

FusionServer Pro High-Density Servers

Upgrade Guide

Issue	19
Date	2024-09-02



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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

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

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy*. For details about this policy, visit the following web page:

<https://support.huawei.com/ecolumnsweb/en/warranty-policy>

Vulnerability

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

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

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

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

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices*. For details about this document, visit the following web page:

<https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789>

Huawei Enterprise End User License Agreement

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

<https://e.huawei.com/en/about/eula>

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy*. For details about this policy, visit the following web page:

<https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761>

About This Document

Purpose

This document describes how to upgrade the component firmware of Huawei FusionServer Pro high-density servers. The server types supported by each component and firmware upgrade methods vary depending on the hardware configuration. For details, see the upgrade procedure of each component.

Intended Audience

This document is intended for:

- Huawei technical support engineers
- Channel partners' technical support engineers
- Enterprise administrators

Symbol Conventions

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

Symbol	Description
	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

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

Issue	Date	Description
19	2024-09-02	This issue is the nineteenth official release. Added the procedure for upgrading the primary image of iBMC versions in x.xx.xx.xx format in 3.1.1.3.1 Performing the Upgrade .
18	2024-01-10	This issue is the eighteenth official release. Added version requirements in 3.1.2.2 Performing the Upgrade .
17	2023-09-20	This issue is the seventeenth official release. - Added 1.5 Upgrading the Controller Card Firmware Using hiraidadm. - Modified 3.10.1 Upgrading the Drive Backplane Expander Firmware Using the CLI (Linux).
16	2023-08-24	This issue is the sixteenth official release. Modified 2 Upgrading the NIC Firmware .

Issue	Date	Description
15	2023-07-07	This issue is the fifteenth official release. • Modified 1 Upgrading the RAID Controller Card Firmware. • Added 4 Upgrading the Drive Firmware. • Updated the name and link of SmartKit.
14	2023-06-07	This issue is the fourteenth official release. Added the description of upgrading the FBGF-RAD-R1-S1 RAID controller card.
13	2023-02-06	This issue is the thirteenth official release. Modified 3.10 Upgrading the Drive Backplane Expander Firmware.
12	2022-12-21	This issue is the twelfth official release. Added some precautions in 1 Upgrading the RAID Controller Card Firmware, 2 Upgrading the NIC Firmware, and 3 Upgrading the Firmware of Chassis Components.
11	2022-11-10	• Added the precautions for upgrading the BIOS in 3.2.1.1.1 Impact of the Upgrade and 3.2.1.3.1 Upgrade Procedure. • Changed the name and link of FusionServer Tools 2.0 SmartKit User Guide.

Issue	Date	Description
10	2021-08-24	Added 1.1 Before You Start for upgrading the RAID controller card firmware.
09	2021-07-26	- Added content about V6 servers. - Modified the method of obtaining the software package.
08	2020-06-19	Modified 3.10.1.3 Performing the Upgrade .
07	2020-05-22	Modified 3.2.1 Using the iBMC Web to Upgrade the BIOS .
06	2020-04-24	- Modified 3.1.1.1.3 Version Requirements. - Modified 3.1.1.3.1 Performing the Upgrade.
05	2020-03-31	- Modified 1.8.2 Performing the Upgrade. - Modified 3.1.2.2 Performing the Upgrade.
04	2020-03-21	- Added the description of upgrading the MSCC SmartRAID 3152-8i RAID controller card. - Added the description of upgrading the MSCC SmartHBA 2100-8i RAID controller card. - Added 3.13 Upgrading Smart Provisioning. - Modified the upgrade operations.
03	2019-11-25	This issue is the second official release.

Issue	Date	Description
02	2019-11-20	Modified 3.2.2 Upgrading the BIOS Using SmartKit .
01	2019-10-18	This issue is the first official release.

Contents

About This Document..... iii

1 Upgrading the RAID Controller Card Firmware..... 1

1.1 Before You Start..... 1

1.2 Upgrading the Controller Card Firmware Using a Script.....4

1.2.1 Before You Start..... 5

1.2.2 Preparing for the Upgrade.....5

1.2.2.1 Obtaining Software Packages..... 5

1.2.2.2 Verifying the Digital Signatures of Software Packages.....7

1.2.3 Performing the Upgrade.....7

1.2.4 Rolling Back a Version..... 10

1.2.4.1 Rollback Rules..... 10

1.2.4.2 Rollback Procedure..... 10

1.3 Upgrading the Controller Card Firmware Using StorCLI..... 10

1.3.1 Before You Start..... 10

1.3.2 Preparing for the Upgrade..... 11

1.3.2.1 Determining Source Version and Target Version..... 11

1.3.2.2 Obtaining Software Packages..... 11

1.3.2.3 Verifying the Digital Signatures of Software Packages..... 13

1.3.3 Performing the Upgrade..... 14

1.3.4 Rolling Back a Version..... 17

1.3.4.1 Rollback Rules..... 17

1.3.4.2 Rollback Procedure..... 17

1.3.5 Common Operations..... 17

1.3.5.1 Querying the Firmware Version of a Controller Card..... 17

1.4 Upgrading the Controller Card Firmware Using ARCCONF..... 18

1.4.1 Before You Start..... 18

1.4.2 Preparing for the Upgrade..... 19

1.4.2.1 Determining Source Version and Target Version..... 19

1.4.2.2 Obtaining Software Packages..... 19

1.4.2.3 Verifying the Digital Signatures of Software Packages..... 21

1.4.3 Performing the Upgrade..... 21

1.4.4 Rolling Back a Version..... 24

1.4.4.1 Rollback Rules..... 24

1.4.4.2 Rollback Procedure.....	24
1.4.5 Common Operations.....	24
1.4.5.1 Querying the Firmware Version of a Controller Card.....	24
1.5 Upgrading the Controller Card Firmware Using hiraidadm.....	25
1.5.1 Before You Start.....	25
1.5.2 Preparing for the Upgrade.....	26
1.5.2.1 Determining Source Version and Target Version.....	26
1.5.2.2 Obtaining Software Packages.....	26
1.5.2.3 Verifying the Digital Signatures of Software Packages.....	28
1.5.3 Performing the Upgrade.....	28
1.5.4 Rolling Back a Version.....	32
1.5.4.1 Rollback Rules.....	32
1.5.4.2 Rollback Procedure.....	32
1.5.5 Common Operations.....	32
1.5.5.1 Querying the Firmware Version of a Controller Card.....	32
1.6 Upgrading the Controller Card Firmware Using Smart Provisioning.....	34
1.6.1 Preparing for the Upgrade.....	34
1.6.1.1 Obtaining Software Packages.....	34
1.6.1.2 Verifying the Digital Signatures of Software Packages.....	36
1.6.2 Performing the Upgrade.....	36
1.6.3 Rolling Back a Version.....	36
1.6.3.1 Rollback Rules.....	36
1.6.3.2 Rollback Procedure.....	36
1.7 Upgrading the Controller Card Firmware Using SmartKit.....	37
1.7.1 Preparing for the Upgrade.....	37
1.7.1.1 Obtaining Software Packages.....	37
1.7.1.2 Verifying the Digital Signatures of Software Packages.....	38
1.7.2 Performing the Upgrade.....	39
1.7.3 Rolling Back a Version.....	39
1.7.3.1 Rollback Rules.....	39
1.7.3.2 Rollback Procedure.....	39
1.8 Upgrading the Controller Card Firmware Using FwUpgrade.....	40
1.8.1 Preparing for the Upgrade.....	40
1.8.1.1 Obtaining Software Packages.....	40
1.8.1.2 Verifying the Digital Signatures of Software Packages.....	41
1.8.2 Performing the Upgrade.....	41
1.8.3 Rolling Back a Version.....	42
1.8.3.1 Rollback Rules.....	42
1.8.3.2 Rollback Procedure.....	42
1.9 Upgrading the Controller Card Firmware Using Toolkit.....	42
1.9.1 Preparing for the Upgrade.....	42
1.9.1.1 Obtaining Software Packages.....	42

- 1.9.1.2 Verifying the Digital Signatures of Software Packages..... 43
- 1.9.2 Performing the Upgrade..... 44
- 1.9.3 Rolling Back the Firmware Version..... 51
 - 1.9.3.1 Rollback Rules..... 51
 - 1.9.3.2 Rollback Procedure..... 51
- 1.10 Others..... 51
 - 1.10.1 Upgrading the LSI SAS3108 RAID Controller Card Using CLI on VMware..... 51
 - 1.10.1.1 Preparing for the Upgrade..... 51
 - 1.10.1.1.1 Obtaining Software Packages..... 51
 - 1.10.1.1.2 Verifying the Digital Signatures of Software Packages..... 52
 - 1.10.1.2 Upgrade Procedure..... 53
 - 1.10.1.3 Rolling Back the Firmware Version..... 56
 - 1.10.1.3.1 Rollback Rules..... 56
 - 1.10.1.3.2 Rollback Procedure..... 56
 - 1.10.2 Upgrading the LSI SAS3108 RAID Controller Card Using CLI on Windows..... 56
 - 1.10.2.1 Preparing for the Upgrade..... 56
 - 1.10.2.1.1 Obtaining Software Packages..... 57
 - 1.10.2.1.2 Verifying the Digital Signatures of Software Packages..... 57
 - 1.10.2.2 Performing the Upgrade..... 58
 - 1.10.2.3 Rolling Back the Firmware Version..... 62
 - 1.10.2.3.1 Rollback Rules..... 62
 - 1.10.2.3.2 Rollback Procedure..... 62
- 2 Upgrading the NIC Firmware..... 63**
 - 2.1 Before You Start..... 63
 - 2.2 Upgrading the NIC Firmware Using a Script..... 64
 - 2.2.1 Preparing for the Upgrade..... 64
 - 2.2.1.1 Obtaining Software Packages..... 64
 - 2.2.1.2 Verifying the Digital Signatures of Software Packages..... 65
 - 2.2.2 Performing the Upgrade..... 65
 - 2.2.3 Rolling Back a Version..... 67
 - 2.2.3.1 Rollback Rules..... 67
 - 2.2.3.2 Rollback Procedure..... 67
 - 2.3 Upgrading the NIC Firmware Using Smart Provisioning..... 68
 - 2.3.1 Preparing for the Upgrade..... 68
 - 2.3.1.1 Obtaining Software Packages..... 68
 - 2.3.1.2 Verifying the Digital Signatures of Software Packages..... 69
 - 2.3.2 Performing the Upgrade..... 69
 - 2.3.3 Rolling Back a Version..... 69
 - 2.3.3.1 Rollback Rules..... 69
 - 2.3.3.2 Rollback Procedure..... 70
 - 2.4 Upgrading the NIC Firmware Using SmartKit..... 70
 - 2.4.1 Preparing for the Upgrade..... 70

2.4.1.1 Obtaining Software Packages.....	70
2.4.1.2 Verifying the Digital Signatures of Software Packages.....	71
2.4.2 Performing the Upgrade.....	71
2.4.3 Rolling Back a Version.....	71
2.4.3.1 Rollback Rules.....	71
2.4.3.2 Rollback Procedure.....	72
2.5 Upgrading the NIC Firmware Using FwUpgrade.....	72
2.5.1 Preparing for the Upgrade.....	72
2.5.1.1 Obtaining Software Packages.....	72
2.5.1.2 Verifying the Digital Signatures of Software Packages.....	73
2.5.2 Performing the Upgrade.....	74
2.5.3 Rolling Back a Version.....	74
2.5.3.1 Rollback Rules.....	74
2.5.3.2 Rollback Procedure.....	74
3 Upgrading the Firmware of Chassis Components.....	75
3.1 Upgrading the iBMC.....	75
3.1.1 Using the iBMC WebUI to Upgrade the iBMC.....	75
3.1.1.1 Before You Start.....	76
3.1.1.1.1 Impact of the Upgrade.....	76
3.1.1.1.2 Precautions.....	76
3.1.1.1.3 Version Requirements.....	77
3.1.1.2 Preparing for the Upgrade.....	77
3.1.1.2.1 Pre-upgrade Checklist.....	77
3.1.1.2.2 Obtaining the Upgrade Packages and Documents.....	78
3.1.1.2.3 Obtaining the Rollback Package.....	79
3.1.1.2.4 Verifying the Digital Signatures of Software Packages.....	79
3.1.1.3 Upgrading the iBMC.....	80
3.1.1.3.1 Performing the Upgrade.....	80
3.1.1.3.2 Verifying the Upgrade.....	84
3.1.1.4 Upgrading iBMC Language Packs.....	85
3.1.1.4.1 Upgrade Procedure.....	85
3.1.1.4.2 Verifying the Upgrade.....	87
3.1.1.5 Rolling Back the Firmware Version.....	88
3.1.1.5.1 Rollback Rules.....	88
3.1.1.5.2 Rollback Procedure.....	88
3.1.2 Upgrading iBMC Using SmartKit.....	88
3.1.2.1 Preparing for the Upgrade.....	88
3.1.2.1.1 Obtaining the Upgrade Package.....	89
3.1.2.1.2 Obtaining the Rollback Package.....	89
3.1.2.1.3 Verifying the Digital Signatures of Software Packages.....	90
3.1.2.2 Performing the Upgrade.....	90
3.1.2.3 Rolling Back a Version.....	91

3.1.2.3.1 Rollback Rules..... 91

3.1.2.3.2 Rollback Procedure..... 91

3.2 Upgrading the BIOS..... 91

3.2.1 Using the iBMC Web to Upgrade the BIOS..... 91

3.2.1.1 Before You Start..... 92

3.2.1.1.1 Impact of the Upgrade..... 92

3.2.1.1.2 Precautions..... 92

3.2.1.1.3 Version Requirements..... 93

3.2.1.1.4 Upgrade Process..... 93

3.2.1.2 Preparing for the Upgrade..... 93

3.2.1.2.1 Pre-upgrade Checklist..... 93

3.2.1.2.2 Obtaining the Upgrade Packages and Documents..... 94

3.2.1.2.3 Obtaining the Rollback Package..... 95

3.2.1.2.4 Verifying the Digital Signatures of Software Packages..... 95

3.2.1.3 Upgrading the BIOS..... 96

3.2.1.3.1 Upgrade Procedure..... 96

3.2.1.3.2 Verifying the Upgrade..... 100

3.2.1.4 Rolling Back the Firmware Version..... 101

3.2.1.4.1 Rollback Rules..... 101

3.2.1.4.2 Rollback Procedure..... 101

3.2.2 Upgrading the BIOS Using SmartKit..... 101

3.2.2.1 Preparing for the Upgrade..... 101

3.2.2.1.1 Obtaining Software Packages..... 101

3.2.2.1.2 Obtaining the Rollback Package..... 103

3.2.2.1.3 Verifying the Digital Signatures of Software Packages..... 103

3.2.2.2 Upgrade Procedure..... 103

3.2.2.3 Rolling Back the Firmware Version..... 104

3.2.2.3.1 Rollback Rules..... 104

3.2.2.3.2 Rollback Procedure..... 104

3.3 Upgrading the HMM..... 104

3.3.1 Using the iBMC Web to Upgrade the HMM..... 104

3.3.1.1 Before You Start..... 104

3.3.1.1.1 Impact of the Upgrade..... 104

3.3.1.1.2 Precautions..... 105

3.3.1.1.3 Version Requirements..... 105

3.3.1.1.4 Upgrade Process..... 106

3.3.1.2 Preparing for the Upgrade..... 107

3.3.1.2.1 Pre-upgrade Checklist..... 107

3.3.1.2.2 Obtaining the Upgrade Packages and Documents..... 107

3.3.1.2.3 Verifying the Digital Signatures of Software Packages..... 108

3.3.1.3 Upgrading the HMM..... 108

3.3.1.3.1 Upgrade Procedure..... 108

3.3.1.3.2 Verifying the Upgrade.....	111
3.3.1.4 Rolling Back the Firmware Version.....	111
3.3.1.4.1 Rollback Rules.....	111
3.3.1.4.2 Rollback Procedure.....	111
3.4 Upgrading the HMM CPLD.....	112
3.4.1 Preparing for the Upgrade.....	112
3.4.1.1 Obtaining Software Packages.....	112
3.4.1.2 Verifying the Digital Signatures of Software Packages.....	112
3.4.2 Upgrade Procedure.....	113
3.4.3 Rolling Back the Firmware Version.....	114
3.4.3.1 Rollback Rules.....	114
3.4.3.2 Rollback Procedure.....	114
3.5 Upgrading the Mainboard CPLD.....	114
3.5.1 Upgrading the Mainboard CPLD Using the iBMC WebUI.....	114
3.5.1.1 Preparing for the Upgrade.....	114
3.5.1.1.1 Obtaining Software Packages.....	114
3.5.1.1.2 Obtaining the Rollback Package.....	115
3.5.1.1.3 Verifying the Digital Signatures of Software Packages.....	115
3.5.1.2 Upgrade Procedure.....	116
3.5.1.3 Rolling Back the Firmware Version.....	119
3.5.1.3.1 Rollback Rules.....	119
3.5.1.3.2 Rollback Procedure.....	120
3.5.2 Using the iMana 200 to Upgrade the Mainboard CPLD.....	120
3.5.2.1 Preparing for the Upgrade.....	120
3.5.2.1.1 Obtaining Software Packages.....	120
3.5.2.1.2 Obtaining the Rollback Package.....	120
3.5.2.1.3 Verifying the Digital Signatures of Software Packages.....	121
3.5.2.2 Upgrade Procedure.....	121
3.5.2.3 Rolling Back the Firmware Version.....	123
3.5.2.3.1 Rollback Rules.....	123
3.5.2.3.2 Rollback Procedure.....	123
3.5.3 Upgrading the Mainboard CPLD Using SmartKit.....	124
3.5.3.1 Preparing for the Upgrade.....	124
3.5.3.1.1 Obtaining Software Packages.....	124
3.5.3.1.2 Obtaining the Rollback Package.....	125
3.5.3.1.3 Verifying the Digital Signatures of Software Packages.....	126
3.5.3.2 Upgrade Procedure.....	126
3.5.3.3 Rolling Back the Firmware Version.....	126
3.5.3.3.1 Rollback Rules.....	126
3.5.3.3.2 Rollback Procedure.....	126
3.6 Upgrading the Hard Drive Backplane CPLD.....	127
3.6.1 Upgrading the Drive Backplane CPLD Using the iBMC WebUI.....	127

3.6.1.1 Preparing for the Upgrade.....	127
3.6.1.1.1 Obtaining Software Packages.....	127
3.6.1.1.2 Verifying the Digital Signatures of Software Packages.....	127
3.6.1.2 Upgrade Procedure.....	127
3.6.1.3 Rolling Back the Firmware Version.....	131
3.6.1.3.1 Rollback Rules.....	131
3.6.1.3.2 Rollback Procedure.....	131
3.6.2 Using the iMana 200 to Upgrade the Hard Disk Backplane CPLD.....	131
3.6.2.1 Preparing for the Upgrade.....	131
3.6.2.1.1 Obtaining Software Packages.....	131
3.6.2.1.2 Verifying the Digital Signatures of Software Packages.....	132
3.6.2.2 Upgrade Procedure.....	132
3.6.2.3 Rolling Back the Firmware Version.....	134
3.6.2.3.1 Rollback Rules.....	134
3.6.2.3.2 Rollback Procedure.....	134
3.6.3 Upgrading the Drive Backplane CPLD Using SmartKit.....	135
3.6.3.1 Preparing for the Upgrade.....	135
3.6.3.1.1 Obtaining Software Packages.....	135
3.6.3.1.2 Verifying the Digital Signatures of Software Packages.....	136
3.6.3.2 Upgrade Procedure.....	136
3.6.3.3 Rolling Back the Firmware Version.....	136
3.6.3.3.1 Rollback Rules.....	136
3.6.3.3.2 Rollback Procedure.....	137
3.7 Upgrading the Fan Management Board CPLD.....	137
3.7.1 Upgrading the CPLD of the Fan Module Using the iBMC WebUI.....	137
3.7.1.1 Preparing for the Upgrade.....	137
3.7.1.1.1 Obtaining Software Packages.....	137
3.7.1.1.2 Verifying the Digital Signatures of Software Packages.....	137
3.7.1.2 Upgrade Procedure.....	138
3.7.1.3 Rollback.....	140
3.7.1.3.1 Rollback Rules.....	140
3.7.1.3.2 Rollback Procedure.....	140
3.8 Upgrading the Riser Card CPLD.....	140
3.8.1 Upgrading the Riser Card CPLD Using the iBMC WebUI.....	140
3.8.1.1 Preparing for the Upgrade.....	140
3.8.1.1.1 Obtaining Software Packages.....	140
3.8.1.1.2 Verifying the Digital Signatures of Software Packages.....	141
3.8.1.2 Upgrade Procedure.....	141
3.8.1.3 Rolling Back the Firmware Version.....	144
3.8.1.3.1 Rollback Rules.....	145
3.8.1.3.2 Rollback Procedure.....	145
3.8.2 Using the iMana 200 to Upgrade the Riser Card CPLD.....	145

3.8.2.1 Preparing for the Upgrade.....	145
3.8.2.1.1 Obtaining Software Packages.....	145
3.8.2.1.2 Verifying the Digital Signatures of Software Packages.....	145
3.8.2.2 Upgrade Procedure.....	146
3.8.2.3 Rolling Back the Firmware Version.....	148
3.8.2.3.1 Rollback Rules.....	148
3.8.2.3.2 Rollback Procedure.....	148
3.8.3 Upgrading the Riser Card CPLD Using SmartKit.....	148
3.8.3.1 Preparing for the Upgrade.....	148
3.8.3.1.1 Obtaining Software Packages.....	148
3.8.3.1.2 Verifying the Digital Signatures of Software Packages.....	149
3.8.3.2 Upgrade Procedure.....	150
3.8.3.3 Rolling Back the Firmware Version.....	150
3.8.3.3.1 Rollback Rules.....	150
3.8.3.3.2 Rollback Procedure.....	150
3.9 Upgrading the LCD Firmware.....	150
3.9.1 Upgrading the LCD Firmware Using the iBMC WebUI.....	150
3.9.1.1 Preparing for the Upgrade.....	150
3.9.1.1.1 Obtaining Software Packages.....	150
3.9.1.1.2 Verifying the Digital Signatures of Software Packages.....	151
3.9.1.2 Upgrade Procedure.....	151
3.9.1.3 Rolling Back the Firmware Version.....	154
3.9.1.3.1 Rollback Rules.....	154
3.9.1.3.2 Rollback Procedure.....	154
3.9.2 Using the iMana 200 to Upgrade the LCD Firmware.....	154
3.9.2.1 Preparing for the Upgrade.....	154
3.9.2.1.1 Obtaining Software Packages.....	154
3.9.2.1.2 Verifying the Digital Signatures of Software Packages.....	154
3.9.2.2 Upgrade Procedure.....	155
3.9.2.3 Rolling Back the Firmware Version.....	156
3.9.2.3.1 Rollback Rules.....	156
3.9.2.3.2 Rollback Procedure.....	156
3.9.3 Using SmartKit to Upgrade the LCD Firmware.....	157
3.9.3.1 Preparing for the Upgrade.....	157
3.9.3.1.1 Obtaining Software Packages.....	157
3.9.3.1.2 Verifying the Digital Signatures of Software Packages.....	158
3.9.3.2 Upgrade Procedure.....	158
3.9.3.3 Rolling Back the Firmware Version.....	158
3.9.3.3.1 Rollback Rules.....	158
3.9.3.3.2 Rollback Procedure.....	159
3.10 Upgrading the Drive Backplane Expander Firmware.....	159
3.10.1 Upgrading the Drive Backplane Expander Firmware Using the CLI (Linux).....	159

3.10.1.1 Before You Start.....	159
3.10.1.2 Preparing for the Upgrade.....	160
3.10.1.2.1 Obtaining Software Packages.....	160
3.10.1.2.2 Verifying the Digital Signatures of Software Packages.....	160
3.10.1.3 Performing the Upgrade.....	160
3.10.1.4 Rolling Back a Version.....	164
3.10.1.4.1 Rollback Rules.....	164
3.10.1.4.2 Rollback Procedure.....	164
3.11 Upgrading the SD Card Controller Firmware.....	164
3.11.1 Upgrading the SD Card Controller Firmware Using the iBMC WebUI.....	164
3.11.1.1 Preparing for the Upgrade.....	164
3.11.1.1.1 Obtaining Software Packages.....	164
3.11.1.1.2 Verifying the Digital Signatures of Software Packages.....	165
3.11.1.2 Upgrade Procedure.....	165
3.11.1.3 Rolling Back the Firmware Version.....	168
3.11.1.3.1 Rollback Rules.....	168
3.11.1.3.2 Rollback Procedure.....	168
3.11.2 Upgrading the SD Card Controller Firmware Using SmartKit.....	168
3.11.2.1 Preparing for the Upgrade.....	168
3.11.2.1.1 Obtaining Software Packages.....	168
3.11.2.1.2 Verifying the Digital Signatures of Software Packages.....	169
3.11.2.2 Upgrade Procedure.....	170
3.11.2.3 Rolling Back the Firmware Version.....	170
3.11.2.3.1 Rollback Rules.....	170
3.11.2.3.2 Rollback Procedure.....	170
3.12 Upgrading the PSUs.....	170
3.12.1 Preparing for the Upgrade.....	170
3.12.1.1 Obtaining Software Packages.....	170
3.12.1.2 Verifying the Digital Signatures of Software Packages.....	171
3.12.2 Performing the Upgrade.....	171
3.12.3 Rolling Back the Firmware Version.....	172
3.12.3.1 Rollback Rules.....	172
3.12.3.2 Rollback Procedure.....	173
3.13 Upgrading Smart Provisioning.....	173
3.13.1 Upgrade Using Smart Provisioning.....	173
3.13.2 Upgrading Smart Provisioning Using SmartKit.....	173
4 Upgrading the Drive Firmware.....	174
5 Common Operations.....	175
5.1 Querying the IP Address of the iBMC Management Network Port.....	175
5.1.1 Querying the IP Address of the iBMC Management Network Port (Romley/Brickland/Grantley Platform).....	176

5.1.2 Querying the IP Address of the iBMC Management Network Port (Purley/Cedar Island/Whitley Platform)..... 179

5.1.3 Querying the IP Address of the iBMC Management Network Port Using SSH.....183

5.2 Logging In to the iBMC WebUI.....185

5.2.1 Logging In to the iBMC WebUI (iBMC Earlier Than V561)..... 185

5.2.2 Logging In to the iBMC WebUI (iBMC V561 or Later, or iBMC V3.01.00.00 or Later).....189

5.3 Logging In Using the iMana 200 WebUI.....193

5.4 Logging In Using the iBMC WebUI..... 196

5.5 Logging In to the iBMC CLI.....200

5.6 Transferring Files Using the Local Directory..... 203

5.7 Check the Software Version of the Server Node..... 204

5.8 Viewing Server Node Alarms.....205

5.9 Checking the HMM Software Version..... 206

5.10 Viewing HMM Alarm Information..... 207

5.11 Logging In to the Server Over a Network Port by Using PuTTY..... 208

5.12 Transferring Files Using WinSCP..... 210

5.13 Logging In to the Management Module CLI Through the Management Network Port..... 211

5.14 Logging In to the Management Module CLI Through the Management IP Address of the Server Node.....215

1 Upgrading the RAID Controller Card Firmware

NOTICE

After the firmware is upgraded, if you need to restart or power cycle the server for the firmware to take effect, services will be interrupted. Exercise caution when performing this operation.

1.1 Before You Start

1.2 Upgrading the Controller Card Firmware Using a Script

1.3 Upgrading the Controller Card Firmware Using StorCLI

1.4 Upgrading the Controller Card Firmware Using ARCCONF

1.5 Upgrading the Controller Card Firmware Using hiraidadm

1.6 Upgrading the Controller Card Firmware Using Smart Provisioning

1.7 Upgrading the Controller Card Firmware Using SmartKit

1.8 Upgrading the Controller Card Firmware Using FwUpgrade

1.9 Upgrading the Controller Card Firmware Using Toolkit

1.10 Others

1.1 Before You Start

NOTICE

Before the upgrade, read the [Firmware Release Notes](#) of each controller card to understand the version changes, features, and precautions.

- To check the compatibility between servers and NICs, use the [Computing Product Compatibility Checker](#).

- Before using a tool to upgrade the controller card firmware, check the servers supported by the tool.
 - Smart Provisioning: See **Product Overview > Software and Hardware Compatibility** in the [Smart Provisioning User Guide](#).
 - SmartKit Computing: See **Using SmartKit > Firmware Upgrade > Upgrading Server Firmware > Compatibility List** in the [SmartKit Computing User Guide](#).
 - The controller card firmware can be upgraded using FwUpgrade only on V2 and V3 servers.
 - The controller card firmware can be upgraded using Toolkit only on V2 and V3 servers.
- Check the upgrade methods supported by the controller card firmware package. Before downloading the firmware package, read the software description of the firmware package, as shown in **Figure 1-1**.

Figure 1-1 Firmware package software description

☐ NIC-SP670-1822-FW-15.7.6.1-X86.zip FW file, support for Mount Smart Provisioning 1.2.1 on SmartKit	2.22MB	2023-06-30	1	↓	pgp	cms
☐ NIC-SP680-1822-FW-15.7.6.1-X86.zip FW file, support for Mount Smart Provisioning 1.2.1 on SmartKit	2.22MB	2023-06-30	0	↓	pgp	cms
☐ NIC-SP681-1822-FW-15.7.6.1-X86.zip FW file, support for Mount Smart Provisioning 1.2.1 on SmartKit	2.22MB	2023-06-30	0	↓	pgp	cms

[Download](#) [Comment](#)

- The upgrade method varies depending on the controller card type. For details, see **Table 1-1**.

Table 1-1 Mapping between upgrade methods and controller card models

Upgrade Method	Supported Controller Card Model
1.3 Upgrading the Controller Card Firmware Using StorCLI	• LSI SAS2208 • LSI SAS3108^a • Avago SAS3004iMR • Avago SAS3408iMR • Avago SAS3416iMR • Avago SAS3416IT • Avago SAS3508 • Avago SAS3516 • LSI SAS9305-24i • Avago MegaRAID SAS 9440-8i • Avago MegaRAID SAS 9460-8i • Avago MegaRAID SAS 9460-16i

Upgrade Method	Supported Controller Card Model
1.4 Upgrading the Controller Card Firmware Using ARCCONF	• MSCC SmartRAID 3152-8i • MSCC SmartHBA 2100-8i • PM8060 • PM8068 • FBGF-RAD-R1-S1
1.5 Upgrading the Controller Card Firmware Using hiraidadm	• SP686C
1.6 Upgrading the Controller Card Firmware Using Smart Provisioning	• LSI SAS3008IR • LSI SAS3008IT • LSI SAS3108 • Avago SAS3004iMR • Avago SAS3408iMR • Avago SAS3416iMR • Avago SAS3416IT • Avago SAS3508 • Avago SAS3516 • MSCC SmartRAID 3152-8i • MSCC SmartHBA 2100-8i • Avago MegaRAID SAS 9440-8i • Avago MegaRAID SAS 9460-8i • Avago MegaRAID SAS 9460-16i • FBGF-RAD-R1-S1

Upgrade Method	Supported Controller Card Model
1.7 Upgrading the Controller Card Firmware Using SmartKit	• LSI SAS2208 • LSI SAS2308 • LSI SAS3008IR • LSI SAS3008IT • LSI SAS3108 • Avago SAS3004iMR • Avago SAS3408iMR • Avago SAS3416iMR • Avago SAS3416IT • Avago SAS3508 • Avago SAS3516 • MSCC SmartRAID 3152-8i • MSCC SmartHBA 2100-8i • LSI SAS9305-24i • Avago MegaRAID SAS 9440-8i • Avago MegaRAID SAS 9460-8i • Avago MegaRAID SAS 9460-16i • FBGF-RAD-R1-S1
1.9 Upgrading the Controller Card Firmware Using Toolkit	• LSI SAS2308 • LSI SAS3008IR
1.8 Upgrading the Controller Card Firmware Using FwUpgrade	• LSI SAS2208 • LSI SAS2308 • LSI SAS3008IR • LSI SAS3008IT • LSI SAS3108
a: The firmware of the LSI SAS3108 controller card can be upgraded using the StorCLI command line tool in VMware and Windows. For details about the upgrade in VMware, see 1.10.1 Upgrading the LSI SAS3108 RAID Controller Card Using CLI on VMware. For details about the upgrade in Windows, see 1.10.2 Upgrading the LSI SAS3108 RAID Controller Card Using CLI on Windows.	

1.2 Upgrading the Controller Card Firmware Using a Script

1.2.1 Before You Start

Upgrade Scope

For details about the servers supported by the controller card, use the [Computing Product Compatibility Checker](#) to check.

You can use the script to perform the upgrade only on Linux. For details about the OSs supported by a server, use the [Computing Product Compatibility Checker](#).

Impact of the Upgrade

After the upgrade, power cycle the server for the latest firmware version to take effect. Power cycling will interrupt services.

Precautions

Observe the precautions listed in [Table 1-2](#) during the upgrade.

Table 1-2 Precautions for the upgrade

No.	Description
1	Misoperations during the firmware upgrade may cause upgrade failure and make the controller card unavailable.
2	Stop running services on the server before the upgrade.
3	Do not perform any power-off operation during the upgrade and do not change configurations except for those involved in the upgrade guide.
4	Before the upgrade, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to the document, contact technical support.

1.2.2 Preparing for the Upgrade

1.2.2.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-3](#).

Table 1-3 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

Software package description

[Table 1-4](#) lists the files contained in the controller card firmware upgrade package.

Table 1-4 Software package description

File	Description
drivers folder	(Optional) Driver file matching the firmware version. The firmware package may not contain this folder or does not contain the driver of a specified OS. In this case, download the driver by referring to "Procedure".
tools folder	Command line management tool of the control card.

File	Description
• *.rom • *.bin • *.img	Controller card firmware.
	Script file for automatic firmware upgrade.
install.sh	Script file for automatic firmware upgrade.
version.xml	Version description file.

1.2.2.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.2.3 Performing the Upgrade

Prerequisites

- The server hosting the controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.4 Logging In Using the iBMC WebUI](#).
- You have downloaded the OS driver package to the client (such as a PC), and decompressed the package to obtain the driver image.
- You have downloaded the controller card firmware upgrade package to the client (such as a PC) and decompressed it.

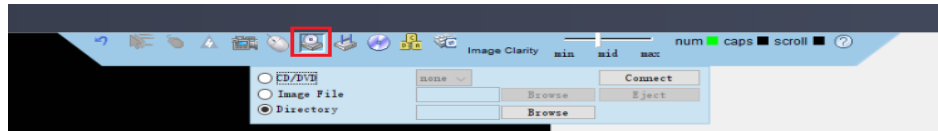
Procedure

Step 1 Mount the upgrade file.

NOTE

The iBMC Remote Virtual Consoles include the Java Remote Virtual Console and HTML5 Integrated Remote Console. The HTML5 Integrated Remote Console does not support local directories. This section uses the Java Remote Virtual Console as an example. For more information, see the [iBMC User Guide](#).

1. On the toolbar of the virtual console, click  to display the screen shown in [Figure 1-2](#).

Figure 1-2 Virtual CD/DVD drive

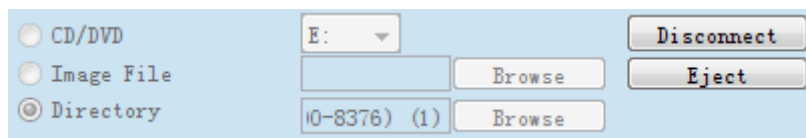
2. Select **Directory** and click **Browse**.
3. Select the folder generated after the controller card firmware upgrade package is decompressed.

NOTE

Select the folder of the target version for an upgrade or the folder of the source version for a rollback.

4. Click **Connect**.

If the **Eject** icon is available, as shown in [Figure 1-3](#), the file is successfully mounted.

Figure 1-3 Toolbar

Step 2 Copy the upgrade file to the server and grant the read and write permissions to the file.

1. On the OS, run the **mkdir fw** command to create the **fw** folder in the **root** directory.
2. Run the **mount /dev/sr0 /mnt** command to mount the local folder to the **/mnt** directory.

NOTE

After you enter **mount /dev/sr**, press **Tab** to display the value following **sr**.

3. Run the **cp -vr /mnt/* /root/fw/** command to copy the mounted file to the **fw** directory.
4. Run the **cd /root/fw/** command to go to the **fw** directory.
5. Run the **chmod 777 *** command to add read and write permissions for the file.

Step 3 Run the following command to upgrade the controller card firmware using the one-click upgrade script:

./install.sh upgrade or bash install.sh upgrade

NOTE

- If the server has multiple controller cards of the same model, the script automatically upgrades the firmware of all these controller cards to the target version.
- You can run the **cat work.log** command to open the **work.log** file to view the upgrade log information.

Step 4 Power off and then power on the server for the firmware to take effect. The procedure is as follows:

1. Click  on the toolbar of the virtual console, and choose **Power Off** from the drop-down list.
2. After the server is powered off, click  on the toolbar of the virtual console, and choose **Power On** from the drop-down list.

NOTE

It takes about 5 to 10 minutes to start the server.

Step 5 Check whether the firmware version after the upgrade is the target version. To check the controller card firmware version, perform the following steps:

- Log in to the iBMC WebUI. For details, see **iBMC WebUI > System > Storage Management** in the [iBMC User Guide](#).

NOTE

The controller card must support out-of-band management. You can use the [Computing Product Compatibility Checker](#) to check whether a controller card supports out-of-band management.

- Log in to the BIOS management page of the controller card, and see the value of **Firmware Version** on the **Controller Management** page. For details, see **Common Tasks > Querying the Firmware Version of a RAID Controller Card** in the *RAID Controller Card User Guide*.
 - For V2 and V3 servers, see the [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
 - For V5 servers, see the [Huawei Server RAID Controller Card User Guide \(x86\)](#).
 - For V6 servers, see the [Huawei V6 Server RAID Controller Card User Guide](#).
- Use the CLI tool on the OS. For details, see the CLI tool section for the corresponding controller card in the *RAID Controller Card User Guide*.
 - For V2 and V3 servers, see the [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
 - For V5 servers, see the [Huawei Server RAID Controller Card User Guide \(x86\)](#).
 - For V6 servers, see the [Huawei V6 Server RAID Controller Card User Guide](#).

Step 6 (Optional) Upgrade the controller card driver to a version that matches the firmware.

For details about how to obtain and upgrade the driver, see section "Installing and Upgrading Drivers and Firmware" in the [Huawei Server OS Installation Guide \(x86\)](#).

----End

1.2.4 Rolling Back a Version

1.2.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

1.2.4.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.2.3 Performing the Upgrade](#).

----End

1.3 Upgrading the Controller Card Firmware Using StorCLI

1.3.1 Before You Start

Upgrade Scope

For details about the servers supported by the controller card, use the [Computing Product Compatibility Checker](#) to check.

This upgrade method applies to the following controller cards:

- LSI SAS2208
- LSI SAS3108^a
- Avago SAS3004iMR
- Avago SAS3408iMR
- Avago SAS3416iMR
- Avago SAS3416IT
- Avago SAS3508
- Avago SAS3516
- LSI SAS9305-24i
- Avago MegaRAID SAS 9440-8i

- Avago MegaRAID SAS 9460-8i
- Avago MegaRAID SAS 9460-16i

Impact of the Upgrade

After the upgrade, power cycle the server for the latest firmware version to take effect. Power cycling will interrupt services.

Precautions

Observe the precautions listed in [Table 1-5](#) during the upgrade.

Table 1-5 Precautions for the upgrade

No.	Description
1	Misoperations during the firmware upgrade may cause upgrade failure and make the controller card unavailable.
2	Stop running services on the server before the upgrade.
3	Do not perform any power-off operation during the upgrade and do not change configurations except for those involved in the upgrade guide.
4	Before the upgrade, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to the document, contact technical support.

1.3.2 Preparing for the Upgrade

1.3.2.1 Determining Source Version and Target Version

Before upgrading the controller card firmware, determine the source firmware version and the target firmware version. This information is required for a rollback. For details, see [1.3.5.1 Querying the Firmware Version of a Controller Card](#).

1.3.2.2 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-6](#).

Table 1-6 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

Software Package Description

[Table 1-7](#) lists the files contained in the controller card firmware upgrade package.

Table 1-7 Software package description

File	Description
drivers folder	(Optional) Driver file matching the firmware version. The firmware package may not contain this folder or does not contain the driver of a specified OS. In this case, download the driver by referring to "Procedure".
tools folder	Command line management tool of the control card.

File	Description
*.rom	Controller card firmware. • When you upgrade the firmware of the Avago SAS3004iMR, Avago SAS3108, Avago SAS3508, or Avago SAS3516, the firmware package may contain the following two ROM files: – xxFW4.rom: used to upgrade the RAID controller card online. – xxFW16.rom: used for burning during production. • When you upgrade the LSI SAS2208 firmware, the upgrade package may contain the following two ROM files: – 2208FW8.rom: used to upgrade the RAID controller card that contains RAID configuration information. – 2208FW32.rom: used to upgrade the RAID controller card that does not contain RAID configuration information or upgrade the RAID controller card in DOS.
install.sh	Script file for automatic firmware upgrade.
version.xml	Version description file.

1.3.2.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.3.3 Performing the Upgrade

NOTICE

- Stop running services on the server before the upgrade.
- Do not power off the OS during the upgrade and do not change configurations except for those involved in the upgrade guide.

Scenarios

Upgrade the controller card firmware using the StorCLI on an operating system (OS).

