

FusionServer Pro XH321 V5 Server Node

Maintenance and Service Guide

Issue	28
Date	2024-09-25



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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

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

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

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

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

About This Document

Purpose

This document describes the XH321 V5 in terms of its appearance, physical structure, product specifications, and methods for removing and installing components.

Intended Audience

This document is intended for:

- Huawei technical support engineers
- Technical support engineers from channel partners
- Enterprise administrators

Symbol Conventions

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

Symbol	Description
	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
	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.

Symbol	Description
 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	Release Date	Description
28	2024-09-25	This issue is the twenty-eighth official release. Added memory installation precautions in 8.4.14 Installing a Memory Module .
27	2024-05-15	This is the twenty-seventh official release. Added the description of importing and replacing certificates in 8.4.26 Installing the Mainboard and Server Node Case .
26	2024-01-12	This issue is the twenty-sixth official release. Modified 8.4.19 Removing a PCIe Card , 8.4.20 Installing a PCIe Card , and 10.2 Logging In to the iBMC WebUI .
25	2023-01-17	Modified 8.4.15 Removing the TPM and 8.4.16 Installing the TPM .
24	2022-10-13	Modified 10.3.2 Logging In to the Independent Remote Console .
23	2022-09-15	- Modified 3.3 Physical Specifications. - Modified 11.2 Product Information.
22	2022-06-30	Added the method of burning the original device serial number to the new mainboard.
21	2021-08-18	Updated content in sections about the LOM port and front panel.
20	2021-06-30	Added the firmware upgrade procedure in sections about the PCIe card and RAID controller card installation.
19	2021-06-01	Updated the storage temperature and humidity.
18	2021-04-12	This issue is the eighteenth official release.
17	2021-03-09	This issue is the seventeenth official release.

Issue	Release Date	Description
16	2021-01-21	This issue is the sixteenth official release.
15	2020-11-07	This issue is the fifteenth official release.
14	2020-09-03	This issue is the fourteenth official release.
13	2020-08-04	This issue is the thirteenth official release.
12	2020-06-05	This issue is the twelfth official release.
11	2020-05-11	This issue is the eleventh official release.
10	2020-04-20	This issue is the tenth official release.
09	2020-03-18	This issue is the ninth official release.
08	2020-03-05	This issue is the eighth official release.
07	2019-12-20	This issue is the seventh official release.
06	2019-08-10	Added the support for the Cascade Lake processors.
05	2019-01-04	- Added the description about X722 LOMs and PCIe slots. - Updated the technical specifications. - Added the description of the NC-SI feature.
04	2018-08-02	- Added the temperature restrictions when the M.2 is used with a PCIe RAID controller card. - Added information about the Avago SAS3004iMR RAID controller card.
03	2018-05-21	Refined the document for easy use.
02	2018-01-22	Optimized the processor installation procedure.
01	2017-12-29	This issue is the first official release.

Contents

About This Document..... iii

1 Overview..... 1

1.1 Product Introduction..... 1

1.2 Physical Structure..... 2

1.3 Logical Structure..... 3

2 Hardware Description..... 5

2.1 Front Panel..... 5

2.1.1 Appearance..... 5

2.1.2 Indicators and Buttons..... 6

2.1.3 Ports..... 8

2.1.4 Installation Positions..... 9

2.2 Processor..... 10

2.3 Memory..... 11

2.3.1 DDR4 Memory..... 11

2.3.1.1 Memory Identifier..... 11

2.3.1.2 Memory Subsystem Architecture..... 12

2.3.1.3 Memory Compatibility..... 13

2.3.1.4 DIMM Installation Rules..... 14

2.3.1.5 Memory Installation Positions..... 15

2.3.1.6 Memory Protection Technologies..... 16

2.4 Storage..... 17

2.4.1 Drive Configurations..... 17

2.4.2 Drive Numbering..... 17

2.4.3 RAID Controller Card..... 18

2.5 Network..... 18

2.5.1 LOMs..... 18

2.6 I/O Expansion..... 20

2.6.1 PCIe Cards..... 20

2.6.2 PCIe Slots..... 21

2.6.3 PCIe Slot Description..... 21

2.7 Boards..... 21

2.7.1 Mainboard..... 22

3 Product Specifications.....	24
3.1 Technical Specifications.....	24
3.2 Environmental Specifications.....	29
3.3 Physical Specifications.....	30
4 Software and Hardware Compatibility.....	31
5 Safety Instructions.....	32
5.1 Safety Instructions.....	32
5.2 Maintenance and Warranty.....	35
6 ESD.....	37
6.1 ESD Prevention.....	37
6.2 Grounding Methods for ESD Prevention.....	38
7 Internal Cabling.....	39
7.1 TPM Cabling.....	39
7.2 Screw-in RAID Controller Card Cabling.....	40
7.3 Cabling of the SATA Controller Integrated in the Southbridge.....	41
7.4 PCIe Card Cabling.....	42
8 Parts Replacement.....	43
8.1 Spare Part Description.....	43
8.2 Tools	44
8.3 Basic Operations.....	45
8.3.1 Power-On Procedure.....	45
8.3.2 Power-Off Procedure.....	46
8.3.3 Removing an XH321 V5.....	47
8.3.4 Installing a Server Node.....	50
8.4 Field Replaceable Units.....	53
8.4.1 Removing an M.2 SSD.....	54
8.4.2 Installing an M.2 SSD.....	55
8.4.3 Removing the Screw-in RAID Controller Card.....	57
8.4.4 Installing the Screw-in RAID Controller Card.....	59
8.4.5 Removing a Supercapacitor.....	61
8.4.6 Installing the Supercapacitor.....	64
8.4.7 Removing the Avago SAS3004iMR PCIe RAID Controller Card.....	66
8.4.8 Installing the Avago SAS3004iMR PCIe RAID Control Card.....	67
8.4.9 Removing an M.2 FRU on the Avago SAS3004iMR PCIe RAID Controller Card.....	67
8.4.10 Installing an M.2 FRU on the Avago SAS3004iMR PCIe RAID Controller Card.....	69
8.4.11 Removing a Processor.....	71
8.4.12 Installing a Processor.....	75
8.4.13 Removing a Memory Module.....	81
8.4.14 Installing a Memory Module.....	82
8.4.15 Removing the TPM.....	85

8.4.16 Installing the TPM.....	87
8.4.17 Removing the Battery.....	90
8.4.18 Installing the Battery.....	92
8.4.19 Removing a PCIe Card.....	93
8.4.20 Installing a PCIe Card.....	96
8.4.21 Removing a PCIe Riser Module.....	100
8.4.22 Installing a PCIe Riser Module.....	102
8.4.23 Removing the Air Duct.....	104
8.4.24 Installing the Air Duct.....	105
8.4.25 Removing the Mainboard and Server Node Case.....	106
8.4.26 Installing the Mainboard and Server Node Case.....	109
9 Troubleshooting Guide.....	112
10 Common Operations.....	113
10.1 Querying the iBMC IP Address.....	113
10.2 Logging In to the iBMC WebUI.....	114
10.3 Logging In to the Desktop of a Server.....	116
10.3.1 Using the Remote Virtual Console.....	116
10.3.1.1 iBMC.....	116
10.3.1.1.1 Versions Earlier Than V600.....	116
10.3.1.1.2 V600 and Later Versions.....	119
10.3.2 Logging In to the Independent Remote Console.....	122
10.4 Logging In to the CLI.....	123
10.4.1 Logging In to the CLI Using PuTTY over a Network Port.....	123
10.4.2 Logging In to the CLI Using PuTTY over a Serial Port.....	125
10.5 Accessing the BIOS.....	126
10.5.1 Accessing the BIOS (V3XX or Earlier).....	127
10.5.2 Accessing the BIOS (V6XX or Later).....	128
11 More Information.....	132
11.1 Obtaining Technical Support.....	132
11.2 Product Information.....	133
11.3 Product Configuration Resources.....	134
11.4 Maintenance Tools.....	134
12 Software and Configuration Utilities.....	136
12.1 iBMC.....	136
12.2 BIOS.....	137
A Appendix.....	139
A.1 Product SN.....	139
A.2 Operating Temperature Limitations.....	140
A.2.1 Operating Temperature Limitations (Supercapacitor for the RAID Controller Card Configured).....	140
A.2.2 Operating Temperature Limitations (Optical Modules Configured).....	142

A.2.3 Operating Temperature Limitations (Avago SAS3004iMR RAID Controller Card + M.2 FRU Configured).....	144
A.2.4 Operating Temperature Limitations (Different Models of Processors).....	146
A.3 RAS Features.....	148
B Glossary.....	151
B.1 A-E.....	151
B.2 F-J.....	152
B.3 K-O.....	152
B.4 P-T.....	152
B.5 U-Z.....	153
C Acronyms and Abbreviations.....	154
C.1 A-E.....	154
C.2 F-J.....	155
C.3 K-O.....	157
C.4 P-T.....	157
C.5 U-Z.....	159

1 Overview

[1.1 Product Introduction](#)

[1.2 Physical Structure](#)

[1.3 Logical Structure](#)

1.1 Product Introduction

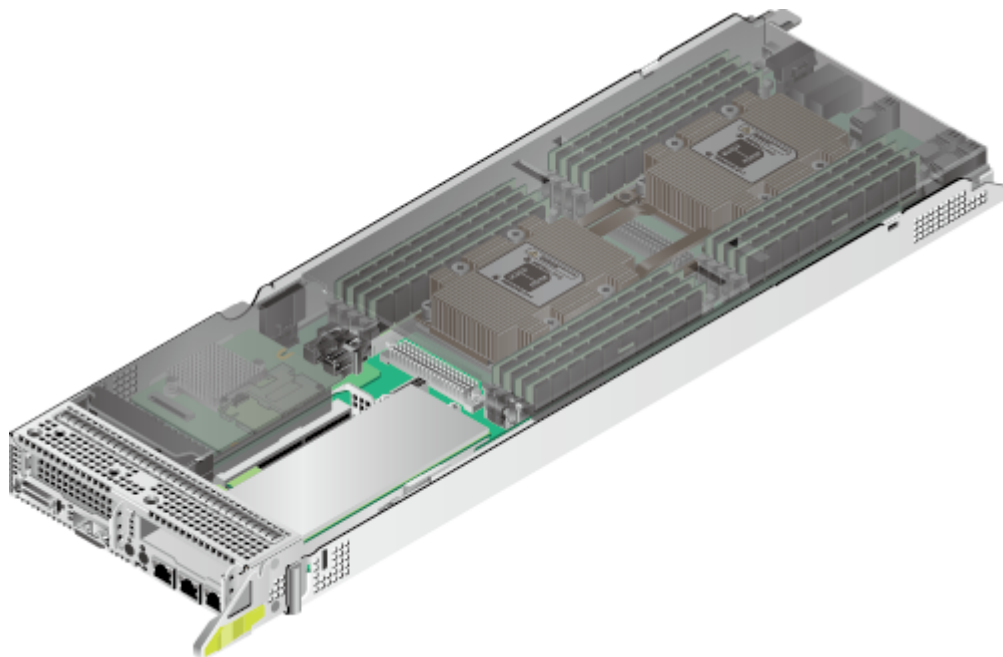
The XH321 V5 is a server node designed for X6000 servers. An X6000 can house up to four XH321 V5 server nodes in a 2U chassis.

The XH321 V5 delivers supreme performance and high storage density in limited space through innovative design. It is easy to manage and maintain.

The XH321 V5 supports six 2.5-inch SAS/SATA drives or NVMe drives, up to 16 DDR4 memory modules, and two PCIe cards.

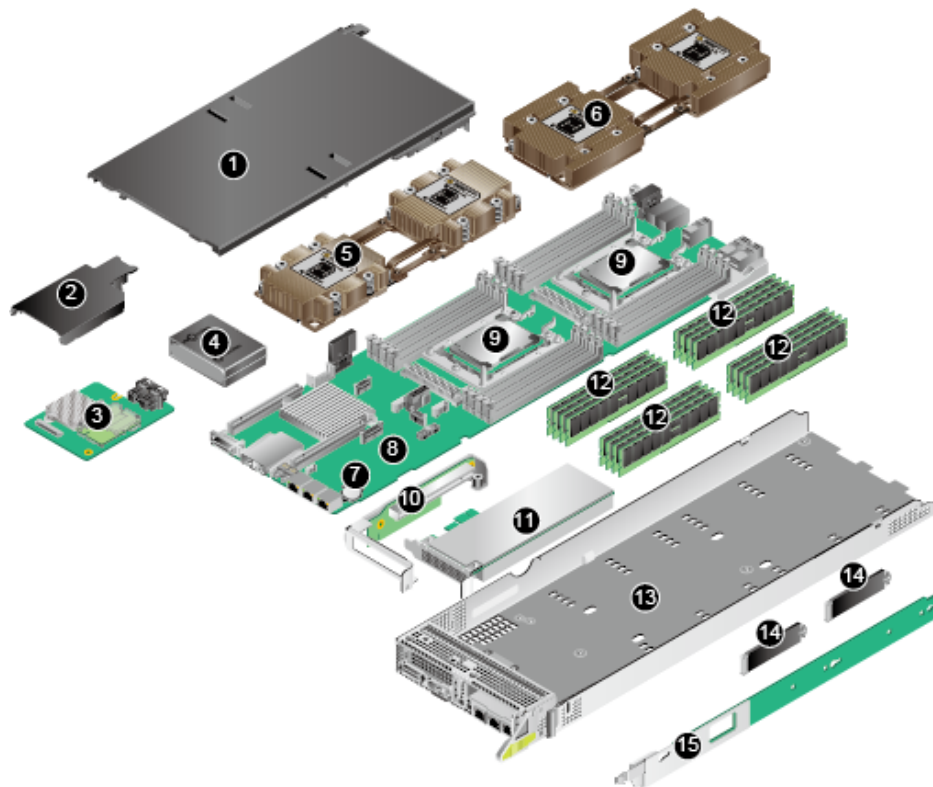
The XH321 V5 is ideal for data center, cloud computing, Big Data, and Internet applications.

Figure 1-1 XH321 V5



1.2 Physical Structure

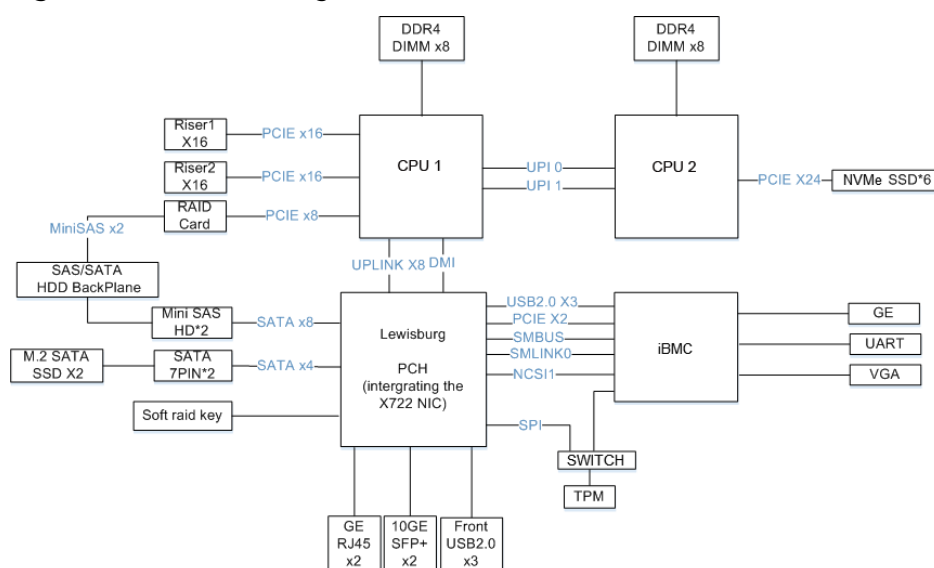
Figure 1-2 XH321 V5 physical structure



1	Air duct	2	Air duct for the supercapacitor
3	RAID controller card/PCIe card	4	Supercapacitor
5	Narrow conjoined heat sink	6	Wide conjoined heat sink
7	Battery	8	Mainboard
9	Processor	10	PCIe riser module
11	PCIe card	12	Memory
13	Node case	14	M.2 SSD card
15	TPM (with M.2 ports)	-	-

1.3 Logical Structure

Figure 1-3 XH321 V5 logical structure



- The server supports one or two Intel® Xeon® Scalable processors.
- The server supports up to 16 memory modules.
- The CPUs (processors) interconnect with each other through two UPI links at a speed of up to 10.4 GT/s.
- The PCIe cards connected to the processors provide service ports.
- The RAID controller card connects to the mainboard using a SAS cable and connects to the system backplane through a connector.
- The iBMC chipset interconnects with the PCH through PCIe and LPC buses to provide a management interface.

- The iBMC integrates the graphics card, video compression, and virtual media component to provide device management functions, such as power control, slot ID acquisition, power supply detection, and KVM over IP.

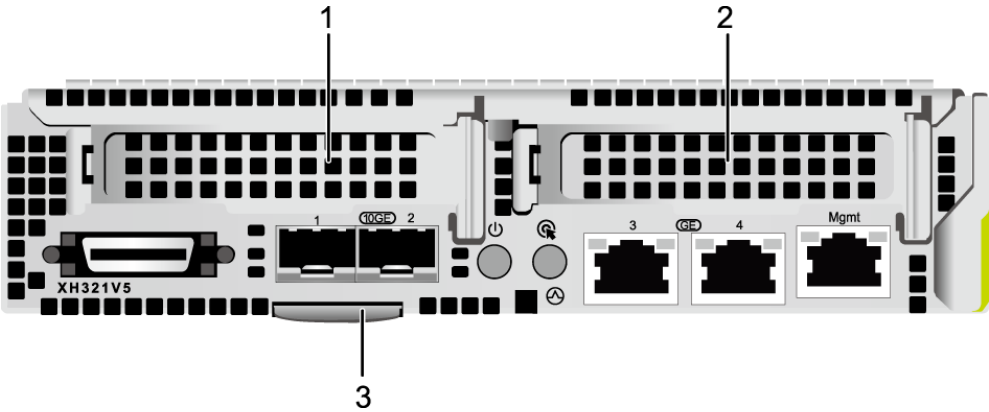
2 Hardware Description

- 2.1 Front Panel
- 2.2 Processor
- 2.3 Memory
- 2.4 Storage
- 2.5 Network
- 2.6 I/O Expansion
- 2.7 Boards

2.1 Front Panel

2.1.1 Appearance

Figure 2-1 Front view



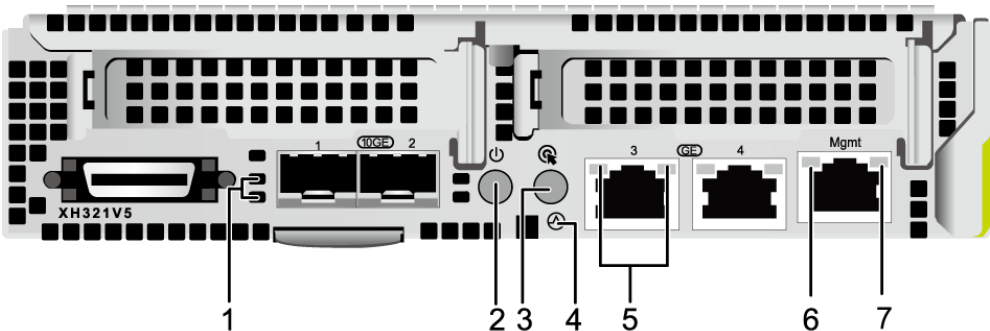
1	PCIe card (RAID controller card not configured)	2	PCIe cards
---	---	---	------------

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

2.1.2 Indicators and Buttons

Positions

Figure 2-2 Indicators and buttons on the front panel



1	LOM port indicator	2	Power button/indicator
3	UID button/indicator	4	Health status indicator
5	LOM port indicator	6	Data transmission status indicator of the management network port
7	Connection status indicator of the management network port	-	-

Indicator and Button Description

Table 2-1 Indicators and buttons on the front panel

Silkscreen	Indicator/ Button	Description
-	LOM port indicator	For details, see 2.5.1 LOMs .

Silkscreen	Indicator/ Button	Description
	Power button/ indicator	Power indicator: - 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. Power button: - When the device is powered on, you can press this button to gracefully shut down the OS. NOTE For different OSs, you may need to shut down the OS as prompted. - When the device is powered on, holding down this button for 6 seconds will forcibly power off the device. - When the power indicator is steady yellow, you can press this button to power on the device.
	Health status indicator	- 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.
	UID button/ indicator	The UID button/indicator helps identify and locate a device. UID indicator: - Off: The device is not being located. - Blinking or steady blue: The device is being located. UID button: - 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.

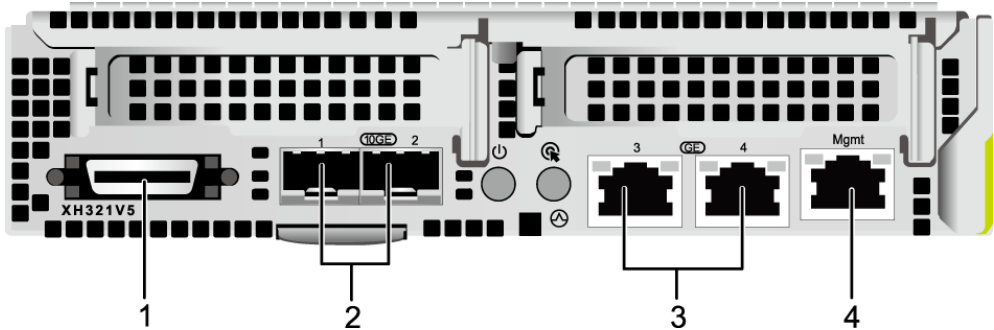
Silkscreen	Indicator/ Button	Description
-	Data transmission status indicator for the management network port	- Off: No data is being transmitted. - Blinking yellow: Data is being transmitted.
-	Connection status indicator for the management network port	- Off: The network port is not connected. - Steady green: The network port is properly connected.

2.1.3 Ports

Port Positions

- Ports on the front panel

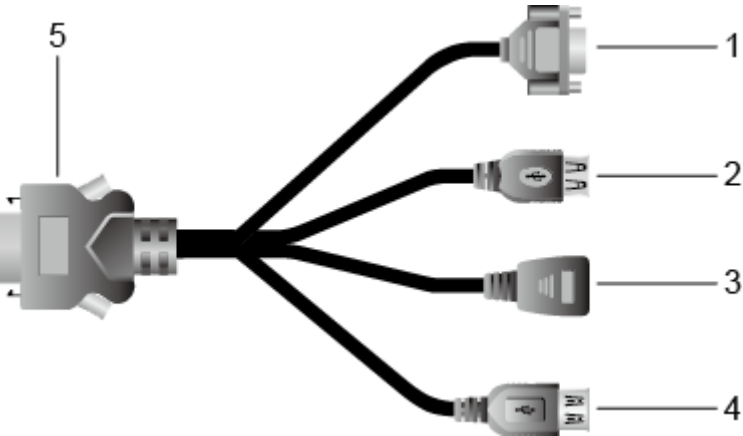
Figure 2-3 Ports on the front panel



1	Universal connector port	2	LOM port 1
3	LOM port 2	4	Management network port

- Ports on the multi-port cable

Figure 2-4 Multi-port cable



1	VGA port	2	Two USB ports
3	Serial port	4	One USB port
5	Multi-port connector	-	-

Port Description

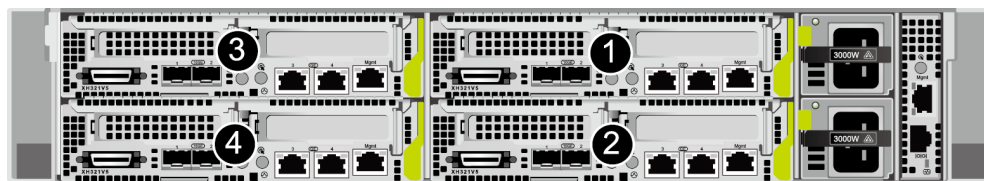
Table 2-2 Ports on the front panel

Port	Type	Quantity	Description
LOM port 1	10GE optical port	2	For details, see 2.5.1 LOMs .
LOM port 2	GE electrical port	2	
Universal connector port	-	1	Used to connect a multi-port cable, which provides one DB-15 VGA port, three USB 2.0 ports, and one RJ45 serial port.
Management network port	RJ45	1	Used for server management. NOTE The management network port is a GE port that supports 100 Mbit/s and 1000 Mbit/s auto-negotiation.

2.1.4 Installation Positions

An X6000 can house a maximum of four XH321 V5 nodes in a 2U chassis.

Figure 2-5 Installation positions



2.2 Processor

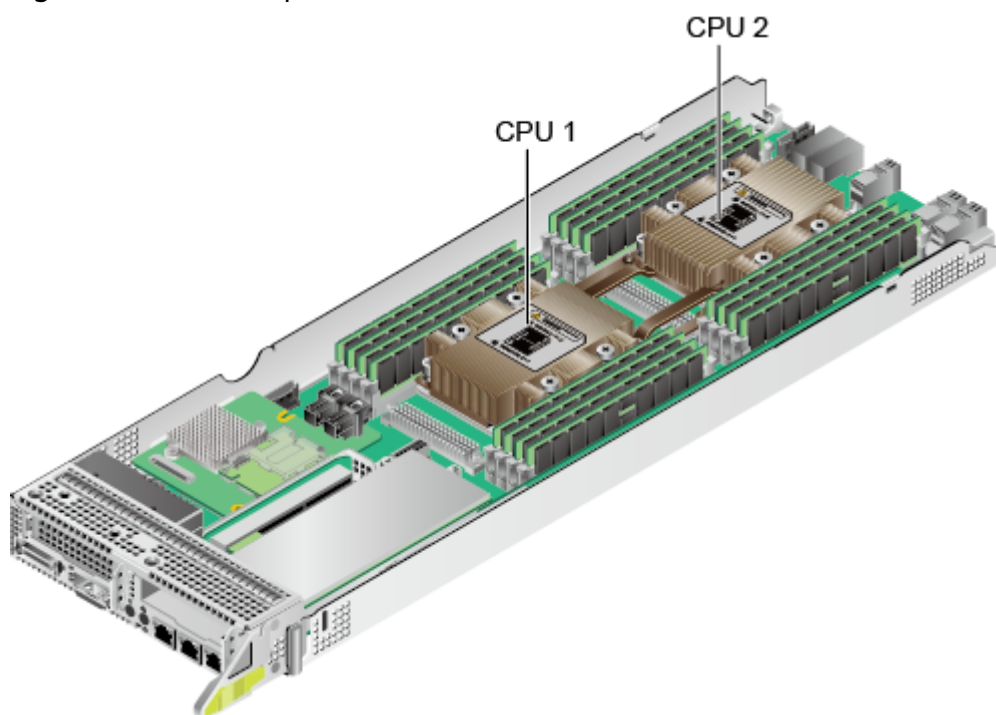
- The server supports one or two processors.
- If only one processor is required:
 - Install it in socket **CPU1**.
 - NVMe SSDs are not supported.
- The processor heat sink varies depending on the processor power:
 - If the maximum processor power is 165 W, use a narrow conjoined heat sink.

NOTE

When Intel® Xeon® Scalable (Gold 6144, Gold 6146, Gold 6244, or Gold 6252N) processors are configured, wide conjoined heat sinks are required to meet the high heat dissipation requirement.

- If the processor power is higher than 165 W, use a wide conjoined heat sink.
- The same model of processors must be used in a server.
- Contact your local Huawei sales representative or use the [Computing Product Compatibility Checker](#) to determine the components to be used.

Figure 2-6 Processor positions



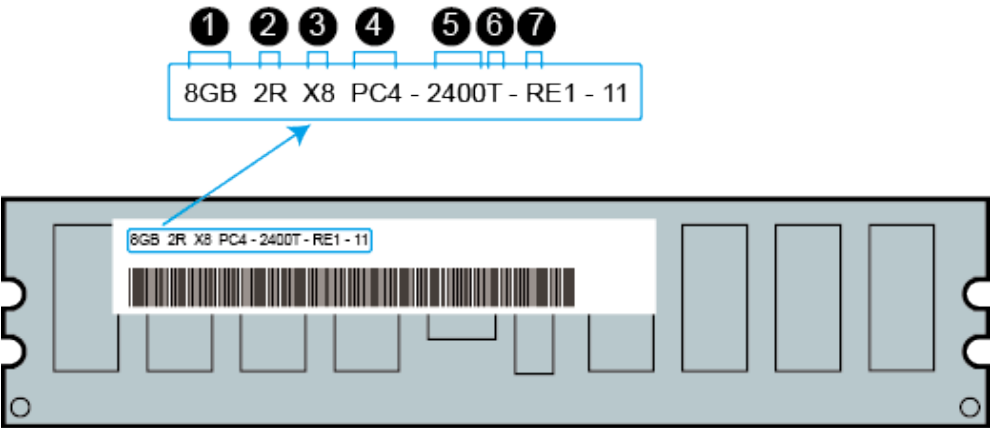
2.3 Memory

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 2-7 Memory identifier



Callout	Description	Definition
1	Capacity of the memory module	• 8 GB • 16 GB • 32 GB • 64 GB • 128 GB
2	Number of ranks of the memory module	• 1R: single-rank • 2R: dual-rank • 4R: quad-rank • 8R: octal-rank
3	Data width on the DRAM	• X4: 4-bit • X8: 8-bit
4	Type of the memory interface	• PC3: DDR3 • PC4: DDR4

Callout	Description	Definition
5	Maximum memory speed	• 2133 MT/S • 2400 MT/S • 2666 MT/S • 2933 MT/S
6	Column Access Strobe (CAS) latency	• P: 15 • T: 17
7	DIMM type	• R: RDIMM • L: LRDIMM

2.3.1.2 Memory Subsystem Architecture

The XH321 V5 provides 16 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	1A (primary)	DIMM000(A)
	1A	DIMM001(G)
	1B	DIMM010(B)
	1C	DIMM020(C)
	1D (primary)	DIMM030(D)
	1D	DIMM031(H)
	1E	DIMM040(E)
	1F	DIMM050(F)
CPU 2	2A (primary)	DIMM100(A)
	2A	DIMM101(G)
	2B	DIMM110(B)
	2C	DIMM120(C)
	2D (primary)	DIMM130(D)
	2D	DIMM131(H)

CPU	Memory Channel	Memory Slot
	2E	DIMM140(E)
	2F	DIMM150(F)

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 Huawei sales representative or use the [Computing Product 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.

- Use the [Computing Product 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)		64
Rated speed (MT/s)		2933
Operating voltage (V)		1.2
Maximum number of DDR4 DIMMs in a node ^a		16
Maximum DDR4 memory capacity of the node (GB) ^b		1024
Maximum operating speed (MT/s)	1DPC ^c	2933 ^d
	2DPC	2666
• a: The maximum number of DDR4 memory modules is based on dual-processor configuration. The value is halved for a server with only one processor. • b: 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

- 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

An XH321 V5 supports a maximum of 16 DDR4 DIMMs. Balanced memory configuration is recommended for optimal memory performance.

NOTICE

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

Figure 2-8 Memory slots

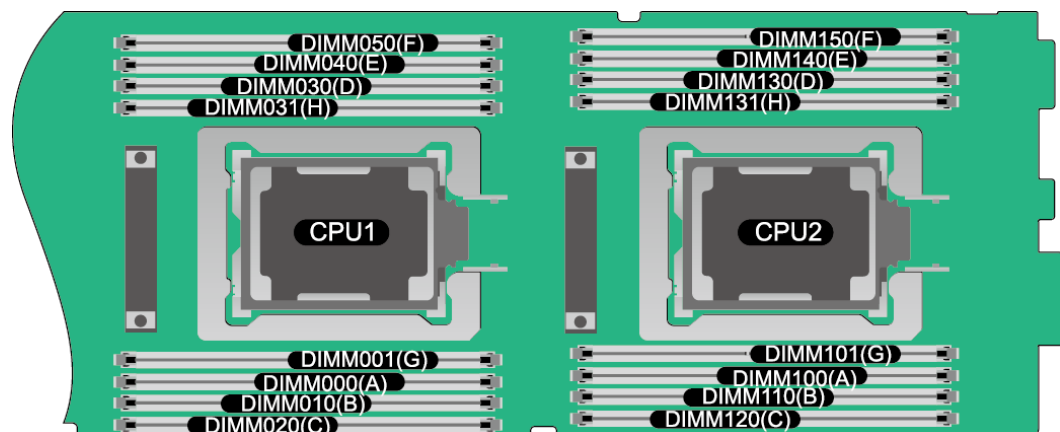


Figure 2-9 DDR4 memory installation guidelines (1 processor)

CPU	Channel	DIMM Slot	Number of DIMMs (✓: recommended ○: not recommended)							
			✓	✓	○	✓	○	✓	○	✓
			1	2	3	4	5	6	7	8
CPU 1	A	DIMM000(A)	•	•	•	•	•	•	•	•
		DIMM001(G)							•	•
	B	DIMM010(B)		•	•	•	•	•	•	•
	C	DIMM020(C)			•		•	•	•	•
	D	DIMM030(D)				•	•	•	•	•
		DIMM031(H)								•
	E	DIMM040(E)				•	•	•	•	•
	F	DIMM050(F)						•	•	•

Figure 2-10 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
CPU 1	A	DIMM000(A)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
		DIMM001(G)													•	•
	B	DIMM010(B)			•	•	•	•	•	•	•	•	•	•	•	•
	C	DIMM020(C)					•	•		•	•	•	•	•	•	•
	D	DIMM030(D)							•	•	•	•	•	•	•	•
		DIMM031(H)								•	•	•	•	•	•	•
	E	DIMM040(E)							•	•	•	•	•	•	•	•
	F	DIMM050(F)										•	•	•	•	•
CPU 2	A	DIMM100(A)		•	•	•	•	•	•	•	•	•	•	•	•	•
		DIMM101(G)													•	•
	B	DIMM110(B)				•	•	•	•	•	•	•	•	•	•	•
	C	DIMM120(C)						•	•		•	•	•	•	•	•
	D	DIMM130(D)							•	•	•	•	•	•	•	•
		DIMM131(H)														•
	E	DIMM140(E)							•	•	•	•	•	•	•	•
	F	DIMM150(F)											•	•	•	•

2.3.1.6 Memory Protection Technologies

The following memory protection technologies are supported:

- ECC
- Full mirroring
- Address range mirroring
- SDDC
- SDDC+1
- Rank sparing mode
- Static virtual lockstep
- Faulty DIMM isolation
- Memory thermal throttling
- Memory address parity protection
- Memory demand/patrol scrubbing
- Device tagging
- Data scrambling

- Adaptive double device data correction (ADDDC)
- ADDDC+1

2.4 Storage

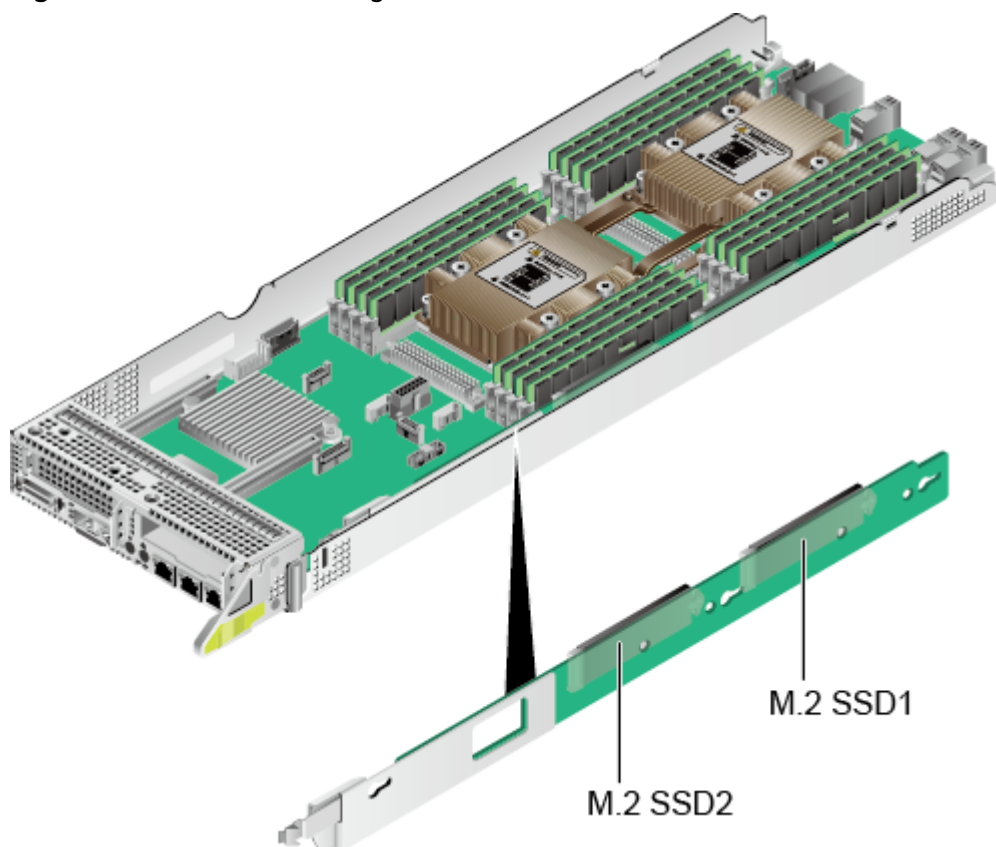
2.4.1 Drive Configurations

Table 2-5 Drive configuration

Configuration	Maximum Drives	Drive Management Mode
Built-in drive	2 • Slots 1 and 2 support only M.2 SSDs^a.	-
• a: The M.2 SSDs come in two sizes 2242 and 2280, and support the SATA interface. • Contact your local Huawei sales representative or use the Computing Product Compatibility Checker to determine the components to be used.		

