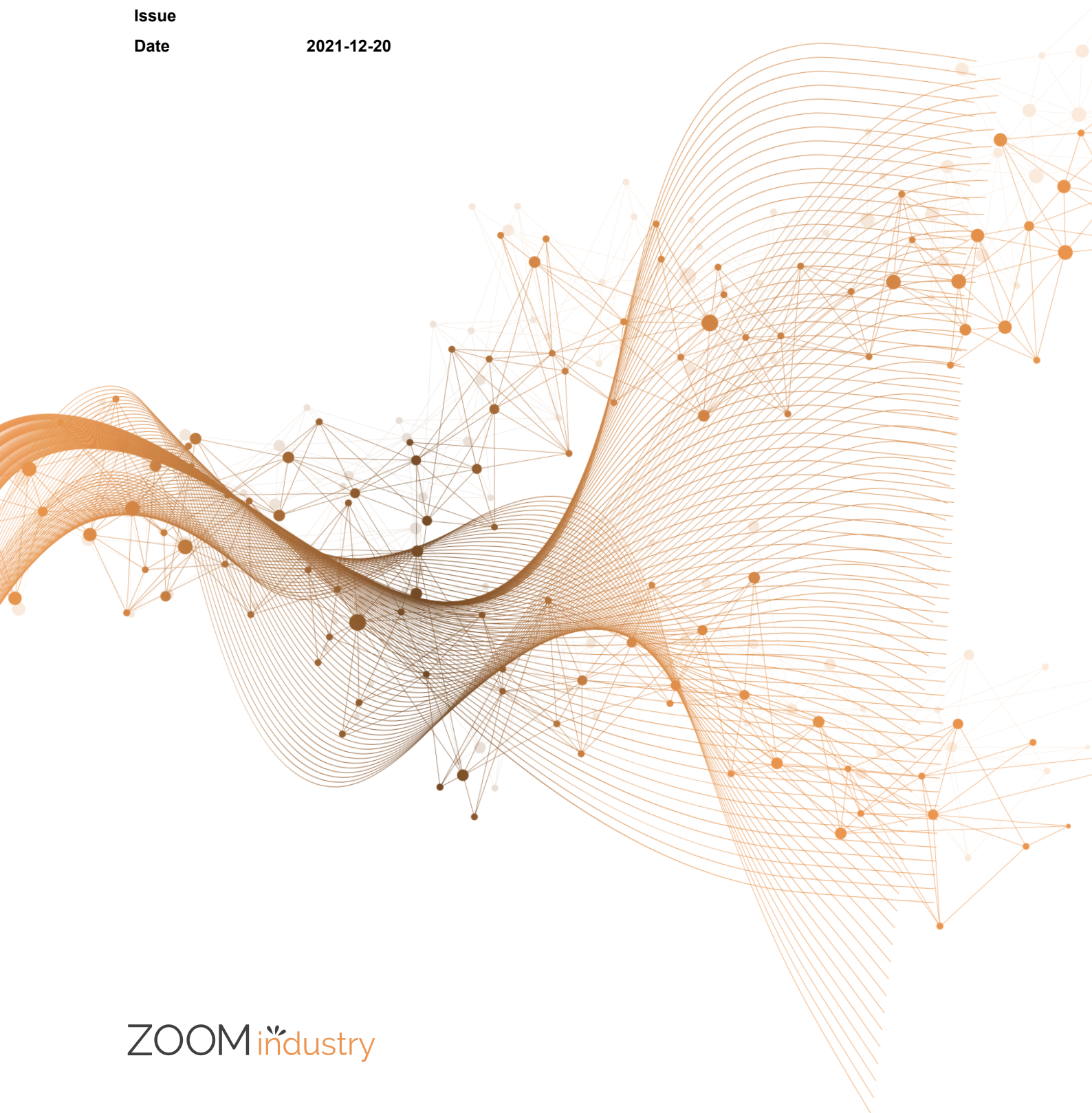


ZOOM Hard' Server 1288H V6 Server User Guide

Issue

Date

2021-12-20



Copyrights © ZOOMtecnologia, Ltda. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of ZOOMtecnologia, Ltda.

Trademarks and Permissions

ZOOM industry, ZOOM Hard'Server and ZOOM tecnologia are trademarks or registered trademarks of ZOOMtecnologia Ltda. Other trademarks, product, service and company names mentioned are the property of their respective owners

Notice

In this document, "ZOOMtecnologia" is used to refer to "ZOOMtecnologia, Ltda." for concise description and easy understanding, which does not mean that "ZOOMtecnologia" may have any other meaning. Any "ZOOMtecnologia" mentioned or described hereof may not be understood as any meaning other than "ZOOMtecnologia, Ltda.", and ZOOMtecnologia, Ltda. shall not bear any liability resulting from the use of "ZOOMtecnologia".

The purchased products, services and features are stipulated by the contract made between xFusion 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.

ZOOMtecnologia, Ltda.

Address: Edifício Office Green - 816
R. da Praça, 241 - Pedra Branca,
Palhoça - SC, 88137-086

Website: www.zoomtecnologia.com.br

ZOOMtecnologia

Contents

About This Document	vii
1 Overview	9
1.1 Overview	9
1.2 Physical Structure	10
1.3 Logical Structure	11
2 Hardware Description	13
2.1 Front Panel	13
2.1.1 Appearance	13
2.1.2 Indicators and Buttons	14
2.1.3 Ports	17
2.2 Rear Panel	20
2.2.1 Appearance	20
2.2.2 Indicators and Buttons	21
2.2.3 Ports	22
2.3 Processors	24
2.4 Memory	24
2.4.1 DDR4 Memory	24
2.4.1.1 Memory ID	24
2.4.1.2 Memory Subsystem Architecture	25
2.4.1.3 Memory Compatibility	27
2.4.1.4 DIMM Installation Rules	28
2.4.1.5 Memory Installation Positions	29
2.4.1.6 Memory Protection Technologies	32
2.5 Storage	32
2.5.1 Drive Configurations	32
2.5.2 Drive Numbering	35
2.5.3 Drive Indicators	43
2.5.4 RAID Controller Card	45
2.6 Network	45
2.6.1 OCP 3.0 Network Adapter	45
2.7 I/O Expansion	46
2.7.1 PCIe Cards	46

2.7.2 PCIe Slots	46
2.7.3 PCIe Slot Description	47
2.8 PSUs	49
2.9 Fan Modules	49
2.10 Boards	51
2.10.1 Mainboard.....	51
2.10.2 Drive Backplane	53
3 Product Specifications.....	56
3.1 Technical Specifications	56
3.2 Environmental Specifications	59
3.3 Physical Specifications	61
4 Software and Hardware Compatibility	63
5 Safety Instructions	64
5.1 Security	64
5.2 Maintenance and Warranty	67
6 ESD	68
6.1 ESD Prevention	68
6.2 Grounding Methods for ESD Prevention.....	68
7 Installation and Configuration.....	70
7.1 Installation Environment Requirements	70
7.1.1 Space and Airflow Requirements.....	70
7.1.2 Temperature and Humidity Requirements	71
7.1.3 Cabinet Requirements.....	71
7.2 Hardware Installation.....	72
7.2.1 Installation Overview.....	72
7.2.2 Unpacking the Server.....	73
7.2.3 Installing Optional Parts	73
7.2.4 Installing Server Guide Rails.....	74
7.2.4.1 Installing L-Shaped Guide Rails.....	74
7.2.4.2 Installing the Static Rail Kit.....	76
7.2.4.3 Installing the Ball Bearing Rail Kit	78
7.2.5 Installing a Server	81
7.2.5.1 Installing the Server on L-Shaped Guide Rails.....	81
7.2.5.2 Installing the Server on the Static Rail Kit.....	82
7.2.5.3 Installing a Server on the Ball Bearing Rail Kit	85
7.2.6 Connecting External Cables.....	91
7.2.6.1 Cabling Guidelines	91
7.2.6.2 Connecting Mouse, Keyboard, and VGA Cables.....	92
7.2.6.3 Connecting Network Cables	93
7.2.6.4 Connecting a Cable to an Optical Port.....	94

7.2.6.5 Connecting an IB Cable	98
7.2.6.6 Connecting a USB Type-C Cable	100
7.2.6.7 Connecting a USB Device	100
7.2.6.8 Connecting a Serial Cable.....	101
7.2.6.9 Connecting PSU Cables.....	102
7.2.6.9.1 Connecting the AC PSU Cable	102
7.2.6.9.2 Connecting the DC PSU Cable	103
7.2.6.10 Checking Cable Connections	104
7.3 Power-On and Power-Off	105
7.3.1 Powering On	105
7.3.2 Powering Off	106
7.4 Initial Configuration	107
7.4.1 Default Information	107
7.4.2 Configuration Overview	108
7.4.3 Changing the Initial Password of the Default iBMC User.....	109
7.4.4 Checking the Server.....	112
7.4.5 Configuring the BMC IP Address	114
7.4.6 Configuring RAID	115
7.4.7 Configuring the BIOS	115
7.4.7.1 Setting the System Boot Sequence	115
7.4.7.2 Setting PXE for a NIC	116
7.4.7.2.1 Setting PXE for an OCP 3.0 NIC.....	116
7.4.7.2.2 Setting PXE for a PCIe NIC	117
7.4.7.3 Setting the BIOS Password.....	118
7.4.7.3.1 Setting the Password of the BIOS Administrator.....	118
7.4.7.3.2 Setting the Password of a Common BIOS User.....	119
7.4.7.4 Setting the Language	120
7.4.8 Installing an OS	120
7.4.9 Upgrading the System.....	120
8 Troubleshooting Guide	122
9 Common Operations	123
9.1 Querying the iBMC IP Address	123
9.2 Logging In to the iBMC WebUI	124
9.3 Logging In to the SmartServer.....	131
9.4 Logging In to the Desktop of a Server	136
9.4.1 Using the Remote Virtual Console.....	136
9.4.1.1 iBMC	136
9.4.2 Logging In to the System Using the Independent Remote Console.....	138
9.4.2.1 Windows	138
9.4.2.2 Ubuntu	141
9.4.2.3 Mac	143

9.4.2.4 Red Hat	146
9.5 Logging In to the Server CLI.....	148
9.5.1 Logging In to the CLI Using PuTTY over a Network Port.....	148
9.5.2 Logging In to the CLI Using PuTTY over a Serial Port	150
9.6 Managing VMD	151
9.6.1 Enabling VMD.....	152
9.6.2 Disabling VMD.....	152
9.7 Accessing the BIOS	153
9.8 Clearing Data from a Storage Device	165
10 More Information.....	168
10.1 Technical Support	168
10.2 Product Information Resources	169
10.3 Product Configuration Resources	169
10.4 Maintenance Tool	170
11 Software and Configuration Utilities	171
11.1 iBMC	171
11.2 BIOS	172
A Appendix	173
B Glossary.....	184
C Acronyms and Abbreviations	187

About This Document

Overview

This document describes the HardServer 1288H V6 in terms of its appearance, functions, structure, hardware installation, basic configuration, OS installation methods, and troubleshooting.






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
01	2021-12-24	This issue is the first official release.

1 Overview

- 1.1 Overview
- 1.2 Physical Structure
- 1.3 Logical Structure

1.1 Overview

Hard' Server 1288H V6 (1288H V6) is a new-generation 1U 2-socket rack server designed for Internet, Internet Data Center (IDC), cloud computing, enterprise, and telecom applications.

The 1288H V6 is ideal for IT core services, cloud computing, virtualization, high-performance computing, distributed storage, big data processing, enterprise or telecom service applications, and other complex workloads.

The reliable 1288H V6 features low power consumption, high scalability, easy deployment, and simplified management.

NOTE

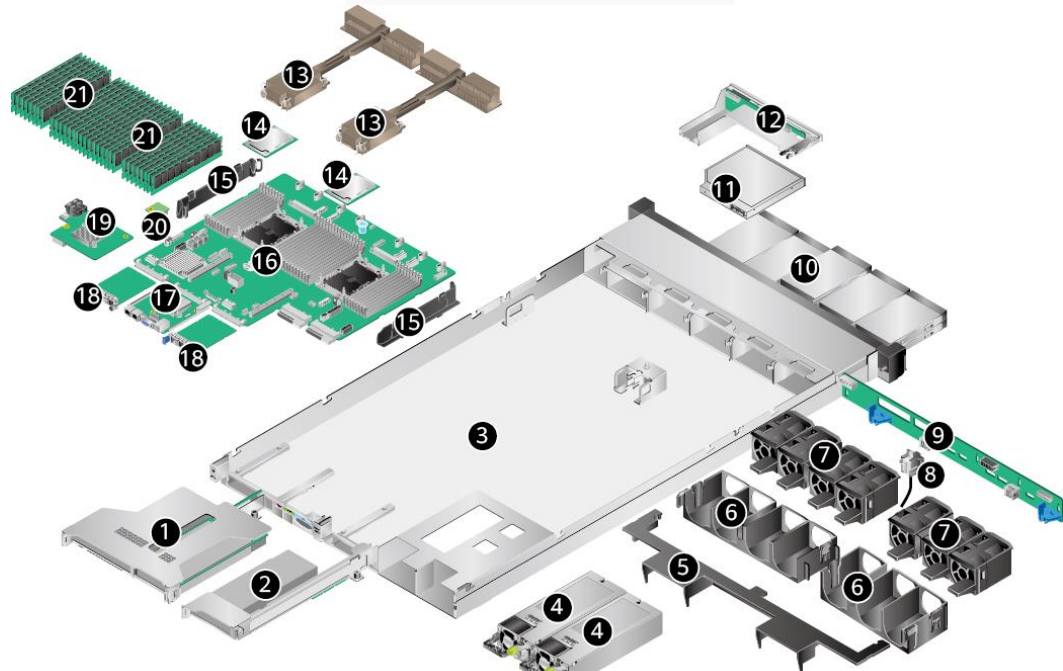
For details about the 1288H V6 nameplate information, see A.3 Nameplate.

Figure 1-1 Physical structure of a 1288H V6 with 8 x 2.5" drives (example)



1.2 Physical Structure

Figure 1-2 Physical structure of a server with 8 x 2.5" drives (example)

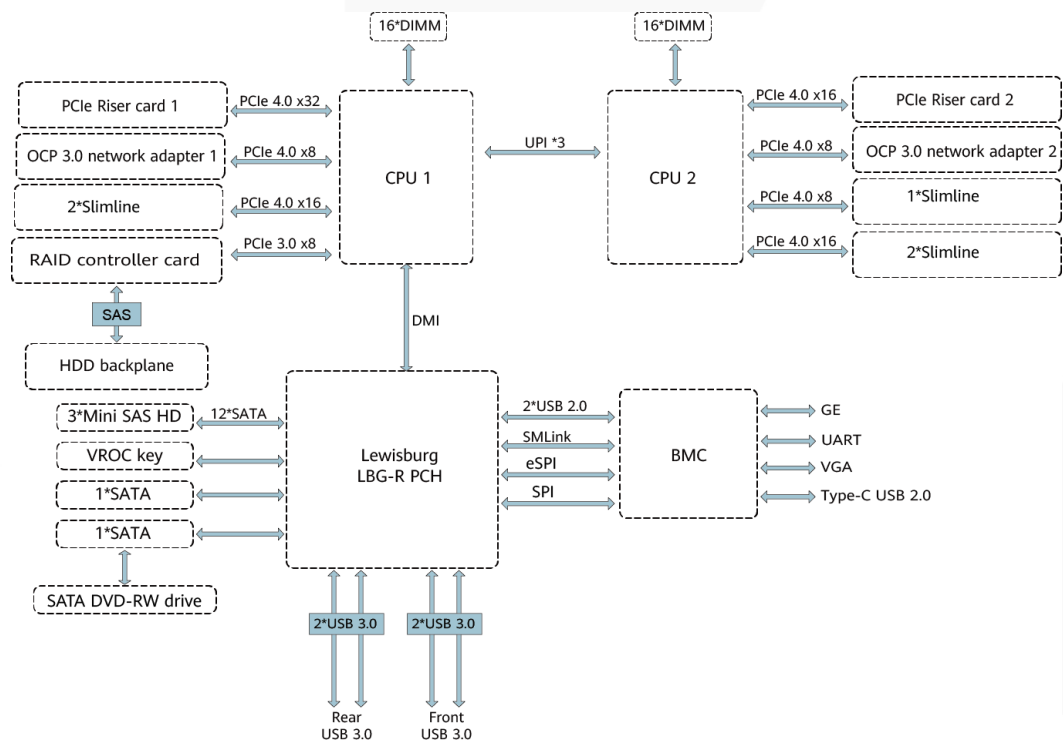


1	I/O module 1	2	I/O module 2
---	--------------	---	--------------

3	Chassis	4	PSUs
5	Air duct	6	Fan module brackets
7	Fan modules	8	Intrusion sensor
9	Front-drive backplane	10	Front drives
11	Built-in DVD drive	12	Indicator board
13	Processor heat sinks	14	Processors
15	Cable organizers	16	Mainboard
17	BMC card	18	OCP 3.0 network adapters
19	Screw-in RAID controller card	20	TPM/TCM
21	Memory modules	-	-

1.3 Logical Structure

Figure 1-3 Logical Structure



- The server supports one or two third-generation Intel® Xeon® Scalable Ice Lake processors.
- The server supports up to 32 memory modules.

- The CPUs (processors) interconnect with each other through three UPI links at a speed of up to 11.2 GT/s.
- The PCIe riser card connects to the processors through PCIe buses to provide ease of expandability and connection.
- CPU1 and CPU2 each support one OCP 3.0 network adapter.
- The screw-in RAID controller card on the mainboard connects to CPU 1 through PCIe buses, and connects to the drive backplane through SAS signal cables. A variety of drive backplanes are provided to support different local storage configurations.
- The LBG-R Platform Controller Hub (PCH) is integrated on the mainboard to support four USB 3.0 ports.
- The BMC management chip integrated on the mainboard supports a video graphic array (VGA) port, a management network port, and a serial port.

2 Hardware Description

- 2.1 Front Panel
- 2.2 Rear Panel
- 2.3 Processors
- 2.4 Memory
- 2.5 Storage
- 2.6 Network
- 2.7 I/O Expansion
- 2.8 PSUs
- 2.9 Fan Modules
- 2.10 Boards

2.1 Front Panel

2.1.1 Appearance

- 4 x 3.5" drive configuration

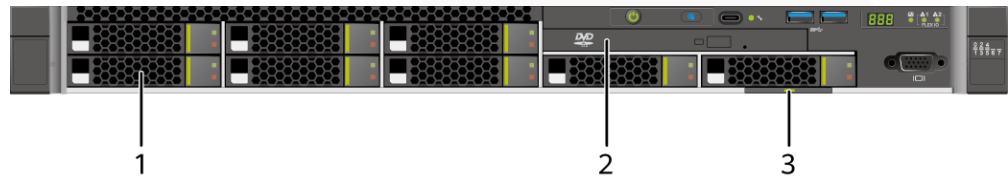
Figure 2-1 Front view



1	Drive	2	Slide-out label plate (with an SN label)
---	-------	---	--

- 8 x 2.5" Drive Configuration

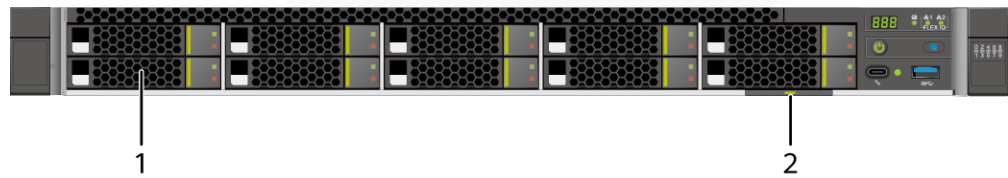
Figure 2-2 Front view



1	Drive	2	(Optional) Built-in DVD drive
3	Label with SN	-	-

- 10 x 2.5" drive configuration

Figure 2-3 Front view



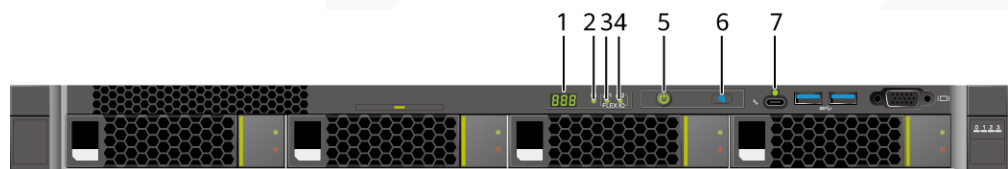
1	Drive	2	Slide-out label plate (with an SN label)
---	-------	---	--

2.1.2 Indicators and Buttons

Indicator and Button Positions

- 4 x 3.5" drive configuration

Figure 2-4 Indicators and buttons on the front panel

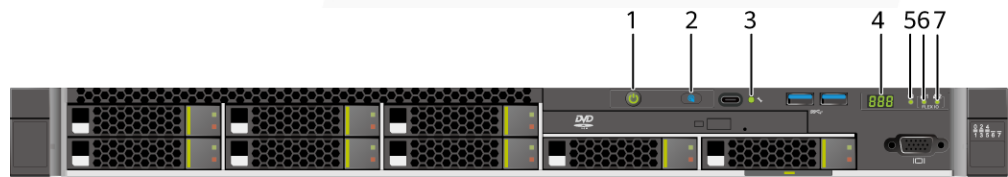


1	Fault diagnosis LED	2	Health status indicator
3	FlexIO card 1 presence	4	FlexIO card 2 presence

	indicator		indicator
5	Power button/indicator	6	UID button/indicator
7	iBMC direct connect management port indicator	-	-

- 8 x 2.5" drive configuration

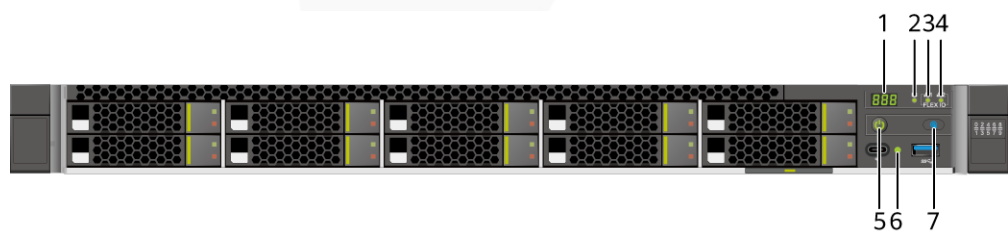
Figure 2-5 Indicators and buttons on the front panel



1	Power button/indicator	2	UID button/indicator
3	iBMC direct connect management port indicator	4	Fault diagnostic LED
5	Health status indicator	6	FlexIO card 1 presence indicator
7	FlexIO card 2 presence indicator	-	-

- 10 x 2.5" drive configuration





Figure 2-6 Indicators and buttons on the front panel





1	Fault diagnosis LED	2	Health status indicator
3	FlexIO card 1 presence indicator	4	FlexIO card 2 presence indicator
5	Power button/indicator	6	iBMC direct connect management port indicator
7	UID button/indicator	-	-

Indicator and Button Descriptions

Table 2-1 Description of indicators and buttons on the front panel

Silkscreen	Indicator and Button	Description
	Fault diagnosis LED	<ul style="list-style-type: none"> ---: The device is operating properly. Error code: A component is faulty. <p>For details about error codes, see the <i>Hard'Server Rack Server iBMC Alarm Handling</i>.</p>
	Health status indicator	<ul style="list-style-type: none"> Off: The device is powered off or is faulty. Blinking red at 1 Hz: A major alarm has been generated on the system. Blinking red at 5 Hz: A critical alarm has been generated on the system. Steady green: The device is operating properly.
	FlexIO card presence indicator	<p>Indicates whether the FlexIO card is detected.</p> <ul style="list-style-type: none"> Off: The FlexIO card is not detected. Blinking green at 0.5 Hz: The FlexIO card is detected but is not powered on. Blinking green at 2 Hz: The FlexIO card is detected and has just been inserted. Steady green: The FlexIO card is detected and the power supply is normal.
	Power button/indicator	<p>Power indicator:</p> <ul style="list-style-type: none"> Off: The device is not powered on. Steady green: The device is powered on. Blinking yellow: The iBMC is starting. The power button is locked and cannot be pressed. The iBMC is started in about 1 minute, and then the power indicator is steady yellow. Steady yellow: The device is standby. <p>Power button:</p> <ul style="list-style-type: none"> When the device is powered on, you can press this button to gracefully shut down the OS. <p>NOTE For different OSs, you may need to shut down the OS as prompted.</p> <ul style="list-style-type: none"> When the device is powered on, you can hold down this button for 6 seconds to forcibly power off the device. When the power indicator is steady yellow, you can press this button to power on the device.

Silkscreen	Indicator and Button	Description
	UID button/indicator	<p>The UID button/indicator helps identify and locate a device.</p> <p>UID indicator:</p> <ul style="list-style-type: none"> • Off: The device is not being located. • Blinking or steady blue: The device is being located. <p>UID button:</p> <ul style="list-style-type: none"> • You can control the UID indicator status by pressing the UID button or using the iBMC. • You can press this button to turn on or off the UID indicator. • You can press and hold down this button for 4 to 6 seconds to reset the iBMC.
	iBMC direct connect management port indicator	<p>Indicates the status when the iBMC direct connect management port connects to a terminal (local PC or Android mobile phone):</p> <ul style="list-style-type: none"> • Off: No terminal is connected. • Blinking green at short intervals for 3 seconds and then off: The port is disabled. • Steady green: The terminal is connected. <p>Indicates the status when the iBMC direct connect management port connects to a USB device:</p> <ul style="list-style-type: none"> • Blinking red at long intervals: The job fails or an error is reported when the job is complete. • Blinking green at short intervals: The job is being executed. • Blinking green at short intervals for 3 seconds and then off: The port is disabled. • Steady green: The server configuration file is being copied from the USB device or the job is successfully completed.

2.1.3 Ports

Port Positions

- 4 x 3.5" drive configuration

Figure 2-7 Ports on the front panel



1	iBMC direct connect management port	2	USB 3.0 port
3	VGA port	-	-

- 8 x 2.5" drive configuration

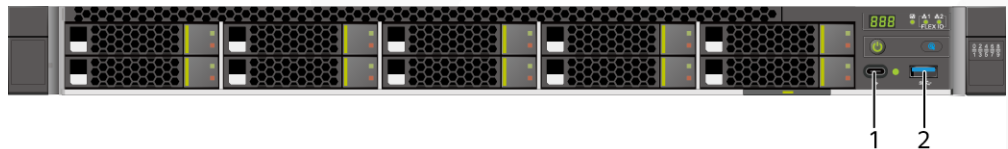
Figure 2-8 Ports on the front panel



1	iBMC direct connect management port	2	USB 3.0 port
3	VGA port	-	-

- 10 x 2.5" drive configuration

Figure 2-9 Ports on the front panel



1	iBMC direct connect management port	2	USB 3.0 port
---	-------------------------------------	---	--------------

Port Description

Table 2-2 Ports on the front panel

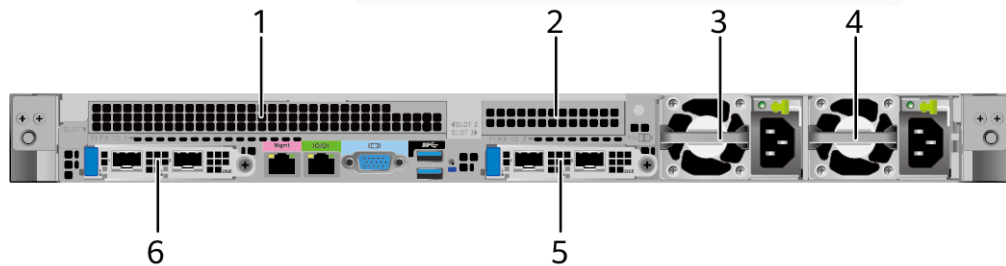
Port	Type	Quantity ^{Note}	Description
VGA port	DB15	1	Used to connect a display terminal, such as a monitor or KVM.
iBMC direct connect management port	USB Type-C NOTE The USB 2.0 protocol is supported.	1	<p>Used to connect to a local PC or mobile phone through a USB Type-C cable to monitor and manage the system.</p> <p>NOTE</p> <p>Only local PCs running Windows 10 and mobile phones running Android are supported.</p> <ul style="list-style-type: none"> To log in to the iBMC from the local PC, enter https://IP address of the iBMC management network port in the address box of the browser on the local PC. When accessing the iBMC through a mobile phone, you need to use the mobile application SmartServer to access the iBMC. <p>For details, see the <i>Server SmartServer User Guide</i>.</p> <p>Used to connect to a USB device.</p> <p>NOTICE</p> <ul style="list-style-type: none"> Before connecting an external USB device, ensure that the USB device functions properly. Otherwise, it may adversely impact the server. For details about how to connect a USB device to the iBMC management port, see <i>Hard'Server iBMC User Guide</i>.
USB port	USB 3.0	2	<p>Used to connect to a USB 3.0 device.</p> <p>NOTICE</p> <ul style="list-style-type: none"> Before connecting an external USB device, ensure that the USB device functions properly. Otherwise, it may adversely impact the server. The USB 3.0 port can be used to supply power to low-power peripherals. However, the USB 3.0 port must comply with the USB specifications. To run advanced peripherals, such as external CD/DVD drives, an

Port	Type	Quantity ^{Note}	Description
			external power supply is required.
Note: The number of ports varies depending on server configuration. This table lists the maximum number of ports in different configurations.			

2.2 Rear Panel

2.2.1 Appearance

Figure 2-10 Rear view



1	I/O module 1	2	I/O module 2
3	PSU 1	4	Power supply 2
5	(Optional) FlexIO card 2 NOTE The FlexIO card slot supports only OCP 3.0 network adapters.	6	(Optional) FlexIO card 1 NOTE The FlexIO card slot supports only OCP 3.0 network adapters.

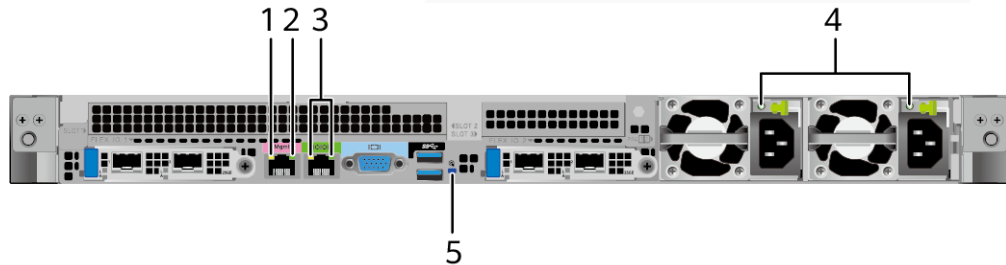
NOTE

- I/O module 1 supports a PCIe riser module or rear drive module.
- I/O module 2 supports only the PCIe riser module.
- For details about the OCP 3.0 network adapter, see 2.6.1 OCP 3.0 Network Adapter .
- The figure is for reference only. The actual configuration may vary.

2.2.2 Indicators and Buttons

Indicator Positions

Figure 2-11 Indicators on the rear panel




1	Data transmission status indicator for the management network port	2	Connection status indicator for the management network port
3	Serial port indicators NOTE Reserved and unavailable currently.	4	PSU indicators
5	UID indicator	-	-

Indicator Description

Table 2-3 Indicators on the rear panel

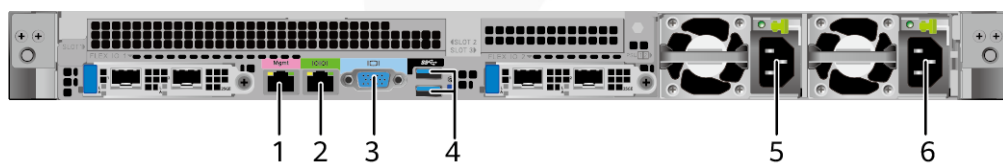
Silkscreen	Indicator	Description
-	Data transmission status indicator for the management network port	<ul style="list-style-type: none"> Off: No data is being transmitted. Blinking yellow: Data is being transmitted.
-	Connection status indicator for the management network port	<ul style="list-style-type: none"> Off: The network port is not connected. Steady green: The network port is connected properly.
-	PSU indicator	<ul style="list-style-type: none"> Off: No power is supplied. Blinking green at 1 Hz: <ul style="list-style-type: none"> The input is normal, and the server is standby. The input is overvoltage or undervoltage. The PSU is in deep hibernation

Silkscreen	Indicator	Description
		<p>mode.</p> <ul style="list-style-type: none"> Blinking green at 4 Hz: The firmware is being upgraded online. Steady green: The power input and output are normal. Steady orange: The input is normal but there is no output. <p>NOTE The possible causes of no power output are as follows:</p> <ul style="list-style-type: none"> Power supply overtemperature protection Power output overcurrent or short-circuit Output overvoltage Short-circuit protection Device failure (excluding failure of all devices)
	UID indicator	<p>The UID indicator helps identify and locate a device.</p> <ul style="list-style-type: none"> Off: The device is not being located. Blinking or steady blue: The device is being located. <p>NOTE You can control the UID indicator status by pressing the UID button or using the iBMC.</p>

2.2.3 Ports

Port Positions

Figure 2-12 Ports on the rear panel



1	Management network port	2	Serial port
3	VGA port	4	USB 3.0 ports
5	Socket for PSU 1	6	Socket for PSU 2

Port Description

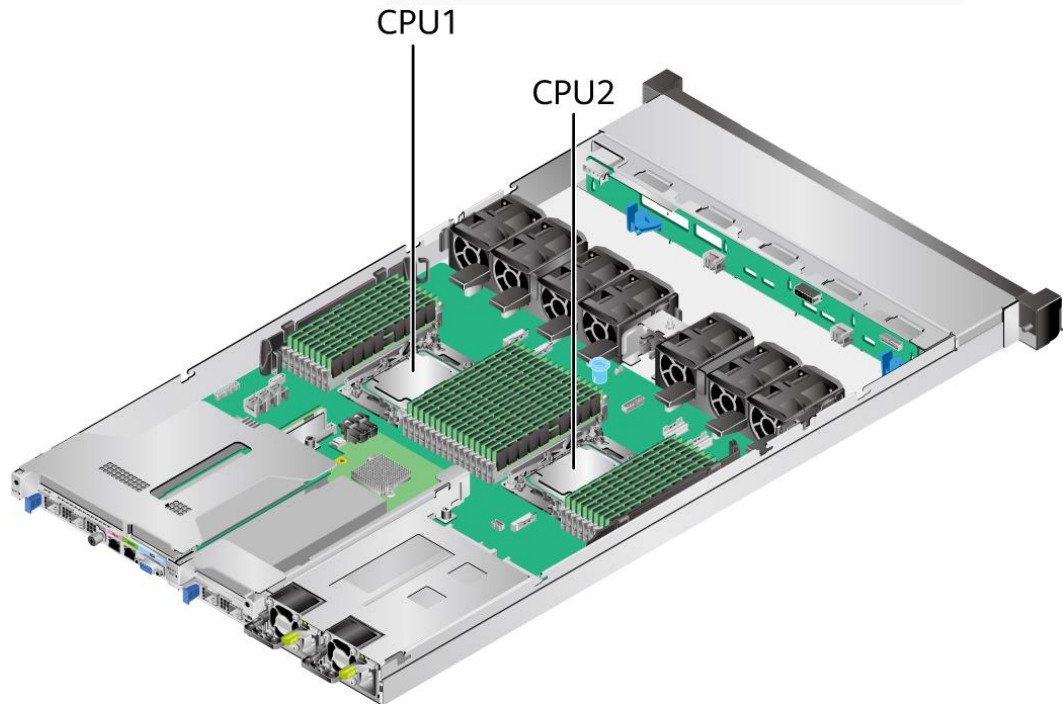
Table 2-4 Ports on the rear panel

Port	Type	Quantity	Description
Management network port	RJ45	1	iBMC management network port, which is used to manage the server. NOTE The management network port is a GE port that supports 100 Mbit/s and 1000 Mbit/s auto-negotiation.
Serial port	RJ45	1	Default operating system serial port used for debugging. You can also set it as the iBMC serial port by using the iBMC command. NOTE The port uses 3-wire serial communication interface, and the default baud rate is 115,200 bit/s.
VGA port	DB15	1	Used to connect a display terminal, such as a monitor or KVM.
USB port	USB 3.0	2	Used to connect to a USB 3.0 device. NOTICE <ul style="list-style-type: none"> • The maximum current is 1.3 A for an external USB device. • Before connecting an external USB device, ensure that the USB device functions properly. Otherwise, it may adversely impact the server. • The USB 3.0 port can be used to supply power to low-power peripherals. However, the USB 3.0 port must comply with the USB specifications. To run advanced peripherals, such as external CD/DVD drives, an external power supply is required.
PSU socket	-	2	Used to connect to a power distribution unit (PDU) through a power cable. You can select the PSUs as required. NOTE When determining the PSUs, ensure that the rated power of the PSUs is greater than that of the server.

2.3 Processors

- The server supports one or two processors.
- If only one processor is required, install it in socket CPU1.
- Processors of the same model must be used in a server.
- Contact your local sales representative or see "Search Parts" in the [Compatibility Checker](#) to determine the components to be used.

Figure 2-13 Processor positions



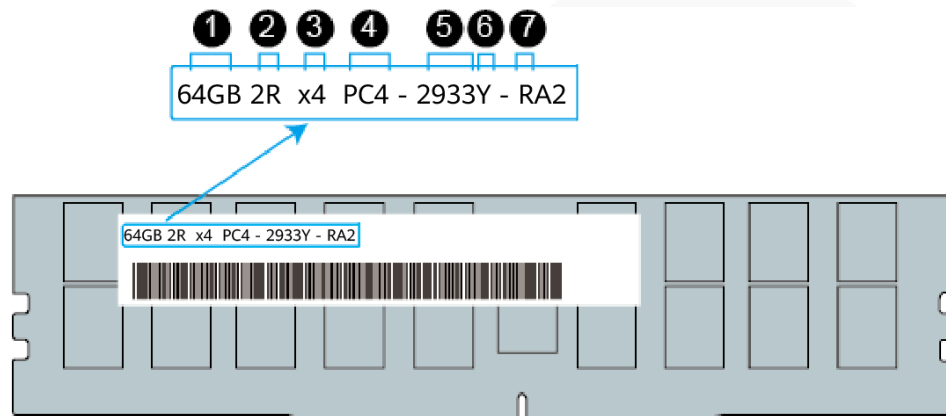
2.4 Memory

2.4.1 DDR4 Memory

2.4.1.1 Memory ID

You can determine the memory module properties based on the label attached to the memory module.

Figure 2-14 Memory identifier



No.	Description	Example
1	Capacity	<ul style="list-style-type: none"> • 16 GB • 32 GB • 64 GB • 128 GB • 256 GB
2	Number of ranks	<ul style="list-style-type: none"> • 1R: single-rank • 2R: dual-rank • 4R: quad-rank • 8R: octal-rank
3	Data width on the DRAM	<ul style="list-style-type: none"> • x4: 4-bit • x8: 8-bit
4	Type of the memory interface	<ul style="list-style-type: none"> • PC4: DDR4
5	Maximum memory speed	<ul style="list-style-type: none"> • 2933 MT/s • 3200 MT/s
6	Memory latency parameters (CL-tRCD-tRP)	<ul style="list-style-type: none"> • W = 20-20-20 • Y = 21-21-21 • AA = 22-22-22
7	DIMM type	<ul style="list-style-type: none"> • R = RDIMM • L = LRDIMM

2.4.1.2 Memory Subsystem Architecture

A server provides 32 memory slots. Each processor integrates eight memory channels.

Install the memory modules in the primary memory channels first. If the primary memory channel is not populated, the memory modules in secondary memory channels cannot be used.

Table 2-5 Memory channels

CPU	Channel	Memory Slot
CPU 1	A (primary)	DIMM000(A)
	A	DIMM001(I)
	B (primary)	DIMM010(B)
	B	DIMM011(J)
	C (primary)	DIMM020(C)
	C	DIMM021(K)
	D (primary)	DIMM030(D)
	D	DIMM031(L)
	E (primary)	DIMM040(E)
	E	DIMM041(M)
	F (primary)	DIMM050(F)
	F	DIMM051(N)
	G (primary)	DIMM060(G)
	G	DIMM061(O)
	H (primary)	DIMM070(H)
	H	DIMM071(P)
CPU2	A (primary)	DIMM100(A)
	A	DIMM101(I)
	B (primary)	DIMM110(B)
	B	DIMM111(J)
	C (primary)	DIMM120(C)
	C	DIMM121(K)
	D (primary)	DIMM130(D)
	D	DIMM131(L)
	E (primary)	DIMM140(E)
	E	DIMM141(M)
	F (primary)	DIMM150(F)
	F	DIMM151(N)
	G (primary)	DIMM160(G)
	G	DIMM161(O)

CPU	Channel	Memory Slot
	H (primary)	DIMM170(H)
	H	DIMM171(P)

2.4.1.3 Memory Compatibility

Observe the following rules when configuring DDR4 memory modules:

NOTICE

- A server must use DDR4 memory modules of the same part number (P/N code), and the memory speed is the minimum value of the following items:
 - Memory speed supported by a CPU
 - Maximum operating speed of a memory module
 - The DDR4 DIMMs of different types (RDIMM and LRDIMM) and specifications (capacity, bit width, rank, and height) cannot be used together.
- Contact your local sales representative or see "Search Parts" in the [Compatibility Checker](#) to determine the components to be used.

