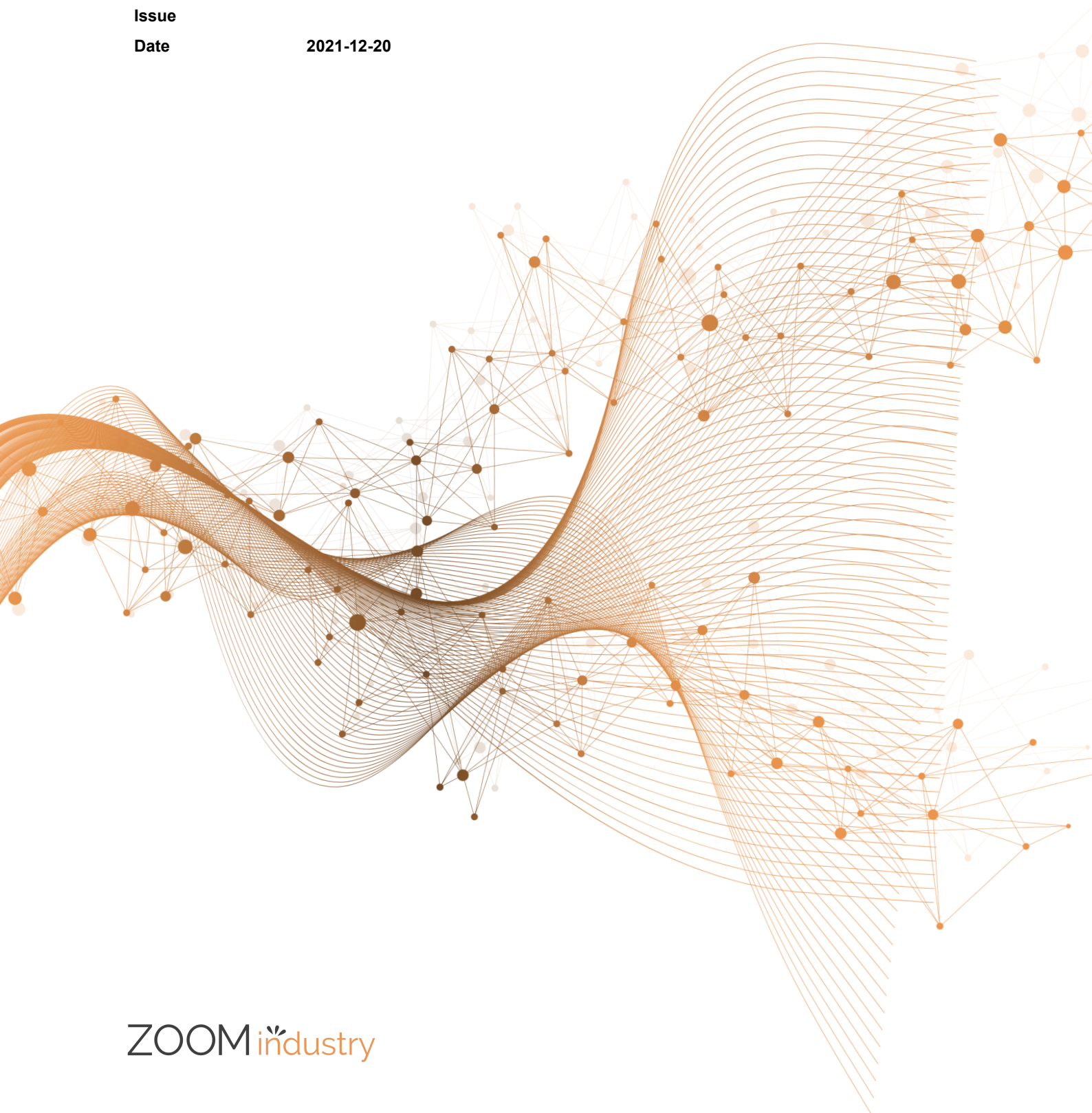


ZOOM Hard' Server 2488H V6 Server User Guide

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

ZOOM tecnologia

Contents

About This Document	vii
1 Overview	9
1.1 Product Introduction	9
1.2 Physical Structure	10
1.3 Logical Structure	12
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	18
2.2 Processor.....	19
2.3 Memory	20
2.3.1 DDR4 Memory	20
2.3.1.1 Memory Identifier.....	20
2.3.1.2 Memory Subsystem Architecture.....	21
2.3.1.3 Memory Compatibility	23
2.3.1.4 DIMM Installation Rules	25
2.3.1.5 Memory Installation Positions	26
2.3.1.6 Memory Protection Technologies	29
2.3.2 DCPMM	30
2.3.2.1 Memory Compatibility	30
2.3.2.2 DIMM Installation Rules	31
2.3.2.3 Memory Installation Positions	32
2.4 Storage	35
2.4.1 Drive Configurations	35
2.4.2 Drive Numbering	36
2.4.3 Drive Indicators	37
2.4.4 RAID Controller Card	38
2.5 Network	38
2.5.1 LOMs.....	38
2.6 I/O Expansion	41
2.6.1 PCIe Cards.....	41

2.6.2 PCIe Slots	41
2.6.3 PCIe Slot Description	41
2.7 PSUs	43
2.8 Fans.....	43
2.9 LCD	44
2.10 Boards.....	46
2.10.1 Mainboard.....	46
2.10.2 Daughter Board.....	48
2.10.3 Drive Backplane	49
3 Product Specifications.....	53
3.1 Technical Specifications	53
3.2 Environmental Specifications	56
3.3 Physical Specifications	58
4 Software and Hardware Compatibility	60
5 Safety Instructions	61
5.1 Security.....	61
5.2 Maintenance and Warranty	64
6 ESD	65
6.1 ESD Prevention	65
6.2 Grounding Methods for ESD Prevention.....	65
7 Installation and Configuration.....	67
7.1 Installation Environment Requirements	67
7.1.1 Space and Airflow Requirements.....	67
7.1.2 Temperature and Humidity Requirements	68
7.1.3 Cabinet Requirements.....	68
7.2 Hardware Installation.....	69
7.2.1 Installation Overview.....	69
7.2.2 Unpacking the Server.....	70
7.2.3 Installing Optional Parts	70
7.2.4 Installing Server Guide Rails	71
7.2.4.1 Installing L-Shaped Guide Rails.....	71
7.2.4.2 Installing the Static Rail Kit.....	73
7.2.4.3 Installing the Ball Bearing Rail Kit	74
7.2.4.3.1 Ball Bearing Rail Kit 1	74
7.2.4.3.2 Ball Bearing Rail Kit 2	75
7.2.5 Installing a Server	77
7.2.5.1 Installing a Server on L-Shaped Guide Rails or the Static Rail Kit	77
7.2.5.2 Installing a Server on the Ball Bearing Rail Kit	78
7.2.6 Connecting External Cables.....	82
7.2.6.1 Cabling Guide.....	82

7.2.6.2 Connecting Mouse, Keyboard, and VGA Cables	83
7.2.6.3 Connecting Network Cables	83
7.2.6.4 Connecting a Cable to an Optical Port	85
7.2.6.5 Connecting a USB Device	88
7.2.6.6 Connecting a Serial Cable	89
7.2.6.7 Connecting PSU Cables	90
7.2.6.7.1 Connecting the AC PSU Cable	90
7.2.6.7.2 Connecting the DC PSU Cable	91
7.2.6.8 Checking Cable Connections	92
7.3 Power-On and Power-Off	93
7.3.1 Power-On Procedure	93
7.3.2 Power-Off Procedure	94
7.4 Initial Configuration	95
7.4.1 Default Information	95
7.4.2 Configuration Overview	96
7.4.3 Changing Initial Passwords	97
7.4.3.1 Changing the Initial Password of the Default iBMC User	97
7.4.3.1.1 Changing the Initial Password of the Default iBMC User (Versions Earlier Than V600)	97
7.4.3.1.2 Changing the Initial Password of the Default iBMC User (V600 and Later Versions)	99
7.4.3.2 Changing the Initial Password of the iBMC U-Boot	101
7.4.4 Checking the Server	102
7.4.4.1 Checking the Server (Versions Earlier than V600)	103
7.4.4.2 Checking the Server (V600 and Later Versions)	104
7.4.5 Configuring the iBMC IP Address	106
7.4.6 Configuring RAID	107
7.4.7 Configuring the BIOS	108
7.4.7.1 Accessing the BIOS	109
7.4.7.2 Setting the System Boot Sequence	109
7.4.7.3 Configuring PXE for a NIC	110
7.4.7.4 Setting the BIOS Password	110
7.4.7.5 Switching the GUI Language	111
7.4.7.6 Restarting the Server	112
7.4.8 Installing an OS	112
7.4.9 Upgrading the System	113
8 Troubleshooting Guide	114
9 Common Operations	115
9.1 Querying the iBMC IP Address	115
9.2 Logging In to the iBMC WebUI	116
9.2.1 Logging In to the iBMC WebUI (Versions Earlier Than V600)	116
9.2.2 Logging In to the iBMC WebUI (V600 and Later Versions)	120
9.3 Logging In to the Desktop of a Server	125

9.3.1 Using the Remote Virtual Console.....	125
9.3.1.1 iBMC	125
9.3.1.1.1 Versions Earlier Than V600	125
9.3.1.1.2 V600 and Later Versions	128
9.3.2 Logging In to a Server Using the Independent Remote Console	131
9.3.2.1 Versions Earlier Than V600	131
9.3.2.1.1 Windows	131
9.3.2.1.2 Ubuntu	133
9.3.2.1.3 Mac	136
9.3.2.1.4 Red Hat	138
9.3.2.2 V600 and Later Versions	140
9.3.2.2.1 Windows	140
9.3.2.2.2 Ubuntu	143
9.3.2.2.3 Mac	145
9.3.2.2.4 Red Hat	148
9.4 Logging In to the CLI	150
9.4.1 Logging In to the CLI Using PuTTY over a Network Port	150
9.4.2 Logging In to the CLI Using PuTTY over a Serial Port	152
9.5 Managing VMD	153
9.5.1 Enabling VMD	154
9.5.2 Disabling VMD	154
9.6 Accessing the BIOS	155
9.6.1 Accessing the BIOS (V3XX or Earlier)	155
9.6.2 Accessing the BIOS (V6XX or Later)	157
10 More Information.....	161
10.1 Obtaining Technical Support	161
10.2 Product Information	162
10.3 Product Configuration Resources	162
10.4 Maintenance Tools	163
11 Software and Configuration Utilities	164
11.1 iBMC	164
11.2 BIOS	165
A Appendix	166
B Glossary.....	176
C Acronyms and Abbreviations	179

About This Document

Overview

This document describes the 2488H V5 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	2021-12-20	This issue is the first official release.

1 Overview

- [1.1 Product Introduction](#)
- [1.2 Physical Structure](#)
- [1.3 Logical Structure](#)

1.1 Product Introduction

Hard'Server 2488H V5 (2488H V5) is a 2U 4-socket rack server developed for Internet data center (IDC), cloud computing, enterprise, and telecom service applications.

The 2488H V5 is ideal for applications such as databases, cloud computing, virtualization, and in-memory computing.

The secure, compact 2488H V5 is a highly expandable server delivering high-performance computing, large storage capacity and low power consumption. It is easy to deploy and manage and supports virtualization.

NOTE

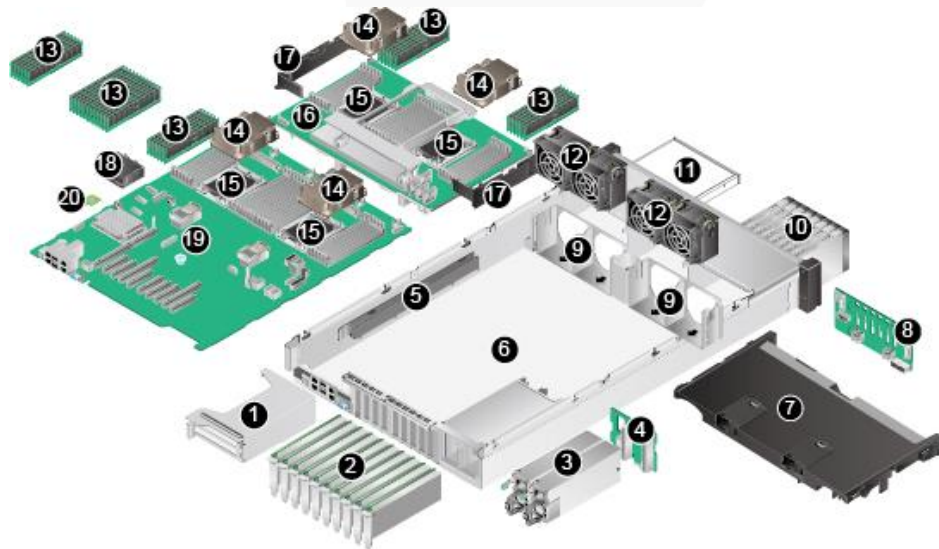
For details about the 2488H V5 nameplate information, see A.3 Nameplate .

Figure 1-1 2488H V5 (with 25 drives)



1.2 Physical Structure

Figure 1-2 Physical structure of a 2488H V5 with 8 x 2.5" drives (example)



1	Riser card	2	PCIe card
3	Power supply unit (PSU)	4	PSU backplane
5	Cable organizer	6	Chassis

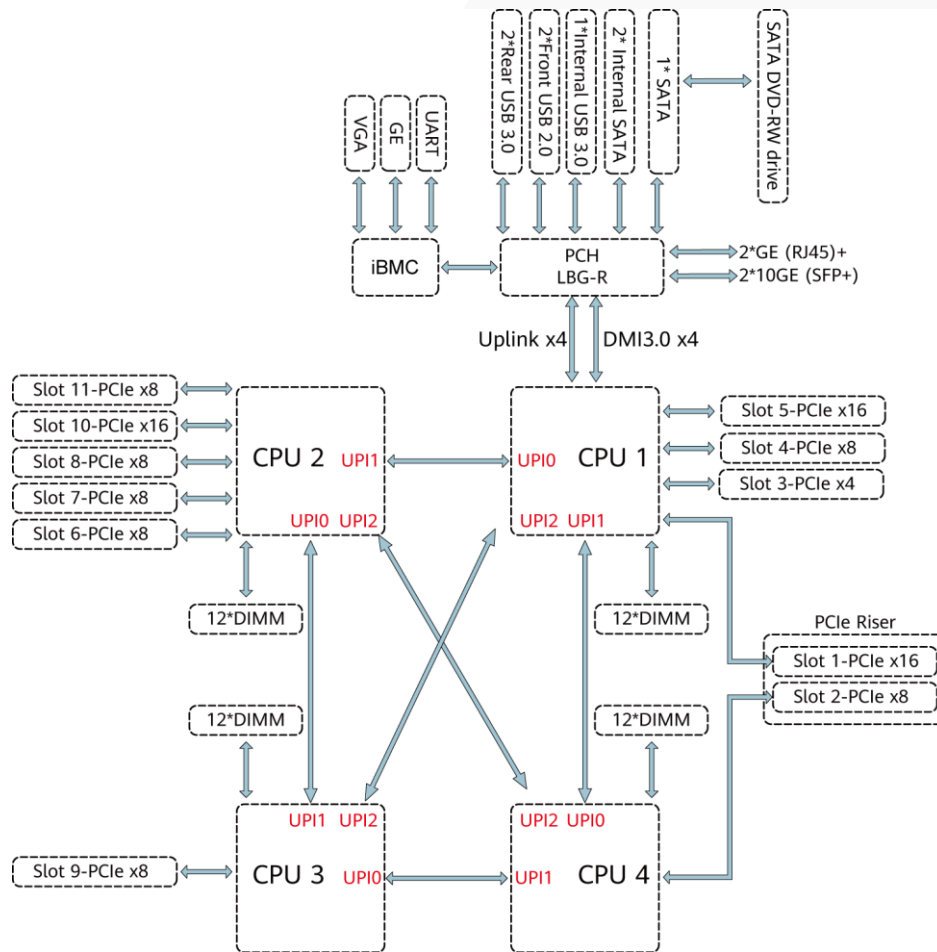
7	Air duct	8	Drive Backplane
9	Fan module bracket	10	Drive
11	DVD drive (or LCD)	12	Fan module
13	Memory	14	Heat sink
15	Processor	16	Daughter board
17	Cable organizer of the daughter board	18	Supercapacitor
19	Mainboard	20	TPM/TCM

 **NOTE**

- CPUs 1 and 2 are located on the mainboard, and CPUs 3 and 4 are located on the daughter board.
- If the server is configured with a daughter board, the air duct is not required. If the server is not configured with a daughter board, the air duct is required.

1.3 Logical Structure

Figure 1-3 2488H V5 logical structure



- The server supports two or four Intel® Xeon® Scalable processors.
- The server supports up to 48 memory modules.
- The CPUs (processors) interconnect with each other through three UPI links at a speed of up to 10.4 GT/s.
- The server provides 11 standard PCIe 3.0 slots of various specifications.
- The server provides low-speed I/O ports, such as the VGA port, USB 3.0 ports, and serial ports (RJ45).
- The server provides four LOM ports, including two 10GE optical ports and two GE electrical ports.

2 Hardware Description

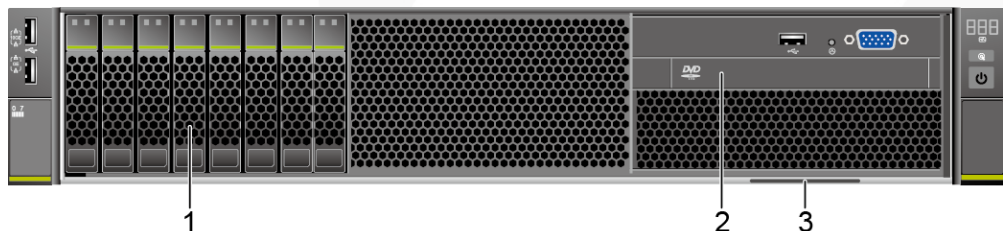
- 2.1 Front Panel
- 2.2 Processor
- 2.3 Memory
- 2.4 Storage
- 2.5 Network
- 2.6 I/O Expansion
- 2.7 PSUs
- 2.8 Fans
- 2.9 LCD
- 2.10 Boards

2.1 Front Panel

2.1.1 Appearance

- 8 x 2.5" SAS/SATA drive configuration

Figure 2-1 Front view



1	Drives	2	Built-in DVD drive or touchable LCD
---	--------	---	-------------------------------------

3	Slide-out label plate (with an SN label)	-	-
---	--	---	---

- 24 x 2.5" (24 x SAS/SATA or NVMe or 16 x SAS/SATA + 8 x NVMe) drive configuration

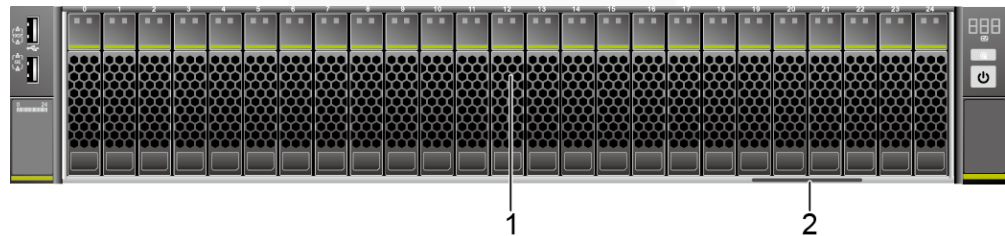
Figure 2-2 Front view



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

- 25 x 2.5" SAS/SATA drive configuration

Figure 2-3 Front view



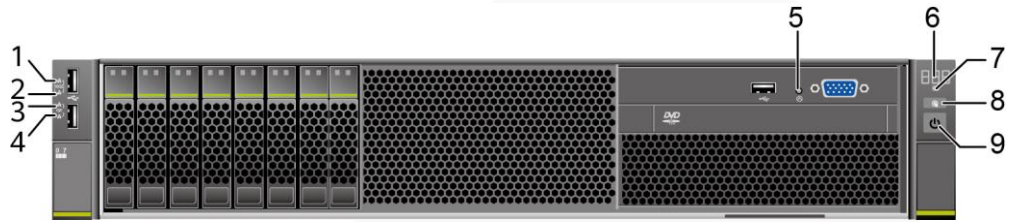
1	Drives	2	Slide-out label plate (with an SN label)
---	--------	---	--

2.1.2 Indicators and Buttons

Indicator and Button Positions

- 8 x 2.5" SAS/SATA drive configuration

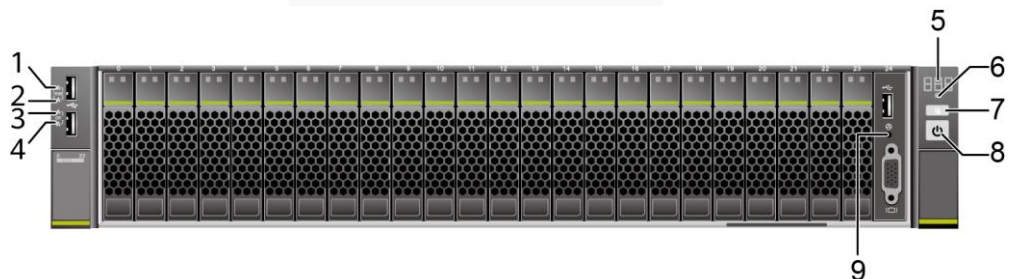
Figure 2-4 Indicators and buttons on the front panel



1	Connection status indicator for 10GE LOM port 1	2	Connection status indicator for 10GE LOM port 2
3	Connection status indicator for GE LOM port 1	4	Connection status indicator for GE LOM port 2
5	Non-Maskable Interrupt (NMI) button	6	Fault diagnosis LED
7	Health status indicator	8	UID button/indicator
9	Power button/indicator	-	-

- 24 x 2.5" (24 x SAS/SATA or NVMe or 16 x SAS/SATA + 8 x NVMe) drive configuration

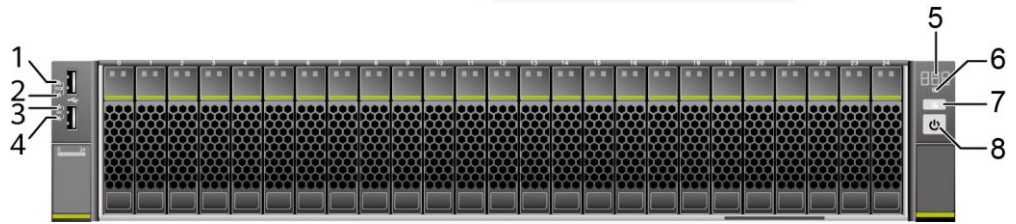
Figure 2-5 Indicators and buttons on the front panel



1	Connection status indicator for 10GE LOM port 1	2	Connection status indicator for 10GE LOM port 2
3	Connection status indicator for GE LOM port 1	4	Connection status indicator for GE LOM port 2
5	Fault diagnosis LED	6	Health status indicator
7	UID button/indicator	8	Power button/indicator
9	NMI button	-	-

- 25 x 2.5" SAS/SATA drive configuration

Figure 2-6 Indicators and buttons on the front panel







1	Connection status indicator for 10GE LOM port 1	2	Connection status indicator for 10GE LOM port 2
3	Connection status indicator for GE LOM port 1	4	Connection status indicator for GE LOM port 2
5	Fault diagnosis LED	6	Health status indicator
7	UID button/indicator	8	Power button/indicator

Indicator and Button Descriptions

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

Sign	Indicator and Button	Description
	Fault diagnosis LED	<ul style="list-style-type: none"> ---: The device is operating properly. Error code: A component is faulty. For details about error codes, see the FusionServer Rack Server iBMC Alarm Handling.
	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, holding down this button for 6 seconds will forcibly power off the device.

Sign	Indicator and Button	Description
		<ul style="list-style-type: none"> When the power indicator is steady yellow, you can press this button to power on the device.
	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 description:</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.
	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.
	NMI button	<p>A non-maskable interrupt (NMI) is generally triggered to stop the OS for debugging. To trigger an NMI, press this button or click the button on the iBMC WebUI.</p> <p>NOTICE</p> <ul style="list-style-type: none"> Press the NMI button only when the OS is abnormal. Do not press this button when the server is operating properly. An NMI does not gracefully shut down the OS and causes service interruption and data loss. Before pressing the NMI button, ensure that the OS has the NMI processing program. Otherwise, the OS may crash. Exercise caution when pressing this button.
	LOM port connection status indicator	<p>Each indicator shows the connection status of an Ethernet LOM port.</p> <ul style="list-style-type: none"> Off: The network port is not in use or has failed. Steady green: The network port is properly connected. <p>NOTE</p> <ul style="list-style-type: none"> The indicators correspond to two 10GE and two GE network ports on the mainboard. The LOM has a standby power supply and will not be powered off even if the service system is powered off. As long as the LOM ports are properly connected to other working network devices, the network ports will

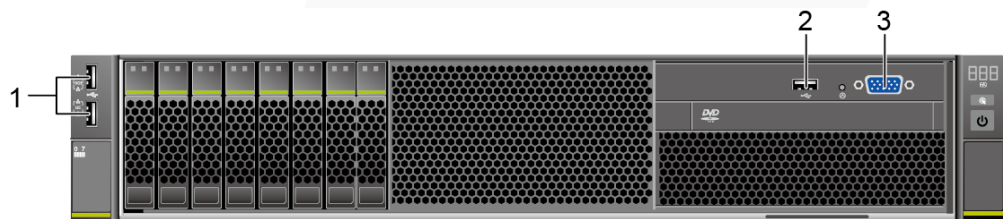
Sign	Indicator and Button	Description
		remain connected and the indicators are on.

2.1.3 Ports

Port Positions

- 8 x 2.5" SAS/SATA drive configuration

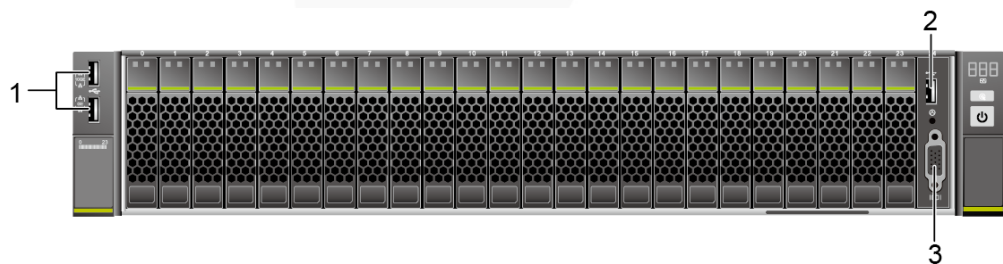
Figure 2-7 Ports on the front panel



1	USB 2.0 ports	2	USB 3.0 port
3	VGA port	-	-

- 24 x 2.5" (24 x SAS/SATA or NVMe or 16 x SAS/SATA + 8 x NVMe) drive configuration

Figure 2-8 Ports on the front panel



1	USB 2.0 ports	2	USB 3.0 port
3	VGA port	-	-

- 25 x 2.5" SAS/SATA drive configuration

Figure 2-9 Ports on the front panel



1	USB 2.0 ports	-	-
---	---------------	---	---

Port Description

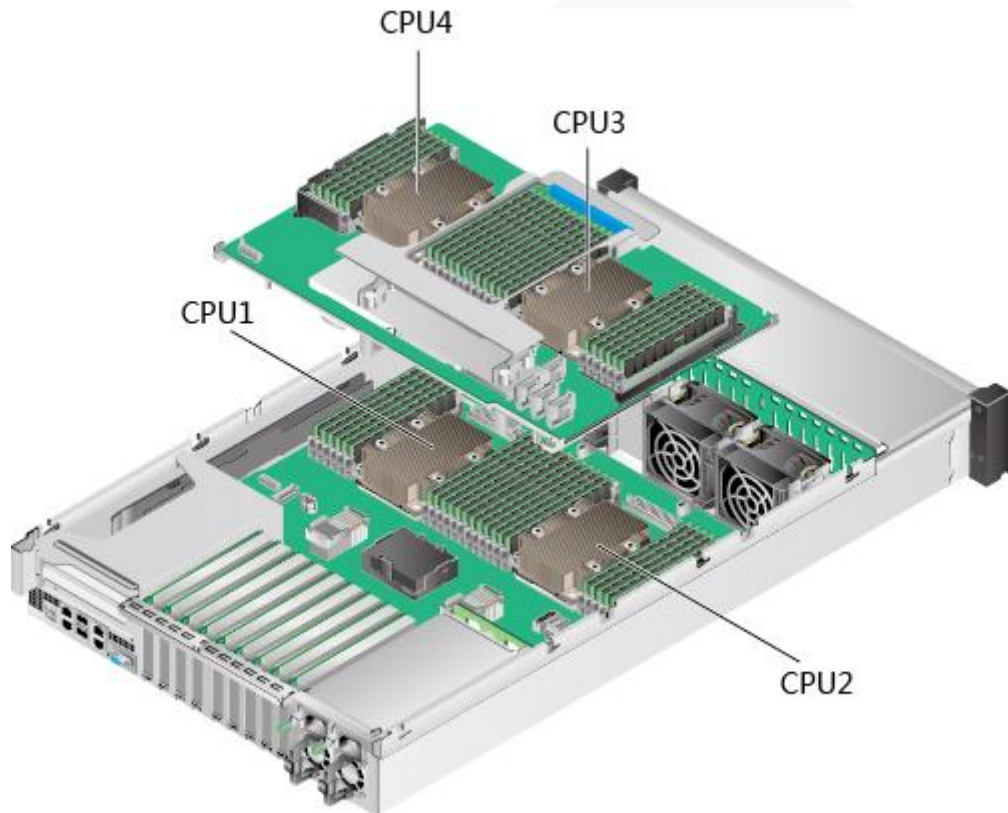
Table 2-2 Ports on the front panel

Port	Type	Quantity ^{Note}	Description
VGA port	DB15	1	Used to connect a display terminal, such as a monitor or KVM.
USB port	USB 2.0	2	Used to connect to a USB device. NOTICE Before connecting an external USB device, check that the USB device functions properly. The server may operate abnormally if an abnormal USB device is connected.
	USB 3.0	1	
Note: The number of ports varies depending on server configuration. This table lists the maximum number of ports in different configurations.			

2.2 Processor

- The server supports two or four processors.
- If two processors are required, install them in sockets **CPU1** and **CPU2**.
- The same model of processors must be used in a server.
- Contact your local sales representative or use the [Compatibility Checker](#) to determine the components to be used.

Figure 2-10 Processor positions



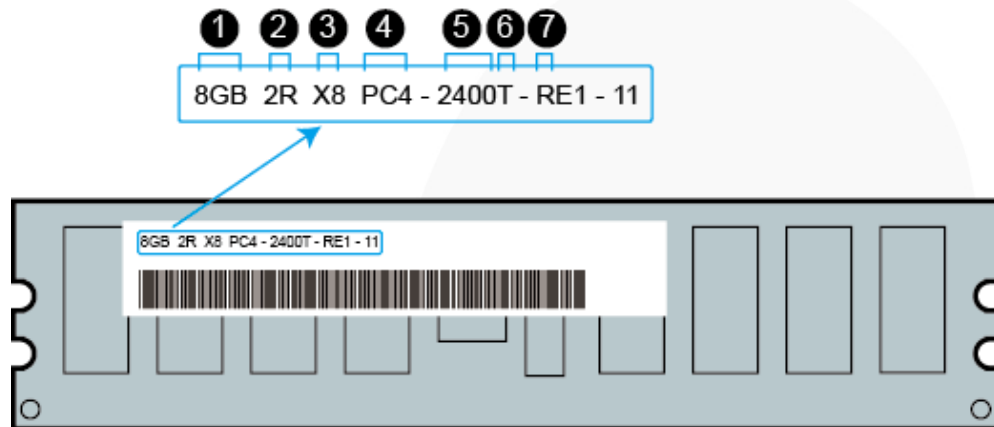
2.3 Memory

2.3.1 DDR4 Memory

2.3.1.1 Memory Identifier

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

Figure 2-11 Memory identifier



Callout	Description	Definition
1	Capacity of the memory module	<ul style="list-style-type: none"> • 8 GB • 16 GB • 32 GB • 64 GB • 128 GB
2	Number of ranks of the memory module	<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"> • PC3: DDR3 • PC4: DDR4
5	Maximum memory speed	<ul style="list-style-type: none"> • 2133 MT/S • 2400 MT/S • 2666 MT/S • 2933 MT/S
6	Column Access Strobe (CAS) latency	<ul style="list-style-type: none"> • P: 15 • T: 17
7	DIMM type	<ul style="list-style-type: none"> • R: RDIMM • L: LRDIMM

2.3.1.2 Memory Subsystem Architecture

The 2488H V5 provides 48 memory slots. Each processor integrates six 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 2-3 Memory channels

CPU	Memory Channel	Memory Slot
CPU 1	A (primary)	DIMM000(A)
	A	DIMM001(G)
	B (primary)	DIMM010(B)
	B	DIMM011(H)
	C (primary)	DIMM020(C)
	C	DIMM021(I)
	D (primary)	DIMM030(D)
	D	DIMM031(J)
	E (primary)	DIMM040(E)
	E	DIMM041(K)
	F (primary)	DIMM050(F)
	F	DIMM051(L)
CPU 2	A (primary)	DIMM100(A)
	A	DIMM101(G)
	B (primary)	DIMM110(B)
	B	DIMM111(H)
	C (primary)	DIMM120(C)
	C	DIMM121(I)
	D (primary)	DIMM130(D)
	D	DIMM131(J)
	E (primary)	DIMM140(E)
	E	DIMM141(K)
	F (primary)	DIMM150(F)
	F	DIMM151(L)
CPU 3	A (primary)	DIMM200(A)
	A	DIMM201(G)
	B (primary)	DIMM210(B)
	B	DIMM211(H)

CPU	Memory Channel	Memory Slot
	C (primary)	DIMM220(C)
	C	DIMM221(I)
	D (primary)	DIMM230(D)
	D	DIMM231(J)
	E (primary)	DIMM240(E)
	E	DIMM241(K)
	F (primary)	DIMM250(F)
	F	DIMM251(L)
CPU 4	A (primary)	DIMM300(A)
	A	DIMM301(G)
	B (primary)	DIMM310(B)
	B	DIMM311(H)
	C (primary)	DIMM320(C)
	C	DIMM321(I)
	D (primary)	DIMM330(D)
	D	DIMM331(J)
	E (primary)	DIMM340(E)
	E	DIMM341(K)
	F (primary)	DIMM350(F)
	F	DIMM351(L)

2.3.1.3 Memory Compatibility

Observe the following rules when configuring DDR4 DIMMs:

NOTICE

- A server must use the same model of DDR4 DIMMs, and all the DIMMs operate at the same speed, which is the smallest value of:
 - Memory speed supported by a processor
 - Maximum operating speed of a DIMM
 - 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 use the [Compatibility Checker](#) to determine the components to be used.
-
- The memory can be used with Intel® Xeon® Scalable Skylake and Cascade Lake processors. The maximum memory capacity supported varies depending on the processor model.
 - Skylake processors
 - M processors: 1.5 TB/socket
 - Other processors: 768 GB/socket
 - Cascade Lake processors
 - L processors: 4.5 TB/socket
 - M processors: 2 TB/socket
 - Other processors: 1 TB/socket
 - The total memory capacity is the sum of the capacity of all DDR4 DIMMs.

NOTICE

- The total memory capacity cannot exceed the maximum memory capacity supported by the CPUs.
 - The total memory capacity refers to the capacity when DDR4 DIMMs are fully configured. For details about the memory capacity when DCPMMs are used together with DDR4 DIMMs, see 2.3.2.1 Memory Compatibility.
-
- Use the [Compatibility Checker](#) to determine the capacity type of a single memory module.
 - The maximum number of DIMMs supported by a server varies depending on the CPU type, memory type, rank quantity, and operating voltage.

