FusionCube 1000H, 1000D, Nemo 610, Nemo 620, and Parts 8.2.1

Firmware and Driver Upgrade Guide

Issue 02

Date 2025-08-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Contents

1 Before You Start

1.1 Firmware List

Obtain the firmware list as well as the corresponding software packages and download paths involved in FusionCube. For details, see the corresponding version mapping.

Currently, the *Version Mapping* consists of multiple sheets.

- **Version Mapping**: Includes the software and operating systems used with FusionCube.
- **Hardware Form**: Includes information about server hardware used with FusionCube.
- **Hardware Compatibility**: Includes firmware and driver information of hardware supported by FusionCube.

Firmware is generally involved in upgrade or installation scenarios:

- Firmware of the iBMC, BIOS, CPLD, data cluster modules is involved in upgrade scenarios only.
- Firmware or drivers, such as NICs and disks, in an OS are involved in installation and upgrade scenarios. An installation scenario refers to the scenario where the OS needs to be reinstalled or a driver needs to be reinstalled due to other reasons.

NOTE

- The interfaces, methods, and processes for upgrading firmware of different hardware configurations on the iBMC WebUI are the same. The decompressed ***.hpm** packages are used for upgrade.
- The firmware information varies with the hardware configuration. Download the correct firmware according to the configuration item corresponding to the actual hardware.
- In the *Version Mapping*, ***** in **V***.zip** indicates the firmware version. Replace it with the actual firmware version. For example, if the current iBMC firmware version is 3.00 and the target iBMC firmware version is 3.08, the iBMC firmware package you need to obtain is **2288H V5&5288 V5&2288 V5-iBMC-V308.zip**. For details about how to obtain the firmware packages, consult maintenance personnel.

1.2 Precautions

- You are advised to perform an upgrade during off-peak hours or idle time.
- If alarms exist on the iBMC system before the upgrade, do not perform an upgrade. Instead, contact maintenance engineers to determine whether the alarms affect the upgrade.
- During a firmware upgrade, you are allowed to run upgrade commands but cannot perform any other operations on the iBMC system.
- Upgrade firmware one by one. That is, you can upgrade another piece of firmware only after an upgrade of a piece of firmware completes and takes effect.
- During a firmware upgrade, do not reset the system or iBMC. Power on and off the system as instructed in the guide. If a power supply failure occurs during an upgrade, rectify the fault by following the operations described in **4 Troubleshooting**.
- Do not upgrade the iBMC, BIOS, or CPLD firmware and collect iBMC system logs at the same time.
- If an exception or a failure occurs during an upgrade, contact service or maintenance engineers.
- Before upgrading the RAID controller card firmware, stop service provisioning.
- If possible, upgrade the firmware using SmartKit.
- This document does not apply to the firmware and driver upgrade for the DP2220 server. If you need to upgrade the firmware and driver for the DP2220 server, contact technical support to obtain the firmware and driver upgrade reference document of the DP2220 server.

2 Preparing for the Upgrade

You are advised to check the node firmware and driver versions against the *Version Mapping*. If the firmware and driver versions do not meet the requirements in the version mapping, upgrade the firmware and driver as instructed in related sections.

2.1 Preparing for the Upgrade of iBMC, BIOS, and CPLD

2.1.1 Logging In to the iBMC WebUI

2.1.1.1 Logging In to the iBMC WebUI (iBMC Earlier Than V561)

Scenarios

This section describes how to log in to the iBMC WebUI using a browser on a local PC. The following 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

If the remote control function is required, ensure that the web browser and Java Runtime Environment (JRE) of the required versions have been installed on the local PC. **Table 2-1** lists 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 2-1 Operating environment requirements

OS	Browser	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
	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 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 or later.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	

OS	Browser	JRE
	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 does not meet requirements, obtain it from the official website and install it.

Table 2-2 lists the data to be obtained before performing the operation.

Table 2-2 Data to be obtained

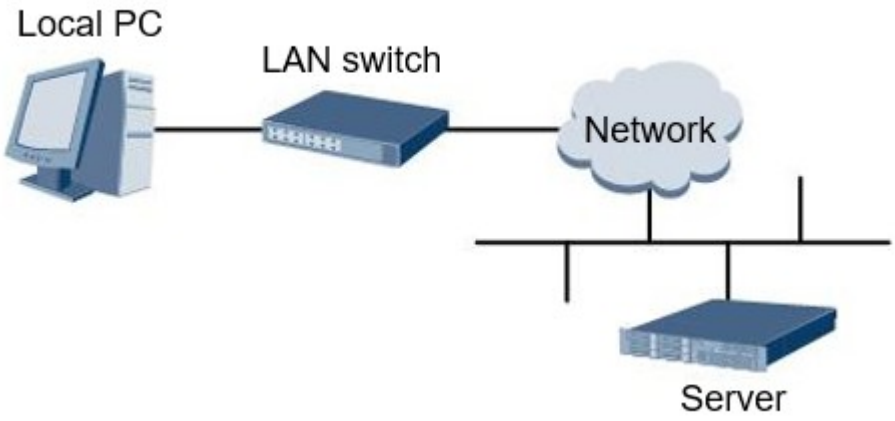
Category	Parameter	Description	Example
User login information	Username	User name for logging in to the iBMC WebUI	• Grantley/Romley/Brickland platform: **root** • Purley/Cedar Island/Whitley platform: **Administrator**
	Password	User password for logging in to the iBMC WebUI	• Grantley/Romley/Brickland 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 using a crossover cable or twisted pair cable.

Figure 2-1 shows the network diagram.

Figure 2-1 Network diagram



Step 2 Open Internet Explorer on the local PC.

Step 3 In the address box, enter the iBMC address in the format of **https://***IP address of the iBMC management network port on the server* (for example, **https://***192.168.2.100*).

Step 4 Press **Enter**.

The iBMC login page is displayed, as shown in Figure 2-2.

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 system displays the **Security Alert** dialog box indicating a certificate error, click **Yes**.

Figure 2-2 iBMC login page

Step 5 On the iBMC login page, enter the user name and password for logging in to the iBMC.

NOTE

The user account will be locked after five consecutive login failures with wrong passwords. In this case, log in again 5 minutes later.

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

Step 7 Click **Log In**.

The home page is displayed. The login username is displayed in the upper right corner of the page.

----End

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

Scenarios

This section describes how to log in to the iBMC WebUI using a browser on a local PC. The following 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

If the remote control function is required, ensure that the web browser and JRE of the required versions have been installed on the local PC. **Table 2-3** lists 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 2-3 Operating environment requirements

OS	Browser	JRE
Windows 7 32-bit Windows 7 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 8 32-bit Windows 8 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 10 64-bit	Internet Explorer 11.0 Microsoft Edge	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 79.0	
	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	

OS	Browser	JRE
	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 does not meet requirements, obtain it from the official website and install it.

Table 2-4 lists the data to be obtained before performing the operation.

Table 2-4 Data to be obtained

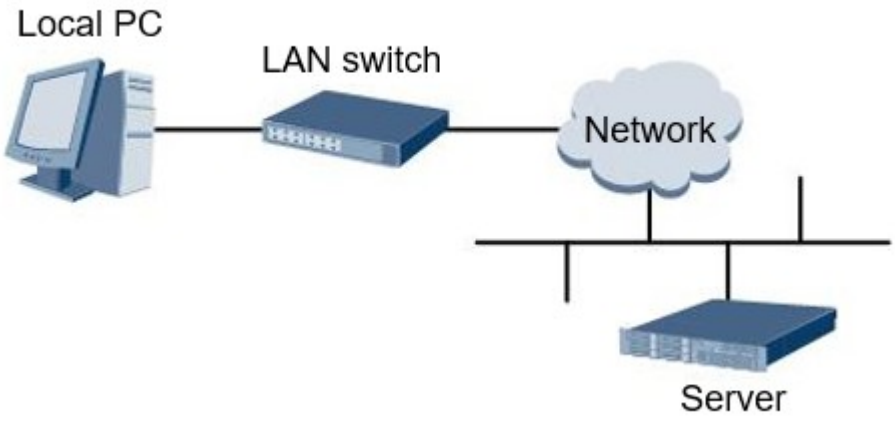
Category	Parameter	Description	Example
User login information	Username	User name for logging in to the iBMC WebUI	• Grantley/Romley/Brickland platform: **root** • Purley/Cedar Island/Whitley platform: **Administrator**
	Password	User password for logging in to the iBMC WebUI	• Grantley/Romley/Brickland 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 using a crossover cable or twisted pair cable.

Figure 2-3 shows the network diagram.

Figure 2-3 Network diagram



Step 2 Open Internet Explorer on the local PC.

Step 3 In the address box, enter the iBMC address in the format of **https://***IP address of the iBMC management network port on the server* (for example, **https://***192.168.2.100*).

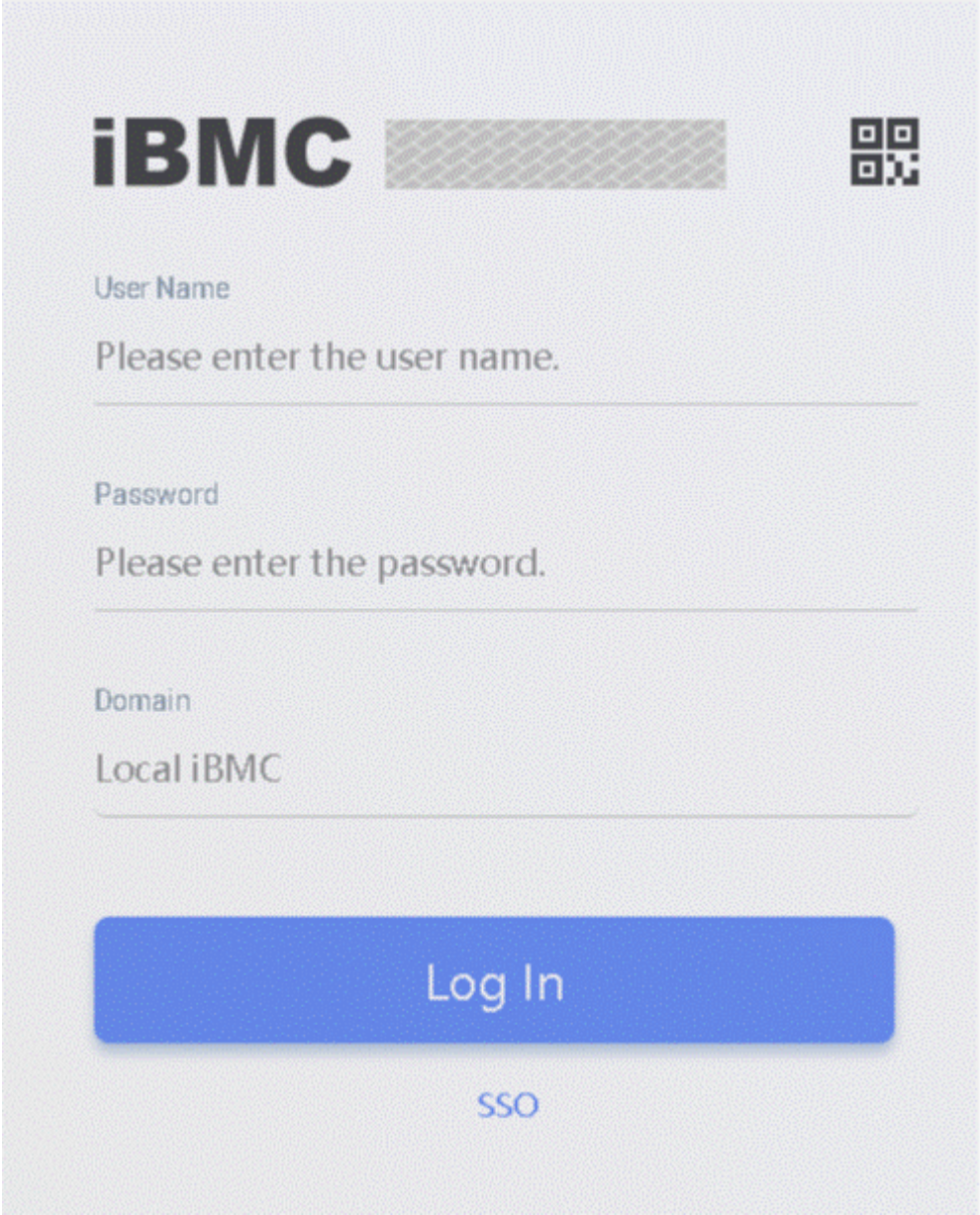
Step 4 Press **Enter**.

The iBMC login page is displayed, as shown in Figure 2-4.

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 system displays the **Security Alert** dialog box indicating a certificate error, click **Yes**.

Figure 2-4 iBMC login page



Step 5 On the iBMC login page, enter the user name and password for logging in to the iBMC.

NOTE

The user account will be locked after five consecutive login failures with wrong passwords. In this case, log in again 5 minutes later.

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

Step 7 Click **Log In**.

The home page is displayed. The login username is displayed in the upper right corner of the page.

----End

2.1.2 Resetting the iBMC

The iBMC system supports the upgrade of the iBMC, BIOS, mainboard CPLD, BBU, BIOS and CPLD of the I/O bridge card and PSUs. The firmware upgrade packages consume the iBMC memory space. To ensure that the iBMC system has abundant memory space during an upgrade, you are advised to reset the iBMC system before upgrading the firmware.

NOTE

You need to reset the iBMC system before upgrading one or multiple pieces of firmware consecutively. Example:

1. If you need to upgrade iBMC, BIOS, and mainboard CPLD, reset the iBMC system only once before the upgrades.
2. If you need to upgrade only the iBMC system instead of other firmware, you also need to reset the iBMC system before the upgrade.
3. The firmware upgrade lists (such as iBMC, BIOS, mainboard CPLD, BBU, I/O board, and I/O board CPLD) supported by different hardware configurations vary. Upgrade the firmware in the firmware list according to the product hardware configuration.

Procedure

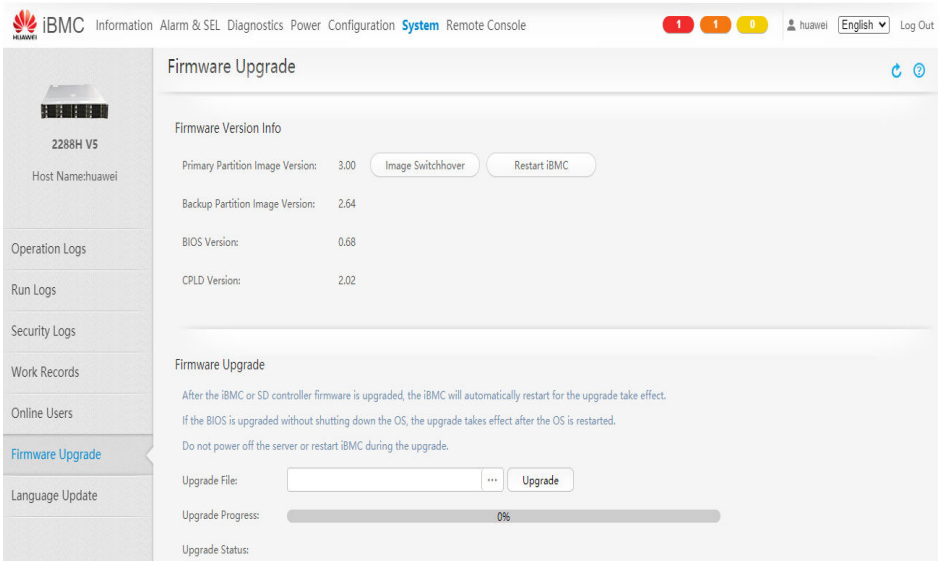
Step 1 Log in to the iBMC WebUI as instructed in **2.1.1 Logging In to the iBMC WebUI**.

Step 2 Choose **iBMC Settings** > **Firmware Upgrade**. On the **Firmware Upgrade** page that is displayed, click **Restart iBMC**. In the dialog box that is displayed, click **Yes**.

- If the iBMC version is earlier than V561, choose **System** > **Firmware Upgrade** on the iBMC WebUI.

  The **Firmware Upgrade** page is displayed, as shown in **Figure 2-5**.

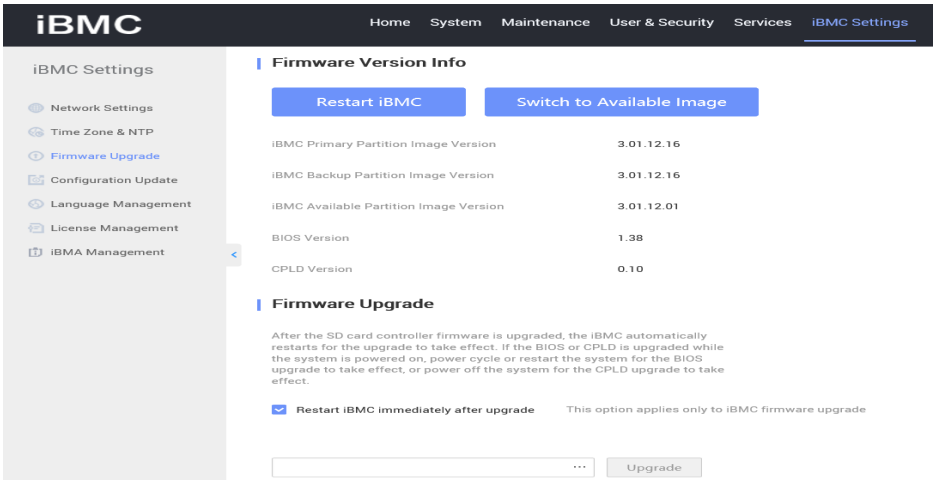
  Figure 2-5 iBMC WebUI (iBMC version earlier than V561)



- If the iBMC version is V561 or later or the iBMC version is in the *x.xx.xx.xx* format, choose **iBMC Settings** > **Firmware Upgrade** on the iBMC WebUI.

  The **Firmware Upgrade** page is displayed, as shown in **Figure 2-6**.

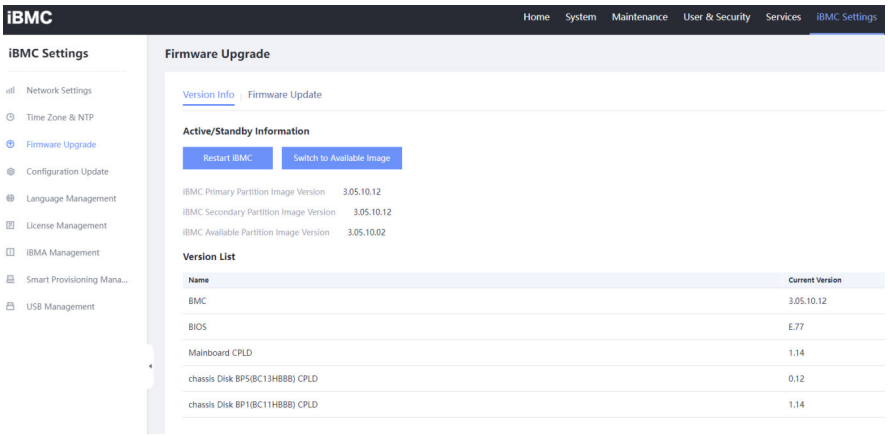
Figure 2-6 iBMC WebUI (iBMC V561 or later or iBMC *x.xx.xx.xx*)



- If the iBMC version is 3.05.00.00 or later, choose **iBMC Settings** > **Firmware Upgrade**.

  The **Firmware Upgrade** page is displayed, as shown in **Figure 2-7**.

Figure 2-7 iBMC WebUI (iBMC 3.05.00.00 or later)



Step 3 Log out of the iBMC WebUI. The iBMC will be reset. The reset takes about 3 minutes. After the iBMC is successfully reset, log in to the iBMC WebUI again and perform subsequent operations.

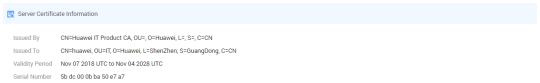
----End

2.1.3 Preparing for the iBMC Upgrade

2.1.3.1 Performing a Pre-upgrade Check

Before the upgrade, check the items listed in **Table 2-5** in sequence and record the check results.

Table 2-5 Pre-upgrade checklist

No.	Item	Operations and Criteria
1	Software version	**NOTE** 1. Query and record the current iBMC software version of the server in the system. 2. Determine the target version.
2	System status	**NOTICE** Check the iBMC system. • If no alarm exists, perform the upgrade. • If any alarm exists, contact Huawei technical support.
3	SSL certificate status	**CAUTION** Check whether the certificate validity period is from Nov 07 2018 UTC to Nov 04 2028 UTC, as shown in **Figure 2-8**. If yes, **import the iBMC SSL certificate** before the upgrade. Otherwise, the iBMC web service and the Redfish service cannot be used after the upgrade. **Figure 2-8** Default BMC certificate information 

Checking the Software Version

1. Log in to the iBMC WebUI.

   For details, see **2.1.1 Logging In to the iBMC WebUI**.

2. Query the iBMC version.
   - If the iBMC version is earlier than V561, choose **Information** > **System Info** > **Product Info** > **Mainboard Info** on the iBMC WebUI.

     Query the current iBMC firmware version on the page that is displayed.
   - If the iBMC version is V561 or later or in the *x.xx.xx.xx* format, choose **System** > **System Info** > **Product Info** > **Mainboard Info** on the iBMC WebUI.

     Query the current iBMC firmware version on the page that is displayed.

2.1.3.2 Obtaining the Software Package

Step 1 Download the version mapping of the desired version (for example, *FusionCube 1000H 8.2.1 Version Mapping (Virtualization) 01*) from the Huawei Support website and open it.

Step 2 Click the **Hardware Compatibility** sheet in the version mapping.

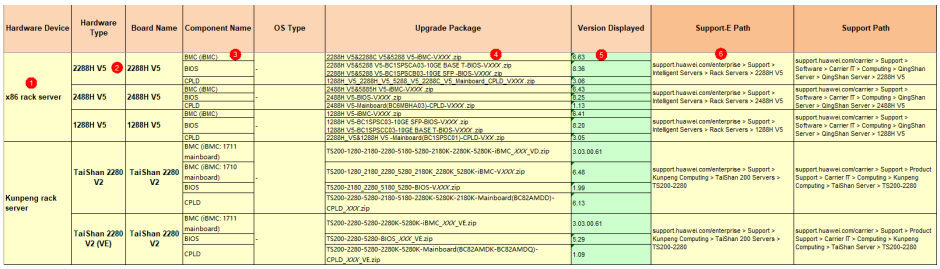
Step 3 Locate the row that contains the iBMC firmware based on the hardware device, hardware type, BMC (iBMC), upgrade package name, and displayed version.

Step 4 Find the target firmware version in the **Version Displayed** column of the row located in **Step 3**.

Step 5 Visit the download address of the desired firmware from the **Support-E Path** or **Support Path** column of the row located in **Step 3**, download the upgrade package and digital signature file to the client (local PC), and decompress the upgrade package.

Figure 2-9 shows an example path of finding firmware: x86 rack server > 2288H V5 > BMC (iBMC) > version number (6.63), software package name, and download link in the corresponding row.

Figure 2-9 Locating the desired iBMC in the version mapping



Hardware Device	Hardware Type	Board Name	Component Name	OS Type	Upgrade Package	Version Displayed	Support-E Path	Support Path
x86 rack server	2288H V5	2288H V5	BMC (iBMC)	-	2288H V5&2288C V5&5288 V5-iBMC-VXXX.zip	6.63	support.huawei.com/enterprise > Support > Intelligent Servers > Rack Servers > 2288H V5	support.huawei.com/carrier > Support > Software > Carrier IT > Computing > QingShan Server > QingShan Server > 2288H V5
			BIOS		2288H V5&5288 V5-BC1SPSCA03-10GE BASE T-BIOS-VXXX.zip	6.36		
			CPLD		2288H V5&5288 V5-BC1SPSCB03-10GE SFP-BIOS-VXXX.zip	3.06		
	2488H V5	2488H V5	BMC (iBMC)	-	1288H_V5_2288H_V5_5288_V5_2288C_V5_Mainboard_CPLD_VXXX.zip	6.43	support.huawei.com/enterprise > Support > Intelligent Servers > Rack Servers > 2488H V5	support.huawei.com/carrier > Support > Software > Carrier IT > Computing > QingShan Server > QingShan Server > 2488H V5
			BIOS		2488H V5&5885H V5-iBMC-VXXX.zip	6.25		
			CPLD		2488H V5-BIOS-VXXX.zip	6.13		
	1288H V5	1288H V5	BMC (iBMC)	-	2488H V5-Mainboard(BC6M8HA03)-CPLD-VXXX.zip	6.41	support.huawei.com/enterprise > Support > Intelligent Servers > Rack Servers > 1288H V5	support.huawei.com/carrier > Support > Software > Carrier IT > Computing > QingShan Server > 1288H V5
			BIOS		1288H V5-BMC-VXXX.zip	6.20		
			CPLD		1288H V5-BC1SPSC03-10GE SFP-BIOS-VXXX.zip	3.05		
Kunpeng rack server	TaiShan 2280 V2	TaiShan 2280 V2	BMC (iBMC: 1711 mainboard)	-	1288H V5-BC1SPSC01-10GE BASE T-BIOS-VXXX.zip	3.03.00.61	support.huawei.com/enterprise > Support > Kunpeng Computing > TaiShan 200 Servers > TS200-2280	support.huawei.com/carrier > Support > Product Support > Carrier IT > Computing > Kunpeng Computing > TaiShan Server > TS200-2280
			BMC (iBMC: 1710 mainboard)		2288H_V5&1288H V5 -Mainboard(BC1SPSC01)-CPLD-VXX.zip	6.48		
			BIOS		TS200-1280-2180-2280-5180-5280-2180K-2280K-5280K-iBMC_XXX_VD.zip	1.99		
			CPLD		TS200-2180_2280_5180_5280-BIOS-VXXX.zip	6.13		
	TaiShan 2280 V2 (VE)	TaiShan 2280 V2	BMC (iBMC: 1711 mainboard)	-	TS200-2280-5280-2180-5180-2280K-5280K-2180K-Mainboard(BC82AMDD)-CPLD_XXX.zip	3.03.00.61	support.huawei.com/enterprise > Support > Kunpeng Computing > TaiShan 200 Servers > TS200-2280	support.huawei.com/carrier > Support > Product Support > Carrier IT > Computing > Kunpeng Computing > TaiShan Server > TS200-2280
			BIOS		TS200-2280-5280-2180K-5280K-iBMC_XXX_VE.zip	5.29		
			CPLD		TS200-2280-5280-2280K-5280K-Mainboard(BC82AMDK-BC82AMDQ)-CPLD_XXX_VE.zip	1.09		

NOTE

To obtain the iBMC firmware of other third-party servers, contact the official team of the servers.

----End

2.1.3.3 Verifying the Software Package Digital Signature

To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification when downloading the software package.

After the software package is downloaded from the support website, verify its PGP digital signature according to the *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use the software package, and contact Huawei technical support engineers.

Before a software package is used in installation or upgrade, 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.

2.1.4 Preparing for the BIOS Upgrade

2.1.4.1 Performing a Pre-upgrade Check

Before the upgrade, check the items listed in **Table 2-6** and record the check results.

Table 2-6 Pre-upgrade checklist

Item	Operations and Criteria
Software version	1. Query and record the current software version of the server BIOS in the system. 2. Determine the target version.
System status	Check the iBMC system. • If no alarm exists, perform the upgrade. • If any alarm exists, contact Huawei technical support.

Checking the Software Version

1. Log in to the iBMC WebUI.
   For details, see **2.1.1 Logging In to the iBMC WebUI**.
2. Query the BIOS version of the mainboard.
   – If the iBMC version is earlier than V561, choose **Information** > **System Info** > **Product Info** > **Mainboard Info** on the iBMC WebUI.
   Query the current BIOS version on the page that is displayed.
   – If the iBMC version is V561 or later or in the *x.xx.xx.xx* format, choose **System** > **System Info** > **Product Info** > **Mainboard Info** on the iBMC WebUI.
   Query the current BIOS version on the page that is displayed.

2.1.4.2 Obtaining the Software Package

Step 1 Download the version mapping of the desired version (for example, *FusionCube 1000H 8.2.1 Version Mapping (Virtualization) 01*) from the Huawei Support website and open it.

Step 2 Click the **Hardware Compatibility** sheet in the version mapping.

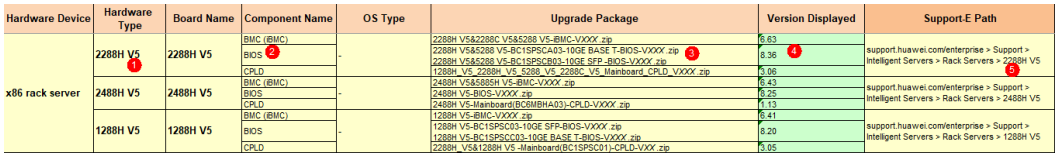
Step 3 Locate the row that contains the BIOS firmware based on the hardware device, hardware type, BIOS, upgrade package name, and displayed version.

Step 4 Find the target firmware version in the **Version Displayed** column of the row located in **Step 3**.

Step 5 Visit the download address of the desired firmware from the **Support-E Path** or **Support Path** column of the row located in **Step 3**, download the upgrade package and digital signature file to the client (local PC), and decompress the upgrade package.

Figure 2-10 shows an example path of finding the firmware: x86 rack server > 2288H V5 > BIOS > version number (8.36) and download link in the corresponding row.

Figure 2-10 Locating the desired BIOS in the version mapping



NOTE

To obtain the BIOS firmware of other third-party servers, contact the official team of the servers.

----End

2.1.4.3 Verifying the Software Package Digital Signature

To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification when downloading the software package.

After the software package is downloaded from the support website, verify its PGP digital signature according to the *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use the software package, and contact Huawei technical support engineers.

Before a software package is used in installation or upgrade, 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.

2.1.5 Preparing for the Mainboard CPLD Upgrade

2.1.5.1 Performing a Pre-upgrade Check

Before the upgrade, check the items listed in **Table 2-7** and record the check results.

Table 2-7 Pre-upgrade checklist

Item	Operations and Criteria
Software version	1. Query and record the current software version of the server mainboard CPLD in the system. 2. Determine the target version.
System status	Check the iBMC system. • If no alarm exists, perform the upgrade. • If any alarm exists, contact Huawei technical support.

Checking the Software Version

1. Log in to the iBMC WebUI.

   For details, see **2.1.1 Logging In to the iBMC WebUI**.
2. Query the mainboard CPLD version.
   - If the iBMC version is earlier than V561, choose **Information** > **System Info** > **Product Info** > **Mainboard Info** on the iBMC WebUI.

     Query the current CPLD version on the page that is displayed.

– If the iBMC version is V561 or later or in the *x.xx.xx.xx* format, choose **System** > **System Info** > **Product Info** > **Mainboard Info** on the iBMC WebUI.

  Query the current CPLD version on the page that is displayed.

2.1.5.2 Obtaining the Software Package

Step 1 Download the version mapping of the desired version (for example, *FusionCube 1000H 8.2.1 Version Mapping (Virtualization) 01*) from the Huawei Support website and open it.

Step 2 Click the **Hardware Compatibility** sheet in the version mapping.

Step 3 Locate the row that contains the mainboard CPLD firmware based on the hardware device, hardware type, CPLD, upgrade package name, and displayed version.

Step 4 Find the target firmware version in the **Version Displayed** column of the row located in **Step 3**.

Step 5 Visit the download address of the desired firmware from the **Support-E Path** or **Support Path** column of the row located in **Step 3**, download the upgrade package and digital signature file to the client (local PC), and decompress the upgrade package.

Figure 2-11 shows an example path of finding the firmware: x86 rack server > 2288H V5 > CPLD > version number (3.06) and download link in the corresponding row.

Figure 2-11 Locating the desired mainboard CPLD in the version mapping

Hardware Device	Hardware Type	Board Name	Component Name	OS Type	Upgrade Package	Version Displayed	Support-E Path
x86 rack server	2288H V5 ①	2288H V5	BMC (iBMC)	-	2288H V5&2288C V5&5288 V5-iBMC-VXXX.zip	6.83	support.huawei.com/enterprise > Support > Intelligent Servers > Rack Servers > 2288H V5
			BIOS		2288H V5&5288 V5-BC1SPSCA03-10GE BASE T-BIOS-VXXX.zip 2288H V5&5288 V5-BC1SPSCB03-10GE SFP -BIOS-VXXX.zip	8.36	
			CPLD ②		1288H_V5_2288H_V5_5288_V5_2288C_V5_Mainboard_CPLD_VXXX.zip ③	3.06 ④	⑤
	2488H V5	2488H V5	BMC (iBMC)	-	2488H V5&5885H V5-iBMC-VXXX.zip	6.43	support.huawei.com/enterprise > Support > Intelligent Servers > Rack Servers > 2488H V5
			BIOS		2488H V5-BIOS-VXXX.zip	5.25	
			CPLD		2488H V5-Mainboard(BC6MBHA03)-CPLD-VXXX.zip	1.13	
	1288H V5	1288H V5	BMC (iBMC)	-	1288H V5-iBMC-VXXX.zip	6.41	support.huawei.com/enterprise > Support > Intelligent Servers > Rack Servers > 1288H V5
			BIOS		1288H V5-BC1SPSC03-10GE SFP-BIOS-VXXX.zip 1288H V5-BC1SPSC03-10GE BASE T-BIOS-VXXX.zip	8.20	
			CPLD		2288H_V5&1288H V5 -Mainboard(BC1SPSC01)-CPLD-VXX.zip	3.05	

NOTE

To obtain the CPLD firmware of other third-party servers, contact the official team of the servers.

----End

2.1.5.3 Verifying the Software Package Digital Signature

To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification when downloading the software package.

After the software package is downloaded from the support website, verify its PGP digital signature according to the *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use the software package, and contact Huawei technical support engineers.

Before a software package is used in installation or upgrade, 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.

2.2 Preparing for the RAID Controller Card Driver or Firmware Upgrade

Before upgrading the driver or firmware, you need to query the current version to check whether an upgrade is required.

2.2.1 Querying the Node OS Architecture and Version

Step 1 Log in to the target node.

1. Use PuTTY to log in to the node.
   - Host name: *Management IP address of the node*
   - Default username: **manageromm**
   - Default password: *User-defined public password*
2. Switch to user **root**.
   a. Run the following command:
   ```
   su - root
   ```
   b. Enter the password of user **root** as prompted. The default password is the user-defined public password.

Step 2 Run the **uname -r** command to obtain the OS architecture and version and record the information.

```
[root@MCNA01]# uname -r
5.10.0-136.12.0.86.h1687.eulerosv2r12.x86_64
```

In the preceding example, the EulerOS version is V2R12 and the OS architecture is x86_64.

----End

2.2.2 Querying the Node RAID Controller Card Driver or Firmware Version

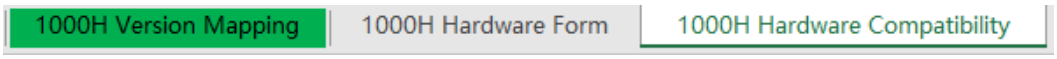
Step 1 Query the RAID controller card model of the target node as instructed in **3.3.7 Installing/Upgrading the RAID Controller Card Firmware and Driver**, and then record the model.

Step 2 Query the driver or firmware version of the preceding RAID controller card on the target node. For details, see **3.3.7 Installing/Upgrading the RAID Controller Card Firmware and Driver**. After the query, record the version.

----End

2.2.3 Querying the Version of the RAID Controller Card Driver or Firmware

Step 1 Open the specific version mapping and click the **Hardware Compatibility** sheet in the lower right corner.



Step 2 Based on the OS architecture and RAID controller card model, find the driver or firmware version in the **Version Displayed** column and record the version number. The download link of the driver or firmware package is displayed in the **Support-E Path** or **Support Path** column. If you need to upgrade the driver or firmware, obtain the driver or firmware package based on the path.

Hardware Device	Hardware Type	Board Name	Component Name	OS Type	Upgrade Package	Version Displayed	Support-E Path
Avago SAS3508 1	3508	3508	Firmware	-	PANGEA_V600R008C10_RAID-FW-3508-5.140.00-3515.*.zip	5.140.00-3515	support.huawei.com/enterprise > Support > Management Software > iDriver > FusionServer iDriver > FusionServer iDriver 3.0.34
			Driver	UOS	Integrated into the FusionCube driver	07.722.02.00	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	RHEL 7.6	Integrated into the FusionCube driver	4.7-3.2.9.0	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	RHEL 7.9	Integrated into the FusionCube driver	5.1-2.3.7.1	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	RHEL 8.4	Integrated into the FusionCube driver	07.714.04.00	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	RHEL 8.6	Integrated into the FusionCube driver	07.719.03.00	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	RHEL 9.0	Integrated into the FusionCube driver	07.719.03.00	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	RHEL 9.2	Integrated into the FusionCube driver	07.719.03.00	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H
			Driver	UVP 2	Integrated into the FusionCube driver (RAID-Driver-Eulerv2r12-megaraid_sas-07.723.02.00.x86_64.rpm) 3	07.723.02.00 4	support.huawei.com/enterprise > Support > Distributed Storage > FusionCube > FusionCube 1000H 5

----End

2.2.4 Determining Whether to Upgrade the Driver or Firmware After Version Comparison

Step 1 Compare the RAID controller card driver or firmware version queried on the target node with that in the version mapping.

Step 2 If there is any inconsistency, upgrade the driver or firmware as instructed in **3.3.7 Installing/Upgrading the RAID Controller Card Firmware and Driver**.

If there is no inconsistency, no upgrade is required.

----End

2.3 Preparing for the NIC Upgrade

2.3.1 Querying the Node OS Architecture and NIC Firmware or Driver Version

Step 1 Log in to the target node.

1. Use PuTTY to log in to the node.
   - Host name: *Management IP address of the node*
   - Default username: **manageromm**
   - Default password: *User-defined public password*
2. Switch to user **root**.
   a. Run the following command:
   ```
   su - root
   ```
   b. Enter the password of user **root** as prompted. The default password is the user-defined public password.

Step 2 Run the **cat /etc/os-release** command to obtain and record the OS type and version.

```
[root@MCNA01 ]# cat /etc/os-release
NAME="EulerOS"
VERSION="2.0 (SP12x86_64)"
ID="euleros"
VERSION_ID="2.0"
PRETTY_NAME="EulerOS 2.0 (SP12x86_64)"
ANSI_COLOR="0;31"
```

In the preceding example, the OS type is EulerOS and the OS architecture is x86_64.

Step 3 Run the **ethtool -i** *<Network port name>* command to query the driver and firmware versions of the network port.

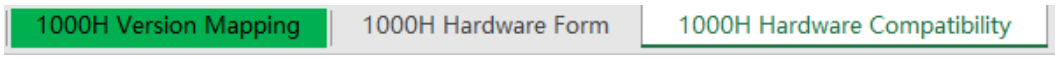
```
[root@MCNA01 ]# ethtool -i eno3np0
driver: mlx5_core
version: 5.0-0 - HW:2.0
firmware-version: 14.32.1010 (HUA0000000026)
expansion-rom-version:
bus-info: 0000:ca:00.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: yes
```

In the preceding example, the driver version is 5.0-0 and the firmware version is 14.32.1010.

----End

2.3.2 Querying the NIC Driver or Firmware Version

Step 1 Open the specific version mapping and click the **Hardware Compatibility** sheet in the lower right corner.



Step 2 Find and record the driver or firmware version in the **Version Displayed** column based on the OS version and server type of the target node. The following figure shows an example.

Hardware Device	Hardware Type	Board Name	Component Name	OS Type	Upgrade Package	Version Displayed	Support-E Path
SP380	SP380 1	ConnectX-4	Firmware 2	-	NIC-SP380-CX4Lx-FW-*XXX*.zip	14.32.1010 3	support.huawei.com/enterprise > Support > Management Software > iDriver > FusionServer iDriver
			Driver	RHEL 7.6	MLNX_OFED_LINUX-4.7-3.2.9.0-rhel7.6-x86_64.tgz	4.7-3.2.9	http://content.mellanox.com/ofed/MLNX_OFED-4.7-3.2.9.0/MLNX_OFED_LINUX-4.7-3.2.9.0-rhel7.6-x86_64.tgz
				RHEL 8.4	MLNX_OFED_LINUX-5.7-1.0.2.0-rhel8.4-x86_64.tgz	5.7-1.0.2.0	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				RHEL 8.6	MLNX_OFED_LINUX-5.7-1.0.2.0-rhel8.6-x86_64.tgz	5.7-1.0.2.0	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				RHEL 9.0	MLNX_OFED_LINUX-5.7-1.0.2.0-rhel9.0-x86_64.tgz	5.7-1.0.2.0	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				RHEL 9.2	MLNX_OFED_LINUX-23.04-1.1.3.0-rhel9.2-x86_64.tgz	23.04-1.1.3.0	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				UOS	MLNX_OFED_LINUX-5.7-1.0.2.0-uos20.1020-aarch64.tgz MLNX_OFED_LINUX-5.7-1.0.2.0-uos20.1020-x86_64.tgz	5.7-1.0.2.0	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				Kylin SP2	MLNX_OFED_LINUX-5.7-1.0.2.0-kylin10sp2-aarch64.tgz	5.7-1.0.2.0	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				Kylin SP3	MLNX_OFED_LINUX-23.04-0.5.3.3-kylin10sp3-aarch64.tgz	23.04-0.5.3.3	https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/
				RHEL 7.9	MLNX_OFED_LINUX-5.1-2.3.7.1-rhel7.9-x86_64.tgz	5.1-2.3.7	http://content.mellanox.com/ofed/MLNX_OFED-5.1-2.3.7.1/MLNX_OFED_LINUX-5.1-2.3.7.1-rhel7.9-x86_64.tgz
				EulerOS 4	OceanStor-Pacific_8.2.0.RC1_Driver-RDMA_aarch64.zip OceanStor-Pacific_8.2.0.RC1_Driver-RDMA_x86-64.zip	5.0-0 5	support.huawei.com/enterprise > Support > Software Download > Distributed Storage > OceanStor Pacific Series > OceanStor Pacific

----End

2.3.3 Determining Whether to Upgrade the Driver or Firmware After Version Comparison

Step 1 Compare the NIC driver or firmware version queried on the target node with that in the version mapping.

Step 2 If there is any inconsistency, upgrade the driver or firmware as instructed in **3.3.9 Installing/Upgrading the NIC Firmware and Driver**.

If there is no inconsistency, no upgrade is required.

----End

2.4 Software Package Digital Signature Verification

To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification when downloading the software package.

After the software package is downloaded, verify its PGP digital signature according to the *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use the software package, and contact Huawei technical support.

Before a software package is used in installation or upgrade, 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.

- Carrier users: **https://support.huawei.com/carrier/digitalSignatureAction**
- Enterprise users: **https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054**

3 Installing/Upgrading the Firmware and Driver

3.1 Upgrade Impact

CAUTION

1. After the firmware or driver of a single node is successfully upgraded, the BMC or server OS needs to be restarted or the server needs a power cycle for the upgrade to take effect. This may result in service unavailability on the current node for a short period of time.
2. If the firmware of multiple nodes is manually upgraded at the same time, services may be interrupted. Contact technical support engineers to determine the upgrade scheme and then perform the upgrade.

Accommodating the upgrade impact, the overall upgrade process for the firmware or driver is as follows:

Step 1 Enter the maintenance mode.

NOTICE

Perform this step only when the node to be upgraded has been added to a storage pool.

- Enter the maintenance mode using DeviceManager:
  a. Log in to DeviceManager.

b. Choose **Cluster** > **Cluster** > **Hardware**. The hardware page is displayed.
c. In the **Nodes** list, locate the faulty node and choose **More** > **Set Maintenance Mode**.

- Enter the maintenance mode using a command:

  Use the SSH tool to log in to the management node as user **fsadmin**. Run the **minisystem** command and enter the password of user **root** to go to the minisystem view. Run the following command to switch the faulty node to the maintenance mode. To run the following command, enter the name and password of CLI super administrator **admin** as prompted.

  ```
  dswareTool.sh --op setServerStorageMode -ip Management IP address of the faulty node -mode 1
  ```

Step 2 Upgrade the firmware and drivers node by node according to the upgrade guide.

Step 3 Exit the maintenance mode after the firmware and drivers are successfully upgraded and take effect.

NOTICE

Perform this step only when the node to be upgraded has been added to a storage pool.

