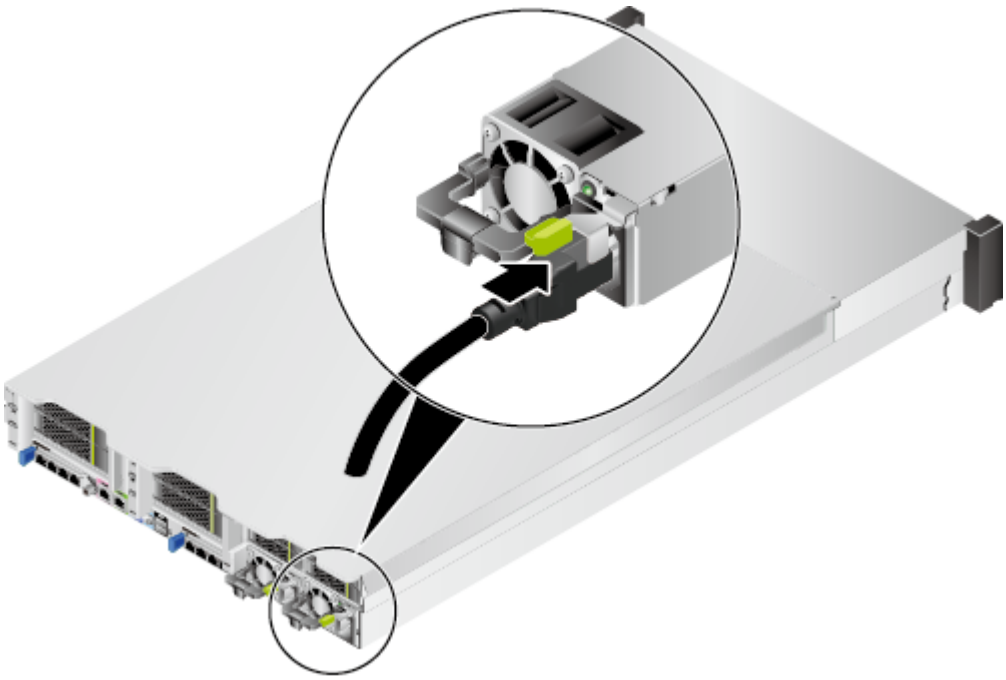
5.8.7.1 Connecting an AC Power Cable

Use power cables only for dedicated devices. Do not use them for other devices.

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

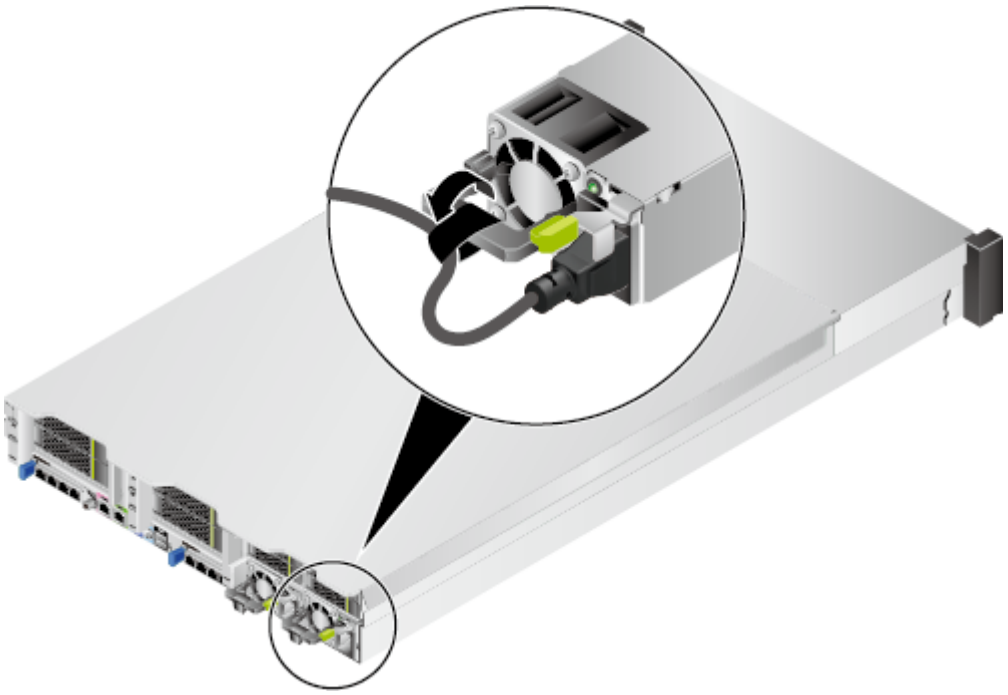
Step 2 Connect one end of the power cable to the cable port on the AC PSU of the server. See **Figure 5-17**.

Figure 5-17 Connecting a power cable



Step 3 Secure the power cable using a velcro strap. See **Figure 5-18**.

Figure 5-18 Securing a power cable



Step 4 Insert the other end of the power cable into the AC power distribution unit (PDU) on the cabinet.

The AC PDU is located horizontally at the rear of the cabinet. Select an appropriate jack on the PDU for the connection.

Step 5 Bind the power cable to the cable management arm (CMA) using cable ties.

----End

5.8.7.2 Connecting a DC Power Cable

NOTICE

- Use dedicated power cables to ensure equipment and personal safety.
- Use power cables only for dedicated servers. Do not use them for other devices.
- Connect the power cables of the active and standby PSUs to different power distribution units (PDUs) to ensure reliable server operation.
- Ground the equipment before powering it on.

Procedure

Step 1 Put on an ESD wrist strap. For details, see **5.3 ESD Protection**.

Step 2 Take the spare part out of its ESD bag.

Step 3 Connect the power cables to the PSUs.

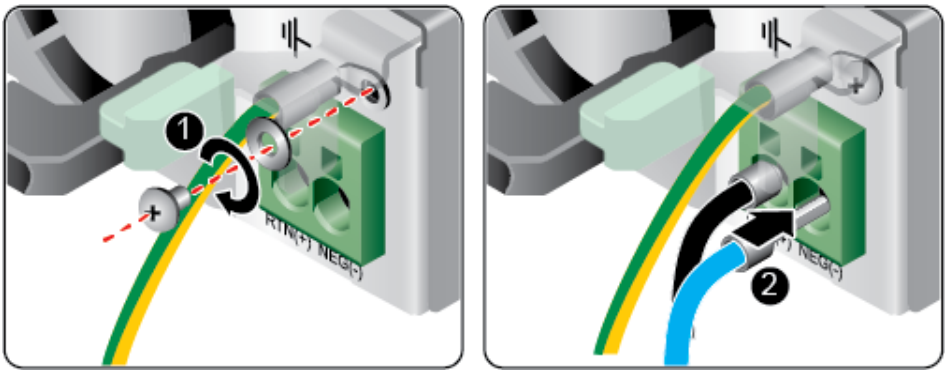
- For a non-2000 W PSU:

a. Put the OT terminal (for the ground cable) on the screw removed from the ground hole, install the screw on the ground hole, and tighten the screw. See (1) in **Figure 5-19**.

b. Insert the power cables to the wiring terminals on the PSU until the cables click into position. See (2) in **Figure 5-19**.

- Connect the cord end terminal of the negative power cable (blue) to the NEG(-) wiring terminal on the PSU.
- Connect the cord end terminal of the positive power cable (black) to the RTN(+) wiring terminal on the PSU.

Figure 5-19 Connecting power cables to a non-2000 W PSU



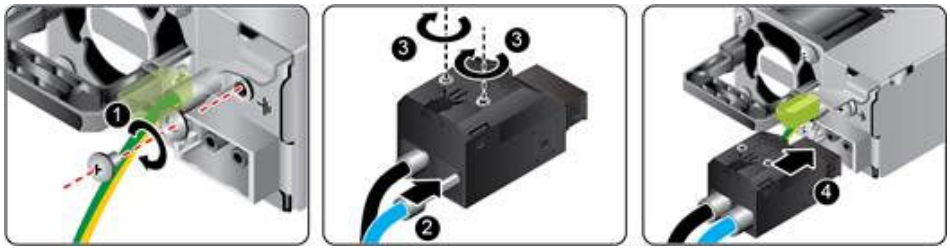
- For a 2000 W PSU:

a. Put the OT terminal (for the ground cable) on the screw removed from the ground hole, install the screw on the ground hole, and tighten the screw. See (1) in **Figure 5-20**.

b. Insert one end of the power cable into the quick connector, and tighten the two screws on the quick connector using a screwdriver. See (2) and (3) in **Figure 5-20**.

c. Insert the quick connector of the power cable into the wiring terminal of the PSU. See (4) in **Figure 5-20**.

Figure 5-20 Connecting power cables to a 2000 W PSU



Step 4 Connect the other end of the power cable to the DC power distribution unit (PDU) in the cabinet.

The DC PDU is located horizontally at the rear of the cabinet. Select an appropriate jack on the PDU for the connection.

Step 5 Bind the power cable to the cable management arm (CMA) using cable ties.

----End

5.8.8 Checking Cable Connections

CAUTION

Before checking cable connections, ensure that the power is cut off. Otherwise, any incorrect or loose connection may cause human injury or device damage.

Table 5-4 describes the cable connection checklist.

Table 5-4 Cable connection checklist

Item	Description
Power cable	Power cables are correctly connected to the rear of the chassis.
Network cable	Network cables are connected correctly to the management network port or service ports on the rear panel of the chassis.
Ground cable	The server does not provide a separate ground port. It is grounded through the ground cable of a power cable. Ensure that the power cables of the PSUs are in good contact.

5.9 Powering On the Server

NOTICE

- Before powering on a server, ensure that the server is powered off, all cables are connected correctly, and the power supply voltage meets service requirements.
- Do not remove or insert components or cables during power-on.
- If the power supply to a server is disconnected, wait for at least one minute before powering it on again.

Power on the server using one of the following methods:

- If the PSUs are properly installed but are not connected to an external power supply:

  Connect the PSUs to the external power supply. Then the server will power on with the PSUs.

  NOTE

  The default value of **System State Upon Power Supply** is **Power on**, which indicates that the server automatically powers on after power is supplied to the PSUs. You can use the iBMC to modify the **System State Upon Power Supply** setting or the BIOS to modify the **Restore on AC Power Loss** setting.
- If the PSUs are properly installed and are connected to an external power supply, and the server is in the standby state (the power indicator is steady yellow):

- Press the power button on the front panel to power on the server. For details about the power button location, see **2.2 Indicators and Buttons on the Front Panel**.
- Power on the server using the iBMC WebUI.
  i. Log in to the iBMC WebUI. For details, see **5.11.4 Logging In to the iBMC WebUI** or **5.12.4 Logging In to the iBMC WebUI**.
  ii. Go to the **Power Control** page.
    - If the iBMC version is V549 or earlier, choose **Power** > **Power Control**.
    - If the iBMC version is V561, V3.01.00.00, or later, choose **System** > **Power** > **Power Control**.
  iii. Click **Power On**. In the displayed dialog box, click **Yes** to power on the server.
- Power on the server using remote virtual consoles.

  HTML5 Integrated Remote Console

  i. Log in to the Remote Virtual Console. For details, see **8.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI** or **9.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI**.
  ii. On the KVM screen, click  on the toolbar, and choose **Power On**.
  iii. Click **OK**.
  The server is powered on.

  Java Integrated Remote Console

  i. Log in to the Remote Virtual Console. For details, see **8.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI** or **9.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI**.
  ii. On the KVM screen, click  on the toolbar, and choose **Power On**.
  The **Select an Option** dialog box is displayed.
  iii. Click **OK**.
  The server is powered on.
- Power on the server using the iBMC CLI.
  i. Log in to the iBMC CLI. For details, see **8.3 Logging In to the iBMC CLI** or **9.3 Logging In to the iBMC CLI**.
  ii. On the iBMC CLI, run the **ipmcset -d powerstate -v 1** command.
  iii. Enter **y** or **Y** to power on the server.

5.10 Powering Off the Server

NOTE

- Services and programs running on a server will be interrupted when the server is powered off. Before powering off the server, ensure that all services and programs have been stopped or switched to other servers.
- "Power-off" in this section indicates to power off the server to the standby state (the power indicator is steady yellow).
- After the server is forcibly powered off, wait for more than 10 seconds to ensure that the server is powered off completely. Then you can power it on again.

NOTICE

A forced power-off may cause data loss or program damage. Exercise caution when performing this operation.

Power off the server using one of the following methods:

- Use cables to connect the server to a video display, keyboard, and mouse, and shut down the server OS to power off the server.
- Press the power button on the front panel to power off the server. For details about the power button location, see **2.2 Indicators and Buttons on the Front Panel**.
  - When the server is powered on, press the power button on the front panel to power off the server.

    NOTE

    If the server OS is running, shut it down following instructions on the OS screen.
  - When the server is powered on, hold down the power button on the front panel for 6 seconds to force the server to power off.
- Power off the server using the iBMC WebUI.
  a. Log in to the iBMC WebUI. For details, see **5.11.4 Logging In to the iBMC WebUI** or **5.12.4 Logging In to the iBMC WebUI**.
  b. Go to the **Power Control** page.
     - If the iBMC version is V549 or earlier, choose **Power** > **Power Control**.
     - If the iBMC version is V561, V3.01.00.00, or later, choose **System** > **Power** > **Power Control**.
  c. Click **Power Off** or **Forced Power Off**. In the displayed dialog box, click **Yes** to power off the server.
- Power off the server using remote virtual consoles.

  HTML5 Integrated Remote Console

  a. Log in to the Remote Virtual Console. For details, see **8.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI** or **9.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI**.

b. On the KVM screen, click  on the toolbar, and choose **Power Off** or **Forced Power Off** from the menu.

c. Click **OK**.

The server is powered off.

Java Integrated Remote Console

a. Log in to the Remote Virtual Console. For details, see **8.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI** or **9.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI**.

b. On the KVM screen, click  on the toolbar, and choose **Power Off** or **Forced Power Off** from the menu.

The **Select an Option** dialog box is displayed.

c. Click **OK**.

The server is powered off.

- Power off the server using the iBMC CLI.

a. Log in to the iBMC CLI. For details, see **8.3 Logging In to the iBMC CLI** or **9.3 Logging In to the iBMC CLI**.

b. On the iBMC CLI, run the **ipmcset -d powerstate -v 0** command to power off the server or the **ipmcset -d powerstate -v 2** command to forcibly power it off.

c. Enter **y** or **Y** to power off the server.

5.11 Initial Configuration (iBMC V250 and Later)

If the server uses a Hi1710 management chip, the iBMC version is in *X.XX* format, which is also referred to as *VXXX*. For example, 2.50, which is also referred to as V250.

5.11.1 Default Data

NOTE

iBMC V663 and later versions do not support U-Boot.

Table 5-5 Default data

Item	Name	Default Value
iBMC management network port data	IP address and subnet mask	• IP address: 192.168.2.100 • Subnet mask: 255.255.255.0

Item	Name	Default Value
iBMC login data	User name and password	• For the default user name, see **TaiShan Server Account List**. • For the default password, see **TaiShan Server Account List**.
BIOS data	Password	See **TaiShan Server Account List**.
iBMC U-Boot data	Password	See **TaiShan Server Account List**.

5.11.2 Configuration Process

Figure 5-21 Initial configuration process

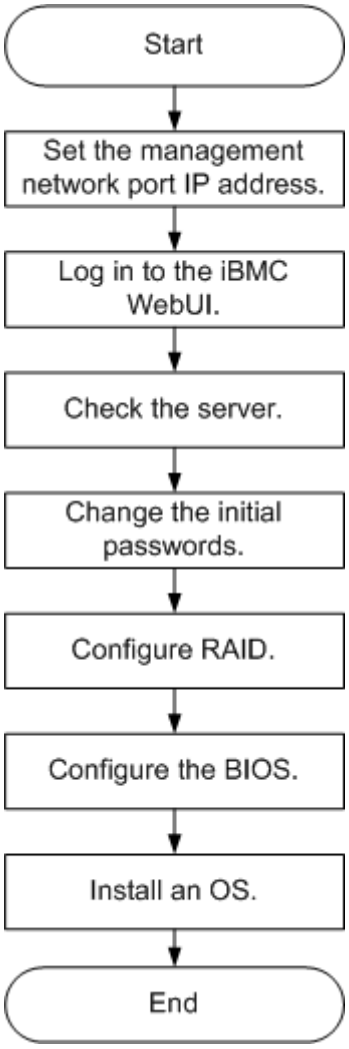


Table 5-6 Configuration process

Step	Action
Set the management network port IP address.	Set an IP address for the management network port.
Log in to the iBMC WebUI.	Log in to the iBMC WebUI from a local PC.
Check the server.	• Check that the server version information is correct. • Check that no alarm exists on the server.
Change the initial password.	• Change your password for logging in to the server iBMC. • Change the U-boot password.
Configure RAID.	Configure RAID for the server. For details, see **RAID Controller Card User Guide (Kunpeng Processors)**.
Configure the BIOS.	Configure the server BIOS, including the boot mode and BIOS password.
Install an OS.	Install an OS for the server.

5.11.3 Querying the iBMC IP Address

Scenario

This section describes how to set the iBMC IP address on the BIOS.

Default IP Address

The default IP address of the iBMC management network port is 192.168.2.100.

Procedure

Step 1 Access the BIOS. For details, see **5.11.8.1 Accessing the BIOS**.

Step 2 Choose **Advanced > IPMI iBMC Configuration> iBMC Configuration** and press **Enter**.

The **iBMC Config** screen is displayed. See **Figure 5-22** and **Figure 5-23**.

Figure 5-22 iBMC Config screen 1

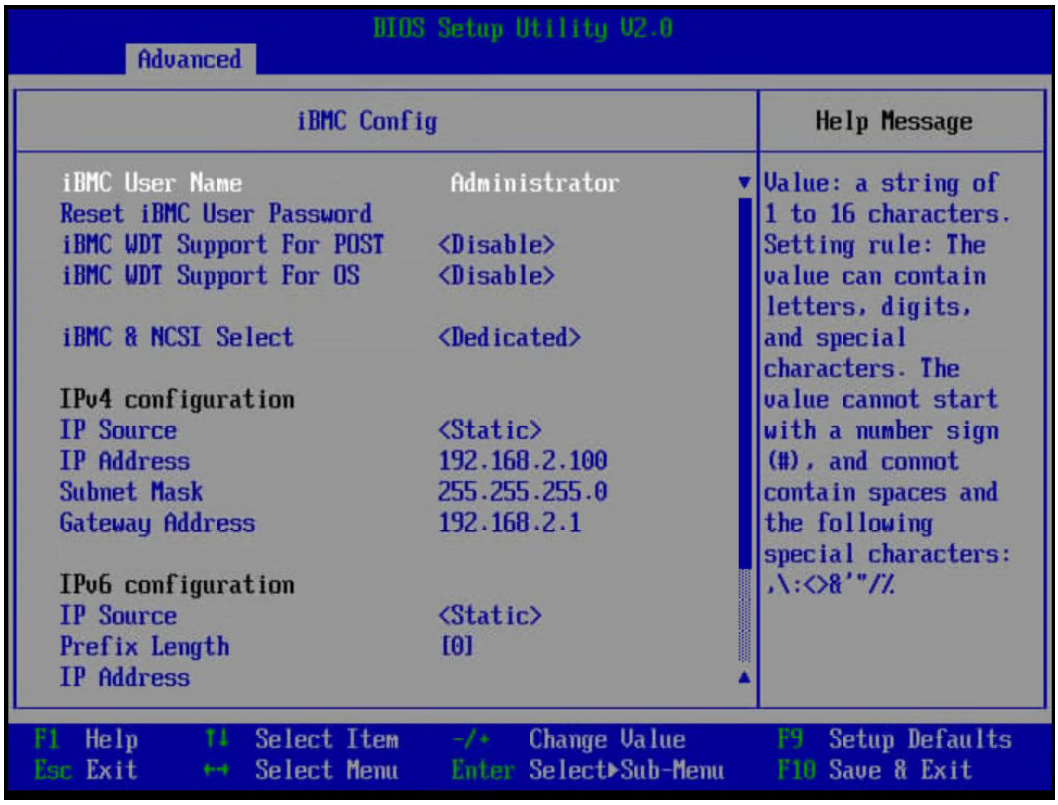
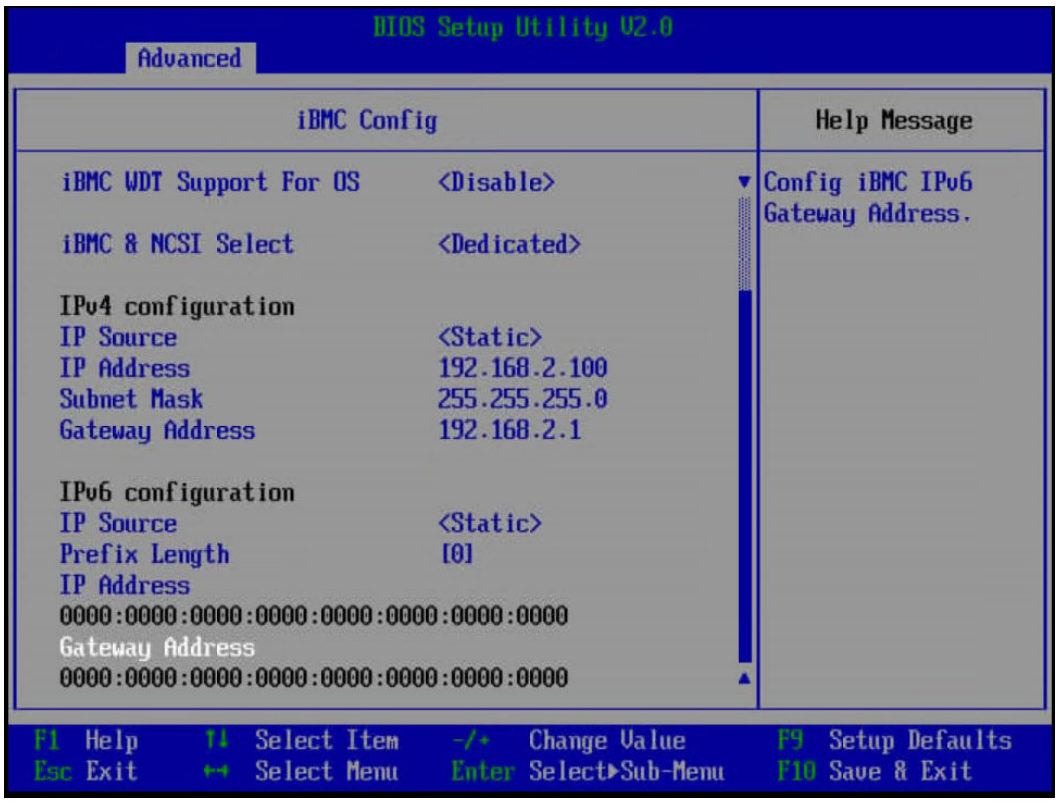


Figure 5-23 iBMC Config screen 2



----End

5.11.4 Logging In to the iBMC WebUI

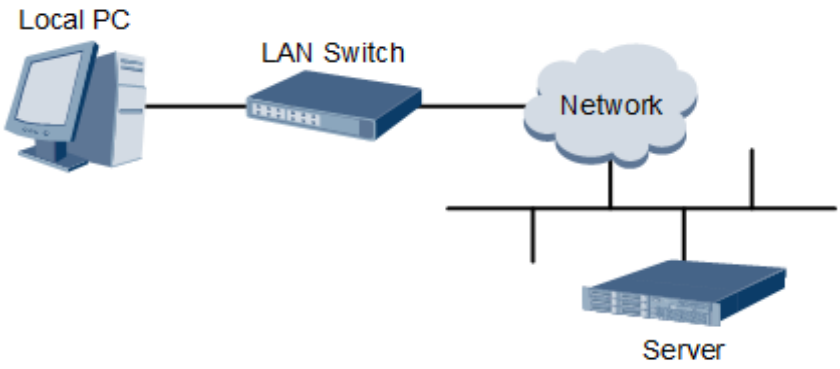
This section uses a PC running Windows 7 and Internet Explorer 11.0 as an example.

For details about system configuration requirements of the local PC, see **TaiShan Rack Server iBMC User Guide**.

Step 1 Use a crossover cable or twisted pair cable to connect the local PC to the iBMC management network port of the server.

Figure 5-24 shows the network diagram.

Figure 5-24 Network diagram



Step 2 Open Internet Explorer on the local PC.

Step 3 In the address box, enter the iBMC address in the format:

https://*IP address of the iBMC management network port on the server*

Example: **https://192.168.2.100**

Step 4 Press **Enter**.

The iBMC login page is displayed.

NOTE

- If the message "There is a problem with this website's security certificate" is displayed, click **Continue to this website (not recommended)**.
- If the **Security Alert** dialog box is displayed indicating a certificate error, click **Yes**.

Step 5 On the iBMC login page, enter your user name and password.

For details about the default user name and password of the iBMC, see **TaiShan Server Account List**.

NOTE

If the account is locked due to five consecutive failed attempts, try again in 5 minutes.

Step 6 In the **Domain** drop-down list, select **This iBMC**.

Step 7 Click **Log In**.

If the login is successful, the **Home** page is displayed.

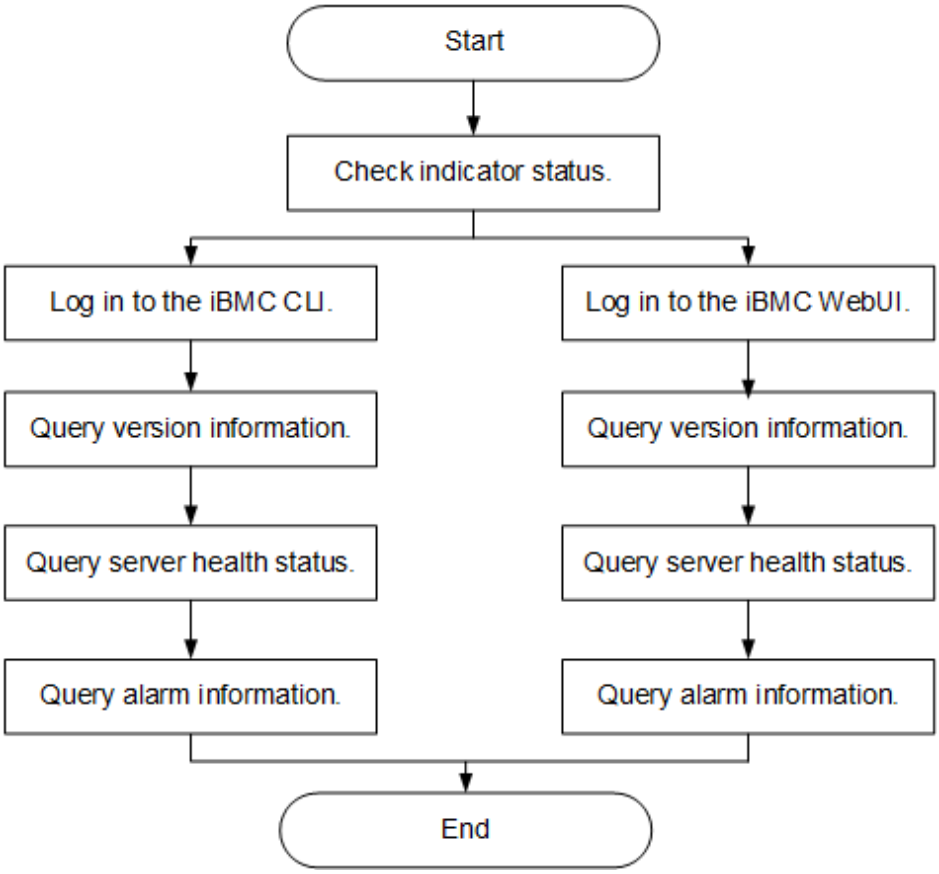
----End

5.11.5 Checking the Server

Check the server in the sequence shown in **Figure 5-25**. Choose a method based on the actual situation.

For details about CLI commands, see **TaiShan Rack Server iBMC User Guide**.

Figure 5-25 Checking the server



Procedure

Step 1 Check the indicator status.

Ensure that hardware devices are working properly.

For details, see **2.2 Indicators and Buttons on the Front Panel** and **2.4 Indicators on the Rear Panel**.

Step 2 Check the server.

- Check the server using the iBMC WebUI.
  a. Log in to the iBMC over the WebUI. For details, see **5.11.4 Logging In to the iBMC WebUI**.

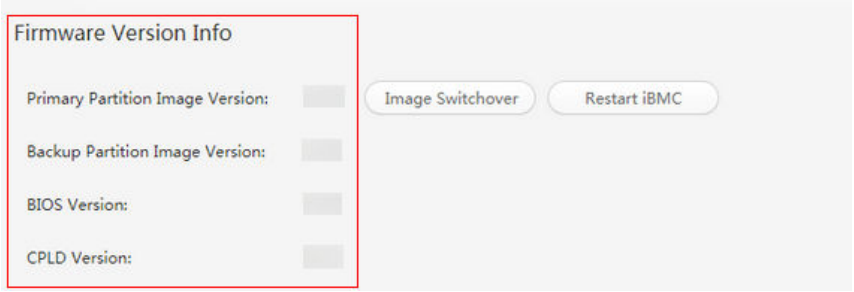
NOTE

You are advised to change the initial password when logging in to the iBMC for the first time. For details, see **5.11.6 Changing Initial Passwords**.

b. Check the server firmware version.

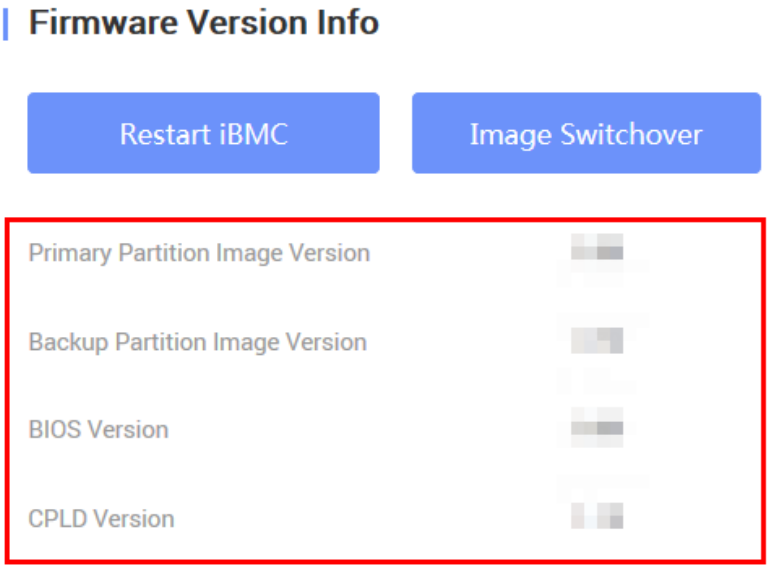
- If the iBMC version is V549 or earlier, choose **System** > **Firmware Upgrade**. The page shown in **Figure 5-26** is displayed.