2.4.2 Drive Numbering

Figure 2-11 Drive numbering



2.4.3 RAID Controller Card

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

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

2.5 Network

2.5.1 LOMs

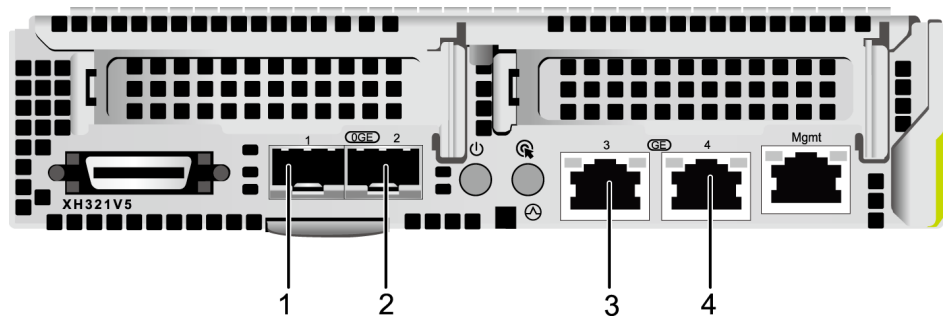
LOMs provide network expansion capabilities.

Table 2-6 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)	10,000 Mbit/s	10/100/1000 Mbit/s
		GE electrical port	2	Auto-negotiation 1000 Mbit/s (full duplex)	1000 Mbit/s	10/100 Mbit/s

- Use [Computing Product Compatibility Checker](#) to obtain information about the cables and optical modules supported by the LOM ports.
- 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 Wake on LAN (WOL) function of the LOM ports. To restore the NC-SI connection, refresh the iBMC WebUI.

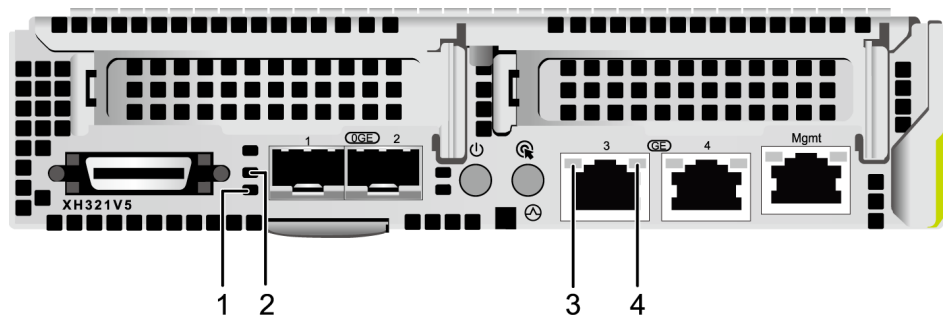
Figure 2-12 LOM port



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

Indicator Positions

Figure 2-13 LOM indicators



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

Indicator Description

Table 2-7 LOM indicators

Indicator	Description
Connection status indicator/Data transmission status indicator for a 10GE optical port	• 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	• Off: The network port is not connected. • Steady green: The data transmission rate is 10 Gbit/s.
Connection status indicator of a GE electrical port	• Off: The network port is not connected. • Steady green: The network port is properly connected.
Data transmission status indicator of a GE electrical port	• Off: Inactive. • Steady yellow: Active, but no data is being transmitted. • Blinking yellow: Data is being transmitted.

2.6 I/O Expansion

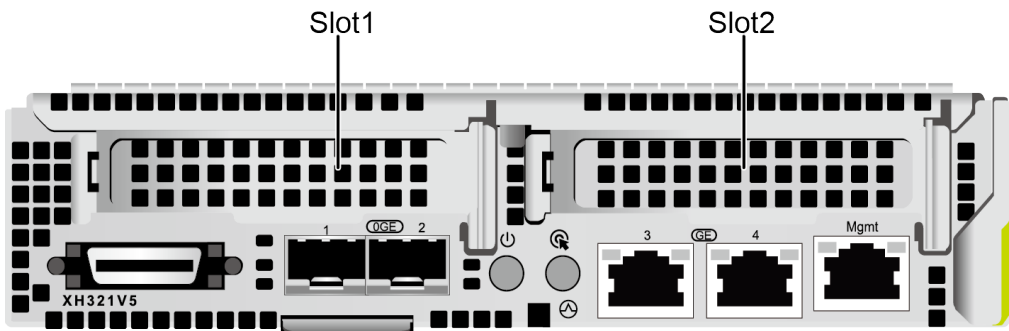
2.6.1 PCIe Cards

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 Huawei sales representative or use the [Computing Product 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

Figure 2-14 PCIe Slot



2.6.3 PCIe Slot Description

NOTE

If CPU 2 is not installed, its PCIe slots are unavailable.

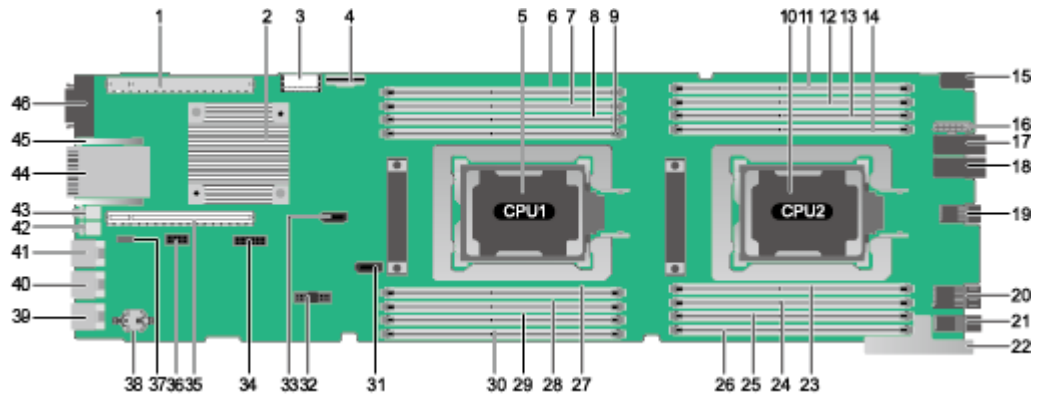
Table 2-8 PCIe slot description

PCIe Slot	CPU	PCIe Standards	Connector Width	Bus Width	Port No.	B/D/F	Slot Size
RAID controller card	CPU 1	PCIe 3.0	x8	x8	Port1C	1c/00/0	-
LOM	CPU 1	PCIe 3.0	-	x8	Port1A	17/00/0	-
Slot 1	CPU 1	PCIe 3.0	x16	x16	Port3A	5d/00/0	HHHL
Slot 2	CPU 1	PCIe 3.0	x16	x16	Port2A	3a/00/0	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.							

2.7 Boards

2.7.1 Mainboard

Figure 2-15 XH321 V5 mainboard



1	PCIe slot 1	2	Southbridge
3	RAID controller card connector	4	Slimline connector
5	CPU 1	6	DIMM050 connector
7	DIMM040 connector	8	DIMM030 connector
9	DIMM031 connector	10	CPU 2
11	DIMM150 connector	12	DIMM140 connector
13	DIMM130 connector	14	DIMM131 connector
15	Left guide sleeve	16	Slimline connector
17	Power connector	18	Power connector
19	Signal connector	20	Signal connector
21	Signal connector	22	Right guide sleeve
23	DIMM101 connector	24	DIMM100 connector
25	DIMM110 connector	26	DIMM120 connector
27	DIMM001 connector	28	DIMM000 connector
29	DIMM010 connector	30	DIMM020 connector
31	M.2 connector port 0	32	OPA signal connector
33	M.2 connector port 1	34	TPM signal connector
35	PCIe slot 2	36	NC-SI connector
37	SoftRAID key connector ^a	38	Battery
39	iBMC management network port	40	LOM GE port 4

41	LOM GE port 3	42	UID button/indicator
43	Power button/indicator	44	2 x 10GE optical ports
45	Optical port indicator	46	Universal connector port
a: Reserved.			

3 Product Specifications

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

3.1 Technical Specifications

Table 3-1 Technical specifications

Category	Specifications
Form factor	2U4 server node
Chipset	Intel® C622
Processors	Supports one or two processors. - 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 - Two 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 NOTE The preceding information is for reference only. The actual configuration may vary. For details, check part compatibility using Computing Product Compatibility Checker.

Category	Specifications
Memory	Supports 16 memory modules of the following types: • Up to 16 DDR4 memory modules • Max. 2933 MT/s memory speed • 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. NOTE The preceding information is for reference only. The actual configuration may vary. For details, check part compatibility using Computing Product Compatibility Checker.

Category	Specifications
Storage	Supports a variety of drive configurations. For details, see 2.4.1 Drive Configurations. - Supports two or four M.2 SSDs. - The PCH supports two M.2 SSDs. If an Avago SAS3004iMR RAID controller card is configured, the Avago SAS3004iMR supports two M.2 SSDs. - When the Avago SAS3004iMR RAID controller card is used with an SR450C-M, SR430C-ML, or SR150-M RAID controller card, the drive letter of the M.2 SSDs managed by the Avago SAS3004iMR RAID controller card cannot be sda on the OS. NOTE - 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: - 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. - Supports hot swap of SAS/SATA drives. - Supports a variety of RAID controller cards. Use the Computing Product Compatibility Checker to obtain information about the specific RAID controller cards supported. - The RAID controller card supports RAID configuration, RAID level migration, and drive roaming. - The RAID controller card does not occupy a standard PCIe slot. For details about the RAID controller card, see Huawei V5 Server RAID Controller Card User Guide.

Category	Specifications
Network	Supports LOM. - Supports two 10GE optical ports and two GE electrical ports via the NIC chip integrated on the mainboard. - The LOM ports support NC-SI, WOL, and PXE. 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. - 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.
I/O expansion	3 PCIe 3.0 slots: - One slot dedicated for a screw-in RAID controller card and two for standard PCIe cards. For details, see 2.6.2 PCIe Slots and 2.6.3 PCIe Slot Description. - Support Huawei proprietary 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. NOTE The preceding information is for reference only. The actual configuration may vary. For details, check part compatibility using Computing Product Compatibility Checker.
Ports	Supports a variety of ports. - Ports on the front panel: - One universal connector port - One system management port - Two GE electrical ports - Two 10GE optical ports - Built-in ports: - Two SATADOM ports

Category	Specifications
Video card	An SM750 video chip with 32 MB display memory is integrated on the mainboard. The maximum display resolution is 1920 x 1200 at 60 Hz with 16 M colors. NOTE - 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.
System management	- UEFI - iBMC - NC-SI - Integration with third-party management systems
Security features	- Power-on password - Administrator password - TPM (only outside China) - Secure boot

3.2 Environmental Specifications

Table 3-2 Environmental specifications

Category	Specifications
Temperature	- Operating temperature: 5°C to 35°C (41°F to 95°F) (ASHRAE Class A1/A2 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 NOTE - If a single fan is faulty: - The highest operating temperature supported is 30°C (86°F). - If the power consumption of the processor is 125 W or higher, the system performance may be affected or a temperature alarm may be generated. - When the server is configured with 6248R or 6258R processors, the highest operating temperature is 30°C (86°F). - The highest operating temperature varies depending on the server configuration. For details, see A.2 Operating Temperature Limitations.
Relative humidity (RH, non-condensing)	- 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
Operating altitude	≤3050m - 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). - HDDs cannot be used at an altitude of over 3050 m (10006.44 ft). - Titanium PSUs are required for the altitude higher than 3050 m (10006.44 ft).

Category	Specifications
Corrosive gaseous contaminant	Maximum corrosion product thickness growth rate: • Copper corrosion rate test: 300 Å/month (meeting level G1 requirements of the ANSI/ISA-71.04-2013 standard on gaseous corrosion) • Silver corrosion rate test: 200 Å/month
Particle contaminant	• The equipment room environment meets the requirements of ISO 14644-1 Class 8. • There is no explosive, conductive, magnetic, or corrosive dust in the equipment room. NOTE It is recommended that the particulate pollution in the equipment room be monitored by a professional agency.

 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)	40.5 mm x 177.9 mm x 545.5 mm (1.59 in. x 7.00 in. x 17.89 in.)
Weight in full configuration	• Net weight: 4.2 kg (9.26 lb) • Packaging materials: 2.73 kg (6.02 lb)

4 Software and Hardware Compatibility

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

NOTICE

- Do not use incompatible components. Otherwise, the server may fail to work properly. The technical support and warranty do not cover faults caused by incompatible components.
 - 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 Huawei 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 Safety Instructions](#)

[5.2 Maintenance and Warranty](#)

5.1 Safety Instructions

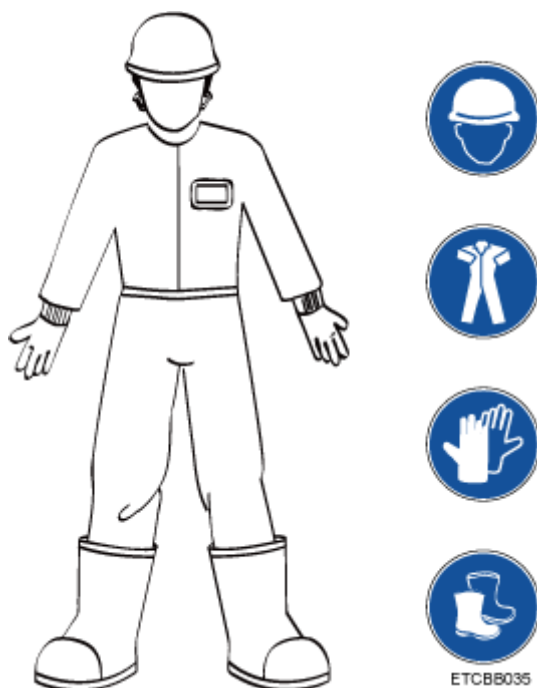
General Statement

- 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 personnel certified or authorized by Huawei are allowed to install devices.
- 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.

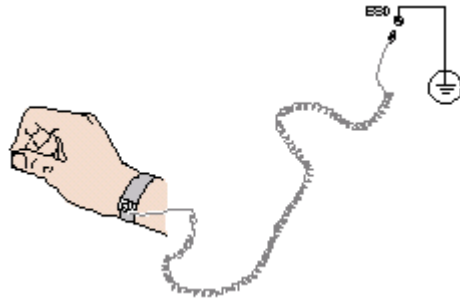
Figure 5-2 Removing conductive objects



[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 [Computing Product 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)	• Male: 15/33.08 • Female: 10/22.05

For more information about safety instructions, see [Huawei 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 Service](#).

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 Internal Cabling

[7.1 TPM Cabling](#)

[7.2 Screw-in RAID Controller Card Cabling](#)

[7.3 Cabling of the SATA Controller Integrated in the Southbridge](#)

[7.4 PCIe Card Cabling](#)

7.1 TPM Cabling

Figure 7-1 TPM cabling

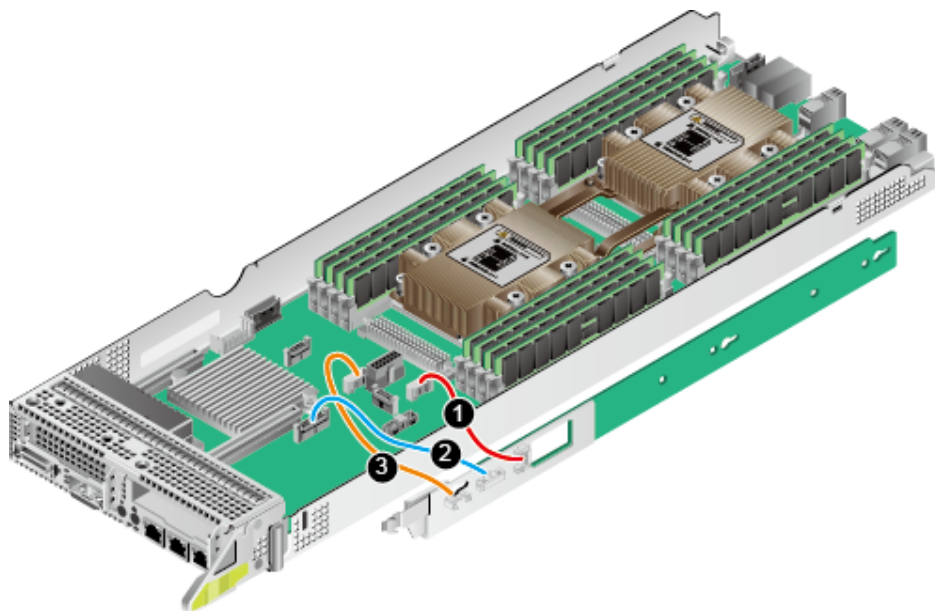


Table 7-1 TPM cabling

No.	P/N Code	Description
1	04051409-003	Signal cable for connecting the TPM to the M.2 connector on the mainboard
2	04080547	Signal cable for connecting the TPM to the TPM connector on the mainboard
3	04051409-004	Signal cable for connecting the TPM to the M.2 connector on the mainboard

7.2 Screw-in RAID Controller Card Cabling

Figure 7-2 Screw-in RAID controller card cabling

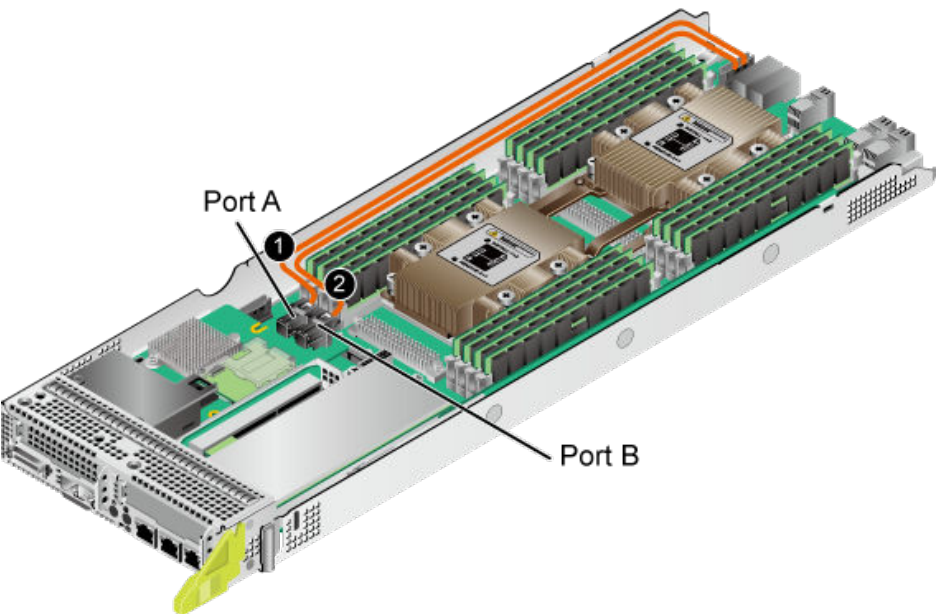


Table 7-2 Screw-in RAID controller card cabling

No.	P/N Code	Description
1	04052070	Slimline cable for connecting the screw-in RAID controller card (Port A) to the Slimline connector
2	04052070	Slimline cable for connecting the screw-in RAID controller card (Port B) to the Slimline connector

7.3 Cabling of the SATA Controller Integrated in the Southbridge

Figure 7-3 Internal cabling for the SATA controller integrated in the southbridge

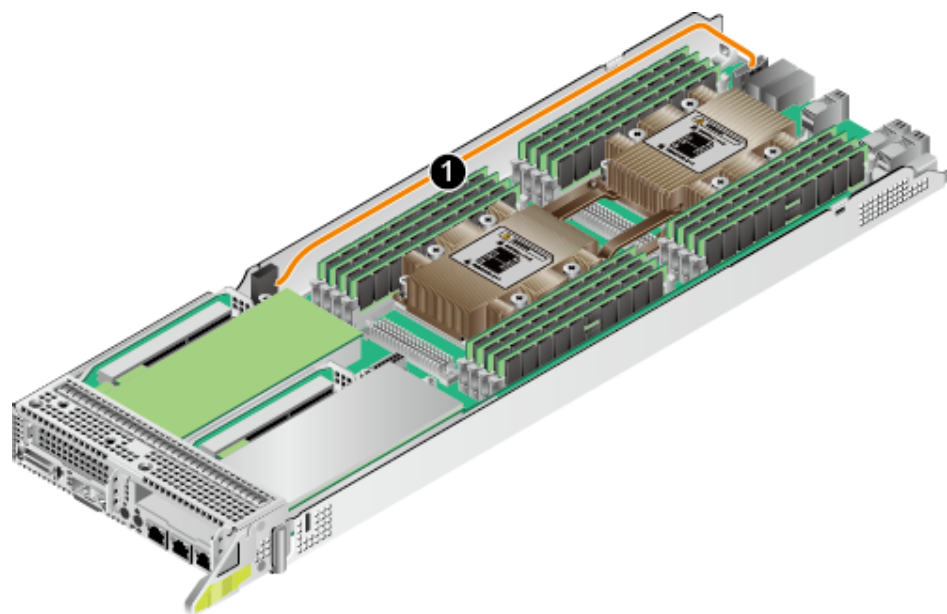


Table 7-3 Cabling of the SATA Controller Integrated in the Southbridge

No.	P/N Code	Description
1	04052068	Slimline cable for connecting the southbridge to the Slimline connector

7.4 PCIe Card Cabling

Figure 7-4 PCIe card cabling

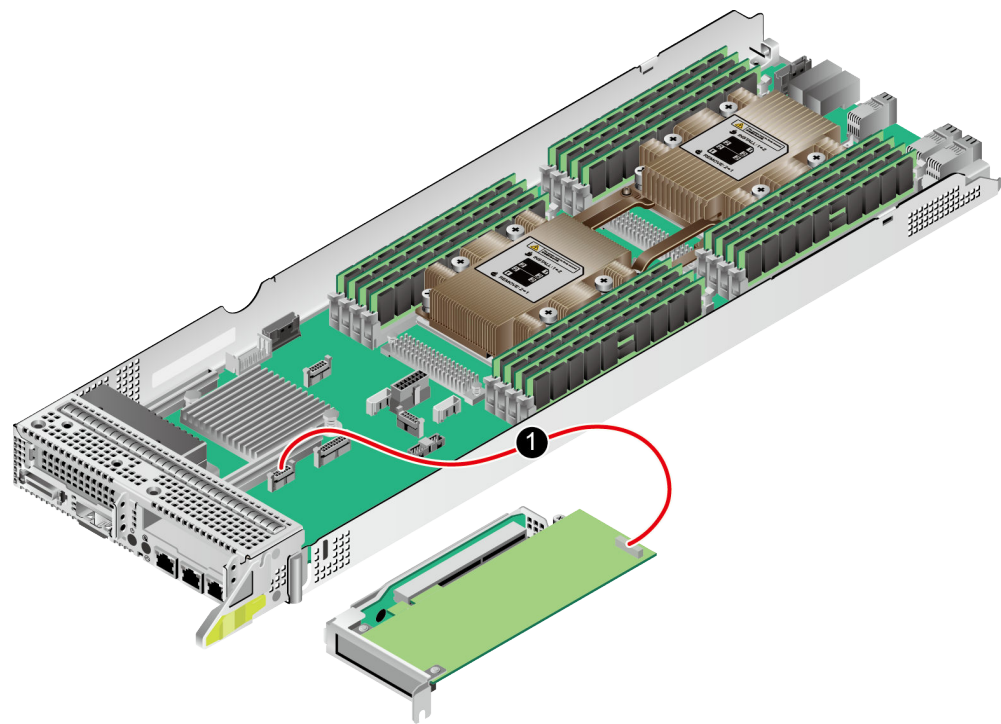


Table 7-4 PCIe card cabling

No.	P/N Code	Description
1	04080606	Signal cable for connecting the PCIe card to the NC-SI connector

 NOTE

This cable is required only when the PCIe card is an SP380 NIC (BOM code: 02312JBD).

8

Parts Replacement

Before touching a device, wear an ESD wrist strap or ESD gloves. For more information, see [5 Safety Instructions](#).

[8.1 Spare Part Description](#)

[8.2 Tools](#)

[8.3 Basic Operations](#)

[8.4 Field Replaceable Units](#)

8.1 Spare Part Description

NOTICE

- A part number (P/N) uniquely identifies a server component. You can find the number on a component or component package.
- Before replacement, confirm the part number (P/N code) of the component to be replaced using [Computing Product Spare Parts Checker](#) and apply for a spare part.

Table 8-1 Spare parts description

Category	Description	Property	Application Scenarios
Regular Spare Part (RSP)	Regular spare part	Regular spare parts include boards and modules. Safety stock is recommended.	Stored in the warehouses near sites based on the contract service type, Service Level Agreement (SLA), and service sites.

Category	Description	Property	Application Scenarios
Non-Regular Spare Part (NRSP)	Non-regular spare part	Mechanical parts, accessories, and cables. Generally, safety stock is not kept for NRSPs. NRSPs are provided on demand; however, the lead time is not committed.	Stored in a country's warehouses based on the contract service type.
Non-Spare Part (NSP)	NSPs are not spare parts and do not have replaceable units at lower levels.	NSPs are not spare parts and do not have replaceable units at lower levels.	Not supplied or stored.
RSP&SUB (Sub-Part)	Regular spare parts with replaceable units at lower levels.	It is classified as a type of RSP and has RSPs or NRSPs at lower levels.	Stored in the warehouses near sites based on the contract service type, SLA, and service sites. Lower-level parts vary with actual demands.
NRSP&SUB	Non-regular spare parts with replaceable units at lower levels.	It is classified as a type of NRSP and has RSPs or NRSPs at lower levels.	Stored in a country's warehouses based on the contract service type. Lower-level parts vary with actual demands.
NSP&SUB	Non-spare parts with spare parts at lower levels.	It is not a spare part, but has RSPs or NRSPs at lower levels.	This part is not stored. Lower-level parts vary with actual demands.

8.2 Tools

Ensure that the following tools are available:

- ESD wrist strap or ESD gloves
- Protective gloves

- ESD bags
- Box cutter
- M3 Phillips screwdriver
- PH1 screwdriver
- Flat-head screwdriver
- Die-casting pliers

Used to remove LC optical fibers, pluggable optical modules, and unshielded network cables.

Figure 8-1 Die-casting pliers



8.3 Basic Operations

8.3.1 Power-On Procedure

NOTICE

- Before powering on a server node, ensure that the server node 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 node is disconnected, wait for at least one minute before powering it on again.

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

- If the server node is installed but the chassis is not yet powered on, power on the chassis.
The server node will be powered on along with the chassis.
- If the chassis is powered on but the server node is not installed, install the server node.
The server node will be automatically powered on after it is installed.
- If the chassis is powered on but the server node is not running properly, hold the power button the front panel for six seconds to power off the service node forcibly, and then press the power button to power it on.
- If the chassis is powered on and the server node is in standby state (the power indicator is steady yellow), you can use any of the following methods to power on the server node:

- Use the iBMC WebUI.
 - i. Log in to the iBMC WebUI.
For details, see [10.2 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 [10.4 Logging In to the CLI](#).
 - ii. Run the following command:
ipmcset -d powerstate -v 1
 - iii. Type **y** or **Y** and press **Enter**.
- Use the Remote Virtual Console.
 - i. Log in to the Remote Virtual Console.
For details, see [10.3 Logging In to the Desktop of a Server](#).
 - ii. On the KVM screen, click  or  on the toolbar.
 - iii. Select **Power On**.
A dialog box is displayed.
 - iv. Click **Yes**.
Power on the server node.

8.3.2 Power-Off Procedure

NOTE

- Powering off a server node will interrupt all services and programs running on it. Therefore, before powering off a server node, ensure that all services and programs have been stopped or migrated to other server nodes.
- The "power-off" mentioned here is an operation performed to change the server node to the standby state (the power indicator is steady yellow).
- After a server node is powered off forcibly, wait for more than 10 seconds for the server node to power off completely. Do not power on the server node 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 node can be powered off in any of the following ways:

- Power off the chassis.
The server node will be powered off along with the chassis.
- When the server node is in power-on state, pressing the power button on the server node front panel can power off the server node gracefully.

 NOTE

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

For details, see [2.1.2 Indicators and Buttons](#).

- When the server node is in power-on state, holding down the power button on the server node front panel for six seconds can power off the server node forcibly.

For details, see [2.1.2 Indicators and Buttons](#).

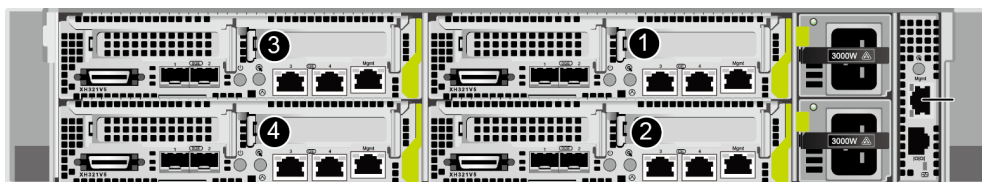
- Use the iBMC WebUI.
 - a. Log in to the iBMC WebUI.
For details, see [10.2 Logging In to the iBMC WebUI](#).
 - b. Choose **Power > Power Control**.
The **Power Control** page is displayed.
 - c. Click **Power Off** or **Forced Power Off**.
A confirmation message is displayed.
 - d. Click **OK**.
The server starts to be powered off.
- Use the iBMC CLI.
 - a. Log in to the iBMC CLI.
For details, see [10.4 Logging In to the CLI](#).
 - b. Run the following command:
 - To power off the server node gracefully, run the **ipmcset -d powerstate -v 0** command.
 - To power off the server node forcibly, run the **ipmcset -d powerstate -v 2** command.
 - c. Type **y** or **Y** and press **Enter**.
- Use the Remote Virtual Console.
 - a. Log in to the Remote Virtual Console.
For details, see [10.3 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**.
A dialog box is displayed.
 - d. Click **Yes**.

8.3.3 Removing an XH321 V5

Procedure

Step 1 Determine the position of the server node in the chassis.

Figure 8-2 Positions and slots of server nodes



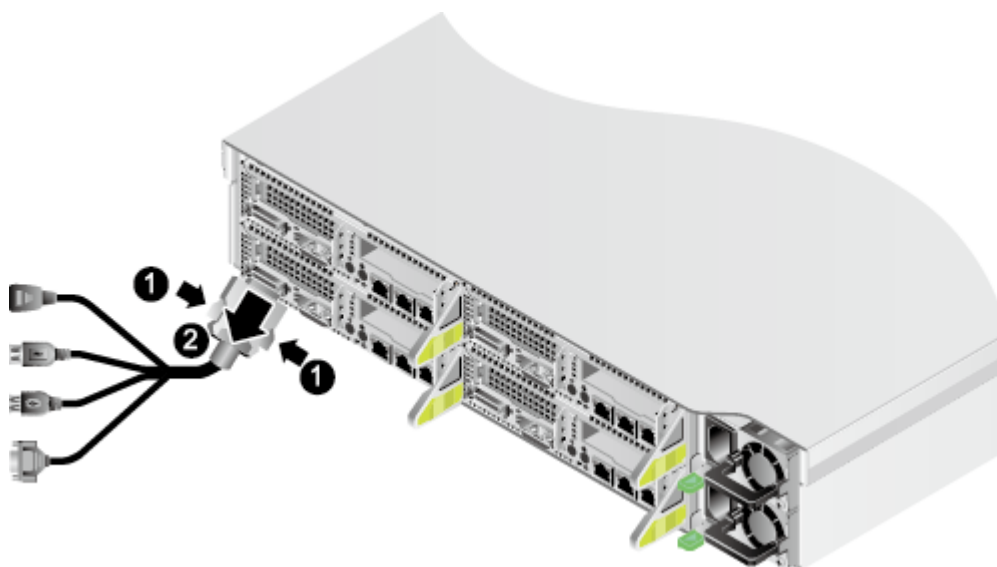
Step 2 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 3 Remove the multi-port cable.

1. Press the two tabs on the multi-port cable connector. See (1) in [Figure 8-3](#).
2. Remove the multi-port cable from the universal connector port (UCP) on the server. See (2) in [Figure 8-3](#).

Figure 8-3 Removing the multi-port cable



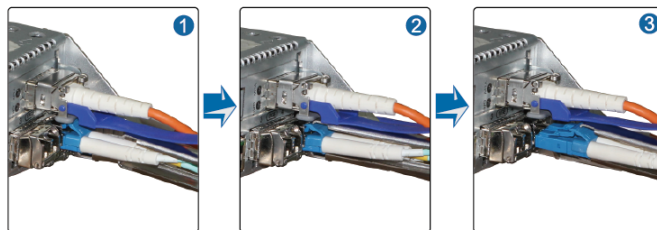
Step 4 Remove the optical cables and modules.

NOTICE

- Replacing the optical cable, network cable, or optical module will interrupt services.
- Wear ESD gloves or an ESD wrist strap when using die-casting pliers to replace optical or network cables or optical modules.
- Do not exert too much force when using the die-casting pliers to prevent damage to the optical or network cables or optical modules.

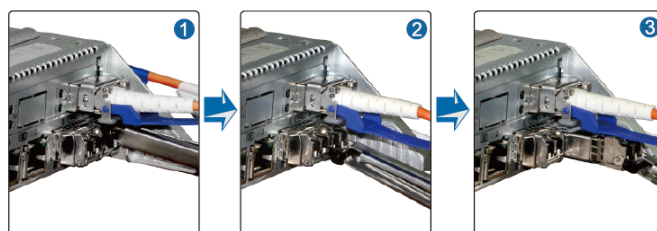
1. Use the die-casting pliers to clamp the optical cable connector and remove it from the port.

Figure 8-4 Removing optical cables using die-casting pliers



2. Use the die-casting pliers to clamp the optical module, unlock the security pin, and remove the optical module.

Figure 8-5 Removing an optical module using die-casting pliers



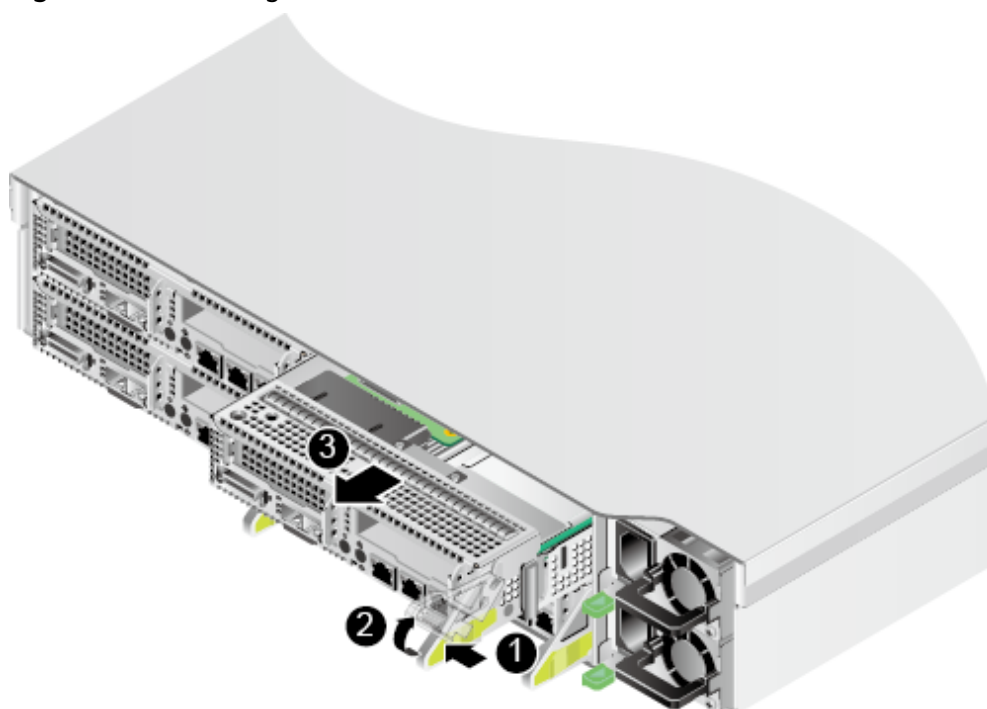
Step 5 Remove the server node.

NOTICE

- When removing a device, wear protective gloves to avoid burns.
- To prevent device damage or personal injury, hold the bottom of the device with both hands when removing it.