- Exit the maintenance mode using DeviceManager:
  a. Log in to DeviceManager.
  b. Choose **Cluster** > **Cluster** > **Hardware**. The hardware page is displayed.
  c. In the **Nodes** list, locate the faulty node and choose **More** > **Cancel Maintenance Mode**.
- Exit the maintenance mode using a command:

  Use the SSH tool to log in to the management node as user **fsadmin**. Run the **minisystem** command and enter the password of user **root** to go to the minisystem view. Run the following command to switch the faulty node to the normal mode. To run the following command, enter the name and password of CLI super administrator **admin** as prompted.

  ```
  dswareTool.sh --op setServerStorageMode -ip Faulty node's internal management IP address -mode 0
  ```

Step 4 Check the system status.

On SmartKit, choose **Home** > **Storage** > **Routine Maintenance** > **More** > **Inspection** to check the system status.

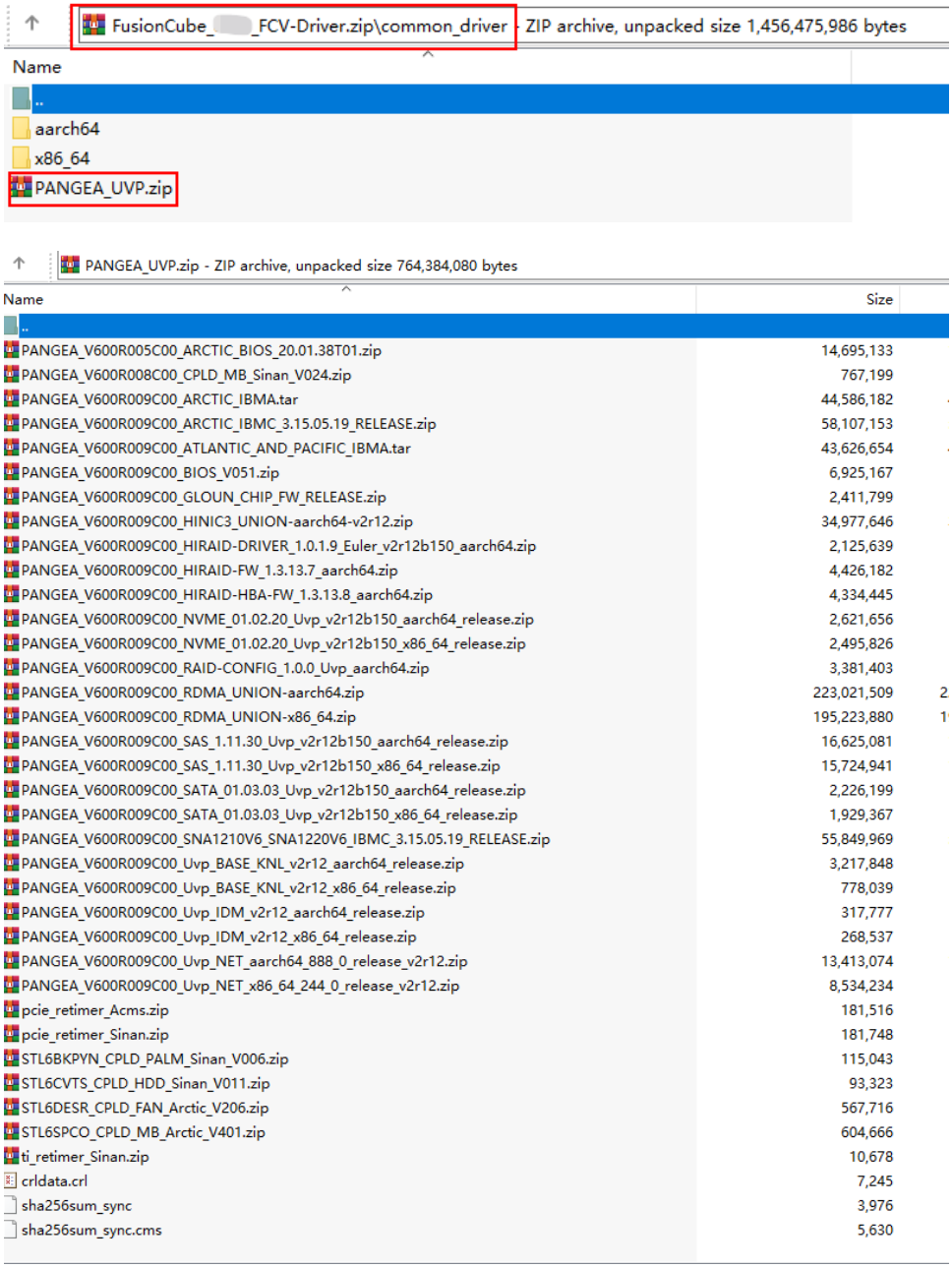
- If all inspection items are passed, the inspection is successful.
- If any inspection item fails, the inspection fails. In this case, rectify the faults by performing the recommended actions in the inspection reports. Perform the inspection again after fault rectification. If the inspection still fails, contact technical support.

----End

3.2 Obtaining the Card Firmware/Driver Package

Obtain the card firmware/driver package based on the version mapping table. If the firmware path contains **PANGEA_UVP.zip**, download the

FusionCube_*version*_**FCV-Driver.zip** package, obtain **PANGEA_UVP.zip** from the **FusionCube**_*version*_**FCV-Driver.zip/common_driver** directory, and decompress **PANGEA_UVP.zip** to obtain the corresponding firmware/driver package. The following figures show an example.



3.3 Manually Installing/Upgrading the Firmware and Driver

3.3.1 Upgrading the iBMC Firmware

3.3.1.1 Preparing for the Upgrade

3.3.1.1.1 Decompressing the iBMC Firmware Package

Upload the iBMC firmware package to a specified directory on the local PC and decompress the package. For details about how to obtain the firmware package, see **2 Preparing for the Upgrade**. **Figure 3-1** shows the files extracted from the firmware package. The firmware package contains two files, as described in **Table 3-1**.

Figure 3-1 Files in the iBMC firmware package

Table 3-1 Files extracted from the iBMC firmware package

File Name	Description
rootfs_PangeaV6_Atlantic.hpm	iBMC firmware.
version.xml	Version configuration table.

NOTE

- The iBMC firmware name varies with the hardware configuration. The actual firmware name is used. The upgrade process is the same regardless of the firmware name.
- The firmware package varies slightly with the hardware configuration. For details, see the product documentation. If you have any questions, contact the maintenance personnel.

3.3.1.1.2 Checking Versions

Check the version of the two partition images of iBMC and the version in the **version.xml** file. If the versions are different, an upgrade is necessary. To check the versions, perform the following operations.

Procedure

Step 1 Log in to the iBMC WebUI and access the **Firmware Upgrade** page. For iBMC 3.01.*x.x*, choose **iBMC Settings** > **Firmware Upgrade**. For iBMC 3.09.00.*x* or later, choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Update**. The **Firmware Upgrade** page is displayed. The following figures show the iBMC WebUIs of different versions.

Figure 3-2 Querying the iBMC firmware version on the iBMC WebUI (3.01.08.*x*)

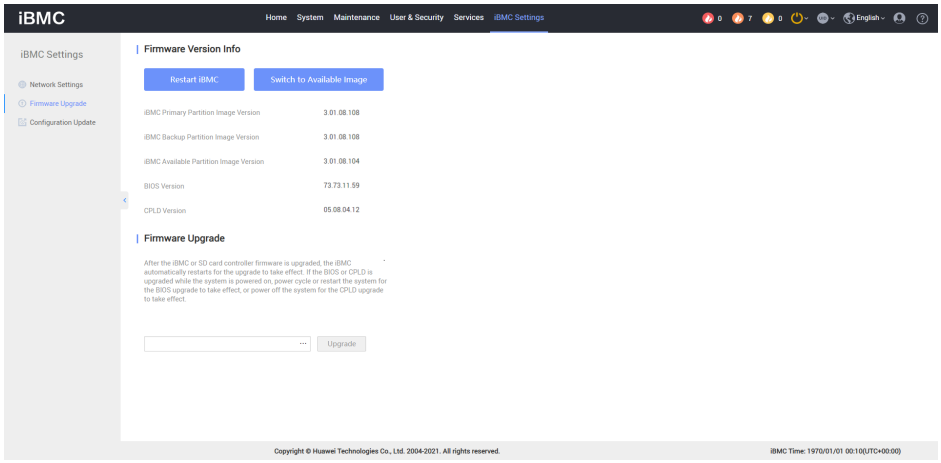


Figure 3-3 Querying the iBMC firmware version on the iBMC WebUI (3.01.17.*x*)

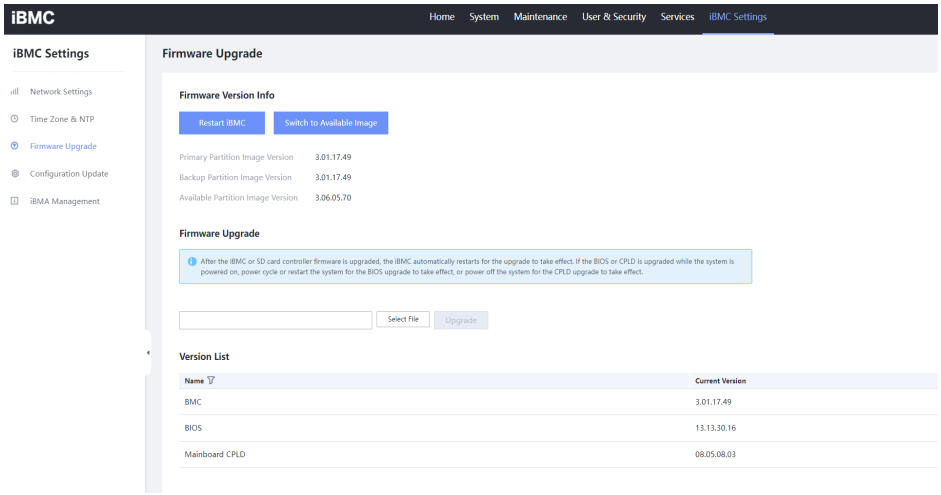


Figure 3-4 Querying the iBMC firmware version on the iBMC WebUI (3.09.00.*x* or later)

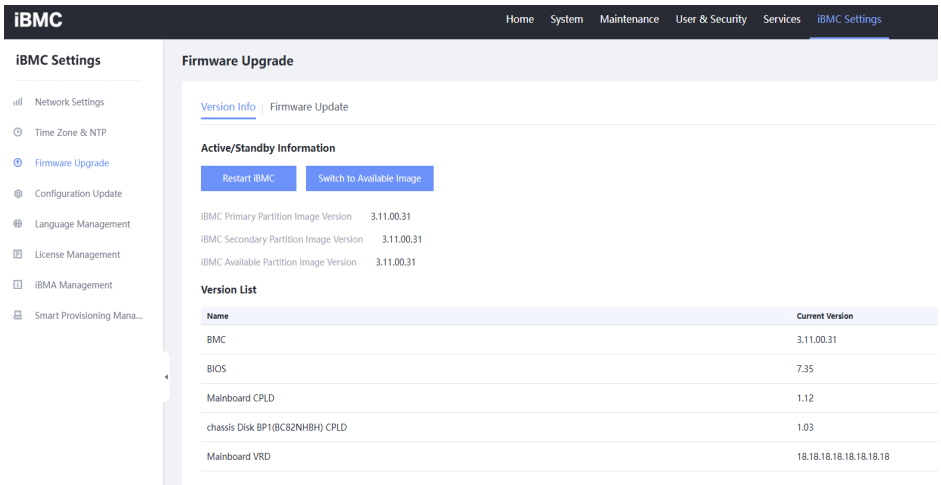
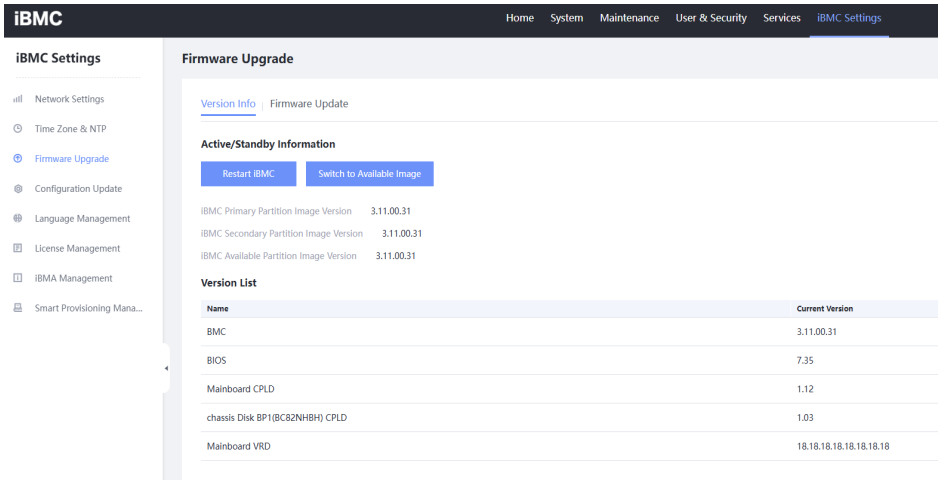


Figure 3-5 Querying the iBMC firmware version on the iBMC WebUI (3.11.00.25 or later)



Step 2 Check the firmware version in the **version.xml** file. For example, the **<Version>3.01.08.52</Version>** attribute in the configuration file indicates that the iBMC firmware version is 3.01.08.52, as shown in **Figure 3-6**.

Figure 3-6 iBMC firmware version information contained in the XML file

```
<?xml version="1.0" encoding="utf-8"?>
<FirmwarePackage version="V1.2">
 <!--Firmware packages description-->
    <Package>
        <PackageName>PANGEA_V600R005C00_ATLANTIC_IBMC</PackageName>
        <FileName>rootfs_rw_PangeaV6_Atlantic.hpm</FileName>
        <Version>3.01.08.52</Version>
        <!--<VersionPattern>(\d|(1[0-5]))\.(0\d|(1[0-5]))\s*$</VersionPattern>-->
        <!--FileType:1.Firmware,2.Dirver,3.Software-->
        <FileType>Firmware</FileType>
        <!--Module:1.MM/HMM,2.iMana/iBMC,3.BIOS,4.CPLD,5.LCD,6.Base/Fabric,7.FAN,8.PSU,
            9.FPGA,10.HBA,11.CNA,12.NIC,13.RAID,14.IB,15.SSD,16.GPU,17.NVDIMM-->
        <Module>iBMC</Module>
        <Vendor>Huawei Technology Co.</Vendor>
        <SupportModel>PangeaV6_Atlantic</SupportModel>
        <!--Multiple models are separated by semicolons-->
        <SupportModelUID>0x020d1b00</SupportModelUID>
        <!--UpgradeAgent:1.SMM, 2.BMC, 3.BMA 4.Switch 5.FC -->
        <UpgradeAgent>BMC</UpgradeAgent>
        <!--UpgradeTime:unit second-->
        <UpgradeTime>600</UpgradeTime>
        <!--UpgradeOvertime:unit second-->
        <MaxUpgradeTime>900</MaxUpgradeTime>
        <!--ActiveMode:1.Immediately,2.ResetMM,3.ResetBMC,4.ResetOS,5.ResetServer,6.ResetSwitch,
            7.ColdResetSwitch,8.EnclosureReset-->
        <ActiveMode>ResetBMC</ActiveMode>
        <!-- (Optional) Upgrade impact displayed on the web UI. The options are as follows:1.NONE,2.BMC,3.MM,4.Host,5.Base,6.Fabric,7.Chassis -->
        <ActiveEffect>BMC</ActiveEffect>
        <!--ActiveTime:unit second-->
        <ActiveTime>180</ActiveTime>
        <!--ActiveOvertime:unit second-->
        <MaxActivetime>600</MaxActivetime>
        <!--UpgradeMode:1.MANUAL,2.AUTO-->
        <UpgradeMode>MANUAL</UpgradeMode>
        <!--Size:unit Byte-->
        <!--<Size>54257</Size>-->
        <!--<OldVersion>N/A</OldVersion>-->
        <!--<VersionPattern>(\d|(1[0-5]))\.(0\d|(1[0-5]))\s*$</VersionPattern>-->
        <!--<ActiveTimes>1</ActiveTimes>-->
        <!--For CPLD,Object is BOARD Names-->
        <Object>iBMC</Object>
        <!--For CPLD,ObjectID is BOARD ID-->
        <ObjectID>0x0d1b</ObjectID>
        <!--RpmName is the package name of this firmware, this name is unique-->
        <RpmName>PangeaV6--PangeaV6_Atlantic-iBMC-Firmware for Huawei Storage.</RpmName>
        <!--brief introduction-->
        <Summary>PangeaV6--PangeaV6_Atlantic-iBMC-Firmware for Huawei Storage.</Summary>
        <!--Detailed description of related functions-->
        <Description>PangeaV6-PangeaV6_Atlantic-iBMC-Firmware for Huawei Storage.</Description>
    </Package>
</FirmwarePackage>
```

----End

NOTE

The procedures for upgrading and rolling back the iBMC firmware are the same. You can upgrade and roll back the firmware to the same version for multiple times.

3.3.1.2 Performing the Upgrade

Procedure

Step 1 Log in to the iBMC WebUI.

Step 2 Go to the page for firmware upgrade. For iBMC 3.01.*x.x*, choose **iBMC Settings** > **Firmware Upgrade**. For iBMC 3.09.00.*x* or later, choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Update**. The **Firmware Upgrade** page is displayed.

Figure 3-7 Firmware Upgrade page (iBMC 3.01.08.*x*)

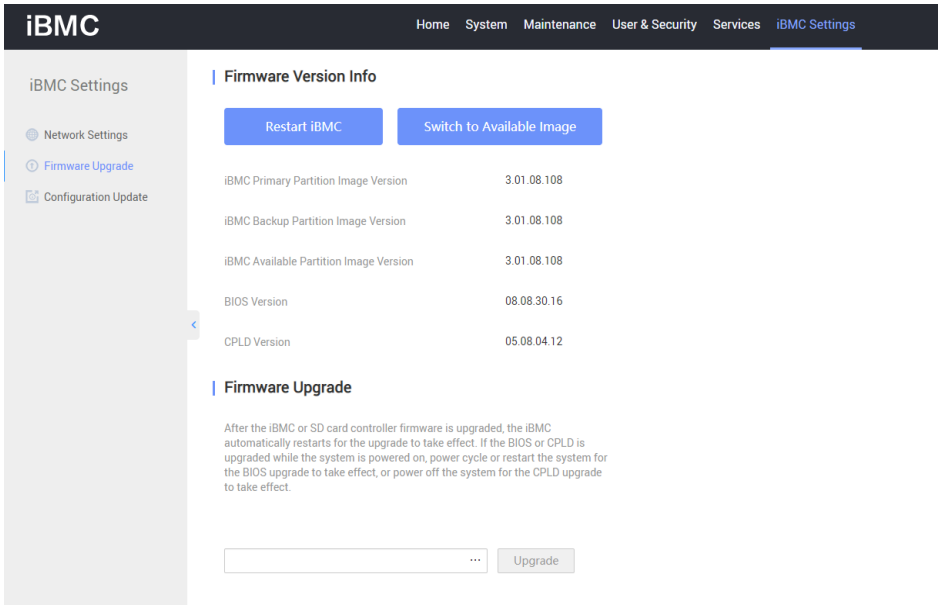


Figure 3-8 Firmware Upgrade page (iBMC 3.01.17.*x*)

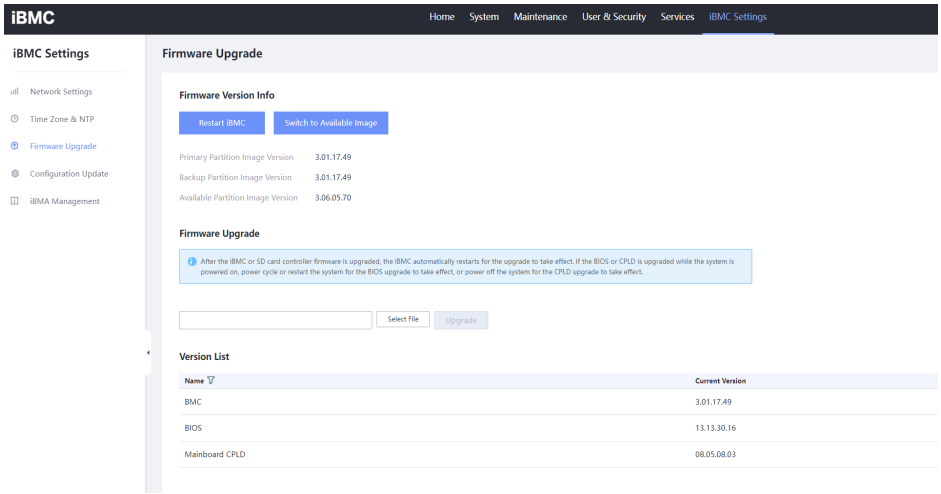


Figure 3-9 Firmware Upgrade page (iBMC 3.09.00.*x* or later)

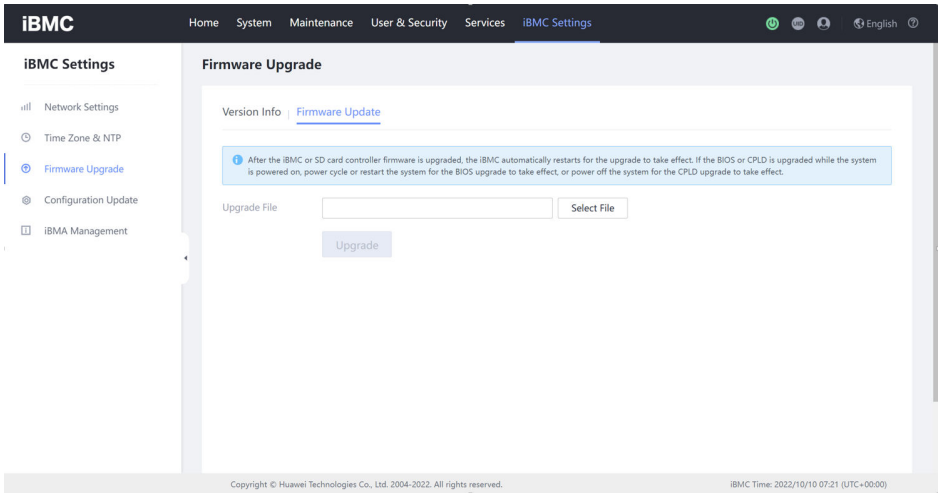
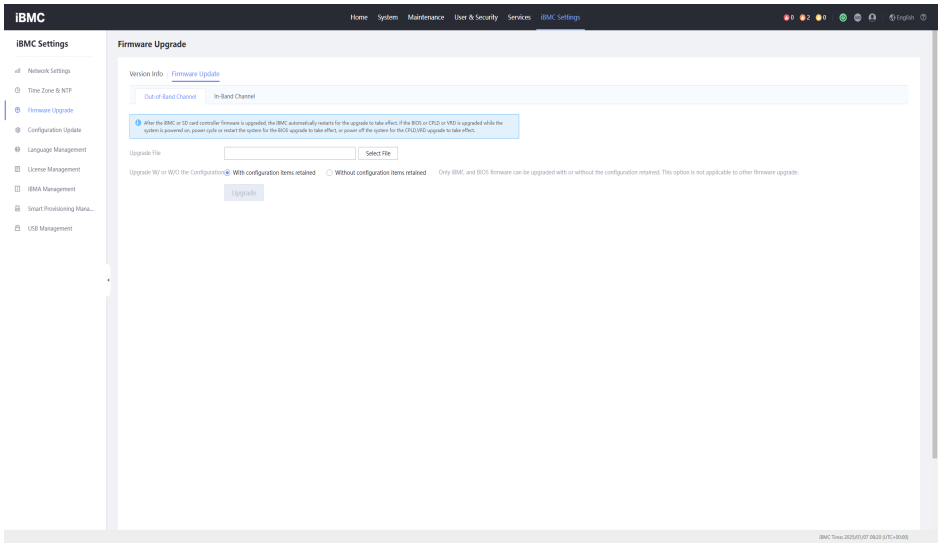


Figure 3-10 Firmware Upgrade page (iBMC 3.11.00.25 or later)



NOTE

Different hardware configurations support repeated upgrades to the same firmware version.

Step 3 Select the target firmware. For iBMC 3.01.08.*x*, click ... and select the ***.hpm** firmware for upgrade. For iBMC 3.01.17.*x* or 3.09.00.*x* or later, click Select File and select the ***.hpm** firmware for upgrade. The iBMC system automatically restarts after the upgrade is completed. The following figures show the iBMC WebUIs of different versions.

Figure 3-11 Firmware Upgrade page (iBMC 3.01.08.*x*)

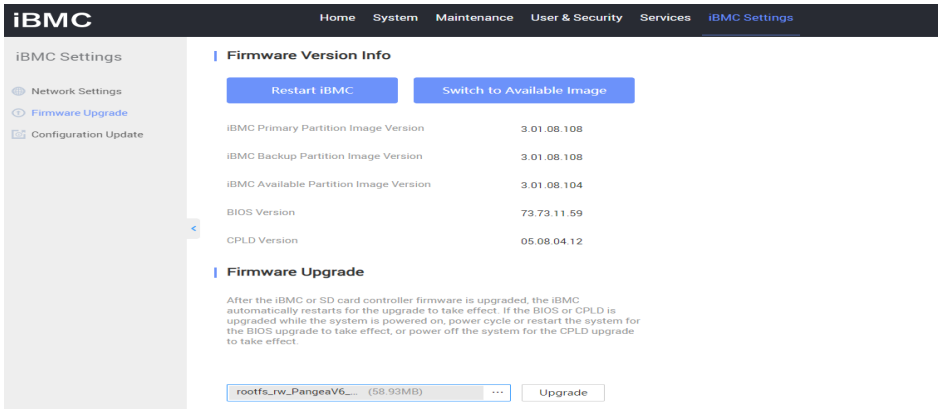


Figure 3-12 Firmware Upgrade page (iBMC 3.01.17.*x*)

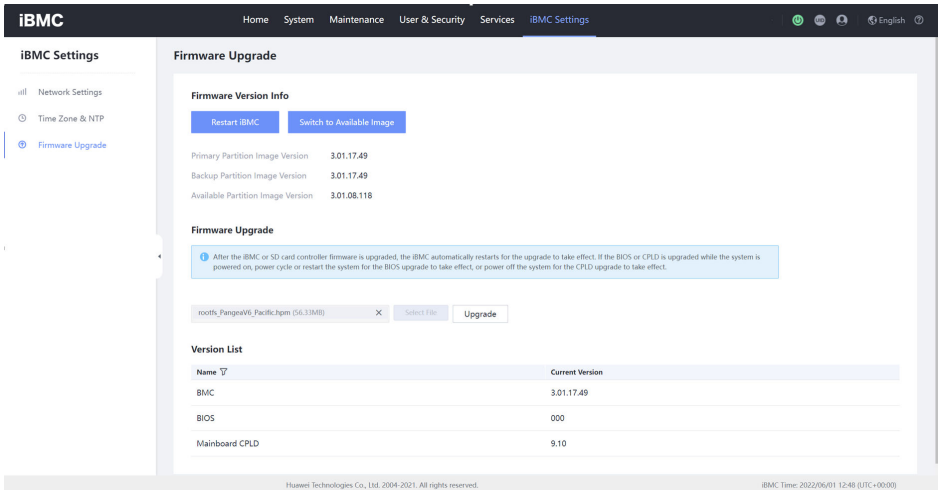


Figure 3-13 Firmware Upgrade page (iBMC 3.09.00.*x* or later)

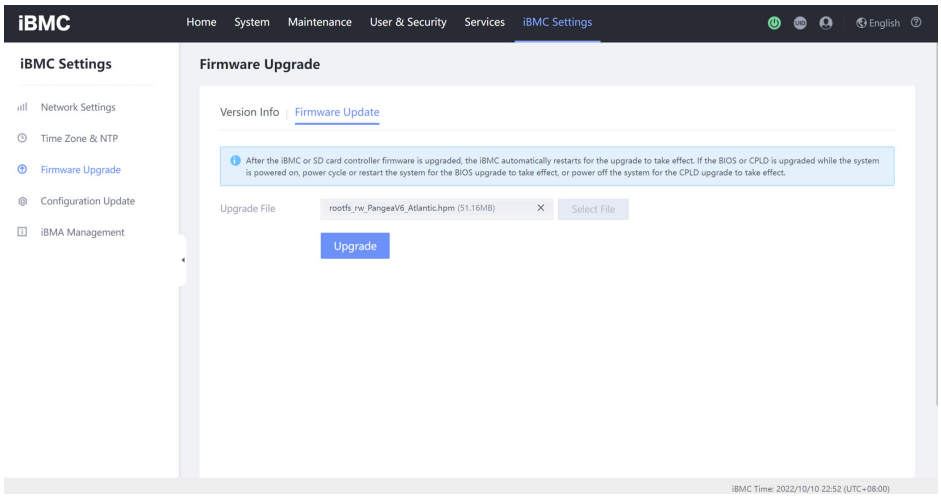
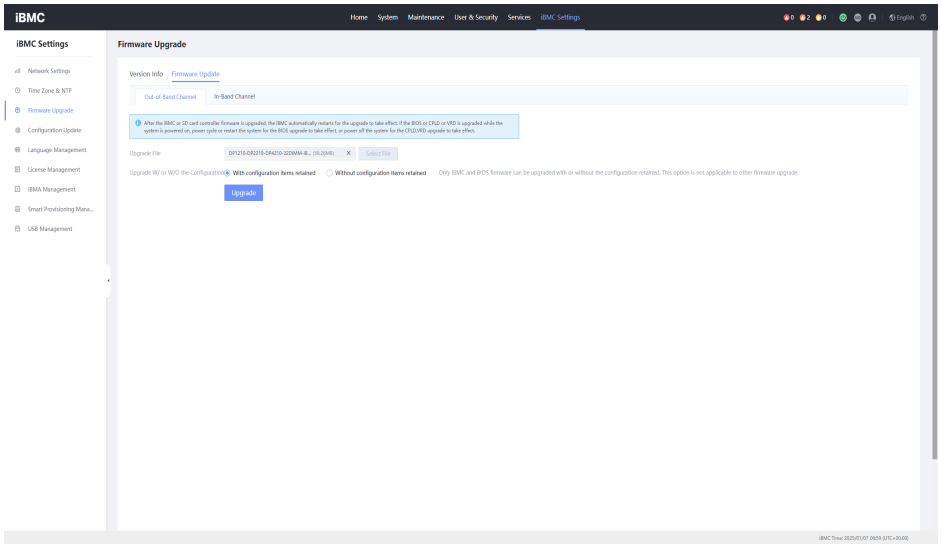


Figure 3-14 Firmware Upgrade page (iBMC 3.11.00.25 or later)



NOTE

- For different hardware forms, use the correct firmware package for upgrade according to the actual hardware information.
- The upgrade page varies with the hardware or iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- If **Out-of-Band Channel** and **In-Band Channel** are available for upgrade, you are advised to use **Out-of-Band Channel** for upgrade.

Step 4 Perform the upgrade. After you click **Start Upgrade** or **Upgrade**, the **Confirm** dialog box is displayed. To confirm the upgrade, click **Yes**. Otherwise, click **No** to cancel the upgrade.

Figure 3-15 Confirming the firmware upgrade

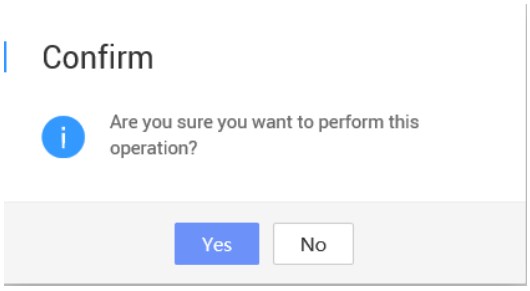


Figure 3-16 Upgrading firmware (iBMC 3.01.08.*x*)

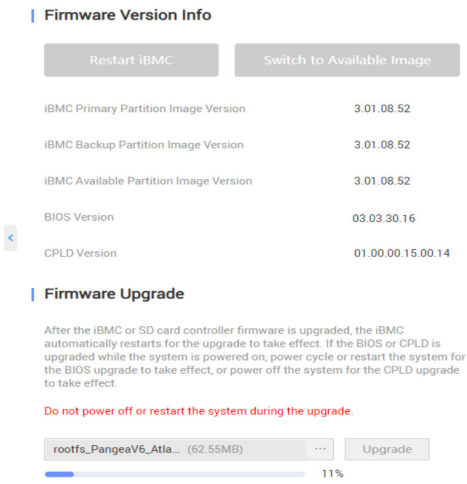


Figure 3-17 Upgrading firmware (iBMC 3.01.17.*x*)

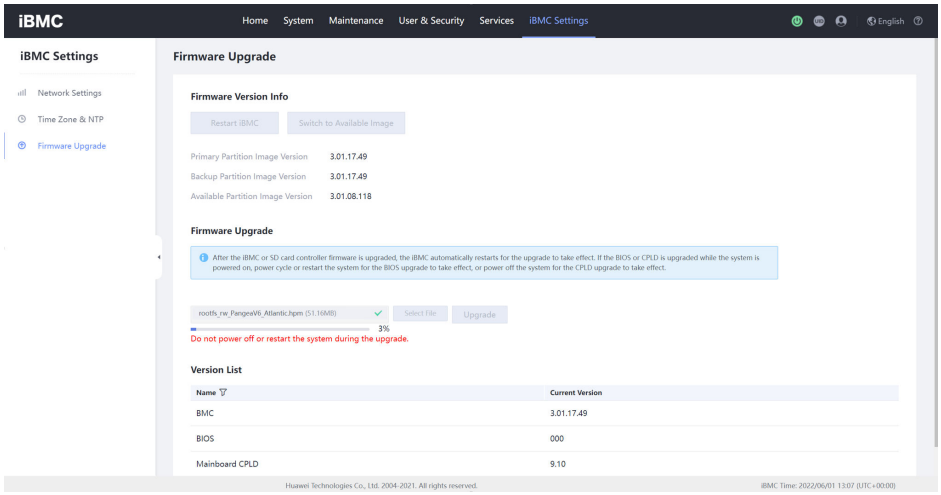


Figure 3-18 Upgrading firmware (iBMC 3.09.00.*x* or later)

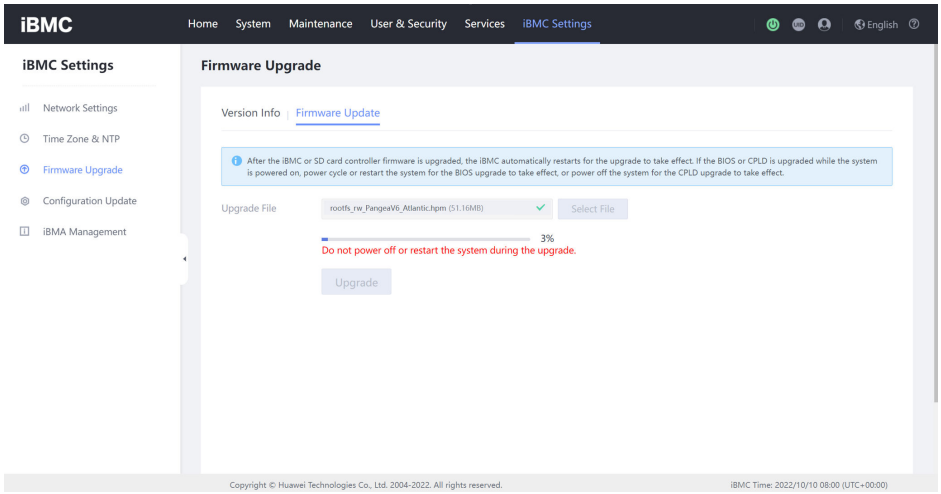
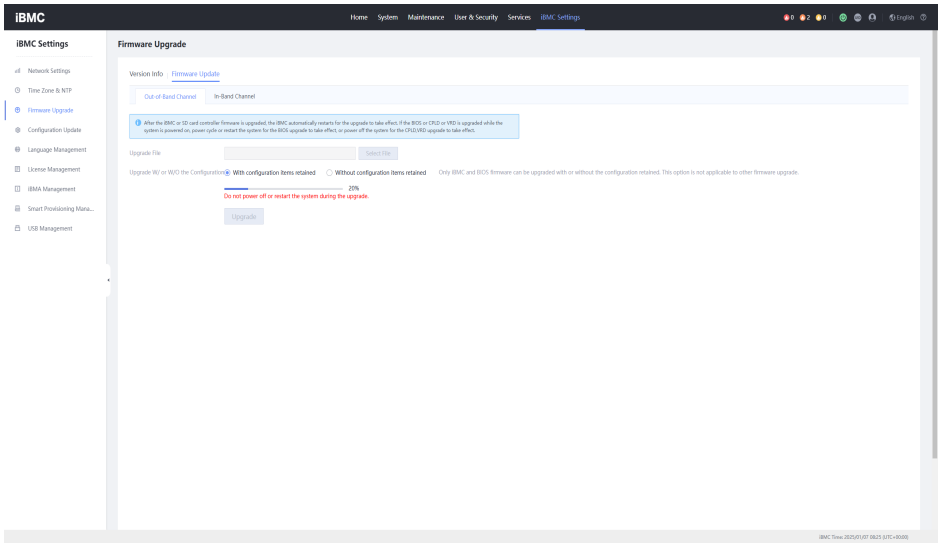


Figure 3-19 Upgrading firmware (iBMC 3.11.00.25 or later)



NOTICE

During the firmware upgrade, buttons on the iBMC WebUI are unavailable. Do not perform any other operation before the upgrade is completed. The iBMC firmware upgrade takes about 10 to 15 minutes. If an exception occurs during the upgrade, contact technical support.

Step 5 Wait for the upgrade to complete. After the iBMC firmware upgrade is complete, the iBMC system automatically resets. Wait for 3 minutes until the iBMC restart is complete. The following figures show the iBMC WebUIs of different versions.

Figure 3-20 iBMC upgraded successfully (iBMC 3.01.08.*x*)

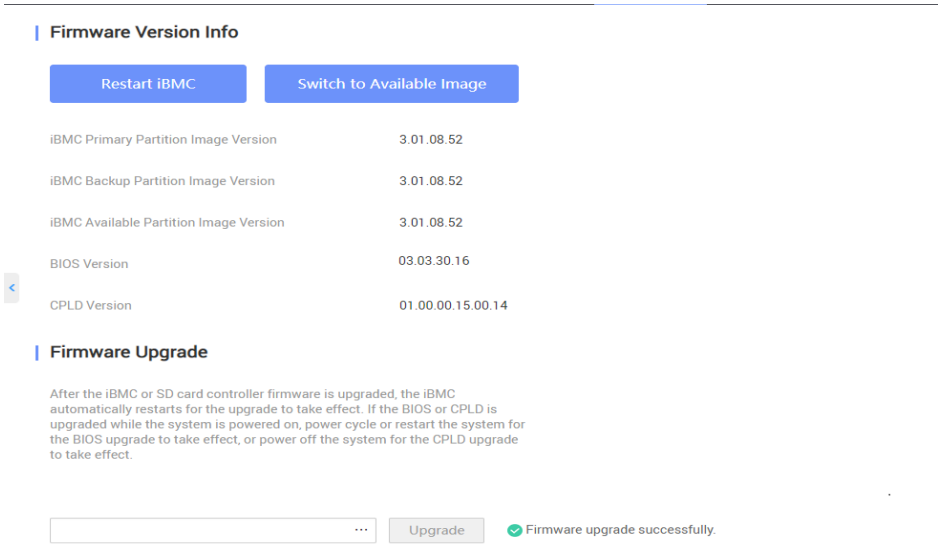


Figure 3-21 iBMC upgraded successfully (iBMC 3.01.17.*x*)

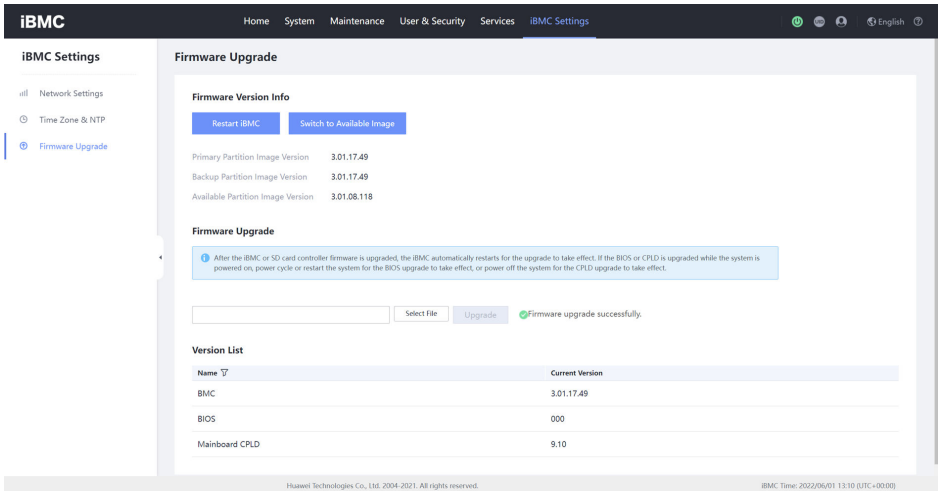


Figure 3-22 iBMC upgraded successfully (iBMC 3.09.00.*x* or later)

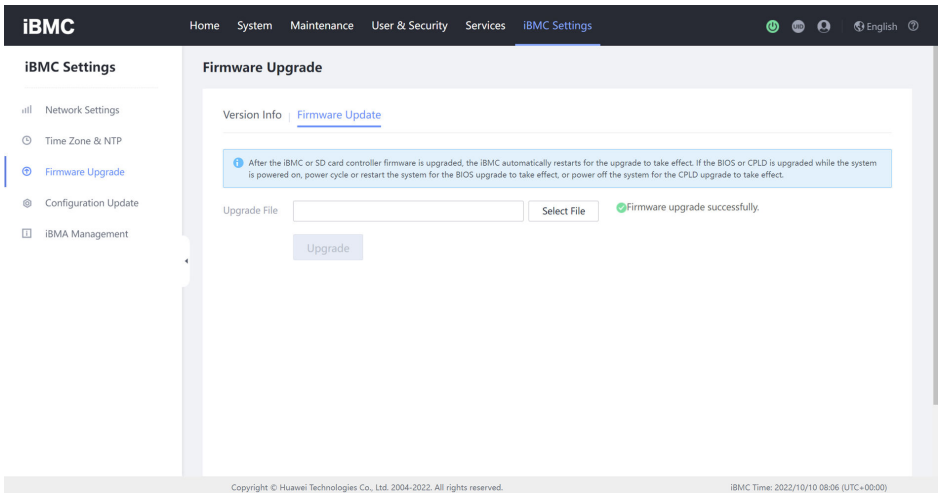
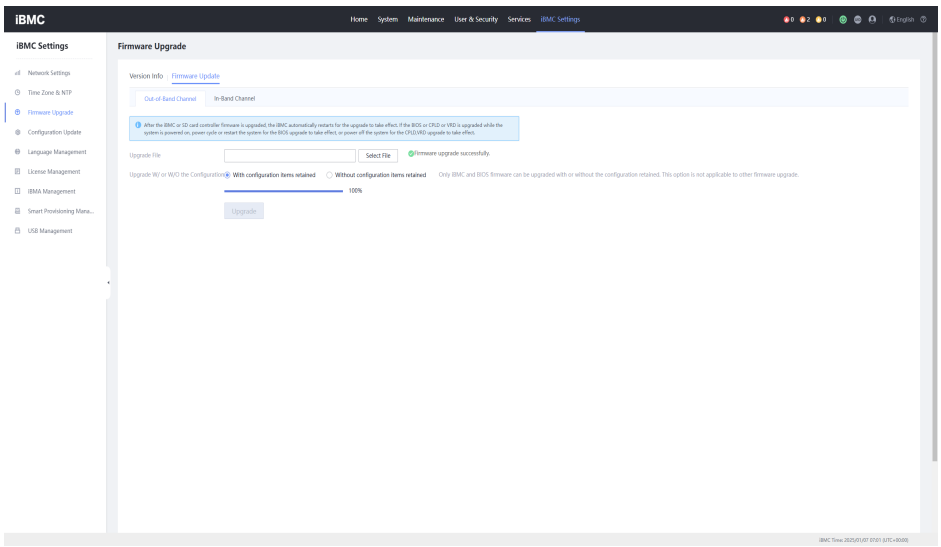


Figure 3-23 iBMC upgraded successfully (iBMC 3.11.00.25 or later)



NOTE

The upgrade result varies with the firmware package. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

----End

3.3.1.3 Verifying the Upgrade

After the upgrade is complete, you need to check whether the latest iBMC firmware version takes effect. You need to log in to the iBMC WebUI again and check the version by following instructions in **2 Preparing for the Upgrade**. If the primary partition image version of the iBMC and the version in **version.xml** are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

NOTICE

The iBMC has multiple image partitions. Only the backup partition image can be upgraded. After the upgrade is successful, the iBMC automatically restarts and the backup partition image is automatically activated. No manual switchover is required. If you need to upgrade multiple partition images to the latest version, you need to perform the upgrade twice. It is recommended that the iBMC versions of multiple partitions be the same.