Figure 5-26 Querying firmware information (iBMC V549 or earlier)



- If the iBMC version is V561 or later, choose **iBMC Settings** > **Firmware Upgrade**. The page shown in **Figure 5-27** is displayed.

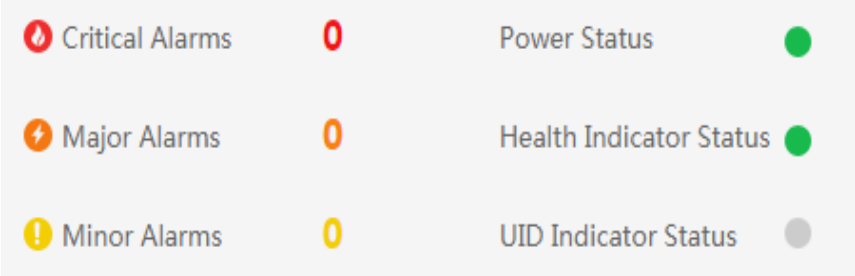
Figure 5-27 Querying firmware information (iBMC V561 or later)



c. Check the server health status.

- If the iBMC version is V549 or earlier, choose **Information** > **Overview**. The page shown in **Figure 5-28** is displayed.

Figure 5-28 Querying alarm information (iBMC V549 or earlier)



- If the iBMC version is V561 or later, view **Alarm Statistics** on the **Home** page, as shown in **Figure 5-29**.

Figure 5-29 Querying alarm information (iBMC V561 or later)

d. Clear any alarms if present. For details, see **TaiShan Rack Server iBMC Alarm Handling**.

- Check the server using the iBMC CLI.

a. Set an IP address for the PC, and ensure that the IP address is on the same network segment as the iBMC management network port.

b. Connect the network port on a PC to the iBMC management network port of the server using a network cable.

c. Start a CLI management tool (such as SSH and PuTTY) on the PC. Enter the iBMC management network port IP address, your user name, and password to log in to the CLI.

NOTE

By default, SSH is used to log in to the iBMC. If the SSH service is disabled, enable it by choosing **Configuration** > **Services** on the iBMC WebUI.

d. Run the **ipmcget -d ver** command to view the server version. Check that the server version meets site requirements.

```
iBMC:/->ipmcget -d ver
------------------- iBMC INFO --------------------
IPMC CPU: Hi1710
IPMI Version: 2.0
CPLD Version: (U6076)1.00
Active iBMC Version: (U68)3.32
Active iBMC Build: 003
Active iBMC Built: 14:32:33 Apr 15 2019
Backup iBMC Version: 3.32
SDK Version: 3.26
SDK Built: 10:53:30 Mar 18 2019
Active Uboot Version: 2.1.13 (Dec 24 2018 - 20:23:20)
Backup Uboot Version: 2.1.13 (Dec 24 2018 - 20:23:20)
----------------- Product INFO -----------------
Product ID: 0x0001
Product Name: XXXX
iME Version: 0.66
```



```
BIOS Version: (U75)0.90
---------- Mother Board INFO ----------
Mainboard BoardID: 0x00b9
Mainboard PCB: .A
---------- Riser Card INFO ----------
Riser1 BoardName: BC11PRUCRiser1
BoardID: 0x0090
Riser1 PCB: .A
Riser2 BoardName: BC82PRNE
Riser2 BoardID: 0x0032
Riser2 PCB: .A
---------- HDD Backplane INFO ----------
Disk BP1 BoardName:  BC11THBQ
Disk BP1 BoardID: 0x0073
Disk BP1 PCB: .A
Disk BP1 CPLD Version:(U3)1.10
---------- IO Board INFO ----------
IOBoard5 ProductName: BC82IOBA
IOBoard5 BoardID: 0x0069
IOBoard5 PCB: .A
IOBoard5 CPLD Version: (U12)0.01
```

- **CPLD Version**: CPLD version of the server
- **BIOS Version**: BIOS version of the server
- **Active iBMC Version**: active iBMC version of the server
- **Backup iBMC Version**: backup iBMC version of the server

e. Query the server health status.

```
iBMC:/->ipmcget -d health
System in health state
```

- If "System in health state" is displayed, no further action is required.
- If alarm information is displayed, go to the next step.

f. Query any generated alarms.

```
iBMC / # ipmcget -d healthevents
Event Num  | Event Time          | Alarm Level  | Event Code   | Event Description
1          | 2019-02-10 00:52:23  | Minor        | 0x12000021   | get description failed.
2          | 2019-02-10 01:37:42  | Minor        | 0x12000013   | Failed to obtain data of the air inlet
temperature.
3          | 2019-02-10 00:52:23  | Minor        | 0x12000019   | Right mounting ear is not present.
4          | 2019-02-10 00:52:19  | Major        | 0x28000001   | The SAS or PCIe cable to front disk
backplane is incorrectly connected.
```

g. Clear alarms. For details, see **TaiShan Rack Server iBMC Alarm Handling**.

----End

5.11.6 Changing Initial Passwords

Change the following initial user passwords:

- Initial password of the default iBMC user
- Initial password for the iBMC U-Boot

NOTE

- For details about the default iBMC user account, see **TaiShan Server Account List**.
- U-Boot is a piece of underlying software used to configure basic settings, for example, initializing hardware devices and setting up memory space mapping, to prepare for commissioning the OS.
- To ensure system security, change your initial password at your first login and change the password periodically.
- A simple password is easy to crack, which makes the system vulnerable. You are advised to use a password that meets complexity requirements or to enable the password complexity check function.
- The password complexity check function is enabled by default.

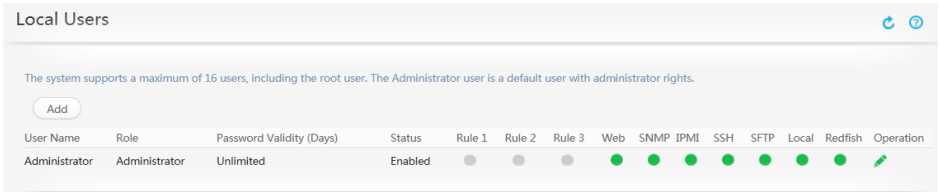
You can change an iBMC user password on the iBMC WebUI or CLI. The following describes how to change a user password on the iBMC WebUI. For details about operations on the iBMC CLI, see **TaiShan Rack Server iBMC User Guide**.

Changing the Initial Password of the Default iBMC User

Step 1 Log in to the iBMC WebUI and open the **Local User** page.

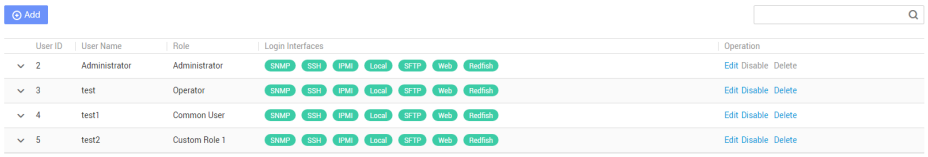
- If the iBMC version is V549 or earlier, choose **Configuration** > **Local Users**. The page shown in **Figure 5-30** is displayed.

Figure 5-30 Local Users page (iBMC V549 or earlier)



- If the iBMC version is V561 or later, choose **User & Security** > **Local Users**. The page shown in **Figure 5-31** is displayed.

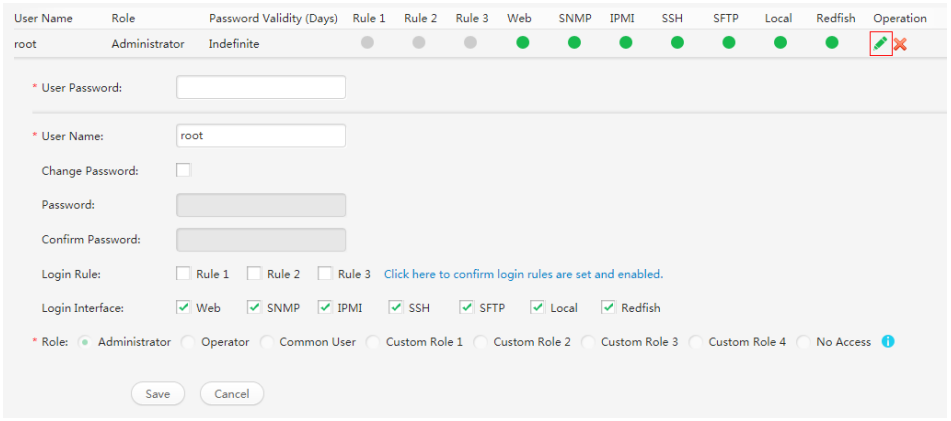
Figure 5-31 Local Users page (iBMC V561 or later)



Step 2 Modify user information.

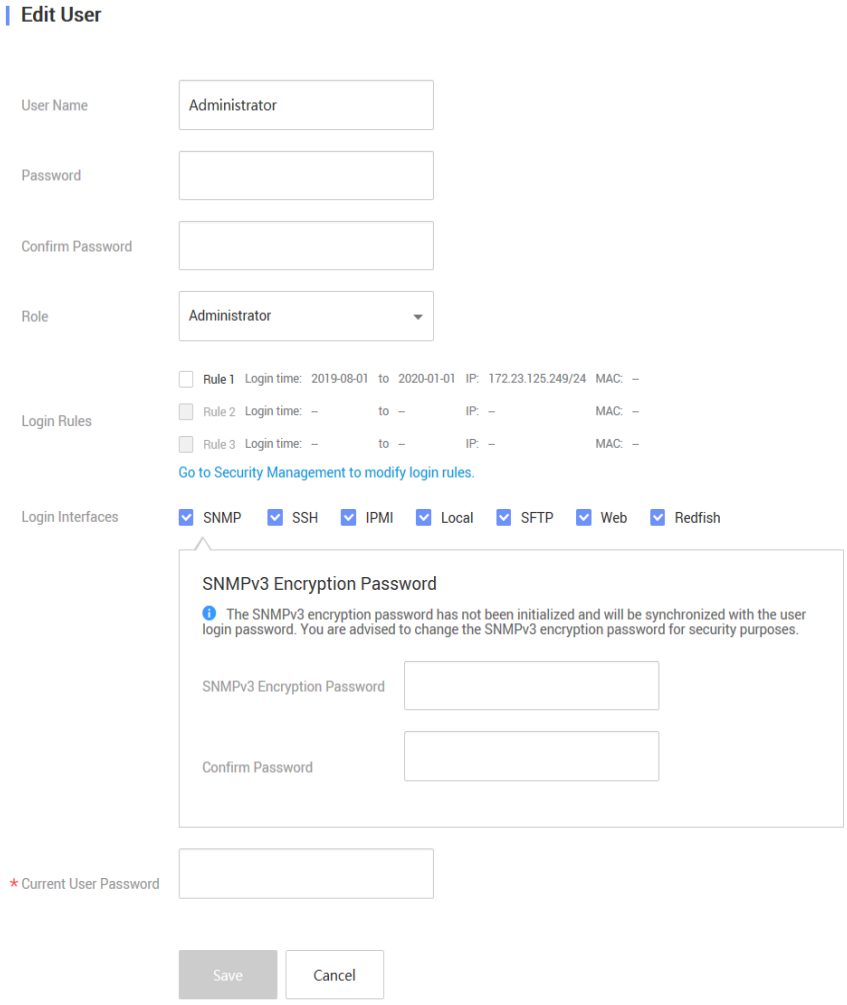
- If the iBMC version is V549 or earlier, locate the user and click . The page shown in **Figure 5-32** is displayed.

Figure 5-32 Modifying user information (iBMC V549 or earlier)



- If the iBMC version is V561 or later, locate the user and click **Edit**. The page shown in **Figure 5-33** is displayed.

Figure 5-33 Modifying user information (iBMC V561 or later)



Step 3 Change the user password following on-screen instructions.

The password must meet the following complexity requirements:

- Contains 8 to 20 characters.
- Contains at least one space or one of the following special characters: `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Contains at least two types of the following characters:
  - Lowercase letters a to z
  - Uppercase letters A to Z
  - Digits 0 to 9
- Cannot be the same as the user name or the user name spelled backwards.

----End

Changing the Initial iBMC U-Boot Password

NOTE

iBMC V663 and later versions do not support U-Boot.

Step 1 Log in to the iBMC CLI over the serial port.

Step 2 Run the following command to restart the iBMC:

iBMC:/->ipmcset -d reset

The command output is as follows:

```
This operation will reboot IPMC system. Continue? [Y/N]:
```

Step 3 Enter **y**.

The system restarts.

Step 4 Press **Ctrl+B** immediately when the system displays the following message:

```
Hit 'ctrl + b' to stop autoboot: 1
```

Step 5 Enter the default password for the iBMC U-Boot.

The following prompt indicates that you have logged in to the U-Boot.

```
U-boot>
```

Step 6 Run the following command to change the U-Boot password:

U-boot> passwd

The following information is displayed:

```
Enter old password:
```

Step 7 Enter the old password.

NOTE

For the default password, see **TaiShan Server Account List**.

The following information is displayed:

```
Enter new password:
```

Step 8 Enter a new password.

The following information is displayed:


```
Enter the new password again:
```

Step 9 Enter the new password again.

If the command output is as follows, the password has been changed:

```
. done
Un-Protected 1 sectors
Erasing Flash...
. done
Erased 1 sectors
Writing to Flash... done
. done
Protected 1 sectors

password be changed successfully.
```

Step 10 Run the **boot** command to exit U-Boot.

----End

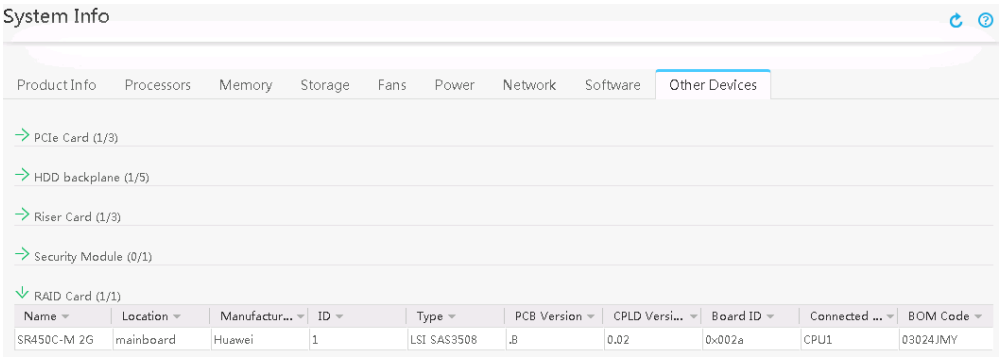
5.11.7 Configuring RAID

Step 1 Log in to the iBMC WebUI. For details, see **5.11.4 Logging In to the iBMC WebUI**.

Step 2 Query RAID controller card information.

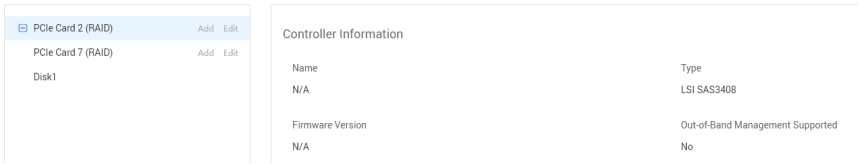
- If the iBMC version is V549 or earlier, choose **Information** > **System Info** > **Other Devices**. The page shown in **Figure 5-34** is displayed.

Figure 5-34 RAID controller card information (iBMC V549 or earlier)



- If the iBMC version is V561 or later, choose **System** > **Storage Management**. The page shown in **Figure 5-35** is displayed.

Figure 5-35 RAID controller card information (iBMC V561 or later)



NOTE

The previous screen information is for reference only. The actual information may differ.

Step 3 Configure RAID.

The RAID configuration method varies according to the RAID controller card model. For details, see **RAID Controller Card User Guide (Kunpeng Processors)**.

----End

5.11.8 Configuring the BIOS

For details about how to configure the BIOS, see **BIOS Parameter Reference (Kunpeng 920 Processor)**.

5.11.8.1 Accessing the BIOS

Step 1 Log in to the Remote Virtual Console. For details, see **8.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI**.

Step 2 On the menu bar of the Remote Virtual Console, click  or  to choose **Power On** or **Forced System Reset** to power on the server.

NOTICE

A forced restart may damage user programs or unsaved data. Exercise caution when performing this operation.

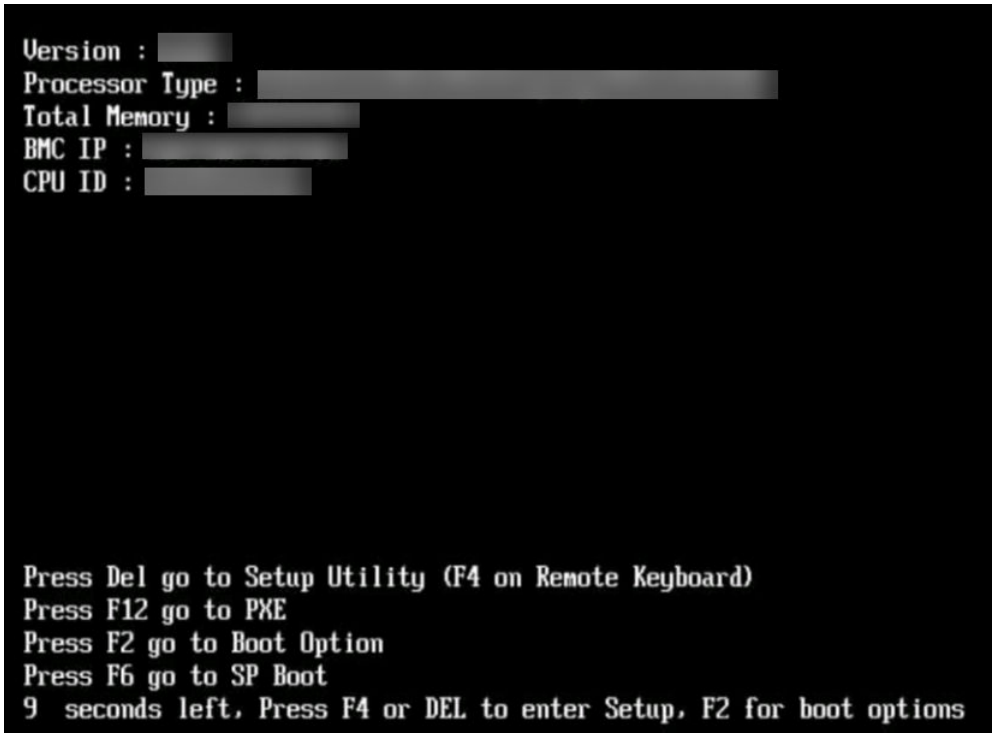
Step 3 When the screen shown in **Figure 5-36** is displayed, press **Delete** or **F4**.

- If the dialog box for entering the password is displayed, as shown in **Figure 5-37**, go to **Step 4**.
- If the dialog box for setting a new password is displayed, as shown in **Figure 5-38**, go to **Step 5**.

NOTE

- Press **F12** to boot from the network.
- Press **F2** for boot options.
- Press **F6** to go to the Smart Provisioning boot screen.

Figure 5-36 BIOS boot screen



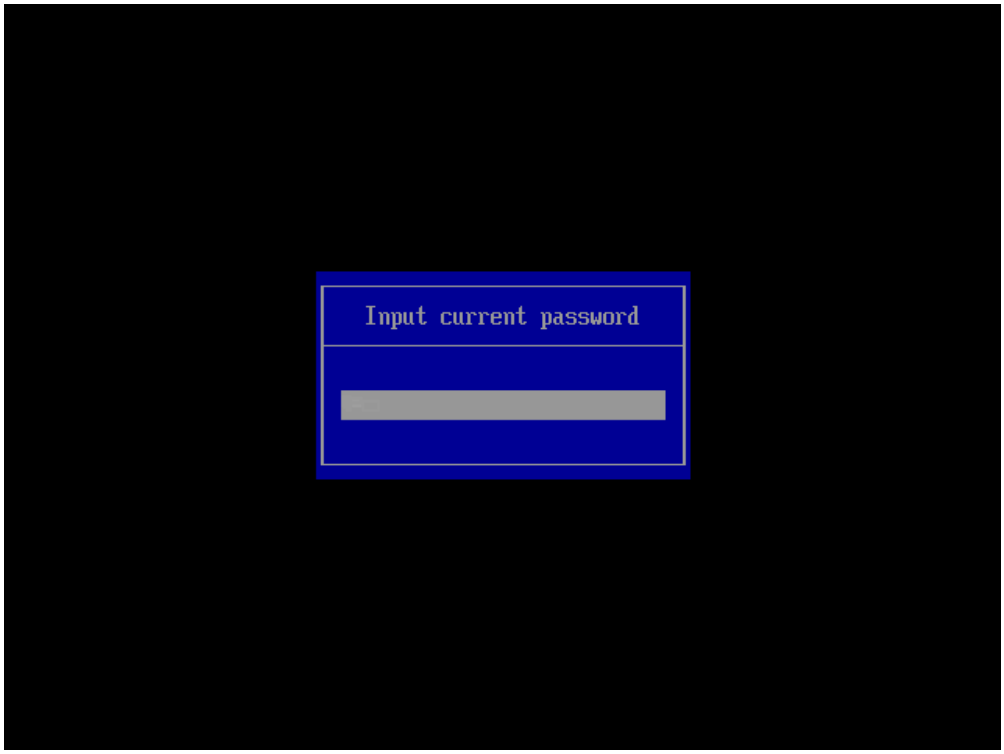
Step 4 Enter the current password.

In the **Input current password** dialog box that is displayed, enter the current password, as shown in **Figure 5-37**.

NOTE

- The BIOS default password is listed in the **TaiShan Server Account List**. Set the administrator password immediately upon the first login. For details, see **5.11.8.4 Setting the BIOS Password**. If you do not want to change the password, press **Enter** when the system prompts you to change the password. Then the **Setup** screen is displayed.
- For security purposes, change the administrator password periodically.
- By default, the server will be locked after three consecutive failed password attempts.

Figure 5-37 Dialog box for entering the current password



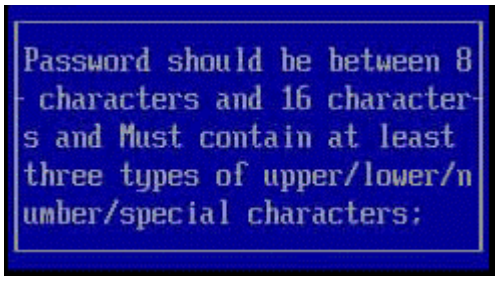
Step 5 Enter a new password.

NOTE

If the BIOS version supports the first-login password function (The BIOS does not have a password by default, and the system prompts you to set a new password when you access the **Setup** screen for the first time), you must set a new password before logging in to the **Setup** screen.

1. In the displayed dialog box shown in **Figure 5-38**, press **Enter**.

Figure 5-38 Setting a new password

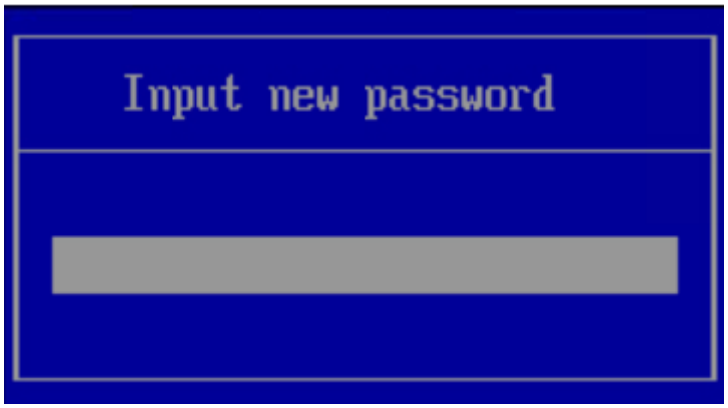


2. In the **Input new password** dialog box that is displayed, enter the new password, as shown in **Figure 5-39**.

NOTE

The password must be a string of 8 to 16 characters, and contain at least three types of the following characters: special characters (mandatory), uppercase letters, lowercase letters, and digits.

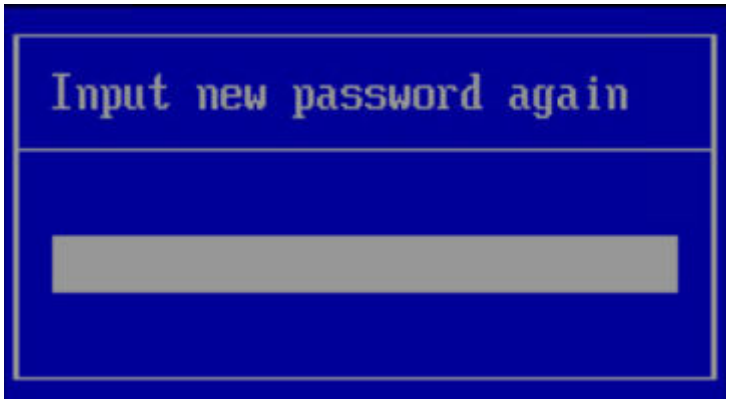
Figure 5-39 Dialog box for entering a new password



3. Input a new password and press **Enter**.

   The dialog box shown in **Figure 5-40** is displayed.

Figure 5-40 Confirmation dialog box



4. Input the password again and press **Enter**.

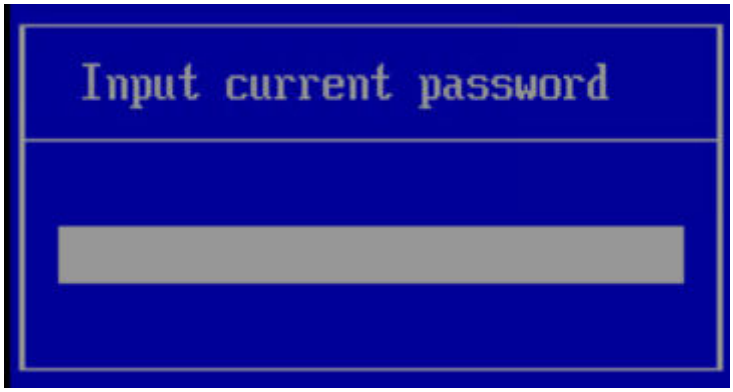
   A dialog box is displayed, indicating that the new password is set successfully, as shown in **Figure 5-41**.

Figure 5-41 Setting a new password

5. Press **Enter**.

   The **Input current password** dialog box is displayed, as shown in **Figure 5-42**.

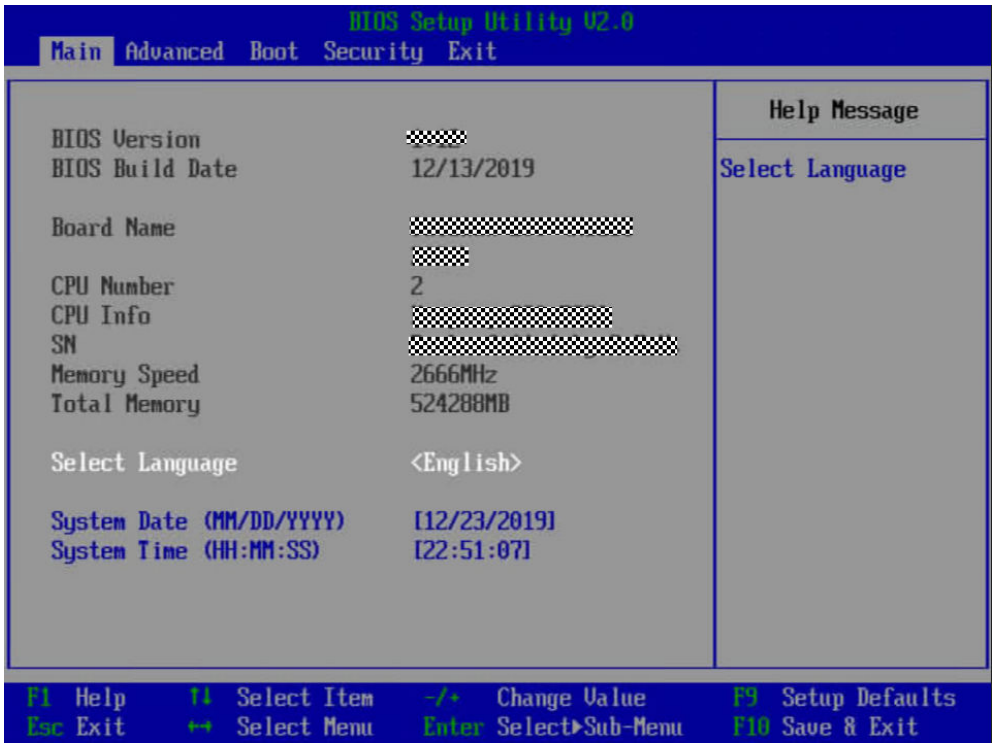
Figure 5-42 Dialog box for entering the current password



6. Enter the new password.

Step 6 Press **Enter**. The **Main** screen is displayed, as shown in **Figure 5-43**.

Figure 5-43 Main screen



----End

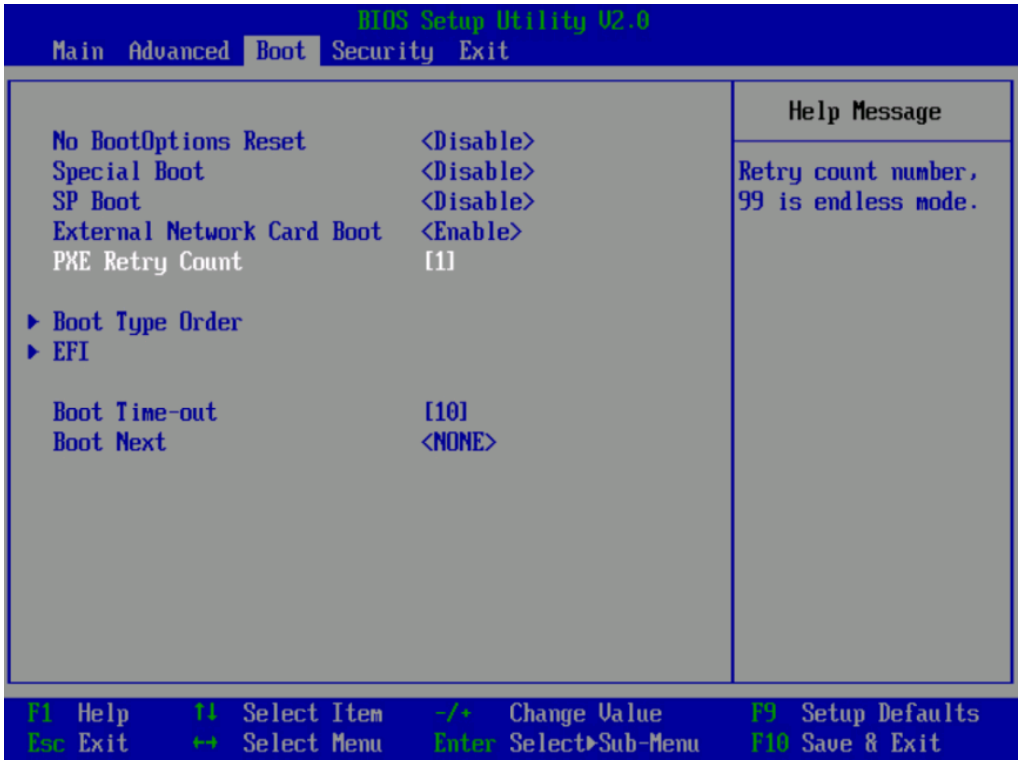
5.11.8.2 Setting the Server Boot Priority

Set the order of boot options using the BIOS.