Prerequisites

- The server hosting the controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).
- You have downloaded the OS driver package to the client (such as a PC), and decompressed the package to obtain the driver image.
- You have downloaded the controller card firmware upgrade package to the client (such as a PC) and decompressed it.

Procedure

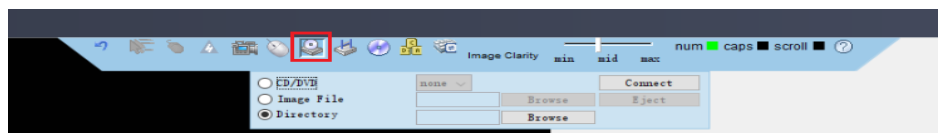
Step 1 Mount the upgrade file.

NOTE

The iBMC Remote Virtual Consoles include the Java Remote Virtual Console and HTML5 Integrated Remote Console. The HTML5 Integrated Remote Console does not support local directories. This section uses the Java Remote Virtual Console as an example. For more information, see the [iBMC User Guide](#).

1. On the toolbar of the virtual console, click  to display the screen shown in [Figure 1-4](#).

Figure 1-4 Virtual CD/DVD drive



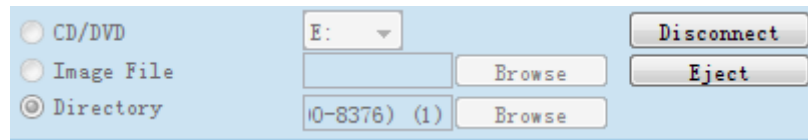
2. Select **Directory** and click **Browse**.
3. Select the folder generated after the controller card firmware upgrade package is decompressed.

NOTE

Select the folder of the target version for an upgrade or the folder of the source version for a rollback.

4. Click **Connect**.

If the **Eject** icon is available, as shown in [Figure 1-5](#), the file is successfully mounted.

Figure 1-5 Toolbar

Step 2 Copy the upgrade file to the server and grant the read and write permissions to the file.

1. On the OS, run the **mkdir fw** command to create the **fw** folder in the **root** directory.
2. Run the **mount /dev/sr0 /mnt** command to mount the local folder to the **/mnt** directory.

NOTE

After you enter **mount /dev/sr**, press **Tab** to display the value following **sr**.

3. Run the **cp -vr /mnt/* /root/fw/** command to copy the mounted file to the **fw** directory.
4. Run the **cd /root/fw/** command to go to the **fw** directory.
5. Run the **cp -vr /tools/* /root/fw/** command to copy the mounted file to the **fw** directory.
6. Run the **chmod 777 *** command to add read and write permissions for the file.

Step 3 Run the **./storcli64 show** command to view the controller IDs of all controller cards that support the StorCLI in the system.

Assume that a server has one Avago SAS3508.

```
[root@localhost ~]# ./storcli64 show
```

```
Status Code = 0
```

```
Status = Success
```

```
Description = None
```

```
Number of Controllers = 1
```

```
...
```

```
System Overview :
```

```
=====
```

```
-----  
Ctl Model  Ports PDs DGs DNOpt VDs VNOpt BBU sPR DS  EHS ASOs Hlth  
-----
```

```
0 SAS3508   8  3  1   0  1   0 Opt On 1&2 Y   3 Opt  
-----
```

Step 4 Run the **./storcli64 /cController_ID download file=xxxx.rom [noverchk]** command to upgrade the firmware of a specified controller card.

 NOTE

- *Controller_ID* indicates the value of **Ctl** queried in [Step 3](#).
- If **Status = Success** is displayed in the command output, the command is executed successfully.
- **xxxx.rom** indicates the firmware package name. The firmware package name varies depending on the controller card. For details, see the ROM file in the controller card software package.
- When you upgrade the firmware of the Avago SAS3004iMR, Avago SAS3108, Avago SAS3508, or Avago SAS3516, the firmware package may contain the following two ROM files:
 - **xxFW4.rom**: used to upgrade the RAID controller card online.
 - **xxFW16.rom**: used for burning during production.
- When you upgrade the LSI SAS2208 firmware, the upgrade package may contain the following two ROM files:
 - **2208FW8.rom**: used to upgrade the RAID controller card that contains RAID configuration information.
 - **2208FW32.rom**: used to upgrade the RAID controller card that does not contain RAID configuration information or upgrade the RAID controller card in DOS.

Upgrade the firmware of the Avago SAS3508 whose ID is 0.

```
[root@localhost fw]# ./storcli64 /c0 download file =3508FW4.rom noverchk
```

Download Completed.

Flashing image to adapter...

Controller = 0

Status = Success

Description = F/W Flash Completed.Please reboot the system for the changes to take effect.

Step 5 Power off and then power on the server for the firmware to take effect. The procedure is as follows:

1. Click  on the toolbar of the virtual console, and choose **Power Off** from the drop-down list.
2. After the server is powered off, click  on the toolbar of the virtual console, and choose **Power On** from the drop-down list.

 NOTE

It takes about 5 to 10 minutes to start the server.

Step 6 Check whether the firmware version after the upgrade is the target version. For details about how to query the controller card firmware version, see [1.3.5.1 Querying the Firmware Version of a Controller Card](#).

If no error information is displayed during the upgrade process and the version queried after the upgrade is the target version, the upgrade is successful.

Step 7 (Optional) Upgrade the controller card driver to a version that matches the firmware.

For details about how to obtain and upgrade the driver, see section "Installing and Upgrading Drivers and Firmware" in the [Huawei Server OS Installation Guide \(x86\)](#).

----End

1.3.4 Rolling Back a Version

1.3.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.3.4.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.3.3 Performing the Upgrade](#).

-----End

1.3.5 Common Operations

1.3.5.1 Querying the Firmware Version of a Controller Card

You can use any of the following methods to query the controller card firmware version:

- Log in to the iBMC WebUI. For details, see **iBMC WebUI > System > Storage Management** in the [iBMC User Guide](#).

NOTE

The controller card must support out-of-band management. You can use the [Computing Product Compatibility Checker](#) to check whether a controller card supports out-of-band management.

- Log in to the BIOS management page of the controller card, and see the value of **Firmware Version** on the **Controller Management** page. For details, see **Common Tasks > Querying the Firmware Version of a RAID Controller Card** in the *RAID Controller Card User Guide*.
 - For V2 and V3 servers, see the [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
 - For V5 servers, see the [Huawei Server RAID Controller Card User Guide \(x86\)](#).
 - For V6 servers, see the [Huawei V6 Server RAID Controller Card User Guide](#).
- Use the StorCLI on the OS.

Query the firmware version of the Avago SAS3508. The **FW Version** field in the command output indicates the firmware version of the controller card.

```
[root@localhost fw]# ./storcli64 /c0 show
```

Generating detailed summary of the adapter, it may take a while to complete.

```
Controller = 0  
Status = Success  
Description = None
```

```
Product Name = SAS3508  
Serial Number = FW-00000000  
SAS Address = 5000000012345678  
PCI Address = 00:1b:00:00  
System Time = 11/14/2016 00:10:45  
Mfg. Date = 00/00/00  
Controller Time = 11/13/2016 16:10:45  
FW Package Build = 50.1.0-0537  
BIOS Version = 07.01.05.1_4.17.08.00_0x07010701  
FW Version = 5.010.00-0755  
Driver Name = megaraid_sas  
Driver Version = 07.701.17.00  
.....
```

1.4 Upgrading the Controller Card Firmware Using ARCCONF

1.4.1 Before You Start

Upgrade Scope

For details about the servers supported by the controller card, use the [Computing Product Compatibility Checker](#) to check.

This upgrade method applies to the following controller cards:

- MSCC SmartRAID 3152-8i
- MSCC SmartHBA 2100-8i
- PM8060
- PM8068
- FBGF-RAD-R1-S1

Impact of the Upgrade

After the upgrade, power cycle the server for the latest firmware version to take effect. Power cycling will interrupt services.

Precautions

Observe the precautions listed in [Table 1-8](#) during the upgrade.

Table 1-8 Precautions for the upgrade

No.	Description
1	Misoperations during the firmware upgrade may cause upgrade failure and make the controller card unavailable.
2	Stop running services on the server before the upgrade.
3	Do not perform any power-off operation during the upgrade and do not change configurations except for those involved in the upgrade guide.
4	Before the upgrade, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to the document, contact technical support.

1.4.2 Preparing for the Upgrade

1.4.2.1 Determining Source Version and Target Version

Before upgrading the controller card firmware, determine the source firmware version and the target firmware version. This information is required for a rollback. For details, see [1.4.5.1 Querying the Firmware Version of a Controller Card](#).

1.4.2.2 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-9](#).

Table 1-9 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

Software Package Description

[Table 1-10](#) lists the files contained in the controller card firmware upgrade package.

Table 1-10 Software package description

File	Description
drivers folder	(Optional) Driver file matching the firmware version. The firmware package may not contain this folder or does not contain the driver of a specified OS. In this case, download the driver by referring to "Procedure".
tools folder	Command line management tool of the control card.
fw.crl	(Optional) Certificate revocation list (CRL).
*.bin	Controller card firmware.

File	Description
*.bin.cms	(Optional) Automatic signature verification.
install.sh	Script file for automatic firmware upgrade.
version.xml	Version description file.

1.4.2.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.4.3 Performing the Upgrade

NOTICE

- Stop running services on the server before the upgrade.
- Do not power off the OS during the upgrade and do not change configurations except for those involved in the upgrade guide.

Scenarios

Upgrade the controller card firmware using the ARCCONF on an OS.

Prerequisites

- The server hosting the controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).
- You have downloaded the OS driver package to the client (such as a PC), and decompressed the package to obtain the driver image.
- You have downloaded the controller card firmware upgrade package to the client (such as a PC) and decompressed it.

Procedure

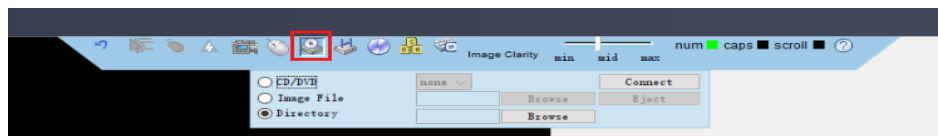
Step 1 Mount the upgrade file.

NOTE

The iBMC Remote Virtual Consoles include the Java Remote Virtual Console and HTML5 Integrated Remote Console. The HTML5 Integrated Remote Console does not support local directories. This section uses the Java Remote Virtual Console as an example. For more information, see the [iBMC User Guide](#).

1. On the toolbar of the virtual console, click  to display the screen shown in [Figure 1-6](#).

Figure 1-6 Virtual CD/DVD drive



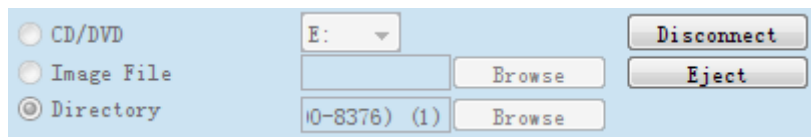
2. Select **Directory** and click **Browse**.
3. Select the folder generated after the controller card firmware upgrade package is decompressed.

NOTE

Select the folder of the target version for an upgrade or the folder of the source version for a rollback.

4. Click **Connect**.
If the **Eject** icon is available, as shown in [Figure 1-7](#), the file is successfully mounted.

Figure 1-7 Toolbar



Step 2 Copy the upgrade file to the server and grant the read and write permissions to the file.

1. On the OS, run the **mkdir fw** command to create the **fw** folder in the **root** directory.
2. Run the **mount /dev/sr0 /mnt** command to mount the local folder to the **/mnt** directory.

NOTE

After you enter **mount /dev/sr**, press **Tab** to display the value following **sr**.

3. Run the **cp -vr /mnt/* /root/fw/** command to copy the mounted file to the **fw** directory.
4. Run the **cd /root/fw/** command to go to the **fw** directory.
5. Run the **cp -vr /tools/* /root/fw/** command to copy the mounted file to the **fw** directory.

6. Run the **chmod 777 *** command to add read and write permissions for the file.

Step 3 Run the **./arccnf list** command to view the IDs of all controller cards that support the ARCCNF on a server.

Assume that the server has one MSCC SmartRAID 3152-8i.

```
[root@localhost ~]# ./arccnf list
Controllers found: 1

-----
Controller information
-----
Controller ID      : Status, Slot, Mode, Name, SerialNumber, WWN
-----
Controller 1:      : Optimal, Slot 1, Mixed, MSCC Adaptec SmartRAID 3152-8i, 7A45F30016A,
50000D1E00189F30

Command completed successfully.
```

Step 4 Run the **./arccnf romupdate *Controller_ID* XXX.bin [noprompt]** command to upgrade the controller card firmware.

Upgrade the firmware of the MSCC SmartRAID 3152-8i controller card whose ID is 1.

```
[root@linux 2.93]# ./arccnf romupdate 1 SmartFWx100.bin
Controllers found: 1

Are you sure you want to continue?
Press y, then ENTER to continue or press ENTER to abort: y

Updating controller 1 firmware...
Succeeded
You must restart the system for firmware updates to take effect.

Command completed successfully.
```

NOTE

- The value of *Controller_ID* is the controller ID queried in [Step 3](#).
- The command is executed successfully if **Command completed successfully** is displayed.
- The controller card does not support the delivery of multiple firmware upgrade or downgrade commands at the same time. The commands must be executed one by one.
- If the **noprompt** parameter is not added to the command, enter **y** to confirm the upgrade. If the **noprompt** parameter is specified, the upgrade is performed without confirmation.

Step 5 Power off and then power on the server for the firmware to take effect. The procedure is as follows:

1. Click  on the toolbar of the virtual console, and choose **Power Off** from the drop-down list.
2. After the server is powered off, click  on the toolbar of the virtual console, and choose **Power On** from the drop-down list.

NOTE

It takes about 5 to 10 minutes to start the server.

- Step 6** Check whether the firmware version after the upgrade is the target version. For details about how to query the controller card firmware version, see [1.4.5.1 Querying the Firmware Version of a Controller Card](#).

If no error information is displayed during the upgrade process and the version queried after the upgrade is the target version, the upgrade is successful.

- Step 7** (Optional) Upgrade the controller card driver to a version that matches the firmware.

For details about how to obtain and upgrade the driver, see section "Installing and Upgrading Drivers and Firmware" in the [Huawei Server OS Installation Guide \(x86\)](#).

----End

1.4.4 Rolling Back a Version

1.4.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.4.4.2 Rollback Procedure

- Step 1** Determine the target version.

- Step 2** Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.4.3 Performing the Upgrade](#).

----End

1.4.5 Common Operations

1.4.5.1 Querying the Firmware Version of a Controller Card

You can use any of the following methods to query the controller card firmware version:

- Log in to the iBMC WebUI. For details, see **iBMC WebUI > System > Storage Management** in the [iBMC User Guide](#).

 NOTE

The controller card must support out-of-band management. You can use the [Computing Product Compatibility Checker](#) to check whether a controller card supports out-of-band management.

- Log in to the BIOS management page of the controller card, and see the value of **Firmware Version** on the **Controller Information** page. For details, see **Common Tasks > Querying the Firmware Version of a RAID Controller Card** in the *RAID Controller Card User Guide*.
 - For V2 and V3 servers, see the [Huawei V2 and V3 Server RAID Controller Card User Guide](#).
 - For V5 servers, see the [Huawei Server RAID Controller Card User Guide \(x86\)](#).
 - For V6 servers, see the [Huawei V6 Server RAID Controller Card User Guide](#).
- On the OS, use the ARCCONF controller card CLI tool to query the IP address.

arccnf getversion

Query the MSCC SmartRAID 3152-8i firmware version. The **Firmware** field in the command output indicates the firmware version of the controller card.

```
[root@localhost ~]# arccnf getversion
Controllers found: 1
Controller #1
=====
Firmware           : 1.61[0] (0)
Driver             : Linux 1.1.4-130 (0)
```

Command completed successfully.

1.5 Upgrading the Controller Card Firmware Using hiraidadm

1.5.1 Before You Start

Upgrade Scope

For details about the servers supported by the controller card, use the [Computing Product Compatibility Checker](#) to check.

This upgrade method applies to the following controller cards:

- SP686C

Impact of the Upgrade

After the upgrade, power cycle the server for the latest firmware version to take effect. Power cycling will interrupt services.

Precautions

Observe the precautions listed in [Table 1-11](#) during the upgrade.

Table 1-11 Precautions for the upgrade

No.	Description
1	Misoperations during the firmware upgrade may cause upgrade failure and make the controller card unavailable.
2	Stop running services on the server before the upgrade.
3	Do not perform any power-off operation during the upgrade and do not change configurations except for those involved in the upgrade guide.
4	Before the upgrade, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to the document, contact technical support.

1.5.2 Preparing for the Upgrade

1.5.2.1 Determining Source Version and Target Version

Before upgrading the controller card firmware, determine the source firmware version and the target firmware version. This information is required for a rollback. For details, see [1.5.5.1 Querying the Firmware Version of a Controller Card](#).

1.5.2.2 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-12](#).

Table 1-12 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

Software Package Description

[Table 1-13](#) lists the files contained in the controller card firmware upgrade package.

Table 1-13 Software package description

File	Description
drivers folder	(Optional) Driver file matching the firmware version. The firmware package may not contain this folder or does not contain the driver of a specified OS. In this case, download the driver by referring to "Procedure".
tools folder	Command line management tool of the control card.
*.img	Controller card firmware.

File	Description
	Script file for automatic firmware upgrade.
install.sh	Script file for automatic firmware upgrade.
version.xml	Version description file.

1.5.2.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.5.3 Performing the Upgrade

NOTICE

- Stop running services on the server before the upgrade.
- Do not power off the OS during the upgrade and do not change configurations except for those involved in the upgrade guide.

Scenarios

Upgrade the controller card firmware using the hiraidadm on an OS.

Prerequisites

- The server hosting the controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).
- You have downloaded the OS driver package to the client (such as a PC), and decompressed the package to obtain the driver image.
- You have downloaded the controller card firmware upgrade package to the client (such as a PC) and decompressed it.

Procedure

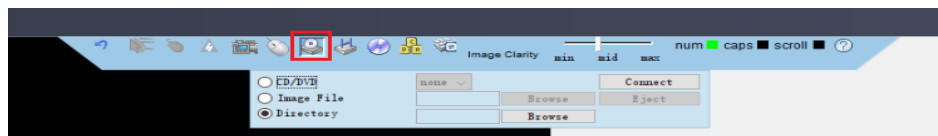
Step 1 Mount the upgrade file.

NOTE

The iBMC Remote Virtual Consoles include the Java Remote Virtual Console and HTML5 Integrated Remote Console. The HTML5 Integrated Remote Console does not support local directories. This section uses the Java Remote Virtual Console as an example. For more information, see the [iBMC User Guide](#).

1. On the toolbar of the virtual console, click  to display the screen shown in [Figure 1-8](#).

Figure 1-8 Virtual CD/DVD drive



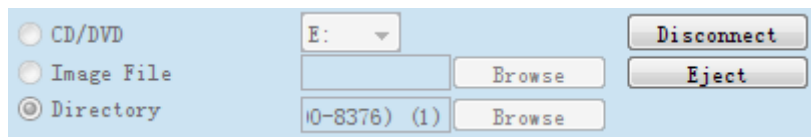
2. Select **Directory** and click **Browse**.
3. Select the folder generated after the controller card firmware upgrade package is decompressed.

NOTE

Select the folder of the target version for an upgrade or the folder of the source version for a rollback.

4. Click **Connect**.
If the **Eject** icon is available, as shown in [Figure 1-9](#), the file is successfully mounted.

Figure 1-9 Toolbar



Step 2 Copy the upgrade file to the server and grant the read and write permissions to the file.

1. On the OS, run the **mkdir fw** command to create the **fw** folder in the **root** directory.
2. Run the **mount /dev/sr0 /mnt** command to mount the local folder to the **/mnt** directory.

NOTE

After you enter **mount /dev/sr**, press **Tab** to display the value following **sr**.

3. Run the **cp -vr /mnt/* /root/fw/** command to copy the mounted file to the **fw** directory.
4. Run the **cd /root/fw/** command to go to the **fw** directory.
5. Run the **cp -vr /tools/* /root/fw/** command to copy the mounted file to the **fw** directory.

6. Run the **chmod 777 *** command to add read and write permissions for the file.

Step 3 Run the **./hraidadm show allctrl** command to view the IDs of all controller cards that support the hraidadm.

Assume that a server has an SP686C.

```
[root@localhost fw]# ./hraidadm show allctrl
```

```
===== Hraidadm Information
=====
```

```
Name: hraidadm
Version :1.2.0.1
Build Time:Jun 14 2022 22:33:41
=====
```

```
=====
Status Code = 0
Status = Success
Description = None
=====
```

```
=====
Controllers Number = 1
=====
```

```
Controller Id      | 0
Device Name       | /dev/bsg/hraid0
Pcie Bus Domain   | 0000
Bus Number        | 04
Device Number     | 00
Function Number    | 00
PCI Address       | 0000:04:00.0
```

Step 4 Run the **./hraidadm ccontroller_id update fw file=xxx.img** command to perform the upgrade.

Upgrade the firmware of the SP686C controller card.

```
[root@localhost fw]# ./hraidadm c0 update fw file=packet_raid.img
```

```
===== Hraidadm Information
=====
```

```
Name: hraidadm
Version :1.2.0.1
Build Time:Jun 14 2022 22:33:41
=====
```

```
=====
update controller firmware done,duration: 2min42s
=====
```

```
=====
Status Code = 0
Status = Success
Description = None
=====
```

NOTE

- The value of **Controller_ID** is the value of **Controller Id** queried in [Step 3](#).
- **xxx.img** is the .img firmware file obtained after decompression.
- If **Status = Success** is displayed in the command output, the command is executed successfully.

Step 5 After the upgrade command is executed, use either of the following methods to make the firmware take effect:

- Run the **./hraidadm ccontroller_id active fw type=hot** command to use the hot activation mode. The upgrade can be completed without restarting the server.

NOTICE

To use the hot activation mode, ensure that the following requirements are met:

- The version number is in the format of *x.y.n.z*. Hot activation is supported only when the values of *x*, *y*, and *n* of the source version and those of the target version are the same. For example, the upgrade from 1.0.17.1 to 1.0.17.2 supports hot activation, but the upgrade from 1.0.17.1 to 1.0.18.1 does not support hot activation.
- SP686C does not have pinned cache in the current system. That is, no dirty data that cannot be delivered exists in the cache when the logical unit number is invalid. If pinned cache exists, delete the pinned cache or restore the faulty RAID.
- No task, such as rebuild, pre-copy, copyback, initialization, or capacity expansion, is running in the system. If such a task is running, wait until the task is complete or stopped. To view the current background tasks of the controller card, run the **hiraidadm ccontroller_id show bgtask** command.
- No sanitize or erase task is being executed in the system. If such a task is running, wait until the task is complete or stopped. To view the erasure status of a drive, run the **hiraidadm ccontroller_id:enclosure_id:slot_id show sanitize** or **hiraidadm ccontroller_id:enclosure_id:slot_id show erase** command.
controller_id indicates the controller card ID, *enclosure_id* indicates the ID of the enclosure where the drive resides, and *slot_id* indicates the ID of the slot where the drive resides.
- During the SP686C activation, if the cache data and delivered I/O data cannot be processed within the specified time, the activation will be terminated and a failure message will be returned to prevent I/O exceptions. In this case, try again later.

If **Status = Success** is displayed, the command is successfully executed.

```
[root@localhost fw]# ./hiraidadm c0 active fw type=hot
```

```
===== Hiraidadm Information
```

```
=====
```

```
Name: hiraidadm
Version :1.2.0.1
Build Time:Jun 14 2022 22:33:41
```

```
=====
```

```
=====
```

```
=====
```

```
=====
```

```
Status Code = 0
Status = Success
Description = None
```

```
=====
```

```
=====
```

- Restart the server for the firmware to take effect in cold activation mode.

 NOTE

- It takes about 5 to 10 minutes to start the server.
- After the upgrade, the cold activation mode is used by default when the server is restarted without any activation command.

- Step 6** Check whether the firmware version after the upgrade is the target version. For details about how to query the controller card firmware version, see [1.5.5.1 Querying the Firmware Version of a Controller Card](#).

If no error information is displayed during the upgrade process and the version queried after the upgrade is the target version, the upgrade is successful.

- Step 7** (Optional) Upgrade the controller card driver to a version that matches the firmware.

For details about how to obtain and upgrade the driver, see section "Installing and Upgrading Drivers and Firmware" in the [Huawei Server OS Installation Guide \(x86\)](#).

----End

1.5.4 Rolling Back a Version

1.5.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.5.4.2 Rollback Procedure

- Step 1** Determine the target version.

- Step 2** Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.5.3 Performing the Upgrade](#).

----End

1.5.5 Common Operations

1.5.5.1 Querying the Firmware Version of a Controller Card

You can use any of the following methods to query the controller card firmware version:

- Log in to the iBMC WebUI. For details, see **iBMC WebUI > System > Storage Management** in the [iBMC User Guide](#).

 NOTE

The controller card must support out-of-band management. You can use the [Computing Product Compatibility Checker](#) to check whether a controller card supports out-of-band management.

- Log in to the BIOS management page of the controller card, and see the value of **Firmware Version** on the **Controller Management** page. For details, see **Common Tasks > Querying the Firmware Version of a RAID Controller Card** in the *Controller Card User Guide*.
 - For V5 servers, see the [Huawei Server RAID Controller Card User Guide \(x86\)](#).
 - For V6 servers, see the [Huawei V6 Server RAID Controller Card User Guide](#).
- After the server starts, use the hiraidadm controller card CLI tool on the OS to query the firmware version.

./hiraidadm cController_ID show status

In the command output, **FW Version0** and **FW Version1** indicate the firmware versions in the active and standby areas, respectively. **Current FW** indicates the running partition of the controller card.

Query the SP686C version.

```
[root@localhost fw]# ./hiraidadm c0 show status
```

```
===== Hiraidadm Information  
=====
```

```
Name: hiraidadm  
Version :1.2.0.1  
Build Time:Jun 14 2022 22:33:41
```

```
=====
```

```
=====
```

```
Status Code = 0  
Status = Success  
Description = None
```

```
=====
```

```
SAS Address      | 50c31dc5b71e8000  
FW Version0    | 1.0.17.1  
FW Version1    | 1.0.17.1  
Current FW       | 0  
Vendor Id        | 19e5  
Device Id        | 3758  
SubVendor Id     | 19e5  
SubDevice Id     | 01a4  
Pcie Bus Domain  | 0000  
Bus Number       | 04  
Device Number    | 00  
Function Number  | 00  
Board SN         | 2102313XXGFSN4000070  
PF0              | Enable  
PF1              | Disable  
EP PCIe Width    | x8  
EP PCIe Speed    | 4G  
Chip Name        | B80121  
Chip Version     | V100  
Die ID           | 599e5b94 0121275e 00000000 00000000 001fc003  
Tempature        | 66c  
PD Number        | 11  
VD Number        | 1  
VD Degrade Number | 0  
VD Fault Number  | 0  
Raid Number      | 1
```

```
PreFail Number | 0
Fail Number    | 0
DDR Size       | 4096MB
DDR ECC Count   | 0
DDR ECC Bucket Size | 16
DDR CE Count    | 0
DDR UCE Count   | 0
SRAM ECC Count  | 0
SRAM UCE Count  | 0
Cache Pinned    | 0
Board Error     | 0
Board Clock Error | 0
Board Power Error | 0
Board Capacity Error | 0
Board Flash Error | 0
Board Name      | SP686C-M-16i 4G
```

1.6 Upgrading the Controller Card Firmware Using Smart Provisioning

The following controller cards can be upgraded using Smart Provisioning only on V5 and V6 servers:

- LSI SAS3008IR
- LSI SAS3008IT
- LSI SAS3108
- Avago SAS3004iMR
- Avago SAS3408iMR
- Avago SAS3416iMR
- Avago SAS3416IT
- Avago SAS3508
- Avago SAS3516
- MSCC SmartRAID 3152-8i
- MSCC SmartHBA 2100-8i
- Avago MegaRAID SAS 9440-8i
- Avago MegaRAID SAS 9460-8i
- Avago MegaRAID SAS 9460-16i
- FBGF-RAD-R1-S1

1.6.1 Preparing for the Upgrade

1.6.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-14](#).

Table 1-14 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Smart Provisioning tool package	- Enterprise users: - Log in to the Smart Provisioning download page. - You are advised to select the latest version. - Download the Smart Provisioning tool package and digital signature file from the software list. - Decompress the Smart Provisioning tool package to obtain the .iso file of Smart Provisioning. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- The required Smart Provisioning version varies depending on the firmware package version. For details, see the firmware package description at the download website.
- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

1.6.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.6.2 Performing the Upgrade

For details, see **Using Smart Provisioning > GUI Introduction > Performing Upgrades > Upgrading Firmware** in the *Smart Provisioning User Guide*.

NOTE

The required Smart Provisioning version varies depending on the firmware package version. For details, see the firmware package description at the download website.

1.6.3 Rolling Back a Version

1.6.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.6.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see the *Smart Provisioning User Guide*.

----End

1.7 Upgrading the Controller Card Firmware Using SmartKit

The following controller cards can be upgraded using SmartKit only on V5 and V6 servers:

- LSI SAS2208
- LSI SAS2308
- LSI SAS3008IR
- LSI SAS3008IT
- LSI SAS3108
- Avago SAS3004iMR
- Avago SAS3408iMR
- Avago SAS3416iMR
- Avago SAS3416IT
- Avago SAS3508
- Avago SAS3516
- MSCC SmartRAID 3152-8i
- MSCC SmartHBA 2100-8i
- LSI SAS9305-24i
- Avago MegaRAID SAS 9440-8i
- Avago MegaRAID SAS 9460-8i
- Avago MegaRAID SAS 9460-16i
- FBGF-RAD-R1-S1

1.7.1 Preparing for the Upgrade

1.7.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-15](#).

Table 1-15 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

1.7.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.7.2 Performing the Upgrade

For details, see the latest *SmartKit Computing User Guide*. There are two *SmartKit Computing User Guide* editions for common users and engineers, respectively.

- In the *SmartKit Computing User Guide* for common users, see section "Using SmartKit" > "Firmware Upgrade" > "Upgrading PCIe Card and Hard Disk Firmware".
- In the *SmartKit Computing User Guide (for Engineers)*, there are two upgrade methods.
 - For details, see section "Using SmartKit" > "Firmware Upgrade" > "Upgrading PCIe Card and Hard Disk Firmware".
 - For details, see section "Using SmartKit" > "Bundle Upgrade" > "Bundle Upgrade".

1.7.3 Rolling Back a Version

1.7.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.7.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plugin version.

----End

1.8 Upgrading the Controller Card Firmware Using FwUpgrade

The following controller cards can be upgraded using FwUpgrade only on V2 and V3 servers:

- LSI SAS2208
- LSI SAS2308
- LSI SAS3008IR
- LSI SAS3008IT
- LSI SAS3108

1.8.1 Preparing for the Upgrade

1.8.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-16](#).

Table 1-16 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	• Enterprise users: 1. Log in to FusionServer iDriver or Computing Component iDriver. 2. Click the recommended version. The software list is displayed. 3. Set Software Type to FW. 4. Download the required firmware upgrade package to the client (local PC) and decompress it. • Carrier users: Contact technical support of your local Huawei office.

Type	How to Obtain
FwUpgrade tool package	- Enterprise users: - Visit the SmartKit Computing website. - You are advised to select the latest version. - Download the FwUpgrade tool package and digital signature file from the tool list. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86) .

 NOTE

- The required FwUpgrade version varies depending on the firmware package version. For details, see the description of the firmware package.
- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

1.8.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.8.2 Performing the Upgrade

For details, see "Using FwUpgrade" in the [SmartKit Computing 1.0.0 FwUpgrade User Guide](#).

1.8.3 Rolling Back a Version

1.8.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.8.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see the [SmartKit Computing 1.0.0 FwUpgrade User Guide](#).

----End

1.9 Upgrading the Controller Card Firmware Using Toolkit

The following controller cards can be upgraded using Toolkit only on V2 and V3 servers:

- LSI SAS2308
- LSI SAS3008IR

1.9.1 Preparing for the Upgrade

1.9.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-17](#).

Table 1-17 Obtaining the software packages

Type	How to Obtain
Controller card firmware upgrade package	- Enterprise users: - Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Toolkit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select the latest version. - Download the required Toolkit package. - Carrier users: Contact technical support of your local Huawei office.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

 NOTE

- If a controller card firmware package cannot be found in the specified iDriver version, search for the firmware package by controller card keyword (for example, controller card model).
- Use the same method to download the firmware upgrade packages of the source and target versions.

1.9.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.9.2 Performing the Upgrade

NOTICE

- After the Toolkit is mounted, the server must be rebooted. Services are interrupted during the reboot process.
- Do not power off the OS during the upgrade and do not change configurations except for those involved in the upgrade guide.

Scenarios

The firmware of the LSI SAS2308 and LSI SAS3008IR controller cards has been integrated into Toolkit. This section uses LSI SAS2308 as an example to describe how to use Toolkit to upgrade the controller card firmware.

NOTE

Although the LSI HBA SAS 9217-8i control card is not self-developed by Huawei, it supports this upgrade method.

Prerequisites

- The server hosting the controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).
- You have downloaded and decompressed the **RAID_card(2208&2308&3008&3108)-FW-Vxxx.zip** firmware upgrade package and obtained **FusionServer-RAID_card(2208&2308&3008&3108)-FW-Vxxx.iso**.

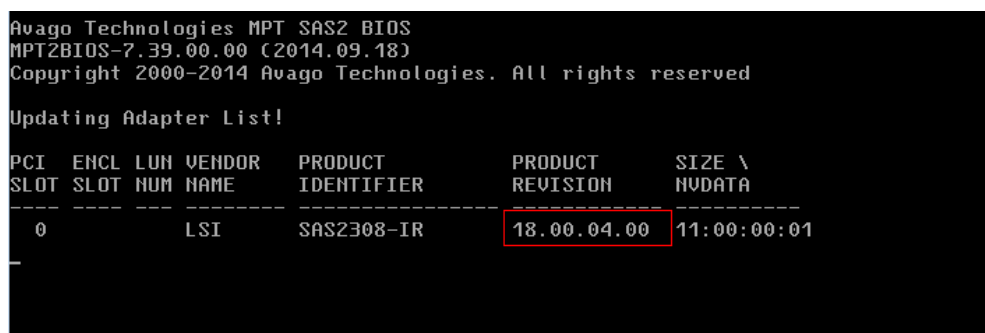
Procedure

Step 1 Check the source firmware version.

Use either of the following methods to obtain the source firmware version:

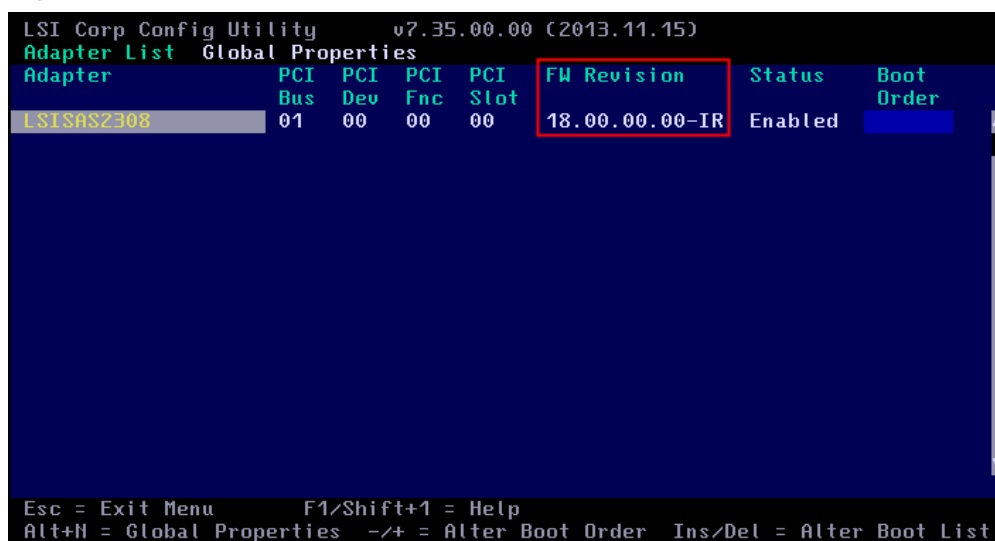
- View the firmware version during the server startup process, as shown in [Figure 1-10](#).

Figure 1-10 Firmware version (1)



- Obtain the firmware version on the Config Utility screen of the controller card, as shown in [Figure 1-11](#).

Figure 1-11 Firmware version (2)



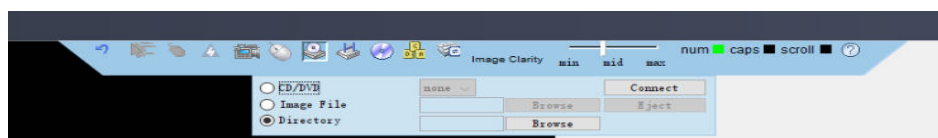
Step 2 Set the system boot device to DVD-ROM drive.

- On the iBMC WebUI, choose **Configure > Boot Option**.
The **Boot Option** page is displayed.
- Select **DVD-ROM**, and click **Save**.

Step 3 Mount the ISO file.

- Open the Remote Virtual Console.
- Click  on the toolbar.
The screen shown in [Figure 1-12](#) is displayed.

Figure 1-12 Virtual CD/DVD drive



- Select **Image File**, and click **Browse**.
The **Open** dialog box is displayed.

4. Select **FusionServer-RAID_card(2208&2308&3008&3108)-FW-Vxxx.iso**, and click **Connect** in the screen shown in [Figure 1-12](#).

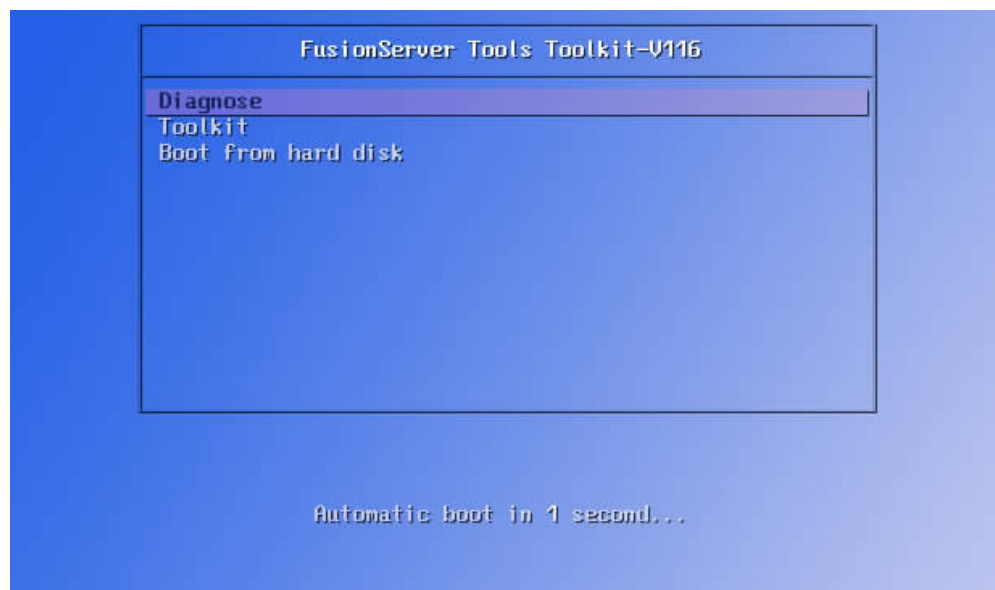
Step 4 Start the server.

1. On the toolbar, click  and choose **Power Off** or **Normal Power Off**.
A confirmation dialog box is displayed.

 NOTE

- **Forced Power Off, Reset, Forced System Reset, and Forced Power Cycle** may damage user programs or unsaved data.
 - When **Power-off Timeout** is enabled, the iBMC forcibly powers off the OS if the OS cannot be powered off within the specified time. For details about how to configure the **Power-off Timeout**, see "Power Control" in the *iBMC User Guide*.
2. Click **Yes**.
The server is powered off.
 3. On the toolbar, click  and choose **Power On**.
A confirmation dialog box is displayed.
 4. Click **Yes**.
The server is being powered on. The startup screen is displayed, as shown in [Figure 1-13](#).

Figure 1-13 Toolkit startup screen



Step 5 Switch to the Toolkit CLI.

1. Select **Toolkit**, and press **Enter**.
2. When information shown in [Figure 1-14](#) is displayed, enter **C** and press **Enter**.