3.3.2 Upgrading the iBMC Firmware of a Data Cluster Module

The procedure for upgrading the iBMC firmware for a data cluster module is the same as that for upgrading the iBMC firmware. After downloading the iBMC firmware of a data cluster module, upgrade it by following instructions in **3.3.1 Upgrading the iBMC Firmware**.

CAUTION

If the iBMC firmware of two data cluster modules is upgraded at the same time, services may be interrupted. Contact technical support engineers to determine the upgrade scheme and then perform the upgrade.

3.3.3 Upgrading the BIOS Firmware

3.3.3.1 Preparing for the Upgrade

3.3.3.1.1 Checking the Upgrade Scenario

Before performing a BIOS firmware upgrade, check the upgrade scenario and determine the corresponding upgrade method. The upgrade scenarios are as follows:

- If the AC power supply to the chassis fails during the BIOS firmware upgrade and the system cannot be started, manually upgrade the BIOS firmware to

restore the environment. For details, see **4.2.4 Power Supply Fails During a BIOS Firmware Upgrade and the System Cannot Be Started**.

- If the system is powered on or off during the BIOS firmware upgrade and the system cannot be started, manually upgrade the BIOS firmware to restore the environment. For details, see **4.2.1 System Resetting During the BIOS Upgrade**.
- If the system can be started properly and the BIOS firmware needs to be manually upgraded during site deployment or parts replacement, perform the upgrade by following instructions in **3.3.3.1.2 Decompressing the BIOS Firmware Package**.
- If the system is reset during the BIOS firmware upgrade and the system cannot be started, manually upgrade the BIOS firmware to restore the environment. For details, see **4.2.1 System Resetting During the BIOS Upgrade**.
- In other scenarios, perform the upgrade by following instructions in this section.

3.3.3.1.2 Decompressing the BIOS Firmware Package

Upload the BIOS firmware package to a specified directory on the local PC and decompress the package. For details about how to obtain the firmware package, see **2 Preparing for the Upgrade**. **Figure 3-24** shows the files in the decompressed firmware package. The firmware package contains three files. **Table 3-2** lists these files.

Figure 3-24 Files in a BIOS firmware package

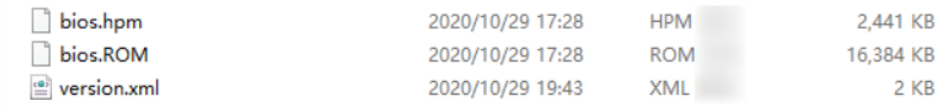


Table 3-2 Description of files in a BIOS firmware package

File Name	Description
bios.ROM	Source file of BIOS firmware
bios.hpm	BIOS firmware
version.xml	Version configuration table, which records the BIOS firmware version

NOTE

The BIOS firmware packages for different hardware configurations are in the same format and the upgrade processes are the same. Obtain the BIOS firmware version based on the actual hardware configuration. If you have any questions, contact the maintenance personnel.

NOTICE

During a BIOS firmware upgrade, the system needs to be reset or powered off and powered on for the firmware to take effect, which will interrupt services.

3.3.3.1.3 Checking Versions

Check the current BIOS version on the iBMC WebUI and the version in the **version.xml** file. If the versions are different, an upgrade is necessary. This section describes how to check the versions.

Procedure

Step 1 Log in to the iBMC WebUI. For iBMC 3.01.*x.x*, choose **iBMC Settings** > **Firmware Upgrade**. For iBMC 3.09.00.*x* or later, choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Version Info**. The **Firmware Version Info** page is displayed. The following figures show the iBMC WebUIs of different versions.

Figure 3-25 Querying the BIOS firmware version (iBMC 3.01.08.*x*)

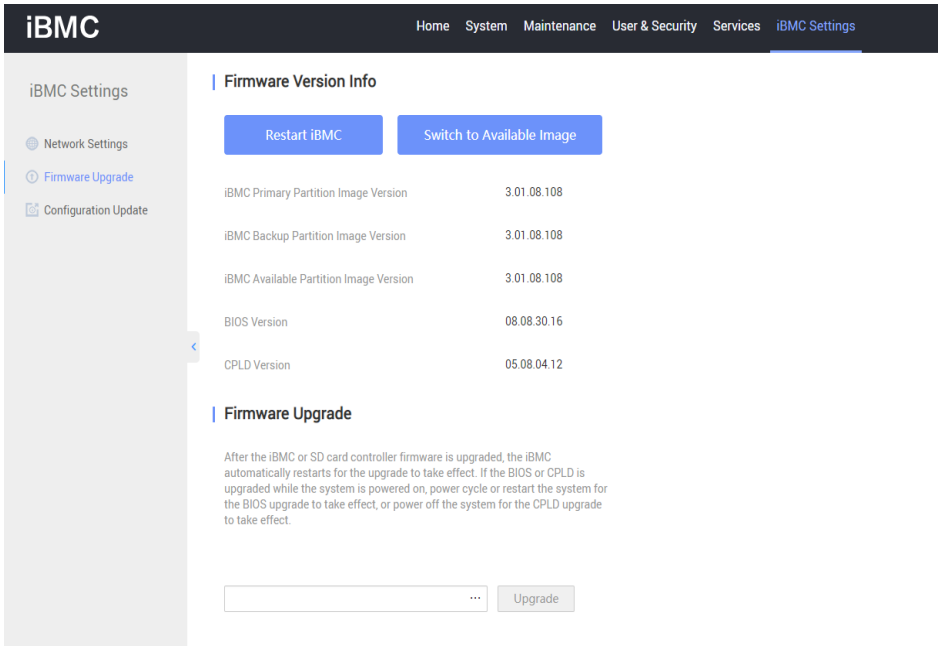


Figure 3-26 Querying the BIOS firmware version (iBMC 3.01.17.*x*)

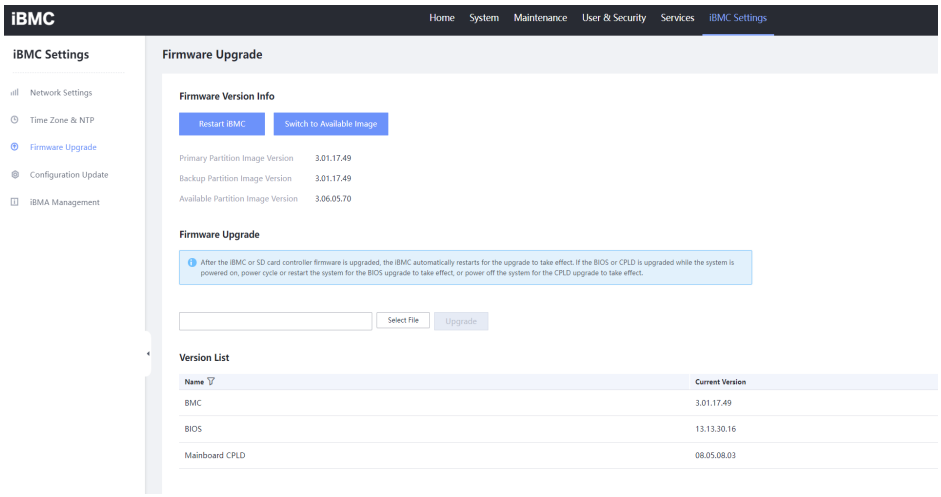


Figure 3-27 Querying the BIOS firmware version (iBMC 3.09.00.*x* or later)

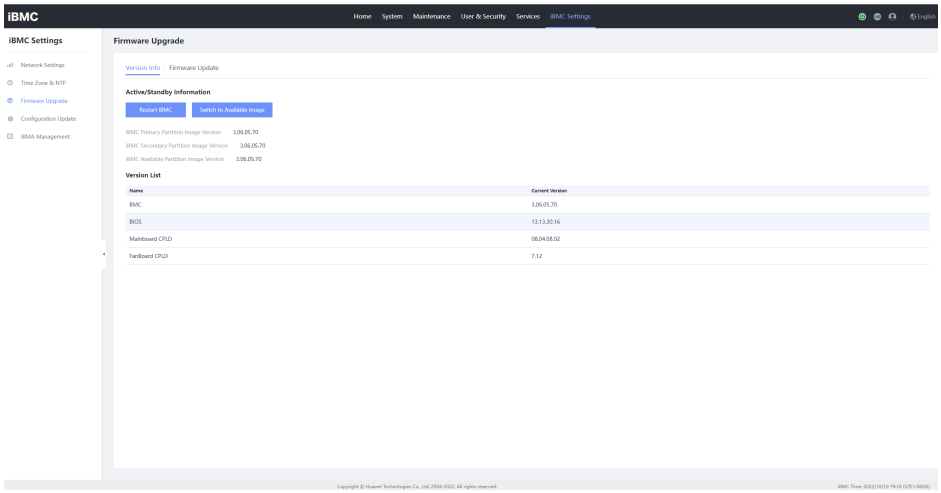
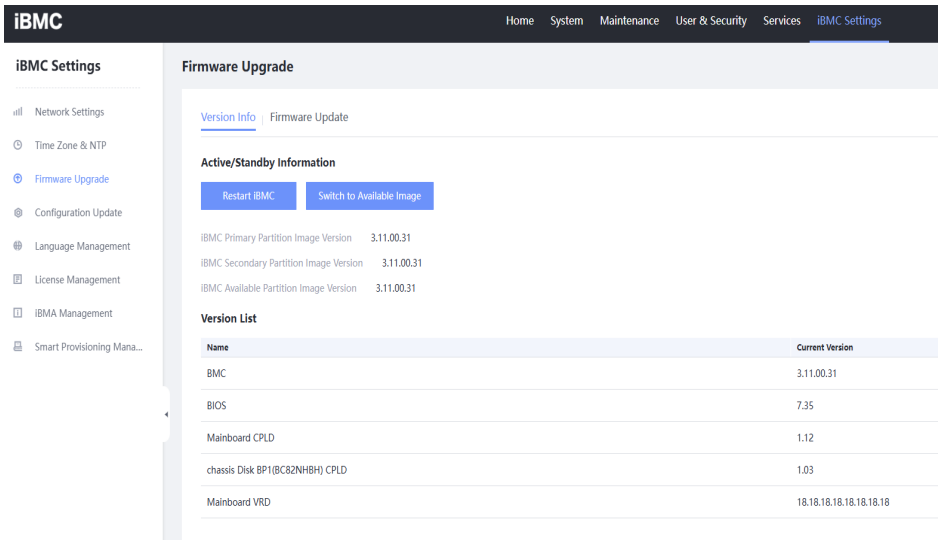


Figure 3-28 Querying the BIOS firmware version (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 2 Check the firmware version in the **version.xml** file. For example, the **<Version>03.03.30.16</Version>** attribute in the configuration file indicates that the BIOS firmware version is 03.03.30.16, as shown in **Figure 3-29**.

Figure 3-29 BIOS firmware version information contained in the version.xml file

```
<?xml version="1.0" encoding="UTF-8"?>
- <FirmwarePackage version="V1.2">
      <!--Firmware packages description-->
    - <Package>
        <PackageName>V6R5-Pacific-BIOS-v003.zip</PackageName>
        <FileName>bios.hpm</FileName>
        <Version>03.03.30.16</Version>
        <BiosVersion>30.01.11T03</BiosVersion>
        <ImuVersion>30.01.11T03</ImuVersion>
        <M7Version>10.02.30T16</M7Version>
        <VersionPattern>(\d+)\.(\d+)\s*$</VersionPattern>
        <FileType>Firmware</FileType>
        <Module>BIOS</Module>
        <Vendor>Huawei Technology Co.</Vendor>
        <SupportModel>STL6SPCM</SupportModel>
        <SupportModelUID>0x020d1700;0x020d1b00</SupportModelUID>
        <UpgradeAgent>BMC</UpgradeAgent>
        <UpgradeTime>600</UpgradeTime>
        <MaxUpgradeTime>900</MaxUpgradeTime>
        <ActiveMode>ResetServer</ActiveMode>
        <ActiveEffect>None</ActiveEffect>
        <ActiveTime>180</ActiveTime>
        <MaxActivetime>360</MaxActivetime>
        <UpgradeMode>MANUAL</UpgradeMode>
        <Size>2725848</Size>
        <RpmName>Pangea V6R5 Pacific-CPLD-Firmware</RpmName>
        <Summary>Pangea V6R5 Pacific-CPLD-Firmware Firmware for Huawei Server.</Summary>
        <Description>Pangea V6R5 Pacific-CPLD-Firmware Firmware for Huawei Server.</Description>
    </Package>
</FirmwarePackage>
```

----End

3.3.3.1.4 Upgrading the BIOS When the OS Is Powered Off

After the BIOS is upgraded on the iBMC WebUI, the BIOS takes effect only after the system is powered off. Therefore, a reset operation is required. If the system does not have the power backup capability, data may be lost. Therefore, you are advised to upgrade the BIOS when the OS is powered off.

3.3.3.2 Performing the Upgrade

Procedure

Step 1 Log in to the iBMC WebUI.

Step 2 Query the system power status. Choose **System** > **Power** > **Power Control**. The **Power Control** page is displayed. The following figures show the iBMC WebUIs of different versions.

Figure 3-30 Power Control page (iBMC 3.01.08.*x*)

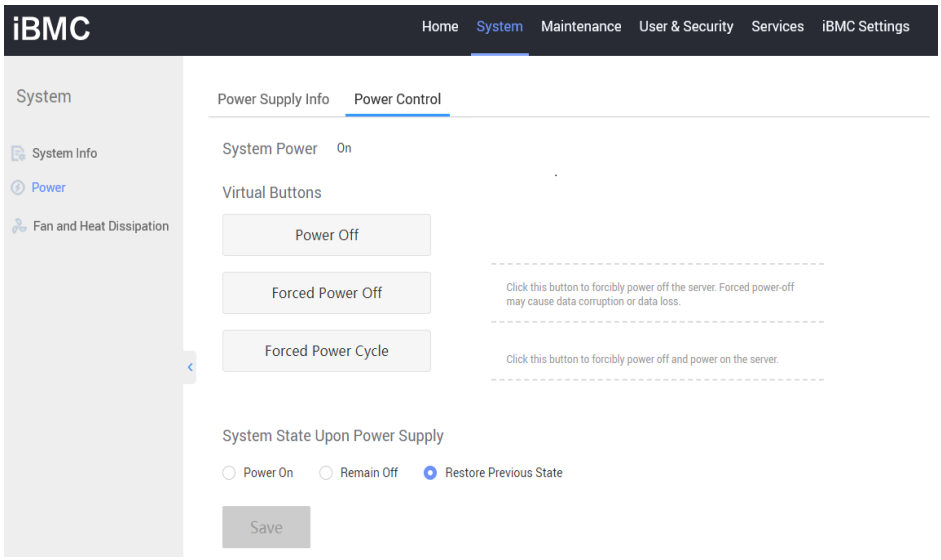


Figure 3-31 Power Control page (iBMC 3.01.17.*x* or 3.09.00.*x* or later)

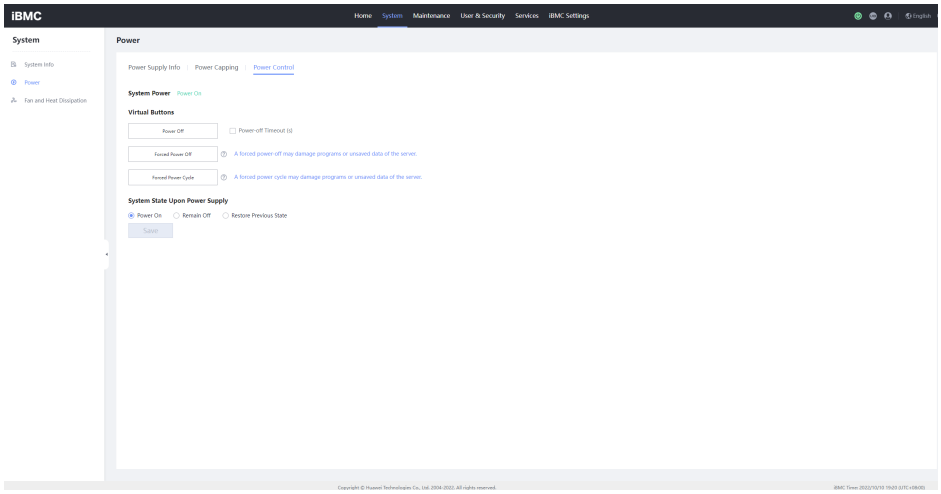
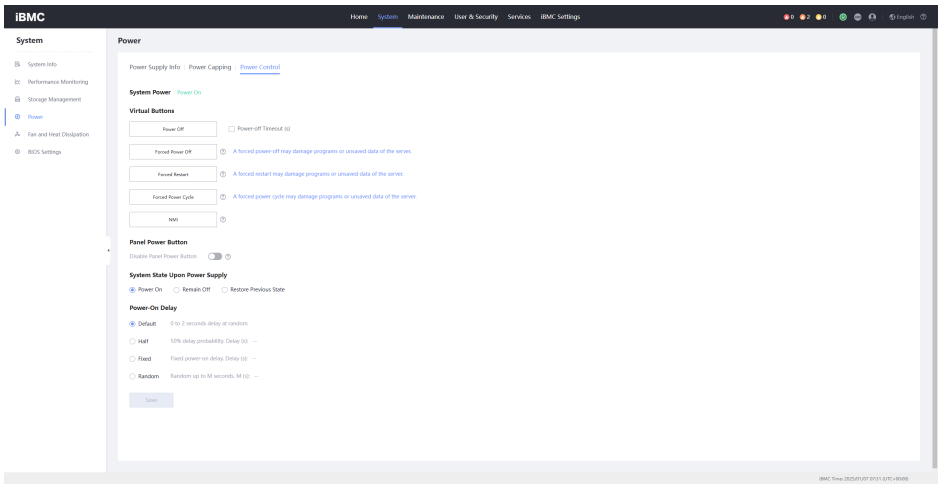


Figure 3-32 Power Control page (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 3 Check the system power status in **System Power**. Upgrade the BIOS when **System Power** is **Off** or **Power Off**. The following figures show the iBMC WebUIs of different versions.

Figure 3-33 Querying the system power status (iBMC 3.01.08.*x*)

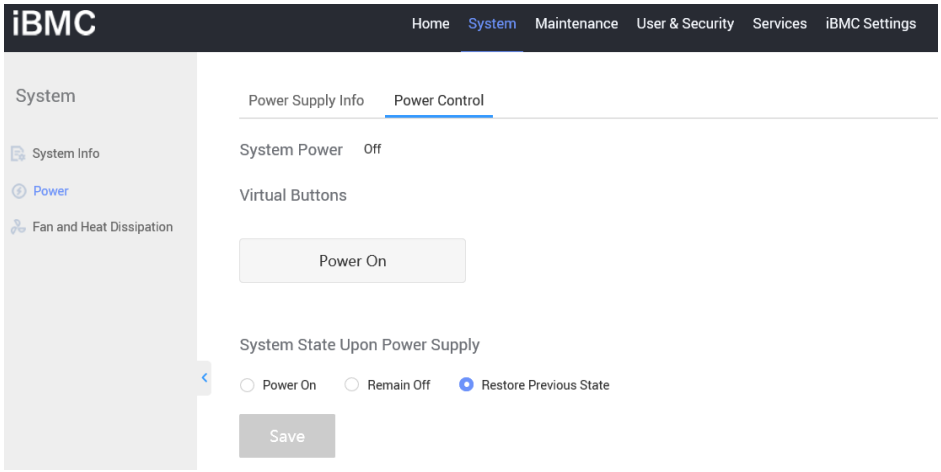


Figure 3-34 Querying the system power status (iBMC 3.01.17.*x* or 3.09.00.*x* or later)

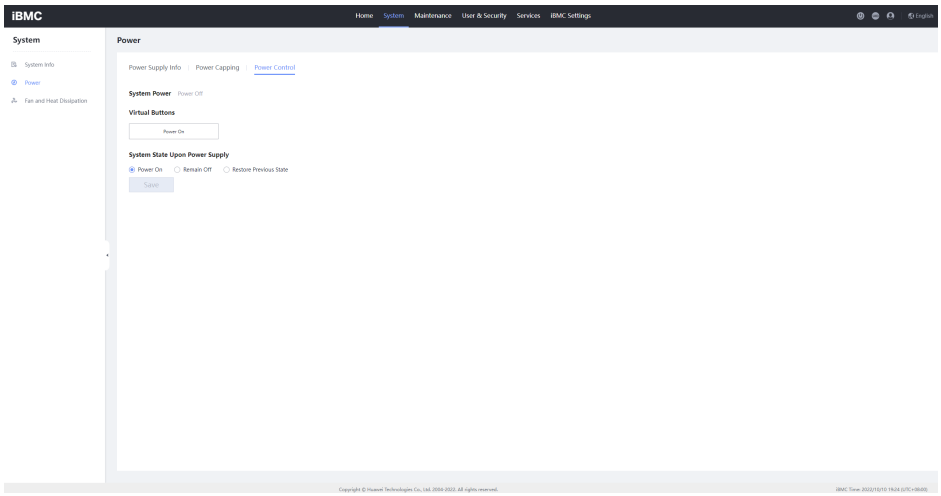
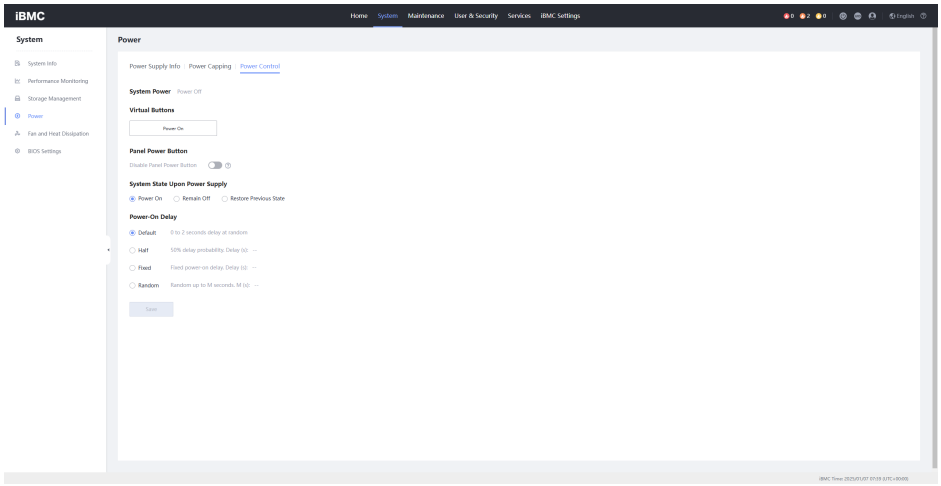


Figure 3-35 Querying the system power status (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 4 Go to the page for firmware upgrade. For iBMC 3.01.*x.x*, choose **iBMC Settings** > **Firmware Upgrade**. For iBMC 3.09.00.*x* or later, choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Update**. The **Firmware Upgrade** page is displayed. The following figures show the iBMC WebUIs of different versions.

Figure 3-36 Firmware Upgrade page (iBMC 3.01.08.*x*)

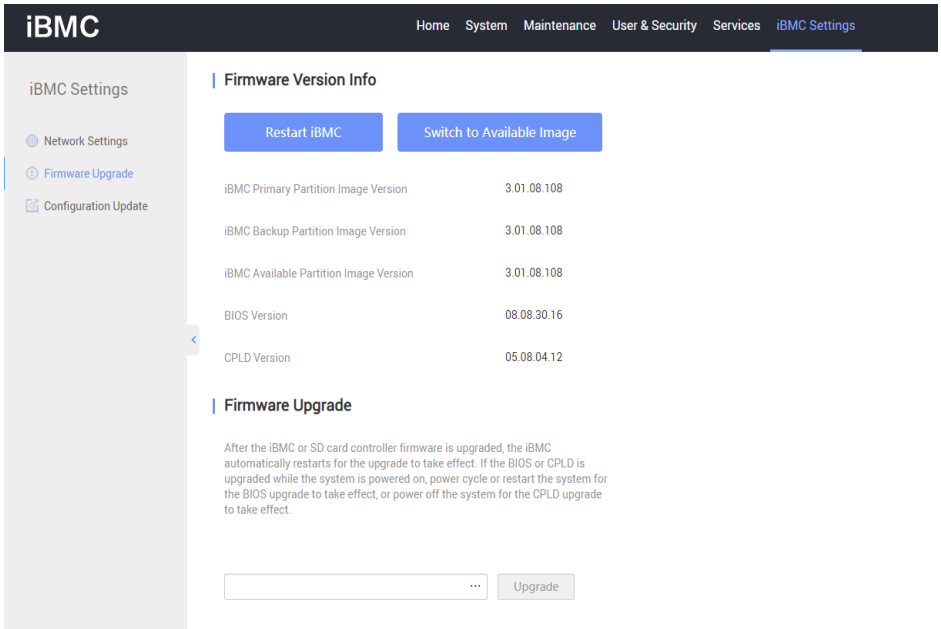


Figure 3-37 Firmware Upgrade page (iBMC 3.01.17.*x*)

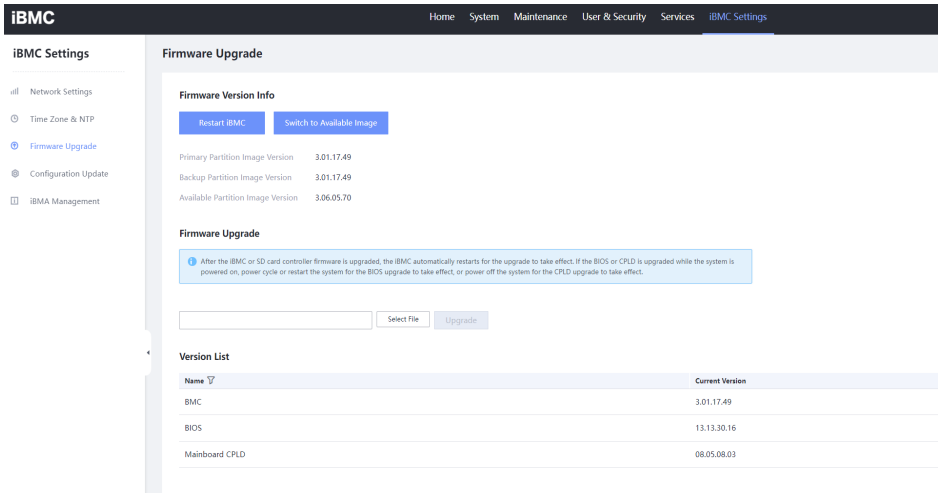


Figure 3-38 Firmware Upgrade page (iBMC 3.09.00.*x* or later)

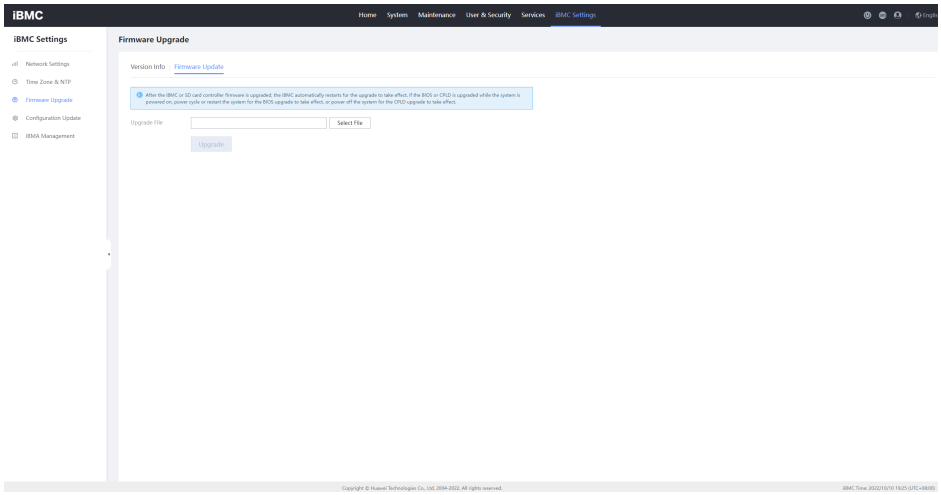
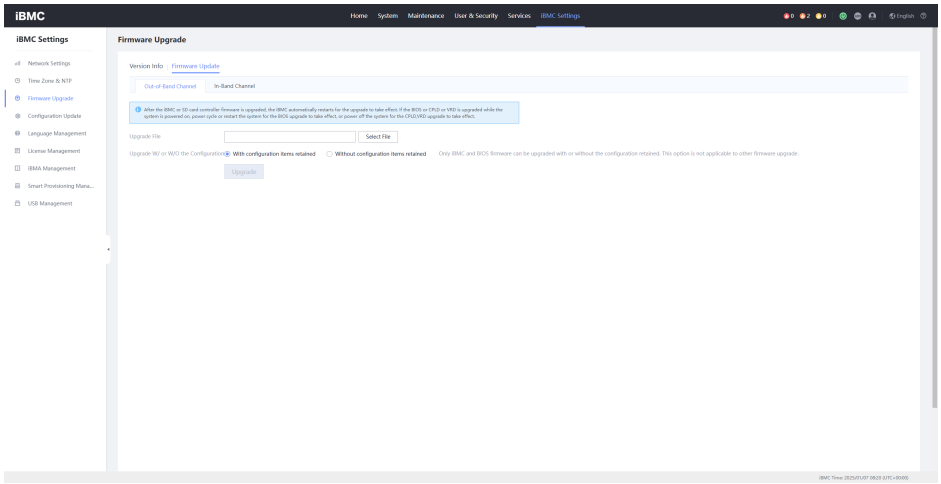


Figure 3-39 Firmware Upgrade page (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 5 Select the target firmware. For iBMC 3.01.08.*x*, click ... and select the **bios.hpm** firmware for upgrade. For iBMC 3.01.17.*x* or 3.09.00.*x* or later, click Select File and select the **bios.hpm** firmware for upgrade. The following figures show the iBMC WebUIs of different versions.

Figure 3-40 Selecting the target firmware (iBMC 3.01.08.*x*)

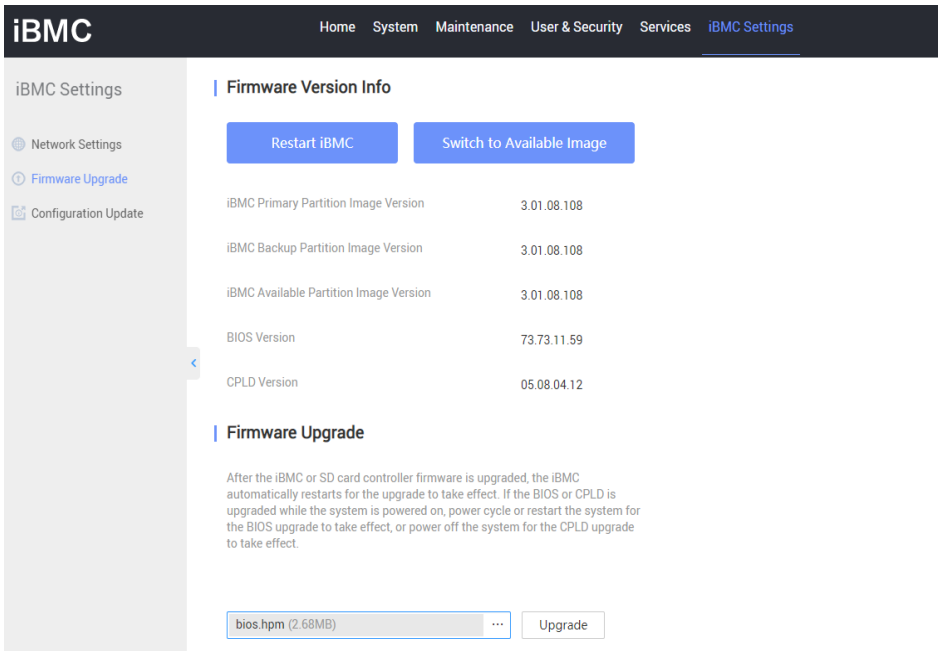


Figure 3-41 Selecting the target firmware (iBMC 3.01.17.*x*)

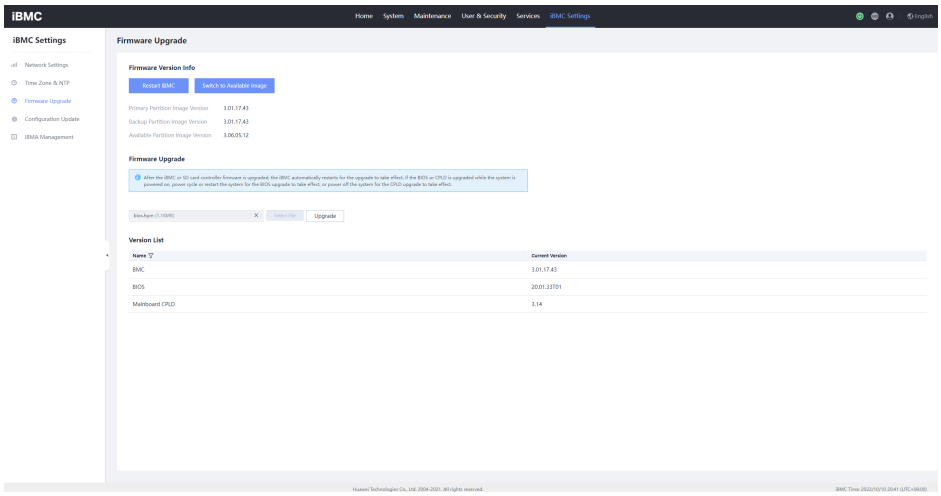


Figure 3-42 Selecting the target firmware (iBMC 3.09.00.*x* or later)

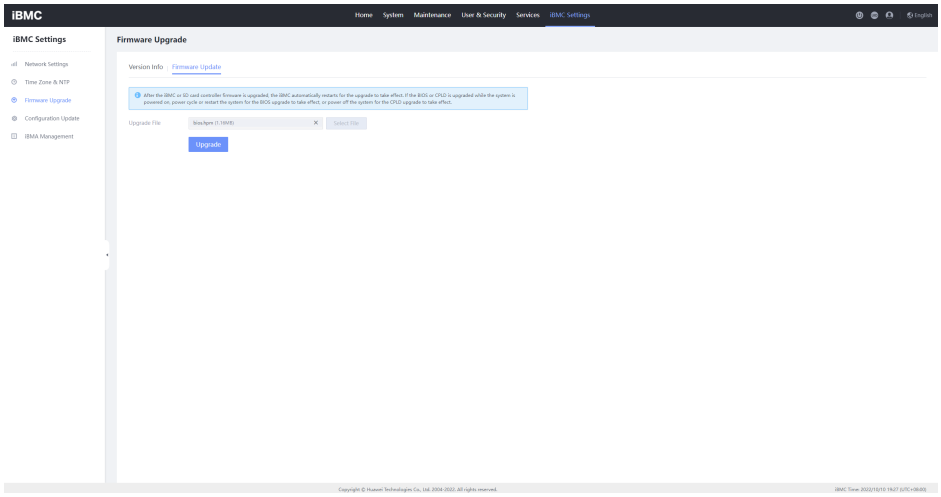
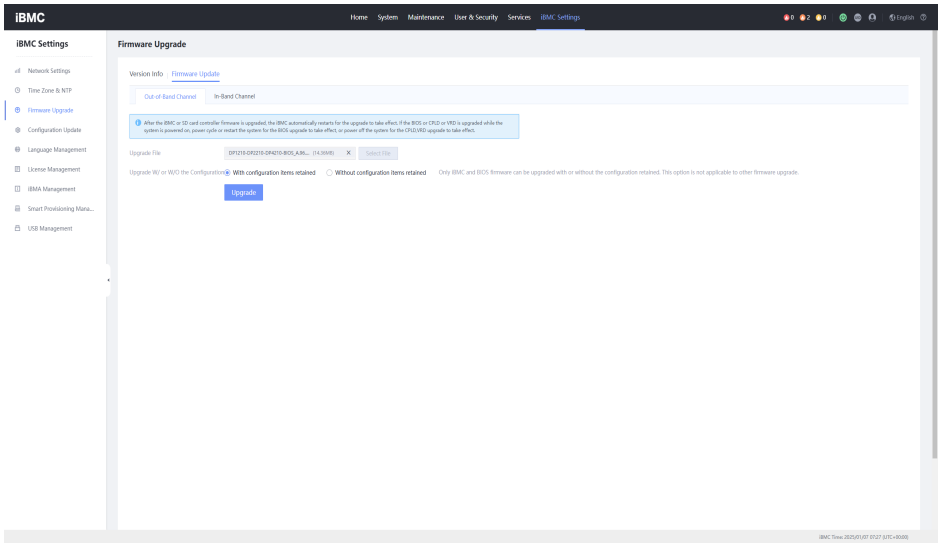


Figure 3-43 Selecting the target firmware (iBMC 3.11.00.25 or later)



NOTE

- The BIOS firmware package varies with the hardware model. Select the correct firmware package according to the specific model.
- The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 6 Perform the upgrade. After you click **Start Upgrade** or **Upgrade**, the **Confirm** dialog box is displayed. To confirm the upgrade, click **Yes**. Otherwise, click **No** to cancel the upgrade.

Figure 3-44 Confirming the firmware upgrade

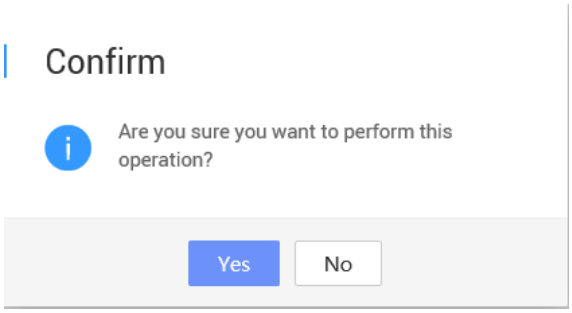


Figure 3-45 Upgrading firmware (iBMC 3.01.08.*x*)

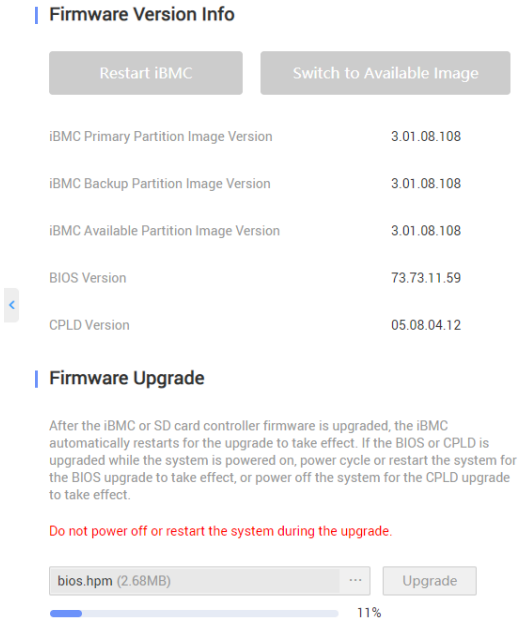


Figure 3-46 Upgrading firmware (iBMC 3.01.17.*x*)

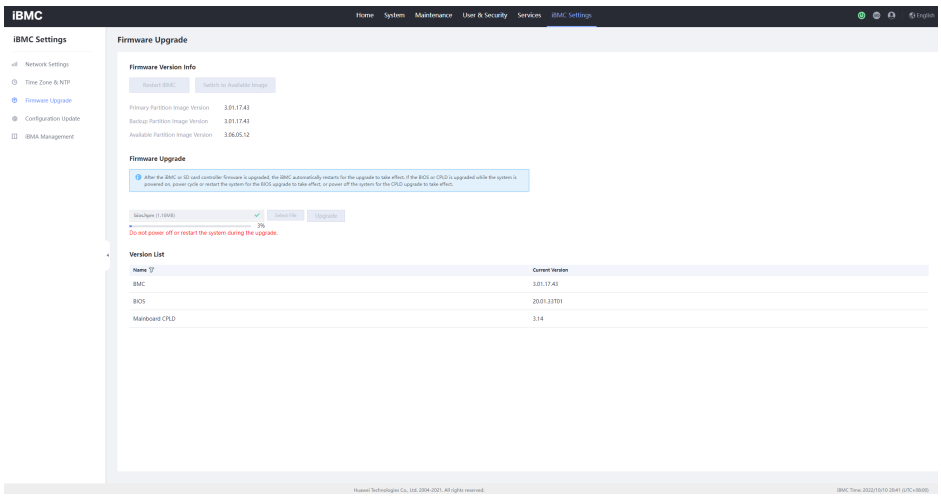


Figure 3-47 Upgrading firmware (iBMC 3.09.00.*x* or later)

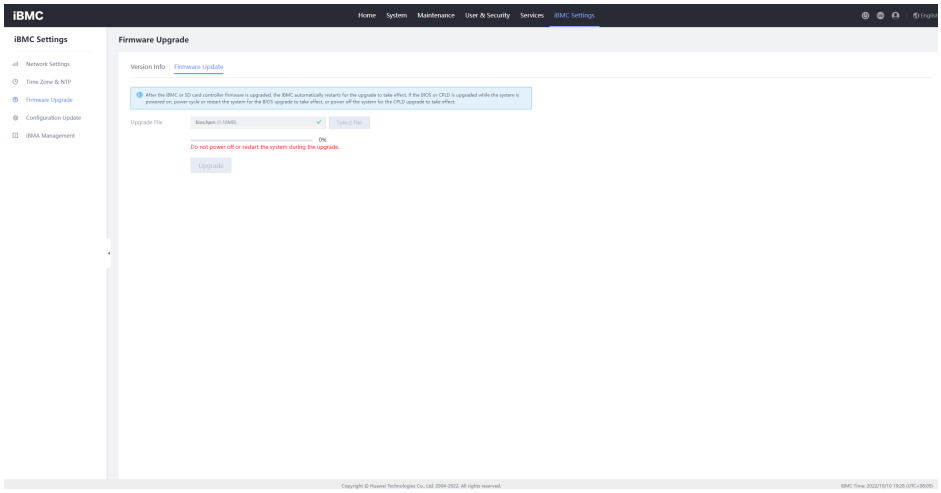
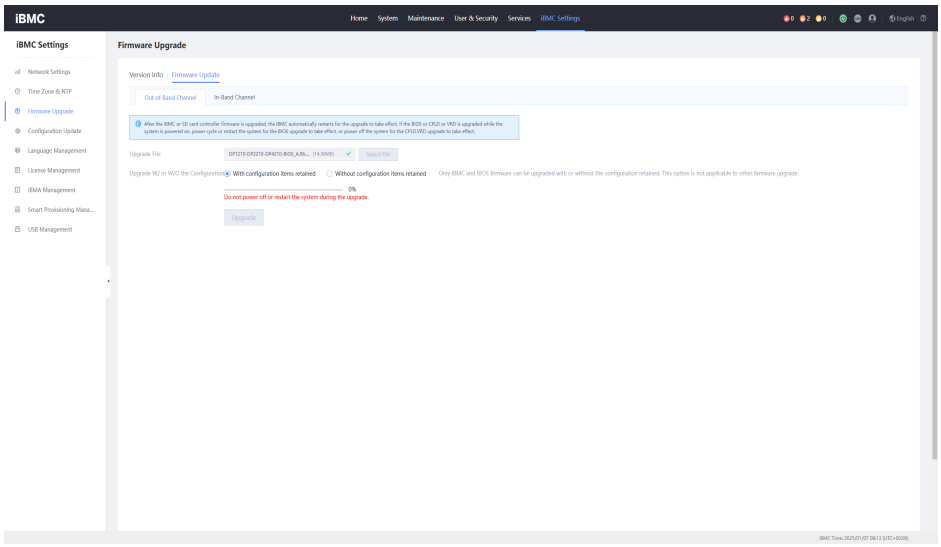


Figure 3-48 Upgrading firmware (iBMC 3.11.00.25 or later)



NOTE

- During the firmware upgrade, buttons on the iBMC WebUI are unavailable. Do not perform any other operation before the upgrade is completed. If a fault occurs during the firmware upgrade, see **4.2 iBMC, BIOS, and CPLD Installation/Upgrade Troubleshooting (iBMC V561 or Later, or iBMC V3.01.00.00 or Later)** or contact maintenance or development personnel.
- The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 7 Upload the upgrade file. After the upload is completed, a message is displayed, indicating that the upgrade file is uploaded successfully and the upgrade takes effect after the system is powered off or restarted. The following figures show the iBMC WebUIs of different versions.