NOTE

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

Number of DIMMs supported by each channel \leq Number of ranks supported by each memory channel / Number of ranks supported by each DIMM

- 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 2-4 DDR4 memory specifications

Parameter		Specifications
Maximum capacity per DDR4 DIMM (GB)		128
Rated speed (MT/s)		2933
Operating voltage (V)		1.2
Maximum number of DDR4 DIMMs in a server ^a		48
Maximum DDR4 memory capacity of the server (GB) ^b		6144
Maximum operating speed (MT/s)	1DPC ^c	2933 ^d
	2DPC	2666
<ul style="list-style-type: none"> • a: The maximum number of DDR4 memory modules is based on four-processor configuration. The value is halved for a server with two processors. • b: The maximum DDR4 memory capacity varies depending on the processor type. The value listed in this table is based on the assumption that DIMMs are fully configured. • c: DPC (DIMM per channel) indicates the number of DIMMs per channel. • d: If the Cascade Lake processor is used, the maximum operating speed of a DIMM can reach 2933 MT/s. If the Skylake processor is used, the maximum operating speed of a DIMM can reach 2666 MT/s only. 		

2.3.1.4 DIMM Installation Rules

 **NOTE**

This section applies to a server fully configured with DDR4 DIMMs. If DCPMMs are used together, see 2.3.2.2 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:
 - Memory sparing mode
 - Comply with the general installation guidelines.
 - Each memory channel must have a valid online spare configuration.
 - The channels can have different online spare configurations.
 - Each populated channel must have a spare rank.
 - Memory mirroring mode
 - Comply with the general installation guidelines.
 - Each processor supports two integrated memory controllers (IMCs). At least two channels of each IMC are used for installing memory modules (channels 1 and 2, or channels 1, 2, and 3). 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.

2.3.1.5 Memory Installation Positions

A 2488H V5 supports a maximum of 48 DDR4 DIMMs. To maximize the performance, balance the total memory capacity between the installed processors and load the channels similarly whenever possible.

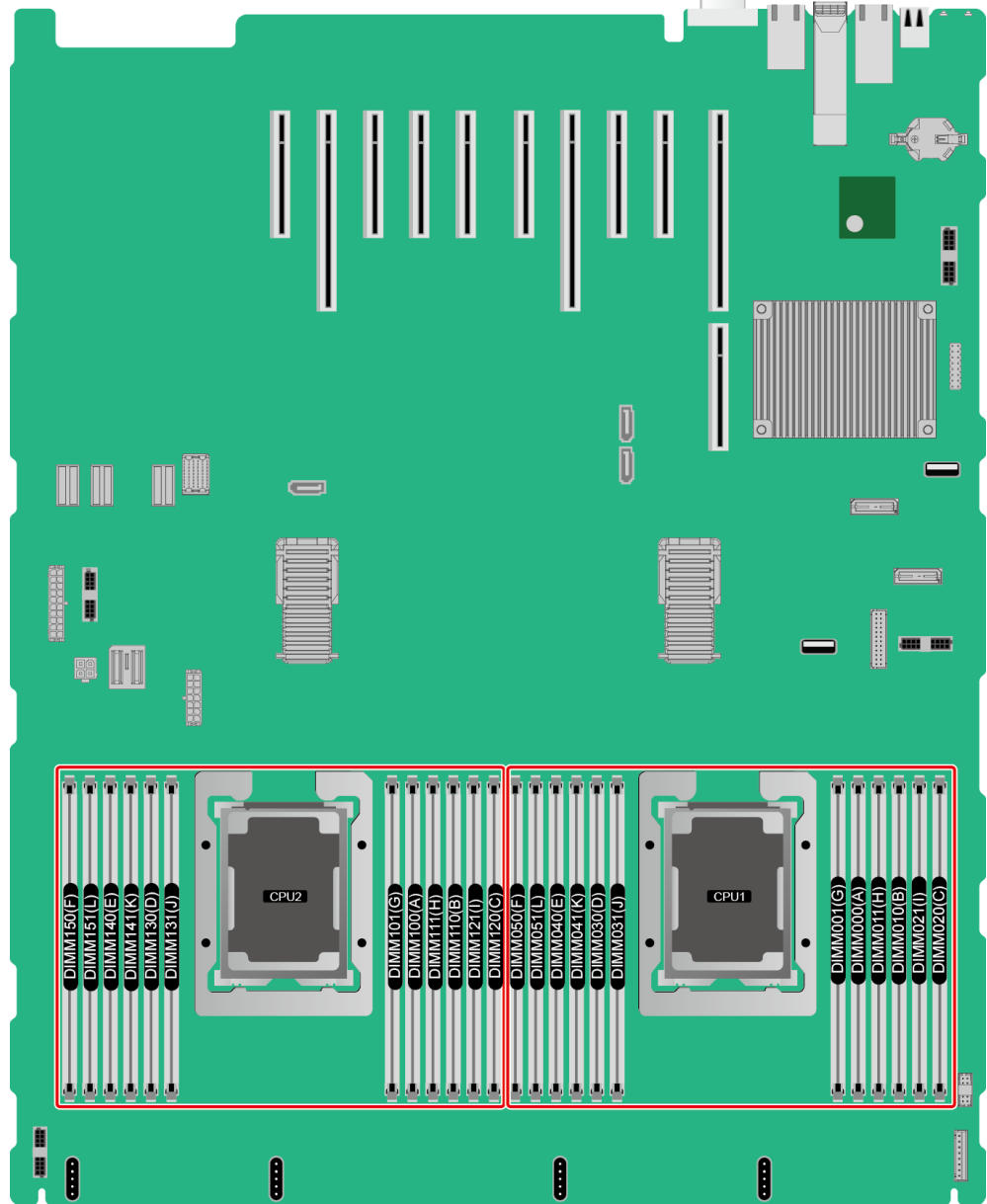
NOTICE

At least one DDR4 DIMM must be installed in the memory slots corresponding to CPU 1.

CPUs 1 and 2 are located on the mainboard, and CPUs 3 and 4 are located on the daughter board.

- Memory slots on the mainboard

Figure 2-12 Memory slots (mainboard)



- Memory slots on the daughter board

Figure 2-13 Memory slots (daughter board)

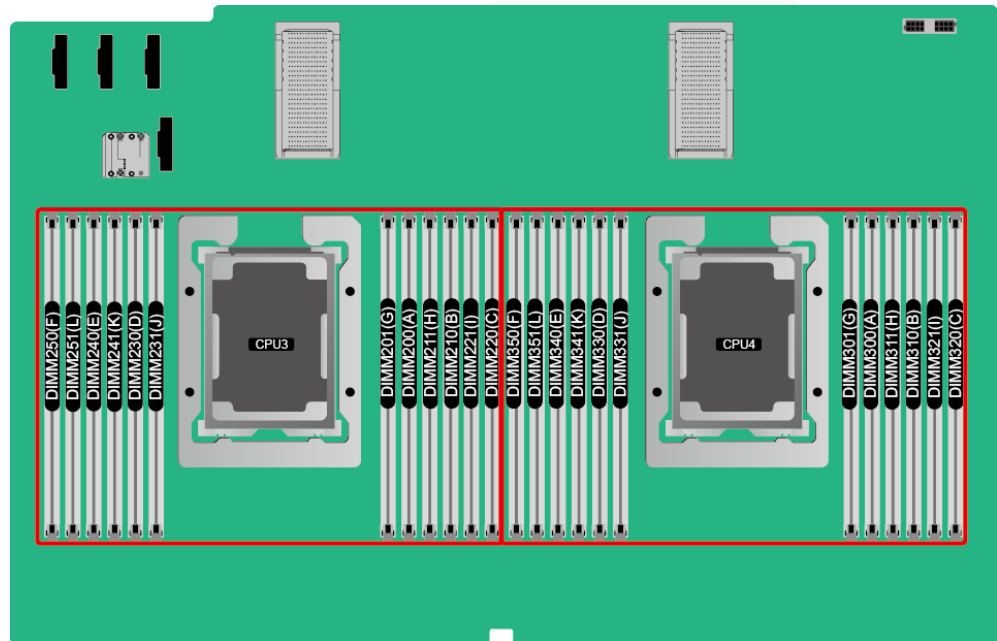


Figure 2-14 DDR4 memory installation guidelines (2 processors)

CPU	Channel	DIMM Slot	Number of DIMMs																							
			(✓: recommended ○: not recommended)																							
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
CPU1	A	DIMM000(A)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM001(G)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	B	DIMM010(B)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM011(H)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	C	DIMM020(C)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM021(I)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	D	DIMM030(D)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM031(J)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	E	DIMM040(E)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM041(K)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	F	DIMM050(F)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM051(L)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
CPU2	A	DIMM100(A)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
		DIMM101(G)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
	B	DIMM110(B)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
		DIMM111(H)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
	C	DIMM120(C)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
		DIMM121(I)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
	D	DIMM130(D)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
		DIMM131(J)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○		
	E	DIMM140(E)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM141(K)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	F	DIMM150(F)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
		DIMM151(L)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	

2.3.2 DCPMM

2.3.2.1 Memory Compatibility

Observe the following rules when configuring DC persistent memory modules (DCPMMs):

NOTICE

- The DCPMMs must be used with the DDR4 memory modules. For details, see the [FusionServer DCPMM User Guide](#).
 - Contact your local sales representative or use the [Compatibility Checker](#) to determine the components to be used.
-
- The memory must be used with Intel® Xeon® Scalable Cascade Lake processors. The maximum memory capacity supported varies depending on the processor model.
 - L processors: 4.5 TB/socket
 - M processors: 2 TB/socket
 - Other processors: 1 TB/socket
 - The DCPMM can work only in App Direct Mode (AD) and Memory Mode (MM). The total supported memory capacity is calculated as follows:
 - DCPMM in AD mode
Total memory capacity = Total capacity of all DCPMMs + Total capacity of all DDR4 memory modules
 - DCPMM in MM mode
Total memory capacity = Total capacity of all DCPMMs (The DDR4 memory modules are used as the cache and therefore are not calculated as memory capacity.)

NOTICE

- The total memory capacity cannot exceed the maximum memory capacity supported by the CPUs.
 - For details about the AD and MM modes, see "Operating Modes" in [FusionServer DCPMM User Guide](#).
-
- Use the [Compatibility Checker](#) to determine the capacity type of a single memory module.

Table 2-5 DCPMM specifications

Item	Specifications		
Capacity per DCPMM (GB)	128	256	512
Rated speed (MT/s)	2666	2666	2666
Operating voltage (V)	1.2	1.2	1.2
Maximum number of DCPMMs in a server ^a	12	12	12

Item	Specifications		
Maximum capacity of the server (GB) ^b	4608	9216	15360
Maximum operating speed (MT/s)	2666	2666	2666
<ul style="list-style-type: none"> • a: The maximum number of DCPMMs is based on dual-processor configuration. The value is halved for a server with only one processor. • b: The maximum memory capacity varies depending on the CPU type and DCPMM working mode. The value listed in this table is based on the assumption that 12 DCPMMs and 12 DDR4 memory modules are used with the L series CPUs and the DCPMMs work in AD mode. • The information listed in this table is for reference only. For details, consult the local sales representative. 			

2.3.2.2 DIMM Installation Rules

- The following are general guidelines for DCPMM installation:
 - The DDR4 memory modules used with the DCPMMs include RDIMMs and LRDIMMs.
 - The DCPMMs used in a server must have the same part number (P/N code).
 - The DDR4 memory modules used with the DCPMMs in a server must have the same part number (P/N code).
- Observe the following when configuring DCPMMs in specific operating mode:
 - MM mode:
 - On the same server, it is recommended that the ratio of FM to NM be 2:1 to 16:1.

 **NOTE**

- Near memory (NM): capacity of DDR4 DIMMs used as the cache.
- Far memory (FM): capacity of the DCPMMs in MM.
- The mapping between the DCPMM and CPU is as follows:
 - DCPMMs require Cascade Lake Platinum or Gold CPU.
 - Table 2-6 lists the maximum memory capacity supported by different CPUs.

Table 2-6 Maximum memory capacity supported by a CPU

CPU Type	Maximum Memory Capacity Supported by a CPU (DDR4 and DCPMM Capacities)
Full-series	1 TB
M series	2 TB
L series	4.5 TB

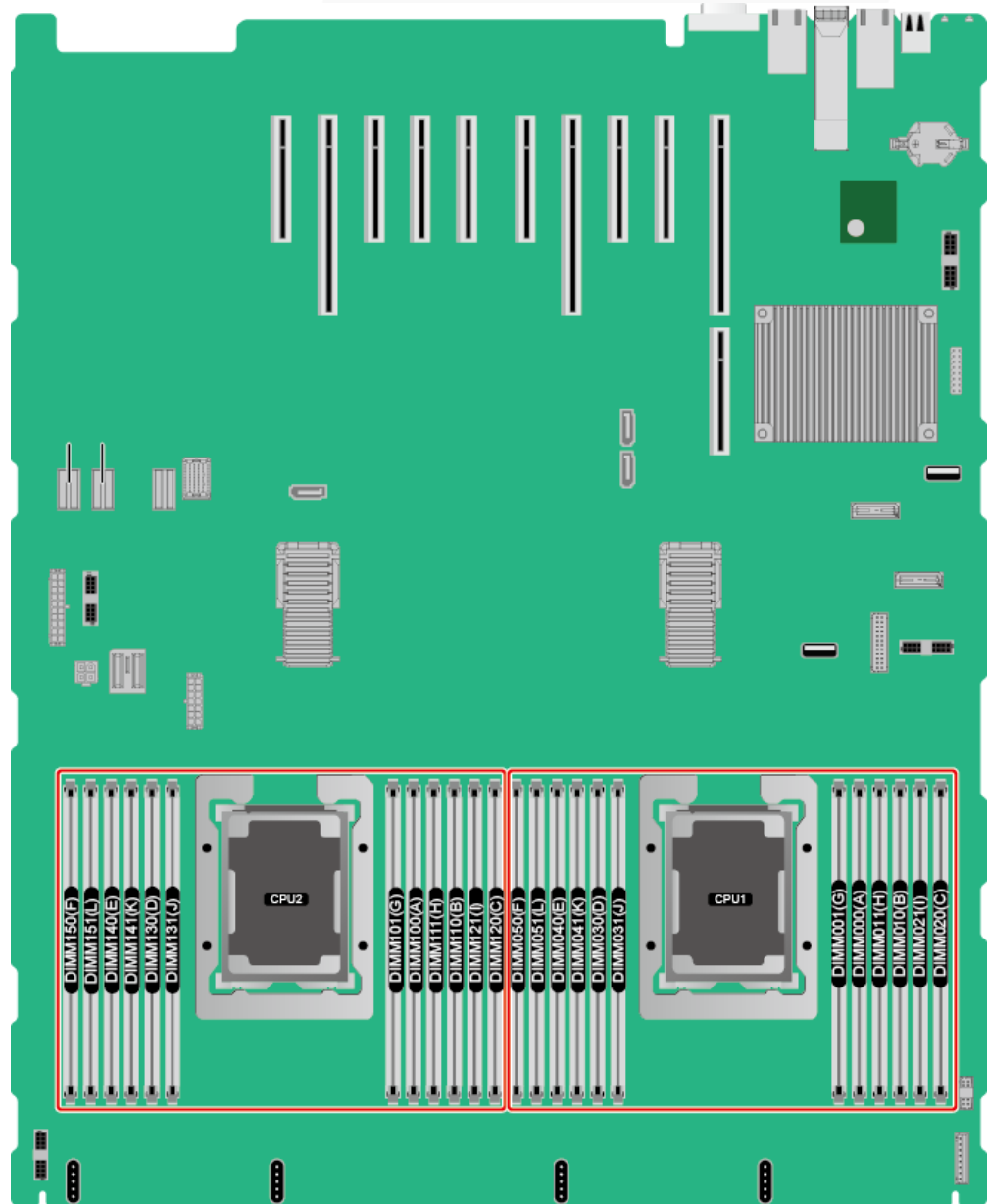
2.3.2.3 Memory Installation Positions

A 2488H V5 supports a maximum of 24 DCPMMs. The DCPMMs must be used with DDR4 DIMMs.

CPU1 and 2 are located on the mainboard, and CPU3 and 4 are located on the daughter board.

- Memory slots on the mainboard

Figure 2-16 Memory slots (mainboard)



- Memory slots on the daughter board

Figure 2-17 Memory slots (daughter board)

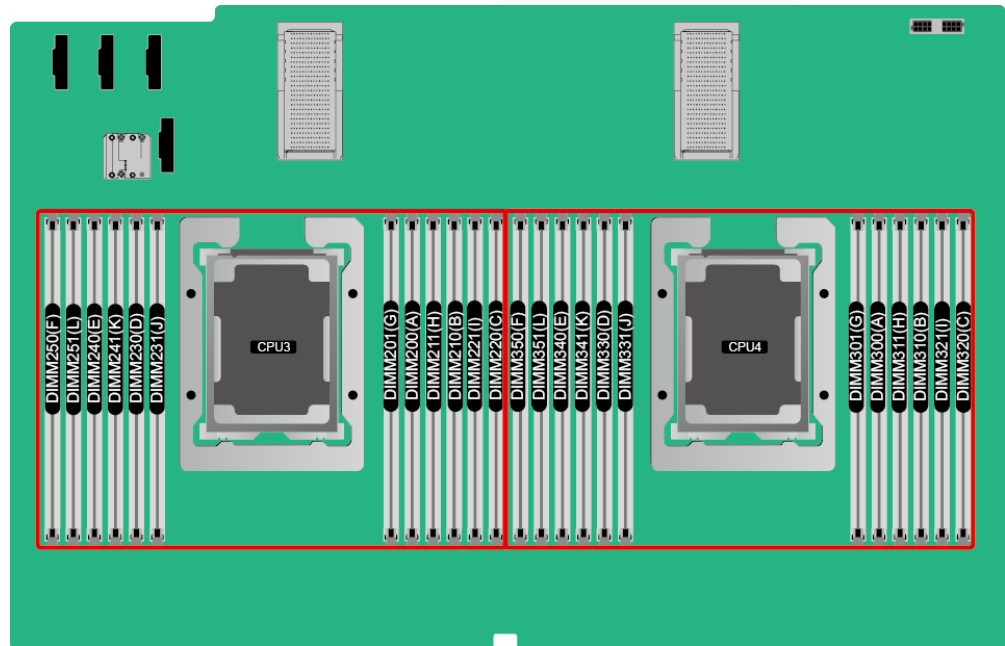


Figure 2-18 DCPMM and DDR4 memory configuration guidelines (2 processors)

CPU	Channel	DIMM Slot	Configurations in Different Modes (●: DDR4 DIMM ○: DCPMM)									
			AD		MM		AD		MM			
			2-2-2	MM	2-2-1	MM	2-1-1	MM	1-1-1	MM		
CPU1	IMC0	A	●	○	○	○	○	○	○	○	○	○
		B	●	○	○	○	○	○	○	○	○	○
		C	●	○	○	○	○	○	○	○	○	○
		D	●	○	○	○	○	○	○	○	○	○
		E	●	○	○	○	○	○	○	○	○	○
		F	●	○	○	○	○	○	○	○	○	○
	IMC1	D	●	○	○	○	○	○	○	○	○	○
		E	●	○	○	○	○	○	○	○	○	○
		F	●	○	○	○	○	○	○	○	○	○
		A	●	○	○	○	○	○	○	○	○	○
		B	●	○	○	○	○	○	○	○	○	○
		C	●	○	○	○	○	○	○	○	○	○
CPU2	IMC0	D	●	○	○	○	○	○	○	○	○	○
		E	●	○	○	○	○	○	○	○	○	○
		F	●	○	○	○	○	○	○	○	○	○
	IMC1	D	●	○	○	○	○	○	○	○	○	○
		E	●	○	○	○	○	○	○	○	○	○
		F	●	○	○	○	○	○	○	○	○	○

Figure 2-19 DCPMM and DDR4 memory configuration guidelines (4 processors)

CPU	Channel	DIMM Slot	Configurations in Different Modes (●: DDR4 DIMM ○: DCPMM)							
			2-2-2		2-2-1		2-1-1		1-1-1	
			AD	MM	AD	MM	AD	MM	AD	MM
CPU1	IMC0	A	●	●	●	●	●	●	●	●
			○	○	○	○	○	○	○	○
		B	●	●	●	●	●	●	●	●
			○	○	○	○	○	○	○	○
		C	●	●	●	●	●	●	●	●
			○	○	○	○	○	○	○	○
	IMC1	D	●	●	●	●	●	●	●	●
			○	○	○	○	○	○	○	○
		E	●	●	●	●	●	●	●	●
			○	○	○	○	○	○	○	○
		F	●	●	●	●	●	●	●	●
			○	○	○	○	○	○	○	○
CPU2	IMC0	A	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		B	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		C	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
	IMC1	D	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		E	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		F	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
CPU3	IMC0	A	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		B	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		C	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
	IMC1	D	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		E	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		F	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
CPU4	IMC0	A	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		B	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		C	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
	IMC1	D	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		E	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	
		F	●	●	●	●	●	●	●	
			○	○	○	○	○	○	○	

Figure 2-20 DCPMM and DDR4 memory configuration guidelines

DCPMM and DDR4 Memory Configuration Guidelines					
Capacity per DCPMM	Single iMC Installation Method	Matchable Capacity per DDR4 Memory			
		16 GB	32 GB	64 GB	128 GB
128 GB	2-2-2	✓	✓	✓	
	2-2-1	✓	✓		
	2-1-1	✓			
	1-1-1	✓	✓		
256 GB	2-2-2	✓	✓	✓	✓
	2-2-1	✓	✓	✓	
	2-1-1	✓	✓		
	1-1-1	✓	✓	✓	
512 GB	2-2-2		✓	✓	✓
	2-2-1		✓	✓	✓
	2-1-1	✓	✓	✓	
	1-1-1	✓	✓	✓	✓

2.4 Storage

2.4.1 Drive Configurations

Table 2-7 Drive Configuration

Configuration	Maximum Front Hard Disks	Drive Management Mode
8 x 2.5" Drive Configuration (8 x SAS/SATA)	<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. 	1 x RAID controller card PCIe RAID controller card: must be installed in slot 4.
24 x 2.5" drive configuration (24 x SAS/SATA)	<ul style="list-style-type: none"> Front drives: 24 x 2.5" <ul style="list-style-type: none"> Slots 0 to 23 support only SAS/SATA drives. 	3 x RAID controller cards PCIe RAID controller card: must be installed in slots 4, 6, and 8.
24 x 2.5" (16 x SAS/SATA + 8 x NVMe) drive configuration	<ul style="list-style-type: none"> Front drives: 24 x 2.5" <ul style="list-style-type: none"> Slots 0 to 3 and slots 20 to 23 support only NVMe drives. Slots 4 to 19 support only SAS/SATA drives. 	1 x PCIe RAID controller card + 2 x NVMe adapters <ul style="list-style-type: none"> PCIe RAID controller card: must be installed in slot 4. NVMe adapter: must be installed in slots 5 and 10.

Configuration	Maximum Front Hard Disks	Drive Management Mode
24 x 2.5" drive configuration (24 x NVMe)	<ul style="list-style-type: none"> Front drives: 24 x 2.5" <ul style="list-style-type: none"> Slots 0 to 23 support NVMe drives. 	CPU (directly connected through the NVMe adapter)
25 x 2.5" Drive Configuration (25 x SAS/SATA)	<ul style="list-style-type: none"> Front drives: 25 x 2.5" <ul style="list-style-type: none"> Slots 0 to 24 support only SAS/SATA drives. 	1 x PCIe RAID controller card PCIe RAID controller card: must be installed in slot 4.
<ul style="list-style-type: none"> Contact your local sales representative or use the Compatibility Checker to determine the components to be used. 		

2.4.2 Drive Numbering

- 8 x 2.5" drive configuration (8 x SAS/SATA)

Figure 2-21 Drive numbering



- 24 x 2.5" (24 x SAS/SATA or NVMe or 16 x SAS/SATA + 8 x NVMe) drive configuration

Figure 2-22 Drive numbering



- 25 x 2.5" drive configuration (25 x SAS/SATA)

Figure 2-23 Drive numbering



2.4.3 Drive Indicators

SAS/SATA Drive Indicators

Figure 2-24 SAS/SATA drive indicators

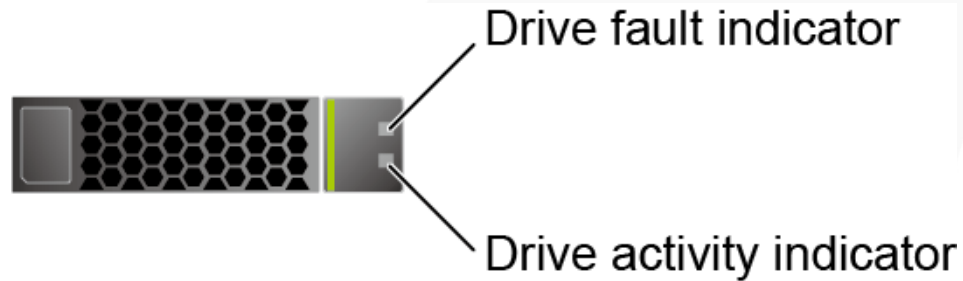


Table 2-8 Description of SAS/SATA drive indicators

Activity Indicator (Green)	Fault Indicator (Yellow)	Description
Steady on	Off	The drive is detected.
Blinking at 4 Hz	Off	Data is being read or written normally, 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 member drive in the RAID array is removed.
Steady on	Steady on	The drive is faulty.

NVMe Drive Indicators

Figure 2-25 NVMe drive indicators

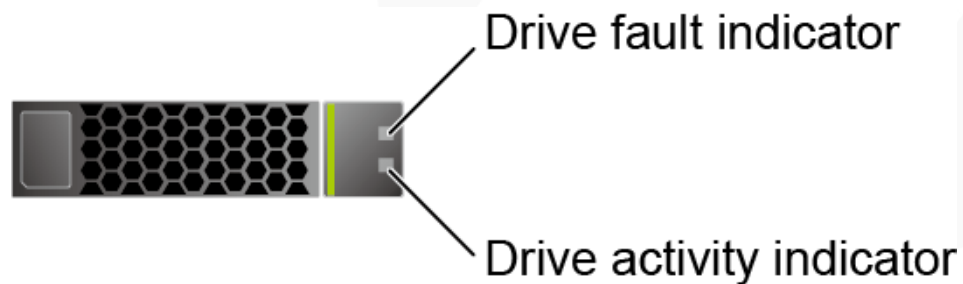


Table 2-9 Description of NVMe drive indicators (only orderly hot swap supported)

Activity Indicator (Green)	Fault Indicator (Yellow)	Description
Off	Off	The NVMe drive cannot be detected.
Steady on	Off	The NVMe drive is working 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 hot removal process is complete, and the NVMe drive is removable.
Steady on/Off	Steady on	The NVMe drive is faulty.

2.4.4 RAID Controller Card

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

- Contact your local sales representative or use the [Compatibility Checker](#) to determine the components to be used.
- For details about the RAID controller card, see [FusionServer V5 Server RAID Controller Card User Guide](#).

2.5 Network

2.5.1 LOMs

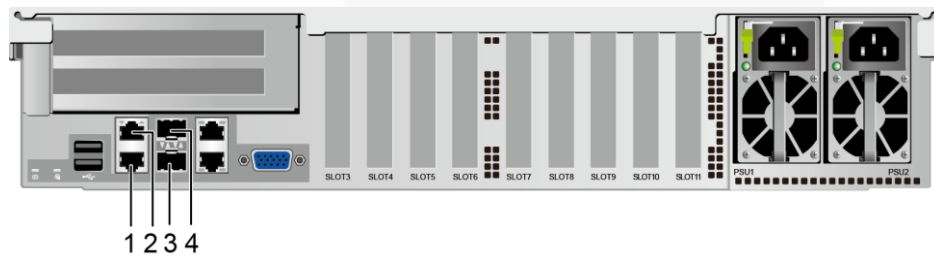
LOMs provide network expansion capabilities.

Table 2-10 LOM description

NIC Type	Chip Model	Port Type	Number of Ports	Rate Negotiation Mode	Supported Rates	Rates Not Supported
LOMs	X722	10GE optical port	2	Auto-negotiation 10,000 Mbit/s (full duplex)	10000M	10/100/1000M
		GE electrical port	2	Auto-negotiation 1000 Mbit/s (full duplex)	1000M	10/100M

NIC Type	Chip Model	Port Type	Number of Ports	Rate Negotiation Mode	Supported Rates	Rates Not Supported
<ul style="list-style-type: none"> • Use Compatibility Checker to obtain information about the cables and optical modules supported by the LOM ports. • The LOM ports support NC-SI and PXE. • The LOM ports do not support forced rates. • The electrical LOM ports cannot be connected to power over Ethernet (PoE) devices (such as a switch with PoE enabled). Connecting a LOM port to a PoE device may cause link communication failure or even damage the NIC. • The electrical LOM ports (GE electrical ports) do not support SR-IOV. • Forcibly powering off a server will cause intermittent NC-SI disconnection and disable the WOL function of the LOM ports. To restore the NC-SI connection, refresh the iBMC WebUI. 						

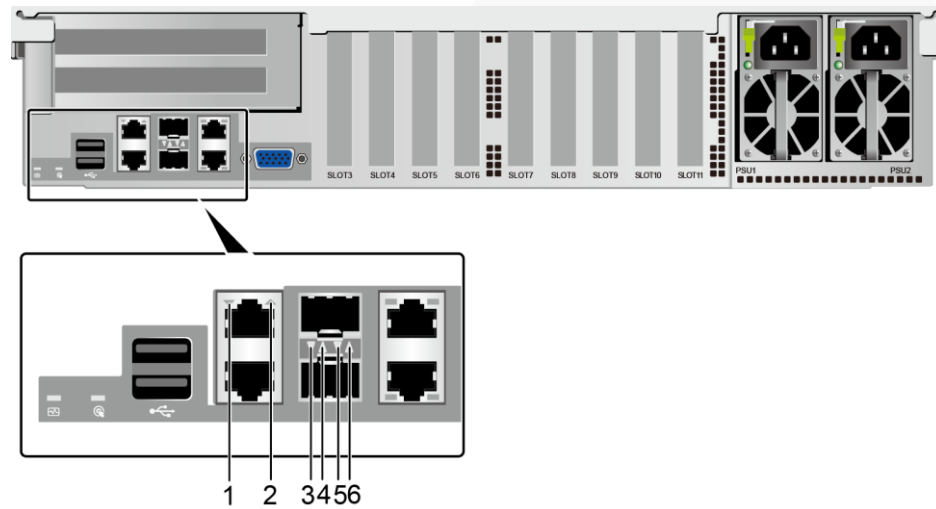
Figure 2-26 LOM port



1	GE electrical port (LOM port 2)	2	GE electrical port (LOM port 1)
3	10GE optical port (LOM port 4)	4	10GE optical port (LOM port 3)

Indicator Positions

Figure 2-27 LOM indicators



1	Connection status indicator/Data transmission status indicator for GE electrical port 1	2	Connection status indicator/Data transmission status indicator for GE electrical port 2
3	Connection status indicator/Data transmission status indicator for 10GE optical port 4	4	Connection status indicator/Data transmission status indicator for 10GE optical port 3
5	Data transmission rate indicator for 10GE optical port 4	6	Data transmission rate indicator for 10GE optical port 3

Indicator Description

Table 2-11 LOM indicators

Indicator	Description
Connection status indicator/Data transmission status indicator for a 10GE optical port	<ul style="list-style-type: none"> Off: The network port is not connected. Blinking green: Data is being transmitted. Steady green: The network port is properly connected.
Data transmission rate indicator for a 10GE optical port	<ul style="list-style-type: none"> Off: The network port is not connected. Steady green: The data transmission rate is 10 Gbit/s.
Connection status	<ul style="list-style-type: none"> Off: The network port is not connected.

Indicator	Description
indicator/Data transmission status indicator for a GE electrical port	<ul style="list-style-type: none"> Blinking green: Data is being transmitted. Steady green: The network port is properly connected.

2.6 I/O Expansion

2.6.1 PCIe Cards

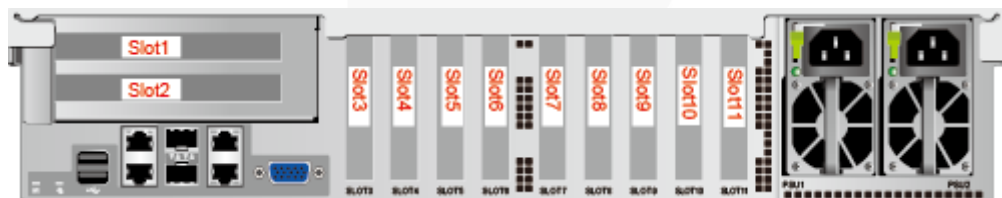
PCIe cards provide ease of expandability and connection.

- The electrical ports provided by PCIe NICs cannot be connected to power over Ethernet (PoE) devices (such as a switch with PoE enabled). Connecting such an electrical port to a PoE device may cause link communication failure or even damage the NIC.
- Contact your local sales representative or use 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.

2.6.2 PCIe Slots

PCIe Slots

Figure 2-28 PCIe slots



- Slots 1 and 2 are provided by the PCIe riser module.
- Slots 3 to 11 are provided by the mainboard.

2.6.3 PCIe Slot Description

NOTE

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

Table 2-12 PCIe slot description

PCIe Slot	CPU	PCIe Standards	Connector Width	Bus Width	Port No.	Bus/Device/Function Number (B/D/F)	Slot Size
LOM	CPU 1	PCIe 3.0	-	x4	Port2D	0x24/0x03/0x00	-
Slot 1	CPU 1	PCIe 3.0	x16	x16	Port3A	0x32/0x00/0x00	Full-height, 3/4-length
Slot 2	CPU 4	PCIe 3.0	x8	x8	Port2A	0xE2/0x00/0x00	FHHL
Slot 3	CPU 1	PCIe 3.0	x8	x4	Port2C	0x24/0x02/0x00	HHHL
Slot 4	CPU 1	PCIe 3.0	x8	x8	Port2A	0x24/0x00/0x00	HHHL
Slot 5	CPU 1	PCIe 3.0	x16	x16	Port1A	0x08/0x00/0x00	HHHL
Slot 6	CPU 2	PCIe 3.0	x8	x8	Port2C	0x62/0x02/0x00	HHHL
Slot 7	CPU 2	PCIe 3.0	x8	x8	Port2A	0x62/0x00/0x00	HHHL
Slot 8	CPU 2	PCIe 3.0	x8	x8	Port1A	0x43/0x00/0x00	HHHL
Slot 9	CPU 3	PCIe 3.0	x8	x8	Port2A	0xA2/0x00/0x00	HHHL
Slot 10	CPU 2	PCIe 3.0	x16	x16	Port3A	0x71/0x00/0x00	HHHL
Slot 11	CPU 2	PCIe 3.0	x8	x8	Port1C	0x43/0x02/0x00	HHHL

- The B/D/F (Bus/Device/Function Number) values are the default values when the server is fully configured with PCIe devices. The values may vary if the server is not fully configured with PCIe devices or if a PCIe card with a PCI bridge is configured.
- The PCIe x16 slots are backward compatible with 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.
- Full-height 3/4-length PCIe slots are backward compatible with full-height half-length and half-height half-length PCIe cards. Full-height half-length PCIe slots are backward compatible with half-height half-length PCIe cards.
- All slots support PCIe cards of up to 75 W. The power of a PCIe card varies depending

PCIe Slot	CPU	PCIe Standards	Connector Width	Bus Width	Port No.	Bus/Device/Function Number (B/D/F)	Slot Size
on its model.							