Figure 1-14 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:
```

3. Enter the user name and password as prompted.
The CLI is displayed.

NOTE

The default user is **root**, and the password is **Huawei12#\$**.

Step 6 Upgrade the firmware.

1. Run the **cd /home/Project/tools/upgrade/raid/tool/** command.
2. Run **./FwUpgrade.py FwUpgrade.xml** to upgrade the controller card firmware.

After the upgrade is complete, the information shown in [Figure 1-15](#) is displayed.

NOTE

- The firmware of the LSI SAS2308 controller card can be upgraded but cannot be downgraded.
- The **xxxxupgrade.log** file in the **/home/Project/FTK/upgrade/raid/tool/** directory records the upgrade process of the RAID controller card. If the upgrade fails, provide this file to Huawei technical support engineers for locating faults.
- If a rollback is required, contact Huawei technical support.

Figure 1-15 Upgrade completed

```
linux:/home/Project/tools/upgrade/raid/tool # ./FwUpgrade.py FwUpgrade.xml
Input parameter is: FwUpgrade.xml
FwUpgrade OK NA NA
***Start LSI2208 upgrade***
FwUpgrade OK NA Upgrade device[LSI2208] is not exist
***LSI2208 upgrade end***
***Start LSI2308 upgrade***
LSI2308 upgrade succeed!
***LSI2308 upgrade end***
***Start LSI3008 upgrade***
FwUpgrade OK NA Upgrade device[LSI3008] is not exist
***LSI3008 upgrade end***
***Start LSI3108 upgrade***
FwUpgrade OK NA Upgrade device[LSI3108] is not exist
***LSI3108 upgrade end***
linux:/home/Project/tools/upgrade/raid/tool #
```

Step 7 Power off and then power on the server for the firmware to take effect. The procedure is as follows:

1. Click  on the toolbar of the virtual console, and choose **Power Off** from the drop-down list.
2. After the server is powered off, click  on the toolbar of the virtual console, and choose **Power On** from the drop-down list.

During the restart, the firmware information of the controller card is displayed, as shown in [Figure 1-16](#).

 NOTE

It takes about 5 to 10 minutes to start the server. The time varies according to the actual configuration.

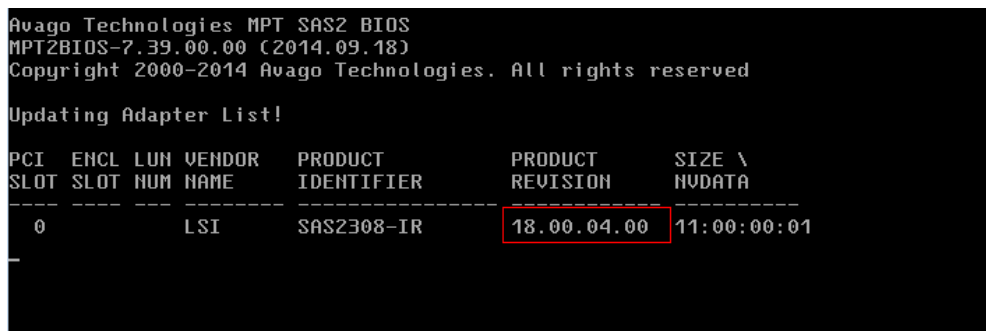
Step 8 Check whether the firmware version is the target version.

If no error information is displayed during the upgrade process and the version queried after the upgrade is the target version, the upgrade is successful.

Use either of the following methods to obtain the target firmware version:

- View the firmware version during the server startup process, as shown in [Figure 1-17](#).

Figure 1-16 Firmware version (1)



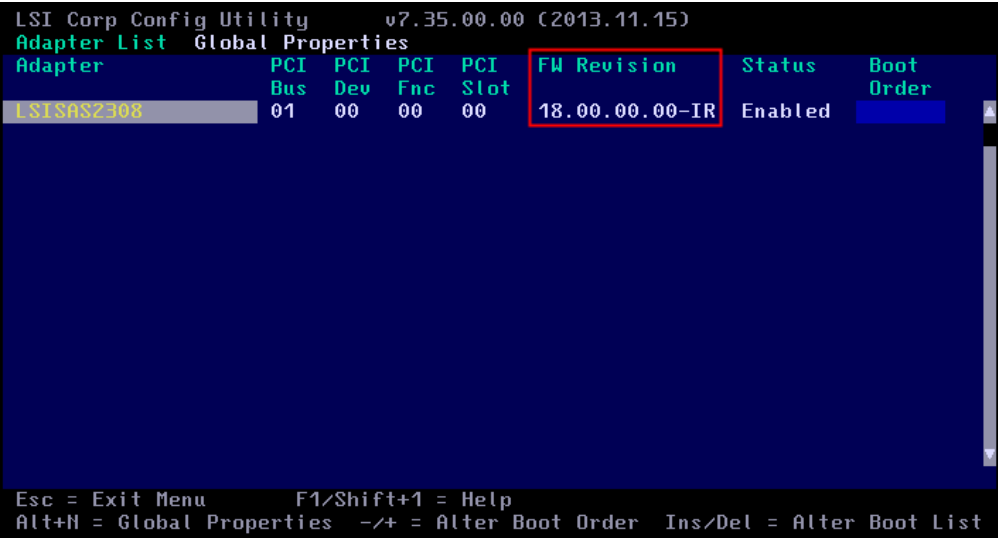
```
Avago Technologies MPT SAS2 BIOS
MPT2BIOS-7.39.00.00 (2014.09.18)
Copyright 2000-2014 Avago Technologies. All rights reserved

Updating Adapter List!

PCI  ENCL  LUN  VENDOR  PRODUCT  PRODUCT  SIZE \
SLOT SLOT NUM NAME  IDENTIFIER  REVISION  NVDATA
-----
0      LSI    SAS2308-IR  18.00.04.00  11:00:00:01
```

- Obtain the firmware version on the Config Utility screen of the controller card, as shown in [Figure 1-16](#).

Figure 1-17 Firmware version (2)



----End

Additional Information

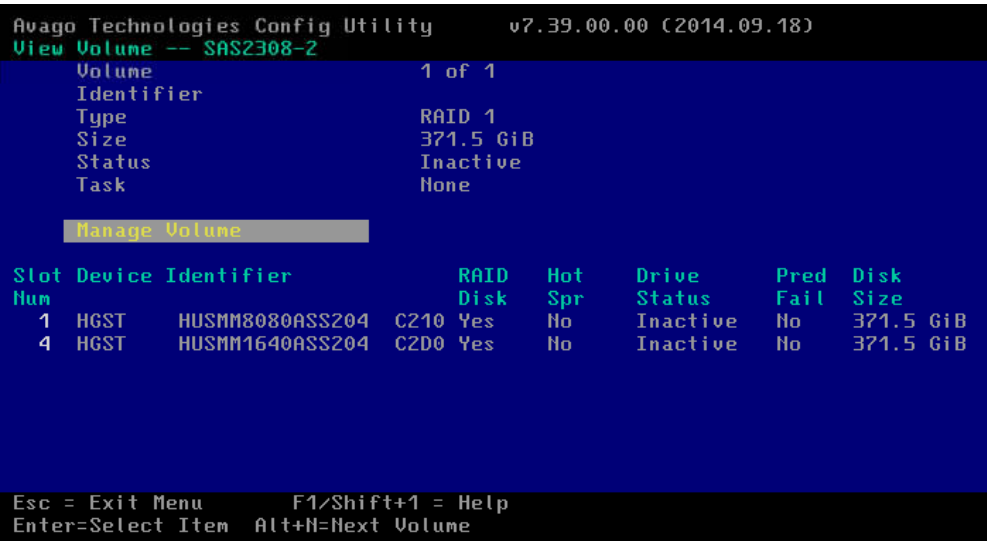
Related Tasks

After upgrading the LSI SAS2308 RAID controller card firmware, activate the RAID array and configure the boot option as follows:

1. When the message "Press Ctrl-C to Start LSI Corp Configuration Utility..." is displayed during server startup, press **Ctrl+C**.
2. On the Config Utility screen, select the LSI SAS2308 RAID controller card, and press **Enter**.
3. On the **Adapter Properties** screen, choose **RAID Properties > View Existing Volume**.

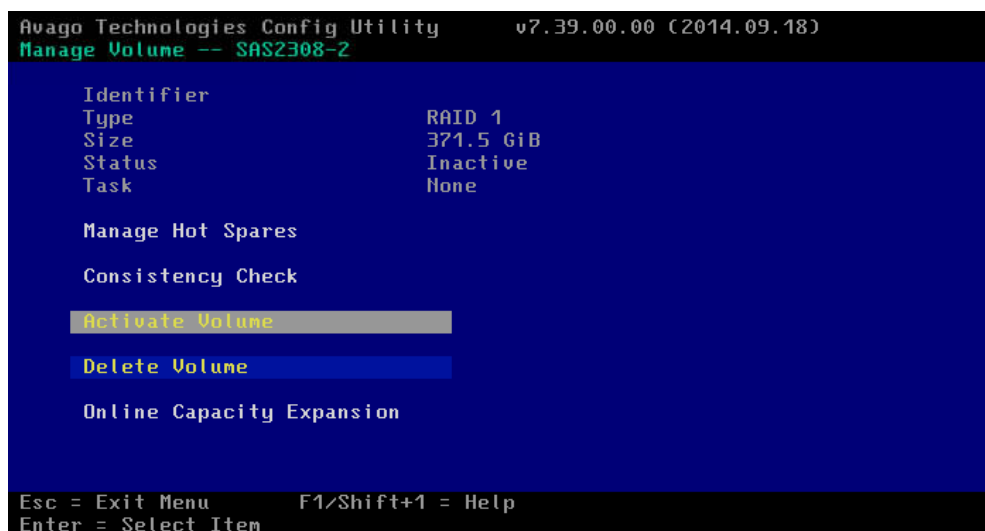
The RAID array status is **Inactive**, as shown in [Figure 1-18](#).

Figure 1-18 View Volume



4. Select **Manage Volume**, and press **Enter**.
The **Manage Volume** screen is displayed, as shown in [Figure 1-19](#).

Figure 1-19 Manage Volume



5. Select **Activate Volume**, and press **Enter**.
A confirmation dialog box is displayed.
6. Press **Y** to activate the RAID array and return to the **Manage Volume** screen.
7. Press **Esc** to return to the **Adapter Properties** screen.
8. Select **SAS Topology**, and press **Enter**.
9. Select the RAID array or drive on which the OS is installed, and press **Alt+B** to set it as the boot device.

Boot is displayed in the **Device Info** column of the boot device, as shown in [Figure 1-20](#).

Figure 1-20 Setting the boot drive



10. Press **Esc** repeatedly to save the settings and exit the CU, and restart the server.

1.9.3 Rolling Back the Firmware Version

1.9.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

1.9.3.2 Rollback Procedure

To roll back the firmware version of a controller card, contact Huawei technical support.

1.10 Others

1.10.1 Upgrading the LSI SAS3108 RAID Controller Card Using CLI on VMware

1.10.1.1 Preparing for the Upgrade

1.10.1.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-18](#).

Table 1-18 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of a RAID controller card	- Enterprise users: - Visit the FusionServer iDriver web page. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Management tool of the RAID controller card	- Log in to the page of the RAID card on the BROADCOM website. - On the DOWNLOADS tab page, click Management Software and Tools. The list of management software and tools is displayed. - Download the StorCLI tool of the latest version. - After the decompression, the tool packages that are applicable to different operating systems will be obtained.

1.10.1.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.10.1.2 Upgrade Procedure

Scenarios

Upgrade the LSI SAS3108 RAID controller card firmware using CLI on VMware.

NOTICE

- Stop running services on the server before the upgrade.
- Do not power off the OS during the upgrade and do not change configurations except for those involved in the upgrade guide.

Prerequisites

Conditions

- The server hosting the LSI SAS3108 RAID controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

You have downloaded and decompressed the firmware upgrade package (for example, **RAID card(BC6ESML01)-SR430C(3108)-FW-V110(FW 4.660.00-8270).zip**) and StorCLI tool package to the client (a PC). For details, see [1.10.1.1 Obtaining Software Packages](#).

Procedure

Step 1 Check the current firmware version.

You can obtain the firmware version using either of the following methods:

- View the firmware version during the server startup process, as shown in [Figure 1-21](#).

Figure 1-21 RAID controller card firmware version

```
Battery Status: Not present
PCI Slot Number: 0

ID LUN VENDOR  PRODUCT                REVISION  CAPACITY
-- -- -
   0  LSI      SAS3108                4.660.00-8270  1024MB

0 Virtual Drive(s) found on the host adapter.

0 Virtual Drive(s) handled by BIOS
Press <Ctrl><R> to Run MegaRAID Configuration Utility
```

- After the server is started, use the RAID controller card CLI tool Storcli to query the firmware version. For details, see [Figure 1-22](#).

Figure 1-22 Querying the firmware information of the RAID controller card

```
[root@localhost:/opt/lsi/storcli] ./storcli /c0 show
Generating detailed summary of the adapter, it may take a while to complete.

Controller = 0
Status = Success
Description = None

Product Name = SAS3108
Serial Number = 033QQQ1359777777
SAS Address = 559e4c64a
PCI Address = 00:01:00:00
System Time = 11/16/2017 13:23:33
Mfg. Date = 00/00/00
Controller Time = 11/16/2017 13:23:34
FW Package Build = 24.16.0-0109
BIOS Version = 6.32.02.0 4.17.08.00_0x06150500
FW Version = 4.660.00-8270
```

Step 2 Install a VMware tool.

1. Use a file transfer tool (such as WinSCP) to upload the package applicable to VMware to a directory (such as the **/tmp** directory) on the server OS.
2. On the VMware CLI, run the **esxcli software vib install -v=/tmp/vmware-xxx-storcli.vib --no-sig-check** command to install the StorCLI tool. **/tmp/vmware-xxx-storcli.vib** is the complete path of the StorCLI tool file.
esxcli software vib install -v=/tmp/vmware-xxx-storcli.vib --no-sig-check

 NOTE

The StorCLI installation directory is **/opt/lsi/storcli/**. You need to access the directory and run RAID card commands.

3. After the installation is complete, run the **./storcli /c0 show** command to query the RAID controller card firmware information in the **/opt/lsi/storcli** directory, as shown in [Figure 1-23](#).
./storcli /c0 show

Figure 1-23 Querying the firmware information of the RAID controller card

```
[root@localhost:/opt/lsi/storcli] ./storcli /c0 show
Generating detailed summary of the adapter, it may take a while to complete.

Controller = 0
Status = Success
Description = None

Product Name = SAS3108
Serial Number = 033QQQ1359777777
SAS Address = 559e4c64a
PCI Address = 00:01:00:00
System Time = 11/16/2017 13:23:33
Mfg. Date = 00/00/00
Controller Time = 11/16/2017 13:23:34
FW Package Build = 24.16.0-0109
BIOS Version = 6.32.02.0 4.17.08.00_0x06150500
FW Version = 4.660.00-8102
```

Step 3 Upgrade the firmware of the RAID controller card.

1. Copy the firmware upgrade package **RAID card(BC6ESML01)-SR430C(3108)-FW-V110(FW 4.660.00-8270).zip** to a directory in the VMware OS by using WinSCP.
2. Run the **Unzip directory\xxx.zip** to decompress the package, as shown in [Figure 1-24](#).
xxx indicates the firmware upgrade package name of the RAID controller card.

Figure 1-24 Decompressing the firmware upgrade package

```
[root@localhost:/var] unzip RAID\ card\ (BC6ESML01)\ -SR430C\ (3108)\ -FW-V110\ (FW\ 4.660.00-8270\).zip
Archive:  RAID card(BC6ESML01)-SR430C(3108)-FW-V110(FW 4.660.00-8270).zip
  inflating: storcli64
  inflating: UPDATE.BAT
  inflating: version.xml
  inflating: 3108FW4.rom
  inflating: 3108FW16.rom
  inflating: BB4K.ROM
  inflating: DOS4GW.EXE
  inflating: FLASHIN.BAT
  inflating: MEGACLI.EXE
  inflating: MEGAREC.EXE
  inflating: readme.txt
```

3. After decompression, run **/opt/lsi/storcli/storcli /cController_IDdownload file=3108FW4.rom noverchk** to upgrade the firmware. If **Status = Success** is displayed, the upgrade is successful. See [Figure 1-25](#).

In the command, **Controller_ID** indicates the ID of the RAID controller card. You need to specify this parameter for each RAID controller card when configuring multiple RAID controller cards.

```
/opt/lsi/storcli/storcli /c0 download file=3108FW4.rom noverchk
```

Figure 1-25 Upgrading the firmware

```
[root@localhost:/var] /opt/lsi/storcli/storcli /c0 download file=3108FW4.rom noverchk
Download Completed.
Flashing image to adapter...
Controller = 0
Status = Success
Description = F/W Flash Completed. Please reboot the system for the changes to take effect
```

4. Power off and then power on the server for the firmware to take effect. The procedure is as follows:
 - a. Run the **poweroff** command to power off the server.
poweroff

- b. After the server is powered off, click  on the toolbar of the virtual console, and choose **Power On** from the drop-down list.

During the restart, the RAID controller card firmware information is displayed, as shown in [Figure 1-26](#).

Figure 1-26 RAID controller card firmware version

```
Battery Status: Not present
PCI Slot Number: 0

ID LUN VENDOR  PRODUCT                REVISION  CAPACITY
-- -- -
0 0 LSI SAS3108 4.660.00-8270 1024MB

0 Virtual Drive(s) found on the host adapter.

0 Virtual Drive(s) handled by BIOS
Press <Ctrl><R> to Run MegaRAID Configuration Utility
```

Step 4 Check whether the firmware version is the target version.

NOTE

If no error information is displayed during the upgrade process and the version queried after the upgrade is the target version, the upgrade is successful.

You can check the firmware version using one of the following methods:

- View the firmware version during the server startup process, as shown in [Figure 1-26](#).
- After the server reboots, use the RAID card CLI tool **storcli** to query the firmware version of the RAID controller card, as shown in [Figure 1-27](#).

Figure 1-27 Querying the firmware information of the RAID controller card

```
[root@localhost:/opt/lsi/storcli] ./storcli /c0 show
Generating detailed summary of the adapter, it may take a while to complete.

Controller = 0
Status = Success
Description = None

Product Name = SAS3108
Serial Number = 033QQQ1359777777
SAS Address = 559e4c64a
PCI Address = 00:01:00:00
System Time = 11/16/2017 13:23:33
Mfg. Date = 00/00/00
Controller Time = 11/16/2017 13:23:34
FW Package Build = 24.16.0-0109
BIOS Version = 6.32.02.0_4.17.08.00_0x06150500
FW Version = 4.660.00-8270
```

----End

1.10.1.3 Rolling Back the Firmware Version

1.10.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

1.10.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.10.1.2 Upgrade Procedure](#).

----End

1.10.2 Upgrading the LSI SAS3108 RAID Controller Card Using CLI on Windows

1.10.2.1 Preparing for the Upgrade

1.10.2.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 1-19](#).

Table 1-19 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of a RAID controller card	- Enterprise users: - Visit the FusionServer iDriver web page. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
Management tool of the RAID controller card	- Log in to the page of the RAID card on the BROADCOM website. - On the DOWNLOADS tab page, click Management Software and Tools. The list of management software and tools is displayed. - Download the StorCLI tool of the latest version. - After the decompression, the tool packages that are applicable to different operating systems will be obtained.

1.10.2.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

1.10.2.2 Performing the Upgrade

Scenarios

Upgrade the LSI SAS3108 RAID controller card firmware using the CLI on an OS, such as Windows Server 2012 R2.

NOTICE

- Stop running services on the server before the upgrade.
- Do not power off the OS during the upgrade and do not change configurations except for those involved in the upgrade guide.

Prerequisites

Conditions

- The server hosting the LSI SAS3108 RAID controller card is powered on.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

- You have downloaded the OS driver package to the client (such as a PC), and decompressed the package to obtain the driver image.
- You have downloaded the RAID controller card firmware upgrade package to the client (such as a PC) and decompressed the package.

Procedure

- Step 1** On the OS CLI, run the **storcli64 show** command to query the controller ID of the RAID controller card.

```
storcli64 show
```

NOTE

- If the server is configured with multiple RAID controller cards, perform this step to query the ID of each RAID controller card.
- **Ctl** indicates the ID of each RAID controller card.

Step 2 (Optional) Upgrade the RAID controller card driver.

1. Visit [Computing Component iDriver](#) and download the driver mapping table and driver package.
2. Upgrade the driver by referring to the Readme file in the driver package.

Step 3 Perform a pre-upgrade check.

1. Open the PowerShell window.
2. Run the **cd .\Desktop** command to go to the directory where the tool is stored.
`cd .\Desktop`
3. Run the **.\storcli64.exe /c0/v1 show all** command to view the RAID array information. **TYPE** indicates the RAID array level, **State** indicates the RAID array status, **Cache** indicates the read/write policy of the RAID array, and **PDs for VD 1** indicates the physical drives that form the RAID array, **Strip Properties** indicates the strip size of the RAID array.
`.\storcli64.exe /c0/v1 show all`

Figure 1-28 Querying RAID array information

```
PS C:\Users\Administrator> .\storcli64.exe /c0/v1 show all
Controller = 0
Status = Success
Description = None

/c0/v1 :
=====

DG\VD TYPE State Access Consist Cache Cac sCC Size Name
-----
0/1 RAID0 Opt1 RW Yes RWTD - ON 556.929 GB

Cac=CacheCade|Rec=Recovery|OfLn=OffLine|Pdgd=Partially Degraded|Dgrd=Degraded
Opt1=Optimal|RO=Read Only|RW=Read Write|HD=Hidden|TRANS=TransportReady|B=Blocked|
Consist=Consistent|R=Read Ahead Always|NR=No Read Ahead|WB=WriteBack|
AWB=Always WriteBack|WT=WriteThrough|C=Cached IO|D=Direct IO|sCC=Scheduled
Check Consistency

PDs for VD 1 :
=====

EID:SlT DID State DG Size Intf Med SED PI SeSz Model Sp
-----
34:7 63 OnLn 0 837.258 GB SAS HDD N N 512B ST900MM0168 U
34:6 62 OnLn 0 278.464 GB SAS HDD N N 512B ST300MM0008 U

EID-Enclosure Device ID|SlT-SlT No.|DID-Device ID|DG-DriveGroup
DHS-Dedicated Hot Spare|UGood-Unconfigured Good|GHS-Global Hotspare
UBad-Unconfigured Bad|OnLn-Online|OffLn-Offline|Intf-Interface
Med-Media Type|SED-Self Encryptive Drive|PI-Protection Info
SeSz-Sector Size|Sp-Spun|U-Up|D-Down/PowerSave|T-Transition|F-Foreign
UGUnsp-Unsupported|UGShld-UnConfigured shielded|HSPShld-Hotspare shielded
CFShld-Configured shielded|Cpybck-CopyBack|CBShld-Copyback Shielded

VD1 Properties :
=====
Strip Size = 256 KB
Number of Blocks = 1167966208
VD has Emulated PD = No
Span Depth = 1
Number of Drives Per Span = 2
Write Cache(initial setting) = WriteBack
Disk Cache Policy = Disk's Default
Encryption = None
Data Protection = Disabled
Active Operations = None
```

4. Run the **.\storcli64.exe /c0 show bootdrive** command to check whether the RAID array has been set as the boot drive. The command output shown in [Figure 1-29](#) indicates that the boot drive is **VD:1**.
`.\storcli64.exe /c0 show bootdrive`

Figure 1-29 Querying the boot drive

```
PS C:\Users\Administrator> .\storcli64.exe /c0 show bootdrive
Controller = 0
Status = Success
Description = None

Controller Properties :
=====
Ctrl_Prop Value
-----
BootDrive VD:1
-----
```

5. Run the `.\storcli64.exe /c0 show` command to query RAID array information. In the command output, **FW version** indicates the firmware version of the RAID controller card.
`.\storcli64.exe /c0 show`

Figure 1-30 Querying RAID controller card version information

```
PS C:\Users\Administrator> .\storcli64.exe /c0 show
Generating detailed summary of the adapter, it may take a while to complete.

Controller = 0
Status = Success
Description = None

Product Name = SAS3108
Serial Number =
SAS Address = 5101b5442bcc7000
PCI Address = 00:1c:00:00
System Time = 11/26/2019 16:22:10
Mfg. Date = 00/00/00
Controller Time = 11/26/2019 16:22:10
FW Package Build = 24.16.0-0106
BIOS Version = 6.32.02.0_4.17.08.00_0x06150500
FW Version = 4.660.00-8102
Driver Name = megasas2.sys
Driver Version = 6.712.13.00
Current Personality = RAID-Mode
Vendor Id = 0x1000
Device Id = 0x5D
SubVendor Id = 0x19E5
SubDevice Id = 0xD207
Host Interface = PCI-E
Device Interface = SAS-12G
Bus Number = 28
Device Number = 0
Function Number = 0
Drive Groups = 1

TOPOLOGY :
=====
DG Arr Row EID:Slot DID Type State BT Size PDC PI SED DS3 FSpace TR
-----
0 - - - - RAID0 Optl N 556.929 GB dflt N N none N N
0 0 - - - RAID0 Optl N 556.929 GB dflt N N none N N
0 0 0 34:7 63 DRIVE Onln N 837.258 GB dflt N N none - N
0 0 1 34:6 62 DRIVE Onln N 278.464 GB dflt N N none - N
```

6. Run the `.\storcli64.exe /c0/eall/sall show` command to query hard drive information.
`.\storcli64.exe /c0/eall/sall show`

```
PS C:\Users\Administrator> .\storcli64.exe /c0/eall/sall show
Controller = 0
Status = Success
Description = Show Drive Information Succeeded.

Drive Information :
=====
EID:Slr DID State DG          Size Intf Med SED PI SeSz Model          Sp
-----
34:2    58 UGood -    1.745 TB SAS  SSD N   N  512B SDLL1CLR020T5CHS U
34:3    59 UGood -    1.454 TB SAS  SSD N   N  512B SDLL1CLR016T5CHS U
34:4    60 UGood -    1.454 TB SAS  SSD N   N  512B SDLL1CLR016T5CHS U
34:5    61 UGood -    1.454 TB SAS  SSD N   N  512B SDLL1CLR016T5CHS U
34:6    62 Onln  0   278.464 GB SAS  HDD N   N  512B ST300MM0008      U
34:7    63 Onln  0   837.258 GB SAS  HDD N   N  512B ST900MM0168      U
=====
```

Step 4 Upgrade the firmware of the RAID controller card. **NOTE**

If the upgrade fails or a rollback is required, contact technical support.

Run the **.\storcli64.exe /CController_ID download file=3108FW4.rom noverchk** command to upgrade the firmware.

In the command, **Controller_ID** indicates the ID of the RAID controller card. You need to specify this parameter for each RAID controller card when configuring multiple RAID controller cards.

```
.\storcli64.exe /C0 download file=3108FW4.rom noverchk
```

 NOTE

- The firmware upgrade package contains two ROM files, **3108FW4.rom** and **3108FW16.rom**.
- **3108FW4.rom** is used to upgrade a RAID controller card that contains RAID information.
- **3108FW16.rom** is used to:
 - Upgrade a RAID controller card that does not contain RAID information.
 - Upgrade a RAID controller card in the DOS system.