Figure 3-49 Upgrade completed (iBMC 3.01.08.*x*)

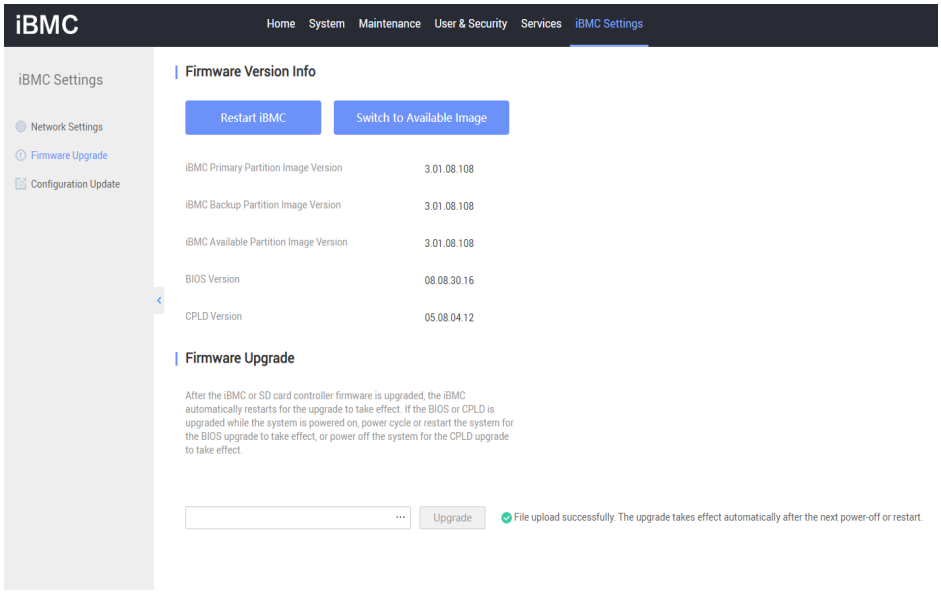


Figure 3-50 Upgrade completed (iBMC 3.01.17.*x*)

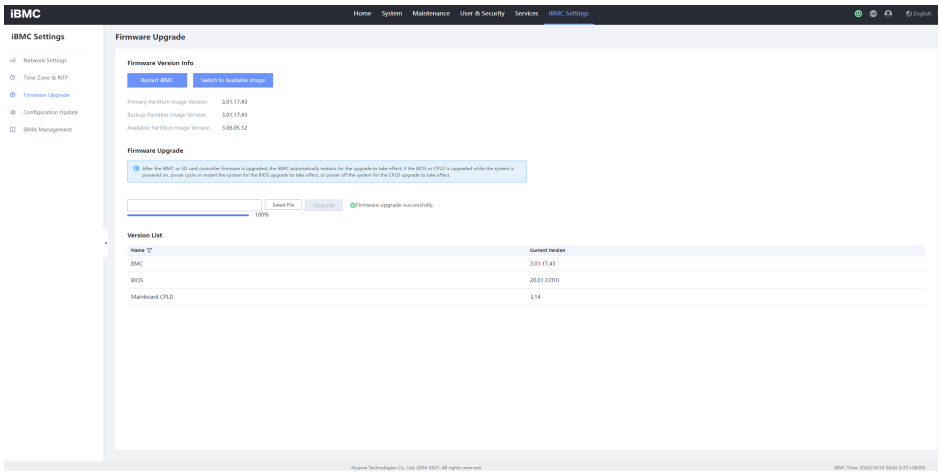


Figure 3-51 Upgrade completed (iBMC 3.09.00.*x* or later)

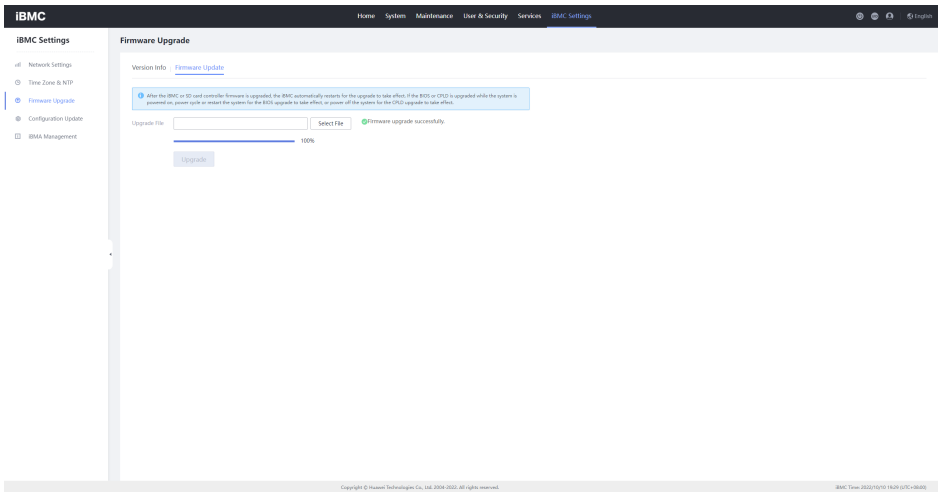
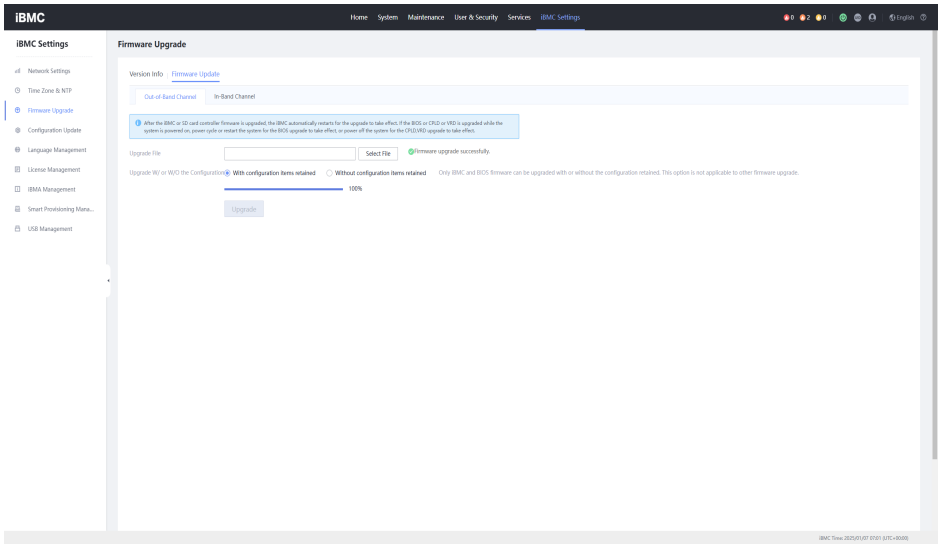


Figure 3-52 Upgrade completed (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 8 Make the upgrade take effect. Select one of the following methods to make the upgrade take effect based on the site requirements.

1. Choose **System** > **Power** > **Power Control**. On the displayed page, click **Power On**. In the displayed dialog box, click **OK**. The following figures show the iBMC WebUIs of different versions.

Figure 3-53 Powering on the system (iBMC 3.01.08.*x*)

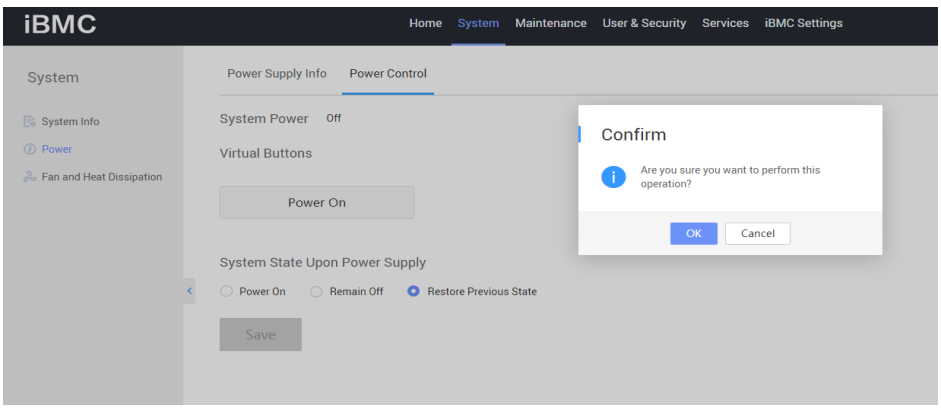
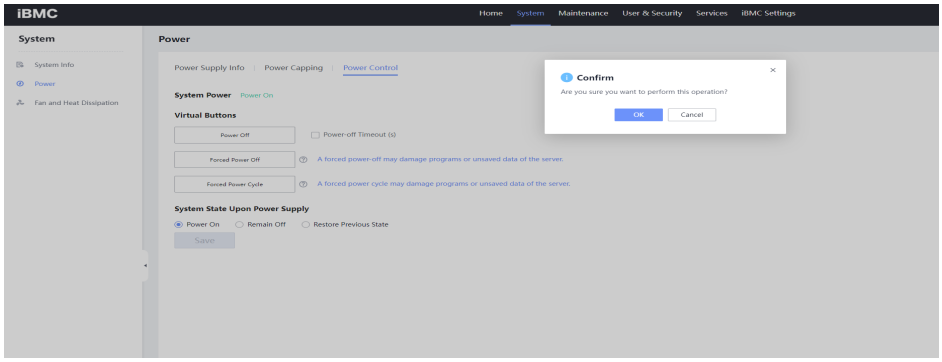


Figure 3-54 Powering on the system (iBMC 3.01.17.*x* or 3.09.00.*x* or later)



NOTE

- The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- After the operation is completed, wait for about 20 to 60 seconds and check whether **System Power** changes to **On**. If **System Power** is **On**, the system has been powered on and the upgrade has taken effect. Otherwise, contact maintenance personnel or technical support engineers.

2. Choose **System** > **Power** > **Power Control**. On the displayed page, click **Forced Power Cycle**. In the displayed dialog box, click **OK**. The following figures show the iBMC WebUIs of different versions. The upgrade takes effect after the system restart is completed.

Figure 3-55 Forced Power Cycle (iBMC 3.01.08.*x*)

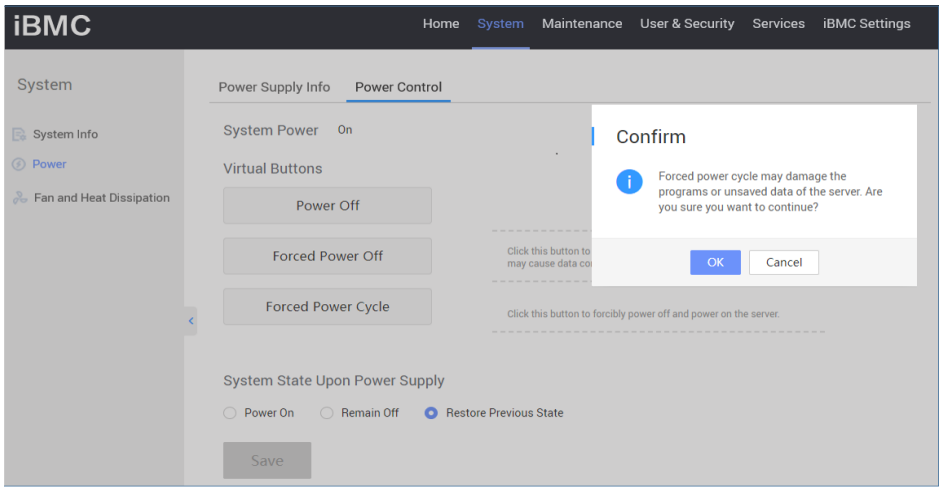


Figure 3-56 Forced Power Cycle (iBMC 3.01.17.*x* or 3.09.00.*x* or later)

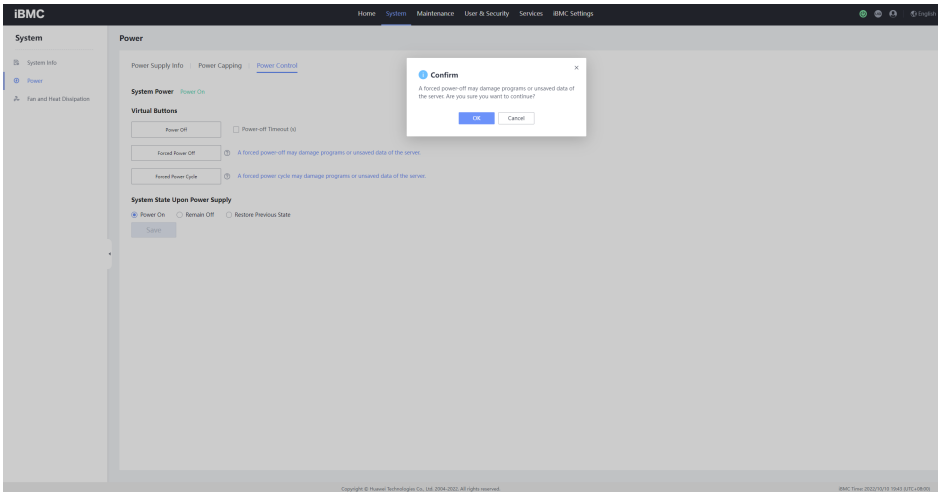
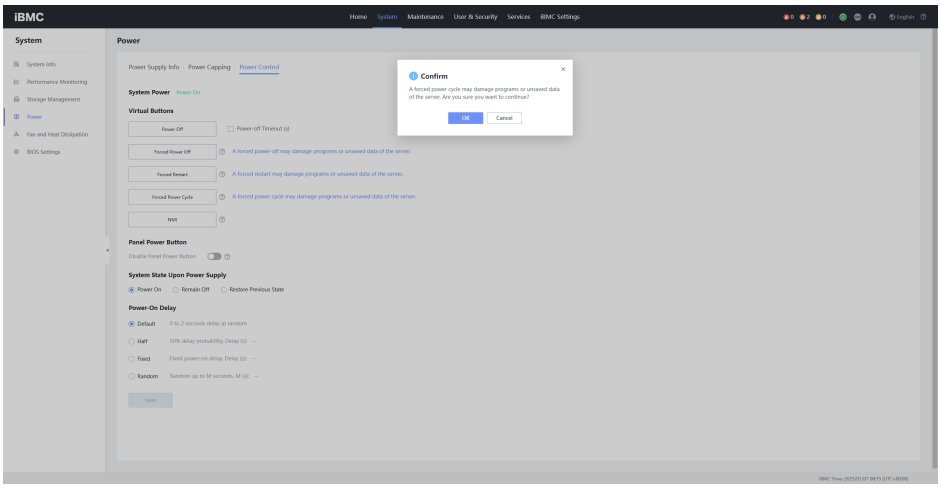


Figure 3-57 Forced Power Cycle (iBMC 3.11.00.25 or later)

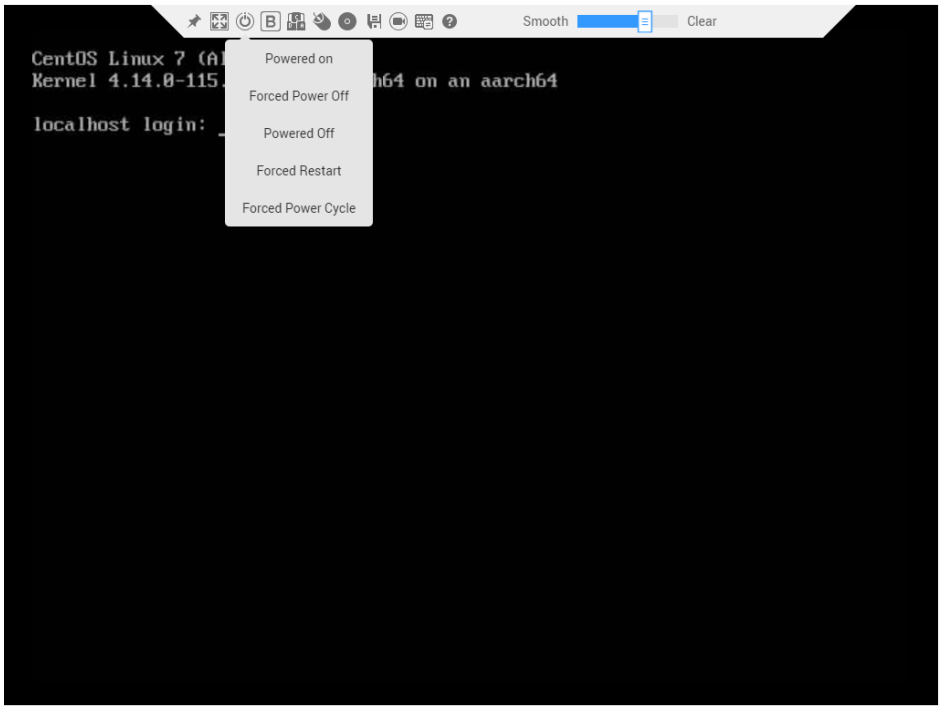


NOTE

- The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- After the operation is completed, wait for about 20 to 60 seconds and check whether **System Power** changes to **On**. If **System Power** is **On**, the system has been powered on and the upgrade has taken effect. Otherwise, contact maintenance personnel or technical support engineers.

3. Click **Forced Power Cycle** on the KVM, as shown in **Figure 3-58**. The upgrade takes effect after the system restarts. The restart takes about 15 minutes.

Figure 3-58 Forced Power Cycle on the KVM

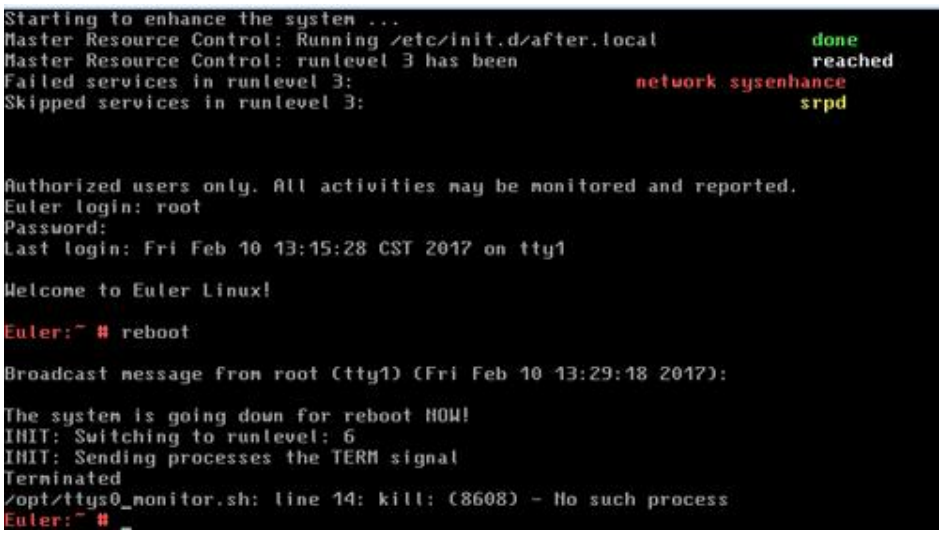


NOTE

The KVM can be used only when the Java environment is configured according to **2.1.1 Logging In to the iBMC WebUI**. Log in to the iBMC WebUI and choose **Home** > **Virtual Console**. Select a KVM login mode (shared mode or private mode) for the remote virtual console.

4. Use the KVM to go the OS and restart the system on the OS page, as shown in **Figure 3-59**. The upgrade takes effect after the system restart is completed. The restart takes about 15 minutes.

Figure 3-59 Restarting the Euler system over the KVM



NOTE

The KVM can be used only when the Java environment is configured according to 2.1.1 Logging In to the iBMC WebUI. Log in to the iBMC WebUI and choose **Home** > **Virtual Console**. Select a KVM login mode (shared mode or private mode) for the remote virtual console.

----End

3.3.3.3 Verifying the Upgrade

After the upgrade is completed, you need to check whether the latest BIOS firmware version takes effect. For details about how to check versions, see 2.1.4.1 Performing a Pre-upgrade Check. If the BIOS version and the version in the **version.xml** file are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.4 Upgrading the Mainboard CPLD

3.3.4.1 Preparing for the Upgrade

3.3.4.1.1 Decompressing the Mainboard CPLD Firmware Package

Upload the mainboard CPLD firmware package to a specified directory on the local PC and decompress the package. For details about how to obtain the firmware package, see 2 Preparing for the Upgrade. Figure 3-60 shows the files in the decompressed firmware package. The firmware package contains two files. Table 3-3 lists these files.

Figure 3-60 Files in a mainboard CPLD firmware package

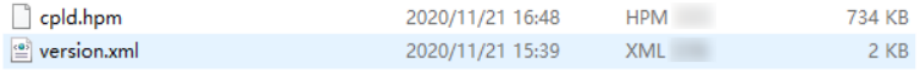


Table 3-3 Description of files in a mainboard CPLD firmware package

File Name	Description
cpld.hpm	CPLD firmware
version.xml	Version configuration table, which records the CPLD firmware version

NOTE

The mainboard CPLD firmware packages for different hardware configurations are in the same format and the upgrade processes are the same. Obtain the mainboard CPLD firmware version based on the actual hardware configuration. If you have any questions, contact the maintenance personnel.

NOTICE

During a mainboard CPLD firmware upgrade, the system needs to be powered off and powered on for the firmware to take effect, which will interrupt services.

3.3.4.1.2 Checking Versions

Check the current mainboard CPLD version on the iBMC WebUI and the version in the **version.xml** file. If the versions are different, an upgrade is necessary. This section describes how to check the versions.

Procedure

Step 1 Log in to the iBMC WebUI. For iBMC 3.01.*x.x*, choose **iBMC Settings** > **Firmware Upgrade**. For iBMC 3.09.00.*x* or later, choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Version Info**. The **Firmware Version Info** page is displayed. The following figures show the iBMC WebUIs of different versions.

Figure 3-61 Querying the mainboard CPLD firmware version (iBMC 3.01.08.*x*)

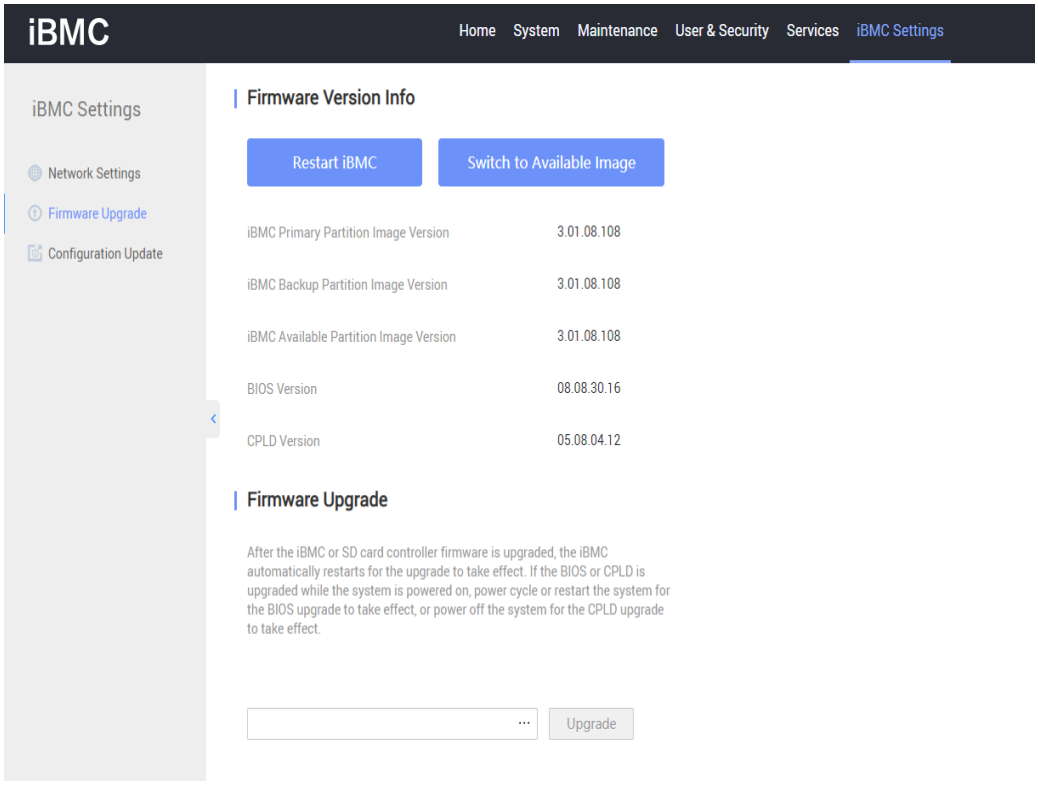


Figure 3-62 Querying the mainboard CPLD firmware version (iBMC 3.01.17.*x*)

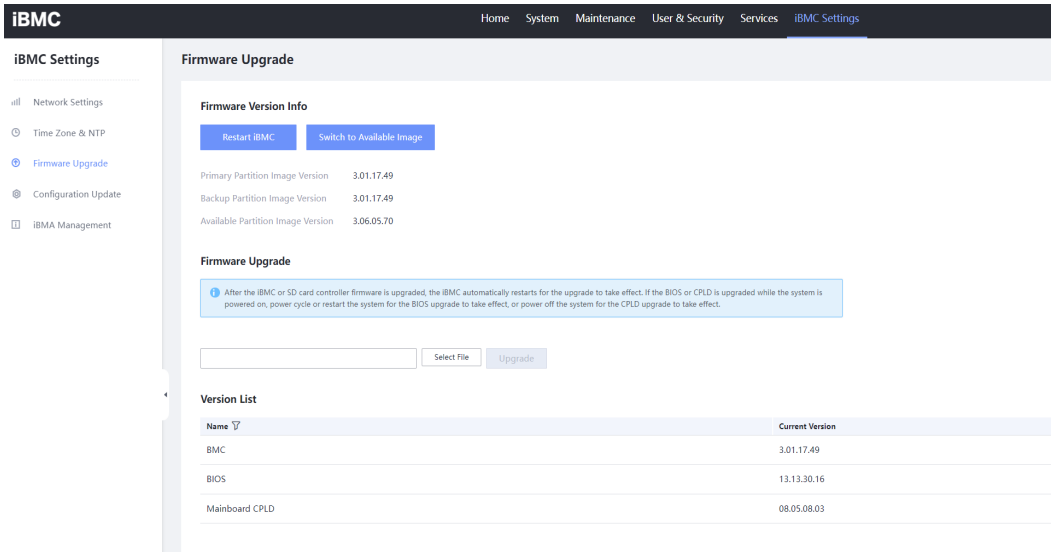


Figure 3-63 Querying the mainboard CPLD firmware version (3.09.00.*x* or later)

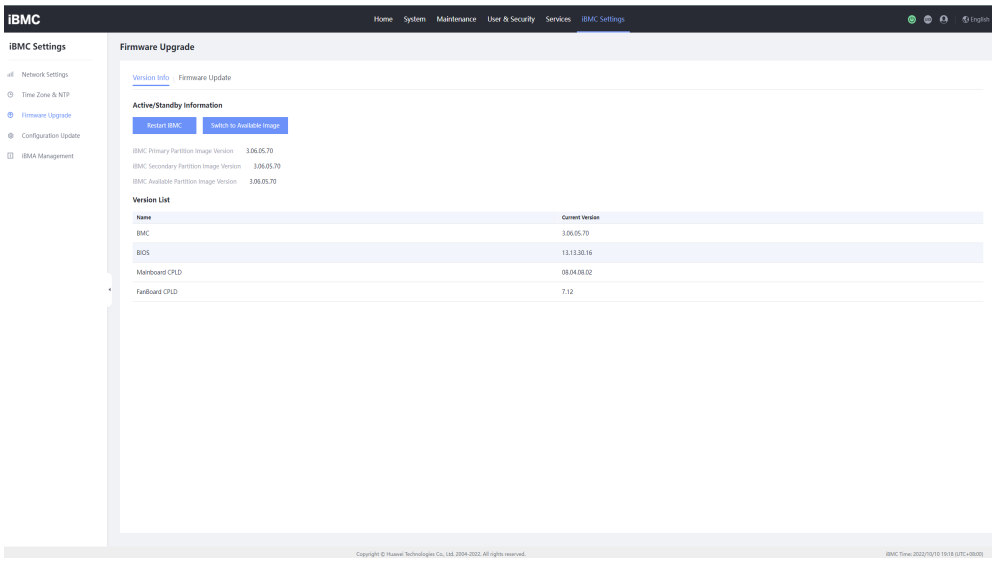
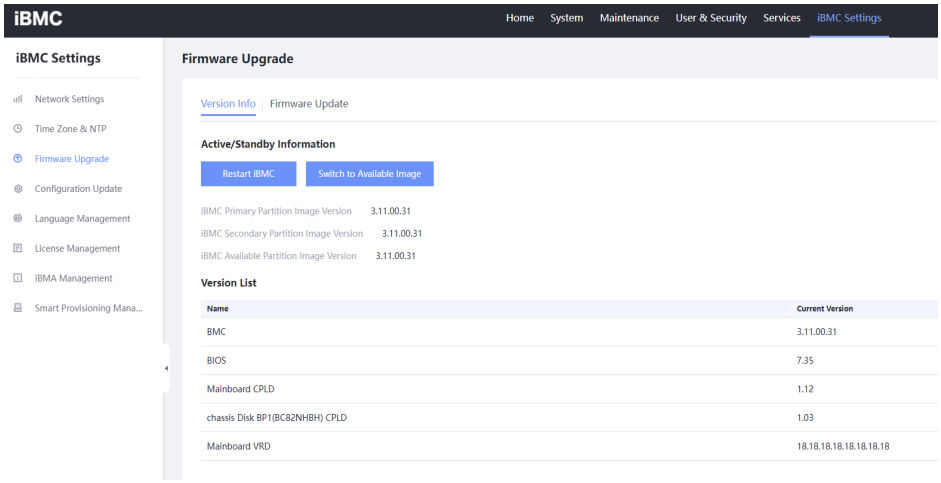


Figure 3-64 Querying the mainboard CPLD firmware version (3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 2 Check the firmware version in the **version.xml** file. For example, the **<Version>01.01.01.00.00.15</Version>** attribute in the configuration file indicates that the mainboard CPLD firmware version is 01.01.01.00.00.15, as shown in **Figure 3-65**.

Figure 3-65 Mainboard CPLD firmware version information contained in the XML file

```
<?xml version="1.0" encoding="utf-8"?>
<FirmwarePackage version="V1.2">
<!--Firmware packages description-->
    <Package>
        <PackageName>PANGEA-V600R005C00-CPLD-MB-Atlantic-V025.zip</PackageName>
        <FileName>PANGEA-V600R005C00-CPLD-MB-Atlantic-V025.zip.hpm</FileName>
        <Version>01.01.01.00.00.15</Version>
        <VersionPattern>(\d+)\.(\d+)\s*$</VersionPattern>
        <FileType>Firmware</FileType>
        <Module>BIOS</Module>
        <Vendor>Huawei Technology Co.</Vendor>
        <SupportModel>PangeaV6_Atlantic</SupportModel>
        <SupportModelUID>0x020d1b00</SupportModelUID>
        <UpgradeAgent>BMC</UpgradeAgent>
        <UpgradeTime>600</UpgradeTime>
        <MaxUpgradeTime>900</MaxUpgradeTime>
        <ActiveMode>ResetServer</ActiveMode>
        <ActiveEffect>None</ActiveEffect>
        <ActiveTime>180</ActiveTime>
        <MaxActivetime>360</MaxActivetime>
        <UpgradeMode>MANUAL</UpgradeMode>
        <Size>2725848</Size>
        <RpmName>Pangea V6R5 Atlantic-CPLD-Firmware</RpmName>
        <Summary>Pangea V6R5 Atlantic-CPLD-Firmware Firmware for Huawei Server.</Summary>
        <Description>Pangea V6R5 Atlantic-CPLD-Firmware Firmware for Huawei Server.</Description>
    </Package>
</FirmwarePackage>
```

----End

3.3.4.2 Performing the Upgrade

After the mainboard CPLD is uploaded on the upgrade page of the iBMC WebUI, the CPLD firmware takes effect only after the system is powered off. Therefore, you need to power off the system. If the system does not have the power backup capability, data may be lost. Therefore, you are advised to upgrade the mainboard CPLD firmware when the system is powered off.

Procedure

Step 1 Log in to the iBMC WebUI.

Step 2 Query the system power status. For iBMC 3.01.08.x, choose **System** > **Power** > **Power Control**. For iBMC 3.01.17.x or 3.09.00.x or later, choose **System** > **Power** > **Power Control**. The **Power Control** page is displayed. Check the value of **System Power**. If the value is **On**, you need to power off the system after the mainboard CPLD is upgraded for the upgrade to take effect. If **System Power** is **Off**, the mainboard CPLD takes effect automatically after the upgrade is complete.

Figure 3-66 Querying the system power status (iBMC 3.01.08.*x*)

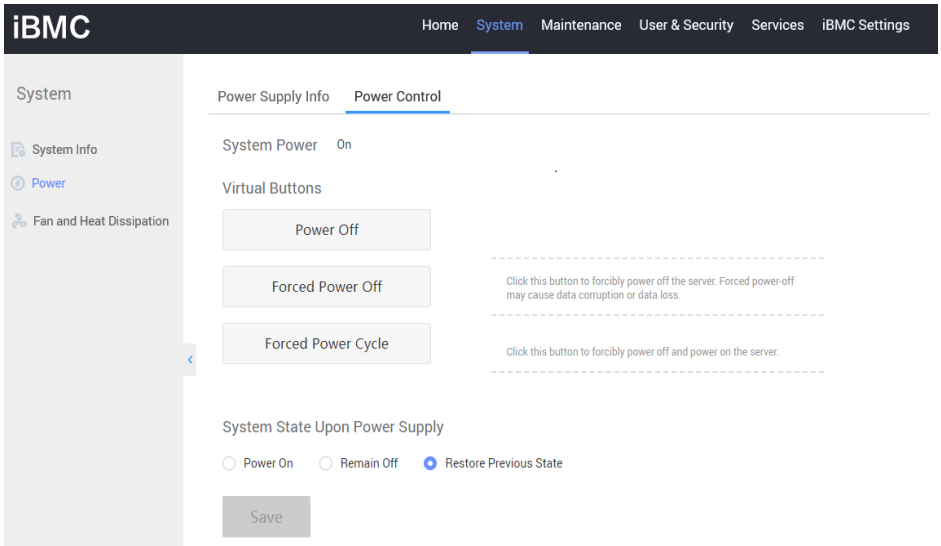


Figure 3-67 Querying the system power status (iBMC 3.01.17.*x* or 3.09.00.*x* or later)

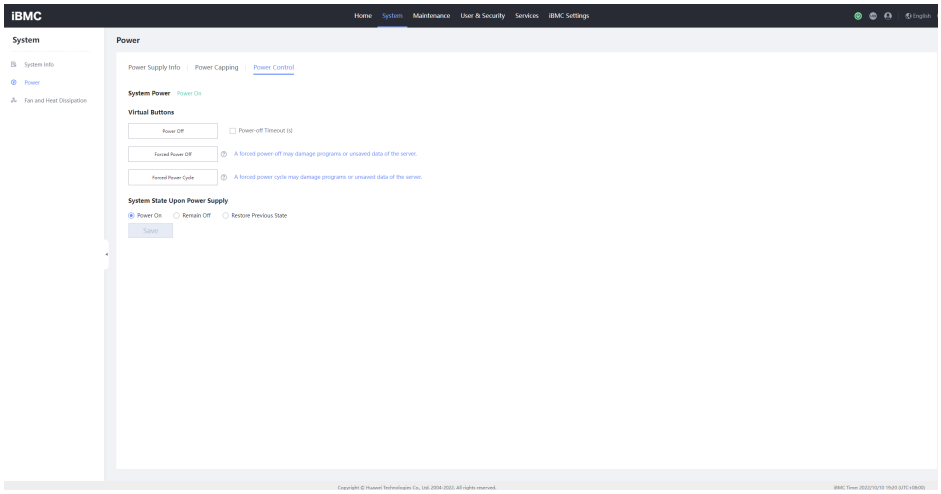
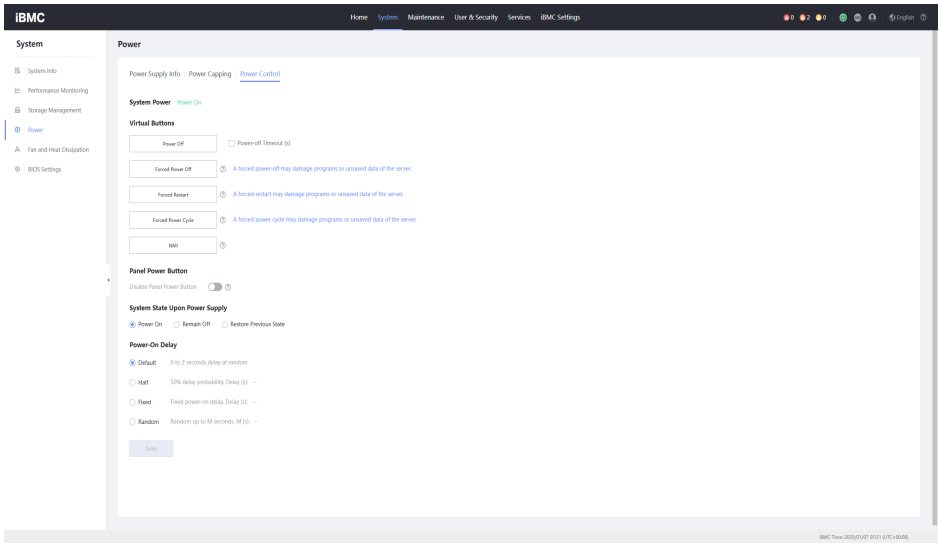


Figure 3-68 Querying the system power status (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 3 Go to the page for firmware upgrade. For iBMC 3.01.x.x, choose **iBMC Settings** > **Firmware Upgrade**. For iBMC 3.09.00.x or later, choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Update**. The **Firmware Upgrade** page is displayed.

Figure 3-69 Firmware Upgrade page (iBMC 3.01.08.*x*)

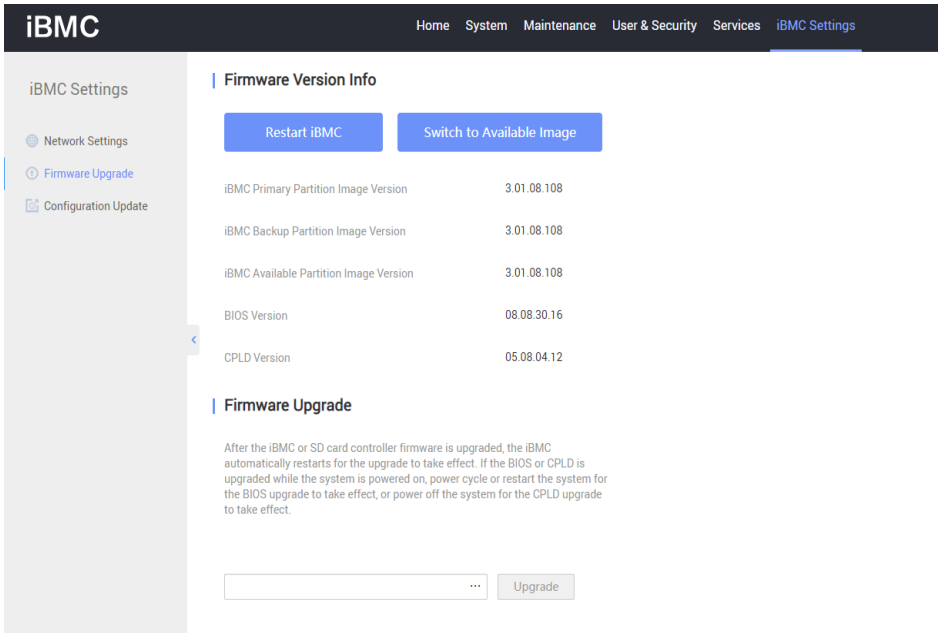


Figure 3-70 Firmware Upgrade page (iBMC 3.01.17.*x*)

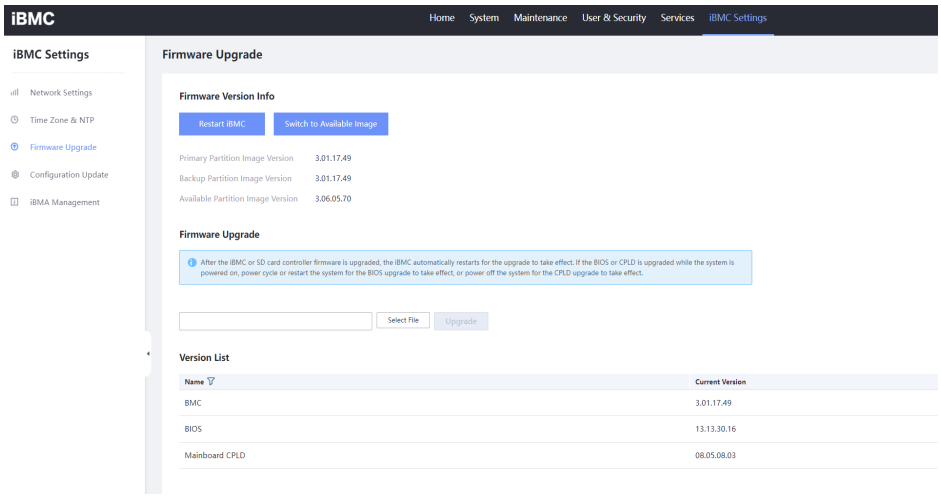


Figure 3-71 Firmware Upgrade page (iBMC 3.09.00.*x* or later)

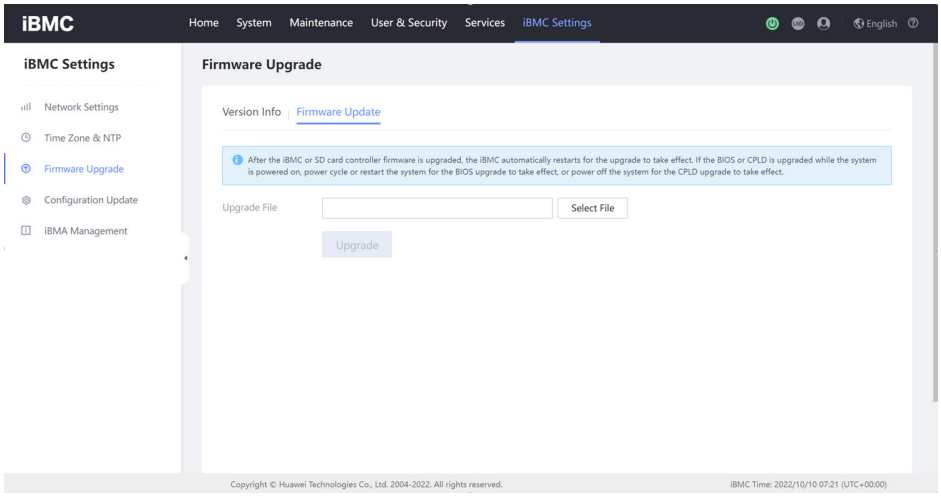
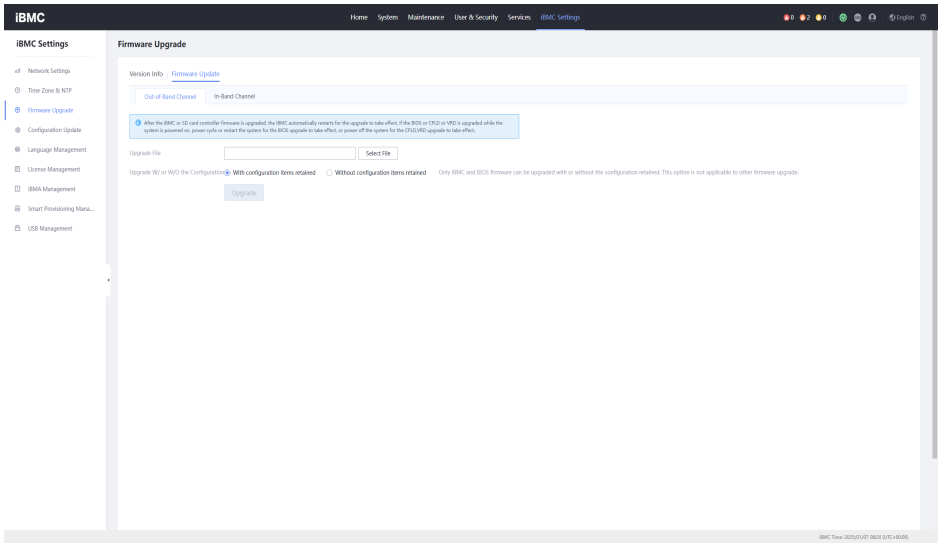


Figure 3-72 Firmware Upgrade page (iBMC 3.11.00.25 or later)



NOTE

The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 4 Select the target firmware. For iBMC 3.01.08.*x*, click ... and select the **cpld.hpm** firmware for upgrade. For iBMC 3.01.17.*x* or 3.09.00.*x* or later, click Select File and select the **cpld.hpm** firmware for upgrade. The following figures show the iBMC WebUIs of different versions.