Step 1 Access the BIOS. For details, see **5.11.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Boot** screen, as shown in **Figure 5-44**.

Figure 5-44 Boot screen



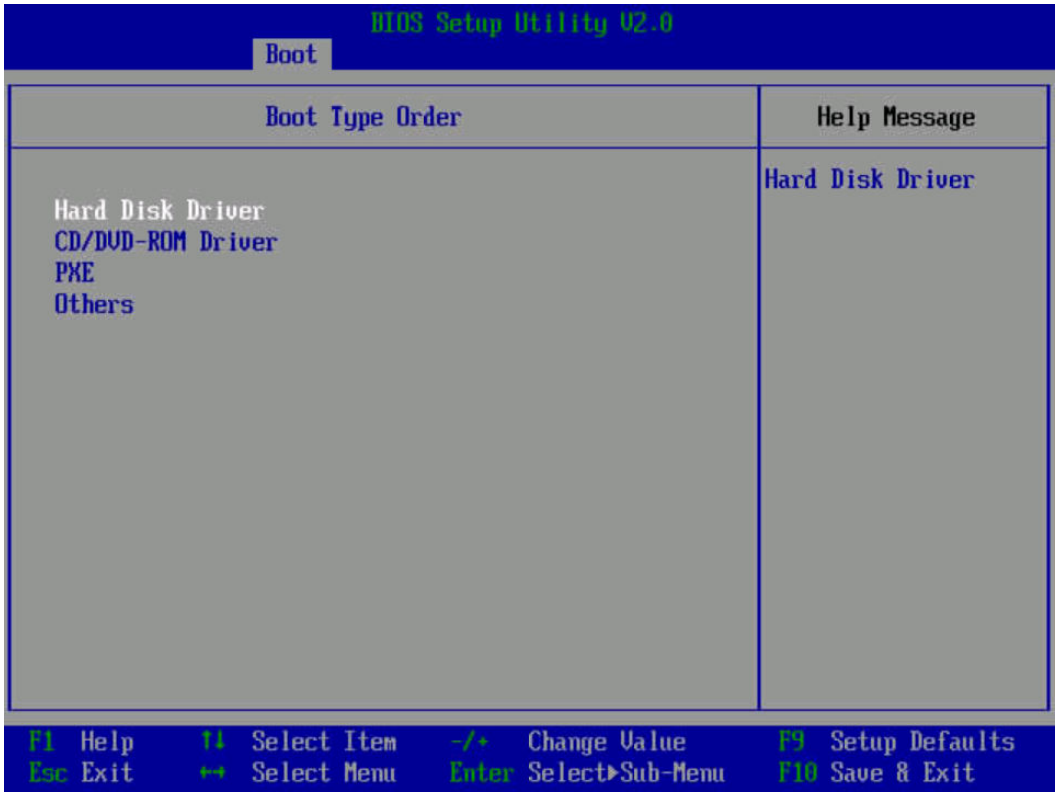
Step 3 Select **Boot Type Order** and press **Enter**.

The **Boot Type Order** screen is displayed, as shown in **Figure 5-45**.

NOTE

The default boot sequence is as follows: **Hard Disk Driver**, **CD/DVD-ROM Driver**, **PXE**, and **Others**.

Figure 5-45 Boot Type Order screen



Step 4 Select a boot option, press **+** or **-** to move the option upward or downward to change the boot order.

NOTE

The server boots in the order specified on this screen.

Step 5 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 6 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

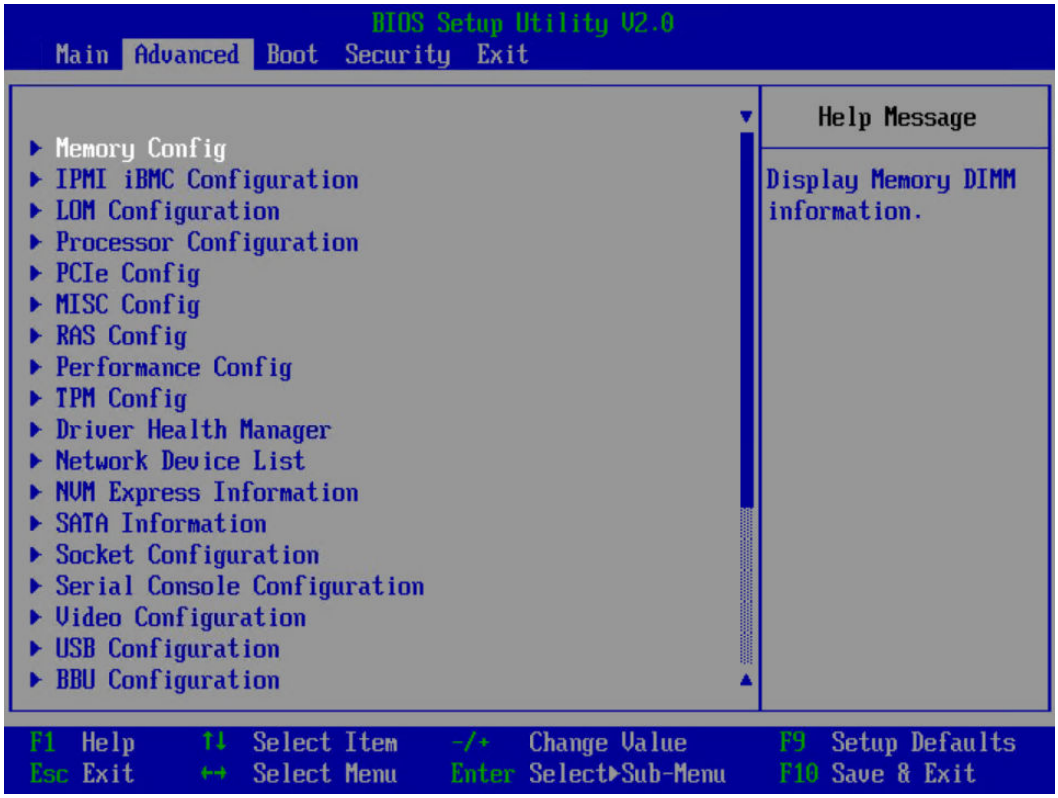
5.11.8.3 Configuring the PXE Function of an NIC

Configuring the LOM PXE

Step 1 Access the BIOS. For details, see **5.11.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Advanced** screen, as shown in **Figure 5-48**.

Figure 5-46 Advanced screen



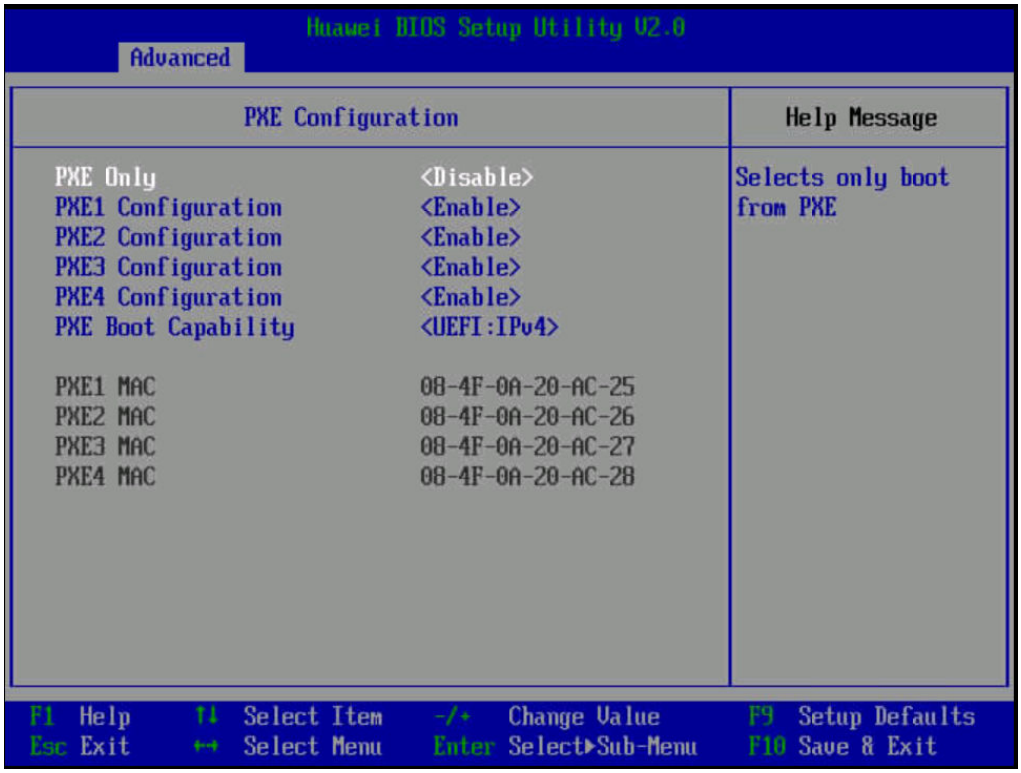
Step 3 Choose **LOM Configuration** > **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed, as shown in **Figure 5-47**.

NOTE

The **PXE Configuration** screen may vary according to the server.

Figure 5-47 PXE Configuration screen



Step 4 Configure the PXE function.

1. Select the network port such as **PXE1 Configuration**, and press **Enter**.
2. In the dialog box that is displayed, select **Enable** and press **Enter**.

Step 5 Select a network protocol for PXE boot.

1. Select **PXE Boot Capability** and press **Enter**.
2. In the dialog box that is displayed, select a network protocol that needs to be supported.
   - UEFI: IPv4
   - UEFI: IPv6
   - UEFI: IPv4/IPv6

Step 6 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 7 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

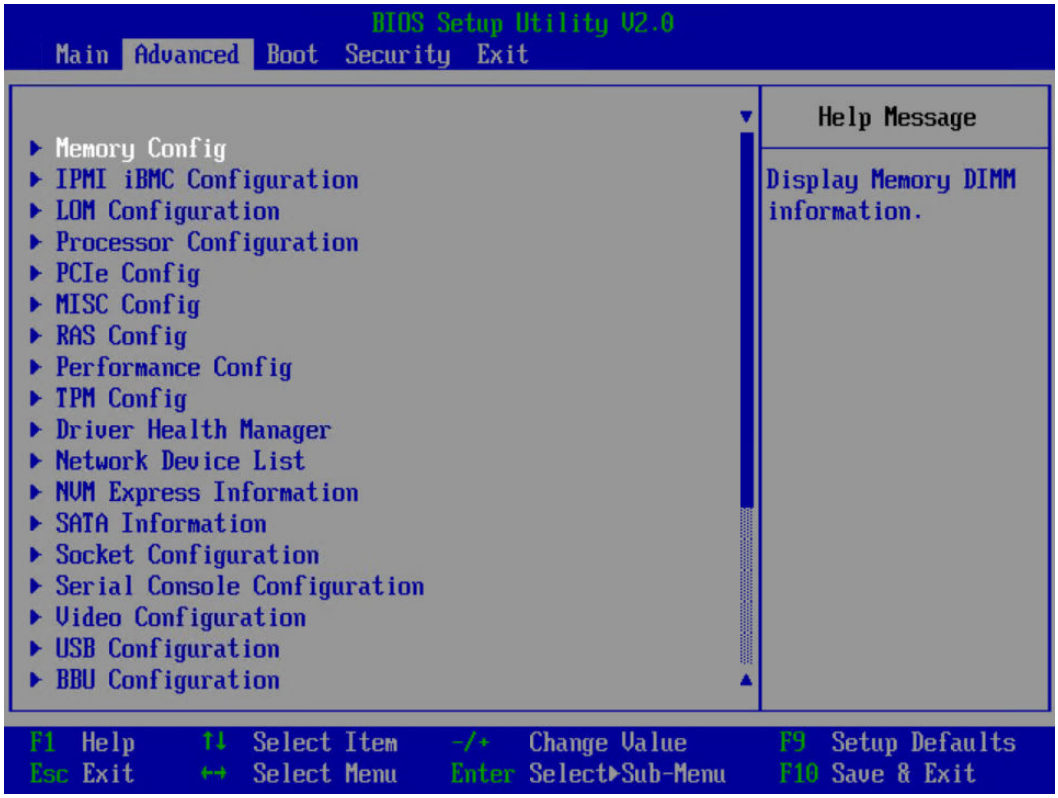
----End

Configuring the PXE Function of a PCIe NIC

Step 1 Access the BIOS. For details, see **5.11.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Advanced** screen, as shown in **Figure 5-48**.

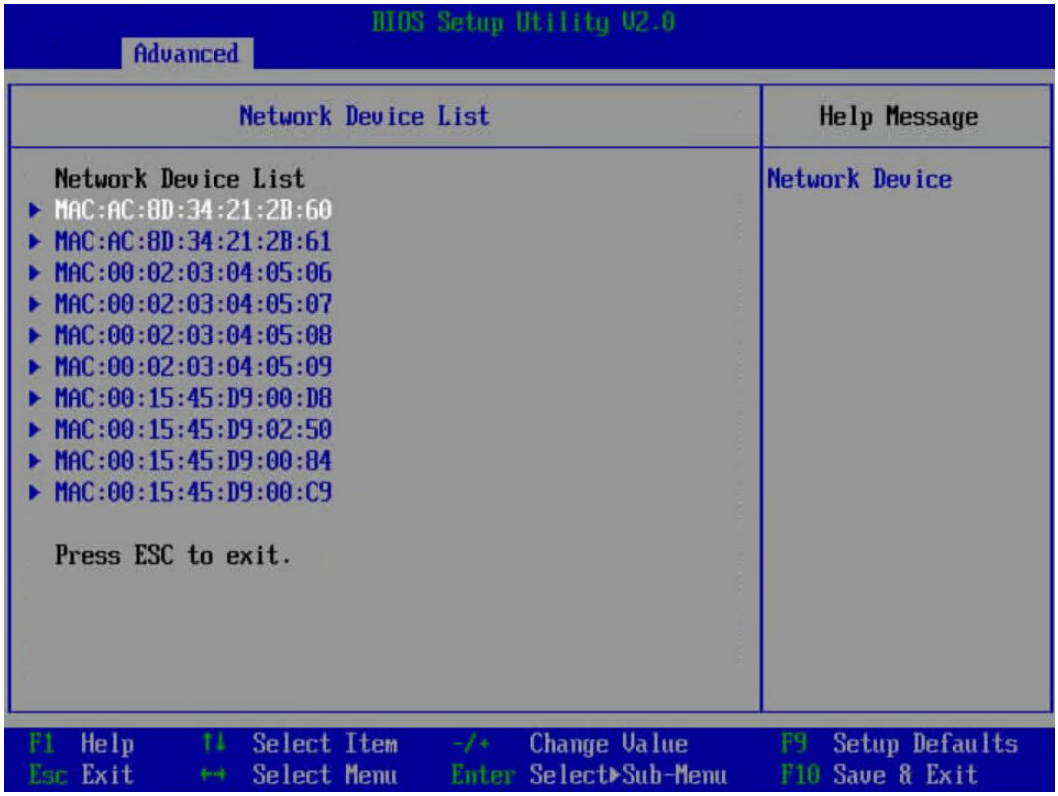
Figure 5-48 Advanced screen



Step 3 Select **Network Device List** and press **Enter**.

The **Network Device List** screen is displayed, as shown in **Figure 5-49**.

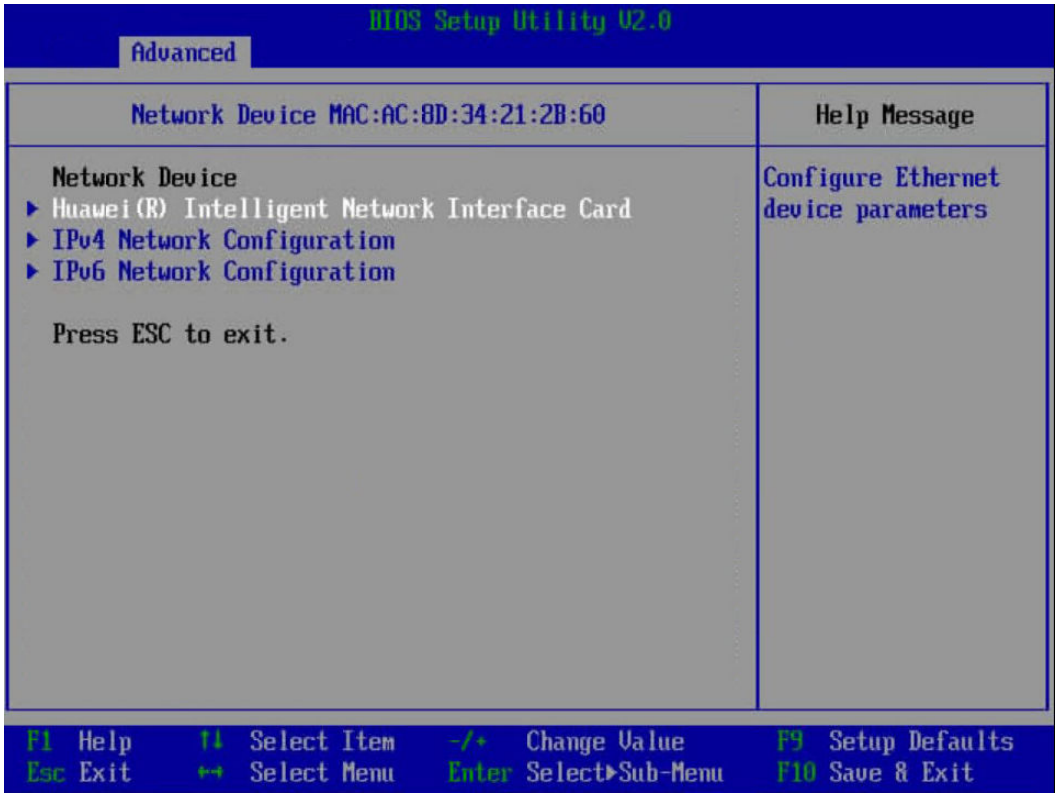
Figure 5-49 Network Device List screen



Step 4 Select the network port (such as **MAC:AC:8D:34:21:2B:60**) of the external NIC, and press **Enter**.

The **Network Device MAC:AC:8D:34:21:2B:60** screen is displayed, as shown in **Figure 5-50**.

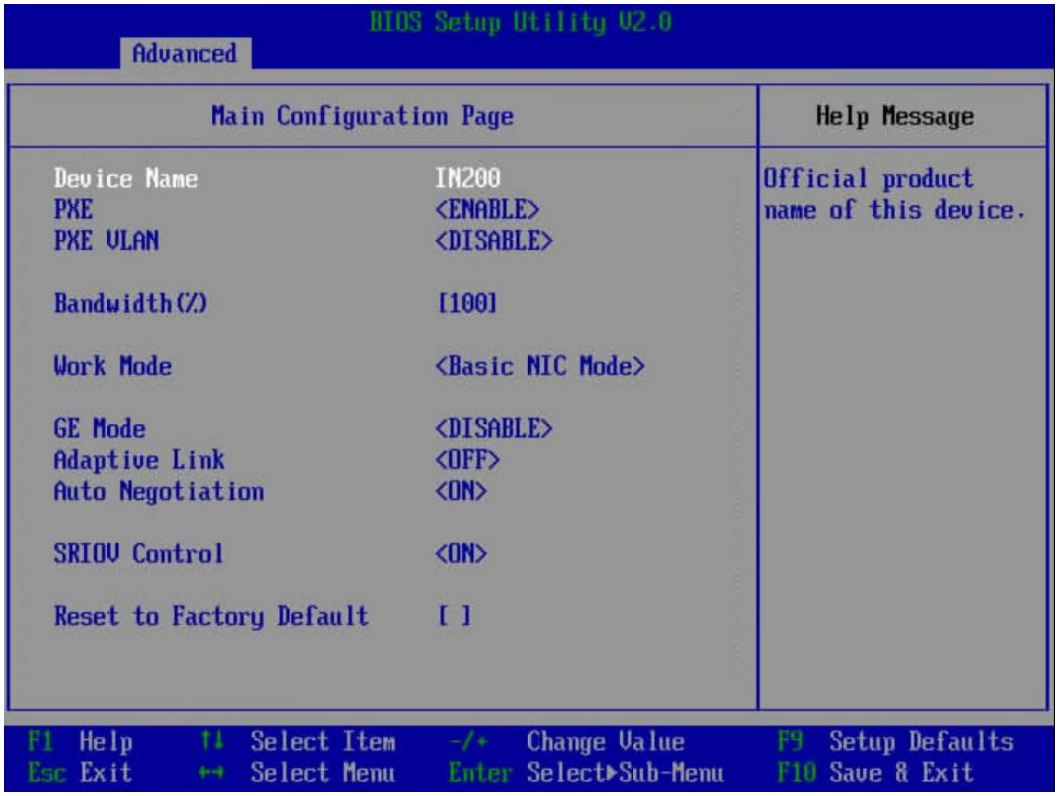
Figure 5-50 Network Device MAC:AC:8D:34:21:2B:60 screen



Step 5 Select **Huawei (R) Intelligent Network Interface Card** and press **Enter**.

The **Main Configuration Page** screen is displayed, as shown in **Figure 5-51**.

Figure 5-51 Main Configuration Page screen



Step 6 Set **PXE** to **ENABLE**.

NOTE

Set other parameters in **Figure 5-51**.

Step 7 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 8 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

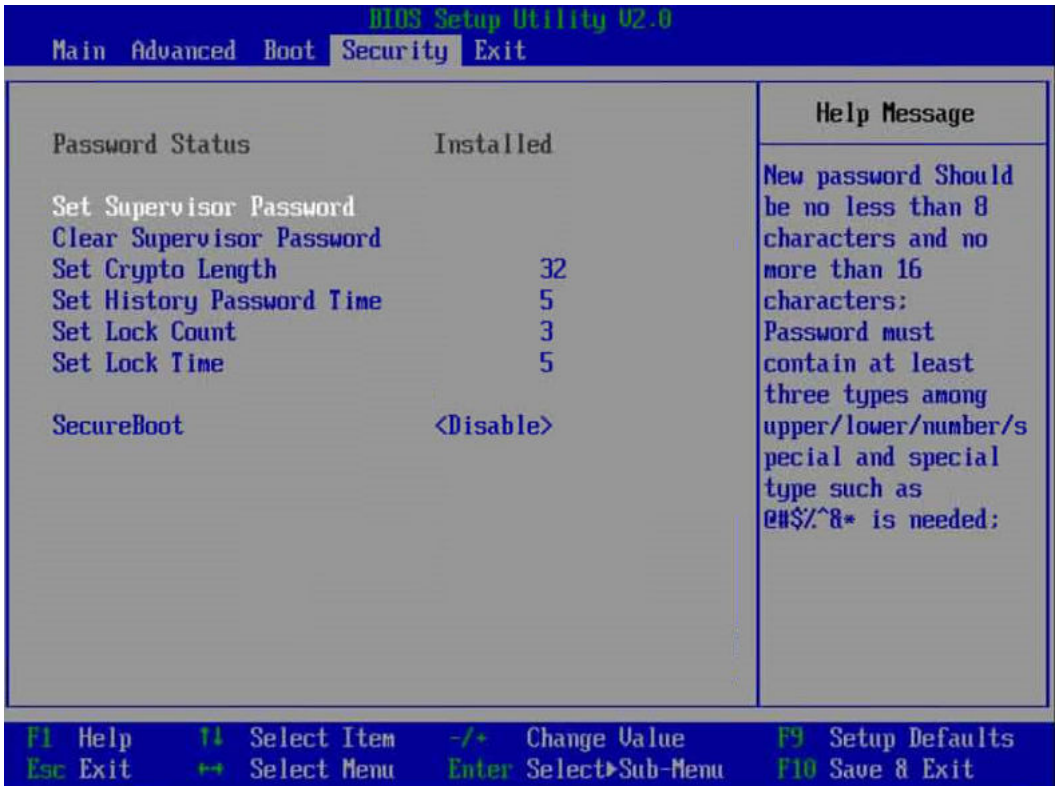
----End

5.11.8.4 Setting the BIOS Password

Step 1 Access the BIOS. For details, see **5.11.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Security** screen, as shown in **Figure 5-52**.

Figure 5-52 Security screen



Step 3 Select **Set Supervisor Password**, press **Enter**, input the original password, and set the administrator password.

NOTE

- The administrator password must be a string of 8 to 16 characters, and contain at least three types of the following characters: special characters including spaces (mandatory), uppercase letters, lowercase letters, and digits.
- The new password cannot be the same as any of the 3 to 6 previously used passwords.
- For details about the default BIOS password, see **TaiShan Server Account List**.

Step 4 (Optional) After the setting is successful, click **Clear Supervisor Password**. Before clearing the password, enter the current password.

Step 5 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 6 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

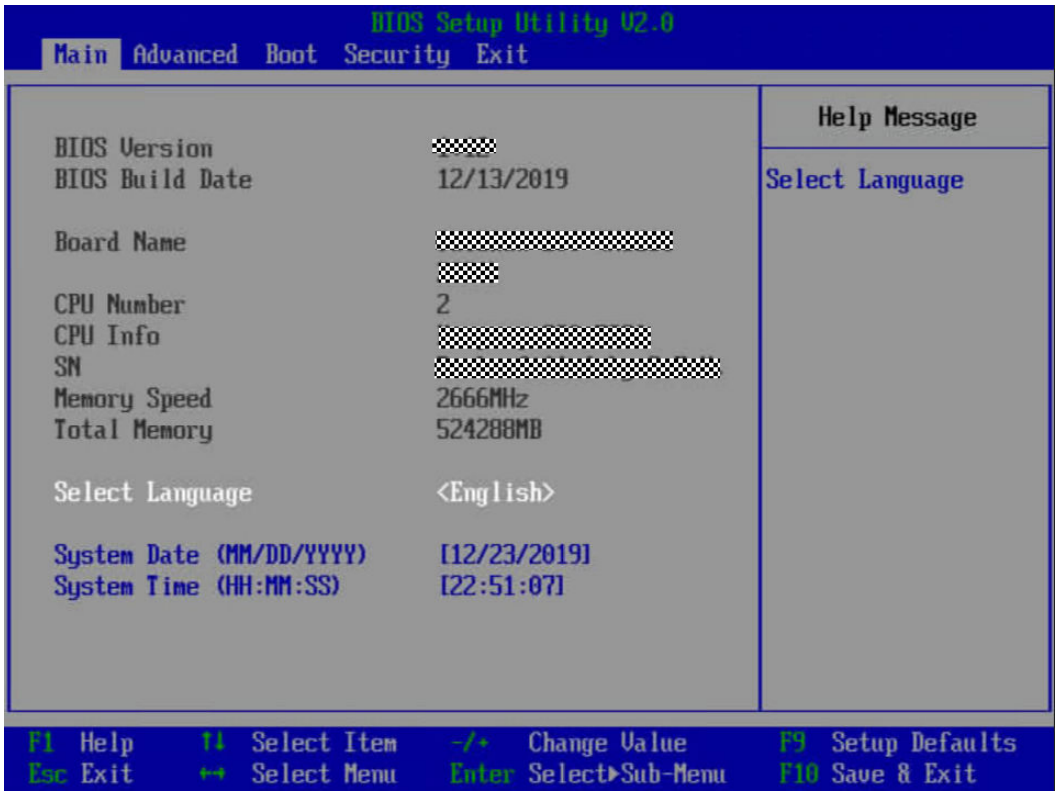
----End

5.11.8.5 Setting the BIOS Language

Step 1 Access the BIOS. For details, see **5.11.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Main** screen, as shown in **Figure 5-53**.

Figure 5-53 Main screen



Step 3 Choose **Select Language**.

Step 4 Press **Enter**.

The **Language** screen is displayed.

Step 5 Select the language to be used and press **Enter**.

Step 6 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 7 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

5.11.9 Installing an OS

The server supports multiple types of OSs. For details, see **Computing Product Compatibility Checker**.

The installation method varies according to the OS type. For details, see the installation guide of the OS you use.

NOTE

Log in to **Kunpeng Computing** and click the product model. On the product documentation page that is displayed, search for, browse, and download the OS installation guide.

5.11.10 Upgrading the System

Upgrade the server software and firmware when needed.

- Enterprise customers: Refer to the upgrade guide of the server you use.
- Telecom carriers: Contact the technical support of your local Huawei office.

Upgrading Firmware or Management Software

Use the iBMC WebUI to upgrade the drive backplane, LCD firmware, mainboard CPLD, and drive backplane CPLD. For details, see **TaiShan Rack Server Upgrade Guide**.

Updating Drivers

If the existing driver versions on a server are inconsistent with those in the driver version mapping, install the drivers of required versions. Otherwise, the server may operate improperly. For details, see the installation guide for each OS, ***Computing Component iDriver*** *Release Notes (ARM)*, and ***Computing Component iDriver*** *Driver Version Mapping (ARM)*.

5.12 Initial Configuration (iBMC V3.01.00.00 or Later)

If the server uses a Hi1711 management chip, the iBMC version is in *X.XX.XX.XX* format, which is also referred to as *VX.XX.XX.XX*. For example, 3.01.00.00, which is also referred to as V3.01.00.00.

5.12.1 Default Data

Table 5-7 Default data

Item	Name	Default Value
iBMC management network port data	IP address and subnet mask	• IP address: 192.168.2.100 • Subnet mask: 255.255.255.0
iBMC login data	User name and password	• For the default user name, see **TaiShan Server Account List**. • For the default password, see **TaiShan Server Account List**.
BIOS data	Password	See **TaiShan Server Account List**.