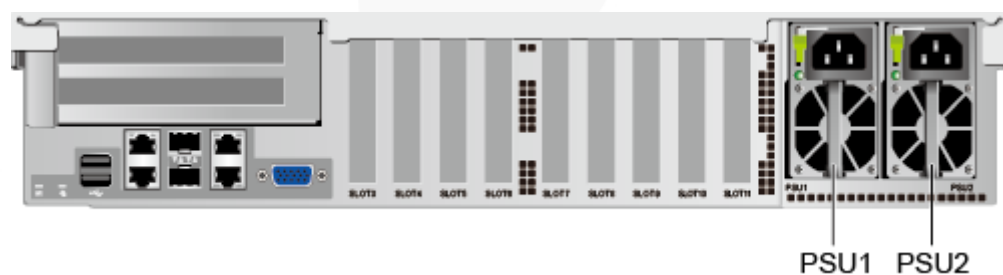
2.7 PSUs

- 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.
- The same model of PSUs 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.
- Contact your local sales representative or use the [Compatibility Checker](#) to determine the components to be used.

NOTE

- When one or two 1500 W AC Platinum PSUs are configured:
 - When the input voltage ranges from 100 V AC to 127 V AC, the output power decreases to 1000 W.
 - Two 1500 W AC Platinum PSUs can serve as 1700 W PSUs.
- When one or two 2000 W AC Platinum PSUs are configured and the input voltage ranges from 200 V AC to 220 V AC, the output power decreases to 1800 W.

Figure 2-29 PSU positions

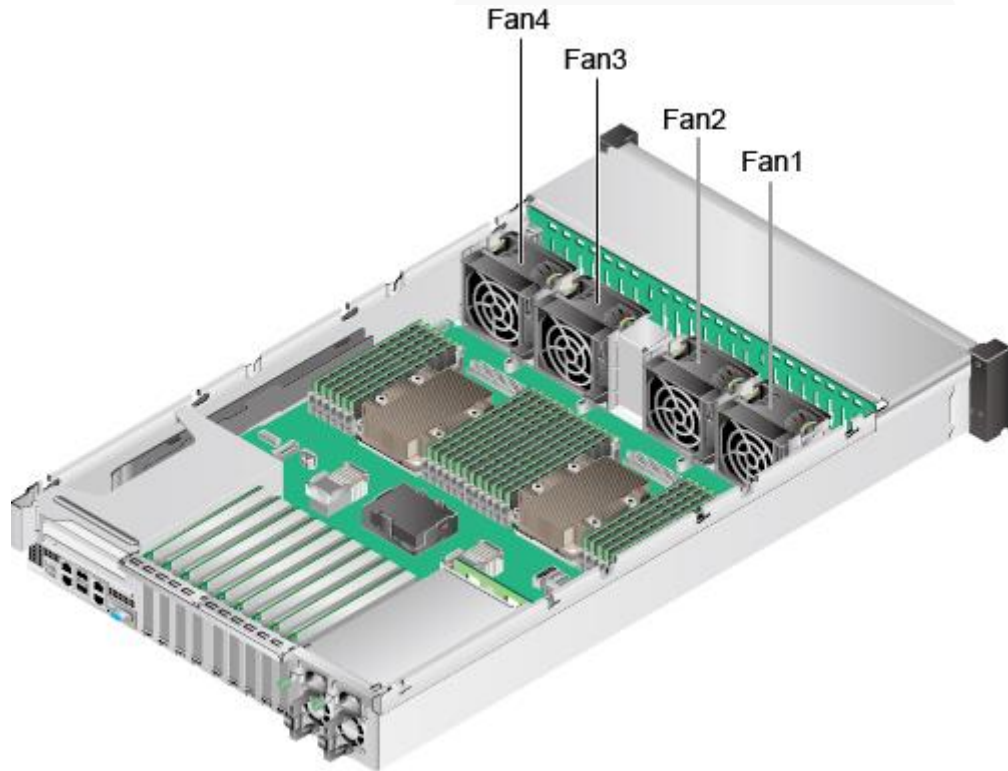


2.8 Fans

- The server supports four fan modules.
- The fan modules are hot-swappable.
- The server tolerates failure of a single fan.

- The fan speed can be adjusted.
- The same model of fan modules must be used in a server.

Figure 2-30 Fan module positions



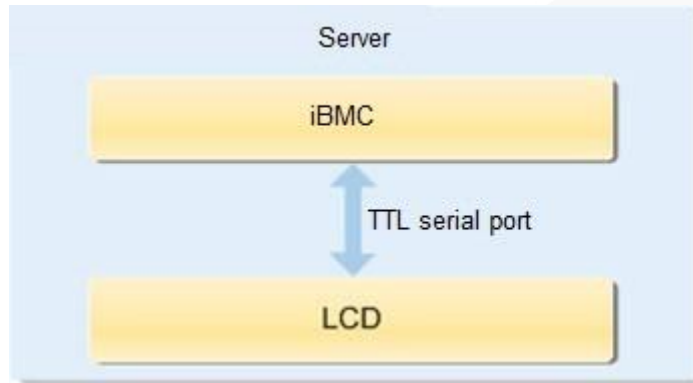
2.9 LCD

Function

The LCD displays the installation status and running status of server components and enables users to set the IP address of the iBMC management network port on the server.

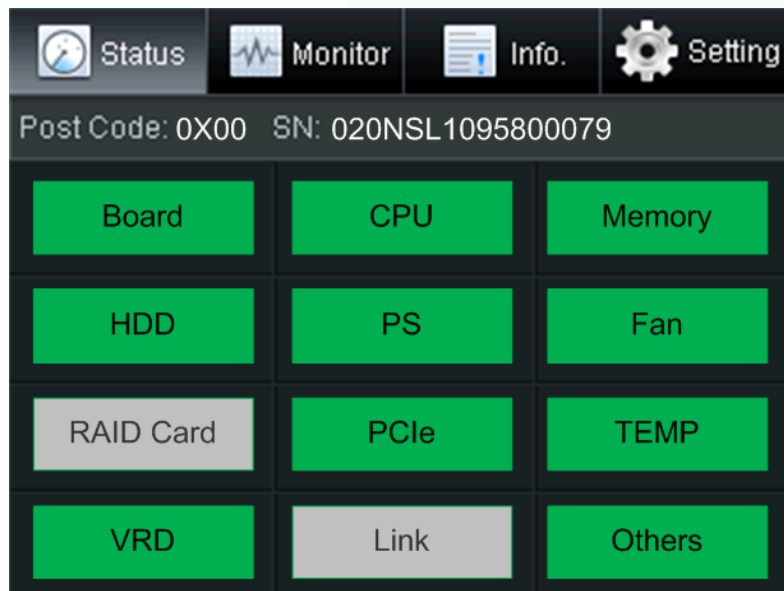
The LCD and the server iBMC form an LCD subsystem. The LCD directly obtains device information from the iBMC. The LCD subsystem does not store device data.

Figure 2-31 LCD subsystem working principle



UI

Figure 2-32 LCD screen



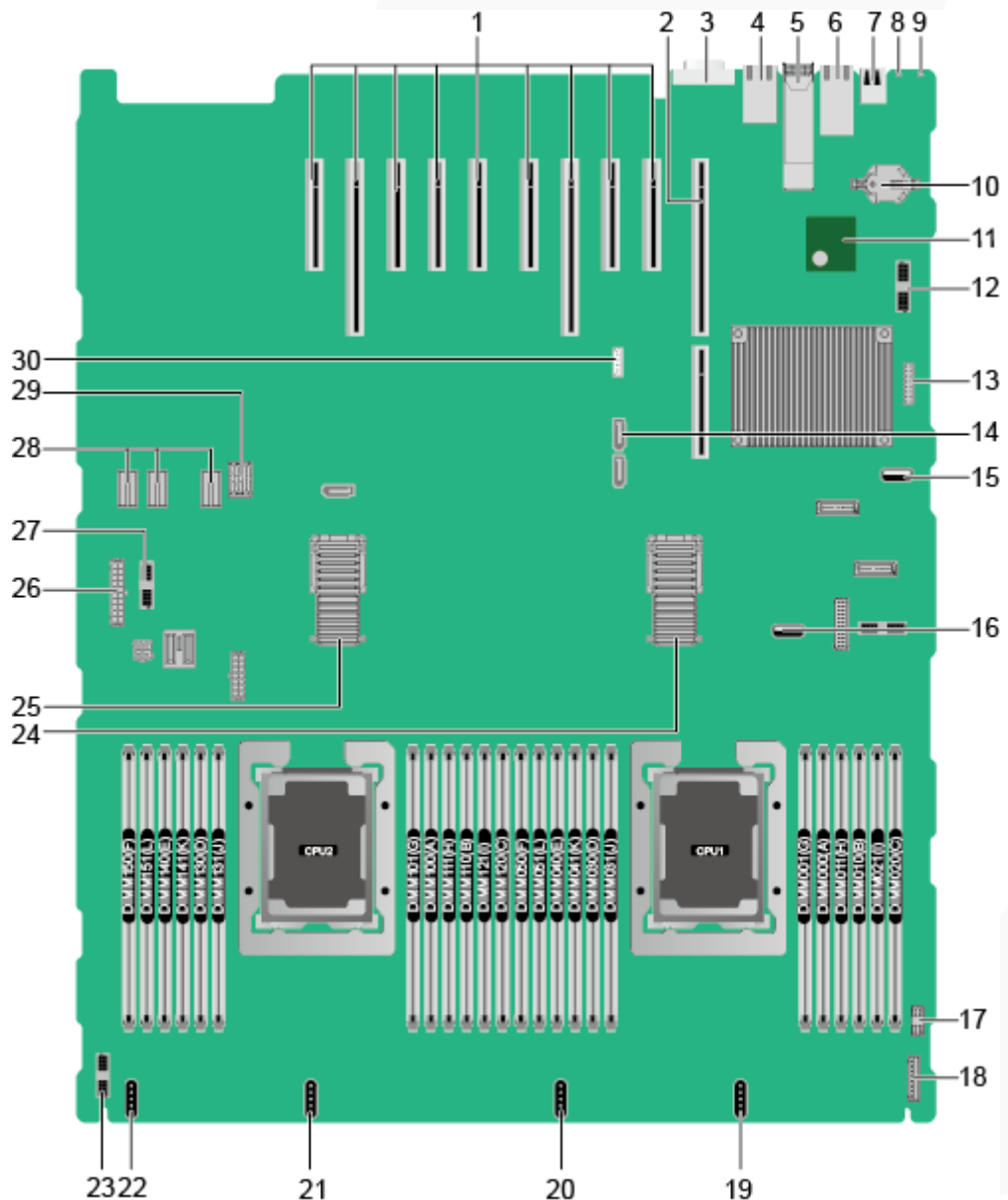
Tab	Function
Status	Displays the port 80 status, serial number, component status, and component alarms of the server.
Monitor	Displays the current power, CPU temperature, and inlet temperature of the server.
Info.	Displays the IP address and MAC address of the iBMC management network port, MAC addresses of host LOM ports, device SNs, asset information, and firmware version.
Setting	Sets the IP address of the iBMC management network port.

For details about how to use the LCD, see [FusionServer 2488H V5 Server LCD User Guide](#).

2.10 Boards

2.10.1 Mainboard

Figure 2-33 2488H V5 mainboard



1	PCIe card slots (3 to 11 from right to left)	2	PCIe riser slots (J207 for CPU 1 and J230 for CPU 4)
---	--	---	--

3	VGA connector (VGA CONN/J169)	4	System serial port and management network port (J242) ^a
5	10GE optical port (10GE PORT0&PORT1/J140)	6	GE electrical port (GE PORT2&PORT3/J138)
7	USB 3.0 port (REAR USB 3.0/J172)	8	UID Indicator
9	Health status indicator	10	System battery (U4042)
11	TPM/TCM port (TPM CONN/J55)	12	Right mounting ear connector (J131)
13	Jumper (J93) ^b	14	SATA DVD drive connector (J130)
15	USB 3.0 port (FRONT USB3.0/J190) ^c	16	USB 3.0 port (INNER USB3.0/J182)
17	VGA connector (J233)	18	LCD connector (LCD CONN/J87)
19	Fan port 4 (FAN4/J102)	20	Fan port 3 (FAN3/J103)
21	Fan port 2 (FAN2/J104)	22	Fan port 1 (FAN1/J105)
23	Signal connector for the drive backplane (HDD BP/J235)	24	High-speed backplane connector (J244) ^d
25	High-speed backplane connector (J243) ^d	26	Drive backplane power connector (BP PWR/J237)
27	Left mounting ear connector (LEFT EAR CONN BOARD/J115)	28	PSU backplane power connector (J225/J226/J239)
29	PSU backplane signal connector (J238)	30	VROC key port (J144) ^e
<ul style="list-style-type: none"> • a: The upper one is an RJ45 serial port, and the lower one is an RJ45 management port. • b: BMC_SER_MANUAL PIN is used to change the connection direction of the physical serial port. CLEAR_BMC_PW PIN is used to restore the default iBMC configuration (for iBMC V350 and later versions, restoring the default iBMC configuration through a jumper is not supported). • c: The built-in USB 3.0 port can be connected to the front USB 3.0 port through a USB cable. It cannot be used directly. • d: CPUs 1 and 2 are on the mainboard, and CPUs 3 and 4 are on the daughter board. The mainboard and daughter board are interconnected through high-speed backplane connectors. • e: The port is reserved. 			

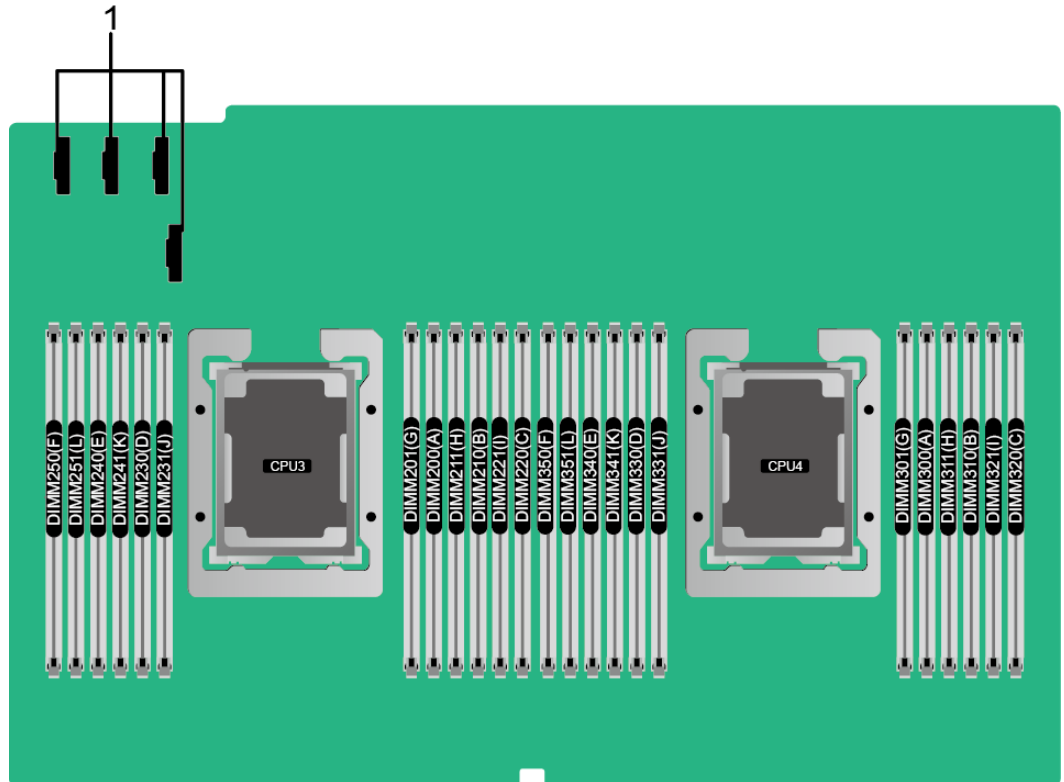
2.10.2 Daughter Board

Figure 2-34 shows the daughter board of the 2488H V5. Figure 2-35 shows the connection between the daughter board and the mainboard.

NOTE

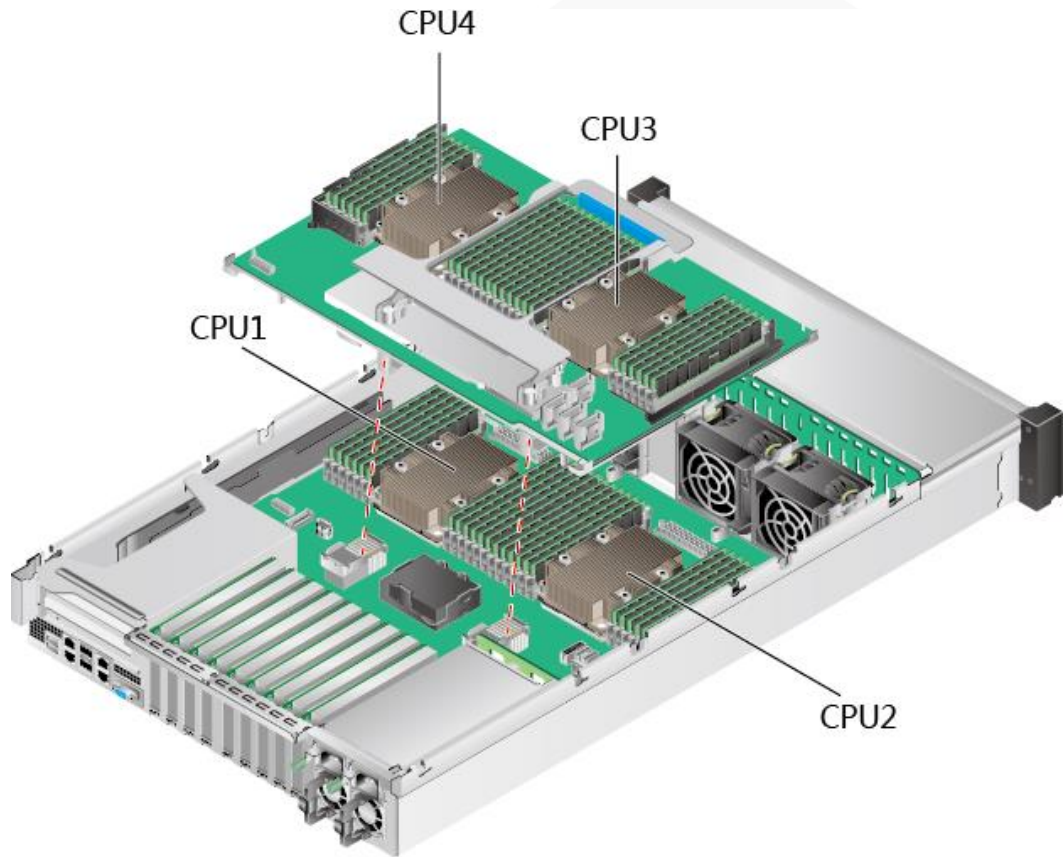
CPU 1 and 2 are on the mainboard, and CPUs 3 and 4 are on the daughter board. The mainboard and daughter board are interconnected through high-speed backplane connectors.

Figure 2-34 Daughter board



1	Slimline connector (reserved)	-	-
---	-------------------------------	---	---

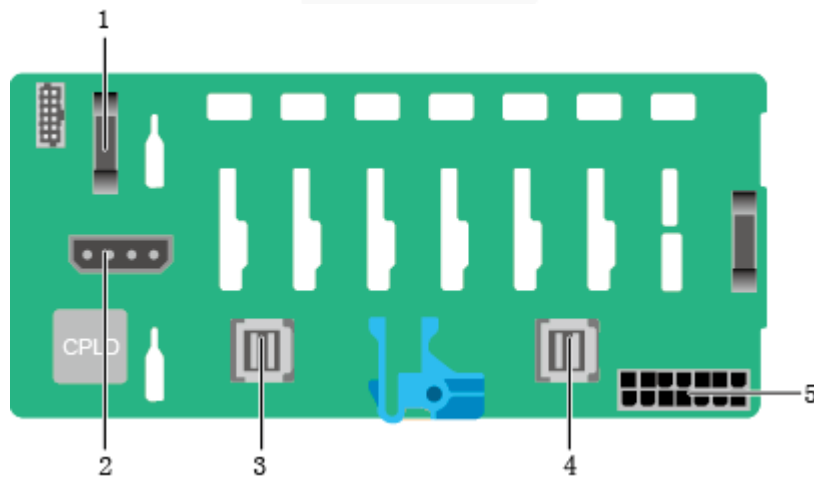
Figure 2-35 Connection between the daughter board and the mainboard



2.10.3 Drive Backplane

- 8 x 2.5" drive backplane (8 x SAS/SATA)

Figure 2-36 8 x 2.5" drive backplane (8 x SAS/SATA)

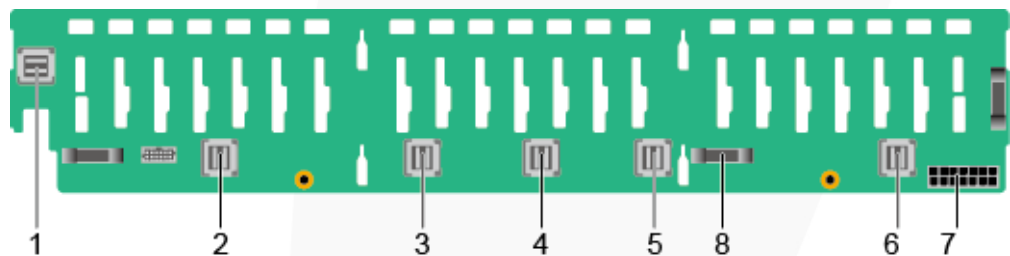


1	Signal cable connector (J1)	2	DVD drive power connector
---	-----------------------------	---	---------------------------

			(J11)
3	SAS cable connector (PORT B/J29)	4	SAS cable connector (PORT A/J28)
5	Backplane power connector (J24)	-	-

- 24 x 2.5" drive backplane (24 x SAS/SATA)

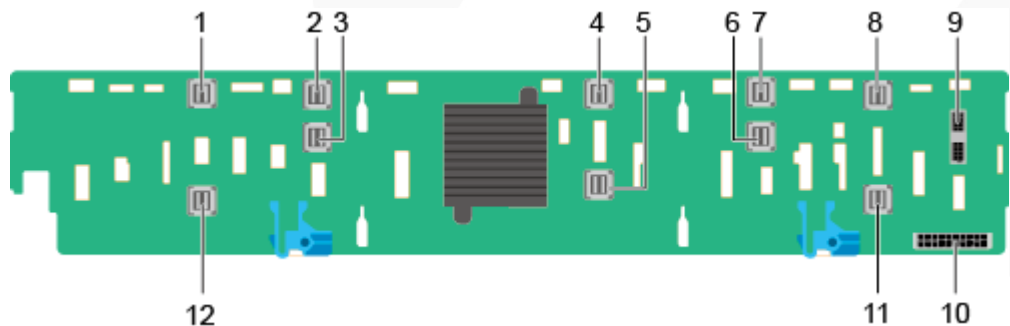
Figure 2-37 24 x 2.5" drive backplane (24 x SAS/SATA) (BOM: 03022JWW)



1	SAS cable connector (PORT 3B/J33)	2	SAS cable connector (PORT 3A/J39)
3	SAS cable connector (PORT 2B/J31)	4	SAS cable connector (PORT 2A/J30)
5	SAS cable connector (PORT 1B/J29)	6	SAS cable connector (PORT 1A/J28)
7	Backplane power connector (J24)	8	Backplane signal cable connector (J1)

- 24 x 2.5" drive backplane (16 x SAS/SATA + 8 x NVMe)

Figure 2-38 24 x 2.5" drive backplane (16 x SAS/SATA + 8 x NVMe)

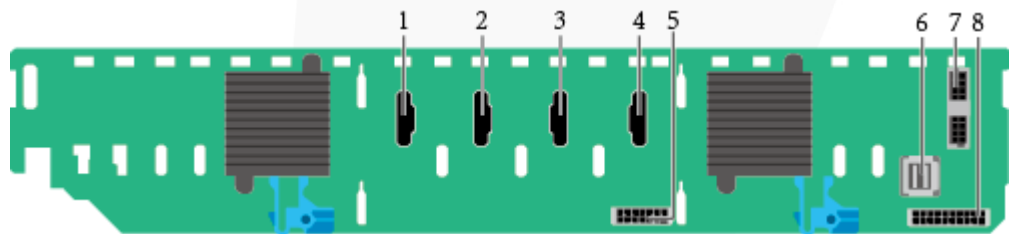


1	NVMe (PORT B_N2/J26)	2	NVMe (PORT B_N0/J24)
---	----------------------	---	----------------------

3	NVMe (PORT B_N1/J25)	4	SAS cable connector (PORT C_0/J28)
5	SAS cable connector (PORT C_1/J29)	6	NVMe (PORT A_N1/J21)
7	NVMe (PORT A_N0/J20)	8	NVMe (PORT A_N2/J22)
9	Backplane signal cable connector (J1)	10	Backplane power connector (J3)
11	NVMe (PORT A_N3/J23)	12	NVMe (PORT B_N3/J27)

- 24 x 2.5" drive backplane (24 x NVMe)

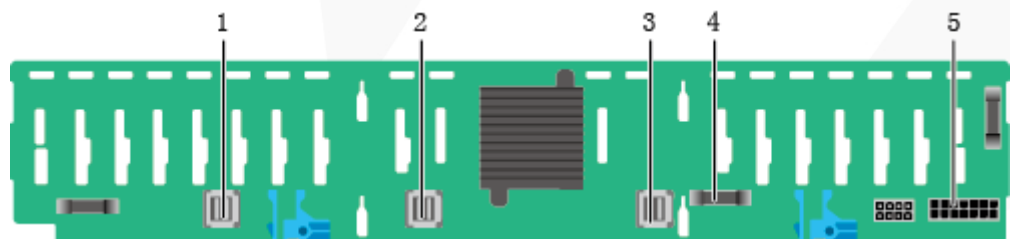
Figure 2-39 24 x 2.5" drive backplane (24 x NVMe)



1	Slimline A connector (J6)	2	Slimline B connector (J5)
3	Slimline C connector (J7)	4	Slimline D connector (J8)
5	Power connector 2 (J34)	6	mini-SAS HD connector (PORT A/J52)
7	Backplane signal cable connector (J3)	8	Power connector 1 (J2)

- 25 x 2.5" drive backplane (25 x SAS/SATA)

Figure 2-40 25 x 2.5" drive backplane (25 x SAS/SATA)



1	SAS cable connector (PORT A/J28)	2	SAS cable connector (PORT B/J29)
---	----------------------------------	---	----------------------------------

3	SAS cable connector (REAR PORT/J31)	4	Backplane signal cable connector (J1)
5	Backplane power connector (J24)	-	-

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	2U rack server
Chipset	Intel® C622
Processor	<p>Supports two or four processors.</p> <ul style="list-style-type: none"> • Intel® Xeon® Scalable (Skylake and Cascade Lake) processors • Built-in memory controller and six memory channels • Built-in PCIe controller, supporting PCIe 3.0 and 48 lanes per processor • Three UPI buses between processors, providing up to 10.4GT/s transmission per channel • Up to 28 cores per processor • Max. 3.8 GHz • Min. 1.375 MB L3 cache per core • Max. 205 W TDP <p>NOTE The preceding information is for reference only. Use the Compatibility Checker to obtain specific information.</p>
DIMM	<p>Supports 48 memory modules of the following types:</p> <ul style="list-style-type: none"> • Up to 48 DDR4 memory modules <ul style="list-style-type: none"> – Max. 2933 MT/s memory speed

Component	Specifications
	<ul style="list-style-type: none"> - RDIMM and LRDIMM support - The DDR4 memory modules of different types (RDIMM and LRDIMM) and specifications (capacity, bit width, rank, and height) cannot be used together. • Up to 24 DCPMMs <ul style="list-style-type: none"> - The DCPMMs must be used with DDR4 memory modules together. - The DCPMMs support the AD or MM mode. - Max. 2666 MT/s memory speed - The DCPMMs of different specifications cannot be used together. - For details about the DCPMMs, see the <i>FusionServer DCPMM User Guide</i>. <p>NOTE The preceding information is for reference only. Use the Compatibility Checker to obtain specific information.</p>
Storage	<p>Supports a variety of drive configurations. For details, see 2.4.1 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 only when the server is configured with an Avago SAS3004iMR RAID controller card. - The drive letter of the M.2 SSDs managed by the Avago SAS3004iMR RAID controller card can be set to sda by modifying the GRUB parameters only when the RAID controller card is used with a SmartRAID 3152-8i or SmartHBA 2100-8i RAID controller card. <p>NOTE</p> <ul style="list-style-type: none"> • The M.2 SSD module is used only as the boot device when the OS is installed. 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. Use enterprise-level high endurance (HE) SSDs or HDDs for data storage. • The M.2 SSD is not recommended for write-intensive service software due to poor endurance. • Do not use the M.2 SSD as the cache. <ul style="list-style-type: none"> • Supports hot swap of SAS/SATA drives. • Supports a variety of RAID controller cards. Use the

Component	Specifications
	<p>Compatibility Checker to obtain information about the specific RAID controller cards supported.</p> <ul style="list-style-type: none"> - The RAID controller card supports RAID configuration, RAID level migration, and drive roaming. - The PCIe RAID controller card occupies one standard PCIe slot. <p>For details about the RAID controller card, see FusionServer V5 Server RAID Controller Card User Guide.</p> <ul style="list-style-type: none"> • Supports a SAS RAID controller card (with a 1 GB, 2 GB, or 4 GB cache) and a supercapacitor (providing power-off protection) to improve storage performance and data security.
Network	<p>Supports LOM.</p> <ul style="list-style-type: none"> • Supports two 10GE optical ports and two GE electrical ports via the NIC chip integrated on the mainboard. • The LOM ports support NC-SI and PXE. <p>NOTE The electrical ports provided by LOMs and PCIe NICs cannot be connected to PoE devices (such as a switch with PoE enabled). Connecting such an electrical port to a PoE device may cause link communication failure or even damage the NIC.</p>
I/O expansion	<p>11 PCIe 3.0 slots:</p> <ul style="list-style-type: none"> • Two slots for riser cards and nine onboard slots. <p>For details, see 2.6.2 PCIe Slots and 2.6.3 PCIe Slot Description.</p> <ul style="list-style-type: none"> • Support PCIe SSD cards to bolster I/O performance for applications such as searching, caching, and download services. • 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. <p>NOTE The preceding information is for reference only. Use the Compatibility Checker to obtain specific information.</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"> - Two USB 2.0 ports - One USB 3.0 port - One DB15 VGA port <p>NOTE For the server that uses 25 x 2.5" drive configuration, the front panel provides only two USB 2.0 ports.</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

Component	Specifications
	<ul style="list-style-type: none"> - One RJ45 serial port - One RJ45 system management port - Two GE electrical ports - Two 10GE optical ports • Built-in ports: <ul style="list-style-type: none"> - Two USB 3.0 ports <p>NOTE In the 8 x 2.5" or 24 x 2.5" drive configuration, only one USB3.0 built-in port is provided.</p> <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"> • SM750 is not supported by servers running the Windows Server 2019 or Windows Server 2019 Hyper-V operating systems that are in secure boot mode. • 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 the chassis provides the front and rear VGA ports but only one VGA port is connected to a monitor, the display effect may be affected.
System management	<ul style="list-style-type: none"> • Supports UEFI. • Supports iBMC. • Supports NC-SI. • Supports 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)

3.2 Environmental Specifications

Table 3-2 Environmental specifications

Category	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 hour, 5°C (9°F) per 15 minutes <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 change rate: 20%/h
Air volume	≥ 196 cubic feet per minute (CFM)
Operating altitude	<p>≤3050m</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 (984.25 ft). When the configuration complies with ASHRAE Class A3 standards 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</p>

Category	Specifications
	It is recommended that the particulate pollution in the equipment room be monitored by a professional agency.
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 reported in accordance with ISO 9296 (ECMA 109).</p> <ul style="list-style-type: none"> • Idle: <ul style="list-style-type: none"> - LWAd: 5.3 Bels - LpAm: 38.1 dBA • Operating: <ul style="list-style-type: none"> - LWAd: 6.3 Bels - LpAm: 48.2 dBA <p>NOTE The noise generated during operation varies depending on the 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)	86.1 mm x 447 mm x 748 mm (3.39 in. x 17.60 in. x 29.45 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 ≥ 900 mm (35.43 in.) • Requirements for guide rail installation:

Category	Description
	<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 543.5 mm to 848.5 mm (21.40 in. to 33.41 in.) between the front and rear mounting bars. - Ball bearing rail kit: applies to cabinets with a distance of 610 mm to 914 mm (24.02 in. to 35.98 in.) between 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"> - Chassis with 8 x 2.5" drives: 28 kg (61.74 lb) - Chassis with 24 x 2.5" drives: 30 kg (66.15 lb) - Chassis with 25 x 2.5" drives: 31 kg (68.36 lb) • Packaging materials: 5 kg (11.03 lb)
Power consumption	<p>The power consumption parameters vary with server configurations, including the configurations complying with energy-related products (ErP) requirements. Use the Power Calculator to obtain specific information.</p>

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 sales personnel 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

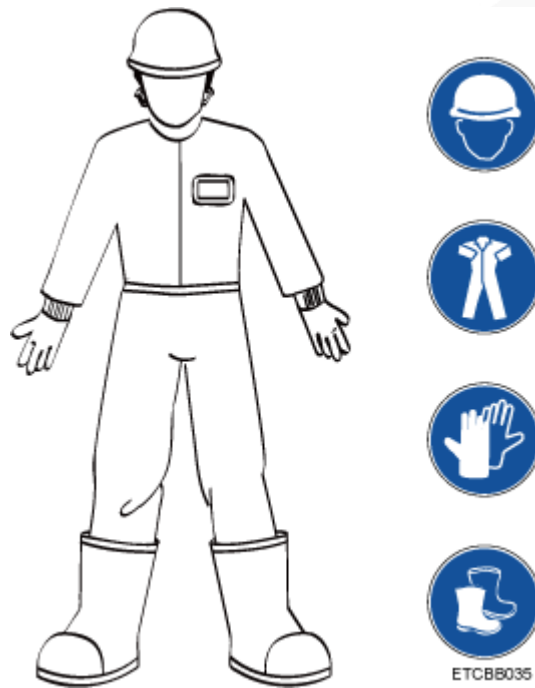
General Statement

- 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 area as it is likely to cause radio interference.

Human Safety

- Only certified or authorized personnel are allowed to install the device.
- 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.

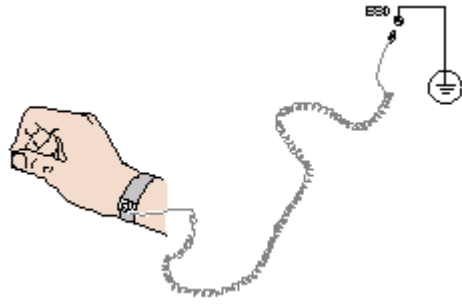
Figure 5-2 Removing conductive objects



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 the device is higher than the shoulders of the installation personnel, use a vehicle such as a lift to facilitate installation. Prevent the equipment from falling down and causing personal injury or damage to the equipment.
- 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.
- When connecting, testing, or replacing an optical cable, do not look into the optical port without eye protection.

Equipment Safety

- 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 that could cause personal injury.
- If the device is configured with active and standby PSUs, connect power cables of active and standby PSUs to different power distribution units (PDUs) to ensure reliable system operating.
- Ground the equipment before powering it on.

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 the equipment 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 GPUs and SSDs) separately.