- The memory can be used with the third-generation Intel® Xeon® Scalable Ice Lake processors. The maximum memory capacity supported by all processor models is the same.
- For details about the capacity type of a single memory module, see "Search Parts" in the [Compatibility Checker](#).
- The maximum number of memory modules supported depends on the memory type and rank quantity.

NOTE

Each memory channel supports a maximum of 8 ranks. The number of memory modules supported by each channel varies depending on the number of ranks supported by each channel:

Number of memory modules supported by each channel ≤ Number of ranks supported by each memory channel / Number of ranks supported by each memory module

- A memory channel supports more than eight ranks for LRDIMMs.

NOTE

A quad-rank LRDIMM generates the same electrical load as a single-rank RDIMM on a memory bus.

Table 2-6 DDR4 memory specifications

Parameter	Specifications				
Capacity per DDR4 memory module (GB)	16	32	64	128	256
Type	RDIMM	RDIMM	RDIMM	LRDIMM	RDIMM
Rated speed (MT/s)	3200	3200	3200	3200	2933

Parameter		Specifications				
Operating voltage (V)		1.2	1.2	1.2	1.2	1.2
Maximum number of DDR4 DIMMs in a server ^a		32	32	32	32	32
Maximum DDR4 memory capacity of the server (GB)		512	1024	2048	4096	8192
Actual rate (MT/s)	1DPC ^b	3200	3200	3200	3200	2933
	2DPC	3200	3200	3200	3200	2933
<ul style="list-style-type: none"> • a: The maximum number of DDR4 memory modules is based on dual-processor configuration. The value is halved for a server with only one processor. • b: DPC (DIMM per channel) indicates the number of memory modules per channel. • The information listed in this table is for reference only. For details, consult the local sales representative. 						

2.4.1.4 DIMM Installation Rules

Observe the following when configuring DDR4 memory modules:

- Install memory modules only when corresponding processors are installed.
- Do not install LRDIMMs and RDIMMs in the same server.
- Install filler memory modules in vacant slots.

Observe the following when configuring DDR4 memory modules in specific operating mode:

- Rank sparing mode
 - Comply with the general installation guidelines.
 - At least two ranks must be configured for each channel.
 - A maximum of two standby ranks can be configured for each channel.
 - The capacity of a standby rank must be greater than or equal to that of other ranks in the same channel.
- Memory mirroring mode
 - Comply with the general installation guidelines.
 - Each processor supports four integrated memory controllers (IMCs), and each IMC has two channels for installing memory modules. The installed memory modules must be identical in size and organization.
 - For a multi-processor configuration, each processor must have a valid memory mirroring configuration.
- Memory scrubbing mode
 - Comply with the general installation guidelines.

2.4.1.5 Memory Installation Positions

A server supports a maximum of 32 DDR4 memory modules. To maximize performance, balance the total memory capacity between the installed processors and to load the channels similarly whenever possible.

Observe the memory module installation rules when configuring memory modules. For details, see [Memory Configuration Assistant](#).

NOTICE

At least one DDR4 memory module must be installed in the primary memory channels corresponding to CPU 1.

Figure 2-15 Memory slots

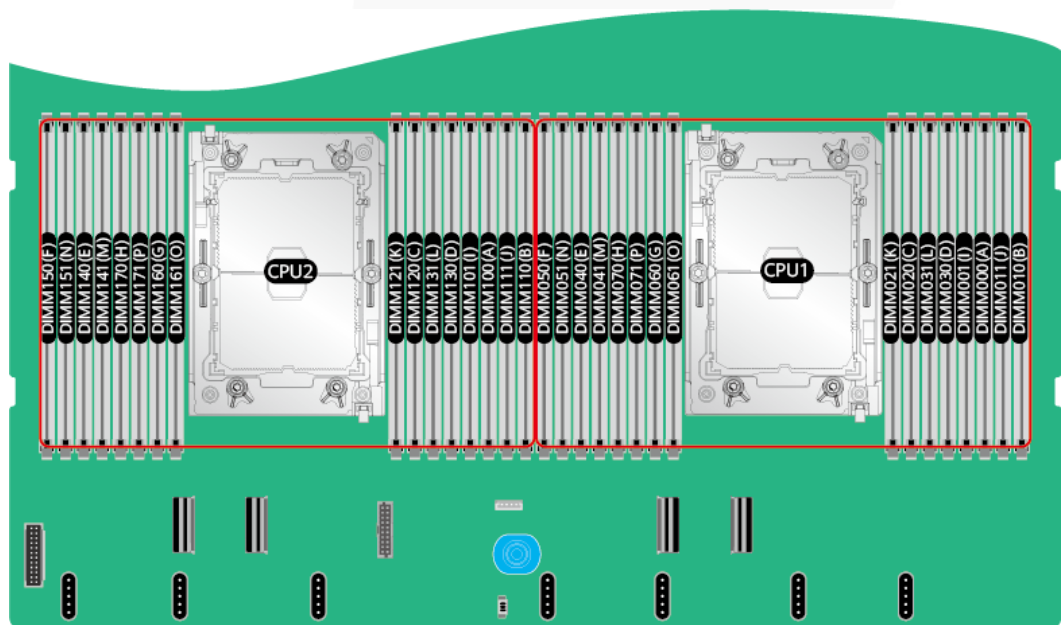


Figure 2-16 DDR4 memory module installation guidelines (1 processor)

CPU	Channel	DIMM Slot	Number of DIMMs (✓: recommended ○: not recommended)								
			✓	✓	✓	✓	✓	✓	○	✓	
			1	2	4	6	8	12	12	16	
CPU1	A	DIMM000(A)	●	●	●	●	●	●	●	●	●
		DIMM001(I)							●	●	●
	B	DIMM010(B)				●	●	●	●	●	●
		DIMM011(J)							●		●
	C	DIMM020(C)			●	●	●	●	●	●	●
		DIMM021(K)							●	●	●
	D	DIMM030(D)					●		●	●	●
		DIMM031(L)									●
	E	DIMM040(E)		●	●	●	●	●	●	●	●
		DIMM041(M)							●	●	●
	F	DIMM050(F)				●	●	●	●	●	●
		DIMM051(N)							●		●
	G	DIMM060(G)			●	●	●	●	●	●	●
		DIMM061(O)							●	●	●
	H	DIMM070(H)					●		●	●	●
		DIMM071(P)									●
Note	When 12 DIMMs are configured, the recommended installation (marked with ✓) achieves better performance than the installation that is not recommended (marked with ○). However, only the installation that is not recommended (marked with ○) supports SNC2, Hemi, SGX, and UMA X-skt.										

Figure 2-17 DDR4 memory module installation guidelines (2 processors)

CPU	Channel	DIMM Slot	Number of DIMMs								
			(✓: recommended ○: not recommended)								
			✓	✓	✓	✓	✓	✓	○	✓	
			2	4	8	12	16	24	24	32	
CPU1	A	DIMM000(A)	●	●	●	●	●	●	●	●	●
		DIMM001(I)							●	●	●
	B	DIMM010(B)				●	●	●	●	●	●
		DIMM011(J)							●		●
	C	DIMM020(C)			●	●	●	●	●	●	●
		DIMM021(K)							●	●	●
	D	DIMM030(D)					●		●	●	●
		DIMM031(L)									●
	E	DIMM040(E)		●	●	●	●	●	●	●	●
		DIMM041(M)							●	●	●
	F	DIMM050(F)				●	●	●	●	●	●
		DIMM051(N)							●		●
	G	DIMM060(G)			●	●	●	●	●	●	●
		DIMM061(O)							●	●	●
	H	DIMM070(H)					●		●	●	●
		DIMM071(P)									●
CPU2	A	DIMM100(A)	●	●	●	●	●	●	●	●	●
		DIMM101(I)							●	●	●
	B	DIMM110(B)				●	●	●	●	●	●
		DIMM111(J)							●		●
	C	DIMM120(C)			●	●	●	●	●	●	●
		DIMM121(K)							●	●	●
	D	DIMM130(D)					●		●	●	●
		DIMM131(L)									●
	E	DIMM140(E)		●	●	●	●	●	●	●	●
		DIMM141(M)							●	●	●
	F	DIMM150(F)				●	●	●	●	●	●
		DIMM151(N)							●		●
	G	DIMM160(G)			●	●	●	●	●	●	●
		DIMM161(O)							●	●	●
	H	DIMM170(H)					●		●	●	●
		DIMM171(P)									●
Note	When 24 DIMMs are configured, the recommended installation (marked with ✓) achieves better performance than the installation that is not recommended (marked with ○). However, only the installation that is not recommended (marked with ○) supports SNC2, Hemi, SGX, and UMA X-skt.										

2.4.1.6 Memory Protection Technologies

The following memory protection technologies are supported:

- ECC
- Memory Mirroring
- Memory Single Device Data Correction (SDDC, +1)
- Failed DIMM Isolation
- Memory Thermal Throttling
- Command/Address Parity Check and Retry
- Memory Demand/Patrol Scrubbing
- Memory Data Scrambling
- Memory Multi Rank Sparing
- Post Package Repair (PPR)
- Write Data CRC Protection
- Adaptive Data Correction - Single Region (ADC-SR)
- Adaptive Double Device Data Correction - Multiple Region (ADDDC-MR, +1)

2.5 Storage

2.5.1 Drive Configurations

Table 2-7 Drive configuration

Configuration	Front Drive	Rear Drive	Drive Management Mode
4 x 3.5" drive pass-through configuration 1	<ul style="list-style-type: none"> • Front drive: 4 x 3.5 <ul style="list-style-type: none"> – Slots 0 to 3 support only SATA drives. 	-	<ul style="list-style-type: none"> • PCH
4 x 3.5" drive pass-through configuration 2	<ul style="list-style-type: none"> • Front drive: 4 x 3.5 <ul style="list-style-type: none"> – Slots 0 to 3 support only SAS/SATA drives. 	<ul style="list-style-type: none"> • I/O module 1: 2 x 2.5" <ul style="list-style-type: none"> – Slots 12 and 13 support only SAS/SATA drives. 	<ul style="list-style-type: none"> • 1 x screw-in RAID controller card
4 x 3.5" drive pass-through configuration 3	<ul style="list-style-type: none"> • Front drive: 4 x 3.5 <ul style="list-style-type: none"> – Slots 0 to 3 support only 	-	<ul style="list-style-type: none"> • 1 x PCIe RAID controller card

Configuration	Front Drive	Rear Drive	Drive Management Mode
	SAS/SATA drives.		
8 x 2.5" drive pass-through configuration 1	<ul style="list-style-type: none"> • Front drive: 8 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 7 support only SATA drives. 	-	<ul style="list-style-type: none"> • PCH
8 x 2.5" drive pass-through configuration 2	<ul style="list-style-type: none"> • Front drive: 8 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 7 support only SAS/SATA drives. 	-	<ul style="list-style-type: none"> • 1 x screw-in RAID controller card
8 x 2.5" drive pass-through configuration 3	<ul style="list-style-type: none"> • Front drive: 8 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 7 support only SAS/SATA drives. 	-	<ul style="list-style-type: none"> • 1 x PCIe RAID controller card
10 x 2.5" drive pass-through configuration 1	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 9 support only SAS/SATA drives. 	<ul style="list-style-type: none"> • I/O module 1: 2 x 2.5" <ul style="list-style-type: none"> – Slots 12 and 13 support only SAS/SATA drives. 	<ul style="list-style-type: none"> • 1 x screw-in RAID controller card
10 x 2.5" drive pass-through configuration 2	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 9 support only SAS/SATA drives. 	-	<ul style="list-style-type: none"> • 1 x PCIe RAID controller card
10 x 2.5" drive pass-through configuration 3	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 5 support only SATA drives. – Slots 6 and 7 support only SATA/NVMe drives. – Slots 8 to 9 support only NVMe 	-	<ul style="list-style-type: none"> • SATA drive: PCH • NVMe drive: CPU

Configuration	Front Drive	Rear Drive	Drive Management Mode
	drives.		
10 x 2.5" drive pass-through configuration 4	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 5 support only SAS/SATA drives. – Slots 6 and 7 support SAS/SATA/NVMe drives. – Slots 8 and 9 support only NVMe drives. 	-	<ul style="list-style-type: none"> • SAS/SATA drive: 1 x screw-in RAID controller card • NVMe drive: CPU
10 x 2.5" drive pass-through configuration 5	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 5 support only SAS/SATA drives. – Slots 6 and 7 support SAS/SATA/NVMe drives. – Slots 8 and 9 support only NVMe drives. 	-	<ul style="list-style-type: none"> • SAS/SATA drive: 1 x PCIe RAID controller card • NVMe drive: CPU
10 x 2.5" drive NVMe configuration 1	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 3 support only SATA/NVMe drives. – Slots 4 to 9 support only NVMe drives. 	-	<ul style="list-style-type: none"> • SATA drive: PCH • NVMe drive: CPU
10 x 2.5" drive NVMe configuration 2	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 3 support SAS/SATA/NVMe drives. 	<ul style="list-style-type: none"> • I/O module 1: 2 x 2.5" <ul style="list-style-type: none"> – Slots 12 and 13 support only SAS/SATA 	<ul style="list-style-type: none"> • SAS/SATA drive: 1 x screw-in RAID controller card • NVMe drive: CPU

Configuration	Front Drive	Rear Drive	Drive Management Mode
	<ul style="list-style-type: none"> – Slots 4 to 9 support only NVMe drives. 	drives.	
10 x 2.5" drive NVMe configuration 3	<ul style="list-style-type: none"> • Front drive: 10 x 2.5" <ul style="list-style-type: none"> – Slots 0 to 3 support SAS/SATA/NVMe drives. – Slots 4 to 9 support only NVMe drives. 	<ul style="list-style-type: none"> • I/O module 1: 2 x 2.5" <ul style="list-style-type: none"> – Slots 12 and 13 support only SAS/SATA drives. 	<ul style="list-style-type: none"> • SAS/SATA drive: 1 x PCIe RAID controller card • NVMe drive: CPU
Note: For details about component options, consult the local sales representatives.			

2.5.2 Drive Numbering

NOTICE

The drive numbers identified by the RAID controller card vary depending on the cabling of the RAID controller card. The drive numbers identified by the RAID controller card in this section are provided based on the default cabling described in "Internal Cabling"

- 4 x 3.5" drive pass-through configuration
Corresponds to 4 x 3.5" drive pass-through configuration 1 in 2.5.1 Drive Configurations .

Figure 2-18 Slot Numbers



Table 2-8 Slot numbers

Drive No.	Drive Number Identified by the iBMC
0	0
1	1
2	2

Drive No.	Drive Number Identified by the iBMC
3	3

- 4 x 3.5" drive pass-through configuration
 Corresponds to 4 x 3.5" drive pass-through configuration 2 in 2.5.1 Drive Configurations .

Figure 2-19 Slot Numbers

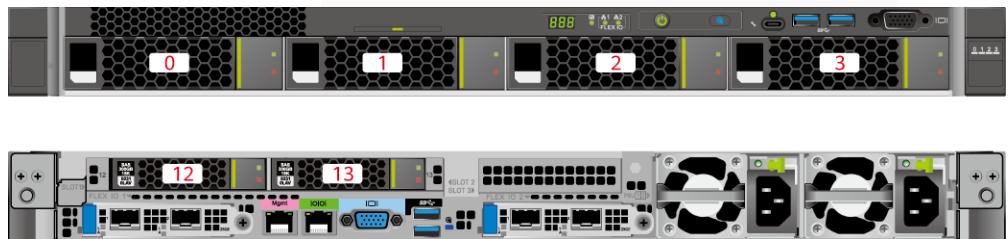


Table 2-9 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0
1	1	1
2	2	2
3	3	3
12	12	4
13	13	5

- 4 x 3.5" drive pass-through configuration
 Corresponds to 4 x 3.5" drive pass-through configuration 3 in 2.5.1 Drive Configurations .

Figure 2-20 Slot Numbers



Table 2-10 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
-----------	-------------------------------------	--

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0
1	1	1
2	2	2
3	3	3

- 8 x 2.5" drive pass-through configuration
Corresponds to 8 x 2.5" drive pass-through configuration 1 in 2.5.1 Drive Configurations .

Figure 2-21 Slot numbers



Table 2-11 Slot numbers

Drive No.	Drive Number Identified by the iBMC
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

- 8 x 2.5" drive pass-through configuration
Corresponds to 8 x 2.5" drive pass-through configuration 2 and 8 x 2.5" drive pass-through configuration 3 in 2.5.1 Drive Configurations .

Figure 2-22 Slot Numbers



Table 2-12 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

- 10 x 2.5" drive pass-through configuration
Corresponds to 10 x 2.5" drive pass-through configuration 1 in 2.5.1 Drive Configurations .

Figure 2-23 Slot numbers

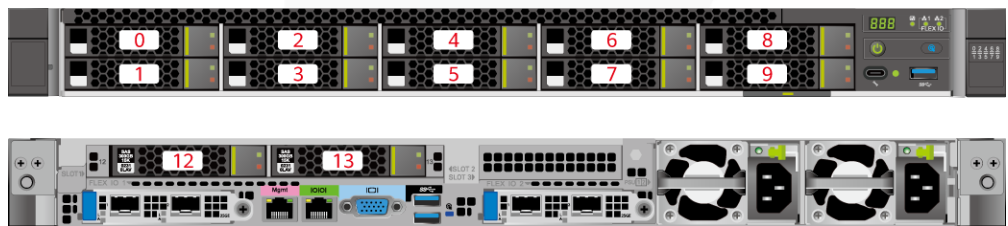


Table 2-13 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
8	8	8
9	9	9
12	12	12
13	13	13

- 10 x 2.5" drive pass-through configuration
Corresponds to 10 x 2.5" drive pass-through configuration 2 in 2.5.1 Drive Configurations .

Figure 2-24 Slot numbers



Table 2-14 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9

- 10 x 2.5" drive pass-through configuration
Corresponds to 10 x 2.5" drive pass-through configuration 3 in 2.5.1 Drive Configurations .

Figure 2-25 Slot Numbers



Table 2-15 Slot numbers

Drive No.	Drive Number Identified by the iBMC
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

- 10 x 2.5" drive pass-through configuration
Corresponds to 10 x 2.5" drive pass-through configuration 4 and 10 x 2.5" drive pass-through configuration 5 in 2.5.1 Drive Configurations .

Figure 2-26 Slot Numbers



Table 2-16 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
5	5	5
6	6	6 ^{Note}
7	7	7 ^{Note}
8	8	-
9	9	-

Note: If the slot is configured with a SAS/SATA drive, the RAID controller card can manage the drive and allocate a number to the drive.

- 10 x 2.5" NVMe drive configuration
 Corresponds to 10 x 2.5" drive NVMe configuration 1 in 2.5.1 Drive Configurations .

Figure 2-27 Slot Numbers



Table 2-17 Slot numbers

Drive No.	Drive Number Identified by the iBMC
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

- 10 x 2.5" NVMe drive configuration
 Corresponds to 10 x 2.5" NVMe drive configuration 2 and 10 x 2.5" NVMe drive configuration 3 in 2.5.1 Drive Configurations .

Figure 2-28 Slot Numbers

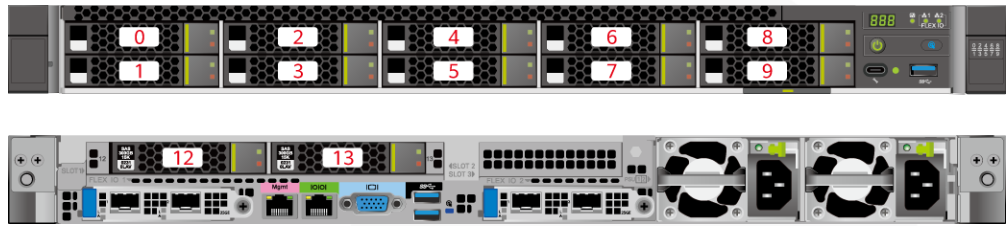


Table 2-18 Slot numbers

Drive No.	Drive Number Identified by the iBMC	Drive Number Identified by the RAID Controller
0	0	0 ^{Note}
1	1	1 ^{Note}
2	2	2 ^{Note}
3	3	3 ^{Note}
4	4	-
5	5	-
6	6	-
7	7	-
8	8	-
9	9	-
12	12	4
13	13	5

Note: If the slot is configured with a SAS/SATA drive, the RAID controller card can manage the drive and allocate a number to the drive.

2.5.3 Drive Indicators

SAS/SATA Drive Indicators

Figure 2-29 SAS/SATA drive indicators

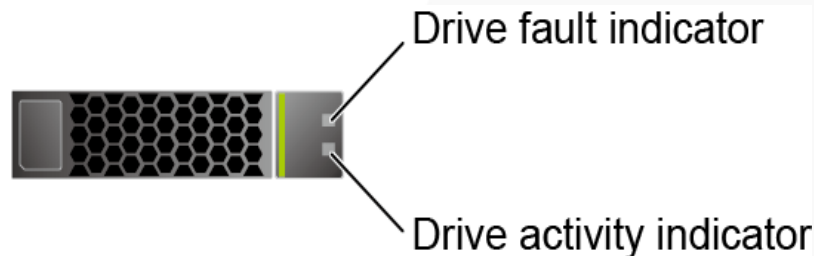
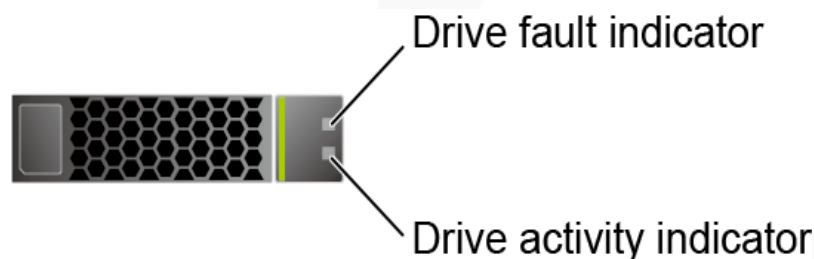


Table 2-19 SAS/SATA drive indicators

Activity Indicator (Green)	Fault Indicator (Yellow)	Description
Off	Off	The drive is not in position.
Steady on	Off	The drive is detected.
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.
Blinking at 1 Hz	Blinking at 1 Hz	Data on the secondary drive is being rebuilt.
Off	Steady on	A drive in a RAID array is removed.
Steady on	Steady on	The drive is faulty.

NVMe Drive Indicators

Figure 2-30 NVMe drive indicators



- If the VMD function is enabled and the latest VMD driver is installed, the NVMe drives support surprise hot swap.

Table 2-20 NVMe drive indicators (VMD enabled)

Activity Indicator (Green)	Fault Indicator (Yellow)	Description
Off	Off	The NVMe drive is not detected.
Steady on	Off	The NVMe drive is detected and operating properly.
Blinking at 2 Hz	Off	Data is being read from or written to the NVMe drive.
Off	Blinking at 2 Hz	The NVMe drive is being located.
Off	Blinking at 8 Hz	The data on the secondary NVMe drive is being rebuilt.
Steady on/Off	Steady on	The NVMe drive is faulty.

- If the VMD function is disabled, NVMe drives support only orderly hot swap.

Table 2-21 NVMe drive indicators (VMD disabled)

Activity Indicator (Green)	Fault Indicator (Yellow)	Description
Off	Off	The NVMe drive is not detected.
Steady on	Off	The NVMe drive is detected and operating properly.
Blinking at 2 Hz	Off	Data is being read from or written to the NVMe drive.
Off	Blinking at 2 Hz	The NVMe drive is being located or hot-swapped.
Off	Blinking at 0.5 Hz	The NVMe drive has completed the hot swap process and is removable.
Steady on/Off	Steady on	The NVMe drive is faulty.

M.2 FRU Indicators

The server supports the Avago SAS3004iMR RAID controller card, which supports two M.2 FRUs.

Figure 2-31 M.2 FRU indicators

M.2 FRU fault indicator M.2 FRU activity indicator

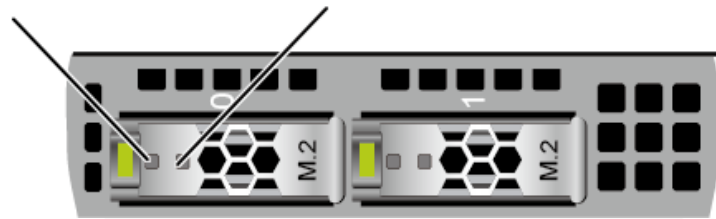


Table 2-22 M.2 FRU indicators

M.2 FRU Active Indicator (Green)	M.2 FRU Fault Indicator (Yellow)	Description
Off	Off	The M.2 FRU is not detected.
Steady on	Off	The M.2 FRU is inactive.
Blink	Off	The M.2 FRU is in the read/write or synchronization state.
Steady on	Blink	The M.2 FRU is being located.
Blink	Blink	The RAID array is being rebuilt.
Off	Steady on	The M.2 FRU cannot be detected or is faulty.
Steady on	Steady on	The M.2 FRU RAID status is abnormal.

2.5.4 RAID Controller Card

The RAID controller card supports RAID configuration, RAID level migration, and drive roaming.

- Contact your local sales representative or see "Search Parts" in the [Compatibility Checker](#) to determine the components to be used.
- For details about the RAID controller card, see *V6 Server RAID Controller Card User Guide*.

2.6 Network

2.6.1 OCP 3.0 Network Adapter

OCP 3.0 network adapters provide network expansion capabilities.

- The FlexIO slot supports the OCP 3.0 network adapter, which can be configured as required.

- Contact your local sales representative or see "Search Parts" in the [Compatibility Checker](#) to determine the components to be used.
- For details about the OCP 3.0 network adapter, see the documents of each OCP 3.0 network adapter.

2.7 I/O Expansion

2.7.1 PCIe Cards

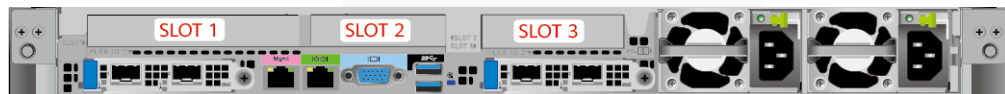
PCIe cards provide ease of expandability and connection.

- A maximum of three PCIe 4.0 slots are supported.
- Contact your local sales representative or see "Search Parts" in the [Compatibility Checker](#) to determine the components to be used.
- When IB cards are used to build an IB network, ensure that the IPoIB modes of the IB cards at both ends of the network are the same. For details, contact technical support.

2.7.2 PCIe Slots

PCIe Slots

Figure 2-32 PCIe slots

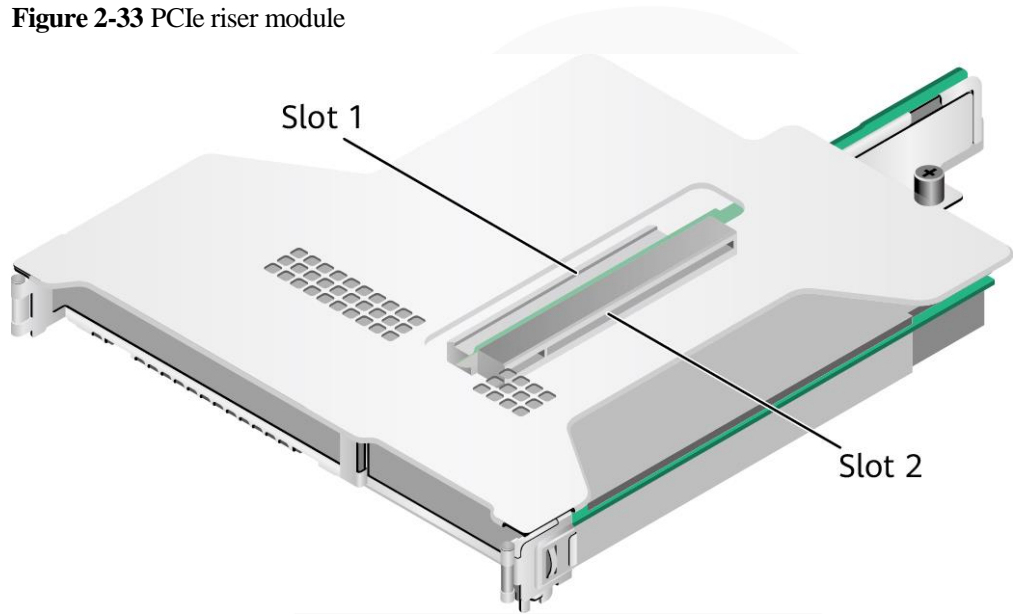


- I/O module 1 provides slots 1 and 2.
- I/O module 2 provides slot 3.

PCIe Riser Modules

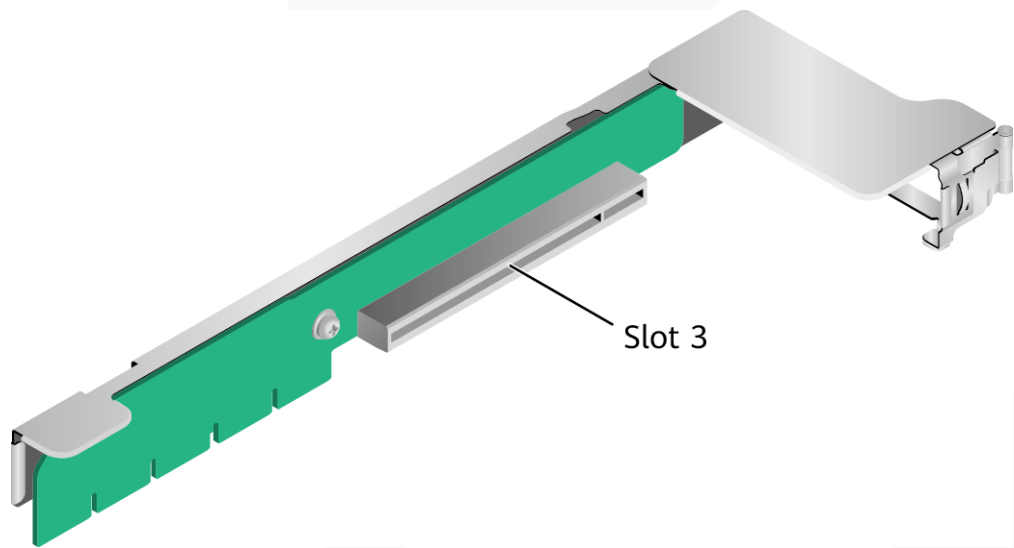
- PCIe riser module 1
Provides PCIe slots 1 and 2 in I/O module 1.

Figure 2-33 PCIe riser module



- PCIe riser module 2
Provides PCIe slot 3 in I/O module 2.

Figure 2-34 PCIe riser module



2.7.3 PCIe Slot Description

NOTE

The PCIe slots mapping to a vacant CPU socket are unavailable.

Table 2-23 PCIe slot description

PCIe Slot	CPU	PCIe Standards	Connector Width	Bus Width	Port No.	Root Port (B/D/F)	Device (B/D/F)	Slot Size
Screw-in RAID controller card	CPU1	PCIe 3.0	x8	x8	Port0A	16/02/0	17/00/0	-
FlexIO card 1	CPU1	PCIe 4.0	x16	x8 Expansion cables used by the mainboard: x8 + x8 ^a	Port0C	16/04/0	18/00/0	OCP 3.0 specifications
FlexIO card 2	CPU2	PCIe 4.0	x16	x8 Expansion cable used by the mainboard: x16	Port2A	C9/02/0	CA/00/0	OCP 3.0 specifications
Slot1	CPU1	PCIe 4.0	x16	x16	Port1A	30/02/0	31/00/0	FHHL
Slot2	CPU1	PCIe 4.0	x16	x16	Port2A	4A/02/0	4B/00/0	HHHL
Slot3	CPU2	PCIe 4.0	x16	x16	Port0A	97/02/0	98/00/0	HHHL

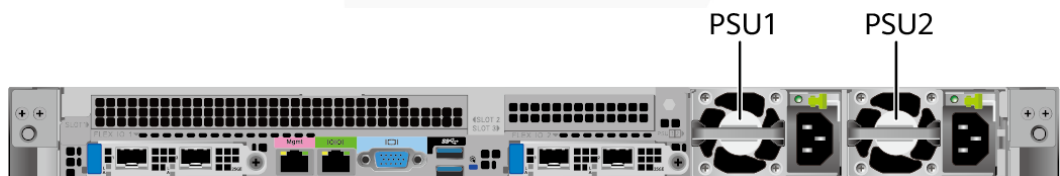
- a: When CPU1 and CPU2 use x8 signals, the socket-direct function is supported.
- The B/D/F (Bus/Device/Function Number) is the default value when the server is fully configured with PCIe cards. The value may differ if the server is not fully configured with PCIe cards or if a PCIe card with a PCI bridge is configured.
- Root Port (B/D/F) indicates the B/D/F of an internal PCIe root port of the processor.
- Device (B/D/F) indicates the B/D/F (bus address displayed on the OS) of an onboard or extended PCIe device.
- The PCIe x16 slots are compatible with PCIe x16, PCIe x8, PCIe x4, and PCIe x1 cards. The PCIe cards are not forward compatible. That is, the PCIe slot width cannot be smaller than the PCIe card link width.
- The full-height half-length (FHHL) PCIe slots are compatible with FHHL PCIe cards and half-height half-length (HHHL) PCIe cards.

PCIe Slot	CPU	PCIe Standards	Connector Width	Bus Width	Port No.	Root Port (B/D/F)	Device (B/D/F)	Slot Size
<ul style="list-style-type: none"> The maximum power supply of each PCIe slot is 75 W. 								

2.8 PSUs

- The server supports one or two PSUs.
- The server supports AC or DC PSUs.
- The PSUs are hot-swappable.
- The server supports two PSUs in 1+1 redundancy.
- PSUs of the same part number (P/N code) must be used in a server.
- The PSUs are protected against short circuit. Double-pole fuse is provided for the PSUs with dual input live wires.
- If the DC power supply is used, purchase the DC power supply that meets the requirements of the safety standards or the DC power supply that has passed the CCC certification.
- Contact your local sales representative or see "Search Parts" in the [Compatibility Checker](#) to determine the components to be used.

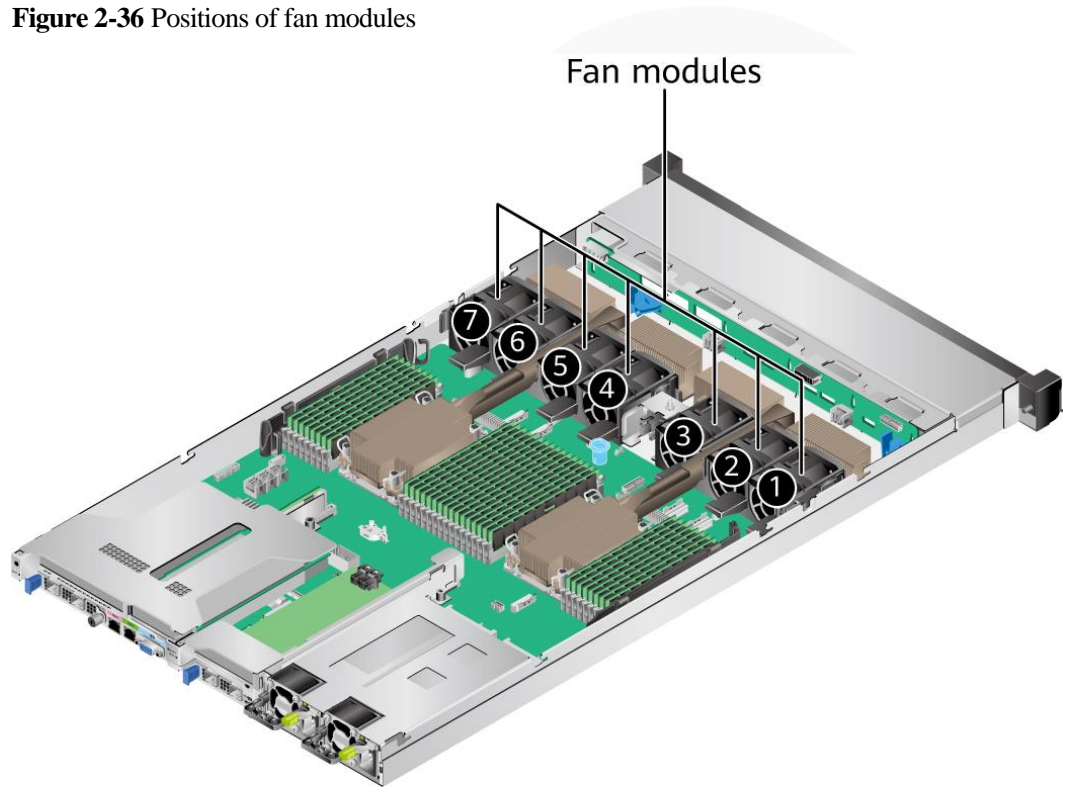
Figure 2-35 Positions of PSUs



2.9 Fan Modules

- The server supports seven fan modules.
- The fan modules are hot-swappable.
- N+1 redundancy is supported. That is, the server can work properly when a single fan fails.
- The fan speed can be adjusted.
- Fan modules of the same part number (P/N code) must be used in a server.

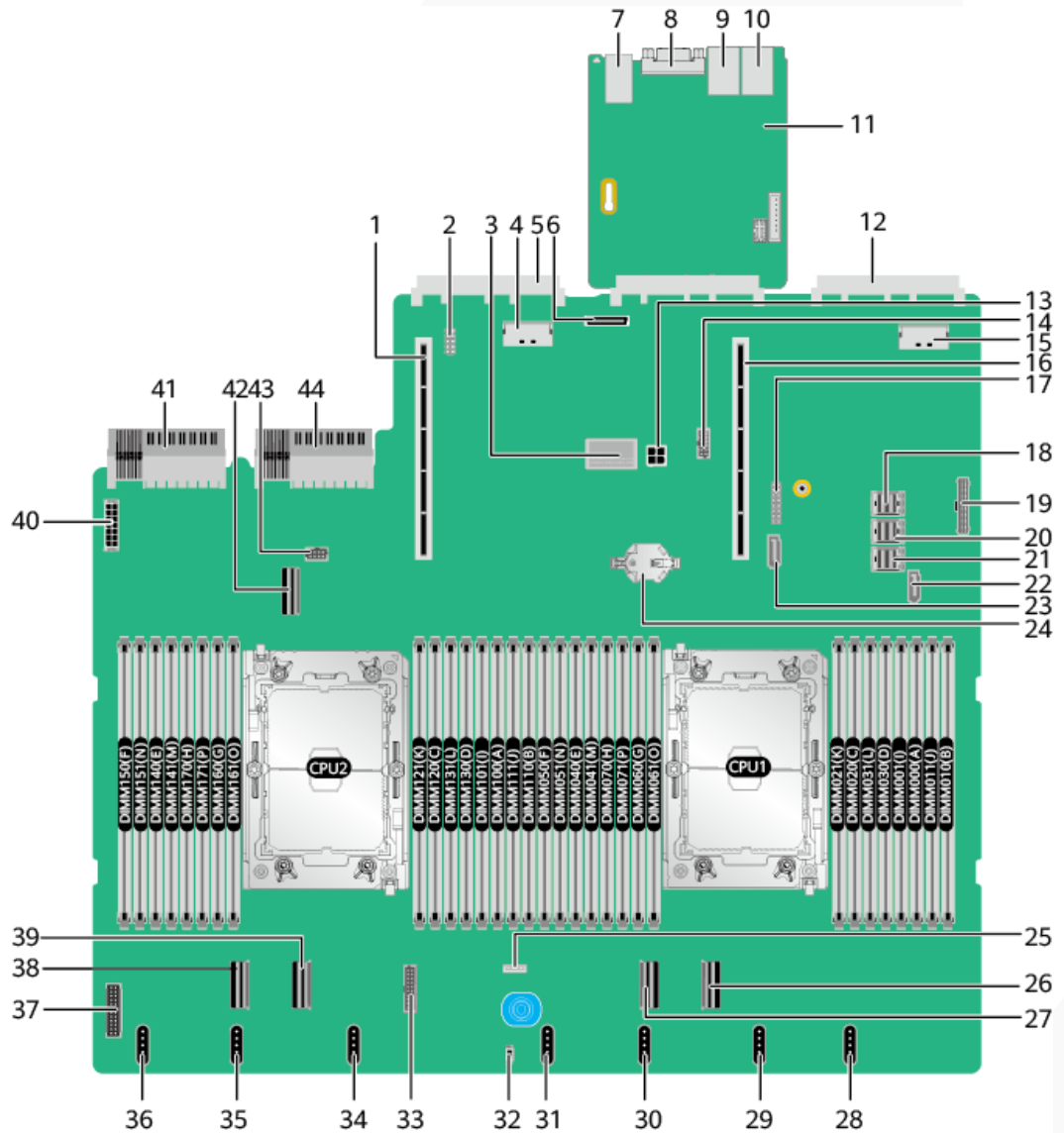
Figure 2-36 Positions of fan modules



2.10 Boards

2.10.1 Mainboard

Figure 2-37 1288H V6 mainboard



1	PCIe riser 2 slot (PCIE RISER2/J51)	2	Debugging pin (J103)
3	Screw-in RAID controller card connector (RAID CARD/J86)	4	LP slimline 7 connector for OCP 3.0 network adapter 2 (SLIMLINE7/J31)
5	OCP 3.0 network adapter 2 connector (OCP2 CONN/J109)	6	Built-in storage expansion port (SD CARD/J87)

7	2 x USB 3.0 ports (USB3.0 CONN/J88)	8	Rear VGA port (VGA CONN/J60)
9	Serial port (COM/J6020)	10	BMC management network port (BMC_GE /J6019)
11	BMC management board	12	OCP 3.0 network adapter 1 connector (OCP1 CONN/J108)
13	Rear 4-pin power connector 2 (REAR BP PWR2/J21)	14	NC-SI connector (NCSI CONN/J114)
15	LP slimline 6 connector for OCP 3.0 network adapter 1 (SLIMLINE6/J13)	16	PCIe riser 1 slot (PCIE RISER1/J50)
17	TPM/TCM connector (J10)	18	Mini-SAS HD connector C (MiniHD PORTC/J4)
19	Right mounting ear connector (RCIA BOARD/J113)	20	Mini-SAS HD connector B (MiniHD PORTB/J5)
21	Mini-SAS HD connector A (MiniHD PORTA/J6)	22	SATA 9-pin connector 1 (SATA1/J1)
23	SATA 9-pin connector 2 (SATA2/J2)	24	Cell battery holder (U9)
25	VROC key connector (Soft RAID KEY/J3) ^a	26	LP slimline 1 connector (SLIMLINE1/J11)
27	LP slimline 2 connector (SLIMLINE2/J84)	28	Fan module 7 connector (1U FAN7/J99)
29	Fan module 6 connector (1U FAN6/J98)	30	Fan module 5 connector (1U FAN5/J96)
31	Fan module 4 connector (1U FAN4/J94)	32	Intrusion sensor connector (INTRUDER CONN/S1)
33	Front low-speed signal connector (FRONT HDD BP/J75)	34	Fan module 3 connector (1U FAN3/J92)
35	Fan module 2 connector (1U FAN2/J101)	36	Fan module 1 connector (1U FAN1/J67)
37	Left mounting ear connector (LCIA BOARD/J106)	38	LP slimline 4 connector (SLIMLINE4/J12)
39	LP slimline 3 connector (SLIMLINE3/J85)	40	Front 14-pin power connector 1 (HDD BP PWR1/J26)
41	PSU 2 connector (PSU2/J56)	42	LP slimline 5 connector (SLIMLINE5/J30)
43	Built-in low-speed signal connector (INNER HDD	44	PSU 1 connector (PSU1/J28)

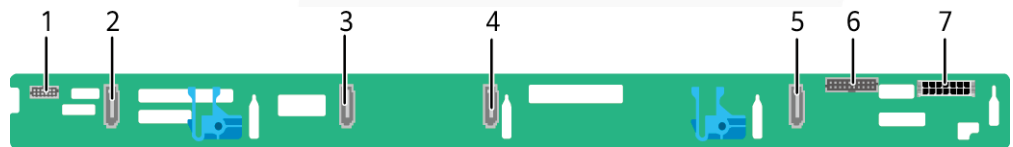
	BP/J27)		
a: Reserved and unavailable currently.			

