FusionServer Pro Rack Server iBMC V260 to V278

User Guide

Issue	22
Date	2022-07-29

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	https://e.huawei.com

About This Document

Purpose

This document describes the underlying management software Intelligent Baseboard Management Controller (iBMC) of the servers. It includes the following:

- Functions and features of the iBMC
- iBMC web user interface (WebUI)
- iBMC command line interface (CLI)
- Commands used on the iBMC

> **NOTE**
>
> This document describes only the commands used to deploy and maintain servers. It does not include the following commands:
>
> - Commands for server manufacturing, assembling, and factory inspection and repair.
> - Commands for engineering implementation or fault locating.
>
> Inappropriate use of these commands may result in device faults or service interruption. To obtain information about these commands, contact technical support.

This document applies to the following FusionServer Pro servers:

- RH1288A V2 and RH2288A V2
- 5288 V3, RH1288 V3, RH2288 V3, RH2288H V3, RH5885 V3, RH5885H V3, and RH8100 V3
- 1288H V5, 2288 V5, 2288C V5, 2288H V5, 2488 V5, 2488H V5, 5885H V5, and 8100 V5

Intended Audience

This document is intended for:

- Server installation engineers
- Server maintenance engineers

The person who installs, manages, and troubleshoots servers must be qualified in servicing servers and trained in recognizing hazards in products with hazardous energy levels.

Symbol Conventions

The following table lists the symbols that may be found in this document.

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Issue	Date	Description
22	2022-07-29	Updated **6.5 Configuring the SMTP Function on the iBMC WebUI**.
21	2022-07-25	Deleted the function of clearing logs.
20	2021-07-05	Updated **3.7.2 LDAP**.
19	2021-06-07	Updated **3.8.6 Firmware Upgrade**.
18	2021-04-21	Updated **6.3 Restoring Default iBMC Settings**.

Issue	Date	Description
17	2021-03-17	Updated **3.7.6 Services** and **3.10.1 Failed to Open the Remote Virtual Console**.
16	2021-02-05	Updated **3.6.4 Smart Cooling**.
15	2020-11-15	Updated **3.7.10 Import/Export**, **3.9 Remote Console**, **4.2.2 Querying the IP Address of the Management Network Port**, **6.10 Configuring Syslog on the iBMC WebUI** and **6.11 Logging In to a Server Using VNC**.
14	2019-11-11	Updated **3.8.6 Firmware Upgrade**, **4.3.28 Mounting a File to the Virtual CD-ROM Drive (vmm -d connect)**, and **4.8.21 Querying and Setting the In-Band User Management Status (user -d usermgmtbyhost)**.
13	2019-07-30	Changed the document name.
12	2019-05-30	Updated **4.3.28 Mounting a File to the Virtual CD-ROM Drive (vmm -d connect)**, **4.7.9 Querying the Serial Number of the Server (serialnumber)**, and **4.8.17 Importing the Weak Password Dictionary (weakpwddic -v import)**.
11	2019-02-22	Updated **4.5.1 Querying and Setting Syslog (syslog -d state)**.
10	2018-11-05	Updated **3.8.6 Firmware Upgrade**, **3.9.1 Java Integrated Remote Console**, and **7 Independent Remote Console**.
09	2018-08-08	● Updated **3.1 Logging In to the iBMC WebUI**, and **3.9.1 Java Integrated Remote Console**. ● Added section **6.12 Importing the iBMC Trust and Root Certificates**.
08	2018-07-05	Updated **3.4.3 Alarm Settings**, and **3.9 Remote Console**.
07	2018-06-07	Added section **7.5 Logging In to a Server Using the Independent Remote Console (Red Hat)**.
06	2018-05-30	Updated **3.7.7 System** and **3.11 One-Click Information Collection**.

Issue	Date	Description
05	2018-03-29	Updated **3.6.1 Power Control**, **3.6.3 Energy Saving Settings** and **4.10.3 Setting the UID Indicator Status (locate)**.
04	2018-02-11	Updated **Table 3-44**.
03	2018-01-31	• Modified the product asset tag description in **Table 3-3**. • Updated **Table 3-70**. • Added section **8 Smart Provisioning**.
02	2017-12-28	Modified **3.5.4 Black Box**.
01	2017-11-12	This issue is the first official release.

Contents

1 iBMC Overview

1.1 iBMC Functions

The intelligent Baseboard Management Controller (iBMC) is an intelligent management system that remotely manages servers. It provides rich management functions and features.

- Multiple management interfaces for system integration

  The iBMC supports the following interfaces:

  - Data Center Manageability Interface Specification v1.5 (DCMI 1.5)

  - Intelligent Platform Management Interface (IPMI) 1.5 and 1.2

  - Command-line interface (CLI)

  - Redfish interface

  - Hypertext Transfer Protocol Secure (HTTPS) interface

  - Simple Network Management Protocol (SNMP)

- Fault monitoring and diagnostics

  The iBMC detects hidden risks and ensures stable, uninterrupted 24/7 system operation by providing the following features:

  - System breakdown screenshots and video playback

    Help identify the cause of system breakdown.

  - Screen snapshots and videos

    Simplify routine preventive maintenance, recording, and auditing.

  - Fault diagnosis & management (FDM)

    Provides precise fault diagnosis based on components, facilitating identifying and replacement of faulty parts.

  - Report of alarms using syslog, trap, and email

    Facilitates report of server alarms to the upper-layer network management system (NMS) and helps users learn about server alarms in a timely manner.

  - Support for the LCD to obtain device information from the iBMC

- Security management

- The iBMC uses image mirroring to improve system security. Even if the running software breaks down, the system can start from the backup image.

- Diversified user security control interfaces ensure login security.

- The iBMC supports import and replacement of multiple types of certificates to ensure data transmission security.

- System maintenance interfaces

  - The iBMC supports keyboard, video, and mouse (KVM) and virtual media to facilitate remote maintenance.

  - The iBMC supports RAID out-of-band monitoring and configuration, improving RAID configuration efficiency and management.

  - The Smart Provisioning implements OS installation, RAID configuration, and upgrades without a DVD, simplifying server installation and configuration.

- Diversified network protocols

  - The iBMC supports the Network Time Protocol (NTP) to facilitate time settings and ensure time synchronization.

  - The iBMC supports domain management and directory services to simplify network management.

- Intelligent power supply management

  The iBMC provides power capping to improve deployment density and dynamic energy saving to reduce the operating expense (OPEX).

1.2 Security Features

- NC-SI

  The iBMC implements isolation between the management plane and the service plane. The Network Controller Sideband Interface (NC-SI) allows the iBMC and the service plane to share the same network interface card (NIC). Although the management and service planes share a physical network port, they are logically isolated by VLANs and are invisible to each other.

- Protocol and port protection against attacks

  The iBMC provides the minimum required network service ports. By default, unnecessary services are disabled, network service ports for debugging are disabled during server normal operation, and network ports for insecure protocols are disabled.

- Condition-based login restrictions

  The iBMC ensures secure web access by using login rules and user roles. A role specifies the operation permission of a user, and login rules implement time- and location-based access.

  A maximum of three login rules can be configured. Each login rule contains three conditions: login duration, source IP address segment, and source MAC address segment. Users who comply with any one of the three rules can log in to the iBMC.

- User account security

  The iBMC ensures user account security through the following settings:

- – Password complexity rule
- – Weak password dictionary
- – Password validity period
- – Minimum password age
- – Account inactive period
- – Emergency login user
- – Number of restricted previous passwords
- – Maximum number of login failures before account lockout

- Certificate management

  The iBMC supports encryption and replacement of Secure Sockets Layer (SSL) certificates. Users can replace the certificates on the WebUI.

  It is recommended that the original certificate and keys be replaced with customized certificate and public and private key pairs in time for security purposes.

  The iBMC supports import of an LDAP certificate, which makes LDAP data transmission confidential and secure.

- Operation log management

  The iBMC records all non-query operations performed on the iBMC. The operation logs are classified into Linux system process logs and user process logs. Each user process log contains the time when the operation was performed, the interface on which the operation was performed, source IP address, user name, and operation.

- Encryption of data transmitted

  The iBMC allows you to enable Transport Layer Security (TLS) for Simple Mail Transfer Protocol (SMTP) to ensure data transmission security.

  The iBMC also allows you to enable the KVM and VNC encryption functions, which encrypt data transmitted to and from the Remote Virtual Console.

1.3 Common Operation Interfaces

The iBMC supports a variety of operation interfaces, such as the IPMI for internal communication, the SNMP interface for interworking with the upper-layer network management system, and single-server operation interfaces. The following describes the common operation interface for single server management.

1.3.1 iBMC WebUI

The iBMC web user interface (WebUI) provides an intuitive interface for users to perform server management. Similar tasks are grouped for easy navigation and workflow. The iBMC WebUI provides the **Information**, **Alarm & SEL**, **Diagnostics**, **Power**, **Configuration**, **System**, and **Remote Console** modules. The navigation tree in the left further divides the tasks in each module.

When using the iBMC WebUI, you can click at the upper right corner of the page to obtain help information.

The iBMC WebUI supports Chinese, English, Japanese, and French. You can select the language to be used from the text box at the upper right corner of the page.

For more details, see **3 iBMC WebUI**.

1.3.2 iBMC CLI

The iBMC command-line interface (CLI) provides the **ipmcset** command for set operations and the **ipmcget** command for query operations. You can perform operations on the iBMC through the CLI.

For details, see **4 iBMC CLI**.

1.3.3 Redfish Interface

The iBMC supports the standard Redfish interface. The Redfish client (Redfish interface tool, for example, Chrome Postman) sends HTTPS operation requests to the server, and implements information query, configuration, and monitoring of the server using the **GET**, **PUT**, **PATCH**, **POST**, and **DELETE** commands.

For details, see the **iBMC Redfish API Description**.

1.3.4 iBMC SmartServer Mobile

SmartServer Mobile is a mobile application that allows users to access iBMC using a mobile device. SmartServer Mobile directly interacts with the iBMC to implement configuration and monitoring of services.

For details, see the **Huawei Server SmartServer User Guide**.

2 Before You Start

2.1 Guidelines for Using the iBMC

- Use a dedicated network to configure the iBMC.
- Do not connect the iBMC with the Internet.
- Disable the protocols and ports that are not used or pose security risks.
- Change the initial user name and password in time and keep them secure.
- Periodically audit the operation logs.

2.2 Obtaining the iBMC Version

The iBMC version *X.XX* is also referred to as *VXXX*. For example, version **2.60** is also referred to as **V260**.

You can obtain iBMC version information from any of the following:

- iBMC Release Notes

    a. Select the server model and click **Software Download**.

    b. Click the server version.

    c. Obtain the iBMC Release Notes.

    The iBMC version number is included in the name of the Release Notes.
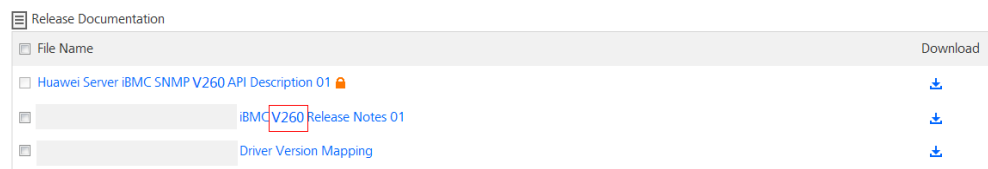
- iBMC WebUI

    Log in to the iBMC WebUI and click the **Information** menu.

    The **iBMC Firmware Version** parameter in the **Basic Info** area indicates the iBMC version.
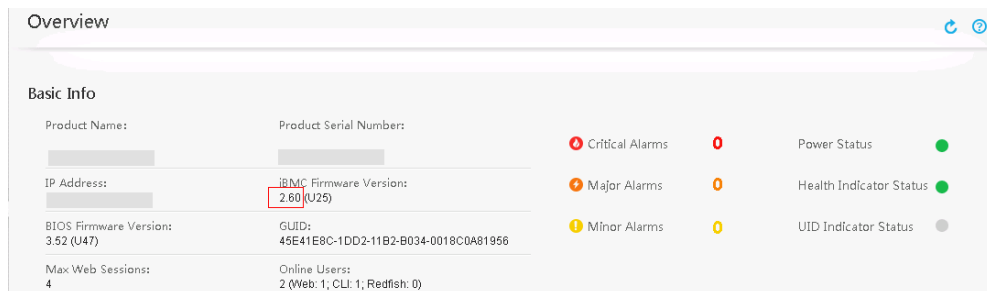
- iBMC CLI

  Log in to the iBMC CLI and run the **ipmcget -d version** command.

  The command output displays the iBMC version.

  ```
  ......
  Active iBMC    Version:       (U25)2.60
  Active iBMC     Build:        002
  ......
  ```

2.3 Default Credentials

Table 2-1 lists the default credentials for the iBMC. The default credentials are used for first login or login after you restore the iBMC to factory settings. For security purposes, change the default password at the first login and change your password periodically.

Table 2-1 Default credentials

Parameter	Default Credentials for V3 Servers	Default Credentials for V5 Servers
iBMC user name and password	User name: **root** Password: **Huawei12#$**	User name: **Administrator** Password: **Admin@9000**

iBMC management port IP address	• RH8100 V3/8100 V5:
	   – 8-socket single system: 192.168.2.100
	   – 4-socket dual systems:
	     – Primary management network port: 192.168.2.100
	     – Secondary management network port: 192.168.2.101
	 • Other rack servers: 192.168.2.100
		• RH8100 V3/8100 V5:
		   – 8-socket single system: 192.168.2.100
		   – 4-socket dual systems:
		     – Primary management network port: 192.168.2.100
		     – Secondary management network port: 192.168.2.101
		 • Other rack servers: 192.168.2.100

U-Boot password	Huawei12#$	Admin@9000

Parameter	Default Credentials for V3 Servers	Default Credentials for V5 Servers
SNMP read-only community name	roAdmin12#$	roAdministrator@9000
SNMP read-write community name	rwAdmin12#$	rwAdministrator@9000
Trap community name	TrapAdmin12#$	TrapAdmin12#$

2.4 Login Precautions

iBMC IP Address

- For the first time to log in, use the default iBMC IP address.

  You can obtain the default IP address from the server nameplate or **2.3 Default Credentials**.

- After your first login, change the iBMC IP address based on service requirements and keep it secure for subsequent network configuration.

  The iBMC IP address can be changed as follows:

  - Access the iBMC WebUI and change the IP address. For details, see **3 iBMC WebUI**.

  - Access the iBMC CLI and change the IP address. For details, see **4 iBMC CLI**.

  - Access the BIOS setup utility and change the IP address. For details, see the *BIOS Parameter Reference*.

  - Change the IP address through the specific interface (SNMP or Redfish) from the upper-layer NMS.

- If the iBMC is configured with a DNS or DHCP server, the iBMC address will be dynamically allocated.

  You can obtain the iBMC IP address as follows:

  - On the DHCP server, query the iBMC address based on the MAC address.

  - On the upper-layer NMS, query the iBMC IP address of the server managed by the NMS.

  - Connect to the iBMC serial port from a PC, and query the IP address on the CLI.

  - Connect to the BIOS using a KVM and query the iBMC IP address.

iBMC Users

The iBMC supports the following two types of users:

- Local users: The iBMC supports a maximum of 16 local users. The local access mode is deal for small environments, such as labs and small- and medium-size enterprises (SMEs).

● Lightweight Directory Access Protocol (LDAP) users: The number of users and user rights are set on the LDAP server, which allows more users to access the iBMC. This access mode is ideal for environments with many users.

iBMC Clients

The clients used to log in to the iBMC WebUI must meet the following requirements. If the remote console needs to be used, use the browser and Java of the correct version.

Table 2-2 Running environment

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	

OS	Browser	JRE
Windows Server 2008 R2 64-bit	Internet Explorer 9.0 to 11.0 **NOTE** HTML5 supports only Internet Explorer 10.0 or later.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Windows Server 2012 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45 JRE 1.8 U45 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 OS 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	

3 iBMC WebUI

3.1 Logging In to the iBMC WebUI

This section uses Internet Explorer 11 as an example to describe how to log in to the iBMC WebUI.

📖 **NOTE**

- A maximum of four users can log in to the iBMC WebUI at the same time.

- By default, the system timeout period is 5 minutes. If no operation is performed on the WebUI within 5 minutes, the user will be automatically logged out of the WebUI.

- The system locks a user account if the user enters incorrect passwords for five consecutive times. The user account is automatically unlocked five minutes later. The system administrator can also unlock a user account using the command line.

- For security purposes, change the initial password after the first login and change your password periodically.

Step 1 Check that the OS and browser versions of the iBMC client (a local PC) are as per requirements. If the remote control function needs to be used, ensure that the Java Runtime Environment (JRE) version is as per requirements.

See **Table 3-70** for version requirements.

Step 2 Set an IP address for the PC, and ensure that the IP address is on the same network segment as the iBMC management network port.

- For a single-system rack server, the default IP address of the iBMC management network port is **192.168.2.100**.

- For a dual-system rack server, the default IP address is **192.168.2.100** for the primary iBMC management network port and **192.168.2.101** for the secondary iBMC management network port.

Step 3 Connect the PC to the iBMC management network port using a network cable.

Step 4 Open Internet Explorer, enter https://*IP address of the iBMC management network port* in the address box, and press **Enter**. For details about how to obtain the IP address, see **4.2.2 Querying the IP Address of the Management Network Port**.

Information shown in **Figure 3-1** is displayed.

Figure 3-1 Website security alert
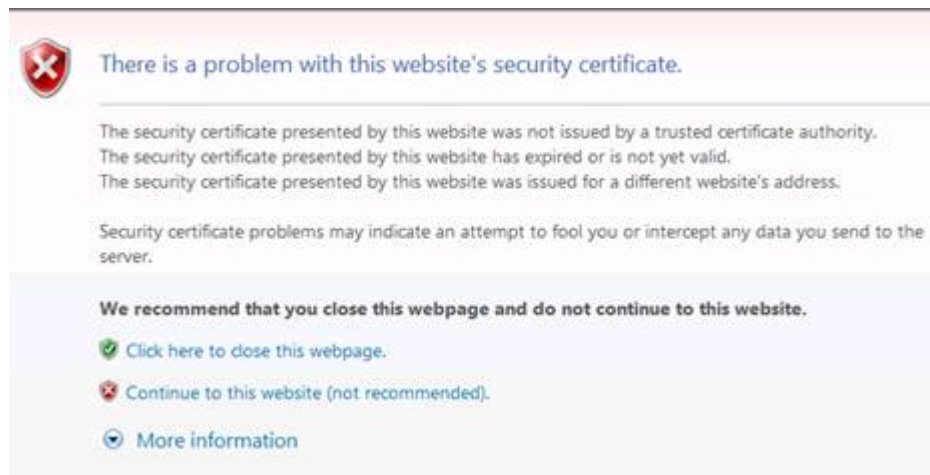
📖 **NOTE**

● If the language of the browser you use to log in to the iBMC WebUI is not Chinese, English, or Japanese, upgrade the iBMC to V260 or later. Otherwise, the login page may fail to display.

