

**CH242 V3 Compute Node
V100R001**

User Guide

Issue	16
Date	2023-10-30



Copyright © Huawei Technologies Co., Ltd. 2023. 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://e.huawei.com>

Security Declaration

Product Life Cycle

Huawei's regulations on product life cycle are subject to the Product End of Life Policy. For details about the policy, see the following website: <https://support.huawei.com/ecolumnsweb/en/warranty-policy>

Vulnerability

Huawei's regulations on product vulnerability management are subject to "Vul. Response Process". For details about the policy, see the following website: <https://www.huawei.com/en/psirt/vul-response-process>

For enterprise customers who need to obtain vulnerability information, visit: <https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Preconfigured Digital Certificate

Huawei has released the Huawei Preset Digital Certificate Disclaimer for the preconfigured digital certificates delivered with devices. For details about the disclaimer, visit the following website: <https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789>

Life Cycle of Product Documentation

Huawei released the Huawei Product Documentation Lifecycle Policy for after-sales customer documentation. For details about this policy, see the website of Huawei's official website.: <https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761>

About This Document

Purpose

This document describes the CH242 V3 in terms of its appearance, functions, structure, configuration, how to install and remove it, and how to install the operating system (OS) supported.

The document provides guidance on how to replace internal components, configure boot options, redundant array of independent disks (RAIDs), and IP addresses for the iMana 200 on the server, log in to the web user interface (WebUI), and install the OS.

Intended Audience

This document is intended for the following engineers:

- Technical support engineers
- Installation and commissioning engineers
- Onsite maintenance engineers
- System maintenance engineers

Symbol Conventions

Symbols that may be found in this document are defined in the following table.

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.

Symbol	Description
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Changes between document issues are cumulative. Therefore, the latest document issue contains all the changes made in earlier issues.

Issue	Release Date	Change Description
16	2023-10-30	Added related precautions in 5.27 Removing a BIOS Battery .
15	2022-06-30	Added the method of burning the original device serial number to the new mainboard.
14	2021-06-08	Updated environment specifications. For details, see 2.10 Technical Specifications .
13	2019-11-30	This issue is the thirteenth official release.
12	2019-07-08	Modified 5.21 Removing a microSD Card and 5.22 Installing a microSD Card .
11	2017-12-28	Added 6.8 Erasing Storage Media Data .
10	2017-01-18	Added support for the CPU installation tool.
09	2016-08-05	This issue is the ninth official release.
08	2016-03-31	This issue is the eighth official release.

Issue	Release Date	Change Description
07	2015-10-19	- Modified 2.10 Technical Specifications and updated the storage temperature and humidity. - Modified 5.8 Installing a PCIe Card (Riser Card Slots 1 and 2). - Updated the figures of the drive backplane in 2.7 Physical Structure (4HDD) and 2.6 Physical Structure (8HDD). - Added the description of the product serial number format in 2.2 Appearance.
06	2015-02-16	Optimized the table content in 2.7 Physical Structure (4HDD) and 2.6 Physical Structure (8HDD) .
05	2014-11-10	- Added sections 5.30 Installing the Mainboard and Compute Node Case and 5.29 Removing the Mainboard and Compute Node Case. - Modified 5.23 Removing an iBBU and 5.24 Installing an iBBU.
04	2014-09-15	- Deleted the trademark Tecal from the document. - Updated the power consumption and altitude in 2.10 Technical Specifications. - Added the USB 2.0 port in the component diagrams and component descriptions in 2.7 Physical Structure (4HDD) and 2.6 Physical Structure (8HDD).
03	2014-07-30	- Modified the description of CH242 V3 8HDD in 2.6 Physical Structure (8HDD) and CH242 V3 4HDD in 2.7 Physical Structure (4HDD). - Modified 2.10 Technical Specifications, and added the CH242 V3 8HDD key components to 2.6 Physical Structure (8HDD) and the CH242 V3 4HDD key components to 2.7 Physical Structure (4HDD). - Added the link of the compatibility list of supported software and hardware to 2.9 Software and Hardware Compatibility. - Modified the RAID configuration and 6.6 Reconfiguring the RAID, and described the models supported by the RAID controller card.
02	2014-05-13	Added the description of video cards in 2.10 Technical Specifications .
01	2014-02-28	This issue is the first official release.

Contents

About This Document.....	iii
1 Safety Instructions.....	1
2 Introduction.....	5
2.1 Functions.....	5
2.2 Appearance.....	6
2.3 Indicators.....	9
2.4 Ports.....	11
2.5 Drive numbering.....	12
2.6 Physical Structure (8HDD).....	12
2.7 Physical Structure (4HDD).....	20
2.8 Logical Structure.....	28
2.9 Software and Hardware Compatibility.....	30
2.10 Technical Specifications.....	30
3 Installing and Removing the CH242 V3.....	33
3.1 Installing a CH242 V3.....	33
3.2 Removing a CH242 V3.....	40
4 Configuring the CH242 V3.....	45
4.1 Overview.....	45
4.2 Default Information.....	48
4.3 Checking the CH242 V3.....	50
4.4 Changing the Default iMana 200 User Password.....	56
4.5 Configuring the iMana 200 IP Address.....	59
4.6 Changing the iMana 200 U-boot Password.....	60
4.7 Logging In to the Real-Time Desktop.....	62
4.8 Configuring the RAID.....	68
4.9 Configuring the BIOS.....	68
4.10 Installing the OS.....	72
5 Removing and Installing Components of the CH242 V3.....	74
5.1 Removing a Hard Disk.....	75
5.2 Installing a Hard Disk.....	77
5.3 Removing a PCIe SSD Disk (8HDD).....	80

5.4 Installing a PCIe SSD Disk (8HDD).....	81
5.5 Removing the Cover.....	83
5.6 Installing the Cover.....	84
5.7 Removing a PCIe Card (Riser Card Slots 1 and 2).....	85
5.8 Installing a PCIe Card (Riser Card Slots 1 and 2).....	87
5.9 Removing a PCIe Card (Hard Disk Backplane).....	90
5.10 Installing a PCIe Card (Hard Disk Backplane).....	92
5.11 Removing a DIMM and an Air Duct.....	95
5.12 Installing a DIMM and an Air Duct.....	96
5.13 Removing a USB Flash Drive.....	99
5.14 Installing a USB Flash Drive.....	101
5.15 Removing a CPU.....	103
5.16 Installing a CPU.....	107
5.17 Removing a TPM.....	114
5.18 Installing a TPM.....	116
5.19 Removing the Mezz Modules.....	118
5.20 Installing the Mezz Modules.....	121
5.21 Removing a microSD Card.....	125
5.22 Installing a microSD Card.....	127
5.23 Removing an iBBU.....	130
5.24 Installing an iBBU.....	132
5.25 Removing a RAID Controller Card.....	135
5.26 Installing a RAID Controller Card.....	138
5.27 Removing a BIOS Battery.....	143
5.28 Installing a BIOS Battery.....	144
5.29 Removing the Mainboard and Compute Node Case.....	146
5.30 Installing the Mainboard and Compute Node Case.....	148
6 Common Operations.....	152
6.1 Logging In to a Compute Node or a Switch Module over MM910 SOL.....	152
6.2 Logging In to the MM910 CLI Over a Network Port by Using PuTTY.....	155
6.3 Logging In to a Device Over a Serial Port by Using PuTTY.....	158
6.4 Performing Operations by Using the Local KVM Connected to the MM910.....	160
6.5 Logging in to the MM910 WebUI.....	164
6.6 Reconfiguring the RAID.....	170
6.7 Powering On and Off the CH242 V3.....	171
6.7.1 Powering On the CH242 V3.....	171
6.7.2 Powering Off the CH242 V3.....	177
6.8 Erasing Storage Media Data.....	185
7 U-boot.....	191
7.1 Logging In to the U-boot.....	191
7.2 U-boot Commands.....	193

1 Safety Instructions

General Instructions

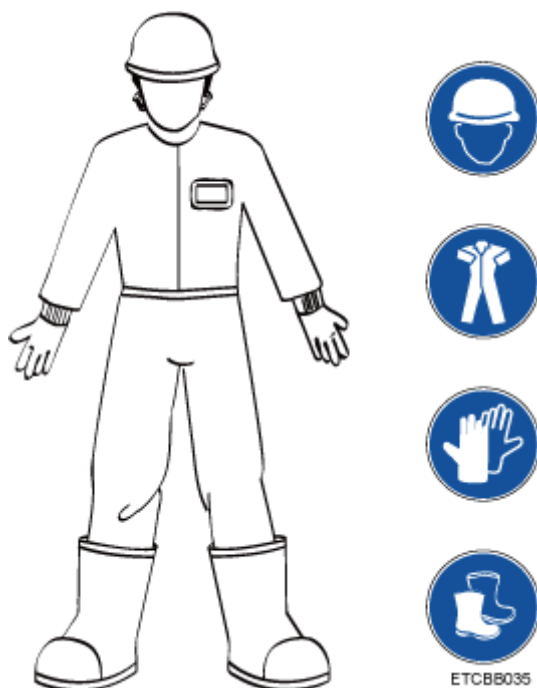
- Comply with all local laws and regulations when installing the hardware. The safety instructions in this document are only supplemental to local laws and regulations.
- Observe the safety instructions that accompany all "DANGER", "WARNING", "CAUTION", and "NOTICE" symbols in this document. These instructions are only supplemental to other safety measures.
- When installing hardware, follow all safety instructions provided on the device labels and in this document.
- Operations involving high voltages or moving equipment must be performed by authorized, qualified personnel.
- Take protective measures before operating the device in residential areas as it is likely to cause radio interference.

Personal Safety

To ensure personal safety, note the following points:

- Only personnel certified or authorized by Huawei are allowed to install the hardware.
- Discontinue any dangerous operations and take protective measures. Report any problems that may cause personal injury or equipment damage to a project supervisor.
- Do not perform certain operations, including moving devices, installing racks, and installing power cables, on rainy days or during thunderstorms.
- Wear clean protective gloves, ESD clothing, a protective hat, and protective shoes, as shown in [Figure 1-1](#).

Figure 1-1 Protective clothing



- Before carrying devices, note the following points:
 - Do not carry more weight than is permitted by local laws or regulations.
 - Arrange for enough personnel to carry the devices.
- Before touching a device, ensure that you are wearing ESD clothing and ESD gloves (or wrist strap), and remove any conductive objects (such as watches and jewelry).

Figure 1-2 shows conductive objects that must be removed before you touch a device.

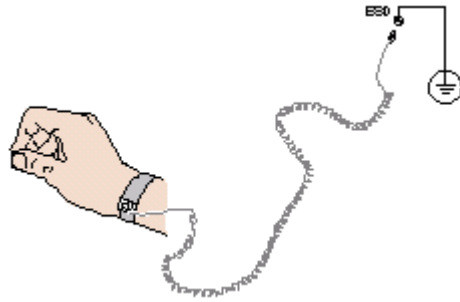
Figure 1-2 Conductive objects to be removed



Figure 1-3 shows how to wear an ESD wrist strap.

- Secure the ESD wrist strap around your wrist.
- Fasten the strap buckle and ensure that the ESD wrist strap is touching your skin.
- Insert the ground terminal attached to the ESD wrist strap into the jack on the grounded rack or chassis.

Figure 1-3 Wearing an ESD wrist strap



- Exercise caution when using tools that could cause personal injury.
- Use a stacker to lift a device above shoulder height. This will prevent it from falling.
- Do not touch high-voltage cables directly or indirectly.
- Before powering on a device, ensure that it has been properly grounded.
- Do not use a ladder alone.
- To avoid damaging your eyes when installing, testing, or replacing optical cables, do not look into optical ports without eye protection.

Equipment Safety

- Use the recommended power cables at all times.
- Always use the power cables delivered with the devices.
- Wear ESD clothing and gloves before handling a device. This prevents electrostatic damage.
- When moving a device, make sure to hold the handles of the device (or the bottom of the devices). Do not hold the handles of the installed modules, such as power modules, fan modules, hard disks, or boards.
- Exercise caution to prevent damage to the device when using tools during installation or maintenance.
- Connect the power cables from the active power supply to one power distribution unit (PDU), and the cables from the backup power supply to another PDU.
- Ensure that a device is properly grounded before powering it on.

Transportation Precautions

Exercise caution when transporting equipment.

- The logistics company engaged to transport the equipment must be reliable and comply with international standards for transporting electronics.
- Ensure that the equipment being transported is always upright. Take necessary precautions to prevent collisions, corrosion, package damage, damp conditions and pollution.
- Transport the equipment in its original packaging.
- Package heavy, bulky parts (such as chassis and blades) and fragile parts (such as PCIe GPUs and SSDs) separately.

 NOTE

Use the Huawei Server Compatibility Checker for details about parts supported by a server.

- Ensure that all devices are powered off before transportation.
- Do not transport hazardous materials.

For further details, contact the manufacturer.

Limits for the Maximum Weight Carried Per 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 1-1 lists the maximum weight one person is permitted to carry as stipulated by a number of organizations.

Table 1-1 Maximum weight one person is permitted to carry

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)	• Men: 15/33.01 • Women: 10/22.05

2 Introduction

- [2.1 Functions](#)
- [2.2 Appearance](#)
- [2.3 Indicators](#)
- [2.4 Ports](#)
- [2.5 Drive numbering](#)
- [2.6 Physical Structure \(8HDD\)](#)
- [2.7 Physical Structure \(4HDD\)](#)
- [2.8 Logical Structure](#)
- [2.9 Software and Hardware Compatibility](#)
- [2.10 Technical Specifications](#)

2.1 Functions

This topic describes the functions and components of the CH242 V3.

The CH242 V3 compute node(CH242 V3 for short) is a large-memory, full-width compute node that uses the new-generation Intel® Xeon® E7-4800 v2 or E7-8800 v2 (IVY Bridge-EX) processors. It provides strong computing capabilities and flexible scalability.

The CH242 V3 has two types of specifications:

- CH242 V3 8HDD
Supports SAS HDDs, SATA HDDs, and SSDs, and provides two customized PCIe cards.
- CH242 V3 4HDD
Supports SAS HDDs, SATA HDDs, and SSDs, and provides one standard PCIe card of full-height, half-length and two customized PCIe cards.

The CH242 V3 is installed in an E9000 chassis and managed by the MM910 management module in a centralized manner.

The CH242 V3 features high density, large-capacity memory and storage, high network I/O capability, and high reliability, suiting enterprise applications such as virtualization and high-performance computing (HPC).

2.2 Appearance

This topic describes the appearance, front panel, installation position, and slot numbering of the CH242 V3.

Appearance

Figure 2-1 shows the CH242 V3 8HDD appearance.

Figure 2-1 CH242 V3 8HDD appearance



Figure 2-2 shows the CH242 V3 4HDD appearance.

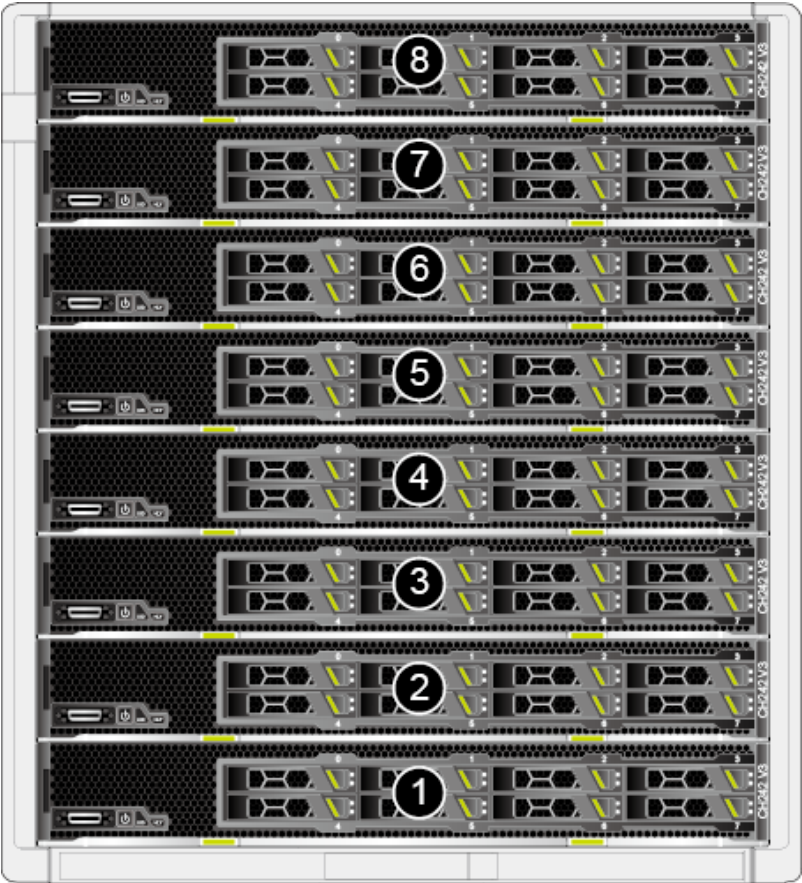
Figure 2-2 CH242 V3 4HDD appearance



Installation Position

The CH242 V3s are installed in the front full-width slots of the E9000 chassis. A chassis houses a maximum of eight CH242 V3. The installation positions and slots for the CH242 V3 8HDD are the same as those for the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 2-3](#) shows the installation positions of the CH242 V3 and their slot numbers in the chassis.

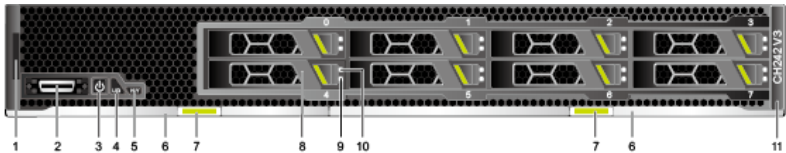
Figure 2-3 Installation positions and slot numbering



Front panel

[Figure 2-4](#) shows the front panel of a CH242 V3 8HDD.

Figure 2-4 CH242 V3 8HDD front panel

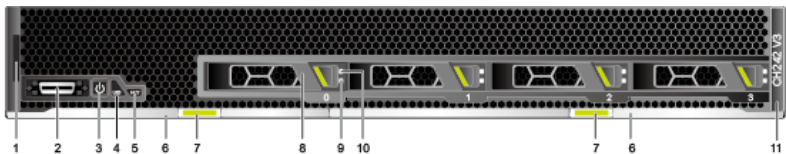


1	Customization label (with an ESN label)	2	High-density port
---	---	---	-------------------

3	Power button/indicator	4	UID button/indicator
5	HLV indicator	6	Ejector lever
7	Spring	8	Hard disk
9	Hard disk active indicator	10	Hard disk fault indicator
11	Product model	-	-

Figure 2-5 shows the front panel of a CH242 V3 4HDD.

Figure 2-5 CH242 V3 4HDD front panel



1	Customization label (with an ESN label)	2	High-density port
3	Power button/indicator	4	UID button/indicator
5	HLV indicator	6	Ejector lever
7	Spring	8	Hard disk
9	Hard disk active indicator	10	Hard disk fault indicator
11	Product model	-	-

ESNs

An Equipment Serial Number (ESN) uniquely identifies a product. An ESN is required when you request Huawei technical support.

Figure 2-6 shows the ESN format.

Figure 2-6 ESN example



Callout No.	Description
1	ESN ID (two characters), which is 21 by default.
2	Material identification code (eight characters), that is, processing code.
3	Vendor code (two characters). The code 10 indicates Huawei, and other values indicate outsourcing vendors.
4	Year and month (two characters). • The first character indicates the year, where: – Digits 1 to 9 indicate 2001 to 2009, respectively. – Letters A to H indicate 2010 to 2017, respectively. – Letters J to N indicate 2018 to 2022, respectively. – Letters P to Y indicate 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, where: – Digits 1 to 9 indicate January to September, respectively. – Letters A to C indicate October to December, respectively.
5	Serial number (six characters).
6	RoHS compliance (one character). Y indicates environmental protection processing.
7	Internal model, that is, product name.

2.3 Indicators

This topic describes the names, meanings, colors, and status of the indicators on the CH242 V3.

You can learn about the status of the CH242 V3 by observing the indicators. [Table 2-1](#) describes the indicators on the CH242 V3.

Table 2-1 Indicators on the front panel

Indicator	Meaning	Color	State Description
PWR	Power button/ indicator	Yellow and green	• Off: The compute node is not powered on. • Blinking yellow: The power button on the compute node is locked. When iMana 200 is being started during the compute node power-on process, the power button is locked. • Steady yellow: The compute node is to be powered on. • Steady green: The compute node is properly powered on. NOTE • When the server is powered on, pressing this button will shut down the OS properly or cause the server to become unresponsive. • When the server is powered on, holding down this button for 6 seconds will power off the server. • When the server is in the standby state, pressing this button will power on the server.
UID	UID button/ indicator	Blue	The Unit Identification (UID) indicator helps locate a compute node in a chassis. You can control the UID indicator status (off, on, or blinking) by remotely using the MM910. • Off: The compute node is not located or is not powered on. • On: The compute node is located. • Blinking: The compute node is being located. NOTE • You can press this button to turn on or off the UID indicator. • You can hold down the UID button for 4 to 6 seconds to reset iMana 200.

Indicator	Meaning	Color	State Description
HLV	Health status indicator	Red and green	• Off: The compute node is not powered on. • Steady green: The compute node hardware is operating properly. • Blinking red (at 1 Hz): A major alarm is generated for the compute node. • Blinking red (at 5 Hz): A critical alarm is generated for the compute node, or the compute node is not securely installed.
	Hard disk active indicator	Green	• Off: The hard disk is not detected or is faulty. • Blinking green: Data is being read from or written to the hard disk. • Steady green: The hard disk is inactive.
	Hard disk fault indicator	Yellow	• Off: The hard disk is operating properly. • Blinking yellow: The hard disk is being located, or RAID is being rebuilt. • Steady yellow: The hard disk is not detected or is faulty.

2.4 Ports

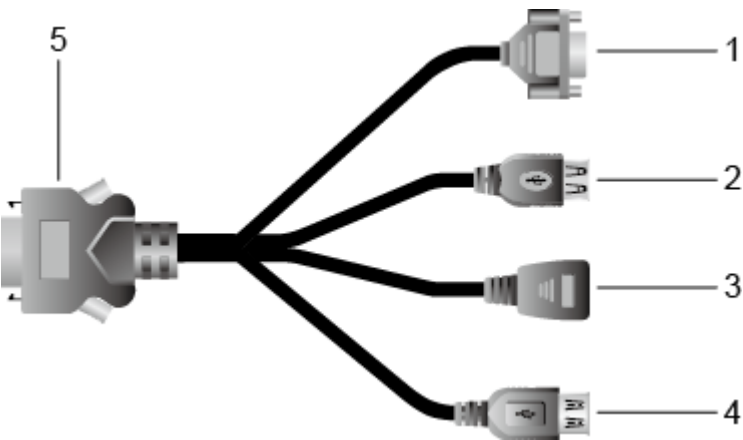
This topic describes the ports on the CH242 V3 and provides detailed information about the high-density port.

Table 2-2 describes the ports on the CH242 V3.

Table 2-2 Port description

Port	Category	Quantity	Description
High-density port	-	1	The high-density port on the front panel connects to a high-density cable, which provides a DB15 video graphics array (VGA) video port, three USB 2.0 ports, and a RJ45 serial port.

Figure 2-7 High-density cable



1	VGA port	2	Two USB 2.0 ports
3	Serial port	4	One USB 2.0 port
5	High-density port	-	-

2.5 Drive numbering

This section describes the slot information about the CH242 V3 drive numbers.

Figure 2-8 Drive numbering (CH242 V3 8HDD)

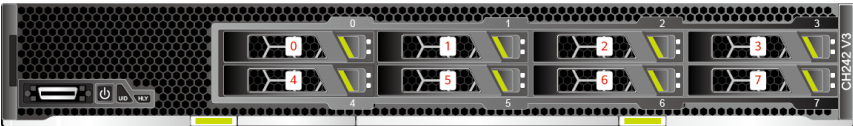
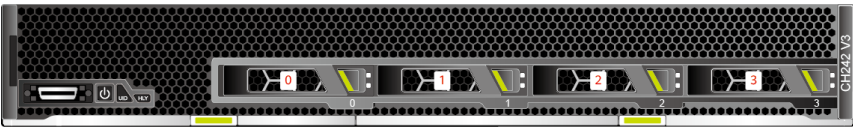


Figure 2-9 Drive numbering (CH242 V3 4HDD)

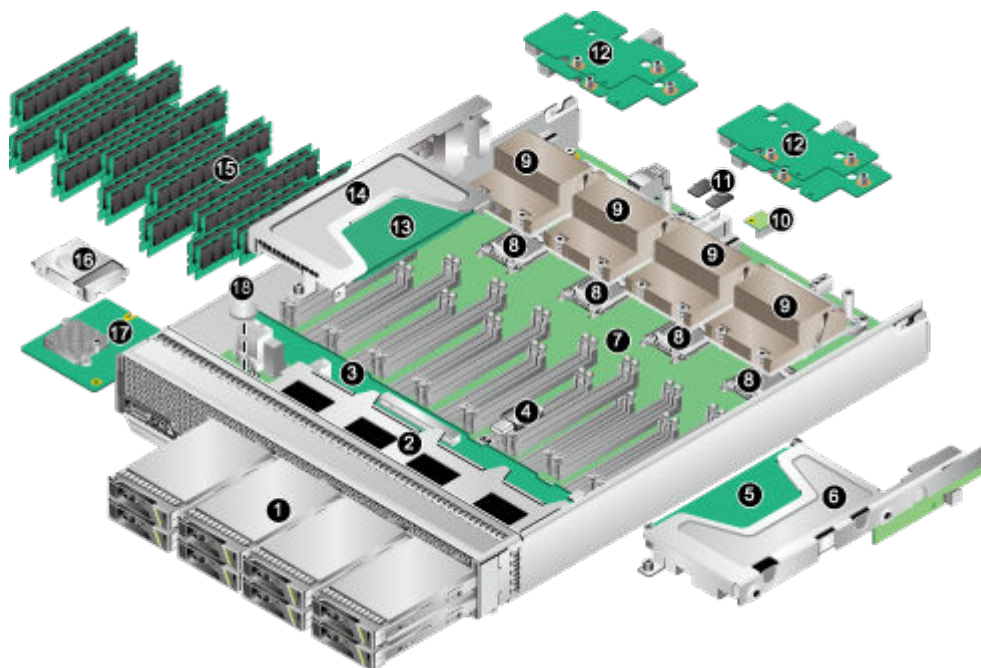


2.6 Physical Structure (8HDD)

This section describes the components of the CH242 V3 8HDD and the layout of the mainboard and drive backplane.

CH242 V3 8HDD components

Figure 2-10 shows the components of the CH242 V3 8HDD.

Figure 2-10 Components

1	Drives	2	Drive cage
3	Drive backplane	4	(Optional) USB 2.0
5	(Optional) PCIe card 1	6	(Optional) PCIe card tray 1
7	Mainboard	8	CPU
9	Heat sink	10	(Optional) TPM
11	(Optional) MicroSD card	12	Mezzanine card
13	(Optional) PCIe card 2	14	(Optional) PCIe card tray 2
15	DIMM	16	(Optional) iBBU
17	Screw-in RAID controller card	18	BIOS battery

Table 2-3 describes the components of the CH242 V3 8HDD.

Table 2-3 Component description

No.	Component	Remarks
1	Drives	The compute node supports a maximum of eight 2.5-inch HDDs or SSDs and allows mixed configuration of HDDs and SSDs. Each HDD can be installed and removed independently. The drive backplane provides eight SAS/SATA ports for connecting to HDDs.
2	Drive cage	The drive cage holds drives.
3	Drive backplane	The drive backplane helps expand storage capacity and control drives in real time.
4	(Optional) USB 2.0	The USB port on the mainboard connects to a USB 2.0 device. The size of the device cannot exceed 40.00 mm x 15.00 mm x 13.00 mm.
5	(Optional) PCIe card 1	PCIe card 1 is on the left of the mainboard and can be a customized PCIe card or a standard PCIe SSD. If a standard PCIe card of full-height, half-length is installed, no DIMMs can be inserted into the 10 DIMM slots below the PCIe card due to space limitations. NOTE - You can configure either PCIe card tray 1 and PCIe card 1 or PCIe card tray 2 and PCIe card 2. - When PCIe card 1 is a standard PCIe SSD, you need to remove the below 10 DIMMs and configure air ducts in the middle and right. The CH242 V3 supports a maximum operating temperature of 35°C.
6	(Optional) PCIe card tray 1	The PCIe card tray is placed above the DIMMs. Each PCIe card tray provides one PCIe x16 slot by using a riser card.
7	Mainboard	The mainboard holds the CPUs, DIMMs, drive interface modules, power control module, iMana 200, logic module, chipset, and video adapter. The compute node chipset uses the Intel® C602J chip. The video card is integrated in the FPGA chip of iMana 200 and provides 16 MB display memory. The maximum resolution is 1280 x 1024 at 60 Hz with 16 M colors.

No.	Component	Remarks
8	CPU	The mainboard supports two or four processors: • The following CPU models are supported: – Intel® Xeon® E7-4800 v2 (Ivy Bridge-EX) processors of 105 W, 130 W, and 155 W, with a maximum of 15 cores per processor. – Intel® Xeon® E7-8800 v2 (Ivy Bridge-EX) processors of 105 W, 130 W, and 155 W, with a maximum of 15 cores per processor. • Each processor integrates a memory controller for supporting eight memory channels. Each channel supports one DDR3 DIMMs of 1333 MHz or 1600 MHz. • Each processor integrates a PCIe controller supporting PCIe 3.0. Two processors provide 32 lanes. • Every two CPUs are interconnected through one QuickPath Interconnect (QPI) link, delivering up to 8.0 GT/s. • Maximum clock speed: 2.8 GHz.
9	Heat sink	The heat sink is used to cool processors. Each processor is configured with one heat sink.
10	(Optional) TPM	The TPM is a cost-effective security solution that complies with the Trusted Computing Group (TCG) standards. It enhances platform security by preventing viruses or unauthorized operations.
11	(Optional) MicroSD card	The mainboard provides two microSD card slots. Each slot supports a microSD card with a maximum capacity of 32 GB, and the microSD card can be used as the boot medium for a compute node. If two microSD cards are installed, they are configured as RAID 1.

No.	Component	Remarks
12	Mezzanine card	The CH242 V3 provides four mezzanine card connectors to connect to switch modules or pass-through modules through the backplane. • Mezz1 and Mezz3 are upper-layer daughter cards, and Mezz2 and Mezz4 are lower-layer daughter cards. • Socket CPU 2 provides PCIe x16 bandwidth for connecting to Mezz1 and Mezz2 respectively, socket CPU 3 provides PCIe x16 bandwidth for connecting to Mezz3, and socket CPU 4 provides PCIe x16 bandwidth for connecting to Mezz4. • Mezz1 and Mezz3 connect to slots 2X and 3X at the rear of the E9000 chassis. • Mezz2 and Mezz4 connect to slots 1E and 4E at the rear of the E9000 chassis.
13	(Optional) PCIe card 2	PCIe card 2 is on the right of the mainboard and can be a customized PCIe card or a standard GPU. If a standard PCIe card of full-height, half-length is installed, no DIMMs can be inserted into the 10 DIMM slots below the PCIe card due to space limitations. NOTE • You can configure either PCIe card tray 1 and PCIe card 1 or PCIe card tray 2 and PCIe card 2. • When PCIe card 2 is a standard GPU, you need to remove the below 10 DIMMs and configure air ducts in the middle and right. The CH242 V3 supports a maximum operating temperature of 35°C.
14	(Optional) PCIe card tray 2	The PCIe card tray is placed above the DIMMs. Each PCIe card tray provides one PCIe x16 slot by using a riser card.

No.	Component	Remarks
15	DIMM	The mainboard provides up to 32 slots for installing DDR3 DIMMs (8 DIMMs for each processor). • Maximum memory speed: 1600 MHz • Memory protection: ECC, memory mirroring, and memory sparing • DIMM types: RDIMMs and LRDIMMs. DIMMs on the same compute node must be of the same type (RDIMM or LRDIMM) and the same specifications (capacity, bit width, rank, and height), and have the same BOM code. To query DIMM BOM numbers, use the Computing Product Compatibility Checker. – RDIMMs: up to 512 GB for 32 x 16 GB RDIMMs and four CPUs – LRDIMMs: up to 2 TB for 32 x 64 GB LRDIMMs and four CPUs
16	(Optional) iBBU	When the LSISAS2208 controller card is installed, you can install an iBBU to protect data from power failures.
17	Screw-in RAID controller card	It provides eight SAS or SATA ports for drive expandability. The CH242 V3 8HDD supports LSISAS2208 and LSISAS2308 RAID controller cards. • LSISAS2208: supports RAID 0, 1, 5, 6, 10, 50, and 60. • LSISAS2308: supports RAID 0, 1, 1E, and 10.
18	BIOS battery	When the compute node is not powered on, the BIOS battery supplies power to the real time clock (RTC).

PCIe Slots

[Table 2-4](#) describes the mapping between PCIe slots and CPUs, and the PCIe specifications of the CH242 V3.

NOTE

The PCIe devices mapping to vacant CPU sockets are unavailable.

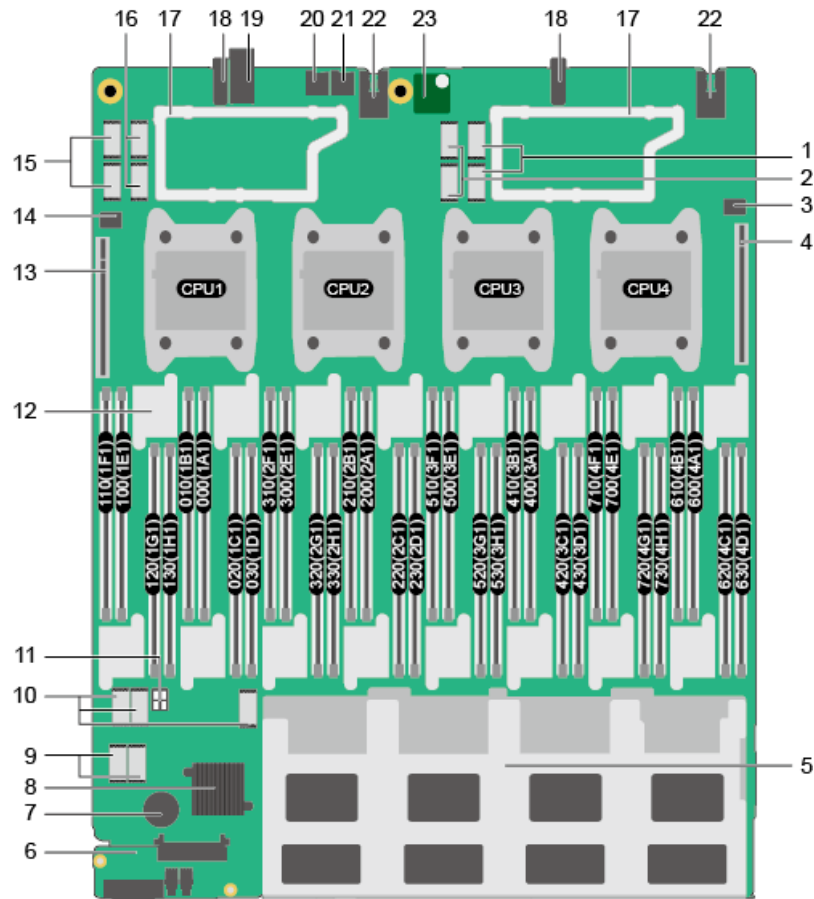
Table 2-4 PCIe slots

PCIe Device	Device Name on the BMC	CPU Connected	PCIe Standard	Connect or Width	Bus Width	Port No.	Slot Size
Screw-in RAID controller card	\	CPU 1	PCIe3.0	x8	x8	Port 3C	Non-standard device
Mezz1	\	CPU 2	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 3A or (Port 3A+Port 3C)	Non-standard device
Mezz2	\	CPU 2	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 2A or (Port 2A+Port 2C)	Non-standard device
Mezz3	\	CPU 3	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 2A or (Port 2A+Port 2C)	Non-standard device
Mezz4	\	CPU 4	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 3A or (Port 3A+Port 3C)	Non-standard device
PCIe Riser1	PCIe Riser Card1	CPU 3	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 3A or (Port 3A+Port 3C)	Full-height half-length (FHHL)
PCIe Riser2	PCIe Riser Card2	CPU 4	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 2A or (Port 2A+Port 2C)	Full-height half-length (FHHL)
PCIe SSD0	Disk0	CPU 1	PCIe3.0	x4	x4	Port 2D	2.5-inch drive
PCIe SSD1	Disk1	CPU 1	PCIe3.0	x4	x4	Port 2C	2.5-inch drive
PCIe SSD2	Disk2	CPU 1	PCIe3.0	x4	x4	Port 3C	2.5-inch drive
PCIe SSD3	Disk3	CPU 1	PCIe3.0	x4	x4	Port 3D	2.5-inch drive

Mainboard Layout

Figure 2-11 shows the positions of connectors and other components on the mainboard of the CH242 V3 8HDD.

Figure 2-11 Positions of the connectors and components



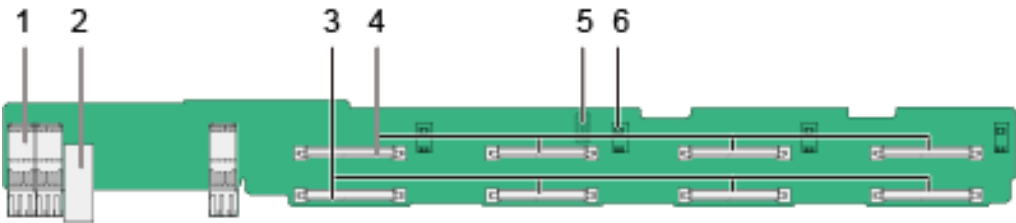
1	Mezzanine card connector 4	2	Mezzanine card connector 3
3	Riser card power connector 2	4	Riser card connector 2
5	Drive cage	6	User interface board
7	BIOS battery	8	PCH (Platform Controller Hub)
9	RAID controller card connectors	10	Drive backplane connector
11	HDD backplane power connector	12	Jordan Creek
13	Riser card connector 1	14	Riser card power connector 1
15	Mezzanine card connector 1	16	Mezzanine card connector 2
17	Mezzanine card tray	18	Positioning pin

19	Midplane signal connector	20	microSD card connector 2
21	microSD card connector 1	22	Power connector
23	TPM connector	-	-

Drive Backboard Layout

Figure 2-12 shows the positions of connectors and other components on the CH242 V3 8HDD drive backplane.

Figure 2-12 Drive backplane



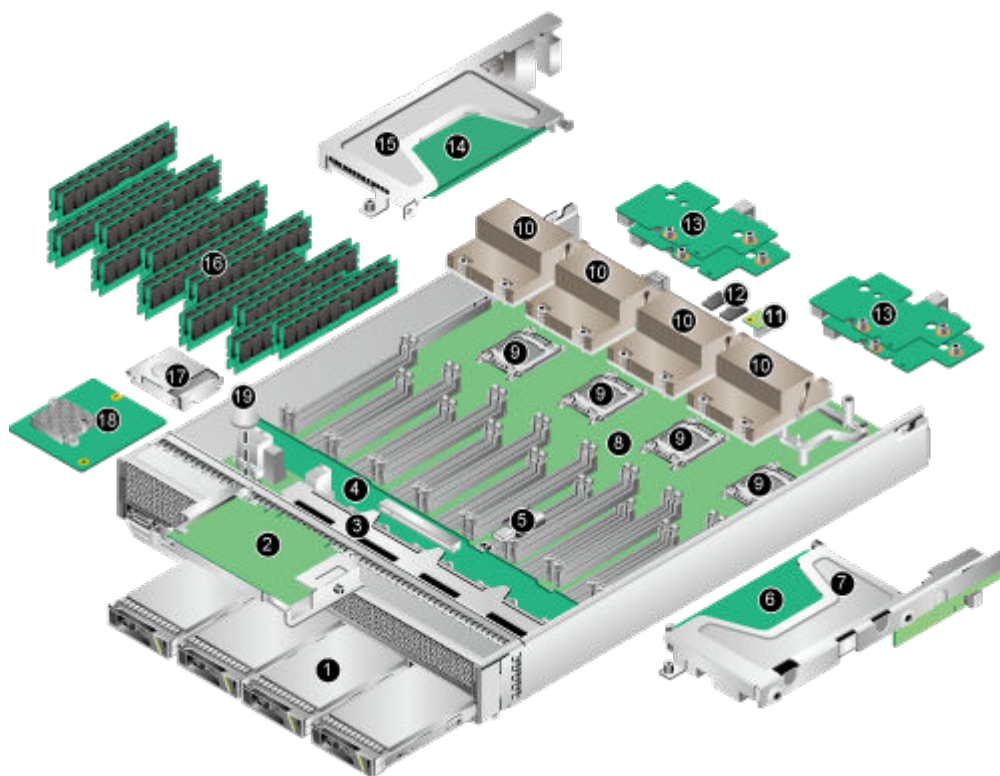
1	Signal connector, connecting to the mainboard	2	Power connector, connecting to the mainboard
3	SAS connector, supporting SAS and SATA	4	SAS connector, supporting SAS, SATA, and PCIe
5	USB port at the back of the drive backplane	6	Drive indicator

2.7 Physical Structure (4HDD)

This section describes the components of the CH242 V3 4HDD and the layout of the mainboard and drive backplane.

Components

Figure 2-13 shows the components of the CH242 V3 4HDD.

Figure 2-13 Components

1	Drives	2	PCIe Card
3	Drive cage	4	Drive backplane
5	(Optional) USB 2.0	6	(Optional) PCIe card 1
7	(Optional) PCIe card tray 1	8	Mainboard
9	CPU	10	Heat sink
11	(Optional) TPM	12	(Optional) MicroSD card
13	Mezzanine card	14	(Optional) PCIe card 2
15	(Optional) PCIe card tray 2	16	DIMM
17	(Optional) iBBU	18	Screw-in RAID controller card
19	BIOS battery	-	-

Table 2-5 describes the components of the CH242 V3 4HDD.

Table 2-5 Component description

No.	Component	Description
1	Drives	The CH221 V5 supports four 2.5-inch HDDs or SSDs and allows mixed configuration of HDDs and SSDs. Each drive can be independently installed, removed, and hot-swapped.
2	PCIe Card	The hard disk backplane provides one PCIe x16 slot for installing a standard full-height half-length PCIe card.
3	Drive cage	The drive cage holds drives.
4	Drive backplane	The drive backplane helps expand storage capacity and control drives in real time.
5	(Optional) USB 2.0	The USB port on the mainboard connects to a USB 2.0 device. The size of the device cannot exceed 40.00 mm x 15.00 mm x 13.00 mm.
6	(Optional) PCIe card 1	PCIe card 1 is on the left of the mainboard and can be a customized PCIe card or a standard PCIe SSD. If a standard PCIe card of full-height, half-length is installed, no DIMMs can be inserted into the 10 DIMM slots below the PCIe card due to space limitations. NOTE - You can configure either PCIe card tray 1 and PCIe card 1 or PCIe card tray 2 and PCIe card 2. - When PCIe card 1 is a standard PCIe SSD, you need to remove the below 10 DIMMs and configure air ducts in the middle and right. The CH242 V3 supports a maximum operating temperature of 35°C.
7	(Optional) PCIe card tray 1	The PCIe card tray is placed above the DIMMs. Each PCIe card tray provides one PCIe x16 slot by using a riser card.
8	Mainboard	The mainboard holds the CPUs, DIMMs, drive interface modules, power control module, iMana 200, logic module, chipset, and video adapter. The compute node chipset uses the Intel® C602J chip. The video card is integrated in the FPGA chip of iMana 200 and provides 16 MB display memory. The maximum resolution is 1280 x 1024 at 60 Hz with 16 M colors.

No.	Component	Description
9	CPU	The mainboard supports two or four processors: • The following CPU models are supported: – Intel® Xeon® E7-4800 v2 (Ivy Bridge-EX) processors of 105 W, 130 W, and 155 W, with a maximum of 15 cores per processor. – Intel® Xeon® E7-8800 v2 (Ivy Bridge-EX) processors of 105 W, 130 W, and 155 W, with a maximum of 15 cores per processor. • Each processor integrates a memory controller for supporting eight memory channels. Each channel supports one DDR3 DIMMs of 1333 MHz or 1600 MHz. • Each processor integrates a PCIe controller supporting PCIe 3.0. Two processors provide 32 lanes. • Every two CPUs are interconnected through one QuickPath Interconnect (QPI) link, delivering up to 8.0 GT/s. • Maximum clock speed: 2.8 GHz.
10	Heat sink	The heat sink is used to cool processors. Each processor is configured with one heat sink.
11	(Optional) TPM	The TPM is a cost-effective security solution that complies with the Trusted Computing Group (TCG) standards. It enhances platform security by preventing viruses or unauthorized operations.
12	(Optional) MicroSD card	The mainboard provides two microSD card slots. Each slot supports a microSD card with a maximum capacity of 32 GB, and the microSD card can be used as the boot medium for a compute node. If two microSD cards are installed, they are configured as RAID 1.

No.	Component	Description
13	Mezzanine card	The CH242 V3 provides four mezzanine card connectors to connect to switch modules or pass-through modules through the backplane. • Mezz1 and Mezz3 are upper-layer daughter cards, and Mezz2 and Mezz4 are lower-layer daughter cards. • Socket CPU 2 provides PCIe x16 bandwidth for connecting to Mezz1 and Mezz2 respectively, socket CPU 3 provides PCIe x16 bandwidth for connecting to Mezz3, and socket CPU 4 provides PCIe x16 bandwidth for connecting to Mezz4. • Mezz1 and Mezz3 connect to slots 2X and 3X at the rear of the E9000 chassis. • Mezz2 and Mezz4 connect to slots 1E and 4E at the rear of the E9000 chassis.
14	(Optional) PCIe card 2	PCIe card 2 is on the right of the mainboard and can be a customized PCIe card or a standard GPU. If a standard PCIe card of full-height, half-length is installed, no DIMMs can be inserted into the 10 DIMM slots below the PCIe card due to space limitations. NOTE • You can configure either PCIe card tray 1 and PCIe card 1 or PCIe card tray 2 and PCIe card 2. • When PCIe card 2 is a standard GPU, you need to remove the below 10 DIMMs and configure air ducts in the middle and right. The CH242 V3 supports a maximum operating temperature of 35°C.
15	(Optional) PCIe card tray 2	The PCIe card tray is placed above the DIMMs. Each PCIe card tray provides one PCIe x16 slot by using a riser card.

No.	Component	Description
16	DIMM	The mainboard provides up to 32 slots for installing DDR3 DIMMs (8 DIMMs for each processor). • Maximum memory speed: 1600 MHz • Memory protection: ECC, memory mirroring, and memory sparing • DIMM types: RDIMMs and LRDIMMs. DIMMs on the same compute node must be of the same type (RDIMM or LRDIMM) and the same specifications (capacity, bit width, rank, and height), and have the same BOM code. To query DIMM BOM numbers, use the Computing Product Compatibility Checker. – RDIMMs: up to 512 GB for 32 x 16 GB RDIMMs and four CPUs – LRDIMMs: up to 2 TB for 32 x 64 GB LRDIMMs and four CPUs
17	(Optional) iBBU	When the LSISAS2208 controller card is installed, you can install an iBBU to protect data from power failures.
18	Screw-in RAID controller card	It provides four SAS or SATA ports for drive expandability. The CH242 V3 4HDD supports LSISAS2208 and LSISAS2308 RAID controller cards. • LSISAS2208: supports RAID 0, 1, 5, 6, 10, 50, and 60. • LSISAS2308: supports RAID 0, 1, 1E, and 10.
19	BIOS battery	When the compute node is not powered on, the BIOS battery supplies power to the real time clock (RTC).

PCIe Slots

[Table 2-6](#) describes the mapping between PCIe slots and CPUs, and the PCIe specifications of the CH242 V3.

NOTE

The PCIe devices mapping to vacant CPU sockets are unavailable.