2.10.2 Drive Backplane

Front Drive Backplane

- 4 x 3.5" drive pass-through backplane
Configure this backplane in 4 x 3.5" drive pass-through configuration 1, 4 x 3.5" drive pass-through configuration 2, and 4 x 3.5" drive pass-through configuration 3 in 2.5.1 Drive Configurations .

Figure 2-38 4 x 3.5" drive pass-through backplane



1	Backplane indicator signal cable connector (SGPIO/J6)	2	SAS3 signal connector (PORT3/J5)
3	SAS2 signal connector (PORT2/J4)	4	SAS1 signal connector (PORT1/J3)
5	SAS0 signal connector (PORT0/J2)	6	Backplane signal cable connector (HDD_BP/J1)
7	Backplane power connector (HDD POWER/J24)	-	-

- 8 x 2.5" drive pass-through backplane
Configure this backplane in 8 x 2.5" drive pass-through configuration 1, 8 x 2.5" drive pass-through configuration 2, and 8 x 2.5" drive pass-through configuration 3 in 2.5.1 Drive Configurations .

Figure 2-39 8 x 2.5" drive pass-through backplane

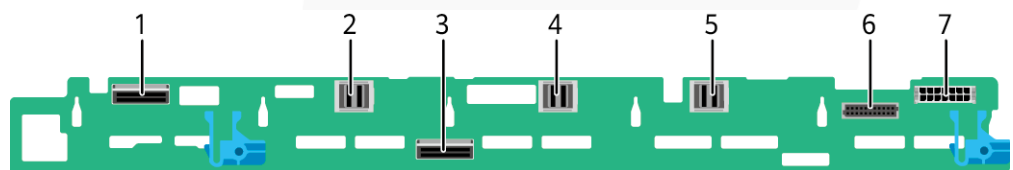


1	Built-in DVD drive connector (DVD_POWER/J11)	2	Mini-SAS HD connector (PORT B/J29)
---	--	---	------------------------------------

3	Backplane power connector (HDD POWER/J24)	4	Mini-SAS HD connector (PORT A/J28)
5	Backplane signal cable connector (HDD_BP/J1)	-	-

- 10 x 2.5" drive pass-through backplane
Configure this backplane in 10 x 2.5" drive pass-through configuration 1, 10 x 2.5" drive pass-through configuration 2, 10 x 2.5" drive pass-through configuration 3, 10 x 2.5" drive pass-through configuration 4, and 10 x 2.5" drive pass-through configuration 5 in 2.5.1 Drive Configurations .

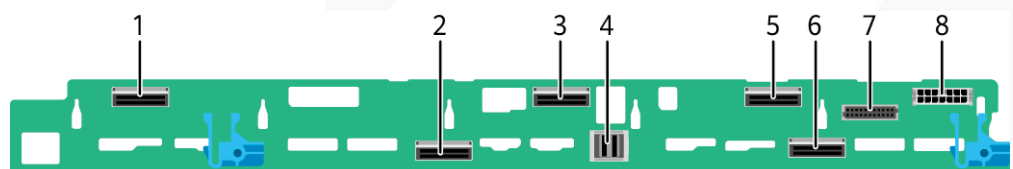
Figure 2-40 10 x 2.5" drive pass-through backplane



1	LP slimline 2 connector (SLIM A/SLIM2/J12)	2	Mini-SAS HD connector (PORT C/J15)
3	LP slimline 1 connector (SLIM B/SLIM1/J11)	4	Mini-SAS HD connector (PORT B/J14)
5	Mini-SAS HD connector (PORT A/J13)	6	Backplane signal cable connector (HDD BP/J1)
7	Backplane power connector (HDD POWER/J24)	-	-

- 10 x 2.5" drive NVMe backplane
Configure this backplane in 10 x 2.5" NVMe drive configuration 1, 10 x 2.5" NVMe drive configuration 2, and 10 x 2.5" NVMe drive configuration 3 in 2.5.1 Drive Configurations .

Figure 2-41 10 x 2.5" drive NVMe backplane



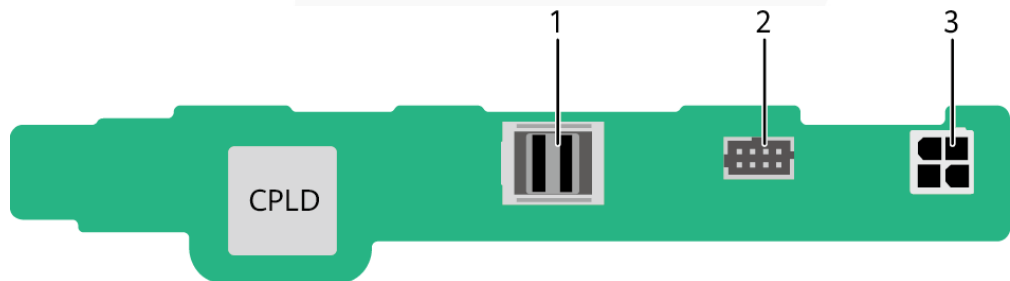
1	LP slimline 2 connector (SLIM A/ SLIM_2/ SLIM_5/J3)	2	LP slimline 1 connector (SLIM B/ SLIM_1/PORT_2B/J2)
---	---	---	---

3	LP slimline 4 connector (SLIM C/SLIM_4/PORT_2A/J5)	4	Mini-SAS HD connector (PORT A/J6)
5	LP slimline 3 connector (SLIM D/SLIM_3/PORT_1B/J4)	6	LP slimline 5 connector (SLIM E/SLIM_5/PORT_1A/J17)
7	Backplane low-speed signal connector (HDD BP/J1)	8	Backplane power connector (HDD POWER/J30)

Rear-drive backplane

- 2 x 2.5" drive backplane

Figure 2-42 2 x 2.5" drive backplane



1	Mini-SAS HD connector (PORT/J3)	2	Low-speed signal connector (HDD_BP/J1)
3	Power connector (HDD_POWER/J2)	-	-

3 Product Specifications

- 3.1 Technical Specifications
- 3.2 Environmental Specifications
- 3.3 Physical Specifications

3.1 Technical Specifications

Table 3-1 Technical specifications

Component	Specifications
Form factor	1U rack server
Chipset	Intel® C621A
Processor	<p>Supports one or two processors.</p> <ul style="list-style-type: none"> • Third-generation Intel® Xeon® Scalable Ice Lake processors • Built-in memory controller and eight memory channels per processor • Built-in PCIe controller, supporting PCIe 4.0 and 64 lanes per processor • Three UPI buses between processors, providing up to 11.2 GT/s transmission per channel • Up to 40 cores • Max. 3.6 GHz • Min. 1.5 MB L3 cache per core • Max. 270 W TDP <p>NOTE The preceding information is for reference only. For details, see "Search Parts" in the Compatibility Checker.</p>
DIMM	<p>Supports 32 memory module slots.</p> <ul style="list-style-type: none"> • Up to 32 DDR4 memory modules

Component	Specifications
	<ul style="list-style-type: none"> - RDIMM and LRDIMM support - Max. 3200 MT/s memory speed - The DDR4 memory modules of different types (RDIMM and LRDIMM) and specifications (capacity, bit width, rank, and height) cannot be used together. - A server must use DDR4 memory modules of the same part number (P/N code). <p>NOTE The preceding information is for reference only. For details, see "Search Parts" in the Compatibility Checker.</p>
Storage	<p>Supports a variety of drive configurations. For details, see 2.5.1 Drive Configurations .</p> <ul style="list-style-type: none"> • Supports two M.2 SSDs. <ul style="list-style-type: none"> - M.2 SSDs are supported for RAID configuration when the server is configured with an Avago SAS3004iMR RAID controller card. <p>NOTE</p> <ul style="list-style-type: none"> • The M.2 SSD is used only as a boot device for installing the OS. Small-capacity (32 GB or 64 GB) M.2 SSDs do not support logging due to poor endurance. If a small-capacity M.2 SSD is used as the boot device, a dedicated log drive or log server is required for logging. For example, you can dump VMware logs in either of the following ways: <ul style="list-style-type: none"> • Redirect /scratch. For details, see https://kb.vmware.com/s/article/1033696. • Configure syslog. For details, see https://kb.vmware.com/s/article/2003322. • The M.2 SSD cannot be used to store data due to poor endurance. In write-intensive applications, the M.2 SSD will wear out in a short time. If you want to use SSDs or HDDs as data storage devices, use enterprise-level SSDs or HDDs with high DDPD. • The M.2 SSD is not recommended for write-intensive service software due to poor endurance. • Do not use M.2 SSDs for cache. <ul style="list-style-type: none"> • Supports hot swap of SAS/SATA/NVMe drives. <p>NOTE The NVMe drives support:</p> <ul style="list-style-type: none"> • Before using the VMD function, contact technical support engineers of the OS vendor to check whether the OS supports the VMD function. If yes, check whether the VMD driver needs to be manually installed and check the installation method. • Surprise hot swap if the VMD function is enabled and the latest Intel VMD driver is installed. • Orderly hot swap if the VMD function is disabled. <ul style="list-style-type: none"> • Supports a variety of RAID controller cards. For details, consult the local sales representative. <ul style="list-style-type: none"> - The RAID controller card supports RAID configuration, RAID level migration, and drive roaming.

Component	Specifications
	<ul style="list-style-type: none"> - The RAID controller card supports a supercapacitor for power-off protection to ensure user data security. - The PCIe RAID controller card occupies one PCIe slot. <p>For details about the RAID controller card, see <i>V6 Server RAID Controller Card User Guide</i>.</p> <p>NOTE If the BIOS is in legacy mode, the 4K drive cannot be used as the boot drive.</p>
Network	<p>Supports expansion capability of multiple types of networks.</p> <ul style="list-style-type: none"> • OCP 3.0 network adapter <ul style="list-style-type: none"> - The two FlexIO card slots support two OCP 3.0 network adapter respectively, which can be configured as required. - Supports orderly hot swap. <p>NOTE The OCP 3.0 network adapter supports orderly hot swap only when the VMD function is disabled.</p> <ul style="list-style-type: none"> - Supports a variety of OCP 3.0 network adapters. For details, see "Search Parts" in the Compatibility Checker.
I/O expansion	<p>Supports 6 PCIe slots.</p> <ul style="list-style-type: none"> • One PCIe slot dedicated for a screw-in RAID controller card, two FlexIO slots dedicated for OCP 3.0 network adapters, and three PCIe slots for standard PCIe cards. <p>For details, see 2.7.2 PCIe Slots and 2.7.3 PCIe Slot Description.</p> <ul style="list-style-type: none"> • Support GPU cards. <p>NOTE The preceding information is for reference only. For details, see "Search Parts" in the Compatibility Checker.</p>
Port	<p>Supports a variety of ports.</p> <ul style="list-style-type: none"> • Ports on the front panel: <ul style="list-style-type: none"> - One USB Type-C iBMC direct connect management port - Two USB 3.0 ports - One DB15 VGA port <p>NOTE The front panel of a server with 10 x 2.5" drives provides only one USB Type-C iBMC direct connect management port and one USB 3.0 port.</p> <ul style="list-style-type: none"> • Ports on the rear panel: <ul style="list-style-type: none"> - Two USB 3.0 ports - One DB15 VGA port - One RJ45 serial port - One RJ45 management network port

Component	Specifications
	<ul style="list-style-type: none"> Built-in ports: <ul style="list-style-type: none"> Two SATA ports <p>NOTE You are not advised to install the operating system on the USB storage media.</p>
Video card	<p>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.</p> <p>NOTE</p> <ul style="list-style-type: none"> 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 are connected to monitors, only the monitor connected to the front VGA port displays information.
System management	<ul style="list-style-type: none"> UEFI iBMC NC-SI Integration with third-party management systems
Security feature	<ul style="list-style-type: none"> Power-on password Administrator password TCM (only in China)/TPM Secure boot Front bezel (optional) Chassis cover opening detection

3.2 Environmental Specifications

Table 3-2 Environmental specifications

Category	Specifications
Temperature	<ul style="list-style-type: none"> Operating temperature: 5°C to 45°C (41°F to 113°F) (ASHRAE Classes A1 to A4 compliant) Storage temperature (within three months): -30°C to +60°C (-22°F to 140°F) Storage temperature (within six months): -15°C to +45°C (5°F to 113°F) Storage temperature (within one year): -10°C to +35°C (14°F to 95°F) Maximum rate of temperature change: 20°C (36°F) per

Category	Specifications
	<p>hour, 5°C (9°F) per 15 minutes</p> <p>NOTE The highest operating temperature varies depending on the server configuration. For details, see A.2 Operating Temperature Limitations.</p>
Relative humidity (RH, non-condensing)	<ul style="list-style-type: none"> • Operating humidity: 8% to 90% • Storage humidity (within three months): 8% to 85% • Storage humidity (within six months): 8% to 80% • Storage humidity (within one year): 20% to 75% • Maximum humidity change rate: 20%/h
Air volume	≥ 96 cubic feet per minute (CFM)
Operating altitude	<p>≤ 3050 m (10006.44 ft)</p> <ul style="list-style-type: none"> • When the server configuration complies with ASHRAE Classes A1 and A2 and the altitude is above 900 m (2952.76 ft), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 300 m (984.24 ft). • When the server configuration complies with ASHRAE Class A3 and the altitude is above 900 m (2952.76 ft), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 175 m (574.14 ft). • When the server configuration complies with ASHRAE Class A4 and the altitude is above 900 m (2952.76 ft), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 125 m (410.1 ft). • HDDs cannot be used at an altitude of over 3050 m (10006.44 ft).
Corrosive gaseous contaminant	<p>Maximum corrosion product thickness growth rate:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • The equipment room environment meets the requirements of ISO 14664-1 Class 8. • There is no explosive, conductive, magnetic, or corrosive dust in the equipment room. <p>NOTE It is recommended that the particulate pollutants in the equipment room be monitored by a professional organization.</p>
Acoustic noise	<p>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).</p> <ul style="list-style-type: none"> • Idle: <ul style="list-style-type: none"> – LWAd: 6.2 Bels

Category	Specifications
	<ul style="list-style-type: none"> - LpAm: 45.3 dBA • Operating: <ul style="list-style-type: none"> - LWAd: 6.97 Bels - LpAm: 52.6 dBA <p>NOTE Actual sound levels generated during server operation vary depending on server configuration, load, and ambient temperature.</p>

 **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 storage temperature and humidity specified in the preceding table, 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

Table 3-3 Physical specifications

Category	Description
Dimensions (H x W x D)	<ul style="list-style-type: none"> • Chassis with 3.5" drives: 43.5 mm x 447 mm x 790 mm (1.71 in. x 17.60 in. x 31.10 in.) • Chassis with 2.5" drives: 43.5 mm x 447 mm x 790 mm (1.71 in. x 17.60 in. x 31.10 in.)
Installation space	<ul style="list-style-type: none"> • Requirements for cabinet installation: Cabinet compliant with the International Electrotechnical Commission (IEC) 297 standard <ul style="list-style-type: none"> - Cabinet width: 482.6 mm (19.00 in.) - Cabinet depth ≥ 1000 mm (39.37 in.) • Requirements for guide rail installation: <ul style="list-style-type: none"> - L-shaped guide rails: apply only to our company's cabinets. - Static rail kit: applies to cabinets with a distance of 610 mm to 950 mm (24.02 in. to 37.40 in.) between the front and rear mounting bars. - Ball bearing rail kit: applies to cabinets with a distance of 609 mm to 950 mm (23.98 in. to 37.40 in.) between

Category	Description
	the front and rear mounting bars.
Weight in full configuration	<ul style="list-style-type: none"> • Maximum net weight: <ul style="list-style-type: none"> – Server with 4 x 3.5" drives: 20.5 kg (45.19 lb) – Server with 8 x 2.5" drives: 18.0 kg (39.68 lb) – Server with 10 x 2.5" drives: 18.5 kg (40.79 lb) • Packaging materials: 5 kg (11.03 lb)
Power consumption	The power consumption parameters vary with hardware configurations (including the configurations complying with EU ErP). Use the Power Calculator to obtain specific information.

4 Software and Hardware Compatibility

Use the [Compatibility Checker](#) to obtain information about the operating systems and hardware supported.

NOTICE

- If incompatible components are used, the device may be abnormal. This fault is beyond the scope of technical support and warranty.
 - The performance of servers is closely related to application software, basic middleware software, and hardware. The slight differences of the application software, middleware basic software, and hardware may cause performance inconsistency between the application layer and test software layer.
 - If the customer has requirements on the performance of specific application software, contact technical support to apply for POC tests in the pre-sales phase to determine detailed software and hardware configurations.
 - If the customer has requirements on hardware performance consistency, specify the specific configuration requirements (for example, specific drive models, RAID controller cards, or firmware versions) in the pre-sales phase.
-

5 Safety Instructions

5.1 Security

5.2 Maintenance and Warranty

5.1 Security

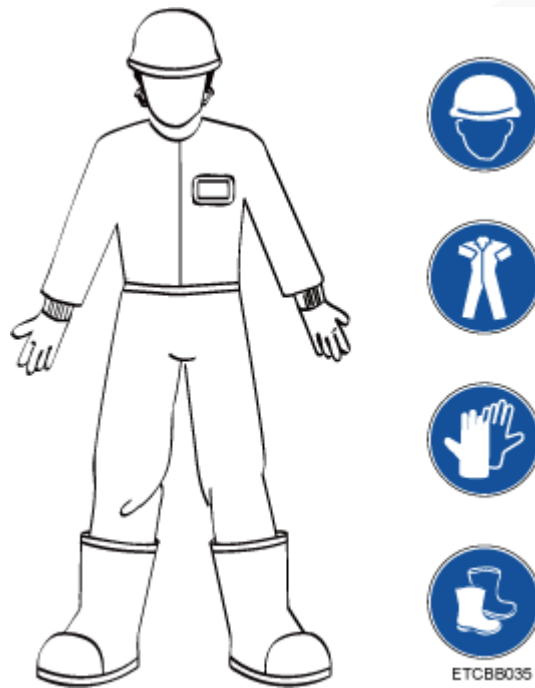
General Statement

- Comply with local laws and regulations when installing devices. These Safety Instructions are only a supplement.
- The "DANGER", "WARNING", and "CAUTION" information in this document does not represent all the safety instructions, but supplements to the safety instructions.
- Observe all safety instructions provided on the device labels when installing hardware. Follow them in conjunction with these Safety Instructions.
- Only qualified personnel are allowed to perform special tasks, such as performing high-voltage operations and driving a forklift.
- This is a class A product, which may cause radio interference in a domestic environment. Take protective measures before operating this product in a residential environment.

Personal Safety

- Only personnel certified or authorized are allowed to install equipment.
- Discontinue any dangerous operations and take protective measures. Report anything that could cause personal injury or device damage to a project supervisor.
- Do not move devices or install racks and power cables in hazardous weather conditions.
- Do not carry the weight that is over the maximum load per person allowed by local laws or regulations. Before moving or installing equipment, check the maximum equipment weight and arrange required personnel.
- Wear clean protective gloves, ESD clothing, a protective hat, and protective shoes, as shown in Figure 5-1.

Figure 5-1 Safety work wear



- Before touching a device, wear ESD clothing and gloves (or wrist strap), and remove any conductive objects (such as watches and jewelry). Figure 5-2 shows conductive objects that must be removed before you touch a device.

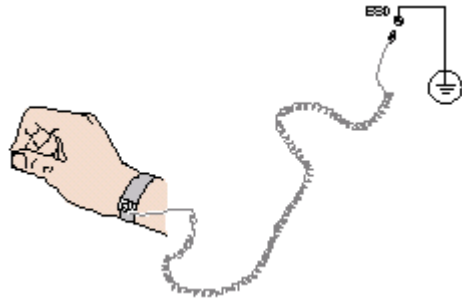
Figure 5-2 Removing conductive objects



Figure 5-3 shows how to wear an ESD wrist strap.

- Put your hands into the ESD wrist strap.
- Tighten the strap buckle and ensure that the ESD wrist strap is in contact with your skin.
- Insert the ground terminal attached to the ESD wrist strap into the jack on the grounded rack or chassis.

Figure 5-3 Wearing an ESD wrist strap



- Exercise caution when using tools.
- If the installation position of a device is higher than the shoulders of the installation personnel, use a vehicle such as a lift to facilitate installation. Prevent the device from falling down and causing personal injury or damage to the device.
- The equipment is powered by high-voltage power sources. Direct or indirect contact (especially through damp objects) with high-voltage power sources may result in serious injury or death.
- Ground the equipment before powering it on. Otherwise, personal injury may be caused by high electricity leakage.
- When a ladder is used, ensure that another person holds the ladder steady to prevent accidents.
- Do not look into optical ports without eye protection.

Device Security

- Use the recommended power cables at all times.
- Use power cables only for dedicated servers. Do not use them for other devices.
- Before operating equipment, wear ESD clothes and gloves to prevent electrostatic-sensitive devices from being damaged by ESD.
- When moving a device, hold the bottom of the device. Do not hold the handles of the installed modules, such as the PSUs, fan modules, drives, and the mainboard. Handle the equipment with care.
- Exercise caution when using tools.
- Connect the primary and secondary power cables to different power distribution units (PDUs) to ensure reliable system operation.
- Ground a device before powering it on. Otherwise, high leakage current may cause device damage.

Transportation Precautions

Improper transportation may damage equipment. Contact the manufacturer for precautions before attempting transportation.

Transportation precautions include but are not limited to:

- The logistics company engaged to transport the device must be reliable and comply with international standards for transporting electronics. Ensure that the equipment being transported is always kept upright. Take necessary precautions to prevent collisions, corrosion, package damage, damp conditions and pollution.

- Transport each device in its original packaging.
- If the original packaging is unavailable, package heavy, bulky parts (such as chassis and blades) and fragile parts (such as PCIe cards and optical modules) separately.

 **NOTE**

For details about the components supported by the server, see "Compatibility" in the [Compatibility Checker](#).

- Power off all devices before transportation.

Maximum Weight Carried by a Person

 **CAUTION**

Comply with local regulations for the maximum load per person.

Table 5-1 lists the maximum weight one person is permitted to carry as stipulated by a number of organizations.

Table 5-1 Maximum weight carried per person

Organization	Weight (kg/lb)
European Committee for Standardization (CEN)	25/55.13
International Organization for Standardization (ISO)	25/55.13
National Institute for Occupational Safety and Health (NIOSH)	23/50.72
Health and Safety Executive (HSE)	25/55.13
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China (AQSIQ)	<ul style="list-style-type: none">• Male: 15/33.08• Female: 10/22.05

For more information about safety instructions, see *Server Safety Information*.

5.2 Maintenance and Warranty

For details about the maintenance policy, visit [Customer Support Service](#).

For details about the warranty policy, visit [Warranty](#).

6 ESD

6.1 ESD Prevention

6.2 Grounding Methods for ESD Prevention

6.1 ESD Prevention

The static electricity released by the human body or conductors may damage the mainboard or other electrostatic-sensitive devices. The damage caused by static electricity will shorten the service time of the devices.

To prevent electrostatic damage, observe the following:

- Use the ESD floor (or ESD mat) and ESD chairs in the equipment room. Use ESD materials for partition boards, screens, and curtains in the equipment room.
- All floor-standing electric devices, metal frames, and metal rack shells in the equipment room must be directly grounded. All electric meters or tools on a workbench must be connected to the common ground point of the workbench.
- Monitor the temperature and humidity in the equipment room. The heating system may reduce the humidity and increases static electricity indoors.
- Place the product in an ESD bag to avoid direct contact during transportation and storage.
- Before transporting electrostatic-sensitive components to a work area that is not affected by static electricity, store them in their original packages.
- Place the component on a grounded surface and then take it out of the package.
- Before installing or removing a server component, wear an ESD wrist strap that is properly grounded.
- During parts replacement, keep new components in ESD bags before installation, and place removed components on conductive mats for temporary storage.
- Do not touch pins, wires, or circuits.

6.2 Grounding Methods for ESD Prevention

Use one or more of the following grounding methods when handling or installing electrostatic-sensitive devices:

- Use an ESD wrist strap that connects to a grounded work area or computer chassis through a ground cable. The wrist strap must be scalable, and the resistance of the ground cable must be at least 1 megohm ($\pm 10\%$). Wear the wrist strap tightly against your skin.
- Use a heel-grounded, toe-grounded, or shoe-grounded ESD strap when working in a standing position. When standing on a conductive floor or electrostatic dissipative floor mat, tie a strap on your feet.
- Use conductive maintenance tools.
- Use a folding tool mat that dissipates static electricity and a portable field service kit.

7 Installation and Configuration

- [7.1 Installation Environment Requirements](#)
- [7.2 Hardware Installation](#)
- [7.3 Power-On and Power-Off](#)
- [7.4 Initial Configuration](#)

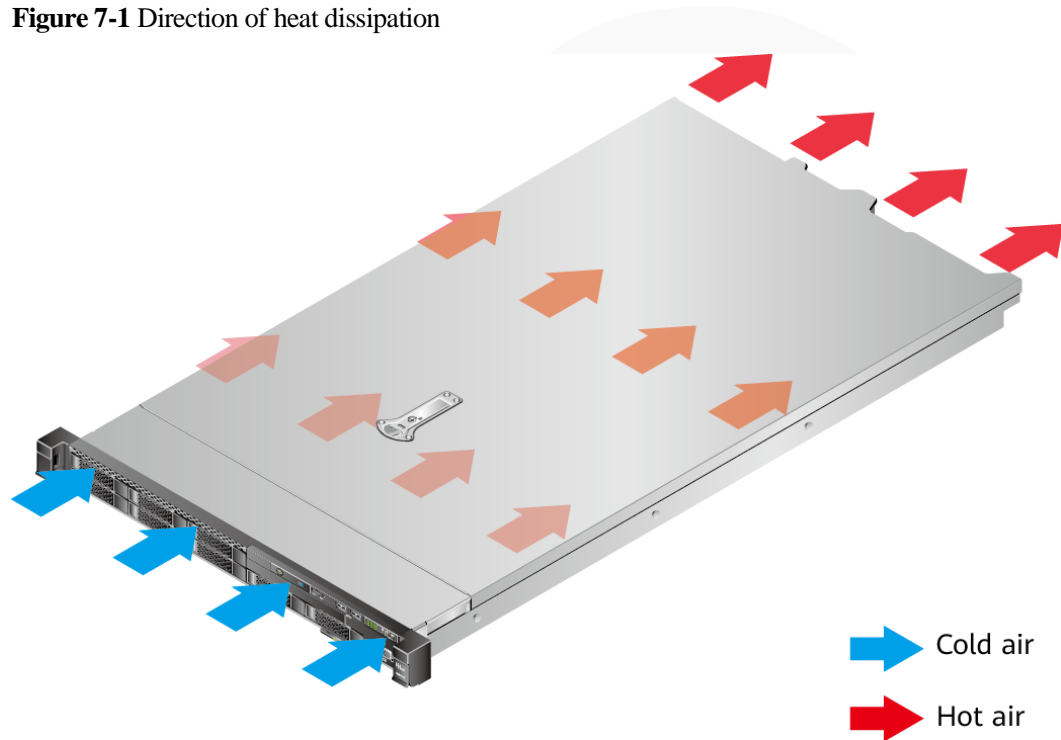
7.1 Installation Environment Requirements

7.1.1 Space and Airflow Requirements

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 device maintenance, leave a clearance of 1000 mm in front of the cabinet and a clearance of 800 mm at the rear of the cabinet.
- Do not block the air intake vents. Otherwise, air intake 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.

Figure 7-1 Direction of heat dissipation



7.1.2 Temperature and Humidity Requirements

To ensure continued safe and reliable device operation, install or position the device in a well-ventilated, climate-controlled environment.

- Use temperature control devices all year long in any climates.
- Use humidifiers and dehumidifiers in dry or humid areas to maintain ambient humidity within range.

Table 7-1 Temperature and humidity requirements in the equipment room

Item	Description
Temperature	5°C to 35°C (41°F to 95°F)
Humidity (non-condensing)	8% RH to 90% RH

7.1.3 Cabinet Requirements

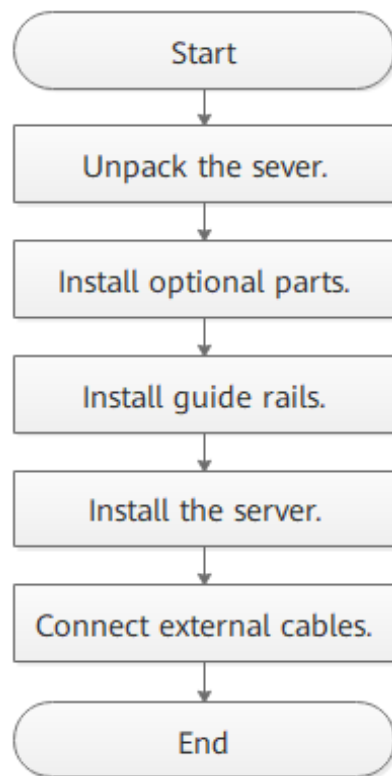
- A general 19-inch cabinet with a depth of more than 1000 mm (39.37 in.) which complies with the International Electrotechnical Commission 297 (IEC 297) standard.
- Air filters installed on cabinet doors.

7.2 Hardware Installation

7.2.1 Installation Overview

Installation process

Figure 7-2 Installation process



Precautions

- Properly ground the server before installation to avoid damage to electronic components from electrostatic discharge. Improper grounding may cause ESD.
For details about how to prevent electrostatic discharge, see 6 ESD.
- Before installing multiple components, read the installation instructions for all the components and identify similar actions to simplify the installation process.
For details about component compatibility, see "Search Parts" in the [Compatibility Checker](#).

 **CAUTION**

Wait until overheating devices have cooled down before touching them to avoid injury.

7.2.2 Unpacking the Server

Procedure

Step 1 Check whether the packing case and seals are in good conditions.

 **NOTE**

If the packing case is soaked or deformed, or the seals or pressure-sensitive adhesive tapes are not intact, contact technical support to obtain the *Cargo Problem Feedback Form*.

Step 2 Use a box cutter to open the packing case.

 **CAUTION**

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

Step 3 Unpack the packing case.

Step 4 Ensure that the components are complete and in good condition without defects such as oxidation, chemical corrosion, missing components, or other damage incurred during transport.

Table 7-2 Packing list

No.	Description
1	(Optional) Documentation bag containing a warranty card and quick start guide
2	(Optional) Server guide rails
3	One rack server

----End

7.2.3 Installing Optional Parts

Before installing and configuring a server, you need to install all optional parts required, such as purchased CPUs, drives, and PCIe cards.

Procedure

Step 1 Install the optional parts for the 1288H V6.

----End

7.2.4 Installing Server Guide Rails

7.2.4.1 Installing L-Shaped Guide Rails

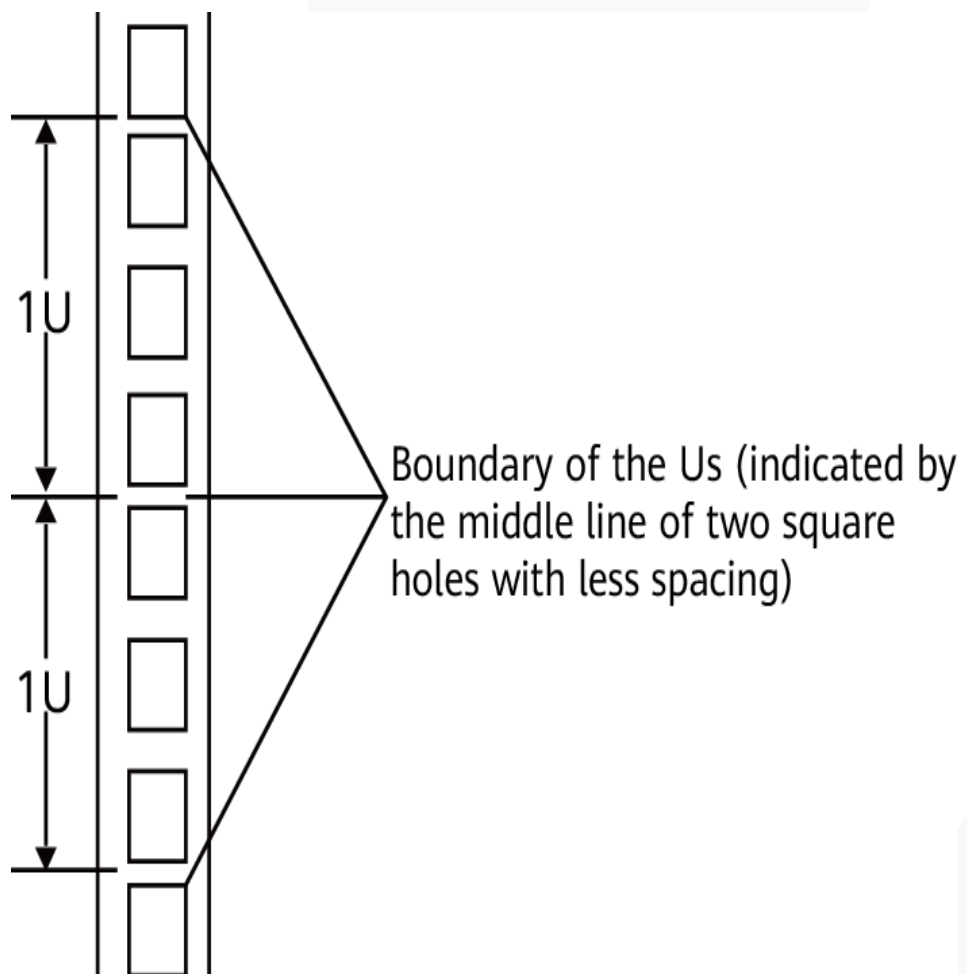
L-shaped guide rails apply only to our company's cabinets only.

Procedure

Step 1 Install floating nuts.

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

Figure 7-3 Spacing of 1U on a mounting bar of a cabinet

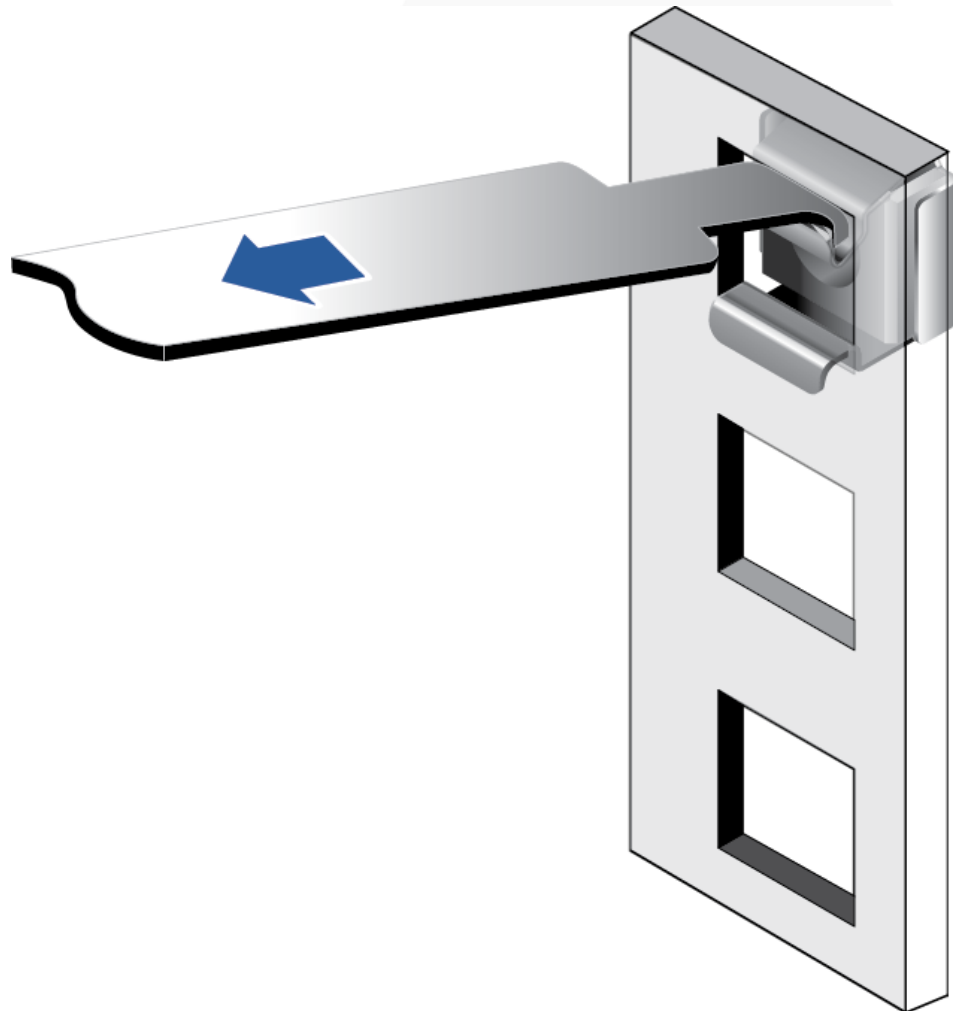


NOTE

- Floating nuts are used to tighten screws.
 - The boundary between Us is used as the reference for calculating device installation space.
2. Fasten the lower end of a floating nut to the target square hole in a mounting bar at the front of the cabinet.

3. Use a floating nut hook to pull the upper end of the floating nut, and fasten it to the upper edge of the square hole.

Figure 7-4 Installing a floating nut

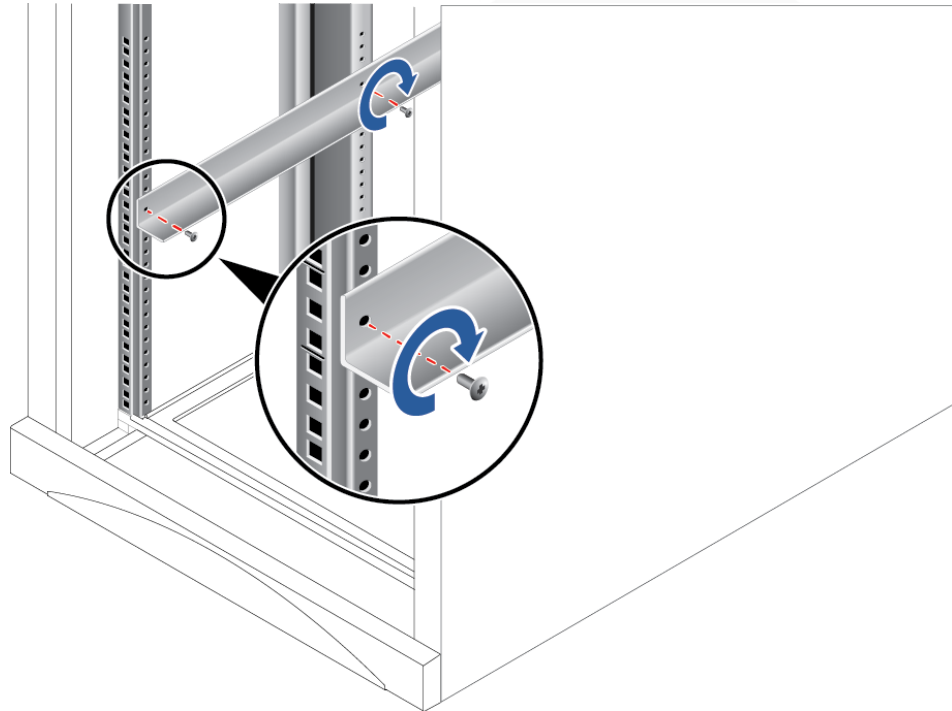


4. Install the other floating nut in the same way.

Step 2 Install the L-shaped guide rails.