● If a website security alert is displayed, you can ignore this message or perform any of the following to shield this alert:

– Import a trust certificate and a root certificate to the iBMC. For details, see **6.12 Importing the iBMC Trust and Root Certificates**.

– If no trust certificate is available, add the iBMC to the **Exception Site List** on **Java Control Panel**. This operation, however, poses security risks.

Step 5 Click **Continue to this website (not recommended)**.

The login page is displayed, as shown in **Figure 3-2**.

Figure 3-2 iBMC login page
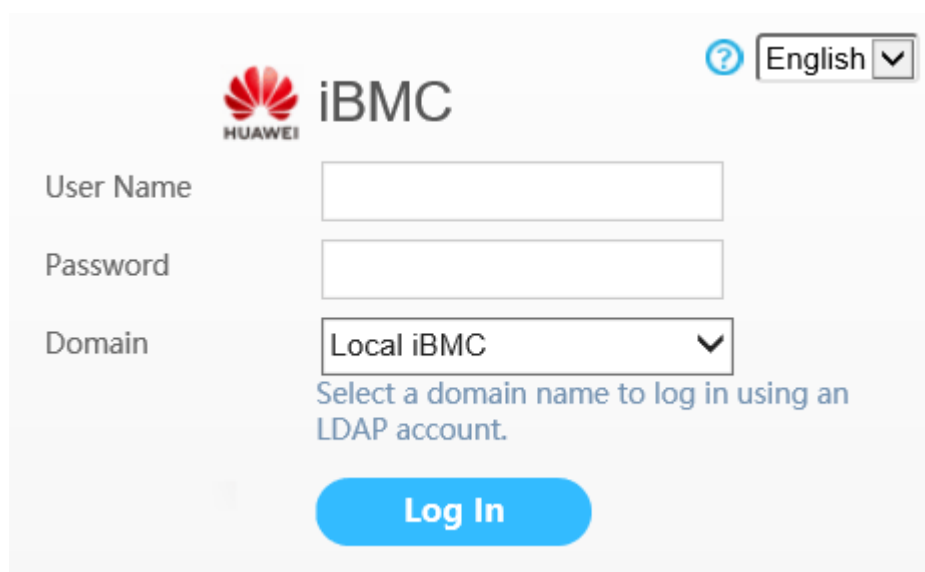
Step 6 Log in to the iBMC WebUI.

> 📖 **NOTE**
>
> ● When **Domain** is **Local iBMC**, the maximum length of the user name is 20 characters.
>
> ● When **Domain** is not **Local iBMC**, the maximum length of the user name is 255 characters.
>
> ● In versions earlier than iBMC V294, the maximum length of the password for an LDAP user to log in to the iBMC WebUI is 20 characters. In iBMC V294 and later versions, the maximum length of the password for an LDAP user to log in to the iBMC WebUI is 255 characters.

Logging In as a Local User

1. Select the language to be used.

2. Enter the user name and password.

   > 📖 **NOTE**
   >
   > – The default iBMC user name is **root**, and default password is **Huawei12#$** for V3 servers.
   >
   > – The default iBMC user name is **Administrator**, and default password is **Admin@9000** for V5 servers.

3. Select **Local iBMC** or **Automatic matching** from the **Domain** drop-down list.

4. Click **Log In**.

   The **Information** page is displayed, showing the user name in the upper right corner.

   > 📖 **NOTE**
   >
   > – The system may display a message indicating incorrect user name or password when you attempt to log in using Internet Explorer after the system is upgraded. If this occurs, press **Ctrl**+**Shift**+**DEL**, click **Delete** in the dialog box displayed to clear the browser cache, and attempt to log in again.
   >
   > – If the login still fails, choose **Tools** > **Internet Options** > **Advanced** in the menu bar and click **Reset** to restore default settings of Internet Explorer. Then attempt to log in again.

Logging In as a Domain User

Before login, ensure that the following settings meet the requirements:

● A domain controller exists on the network, and a user domain and Lightweight Directory Access Protocol (LDAP) users have been created on the domain controller.

   > 📖 **NOTE**
   >
   > For details about how to create a domain controller, a user domain, and LDAP users, see domain controller documents. The iBMC provides only the access function for LDAP users.

● On the iBMC WebUI, the LDAP function has been enabled, and a user domain and LDAP users have been set. For details, see the **LDAP** page.

   a. Select the language to be used.

   b. Enter the LDAP user name and password.

NOTE

The user name in the following formats are supported:

- LDAP user name (**Domain** can be **Automatic matching** or a specified domain)

- *LDAP user name@Domain name* (**Domain** must be **Automatic matching**)

In versions earlier than iBMC V294, the maximum password length for an LDAP user is 20 characters. In iBMC V294 and later versions, the maximum password length for an LDAP user is 255 characters.

c. Select the LDAP user domain from the **Domain** drop-down list.

NOTE

The **Domain** drop-down list contains the following options:

- **Local iBMC**: Select this option to log in as a local user. The iBMC automatically locates the user from the local user list.

- **Configured domain server**: Select a domain server to log in as an LDAP user. The iBMC locates the user from the domain server.

- **Automatic matching**: If this option is selected, the iBMC searches for the user from the local user list first. If no match is found, the iBMC searches from the domain servers in the sequence displayed in the **Domain** drop-down list.

d. Click **Log In**.

The **Information** page is displayed, showing the user name in the upper right corner.

----End

3.2 Getting Started

3.2.1 Basic Operations

Table 3-1 describes the basic operations on the iBMC WebUI.

Table 3-1 Basic operations

Operation	Procedure
Select a language.	On the login page, select the language to be used from the drop-down list.

Operation	Procedure
View server basic information.	Choose **Information** > **Overview**. The **Basic Info** area lists server information, including: ● Server model and serial number ● IP address and firmware version of the iBMC ● BIOS firmware version and globally unique identifier (GUID) ● Maximum web session allowed and the number of online users ● Alarm and indicator status
Obtain online help information.	On the **System** page, click ⑦.
Query user information.	After you log in to iBMC, click the user name (for example, **test**) next to 👤 in the upper right corner. The **Current User Info** window is displayed, showing the user information.
View alarm information.	Click an alarm icon in the upper right corner of the iBMC WebUI. The **Current Alarms** page is displayed, showing the severity, description, error code of the alarm, the time when the alarm was generated, and suggestions on how to clear the alarm.
Log out of the iBMC WebUI.	Click **Logout** in the upper right corner.
Refresh the current page.	Click 🔄 in the upper right corner of the iBMC WebUI.

3.3 Information

3.3.1 Overview

Function Description

The **Overview** page provides basic information about the server, virtual buttons, and common operation shortcuts.

GUI

Choose **Information** from the main menu, and select **Overview** from the navigation tree.

The **Overview** page is displayed.

The **Overview** page consists of four areas, as shown in **Figure 3-4**, **Figure 3-5**, and **Figure 3-5**.

Table 3-2 describes the information displayed in each area.

📖 **NOTE**

> The content of the **Overview** page varies depending on the work mode of the RH8100 V3 or 8100 V5 server. The **Overview** page for the RH8100 V3 or 8100 V5 server in dual-system mode provides the **VGA/USB/DVD** parameter and **Node Redirect** shortcut.

Figure 3-3 Overview page of the 8100 V5 in single-system mode
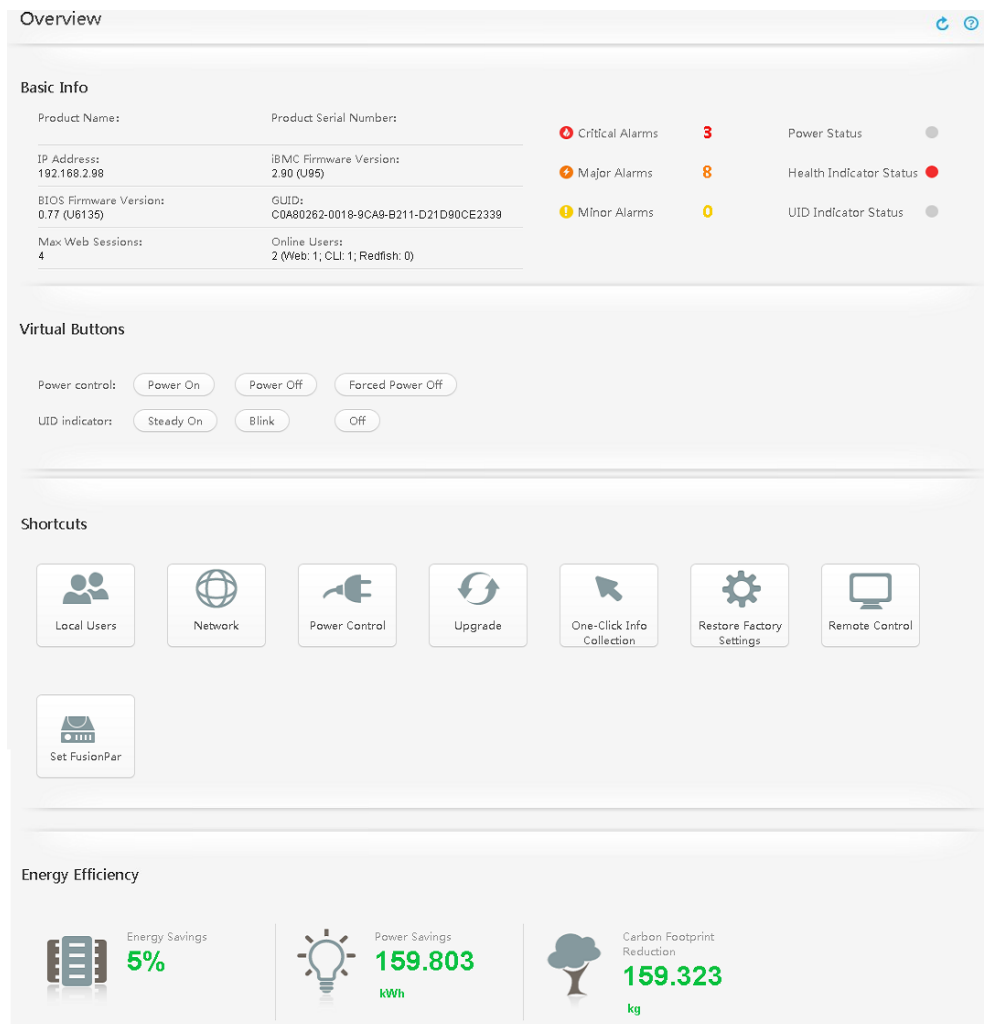
Figure 3-4 Overview page of the 8100 V5 in dual-system mode

Figure 3-5 Overview page of other servers (view product models on actual pages)
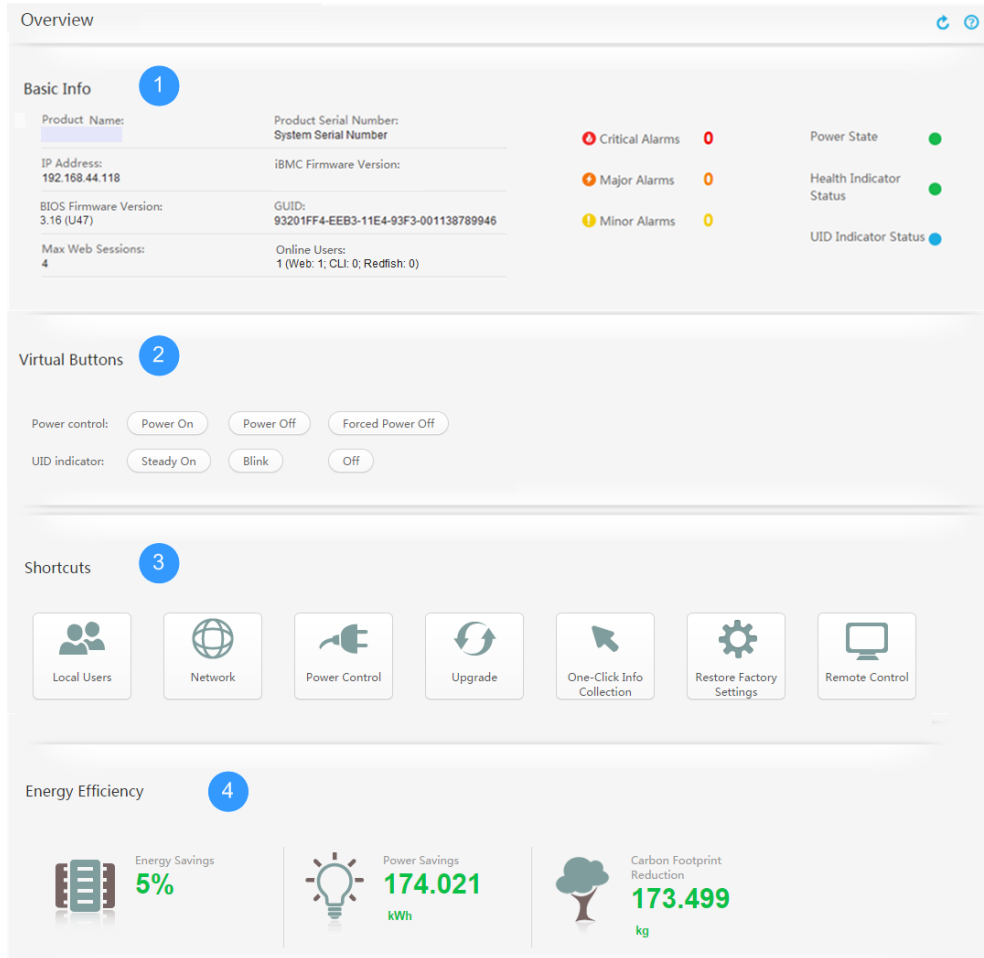
Parameter Description

Table 3-2 Description of the **Overview** page

N o.	Area	Displayed Information
1	Basic Info	Provides brief information about the server, including: ● **Product Name**: indicates the server model. ● **Product Serial Number**: indicates the server serial number. ● **IP Address**: indicates the IP address for logging in to the iBMC. ● **iBMC Firmware Version**: indicates the iBMC firmware version. ● **BIOS Firmware Version**: indicates the basic input/output system (BIOS) firmware version. ● **GUID**: indicates the globally unique identifier (GUID) of the server. ● **Max Web Sessions**: indicates the maximum number of users allowed to access the iBMC WebUI at the same time. ● **Online Users**: indicates the number of online users. For example, **4 (Web: 1; CLI: 2; Redfish: 1)** indicates that there are four online users: one that has logged in through the web interface, two through the command line interface, and one through Redfish. ● **Power Status**: Green indicates that the server OS is started. Gray indicates that the server OS is shut down. ● **Health Indicator Status**: shows the server health status. The indicator status is the same as that on the server. ● **UID Indicator Status**: pinpoints the location of the server in a chassis. The indicator status is the same as that on the server. ● **Critical Alarms**: indicates the total number of critical alarms. A critical alarm may power off the server, and even interrupt system services. You must take corrective actions immediately. ● **Major Alarms**: indicates the total number of major alarms. A major alarm has a major impact on the system. It affects the normal operating of the system or may cause service interruption. ● **Minor Alarms**: indicates the total number of minor alarms. A minor alarm has a minor impact on the system, but you need to take corrective actions as soon as possible to prevent a more severe alarm.

N o.	Area	Displayed Information

2	Virtual Buttons	Provides virtual buttons that are commonly used.
		● **Power control**
		  – **Power On**: Power on the server.
		  – **Power Off**: Power off the server.
		  – **Forced Power Off**: Forcibly power off the server.
		● **UID indicator**
		  – **Steady On**: Activate the UID indicator to pinpoint the location of the server in a chassis.
		  – **Blink**: Distinguishes the server from multiple servers that have also been located.
		  – **Off**: Deactivate the UID indicator.
		● **VGA/USB/DVD** (available only for the RH8100 V3 and 8100 V5): displayed only when the RH8100 V3 is in dual-system mode. If it is set to ⬤ON, the VGA port, USB port, and DVD-ROM drive on the server are connected to the current node and disconnected from the other node.

N o.	Area	Displayed Information
3	Shortcuts	Provides shortcuts for the following operations: ● **Local Users** ● **Network** ● **Power Control** ● **Upgrade** ● **One-Click Info Collection** For details about the data collected, see **3.11 One-Click Information Collection**. ● **Restore Factory Settings** The settings restored include but not limited to the following: – Serial port connection status – Power capping settings – LDAP and SSL certificates uploaded (the certificates will be deleted) – User names, passwords, validity periods, user group settings, and user lockout settings – IP address assignment mode, IP addresses, subnet masks, and default gateways – SNMP settings – SNMP trap and SNMP settings for alarm reporting The LDAP and SSL certificates uploaded by users will be deleted after the factory settings are restored. ● **Remote Control** ● **Set FusionPar** (available only for RH8100 V3 and 8100 V5) ● **Node Redirect** (available only for RH8100 V3 and 8100 V5 in dual-system mode)
4	Energy Efficiency	Displays energy saving information of the server. ● **Energy Savings**: displays the energy saving rate of the server. ● **Power Savings**: indicates the power saved by the server. ● **Carbon Footprint Reduction**: indicates the carbon emission reduced by the server. NOTE ● **Energy Savings** is a comprehensive indicator. It is **5%** by default. ● **Power Savings** = Actual power consumption x (1/(1 - **Energy Savings**) -1) ● The saving of 1 kWh power equals reduction of 0.997 kg carbon dioxide emissions. To refresh energy saving statistics, choose **Power** > **Power Capping** and click **Reset Statistics**.

3.3.2 System Info

Function Description

On the **System Info** page, you can view the server system information and configure and manage the RAID controller card.

GUI

Choose **Information**, and select **System Info** from the navigation tree.

The **System Info** page is displayed.