```
PS C:\Users\Administrator\Desktop> .\storcli64.exe /c0 download file=3108FW4.rom noverchk
Download Completed.
Flashing image to adapter...
Controller = 0
Status = Success
Description = F/W Flash Completed. Please reboot the system for the changes to take effect
```

Step 5 Power off and then power on the server for the firmware to take effect. The procedure is as follows:

1. Run the **poweroff** command to power off the server.
poweroff
2. After the server is powered off, click  on the toolbar of the virtual console, and choose **Power On** from the drop-down list.

Step 6 Verify the upgrade.

Repeat [Step 3](#) to query the firmware version, RAID array, and hard drive information.

The upgrade is successful if the firmware version of the RAID controller card is the target version and the RAID array and hard drive information is the same as that before the upgrade.

----End

1.10.2.3 Rolling Back the Firmware Version

1.10.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

1.10.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.10.2.2 Performing the Upgrade](#).

----End

2 Upgrading the NIC Firmware

NOTICE

Before upgrading the NIC firmware, query the value of **Secure Boot Status**.

- If the value is **Disabled**, perform the upgrade directly.
- If the value is **Enabled**, set **Secure Boot Status** to **Disabled** before upgrading the NIC. After the NIC is upgraded, set **Secure Boot Status** to **Enabled**.

For details about how to query and set **Secure Boot Status**, see "Front Page" > "Administer Secure Boot" in the [Huawei Server Purley Platform BIOS Parameter Reference](#).

After the firmware is upgraded, if you need to restart or power cycle the server for the firmware to take effect, services will be interrupted. Exercise caution when performing this operation.

[2.1 Before You Start](#)

[2.2 Upgrading the NIC Firmware Using a Script](#)

[2.3 Upgrading the NIC Firmware Using Smart Provisioning](#)

[2.4 Upgrading the NIC Firmware Using SmartKit](#)

[2.5 Upgrading the NIC Firmware Using FwUpgrade](#)

2.1 Before You Start

- Use the [Computing Product Compatibility Checker](#) to check the compatibility between servers and NICs.
- To check the servers supported by the tools, perform the following steps:
 - Smart Provisioning: See **Product Overview > Software and Hardware Compatibility** in the [Smart Provisioning User Guide](#).
 - SmartKit Computing: See **Using SmartKit > Firmware Upgrade > Upgrading Server Firmware > Compatibility List** in the [SmartKit Computing User Guide](#).
 - The NIC firmware can be upgraded using FwUpgrade on only V2 and V3 servers.

- Check the upgrade methods supported by the NIC firmware package. Before downloading the firmware package, read the software description of the firmware package, as shown in [Figure 2-1](#).

Figure 2-1 Firmware package software description

Software Name	Size	Publication Date	Downloads	Download software	Manual Verification Signature File	Automatic Verification Signature File
☐ NIC-SP670-1822-FW-15.7.6.1-X86.zip FW file, support for Mount Smart Provisioning 1.2.1 on SmartKit	2.22MB	2023-06-30	1	↓	pgp	cms
☐ NIC-SP680-1822-FW-15.7.6.1-X86.zip FW file, support for Mount Smart Provisioning 1.2.1 on SmartKit	2.22MB	2023-06-30	0	↓	pgp	cms
☐ NIC-SP681-1822-FW-15.7.6.1-X86.zip FW file, support for Mount Smart Provisioning 1.2.1 on SmartKit	2.22MB	2023-06-30	0	↓	pgp	cms

2.2 Upgrading the NIC Firmware Using a Script

2.2.1 Preparing for the Upgrade

2.2.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 2-1](#).

Table 2-1 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of a NIC	1. Log in to FusionServer iDriver or Computing Component iDriver. 2. Click the recommended version. The software list is displayed. 3. Set Software Type to FW. 4. Download the required firmware upgrade package to the client (local PC) and decompress it. NOTE Download the driver package based on the driver version mapping table. For details about how to install the drivers, see "Installing and Upgrading the Drivers" in the corresponding OS installation guide.
Driver package	Download the driver package by referring to the driver version mapping table. For details about how to obtain and upgrade the drivers, see "Installing and Upgrading Drivers and Firmware" in the Huawei Server OS Installation Guide (x86).

Software Package Description

Table 1-4 lists the files contained in the NIC firmware upgrade package.

Table 2-2 Software package description

File	Description
drivers folder	(Optional) Driver file matching the firmware version. The firmware package may not contain this folder or does not contain the driver of a specified OS. In this case, download the driver by referring to "Procedure".
tools folder	NIC command line management tool.
• *.rom • *.bin • *.img	NIC firmware.
	Script file for automatic firmware upgrade.
install.sh	Script file for automatic firmware upgrade.
version.xml	Version description file.

2.2.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After the software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

2.2.2 Performing the Upgrade

Conditions

- The NIC driver has been installed.
- You have downloaded the NIC firmware upgrade package.

For details about the upgrade package name and how to obtain the upgrade package, see [1.2.2.1 Obtaining Software Packages](#).

Impact

Do not perform any power-off operation during the upgrade and do not change configurations except for those involved in the upgrade guide.

Procedure

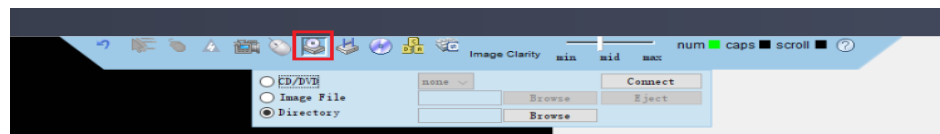
Step 1 Mount the upgrade file.

NOTE

The iBMC Remote Virtual Consoles include the Java Remote Virtual Console and HTML5 Integrated Remote Console. The HTML5 Integrated Remote Console does not support local directories. This section uses the Java Remote Virtual Console as an example. For more information, see the [iBMC User Guide](#).

1. On the toolbar of the virtual console, click  to display the screen shown in [Figure 2-2](#).

Figure 2-2 Virtual CD/DVD drive



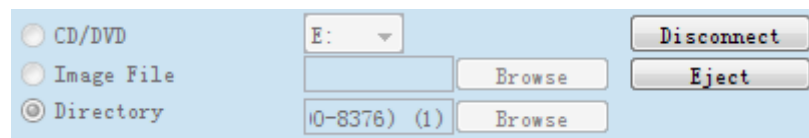
2. Select **Directory** and click **Browse**.
3. Select the folder generated after the controller card firmware upgrade package is decompressed.

NOTE

Select the folder of the target version for an upgrade or the folder of the source version for a rollback.

4. Click **Connect**.
If the **Eject** icon is available, as shown in [Figure 2-3](#), the file is successfully mounted.

Figure 2-3 Toolbar



Step 2 Copy the upgrade file to the server and grant the read and write permissions to the file.

1. On the OS, run the **mkdir fw** command to create the **fw** folder in the **root** directory.
2. Run the **mount /dev/sr0 /mnt** command to mount the local folder to the **/mnt** directory.

 NOTE

After you enter **mount /dev/sr**, press **Tab** to display the value following **sr**.

3. Run the **cp -vr /mnt/* /root/fw/** command to copy the mounted file to the **fw** directory.
4. Run the **cd /root/fw/** command to go to the **fw** directory.
5. Run the **chmod 777 *** command to add read and write permissions for the file.

Step 3 Run the following command to upgrade the NIC firmware using the one-click upgrade script:

./install.sh upgrade or **bash install.sh upgrade**

 NOTE

- If the server has multiple NICs of the same model, the script automatically upgrades the NICs of all these controller cards to the target version.
- You can run the **cat work.log** command to open the **work.log** file to view the upgrade log information.

Step 4 Run the following command to restart the server for the firmware to take effect:

reboot

 NOTE

- It takes 5 to 10 minutes for the server to restart.
- After upgrading the firmware, upgrade the controller card driver to a version that matches the firmware. For details about how to obtain and upgrade the driver, see "Installing and Upgrading Drivers and Firmware" in [Huawei Server OS Installation Guide \(Arm\)](#).

Step 5 (Optional) Upgrade the NIC driver to a version that matches the firmware.

For details about how to obtain and upgrade the driver, see section "Installing and Upgrading Drivers and Firmware" in the [Huawei Server OS Installation Guide \(x86\)](#).

----End

2.2.3 Rolling Back a Version

2.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

2.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [1.2.3 Performing the Upgrade](#).

----End

2.3 Upgrading the NIC Firmware Using Smart Provisioning

NOTICE

For details about the servers supported by Smart Provisioning, see the **Supported server** table in "User Guide" > "Overview" in the [Smart Provisioning User Guide](#).

2.3.1 Preparing for the Upgrade

2.3.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 2-3](#).

Table 2-3 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of a NIC	- Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. NOTE - The required Smart Provisioning version varies depending on the firmware package version. For details, see the software description at the download website. - Download the driver package based on the driver version mapping table. For details about how to install the drivers, see "Installing and Upgrading the Drivers" in the corresponding OS installation guide.

Type	How to Obtain
Smart Provisioning tool package	1. Log in to the Smart Provisioning download page. 2. You are advised to select the latest version. 3. Download the Smart Provisioning tool package and digital signature file from the software list. 4. Decompress the Smart Provisioning tool package to obtain the .iso file of Smart Provisioning.

2.3.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

2.3.2 Performing the Upgrade

For details, see **Using Smart Provisioning > GUI Introduction > Performing Upgrades > Upgrading Firmware** in the [Smart Provisioning User Guide](#).

2.3.3 Rolling Back a Version

2.3.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

2.3.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see the [Smart Provisioning User Guide](#).

----End

2.4 Upgrading the NIC Firmware Using SmartKit

NOTE

For details about the servers supported by SmartKit Computing, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" > "Compatibility List" in the [SmartKit Computing User Guide](#).

2.4.1 Preparing for the Upgrade

2.4.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 2-4](#).

Table 2-4 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of a NIC	- Log in to FusionServer iDriver or Computing Component iDriver. - Click the recommended version. The software list is displayed. - Set Software Type to FW. - Download the required firmware upgrade package to the client (local PC) and decompress it. NOTE Download the driver package based on the driver version mapping table. For details about how to install the drivers, see "Installing and Upgrading the Drivers" in the corresponding OS installation guide.

Type	How to Obtain
SmartKit tool package	1. Click the following link to go to the page for downloading SmartKit Computing: • Enterprise users: SmartKit Computing download page • Carrier website users: SmartKit Computing download page 2. Select All next to Select Version. 3. Click the latest SmartKit Computing version. The software list is displayed. 4. Select the SmartKit tool package from the software list. 5. Download the SmartKit tool package and digital signature file.

2.4.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

2.4.2 Performing the Upgrade

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading PCIe Card and Hard Disk Firmware" in the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plug-in version.

2.4.3 Rolling Back a Version

2.4.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

2.4.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plugin version.

----End

2.5 Upgrading the NIC Firmware Using FwUpgrade

NOTICE

The NIC firmware can be upgraded using FwUpgrade only on V2 and V3 servers.

2.5.1 Preparing for the Upgrade

2.5.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 2-5](#).

Table 2-5 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of a NIC	1. Log in to FusionServer iDriver or Computing Component iDriver. 2. Click the recommended version. The software list is displayed. 3. Set Software Type to FW. 4. Download the required firmware upgrade package to the client (local PC) and decompress it. NOTE • The required FwUpgrade version varies depending on the firmware package version. For details, see the software description at the download website. • Download the driver package based on the driver version mapping table. For details about how to install the drivers, see "Installing and Upgrading the Drivers" in the corresponding OS installation guide.
FwUpgrade tool package	1. Visit the SmartKit Computing website. 2. You are advised to select the latest version. 3. Download the FwUpgrade tool package and digital signature file from the tool list.

2.5.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

2.5.2 Performing the Upgrade

For details, see "Using FwUpgrade" in the [SmartKit Computing 1.0.0 FwUpgrade User Guide](#).

2.5.3 Rolling Back a Version

2.5.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

2.5.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see the [SmartKit Computing 1.0.0 FwUpgrade User Guide](#).

----End

3 Upgrading the Firmware of Chassis Components

NOTICE

After the firmware is upgraded, if you need to restart or power cycle the server for the firmware to take effect, services will be interrupted. Exercise caution when performing this operation.

- [3.1 Upgrading the iBMC](#)
- [3.2 Upgrading the BIOS](#)
- [3.3 Upgrading the HMM](#)
- [3.4 Upgrading the HMM CPLD](#)
- [3.5 Upgrading the Mainboard CPLD](#)
- [3.6 Upgrading the Hard Drive Backplane CPLD](#)
- [3.7 Upgrading the Fan Management Board CPLD](#)
- [3.8 Upgrading the Riser Card CPLD](#)
- [3.9 Upgrading the LCD Firmware](#)
- [3.10 Upgrading the Drive Backplane Expander Firmware](#)
- [3.11 Upgrading the SD Card Controller Firmware](#)
- [3.12 Upgrading the PSUs](#)
- [3.13 Upgrading Smart Provisioning](#)

3.1 Upgrading the iBMC

3.1.1 Using the iBMC WebUI to Upgrade the iBMC

3.1.1.1 Before You Start

3.1.1.1.1 Impact of the Upgrade

Before you upgrade to a new version, read this section carefully to find out the possible impact on the system.

Impact on the System

Table 3-1 describes the impact of the upgrade on the system.

Table 3-1 Impact on the system

No.	Item	Impact	Impact Description
1	iBMC	Impact on services	None
		Impact on O&M	- Other operations are not allowed during the upgrade. - After the iBMC is upgraded, restart the iBMC for the new version to take effect. You can restart the system immediately or later. - During the iBMC restart process, the fans rotate at full speed, which increases and the power consumption. Insufficient power supply causes power-off of the cabinet. NOTE iBMC 2.36 and later will restart automatically after the upgrade.
2	iBMC language pack	Impact on services	None
		Impact on O&M	None

Impact on the Parts

None

3.1.1.1.2 Precautions

Table 3-2 describes the precautions for upgrading the server.

Table 3-2 Precautions for the upgrade

No.	Description
1	Read this document before upgrading the server. For any problems or suggestions pertaining to the document, contact technical support.
2	Perform the upgrade during off-peak hours to minimize the impact on the system and services.
3	Time required for a software upgrade: • iBMC: 15 to 20 minutes • iBMC language pack: 2 minutes

3.1.1.1.3 Version Requirements

If you need to upgrade the iBMC from a version earlier than an intermediate version to a version later than the intermediate version, upgrade the iBMC to the intermediate version and then the target version. If the upgrade to the intermediate version fails, restart the iBMC and try again. [Table 3-3](#) lists the server models and their intermediate iBMC versions. For example, if the source iBMC version of an XH622 V3 is earlier than V296 and the target version is later than V296, you need to upgrade the iBMC to V296 and then to the target version. If the upgrade to V296 fails, restart the iBMC and try again.

Table 3-3 Mapping between intermediate iBMC versions and server models

Intermediate Version	Model
296	XH620 V3/XH622 V3/XH628 V3/XH321 V3/XH310 V3

NOTE

VLAN configuration is supported for iBMC 510 and later versions when the management network port is in dedicated mode. If the iBMC is upgraded from a version later than 510 to 510 or an earlier version, VLAN configuration is not supported although the management network port is in dedicated mode, but the VLAN configuration before the upgrade is still valid. To use the VLAN configuration function in dedicated mode of the management network port, ensure that the iBMC version is 510 or later.

3.1.1.2 Preparing for the Upgrade

3.1.1.2.1 Pre-upgrade Checklist

Perform a check according to [Table 3-4](#) and record the check results.

Table 3-4 Pre-upgrade checklist

No.	Item	Operation and Expected Result
1	System software version	1. View and record the current iBMC versions. For details, see 5.7 Check the Software Version of the Server Node.. 2. Check that the source versions are earlier than target versions.
2	System operating status	Check iBMC system operating status: • If no minor alarm, major alarm, or critical alarm is generated, continue the upgrade process. For details, see 5.8 Viewing Server Node Alarms. • If an alarm is generated, contact technical support.

3.1.1.2.2 Obtaining the Upgrade Packages and Documents

You can obtain the upgrade packages and documents as follows:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Select the server to be upgraded.
The server version list is displayed.
 - c. Select the target version.
The version list displays all the supported software versions.
 - d. Download and decompress the upgrade packages to a local PC. [Table 3-5](#) lists the upgrade packages to be obtained.

 NOTE

You are advised to decompress the upgrade package to an English path.
Otherwise, the upgrade may fail.

Table 3-5 Firmware package

Name	Function	Required File after Decompression
iBMC	iBMC firmware upgrade package	image.hpm or <i>server model-iBMC-iBMC version.hpm</i>

- e. Download the documents required for the upgrade from the same page.
Documents to be obtained are as follows:
 - *Release Notes*
 - *Upgrade Guide*
 - *Version Mapping*

- Carrier users: Contact technical support of your local Huawei office.

3.1.1.2.3 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - a. Log in to [Intelligent Servers](#).
 - b. In the server list, click the server on which you want to perform a firmware rollback.
The server version list is displayed.
 - c. Check the current firmware version according to the procedure described in [3.1.1.2.1 Pre-upgrade Checklist](#).
 - d. Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to [e](#).
 - If the target version is not in the version list, contact technical support.
 - e. Download the rollback package to a client (local PC) and decompress it. [Table 3-6](#) lists the rollback package to be obtained.

Table 3-6 Firmware package

Name	Function	Required File after Decompression
iBMC	iBMC firmware rollback package	image.hpm or <i>server model-iBMC-iBMC version.hpm</i>

- Carrier users: Contact technical support of your local Huawei office.

3.1.1.2.4 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.1.1.3 Upgrading the iBMC

3.1.1.3.1 Performing the Upgrade

Scenarios

Upgrade the iBMC.

NOTE

- The system user name and password remain unchanged after the upgrade.
- Do not refresh the current upgrade page of the browser during the upgrade.
- If the iBMC version is in Vxxx format, you need to upgrade the backup image first. After the backup image is upgraded, the primary iBMC image is automatically restarted and an automatic primary/backup image switchover is performed without the need to click **Image Switchover**. After the switchover is complete, upgrade the backup image (the original primary image before the switchover). If the iBMC version is in x.xx.xx.xx format, only one upgrade operation is required to upgrade both the primary and backup images, and you can perform another upgrade for upgrading the available partition image.
- During the iBMC restart process, the fans rotate at full speed, which increases and the power consumption. Insufficient power supply causes power-off of the cabinet.
- VLAN configuration is supported for iBMC 510 and later versions when the management network port is in dedicated mode. If the iBMC is upgraded from a version later than 510 to 510 or an earlier version, VLAN configuration is not supported although the management network port is in dedicated mode, but the VLAN configuration before the upgrade is still valid. To use the VLAN configuration function in dedicated mode of the management network port, ensure that the iBMC version is 510 or later.

If you need to upgrade the iBMC from a version earlier than an intermediate version to a version later than the intermediate version, upgrade the iBMC to the intermediate version and then the target version. If the upgrade to the intermediate version fails, restart the iBMC and try again. [Table 3-7](#) lists the server models and their intermediate iBMC versions. For example, if the source iBMC version of an XH622 V3 is earlier than V296 and the target version is later than V296, you need to upgrade the iBMC to V296 and then to the target version. If the upgrade to V296 fails, restart the iBMC and try again.

Table 3-7 Mapping between intermediate iBMC versions and server models

Intermediate Version	Model
296	XH620 V3/XH622 V3/XH628 V3/XH321 V3/XH310 V3

Impact on the System

Upgrading the iBMC will cause the iBMC system to restart twice. Perform the upgrade during the off-peak hours.

Prerequisites

Conditions

- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).
- There is no minor, major, or critical alarm on the iBMC.

Data

This operation requires no data preparation.

Software

You have obtained and decompressed the upgrade package. For details, see [3.1.1.2.2 Obtaining the Upgrade Packages and Documents](#).

Procedure

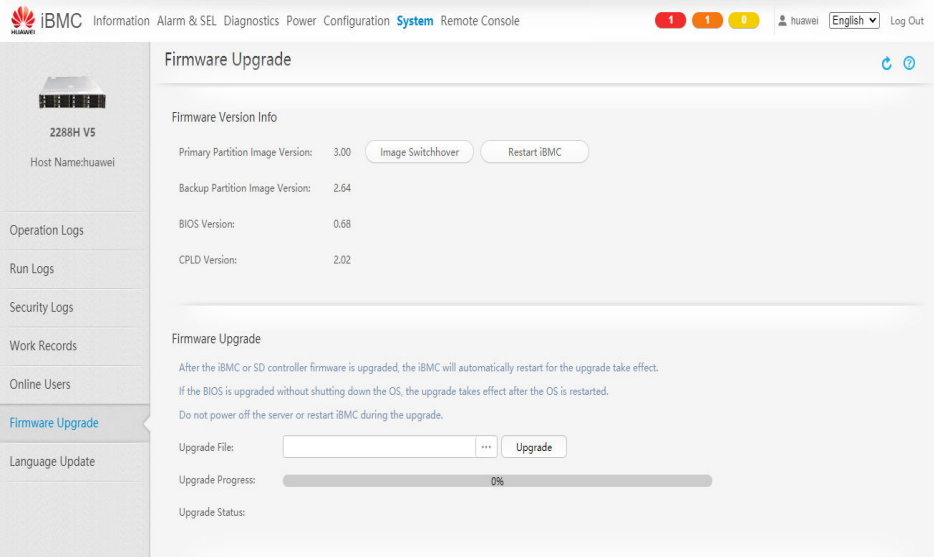
NOTICE

If the iBMC version is earlier than 2.56, restart the iBMC before upgrading the firmware. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System > Firmware Upgrade**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.2 Logging In to the iBMC WebUI](#).
 - Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).
-

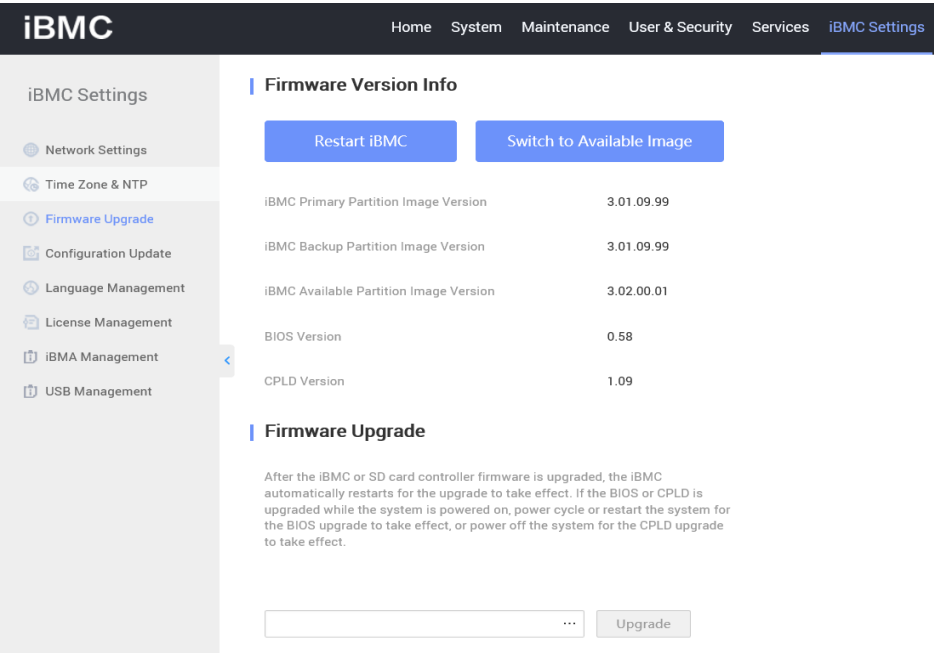
- Step 1** Upgrade the backup iBMC image. The iBMC WebUI varies depending on the iBMC version.
- If the iBMC version is earlier than V561, choose **System > Firmware Upgrade**. The **Firmware Upgrade** page is displayed, as shown in [Figure 3-1](#).

Figure 3-1 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in *x.xx.xx.xx* format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The **Firmware Upgrade** page is displayed, as shown in [Figure 3-2](#).

Figure 3-2 Firmware Upgrade page (iBMC V561 or later)



NOTE

The page displayed for firmware upgrade varies depending on the iBMC version.

Step 2 In the **Firmware Upgrade** area, click .

A window is displayed for you to select the upgrade file.

Step 3 Select the upgrade file from a directory on the PC.

Step 4 Click **Open**.

After the upgrade file is selected, the **Firmware Upgrade** page is displayed.

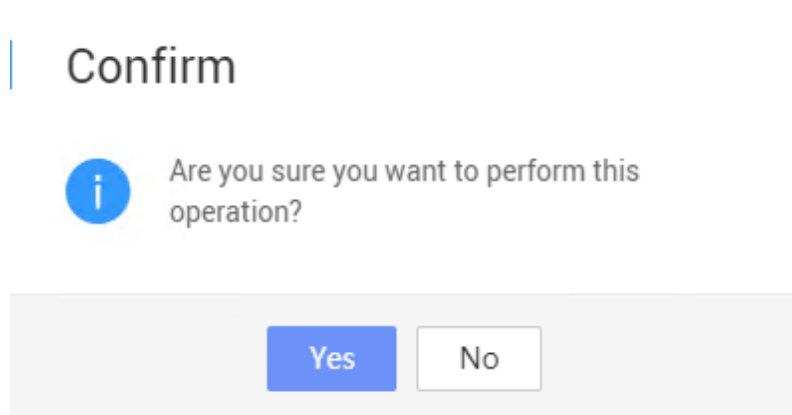
 NOTE

Select "Restart iBMC immediately after upgrade" if this option is available.

Step 5 Click **Upgrade**.

A confirmation dialog box is displayed, as shown in [Figure 3-3](#).

Figure 3-3 Confirm dialog box



 NOTE

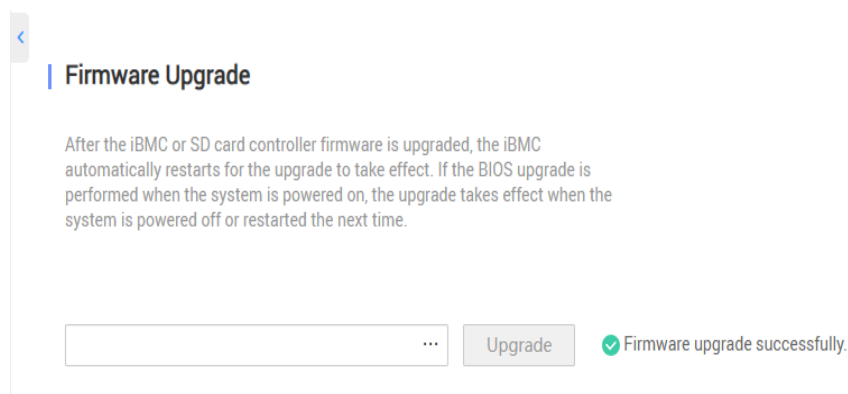
The **Confirm** dialog box varies depending on the iBMC version.

Step 6 Click **Yes**.

The iBMC then starts the upgrade.

Upgrade of the backup iBMC image takes about 5 to 10 minutes.

After the upgrade is successful, the following message is displayed on the **Firmware Upgrade** page:



 NOTE

- After the upgrade is completed, the iBMC system automatically restarts, and an automatic primary/backup image switchover is performed. You do not need to click **Image Switchover** on the iBMC WebUI.
- If the iBMC version is in Vxxx format, go to [Step 7](#). If the iBMC version is in x.xx.xx.xx format, perform [Step 8](#) and [Step 9](#).

Step 7 Upgrade the original primary iBMC image.

1. Log in to the iBMC WebUI again.
2. Repeat [Step 1](#) to [Step 6](#) to upgrade the original primary iBMC image.

Step 8 After the iBMC is restarted, log in to the iBMC WebUI again. The primary and backup images are of the latest version.

Step 9 Repeat [Step 1](#) to [Step 6](#) to upgrade the iBMC available partition image.

----End

3.1.1.3.2 Verifying the Upgrade

Verification Checklist

[Table 3-8](#) describes the iBMC upgrade verification checklist.

Table 3-8 Verification checklist

No.	Item	Expected Result
1	Log in to the iBMC WebUI	You can log in to the iBMC WebUI using the Internet Explorer.
2	iBMC version	The iBMC is of the target version.

Verification Procedure and Troubleshooting

Procedure

1. Log in to the iBMC WebUI again.
For details, see [5.2 Logging In to the iBMC WebUI](#).
2. Check the iBMC version.
For details, see [5.7 Check the Software Version of the Server Node..](#)
Check that the iBMC is of the target version.

Troubleshooting

- If you cannot log in to the iBMC WebUI after the iBMC upgrade, contact technical support.
- If the iBMC is not of the target version or an error message is displayed, upgrade the iBMC again. If the iBMC still cannot be upgraded successfully, record the steps you have taken and the results, and send the information to technical support.

3.1.1.4 Upgrading iBMC Language Packs

3.1.1.4.1 Upgrade Procedure

Scenarios

Update the iBMC language packages.

NOTE

- Only iBMC 2.56 and later versions allows users to install and uninstall language packages.
- Only administrators and users with common setting permissions have the rights to install and uninstall language packages.
- The English and Chinese language packages cannot be uninstalled.

Impact on the System

None

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

This operation requires no data preparation.

Software

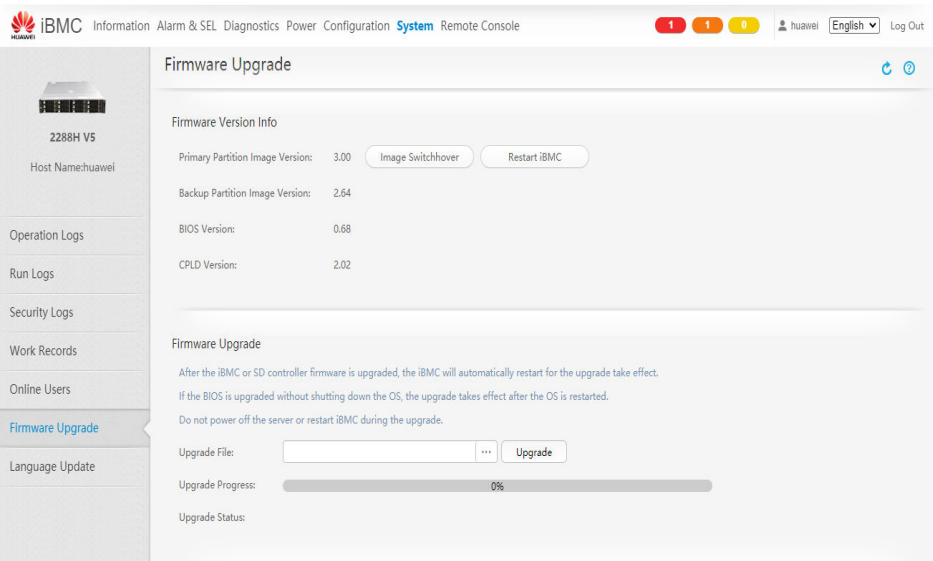
You have obtained **XXX-iBMC-LANG-XX-Vxxx.hpm**. For details, see [3.1.1.2.2 Obtaining the Upgrade Packages and Documents](#).

Procedure

Step 1 Update the iBMC WebUI language packages.

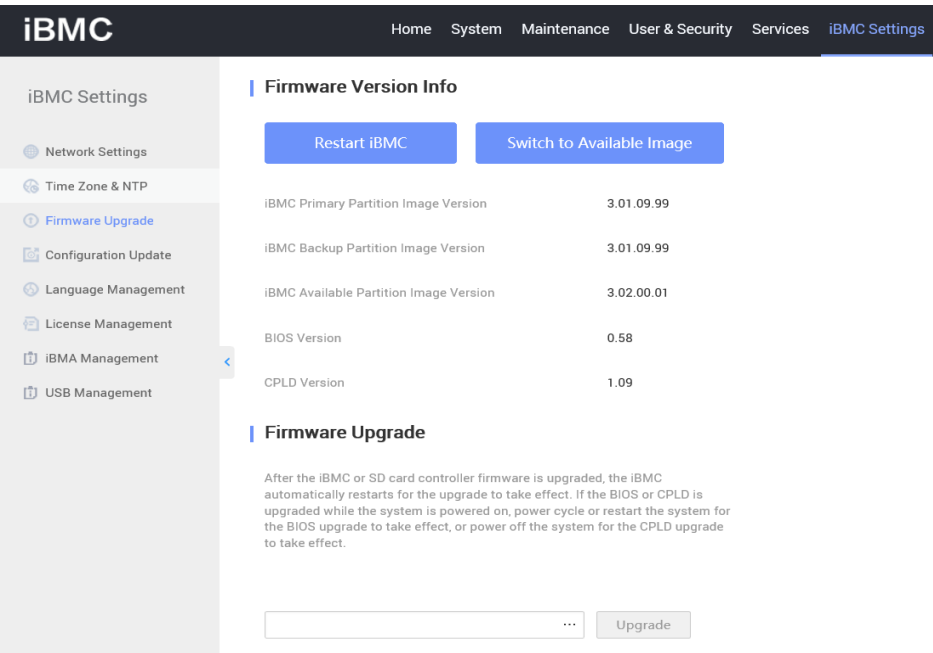
1. Open the **Firmware Upgrade** page on the iBMC WebUI. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System > Firmware Upgrade** on the iBMC WebUI.
The page shown in [Figure 3-4](#) is displayed.

Figure 3-4 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The page shown in [Figure 3-5](#) is displayed.

Figure 3-5 Firmware Upgrade page (iBMC V561 or later)

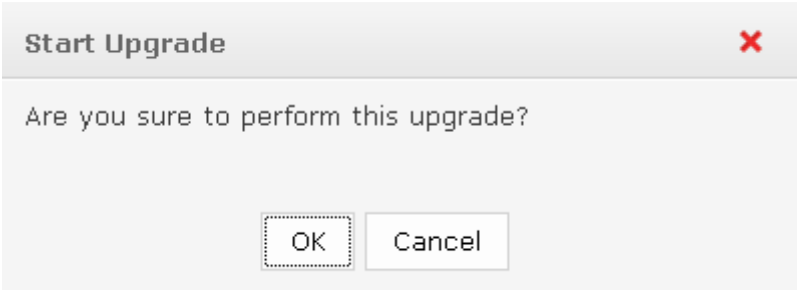


NOTE

The page displayed for firmware upgrade varies with iBMC versions.

2. In the **Firmware Upgrade** area, click .
A window is displayed for you to select the upgrade file.
3. Select the upgrade file, for example, **image.hpm**, from a local directory on the PC.

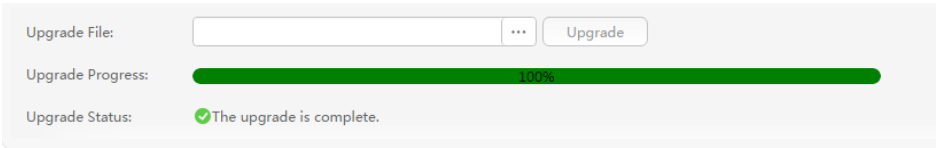
4. Click **Open**.
After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
5. Click **Upgrade**.
A confirmation dialog box is displayed.



 NOTE

The confirmation dialog box varies depending on the iBMC version.

6. Click **OK**.
The iBMC then starts the upgrade.
The language package update takes about 2 minutes.
After the upgrade is successful, the following message is displayed on the **Firmware Upgrade** page:



Step 2 After the update is complete, you can change the language of the iBMC WebUI to the language selected in the upper right corner of the page.

-----End

3.1.1.4.2 Verifying the Upgrade

Verification Checklist

Table 3-9 describes the iBMC language pack update verification checklist.

Table 3-9 Verification checklist

No.	Item	Expected Result
1	Whether the newly supported languages can be selected on the iBMC WebUI	You can change the language of the iBMC WebUI to the language selected in the upper right corner of the page.
2	Whether the iBMC language pack version is updated	The iBMC language pack versions are the target versions.

Verification Procedure and Troubleshooting

Procedure

1. Open the **Language management** page. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System > Language Update**.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Language Management**.
2. Check the language and language package version.
3. Change the language of the iBMC WebUI to the language selected in the upper right corner of the page.

If the iBMC system language can be changed to the selected language and the language pack versions are the target versions, the update is successful.

Troubleshooting

If the iBMC language pack versions are not the target ones or an update failure message is displayed, update the iBMC language packs again. If the update still fails, record the fault information, steps you have taken, and results, and contact technical support.

3.1.1.5 Rolling Back the Firmware Version

3.1.1.5.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.1.1.5.2 Rollback Procedure

Step 1 Determine the target version.

You are advised to roll back the software to the source version.

Step 2 Roll back the software.

The rollback procedure is similar to the upgrade procedure.

----End

3.1.2 Upgrading iBMC Using SmartKit

3.1.2.1 Preparing for the Upgrade

3.1.2.1.1 Obtaining the Upgrade Package

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-10](#).

Table 3-10 Obtaining the software packages

Type	How to Obtain
iBMC upgrade package	- Enterprise users: - Log in to Intelligent Servers. - Select the server to be upgraded. The server version list is displayed. - Select the target version. The version list displays all the supported software versions. - Download the required upgrade package. - Carrier users: Contact technical support of your local Huawei office.
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.1.2.1.2 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. In the server list, click the server on which you want to perform a firmware rollback.
The server version list is displayed.
 - c. Check the current firmware version according to the procedure described in [3.1.1.2.1 Pre-upgrade Checklist](#).
 - d. Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to [e](#).
 - If the target version is not in the version list, contact technical support.
 - e. Download the required rollback file corresponding to the firmware.
- Carrier users: Contact technical support of your local Huawei office.

3.1.2.1.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.1.2.2 Performing the Upgrade

Version Requirements

If you need to upgrade the iBMC from a version earlier than an intermediate version to a version later than the intermediate version, upgrade the iBMC to the intermediate version and then the target version. If the upgrade to the intermediate version fails, restart the iBMC and try again. [Table 3-11](#) lists the server models and their intermediate iBMC versions. For example, if the source iBMC version of an XH622 V3 is earlier than V296 and the target version is later than V296, you need to upgrade the iBMC to V296 and then to the target version. If the upgrade to V296 fails, restart the iBMC and try again.

Table 3-11 Mapping between intermediate iBMC versions and server models

Intermediate Version	Model
296	XH620 V3/XH622 V3/XH628 V3/XH321 V3/XH310 V3

 NOTE

VLAN configuration is supported for iBMC 510 and later versions when the management network port is in dedicated mode. If the iBMC is upgraded from a version later than 510 to 510 or an earlier version, VLAN configuration is not supported although the management network port is in dedicated mode, but the VLAN configuration before the upgrade is still valid. To use the VLAN configuration function in dedicated mode of the management network port, ensure that the iBMC version is 510 or later.

Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the *SmartKit Computing XXX User Guide* corresponding to the SmartKit plug-in version.

3.1.2.3 Rolling Back a Version

3.1.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.1.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is the same as the upgrade procedure. For details, see the *SmartKit Computing User Guide* corresponding to the SmartKit plug-in version.

----End

3.2 Upgrading the BIOS

3.2.1 Using the iBMC Web to Upgrade the BIOS

3.2.1.1 Before You Start

3.2.1.1.1 Impact of the Upgrade

Before you upgrade to a new version, read this section carefully to find out the possible impact on the system.

Impact on the System

[Table 3-12](#) describes the impact of the upgrade on the system.

Table 3-12 Impact on the system

Impact	Impact Description
Impact on services	The server must be restarted after the upgrade, and services will be interrupted. NOTICE - When upgrading the BIOS with the server powered on, do not forcibly restart or power cycle the server if the following conditions are met: The OS has been installed on the server and is running properly, the TPM has been installed on the server, and the TXT function has been enabled. Instead, you need to enter the OS to restart the OS for the new BIOS version to take effect. For details about the TPM and TXT status, see sections "Security" and "Setting TXT" in the Huawei Server Purley Platform BIOS Parameter Reference. - When upgrading the BIOS with the server powered off, do not forcibly power off the server if the following conditions are met: The OS has been installed on the server and is running properly, the TPM has been installed on the server, and the TXT function has been enabled. Instead, you need to enter the OS to power off the server before the upgrade.
Impact on the OS	If power-off upgrade is used, the OS will be shut down and services are unavailable.
Impact on O&M	None NOTE The server must not be restarted during the upgrade.

Impact on the Parts

None.

3.2.1.1.2 Precautions

[Table 3-13](#) describes the precautions for upgrading the server.

Table 3-13 Precautions for the upgrade

No.	Description
1	Read this document before upgrading the server. For any problems or suggestions pertaining to this document, contact technical support.
2	Perform the upgrade during off-peak hours to minimize the impact on the system and services.
3	The upgrade takes about 10 minutes.

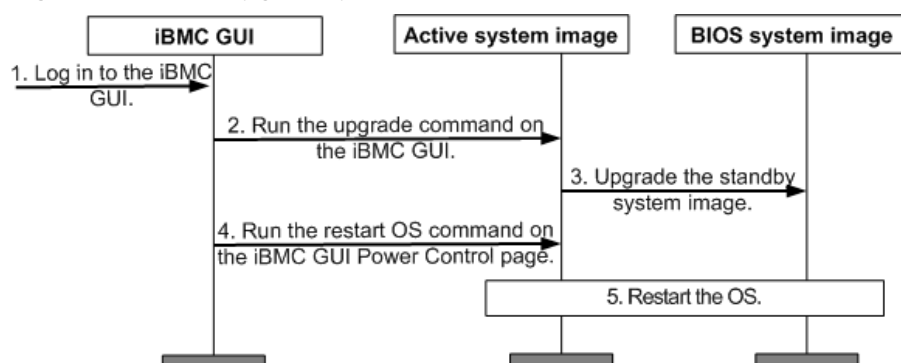
3.2.1.1.3 Version Requirements

The upgrade has no version requirement.

3.2.1.1.4 Upgrade Process

BIOS Upgrade Process

Figure 3-6 shows the BIOS upgrade process.

Figure 3-6 BIOS upgrade process

The following describes the upgrade process:

1. Log in to the iBMC WebUI.
2. Run the upgrade command on the iBMC WebUI.
3. Upgrade the BIOS image.
4. Run the restart OS command on the iBMC WebUI.
5. Restart the OS.

3.2.1.2 Preparing for the Upgrade

3.2.1.2.1 Pre-upgrade Checklist

Perform a check according to **Table 3-14** and record the check results.

Table 3-14 Pre-upgrade checklist

No.	Item	Operation and Expected Result
1	System software version	1. View and record the current BIOS versions. For details, see 5.7 Check the Software Version of the Server Node. 2. Determine the target version.
2	System operating status	Check iBMC system operating status: • If no minor alarm, major alarm, or critical alarm is generated, continue the upgrade process. For details, see 5.8 Viewing Server Node Alarms. • If an alarm is generated, contact technical support.

3.2.1.2.2 Obtaining the Upgrade Packages and Documents

To obtain the upgrade package and related documents, perform the following steps:

- Enterprise users:
 - a. Log in to [Intelligent Servers](#).
 - b. Select the server to be upgraded.
The server version list is displayed.
 - c. Select the target version.
The version list displays all the supported software versions.
 - d. Download and decompress the upgrade packages to a local PC. [Table 3-15](#) lists the upgrade packages to be obtained.

Table 3-15 Upgrade package

Name	Function	Required File after Decompression
BIOS	Firmware upgrade package of BIOS	biosimage.hpm or <i>server model-BIOS-version.hpm</i> or <i>server model-BIOS_version.hpm</i>

- e. Download the documents required for the upgrade from the same page.
Documents to be obtained are as follows:
 - *Release Notes*
 - *Upgrade Guide*
 - *Version Mapping*
- Carrier users: Contact technical support of your local Huawei office.

3.2.1.2.3 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - a. Log in to [Intelligent Servers](#).
 - b. In the server list, click the server on which you want to perform a firmware rollback.
The server version list is displayed.
 - c. Check the current firmware version according to the procedure described in [3.2.1.2.1 Pre-upgrade Checklist](#).
 - d. Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to [e](#).
 - If the target version is not in the version list, contact technical support.
 - e. Download the rollback package to a client (local PC) and decompress it. [Table 3-16](#) lists the rollback package to be obtained.

Table 3-16 Software package

Name	Function	Required File after Decompression
BIOS	BIOS firmware rollback package	biosimage.hpm or <i>server model-BIOS-version.hpm</i> or <i>server model-BIOS_version.hpm</i>

- Carrier users: Contact technical support of your local Huawei office.

3.2.1.2.4 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.2.1.3 Upgrading the BIOS

3.2.1.3.1 Upgrade Procedure

Scenarios

Upgrade the server BIOS on the **Upgrade Firmware** page of the iBMC.

The BIOS can be upgraded when the OS is powered on or powered off. After the upgrade, the OS needs to be restarted for the upgrade to take effect. The restart interrupts running services.

NOTICE

- When upgrading the BIOS with the server powered on, do not forcibly restart or power cycle the server if the following conditions are met: The OS has been installed on the server and is running properly, the TPM has been installed on the server, and the TXT function has been enabled. Instead, you need to enter the OS to restart the OS for the new BIOS version to take effect. For details about the TPM and TXT status, see sections "Security" and "Setting TXT" in the [Huawei Server Purley Platform BIOS Parameter Reference](#).
- When upgrading the BIOS with the server powered off, do not forcibly power off the server if the following conditions are met: The OS has been installed on the server and is running properly, the TPM has been installed on the server, and the TXT function has been enabled. Instead, you need to enter the OS to power off the server before the upgrade.

The BIOS can be upgraded in either of the following modes:

- Use the iBMC WebUI. For details, see **Procedure** in this section.
- Use the iBMC CLI. Run the **ipmcset -d upgrade -v <filepath>** command. For details, see the [iBMC User Guide](#).

Impact on the System

If the system does not respond or the server powers on and then off repeatedly during the BIOS upgrade, power off and then power on the server.

Procedure

Step 1 Obtain the BIOS upgrade package.

Obtain and decompress the upgrade package. For details about how to obtain the upgrade package, see [3.2.1.2.2 Obtaining the Upgrade Packages and Documents](#).

Step 2 Log in to the iBMC WebUI.

Log in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

NOTICE

If the iBMC version is in the Vxxx format and earlier than V256, restart the iBMC and then perform the upgrade. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System > Upgrade Firmware**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.2 Logging In to the iBMC WebUI](#).
- Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).

Step 3 Upgrade the BIOS.

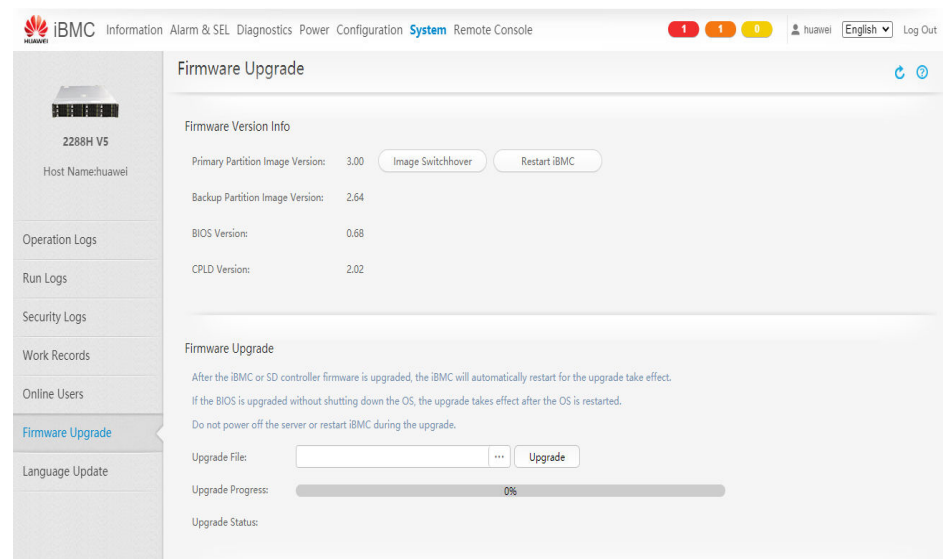
NOTE

Do not power on, power off, reset, or restart the server OS during the upgrade.

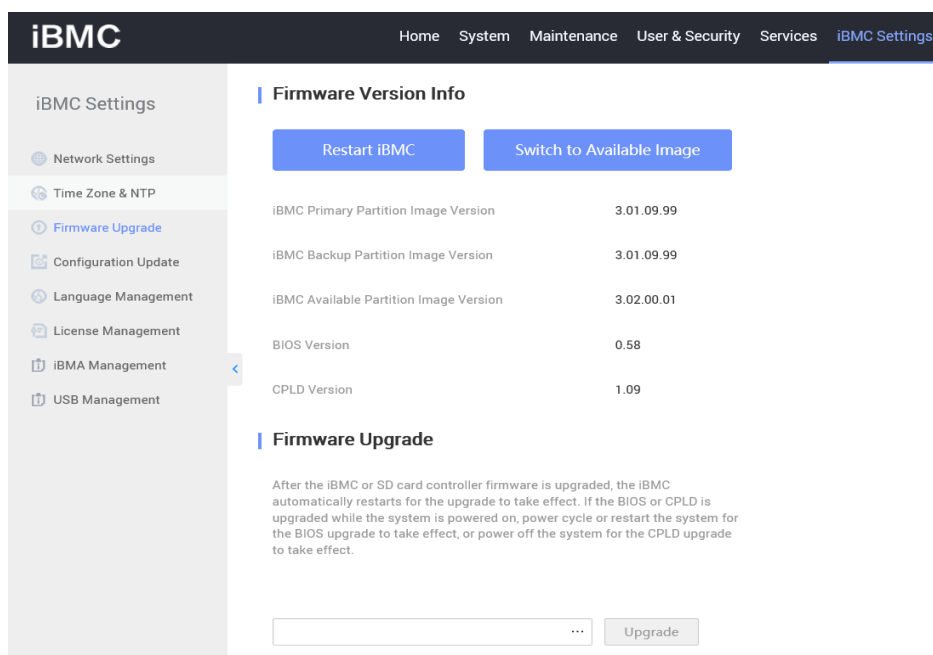
1. Open the **Firmware Upgrade** page on the iBMC WebUI. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System > Firmware Upgrade**.

The **Firmware Upgrade** page is displayed, as shown in [Figure 3-7](#).

Figure 3-7 iBMC web page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The **Firmware Upgrade** page is displayed, as shown in [Figure 3-8](#).

Figure 3-8 Firmware Upgrade page (iBMC V561 or later)**NOTE**

The page displayed for firmware upgrade varies with iBMC versions.

- -
 - In the **Firmware Upgrade** area, click .
 -
- In the displayed dialog box, select the upgrade file (for example, **XH321V6-BIOS_0.08.hpm**) from a directory on the PC, and click **Open**.

After the upgrade file is selected, the **Firmware Upgrade** page is displayed.

-
-
-
- Click **Upgrade**.
- Click **OK**.

The iBMC starts the upgrade. The upgrade preparation takes about 2 minutes. Then, the upgrade starts. The upgrade status displayed after the upgrade varies depending on the power-on or power-off status of the server during the upgrade.

- If the server is in power-off state during the upgrade, "The upgrade is complete" will be displayed after the upgrade.
- If the server is in power-on state during the upgrade:
 - For V2 servers or V3 servers whose iBMC version is earlier than V252, "The upgrade is complete" will be displayed after the upgrade.
 - For V5 or V6 servers or V3 servers whose iBMC version is V252 or later, "File upload successfully. The upgrade takes effect automatically after the next power-off or restart" will be displayed after the upgrade.

Step 4 Make the BIOS upgrade take effect.

NOTICE

- When upgrading the BIOS with the server powered on, do not forcibly restart or power cycle the server if the following conditions are met: The OS has been installed on the server and is running properly, the TPM has been installed on the server, and the TXT function has been enabled. Instead, you need to enter the OS to restart the OS for the new BIOS version to take effect. For details about the TPM and TXT status, see sections "Security" and "Setting TXT" in the [Huawei Server Purley Platform BIOS Parameter Reference](#).
 - When upgrading the BIOS with the server powered off, do not forcibly power off the server if the following conditions are met: The OS has been installed on the server and is running properly, the TPM has been installed on the server, and the TXT function has been enabled. Instead, you need to enter the OS to power off the server before the upgrade.
-
- If the upgrade is performed while the server is powered off, power on the server for the upgrade to take effect.
 - If the iBMC version is earlier than V561, choose **Power > Power Control**, click **Power On**, and click **Yes** in the dialog box displayed.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, click **Power On**, and click **Yes** in the dialog box displayed.
 - If the BIOS is upgraded in power-on state, the operations vary depending on whether an OS is installed.

NOTICE

- The **Power Control** page varies slightly depending on the iBMC version. For details, see the iBMC online help.
 - You can use the remote virtual console to view the server power-on process.
 - If the iBMC version is earlier than V561, click **Remote Control** on the iBMC WebUI and click an installed remote console in the **Integrated Remote Console** area.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, click an installed remote console in **Virtual Console** on the **Home** page.
 - If the OS has been installed and is running properly on the server, forcibly restarting the server on the iBMC WebUI may damage user programs or unsaved user data. Select an appropriate restart mode based on actual requirements.
 - If the server fails to start after a forced restart, shut down the server, roll back the BIOS to the source version, and then upgrade the BIOS to the target version. For details, see [Step 1](#) to [Step 4](#).
-
- If the OS has been installed:

- Start the OS, log in to the OS, and restart it. The new BIOS version takes effect about 10 minutes after the server is restarted.
- If the OS cannot be started, forcibly restart the server on the iBMC WebUI.
If the iBMC version is earlier than V561, choose **Power > Power Control**, click **Forced System Reset**, and click **Yes** in the dialog box displayed.
If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, click **Forced Restart**, and click **OK** in the dialog box displayed.
The new BIOS version takes effect about 10 minutes after the server is restarted.
- If the OS has not been installed:
 - Press **Ctrl+Alt+Delete** to restart the server. The new BIOS version takes effect about 10 minutes after the server is restarted.
 - If the server does not respond, forcibly restart the server on the iBMC WebUI.
If the iBMC version is earlier than V561, choose **Power > Power Control**, click **Forced System Reset**, and click **Yes** in the dialog box displayed.
If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, click **Forced Restart**, and click **OK** in the dialog box displayed.
The new BIOS version takes effect about 10 minutes after the server is restarted.

Step 5 (Optional) If you need to modify the BIOS configuration, press **Delete** during system startup to enter the BIOS.

----End

3.2.1.3.2 Verifying the Upgrade

Verification Checklist

Table 3-17 describes the BIOS upgrade verification checklist.

Table 3-17 Verification checklist

No.	Item	Expected Result
1	BIOS operating status	The server BIOS is operating properly.
2	BIOS version	The BIOS is of the target version.

Verification Procedure and Troubleshooting

Procedure

Check whether the BIOS is of the target version after system power-on. For details, see [5.7 Check the Software Version of the Server Node.](#)

Troubleshooting

Contact technical support if the BIOS does not start after the upgrade.

If the BIOS is not of the target version or an error message is displayed, upgrade the BIOS again. If the BIOS still cannot be upgraded successfully, record the steps you have taken and the results, and send the information to technical support.

3.2.1.4 Rolling Back the Firmware Version

3.2.1.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.2.1.4.2 Rollback Procedure

Step 1 Determine the target version.

You are advised to roll back the software to the source version.

Step 2 Roll back the software.

The rollback procedure is similar to the upgrade procedure.

----End

3.2.2 Upgrading the BIOS Using SmartKit

3.2.2.1 Preparing for the Upgrade

3.2.2.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-18](#).

Table 3-18 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of BIOS	- Enterprise users: - Log in to Intelligent Servers. - Select the server model. - Click Software Download. The server software list is displayed. - Determine the current firmware version based on Pre-upgrade Checklist. - Select the target version. The version list displays all the supported software versions. - If the target version is in the version list, go to f. - If the target version is not in the version list, contact technical support. - Download the required firmware upgrade package to the client (local PC) and decompress it. - Carrier users: Contact technical support of your local Huawei office.
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.2.2.1.2 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - a. Log in to [Intelligent Servers](#).
 - b. Select the server model.
 - c. Click **Software Download**. The server software version list is displayed.
 - d. Check the current firmware version according to the procedure described in [3.2.1.2.1 Pre-upgrade Checklist](#).
 - e. Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to [6](#).
 - If the target version is not in the version list, contact technical support.
 - f. Download the rollback package and digital signature file to a client (local PC).
- Carrier users: Contact technical support of your local Huawei office.

3.2.2.1.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.2.2.2 Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plug-in version.

3.2.2.3 Rolling Back the Firmware Version

3.2.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.2.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is the same as the upgrade procedure. For details, see the [SmartKit Computing User Guide](#) corresponding to the SmartKit plug-in version.

----End

3.3 Upgrading the HMM

X6000 V6 servers do not involve HMM upgrade.

3.3.1 Using the iBMC Web to Upgrade the HMM

3.3.1.1 Before You Start

3.3.1.1.1 Impact of the Upgrade

Impact on the System

Table 3-19 describes the impact of the upgrade on the system.

Table 3-19 Impact on the system

Impact	Impact Description
Impact on services	None

Impact	Impact Description
Impact on O&M	No other operations are allowed during the upgrade. After the HMM is upgraded, restart the HMM for the new version to take effect. You can restart the system immediately or later. NOTE iBMC 2.36 and later will restart automatically after the upgrade.

Impact on the Parts

None.

3.3.1.1.2 Precautions

[Table 3-20](#) describes the precautions for upgrading the server.

Table 3-20 Precautions for the upgrade

No.	Description
1	Before the upgrade, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to this document, contact technical support.
2	Perform the upgrade during off-peak hours to minimize the impact on the system and services.
3	The upgrade takes about 20 minutes. NOTE The HMM has two images working in active/standby mode. The two images must be upgraded individually. Upgrading one image takes 5 minutes to 10 minutes. For details, see 3.3.1.3.1 Upgrade Procedure.

3.3.1.1.3 Version Requirements

If you need to upgrade the HMM from a version earlier than an intermediate version to a version later than the intermediate version, upgrade the HMM to the intermediate version and then the target version. If the upgrade to the intermediate version fails, restart the HMM and try again. [Table 3-21](#) lists the compute node models and their intermediate versions. For example, if the HMM source version of an MM630 is earlier than V272 and the target version is later than V272, you need to upgrade the HMM to V272 and then to the target version. If the upgrade to V272 fails, restart the HMM and try again.

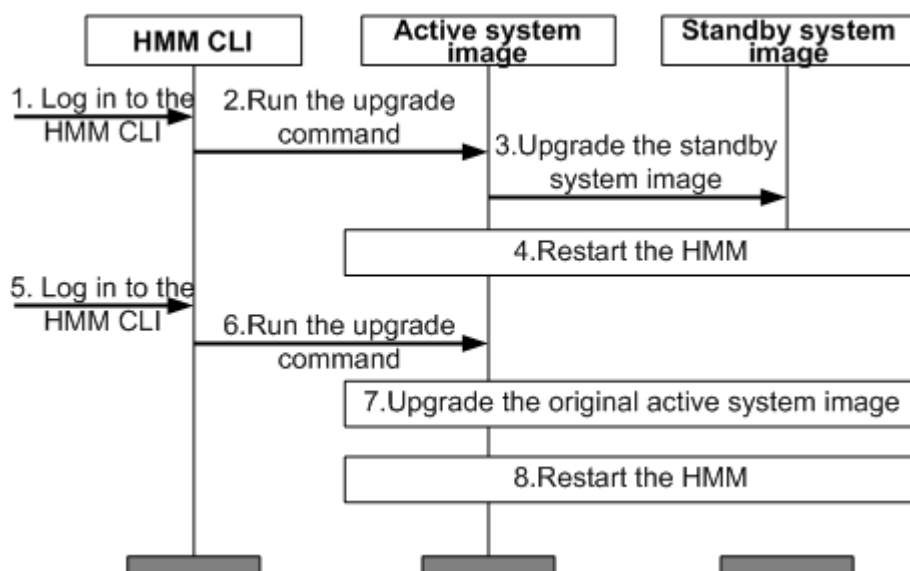
Table 3-21 HMM intermediate versions and compute node models

Intermediate Version	Model
272	MM630
330	MM810

3.3.1.1.4 Upgrade Process

HMM Upgrade Process

Figure 3-9 shows the HMM upgrade process.

Figure 3-9 HMM Upgrade Process

The detailed process description is as follows:

- Log in to the HMM CLI.
- Run the upgrade command on the HMM CLI.
- Upgrade the backup HMM system image.

NOTE

The HMM that the user has accessed is the primary system image.

- Restart the HMM system. The current login user is logged out after the system restarts, and the image file is automatically switched to the upgraded backup system image.
- Log in to the HMM CLI again.
- Run the upgrade command again on the HMM CLI.
- Upgrade the original primary HMM system image.

8. Restart the HMM system.

3.3.1.2 Preparing for the Upgrade

3.3.1.2.1 Pre-upgrade Checklist

Table 3-22 lists the items to be checked before the upgrade.

Table 3-22 Pre-upgrade checklist

No.	Item	Operation and Expected Result
1	System software version	1. View and record the current iBMC and HMM versions. For details, see 5.7 Check the Software Version of the Server Node. and 5.9 Checking the HMM Software Version. 2. Check that the source versions are earlier than target versions.
2	System operating status	Check iBMC system operating status: • If no minor alarm, major alarm, or critical alarm is generated, continue the upgrade process. For details, see 5.7 Check the Software Version of the Server Node. • If there are active alarms, contact technical support to confirm the alarms.

3.3.1.2.2 Obtaining the Upgrade Packages and Documents

To obtain the upgrade package and related documents, perform the following steps:

- Enterprise users:
 - a. Log in to the [Huawei Enterprise support](#) website.
 - b. On the home page, click **Software Download**.
 - c. In the displayed NIC list, select **Server**.
 - d. In the server list, select the server to be upgraded.
The server version list is displayed.
 - e. Select the target version.
 - f. Download and decompress the upgrade packages to a local PC. [Table 3-23](#) lists the upgrade packages to be obtained.

Table 3-23 Upgrade package

Name	Function	Required File after Decompression
HMM	HMM upgrade package	image.hpm NOTE Do not confuse the HMM upgrade package with the iBMC upgrade package. Otherwise, the HMM cannot run properly.

- g. Download the documents required for the upgrade from the same page. Documents to be obtained are as follows:
- Release Notes
 - Upgrade Guide
 - *Version Mapping*
- Carrier users: Contact technical support of your local Huawei office.

3.3.1.2.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.3.1.3 Upgrading the HMM

3.3.1.3.1 Upgrade Procedure

Scenarios

Upgrade the HMM.

If you need to upgrade the HMM from a version earlier than the intermediate version to a version later than the intermediate version, upgrade the HMM to the intermediate version and then to the target version. If the upgrade to the

intermediate version fails, restart the HMM and try again. [Table 3-24](#) lists the compute node models and their intermediate versions. For example, if the HMM source version of an MM630 is earlier than V272 and the target version is later than V272, you need to upgrade the HMM to V272 and then to the target version. If the upgrade to V272 fails, restart the HMM and try again.

Table 3-24 HMM intermediate versions and compute node models

Intermediate Version	Model
272	MM630
330	MM810

 NOTE

- The system user name and password remain unchanged after the upgrade.
- The active and standby images of the HMM must be upgraded individually.
- Upgrade the standby image first. After the standby image is upgraded, restart the server and upgrade the original active image.

Impact on the System

The HMM system restarts twice during the HMM software upgrade. Upgrade the HMM during off-peak hours to minimize the impact on services.

Prerequisites

Conditions

- You have logged in to the server using PuTTY. For details, see [5.11 Logging In to the Server Over a Network Port by Using PuTTY](#).
- There is no minor, major, or critical alarm on the HMM.

Data

This operation requires no data preparation.

Software

You have obtained **image.hpm**. For details, see [3.3.1.2.2 Obtaining the Upgrade Packages and Documents](#).

 NOTE

The X6000 has two HMM models, MM630 and MM650. Before obtaining the software package, you need to query the model and then download the software upgrade package of a proper model.

To view the HMM model, run the **ipmcget -d version** command on the HMM CLI. In the command output, **Product Name** indicates the model.

Procedure

Step 1 Log in to the HMM.

1. Log in to the HMM to upload the upgrade package. Select one of the following methods to log in to the HMM:
 - Method 1: Use the HMM IP address to log in to the HMM.
 - i. Use a cross-platform file transfer tool to connect to the HMM address.
WinSCP is an example of the cross-platform file transfer tool. For details, see [5.12 Transferring Files Using WinSCP](#).
 - ii. Copy the HMM upgrade package to the **/tmp** directory of the HMM.
 - Method 2: Use Network Address Translation (NAT) to log in to the HMM.
 - i. Log in to the HMM CLI using the server node management IP address. For details, see [5.14 Logging In to the Management Module CLI Through the Management IP Address of the Server Node](#).
 - ii. Use a cross-platform file transfer tool to connect to the iBMC management network port IP address of the server node.
WinSCP is an example of the cross-platform file transfer tool. For details, see [5.12 Transferring Files Using WinSCP](#).

NOTE

In method 2, the iBMC management network port IP address of the server node and the port number of the HMM SSH NAT service are used. The port number is **30022** by default.

Step 2 Upgrade the standby HMM image.

1. Run the **ipmcset -d notimeout -v enabled** command on the CLI to disable logout on timeout.
2. Run the **ipmcset -d upgrade -v /tmp/image.hpm** command to upgrade the HMM software.
3. Wait for the HMM system to complete the upgrade.

This process takes about 5 to 10 minutes. Ensure that the HMM is not powered off during the upgrade.

When **Update successfully** is displayed, the upgrade is successful.