1. Position a guide rail horizontally in contact with the mounting bars in the cabinet.
2. Tighten the screws to secure the guide rail.

Figure 7-5 Installing an L-shaped guide rail



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

----End

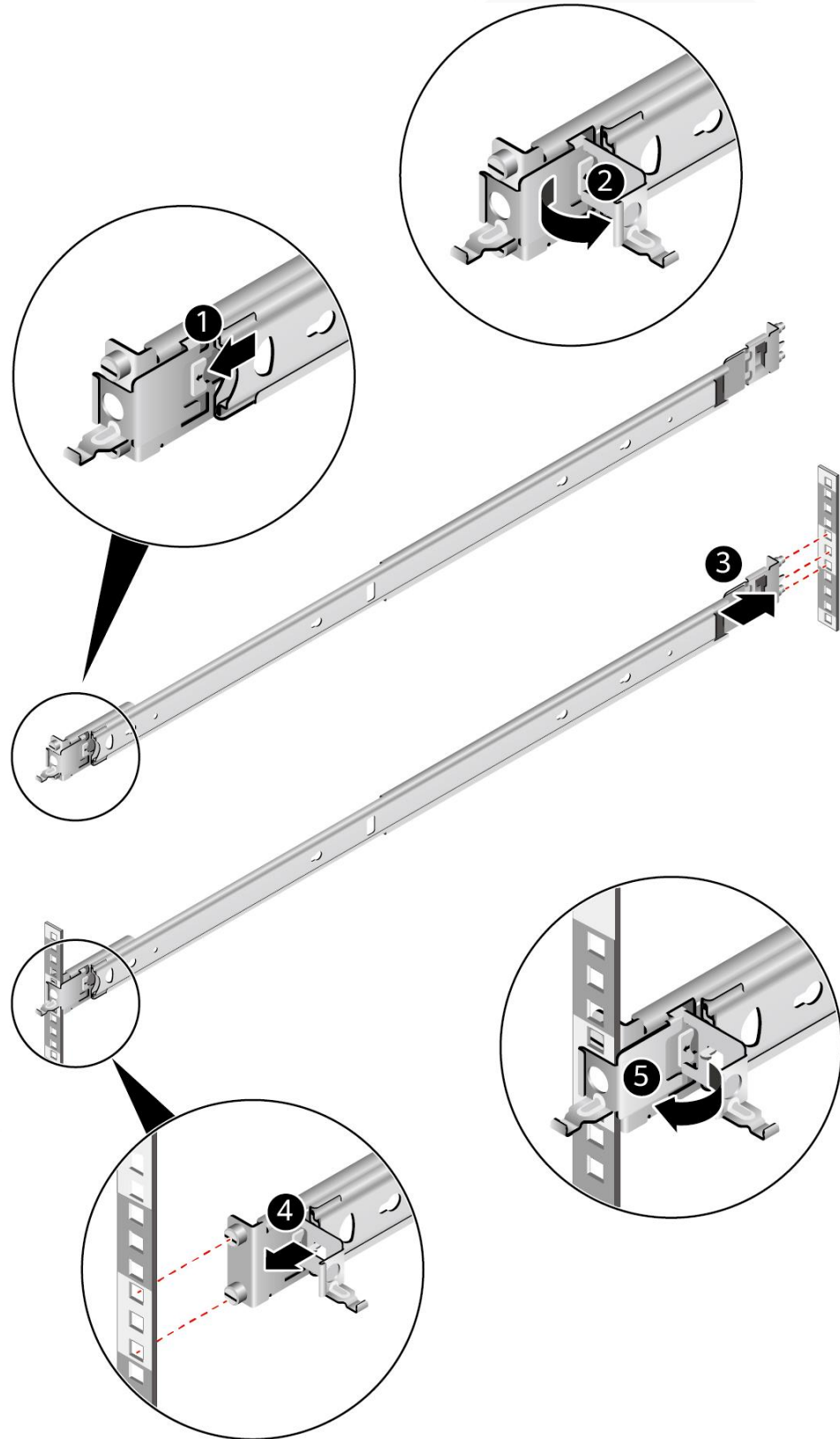
7.2.4.2 Installing the Static Rail Kit

The static rail kit applies to cabinets with a distance of 610 mm to 950 mm (24.02 in. to 37.40 in.) between the front and rear mounting bars.

Procedure

- Step 1** Push the release latch on the front of the rail and pull out the hook. See (1) and (2) in Figure 7-6.
- Step 2** Insert the positioning pin at the rear of the rail into the hole on the rear column of the cabinet. See (3) in Figure 7-6.
- Step 3** Keep the rail horizontal, and push the front end of the rail until it is inserted into the hole on the front column of the cabinet. See (4) in Figure 7-6.
- Step 4** Hook the rail. See (5) in Figure 7-6.

Figure 7-6 Installing a static rail



Step 5 Install the other guide rail in the same way.

----End

7.2.4.3 Installing the Ball Bearing Rail Kit

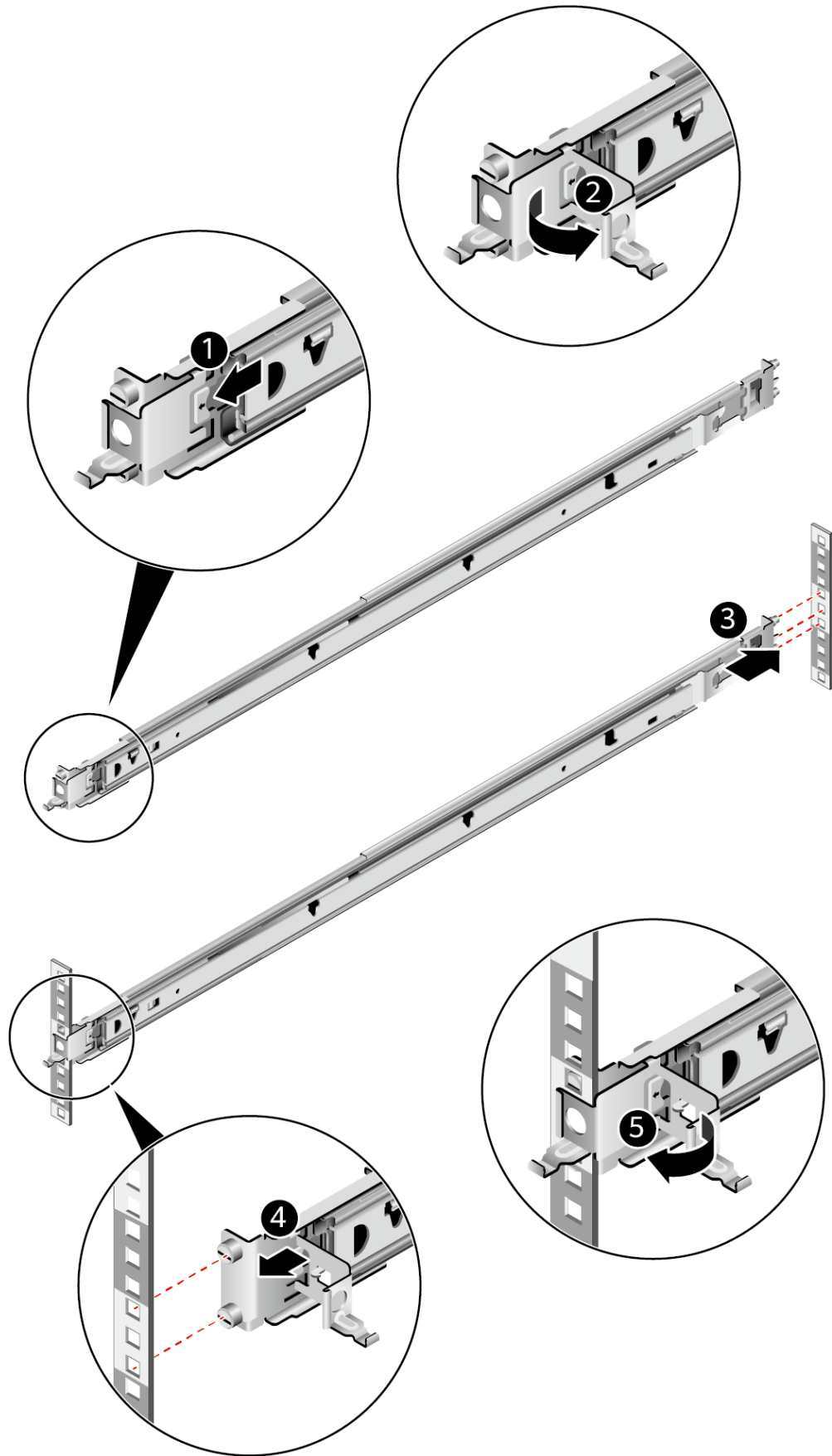
The ball bearing rail kit applies to cabinets with a distance of 609 mm to 950 mm (23.98 in. to 37.40 in.) between the front and rear mounting bars.

Procedure

- Step 1** Push the release latch on the front of the rail and pull out the hook. See (1) and (2) in Figure 7-7.
- Step 2** Insert the positioning pin at the rear of the rail into the hole on the rear column of the cabinet. See (3) in Figure 7-7.
- Step 3** Keep the rail horizontal, and push the front end of the rail until it is inserted into the hole on the front column of the cabinet. See (4) in Figure 7-7.
- Step 4** Hook the rail. See (5) in Figure 7-7.

Figure 7-7 Installing a ball bearing rail





Step 5 Install the other guide rail in the same way.

----End

7.2.5 Installing a Server

7.2.5.1 Installing the Server on L-Shaped Guide Rails

- Before installing the server, ensure that the L-shaped guide rails are properly installed. For details, see 7.2.4.1 Installing L-Shaped Guide Rails .
- The 1288H V6 servers are not stackable onto L-shaped guide rails.

Procedure

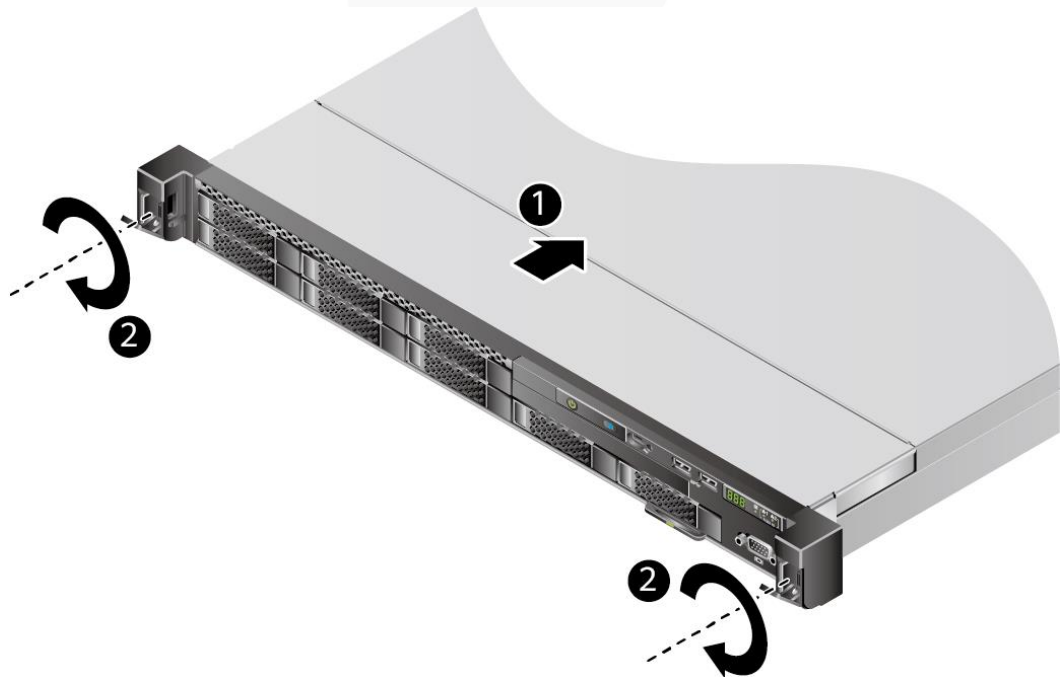
Step 1 Install the server.

CAUTION

At least two people are required to move the device. Otherwise, personal injury or device damage may occur.

1. At least two people are required to lift the server vertically from both sides, place it on the guide rails, and push it into the cabinet. See (1) in Figure 7-8.
2. Align both sides of the server with the mounting bars and tighten the captive screws on the panel. See (2) in the Figure 7-8.

Figure 7-8 Installing a server



Step 2 Connect external cables as required, such as network cables, VGA cables, and USB devices.

Step 3 Connect the cables to the PSU.

For details, see 7.2.6.9 Connecting PSU Cables.

Step 4 Power on the server.

For details, see 7.3.1 Powering On .

Step 5 Check indicator status.

For details, see 2.1.2 Indicators and Buttons .

----End

7.2.5.2 Installing the Server on the Static Rail Kit

- Before installing the server, ensure that the static rail kit is properly installed. For details, see 7.2.4.2 Installing the Static Rail Kit.
- The 1288H V6 servers are stackable onto the static rail kit.

Procedure

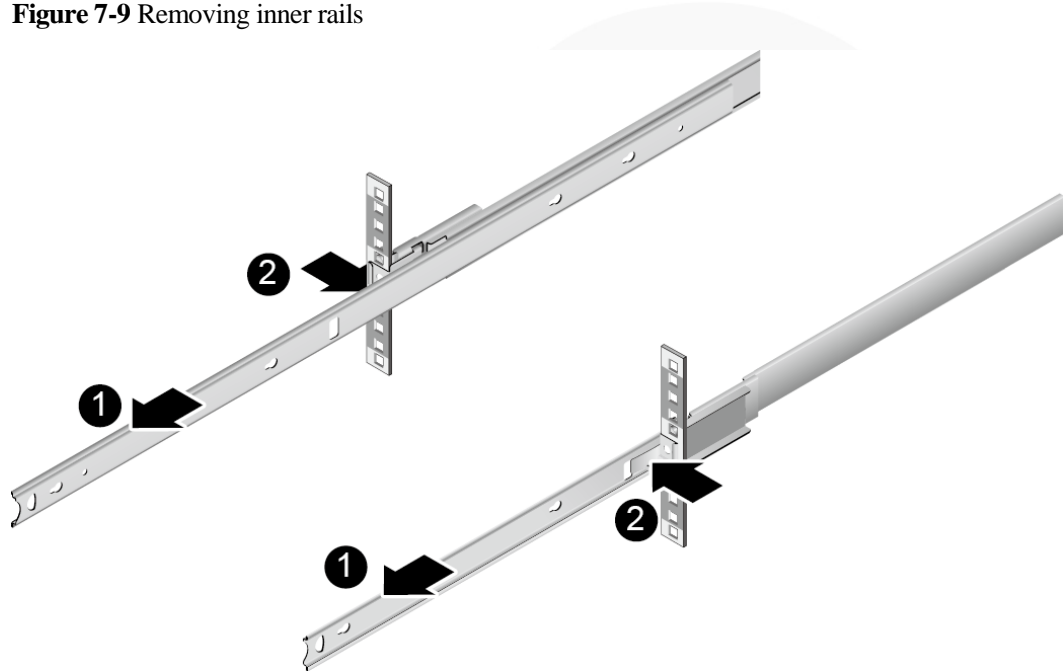
Step 1 Install the server.

 **CAUTION**

At least two people are required to move the device. Otherwise, personal injury or device damage may occur.

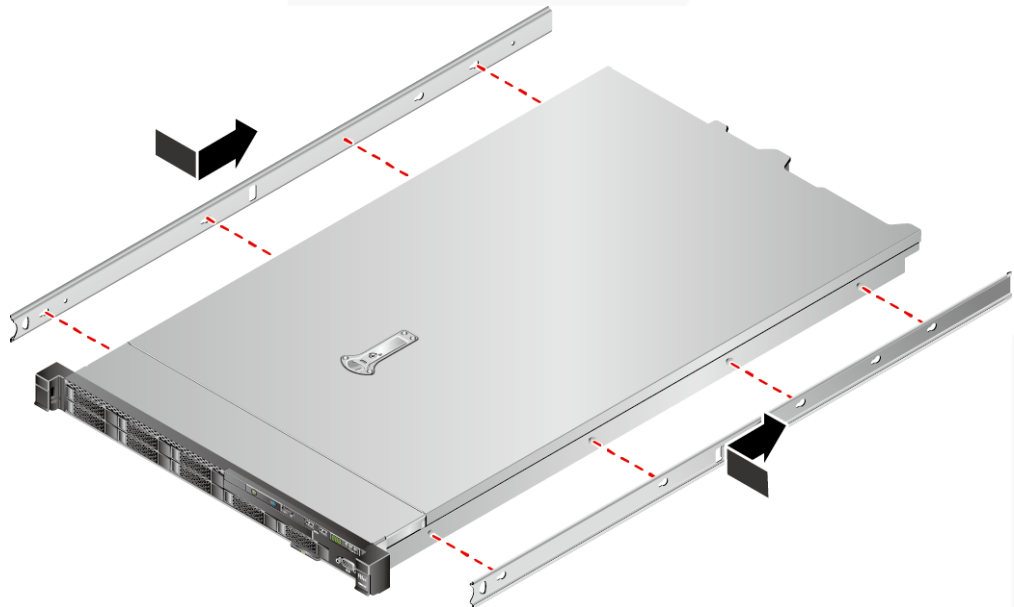
1. Pull the inner rail out of the rail until it does not move. See (1) in Figure 7-9.
2. Press the buckles on both sides of the inner rails and remove the inner rails See (2) in Figure 7-9.

Figure 7-9 Removing inner rails



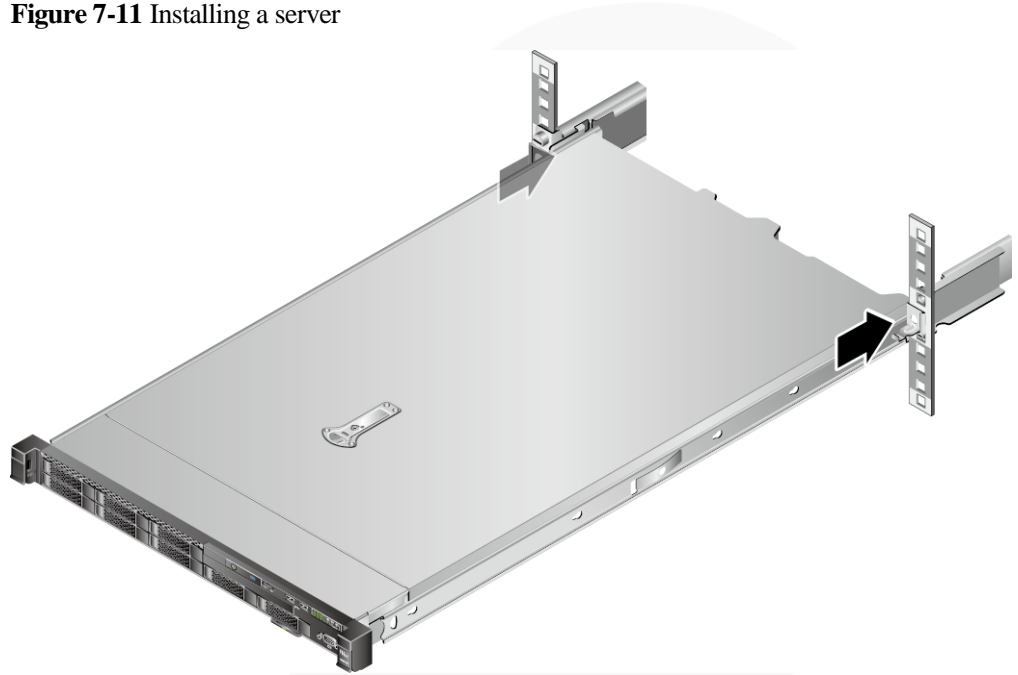
3. Align the holes on the inner rails with the nail heads on both sides of the server, and install the inner rails in the arrow direction.

Figure 7-10 Installing a server on inner rails



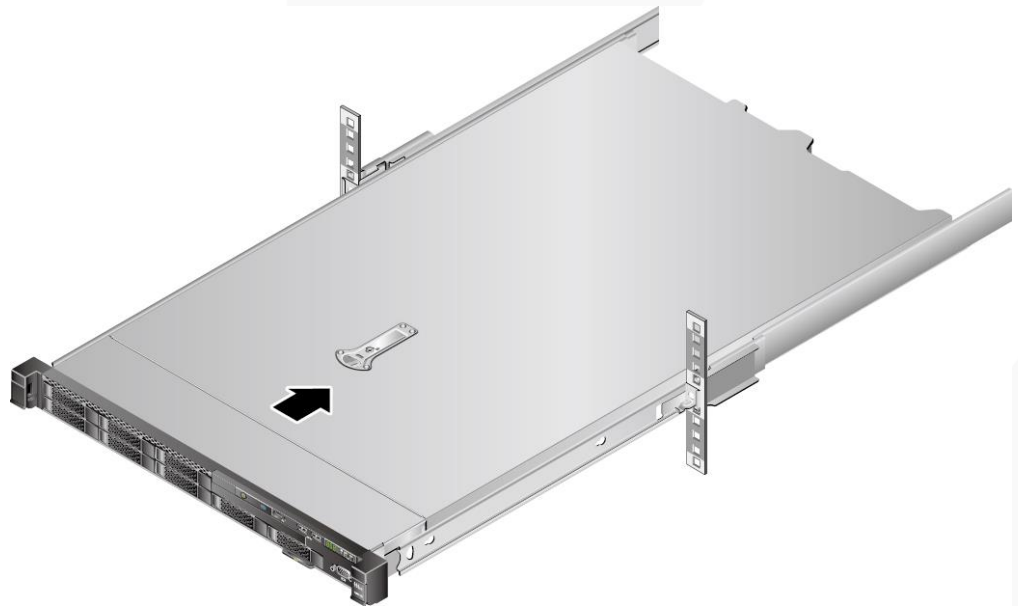
4. At least two people are required to lift the server vertically from both sides and install it on the guide rails.

Figure 7-11 Installing a server



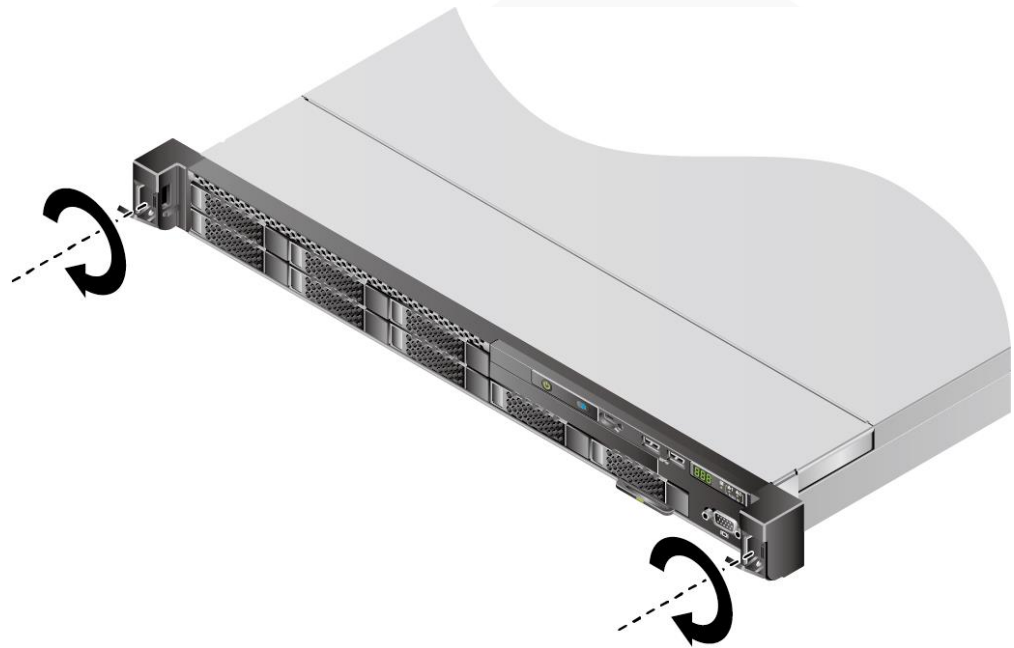
5. Push the server on the inner rails until it cannot move.

Figure 7-12 Pushing the server into the static rail kit



6. Open the baffle plate of the captive screws on the panel and tighten the captive screws.

Figure 7-13 Securing a server



Step 2 Connect external cables as required, such as network cables, VGA cables, and USB devices.

Step 3 Connect the cables to the PSU.

For details, see 7.2.6.9 Connecting PSU Cables.

Step 4 Power on the server.

For details, see 7.3.1 Powering On .

Step 5 Check indicator status.

For details, see 2.1.2 Indicators and Buttons .

----End

7.2.5.3 Installing a Server on the Ball Bearing Rail Kit

- Before installing the server, ensure that the ball bearing rail kit is properly installed. For details, see 7.2.4.3 Installing the Ball Bearing Rail Kit.
- The 1288H V6 servers are stackable onto the ball bearing rail kit.

Procedure

Step 1 Install the server.

⚠ CAUTION

At least two people are required to move the device. Otherwise, personal injury or device damage may occur.

1. Pull out the inner rails as far as they will go.

Figure 7-14 Pulling out an inner rail



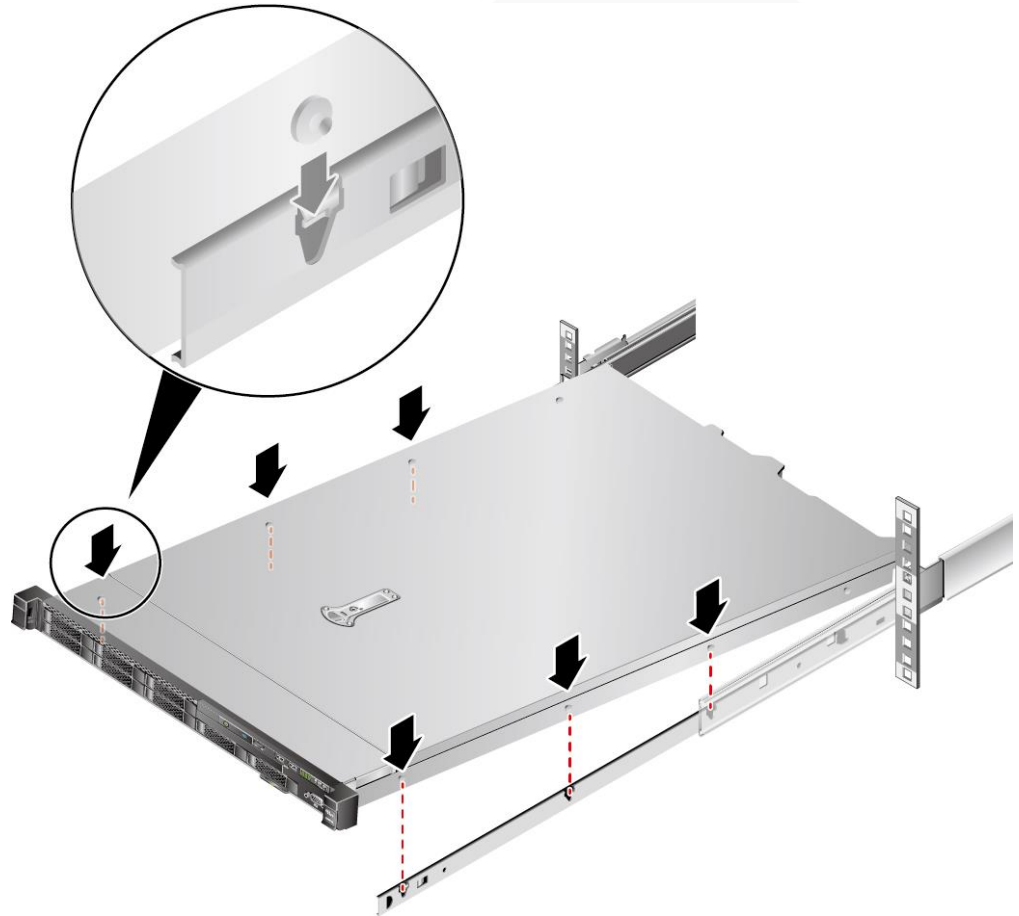
2. At least two people are required to lift the server vertically from both sides, align the two mounting screws at the rear of the server with the fixing holes on the inner rails, and place the server vertically at the rear of the server. Then push the server horizontally as far as it will go. See Figure 7-15.

Figure 7-15 Securing the server to inner rails (1)



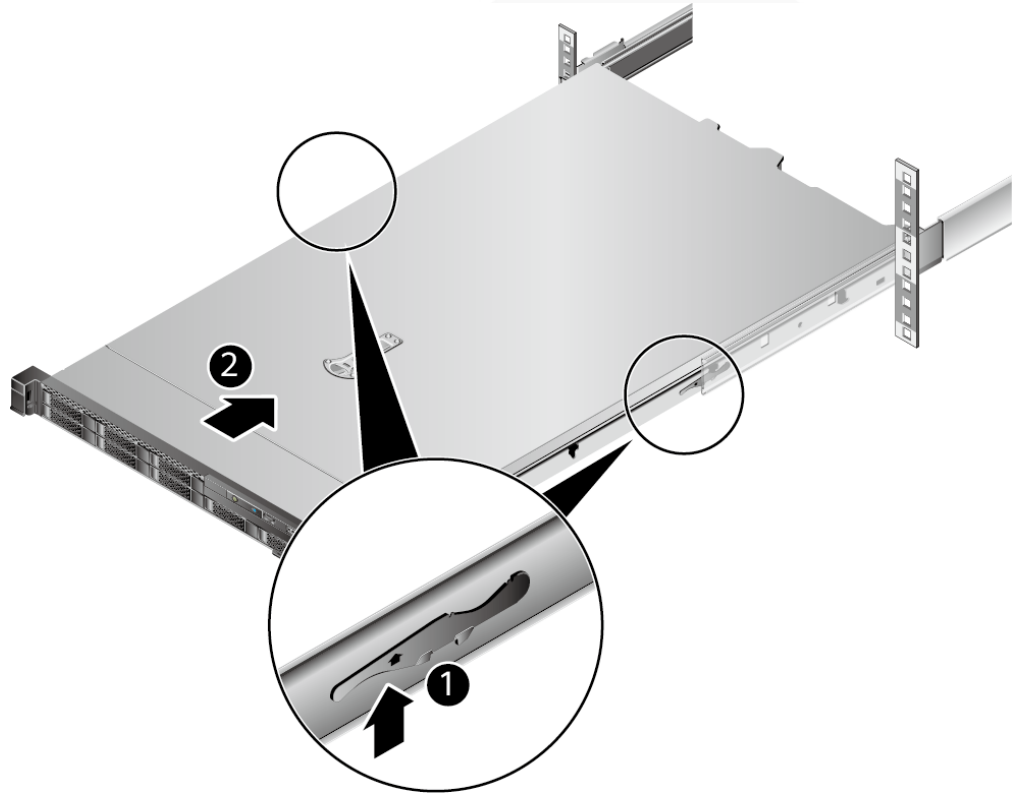
3. Aligning the six mounting screws at the front of the server with the fixing holes on the inner rails, place the server vertically to ensure that the server is secured to the inner rails. See Figure 7-16.

Figure 7-16 Securing a server to inner rails (2)



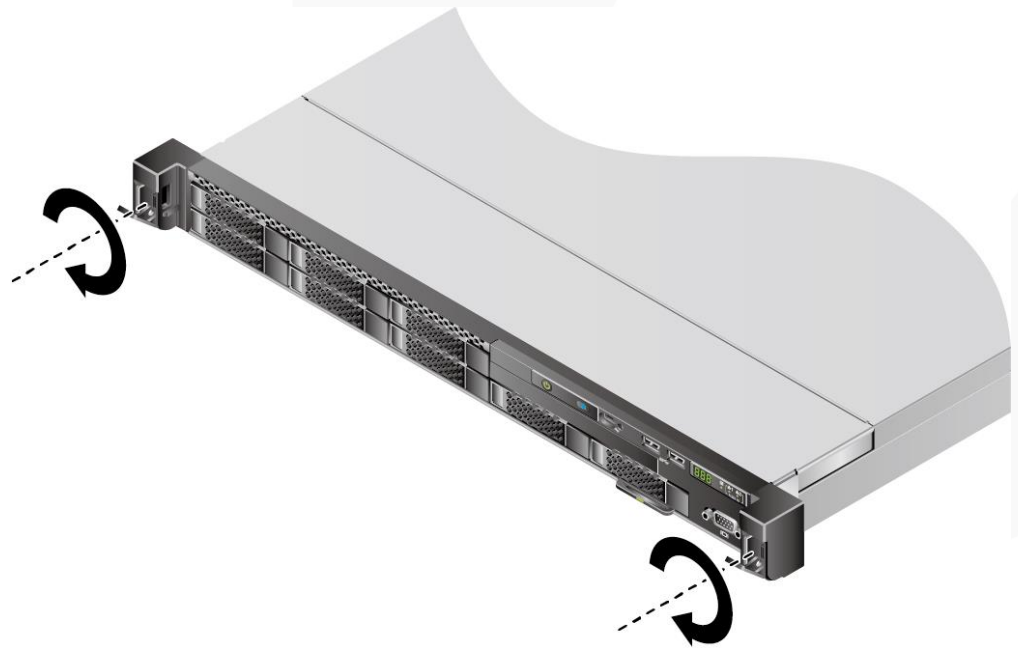
4. Unlock the release latches on both sides of the inner rails and push the server as far as it will go. See (1) and (2) in Figure 7-17.

Figure 7-17 Pushing the server into the ball bearing rail kit



5. Open the baffle plate of the captive screws on the panel and tighten the captive screws.

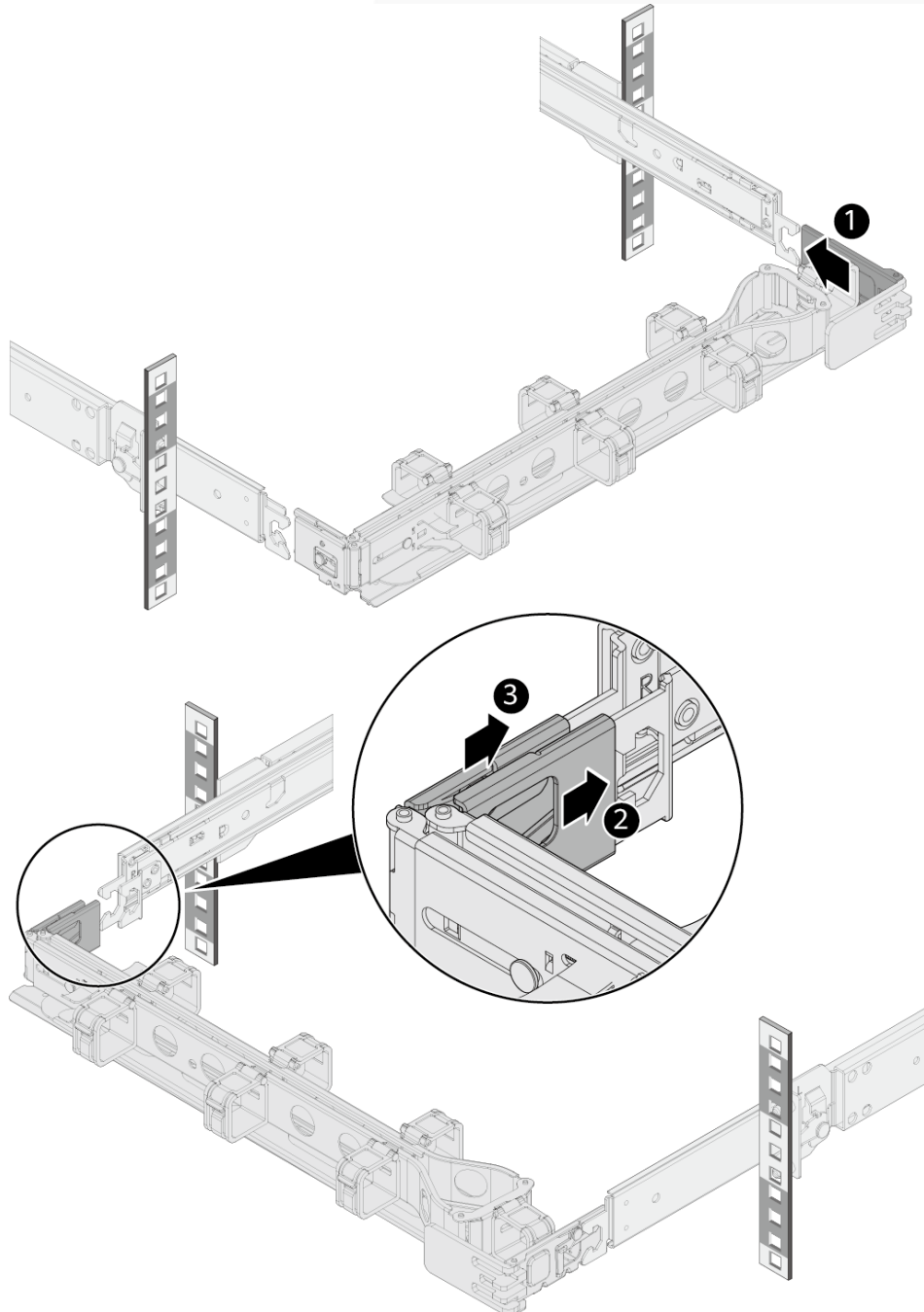
Figure 7-18 Securing a server



Step 2 Install a cable management arm (CMA).

1. Insert the bracket on the right of the CMA into the right guide rail. See (1) in Figure 7-19.
2. Insert the internal bracket on the left of the CMA into the left guide rail. See (2) in Figure 7-19.
3. Insert the external bracket on the left of the CMA into the left guide rail. See (3) in Figure 7-19.

Figure 7-19 Installing a CMA



Step 3 Connect external cables as required, such as network cables, VGA cables, and USB devices.

Step 4 Connect the cables to the PSU.

For details, see 7.2.6.9 Connecting PSU Cables.

Step 5 Power on the server.

For details, see 7.3.1 Powering On .

Step 6 Check indicator status.

For details, see 2.1.2 Indicators and Buttons .

----End

7.2.6 Connecting External Cables

7.2.6.1 Cabling Guidelines

Basic Guidelines

NOTICE

Do not block the air exhaust vents on the rear panel of the server when you lay out cables. Otherwise, heat dissipation of the server may be affected.

- Lay out and bind cables of different types (such as power and signal cables) separately. Cables of the same type must be in the same direction.
 - Cables at a small distance can be laid out in crossover mode.
 - When laying out cables in parallel, the distance between power cables and signal cables must be longer than or equal to 30 mm (1.18 in.).
- If you cannot identify cables according to the cable labels, attach an engineering label to each cable.
- Cables must be protected from burrs, heat sinks, and active accessories, which may damage the insulation layers of the 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 the excess lengths of the cable ties and ensure that the cuts are neat and smooth.
- Ensure that cables are properly laid out, supported, or fixed within the cable troughs inside the cabinet to prevent loose connections and cable damage.
- Surplus cable lengths must be coiled and bound to a proper position inside the cabinet.
- Cables must be laid out straightly and bound 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 diameter of the cable, and the cable must be bound before it is bent.

- Do not use cable ties at a place where the cables are bent. Otherwise, the cables may break.

Common Methods

The methods of laying out cables inside a cabinet are described as follows:

- Choose overhead or underfloor cabling for power cables based on equipment room conditions (such as the AC power distribution frame, surge protector, and terminal blocks).
- Choose overhead or underfloor cabling for service data cables (for example, signal cables) based on equipment room conditions.
- Place the connectors of all service data cables at the bottom of the cabinet so that the connectors are difficult to reach.

7.2.6.2 Connecting Mouse, Keyboard, and VGA Cables

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

Users can connect a keyboard and mouse to the USB port on the front or rear panel based on site installation conditions. There are two connection methods:

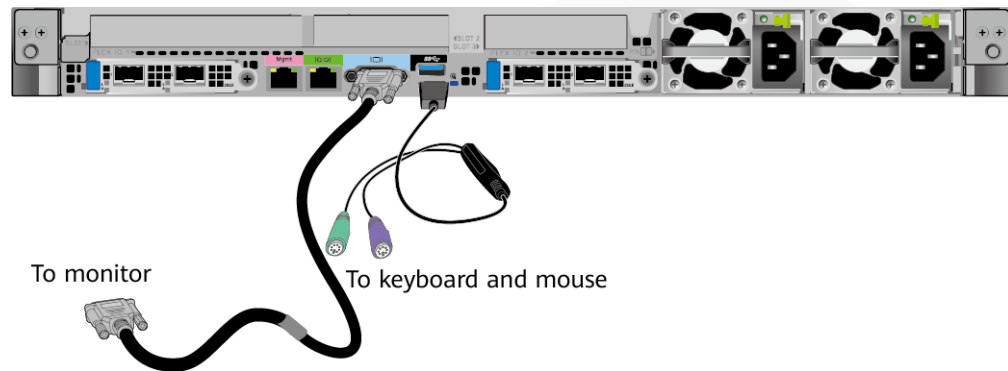
- Connect the keyboard and mouse to the USB ports.
- Connect the keyboard and mouse using a USB-to-PS/2 cable.