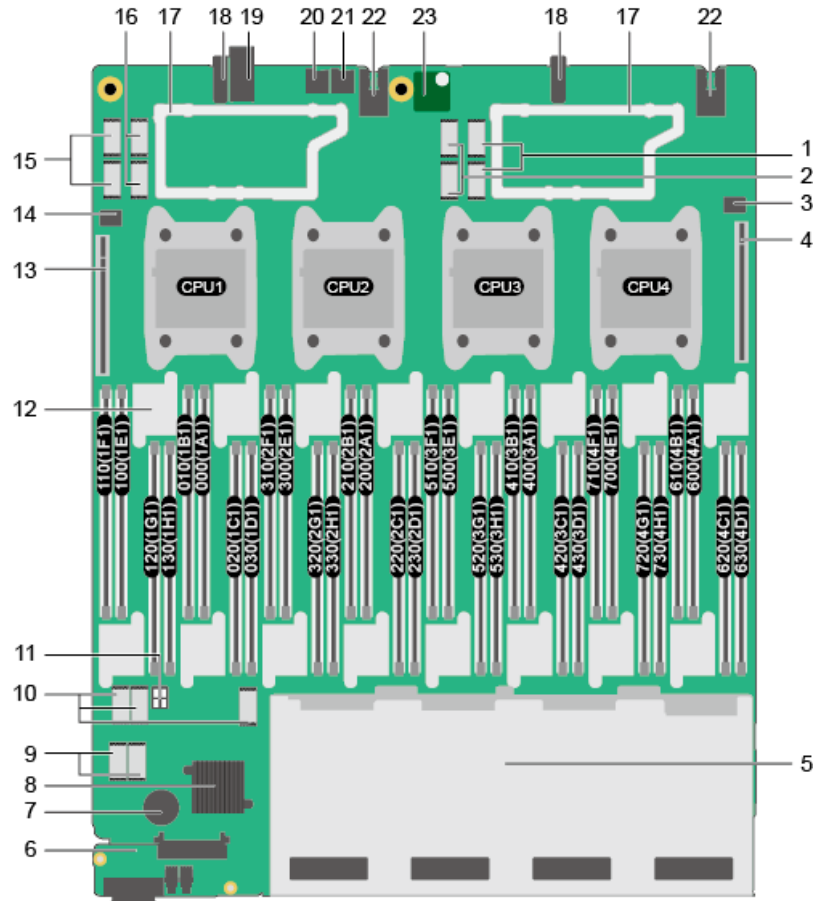
Table 2-6 PCIe slots

PCIe Device	Device Name on the BMC	CPU Connected	PCIe Standard	Connect or Width	Bus Width	Port No.	Slot Size
Screw-in RAID controller card	\	CPU1	PCIe3.0	x8	x8	Port 3C	Non-standard device
Mezz1	\	CPU2	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 3A or (Port 3A+Port 3C)	Non-standard device
Mezz2	\	CPU2	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 2A or (Port 2A+Port 2C)	Non-standard device
Mezz3	\	CPU3	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 2A or (Port 2A+Port 2C)	Non-standard device
Mezz4	\	CPU4	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 3A or (Port 3A+Port 3C)	Non-standard device
PCIe Riser1	PCIe Riser Card1	CPU3	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 3A or (Port 3A+Port 3C)	Full-height half-length (FHHL)
PCIe Riser2	PCIe Riser Card2	CPU4	PCIe3.0	x16 or x8x8	x16 or x8x8	Port 2A or (Port 2A+Port 2C)	Full-height half-length (FHHL)
PCIe SSD0	Disk0	CPU1	PCIe3.0	x4	x4	Port 2D	2.5-inch drive
PCIe SSD1	Disk1	CPU1	PCIe3.0	x4	x4	Port 2C	2.5-inch drive
PCIe SSD2	Disk2	CPU1	PCIe3.0	x4	x4	Port 3C	2.5-inch drive
PCIe SSD3	Disk3	CPU1	PCIe3.0	x4	x4	Port 3D	2.5-inch drive

Mainboard Layout

Figure 2-14 shows the positions of connectors and other components on the mainboard of the CH242 V3 4HDD.

Figure 2-14 Positions of the connectors and components



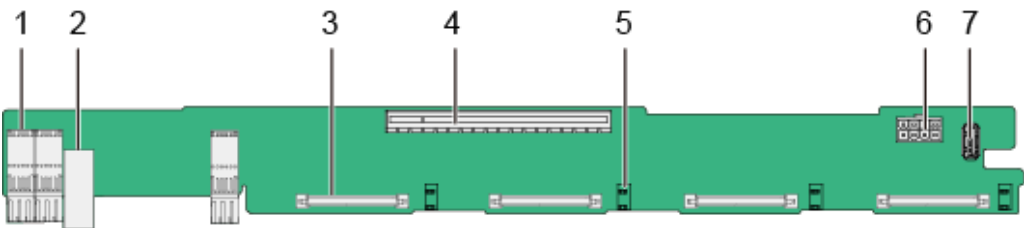
1	Mezzanine card connector 4	2	Mezzanine card connector 3
3	Riser card power connector 2	4	Riser card connector 2
5	Drive cage	6	User interface board
7	BIOS battery	8	PCH (Platform Controller Hub)
9	RAID controller card connectors	10	Drive backplane connector
11	HDD backplane power connector	12	Jordan Creek
13	Riser card connector 1	14	Riser card power connector 1
15	Mezzanine card connector 1	16	Mezzanine card connector 2

17	Mezzanine card tray	18	Positioning pin
19	Midplane signal connector	20	microSD card connector 2
21	microSD card connector 1	22	Midplane power connector
23	TPM connector	-	-

Drive Backboard Layout

Figure 2-15 shows the positions of connectors and other components on the CH242 V3 4HDD drive backplane.

Figure 2-15 Drive backplane



1	Signal connector, connecting to the mainboard	2	Power connector, connecting to the mainboard
3	SAS connector, supporting SAS and SATA	4	PCIe 3.0 x16 connector
5	Drive indicator	6	Auxiliary PCIe card power connector
7	USB port	-	-

2.8 Logical Structure

This topic describes the logical structure of the CH242 V3 CPUs, dual in-line memory modules (DIMMs), and platform controller hub (PCH) and ports on the CH242 V3.

- CPU: The CH242 V3 supports a maximum of four Intel® Ivy bridge-EX CPUs.
 - Each CPU has two memory controllers. Each memory controller supports two Intel® Serial Management Interfaces (SMIs). Each SMI supports one Jordan Creek , and each Jordan Creek supports two memory channels.
 - A CPU integrates three QuickPath Interconnect (QPI) 1.1 interfaces. CPUs are interconnected over the QPI bus with a transmission rate of 8.0 GT/s.
 - The CPUs are interconnected with the PCH over the DMI2 bus with a transmission rate of 5 GT/s.
- DIMM: The CH242 V3 can be configured with a maximum of 32 DIMMs. Each DIMM provides a maximum capacity of 32 GB.

- As the PCH, the Patsburg-J chip is an Intel southbridge for server platforms to provide external I/O ports and bus expandability. The PCH connects to the integrated management module (iMana 200) to provide management and service ports.
- I/O ports: The CH242 V3 connects to switch modules and pass through modules by using four mezz modules.
- Hard disk interface module:
 - CH242 V3 8HDD: Hard disk interface module: The hard disk interface module consists of the hard disk backplane and a RAID controller card. The hard disk backplane for eight hard disks provides eight Serial Attached SCSI (SAS) or Serial Advanced Technology Attachment (SATA) ports.
 - CH242 V3 4HDD: Hard disk interface module: The hard disk interface module consists of the hard disk backplane and a RAID controller card. The hard disk backplane for four hard disks provides four SAS or SATA ports and one PCIe x16 port.
- The iMana 200 provides device management functions, such as compute node power control, slot ID obtaining, power detection, and KVM over IP.

Figure 2-16 shows the CH242 V3 8HDD logical structure.

Figure 2-16 Logical CH242 V3 8HDD structure

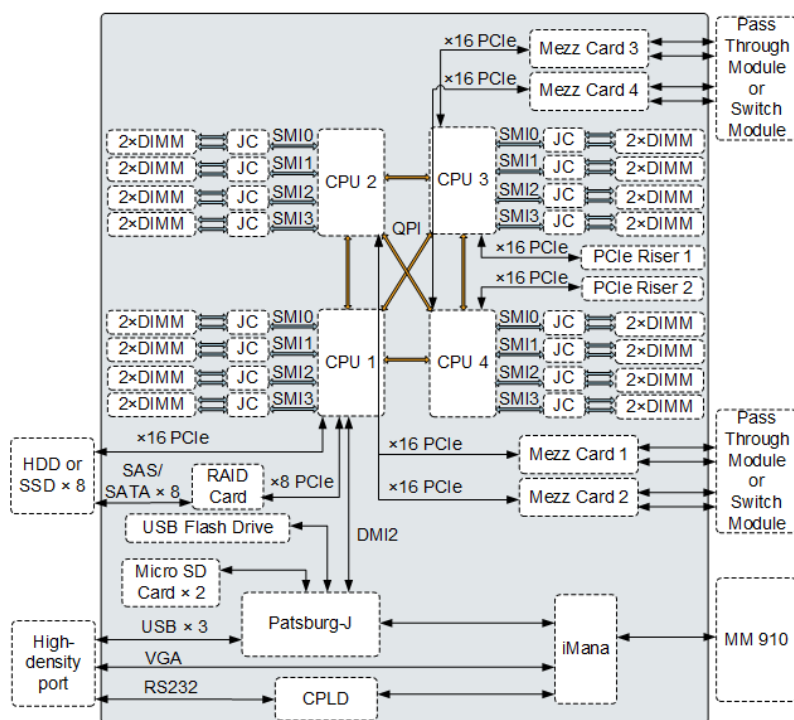
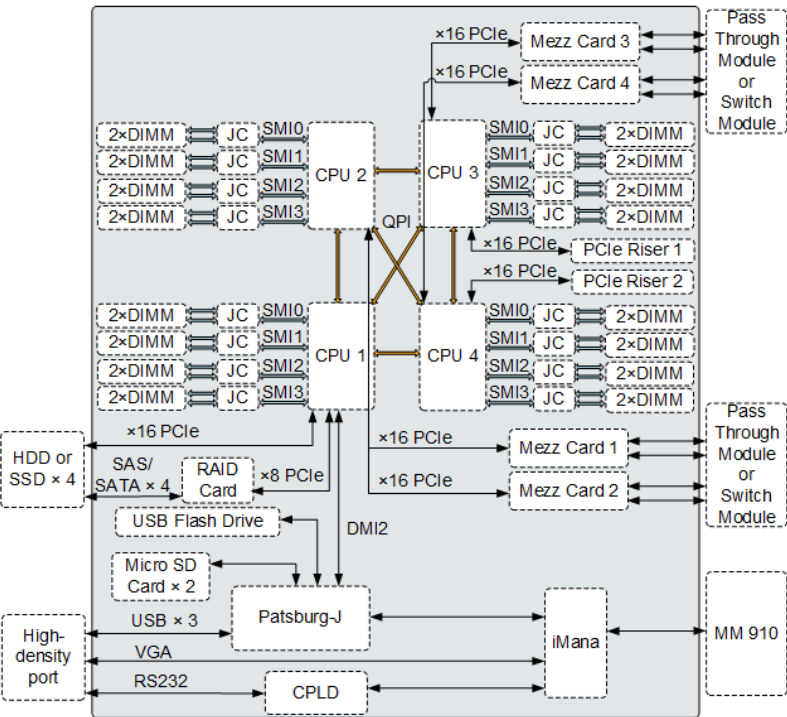


Figure 2-17 shows the CH242 V3 4HDD logical structure.

Figure 2-17 Logical CH242 V3 4HDD structure



2.9 Software and Hardware Compatibility

This section describes the software and hardware supported by the CH242 V3.

Use the [Computing Product Compatibility Checker](#) to check the software and hardware supported by the CH242 V3.

2.10 Technical Specifications

This topic describes specifications of the CH242 V3.

[Table 2-7](#) describes the technical specifications of the CH242 V3.

Table 2-7 Technical Specifications

Category	Item	Specifications
Physical specifications	Dimensions (H x W x D)	60.46 mm x 423 mm x 537.2 mm (2.4 in. x 16.65 in. x 21.14 in.)
	Color	- Front panel: black - Cover: silver white
	Weight	Net: 16 kg to 17 kg (35.27 lb to 37.48 lb) Packing materials: 3.6 kg (7.94 lb)

Category	Item	Specifications
Environmental specifications	Temperature	- Operating temperature: 5°C to 40°C (41°F to 104°F) (ASHRAE Classes A2 and A3 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 standard GPU is installed in PCIe card 2 on the right of the mainboard or a standard NVMe PCIe SSD is installed in PCIe card 1 on the left of the mainboard, the CH242 V3 supports a maximum operating temperature of 35°C.
	Relative humidity (RH, non-condensing)	- Operating humidity: 5% to 85% - 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
	Altitude	At an altitude of 900 m (2952.72 ft), the highest operating temperature is 40°C (104°F). When the device is used at an altitude of 900 m to 5000 m (2952.8 ft to 16404.2 ft), the highest operating temperature decreases by 1°C (1.8°F) for every increase of 300 m (984.24 ft). HDDs are not supported at an altitude of over 3000 m (9842.5 ft).
	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

Category	Item	Specifications
	Particle contaminant	• The equipment room environment meets the requirements of ISO 14664-1 Class 8. • There is no explosive, conductive, magnetic, or corrosive dust in the equipment room. NOTE It is recommended that the particulate pollution in the equipment room be monitored by a professional agency.
Input power supply	Rated input voltage	12 V DC
Power consumption	Maximum power consumption	• CH242 V3 8HDD: 1259 W • CH242 V3 4HDD: 1265 W

3 Installing and Removing the CH242 V3

This topic describes the precautions and procedures for installing and removing the CH242 V3.

[3.1 Installing a CH242 V3](#)

[3.2 Removing a CH242 V3](#)

3.1 Installing a CH242 V3

This topic describes the precautions and procedures for installing the CH242 V3 in the E9000 chassis.

Scenarios

Install the CH242 V3 in the HUAWEI E9000chassis. Before the operation, you must get familiar with the hardware devices. The procedure for installing the CH242 V3 8HDD is the same that for installing the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

The chassis has been installed.

Data

Data preparation is not required for this operation.

Tools

The following tools are available:

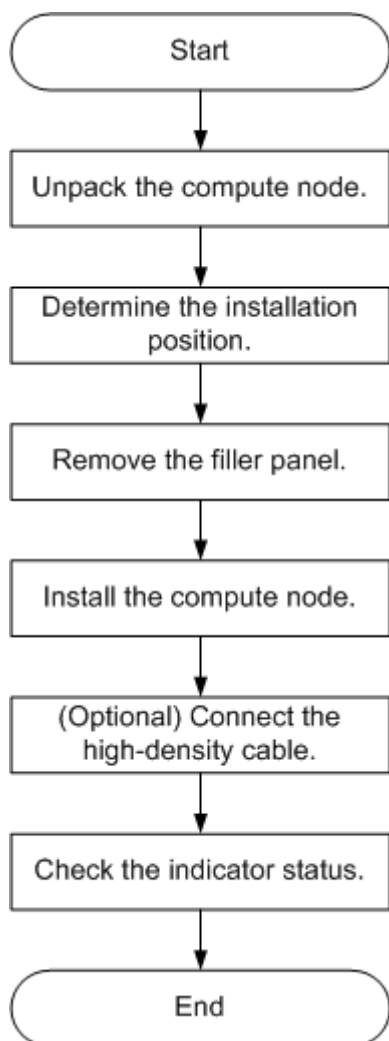
- Protective gloves.
- Electrostatic discharge (ESD) gloves.

- ESD wrist strap.
- Paper knife.

Workflow

Figure 3-1 shows the procedure for installing the CH242 V3.

Figure 3-1 Installation procedure



Procedure

Step 1 Unpack the compute node.

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

NOTE

If the packing case is damaged (for example, the packing case is soaked or deformed, or the seals or pressure sensitive adhesive tape is unsealed), fill in the *Cargo Problems Feedback Form*.

2.

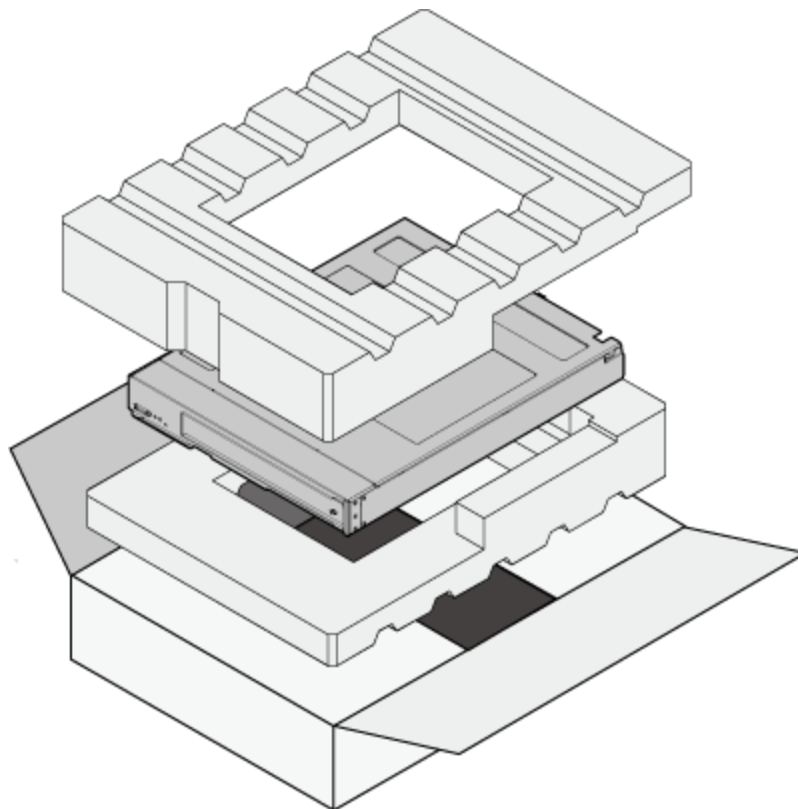
CAUTION

When using a paper knife to unpack a packing case, ensure that the knife edge is of a proper protrusion to avoid hurting hands or damaging the device in the packing case.

Use a paper knife to cut the pressure sensitive adhesive tape of the packing case.

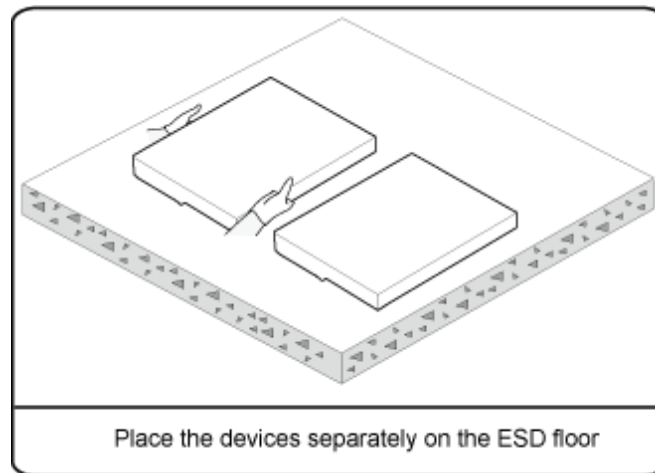
3. Unpack the compute node, as shown in [Figure 3-2](#).

Figure 3-2 Unpacking the compute node



4. Take out the compute nodes together with ESD bags and place them separately on the ESD floor, as shown in [Figure 3-3](#).

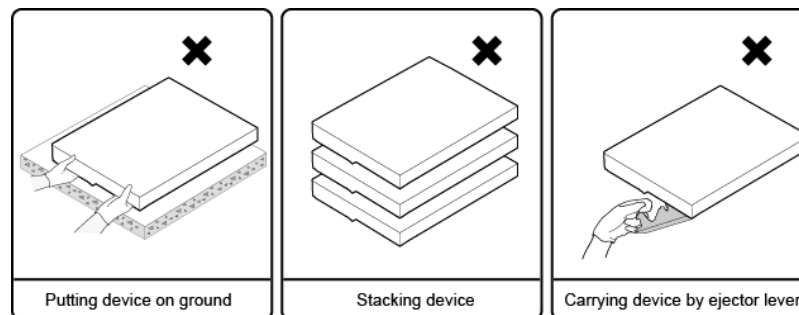
Figure 3-3 Proper operations



NOTE

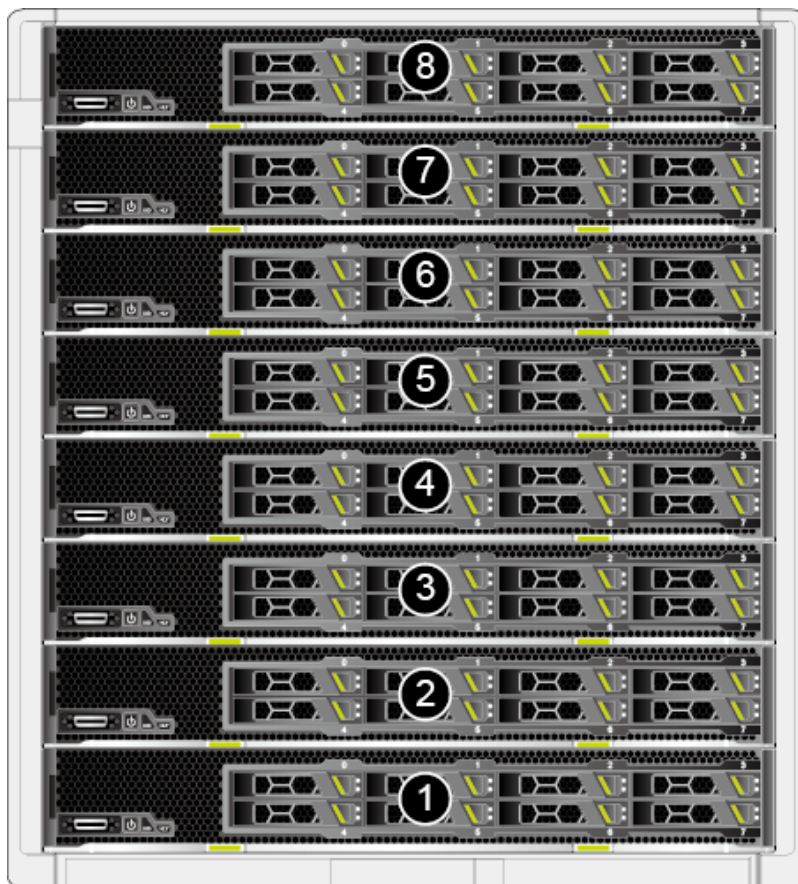
Do not take the compute node out of its ESD bag if you do not install it immediately.

Figure 3-4 Improper operations



Step 2 Determine the slots for installing the compute node in the chassis. For details about the slot numbers for the compute nodes, see [Figure 3-5](#).

Figure 3-5 Slot numbers



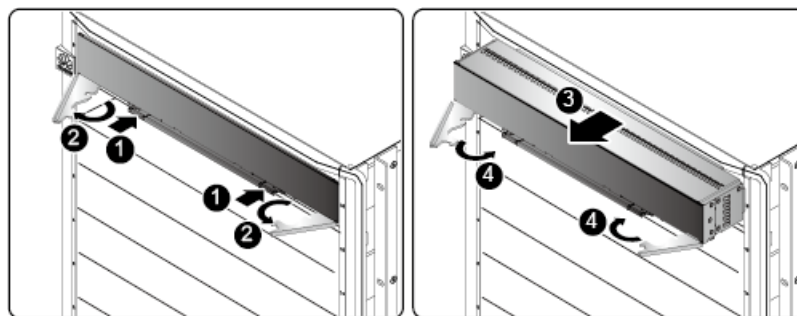
NOTE

- A maximum of eight full-width compute nodes can be installed in an E9000 chassis.
- You are advised to install compute nodes from bottoms up by following the slot numbers in ascending order.

Step 3 Remove the filler panel.

1. Press the springs on the filler panel. See step (1) in [Figure 3-6](#).

Figure 3-6 Removing the filler panel



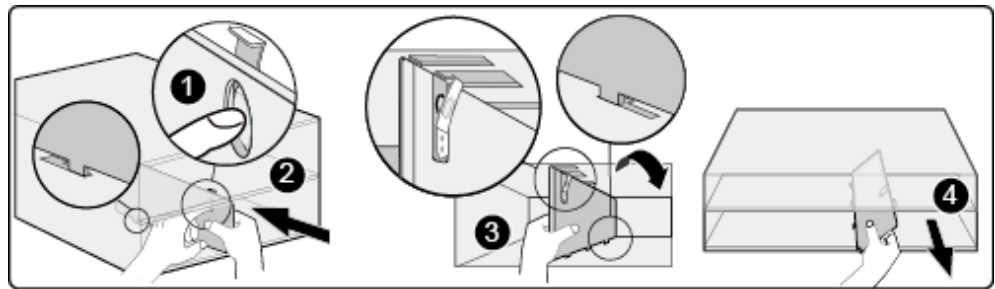
2. Raise the ejector levers on the filler panel completely. See step (2) in [Figure 3-6](#).
3. Pull the filler panel out of the chassis. See step (3) in [Figure 3-6](#).

4. Lower the ejector levers on the filler panel. See step (4) in [Figure 3-6](#).
5. Store the removed filler panel properly for future use.

Step 4 Install the CH242 V3.

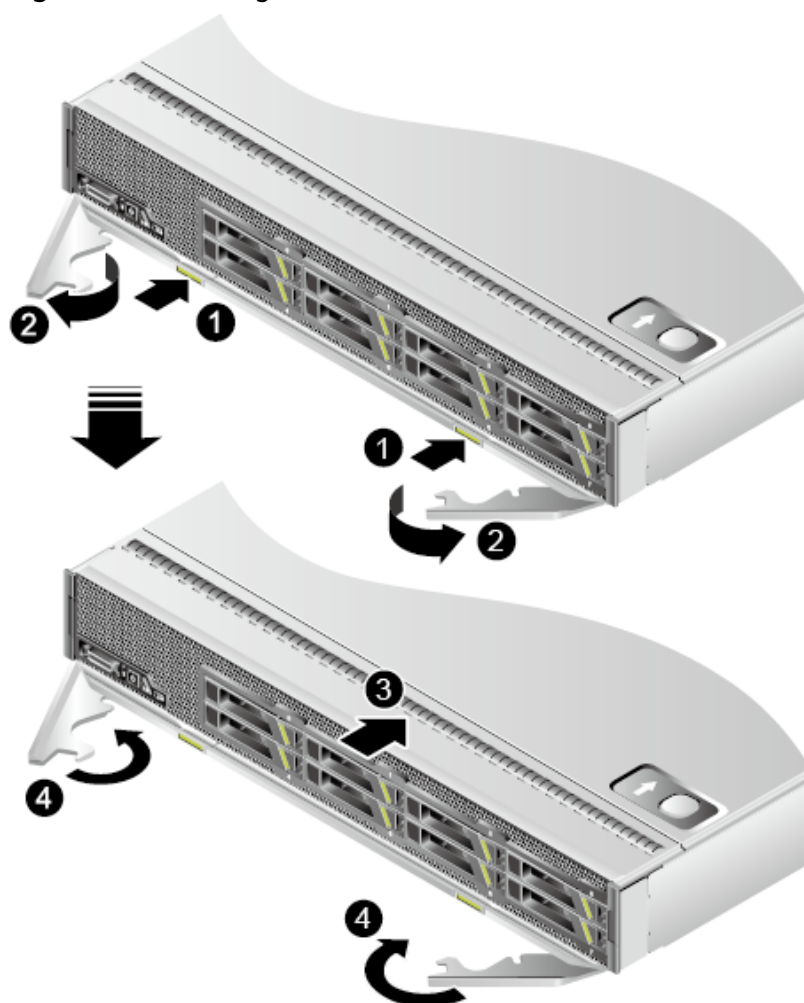
1. (Optional) Remove the partition board, as shown in [Figure 3-7](#).
The partition board must be removed before you install a full-width compute node.
 - a. Press and hold down the hole and push the partition board inwards. See steps (1) and (2) in [Figure 3-7](#).
 - b. Move the partition board rightwards and remove the partition board. See steps (3) and (4) in [Figure 3-7](#).

Figure 3-7 Removing the partition board



2. Press the springs on the CH242 V3. See step (1) in [Figure 3-8](#).

Figure 3-8 Installing the CH242 V3

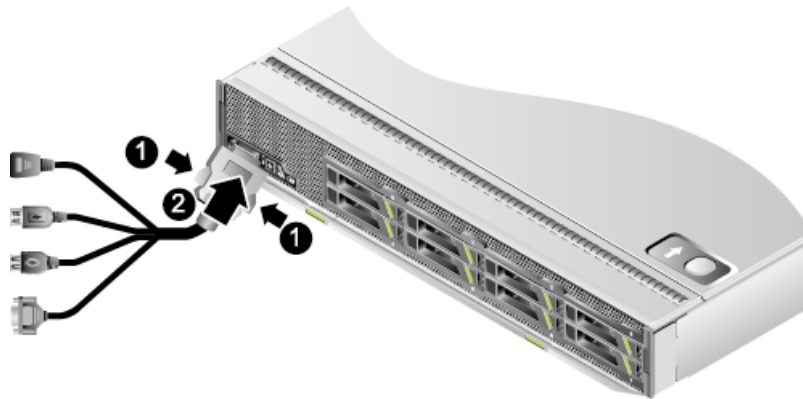


3. Raise the ejector levers on the CH242 V3 completely. See step (2) in [Figure 3-8](#).
4. Insert the CH242 V3 horizontally into the chassis. See step (3) in [Figure 3-8](#).
5. Lower the two ejector levers on the CH242 V3. See step (4) in [Figure 3-8](#).

Step 5 (Optional) Connect the high-density cable.

1. Press the two tabs on the high-density cable connector. See step (1) in [Figure 3-9](#).

Figure 3-9 Connecting the high-density cable



2. Insert the cable horizontally into the high-density port on the CH242 V3. See step (2) in [Figure 3-9](#).
Check the indicator status.
3. Check the status of the indicators on the CH242 V3 after the CH242 V3 is powered on.
For details about the indicators, see [Table 2-1](#).

----End

3.2 Removing a CH242 V3

This topic describes the precautions and procedures for removing the CH242 V3 from the E9000 chassis.

Scenarios

Remove the CH242 V3 from the HUAWEI E9000 chassis. Before the operation, you must get familiar with the hardware devices. The procedure for removing the CH242 V3 8HDD is the same that for removing the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example.

Impact on the System

After the CH242 V3 is removed, all services running on the CH242 V3 stop.

Prerequisites

Conditions

There are no special conditions for this operation.

Data

Data preparation is not required for this operation.

Tools

The following tools are available:

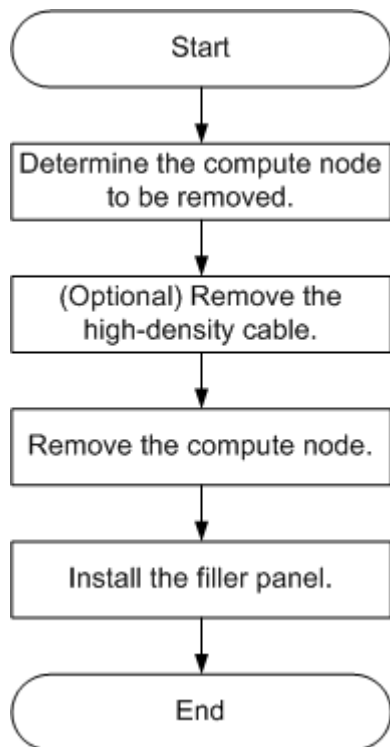
- Protective gloves.

- Electrostatic discharge (ESD) gloves or wrist strap.
- ESD bag.

Workflow

Figure 3-10 shows the procedure for removing the CH242 V3.

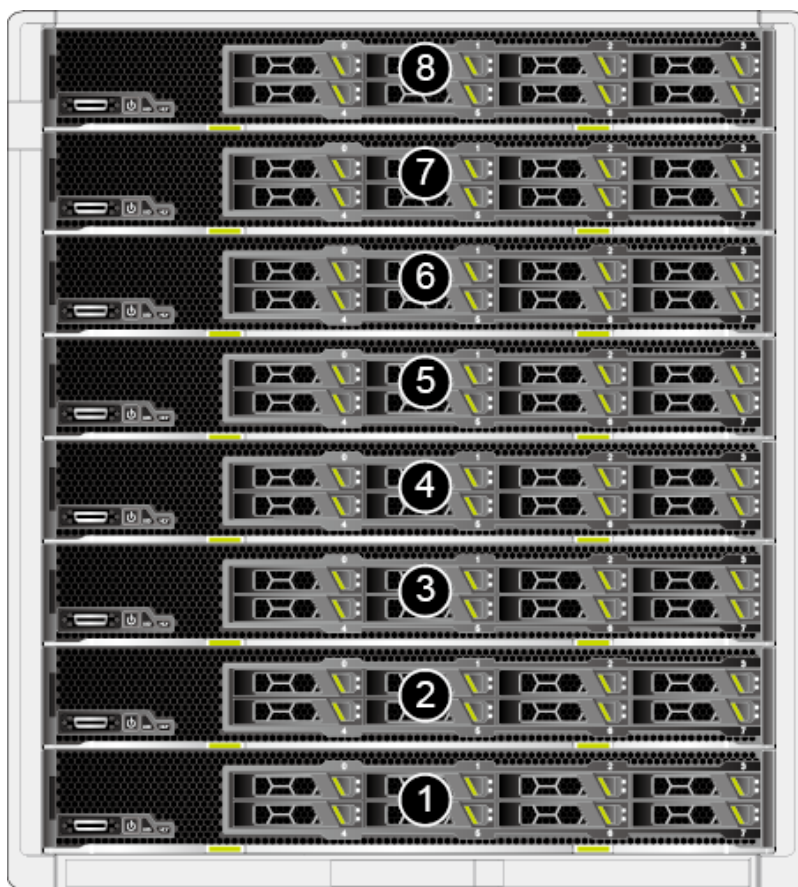
Figure 3-10 Procedure for removing the compute node



Procedure

- Step 1** Determine the CH242 V3 to be removed. For details about the slot numbers for the compute nodes, see **Figure 3-11**.

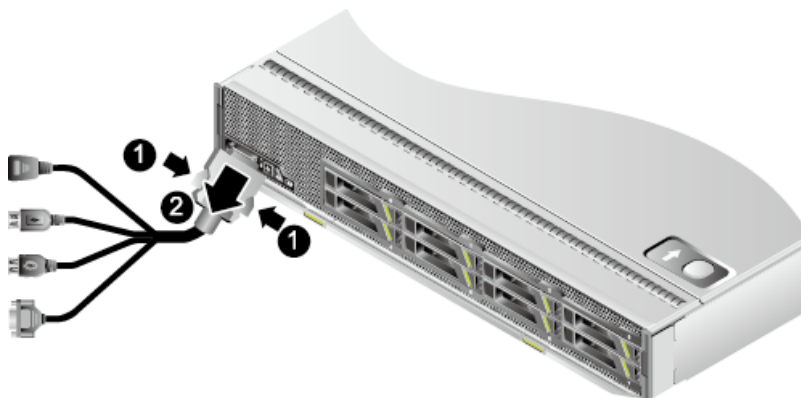
Figure 3-11 Slot numbers



Step 2 (Optional) Remove the high-density cable.

1. Press the two tabs on the high-density cable connector. See step (1) in [Figure 3-12](#).

Figure 3-12 Removing the high-density cable

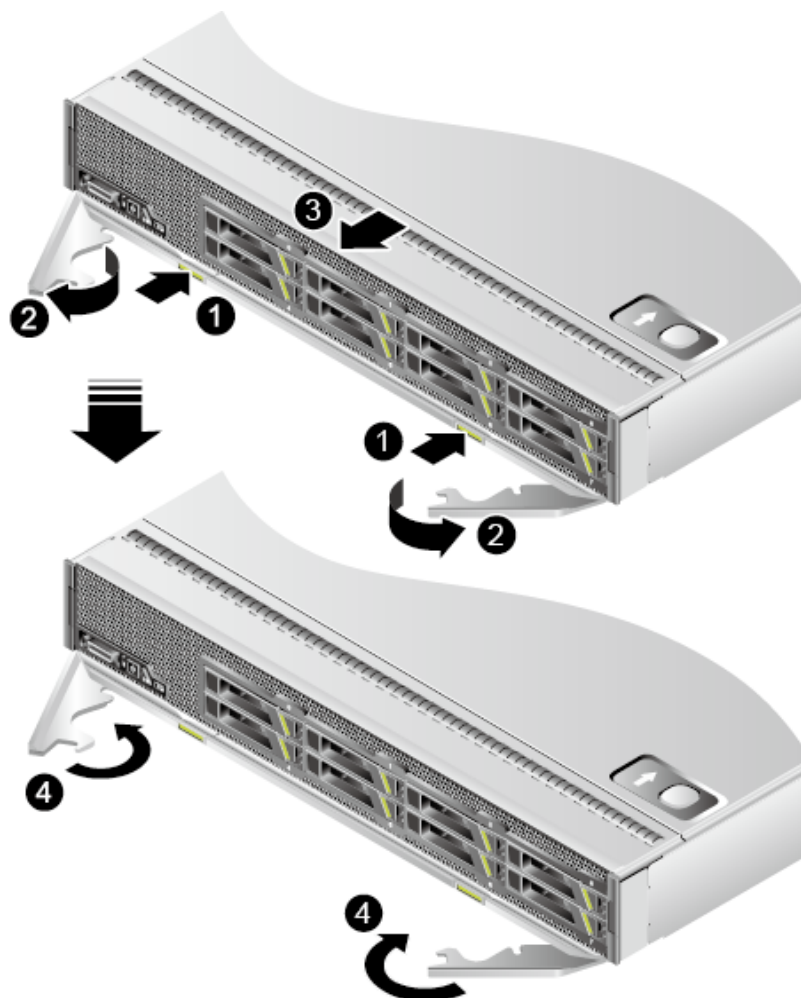


2. Remove the high-density cable from the high-density port on the CH242 V3. See step (2) in [Figure 3-12](#).

Step 3 Remove the CH242 V3.

1. Press the springs on the CH242 V3. See step (1) in [Figure 3-13](#).

Figure 3-13 Removing the CH242 V3



2. Raise the ejector levers on the CH242 V3 completely. See step (2) in [Figure 3-13](#).
3. Pull out the CH242 V3 horizontally from the chassis. See step (3) in [Figure 3-13](#).
4. Lower the two ejector levers on the CH242 V3. See step (4) in [Figure 3-13](#).

NOTICE

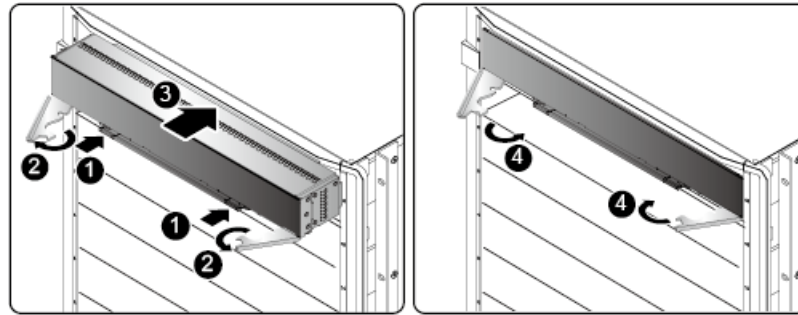
5. An ESD bag can hold only one CH242 V3.

Place the removed CH242 V3 in an ESD bag.

Step 4 Install a filler panel.

1. Press the springs on the filler panel. See step (1) in [Figure 3-14](#).

Figure 3-14 Installing a filler panel



2. Raise the ejector levers on the filler panel completely. See step (2) in [Figure 3-14](#).
3. Insert the filler panel into the chassis slot horizontally. See step (3) in [Figure 3-14](#).
4. Lower the ejector levers on the filler panel. See step (4) in [Figure 3-14](#).

 NOTE

Install a filler panel in a vacant slot. Otherwise, the ventilation, heat dissipation, electromagnetic shielding, and dust resistance effect of the chassis will be affected.

----End

4 Configuring the CH242 V3

This topic describes how to configure the CH242 V3 after it is installed. You need to configure the redundant array of independent disks (RAID), basic input/output system (BIOS), and integrated management module (iMana 200) IP address, and install the operating system (OS) on the CH242 V3.

[4.1 Overview](#)

[4.2 Default Information](#)

[4.3 Checking the CH242 V3](#)

[4.4 Changing the Default iMana 200 User Password](#)

[4.5 Configuring the iMana 200 IP Address](#)

[4.6 Changing the iMana 200 U-boot Password](#)

[4.7 Logging In to the Real-Time Desktop](#)

[4.8 Configuring the RAID](#)

[4.9 Configuring the BIOS](#)

[4.10 Installing the OS](#)

4.1 Overview

This topic describes how to configure the CH242 V3.

Configuration Process

Figure 4-1 shows the process for configuring the CH242 V3.

Figure 4-1 Initial configuration process for the CH242 V3

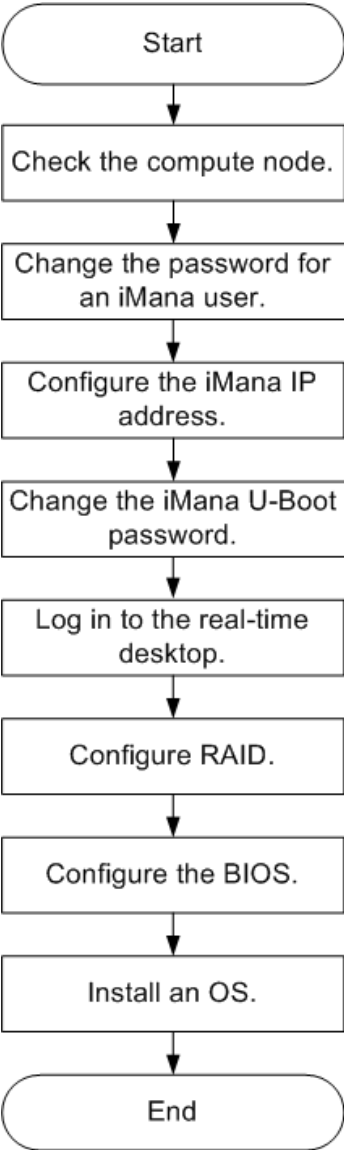


Table 4-1 describes the process for configuring the CH242 V3.

Table 4-1 Process for configuring

Procedure	Description
Check the compute node.	- Check the version information about the compute node and ensure that the version meets the site requirements. - Check for alarms about the compute node.
Change the Password for a integrated management module (iMana 200) User.	Change the default password for the administrator root .

Procedure	Description
Configure the iMana 200 IP address.	-
Change the U-boot Password.	-
Log In to the Real-Time Desktop.	Log in to the CH242 V3 through the web user interface (WebUI) of the MM910.
Configure the redundant array of independent disks (RAID).	The CH242 V3 supports the LSISAS2208 and LSISAS2308 RAID controller cards. Select one of the following RAID properties as required: CH242 V3 8HDD: • LSISAS2208: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and RAID 60 • LSISAS2308: RAID 0, RAID 1, RAID 10 and RAID 1E CH242 V3 4HDD: • LSISAS2208: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and RAID 60 • LSISAS2308: RAID 0, RAID 1, RAID 10 and RAID 1E
Set the basic input/output system (BIOS).	Configure the compute node BIOS, including the boot mode, network drive, preboot execution environment (PXE) options of the network interface card (NIC), and BIOS password.
Install the operating system (OS).	Install the OS for the CH242 V3.

Related Manuals

Manuals for configuring and maintaining the CH242 V3 are as follows:

- To configure iMana 200, see [E9000 Server V100R001 iMana 200 User Guide](#).
- To configure RAID, see [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
- To configure the BIOS, see [Huawei Server Brickland Platform BIOS Parameter Reference](#).
- To install an operating system, see [Huawei Server OS Installation Guide](#).
- To handle alarms, see [FusionServer Pro E9000 Server V100R001 HMM Alarm Handling](#).
- To troubleshoot problems, see [Huawei Servers Troubleshooting](#).

4.2 Default Information

This topic describes the default information used for configuring the compute nodes.

Table 4-2 provides the default information of compute nodes.

Table 4-2 Default information

User Name	User Description	Default Password	User Type	User Status	Login Method
root	A BMC user	Huawei12#\$	Administrator	Enabled	Remote and local login
–	A user who logs in to U-Boot over a serial port. No user name is used. This applies to all compute nodes.	Huawei12#\$	Administrator	Enabled	Local login

User Name	User Description	Default Password	User Type	User Status	Login Method
–	A user who logs in to the basic input/output (BIOS) Setup menu over a serial port or KVM. No user name is used. This applies to all compute nodes.	Huawei12#\$ NOTE • During system boot, you can press F5 to select a keyboard type (French or American keyboard). • The default BIOS password is Huawei 12#\$ for the French or American keyboard and is Huawei 12£\$ for the English keyboard.	Administrator	Enabled	Remote and local login
ftp	An FTP user who transmits files over FTP.	–	System account	Locked	Login prohibited

User Name	User Description	Default Password	User Type	User Status	Login Method
sshd	A user of the Secure Shell daemon (sshd). The SSH protocol allows a user to remotely log in to the host execution program, implementing secure management for the host.	Huawei12#\$	Administrator	Enabled	Remote and local login
nobody	An anonymous user. The nobody account requires no special rights to allocate software processes.	–	System account	Locked	Login prohibited
telnetd	A user for the Telnet service. You must enable the user.	–	System account	Locked	Login prohibited

 NOTE

The iBMC or iMana 200 does not have a default IP address.

4.3 Checking the CH242 V3

Log in to the MM910 command line interface (CLI) to check the health status of the CH242 V3.

Scenarios

Log in to the MM910 CLI to check the health status of the CH242 V3. Ensure that it meets the environmental requirements for software installation.

Prerequisites

Conditions

The CH242 V3 has been powered on.

Data

The following data is available:

- User name for logging in to the MM910 to be connected.
- Password for logging in to the MM910 to be connected.

Procedure

Step 1 Log in to the MM910 CLI.

1. (Optional) Check the MM910 management network port out mode.

You can log in to the MM910 WebUI through a serial port and run the **outportmode** command to query and set the management network port out mode. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).

NOTE

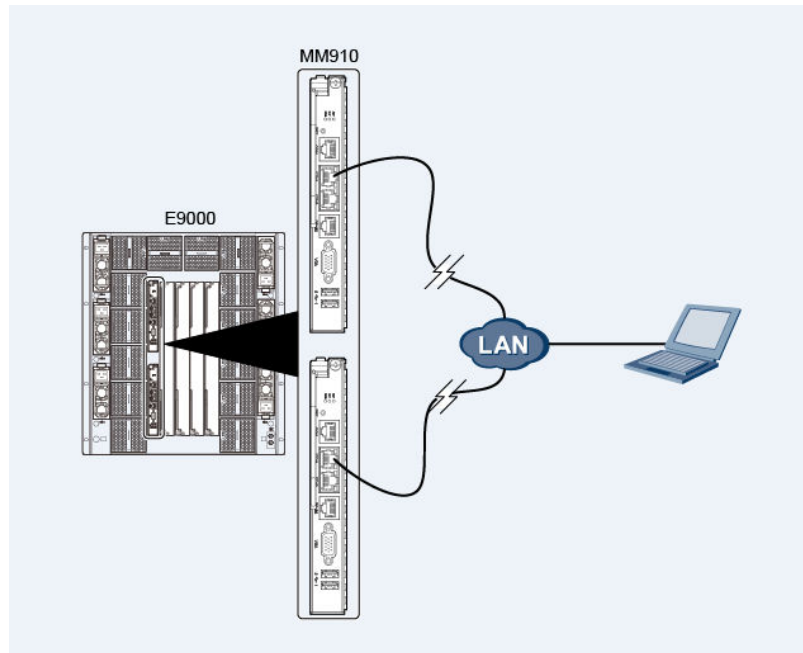
The MM910 management port is provided by two modes.

- An Ethernet port on the switch module in slot 2X or 3X can be used as the MM910 management port. However, if a CX910/CX911/CX912/CX913/CX915 is in slot 2X or 3X, only a GE port can be used; if a CX920 is in slot 2X or 3X, only a 10GE port can be used; if a CX916/CX916L/CX930 is in slot 2X or 3X, only a 25GE port can be used. If a CX110/CX111/CX310/CX311/CX312/CX320/CX710 is in slot 2X or 3X, any port can be used. The CX910/CX911/CX912/CX913 are not recommended for providing the management network port of the management module.
 - The MGMT port on the MM910 panel can be used as the MM910 management port.
 - For MM910 (U54) 2.25 or earlier, the port on the switch module in slot 2X or 3X is used as the management network port by default. In this case, do not connect the MGMT port on the MM910 and the port on the switch module to the same network at the same time, otherwise, a network storm occurs and the network is interrupted. For MM910 (U54) 2.26 or later, the MGMT port is used as the management network port by default. For details about how to query the version, see the [MM910 Management Module V100R001 User Guide](#).
 - You can run the **outportmode** command to change the mode in which the management network port is provided. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).
2. Connect the local PC to the MM910 management network port based on the MM910 management network port out mode.
 - MGMT port on the MM910 panel

- Connect the Ethernet port on the PC to the MGMT port on the active or standby MM910 over a local area network (LAN).

[Figure 4-2](#) shows the network connection.

Figure 4-2 Network connection

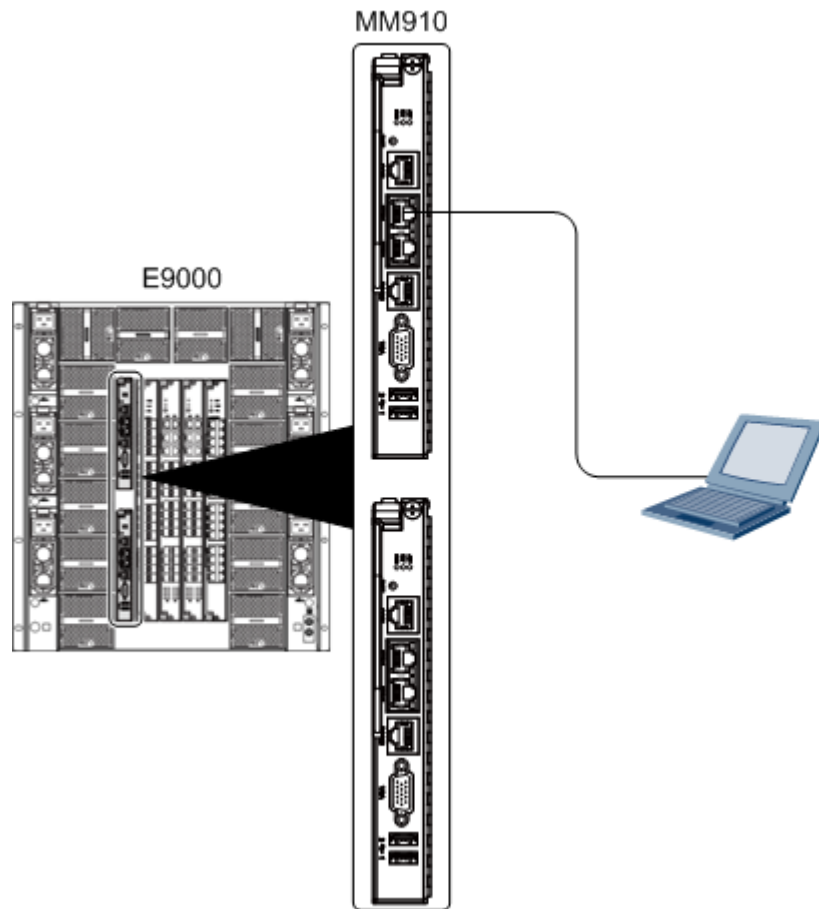


- Connect the Ethernet port on the PC to the MGMT port on the active MM910.