```
iBMC:->ipmcset -d upgrade -v /tmp/image.hpm
Please make sure the iBMC is working while upgrading.
Updating...
100%
Update successfully.
```

After the upgrade is complete, the HMM system automatically restarts.

Step 3 Upgrade the original active HMM image.

1. Log in to the HMM CLI again after the restart.
2. Repeat [Step 1](#) to upload the software package.
3. Repeat [2](#) in [Step 2](#) to [1](#) in [step 3](#) to upgrade the original primary HMM image.

----End

3.3.1.3.2 Verifying the Upgrade

Verification Checklist

Table 3-25 describes the HMM upgrade verification checklist.

Table 3-25 Verification checklist

No.	Item	Expected Result
1	HMM version	The HMM is of the target version.

Verification Procedure and Troubleshooting

Procedure

1. Log in to the HMM CLI again.
For details, see [5.11 Logging In to the Server Over a Network Port by Using PuTTY](#).
2. Check whether the HMM is of the target version.
For details, see [5.9 Checking the HMM Software Version](#).
Ensure that the HMM version is correct.

Troubleshooting

If the login fails, contact technical support.

If the HMM is not of the target version or an error message is displayed, upgrade the HMM again. If the upgrade still fails, record the operations you have taken, and send the information to technical support.

3.3.1.4 Rolling Back the Firmware Version

3.3.1.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.3.1.4.2 Rollback Procedure

Step 1 Determine the target version.

You are advised to roll back the software to the source version.

Step 2 Roll back the software.

The operations of rolling back software to a specified version are the same as that those of upgrading the software.

----End

3.4 Upgrading the HMM CPLD

X6000 V6 servers do not involve HMM CPLD upgrade.

3.4.1 Preparing for the Upgrade

3.4.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.4.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.4.2 Upgrade Procedure

Prerequisites

Conditions

You have logged in to the HMM CLI from a client (for example, a PC).

Data

- Port ID of the login IP address.
- User name and password for logging in to the HMM. For the X6000 V3 and X6800 V3 servers, the default user name and password are **root** and **Huawei12#\$**. For the X6000 V5, X6000 V6, and X6800 V5 servers, the default user name and password are **Administrator** and **Admin@9000**.

Tools

- Secure file transfer tool, for example, XShell
- Secure terminal simulator, for example, PuTTY

Software

You have downloaded the upgrade package, for example, **X6800-HMM(BC2SMMA01)-CPLD-V005.zip**, to the client (a PC), and decompressed it to obtain the upgrade file, for example **BC2SMMA01005.hpm**.

Procedure

Step 1 Use a file transfer tool (such as XShell) to upload **BC2SMMA01005.hpm** from the client (such as a PC) to the **/tmp** directory of the HMM.

The operations vary with the tool you use. Refer to the user guide of the tool.

Step 2 On the HMM CLI, run the **ipmcget -d version** command to check the CPLD version information.

Step 3 On the HMM CLI, run the **ipmcset -d upgrade -v /tmp/BC2SMMA01005.hpm** command.

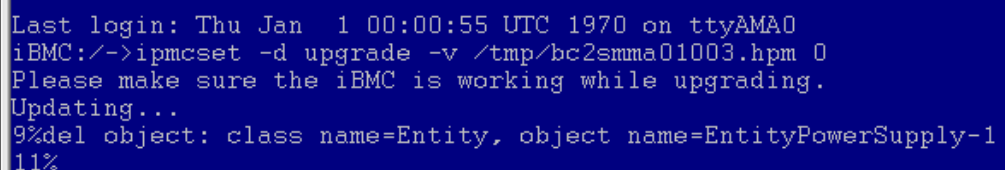
The upgrade starts, as shown in [Figure 3-10](#).

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the HMM CLI and upgrade the CPLD again.

After the upgrade is complete, the HMM restarts automatically.

Figure 3-10 Upgrading the HMM CPLD



```
Last login: Thu Jan  1 00:00:55 UTC 1970 on ttyAMA0
iBMC:/->ipmcset -d upgrade -v /tmp/bc2smma01003.hpm 0
Please make sure the iBMC is working while upgrading.
Updating...
9%del object: class name=Entity, object name=EntityPowerSupply-1
11%
```

Step 4 Upon HMM startup, run the **ipmcget -d version** command on the HMM CLI to check the CPLD version information.

----End

3.4.3 Rolling Back the Firmware Version

3.4.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.4.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.4.2 Upgrade Procedure](#).

----End

3.5 Upgrading the Mainboard CPLD

3.5.1 Upgrading the Mainboard CPLD Using the iBMC WebUI

3.5.1.1 Preparing for the Upgrade

3.5.1.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.

- e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.5.1.1.2 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server on which you want to perform a firmware rollback. The server version list is displayed.
 - c. On the displayed page, click **Software Download**. The server software version list is displayed.
 - d. Check the current firmware version.
 - If the iBMC version is earlier than V561, choose **Information > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.
 - e. Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to [f](#).
 - If the target version is not in the version list, contact technical support.
 - f. Download the rollback package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.5.1.1.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.5.1.2 Upgrade Procedure

Scenarios

Upgrade the server mainboard CPLD using the iBMC WebUI.

The mainboard CPLD can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the mainboard CPLD when the server is powered off.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

You have downloaded the mainboard CPLD upgrade package to the client (such as a PC), decompressed the package, and obtained the upgrade file.

Procedure

NOTICE

If the iBMC version is earlier than 2.56, restart the iBMC before upgrading the firmware. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System** > **Upgrade Firmware**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.4 Logging In Using the iBMC WebUI](#).
 - Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).
-

Step 1 Check the current firmware version.

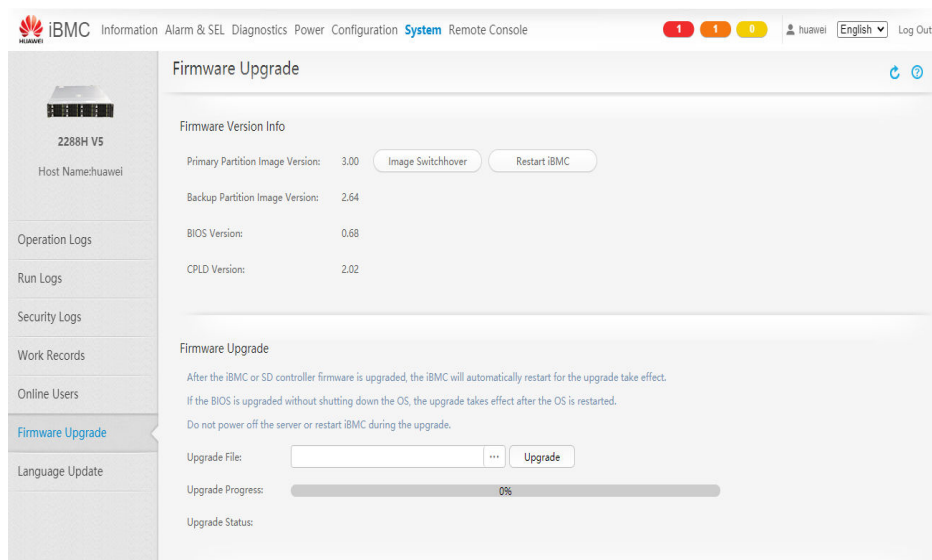
- If the iBMC version is earlier than V561, choose **Information** > **System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.

- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.

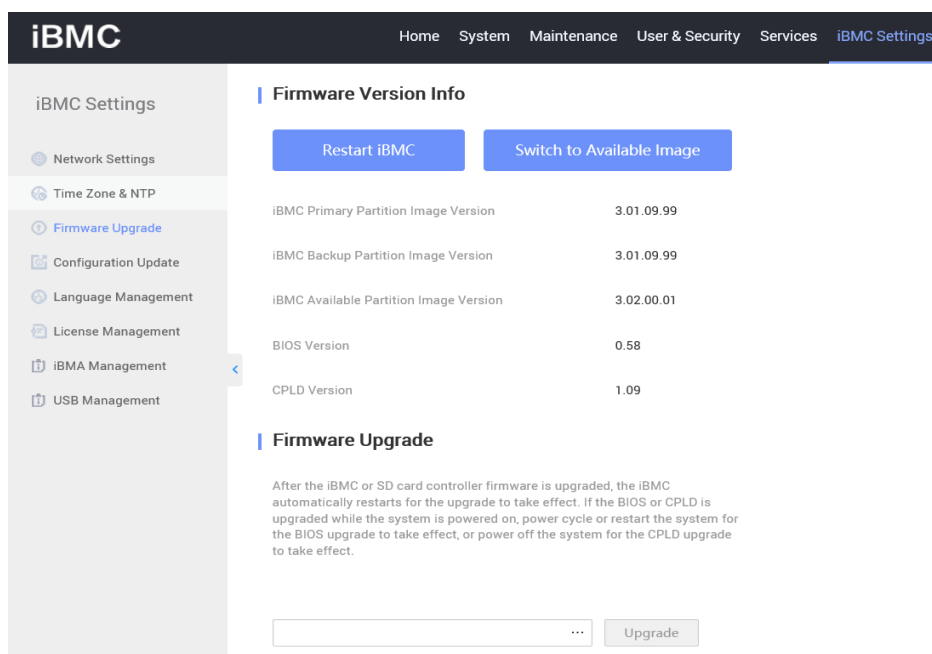
Step 2 Upgrade the mainboard CPLD.

1. Open the **Firmware Upgrade** page on the iBMC WebUI.
 - If the iBMC version is earlier than V561, choose **System > Firmware Upgrade** on the iBMC WebUI.
The page shown in [Figure 3-11](#) is displayed.

Figure 3-11 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI.
The page shown in [Figure 3-12](#) is displayed.

Figure 3-12 Firmware Upgrade page (iBMC V561 or later)**NOTE**

The page displayed for firmware upgrade varies with iBMC versions.

- In the **Firmware Upgrade** area, click .
- A window is displayed for you to select the upgrade file.
- Select the upgrade file.
- Click **Open**.
- After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
- Click **Upgrade**.
- A dialog box is displayed asking you whether to start the upgrade.
- Click **Yes** to start the upgrade.

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iBMC and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state in which the system is while the upgrade is performed.

- If the upgrade is performed while the server is powered off, perform the following steps:
 - For a V3 server, the iBMC is automatically reset after the CPLD upgrade is complete. After the iBMC is reset, the new CPLD takes effect. In addition, the iBMC automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually.
- For V5 and V6 servers, the iBMC automatically powers off and then powers on after the CPLD upgrade is complete. The new CPLD takes effect after the server is powered on.
- If the upgrade is performed while the server is powered on, perform the following steps:
After the CPLD upgrade is complete, power off the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power Off**. The new CPLD takes effect after the iBMC is automatically reset. In addition, the iBMC automatically powers on or off the server based on the setting of **System State Upon Power Supply**.
 - If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
 - If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually.
 - If the iBMC version is earlier than V561, choose **Power > Power Control**, and click **Power On**.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, and click **Power On**.

 NOTE

A forced power-off may cause data loss or program damage. Forcibly power off the server only when necessary.

Step 4 Check whether the firmware version is the target version.

- If the iBMC version is earlier than V561, choose **Information > System Info** on the iBMC WebUI.
Check the mainboard CPLD version information on the page displayed.
- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > System Info**.
Check the mainboard CPLD version information on the page displayed.

----End

3.5.1.3 Rolling Back the Firmware Version

3.5.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.

- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.5.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.5.1.2 Upgrade Procedure](#).

----End

3.5.2 Using the iMana 200 to Upgrade the Mainboard CPLD

3.5.2.1 Preparing for the Upgrade

3.5.2.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.5.2.1.2 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server on which you want to perform a firmware rollback. The server version list is displayed.
 - c. On the displayed page, click **Software Download**. The server software version list is displayed.

- d. Check the current firmware version.
 - If the iBMC version is earlier than V561, choose **Information > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.
 - e. Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to **f**.
 - If the target version is not in the version list, contact technical support.
 - f. Download the rollback package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.5.2.1.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.5.2.2 Upgrade Procedure

Scenarios

Upgrade the server mainboard CPLD using the iMana 200 WebUI.

The mainboard CPLD can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the mainboard CPLD when the server is powered off.

Prerequisites

Conditions

You have logged in to the iMana 200 WebUI.

Data

None

Software

You have downloaded and decompressed the mainboard CPLD upgrade package to the client (a PC) and obtained the upgrade file (for example, **cpldimage.hpm**).

Procedure

Step 1 Check the firmware version before the upgrade.

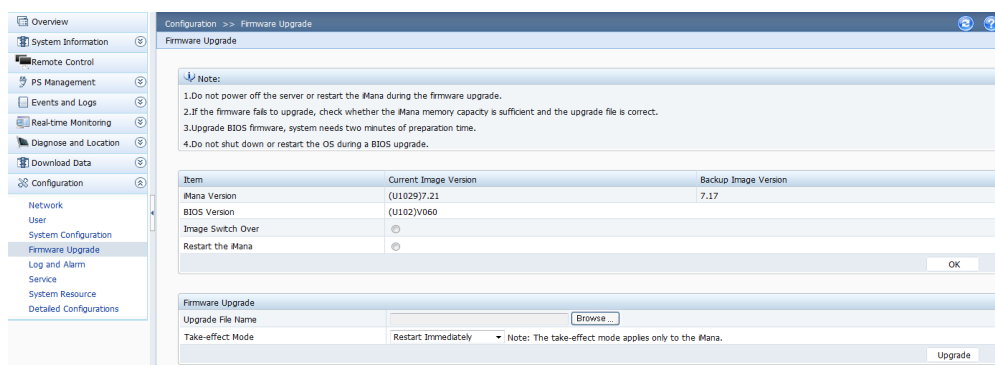
On the iBMC WebUI, choose **System Information > Firmware Version**.

Check the mainboard CPLD version on the page displayed.

Step 2 Upgrade the mainboard CPLD.

1. On the iMana 200 WebUI, choose **Configuration > Firmware Upgrade**.
The **Firmware Upgrade** page is displayed, as shown in [Figure 3-13](#).

Figure 3-13 Firmware Upgrade



2. Click **Browse**, and select the upgrade file.
3. Click **Upgrade**.
A confirmation dialog box is displayed.
4. Click **Yes**.

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iMana 200 and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state in which the system is while the upgrade is performed.

1. If the upgrade is performed while the server is powered off, perform the following steps:
After the CPLD upgrade is complete, the iMana 200 is automatically reset after the CPLD upgrade is complete. After the iMana 200 is reset, the new

CPLD takes effect. In addition, the iMana 200 automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iMana 200 automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.

2. If the upgrade is performed while the server is powered on, perform the following steps:

After the CPLD upgrade is complete, power off the server by choosing **Power > Power Control** in the navigation tree and clicking **Power Off** on the **Power Control** page. The CPLD of the new version takes effect after the iMana 200 is automatically reset. The iMana 200 automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.

 NOTE

A forced power-off may cause data loss or program damage. Forcibly power off the server only when necessary.

- Step 4** Check whether the firmware version is the target version.

On the iMana 200 WebUI, choose **System Information > Firmware Version**.

View the mainboard CPLD version information on the page displayed.

----End

3.5.2.3 Rolling Back the Firmware Version

3.5.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.5.2.3.2 Rollback Procedure

- Step 1** Determine the target version.

- Step 2** Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.5.2.2 Upgrade Procedure](#).

----End

3.5.3 Upgrading the Mainboard CPLD Using SmartKit

3.5.3.1 Preparing for the Upgrade

3.5.3.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-26](#).

Table 3-26 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of the chassis components	- Enterprise users: - Log in to Intelligent Servers. - Click the server whose firmware is to be upgraded. The server version list is displayed. - On the displayed page, click Software Download. The server software version list is displayed. - Select the target version. - Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package. - Carrier users: Contact technical support of your local Huawei office.

Type	How to Obtain
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.5.3.1.2 Obtaining the Rollback Package

Scenario

Version rollback is required when the version upgrade fails and the software version is not the source version. This section describes how to obtain the required rollback package before the upgrade.

Procedure

- Enterprise users:
 - Visit [Intelligent Servers](#).
 - Click the server on which you want to perform a firmware rollback.
The server version list is displayed.
 - On the displayed page, click **Software Download**.
The server software version list is displayed.
 - Check the current firmware version.
 - If the iBMC version is earlier than V561, choose **Information > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > System Info** on the iBMC WebUI.
Check the mainboard CPLD version on the page displayed.
 - Select the target version.
The version list displays all the supported software versions.
 - If the target version is in the version list, go to [f](#).
 - If the target version is not in the version list, contact technical support.

- f. Download the rollback package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.5.3.1.3 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.5.3.2 Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the *SmartKit Computing XXX User Guide* corresponding to the SmartKit plug-in version.

3.5.3.3 Rolling Back the Firmware Version

3.5.3.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.5.3.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see the *SmartKit Computing XXX User Guide* corresponding to the SmartKit plugin version.

----End

3.6 Upgrading the Hard Drive Backplane CPLD

X6000 V6 servers do not involve drive backplane CPLD upgrade.

3.6.1 Upgrading the Drive Backplane CPLD Using the iBMC WebUI

3.6.1.1 Preparing for the Upgrade

3.6.1.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.6.1.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.6.1.2 Upgrade Procedure

Scenarios

Upgrade the hard drive backplane CPLD using the iBMC WebUI.

The hard drive backplane CPLD can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the hard drive backplane CPLD when the server is powered off.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

You have downloaded and decompressed the CPLD upgrade package to the client (a PC) and obtained the upgrade file (for example, **cpldimage.hpm**).

Procedure

NOTICE

If the iBMC version is earlier than 2.56, restart the iBMC before upgrading the firmware. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System** > **Upgrade Firmware**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.4 Logging In Using the iBMC WebUI](#).
- Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).

Step 1 Check the current firmware version.

- If the iBMC version is earlier than V561, choose **Information** > **System Info** > **Other Devices** on the iBMC WebUI and view the current drive backplane CPLD version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System** > **System Info** > **Others** on the iBMC WebUI and view the current drive backplane CPLD version.

Step 2 Upgrade the hard drive backplane CPLD.

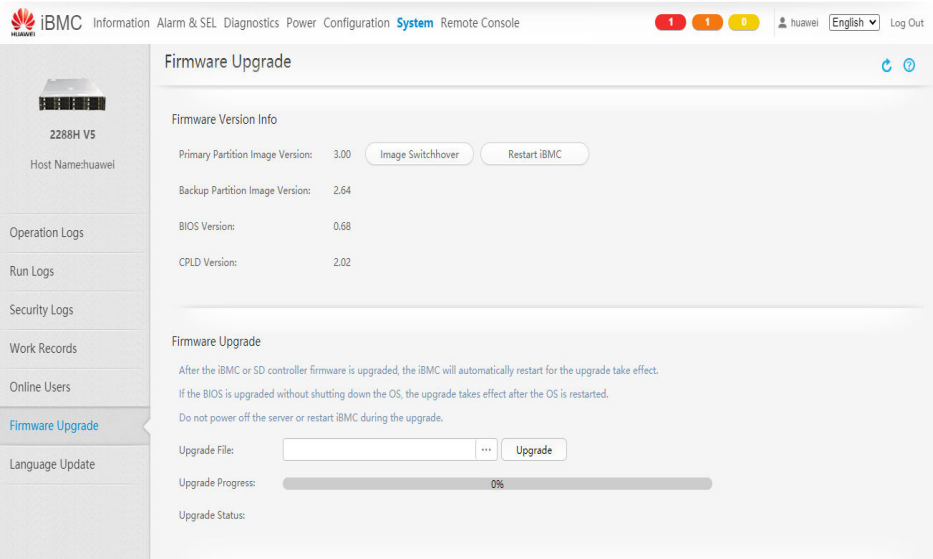
NOTE

For the X6000 server, you need to upgrade the hard drive backplane CPLD on server node 1.

1. Open the **Firmware Upgrade** page on the iBMC WebUI. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System** > **Firmware Upgrade** on the iBMC WebUI.

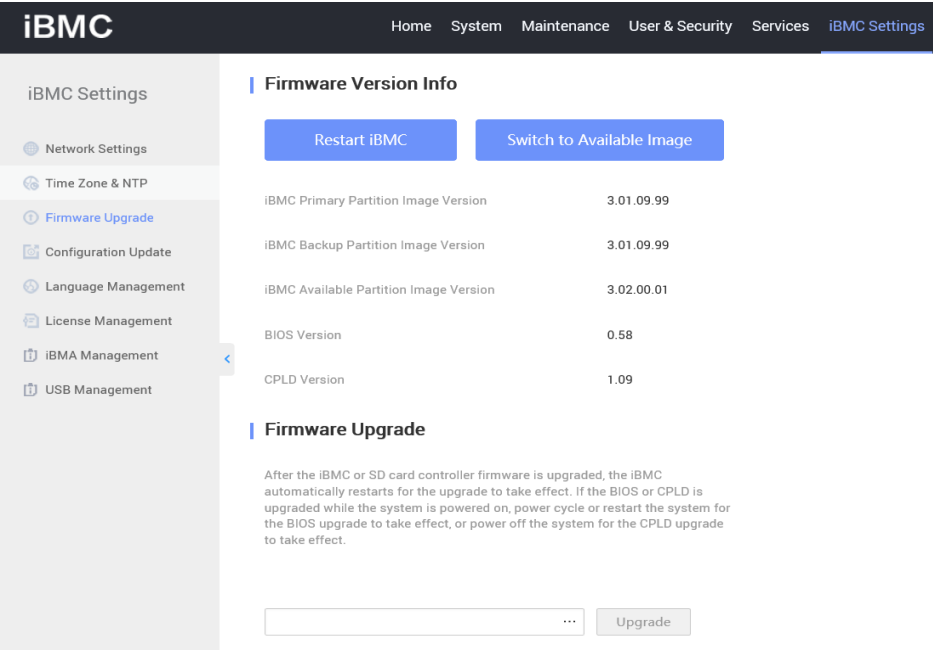
The page shown in [Figure 3-14](#) is displayed.

Figure 3-14 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The page shown in [Figure 3-15](#) is displayed.

Figure 3-15 Firmware Upgrade page (iBMC V561 or later)



NOTE

The page displayed for firmware upgrade varies with iBMC versions.

2. In the **Firmware Upgrade** area, click . A window is displayed for you to select the upgrade file.

3. Select the upgrade file.
4. Click **Open**.
After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
5. Click **Upgrade**.
A dialog box is displayed asking you whether to start the upgrade.
6. Click **Yes** to start the upgrade.

 NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iBMC and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state in which the system is while the upgrade is performed.

- If the upgrade is performed while the server is powered off, perform the following steps:
 - For a V3 server, the iBMC is automatically reset after the CPLD upgrade is complete. After the iBMC is reset, the new CPLD takes effect. In addition, the iBMC automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.
 - If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
 - If **System State Upon Power Supply** is set to **Power Off** or **Restore Previous State**, you need to power on the server by choosing **Power > Power Control** in the navigation tree and clicking **Power On** on the **Power Control** page.
 - For V5 and V6 servers, the iBMC automatically powers off and then powers on after the CPLD upgrade is complete. The new CPLD takes effect after the server is powered on.
- If the upgrade is performed while the server is powered on, you need to manually power off the server after the CPLD upgrade as follows:
 - If the iBMC version is earlier than V561, choose **Power > Power Control**, and click **Power Off**.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, and click **Power Off**.

The new CPLD takes effect after the iBMC is automatically reset. In addition, the iBMC automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually.
 - If the iBMC version is earlier than V561, choose **Power > Power Control**, and click **Power On**.

- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System** > **Power** > **Power Control**, and click **Power On**.

 NOTE

A forced power-off may cause data loss or program damage. Forcibly power off the server only when necessary.

Step 4 Check whether the firmware version is the target version.

- If the iBMC version is earlier than V561, choose **Information** > **System Info** > **Other Devices** on the iBMC WebUI and query the drive backplane CPLD version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System** > **System Info** > **Others** on the iBMC WebUI and query the drive backplane version.

----End

3.6.1.3 Rolling Back the Firmware Version

3.6.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.6.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.6.1.2 Upgrade Procedure](#).

----End

3.6.2 Using the iMana 200 to Upgrade the Hard Disk Backplane CPLD

3.6.2.1 Preparing for the Upgrade

3.6.2.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.6.2.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.6.2.2 Upgrade Procedure

Scenarios

Upgrade the hard drive backplane CPLD using the iMana 200 WebUI.

The hard drive backplane CPLD can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the hard drive backplane CPLD when the server is powered off.

Prerequisites

Conditions

You have logged in to the iMana 200 WebUI.

Data

None

Software

You have downloaded and decompressed the CPLD upgrade package to the client (a PC) and obtained the upgrade file (for example, **hddcpld.hpm**).

Procedure

Step 1 Check the current CPLD version.

On the iBMC WebUI, choose **System Information > Firmware Version**.

View the CPLD version information on the page displayed.

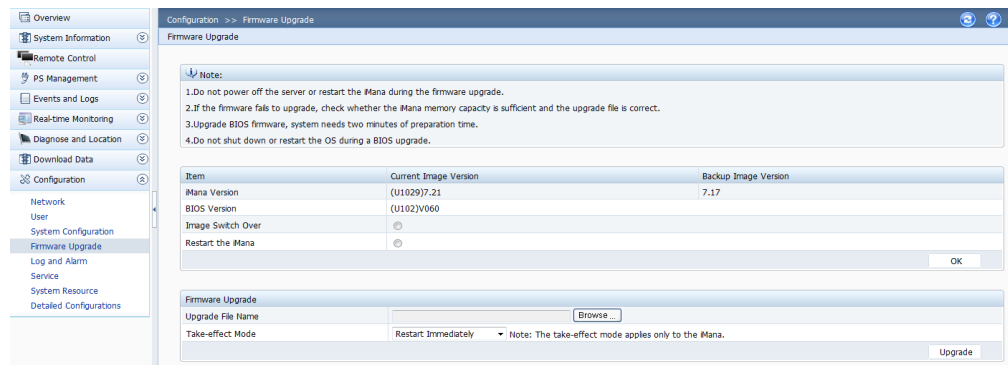
Step 2 Upgrade the hard drive backplane CPLD.

NOTE

For the X6000 server, you need to upgrade the hard drive backplane CPLD on server node 1.

1. On the iMana 200 WebUI, choose **Configuration > Firmware Upgrade**.
The **Firmware Upgrade** page is displayed, as shown in [Figure 3-16](#).

Figure 3-16 Firmware upgrade



2. Click **Browse**, and select the upgrade file.
3. Click **Upgrade**.
A confirmation dialog box is displayed.
4. Click **Yes** to start the upgrade.

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iMana 200 and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state in which the system is while the upgrade is performed.

1. If the upgrade is performed while the server is powered off, perform the following steps:

The CPLD of the new version takes effect after the iMana 200 is automatically reset. The iMana 200 automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iMana 200 automatically powers on the server.

- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.
- 2. If the upgrade is performed while the server is powered on, perform the following steps:
After the CPLD upgrade is complete, power off the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power Off**. The CPLD of the new version takes effect after the iMana 200 is automatically reset. The iMana 200 automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.
 - If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
 - If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.

 NOTE

A forced power-off may cause data loss or program damage. Forcibly power off the server only when necessary.

Step 4 Check whether the CPLD version is the target version.

On the iMana 200 WebUI, choose **System Information > Firmware Version**.

View the CPLD version information on the page displayed.

----End

3.6.2.3 Rolling Back the Firmware Version

3.6.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.6.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.6.2.2 Upgrade Procedure](#).

----End

3.6.3 Upgrading the Drive Backplane CPLD Using SmartKit

3.6.3.1 Preparing for the Upgrade

3.6.3.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-27](#).

Table 3-27 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of the chassis components	- Enterprise users: - Log in to Intelligent Servers. - Click the server whose firmware is to be upgraded. The server version list is displayed. - On the displayed page, click Software Download. The server software version list is displayed. - Select the target version. - Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package. - Carrier users: Contact technical support of your local Huawei office.

Type	How to Obtain
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.6.3.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.6.3.2 Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plug-in version.

3.6.3.3 Rolling Back the Firmware Version

3.6.3.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.

- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.6.3.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plugin version.

----End

3.7 Upgrading the Fan Management Board CPLD

3.7.1 Upgrading the CPLD of the Fan Module Using the iBMC WebUI

3.7.1.1 Preparing for the Upgrade

3.7.1.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.7.1.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.7.1.2 Upgrade Procedure

NOTICE

You can upgrade the CPLD of the fan management module only on the iBMC WebUI of the node in slot 1.

Scenarios

Use iBMC WebUI to upgrade the CPLD of the fan management board on an X6000 V6 server.

The fan management board CPLD can be upgraded while the OS is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the fan management board CPLD while the OS is powered off.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

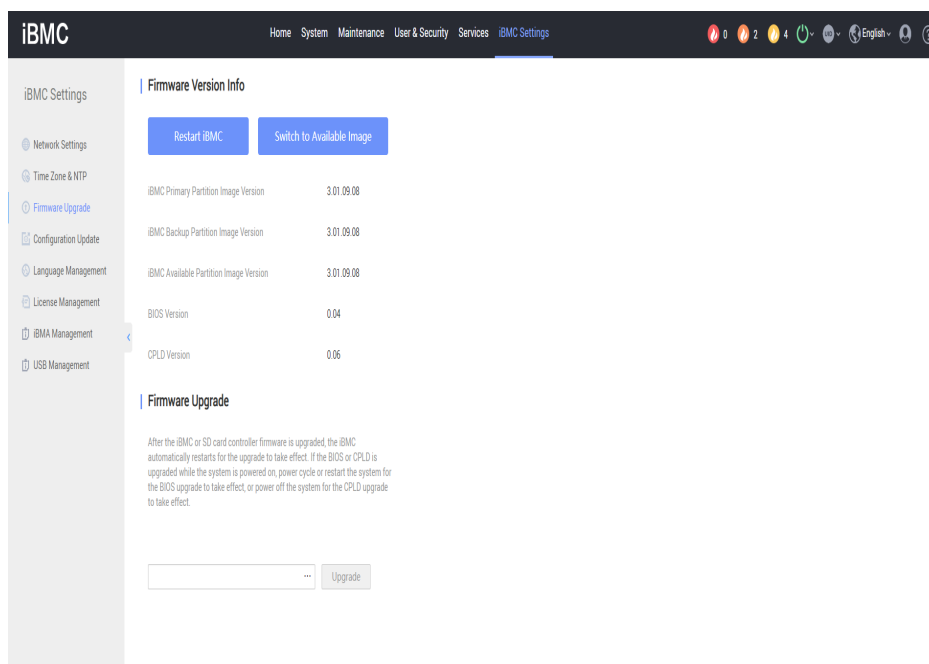
None

Software

You have downloaded the fan management board CPLD upgrade package to the client (such as a PC), decompressed the package, and obtained the upgrade file.

Procedure

- Step 1** Run the **ipmcget -d v** command on the remote console to check the CPLD version of the fan management board before the upgrade.
- Step 2** Upgrade the fan management board CPLD.
 1. On the iBMC WebUI, choose **iBMC Settings > Firmware Upgrade**.
The **Firmware Upgrade** page is displayed, as shown in [Figure 3-17](#).

Figure 3-17 Firmware upgrade page**NOTE**

The page displayed for firmware upgrade varies with iBMC versions.

- In the **Firmware Upgrade** area, click .
- A window is displayed for you to select the upgrade file.
- Select the upgrade file.
- Click **Open**.
- After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
- Click **Upgrade**.
- A dialog box is displayed asking you whether to start the upgrade.
- Click **Yes** to start the upgrade.

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iBMC using the NCSI management network port and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state of the node when the upgrade was performed.

- If the chassis contains powered-on nodes during the upgrade of the fan management board CPLD, you need to manually power off the nodes after the upgrade. When all nodes in the chassis are powered off, the node in slot 1 automatically resets the iBMC. Then the new CPLD of the fan management board takes effect after the reset.

- If all nodes in the chassis are powered off during the upgrade of the fan management board CPLD, the iBMC automatically resets after the upgrade. The new CPLD takes effect after the reset.

Step 4 Run the **ipmcget -d v** command on the remote console to check whether the firmware version of the CPLD of the fan management board is the target version.

----End

3.7.1.3 Rollback

3.7.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.7.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.6.1.2 Upgrade Procedure](#).

----End

3.8 Upgrading the Riser Card CPLD

X6000 V6 servers do not involve the riser card CPLD upgrade.

3.8.1 Upgrading the Riser Card CPLD Using the iBMC WebUI

3.8.1.1 Preparing for the Upgrade

3.8.1.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.

- c. On the displayed page, click **Software Download**.
The server software version list is displayed.
- d. Select the target version.
- e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.8.1.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.8.1.2 Upgrade Procedure

Scenarios

Upgrade the riser card CPLD using the iBMC WebUI.

The riser card CPLD can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the riser card CPLD when the server is powered off.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

You have downloaded and decompressed the riser card CPLD upgrade package to the client (a PC) and obtained the upgrade file (for example, **cpldimage_for_ibmc.hpm**).

Procedure

NOTICE

If the iBMC version is earlier than 2.56, restart the iBMC before upgrading the firmware. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System > Upgrade Firmware**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.4 Logging In Using the iBMC WebUI](#).
- Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).

Step 1 Check the current firmware version.

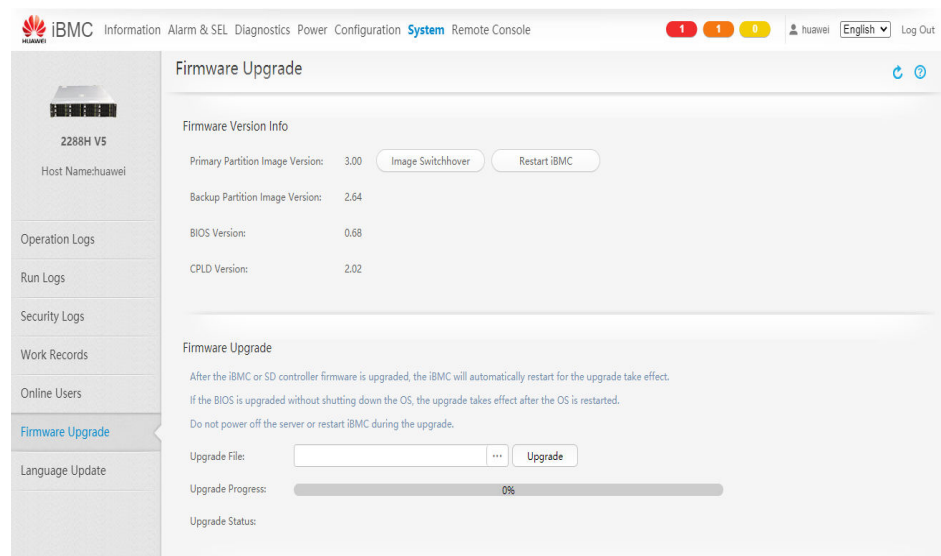
- If the iBMC version is earlier than V561, choose **Information > System Info > Other Devices** on the iBMC WebUI and query the riser card CPLD version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System > System Info > Others** on the iBMC WebUI and query the riser card CPLD version.

Step 2 Upgrade the riser card CPLD.

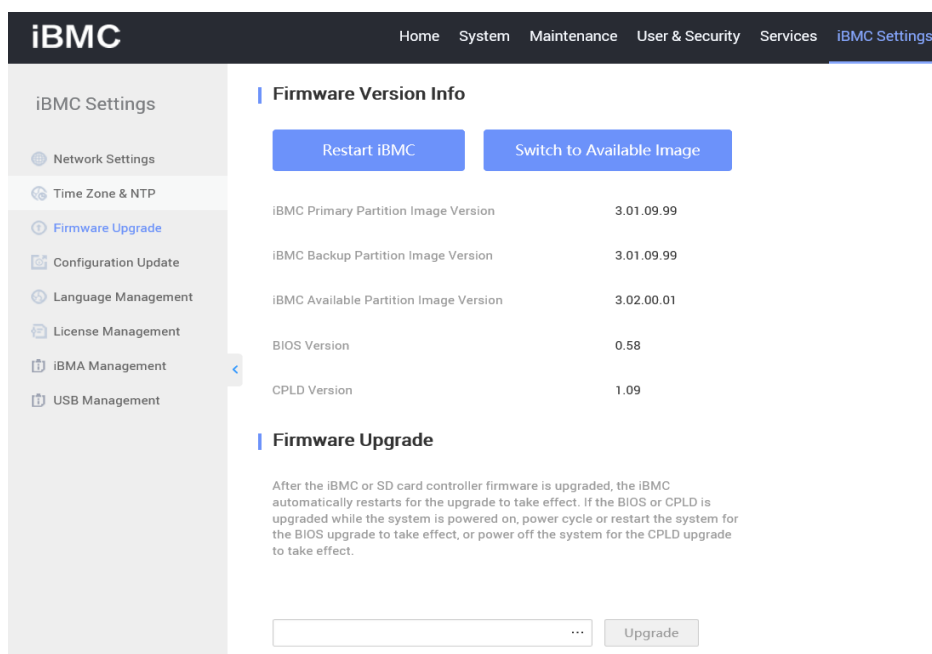
- Open the **Firmware Upgrade** page on the iBMC WebUI. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System > Firmware Upgrade** on the iBMC WebUI.

The page shown in [Figure 3-18](#) is displayed.

Figure 3-18 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The page shown in [Figure 3-19](#) is displayed.

Figure 3-19 Firmware Upgrade page (iBMC V561 or later)**NOTE**

The page displayed for firmware upgrade varies with iBMC versions.

- In the **Firmware Upgrade** area, click .
- A window is displayed for you to select the upgrade file.
- Select the upgrade file.
- Click **Open**.
- After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
- Click **Upgrade**.
- A dialog box is displayed asking you whether to start the upgrade.
- Click **Yes** to start the upgrade.

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iBMC and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state in which the system is while the upgrade is performed.

- If the upgrade is performed while the server is powered off, perform the following steps:
 - For a V3 server, the iBMC is automatically reset after the CPLD upgrade is complete. After the iBMC is reset, the new CPLD takes effect. In addition, the iBMC automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.
- For a V5 server, the iBMC automatically powers off and then powers on after the CPLD upgrade is complete. The new CPLD takes effect after the server is powered on.
- If the upgrade is performed while the server is powered on, perform the following steps:
 - After the CPLD is upgraded on a V3/V5 server, you need to manually power off the server. The detailed operations are as follows:
 - If the iBMC version is earlier than V561, choose **Power > Power Control**, and click **Power Off**.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, and click **Power Off**.

The new CPLD takes effect after the iBMC is automatically reset. In addition, the iBMC automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually.
 - If the iBMC version is earlier than V561, choose **Power > Power Control**, and click **Power On**.
 - If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **System > Power > Power Control**, and click **Power On**.

NOTE

A forced power-off may cause data loss or program damage. Forcibly power off the server only when necessary.

Step 4 Check whether the firmware version is the target version.

- If the iBMC version is earlier than V561, choose **Information > System Info > Other Devices** on the iBMC WebUI and query the riser card CPLD version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System > System Info > Others** on the iBMC WebUI and query the riser card version.

----End

3.8.1.3 Rolling Back the Firmware Version

3.8.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.8.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.8.1.2 Upgrade Procedure](#).

----End

3.8.2 Using the iMana 200 to Upgrade the Riser Card CPLD

3.8.2.1 Preparing for the Upgrade

3.8.2.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Log in to [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.8.2.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.8.2.2 Upgrade Procedure

Scenarios

Upgrade the riser card CPLD using the iMana 200 WebUI.

The riser card CPLD can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the riser card CPLD when the server is powered off.

Prerequisites

Conditions

You have logged in to the iMana 200 WebUI.

Data

None

Software

You have downloaded and decompressed the riser card CPLD upgrade package to the client (a PC) and obtained the upgrade file (for example, **cpldimage_for_ibmc.hpm**).

Procedure

Step 1 Check the firmware version before the upgrade.

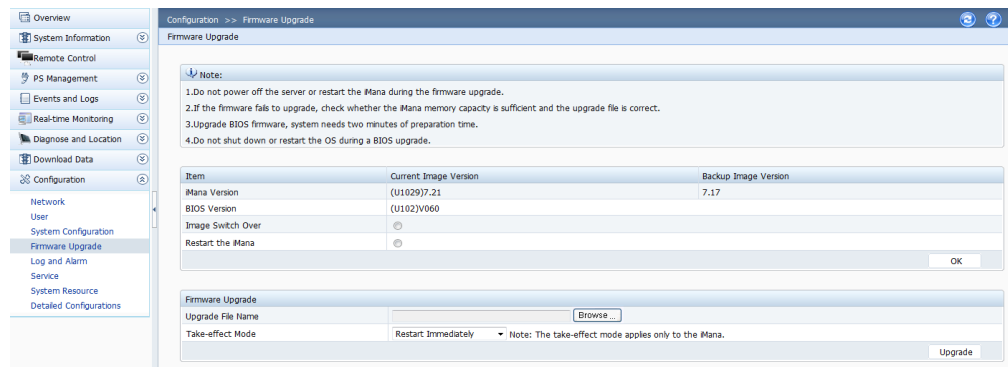
On the iBMC WebUI, choose **System Information > Firmware Version**.

You can obtain the riser card CPLD version information on the page displayed.

Step 2 Upgrade the riser card CPLD.

1. On the iMana 200 WebUI, choose **Configuration > Firmware Upgrade**.

The **Firmware Upgrade** page is displayed, as shown in [Figure 3-20](#).

Figure 3-20 Firmware Upgrade

2. Click **Browse**, and select the upgrade file.
3. Click **Upgrade**.
A confirmation dialog box is displayed.
4. Click **Yes**.

NOTE

During the CPLD upgrade, do not power off the server. If the server is abnormal due to an unexpected power-off during the upgrade, log in to the iMana 200 and upgrade the CPLD again.

The upgrade process takes about 3 minutes. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Make the upgrade take effect. The operations vary depending on the state in which the system is while the upgrade is performed.

1. If the upgrade is performed while the server is powered off, perform the following steps:

After the CPLD upgrade is complete, the iMana 200 is automatically reset after the CPLD upgrade is complete. After the iMana 200 is reset, the new CPLD takes effect. In addition, the iMana 200 automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iMana 200 automatically powers on the server.
- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.

2. If the upgrade is performed while the server is powered on, perform the following steps:

After the CPLD upgrade is complete, power off the server by choosing **Power > Power Control** in the navigation tree and clicking **Power Off** on the **Power Control** page. The CPLD of the new version takes effect after the iMana 200 is automatically reset. The iMana 200 automatically powers on or powers off the server based on the setting of **System State Upon Power Supply**.

- If **System State Upon Power Supply** is set to **Power On**, the iBMC automatically powers on the server.

- If **System State Upon Power Supply** is set to **Remain Off** or **Restore Previous State**, you need to power on the server manually. On the iBMC WebUI, choose **Power > Power Control**, and click **Power On**.

 NOTE

A forced power-off may cause data loss or program damage. Forcibly power off the server only when necessary.

Step 4 Check whether the firmware version is the target version.

On the iMana 200 WebUI, choose **System Information > Firmware Version**.

View the CPLD version information on the page displayed.

----End

3.8.2.3 Rolling Back the Firmware Version

3.8.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.8.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the CPLD version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.8.2.2 Upgrade Procedure](#).

----End

3.8.3 Upgrading the Riser Card CPLD Using SmartKit

3.8.3.1 Preparing for the Upgrade

3.8.3.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-28](#).

Table 3-28 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of the chassis components	- Enterprise users: - Log in to Intelligent Servers. - Click the server whose firmware is to be upgraded. The server version list is displayed. - On the displayed page, click Software Download. The server software version list is displayed. - Select the target version. - Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package. - Carrier users: Contact technical support of your local Huawei office.
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.8.3.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.8.3.2 Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the *SmartKit Computing XXX User Guide* corresponding to the SmartKit plug-in version.

3.8.3.3 Rolling Back the Firmware Version

3.8.3.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.8.3.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is the same as the upgrade procedure. For details, see the *SmartKit Computing User Guide* corresponding to the SmartKit plug-in version.

----End

3.9 Upgrading the LCD Firmware

X6000 V6 servers do not involve the LCD Firmware upgrade.

3.9.1 Upgrading the LCD Firmware Using the iBMC WebUI

3.9.1.1 Preparing for the Upgrade

3.9.1.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.9.1.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.9.1.2 Upgrade Procedure

Scenarios

Upgrade the firmware of the liquid crystal display (LCD) using the iBMC WebUI.

The LCD firmware can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the LCD firmware when the server is powered off.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

You have downloaded and decompressed the firmware upgrade package, to the client (a PC) and obtained the upgrade file (for example, **lcdimage.hpm**).

Procedure

NOTICE

If the iBMC version is earlier than 2.56, restart the iBMC before upgrading the firmware. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System > Upgrade Firmware**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.4 Logging In Using the iBMC WebUI](#).
- Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).

Step 1 Check the current firmware version.

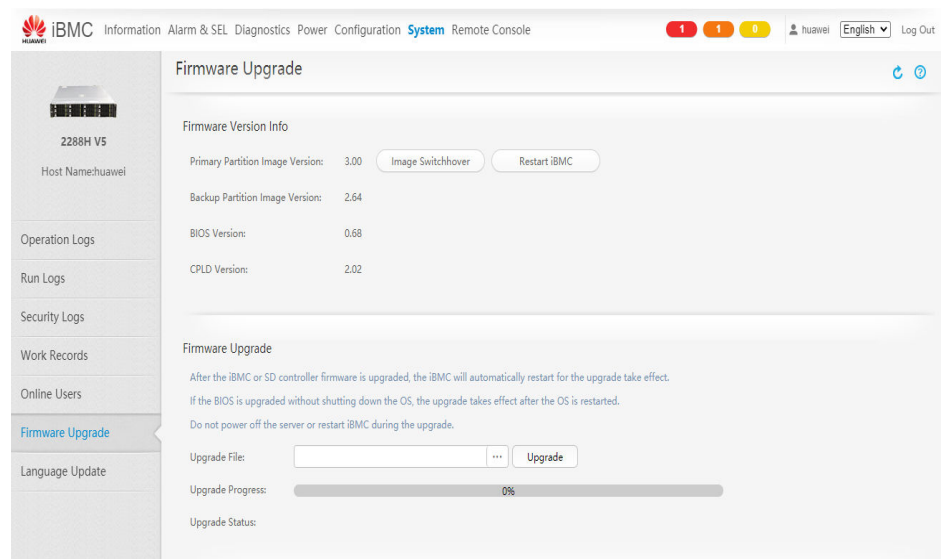
- If the iBMC version is earlier than V561, choose **Information > System Info > Other Devices** on the iBMC WebUI and query the LCD firmware version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System > System Info > Others** on the iBMC WebUI and query the LCD firmware version.

Step 2 Upgrade the LCD firmware.

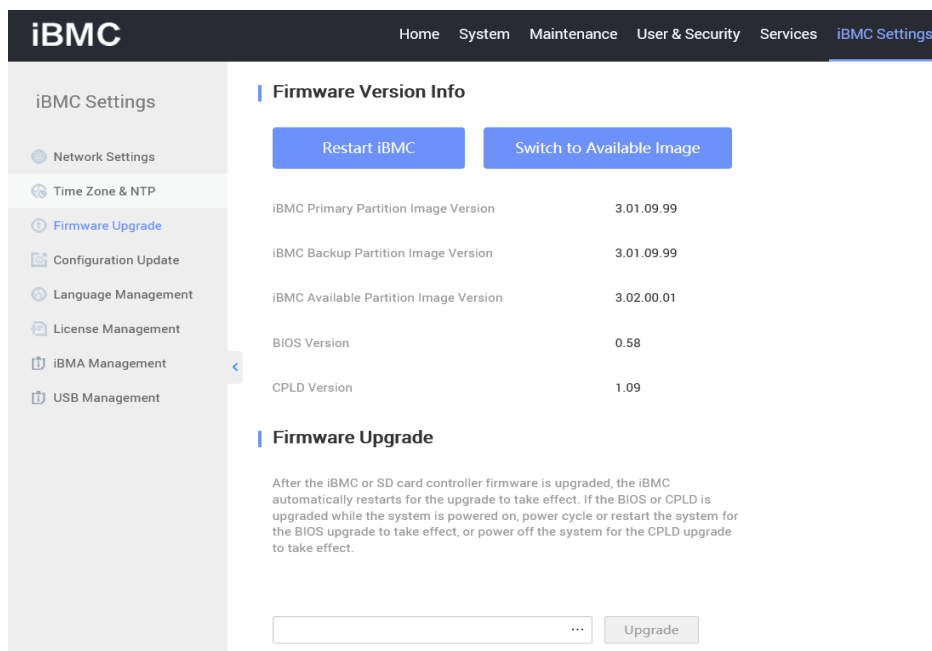
- Open the **Firmware Upgrade** page on the iBMC WebUI. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System > Firmware Upgrade** on the iBMC WebUI.

The page shown in [Figure 3-21](#) is displayed.

Figure 3-21 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The page shown in [Figure 3-22](#) is displayed.

Figure 3-22 Firmware Upgrade page (iBMC V561 or later)**NOTE**

The page displayed for firmware upgrade varies with iBMC versions.

2. In the **Firmware Upgrade** area, click .
A window is displayed for you to select the upgrade file.
3. Select the upgrade file.
4. Click **Open**.
After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
5. Click **Upgrade**.
A dialog box is displayed asking you whether to start the upgrade.
6. Click **Yes** to start the upgrade.
The upgrade process takes about 1 minute. If "The upgrade is complete" is displayed, the upgrade is successful.

Step 3 Check whether the firmware version is the target version.

- If the iBMC version is earlier than V561, choose **Information > System Info > Other Devices** on the iBMC WebUI and query the LCD firmware version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System > System Info > Others** on the iBMC WebUI and query the LCD firmware version.

----End

3.9.1.3 Rolling Back the Firmware Version

3.9.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.9.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.9.1.2 Upgrade Procedure](#).

-----End

3.9.2 Using the iMana 200 to Upgrade the LCD Firmware

3.9.2.1 Preparing for the Upgrade

3.9.2.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.9.2.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.9.2.2 Upgrade Procedure

Scenarios

Upgrade the firmware of the LCD using the iMana 200 WebUI.

The LCD firmware can be upgraded when the server is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the LCD firmware when the server is powered off.

Prerequisites

Conditions

You have logged in to the iMana 200 WebUI.

Data

None

Software

You have downloaded and decompressed the LCD firmware upgrade package to the client (a PC) and obtained the upgrade file (for example, **lcdimage.hpm**).

Procedure

Step 1 Check the firmware version before the upgrade.

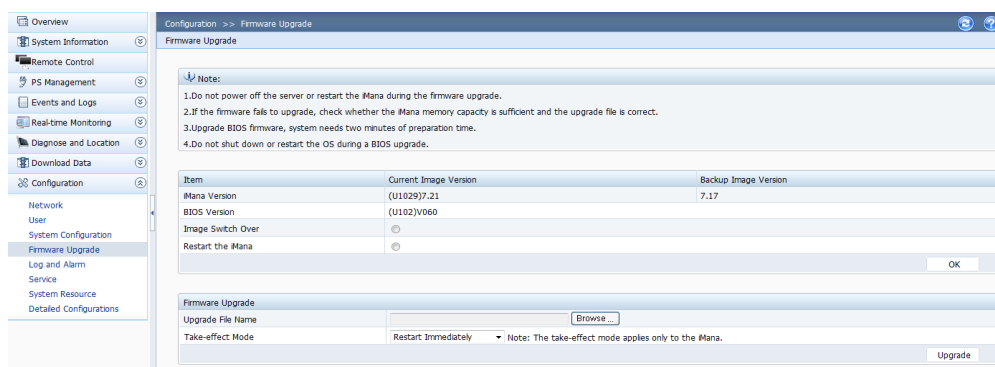
On the iBMC WebUI, choose **System Information** > **Firmware Version**.

View the firmware version information on the page displayed.

Step 2 Upgrade the LCD firmware.

1. On the iMana 200 WebUI, choose **Configuration** > **Firmware Upgrade**.

The **Firmware Upgrade** page is displayed, as shown in [Figure 3-23](#).

Figure 3-23 Firmware Upgrade

2. Click **Browse**, and select the upgrade file.
3. Click **Upgrade**.

A confirmation dialog box is displayed.

4. Click **Yes**.

If "The upgrade is complete" is displayed, the upgrade is successful. The upgrade process takes about 1 minute.

Step 3 Check whether the firmware version is the target version.

On the iMana 200 WebUI, choose **System Information > Firmware Version**.

View the firmware version information on the page displayed.

----End

3.9.2.3 Rolling Back the Firmware Version

3.9.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.9.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.9.2.2 Upgrade Procedure](#).

----End

3.9.3 Using SmartKit to Upgrade the LCD Firmware

3.9.3.1 Preparing for the Upgrade

3.9.3.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-29](#).

Table 3-29 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of the chassis components	- Enterprise users: - Log in to Intelligent Servers. - Click the server whose firmware is to be upgraded. The server version list is displayed. - On the displayed page, click Software Download. The server software version list is displayed. - Select the target version. - Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package. - Carrier users: Contact technical support of your local Huawei office.

Type	How to Obtain
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.9.3.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from the Support website, verify its PGP digital signature. See *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use it, and contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.9.3.2 Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the *SmartKit Computing XXX User Guide* corresponding to the SmartKit plug-in version.

3.9.3.3 Rolling Back the Firmware Version

3.9.3.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.

- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.9.3.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is the same as the upgrade procedure. For details, see the [SmartKit Computing User Guide](#) corresponding to the SmartKit plug-in version.

----End

3.10 Upgrading the Drive Backplane Expander Firmware

Upgrade the drive backplane Expander firmware

X6000 V6 servers do not involve drive backplane firmware upgrade.

3.10.1 Upgrading the Drive Backplane Expander Firmware Using the CLI (Linux)

3.10.1.1 Before You Start

Precautions

Observe the precautions listed in [Table 3-30](#) during the upgrade.

Table 3-30 Precautions for the upgrade

No.	Description
1	Before performing the upgrade without the install.sh script, determine the SG device number of the board to be upgraded. Otherwise, irreversible hardware faults may occur.
2	Before the upgrade, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to the document, contact Huawei technical support.
3	Perform the upgrade during off-peak hours to minimize the impact on the system and services.

Version Requirements

None

3.10.1.2 Preparing for the Upgrade

3.10.1.2.1 Obtaining Software Packages

Obtain the required software packages before the upgrade.

- Enterprise users:
 - a. Log in to [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.10.1.2.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.10.1.3 Performing the Upgrade

Scenarios

Upgrade the Expander firmware of the drive backplane using the CLI.

Precautions

Before the upgrade, check the RAID controller card model and firmware version. If the RAID controller card model is 9440-8i, 9460-8i, or 9460-16i and the RAID controller card firmware version is earlier than 5.130.00-3059, upgrade the RAID controller card firmware before upgrading the drive backplane Expander firmware. Otherwise, either of the following consequences may occur:

- Consequence 1: The firmware upgrade failed. The backplane is not reset and the upgraded firmware does not take effect, but the backplane can be identified.

In this case, perform the following steps to perform the upgrade again:

- a. Use the Expander firmware package of the original version to perform a rollback. Use the `sg_write` method during rollback.
 - i. Roll back the boot file.

`sg_write_buffer -b 4k -l boot_mips.bin -m 7 /dev/SG device number corresponding to the Expander`

 NOTE

You can run the `ls SCSI -g | grep -i expander` command to query the SG device number.

- ii. Roll back the firmware configuration file.

`sg_write_buffer -b 4k -l istr_flash_pmxxx.bin -m 7 /dev/SG device number corresponding to the Expander`

 NOTE

pmxxx indicates the model of the Expander main chip on the drive backplane. Set this parameter to the actual model.

- iii. Roll back the firmware upgrade file.

`sg_write_buffer -b 4k -l sxp_evbd_rom.bin -m 7 /dev/SG device number corresponding to the Expander`

- b. Upgrade the RAID controller card firmware. For details, see [1 Upgrading the RAID Controller Card Firmware](#).
 - c. Upgrade the expander firmware of the drive backplane again according to the procedure described in this section.
- Consequence 2: The firmware upgrade failed. The backplane is reset and the upgraded firmware takes effect, but the backplane cannot be identified.

In this case, you can only replace the drive backplane. For details, see the *Maintenance and Service Guide* or *User Guide* of the corresponding server model.

Prerequisites

- You have backed up the data and programs on the server.
- You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Procedure

Upgrade the Expander firmware of the front 12-drive, 24-drive, or 25-drive backplane on a server.

Before the upgrade, download the controller card firmware upgrade package to the client (such as a PC) and decompress it.

Step 1 Check the source firmware version.

Run the **./expanderTool query /dev/sg device number of the Expander** command to query the firmware version.

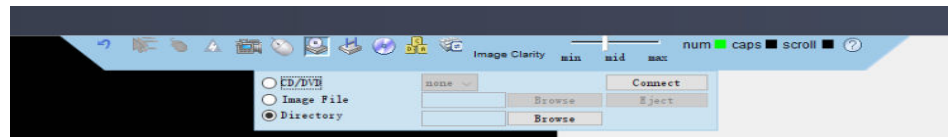
Step 2 Upload the upgrade package.

1. Open the Remote Virtual Console.

2. Click  on the toolbar.

The screen shown in [Figure 3-24](#) is displayed.

Figure 3-24 Virtual CD/DVD drive



3. Select **Directory** and click **Browse**.

The **Open** dialog box is displayed.

4. Select the drive backplane upgrade package from the PC, and click **Connect**.

5. Upload the upgrade package to the OS, and run the **chmod +x *** command to add the read and write permissions to all the files.

Step 3 Run the **ls SCSI -g** command to query the sg device number corresponding to the drive backplane.

In the command output, "expander" indicates the drive backplane. In the following example, **"/dev/sg4"** indicates the sg device number.