Figure 3-6 System Info page
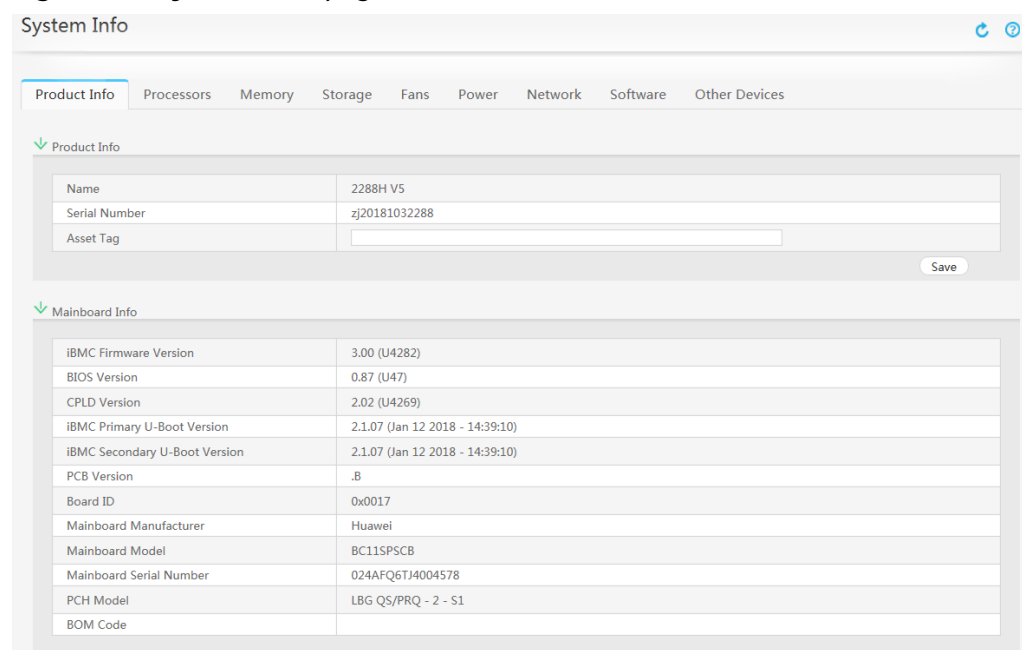
Parameter Description

Table 3-3 Product Info tab

Parameter	Description
Product Info	
Name	Server model.
Serial Number	Serial number of the server.

Parameter	Description
Asset Tag	Asset tag of the server. Value: a string of up to 48 bytes, allowing digits, letters, and special characters. **NOTE** Common users cannot set this parameter. Only the administrator, operator, and custom user with the **Basic Mgmt** rights can set the asset tag of a server.
Mainboard Info	
iBMC Firmware Version	iBMC firmware version.
BIOS Version	Basic input/output system (BIOS) version.
CPLD Version	Complex programmable logical device (CPLD) version.
iBMC Primary U-Boot Version	Version of the primary image of the Universal Boot Loader (U-Boot).
iBMC Secondary U-Boot Version	Version of the secondary image of the U-Boot.
PCB Version	Printed circuit board (PCB) version.
Board ID	Board ID.
Mainboard Manufacturer	Manufacturer of the mainboard.
Mainboard Model	Mainboard model.
Mainboard Serial Number	Mainboard serial number.
PCH model	Model of the PCH. **NOTE** This parameter is available only for V5 servers.
BOM Code	BOM code of the component.

Table 3-4 Processors tab

Parameter	Description
Processors	Provides the following information about each processor installed in the server: ● Name, manufacturer, model, CPU ID, clock speed, and BOM code of each processor ● Number of cores and threads ● L1, L2, and L3 cache capacity ● Processor status ● Other parameters

Table 3-5 Memory tab

Parameter	Description
Memory	Provides DIMM information, which includes the following: ● Maximum and actual number of DIMMs

Table 3-6 Storage tab

Parameter	Description
Views	Displays the storage devices of the server in a tree structure. **NOTE** If iBMA 2.0 has not been installed on the server, obtain the latest iBMA documentation and software package and install iBMA 2.0.

Parameter	Description
	RAID controller information: ● RAID controller name, type, driver name and version, firmware version, support for out-of-band management, health status, mode, NVDATA version, memory size, device interface, SAS address, supported strip size range, cache pinned status, maintain PD fail history, copyback status, copyback on SMART error status, and JBOD status. ● BBU name, status, and health status. NOTE ● If the RAID controller card does not support out-of-band management and the iBMA 2.0 is not installed, only the RAID controller name, type, firmware version, and support for out-of-band management are displayed. ● You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management. ● Do not set the working mode of the RAID controller card to JBOD on the Configuration Utility screen of the RAID controller card. Otherwise, the iBMC cannot identify the RAID controller card. For details, see the RAID controller card user guide of the server you use.
	Logical drive information: Name, status, RAID level and capacity, strip size, SSCD caching status, default read policy, current read policy, default write policy, current write policy, default IO policy, current IP policy, disk cache status, access policy, initialization type, BGI status, L2 cache status, consistency check status, OS drive letter, and whether it is the boot disk. NOTE ● If the RAID controller card does not support out-of-band management and the iBMA 2.0 is not installed, logical drives managed by the RAID controller card cannot be displayed. ● You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

Parameter	Description
	Disk information: Manufacturer, capacity, model, serial number, firmware version and status, media type, interface type, maximum speed, link speed, SAS address (0), SAS address (1), power status, temperature, hot spare status, rebuild status, patrol status, health status, remnant media wearout, location status, and power-on hours. **NOTE** - If the RAID controller card does not support out-of-band management and the iBMA 2.0 is not installed, only the interface types of the physical drives under the RAID controller card are displayed. - For pass-through drives, only the health status, location status, and interface type are displayed and the interface type is **SAS/SATA**. - You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management. - The power-on hours of only the SATA disks and Seagate SAS disks can be queried. - The Windows or VMware OS does not support speed negotiation of NVMe disks. Therefore, if the server uses a Windows or VMware OS, **Link Speed** is **NA** for NVMe disks.
Configure	Allows you to configure the RAID controller.
	RAID controller setup: - Copyback State - Copyback on SMART Error State - JBOD State To restore the default settings, click **Restore settings**.
	Logical drive setup: - Create a logical drive - Delete a logical drive - Modify a logical drive **NOTE** If the RAID controller card is in JBOD mode, logical drive information cannot be queried or configured.
	Physical drive setup: - Hot spare status - Firmware status - Location status

 NOTE

- The data on the **Storage** tab page is unavailable when the OS is shut down or is being started. After the OS starts, the iBMC identifies all disks again.
- If a disk is being rebuilt during the drive identification process, the disk data is available only after the disk is identified. If a disk fails to be identified, a "Drive Fault" alarm will be generated.

Table 3-7 Fans tab

Parameter	Description
Fans	Provides fan information: - Maximum and actual number of fans - Name, model, BOM code, speed, and speed ratio of each fan **NOTE** If an incompatible fan module is installed or a fan module is faulty, **FAULT** is displayed in **Model**. Fan information is not displayed on the standby system of the 8100 V3 or 8100 V5 server in dual-system mode.

Table 3-8 Power tab

Parameter	Description
Power	Provides power supply information: - Maximum and actual number of power supply units (PSUs) - Slot ID, manufacturer, type, SN, firmware version, rated power, input mode, and BOM code of each power supply **NOTE** Power supply information is not displayed on the standby system of the 8100 V3 or 8100 V5 server in dual-system mode.

Table 3-9 Network tab

Parameter	Description
NOTE - Complete network information can be displayed on the **Network** page only after iBMA 2.0 has started. - If iBMA 2.0 has not been installed on the server, obtain the latest iBMA documentation and software package and install iBMA 2.0.	

Parameter	Description
NIC	Displays information about LOMs and PCIe NICs. Information about a NIC includes the NIC name, manufacturer, model, chip model, chip vendor, PCB version, board ID, connected resource, firmware version, and driver name and version. **NOTE** ● Click ⟶ of a NIC to view network port details. The network port list displays the port name, port number, MAC address, type, media type, IPv4 address, IPv6 address, and VLAN status of each network port. ● If the firmware version of a NIC does not support a network port, the network attribute of the port is empty. For example, a NIC has two network ports: port 1 and port 2. If the firmware of the NIC does not support port 2, the network attribute of port 2 is empty.
FC Adapter	Displays FC adapter information, which includes the adapter name, manufacturer, model, chip model, firmware version, and driver name and version. **NOTE** Click ⟶ of an FC adapter to view detailed information.
Bridge	Displays bridge port information, which includes the port name, status, IPv4 and IPv6 information (address/subnet mask/gateway), MAC address, and VLAN information (VLAN ID and whether VLAN and VLAN priority are enabled). **NOTE** Click ⟶ of a bridge port to view detailed information.
Team	Displays aggregated network port information, which includes the port name, status, working mode, IPv4 and IPv6 information (address/subnet mask/gateway), MAC address, and VLAN information (VLAN ID and whether VLAN and VLAN priority are enabled). **NOTE** Click ⟶ of an aggregated network port to view detailed information.
Optical Modules	Displays optical module information, which includes the manufacturer, component name, serial number, production date, transceiver type, module type, transmission mode, wavelength, speed, and network port. **NOTE** Click ⟶ of an optical module to view detailed information.

Table 3-10 Software tab

Parameter	Description
NOTE ● Complete system software information can be displayed on the **Software** page only after iBMA 2.0 has started. ● If iBMA 2.0 has not been installed on the server, obtain the latest iBMA documentation and software package and install iBMA 2.0.	
Computer Name	Computer name defined by the server OS.
Computer Description	Supplementary information about the server.
OS Version	OS version.
OS Kernel Version	Kernel version if the Linux OS is used.
Domain/Workgroup	Domain name or workgroup on the OS of the server.
iBMA Service	iBMA version.
iBMA Running Status	iBMA running status.
iBMA Driver	iBMA driver version.

Table 3-11 Other Devices tab

Parameter	Description
PCIe Card	Provides PCIe card information: ● Maximum number of PCIe cards and number of present PCIe cards ● Description, manufacturer, slot number, vendor ID, device ID and connected resource of each PCIe card **NOTE** Click ➔ of a PCIe card to view its subcard information.
PCIe Adapter	Provides PCIe adapter information, including the name, description, slot, PCB version, and board ID.
HDD Backplane	Provides hard disk backplane information: ● Maximum and actual number of hard disk backplanes ● Name, manufacturer, type, PCB version, CPLD version, and Board ID of each hard disk backplane

Parameter	Description

Riser Card	Provides riser card information:
	● Maximum and actual number of riser cards
	● Name, manufacturer, slot, type, and board ID of each Riser card
	NOTE
	Riser card information of the RH8100 V3 is not displayed independently. The quantity of riser cards can be determined from the maximum number of supported PCIe cards.
	  ● If the number is 10, no riser card is configured.
	  ● If the number is 13, one riser card is configured.
	  ● If the number is 16, two riser cards are configured.

SD Card	Provides microSD card information: ● Maximum and actual number of microSD cards ● Manufacturer, SN, and volume of each microSD card **NOTE** V5 servers do not support SD cards. For the RH8100 V3 in single-system mode, only the microSD cards of the primary iBMC are displayed. For the RH8100 V3 in dual-system mode, all microSD cards are displayed.
Security Module	Provides security module information: ● Maximum and actual number of security modules ● Specification type, specification version, manufacturer, manufacturing version, and self-test status of each security module
RAID Card	Provides RAID controller card information: ● Maximum and actual number of RAID controller cards ● Name, location, manufacturer, number, type, supported RAID levels, PCB version, CPLD version, board ID and connected resource of each RAID controller card
SD Card Controller	Provides microSD card controller information: ● Maximum and actual number of microSD card controllers ● Manufacturer and version of each microSD card controller **NOTE** V5 servers do not support SD controllers.
LCD	Provides LCD firmware version. **NOTE** The RH5885 V3 does not support LCDs. No LCD information is displayed. The RH5885H V3 supports LCDs. LCD information is displayed.

Parameter	Description
CPU Board	Provides CPU board information: ● Maximum and actual number of present CPU boards ● Name, manufacturer, slot number, type, PCB version, CPLD version, board ID, and power of each CPU board **NOTE** Only the 8100 V5 server supports display of the CPU board power.
Memory Board	Provides memory board information: ● Maximum and actual number of memory boards ● Name, manufacturer, slot number, type, PCB version, and board ID of each memory board **NOTE** The RH5885 V3 does not support memory boards. No memory board information is displayed. The RH5885H V3 supports memory boards. Memory board information is displayed.
I/O Board	Provides I/O board information: ● Maximum and actual number of I/O boards ● Name, manufacturer, type, PCB version, CPLD version, board ID, and power of each I/O board **NOTE** Only the 8100 V5 server supports display of the I/O board power.
M.2 Adapter	Provides M.2 adapter information, including name, description, PCB version, and board ID. **NOTE** Only the RH2288 V3, RH2288H V3, 1288H V5 and 2288H V5 support M.2 adapters.

Querying System Information

1. On the menu bar, choose **Information**.

2. In the navigation tree, choose **System Info**.

   The **System Info** page is displayed.

3. View information about the server and its components.

Querying RAID Controller Card Properties

📖 NOTE

Before performing this operation, ensure that the following conditions are met:

● The RAID controller card supports iBMC out-of-band management or iBMA 2.0 is running on the OS. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

● The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.

2. On the **Views** tab page, select the RAID controller card to be queried.

The RAID controller card properties are displayed in the right pane, as shown in **Figure 3-7**.

Figure 3-7 Querying RAID controller card properties
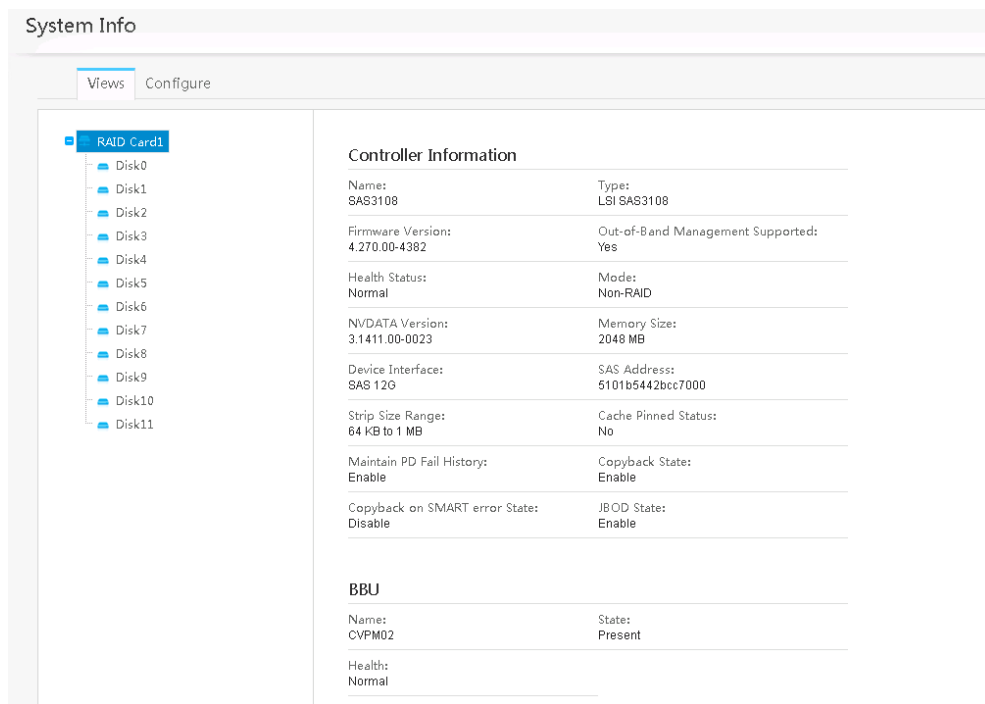
Querying RAID Array Properties

☐ NOTE

Before performing this operation, ensure that the following conditions are met:

- The RAID controller card supports iBMC out-of-band management or iBMA 2.0 is running on the OS. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
- The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.
2. On the **Views** tab page, select the RAID array to be queried.

The RAID array properties are displayed in the right pane, as shown in **Figure 3-8**.

Figure 3-8 Querying RAID array properties
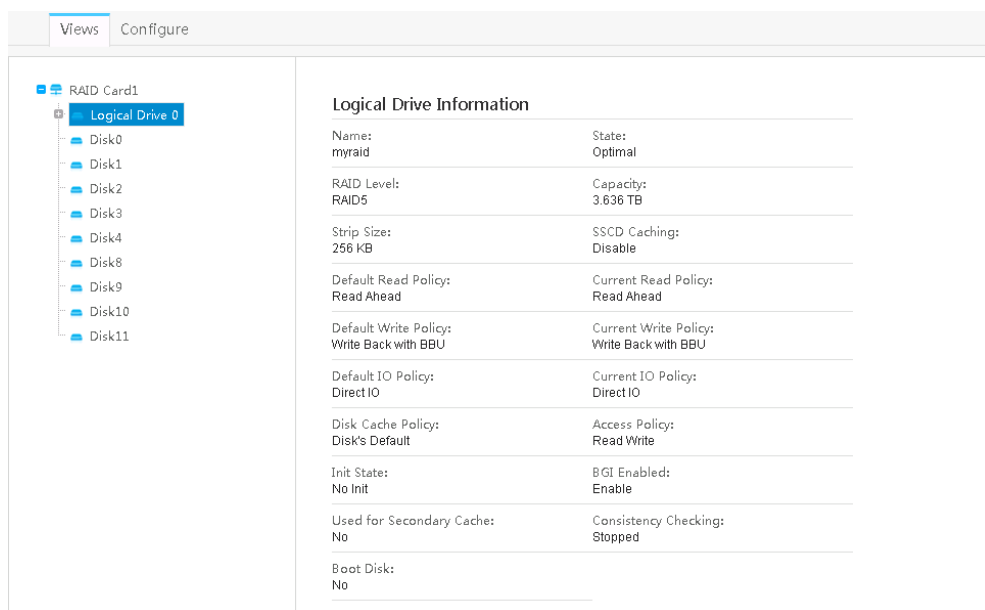
Querying Hard Disk Properties

📖 **NOTE**

Before performing this operation, ensure that the following conditions are met:

- The hard drives are managed by a RAID controller card that supports creation of logical drives.

- The RAID controller card supports iBMC out-of-band management or iBMA 2.0 is running on the OS. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

- The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.

2. On the **Views** tab page, select the hard disk (a member disk in a RAID array or an independent hard disk) to be queried.

   The hard disk properties are displayed in the right pane, as shown in **Figure 3-9** and **Figure 3-10**.

Figure 3-9 Querying properties of a member disk in a RAID array

Figure 3-10 Querying properties of an independent hard disk

Modifying RAID Controller Card Properties

📖 NOTE

> Before performing this operation, ensure that the following conditions are met:
> - The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
> - The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.

2. Click the **Configure** tab.

   The RAID controller configuration page is displayed.

3. Select the RAID controller card to be managed.

4. Click ⟶ next to **RAID Controller**.

   The RAID controller setting area is displayed. **Table 3-12** describes the parameters.