 **NOTE**

Use [Compatibility Checker](#) to obtain information about the components supported by a node or server.

- Power off all devices before transportation.

Maximum Weight Carried by a Person

 **CAUTION**

To reduce the risk of personal injury, comply with local regulations with regard to the maximum weight one person is permitted to carry.

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 ($\pm 10\%$). For grounding purposes, 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](#)

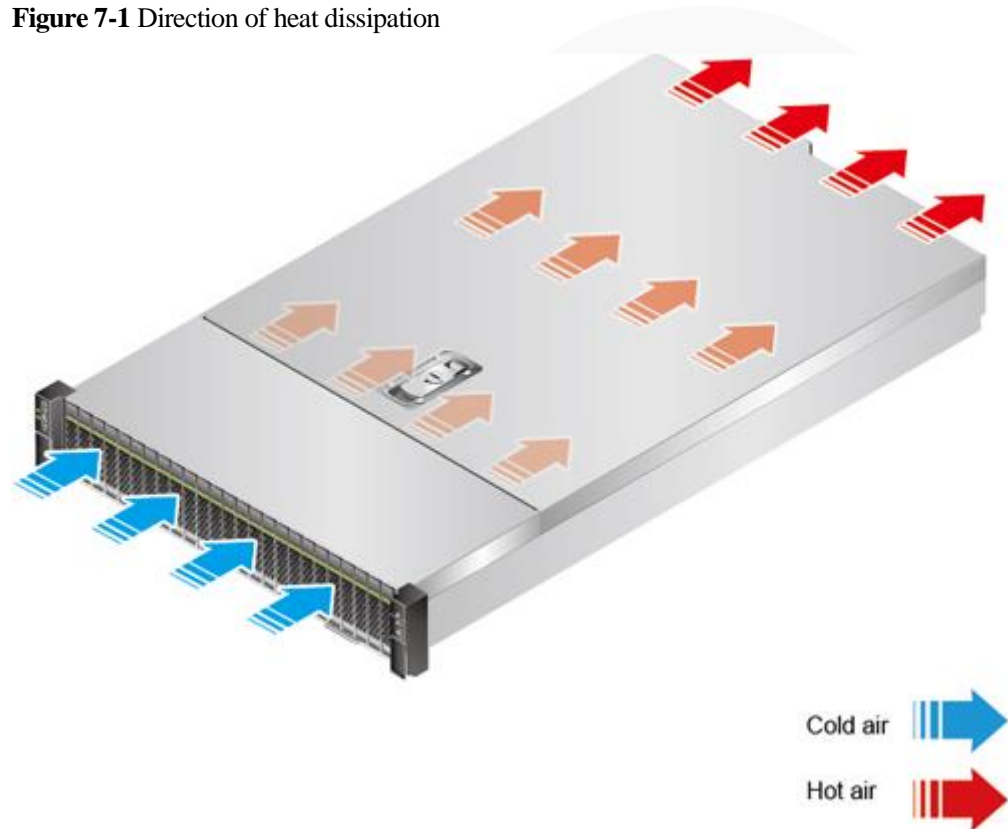
7.1 Installation Environment Requirements

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 maintenance, keep a clearance of 800 mm (31.50 in.) between walls and the front and rear doors of the cabinet.
- Do not block the air intake vents. Otherwise, air intaking and heat dissipation will be affected.
- The air conditioning system in the equipment room provides enough wind to ensure proper heat dissipation of all components.

Figure 7-1 Direction of heat dissipation



7.1.2 Temperature and Humidity Requirements

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

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

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	8% RH to 90% RH (non-condensing)

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.

NOTE

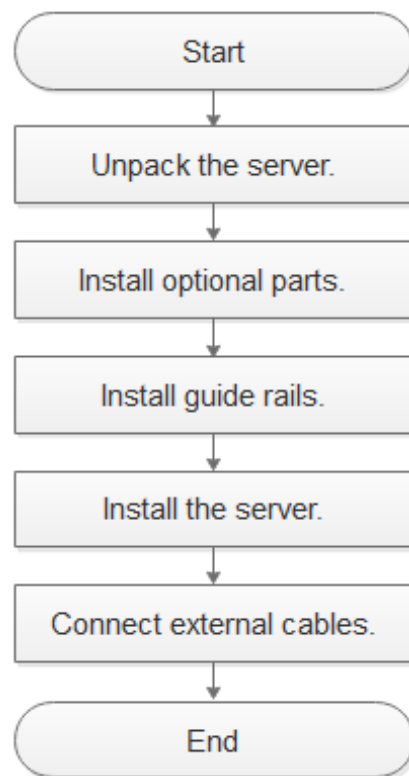
The 2488H V5 is 2 U high and stackable. If space is sufficient, leave a distance of 1 U between two adjacent servers.

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 electrostatic discharge. 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.

Use the [Compatibility Checker](#) to obtain information about the components supported.

 **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 extra CPUs, drives, and PCIe cards.

Procedure

Step 1 Install the optional parts for the 2488H V5.

For details, see [FusionServer 2488H V5 Server Maintenance and Service Guide](#).

----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.

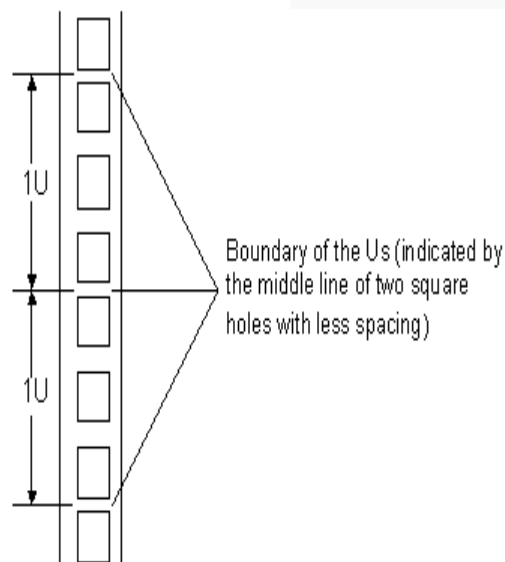
The 2488H V5 servers are stackable onto L-shaped guide rails.

Procedure

Step 1 Install floating nuts.

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

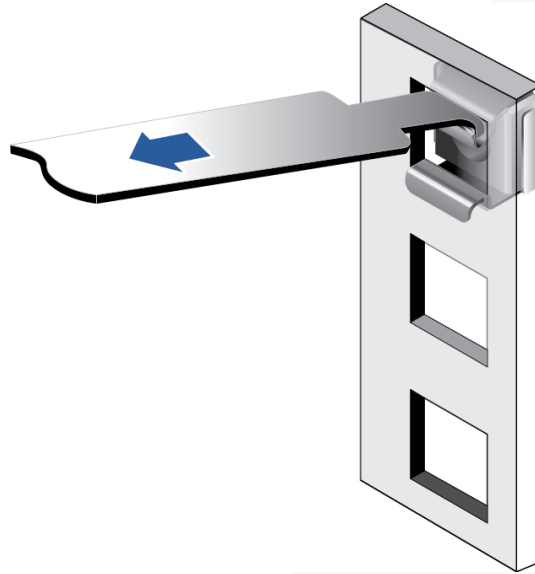
Figure 7-3 Spacing of 1U on a mounting bar of a cabinet



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

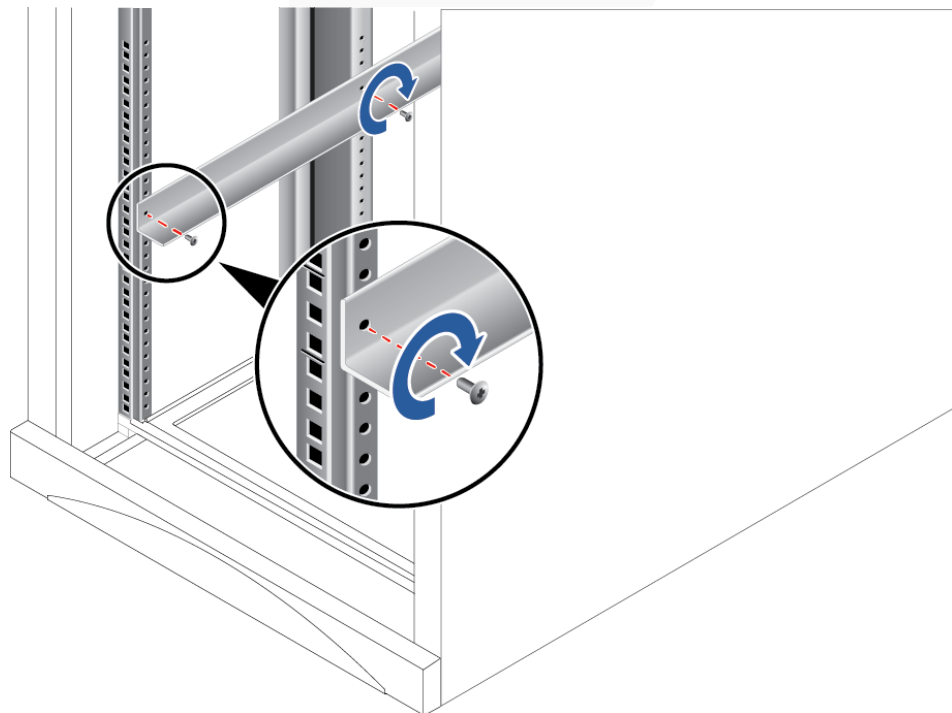


4. Install the other floating nut in the same way.

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 543.5 mm to 848.5 mm (21.40 in. to 33.41 in.) between the front and rear mounting bars.

The 2488H V5 servers are stackable onto the static rail kit.

Procedure

Step 1 Place the rail horizontally in the planned position. Stretch the rail on both sides of the cabinet based on the cabinet length, keeping it in contact with the mounting bar in the cabinet, and hook the rail. See (1) in Figure 7-6.

 **NOTE**

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

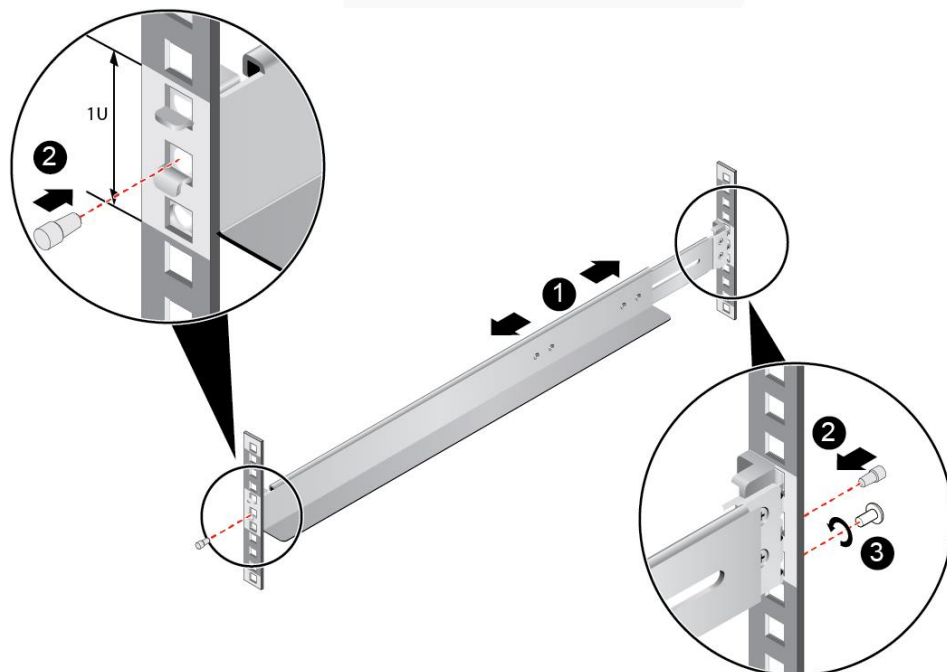
Step 2 Plug the second square holes at the front and rear of the rail. See (2) in Figure 7-6.

Step 3 On the first lower square hole at the rear of the rail, insert an M6 screw. See (3) in Figure 7-6.

 **NOTE**

Although the static rail kit does not need screws for installation, you can perform this operation to improve the shockproof level and fastening degree of the server.

Figure 7-6 Installing a static rail



Step 4 Install the other rail in the same way.

----End

7.2.4.3 Installing the Ball Bearing Rail Kit

7.2.4.3.1 Ball Bearing Rail Kit 1

This section applies to the ball bearing rail kit whose part number is 21241258.

The ball bearing rail kit applies to cabinets with a distance of 610 mm to 914 mm (24.02 in. to 35.98 in.) between the front and rear mounting bars.

The 2488H V5 servers are stackable onto the ball bearing rail kit.

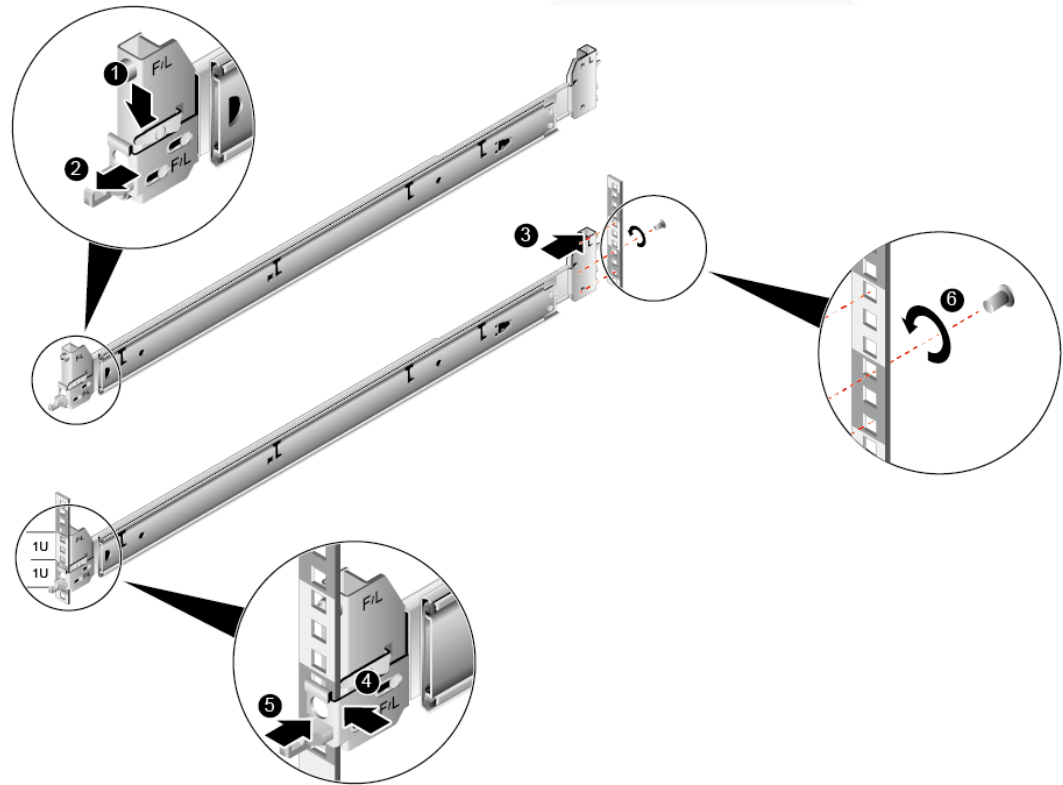
Procedure

- Step 1** Press the release latch at the front of the rail and stretch the hook horizontally as far as it will go. 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** Align the front end of the rail with the hole on the front column of the cabinet, push the rail horizontally, and insert the rail into the hole on the column from the side. See (4) in Figure 7-7.
- Step 4** Push the hook horizontally until the release latch clicks into place. See (5) in Figure 7-7.
- Step 5** On the third square hole at the rear of the rail, insert an M6 screw. See (6) in Figure 7-7.

NOTE

Although the ball bearing rail kit does not need screws for installation, we recommend you use M6 screws at the rear end to make the server more shockproof and secure.

Figure 7-7 Installing the ball bearing rail kit



Step 6 Install the other rail in the same way.

----End

7.2.4.3.2 Ball Bearing Rail Kit 2

This section applies to the ball bearing rail kit whose part number is 21241258-002.

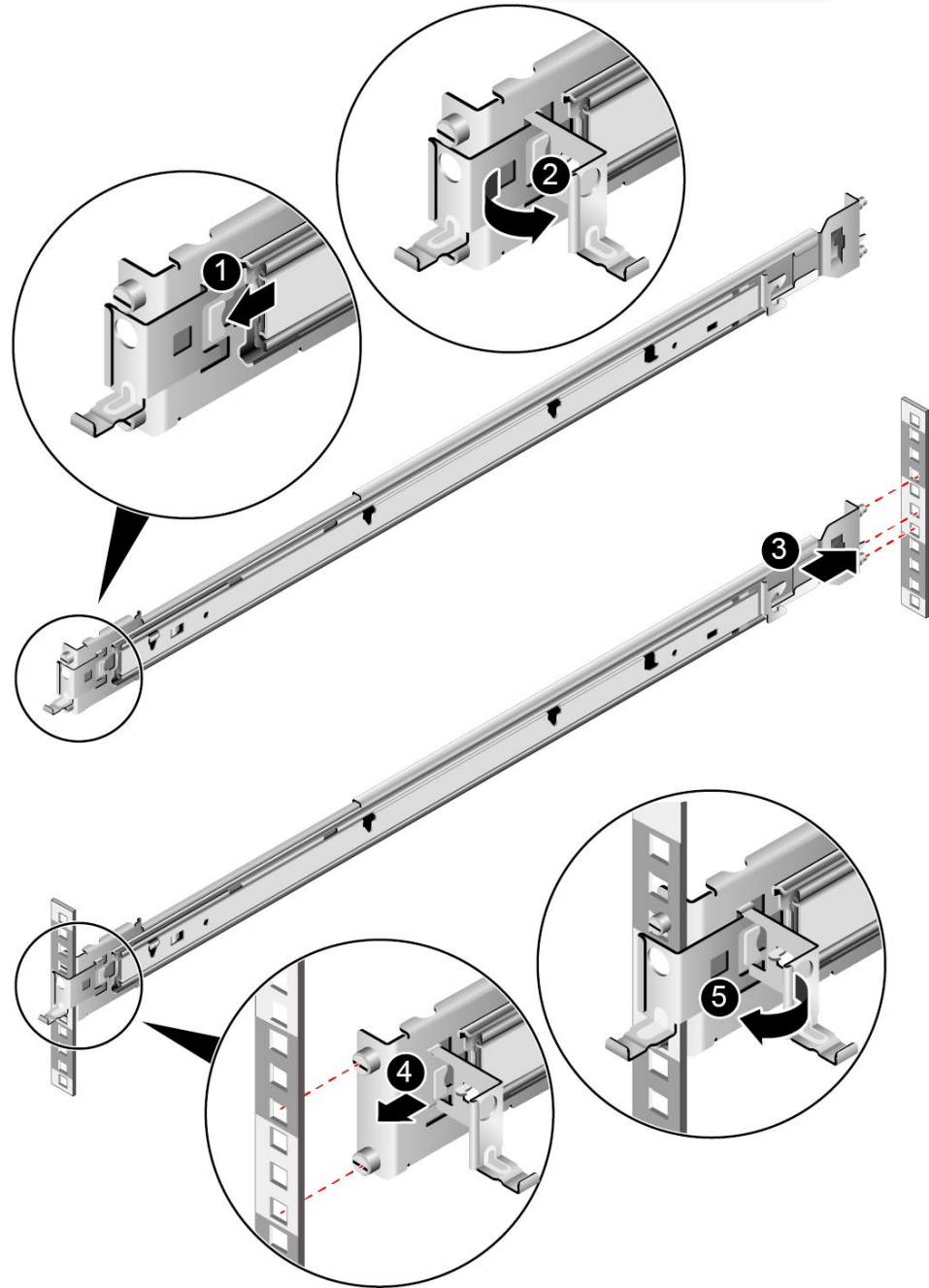
The ball bearing rail kit applies to cabinets with a distance of 610 mm to 914 mm (24.02 in. to 35.98 in.) between the front and rear mounting bars.

The 2488H V5 servers are stackable onto the ball bearing rail kit.

Procedure

- Step 1** Push the release latch on the front of the rail and pull out the hook. See (1) and (2) in Figure 7-8.
- Step 2** Insert the positioning pin at the rear of the rail into the hole on the rear post of the cabinet. See (3) in Figure 7-8.
- Step 3** Keep the rail horizontal, and push the front end of the rail until it is inserted into the hole on the front post of the cabinet. See (4) in Figure 7-8.
- Step 4** Hook the rail. See (5) in Figure 7-8.

Figure 7-8 Installing the ball bearing rail kit



Step 5 Install the other rail in the same way.

----End

7.2.5 Installing a Server

7.2.5.1 Installing a Server on L-Shaped Guide Rails or the Static Rail Kit

Before installing the server, properly install the L-shaped guide rails or static rail kit. For details, see 7.2.4.1 Installing L-Shaped Guide Rails/7.2.4.2 Installing the Static Rail Kit.

Procedure

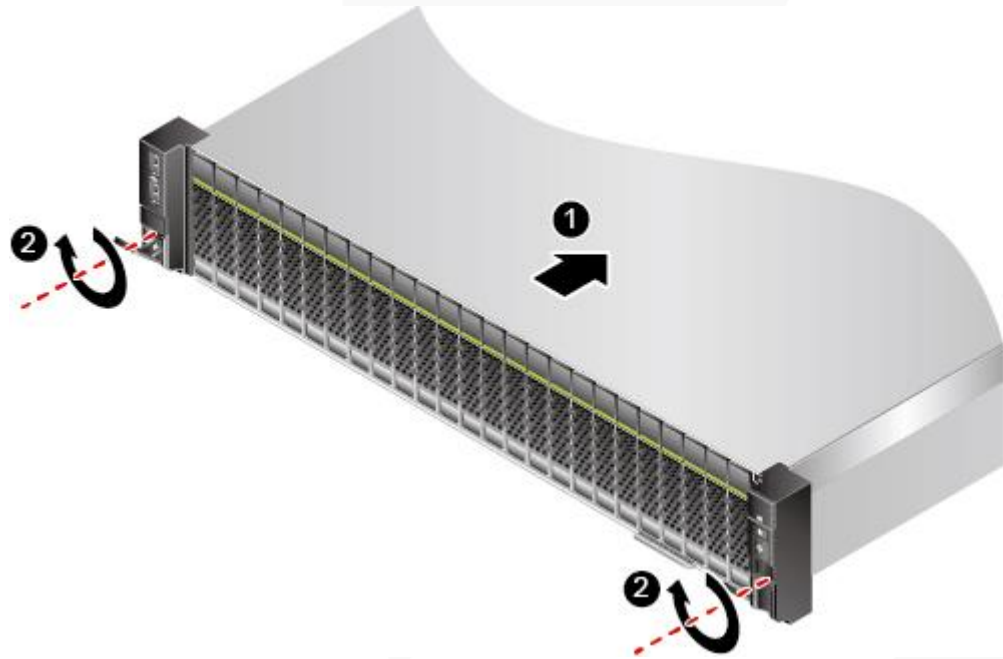
Step 1 Install the server.

NOTICE

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

1. Lift the server, place it on guide rails, and slide it into the chassis. At least two people are required to move the server. See (1) in Figure 7-9.
2. Align the mounting ears on both sides of the server with the mounting bars and tighten the captive screws on the mounting ears. See (2) in Figure 7-9.

Figure 7-9 Installing a server



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

Step 3 Connect the power cables to the PSUs.

For details, see 7.2.6.7 Connecting PSU Cables.

Step 4 Power on the server.

For details, see 7.3.1 Power-On Procedure.

Step 5 Check indicator status.

For details, see 2.1.2 Indicators and Buttons.

----End

7.2.5.2 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.

Procedure

Step 1 Install the server.

NOTICE

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

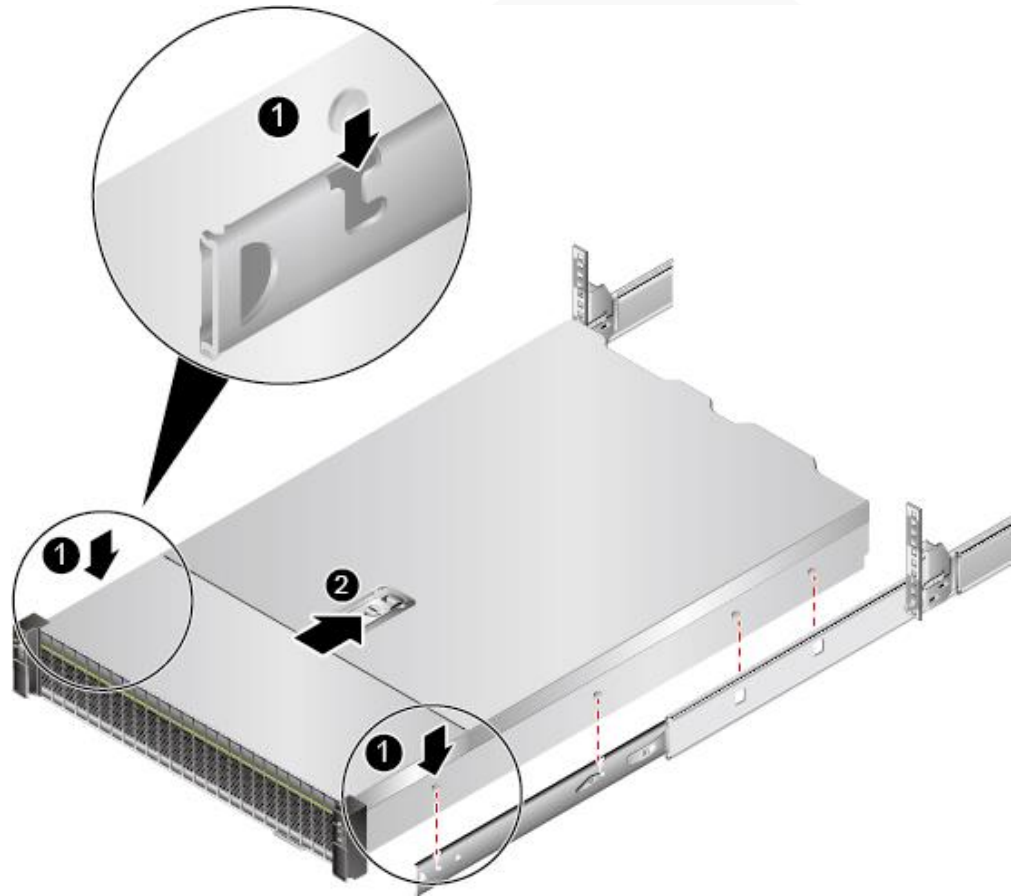
1. Pull out the inner rails as far as they will go.

Figure 7-10 Pulling out an inner rail



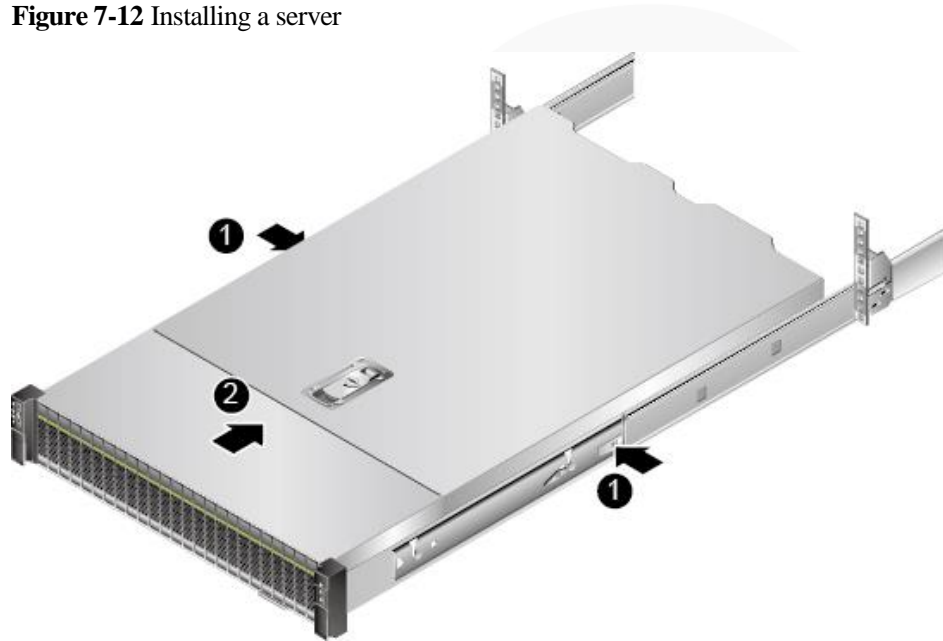
2. Lift the server (at least two people are required), align the positioning pins on the server with the holes on the inner guide rails, and push the server in the arrow direction until the locking pins engage. See (1) and (2) in Figure 7-11.

Figure 7-11 Installing a server on inner rails



3. Press the release buttons on both sides and push the server into the rails. See (1) and (2) in Figure 7-12.

Figure 7-12 Installing a server

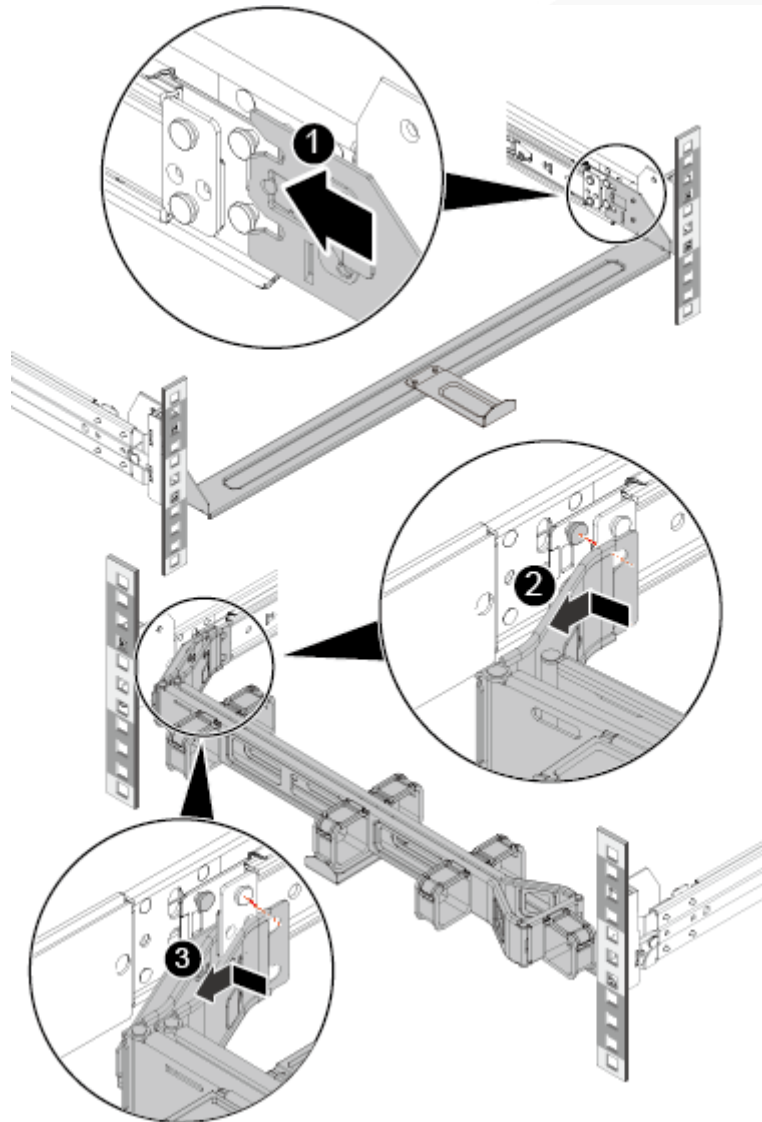


4. Tighten the captive screws on the mounting ears to secure the server.

Step 2 Install a cable management arm (CMA).

1. Insert the support levers into the outer rails on both sides. See (1) in Figure 7-13.
2. Insert the nail heads on the outer left rail into the holes on the outer support lever of the CMA, and pull the CMA in the arrow direction. See (2) in Figure 7-13.
3. Insert the nail heads on the inner left rail into the holes on the inner support lever of the CMA, and pull the CMA in the arrow direction. See (3) in Figure 7-13.

Figure 7-13 Installing the CMA



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

Step 4 Connect the power cables to the PSUs.

For details, see 7.2.6.7 Connecting PSU Cables.

Step 5 Power on the server.

For details, see 7.3.1 Power-On Procedure.

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 Guide

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.

You 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:

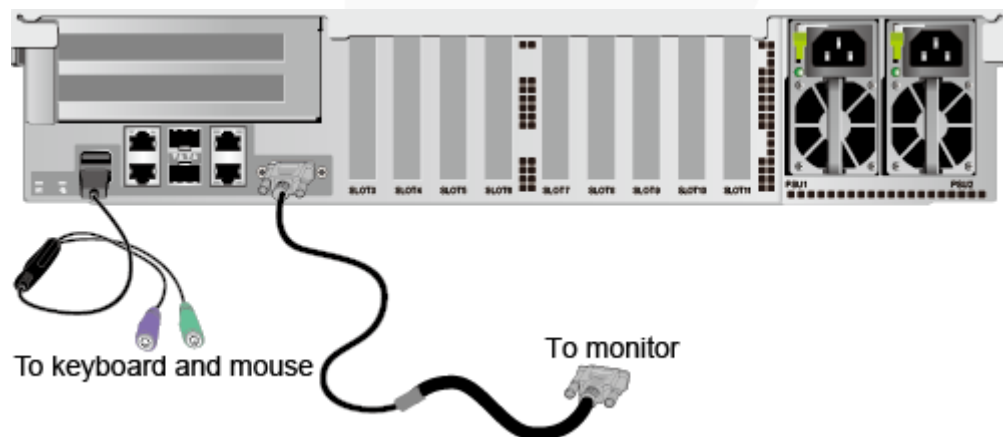
- Connect the keyboard and mouse to the USB ports.
- Connect the keyboard and mouse using a USB-to-PS/2 cable.

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 7-14 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**

According to the result of the EMC test, if a non-shielded cable is used, the system cannot respond to the ESD. As a result, the system is suspended and restarts.

- 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.

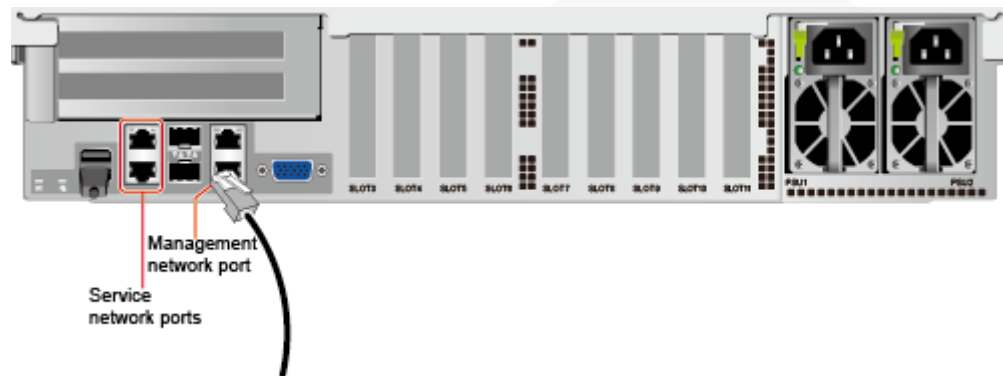
Step 4 Remove the network cable to be replaced.

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 7-15 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.