5.12.2 Configuration Process

Figure 5-54 Initial configuration process

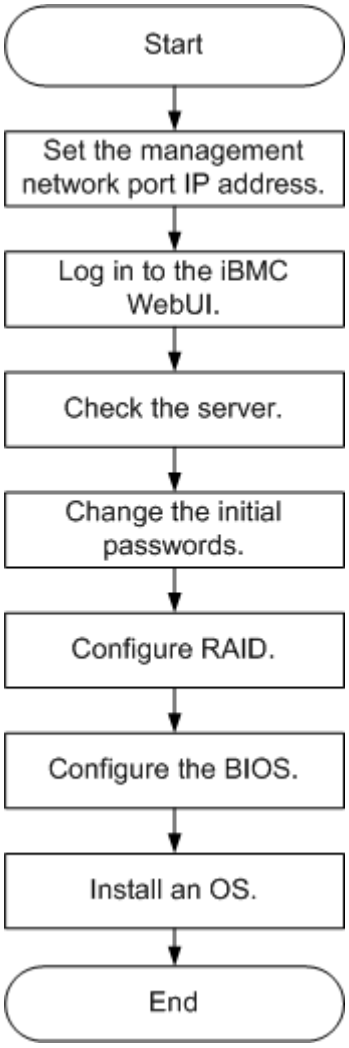


Table 5-8 Configuration process

Step	Action
Set the management network port IP address.	Set an IP address for the management network port.
Log in to the iBMC WebUI.	Log in to the iBMC WebUI from a local PC.
Check the server.	• Check that the server version information is correct. • Check that no alarm exists on the server.
Change the initial password.	Change your password for logging in to the server iBMC.

Step	Action
Configure RAID.	Configure RAID for the server. For details, see **RAID Controller Card User Guide (Kunpeng Processors)**.
Configure the BIOS.	Configure the server BIOS, including the boot mode and BIOS password.
Install an OS.	Install an OS for the server.

5.12.3 Querying the iBMC IP Address

Scenario

This section describes how to set the iBMC IP address on the BIOS.

Default IP Address

The default IP address of the iBMC management network port is 192.168.2.100.

Procedure

Step 1 Access the BIOS. For details, see **5.12.8.1 Accessing the BIOS**.

Step 2 Choose **Advanced > IPMI iBMC Configuration> iBMC Configuration** and press **Enter**.

The **iBMC Config** screen is displayed. See **Figure 5-55** and **Figure 5-56**.

Figure 5-55 iBMC Config screen 1

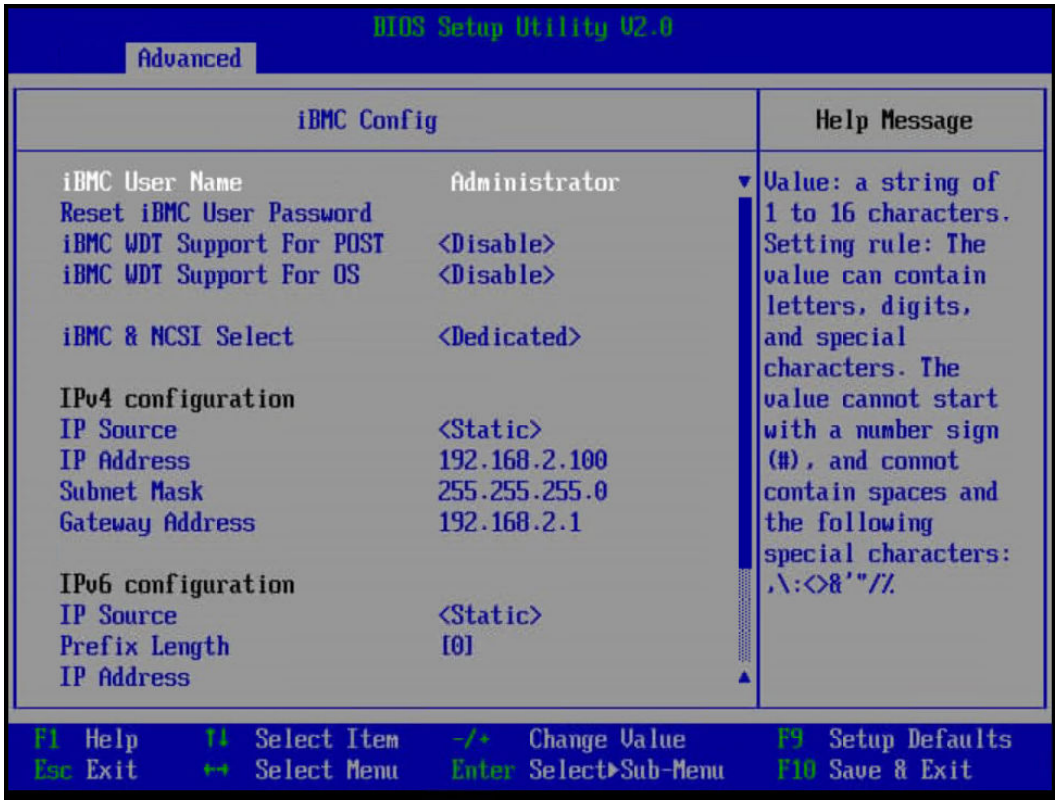
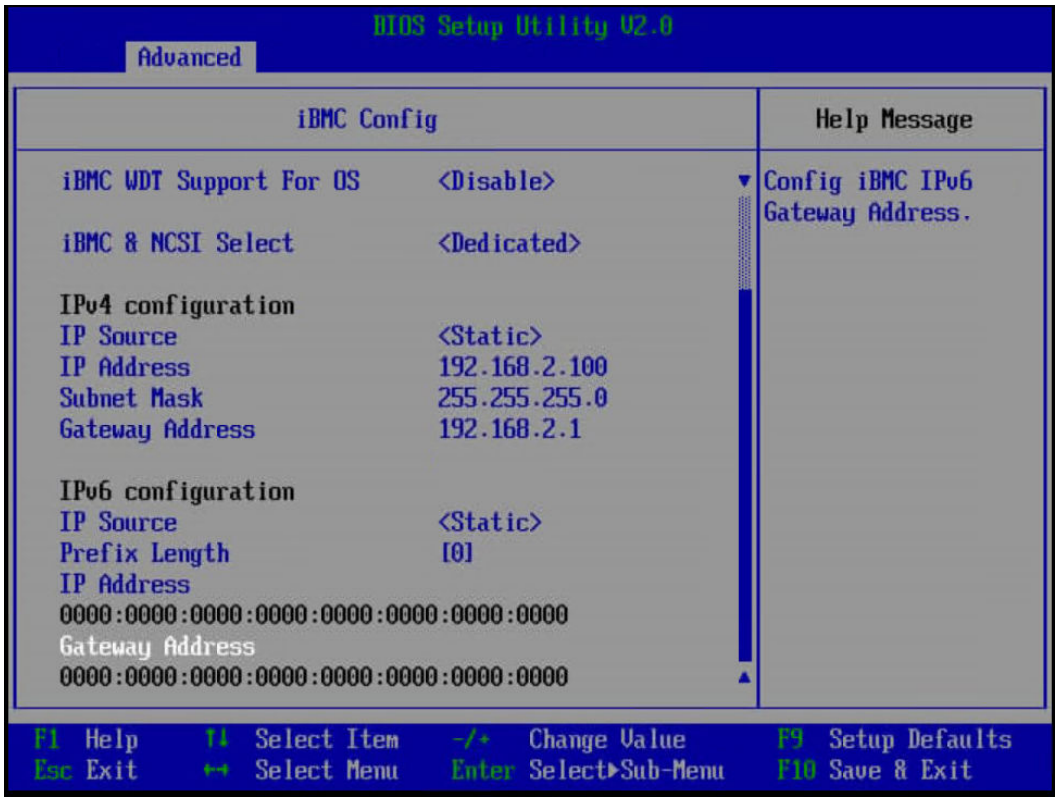


Figure 5-56 iBMC Config screen 2



----End

5.12.4 Logging In to the iBMC WebUI

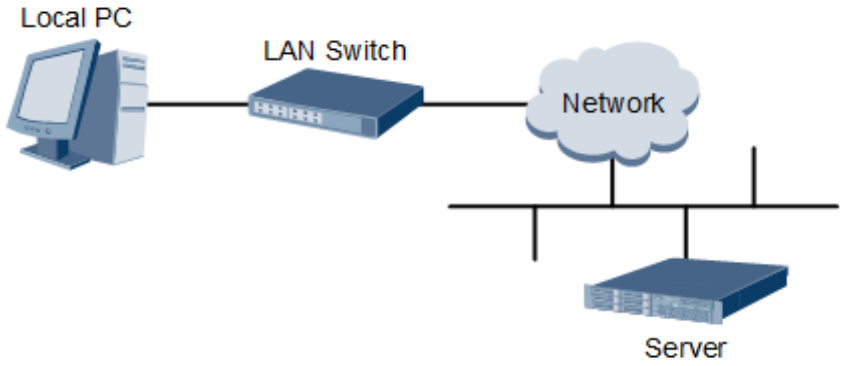
This section uses a PC running Windows 7 and Internet Explorer 11.0 as an example.

For details about system configuration requirements of the local PC, see **TaiShan Rack Server iBMC User Guide**.

Step 1 Use a crossover cable or twisted pair cable to connect the local PC to the iBMC management network port of the server.

Figure 5-57 shows the network diagram.

Figure 5-57 Network diagram



Step 2 Open Internet Explorer on the local PC.

Step 3 In the address box, enter the iBMC address in the format:

https://*IP address of the iBMC management network port on the server*

Example: **https://192.168.2.100**

Step 4 Press **Enter**.

The iBMC login page is displayed.

NOTE

- If the message "There is a problem with this website's security certificate" is displayed, click **Continue to this website (not recommended)**.
- If the **Security Alert** dialog box is displayed indicating a certificate error, click **Yes**.

Step 5 On the iBMC login page, enter your user name and password for logging in to the iBMC.

For the default iBMC user name and password, see **TaiShan Server Account List**.

NOTE

If the account is locked due to five consecutive failed attempts, try again 5 minutes later.

Step 6 In the **Domain** drop-down list, select **This iBMC**.

Step 7 Click **Log In**.

If the login is successful, the **Home** page is displayed.

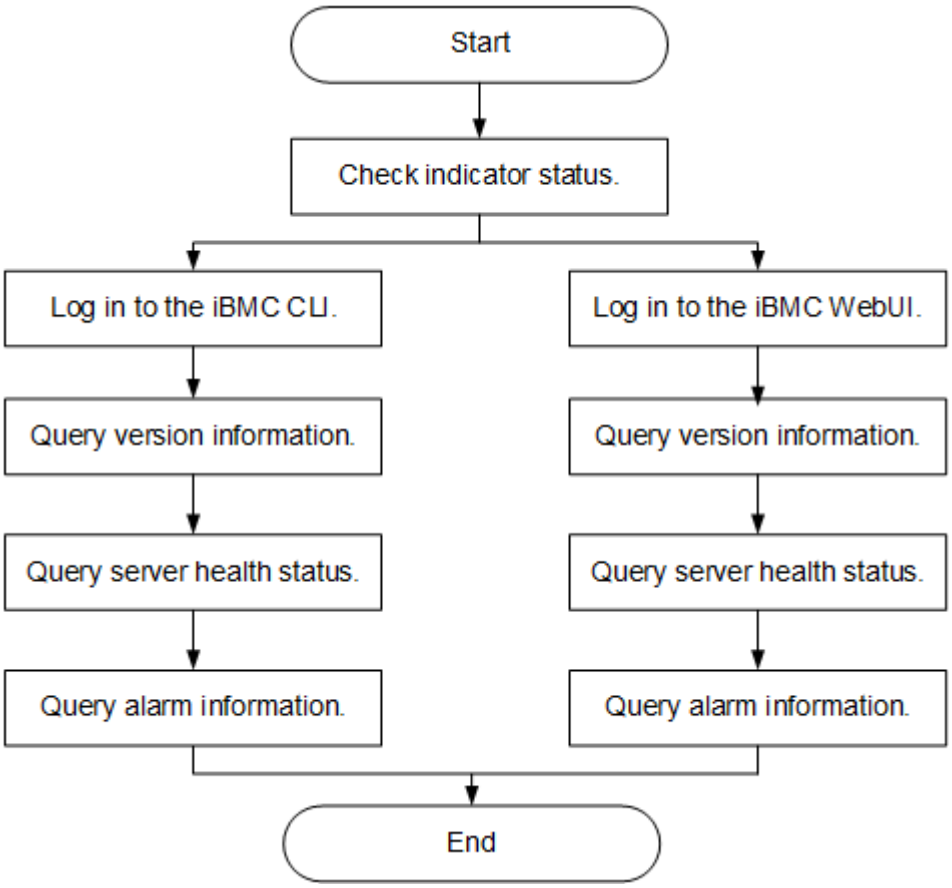
----End

5.12.5 Checking the Server

Check the server in the sequence shown in **Figure 5-58**. Choose a method based on the actual situation.

For details about CLI commands, see **TaiShan Rack Server iBMC User Guide**.

Figure 5-58 Checking the server



Procedure

Step 1 Check the indicator status.

Ensure that hardware devices are working properly.

For details, see **2.2 Indicators and Buttons on the Front Panel** and **2.4 Indicators on the Rear Panel**.

Step 2 Check the server.

- Check the server using the iBMC WebUI.
  a. Log in to the iBMC over the WebUI. For details, see **5.12.4 Logging In to the iBMC WebUI**.

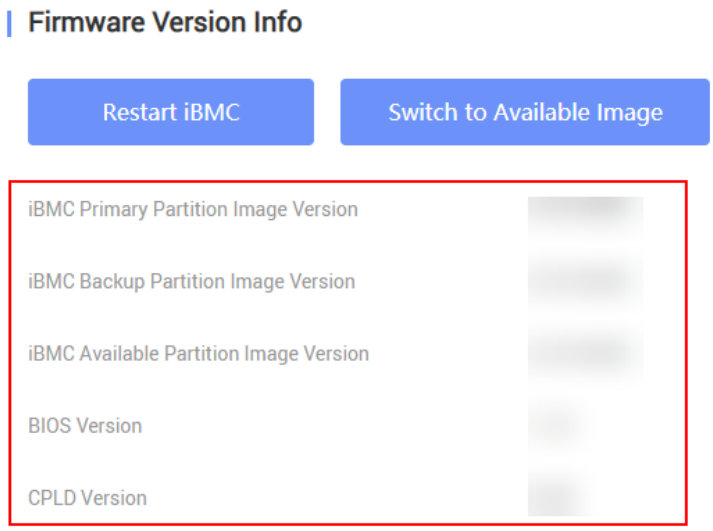
  NOTE

  You are advised to change the initial password when logging in to the iBMC for the first time. For details, see **5.12.6 Changing Initial Passwords**.

  b. Choose **iBMC Settings** on the menu bar, and select **Firmware Upgrade** in the navigation tree. The page shown in **Figure 5-59** is displayed.

  Check that the server version meets site requirements.

Figure 5-59 Firmware version information



c. Check the server status at the upper right corner of the iBMC WebUI, as shown in **Figure 5-60**.

Figure 5-60 Querying the server health status

Icon	Meaning	Description
	Alarm statistics	A critical alarm may power off the server, and even interrupt system services. You must take corrective actions immediately.
		A major alarm has a major impact on the system. It affects the normal operating of the system or may cause service interruption.
		A minor alarm has a minor impact on the system, but you need to take corrective actions as soon as possible to prevent a more severe alarm.
	Power status	Displays server power status. You can click ▾ on the right of the indicator to power on or off the server.
	UID status	Pinpoints the location of the server in a chassis. You can click ▾ on the right of the indicator to control the state of the UID indicator.

d. Clear any alarms if present. For details, see **TaiShan Rack Server iBMC Alarm Handling**.

- Check the server using the iBMC CLI.

a. Set an IP address for the PC. This IP address must be on the same network segment as the iBMC management network port.

b. Connect the network port on a PC to the iBMC management network port of the server using a network cable.

c. Start a CLI management tool (such as SSH and PuTTY) on the PC. Enter the iBMC management network port IP address, your user name, and password to log in to the CLI.

   NOTE

   By default, SSH is used to log in to the iBMC. If the SSH service is disabled, enable it by choosing **Services** > **Port Services** on the iBMC WebUI.

d. Run the **ipmcget -d version** command to view the server version information.

   Check that the server version meets site requirements.

```
iBMC:/->ipmcget -d version
------------------- iBMC INFO --------------------
IPMC              CPU:           Hi1711
IPMI           Version:          2.0
CPLD           Version:          (U151)0.15
Active iBMC    Version:          (U68)3.01.01.00
Active iBMC     Build:           005
Active iBMC     Built:           18:43:56 Mar  6 2020
Backup iBMC    Version:          3.01.01.00
Available iBMC Version:          3.01.01.00
Available iBMC  Build:           005
SDK            Version:          5.0.80.0
SDK              Built:          21:11:10 Feb 29 2020
Active Uboot   Version:          5.0.80.0 (21:21:56 Feb 29 2020)
Backup Uboot   Version:          5.0.80.0 (21:21:56 Feb 29 2020)
Active Secure Bootloader Version: 5.0.80.0 (21:21:55 Feb 29 2020)
Backup Secure Bootloader Version: 5.0.80.0 (21:21:55 Feb 29 2020)
Active Secure Firmware   Version: 5.0.80.0 (21:21:55 Feb 29 2020)
Backup Secure Firmware   Version: 5.0.80.0 (21:21:55 Feb 29 2020)
----------------- Product INFO -----------------
Product            ID:           0x0007
Product          Name:           XXXX
BIOS           Version:          (U75)1.13
-------------- Mother Board INFO ----------------
Mainboard      BoardID:          0x0005
Mainboard        PCB:            .A
------------------- NIC INFO --------------------
NIC 1 (XXX)  BoardID:            0x0067
NIC 1 (XXX)     PCB:             .A
--------------- Riser Card INFO -----------------
Riser1       BoardName:          BC82PRUN
Riser1         BoardID:          0x0093
Riser1           PCB:            .A
Riser2       BoardName:          BC82PRUN
Riser2         BoardID:          0x0093
Riser2           PCB:            .A
-------------- HDD Backplane INFO --------------
Disk BP0      BoardName:         BC82THBB
Disk BP0       BoardID:          0x004a
Disk BP0         PCB:            .A
Disk BP0     CPLD Version:       (U31)0.05
---------------- IO Board INFO ----------------
IOBoard0  ProductName:           BC82IOEA
IOBoard0      BoardID:           0x0063
IOBoard0        PCB:             .A
-------------------- PSU INFO --------------------
PS1            Version:          DC:113 PFC:113
PS2            Version:          DC:111 PFC:111
------------- Security Module INFO -------------
```



```
Specification     Type:          TPM/TCM
Specification  Version:          N/A
Manufacturer      Name:          N/A
Manufacturer   Version:          N/A
```

- **CPLD Version**: CPLD version of the server
- **BIOS Version**: BIOS version of the server
- **Active iBMC Version**: active iBMC version of the server
- **Backup iBMC Version**: backup iBMC version of the server

e. Query the server health status.

```
iBMC:/->ipmcget -d health
System in health state.
```

- If "System in health state" is displayed, no further action is required.
- If alarm information is displayed, go to the next step.

f. Query any generated alarms.

```
iBMC:/->ipmcget -d healthevents
Event Num  | Event Time          | Alarm Level  | Event Code   | Event Description
1          | 2019-02-10 00:52:23  | Minor        | 0x12000021   | get description failed.
2          | 2019-02-10 01:37:42  | Minor        | 0x12000013   | Failed to obtain data of the air inlet
temperature.
3          | 2019-02-10 00:52:23  | Minor        | 0x12000019   | Right mounting ear is not present.
4          | 2019-02-10 00:52:19  | Major        | 0x28000001   | The SAS or PCIe cable to front disk
backplane is incorrectly connected.
```

g. Clear alarms. For details, see **TaiShan Rack Server iBMC Alarm Handling**.

----End

5.12.6 Changing Initial Passwords

You can change an iBMC user password on the iBMC WebUI or CLI. The following describes how to change a user password on the iBMC WebUI. For details about operations on the iBMC CLI, see **TaiShan Rack Server iBMC User Guide**.

NOTE

- For details about the default iBMC user account, see **TaiShan Server Account List**.
- To ensure system security, change your initial password at your first login and change the password periodically.
- A simple password is easy to crack, which makes the system vulnerable. You are advised to use a password that meets complexity requirements or to enable the password complexity check function.
- The password complexity check function is enabled by default.

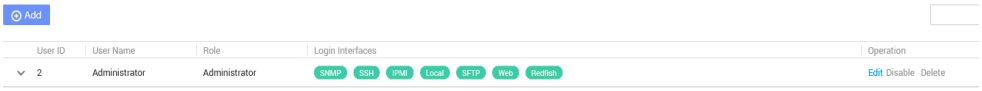
Changing the Initial Password of the Default iBMC User

Step 1 On the iBMC WebUI, choose **User & Security** > **Local Users**.

The **Local Users** page is displayed.

Step 2 Click **Edit** next to the user whose password is to be changed. See **Figure 5-61**.

Figure 5-61 Local Users page



Step 3 Change the user password following on-screen instructions.

The password must meet the following complexity requirements:

- Contains 8 to 20 characters.
- Contains at least one space or one of the following special characters: `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Contains at least two types of the following characters:
  - Lowercase letters a to z
  - Uppercase letters A to Z
  - Digits 0 to 9
- Cannot be the same as the user name or the user name spelled backwards.

----End

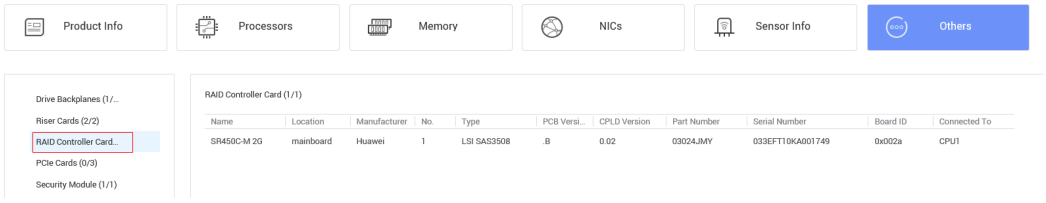
5.12.7 Configuring RAID

Step 1 Log in to the iBMC WebUI. For details, see **5.12.4 Logging In to the iBMC WebUI**.

Step 2 On the top menu bar, choose **System > System Info**. The **System Info** page is displayed.

Step 3 Click the **Others** tab and view the RAID controller card model. See **Figure 5-62**.

Figure 5-62 RAID controller card information



NOTE

The previous screen information is for reference only. The actual information may differ.

Step 4 Configure RAID.

The RAID configuration method varies according to the RAID controller card model. For details, see **RAID Controller Card User Guide (Kunpeng Processors)**.

----End

5.12.8 Configuring the BIOS

For details about how to configure the BIOS, see **BIOS Parameter Reference (Kunpeng 920 Processor)**.

5.12.8.1 Accessing the BIOS

Step 1 Log in to the Remote Virtual Console. For details, see **9.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI**.

Step 2 On the menu bar of the Remote Virtual Console, click or to choose **Power On** or **Forced System Reset** to power on the server.

NOTICE

A forced restart may damage user programs or unsaved data. Exercise caution when performing this operation.

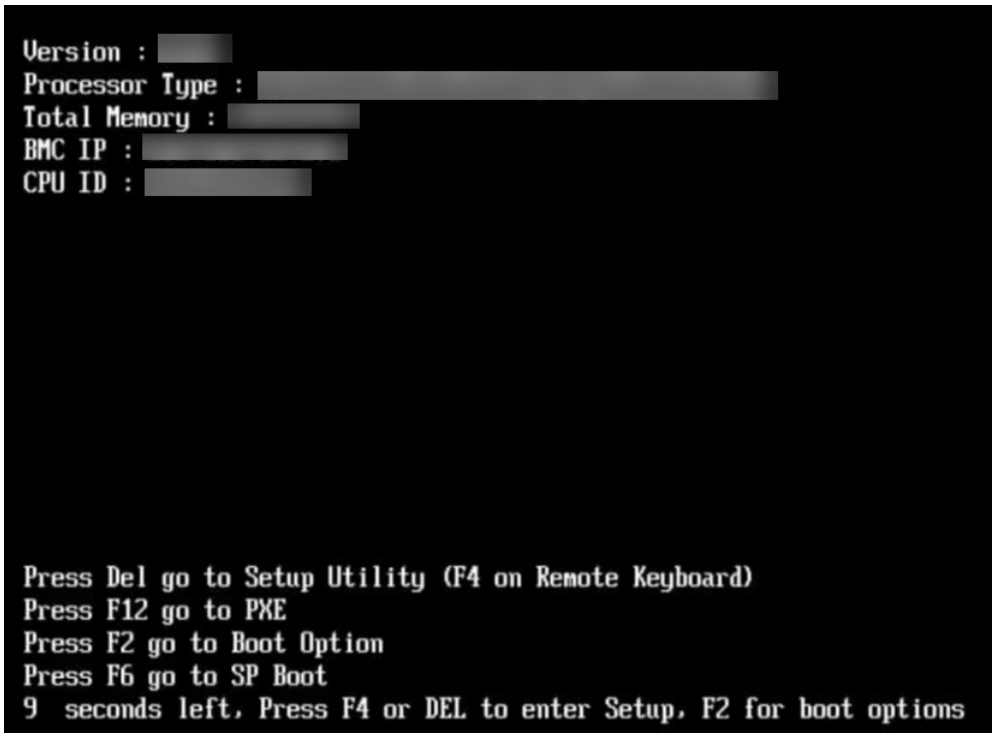
Step 3 When the screen shown in **Figure 5-63** is displayed, press **Delete** or **F4**.

- If the dialog box for entering the password is displayed, as shown in **Figure 5-64**, go to **Step 4**.
- If the dialog box for setting a new password is displayed, as shown in **Figure 5-65**, go to **Step 5**.

NOTE

- Press **F12** to boot from the network.
- Press **F2** for boot options.
- Press **F6** to go to the Smart Provisioning boot screen.

Figure 5-63 BIOS boot screen



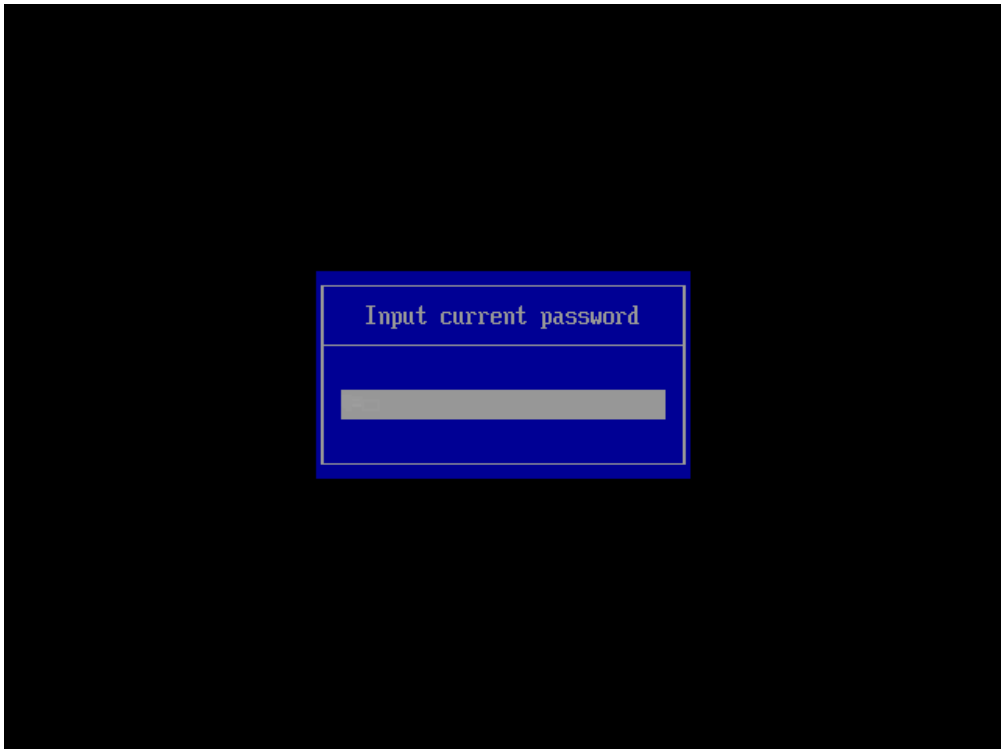
Step 4 Enter the current password.

In the **Input current password** dialog box that is displayed, enter the current password, as shown in **Figure 5-64**.

NOTE

- The BIOS default password is listed in the **TaiShan Server Account List**. Set the administrator password immediately upon the first login. For details, see **5.12.8.4 Setting the BIOS Password**. If you do not want to change the password, press **Enter** when the system prompts you to change the password. Then the **Setup** screen is displayed.
- For security purposes, change the administrator password periodically.
- By default, the server will be locked after three consecutive failed password attempts.

Figure 5-64 Dialog box for entering the current password



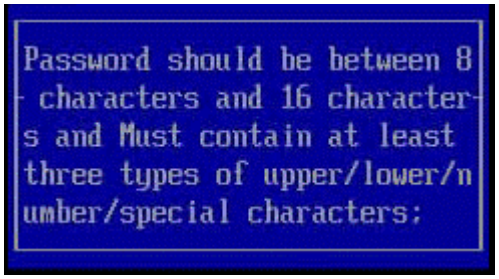
Step 5 Enter a new password.

NOTE

If the BIOS version supports the first-login password function (The BIOS does not have a password by default, and the system prompts you to set a new password when you access the **Setup** screen for the first time), you must set a new password before logging in to the **Setup** screen.

1. In the displayed dialog box shown in **Figure 5-65**, press **Enter**.

Figure 5-65 Setting a new password

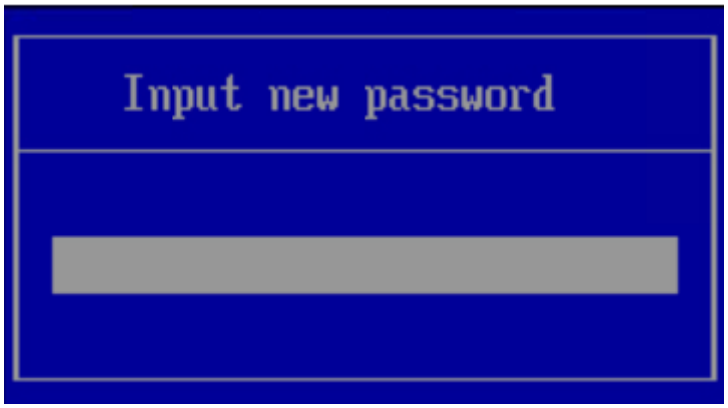


2. In the **Input new password** dialog box that is displayed, enter the new password, as shown in **Figure 5-66**.

   NOTE

   The password must be a string of 8 to 16 characters, and contain at least three types of the following characters: special characters (mandatory), uppercase letters, lowercase letters, and digits.