```
[root@localhost ~]# ls SCSI -g
[3:0:0:0] disk ATA INTEL SSDSC2BA20 0270 /dev/sda /dev/sg0
[15:0:0:0] enclosu HuaWei Expander 135 - /dev/sg4
```

 NOTE

If the sg device number cannot be obtained, load the **modprobe sg.ko** driver.

Step 4 Upgrade the firmware.

 NOTE

Repeat [Step 4.1](#) to [Step 4.4](#) for each drive backplane queried in [Step 3](#). The *sg device number of the expander* is the SG device number of the drive backplane. The following uses the drive backplane with the SG device No. 4 as an example.

1. Run **./expanderTool query /dev/sg device number of the Expander** to query the firmware version.

```
linux: ~/expander #
linux: ~/expander #./expanderTool query /dev/sg4
Active Image: image1
Image Version: 912
Active Data: data0
Data Version: 118
```

2. Run **./expanderTool download=boot_mips.bin /dev/sg device number of the Expander** to update the boot file.

If the firmware package does not contain the **boot_mips.bin** file, skip this step.

```
linux: ~/expander #
linux: ~/expander #./expanderTool download=boot_mips.bin /dev/sg4
Please Wait for downloading...
Firmware update success!
```

WARNING

Do not power off or reset the server during the upgrade.

3. Run **./expanderTool download=istr_flash_pm8053.bin /dev/sg device number of the Expander** to update the firmware configuration file.
pm8053 is the main chip model of the drive backplane Expander. Replace it with the actual model.

```
linux: ~/expander #
linux: ~/expander #./expanderTool download=istr_flash_pm8053.bin /dev/sg4
Please Wait for downloading...
Firmware update success!
linux: ~/expander #
```

WARNING

Do not power off or reset the server during the upgrade.

4. Run **./expanderTool download=sxp_evbd_rom.bin /dev/sg device number of the Expander** to update the firmware file.

```
linux: ~/expander #
linux: ~/expander #./expanderTool download=sxp_evbd_rom.bin /dev/sg4
Please Wait for downloading...
Swap active rom...
Firmware update success!
linux: ~/expander #
```

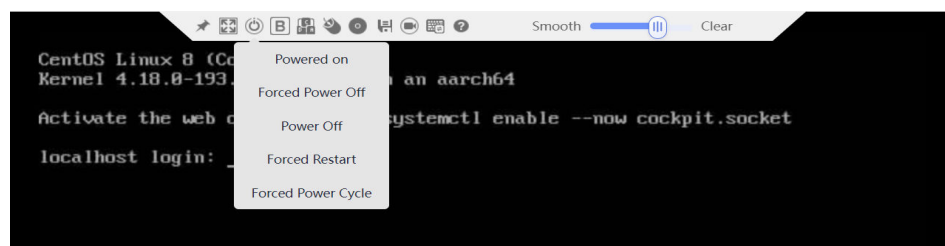
WARNING

Do not power off or reset the server during the upgrade.

Step 5 Power off and then power on the server for the firmware to take effect.

1. Open the Remote Virtual Console.
2. Click  or  on the toolbar. The power control menu is displayed, as shown in [Figure 3-25](#).

Figure 3-25 Power control menu



3. Click **Power Off**.
4. After the server is powered off, click **Powered On**.

 NOTE

It takes about 5 to 10 minutes to start the server. The time varies according to the actual configuration.

Step 6 Check whether the firmware version is the target version.

Run `./expanderTool query /dev/sg device number of the Expander` to query the firmware version.

----End

3.10.1.4 Rolling Back a Version

3.10.1.4.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. Determine whether to perform a rollback in any of the following cases:

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in business hours caused by the upgrade, a rollback is required.

3.10.1.4.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.10.1.3 Performing the Upgrade](#).

----End

3.11 Upgrading the SD Card Controller Firmware

X6000 V6 servers do not involve the SD card controller firmware upgrade.

3.11.1 Upgrading the SD Card Controller Firmware Using the iBMC WebUI

3.11.1.1 Preparing for the Upgrade

3.11.1.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.
 - d. Select the target version.
 - e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.11.1.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.11.1.2 Upgrade Procedure

Scenarios

Upgrade the SD card controller firmware using the iBMC WebUI.

The SD card controller firmware can be upgraded when the operating system (OS) is powered on or off, and the upgrade procedures are similar. This section describes how to upgrade the SD card controller firmware when the server is powered off.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

None

Software

You have downloaded and decompressed the firmware upgrade package to the client (a PC) and obtained the upgrade file (for example, **TwinSD.hpm**).

Procedure

NOTICE

If the iBMC version is earlier than 2.56, restart the iBMC before upgrading the firmware. To restart the iBMC, do as follows:

- Log in to the iBMC WebUI, choose **System > Upgrade Firmware**, and click **Restart iBMC** in the **Firmware Version Info** area. For details about how to log in to the iBMC WebUI, see [5.4 Logging In Using the iBMC WebUI](#).
- Log in to the iBMC CLI, and run the **ipmcset -d reset** command to restart the iBMC. For details about how to log in to the iBMC CLI, see [5.5 Logging In to the iBMC CLI](#).

Step 1 Check the current firmware version.

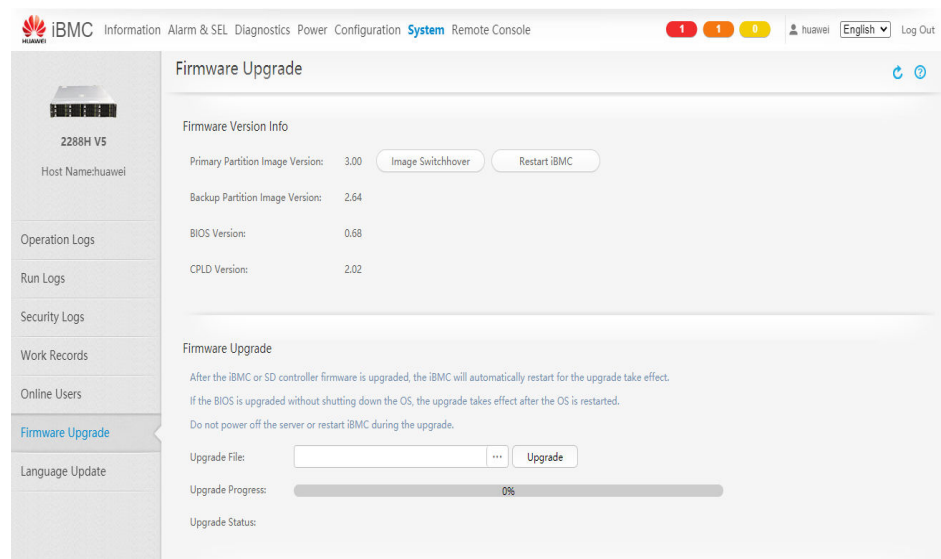
- If the iBMC version is earlier than V561, choose **Information > System Info > Other Devices** on the iBMC WebUI and query the SD card controller firmware version.
- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System > System Info > Others** on the iBMC WebUI and query the SD card controller firmware version.

Step 2 Upgrade the SD card controller firmware.

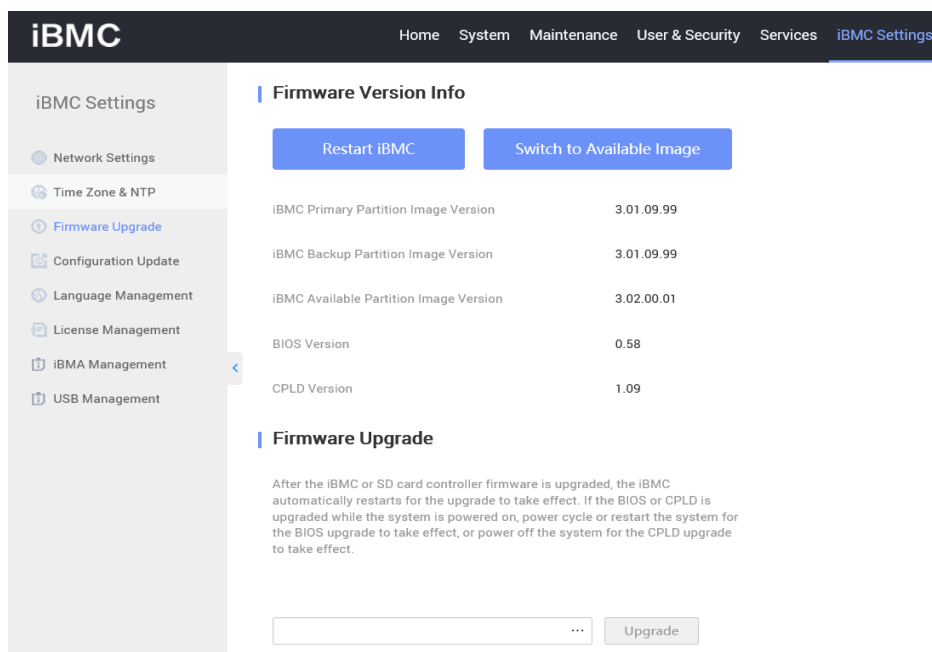
- Open the **Firmware Upgrade** page on the iBMC WebUI. The iBMC WebUI varies depending on the iBMC version.
 - If the iBMC version is earlier than V561, choose **System > Firmware Upgrade** on the iBMC WebUI.

The page shown in [Figure 3-26](#) is displayed.

Figure 3-26 Firmware Upgrade page (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in x.xx.xx.xx format, choose **iBMC Settings > Firmware Upgrade** on the iBMC WebUI. The page shown in [Figure 3-27](#) is displayed.

Figure 3-27 Firmware Upgrade page (iBMC V561 or later)**NOTE**

The page displayed for firmware upgrade varies with iBMC versions.

2. In the **Firmware Upgrade** area, click .
A window is displayed for you to select the upgrade file.
3. Select the upgrade file.
4. Click **Open**.
After the upgrade file is selected, the **Firmware Upgrade** page is displayed.
5. Click **Upgrade**.
A dialog box is displayed asking you whether to start the upgrade.
6. Click **Yes** to start the upgrade.
The upgrade process takes about 1 minute. If "The upgrade is complete" is displayed, the upgrade is successful.

NOTE

The iBMC restarts immediately after the upgrade is complete.

Step 3 Check whether the firmware version is the target version.

- If the iBMC version is earlier than V561, choose **Information > System Info > Other Devices** on the iBMC WebUI and query the SD card controller firmware version.

- If the iBMC version is V561 or later or the iBMC version is in the x.xx.xx.xx format, choose **System** > **System Info** > **Others** on the iBMC WebUI and query the SD card controller firmware version.

----End

3.11.1.3 Rolling Back the Firmware Version

3.11.1.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.11.1.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.11.1.2 Upgrade Procedure](#).

----End

3.11.2 Upgrading the SD Card Controller Firmware Using SmartKit

3.11.2.1 Preparing for the Upgrade

3.11.2.1.1 Obtaining Software Packages

Scenarios

Obtain the required software packages before the upgrade.

Procedure

Obtain the required software packages using the methods described in [Table 3-31](#).

Table 3-31 Obtaining the software packages

Type	How to Obtain
Firmware upgrade package of the chassis components	- Enterprise users: - Log in to Intelligent Servers. - Click the server whose firmware is to be upgraded. The server version list is displayed. - On the displayed page, click Software Download. The server software version list is displayed. - Select the target version. - Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package. - Carrier users: Contact technical support of your local Huawei office.
SmartKit tool package	- Enterprise users: - Log in to the SmartKit Computing website. - Select All next to Select Version. - Click the latest SmartKit Computing version. The software list is displayed. - Select the SmartKit tool package from the software list. - Download the SmartKit tool package and digital signature file. - Carrier users: Contact technical support of your local Huawei office.

3.11.2.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.11.2.2 Upgrade Procedure

For details, see "Using SmartKit" > "Firmware Upgrade" > "Upgrading Server Firmware" in the *SmartKit Computing XXX User Guide* corresponding to the SmartKit plug-in version.

3.11.2.3 Rolling Back the Firmware Version

3.11.2.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.11.2.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the firmware version.

The rollback procedure is the same as the upgrade procedure. For details, see the *SmartKit Computing User Guide* corresponding to the SmartKit plug-in version.

----End

3.12 Upgrading the PSUs

3.12.1 Preparing for the Upgrade

3.12.1.1 Obtaining Software Packages

Perform the following steps to obtain the upgrade software packages:

- Enterprise users:
 - a. Visit [Intelligent Servers](#).
 - b. Click the server whose firmware is to be upgraded.
The server version list is displayed.
 - c. On the displayed page, click **Software Download**.
The server software version list is displayed.

- d. Select the target version.
- e. Download the upgrade package of the component to be upgraded to the client (local PC) and decompress the package.
- Carrier users: Contact technical support of your local Huawei office.

3.12.1.2 Verifying the Digital Signatures of Software Packages

To avoid using software packages that have been tampered with during transmission or storage, download their digital signature files for integrity check while downloading the software packages.

After a software package is downloaded from <https://support.huawei.com>, verify its PGP digital signature as instructed in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package but contact Huawei technical support.

Before a software package is used in installation or update, its digital signature also needs to be verified according to the *OpenPGP Signature Verification Guide* to ensure that the software package is not tampered with.

For carriers: <https://support.huawei.com/carrier/digitalSignatureAction>.

For enterprise users: <https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054>.

3.12.2 Performing the Upgrade

Scenarios

Upgrade the power supply unit (PSU) firmware of the X6000 or X6800 server.

NOTE

- Do not remove, insert, or power off PSUs during the firmware upgrade.
- If the upgrade of one of the PSUs fails, the whole upgrade process fails. The upgrade result of each PSU is displayed.
- If only one power module is installed, the upgrade is not supported.

Prerequisites

Conditions

- There are no "AC Lost" alarms.
- You have logged in to the HMM CLI from a client (for example, a PC).
- For the X6000 server:

Ensure that the server has two PSUs installed and at least one PSU (excluding those being upgraded) is working properly.

Data

- IP address of the HMM management network port.
- User name and password for logging in to the HMM. For the X6000 V3 and X6800 V3 servers, the default user name and password are **root** and

Huawei12#\$. For the X6000 V5 and X6800 V5 servers, the default user name and password are **Administrator** and **Admin@9000**.

Tools

- Secure file transfer tool, for example, XShell
- Secure terminal simulator, for example, PuTTY

Software

You have downloaded and decompressed the PSU firmware upgrade package to the client, and obtained the upgrade file.

Procedure

Step 1 Use a file transfer tool (such as XShell) to upload **PSU_001019.hpm** from the client (such as a PC) to the **/tmp** directory of the HMM.

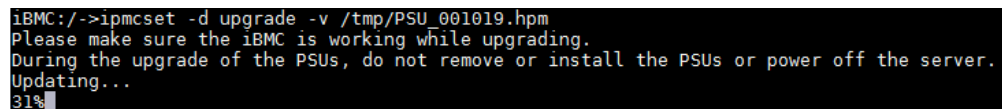
The operations vary with the tool you use. Refer to the user guide of the tool.

Step 2 On the HMM CLI, run the **ipmcget -d version** or **ipmcget -d psuinfo** command to check the PSU version information.

Step 3 On the HMM CLI, run **ipmcset -d upgrade -v /tmp/ PSU_001019.hpm**.

The upgrade starts, as shown in [Figure 3-28](#).

Figure 3-28 Upgrading PSU firmware