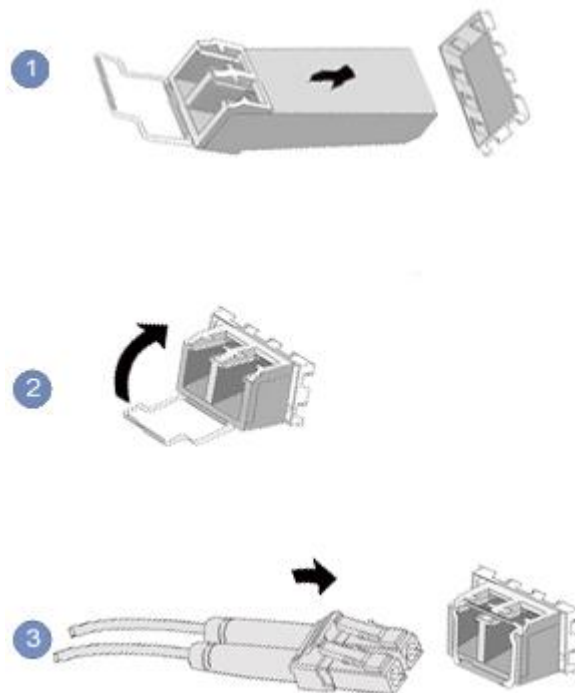
Step 4 Connect the cable to an optical port.

- 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 7-16.
 - ii. Close the latch on the optical module to secure it. See (2) in Figure 7-16.
 - iii. Insert the optical cable into the optical module. See (3) in Figure 7-16.

Figure 7-16 Connecting an optical cable

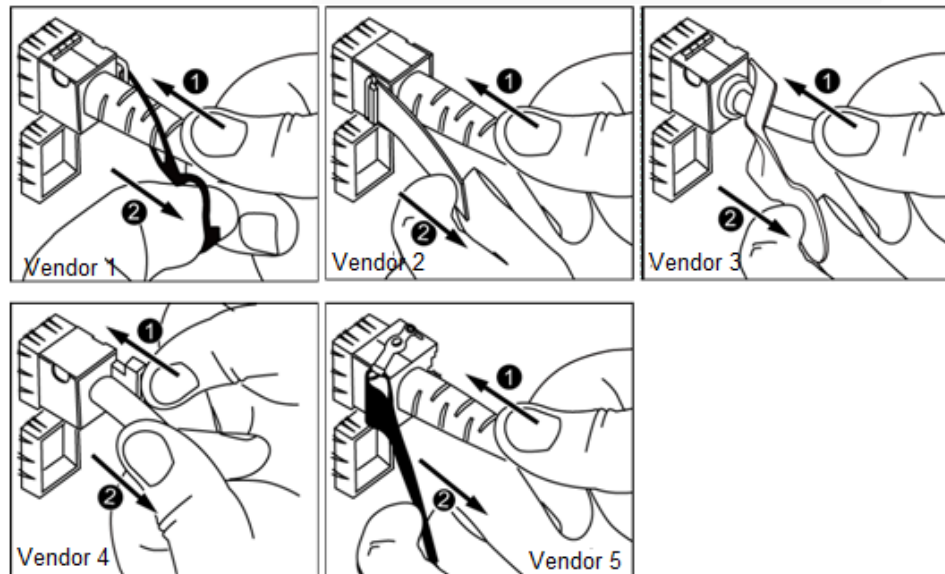


- When you use an SFP+ cable:
 1. Remove the SFP+ cable to be replaced.
Gently push the power connector inwards and pull the latch out to remove the SFP+ cable.

NOTICE

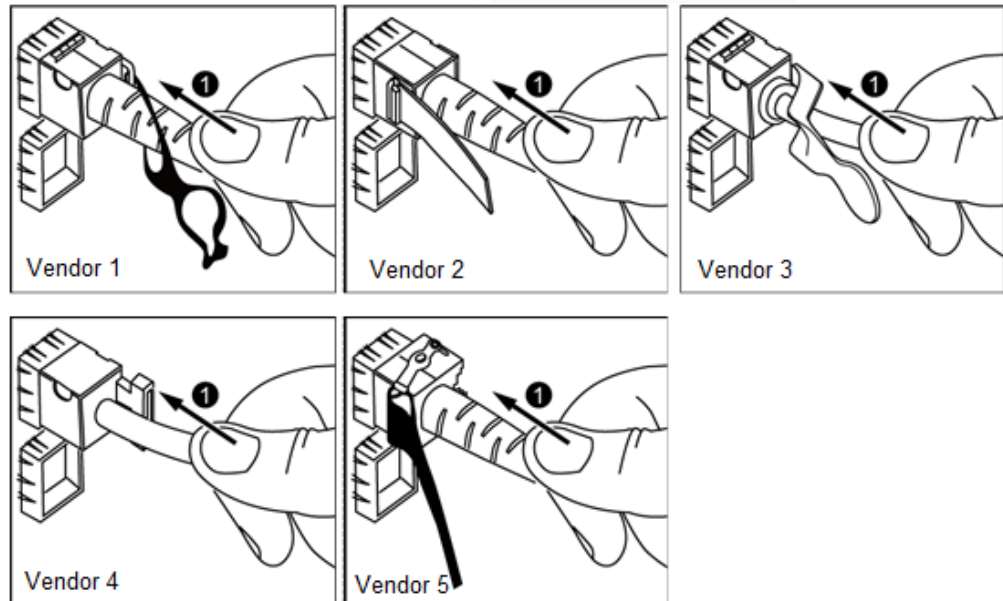
Do not directly pull out the latch.

Figure 7-17 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 7-18 Connecting an SFP+ cable



Step 5 Check whether the new cable is properly connected.

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

- 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.

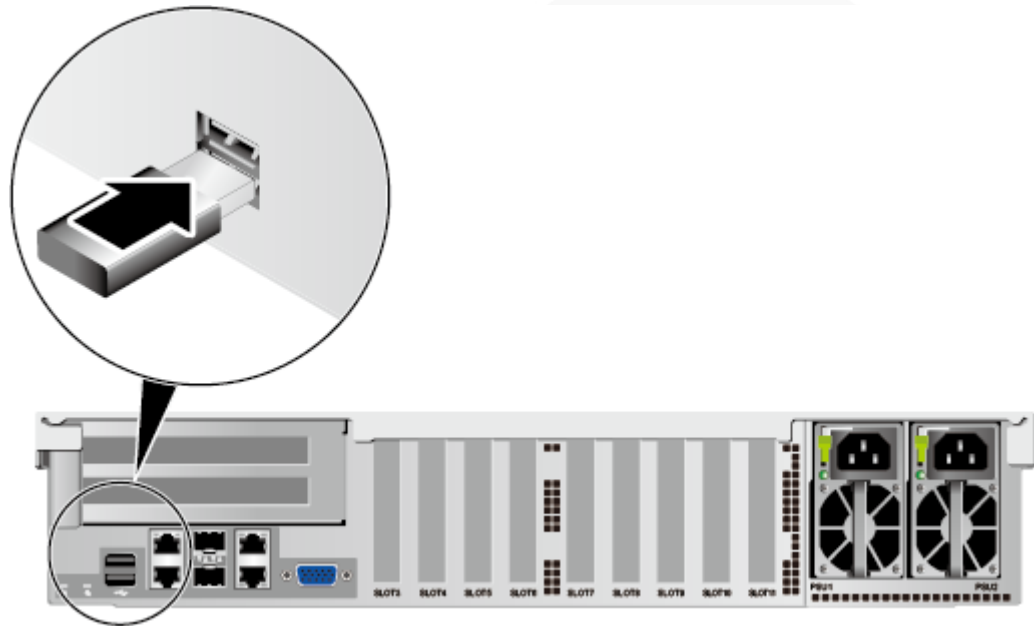
----End

7.2.6.5 Connecting a USB Device

Procedure

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

Figure 7-19 Connecting a USB device



----End

7.2.6.6 Connecting a Serial Cable

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

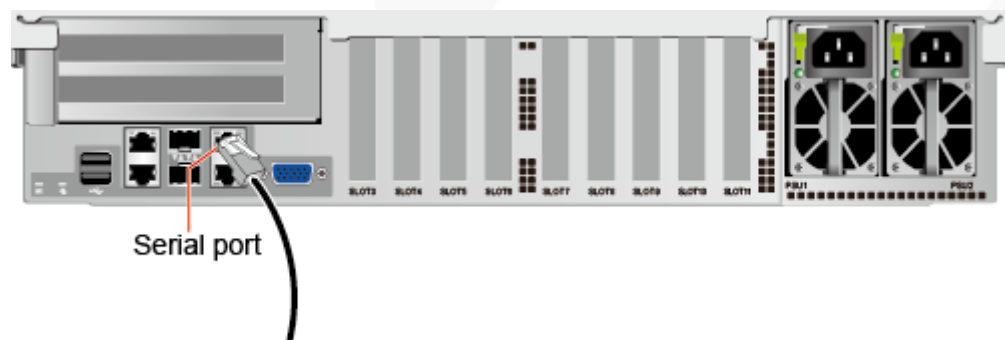
The serial port can be used as:

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

Procedure

Step 1 Connect the serial cable.

Figure 7-20 Connecting a serial cable



----End

7.2.6.7 Connecting PSU Cables

7.2.6.7.1 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

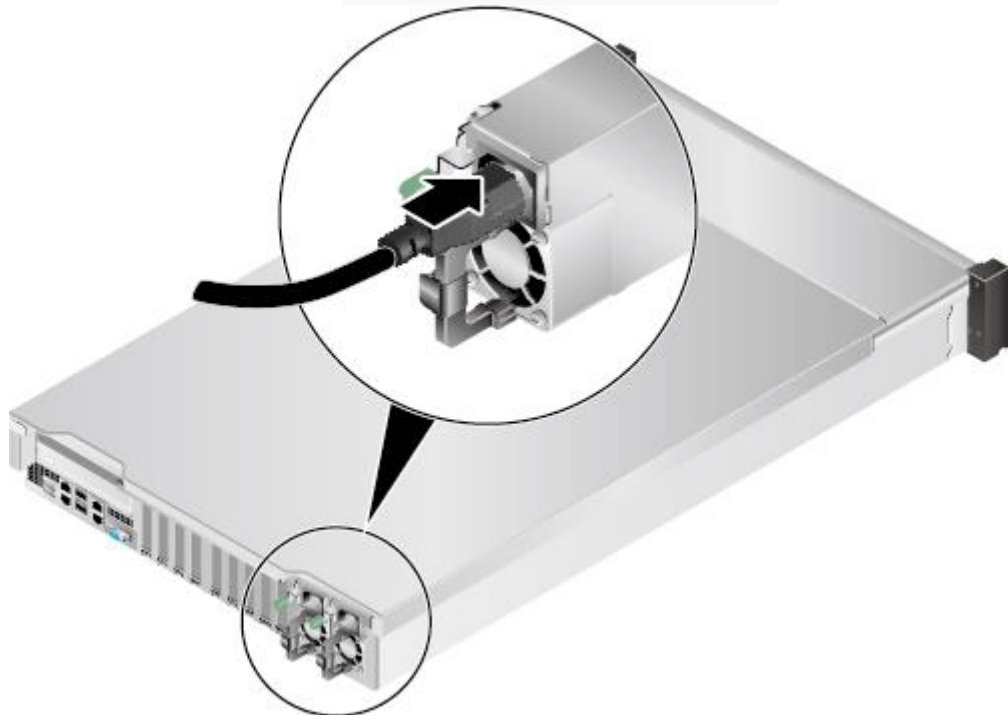
- Use dedicated power cables to ensure equipment and personal safety.
- Use power cables only for dedicated servers. Do not use them for other devices.
- Connect the power cables of the active and standby PSUs to different power distribution units (PDUs) to ensure reliable system operation.
- Ground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

Procedure

Step 1 Take the component out of its ESD bag.

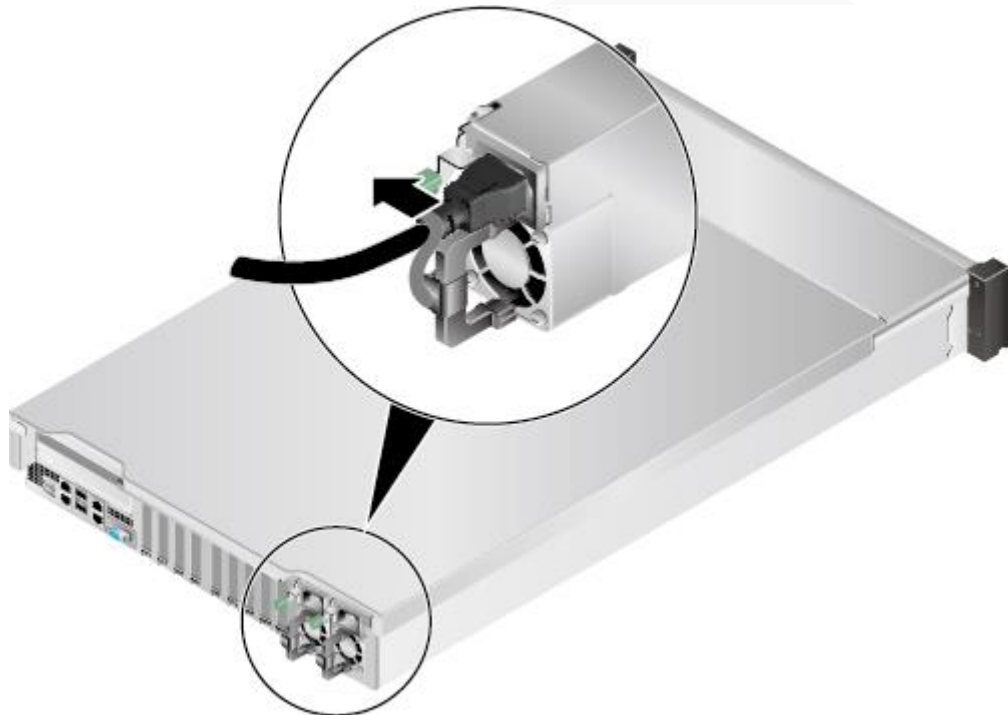
Step 2 Connect one end of the power cable to the power socket on the PSU of the server.

Figure 7-21 Connecting a cable



Step 3 Secure the power cable using a velcro strap.

Figure 7-22 Securing a cable



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

The AC PDU is fastened horizontally in the rear of the cabinet. Connect the power cable to the socket on the PDU according to the plan.

Step 5 Bundle the power cable to the cable guide using cable ties.

----End

7.2.6.7.2 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 power distribution units (PDUs) to ensure reliable system operation.
- Ground the equipment before powering it on.

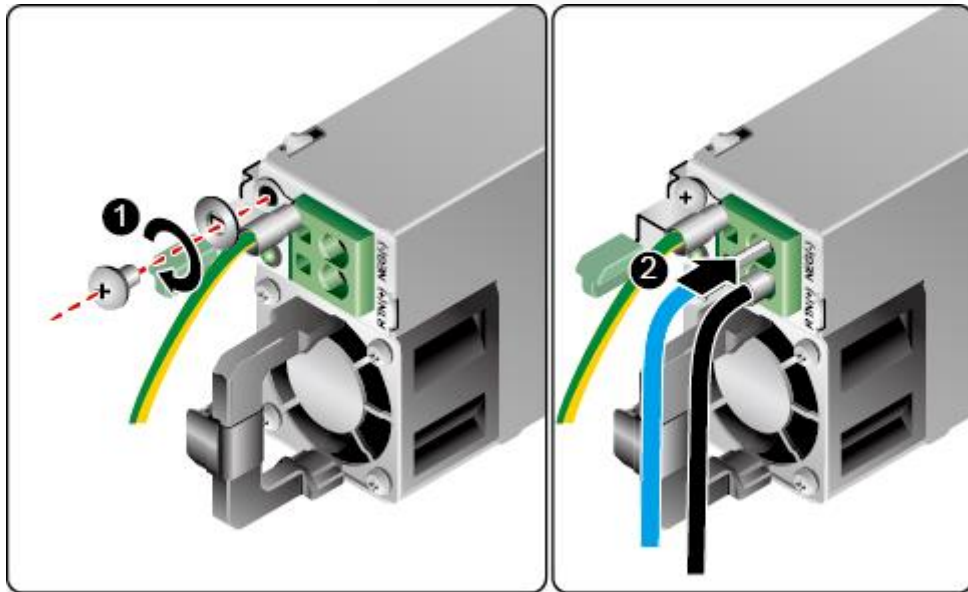
Procedure

Step 1 Take the component out of its ESD bag.

Step 2 Connect the cables to the PSUs.

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 7-23.
2. Insert the power cables to the wiring terminals on the PSU until the cables click into position. See (2) in Figure 7-23.
 - 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 7-23 Connecting cables



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

The DC PDU is fastened horizontally in the rear of the cabinet. Connect the power cable to the socket on the PDU according to the plan.

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

----End

7.2.6.8 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
------	-------------

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	<p>The server does not provide a separate ground port.</p> <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 Power-On Procedure

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 the power-on process, do not remove and insert drives or disconnect and connect network cables or Console port 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

The default value of **System State Upon Power Supply** is **Power On**, which indicates that the server automatically powers on after power is supplied to PSUs. To change the value of **System Power**, log in to the iBMC WebUI and choose **Power > Power Control**.

- If the PSUs are powered on and the server is in standby state (the power indicator is steady yellow), you can 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 **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 9.4 Logging In to the CLI.
 - ii. Run the following command:
ipmcset -d powerstate -v 1
 - iii. Enter **y** or **Y** and press **Enter**.
Power on the server.
- Use the Remote Virtual Console.
 - i. Log in to the Remote Virtual Console.
For details, see 9.3 Logging In to the Desktop of a Server.
 - ii. On the KVM screen, click  or  on the toolbar.
 - iii. Select **Power On**.
The **Select an Option** dialog box is displayed.
 - iv. Click **Yes**.

7.3.2 Power-Off Procedure

NOTE

- 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.
- The "power-off" mentioned here is an operation performed to change the server to the standby state (the power indicator is steady yellow).
- 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.
- Forced power-off may damage user programs or unsaved data. Exercise caution when performing this operation.

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 **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 9.4 Logging In to the CLI.
 - b. Run the following command:
 - To perform graceful power-off, run the **ipmcset -d powerstate -v 0** command.
 - To perform forcible power-off, run the **ipmcset -d powerstate -v 2** command.
 - c. Enter **y** or **Y** and press **Enter**.
Power off the server.
- Use the Remote Virtual Console.
 - a. Log in to the Remote Virtual Console.
For details, see 9.3 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**.
The **Select an Option** dialog box is displayed.
 - d. Click **Yes**.

7.4 Initial Configuration

7.4.1 Default Information

Table 7-4 Default information

Type	Port	Default Value
iBMC management network port data	IP address and subnet mask of the management network port.	<ul style="list-style-type: none"> • IP address: 192.168.2.100 • Subnet mask: 255.255.255.0
iBMC login data	User name and password	<ul style="list-style-type: none"> • User name: Administrator • Password: Admin@9000
BIOS data	Password	<ul style="list-style-type: none"> • Default password: Admin@9000
iBMC U-Boot data	Password	<ul style="list-style-type: none"> • Default password: Admin@9000

7.4.2 Configuration Overview

Configuration Process

Figure 7-24 Initial configuration process

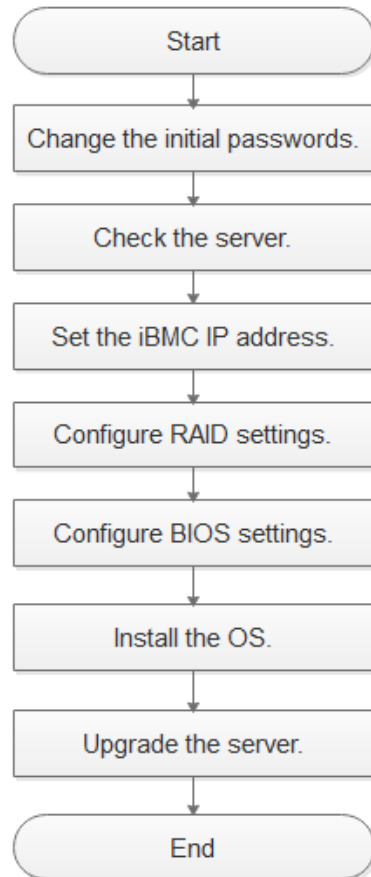


Table 7-5 Initial configuration process

Process	Description
Change the initial passwords.	<ul style="list-style-type: none"> Change the initial password of the default iBMC user. Change the initial password of the iBMC U-Boot.
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.	Configure the iBMC IP address of the server.

Process	Description
Configure RAID settings.	Configure the RAID array based on service requirements.
Configure BIOS settings.	Configure the BIOS settings of the server, including the boot mode, NIC PXE function, and BIOS password.
Install the OS.	Install an OS for the server.
Upgrade the system.	Upgrade software or 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 *FusionServer Rack Server iBMC User Guide*.
- For details about how to configure the RAID controller card, see the *FusionServer V5 Server RAID Controller Card User Guide*.
- For details about how to configure the BIOS, see the *FusionServer Server Purley Platform BIOS Parameter Reference*.
- Install the OS. For details, see *FusionServer Server OS Installation Guide*.
- Handle alarms. For details, see *FusionServer Rack Server iBMC Alarm Handling*.
- Rectify faults. For details, see *FusionServer Servers Troubleshooting*.

7.4.3 Changing Initial Passwords

7.4.3.1 Changing the Initial Password of the Default iBMC User

7.4.3.1.1 Changing the Initial Password of the Default iBMC User (Versions Earlier Than V600)

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 details, see the *FusionServer Rack 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 change the password periodically.
- You are advised to use a password that meets complexity requirements or to enable the password complexity check function.
- The password complexity check function is enabled by default.

Procedure

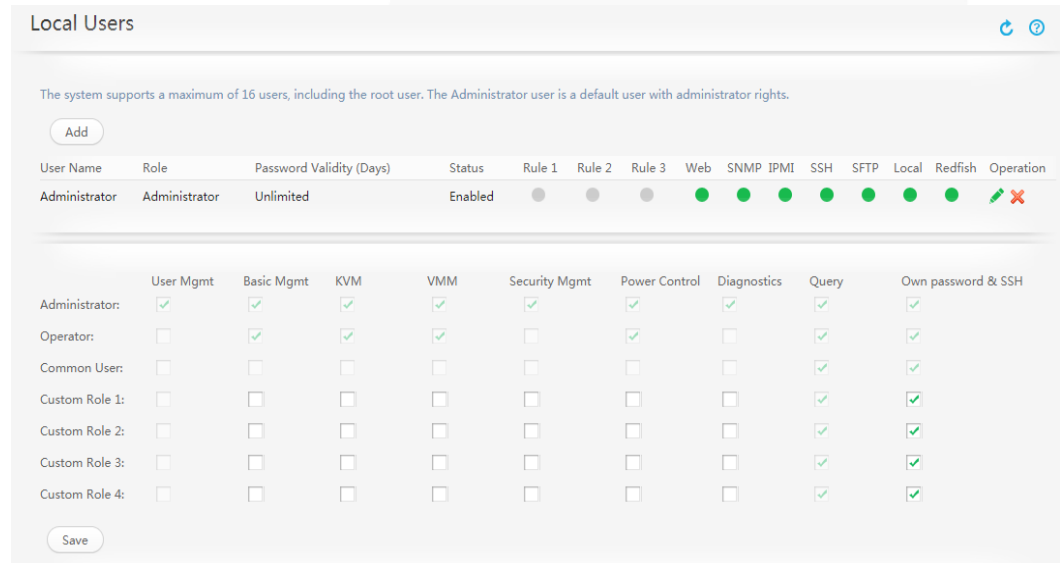
Step 1 Log in to the iBMC WebUI.


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

Step 2 Choose **Configuration > Local Users** from the main menu.

The **Local Users** page is displayed.

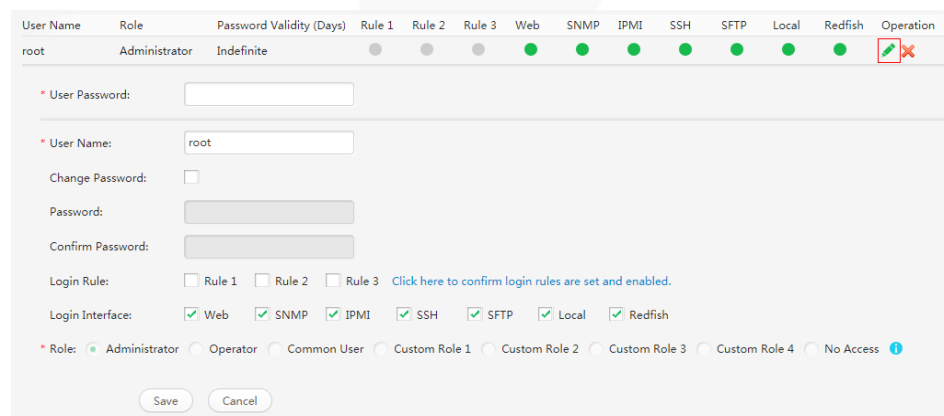
Figure 7-25 The Local Users page



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

The page for changing the password is displayed.

Figure 7-26 Changing password



Step 4 Enter the current password in the **User Password** text box.

Step 5 Select **Change Password**.

Step 6 Enter a new password in **New Password** and **Confirm Password**.

 **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:
`~!@#%&*()-_+=\|{ } ; : ' " , < . > / ?
- Contain 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.
- Contain at least two new characters when compared with the old password.

Step 7 Click **SAVE**.

The initial password of the iBMC is changed.

----End

7.4.3.1.2 Changing the Initial Password of the Default iBMC User (V600 and Later Versions)

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 details, see the [HardServer Rack 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 change the password periodically.
- You are advised to use a password that meets complexity requirements or to enable the password complexity check function.
- The password complexity check function is enabled by default.

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 7-27 The Local Users page

User ID	User Name	Role	Login Interfaces	Operation
2	Administrator	Administrator	SNMP SSH IPMI Local SFTP Web Redfish	Edit Disable Delete
3	albert	Administrator	SNMP SSH IPMI Local SFTP Web Redfish	Edit Disable Delete
4	root	Administrator	SNMP SSH IPMI Local SFTP Web Redfish	Edit Disable Delete

Step 3 Click **Edit** on the right of the user whose password you want to change. The **Edit User** page is displayed.

Figure 7-28 Editing user

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

i 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 **New Password** and **Confirm Password**.

 **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:
`~!@#%&*()-_+=\|[{ }];:","<.>/?
- Contain 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.
- Contain at least two new characters when compared with the old password.

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

7.4.3.2 Changing the Initial Password of the iBMC U-Boot

 **NOTE**

- U-Boot is a kind of underlying software used to configure basic settings, for example, initialize hardware devices and set up memory space mapping, to prepare for commissioning the OS.
- For security purposes, change the initial password upon the first login, and change the password periodically.
- For security purposes, enable password complexity check.
- The password complexity check function is enabled by default.

Procedure

Step 1 Log in to the iBMC CLI.

For details, see 9.4 Logging In to the CLI.

Step 2 Restart the iBMC system.

ipmcset -d reset

Information similar to the following is displayed:

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

Step 3 Type **y** and press **Enter**.

The system restarts.

Step 4 Press **Ctrl+B** immediately when the following information is displayed:

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

Step 5 Enter the default password (**Admin@9000**).

The U-Boot interface is displayed.

```
u-boot>
```

Step 6 Switch to the interface for changing the U-Boot password.

passwd

Information similar to the following is displayed:

```
Enter old password:
```

Step 7 Enter the old password.

Information similar to the following is displayed:

```
Enter new password:
```

Step 8 Enter a new password.

Information similar to the following is displayed:

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

Step 9 Enter the new password again.