This section describes how to connect a keyboard and mouse using a USB-to-PS/2 cable and connect a monitor using a VGA cable.

Procedure

- Step 1** Connect the USB connector of the USB-to-PS/2 cable to a USB port on the front or rear panel of the server.
- Step 2** Connect the PS/2 connectors of the USB-to-PS/2 cable to the keyboard and mouse.
- Step 3** Connect the DB15 connector of the VGA cable to the VGA port on the front or rear panel of the server and tighten the two screws.
- Step 4** Connect the other connector of the VGA cable to the VGA port on the monitor and tighten the two screws.

Figure 7-20 Connecting a USB-to-PS/2 cable and VGA cable



----End

7.2.6.3 Connecting Network Cables

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

Procedure

Step 1 Determine the model of the new network cable.

- Shielded cables are recommended.

NOTE

If a non-shielded cable is used, the system cannot respond to ESD. As a result, the server may work abnormally.

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

Step 2 Number the new network cable.

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

Step 3 Lay out the new network cable.

- Lay out the new cable in the same way as the old one. Underfloor cabling is recommended because it is tidy and easy.
- Lay out network cables in the cabinet based on installation requirements. You are advised to arrange cables in the same way as existing cables. Ensure that cables are routed neatly and undamaged.
- Separate network cables from power cables and signal cables when laying out the cables.
- The minimum bend radius of a network cable is 4 cm (1.57 in.). Ensure that the cable insulation layer is intact.
- Ensure that cables are laid out for easy maintenance and capacity expansion.

- Network cables must be bound using cable ties. Ensure that network cables are bound closely, neatly, and straight, and cable ties are in even distance and fastened properly.

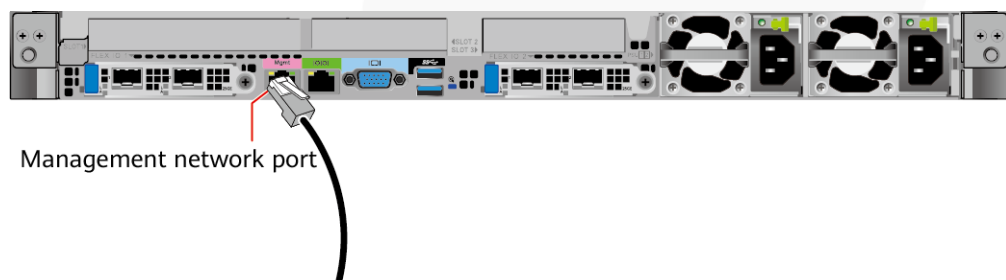
Step 4 Remove the network cable to be replaced.

Remove the network cable from the network interface card (NIC) or board in the cabinet.

Step 5 Connect the new network cable to the NIC or board.

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

Figure 7-21 Connecting a network cable



Step 6 Connect the new network cable to the peer network port.

- Connect the other cable connector 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 7 Check whether the new network cable is functioning properly.

Power on the device. Check whether the communication with the peer device is normal by running the **ping** command.

- If yes, 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 existing cable ties and bind all network cables again if necessary.
- If no, check whether the network cable is damaged or whether the connector of the network cable is not securely inserted.

----End

7.2.6.4 Connecting a Cable to an Optical Port

Procedure

Step 1 Determine the model of the new cable.

You can use an optical cable or an SFP+ cable to connect to the optical port.

Step 2 Number the new cable.

- The number of the new cable must be the same as that of the old one.
- Use the same type of labels for the optical cable.
 - Record the name and number of the local device to be connected on one side of the label, and those of the peer device on the other side.
 - Attach the label 2 cm (0.79 in.) away from the end of the optical cable.

Step 3 Lay out the new cable.

- Lay out the new cable in the same way as the old one.
For example, if the old cable is laid out in underfloor cabling mode, so is the new cable.
- Lay out optical cables or SFP+ cables in the cabinet based on installation requirements.
You are advised to arrange cables in the same way as existing cables. Ensure that cables are routed neatly and undamaged.
- Separate optical cables or SFP+ cables from power cables and signal cables when laying out the cables.
- The minimum bend radius of an optical cable or SFP+ cables is 4 cm (1.57 in.).
- Ensure that optical cables or SFP+ cables are laid out for easy maintenance and capacity expansion.
- Optical cables must be bound using cable ties. Ensure that:
 - Optical cables are bound closely, neatly, and straight.
 - Cable ties are in even distance and fastened properly.

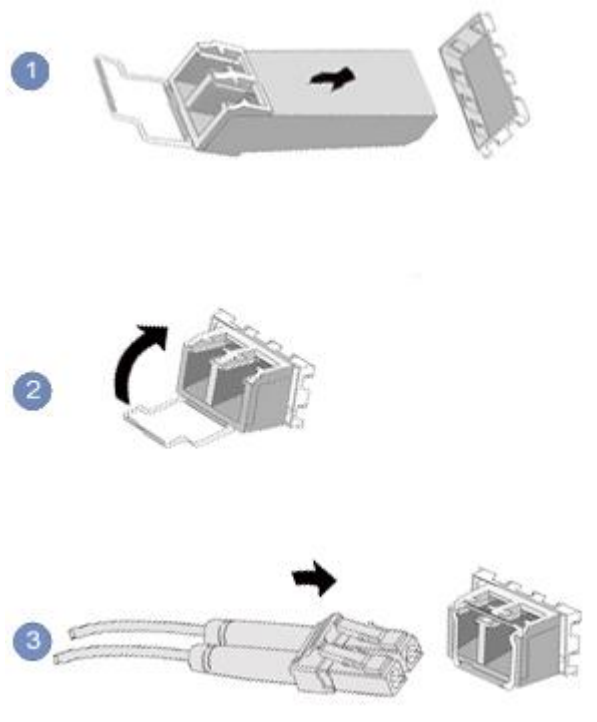
Step 4 Connect the cable to an optical port.

- When you use an optical cable:
 - a. Remove the optical cable to be replaced.
 - b. Connect the new optical cable.

 **NOTE**

- Connect the new optical cable to the same port as the removed one.
- Connect the optical cable to the optical module securely.
 - i. Insert the optical module into the optical port. See (1) in Figure 7-22.
 - ii. Close the latch on the optical module to secure it. See (2) in Figure 7-22.
 - iii. Insert the optical cable into the optical module. See (3) in Figure 7-22.

Figure 7-22 Connecting an optical cable

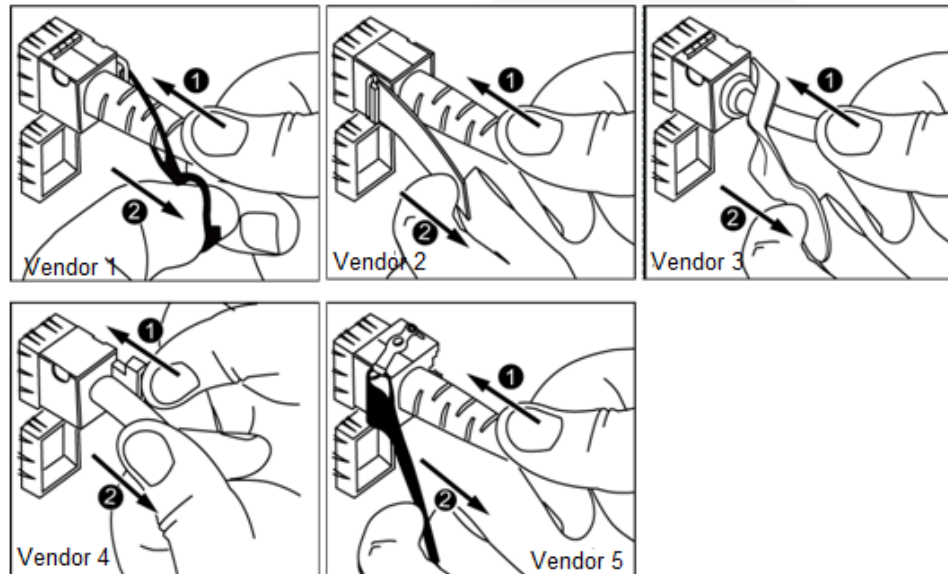


- When you use an SFP+ cable:
 1. Remove the SFP+ cable to be replaced.
Gently push the power connector inwards and pull the latch out to remove the SFP+ cable.

NOTICE

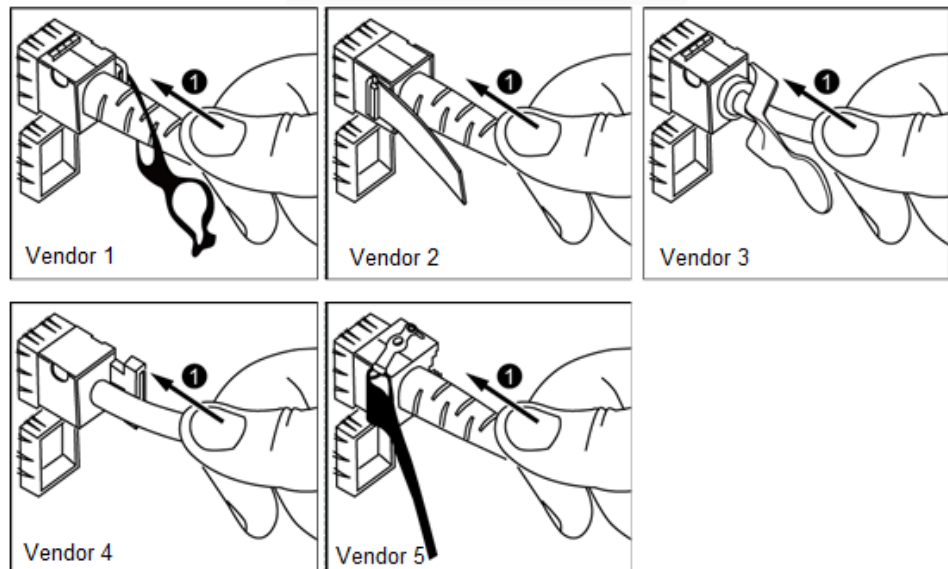
Do not directly pull out the latch.

Figure 7-23 Removing an SFP+ cable



2. Connect the new SFP+ cable.
Remove the dust-proof cap on the port, and insert the cable connector into the port. When you hear a "click" and the cable cannot be pulled out, the connector is secured.

Figure 7-24 Connecting an SFP+ cable



Step 5 Check whether the new cable is properly connected.

Power on the device. Check whether the port indicator is normal.

- If yes, go to [Step 7](#).
- If no, go to [Step 6](#).

Step 6 If the peer device cannot be pinged, check whether the cable is intact or the connector is securely connected.

- If yes, contact technical support.
- If no, replace the cable or insert the connector securely, and go to [Step 5](#).

Step 7 Bind the new optical cable.

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

----End

7.2.6.5 Connecting an IB Cable

Procedure

Step 1 Determine the model of the new cable.

You can use QSFP+ cables to connect IB cables.

Step 2 Number the new cable.

The number of the new cable must be the same as that of the old one.

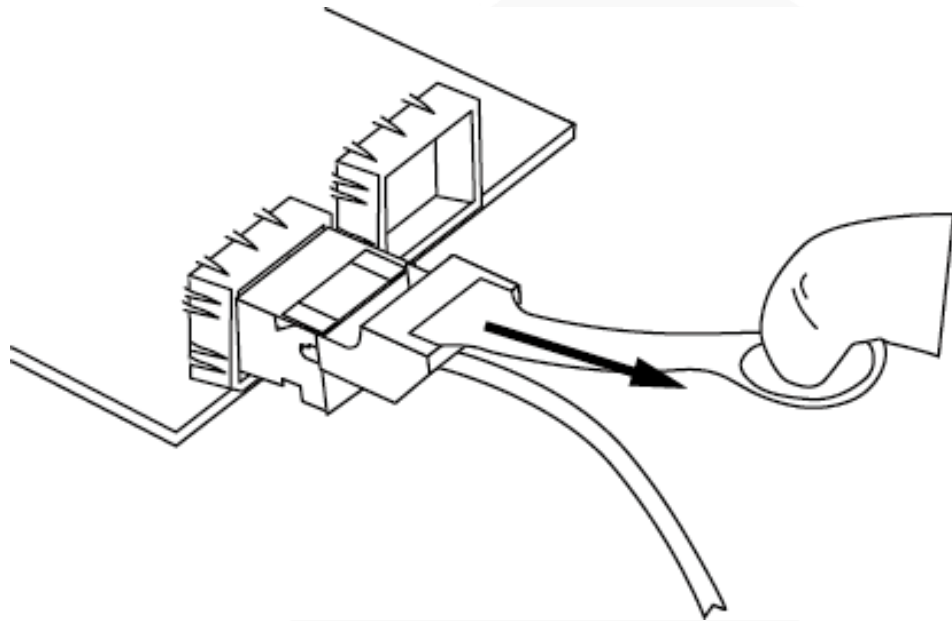
Step 3 Lay out the new cable.

- Lay out the new cable in the same way as the old one.
For example, if the old cable is laid out in underfloor cabling mode, so is the new cable.
- Lay out QSFP+ cables in the cabinet based on installation requirements.
You are advised to arrange cables in the same way as existing cables. Ensure that cables are routed neatly and undamaged.
- Separate QSFP+ cables from power cables and signal cables when laying out the cables.
- The minimum bend radius of QSFP+ cables is 4 cm (1.57 in.).
- Ensure that QSFP+ cables are routed for easy maintenance and capacity expansion.

Step 4 Replace the cable.

1. Remove the cable to be replaced.
Release the latch and remove the cable.

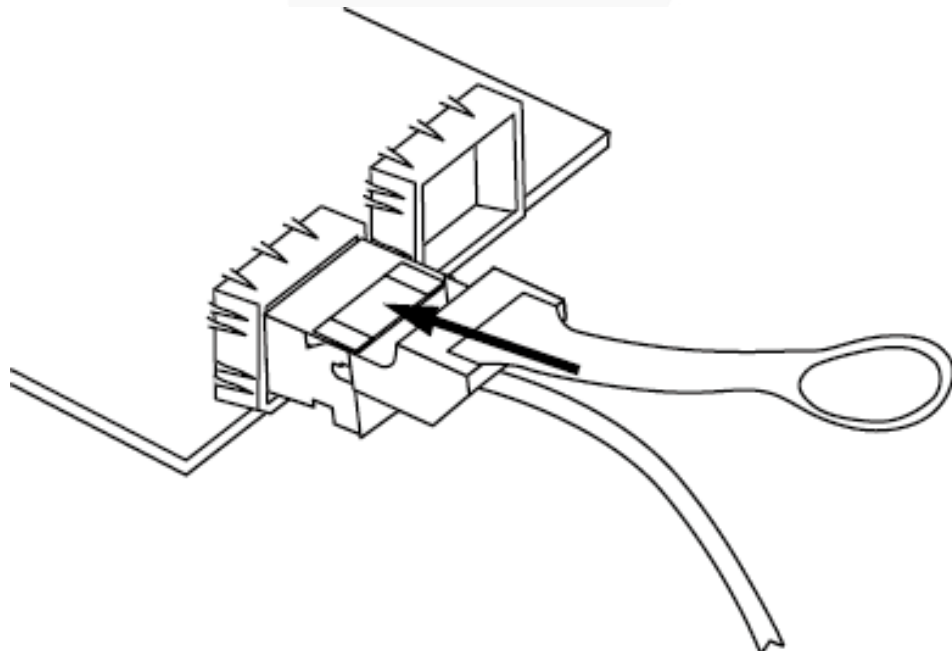
Figure 7-25 Removing a cable (for an IB NIC with two 56 Gbit/s ports as an example)



2. Connect the new cable.

Remove the dust-proof cap on the port, and insert the cable connector into the port. When you hear a "click" and the cable cannot be pulled out, the connector is secured.

Figure 7-26 Connecting a cable (for an IB NIC with two 56 Gbit/s ports as an example)



Step 5 Check whether the new cable is properly connected.

Power on the device. If the LOM indicator is green, the cable is properly connected.

----End

7.2.6.6 Connecting a USB Type-C Cable

The server panel provides an iBMC management port, which is connected to a PC or mobile phone through a USB Type-C cable to monitor and manage the system.

There are two types of USB Type-C cables:

- Both ends of the cable are USB Type-C ports.
- One end of the cable is a USB Type-C port, and the other end is a USB port.

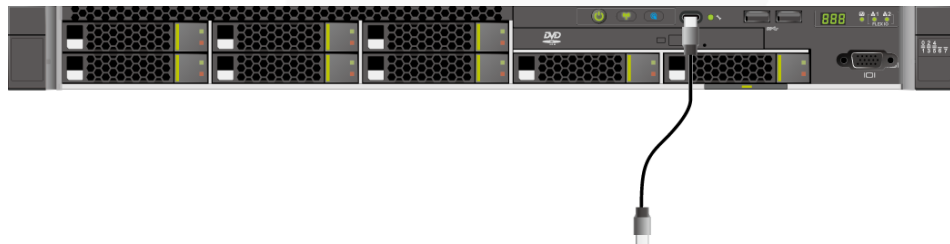
Procedure

Step 1 Connect the USB Type-C connector of the cable to the USB Type-C port on the server panel.

Step 2 Connect the other end of the adapter cable to a PC or mobile phone.

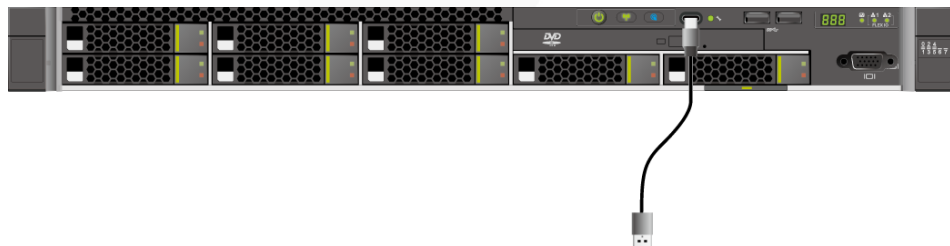
- Connect the other end of the adapter cable to the USB Type-C port on the laptop or mobile phone.

Figure 7-27 Connecting a cable to the USB Type-C port



- Connect the other end of the adapter cable to the USB port on the PC.

Figure 7-28 Connecting a USB Type-C to USB cable



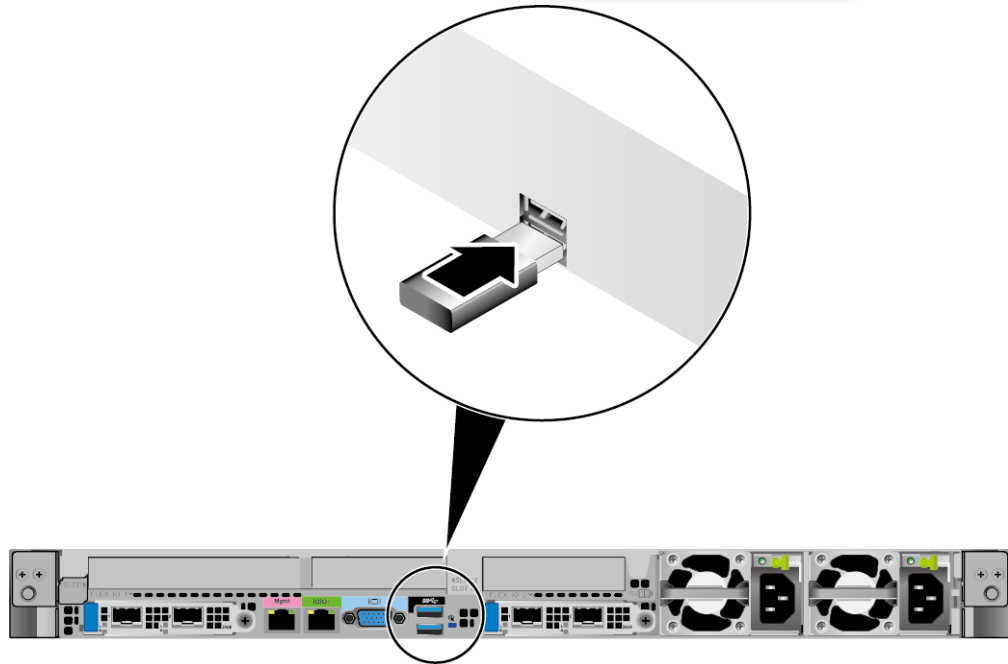
----End

7.2.6.7 Connecting a USB Device

Procedure

Step 1 Connect the USB device to a USB port of the server.

Figure 7-29 Connecting a USB device



----End

7.2.6.8 Connecting a Serial Cable

The rear panel of the server provides a standard RJ45 serial port (3-wire), which works as the OS serial port by default. You can set it as the iBMC serial port by using the iBMC CLI.

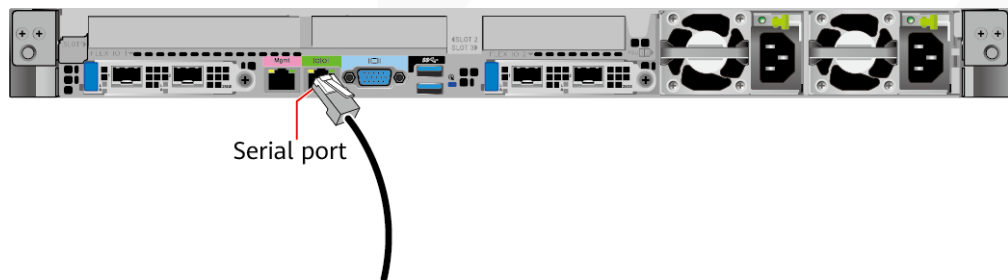
The serial port can be used as:

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

Procedure

Step 1 Connect the serial cable.

Figure 7-30 Connecting a serial cable



----End

7.2.6.9 Connecting PSU Cables

7.2.6.9.1 Connecting the AC PSU Cable

Before connecting power cables, ensure that the server has been correctly installed. For details, see 7.2.5 Installing a Server .

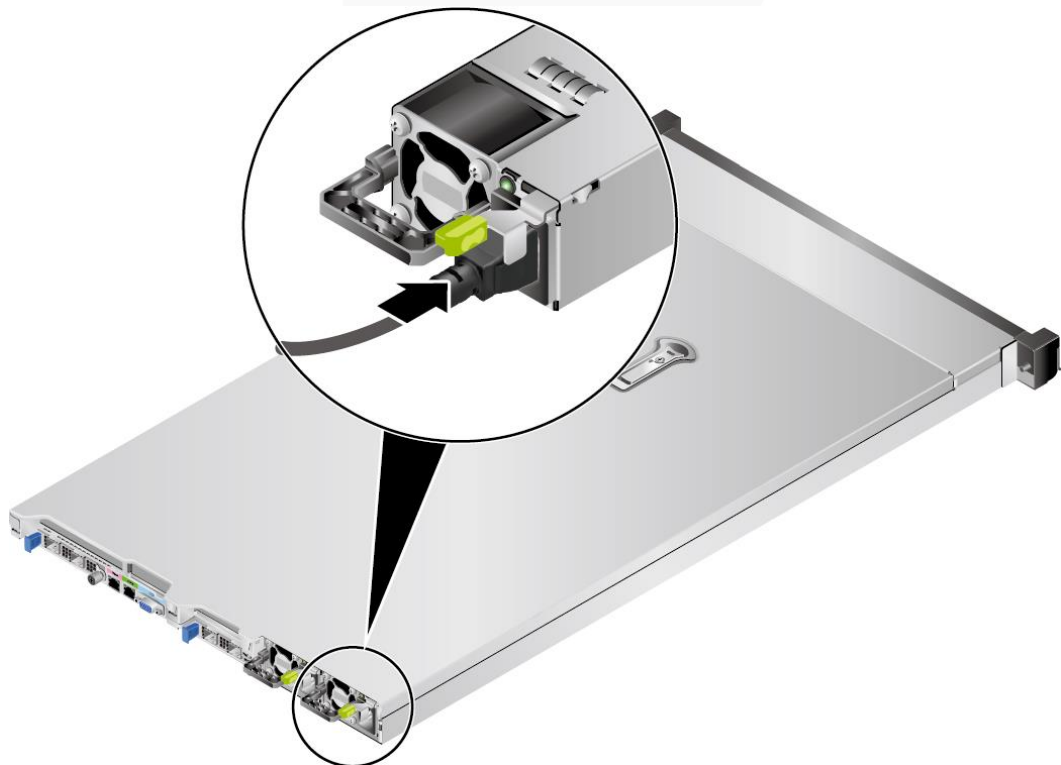
NOTICE

- 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 PDUs to ensure reliable system operation.
- Ground the equipment before powering it on. In AC or HVDC environment, the power cables of AC PSUs are grounded. Ensure that the power cables are in good contact.

Procedure

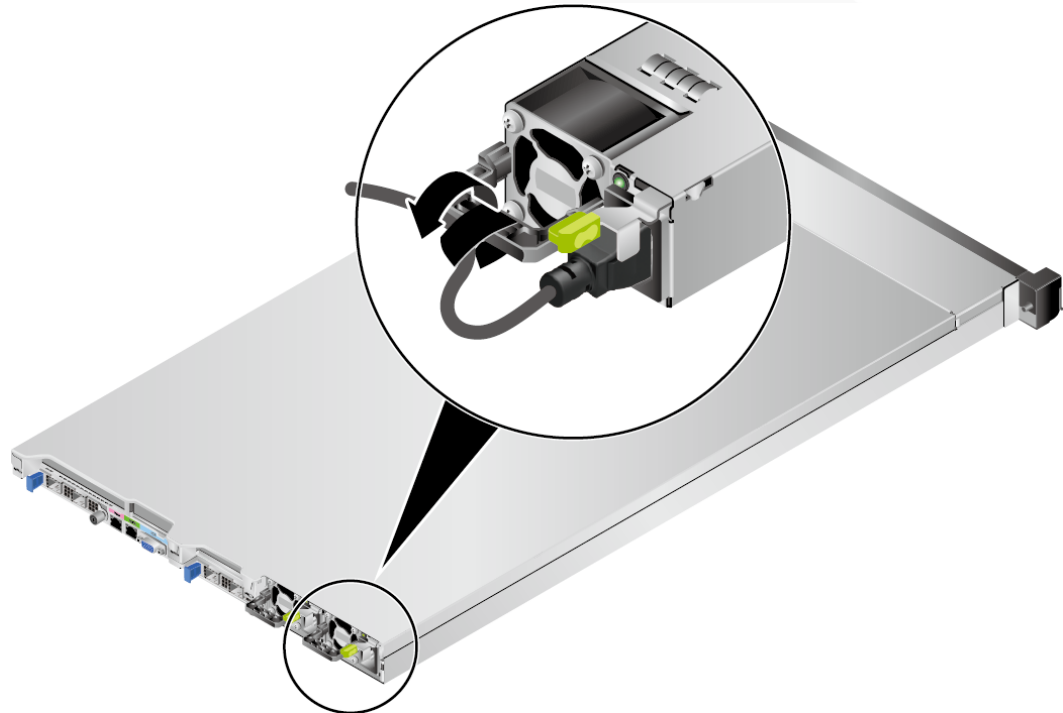
- Step 1** Take the component out of its ESD bag.
- Step 2** Connect one end of the power cable to the power socket on the PSU of the server.

Figure 7-31 Connecting the cable



- Step 3** Secure the power cable using a velcro strap.

Figure 7-32 Securing the cable



Step 4 Connect the other end of the power cable to the AC PDU in the cabinet.

The AC PDU is fastened in the rear of the cabinet. Connect the power cable to the nearest jack on the AC PDU.

Step 5 Bind the power cables to the cable guide using cable ties.

----End

7.2.6.9.2 Connecting the DC PSU Cable

Before connecting power cables, ensure that the server has been correctly installed. For details, see 7.2.5 Installing a Server .

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 PDUs to ensure reliable system operation.
 - Ground the equipment before powering it on. In DC environment, the ground terminals of DC PSUs are grounded. Ensure that the ground cables are in good contact.
-

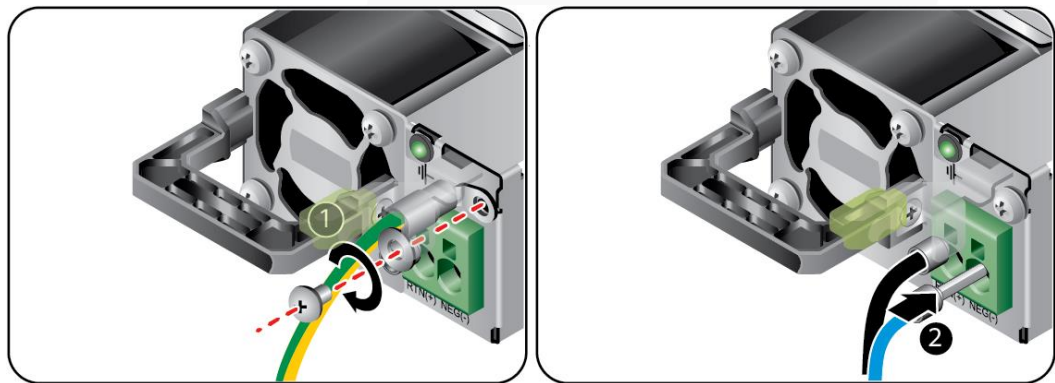
Procedure

Step 1 Take the component out of its ESD bag.

Step 2 Connect the cables to the PSU.

1. 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 7-33.
2. Insert the power cables to the wiring terminals on the PSU until the cables click into position. See (2) in Figure 7-33.
 - 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 7-33 Connecting cables



Step 3 Connect the other end of the power cable to the DC PDU in the cabinet.

The DC PDU is fastened in the rear of the cabinet. Connect the power cable to the nearest jack on the DC PDU.

Step 4 Bind the power cables to the cable guide using cable ties.

----End

7.2.6.10 Checking Cable Connections

CAUTION

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

Table 7-3 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 port or service ports on the rear panel of the chassis.
Ground cable	The server does not provide a separate ground port.

Item	Description
	<ul style="list-style-type: none">• In AC or HVDC environment, the power cables of AC PSUs are grounded. Ensure that the power cables are in good contact.• In DC environment, the ground terminals of DC PSUs are grounded. Ensure that the ground cables are in good contact.

7.3 Power-On and Power-Off

7.3.1 Powering On

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.
- During power-on, do not remove or insert server components or cables, such as drive modules, network cables, and console cables.
- If the power supply to a server is disconnected, wait for at least one minute before powering it on again.



The server can be powered on in any of the following ways:

- If PSUs are properly installed but are not connected to an external power supply, the server is powered off.
Connect the external power supply to the PSUs. Then the server will be powered on with the PSUs.

NOTE

System State Upon Power Supply is set to **Power On** by default, which indicates that the server automatically powers on after power is supplied to PSUs. You can log in to the iBMC WebUI, choose **System > Power > Power Control**, to view and change the setting,

- If the PSUs are powered on and the server is in standby state (the power indicator is steady yellow), use any of the following methods to power on the server:
 - Press the power button on the front panel.
For details, see 2.1.2 Indicators and Buttons .
 - Use the iBMC WebUI.
 - i. Log in to the iBMC WebUI.
For details, see 9.2 Logging In to the iBMC WebUI .
 - ii. Choose **System > Power > Power Control**.
The **Power Control** page is displayed.
 - iii. Click **Power On**.
A confirmation message is displayed.
 - iv. Click **OK**.

- The server starts to be powered on.
- Use the iBMC CLI.
 - i. Log in to the iBMC CLI.
For details, see 9.5 Logging In to the Server CLI.
 - ii. Run the following command:
ipmcset -d powerstate -v 1
 - iii. Type **y** or **Y** and press **Enter**.
The server starts to be powered on.
 - Use the Remote Virtual Console.
 - i. Log in to the Remote Virtual Console.
For details, see 9.4 Logging In to the Desktop of a Server.
 - ii. On the KVM screen, click  or  on the toolbar.
 - iii. Select **Power On**.
A dialog box is displayed.
 - iv. Click **OK**.
The server starts to be powered on.

7.3.2 Powering Off

NOTE

- The "power-off" mentioned here is an operation performed to change the server to the standby state (the power indicator is steady yellow).
- Powering off a server will interrupt all services and programs running on it. Therefore, before powering off a server, ensure that all services and programs have been stopped or migrated to other servers.
- After a server is powered off forcibly, wait for more than 10 seconds for the server to power off completely. Do not power on the server again before it is completely powered off.
- A forced power-off may cause data loss or program damage. Select an appropriate operation based on your actual situation.

The server can be powered off in any of the following ways:



- Connect a keyboard, video, and mouse (KVM) to the server and shut down the operating system of the server using the KVM.
- When the server is in power-on state, pressing the power button on the server front panel can power off the server gracefully.

NOTE

If the server OS is running, shut down the OS according to the onscreen instructions.

For details, see 2.1.2 Indicators and Buttons .

- When the server is in power-on state, holding down the power button on the server front panel for six seconds can power off the server forcibly.
For details, see 2.1.2 Indicators and Buttons .
- Use the iBMC WebUI.
 - a. Log in to the iBMC WebUI.
For details, see 9.2 Logging In to the iBMC WebUI .
 - b. Choose **System > Power > Power Control**.

- The **Power Control** page is displayed.
 - c. Click **Power Off** or **Forced Power Off**.
A confirmation message is displayed.
 - d. Click **OK**.
The server starts to be powered off.
 - Use the iBMC CLI.
 - a. Log in to the iBMC CLI.
For details, see 9.5 Logging In to the Server CLI.
 - b. Run the following command:
 - To power off the compute node gracefully, run the **ipmcset -d powerstate -v 0** command.
 - To power off the compute node forcibly, run the **ipmcset -d powerstate -v 2** command.
 - c. Type **y** or **Y** and press **Enter**.
The server starts to be powered off.
 - Use the Remote Virtual Console.
 - a. Log in to the Remote Virtual Console.
For details, see 9.4 Logging In to the Desktop of a Server.
 - b. On the KVM screen, click  or  on the toolbar.
 - c. Choose **Power Off** or **Forced Power Off**.
A dialog box is displayed.
 - d. Click **OK**.
The server starts to be powered off.

7.4 Initial Configuration

7.4.1 Default Information

Table 7-4 Default information

Category	Item	Default Value
iBMC management network port data	IP address and subnet mask of the management network port	<ul style="list-style-type: none"> • Default IP address: 192.168.2.100 <p>NOTE If the local PC is connected to the iBMC using a USB Type-C cable, the IP address of the iBMC management port is 169.254.1.5.</p> <ul style="list-style-type: none"> • Default subnet mask: 255.255.255.0
iBMC login data	User name and password	<ul style="list-style-type: none"> • Default user name: Administrator • Default password: Admin@9000
BIOS data	Password	<ul style="list-style-type: none"> • Default password: Admin@9000

7.4.2 Configuration Overview

Configuration Process

Figure 7-34 Initial configuration process

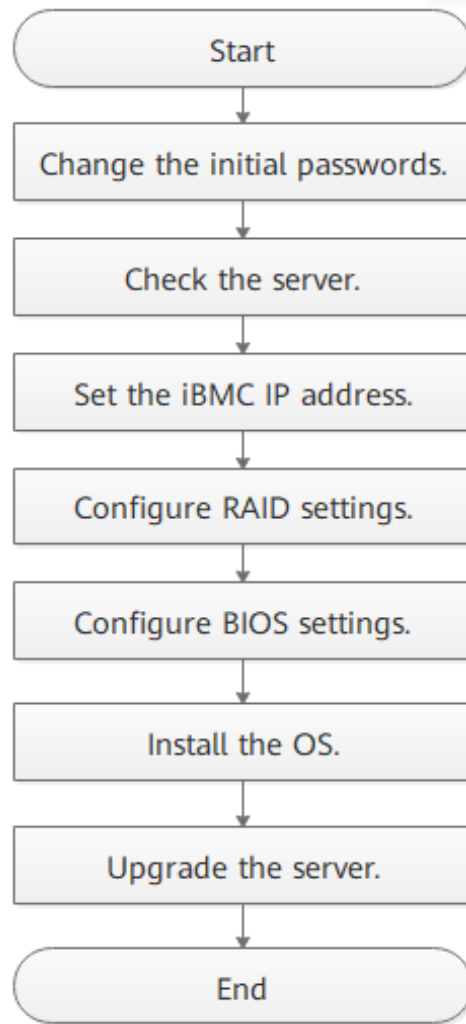


Table 7-5 Initial configuration process

Process	Description
Change the initial passwords.	Change the initial password of the default iBMC user.
Check the server.	<ul style="list-style-type: none"> • Ensure that the server version meets site requirements. • Ensure that no alarm is generated for the server.
Set the iBMC IP address.	Set an iBMC IP address for the server.
Configure RAID	Configure the RAID array based on service requirements.

Process	Description
settings.	
Configure BIOS settings.	Configure the BIOS of the server, including the boot sequence, NIC PXE function, and BIOS password.
Install the OS.	Install an OS for the server.
Upgrade the system.	Upgrade software and firmware, and install or update drivers to the latest versions.

Documents

- Configure the iBMC. The iBMC configuration method varies depending on the iBMC version. For details, see *Hard' Server iBMC User Guide*.
- For details about how to configure the RAID controller card, see the *V6 Server RAID Controller Card User Guide*.
- For details about how to configure the BIOS, see the *Server Whitley Platform BIOS Parameter Reference*.
- Install the OS. For details, see *Server OS Installation Guide*.
- Handle alarms.
- Rectify faults. For details, see *Servers Troubleshooting*.

7.4.3 Changing the Initial Password of the Default iBMC User

Scenario

This section describes how to change the initial password of the default iBMC user on the iBMC WebUI.

You can change the initial password of the default iBMC user on:

- iBMC WebUI
- iBMC CLI

For more information about the iBMC, see the *Hard' Server iBMC User Guide*.

NOTE

- The default user name of the iBMC is **Administrator**, and the default password is **Admin@9000**.
- For security purposes, change the initial password upon the first login and periodically change the password.
- For security purposes, enable password complexity check.
- The password complexity check function is enabled by default.

Procedure

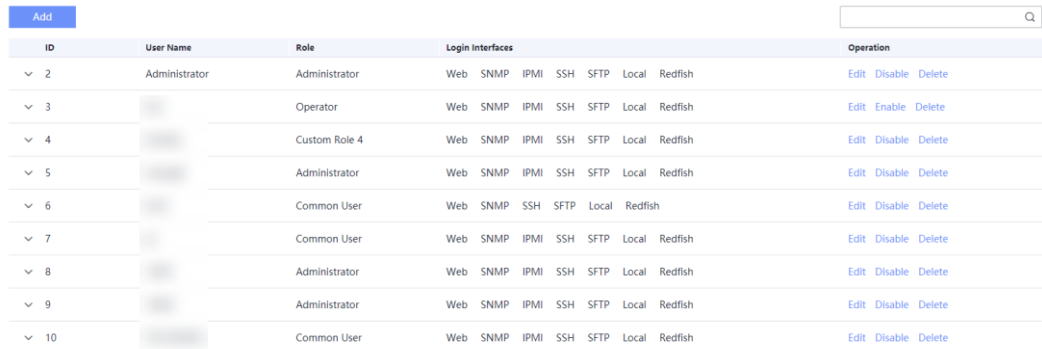
Step 1 Log in to the iBMC WebUI.

For details, see 9.2 Logging In to the iBMC WebUI .

Step 2 Choose **User & Security > Local Users**.

The **Local Users** page is displayed.

Figure 7-35 Local Users page



ID	User Name	Role	Login Interfaces	Operation
2	Administrator	Administrator	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete
3		Operator	Web SNMP IPMI SSH SFTP Local Redfish	Edit Enable Delete
4		Custom Role 4	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete
5		Administrator	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete
6		Common User	Web SNMP SSH SFTP Local Redfish	Edit Disable Delete
7		Common User	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete
8		Administrator	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete
9		Administrator	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete
10		Common User	Web SNMP IPMI SSH SFTP Local Redfish	Edit Disable Delete

Step 3 Click **Edit** on the right of the user whose password is to be changed.

The **Edit User** page is displayed.

Figure 7-36 Edit User page

Edit User

User Name: Administrator

Password: []

Confirm Password: []

Role: Administrator

Login Rules:

- Rule 1 Login time: -- to -- IP: -- MAC: --
- Rule 2 Login time: -- to -- IP: -- MAC: --
- Rule 3 Login time: -- to -- IP: -- MAC: --

[Go to Security Management to modify login rules.](#)

Login Interfaces: SNMP SSH IPMI Local SFTP Web Redfish

SNMPv3 Encryption Password

The SNMPv3 encryption password has not been initialized and will be synchronized with the user login password. You are advised to change the SNMPv3 encryption password for security purposes.

SNMPv3 Encryption Password: []

Confirm Password: []

* Current User Password: []

Save Cancel

Step 4 Enter a new password in the **Password** and **Confirm Password** text boxes.

NOTE

The password must meet the following requirements:

- Contain 8 to 20 characters.
- Contain 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 in reverse order.

Step 5 Enter the current password in the **Current User Password** text box.

Step 6 Click **Save**.

The initial password of the iBMC is changed.

----End

7.4.4 Checking the Server

Scenario

This section describes how to check the server on the iBMC WebUI.