Figure 3-73 Selecting the target firmware (iBMC 3.01.08.*x*)

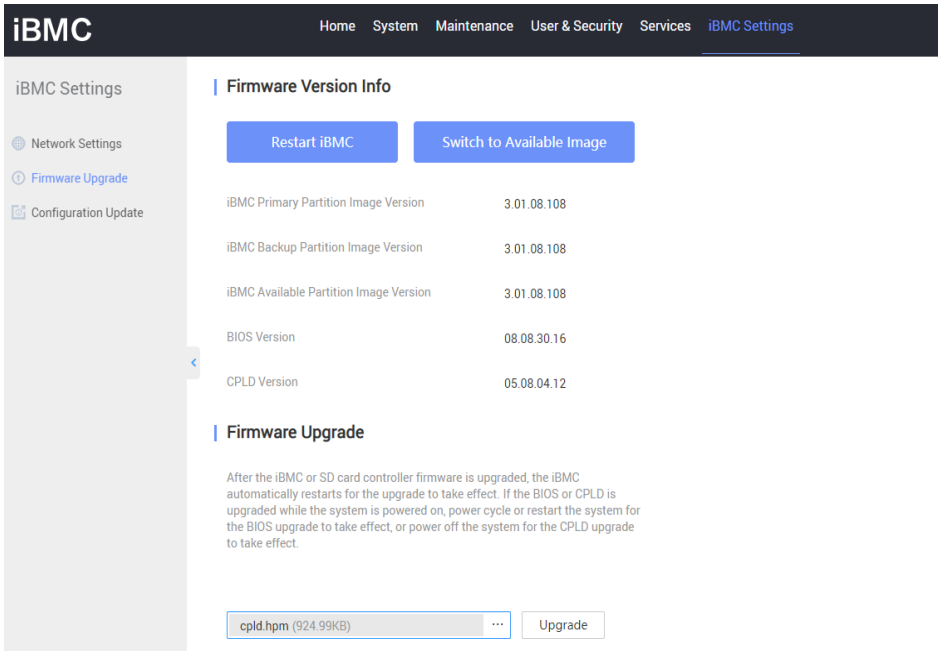


Figure 3-74 Selecting the target firmware (iBMC 3.01.17.*x*)

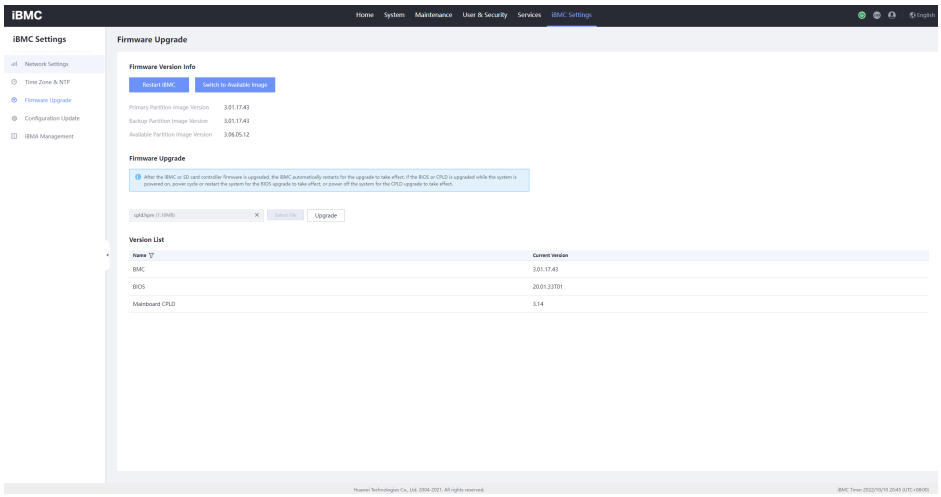


Figure 3-75 Selecting the target firmware (iBMC 3.09.00.*x* or later)

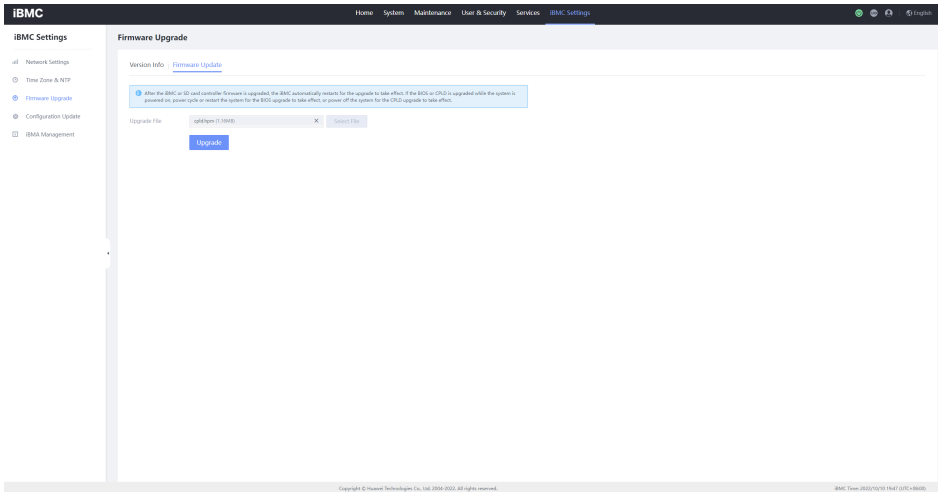
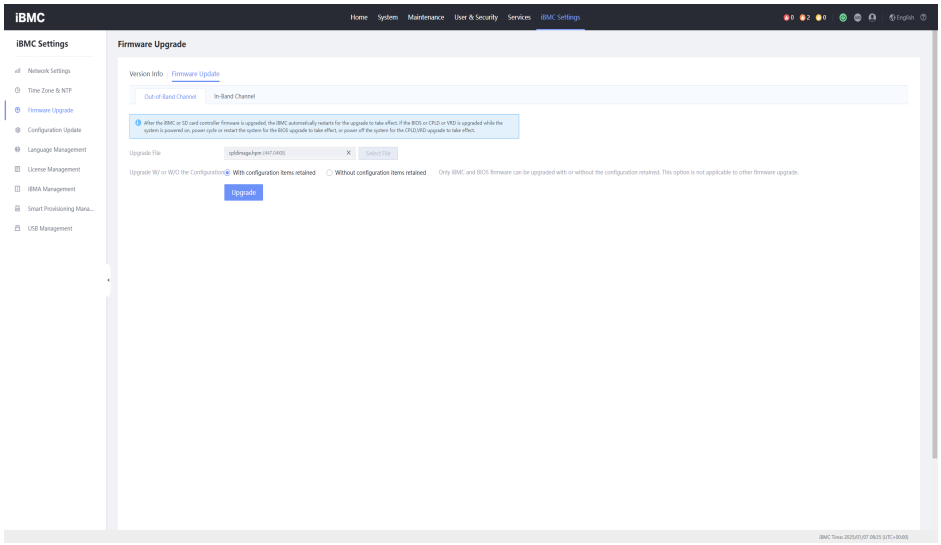


Figure 3-76 Selecting the target firmware (iBMC 3.11.00.25 or later)



NOTE

- The information displayed on this page varies with the iBMC version. Perform operations as instructed on the actual page.
- The mainboard CPLD firmware package varies with the hardware configuration. Select the correct firmware package according to the hardware model. If you have any questions, contact the maintenance personnel.

Step 5 Perform the upgrade. Click **Upgrade**. In the displayed dialog box, click **Yes**.

Figure 3-77 Confirming the firmware upgrade

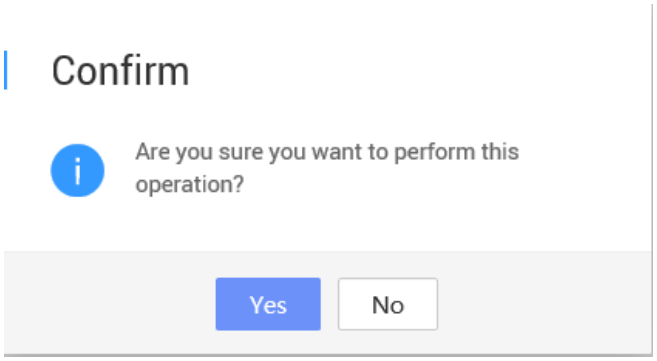


Figure 3-78 Upgrading firmware (iBMC 3.01.08.*x*)

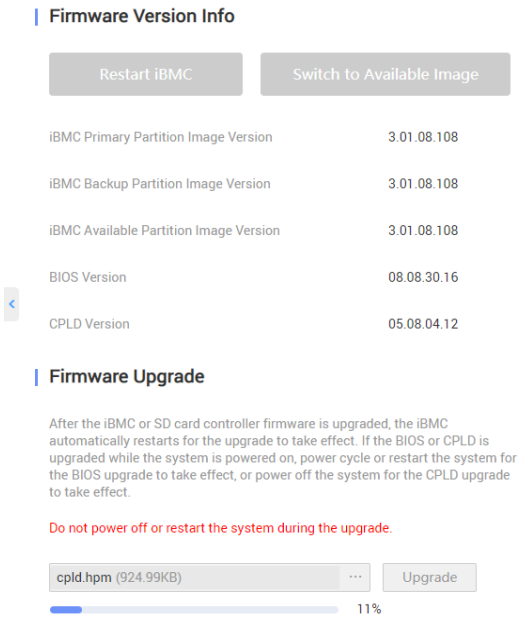


Figure 3-79 Upgrading firmware (iBMC 3.01.17.*x*)

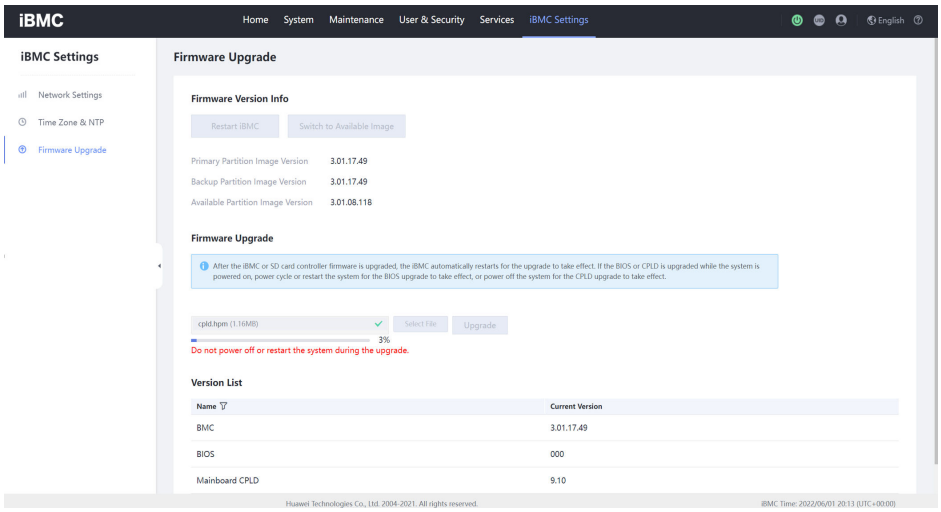


Figure 3-80 Upgrading firmware (iBMC 3.09.00.*x* or later)

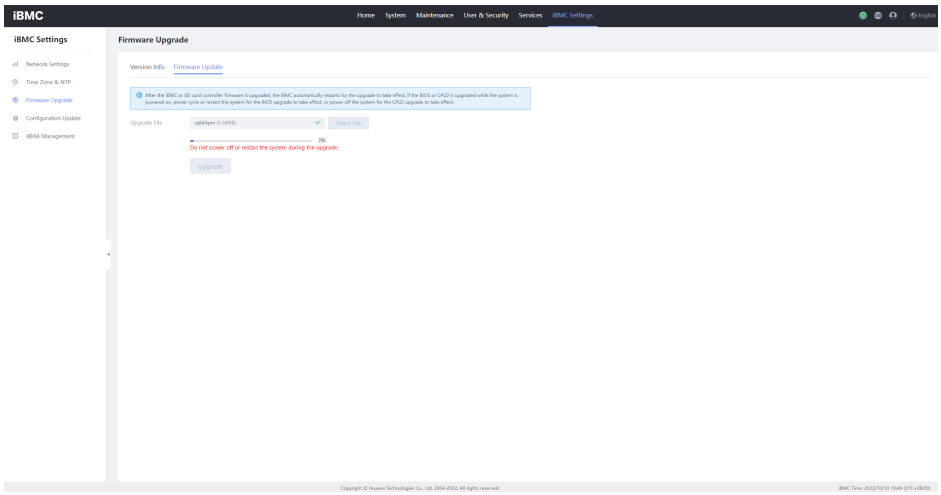
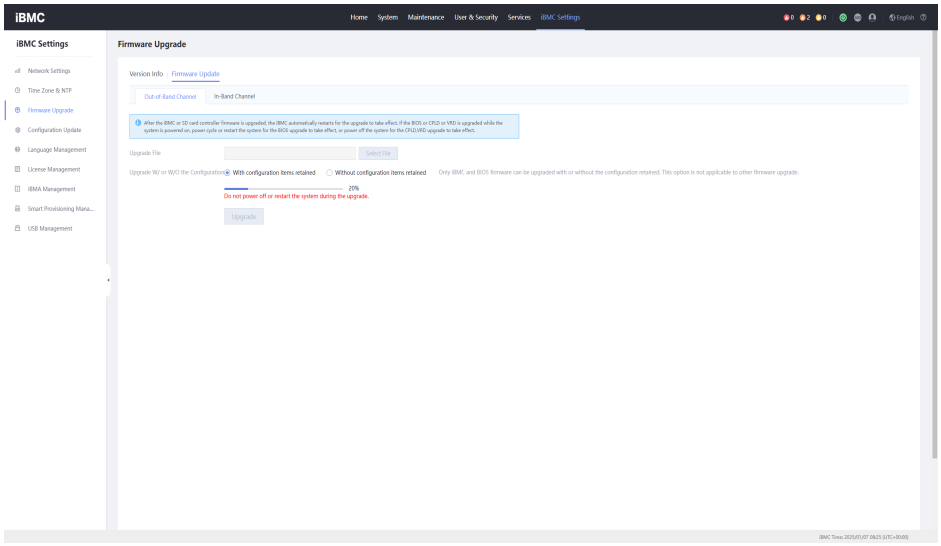


Figure 3-81 Upgrading firmware (iBMC 3.11.00.25 or later)



NOTE

The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

NOTICE

During the firmware upgrade, buttons on the iBMC WebUI are unavailable. Do not perform any other operation before the upgrade is completed. The mainboard CPLD firmware upgrade takes about five minutes. If a fault occurs during the firmware upgrade, see **4.2 iBMC, BIOS, and CPLD Installation/Upgrade Troubleshooting (iBMC V561 or Later, or iBMC V3.01.00.00 or Later)** or contact maintenance or development personnel.

Step 6 Upload the upgrade file. After the upload is completed, a message is displayed, indicating that the upgrade file is uploaded successfully and the upgrade takes

effect after the system is powered off or restarted. The following figures show the iBMC WebUIs of different versions.

Figure 3-82 Upgrade completed (iBMC 3.01.08.*x*)

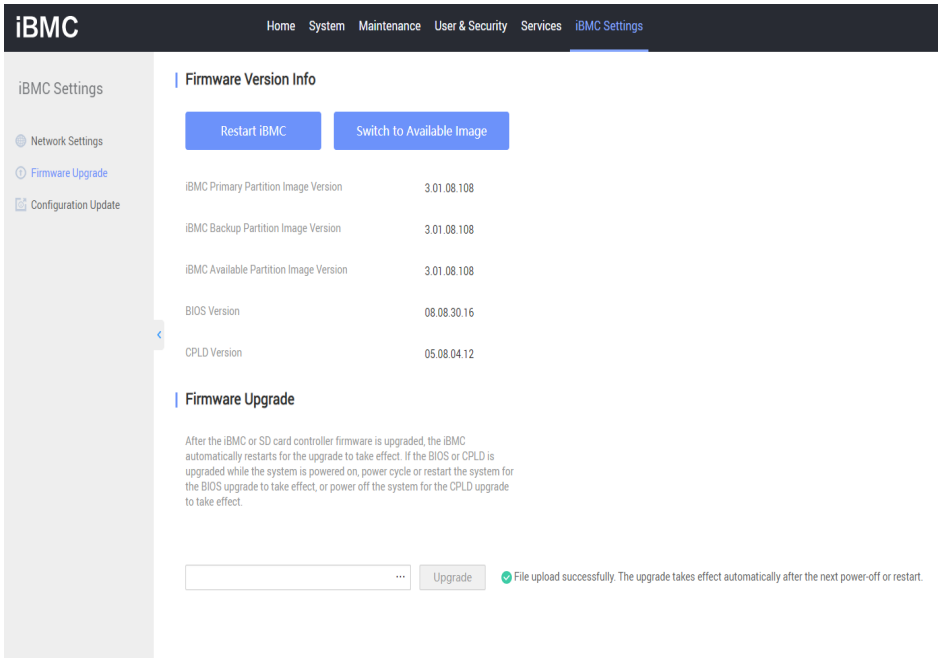


Figure 3-83 Upgrade completed (iBMC 3.01.17.*x*)

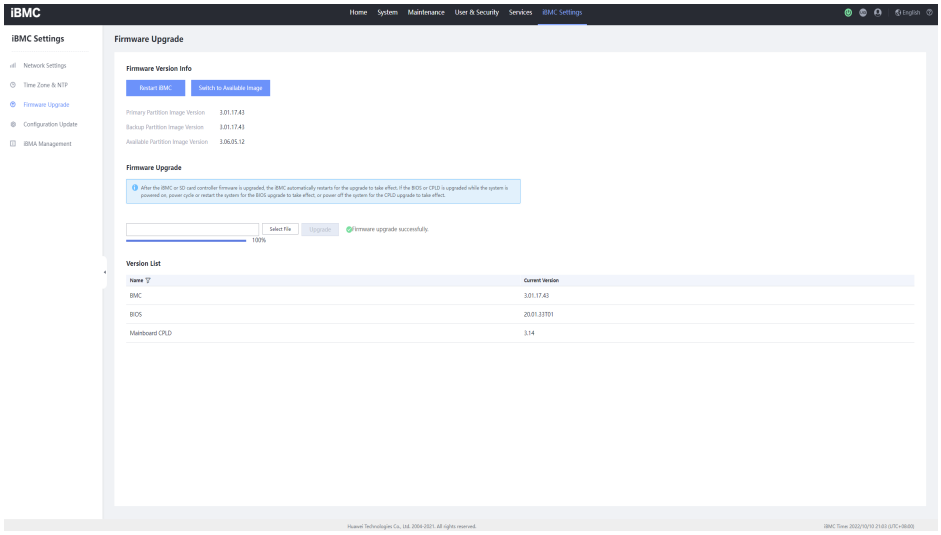


Figure 3-84 Upgrade completed (iBMC 3.09.00.*x* or later)

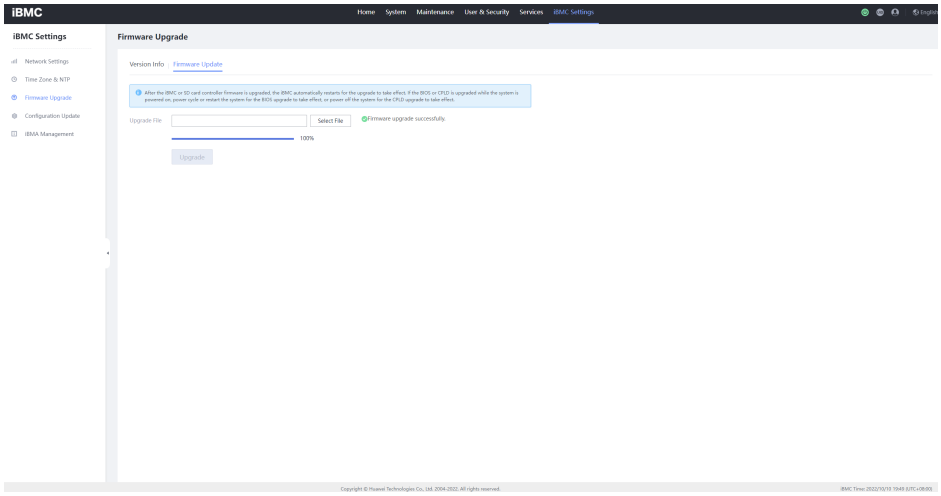
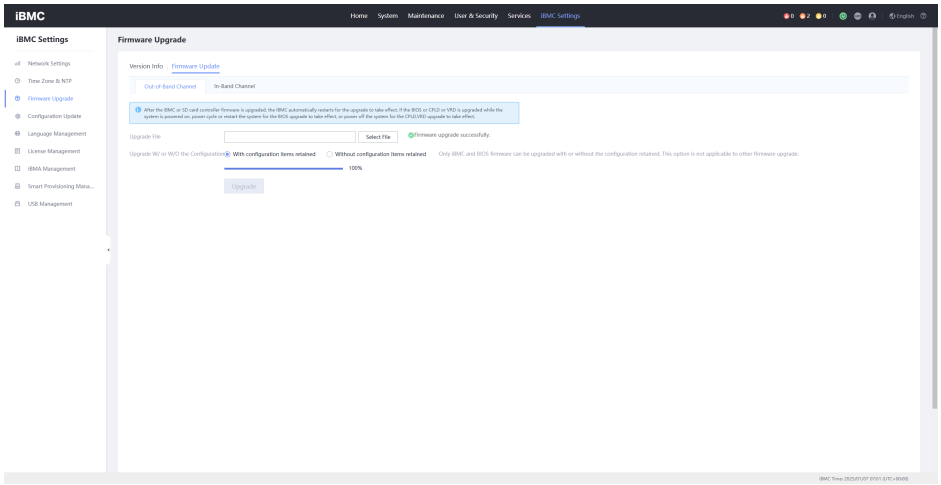


Figure 3-85 Upgrade completed (iBMC 3.11.00.25 or later)



NOTE

The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 7 Make the upgrade take effect. If **System Power** in **Step 2** is **On**, forcibly power off the system. Otherwise, do not perform any operation. Perform either of the following operations to make the upgrade take effect.

1. Choose **System** > **Power** > **Power Control**. On the displayed page, click **Forced Power Cycle**. In the displayed dialog box, click **OK**. The following figures show the iBMC WebUIs of different versions.

Figure 3-86 Forced Power Cycle (iBMC 3.01.08.*x*)

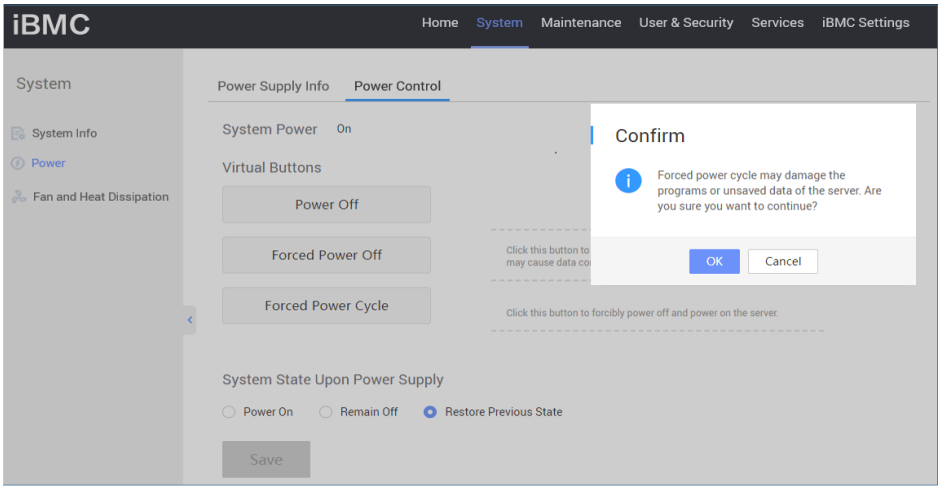


Figure 3-87 Forced Power Cycle (iBMC 3.01.17.*x* or 3.09.00.*x* or later)

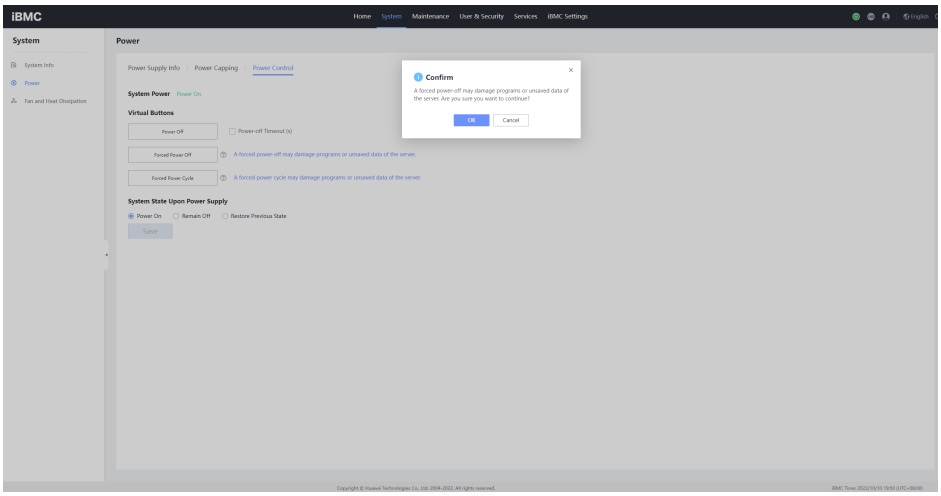
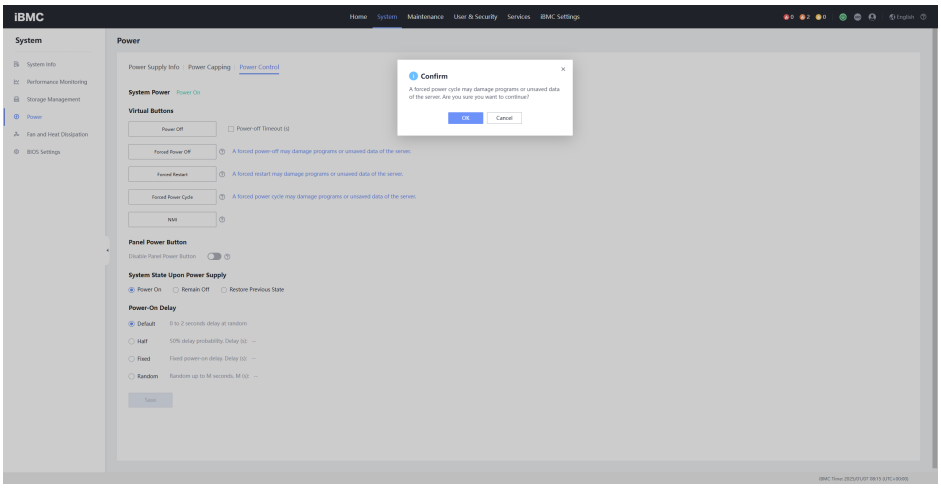
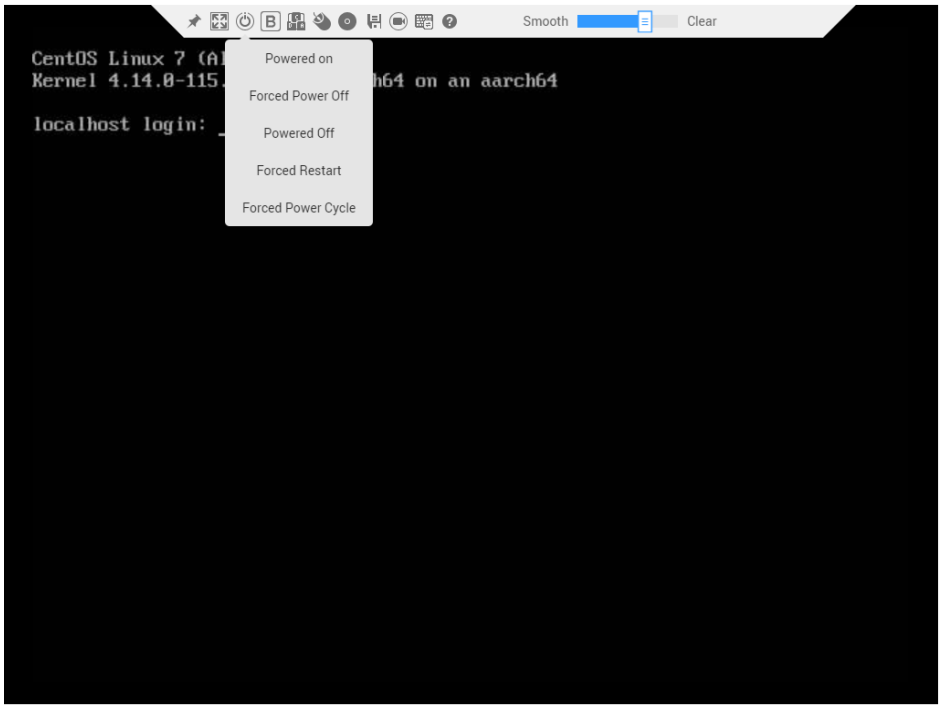


Figure 3-88 Forced Power Cycle (iBMC 3.11.00.25 or later)



2. Click **Forced Power Cycle** on the KVM, as shown in **Figure 3-89**.

Figure 3-89 Forced Power Cycle on the KVM



NOTE

- The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- The KVM can be used only when the Java environment is configured according to **2.1.1 Logging In to the iBMC WebUI**. Log in to the iBMC WebUI and choose **Home** > **Virtual Console**. Select a KVM login mode (shared mode or private mode) for the remote virtual console.

----End

3.3.4.3 Verifying the Upgrade

After the upgrade is completed, you need to check whether the latest mainboard CPLD firmware version takes effect. For details about how to check versions, see **3.3.4.1.2 Checking Versions**. If the mainboard CPLD version and the version in the **version.xml** file are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.5 PMC Expander Firmware

NOTE

- The firmware can be upgraded only for 12-slot and 25-slot disk backplane expanders.
- After the disk backplane firmware is upgraded, restart the system for the upgrade to take effect. Before the upgrade, ensure that the host is in maintenance mode and services have been migrated to other nodes.
- Before the upgrade, you are advised to upgrade the RAID controller card firmware driver to the matching version by referring to **3.3.7 Installing/Upgrading the RAID Controller Card Firmware and Driver**.

3.3.5.1 Preparing for the Upgrade

Table 3-4

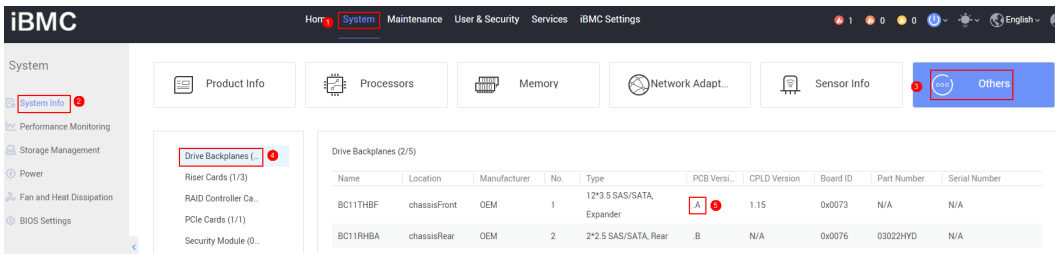
Firmware	Version	Firmware Package	How to Obtain
12-slot 3.5-inch EXP backplane expander firmware (pm8053)	140	TS200-2280-2180-TS100-2280-2180-2288HV5-2288HV3-5288V5-5288V3-12HDD-Expander-Backplane(BC1THBF02)_140_Firmware_ARM_x86.zip	Click here.
12-slot 3.5-inch EXP backplane expander firmware (pm8054)	340	TS200-2280-2180-TS100-2280-2180-2288HV5-2288HV3-5288V5-5288V3-(8054+12)HDD-Expander-Backplane(BC11THBQA01)_340_Firmware_ARM_x86.zip	Click here.
25-slot 2.5-inch EXP backplane expander firmware	140	TS200-2280-2180-2480-TS100-2280-2288HV5-2288HV3-2488HV5-5885HV5-25HDD-Expander-Backplane(BC1THBH02)_140_Firmware_ARM_x86.zip	Click here.

Checking the Backplane Type

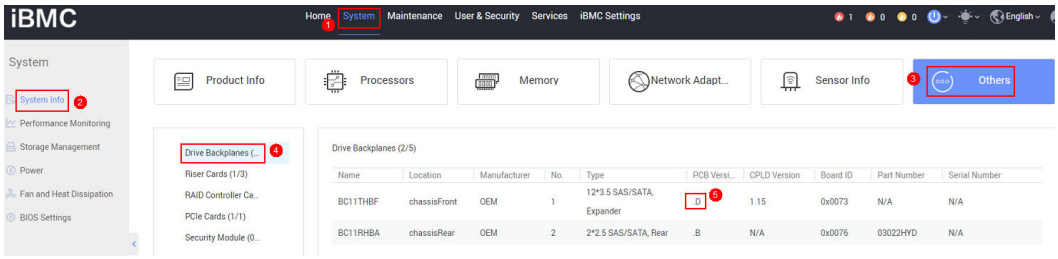
Step 1 Log in to the BMC WebUI and choose **System** > **System Info** > **Others** > **Drive Backplanes**.

Step 2 Check the PCB version of the corresponding 12-slot backplane.

PCB version .A of disk backplane 12*3.5 SAS/SATA Expander indicates the PM8053 chip backplane, as shown in the following figure.



PCB version .D of disk backplane 12*3.5 SAS/SATA Expander indicates the PM8054 chip backplane, as shown in the following figure.



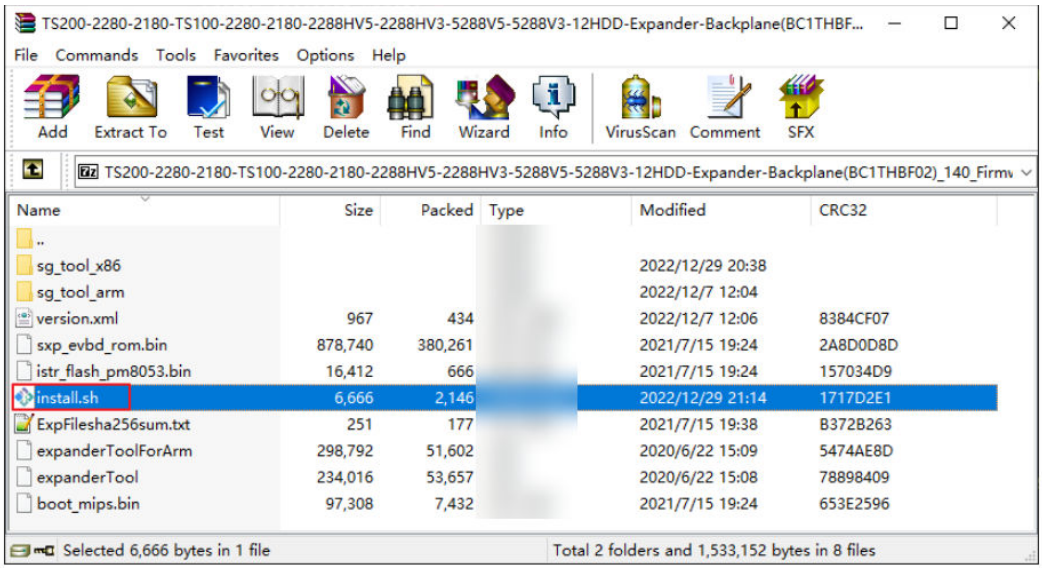
----End

3.3.5.2 Upgrading the Firmware

Checking Whether the install.sh Script Exists in the Software Package

Step 1 Use the decompression tool to view the files in the software package.

Step 2 Check whether the **install.sh** script exists. If the following information is displayed, the script exists. Otherwise, the script does not exist.

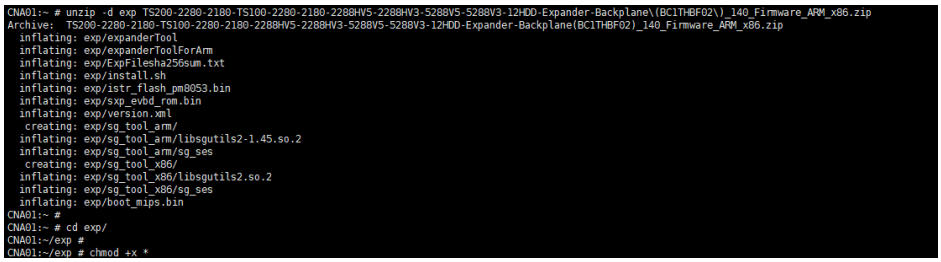


----End

3.3.5.2.1 Performing the Upgrade (With the install.sh Script)

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Upload the firmware package to the system and decompress it. Run the **chmod +x *** command to add the execute permission for all files.



Step 3 Run the **./install.sh upgrade** command to perform an automatic upgrade. If the following information is displayed, the upgrade is successful.

```
CNA01:~/exp # ll
total 1524
-rwxr-x--- 1 root root  97308 Jul 15  2021 boot_mips.bin
-rwxr-x--- 1 root root 234016 Jun 22  2020 expanderTool
-rwxr-x--- 1 root root 298792 Jun 22  2020 expanderToolForArm
-rwxr-x--- 1 root root    251 Jul 15  2021 ExpFilesha256sum.txt
-rwxr-x--- 1 root root   6666 Dec 29  2022 install.sh
-rwxr-x--- 1 root root  16412 Jul 15  2021 istr_flash_pm8053.bin
drwxr-x--- 2 root root   4096 Dec  7  2022 sg_tool_arm
drwxr-x--- 2 root root   4096 Dec 29  2022 sg_tool_x86
-rwxr-x--- 1 root root 878740 Jul 15  2021 sxp_evbd_rom.bin
-rwxr-x--- 1 root root    967 Dec  7  2022 version.xml
CNA01:~/exp #
CNA01:~/exp # ./install.sh upgrade
This is PM8053.
istr_flash_pm8053.bin
File verification succeeded.
Update boot mips...
Update init string...
Update firmware...
Update finished! Manually power off and then power on for the upgrade to take effect...
The current_boot_image is 0
The next_boot_image is 1
Manually power off and then power on for the upgrade to take effect.
CNA01:~/exp #
```

CAUTION

Do not power off or reset the system during the upgrade.

Strictly follow the upgrade guide to perform the upgrade. Do not perform the upgrade repeatedly. Otherwise, the backplane may fail to start.

Step 4 Run the **ipmitool power cycle** command to power off and then power on the server for the disk backplane firmware to take effect.

----End

3.3.5.2.2 Performing the Upgrade (Without the install.sh Script)

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Upload the firmware package to the system and decompress it. Run the **chmod +x *** command to add the execute permission for all files.

```
SCNA:~ # unzip -d exp TS200-2280-2180-2480-TS100-2280-2288HV5-2288HV3-2488HV5-588SHV5-25HDD-Expander-Backplane\(BC1THBH02\)_140_Firmware_ARM_x86.zip
Archive:  TS200-2280-2180-2480-TS100-2280-2288HV5-2288HV3-2488HV5-588SHV5-25HDD-Expander-Backplane(BC1THBH02)_140_Firmware_ARM_x86.zip
  inflating: exp/boot_mips.bin
  inflating: exp/expanderTool
  inflating: exp/expanderToolForArm
  inflating: exp/ExpFilesha256sum.txt
  inflating: exp/istr_flash_pm8054.bin
  inflating: exp/sxp_evbd_rom.bin
SCNA:~ #
SCNA:~ # cd exp/
SCNA:~/exp #
SCNA:~/exp # chmod +x *
SCNA:~/exp #
SCNA:~/exp # ll
total 1504
-rwxr-x--- 1 root root  97308 Jul 15  2021 boot_mips.bin
-rwxr-x--- 1 root root 234016 Jun 22  2020 expanderTool
-rwxr-x--- 1 root root 298792 Jun 22  2020 expanderToolForArm
-rwxr-x--- 1 root root    251 Jul 27  2021 ExpFilesha256sum.txt
-rwxr-x--- 1 root root  16412 Jul 15  2021 istr_flash_pm8054.bin
-rwxr-x--- 1 root root 878740 Jul 15  2021 sxp_evbd_rom.bin
SCNA:~/exp #
```

Step 3 Run the **lsscsi -g** command to query the sg device ID of the disk backplane.

The **Expander** identifier in the command output indicates the disk backplane, for example, **/dev/sg0** in the command output.


```
SCNA:~/exp # lsscsi -g
[0:1:123:0]  enclosu HUAWEI   Expander 12G28F0 140   -          /dev/sg0
[0:2:0:0]    disk    HUAWEI   HSSD-D7T23AL3T8N 3308  /dev/sda   /dev/sg1
[0:2:1:0]    disk    HUAWEI   HSSD-D7T23AL3T8N 3308  /dev/sdb   /dev/sg2
[0:2:2:0]    disk    HUAWEI   HSSD-D7T23AL3T8N 3308  /dev/sdc   /dev/sg3
[0:2:3:0]    disk    HUAWEI   HSSD-D7T23AL3T8N 3308  /dev/sdd   /dev/sg4
[0:2:4:0]    disk    HUAWEI   HSSD-D7T23AL3T8N 3308  /dev/sde   /dev/sg5
[0:2:5:0]    disk    HUAWEI   HSSD-D7T23AL3T8N 3308  /dev/sdf   /dev/sg6
[0:3:111:0]  disk    BROADCOM MR9560-8i        5.20  /dev/sdg   /dev/sg7
[15:0:0:0]   cd/dvd  Virtual  DVD-ROM VM 1.1.0  225  /dev/sr0   /dev/sg8
SCNA:~/exp #
```

Step 4 Run the **./expanderTool query /dev/***sg device ID corresponding to the expander* command to query the firmware version. If the firmware version is inconsistent with the matching version, upgrade the firmware.

NOTE

For TaiShan servers, use Arm version tool expanderToolForArm in the firmware package to replace expanderTool of the x86 version.

CAUTION

Do not power off or reset the system during the upgrade.

Strictly follow the upgrade guide to perform the upgrade. Do not perform the upgrade repeatedly. Otherwise, the backplane may fail to start.

Step 5 Run the following command to upgrade the boot file:

./expanderTool download=boot_mips.bin /dev/*sg device number corresponding to the expander*

```
SCNA:~/exp # ./expanderTool download=boot_mips.bin /dev/sg0
Please Wait for downloading...
Firmware update success!
SCNA:~/exp #
```

Step 6 Run the following command to upgrade the firmware configuration file:

./expanderTool download=istr_flash_*Chip model*.bin /dev/*sg device number corresponding to the expander*

```
SCNA:~/exp # ./expanderTool download=istr_flash_pm8054.bin /dev/sg0
Please Wait for downloading...
Firmware update success!
SCNA:~/exp #
```

Step 7 Run the following command to upgrade the firmware file:

./expanderTool download=sxp_evbd_rom.bin /dev/*sg device number corresponding to the expander*

```
SCNA:~/exp # ./expanderTool download=sxp_evbd_rom.bin /dev/sg0
Please Wait for downloading...
Swap active rom...
Firmware update success!
SCNA:~/exp #
```

Step 8 Run the **ipmitool power cycle** command to power off and then power on the server for the disk backplane firmware to take effect.

----End

3.3.5.3 Verifying the Upgrade

Step 1 After the system is powered on, log in to the OS again and switch to user **root**.

Step 2 Run the **./expanderTool query /dev/***sg device ID corresponding to the expander* command to check whether the firmware version is the target version. As shown in the following figure, the configuration file version and firmware version have been upgraded to **140**.

```
SCNA:~/exp # ./expanderTool query /dev/sg0
Active Image:  image0
Image Version: 140
Active Data:   data0
Data Version:  140
```

----End

3.3.6 Upgrading the CPLD Firmware of a Data Cluster Module

The procedure for upgrading the CPLD firmware for a data cluster module is the same as that for upgrading the mainboard CPLD firmware. After downloading the CPLD firmware of a data cluster module, upgrade it by following instructions in **3.3.4 Upgrading the Mainboard CPLD**.