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

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

password be changed successfully.
```

Step 10 Exit the U-Boot interface.

boot

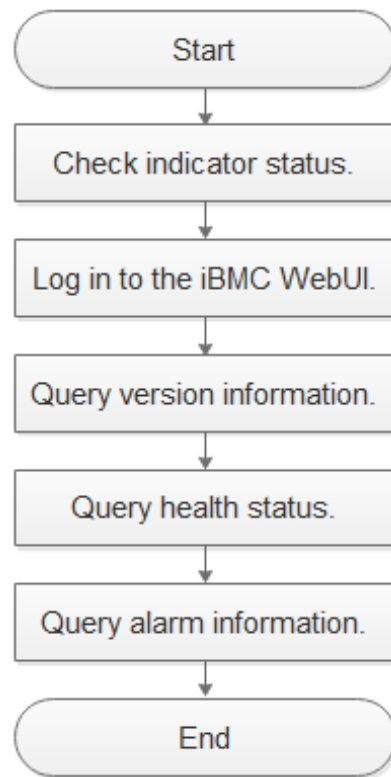
----End

7.4.4 Checking the Server

Workflow

Check the server by performing the following operations:

Figure 7-29 Check process



7.4.4.1 Checking the Server (Versions Earlier than V600)

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 menu bar, choose **System**.
 2. In the navigation tree, choose **Firmware Upgrade** to query the version information of the server.

Figure 7-30 Querying version information

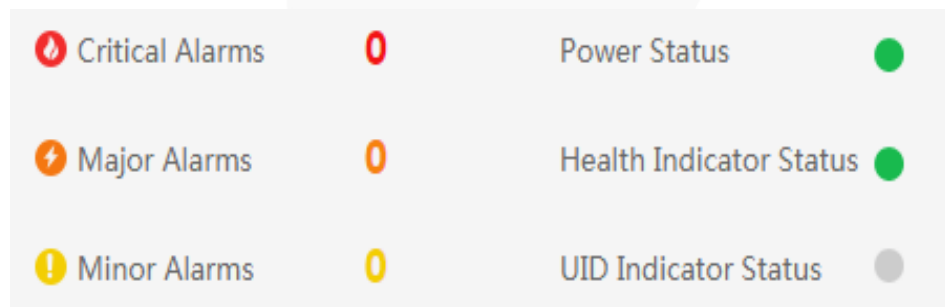


3. Check whether the versions meet site requirements.
 - If yes, go to [Step 4](#).
 - If no, go to [Step 3.4](#).
4. Upgrade the firmware to the target version.
For details, see the [FusionServer Rack Server Upgrade Guide](#).

Step 4 Query health status.

1. On the menu bar, choose **Information**.
2. In the navigation tree, choose **Overview** to query the health status.

Figure 7-31 Querying health status



Step 5 Query alarm information.

Check whether any alarm is generated.

- If yes, handle the alarms.
For details, see the [FusionServer Rack Server iBMC Alarm Handling](#).
- If no, no further action is required.

----End

7.4.4.2 Checking the Server (V600 and Later Versions)

Procedure

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

For details, see 2.1.2 Indicators and Buttons.

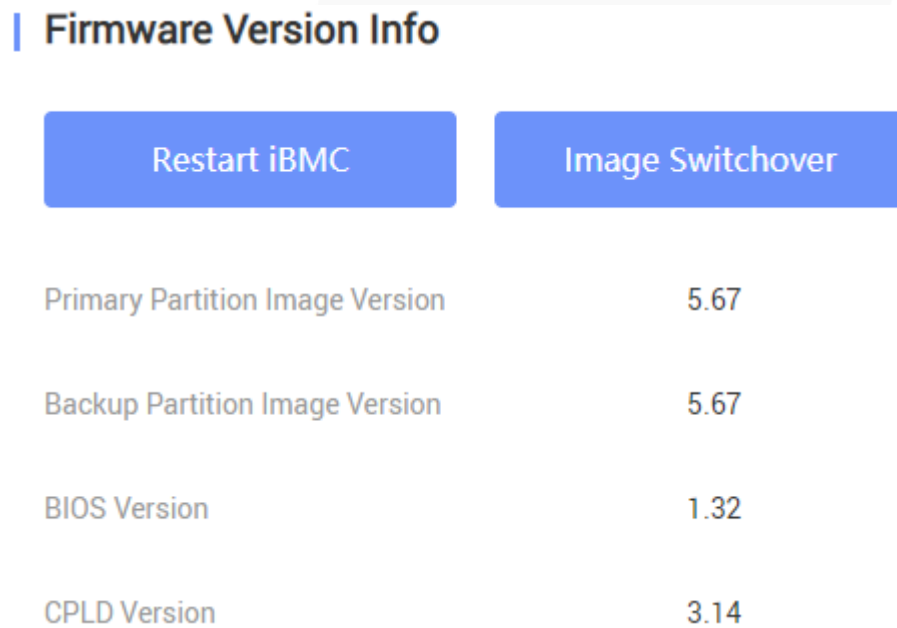
Step 2 Log in to the iBMC WebUI.

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

Step 3 Query version information.

1. On the menu bar, choose **iBMC Settings**.
2. In the navigation tree, choose **Firmware Upgrade** to query the version information of the server.

Figure 7-32 Querying version information



3. Check whether the versions meet site requirements.
 - If yes, go to [Step 4](#).
 - If no, go to [Step 3.4](#).
4. Upgrade the firmware to the target version.
For details, see the *FusionServer Rack Server Upgrade Guide*.

Step 4 Query health status.

1. On the menu bar, choose **Maintenance**.
2. In the navigation tree, choose **Alarm & SEL** to query the health status.

Figure 7-33 Querying health status



Step 5 Query alarm information.

Check whether any alarm is generated.

- If yes, handle the alarms.
For details, see the *FusionServer Rack Server iBMC Alarm Handling*.
- If no, no further action is required.

----End

7.4.5 Configuring the iBMC IP Address

Scenario

This section describes how to configure the iBMC IP address using the BIOS.

You can set the iBMC IP address on:

- BIOS
- LCD
- iBMC WebUI
For details, see the *FusionServer Rack Server iBMC User Guide*.
- iBMC CLI
Run the `ipmcset -d ipaddr` command.
For details, see the *FusionServer Rack Server iBMC User Guide*.

Default IP Address

Default IP Address	Default Subnet Mask
192.168.2.100	255.255.255.0

Procedure (on the BIOS)

- Step 1** Restart the server, and enter the BIOS.
For details, see 9.6 Accessing the BIOS.
- Step 2** Choose **Advanced > IPMI iBMC Configuration** and press **Enter**.
The **IPMI iBMC Configuration** screen is displayed.
- Step 3** Select **iBMC Configuration** and press **Enter**.
The **iBMC Configuration** screen is displayed, showing the iBMC IP address.
- Step 4** Select **IPv4 IP Address** or **IPv6 Static IP Address** and press **Enter**.
The IPv4 or IPv6 address configuration screen is displayed.
- Step 5** Change the IPv4 or IPv6 address of the iBMC management network port.
- Step 6** Press **F10**.
Save the settings and exit.

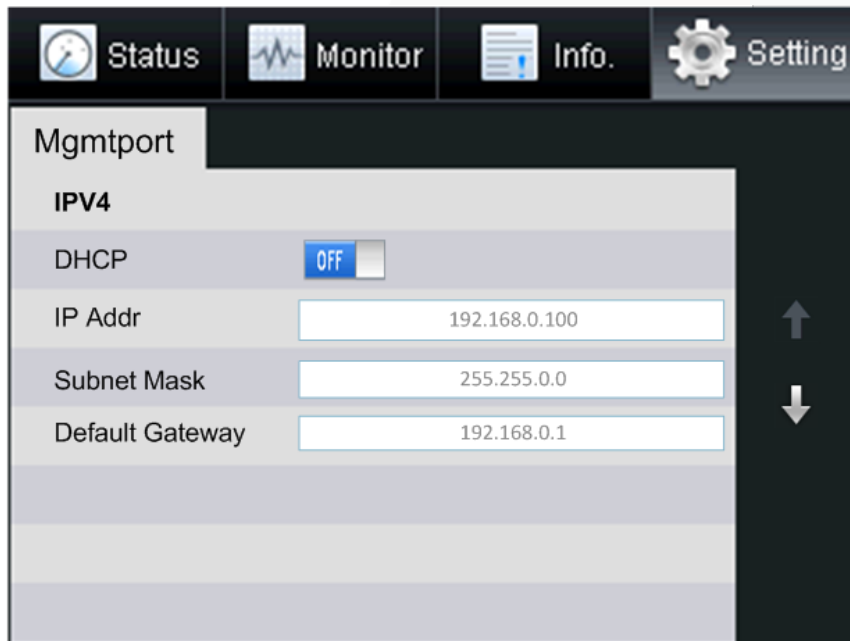
----End

Procedure (on the LCD)

Step 1 On the LCD, tap the **Setting** tab.

The **Setting** screen is displayed.

Figure 7-34 Setting screen



Step 2 Tap the **Mgmt Port** tab.

The **Mgmt Port** screen is displayed.

Step 3 Set an IP address for the management network port.

NOTE

The soft keyboard is displayed when you tap the text box. Use the soft keyboard to set IP address information or tap **Cancel** to return to the **Mgmt Port** tab.

----End

7.4.6 Configuring RAID

The 2488H V5 supports multiple types of RAID controller cards.

- Use [Compatibility Checker](#) to obtain information about the compatible RAID controller cards.
- For details about how to configure the RAID controller card, see the [Hard' Server V5 Server RAID Controller Card User Guide](#).

7.4.7 Configuring the BIOS

Scenario

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

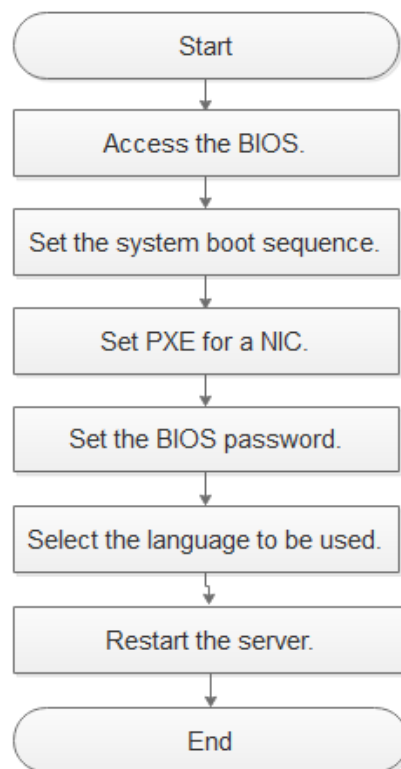
To configure the BIOS, perform the following operations:

- 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 *FusionServer Server Purley Platform BIOS Parameter Reference*.

Workflow

Figure 7-35 Process for configuring the BIOS



7.4.7.1 Accessing the BIOS

Procedure

Step 1 Restart the server, and enter the BIOS.

For details, see 9.6 Accessing the BIOS.

----End

7.4.7.2 Setting the System Boot Sequence

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

Procedure

Step 1 On the BIOS main screen, choose **Boot**.

The **Boot** screen is displayed.

Step 2 Select **Boot Type** and press **Enter**.

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

Step 3 Select **Legacy Boot** or **UEFI Boot**, and then press **Enter**.

NOTE

- The default boot mode is UEFI.
- For some OSs, if the capacity of the drive or RAID array for installing the OS is greater than 2 TB, use the UEFI boot 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 boot mode supports more boot devices than the Legacy boot mode. The UEFI boot mode is recommended if a server is configured with multiple boot devices. Some devices may fail to boot in the Legacy mode. If the legacy mode has to be set, disable serial port redirection or NIC PXE based on service requirements so that the OS can start. For details, see "Setting PXE for a NIC" and "Setting Serial Port Redirection" in *FusionServer Server Purley Platform BIOS Parameter Reference*.

Step 4 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 > Others**.

Step 5 Select the target boot device and press **F5** or **F6** to change the boot order.

- 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.

----End

7.4.7.3 Configuring PXE for a NIC

If a server is configured with multiple NICs, you can set the PXE function for the NICs on the BIOS.

NOTE

If multiple boot devices of the same type are configured for a server, you can set the system boot sequence on the BIOS. For details about how to set different boot devices, see the [FusionServer Server Purley Platform BIOS Parameter Reference](#).

Procedure

Step 1 On the BIOS main screen, choose **Advanced**.

The **Advanced** screen is displayed.

Step 2 Select **PXE Configuration** and press **Enter**.

The **PXE Configuration** screen is displayed.

NOTE

- Four on-board network ports can be displayed on the PXE screen. The default value is **Enabled** for PXE1 and PXE3 and **Disabled** for other network ports.
- The I/O NIC ports are also displayed on the **PXE Configuration** screen.

Step 3 Select the network port to be configured and press **Enter**.

The dialog box for setting the network port is displayed.

Step 4 Select **Enabled** and press **Enter**.

NOTE

To disable PXE for a network port, select **Disabled** and press **Enter**.

----End

7.4.7.4 Setting the BIOS Password

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

NOTE

- The password complexity check function is enabled by default.
- You are advised to use a password that meets complexity requirements or to enable the password complexity check function.
- For security purposes, change the administrator password periodically.

Procedure

Step 1 On the BIOS main screen, choose **Security**.

The **Security** screen is displayed.

Step 2 Select **Manage Supervisor Password** and press **Enter**.

The **Manage Supervisor Password** screen is displayed.

Step 3 Change the BIOS password.

 **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 administrator 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 previous five passwords cannot be reused as a new password.
- After the administrator password is set, the **Delete Supervisor Password** parameter is displayed, which can be used to clear the 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 will reduce system security. Exercise caution when enabling this function.

----End

7.4.7.5 Switching the GUI Language

Procedure

Step 1 On the BIOS main screen, choose **Main**.

The **Main** screen is displayed.

Step 2 Select **Language** and press **Enter**.

The **Language** screen is displayed.

Figure 7-36 Switching the language (V3XX and earlier versions)



Step 3 Select the language to be used and press **Enter**.

The target language is set for the GUI.

----End

7.4.7.6 Restarting the Server

After the settings, you need to restart the server for the settings to take effect.

Procedure

Step 1 On the BIOS, press **F10**.

The **Save Changes&Exit** dialog box is displayed.

Step 2 Select **Yes** and press **Enter**.

Settings are saved and the BIOS is exited. The server automatically restarts for the settings to take effect.

----End

7.4.8 Installing an OS

The 2488H V5 supports multiple types of OSs.

- Use [Compatibility Checker](#) to obtain information about the compatible operating systems.
- For details about how to install the OS, see [FusionServer 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](#)
- [FusionServer Server OS Installation Guide](#)
- [FusionServer Rack Server Upgrade Guide](#)
- [FusionServer iDriver List](#)

Upgrading Software or Firmware

- Upgrade the iBMC, BIOS, CPLD, or other firmware. For details, see the [FusionServer Rack Server Upgrade Guide](#).

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 [Compatibility Checker](#).
For example, the Windows V304 driver package is [FusionServer iDriver-Windows-Driver-V304.zip](#).
- Install or upgrade the driver. For details, see [FusionServer 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 *FusionServer 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**
Preventive maintenance promptly detects, diagnoses, and rectifies server faults.

9 Common Operations

- 9.1 Querying the iBMC IP Address
- 9.2 Logging In to the iBMC WebUI
- 9.3 Logging In to the Desktop of a Server
- 9.4 Logging In to the CLI
- 9.5 Managing VMD
- 9.6 Accessing the BIOS

9.1 Querying the iBMC IP Address

Scenario

Query the IP address of the iBMC management network port. The following describes how to query the iBMC IP address on the BIOS.

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

- BIOS
- iBMC WebUI
For details, see the *FusionServer Rack Server iBMC User Guide*.
- iBMC CLI
Run the `ipmcget -d ipinfo` command.
For details, see the *FusionServer Rack Server iBMC User Guide*.

Procedure

- Step 1** Access the BIOS.
- Step 2** Choose **Advanced > IPMI iBMC Configuration**, and press **Enter**.
The **IPMI iBMC Configuration** screen is displayed.
- Step 3** Select **iBMC Configuration** and press **Enter**.
The **iBMC 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

9.2.1 Logging In to the iBMC WebUI (Versions Earlier Than V600)

Scenario

This section describes how to log in to the iBMC WebUI. The following uses Internet Explorer 11.0 as an example.

NOTE

- 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 user enters incorrect passwords for five consecutive times. The user account is automatically unlocked 5 minutes later. The system administrator can also unlock a user account using the CLI.
- For security purposes, change the initial password upon the first login and periodically change the password.
- 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.

Procedure

Step 1 Ensure that the client used to access the iBMC meets the operating environment requirements.

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

Table 9-1 Operating environment requirements

OS	Web Browser	Java Runtime Environment (JRE)
Windows 7 (32-bit) Windows 7 (64-bit)	Internet Explorer 9.0 to 11.0	JRE 1.7 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U45
	Google Chrome 21.0 to 44.0	JRE 1.8 U144
Windows 8 (32-bit) Windows 8 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U45
	Google Chrome 21.0 to 44.0	JRE 1.8 U144
Windows 10 (64-bit)	Internet Explorer 11.0	JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144

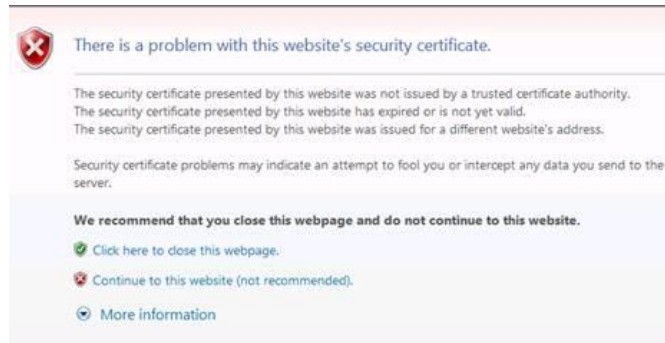
OS	Web Browser	Java Runtime Environment (JRE)
Windows Server 2012 R2 64-bit	Internet Explorer 11.0	JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
Windows 2016 (64-bit)	Internet Explorer 11.0	JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
Windows Server 2008 R2 (64-bit)	Internet Explorer 9.0 to 11.0	JRE 1.7 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U45
	Google Chrome 21.0 to 44.0	JRE 1.8 U144
Windows Server 2012 (64-bit)	Internet Explorer 10.0 to 11.0	JRE 1.7 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U45
	Google Chrome 21.0 to 44.0	JRE 1.8 U144
Red Hat 6.0 (64-bit)	Mozilla Firefox 39.0 to 54.0	JRE 1.7 U45
		JRE 1.8 U45
		JRE 1.8 U144
MAC OS X v10.7	Safari 8.0	JRE 1.7 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U45
		JRE 1.8 U144

- Step 2** Use a network cable to connect the Ethernet port on the local PC to the iBMC management network port.
- Step 3** Set an IP address and subnet mask or route information for the local PC to enable the PC to communicate with the iBMC.
- Step 4** Open the browser on the local PC, enter **https://iBMC management network port IP address** in the address box, and press **Enter**.

The iBMC login page is displayed.

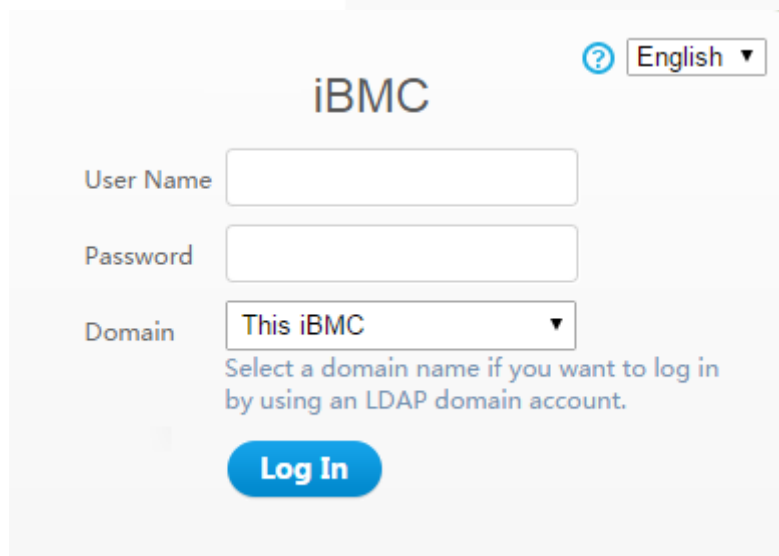
 **NOTE**

- If the language of the browser you use to log in to the iBMC WebUI is not Chinese, English, or Japanese, upgrade the iBMC to V260 or later. Otherwise, the login page may fail to display.
- If the message "There is a problem with this website's security certificate" is displayed, click **Continue to this website (not recommended)**.



- If a security alert is displayed, you can ignore this message or perform any of the following to shield this alert:
- Import a trusted certificate and a root certificate to the iBMC.
For details, see "Importing the 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.

Figure 9-1 iBMC login page



Step 5 Log in to the iBMC.

- Log in as a local user.
 - a. Select a language.
 - b. On the login page displayed, enter the user name and password.

NOTE

- The system provides a default user of the administrator group. The default user is **Administrator**, and the default password is **Admin@9000**.
- 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.
- c. Select **Local iBMC** or **Automatic matching** from the **Domain** drop-down list.
- d. Click **Log In**.

After the login is successful, the **Overview** page is displayed, showing the user name in the upper right corner.

 **NOTE**

- The system may display a message indicating an incorrect user name or password when you attempt to log in using Internet Explorer after the system is upgraded. If this occurs, press **Ctrl+Shift+DEL**, click **Delete** to clear the browser cache, and attempt to log in again.
- If you fail to log in to the iBMC WebUI through an Internet Explorer, choose **Tools > Internet Options > Advanced** in the menu bar and click **Reset** to restore default settings of Internet Explorer. Then attempt to log in again.
- Log in to the iBMC as an LDAP user.

NOTICE

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.

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 **Configuration > 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.

-
- a. Select a language.
 - b. Enter the LDAP user name and password.

 **NOTE**

- LDAP user name (In this case, **Domain** can be **Automatic matching** or a specified domain.)
- LDAP user name@Domain name (In this case, **Domain** must be **Automatic matching**.)
- In versions earlier than iBMC V294, the maximum password length for an LDAP user is 20 characters. In iBMC V294 and later versions, the maximum password length for an LDAP user is 255 characters.
- c. Select the LDAP user domain from the **Domain** drop-down list.

 **NOTE**

- **Configured domain servers:** Select a domain server to log in as an LDAP user. The iBMC automatically locates the user from the domain server.