You can check the server on:

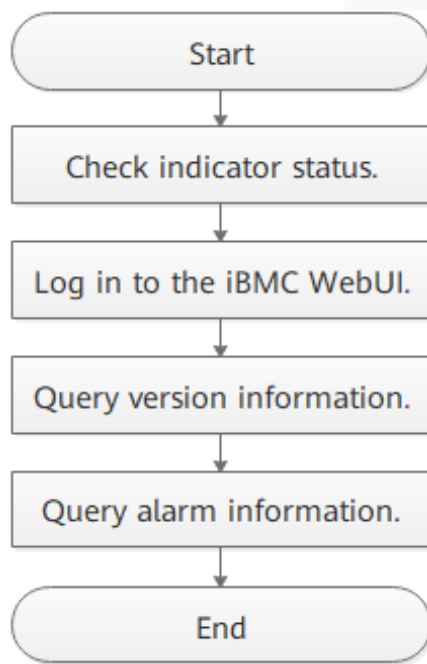
- iBMC WebUI
- iBMC CLI

For more information about the iBMC, see the *Hard' Server iBMC User Guide*.

Workflow

Check the server by performing the following operations:

Figure 7-37 Check process



Procedure

Step 1 Determine the hardware status by observing the indicators on the front panel.

For details, see 2.1.2 Indicators and Buttons .

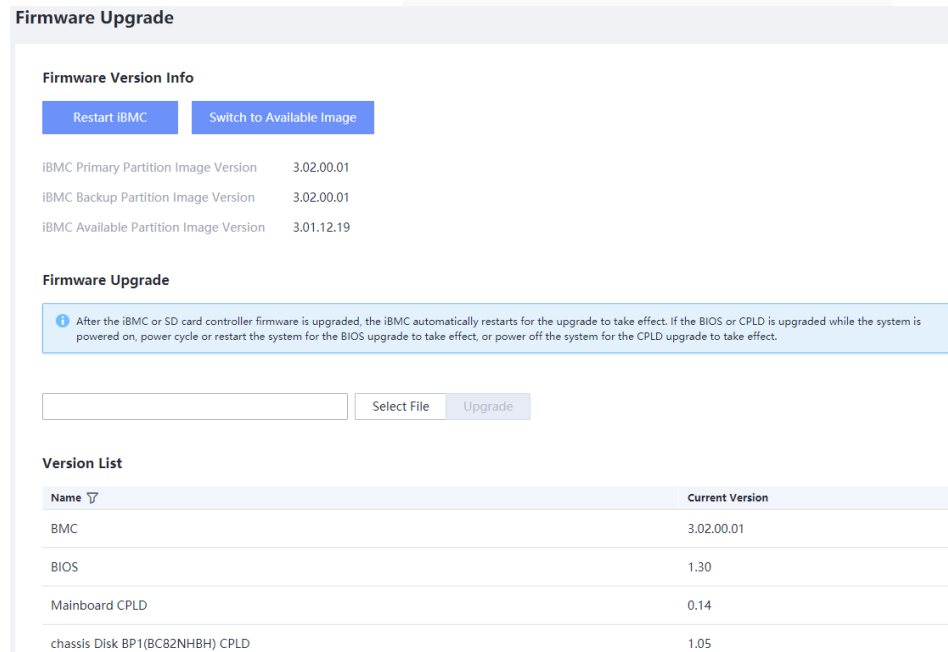
Step 2 Log in to the iBMC WebUI.

For details, see 9.2 Logging In to the iBMC WebUI .

Step 3 Query version information.

1. On the iBMC home page, choose **iBMC Settings > Firmware Upgrade**. The **Firmware Version Info** page is displayed.

Figure 7-38 Firmware Version Info page



2. Check whether the versions meet site requirements.
 - If yes, go to [Step 4](#).
 - If no, go to [Step 3.3](#).
3. Upgrade the firmware to the target version.


Step 4 Query alarm information.

1. On the menu bar, choose **Maintenance**.
2. In the navigation tree on the left, choose **Alarm&Event** and check whether there are alarms under **Current Alarms**

Figure 7-39 Querying health status

No.	Severity	Object Type	Event Code	Generated	Description	Handling Sugges...
3	Minor	BMC	0x1A000045	2021-08-10 14:42:12	get description failed	
2	Major	Disk Backplane	0x05000001	2021-08-05 17:17:23	Power supply to front disk backplane 5V failed.	View
1	Minor	System	0x2C000073	2021-07-16 14:42:07	The total power consumption (228.000 W) of the system exceeds the alarm ...	View

- If yes, handle the alarms.
 - indicates a critical alarm, which may power off the server and even interrupt services. Corrective actions must be taken immediately.
 - indicates a major alarm, which may affect the normal operating of the system or interrupt services.

-  indicates a minor alarm, which has minor impact on the system but requires corrective action as soon as possible. Otherwise, a more severe alarm will be generated.
- If no, no further action is required.

----End

7.4.5 Configuring the BMC IP Address

Scenario

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

You can set the iBMC IP address on:

- BIOS
- iBMC WebUI
- iBMC CLI

Run the **ipmcset -d ipaddr** command.

For more information about the iBMC, see the *Hard' Server iBMC User Guide*.

Default IP Address

Default IP Address	Default Subnet Mask
192.168.2.100	255.255.255.0

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

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

The **iBMC Configuration** screen is displayed,

Step 3 Select **iBMC IPv4/IPv6 Configuration** and press **Enter**.

The **iBMC IPv4/IPv6 Configuration** screen is displayed, showing the iBMC IP address.

Step 4 Select the IP address to be configured.

- To configure an IPv4 address, select **IPv4 IP Address** and press **Enter**.
The IPv4 address configuration screen is displayed.
- To configure an IPv6 address, select **IPv6 Static IP Address** and press **Enter**.
The IPv6 address configuration screen is displayed.

Step 5 Set the iBMC IP address

Step 6 Press **F10**.

"Exit Saving Changes?" is displayed.

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

The server automatically restarts for the settings to take effect.

----End

7.4.6 Configuring RAID

The 1288H V6 supports multiple types of RAID controller cards.

- For details about the compatible RAID controller cards, see "Search Parts" in the [Compatibility Checker](#).
- For details about how to configure the RAID controller card, see the *V6 Server RAID Controller Card User Guide*.

7.4.7 Configuring the BIOS

This section describes how to configure the BIOS of the server.

To configure the BIOS, perform the following operations:

- Set the system boot sequence
- Set PXE for a NIC
- Set the BIOS password
- Select a language

For details about other configuration items, see the *Server Whitley Platform BIOS Parameter Reference*.

7.4.7.1 Setting the System Boot Sequence

If multiple boot devices are configured for the server, you can set the system boot sequence on the BIOS.

NOTE

If the BIOS password is enabled, this operation is supported only when you enter the **Setup Utility** screen using the BIOS administrator password.

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Boot**.

The **Boot** screen is displayed.

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

The **Boot Type** dialog box is displayed.

Step 4 Select **Legacy Boot Type** or **UEFI Boot Type** and press **Enter**.

 **NOTE**

- The UEFI mode is used by default.
- For some OSs, if the capacity of the drive or RAID array for installing the OS is greater than 2 TB, use the UEFI mode. For details, see the release notes of the OS.
- If the OS is installed on an NVMe drive, the boot mode must be the UEFI boot.
- The UEFI mode supports more boot devices than the legacy mode. If a server is configured with multiple boot devices, some devices may fail to start in legacy mode. In this case, the UEFI mode is recommended. If the legacy mode needs to be set, disable serial port redirection or NIC PXE function based on service requirements so that the OS can start. For details, see "Setting PXE for a NIC" and "Setting Serial Port Redirection" in *Server Whitley Platform BIOS Parameter Reference*.

Step 5 Select **Boot Sequence** and press **Enter**.

The **Boot Sequence** screen is displayed.

 **NOTE**

The default boot sequence is **Hard Disk Drive > DVD-ROM Drive > PXE > Other Device**.

Step 6 Select the target boot option and press **F5** or **F6** to change the boot sequence.

- Press **F5** to move a boot option down.
- Press **F6** to move a boot option up.

 **NOTE**

- The server boots in the order specified on this screen.
- You can click the switch button on the right of a boot option to enable or disable the boot option.

Step 7 Press **F10**.

"Exit Saving Changes?" is displayed.

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

The server automatically restarts for the settings to take effect.

----End

7.4.7.2 Setting PXE for a NIC

7.4.7.2.1 Setting PXE for an OCP 3.0 NIC

Enable or disable the PXE function for the OCP 3.0 network adapter in a FlexIO card slot on the BIOS.

 **NOTE**

If the BIOS password is enabled, this operation is supported only when you enter the **Setup Utility** screen using the BIOS administrator password.

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Advanced**.

The **Advanced** screen is displayed.

Step 3 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed.

 **NOTE**

The 1288H V6 supports a maximum of two OCP 3.0 network adapters. (Each OCP 3.0 network adapter supports a maximum of two network ports, that is, a maximum of four network ports are supported.)

- In UEFI mode, the default value is **Enabled** for all network ports by default.
- In Legacy mode, only the first network port of each NIC is enabled by default. That is, the default value is **Enabled** for PXE Port1 and **Disabled** for PXE Port2.

Step 4 Select the network port of the OCP 3.0 network adapter to be configured and press **Enter**.

The dialog box for setting the network port is displayed.

Step 5 In the dialog box displayed, select **Enabled** or **Disabled** and press **Enter**.

- **Enabled**: enables the PXE function for the network port.
- **Disabled**: disables the PXE function for the network port.

Step 6 Press **F10**.

"Exit Saving Changes?" is displayed.

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

The server automatically restarts for the settings to take effect.

----End

7.4.7.2.2 Setting PXE for a PCIe NIC

Enable or disable the PXE function for a PCIe NIC on the BIOS.

 **NOTE**

If the BIOS password is enabled, this operation is supported only when you enter the **Setup Utility** screen using the BIOS administrator password.

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Advanced**.

The **Advanced** screen is displayed.

Step 3 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed.

Step 4 Select **Slot PXE Control** and press **Enter**.

Step 5 In the dialog box displayed, select **Enabled** or **Disabled** and press **Enter**.

- **Enabled**: enables the PXE function for the PCIe NIC.

 **NOTE**

After the PXE function is enabled, you can enable or disable the PXE function for a specific network port (for example, CPU2 First Slot Port1) on the PCIe NIC.

- **Disabled:** disables the PXE function for the PCIe NIC.

 **NOTE**

After the PXE function of a PCIe NIC is disabled, the PXE configuration menu of a single PCIe NIC port is hidden and cannot be configured.

Step 6 Select the PCIe NIC network port to be configured and press **Enter**.

The dialog box for setting the network port is displayed.

Step 7 In the dialog box displayed, select **Enabled** or **Disabled** and press **Enter**.

- **Enabled:** enables the PXE function for the network port.
- **Disabled:** disables the PXE function for the network port.

Step 8 Press **F10**.

"Exit Saving Changes?" is displayed.

Step 9 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

7.4.7.3 Setting the BIOS Password

7.4.7.3.1 Setting the Password of the BIOS Administrator

For security purposes, change the administrator password upon the first login.

 **NOTE**

- The password complexity check function is enabled by default.
- For security purposes, enable password complexity check.
- For security purposes, change the administrator password periodically.
- If the BIOS password is enabled, this operation is supported only when you enter the **Setup Utility** screen using the BIOS administrator password.

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Security**.

The **Security** screen is displayed.

Step 3 Select **Set Supervisor Password** and press **Enter**.

The page for changing the administrator login password is displayed.

Step 4 Enter the BIOS administrator password, new password, and confirm password, and click **Yes**.

 **NOTE**

- The current password of the system administrator is required before you change the password. The system will be locked if an incorrect password is entered three consecutive times. You can unlock the system by restarting it.
- The default BIOS password is **Admin@9000**.
- The requirements for setting the password are as follows:
- The password must be a string of 8 to 16 characters and contain special characters (including spaces) and at least two types of uppercase letters, lowercase letters, and digits.
- The new password cannot be the same as the previous five passwords and cannot be set to the default password.
- The administrator password cannot be the same as the common user password.
- After the administrator password is set, the **Delete Supervisor Password** parameter is displayed, which can be used to clear the configured BIOS administrator password. Clearing the administrator password will reduce system security. Exercise caution when performing this operation.
- If **Simple Password** is set to **Enabled**, the system does not verify the password complexity, but the password length must be 8 to 16 digits.
- Enabling the simple password function reduces system security. Exercise caution when enabling this function.

Step 5 Press **F10**.

"Exit Saving Changes?" is displayed.

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

The server automatically restarts for the settings to take effect.

----End

7.4.7.3.2 Setting the Password of a Common BIOS User

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Security**.

The **Security** screen is displayed.

Step 3 Select **Set User Password** and press **Enter**.

The page for changing the password of a common user is displayed.

Step 4 Enter the password and confirm password of the common user, and click **Yes**.

 **NOTE**

- If a common user password already exists, you need to enter the password.
- The requirements for setting the password are as follows:
- The password must be a string of 8 to 16 characters and contain special characters (including spaces) and at least two types of uppercase letters, lowercase letters, and digits.
- The new password cannot be the same as the previous five passwords and cannot be set to the default password.
- The administrator password cannot be the same as the common user password.

- After the password of a common BIOS user is set, the **Delete User Password** parameter is displayed, which can be used to clear the configured password of the common BIOS user.
- If **Simple Password** is set to **Enabled**, the system does not verify the password complexity, but the password length must be 8 to 16 digits.
- Enabling the simple password function reduces system security. Exercise caution when enabling this function.

Step 5 Press **F10**.

"Exit Saving Changes?" is displayed.

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

The server automatically restarts for the settings to take effect.

----End

7.4.7.4 Setting the Language

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Main**.

The **Main** screen is displayed.

Step 3 Select **Language** and press **Enter**.

The **Language** screen is displayed.

Step 4 Select the language to be used and press **Enter**.

The target language is set for the GUI.

Step 5 Press **F10**.

"Exit Saving Changes?" is displayed.

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

The server automatically restarts for the settings to take effect.

----End

7.4.8 Installing an OS

The 1288H V6 supports multiple types of OSs.

- For details about the compatible OSs, see "Search OSs" in the [Compatibility Checker](#).
- For details about how to install the OS, see *Server OS Installation Guide*.

7.4.9 Upgrading the System

NOTICE

Unless the software or components to be installed require an earlier version, keep the system in the latest state before using the server for the first time.

Obtaining Related Documents

- *Release Notes*
- *Server OS Installation Guide*

Upgrading Software or Firmware

- Upgrade the iBMC, BIOS, CPLD, and other firmware.

Installing or Updating the Driver

If the driver versions on the server are inconsistent with the driver list or some chip drivers are not installed, install the drivers of the required versions. Otherwise, the server may operate abnormally.

- Obtain the driver installation package. For details, see "Search OSs" in the [Compatibility Checker](#).
- Install or upgrade the driver. For details, see *Server OS Installation Guide*.

NOTICE

Back up the original drivers before installing or upgrading the drivers.

The driver installation package and procedure vary depending on the operating system.

8 Troubleshooting Guide

For details about how to troubleshoot servers, see the *Server Troubleshooting*. It covers the following content:

- **Troubleshooting process**
Use appropriate methods to find the cause of a fault and rectify the fault. Analyze possible causes for a fault and narrow down the scope 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 according to 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**
Check for, diagnoses, and rectifies server faults through routine preventive maintenance inspection.

9 Common Operations

- 9.1 Querying the iBMC IP Address
- 9.2 Logging In to the iBMC WebUI
- 9.3 Logging In to the SmartServer
- 9.4 Logging In to the Desktop of a Server
- 9.5 Logging In to the Server CLI
- 9.6 Managing VMD
- 9.7 Accessing the BIOS
- 9.8 Clearing Data from a Storage Device

9.1 Querying the iBMC IP Address

Scenario

This section describes how to query the IP address of the iBMC management network port on the BIOS.

You can query the IP address of the iBMC management network port on:

- BIOS
- iBMC WebUI
- iBMC CLI

Run the **ipmcget -d ipinfo** command.

For more information about the iBMC, see the *Hard'Server iBMC User Guide*.

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

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

The **iBMC Configuration** screen is displayed.

Step 3 Select **iBMC IPv4/IPv6 Configuration** and press **Enter**.

The **iBMC IPv4/IPv6 Configuration** screen is displayed.

Step 4 Check the IP address of the iBMC management network port.

----End


9.2 Logging In to the iBMC WebUI

Scenario

Log in to the iBMC WebUI. The following uses Internet Explorer 11.0 as an example.

- A maximum of four users can log in to the WebUI at the same time.
- By default, the system timeout period is 5 minutes. If no operation is performed on the WebUI within 5 minutes, the user will be automatically logged out of the WebUI.
- The system locks a user account if the number of consecutive incorrect password attempts reaches the maximum for the user account. The user account is automatically unlocked after the locking duration reaches the value specified.
- For security purposes, change the initial password upon the first login and change the password periodically.
- If resources fail to be obtained due to unstable network connection, the iBMC WebUI may be displayed abnormally. If this occurs, refresh the browser and log in to the iBMC WebUI again.

NOTE

- If TLS version is set to **Only TLS 1.3** on the **User & Security > Security Management** page, the following browser versions are not supported:
 - All Internet Explorer versions
 - Safari 11.0 to 12.0
 - Microsoft Edge 12 to 18
 - Before using Internet Explorer to log in to the iBMC WebUI, enable the compatibility view and select "Use TLS 1.2".
 - Enable the compatibility view:
 - Click  in the upper right corner of the browser.
 - 1. On the shortcut menu displayed, click **Compatibility View Settings**.
 - 2. In the **Compatibility View Settings** dialog box displayed, enter the iBMC IP address in the **Add this website** text box and click **Add**.
 - 3. Deselect **Use Microsoft compatibility lists**.
- After the iBMC IP address is added to the compatibility view, improper display on the iBMC WebUI will be rectified.
- Select "Use TLS 1.2" as follows:
 - Choose **Internet Options > Advanced**.

1. In the **Security** area, select **Use TLS 1.2**.

Procedure

Step 1 Check that the client (for example, a local PC) used to access the iBMC meets the operating environment requirements.

If you want to use the Java Integrated Remote Console, ensure that the Java Runtime Environment (JRE) meets requirements.

Table 9-1 Operating environment

OS	Web Browser	Java Runtime Environment (JRE)
Windows 7 (32-bit) Windows 7 (64-bit)	Internet Explorer 11.0 or later	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
Windows 8 (32-bit) Windows 8 (64-bit)	Mozilla Firefox 63.0 or later	
Windows Server 2008 R2 (64-bit)	Google Chrome 70.0 or later	
Windows Server 2012 (64-bit)		
Windows Server 2012 R2 (64-bit)		
Windows Server 2016 (64-bit)		
Windows 10 (64-bit)	Internet Explorer 11.0 or later	
	Microsoft Edge	
	Mozilla Firefox 63.0 or later	
	Google Chrome 70.0 or later	
CentOS 7	Mozilla Firefox 63.0 or later	
MAC OS X v10.7	Safari 11.0 and later	
	Mozilla Firefox 63.0 or later	

Step 2 Configure an IP address and subnet mask or route information for the local PC to enable communication with the iBMC management network port.

Step 3 Connect the local PC to the iBMC using any of the following methods:

- Connect the local PC to the iBMC management network port using a network cable.
- Connect the local PC to the iBMC management network port over a LAN.

- Connect the local PC to the iBMC direct connect management port using a USB Type-C cable.

 **NOTE**

- Only servers configured with the iBMC direct management port support this operation.
- If you use a USB Type-C cable to connect the local PC to the iBMC direct connect management port, the local PC can run only Windows 10.

Step 4 Choose **Control Panel > Network and Internet > Network Connections**, and check whether the local PC is connected to the iBMC network.

 **NOTE**

- If the local PC is connected to the iBMC using a USB Type-C cable, the iBMC network name is **Remote NDS Compatible Device**.
- If the local PC is connected to the iBMC using a network cable or over a LAN, the iBMC network name varies depending on the NIC used on the local PC.
- If yes, go to [Step 5](#).
- If no, contact technical support for assistance.

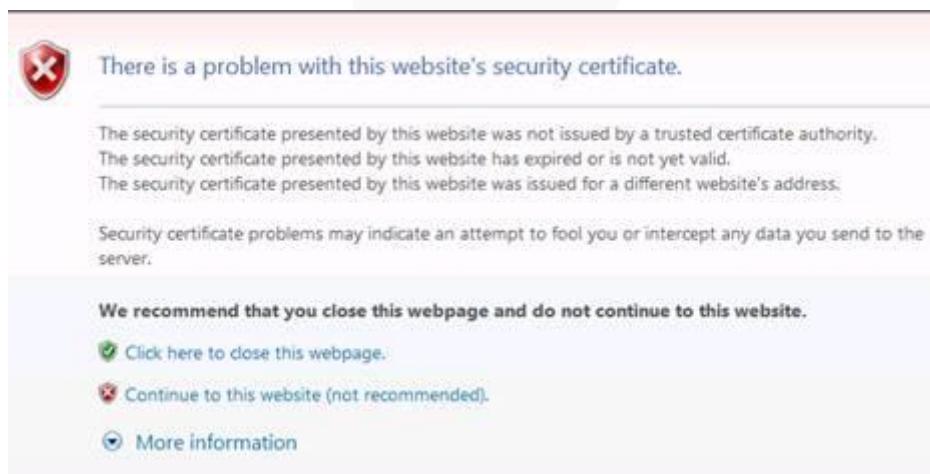
Step 5 Open Internet Explorer, enter **https://iBMC management network port IP address** in the address box, and press **Enter**.

 **NOTE**

- If the local PC is connected to the iBMC direct connect management port using a USB Type-C cable, the IP address of the iBMC management network port is **169.254.1.5**.
- If the local PC is connected to the iBMC management network port using a network cable or over a LAN, the default IP address of the iBMC management network port is **192.168.2.100**.
- Enter the IP address of the iBMC management network port based on actual situation:
- If an IPv6 address is used, use [] to enclose the IPv6 address, for example, [fc00::64].
- If an IPv4 address is used, enter the IPv4 address, for example, **192.168.100.1**.

A security alert dialog box is displayed.

Figure 9-1 Security warning



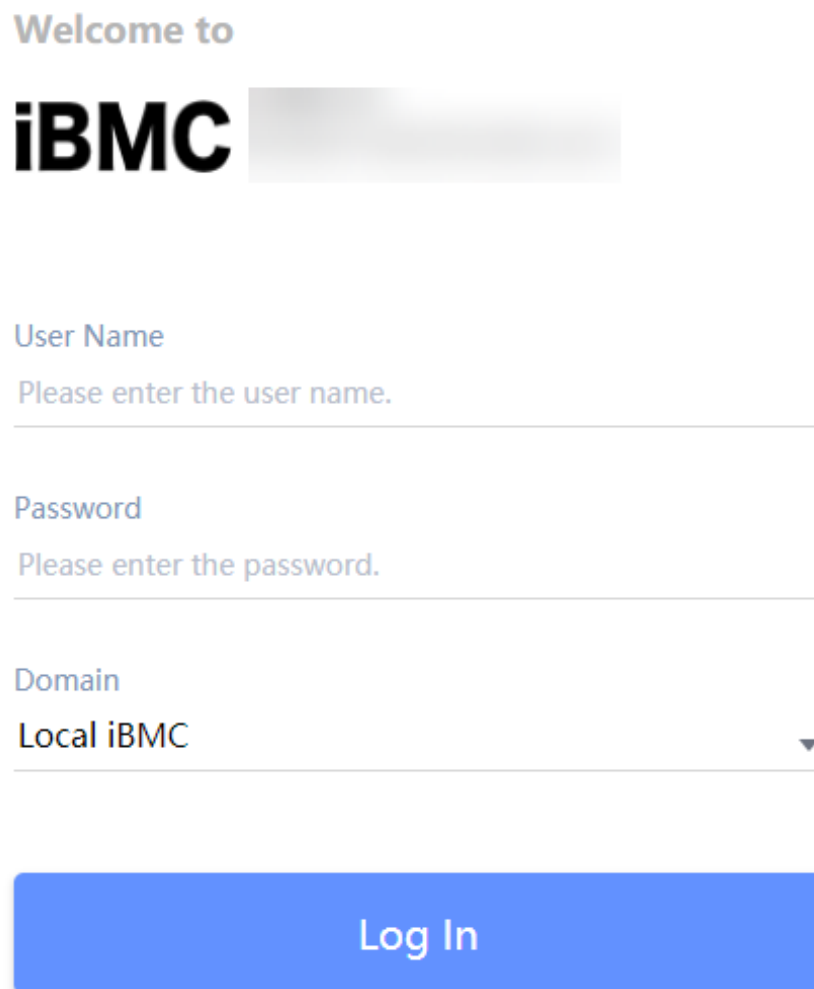
 **NOTE**

- If a security alert is displayed, you can ignore this message or perform any of the following to shield this alert:
- Import a trust certificate and a root certificate to the iBMC.
For details, see "Importing the iBMC Trust Certificate and Root Certificate" in the iBMC user guide of the server you use.
- If no trust certificate is available and network security can be ensured, add the iBMC to the **Exception Site List on Java Control Panel** or reduce the Java security level.
This operation poses security risks. Exercise caution when performing this operation.

Step 6 Click **Continue to this website (not recommended)**.

The iBMC login page is displayed.

Figure 9-2 iBMC login page



The screenshot shows the iBMC login page. At the top, it says "Welcome to" followed by the iBMC logo and a blurred area. Below the logo, there are three input fields: "User Name" with the prompt "Please enter the user name.", "Password" with the prompt "Please enter the password.", and "Domain" with a dropdown menu currently showing "Local iBMC". At the bottom, there is a large blue button labeled "Log In".

Table 9-2 User login

Parameter	Description
Username	<p>Username for logging in to the iBMC WebUI.</p> <ul style="list-style-type: none"> When Domain is Local iBMC, the maximum length of the user name is 20 characters. When Domain is not Local iBMC, the maximum length of the user name is 255 characters. <p>Pay attention to the following points when logging in to the system:</p> <ul style="list-style-type: none"> When you log in to the iBMC as a local user, you can set Domain to Local iBMC or Automatic matching. To log in as an LDAP user, the user name can be in either of the following formats: <ul style="list-style-type: none"> LDAP user name (In this case, Domain can be Automatic matching or a specified domain.) LDAP user name@Domain name (In this case, Domain can be Automatic matching or a specified domain.) To log in as a Kerberos user, the user name can be in either of the following formats: <ul style="list-style-type: none"> Kerberos user name (in this case, Domain can be Automatic matching or a specified domain) Kerberos user name@domain name (in this case, Domain can be Automatic matching or a specified domain, and uppercase letters must be used in the domain name) Both Kerberos user name and Kerberos user name@Domain name formats support single sign-on (SSO).
Password	<p>Password of the login user. For security purposes, periodically change your login password.</p> <p>NOTE</p> <p>When you log in to the iBMC WebUI as an LDAP or Kerberos user, the password can contain a maximum of 255 characters.</p>

Step 7 Log in to the iBMC WebUI.

- Log in to the WebUI as a local user.
- Logging in as a Lightweight Directory Access Protocol (LDAP) User
- To log in to the iBMC WebUI as a Kerberos user, perform the following steps:

----End

Log in to the WebUI as a local user.

Step 1 (Optional) On the login page, switch to the target language.

Step 2 Enter the user name and password for logging in to the iBMC WebUI. For details, see Table 9-2.

 **NOTE**

The default user name for logging in to the iBMC system is **Administrator**, and the default password is **Admin@9000**.

Step 3 Select **Local iBMC** or **Automatic matching** from the **Domain** drop-down list.

Step 4 Click **Log In**.

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

 **NOTE**

- If you use Internet Explorer to log in to the iBMC WebUI for the first time after an upgrade, the system may display a message indicating that the login fails due to incorrect user name or password. If this occurs, press **Ctrl+Shift+Delete**, and click **Delete** in the dialog box displayed to clear the cache of Internet Explorer. Then, attempt to log in again.
- If you cannot log in to the iBMC WebUI using Internet Explorer, choose **Tools > Internet Options > Advanced** and click **Reset**. Then you can log in to the iBMC WebUI.

----End

Logging in as a Lightweight Directory Access Protocol (LDAP) User

Before login, ensure that the following settings meet the requirements:

- A domain controller exists on the network, and a user domain and LDAP users have been created on the domain controller.

 **NOTE**

For details about how to create a domain controller, a user domain, and LDAP users who belong to the user domain, see related documents about the domain controller. The iBMC provides only the access function for LDAP users.

- On the **User & Security > LDAP** page of the iBMC WebUI, the LDAP function is enabled, and the user domain and the LDAP user who belong to the user domain are set.

Step 1 (Optional) On the iBMC login page, switch to the target language.

Step 2 Enter the LDAP user name and password for logging in to the iBMC WebUI. For details, see Table 9-2.

 **NOTE**

- To log in as an LDAP user, the user name can be in either of the following formats:
- LDAP user name (In this case, **Domain** can be **Automatic matching** or a specified domain.)
- LDAP user name@Domain name (In this case, **Domain** can be **Automatic matching** or a specified domain.)
- When you log in to the iBMC WebUI over LDAP, the password can contain a maximum of 255 characters.

Step 3 Select the LDAP user domain from the Domain drop-down list.

 **NOTE**

The Domain drop-down list contains the following options:

- **This iBMC**: Select this option to log in as a local user. The system automatically locates the user from the local user list.
- **Configured domain servers**: Select a domain server to log in as an LDAP user. The system automatically locates the user from the domain server.

- **Automatic matching:** If this option is selected, the system searches for the user from the local user list first. If no match is found, the system searches from the domain servers in the sequence displayed in the **Domain** drop-down list.

Step 4 Click Log In.

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

----End

To log in to the iBMC WebUI as a Kerberos user, perform the following steps:

Kerberos environment:

- The client supports the Windows 10 64-bit operating system and the Internet Explorer 11 browser.
- The Kerberos server supports the Windows Server 2012 R2 64-bit and Windows Server 2016 64-bit OSs.

Before login, ensure that the following settings meet the requirements:

- Kerberos is enabled and Kerberos function and user group are configured on the **User & Security > Kerberos** page of the iBMC WebUI.
- The Kerberos user group and user have been created on the Kerberos server, and the user has been added to the Kerberos user group. This user is a user of the client OS.

Kerberos users can log in to the WebUI in either of the following modes:

- Logging in as a Kerberos domain user
 - a. On the iBMC login page, switch to the target language.
 - b. Enter the Kerberos user name and password for logging in to the iBMC WebUI. For details, see Table 9-2.
 - c. In the **Domain** drop-down list, select a Kerberos user domain (for example, **ADMIN.COM(KRB)**) or **Automatic matching**.
 - d. Click **Log In**.
After the login is successful, the **Home** page is displayed.
- Logging in over SSO
 - a. Use the Kerberos user name and password configured on the Kerberos server to log in to the client OS.
 - b. Enter the FQDN of the iBMC in the address box of the browser, for example, **https://host name.domain name**.
The iBMC login page is displayed.
 - c. Click **SSO**.
After the login is successful, the **Home** page is displayed.

9.3 Logging In to the SmartServer

Scenario

SmartServer is the mobile version of Intelligent Baseboard Management Controller (iBMC). After SmartServer is installed on your mobile phone, you can query, configure, and manage servers using your mobile phone.

The SmartServer application supports Android 9.0 or later.

For details about how to use SmartServer, see *Server SmartServer User Guide*.

Procedure

Step 1 Download and install the SmartServer application on a mobile phone.

1. Open Google Play Store or an app store on your phone.
2. Search for **SmartServer**.
3. Download and install the SmartServer application of the latest version.

After the installation is complete, the SmartServer icon  is displayed on the screen of the mobile phone.

 **NOTE**

During the installation, grant required permissions for SmartServer.

Step 2 Start SmartServer.

If it is your first time to use SmartServer Mobile, you are prompted to set a password for using this tool for security purposes.

 **NOTE**

After the password is set, you need to enter the password each time when you start SmartServer.

Figure 9-3 Setting a password

Verify

Enter the password.

--	--	--	--	--	--

1	2	3
4	5	6
7	8	9
Clear	0	Delete

Step 3 Enter a password.

After the password is set, the **Devices** screen is displayed.

Figure 9-4 Device management



Step 4 Add devices.

Add a server to the SmartServer device list. After the server is added, you can use SmartServer to manage it.






- Click  in the upper right corner of the screen.
- In the lower part of the screen, touch **Discover** > **Add Device**.

Figure 9-5 Add Device

Step 5 Set parameters.

Table 9-3 Parameter Description

Parameter	Description	Specifications
Access mode	Mode for accessing the server to be managed.	<ul style="list-style-type: none"> Network USB tethering <p>This access mode requires the connection to the iBMC direct connect management port of the server.</p> <p>NOTE Only Android supports this method.</p>
Host	Domain name or IP address of the server to be managed.	<p>It can be an IPv4 or IPv6 address or a domain name.</p> <p>NOTE If the access mode is USB tethering, you do not need to set this parameter.</p>

Parameter	Description	Specifications
Port	Number of the port for accessing the server.	The default value is 443 .
User	User name for accessing the server.	The default user name is Administrator .
Password	Password for accessing the server. NOTE <ul style="list-style-type: none">  : The password is entered in cipher text.  : The password is entered in plaintext. You can touch the icon to alternate between the two options. 	The default password is Admin@9000 .
Remember Password	Specifies whether to remember the password. NOTE <ul style="list-style-type: none">  : enables the password to be remembered.  : disables the function of remembering the password. You can touch the icon to alternate between the two options. 	Enabled or disabled. After this function is enabled, you do not need to enter the password when logging in to the server the next time.

Step 6 Touch **OK**.

After the connection is set up, the scanned server is displayed on the screen.

Step 7 Click the target device.

If you do not enable the Remember Password function when adding the device, you need to enter the password.

Step 8 Touch **OK**.

The management screen of the device is displayed.

----End

9.4 Logging In to the Desktop of a Server

9.4.1 Using the Remote Virtual Console

9.4.1.1 iBMC

Scenario

Log in to the desktop of a server using the iBMC Remote Virtual Console.

Procedure

Step 1 Log in to the iBMC WebUI.

For details, see 9.2 Logging In to the iBMC WebUI .

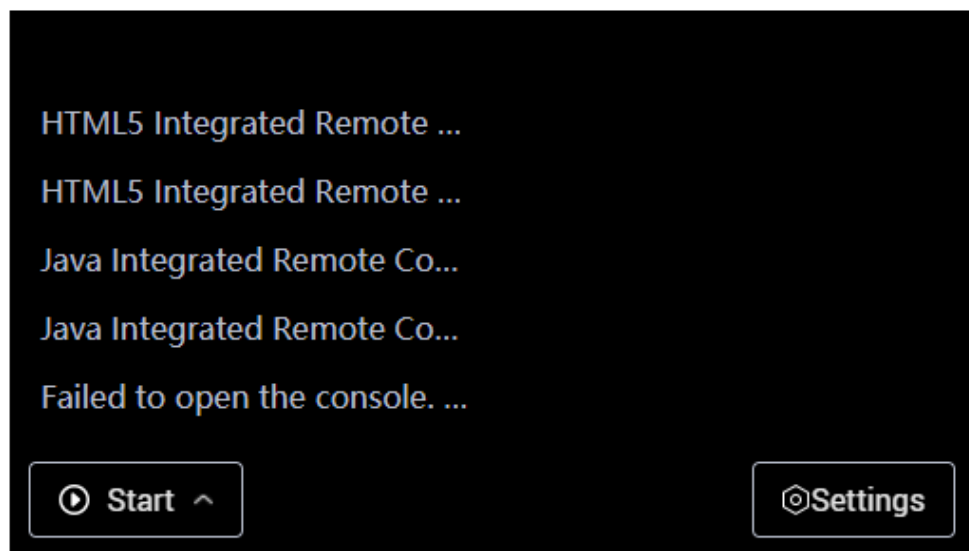
Step 2 Choose **Home** from the menu.

The home page is displayed.

Step 3 In the **Virtual Console** area, click **Start** and select **Java Integrated Remote Console** or **HTML5 Integrated Remote Console** from the drop-down list box.

Figure 9-6 Virtual console

Virtual Console



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.
- If you want to use the Java Integrated Remote Console, ensure that the Java Runtime Environment (JRE) meets requirements listed in Table 9-1. If the JRE is not installed, click **Failed to open the console ...** and click **here** to download the JRE from the official AdoptOpenJDK website. If you still cannot use the console after installing the JRE, click the links under **Troubleshooting Remote Virtual Console Problems** to obtain more information.
- For details about the virtual console, see "Virtual Console" in the iBMC user guide of the server you use.

Figure 9-7 Java Integrated Remote Console

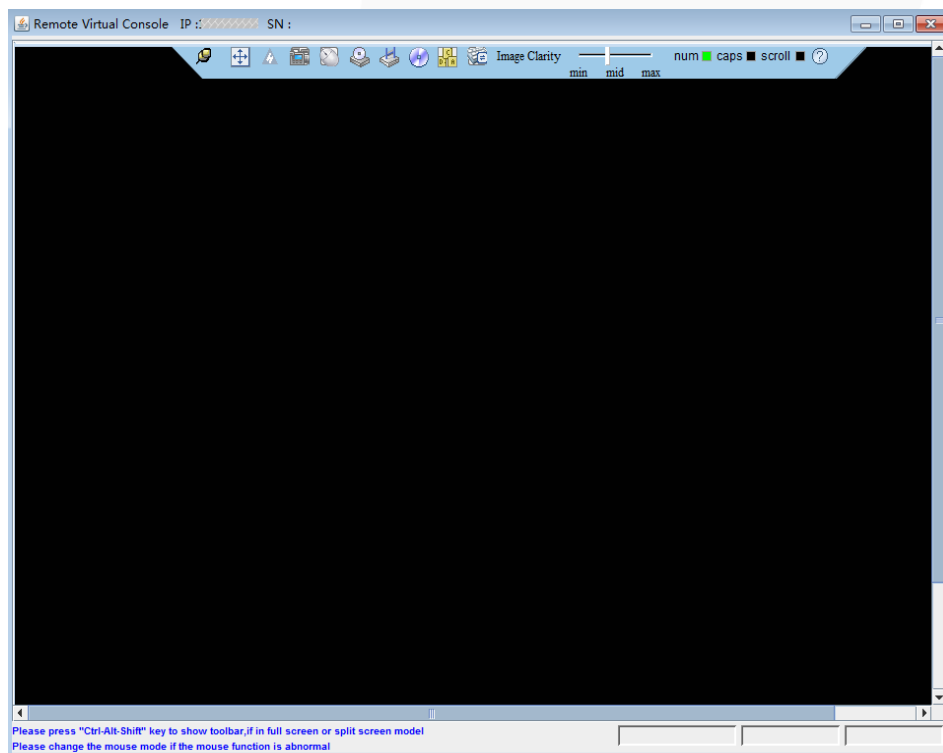
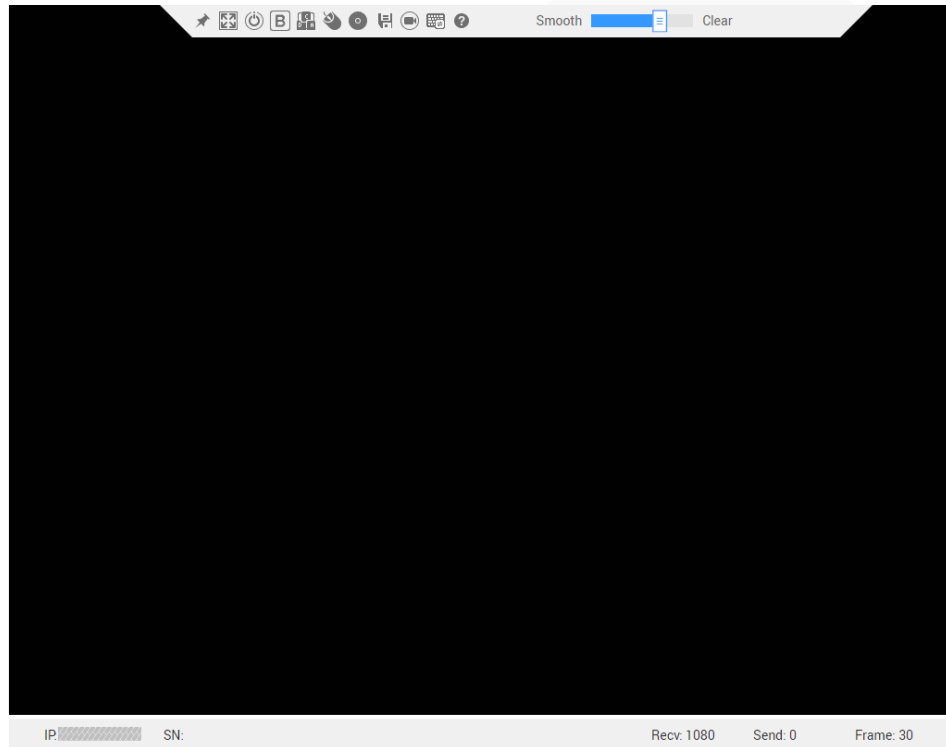


Figure 9-8 HTML5 Integrated Remote Console



----End

9.4.2 Logging In to the System Using the Independent Remote Console

Log in to the desktop of a server using the Independent Remote Console.

NOTE

The independent remote console is a remote control tool developed based on the server management software iBMC. It plays the same functions as **Virtual Console** provided by the iBMC 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.