NOTE

If the MGMT port of the active MM910 is available, use this port.

Figure 4-3 Connection between the local PC and the active MM910 (in slot MM2 in this example)

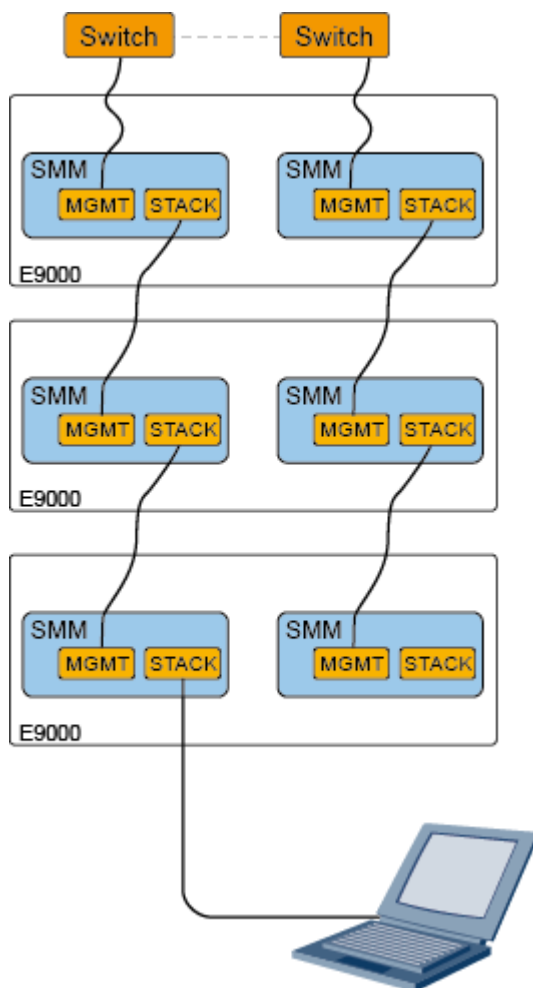


- Connect the Ethernet port on the local PC to the MGMT or STACK port on the active MM910.

NOTE

If the MGMT port on the active MM910 is unavailable, connect the PC to the STACK port on the active MM910. If the STACK port is used to stack the MGMT port in another chassis, connect the PC to an idle STACK port on an active MM910 in a chassis cascaded with the E9000 chassis.

Figure 4-4 Connection between the local PC and an idle STACK port on an MM910 stacked



- An Ethernet port on the switch module

Connect the Ethernet port on the PC to a port on the switch module in slot 2X or 3X over a LAN.

NOTE

- Switch modules can be also installed in slots 1E and 4E of the E9000 chassis, but only the switch modules in slots 2X and 3X provide the management network ports.
 - If the ports on switch modules in slots 2X and 3X are used to access the management plane, isolate the management VLAN from the service VLAN for the switch modules for security purposes.
3. Open an SSH connection tool and enter the floating IP address of the MM910 to visit the MM910 CLI.

In this document, PuTTY is used as an example during login over SSH. For details, see Logging In to the Server Over a Network Port by Using the PuTTY.

Step 2 Check the version and health status of the CH242 V3.

1. Run the following command to query the CH242 V3 version information:
smmget -l blade/V -d version

In the command, *N* indicates the slot number of the CH242 V3 to be queried. For example, to query the version information about the CH242 V3 in slot 2, run the following command:

smmget -l blade2 -d version

The command output similar to the following is displayed if the command is run successfully:

```
blade2 Version Information:
IPMC      CPU:      SPEAr310
IPMI      Version:  2.0
FPGA      Version:  (U23)021
CPLD      Version:  (U108)007
BIOS      Version:  (U6004)V011
Active iMana Version: (U20)3.18
Active iMana Built:   17:41:18 Jul 24 2013
Backup iMana Version: 3.16
Driver    Version:  1.00
Driver    Built:    17:41:26 Jul 24 2013
Uboot     Version:  U-Boot 1.3.5 (Feb 22 2013 - 10:17:12)-SPEAr310
SBCB      BoardID:  0x0252
SBCB      PCB:      .B
RAID CARD BoardID:  0x0021
RAID CARD PCB:      .B
HDD BACKPLANE BoardID: 0x0041
HDD BACKPLANE PCB:    .A
MEZZ CARD3 BoardID:  0x008b
MEZZ CARD3 PCB:      .A
IPMB      Address:  0x82
```

- **CPLD Version:** indicates the CPLD version of the compute node.
 - **BIOS Version:** indicates the BIOS version of the compute node.
 - **Active iMana Version:** indicates the main iMana version of the compute node.
 - **Backup iMana Version:** indicates the standby iMana version of the compute node.
 - **SBCB BoardID:** indicates the version of the compute node.
2. Check whether the CH242 V3 software versions are consistent with the data plan.
 - If yes, go to [Step 2.4](#).
 - If no, go to [Step 2.3](#).
 3. Upgrade the integrated management module (iMana 200), basic input/output system (BIOS), or complex programmable logical device (CPLD). For details, see the [FusionServer Pro Blade Server Upgrade Guide](#).
 4. Run the following command to check whether alarms are generated for the CH242 V3:

smmget -l bladeN -d healthevents

In the command, *N* indicates the slot number of the CH242 V3 to be queried. For example, to query alarms about the CH242 V3 in slot 2, run the following command:

smmget -l blade2 -d healthevents

- No alarm is generated for the CH242 V3 if the following information is displayed:
blade2 has no problem.
- The information similar to the following indicates an alarm:

Wed Oct 17 11:51:02 2012 RTC Battery: Battery low. Assertion [Major]

5. Check whether alarms are generated.
 - If yes, go to [Step 2.6](#).
 - If no, no further action is required.
6. Handle the alarms. For details, see [FusionServer Pro E9000 Server V100R001 HMM Alarm Handling](#).

----End

4.4 Changing the Default iMana 200 User Password

This topic describes how to change the password for an integrated management module (iMana 200) user.

Scenarios

Change the password for an iMana 200 user of the CH242 V3 to improve the security of system operation and maintenance.

NOTE

- Ensure that the password complexity check is enabled. The password complexity check is enabled by default.
- For security purposes, change the initial password upon the first login, and then change the password regularly.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

You have installed the high-density cable to the compute node.

Data

Default iMana 200 user name and password are shown in [Table 4-3](#).

Table 4-3 Default iMana 200 User Name and Password

Default iMana 200 User Name and Password	Description
• User name: root • Password: Huawei12#\$	The default user for the iMana 200 system belongs to the administrator group. The default user can access all resources in the iMana 200 system and perform all available functions.

Tools

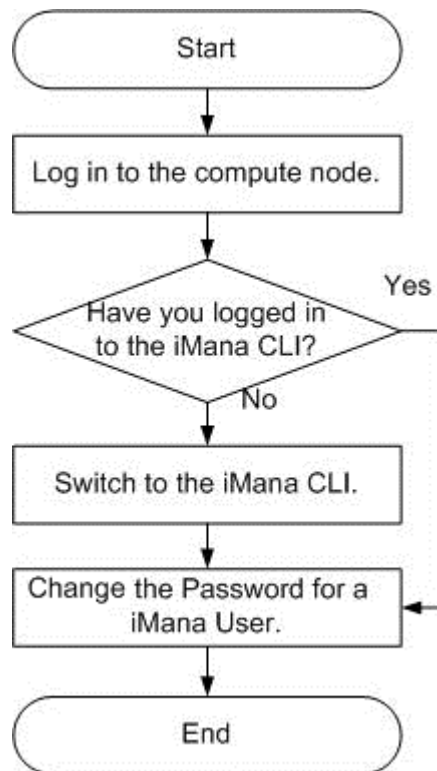
If you want to log in to a server CLI over a serial port, prepare the following:

- PC with an RS232 serial port.
- DB9-RJ45 cable.

Workflow

Figure 4-5 shows the process for Changing the Password for a iMana 200 User.

Figure 4-5 Changing the Password for a iMana 200 User



Procedure

Step 1 Connect the serial port of the high-density port to the serial port of a PC with a serial cable.

NOTE

If you cannot log in to the compute node over a serial port, log in by using the method described in Logging In to a Compute Node or a Switch Module over SOL.

Step 2 Log in to the compute node over a serial port by using the PuTTY. For details, see Logging In to the Server Over a Serial Port by Using the PuTTY.

Key communication parameters:

- Serial Line to connect to: COM n
- Speed (baud): 115200
- Data bits: 8
- Stop bits: 1

- Parity: None
- Flow control: None

n indicates the serial port number, and the value is an integer.

You can log in to the operating system (OS) or iMana 200 after logging in to a compute node.

- You have logged in to the iMana 200 command-line interface (CLI) if the following information is displayed:

```
Wind River Linux release 3.0
Kernel 2.6.27_stm23_003 on armv5tejl (console)
BMC login:
```

- You have logged in to the OS CLI if the following information is displayed:
linux-SMM-Test1:~#

Test1 on the left of the prompt indicates the OS name. The value varies according to the OS name set by users.

Step 3 Determine whether you have logged in to the iMana 200 CLI.

- If yes, go to [Step 8](#).
- If not, go to [Step 4](#).

Step 4 Connect the RS-232 serial port on the PC and the **COM** port on the active MM910 by using a DB9-RJ45 cable.

Step 5 Log in to the MM910 CLI by using a serial port communication tool.

The key communication parameters are as follows:

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

n indicates the serial port number, and the value is an integer.

The PuTTY is used to log in to the MM910 CLI. For details, see Logging In to the Server Over a Serial Port by Using the PuTTY.

Step 6 Run the following command to switch to the iMana 200:

```
smmset -l bladeN -d switchcom -v 4
```

For example, if the slot number is 16, run the following command:

```
smmset -l blade16 -d switchcom -v 4
```

The following information is displayed, indicating that the interface is successfully switched.

```
Success
```

Step 7 Log in to the iMana 200 of the compute node again over the serial port. For details, see [Step 1](#) and [Step 2](#).

Step 8 Enter the iMana 200 user name and password.

Step 9 Run the following command to check the iMana 200 users and rights assigned to the users:

```
root@BMC:/#ipmcget -d userlist
```

Step 10 Run the following command to change the password for a iMana 200 user:

```
ipmcset -d password -v username
```

For example, to change the password of the user **root**, run the following command:

```
ipmcset -d password -v root
```

Step 11 Enter the current user password (default password is Huawei12#\$).

Step 12 Set a new password.

Step 13 Enter the new password again.

The following information is displayed, indicating that the password is successfully changed.

```
Set user password successfully.
```

```
----End
```

4.5 Configuring the iMana 200 IP Address

This topic describes how to configure integrated management module (iMana 200) IP address of the CH242 V3.

Scenarios

Log in to the CH242 V3 over a serial port and configure the CH242 V3 iMana 200 IP address.

Prerequisites

Conditions

The compute node iMana 200 IP address cannot be on the network segment for the chassis management plane.

NOTE

The network segment for the chassis management plane is used for functions such as HMM and iMana200 heartbeats.

Data

The CH242 V3 iMana 200 IP address and subnet mask must be available.

Procedure

Step 1

NOTICE

To avoid conflicts with the network segment for the chassis management plane (172.31), the compute node iMana 200 IP address cannot be on the 172.31 network segment. If you need to set it to be on the 172.31 network segment, change the network segment for the chassis management plane first. For details, see section "Querying and Setting a Network Segment for the Management Plane of a Chassis (subnet)" in the [MM910 Management Module V100R001 Command Reference](#).

Run the following command to configure the iMana 200 IP address of the compute node:

```
ipmcset -t network port number -d ipaddr -v iMana IP address subnet mask
```

The network port number of iMana 200 is **eth0**, if iMana 200 IP address is **192.168.100.194**, and the subnet mask is **255.255.255.0**, run the following command:

```
ipmcset -t eth0 -d ipaddr -v 192.168.100.194 255.255.255.0
```

The iMana 200 IP address is successfully configured if the following information is displayed:

```
Set IP address 192.168.100.194 successfully .  
Set MASK address 255.255.255.0 successfully .
```

Step 2 Run the following command to view the configured iMana 200 IP address:

```
ipmcget -t eth0 -d ipinfo
```

The following information is displayed:

```
Enabled : Enable  
Mode : static  
Inet addr : 192.168.100.194  
Subnet Mask : 255.255.255.0  
Default Gateway :  
HWaddr : 00:18:82:59:23:03
```

----End

4.6 Changing the iMana 200 U-boot Password

This topic describes how to change the initial integrated management module (iMana 200) U-boot password.

Scenarios

Log in to the CH242 V3 over a serial port and change the initial iMana 200 U-boot password to improve the security of system operation and maintenance.

 NOTE

- Ensure that the password complexity check is enabled. The password complexity check is enabled by default.
- For security purposes, change the initial password upon the first login, and then change the password regularly.

The iMana 200 U-boot is software used to configure basic settings, such as hardware initialization and memory space mapping, to prepare for operating system (OS) triggering.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

You have logged in to iMana 200 over the serial port.

Data

Default iMana 200 U-boot password: Huawei12#\$.

Procedure

- Step 1** Run the following command to reboot the iMana 200 system of the compute node:

```
root@BMC:/#ipmcset -d reset
```

The following information is displayed:

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

- Step 2** Press **Y**.

The system starts to reboot.

- Step 3** When the message "Hit 'ctrl + b' to stop autoboot: 1" is displayed, press **Ctrl+B** immediately.

- Step 4** Enter the default iMana 200 U-boot password.

The following information is displayed, indicating that you have logged in to the U-boot command-line interface (CLI).

```
u-boot>
```

- Step 5** Run the following command to change the U-boot password:

```
u-boot> passwd
```

The following information is displayed:

```
Enter old password:
```

- Step 6** Enter an old password.

The following information is displayed:

```
Enter new password:
```

- Step 7** Enter a new password.

The following information is displayed:

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

Step 8 Enter the new password again.

The following information is displayed, indicating that the password is successfully changed.

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

password be changed successfully.
```

Step 9 Run the following command to exit the U-boot:

```
boot

----End
```

4.7 Logging In to the Real-Time Desktop

This topic describes how to log in to the CH242 V3 real-time desktop over the web user interface (WebUI) of the management module.

Scenarios

Log in to the CH242 V3 real-time desktop in remote control mode over the MM910 WebUI.

Prerequisites

Conditions

There are no special conditions for this operation.

Data

The following data is available:

- User name for logging in to the MM910 to be connected.
- Password for logging in to the MM910 to be connected.

Procedure

Step 1 Logging in to the MM910 WebUI

1. (Optional) Check the MM910 management network port out mode.

You can log in to the MM910 WebUI through a serial port and run the **outportmode** command to query and set the management network port out mode. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).

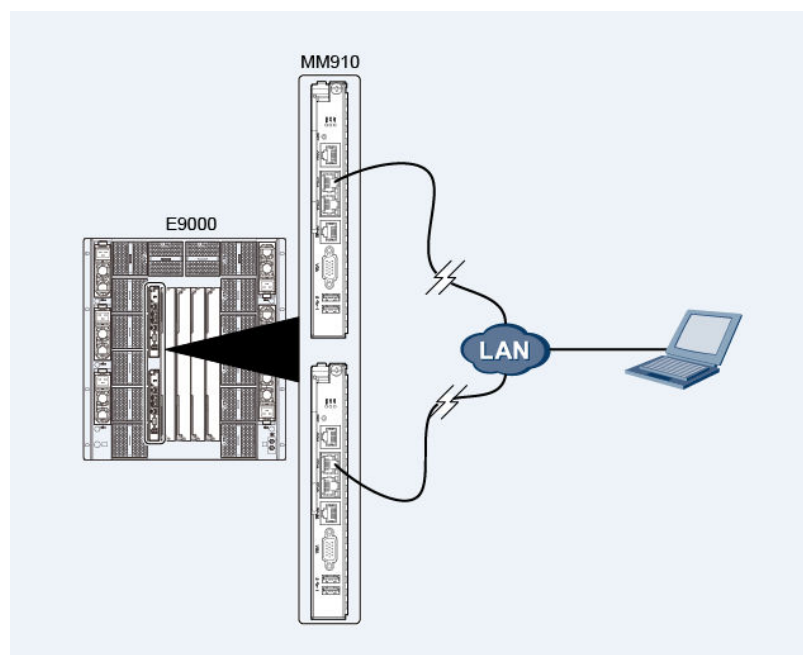
NOTE

The MM910 management port is provided by two modes.

- An Ethernet port on the switch module in slot 2X or 3X can be used as the MM910 management port. However, if a CX910/CX911/CX912/CX913/CX915 is in slot 2X or 3X, only a GE port can be used; if a CX920 is in slot 2X or 3X, only a 10GE port can be used; if a CX916/CX916L/CX930 is in slot 2X or 3X, only a 25GE port can be used. If a CX110/CX111/CX310/CX311/CX312/CX320/CX710 is in slot 2X or 3X, any port can be used. The CX910/CX911/CX912/CX913 are not recommended for providing the management network port of the management module.
 - The MGMT port on the MM910 panel can be used as the MM910 management port.
 - For MM910 (U54) 2.25 or earlier, the port on the switch module in slot 2X or 3X is used as the management network port by default. In this case, do not connect the MGMT port on the MM910 and the port on the switch module to the same network at the same time, otherwise, a network storm occurs and the network is interrupted. For MM910 (U54) 2.26 or later, the MGMT port is used as the management network port by default. For details about how to query the version, see the [MM910 Management Module V100R001 User Guide](#).
 - You can run the **outportmode** command to change the mode in which the management network port is provided. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).
2. Connect the local PC to the MM910 management network port based on the MM910 management network port out mode.
- MGMT port on the MM910 panel
 - Connect the Ethernet port on the PC to the MGMT port on the active or standby MM910 over a local area network (LAN).

Figure 4-6 shows the network connection.

Figure 4-6 Network connection

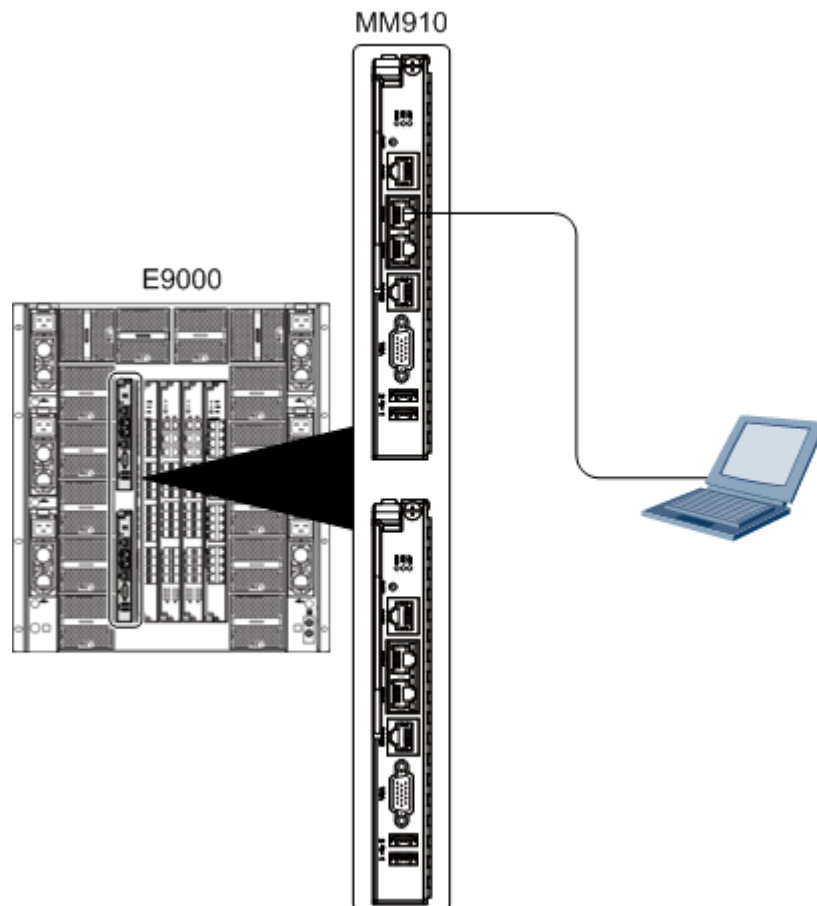


- Connect the Ethernet port on the PC to the MGMT port on the active MM910.

 NOTE

If the MGMT port of the active MM910 is available, use this port.

Figure 4-7 Connection between the local PC and the active MM910 (in slot MM2 in this example)

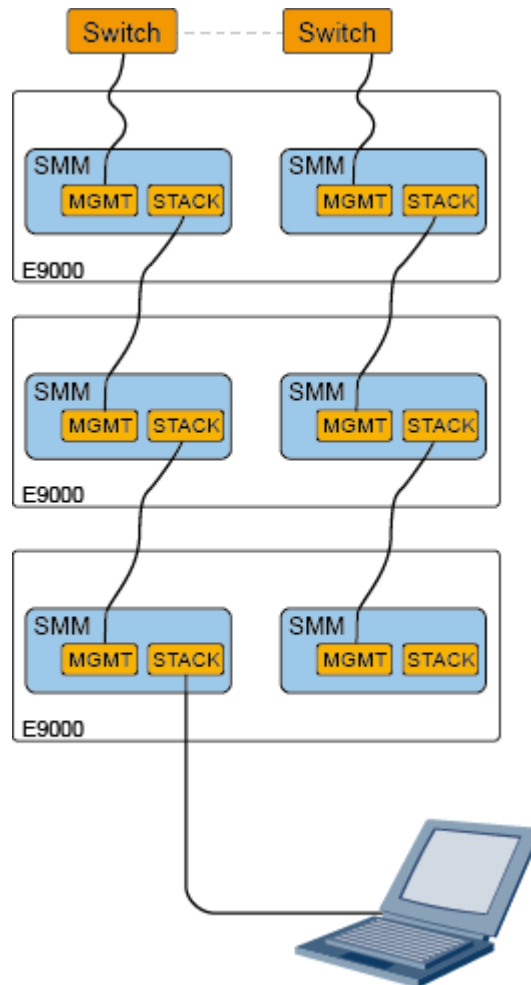


- Connect the Ethernet port on the local PC to the MGMT or STACK port on the active MM910.

 NOTE

If the MGMT port on the active MM910 is unavailable, connect the PC to the STACK port on the active MM910. If the STACK port is used to stack the MGMT port in another chassis, connect the PC to an idle STACK port on an active MM910 in a chassis cascaded with the E9000 chassis.

Figure 4-8 Connection between the local PC and an idle STACK port on an MM910 stacked



- An Ethernet port on the switch module

Connect the Ethernet port on the PC to a port on the switch module in slot 2X or 3X over a LAN.

NOTE

- Switch modules can be also installed in slots 1E and 4E of the E9000 chassis, but only the switch modules in slots 2X and 3X provide the management network ports.
 - If the ports on switch modules in slots 2X and 3X are used to access the management plane, isolate the management VLAN from the service VLAN for the switch modules for security purposes.
- Set an IP address and a subnet mask or add route information for the PC, and ensure that the PC can properly communicate with the MM910.
 - Open Internet Explorer, click  and choose **Internet Options**. The **Internet Options** dialog box is displayed.
 - Choose **Connections** and click **LAN Settings**. The **LAN Settings** dialog box is displayed.

6. In the **Proxy server** group box, deselect **Use a proxy server for your LAN** and click **OK**.
The **LAN Settings** dialog box is closed.
7. Click **OK**.
The **Internet Options** dialog box is closed.
8. Open Internet Explorer again, enter `https://MM910 floating IP address`, for example `https://192.168.2.3`, in the address box, and press **Enter**.

NOTE

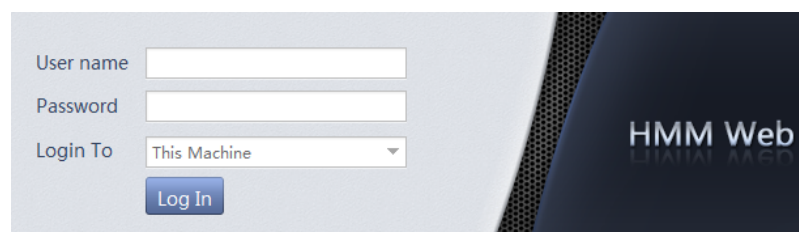
You can query or configure the MM910 floating IP address in any of the following ways:

- Use the chassis intelligent display. For details, see [FusionServer Pro E9000 Server V100R001 Chassis Intelligent Display Parameter Reference](#).
- Use the HMM WebUI. For details, see [Configuring the MM910 IP Addresses in MM910 Management Module V100R001 User Guide](#).
- Run the floatip command on the MM910 CLI. For details, see [MM910 Management Module V100R001 Command Reference](#).

The message "There is a problem with this website's security certificate" is displayed.

9. (Optional) Add the MM910 IP address to the **Trusted sites** zone.
By default, Internet Explorer enhanced security configuration is enabled on the Windows Server series OSs. Add the MM910 IP address to the trusted sites zone as follows:
 - a. On Internet Explorer, choose **Tools > Internet Options**.
The **Internet Options** dialog box is displayed.
 - b. Click the **Security** tab.
 - c. Click **Trusted sites**, and click **Sites**.
 - d. In the **Trusted sites** dialog box, click **Add** to add the MM910 IP address to the trusted site list, and click **Close**.
 - e. Refresh the page.
 - f. In the status bar of a browser, check whether the MM910 IP address is in the **Trusted sites** zone.
10. Click **Continue to this website (not recommended)**.
The **HMM Web** login page is displayed, as shown in [Figure 4-9](#).

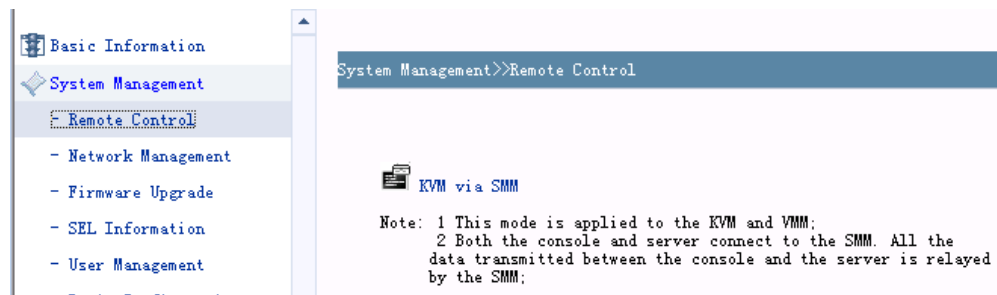
Figure 4-9 Logging in to HMM Web of version V603

**NOTE**

The login page varies slightly with the HMM software version.

Step 2 Log in to the real-time desktop of the compute node.

1. Perform operations based on the MM910 versions.
 - If the MM910 version is later than **(U54) 2.20**, go to [Step 2.3](#) to [Step 2.6](#).
 - If the MM910 version is **(U54) 2.20** or earlier, go to [Step 2.2](#) to [Step 2.6](#).
You can run the **smmget -l smm -d version** command on the MM910 CLI to check the software version.
2. In the navigation tree on the left, choose **System Management > Remote Control**, as shown in [Figure 4-10](#).

Figure 4-10 Remote control page

3. Perform operations based on the MM910 versions.
 - If the MM910 version is **(U54) 2.20** or earlier, Click **KVM via SMM**.
 - If the MM910 version is later than **(U54) 2.20**, Click **KVM via MM**.
A **Security Warning** is displayed.
4. Click **Yes**.
The **Warning-Security** page is displayed.
5. Click **Yes**.
Enter remote KVM page, as shown in [Figure 4-11](#).

Figure 4-11 KVM page

6. Click the compute node number.
The real-time desktop of the compute node is displayed.

NOTE

The resolution and colors of the desktop may differ slightly from the actual one due to the image compression algorithm.

----End

4.8 Configuring the RAID

This topic describes the procedure for configuring the redundant array of independent disks (RAID).

CH242 V3 4HDD supports two types of RAID controller cards: LSI SAS2208 and LSI SAS2308.

- LSI SAS2208: supports RAID 0, 1, 5, 6, 10, 50, and 60.
- LSI SAS2308: supports RAID 0, 1, 1E, and 10.

CH242 V3 8HDD supports two types of RAID controller cards: LSI SAS2208 and LSI SAS2308.

- LSI SAS2208: supports RAID 0, 1, 5, 6, 10, 50, and 60.
- LSI SAS2308: supports RAID 0, 1, 1E, and 10.

For details, see [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

4.9 Configuring the BIOS

This topic describes how to configure the basic input/output system (BIOS) for the CH242 V3.

Scenarios

Remotely configure the BIOS for the CH242 V3 by using the HMM Web management software. In this document, CH242 V3 is also referred to as the compute node.

You need to set the following configuration items:

- Compute node boot mode
- BIOS password

For details about other configuration items, see the [Huawei Server Brickland Platform BIOS Parameter Reference](#).

NOTE

- Ensure that the password complexity check is enabled. The password complexity check is enabled by default.
- For security purposes, change the initial password upon the first login, and then change the password regularly.

Prerequisites

Conditions

The compute node is powered on.

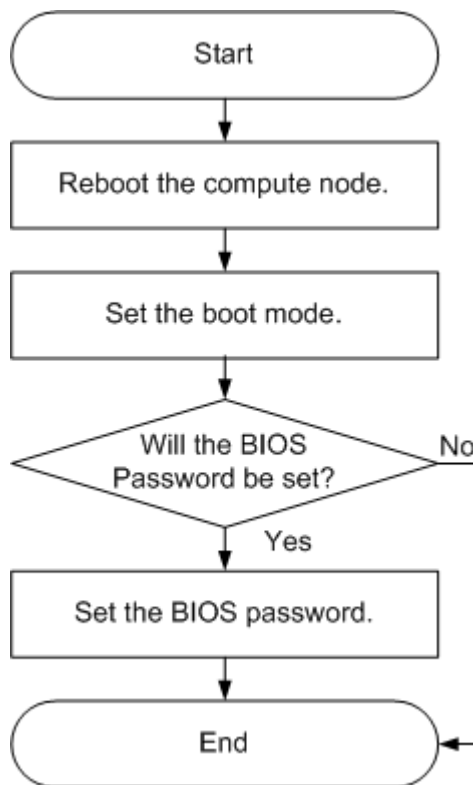
Data

Data preparation is not required for this operation.

Workflow

Figure 4-12 shows the process for configuring the BIOS.

Figure 4-12 Process for configuring the BIOS



Procedure

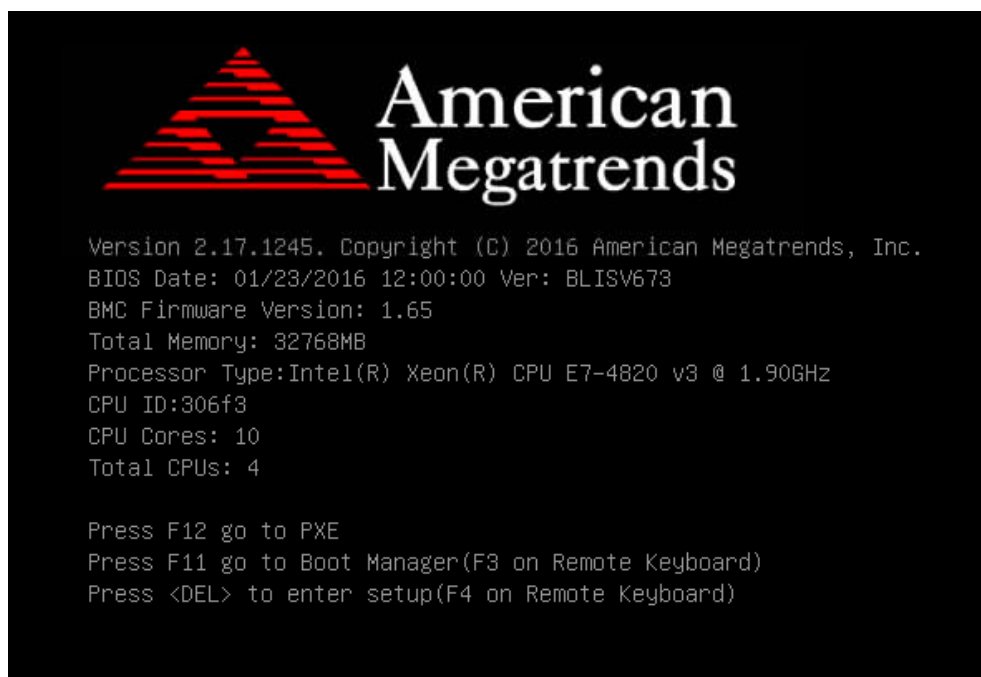
Step 1 Reboot the server.

1. Choose  on the menu bar that is in the upper part of the real-time compute node desktop.
2. Select **Forced System Reset**.
The message "Are you sure to perform this operation?" is displayed.
3. Click **Yes**.
The compute node is rebooted.
4. Press **Del** on the screen shown in **Figure 4-13** to start the BIOS Setup Utility.

NOTE

- Press **Delete** to go to the **BIOS Setup Utility** screen is displayed.
From a remote serial port, you can press **F4** to go to the **BIOS Setup Utility** screen.
- Press **F11** to go the boot manager screen for selecting boot options.
From a remote serial port, you can press **F3** to go the boot manager screen for selecting boot options.
- Press **F12** to boot from the network.

Figure 4-13 BIOS startup screen

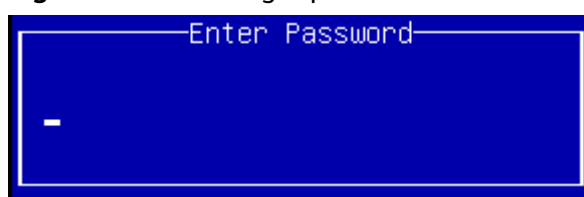


5. During the startup, a dialog box is displayed asking you to enter the password, as shown in [Figure 4-14](#).

 NOTE

- During system boot, you can press **F5** to select the keyboard type (French or American keyboard).
- The default BIOS password is **Huawei12#\$** for the French or American keyboard and is **Huawei12£\$** for the English keyboard.
- If an incorrect BIOS password is entered for three consecutive times, the BIOS is locked. You can press **Ctrl+Alt+Del** to unlock the BIOS.

Figure 4-14 Entering a password



Step 2 Set the server boot mode.

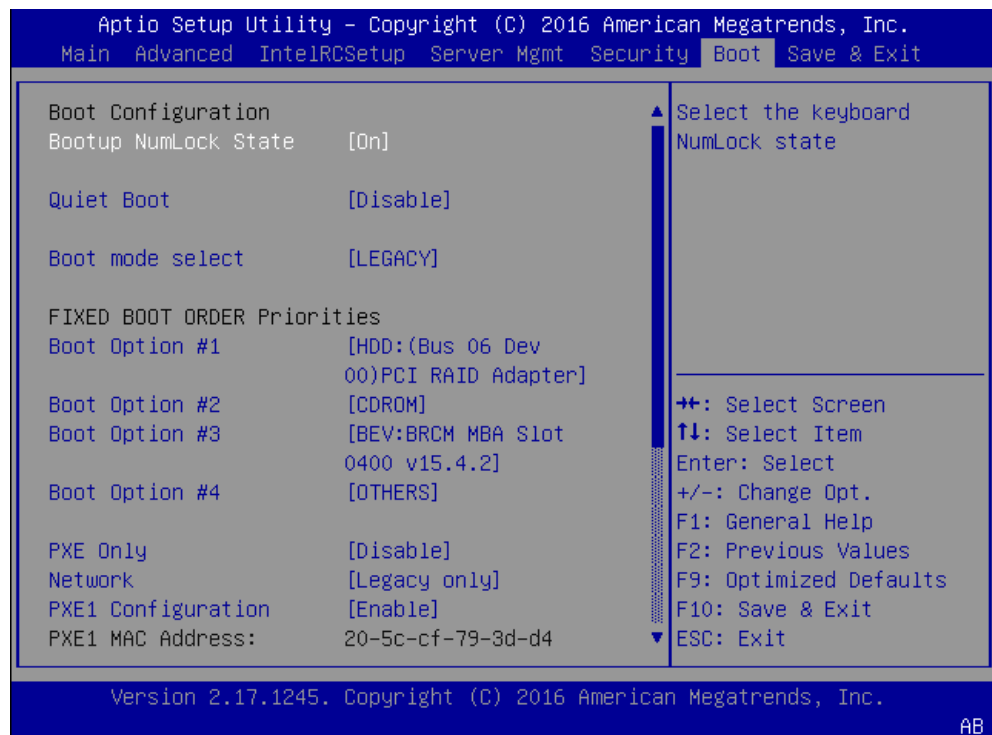
1. Choose **Boot**.

The **Boot** screen appears, as shown in [Figure 4-15](#).

 NOTE

Boot options are displayed under **FIXED BOOT ORDER Priorities** based on the preset priority. The default boot sequence is **HDD > CDROM > BEV > OTHERS**.

Figure 4-15 Boot screen



2. Select **Boot mode select** and press **Enter**.
3. In the displayed dialog box, select **LEGACY**, **UEFI** or **DUAL**, and press **Enter**.

NOTE

- The default boot mode is **LEGACY**.
 - If the boot type is changed after the OS has been installed in **Legacy** or **UEFI** mode, the OS will be inaccessible. To access the OS, you need to change the boot type to that used when the OS is installed. If the OS needs to be reinstalled, select the **Legacy** or **UEFI** mode based on actual situation.
 - If the capacity of the target hard drive or RAID group is greater than 2 TB, set **Boot Type** to **UEFI Boot**.
 - If the OS is to be installed on an NVMe hard drive, you can only set **Boot Type** to **UEFI Boot**.
 - If multiple boot devices are configured, you are advised to set **Boot Type** to **UEFI Boot** because certain boot devices may fail to boot if **Boot Type** is set to **Legacy Boot**. If you still want to set **Boot Type** to **Legacy Boot**, then disable redirection for certain serial ports or disable PXE for certain NICs based on the services in use. For details, see *Setting PXE for a NIC* and *Setting Serial Port Redirection* in the [Huawei Server Brickland Platform BIOS Parameter Reference](#).
4. Select the boot options to be set and press + or - to change the displayed sequence of the boot options.
 - Press + to move up a boot option.
 - Press - to move down a boot option.

NOTE

Boot options are booted in the displayed sequence.

5. Press **F10**.
The **Exit Saving changes?** dialog box appears.

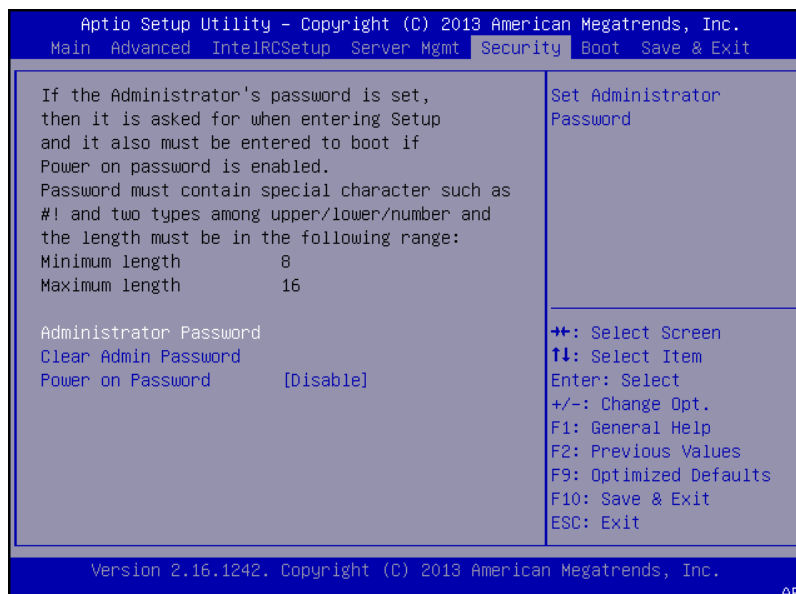
6. Select **Yes** and press **Enter** to save the setting.

Step 3 Set the BIOS password.

1. Select the **Security** tab.

The **Security** screen is displayed, as shown in [Figure 4-16](#).

Figure 4-16 Security screen



2. Select **Administrator Password** and press **Enter**. Set an administrator password.

NOTE

- The administrator password must be a string of 8 to 16 characters, and must contain special characters (including spaces), uppercase letters, lowercase letters, and digits.
 - The default BIOS password is **Huawei12#\$** for the French or American keyboard and is **Huawei12£\$** for the English keyboard.
3. (Optional) After the setting, select **Clear Administrator Password** to clear the password.
 4. Press **F10**.
The **Save configuration and exit?** dialog box appears.
 5. Select **Yes** and press **Enter** to save the setting.

----End

4.10 Installing the OS

This topic describes how to install an operating system (OS) for the CH242 V3.

For details about OSs supported by the CH242 V3, see [Computing Product Compatibility Checker](#).

The following list some of the OSs supported by the CH242 V3:

- Microsoft Windows Server 2008 SP2 32bit
- Microsoft Windows Server 2012 64bit
- Red Hat Enterprise Linux 6 Update 1 Server for x86
- SUSE Linux Enterprise Server 11 Service Pack 1 for x86

For details about how to install these OSs, see the [*Huawei Server OS Installation Guide*](#).

After installing an OS, use software and plug-ins to manage and diagnose server components for real-time monitoring.

5 Removing and Installing Components of the CH242 V3

This topic describes the precautions and procedure for removing and installing components of the CH242 V3.

[5.1 Removing a Hard Disk](#)

[5.2 Installing a Hard Disk](#)

[5.3 Removing a PCIe SSD Disk \(8HDD\)](#)

[5.4 Installing a PCIe SSD Disk \(8HDD\)](#)

[5.5 Removing the Cover](#)

[5.6 Installing the Cover](#)

[5.7 Removing a PCIe Card \(Riser Card Slots 1 and 2\)](#)

[5.8 Installing a PCIe Card \(Riser Card Slots 1 and 2\)](#)

[5.9 Removing a PCIe Card \(Hard Disk Backplane\)](#)

[5.10 Installing a PCIe Card \(Hard Disk Backplane\)](#)

[5.11 Removing a DIMM and an Air Duct](#)

[5.12 Installing a DIMM and an Air Duct](#)

[5.13 Removing a USB Flash Drive](#)

[5.14 Installing a USB Flash Drive](#)

[5.15 Removing a CPU](#)

[5.16 Installing a CPU](#)

[5.17 Removing a TPM](#)

[5.18 Installing a TPM](#)

[5.19 Removing the Mezz Modules](#)

[5.20 Installing the Mezz Modules](#)

[5.21 Removing a microSD Card](#)

- [5.22 Installing a microSD Card](#)
- [5.23 Removing an iBBU](#)
- [5.24 Installing an iBBU](#)
- [5.25 Removing a RAID Controller Card](#)
- [5.26 Installing a RAID Controller Card](#)
- [5.27 Removing a BIOS Battery](#)
- [5.28 Installing a BIOS Battery](#)
- [5.29 Removing the Mainboard and Compute Node Case](#)
- [5.30 Installing the Mainboard and Compute Node Case](#)

5.1 Removing a Hard Disk

You need to remove a hard disk before replacing it with a new one.

Scenarios

Remove a hard disk in any of the following scenarios:

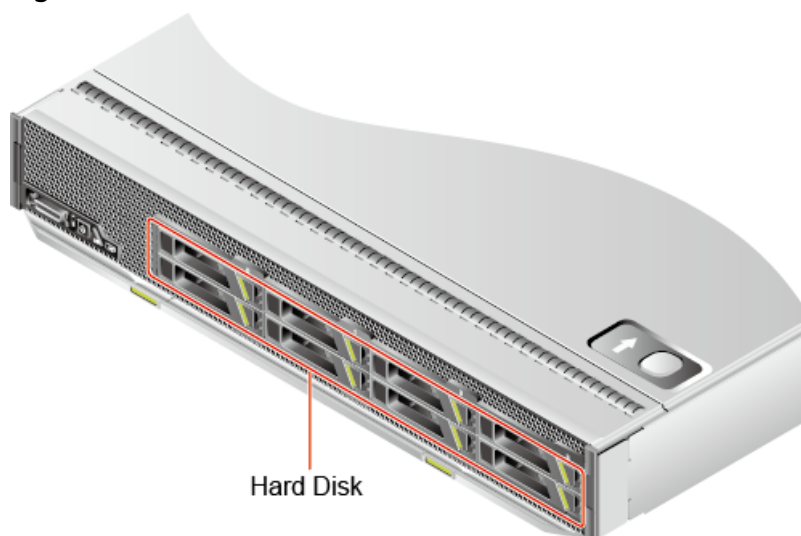
- The hard disk is faulty.
- The hard disk needs to be replaced with a newer model.
- The hard disk has no free space.

NOTE

- For details about how to erase data from a hard disk, see [6.8 Erasing Storage Media Data](#).
- Before removing a hard disk, check the following:
 - If no OS is installed on the hard disk, the compute node does not need to be powered off.
 - If an OS is installed on the hard disk, and the hard disk is configured in a RAID with redundancy, the compute node does not need to be powered off.
 - If an OS is installed on the hard disk, and the hard disk is not configured in a RAID or is configured in a RAID without redundancy (for example, RAID 0), the compute node needs to be powered off.

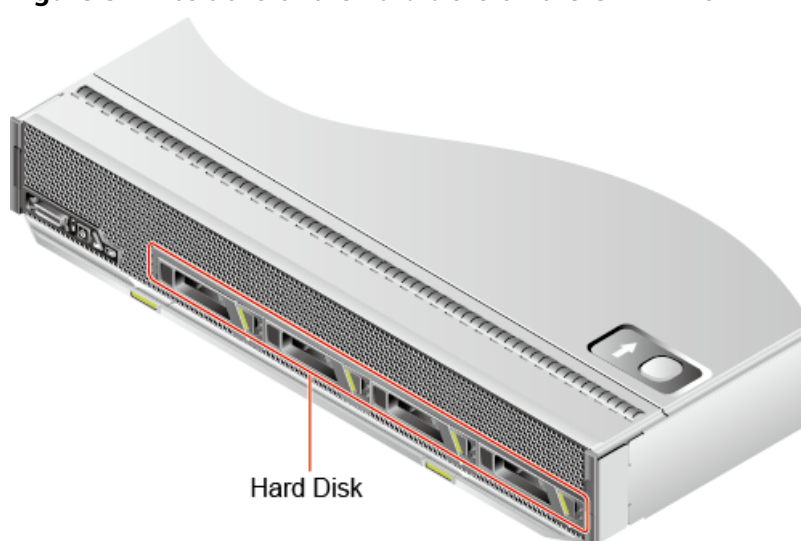
The CH242 V3 8HDD supports a maximum of eight hard disks. [Figure 5-1](#) shows the positions of the hard disks.

Figure 5-1 Positions of the hard disks on the CH242 V3 8HDD



The CH242 V3 4HDD supports a maximum of four hard disks. [Figure 5-2](#) shows the positions of the hard disks.

Figure 5-2 Positions of the hard disks on the CH242 V3 4HDD



Prerequisites

Conditions

You have determined whether data backup is required.

- If the hard disk to be removed is not configured in a RAID or is configured in a RAID without redundancy (for example, RAID 0), you have need to back up data on the hard disk.
- If the hard disk to be removed is configured in a RAID with redundancy, you can remove the hard disk without data backup.

Data

Data preparation is not required for this operation.

Tools

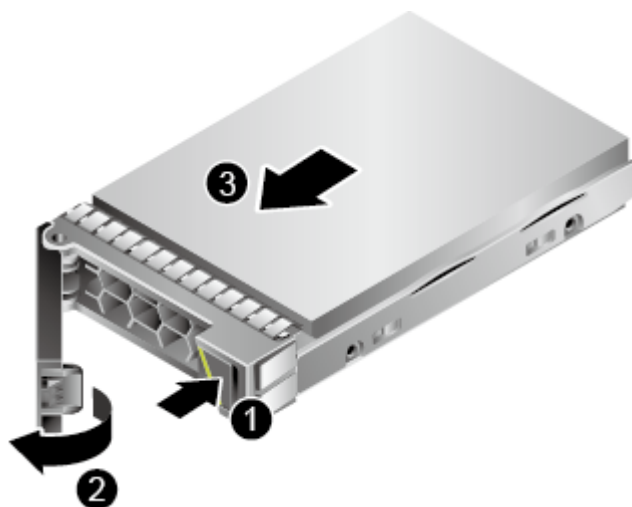
- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, an ESD bag.

Procedure

Step 1 Push the release button that fastens the hard disk ejector lever. See step (1) in [Figure 5-3](#).

The ejector lever automatically ejects.

Figure 5-3 Removing the hard disk



Step 2 Fully open the ejector lever. See step (2) in [Figure 5-3](#).

Step 3 Hold the ejector lever of the hard disk, and pull out the hard disk for about 3 cm (1.18 in.). Wait for at least 30s until the hard disk stops working. Remove the hard disk from the slot. See step (3) in [Figure 5-3](#).

Step 4 Place the removed hard disk in an ESD bag.

Step 5 (Optional) Install a filler module in the hard disk slot if you do not want to install a hard disk immediately.

----End

5.2 Installing a Hard Disk

You need to install a hard disk to replace the original one.

Scenarios

Install a hard disk in any of the following scenarios:

- A faulty hard disk needs to be replaced.
- A hard disk of a newer model needs to be used.
- A hard disk without free space needs to be replaced.

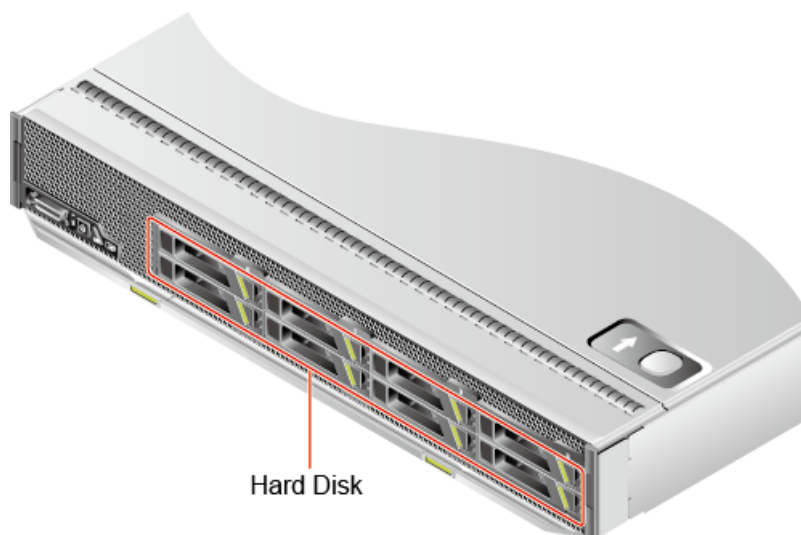
- A hard disk needs to be added.

NOTE

You do not need to power off the compute node when installing a hard disk.

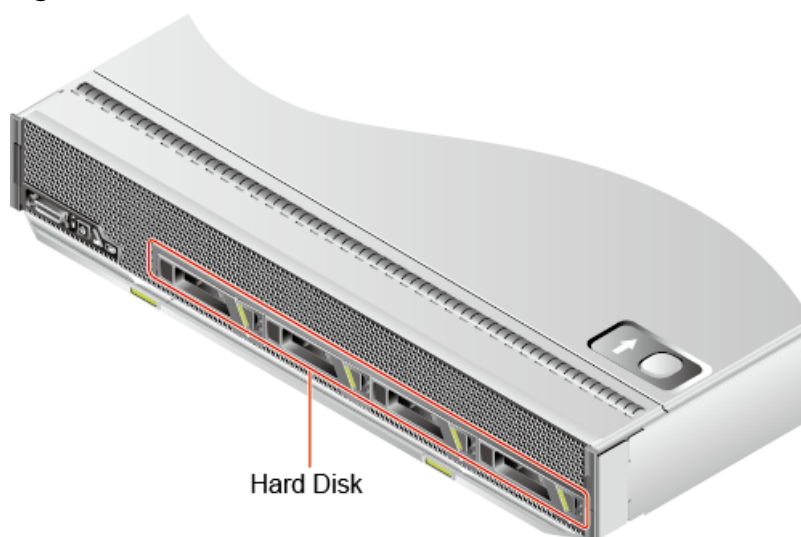
The CH242 V3 8HDD supports a maximum of eight hard disks. [Figure 5-4](#) shows the positions of the hard disks.

Figure 5-4 Positions of the hard disks on the CH242 V3 8HDD



The CH242 V3 4HDD supports a maximum of four hard disks. [Figure 5-5](#) shows the positions of the hard disks.

Figure 5-5 Positions of the hard disks on the CH242 V3 4HDD



Prerequisites

Conditions

There are no special conditions for this operation.

Data

Data preparation is not required for this operation.

Tools

Electrostatic discharge (ESD) gloves.

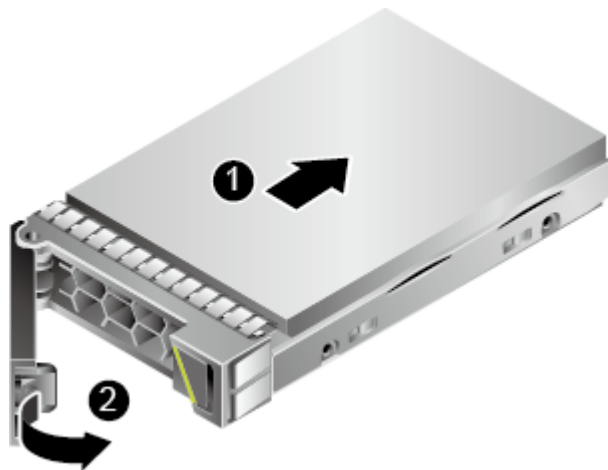
Hardware

Spare hard disk.

Procedure

- Step 1** Take the spare hard disk out of its ESD bag.
- Step 2** Fully open the ejector lever on the hard disk and insert the hard disk until it does not move. See step (1) in [Figure 5-6](#).

Figure 5-6 Installing a hard disk



- Step 3** Ensure that the handle is fastened to the beam, and close the handle to completely insert the HDD into the slot. See step (2) in [Figure 5-6](#).
- Step 4** Follow-up Procedure.
- The following is only for reference:
- If the original hard drive is not in the RAID group, the new hard drive becomes idle. You are advised to set the new hard drive as a global or dedicated hot spare drive. The procedure ends.
 - If the original RAID array (for example, RAID 0) does not support redundancy, reconfigure RAID. The procedure ends.
 - If the original RAID array is redundant and has a hot spare drive, the new hard drive becomes idle. You are advised to set the new hard drive as a global or dedicated hot spare drive. The procedure ends.
 - If the original RAID array is redundant but does not have a hot spare drive, data is automatically rebuilt to the new hard drive. The procedure ends.

For details, see [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

----End

5.3 Removing a PCIe SSD Disk (8HDD)

You need to remove a Peripheral Component Interconnect Express (PCIe) solid-state drive (SSD) disk when replacing it with a new one.

Scenarios

NOTICE

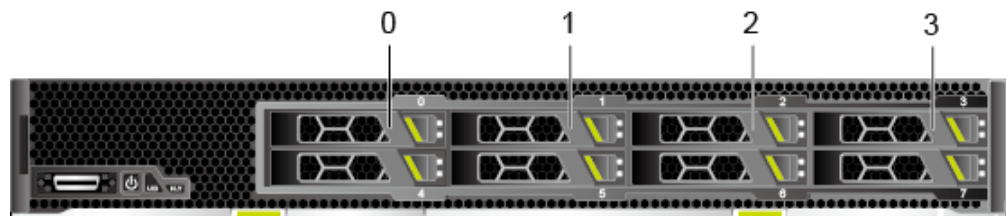
Power off the compute node before removing a PCIe SSD disk. PCIe SSD disks do not support hot swap. Removing a PCIe SSD disk without powering off the compute node will cause data loss in the disk.

Remove a PCIe SSD disk in any of the following scenarios:

- A faulty PCIe SSD disk needs to be replaced.
- A PCIe SSD disk of a new model needs to be used.
- A PCIe SSD disk that has no free space needs to be replaced with a new one.

The CH242 V3 8HDD supports a maximum of four PCIe SSDs, which can be installed in slots 0 to 3. [Figure 5-7](#) shows the positions and numbers.

Figure 5-7 CH242 V3 8HDD PCIe SSD positions and numbers



Impact on the System

Before removing a PCIe SSD disk, you have powered off the CH242 V3 and stopped all services running on the CH242 V3.

Prerequisites

Conditions

The compute node is powered off.

Data

Data preparation is not required for this operation.

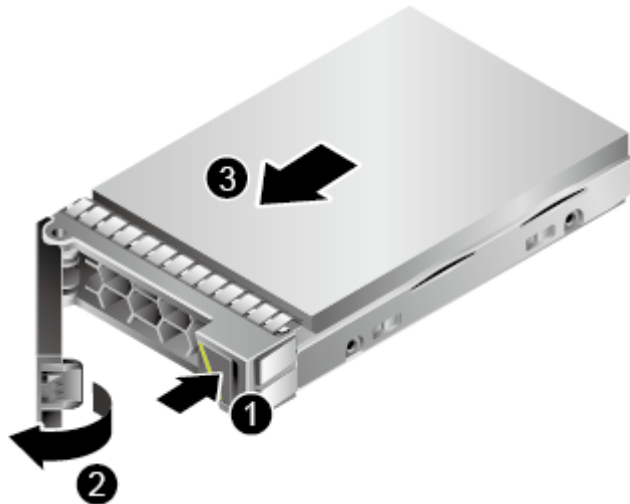
Tools

- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, an ESD bag.

Procedure

- Step 1** Push the spring that fastens the hard disk ejector lever. See step (1) in [Figure 5-8](#). The ejector lever automatically ejects.

Figure 5-8 Removing the hard disk



- Step 2** Fully raise the ejector lever. See step (2) in [Figure 5-8](#).
- Step 3** Hold the ejector lever of the hard disk, and pull out the hard disk for about 3 cm (1.18 in.), remove the hard disk from the slot. See step (3) in [Figure 5-8](#).
- Step 4** Place the removed hard disk in an ESD bag.
- Step 5** (Optional) Install a filler module in the hard disk slot if you do not want to install a hard disk immediately.

----End

5.4 Installing a PCIe SSD Disk (8HDD)

You need to install a Peripheral Component Interconnect Express (PCIe) solid-state drive (SSD) disk to replace the original one.

Scenarios

NOTICE

Power off the compute node before removing a PCIe SSD disk. PCIe SSD disks do not support hot swap. Removing a PCIe SSD disk without powering off the compute node will cause data loss in the disk.

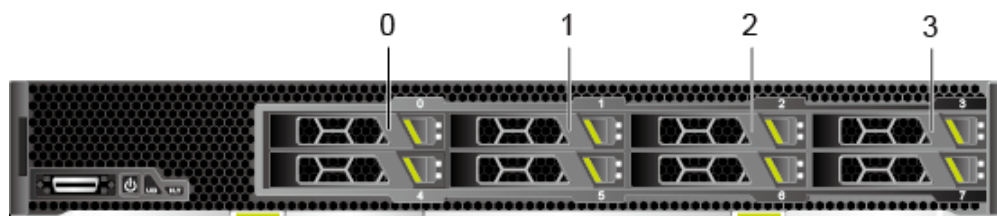
Install a PCIe SSD disk in any of the following scenarios:

- A faulty PCIe SSD disk needs to be replaced.
- A PCIe SSD disk of a new model needs to be used.

- A PCIe SSD disk that has no free space needs to be replaced with a new one.
- A PCIe SSD disk needs to be added.

The CH242 V3 8HDD supports a maximum of four PCIe SSDs, which can be installed in slots 0 to 3. [Figure 5-9](#) shows the positions and numbers.

Figure 5-9 CH242 V3 8HDD PCIe SSD positions and numbers



Impact on the System

Before installing a PCIe SSD disk, you have powered off the CH242 V3 and stopped all services running on the CH242 V3.

Prerequisites

Conditions

The compute node is powered off.

Data

Data preparation is not required for this operation.

Tools

Electrostatic discharge (ESD) gloves.

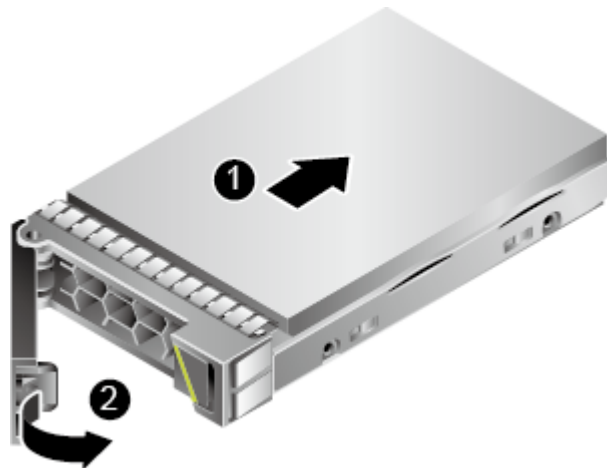
Hardware

Spare hard disk.

Procedure

- Step 1** Take the spare hard disk out of its ESD bag.
- Step 2** Fully open the ejector lever on the hard disk and insert the hard disk until it does not move. See step (1) in [Figure 5-10](#).

Figure 5-10 Installing a hard disk



Step 3 Ensure that the handle is fastened to the beam, and close the handle to completely insert the HDD into the slot. See step (2) in [Figure 5-10](#).

----End

5.5 Removing the Cover

You need to remove the CH242 V3 cover before replacing the CH242 V3 components.

Scenarios

Remove the CH242 V3 cover before replacing the CH242 V3 components. The procedure for removing the cover of the CH242 V3 8HDD is the same that for removing the cover of the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example.

Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

Electrostatic discharge (ESD) gloves.

Procedure

Step 1 Hold down the button on the CH242 V3 cover, and push the cover away from the CH242 V3. See steps (1) and (2) in [Figure 5-11](#).

Figure 5-11 Removing the CH242 V3 cover



Step 2 Lift the cover off the CH242 V3 and set it aside. See step (3) in [Figure 5-11](#).

----End

5.6 Installing the Cover

You need to install the CH242 V3 cover after replacing the CH242 V3 components.

Scenarios

Install the CH242 V3 cover after replacing the CH242 V3 components. The procedure for installing the cover of the CH242 V3 8HDD is the same that for installing the cover of the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example.

Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

Electrostatic discharge (ESD) gloves.

Procedure

Step 1 Insert the bottom tabs of the cover into the matching slots in the CH242 V3 chassis, and place the cover vertically on the CH242 V3. See step (1) in [Figure 5-12](#).

Figure 5-12 Installing the CH242 V3 cover



Step 2 Push the cover back in place on the CH242 V3. See step (2) in [Figure 5-12](#).

----End

5.7 Removing a PCIe Card (Riser Card Slots 1 and 2)

You need to remove a PCIe card before replacing it with a new one.

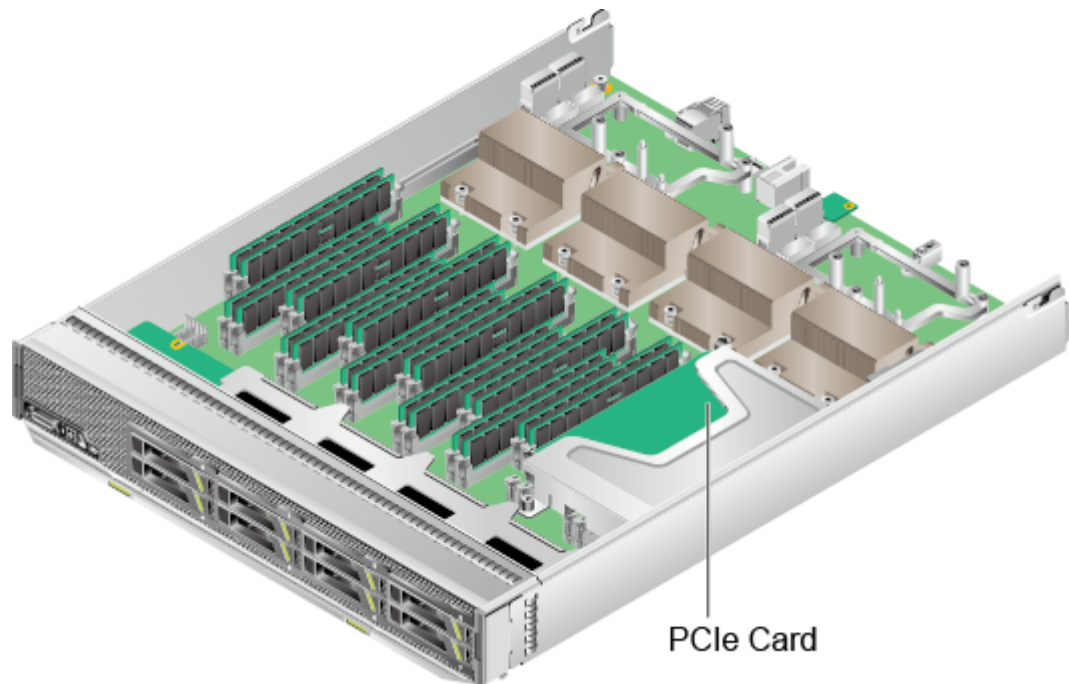
Scenarios

Remove a PCIe card in any of the following scenarios:

- A PCIe card fails.
- A PCIe card needs to be replaced with a new model.

Whether the CH242 V3 is configured with four or eight HDDs, the methods for removing PCIe cards on the riser card slots are the same. The following uses the CH242 V3 8HDD as an example and describes how to remove a PCIe card on the riser card slot 2 of the mainboard. [Figure 5-13](#) shows the PCIe card installation position on the CH242 V3 8HDD.

Figure 5-13 PCIe card installation position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

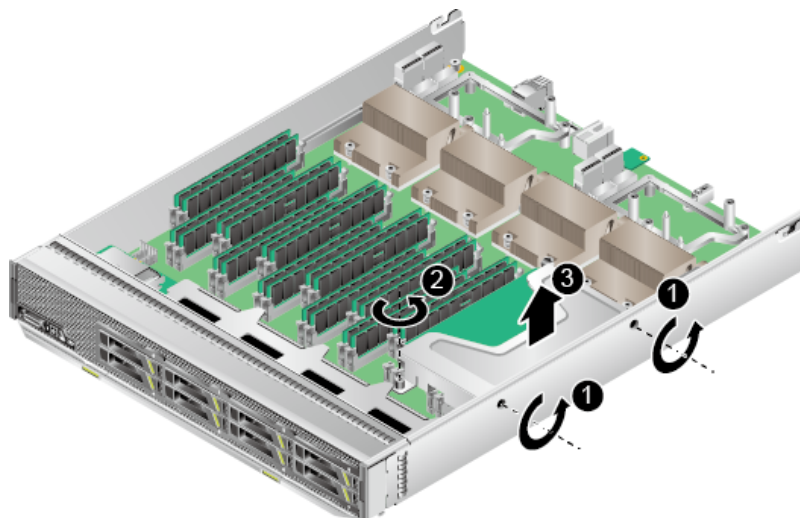
Tools

- Electrostatic discharge (ESD) gloves.
- M3 Phillips screwdriver.
- Packaging materials, for example, an ESD bag.

Procedure

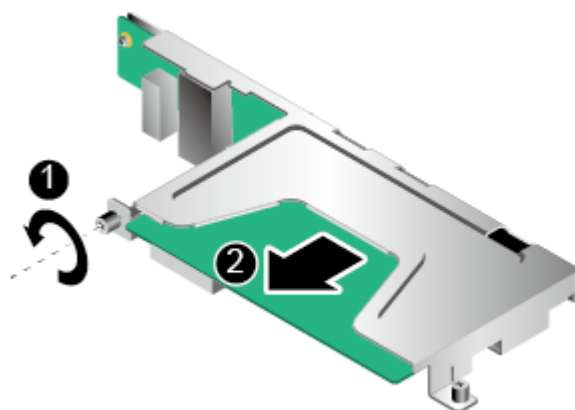
- Step 1** Use the Phillips screwdriver to loosen the two screws on two sides. See step (1) in [Figure 5-14](#).

Figure 5-14 Removing the PCIe card tray



- Step 2** Use a Phillips screwdriver to loosen the captive screws. See step (2) in [Figure 5-14](#).
- Step 3** Remove the PCIe card tray. See step (3) in [Figure 5-14](#).
- Step 4** Use a Phillips screwdriver to loosen the captive screws that secure the PCIe card tray. See step (1) in [Figure 5-15](#).

Figure 5-15 Removing a PCIe Card



- Step 5** Remove the PCIe card. See step (2) in [Figure 5-15](#).
- Step 6** Place the removed PCIe card in an ESD bag.

----End

5.8 Installing a PCIe Card (Riser Card Slots 1 and 2)

You need to install a PCIe card to replace the original one.

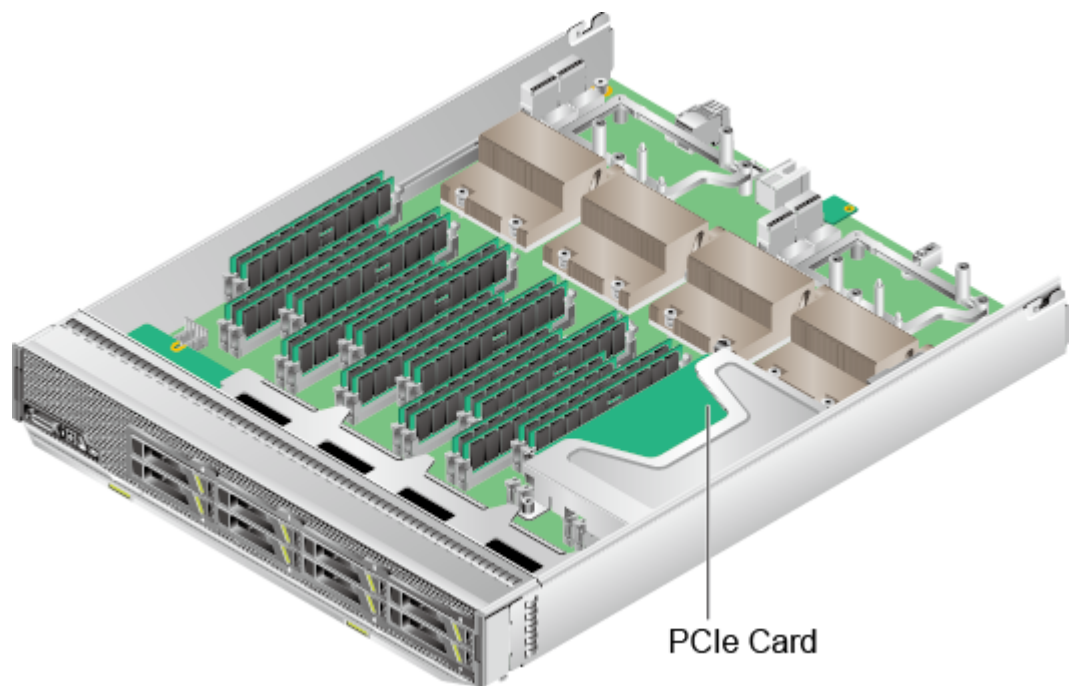
Scenarios

Install a PCIe card in any of the following scenarios:

- A PCIe card fails.
- A PCIe card needs to be replaced with a new model.
- A PCIe card needs to be added.

Whether the CH242 V3 is configured with four or eight HDDs, the methods for installing PCIe cards on the riser card slots are the same. The following uses the CH242 V3 8HDD as an example and describes how to install a PCIe card on the riser card slot 2 of the mainboard. **Figure 5-16** shows the PCIe card installation position on the CH242 V3 8HDD.

Figure 5-16 PCIe card installation position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.
- Before installing a full-height half-length PCIe card, remove the 10 DIMMs under the Riser card. For details, see [5.11 Removing a DIMM and an Air Duct](#).

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- M3 phillips screwdriver.