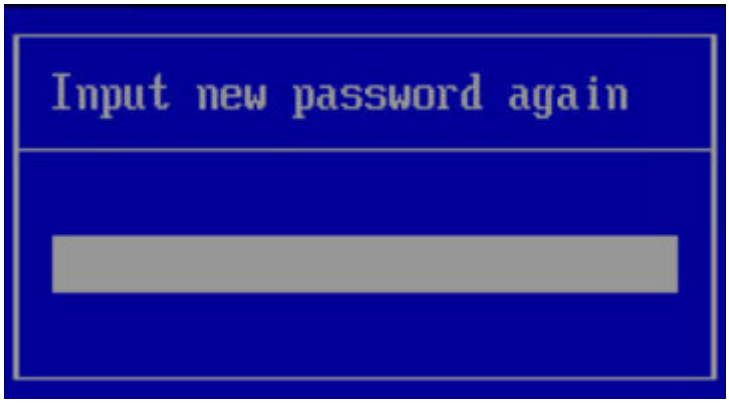
Figure 5-66 Dialog box for entering a new password



3. Input a new password and press **Enter**.

   The dialog box shown in **Figure 5-67** is displayed.

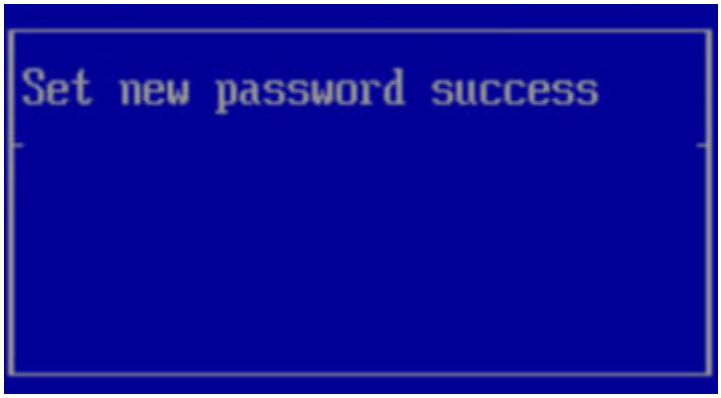
Figure 5-67 Confirmation dialog box



4. Input the password again and press **Enter**.

   A dialog box is displayed, indicating that the new password is set successfully, as shown in **Figure 5-68**.

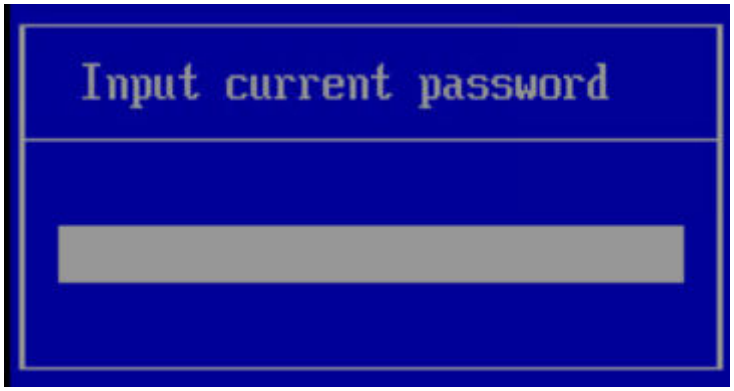
Figure 5-68 Setting a new password



5. Press **Enter**.

   The **Input current password** dialog box is displayed, as shown in **Figure 5-69**.

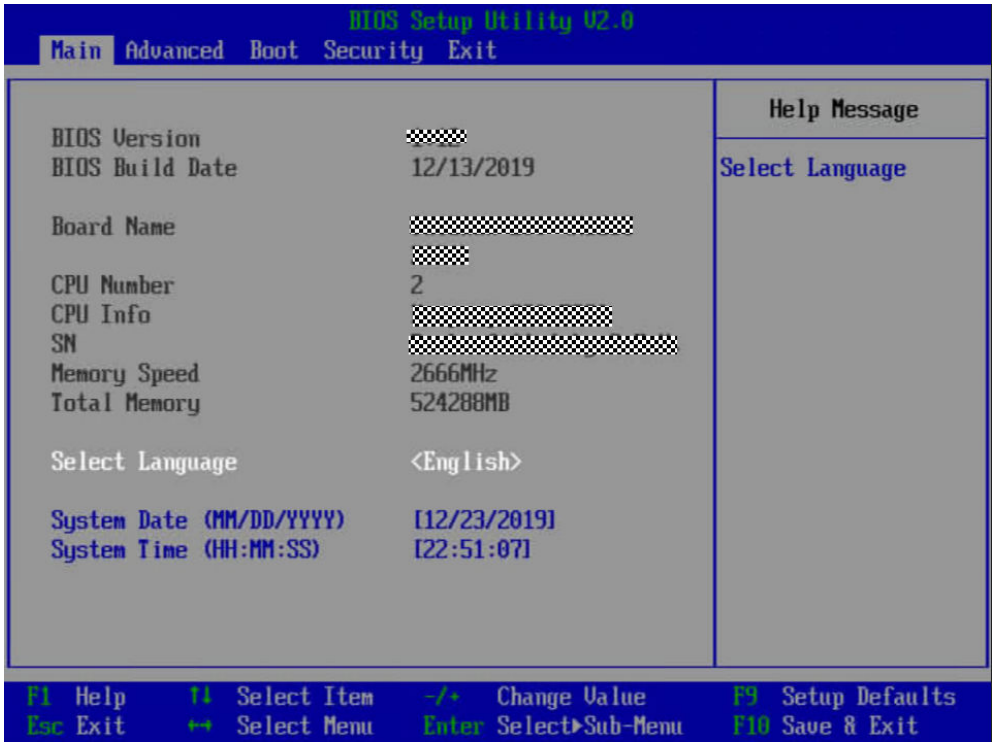
Figure 5-69 Dialog box for entering the current password



6. Enter the new password.

Step 6 Press **Enter**. The **Main** screen is displayed, as shown in **Figure 5-70**.

Figure 5-70 Main screen



----End

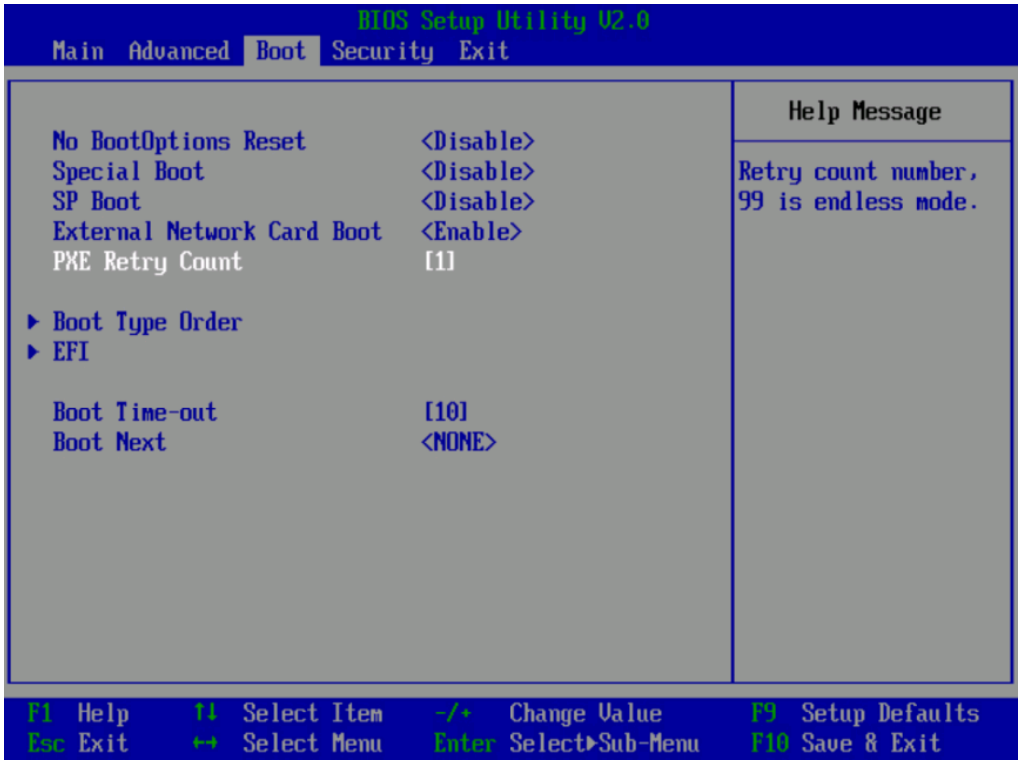
5.12.8.2 Setting the Server Boot Priority

Set the order of boot options using the BIOS.

Step 1 Access the BIOS. For details, see **5.12.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Boot** screen, as shown in **Figure 5-71**.

Figure 5-71 Boot screen



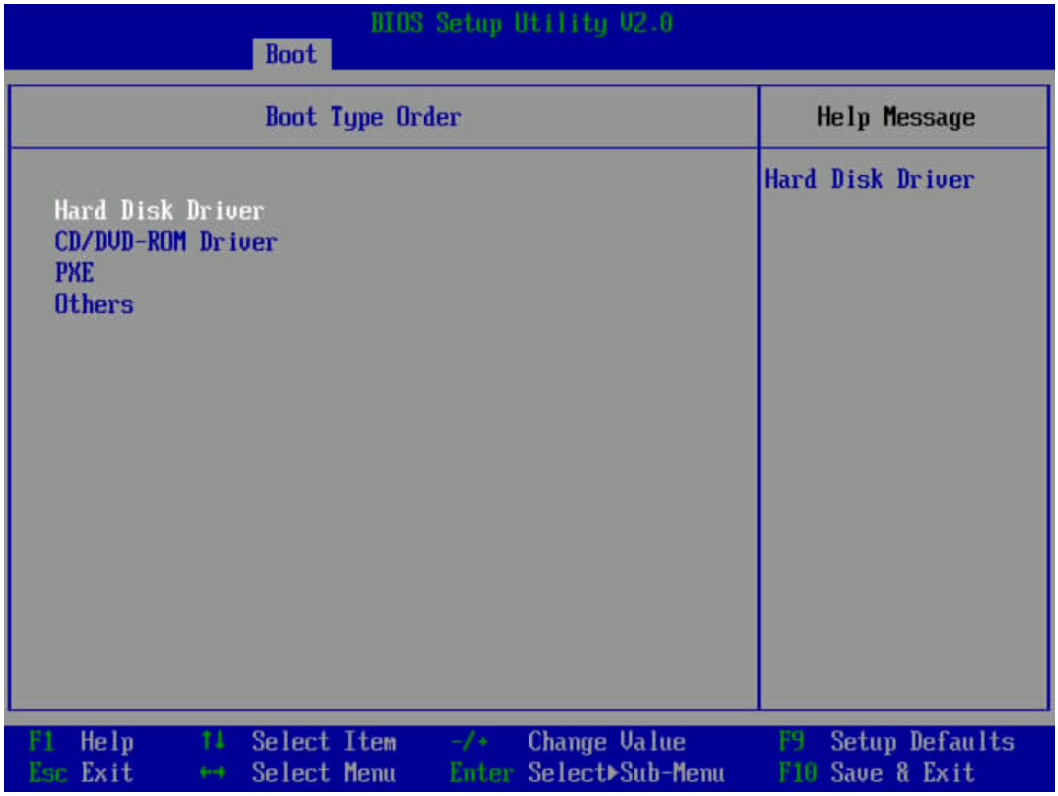
Step 3 Select **Boot Type Order** and press **Enter**.

The **Boot Type Order** screen is displayed, as shown in **Figure 5-72**.

NOTE

The default boot sequence is as follows: **Hard Disk Driver**, **CD/DVD-ROM Driver**, **PXE**, and **Others**.

Figure 5-72 Boot Type Order screen



Step 4 Select a boot option, press **+** or **-** to move the option upward or downward to change the boot order.

NOTE

The server boots in the order specified on this screen.

Step 5 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 6 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

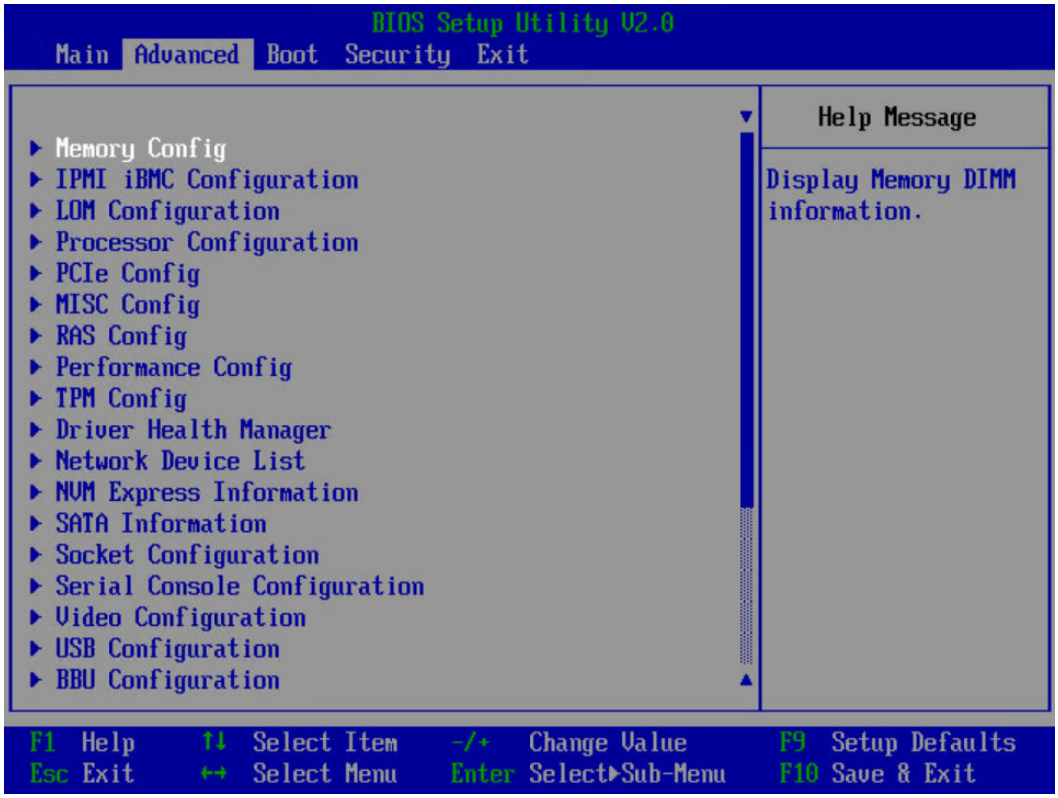
5.12.8.3 Configuring the PXE Function of an NIC

Configuring the LOM PXE

Step 1 Access the BIOS. For details, see **5.12.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Advanced** screen, as shown in **Figure 5-75**.

Figure 5-73 Advanced screen



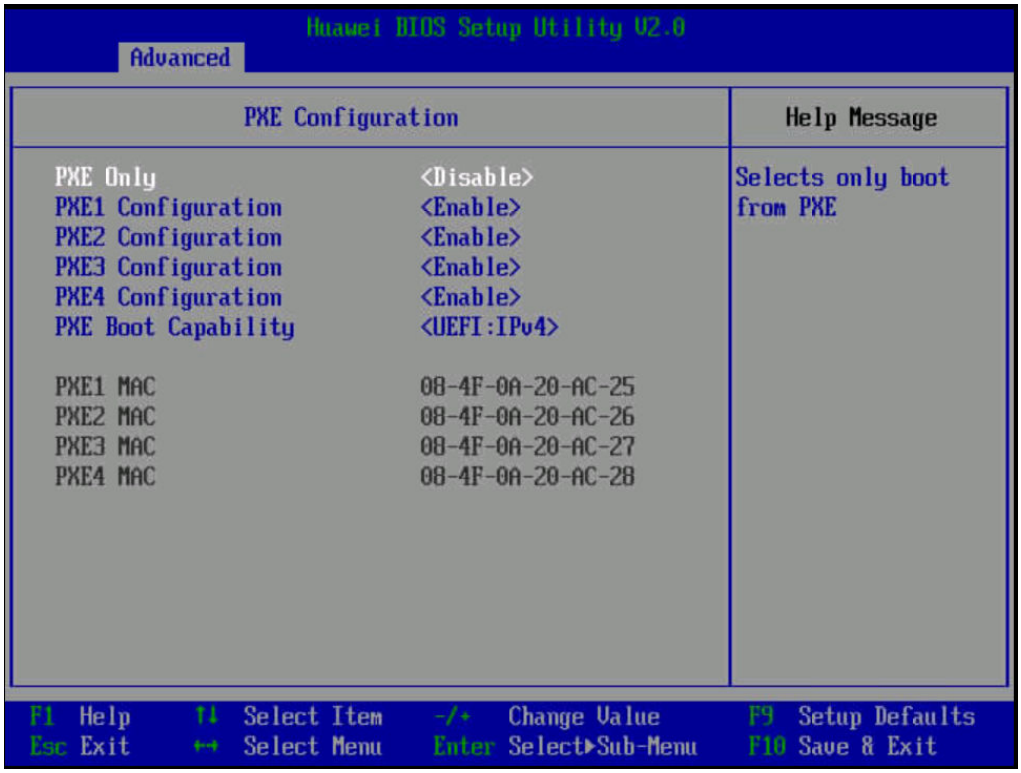
Step 3 Choose **LOM Configuration** > **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed, as shown in **Figure 5-74**.

NOTE

The **PXE Configuration** screen may vary according to the server.

Figure 5-74 PXE Configuration screen



Step 4 Configure the PXE function.

1. Select the network port such as **PXE1 Configuration**, and press **Enter**.
2. In the dialog box that is displayed, select **Enable** and press **Enter**.

Step 5 Select a network protocol for PXE boot.

1. Select **PXE Boot Capability** and press **Enter**.
2. In the dialog box that is displayed, select a network protocol that needs to be supported.
   - UEFI: IPv4
   - UEFI: IPv6
   - UEFI: IPv4/IPv6

Step 6 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 7 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

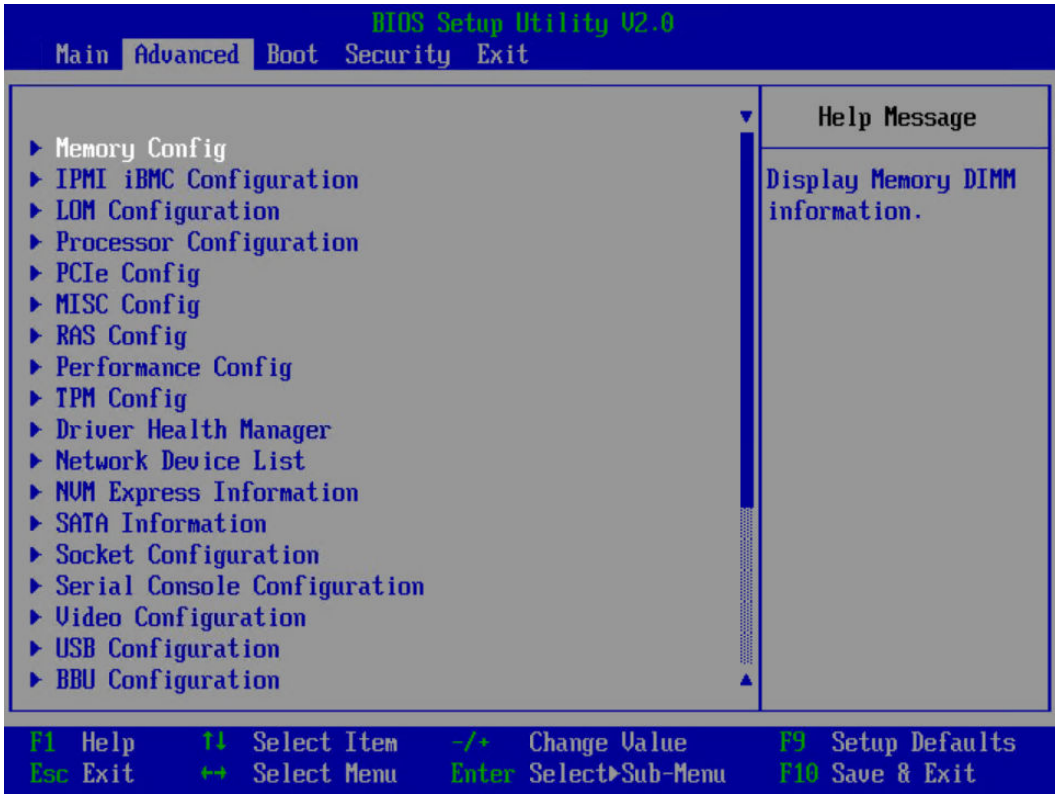
----End

Configuring the PXE Function of a PCIe NIC

Step 1 Access the BIOS. For details, see **5.12.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Advanced** screen, as shown in **Figure 5-75**.

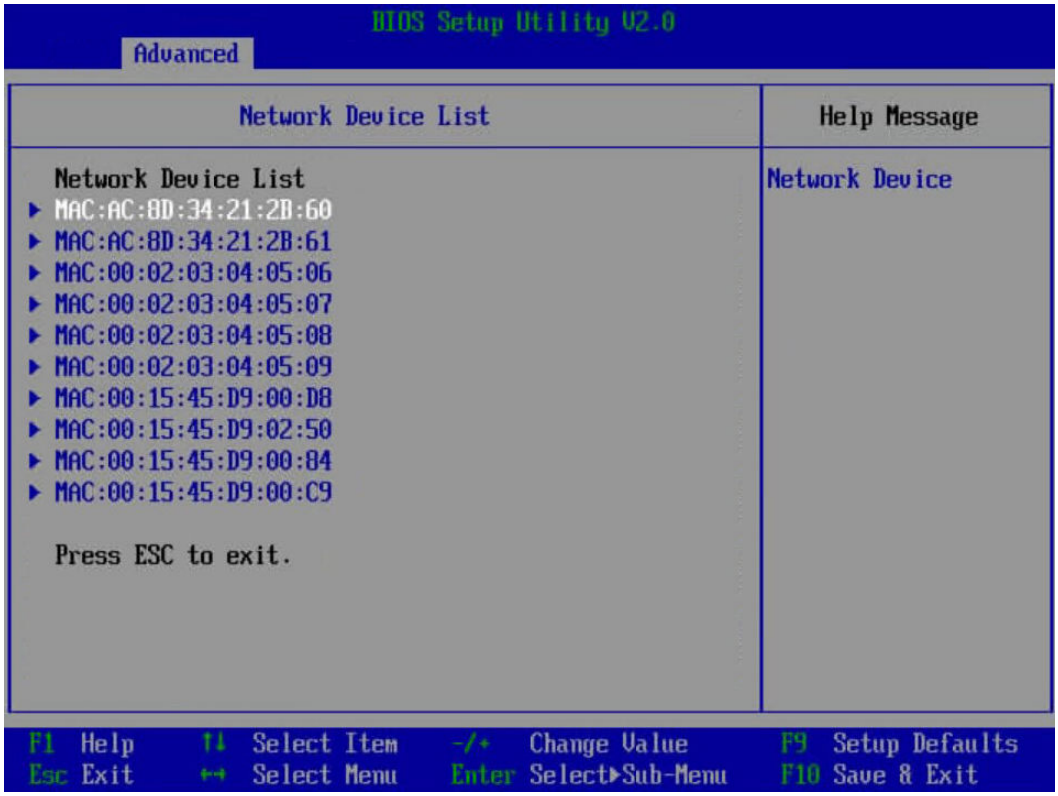
Figure 5-75 Advanced screen



Step 3 Select **Network Device List** and press **Enter**.

The **Network Device List** screen is displayed, as shown in **Figure 5-76**.

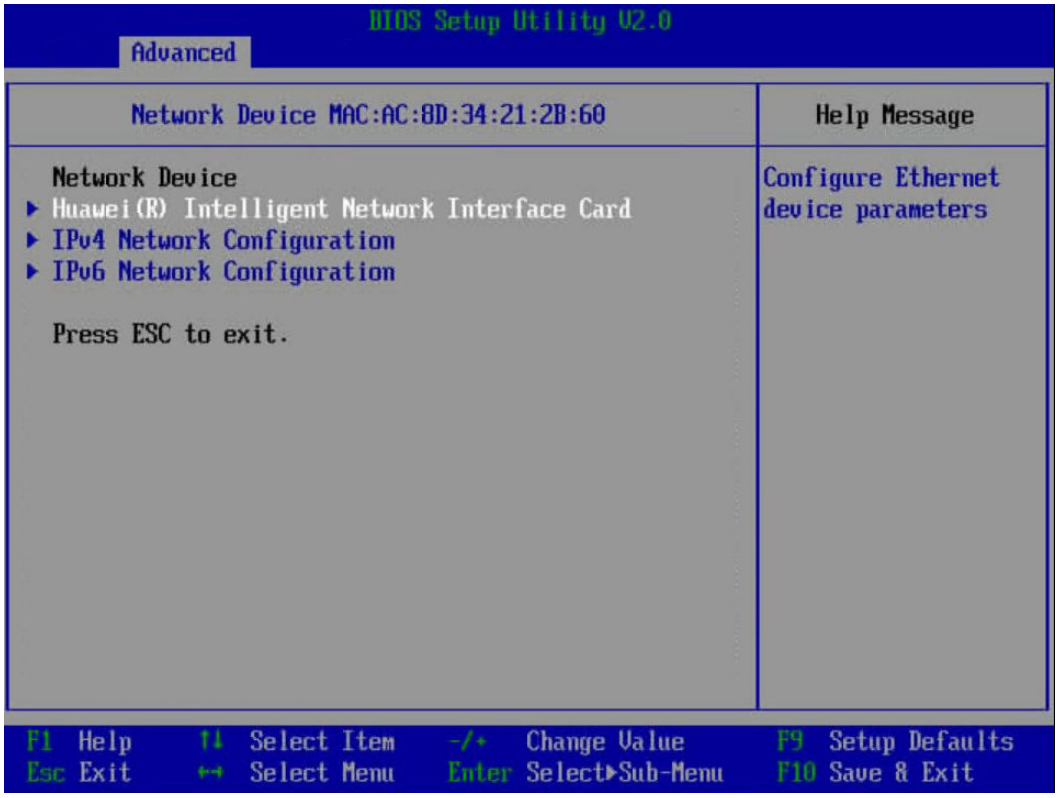
Figure 5-76 Network Device List screen



Step 4 Select the network port (such as **MAC:AC:8D:34:21:2B:60**) of the external NIC, and press **Enter**.

The **Network Device MAC:AC:8D:34:21:2B:60** screen is displayed, as shown in **Figure 5-77**.

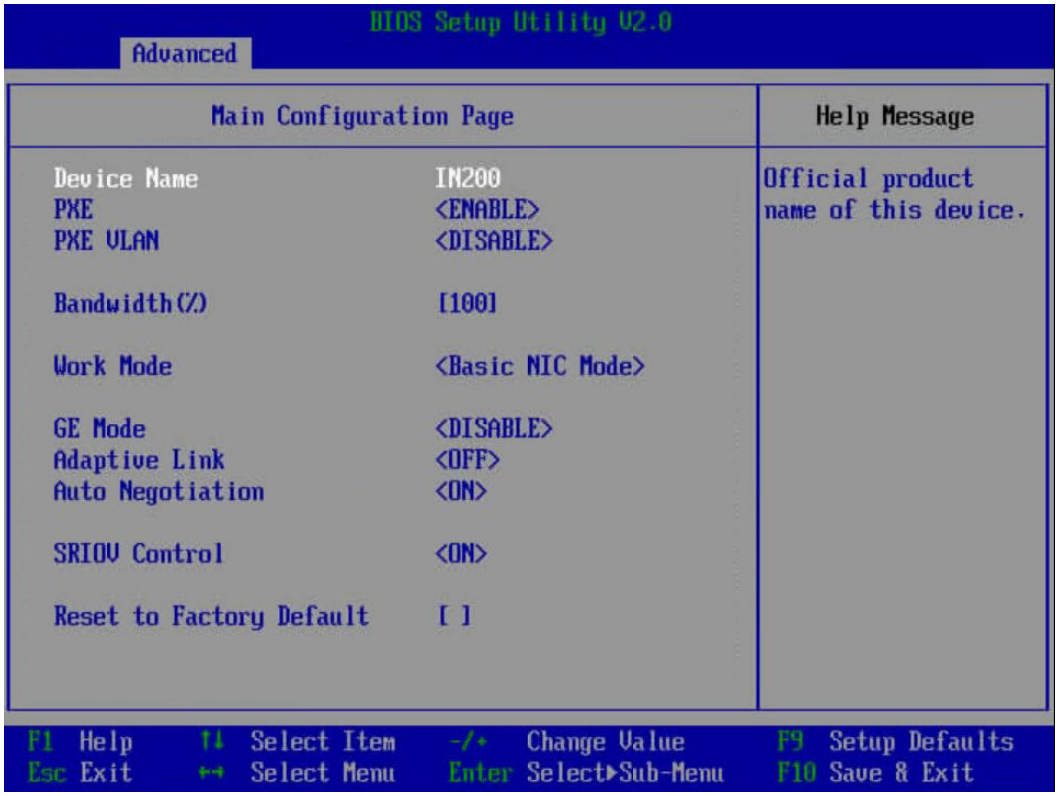
Figure 5-77 Network Device MAC:AC:8D:34:21:2B:60 screen



Step 5 Select **Huawei (R) Intelligent Network Interface Card** and press **Enter**.

The **Main Configuration Page** screen is displayed, as shown in **Figure 5-78**.

Figure 5-78 Main Configuration Page screen



Step 6 Set **PXE** to **ENABLE**.

NOTE

Set other parameters in **Figure 5-78**.

Step 7 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 8 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

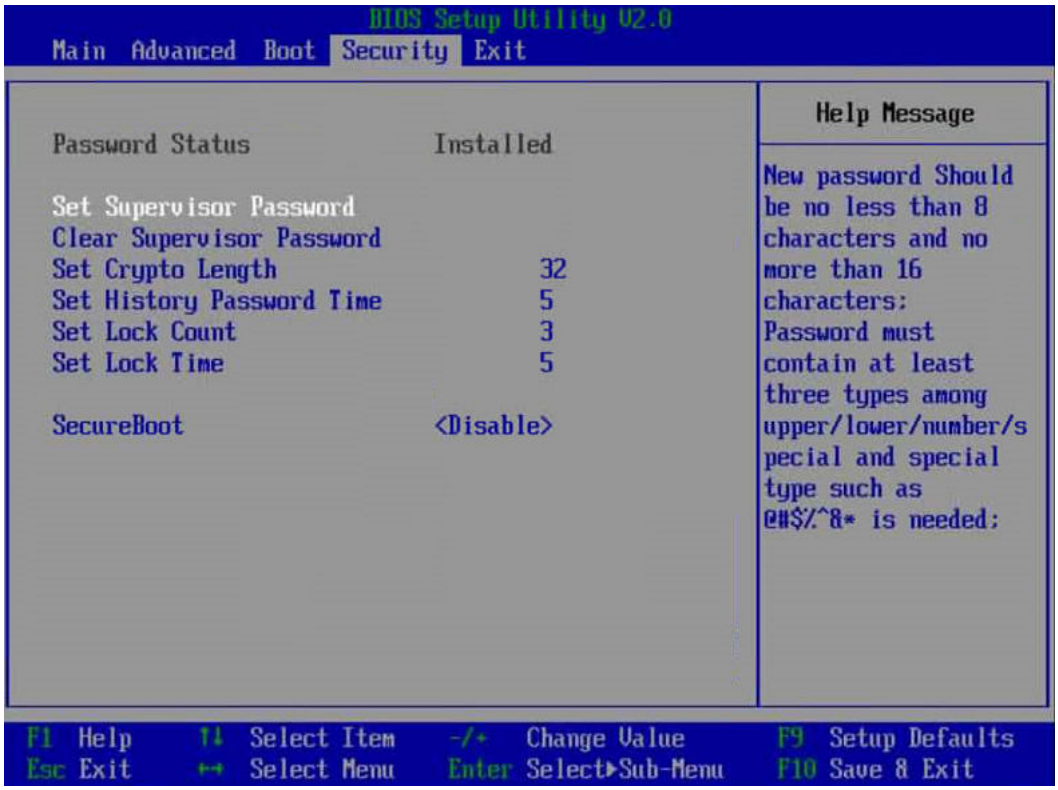
----End

5.12.8.4 Setting the BIOS Password

Step 1 Access the BIOS. For details, see **5.12.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Security** screen, as shown in **Figure 5-79**.