CAUTION

If the CPLD firmware of two data cluster modules is upgraded at the same time, services may be interrupted. Contact technical support engineers to determine the upgrade scheme and then perform the upgrade.

3.3.7 Installing/Upgrading the RAID Controller Card Firmware and Driver

3.3.7.1 Installing the RAID Controller Card CLI Tool

Querying the RAID Controller Card Model

NOTE

The RAID CLI tool may be used in the following operations. For details about how to obtain and install the RAID CLI tool, see **Obtaining the RAID Controller Card Tool**.

Step 1 Run the following commands in sequence and check whether any command output is displayed:

- **lspci | grep -i LSI**
  a. If the following command output is displayed, the BROADCOM RAID controller card is used in the environment. In this case, obtain and install the corresponding RAID CLI tool by following instructions provided in **Obtaining the RAID Controller Card Tool**. Then go to **Step 2**.

The following command output uses SAS3508 as an example:

```
[root@localhost ~]# lspci | grep -i LSI
02:00.0 RAID bus controller: LSI Logic / Symbios Logic MegaRAID Tri-Mode SAS3508 (rev 01)
```

b. If no command output is displayed, run the subsequent commands to check whether any command output is displayed.

- **lspci | grep -i PQI**

  a. If the following command output is displayed, the MICROSEMI RAID controller card is used in the environment. In this case, obtain and install the corresponding RAID CLI tool by following instructions provided in **Obtaining the RAID Controller Card Tool**. Then go to **Step 3**.

  The following command output uses SAS3152 as an example:

  ```
  [root@localhost ~]# lspci | grep -i PQI
  5e:00.0 Serial Attached SCSI controller: Adaptec Smart Storage PQI 12G SAS/PCIe 3 (rev 01)
  ```

  b. If no command output is displayed, run the subsequent commands to check whether any command output is displayed.

- **lspci | grep -iE "3758"**

  a. If the following command output is displayed, the HUAWEI SP686C-M-16i/SP686C-M-40i RAID controller card is used in the environment. In this case, obtain and install the corresponding RAID CLI tool by following instructions provided in **Obtaining the RAID Controller Card Tool**.

  The command output is as follows:

  ```
  [root@localhost ~]# lspci | grep -iE "3758"
  87:00.0 RAID bus controller: Huawei Technologies Co., Ltd. Device 3758 (rev 21
  ```

  b. If no command output is displayed, run the subsequent commands to check whether any command output is displayed.

- **lspci | grep -iE "3858"**

  a. If the following command output is displayed, the HUAWEI SP186-M-8i RAID controller card is used in the environment. In this case, obtain and install the corresponding RAID CLI tool by following instructions provided in **Obtaining the RAID Controller Card Tool**.

  The command output is as follows:

  ```
  [root@localhost ~]# lspci | grep -iE "3858"
  01:00.0 RAID bus controller: Huawei Technologies Co., Ltd. Device 3858 (rev 21)
  ```

  b. If no command output is displayed, no RAID controller card is used in the environment. No further action is required.

Step 2 Run the following commands to query the RAID controller card information:

```
[root@localhost ~]# /opt/MegaRAID/storcli/storcli64 show
Status Code = 0
Status = Success
Description = None

Number of Controllers = 1
Host Name = localhost.localdomain
Operating System  = Linux 4.19.36-vhulk1907.1.0.h619.eulerosv2r8.aarch64
StoreLib IT Version = 07.0400.0200.0400

System Overview :
===============

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



```
 0 SAS3508    8  14   1    0   1    0 Opt On  1&2 Y      3 Opt
-----------------------------------------------------------------------

Ctl=Controller Index|DGs=Drive groups|VDs=Virtual drives|Fld=Failed
PDs=Physical drives|DNOpt=DG NotOptimal|VNOpt=VD NotOptimal|Opt=Optimal
Msng=Missing|Dgd=Degraded|NdAtn=Need Attention|Unkwn=Unknown
sPR=Scheduled Patrol Read|DS=DimmerSwitch|EHS=Emergency Hot Spare
Y=Yes|N=No|ASOs=Advanced Software Options|BBU=Battery backup unit
Hlth=Health|Safe=Safe-mode boot
```

If the value of **Number of Controllers** is not **0** in the preceding command output, the BROADCOM RAID controller card is used in the environment and the RAID controller card information is displayed in the command output.

Step 3 Run the following commands to query the RAID controller card information:

```
[root@localhost ~]# arcconf list
Controllers found: 1
----------------------------------------------------------------------
Controller information
----------------------------------------------------------------------
  Controller ID              : Status, Slot, Mode, Name, SerialNumber, WWN
----------------------------------------------------------------------
  Controller 1:              : Optimal, Slot 3, Mixed, Adaptec SmartRAID 3152-8i, 9A38F300930,
50000D1E002AEA80

Command completed successfully.
```

If the value of **Controllers found** is not **0** in the preceding command output, the MICROSEMI RAID controller card is used in the environment and the RAID controller card information is displayed in the command output.

----End

Obtaining the RAID Controller Card Tool

You can obtain the CLI tool of the RAID controller card from the version mapping of the corresponding version as follows:

Step 1 Find the firmware download link of the corresponding RAID controller card model in the version mapping and click it for downloading. (For details about the mappings between RAID controller card models and tools, see the following note.)

NOTE

- The common tool for the BROADCOM 3004iMR, 3108, 3408IT, 3408iMR, 3416IT, 3416iMR, 3508, 3516, and 3908 RAID controller cards is StorCLI.
- The common tool for the BROADCOM 3008IR and 3008IT RAID controller cards is SAS3IRCU.
- The common tool for the MICROSEMI 3152-8i, FBGF-RAD-R1-S1, and 2100-8i RAID controller cards is ARCCONF.
- The common tool for the HUAWEI SP686C-M-16i, SP686C-M-40i, and SP186-M-8i RAID controller cards is hiraidadm.

Step 2 Decompress the downloaded firmware package and find the required tool in the decompressed file.

The 3508 PCIe plug-in RAID controller card is used as an example.

1. Download 9460-8i PCIe plug-in RAID controller card firmware package **RAID-9460-8i-3508MR-FW-5.140.00-3408.zip** based on the version mapping.

2. Decompress the firmware package.

3. Find the required tool, for example, **storcli64**, in the decompressed directory or the **tools** directory.

Step 3 Put the found tool to the target node.

Example:

1. Create a directory for storing the tool. (The directory can be customized.)

```
[root@localhost ~]# mkdir -p /opt/MegaRAID/storcli/
```

2. Place the tool in the created path and grant the execute permission on the tool.

```
[root@localhost ~]# chmod +x /opt/MegaRAID/storcli/storcli64
```

3. Run the following command. If the command output is displayed normally, the tool is successfully installed.

```
[root@localhost ~]# /opt/MegaRAID/storcli/storcli64

    StorCli SAS Customization Utility Ver 007.1912.0000.0000 Nov 23, 2021

  (c)Copyright 2021, Broadcom Inc. All Rights Reserved.


help - lists all the commands with their usage. E.g. storcli help
<command> help - gives details about a particular command. E.g. storcli add help
```

----End

3.3.7.2 Checking Versions

Prerequisites

The RAID CLI tool may be used in the following operations. For details about how to obtain and install the RAID CLI tool, see **3.3.7.1 Installing the RAID Controller Card CLI Tool**.

Checking the Driver Version

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Run the corresponding command to check the driver version.

- **3008IR/3408IT/3416IT RAID controller card:**

  Run the following command to check the driver version:

  ```
  [root@localhost ~]# modinfo mpt3sas | grep -iw version
  version:        26.100.00.00
  ```

- **3108/3408iMR/3416iMR/3508/3516/3908 RAID controller card:**

  Run the following command to check the driver version:

  ```
  [root@localhost ~]# /opt/MegaRAID/storcli/storcli64 /c0 show | grep -i "Driver Version"
  Driver Version = 07.706.07.00
  ```

- **3152-8i/2100-8i/FBGF-RAD-R1-S1 RAID controller card:**

  Run the following command to check the driver version:

  ```
  [root@localhost ~]# arcconf getversion 1 | grep -i "Driver"
  Driver                          : Linux 1.2.6-015
  ```

- **SP686C-M-16i/SP686C-M-40i/SP186-M-8i RAID controller card:**

  Run the following command to check the driver version:

  ```
  [root@localhost ~]# rpm -qa | grep kmod-hiraid
  kmod-hiraid-1.0.1.8-1.aarch64
  ```

1.0.1.8 in the command output is the driver version.

----End

Checking the Firmware Version

3008 RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Run the following command to check the firmware version:

```
[root@localhost ~]# ./sas3ircu 0 display | grep -i "Firmware version"
  Firmware version                : 15.00.07.00
```

----End

3108/3408/3416/3508/3516/3908 RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Run the following command to check the firmware version:

```
[root@localhost ~]# /opt/MegaRAID/storcli/storcli64 /c0 show | grep -i "FW Version"
FW Version = 5.060.00-2139
```

----End

3152-8i/2100-8i/FBGF-RAD-R1-S1 RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Run the following command to check the firmware version:

```
[root@localhost ~]# arcconf getversion 1 | grep -i "Firmware"
Firmware                        : 2.93[0]
```

----End

SP686C-M-16i/SP686C-M-40i RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Use a file transfer tool to upload the corresponding firmware package to a directory in the OS (for example, **/home**).

Go to the directory where the firmware package is stored and decompress the firmware package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_V600R008C10_HIRAID-FW-1.2.11.2-aarch64.zip
```

After the decompression, run the following command to query the firmware version.

```
[root@localhost ~]# sh install.sh getver
0:1.2.11.2
```

The preceding command output indicates that the firmware version of the RAID controller card whose ID is 0 is 1.2.11.2.

----End

SP186-M-8i RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Use a file transfer tool to upload the corresponding firmware package to a directory in the OS (for example, **/home**).

Go to the directory where the firmware package is stored and decompress the firmware package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_V600R008C10-HIRAID-HBA-FW-1.3.11.11-aarch64.zip
```

After the decompression, run the following command to query the firmware version:

```
[root@localhost ~]# sh install.sh getver
0:1.3.11.11
```

The preceding command output indicates that the firmware version of the RAID controller card whose ID is 0 is 1.2.11.2.

----End

3.3.7.3 Installing the Driver

NOTE

This section uses the v2r12 driver package as an example. For details about the mappings between RAID controller cards and driver packages and how to obtain the driver packages, see *Version Mapping* of the corresponding version.

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Run the following command to query the OS and kernel versions:

```
[root@localhost ~]# uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r12.aarch64
```

The preceding command output indicates that the OS is EulerOS V2R12 Arm.

NOTE

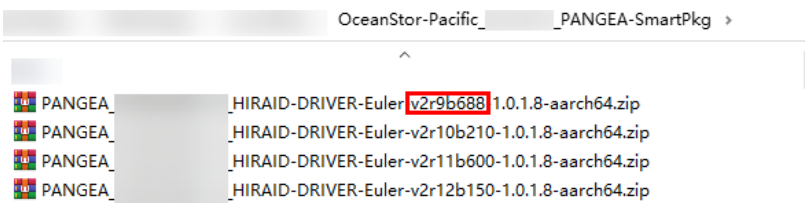
If the OS version is **v2r9**, continue to query the B version of the system and use the driver package whose B version is the same as that of the system for installation or upgrades. For details, see the following steps:

1. Run the following command to query the B version of the system:

   ```
   [root@localhost pr]# cat /etc/euleros-latest
   eulerversion=EulerOS_Server_V200R009C10SPC201B688_aarch64
   compiletime=2021-04-24-01-23-21
   kernelversion=4.18.0-147.5.1.6.h451
   ```

   The preceding command output indicates that the B version of the system is B688.

2. Obtain the driver package of the B version queried in the previous step from the **OceanStor-Pacific**_*XXX*_**PANGEA-SmartPkg** package of the corresponding version. In this example, the driver package of the v2r9b688 version is used for installation and upgrades, as shown in the following figure.



Step 3 Use a file transfer tool to upload the driver package corresponding to the RAID controller card model to a directory in the OS (for example, **/home**).

Step 4 Go to the directory where the driver package is stored and run the following commands to perform the installation or upgrade using the driver package.

SP686C-M-16i/SP686C-M-40i/3008/3108/3408/3508/3908/3152/SP186-M-8i/FBGF-RAD-R1-S1 RAID controller card (SP686C-M-16i/SP686C-M-40i is used as an example):

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_V600R008C10_HIRAID-DRIVER-Eulerv2r12-1.0.1.2-aarch64.zip
```

After decompressing the driver package, run the following command to install or upgrade the driver. If **success** is displayed, the command is successfully executed.

```
[root@localhost ~]# sh install.sh upgrade
success
```

Run the following commands to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh install.sh getupgraderate
upgrading 50
[root@localhost ~]# sh install.sh getupgraderate
success
```

Step 5 Restart the server for the driver to take effect.

----End

3.3.7.4 Upgrading the Firmware

Prerequisites

The RAID CLI tool may be used in the following operations. For details about how to obtain and install the RAID CLI tool, see **3.3.7.1 Installing the RAID Controller Card CLI Tool**.

Procedure

NOTE

- All services must be stopped before a firmware upgrade.
- For details about the mappings between RAID controller cards and firmware packages and how to obtain the firmware packages, see *Version Mapping* of the corresponding version.

3008 RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Use a file transfer tool to upload the firmware package corresponding to the RAID controller card model to a directory in the OS (for example, **/home**) and decompress the package.

Step 3 Go to the decompression directory and run the following command to grant execution permissions on the binary tool in the **tools** directory:


```
[root@localhost ~]# chmod +x ./tools/*
```

Step 4 Perform the upgrade.

- Run the **./tools/sas3flash -c 0 -f** *<RAID controller card firmware file>* command to upgrade the firmware of the RAID controller card.

  Example:

```
[root@localhost ~]# ./tools/sas3flash -c 0 -f 3008IR.bin
Avago Technologies SAS3 Flash Utility
Version 13.00.00.00 (2016.03.07)
Copyright 2008-2016 Avago Technologies. All rights reserved.

        Adapter Selected is a Avago SAS: SAS3008(C0)

        Executing Operation: Flash Firmware Image

                Firmware Image has a Valid Checksum.
                Firmware Version 15.00.07.00
                Firmware Image compatible with Controller.

                Valid NVDATA Image found.
                NVDATA Major Version 0e.00
                Checking for a compatible NVData image...

                NVDATA Device ID and Chip Revision match verified.
                NVDATA Versions Compatible.
                Valid Initialization Image verified.
                Valid BootLoader Image verified.

                Beginning Firmware Download...
                Firmware Download Successful.

                Verifying Download...

                Firmware Flash Successful.

                Resetting Adapter...
                Adapter Successfully Reset.

                NVDATA Version 0e.00.00.01
        Finished Processing Commands Successfully.
        Exiting SAS3Flash.
```

- Run the **./tools/sas3flash -c 0 -b** *<RAID controller card BIOS file 1>* command to upgrade the BIOS of the RAID controller card.

  Example:

```
[root@localhost ~]# ./tools/sas3flash -c 0 -b mptsas3.rom
Avago Technologies SAS3 Flash Utility
Version 13.00.00.00 (2016.03.07)
Copyright 2008-2016 Avago Technologies. All rights reserved.

        Adapter Selected is a Avago SAS: SAS3008(C0)

        Executing Operation: Flash BIOS Image

                Validating BIOS Image...

                BIOS Header Signature is Valid

                BIOS Image has a Valid Checksum.

                BIOS PCI Structure Signature Valid.

                BIOS Image Compatible with the SAS Controller.

                Attempting to Flash BIOS Image...
```

```
        Verifying Download...

        Flash BIOS Image Successful.

    Finished Processing Commands Successfully.
    Exiting SAS3Flash.
```

- Run the **./tools/sas3flash -c 0 -b** *<RAID controller card BIOS file 2>* command to upgrade the BIOS of the RAID controller card.

  Example:

```
[root@localhost ~]# ./tools/sas3flash -c 0 -b mpt3x64.rom
Avago Technologies SAS3 Flash Utility
Version 13.00.00.00 (2016.03.07)
Copyright 2008-2016 Avago Technologies. All rights reserved.

    Adapter Selected is a Avago SAS: SAS3008(C0)

    Executing Operation: Flash BIOS Image

        Validating BIOS Image...

        BIOS Header Signature is Valid

        BIOS Image has a Valid Checksum.

        BIOS PCI Structure Signature Valid.

        BIOS Image Compatible with the SAS Controller.

        Attempting to Flash BIOS Image...

        Verifying Download...

        Flash BIOS Image Successful.

    Finished Processing Commands Successfully.
    Exiting SAS3Flash.
```

  Note: The BIOS and firmware of a RAID controller card have version mapping relationships. You are advised to upgrade the BIOS and firmware of a RAID controller card together.

Step 5 Restart the server for the upgraded firmware to take effect.

----End

3108/3516 RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Use a file transfer tool to upload the firmware package corresponding to the RAID controller card model to a directory in the OS (for example, **/home**) and decompress the package.

Step 3 Go to the decompression directory and run the **/opt/MegaRAID/storcli/storcli64 /c0 download file=***<Firmware ROM file>* **noverchk** command to upgrade the firmware.

Example:

```
[root@localhost ~]# /opt/MegaRAID/storcli/storcli64 /c0 download file=3508FW4.rom noverchk
Download Completed.
Flashing image to adapter...
CLI Version = 007.0504.0000.0000 Nov 22, 2017
Operating system = Linux 3.10.0-862.14.1.2.h249.eulerosv2r7.x86_64
Controller = 0
```



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

Step 4 Restart the server for the upgraded firmware to take effect.

----End

3152-8i/2100-8i RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Use a file transfer tool to upload the firmware package corresponding to the RAID controller card model to a directory in the OS (for example, **/home**) and decompress the package.

Step 3 Go to the decompression directory and run the **arcconf ROMUPDATE 1** *<Firmware file>* **noprompt** command to upgrade the firmware.

Example:

```
[root@localhost ~]# arcconf ROMUPDATE 1 /home/SmartFWx100.bin noprompt
Controllers found: 1

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


Command completed successfully.
```

Step 4 Restart the server for the upgraded firmware to take effect.

----End

SP686C-M-16i/SP686C-M-40i/3408/3416/3508/3908 RAID/SP186-M-8i/FBGF-RAD-R1-S1 RAID controller card:

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Use a file transfer tool to upload the firmware package corresponding to the RAID controller card model to a directory in the OS (for example, **/home**).

Step 3 Go to the directory where the firmware package is stored and decompress the firmware package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_V600R008C10-HIRAID-HBA-FW-1.3.11.11-aarch64.zip
```

After decompressing the firmware package, run the following command to upgrade the firmware. If **success** is displayed, the upgrade is successful.

```
[root@localhost ~]# sh install.sh upgrade
success
```

Run the following commands to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh install.sh getupgraderate
upgrading 50
[root@localhost ~]# sh install.sh getupgraderate
success
```


Step 4 Restart the server for the upgraded firmware to take effect.

----End

3.3.7.5 Verifying the Upgrade

After the upgrade is complete, view the driver/firmware version to check whether the upgrade takes effect. For details about how to check versions, see **3.3.7.2 Checking Versions**. If the version is the same as that in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.8 Installing/Upgrading the Palm Disk Firmware

NOTE

This section applies only to the installation/upgrade of palm disk firmware on DPE60000.

3.3.8.1 Obtaining the Software Packages

Find the corresponding path based on the version mapping table of the disk model, and download the palm disk management tool and firmware packages.

Table 3-5

Palm Disk Model	Palm Disk Management Tool	Firmware Package
ES3000 V5	ES3000_V5_Tool_*.zip	ES3000_V5_Firmware_*.zip
ES3000 V6	HUAWEI_SSD_Tool_*.zip	ES3000V6_FW_*.zip

3.3.8.2 Checking the Palm Disk Management Tool Version

Procedure

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the **hioadm -v** command to query the tool version.

Example:

```
[root@localhost ~]# hioadm -v
hioadm version 5.0.3.8 Copyright (c) 2015-2020 Huawei
```

NOTE

If a message is displayed indicating that the preceding command fails to be found, the tool has not been installed.

----End

3.3.8.3 Installing/Upgrading the Palm Disk Management Tool

Procedure

Step 1 Use a remote connection tool to log in to the Linux OS as user **manageromm**, upload the management tool software package, switch to user **root**, decompress the software package, and find the corresponding tool.

Tool name: **hioadm-*.rpm**

Step 2 Run the **rpm -qa | grep -i** *<Tool name keyword>* command to check whether the tool has been installed and whether the tool version meets the requirements.

Example:

```
rpm -qa | grep -i hioadm
```

- If yes, no further action is required.
- If no, go to **3**.

Step 3 Create a directory named **/home/manageromm** for storing related files of palm disks (if the directory exists, skip this operation) and use a file transfer tool to upload the management tool package to the directory.

```
mkdir -p Directory name
```

Step 4 Copy the file and modify the permission.

Run the **mkdir -p** *Directory name* command to create the **/home/palm** directory.

Copy the management tool to the specified directory.

```
cp -rf /home/manageromm/<Tool package name> /home/palm/
```

Modify the file permission.

```
chown root:root /home/palm/<Tool package name>
chmod 750 /home/palm/<Tool package name>
```

Step 5 Install or upgrade the tool package.

- Access the tool package directory.
  ```
  cd /home/palm/ <Tool package name>/linux/aarch64
  ```
- If the tool package has not been installed on the device, run the **rpm -ivh** *<Tool package name>* command.
  ```
  rpm -ivh hioadm-6.0.1.1-1.aarch64.rpm
  ```
- If the tool package has been installed and you need to upgrade the tool package, run the **rpm -Uvh** *<Tool package name>* command.
  ```
  rpm -Uvh hioadm-6.0.1.1-1.aarch64.rpm
  ```

Step 6 After the installation, run the following commands to obtain the tool's help information or query information about the installed tool.

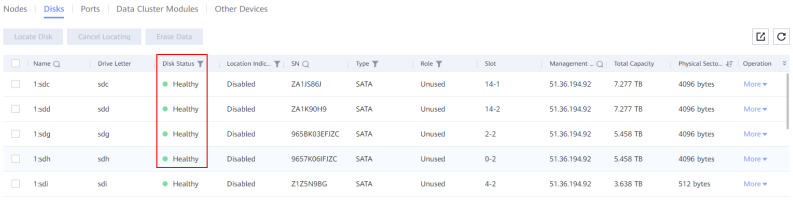
```
hioadm -h
hioadm --help
rpm -qa | grep hioadm
```

----End

3.3.8.4 Performing a Pre-upgrade Check

Procedure

Step 1 Log in to DeviceManager (**https://***Floating IP address of MetaVision*:**28443**). Choose **Cluster** > **Hardware** > **Disks** and check whether **Disk Status** of the disk to be upgraded is **Erasing** or **Verifying erased data**. If yes, upgrade the firmware after the disk is erased.



----End

3.3.8.5 Upgrading the Palm Disk Firmware

Procedure

Step 1 Use a remote connection tool to log in to the Linux OS as user **manageromm**, upload the **ES3000V*_FW_*.zip** software package to the **/home/manageromm** directory, and switch to user **root**. Copy the software package to the **/root** directory and decompress it.

Step 2 Query the health status of disks.

1. Log in to DeviceManager (**https://***Floating IP address of MetaVision*:**28443**), choose **Resources** > **Storage Pool**, and query the ID of the storage pool where the disks reside.
2. Log in to MetaVision through the floating IP address.
3. Switch to the **root** user.
   ```
   su - root
   ```
4. Run the following command to switch to the operation directory:
   ```
   cd /opt/dsware/client/bin/
   ```
5. Run the following command to query the status of disks in the storage pool:
   ```
   su - dsware -s /bin/bash -c "/opt/dsware/client/bin/dswareTool.sh --op queryStorageNodeInfo -id Storage pool ID"
   ```
   The username and password are those for logging in to DeviceManager.

   In the command output, if the values of all **diskStatus** fields are **0**, all the disks in the storage pool are healthy and the disk firmware can be upgraded.

Step 3 Set the maintenance mode.

NOTE

In maintenance mode, the fault isolation time increases by 45 minutes. If the upgrade is not complete during this period, exit the maintenance mode by performing 13 and run the following commands again to increase the fault isolation time.

```
cd /opt/fusionstorage/agent/tool/
./dsware_agent_tool --op add_dsware_lock
```



```
[root@localhost tool]# ./dsware_agent_tool --op add_dsware_lock
add dsware lock success
[root@localhost tool]#
```

Step 4 Log in to the node (physical host) whose disks need to be upgraded through the management IP address.

Step 5 Query the firmware versions of NVMe SSDs on the server and obtain the IDs of the NVMe SSDs that you want to upgrade.

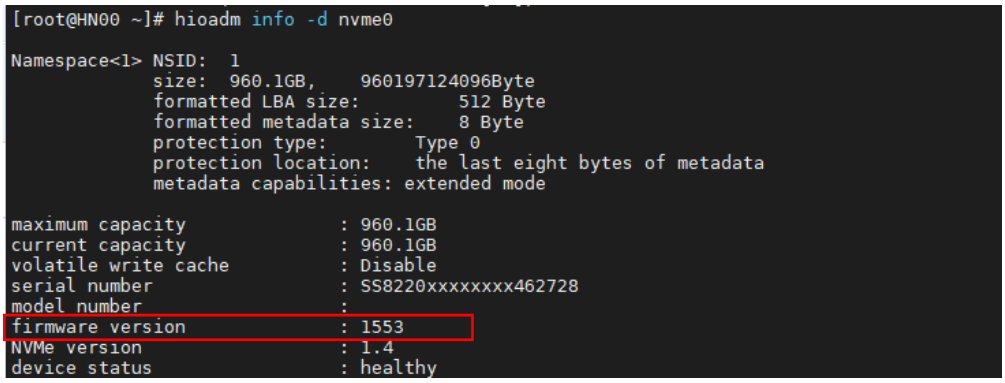
Run the following command. The **Node** field indicates the disk ID and the **FW Rev** field indicates the firmware version.

```
/opt/fusionstorage/persistence_layer/agent/tool/libstorage-list
```

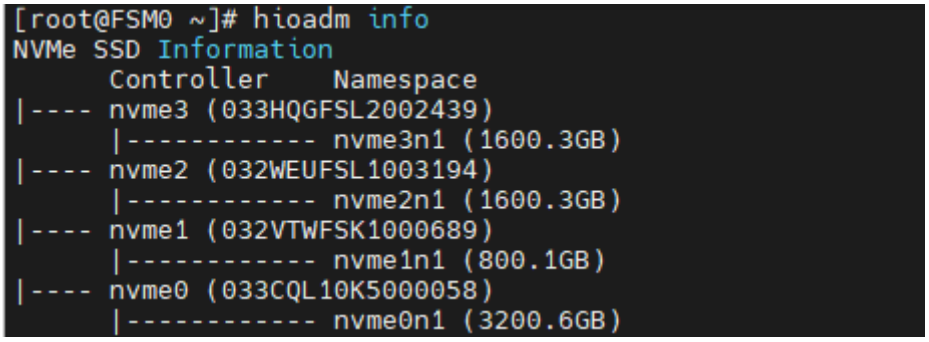
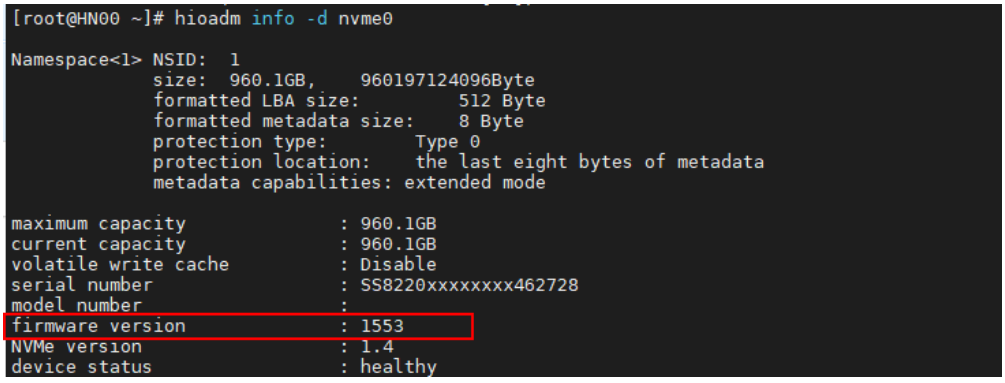
```
[root@localhost bin]# /opt/fusionstorage/persistence_layer/agent/tool/libstorage-list
```

Node	SN	Model	Size	Format	FW Rev
0000:5f:00.0	032WEUFSK2000305	HWE52P431T6M002N	1490 GB	512 + 8	1037
0000:86:00.0	032WEUFSK2000124	HWE52P431T6M002N	1490 GB	512 + 8	1037
0000:87:00.0	032JHDFSJ7000108	HWE32P43020M000N	1863 GB	512 + 8	3.10
0000:88:00.0	032WEUFSK1001689	HWE52P431T6M002N	1490 GB	512 + 8	1035
0000:89:00.0	032WEUFSK1001904	HWE52P431T6M002N	1490 GB	512 + 8	1035
0000:af:00.0	032WEUFSK1001797	HWE52P431T6M002N	1490 GB	512 + 8	1035
0000:b0:00.0	032WEUFSK1001447	HWE52P431T6M002N	1490 GB	512 + 8	1035

NOTE

1. Run the following command to check whether NVMe SSDs are taken over:
   ```
   nvme list|grep xxx
   ```
   xxx indicates the ESN of the NVMe SSD on the node. If any command output is displayed, the NVMe SSD is not taken over. If no command output is displayed, the NVMe SSD has been taken over.
2. For NVMe SSDs that are not taken over, perform the following steps: Go to 7. Run the following command for each **Device name** to query the firmware version. **nvme0** is used as an example. If the NVMe SSDs have been taken over, go to 5.
   ```
   hioadm info -d nvme0
   ```
   
   ```
   [root@HN00 ~]# hioadm info -d nvme0

   Namespace<1> NSID:  1
                size:  960.1GB,    960197124096Byte
                formatted LBA size:         512 Byte
                formatted metadata size:    8 Byte
                protection type:        Type 0
                protection location:    the last eight bytes of metadata
                metadata capabilities: extended mode

   maximum capacity              : 960.1GB
   current capacity              : 960.1GB
   volatile write cache          : Disable
   serial number                 : SS8220xxxxxxxx462728
   model number                  :
   firmware version              : 1553
   NVMe version                  : 1.4
   device status                 : healthy
   ```
3. If the storage software is not installed, run the following command to query the drive letters:
   ```
   hioadm info
   ```
   
   ```
   [root@FSM0 ~]# hioadm info
   NVMe SSD Information
         Controller    Namespace
   |---- nvme3 (033HQGFSL2002439)
         |------------ nvme3n1 (1600.3GB)
   |---- nvme2 (032WEUFSL1003194)
         |------------ nvme2n1 (1600.3GB)
   |---- nvme1 (032VTWFSK1000689)
         |------------ nvme1n1 (800.1GB)
   |---- nvme0 (033CQL10K5000058)
         |------------ nvme0n1 (3200.6GB)
   ```
   For each NVMe SSD, run the following command to query the firmware version. **nvme0** is used as an example.
   ```
   hioadm info -d nvme0
   ```
   
   ```
   [root@HN00 ~]# hioadm info -d nvme0

   Namespace<1> NSID:  1
                size:  960.1GB,    960197124096Byte
                formatted LBA size:         512 Byte
                formatted metadata size:    8 Byte
                protection type:        Type 0
                protection location:    the last eight bytes of metadata
                metadata capabilities: extended mode

   maximum capacity              : 960.1GB
   current capacity              : 960.1GB
   volatile write cache          : Disable
   serial number                 : SS8220xxxxxxxx462728
   model number                  :
   firmware version              : 1553
   NVMe version                  : 1.4
   device status                 : healthy
   ```
4. Perform 8 to complete the upgrade.

Step 6 Stop services on the server.

```
cd /opt/fusionstorage/persistence_layer/osd/bin/
mv dsware_osd dsware_osd_bk
```



```
cd /opt/fusionstorage/agent/bin/
mv dsware_agent dsware_agent_bk
killall dsware_osd
killall dsware_agent
```

NOTE

After this step is performed, it is normal that alarms related to FSA and OSD processes on the node will be reported on DeviceManager. After the upgrade is complete, the alarms will be automatically cleared.

Step 7 Cancel the takeover.

Run the following command:

```
/opt/fusionstorage/persistence_layer/agent/script/spdk_setup.sh reset_device 0000:5f:00.0 (disk ID obtained in 4)
```

```
[root@localhost bin]# /opt/fusionstorage/persistence_layer/agent/script/spdk_setup.sh reset_device 0000:5f:00.0
reset nvme devices 0000:5f:00.0
```

Step 8 Run the following command to query the drive letters of the disks:

```
/opt/fusionstorage/persistence_layer/agent/script/spdk_setup.sh status
```

```
[root@localhost bin]# /opt/fusionstorage/persistence_layer/agent/script/spdk_setup.sh status
NVMe devices
BDF             Numa Node       Driver name             Device name
0000:5f:00.0    0               nvme                    nvme0
0000:86:00.0    1               uio_pci_generic         -
0000:87:00.0    1               uio_pci_generic         -
0000:88:00.0    1               uio_pci_generic         -
0000:89:00.0    1               uio_pci_generic         -
0000:af:00.0    1               uio_pci_generic         -
0000:b0:00.0    1               uio_pci_generic         -
```

Step 9 Perform the upgrade.

Run the following command to query the disk information:

```
hioadm label -d nvme0 |grep VendorName |awk -F "=" '{print $2}'
```

nvme0 is the drive letter of the corresponding disk.

If the command output is **RAMAXEL**, use method 1 to perform the upgrade.

Otherwise, use method 2 to perform the upgrade.

Method 1:

Switch to the disk firmware directory and run the following command:

```
nvme fw-download -f 14-DPH311T4T003T2_signed.dfw /dev/nvme1n1
```

14-DPH311T4T003T2_signed.dfw is the firmware name.
/dev/nvme1n1 is the path of the corresponding disk.

If the following information is displayed, the upgrade is successful.

```
[root@localhost tzm]# nvme fw-download -f IDVI_FW_6020.bin /dev/nvme1n1
Firmware download success
```

Run the following command to activate the firmware:

```
nvme fw-activate -s 0 -a 3 /dev/nvme1n1
```

/dev/nvme1n1 is the path of the corresponding disk.

If the following information is displayed, the activation is successful.

```
[root@localhost tzm]# nvme fw-activate -s 0 -a 3 /dev/nvme1n1
Success committing firmware action:3 slot:0
```


Method 2:

Run the following command:

```
hioadm updatefw -d nvme0 -f /xxx/ES3000V5_FW_2158.bin
```

nvme0 is the drive letter of the corresponding disk.
xxx indicates the firmware path.
ES3000V5_FW_2158.bin is the firmware package name.

```
[root@localhost bin]# hioadm updatefw -d nvme0 -f /root/ES3000V5_FW_2158.bin
slot  version   activation
1     1037      current
2     0


WARNING! You have selected slot <2> to update the firmware image.
Proceed with this operation? (Y|N): y
Please do not remove driver or SSD device during the update
Loading...OK
Downloading and replacing the firmware image at slot <2> succeeded.
Activating the firmware image at slot <2> succeeded.
```

Step 10 Repeat **Step 7** to **Step 9** to upgrade other disks.

Step 11 Restart the node for the upgraded firmware to take effect.

Step 12 Restore services.

Log in to the node where the firmware is upgraded, switch to user **root**, and run the following commands:

```
cd /opt/fusionstorage/persistence_layer/osd/bin/
mv dsware_osd_bk dsware_osd
cd /opt/fusionstorage/agent/bin/
mv dsware_agent_bk dsware_agent
```

Wait until the **dsware_osd** and **dsware_agent** processes are restarted.

Run the following commands to check whether the processes are started:

```
ps -ef |grep dsware_agent
ps -ef |grep dsware_osd
```

```
[root@HN00 ~]# ps -ef |grep dsware_agent
omm       581919 1232079  2 16:03 ?        00:00:00 [dsware_agent_ha] <defunct>
root      582152 3755556  0 16:03 pts/4    00:00:00 grep --color=auto dsware_agent
omm      1232079       1  1 11:46 ?        00:02:51 ./dsware_agent
```

```
[root@HN_0_0 half_palm]# ps -ef |grep dsware_osd
root      15886      1 11 Jun16 ?        17:07:48 ./dsware_osd -i 0 -r 0
root      18233 29639  0 16:02 pts/2    00:00:00 grep --color=auto dsware_osd
```

Step 13 Check whether the firmware of the disk is upgraded to the target version and the takeover restores.

Run the following command:

```
/opt/fusionstorage/persistence_layer/agent/tool/libstorage-list
```

```
[root@localhost bin]# /opt/fusionstorage/persistence_layer/agent/tool/libstorage-list

----------------------------------------------------------------------------------------------------------
Node            SN                   Model                            Size           Format      FW Rev
--------------- -------------------- -------------------------------- -------------- ----------- ------
0000:5f:00.0    032WEUFSK2000305     HWE52P431T6M002N                 1490 GB        512  + 8    2158
0000:86:00.0    032WEUFSK2000124     HWE52P431T6M002N                 1490 GB        512  + 8    1037
0000:87:00.0    032JHDFSJ7000108     HWE32P43020M000N                 1863 GB        512  + 8    3.10
0000:88:00.0    032WEUFSK1001689     HWE52P431T6M002N                 1490 GB        512  + 8    1035
0000:89:00.0    032WEUFSK1001904     HWE52P431T6M002N                 1490 GB        512  + 8    1035
0000:af:00.0    032WEUFSK1001797     HWE52P431T6M002N                 1490 GB        512  + 8    1035
0000:b0:00.0    032WEUFSK1001447     HWE52P431T6M002N                 1490 GB        512  + 8    1035
----------------------------------------------------------------------------------------------------------
```

Step 14 Log in through the floating IP address and disable the maintenance mode.

```
cd /opt/fusionstorage/agent/tool/
./dsware_agent_tool --op release_dsware_lock
```

```
[root@localhost ~]# cd /opt/fusionstorage/agent/tool/
[root@localhost tool]# ./dsware_agent_tool --op release_dsware_lock
release dsware lock success
[root@localhost tool]#
```

Step 15 After the storage pool recovers, perform **1** to **Step 14** to upgrade the disk firmware of other servers.

----End

3.3.8.6 Verifying the Upgrade

After the upgrade is complete, view the firmware version to check whether the new version takes effect. For details about how to check the firmware version, see **Step 5**. If the version is the same as that in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.9 Installing/Upgrading the NIC Firmware and Driver

NOTE

To view the NIC model of a server, log in to the iBMC WebUI and choose **System** > **System Info** > **Network Adapters**. For details about the NIC firmware and driver versions, see the version mapping table. Some NIC drivers are native drivers of the OS and their upgrade is not introduced here.

3.3.9.1 Installing/Upgrading the 1822 Interface Module Firmware and Driver

NOTE

For details about how to obtain the NET driver package, see the desired version mapping.

3.3.9.1.1 Checking Versions

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS:

```
[root@localhost ~]# uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r10.aarch64
```

The preceding command output indicates that the OS is EulerOS (Arm).

Step 3 Use a file transfer tool to upload the NET driver package corresponding to the OS version to a directory in the OS (for example, **/home**). Go to the directory where the driver package is stored and decompress the driver package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_xxx_Uvp_NET_aarch64_xxx_release_yyy.zip
```

NOTE

Here, ***xxx*** indicates the version number and ***yyy*** indicates the OS version. For details about the package name, see the version mapping table.

Step 4 Run the following command to query the driver version:

```
[root@localhost ~]# sh install.sh getver
888_0
```

----End

3.3.9.1.2 Installing the NIC Driver Firmware Package

Procedure

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS:

```
[root@localhost ~]# uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r10.aarch64
```

The preceding command output indicates that the OS is EulerOS (Arm).

Step 3 Use a file transfer tool to upload the NET driver package corresponding to the OS version to a directory in the OS (for example, **/home**). Go to the directory where the driver package is stored and decompress the driver package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_xxx_Uvp_NET_aarch64_xxx_release_yyy.zip
```

NOTE

Here, ***xxx*** indicates the version number and ***yyy*** indicates the OS version. For details about the package name, see the version mapping table.

After the driver package is decompressed, run the following command to install or upgrade the driver.

```
[root@localhost ~]# sh install.sh upgrade
success
```

Run the following command to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh install.sh getupgraderate
upgrading 50
[root@localhost ~]# sh install.sh getupgraderate
success
```

Step 4 Restart the server for the driver to take effect.

----End

3.3.9.1.3 Verifying the Upgrade

After the upgrade is complete, check the driver version to verify that the new version has taken effect. For details, see **3.3.9.1.1 Checking Versions**. If the version number is the same as that recorded in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.9.2 Installing/Upgrading the Hi1822V120 NIC Firmware and Driver

3.3.9.2.1 Checking Versions

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to query the CPU type and EulerOS version:

```
Euler:~ # uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r10.aarch64
```

```
Euler:~ # uname -r
4.18.0-147.5.2.2.h657.eulerosv2r10.x86_64
```

NOTE

- If the command output contains **eulerosv2r10.aarch64**, **eulerosv2r11.aarch64**, or **eulerosv2r12.aarch64**, the OS version is EulerOS V2R10, V2R11, or V2R12, respectively, and the Arm CPU supports the installation and upgrade of the Hi1822V120 NIC firmware and driver. Go to **Step 4**.
- In other scenarios, where the Hi1822V120 NIC firmware and driver cannot be installed or upgraded, you do not need to install or upgrade the firmware and driver.

Step 4 Run the following command to check whether the Hi1822V120 NIC exists:

```
Euler:~ # lspci | grep -E "Device 0222|Device 0220"
01:00.0 Ethernet controller: Huawei Technologies Co., Ltd. Device 0222 (rev 21)
01:00.1 Ethernet controller: Huawei Technologies Co., Ltd. Device 0222 (rev 21)
0d:00.0 Ethernet controller: Huawei Technologies Co., Ltd. Device 0222 (rev 21)
0d:00.1 Ethernet controller: Huawei Technologies Co., Ltd. Device 0222 (rev 21)
```

NOTE

- If the command output contains **Device 0222** or Device 0220, the Hi1822V120 NIC exists on the server. Go to **Step 5**.
- Otherwise, you do not need to install or upgrade the hardware and driver.

Step 5 Run the following command to create the **/home/hinic3** directory for storing the Hi1822V120 NIC firmware and driver files:

```
Euler:~ # mkdir -p /home/hinic3
```

Step 6 Use a file transfer tool to upload the Hi1822V120 NIC driver package (for example, **PANGEA_V600R007C00_HINIC3_UNION-aarch64.zip**) corresponding to the OS version to a directory (for example, **/home/hinic3**) in the OS. Go to the directory where the driver package is stored and decompress the driver package.

```
Euler:~ # cd /home/hinic3
Euler:~ # unzip PANGEA_V600R007C00_HINIC3_UNION-aarch64.zip
Archive:  PANGEA_V600R007C00_HINIC3_UNION-aarch64.zip
  inflating: appctl
   creating: east_sea/
   creating: east_sea/driver/
  inflating: east_sea/driver/hinic3-15.6.2.1_4.19.90_vhulk2107.1.0.h699.eulerosv2r10.aarch64-1.aarch64.rpm
  inflating: east_sea/driver/hisdk3-15.6.2.1_4.19.90_vhulk2107.1.0.h699.eulerosv2r10.aarch64-1.aarch64.rpm
   creating: east_sea/fw/
   creating: east_sea/fw/hinic3_flash_2x100ge/
  inflating: east_sea/fw/hinic3_flash_2x100ge/Hinic3_flash.bin
   creating: east_sea/fw/hinic3_flash_2x25ge/
  inflating: east_sea/fw/hinic3_flash_2x25ge/Hinic3_flash.bin
   creating: east_sea/fw/hinic3_flash_4x25ge/
  inflating: east_sea/fw/hinic3_flash_4x25ge/Hinic3_flash.bin
   creating: east_sea/tools/
  inflating: east_sea/tools/hinicadm3-15.6.2.1-1.aarch64.rpm
  inflating: version.xml
```


Step 7 Run the following commands to check the version number:

```
Euler:~ # chmod +x appctl
Euler:~ # ./appctl get_version
15621-0
```

NOTE

- After the Hi1822V120 NIC is replaced, you do not need to pay attention to the version number check result. Perform operations by referring to **3.3.9.2.2 Installing the Hi1822V120 Driver Firmware**. In other scenarios, determine whether to install or upgrade the firmware driver based on the version number check result.
- If the queried version information does not match that in the *Version Mapping*, install the firmware and driver by following instructions provided in **3.3.9.2.2 Installing the Hi1822V120 Driver Firmware**.
- If the queried version information matches that in the *Version Mapping*, no upgrade is required.