Figure 3-11 Modifying RAID controller card properties

Table 3-12 Parameter description

Parameter	Description
Copyback State	The copyback feature allows data to be copied from a source drive to a destination drive.
	If a member drive of a RAID array with redundancy becomes faulty, the hot spare drive automatically takes over the failed drive and starts data synchronization. After a new drive is installed to replace the faulty one, data is copied from the hot spare drive to the new drive. As the data copyback is complete, the hot spare drive restores its hot spare state.
Copyback on SMART error State	Copyback can be initiated when the first Self-Monitoring Analysis and Reporting Technology (SMART) error occurs on a drive.

Parameter	Description
JBOD State	Just a bunch of disks (JBOD) allows commands to be directly transferred from the RAID controller to the connected hard drives without the need of configuring logical drives. This feature allows the upper-layer service or management software to access and control physical drives.

5. Set the parameters and click **Save**.

Creating a Logical Drive

⚲ NOTE

Before performing this operation, ensure that the following conditions are met:

- The hard drives are managed by a RAID controller card that supports creation of logical drives.
- The physical drives to be added as logical drives are in **UNCONFIGURED GOOD** state.
- The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
- The number of logical drives on the RAID controller card does not reach the maximum.
- The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.
2. Click the **Configure** tab.

   The RAID controller configuration page is displayed.
3. Select the RAID controller card to be managed.
4. Click ➔ next to **Logical Drive**.

   The logical drive configuration page is displayed.
5. Click the option button before **Create**.

   The logical drive setting area shown in **Figure 3-12** is displayed. **Table 3-13** describes the parameters.

Figure 3-12 Creating a logical drive

Table 3-13 Parameter description

Parameter	Description
Name	Identifies a logical drive.
Secondary Cache	Specifies whether to enable CacheCade.
Strip Size	Specifies the size of a data strip on each physical drive.
Read Policy	Specifies the data read policy of the logical drive. Value: ● **Read Ahead**: The RAID controller pre-reads sequential data or the data predicted to be used and saves it in the cache. ● **No Read Ahead**: The Read Ahead feature is disabled.

Parameter	Description
Write Policy	Specifies the data write policy of the logical drive. Value: ● **Write Through**: After the drive receives all data, the controller sends the host a message indicating that data transmission is complete. ● **Write Back with BBU**: When no battery backup unit (BBU) is configured or the configured BBU is faulty, the RAID controller automatically switches to the Write Through mode. ● **Write Back**: After the controller cache receives all data, the controller sends the host a message indicating that data transmission is complete.
IO Policy	Specifies the input/output (I/O) policy for reading data from special logical drives. This policy does not affect the pre-reading cache. Value: ● **Cached IO**: All the read and write requests are processed by the cache of the RAID controller. Select this value only when CacheCade 1.1 is configured. ● **Direct IO**: This value has different meanings in read and write scenarios. – In read scenarios, data is directly read from physical drives. (If **Read Policy** is set to **Read Ahead**, data read requests are processed by the cache of the RAID controller.) – In write scenarios, data write requests are processed by the cache of the RAID controller. (If **Write Policy** is set to **Write Through**, data is directly written to physical drives.)

Parameter	Description
Disk Cache Status	The disk cache status can be any of the following: ● **Enable**: writes data to the cache before writing data to the hard drive. This option improves data write performance. However, data will be lost if there is no protection mechanism against power failures. ● **Disable**: writes data to a hard drive without caching the data. Data is not lost if power failures occur. ● **Disk's default**: uses the default cache policy.
Access Policy	Specifies the access policy for the logical drive. Value: ● **Read/Write**: Read and write operations are allowed. ● **Read Only**: The logical drive is read-only. ● **Blocked**: Access to the logical drive is denied.
Init State	Specifies whether to initialize the logical drive created. Value: ● **No Init**: Initialization is not performed. ● **Quick Init**: writes zeros to the first 100 MB of the logical drive. Then, the logical drive status changes to **Optimal**. ● **Full Init**: initializes the logical drive. Before the initialization is complete, the logical drive status is **initialization**.
Level	Specifies the RAID level of the logical drive.
Number of drives per span	Set this parameter when the RAID level is 10, 50, or 60.
Disk	Specifies the disks to be added to the logical drive.
Capacity	Specifies the capacity of the logical drive.

6. Set the parameters and click **Save**.

Removing Logical Drives

📖 NOTE

Before performing this operation, ensure that the following conditions are met:

- The hard drives are managed by a RAID controller card that supports creation of logical drives.
- The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
- The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.
2. Click the **Configure** tab.

   The RAID controller configuration page is displayed.
3. Select the RAID controller card to be managed.

4. Click → next to **Logical Drive**.

   The logical drive configuration page is displayed.
5. Click the option button before **Delete**.

   The logical drive setting area shown in **Figure 3-13** is displayed.

Figure 3-13 Removing logical drives
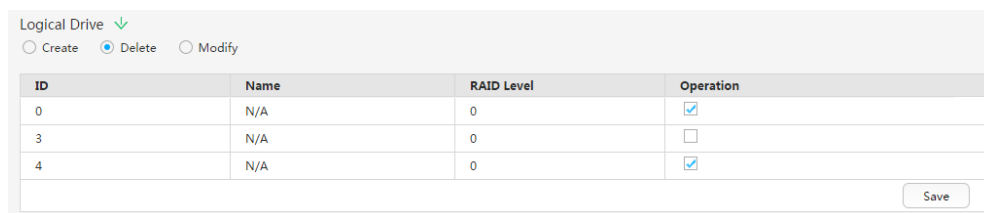
6. Select the logical drives to be deleted and click **Save**.

Modifying Logical Drive Properties

📖 NOTE

Before performing this operation, ensure that the following conditions are met:

- The hard drives are managed by a RAID controller card that supports creation of logical drives.
- The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
- The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.
2. Click the **Configure** tab.

   The RAID controller configuration page is displayed.
3. Select the RAID controller card to be managed.

4. Click → next to **Logical Drive**.

The logical drive configuration page is displayed.

5. Click the option button before **Modify**.

The logical drive setting area shown in **Figure 3-14** is displayed. **Table 3-14** describes the parameters.

Figure 3-14 Modifying logical drive properties

Table 3-14 Parameter description

Parameter	Description
Name	Identifies a logical drive.
Read Policy	Specifies the data read policy of the logical drive. Value: ● **Read Ahead**: The RAID controller pre-reads sequential data or the data predicted to be used and saves it in the cache. ● **No Read Ahead**: The Read Ahead feature is disabled.

Parameter	Description
Write Policy	Specifies the data write policy of the logical drive. Value: ● **Write Through**: After the drive receives all data, the controller sends the host a message indicating that data transmission is complete. ● **Write Back with BBU**: When no battery backup unit (BBU) is configured or the configured BBU is faulty, the RAID controller automatically switches to the Write Through mode. ● **Write Back**: After the controller cache receives all data, the controller sends the host a message indicating that data transmission is complete.

IO Policy	Specifies the input/output (I/O) policy for reading data from special logical drives. This policy does not affect the pre-reading cache.
	
	Value:
	
	● **Cached IO**: All the read and write requests are processed by the cache of the RAID controller. Select this value only when CacheCade 1.1 is configured.
	
	● **Direct IO**: This value has different meanings in read and write scenarios.
	
	  – In read scenarios, data is directly read from physical drives. (If **Read Policy** is set to **Read Ahead**, data read requests are processed by the cache of the RAID controller.)
	
	  – In write scenarios, data write requests are processed by the cache of the RAID controller. (If **Write Policy** is set to **Write Through**, data is directly written to physical drives.)

Parameter	Description
Disk Cache Status	The disk cache status can be any of the following: ● **Enable**: writes data to the cache before writing data to the hard drive. This option improves data write performance. However, data will be lost if there is no protection mechanism against power failures. ● **Disable**: writes data to a hard drive without caching the data. Data is not lost if power failures occur. ● **Disk's default**: uses the default cache policy.
Access Policy	Specifies the access policy for the logical drive. The options are as follows: Value: ● **Read/Write**: Read and write operations are allowed. ● **Read Only**: The logical drive is read-only. ● **Blocked**: Access to the logical drive is denied.
BGI Status	Specifies whether to enable background initialization.
SSCD Caching	Specifies whether to use CacheCade drive as the cache.
Boot Disk	Specifies whether the logical drive is the boot drive.

6. Select the logical drive to be modified.

7. Set the parameters and click **Save**.

Modifying Member Drive Properties

📖 **NOTE**

Before performing this operation, ensure that the following conditions are met:

● The hard drives are managed by a RAID controller card that supports creation of logical drives.

● The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

● The BIOS has started.

1. On the **System Info** page, click the **Storage** tab.

2. Click the **Configure** tab.

    The RAID controller configuration page is displayed.

3. Select the RAID controller card to be managed.

4. Click → next to **Physical Drive**.

The physical drive setting area shown in **Figure 3-15** is displayed. **Table 3-15** describes the parameters.

Figure 3-15 Modifying physical drive properties

Physical Drive ↓		
Disk0 ▼		
Property	**Value**	
Hot Spare State	None ▼	
Firmware State	ONLINE ▼	
Location State	Off ▼	
		Save
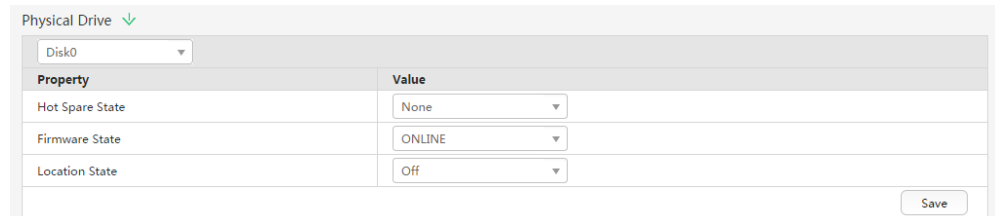
Table 3-15 Parameter description

Parameter	Description
Hot Spare State	Specifies the hot spare status of the physical drive. Value: ● **None**: The drive is not a hot spare disk. ● **Global**: indicates global hot spare disk. ● **Dedicated**: indicates a dedicated hot spare disk.
Firmware State	Specifies the status of the physical drive. Value: ● **UNCONFIGURED BAD**: The drive is unavailable. ● **ONLINE**: The drive is online. ● **OFFLINE**: The drive is offline. ● **UNCONFIGURED GOOD**: The drive is idle. ● **JBOD**: The drive is directly managed by the OS.
Location State	Specifies whether the locating indicator is lit for the drive.

5. Select the member disk to be modified.
6. Set the parameters and click **Save**.

3.3.3 Real-Time Monitoring

Function Description

The **Real-Time Monitoring** page provides the following information:

- Capacity and usage of all disk partitions
- CPU usage of the last one hour
- Memory usage of the last one hour
- Historical data about the air inlet temperature
- Bandwidth usage of all network ports

GUI

Choose **Information** from the main menu, and select **Real-Time Monitoring** from the navigation tree.

The **Real-Time Monitoring** page is displayed.
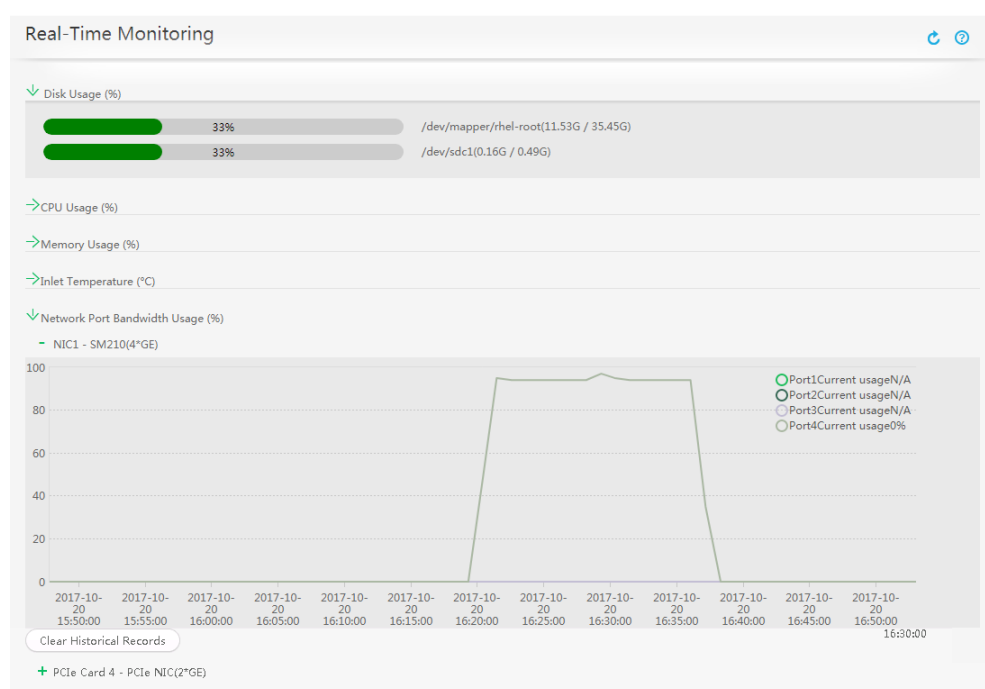
Parameter Description

Table 3-16 Disk usage

Parameter	Description
Disk Usage (%)	The **Disk Usage** area provides the following information: ● Percentage of the used partition space to the total partition space ● Disk partition information ● Total capacity and usage capacity of each partition **NOTE** If disk usage is not displayed, install and run iBMA 2.0.

Table 3-17 CPU usage

Parameter	Description
CPU Usage (%)	Percentage of CPU resources used by applications in running. **NOTE** ● If iBMA 2.0 has been installed and started on the OS, iBMA 2.0 provides the CPU usage data, which is consistent with that collected by the OS. ● If iBMA 2.0 is not installed or started, the Intel management Engine (ME) provides the CPU usage data, which is compute utilization per second of all cores calculated by CPU internal modules. ● If iBMA 2.0 has not been installed on the server, obtain the latest iBMA documentation and software package and install iBMA 2.0.

Table 3-18 Memory usage

Parameter	Description
Memory Usage (%)	Percentage of memory resources used by applications in running. **NOTE** ● If iBMA 2.0 has been installed and started on the OS, iBMA 2.0 provides the memory usage data, which is consistent with that collected by the OS. ● If iBMA 2.0 is not installed or started, the Intel ME provides the memory bandwidth usage, which is different from the memory usage collected by the OS. ● If iBMA 2.0 has not been installed on the server, obtain the latest iBMA documentation and software package and install iBMA 2.0.

Table 3-19 Inlet temperature

Parameter	Description
Inlet Temperature (°C)	Air inlet temperature data sampled every 10 minutes within the last one week.

Table 3-20 Network port bandwidth usage

Parameter	Description
Network Port Bandwidth Usage (%)	Percentage of the bandwidth used by all the ports of the server NICs to the total bandwidth. **NOTE** If network port bandwidth usage is not displayed, install and run iBMA 2.0.

Procedure

1. Choose **Information** from the main menu, and select **Real-Time Monitoring** from the navigation tree.

   The **Real-Time Monitoring** page is displayed.

2. Click ⟶ to view more information about the monitored object.

   To collapse real-time monitoring information, click ↓.

   📖 NOTE

   To clear statistic data, click the **Clear Historical Records** button in the **Inlet Temperature (°C)**, or **Network Port Bandwidth Usage (%)** area.

3.3.4 Sensor Info
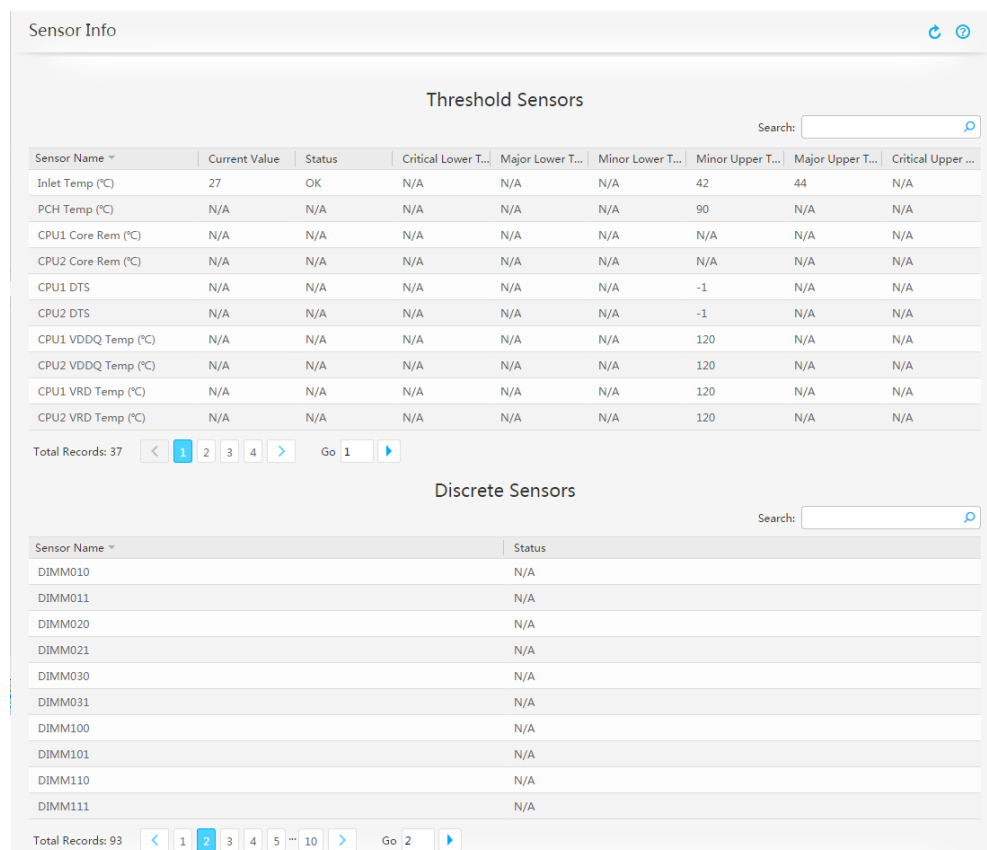
Function Description

The **Sensor Info** page provides information about threshold sensors and discrete sensors.

GUI

Choose **Information** from the main menu, and select **Sensor Info** from the navigation tree.

The **Sensor Info** page is displayed.