Hardware

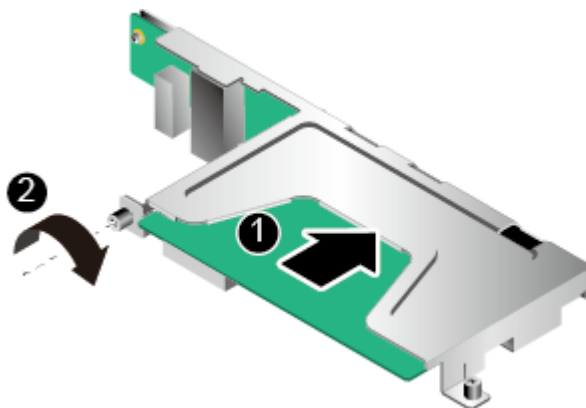
Spare PCIe card.

Procedure

Step 1 Take the PCIe card to be installed out of the ESD bag.

Step 2 Insert the PCIe card into the PCIe card tray. See step (1) in [Figure 5-17](#).

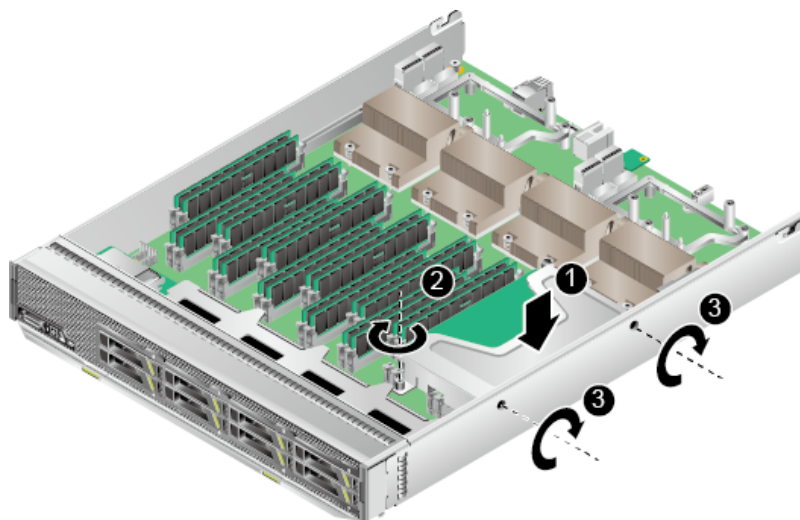
Figure 5-17 Installing a PCIe card



Step 3 Use a Phillips screwdriver to tighten the captive screws that secure the PCIe card tray. See step (2) in [Figure 5-17](#).

Step 4 Place the PCIe card tray on the compute node. See step (1) in [Figure 5-18](#).

Figure 5-18 Installing the PCIe card tray



Step 5 Use a Phillips screwdriver to tighten the captive screws that secure the PCIe card tray. See step (2) in [Figure 5-18](#).

Step 6 Use the Phillips screwdriver to tighten the two screws on two sides. See step (3) in [Figure 5-18](#).

----End

5.9 Removing a PCIe Card (Hard Disk Backplane)

You need to remove a PCIe card before replacing it with a new one.

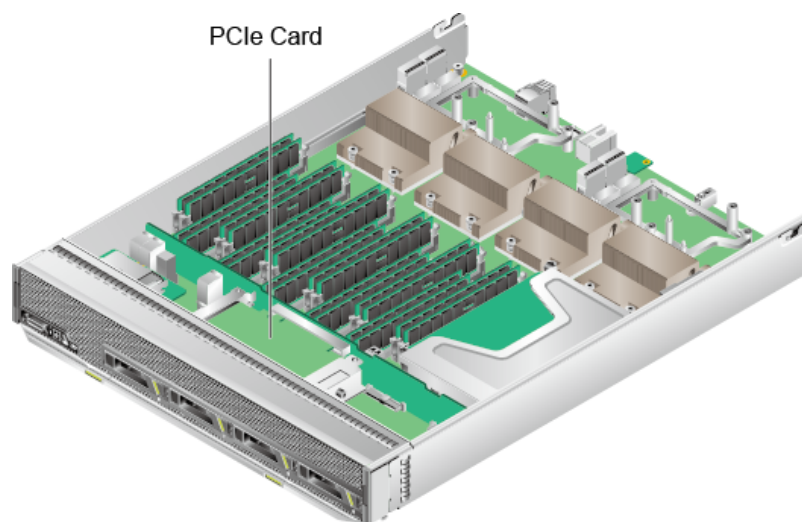
Scenarios

Remove a PCIe card in any of the following scenarios:

- A PCIe card fails.
- A PCIe card needs to be replaced with a new model.

Figure 5-19 shows the PCIe card position on the CH242 V3 4HDD backplane.

Figure 5-19 PCIe card position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- The iBBU has been removed. For details, see [5.23 Removing an iBBU](#).

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- M3 Phillips screwdriver.
- Packaging materials, for example, an ESD bag.

Procedure

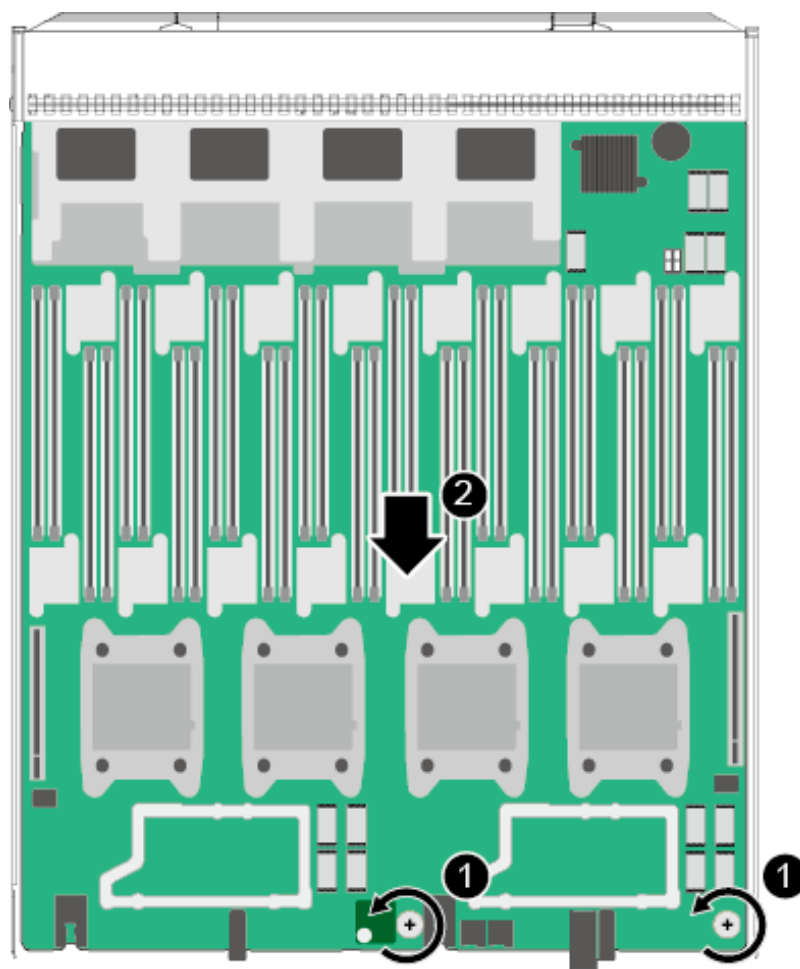
Step 1

NOTICE

Only personnel authorized by Huawei and Huawei technical support personnel can remove the compute node mainboard.

Use the Phillips screwdriver to remove the two captive screws on the CH242 V3 mainboard. See step (1) in [Figure 5-20](#).

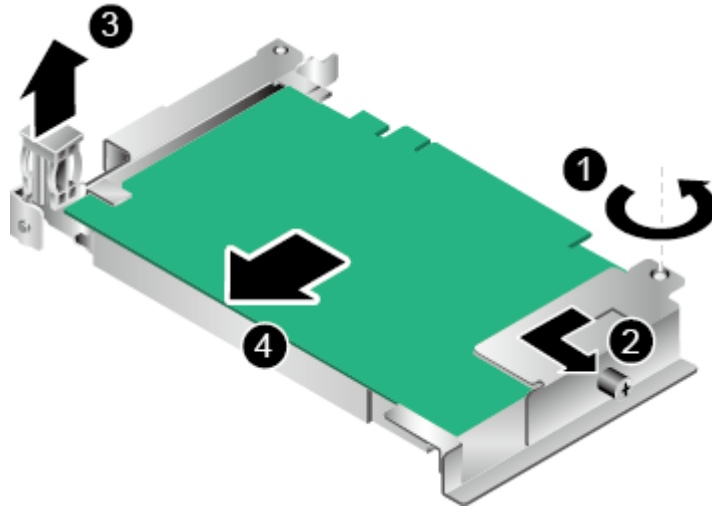
Figure 5-20 Removing the mainboard



Step 2 Pull the CH242 V3 mainboard 1 cm out from the chassis in the direction shown in step (2) in [Figure 5-20](#), lift the mainboard 6 mm up, and then pull out one fourth of the mainboard.

Step 3 Use a Phillips screwdriver to loosen the captive screws that secure the PCIe card, Push the hard disk tray outwards. See step (1) (2) in [Figure 5-21](#).

Figure 5-21 Removing a PCIe card



Step 4 Remove the plastic part of the PCIe card. See step (2) in [Figure 5-21](#).

Step 5 Remove the PCIe card. See step (3) in [Figure 5-21](#).

Step 6 Place the removed PCIe card in an ESD bag.

-----End

5.10 Installing a PCIe Card (Hard Disk Backplane)

You need to install a PCIe card to replace the original one.

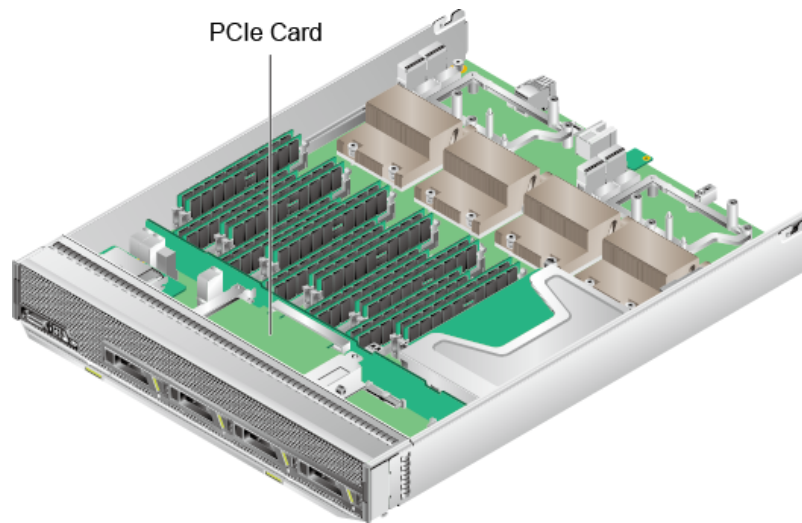
Scenarios

Install a PCIe card in any of the following scenarios:

- A PCIe card fails.
- A PCIe card needs to be replaced with a new model.
- A PCIe card needs to be added.

[Figure 5-22](#) shows the PCIe card position on the CH242 V3 4HDD backplane.

Figure 5-22 PCIe card position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- M3 phillips screwdriver.

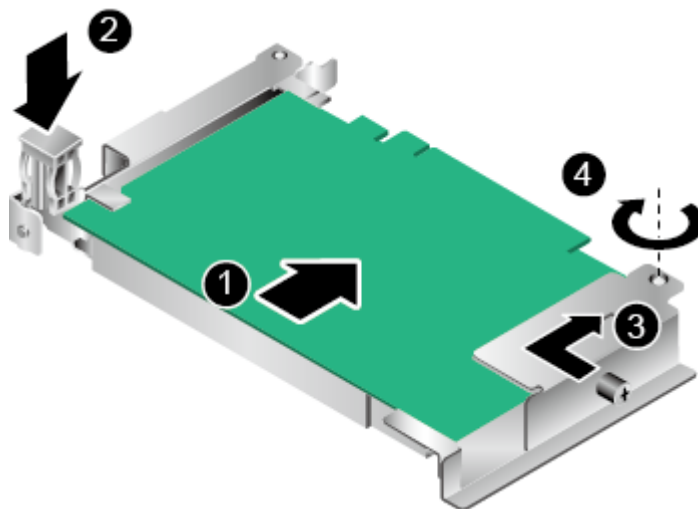
Hardware

Spare PCIe card.

Procedure

- Step 1** Insert the PCIe card. See step (1) in [Figure 5-23](#).
- Step 2** Press the plastic part of the PCIe card. See step (2) in [Figure 5-23](#).
- Step 3** Push the hard disk tray back, Use a Phillips screwdriver to tighten the captive screws that secure the PCIe card. See step (3) (4) in [Figure 5-23](#).

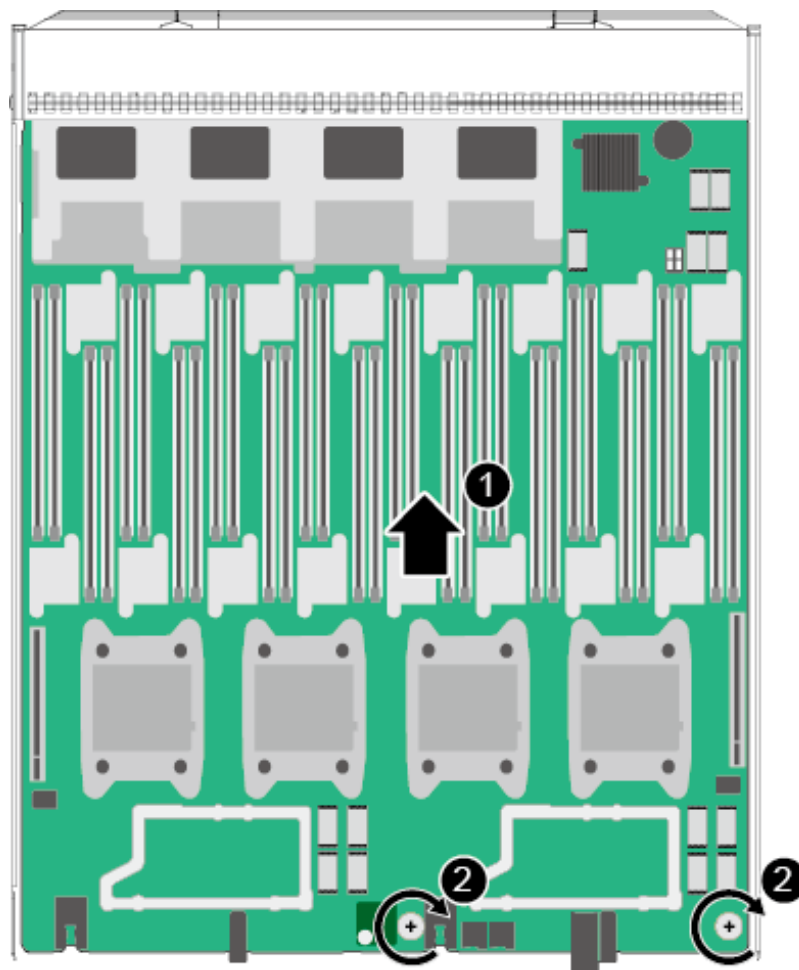
Figure 5-23 Installing a PCIe card



Step 4 Push the CH242 V3 mainboard to the tray. See step (1) in [Figure 5-24](#).

Step 5 Use a Phillips screwdriver to tighten the two captive screws on the CH242 V3 mainboard. See step (2) in [Figure 5-24](#).

Figure 5-24 Installing a mainboard



----End

5.11 Removing a DIMM and an Air Duct

You need to remove a dual-inline memory module (DIMM) before replacing it with a new one.

Scenarios

Remove a DIMM in any of the following scenarios:

- The DIMM is faulty.
- The DIMM needs to be replaced by a newer model.

Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

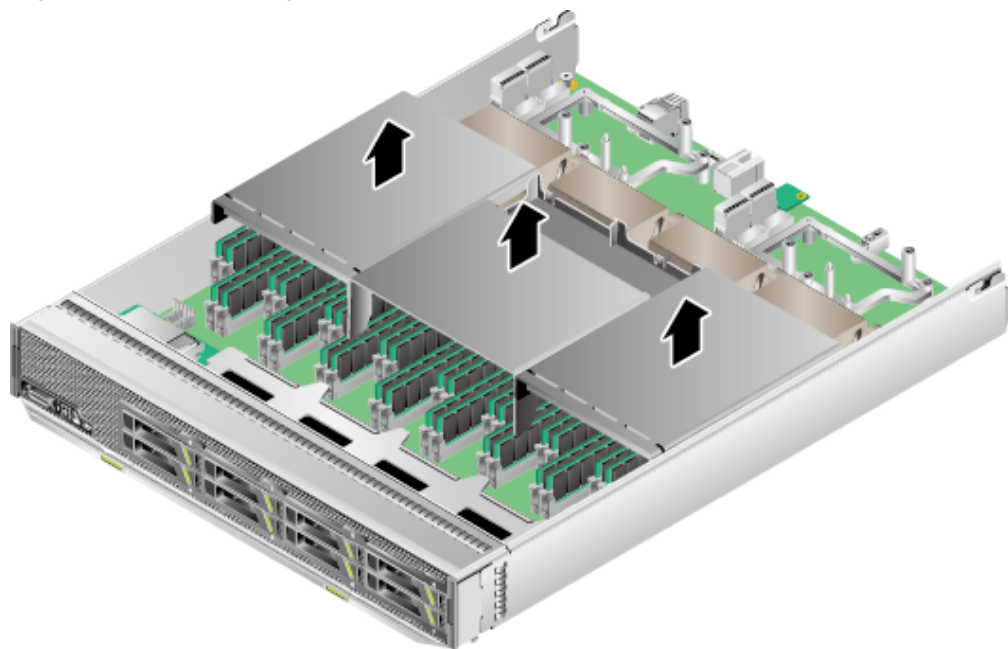
Tools

- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, ESD bag.

Procedure

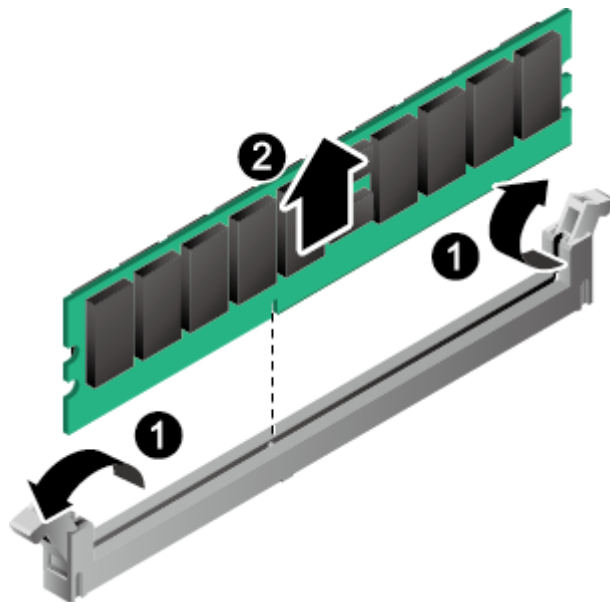
Step 1 Lift both sides of the air duct, as shown in [Figure 5-25](#).

Figure 5-25 Removing an air duct



- Step 2** Open the two fixing clips of the DIMM slot at the same time. See step (1) in [Figure 5-26](#).

Figure 5-26 Removing the DIMM



- Step 3** Remove the DIMM from the slot. See step (2) in [Figure 5-26](#).
- Step 4** Place the removed DIMM in an ESD bag.
- Step 5** (Optional) Install a protective cover in the DIMM slot if you do not want to install a DIMM immediately.

----End

5.12 Installing a DIMM and an Air Duct

You need to install a new dual in-line memory module (DIMM) to replace the original one or to expand the memory capacity.

Scenarios

Install a DIMM in any of the following scenarios:

- A faulty DIMM needs to be replaced.
- A DIMM of a newer model needs to be used.
- A DIMM is installed to expand the system memory capacity.

The CH242 V3 supports two or four CPUs and a maximum of 32 DIMMs. [Table 5-1](#) describes the DIMM installation rules. Refer to [Figure 2-14](#) and [Figure 2-11](#) for the CPU and DIMM slot numbering.

Table 5-1 Memory slot configuration rules

CPU	DIMM
CPU1, CPU2	000(1A1), 010(1B1), 200(2A1), 210(2B1), 020(1C1), 030(1D1), 220(2C1), 230(2D1), 100(1E1), 110(1F1), 300(2E1), 310(2F1), 120(1G1), 130(1H1), 320(2G1), 330(2H1)
CPU1, CPU2, CPU3, and CPU4	000(1A1) ^a , 010(1B1) ^a , 200(2A1), 210(2B1), 400(3A1), 410(3B1), 600(4A1) ^b , 610(4B1) ^b , 020(1C1) ^a , 030(1D1) ^a , 220(2C1), 230(2D1), 420(3C1) ^b , 430(3D1) ^b , 620(4C1) ^b , 630(4D1) ^b , 100(1E1) ^a , 110(1F1) ^a , 300(2E1) ^a , 310(2F1) ^a , 500(3E1), 510(3F1), 700(4E1) ^b , 710(4F1) ^b , 120(1G1) ^a , 130(1H1) ^a , 320(2G1), 330(2H1), 520(3G1), 530(3H1), 720(4G1) ^b , 730(4H1) ^b
Note: If a server is configured with four CPUs and full-height half-length PCIe cards, the DIMM slots under the PCIe cards cannot be used. • If a full-height half-length PCIe card is installed on the riser card 1, you do not need to install DIMMs in the slots marked with a. • If a full-height half-length PCIe card is installed on the riser card 2, you do not need to install DIMMs in the slots marked with b. If a server is configured with four CPUs and PCIe cards thinner than 10 mm, the DIMM slots under the PCIe cards are available.	

Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

Electrostatic discharge (ESD) gloves.

Hardware

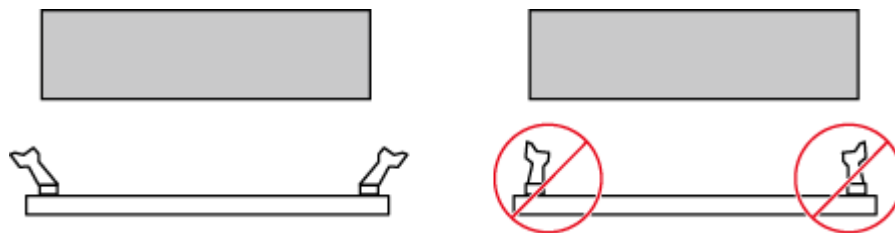
New DIMM.

Procedure

Step 1 Take the new DIMM out of the ESD bag.

Step 2 Ensure that the two fixing clips of the DIMM slot are open, as shown in [Figure 5-27](#).

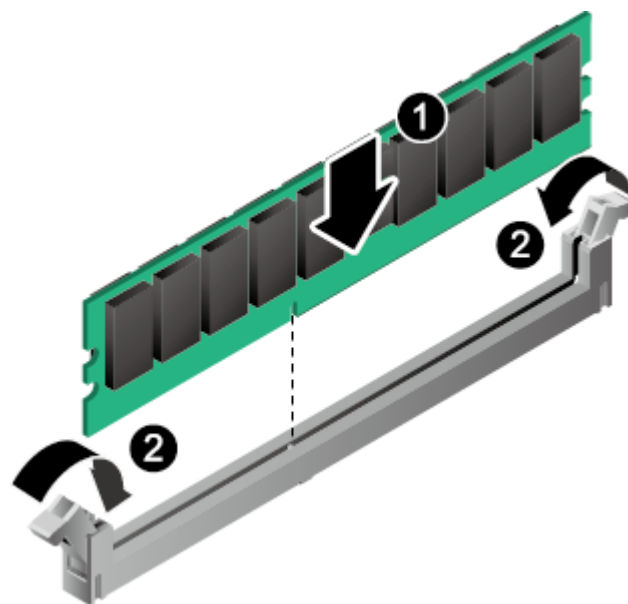
Figure 5-27 Opening the fixing clips on the DIMM slot



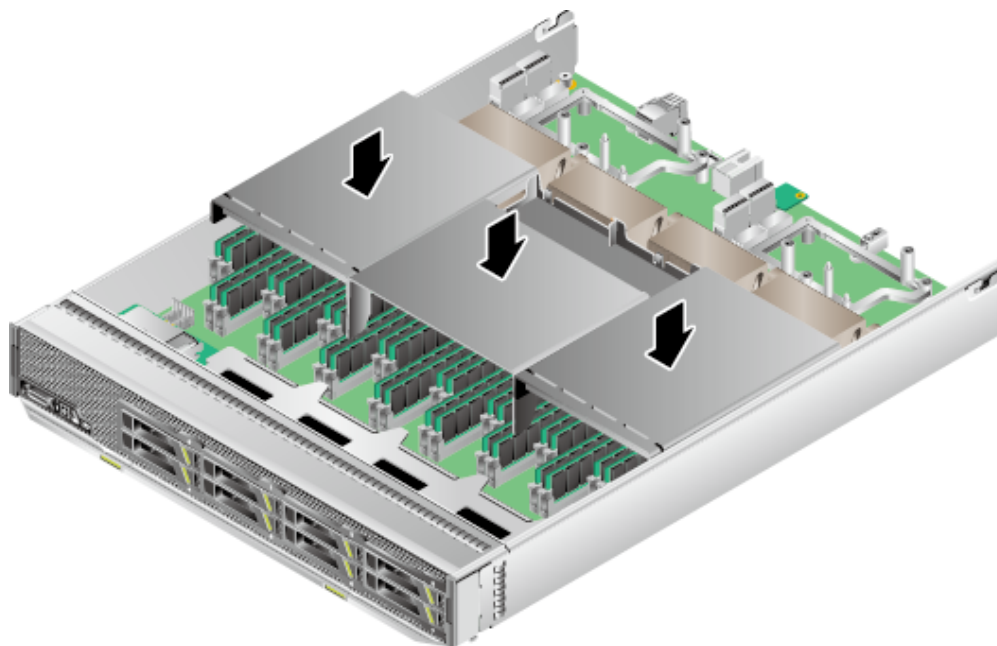
Step 3 Align the DIMM with the DIMM slot, and insert the DIMM into the slot, as shown in [Figure 5-28](#).

The two fixing clips close automatically.

Figure 5-28 Installing the DIMM



Step 4 Align the right edge of the air duct with the edges around DIMMs on the right, and the left edge of the air duct with the edges of DIMMs on the left and the heat sink, and then install the air duct, as shown in [Figure 5-29](#).

Figure 5-29 Installing an air duct**Step 5** Verification.

1. Power on the compute node.
2. In the address bar of Internet Explorer, enter *https://IP address of the iMana 200 management network port*.
3. On the iMana 200 login page, enter the user name and password.
 - **User Name** : Enter the default user name **root**.
 - **Password** : Enter the default password **Huawei12#\$**.
4. Click **Log In**. The **iMana 200** UI appears.
5. Choose **System Information > System Hardware**.
6. Check the DIMM information to ensure that the replacement is successful.
 - If the information about the new DIMM is displayed, the replacement is successful.
 - If the information about the original DIMM is displayed, enter the BIOS, and view the DIMM information. For details, see [Huawei Server Brickland Platform BIOS Parameter Reference](#).

----End

5.13 Removing a USB Flash Drive

You need to remove a USB flash drive before replacing it with a new one.

Scenarios

Remove a USB flash drive in either of the following scenarios:

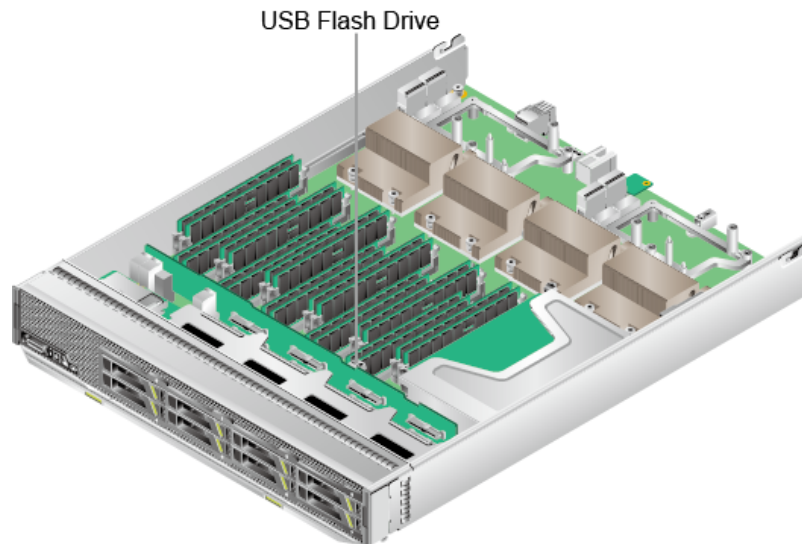
- The USB flash drive is faulty.
- The USB flash drive needs to be replaced with a newer model.

 NOTE

For details about how to erase data from a USB flash drive, see [6.8 Erasing Storage Media Data](#).

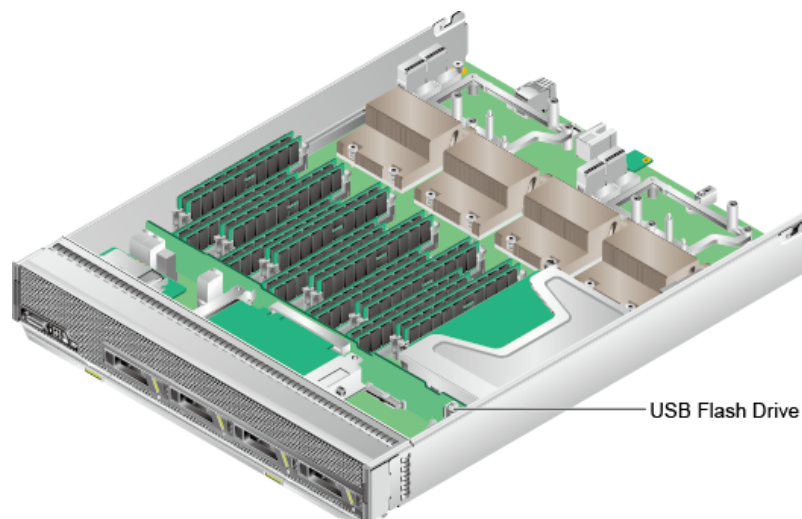
[Figure 5-30](#) shows the position of the USB flash drive on the CH242 V3 8HDD.

Figure 5-30 Position of the USB flash drive on the CH242 V3 8HDD



[Figure 5-31](#) shows the position of the USB flash drive on the CH242 V3 4HDD.

Figure 5-31 Position of the USB flash drive on the CH242 V3 4HDD



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).

- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

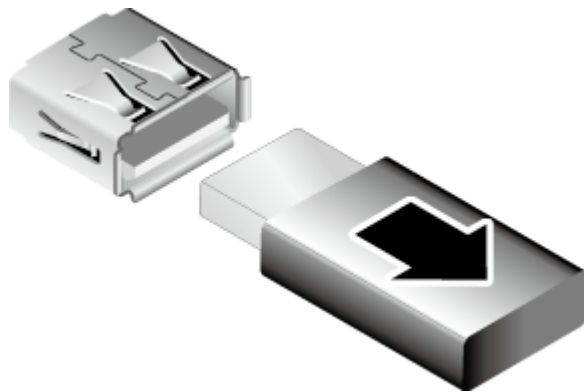
Tools

- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, ESD bag.

Procedure

- Step 1** Remove the USB flash drive from the connector on the compute node, as shown in [Figure 5-32](#).

Figure 5-32 Removing the USB flash drive



- Step 2** Place the removed USB flash drive in an ESD bag.

----End

5.14 Installing a USB Flash Drive

You need to install a USB flash drive to replace the original one.

Scenarios

Install a USB flash drive in either of the following scenarios:

- Replace a faulty USB flash drive.
- Replace a USB flash drive with a new model.

[Figure 5-33](#) shows the position of the USB flash drive on the CH242 V3 8HDD.

Figure 5-33 Position of the USB flash drive on the CH242 V3 8HDD

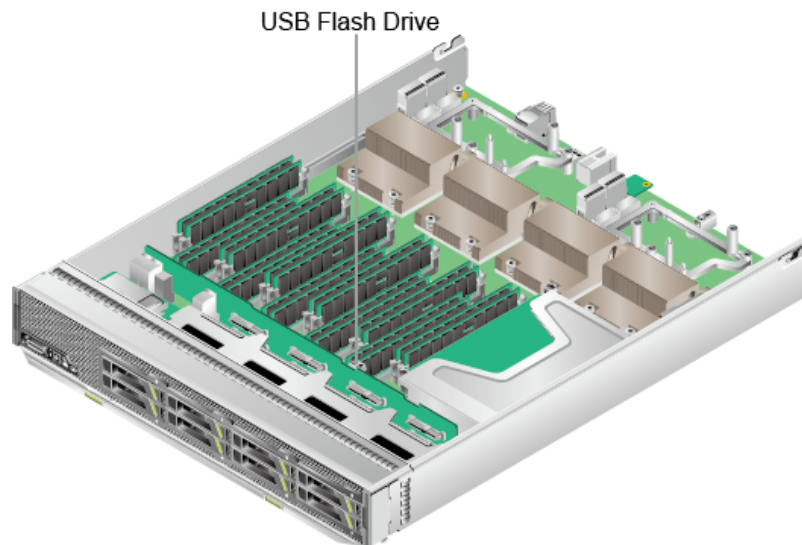
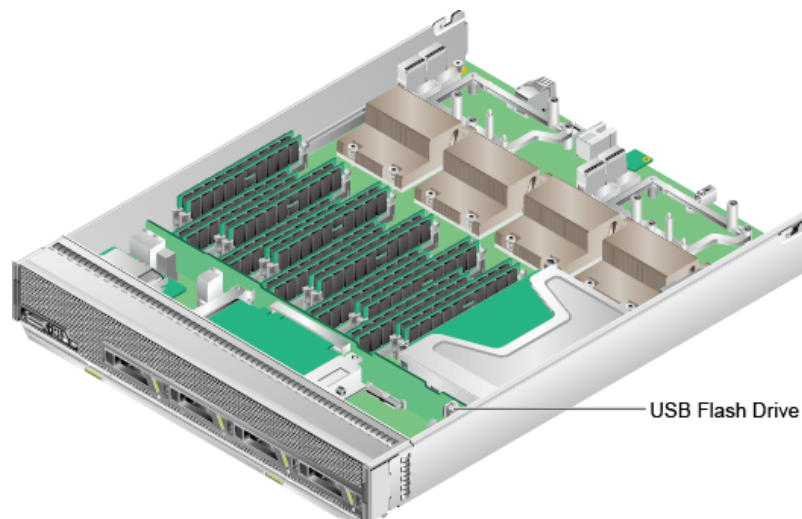


Figure 5-34 shows the position of the USB flash drive on the CH242 V3 4HDD.

Figure 5-34 Position of the USB flash drive on the CH242 V3 4HDD



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

There are no special conditions for this operation.

Tools

Electrostatic discharge (ESD) gloves.

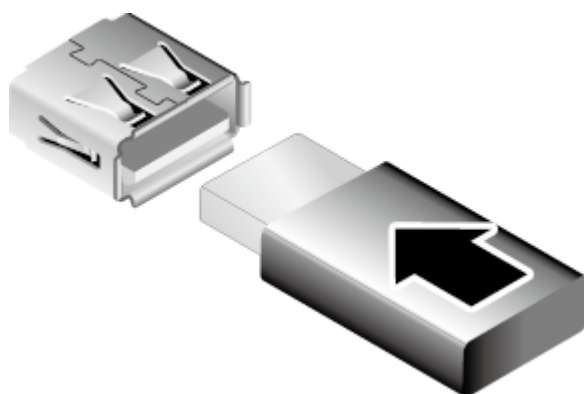
Hardware

Spare USB flash drive.

Procedure

- Step 1** Take the new USB flash drive out of its ESD bag.
- Step 2** Insert the USB flash drive into the connector, as shown in [Figure 5-35](#).

Figure 5-35 Installing a USB flash drive



----End

5.15 Removing a CPU

You need to remove a CPU before replacing it with a new one.

Scenarios

NOTICE

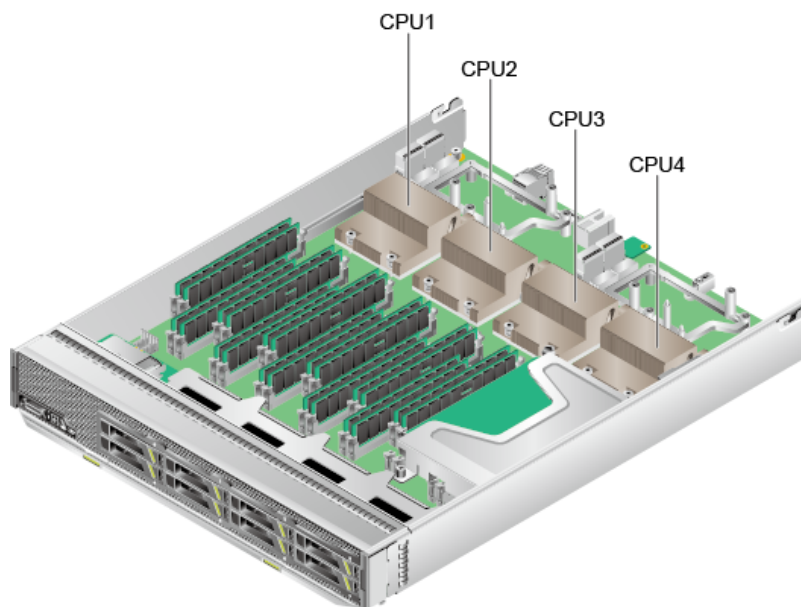
- Only personnel authorized by Huawei and Huawei technical support personnel can remove CPUs.
 - Do not wear ESD gloves because they may damage the pins on the CPU socket.
-

Remove a CPU in any of the following scenarios:

- The CPU is faulty.
- The CPU needs to be replaced with a newer model.

The procedure for removing a CPU from the CH242 V3 8HDD is the same that for removing a CPU from the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. The CH242 V3 supports a maximum of four CPUs. [Figure 5-36](#) shows the CPU installation positions and numbers.

Figure 5-36 CPU positions and CPU numbers



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

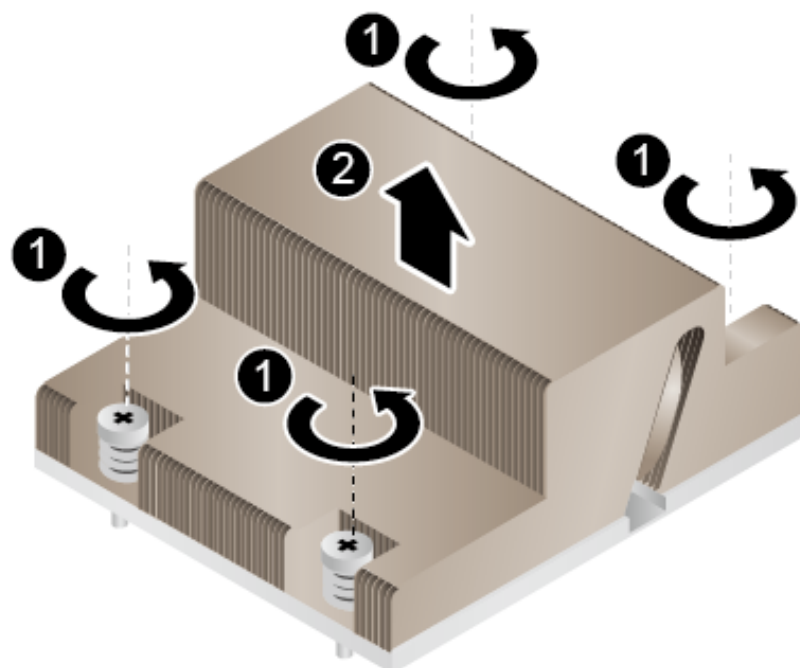
Tools

- Electrostatic discharge (ESD) wrist strap.
- M3 Phillips screwdriver.
- Packing materials, for example, ESD bag.

Procedure

- Step 1** Use the Phillips screwdriver to loosen the four screws securing the heat sink in a diagonal sequence. See step (1) in [Figure 5-37](#).

Figure 5-37 Removing the heat sink



Step 2 Lift the heat sink out of the server. See step (2) in [Figure 5-37](#).

Step 3

NOTICE

Do not use any tool or sharp object to lift the securing rod on the CPU socket. Otherwise, the compute node may be damaged.

Raise the securing rod near the  or  label. See step (1) in [Figure 5-38](#).

Figure 5-38 Removing the CPU

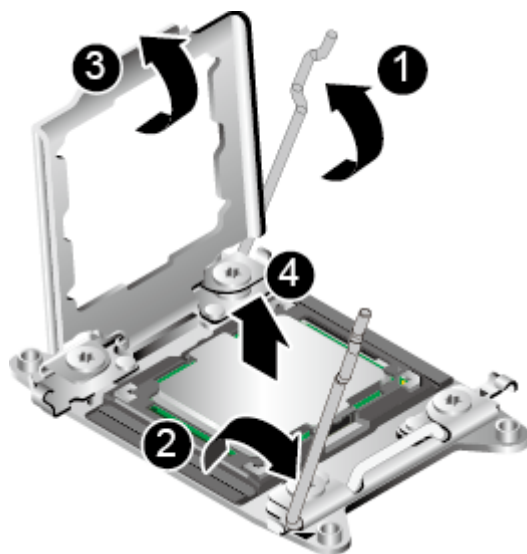
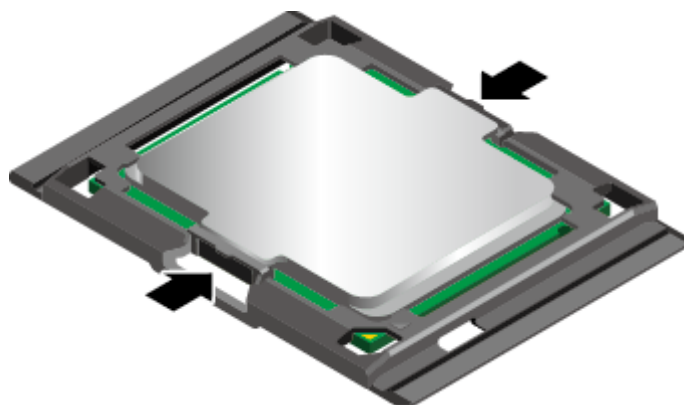


Figure 5-39 Positions for squeezing a CPU installation tool

- Step 4** Raise the securing rod near the  or  label. See step (2) in [Figure 5-38](#).
- Step 5** Open the CPU load plate, squeeze two sides (shown in [Figure 5-39](#)) of the CPU installation tool, and raise the tool with the CPU inside vertically. See steps (3) and (4) in [Figure 5-38](#).
- Step 6** Use a tissue to clean off any residual thermal paste from the CPU, and place the CPU installation tool with the CPU inside in an ESD bag.

NOTICE

Ensure that CPU sockets are populated with CPUs or CPU protection caps during transportation and storage.

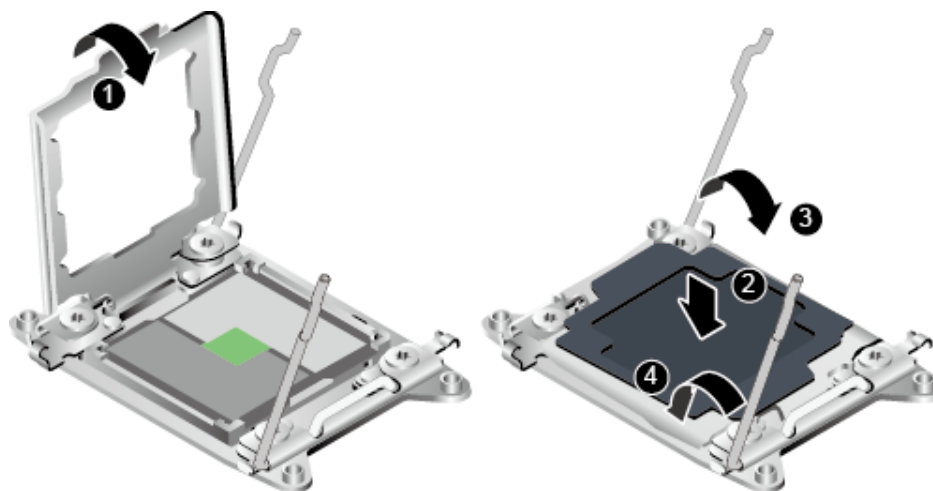
Step 7 (Optional) Install a CPU protection cap.

1. Close the CPU socket cover. See step (1) in [Figure 5-40](#).
2. Hold the CPU protection cap horizontally, aligning its edges with those of the CPU socket, and fit the protection cap securely onto the socket. See step (2) in [Figure 5-40](#).

 NOTE

An ill-positioned CPU protection cap may damage the pins in the corners of the CPU socket.

3. Close the securing rods. See steps (3) and (4) in [Figure 5-40](#).

Figure 5-40 Installing a CPU protection cap

----End

5.16 Installing a CPU

Install a new CPU to replace the original one.

Scenarios

NOTICE

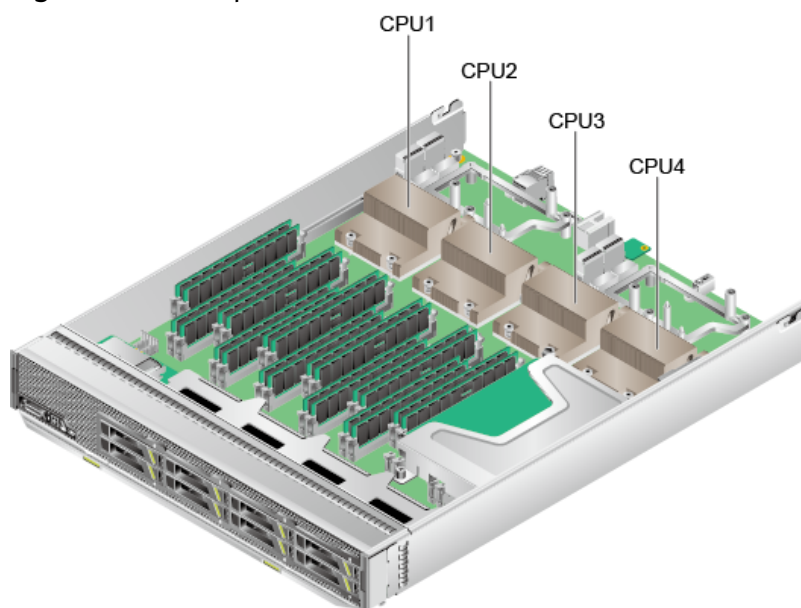
- Only personnel authorized by Huawei and Huawei technical support personnel can install CPUs.
 - Do not wear electrostatic discharge (ESD) gloves because they may damage the pins on the CPU socket.
-

Install a CPU if:

- A faulty CPU needs to be replaced.
- A CPU of a newer model needs to be used.

The procedure for installing a CPU on the CH242 V3 8HDD is the same that for installing a CPU on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. The CH242 V3 supports a maximum of four CPUs. [Figure 5-41](#) shows the CPU installation positions and numbers.

Figure 5-41 CPU positions and CPU numbers



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

- ESD wrist strap.
- Finger cots.
- M3 Phillips screwdriver.

Hardware

New CPU.

Procedure

Step 1 Take the spare CPU out of its ESD bag.

Step 2 Before installing CPUs, ensure that CPU sockets do not have bent pins and are free from foreign objects.

NOTICE

If a CPU socket has bent pins or foreign objects, stop installing the CPU and contact Huawei technical support.

- Step 3** Before installing a CPU or heat sink, use tissue to clean up the oil, remaining thermal compound, or foreign objects on their surfaces.
- Step 4** Wear finger cots and latch the CPU into one side of the CPU installation tool. Ensure that the triangle marks (polarities) on the CPU, CPU socket cover, and CPU socket face the same direction. [Figure 5-42](#) shows the triangle marks (polarities). [Figure 5-43](#) shows the operation procedure.

Figure 5-42 Triangle marks (polarities)

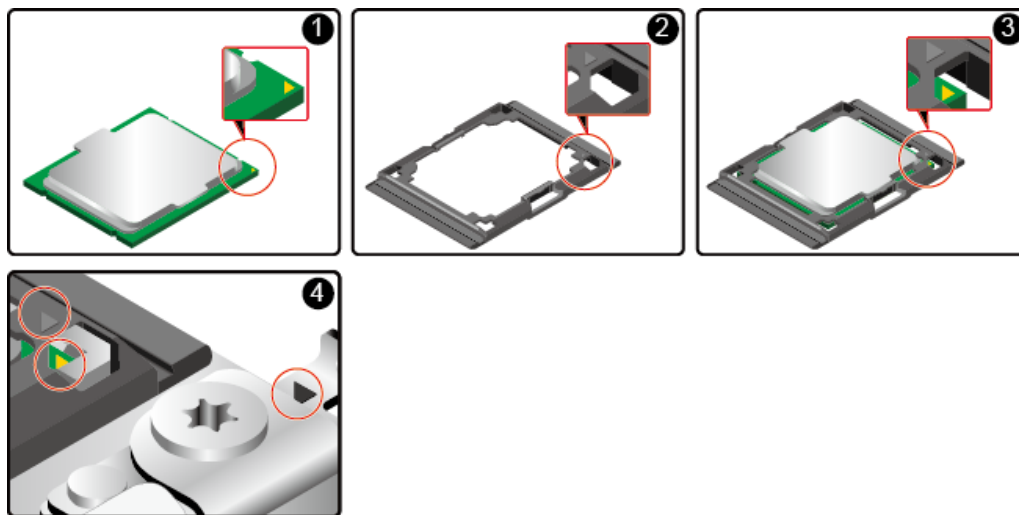
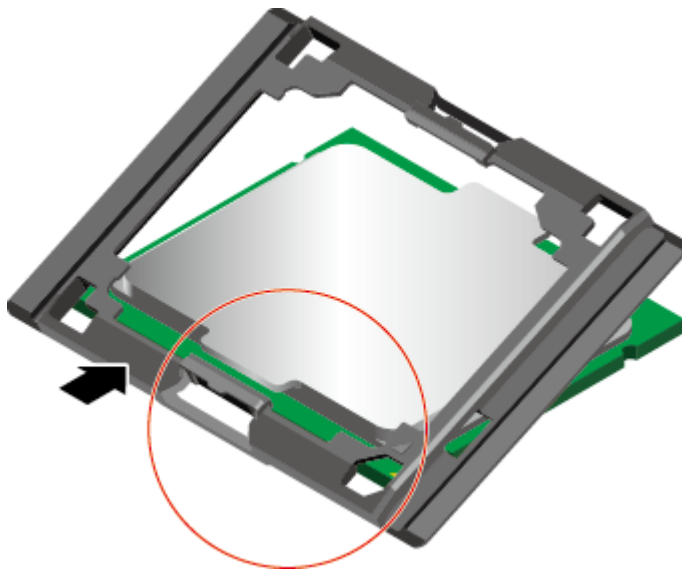
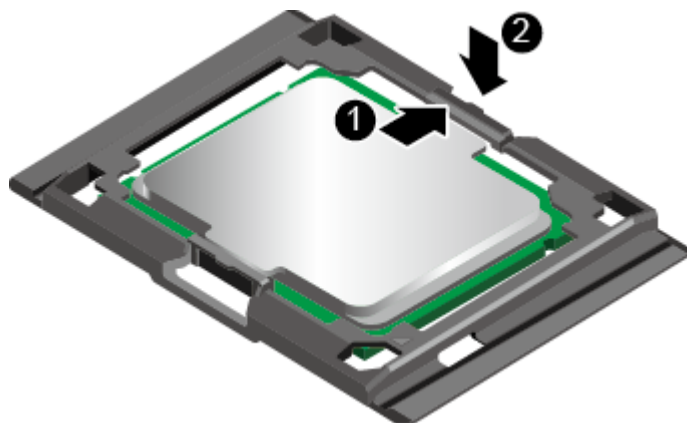


Figure 5-43 Latching a CPU into one side of a CPU installation tool



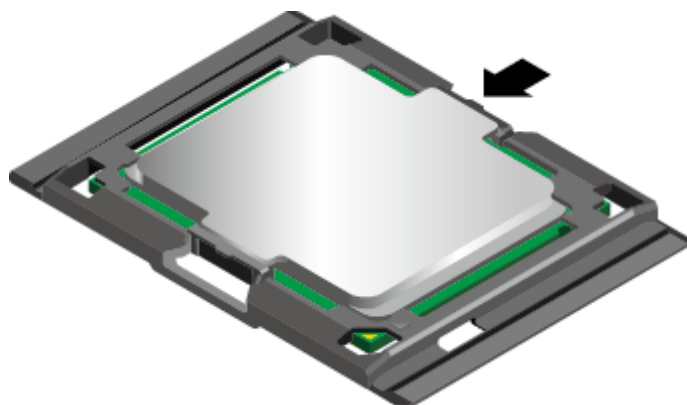
- Step 5** Pull out the other side of the CPU installation tool and squeeze the tool downward to latch the CPU. See [Figure 5-44](#).

Figure 5-44 Pulling out the other side of a CPU installation tool



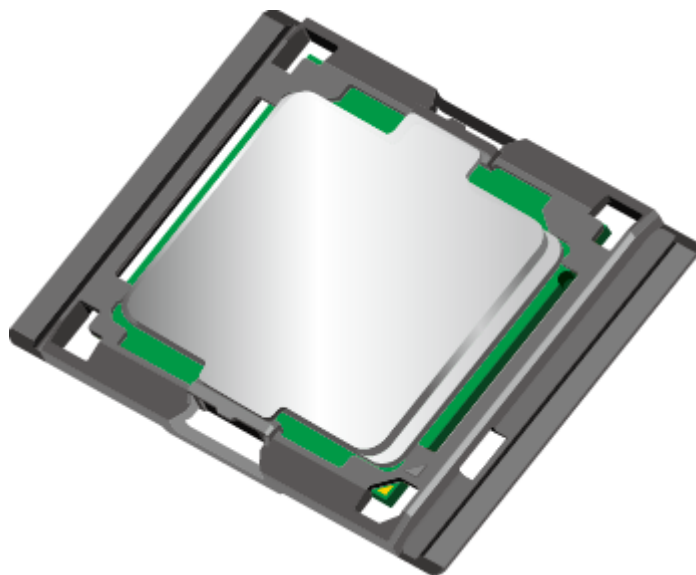
Step 6 Latch the CPU into the other side of the CPU installation tool. See [Figure 5-45](#).

Figure 5-45 Latching a CPU into the other side of a CPU installation tool



Step 7 Ensure that the CPU are properly latched into the two sides of the CPU installation tool. See [Figure 5-46](#).

Figure 5-46 CPU installation tool with the CPU inside



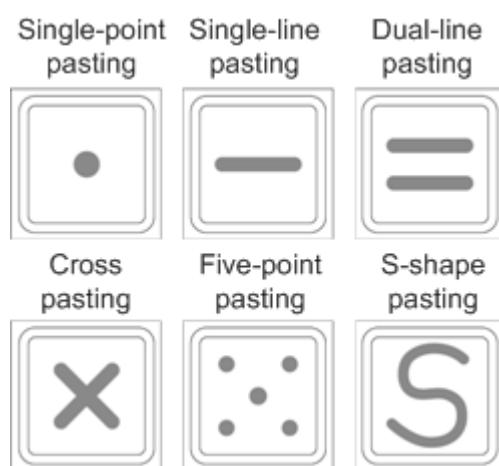
- Step 8** Determine the area on the CPU for contacting the heat sink, and paste 0.4 ml of thermal compound on the area.

 NOTE

The thermal compound injector has volume marks.

You can paste thermal compound using any of the six methods shown in [Figure 5-47](#). Dual-line, five-point, and S-shape, and cross pasting methods are recommended.

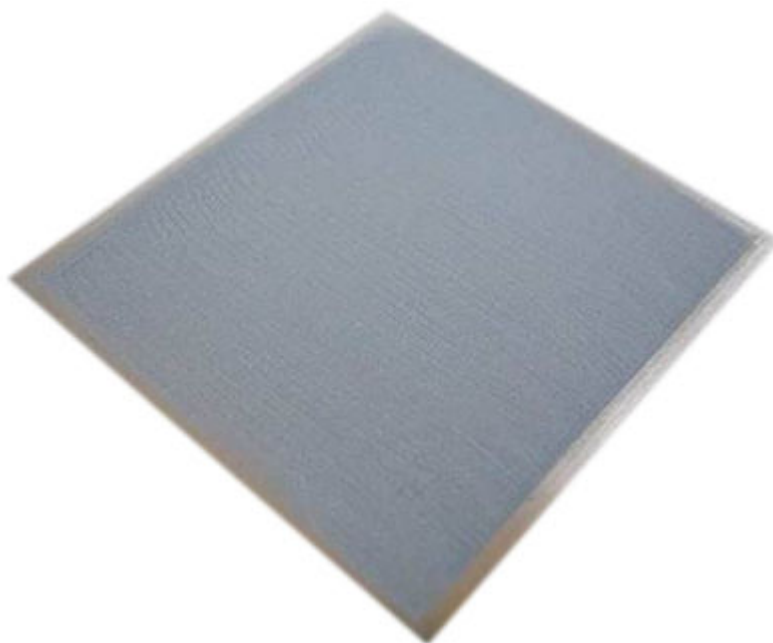
Figure 5-47 Pasting methods



- Step 9** Use a clean card to smear the thermal compound over the entire center of the CPU and ensure that the CPU installation tool is free of thermal compound.

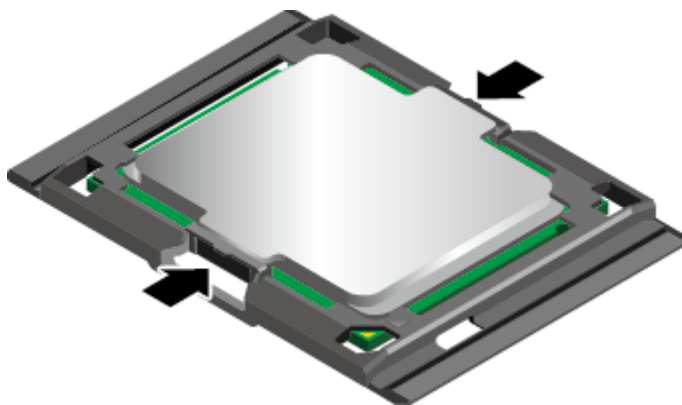
The thermal compound layer is as thick as a common piece of paper. [Figure 5-48](#) shows the smeared thermal grease layer. Ensure that the thermal compound is evenly and fully painted.

Figure 5-48 Smeared thermal compound layer



Step 10 Squeeze two sides of the CPU installation tool and raise the tool with the CPU inside. See [Figure 5-49](#).

Figure 5-49 Raising a CPU installation tool with a CPU inside



Step 11

NOTICE

- To prevent damage to the CPU, CPU socket, or mainboard, ensure that the securing rod on the CPU socket is fully open before you install the CPU in the socket.
 - When you close the securing rod, do not exert excessive force or touch any components and gold pins on the CPU.
 - Do not move the CPU if it is not correctly placed to avoid any twisted pins. Lift the CPU until it is out of the socket, and then place it in the socket properly.
-

Hold the CPU horizontally, align it with the CPU socket, and place the CPU vertically downwards into the socket. See step (1) in [Figure 5-50](#).

Align the triangle mark on the CPU with the triangle mark on the CPU socket to ensure that the CPU is properly installed. [Figure 5-51](#) shows a CPU that is incorrectly placed.

Figure 5-50 Installing a CPU

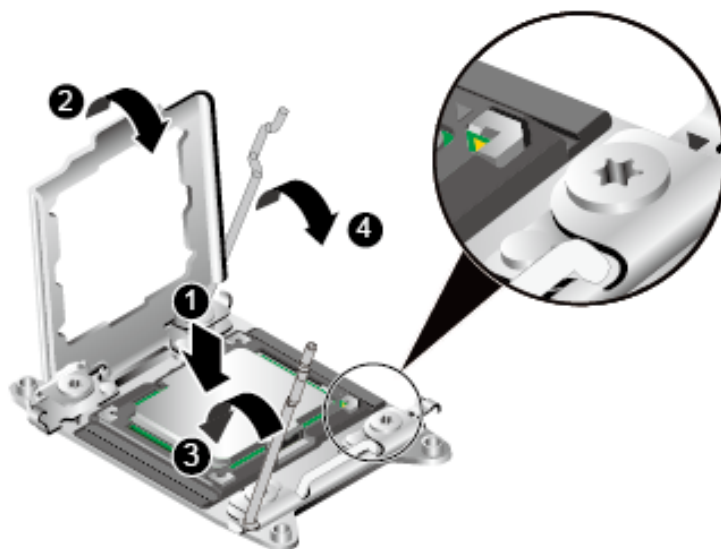
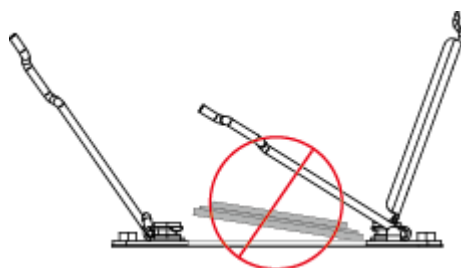


Figure 5-51 Wrong way to place a CPU

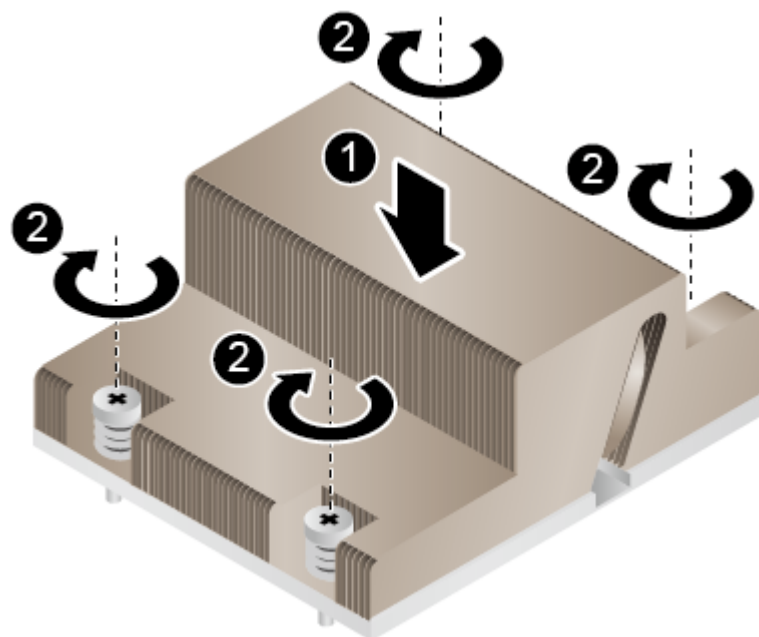


Step 12 Close the cover that secures the CPU. See step (2) in [Figure 5-50](#).

Step 13 Lower the securing rod near the  or  label. See step (3) in [Figure 5-50](#).

Step 14 Lower the securing rod near the  or  label. See step (4) in [Figure 5-50](#).

Step 15 Align the heat sink with the fastening studs on the CPU socket, and place the heat sink on the CPU. See step (1) in [Figure 5-52](#).

Figure 5-52 Installing the heat sink

Step 16 Use the Phillips screwdriver to tighten the four screws securing the heat sink in a diagonal sequence. See step (2) in [Figure 5-52](#).

Step 17 Verification Method.

1. Power on the compute node.
2. In the address bar of Internet Explorer, enter *https://IP address of the iMana 200 management network port*.
3. On the iMana 200 login page, enter the user name and password.
 - **User Name** : Enter the default user name **root**.
 - **Password** : Enter the default password **Huawei12#\$**.
4. Click **Log In**. The **iMana 200** UI appears.
5. Choose **System Information > System Hardware**.
6. Check the CPU information to ensure that the replacement is successful.
 - If the information about the new CPU is displayed, the replacement is successful.
 - If the information about the original CPU is displayed, enter the BIOS, and view the CPU information. For details, see [Huawei Server Brickland Platform BIOS Parameter Reference](#).

----End

5.17 Removing a TPM

You need to remove a Trusted Platform Module (TPM) before replacing it with a new one.

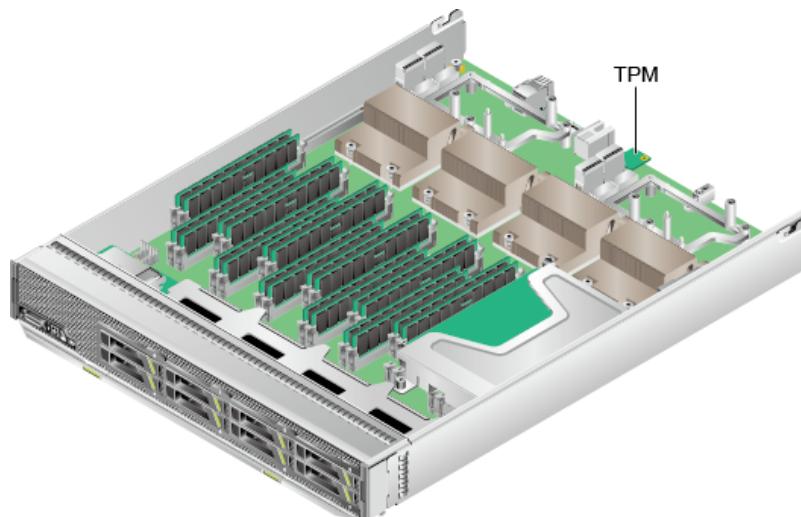
Scenarios

Remove a TPM in any of the following scenarios:

- The TPM is faulty.
- The TPM needs to be replaced with a newer model.

The procedure for removing a TPM on the CH242 V3 8HDD is the same that for removing a TPM on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-53](#) shows the TPM installation position.

Figure 5-53 TPM position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

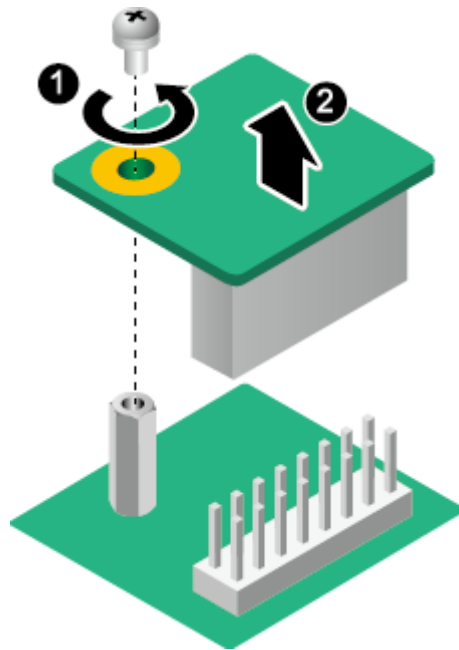
Tools

- Electrostatic discharge (ESD) gloves.
- M3 Phillips screwdriver.
- Packing materials, for example, ESD bag.

Procedure

- Step 1** Use the Phillips screwdriver to remove the screws that secure TPM. See step (1) in [Figure 5-54](#).

Figure 5-54 Removing the TPM



Step 2 Remove the TPM from the mainboard. See step (2) in [Figure 5-54](#).

Step 3 Place the removed TPM in an ESD bag.

----End

5.18 Installing a TPM

You need to install a new Trusted Platform Module (TPM) to replace the original one.

Scenarios

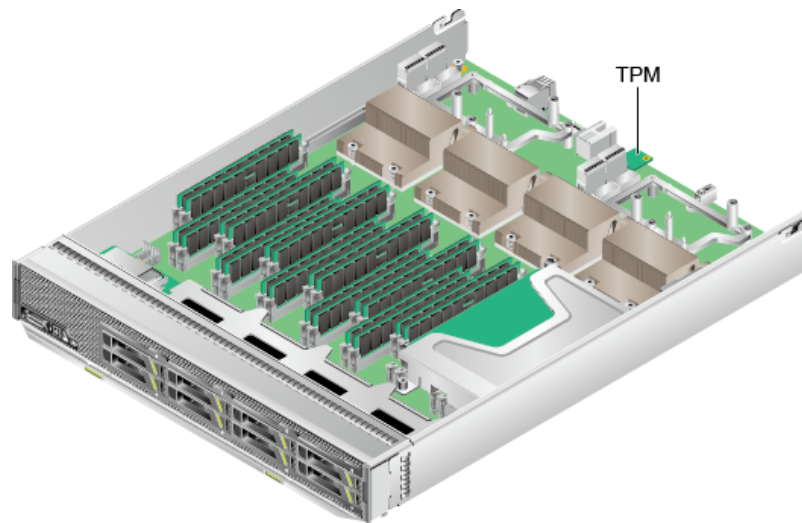
Install a TPM in any of the following scenarios:

- A faulty TPM needs to be replaced.
- A TPM needs to be replaced with another model.

The procedure for installing a TPM on the CH242 V3 8HDD is the same that for installing a TPM on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example.

[Figure 5-55](#) shows the TPM position.

Figure 5-55 TPM position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- M3 phillips screwdriver.

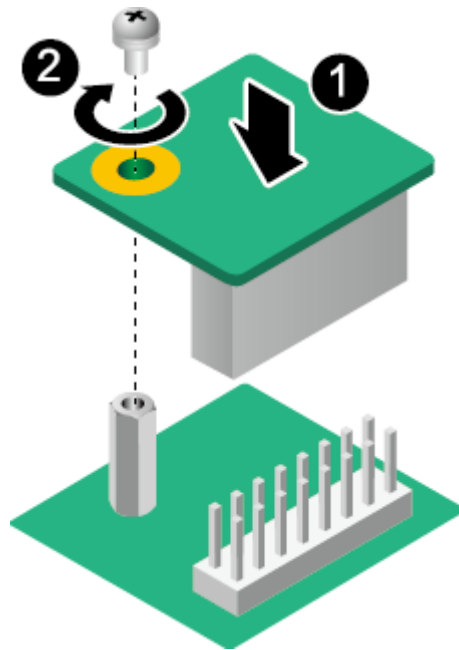
Hardware

Spare TPM.

Procedure

- Step 1** Take the spare TPM out of its ESD bag.
- Step 2** Press the TPM vertically downwards until it seats into the connector on the mainboard. See step (1) in [Figure 5-56](#).

Figure 5-56 Installing the TPM



Step 3 Use the Phillips screwdriver to secure the screws to secure TPM. See step (2) in [Figure 5-56](#).

----End

5.19 Removing the Mezz Modules

You need to remove mezzanine cards before replacing them with new ones.

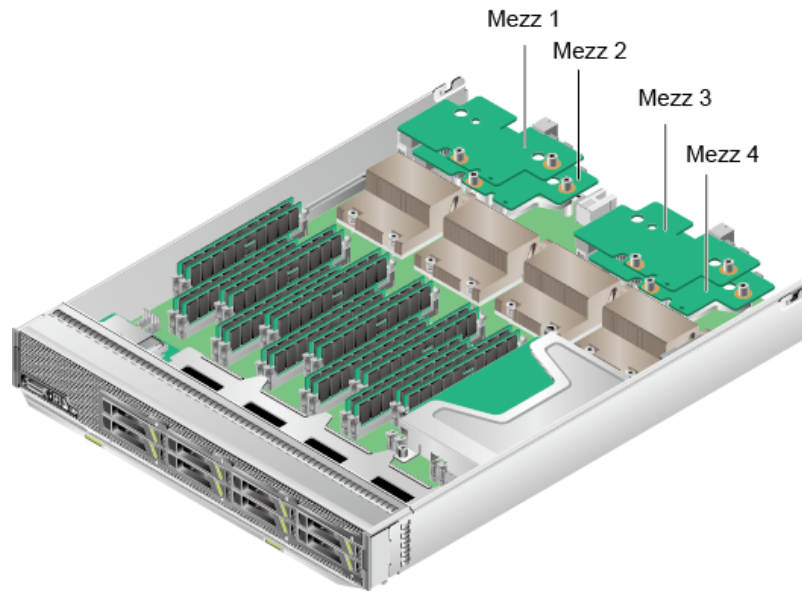
Scenarios

Remove mezzanine cards in any of the following scenarios:

- The mezzanine cards fail.
- The mezzanine cards need to be replaced with a new model.

The procedure for removing a mezz module from the CH242 V3 8HDD is the same that for removing a mezz module from the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-57](#) shows the mezz module installation position and numbers.

Figure 5-57 Positions and numbers of the mezz modules



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- You have recorded the mezzanine card configuration.

 NOTE

- Reboot the server before the operation, please migrate VMs to other hosts in advance to prevent service interruption.
- If the mezzanine card model is the same as the original one (MZ220, MZ510, MZ512, MZ910, or MZ912), and stateless computing configuration is enabled, you do not need to record the mezzanine card configuration.
- If stateless computing configuration is disabled, record the following before removing the mezzanine cards.
 - BIOS configuration, including the UMC (MZ510 or MZ512), PXE (MZ510, MZ512, or MZ910), SR-IOV (MZ510 or MZ512), SAN Boot, iSCSI Boot (MZ510 or MZ512), and iBFT (MZ910). For details about how to query the information, see the BIOS configuration section in the [MZxxx NIC User Guide](#).
 - OS configuration, including IP addresses, VLAN IDs, and NIC bonding configuration.

Query IP addresses as follows: For Windows, check the NIC properties. For VMware, log in, press **ALT+F2**, and perform query on the configuration screen. For Linux, run the **ifconfig -a** command.

For details about how to query VLAN IDs and NIC bonding configuration, see the [MZxxx NIC User Guide](#).
 - Switch configuration (such as the VLAN configuration of Ethernet switches and zoning configuration of FC switches). For details about the query method, see the switch configuration guide.
 - LUN configuration of the FC disk array. For details about the query method, see the FC disk array configuration guide.
 - NIC port numbers. Query method: For Windows, check the Network and Sharing Center. For VMware, run the **esxcli network nic list** command. For Linux, run the **ifconfig -a** command.
 - WWPN of the FC card. If the Windows operating system, you can use the management tool of the FC card to query the WWPN. If the VMware ESXi is used, run the **esxcli storage san fc list** command to query the WWPN. If the Linux (SUSE Linux 10 for example) is used, run the **cat /sys/class/fc_host**/port_name** command to query the WWPN.
 - Bus information of the NIC. You can run the **lspci** command to query the bus information of the NIC. For details, see the [MZxxx NIC User Guide](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

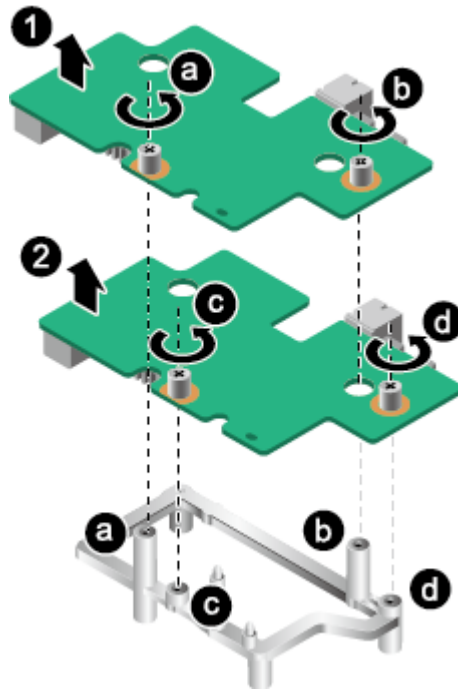
- Electrostatic discharge (ESD) gloves.
- M3 Phillips screwdriver.
- Hex Socket.
- Packing materials, for example, ESD bag.

Procedure

- Step 1** Use the Phillips screwdriver to loosen the two captive screws a and b for the upper mezzanine card, as shown in [Figure 5-58](#).

- Step 2** Pull the upper mezzanine card vertically upwards away from the connector on the mounting base. See step (1) in [Figure 5-58](#).

Figure 5-58 Removing the mezzanine cards



- Step 3** Place the removed mezzanine card in an ESD bag.
- Step 4** Use the Phillips screwdriver to loosen the two captive screws c and d for the lower mezzanine card, as shown in [Figure 5-58](#).
- Step 5** Pull the lower mezzanine card vertically upwards away from the connector on the mounting base. See step (2) in [Figure 5-58](#).
- Step 6** Place the removed mezzanine card in an ESD bag.

----End

5.20 Installing the Mezz Modules

You need to install a new mezzanine card to replace the original one.

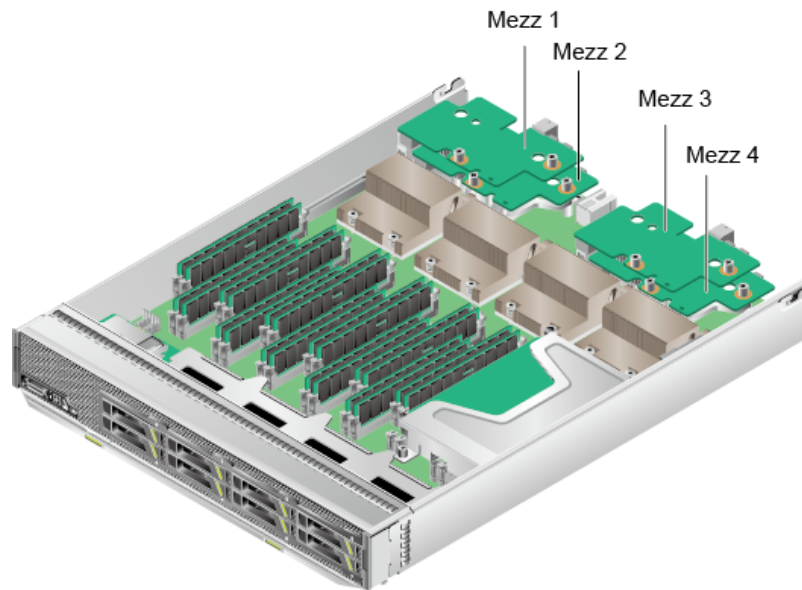
Scenarios

Install a mezzanine card in any of the following scenarios:

- A mezzanine card fails.
- A mezzanine card needs to be replaced with a new model.
- A mezzanine card needs to be added.

The procedure for installing a mezz module on the CH242 V3 8HDD is the same that for installing a mezz module on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-59](#) shows the mezz module positions and numbers.

Figure 5-59 Positions and numbers of the mezz modules



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- M3 phillips screwdriver.

Hardware

Spare mezzanine card.

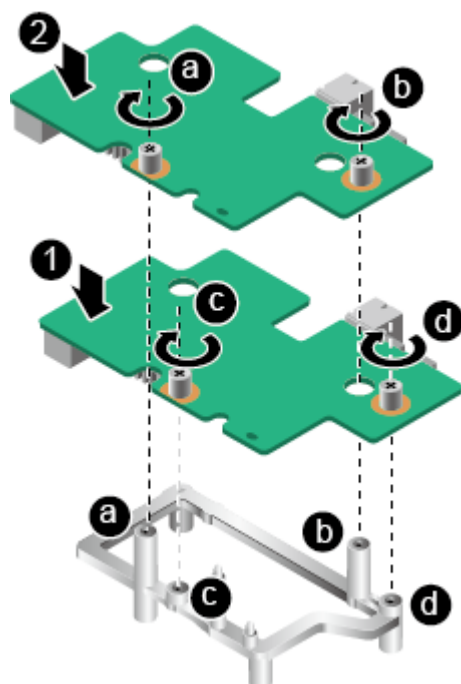
Procedure

NOTE

If the new mezzanine card model is different from the original one, ensure that the new mezzanine card can provide all functions required.

Step 1 Take a spare mezzanine card out of its ESD bag.

Step 2 Align the lower mezzanine card with the positioning holes and metallic studs on the mainboard, and place the mezzanine card vertically downwards into the connector on the mounting base. See step (1) in [Figure 5-60](#).

Figure 5-60 Installing a mezzanine card

- Step 3** Use the Phillips screwdriver to tighten the two captive screws c and d to secure the mezzanine card, as shown in [Figure 5-60](#).
- Step 4** Align the upper mezzanine card with the connector, positioning holes, and metallic studs on the mounting base, and press the mezzanine card vertically downwards until it seats into the connectors on the mainboard. See step (2) in [Figure 5-60](#).
- Step 5** Use the Phillips screwdriver to tighten the two captive screws a and b to secure the mezzanine card, as shown in [Figure 5-60](#).
- Step 6** Verification.
1. Power on the compute node.
 2. In the address bar of Internet Explorer, enter *https://IP address of the iMana 200 management network port*.
 3. On the iMana 200 login page, enter the user name and password.
 - **User Name** : Enter the default user name **root**.
 - **Password** : Enter the default password **Huawei12#\$**.
 4. Click **Log In**. The **iMana 200** UI appears.
 5. Choose **System Information > System Hardware**.
 6. Check the NIC information. If the information about the new NIC is displayed, the replacement is successful.
- Step 7** Follow-up Procedure.
1. Configure the mezzanine card.
 - a. If the mezzanine card is MZ220, MZ510, MZ512, MZ910, or MZ912, and stateless computing configuration is enabled, you do not need to reconfigure the mezzanine card.

 NOTE

Stateless computing does not include network port number settings, so the network port numbers may change after the mezzanine card replacement. For details, see the related operations ([If the mezzanine card port num...](#)) in this topic.