----End

3.3.9.2.2 Installing the Hi1822V120 Driver Firmware

Procedure

Step 1 Run the following command to start the installation and upgrade of the firmware and driver. Information similar to the following is displayed:

```
Euler:~ # ./appctl update
success
```

NOTE

If **failure** is displayed in the command output, the installation fails to be started. Contact R&D engineers to locate the fault.

Step 2 Run the following command to query the upgrade progress. Information similar to the following is displayed:

```
Euler:~ # ./appctl get_progress
upgrading 50
```

NOTE

- The upgrade takes 3 to 6 minutes (for two Hi1822V120 NICs). If there are a large number of Hi1822V120 NICs in the environment, the upgrade takes a longer time.
- If **upgrading** followed by a digit is displayed in the command output, the upgrade is in progress. Query the upgrade again later. If **success** is displayed, go to **Step 3**. If **failure** is displayed, the installation fails. Contact R&D engineers to locate the fault.

Step 3 Run the following command to restart the system for the installation to take effect:

```
[root@localhost ~]# reboot
```

----End

3.3.9.2.3 Verifying the Upgrade

After the upgrade is complete, view the firmware version to check whether the new version takes effect. For details about how to check versions, see **3.3.9.2.1 Checking Versions**. If the new version and the version in the *Version Mapping* are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.9.3 Installing/Upgrading the Mellanox NIC Driver

NOTE

In the version mapping table, the board whose name is **ConnectX-4**, **ConnectX-4 LX**, or **ConnectX-5** is a Mellanox NIC. You can log in to the iBMC WebUI, choose **System** > **System Info** > **Network Adapters** and select the desired NIC to view its information. You can see that the NIC chip vendor is Mellanox.

3.3.9.3.1 Querying the NIC Driver Mapping

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS:

```
cat /etc/os-release
```

Example:

```
MCNA01:/home/manageromm/ # cat /etc/os-release
NAME="EulerOS"
VERSION="2.0 (SP12)"
ID="euleros"
VERSION_ID="2.0"
PRETTY_NAME="EulerOS 2.0 (SP12)"
ANSI_COLOR="0;31"
```

The OS in the example is EulerOS.

Step 3 Select an upgrade mode based on the matched driver in the version mapping table.

----End

NOTE

The Mellanox NIC driver varies with the OS. If the OS uses the **FusionCube**_*xxx*_**Driver-RDMA**_*yyy*.**zip** driver, perform the upgrade as instructed in **3.3.9.3.2 Installing/Upgrading the RDMA Firmware and Driver**. If the **MLNX_OFED_LINUX-***xxx*.**tgz** driver is used, perform the upgrade as instructed in **3.3.9.3.3 Installing/Upgrading the Mellanox Driver**. For details about how to upgrade the NIC firmware, see **3.3.9.4 Upgrading the Firmware of Other NICs**.

3.3.9.3.2 Installing/Upgrading the RDMA Firmware and Driver

3.3.9.3.2.1 Checking Versions

Step 1 Use a remote connection tool to log in to the Linux OS and switch to user **root**.

Step 2 Run the following command to query the driver version. For example:

```
Euler:~ # rdma_ver
4.19-31-arm-2-0
```

```
Euler:~ # rdma_ver
4.19-31-x86-2-0
```


NOTE

- If the **rdma_ver** command is not supported or the queried version information does not match the version information in the desired version mapping, see **Installing the RDMA NIC Firmware and Driver**.
- If the queried version information matches the version information in the desired version mapping, no upgrade is required.

----End

3.3.9.3.2.2 Installing the RDMA NIC Firmware and Driver

Prerequisites

You have obtained the firmware and driver packages according to **2.3 Preparing for the NIC Upgrade**.

Procedure

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
[root@localhost ~]# systemctl stop secAgent
```

Step 3 Run the following command to create the **/home/rdma** directory for storing the NIC firmware and driver file:

```
[root@localhost home]# mkdir -p /home/rdma
```

Step 4 Upload the NIC firmware and driver file (for example, **FusionCube**_*XXX*_**Driver-RDMA_x86-64.zip**) to the directory created in **Step 3**, and go to **Step 6**. If you have no permission to upload the file to the directory created in **Step 3**, go to **Step 5**.

Step 5 Upload the NIC firmware and driver file to a directory on which you have permission, for example, **/home/manageromm**. Run the following command to copy the uploaded file to the directory created in **Step 3**. Information similar to the following is displayed. **FusionCube**_*XXX*_**Driver-RDMA_x86-64.zip** indicates the driver package name.

```
[root@localhost home]# cp /home/manageromm/FusionCube_XXX_Driver-RDMA_x86-64.zip /home/rdma/
```

Step 6 Run the following command to switch to the **/home/rdma** directory where the NIC firmware and driver file are stored, and decompress the installation package. **PANGEA**_*XXX*_**RDMA**_*XXX*.**zip** indicates the driver package name.

```
[root@localhost home]# unzip FusionCube_XXX_Driver-RDMA_x86-64.zip
```

Step 7 After decompression, run the following commands to switch to the **action** directory and modify the permission on the installation script:

```
[root@localhost home]# cd action/
[root@localhost home]# chmod +x appctl
```

Step 8 Run the following command to start the installation and upgrade of the firmware and driver. Information similar to the following is displayed:

```
[root@localhost home]# ./appctl update
success
```


NOTE

If **failure** is displayed in the command output, the installation fails to be started. Contact R&D engineers to locate the fault.

Step 9 Run the following command to query the upgrade progress. Information similar to the following is displayed:

```
Euler:~ # ./appctl get_progress
upgrading 0
```

NOTE

The upgrade takes 3 to 6 minutes (for two RDMA NICs). If there are a large number of RDMA NICs in the environment, the upgrade takes a longer time.

If **upgrading** followed by a digit is displayed in the command output, the upgrade is in progress. Query the upgrade again later. If **success** is displayed, go to **Step 10**. If **failure** is displayed, the installation fails. Contact R&D engineers to locate the fault.

Step 10 Run the following command to restart the system for the installation to take effect:

```
[root@localhost ~]# reboot
```

----End

3.3.9.3.2.3 Verifying the Upgrade

After the upgrade is complete, you need to view the firmware version to check whether the new version takes effect. For details about how to check versions, see **Checking Versions**. If the new version and the version in the *Version Mapping* are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.9.3.3 Installing/Upgrading the Mellanox Driver

3.3.9.3.3.1 Checking Versions

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the driver version:

```
ethtool -i Network port name
```

Example:

```
[root@DBN01 ]# ethtool -i ibs7f0
driver: mlx5_core[ib_ipoib]
version: 5.7-1.0.2
firmware-version: 16.32.1010 (HUA0000000004)
expansion-rom-version:
bus-info: 0000:d8:00.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: yes
```

Here, **version** (5.7-1.0.2) indicates the NIC driver version.

----End

3.3.9.3.3.2 Installing/Upgrading the Mellanox Driver

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to create the driver directory **/home/mlnx**:

```
mkdir /home/mlnx
```

Step 3 Upload the driver file to an authorized directory (for example, **/home/manageromm**) and run the following command to copy the driver file to the created **/home/mlnx** directory:

```
cp Uploaded directory/Driver file name /home/mlnx
```

Example:

```
cp /home/manageromm/MLNX_OFED_LINUX-xxx.tgz /home/mlnx
```

NOTE

MLNX_OFED_LINUX-*xxx*.tgz is not the actual driver package name. For details about the actual driver package name, see the version mapping table.

Step 4 Run the following command to go to the **/home/mlnx** directory:

```
cd /home/mlnx
```

Step 5 Run the following command to decompress the driver package:

```
tar -zxvf MLNX_OFED_LINUX-xxx.tgz
```

Example:

```
tar -zxvf MLNX_OFED_LINUX-xxx.tgz
```

Step 6 Run the following command to go to the **MLNX_OFED_LINUX-*xxx*** directory:

```
cd MLNX_OFED_LINUX-xxx/
```

Example:

```
cd MLNX_OFED_LINUX-xxx/
```

Step 7 Run the following command to install the driver software:

```
echo "y" |./mlnxofedinstall --without-depcheck --without-fw-update --force
```

NOTE

The upgrade takes about 3 to 6 minutes (for two Mellanox NICs). If there are a large number of Mellanox NICs in the environment, the upgrade takes a longer time.

Step 8 Run the following command to restart the system for the installation to take effect:

```
reboot
```

----End

3.3.9.3.3.3 Verifying the Upgrade

After the upgrade is complete, view the firmware version to check whether the new version takes effect. For details about how to check versions, see **Checking Versions**. If the new version and the version in the version mapping table are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.9.3.4 (Optional) Switching the Network Adapter Mode

The default mode of the ConnectX-5 card may be IB or RoCE. You need to manually switch the mode to the corresponding mode based on the networking mode.

NOTE

Before switching the NIC mode, ensure that the NIC driver is installed and the firmware is upgraded to the latest version. If the driver is not installed, install the NIC firmware driver as instructed in **3.3.9.3.2 Installing/Upgrading the RDMA Firmware and Driver** or **3.3.9.3.3 Installing/Upgrading the Mellanox Driver** and then switch the NIC mode.

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
[root@localhost ~]# systemctl stop secAgent
```

Step 3 Run the following command to query the PSID of the NIC. In the following command output, **/dev/mst/***xxxx* is the PSID.

```
[root@localhost ~]# mst start
[root@localhost ~]# mst status
MST modules:
------------
   MST PCI module is not loaded
   MST PCI configuration module loaded

MST devices:
------------
/dev/mst/mt4123_pciconf0         - PCI configuration cycles access.
                                   domain:bus:dev.fn=0000:01:00.0 addr.reg=88 data.reg=92 cr_bar.gw_offset=-1
                                   Chip revision is: 00
```

Step 4 Run the following command to query the current mode of the NIC (replace **/dev/mst/***xxxxx* with the queried PSID). If the following information is displayed, port 1 of the NIC is in ETH mode and port 2 is in IB mode.

```
[root@localhost ~]# mlxconfig -d /dev/mst/xxxxx q | grep LINK_TYPE
        LINK_TYPE_P1                ETH(2)
        LINK_TYPE_P2                IB(1)
```

Step 5 If the NIC port mode is IB but the expected mode is RoCE, go to **Step 6**. If the NIC port mode is RoCE but the expected mode is IB, go to **Step 7**. Otherwise, go to **Step 8**.

Step 6 If the NIC port mode is IB but the expected mode is RoCE, perform this step. Run the following command to set the specified NIC port to the RoCE mode. Replace **/dev/mst/***xxxx* with the PSID queried in **Step 3**. LINK_TYPE_P1 indicates the first port, LINK_TYPE_P2 indicates the second port. **set LINK_TYPE_P1=2** indicates that the first port of the NIC is set to mode 2.

```
[root@localhost ~]# mlxconfig -d /dev/mst/xxxx set LINK_TYPE_P1=2

Device #1:
----------

Device type:    ConnectX6
Name:           SL6TIIB2A
Description:    Huawei Storage STL6TIIB2A ConnectX6 IB HDR100 and 100Ge dual-port QSFP56 PCIE Gen4 X16 Single Host
Device:         /dev/mst/mt4123_pciconf0

Configurations:                          Next Boot       New
```

```
        LINK_TYPE_P1                ETH(2)          ETH(2)

 Apply new Configuration? (y/n) [n] : y
Applying... Done!
-I- Please reboot machine to load new configurations.
```

NOTE

mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P1=2 indicates that the first port of the NIC is set to mode 2 (ETH mode is RoCE mode). If the NIC has multiple ports, specify the port mode for multiple times. For example, if two ports need to be set to the RoCE mode, run the following commands:

mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P1=2

mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P2=2

Step 7 If the NIC port mode is RoCE but the expected mode is IB, perform this step. Run the following command to set the NIC port to the IB mode. Replace **/dev/mst/***xxxx* with the PSID queried in **Step 3**. LINK_TYPE_P1 indicates the first port, LINK_TYPE_P2 indicates the second port. **set LINK_TYPE_P1=1** indicates that the first port of the NIC is set to mode 1 (IB mode).

```
[root@localhost ~]# mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P2=1

Device #1:
----------

Device type:    ConnectX6
Name:           SL6TIIB2A
Description:    Huawei Storage STL6TIIB2A ConnectX6 IB HDR100 and 100Ge dual-port QSFP56 PCIE Gen4
X16 Single Host
Device:         /dev/mst/mt4123_pciconf0

Configurations:                          Next Boot       New
        LINK_TYPE_P2                      IB(1)          IB(1)

 Apply new Configuration? (y/n) [n] : y
Applying... Done!
-I- Please reboot machine to load new configurations.
```

NOTE

mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P1=1 indicates that the first port of the NIC is set to mode 1 (ETH mode is RoCE mode). If the NIC has multiple ports, specify the port mode for multiple times. For example, if two ports need to be set to the IB mode, run the following commands:

mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P1=1

mlxconfig -d /dev/mst/mt4123_pciconf0 set LINK_TYPE_P2=1

Step 8 Run the following command to restart the system for the installation to take effect:

```
[root@localhost ~]# reboot
```

Step 9 Repeat **Step 1** to **Step 4** to check whether the NIC mode switchover takes effect.

----End

3.3.9.4 Upgrading the Firmware of Other NICs

NOTE

This section describes how to upgrade the firmware of NICs listed in the version mapping table. For details about how to upgrade the NIC firmware that is not listed in the version mapping table, see the official NIC documentation.

3.3.9.4.1 Checking Versions

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the firmware version:

```
ethtool -i Network port name
```

Example:

```
SCNA01:/home/manageromm/ # ethtool -i eth4
driver: ixgbe
version: 5.10.0-136.12.0.86.h2059.eulero
firmware-version: 0x800003df
expansion-rom-version:
bus-info: 0000:3b:00.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: yes
```

firmware-version (0x800003df) indicates the NIC firmware version.

----End

3.3.9.4.2 Upgrading the Firmware

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to create the driver directory **/home/firmware**:

```
mkdir /home/firmware
```

Step 3 Upload the firmware file to an authorized directory (for example, **/home/manageromm**) and run the following command to copy the firmware file to the created **/home/firmware** directory:

```
cp Uploaded directory/Firmware file name /home/firmware
```

Example:

```
cp /home/manageromm/NIC-SP380-CX4Lx-FW_14.32.1010_X86.zip /home/firmware
```

Step 4 Run the following command to decompress the firmware file:

```
unzip Firmware file name
```

Example:

```
unzip NIC-SP380-CX4Lx-FW_14.32.1010_X86.zip
```

Step 5 Run the following commands to add the execute permission to the installation script:

```
chmod +x install.sh
```

Step 6 Run the following command to upgrade the NIC firmware:

```
./install.sh upgrade
```


or

```
bash install.sh upgrade
```

NOTE

- If the server has multiple NICs of the same model, the script automatically upgrades the firmware of all NICs of the same model to the target version.
- You can run the **cat work.log** command to open the **work.log** file in the directory where the upgrade log file is located to view the upgrade log information, or run the **cat result.xml** command to open the **result.xml** file to view the upgrade result.

Step 7 Restart the server for the firmware to take effect.

----End

3.3.9.4.3 Verifying the Upgrade

After the upgrade is complete, view the firmware version to check whether the new version takes effect. For details about how to check versions, see **3.3.9.4.1 Checking Versions**. If the new version and the version in the version mapping table are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.10 Installing/Upgrading the SATA Driver

NOTE

This section applies only to the installation/upgrade of the SATA driver on DPE60000.

3.3.10.1 Checking the Driver Version

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the driver version:

```
Euler:~ # rpm -qi pangea-sata-driver |grep -i  version
Version     : 01.02.21
```

----End

3.3.10.2 Installing the Driver

NOTE

This section uses the v2r12 driver package as an example. For details about how to obtain the SATA driver package, see the version mapping.

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS and kernel versions:

```
[root@localhost ~]# uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r12.aarch64
```

The preceding command output indicates that the OS is Euler ARM V2R12.

Step 3 Use a file transfer tool to upload the SATA driver package corresponding to the OS version to a directory in the OS (for example, **/home**).

Go to the directory where the driver package is stored and decompress the driver package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_xxx_SATA_xxx_Uvp_yyy_aarch64_release.zip
```

NOTE

Here, ***xxx*** indicates the version number and ***yyy*** indicates the OS version. For details about the package name, see the version mapping table.

After decompressing the driver package, run the following command to install or upgrade the driver. If **success** is displayed, the command is successfully executed.

```
[root@localhost ~]# sh install.sh upgrade
success
```

Run the following command to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh install.sh getupgraderate
upgrading 50
[root@localhost ~]# sh install.sh getupgraderate
success
```

Step 4 Restart the server for the driver to take effect.

----End

3.3.10.3 Verifying the Upgrade

After the upgrade is complete, you need to view the firmware version to check whether the new version takes effect. For details about how to check versions, see **3.3.10.1 Checking the Driver Version**. If the version is the same as that in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.11 Installing/Upgrading the SAS Driver

NOTE

This section applies only to the installation/upgrade of the SAS driver on DPE60000.

3.3.11.1 Checking the Driver Version

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the driver version:

```
[root@localhost ~]# rpm -qi pangea-hisisas-driver | grep -i version
Version     : 1.06.90
```

----End

3.3.11.2 Installing the Driver

NOTE

This section uses the v2r12 driver package as an example. For details about how to obtain the SAS driver package, see the version mapping table.

Procedure

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS and kernel versions:

```
[root@localhost ~]# uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r12.aarch64
```

The preceding command output indicates that the OS is Euler ARM V2R12.

Step 3 Use a file transfer tool to upload the SAS driver package corresponding to the OS version to a directory in the OS (for example, **/home**).

Go to the directory where the driver package is stored and decompress the driver package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_xxx_SAS_xxx_Uvp_yyy_aarch64_release.zip
```

NOTE

Here, ***xxx*** indicates the version number and ***yyy*** indicates the OS version. For details about the package name, see the version mapping table.

After decompressing the driver package, run the following command to install or upgrade the driver. If **success** is displayed, the command is successfully executed.

```
[root@localhost ~]# sh install.sh upgrade
success
```

Run the following command to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh install.sh getupgraderate
upgrading 50
[root@localhost ~]# sh install.sh getupgraderate
success
```

Step 4 Restart the server for the driver to take effect.

----End

3.3.11.3 Verifying the Upgrade

After the upgrade is complete, view the driver/firmware version to check whether the upgrade takes effect. For details about how to check versions, see **3.3.11.1 Checking the Driver Version**. If the version is the same as that in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.12 Installing/Upgrading the NVMe Driver

NOTE

This section applies only to the installation/upgrade of the NVMe driver on DPE60000.

3.3.12.1 Checking the Driver Version

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the driver version:

```
Euler:~ # rpm -qi pangea-nvme-driver |grep -i  version
Version     : 01.01.03
```

----End

3.3.12.2 Installing the Driver

NOTE

This section uses the v2r12 driver package as an example. For details about how to obtain the NVMe driver package, see the version mapping.

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS and kernel versions:

```
[root@localhost ~]# uname -r
4.19.90-vhulk2108.6.0.h832.eulerosv2r12.aarch64
```

The preceding command output indicates that the OS is Euler ARM V2R12.

Step 3 Use a file transfer tool to upload the NVMe driver package corresponding to the OS version to a directory in the OS (for example, **/home**).

Go to the directory where the driver package is stored and decompress the driver package.

```
[root@localhost ~]# cd /home
[root@localhost ~]# unzip PANGEA_xxx_NVME_xxx_Uvp_yyy_aarch64_release.zip
```

NOTE

Here, ***xxx*** indicates the version number and ***yyy*** indicates the OS version. For details about the package name, see the version mapping table.

After decompressing the driver package, run the following command to install or upgrade the driver. If **success** is displayed, the command is successfully executed.

```
[root@localhost ~]# sh install.sh upgrade
success
```

Run the following command to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh install.sh getupgraderate
upgrading 50
[root@localhost ~]# sh install.sh getupgraderate
success
```

Step 4 Restart the server for the driver to take effect.

----End

3.3.12.3 Verifying the Upgrade

After the upgrade is complete, you need to view the firmware version to check whether the new version takes effect. For details about how to check versions, see **3.3.12.1 Checking the Driver Version**. If the version is the same as that in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.13 Installing/Upgrading Basic Drivers

NOTE

This section applies only to the installation/upgrade of basic drivers on DPE60000.

3.3.13.1 Checking Basic Driver Versions

Procedure

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following commands to query the driver versions. If no driver is installed, install a driver first and then query its version.

Query the version of each basic driver (9950 does not have the cma component):

```
[root@localhost ~]# rpm -qa |grep pcieinf
pangea-pcieinf-drv-euler-5.10.0-0.0006-0.002A.aarch64
```

pcieinf version: 0.0006-0.002A

```
Euler:~ # rpm -qa |grep bsp
pangea-bsp-drv-euler-5.10.0-000C.0068.0021.aarch64
```

bsp version: 000C.0068.0021

Step 3 Query the overall version of the basic driver:

```
Euler:~ # if which base_getversion.sh > /dev/null 2>&1; then base_getversion.sh; fi
0019.002A.0006-000C.0069.0021-0001.0006-0.0006.0.000B
```

----End

3.3.13.2 Installing/Upgrading Basic Drivers

NOTE

This section uses the v2r12 driver package as an example. For details about how to obtain the BASE_KNL driver package, see the version mapping table.

Procedure

Step 1 Use a remote connection tool to log in to Linux and switch to user **root**.

Step 2 Run the following command to query the OS and kernel versions:

```
[root@localhost ~]# uname -r
5.10.0-136.12.0.86.h1429.eulerosv2r12.aarch64
```

The preceding command output indicates that the OS is Euler ARM V2R12.

Step 3 Create a **/home/pangea_baseknl** directory for storing the **BASE_KNL** driver package.

```
[root@localhost home]# mkdir -p /home/pangea_baseknl
```

Step 4 Use a file transfer tool to upload the **BASE_KNL** driver package of the corresponding OS version to the **/home/pangea_baseknl** directory.

Decompress the driver package.

```
[root@localhost ~]# unzip PANGEA_xxx_Uvp_BASE_KNL_yyy_aarch64_release.zip
```


NOTE

Here, ***xxx*** indicates the version number and ***yyy*** indicates the OS version. For details about the package name, see the version mapping table.

After the driver package is decompressed, run the following command to install or upgrade the driver.

```
[root@localhost pangea_baseknl]# sh action/appctl UpgradeVersion
success
```

Run the following command to query the upgrade progress and check whether the upgrade is successful. If **upgrading 50** is displayed, the upgrade progress is 50%. You can query the upgrade progress for multiple times until **success** is displayed.

```
[root@localhost ~]# sh action/appctl GetUpgradeStatus
upgrading 50
[root@localhost ~]# sh action/appctl GetUpgradeStatus
success
```

Step 5 After the installation is completed, run the **reboot** command to restart the system.

----End

3.3.13.3 Verifying the Upgrade

After the upgrade is complete, view the firmware version to check whether the new version takes effect. For details about how to check versions, see **3.3.13.1 Checking Basic Driver Versions**. If the version is the same as that in the version mapping, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

3.3.14 Upgrading Retimer Chips

NOTE

This section applies only to the upgrade of Retimer chips on DPE60000.

3.3.14.1 Preparing for the Upgrade

3.3.14.1.1 Selecting the Retimer Chip Firmware Package

The operations on the PCIe Retimer 5902H are different from Retimer. You need to manually distinguish Retimer from new Retimer (5902H) to select the correct chip firmware package for installation or upgrade. You can check whether the Retimer or Retimer (5902H) is used by querying the Retimer version format in the environment. The check method is as follows.

Procedure

Step 1 Query the version of the Retimer chip.

Query the version using the CLI:

Use SSH (a remote login tool) to log in to the iBMC CLI and run the **ipmcget -d version** command. The version is the value of **Retimer Version** in the command output. There are three records.

```
......
---------- RETIMER INFO ----------
Mainboard Retimer 0   Version:     10.01.18.02
Mainboard Retimer 1   Version:     10.01.18.02
Mainboard Retimer 2   Version:     10.01.18.02
```

The version query result of Retimer (5902H) is as follows:

```
......
---------- RETIMER INFO ----------
Mainboard Retimer 0   Version:     1
Mainboard Retimer 1   Version:     1
Mainboard Retimer 2   Version:     1
```

If the version is in AA.BB.CC.DD format, for example, 10.01.18.02, the old Retimer is used. In this case, select **pcie_retimer_Sinan.zip**. If the version is in AA single-segment format, for example, 1, the new Retimer (5902H) is used. In this case, select **ti_retimer_Sinan.zip**.

----End

3.3.14.1.2 Decompressing the Retimer Chip Firmware Package

Upload the Retimer chip firmware package to a specified directory on the local PC and decompress the package. For details about how to obtain the firmware package, see **1.1 Firmware List**. **Figure 3-90** shows the files extracted from the firmware package. The firmware package contains two files, as described in **Table 3-6**. **Figure 3-91** shows the files in the decompressed Retimer (5902H) firmware package. The firmware package contains two files, as described in **Table 3-7**.

Figure 3-90 Files in the Retimer chip firmware package

Figure 3-91 Files in the Retimer (5902H) chip firmware package

Table 3-6 Description of the files in the Retimer chip firmware package

File Name	Description
pcie_retimer_Sinan.hpm	Retimer chip firmware.
version.xml	Version configuration table, which records the Retimer chip firmware version.

Table 3-7 Description of the files in the Retimer (5902H) chip firmware package

File Name	Description
ti_retimer_Sinan.hpm	Retimer (5902H) chip firmware
version.xml	Version configuration table, which records the Retimer (5902H) chip firmware version.

NOTE

- The Retimer chip firmware name varies with the hardware configuration. The actual firmware name is used. The upgrade process is the same regardless of the firmware name.
- The firmware package varies slightly with the hardware configuration. For details, see the product documentation. If you have any questions, contact the maintenance personnel.
- The only difference between Retimer and Retimer (5902H) lies in the chip. After the correct firmware package is selected, the subsequent upgrade process is the same.

3.3.14.1.3 Checking Versions

Check whether the current version of the Retimer chip is the same as the version in the **version.xml** file. If no, perform an upgrade. This section describes how to check the versions.

Procedure

Step 1 Query the version of the Retimer chip.

Query the version using the CLI:

Use SSH (a remote login tool) to log in to the iBMC CLI and run the **ipmcget -d version** command. The version is the value of **Retimer Version** in the command output. There are three records.

```
......
---------- RETIMER INFO ----------
Mainboard Retimer 0   Version:      10.01.18.02
Mainboard Retimer 1   Version:      10.01.18.02
Mainboard Retimer 2   Version:      10.01.18.02
```

Step 2 Check the firmware version in the **version.xml** file. For example, the **<Version>10.01.18.02</Version>** attribute in the configuration file indicates that the firmware version of the Retimer chip is 10.01.18.02, as shown in the following figure.

Figure 3-92 Retimer chip version contained in the XML file