Sensor Info								↻ ⊘
Threshold Sensors								
							Search:	🔍
Sensor Name ▾	Current Value	Status	Critical Lower T...	Major Lower T...	Minor Lower T...	Minor Upper T...	Major Upper T...	Critical Upper ...
Inlet Temp (°C)	27	OK	N/A	N/A	N/A	42	44	N/A
PCH Temp (°C)	N/A	N/A	N/A	N/A	N/A	90	N/A	N/A
CPU1 Core Rem (°C)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CPU2 Core Rem (°C)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CPU1 DTS	N/A	N/A	N/A	N/A	N/A	-1	N/A	N/A
CPU2 DTS	N/A	N/A	N/A	N/A	N/A	-1	N/A	N/A
CPU1 VDDQ Temp (°C)	N/A	N/A	N/A	N/A	N/A	120	N/A	N/A
CPU2 VDDQ Temp (°C)	N/A	N/A	N/A	N/A	N/A	120	N/A	N/A
CPU1 VRD Temp (°C)	N/A	N/A	N/A	N/A	N/A	120	N/A	N/A
CPU2 VRD Temp (°C)	N/A	N/A	N/A	N/A	N/A	120	N/A	N/A

Total Records: 37　<　**1**　2　3　4　>　Go 1　▶

Discrete Sensors	
	Search: 🔍
Sensor Name ▾	Status
DIMM010	N/A
DIMM011	N/A
DIMM020	N/A
DIMM021	N/A
DIMM030	N/A
DIMM031	N/A
DIMM100	N/A
DIMM101	N/A
DIMM110	N/A
DIMM111	N/A

Total Records: 93　<　1　**2**　3　4　5　...　10　>　Go 2　▶

Parameter Description

Table 3-21 Parameters on the **Sensor Info** page

Parameter	Description
Sensor Name	Identifies a logical module or physical entity that monitors indicators of the server.
Current Value	Current value of an indicator. The value **N/A** indicates that the sensor does not obtain indicator information.
Status	Status of a threshold sensor. ● **OK**: The sensor is working properly. ● **N/A**: The sensor does not obtain indicator information. ● **NC**: The sensor detects a minor alarm. ● **CR**: The sensor detects a major alarm. ● **NR**: The sensor detects a critical alarm. Status of a discrete sensor. ● **N/A**: The sensor does not detect a value or status. The monitored device is not installed. ● **0x***XXXX*: A hexadecimal number defined based on Intelligent Platform Management Interface (IPMI) specifications to indicate the sensor status, for example, **0x8000**. For details, see the alarm manual of your server.
Critical Lower Threshold	Lower threshold set for a sensor to generate a critical alarm.
Major Lower Threshold	Lower threshold set for a sensor to generate a major alarm.
Minor Lower Threshold	Lower threshold set for a sensor to generate a minor alarm.
Minor Upper Threshold	Upper threshold set for a sensor to generate a minor alarm.
Major Upper Threshold	Upper threshold set for a sensor to generate a major alarm.
Critical Upper Threshold	Upper threshold set for a sensor to generate a critical alarm.

Procedure

1. Choose **Information** from the main menu, and select **Sensor Info** from the navigation tree.
   The **Sensor Info** page is displayed.

2.   View sensor information.

📖 NOTE

You can enter a keyword in the **Search** text box to search for sensor information.

3.4 Alarm & SEL

3.4.1 Current Alarms

Function Description

The **Current Alarms** page provides information about all the active alarms that have not been cleared.

GUI

Choose **Alarm & SEL** from the main menu, and select **Current Alarms** from the navigation tree.

The **Current Alarms** page is displayed.
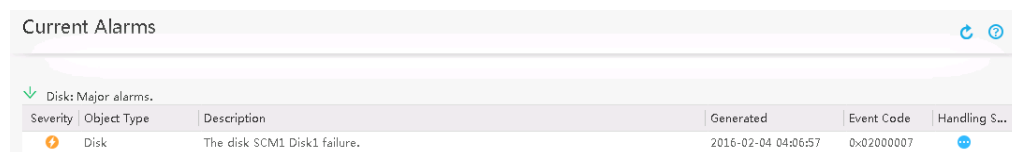
Parameter Description

Table 3-22 Parameters in the current alarms list

Parameter	Description
Severity	Severity of an alarm. Value: **Critical**, **Major**, or **Minor** ● 🔴: A critical alarm may power off the server, and even interrupt system services. You must take corrective actions immediately. ● 🟠: A major alarm has a major impact on the system. It affects the normal operating of the system or may cause service interruption. ● 🟡: A minor alarm has a minor impact on the system, but you need to take corrective actions as soon as possible to prevent a more severe alarm.
Object Type	Type of the component, for which the alarm was generated.
Description	Supplementary information about the alarm.

Parameter	Description
Generated	Date and time when the alarm was generated.
Event Code	Uniquely identifies an alarm.
Handling Suggestion	Suggestions on how to clear the alarm. Click ⬤ to view the suggestions.

Procedure

1. Choose **Alarm & SEL** from the main menu, and select **Current Alarms** from the navigation tree.

   The **Current Alarms** page is displayed.

2. View alarm information.

   You can click → next to an event type to view alarm details, and click ↓ to collapse it.

3.4.2 System Events
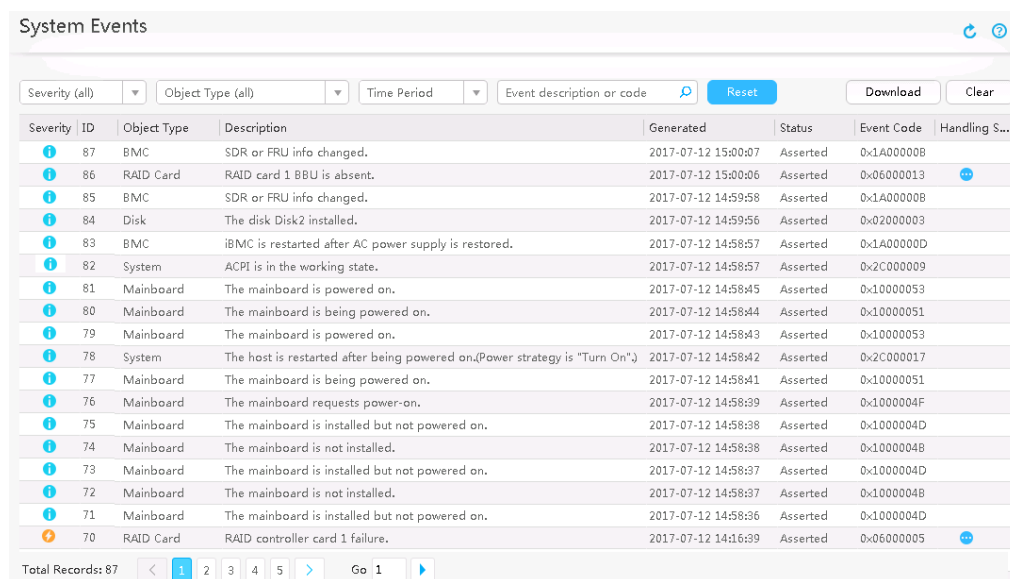
Function Description

The **System Events** page allows you to view, download, and delete system events.

GUI

Choose **Alarm & SEL** from the main menu, and select **System Events** from the navigation tree.

The **System Events** page is displayed.

Parameter Description

Table 3-23 Parameters in the System Events list

Parameter	Description
Severity	Severity of the system event. Value: **All**, **Critical**, **Major**, **Minor**, or **Informational**
ID	Serial number of the system event.
Object Type	Type of the component, for which the system event was generated.
Description	Supplementary information about the system event.
Generated	Date and time when the system event was generated.
Status	Status of the system event. Value: ● **Asserted**: indicates that a system event is generated. ● **Deasserted**: indicates that a system event is cleared.
Event Code	Uniquely identifies the system event.
Handing Suggestion	Suggestions on how to clear the system event. Click ⬤ to view the suggestions.

Procedure

Searching for System Events

1. Choose **Alarm & SEL** from the main menu, and select **System Events** from the navigation tree.

   The **System Events** page is displayed.

2. Specify search criteria.

   For details about the parameters, see **Table 3-24**.

Table 3-24 Description for search criteria

Parameter	Description
Severity	Severity of the system event. Value: **All**, **Critical**, **Major**, **Minor**, or **Informational**
Object Type	Component for which the system event was generated. Value: the value range varies according to the server model.

Parameter	Description
Time Period	Time period within which the system events were generated. Value: ● **Today** ● **Recent 7 days** ● **Recent 30 days** ● **Custom** NOTE If you select **Custom**, you must specify the start date and end date.
Event description or code	Description or code of the system event, which can be either of the following: ● Any consecutive character strings in the event description. ● Complete event code, with or without **0x**. Enter the event description or event code, and click 🔍 or press **Enter**.

Deleting All System Events

NOTICE

Deleted system events cannot be restored. Exercise caution when deleting system events.

---

1. On the **System Events** page, click **Clear**.

   A message is displayed asking you whether to clear the logs.

2. Click **Yes**.

Downloading System Events

On the **System Events** page, click **Download**. The system event file is automatically downloaded to the default path of the local PC.

3.4.3 Alarm Settings

Function Description

The **Alarm Settings** page allows you to configure:

● Syslog notifications: enables logs to be sent to a third-party server via syslog messages.

● Trap notifications: enables alarms, events, and trap properties to be sent to a third-party server via trap messages.

> 🕮 **NOTE**
>
> Traps are messages that are sent from the iBMC to a third-party server without being explicitly requested. Traps are used to report events and critical, major, and minor alarms.

- Email notifications: enables an email to be sent to the specified mailboxes over a Simple Mail Transfer Protocol (SMTP) server when an alarm is generated.

GUI

Choose **Alarm & SEL** from the main menu, and select **Alarm Settings** from the navigation tree.

The **Alarm Settings** page is displayed.

Parameter Description

Table 3-25 Syslog Notification Settings area

Parameter	Description
Syslog Notifications	Function for sending notifications through syslog messages. Click OFF or ON, and click **Save**. ● To enable it, set this parameter to ON. ● To disable it, set this parameter to OFF.
Syslog Server Identity	Source of the syslog message. Values: ● Board Serial Number ● Product Asset Tag ● Host Name
Include Alarm Severities	Severities of alarms to be sent through syslog messages. Value: ● **Critical**: Only critical alarms are reported. ● **Major**: Major and critical alarms are reported. ● **Minor**: Minor, major, and critical alarms are reported. ● **Normal**: Events and minor, major, and critical alarms are reported.
Transmission Protocol	Protocol used to transmit syslog messages between the iBMC and the syslog server. Values: ● **TLS**: a connection-oriented protocol that ensures confidentiality and integrity of the transmitted data. ● **TCP**: a connection-oriented protocol that sends data only after a reliable connection is set up between the sender and the receiver. ● **UDP**: a connectionless protocol that sends data without establishing a connection between the sender and the receiver.
Authentication Mode	Mode for authenticating syslog certificates. Set this parameter only when **Transmission Protocol** is **TLS**. Value: ● **One-way**: authenticates only the syslog server certificate. ● **Two-way**: authenticates certificates of both the syslog server and client.
Server Root Certificate	Certificate used to verify the messages sent from the syslog server before a connection is established.

Parameter	Description
Root Certificate Info	Information about the server root certificate uploaded. The certificate information includes the following: • Authority that issued the root certificate. • User to which the root certificate was issued. • Validity period of the root certificate. • Serial number of the root certificate.
Local Certificate	Certificate used for authenticating the Syslog client (iBMC) before a connection is established with the syslog server. Before establishing a connection, the iBMC sends a packet carrying the local certificate information to the syslog server. The connection can be established only when the authentication is successful.
Certificate Password	Password used for decrypting the client certificate. This password is generated with the client certificate generated by the certificate server.
Local Certificate Info	Information about the client certificate to be uploaded. The certificate information includes the issuer, user, validity period, and serial number of the certificate.
Syslog Server and Message Format	
No.	Channel for sending syslog messages. A maximum of four channels can be set.
Current Status	Current status of the channel, which can be enabled or disabled. OFF indicates disabled, and ON indicates enabled.
Server Address	Address of the syslog server.
Syslog Port	Port number of the syslog server.
Log Type	Type of logs contained in the syslog message.
Operation	Click . The following parameters are displayed:
Current Status	Current status of the channel, which can be enabled or disabled. Click OFF or ON , and click **Save**. • To enable it, set this parameter to ON . • To disable it, set this parameter to OFF .

Parameter	Description
Server Address	Address of the syslog server. Values: IPv4 address, IPv6 address, or domain name **NOTE** Enter a domain name if **Transmission Protocol** is **TLS**. In addition, DNS information must have been correctly configured on **Configuration** > **Network**.
Syslog Port	Port number of the syslog server. Value range: 1 to 65535
Log Type	Type of logs reported through syslog messages. Values: **All**, **Operation**, **Security**, and **Event**
Test	Function to test whether the syslog channel is available. Click **Test** for a channel. If "Operation successful" is displayed, the channel is available.

Table 3-26 Parameters in the **Trap Notification Settings** area

Parameter	Description
Trap Function	Function for sending alarms through trap messages. ● To enable it, set this parameter to ON . ● To disable it, set this parameter to OFF .
Trap Version	SNMP version used for sending traps. Value: ● **SNMPv1**: the first official SNMP version defined in Request for Comments (RFC) 1157. ● **SNMPv2c**: a version added community-based management architecture to SNMPv2. ● **SNMPv3**: a version added security and remote configuration enhancements to SNMP. **NOTE** ● SNMPv3 trap is recommended. Exercise caution when using SNMPv1 and SNMPv2c, because they pose security risks. ● For details about how to set authentication and encryption algorithms for SNMPv3, see **3.7.7 System**. Default value: **SNMPv1**
SNMPv3 User	SNMPv3 user name. Set this parameter only when **Trap Version** is **SNMPv3**. The default user name is **root** for V3 servers and **Administrator** for V5 servers.

Parameter	Description
Trap Mode	Mode for reporting trap information. Value: ● **Precise Alarm (recommended)**: The SNMP node OID that is in one-to-one mapping with the event is used as the ID of a Trap event. Compared with **OID** and **Event Code**, this mode provides more accurate information. ● **OID**: the OID of an SNMP node is used as the ID of a Trap event. ● **Event Code**: The event code is used as the ID of a Trap event. Default value: The default value is **Event Code** for V3 servers and **Precise Alarm (recommended)** for V5 server.
Trap Server Identity	Source of the trap message. Value: ● Board Serial Number ● Product Asset Tag ● Host Name

Community Name	SNMP community string for trap authentication if SNMPv1 or SNMPv2c is used.
	The value range varies depending on whether password complexity check is enabled.
	● If password complexity check is disabled, the value is a string of 1 to 18 characters consisting of letters, digits, and special characters (excluding spaces).
	● If password complexity check is enabled, the community name must meet the following requirements:
	  – Contain 8 to 18 characters
	  – Contain at least two of the following: uppercase letters A to Z, lowercase letters a to z, digits 0 to 9
	  – Contain at least one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/?
	  – Have at least two new characters when compared with the previous community name.
	  – Cannot contain spaces.
	Default value: **TrapAdmin12#$**

Confirm Community Name	Enter the community name again for consistency.

Parameter	Description
Include Alarm Severities	Severities of alarms to be sent to a third-party server through trap messages. Value: ● **Critical**: Only critical alarms are reported. ● **Major**: Major and critical alarms are reported. ● **Minor**: Minor, major, and critical alarms are reported. ● **Normal**: Events and minor, major, and critical alarms are reported.
Trap Server and Message Format	
No.	Identifies a trap channel for sending alarms. A maximum of four channels can be specified.
Operation	Click 🖊. The following parameters are displayed:
Current State	Current status of the trap channel. Click OFF or ON, and click **Save**. ● To enable it, set this parameter to ON. ● To disable it, set this parameter to OFF.
Trap Server Address	Server address for receiving alarms sent through trap messages. The server address can be an IPv4 or IPv6 address or a domain name.
Trap Port	Port number for receiving alarms sent through trap messages. Value range: 1 to 65535 Default value: **162** **NOTE** To restore the trap port number to the default value **162**, click **Restore Defaults**.
Message Delimiter	Delimiter that separates the keywords in trap messages. For example, **;**.
Select Message Content	Content to be included in trap messages.
Display Keyword in Message	Specifies whether to display the specified keywords in trap messages. **NOTE** An example will be provided on the right of the check box depending on whether **Message Delimiter**, **Select Message Content**, or **Display Keyword in Message** are selected.

Parameter	Description
Test	Function for testing whether the trap channel is available. Click **Test** for a channel. If "Operation successful" is displayed, the channel is available.

Table 3-27 Parameters in the **Email Notification Settings** area

Parameter	Description
SMTP Function	Function for sending email notifications through the SMTP server. Click ⬭OFF or 🟢ON , and click **Save**. ● To enable it, set this parameter to 🟢ON . ● To disable it, set this parameter to ⬭OFF .
SMTP Server Address	IPv4 or IPv6 address or domain name of the SMTP server.
TLS Enabled	Function for enabling Transport Layer Security (TLS) for data transmission. If TLS is disabled, data is transmitted in plain text. **NOTE** ● By default, the SMTP server supports TLS. You are advised to enable the TLS function for security purposes. ● After enabling TLS on the iBMC WebUI, enable TLS and configure identity authentication on the SMTP server. The SMTP server can receive emails from the iBMC only after TLS is enabled.
Anonymous Login Allowed	Function for allowing anonymous login. If anonymous login is allowed, the SMTP server transfers alarm emails without authenticating user name and password. If anonymous login is not allowed, the SMTP server transfers alarm emails only after the correct user name and password are entered. The user name and password must have been set on the SMTP server. **NOTE** By default, the SMTP server does not allow anonymous login. For security purposes, do not use anonymous login.
Email Info	

Parameter	Description
Sender User Name/Sender Password	User name and password used when **Anonymous Login Allowed** is set to **No**. The user name and password must be the same as the user name and password set on the SMTP server. Value range: ● User name: a string of 1 to 64 characters, consisting of letters, digits, and special characters. It cannot be left blank. ● Password: a string of 1 to 50 characters **NOTE** If the SMTP function is disabled, **Sender User Name** and **Sender Password** can be empty.
Sender Address	Email address from which alarms are sent. Value: a string of up to 255 characters The value can contain letters, digits, and special characters.
Email Subject/ Email Subject Contains	Subject of the email. Value: a string of 0 to 255 characters, consisting of letters, digits, and special characters. Enter the subject in **Email Subject**, and select the keywords to be contained in the email subject. For example, if you select **Host Name** and **Board Serial Number**, the email subject will contain the host name and board serial number.
Include Alarm Severities	Severities of alarms to be sent through the SMTP server. Value: ● **Critical**: Only critical alarms are reported. ● **Major**: Major and critical alarms are reported. ● **Minor**: Minor, major, and critical alarms are reported. ● **Normal**: Events and minor, major, and critical alarms are reported.
Recipient Addresses	Email addresses for receiving emails. The addresses must have been set on the SMTP server. Value: a string of up to 255 characters in the *xx@xxx.xx* format. The value can contain letters, digits, and special characters.
Description	Supplementary information about email addresses for receiving emails. Value: a string of 0 to 255 characters, consisting of letters, digits, and special characters.
Test	Function to test whether an email can be successfully sent to the recipient.