Figure 5-79 Security screen



Step 3 Select **Set Supervisor Password**, press **Enter**, input the original password, and set the administrator password.

NOTE

- The administrator password must be a string of 8 to 16 characters, and contain at least three types of the following characters: special characters including spaces (mandatory), uppercase letters, lowercase letters, and digits.
- The new password cannot be the same as any of the 3 to 6 previously used passwords.
- For details about the default BIOS password, see **TaiShan Server Account List**.

Step 4 (Optional) After the setting is successful, click **Clear Supervisor Password**. Before clearing the password, enter the current password.

Step 5 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 6 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

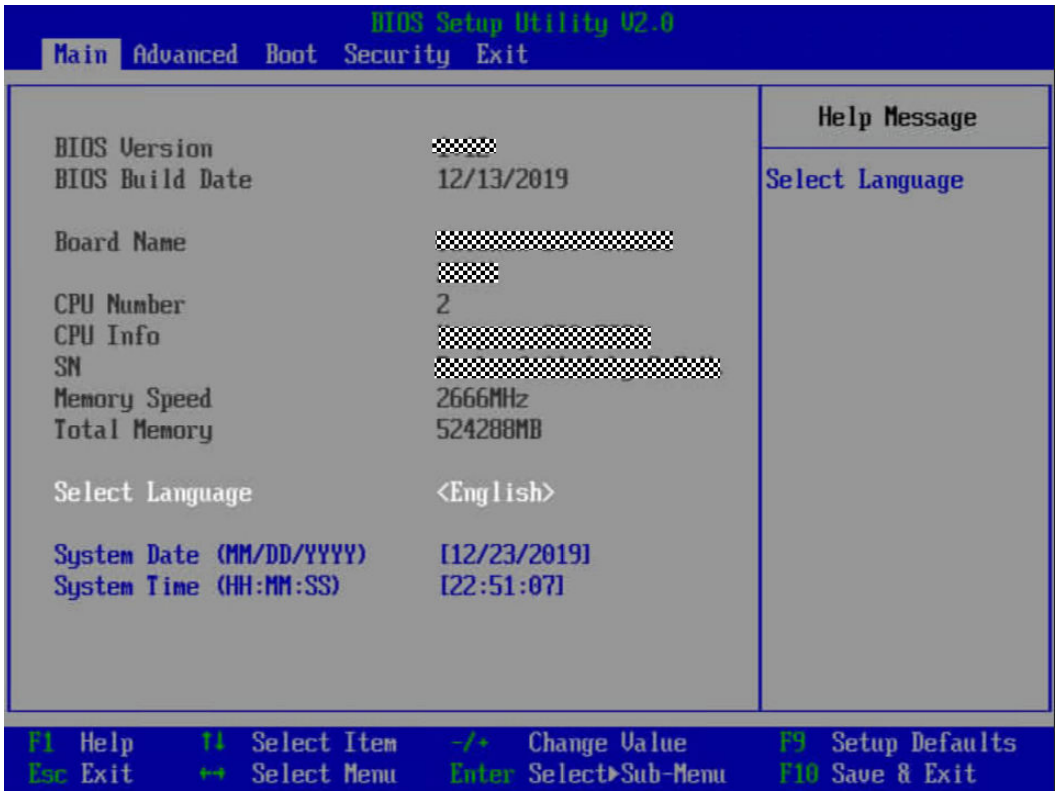
----End

5.12.8.5 Setting the BIOS Language

Step 1 Access the BIOS. For details, see **5.12.8.1 Accessing the BIOS**.

Step 2 Press ← or → to switch to the **Main** screen, as shown in **Figure 5-80**.

Figure 5-80 Main screen



Step 3 Choose **Select Language**.

Step 4 Press **Enter**.

The **Language** screen is displayed.

Step 5 Select the language to be used and press **Enter**.

Step 6 Press **F10**.

The "Save configuration changes and exit?" dialog box is displayed.

Step 7 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

5.12.9 Installing an OS

The server supports multiple types of OSs. For details, see **Computing Product Compatibility Checker**.

The installation method varies according to the OS type. For details, see the installation guide of the OS you use.

NOTE

Log in to **Kunpeng Computing** and click the product model. On the product documentation page that is displayed, search for, browse, and download the OS installation guide.

5.12.10 Upgrading the System

Upgrade the server software and firmware when needed.

- Enterprise customers: Refer to the upgrade guide of the server you use.
- Telecom carriers: Contact the technical support of your local Huawei office.

Upgrading Firmware or Management Software

Use the iBMC WebUI to upgrade the drive backplane, LCD firmware, mainboard CPLD, and drive backplane CPLD. For details, see **TaiShan Rack Server Upgrade Guide**.

Updating Drivers

If the existing driver versions on a server are inconsistent with those in the driver version mapping, install the drivers of required versions. Otherwise, the server may operate improperly. For details, see the installation guide for each OS, ***Computing Component iDriver*** *Release Notes (ARM)*, and ***Computing Component iDriver*** *Driver Version Mapping (ARM)*.

6 Troubleshooting

For details about troubleshooting, see **TaiShan Server Troubleshooting**, which covers:

- Troubleshooting process

  Troubleshooting is a process of using appropriate methods to find the cause of a fault and rectify the fault. The troubleshooting process is to narrow down the scope of possible causes for a fault to reduce troubleshooting complexity, identify the root cause, and rectify the fault.
- Fault information collection

  Collect logs for fault diagnosis when a fault occurs on a server.
- Fault diagnosis

  Fault diagnosis rules and tools help technical support engineers and maintenance engineers to analyze and rectify faults based on alarms and hardware fault symptoms.
- Software and firmware upgrade

  Obtain and install the software and firmware upgrade packages based on the server model.
- Preventive maintenance

  Preventive maintenance helps you detect, diagnose, and rectify server faults in time.

7 Warranty and Safety

7.1 Maintenance and Warranty

For details about maintenance, see **Customer Support Service** and **Maintenance Status**.

For details about warranty, see **Warranty Service**.

7.2 Safety

For details, see **Huawei Server Safety Information**.

8 Common Operations (iBMC V250 or Later)

If the server uses a Hi1710 management chip, the iBMC version is in *X.XX* format, which is also referred to as *VXXX*. For example, 2.50, which is also referred to as V250.

8.1 Login Precautions

The clients used for logging in to the iBMC WebUI must meet certain requirements. For details, see section "Before You Start" in **TaiShan Rack Server iBMC User Guide**.

8.2 Logging In to the Remote Virtual Console

8.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI

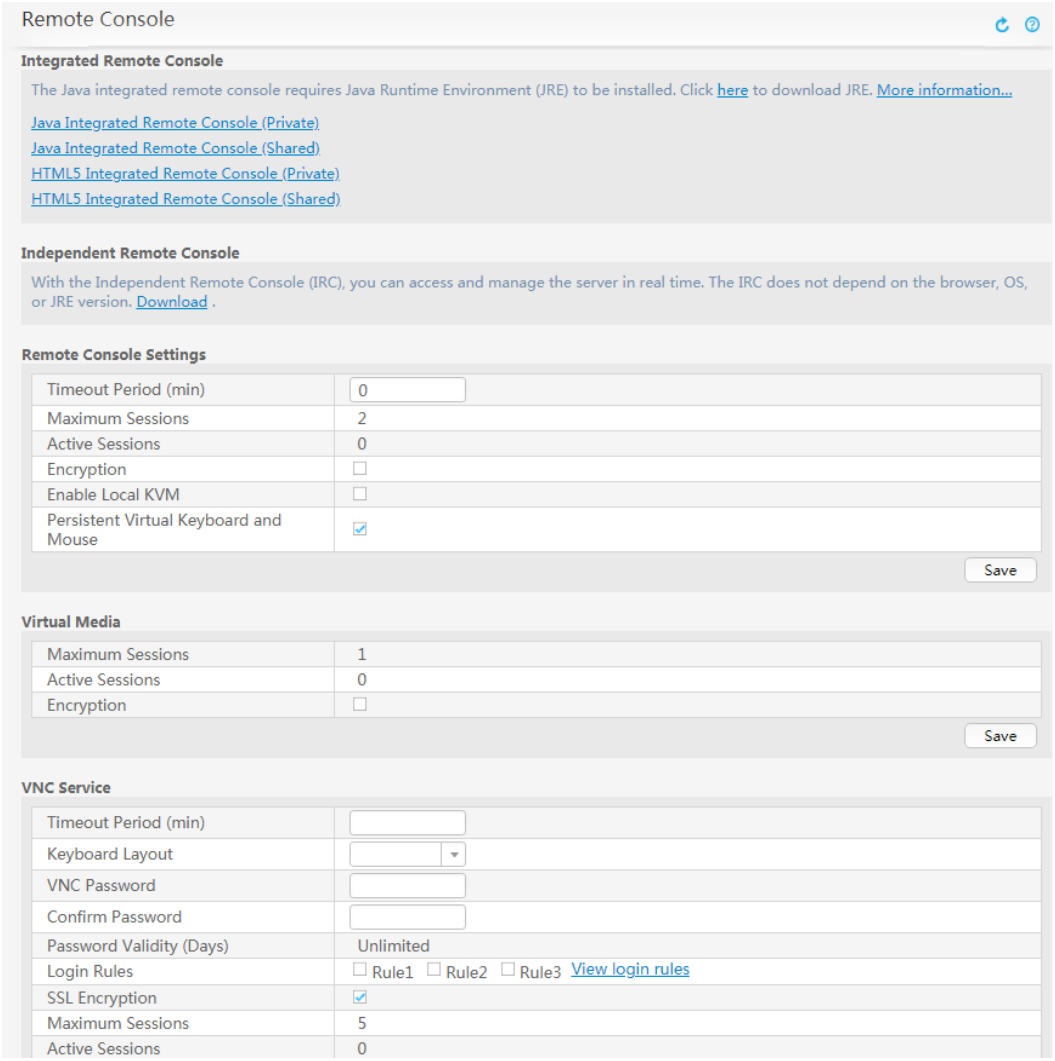
Procedure (iBMC V549 or Earlier)

Step 1 Log in to the iBMC WebUI.

For details, see **5.11.4 Logging In to the iBMC WebUI**.

Step 2 On the menu bar, click **Remote Console**. The **Remote Console** page is displayed, as shown in **Figure 8-1**.

Figure 8-1 Remote Console



Step 3 Click **Java Integrated Remote Console (Private)**, **Java Integrated Remote Console (Shared)**, **HTML5 Integrated Remote Console (Private)**, or **HTML5 Integrated Remote Console (Shared)** to access the real-time operation console of the server, as shown in **Figure 8-2** or **Figure 8-3**.

NOTE

- **Java Integrated Remote Console (Private)**: allows only one local user or VNC user to access and manage the server at a time.
- **Java Integrated Remote Console (Shared)**: allows two local users or five VNC users to access and manage the server at a time. The users can see each other's operations.
- **HTML5 Integrated Remote Console (Private)**: allows only one local user or VNC user to access and manage the server at a time.
- **HTML5 Integrated Remote Console (Shared)**: allows two local users or five VNC users to access and manage the server at a time. The users can see each other's operations.

Figure 8-2 Real-time operation console (Java)

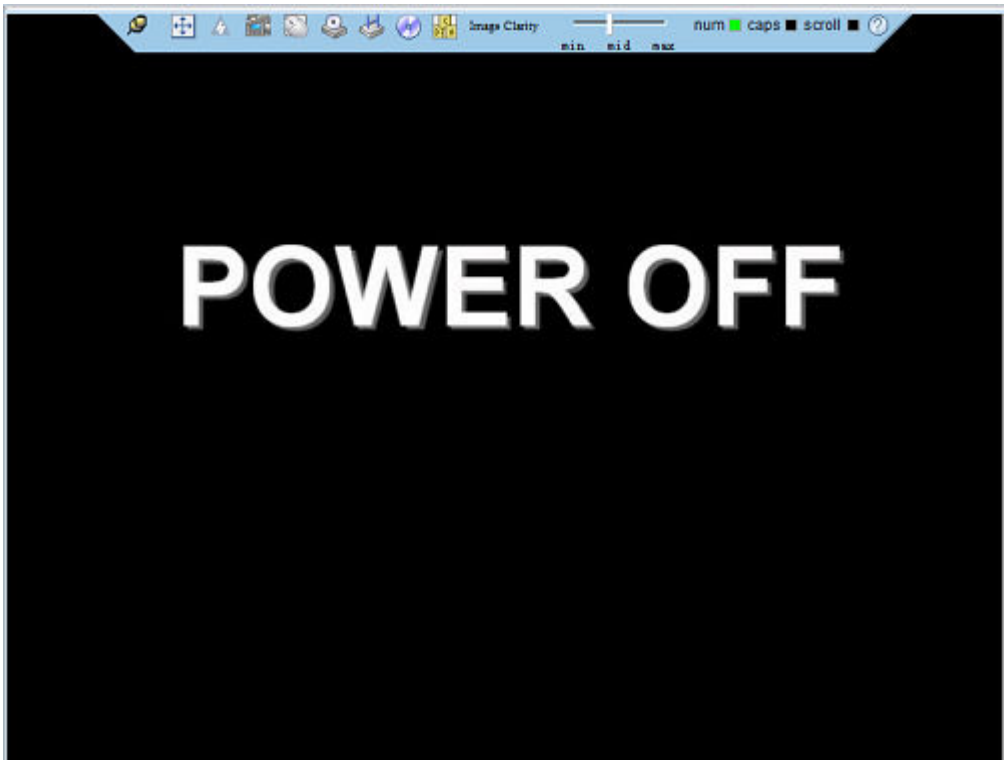
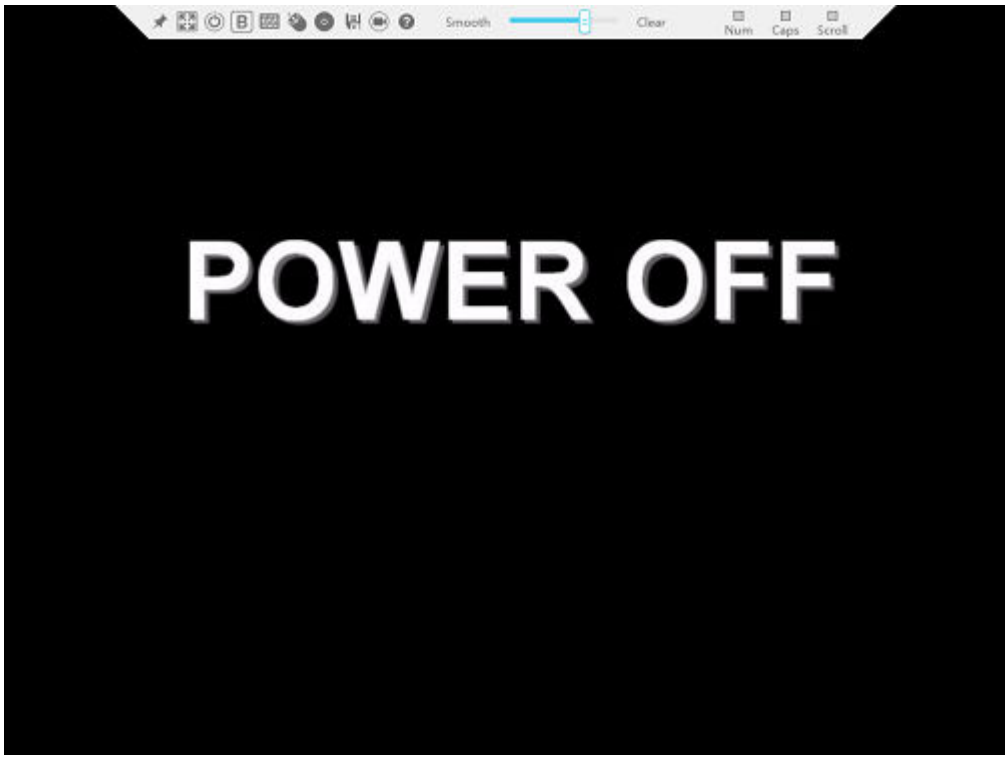


Figure 8-3 Real-time operation console (HTML5)



----End

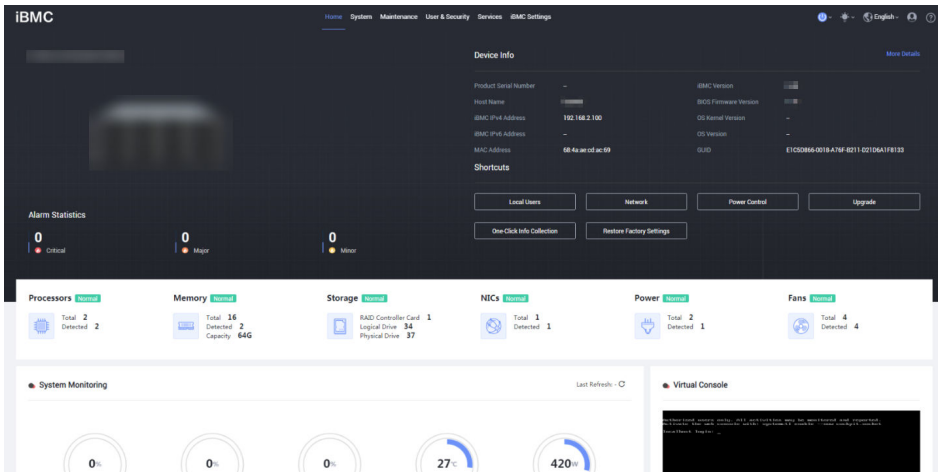
Procedure (iBMC V561 and Later)

Step 1 Log in to the iBMC WebUI.

For details, see **5.11.4 Logging In to the iBMC WebUI**.

Step 2 In the lower right corner of the home page, click **Virtual Console**, as shown in **Figure 8-4**.

Figure 8-4 Virtual console



Step 3 Click  next to **Start** and select **Java Integrated Remote Console (Private)**, **Java Integrated Remote Console (Shared)**, **HTML5 Integrated Remote Console (Private)**, or **HTML5 Integrated Remote Console (Shared)** to log in to the remote virtual console. See **Figure 8-5** or **Figure 8-6**.

NOTE

- **Java Integrated Remote Console (Private)**: allows only one local user or VNC user to access and manage the server at a time.
- **Java Integrated Remote Console (Shared)**: allows two local users or five VNC users to access and manage the server at a time. The users can see each other's operations.
- **HTML5 Integrated Remote Console (Private)**: allows only one local user or VNC user to access and manage the server at a time.
- **HTML5 Integrated Remote Console (Shared)**: allows two local users or five VNC users to access and manage the server at a time. The users can see each other's operations.

Figure 8-5 Real-time operation console (Java)

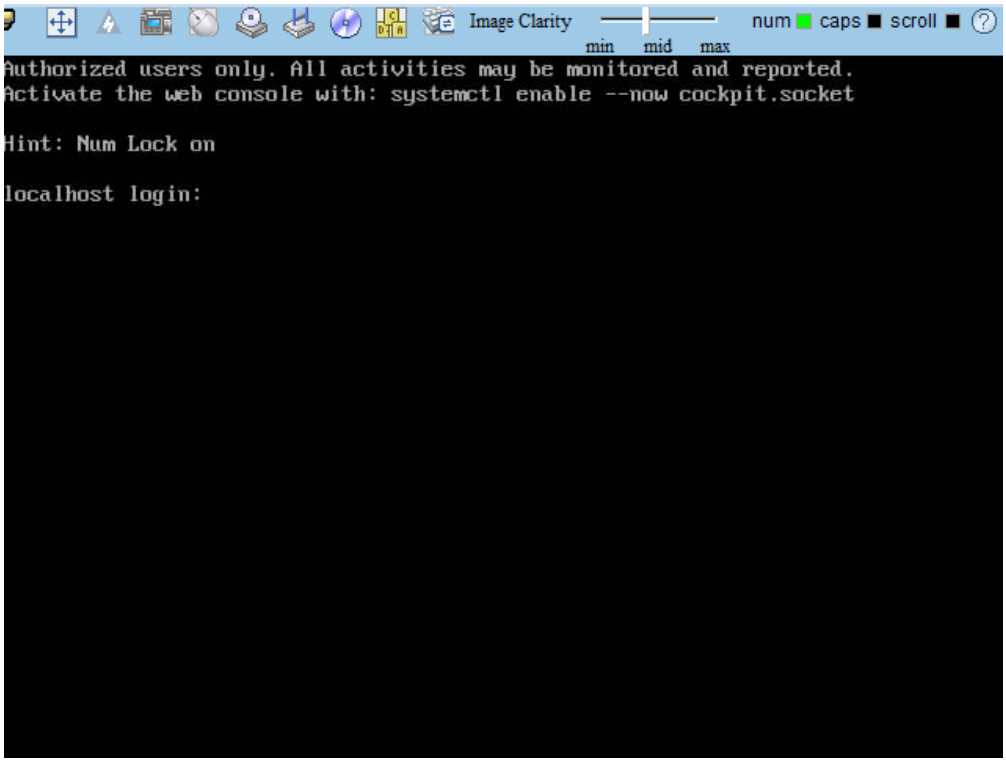
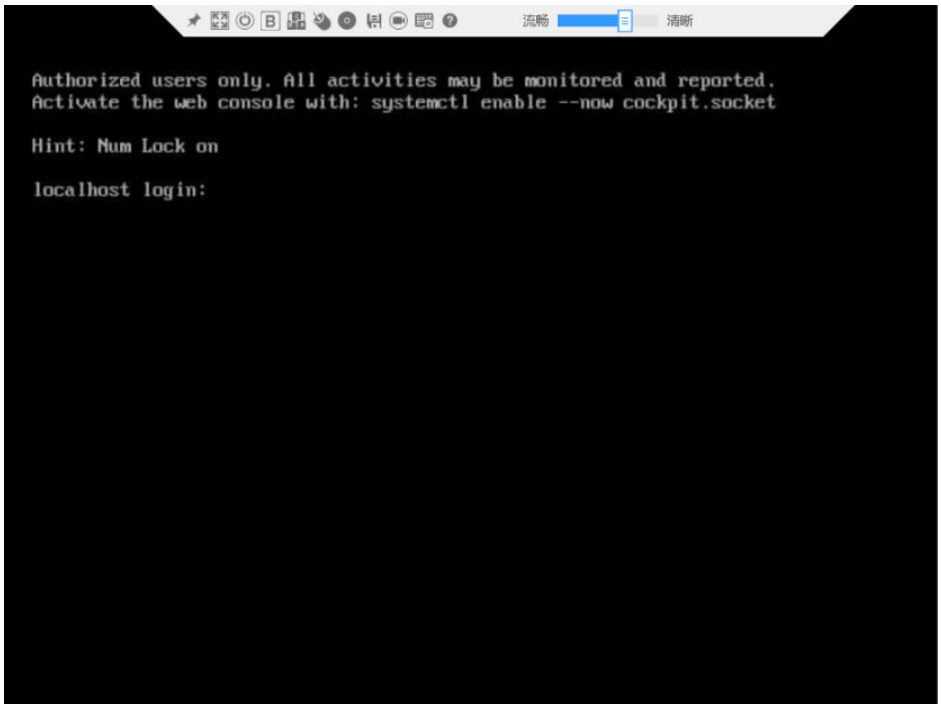


Figure 8-6 Real-time operation console (HTML5)



----End

8.2.2 Logging In to the Server Using the IRC

The Independent Remote Console (IRC) is a remote management tool developed by Huawei based on the server management software iBMC and iMana 200. It offers the same functions as the Remote Virtual Console of the iBMC WebUI and iMana 200 WebUI. This tool allows you to remotely access and manage a server, without worrying about the compatibility between the client's browser and the JRE.

Table 8-1 Instructions for using the IRC

Software Package	How to Obtain	OS Type	Version	Procedure
kvm_client_windows.zip	**SmartKit Computing 23.1.0** **NOTE** Downloading the software indicates your acknowledgement and agreement to the terms and conditions of **Huawei Enterprise Software User License Agreement**.	Windows	Windows 7 (32-bit/64-bit)	For details about how to log in to the server using the IRC, see **SmartKit Computing V2R2 Independent Remote Console User Guide**.
			Windows 8 (32-bit/64-bit)	
			Windows 10 (32-bit/64-bit)	
			Windows Server 2008 R2 (32-bit/64-bit)	
			Windows Server 2012 64-bit	
kvm_client_ubuntu.zip		Ubuntu	Ubuntu 14.04 LTS	
			Ubuntu 16.04 LTS	
kvm_client_mac.zip		macOS	macOS X El Capitan	
kvm_client_linux.zip		Red Hat	Red Hat 6.9	
			Red Hat 7.3	

8.3 Logging In to the iBMC CLI

NOTE

- The system locks a user account if the user enters incorrect passwords for consecutive five times. The user is automatically unlocked 5 minutes later, or an administrator can unlock the user on the CLI.
- For security purposes, change your initial password at your first login and change the password periodically.
- By default, the CLI timeout interval is 15 minutes.

Logging In over SSH

Secure Shell (SSH) provides secure remote login and other network services on a non-secure network. A maximum of five users can log in over SSH at the same time.

NOTE

SSH supports the **AES128-CTR**, **AES192-CTR**, and **AES256-CTR** encryption algorithms. When you log in to the iBMC over SSH, select a proper encryption algorithm.

Step 1 Download an SSH communication tool to a local client.

Step 2 Connect the client to the server management network port directly or through a network.

Step 3 Set the client IP address so that the client can communicate with the iBMC management network port of the server.

Step 4 On the client, start the SSH communication tool and set required parameters, such as the IP address.

Step 5 Connect to the iBMC and enter your user name and password.

NOTE

- Local and LDAP users can both log in to the iBMC CLI over SSH.
- LDAP users do not need to enter the domain server information, which is automatically matched by the system.

----End

Logging In over the Serial Port

Step 1 Set the serial port connection direction to the iBMC serial port.

1. Log in to the iBMC CLI over SSH.
2. Run the following command to change the serial port direction:

   ipmcset -d serialdir -v *<option>*

Parameter	Description	Value
<option>	Serial port direction	The value options of this parameter and the value meanings vary according to the server model. You are advised to run the **ipmcget -d serialdir** command to view the value options. For the server, the options are as follows: – **0**: sets the serial port on the server panel as the system serial port. – **1**: sets the serial port on the server panel as the iBMC serial port. – **2**: sets the SOL port as the system serial port. – **3**: sets the SOL port as the iBMC serial port. – **4**: sets the serial port on the SDI V3 card panel as an SCCL port. – **5**: sets the serial port on the SDI V3 card panel as an IMU port. – **6**: sets the serial port on the SDI V3 card panel as an SCCL port. – **7**: sets the serial port on the SDI V3 card panel as an IMU port. To set the panel serial port as the iBMC serial port, run the **ipmcset -d serialdir -v 1** command. **NOTE** – If no SDI V3 is installed in a server, <option> can be 0 to 3 only. – If one SDI V3 card is installed, the values 4 and 5 are available for setting the ports on the SDI V3 in I/O module 1 or 2. – If two SDI V3 cards are installed, the values 4 to 7 are available. The values 4 and 5 are used for setting the ports on the SDI V3 in I/O module 1, while the values 6 and 7 are for the ports on the SDI V3 in I/O module 2.

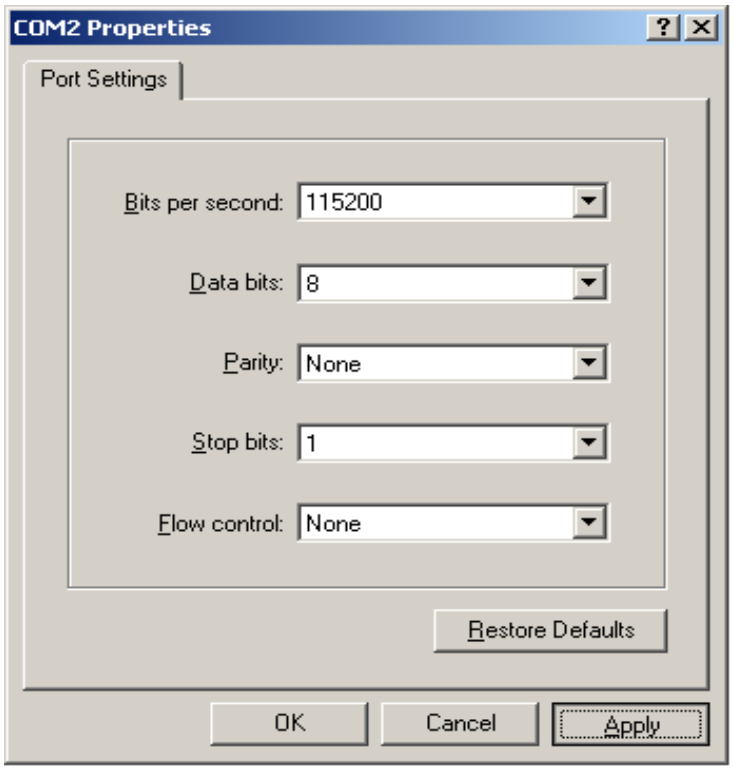
Step 2 Use a serial cable to connect the terminal serial port and the server serial port.

Step 3 Open the HyperTerminal and set the following parameters:

- **Bits per second**: 115200
- **Data bits**: 8
- **Parity**: None
- **Stop bits**: 1
- **Flow control**: None

Figure 8-7 shows the parameter settings.

Figure 8-7 HyperTerminal Properties



Step 4 Enter your user name and password to access the CLI.

----End

8.4 Logging In to the Server over a Serial Port Using PuTTY

Use PuTTY to log in to the server over a serial port in either of the following scenarios:

- The server is configured for the first time at a site.
- A remote connection to the server cannot be established.