```
<?xml version="1.0" encoding="utf-8"?>
<FirmwarePackage version="V1.0">
<!--Firmware packages description-->
    <Package>
        <FileName>pcie_retimer_Sinan.hpm</FileName>
        <!--Multiple files are separated by semicolons-->
        <Module>pcie_retimer</Module>
        <Vendor>Huawei Technology Co.</Vendor>
        <Version>10.01.18.11</Version>
        <ActiveMode>ResetServer</ActiveMode>
        <!--Active mode:Immediately/ResetOS/ResetServer/ResetMM/ResetBMC-->
        <SupportModel>STL6SPCY</SupportModel>
        <!--Multiple models are separated by semicolons-->
        <SupportModelUID>0x020dfa00</SupportModelUID>
        <PackageName>Pcie_Retimer_Sinan_Firmware_V100</PackageName>
        <UpgradeAgent>BMC</UpgradeAgent>
        <VersionPattern>(\d+)\.(\d+)\s*$</VersionPattern>
        <FileType>Firmware</FileType>
        <UpgradeTime>90</UpgradeTime>
        <MaxUpgradeTime>180</MaxUpgradeTime>
        <ActiveEffect>Host</ActiveEffect>
        <ActiveTime>180</ActiveTime>
        <MaxActivetime>1800</MaxActivetime>
        <UpgradeMode>MANUAL</UpgradeMode>
        <Size>TMP_SIZE</Size>
        <OldVersion>N/A</OldVersion>
        <ActiveTimes>1</ActiveTimes>
        <RpmName>pcie_retimer_Sinan.hpm</RpmName>
        <Summary>pcie retimer upgrade package.</Summary>
        <Description>pcie retimer upgrade for all server</Description>
        <Object></Object>
    </Package>
</FirmwarePackage>
```

----End

3.3.14.2 Performing the Upgrade

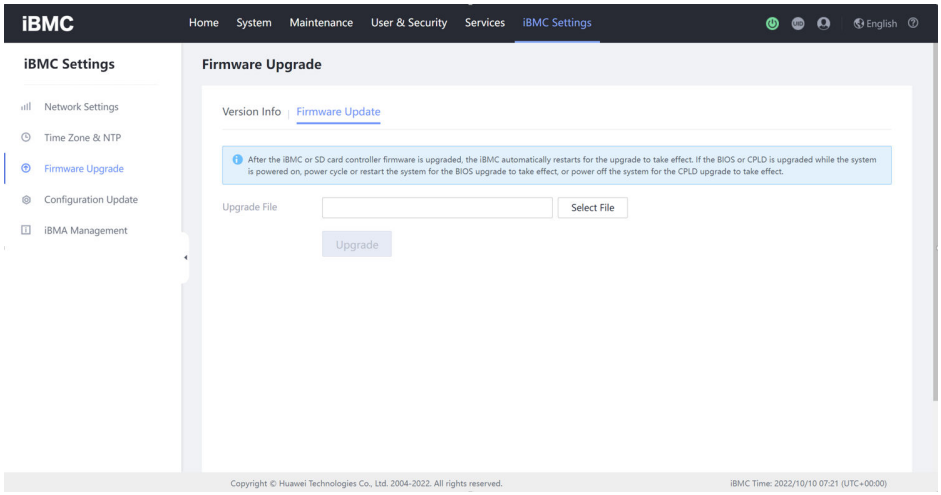
After the Retimer chip firmware is upgraded on the iBMC WebUI, the firmware takes effect only after the system is powered off.

Procedure

Step 1 Log in to the iBMC WebUI.

Step 2 Choose **iBMC Settings** > **Firmware Upgrade** > **Firmware Update**.

Figure 3-93 Firmware upgrade page

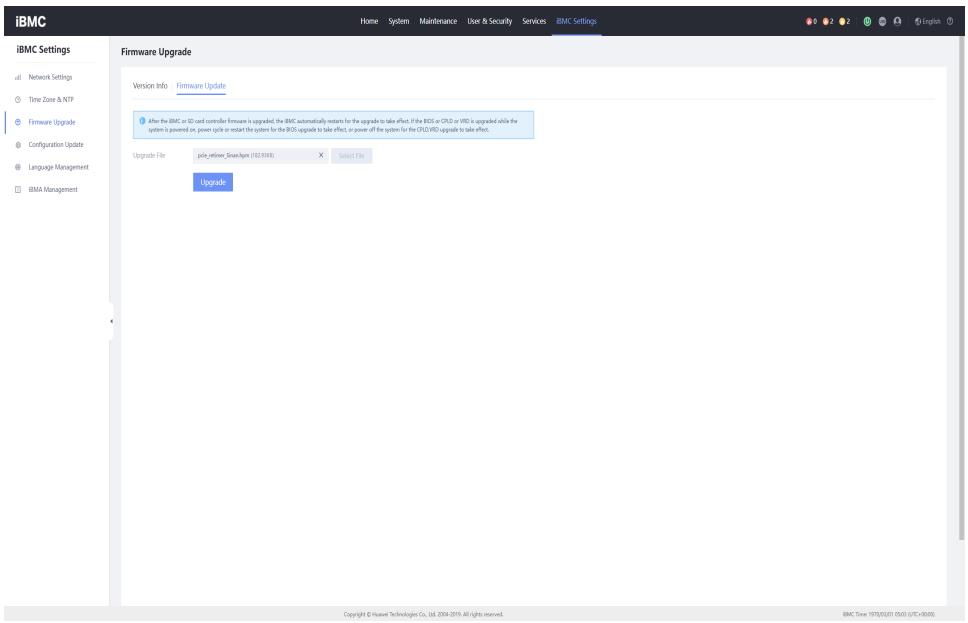


NOTE

The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 3 Click Select File to select the **pcie_retimer_Sinan.hpm** firmware to be upgraded. The following figure shows the iBMC WebUI.

Figure 3-94 Selecting the target firmware

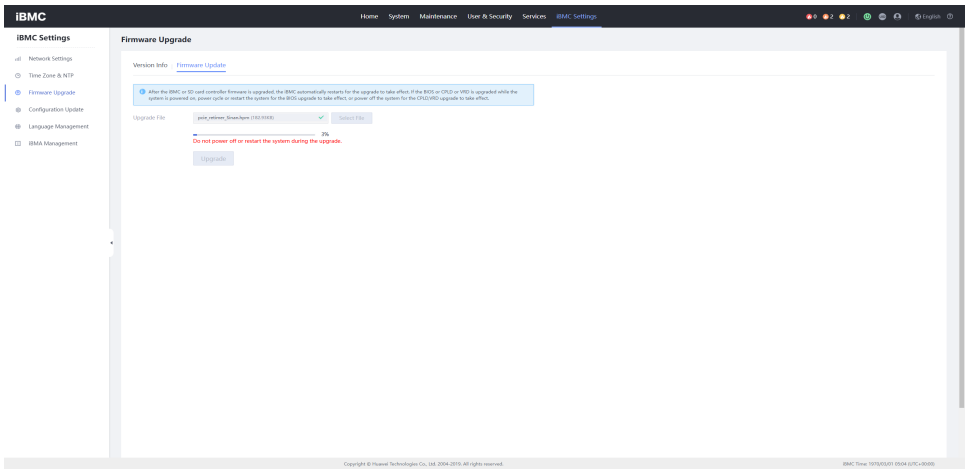


NOTE

The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 4 Click **Upgrade**. In the displayed dialog box, click **Yes** to perform the upgrade.

Figure 3-95 Upgrading the firmware



NOTE

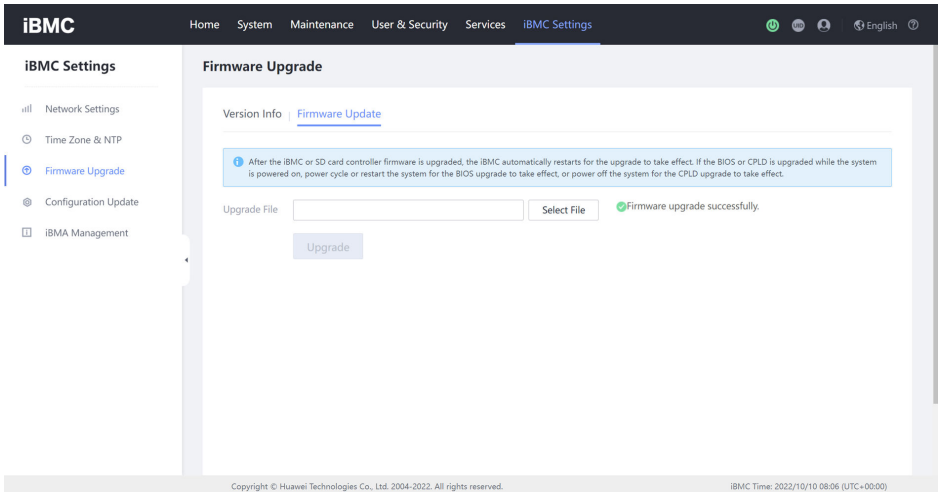
The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

NOTICE

During the firmware upgrade, buttons on the iBMC WebUI are unavailable. Do not perform any other operation before the upgrade is completed. The Retimer firmware upgrade takes about five minutes. If a fault occurs during the firmware upgrade, see **4 Troubleshooting** or contact maintenance or development personnel.

Step 5 Wait for the upgrade to complete. If **Firmware upgrade successfully** is displayed, the upgrade is completed. The following figure shows the iBMC WebUI.

Figure 3-96 Firmware upgraded successfully



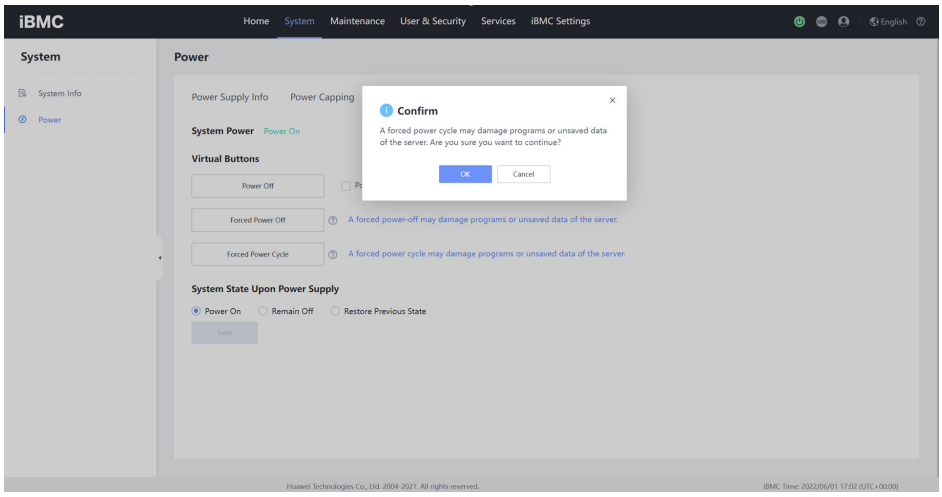
NOTE

The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Step 6 Make the upgrade take effect. If **System Power** is **Power On**, forcibly power off the system. Otherwise, do not perform any operation. Perform either of the following operations to make the upgrade take effect.

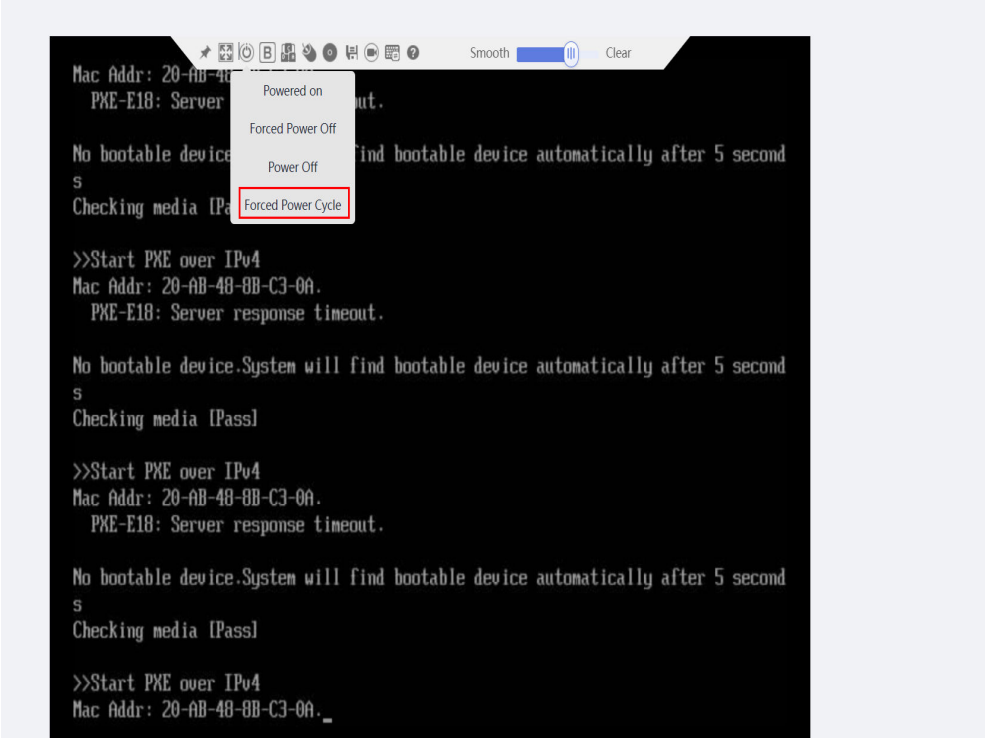
1. Choose **System** > **Power** > **Power Control**, click **Forced Power Cycle**, and click **OK** in the displayed dialog box. The following figure shows the iBMC WebUI.

Figure 3-97 Forced Power Cycle



2. Click **Forced Power Cycle** on the KVM, as shown in **Figure 3-98**.

Figure 3-98 Forced Power Cycle on the KVM



NOTE

- The information displayed on the iBMC WebUI varies with the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- Log in to the iBMC WebUI and choose **Home** > **Virtual Console**. Select a KVM login mode (shared mode or private mode) for the remote virtual console.

----End

3.3.14.3 Verifying the Upgrade

After the upgrade is complete, view the firmware version to check whether the new version takes effect. For details, see **3.3.14.1.3 Checking Versions**. If the new version and the version in the **version.xml** file are the same, the upgrade is successful. Otherwise, the upgrade fails and you need to contact maintenance or development personnel.

NOTE

The upgrade does not take effect immediately upon completion. Wait about 20 minutes and then verify if the upgrade is effective. If it has not taken effect after one hour, contact maintenance personnel.

3.3.15 Upgrading a Third-Party Card

For details about how to upgrade the firmware/driver of third-party cards (such as GPUs, NICs, and data collection cards), see the upgrade service and documents provided on the official website of the cards.

4 Troubleshooting

4.1 iBMC, BIOS, and CPLD Installation/Upgrade Troubleshooting (iBMC Earlier Than V561)

4.1.1 System Resetting During the BIOS Upgrade

Symptom

The system resets during the BIOS upgrade.

Possible Causes

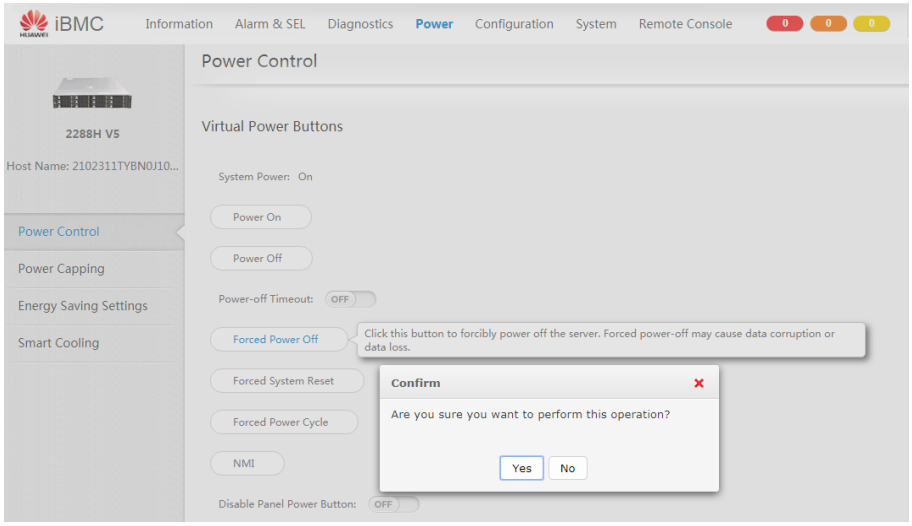
N/A

Handling Suggestion

Step 1 Wait about 15 minutes until the BIOS upgrade is complete. Perform the following operations no matter the BIOS upgrade is successful or not.

Step 2 Power off the system. Choose **Power** > **Power Control**. If the value of **System Power** is **On**, click **Forced Power Off** to power off the system. In the displayed dialog box, click **Yes**, as shown in **Figure 4-1**.

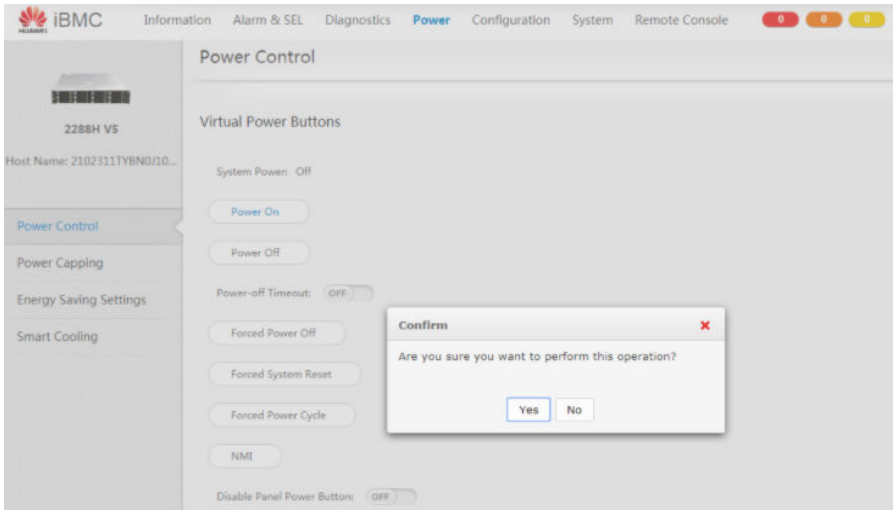
Figure 4-1 Powering off the system



After **Operation Successful** is displayed, wait about 20 seconds and check whether the value of **System Power** is **Off**, as shown in **Figure 4-1**. If **System Power** is **Off**, the system has been powered off and you can perform subsequent operations. Otherwise, contact maintenance or development personnel.

Step 3 Power on the system. Choose **Power** > **Power Control**, and click **Power On**. In the displayed dialog box, click **Yes**, as shown in **Figure 4-2**.

Figure 4-2 Powering on the system



After **Operation Successful** is displayed, wait about 20 seconds and check whether the value of **System Power** is **On**. If **System Power** is **On**, the system has been powered on and you can perform subsequent operations. Otherwise, contact maintenance or development personnel.

Step 4 Power off the system. Repeat **Step 2** to power off the system.

Step 5 Perform the upgrade.

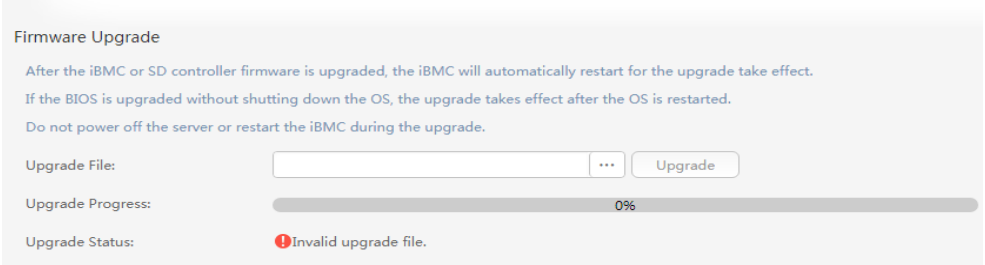
----End

4.1.2 Invalid Firmware Upgrade Package

Symptom

During an upgrade, **Invalid upgrade file** is displayed and the upgrade terminates, as shown in **Figure 4-3**.

Figure 4-3 Invalid firmware package



Possible Causes

- The firmware upgrade package does not match the device type. For example, the firmware of 2288H V5 is used on 5288 V5.
- The firmware upgrade package is corrupted.

Handling Suggestion

Step 1 Check whether the firmware upgrade package matches the device by following instructions in **1.1 Firmware List**.

Step 2 Obtain the firmware upgrade package and perform the upgrade again. If the upgrade still fails, contact maintenance or development personnel.

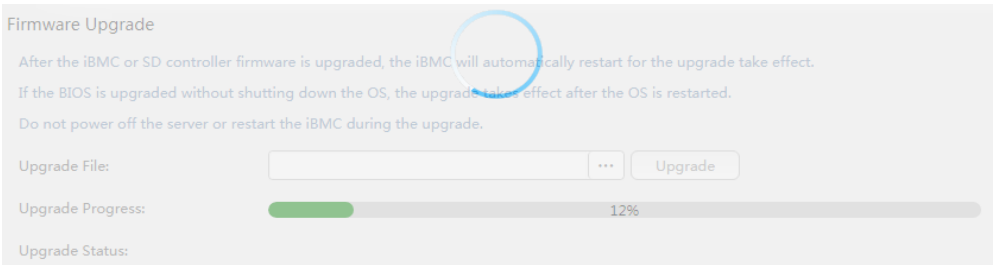
----End

4.1.3 Suspended Upgrade Progress

Symptom

During an upgrade, the upgrade progress is suspended at a value and does not update on the WebUI, as shown in **Figure 4-4**.

Figure 4-4 Upgrade progress suspended



Possible Causes

- The **Firmware Upgrade** page on the iBMC WebUI is frozen and the progress bar cannot be updated.
- During the upgrade, the iBMC system memory is insufficient and the system is suspended. As a result, the progress bar cannot be updated.

Handling Suggestion

Wait about 15 minutes, manually refresh the **Firmware Upgrade** page, and perform the upgrade again. Obtain the firmware upgrade package and perform the upgrade again. If the upgrade still fails, contact maintenance or development personnel.

4.1.4 Power Supply Fails During a BIOS Firmware Upgrade and the System Cannot Be Started

Symptom

The power supply fails during a BIOS firmware upgrade, and the system cannot be started after the power supply recovers.

Possible Causes

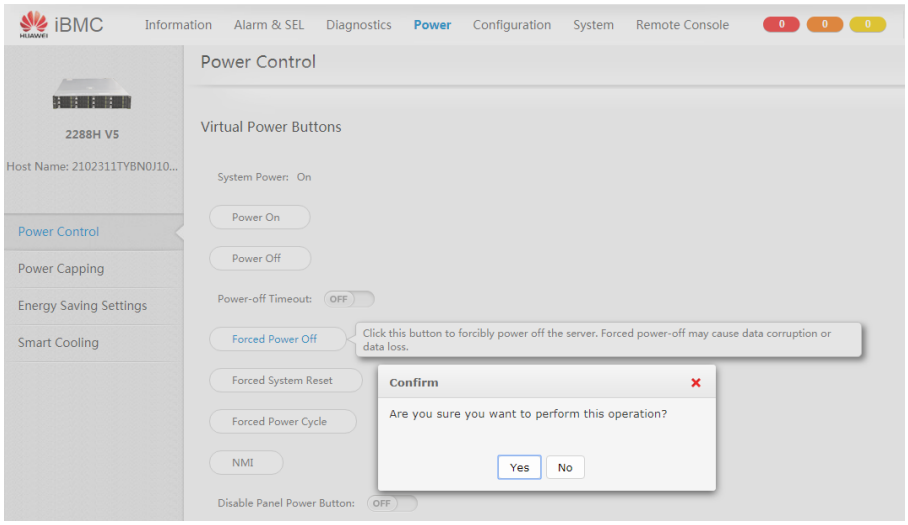
The BIOS program area or data area is corrupted. As a result, the BIOS cannot be started properly.

Handling Suggestion

Step 1 Log in to the iBMC WebUI.

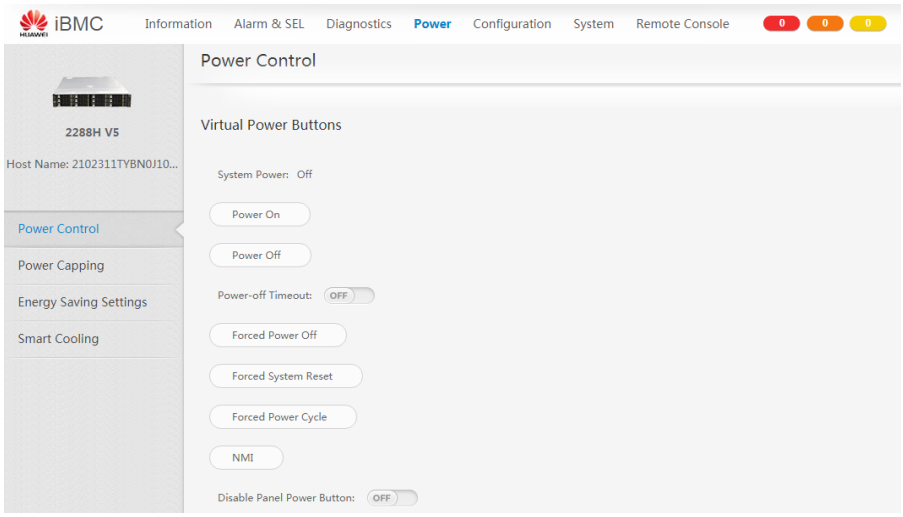
Step 2 Power off the system. Choose **Power** > **Power Control**. If the value of **System Power** is **On**, click **Forced Power Off** to power off the system. In the displayed dialog box, click **Yes**, as shown in **Figure 4-5**.

Figure 4-5 Powering off the system



After **Operation Successful** is displayed, wait about 20 seconds and check whether the value of **System Power** is **Off**, as shown in **Figure 4-6**. If **System Power** is **Off**, the system has been powered off and you can perform subsequent operations. Otherwise, contact maintenance or development personnel.

Figure 4-6 Querying the system power status



Step 3 Perform the upgrade.

----End

4.1.5 Power Supply Fails During a Mainboard CPLD Firmware Upgrade and the System Cannot Be Powered On

Symptom

The power supply fails during a mainboard CPLD firmware upgrade, and the system cannot be powered on after the power supply recovers.

Possible Causes

The CPLD program area is corrupted. As a result, the CPLD cannot be started properly.

Handling Suggestion

After the iBMC is powered on, log in to the WebUI to upgrade the mainboard CPLD firmware again. If the upgrade still fails, contact maintenance or development personnel.

4.2 iBMC, BIOS, and CPLD Installation/Upgrade Troubleshooting (iBMC V561 or Later, or iBMC V3.01.00.00 or Later)

4.2.1 System Resetting During the BIOS Upgrade

Symptom

The system resets during the BIOS upgrade.

Possible Causes

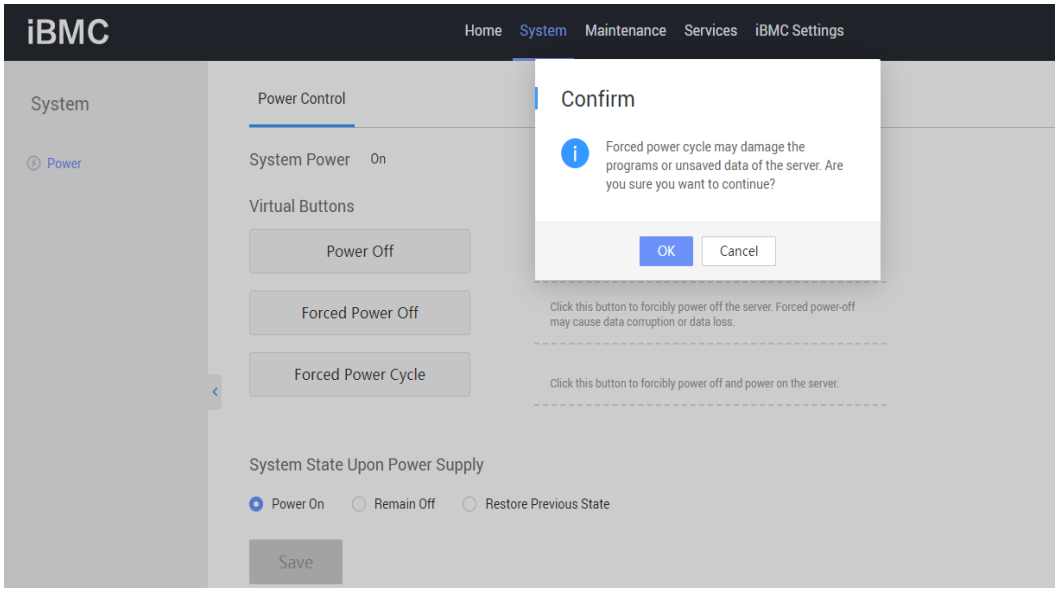
N/A

Handling Suggestion

Step 1 Wait about 15 minutes until the BIOS upgrade is complete. Perform the following operations no matter the BIOS upgrade is successful or not.

Step 2 Power off the system. Choose **System** > **Power** > **Power Control**. If the value of **System Power** is **On**, click **Forced Power Off** to power off the system. In the displayed dialog box, click **Yes**, as shown in **Figure 4-7**.

Figure 4-7 Powering off the system

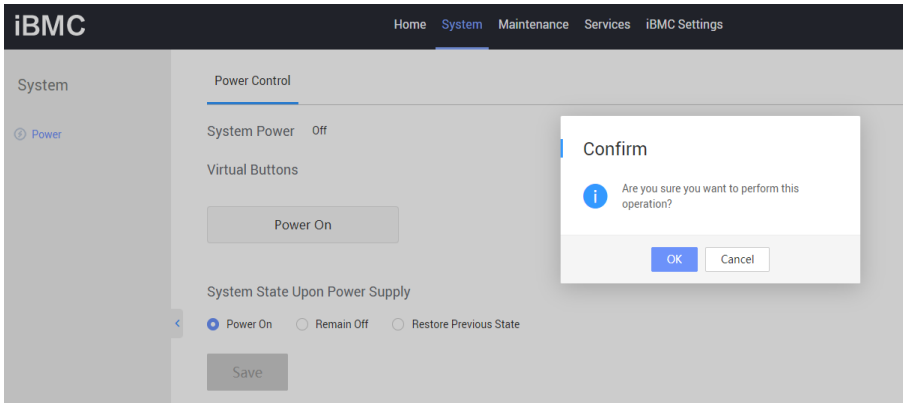


NOTE

- The information displayed on this page varies depending on the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- After the power-off operation, wait for about 20 to 60 seconds and check whether the value of **System Power** is **Off**, as shown in **Figure 4-7**. If **System Power** is **Off**, the system has been powered off, and you can perform subsequent operations. Otherwise, contact maintenance or technical support personnel.

Step 3 Power on the system. Choose **System** > **Power** > **Power Control**, click **Power On**, and click **OK** in the displayed dialog box, as shown in **Figure 4-8**.

Figure 4-8 Powering on the system



NOTE

- The information displayed on this page varies depending on the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- After the power-off operation, wait for about 20 to 60 seconds and check whether the value of **System Power** is **On**, as shown in **Figure 4-8**. If **System Power** is **On**, the system has been powered on, and you can perform subsequent operations. Otherwise, contact maintenance or technical support personnel.

Step 4 Power off the system. Repeat **Step 2** to power off the system.

Step 5 Perform the upgrade.

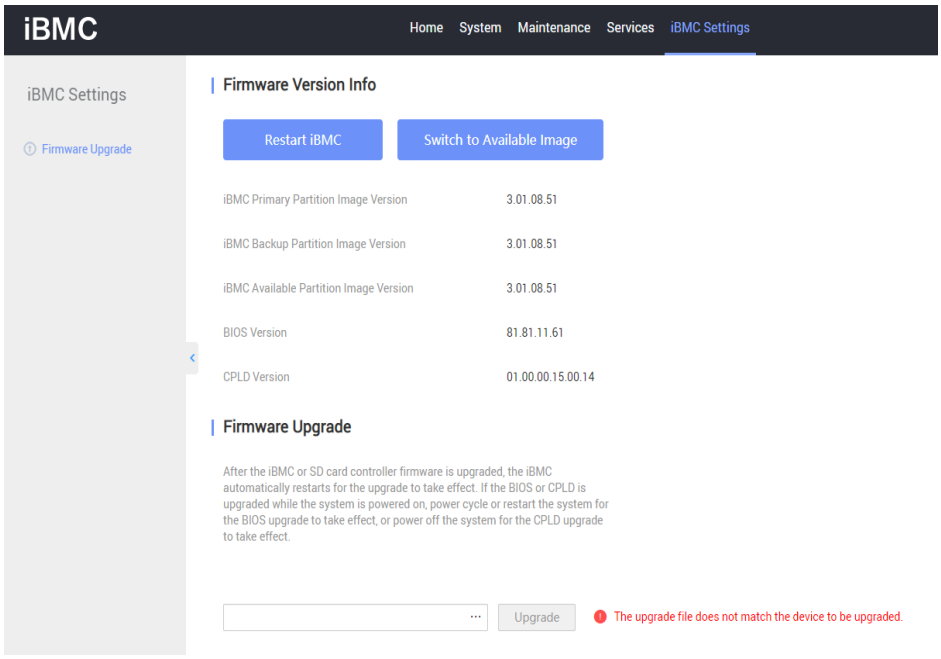
----End

4.2.2 The Upgrade File Does Not Match the Device to Be Upgraded

Symptom

During the upgrade, the message "The upgrade file does not match the device to be upgraded" is displayed and the upgrade stops, as shown in **Figure 4-9**.

Figure 4-9 Mismatching of the upgrade file and the device to be upgraded



NOTE

- The information displayed on this page varies depending on the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Possible Causes

- The firmware upgrade package does not match the device type. For example, the firmware of Taishan 2280 V2 is used on 2288H V5.
- The firmware upgrade package is corrupted.

Handling Suggestion

Step 1 Check whether the firmware upgrade package matches the device by following instructions in **1.1 Firmware List**.

Step 2 Obtain the firmware upgrade package and perform the upgrade again. If the upgrade still fails, contact maintenance or development personnel.

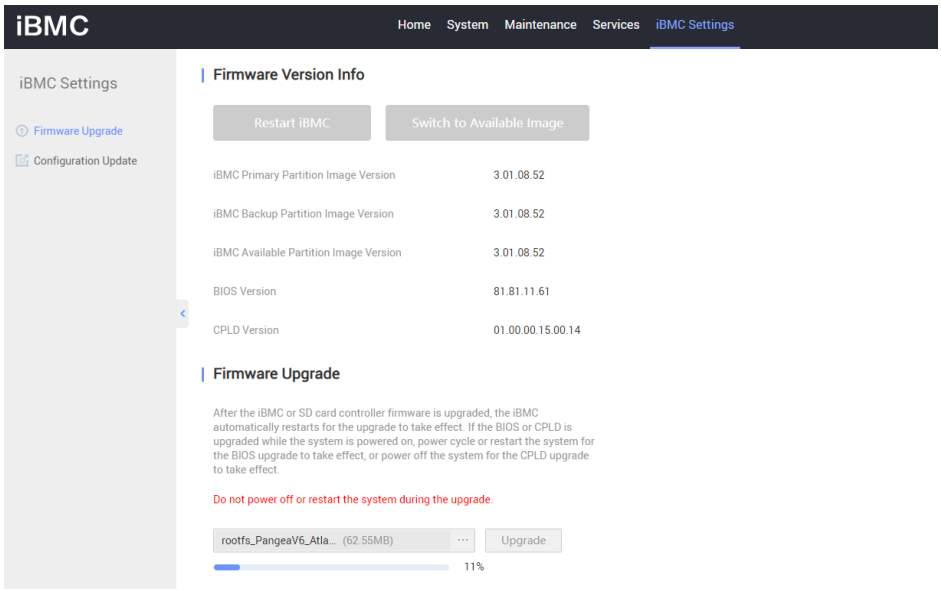
----End

4.2.3 Suspended Upgrade Progress

Symptom

During an upgrade, the upgrade progress is suspended at a value and does not update on the WebUI, as shown in **Figure 4-10**.

Figure 4-10 Upgrade progress suspended



NOTE

- The information displayed on this page varies depending on the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.

Possible Causes

- The **Firmware Upgrade** page on the iBMC WebUI is frozen and the progress bar cannot be updated.
- During the upgrade, the iBMC system memory is insufficient and the system is suspended. As a result, the progress bar cannot be updated.

Handling Suggestion

Wait about 15 minutes, manually refresh the **Firmware Upgrade** page, and perform the upgrade again. Obtain the firmware upgrade package and perform the upgrade again. If the upgrade still fails, contact maintenance or development personnel.

4.2.4 Power Supply Fails During a BIOS Firmware Upgrade and the System Cannot Be Started

Symptom

The power supply fails during a BIOS firmware upgrade, and the system cannot be started after the power supply recovers.

Possible Causes

The BIOS program area or data area is corrupted. As a result, the BIOS cannot be started properly.

Handling Suggestion

Step 1 Log in to the iBMC WebUI.

Step 2 Power off the system. Choose **System** > **Power** > **Power Control**. If the value of **System Power** is **On**, click **Forced Power Off** to power off the system. In the displayed dialog box, click **Yes**, as shown in **Figure 4-11**.

Figure 4-11 Powering off the system

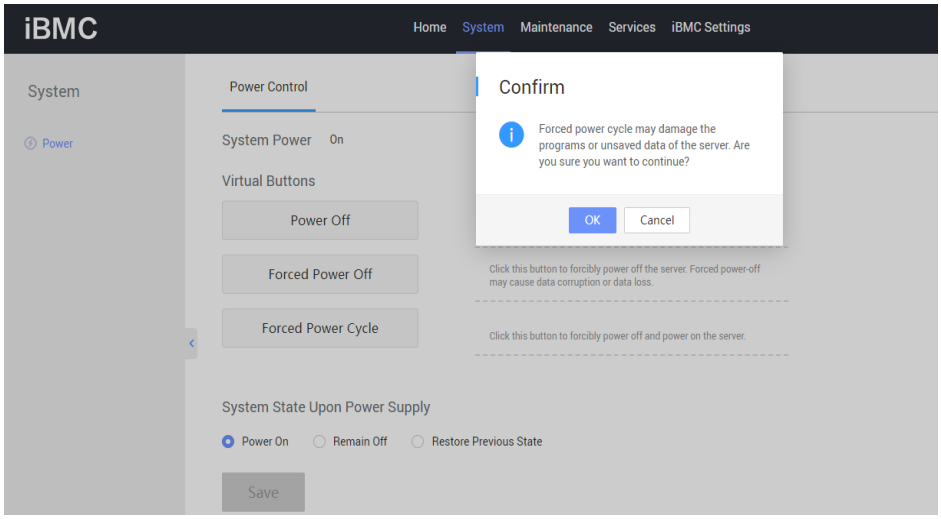
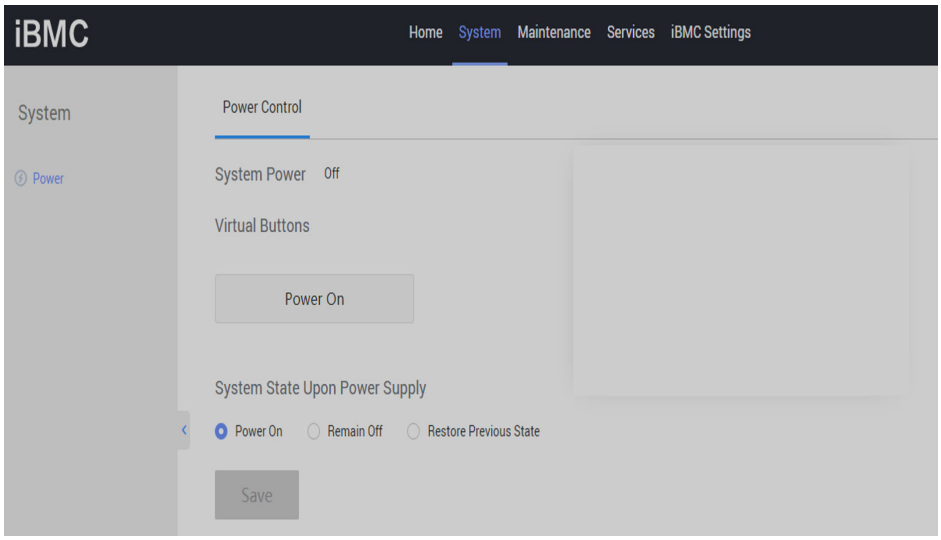


Figure 4-12 System in the power-off status



NOTE

- The information displayed on this page varies depending on the iBMC version. Perform operations as instructed on the actual page. If you have any questions, contact the maintenance personnel.
- After the power-off operation, wait for about 20 to 60 seconds and check whether the value of **System Power** is **Off**, as shown in **Figure 4-12**. If **System Power** is **Off**, the system has been powered off, and you can perform subsequent operations. Otherwise, contact maintenance or technical support personnel.

Step 3 Perform the upgrade.

----End

4.2.5 Power Supply Fails During a Mainboard CPLD Firmware Upgrade and the System Cannot Be Powered On

Symptom

The power supply fails during a mainboard CPLD firmware upgrade, and the system cannot be powered on after the power supply recovers.

Possible Causes

The CPLD program area is corrupted. As a result, the CPLD cannot be started properly.

Handling Suggestion

After the iBMC is powered on, log in to the WebUI to upgrade the mainboard CPLD firmware again. If the upgrade still fails, contact maintenance or development personnel.

4.3 Troubleshooting for Installing/Upgrading an RDMA NIC Driver, Basic Driver, SAS Expansion Module Driver, SATA System Disk Driver, and 1822 Interface Card Driver

4.3.1 OS Reset During the Upgrade

Symptom

During the upgrade of an RDMA NIC driver, basic driver, SATA system disk driver, SAS expansion module driver, and 1822 interface card driver, the OS resets.

Possible Causes

N/A

Handling Suggestion

After the OS is powered on, upgrade the components that are being upgraded before the restart.

5 FAQ

5.1 How Do I Upgrade SP?

See the SP user guide at the Huawei technical support website.

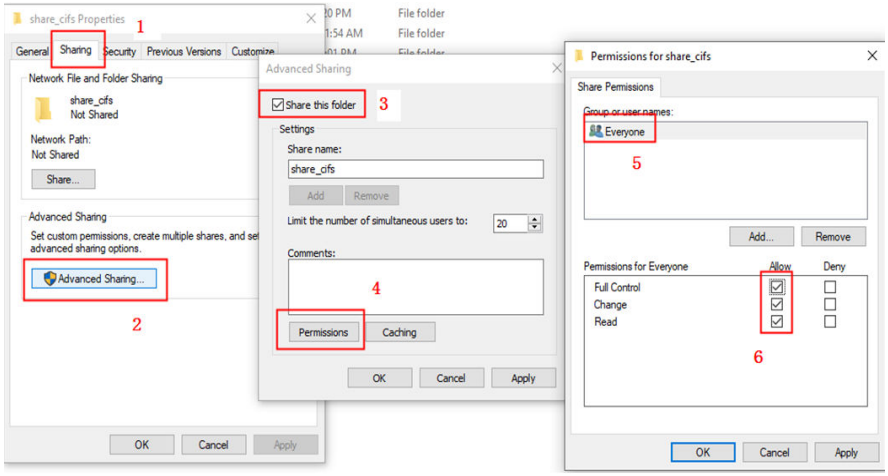
5.2 How Do I Enable CIFS Sharing?

The following uses Windows 10 as an example.

Step 1 Create a folder and copy the SP image file to the created folder.

Step 2 Configure folder sharing, as shown in **Figure 5-1**.

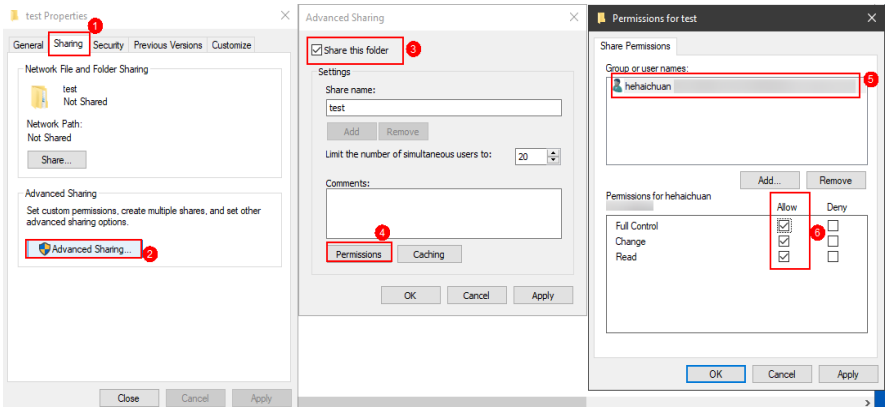
Figure 5-1 Configuring folder sharing on Windows 10



1. Right-click the created folder and choose **Properties** from the shortcut menu. The **share_cifs Properties** window is displayed.

2. Click the **Sharing** tab.
3. Click **Advanced Sharing**. The **Advanced Sharing** window is displayed.
4. Select **Share this folder** and click **Permissions**. The **Share Permissions** tab page is displayed.
5. Select **Full Control**, **Change**, and **Read** as required.

   If there are security restrictions on **Everyone**, delete **Everyone** and add a specified user.



6. Click **OK** to complete the configuration.

Step 3 Use another PC to view the shared file.

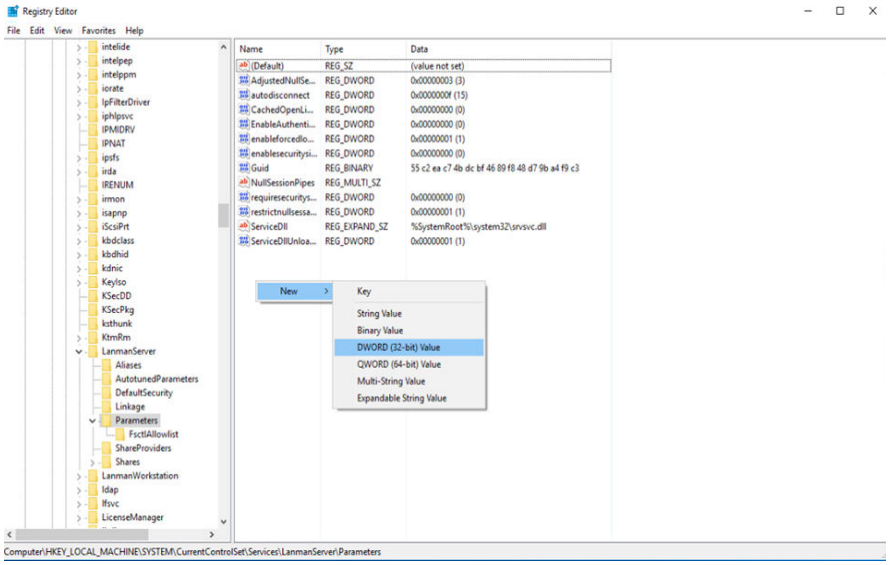
Step 4 Configure the registry and enable the SMB1 function.

NOTE

- The tool supports upgrade operations only in SMB (CIFS) 1.0.
- Back up the registry before configuration. The procedure is as follows:
- Click **Start** in the lower left corner, enter **regedit.exe** in the search box, and press **Enter**. The **Registry Editor** window is displayed.
  1. Right-click the subkey to be backed up and choose **Export** from the shortcut menu.
  2. Select the location where you want to save the backup file, enter the name of the backup file in the **File name** field, and then click **Save**.

1. Open registry folder **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**.
2. Search for the file whose registry entry is **SMB1**. If the file whose registry key is **SMB1** is not found, manually create a file named **SMB1**, as shown in **Figure 5-2**.

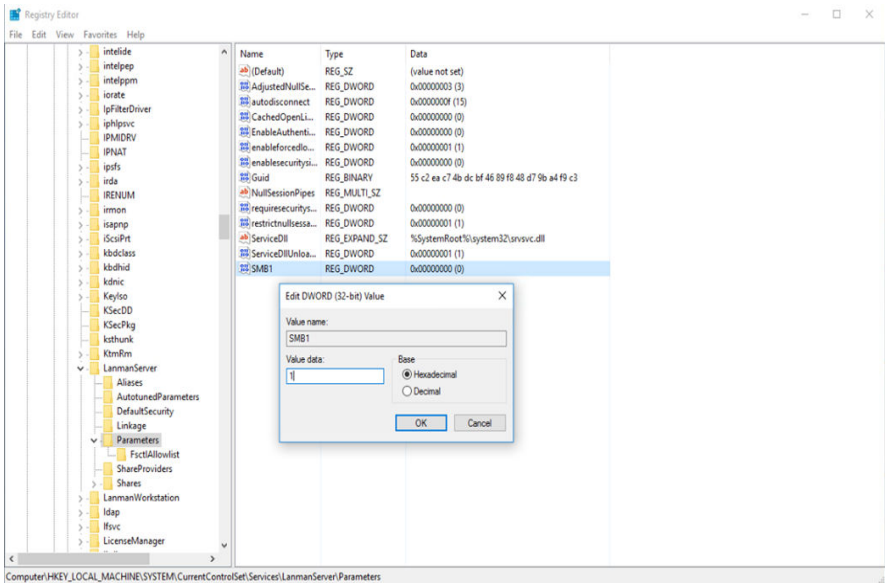
Figure 5-2 Creating SMB1



Step 5 Open SMB1 and change the value of **Value data** to 1, as shown in **Figure 5-3**. Then the SMB (CIFS) version of the registry is set to **1.0**.

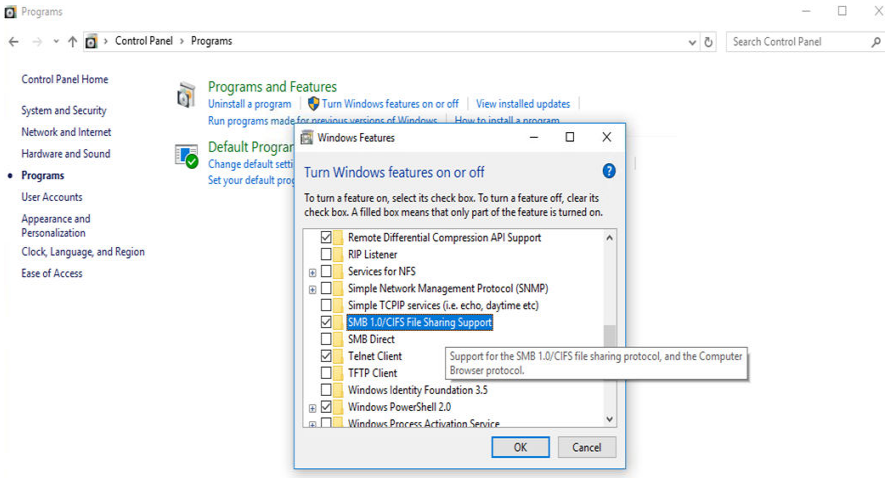
- If **Value data** is **0**, SMB is disabled.
- If **Value data** is **1**, SMB is enabled.
- The default value is 1, indicating that SMB is enabled (no registry entry is created).

Figure 5-3 Modifying SMB1



Step 6 Enable **SMB 1.0/CIFS File Sharing Support**, as shown in **Figure 5-4**.

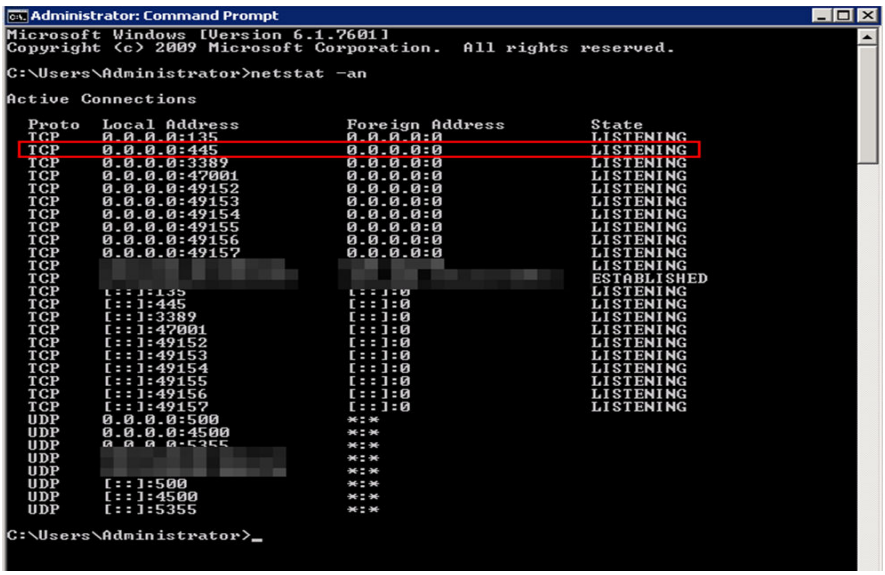
Figure 5-4 Enabling SMB 1.0/CIFS File Sharing Support



Step 7 After the configuration is complete, restart the computer for the configuration to take effect.

Step 8 Run the **netstat -an** command on the Windows CLI to query whether port 445 is enabled (port 445 is required by Windows CIFS). If information shown in **Figure 5-5** is displayed, port 445 is enabled.

Figure 5-5 Status of port 445 on Windows



----End

5.3 Importing the iBMC SSL Certificate

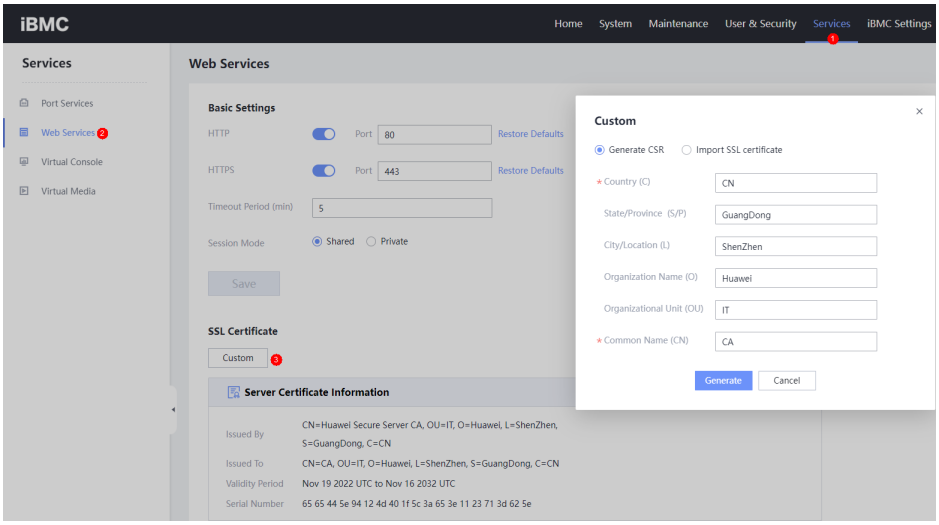
Customizing SSL Certificate Information and Importing an SSL Certificate

NOTE

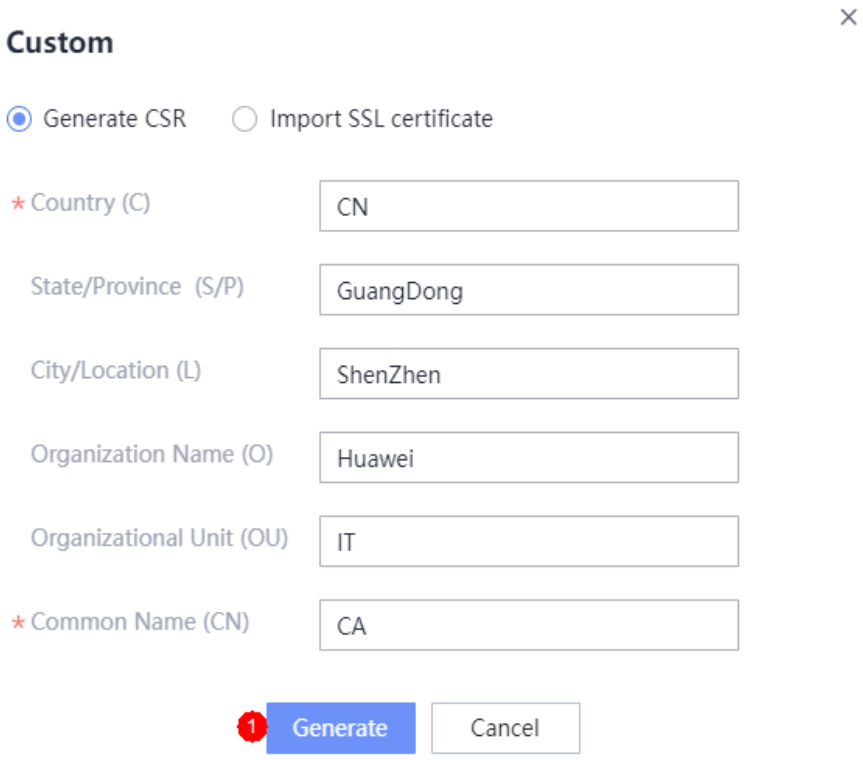
- Perform these operations when you apply for and import an SSL certificate.
- For security purposes, periodically update the certificate.

1. In the **SSL Certificate** area, click **Custom**.

   The **Custom** dialog box is displayed.



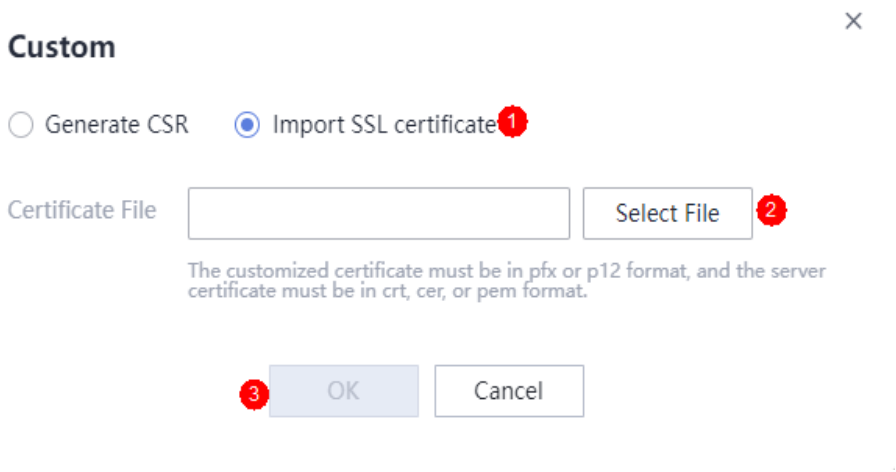
2. Select **Generate CSR**, enter the custom certificate request information, and click **Generate**.



3. Send the generated CSR file to the SSL certificate authority and apply for an SSL certificate.

   After obtaining the official SSL certificate, save it to the client.

4. In the **Custom** dialog box, select **Import SSL Certificate**.
5. Select the SSL certificate to be uploaded.



NOTE

- The certificate file to be imported must be in the **.crt**, **.cer**, **.pem**, **.pfx**, or **.p12** format. The certificate in the **.crt**, **.cer**, or **.pem** format cannot exceed 1 MB. The certificate file in the **.pfx** or **.p12** format cannot exceed 100 KB.
- MD5 is a weak signature algorithm, which poses security risks. The iBMC does not support the import of MD5-based certificates.

6. Click **Save**.
7. Enter the certificate password in **Certificate Password**.
8. Click **OK**.

   The certificate takes effect immediately after being imported.

   NOTE

   The customized CSR file correlates with the device certificate applied from the CA organization. Do not generate a new CSR file before importing the device certificate. Otherwise, you have to apply for a new device certificate from the CA organization.
9. Log in to the iBMC WebUI again.

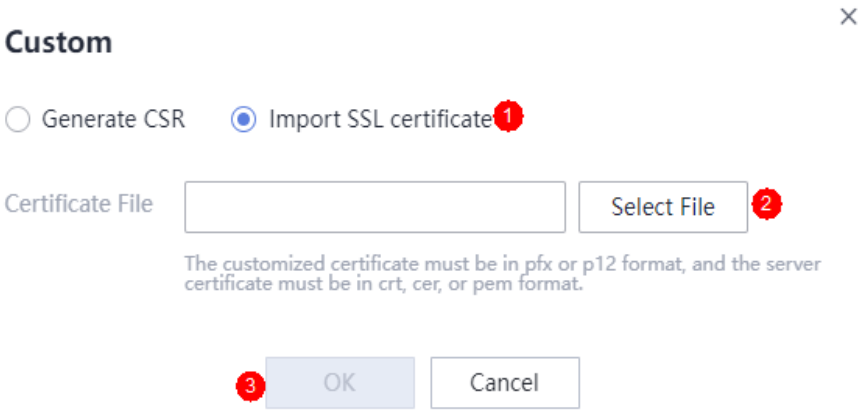
Importing an Existing SSL Certificate

NOTE

- Perform this operation only when an SSL certificate is available on the client.
- For security purposes, use a secure encryption algorithm, for example RSA2048, to encrypt the customized certificate.
- For security purposes, periodically update the certificate.

1. In the **SSL Certificate** area, click **Custom**.

   The **Custom** dialog box is displayed.
2. Select **Import SSL Certificate**.
3. Select an existing SSL certificate file to be imported.



NOTE

- The certificate file to be imported must be in the **.crt**, **.cer**, **.pem**, **.pfx**, or **.p12** format. The certificate in the **.crt**, **.cer**, or **.pem** format cannot exceed 1 MB. The certificate file in the **.pfx** or **.p12** format cannot exceed 100 KB.
- MD5 is a weak signature algorithm, which poses security risks. The iBMC does not support the import of MD5-based certificates.

4. Click **Save**.
5. Enter the certificate password in **Certificate Password**.
6. Click **OK**.

   The certificate takes effect immediately after being imported.

   NOTE

   If the size of the file to be uploaded exceeds 100 MB, a message indicating a page request failure is displayed. You can refresh the page to resolve this issue.
7. Log in to the iBMC WebUI again.