Parameter	Description
Enable	Function for enabling or disabling an email address. Click ⬤OFF or ⬤ON , and click **Save**. ● To enable it, set this parameter to ⬤ON . ● To disable it, set this parameter to ⬤OFF .

Procedure

Setting Syslog Notification

1. Choose **Alarm & SEL** from the main menu, and select **Alarm Settings** from the navigation tree.

   The **Alarm Settings** page is displayed.

2. Set syslog notification parameters.

   For details about the parameters, see **Table 3-25**.

3. Click **Save**.

   If "Operation Successful" is displayed, the syslog notification is set successfully.

Setting Trap Notification

1. Set trap notification parameters.

   For details about the parameters, see **Table 3-26**.

2. Click **Save**.

   If "Operation Successful" is displayed, the trap notification is set successfully.

Setting Email Notification

1. Set email notification parameters.

   For details about the parameters, see **Table 3-27**.

2. Click **Save**.

   If "Operation Successful" is displayed, the email notification is set successfully.

3.5 Diagnostics

3.5.1 FDM PFAE

Function Description

Fault Diagnose Management (FDM) provides automatic fault diagnosis of the entire system. FDM includes fault data collection and analysis, fault diagnosis and locating, fault prewarning, and device health analysis. The iBMC uses proactive failure analysis engine (PFAE) to implement FDM.

During routine operation and maintenance, you can view information about the faulty components and related historical events on the page, and take troubleshooting measures.

Not all the iBMC versions support the FDM PFAE function. If supported, the FDM PFAE function can be used only after it is enabled on the BIOS.

📖 NOTE

- On the BIOS of the Purley platform, choose **Advanced** > **System Event Log** > **FDM** and set the FDM function.
- The 2288H V5 supports the FDM PFAE function from iBMC V260.
- The 1288H V5, 2288 V5, 2488 V5, and 5288 V5 support the FDM PFAE function from iBMC V316.

GUI

Choose **Diagnostics** from the main menu, and select **FDM** from the navigation tree.

The **FDM** page is displayed.

📖 NOTE

The information displayed on this page may vary with the iBMC version.
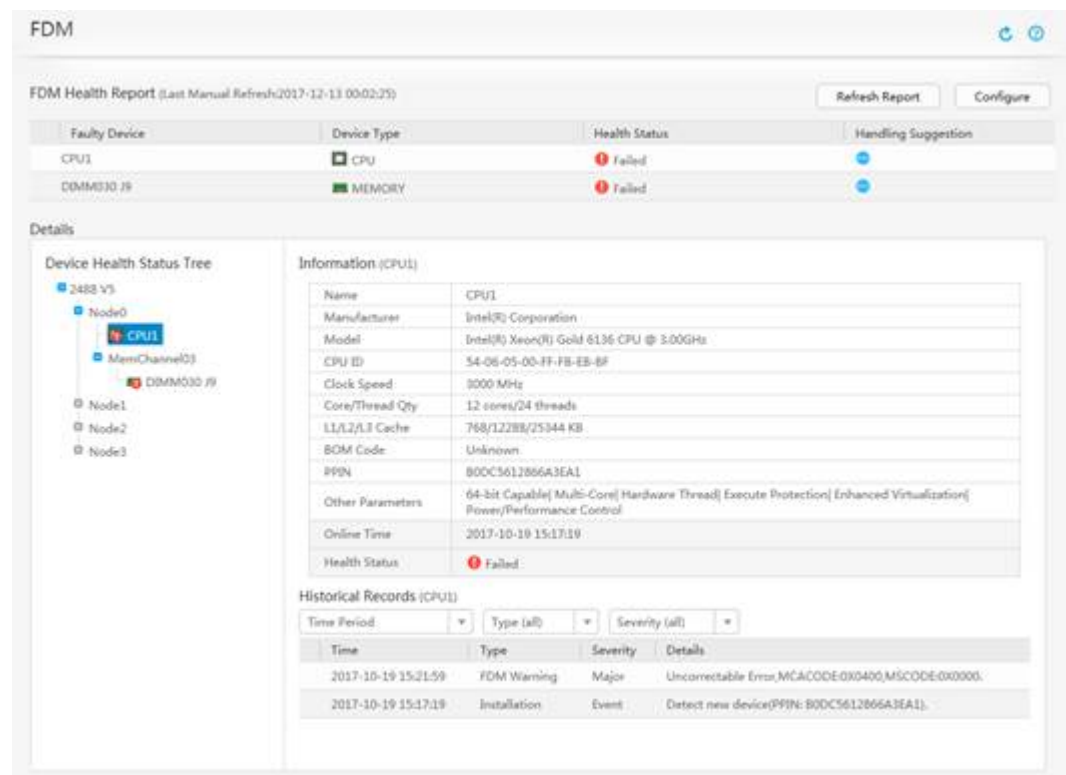
Parameter Description

Table 3-28 FDM page

Parameter	Description
FDM Health Report	
Faulty Device	Name or silkscreen of the faulty device.
Device Type	Type of the faulty device, for example, **CPU** or **DIMM**.
Health Status	Health statusDiagnosis result of the device. The result can be any of the following: ● 🟠 Degraded: The device performance deteriorates. ● 🔴 Failed: The device is faulty.
Handling Suggestion	Click 🔵 to view the handling suggestion.
Refresh Report	Click this button to refresh the FDM report.
Configure	Click this button to set FDM report parameters, including **Last Auto Refresh** and **Diagnostics Data Collection Period**.
Details	
Device Health Status Tree	Displays the health status of the server devices in a tree structure.
Device Information	Provides detailed information, including the basic information, online time, and health status, about the specified device. ● CPU information includes the name, manufacturer, model, CPU ID, clock speed, number of cores and threads, L1/L2/L3 cache, BOM code, PPIN, and other parameters. ● Memory information includes the name, manufacturer, location, capacity, clock speed, SN, type, minimum voltage, and other parameters. ● **Online Time**: time when the device was first installed in the server and identified by the iBMC. ● **Health Status**: Health statusDiagnosis result of the device. 　– 🟢 OKThe device is operating properly. 　– 🟠 Degraded: The device performance deteriorates. 　– 🔴 Failed: The device is faulty.
Historical Records	Historical events of the faulty device.
Time Period	Time when the event was generated.

Parameter	Description
Type	Type of the event. ● **FDM Warning**: indicates an FDM alarm. ● **PFA Warning**: indicates a Predictive Failure Analysis (PFA) event.
Severity	Severity level of the event. ● **Event**: indicates an event. ● **Minor**: indicates a minor alarm. ● **Major**: indicates a major alarm. ● **Critical**: indicates a critical alarm.

Setting FDM Report Parameters

Step 1 Click the **ConfigureSet** button.

The parameters to be set are displayed.

Step 2 Select the automatic refresh interval for the FDM report from the **Auto Refresh Interval** drop-down list.

Step 3 Select the data collection time for the FDM report from the **Diagnostics Data Collection Period**

drop-down list.

Step 4 Click **Save**.

If "Operation successful" is displayed, the parameters are set successfully.

----End

3.5.2 Playback

Function Description

The **Playback** page allows you to perform the following operations:

● Play a video file of the server stored on the local PC.

● Play a video that was automatically recorded on the server.

● Capture a picture during the playback of a video.

📖 **NOTE**

● The video file must be in *.rep format.

● The video recording function is enabled by default. Sensitive service information may be captured during video recording.

Table 3-29 describes the controls in the video playback control window.

Table 3-29 Controls in the video playback control window

Click...	To...
Play button	Play a selected video.
Pause button	Pause a selected video.
Fast Forward button	Fast forward a video at a 1x, 2x, or 4x speed.
Rewind button	Rewind a selected video file at a 1x, 0.5x, or 0.25x speed.
Full Screen button	Maximize the video playback control page. **NOTE** When a video is played in full-screen mode, right-click on the screen to open the shortcut menu.
Open button	Open a *.rep video file stored on the local PC.
Cut Screen button	Capture a picture during video playback.
Seek slider	Play a video file from a specified point. (The slider indicates the playback progress.)
Loop button	Loop a video file. This function is available only for local video files.

You can use the video recording and playback functions to maintain and troubleshoot the server. **Figure 3-16** shows the process for using the video recording and playback functions.

Figure 3-16 Process for using the video recording and playback functions

GUI
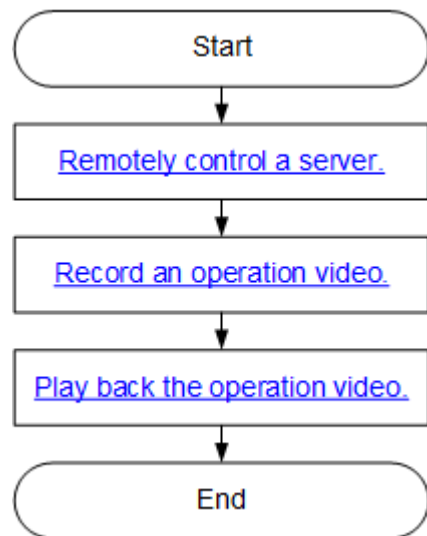
Choose **Diagnostics** from the main menu, and select **Playback** from the navigation tree.

The **Playback** page is displayed.
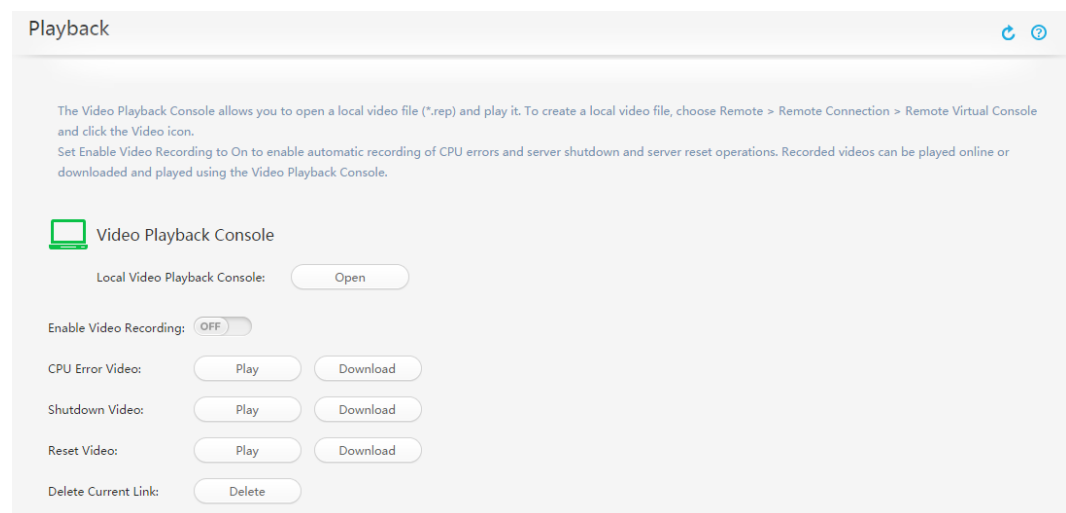
Procedure

Playing a Local Video

1. On the **Playback** page, click **Open** next to **Local Video Playback Console**.

   The **Video Player** window is displayed.

   📖 **NOTE**

   If a security alert dialog box is displayed before you open the **Video Player** window, click **Yes**.

2. In the **Video Player** window, click [icon].

The **Open** dialog box is displayed.

3. Select a video file stored on the local PC, and click **Open**.

The **Video Player** starts to play the video.

– To fast forward the video at a 1x, 2x, or 4x speed, click [icon].

– To rewind the video at a 1x, 0.5x, or 0.25x speed, click [icon].

– To control the playback progress of the video, drag [icon] to the left or right.

– To repeat playback of the video, click [icon].

– To display the **Video Player** window in full-screen mode, click [icon].

Disabling or Enabling the Video Recording Function

📖 NOTE

The video recording function is enabled by default. Sensitive service information may be recorded during video recording.

To enable the video recording function, perform the following steps:

1. Set **Video Recording** to [ON].

The following message is displayed:

Are you sure you want to continue?

2. Click **Yes**.

After the video recording function is enabled, the server automatically records a video when:

● The server is powered off or reset.

● "CPU CAT ERROR" is reported.

The videos are stored in **/tmp**.

📖 NOTE

To disable the video recording function, set **Video Recording** to [OFF].

Playing or Downloading a Video That Was Automatically Recorded on the Server

● To play a video, click the **Play** button.

● To download a video, click the **Download** button and save the video to the local PC.

If the video is being played by another person, click **Stop** next to **Stop Other User's Video Playback** to stop other user's video playback.

Capturing a Picture During Video Playback

1. Click [icon] when a video is played.

The **Save As** dialog box is displayed.

2. Select a local directory to save the picture, and click **Save**.

The picture is saved as a *.jpg file to the specified directory.

3.5.3 Screenshot

Function Description

The **Screenshot** page allows you to perform the following operations:

● Enable or disable the last screenshot function.

The last screenshot function allows automatic capture of the screenshot of the server screen just before the server is restarted or powered off.

● Capture a screenshot of the server desktop in real time.

◫ NOTE

The last screenshot function is enabled by default. Sensitive service information may be captured in the screenshot.

GUI

Choose **Diagnostics** from the main menu, and select **Screenshot** from the navigation tree.

The **Screenshot** page is displayed.
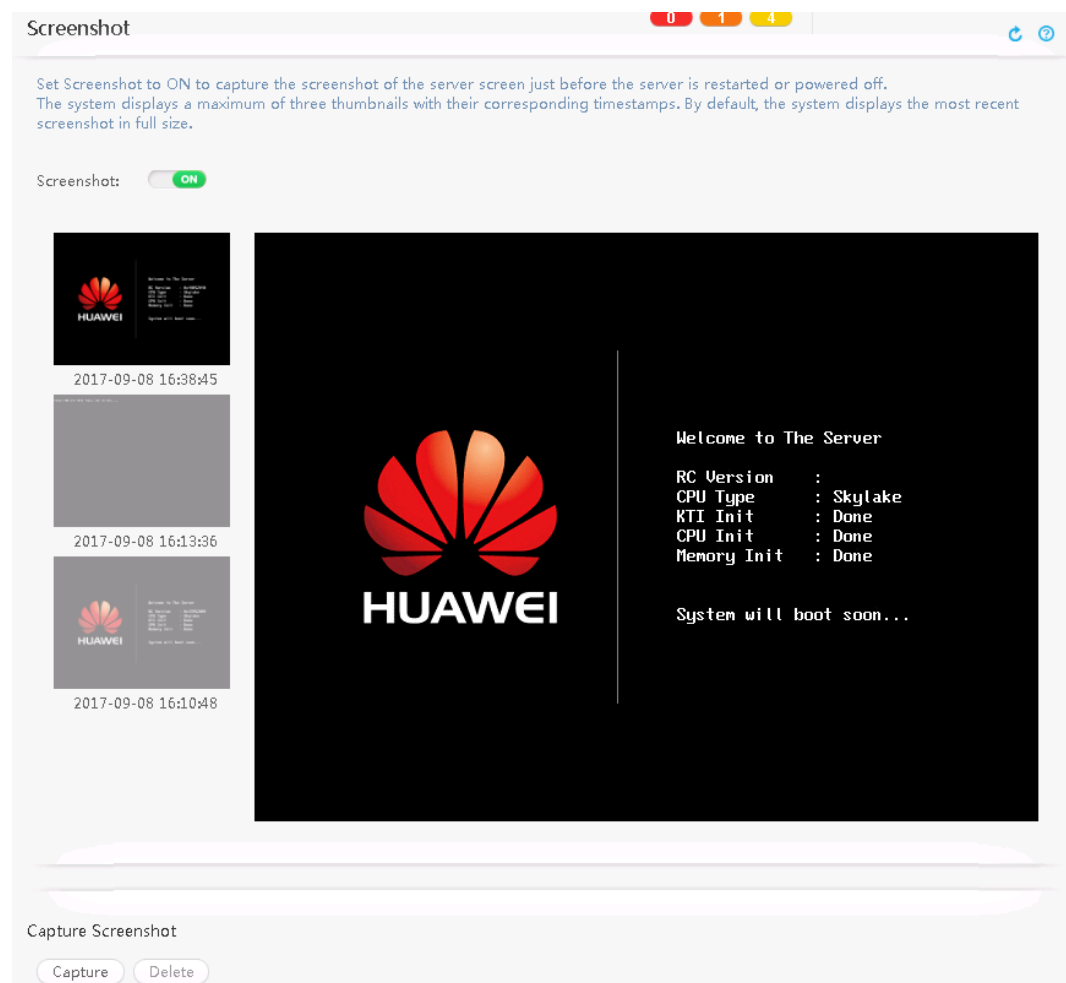
Procedure

Disabling or Enabling the Last Screenshot Function

1. To enable the last screenshot function, set **Screenshot** to . To disable the last screenshot function, set **Screenshot** to .
   The following information is displayed:
   Are you sure you want to perform this operation?

2. Click **Yes**.
   If "Operation Successful" is displayed, the setting is successful.

Viewing the Last Screenshot

1. On the menu bar, choose **Diagnostics**.

2. In the navigation tree, choose **Screenshot**.
   The **Screenshot** page is displayed.

3. View screenshots.
   – The system displays a maximum of three thumbnails with their corresponding timestamps. By default, the system displays the most recent screenshot in full size.
   – Click a thumbnail for a larger image.

Capturing a Screenshot

1. Click the **Capture** button under **Capture Screenshot**.
   A screenshot of the server desktop is displayed. The time when the screenshot was captured is on the upper left section of the screenshot.

If you have captured multiple screenshots, only the latest screenshot and capturing time are displayed.

Deleting a Screenshot

1. Click the **Delete** button under **Capture Screenshot**.
   A confirmation dialog box is displayed.

2. Click **Yes**.

3.5.4 Black Box

Function Description

The **Black Box** page allows you to enable or disable the black box function and download data from the black box memory.

A black box consists of memory and fault monitoring software.

● The memory is a built-in storage chip that records fault information, independent of hard disks on the server.
  The memory provides a maximum of 4 MB storage capacity, and saves kernel information when the OS crashes.

● The fault monitoring software records kernel information when the OS crashes.

Before using the black box function, ensure that the fault monitoring software (for example, iBMA) has been installed on the server. For details about how to install and use the iBMA, see the iBMA user guide.

- If the black box driver has not been installed on V5 servers after the black box function is enabled, unknown devices may be detected on the OS.