NOTE

- Visit the chiark website and download the PuTTY software from the homepage.
- PuTTY of an earlier version may cause server login failures. You are advised to use PuTTY of the latest version.

Procedure

Step 1 Double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed.

Step 2 In the navigation tree, choose **Connection** > **Serial**.

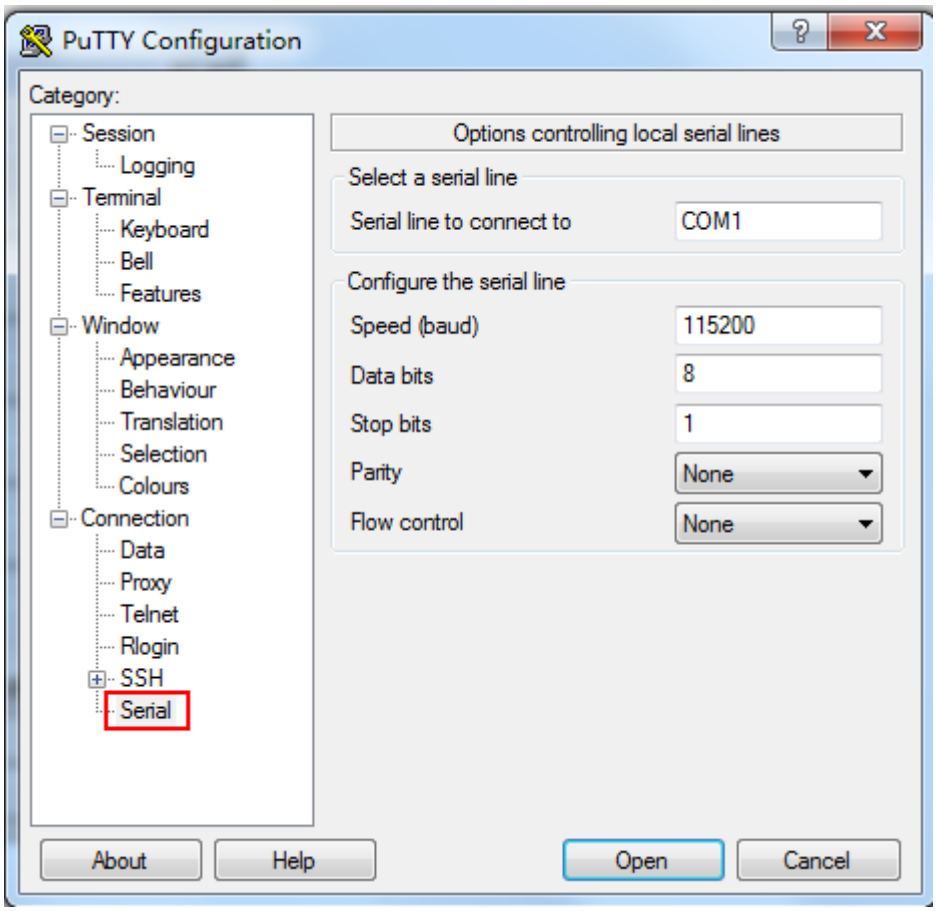
Step 3 Set the login parameters.

Example:

- **Serial Line to connect to**: COM*n*
- **Speed (baud)**: 115200
- **Data bits**: 8
- **Stop bits**: 1
- **Parity**: None
- **Flow control**: None

  n in COM*n* indicates a serial port number and its value is an integer.

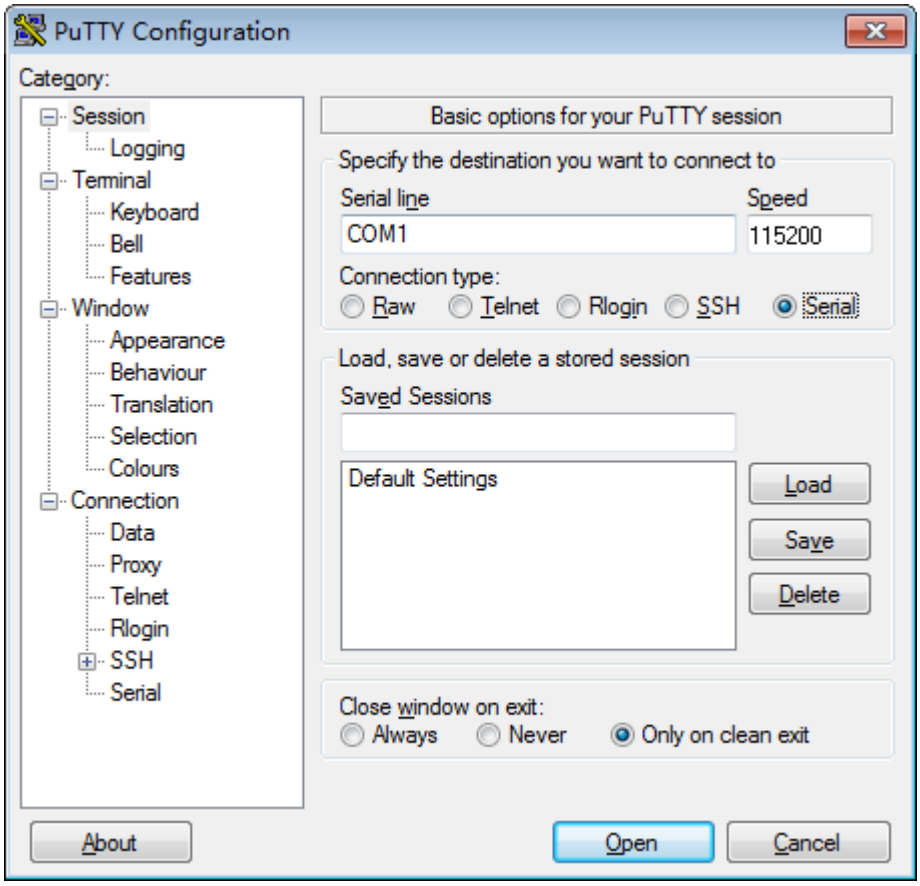
Figure 8-8 PuTTY Configuration - Serial



Step 4 In the navigation tree, click **Session**.

Step 5 Set **Connection type** to **Serial**, as shown in **Figure 8-9**.

Figure 8-9 PuTTY Configuration - Session



Step 6 Set **Close window on exit** to **Only on clean exit**, as shown in **Figure 8-9**.

Set **Saved Sessions** and click **Save**. Next time you can simply double-click the saved settings under **Saved Sessions** to log in to the server.

Step 7 Click **Open**.

The PuTTY window is displayed prompting you to enter your user name next to **login as**.

Step 8 Enter your user name and password.

If the login is successful, the server host name is displayed on the left of the prompt.

----End

8.5 Logging In to the Server over a Network Port Using PuTTY

The login method described in this section applies to components that support SSH access, for example, iBMC and OSs.

Use PuTTY to remotely log in to the server over a local area network (LAN) and configure and maintain the server.

NOTE

- Visit the chiark website and download the PuTTY software from the homepage.
- PuTTY of an earlier version may cause server login failures. You are advised to use PuTTY of the latest version.

Procedure

Step 1 Set an IP address and a subnet mask or add route information for the PC to communicate with the server.

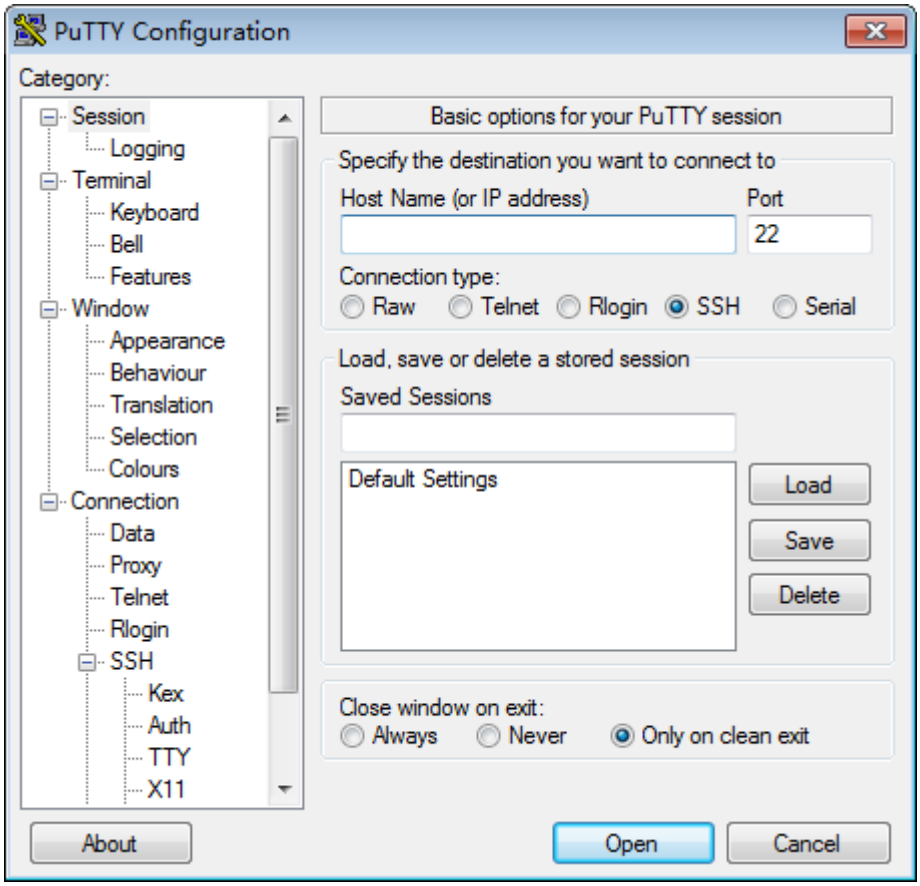
On the PC command-line interface (CLI), run **Ping *Server IP address*** to check whether the IP address is reachable.

- If yes, go to **Step 2**.
- If no, check the network connection, rectify the fault, and go to **Step 1**.

Step 2 Double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed, as shown in **Figure 8-10**.

Figure 8-10 PuTTY Configuration window



Step 3 In the navigation tree, click **Session**.

Step 4 Set the login parameters.

The parameters are described as follows:

- **Host Name (or IP address)**: Enter the IP address of the server to be accessed, for example, **192.168.34.32**.
- **Port**: Retain the default value **22**.
- **Connection type**: Retain the default value **SSH**.
- **Close window on exit**: Retain the default value **Only on clean exit**.

NOTE

Configure **Host Name (or IP address)** and **Saved Sessions**, and click **Save**. You can double-click the saved record under **Saved Sessions** to log in to the server the next time.

Step 5 Click **Open**.

The **PuTTY** window is displayed prompting you to enter your user name next to **login as**.

NOTE

- If this is your first login to the server, the **PuTTY Security Alert** dialog box is displayed. Click **Yes** to proceed.
- If an incorrect user name or password is entered, you must set up a new PuTTY session.

Step 6 Enter the user name and password as prompted.

If the login is successful, the server host name is displayed on the left of the prompt.

----End

9 Common Operations (iBMC V3.01.00.00 or Later)

If the server uses a Hi1711 management chip, the iBMC version is in *X.XX.XX.XX* format, which is also referred to as *VX.XX.XX.XX*. For example, 3.01.00.00, which is also referred to as V3.01.00.00.

9.1 Login Precautions

The clients used for logging in to the iBMC WebUI must meet certain requirements. For details, see section "Before You Start" in **TaiShan Rack Server iBMC User Guide**.

9.2 Logging In to the Remote Virtual Console

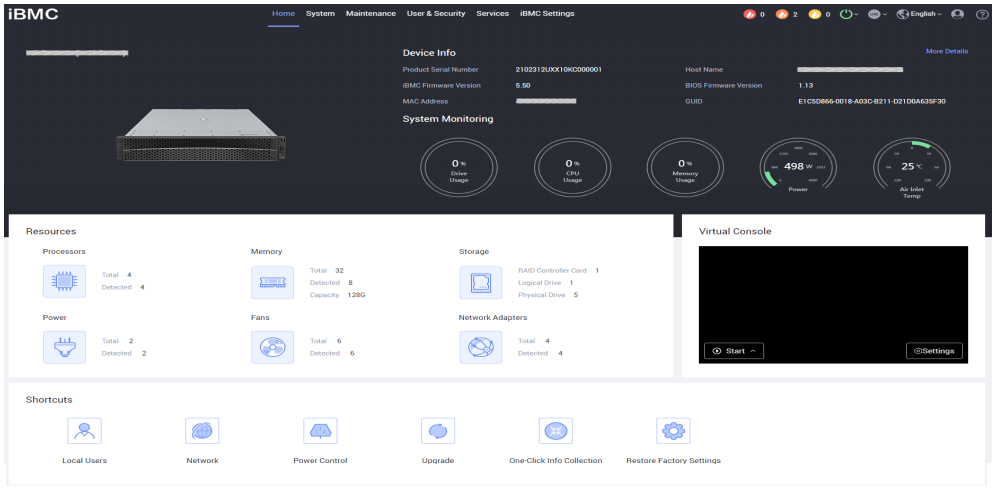
9.2.1 Logging In to the Remote Virtual Console Through the iBMC WebUI

Step 1 Log in to the iBMC WebUI.

For details, see **5.12.4 Logging In to the iBMC WebUI**.

Step 2 In the lower right corner of the home page, click **Virtual Console**, as shown in **Figure 9-1**.

Figure 9-1 Virtual console



Step 3 Click  next to **Start** and select **Java Integrated Remote Console (Private)**, **Java Integrated Remote Console (Shared)**, **HTML5 Integrated Remote Console (Private)**, or **HTML5 Integrated Remote Console (Shared)** to log in to the remote virtual console. See **Figure 9-2** or **Figure 9-3**.

NOTE

- **Java Integrated Remote Console (Private)**: allows only one local user or VNC user to access and manage the server at a time.
- **Java Integrated Remote Console (Shared)**: allows two local users or five VNC users to access and manage the server at a time. The users can see each other's operations.
- **HTML5 Integrated Remote Console (Private)**: allows only one local user or VNC user to access and manage the server at a time.
- **HTML5 Integrated Remote Console (Shared)**: allows two local users or five VNC users to access and manage the server at a time. The users can see each other's operations.

Figure 9-2 Real-time operation console (Java)

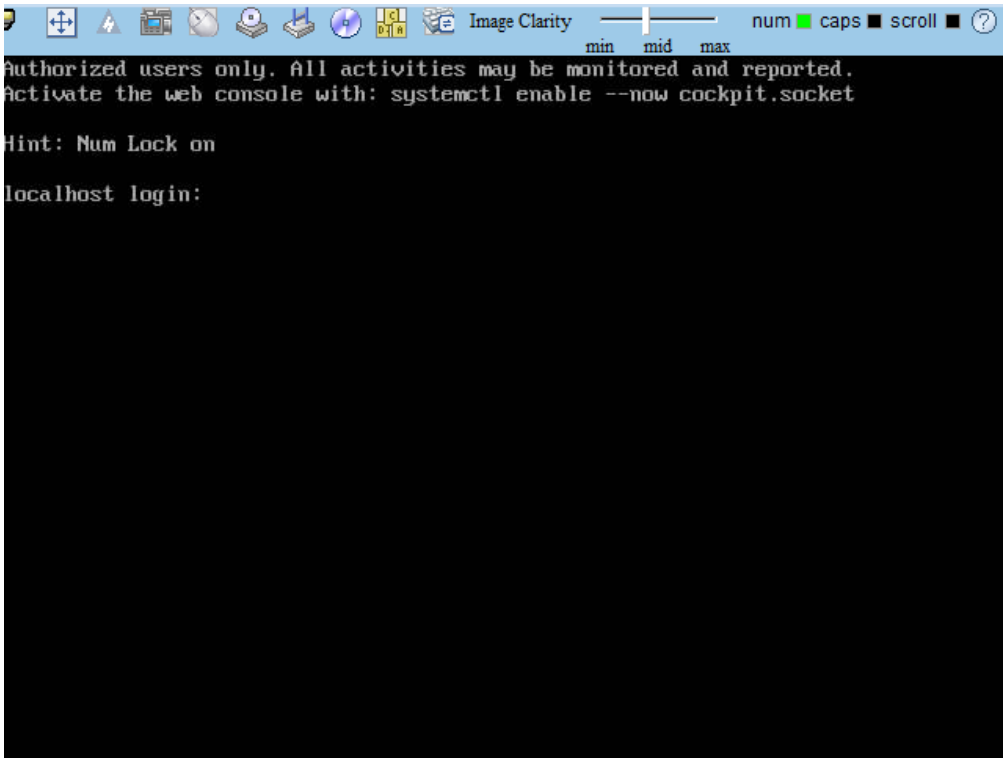
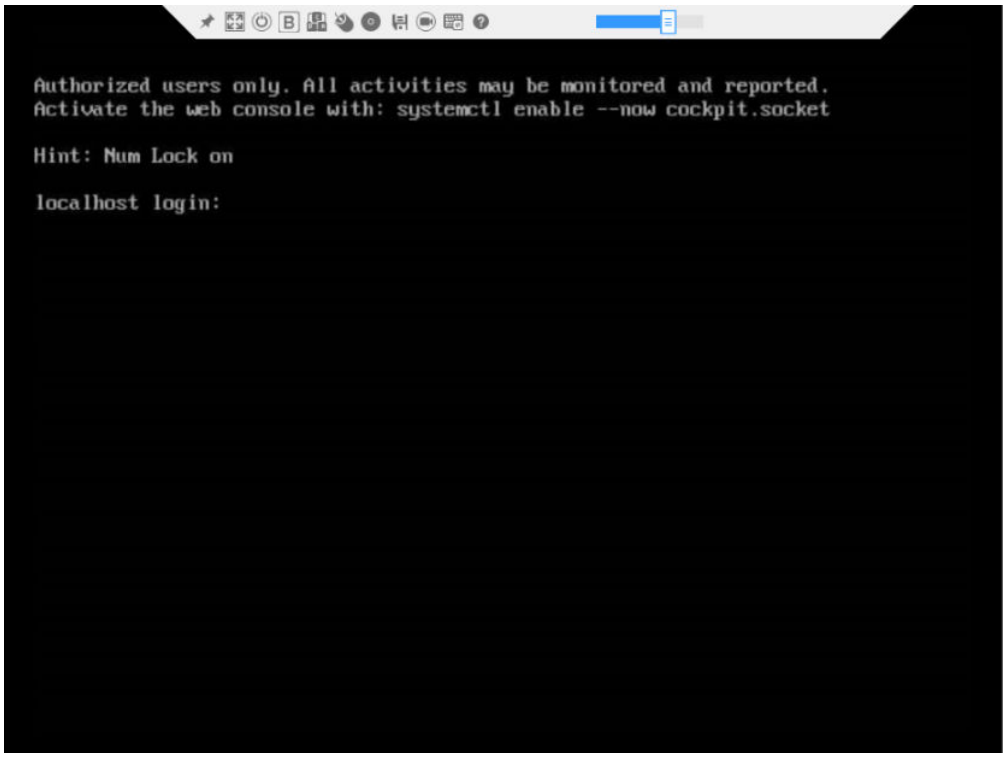


Figure 9-3 Real-time operation console (HTML5)



----End

9.2.2 Logging In to the Server Using the IRC

The Independent Remote Console (IRC) is a remote management tool developed by Huawei based on the server management software iBMC and iMana 200. It offers the same functions as the Remote Virtual Console of the iBMC WebUI and iMana 200 WebUI. This tool allows you to remotely access and manage a server, without worrying about the compatibility between the client's browser and the JRE.

Table 9-1 Instructions for using the IRC

Software Package	How to Obtain	OS Type	Version	Procedure
kvm_client_windows.zip	**SmartKit Computing 23.1.0** **NOTE** Downloading the software indicates your acknowledgement and agreement to the terms and conditions of **Huawei Enterprise Software User License Agreement**.	Windows	Windows 7 (32-bit/64-bit)	For details about how to log in to the server using the IRC, see **SmartKit Computing V2R2 Independent Remote Console User Guide**.
			Windows 8 (32-bit/64-bit)	
			Windows 10 (32-bit/64-bit)	
			Windows Server 2008 R2 (32-bit/64-bit)	
			Windows Server 2012 64-bit	
kvm_client_ubuntu.zip		Ubuntu	Ubuntu 14.04 LTS	
			Ubuntu 16.04 LTS	
kvm_client_mac.zip		macOS	macOS X El Capitan	
kvm_client_linux.zip		Red Hat	Red Hat 6.9	
			Red Hat 7.3	

9.3 Logging In to the iBMC CLI

NOTE

- The system locks a user account if the user enters incorrect passwords for consecutive five times. The user is automatically unlocked 5 minutes later, or an administrator can unlock the user on the CLI.
- For security purposes, change your initial password at your first login and change the password periodically.
- By default, the CLI timeout interval is 15 minutes.

Logging In over SSH

Secure Shell (SSH) provides secure remote login and other network services on a non-secure network. A maximum of five users can log in over SSH at the same time.

NOTE

SSH supports the **AES128-CTR**, **AES192-CTR**, and **AES256-CTR** encryption algorithms. When you log in to the iBMC over SSH, select a proper encryption algorithm.

Step 1 Download an SSH communication tool to a local client.

Step 2 Connect the client to the server management network port directly or through a network.

Step 3 Set the client IP address so that the client can communicate with the server iBMC management network port.

Step 4 On the client, open the SSH tool and set required parameters, such as the IP address.

Step 5 Connect to the iBMC and enter your user name and password.

NOTE

- Local and LDAP users can both log in to the iBMC CLI over SSH.
- To log in to the iBMC, LDAP users do not need to enter information about the domain server, which is automatically assigned by the system.

----End

Logging In over the Serial Port

Step 1 Set the serial port connection direction to the iBMC serial port.

1. Log in to the iBMC CLI over SSH.
2. Run the following command to change the serial port direction:

   ipmcset -d serialdir -v *<option>*

Parameter	Description	Value
<option>	Serial port direction	The value options of this parameter and the value meanings vary according to the server model. You are advised to run the **ipmcget -d serialdir** command to view the value options. For the server, the options are as follows: – **0**: sets the serial port on the server panel as the system serial port. – **1**: sets the serial port on the server panel as the iBMC serial port. – **2**: sets the SOL port as the system serial port. – **3**: sets the SOL port as the iBMC serial port. – **4**: sets the serial port on the SDI V3 card panel as an SCCL port. – **5**: sets the serial port on the SDI V3 card panel as an IMU port. – **6**: sets the serial port on the SDI V3 card panel as an SCCL port. – **7**: sets the serial port on the SDI V3 card panel as an IMU port. To set the panel serial port as the iBMC serial port, run the **ipmcset -d serialdir -v 1** command. **NOTE** – If no SDI V3 is installed in a server, <option> can be 0 to 3 only. – If one SDI V3 card is installed, the values 4 and 5 are available for setting the ports on the SDI V3 in I/O module 1 or 2. – If two SDI V3 cards are installed, the values 4 to 7 are available. The values 4 and 5 are used for setting the ports on the SDI V3 in I/O module 1, while the values 6 and 7 are for the ports on the SDI V3 in I/O module 2.

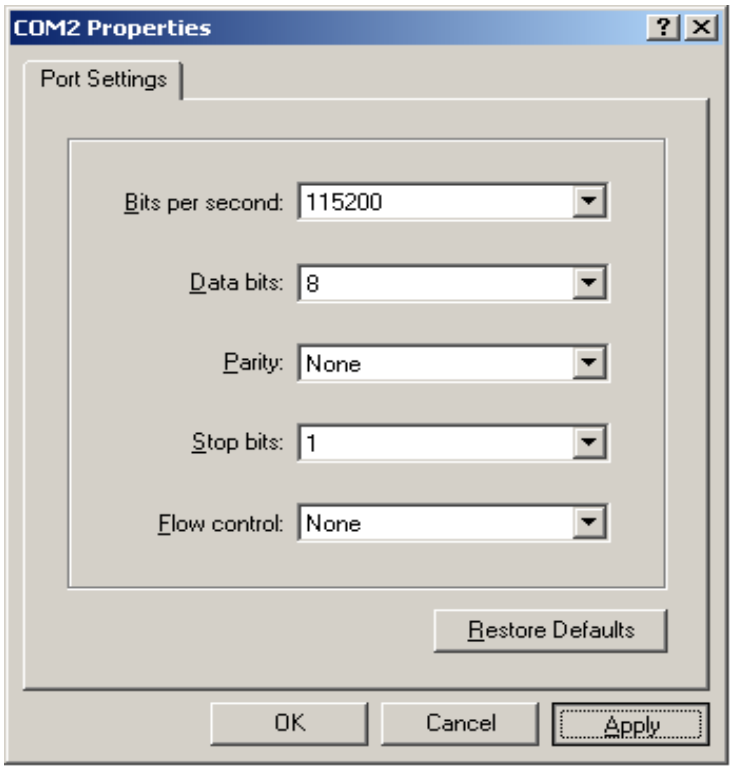
Step 2 Use a serial cable to connect the terminal serial port and the server serial port.

Step 3 Open the HyperTerminal and set the following parameters:

- **Bits per second**: 115200
- **Data bits**: 8
- **Parity**: None
- **Stop bits**: 1
- **Flow control**: None

Figure 9-4 shows the port settings.

Figure 9-4 HyperTerminal Properties



Step 4 Enter your user name and password to access the CLI.

----End

9.4 Logging In to the Server over a Serial Port Using PuTTY

Use PuTTY to log in to the server over a serial port in either of the following scenarios:

- The server is configured for the first time at a site.
- A remote connection to the server cannot be established.

NOTE

- Visit the chiark website and download the PuTTY software from the homepage.
- PuTTY of an earlier version may cause server login failures. You are advised to use PuTTY of the latest version.

Procedure

Step 1 Double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed.

Step 2 In the navigation tree, choose **Connection** > **Serial**.

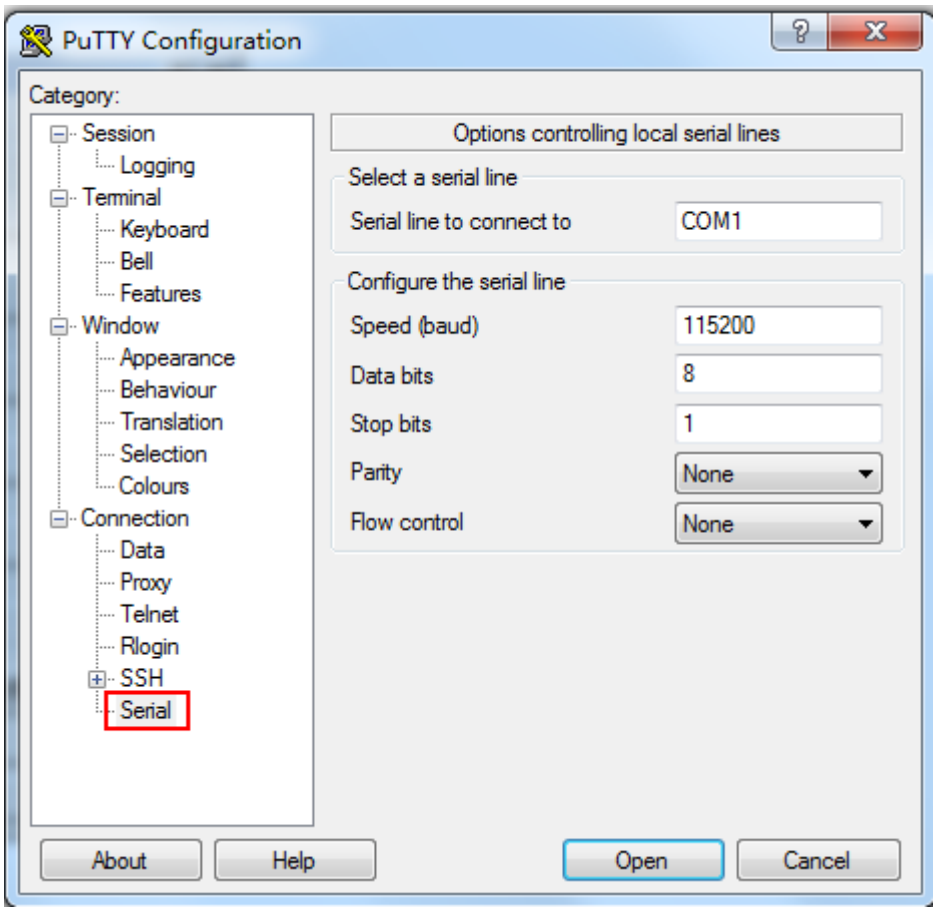
Step 3 Set the login parameters.

Example:

- **Serial Line to connect to**: COM*n*
- **Speed (baud)**: 115200
- **Data bits**: 8
- **Stop bits**: 1
- **Parity**: None
- **Flow control**: None

  n in COM*n* indicates a serial port number and its value is an integer.

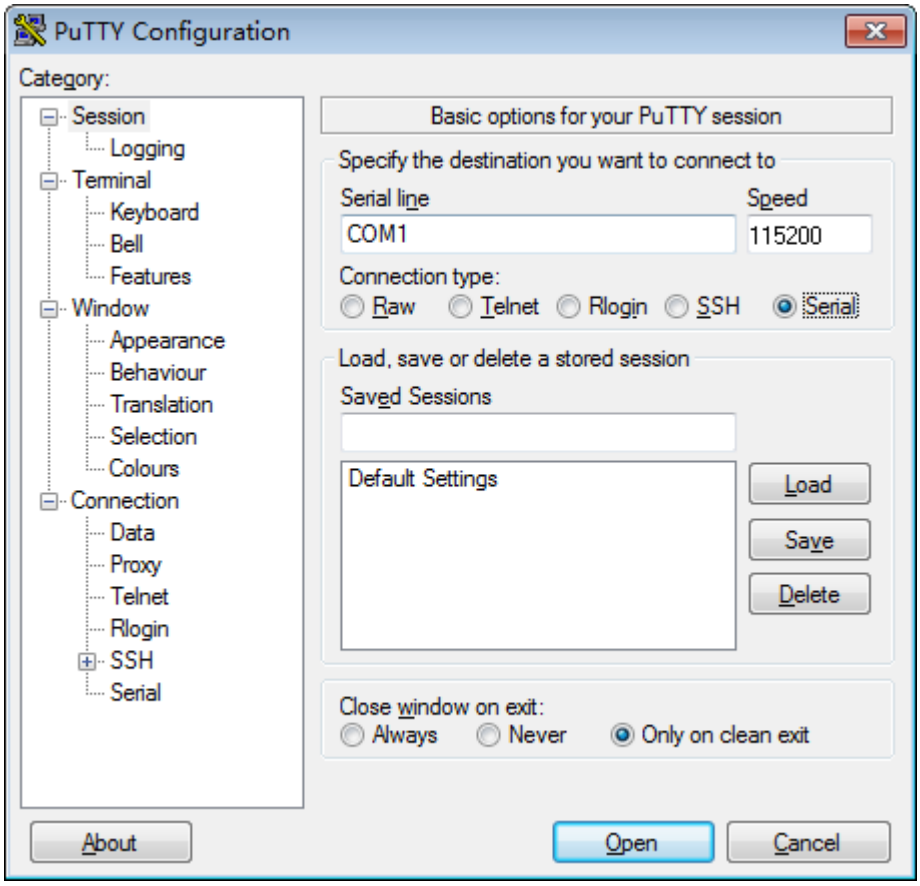
Figure 9-5 PuTTY Configuration - Serial



Step 4 In the navigation tree, click **Session**.