```
iBMC:/->ipmcset -d upgrade -v /tmp/PSU_001019.hpm
Please make sure the iBMC is working while upgrading.
During the upgrade of the PSUs, do not remove or install the PSUs or power off the server.
Updating...
31%
```

Step 4 After the upgrade is complete, run the **ipmcget -d version** or **ipmcget -d psuinfo** command on the HMM CLI to check whether the firmware version is the target version.

----End

3.12.3 Rolling Back the Firmware Version

3.12.3.1 Rollback Rules

If the upgrade fails and the software version is still the source version, you do not need to perform a rollback. If any of the following problems occurs, contact technical support to determine whether a rollback is required.

- A major fault occurred during the upgrade, and cannot be located and rectified within the specified time.
- After the upgrade is complete, the target version functions abnormally.
- The entire upgrade cannot be finished as scheduled. To prevent service interruption in peak hours caused by the upgrade, a rollback is required.

3.12.3.2 Rollback Procedure

Step 1 Determine the target version.

Step 2 Roll back the version.

The rollback procedure is similar to the upgrade procedure. For details, see [3.12.2 Performing the Upgrade](#).

----End

3.13 Upgrading Smart Provisioning

3.13.1 Upgrade Using Smart Provisioning

This section describes how to upgrade Smart Provisioning on a single server. For details, see the [Smart Provisioning User Guide](#).

3.13.2 Upgrading Smart Provisioning Using SmartKit

This section describes how to upgrade Smart Provisioning for multiple servers in batches. For details, see the [SmartKit Computing XXX User Guide](#) corresponding to the SmartKit plugin version.

4 Upgrading the Drive Firmware

For details, see the [*Huawei FusionServer Pro Servers Drive Firmware Upgrade Guide*](#).

5 Common Operations

- [5.1 Querying the IP Address of the iBMC Management Network Port](#)
- [5.2 Logging In to the iBMC WebUI](#)
- [5.3 Logging In Using the iMana 200 WebUI](#)
- [5.4 Logging In Using the iBMC WebUI](#)
- [5.5 Logging In to the iBMC CLI](#)
- [5.6 Transferring Files Using the Local Directory](#)
- [5.7 Check the Software Version of the Server Node.](#)
- [5.8 Viewing Server Node Alarms](#)
- [5.9 Checking the HMM Software Version](#)
- [5.10 Viewing HMM Alarm Information](#)
- [5.11 Logging In to the Server Over a Network Port by Using PuTTY](#)
- [5.12 Transferring Files Using WinSCP](#)
- [5.13 Logging In to the Management Module CLI Through the Management Network Port](#)
- [5.14 Logging In to the Management Module CLI Through the Management IP Address of the Server Node](#)

5.1 Querying the IP Address of the iBMC Management Network Port

The method used to query the iBMC IP address varies depending on the server platform. For details, see *BIOS Parameter Reference* of the specific platform. This section uses the Grantley and Purley platforms as an example to describe how to query the iBMC IP address using the BIOS.

5.1.1 Querying the IP Address of the iBMC Management Network Port (Romley/Brickland/Grantley Platform)

Scenarios

Query the IP address of the iBMC management network port in BIOS. .

Table 5-1 lists the default IP addresses of the iBMC network port.

Table 5-1 Default IP addresses

Slot	IP
Slot 1	10.10.1.101
Slot 2	10.10.1.102
Slot 3	10.10.1.103
Slot 4	10.10.1.104

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

This operation requires no special condition.

Data

This operation requires no data preparation.

Procedure

Step 1 Restart the server.

1. Upon server startup, press **Delete** or **F4** within 3 seconds until the **BIOS Setup Utility** screen is displayed.
2. If a dialog box prompting you to enter the password is displayed during the startup, enter the password, as shown in **Figure 5-1**.

NOTE

The default BIOS password is **Huawei12#\$**.

Figure 5-1 Entering a BIOS password

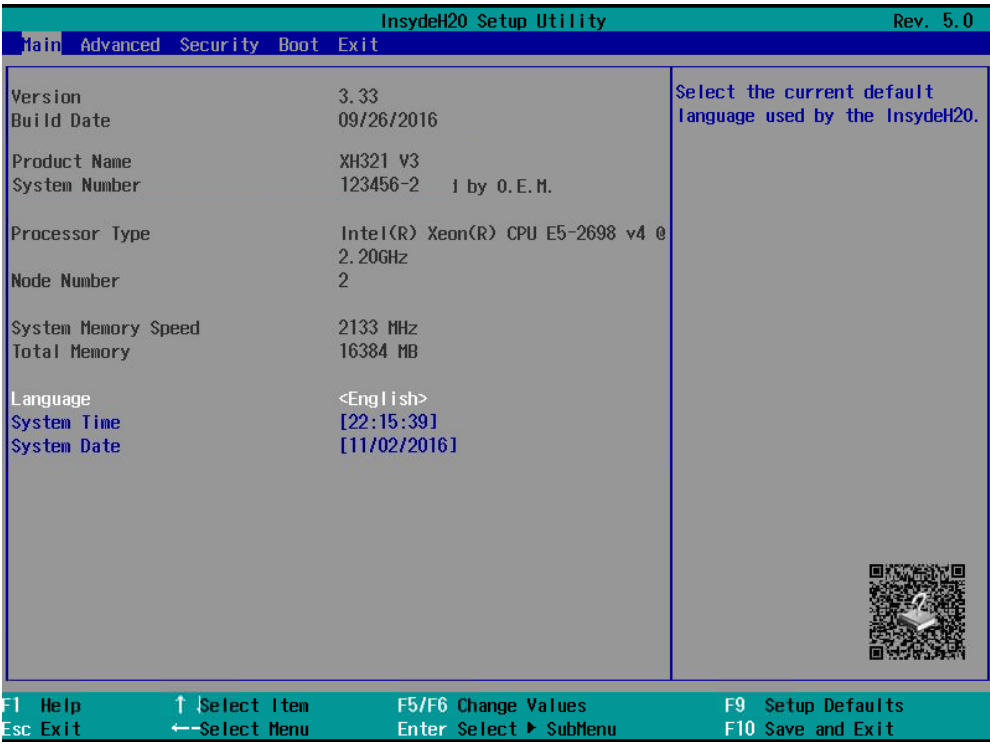


Step 2 The BIOS screen is displayed, as shown in [Figure 5-2](#).

 NOTE

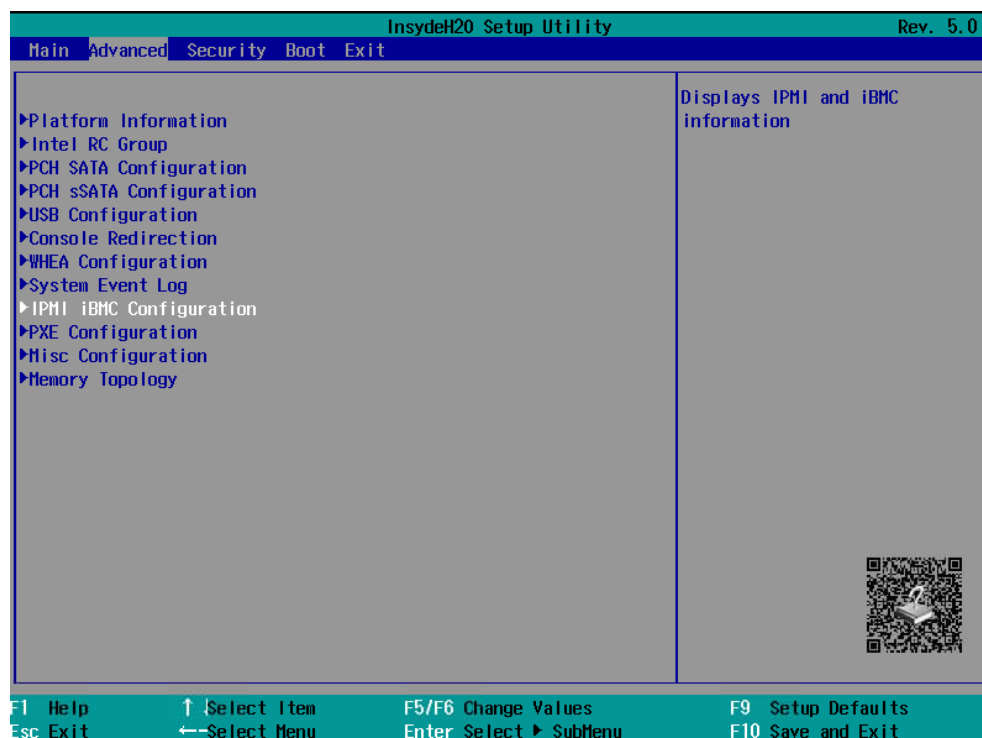
The BIOS setup screen varies according to the CPU platform. For details, see the BIOS document of the server you use.

Figure 5-2 Main screen



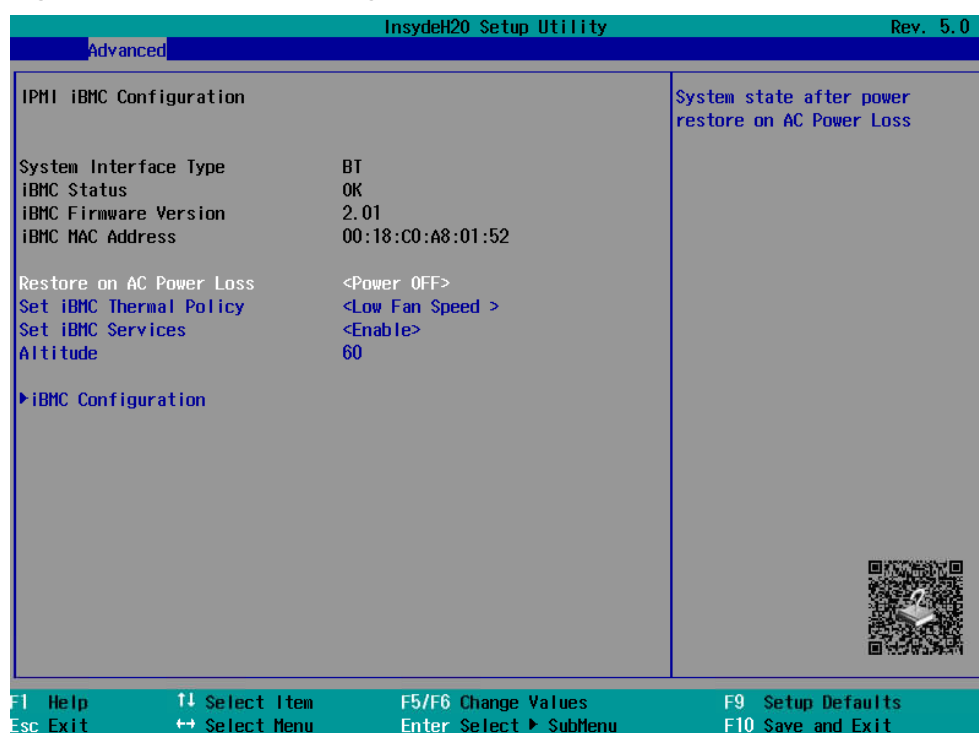
Step 3 Select the **Advanced** screen using arrow keys, as shown in [Figure 5-3](#).

Figure 5-3 Advanced screen



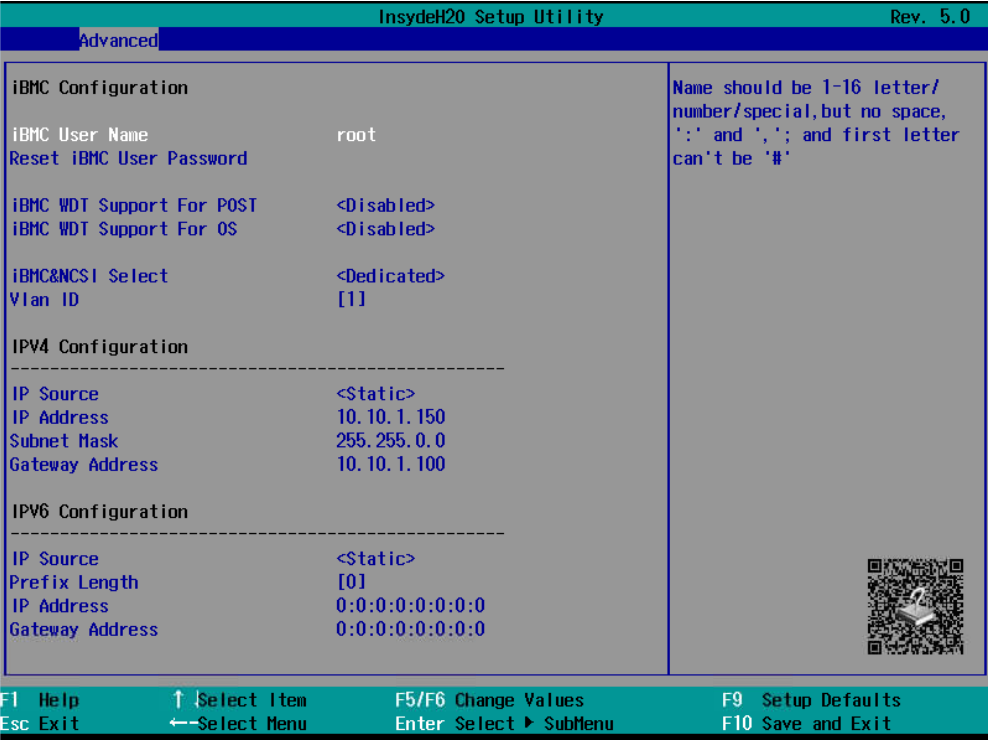
Step 4 On the **Advanced** screen, select **IPMI iBMC Configuration** using arrow keys and press **Enter**, as shown in [Figure 5-4](#).

Figure 5-4 IPMI iBMC Configuration screen



Step 5 On the **IPMI iBMC Configuration** screen, select **iBMC Configuration** using arrow keys and press **Enter**, as shown in [Figure 5-5](#).

Figure 5-5 iBMC Configuration screen



NOTE

The default BIOS password is **Huawei12#\$**.

The server IP address is displayed on this screen.

----End

5.1.2 Querying the IP Address of the iBMC Management Network Port (Purley/Cedar Island/Whitley Platform)

Scenarios

Query the IP address of the iBMC management network port in BIOS. .

Table 5-2 lists the default IP addresses of the iBMC network port.

Table 5-2 Default IP addresses

Slot	IP
Slot 1	10.10.1.101
Slot 2	10.10.1.102
Slot 3	10.10.1.103
Slot 4	10.10.1.104

You can query the IP address of the iBMC management network port in BIOS using the following menus:

Advanced > IPMI iBMC Configuration > iBMC Configuration

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

This operation requires no special condition.

Data

This operation requires no data preparation.

Procedure

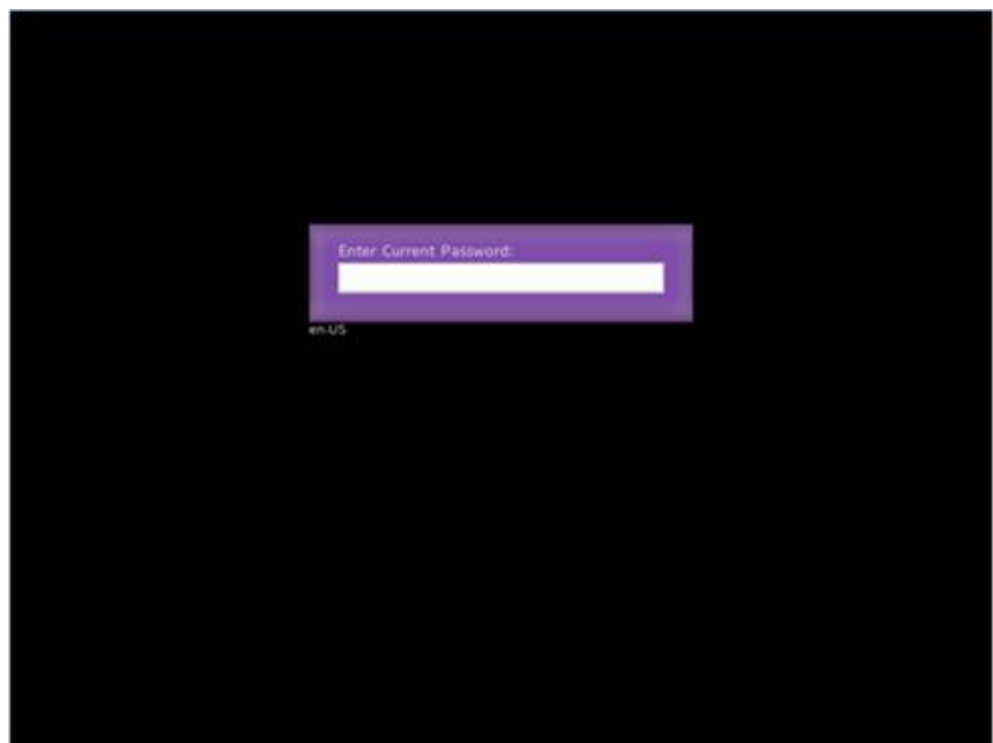
Step 1 Restart the server.

1. Upon server startup, press **Delete** within 3 seconds until the **BIOS Setup Utility** screen is displayed.
2. If a dialog box prompting you to enter the password is displayed during the startup, enter the password, as shown in [Figure 5-6](#).

NOTE

The default BIOS password is **Admin@9000**.

Figure 5-6 Entering a BIOS password

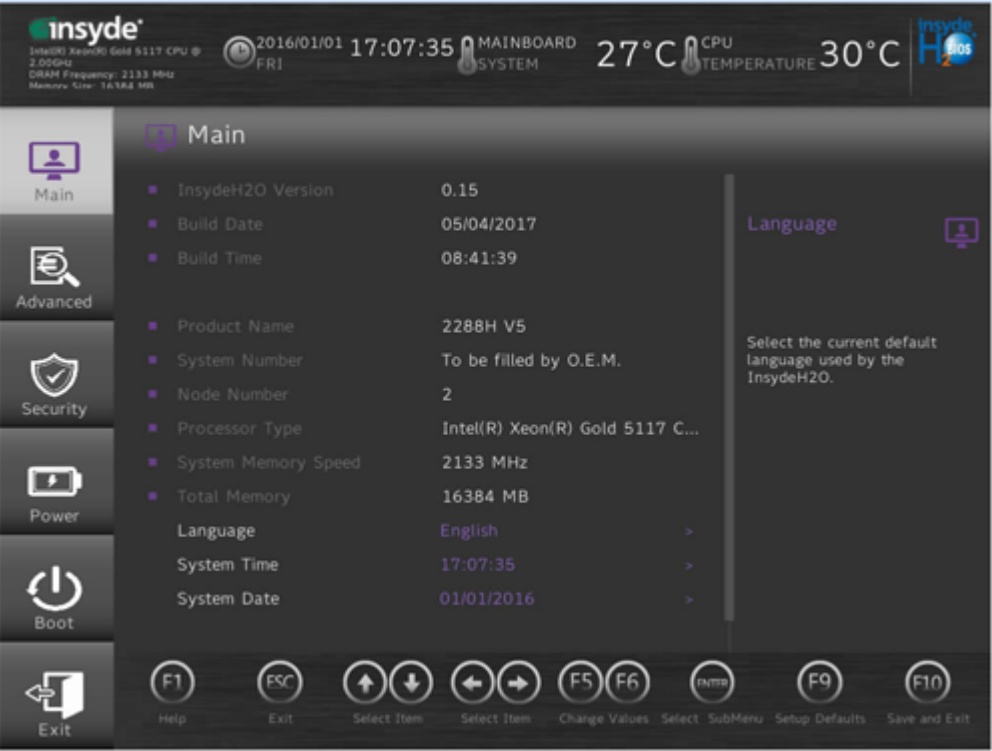


Step 2 The BIOS screen is displayed, as shown in [Figure 5-7](#).

 NOTE

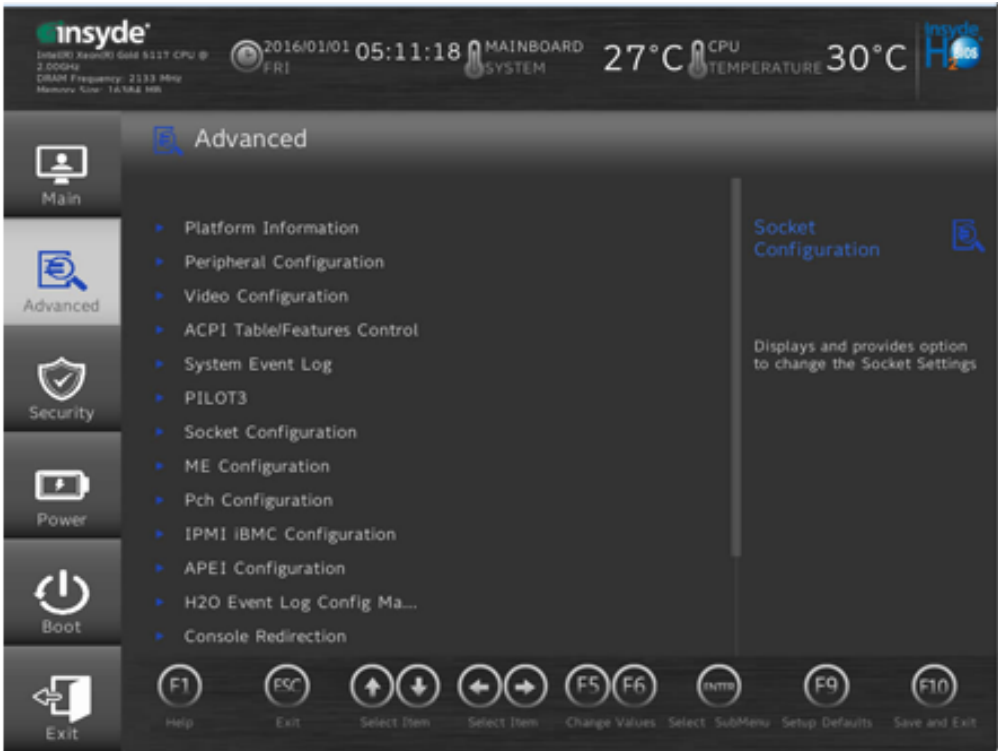
The BIOS setup screen varies according to the CPU platform. For details, see the BIOS document of the server you use.

Figure 5-7 Main screen



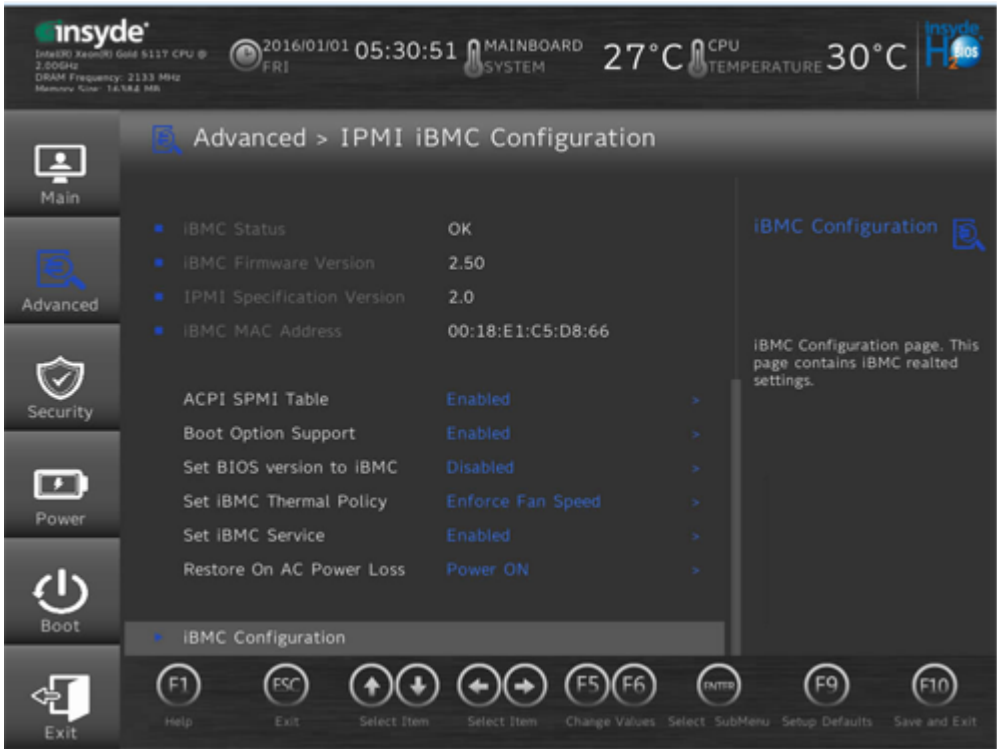
Step 3 Select the **Advanced** screen using arrow keys, as shown in [Figure 5-8](#).

Figure 5-8 Advanced screen



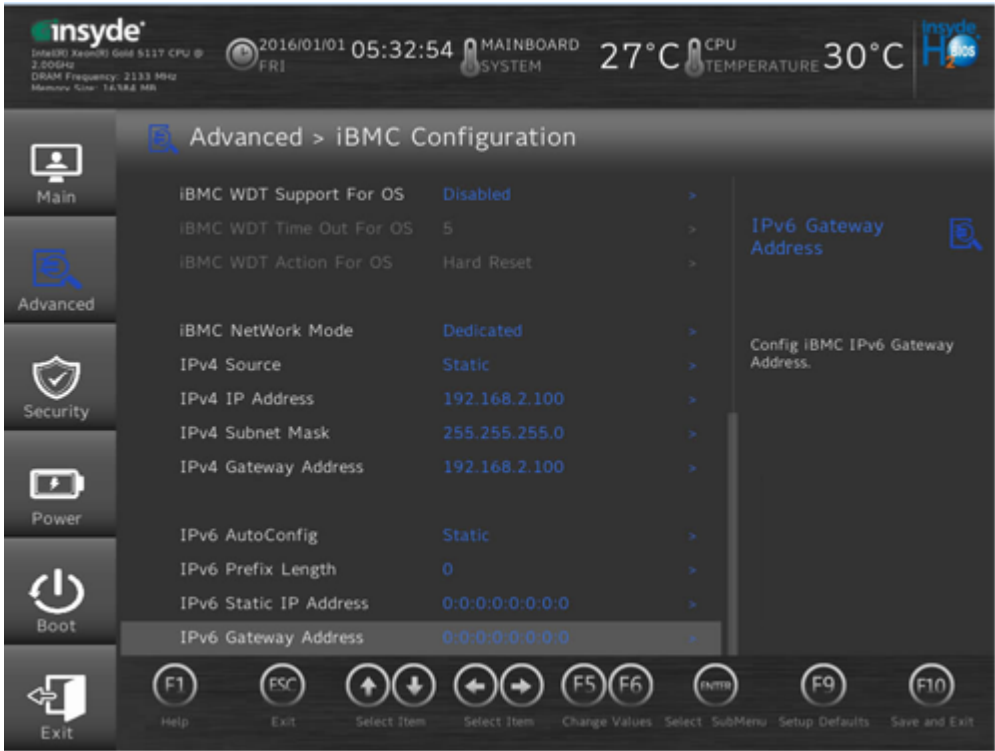
Step 4 On the **Advanced** screen, select **IPMI iBMC Configuration** using arrow keys and press **Enter**, as shown in [Figure 5-9](#).

Figure 5-9 IPMI iBMC Configuration screen



Step 5 On the **IPMI iBMC Configuration** screen, select **iBMC Configuration** using arrow keys and press **Enter**, as shown in **Figure 5-10**.

Figure 5-10 iBMC Configuration screen



The server IP address is displayed on this screen.

----End

5.1.3 Querying the IP Address of the iBMC Management Network Port Using SSH

Scenarios

Query the IP address of the iBMC management network port in the HMM.

For a full-width node, the default IP address of the management network port is 10.10.1.101.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

You have logged in to the HMM CLI. For details, see the section "Logging In to the HMM CLI Through the Management Network Port of a Server Node" in the server user guide.

Data

- Internal network segment IP addresses of the compute node:
 - Slot 1: 172.31.1.129
 - Slot 2: 172.31.1.130
- Default user name and password of the compute node

Procedure

- Step 1** Run the SSH command to log in to the compute node using the internal network segment IP address.

Example:

```
iBMC:/->ssh root@172.31.1.129
The authenticity of host '172.31.1.129 (172.31.1.129)' can't be established.
ECDSA key fingerprint is SHA256:gOgF1v/fGKzvFRkjm1axPEK85NGrFP6UOUSBzt6qx48.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.31.1.129' (ECDSA) to the list of known hosts.
WARNING! This system is PRIVATE and PROPRIETARY and may only be accessed by authorized users.
Unauthorized use of the system is prohibited. The owner, or its agents, may monitor any activity or
communication on the system. The owner, or its agents, may retrieve any information stored within the
system. By accessing and using the system, you are consenting to such monitoring and information retrieval
for law enforcement and other purposes.
root@172.31.1.129's password:
Last login: Thu Nov  2 20:41:30 2017 from 192.168.10.197
iBMC:/->
```

- Step 2** Run the `ipmcget -v ipinfo` command to query the IP address of the iBMC.

Example:

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID      : 1
Net Mode         : Manual
Net Type         : Dedicated
IPv4 Information :
IP Mode          : static
IP Address       : 192.168.10.206
Subnet Mask      : 255.255.255.0
Default Gateway  : 192.168.10.206
MAC Address      : 00:18:c0:a8:0a:cf
IPv6 Information :
IPv6 Mode        : static
IPv6 Address 1   :
Default Gateway IPv6 :
Link-Local Address : fe80::218:c0ff:fea8:acf/64
VLAN Information :
VLAN State       : disabled

EthGroup ID      : 2
Net Mode         : Manual
Net Type         : Dedicated
IPv4 Information :
IP Mode          : static
IP Address       : 172.31.1.129
Subnet Mask      : 255.255.255.0
Default Gateway  :
MAC Address      : 00:18:c0:a8:0a:cf
IPv6 Information :
IPv6 Mode        : static
IPv6 Address 1   :
Default Gateway IPv6 :
Link-Local Address : fe80::218:c0ff:fea8:acf/64
VLAN Information :
```

```
VLAN State      : enabled
VLAN ID         : 4093
```

----End

5.2 Logging In to the iBMC WebUI

5.2.1 Logging In to the iBMC WebUI (iBMC Earlier Than V561)

Scenarios

Log in to the iBMC WebUI using a browser on a local PC. The section uses a PC running Windows 7 and Internet Explorer 9.0 browser as an example to describe how to log in to iBMC.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

The web browser and Java Runtime Environment (JRE) of the required versions have been installed on the local PC. [Table 5-3](#) shows the system configuration requirements of the local PC.

Ensure that the local PC meets the following networking conditions:

- The local PC is connected to the iBMC management network port on the server through a network cable.
- The IP addresses of the local PC and the iBMC management network port are on the same network segment.

Table 5-3 Operating environment requirements

OS	Browser	Java Runtime Environment (JRE)
Windows 7 32-bit Windows 7 (64-bit)	Internet Explorer 9.0 to 11.0 NOTE HTML5 supports only Internet Explorer 10.0 and later versions.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	

OS	Browser	Java Runtime Environment (JRE)
Windows 8 32-bit Windows 8 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Windows 10 (64-bit)	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
Windows Server 2012 R2 64-bit	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
Windows Server 2016 64-bit	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
Windows Server 2008 R2 64-bit	Internet Explorer 9.0 to 11.0 NOTE HTML5 supports only Internet Explorer 10.0 and later versions.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Windows Server 2012 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Red Hat 6.0 64-bit	Mozilla Firefox 39.0 to 54.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
MAC X v10.7	Safari 8.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	

NOTE

If the JRE version does not meet requirements, download the required version from <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

Data

Table 5-4 lists the required data before you log in to the iBMC WebUI.

Table 5-4 Data to be obtained

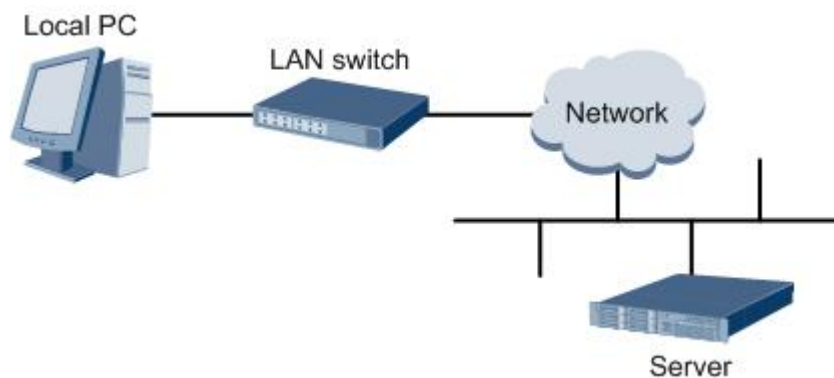
Category	Parameter	Description	Example
User login information	User Name	User name for logging in to the iBMC WebUI. For details about the default user name, see <i>User List</i> .	- Grantley/Romley/Brickland platform: root - Purley/Cedar Island/Whitley platform: Administrator
	Password	Password for logging in to the iBMC WebUI. For details about the default password, see <i>User List</i> .	- Grantley/Romley/Brickland platform: Huawei12#\$ - Purley/Cedar Island/Whitley platform: Admin@9000

Procedure

- Step 1** Connect the local PC to the iBMC management network port on the server by using a crossover cable or twisted pair cable.

Figure 5-11 shows the network diagram.

Figure 5-11 Network diagram



Step 2 Open Internet Explorer on the local PC.

Step 3 In the address box, enter the IP address of the server iBMC management network port (for example, **https://192.168.2.100**).

 NOTE

For details about how to determine the IP address of the iBMC management network port, see [5.1 Querying the IP Address of the iBMC Management Network Port](#).

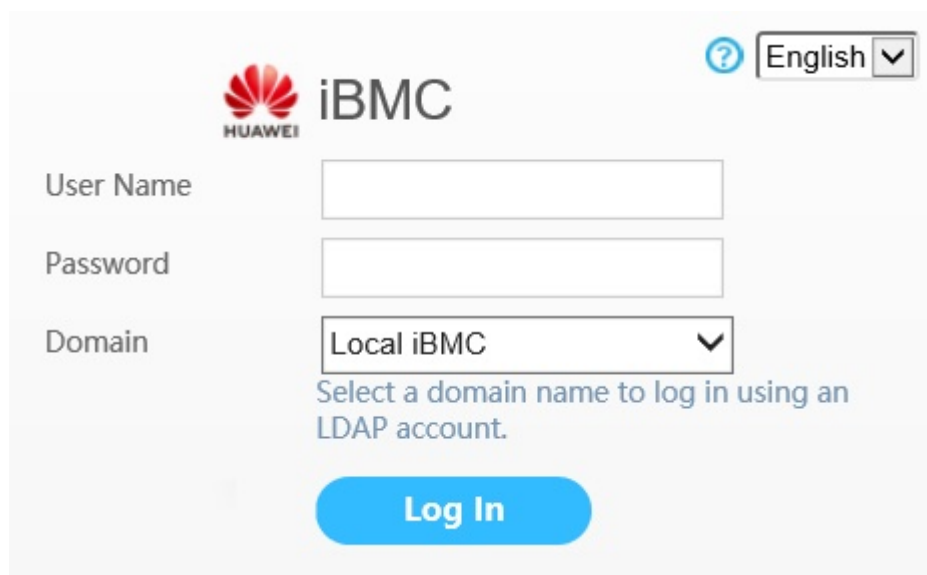
Step 4 Press **Enter**.

The iBMC login page is displayed, as shown in [Figure 5-12](#).

 NOTE

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

Figure 5-12 iBMC login page

The screenshot shows the iBMC login interface. At the top left is the Huawei logo and the text 'iBMC'. At the top right is a language selector set to 'English'. Below the logo are three input fields: 'User Name', 'Password', and 'Domain'. The 'Domain' dropdown menu is currently set to 'Local iBMC'. Below the 'Domain' field is a blue link that says 'Select a domain name to log in using an LDAP account.' At the bottom center is a large blue 'Log In' button.

Step 5 Enter your user name and password.

 NOTE

If you log in with incorrect passwords for five consecutive times, the system will lock your account. If your user account is locked, log in again 5 minutes later.

Step 6 Select **Local iBMC** from the **Domain** drop-down list.

Step 7 Click **Log In**.

The **Information Summary** page is displayed. The login username is displayed in the upper right corner of the page.

----End

5.2.2 Logging In to the iBMC WebUI (iBMC V561 or Later, or iBMC V3.01.00.00 or Later)

Scenarios

Log in to the iBMC WebUI using a browser on a local PC. The section uses a PC running Windows 7 and Internet Explorer 11.0 browser as an example to describe how to log in to iBMC.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

The web browser and Java Runtime Environment (JRE) of the required versions have been installed on the local PC. [Table 5-5](#) shows the system configuration requirements of the local PC.

Ensure that the local PC meets the following networking conditions:

- The local PC is connected to the iBMC management network port on the server through a network cable.
- The IP addresses of the local PC and the iBMC management network port are on the same network segment.

Table 5-5 Operating environment requirements

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

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

 NOTE

If the JRE version does not meet requirements, download the required version from <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

Data

Table 5-6 lists the required data before you log in to the iBMC WebUI.

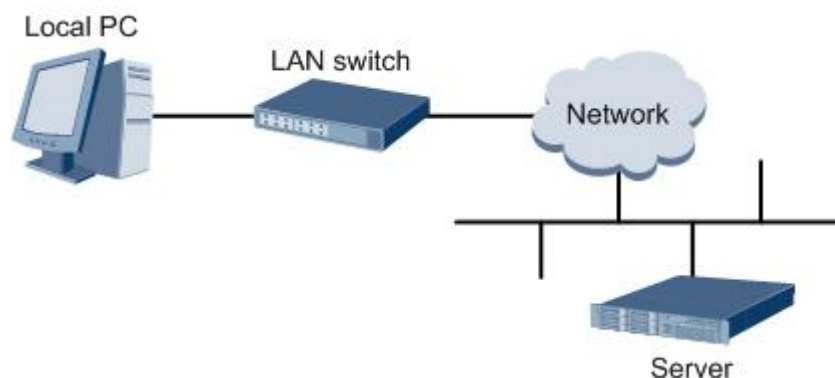
Table 5-6 Data to be obtained

Category	Parameter	Description	Example
User login information	User Name	User name for logging in to the iBMC WebUI. For details about the default user name, see <i>User List</i> .	- Grantley/Romley/Brickland platform: root - Purley/Cedar Island/Whitley platform: Administrator
	Password	Password for logging in to the iBMC WebUI. For details about the default password, see <i>User List</i> .	- Grantley/Romley/Brickland platform: Huawei12#\$ - Purley/Cedar Island/Whitley platform: Admin@9000

Procedure

- Step 1** Connect the local PC to the iBMC management network port on the server by using a crossover cable or twisted pair cable.

Figure 5-13 shows the network diagram.

Figure 5-13 Network diagram

- Step 2** Open Internet Explorer on the local PC.
- Step 3** In the address box, enter the IP address of the server iBMC management network port (for example, **https://192.168.2.100**).

NOTE

For details about how to determine the IP address of the iBMC management network port, see [5.1 Querying the IP Address of the iBMC Management Network Port](#).

Step 4 Press **Enter**.

The iBMC login page is displayed, as shown in [Figure 5-14](#).

 NOTE

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

Figure 5-14 iBMC login page



The screenshot shows the iBMC login interface. At the top, there is the 'iBMC' logo on the left, a grey rectangular placeholder in the center, and a QR code on the right. Below the logo, there are three input fields: 'User Name' with the prompt 'Please enter the user name.', 'Password' with the prompt 'Please enter the password.', and 'Domain' with the text 'Local iBMC'. At the bottom, there is a large blue 'Log In' button and a link labeled 'SSO'.

Step 5 Enter your user name and password.

 NOTE

If you log in with incorrect passwords for five consecutive times, the system will lock your account. If your user account is locked, log in again 5 minutes later.

Step 6 Select **Local iBMC** from the **Domain** drop-down list.

Step 7 Click **Log In**.

The **Information Summary** page is displayed. The login username is displayed in the upper right corner of the page.

----End

5.3 Logging In Using the iMana 200 WebUI

Conditions

The web browser and Java Runtime Environment (JRE) of the required versions have been installed on the client.

Table 1-1 lists the software configuration requirements of the client.

Table 5-7 Required software versions

OS	Browser	Java Runtime Environment (JRE)
- Windows 7 32-bit - Windows 8 32-bit - Windows Server 2008 32-bit	Internet Explorer 8.0 to 10.0	- JRE 1.6.0 U25 (32-bit) - JRE 1.7.0 U40 (32-bit)
	Mozilla Firefox 9.0 to 23.0	
	Google Chrome 13.0 to 31.0	
- Windows 7 64-bit - Windows 8 64-bit - Windows Server 2008 R2 64-bit - Windows Server 2012 64-bit	Internet Explorer 8.0 to 10.0	- JRE 1.6.0 U25 (64-bit) - JRE 1.7.0 U40 (64-bit)
	Mozilla Firefox 9.0 to 23.0	
	Google Chrome 13.0 to 31.0	
- RHEL 4.3 64-bit - RHEL 6.0 64-bit	Mozilla Firefox 9.0 to 23.0	- JRE 1.6.0 U25 - JRE 1.7.0 U40
MAC X v10.7	Safari 5.1	- JRE 1.6.0 U25 - JRE 1.7.0 U40
	Mozilla Firefox 9.0 to 23.0	

Procedure

Step 1 Obtain the following data:

- IP address and subnet mask for the iMana management network port
- User name and password for login to the iMana

Step 2 Configure a login environment.

1. Connect the network port on a PC to the iMana management network port of the server using a network cable.
2. Set an IP address for the PC. Ensure that this IP address is on the same network segment as the IP address of the iMana management network port.
For example, set the IP address to **192.168.2.10**, and the subnet mask to **255.255.255.0**.

Step 3 Set the properties of the Internet Explorer browser.

1. On the menu bar of Internet Explorer, choose **Tools > Internet Options**.
The **Internet Options** dialog box is displayed.

 NOTE

This section uses Windows 7 with Internet Explorer 8 as an example.

2. Click the **Connections** tab, and then click **LAN Settings**.
The **Local Area Network (LAN) Settings** dialog box is displayed.
3. In the **Proxy server** area, deselect **Use a proxy server for your LAN**.

 NOTE

You can also retain the proxy server configuration and add the iMana IP address segment in the **Exceptions** area in the **Advanced** dialog box of the proxy server.

4. Click **OK**.
The **Local Area Network (LAN) Settings** dialog box is closed.
5. Click **OK**.
The **Internet Options** dialog box is closed.

Step 4 Log in to the server management page.

1. Open Internet Explorer, enter **https://IP address for the iMana management network port** in the address box, and press **Enter**.
URL format: **https://IP address of the iMana management network port**.
The **Certificate Error: Navigation Blocked** page is displayed.
2. Click **Continue to this website (not recommended)**.
The login page is displayed, as shown in [Figure 5-1](#).