-
1. Press the ejector release button on the server node. See (1) in [Figure 8-6](#).
 2. Fully open the ejector lever. See (2) in [Figure 8-6](#).
 3. Holding the ejector lever, pull the server node out of the chassis horizontally. See (3) in [Figure 8-6](#).
 4. Close the ejector lever.

Figure 8-6 Removing the server node



Step 6 Place the removed server node in an ESD bag.

NOTICE

Place only one server node in an ESD bag.

Step 7 Install filler modules.

NOTICE

Install filler panels in vacant slots. Otherwise, the ventilation, heat dissipation, electromagnetic shielding, and dustproof effects of the chassis will be affected.

----End

8.3.4 Installing a Server Node

Procedure

Step 1 Determine the position of the server node in the chassis.

Figure 8-7 Positions and slots of server nodes



 NOTE

Install the lower server nodes and then the upper server nodes.

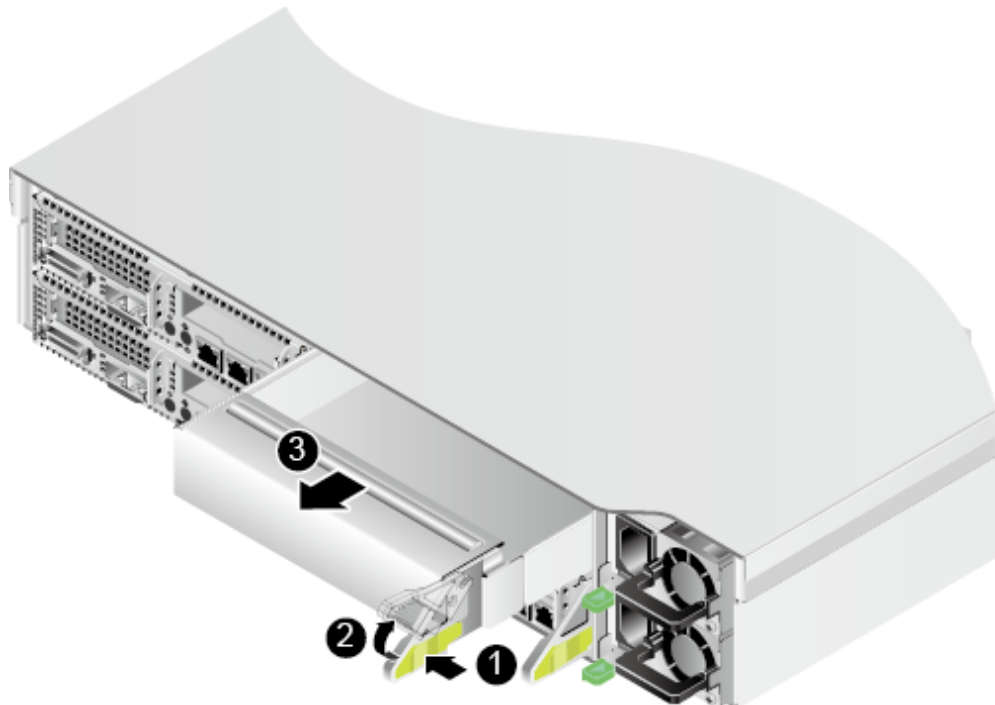
Step 2 Remove filler modules.

 NOTE

Perform this operation only when filler modules are installed.

1. Press the ejector release button on the filler module. See (1) in [Figure 8-8](#).
2. Fully open the ejector lever. See (2) in [Figure 8-8](#).
3. Holding the ejector lever, pull the filler module from the chassis. See (3) in [Figure 8-8](#).

Figure 8-8 Removing a filler panel



4. Close the ejector lever.
5. Place the filler module in an accessory recycle bin.

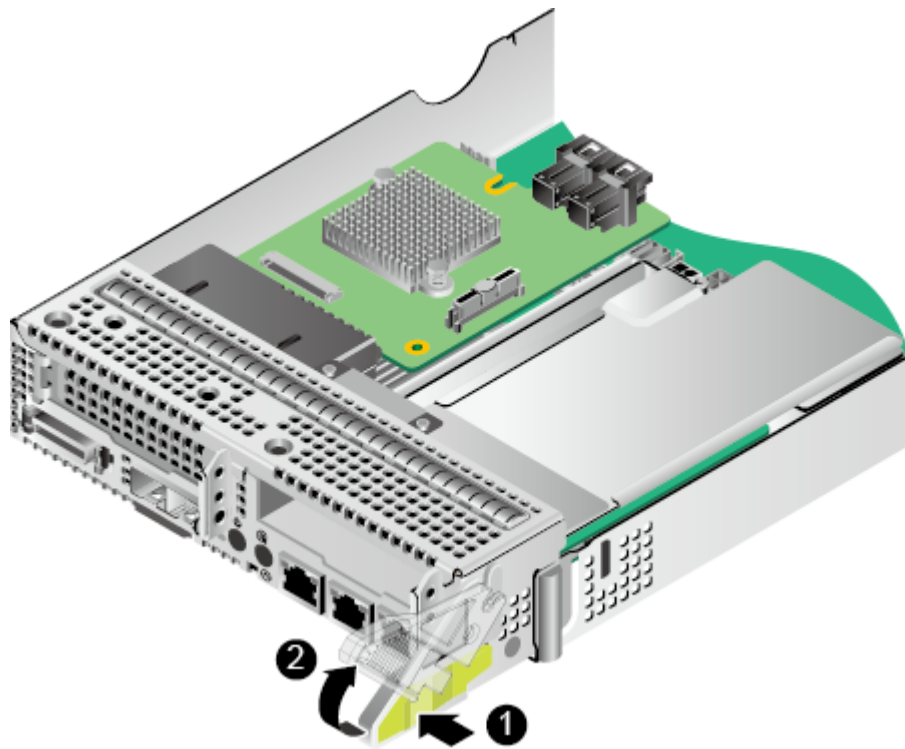
Step 3 Install the server node.

NOTICE

To prevent device damage or personal injury, hold the bottom of the device with both hands when installing it.

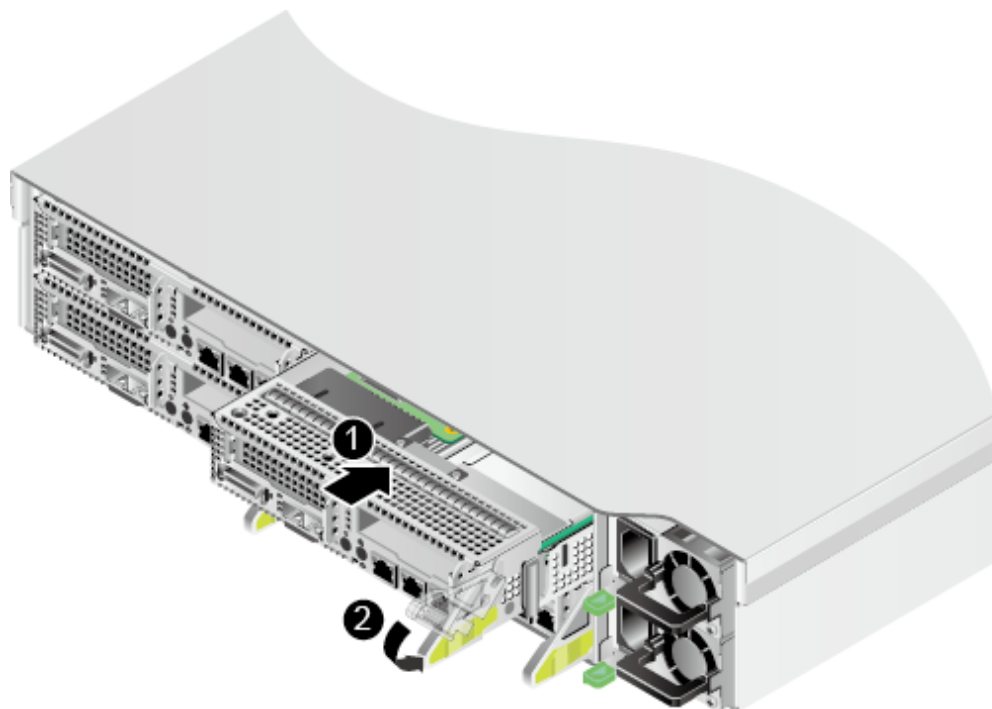
1. Press the ejector release button on the server node. See (1) in [Figure 8-9](#).
2. Fully open the ejector lever. See (2) in [Figure 8-9](#).

Figure 8-9 Opening the ejector lever



3. Slide the server node into the chassis horizontally. See (1) in [Figure 8-10](#).
4. Close the ejector lever. See (2) in [Figure 8-10](#).

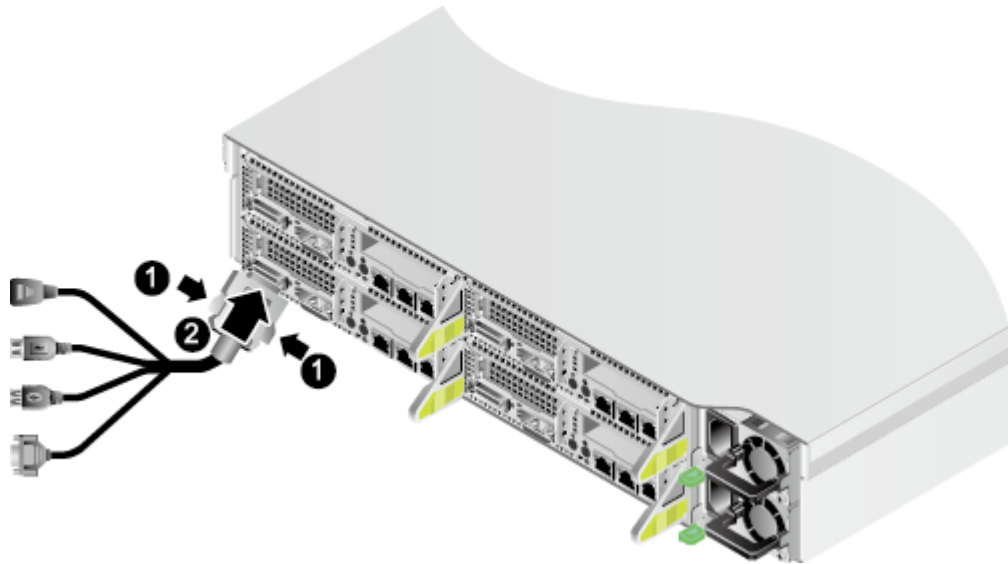
Figure 8-10 Installing a server node



Step 4 Connect the multi-port cable as required.

1. Press the two tabs on the multi-port cable connector. See (1) in [Figure 8-11](#).
2. Connect the multi-port cable to the UCP on the server. See (2) in [Figure 8-11](#).

Figure 8-11 Connecting a multi-port cable



Step 5 Install optical modules and optical cable as required.

NOTICE

Replacing the optical cable, network cable, or optical module will interrupt services.

1. Close the security pin on the optical module, use die-casting pliers to clamp the optical module, and insert it into the optical port until you hear a click.
2. Use die-casting pliers to clamp the optical connector, and insert it into the optical port of an optical module until you hear a click.

Step 6 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 7 Check indicator status.

For details, see [2.1.2 Indicators and Buttons](#).

----End

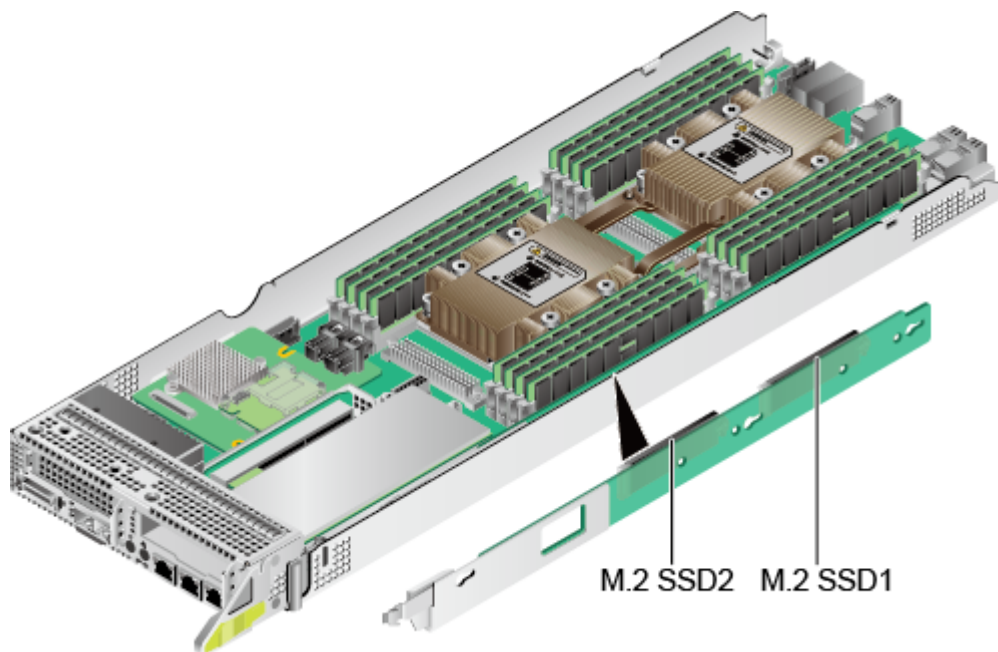
8.4 Field Replaceable Units

8.4.1 Removing an M.2 SSD

Procedure

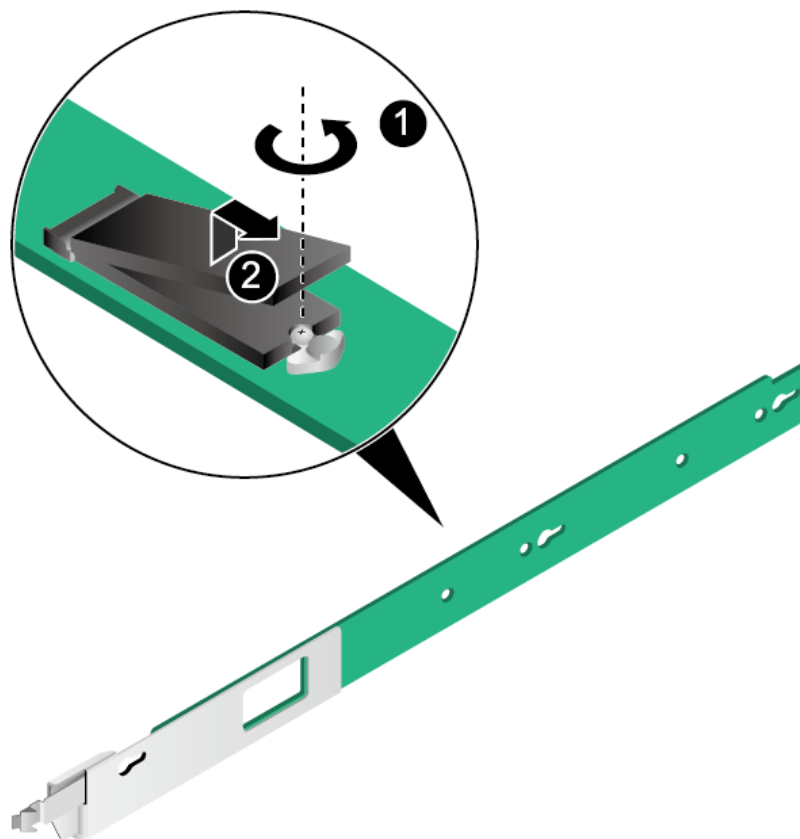
- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Remove the air duct.
For details, see [8.4.23 Removing the Air Duct](#).
- Step 5** Determine the position of the M.2 SSD.

Figure 8-12 Positions of M.2 SSDs



- Step 6** Remove the TPM.
For details, see [8.4.15 Removing the TPM](#).
- Step 7** Remove the M.2 SSD.
1. Use an M2.5 Phillips screwdriver to loosen the screw that secures the M.2 SSD. See (1) in [Figure 8-13](#).
 2. Tilt the M.2 SSD 20° to 30° upwards, and pull it out. See (2) in [Figure 8-13](#).

Figure 8-13 Removing an M.2 SSD



Step 8 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

----End

8.4.2 Installing an M.2 SSD

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

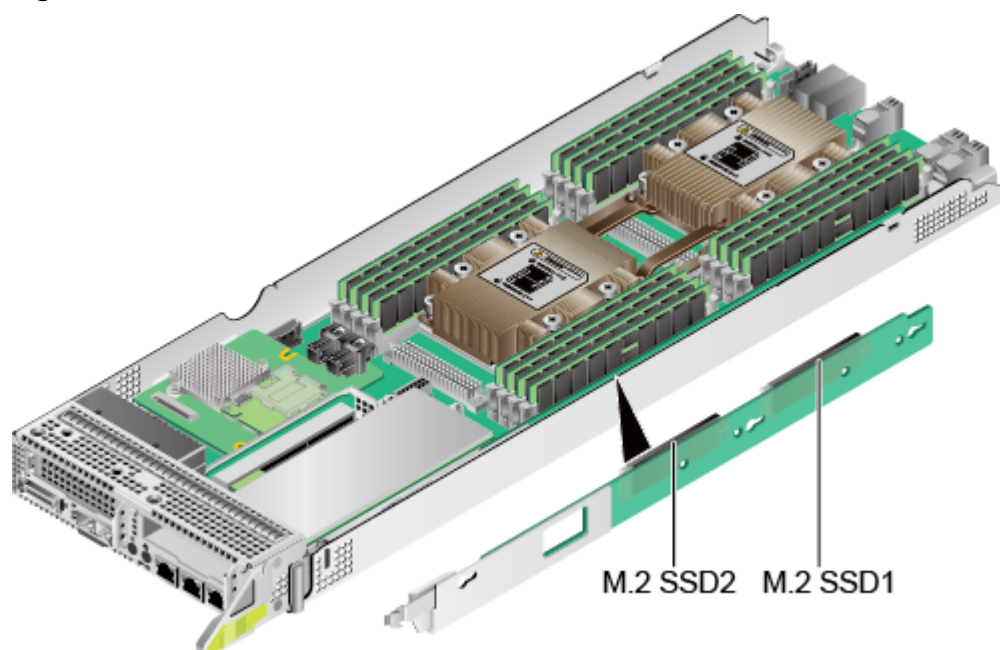
Step 3 Place the server node on the ESD workstation.

Step 4 Remove the air duct.

For details, see [8.4.23 Removing the Air Duct](#).

Step 5 Determine the position of the M.2 SSD.

Figure 8-14 Positions of M.2 SSDs



Step 6 Remove the TPM.

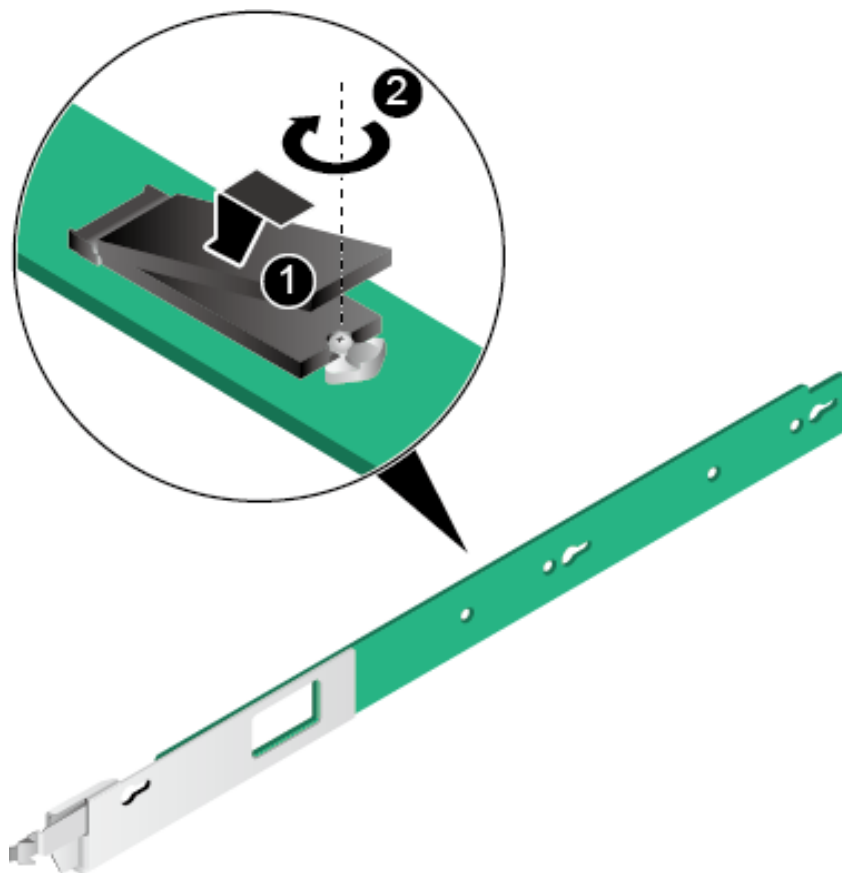
For details, see [8.4.15 Removing the TPM](#).

Step 7 Take the component out of its ESD bag.

Step 8 Install the M.2 SSD.

1. Tilt the M.2 SSD 20° to 30°, install it in the slot, and press it firmly. See (1) in [Figure 8-15](#).
2. Use an M2.5 Phillips screwdriver to tighten the screw to secure the M.2 SSD. See (2) in [Figure 8-15](#).

Figure 8-15 Installing an M.2 SSD



Step 9 Install the TPM.

For details, see [8.4.16 Installing the TPM](#).

Step 10 Install the air duct.

For details, see [8.4.24 Installing the Air Duct](#).

Step 11 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 12 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

----End

8.4.3 Removing the Screw-in RAID Controller Card

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

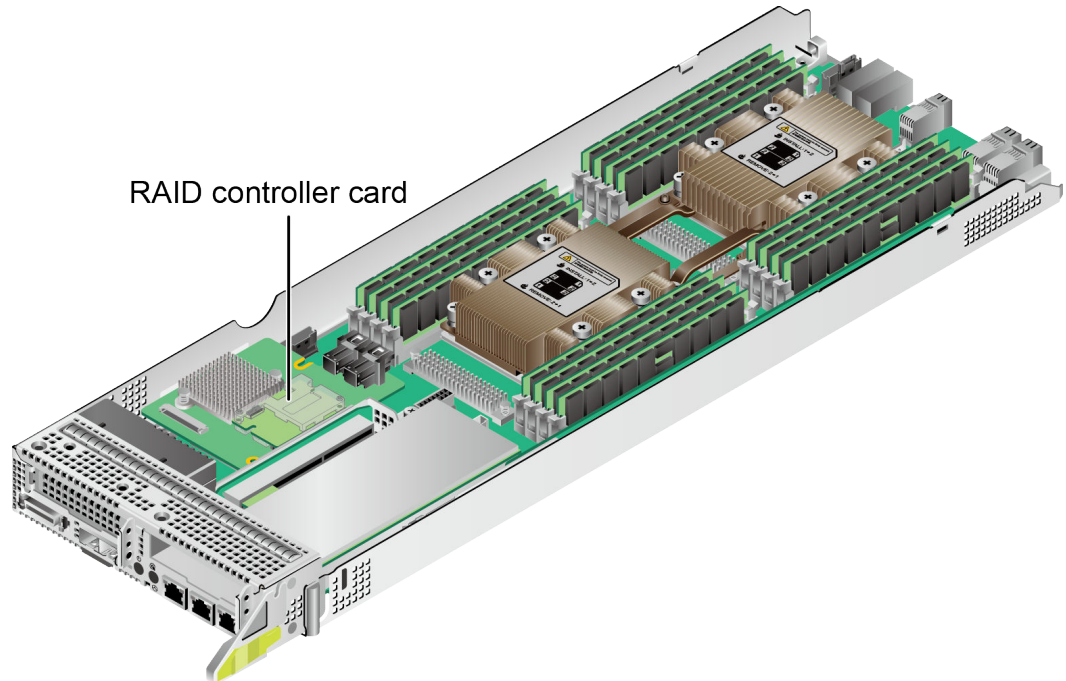
Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

Step 4 Determine the position of the screw-in RAID controller card.

Figure 8-16 Position of the screw-in RAID controller card



Step 5 Check whether a supercapacitor is configured.

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

Step 6 Remove the supercapacitor.

For details, see [8.4.5 Removing a Supercapacitor](#).

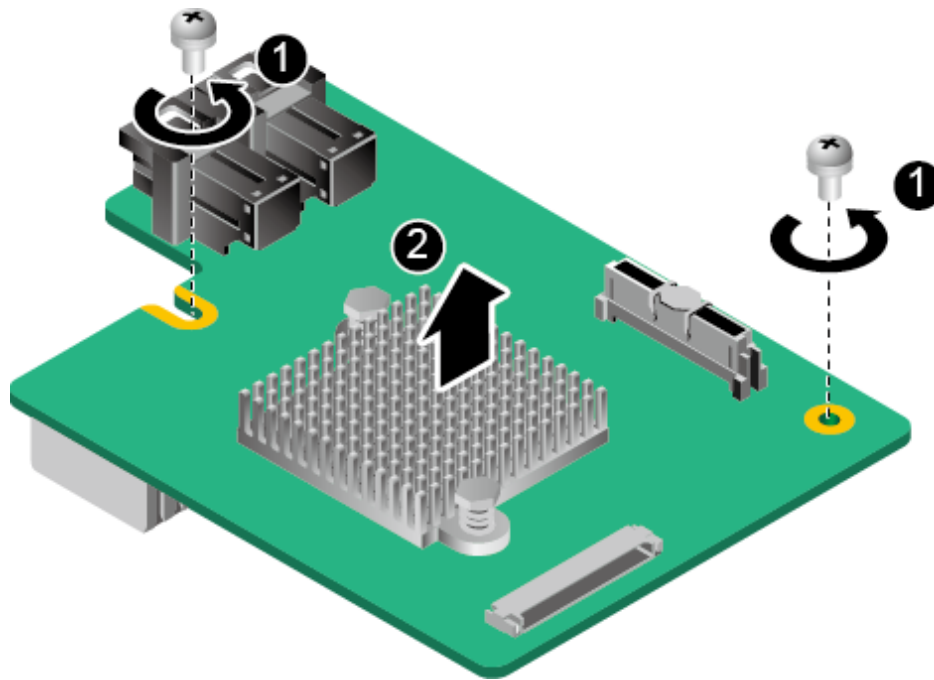
Step 7 Remove the cable from the RAID controller card.

For details, see [7 Internal Cabling](#).

Step 8 Remove the RAID controller card.

1. Loosen the screws that secure the RAID controller card. See (1) in [Figure 8-17](#).
2. Remove the RAID controller card from the connector on the mainboard. See (2) in [Figure 8-17](#).

Figure 8-17 Removing a screw-in RAID controller card



Step 9 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

-----End

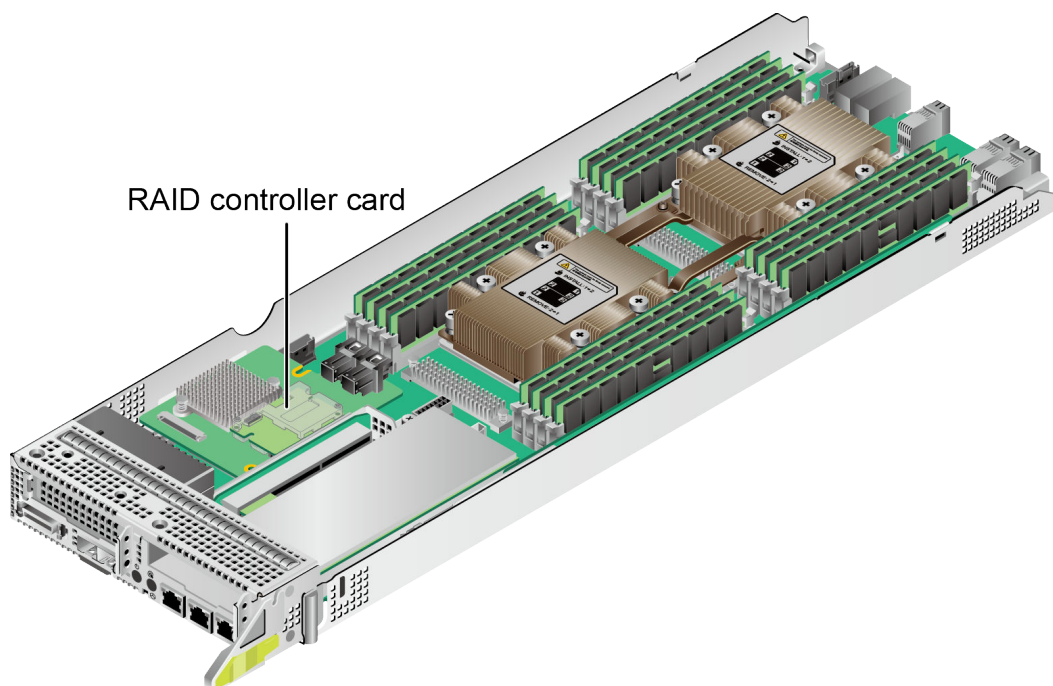
8.4.4 Installing the Screw-in RAID Controller Card

Procedure

- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Take the component out of its ESD bag.
- Step 5** Check whether a supercapacitor is configured.
- If yes, go to [Step 6](#).
 - If no, go to [Step 7](#).
- Step 6** Install the supercapacitor.
For details, see [8.4.6 Installing the Supercapacitor](#).

Step 7 Determine the position of the screw-in RAID controller card.

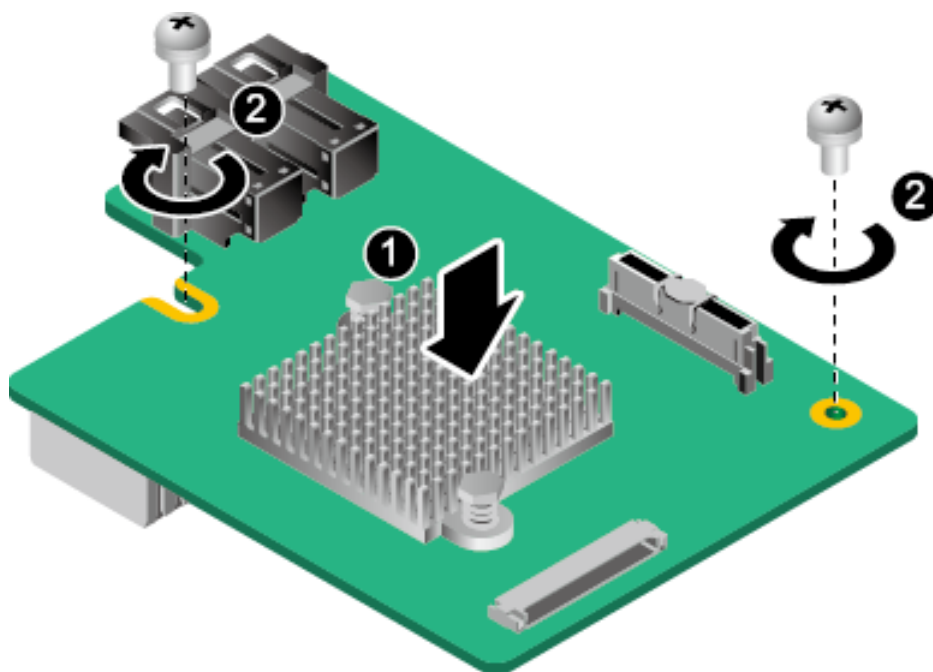
Figure 8-18 Position of the screw-in RAID controller card



Step 8 Install the RAID controller card.

1. Insert the RAID controller card vertically into the connector on the mainboard. See (1) in [Figure 8-19](#).
2. Tighten the screws to secure the RAID controller card. See (2) in [Figure 8-19](#).

Figure 8-19 Installing a screw-in RAID controller card



Step 9 Connect the cable to the RAID controller card.

For details, see [7 Internal Cabling](#).

Step 10 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 11 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 12 Configure the RAID controller card.

For details, see [Huawei V5 Server RAID Controller Card User Guide](#).

Step 13 Upgrade the firmware and driver to the target version.

For details, see [FusionServer Pro High-Density Server Upgrade Guide](#).

-----End

8.4.5 Removing a Supercapacitor

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

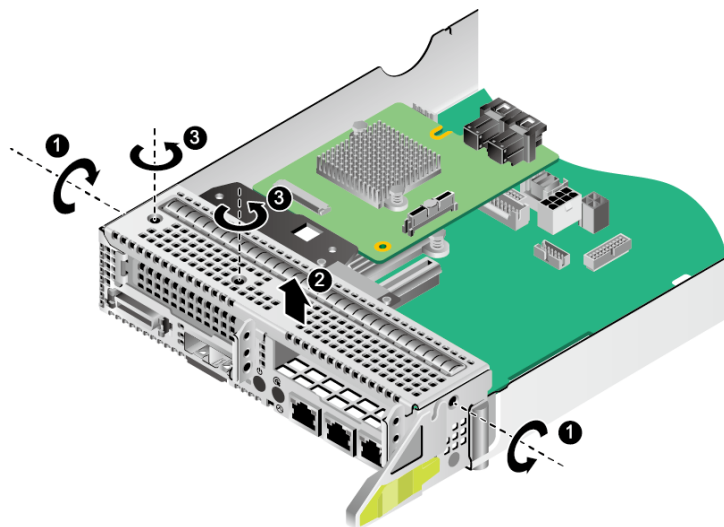
Step 4 Determine the position of the supercapacitor.

Step 5 Remove the air duct for the supercapacitor.

Step 6 Remove the supercapacitor and its holder.

1. Loosen the screws on the server node panel. See (1) in [Figure 8-20](#).
2. Remove the panel. See (2) in [Figure 8-20](#).
3. Loosen the screws that secure the supercapacitor holder and remove the supercapacitor holder. See (3) in [Figure 8-20](#).

Figure 8-20 Removing a supercapacitor holder



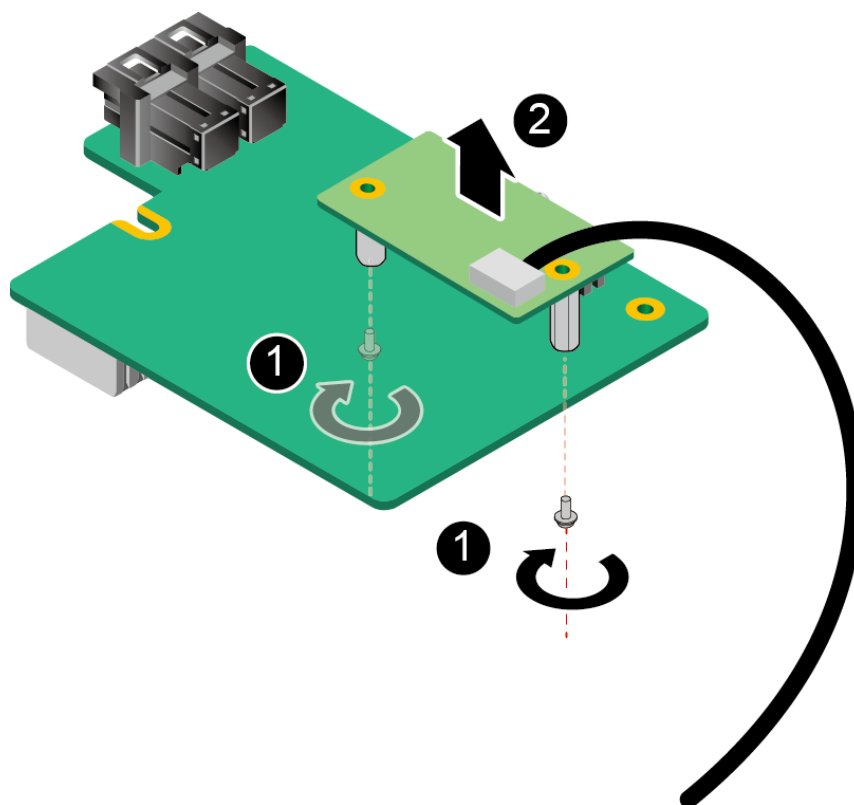
Step 7 Check whether the supercapacitor is configured with a TFM.

- If yes, go to [Step 8](#).
- If no, go to [Step 9](#).

Step 8 Remove the TFM.

1. Remove the screw-in RAID controller card.
For details, see [8.4.3 Removing the Screw-in RAID Controller Card](#).
2. Unscrew the TFM on the screw-in RAID controller card. See (1) in [Figure 8-21](#).
3. Remove the TFM from the RAID controller card. See (2) in [Figure 8-21](#).

Figure 8-21 Removing a TFM

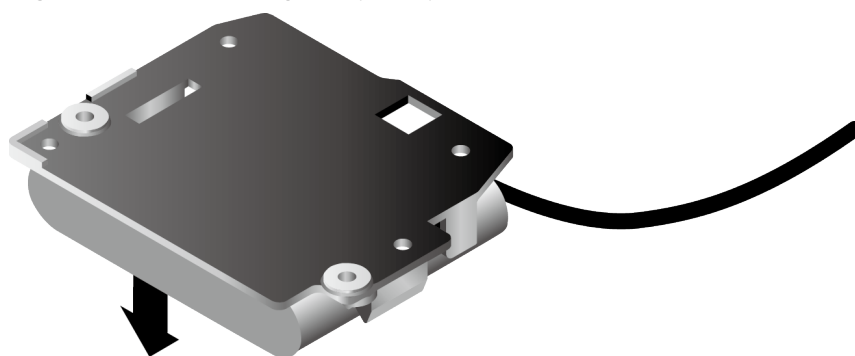


4. Go to [Step 10](#).

Step 9 Remove the cable between the supercapacitor and the RAID controller card.