Step 5 Set **Connection type** to **Serial**, as shown in **Figure 9-6**.

Figure 9-6 PuTTY Configuration - Session



Step 6 Set **Close window on exit** to **Only on clean exit**, as shown in **Figure 9-6**.

Set **Saved Sessions** and click **Save**. Next time you can simply double-click the saved settings under **Saved Sessions** to log in to the server.

Step 7 Click **Open**.

The PuTTY window is displayed prompting you to enter your user name next to **login as**.

Step 8 Enter your user name and password.

If the login is successful, the server host name is displayed on the left of the prompt.

----End

9.5 Logging In to the Server over a Network Port Using PuTTY

The login method described in this section applies to components that support SSH access, for example, iBMC and OSs.

Use PuTTY to remotely log in to the server over a local area network (LAN) and configure and maintain the server.

NOTE

- Visit the chiark website and download the PuTTY software from the homepage.
- PuTTY of an earlier version may cause server login failures. You are advised to use PuTTY of the latest version.

Procedure

Step 1 Set an IP address and a subnet mask or add route information for the PC to communicate with the server.

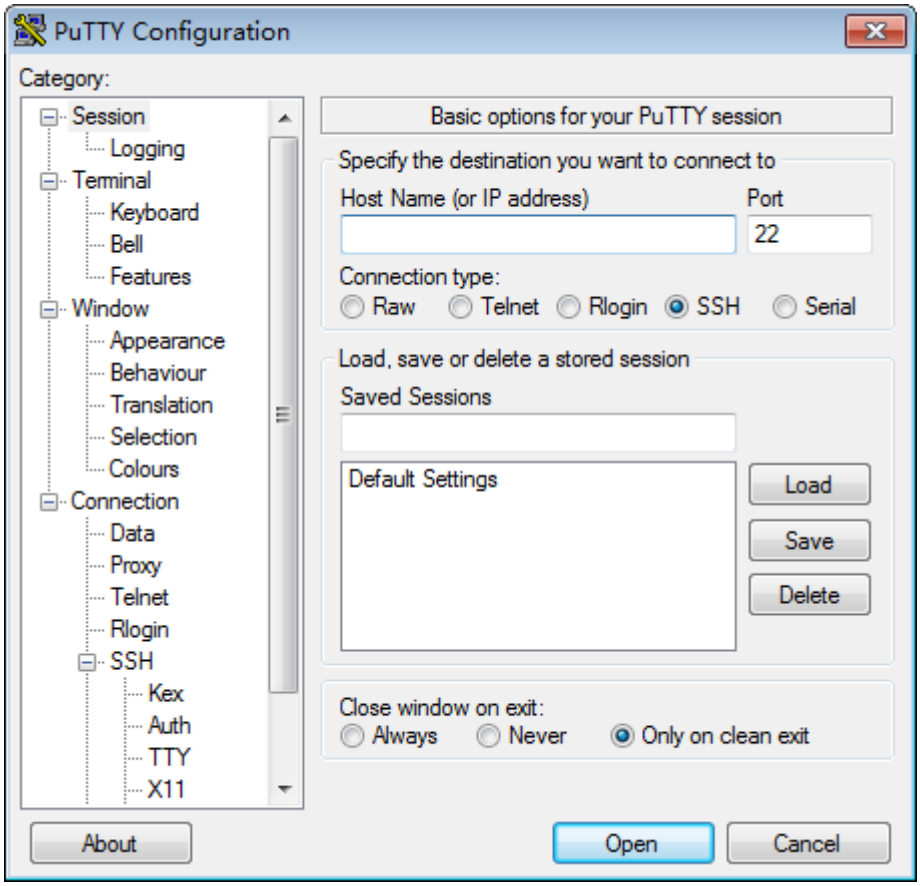
On the PC command-line interface (CLI), run **Ping *Server IP address*** to check whether the IP address is reachable.

- If yes, go to **Step 2**.
- If no, check the network connection, rectify the fault, and go to **Step 1**.

Step 2 Double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed, as shown in **Figure 9-7**.

Figure 9-7 PuTTY Configuration window



Step 3 In the navigation tree, click **Session**.

Step 4 Set the login parameters.

The parameters are described as follows:

- **Host Name (or IP address)**: Enter the IP address of the server to be accessed, for example, **192.168.34.32**.
- **Port**: Retain the default value **22**.
- **Connection type**: Retain the default value **SSH**.
- **Close window on exit**: Retain the default value **Only on clean exit**.

NOTE

Configure **Host Name (or IP address)** and **Saved Sessions**, and click **Save**. You can double-click the saved record under **Saved Sessions** to log in to the server the next time.

Step 5 Click **Open**.

The **PuTTY** window is displayed prompting you to enter your user name next to **login as**.

NOTE

- If this is your first login to the server, the **PuTTY Security Alert** dialog box is displayed. Click **Yes** to proceed.
- If an incorrect user name or password is entered, you must set up a new PuTTY session.

Step 6 Enter the user name and password as prompted.

If the login is successful, the server host name is displayed on the left of the prompt.

----End

10 More Information

10.1 Technical Support

Huawei provides timely and efficient technical support through:

- Local branch offices
- Secondary technical support system
- Telephone technical support
- Remote technical support
- Onsite technical support

Technical Support Website

Technical documents are available at:

- **Huawei Enterprise website**
- **Huawei Carrier website**

Self-Service Platform and Community

Learn more about servers and communicate with experts at:

- **Huawei Server Information Service Platform** for specific server product documentation.
- **Huawei Enterprise iKnow** for Q&A about products.
- **Huawei Enterprise Support Community (Servers)** for learning and discussion.

Bulletins

For notices about product life cycles, warnings, and rectifications, visit **Product Bulletins**.

Cases

To learn server applications, visit **Computing Product Case Library**.

Contact Huawei

Huawei provides comprehensive technical support and services. To obtain assistance, contact Huawei technical support as follows:

- Contact Huawei customer service center.

  Enterprise customers in China:

  - Call 400-822-9999
  - Send emails to **support_e@huawei.com**.

    Enterprise customers outside China: visit **Global Enterprise Service Hotline**.

  Telecom carriers in China:

  - Call 400-830-2118
  - Send emails to **support@huawei.com**.

    Telecom carriers outside China: visit **Global Carrier Service Hotline**.
- Contact the technical support of your local Huawei office.

10.2 Maintenance Tools

Table 10-1 Maintenance tools

Resource	Description	How to Obtain
SmartKit Computing	SmartKit contains tools used for batch deployment, maintenance, and upgrade of servers. • Enterprise users: See **SmartKit Computing User Guide**. • Carrier users: See **SmartKit Computing User Guide**.	• Enterprise users: **SmartKit Computing** **NOTE** Downloading the software indicates your acknowledgement and agreement to the terms and conditions of **Huawei Enterprise Software User License Agreement**. • Carrier users: Contact the technical support of your local Huawei office.

Resource	Description	How to Obtain
Smart Provisioning	Smart Provisioning is used to install OSs, configure RAID, and upgrade firmware. • Enterprise users: Refer to **Smart Provisioning User Guide**. • Carrier users: Refer to **Smart Provisioning User Guide**.	• Enterprise users: Download it from **Smart Provisioning**. **NOTE** Downloading the software indicates your acknowledgement and agreement to the terms and conditions of **Huawei Enterprise Software User License Agreement**. • Carrier users: Contact the technical support of your local Huawei office.
FusionDirector	FusionDirector is the management software for intelligent O&M over the entire server lifecycle. It provides intelligent functions to manage deployment, assets, versions, faults, and energy efficiency. Enterprise users: Refer to **FusionDirector Specifications List**.	• Enterprise users: Download it from **FusionDirector**. **NOTE** Downloading the software indicates your acknowledgement and agreement to the terms and conditions of **Huawei Enterprise Software User License Agreement**. • Carrier users: Contact the technical support of your local Huawei office.
Computing Product Compatibility Checker	A tool used to query the OSs, parts, and peripherals compatible with a server.	Click **Computing Product Compatibility Checker**.
Computing Product Power Calculator	A tool used to calculate server power consumption based on the server configuration.	Click **Intelligent Computing Product Power Calculator**.
Computing Product Memory Configuration Assistant	Shows the DIMM installation sequence in a graphical manner after the product name, CPU quantity, and DIMM quantity are specified.	Click **Computing Product Memory Configuration Assistant**.

A Appendix

A.1 Label Description

Part No.

A part number (P/N) uniquely identifies a server component. You can find the number on a component or component package.

Figure A-1 shows a cable label with the part number 04151201.

NOTE

The actual label may be different from the one in the following figure, which is for reference only.

Figure A-1 Cable label

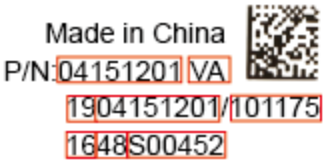


Table A-1 Cable label description

Item	Description
04151201	Part number
VA	Component version
19	Material identification code
101175	Version code
16/48	Year/Week (48th week in 2016)
S00452	Serial number

SN

The serial number (SN) on the label is a string that uniquely identifies a server. The SN is required when you contact Huawei technical support.

Figure A-2 shows the SN format.

Figure A-2 SN example

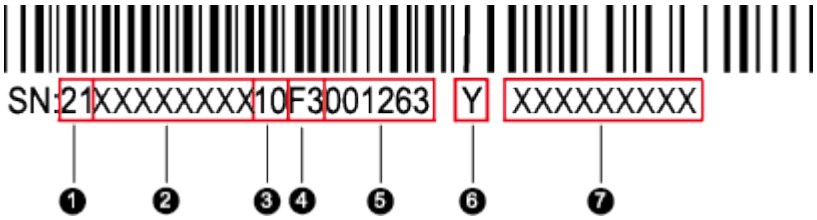


Table A-2 SN description

Callout No.	Description
1	SN ID (two characters), which is **21**.
2	Material identification code (8 characters), that is, the processing code.
3	Vendor code (two characters). **10** indicates Huawei, and other values indicate outsourcing vendors.
4	Year and month (two characters). • The first character indicates the year. – Digits 1 to 9 indicate years 2001 to 2009, respectively. – Letters A to H indicate years 2010 to 2017, respectively. – Letters J to N indicate years 2018 to 2022, respectively. – Letters P to Y indicate years 2023 to 2032, respectively. **NOTE** The years from 2010 are represented by uppercase letters excluding I, O, and Z because the three letters are similar to digits 1, 0, and 2. • The second character indicates the month. – Digits 1 to 9 indicate January to September, respectively. – Letters A to C indicate October to December, respectively.
5	Sequence number (six characters).
6	RoHS compliance (one character). **Y** indicates RoHS compliant.
7	Internal model, that is, product name.

A.2 Spare Parts

Table A-3 Spare parts

Abbreviation	Full Spelling	Definition	Application Scenario
RSP	Regular spare part	Regular spare parts include boards and modules. Safety stock is recommended.	Stored in the warehouses near sites based on the contract service type, Service Level Agreement (SLA), and service sites.
NRSP	Non-regular spare part	Non-regular spare parts include mechanical parts, accessories, and cables. Generally, safety stock is not kept for NRSPs. NRSPs are provided on demand; however, the lead time is not committed.	Stored in a country's warehouses based on the contract service type.
NSP	Non spare part	NSPs are not spare parts and do not have replaceable units at lower levels.	Not supplied or stored.
RSP&SUB	Regular spare parts with replaceable units at lower levels.	It is classified as a type of RSP and has RSPs or NRSPs at lower levels.	Stored in the warehouses near sites based on the contract service type, SLA, and service sites. Lower-level parts vary with actual demands.
NRSP&SUB	Non-regular spare parts with replaceable units at lower levels.	It is classified as a type of NRSP and has RSPs or NRSPs at lower levels.	Stored in a country's warehouses based on the contract service type. Lower-level parts vary with actual demands.
NSP&SUB	Non-spare parts with spare parts at lower levels.	It is not a spare part, but has RSPs or NRSPs at lower levels.	This part is not stored. Lower-level parts vary with actual demands.

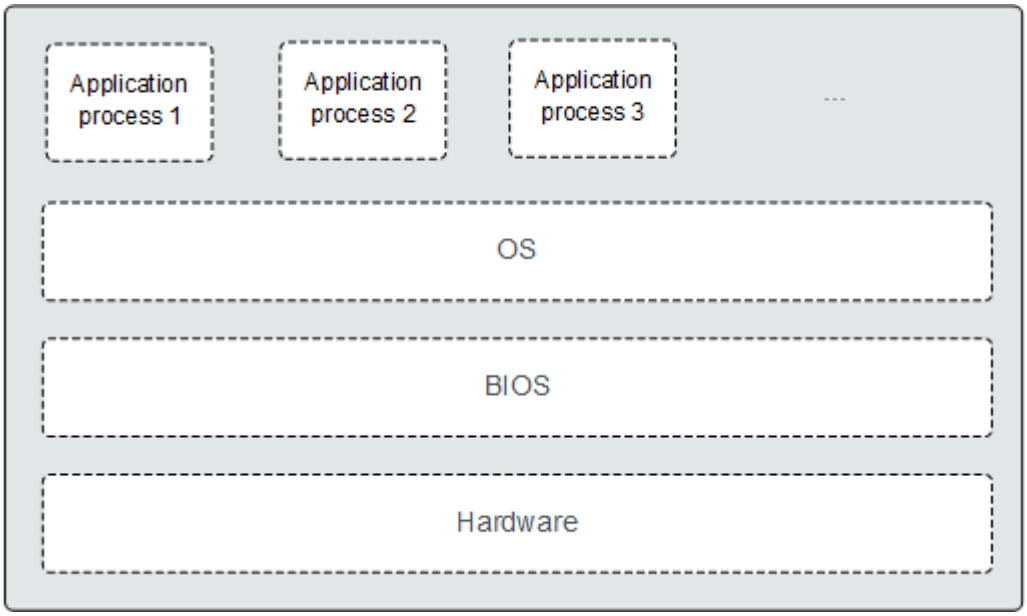
A.3 BIOS

The basic input/output system (BIOS) is the most basic software loaded to a computer hardware system. It provides an abstraction layer between the computer hardware and the OS. It is used to perform hardware initialization during the boot process and provide runtime services for the OS and programs. **Figure A-3** shows the BIOS location in the system.

The BIOS is stored in the SPI flash memory. It performs power-on self-test (POST), initializes the CPU and memory, checks the I/O and boot devices, and finally boots the OS. The BIOS also provides advanced configuration and power interface (ACPI) and hot swap settings.

The patented BIOS product has independent intellectual property rights. It supports customization and provides a variety of in-band and out-of-band configuration functions as well as high scalability.

Figure A-3 BIOS in the system



For details, see **BIOS Parameter Reference (Kunpeng 920 Processor)**.

A.4 iBMC

The iBMC is a remote server management system. The iBMC complies with IPMI 2.0 and supports various functions, including KVM redirection, text console redirection, remote virtual media, and hardware monitoring and management. The iBMC provides the following features:

- Various management interfaces

  IPMI, CLI, DCMI, Redfish, HTTPS, and SNMP are available for system integration.

- Fault detection and alarm management

  The iBMC implements fault detection and alarm management, ensuring stable, uninterrupted 24/7 system operation.
- Virtual KVM and virtual media

  The iBMC provides virtual KVM and virtual media to facilitate remote maintenance.
- WebUI

  The iBMC provides a WebUI for setting and querying device information.
- System breakdown screenshots and video recordings

  The iBMC creates screenshots and videos when the system collapses. The screenshots and videos help to identify the cause of system breakdown.
- Screen snapshots and videos

  The iBMC offers screen snapshots and videos, which simplify routine preventive maintenance.
- DNS and LDAP support

  The iBMC supports Domain Name System (DNS) and Lightweight Directory Application Protocol (LDAP) to implement domain management and directory service.
- Software image backup

  The iBMC provides software image backups, which allow the software to restart from a backup image when a failure occurs. This feature enhances system security.

For details about iBMC, see **TaiShan Rack Server iBMC User Guide**.

A.5 Glossary

B

BMC baseboard management controller

The BMC complies with the Intelligent Platform Management Interface (IPMI) standard, responsible for collecting, processing, and storing sensor signals, and monitoring the operating status of each component. The BMC provides the hardware status and alarm information about the managed objects for the management module, so that the management module can manage the objects.

E

Ethernet A baseband local area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel. Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and supports a data transfer rate of 10 Mbps on multiple cables. The Ethernet specification is the basis for the IEEE 802.3 standard.

H

hot swap	In a running system, insertion or removal of a component does not affect normal running of the system.

K

KVM	keyboard, video, and mouse

M

mezzanine card	A card connected to the mainboard through the connector, level to the mainboard. It is used on a device which has high requirement for space usage.

P

panel	The front-most or rear most element of a server, which serves to mount components, such as handles, indicators, and ports, and also seals the front of the chassis for airflow and electromagnetic compatibility (EMC).
PCIe	A computer expansion bus standard based on the existing PCI programming and communication standards and a faster serial communication system. Intel is a major contributor to this standard. PCIe is used only for interconnection between applications. A PCI system can be turned into a PCIe one by modifying the physical layer instead of software. PCIe delivers a faster speed and can replace almost all existing bus standards including AGP and PCI.

R

RAID	redundant array of independent disks A storage technology that combines multiple drives into a logical unit in several ways called "RAID levels", providing redundancy and delivering higher storage performance than a single disk.
redundancy	The ability of a system to keep functioning normally in the event of a device failure by having a backup device automatically replace the faulty one.

S

system event log (SEL)	A non-volatile storage area and associated interfaces for storing system platform events for later retrieval.
server	A special computer that provides various services for clients over a network.

U

U	A unit defined in International Electrotechnical Commission (IEC) 60297-1 to measure the height of a cabinet, chassis, or subrack. 1 U = 44.45 mm = 1.75 in.

A.6 Acronyms and Abbreviations

A	
AC	Alternating Current
B	
BIOS	Basic Input Output System
BMC	Baseboard Management Controller
C	
CLI	Command-line Interface
D	
DC	Direct Current
DDR4	Double Data Rate 4
DDDC	Double Device Data Correction
DED	Double-Bit Error Detection
DIMM	Dual In-line Memory Module
DRAM	Dynamic Random-Access Memory
DVD	Digital Video Disc
E	
ECC	Error Correcting Code
F	
FC	Fiber Channel
FCC	Federal Communications Commission
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
GPU	Graphics Processing Unit
H	
HA	High Availability

HDD	Hard Disk Drive
HPC	High Performance Computing
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	
iBMC	Intelligent Baseboard Management Controller
IEC	International Electrotechnical Commission
IOPS	Input/Output Operations per Second
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
K	
KVM	Keyboard Video and Mouse
L	
LRDIMM	load-Reduced Dual In-line Memory Module
LED	Light Emitting Diode
LOM	LAN on Motherboard
M	
MAC	Media Access Control
N	
NBD	Next Business Day
NC-SI	Network Controller Sideband Interface
P	
PCIe	Peripheral Component Interconnect Express
PDU	Power Distribution Unit
PHY	Physical Layer
PXE	Preboot Execution Environment
R	
RAID	Redundant Array of Independent Disks

RAS	Reliability, Availability and Serviceability
RDIMM	Registered Dual In-line Memory Module
RJ45	Registered Jack 45
RoHS	Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment
S	
SAS	Serial Attached Small Computer System Interface
SATA	Serial Advanced Technology Attachment
SDDC	Single Device Data Correction
SEC	Single-Bit Error Correction
SMI	Serial Management Interface
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
SSD	Solid-State Drive
T	
TCG	Trusted Computing Group
TCM	Trusted Cryptography Module
TCO	Total Cost of Ownership
TDP	Thermal Design Power
TET	Trusted Execution Technology
TFM	Trans Flash Module
TFTP	Trivial File Transfer Protocol
TPM	Trusted Platform Module
U	
UEFI	Unified Extensible Firmware Interface
UID	Unit Identification Light
UL	Underwriter Laboratories Inc.
USB	Universal Serial Bus
V	
VGA	Video Graphics Array
VLAN	Virtual Local Area Network

A.7 Sensor List (Server Configured with Kunpeng 920 7260 or 5250 Processors)

Sensor	Description	Component
Inlet Temp	Air inlet temperature	Right mounting ear
Outlet Temp	Air outlet temperature	iBMC card
CPU*N* Core Rem	CPU core temperature	CPU. *N* indicates the CPU number. The value is **1** or **2**.
CPU*N* Prochot	CPU Prochot	
CPU*N* VDDQ Temp	CPU VDDQ temperature	CPU 1: components in position U1 on the mainboard. CPU 2: components in position U2 on the mainboard. *N* indicates the CPU number. The value is **1** or **2**.
CPU*N* VRD Temp	CPU VRD temperature	CPU 1: components in position U1 on the mainboard. CPU 2: components in position U2 on the mainboard. *N* indicates the CPU number. The value is **1** or **2**.
CPU*N* MEM Temp	CPU DIMM temperature	DIMMs of CPU*N*. *N* indicates the CPU number. The value is **1** or **2**.
Disk*N* Temp	SSD temperature	*N* indicates the physical drive slot number.
FAN*N* Speed	Fan speed	Fan module. *N* indicates the fan module number. The value ranges from 1 to 4.
Power	Server input power	Total power of all the PSUs.
Power*N*	PSU input power	PSU. *N* indicates the PSU number. The value is **1** or **2**.
CPU*N* Status	CPU status	CPU. *N* indicates the CPU number. The value is **1** or **2**.

Sensor	Description	Component
CPU*N* Memory	DIMM status	DIMMs of CPU*N*. *N* indicates the DIMM number. The value is **1** or **2**.
PS*N* Fan Status	PSU fan fault status	PSU. *N* indicates the PSU number. The value is 1 or 2.
PS*N* Temp Status	PSU presence status	
PS*N* Status	PSU fault status	
Power Button	Power button pressed	Right mounting ear
UID Button	UID button status	
DISK*N*	Drive status	Drive. *N* indicates the physical drive slot number.
FAN*N* Presence	Fan presence	Fan module. *N* indicates the fan module number. The value ranges from 1 to 4.
FAN*N* Status	Fan fault status	
RTC Battery	RTC battery status. An alarm is generated when the voltage is lower than 1 V.	CMOS battery
DIMM*N*	DIMM status	DIMM. *N* indicates the DIMM slot number.
PS*N* Inlet Temp	PSU air inlet temperature	PSU. *N* indicates the PSU number. The value is **1** or **2**.
PS*N* Redundancy	Redundancy failure alarm due to PSU removal	PSU. *N* indicates the PSU number. The value is 1 or 2.
BMC Boot Up	BMC startup event	N/A *N* indicates the component number.
SEL Status	Event of SEL being about to be full or being cleared	
Op. Log Full	Event of operation logs being about to be full or being cleared	
Sec. Log Full	Event of security logs being about to be full or being cleared	
CPU Usage	CPU usage	
Memory Usage	Memory usage	
BMC Time Hopping	Time hopping	

Sensor	Description	Component
NTP Sync Failed	Event of NTP synchronization failure and recovery	
Host Loss	System monitoring software (BMA) link loss detection	
SYS 12V_2	Mainboard 12.0 V voltage (the second output 12 V voltage detection for soft-start: riser module + NIC0 module)	
SYS 12V_3	Mainboard 12.0 V voltage (the third output 12 V voltage detection for soft-start: CPU 1 + fan module)	
SYS 12V_4	Mainboard 12.0 V voltage (the fourth output 12 V voltage detection for soft-start: CPU 2 + fan module)	
SYS 12V_5	Mainboard 12.0 V voltage (the fifth output 12 V voltage detection for soft-start: built-in-drive backplane + CPU 2)	
SYS 12V_6	Mainboard 12.0 V voltage (the sixth output 12 V voltage detection for soft-start: front-drive backplane)	
CPU*N* VDDQ_AB	CPU memory voltage	
CPU*N* VDDQ_CD		
CPU*N* VRD Temp	CPU VRD voltage	
CPU*N* VDDAVS	CPU VDDAVS voltage	
CPU*N* HVCC	CPU HVVC voltage	
CPU*N* N_VDDAVS	CPU N_VDDAVS voltage	
CPU*N* VDDFIX	CPU VDDFIX voltage	
SAS Cable	Entity presence	

Sensor	Description	Component
PS*N* VIN	Input voltage	
PwrOk Sig. Drop	Voltage dip status	
ACPI State	ACPI status	
SysFWProgress	Software process and system startup errors	
SysRestart	System restart cause	
Boot Error	Boot error	
Watchdog2	Watchdog	
Mngmnt Health	Management subsystem health status	
Riser*N* Card	Entity presence	
RAID Presence	RAID controller card presence	
RAID*N* Temp	RAID controller card temperature	
PCIe Status	PCIe status	
PwrOn TimeOut	Power-on timeout	
PwrCap Status	Power capping status	
HDD Backplane	Drive backplane entity presence	
HDD BP Status	Drive backplane health status	
NIC*N* Temp	NIC temperature	
NIC OM Temp	NIC OM temperature	
NIC1-*N* Link Down (*N* 1. 2. 3. 4)	Network port link status of NIC 1	
NIC2-*N* Link Down (*N* 1. 2. 3. 4)	Network port link status of NIC 2	
System Notice	Hot restart reminder and fault diagnosis program information collection	
System Error	System suspension or restart. Check the background logs.	

A.8 Sensor List (Server Configured with the Kunpeng 920 5220 or 3210 Processors)

Sensor	Description	Component
Inlet Temp	Air inlet temperature	Right mounting ear
Outlet Temp	Air outlet temperature	iBMC card
CPU*N* Core Rem	CPU core temperature	CPU. *N* indicates the CPU number. The value is **1** or **2**.
CPU*N* Prochot	CPU Prochot	
CPU*N* VDDQ Temp	CPU VDDQ temperature	CPU 1: components in position U1 on the mainboard. CPU 2: components in position U2 on the mainboard. *N* indicates the CPU number. The value is **1** or **2**.
CPU*N* VRD Temp	CPU VRD temperature	CPU 1: components in position U1 on the mainboard. CPU 2: components in position U2 on the mainboard. *N* indicates the CPU number. The value is **1** or **2**.
CPU*N* MEM Temp	CPU DIMM temperature	DIMMs of CPU*N*. *N* indicates the CPU number. The value is **1** or **2**.
Disks Temp	Highest temperature among the temperatures of all drives	-
FAN*N* Speed	Fan speed	Fan module. *N* indicates the fan module number. The value ranges from **1** to **4**.
Power	Server input power	Total power of all the PSUs.
Power*N*	PSU input power	PSU. *N* indicates the PSU number. The value is **1** or **2**.
CPU*N* Status	CPU status	CPU. *N* indicates the CPU number. The value is **1** or **2**.

Sensor	Description	Component
CPU*N* Memory	DIMM status	DIMMs of CPU*N*. *N* indicates the DIMM number. The value is **1** or **2**.
PS*N* Fan Status	PSU fan fault status	PSU. *N* indicates the PSU number. The value is **1** or **2**.
PS*N* Temp Status	PSU presence status	
PS*N* Status	PSU fault status	
Power Button	Power button pressed	Right mounting ear
UID Button	UID button status	
DISK*N*	Drive status	Drive. *N* indicates the physical drive slot number.
FAN*N* Presence	Fan presence	Fan module. *N* indicates the fan module number. The value ranges from 1 to 4.
FAN*N* Status	Fan fault status	
RTC Battery	RTC battery status. An alarm is generated when the voltage is lower than 1 V.	CMOS battery
DIMM*N*	DIMM status	DIMM. *N* indicates the DIMM slot number.
PS*N* Inlet Temp	PSU air inlet temperature	PSU. *N* indicates the PSU number. The value is **1** or **2**.
PS Redundancy	Redundancy failure alarm due to PSU removal	PSU
BMC Boot Up	BMC startup event	N/A. *N* indicates the component number.
SEL Status	Event of SEL being about to be full or being cleared	
Op. Log Full	Event of operation logs being about to be full or being cleared	
Sec. Log Full	Event of security logs being about to be full or being cleared	
CPU Usage	CPU usage	
Memory Usage	Memory usage	
BMC Time Hopping	Time hopping	

Sensor	Description	Component
NTP Sync Failed	Event of NTP synchronization failure and recovery	
Host Loss	System monitoring software (BMA) link loss detection	
SYS 12V_1	Mainboard 12.0 V voltage (the second output 12 V voltage detection for soft-start: fan module)	
SYS 12V_2	Mainboard 12.0 V voltage (the third output 12 V voltage detection for soft-start: CPU 2 + rear-drive backplane)	
SYS 12V_3	Mainboard 12.0 V voltage (the fourth output 12 V voltage detection for soft-start: CPU 1 + CPU2)	
SYS 12V_4	Mainboard 12.0 V voltage (the fifth output 12 V voltage detection for soft-start: front-drive backplane)	
SYS 12V_5	Mainboard 12.0 V voltage (the sixth output 12 V voltage detection for soft-start: NIC + riser card + RAID controller card + rear-drive backplane)	
CPU*N* VDDQ_AB	CPU memory voltage	
CPU*N* VDDQ_CD		
CPU*N* VRD Temp	CPU VRD voltage	
CPU*N* VDDAVS	CPU VDDAVS voltage	
CPU*N* VDDFIX	CPU VDDFIX voltage	
SAS Cable	Entity presence	
PS*N* VIN	Input voltage	
PwrOk Sig. Drop	Voltage dip status	

Sensor	Description	Component
ACPI State	ACPI status	
SysFWProgress	Software process and system startup errors	
SysRestart	System restart cause	
Boot Error	Boot error	
Watchdog2	Watchdog	
Mngmnt Health	Management subsystem health status	
Riser*N* Card	Entity presence	
RAID Presence	RAID controller card presence	
RAID Temp	RAID controller card temperature	
PCIe Status	PCIe status	
PwrOn TimeOut	Power-on timeout	
PwrCap Status	Power capping status	
HDD Backplane	Drive backplane entity presence	
HDD BP Status	Drive backplane health status	
NIC*N* Temp	NIC temperature	
NIC OM Temp	NIC OM temperature	
NIC1-*N* Link Down (*N* 1. 2. 3. 4)	Network port link status of NIC 1	
NIC2-*N* Link Down (*N* 1. 2. 3. 4)	Network port link status of NIC 2	
System Notice	Hot restart reminder and fault diagnosis program information collection	
System Error	System suspension or restart. Check the background logs.	
Cert OverDue	Certificate expiration check	
RTC time	RTC clock status	