- b. If stateless computing is disabled, manually configure the BIOS, OS, switch, and FC disk array by using the recorded information to ensure consistency between the new and original configuration.

 NOTE

- For details about how to configure the BIOS and OS, see the [MZxxx NIC User Guide](#).
- For details about how to configure the switch, see the switch configuration guide.
- For details about how to configure the FC disk array, see the FC disk array configuration guide.

In addition, check whether the NIC port numbers, MAC addresses, and WWPNs are changed.

 NOTE

- NIC port number query method: For Windows, check the Network and Sharing Center. For VMware, run the **esxcli network nic list** command. For Linux, run the **ifconfig -a** command.
- WWPN of the FC card query method: If the Windows operating system, you can use the management tool of the FC card to query the WWPN. If the VMware ESXi is used, run the **esxcli storage san fc list** command to query the WWPN. If the Linux (SUSE Linux 10 for example) is used, run the **cat /sys/class/fc_host**/port_name** command to query the WWPN.
- If the mezzanine card port numbers, MAC addresses, and WWPNs are consistent with the original ones, no changes are required.
- If the mezzanine card port numbers are different from the original ones, perform the following:
 - IP address configuration: For Windows, set new IP addresses in the mezzanine card properties. For VMware, log in, press **Alt+F2**, and set IP addresses on the configuration screen. For Linux, edit the **/etc/sysconfig/network-scripts/ifcfg-(value)** file to set static IP addresses.
 - For details about how to query VLAN IDs and NIC bonding configuration in the OS, see the [MZxxx NIC User Guide](#).
 - Set port-related information in the user script.
- If the mezzanine card MAC addresses have changed and an Ethernet switch is used with MAC address-based VLAN configuration, modify the VLAN configuration for the switch by referring to the switch configuration guide.
- If the mezzanine card WWPNs have changed and the zoning configuration of FC switches uses WWPNs as zone members, modify the zoning configuration. For details, see the switch configuration guide.
- If the mezzanine card WWPNs have changed, modify related LUN configuration of the FC disk array. For configuration details, see the FC disk array configuration guide.

2. Check the mezzanine card firmware version after the replacement and upgrade the firmware and driver to the latest versions. You can obtain the latest firmware and driver versions from [Huawei Support Website](#).

 NOTE

- You can check the firmware version as follows:
 - If the OS is Linux, VMware ESXi 5.1, or earlier versions, run the **ethtool -i eth <value>** command to check the firmware version. <value> indicates the port number.
 - If the OS is Linux or versions later than VMware ESXi 5.1, run the **esxcli network nic get -n vmnic <value>** command to check the firmware version. <value> indicates the port number.
- For details about how to upgrade the firmware, see the mezzanine card upgrade section in [FusionServer Pro Blade Server Upgrade Guide](#).
- For details about how to upgrade the driver, see the "Software and Firmware Upgrade" section in the [Huawei Server OS Installation Guide](#).

----End

5.21 Removing a microSD Card

You need to remove a microSD card before replacing it with a new one.

Scenarios

Remove a microSD card in either of the following scenarios:

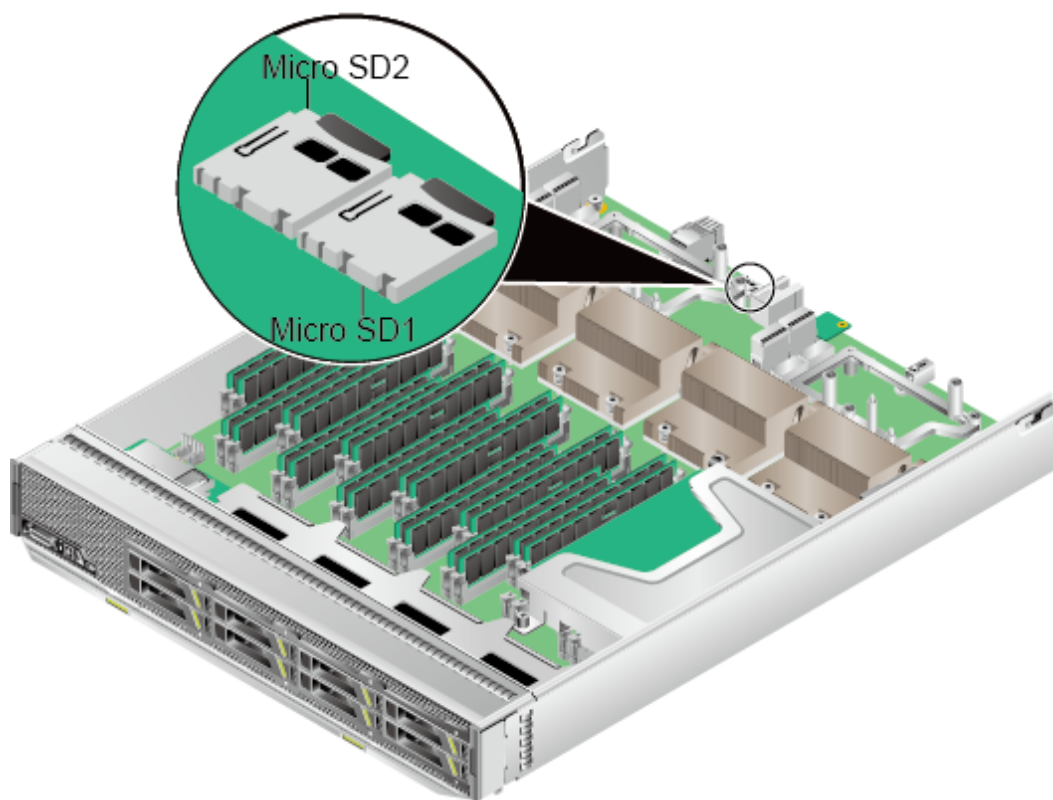
- The microSD card is faulty.
- The microSD card needs to be replaced with a newer model.

 NOTE

For details about how to erase data from a microSD card, see [6.8 Erasing Storage Media Data](#).

The procedure for removing a microSD card on the CH242 V3 8HDD is the same that for removing a microSD card on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-61](#) shows the microSD card installation position and number.

Figure 5-61 Position and number of the microSD card



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

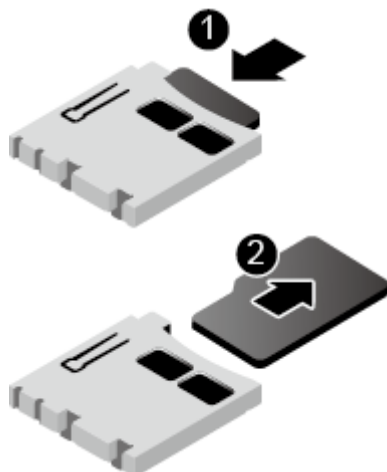
- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, ESD bag.

Procedure

Step 1 Power off the CH242 V3. For details, see [6.7.2 Powering Off the CH242 V3](#).

Step 2 Press the microSD card inwards and then release it. Remove the microSD card after it ejects, as shown in [Figure 5-62](#).

Figure 5-62 Removing the microSD card



Step 3 Place the removed microSD card in an ESD bag.

-----End

5.22 Installing a microSD Card

You need to install a microSD card to replace the original one.

Scenarios

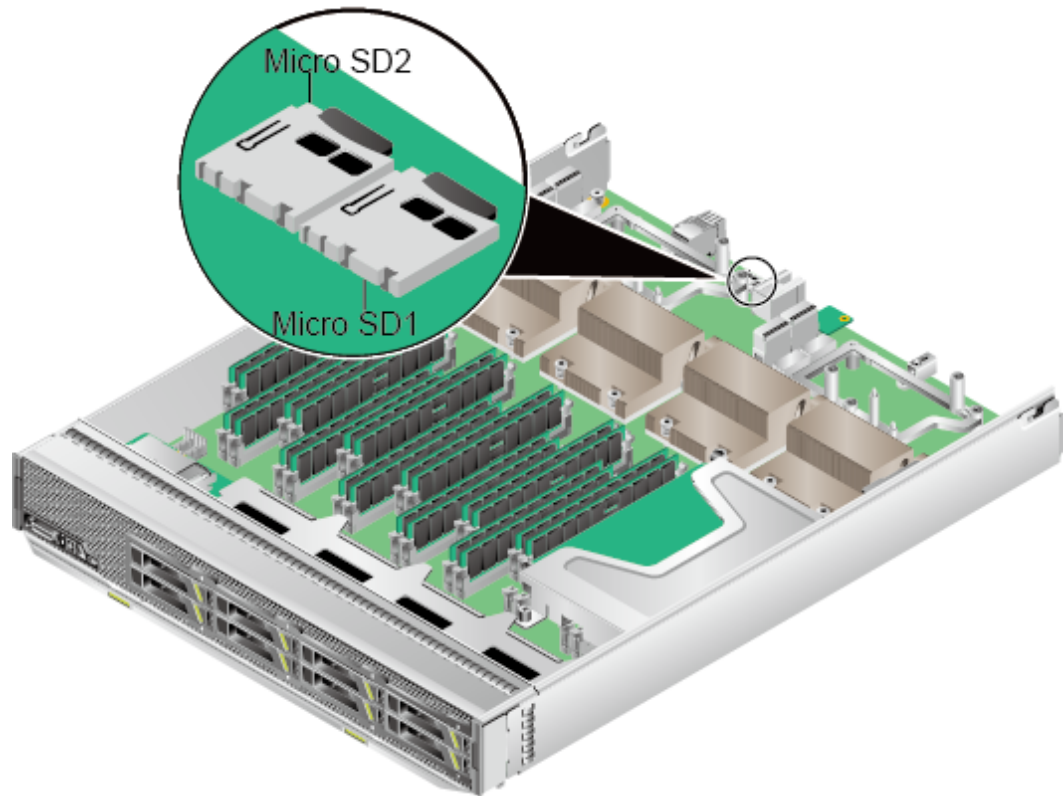
Install a microSD card in any of the following scenarios:

- Replace a faulty microSD card.
- If the microSD card is removed from another blade server, ensure that the microSD card is inserted into the correct slot.

The procedure for installing a microSD card on the CH242 V3 8HDD is the same that for installing a microSD card on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example.

[Figure 5-63](#) shows the microSD card installation position and number.

Figure 5-63 Position and number of the microSD card



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.
- The microSD card of the compute node has been removed. For details, see [5.21 Removing a microSD Card](#).

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, an ESD bag.

Hardware

Spare microSD card.

NOTICE

The spare microSD card cannot contain any data. To view or delete partitions or data on the card, follow the instructions provided in scenario 2 or 3 in [6.8 Erasing Storage Media Data](#).

Procedure

Step 1 Determine the position of the microSD card to be replaced, as shown in [Figure 5-63](#).

NOTE

Install microSD cards based on actual situation.

- If the server is not installed with microSD cards, install microSD cards when the server is powered off.
- If the server is configured with only one microSD card, migrate the important data on the microSD card to another storage device before replacing the microSD card. If the microSD card is faulty, power off the server and replace the microSD card when the server is powered off. If the microSD card is installed with the OS, install the OS on the newly installed microSD card.
- If the server has two microSD cards and only one microSD card is faulty, replace the faulty microSD card when the server is powered off.
- If the server has two microSD cards and both of them are faulty, replace the microSD cards when the server is powered off. If the OS is installed on a microSD card, migrate the important data on the microSD card to another storage device before replacing the microSD card. After replacing the microSD card, reinstall the OS.

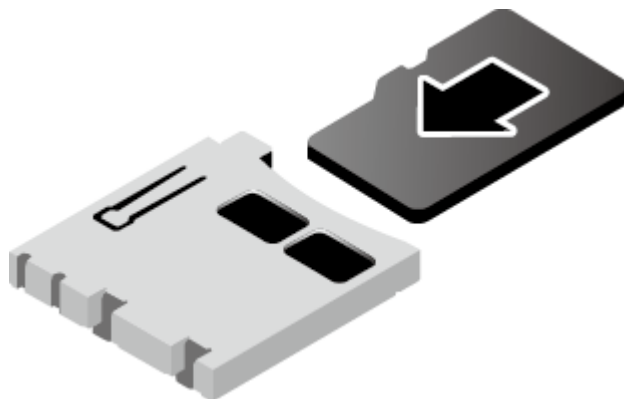
Step 2 Take the spare microSD card out of its ESD bag.

Step 3 Insert the microSD card into the slot until it does not move, as shown in [Figure 5-64](#).

NOTICE

If the server has two microSD cards, install the new microSD cards in the same slots as the replaced ones.

Figure 5-64 Installing a microSD card



Step 4 Check the microSD card status.

- Log in to the iBMC WebUI, choose **Information > System Info**, select the **Other Devices** tab, and check the microSD card status. For details, see the [FusionServer Pro E9000 Server iBMC User Guide](#).

- If one of the two microSD cards is replaced, view the iBMC event log information to check whether the microSD card rebuild is complete.

In the iBMC event log, "Data rebuild starts at SD card *N*" is logged after the server is powered on. *N* indicates the microSD card slot No. "Data rebuild stops at SD card *N*" indicates the microSD card rebuild is complete.

If the microSD card is in abnormal status, contact Huawei technical support.

----End

5.23 Removing an iBBU

You need to remove an intelligent backup battery unit (iBBU) before replacing it with a new one.

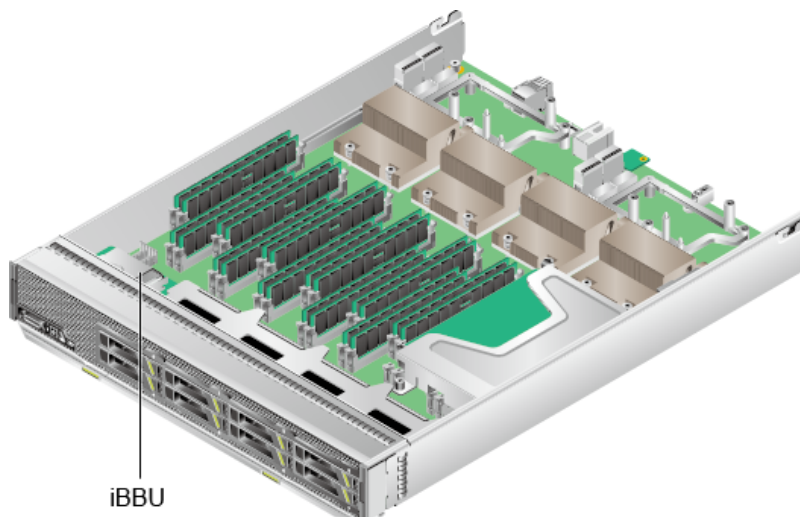
Scenarios

Remove an iBBU in any of the following scenarios:

- The iBBU is faulty.
- The iBBU power is used up.

The procedure for removing an iBBU from the CH242 V3 8HDD is the same that for removing an iBBU from the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-65](#) shows the iBBU position.

Figure 5-65 iBBU position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- Packing materials, for example, ESD bags.

Procedure

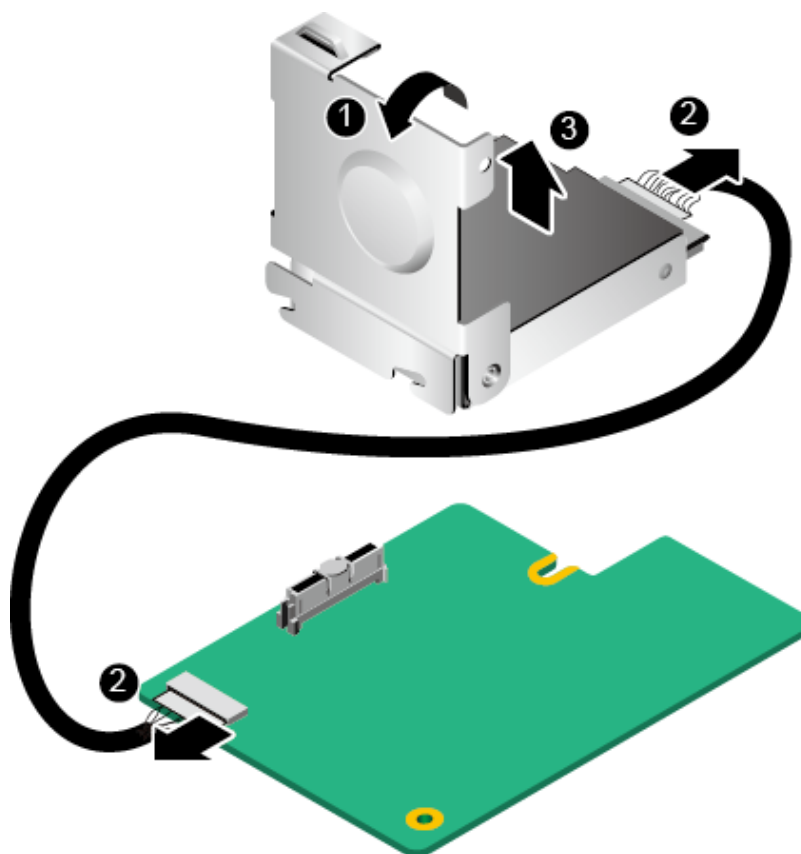
Step 1 Pull the iBBU box out horizontally. See step (1) in [Figure 5-66](#).

Figure 5-66 Removing an iBBU box



Step 2 Lift the iBBU box away from mainboard. See step (2) in [Figure 5-66](#).

Step 3 Open the cover of the iBBU box. See step (1) in [Figure 5-67](#).

Figure 5-67 Removing an iBBU

Step 4 Remove the cable for the iBBU from the cable connector of the RAID controller card. See step (2) in [Figure 5-67](#).

Step 5 Take out the iBBU. See step (3) in [Figure 5-67](#).

Step 6 Place the removed iBBU in an ESD bag.

----End

5.24 Installing an iBBU

You need to install an intelligent backup battery unit (iBBU) to replace the original one.

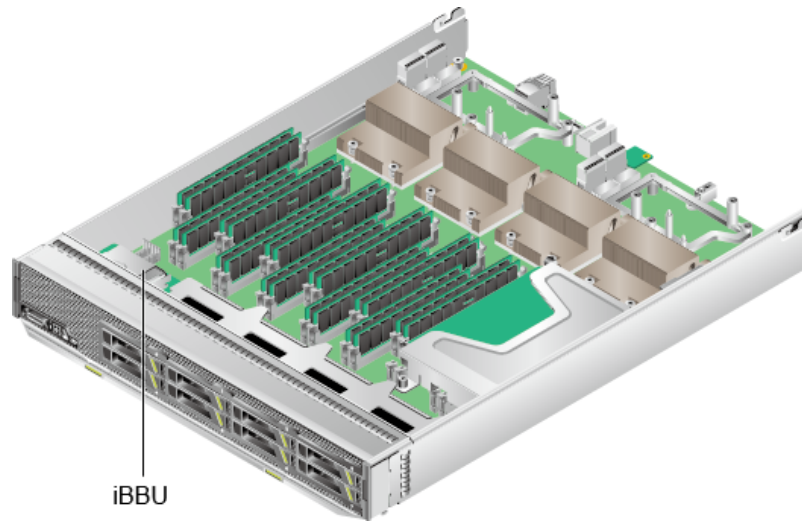
Scenarios

Install an iBBU in any of the following scenarios:

- The iBBU is faulty.
- An iBBU of a new model needs to be used.

The procedure for installing an iBBU on the CH242 V3 8HDD is the same that for installing an iBBU on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-68](#) shows the iBBU position.

Figure 5-68 iBBU position



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

Tools

Electrostatic discharge (ESD) gloves.

Hardware

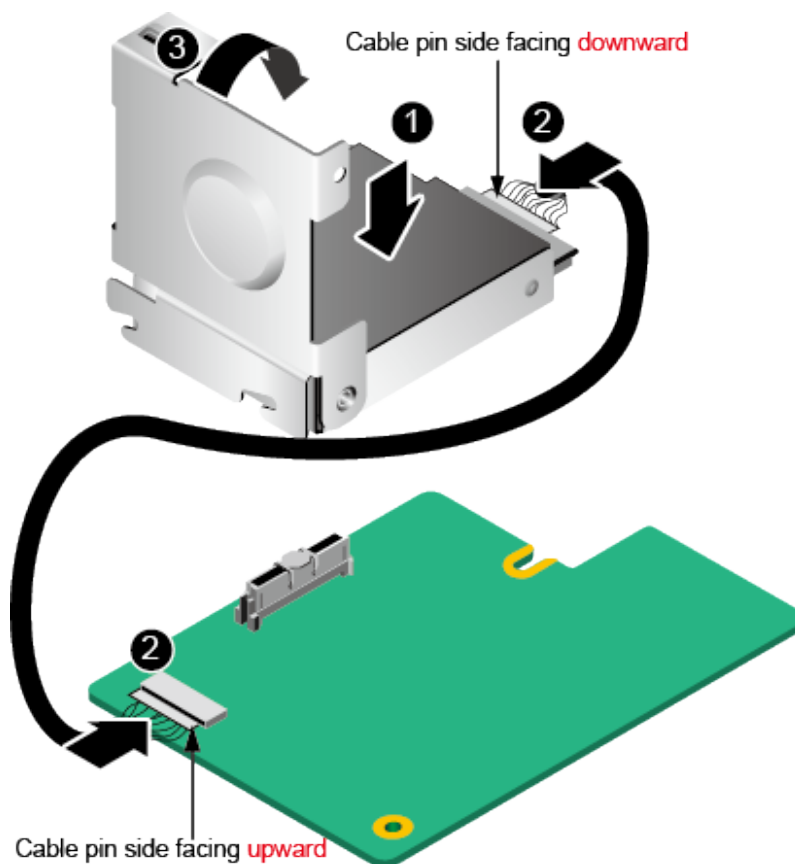
New iBBU.

Procedure

Step 1 Take the new iBBU out of its ESD bag.

Step 2 Put the iBBU into the iBBU box. See step (1) in [Figure 5-69](#).

Figure 5-69 Installing an iBBU



Step 3 Install the cable for the iBBU to the cable connector of the RAID controller card. See step (2) in [Figure 5-69](#).

Step 4 Close the iBBU box cover. See step (3) in [Figure 5-69](#).

Step 5 Put the iBBU box above the compute node. See step (1) in [Figure 5-70](#).

Figure 5-70 Installing an iBBU box



Step 6 Insert the iBBU box horizontally until it is secured into the fastener. See step (2) in [Figure 5-70](#).

----End

5.25 Removing a RAID Controller Card

You need to remove a redundant array of independent disks (RAID) controller card before replacing it with a new one.

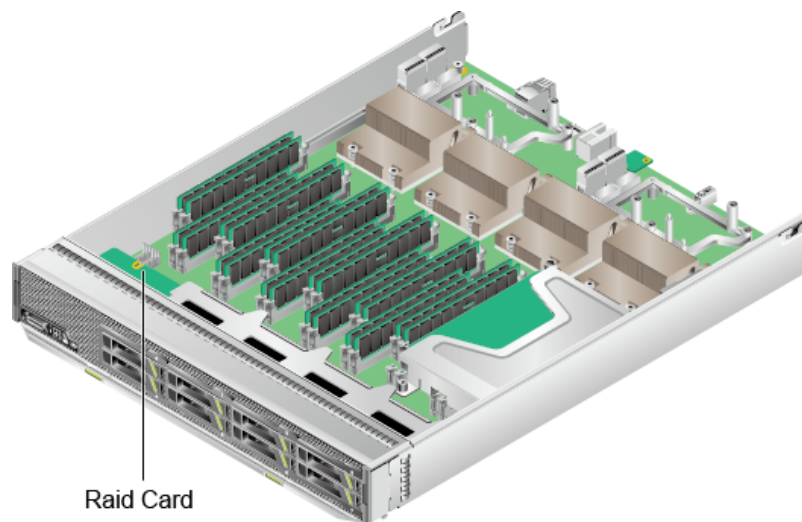
Scenarios

Remove a RAID controller card in any of the following scenarios:

- The RAID controller card is faulty.
- The RAID controller card needs to be replaced by a newer model.

The procedure for removing a RAID controller card from the CH242 V3 8HDD is the same that for removing a RAID controller card from the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-71](#) shows the RAID controller card installation position.

Figure 5-71 Position of the RAID controller card



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- You have confirmed the RAID controller card model. For details, see [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.

Data

Data preparation is not required for this operation.

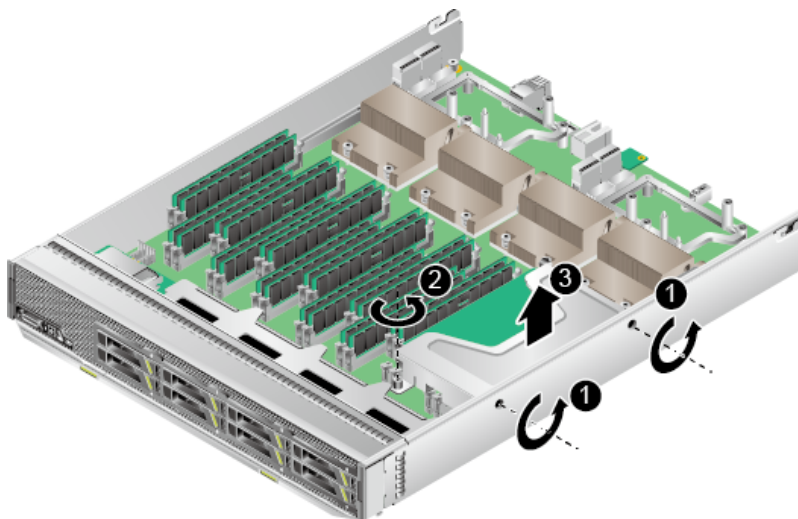
Tools

- Electrostatic discharge (ESD) gloves.
- M3 Phillips screwdriver.
- Hex socket.
- Packaging materials, for example, an ESD bag.

Procedure

- Step 1** Check whether the mainboard is equipped with PCIe cards on the left and right sides.
- If yes, go to [Step 2](#).
 - If no, go to [Step 5](#).
- Step 2** Use the Phillips screwdriver to loosen the two screws on two sides. See step (1) in [Figure 5-72](#).

Figure 5-72 Removing the PCIe card tray

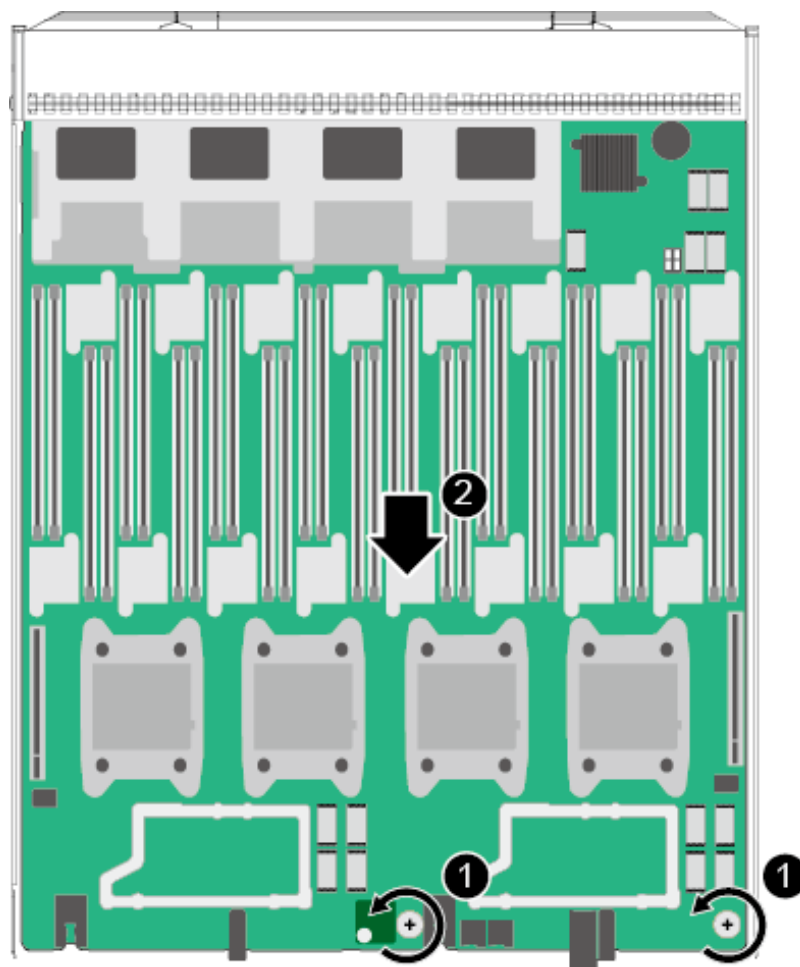


- Step 3** Use a Phillips screwdriver to loosen the captive screws. See step (2) in [Figure 5-72](#).
- Step 4** Remove the PCIe card tray. See step (3) in [Figure 5-72](#).
- Step 5** Use the Phillips screwdriver to remove the two captive screws on the CH242 V3 mainboard. See step (1) in [Figure 5-73](#).

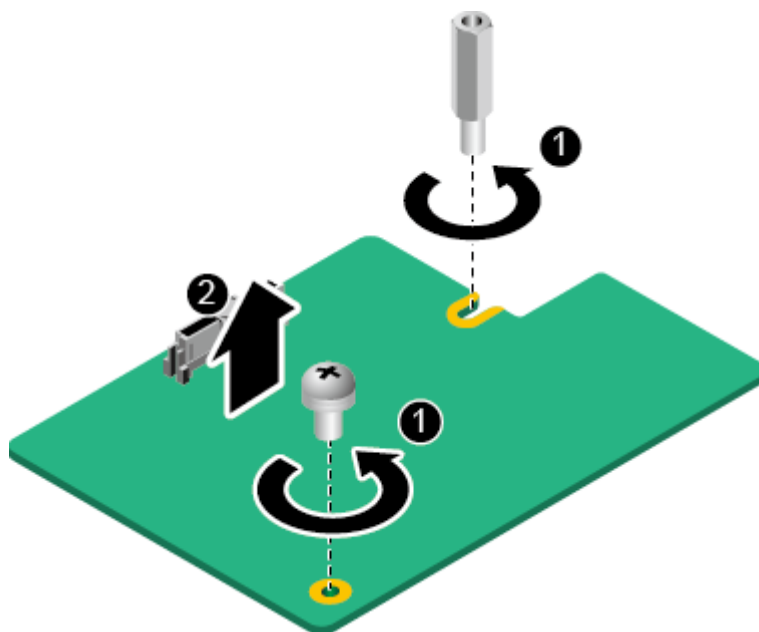
NOTICE

Only personnel authorized by Huawei and Huawei technical support personnel can remove the compute node mainboard.

Figure 5-73 Removing the mainboard



- Step 6** Pull the CH242 V3 mainboard 1 cm out from the chassis in the direction shown in step (2) in [Figure 5-73](#), lift the mainboard 6 mm up, and then pull out one fourth of the mainboard.
- Step 7** Use a Phillips screwdriver to remove the screws that secure the RAID controller card, and use a hex socket to remove the hex bolts. See step (1) in [Figure 5-74](#).

Figure 5-74 Removing the RAID controller card

Step 8 Lift the RAID controller card away from the connector on the mainboard. See step (2) in [Figure 5-74](#).

Step 9 Place the removed RAID controller card in an ESD bag.

----End

5.26 Installing a RAID Controller Card

You need to install a new redundant array of independent disks (RAID) controller card to replace the original one.

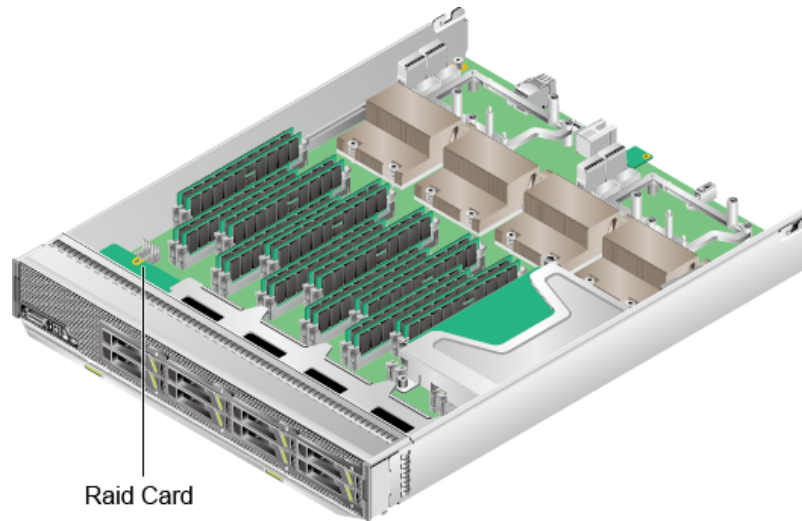
Scenarios

Install a RAID controller card in any of the following scenarios:

- A faulty RAID controller card needs to be replaced.
- A RAID controller card of a newer model needs to be used.

The procedure for installing a RAID controller card on the CH242 V3 8HDD is the same that for installing a RAID controller card on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-75](#) shows the RAID controller card installation position.

Figure 5-75 Position of the RAID controller card



Prerequisites

Conditions

- Refer to [1 Safety Instructions](#).
- You have confirmed the RAID controller card model. For details, see [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) floor.
- The CH242 V3 mainboard has been removed or pulled out. For details, see [5.25 Removing a RAID Controller Card](#).

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) gloves.
- M3 Phillips screwdriver.
- Hex socket.
- Packaging materials, for example, an ESD bag.

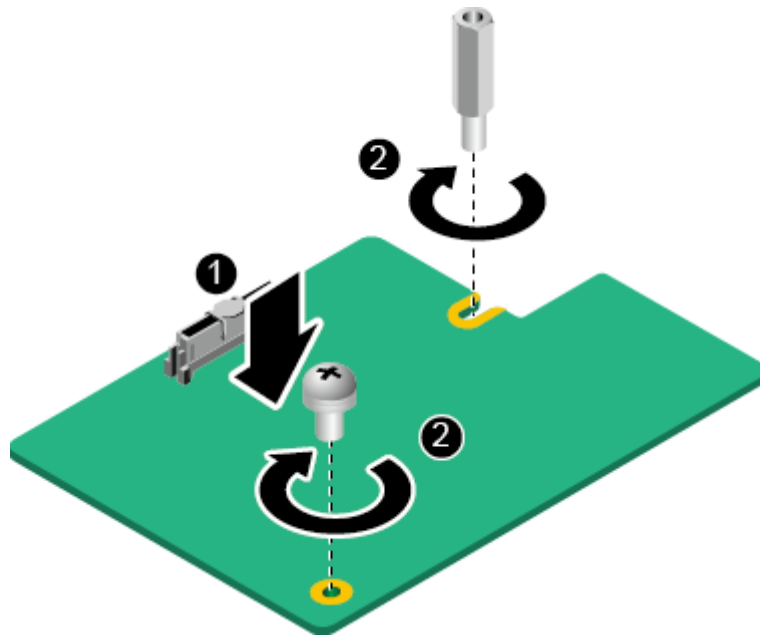
Hardware

Spare RAID controller card.

Procedure

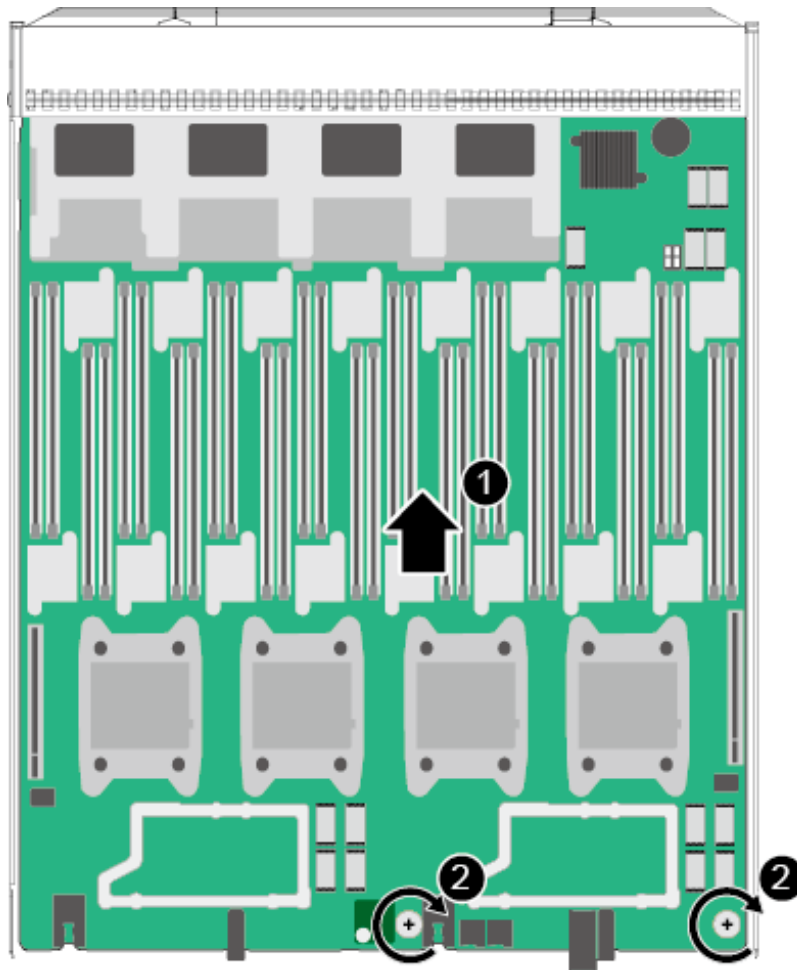
- Step 1** Take the spare RAID controller card out of the ESD bag.
- Step 2** Press the RAID controller card vertically downwards until it seats into the connector on the mainboard. See step (1) in [Figure 5-76](#).

Figure 5-76 Installing the RAID controller card



- Step 3** Use the Phillips screwdriver to tighten the screws to secure the RAID controller card, and use a hex socket to tighten the hex bolts. See step (2) in [Figure 5-76](#).
- Step 4** Push the CH242 V3 mainboard to the tray. See step (1) in [Figure 5-77](#).
- Step 5** Use a Phillips screwdriver to tighten the two captive screws on the CH242 V3 mainboard. See step (2) in [Figure 5-77](#).

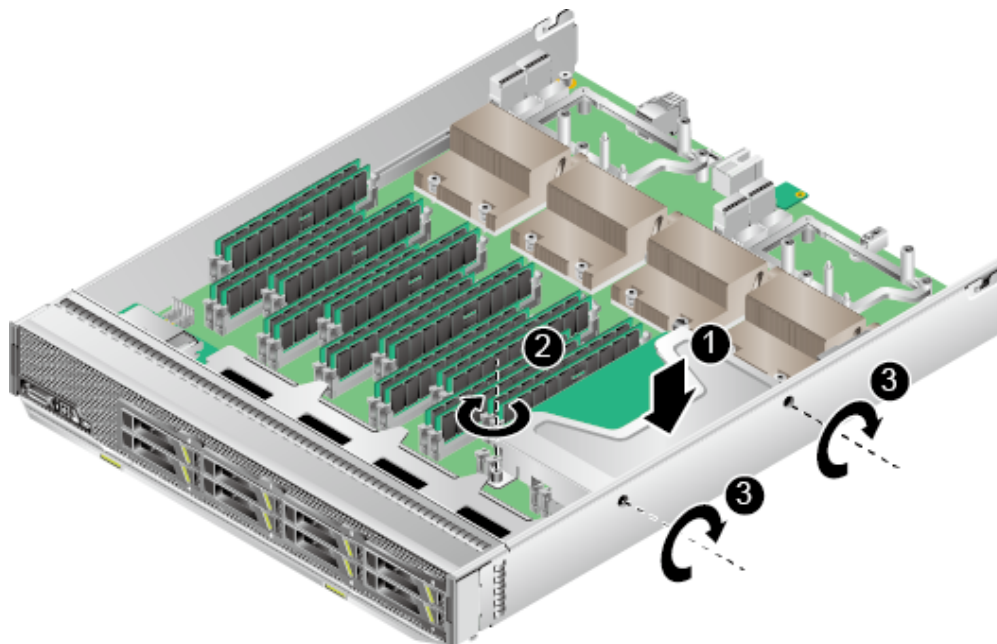
Figure 5-77 Installing a mainboard



Step 6 Check whether the mainboard is equipped with PCIe cards on the left and right sides.

- If yes, go to [Step 7](#).
- If no, no further action is required.

Step 7 Place the PCIe card tray on the compute node. See step (1) in [Figure 5-78](#).

Figure 5-78 Installing the PCIe card tray

Step 8 Use a Phillips screwdriver to tighten the captive screws that secure the PCIe card tray. See step (2) in [Figure 5-78](#).

Step 9 Use the Phillips screwdriver to tighten the two screws on two sides. See step (3) in [Figure 5-78](#).

Step 10 Follow-up Procedure.

Configure a RAID controller card.

- For an LSI SAS2208 or LSI SAS3108 RAID controller card, the procedure is as follows:

Log in to the management screen. For details, see [LSI SAS2208 > Initial Configuration > Logging In to the WebBIOS](#) or [LSI SAS3108 RAID Controller Card > Initial Configuration > Logging In to the WebBIOS](#) in [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

Import external configuration. For details, see [LSI SAS2208 > Common Tasks > Importing Foreign Configurations](#) or [LSI SAS3108 RAID Controller Card > Common Tasks > Importing or Deleting Foreign Configurations](#) in [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

- For an LSI SAS2308 or LSI SAS3008 RAID controller card, the procedure is as follows:

Log in to the CU screen. For details, see [LSI SAS2308 > Initial Configuration > Logging In to the WebBIOS](#) or [LSI SAS3008 RAID Controller Card > Initial Configuration > Logging In to the WebBIOS](#) in [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

Activate RAID configuration. For details, see [LSI SAS2308 > Common Tasks > Activating RAID Configuration](#) or [LSI SAS3008 RAID Controller Card > Common Tasks > Activating RAID Configuration](#) in [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

----End

5.27 Removing a BIOS Battery

If a BIOS battery is faulty or is low in power, remove it before replacing it with a new one.

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.

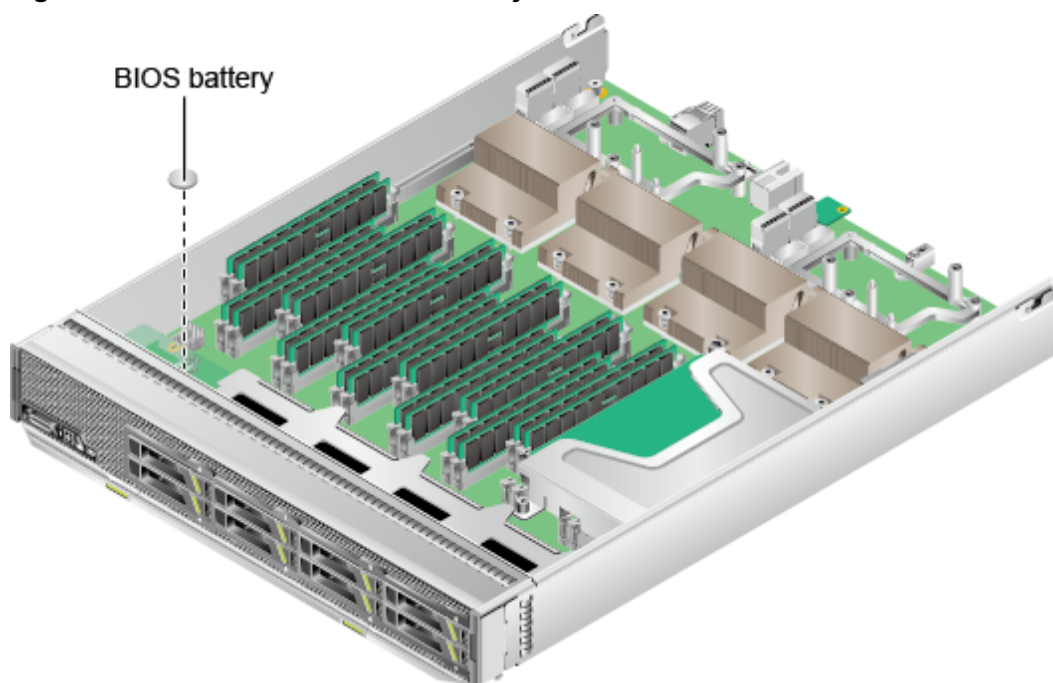
Scenarios

Remove a BIOS battery in either of the following scenarios:

- A faulty BIOS battery is removed.
- A BIOS battery that is low in power is removed.

The procedure for removing a BIOS battery on the CH242 V3 8HDD is the same that for removing a BIOS battery on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-79](#) shows the position of the BIOS battery.

Figure 5-79 Position of the BIOS battery



Prerequisites

Conditions

- For details, see [1 Safety Instructions](#).
- You have removed the compute node cover. For details, see [5.5 Removing the Cover](#).

Data

This operation requires no data preparation.

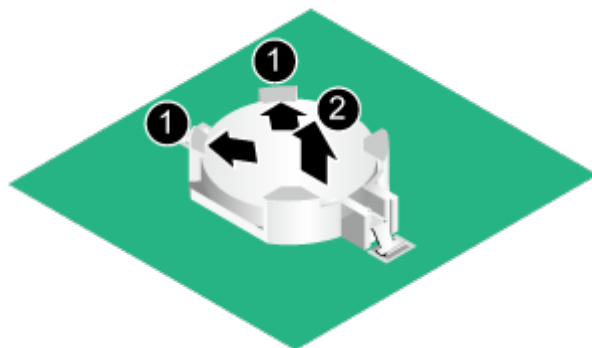
Tools

- Electrostatic discharge (ESD) gloves
- M3 Phillips screwdriver
- Hex socket
- Packaging materials, for example, an ESD bag

Procedure

- Step 1** (Optional) Remove the iBBU if it has been installed. For details, see [5.23 Removing an iBBU](#).
- Step 2** Remove all RAID controller cards. For details, see [5.25 Removing a RAID Controller Card](#).
- Step 3** Press the two latches in the directions shown by (1) in [Figure 5-80](#) until one end of the BIOS battery ejects. Then remove the entire battery from the slot, as shown by (2) in [Figure 5-80](#).

Figure 5-80 Removing a BIOS battery



- Step 4** Place the removed BIOS battery in an ESD bag.

-----End

5.28 Installing a BIOS Battery

After removing a BIOS battery that is faulty or low in power, install a new one.

CAUTION

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

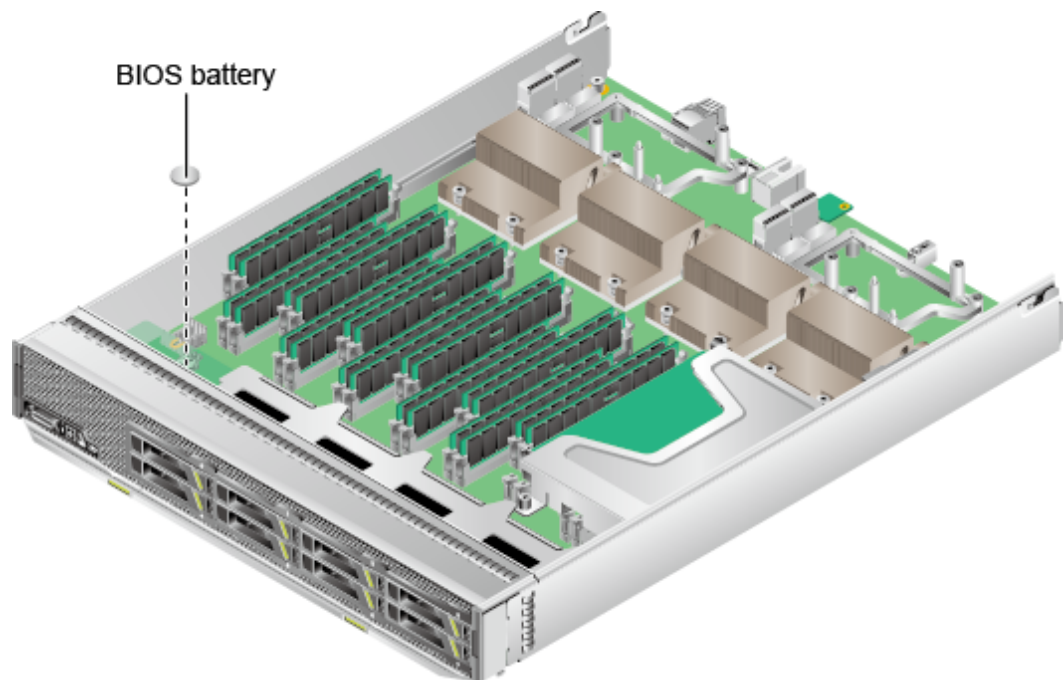
Scenarios

Install a BIOS battery in either of the following scenarios:

- A faulty BIOS battery is removed.
- A BIOS battery that is low in power is removed.

The procedure for removing a BIOS battery on the CH242 V3 8HDD is the same that for removing a BIOS battery on the CH242 V3 4HDD. The following uses the CH242 V3 8HDD as an example. [Figure 5-81](#) shows the position of the BIOS battery.

Figure 5-81 Position of the BIOS battery



Prerequisites

Conditions

- For details, see [1 Safety Instructions](#).
- You have removed the compute node cover. For details, see [5.5 Removing the Cover](#).

Data

This operation requires no data preparation.

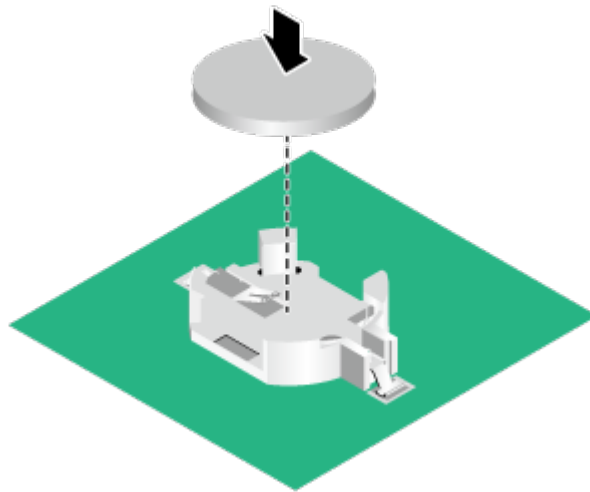
Tools

- Electrostatic discharge (ESD) gloves
- M3 Phillips screwdriver
- Hex socket
- Packaging materials, for example, an ESD bag

Procedure

- Step 1** Take a BIOS battery out of its ESD bag.
- Step 2** Hold the battery with the side marked with text facing upwards, insert the left end of the battery into the slot, and gently press down the battery until it is properly installed in the slot. See [Figure 5-82](#).

Figure 5-82 Installing a BIOS battery



- Step 3** Install the RAID controller card. For details, see [5.26 Installing a RAID Controller Card](#).
- Step 4** (Optional) Install the iBBU. For details, see [5.24 Installing an iBBU](#).
- End

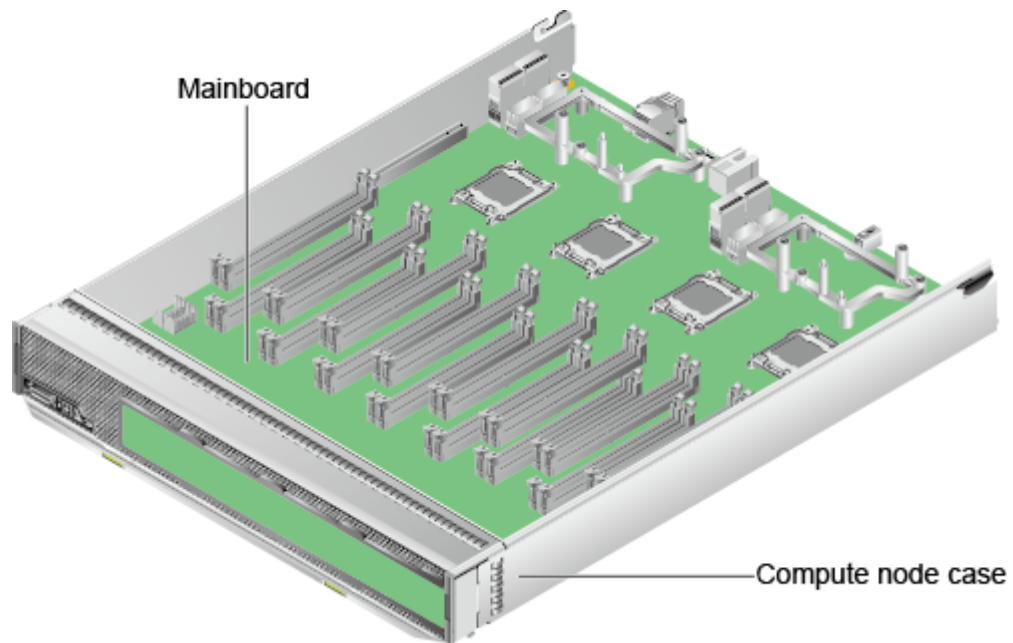
5.29 Removing the Mainboard and Compute Node Case

This topic describes how to remove a mainboard and compute node case.

Scenarios

Remove all components of the faulty mainboard.

Figure 5-83 Positions of the mainboard and the compute node case



NOTE

Replace the mainboard and compute node case together.

Prerequisites

Conditions

- You have read [1 Safety Instructions](#).
- If the mainboard needs to be replaced, record the following information:
 - Record the version numbers of the iMana 200, BIOS, and CPLD. For details, see [4.3 Checking the CH242 V3](#).
 - Record the BIOS configuration if it is customized.
 - Record the compute node IP address and iMana 200 configurations.

NOTE

iMana 200 configurations may involve the iMana firmware version, alarms, power control, local users, LDAP, networks, services, system, boot options, SSL certificates, and remote control. For details about how to query the configurations, see [E9000 Server V100R001 iMana 200 User Guide](#).

- If a compute node is installed in the E9000 chassis, remove it by referring to [3.2 Removing a CH242 V3](#).
- Place the compute node carefully on an electrostatic discharge (ESD) surface.

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) wrist strap.

- M3 Phillips screwdriver.
- Hex socket.
- Packing materials, for example, ESD bag.

Procedure

- Step 1** Removing a Hard Disk. For details, see [5.1 Removing a Hard Disk](#) and [5.3 Removing a PCIe SSD Disk \(8HDD\)](#).
- Step 2** Removing the Cover. For details, see [5.5 Removing the Cover](#).
- Step 3** Removing PCIe cards on the left and right sides of the mainboard. For details, see [5.7 Removing a PCIe Card \(Riser Card Slots 1 and 2\)](#).
- Step 4** Removing a DIMM and an Air Duct. For details, see [5.11 Removing a DIMM and an Air Duct](#).
- Step 5** Removing a USB Flash Drive. For details, see [5.13 Removing a USB Flash Drive](#).
- Step 6** Removing a CPU and heat sink. For details, see [5.15 Removing a CPU](#).
- Step 7** Removing a TPM. For details, see [5.17 Removing a TPM](#).
- Step 8** Removing the Mezzanine Cards. For details, see [5.19 Removing the Mezz Modules](#).
- Step 9** Removing a microSD Card. For details, see [5.21 Removing a microSD Card](#).
- Step 10** Removing a PCIe Card at the hard disk backplane. For details, see [5.9 Removing a PCIe Card \(Hard Disk Backplane\)](#).
- Step 11** Removing an iBBU. For details, see [5.23 Removing an iBBU](#).
- Step 12** Removing a RAID Controller Card. For details, see [5.25 Removing a RAID Controller Card](#).
- Step 13** Place the removed mainboard and compute node case in an ESD bag.

NOTICE

Before placing the mainboard into an ESD bag, check that a protective cover is installed on a vacant CPU socket. For details about how to install a protective cover, see [5.15 Removing a CPU](#).

----End

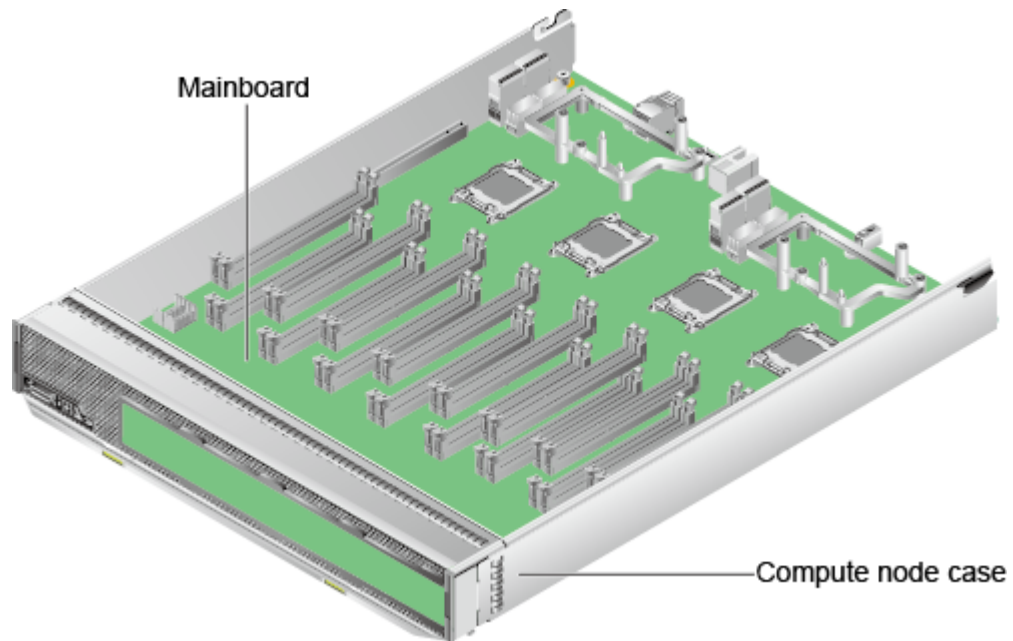
5.30 Installing the Mainboard and Compute Node Case

This topic describes how to install a new mainboard and compute node case.

Scenarios

Install all components of the original mainboard on the new mainboard.

Figure 5-84 Positions of the mainboard and the compute node case



NOTE

Replace the mainboard and compute node case together.

Prerequisites

Conditions

- You have read [1 Safety Instructions](#).
- Place the compute node carefully on an electrostatic discharge (ESD) surface.

Data

Data preparation is not required for this operation.

Tools

- Electrostatic discharge (ESD) wrist strap.
- M3 Phillips screwdriver.
- Hex socket.
- Packing materials, for example, ESD bag.

Hardware

Spare mainboard and compute node case.

Procedure

- Step 1** Take the new mainboard and compute node case out of the ESD bag.
- Step 2** (Optional) Installing a RAID Controller Card. For details, see [5.26 Installing a RAID Controller Card](#).

- Step 3** (Optional) Installing an iBBU. For details, see [5.24 Installing an iBBU](#).
- Step 4** (Optional) Installing a PCIe Card at the hard disk backplane. For details, see [5.10 Installing a PCIe Card \(Hard Disk Backplane\)](#).
- Step 5** (Optional) Installing a USB Flash Drive. For details, see [5.14 Installing a USB Flash Drive](#).
- Step 6** (Required) Installing a CPU and heat sink. For details, see [5.16 Installing a CPU](#).
- Step 7** (Optional) Installing a TPM. For details, see [5.18 Installing a TPM](#).
- Step 8** (Required) Installing the Mezz Cards. For details, see [5.20 Installing the Mezz Modules](#).
- Step 9** (Optional) Installing a microSD Card. For details, see [5.22 Installing a microSD Card](#).
- Step 10** (Required) Installing a DIMM and an Air Duct. For details, see [5.12 Installing a DIMM and an Air Duct](#).
- Step 11** (Optional) Installing PCIe cards on the left and right sides of the mainboard. For details, see [5.8 Installing a PCIe Card \(Riser Card Slots 1 and 2\)](#).
- Step 12** (Required) Installing the Cover. For details, see [5.6 Installing the Cover](#).
- Step 13** (Required) Installing a Hard Disk. For details, see [5.2 Installing a Hard Disk](#) and [5.4 Installing a PCIe SSD Disk \(8HDD\)](#).
- Step 14** After installation, power on the compute node and check the indicator status.
For details, see [Table 2-1](#).
- Step 15** 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 16** Configure the CH242 V3. For details, see [4 Configuring the CH242 V3](#).

 NOTE

- If the mainboard is replaced, the iMana 200 and BIOS configurations will be restored to default settings. You need to reconfigure the iMana 200 and BIOS. For details about the default user name, password, and IP address of the compute node, see [4.2 Default Information](#).
- Configure the mainboard IP address and iMana 200 based on the recorded information. For details, see [E9000 Server V100R001 iMana 200 User Guide](#).
- Upgrade the iMana 200, BIOS, and CPLD to the versions used before the replacement or to the latest versions. The versions used before the replacement are recommended. For details about the upgrade methods, see [FusionServer Pro Blade Server Upgrade Guide](#).
- If the BIOS configuration before the mainboard replacement was customized, customize the BIOS configuration as it was.

----End

6 Common Operations

This topic describes the common operations related to the CH242 V3. The common operations include logging in to the CH242 V3 by using the PuTTY, reconfiguring the redundant array of independent disks (RAID), and powering on and powering off the CH242 V3.

[6.1 Logging In to a Compute Node or a Switch Module over MM910 SOL](#)

[6.2 Logging In to the MM910 CLI Over a Network Port by Using PuTTY](#)

[6.3 Logging In to a Device Over a Serial Port by Using PuTTY](#)

[6.4 Performing Operations by Using the Local KVM Connected to the MM910](#)

[6.5 Logging in to the MM910 WebUI](#)

[6.6 Reconfiguring the RAID](#)

[6.7 Powering On and Off the CH242 V3](#)

[6.8 Erasing Storage Media Data](#)

6.1 Logging In to a Compute Node or a Switch Module over MM910 SOL

Scenarios

Log in to a compute node or a switch module by using the serial over LAN (SOL) function provided by the MM910.

Prerequisites

Conditions

None.

Data

- User name and password for logging in to the MM910.
Default user name: **root**; default password: **Huawei12#\$**.

- User name and password for logging in to the compute nodes to be connected.
Default user name: **root**; default password: **Huawei12#\$**.
- Password for logging in to the switch modules to be connected.
Default password: **Huawei12#\$**.

Procedure

Step 1 Log in to the MM910 CLI by using PuTTY and the floating IP address of the MM910.

For details about how to use PuTTY, see [6.2 Logging In to the MM910 CLI Over a Network Port by Using PuTTY](#).

Step 2 Log in to the SOL CLI.

telnet 0 1101

The command output is as follows:

```
*=====*
```

```
*      Welcome to SMM SOL Server      *
```

```
*      Please log in with SMM account and password.      *
```

```
*=====*
```

user name:

Step 3 Enter the user name and password.

The following information is displayed:

```
Log in Success!
```

```
*=====*
```

```
=====
```

```
      please input the SOL Blade1~Blade16(1 ~ 16), Blade1A~Blade16A(17 ~ 32), Swi1~Swi4(33 ~ 36) and
```

```
COM#(n)
```

```
      press Ctrl+R to return
```

```
*=====*
```

```
=====
```



```
Blade1~Blade16(1 ~ 16)
```

```
Blade1A~Blade16A(17 ~ 32)
```

```
Swi1~Swi4(33 ~ 36)
```

```
Please input your choice:
```

In the information displayed:

- The numbers **1** to **32** indicate the compute nodes in slots 1 to 32 respectively.
- The numbers **33** to **36** indicate the switch modules in slots 1E, 2X, 3X, and 4E respectively.

Step 4 Enter the slot number of the compute node or switch module, and press **Enter**.

- The screen for selecting the serial port is displayed.
 - If you enter the slot number of a compute node, the serial port types supported by the compute node are displayed:
Example:

- **systemcom**: serial port for accessing the OS.
 - **RAIDcom**: serial port for accessing the RAID. Only CH222 and CH222 V3 compute nodes have this serial port.
 - **BMCcom**: serial port for accessing the BMC.
 - **Exboardcom**: serial port for accessing the expansion board. Only CH222 and CH222 V3 compute nodes have this serial port.
 - **SYS COM**: serial port for accessing the OS.
 - **BMC COM**: serial port for accessing the BMC.
- If you enter the slot number of a switch module, the serial port types supported by the switch module are displayed.

Example:

- **BMCcom**: serial port for accessing the BMC.
 - **fabriccom**: serial port for accessing an Ethernet switching plane.
 - **basecom**: reserved and currently disabled.
 - **basecom**: serial port for accessing the CX920 10GE switching plane (available only when connected to the CH121H V3)
 - **FCcom**: serial port for accessing the Fibre Channel (FC) switching plane or Fibre Channel over Ethernet (FCoE) gateway.
 - **bmccom**: serial port for accessing the BMC.
- If an SOL connection has been connected through the serial port, a message will be displayed asking you whether to forcibly disconnect the existing SOL connection.

```
=====
user name:root
PassWord:
Log in Success!
=====
please input the SOL Blade1-Blade16(1 ~ 16), Blade1A-Blade16A(17 ~ 32), Sw
il-Swi4(33 ~ 36) and COM#(n)
press Ctrl+R to return
=====
Blade1-Blade16(1 ~ 16)
Blade1A-Blade16A(17 ~ 32)
Swil-Swi4(33 ~ 36)
Please input your choice:34
Have same connect!
Whether to forcibly exit an existing SOL connection that the other user created.
(Y|N):
```

- Press **Y** to forcibly disconnect the existing SOL connection.
- Press **N** to not disconnect the existing SOL connection. The system stays at the current screen.

Step 5 Enter the number of a serial port, and press **Enter**.

- The serial port CLI is displayed. On this CLI, you can perform operations such as configuring the serial port and querying parameters of the serial port.

- If another user has logged in to the serial port, a message will be displayed asking you whether to forcibly log out the user.

```
-----
You are forcibly logged out by other users,
Please try again later.
-----

Blade1-Blade16(1 ~ 16)
Blade1A-Blade16A(17 ~ 32)
Sw1-Sw16(33 ~ 36)
Please input your choice:34
1 fabriccom
2 hmccom
3 basecom

COM#(1 ~ 3):2
Have same connect!

Whether to forcibly exit an existing SOL connection that the other user created.
(Y/N):y
```

- Press **Y** to forcibly log out the user.
- Press **N** to not forcibly log out the user. The system stays at the current screen.

NOTE

- Only one serial port connection can be set up at a time. Exit the SOL interface after the operation.
- You can press **Ctrl+R** to return to the CLI for selecting a slot in the chassis, as shown in [6.1 Logging In to a Compute Node or a Switch Module over MM910 SOL](#). And you can press **Ctrl+R** twice to log out of the SOL CLI.

----End

6.2 Logging In to the MM910 CLI Over a Network Port by Using PuTTY

Scenarios

Use PuTTY to log in to the MM910 command line interface (CLI) through a network port.

NOTE

The compute nodes and switch modules of the E9000 do not provide the MGMT management port. To log in to a compute node or switch module, see [6.1 Logging In to a Compute Node or a Switch Module over MM910 SOL](#).

Prerequisites

Conditions

The local PC is connected to the MGMT port on the management module using a network cable.

Data

- IP address for logging in to the management module
- User name and password for logging in to the management module

Software

PuTTY, a third-party tool

Procedure

- Step 1** Set an IP address and a subnet mask or add route information for the PC to enable communication between the PC and the management module.

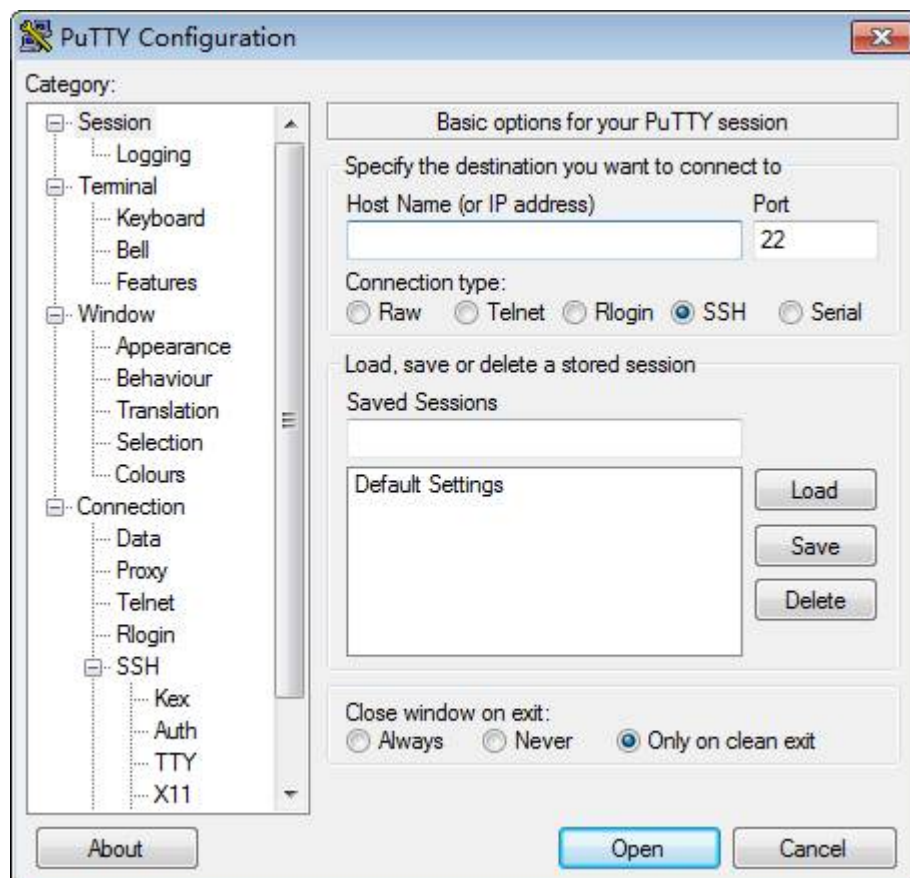
To check whether the network connection is normal, perform the following steps:

1. Run the **cmd** command on the CLI of the PC.
2. Run the **Ping management module IP address** command to check whether the management module can be pinged successfully.

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

The **PuTTY Configuration** window is displayed, as shown in [Figure 6-1](#).

Figure 6-1 PuTTY Configuration



- Step 3** In the navigation tree on the left, choose **Session**.

- Step 4** Set login parameters.

The following is an example:

- **Host Name (or IP address):** Enter the IP address of the management module to be logged in to, for example, **191.100.34.32**.

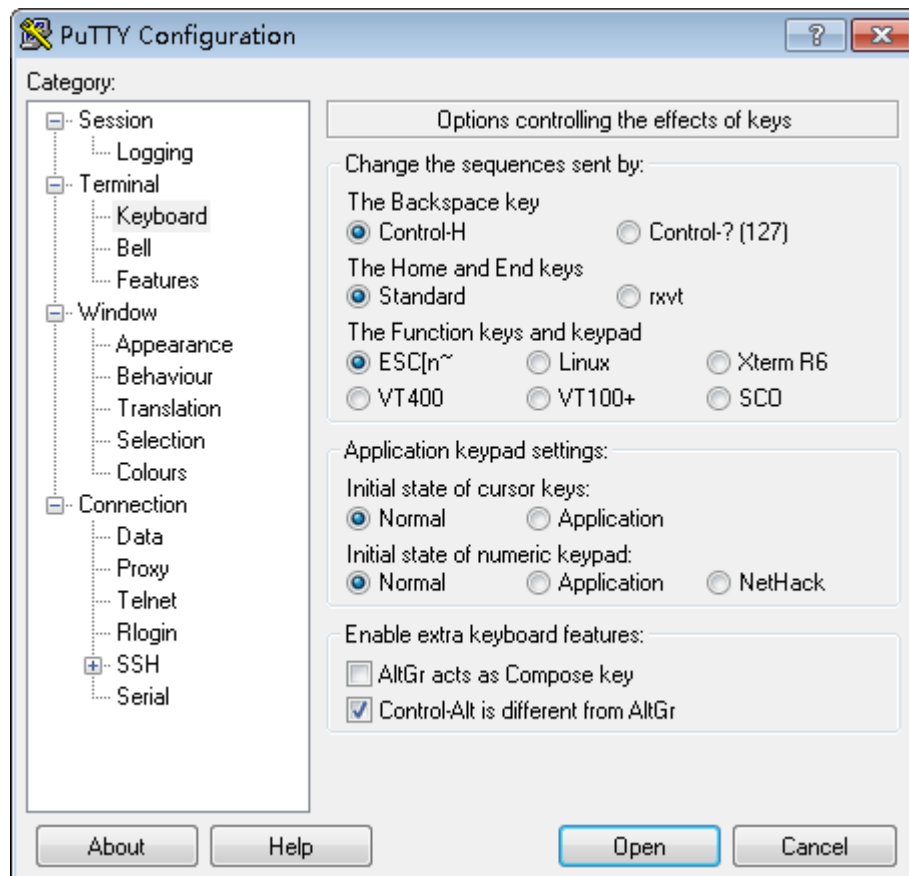
- **Port:** Retain the default value **22**.
- **Connection type:** Retain the default value **SSH**.
- **Close window on exit:** Retain the default value **Only on clean exit**.

 NOTE

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

Step 5 (Optional) After you log in to the Ethernet switching plane using PuTTY, if the characters entered in the command line cannot be deleted by using the backspace key (Backspace), choose **Terminal > Keyboard** in the navigation tree, set **The Backspace key** to **Control-H**, and retain the default values for other parameters, as shown in [Figure 6-2](#).

Figure 6-2 PuTTY Configuration



Step 6 Click **Open**.

The PuTTY window is displayed, and the following information is displayed:

login as:

 NOTE

- If this is your first login to the device, 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 7 Enter the user name and password.

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

----End

6.3 Logging In to a Device Over a Serial Port by Using PuTTY

Scenarios

Log in to a compute node, switch module, or management module in an E9000 chassis over a serial port by using PuTTY when:

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

NOTE

The device that is logged in to is a management module, compute node, or switch module in an E9000 chassis.

When logging in to a management module, you must connect the serial port to the COM serial port of the MM910.

When logging in to a compute node, you can connect the serial port to the SYS serial port or BMC chip of the compute node.

- The E9000 compute nodes do not provide serial ports. To log in to a compute node over a serial port, connect a multi-port cable to a universal connector port (UCP) and log in through the serial port of the multi-port cable. If the compute node does not provide a UCP, you can log in to the compute node only through a network port. For details, see [6.1 Logging In to a Compute Node or a Switch Module over MM910 SOL](#).
- On the MM910 CLI, run the **bmccomstate** and **switchcom** commands to query and switch the objects connected to the serial ports. For details, see the [MM910 Management Module V100R001 Command Reference](#).

When logging in to a switch module, you can connect the serial port to the Ethernet switching plane, FC switching plane, or BMC chip.

- If the switch module panel has the BMC serial port and SYS serial port, the BMC serial port is connected to the BMC chip, and the SYS serial port can be connected to the Ethernet switching plane or FC switching plane.
- If the switch module panel has only the COM serial port, the COM serial port can be connected to the Ethernet switching plane, FC switching plane, or BMC chip.
- If the switch module panel has only the BMC serial port, the BMC serial port is connected to the BMC chip.
- On the MM910 CLI, run the **bmccomstate** and **switchcom** commands to query and switch the objects connected to the serial ports. For details, see the [MM910 Management Module V100R001 Command Reference](#).

Prerequisites

Conditions

- If you need to access a management module, the client is connected to the COM port on the management module through a serial cable.

- If you need to access a compute node, the client is connected to the serial port of the multi-port cable connected to the compute node.
- If you need to access a switch module, the client is connected to the serial port of the switch module through a serial cable.
- PuTTY 0.60 or later has been installed.

Data

User name and password for logging in to the device.

Software

PuTTY 0.60 or later

Procedure

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

The **PuTTY Configuration** window is displayed.

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

Step 3 Set the login parameters.

The following is an example:

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

NOTE

n indicates the serial port number.

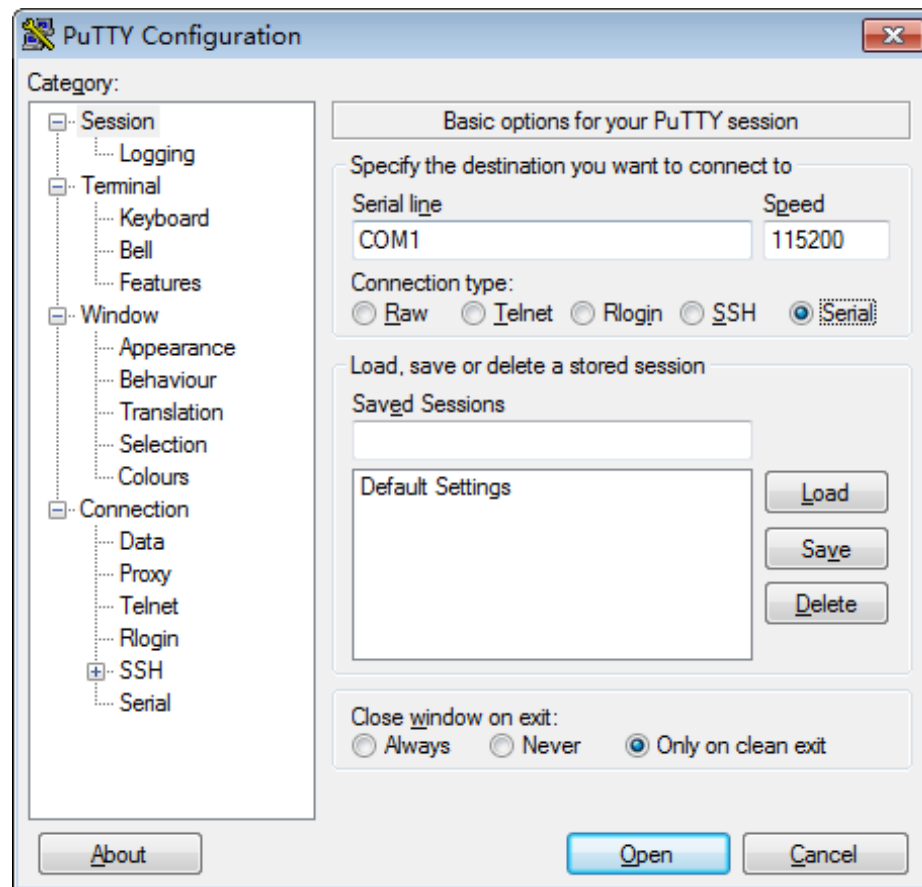
Step 4 Choose **Session** from the navigation tree.

Step 5 Select **Serial** for **Connection type**, and **Close window on exit** is set to **Only on clean exit** by default, as shown in [Figure 6-3](#).

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 6-3 PuTTY Configuration



Step 6 Click **Open**.

The PuTTY window is displayed, and the following information is displayed:

login as:

Step 7 Enter the user name and password as prompted.

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

----End

6.4 Performing Operations by Using the Local KVM Connected to the MM910

Scenarios

Use the local keyboard, video, and mouse (KVM) to perform any of the following operations:

- Log in to the MM910 command-line interface (CLI).
- Log in to the OS of a compute node.
- Mount the DVD-ROM drive to a compute node.
- Access a compute node or switch module over serial over LAN (SOL).

The local KVM function of the MM910 has the following restrictions:

- The CLI does not provide the text editor function.
- The login to the system serial port of the compute node over SOL by using the local KVM is supported.

NOTE

For security purposes, run the **exit** command to exit the CLI when you do not need to use the KVM. Once you have accessed the CLI of the active or standby MM910 or SOL screen (shown in [Figure 6-4](#)) and the timeout timer has not expired, you can access the MM910 without entering the user name and password again.

Prerequisites

Conditions

You have logged in to the MM910 CLI.

Data

- User name and password for logging in to the MM910.
- User name and password for logging in to the compute node or switch module.

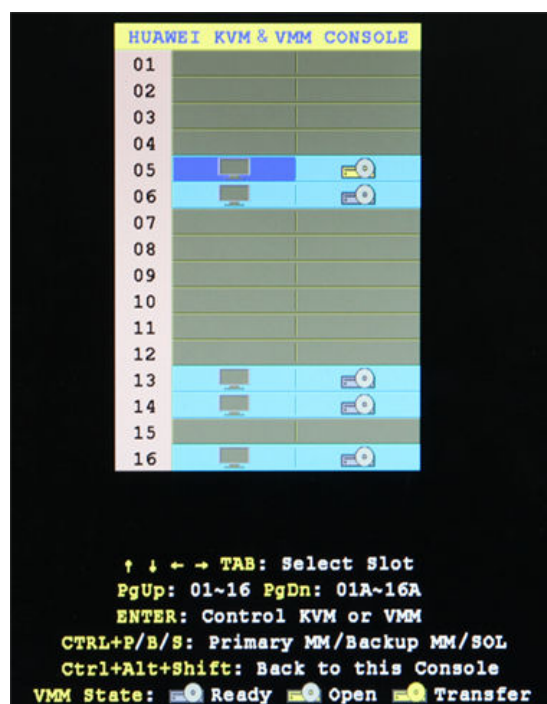
Procedure

Step 1 Connect the keyboard and mouse to the USB ports of the MM910.

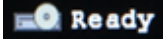
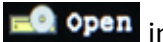
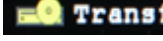
Step 2 Use a VGA cable to connect the monitor to the VGA port of the MM910.

The main screen is displayed, as shown in [Figure 6-4](#).

Figure 6-4 KVM main screen



On the main screen:

- Press ↑, ↓, ←, or → to select , and press **Enter** to enter the OS of the compute node in the specified slot.
- Press ↑, ↓, ←, or → to select , and press **Enter** to mount the CD-ROM drive of the MM910 to the compute node in the specified slot. The CD-ROM drive color of the MM910 represents the status of the connection to the compute node.
 -  indicates that the CD-ROM drive is mounted to the compute node.
 -  indicates that the CD-ROM drive is open.
 -  indicates that data is being accessed.

Step 3 Perform operations on the menu as prompted. For example, press **Ctrl+S**.

Go to the SOL CLI. The following information is displayed:

```
*=====*
*      Welcome to SMM SOL Server      *
*      Please log in with SMM account and password.      *
*=====*

user name:
```

 NOTE

To go to the previous screen, press **Ctrl+Shift+Alt**. To go to the KVM main screen, press **Ctrl+R**.

Step 4 Enter the MM910 user name and password.

The CLI for selecting a slot is displayed.

```
Log in Success!

*=====*
*      please input the SOL Blade1~Blade16(1 ~ 16), Blade1A~Blade16A(17 ~ 32), Swi1~Swi4(33 ~ 36) and COM#(n)      *
*      press Ctrl+R to return      *
*=====*

Blade1~Blade16(1 ~ 16)
Blade1A~Blade16A(17 ~ 32)
Swi1~Swi4(33 ~ 36)
Please input your choice:
```

The sequence numbers in the preceding information are described as follows:

- 1-32 indicate the compute nodes in slots 1 to 32 respectively.
- 33-36 indicate the switch modules in slots 1E, 2X, 3X, and 4E respectively.

Step 5 Enter the slot number of the compute node or switch module to be connected. For example, enter **34** and press **Enter**.

- The screen for selecting the serial port is displayed.

All serial ports on the server to be connected are displayed as follows:

```
Please input your choice:34
1 BMCcom
```

```
2 fabriccom
3 baseccom
4 FCcom
COM#(1 ~ 4)
```

- If an SOL connection has been connected through the serial port, a message will be displayed asking you whether to forcibly disconnect the existing SOL connection.

```
=====
user name:root
PassWord:
Log in Success!
=====
please input the SOL Blade1-Blade16(1 ~ 16), Blade1A-Blade16A(17 ~ 32), Sw
il-Swi4(33 ~ 36) and COM#(n)
press Ctrl+R to return
=====
Blade1-Blade16(1 ~ 16)
Blade1A-Blade16A(17 ~ 32)
Swil-Swi4(33 ~ 36)
Please input your choice:34
Have same connect!
Whether to forcibly exit an existing SOL connection that the other user created.
(Y|N):
```

- Press **Y** to forcibly disconnect the existing SOL connection.
- Press **N** to not disconnect the existing SOL connection. The system stays at the current screen.

Step 6 Enter the number of a serial port to be connected. For example, enter **1** and press **Enter**.

- The serial port CLI is displayed.
- If another user has logged in to the serial port, a message will be displayed asking you whether to forcibly log out the user.