Step 10 Remove the supercapacitor from the holder.

Figure 8-22 Removing a supercapacitor



Step 11 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

----End

8.4.6 Installing the Supercapacitor

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

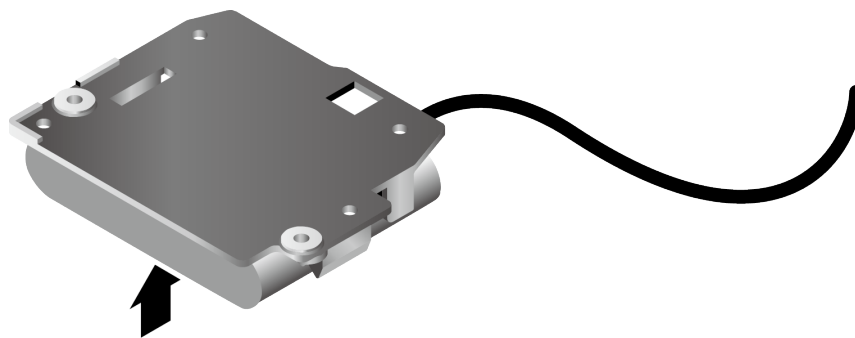
Step 3 Place the server node on the ESD workstation.

Step 4 Take the component out of its ESD bag.

Step 5 Determine the position of the supercapacitor.

Step 6 Vertically insert the supercapacitor into the holder until the supercapacitor is locked.

Figure 8-23 Installing a supercapacitor



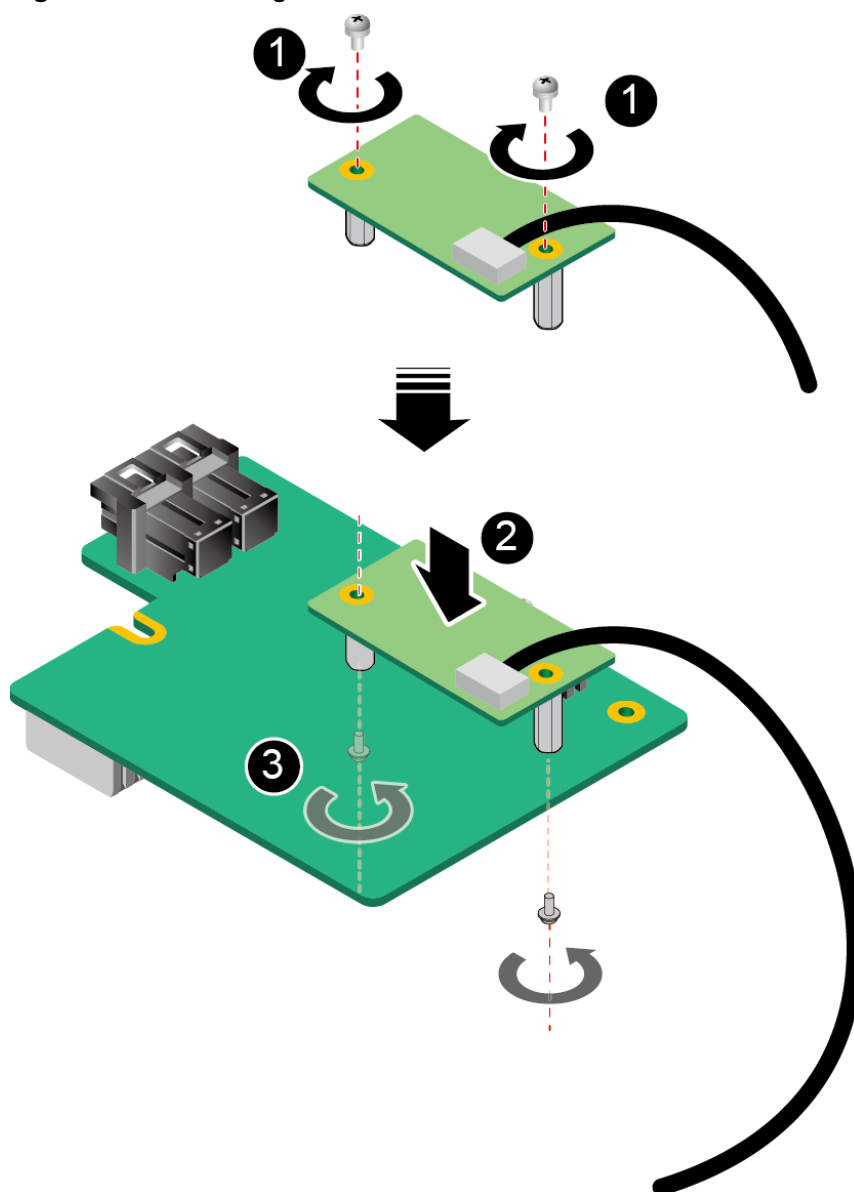
Step 7 Check whether the supercapacitor is configured with a TFM.

- If yes, go to [Step 8](#).
- If no, go to [Step 9](#).

Step 8 Install the TFM.

1. Remove the screw-in RAID controller card.
For details, see [8.4.3 Removing the Screw-in RAID Controller Card](#).
2. Install studs on the TFM. See (1) in [Figure 8-24](#).
3. Insert the TFM into the screw-in RAID controller card. See (2) in [Figure 8-24](#).
4. Tighten the screws to secure the TFM. See (3) in [Figure 8-24](#).

Figure 8-24 Installing a TFM



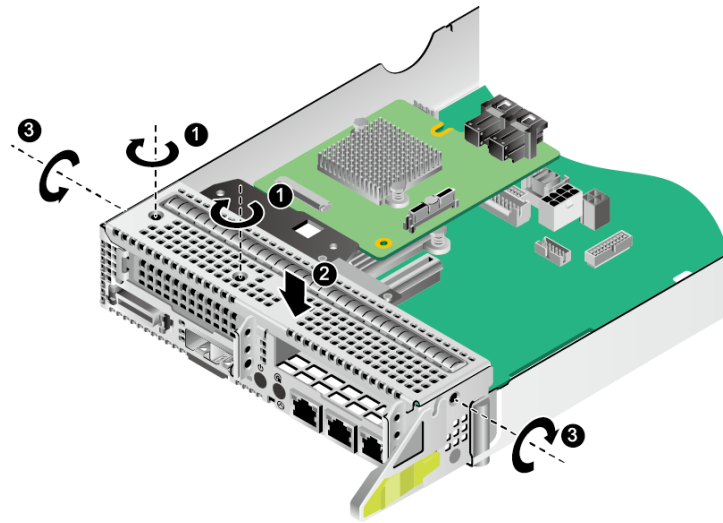
5. Install the screw-in RAID controller card.
For details, see [8.4.4 Installing the Screw-in RAID Controller Card](#).
6. Go to [Step 10](#).

Step 9 Connect the cable between the supercapacitor and the screw-in RAID controller card.

Step 10 Install the supercapacitor and its holder.

1. Install the supercapacitor holder into the node panel and tighten the screws to secure the supercapacitor holder. See (1) in [Figure 8-25](#).
2. Install the node panel. See (2) in [Figure 8-25](#).
3. Tighten the screws to secure the panel. See (3) in [Figure 8-25](#).

Figure 8-25 Installing a supercapacitor holder



Step 11 Install the air duct for the supercapacitor.

Step 12 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 13 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

----End

8.4.7 Removing the Avago SAS3004iMR PCIe RAID Controller Card

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

Step 4 Determine the position of the Avago SAS3004iMR RAID controller card.

Step 5 Remove the M.2 FRU from the Avago SAS3004iMR RAID controller card.

For details, see [8.4.9 Removing an M.2 FRU on the Avago SAS3004iMR PCIe RAID Controller Card](#).

Step 6 Remove the Avago SAS3004iMR RAID controller card.

For details, see [8.4.19 Removing a PCIe Card](#).

Step 7 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

----End

8.4.8 Installing the Avago SAS3004iMR PCIe RAID Control Card

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

Step 4 Take the component out of its ESD bag.

Step 5 Determine the position of the Avago SAS3004iMR RAID controller card.

Step 6 Install the Avago SAS3004iMR RAID controller card.

For details, see [8.4.20 Installing a PCIe Card](#).

Step 7 Install the M.2 FRU on the Avago SAS3004iMR RAID controller card.

For details, see [8.4.10 Installing an M.2 FRU on the Avago SAS3004iMR PCIe RAID Controller Card](#).

Step 8 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 9 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 10 Upgrade the firmware and driver to the target version.

For details, see [FusionServer Pro High-Density Server Upgrade Guide](#).

----End

8.4.9 Removing an M.2 FRU on the Avago SAS3004iMR PCIe RAID Controller Card

The M.2 FRU on the Avago SAS3004iMR RAID controller card is hot swappable.

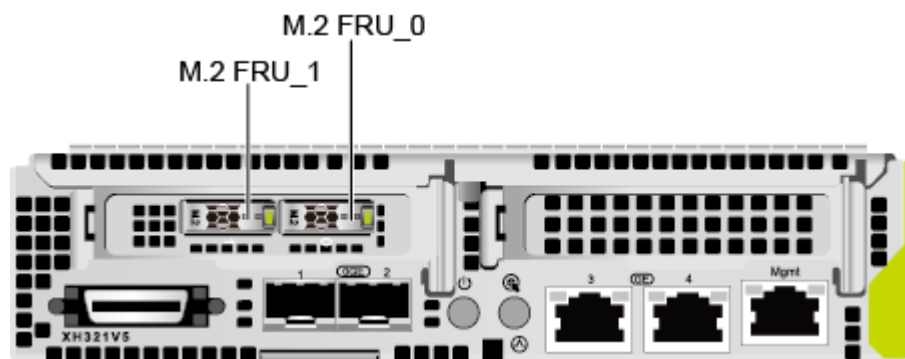
 NOTE

- The M.2 FRU on the Avago SAS3004iMR RAID controller card is hot swappable:
 - If the drive to be removed has no operating system installed, you can remove it without powering off the server node.
 - If the drive to be removed has the operating system installed and is in a RAID array with redundancy, and the removal does not cause a RAID array fault, you can remove it without powering off the server node.
 - If the drive to be removed has the operating system installed but it is not in a RAID array or it is in a RAID array without redundancy (for example, RAID 0), power off the server node before removing it.
- The M.2 FRU on the Avago SAS3004iMR RAID controller card supports RAID configuration:
 - If the drive to be removed is not in a RAID array or is in a RAID array without redundancy (for example, RAID 0), back up the data on the drive before removing it.
 - If the drive to be removed is in a RAID array with redundancy and the removal does not cause a RAID array fault, you do not need to back up data before removing it.

Procedure

- Step 1** Determine the positions and slots of the M.2 FRUs on the Avago SAS3004iMR RAID controller card.

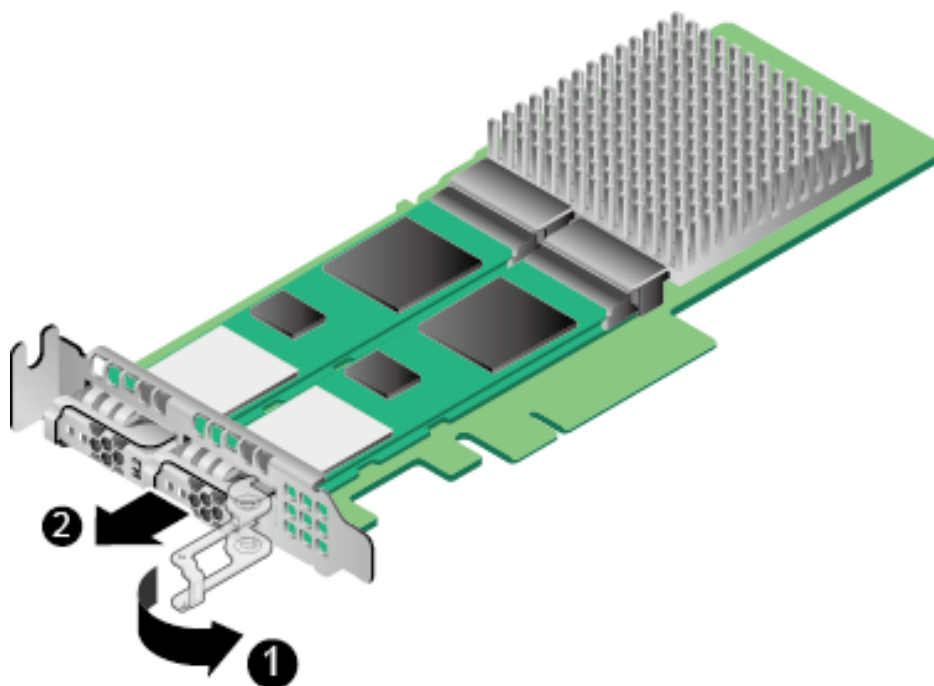
Figure 8-26 Positions and slots of the M.2 FRUs



- Step 2** Remove the M.2 FRU from the Avago SAS3004iMR RAID controller card.

1. Open the handle of the M.2 FRU. See (1) in [Figure 8-27](#).
2. Remove the M.2 FRU. See (2) in [Figure 8-27](#).

Figure 8-27 Removing an M.2 FRU



Step 3 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

Step 4 Install an M.2 FRU filler module to shield the EMC.

 NOTE

Perform this step only when an M.2 FRU is not installed immediately.

----End

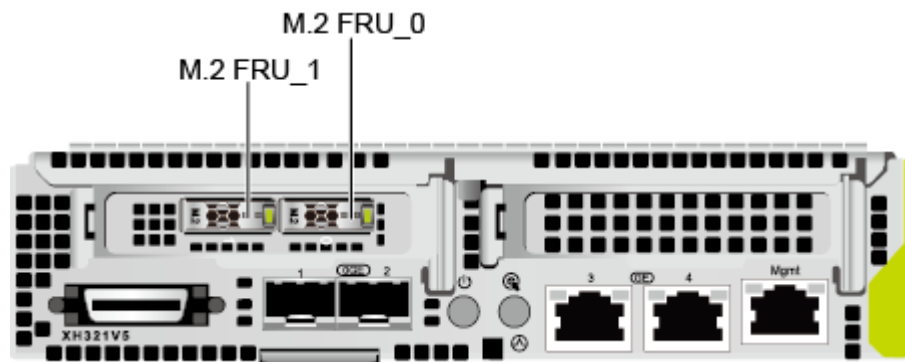
8.4.10 Installing an M.2 FRU on the Avago SAS3004iMR PCIe RAID Controller Card

The M.2 FRU on the Avago SAS3004iMR RAID controller card is hot swappable.

Procedure

Step 1 Determine the positions and slots of the M.2 FRUs on the Avago SAS3004iMR RAID controller card.

Figure 8-28 Positions and slots of the M.2 FRUs



Step 2 Remove the M.2 FRU filler module.

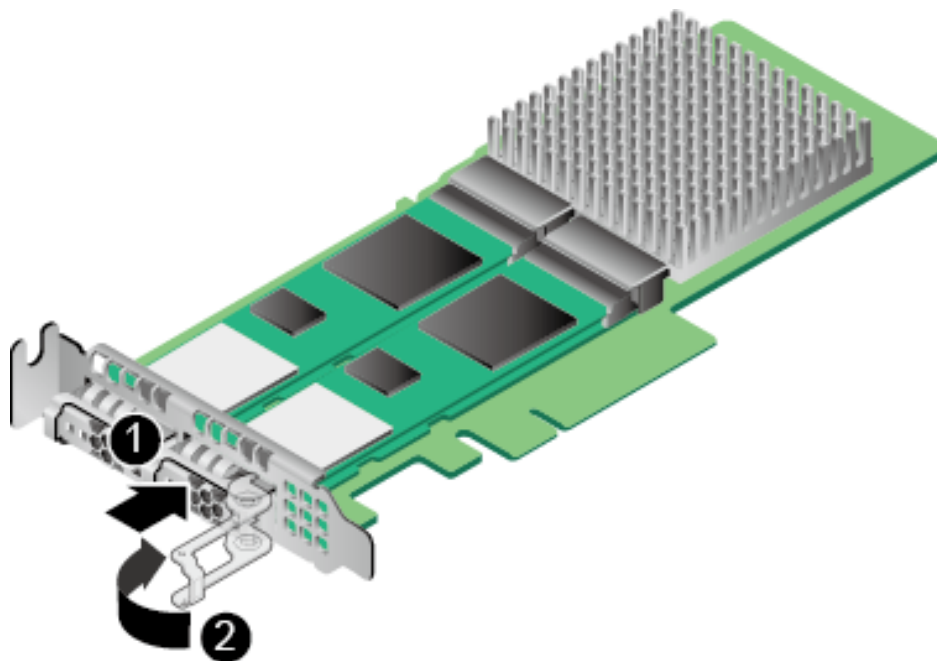
NOTE

Perform this step only when you configure an M.2 FRU filler module.

Step 3 Install an M.2 FRU on the Avago SAS3004iMR PCIe RAID controller card.

1. Take a spare M.2 FRU out of its ESD bag.
2. Open the handle of the M.2 FRU and push the M.2 FRU into the slot of the Avago SAS3004iMR RAID control card. See (1) in [Figure 8-29](#).
3. Close the handle of the M.2 FRU. See (2) in [Figure 8-29](#).

Figure 8-29 Installing an M.2 FRU



Step 4 Check the status of the M.2 FRU indicator on the Avago SAS3004iMR RAID controller card.

Figure 8-30 M.2 FRU indicators

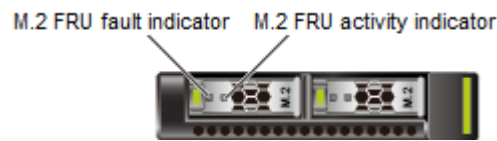


Table 8-2 Indicator status

Indicator	Description
M.2 FRU fault indicator	- Off: The M.2 FRU is running properly. - Blinking yellow: The M.2 FRU is being located, or RAID is being rebuilt. - Steady yellow: The M.2 FRU is faulty or not detected.
M.2 FRU activity indicator	- Off: The M.2 FRU is not in position or is faulty. - Blinking green: Data is being read, written, or synchronized. - Steady green: The M.2 FRU is inactive.

Step 5 Restore the drive data.

 NOTE

Perform this operation only after you replace a drive.

For details, see "Avago SAS3004iMR > Troubleshooting > Hard Drive Fault" in [Huawei V5 Server RAID Controller Card User Guide](#).

----End

8.4.11 Removing a Processor

NOTICE

- Only Huawei technical support or personnel authorized by Huawei can remove the processors from Huawei servers.
- Do not wear ESD gloves during processor replacement. The gloves may catch on pins on the processor socket and damage it.

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

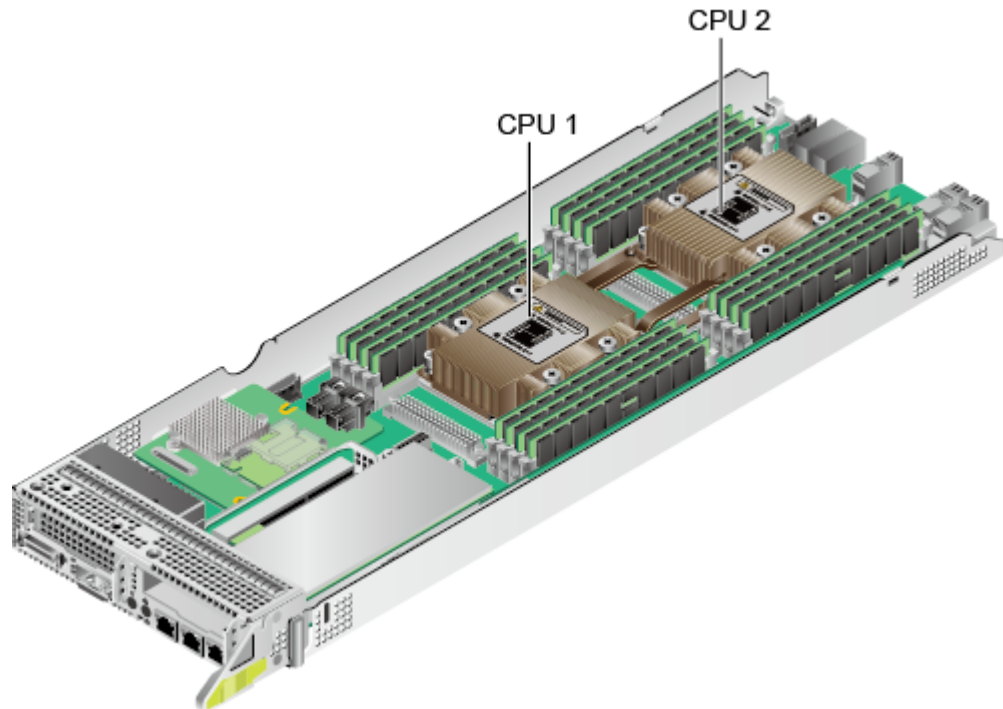
Step 3 Place the server node on the ESD workstation.

Step 4 Remove the air duct.

For details, see [8.4.23 Removing the Air Duct](#).

Step 5 Determine the position of the processor.

Figure 8-31 Positions of processors



Step 6 Remove the conjoined heat sink and processor carrier.

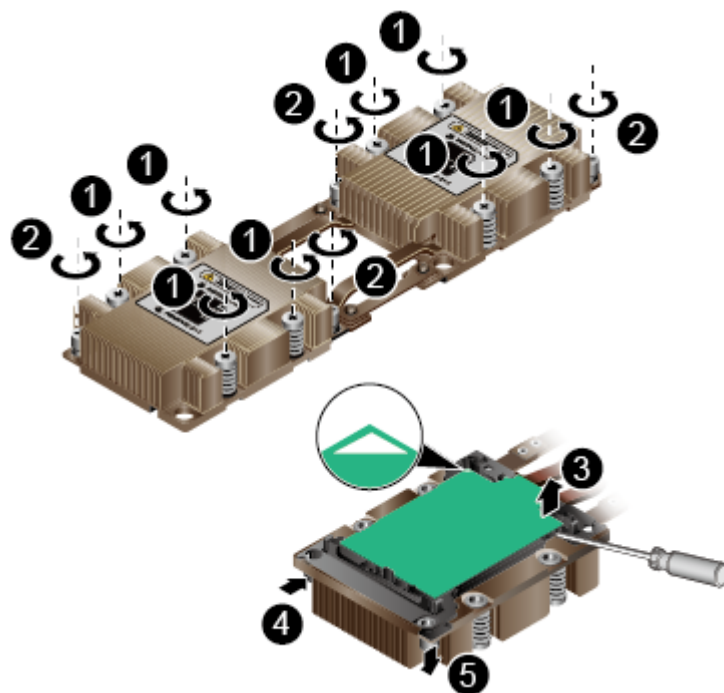
1. Use a Phillips screwdriver to loosen the four screws in the middle of the heat sink in a diagonal sequence.. See (1) in [Figure 8-32](#).
2. Use a Phillips screwdriver to loosen the two diagonal screws on the heat sink.. See (2) in [Figure 8-32](#).
3. Lift the heat sink and place it upside down on the ESD desk.
4. Insert a flat-head screwdriver into the groove of the processor carrier, and twist it to pry up one side of the carrier. See (3) in [Figure 8-32](#).

NOTE

Insert only the tip of the flat-head screwdriver. Do not apply excessive force.

5. Holding the other end of the carrier, remove the carrier and processor in the arrow direction. See (4) and (5) in [Figure 8-32](#).

Figure 8-32 Removing the heat sink and processor carrier

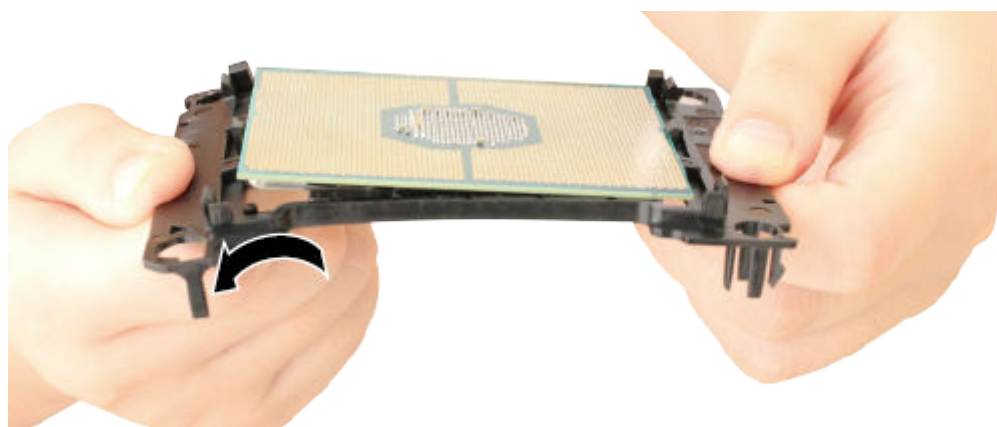


Step 7 Remove the processor.

NOTE

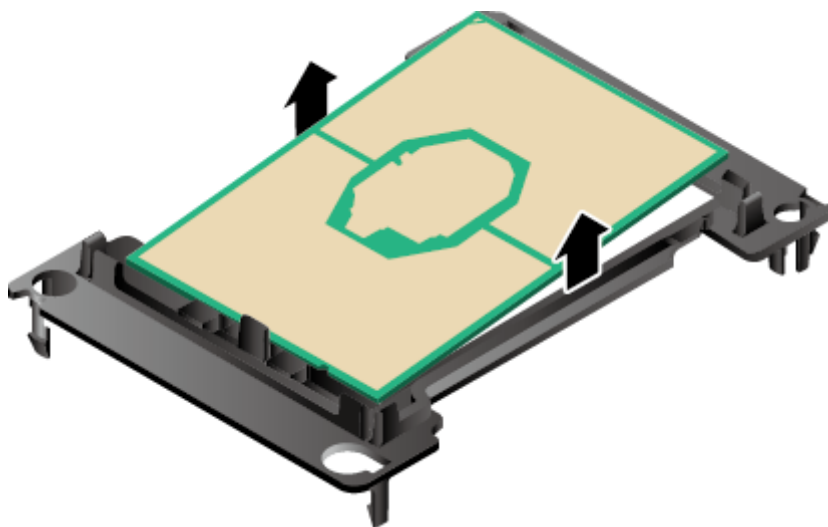
- When removing a processor, hold the processor and its carrier to prevent the processor from falling off.
 - To prevent damage to the pins and processors, do not touch the pins of the processor socket or the corresponding area on the processor.
 - Keep the processor away from the chassis to prevent thermal compound from falling off.
1. Bend the edge of the carrier with the triangular hole to release the processor from the carrier.

Figure 8-33 Removing a processor (1)



2. Hold the two sides of the processor and lift it.

Figure 8-34 Removing a processor (2)



Step 8 Place the removed component in an ESD bag.

 NOTE

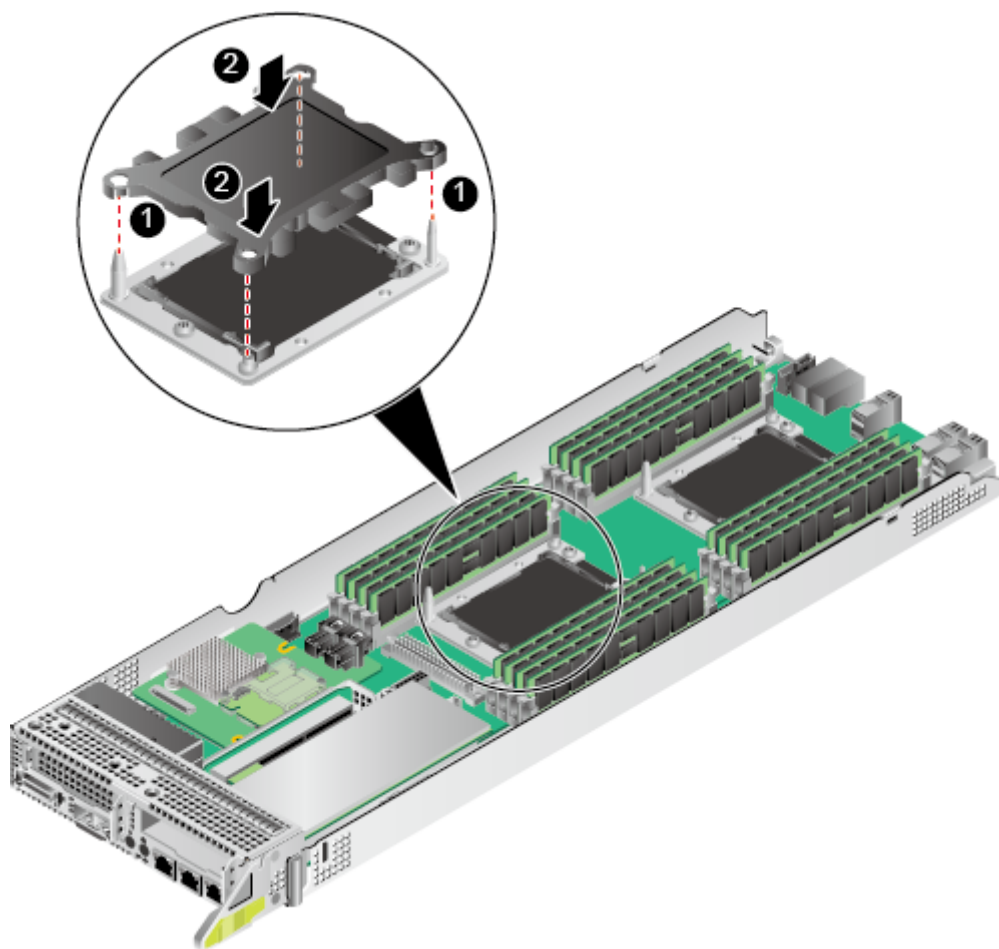
- Clean the thermal compound of the removed processor and put it into an ESD bag.
- Place only one component in an ESD bag.

Step 9 Install a processor socket cover.

 NOTE

- Perform this operation only when a processor is not installed immediately.
 - The processor socket cannot be exposed and must be covered by a processor or cover during transportation and storage.
1. Aligning the processor socket cover with the guide pin on the processor socket, place the cover on the processor socket. See (1) in [Figure 8-35](#).
 2. Press the positions shown by (2) in [Figure 8-35](#) until you hear a click.

Figure 8-35 Installing a CPU socket cover



----End

8.4.12 Installing a Processor

NOTICE

- Only Huawei technical support or personnel authorized by Huawei can install the processors from Huawei servers.
- Do not wear ESD gloves during processor replacement. The gloves may catch on pins on the processor socket and damage it.
- The same model of processors must be used in a server.
- Before installing a processor, clean the surface of the processor, the heat sink, and the processor carrier. If there is residual thermal compound, clean it.

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

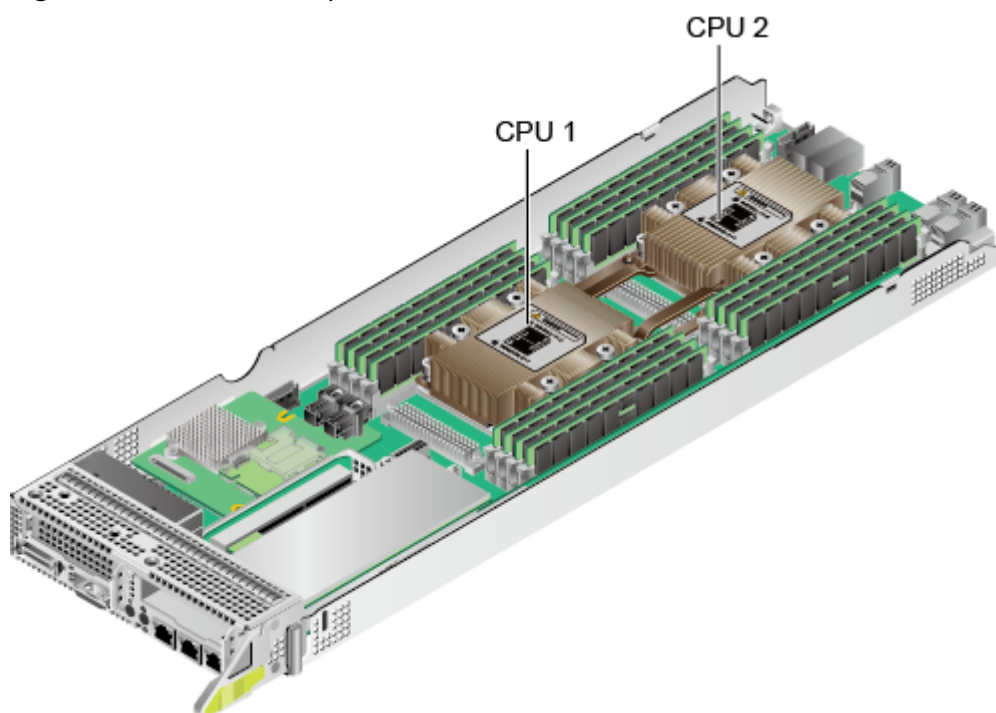
Step 4 Remove the air duct.

For details, see [8.4.23 Removing the Air Duct](#).

Step 5 Take the component out of its ESD bag.

Step 6 Determine the position of the processor.

Figure 8-36 Positions of processors

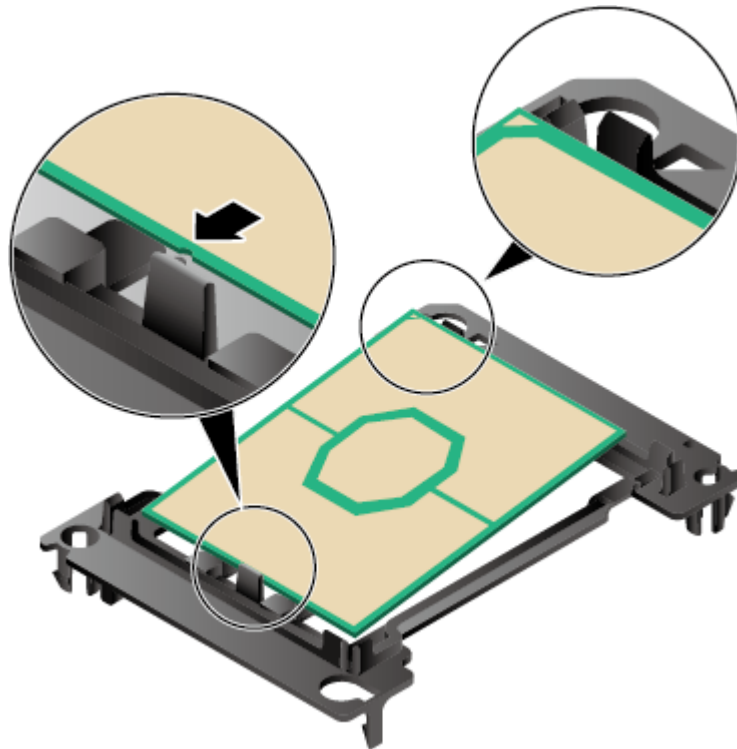


Step 7 Install the processor on the carrier.

1. Take a processor carrier out of an ESD bag.
2. Aligning the notch in one edge of the processor with the protrusion on the processor carrier, secure it.

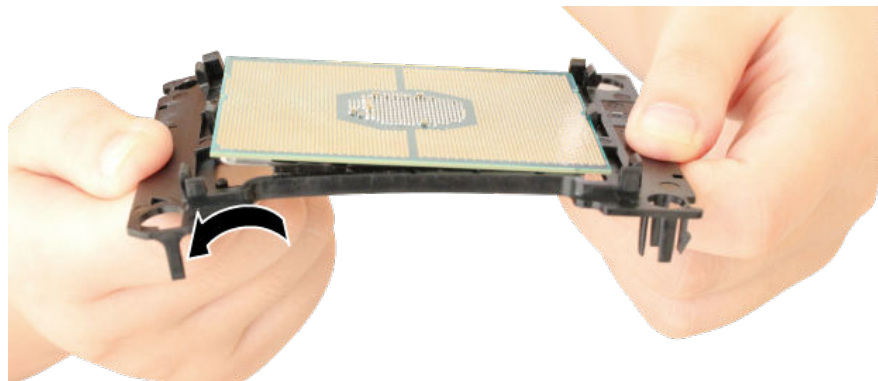
Ensure that the processor corner with a triangle mark is in the corner of the processor carrier with a notched triangle.

Figure 8-37 Installing one end of the processor



3. Bend the other edge of the processor carrier in the arrow direction.

Figure 8-38 Installing the other end of the processor



4. Release the processor carrier so that the other edge of the processor clips into place.
5. Check that the processor and the carrier are level and the processor is firmly secured. If the processor is tilted, gently press the tilted part to fasten it.