GUI

Choose **Diagnostics** from the main menu, and select **Black Box** from the navigation tree.

The **Black Box** page is displayed.
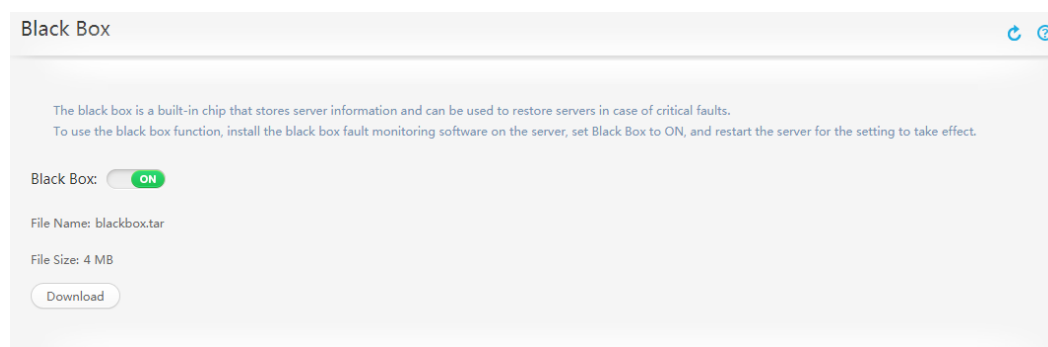
Parameter Description

Table 3-30 Parameters on the Black Box page

Parameter	Description
Black Box	Specifies whether to enable the black box function. This function is disabled for V3 servers and enabled for V5 servers by default. • **ON** : The black box is enabled. • **OFF** : The black box is disabled.
File Name	Server data file monitored by the black box.
File Size	Size of the server data file monitored by the black box.

Procedure

Enabling the Black Box Function

☐ NOTE

After enabling or disabling the black box function, restart the server for the setting to take effect.

1. On the menu bar, choose **Diagnostics**.

2. In the navigation tree, choose **Black Box**.

   The **Black Box** page is displayed.

3. Set **Black Box** to .

4. Restart the server.

Disabling the Black Box Function

1. Set **Black Box** to .

2. Restart the server.

Downloading Black Box Data

> **NOTE**
>
> Ensure that the black box function is enabled.

1. On Internet Explorer, choose **Tools** > **Internet Options**.

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

2. Click the **Security** tab, select **Internet** from the list box, click **Custom Level**, and click **Enable** for **Automatic prompting for file downloads** under **Download**.

3. On the iBMC WebUI, choose **Diagnostics** > **Black Box**.

4. Click **Download**.

   The **Save** dialog box is displayed.

5. Select a local directory for saving the file.

6. Click **Save**.

   The black box data file is saved to the specified directory on the local PC.

   > **NOTE**
   >
   > - The iBMC only downloads the black box data file from the server to the local PC, but does not parse this file. For details about how to parse a black box data file, see the server installation guide.
   > - The file saving information displayed varies with the browser used.

3.5.5 Serial Port Data

Function Description

The **Serial Port Data** page allows you to enable or disable the function for savingrecording data transmitted over the serial port, and download the latest 2 MB data.

The serial port data function is enabled by default.

GUI

Choose **Diagnostics** from the main menu, and select **Serial Port Data** from the navigation tree.

The **Serial Port Data** page is displayed.

Serial Port Data

The latest 2 MB data transferred over the serial port is available on the system.

Serial Port Data: `ON`

File Name: systemcom.tar

Decompressed File Size: 2 MB

Download
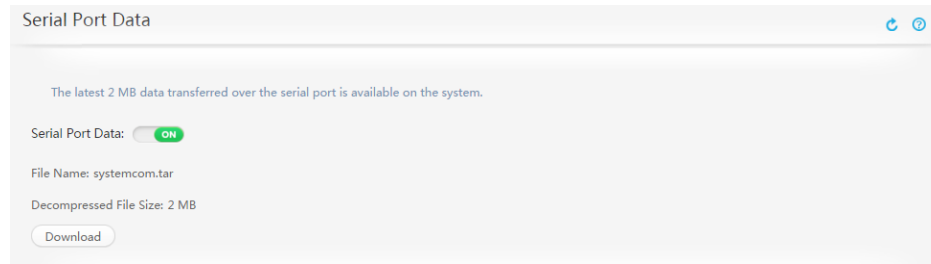
Procedure

1. On the menu bar of Internet Explorer, choose **Tools** > **Internet Options**.

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

2. Click the **Security** tab, select **Internet** from the list box, and click **Custom level**. In the displayed dialog box, click the **Enable** option button for **Automatic prompting for file downloads** under **Downloads**.

3. On the iBMC WebUI, choose **Diagnostics** from the main menu.

4. In the navigation tree, choose **Serial Port Data**.

   The **Serial Port Data** page is displayed.

5. Set **Serial Port Data** to `ON`.

6. Click **Download**.

   The **Save** dialog box is displayed.

7. Select a local directory for saving the downloaded file.

8. Click **Save**.

   The downloaded file is saved to the specified directory on the local PC.

3.5.6 Memory Hot-Swap (Exclusive to RH8100 V3)

Function Description

The **Memory Hot-Swap** page allows you to hot-swap dual in-line memory modules (DIMMs) and monitor the hot swapping process.

📖 NOTE

The **Memory Hot-Swap** page is unavailable for the RH8100 V3 server using Broadwell processors.

GUI

Choose **Diagnostics** from the main menu, and select **Memory Hot-swap** from the navigation tree.

The **Memory Riser Hot Swap** page is displayed.
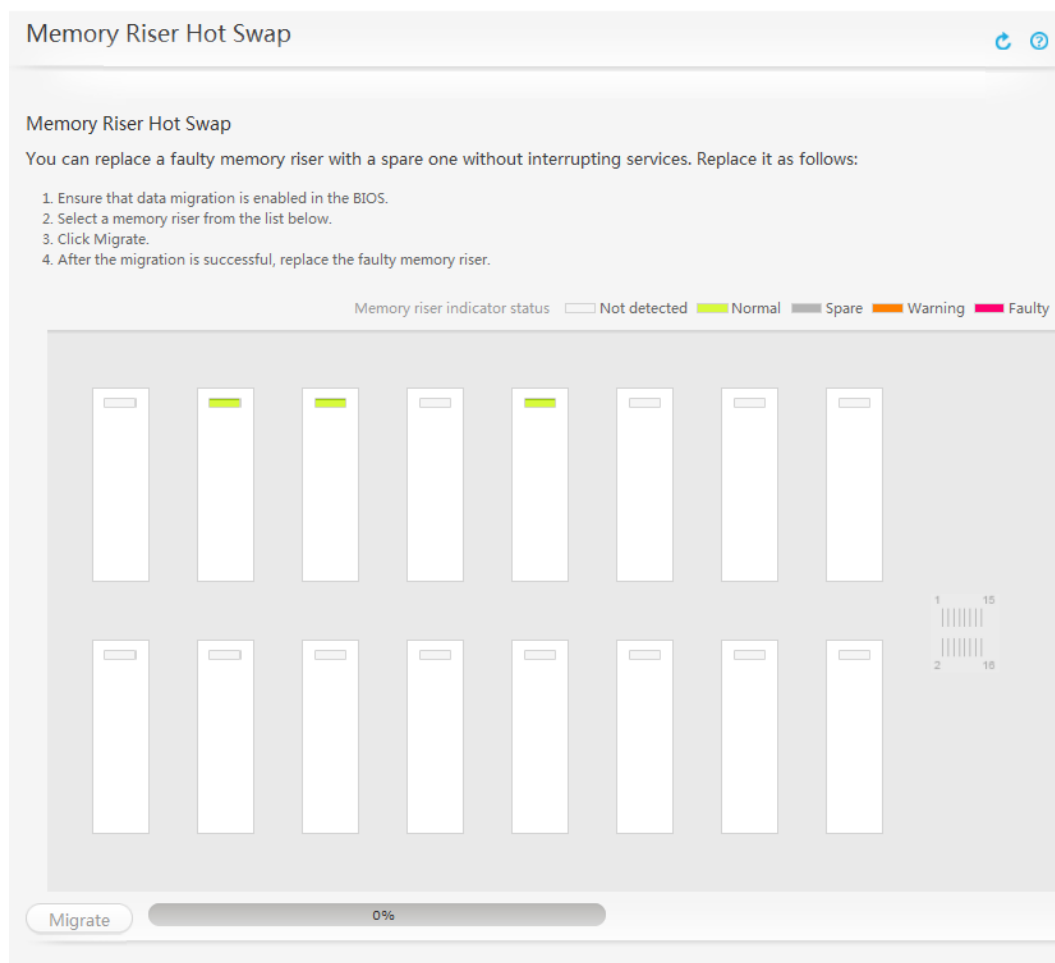
Procedure

1. On the menu bar, choose **Diagnostics**.
2. In the navigation tree, choose **Memory Hot-Swap**.

   The **Memory Riser Hot Swap** page is displayed.
3. Click a memory riser with the green or orange indicator.
4. Click **Migrate**.

   The system starts the migration process, and the progress bar displays the migration progress.

3.6 Power

3.6.1 Power Control

Function Description

The **Power Control** page allows you to perform the following operations:

- Power on, power off, or reset the server OS, or trigger the OS to generate a non-maskable interrupt (NMI).

- Set the power restore policy for the server OS.

An NMI is a special interrupt that cannot be masked by using a standard interrupt masking technology. An NMI is generated typically when a non-recoverable hardware error occurs. Some NMIs can be masked by using special methods.

NOTICE

Before you perform power control on a server, ensure that the operation does not affect services.

GUI

Choose **Power** from the main menu, and select **Power Control** from the navigation tree.

The **Power Control** page is displayed.
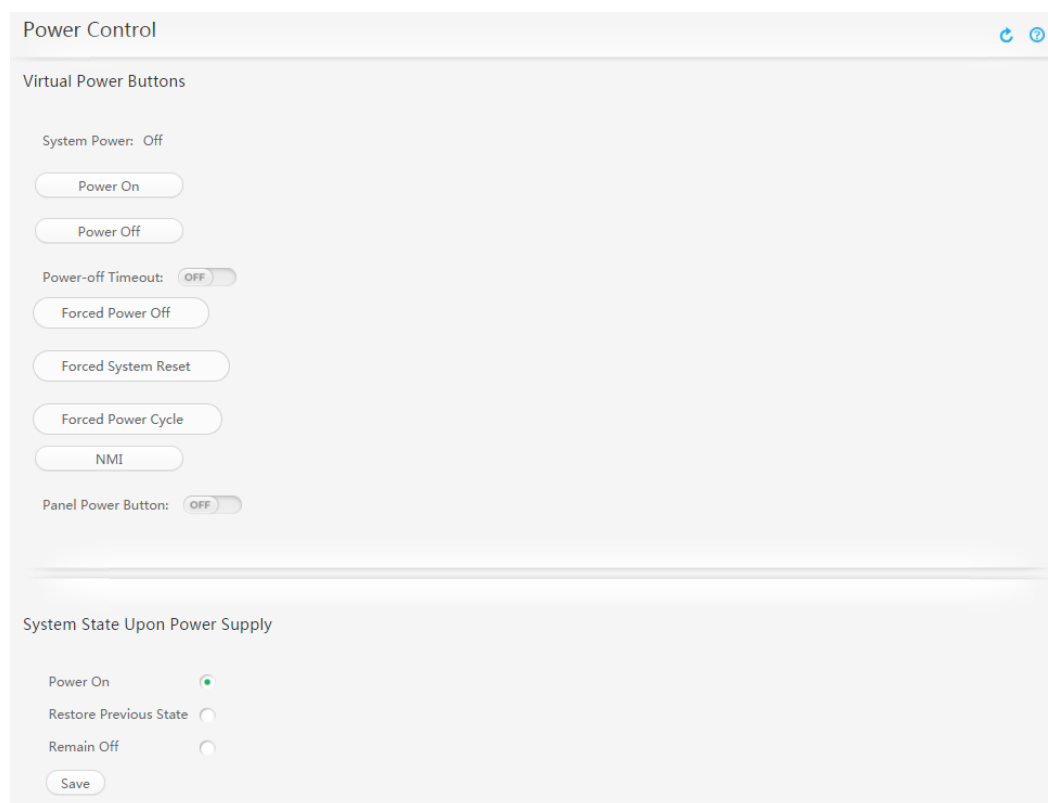
Page Element Description

Table 3-31 Elements on the **Virtual Power Buttons** area

Element	Description
System Power	Current status of the server OS.
Power On	Starts the server OS.

Element	Description
Power Off	Shuts down the server OS.
Power-off Timeout	The iBMC acts according to the setting of **Power-off Timeout** after the **Power Off** button is clicked to shut down the server OS. ● If **Power-off Timeout** is enabled, the iBMC forcibly shuts down the OS when the OS fails to shut down within the specified timeout period. ● If **Power-off Timeout** is disabled, the iBMC does not interfere with the OS shutdown process. The value range and default value of **Timeout Period** vary depending on the server model. For details, see the information displayed on the WebUI. ● To enable the function for power-off timeout, set this parameter to . Click , enter a value in the text box, and click **Save**. ● To disable the function of power-off timeout, set this parameter to .
Forced Power Off	**NOTICE** A forced power-off may cause data corruption or data loss. Forcibly powers off the server OS within 6 seconds after this button is clicked.

Forced System Reset	**NOTICE**
	    A forced reset may damage user programs or unsaved data.
	
	Resets the server OS.
	NOTE
	    ● **Forced System Reset** does not work if the OS is already shut down.
	    ● This operation affects the power-off operation being performed.

Forced Power Cycle	**NOTICE** A forced power cycle may cause data corruption or data loss. Forcibly shuts down the server OS, and about 6 seconds later, starts the OS again.
NMI	**NOTICE** Click this button only for internal commissioning. Before clicking this button, ensure that the OS has the NMI processing program. Otherwise, the OS may crash. Triggers a non-maskable interrupt (NMI). Click this button to trigger an NMI only when the OS is abnormal. Do not click this button when the OS is operating properly.

Element	Description
Panel Power Button Disable Panel Power Button	Disables the power button on the server panel. Click OFF or ON, and click **Save**. Default value: OFF If you set this parameter to ON, the power button on the server panel does not work.

Table 3-32 Options in the **System State Upon Power Supply** area

Option	Description
Power On	Automatically starts the OS after the power supply is restored.
Restore Previous State	Restores the OS to the state before the power failure. ● If the server OS is started before the power failure, the server OS starts automatically after the power supply is restored. ● If the server OS is shut down before the power failure, the server OS is shut down after the power supply is restored.
Remain Off	Keeps the server OS shut down even after the power supply is restored.

Procedure

Table 3-33 Power control operations

Operation	Procedure
Start the server OS.	1. On the **Power Control** page, click the **Power On** button under **Virtual Power Buttons**. The following message is displayed: Are you sure you want to perform this operation? 2. Click **Yes**. The server OS startup time varies according to the server configuration. If "Operation Successful" is displayed, the OS starts successfully. After the OS starts, **System Power** changes to **On**.

Operation	Procedure
Shut down the server OS.	1. On the **Power Control** page, click the **Power Off** button under **Virtual Power Buttons**. The following message is displayed: Are you sure you want to perform this operation? 2. Click **Yes**. If "Operation Successful" is displayed, the server OS is shut down successfully. After the server OS is shut down, **System Power** changes to **Off**.
Forcibly shut down the server OS.	1. On the **Power Control** page, click the **Forced Power Off** button under **Virtual Power Buttons**. The following message is displayed: Are you sure you want to perform this operation? 2. Click **Yes**. If "Operation Successful" is displayed, the server OS is forcibly shut down. After the server OS is forcibly shut down, **System Power** changes to **Off**.
Forcibly Reset the server OS.	1. On the **Power Control** page, click the **Forced System Reset** button under **Virtual Power Buttons**. The following message is displayed: Are you sure you want to perform this operation? 2. Click **Yes**. If "Operation Successful" is displayed, the server OS is forcibly reset.
Power cycle the server OS.	1. On the **Power Control** page, click the **Forced Power Cycle** button under **Virtual Power Buttons**. The following message is displayed: Are you sure you want to perform this operation? 2. Click **Yes**. The time required varies according to the server configuration. If "Operation Successful" is displayed, the server OS is powered off and then on successfully. During the power cycle process, **System Power** changes from **On** to **Off** and then to **On**.

Operation	Procedure
Trigger an NMI	**NOTICE** Perform this operation only when the OS is abnormal. Before clicking this button, ensure that the OS has the NMI processing program. Otherwise, the OS may crash. 1. On the **Power Control** page, click the **NMI** button under **Virtual Power Buttons**. The following message is displayed: Generating an NMI may cause data corruption or data loss. Are you sure you want to continue? 2. Click **Yes**. The time required varies according to the server configuration. If "Operation Successful" is displayed, an NMI is triggered successfully.
Set the power restore policy.	1. On the **Power Control** page, select the power restore policy under **System State Upon Power Supply**. For details about the options, see **Table 3-32**. 2. Click **Save**. If "Operation Successful" is displayed, the setting is successful.
Set the power-off timeout period.	1. On the **Power Control** page, check that **Power-off Timeout** is set to ON. 2. Click ✏, enter a value in the text box. Click ✏ to view the value range. The value range varies according to the server model. The default value is **600**. 3. Click **Save**. If "Operation Successful" is displayed, the setting is successful.
Check the power-off timeout period.	On the **Power Control** page, check the value of **Timeout Period (s)** next to **Power-off Timeout** under the **Virtual Power Buttons** area.

3.6.2 Power Capping

Function Description

The **Power Capping** page allows you to perform the following operations:

- View information about the server power.

- Enable or disable the power capping function, set the power capping value, and specify the action to be taken if power capping fails.

- View the historical average power and peak power line charts of the last week or day, view the power data obtained at each sampling time, and re-collect power statistics.

  The system obtains server power data at an interval of 10 minutes.

NOTICE

- Exercise caution when you set the power capping value. A small power capping value may affect system performance and operations.

- If you set **Forced Shutdown After Power Capping Failure** to , services will be affected. (The RH5885 V3, RH5885H V3, RH8100 V3, and 8100 V5 servers do not provide forced shutdown upon a power capping failure.)

- The **Power Capping** function is unavailable for the iBMC of system B when the RH8100 V3 or 8100 V5 is in dual-system mode.

GUI

Choose **Power** from the main menu, and select **Power Capping** from the navigation tree.

The **Power Capping** page is displayed.