9.4.2.1 Windows

The following Windows OS versions are supported:

- Windows 7 (32-bit/64-bit)
- 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)

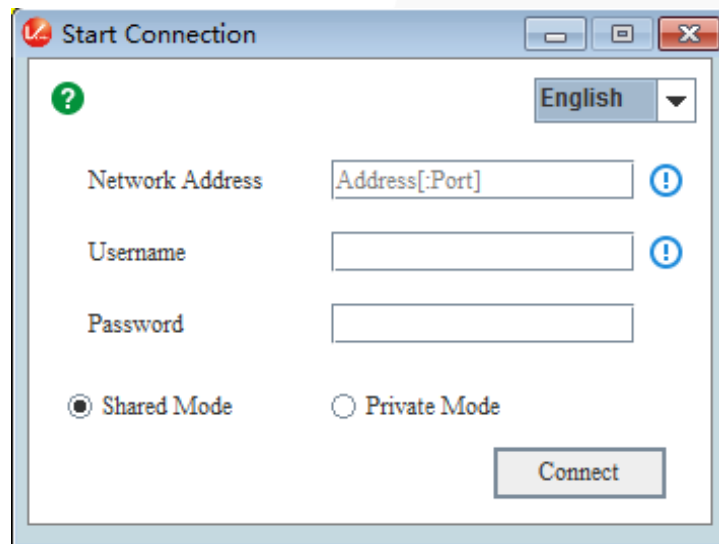
Procedure

Step 1 Configure an IP address for the client (local PC) to enable communication with the iBMC management network port.

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

The Independent Remote Console login page is displayed.

Figure 9-9 Independent Remote Console login page



Step 3 Enter the network address, user name, and password.

NOTE

- Local and LDAP domain users are supported.
- The network address can be in either of the following formats:
 - *iBMC management network port IPv4 or IPv6 address:Port number*
Enter an IPv6 address in brackets or an IPv4 address directly. for example, **[fc00::64]:444** or **192.168.100.1:444**.
 - *iBMC domain name address:Port number*
- When the port number is the default port number, the port number can be left blank.
- The preferred port number is the HTTPS service port number, and then the RMCP+ service port number.

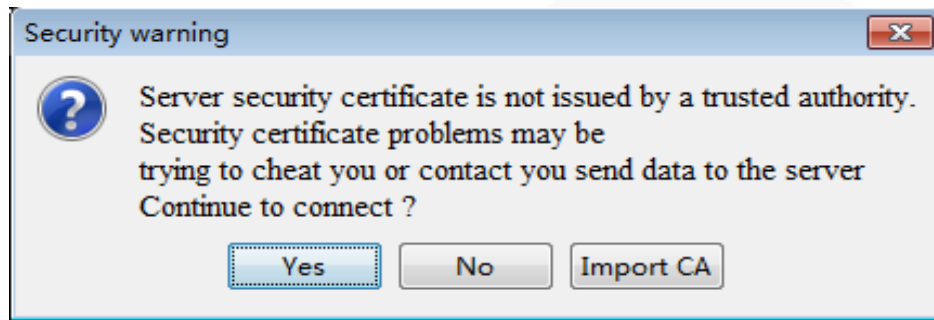
Step 4 Select a login mode.

- **Shared Mode:** allows two users to access and manage a server at the same time. The users can see each other's operations.
- **Private Mode:** allows only one user to access and manage a server at a time.

Step 5 Click **Connect**.

A security warning is displayed.

Figure 9-10 Security warning



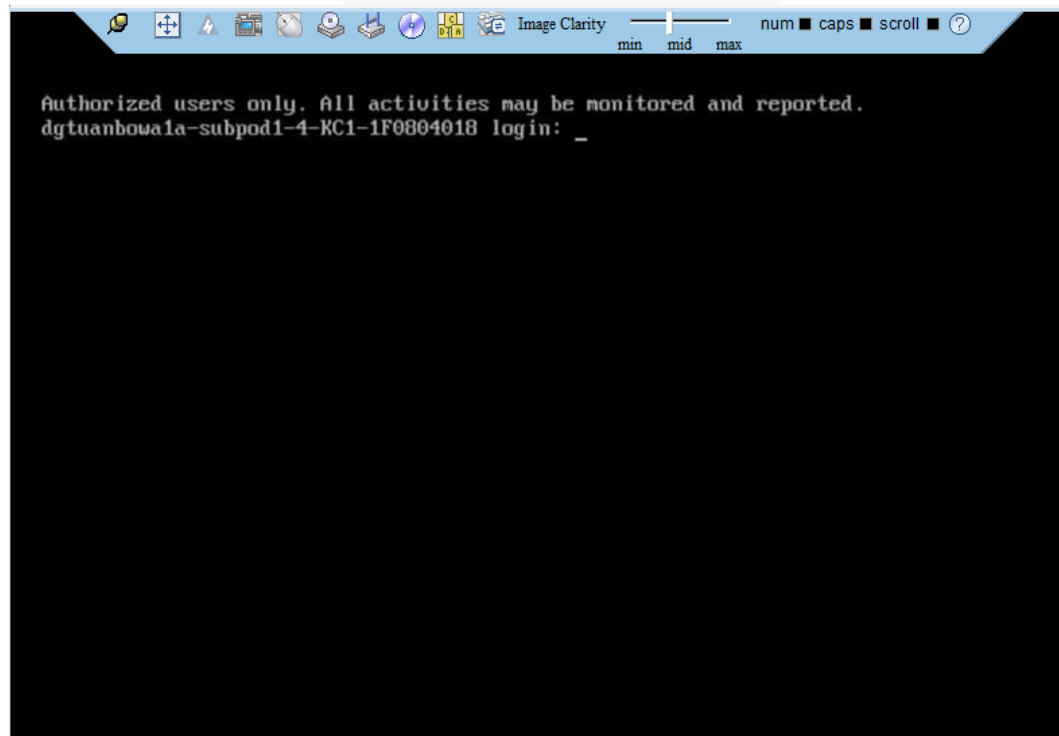
Step 6 Click **Yes**.

Ignore the certificate authentication error and go to the real-time desktop.

NOTE

- Click **No** to return to the login interface.
- Click **Import CA** to import a CA certificate (*.cer, *.crt, or *.pem). After the CA certificate is imported, the security warning dialog box will no longer be displayed.
- You are advised to periodically update the certificate for security purposes.

Figure 9-11 Server desktop



----End

9.4.2.2 Ubuntu

The following Ubuntu OS versions are supported:

- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS

Before the operation, ensure that the IPMItool version later than 1.8.14 has been installed.

Procedure

Step 1 Configure an IP address for the client (local PC) to enable communication with the iBMC management network port.

Step 2 Open the console and set the folder where the Independent Remote Console is stored as the working folder.

Step 3 Set the permissions on the Independent Remote Console.

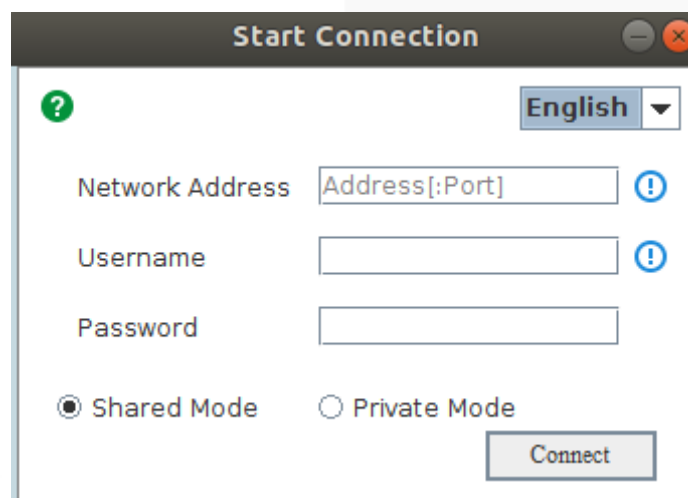
chmod 777 KVM.sh

Step 4 Open the Independent Remote Console.

./KVM.sh

The Independent Remote Console login page is displayed.

Figure 9-12 Independent Remote Console login page



Step 5 Enter the network address, user name, and password.

NOTE

- Local and LDAP domain users are supported.
- The network address can be in either of the following formats:
 - *iBMC management network port IPv4 or IPv6 address:Port number*
Enter an IPv6 address in brackets or an IPv4 address directly. for example, **[fc00::64]:444** or **192.168.100.1:444**.
 - *iBMC domain name address:Port number*

- When the port number is the default port number, the port number can be left blank.
- The preferred port number is the HTTPS service port number, and then the RMCP+ service port number.

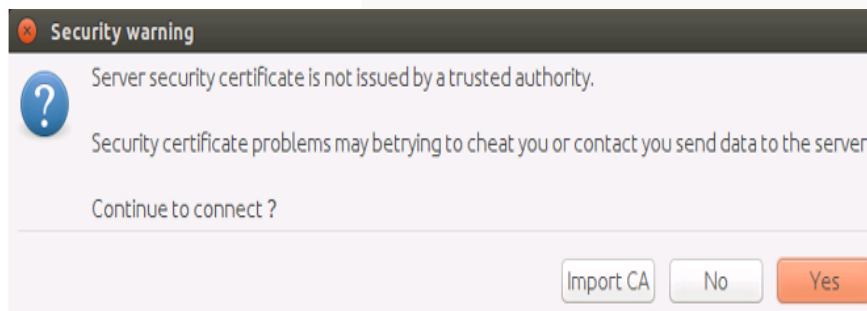
Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage a server at the same time. The users can see each other's operations.
- **Private Mode:** allows only one user to access and manage a server at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-13 Security warning



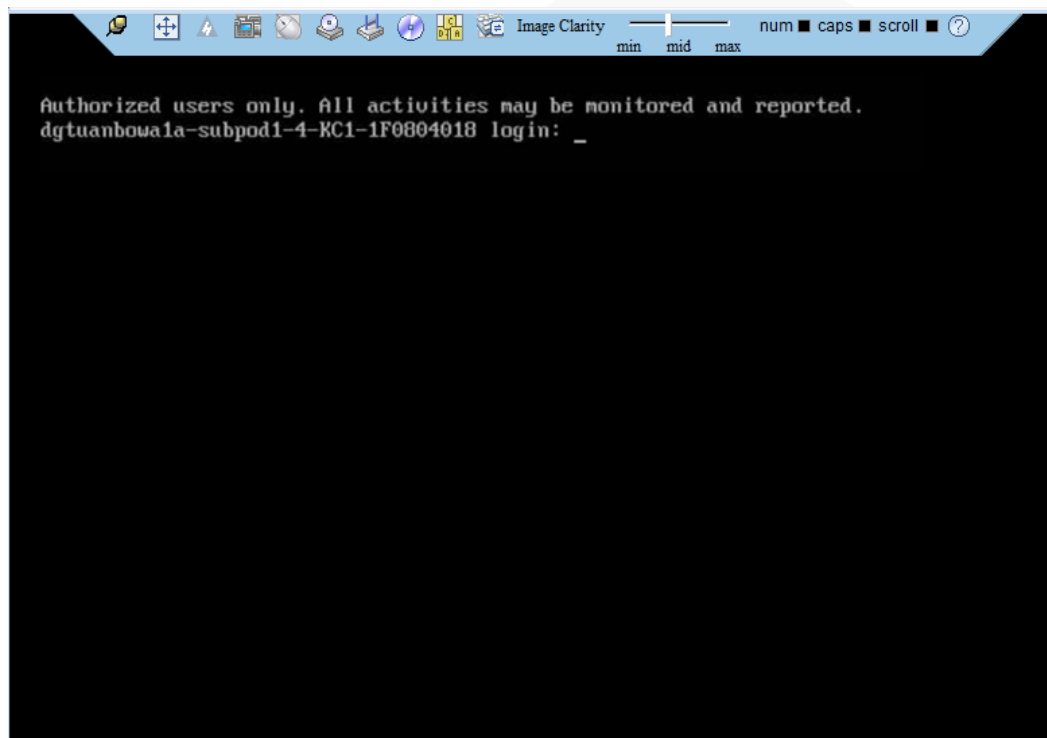
Step 8 Click **Yes**.

Ignore the certificate authentication error and go to the real-time desktop.

NOTE

- Click **No** to return to the login interface.
- Click **Import CA** to import a CA certificate (*.cer, *.crt, or *.pem). After the CA certificate is imported, the security warning dialog box will no longer be displayed.
- You are advised to periodically update the certificate for security purposes.

Figure 9-14 Server desktop



----End

9.4.2.3 Mac

The following macOS version is supported:

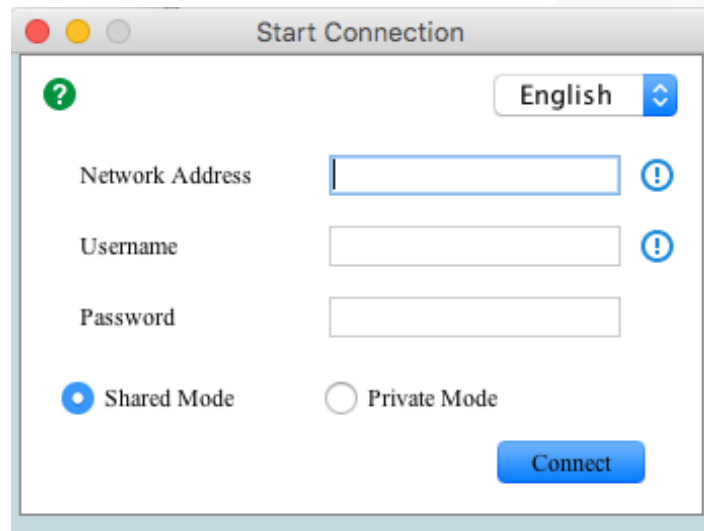
- Mac OS X El Capitan

Before the operation, ensure that the IPMItool version later than 1.8.14 has been installed.

Procedure

- Step 1** Configure an IP address for the client (local PC) to enable communication with the iBMC management network port.
- Step 2** Open the console and set the folder where the Independent Remote Console is stored as the working folder.
- Step 3** Set the permissions on the Independent Remote Console.
chmod 777 KVM.sh
- Step 4** Open the Independent Remote Console.
./KVM.sh
The Independent Remote Console login page is displayed.

Figure 9-15 Independent Remote Console login page



Step 5 Enter the network address, user name, and password.

NOTE

- Local and LDAP domain users are supported.
- The network address can be in either of the following formats:
- *iBMC management network port IPv4 or IPv6 address:Port number*
Enter an IPv6 address in brackets or an IPv4 address directly. for example, **[fc00::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- When the port number is the default port number, the port number can be left blank.
- The preferred port number is the HTTPS service port number, and then the RMCP+ service port number.

Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage a server at the same time. The users can see each other's operations.
- **Private Mode:** allows only one user to access and manage a server at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-16 Security warning



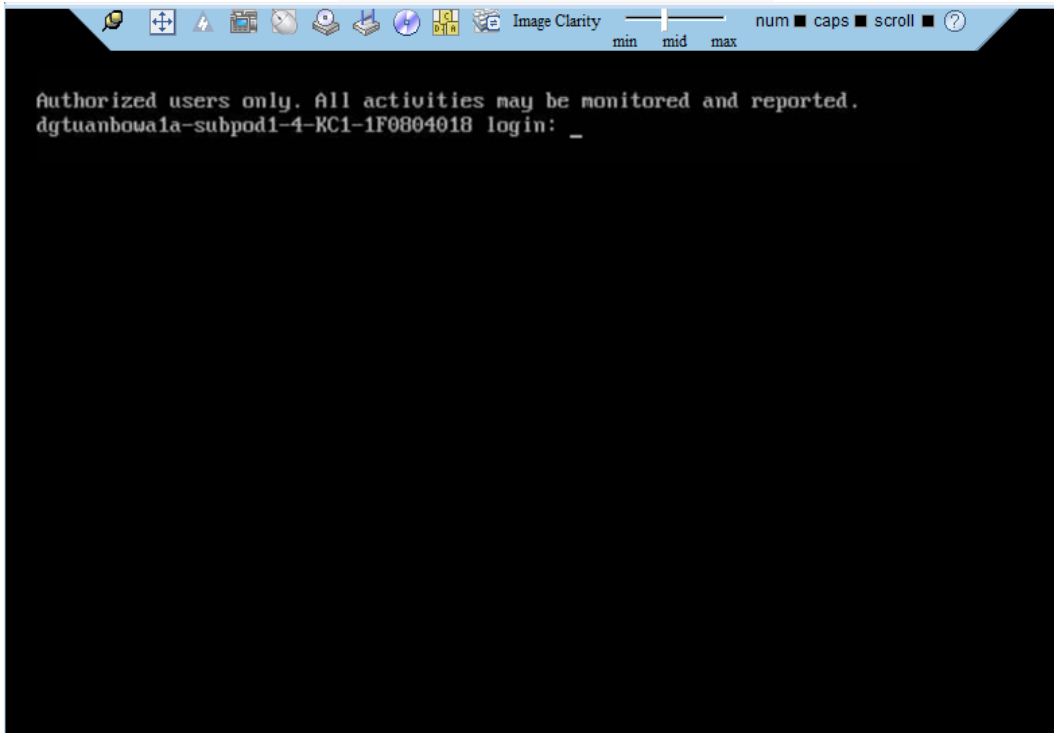
Step 8 Click **Yes**.

Ignore the certificate authentication error and go to the real-time desktop.

NOTE

- Click **No** to return to the login interface.
- Click **Import CA** to import a CA certificate (*.cer, *.crt, or *.pem). After the CA certificate is imported, the security warning dialog box will no longer be displayed.
- You are advised to periodically update the certificate for security purposes.

Figure 9-17 Server desktop



----End

9.4.2.4 Red Hat

The following Red Hat OS versions are supported:

- Red Hat 6.9
- Red Hat 7.3

Before the operation, ensure that the IPMItool version later than 1.8.14 has been installed.

Procedure

Step 1 Configure an IP address for the client (local PC) to enable communication with the iBMC management network port.

Step 2 Open the console and set the folder where the Independent Remote Console is stored as the working folder.

Step 3 Set the permissions on the Independent Remote Console.

chmod 777 KVM.sh

Step 4 Open the Independent Remote Console.

./KVM.sh

The Independent Remote Console login page is displayed.

Figure 9-18 Independent Remote Console login page



Step 5 Enter the network address, user name, and password.

NOTE

- Local and LDAP domain users are supported.
- The network address can be in either of the following formats:
- *iBMC management network port IPv4 or IPv6 address:Port number*
Enter an IPv6 address in brackets or an IPv4 address directly. for example, **[fc00::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*

- When the port number is the default port number, the port number can be left blank.
- The preferred port number is the HTTPS service port number, and then the RMCP+ service port number.

Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage a server at the same time. The users can see each other's operations.
- **Private Mode:** allows only one user to access and manage a server at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-19 Security warning



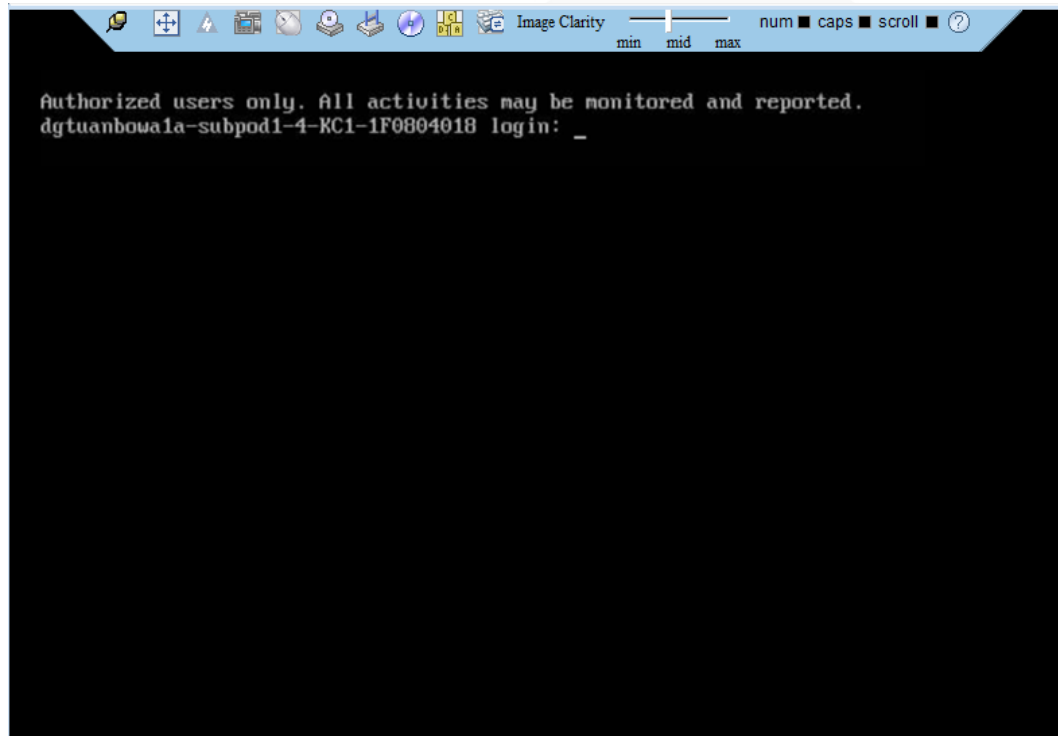
Step 8 Click **Yes**.

Ignore the certificate authentication error and go to the real-time desktop.

NOTE

- Click **No** to return to the login interface.
- Click **Import CA** to import a CA certificate (*.cer, *.crt, or *.pem). After the CA certificate is imported, the security warning dialog box will no longer be displayed.
- You are advised to periodically update the certificate for security purposes.

Figure 9-20 Server desktop



----End

9.5 Logging In to the Server CLI

9.5.1 Logging In to the CLI Using PuTTY over a Network Port

Scenario

Use PuTTY to access a server over a local area network (LAN).

NOTE

- PuTTY is free software. You need to obtain it by yourself.
- You are advised to use PuTTY of the latest version. PuTTY of an earlier version may cause login failures.

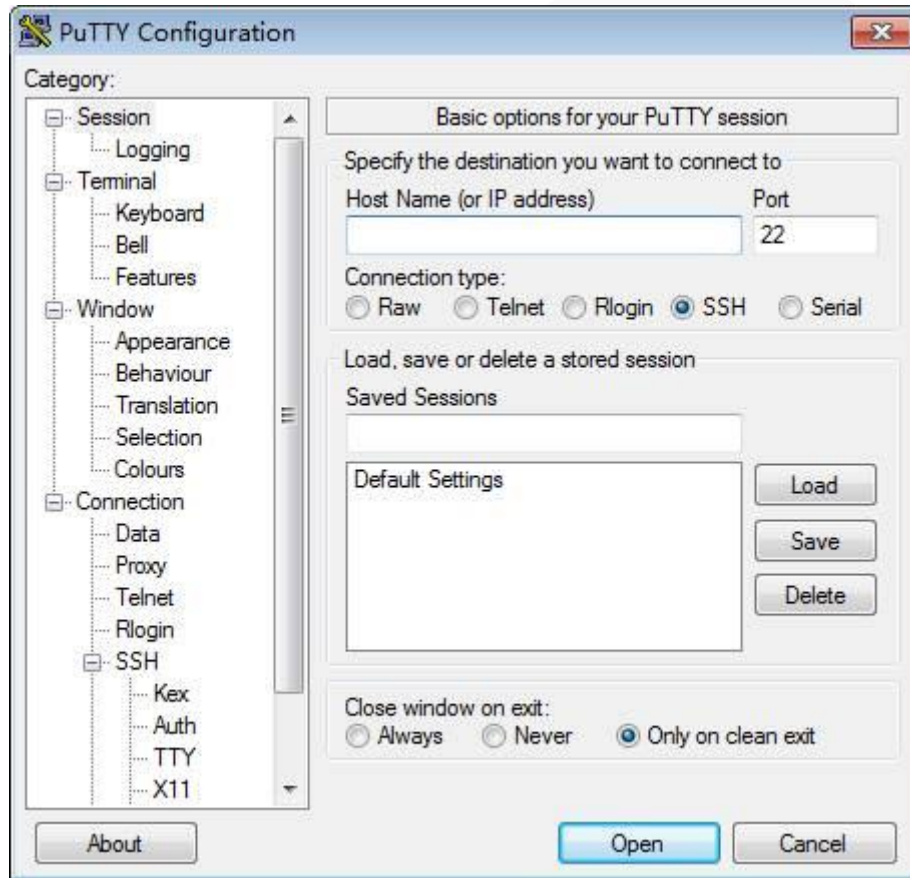
Procedure

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

Step 2 On the PC, double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed.

Figure 9-21 PuTTY Configuration



Step 3 In the navigation pane, choose **Session**.

Step 4 Set 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** and **Saved Sessions**, and click **Save**. You can double-click the saved record in **Saved Sessions** to log in to the server next time.

Step 5 Click **Open**.

The **PuTTY** window is displayed.

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.

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

----End

9.5.2 Logging In to the CLI Using PuTTY over a Serial Port

Scenario

Use PuTTY to log in to a server over a serial port when:

- You want to perform initial configuration of the server.
- The server is inaccessible over a network port.

NOTE

- PuTTY is free software. You need to obtain it by yourself.
- You are advised to use PuTTY of the latest version. PuTTY of an earlier version may cause login failures.

Procedure

Step 1 On the PC, double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed.

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

Step 3 Set login parameters.

The parameters are described as follows:

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

NOTE

n indicates the serial port number, which is an integer.

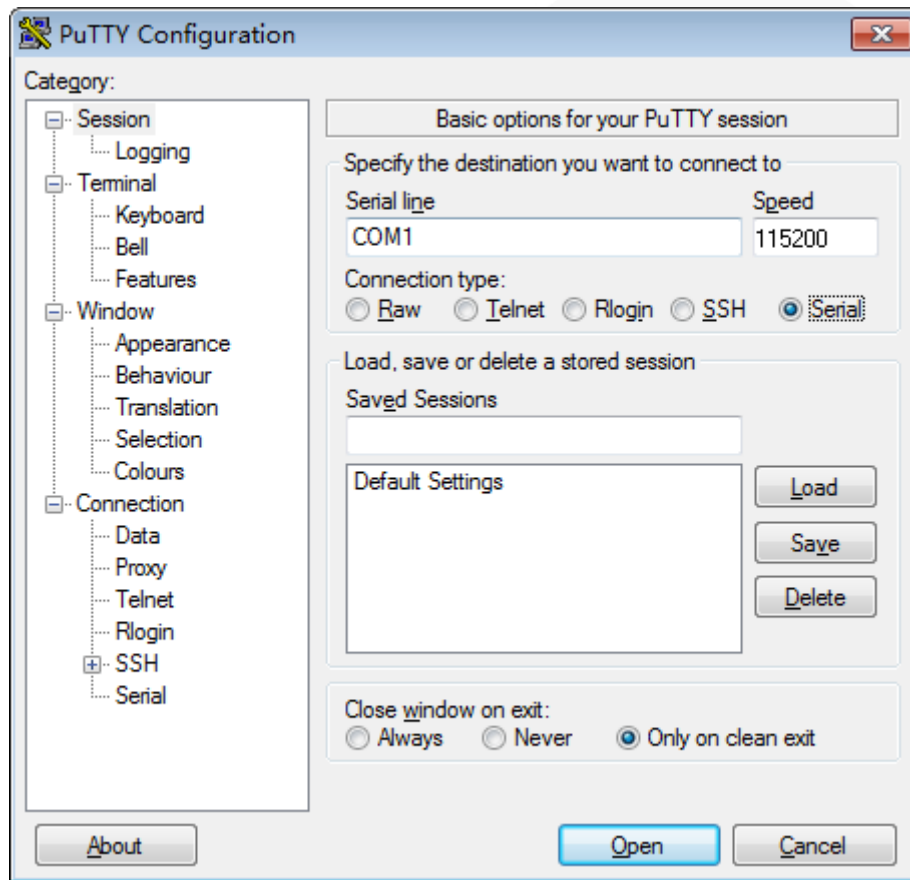
Step 4 In the navigation pane, choose **Session**.

Step 5 Set **Connection type** to **Serial** and **Close window on exit** to **Only on clean exit**.

NOTE

Set **Saved Sessions** and click **Save**. You can double-click the saved record in **Saved Sessions** to log in to the server next time.

Figure 9-22 PuTTY Configuration



Step 6 Click **Open**.

The **PuTTY** window is displayed.

NOTE

If this is your first login to the server, the **PuTTY Security Alert** dialog box is displayed. Click **Yes** to proceed.

Step 7 Enter the user name and password.

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

----End

9.6 Managing VMD

The Intel Volume Management Device (VMD) is a module integrated in the processor on the Whitley platform. It is used for surprise hot plug, management, and error processing of NVMe drives.

- Before using the VMD function, contact technical support engineers of the OS vendor to check whether the OS supports the VMD function. If yes, check whether the VMD driver needs to be manually installed and check the installation method.

- The VMD function must be enabled on the BIOS in UEFI mode only. The BIOS in legacy mode does not support this setting.
- If the VMD function is enabled and the latest VMD driver is installed, the NVMe drives support surprise hot swap.

9.6.1 Enabling VMD

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Advanced**.

Step 3 Select **Socket Configuration** and press **Enter**.

Step 4 Select **IIO Configuration** and press **Enter**.

Step 5 Select **Intel(R) VMD Technology** and press **Enter**.

Step 6 Select **Intel(R) VMD Config** and press **Enter**.

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

NOTE

The VMD function of PCIe devices is disabled by default.

Step 8 Press **F10**.

"Exit Saving Changes?" is displayed.

Step 9 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

9.6.2 Disabling VMD

Procedure

Step 1 Access the BIOS.

For details, see 9.7 Accessing the BIOS .

Step 2 Choose **Advanced**.

Step 3 Select **Socket Configuration** and press **Enter**.

Step 4 Select **IIO Configuration** and press **Enter**.

Step 5 Select **Intel(R) VMD Technology** and press **Enter**.

Step 6 Select **Intel(R) VMD Config** and press **Enter**.

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

Step 8 Press **F10**.

"Exit Saving Changes?" is displayed.

Step 9 Select **Yes** and press **Enter**.

The server automatically restarts for the settings to take effect.

----End

9.7 Accessing the BIOS

Procedure

Step 1 Connect a local PC with the KVM to the server, or access the **Remote Control** page on the iBMC WebUI.

 **NOTE**

For details about how to access the **Remote Control** page on the iBMC WebUI, see *iBMC User Guide* of corresponding server.

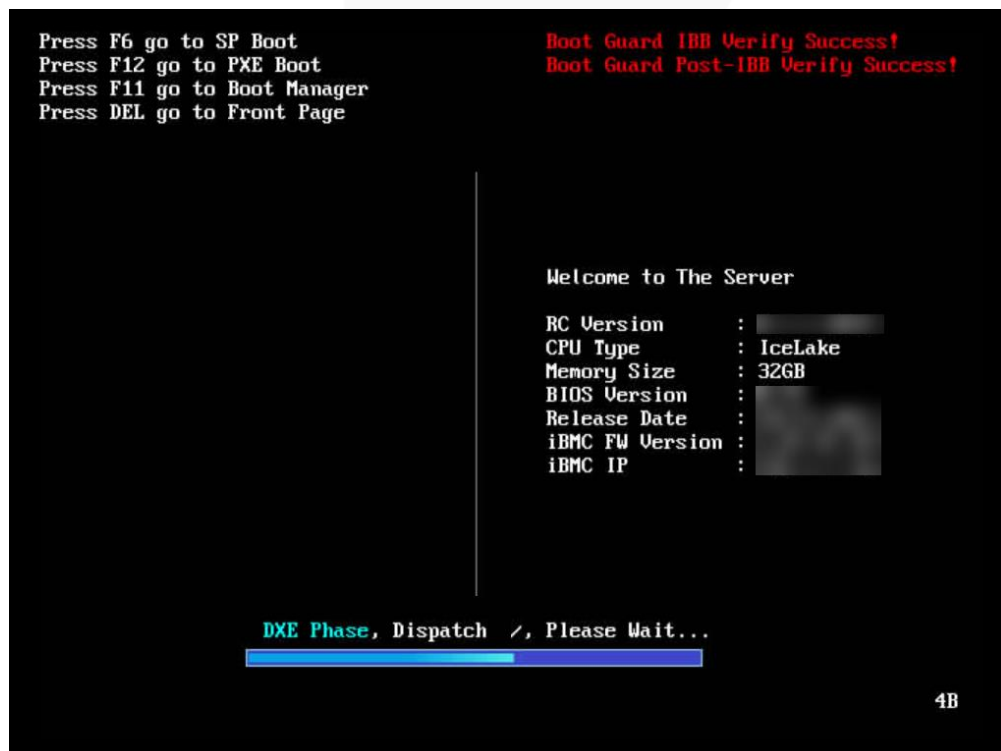
Step 2 Power on or restart the server.

 **NOTE**

Restarting the server will interrupt services. Exercise caution when performing this operation.

Step 3 When the screen shown in Figure 9-23 is displayed, press **Del** or **Delete**.

Figure 9-23 BIOS boot screen



 **NOTE**

- To access the Smart Provisioning GUI, press **F6**.
- To switch to the **Boot Manager** screen, press **F11**.
- To boot from the network, press **F12**.

Step 4 Enter the current password.

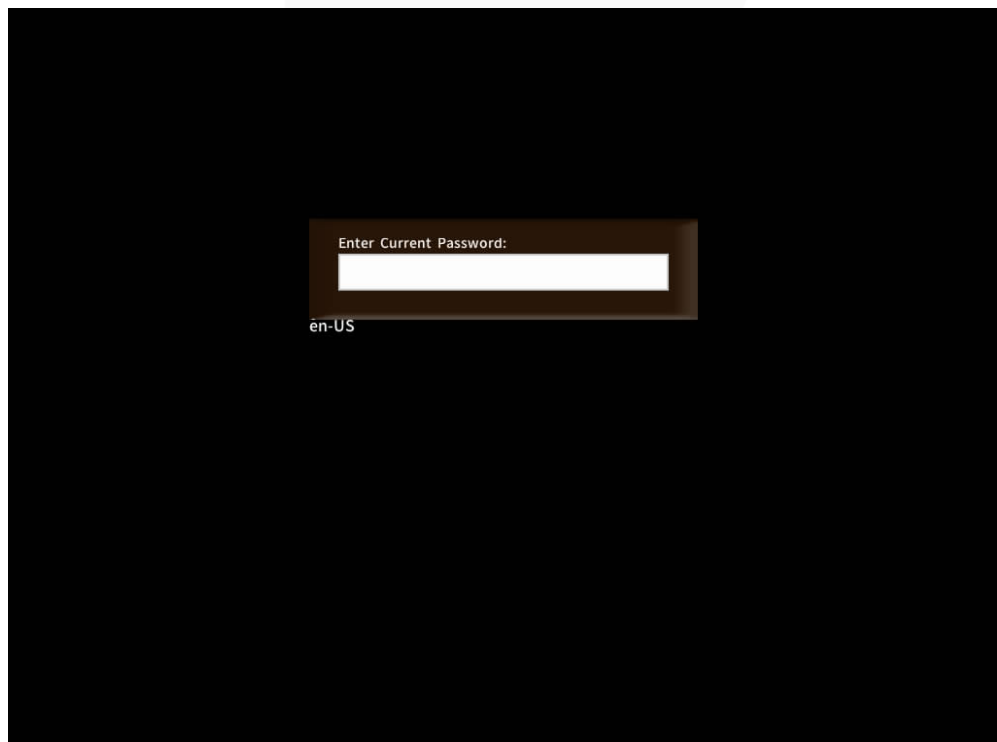
Enter the current password as prompted.

- If you log in to the BIOS for the first time, continue [Step 5](#) and skip [Step 6](#).
- Otherwise, skip [Step 5](#) and go to [Step 6](#).

 **NOTE**

- The default BIOS password is **Admin@9000** (administrator password). When you log in for the first time, the system prompts you to change the default password. You must change the default password before logging in to the BIOS.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- Use the mouse to open the on-screen keyboard and enter the password.
- For security purposes, change the administrator password periodically.
- The system will be locked if an incorrect password is entered three consecutive times. Restart the server to unlock it.

Figure 9-24 Dialog box for entering the current password



Step 5 Change the default password.

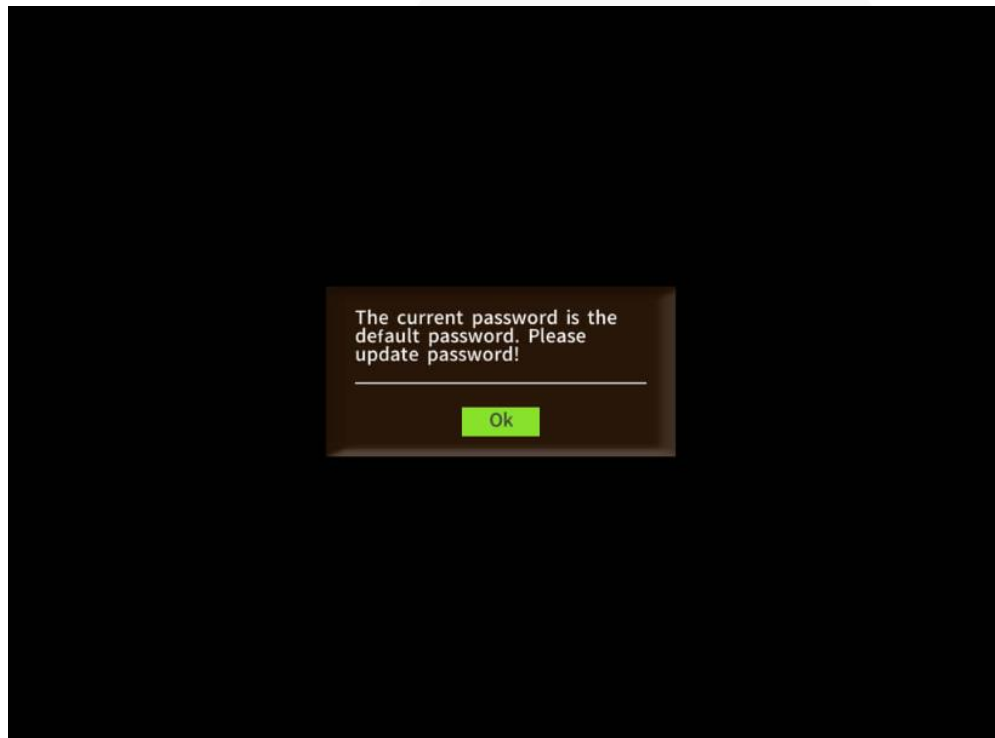
 **NOTE**

When you log in to the BIOS for the first time, change the default password.

1. Enter the default password and press **Enter**.

A dialog box is displayed, prompting you to change the default password.

Figure 9-25 Changing the default password

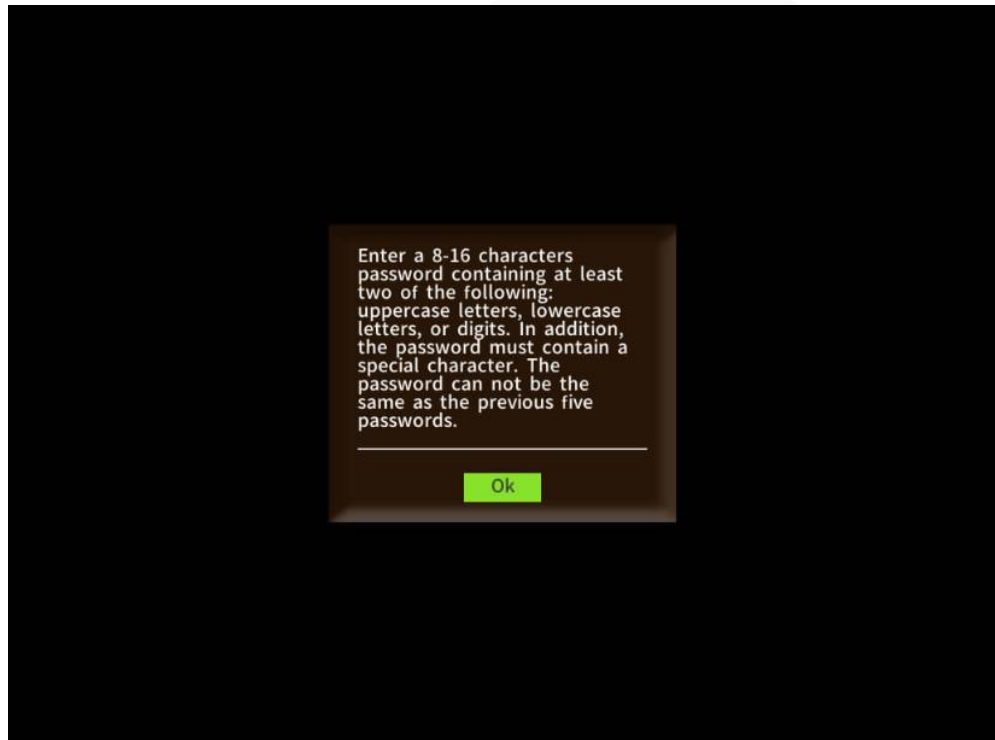


2. Click **Ok**.

The dialog box for password complexity requirements is displayed. A password must:

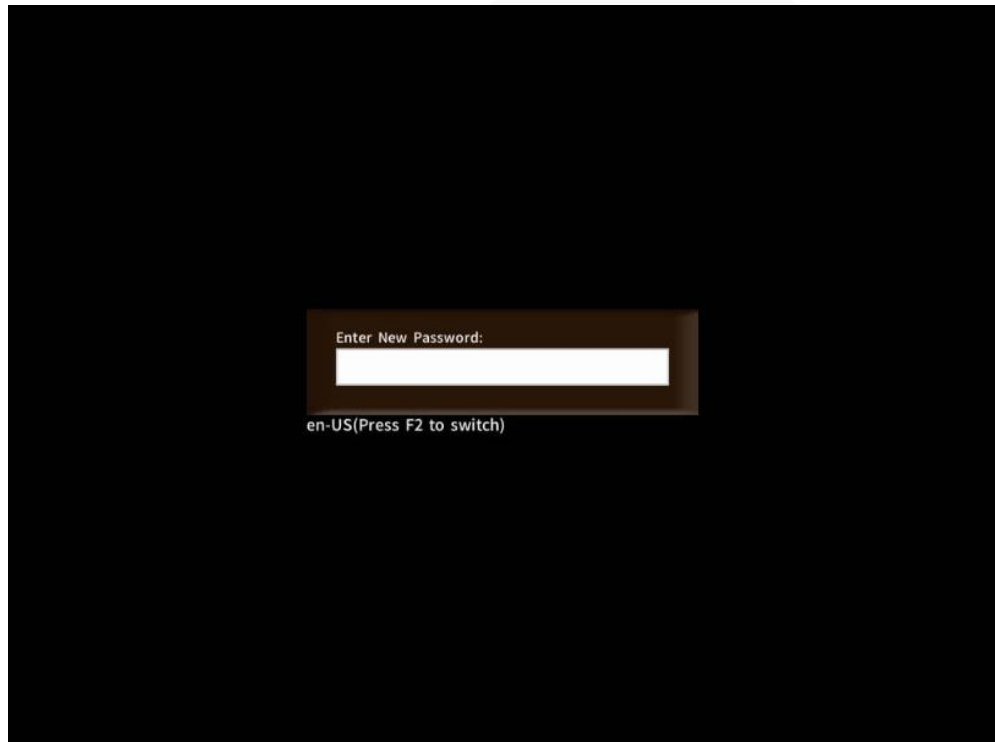
- Contain 8 to 16 characters.
- Contain at least two of the following types of characters: uppercase letters, lowercase letters, and digits.
- Contain at least one special character.
- Be different from the previous five passwords.