```
=====
You are forcibly logged out by other users,
Please try again later.
=====
Blade1-Blade16(1 ~ 16)
Blade1A-Blade16A(17 ~ 32)
Swil-Swi4(33 ~ 36)
Please input your choice:34
1 fabriccom
2 bmccom
3 baseccom
COM#(1 ~ 3):1
Have same connect!
Whether to forcibly exit an existing SOL connection that the other user created.
(Y|N):y
```

- Press **Y** to forcibly log out the user.
- Press **N** to not forcibly log out the user. The system stays at the current screen.

Step 7 Enter the user name and password for connecting the serial port.

Perform configuration and query operations on the serial port CLI.

----End

6.5 Logging in to the MM910 WebUI

This topic describes how to log in to the web user interface (WebUI) by using Internet Explorer.

Scenarios

Log in to the HMM WebUI using a browser.

NOTE

- If there are five consecutive attempts to log in to the MM910 WebUI with incorrect passwords, the account is locked. It will be automatically unlocked after 10 minutes. If you enter a password within this time, the lock is reset to 10 minutes even if the password is correct.
- An account can log in to the HMM WebUI only through one IP address at a time. If an account is logged in and then logs in through another IP address, the account will be logged out.
- After logging in to the MM910 CLI or WebUI, you are logged out of the management UI if you do not perform any operation within a specified time period. The default lockout duration of the CLI is 2 minutes and that of the WebUI is 5 minutes. You can change the values as required.
- The MM910 supports a maximum of 32 clients to log in to the WebUI and 100 clients to log in to the CLI at the same time.
- "This is the standby MM" is displayed for the WebUI of the standby MM910. The standby MM910 WebUI does not display component installation status. On the WebUI of the standby MM910, you can only view monitoring information about the active MM910, set the DHCP and static IP addresses, and set and query the thresholds and hysteresis of the sensors of the standby MM910. To perform other operations, log in to the WebUI of the active MM910.
- For details about the operations on the WebUI, see the Online Help.

Prerequisites

Conditions

The client (a PC) used to access the HMM WebUI must meet the requirements listed in [Table 6-1](#).

Table 6-1 Runtime environment requirements

OS		Web Browser	JRE
Windows	• Windows 7 32-bit/64-bit • Windows 8 32-bit/64-bit • Windows Server 2008 • Windows Server 2012	• Internet Explorer 9 or later • Mozilla Firefox 19.0 to 31.0 • Chrome 22.0 to 31.0	• JRE 1.6 or later if the MM910 version is earlier than (U54)5.51 • JRE 1.7 or later if the MM910 version is (U54)5.51 and later

OS		Web Browser	JRE
Linux	Red Hat Enterprise Linux (RHEL) 4.3 to 6.0	Mozilla Firefox 19.0 to 31.0	

 NOTE

This task uses Internet Explorer 11 in Windows 7 as an example.

Data

User name and password for logging in to the server.

Procedure**Step 1** (Optional) Check the MM910 management network port out mode.

You can log in to the MM910 WebUI through a serial port and run the **outportmode** command to query and set the management network port out mode. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).

 NOTE

The MM910 management port is provided by two modes.

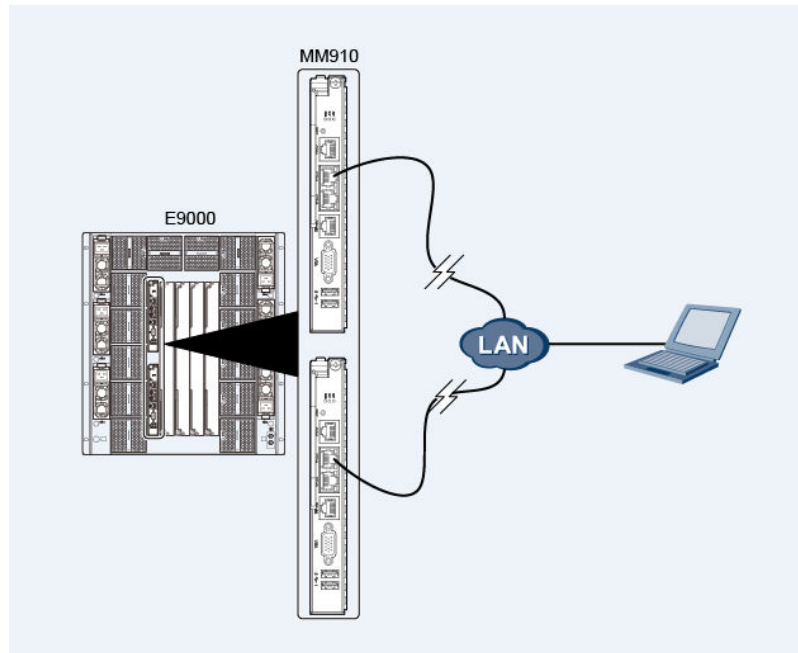
- An Ethernet port on the switch module in slot 2X or 3X can be used as the MM910 management port. However, if a CX910/CX911/CX912/CX913/CX915 is in slot 2X or 3X, only a GE port can be used; if a CX920 is in slot 2X or 3X, only a 10GE port can be used; if a CX916/CX916L/CX930 is in slot 2X or 3X, only a 25GE port can be used. If a CX110/CX111/CX310/CX311/CX312/CX320/CX710 is in slot 2X or 3X, any port can be used. The CX910/CX911/CX912/CX913 are not recommended for providing the management network port of the management module.
- The MGMT port on the MM910 panel can be used as the MM910 management port.
- For MM910 (U54) 2.25 or earlier, the port on the switch module in slot 2X or 3X is used as the management network port by default. In this case, do not connect the MGMT port on the MM910 and the port on the switch module to the same network at the same time, otherwise, a network storm occurs and the network is interrupted. For MM910 (U54) 2.26 or later, the MGMT port is used as the management network port by default. For details about how to query the version, see the [MM910 Management Module V100R001 User Guide](#).
- You can run the **outportmode** command to change the mode in which the management network port is provided. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).

Step 2 Connect the local PC to the MM910 management network port based on the MM910 management network port out mode.

- MGMT port on the MM910 panel
 - Connect the Ethernet port on the PC to the MGMT port on the active or standby MM910 over a local area network (LAN).

[Figure 6-5](#) shows the network connection.

Figure 6-5 Network connection

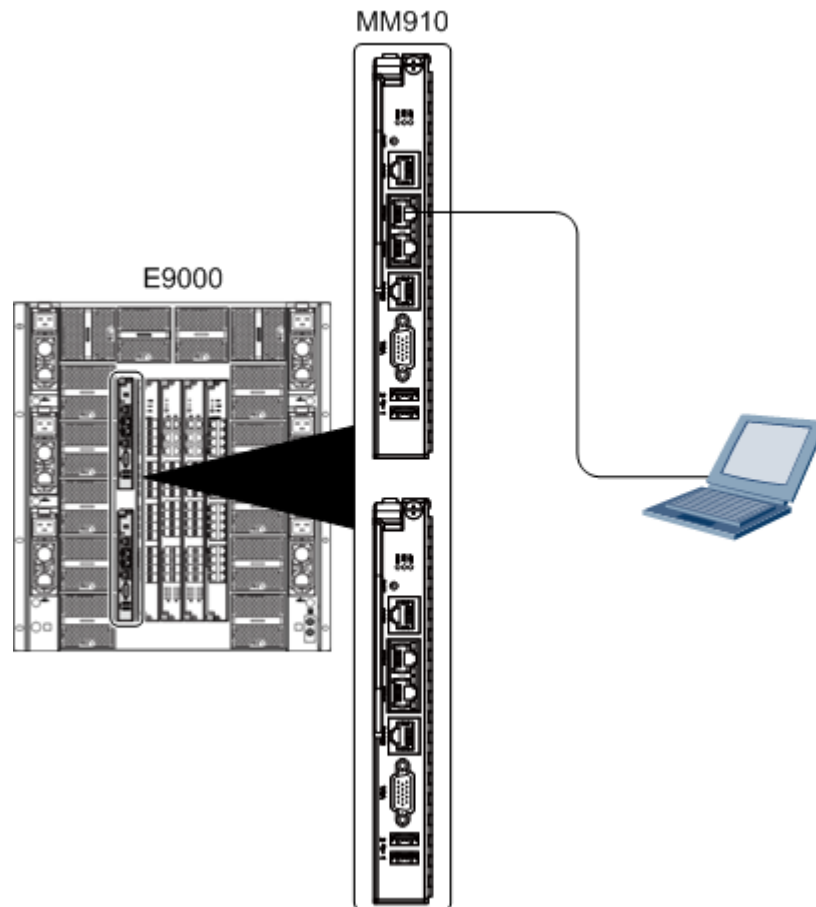


- Connect the Ethernet port on the PC to the MGMT port on the active MM910.

NOTE

If the MGMT port of the active MM910 is available, use this port.

Figure 6-6 Connection between the local PC and the active MM910 (in slot MM2 in this example)

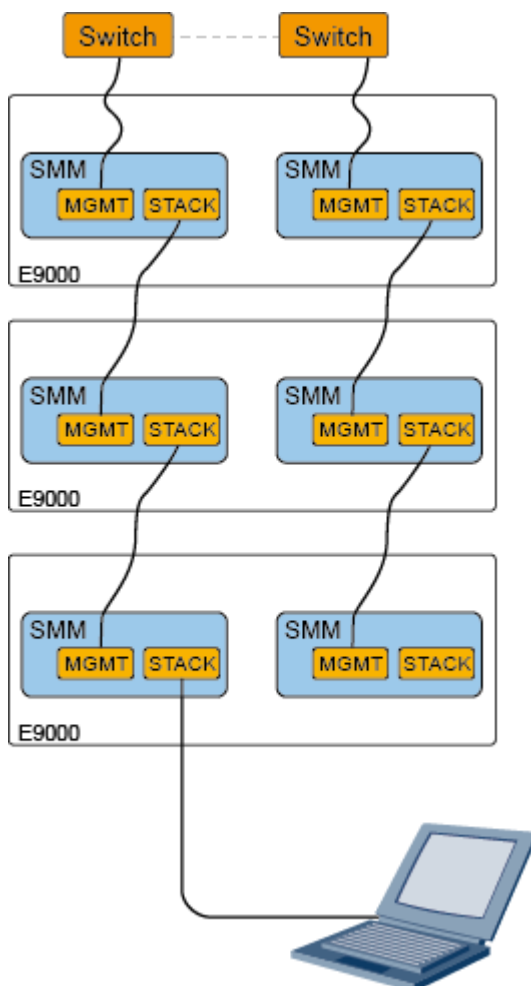


- Connect the Ethernet port on the local PC to the MGMT or STACK port on the active MM910.

NOTE

If the MGMT port on the active MM910 is unavailable, connect the PC to the STACK port on the active MM910. If the STACK port is used to stack the MGMT port in another chassis, connect the PC to an idle STACK port on an active MM910 in a chassis cascaded with the E9000 chassis.

Figure 6-7 Connection between the local PC and an idle STACK port on an MM910 stacked



- An Ethernet port on the switch module

Connect the Ethernet port on the PC to a port on the switch module in slot 2X or 3X over a LAN.

NOTE

- Switch modules can be also installed in slots 1E and 4E of the E9000 chassis, but only the switch modules in slots 2X and 3X provide the management network ports.
- If the ports on switch modules in slots 2X and 3X are used to access the management plane, isolate the management VLAN from the service VLAN for the switch modules for security purposes.

Step 3 Set an IP address and a subnet mask or add route information for the PC, and ensure that the PC can properly communicate with the MM910.

Step 4 Open Internet Explorer, click  and choose **Internet Options**.

The **Internet Options** dialog box is displayed.

Step 5 Choose **Connections** and click **LAN Settings**.

The **LAN Settings** dialog box is displayed.

Step 6 In the **Proxy server** group box, deselect **Use a proxy server for your LAN** and click **OK**.

Step 7 Click **OK**.

The **LAN Settings** dialog box is closed.

Step 8 Click **OK**.

The **Internet Options** dialog box is closed.

Step 9 Open Internet Explorer again, enter `https://MM910 floating IP address`, for example `https://192.168.2.3`, in the address box, and press **Enter**.

 NOTE

You can query or configure the MM910 floating IP address in any of the following ways:

- Use the chassis intelligent display. For details, see [FusionServer Pro E9000 Server V100R001 Chassis Intelligent Display Parameter Reference](#).
- Use the HMM WebUI. For details, see Configuring the MM910 IP Addresses in [MM910 Management Module V100R001 User Guide](#).
- Run the **floatip** command on the MM910 CLI. For details, see [MM910 Management Module V100R001 Command Reference](#).

The message "There is a problem with this website's security certificate" is displayed.

Step 10 (Optional) Add the MM910 IP address to the **Trusted sites** zone.

By default, Internet Explorer enhanced security configuration is enabled on the Windows Server series OSs. Add the MM910 IP address to the trusted sites zone as follows:

1. On Internet Explorer, choose **Tools > Internet Options**.
The **Internet Options** dialog box is displayed.
2. Click the **Security** tab.
3. Click **Trusted sites**, and click **Sites**.
4. In the **Trusted sites** dialog box, click **Add** to add the MM910 IP address to the trusted site list, and click **Close**.
5. Refresh the page.
6. In the status bar of a browser, check whether the MM910 IP address is in the **Trusted sites** zone.

Step 11 Click **Continue to this website (not recommended)**.

The **HMM Web** login page is displayed.

Step 12 Set the login parameters, as shown in [Figure 6-8](#).

 NOTE

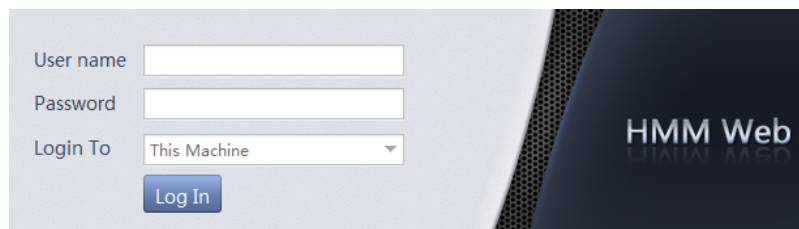
The login page varies slightly with the HMM software version.

- **Language:** Select the language to be used.
- **User name:** Enter the user name. The default user name is **root**.
- **Password:** Enter the password. The default password is **Huawei12#\$**.

If **User must change password at next login** is selected when users are created on the LDAP server, logins will fail. Deselect this option on the LDAP server.

- **Log in to:** Select **This Machine/computer** for a local user. If the system manages domain users over Active Directory (AD), select **LDAP**.

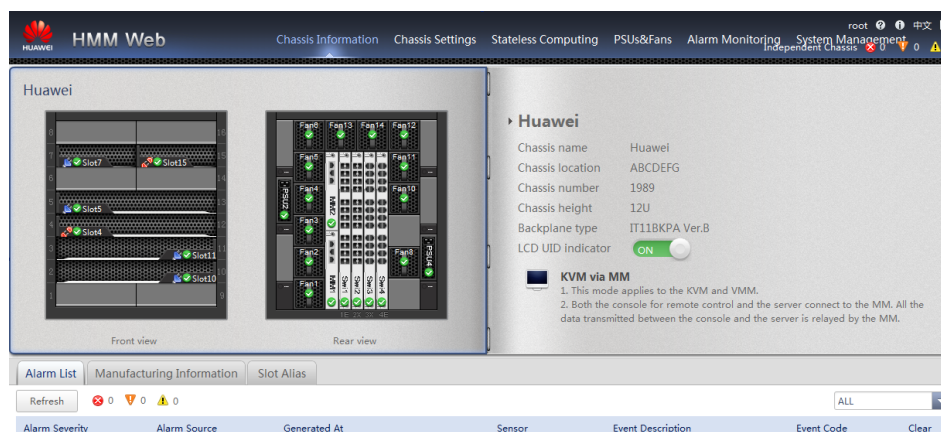
Figure 6-8 Logging in to HMM Web of version V603



Step 13 Click **Log In**.

The **HMM Web** home page is displayed, as shown in [Figure 6-9](#).

Figure 6-9 HMM Web (V603)



----End

6.6 Reconfiguring the RAID

This topic describes how to reconfigure the redundant array of independent disks (RAID).

CH242 V3 4HDD supports two types of RAID controller cards: LSISAS2208 and LSISAS2308.

- LSISAS2208: supports RAID 0, 1, 5, 6, 10, 50, and 60.
- LSISAS2308: supports RAID 0, 1, 1E, and 10.

CH242 V3 8HDD supports two types of RAID controller cards: LSISAS2208 and LSISAS2308.

- LSISAS2208: supports RAID 0, 1, 5, 6, 10, 50, and 60.
- LSISAS2308: supports RAID 0, 1, 1E, and 10.

For details, see [Huawei V2 and V3 Server RAID Controller Card User Guide](#).

6.7 Powering On and Off the CH242 V3

This topic describes how to power on and off the CH242 V3.

6.7.1 Powering On the CH242 V3

This topic describes how to power on the CH242 V3.

Scenarios

Remotely power on the CH242 V3 over the web user interface (WebUI) of the MM910.

NOTE

The following methods can also be used to power on the compute node:

- If the chassis is not powered on, power on the chassis. The compute node will be powered on with the chassis.
- If the chassis is powered on but the compute node is not installed, install the compute node. The compute node is automatically powered on after it is installed.
- If the chassis is powered on and compute node is abnormal, hold down the power switch on the front panel for 6 seconds to power off the compute node and press the power switch to power it on.
- If the chassis is powered on and the compute node is powered off:
 - Power on the compute node on the MM910 WebUI. For details, see this section.
 - Run the **powerstate** command over the MM910 to power on the compute node. For details, see [MM910 Management Module V100R001 Command Reference](#).

Prerequisites

Conditions

- The chassis is installed.
- The power cable is properly connected to the chassis.
- The power supply units (PSUs) and fan modules are properly installed in the chassis.

Data

Data preparation is not required for this operation.

Procedure

Step 1 Log in to the WebUI of the MM910.

1. (Optional) Check the MM910 management network port out mode.
You can log in to the MM910 WebUI through a serial port and run the **outportmode** command to query and set the management network port out mode. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).

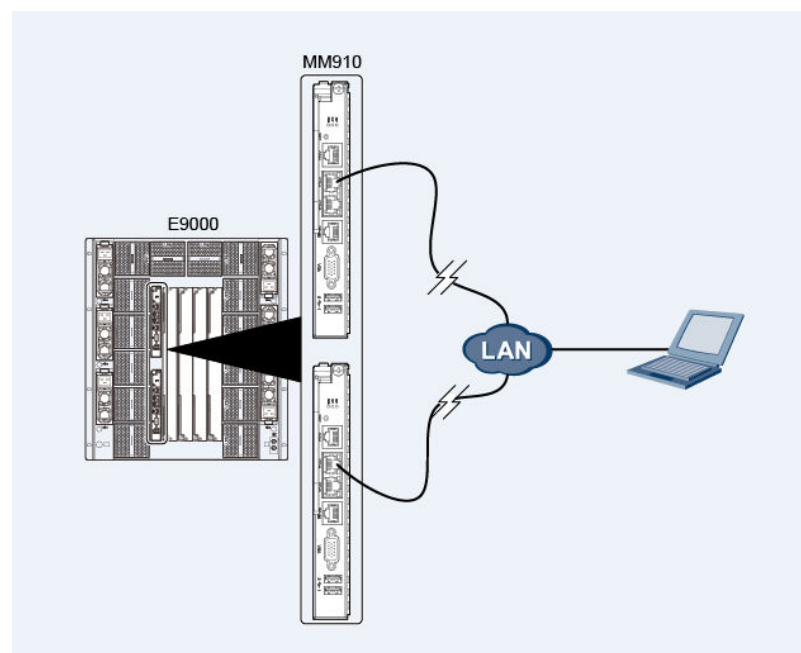
NOTE

The MM910 management port is provided by two modes.

- An Ethernet port on the switch module in slot 2X or 3X can be used as the MM910 management port. However, if a CX910/CX911/CX912/CX913/CX915 is in slot 2X or 3X, only a GE port can be used; if a CX920 is in slot 2X or 3X, only a 10GE port can be used; if a CX916/CX916L/CX930 is in slot 2X or 3X, only a 25GE port can be used. If a CX110/CX111/CX310/CX311/CX312/CX320/CX710 is in slot 2X or 3X, any port can be used. The CX910/CX911/CX912/CX913 are not recommended for providing the management network port of the management module.
 - The MGMT port on the MM910 panel can be used as the MM910 management port.
 - For MM910 (U54) 2.25 or earlier, the port on the switch module in slot 2X or 3X is used as the management network port by default. In this case, do not connect the MGMT port on the MM910 and the port on the switch module to the same network at the same time, otherwise, a network storm occurs and the network is interrupted. For MM910 (U54) 2.26 or later, the MGMT port is used as the management network port by default. For details about how to query the version, see the [MM910 Management Module V100R001 User Guide](#).
 - You can run the **outportmode** command to change the mode in which the management network port is provided. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).
2. Connect the local PC to the MM910 management network port based on the MM910 management network port out mode.
- MGMT port on the MM910 panel
 - Connect the Ethernet port on the PC to the MGMT port on the active or standby MM910 over a local area network (LAN).

Figure 6-10 shows the network connection.

Figure 6-10 Network connection

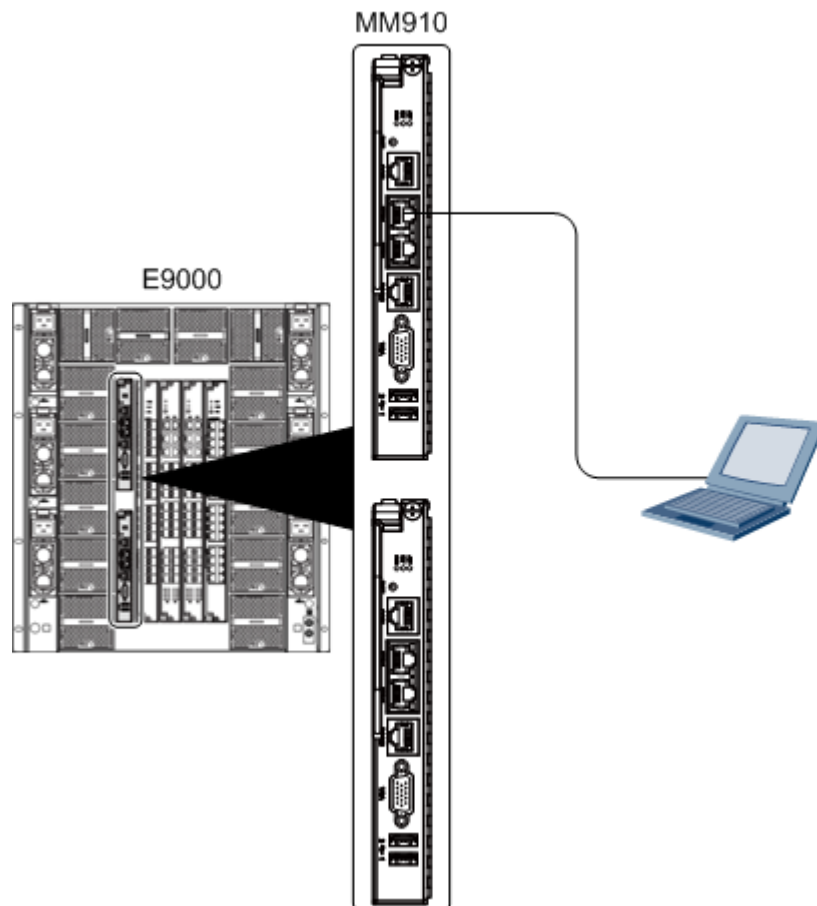


- Connect the Ethernet port on the PC to the MGMT port on the active MM910.

 NOTE

If the MGMT port of the active MM910 is available, use this port.

Figure 6-11 Connection between the local PC and the active MM910 (in slot MM2 in this example)

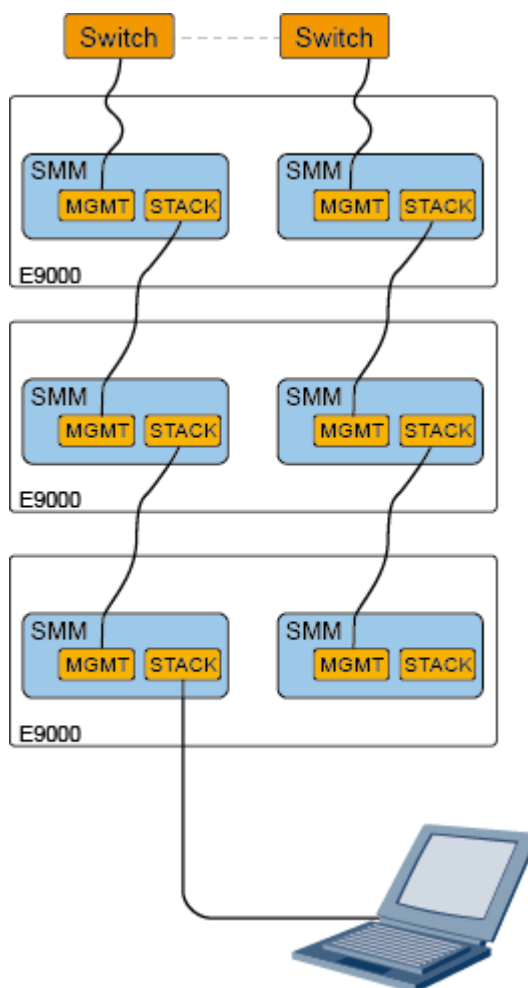


- Connect the Ethernet port on the local PC to the MGMT or STACK port on the active MM910.

 NOTE

If the MGMT port on the active MM910 is unavailable, connect the PC to the STACK port on the active MM910. If the STACK port is used to stack the MGMT port in another chassis, connect the PC to an idle STACK port on an active MM910 in a chassis cascaded with the E9000 chassis.

Figure 6-12 Connection between the local PC and an idle STACK port on an MM910 stacked



- An Ethernet port on the switch module

Connect the Ethernet port on the PC to a port on the switch module in slot 2X or 3X over a LAN.

NOTE

- Switch modules can be also installed in slots 1E and 4E of the E9000 chassis, but only the switch modules in slots 2X and 3X provide the management network ports.
 - If the ports on switch modules in slots 2X and 3X are used to access the management plane, isolate the management VLAN from the service VLAN for the switch modules for security purposes.
3. Set an IP address and a subnet mask or add route information for the PC, and ensure that the PC can properly communicate with the MM910.
 4. Open Internet Explorer, click  and choose **Internet Options**.
The **Internet Options** dialog box is displayed.
 5. Choose **Connections** and click **LAN Settings**.
The **LAN Settings** dialog box is displayed.

6. In the **Proxy server** group box, deselect **Use a proxy server for your LAN** and click **OK**.
The **LAN Settings** dialog box is closed.
7. Click **OK**.
The **Internet Options** dialog box is closed.
8. Open Internet Explorer again, enter `https://MM910 floating IP address`, for example `https://192.168.2.3`, in the address box, and press **Enter**.

NOTE

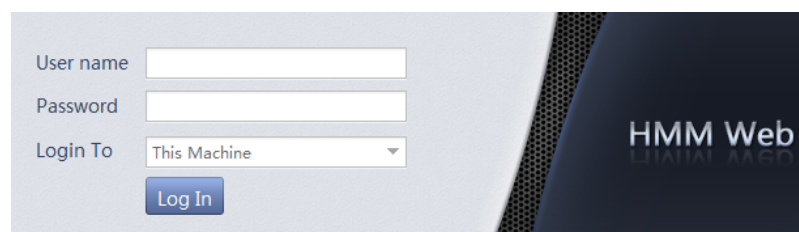
You can query or configure the MM910 floating IP address in any of the following ways:

- Use the chassis intelligent display. For details, see [FusionServer Pro E9000 Server V100R001 Chassis Intelligent Display Parameter Reference](#).
- Use the HMM WebUI. For details, see [Configuring the MM910 IP Addresses in MM910 Management Module V100R001 User Guide](#).
- Run the floatip command on the MM910 CLI. For details, see [MM910 Management Module V100R001 Command Reference](#).

The message "There is a problem with this website's security certificate" is displayed.

9. (Optional) Add the MM910 IP address to the **Trusted sites** zone.
By default, Internet Explorer enhanced security configuration is enabled on the Windows Server series OSs. Add the MM910 IP address to the trusted sites zone as follows:
 - a. On Internet Explorer, choose **Tools > Internet Options**.
The **Internet Options** dialog box is displayed.
 - b. Click the **Security** tab.
 - c. Click **Trusted sites**, and click **Sites**.
 - d. In the **Trusted sites** dialog box, click **Add** to add the MM910 IP address to the trusted site list, and click **Close**.
 - e. Refresh the page.
 - f. In the status bar of a browser, check whether the MM910 IP address is in the **Trusted sites** zone.
10. Click **Continue to this website (not recommended)**.
The **HMM Web** login page is displayed, as shown in [Figure 6-13](#).

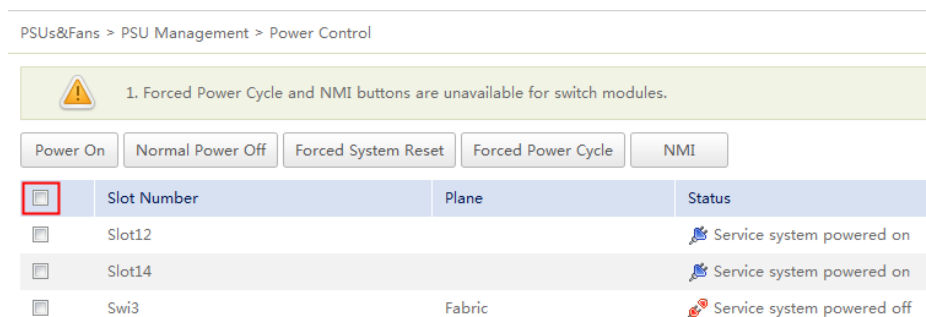
Figure 6-13 Logging in to HMM Web of version V603

**NOTE**

The login page varies slightly with the HMM software version.

Step 2 Remotely power on the compute node.

1. Perform operations based on the version determined after comparing the MM910 interface.
 - If the MM910 version is later than **(U54) 2.20**, go to [Step 2.2](#) to [Step 2.4](#).
 - If the MM910 version is **(U54) 2.20** or earlier, go to [Step 2.5](#) to [Step 2.6](#).
You can run the **smmget -l smm -d version** command on the MM910 CLI to check the software version.
2. Select **PSU&Fans** on the WebUI.
The **PSU&Fans** page is displayed.
3. In the navigation tree, choose **PSU Management > Power Control**, as shown in [Figure 6-14](#).

Figure 6-14 Power control

4. Select the compute node to be powered on, and click **Power On**.
The selected compute nodes are powered on.

NOTE

Selecting the check box marked in red in [Figure 6-14](#) means selecting all compute nodes. Clicking **Power On** powers on all compute nodes.

5. In the navigation tree, choose **Power Supply Management**, and click **Blade Power Control** on the displayed page, as shown in [Figure 6-15](#).

Figure 6-15 Blade power control

Blade Power Control					
Blade	Operation				Status
☐ blade1	☒ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade2	☐ Power On	☒ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade3	☒ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade4	☐ Power On	☒ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade5	☐ Power On	☒ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade6	☒ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade7	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade8	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade9	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade10	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade11	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade12	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade13	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade14	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade15	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade16	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	

Batch Set					
☒ All	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	OK

6. Select the compute node to be powered on in the **Blade** column, select **Power On** in the **Operation** column, and click **OK**.

The operation is complete.

NOTE

To power on all the compute nodes, select **All** in the **Batch Set** table, select **Power On**, and click **OK**.

-----End

6.7.2 Powering Off the CH242 V3

This topic describes how to power off the CH242 V3.

Scenarios

NOTE

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

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

NOTE

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

For details, see [2.3 Indicators](#).

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

For details, see [2.3 Indicators](#).

- Use the MM910 WebUI.

For details, see [MM910 Management Module V100R001 User Guide](#).

- On the MM910 CLI, run the following command:

powerstate

For details, see [MM910 Management Module V100R001 Command Reference](#).

The following describes how to power off a compute node using the MM910 WebUI.

Prerequisites

Conditions

The CH242 V3 service data is backed up.

Data

Data preparation is not required for this operation.

Procedure

Step 1 Log in to the WebUI of the MM910.

1. (Optional) Check the MM910 management network port out mode.

You can log in to the MM910 WebUI through a serial port and run the **outportmode** command to query and set the management network port out mode. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).

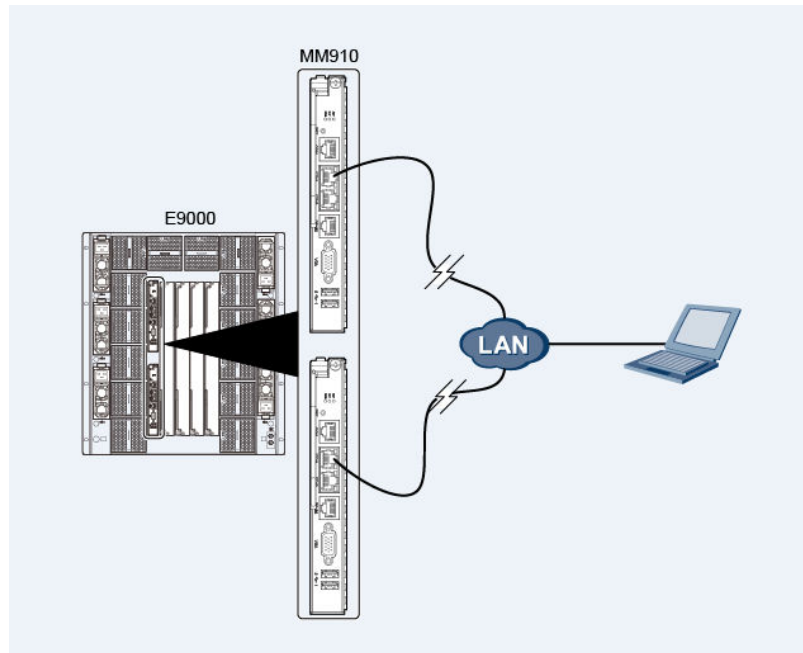
NOTE

The MM910 management port is provided by two modes.

- An Ethernet port on the switch module in slot 2X or 3X can be used as the MM910 management port. However, if a CX910/CX911/CX912/CX913/CX915 is in slot 2X or 3X, only a GE port can be used; if a CX920 is in slot 2X or 3X, only a 10GE port can be used; if a CX916/CX916L/CX930 is in slot 2X or 3X, only a 25GE port can be used. If a CX110/CX111/CX310/CX311/CX312/CX320/CX710 is in slot 2X or 3X, any port can be used. The CX910/CX911/CX912/CX913 are not recommended for providing the management network port of the management module.
 - The MGMT port on the MM910 panel can be used as the MM910 management port.
 - For MM910 (U54) 2.25 or earlier, the port on the switch module in slot 2X or 3X is used as the management network port by default. In this case, do not connect the MGMT port on the MM910 and the port on the switch module to the same network at the same time, otherwise, a network storm occurs and the network is interrupted. For MM910 (U54) 2.26 or later, the MGMT port is used as the management network port by default. For details about how to query the version, see the [MM910 Management Module V100R001 User Guide](#).
 - You can run the **outportmode** command to change the mode in which the management network port is provided. For details, see "Querying and Setting the Network Port Out Mode (outportmode)" in the [MM910 Management Module V100R001 Command Reference](#).
2. Connect the local PC to the MM910 management network port based on the MM910 management network port out mode.
 - MGMT port on the MM910 panel
 - Connect the Ethernet port on the PC to the MGMT port on the active or standby MM910 over a local area network (LAN).

[Figure 6-16](#) shows the network connection.

Figure 6-16 Network connection

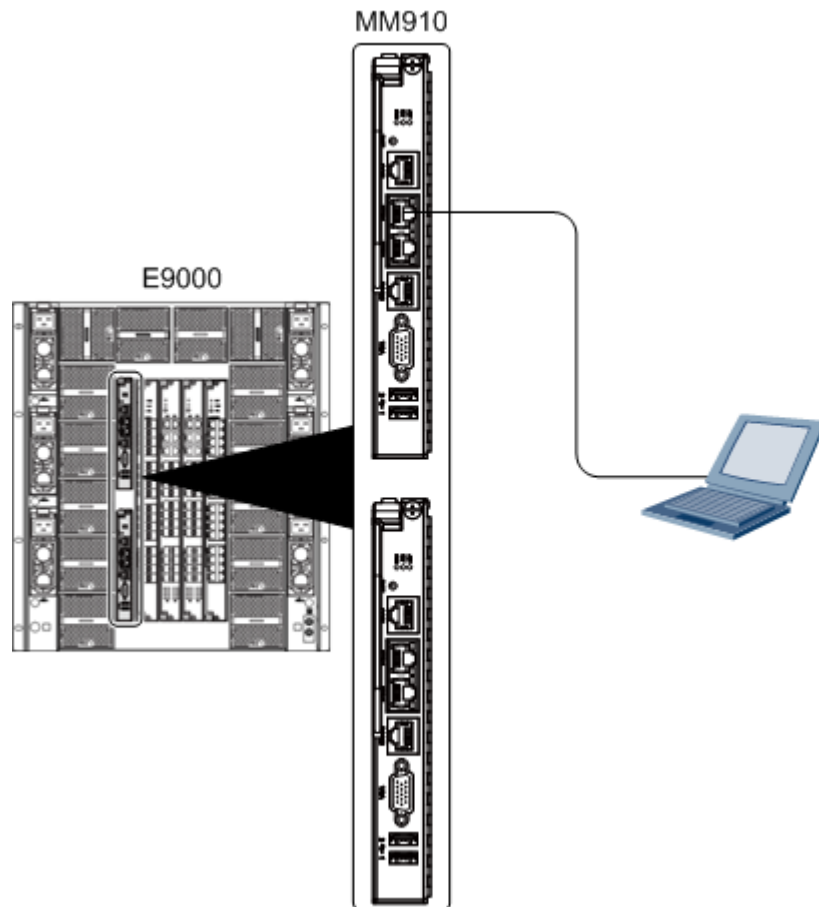


- Connect the Ethernet port on the PC to the MGMT port on the active MM910.

NOTE

If the MGMT port of the active MM910 is available, use this port.

Figure 6-17 Connection between the local PC and the active MM910 (in slot MM2 in this example)

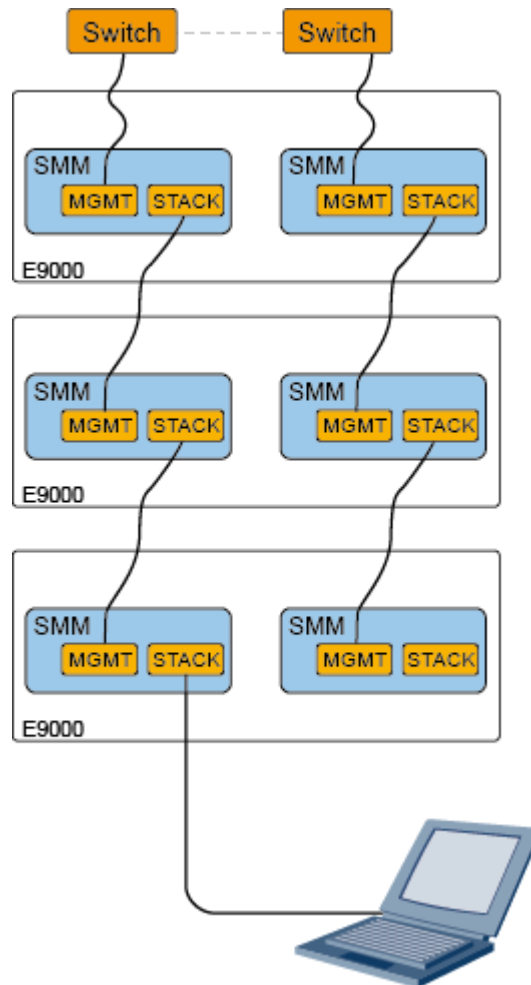


- Connect the Ethernet port on the local PC to the MGMT or STACK port on the active MM910.

NOTE

If the MGMT port on the active MM910 is unavailable, connect the PC to the STACK port on the active MM910. If the STACK port is used to stack the MGMT port in another chassis, connect the PC to an idle STACK port on an active MM910 in a chassis cascaded with the E9000 chassis.

Figure 6-18 Connection between the local PC and an idle STACK port on an MM910 stacked



- An Ethernet port on the switch module

Connect the Ethernet port on the PC to a port on the switch module in slot 2X or 3X over a LAN.

NOTE

- Switch modules can be also installed in slots 1E and 4E of the E9000 chassis, but only the switch modules in slots 2X and 3X provide the management network ports.
 - If the ports on switch modules in slots 2X and 3X are used to access the management plane, isolate the management VLAN from the service VLAN for the switch modules for security purposes.
- Set an IP address and a subnet mask or add route information for the PC, and ensure that the PC can properly communicate with the MM910.
 - Open Internet Explorer, click  and choose **Internet Options**. The **Internet Options** dialog box is displayed.
 - Choose **Connections** and click **LAN Settings**. The **LAN Settings** dialog box is displayed.

6. In the **Proxy server** group box, deselect **Use a proxy server for your LAN** and click **OK**.
The **LAN Settings** dialog box is closed.
7. Click **OK**.
The **Internet Options** dialog box is closed.
8. Open Internet Explorer again, enter `https://MM910 floating IP address`, for example `https://192.168.2.3`, in the address box, and press **Enter**.

NOTE

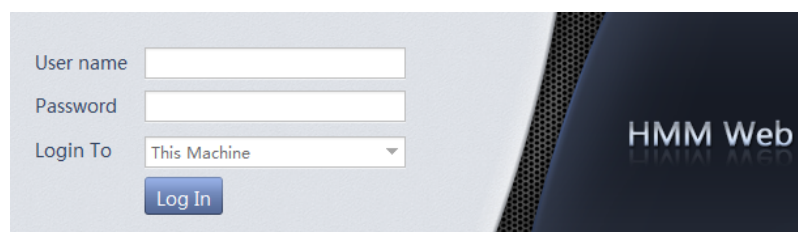
You can query or configure the MM910 floating IP address in any of the following ways:

- Use the chassis intelligent display. For details, see [FusionServer Pro E9000 Server V100R001 Chassis Intelligent Display Parameter Reference](#).
- Use the HMM WebUI. For details, see [Configuring the MM910 IP Addresses in MM910 Management Module V100R001 User Guide](#).
- Run the floatip command on the MM910 CLI. For details, see [MM910 Management Module V100R001 Command Reference](#).

The message "There is a problem with this website's security certificate" is displayed.

9. (Optional) Add the MM910 IP address to the **Trusted sites** zone.
By default, Internet Explorer enhanced security configuration is enabled on the Windows Server series OSs. Add the MM910 IP address to the trusted sites zone as follows:
 - a. On Internet Explorer, choose **Tools > Internet Options**.
The **Internet Options** dialog box is displayed.
 - b. Click the **Security** tab.
 - c. Click **Trusted sites**, and click **Sites**.
 - d. In the **Trusted sites** dialog box, click **Add** to add the MM910 IP address to the trusted site list, and click **Close**.
 - e. Refresh the page.
 - f. In the status bar of a browser, check whether the MM910 IP address is in the **Trusted sites** zone.
10. Click **Continue to this website (not recommended)**.
The **HMM Web** login page is displayed, as shown in [Figure 6-19](#).

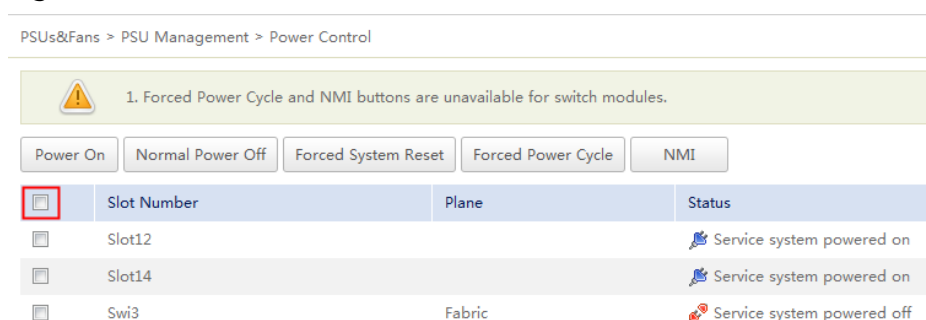
Figure 6-19 Logging in to HMM Web of version V603

**NOTE**

The login page varies slightly with the HMM software version.

Step 2 Remotely power off the compute node.

1. Perform operations based on the version determined after comparing the MM910 information.
 - If the MM910 version is later than **(U54) 2.20**, go to [Step 2.2](#) to [Step 2.3](#).
 - If the MM910 version is **(U54) 2.20** or earlier, go to [Step 2.4](#) to [Step 2.5](#).
You can run the **smmget -l smm -d version** command on the MM910 CLI to check the software version.
2. Select **PSU&Fans** on the WebUI. In the navigation tree, choose **PSU Management > Power Control**, as shown in [Figure 6-20](#).

Figure 6-20 Power control

3. Select one or more compute nodes and click **Normal Power Off**.
The selected compute nodes are powered off.

NOTE

Selecting the check box marked in red in [Figure 6-20](#) means selecting all compute nodes. Clicking **Normal Power Off** powers off all compute nodes.

4. In the navigation tree, choose **Power Supply Management**, and click **Blade Power Control** on the displayed page, as shown in [Figure 6-21](#).

Figure 6-21 Blade power control

Blade Power Control					
Blade	Operation				Status
☐ blade1	☒ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade2	☐ Power On	☒ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade3	☒ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade4	☐ Power On	☒ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade5	☐ Power On	☒ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade6	☒ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade7	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade8	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade9	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade10	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade11	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade12	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade13	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade14	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade15	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	
☐ blade16	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot	

Batch Set				
☒ All	☐ Power On	☐ Power Off	☐ Cold Reset	☐ Graceful reboot

5. Select the compute node to be powered off in the **Blade** column, select **Power Off** in the **Operation** column, and click **OK**.

The operation is complete.

NOTE

To power off all the compute nodes, select **All** in the **Batch Set** table, select **Power Off**, and click **OK**.

----End

6.8 Erasing Storage Media Data

This topic describes how to erase data from storage media by running the Linux command **badblocks** or mounting the toolkit.

Scenarios

- 1: If the storage medium is not configured in a RAID or is configured in a RAID without redundancy and the compute node OS is running properly, run the Linux command **badblocks**.
- 2: If the storage medium is not configured in a RAID or is configured in a RAID without redundancy and the compute node OS is not running properly, mount the toolkit to the compute node.

- 3: If the storage medium is in a RAID with redundancy, move the storage medium to an idle compute node and mount the toolkit to the idle compute node.

Prerequisites

Conditions

- Scenario 1: The storage medium is not configured in a RAID or is configured in a RAID without redundancy and the compute node OS is running properly.
- Scenario 2: The storage medium is not configured in a RAID or is configured in a RAID without redundancy and the compute node OS is not running properly.
- Scenario 3: The storage medium is in a RAID with redundancy.

Data

- Chassis number of the storage device.
- Slot number of the storage device.
- Position of the storage device.

Hardware

An idle compute node. This is required only for scenario 3.

Note

- The Linux **badblocks** command is used to erase data from storage devices. This command erases data by writing all 0s on the storage device based on the command parameters specified.
- The methods described in this topic are for reference only. You can also use other methods to erase storage media data.

NOTICE

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

Procedure

Erasing Data from an HDD or SSD by Running the badblocks Command.

Step 1 Log in to the compute node holding the hard disk to be erased.

For details, see [4.7 Logging In to the Real-Time Desktop](#).

Step 2 Open the command line interface (CLI) and run the **ls SCSI** command to query drive letters.

[Figure 6-22](#) shows an example.

Figure 6-22 Querying drive letters

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

Step 3 Run the **fdisk -l** command to query information about hard disks and the system disk. In [Figure 6-23](#), the hard disk with the * symbol in the **Boot** column is the system disk. In [Figure 6-23](#), **sda** is the system disk.

 NOTE

Do not directly erase system disk data. Before erasing system disk data, erase data from other storage media.

Figure 6-23 Querying hard disk information

```
Linux-hm54:~ # fdisk -l

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

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

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

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

Step 4 Run the **badblocks -swft 0** command to write zeros to the hard disk. For example, if you need to erase data from HD1, whose drive letter is **/dev/sdb**, run the **badblocks -swft 0 /dev/sdb** command.

Figure 6-24 Erasing data

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

 NOTE

- HDDs, SSDs, microSD cards, and USB flash drives may have different drive letters. Check the drive letter of the storage medium before running the **badblocks -swft 0** command.
- This operation may take some time.
- If the **badblocks -swft 0** command fails, contact Huawei technical support.

Step 5 Remove the hard disk.

For details, see [5.1 Removing a Hard Disk](#).

 NOTE

After data is erased, do not restart or remove and reinstall the compute node. Otherwise, data will be reloaded to the hard disks when the compute node restarts.

----End

Erasing Data from a microSD Card by Mounting the Toolkit.

Step 1 On the iBMC WebUI, choose **Configure > Boot Option**.

The **Boot Option** page is displayed.

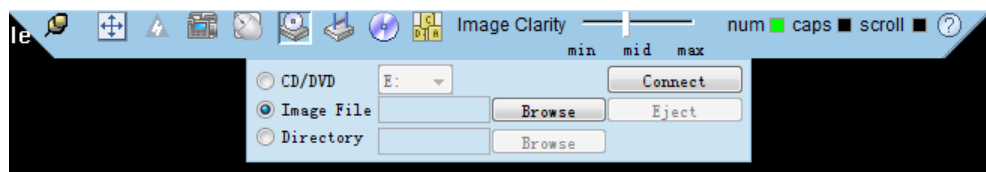
Step 2 Select **DVD-ROM** and click **Save**.

Step 3 Open the Remote Virtual Console.

Step 4 Click  on the toolbar.

The screen shown in [Figure 6-25](#) is displayed.

Figure 6-25 Virtual DVD-ROM drive



Step 5 Select **Image File** and click **Browse**.

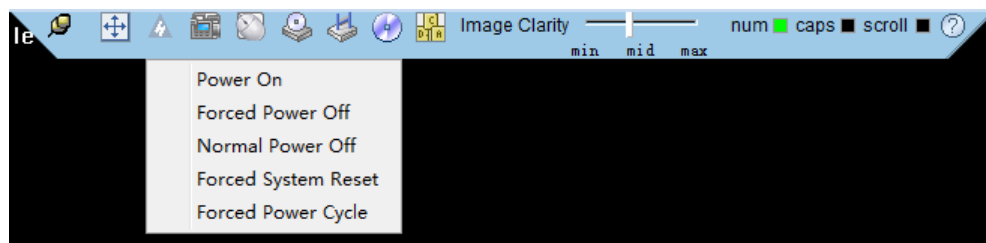
The **Open** dialog box is displayed.

Step 6 Select **FusionServer Tools-Toolkit-Vxxx.iso**, and click **Connect** shown in [Figure 6-25](#).

Step 7 Click  on the toolbar.

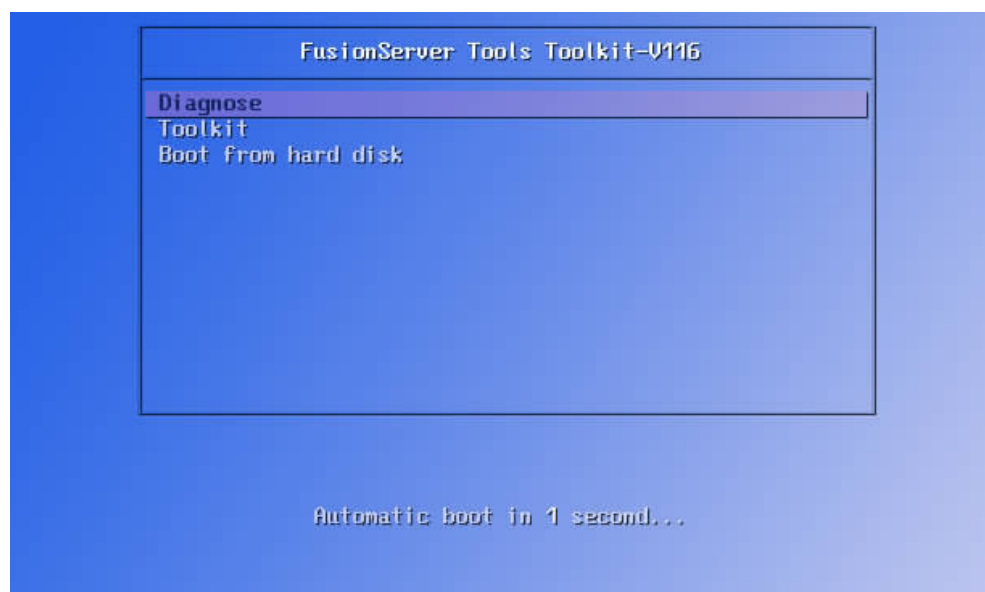
The menu shown in [Figure 6-26](#) is displayed.

Figure 6-26 Power control



Step 8 Select the option based on the actual server status to restart the server.

After the server restarts, the screen shown in [Figure 6-27](#) is displayed.

Figure 6-27 Toolkit startup screen

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

Step 10 When information shown in [Figure 6-28](#) is displayed, enter **C** and press **Enter**.

Figure 6-28 Toolkit menu

```
Master Resource Control: Running /etc/init.d/after.local
Preparing, please wait...
Get cdrom info succeed!!!

+-----+
|                               |
| FusionServer Tools -- Toolkit V116 |
| Release Date: 2016-10-30       |
|                               |
+-----+
| 1. Auto Diagnose              |
| 2. Display Hardware Information |
| 3. Hardware Inspect          |
| 4. CPU Test                   |
| 5. Memory Test               |
| 6. HardDisk Test             |
| 7. Clear HardDisk            |
| 8. LOG Collect               |
| 9. Make Bootable USB Disk    |
| 10. Save Log To USB Disk     |
+-----+
| S/s . Save Log To The Remote Server |
| C/c . Command line              |
| R/r . Reboot                   |
| P/p . Power Off                |
| Thu Nov 17 01:32:58 CST 2016    |
+-----+
Please input your choice:
```

Step 11 Enter the user name and password as prompted.

The CLI is displayed.

NOTE

The default user is **root**, and the password is **Huawei12#\$**.

Step 12 Run the **fdisk -l** command to view the partitions and run the **d** command to delete partitions, as shown in [Figure 6-29](#).

Figure 6-29 Viewing and deleting partitions

```
[root@localhost media]# fdisk -l

Disk /dev/sda: 7948 MB, 7948205568 bytes
81 heads, 10 sectors/track, 19165 cylinders
Units = cylinders of 810 * 512 = 414720 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1             11         19166     7757824    b   W95 FAT32
[root@localhost media]# fdisk /dev/sda

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help): d
Selected partition 1

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
sd 11:0:0:0: [sda] Assuming drive cache: write through
sda:
Syncing disks.
[root@localhost media]#
```

Step 13 Run the **ftk** command to exit the CLI and go back to the Toolkit menu.

----End

7 U-boot

This topic describes how to use the Compute Node U-boot.

[7.1 Logging In to the U-boot](#)

[7.2 U-boot Commands](#)

7.1 Logging In to the U-boot

This topic describes how to log in to the Compute Node U-boot over a serial port to debug the Compute Node.

Scenarios

Log in to the Compute Node U-boot over a high-density cable on the Compute Node panel.

The U-boot is used to initialize hardware, such as serial ports or dual in-line memory modules (DIMMs), reads the kernel image from the flash memory to the random access memory (RAM), and starts the operating system (OS). You can load bottom-layer software and debug bottom-layer devices on the U-boot user interfaces (UIs).

Prerequisites

Conditions

You have installed the high-density cable to the compute code.

Data

- User name for logging in to the compute node to be connected.
- Password for logging in to the compute node to be connected.
- Password for logging in to the compute node U-boot.

Procedure

- Step 1** Connect the serial port of the high-density port to the serial port of a PC with a serial cable.

 NOTE

If you cannot log in to the compute node over a serial port, log in by using the method described in Logging In to a Compute Node or a Switch Module over SOL.

Step 2 Log in to the compute node over a serial port by using the PuTTY. For details, see Logging In to the Server Over a Serial Port by Using the PuTTY.

Key communication parameters:

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

n indicates the serial port number, and the value is an integer.

You can log in to the operating system (OS) or iMana 200 after logging in to a compute node.

- You have logged in to the iMana 200 command-line interface (CLI) if the following information is displayed:
Wind River Linux release 3.0
Kernel 2.6.27_stm23_003 on armv5tejl (console)
BMC login:

- You have logged in to the OS CLI if the following information is displayed:
linux-SMM-Test1:~#

Test1 on the left of the prompt indicates the OS name. The value varies according to the OS name set by users.

Step 3 Determine whether you have logged in to the iMana 200 CLI.

- If yes, go to [Step 8](#).
- If not, go to [Step 4](#).

Step 4 Connect the RS-232 serial port on the PC and the **COM** port on the active MM910 by using a DB9-RJ45 cable.

Step 5 Log in to the MM910 CLI by using a serial port communication tool.

The key communication parameters are as follows:

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

n indicates the serial port number, and the value is an integer.

The PuTTY is used to log in to the MM910 CLI. For details, see Logging In to the Server Over a Serial Port by Using the PuTTY.

Step 6 Run the following command to switch to the iMana 200 CLI:

smmset -l *slot number of the compute node* -d switchcom -v 4

For example, if the slot number is 16, run the following command:

smmset -l blade16 -d switchcom -v 4

Success

The following information is displayed, indicating that the interface is successfully switched.

Success

Step 7 Log in to the iMana 200 of the compute node again over the serial port. For details, see [Step 1](#) and [Step 2](#).

Step 8 Run the following command to reboot the iMana 200 system of the compute node:

ipmcset -d reset

The command output similar to the following is displayed:

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

Step 9 Enter **Y**, and press **Enter**.

The iMana 200 system restarts.

Step 10 When the message "Hit 'ctrl + b' to stop autoboot: 1" is displayed, press **Ctrl+B** immediately.

The command output similar to the following is displayed:

ENTER PASSWD:

Step 11 Enter the password for logging in to the U-boot.

Step 12 Perform operations on the menu based on actual service requirements.

NOTE

- If you type **?** or **help** and press **Enter**, the help for all compute node U-boot commands is displayed.
- After logging in to the U-Boot, you can run the **boot** command to exit the U-Boot and log in to the OS.

----End

7.2 U-boot Commands

On the compute node U-boot command-line interface (CLI), type **?** or **help** and press **Enter**. The help of all compute node U-boot commands is displayed as follows:

```
u-boot> ?  
?      - alias for 'help'  
appfs_cp -copy appfs to flash  
appfs_up -update app file system  
autoscr - run script from memory  
base    - print or set address offset  
bdfinfo - print Board Info structure  
boot    - boot default, i.e., run 'bootcmd'
```

```
bootd - boot default, i.e., run 'bootcmd'
bootm - boot application image from memory
bootp - boot image via network using BootP/TFTP protocol
cdp - Perform CDP network configuration
cmp - memory compare
coninfo - print console devices and information
cp - memory copy
crc32 - checksum calculation
echo - echo args to console
enphy_m - init phy1512 addr1 in multi chip addr mode
enphy_s - init phy1512 addr0 in multi chip addr mode
erase - erase FLASH memory
exit - exit script
flinfo - print FLASH memory information
fsinfo - print information about filesystems
fsload - load binary file from a filesystem image
gmii - test
gmiim - test in multi-chip mode
go - start application at address 'addr'
help - print online help
i2c - I2C sub-system
iminfo - print header information for application image
imls - list all images found in flash
itest - return true/false on integer compare
loadb - load binary file over serial line (kermit mode)
loads - load S-Record file over serial line
loady - load binary file over serial line (ymodem mode)
loop - infinite loop on address range
ls - list files in a directory (default /)
md - memory display
mii - MII utility commands
mm - memory modify (auto-incrementing)
mtest - simple RAM test
mw - memory write (fill)
nfs - boot image via network using NFS protocol
nm - memory modify (constant address)
ping - send ICMP ECHO_REQUEST to network host
printenv - print environment variables
protect - enable or disable FLASH write protection
rarpboot - boot image via network using RARP/TFTP protocol
reset - Perform RESET of the CPU
rootfs_cp - copy rootfs to flash
rootfs_up - update root file system
run - run commands in an environment variable
saveenv - save environment variables to persistent storage
saves - save S-Record file over serial line
setenv - set environment variables
setfreq - change ddr/cpu frequency
sleep - delay execution for some time
test - minimal test like /bin/sh
tftpboot - boot image via network using TFTP protocol
uboot_cp - copy uboot to flash
uboot_up - update uboot
version - print monitor version
writemac - write mac address in I2C memory
u-boot>
```