Step 8 Apply thermal compound.

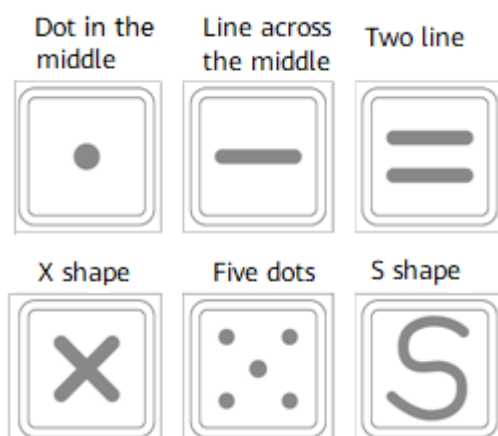
1. Determine the area on the processor that will be in contact with the heat sink, and evenly apply 0.4 ml of thermal compound on the area.

NOTE

- When applying thermal compound, place the processor carrier on the desktop.
- The thermal compound injector has volume marks.

The two-line, five-dot, s-shape, and X-shape patterns are recommended.

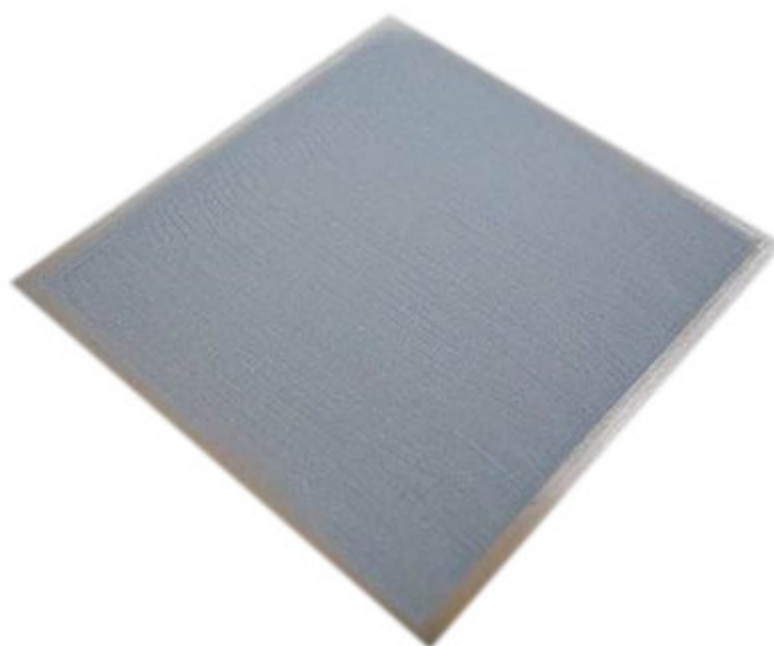
Figure 8-39 Pasting patterns



2. Use a clean card or blade to smear the thermal compound over the entire center of the CPU.

The thickness of the thermal compound is about that of a piece of ordinary paper. Ensure that the thermal compound is evenly and fully coated.

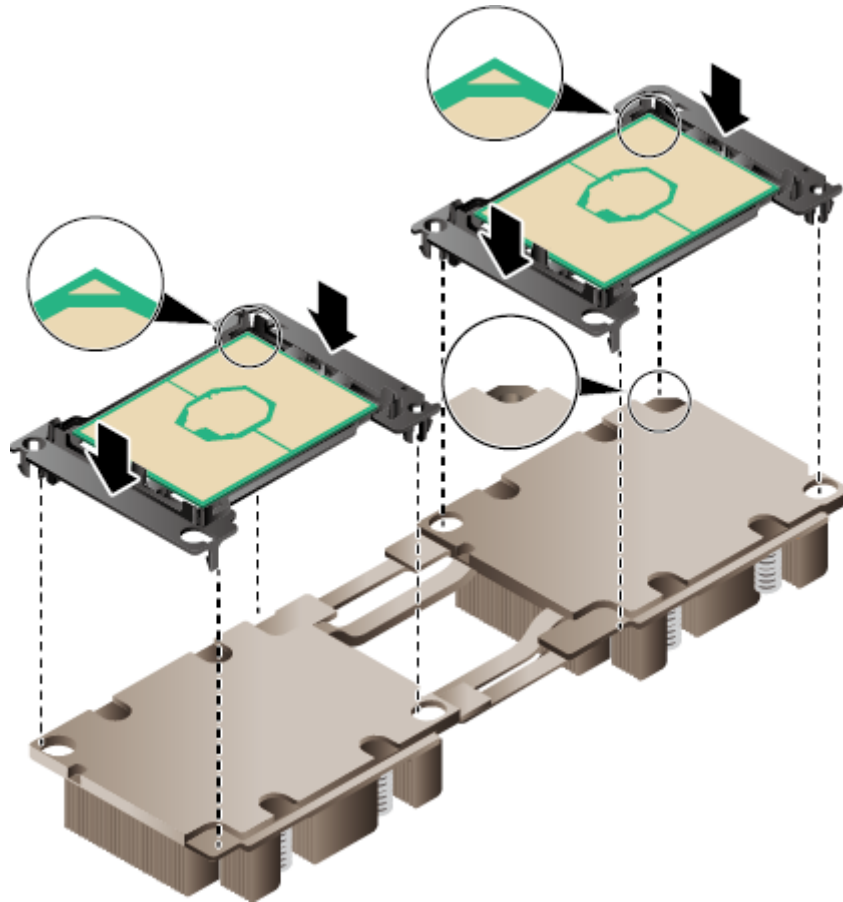
Figure 8-40 Smeared thermal compound layer



Step 9 Install the processor carrier to the conjoined heat sink.

1. Aligning the processor corner with a triangle mark with the corner of the heat sink with a notched triangle, buckle the processor carrier on the heat sink.

Figure 8-41 Installing the processor carrier



2. Place the assembled processor and heat sink upside down on the desk, and check that the processor carrier and the heat sink are firmly secured. If the processor carrier is not firmly buckled with the heat sink, gently press the processor carrier to secure it.

Step 10 Install the processor and conjoined heat sink.

1. Remove the processor socket cover.

NOTICE

When removing the protective cover, pull it out vertically to prevent damage to the pins on the processor socket.

2. Shine a light at various angles onto the processor socket to check for twisted pins, foreign matter, and pad damage.

NOTICE

If bent pins or foreign matters are found or the bonding pad is damaged, stop the operation and contact technical support.

3. Horizontally holding the processor and heat sink, align the notched corner on the heat sink with the notched corner on the processor socket, and place the processor and heat sink downwards on the socket along the guide sleeves.

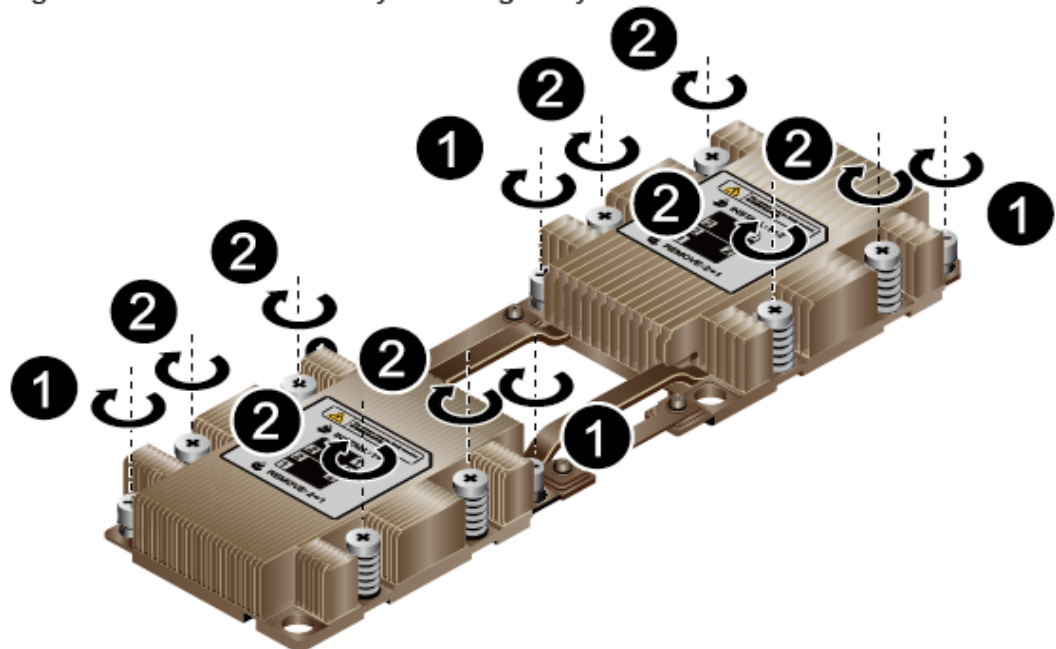
NOTICE

Keep the processor and heat sink parallel with the mainboard to prevent damage to processor socket pins.

4. Use a Phillips screwdriver to tighten the two diagonal screws on the heat sink.. See (1) in [Figure 8-42](#).
5. Use a Phillips screwdriver to tighten the four screws in the middle of the heat sink in a diagonal sequence.. See (2) in [Figure 8-42](#).

Figure 8-42 Installing the heat sink

Tighten the screws until they cannot go any further.



Step 11 Install the air duct.

For details, see [8.4.24 Installing the Air Duct](#).

Step 12 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 13 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

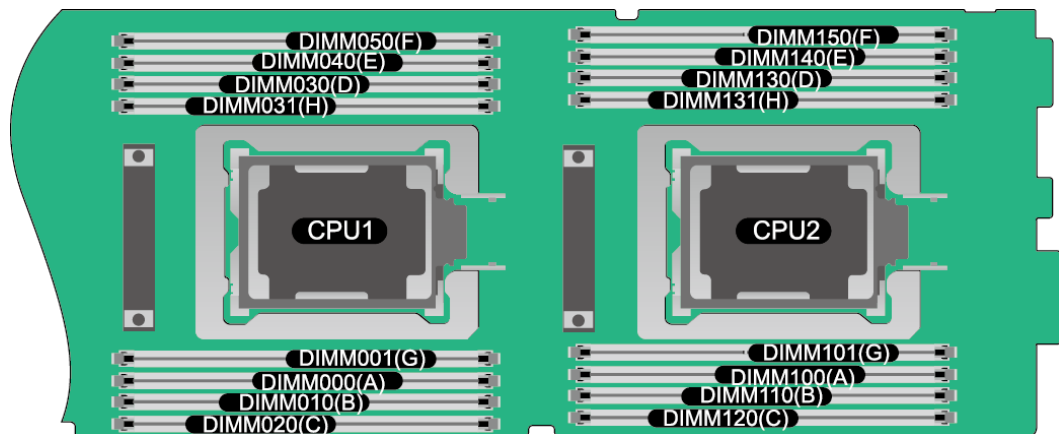
----End

8.4.13 Removing a Memory Module

Procedure

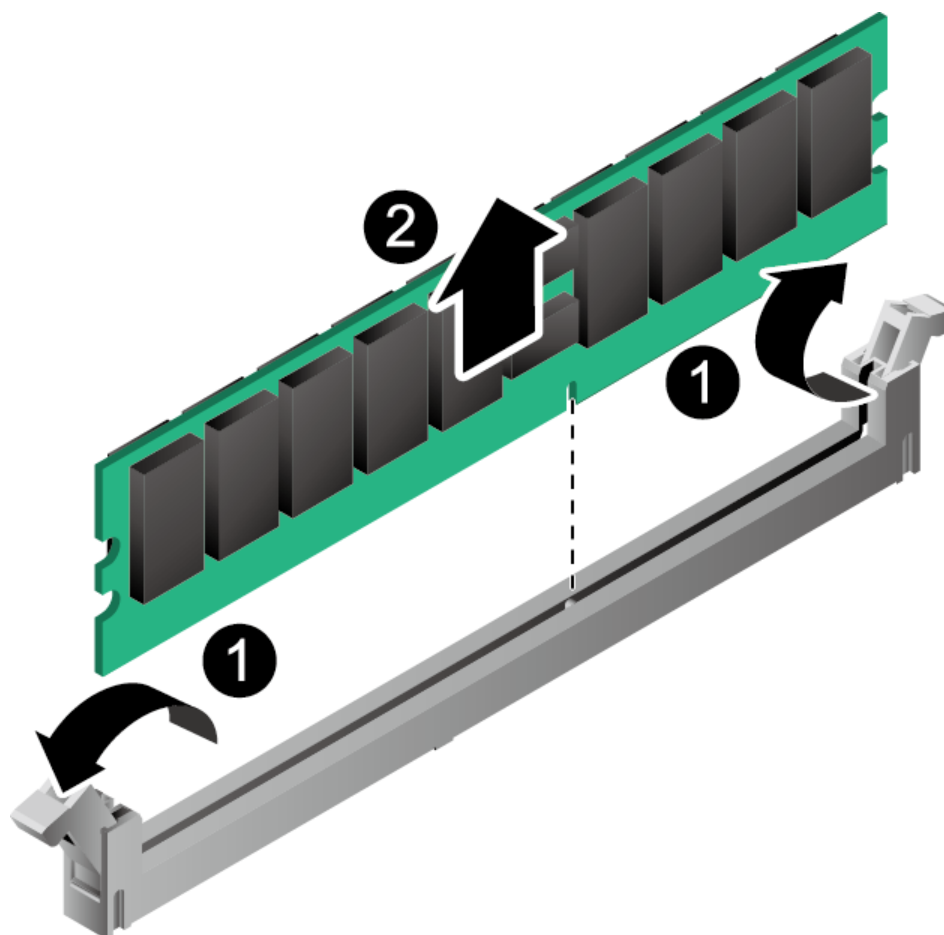
- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Remove the air duct.
For details, see [8.4.23 Removing the Air Duct](#).
- Step 5** Determine the position of the memory module.

Figure 8-43 Memory slots



- Step 6** Remove the memory module.
1. Open the memory module ejectors on the memory slot. See (1) in [Figure 8-44](#).
 2. Remove the memory module from the slot. See (2) in [Figure 8-44](#).

Figure 8-44 Removing a memory module



Step 7 Place the removed memory module in a memory box.

Step 8 Install memory modules.

 NOTE

Perform this operation only when a memory module is not installed immediately.

----End

8.4.14 Installing a Memory Module

NOTICE

Before installing DIMMs, learn about DIMM information, including DIMM compatibility, installation rules, and DIMM slots. For details, see [2.3 Memory](#).

If the processor power is 200 W or 205 W, a wide conjoined heat sink is required, which occupy memory channels DIMM001 and DIMM031.

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

Step 4 Remove the air duct.

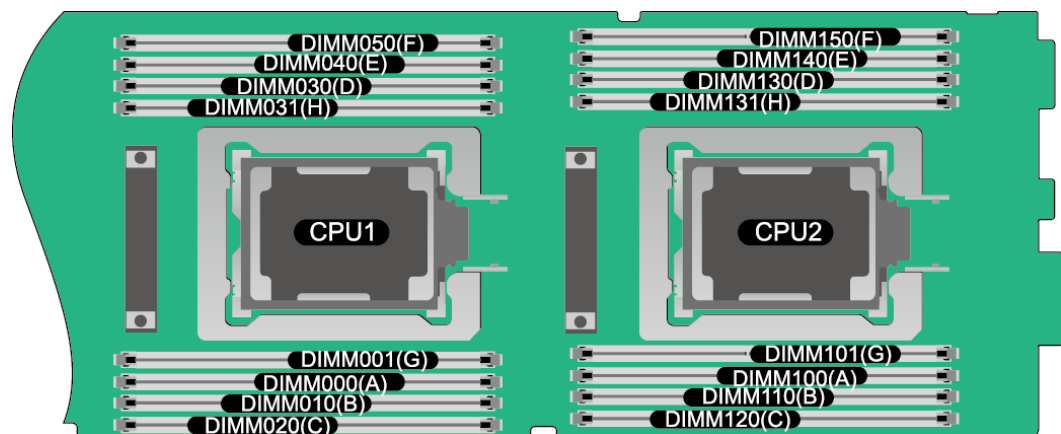
For details, see [8.4.23 Removing the Air Duct](#).

Step 5 Take a spare memory module.

Step 6 Check the positions and installation guidelines of the memory modules.

For details, see [2.3.1.5 Memory Installation Positions](#).

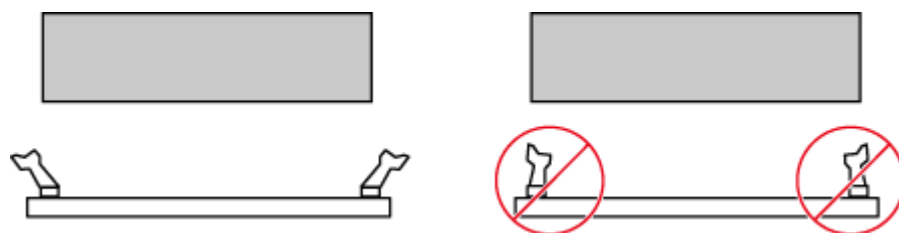
Figure 8-45 Memory slots



Step 7 Install the memory module.

1. Open the two memory module ejectors on the memory slot.

Figure 8-46 Opening the memory module ejectors



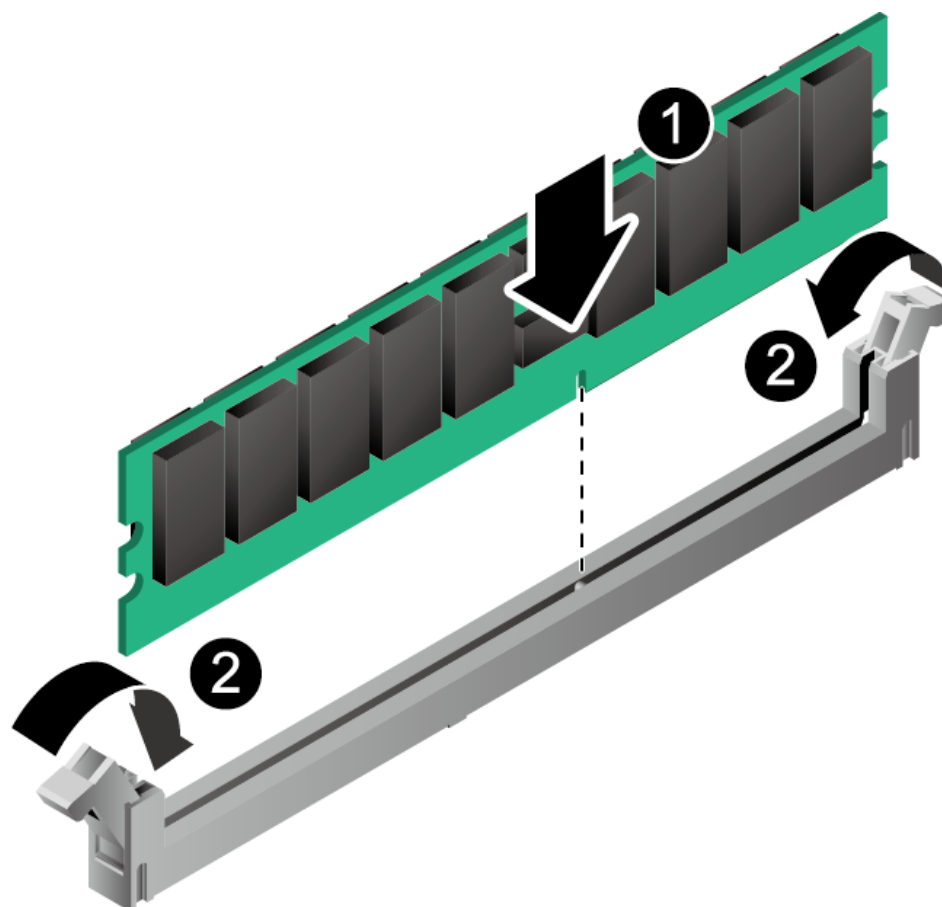
2. Align the edge connector of the memory module with the alignment key of the memory slot, and insert the memory module in the slot.

The two memory ejectors are closed automatically after the memory module is firmly seated.

NOTE

Do not touch the edge connector on a memory module with bare hands. Before installing a memory module, ensure that the edge connector is not contaminated.

Figure 8-47 Installing a memory module



Step 8 Install the air duct.

For details, see [8.4.24 Installing the Air Duct](#).

Step 9 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 10 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 11 Log in to the iBMC WebUI, and check whether the new component is normal.

For details, see [FusionServer Pro X6000 Server iBMC User Guide](#).

NOTE

- If information about the new memory module is displayed, the replacement is successful.
- If information about the original memory module is displayed, access the BIOS and check memory information.

For details, see [Huawei Server Purley Platform BIOS Parameter Reference](#).

----End

8.4.15 Removing the TPM

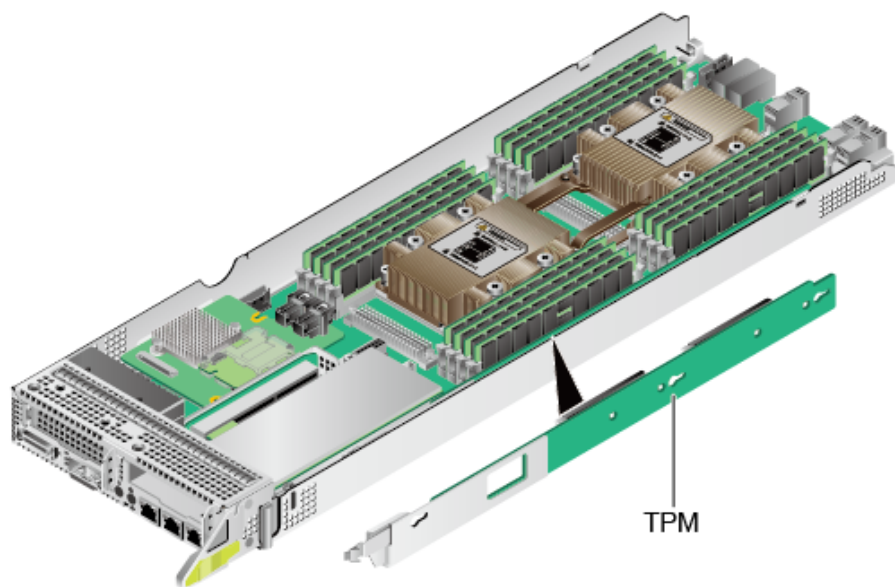
NOTICE

- If the private key of the TPM is used to encrypt data, back up the data before removing the TPM.
If the data is not backed up, the encrypted data cannot be decrypted after the TPM is replaced.
After the data backup is complete, you need to clear the TPM key. For details, see "Security" in [Huawei Server Purley Platform BIOS Parameter Reference](#).
You need to back up and clear data only when the removed TPM is no longer used. If the removed TPM needs to be reinstalled in the original environment, you do not need to back up and clear data.
- If the TPM function has been set on the BIOS, record the settings before removing the TPM. After replacing the TPM, configure the related settings on the BIOS again.
For details, see [Huawei Server Purley Platform BIOS Parameter Reference](#).
- If a broken or disfigured screw is found on a TPM, take appropriate measures to protect data.

Procedure

- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Remove the air duct.
For details, see [8.4.23 Removing the Air Duct](#).
- Step 5** Determine the position of the TPM.

Figure 8-48 Position of the TPM



Step 6 Remove the PCIe riser module.

For details, see [8.4.21 Removing a PCIe Riser Module](#).

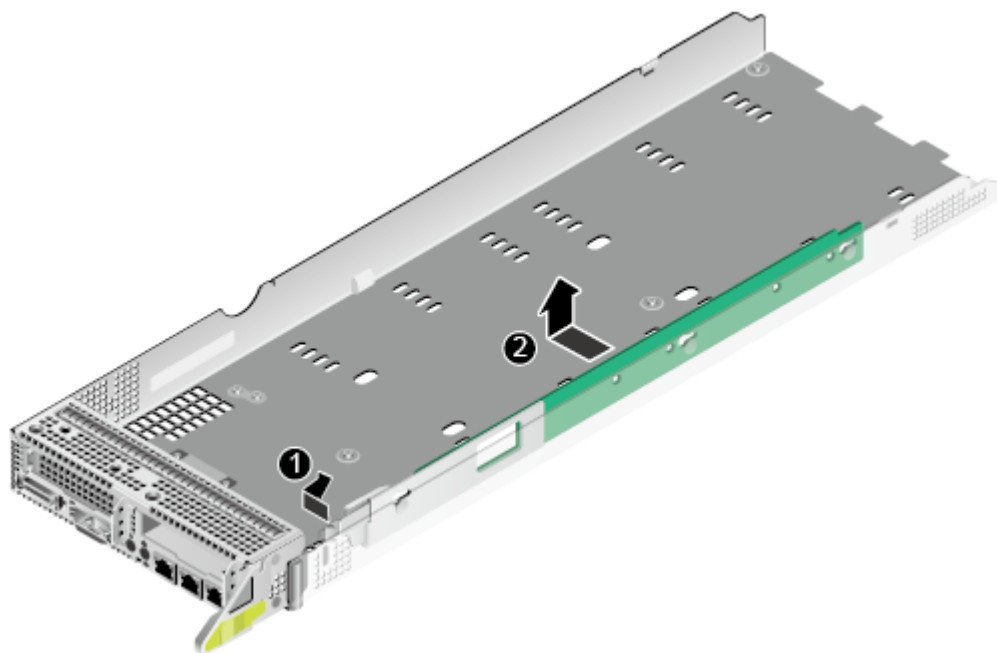
Step 7 Remove the TPM.

1. Remove the cables from the TPM.

For details, see [7.1 TPM Cabling](#).

2. Release the buckle on the TPM in the arrow direction, and push the TPM backwards until it cannot move forward. See (1) in [Figure 8-49](#).
3. Remove the TPM from the dowel pins on the side wall of the server node and take it out upwards. See (2) in [Figure 8-49](#).

Figure 8-49 Removing a TPM



Step 8 Remove M.2 SSDs.

For details, see [8.4.1 Removing an M.2 SSD](#).

Step 9 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

-----End

8.4.16 Installing the TPM

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

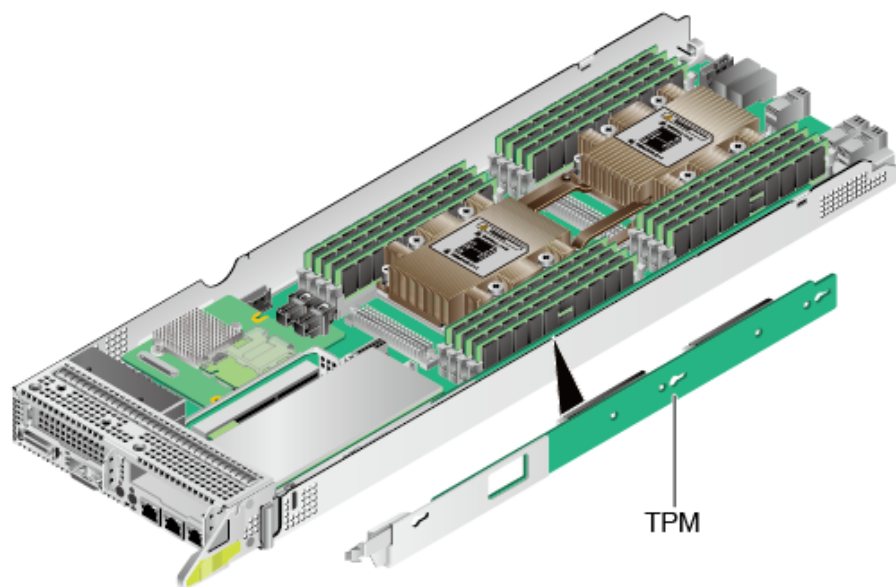
Step 3 Place the server node on the ESD workstation.

Step 4 Remove the air duct.

For details, see [8.4.23 Removing the Air Duct](#).

Step 5 Determine the position of the TPM.

Figure 8-50 Position of the TPM



Step 6 Take the component out of its ESD bag.

Step 7 Remove the PCIe riser module.

For details, see [8.4.21 Removing a PCIe Riser Module](#).

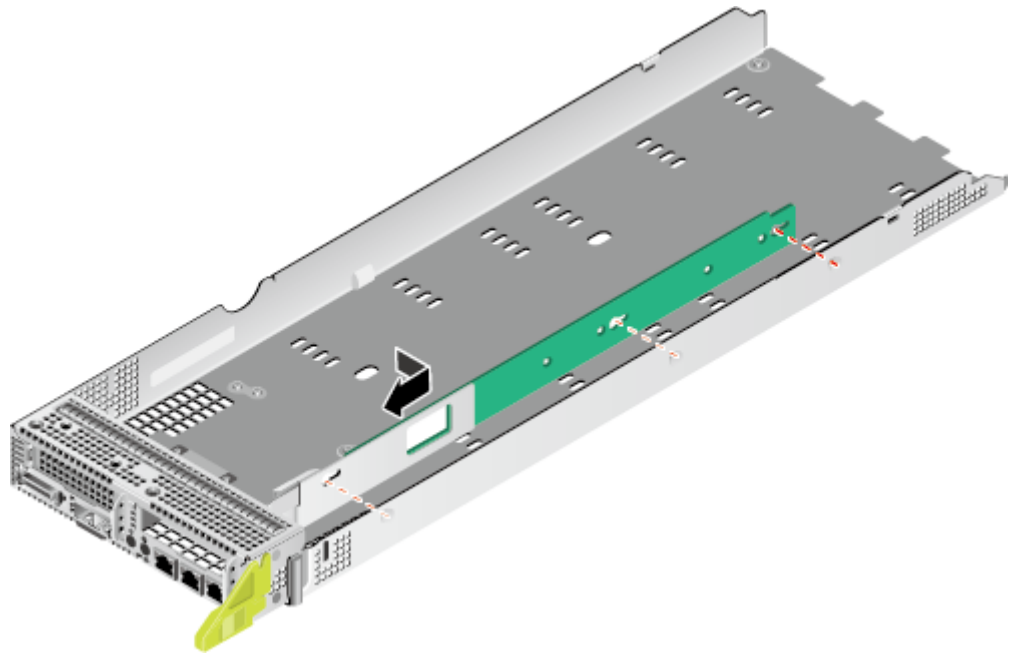
Step 8 Install M.2 SSDs.

For details, see [8.4.2 Installing an M.2 SSD](#).

Step 9 Install the TPM.

1. Align the TPM with the dowel pins on the side wall of the server node, and insert the TPM in the arrow direction.

Figure 8-51 Installing a TPM



2. Connect the cables to the TPM.
For details, see [7.1 TPM Cabling](#).

Step 10 Install the PCIe riser module.

For details, see [8.4.22 Installing a PCIe Riser Module](#).

Step 11 Install the air duct.

For details, see [8.4.24 Installing the Air Duct](#).

Step 12 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 13 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 14 Configure the TPM.

 NOTE

If the TPM 2.0 is installed and the TXT function is enabled, but the TPM 2.0 status on the BIOS is **unknown**, contact technical support.

- If a spare TPM is installed, perform the following operations:
 - a. Set the TPM configuration items on the BIOS to ensure that the TPM settings are the same as the recorded TPM settings. For details, see [Huawei Server Purley Platform BIOS Parameter Reference](#).
 - b. Restore the backup data on the spare TPM to overwrite its factory settings.
- If a removed TPM is reinstalled, perform the following operations:
 - a. Check whether the BIOS version of the mainboard where the TPM is located is earlier than that before the removal.

- If yes, upgrade the BIOS version to ensure that the BIOS version of the mainboard where the TPM is located is not earlier than that before the removal. For details, see [FusionServer Pro High-Density Servers Upgrade Guide](#).
- If no, go to [Step 14.b](#).
- b. Set the TPM configuration items on the BIOS to ensure that the TPM settings are the same as the recorded TPM settings. For details, see [Huawei Server Purley Platform BIOS Parameter Reference](#).

----End

8.4.17 Removing the Battery

Procedure

Step 1 Confirm the BIOS configuration.



CAUTION

After the battery is replaced, the original BIOS configuration will be lost. If the current BIOS parameters have been adjusted based on service scenarios, ensure that the parameter configuration is the same as that before the battery is replaced to ensure that services are not affected after the battery is replaced.

Step 2 Export the BIOS configuration file.

For details, see [FusionServer Pro X6000 Server iBMC User Guide](#).



NOTE

- The iBMC 2.32 and later versions support import and export of configuration files.
- The BIOS configuration file exported from the iBMC can be directly imported after the battery is replaced. If the exported configuration file contains ciphertext, change the ciphertext to plaintext and delete the comment tags from the line. For details about how to import and export configurations, see [FusionServer Pro X6000 Server iBMC User Guide](#).
- The BIOS configuration file exported from the iBMC contains the configuration list. For details, see "Configuration File Description" in [FusionServer Pro X6000 Server iBMC User Guide](#).
- If the iBMC cannot be logged in to or the BIOS configuration file is not exported before the battery is replaced, you need to manually reconfigure the BIOS after replacing the battery.

Step 3 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

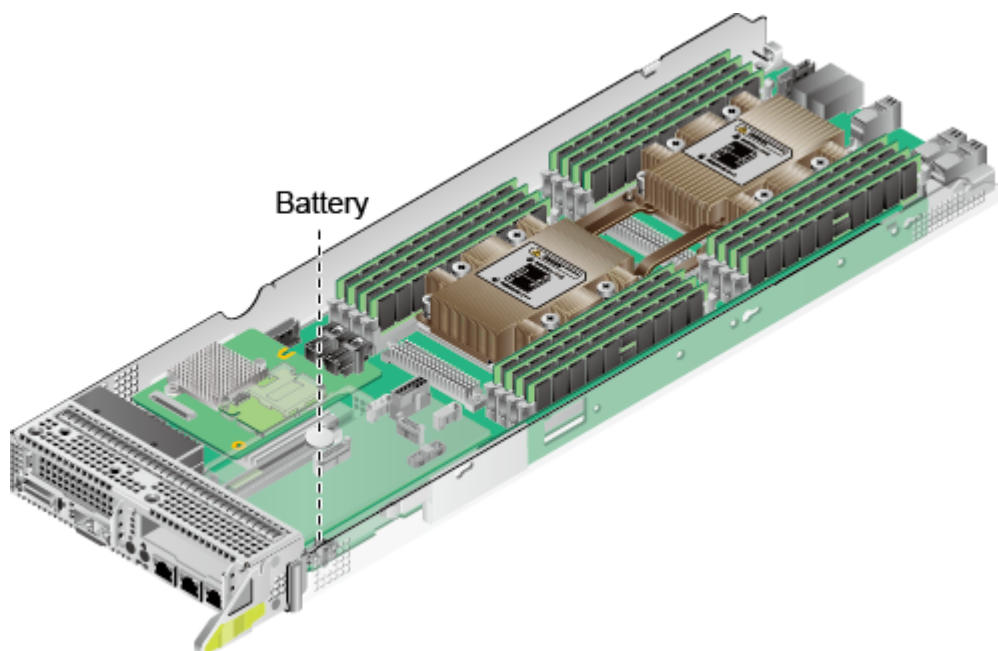
Step 4 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 5 Place the server node on the ESD workstation.

Step 6 Determine the position of the battery.

Figure 8-52 Position of the battery

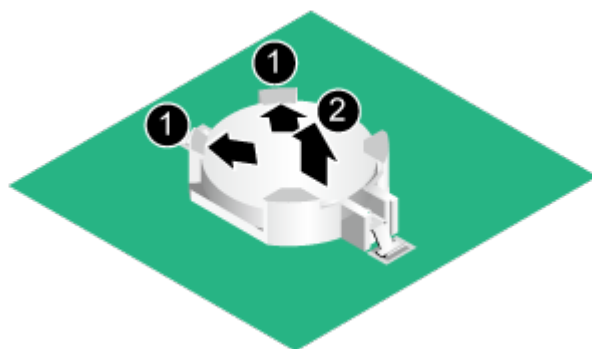


Step 7 Remove the PCIe riser module.

For details, see [8.4.21 Removing a PCIe Riser Module](#).

Step 8 Press and hold the two latches outwards until the battery ejects, and remove the battery vertically. See (1) and (2) in [Figure 8-53](#).