Figure 9-26 Password complexity requirements



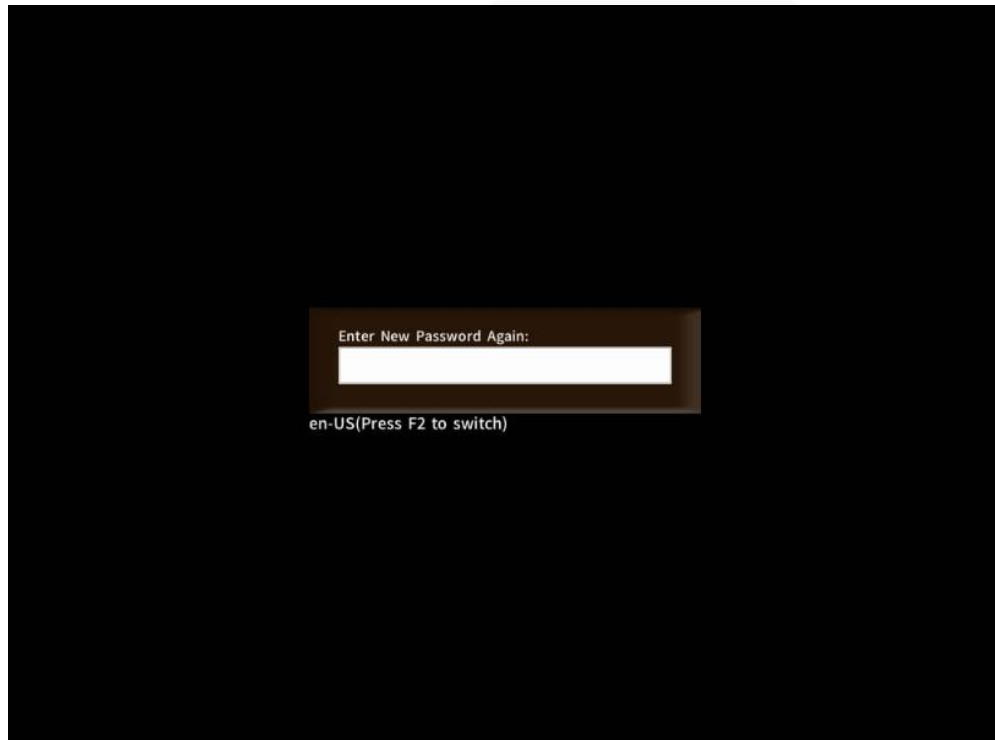
3. Click **Ok**.
The dialog box for entering the new password is displayed.

Figure 9-27 Setting a new password



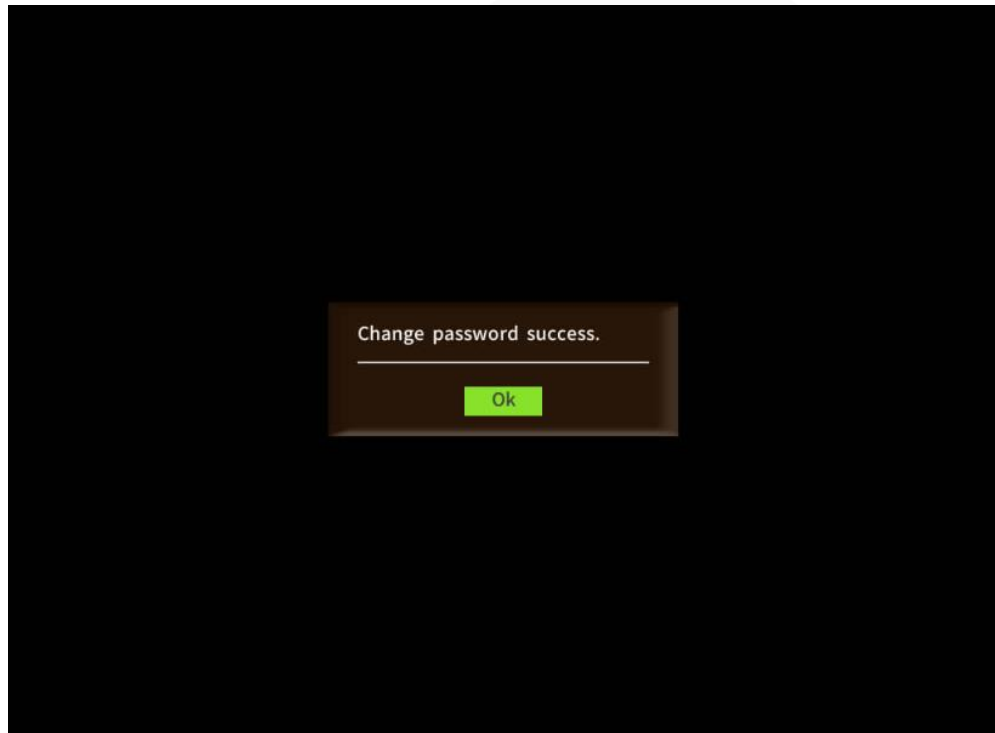
4. Enter a password and press **Enter**.
The dialog box for confirming the new password is displayed.

Figure 9-28 Confirming the new password



5. In the dialog box that is displayed, enter the password again and press **Enter**.
A dialog box is displayed, indicating that the password is changed successfully.

Figure 9-29 Password change success dialog box



6. Click **Ok**.
The front page is displayed.

Figure 9-30 Front Page screen



Step 6 After the password is entered, press **Enter**.

The front page is displayed.

NOTE

- Figure 9-31 and Figure 9-32 show the **Front Page** screen displayed when you log in to the system as the administrator.
- Figure 9-33 shows the **Front Page** screen displayed when you log in to the system as a common user. In this case, only the **Continue** and **Setup Utility** menus are displayed. On the **Setup Utility** page, a common user can only view menu options, set or change the password of the common user (that is, editing the **Set User Password** option on the **Security** page), set parameters (except **Load Defaults**) on the **Exit** page, press **F10** to save and exit. Other options are all dimmed and cannot be edited. **F9** used to restore the default settings is unavailable.

Figure 9-31 Front Page screen (UEFI mode)

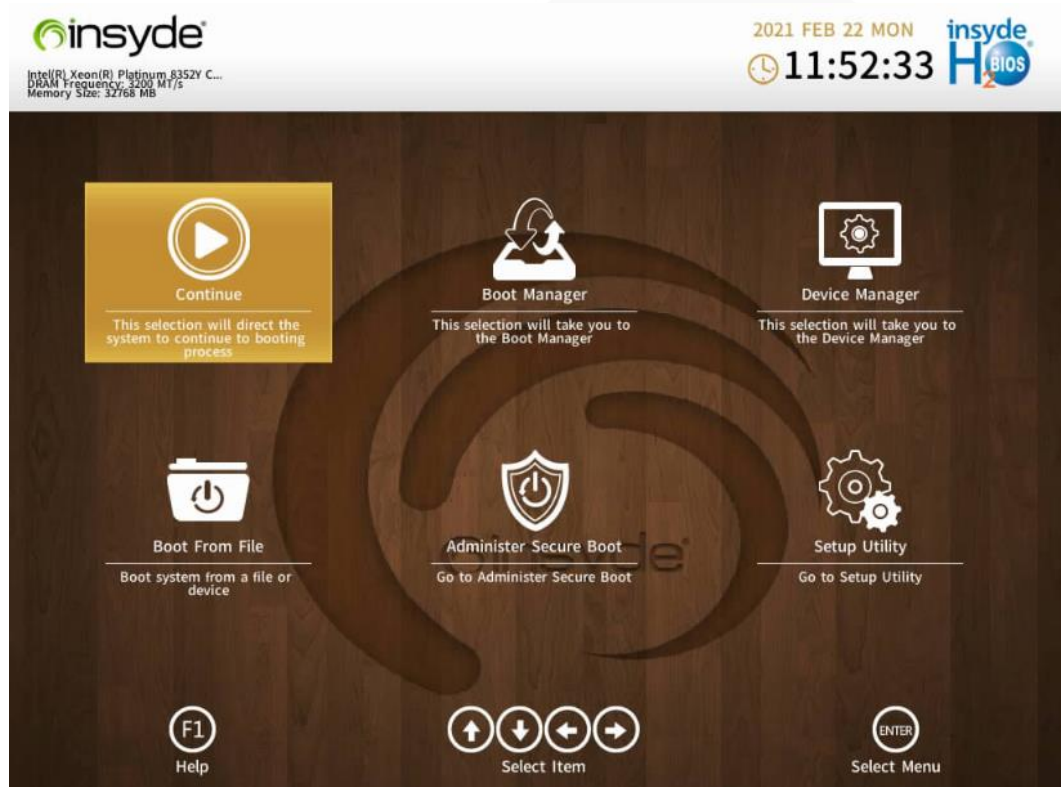


Figure 9-32 Front Page screen (legacy mode)



Figure 9-33 Front Page screen (login using a common user password)

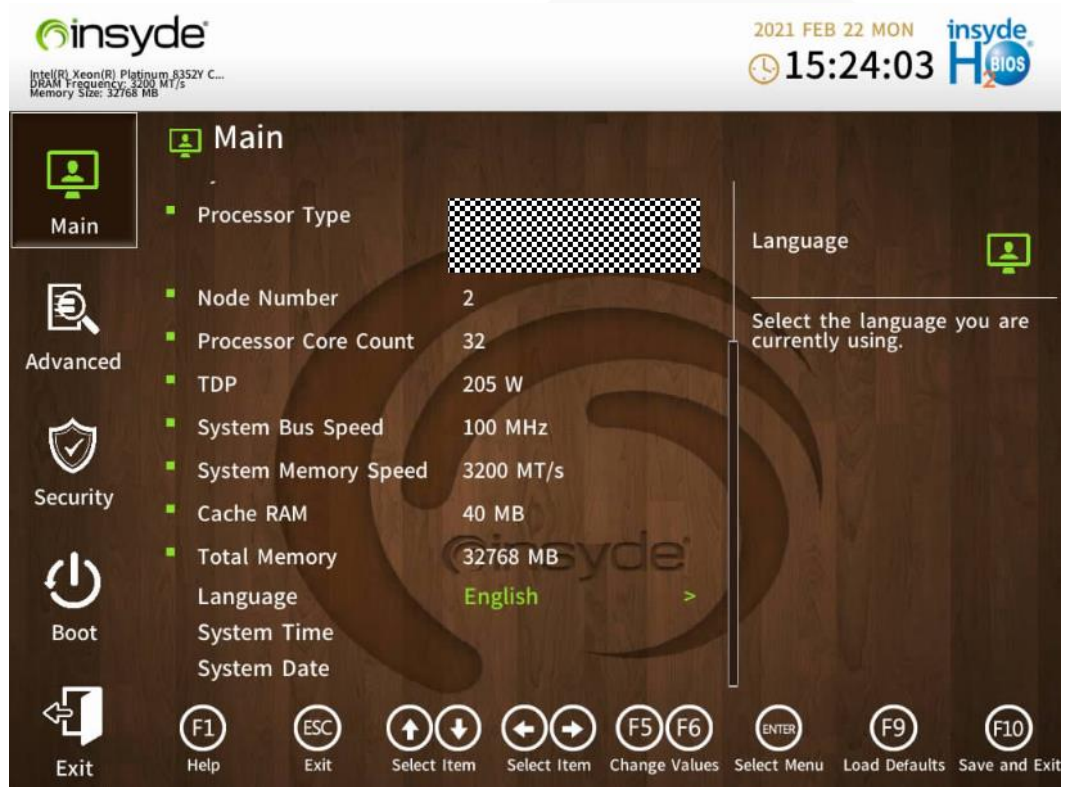


- Step 7** Use arrow keys to select **Setup Utility** and press **Enter**.
The **Main** screen is displayed.

Figure 9-34 Main screen 1



Figure 9-35 Main screen 2



----End

9.8 Clearing Data from a Storage Device

Scenario

Use the Linux **badblocks** command to clear data on a storage device. When running the **badblocks** command, you need to specify parameters to overwrite data on the storage device.

The following describes how to clear the data on one HDD/SSD as an example. This operation is for reference only. You can also use the disk erasing function of Smart Provisioning to erase data from storage media. This function is not applicable to encrypted drives.

For details, see section "Erasing Hard Disks" in the latest *Smart Provisioning User Guide (x86_64)*.

NOTICE

The cleared data cannot be restored. Exercise caution when performing this operation.

Procedure

NOTE

Before performing this operation, check that:

- The storage device is not in a RAID array with redundancy, and the server operating system is running properly.
- You have obtained the server No. and the slot No. and location of the storage device to be cleared.

Step 1 You have accessed the desktop of the server where the target drive is located.

For details, see 9.4.2 Logging In to the System Using the Independent Remote Console .

Step 2 Open the CLI.

Step 3 Query information about drive letters.

lsscsi

Figure 9-36 Querying drive letters

```
Linux-hm54:~ # lsscsi
[0:0:0:0] disk SEAGATE ST900MM0006 B001 /dev/sda
[0:0:1:0] disk SEAGATE ST900MM0006 B001 /dev/sdb
```

Step 4 Query drive information.

fdisk -l

NOTE

- The drive with the * symbol in the **Boot** column is the system drive. As shown in Figure 9-37, **sda** is the system drive.
- Do not directly clear system drive data. Before clearing system drive data, clear data from other storage media.

Figure 9-37 Querying drive information

```
Linux-hm54:~ # fdisk -l
Disk /dev/sda: 900.2 GB, 900185481216 bytes
255 heads, 63 sectors/track, 109441 cylinders, total 1758174768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000181d2

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            *          2048         8386559       4192256   82  Linux swap / Solaris
/dev/sda2            *      8386560     1758173183     874893312   83  Linux

Disk /dev/sdb: 900.2 GB, 900185481216 bytes
255 heads, 63 sectors/track, 109441 cylinders, total 1758174768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdb doesn't contain a valid partition table
```

Step 5 Write 0s to the drive to be cleared.

Command: **badblocks -swft 0 Drive letter**

Example: **badblocks -swft 0 /dev/sdb**

Figure 9-38 Clearing data (example)

```
linux-hm54:~ # badblocks -swft 0 /dev/sdb  
Testing with pattern 0x00: █26.38% done, 19:40 elapsed
```

 **NOTE**

- The drive letters vary with the storage media (HDD, SSD, and USB flash drive). Ensure that the drive letter that you entered is correct.
- This operation takes time.
- If the command fails to execute, contact technical support.

Step 6 Remove the drive.

 **NOTE**

After the data is cleared, do not restart or reinstall the server. Otherwise, the system will reload data to the drives during the startup of the server.

----End

10 More Information

- [10.1 Technical Support](#)
- [10.2 Product Information Resources](#)
- [10.3 Product Configuration Resources](#)
- [10.4 Maintenance Tool](#)

10.1 Technical Support

ZOOMindustry 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 [ZOOMtecnologia website](#).

Contact ZOOMtecnologia

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

- Contact ZOOMtecnologia customer service center.
 - Email: contato@zoomtecnologia.com
- Contact technical support personnel at your local ZOOMtecnologia branch office.

10.2 Product Information Resources

Table 10-1 Product information

Item	Description	How to Obtain
Server product documentation	Documents that provide information about the structure, specifications, installation and removal of components, installation of software, and server configuration.	Visit Technical Support > Documentation > View ALL , select a product model, and download resources you want under Downloadable Product Documentation Package on the Documentation tab page.
Compatibility Checker	A tool used to query the OSs, parts, and peripherals compatible with a server.	Visit Compatibility Checker .

10.3 Maintenance Tool

Table 10-3 Software tools for routine maintenance

Tool	Server Model and Software Version	Description
Hard'Server Tools	See <i>Hard'Server Tools User Guide</i> .	Hard'Server Tools contains tools used for batch deployment, maintenance, and upgrade of servers. Download link: Hard'Server Tools
Smart Provisioning	See <i>Smart Provisioning User Guide</i> .	Smart Provisioning is used to install OSs, configure RAID, and upgrade firmware. Download link: Smart Provisioning

11 Software and Configuration Utilities

11.1 iBMC

11.2 BIOS

11.1 iBMC

The intelligent Baseboard Management Controller (iBMC) complies with DCMI 1.5/IPMI 1.5/IPMI 2.0 and SNMP standards and supports various functions, including KVM redirection, text console redirection, remote virtual media, and hardware monitoring and management.

The iBMC offers the following features:

- Various management interfaces
The iBMC provides IPMI, CLI, Data Center Manageability Interface (DCMI), Redfish interfaces, Hypertext Transfer Protocol Secure (HTTPS), and SNMP.
- 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, facilitating remote maintenance.
- WebUI
The iBMC provides a web-based UI for setting and querying device information.
- System breakdown screenshots and video playback
The iBMC allows screenshots and videos to be created when the system breaks down. 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, recording, and auditing.
- Support for DNS and LDAP
The iBMC supports domain name system (DNS) and Lightweight Directory Application Protocol (LDAP) to implement domain management and directory service.
- Image backup
The iBMC works in active/standby mode to ensure system reliability. If the active iBMC is faulty, the standby iBMC takes over services immediately.

- Intelligent power management
The iBMC uses power capping to increase deployment density, and uses dynamic energy saving to reduce operating expenditure.

For more information about the iBMC, see the *Hard' Server Rack Server iBMC User Guide*.

11.2 BIOS

The basic input/output system (BIOS) is the most basic software loaded on a computer hardware system. The BIOS provides an abstraction layer for the operating system (OS) and the hardware to interact with the keyboard, display, and other input/output (I/O) devices.

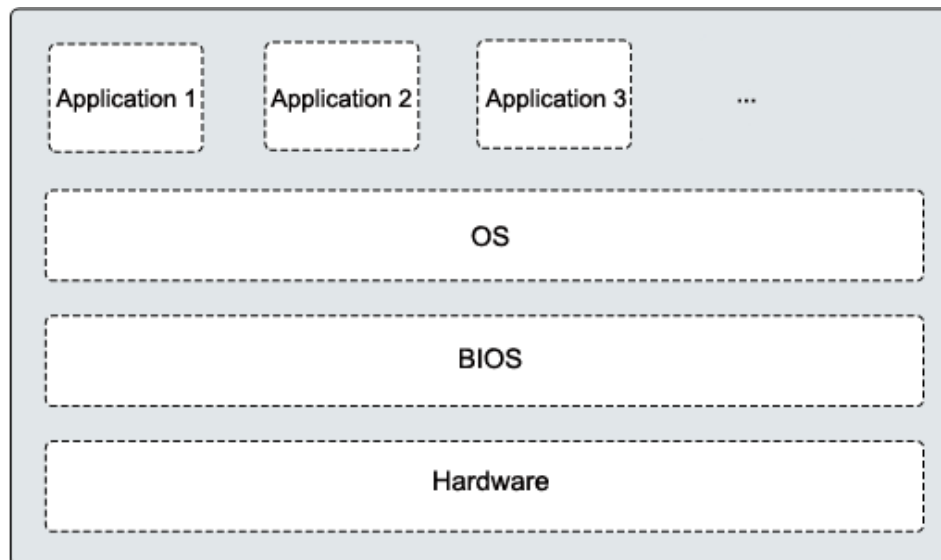
The BIOS data is stored on the Serial Peripheral Interface (SPI) flash memory. The BIOS performs a power-on self-test (POST), initializes CPUs and memory, checks the I/O and boot devices, and finally boots the OS. The BIOS also provides the advanced configuration and power interface (ACPI), hot swap setting, and a management interface in Chinese, English, and Japanese.

The Whitley platform BIOS complies with UEFI 2.7 and ACPI 6.2 specifications.

The BIOS on Whitley-based servers is developed based on the code base of independent BIOS vendors (IBVs). It provides a variety of in-band and out-of-band configuration functions as well as high scalability and supports customization.

For more information about the BIOS, see the *Server Whitley Platform BIOS Parameter Reference*.

Figure 11-1 BIOS in the system



A Appendix

A.1 Product SN

The serial number (SN) on the slide-out label plate uniquely identifies a device. The SN is required when you contact technical support.

Figure A-1 SN example



Table A-1 SN description

No.	Description
1	ESN ID (two characters), which can only be 21 .
2	Material ID (eight characters), that is, the processing code.
3	Vendor code (two characters), that is, the code of the processing place.
4	<p>Year and month (two characters).</p> <ul style="list-style-type: none"> The first character indicates the year. <ul style="list-style-type: none"> 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. <p>NOTE</p> <p>The years from 2010 are represented by upper-case letters excluding I, O, and Z because the three letters are similar to the digits 1, 0, and 2.</p> <ul style="list-style-type: none"> The second character indicates the month. <ul style="list-style-type: none"> Digits 1 to 9 indicate January to September, respectively.

No.	Description
	- Letters A to C indicate October to December, respectively.
5	Serial number (six digits).
6	RoHS compliance (one character). Y indicates RoHS compliant.
7	Internal model, that is, product name.

A.2 Operating Temperature Limitations

Table A-2 Operating temperature limitations

Configuration	Max. 30°C (86°F)	Max. 35°C (95°F)	Max. 40°C (104°F)	Max. 45°C (113°F)
4 x 3.5" drive pass-through configuration	<ul style="list-style-type: none"> Options not supported: 6334/6342/6346/6348/6354/8358P/8351N/8358/8360Y/8368/8380 processors 	<p>Options not supported:</p> <ul style="list-style-type: none"> Rear drives (including HDD/SSD/M.2) 6334/6342/6346/6348/6354/8358P/8351N/8358/8360Y/8368/8380 processors 	<p>Options not supported:</p> <ul style="list-style-type: none"> 5320/6312U/6326/6334/6336Y/6342/6314U/6330/6330N/6338/6338N/6346/6348/6354/8351N/8352V/8352S/8352Y/8358/8358P/8360Y/8368/8380 processors Memory of 256 GB per module or larger Rear drives (including HDD/SSD/M.2) GPU cards IB cards CX5/CX6 NICs OCP 3.0 network adapters with ports of 25GE or higher rate 	<p>Options supported:</p> <ul style="list-style-type: none"> 4309Y/4310/4310T/4314 processors RDIMMs of less than 64 GB per module <p>Options not supported:</p> <ul style="list-style-type: none"> Rear drives (including HDD/SSD/M.2) GPU cards IB cards CX5/CX6 NICs OCP 3.0 network adapters NICs of greater than 25 GB 9460-16i RAID controller cards

Configuration	Max. 30°C (86°F)	Max. 35°C (95°F)	Max. 40°C (104°F)	Max. 45°C (113°F)
8 x 2.5" drive pass-through configuration	<ul style="list-style-type: none"> All options supported 	<p>Options not supported:</p> <ul style="list-style-type: none"> Rear drives (including HDD/SSD/M.2) 	<p>Options not supported:</p> <ul style="list-style-type: none"> 5320/6312 U/6326/633 4/6336Y/63 42/6314U/6 330/6330N/ 6338/6338 N/6346/634 8/6354/835 1N/8352V/ 8352S/8352 Y/8358/835 8P/8360Y/8 368/8380 processors Memory of 256 GB per module or larger Rear drives (including HDD/SSD/M.2) GPU cards IB cards CX5/CX6 NICs OCP 3.0 network adapters with ports of 25GE or higher rate 	<p>Options supported:</p> <ul style="list-style-type: none"> 4309Y/4310/ 4310T/4314 processors RDIMMs of less than 64 GB per module <p>Options not supported:</p> <ul style="list-style-type: none"> Rear drives (including HDD/SSD/M.2) GPU cards IB cards CX5/CX6 NICs OCP 3.0 network adapters NICs of greater than 25 GB 9460-16i RAID controller cards
10 x 2.5" drive pass-through configuration	<ul style="list-style-type: none"> All options supported 	<p>Options not supported:</p> <ul style="list-style-type: none"> Rear drives (including HDD/SSD/M.2) 	<p>Options not supported:</p> <ul style="list-style-type: none"> 5320/6312 U/6326/633 4/6336Y/63 42/6314U/6 330/6330N/ 6338/6338 N/6346/634 8/6354/835 1N/8352V/ 8352S/8352 Y/8358/835 8P/8360Y/8 	<p>Options supported:</p> <ul style="list-style-type: none"> 4309Y/4310/ 4310T/4314 processors RDIMMs of less than 64 GB <p>Options not supported:</p> <ul style="list-style-type: none"> Rear drives (including HDD/SSD/M

Configuration	Max. 30°C (86°F)	Max. 35°C (95°F)	Max. 40°C (104°F)	Max. 45°C (113°F)
			368/8380 processors <ul style="list-style-type: none"> • Memory modules of 256 GB or larger • Rear drives (including HDD/SSD/M.2) • GPU cards • IB cards • CX5/CX6 NICs • OCP 3.0 network adapters with ports of 25GE or higher 	.2) <ul style="list-style-type: none"> • GPU cards • IB cards • CX5/CX6 NICs • OCP 3.0 network adapters • NICs of greater than 25 GB • 9460-16i RAID controller cards
10 x 2.5" NVMe drive configuration	<ul style="list-style-type: none"> • All options supported 	Options not supported: <ul style="list-style-type: none"> • 6334/6342/6348/6346/6354/8358P/8351N/8358/8360Y/8368/8380 processors • Rear drives (including HDD/SSD/M.2) • GPU cards • IB cards • CX5/CX6 NICs • OCP 3.0 network adapters with ports of 25GE or higher rate 	All options not supported	All options not supported

NOTE

- When a single fan is faulty, the highest operating temperature is 5°C (9°F) lower than the rated value.
- When a single fan is faulty, the system performance may be affected.
- Rear GPU cards, rear drives (including HDD/SSD/M.2), IB cards, and OCP 3.0 network adapters of 25GE or higher rate are not supported, when the server is configured with memory of 256 GB per module or larger, or 6342/6348/6346/6354/8352V/8352S/8352Y/8358P/8351N/8358/8360Y/8368/8380 processors are configured.
- It is recommended that servers be deployed at an interval of 1U to reduce server noise and improve server energy efficiency.
- The server does not support 8368Q 38c 270 W 2.6 GHz liquid-cooled processors.

A.3 Nameplate

Certified Model	Usage Restrictions
H12H-06	Global

A.4 RAS Features

The server supports a variety of Reliability, Availability, and Serviceability (RAS) features. You can configure these features for better performance.

A.5 Sensor List

Sensor	Description	Component
Inlet Temp	Air inlet temperature	Indicator board
Outlet Temp	Air outlet temperature	BMC card
PCH Temp	PCH bridge temperature	Mainboard
CPUN Core Rem	CPU core temperature	CPUN <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN DTS	CPU DTS value	CPUN <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN Margin	CPU Margin	CPUN <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN VDDQ Temp	CPU VDDQ temperature	Mainboard <i>N</i> indicates the CPU number. The value ranges

Sensor	Description	Component
		from 1 to 2 .
CPUN VRD Temp	CPU VRD temperature	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN MEM Temp	CPU memory module temperature	Memory module corresponding to CPU <i>N</i> <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN 12V	12 V voltage supplied by the mainboard to the CPU	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
Riser 12V	12 V voltage supplied by the mainboard to the riser card	Mainboard
Disk BP 12V	12 V voltage supplied by the mainboard to the drive backplane	Mainboard
CPUN DDR VDDQ	1.2 V memory module voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN DDR VDDQ2	1.2 V memory module voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN VCCIN	CPU VCCIN voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN VSA	CPU VSA voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN P1V8	CPU P1V8 voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN VCCIO	CPU VCCIO voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN VCCANA	CPU VCCANA voltage	Mainboard <i>N</i> indicates the CPU number. The value is 1 or 2 .
FAN <i>N</i> F Speed	Fan speed	Fan module <i>N</i>
FAN <i>N</i> R Speed		<i>N</i> indicates the fan module number. The value ranges

Sensor	Description	Component
		from 1 to 7 .
Power	Server input power	Power supply unit (PSU)
PSN VIN	PSU <i>N</i> input voltage	PSU <i>N</i> <i>N</i> indicates the PSU number. The value is 1 or 2 .
Disks Temp	Maximum drive temperature	Drive
RAID Temp	Temperature of the RAID controller card	RAID controller card
Power <i>N</i>	PSU input power	PSU <i>N</i> <i>N</i> indicates the PSU number. The value is 1 or 2 .
PCH Status	PCH chip fault diagnosis health status	Mainboard
CPUN UPI Link	CPU UPI link fault diagnosis health status	Mainboard or CPU <i>N</i> <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN Prochot	CPU Prochot	CPUN <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN Status	CPU status	CPUN <i>N</i> indicates the CPU number. The value is 1 or 2 .
CPUN Memory	Status of the memory corresponding to the CPU	Memory module corresponding to CPU <i>N</i> <i>N</i> indicates the CPU number. The value is 1 or 2 .
FAN <i>N</i> F Status	Fan fault status	Fan module <i>N</i> <i>N</i> indicates the fan module number. The value ranges from 1 to 7 .
FAN <i>N</i> R Status		
DIMM <i>N</i>	DIMM status	DIMM <i>N</i> <i>N</i> indicates the DIMM slot number.
RTC Battery	RTC battery status. An alarm is generated when the voltage is lower than 1 V.	RTC battery on the mainboard
PCIE Status	PCIE status error	PCIE card
Power Button	Power button pressed	Mainboard and power button

Sensor	Description	Component
Watchdog2	Watchdog	Mainboard
Mngmnt Health	Management subsystem health status	Management modules
UID Button	UID button status	Mainboard
PwrOk Sig. Drop	Voltage dip status	Mainboard
PwrOn TimeOut	Power-on timeout	Mainboard
PwrCap Status	Power capping status	Mainboard
HDD Backplane	Hardware presence	Drive backplane
HDD BP Status	Drive backplane health status	Drive Backplane
RiserN Card	Hardware presence	Riser card <i>N</i> <i>N</i> indicates the riser card slot number. The value is 1 or 2 .
FANN Presence	Fan presence	Fan module <i>N</i> <i>N</i> indicates the fan module number. The value ranges from 1 to 7 .
RAID Presence	RAID presence	RAID Controller Card
PS Redundancy	Redundancy failure due to PSU removal	Power supply unit (PSU)
RAID Status	RAID controller card health status	RAID Controller Card
RAID PCIE ERR	Health status of the RAID controller card in fault diagnosis	RAID Controller Card
RAID Card BBU	LSI SAS3106 RAID controller card BBU	RAID Controller Card
PSN Status	PSU status	PSU <i>N</i> <i>N</i> indicates the PSU number. The value is 1 or 2 .
PSN Fan Status	PSU fan fault status	PSUN <i>N</i> indicates the PSU number. The value is 1 or 2 .
PSN Temp Status	PSU presence	PSUN <i>N</i> indicates the PSU number. The value is 1 or 2 .
DISKN	Disk status	Drive <i>N</i>

Sensor	Description	Component
		<i>N</i> indicates the drive slot number. The value ranges from 0 to 9 .
PCIe RAID\$ Temp	Temperature of the PCIe RAID controller card	PCIe RAID controller card
M2 Temp(PCIe\$)	Maximum temperature of all M.2 drives of the RAID controller card	PCIe RAID controller card
PCIe\$ OP Temp	PCIe card optical module temperature	PCIe card
PCIe NIC\$ Temp	PCIe card chip temperature	PCIe card
PCIe FC\$ Temp	PCIe card chip temperature	PCIe card
1711 Core Temp	Core temperature of the BMC management chip	BMC card
PS\$ IIn	PSU input current	Power supply unit (PSU)
PS\$ IOut	PSU output current	Power supply unit (PSU)
PS\$ Pout	PSU output power	Power supply unit (PSU)
PS\$ Temp	Maximum internal temperature of the PSU	Power supply unit (PSU)
PS\$ Inlet Temp	PSU air inlet temperature	Power supply unit (PSU)
AreaIntrusion	Listening to the unpacking action	Mainboard
OCP\$ OP Temp	OCP card optical module temperature	OCP 3.0 Network Adapters
OCP\$ Temp	OCP card chip temperature	OCP 3.0 Network Adapters
CPUN PMem Temp	CPU PMem module temperature	PMem module corresponding to CPU <i>N</i> <i>N</i> indicates the CPU number. The value is 1 or 2 .
Riser\$ Temp	Riser card temperature	Riser cards
Disk BP\$ Temp	Drive backplane temperature	Drive Backplanes
SSD Max Temp	Maximum SSD temperature	SSD
RAID BBU Temp	RAID controller card capacitor temperature	Supercapacitor of the RAID controller card
IB\$ Temp	IB NIC temperature	IB card
SAS Cable	Entity presence	SAS cable on the mainboard

Sensor	Description	Component
LCD Status	LCD health status	LCD
LCD Presence	LCD presence	LCD
PCIe\$ Temp	PCIe card chip temperature	PCIe card
PCIe\$ Card BBU	BBU status of the PCIe RAID controller card	PCIe RAID controller card
GPU\$ Power	GPU card power	GPU cards
GPU\$ Temp	GPU temperature	GPU cards
GPU\$ MINI Temp	Mini chip temperature of the GPU card	GPU cards
GPU\$ DDR Temp	DDR chip temperature of the GPU card	GPU cards
GPU\$ HBM Temp	HBM chip temperature of the GPU card	GPU cards
CPU Usage	CPU usage.	N/A
Memory Usage	Memory usage.	
ACPI State	ACPI status	
SysFWProgress	Software process and system startup errors	
System Notice	Hot restart reminder and fault diagnosis program information collection	
System Error	System suspension or restart. Check the background logs.	
SysRestart	Cause of system restart	
Boot Error	Boot error	
BMC Boot Up	BMC startup events	
BMC Time Hopping	Time hopping	
NTP Sync Failed	NTP synchronization failure and recovery events	
SEL Status	SEL full or clearing events	
Op. Log Full	Operation log full or clearing events	
Sec. Log Full	Security log full or clearing events	
Host Loss	System monitoring software	

Sensor	Description	Component
	(BMA) link loss detection	
OAMPort1_ \$ Link	Network port OAM link status	
OAMPort2_ \$ Link	Network port OAM link status	

B Glossary

B.1 A-E

B

BMC	The baseboard management controller (BMC) complies with the Intelligent Platform Management Interface (IPMI). It collects, processes, and stores sensor signals, and monitors the operating status of components. The BMC provides the hardware status and alarm information about the managed objects to the upper-level management system, so that the management system can manage the objects.
------------	--

E

ejector lever	A part on the panel of a device used to facilitate installation or removal of the device.
Ethernet	A baseband local area network (LAN) architecture developed by Xerox Corporation by partnering with Intel and DEC. Ethernet uses the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) access method and allows data transfer over various cables at 10 Mbit/s. The Ethernet specification is the basis for the IEEE 802.3 standard.

B.2 F-J

G

Gigabit Ethernet (GE)	An extension and enhancement of traditional shared media Ethernet standards. It is compatible with 10 Mbit/s and 100 Mbit/s Ethernet and complies with IEEE 802.3z standards.
------------------------------	---

H

hot swap	Replacing or adding components without stopping or shutting down the system.
-----------------	--

B.3 K-O

K

KVM	A hardware device that provides public video, keyboard and mouse (KVM).
------------	---

B.4 P-T

P

panel	An external component (including but not limited to ejector levers, indicators, and ports) on the front or rear of the server. It seals the front and rear of the chassis to ensure optimal ventilation and electromagnetic compatibility (EMC).
Peripheral Component Interconnect Express (PCIe)	A computer bus PCI, which uses the existing PCI programming concepts and communication standards, but builds a faster serial communication system. Intel is the main sponsor for PCIe. PCIe is used only for internal interconnection. A PCI system can be transformed to a PCIe system by modifying the physical layer instead of software. PCIe delivers a faster speed and can replace almost all AGP and PCI buses.

R

redundancy	A mechanism that allows a backup device to automatically take over services from a faulty device to ensure uninterrupted running of the system.
redundant array of independent disks (RAID)	A storage technology that combines multiple physical drives into a logical unit for the purposes of data redundancy and performance improvement.

S

server	A special computer that provides services for clients over a network.
---------------	---

system event log (SEL)	Event records stored in the system used for subsequent fault diagnosis and system recovery.
-------------------------------	---

B.5 U-Z

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
UltraPath Interconnect (UPI)	A point-to-point processor interconnect developed by Intel.

C Acronyms and Abbreviations

C.1 A-E

A

AC	alternating current
AES	Advanced Encryption Standard New Instruction Set
ARP	Address Resolution Protocol
AVX	Advanced Vector Extensions

B

BBU	backup battery unit
BIOS	Basic Input/Output System
BMC	baseboard management controller

C

CCC	China Compulsory Certification
CD	calendar day
CE	Conformite Europeenne
CIM	Common Information Model
CLI	command-line interface

D

DC	direct current
DDR4	Double Data Rate 4
DDDC	double device data correction
DEMT	Dynamic Energy Management Technology
DIMM	dual in-line memory module
DRAM	dynamic random-access memory
DVD	digital video disc

E

ECC	error checking and correcting
ECMA	European Computer Manufacturer Association
EDB	Execute Disable Bit
EN	European Efficiency
ERP	enterprise resource planning
ETS	European Telecommunication Standards

C.2 F-J

F

FB-DIMM	Fully Buffered DIMM
FC	Fiber Channel
FCC	Federal Communications Commission
FCoE	Fibre Channel over Ethernet
FTP	File Transfer Protocol

G

GE	Gigabit Ethernet
GPIO	General Purpose Input/Output
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
IC	Industry Canada
ICMP	Internet Control Message Protocol
IDC	Internet Data Center
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Message Protocol
IOPS	input/output operations per second
IP	Internet Protocol
IPC	Intelligent Power Capability
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface

C.3 K-O

K

KVM	keyboard, video, and mouse
------------	----------------------------

L

LC	Lucent Connector
-----------	------------------

LRDIMM	load-reduced dual in-line memory module
LED	light emitting diode
LOM	LAN on motherboard

M

MAC	media access control
MMC	module management controller

N

NBD	next business day
NC-SI	Network Controller Sideband Interface

O

OCP	Open Compute Project
------------	----------------------

C.4 P-T

P

PCIe	Peripheral Component Interconnect Express
PDU	power distribution unit
PHY	physical layer
PMBUS	power management bus
POK	Power OK
PWM	pulse-width modulation
PXE	Preboot Execution Environment

R

RAID	redundant array of independent disks
-------------	--------------------------------------

RAS	reliability, availability and serviceability
RDIMM	registered dual in-line memory module
REACH	Registration Evaluation and Authorization of Chemicals
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
SCM	supply chain management
SDDC	single device data correction
SERDES	serializer/deserializer
SGMII	serial gigabit media independent interface
SMI	serial management interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOL	serial over LAN
SONCAP	Standards Organization of Nigeria-Conformity Assessment Program
SSD	solid-state drive
SSE	Streaming SIMD Extension

T

TACH	tachometer signal
TBT	Turbo Boost Technology
TCG	Trusted Computing Group
TCM	trusted cryptography module
TCO	total cost of ownership
TDP	thermal design power
TELNET	Telecommunication Network Protocol

TET	Trusted Execution Technology
TFM	TransFlash module
TFTP	Trivial File Transfer Protocol
TOE	TCP offload engine
TPM	trusted platform module

C.5 U-Z

U

UDIMM	unbuffered dual in-line memory module
UEFI	Unified Extensible Firmware Interface
UID	unit identification light
UL	Underwriter Laboratories Inc.
UPI	UltraPath Interconnect
USB	Universal Serial Bus

V

VCCI	Voluntary Control Council for Interference by Information Technology Equipment
VGA	Video Graphics Array
VLAN	virtual local area network
VRD	voltage regulator-down

W

WEEE	waste electrical and electronic equipment
WSMAN	Web Service Management