- **Automatic matching:** If this option is selected, the iBMC searches for the user from the local user list first. If no match is found, the iBMC searches from the domain servers in the sequence displayed in the **Domain** drop-down list.
- d. Click **Log In**.

After the login is successful, the **Overview** page is displayed, showing the user name in the upper right corner.

----End

9.2.2 Logging In to the iBMC WebUI (V600 and Later Versions)

Scenario

This section describes how to log in to the iBMC WebUI. The following uses Internet Explorer 11.0 as an example.

NOTE

- 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. 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 periodically change the password.
- 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.

Procedure

Step 1 Ensure that the client used to access the iBMC meets the operating environment requirements.

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

Table 9-2 Operating environment requirements

OS	Web Browser	Java Runtime Environment (JRE)
Windows 7 (32-bit) Windows 7 (64-bit)	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	
Windows 8 (32-bit) Windows 8 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	
Windows 10 (64-bit)	Internet Explorer 11.0 Microsoft Edge	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	

OS	Web Browser	Java Runtime Environment (JRE)
Windows Server 2008 R2 (64-bit)	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	
Windows Server 2012 (64-bit)	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	
Windows Server 2012 R2 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	
Windows Server 2016 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 to 84.0	
CentOS 7	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
MAC OS X v10.7	Safari 9.0 to 13.1	AdoptOpenJDK 8u222 JRE
	Mozilla Firefox 45.0 to 79.0	AdoptOpenJDK 11.0.6 JRE

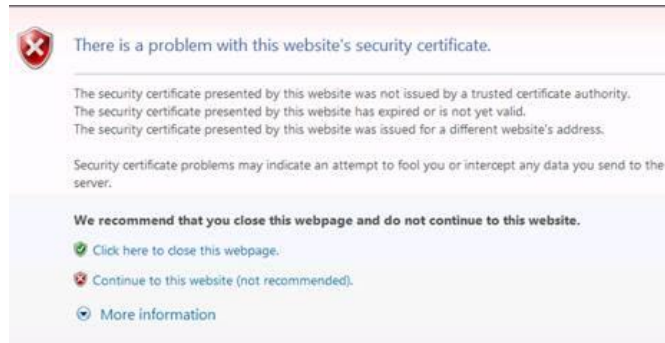
Step 2 Use a network cable to connect the Ethernet port on the local PC to the iBMC management network port.

Step 3 Open the browser on the local PC, enter **https://iBMC management network port IP address** in the address box, and press **Enter**.

The iBMC login page is displayed.

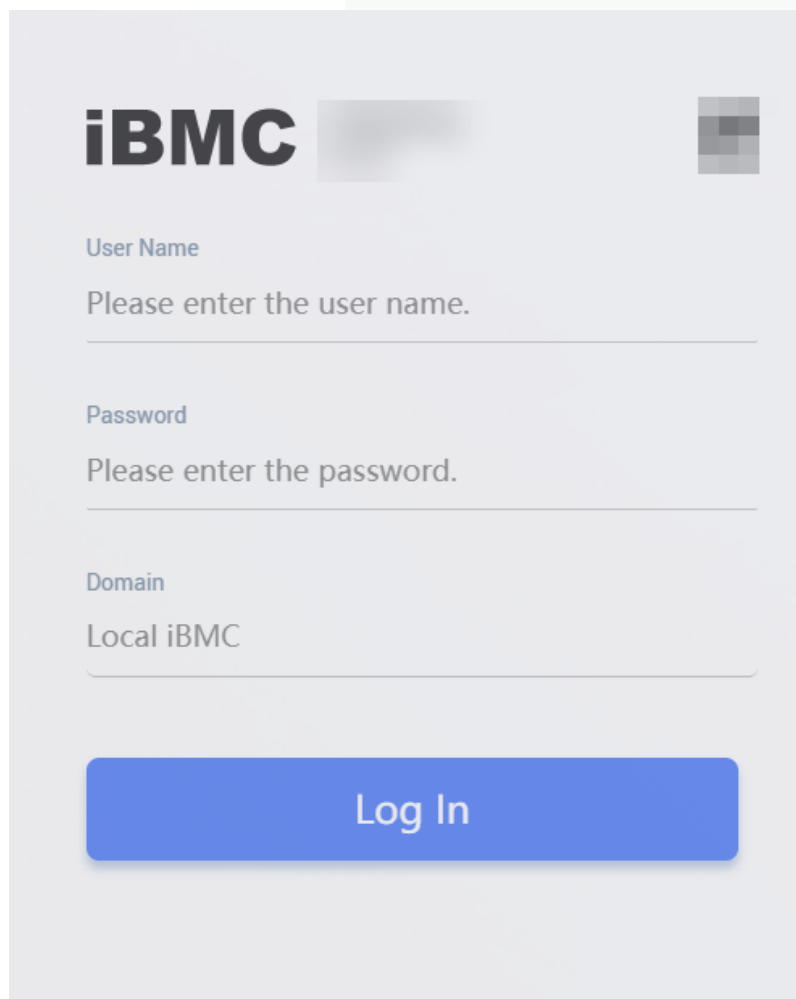
 **NOTE**

- The IPv6 address must be enclosed in brackets. Examples:
- IPv4 address: **192.168.100.1**.
- IPv6 address: **[fc00::64]**.
- If the message "There is a problem with this website's security certificate" is displayed, click **Continue to this website (not recommended)**.



- If a security alert is displayed, you can ignore this message or perform any of the following to shield this alert:
- Import a trusted certificate and a root certificate to the iBMC.
For details, see "Importing the 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.

Figure 9-2 iBMC login page



Step 4 The iBMC login page is displayed.

- Log in as a local user.
 - a. Select a language.
 - b. On the login page displayed, enter the user name and password.

 **NOTE**

- The system provides a default user of the administrator group. The default user is **Administrator**, and the default password is **Admin@9000**.
- 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.
- c. Select **Local iBMC** or **Automatic matching** from the **Domain** drop-down list.
- d. Click **Log In**.

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

 **NOTE**

- The system may display a message indicating an incorrect user name or password when you attempt to log in using Internet Explorer after the system is upgraded. If this occurs, press **Ctrl+Shift+DEL**, click **Delete** to clear the browser cache, and attempt to log in again.
- If you fail to log in to the iBMC WebUI through an Internet Explorer, choose **Tools > Internet Options > Advanced** in the menu bar and click **Reset** to restore default settings of Internet Explorer. Then attempt to log in again.
- Log in to the iBMC as an LDAP user.

NOTICE

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.

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.

-
- a. Select a language.
 - b. Enter the LDAP user name and password.

 **NOTE**

- 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.)
- The password cannot exceed 255 characters.
- c. Select the LDAP user domain from the **Domain** drop-down list.

 **NOTE**

- **Configured domain servers:** Select a domain server to log in as an LDAP user. The iBMC automatically locates the user from the domain server.
- **Automatic matching:** If this option is selected, the iBMC searches for the user from the local user list first. If no match is found, the iBMC searches from the domain servers in the sequence displayed in the **Domain** drop-down list.

d. Click **Log In**.

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

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

 **NOTE**

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.

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

- Logging in as a Kerberos domain user
- Logging in over SSO

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.

Logging In as a Kerberos Domain User

- (Optional) On the iBMC login page, switch to the target language.
- Enter the Kerberos user name and password.

 **NOTE**

- 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 all letters used in the domain name must be in upper case.)
- When you log in to the iBMC WebUI as a Kerberos domain user, the password can contain a maximum of 255 characters.

- 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

- Use the Kerberos user name and password configured on the Kerberos server to log in to the client OS.

- 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.

- Click **SSO**.

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

----End

9.3 Logging In to the Desktop of a Server

9.3.1 Using the Remote Virtual Console

9.3.1.1 iBMC

9.3.1.1.1 Versions Earlier Than V600

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 On the menu bar, choose **Remote Console**. The **Remote Console** page is displayed.

Figure 9-3 Remote Console page

Remote Console ↻ ⓘ

Integrated Remote Console

The Java integrated remote console requires Java Runtime Environment (JRE) to be installed. Click [here](#) to download JRE. [More information...](#)

[Java Integrated Remote Console \(Private\)](#)
[Java Integrated Remote Console \(Shared\)](#)
[HTML5 Integrated Remote Console \(Private\)](#)
[HTML5 Integrated Remote Console \(Shared\)](#)

Independent Remote Console

With the Independent Remote Console (IRC), you can access and manage the server in real time. The IRC does not depend on the browser, OS, or JRE version. [Download](#).

Remote Console Settings

Timeout Period (min)	<input type="text" value="0"/>
Maximum Sessions	2
Active Sessions	0
Encryption	<input type="checkbox"/>
Enable Local KVM	<input checked="" type="checkbox"/>
Persistent Virtual Keyboard and Mouse	<input checked="" type="checkbox"/>

[Save](#)

Virtual Media

Maximum Sessions	1
Active Sessions	0
Encryption	<input type="checkbox"/>

[Save](#)

VNC Service

Timeout Period (min)	<input type="text" value="0"/>
Keyboard Layout	English(US) ▼
VNC Password	<input type="text"/>
Confirm Password	<input type="text"/>
Password Validity (Days)	Unlimited
Login Rules	<input type="checkbox"/> Rule1 <input type="checkbox"/> Rule2 <input type="checkbox"/> Rule3 View login rules
SSL Encryption	<input type="checkbox"/>
Maximum Sessions	5
Active Sessions	0

[Save](#)

Step 3 Click an Integrated Remote Console.

NOTE

- **Java Integrated Remote Console (Private):** allows only one local user or VNC user to access and perform operations on the server through the iBMC.
- **Java Integrated Remote Console (Shared):** allows two local users or up to five VNC users to simultaneously access and perform operations on the server through the iBMC. The users can see each other's operations.
- **HTML5 Integrated Remote Console (Private):** allows only one local user or VNC user to access and perform operations on the server through the iBMC.
- **HTML5 Integrated Remote Console (Shared):** allows two local users or up to five VNC users to simultaneously access and perform operations on the server through the iBMC. The users can see each other's operations.
- For details about the virtual console, see "Virtual Console" in the iBMC user guide of the server you use.

Figure 9-4 Java Integrated Remote Console

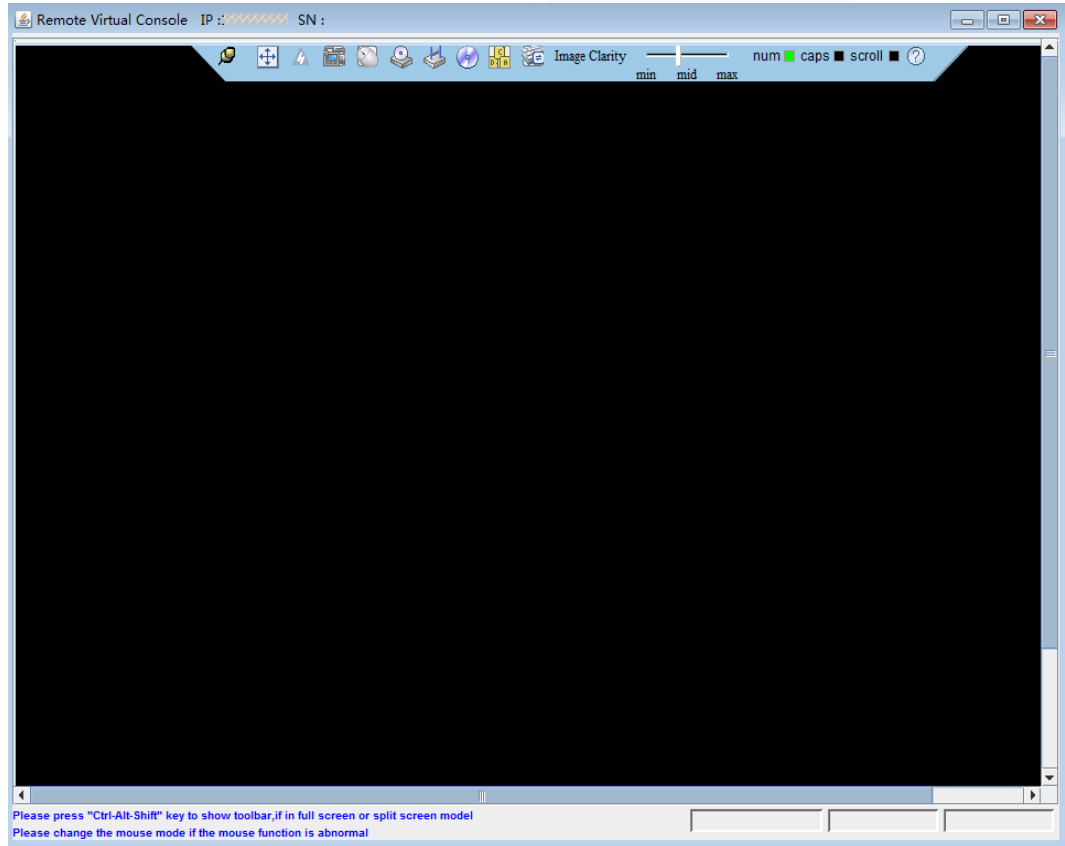
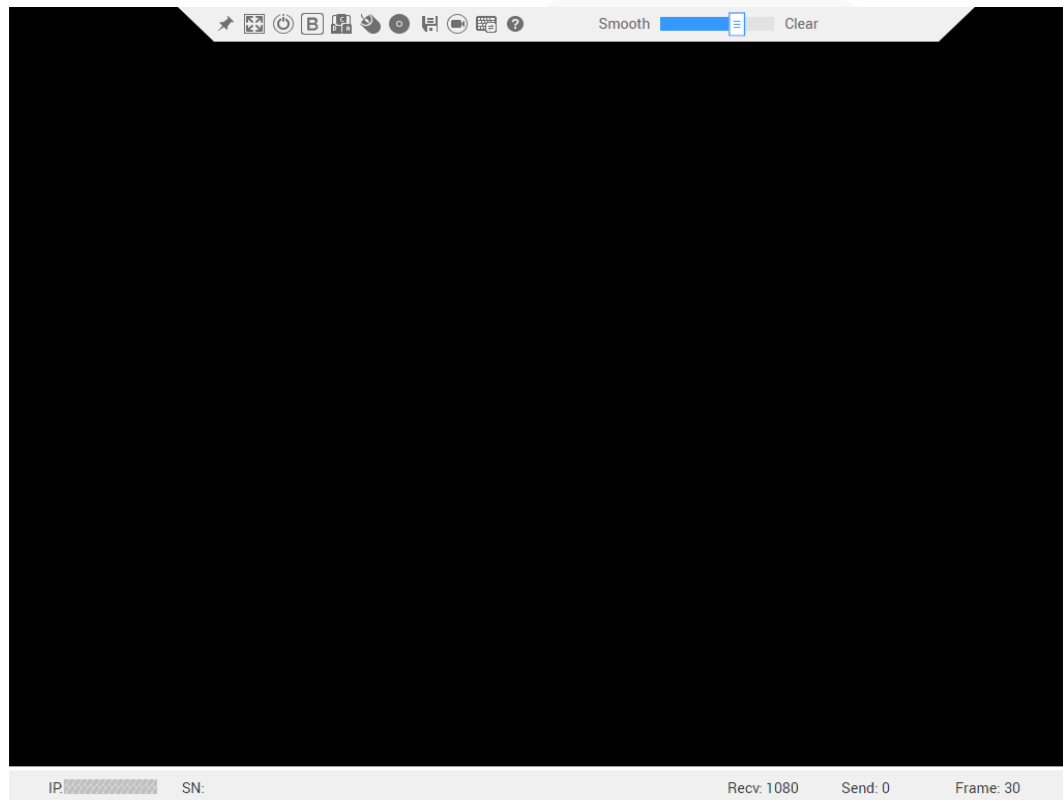


Figure 9-5 HTML5 Integrated Remote Console



----End

9.3.1.1.2 V600 and Later Versions

Scenario

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

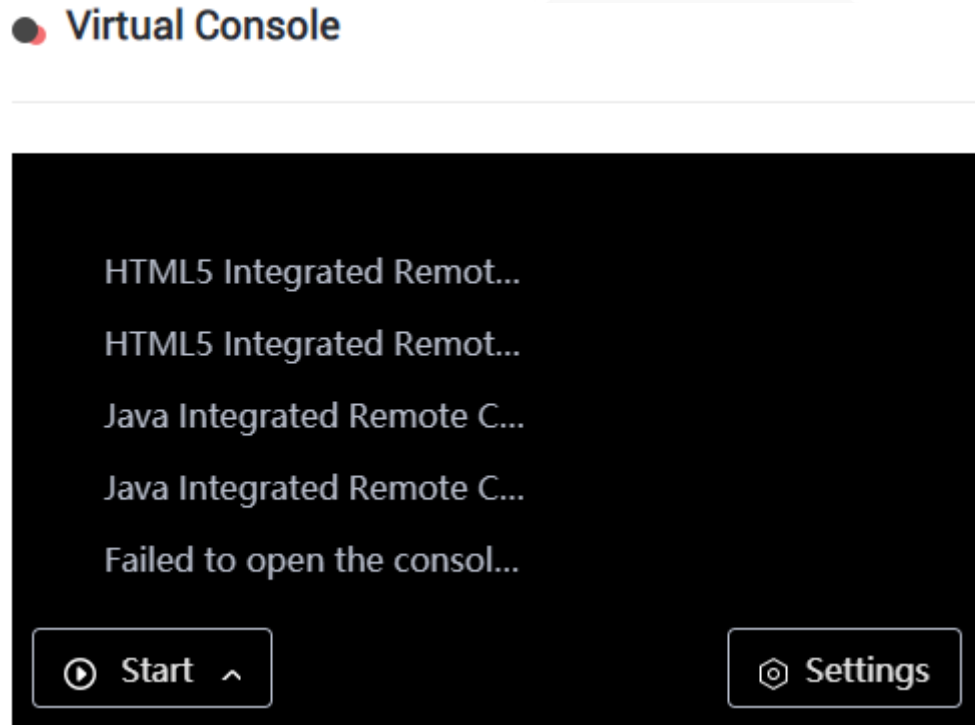
Procedure

Step 1 Log in to the iBMC WebUI.

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

Step 2 Click **Start** in the **Virtual Console** area in the lower right corner of the **Home** page.

Figure 9-6 Virtual Console



Step 3 Click an Integrated Remote Console.

NOTE

- **Java Integrated Remote Console (Private):** allows only one local user or VNC user to access and perform operations on the server through the iBMC.
- **Java Integrated Remote Console (Shared):** allows two local users or up to five VNC users to simultaneously access and perform operations on the server through the iBMC. The users can see each other's operations.
- **HTML5 Integrated Remote Console (Private):** allows only one local user or VNC user to access and perform operations on the server through the iBMC.
- **HTML5 Integrated Remote Console (Shared):** allows two local users or up to five VNC users to simultaneously access and perform operations on the server through the iBMC. The users can see each other's operations.
- 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

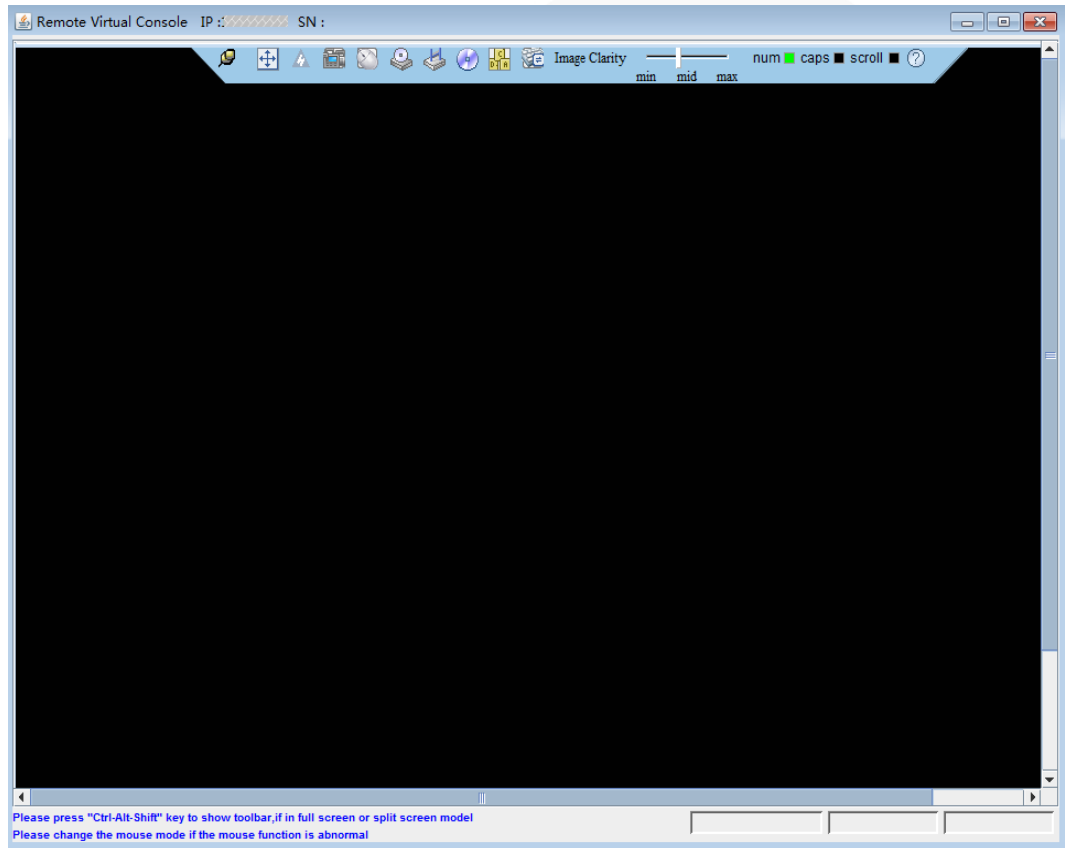
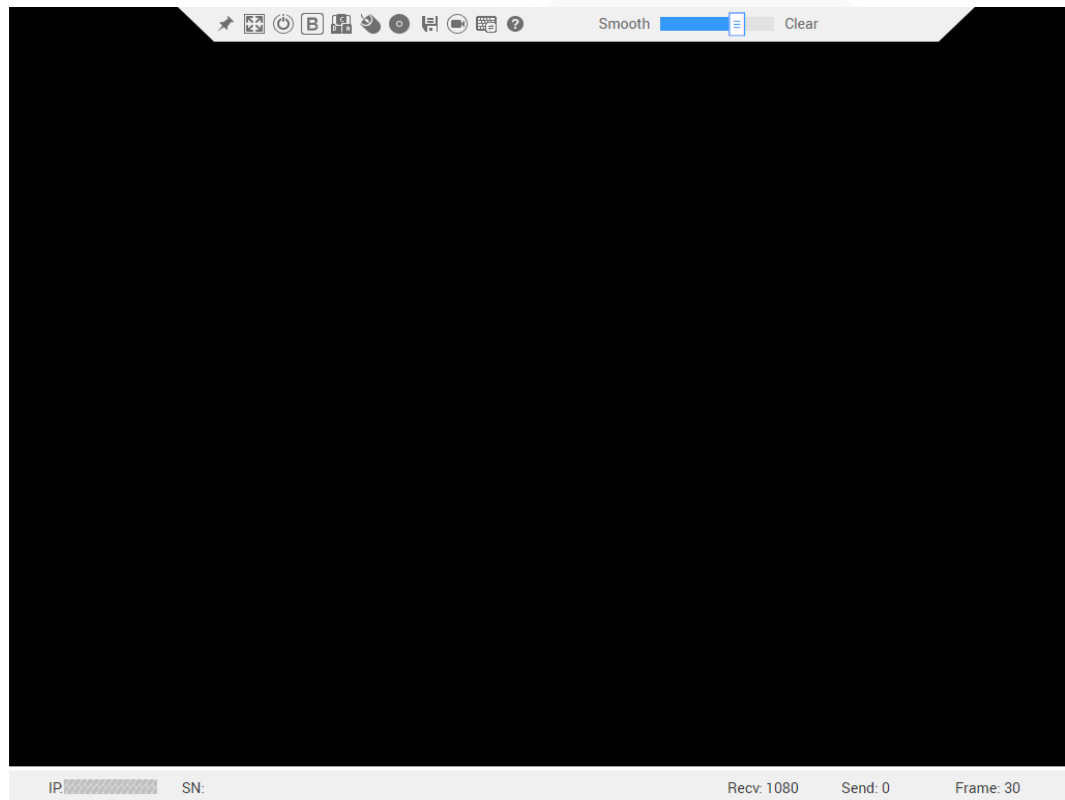


Figure 9-8 HTML5 Integrated Remote Console



----End

9.3.2 Logging In to a Server Using the Independent Remote Console

Scenario

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

NOTE

If the client OS and iBMC versions are compatible with the Independent Remote Console, the Independent Remote Console provides easier operations than the Remote Virtual Console.

9.3.2.1 Versions Earlier Than V600

9.3.2.1.1 Windows

The following Windows OS versions are supported:

- Windows 7 32-bit or 64-bit
- Windows 8 32-bit or 64-bit
- Windows 10 32-bit or 64-bit
- Windows Server 2008 R2 32-bit or 64-bit

- Windows Server 2012 64-bit

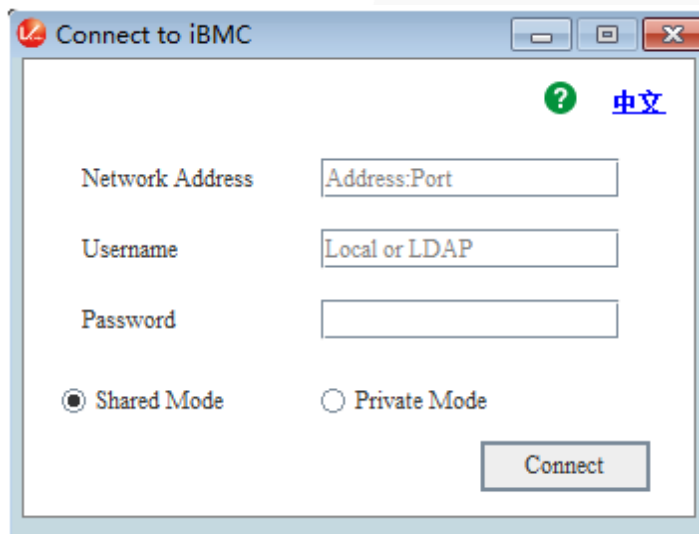
Procedure

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**.

Open the Independent Remote Console.

Figure 9-9 Independent Remote Console login page



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

NOTE

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- iBMC V228 and earlier versions support only local users. iBMC V228 and later versions support local users and LDAP domain users.
- In versions earlier than iBMC V228, the port number is the RMCP+ service port number. In iBMC V228 and later versions, the port number is the HTTPS service port number.
- The default port number can be omitted.

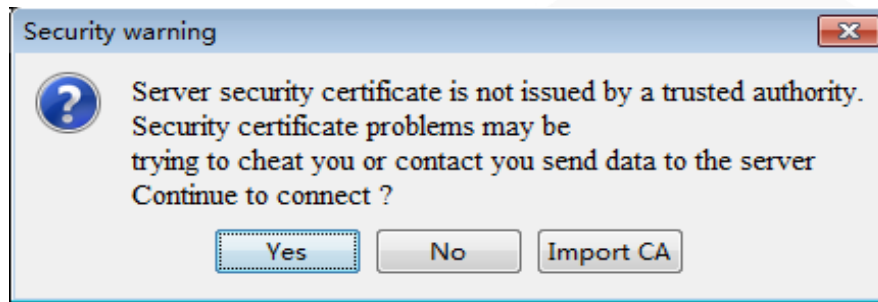
Step 4 Select a login mode.

- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.
- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 5 Click **Connect**.

A security warning is displayed.

Figure 9-10 Security warning



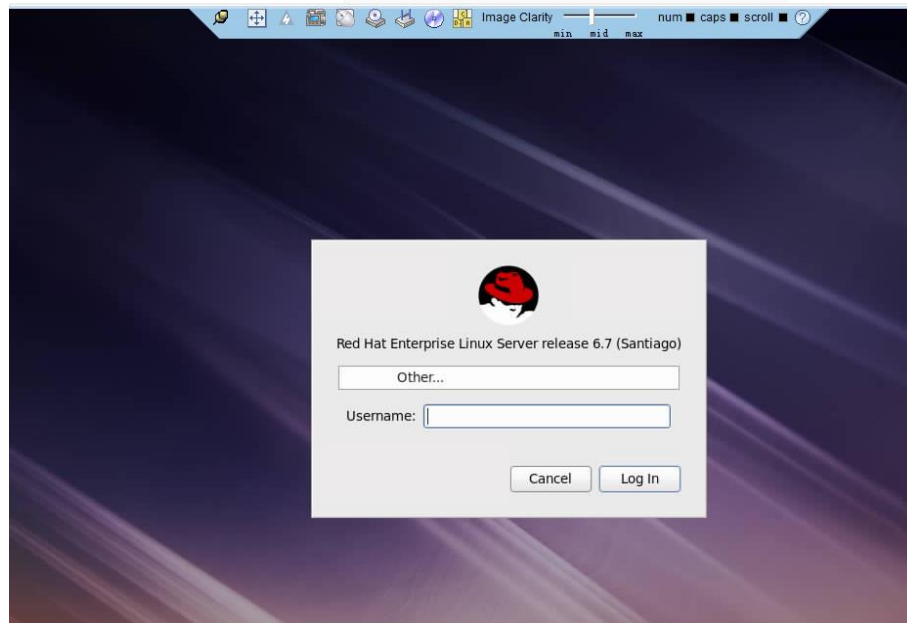
Step 6 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-11 Real-time desktop



----End

9.3.2.1.2 Ubuntu

The following Ubuntu OS versions are supported:

- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS

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 Grant the execute permission on the Independent Remote Console.

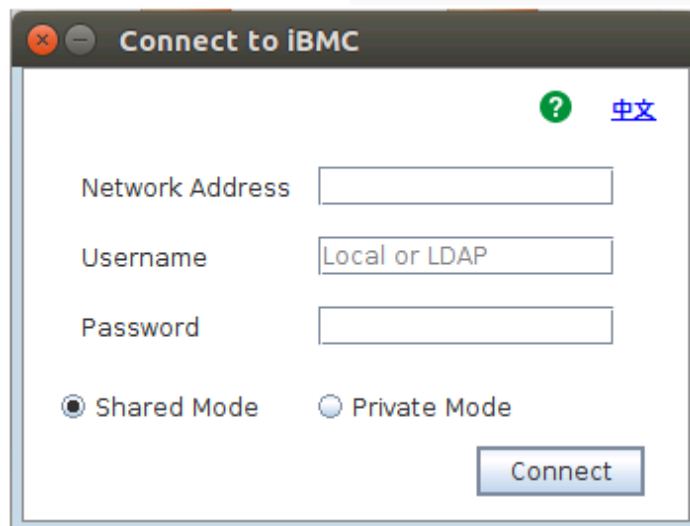
```
chmod 777 KVM.sh
```

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

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- iBMC V228 and earlier versions support only local users. iBMC V228 and later versions support local users and LDAP domain users.
- In versions earlier than iBMC V228, the port number is the RMCP+ service port number. In iBMC V228 and later versions, the port number is the HTTPS service port number.
- The default port number can be omitted.

Step 6 Select a login mode.

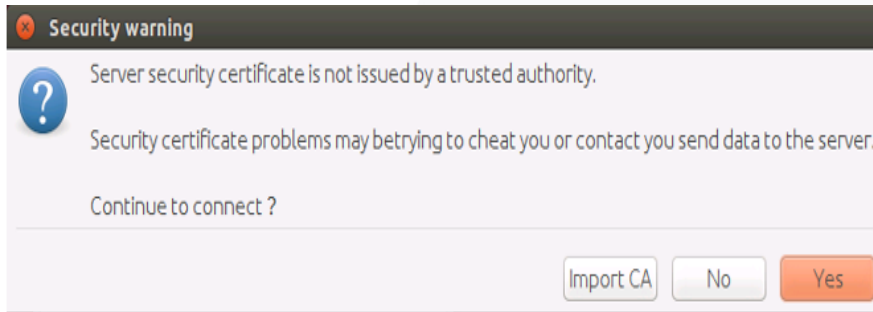
- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.

- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-13 Security warning



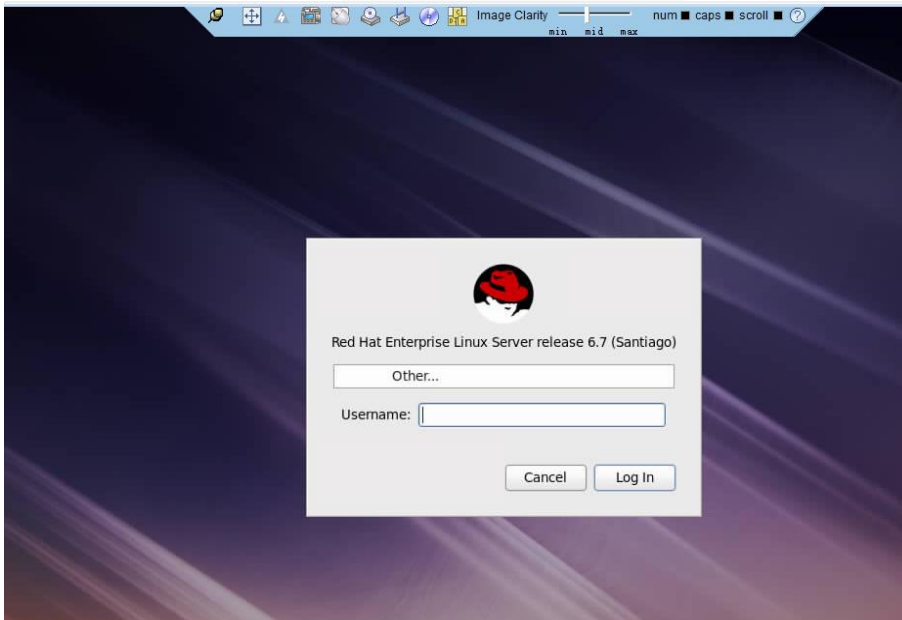
Step 8 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-14 Real-time desktop



----End

9.3.2.1.3 Mac

The following macOS version is supported:

- macOS X El Capitan

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 Grant the execute permission on the Independent Remote Console.

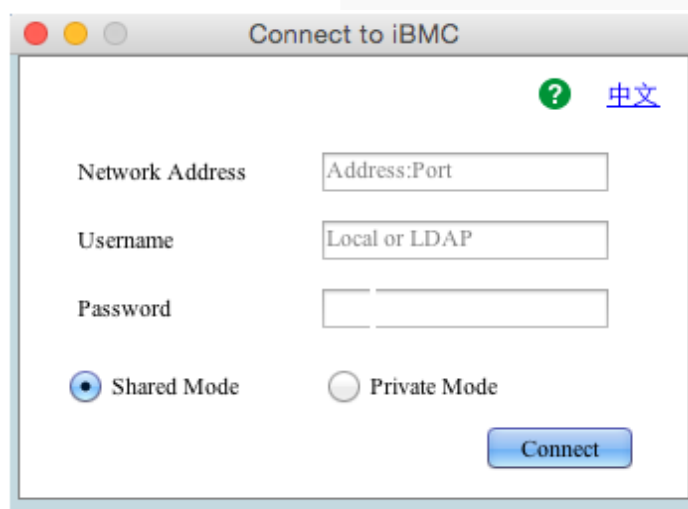
```
chmod 777 KVM.sh
```

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

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- iBMC V228 and earlier versions support only local users. iBMC V228 and later versions support local users and LDAP domain users.
- In versions earlier than iBMC V228, the port number is the RMCP+ service port number. In iBMC V228 and later versions, the port number is the HTTPS service port number.

- The default port number can be omitted.

Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.
- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-16 Security warning



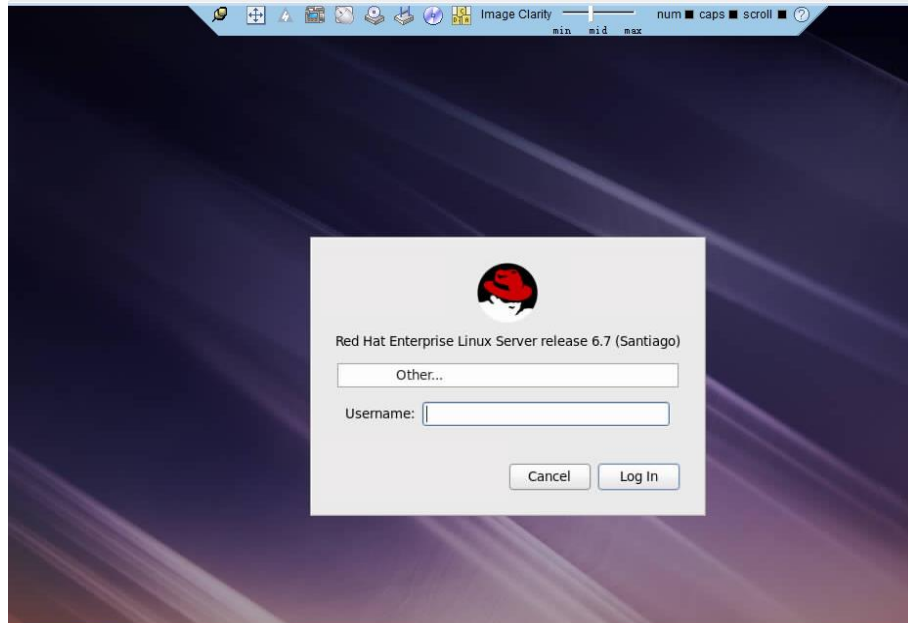
Step 8 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-17 Real-time desktop



----End

9.3.2.1.4 Red Hat

The following Red Hat OS versions are supported:

- RHEL 6.9
- RHEL 7.3

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 Grant the execute permission 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

The screenshot shows a 'Start Connection' dialog box. At the top right, there is a language dropdown menu currently set to 'English' and a help icon (?). Below this, there are three input fields: 'Network Address', 'Username', and 'Password'. Each of the first two fields has an information icon (!) to its right. At the bottom left, there are two radio buttons: 'Shared Mode' (which is selected) and 'Private Mode'. A 'Connect' button is located at the bottom right of the dialog box.

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

NOTE

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- iBMC V228 and earlier versions support only local users. iBMC V228 and later versions support local users and LDAP domain users.
- In versions earlier than iBMC V228, the port number is the RMCP+ service port number. In iBMC V228 and later versions, the port number is the HTTPS service port number.
- The default port number can be omitted.

Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.
- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-19 Security warning



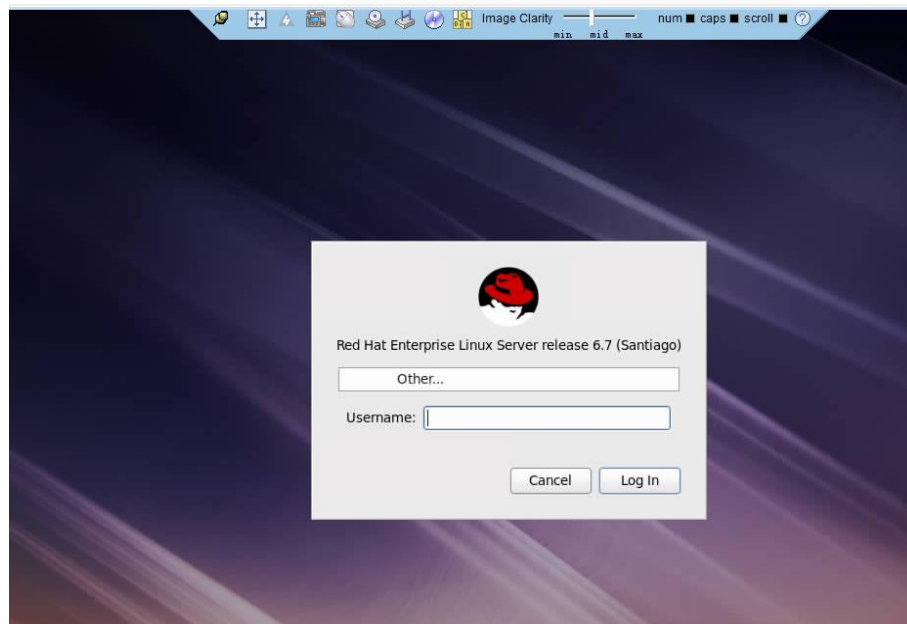
Step 8 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-20 Real-time desktop



----End

9.3.2.2 V600 and Later Versions

9.3.2.2.1 Windows

The following Windows OS versions are supported:

- Windows 7 32-bit or 64-bit
- Windows 8 32-bit or 64-bit
- Windows 10 32-bit or 64-bit
- Windows Server 2008 R2 32-bit or 64-bit
- Windows Server 2012 64-bit

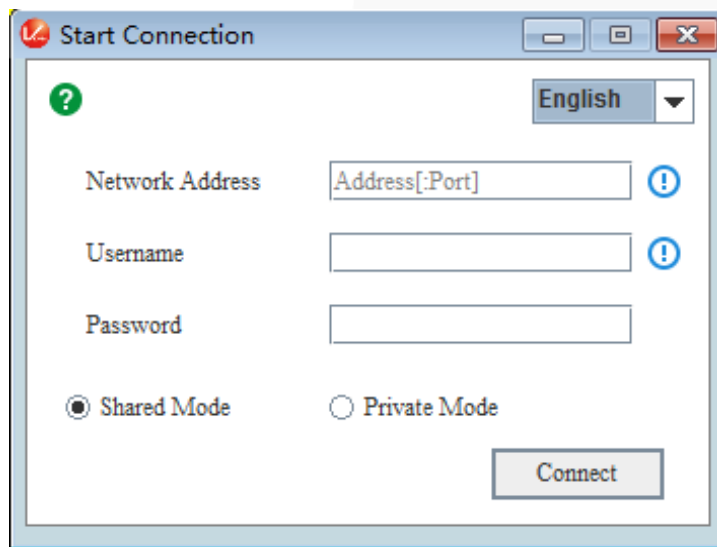
Procedure

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**.

Open the Independent Remote Console.

Figure 9-21 Independent Remote Console login page



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

NOTE

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- Local and LDAP domain users are supported.
- The preferred port number is the HTTPS service port number, and then the RMCP+ service port number.
- The default port number can be omitted.

Step 4 Select a login mode.

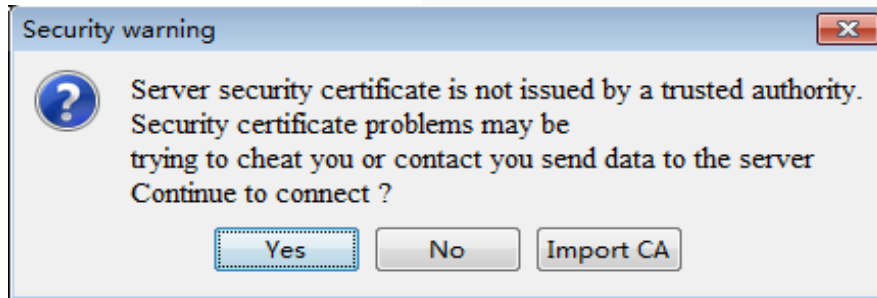
- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.

- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 5 Click **Connect**.

A security warning is displayed.

Figure 9-22 Security warning



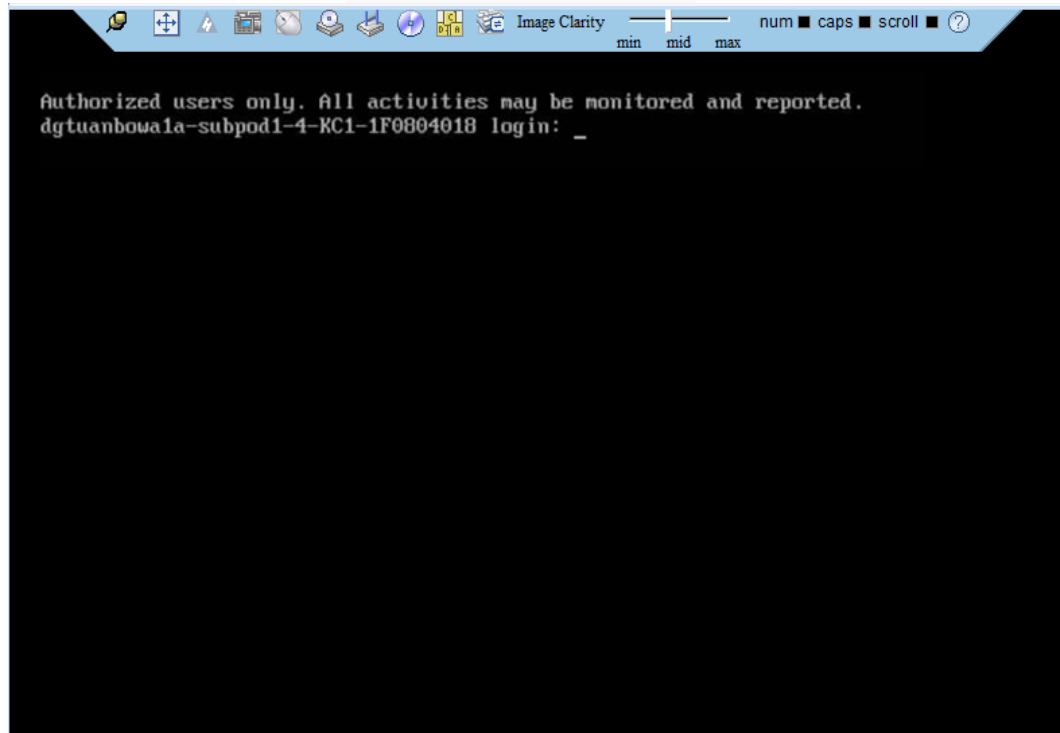
Step 6 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-23 Real-time desktop



----End

9.3.2.2.2 Ubuntu

The following Ubuntu OS versions are supported:

- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS

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 Grant the execute permission on the Independent Remote Console.

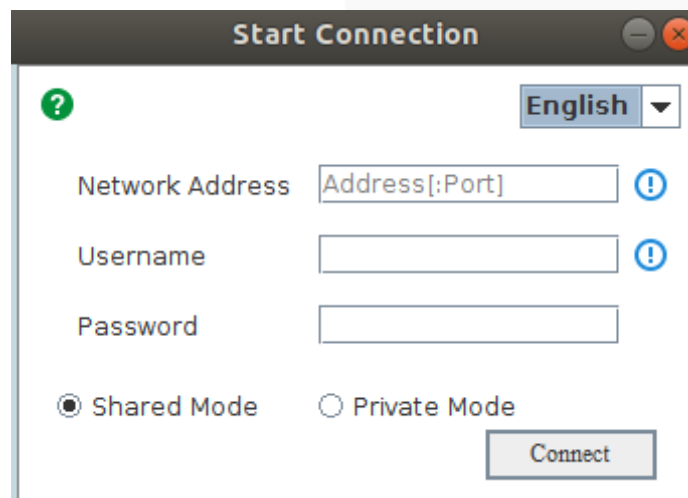
```
chmod 777 KVM.sh
```

Step 4 Open the Independent Remote Console.