Figure 8-53 Removing the battery



Step 9 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

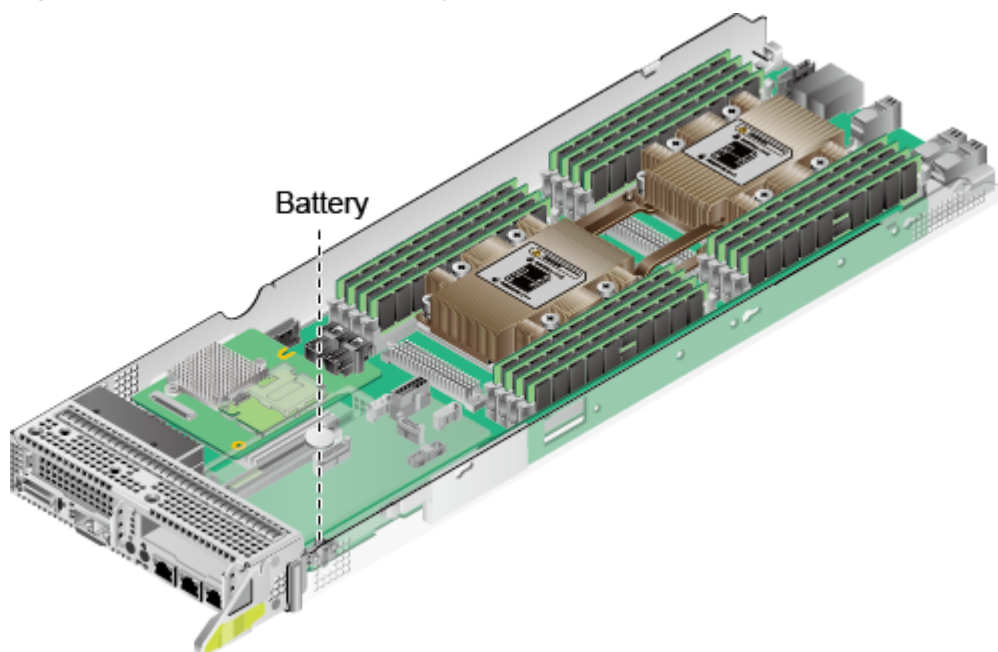
----End

8.4.18 Installing the Battery

Procedure

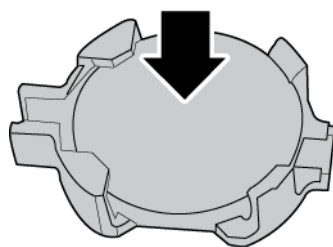
- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Take the component out of its ESD bag.
- Step 5** Determine the position of the battery.

Figure 8-54 Position of the battery



- Step 6** Remove the PCIe riser module.
For details, see [8.4.21 Removing a PCIe Riser Module](#).
- Step 7** Holding the battery with the text side facing upwards, insert the left end of the battery into the slot, and gently press down the whole battery into the slot.

Figure 8-55 Installing the battery



Step 8 Install the PCIe riser module.

For details, see [8.4.22 Installing a PCIe Riser Module](#).

Step 9 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 10 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 11 After the battery is replaced, the BIOS configuration is restored to the factory settings. You need to reconfigure the BIOS based on the site requirements.

 NOTE

- The iBMC 2.32 and later versions support import and export of configuration files.
- The BIOS configuration file exported from the iBMC can be directly imported after the battery is replaced. If the exported configuration file contains ciphertext, change the ciphertext to plaintext and delete the comment tags from the line. For details about how to import and export configurations, see [FusionServer Pro X6000 Server iBMC User Guide](#).
- The BIOS configuration file exported from the iBMC contains the configuration list. For details, see "Configuration File Description" in [FusionServer Pro X6000 Server iBMC User Guide](#).
- If the iBMC cannot be logged in to or the BIOS configuration file is not exported before the battery is replaced, you need to manually reconfigure the BIOS after replacing the battery.

----End

8.4.19 Removing a PCIe Card

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

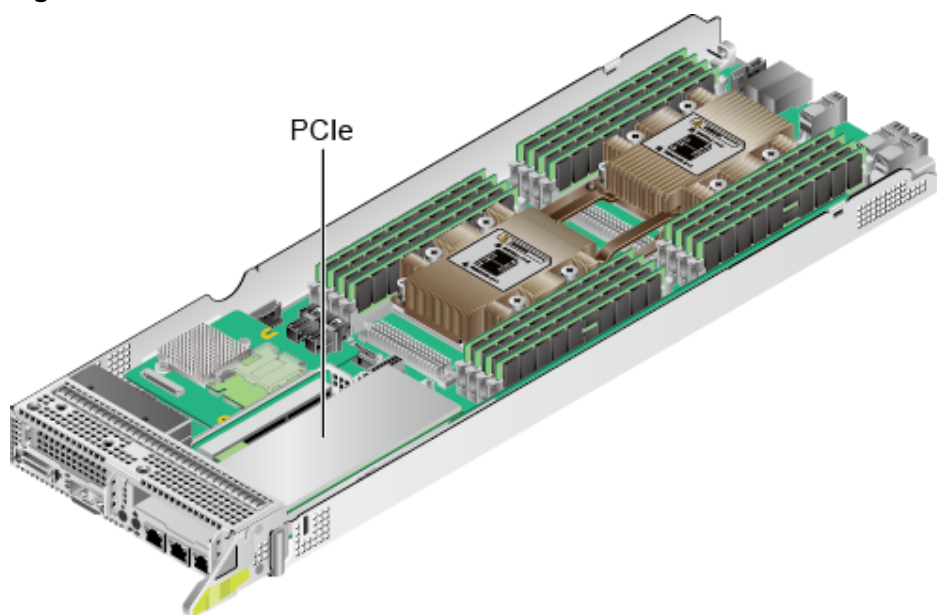
Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

Step 4 Determine the position of the PCIe card.

Figure 8-56 Position of the PCIe card

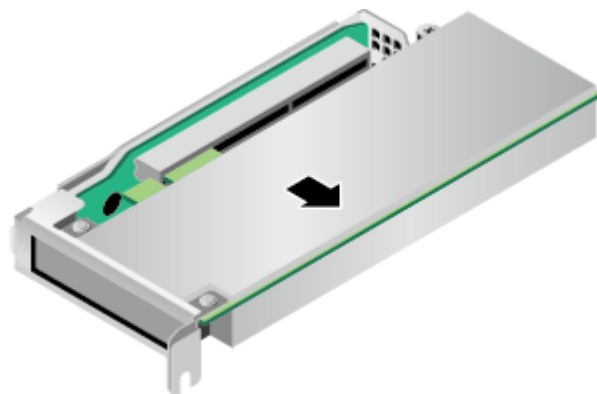


Step 5 Remove the PCIe riser module.

For details, see [8.4.21 Removing a PCIe Riser Module](#).

Step 6 Hold the PCIe riser module and remove the PCIe card in the arrow direction. See (5) in [Figure 8-57](#).

Figure 8-57 Removing a PCIe card



Step 7 Remove the front panel of a faulty PCIe card.

NOTICE

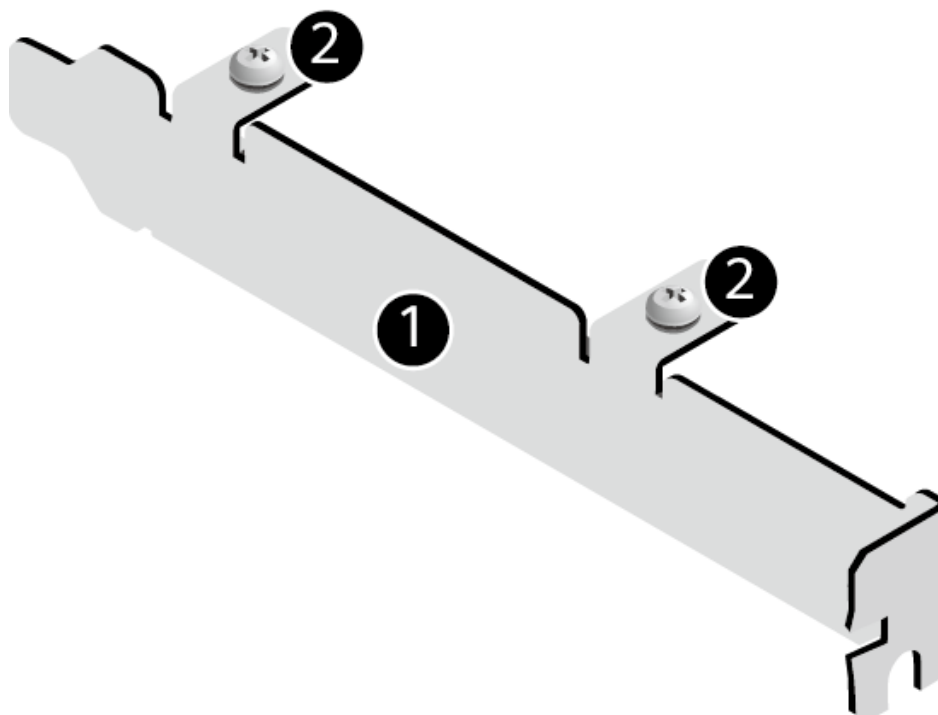
When returning the faulty PCIe card for repair, the customer must remove and retain the front panel and screws of the faulty PCIe card and return only the faulty card.

For details, see the following description:

- If the spare PCIe card does not have a front panel or the front panel of the spare PCIe card is inconsistent with that of the faulty PCIe card, use the front panel of the faulty PCIe card to replace that of the spare PCIe card and then install the spare PCIe card on the server node.
- If the front panel of the spare PCIe card is the same as that of the faulty PCIe card, no replacement is required.

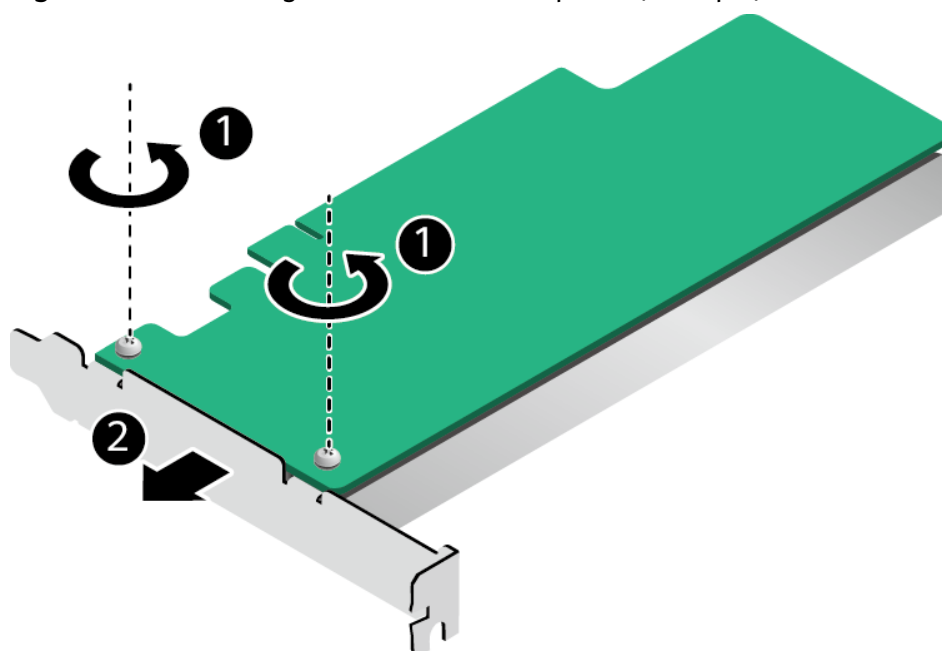
For details about the components that do not need to be returned, see [Figure 8-58](#).

Figure 8-58 Parts that do not need to be returned (example)



Use a Phillips screwdriver to loosen the screws fastening the front panel and remove the front panel. See (1) and (2) in [Figure 8-59](#).

Figure 8-59 Removing the PCIe card front panel (example)



Step 8 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

----End

8.4.20 Installing a PCIe Card

Procedure

- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Take the component out of its ESD bag.
- Step 5** Replace the front panel of the spare PCIe card.

NOTICE

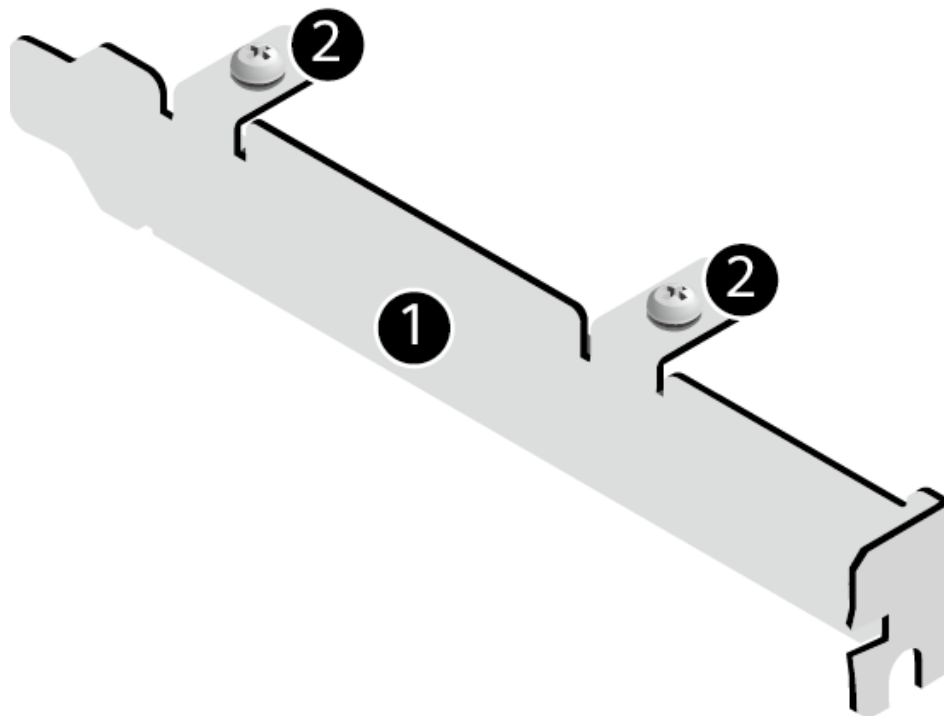
When returning the faulty PCIe card for repair, the customer must remove and retain the front panel and screws of the faulty PCIe card and return only the faulty card.

For details, see the following description:

- If the spare PCIe card does not have a front panel or the front panel of the spare PCIe card is inconsistent with that of the faulty PCIe card, use the front panel of the faulty PCIe card to replace that of the spare PCIe card and then install the spare PCIe card on the server node.
- If the front panel of the spare PCIe card is the same as that of the faulty PCIe card, no replacement is required.

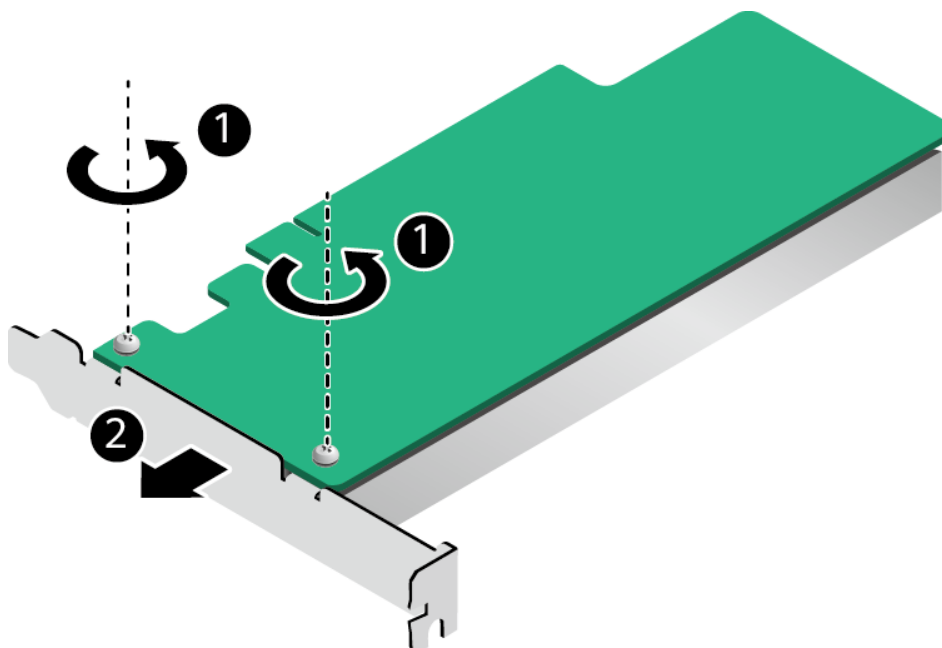
For details about the components that do not need to be returned, see [Figure 8-60](#).

Figure 8-60 Parts that do not need to be returned (example)



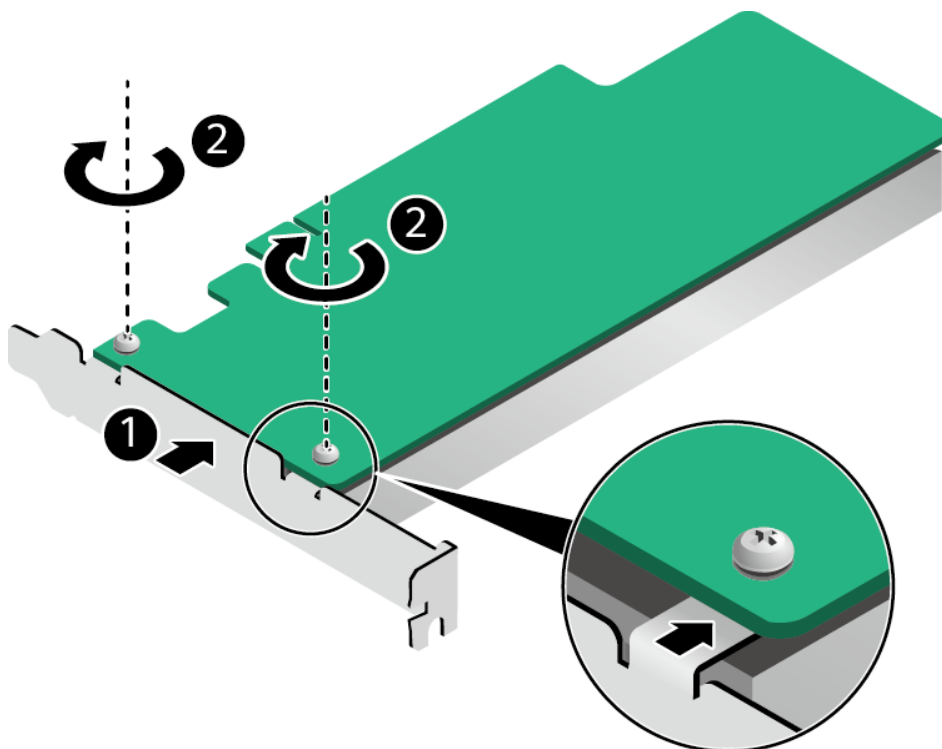
1. Remove the front panel of the spare PCIe card.
Use a Phillips screwdriver to loosen the screws fastening the front panel and remove the front panel. See (1) and (2) in [Figure 8-61](#).

Figure 8-61 Removing the PCIe card front panel (example)



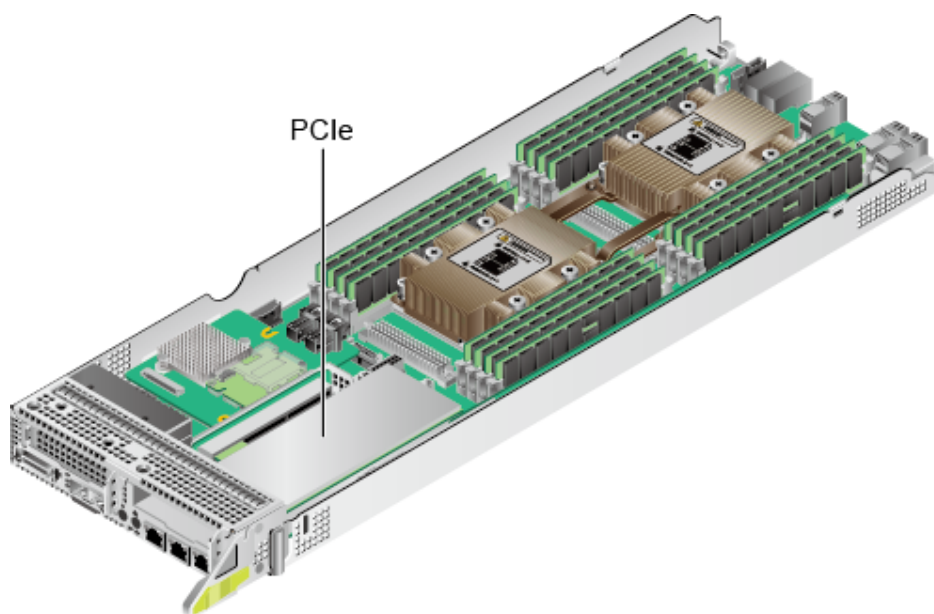
2. Install the front panel of a PCIe card.
Insert the front panel into the PCIe card horizontally, align it with the screw holes on the PCIe card, and tighten the screws on the front panel using a Phillips screwdriver. See (1) and (2) in [Figure 8-62](#).

Figure 8-62 Installing the PCIe card front panel (example)



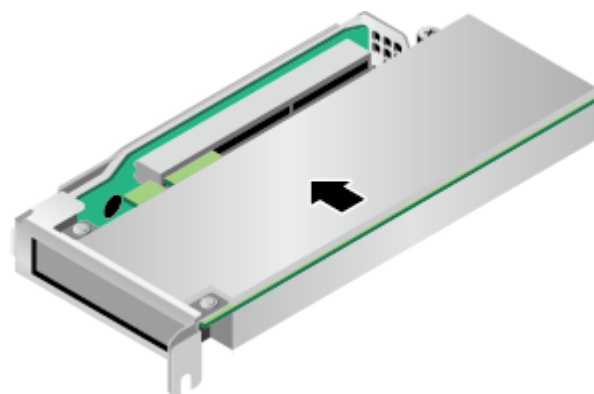
Step 6 Determine the position of the PCIe card.

Figure 8-63 Position of the PCIe card



Step 7 Hold the PCIe riser module and insert the PCIe card module into the PCIe riser module in the arrow direction. See (1) in [Figure 8-64](#).

Figure 8-64 Installing a PCIe card



Step 8 Install the PCIe riser module.

For details, see [8.4.22 Installing a PCIe Riser Module](#).

Step 9 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 10 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 11 Log in to the iBMC WebUI, and check whether the new component is normal.

For details, see [FusionServer Pro X6000 Server iBMC User Guide](#).

Step 12 Install the driver for the PCIe card.

 NOTE

If the new PCIe card model is different from the old PCIe card model, install the new PCIe card driver.

Step 13 Upgrade the firmware and driver to the target version.

For details, see [FusionServer Pro High-Density Server Upgrade Guide](#).

----End

8.4.21 Removing a PCIe Riser Module

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

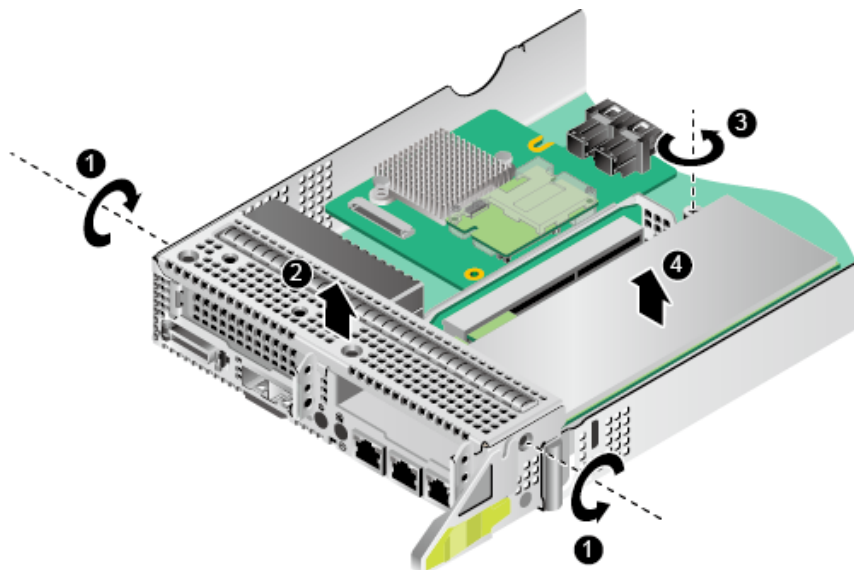
Step 3 Place the server node on the ESD workstation.

Step 4 Determine the position of the PCIe riser module.

Step 5 Remove the PCIe riser module.

1. Use a Phillips screwdriver to loosen the screws on the cover of the server node. See (1) in [Figure 8-65](#).
2. Remove the cover from the server node in the arrow direction. See (2) in [Figure 8-65](#).
3. Use a Phillips screwdriver to loosen the screw that secures the PCIe riser module. See (3) in [Figure 8-65](#).
4. Lift the PCIe riser module in the arrow direction. See (4) in [Figure 8-65](#).

Figure 8-65 Removing a PCIe riser module



Step 6 Disconnect the cable between the PCIe card and the NC-SI port.

For details, see [7.4 PCIe Card Cabling](#).

 NOTE

This operation is required only when the PCIe card is an SP380 NIC (BOM code: 02312JBD).

Step 7 Remove the PCIe card.

For details, see [8.4.19 Removing a PCIe Card](#).

Step 8 Place the removed PCIe riser module and PCIe card in different ESD bags.

NOTICE

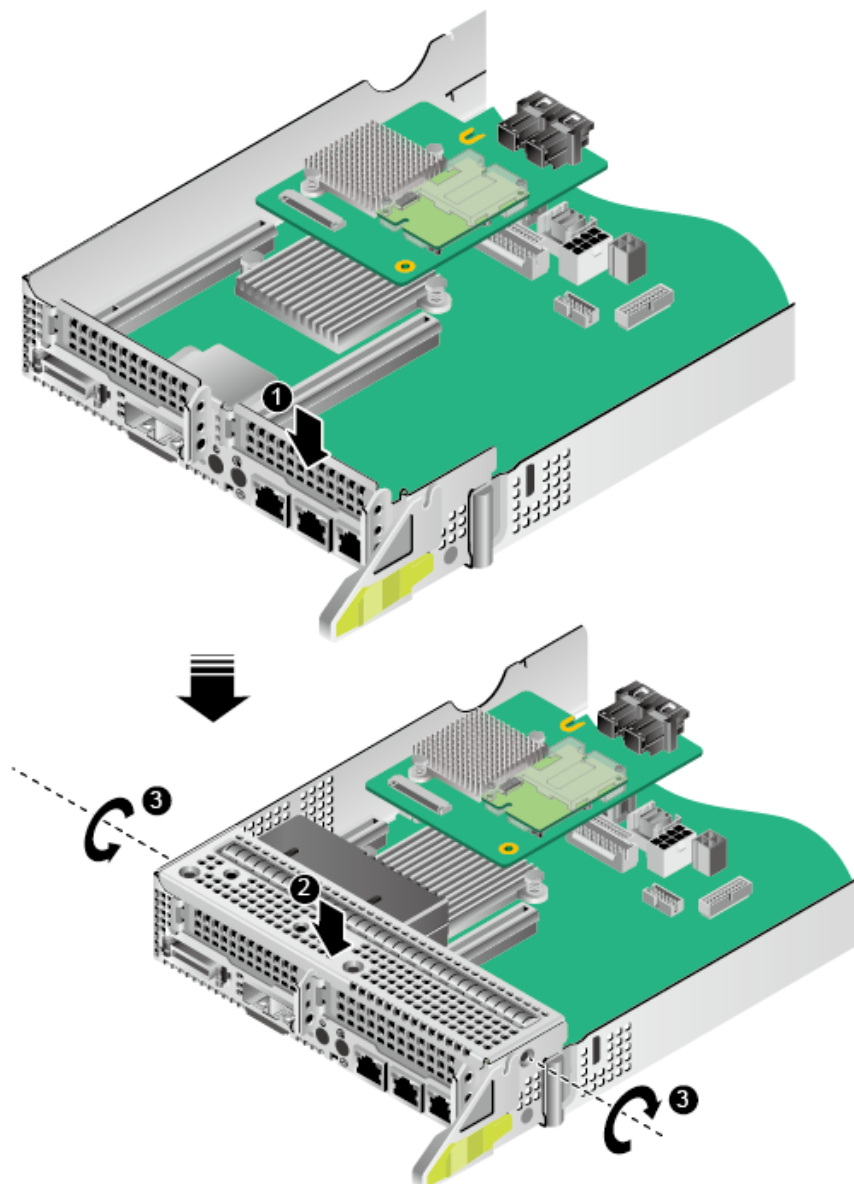
Place only one component in an ESD bag.

Step 9 Install a filler panel.

 NOTE

Perform this operation only when a PCIe riser module is not installed immediately.

Figure 8-66 Installing a filler panel



-----End

8.4.22 Installing a PCIe Riser Module

Procedure

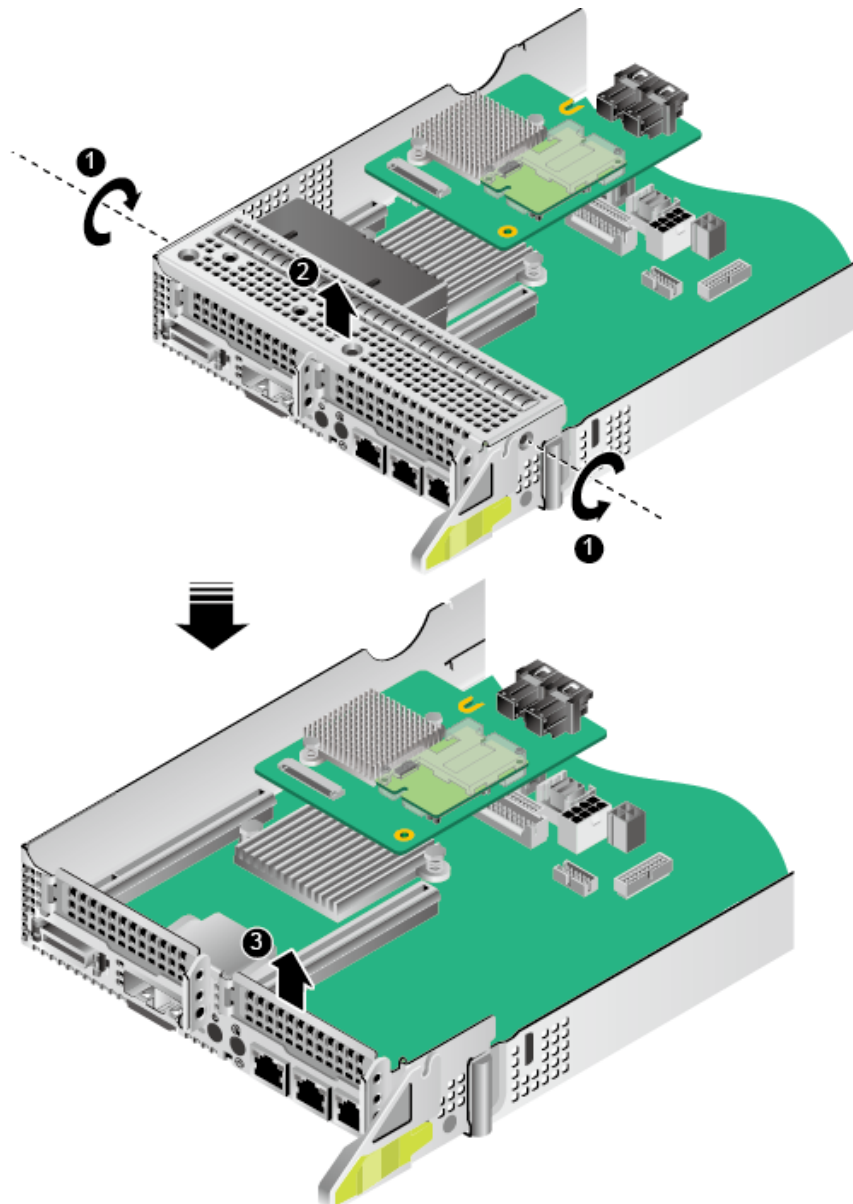
- Step 1** Power off the server node.
For details, see [8.3.2 Power-Off Procedure](#).
- Step 2** Remove the server node.
For details, see [8.3.3 Removing an XH321 V5](#).
- Step 3** Place the server node on the ESD workstation.
- Step 4** Determine the position of the PCIe riser module.

Step 5 Remove the filler panel.

 NOTE

- Perform this operation only when a filler panel is installed.
- Keep the removed filler panel properly.

Figure 8-67 Removing a filler panel



Step 6 Take the component out of its ESD bag.

Step 7 Install the PCIe card.

For details, see [8.4.20 Installing a PCIe Card](#).

Step 8 Connect the cable between the PCIe card and the NC-SI port.

For details, see [7.4 PCIe Card Cabling](#).

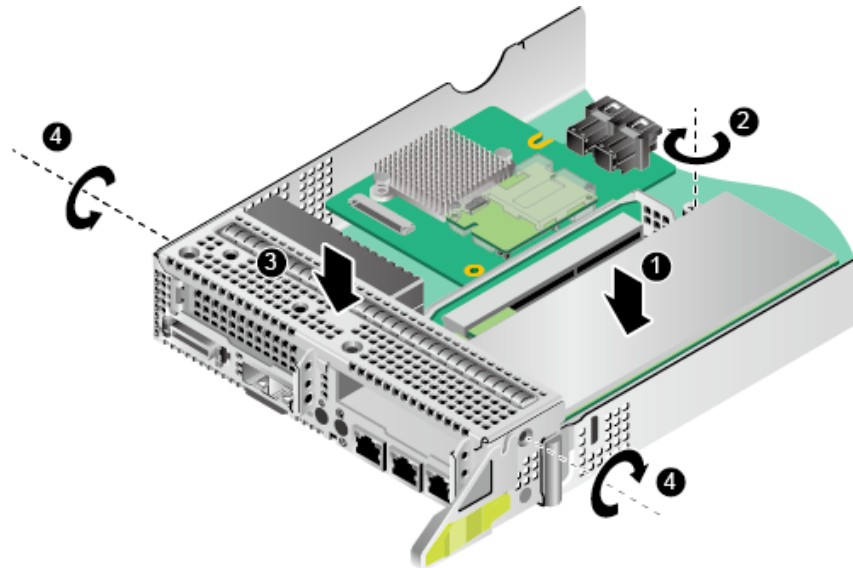
 NOTE

This operation is required only when the PCIe card is an SP380 NIC (BOM code: 02312JBD).

Step 9 Install the PCIe riser module.

1. Insert the PCIe riser module into the front PCIe slot of the server node in the arrow direction. See (1) in [Figure 8-68](#).
2. Use a Phillips screwdriver to tighten the screw to secure the PCIe riser module. See (2) in [Figure 8-68](#).
3. Install the server node panel in the arrow direction. See (3) in [Figure 8-68](#).
4. Use a Phillips screwdriver to tighten the screws on the node panel. See (4) in [Figure 8-68](#).

Figure 8-68 Installing the PCIe riser module



Step 10 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 11 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

----End

8.4.23 Removing the Air Duct

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

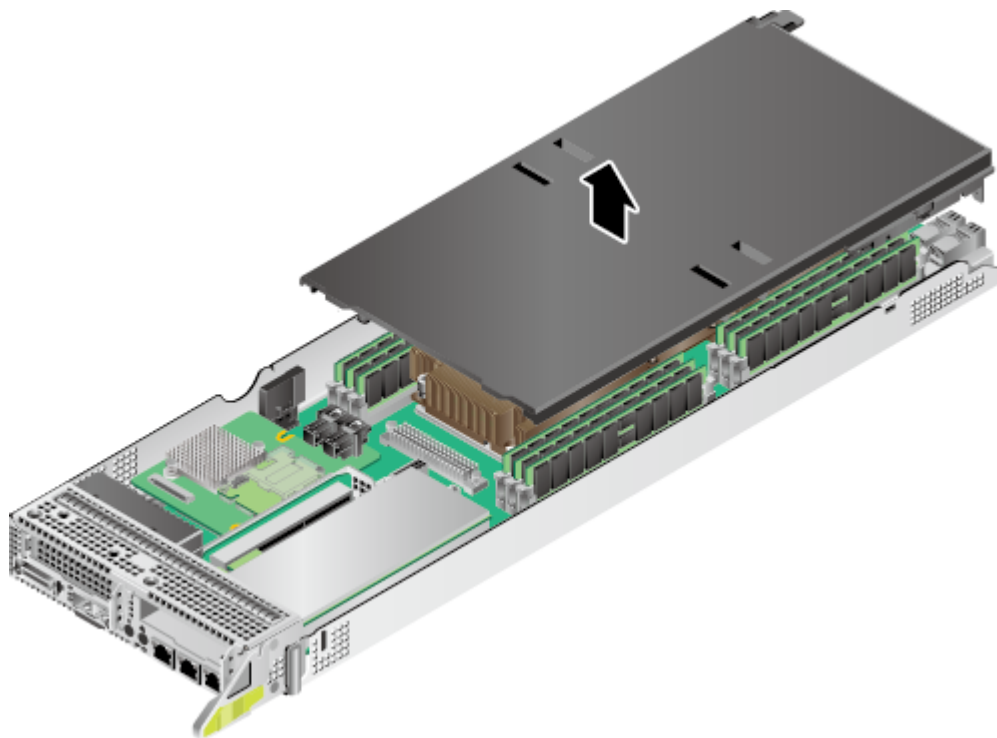
For details, see [8.3.3 Removing an XH321 V5](#).

Step 3 Place the server node on the ESD workstation.

Step 4 Determine the position of the air duct.

Step 5 Lift the air duct.

Figure 8-69 Removing the air duct



Step 6 Place the removed component in an ESD bag.

NOTICE

Place only one component in an ESD bag.