Figure 5-15 iMana login page



3. On the login page, set the parameters as follows:
- a. Select a language.

b. Enter your user name and password. The default user name is **root**, and the default password is **Huawei12#\$** or **root**.

c. Select **This iMana** from the **Log on to** drop-down list.

d. Click **Log In**. The iMana WebUI is displayed, as shown in [Figure 5-16](#). You can click **Reset** to reset the information.

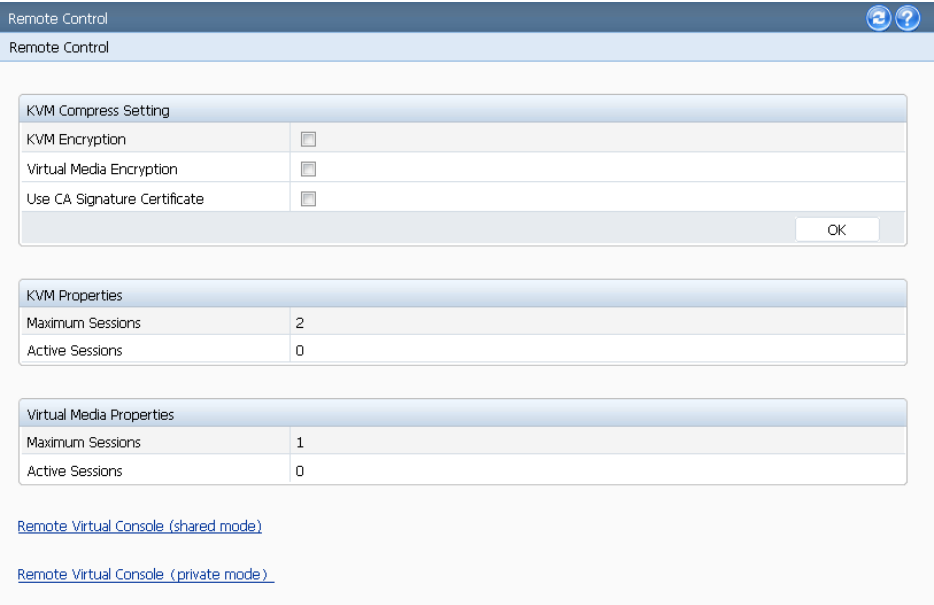
Figure 5-16 iMana WebUI



- Step 5 Open the Remote Virtual Console.
1. In the navigation pane, click **Remote Control**.

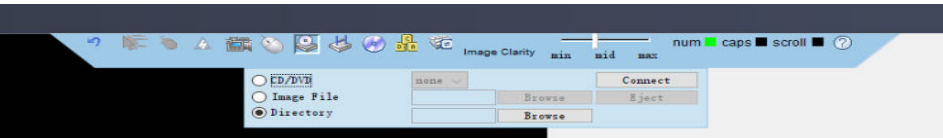
The **Remote Control** page is displayed, as shown in [Figure 5-17](#).

Figure 5-17 Remote Control page



2.
- On the **Remote Control** page, click **Remote Virtual Console (requiring JRE)**. The Remote Virtual Console is displayed, as shown in [Figure 5-18](#).

Figure 5-18 Remote Virtual Console



----End

5.4 Logging In Using the iBMC WebUI

Conditions

The web browser and Java Runtime Environment (JRE) of the required versions have been installed on the client.

[Table 1-2](#) lists the required software versions.

Table 5-8 Required software versions

OS	Browser	Java Runtime Environment (JRE)
Windows 7 32-bit Windows 7 64-bit	Internet Explorer 9.0 to 11.0 NOTE HTML5 supports only Internet Explorer 10.0 or later.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144

OS	Browser	Java Runtime Environment (JRE)
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Windows 8 32-bit Windows 8 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45 JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
	Google Chrome 21.0 to 44.0	
Windows 10 64-bit	Internet Explorer 11.0	JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
Windows 2012 R2 64-bit	Internet Explorer 11.0	JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
Windows 2016 64-bit	Internet Explorer 11.0	JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
Windows Server 2008 R2 64-bit	Internet Explorer 9.0 to 11.0 NOTE HTML5 supports only Internet Explorer 10.0 or later.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Windows Server 2012 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45 JRE 1.8 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U144
	Google Chrome 21.0 to 44.0	

OS	Browser	Java Runtime Environment (JRE)
Red Hat 6.0 64-bit	Mozilla Firefox 39.0 to 54.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
MAC X v10.7	Safari 8.0	JRE 1.7 U45
	Mozilla Firefox 39.0 to 54.0	JRE 1.8 U45 JRE 1.8 U144

Procedure

This section uses iBMC 2.50 as an example. The WebUI varies depending on the iBMC version. For details, see the iBMC online help.

Step 1 Obtain the following data:

- IP address and subnet mask for the iBMC management network port
- User name and password for login to the iBMC

Step 2 Configure a login environment.

1. Connect the network port on a PC to the iBMC management network port of the server using a network cable.
2. Set an IP address for the PC. Ensure that this IP address is on the same network segment as the IP address of the iBMC management network port.
For example, set the IP address to **192.168.2.10** and the subnet mask to **255.255.255.0**.

Step 3 Log in to the server management page.

1. Open Internet Explorer, enter the IP address of the iBMC management network port in the address box, and press **Enter**.

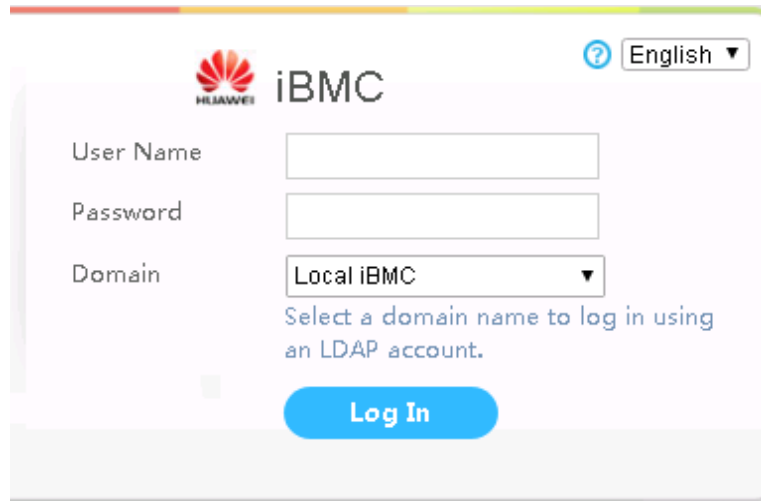
URL format: **http://IP address of the iBMC management network port**.

The iBMC login page is displayed, as shown in [Figure 5-19](#).

 NOTE

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

Figure 5-19 iBMC login page

The image shows the iBMC login page. At the top left is the Huawei logo and the text 'iBMC'. At the top right is a language selector showing 'English'. Below the header are three input fields: 'User Name', 'Password', and 'Domain'. The 'Domain' dropdown menu is currently set to 'Local iBMC'. Below the 'Domain' field is a blue link that says 'Select a domain name to log in using an LDAP account.' At the bottom center is a blue 'Log In' button.

2. On the login page, set the parameters as follows:
 - a. Select a language.
 - b. Enter a user name and password. For the default user name and password, see the [iBMC User Guide](#).
 - c. Select **This iBMC** from the **Log on to** drop-down list.
 - d. Click **Log In**.

The iBMC WebUI is displayed

Step 4 Open the Remote Virtual Console.

1. Choose **Remote Console** from the main menu.

The **Remote Console** page is displayed, as shown in [Figure 5-20](#).

Figure 5-20 Remote Control page

Remote Console

Integrated Remote Console

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

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

Independent Remote Console

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

Remote Console Settings

Timeout Period (min)	0
Maximum Sessions	2
Active Sessions	0
Encryption	☐
Enable Local KVM	☒
Persistent Virtual Keyboard and Mouse	☒

Save

Virtual Media

Maximum Sessions	1
Active Sessions	0
Encryption	☐

Save

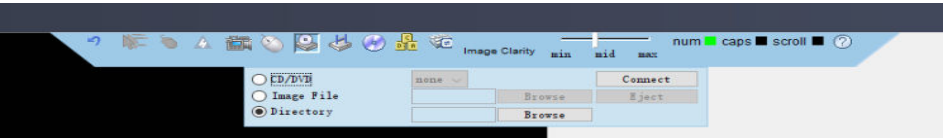
VNC Service

Timeout Period (min)	0
Keyboard Layout	English(US)
VNC Password	
Confirm Password	
Password Validity (Days)	Unlimited
Login Rules	☐ Rule1 ☐ Rule2 ☐ Rule3 View login rules
SSL Encryption	☐
Maximum Sessions	5
Active Sessions	0

Save

2. On the **Remote Control** page, click **Remote Virtual Console**.
The Remote Virtual Console is displayed, as shown in [Figure 5-21](#).

Figure 5-21 Remote Virtual Console



----End

5.5 Logging In to the iBMC CLI

Log in to the command-line interface (CLI) of the iBMC.

Login Modes

You can log in to the iBMC CLI using any of the following methods:

- SSH

A maximum of five users can log in to the Atlas IES over SSH at the same time.

 NOTE

SSH supports AES128-CTR, AES192-CTR, and AES256-CTR encryption algorithms. Use an appropriate encryption algorithm when logging in to the iBMC over SSH.

- Local serial port

 NOTE

- The default user name is **root** and the default password is **Huawei12#\$** for V3 servers. The default user name is **Administrator** and the default password is **Admin@9000** for V5/V6 servers.
- The system locks a user account if the user enters incorrect passwords for consecutive five times. The user account is automatically unlocked five minutes later. The administrator can also unlock the user account using CLI.
- For security purposes, change the initial password after the first login and change your password periodically.
- The default command timeout period is 15 minutes.

Conditions

- Before logging in to the iBMC CLI over the network port, ensure that the configuration terminal can properly communicate with the server management network port.

 NOTE

Do not connect two management network ports at the same time. You can log in to the iBMC through only one management network port.

- Before logging in to the iBMC CLI through the serial port, use a serial cable to connect the serial port of the configuration terminal to the serial port of the server by using a serial cable.

Accessing iBMC CLI Over SSH

1. Download an SSH communication tool on to client.
2. Connect the client to the server management network port directly or over the network.
3. Configure an IP address for the client to connect it to the iBMC management network port.
4. On the client, start the SSH communication tool and configure related parameters (for example, the IP address).
5. Enter the user name and password to log in to the iBMC CLI.

 NOTE

- Both local and LDAP users can log in to the iBMC CLI over SSH.
- Before logging in to the iBMC CLI as an LDAP user, ensure that the connection between the iBMC and the LDAP server is normal.
- The LDAP user can log in to the iBMC CLI without entering the domain server information.

Accessing iBMC CLI Over the Serial Port

NOTICE

Before logging in to the iBMC CLI over the serial port, ensure that the system serial port of the chassis is switched to the iBMC serial port. You can switch over the serial port by running the **serialdir** command on the iBMC CLI or using a jumper (see the user guide of your server).

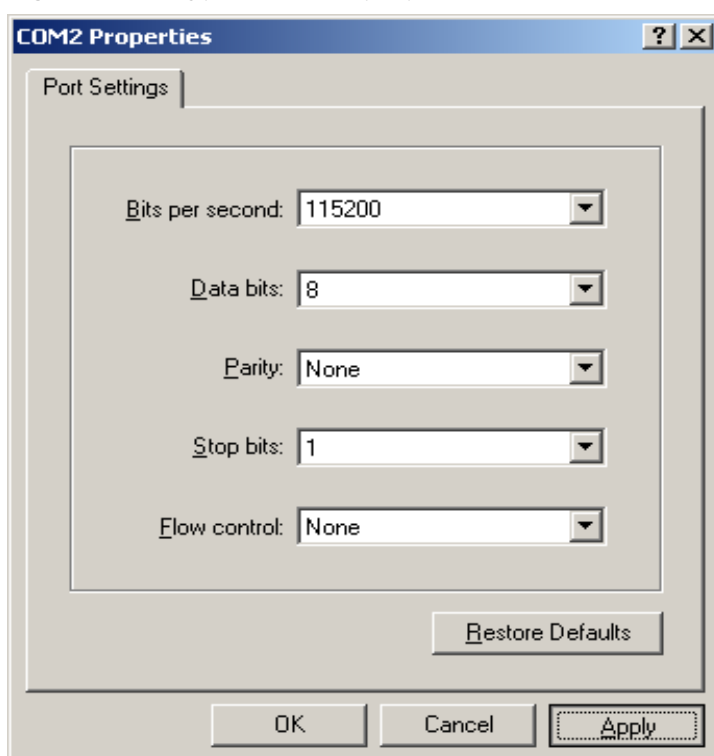
Step 1 Connect the client and the server using a serial cable.

Step 2 Open HyperTerminal and set the following parameters:

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

For details on how to set the parameters, see [Figure 5-22](#).

Figure 5-22 HyperTerminal properties



Step 3 Enter the username and password after the connection is established.

----End

5.6 Transferring Files Using the Local Directory

Use the local **Directory** of the Remote Virtual Console to transfer files between the client and server. The example in this section describes how to send files from a local directory to the server.

Procedure

Step 1 Obtain the following data:

- IP address and subnet mask for the iBMC management network port
- User name and password of the server iBMC

Step 2 Log in to the remote virtual console of the server.

Depending on the management software, see one of the following sections:

- [5.3 Logging In Using the iMana 200 WebUI](#)
- [5.4 Logging In Using the iBMC WebUI](#)

Step 3 Open the local directory.

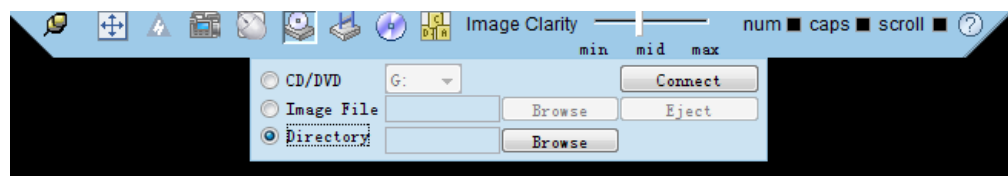
1. Click Remote Virtual Console (Shared Mode) or Remote Virtual Console (Private Mode) on the Remote Control or Remote Console page.

Open the Remote Virtual Console.

2. Click .

The window shown in [Figure 5-23](#) is displayed.

Figure 5-23 Accessing the local directory



3. Click **Directory**.
4. Click **Browse** to select a folder on the client, such as **D:\test**.

NOTE

The folder cannot be empty.

5. Click **Connect**.

The selected directory is identified as a local directory of the server.

Step 4 Place the file to be sent in the target directory.

Copy the file (such as a driver package or script) to the target directory specified in [4](#) of [Step 3](#).

Step 5 Copy the file to the server.

1. Log in to the server as user **root**.

2. Find the local directory specified in 4 of [Step 3](#).
This operation varies depending on the OS type. For details, see the official OS documentation.
3. Copy the file in the directory found in [Step 5.2](#) of [Step 5](#) to a directory on the server (for example, `/tmp`).

-----End

5.7 Check the Software Version of the Server Node.

Scenarios

Check software versions of the iBMC and BIOS.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

This operation requires no data preparation.

Procedure

Step 1 Choose **Information** on the main menu.

Step 2 In the navigation tree, choose **Information Summary**, as shown in [Figure 5-24](#).

Figure 5-24 Information Summary page



NOTE

In the **Basic Info** area:

- **iBMC Firmware Version:** indicates the iBMC version.
- **BIOS Firmware Version:** indicates the BIOS version.

Step 3 View and record the current iBMC and BIOS versions.

Step 4 Compare the version number obtained in [Step 3](#) with the version number of the downloaded software upgrade package.

- If the downloaded upgrade software version is the same as the version obtained in [Step 3](#), the upgrade of the iBMC, and BIOS is successful.
- If the version numbers obtained in [Step 3](#) are smaller than the version numbers downloaded in the upgrade packages, you need to upgrade the components.

----End

5.8 Viewing Server Node Alarms

Scenarios

Query alarms generated for a server.

This section uses iBMC 2.50 as an example. The WebUI varies depending on the iBMC version. For details, see the iBMC online help.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

You have logged in to the iBMC WebUI. For details, see [5.2 Logging In to the iBMC WebUI](#).

Data

This operation requires no data preparation.

Procedure

Step 1 Choose **Information** on the main menu.

Step 2 In the navigation tree, choose **Information Summary**, as shown in [Figure 5-25](#).

Figure 5-25 Information Summary page



Step 3 In the **Device Health Status** area, check alarms of all severities.

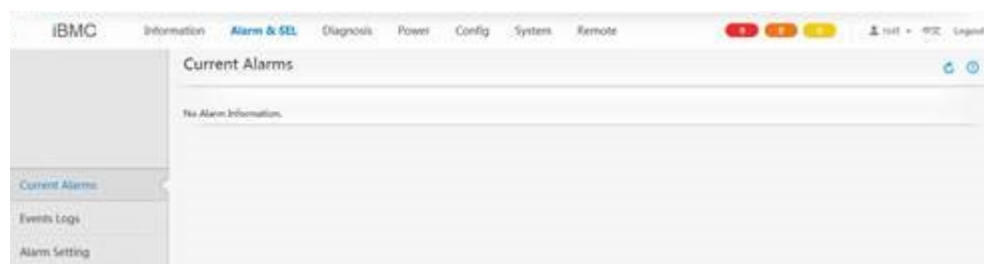
 NOTE

-  : indicates a critical alarm. Critical alarms are generated for faults that may power off devices, and even interrupt the system services. Immediate corrective measures are required.
-  : indicates a major alarm. Major alarms are generated for faults that may affect normal running of the system or interrupt services.
-  : indicates a minor alarm. Minor alarms are generated for the faults that do not have major impact on the system. Prompt corrective measures are required to prevent more serious faults.

Step 4 Choose **Alarm & SEL** on the main menu.

Step 5 In the navigation tree, choose **Current Alarms**, and view the alarm information, as shown in [Figure 5-26](#).

Figure 5-26 Current Alarms page



----End

5.9 Checking the HMM Software Version

Scenarios

Check the software versions of the HMM.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

No special condition is required for this operation.

Data

Data preparation is not required for this operation.

Procedure

Step 1 Log in to the HMM CLI. For details, see [5.11 Logging In to the Server Over a Network Port by Using PuTTY](#).

Step 2 Run the **ipmcget -d version** in the HMM CLI.

```
iBMC:/->ipmcget -d version
----- iBMC INFO -----
IPMC      CPU:      Hi1710
IPMI      Version:  2.0
CPLD      Version:  (U30)0.02
Active iBMC Version: (U9)2.80
Active iBMC Build:   001
Active iBMC Built:   22:11:24 Mar 14 2018
Backup iBMC Version: 2.78
SDK        Version:  3.11
SDK        Built:    10:19:29 Mar 9 2018
Active Uboot Version: 2.1.07 (Dec 21 2017 - 18:01:59)
Backup Uboot Version: 2.1.07 (Dec 21 2017 - 18:01:59)
IPMB      Address:   0x10
----- Product INFO -----
Product   ID:      0x0003
Product   Name:    MM650
----- Mother Board INFO -----
Mainboard BoardID: 0x0068
Mainboard PCB:    .A
----- FAN Board INFO -----
BC21FIMD  BoardID: 0x0059
BC21FIMD  PCB:    .A
----- PS INFO -----
PS1       Version:  DC: 105 PFC: 104
PS2       Version:  DC: 105 PFC: 104
----- Backplane INFO -----
BC21BKPN  BoardID: 0x0044
BC21BKPN  PCB:    .A
```

NOTE

- **Active iBMC Version:** indicates the active system version.
- **Backup iBMC Version:** indicates the backup system version.

----End

5.10 Viewing HMM Alarm Information

Scenarios

View alarm information of the server.

Impact on the System

This operation has no adverse impact on the system.

Prerequisites

Conditions

No special condition is required for this operation.

Data

Data preparation is not required for this operation.

Procedure

Step 1 Log in to the HMM CLI. For details, see [5.11 Logging In to the Server Over a Network Port by Using PuTTY](#).

Step 2 Run the **ipmcget -d healthevents** in the HMM CLI.

```
iBMC:/->ipmcget -d healthevents
```

Event Num	Event Time	Entity Name	Sensor Name	Alarm level	Event Desc
1	2014-10-10 Friday 11:43:43	PowerSupply1	PS1 Status	Critical	Power Supply input lost(AC/DC)
2	2014-10-10 Friday 11:44:39	MainBoard	Mngmnt Health	Minor	Sensor access degraded or unavailable, Sensor is Power1

----End

5.11 Logging In to the Server Over a Network Port by Using PuTTY

Scenarios

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

Prerequisites

Conditions

The PC is connected to the management network port of the server using a network cable.

Data

The following data is required:

- IP address of the server
- User name and password for logging in to the server

Software

PuTTY.exe (free software)

Procedure

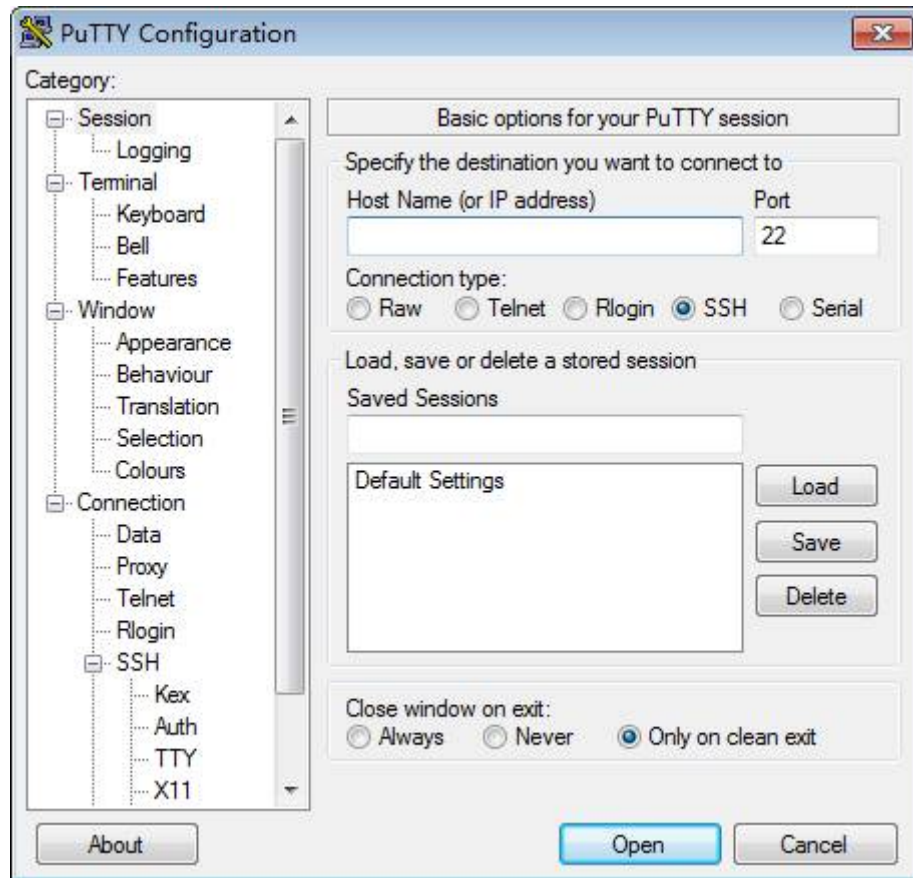
1. Set an IP address and a subnet mask or add route information for the PC, and ensure that the PC can properly communicate with the server.

You can run the **Ping Server IP address** command in the command window of the PC to check the communication between the PC and the server.

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

The **PuTTY Configuration** window is displayed, as shown in [Figure 5-27](#).

Figure 5-27 PuTTY Configuration



3. Set login parameters.

The command-line options are described as follows:

- **Host Name (or IP address):** Enter the IP address of the server, for example, **192.168.2.1**.
- **Port:** Use the default value **22**.
- **Connection type:** Use the default value **SSH**.
- **Close window on exit:** Retain the default value **Only on clean exit**.

NOTE

Configure **Host Name** and **Saved Sessions**, and click **Save**. In future use, you can directly double-click a saved record to log in to the server.

4. Click **Open**.

The **PuTTY** window is displayed.

NOTE

- If it is your first login, the **PuTTY Security Alert** window is displayed. Click **Yes**. Then the **PuTTY** window is displayed.
- If the entered user name is incorrect during server login, the PuTTY must be connected to again.

5. Enter the user name and password.

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

5.12 Transferring Files Using WinSCP

Scenarios

Use WinSCP to transfer files between a PC and a server.

Prerequisites

Conditions

The SFTP service has been enabled on the destination device.

Data

The following data is required:

- IP address of the server to be connected
- User name and password for logging in to the server to be connected

Procedure

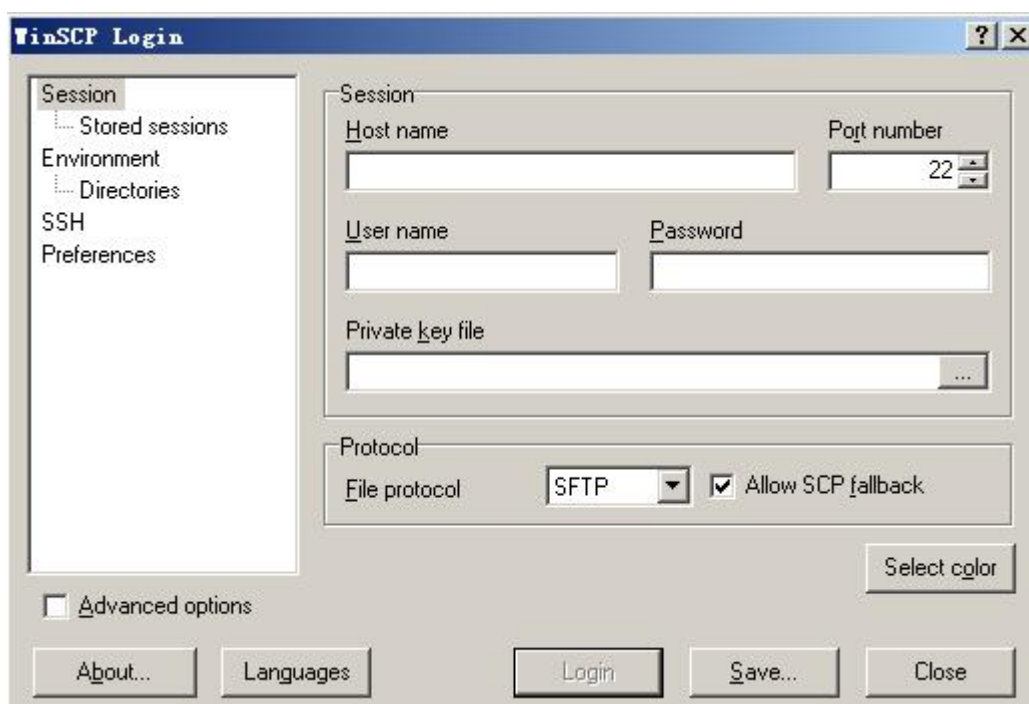
Step 1 Open the **WinSCP** folder, and double-click **WinSCP.exe**.

The **WinSCP Login** dialog box is displayed, as shown in [Figure 5-28](#).

NOTE

You can click **Languages** to select the required system language.

Figure 5-28 WinSCP login



Step 2 Set login parameters.

The parameters are described as follows:

- **Host name:** Enter the IP address of the device to be connected. for example, 191.100.34.32
- **Port number:** Enter the port number. The default value is 22.
- **User name:** Enter the user name. Example: admin123
- **Password:** Enter the password. Example: admin123
- **Private key file:** Retain the default setting, which is empty.
- **File protocol:** Retain the default setting **SFTP**, and select **Allow SCP fallback**.

Step 3 Click **Log In**.

The WinSCP file transfer window is displayed.

 NOTE

- If no private key file is selected during your first login, "Continue connecting and add host key to cache" is displayed. Click **Yes**. Then the WinSCP file transfer page is displayed.
- If Windows 7 is used, **C:\Users\Administrator\Documents** on the local PC is displayed in the left pane and the **/root** directory of the destination device is displayed in the right pane by default.

Step 4 In the left and right panes, create, delete, or copy folders in specific directories as required.

----End

5.13 Logging In to the Management Module CLI Through the Management Network Port

Scenarios

Log in to the management module CLI through the management network port.

Prerequisites

Conditions

The server has been powered on.

Data

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

Software

PuTTY.exe (third-party software)

Procedure

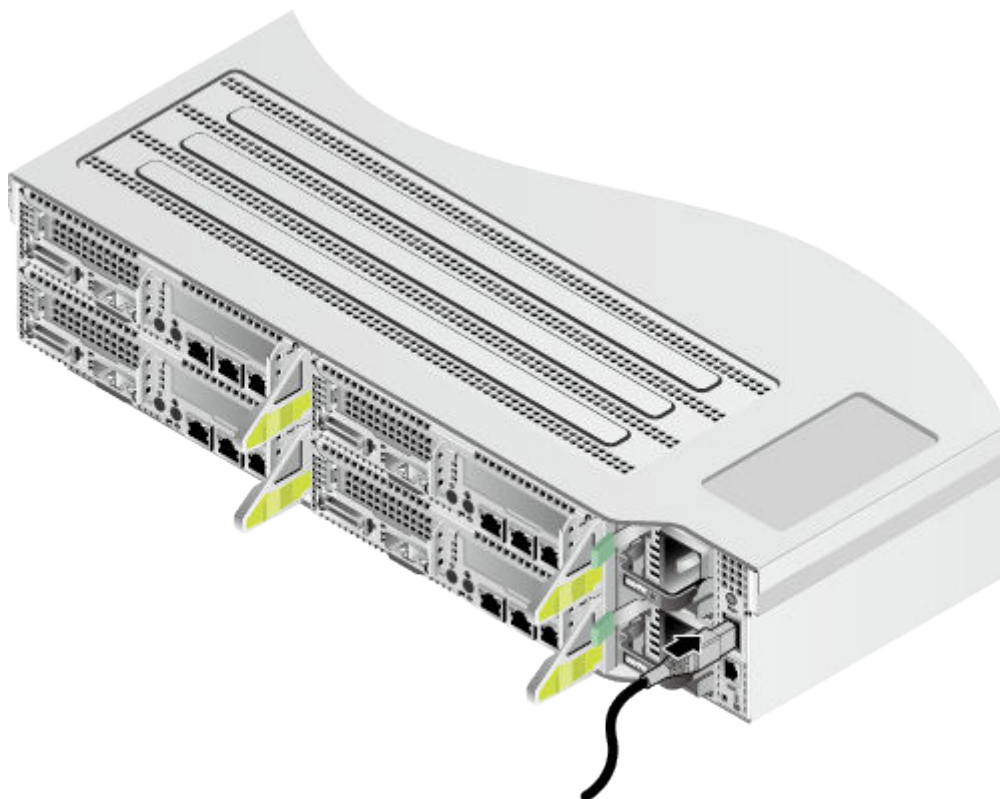
Step 1 Connect the client to the management network port.

1. Connect the client to the management network port on the management module using a network cable, as shown in [Figure 2 Connecting the client to the management network port \(X6000 V3\)](#) or [Figure 5-30](#).

Figure 5-29 Connecting the client to the management network port (X6000 V3)



Figure 5-30 Connecting the client to the management network port (X6000 V5)



Step 2 Set the IP address of the client.

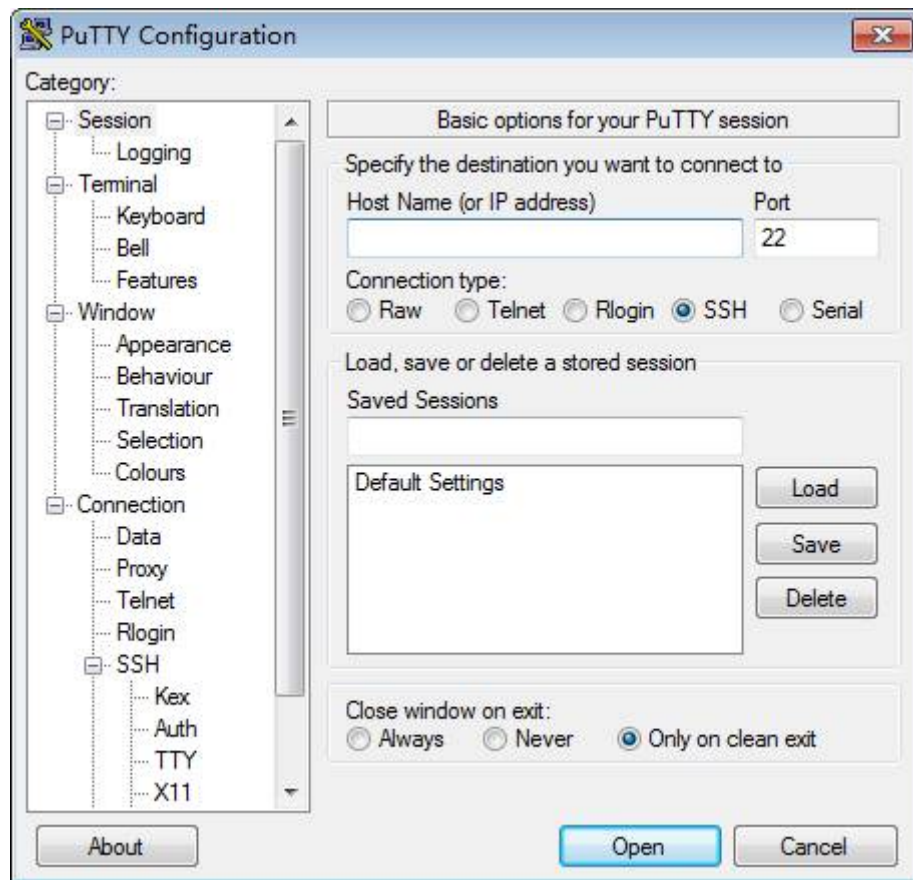
1. Set the IP address, subnet mask, or route of the client to enable the client to interconnect with the management network port.

On the client, choose **Start > Run**, enter **cmd**, and click **OK**. Then, run the **Ping IP address of the aggregated management network port** command to check whether the management network port is reachable.

Step 3 On the client, double-click **PuTTY.exe**.

1. The **PuTTY Configuration** window is displayed, as shown in [Figure 5-31](#).

Figure 5-31 PuTTY Configuration



2. Set the login parameters.

The parameters are described as follows:

- **Host Name (or IP address)**: Enter the IP address of the management network port, for example, **192.168.2.1**.
- **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

After you set **Host Name (or IP address)** and then **Saved Sessions** and click **Save**, you can simply double-click the saved settings under **Saved Sessions** to log in to the server.

3. Click **Open**.

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

NOTE

- If you log in to the server for the first time, the **PuTTY Security Alert** dialog box is displayed. If you trust this site, click **Yes**. The **PuTTY** window is displayed.
- If the entered user name or password is incorrect during server login, PuTTY must be connected again.

4. Enter the user name and password as prompted.

----End

5.14 Logging In to the Management Module CLI Through the Management IP Address of the Server Node

Scenarios

Log in to the management module CLI through the iBMC management IP address on the server node.

Prerequisites

Conditions

The server has been powered on.

Data

- IP address of the iBMC management network port on the server node
- User name and password for logging in to the iBMC of the server node

Software

PuTTY.exe (third-party software)

Procedure

Step 1 Set the IP address of the client.

1. Set the IP address, subnet mask, or route of the client to enable the client to interconnect with the iBMC management network port on the server node.

On the client, choose **Start > Run**, enter **cmd**, and click **OK**. Then, run the **Ping IP address of the aggregated management network port** command to check whether the management network port is reachable.

Step 2 Log in to the iBMC WebUI of the server node.

1. For details, see [5.2 Logging In to the iBMC WebUI](#).

Step 3 Enabling transparent transmission

1. In the navigation tree on the iBMC WebUI of the server node, choose **Configure > Service Settings**.

The **Service Settings** page is displayed.

NOTE

If the iBMC version is earlier than **2.01**, the **Port Settings** page is displayed.

2. Enable **HMM SSH NAT** and set **Port** to **30022**, as shown in [Figure 5-32](#).

Figure 5-32 Enabling transparent transmission

! 开启RMCP或VNC功能会降低系统安全性，请谨慎操作。

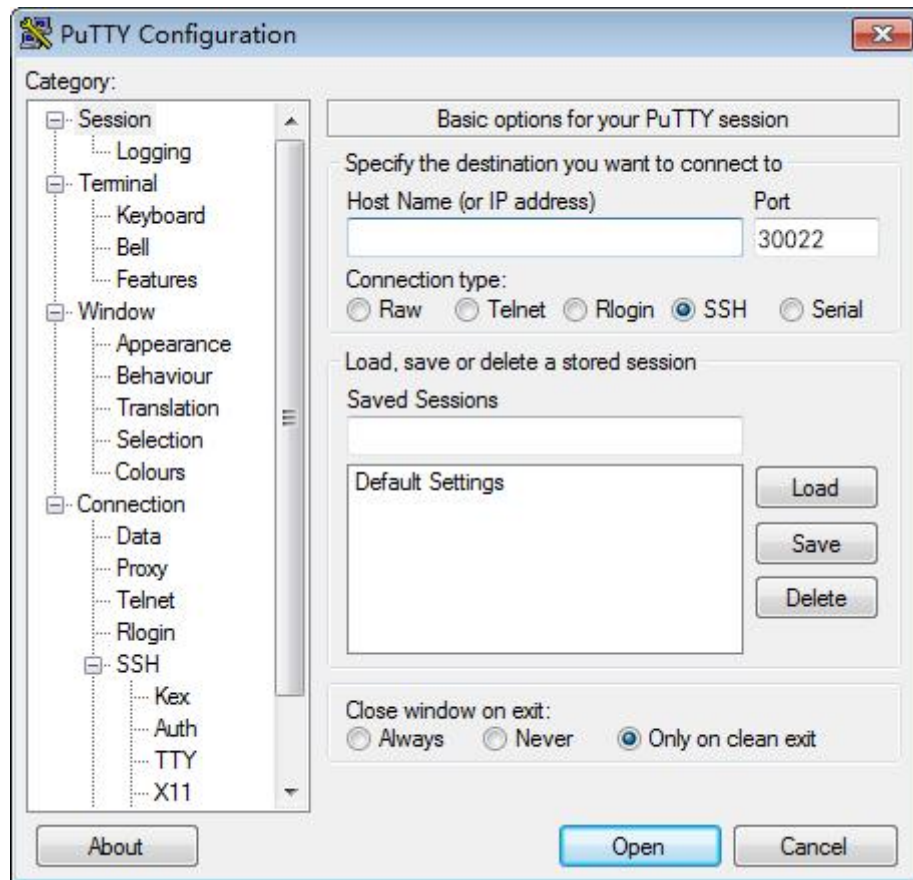
SSH:	☒	Port :	22	恢复默认值
HMM SSH NAT:	☒	Port :	30022	恢复默认值
SNMP Agent:	☒	Port :	161	恢复默认值
KVM:	☒	Port :	2198	恢复默认值
VMM:	☒	Port :	8208	恢复默认值
Video:	☒	Port :	2199	恢复默认值
VNC:	☐	Port :	5900	恢复默认值
Web Server (HTTP):	☒	Port :	80	恢复默认值
Web Server (HTTPS):	☒	Port :	443	恢复默认值
IPMI LAN (RMCP):	☐	Port 1 :	623	恢复默认值
		Port 2 :	664	恢复默认值
IPMI LAN (RMCP+):	☒			

Step 4 Log in to the management module CLI.

1. On the client, double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed, as shown in [Figure 5-33](#).

Figure 5-33 PuTTY Configuration



2. Set the login parameters.

The parameters are described as follows:

- **Host Name (or IP address)**: Enter the IP address of the management network port, for example, **10.10.1.104**.
- **Port**: Retain the default value **30022**.
- **Connection type**: Retain the default value **SSH**.
- **Close window on exit**: Retain the default value **Only on clean exit**.

NOTE

After you set **Host Name (or IP address)** and then **Saved Sessions** and click **Save**, you can simply double-click the saved settings under **Saved Sessions** to log in to the server.

3. Click **Open**.

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

NOTE

- If you log in to the server for the first time, the **PuTTY Security Alert** dialog box is displayed. If you trust this site, click **Yes**. The **PuTTY** window is displayed.
- If the entered user name or password is incorrect during server login, PuTTY must be connected again.

4. Enter the user name and password as prompted.

5. Run the following command to check that **Product Name** is **MM630** or **MM650**, which indicates that the transparent transmission function is configured successfully.

ipmcget -d version

The command output is as follows:

```
iBMC:/->ipmcget -d version
----- iBMC INFO -----
IPMC      CPU:      Hi1710
IPMI      Version:   2.0
CPLD      Version:   (U30)0.02
Active iBMC Version:   (U9)2.80
Active iBMC Build:    001
Active iBMC Built:    22:11:24 Mar 14 2018
Backup iBMC Version:   2.78
SDK        Version:   3.11
SDK        Built:     10:19:29 Mar 9 2018
Active Uboot Version:   2.1.07 (Dec 21 2017 - 18:01:59)
Backup Uboot Version:   2.1.07 (Dec 21 2017 - 18:01:59)
IPMB      Address:    0x10
----- Product INFO -----
Product    ID:      0x0003
Product    Name:    MM650
----- Mother Board INFO -----
Mainboard  BoardID:  0x0068
Mainboard  PCB:    .A
----- FAN Board INFO -----
BC21FIMD   BoardID:  0x0059
BC21FIMD   PCB:    .A
----- PS INFO -----
PS1        Version:   DC: 105 PFC: 104
PS2        Version:   DC: 105 PFC: 104
----- Backplane INFO -----
BC21BKPN   BoardID:  0x0044
BC21BKPN   PCB:    .A
```

----End