```
./KVM.sh
```

The Independent Remote Console login page is displayed.

Figure 9-24 Independent Remote Console login page



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

NOTE

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- Local and LDAP domain users are supported.

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

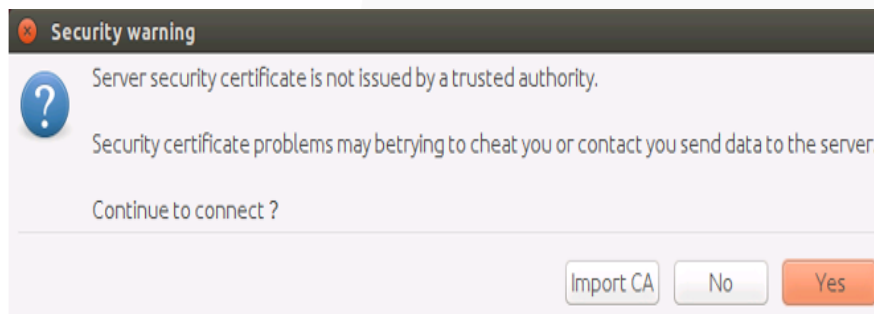
Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.
- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-25 Security warning



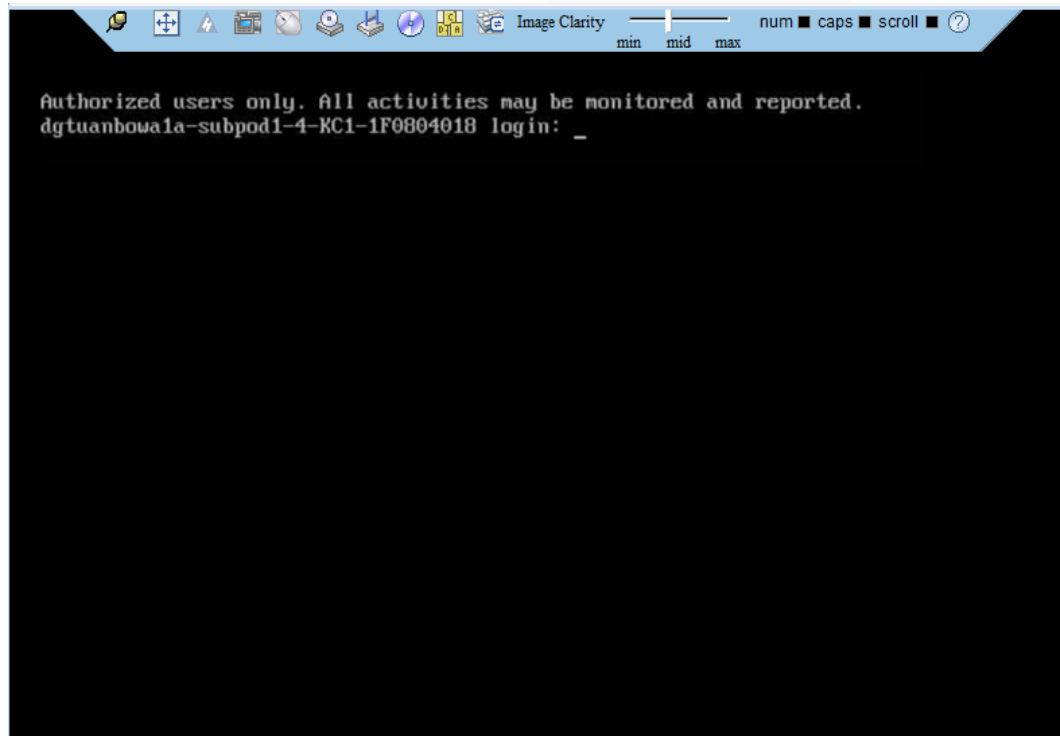
Step 8 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-26 Real-time desktop



----End

9.3.2.2.3 Mac

The following macOS version is supported:

- macOS X El Capitan

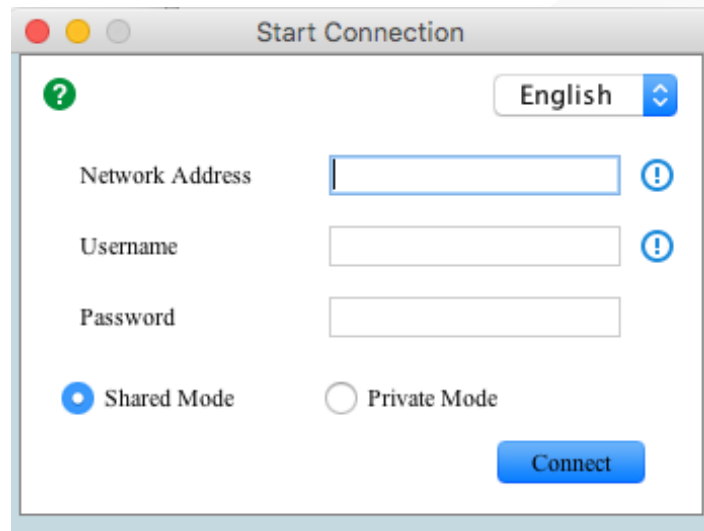
Procedure

- 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** Grant the execute permission 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 9-27 Independent Remote Console login page



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

NOTE

- 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, **[fc::64]:444** or **192.168.100.1:444**.
- *iBMC domain name address:Port number*
- Local and LDAP domain users are supported.
- The preferred port number is the HTTPS service port number, and then the RMCP+ service port number.
- The default port number can be omitted.

Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.
- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-28 Security warning



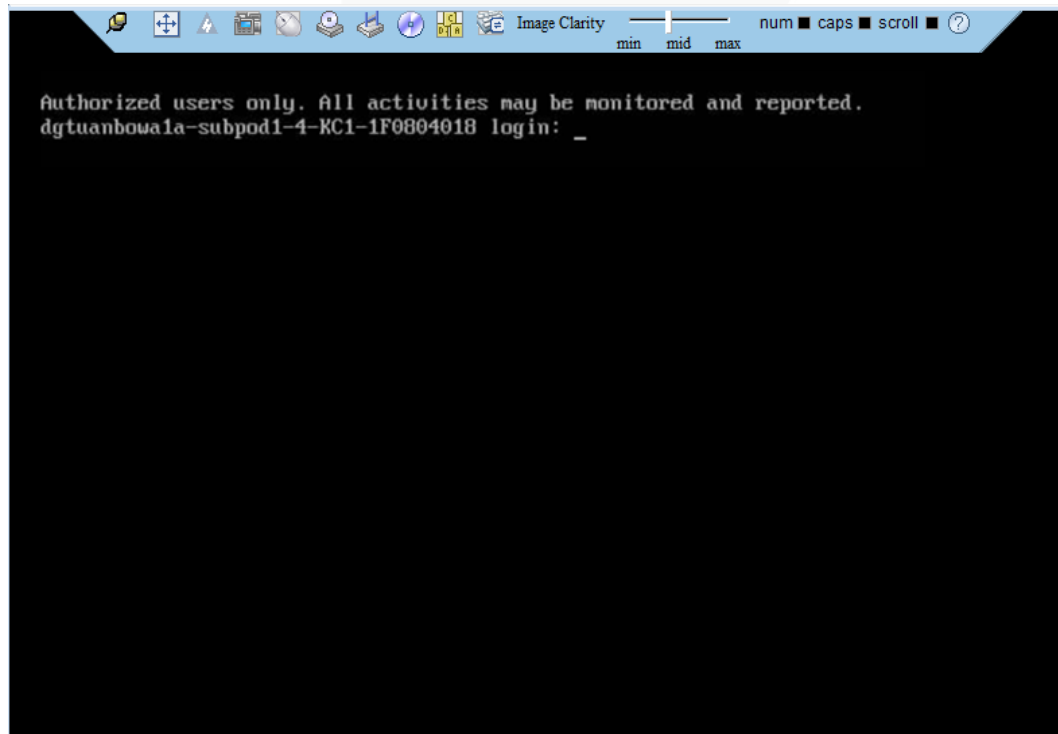
Step 8 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-29 Real-time desktop



----End

9.3.2.2.4 Red Hat

The following Red Hat OS versions are supported:

- RHEL 6.9
- RHEL 7.3

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 Grant the execute permission on the Independent Remote Console.

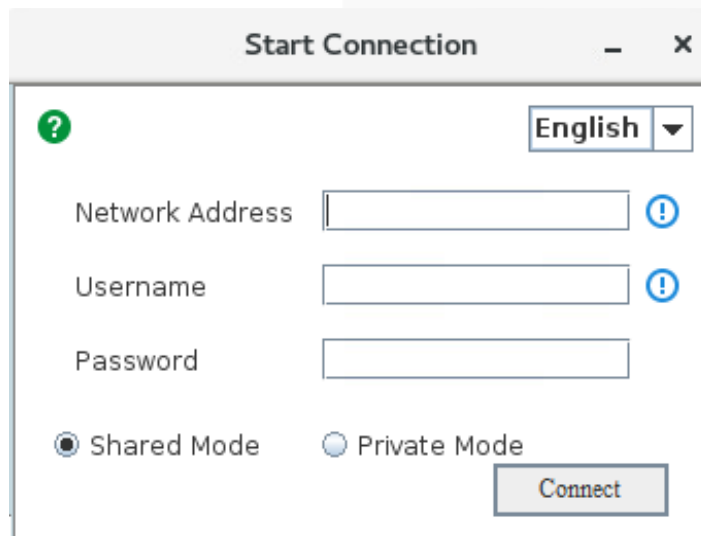
chmod 777 KVM.sh

Step 4 Open the Independent Remote Console.

./KVM.sh

The Independent Remote Console login page is displayed.

Figure 9-30 Independent Remote Console login page



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

NOTE

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

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

Step 6 Select a login mode.

- **Shared Mode:** allows two users to access and manage the server or node at the same time. Each user can view the operations performed by the other user.
- **Private Mode:** allows only one user to access and manage the server or node at a time.

Step 7 Click **Connect**.

A security warning is displayed.

Figure 9-31 Security warning



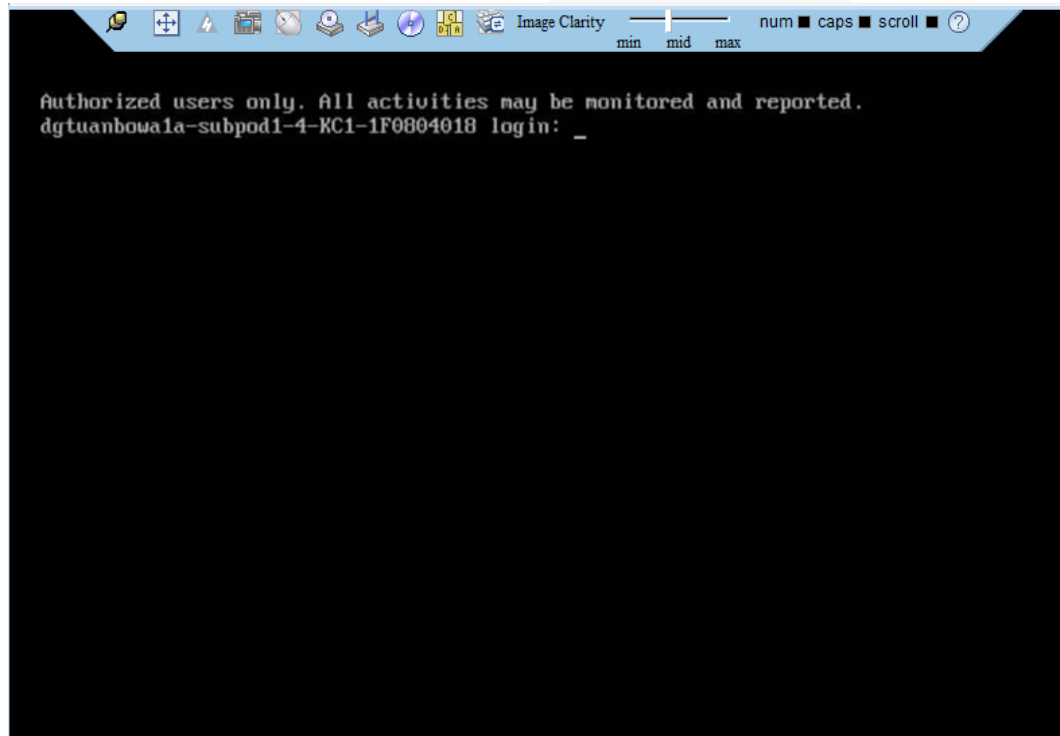
Step 8 Click **Yes**.

NOTE

- Click **No** to return to the login page.
- 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.

The server desktop is displayed.

Figure 9-32 Real-time desktop



----End

9.4 Logging In to the CLI

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

Scenarios

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

NOTE

- You can obtain the PuTTY software from the chiark home page.
- You are advised to use PuTTY of the latest version. PuTTY of an earlier version may cause login failures.

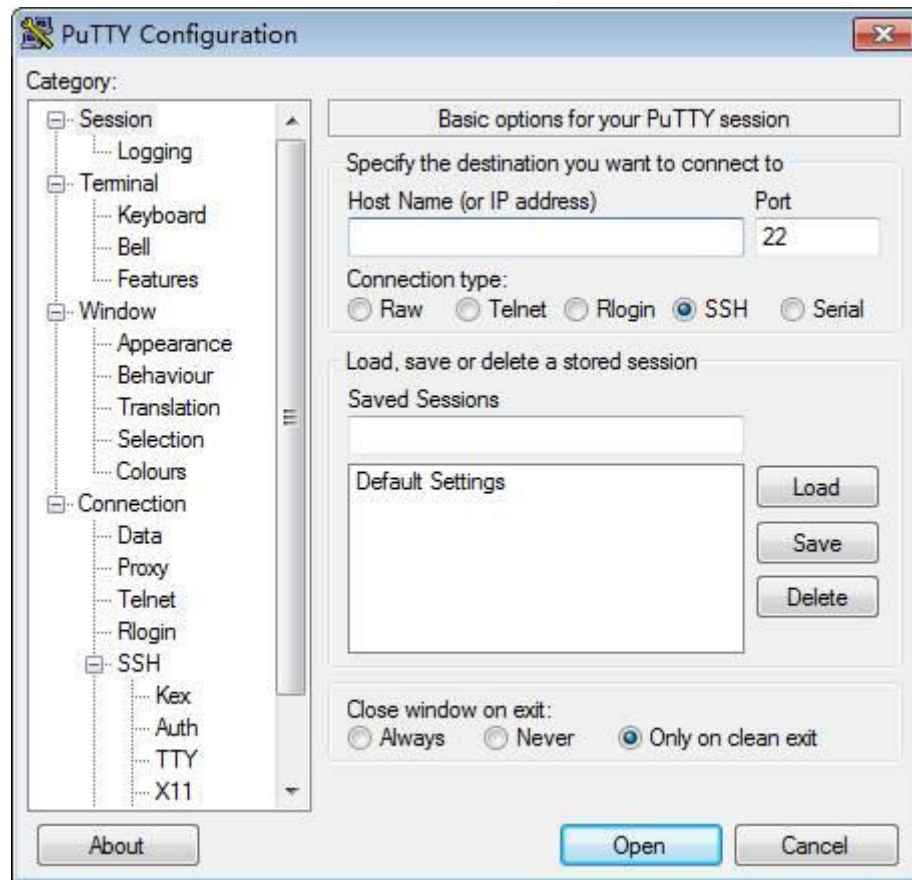
Procedure

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 9-33 PuTTY Configuration



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

Step 4 Set the login parameters.

The parameters are described as follows:

- **Host Name (or IP address):** Enter the IP address of the server to be accessed, for example, **191.100.34.32**.
- **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** screen is displayed. Then the message "login as:" is displayed, prompting you to enter a user name.

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 user name is displayed on the left of the prompt.

----End

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

Scenarios

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

- You can obtain the PuTTY software from the [chiark home page](#).
- 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 the 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 in COM n indicates a serial port number, and its value is an integer.

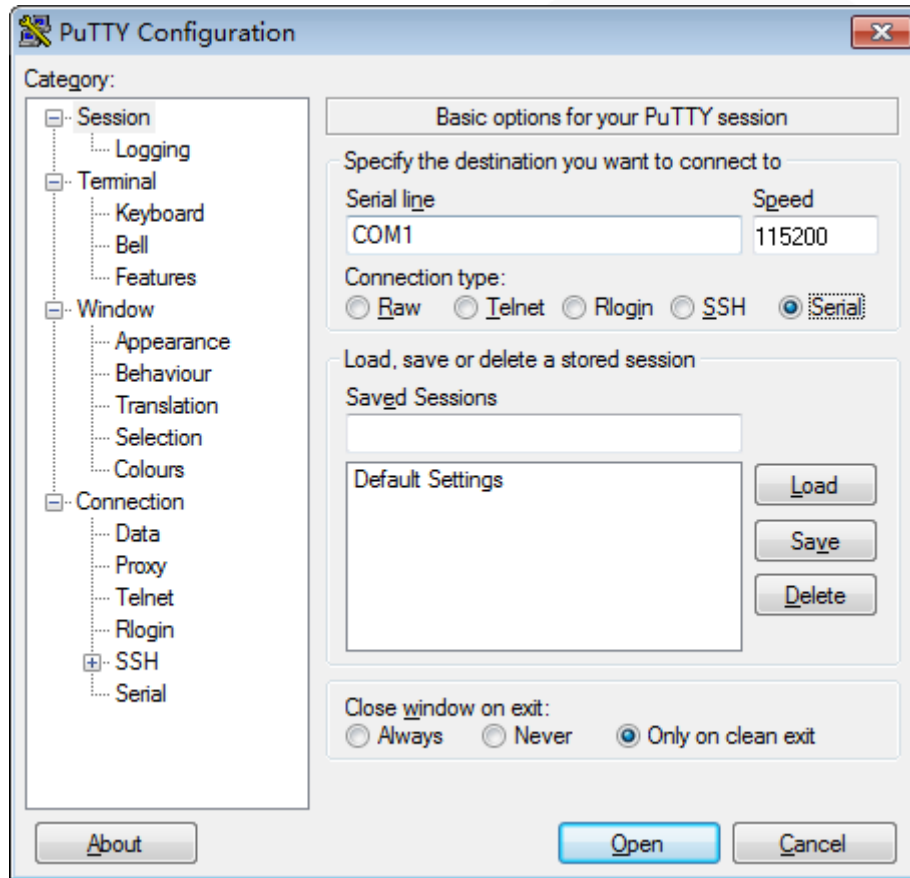
Step 4 In the navigation tree, choose **Session**.

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 9-34 PuTTY Configuration



Step 6 Click **Open**.

The **PuTTY** screen is displayed. Then the message "login as:" is displayed, prompting you to enter a user name.

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 user name is displayed on the left of the prompt.

----End

9.5 Managing VMD

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

- To use the VMD function, the iBMC version must be V320 or later, and the BIOS version must be V110 or later. Otherwise, the iBMC WebUI may fail to display NVMe drive information and the fan speed cannot be adjusted based on the NVMe drive temperature, affecting the heat dissipation of NVMe drives.

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

9.5.1 Enabling VMD

Procedure

- Step 1** Access 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 **Auto** and press **Enter**.
- Step 8** Press **F10**.
The **Save Changes&Exit** dialog box is displayed.
- Step 9** Select **Yes** and press **Enter** to save the settings.
The server automatically restarts for the settings to take effect.
----End

9.5.2 Disabling VMD

Procedure

- Step 1** Access 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**.
The **Save Changes&Exit** dialog box is displayed.
- Step 9** Select **Yes** and press **Enter** to save the settings.
The server automatically restarts for the settings to take effect.

----End

9.6 Accessing the BIOS

9.6.1 Accessing the BIOS (V3XX or Earlier)

Procedure

Step 1 Log in to the desktop of the server.

For details, see 9.3 Logging In to the Desktop of a Server.

Step 2 On the Remote Virtual Console, click  on the menu bar.

Step 3 Choose **Forced System Reset** or **Forced Power Cycle**.

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

NOTICE

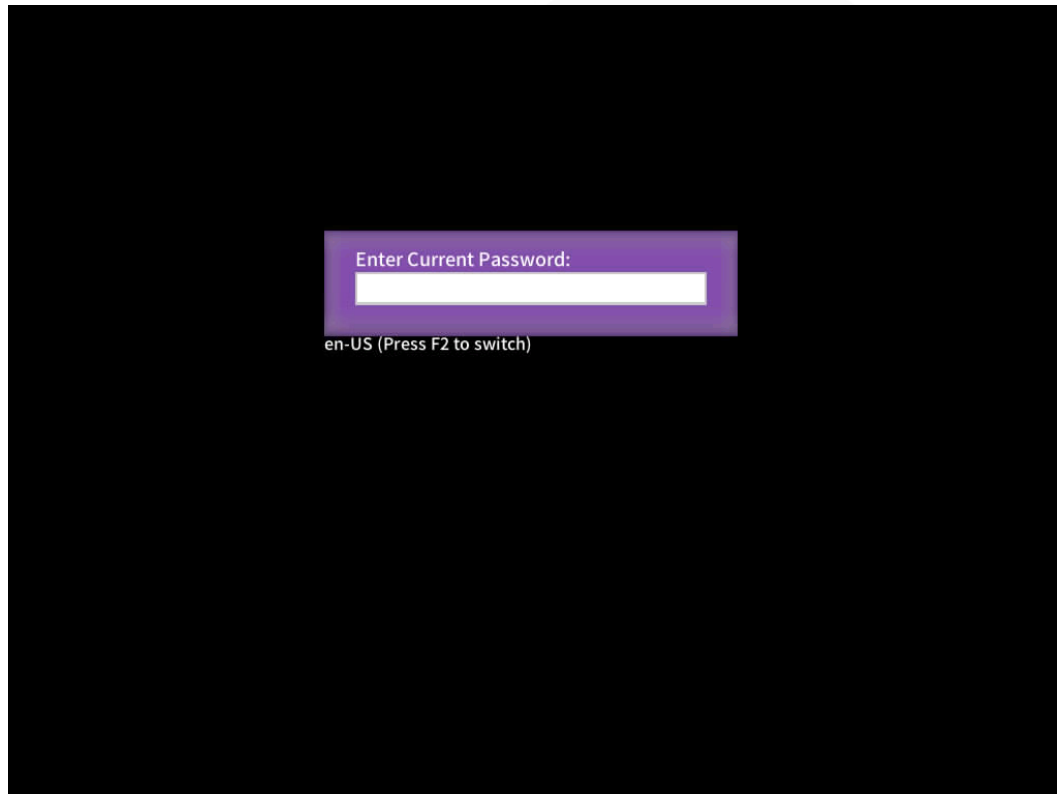
- A forced restart or power cycle may cause data loss or program damage.
 - Before performing a forced restart or power cycle, ensure that no service interruption risk exists.
-

Step 4 Click **Yes**.

The server starts to be forcibly restarted or power cycled.

Step 5 During the restart, press **Delete** or **F4** when the information shown in Figure 9-35 is displayed.

Figure 9-36 Entering the BIOS password



Step 6 Enter the BIOS password.

NOTE

- The default BIOS password is **Admin@9000**.
- Press **F2** to alternate between the English (US), French, and Japanese keyboards.
- For security purposes, change the administrator password periodically.
- The system will be locked if an incorrect password is entered three consecutive times. You can restart the server to unlock it.

The **Main** screen of the Setup Utility program is displayed.

----End

9.6.2 Accessing the BIOS (V6XX or Later)

Procedure

Step 1 Log in to the desktop of the server.

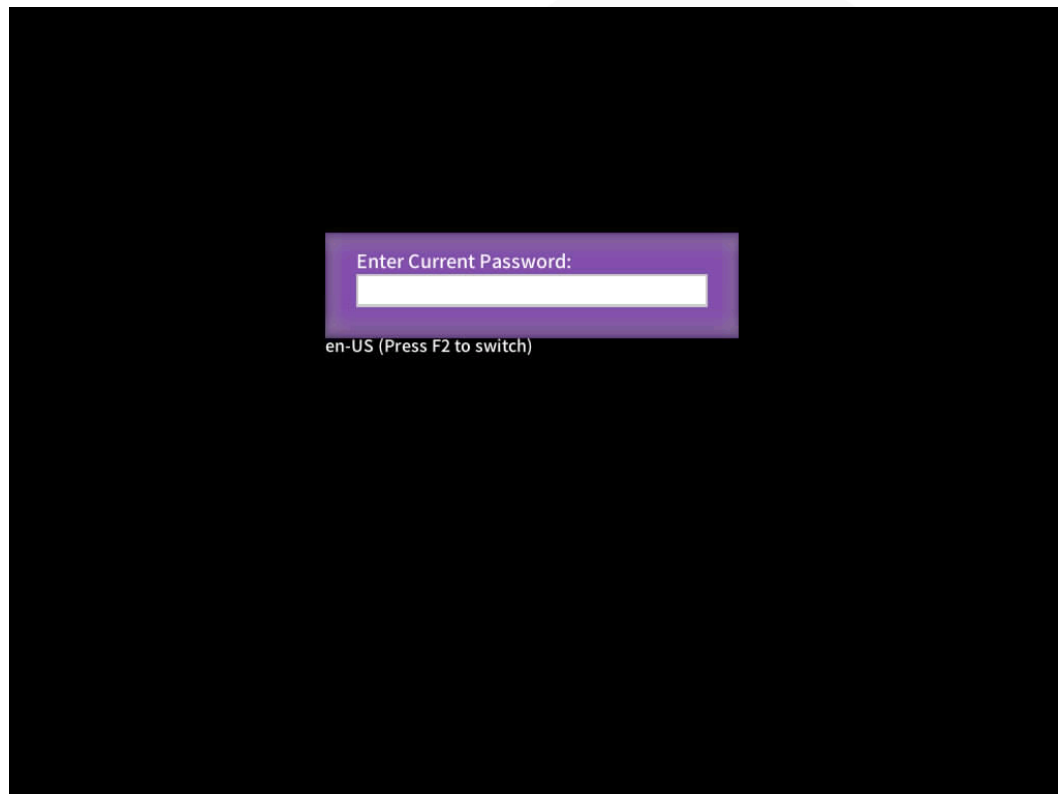
For details, see 9.3 Logging In to the Desktop of a Server.

Step 2 On the Remote Virtual Console, click  on the menu bar.

Step 3 Choose **Forced System Reset** or **Forced Power Cycle**.

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

Figure 9-38 Entering the BIOS password



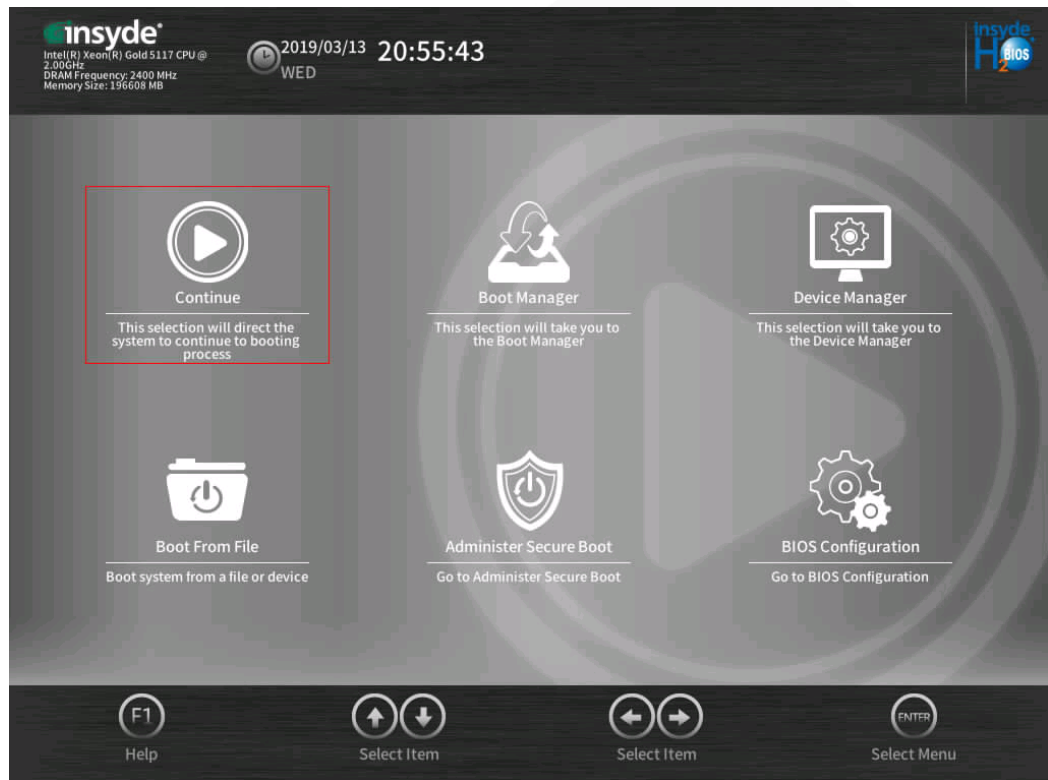
Step 6 Enter the BIOS password.

NOTE

- The default BIOS password is **Admin@9000**.
- 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. You can restart the server to unlock it.

The **Front Page** screen is displayed.

Figure 9-39 Using administrator password to log in to the Front Page



NOTE

- When you log in to the system using a common user password, only the **Continue** and **BIOS Configuration** menu options are displayed on the **Front Page** screen.
- On the **BIOS Configuration** screen, common users can only view menu options, set or change their own passwords, and save and exit. **Set User Password** in the **Security** screen and **Save Changes & Exit** in the **Exit** screen can be configured but other options are dimmed and cannot be edited. You can press **F10** to save and exit, but the function of **F9** (restoring default settings) is unavailable.

Step 7 Select **BIOS Configuration** by pressing arrow keys.

The **Main** screen is displayed.

----End

10 More Information

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

10.1 Technical Support

ZOOMtecnologia 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

Table 10-1 provides common information about servers.

Table 10-1 Product information

Item	Description	How to Obtain
Server product documentation	Server user guide, which provides information about the structure, specifications, and installation of the server.	Visit Technical Support > Documentation > View ALL , select a product model, and view the Documentation tab page.
Computing Product Compatibility Checker	A tool used to query the OSs, parts, and peripherals compatible with a server.	Visit Compatibility Checker .

10.3 Maintenance Tools

Table 10-3 lists the software tools required for routine maintenance of servers.

Table 10-3 Software tools for routine maintenance

Tool	Server Model and Software Version	Description
FusionServer Tools	See <i>FusionServer Tools User Guide</i> .	FusionServer Tools contains tools used for batch deployment, maintenance, and upgrade of servers. Download link: FusionServer 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
FusionDirector	See the <i>FusionDirector Specifications List</i> .	FusionDirector is the management software for intelligent O&M over the entire server lifecycle. It provides intelligent functions to manage deployment, assets, versions, faults, and energy efficiency. Download link: FusionDirector

11 Software and Configuration Utilities

11.1 iBMC

11.2 BIOS

11.1 iBMC

The intelligent baseboard management controller (iBMC) complies with IPMI 2.0 and SNMP standards and supports various functions, including KVM redirection, text console redirection, remote virtual media, and highly reliable hardware monitoring and management.

The iBMC offers the following features:

- Multiple management interfaces for system integration
The iBMC provides IPMI, command-line interface (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.
- Web-based user interface (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 dynamic power saving to reduce operational expenditure (OPEX).

For more information about the iBMC, see the [FusionServer Rack Server iBMC User Guide](#).

11.2 BIOS

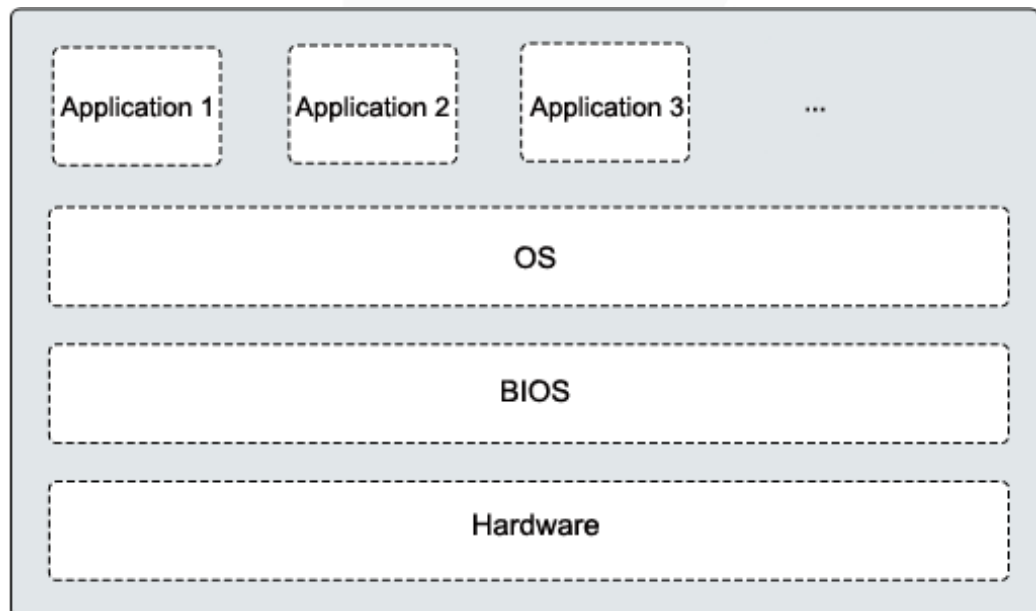
The basic input/output system (BIOS) is the most basic software loaded on a computer hardware system. The BIOS provides an abstraction layer between the computer hardware and the OS. It performs hardware initialization during the boot process and provides runtime services for the OS and programs.

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 features, such as advanced configuration and power interface (ACPI) and hot swap.

Purley-based servers are developed based on Insyde code base. They provide a variety of in-band and out-of-band configuration functions as well as high scalability, and support customization.

For more information about the BIOS, see the [FusionServer Server Purley 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 Example SN



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 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 (product name) of the board.

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)
8 x 2.5" SAS/SATA drive configuration	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> Options supported: processors of up to 165 W Options not supported: GPU cards 	<ul style="list-style-type: none"> Options supported: processors of up to 140 W Options not supported: <ul style="list-style-type: none"> PCIe SSD cards NVMe drives GPU cards
24 x 2.5" SAS/SATA drive configuration	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> Options supported: processors of up to 165 W Options not supported: <ul style="list-style-type: none"> PCIe SSD cards NVMe SSDs GPU cards 	<ul style="list-style-type: none"> Not supported
24 x 2.5" (16 x SAS/SATA + 8 x NVMe) drive configuration	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> Options supported: processors of up to 140 	<ul style="list-style-type: none"> Not supported

Configuration	Max. 30°C (86°F)	Max. 35°C (95°F)	Max. 40°C (104°F)	Max. 45°C (113°F)
			W • Options not supported: • PCIe SSD cards • NVMe drives • GPU cards	
24 x 2.5" NVMe drive configuration	<ul style="list-style-type: none"> Options supported: processors of up to 165 W 	<ul style="list-style-type: none"> Not supported 	<ul style="list-style-type: none"> Not supported 	<ul style="list-style-type: none"> Not supported
25 x 2.5" SAS/SATA drive configuration	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> All options supported 	<ul style="list-style-type: none"> Options supported: processors of up to 165 W Options not supported: PCIe SSD cards NVMe drives GPU cards 	<ul style="list-style-type: none"> Not supported

 **NOTE**

- If a single fan is faulty, the maximum operating temperature is 5°C (9°F) lower than the rated value.
- If P4/T4 GPU cards are configured:
- All configurations except 24 x 2.5" NVMe drive configuration are supported.
- If a P4/T4 GPU card is installed in slot 5 or 10, the maximum operating temperature supported is 30°C (86°F).
- If a P4/T4 GPU card is installed in slot 1, the maximum operating temperature supported is 35°C (95°F).

A.3 Nameplate

Certified Model	Usage Restrictions
H24H-05	Global
H24H-05-I20	India only

A.4 RAS Features

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

For details about how to configure these features, see the [FusionServer Server Purley Platform BIOS Parameter Reference](#).

Table A-3 Supported RAS features

Module	Feature	Description
CPU	Corrected Machine Check Interrupt (CMCI)	Corrects error-triggered interrupts.
Memory	Failed DIMM Isolation	Identifies faulty DIMMs to facilitate isolation and replacement of the faulty DIMMs.
	Memory Thermal Throttling	Automatically adjusts the memory temperature to prevent the memory from being damaged due to overheat.
	Rank Sparing	Uses some memory ranks for backup to prevent the system from breaking down due to uncorrectable errors.
	Memory Address Parity Protection	Detects memory command and address errors.
	Memory Demand and Patrol Scrubbing	Corrects correctable errors upon detection. If these errors are not corrected in a timely manner, uncorrectable errors may occur.
	Memory Mirroring	Provides high reliability for the system via mirroring.
	Single Device Data Correction (SDDC)	Corrects single-chip multi-bit errors to improve memory reliability.
	Device Tagging	Degrades and rectifies memory faults to improve memory availability.
	Data Scrambling	Optimizes data flow distribution to reduce the error probability and improve memory data flow reliability and address error detection.
PCIe	PCIe Advanced Error Reporting	Provides a PCIe advanced error reporting mechanism to improve server serviceability.
UPI	Intel UPI Link Level Retry	Provides a retry mechanism to improve the reliability of UPI links.
	Intel UPI Protocol Protection via CRC	Provides cyclic redundancy check (CRC) protection for UPI data packets to improve system reliability.
System	Core Disable For FRB (Fault	Isolates a faulty CPU core during startup to

Module	Feature	Description
	Resilient Boot)	improve system reliability and availability.
	Corrupt Data Containment Mode	Marks the memory storage unit when a data error occurs to limit the impact on the running program and improve system reliability.
	Socket disable for FRB (Fault Resilient Boot)	Isolates a faulty socket during the BIOS startup process to improve system reliability.
	Architected Error Records	With the features such as eMCA, the BIOS collects error information recorded in hardware registers in compliance with UEFI specifications, notifies the OS through the APEI interface of the ACPI, and locates the error unit, improving system availability.
	Error Injection Support	Implements fault injection to verify RAS features.
	Machine Check Architecture (MCA)	Provides a software repair function to rectify uncorrectable errors to improve system availability.
	Enhanced Machine Check Architecture (eMCA): Gen2	Improves system availability.
	OOB access to MCA registers	The out-of-band system can access MCA registers through the PECL. When a fatal error occurs in the system, the out-of-band system can collect onsite data to facilitate subsequent fault analysis and locating and improve system serviceability.
	BIOS Abstraction Layer for Error Handling	The BIOS processes errors and reports error information to the OS based on specifications, improving system serviceability.
	BIOS-based Predictive Failure Analysis (PFA)	The OS takes the lead. The BIOS provides information about physical memory error units. The OS tracks, predicts, and handles the errors.

A.5 Sensor List

Sensor	Description	Component
Inlet Temp	Air inlet temperature	Left mounting ear
Outlet Temp	Air outlet temperature	Component in position U60 on the mainboard.

Sensor	Description	Component
PCH Temp	PCH bridge temperature	Component in position U4014 on the mainboard.
CPUN Core Rem	CPU core temperature	CPU. <i>N</i> indicates the CPU number. The value ranges from 1 to 4 .
CPUN DTS	CPU DTS value	
CpuN Margin	CPU1 Margin temperature	
CPUN Prochot	CPU Prochot	
CPUN VDDQ Temp	CPU VDDQ temperature	<p>CPU 1: Components in positions U4333 and U4339 on the mainboard.</p> <p>CPU 2: Components in positions U4443 and U4447 on the mainboard.</p> <p>CPU 3: Components in positions U4351 and U4408 on the mainboard.</p> <p>CPU 4: Components in positions U4411 and U4414 on the mainboard.</p> <p><i>N</i> indicates the CPU number. The value ranges from 1 to 4.</p>
CPUN VRD Temp	CPU VRD temperature	<p>CPU 1: Component in position U4316 on the mainboard.</p> <p>CPU 2: Component in position U4430 on the mainboard.</p> <p>CPU 3: Component in position U4370 on the mainboard.</p> <p>CPU 4: Component in position U4401 on the mainboard.</p> <p><i>N</i> indicates the CPU number. The value ranges from 1 to 4.</p>
CPUN MEM Temp	CPU DIMM temperature	DIMMs of CPUN. <i>N</i> indicates the CPU number. The value ranges from 1 to 4 .
SSD DiskN Temp	SSD temperature	SSD. <i>N</i> indicates the physical drive slot number.
FAN/ F Speed	Fan speed sensor	Fan module. <i>N</i> indicates the

Sensor	Description	Component
FAN N R Speed		fan module ID. The value ranges from 1 to 4 .
Power	Server input power	Total PSU power.
Power N	PSU input power	PSU. N indicates the PSU number. The value is 1 or 2 .
CPUN Status	CPU status	CPU. N indicates the CPU number. The value ranges from 1 to 4 .
CPUN Memory	DIMM status	DIMMs of CPUN. N indicates the DIMM number. The value ranges from 1 to 4 .
PSN Fan Status	PSU fan status	PSU. N indicates the PSU number. The value is 1 or 2 .
PSN Temp Status	PSU presence	
PSN Status	PSU status	
Power Button	Power button status	Right mounting ear
UID Button	UID button status	
DISKN	Drive status	Drive. N indicates the physical drive slot number.
FAN N F Presence	Fan presence	Fan module. N indicates the fan module ID. The value ranges from 1 to 4 .
FAN N R Presence		
FAN N F Status	Fan status	
FAN N R Status		
RTC Battery	RTC battery status. An alarm is generated when the voltage is lower than 1 V.	CMOS battery
DIMMN	DIMM status	DIMM. N indicates the DIMM slot number.
PCH Status	PCH chip fault diagnosis health status	Component in position U4014 on the mainboard.
LCD Presence	LCD presence	LCD
LCD Status	LCD health status	
PS Redundancy	Redundancy failure due to PSU removal	PSU. N indicates the PSU number. The value is 1 or 2 .
PSN Inlet Temp	PSU air inlet temperature	
SYS 3.3V	Mainboard 3.3 V voltage	N/A

Sensor	Description	Component
SYS 5V	Mainboard 5.0 V voltage	N indicates the number of the component.
SYS 12V_1	Mainboard 12.0 V voltage (the first output 12 V voltage detection for soft-start (CPU1 +PCIe Slot))	
SYS 12V_2	Mainboard 12.0 V voltage (the second output 12 V voltage detection for soft-start (CPU2 + CPU3))	
SYS 12V_3	Mainboard 12.0 V voltage (the third output 12 V voltage detection for soft-start (CPU4 + fan module))	
SYS 12V_4	Mainboard 12.0 V voltage (the fourth output 12 V output voltage detection for soft-start (drive backplane module))	
SYS 12V_5	Mainboard 12.0 V voltage (the fourth output 12 V output voltage detection for soft-start (drive backplane module))	
Standby 5V	Mainboard standby 5.0 V voltage	
Standby 3.3V	Mainboard standby 3.3 V voltage	
Standby 1.8V	Mainboard standby 1.8 V voltage	
Standby 1.5V	Mainboard standby 1.5 V voltage	
CPUN VCore	1.8 V CPU voltage	
CPUN DDR VDDQ	CPU DIMM voltage	
CPUN DDR VDDQ2		
CPUN VSA	CPU VSA voltage	
CPUN VCCIO	CPU VCCIO voltage	
PCH VPVNN	PCH PVNN voltage	
PCH PRIM 1V05	PCH 1.05 V voltage	

Sensor	Description	Component
SSDN Temp	SSD temperature	
PwrOk Sig. Drop	Voltage dip status	
ACPI State	ACPI status	
SysFWProgress	Software process and system startup errors	
SysRestart	System restart causes	
Boot Error	Boot error	
Watchdog2	Watchdog	
Mngmnt Health	Management subsystem health status	
Riser1 Card	Entity presence	
SAS Cable	Entity presence	
PCIe RAIDN Temp	LSI SAS3508 RAID controller card temperature	
PCIe RAIDN Temp	Avago SAS3004 RAID controller card temperature	
M2 Temp(PCIeN)	Maximum temperature of all M.2 drives of the RAID controller card	
PCIe Status	PCIe status	
PwrOn TimeOut	Power-on timeout	
PwrCap Status	Power capping status	
HDD Backplane	Drive backplane entity presence	
HDD BP Status	Drive backplane health status	
PortN Link Down (N 1. 2. 3. 4)	Network port link status	
CPUN UPI Link (N 1. 2. 3.4)	CPU UPI link fault diagnosis health status	
System Notice	Hot restart reminder and fault diagnosis program information collection	
System Error	System suspension or restart. Check the background logs	

Sensor	Description	Component
BMC Boot Up	iBMC startup 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	
CPU Usage	CPU usage	
Memory Usage	Memory usage	
PCIeN Card BBU	BBU fault or low voltage on a PCIe card	
BMC Time Hopping	Time hopping	
NTP Sync Failed	NTP synchronization failure and recovery events	
Host Loss	System monitoring software (iBMA) link loss detection	
GPU _N Temp	GPU temperature	
PCIe _N Inlet Temp	PCIe smart card air inlet temperature	
PCIe _N Cpu Temp	PCIe smart card CPU temperature	
PCIe _N OP Temp	PCIe card optical module temperature	
PCIe _N NIC Temp	PCIe card chip temperature	
PS _N VIN	Input voltage	

B Glossary

B.1 A-E

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 10M and 100M 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 keyboard, video 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 one 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 or chassis. 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

C

CD	calendar day
CE	Conformite Europeenne
CIM	Common Information Model
CLI	command-line interface

D

DC	direct current
DCPMM	DC persistent memory module

DDR3	Double Data Rate 3
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

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

Q

QPI	Quick Path Interconnect
------------	-------------------------

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 Extensions

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.
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