----End

8.4.24 Installing the Air Duct

Procedure

Step 1 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 2 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

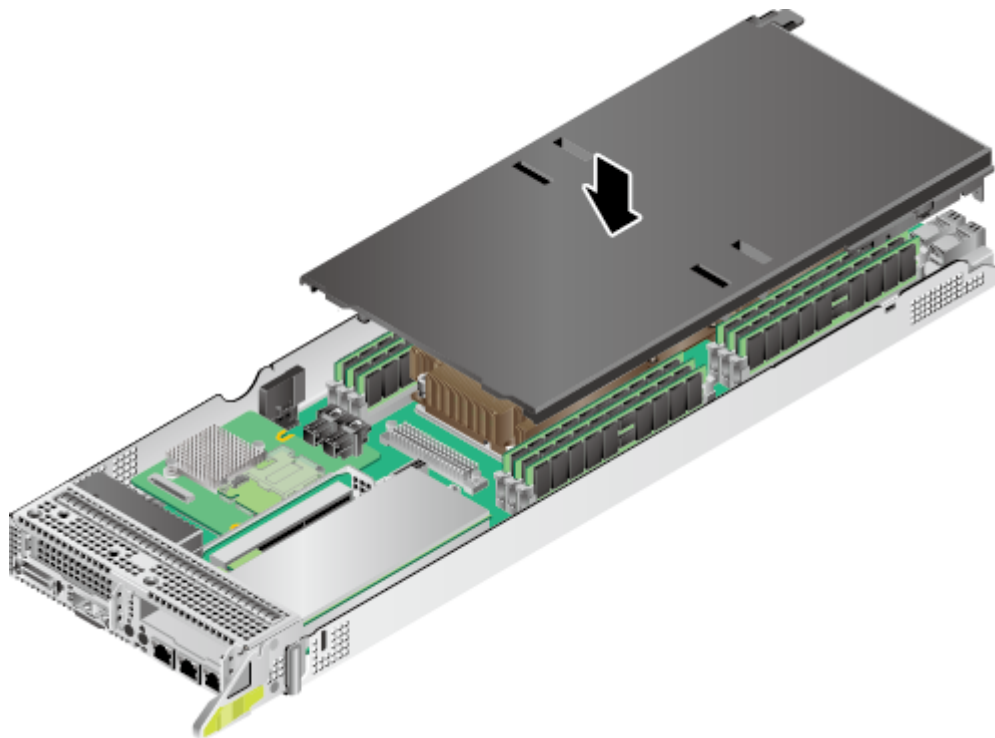
Step 3 Place the server node on the ESD workstation.

Step 4 Take the component out of its ESD bag.

Step 5 Determine the position of the air duct.

Step 6 Align the positioning pins on the air duct with the fixing holes on the chassis according to the instructions on the air duct. Vertically place the air duct downwards.

Figure 8-70 Installing the air duct



Step 7 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 8 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

----End

8.4.25 Removing the Mainboard and Server Node Case

If you cannot log in to the iBMC of the mainboard to be replaced, you do not need to perform [Step 1](#) to [Step 3](#).

Procedure

Step 1 Record the firmware (iBMC, BIOS, and CPLD) versions of the mainboard to be replaced.

- On the iBMC WebUI, choose **Information > System Info > Product Info** to obtain the information.
- On the iBMC CLI, run the **ipmcget -d version** command to obtain the information.

Step 2 Check the iBMC and BIOS configurations.

 CAUTION

After the mainboard is replaced, the original iBMC or BIOS configuration will be lost. If the current iBMC or BIOS parameters have been adjusted based on service scenarios, ensure that the parameter configuration is the same as that before the mainboard is replaced to ensure that services are not affected after the mainboard is replaced.

Step 3 Export the iBMC or BIOS configuration files.

For details, see [FusionServer Pro X6000 Server iBMC User Guide](#).

 NOTE

- iBMC 2.32 and later versions support the import and export of configuration files.
- After replacing the mainboard, import the iBMC and BIOS configuration files that are exported from the iBMC. However, the exported configuration file does not contain password information. You need to manually configure the password for the iBMC user. For details about how to import and export the configuration file, see [FusionServer Pro X6000 Server iBMC User Guide](#).
- The iBMC and BIOS configuration files exported from the iBMC contain the configuration list. For details, see "Configuration File Description" in [FusionServer Pro X6000 Server iBMC User Guide](#).
- If the iBMC and BIOS configuration files are not exported before the mainboard is replaced, manually configure the iBMC and BIOS data after replacing the mainboard.

Step 4 Power off the server node.

For details, see [8.3.2 Power-Off Procedure](#).

Step 5 Remove the server node.

For details, see [8.3.3 Removing an XH321 V5](#).

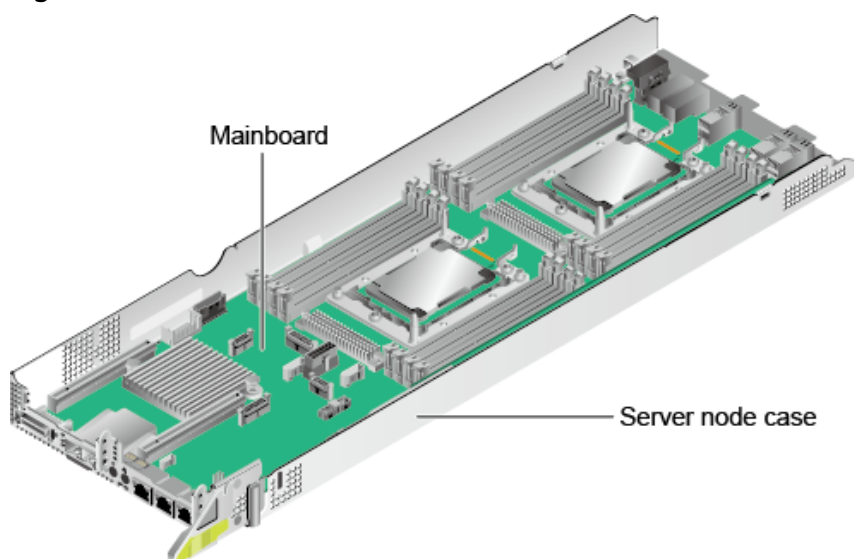
Step 6 Place the server node on the ESD workstation.

Step 7 Remove the air duct.

For details, see [8.4.23 Removing the Air Duct](#).

Step 8 Determine the position of the mainboard and the server node case.

Figure 8-71 Mainboard and server node case



NOTE

The mainboard is packed in the server node case and replaced as a whole package.

- Step 9** Remove the supercapacitor if there is any.
For details, see [8.4.5 Removing a Supercapacitor](#).
- Step 10** Remove the screw-in RAID controller card.
For details, see [8.4.3 Removing the Screw-in RAID Controller Card](#).
- Step 11** Remove the PCIe riser module.
For details, see [8.4.21 Removing a PCIe Riser Module](#).
- Step 12** Remove the PCIe card.
For details, see [8.4.19 Removing a PCIe Card](#).
- Step 13** Remove the TPM.
For details, see [8.4.15 Removing the TPM](#).
- Step 14** Remove M.2 SSDs.
For details, see [8.4.1 Removing an M.2 SSD](#).
- Step 15** Remove memory modules.
For details, see [8.4.13 Removing a Memory Module](#).
- Step 16** Remove processors.
For details, see [8.4.11 Removing a Processor](#).
- Step 17** Remove all cables from the mainboard.
For details, see [7 Internal Cabling](#).
- Step 18** Place the removed server node case (with the mainboard) and components on different ESD workstations.

 NOTE

- If the removed component is no longer used, pack it again using the original packaging materials and store it properly.
- Before placing the mainboard into an ESD bag, ensure that the processor sockets are installed with covers.
- Place only one component in an ESD bag.

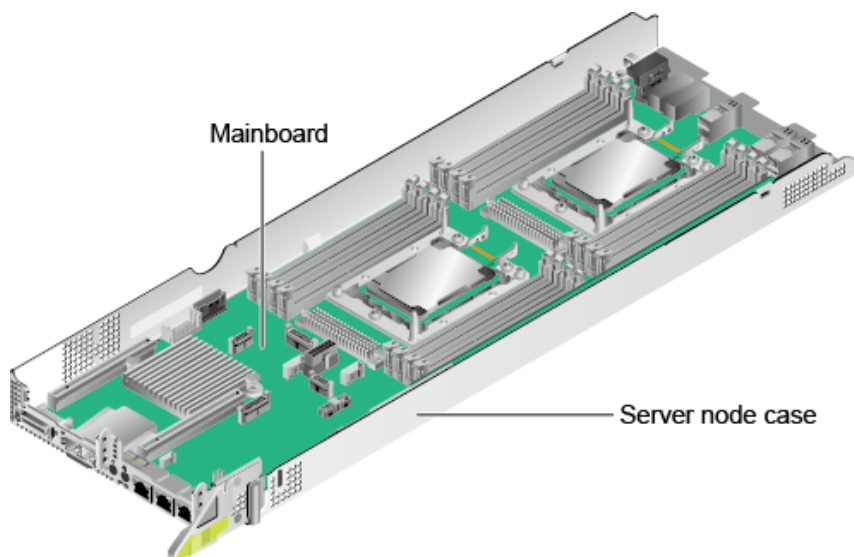
----End

8.4.26 Installing the Mainboard and Server Node Case

Procedure

- Step 1** Take the component out of its ESD bag.
- Step 2** Place the server node on the ESD workstation.
- Step 3** Determine the position of the mainboard and the server node case.

Figure 8-72 Mainboard and server node case



- Step 4** Connect all the cables to the mainboard.
For details, see [7 Internal Cabling](#).
- Step 5** Install processors.
For details, see [8.4.12 Installing a Processor](#).
- Step 6** Install memory modules.
For details, see [8.4.14 Installing a Memory Module](#).
- Step 7** Install M.2 SSDs.
For details, see [8.4.2 Installing an M.2 SSD](#).
- Step 8** Install the TPM.
For details, see [8.4.16 Installing the TPM](#).

Step 9 Install the PCIe card.

For details, see [8.4.20 Installing a PCIe Card](#).

Step 10 Install the PCIe riser module.

For details, see [8.4.22 Installing a PCIe Riser Module](#).

Step 11 Install the screw-in RAID controller card.

For details, see [8.4.4 Installing the Screw-in RAID Controller Card](#).

Step 12 Install the supercapacitor if it is configured.

For details, see [8.4.6 Installing the Supercapacitor](#).

Step 13 Install the air duct.

For details, see [8.4.24 Installing the Air Duct](#).

Step 14 Install the server node.

For details, see [8.3.4 Installing a Server Node](#).

Step 15 Power on the server node.

For details, see [8.3.1 Power-On Procedure](#).

Step 16 Check the indicator status. If the health status indicator is steady green, the server node is running properly.

For details, see [2.1.2 Indicators and Buttons](#).

Step 17 Burn the original SN into the new mainboard after replacement. For details, see section "Modifying Electronic Labels" in the [SmartKit User Guide \(for Engineers\)](#).

NOTICE

- Only authorized engineers can download the ElabelTool plug-in package, import it to SmartKit, and modify electronic labels.
- If the original device SN is not burnt in the new mainboard, the iBMC and OS cannot obtain the device SN. This may affect the running of some services or the monitoring and management on the device.

Step 18 After the mainboard is replaced, the LOM is replaced and the MAC address of the LOM is changed. If the LOM is used for transferring data, you need to configure the LOM data.

Step 19 After the mainboard is replaced, the iBMC and BIOS settings are restored to the default settings of the new mainboard. Configure the iBMC and BIOS based on service requirements.

 NOTE

- If you have exported iBMC and BIOS configuration files on the iBMC before replacing the mainboard, you can import the configuration files after the replacement. However, the exported configuration files do not contain password information. You need to manually configure the password for the iBMC user. For details about how to import and export a configuration file, see the [FusionServer Pro X6000 Server iBMC User Guide](#).
- The iBMC and BIOS configuration files exported from the iBMC contain parameter lists. For details, see "Configuration File Description" in the [FusionServer Pro X6000 Server iBMC User Guide](#).
- iBMC 2.32 and later versions support the import and export of configuration files.
- If the iBMC and BIOS configuration files are not exported before you replace the mainboard, manually configure the iBMC and BIOS after the replacement.
- After the mainboard is replaced, the iBMC SSL certificate is restored to its initial status. If you have imported a requested SSL certificate before replacing the mainboard, import it again after replacing the mainboard.

Step 20 Upgrade the mainboard firmware (iBMC, BIOS, and CPLD) and Smart Provisioning to the latest version.

For details, see [FusionServer Pro High-Density Server Upgrade Guide](#).

-----End

9 Troubleshooting Guide

For details about troubleshooting, see [Huawei Servers Troubleshooting](#).

- Troubleshooting process
Troubleshooting is a process of using appropriate methods to find the cause of a fault and rectify the fault. The troubleshooting process is to narrow down the scope of possible causes for a fault to reduce troubleshooting complexity, identify the root cause, and rectify the fault.
- Fault information collection
If a fault occurs on a server, collect logs for fault diagnosis.
- Fault diagnosis
Fault diagnosis rules and tools help Huawei technical support engineers and maintenance engineers to analyze and rectify faults according to alarms and hardware fault symptoms.
- Software and firmware upgrade
Software and firmware upgrade packages can be downloaded by server model and installed as needed.
- Preventive maintenance
Preventive maintenance promptly detects, diagnoses, and rectifies server faults.

10 Common Operations

[10.1 Querying the iBMC IP Address](#)

[10.2 Logging In to the iBMC WebUI](#)

[10.3 Logging In to the Desktop of a Server](#)

[10.4 Logging In to the CLI](#)

[10.5 Accessing the BIOS](#)

10.1 Querying the iBMC IP Address

Scenarios

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 use any of the following methods to query the IP address of the iBMC management network port:

- BIOS
- iBMC WebUI
For details, see [FusionServer Pro X6000 Server iBMC User Guide](#).
- iBMC CLI
Run the **ipmcget -d ipinfo** command.
For details, see [FusionServer Pro X6000 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

10.2 Logging In to the iBMC WebUI

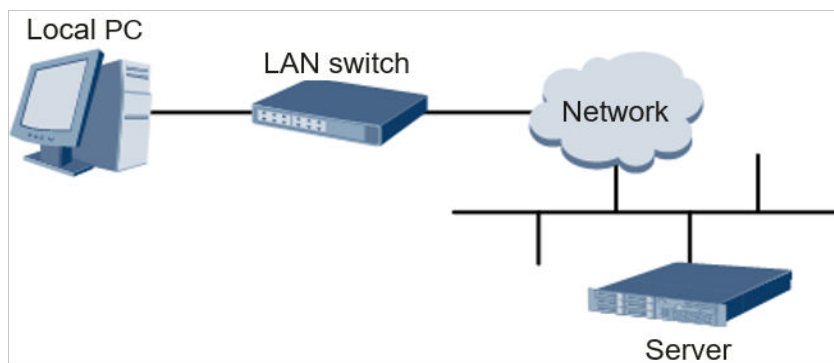
This section uses a PC running Windows 10 and Google Chrome as an example.

For details about the system configuration requirements of the local PC, refer to the [FusionServer Pro X6000 Server iBMC User Guide](#) by choosing **Documentation > All Documents > User Guide**.

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

[Figure 10-1](#) shows the network diagram.

Figure 10-1 Network diagram



Step 2 Open Google Chrome on the local PC.

Step 3 In the address box, enter the iBMC address in the format of **https://*IP_address_of_the_server_iBMC_management_network_port*** (for example, **https://192.168.2.100**).

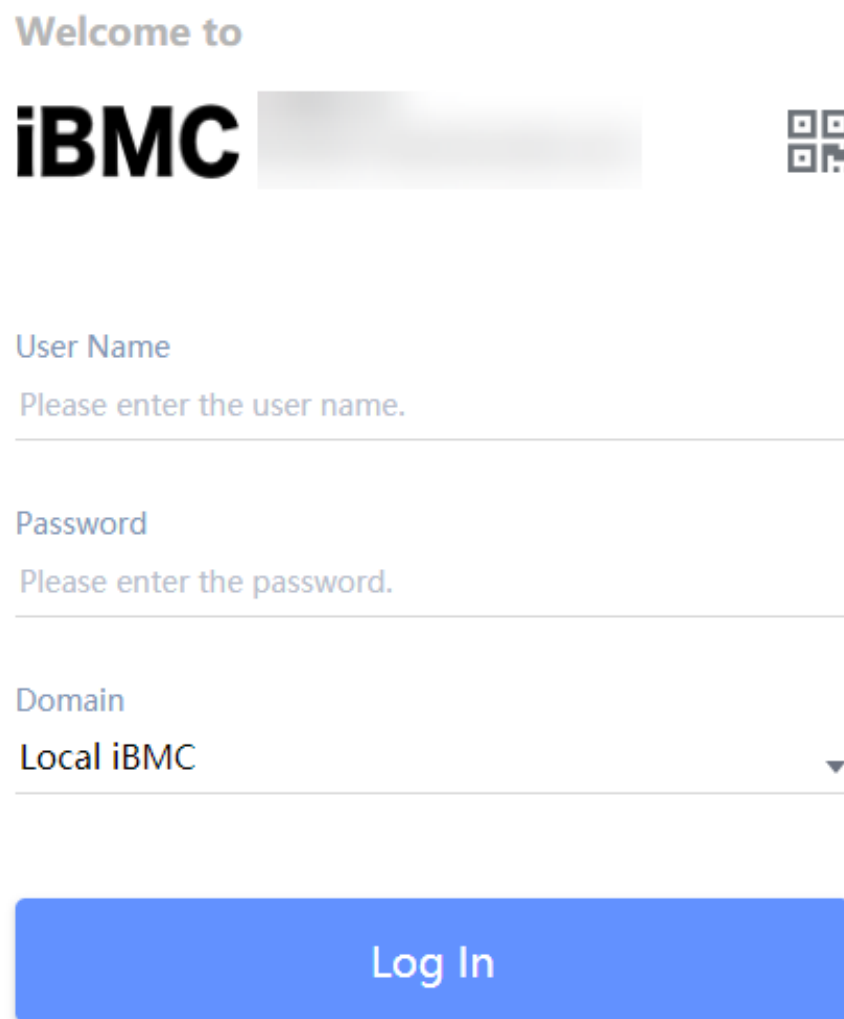
Step 4 Press **Enter**.

The iBMC login page is displayed, as shown in [Figure 10-2](#).

NOTE

- If Google Chrome displays a message indicating that your connection is not private, choose **Advanced > Proceed to**.
- The iBMC login page varies with the iBMC version.

Figure 10-2 Logging in to the iBMC



The image shows the iBMC login interface. At the top, it says "Welcome to" in orange, followed by the "iBMC" logo in large black letters. To the right of the logo is a blurred rectangular area and a QR code icon. Below the logo, there are three input fields: "User Name" with the placeholder "Please enter the user name.", "Password" with the placeholder "Please enter the password.", and "Domain" with a dropdown menu currently showing "Local iBMC". At the bottom, there is a large blue button labeled "Log In".

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

 NOTE

- The default user name of the iBMC is **Administrator**, and the default password is **Admin@9000**.
- The user account will be locked if incorrect passwords are entered for five consecutive times. If your user account is locked, log in again 5 minutes later.

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

Step 7 Click **Log In**.

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

----End

10.3 Logging In to the Desktop of a Server

10.3.1 Using the Remote Virtual Console

10.3.1.1 iBMC

10.3.1.1.1 Versions Earlier Than V600

Scenarios

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 [10.2 Logging In to the iBMC WebUI](#).

Step 2 On the menu bar, choose **Remote Console**. The **Remote Console** page is displayed.

Figure 10-3 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)	0
Maximum Sessions	2
Active Sessions	0
Encryption	☐
Enable Local KVM	☒
Persistent Virtual Keyboard and Mouse	☒

Save

Virtual Media

Maximum Sessions	1
Active Sessions	0
Encryption	☐

Save

VNC Service

Timeout Period (min)	0
Keyboard Layout	English(US) ▼
VNC Password	
Confirm Password	
Password Validity (Days)	Unlimited
Login Rules	☐ Rule1 ☐ Rule2 ☐ Rule3 View login rules
SSL Encryption	☐
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 manage the server at a time.
- **Java Integrated Remote Console (Shared):** allows two local users or five VNC users to access and manage the server at a time. Each user can view the operations performed by the other user.
- **HTML5 Integrated Remote Console (Private):** allows only one local user or VNC user to access and manage the server at a time.
- **HTML5 Integrated Remote Console (Shared):** allows two local users or five VNC users to access and manage the server at a time. Each user can view the operations performed by the other user.
- HTML5 supports only Internet Explorer 10.0 and later versions.

Figure 10-4 Real-time operation console (Java)

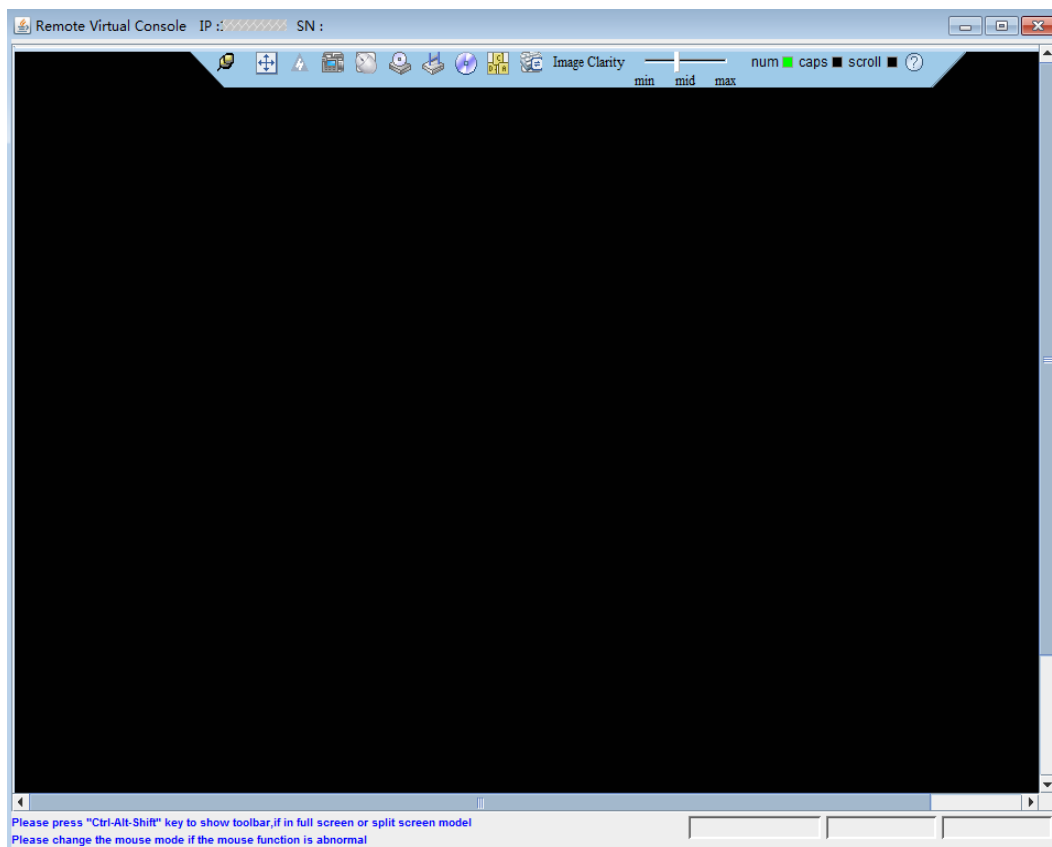
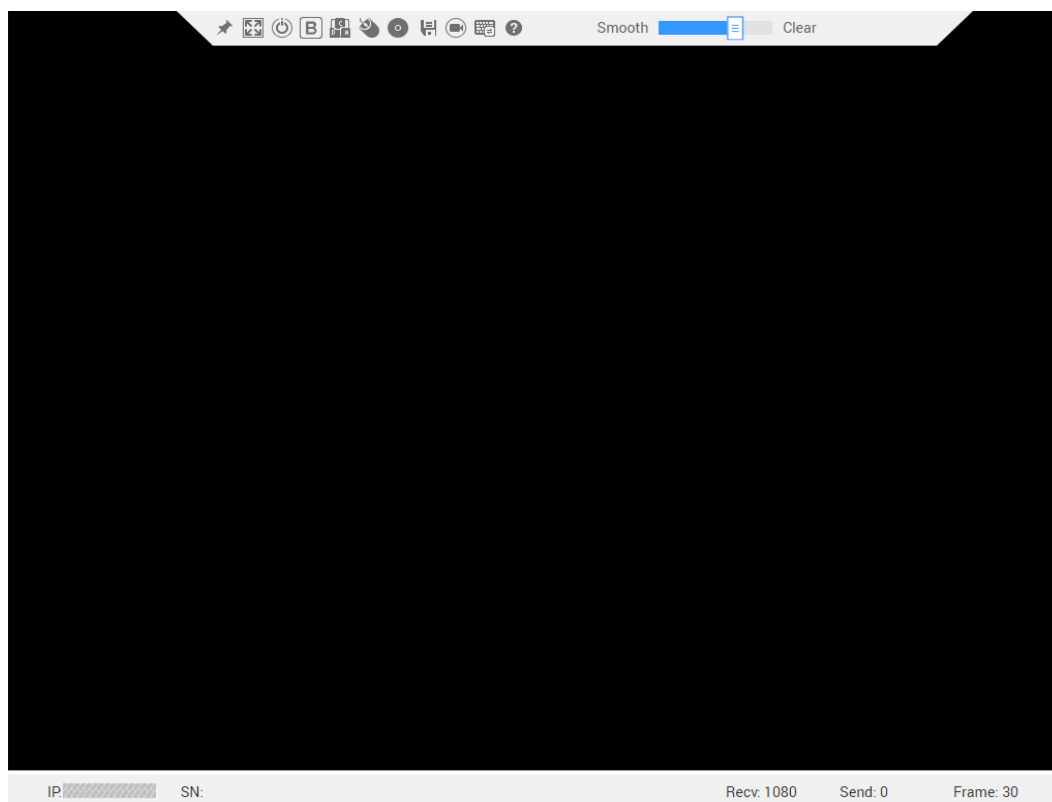


Figure 10-5 Real-time operation console (HTML5)



-----End

10.3.1.1.2 V600 and Later Versions

Scenarios

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

Procedure

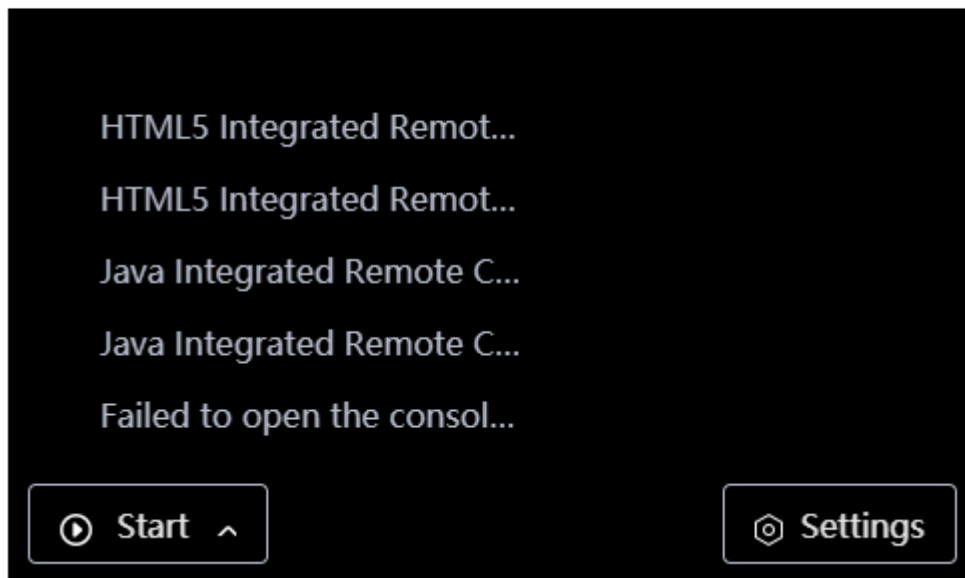
Step 1 Log in to the iBMC WebUI.

For details, see [10.2 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 10-6 Virtual Console

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 manage the server at a time.
- **Java Integrated Remote Console (Shared):** allows two local users or five VNC users to access and manage the server at a time. Each user can view the operations performed by the other user.
- **HTML5 Integrated Remote Console (Private):** allows only one local user or VNC user to access and manage the server at a time.
- **HTML5 Integrated Remote Console (Shared):** allows two local users or five VNC users to access and manage the server at a time. Each user can view the operations performed by the other user.
- HTML5 supports only Internet Explorer 10.0 and later versions.

Figure 10-7 Real-time operation console (Java)

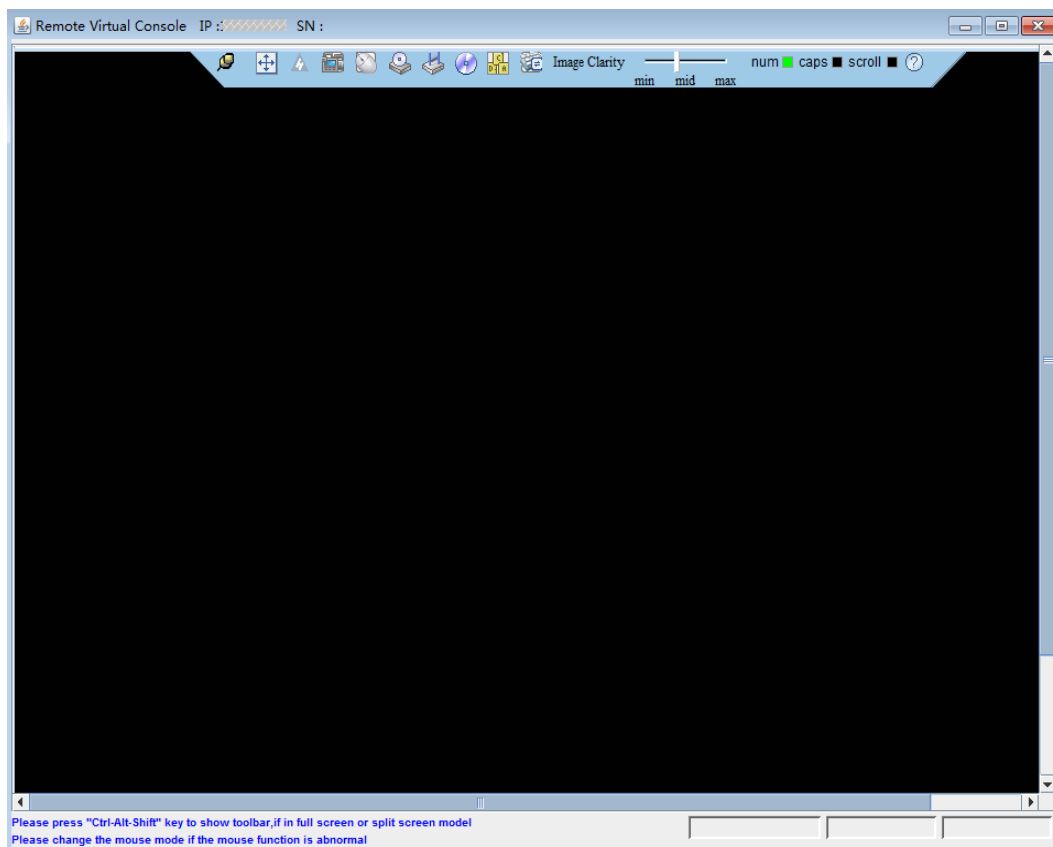
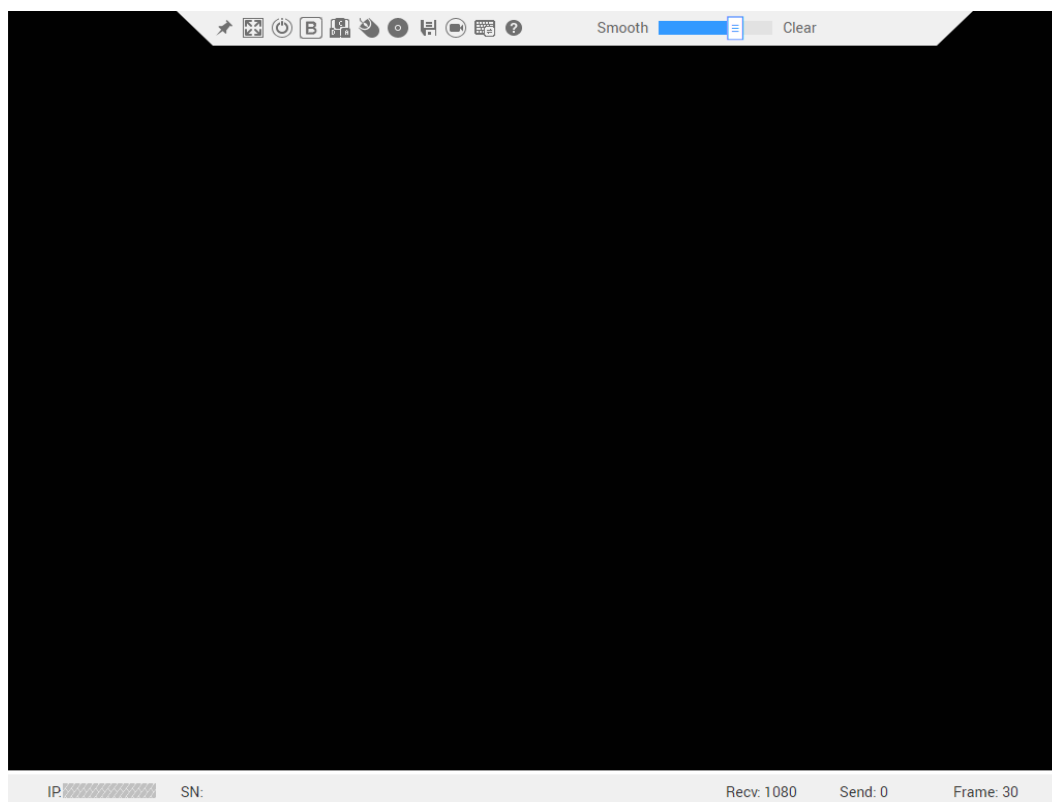


Figure 10-8 Real-time operation console (HTML5)



-----End

10.3.2 Logging In to the Independent Remote Console

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

Table 10-1 Instructions for using the independent remote console

Software Package	How to Obtain	OS Type	Version	Operation Description
kvm_client_windows.zip	You can click SmartKit Computing 23.1.0 to obtain it.	Windows	Windows 7 32-bit or 64-bit	For details about how to log in to the real-time desktop of a server using the independent remote console, see the SmartKit Computing V2R2 Independent Remote Console User Guide .
			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	
kvm_client_ubuntu.zip		Ubuntu	Ubuntu 14.04 LTS	
			Ubuntu 16.04 LTS	
kvm_client_mac.zip		Mac OS	Mac OS X El Capitan	
kvm_client_linux.zip		Red Hat	RHEL 6.9	
			RHEL 7.3	

10.4 Logging In to the CLI

10.4.1 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.

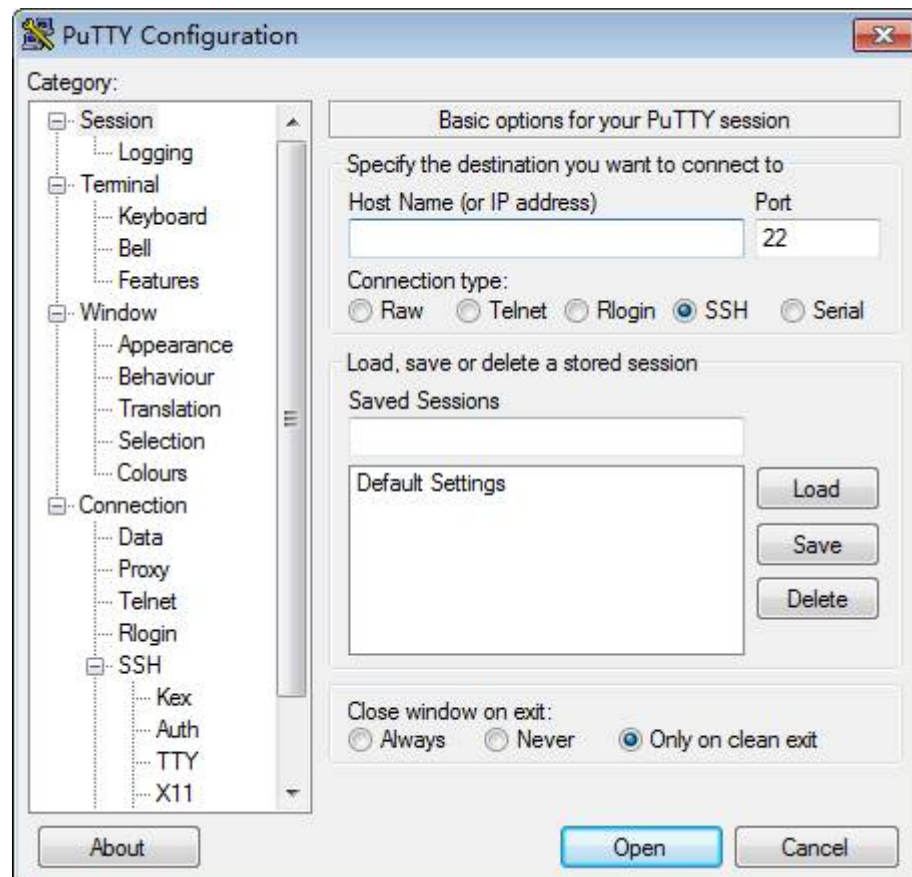
Procedure

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 10-9 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

10.4.2 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.

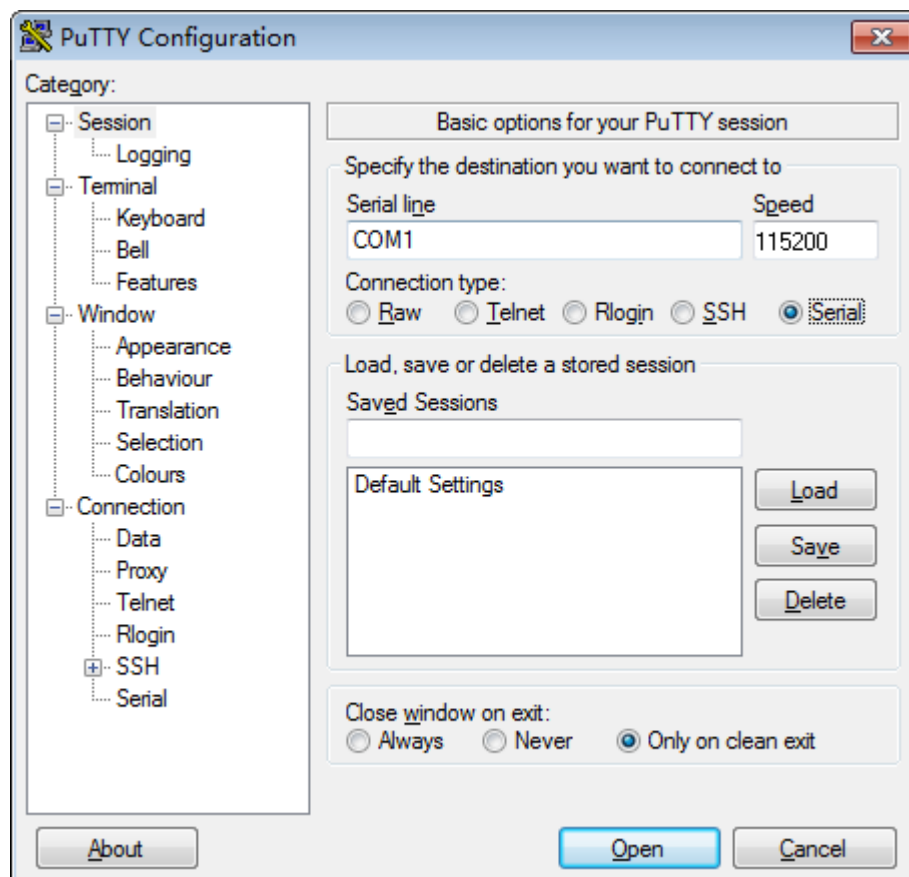
Step 4 In the navigation tree, choose **Session**.

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 10-10 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

10.5 Accessing the BIOS

10.5.1 Accessing the BIOS (V3XX or Earlier)

Procedure

Step 1 Log in to the desktop of the server node.

For details, see [10.3 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

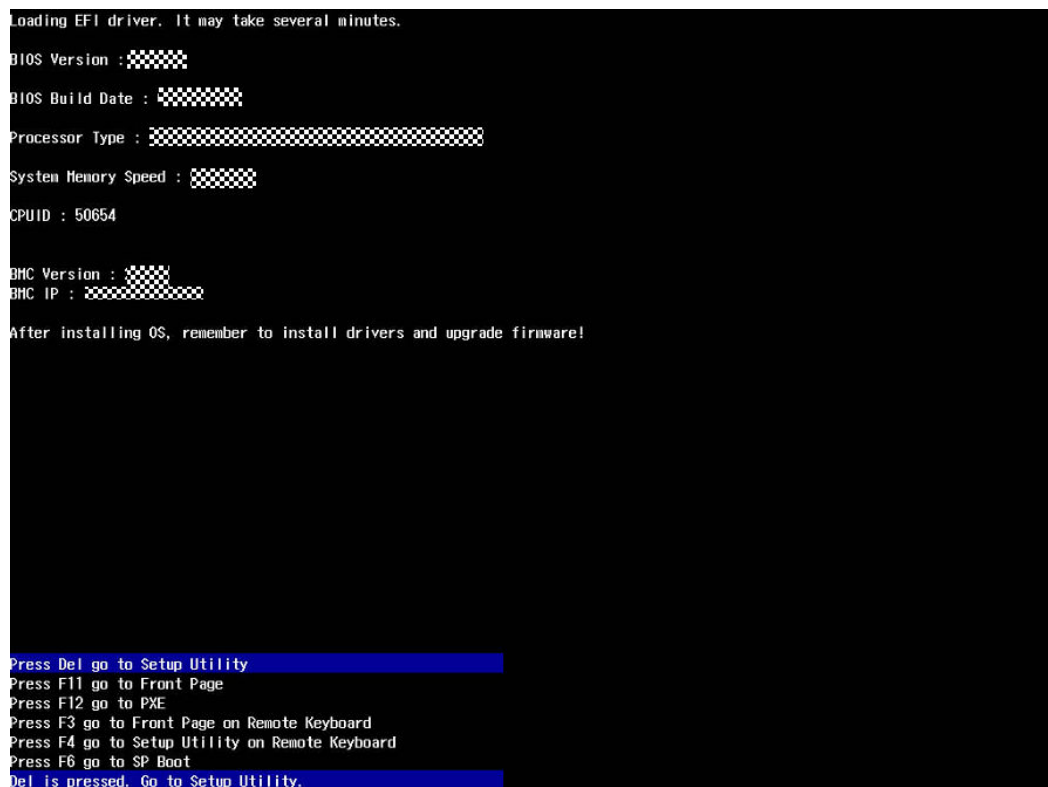
- A forced restart or power cycle may cause data loss or program damage.
- Before performing a forced restart or power cycle, ensure that no service interruption risk exists.

Step 4 Click **Yes**.

The server node starts to be forcibly restarted or power cycled.

Step 5 During the restart, press **Delete** or **F4** when the information shown in [Figure 10-11](#) is displayed.

Figure 10-11 BIOS startup screen

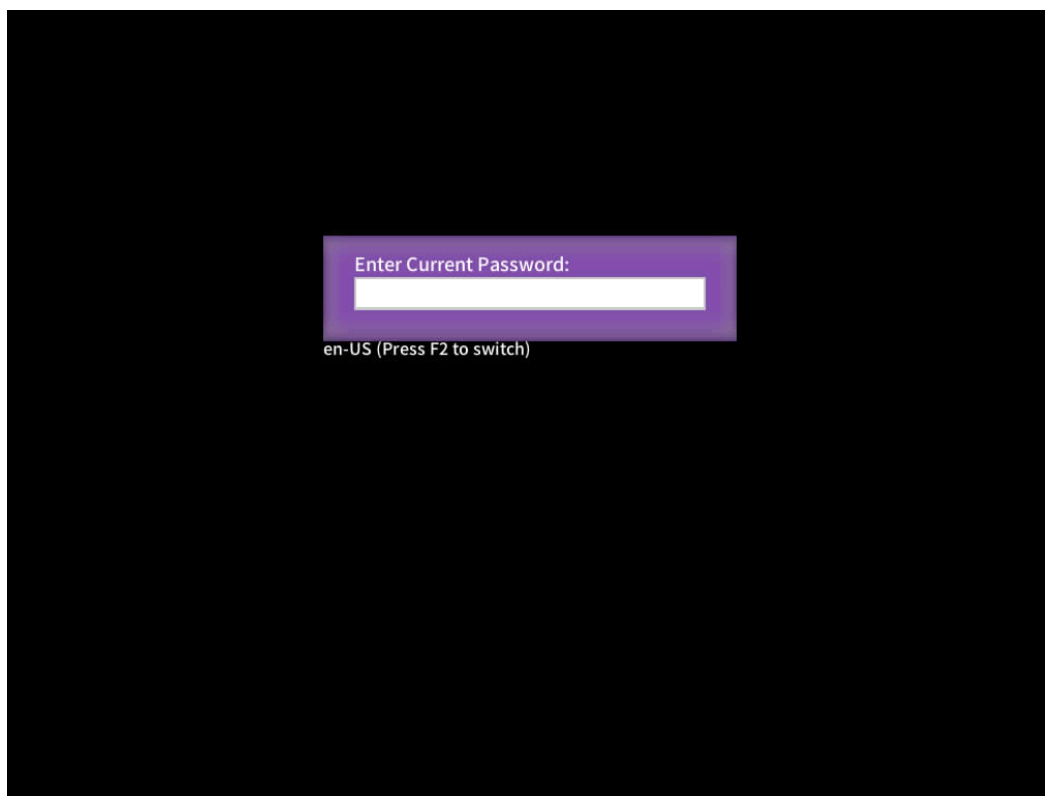


 NOTE

- To go to the BIOS front page, press **F11** or **F3**.
- To boot from the network, press **F12**. Enter the password in the displayed dialog box.
- To access the Smart Provisioning GUI, press **F6**.

The screen for entering the BIOS password is displayed.

Figure 10-12 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 node to unlock it.

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

----End

10.5.2 Accessing the BIOS (V6XX or Later)

Procedure

Step 1 Log in to the desktop of the server node.

For details, see [10.3 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

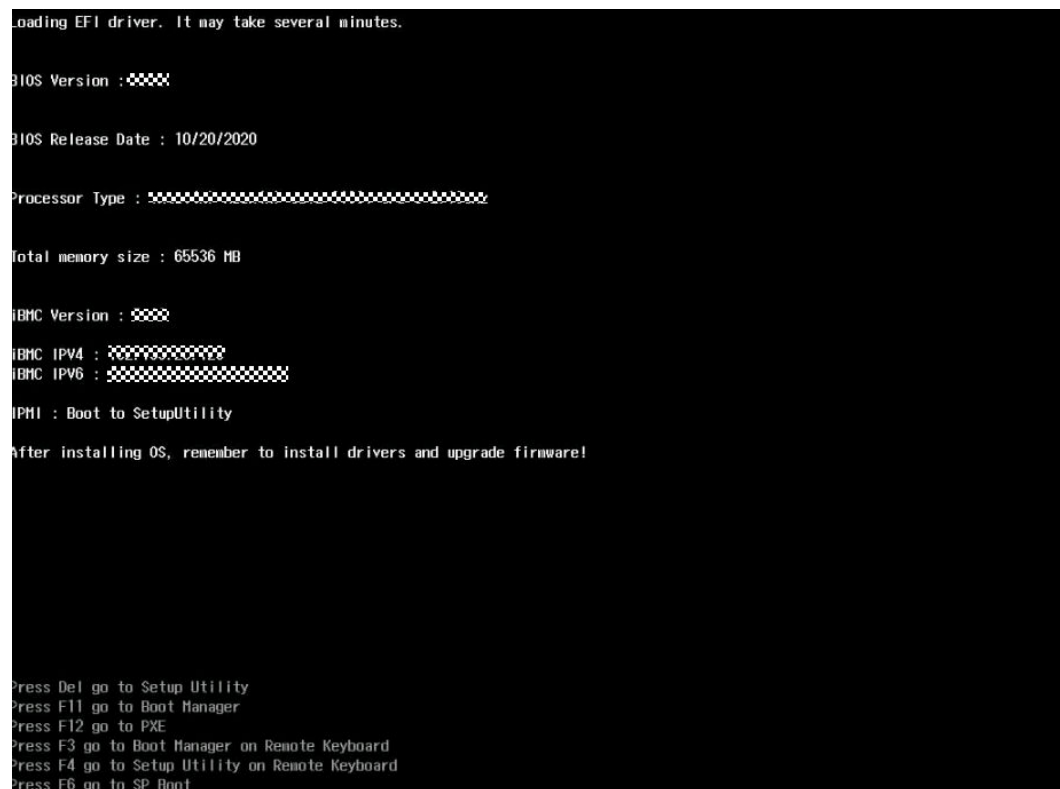
- A forced restart or power cycle may cause data loss or program damage.
- Before performing a forced restart or power cycle, ensure that no service interruption risk exists.

Step 4 Click **Yes**.

The server node starts to be forcibly restarted or power cycled.

Step 5 During the restart, press **Delete** or **F4** when the information shown in [Figure 10-13](#) is displayed.

Figure 10-13 BIOS startup screen

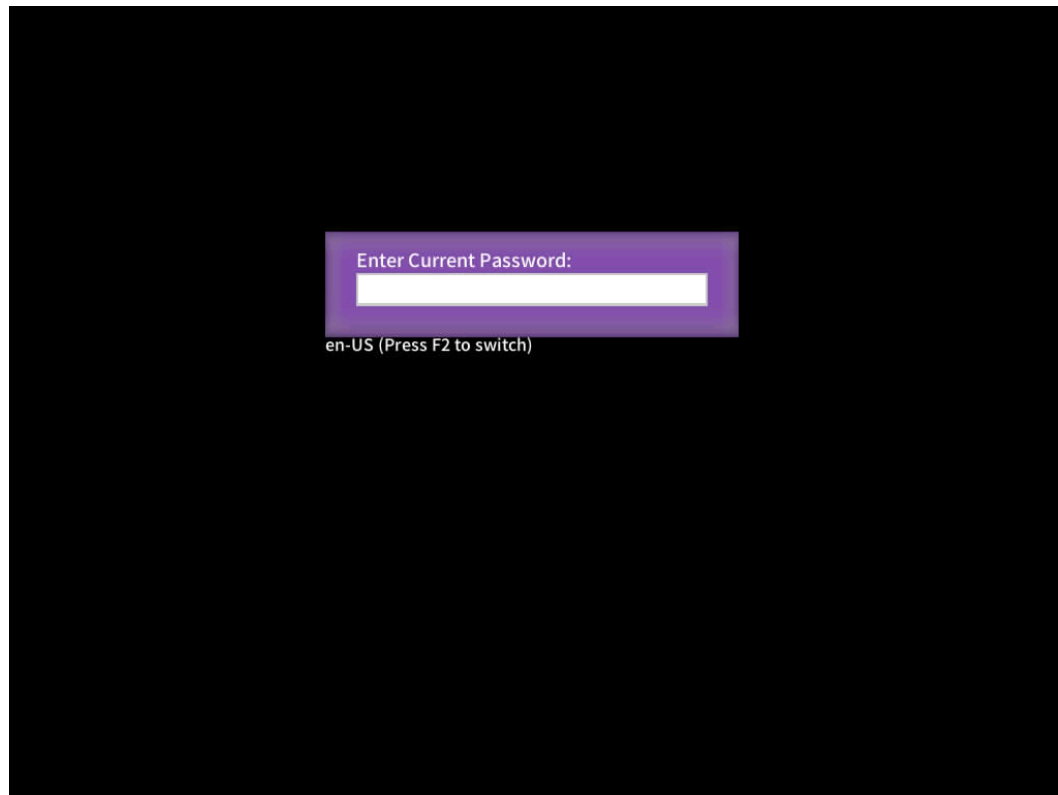


NOTE

- To go to the **Boot Manager** screen, press **F11** or **F3**.
- To boot from the network, press **F12**. Enter the password in the displayed dialog box.
- To access the Smart Provisioning GUI, press **F6**.
- Common users cannot use shortcut keys to access configuration items except the front page during BIOS boot.

The screen for entering the BIOS password is displayed.

Figure 10-14 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 node to unlock it.

The **Front Page** screen is displayed.

Figure 10-15 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

11 More Information

[11.1 Obtaining Technical Support](#)

[11.2 Product Information](#)

[11.3 Product Configuration Resources](#)

[11.4 Maintenance Tools](#)

11.1 Obtaining Technical Support

Huawei provides timely and efficient technical support through local branch offices, secondary technical support system, telephone technical support, remote technical support and onsite technical support.

Technical Support Website

Refer to technical documents at either of the following technical support websites:

- [Huawei Enterprise Website](#)
- [Huawei Carrier Product and Service Website](#)

Self-Service Platform and Community

To learn more about servers and communicate with experts:

- Visit [HUAWEI Server Information Service Platform](#) for specific server product documentation.
- Visit [Huawei Enterprise WeiKnow](#) for quick learning about products.
- Visit [Huawei Enterprise Support Community \(Servers\)](#) for learning and discussion.

Notice

For notices about product life cycles, warnings, and updates, visit [Support > Bulletins > Product Bulletins](#).

Knowledge Base

To learn server applications, visit [Computing Product Case Library](#).

Contact Huawei

If a fault cannot be located or rectified by referring to documents, contact technical support.

- Contact the Huawei customer service center.
Enterprise customers in China:
 - Customer service hotline: 400-822-9999
 - Customer service hotline: support_e@huawei.com.Enterprise customers outside China: [Global Service Hotline](#)
Telecom carriers in China can contact us by:
 - Customer service hotline: 400-830-2118
 - Customer service hotline: support@huawei.com.Telecom carriers outside China: [Global TAC Information](#).
- Contact the technical support personnel at your local Huawei office.

11.2 Product Information

[Table 11-1](#) provides common information about servers.

Table 11-1 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 Support > Intelligent Servers , 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.	Computing Product Compatibility Checker
Maintenance Information Inquiry System	A system used to query the service information about servers.	Visit Maintenance Status .
Computing Product Power Calculator	A tool used to calculate server power consumption based on the server configuration. The power consumption is for reference only.	Computing Product Power Calculator

11.3 Product Configuration Resources

Table 11-2 describes the common product configuration resources of servers.

Table 11-2 Product configuration resources

Tool	Description	How to Obtain
Removal and installation videos	Tutorial videos about how to remove and install hardware.	Multimedia Portal
Computing Product Memory Configuration Assistant	The Computing Product Memory Configuration Assistant is an online application. It demonstrates DIMM installation sequence in a graphical manner after you specify the product name, CPU quantity, and DIMM quantity.	Computing Product Memory Configuration Assistant

11.4 Maintenance Tools

Table 11-3 lists the software tools required for routine maintenance of servers.

Table 11-3 Software tools for routine maintenance

Tool	Server Model and Software Version	Description
SmartKit Computing	See SmartKit Computing XXX User Guide .	SmartKit Computing contains tools used for batch deployment, maintenance, and upgrade of servers. Download address: - Enterprise users: SmartKit Computing - Carrier users: Contact the technical support personnel at your local Huawei office.

Tool	Server Model and Software Version	Description
Smart Provisioning	See Smart Provisioning User Guide .	Smart Provisioning is used to install OSs, configure RAID, and update firmware. Download address: - Enterprise users: Smart Provisioning - Carrier users: Contact the technical support personnel at your local Huawei office.
FusionDirector	See FusionDirector Specifications List .	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 address: - Enterprise users: FusionDirector - Carrier users: Contact the technical support personnel at your local Huawei office.

12 Software and Configuration Utilities

12.1 iBMC

12.2 BIOS

12.1 iBMC

Huawei intelligent Baseboard Management Controller (iBMC) is a Huawei proprietary intelligent system for remotely managing a server. The iBMC complies with IPMI 2.0 and SNMP standards and supports various functions, including KVM redirection, text console redirection, remote virtual media, and hardware monitoring and management.

The iBMC provides 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 details about the iBMC, see [FusionServer Pro X6000 Server iBMC User Guide](#).

12.2 BIOS

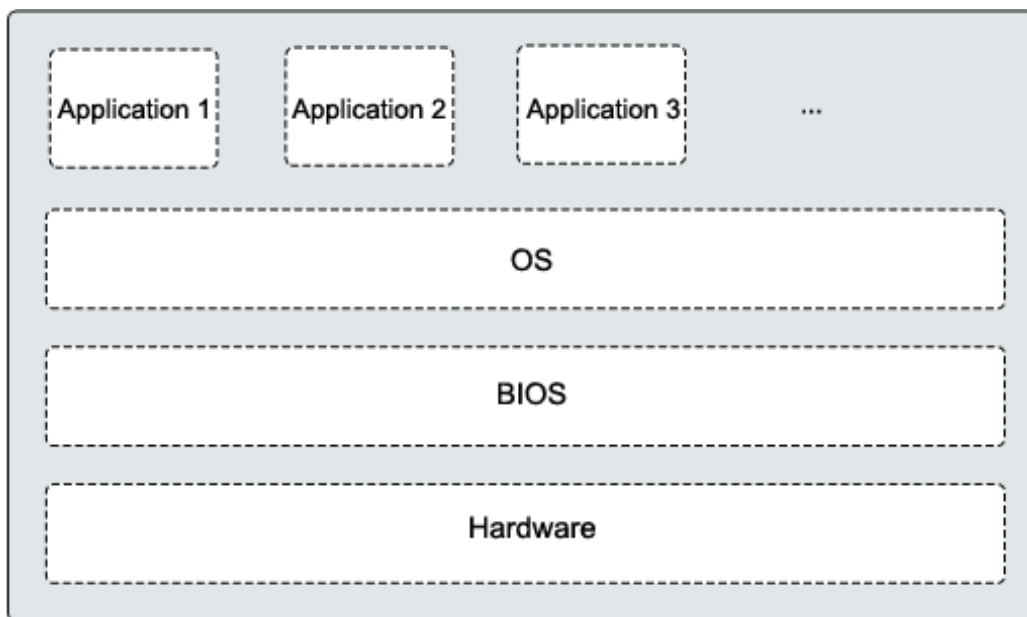
The basic input/output system (BIOS) is the most basic software loaded to a computer hardware system. The BIOS provides an abstraction layer for the operating system (OS) and the hardware to interact with the keyboard, display, and other input/output (I/O) devices.

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

The Huawei Purley-based server is developed based on Insyde code base and uses a proprietary BIOS. It provides a variety of in-band and out-of-band configuration functions as well as high scalability, and supports customization.

For details about the BIOS, see [Huawei Server Purley Platform BIOS Parameter Reference](#).

Figure 12-1 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 Huawei technical support.

Figure A-1 SN example

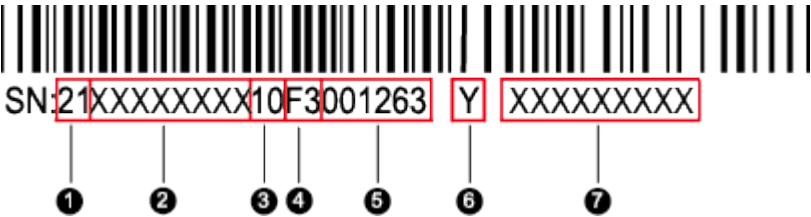


Table A-1 SN description

No.	Description
1	ESN ID (two characters), which can only be 21 .
2	Material ID (eight characters), that is, the processing code.
3	Vendor code (two characters). The value 10 indicates Huawei and other values indicate outsourcing vendors.

No.	Description
4	Year and month (two characters). - The first character indicates the year. - Digits 1 to 9 indicate years 2001 to 2009, respectively. - Letters A to H indicate years 2010 to 2017, respectively. - Letters J to N indicate years 2018 to 2022, respectively. - Letters P to Y indicate years 2023 to 2032, respectively. NOTE The years from 2010 are represented by upper-case letters excluding I, O, and Z because the three letters are similar to the digits 1, 0, and 2. - The second character indicates the month. - Digits 1 to 9 indicate January to September, respectively. - Letters A to C indicate October to December, respectively.
5	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

 NOTE

For configurations not listed in the table, the operating temperature range is 5°C (41°F) to 30°C (86°F). For special configuration and temperature requirements, contact technical support.

A.2.1 Operating Temperature Limitations (Supercapacitor for the RAID Controller Card Configured)

Table A-2 Operating temperature specifications (with a RAID controller card supercapacitor configured)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature
X6000 V5 C00 24 NVMe backplane	16 < Q ≤ 24	P ≤ 165 W	30°C (86°F)
	8 < Q ≤ 16	125 W ≤ P ≤ 165 W	30°C (86°F)
		P < 125 W	35°C (95°F)
X6000 V5 C00 24 SAS backplane	16 < Q ≤ 24	125 W ≤ P ≤ 165 W	32°C (89.6°F)
		P < 125 W	35°C (95°F)
	8 < Q ≤ 16	140 W ≤ P ≤ 165 W	32°C (89.6°F)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature
		$P < 140\text{ W}$	35°C (95°F)
	$0 < Q \leq 8$	$P \leq 165\text{ W}$	35°C (95°F)
X6000 V5 C10 24 NVMe backplane	$16 < Q \leq 24$	$165\text{ W} < P \leq 205\text{ W}$	N/A
		$P \leq 165\text{ W}$	30°C (86°F)
	$8 < Q \leq 16$	$165\text{ W} < P \leq 205\text{ W}$	N/A
		$125\text{ W} \leq P \leq 165\text{ W}$	30°C (86°F)
		$P < 125\text{ W}$	35°C (95°F)
	$0 < Q \leq 8$ (NVMe backplane not used)	/	/
X6000 V5 C10 24 SAS backplane	$16 < Q \leq 24$	$165\text{ W} < P \leq 205\text{ W}$	N/A
		$125\text{ W} \leq P \leq 165\text{ W}$	32°C (89.6°F)
		$P < 125\text{ W}$	35°C (95°F)
	$8 < Q \leq 16$	$165\text{ W} < P \leq 205\text{ W}$	30°C (86°F)
		$140\text{ W} \leq P \leq 165\text{ W}$	32°C (89.6°F)
		$P < 140\text{ W}$	35°C (95°F)
	$0 < Q \leq 8$	$165\text{ W} < P \leq 205\text{ W}$	32°C (89.6°F)
		$P \leq 165\text{ W}$	35°C (95°F)
X6000 V5 C10 12 x 3.5" SAS backplane	$8 < Q \leq 12$	$165\text{ W} < P \leq 205\text{ W}$	N/A
		$125\text{ W} \leq P \leq 165\text{ W}$	32°C (89.6°F)
		$P < 125\text{ W}$	35°C (95°F)
	$4 < Q \leq 8$	$165\text{ W} < P \leq 205\text{ W}$	30°C (86°F)
		$140\text{ W} \leq P \leq 165\text{ W}$	32°C (89.6°F)
		$P < 140\text{ W}$	35°C (95°F)
	$0 < Q \leq 4$	$165\text{ W} < P \leq 205\text{ W}$	32°C (89.6°F)
		$P \leq 165\text{ W}$	35°C (95°F)

A.2.2 Operating Temperature Limitations (Optical Modules Configured)

Table A-3 Operating temperature specifications (with an optical module configured)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature (Onboard Optical Module)	Maximum Temperature (PCIe Optical Module)
X6000 V5 C00 24 NVMe backplane	16 < Q ≤ 24	140 W < P ≤ 165 W	30°C (86°F)	30°C (86°F)
		125 W < P ≤ 140 W	35°C (95°F)	30°C (86°F)
		P ≤ 125 W	35°C (95°F)	35°C (95°F)
	8 < Q ≤ 16	140 W < P ≤ 165 W	30°C (86°F)	30°C (86°F)
		125 W < P ≤ 140 W	35°C (95°F)	30°C (86°F)
		P ≤ 125 W	35°C (95°F)	35°C (95°F)
	0 < Q ≤ 8	140 W < P ≤ 165 W	35°C (95°F)	30°C (86°F)
		P ≤ 140 W	35°C (95°F)	35°C (95°F)
X6000 V5 C00 24 SAS backplane	16 < Q ≤ 24	140 W < P ≤ 165 W	35°C (95°F)	30°C (86°F)
		P ≤ 140 W	35°C (95°F)	30°C/86°F (35°C/95°F for 10GE optical modules)
	8 < Q ≤ 16	140 W < P ≤ 165 W	35°C (95°F)	30°C (86°F)
		P ≤ 140 W	35°C (95°F)	35°C (95°F)
	0 < Q ≤ 8	P ≤ 165 W	35°C (95°F)	35°C (95°F)
X6000 V5 C10 24 NVMe backplane	16 < Q ≤ 24	165 W < P ≤ 205 W	N/A	N/A
		140 W < P ≤ 165 W	30°C (86°F)	30°C (86°F)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature (Onboard Optical Module)	Maximum Temperature (PCIe Optical Module)
		$125\text{ W} < P \leq 140\text{ W}$	35°C (95°F)	30°C (86°F)
		$P \leq 125\text{ W}$	35°C (95°F)	35°C (95°F)
	$8 < Q \leq 16$	$165\text{ W} < P \leq 205\text{ W}$	N/A	N/A
		$140\text{ W} < P \leq 165\text{ W}$	30°C (86°F)	30°C (86°F)
		$125\text{ W} < P \leq 140\text{ W}$	35°C (95°F)	30°C (86°F)
		$P \leq 125\text{ W}$	35°C (95°F)	35°C (95°F)
	$0 < Q \leq 8$	$165\text{ W} < P \leq 205\text{ W}$	30°C (86°F)	30°C (86°F)
		$140\text{ W} < P \leq 165\text{ W}$	35°C (95°F)	30°C (86°F)
		$P \leq 140\text{ W}$	35°C (95°F)	35°C (95°F)
	X6000 V5 C10 24 SAS backplane	$165\text{ W} < P \leq 205\text{ W}$	N/A	N/A
			35°C (95°F)	30°C (86°F)
			35°C (95°F)	30°C/86°F (35°C/95°F for 10GE optical modules)
		$165\text{ W} < P \leq 205\text{ W}$	30°C (86°F)	30°C (86°F)
			35°C (95°F)	30°C (86°F)
			35°C (95°F)	35°C (95°F)
		$0 < Q \leq 8$	35°C (95°F)	30°C (86°F)
			35°C (95°F)	35°C (95°F)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature (Onboard Optical Module)	Maximum Temperature (PCIe Optical Module)
X6000 V5 C10 12 x 3.5" SAS backplane	8 < Q ≤ 12	165 W < P ≤ 205 W	N/A	N/A
		140 W < P ≤ 165 W	35°C (95°F)	30°C (86°F)
		P ≤ 140 W	35°C (95°F)	30°C/86°F (35°C/95°F for 10GE optical modules)
	4 < Q ≤ 8	165 W < P ≤ 205 W	30°C (86°F)	30°C (86°F)
		140 W < P ≤ 165 W	35°C (95°F)	30°C (86°F)
		P ≤ 140 W	35°C (95°F)	35°C (95°F)
	0 < Q ≤ 4	165 W < P ≤ 205 W	35°C (95°F)	30°C (86°F)
		P ≤ 165 W	35°C (95°F)	35°C (95°F)

A.2.3 Operating Temperature Limitations (Avago SAS3004iMR RAID Controller Card + M.2 FRU Configured)

Table A-4 Operating temperature specifications (with Avago SAS3004iMR RAID controller card + M.2 FRU configured)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature
X6000 V5 C00 24 x 2.5" NVMe backplane	16 < Q ≤ 24	140 W < P ≤ 165 W	28°C (82.4°F)
		P ≤ 140 W	32°C (89.6°F)
	8 < Q ≤ 16	140 W < P ≤ 165 W	30°C (86°F)
		P ≤ 140 W	35°C (95°F)
	0 < Q ≤ 8	140 W < P ≤ 165 W	35°C (95°F)
		P ≤ 140 W	35°C (95°F)

Drive Backplane	Drive Quantity (Q)	CPU Power (P)	Maximum Temperature
X6000 V5 C00 24 x 2.5" SAS backplane	16 < Q ≤ 24	140 W < P ≤ 165 W	30°C (86°F)
		P ≤ 140 W	35°C (95°F)
	8 < Q ≤ 16	140 W < P ≤ 165 W	32°C (89.6°F)
		P ≤ 140 W	35°C (95°F)
	0 < Q ≤ 8	P ≤ 165 W	35°C (95°F)
X6000 V5 C10 24 x 2.5" NVMe backplane	16 < Q ≤ 24	165 W < P ≤ 205 W	N/A
		140 W < P ≤ 165 W	30°C (86°F)
		P ≤ 140 W	35°C (95°F)
	8 < Q ≤ 16	165 W < P ≤ 205 W	N/A
		140 W < P ≤ 165 W	32°C (89.6°F)
		P ≤ 140 W	35°C (95°F)
	0 < Q ≤ 8	165 W < P ≤ 205 W	28°C (82.4°F)
		P ≤ 165 W	35°C (95°F)
X6000 V5 C10 24 x 2.5" SAS backplane	16 < Q ≤ 24	165 W < P ≤ 205 W	N/A
		140 W < P ≤ 165 W	30°C (86°F)
		P ≤ 140 W	35°C (95°F)
	8 < Q ≤ 16	165 W < P ≤ 205 W	28°C (82.4°F)
		P ≤ 165 W	35°C (95°F)
	0 < Q ≤ 8	165 W < P ≤ 205 W	32°C (89.6°F)
		P ≤ 165 W	35°C (95°F)
X6000 V5 C10 12 x 3.5" SAS backplane	8 < Q ≤ 12	165 W < P ≤ 205 W	N/A
		140 W < P ≤ 165 W	30°C (86°F)
		P ≤ 140 W	35°C (95°F)
	4 < Q ≤ 8	165 W < P ≤ 205 W	30°C (86°F)
		140 W < P ≤ 165 W	35°C (95°F)
	0 < Q ≤ 4	P ≤ 205 W	35°C (95°F)

A.2.4 Operating Temperature Limitations (Different Models of Processors)

Table A-5 Operating temperature specifications (different models of processors)

Drive Backplane	Processor Model	Heat Sink	Drive and Memory Configuration	Max. Air Inlet Temperature
X6000 V5 C00 24 x 2.5" SAS backplane	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (P ≤ 165 W) ^a	Narrow conjoined heat sinks	• Drives ≤ 24 • DIMMs ≤ 16	35°C (95°F)
X6000 V5 C00 24 x 2.5 NVMe backplane	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (P ≤ 165 W) ^a	Narrow conjoined heat sinks	• Drives ≤ 24 • DIMMs ≤ 16	35°C (95°F)
X6000 V5 C10 24 x 2.5" NVMe backplane	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (165 W < P ≤ 205 W)	Wide conjoined heat sinks	• 0 < drives ≤ 8 • DIMMs ≤ 12	30°C (86°F)
	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (P ≤ 165 W)	Narrow conjoined heat sinks	• Drives ≤ 24 • DIMMs ≤ 16	35°C (95°F)
		Wide conjoined heat sinks ^b	• 0 < drives ≤ 8 • DIMMs ≤ 12	30°C (86°F)
	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (165 W < P ≤ 205 W)	Wide conjoined heat sinks	• 8 < drives ≤ 16 • DIMMs ≤ 12	30°C (86°F)
X6000 V5 C10 24 x 2.5" SAS backplane			• 0 < drives ≤ 8 • DIMMs ≤ 12	35°C (95°F)

Drive Backplane	Processor Model	Heat Sink	Drive and Memory Configuration	Max. Air Inlet Temperature
	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (P ≤ 165 W)	Narrow conjoined heat sinks	• Drives ≤ 24 • DIMMs ≤ 16	35°C (95°F)
		Wide conjoined heat sinks ^b	• 8 < drives ≤ 16 • DIMMs ≤ 12	30°C (86°F)
			• 0 < drives ≤ 8 • DIMMs ≤ 12	35°C (95°F)
X6000 V5 C10 12 x 3.5" SAS backplane	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (165 W < P ≤ 205 W)	Wide conjoined heat sinks	• 4 < drives ≤ 8 • DIMMs ≤ 12	30°C (86°F)
			• 0 < drives ≤ 4 • DIMMs ≤ 12	35°C (95°F)
	Intel® Xeon® Scalable (Skylake and Cascade Lake) processor (P ≤ 165 W)	Narrow conjoined heat sinks	• Drives ≤ 12 • DIMMs ≤ 16	35°C (95°F)
		Wide conjoined heat sinks ^b	• 4 < drives ≤ 8 • DIMMs ≤ 12	30°C (86°F)
			• 0 < drives ≤ 4 • DIMMs ≤ 12	35°C (95°F)
• a: The C00 model does not support Intel® Xeon® Scalable (Gold 6144, Gold 6146, Gold 6244, and Gold 6252N) processors. • b: When Intel® Xeon® Scalable (Gold 6144, Gold 6146, Gold 6244, or Gold 6252N) processors are configured, wide conjoined heat sinks are required to meet the high heat dissipation requirement.				

A.3 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 RAS features, see [Huawei Server Purley Platform BIOS Parameter Reference](#).

Table A-6 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.

Module	Feature	Description
	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 Resilient Boot)	Isolates a faulty CPU core during startup to 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.

Module	Feature	Description
	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.

B Glossary

B.1 A-E

B

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

E

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

B.2 F-J

G

Gigabit Ethernet (GE)	An extension and enhancement of traditional shared media Ethernet standards. It is compatible with 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
BMC	Baseboard Management Controller

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