Figure 3-17 Power Capping page
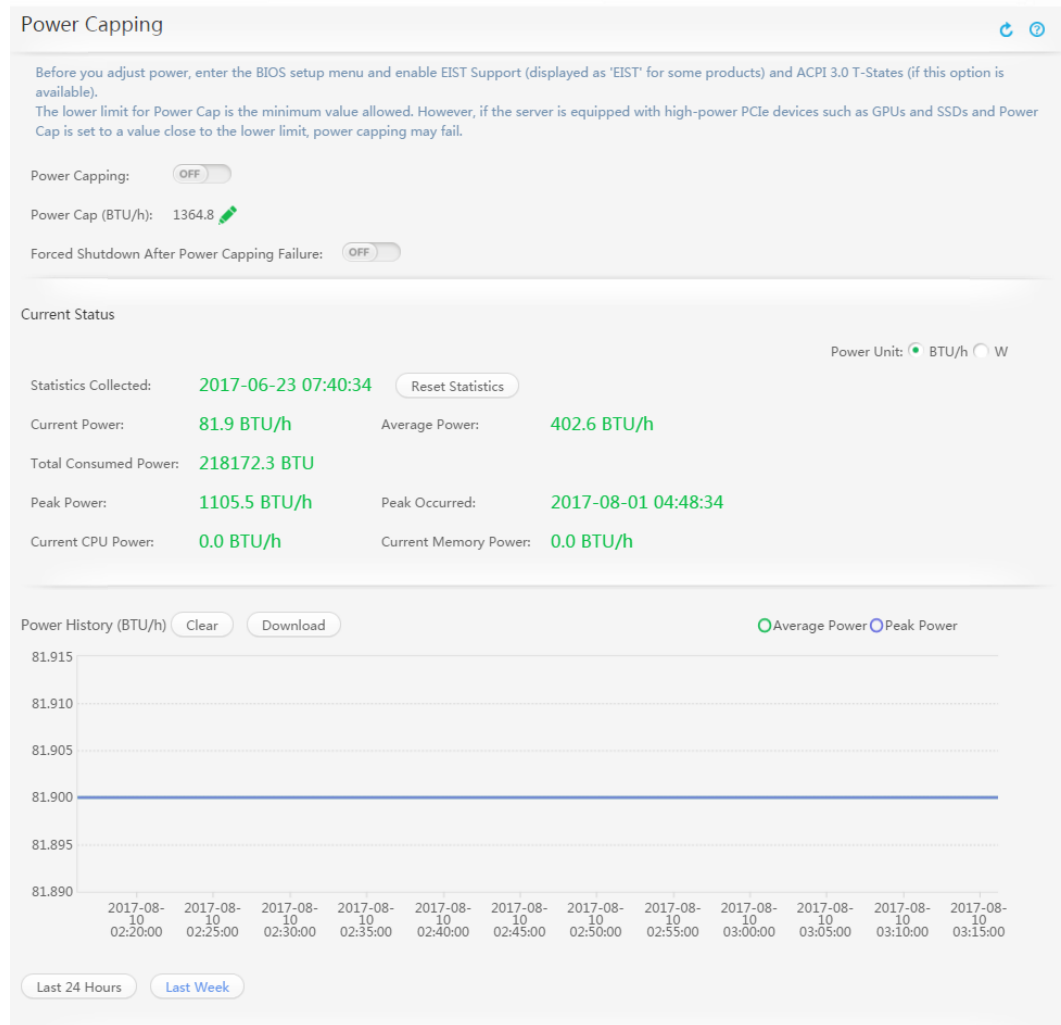
Parameters

Table 3-34 Parameters in the **Power Capping** area

Parameter	Description
Power Capping	Power capping function, which can be enabled or disabled. **NOTE** Before setting the power capping function, ensure that the following parameters are set on the BIOS: ● **EIST Support** or **EIST** is set to **Enabled**. ● **ACPI 3.0 T-States** is set to **Enabled** for a V2 server on the Romley platform. ● **ACPI T-States** is set to **Enabled** for a V3 server on the Brickland platform. (**ACPI T-States** is unavailable for a V3 server on the Grantley platform.) ● **Software Controlled T-States** is set to **Enabled** and **T-State Throttle Level** to the default value **Disabled** for a V5 server on the Purley platform. The power capping function is unavailable for the server in dual-system mode. Power statistics of the server are displayed regardless of the server in single-system or dual-system mode. Click OFF or ON, and click **Save**. ● To enable it, set this parameter to ON. ● To disable it, set this parameter to OFF.
Power Cap (BTU/h)	Maximum power allowed for the server in running. This parameter is unavailable for the server in dual-system mode. Click to view the value range. The value range varies according to the server model. The power cap value cannot be smaller than the lower limit of the recommended value range.
Forced Shutdown After Power Capping Failure (not for RH5885 V3, RH5885H V3, RH8100 V3 and 8100 V5)	Function for automatically shutting down the system 15 seconds after power capping fails. Click OFF or ON, and click **Save**. Set this parameter to ON to automatically shut down the system 15 seconds after power capping fails.

Table 3-35 Parameters in the **Current Status** area

Parameter	Description
Power Unit	Select the power unit, which can be **W** or **BTU/h**. NOTE 1 BTU/h = 0.293 W
Statistics Collected	Start time for power statistics collection.
Current Power	Current power of the server.
Average Power	Average power collected since the first time the server was powered on or since the last statistics collection start time.
Total Consumed Power	Total power collected since the first time the server was powered on or since the last statistics collection start time.
Peak Power	Maximum power collected since the first time the server was powered on or since the last statistics collection start time.
Peak Occurred	Time when the peak power is collected since the first server power-on or the last statistics collection start time.
Current CPU Power	Current CPU power of the server.
Current Memory Power	Current memory power of the server.

Table 3-36 Parameters in the Power History area

Parameter	Description
Power history line chart	
Average power	Average power collected within the last week, day, or the period from the last statistics collection start time to 10 minutes ago.
Peak power	Peak power collected within the last week, day, or the period from the last statistics collection start time to 10 minutes ago.

Procedure

Viewing Server Power

1. On the menu bar, choose **Power**.

2. In the navigation tree, choose **Power Capping**.

   The **Power Capping** page is displayed.

3. View server power data in the **Current State** area.

Re-Collecting Statistics About Server Power

1. Click **Reset Statistics**.

    The following information is displayed:

    Are you sure you want to perform this operation?

2. Click **Yes**.

    The system deletes historical server power statistics.

Setting Power Capping

1. Click ⬤OFF next to **Power Capping**.

    The following information is displayed:

    Are you sure you want to perform this operation?

2. Click **Yes**.

    If "Operation Successful" is displayed and ⬤OFF changes to ⬤ON, the power capping function is enabled.

3. Click ✏, and enter a value in the **Power Cap** text box.

    The value must be within the value range displayed next to the text box.

4. Click **Save**.

    If "Operation Successful" is displayed, the configuration is complete.

Disabling the Power Capping Function

1. Click ⬤ON next to **Power Capping**.

    The following information is displayed:

    Are you sure you want to perform this operation?

2. Click **Yes**.

    If "Operation Successful" is displayed and ⬤ON changes to ⬤OFF, the power capping function is disabled.

Enabling Forced Shutdown After Power Capping Failure

1. Click ⬤OFF next to **Forced Shutdown After Power Capping Failure**.

    The following information is displayed:

    Are you sure you want to perform this operation?

2. Click **Yes**.

    If "Operation Successful" is displayed and ⬤OFF changes to ⬤ON, the server will automatically power off 15 seconds after power capping fails.

Deleting Historical Power Statistics

1. Click **Reset Statistics**.

    The following information is displayed:

    Are you sure you want to perform this operation?

2. Click **Yes**.

The system deletes historical server power statistics and collects server power statistics immediately.

Downloading Historical Power Statistics

Click **Download**.

The historical power data file is automatically saved to the local PC.

Viewing the Power History of the Last Week

1. In the **Power History** area, click **Last week**.

    The peak and average power statistics of the last week are displayed. If the period from the latest statistics collection start time to the current time is less than one week, only the power statistics generated since the latest statistics collection start time are displayed.

Viewing the Power History of the Last 24 Hours

In the **Power History** area, click **Last 24 Hours**.

The peak and average power statistics of the last 24 hours are displayed.

3.6.3 Energy Saving Settings

Function Description

The **Energy Saving Settings** page allows you to adjust the P-states (CPU operating frequency) and T-states (CPU duty cycle) to reduce power consumption.

NOTICE

Energy saving settings may affect system performance. Exercise caution when configuring energy saving settings.

Before adjusting the server power, ensure that the following parameters are set on the BIOS:

- **EIST Support** or **EIST** is set to **Enabled**.
- **ACPI 3.0 T-States** is set to **Enabled** for a V2 server on the Romley platform.
- **ACPI T-States** is set to **Enabled** for a V3 server on the Brickland platform. (**ACPI T-States** is unavailable for a V3 server on the Grantley platform.)
- **Software Controlled T-States** is set to **Enabled** and **T-State Throttle Level** to the default value **Disabled** for a V5 server on the Purley platform.

GUI

Choose **Power** from the main menu, and select **Energy Saving Settings** from the navigation tree.

The **Energy Saving Settings** page is displayed.

The **Energy Saving Settings** area consists of two sections: **Power Adjustment** and **PSU settings**.

Figure 3-18 Energy Saving Settings page of the RH8100 V3
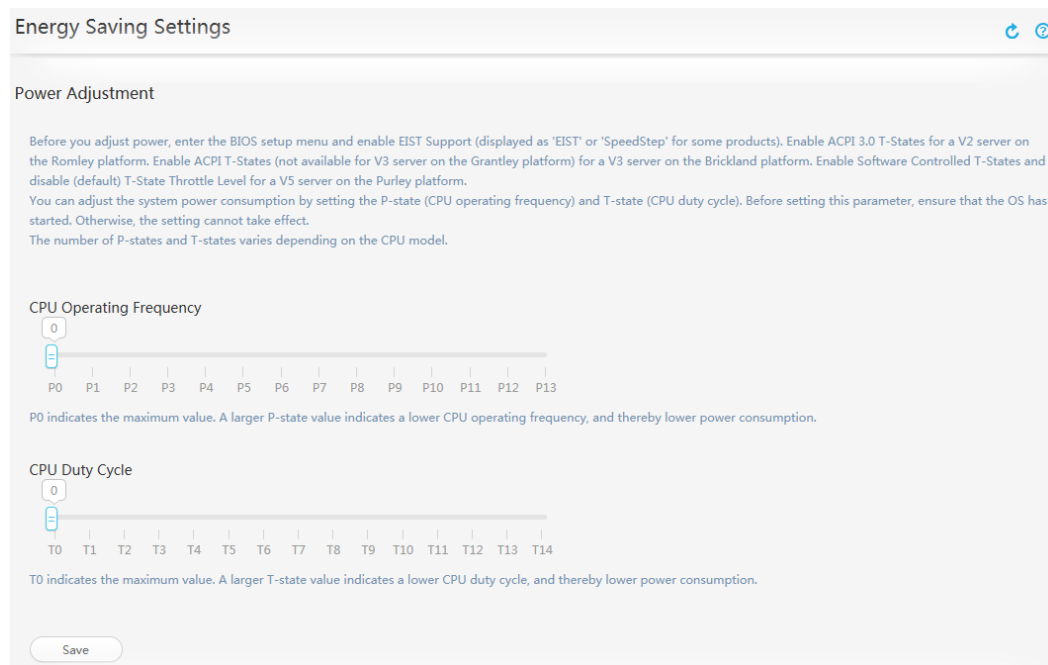
Figure 3-19 Energy Saving Settings page of other rack servers
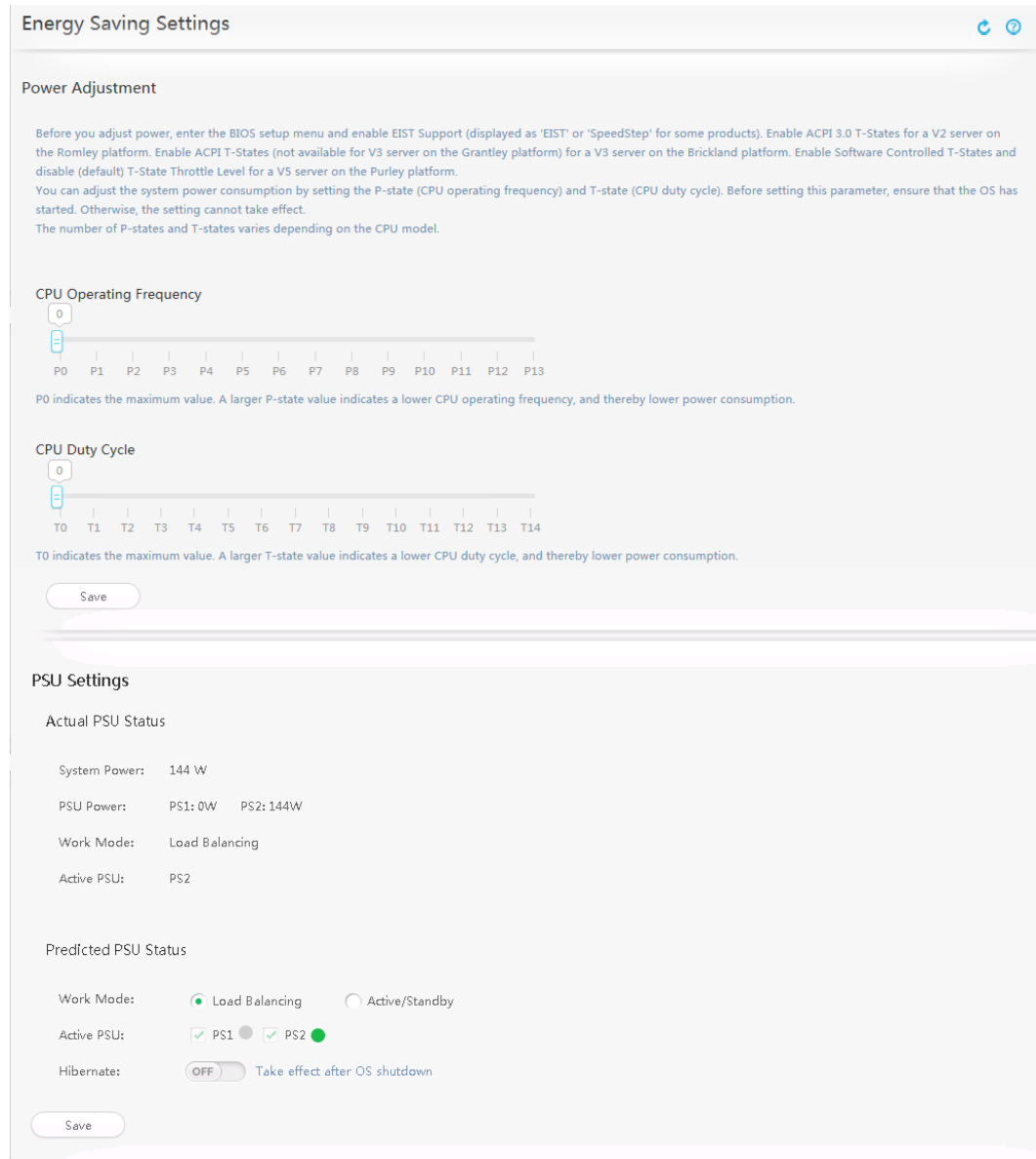
Parameter Description

Table 3-37 Parameters in the **Power Adjustment** section

Parameter	Description
CPU Operating Frequency	Drag the slider bar to adjust the CPU operating frequency (P-states).
	The number of P-states varies according to the CPU model. P0 is the maximum value. A larger P-state value indicates a lower CPU operating frequency, and thereby lower power consumption.
	NOTE
	- If the actual server power exceeds the power cap value after the P-state and T-state are adjusted, the P-state and T-state values will be automatically adjusted to the normal values.
	- Before setting this parameter, ensure that the OS has started. Otherwise, the setting cannot take effect.
CPU Duty Cycle	Drag the slider bar to adjust the CPU duty cycle (T-states).
	The number of T-states varies according to the CPU model. T0 is the maximum value. A larger T-state value indicates a lower CPU duty cycle, and thereby lower power consumption.
	NOTE
	- If the actual server power exceeds the power cap value after the P-state and T-state are adjusted, the P-state and T-state values will be automatically adjusted to the normal values.
	- Before setting this parameter, ensure that the OS has started. Otherwise, the setting cannot take effect.

Table 3-38 Parameters in **PSU settings** (not for the RH8100 V3)

Parameter	Description
Actual PSU Status	
System Power	Current server power.
PSU Power	Current power of all power supply units (PSUs) in the server.
Work Mode	Current PSU working mode.
Active PSU	Active PSUs.
	NOTE
	If **Work Mode** is set to **Load Balancing**, all detected PSUs are displayed.
Predicted PSU Status	

Parameter	Description
Work Mode	PSU working mode. Value: ● **Load Balancing**: Multiple PSUs simultaneously supply power to the system and share the system power consumption. This mode provides a high power supply capability for the entire system and has minor impact on the standby PSUs if one PSU is faulty. However, the PSUs in this mode have low power supply efficiency and consume more electricity. ● **Active/Standby**: One or more active PSUs supply power to the system, and the other PSUs are in standby state. This mode provides a higher power supply efficiency and less power consumption, and extends the PSU service life. However, it has a lower power supply capability. Default value: **Load Balancing** NOTE ● When the system power consumption is low, select **Active/Standby** to decrease server power consumption. ● If the system power consumption is greater than or equal to 75% of the power ratings of the active PSUs, the PSU working mode automatically changes to **Load Balancing**. ● Currently the active/standby mode (1+1 redundancy) can be used only when two PSUs are configured.
Active PSU	Active PSUs.

Parameter	Description
Hibernate	**NOTICE** After deep hibernation is enabled and the server is powered off, if all active PSUs are removed or stop outputting power due to faults, the entire server loses power for about 10 seconds and then the PSUs in deep hibernation mode automatically turn on to output power. Specifies whether deep hibernation is enabled. If deep hibernation is enabled, certain PSUs enter the deep hibernation mode and stop outputting power when the server is powered off. When the server is powered on, the PSUs in deep hibernation mode continue to output power. Click (OFF) or (ON), and click **Save**. ● (ON): enables deep hibernation. The setting takes effect when the OS is powered off. ● (OFF): disables deep hibernation. The setting takes effect when the OS is powered off. **NOTE** ● The deep hibernation setting is available only for the 1288H V5, 2288H V5, 2488 V5, 2488H V5, and 5885H V5 servers. ● If deep hibernation is enabled, the PSUs will be in hibernation after the OS is powered off.

Procedure

Configuring CPU Energy Saving Policy

1. On the menu bar, choose **Power**.

2. In the navigation tree, choose **Energy Saving Settings**.

    The **Energy Saving Settings** page is displayed.

3. Drag the slider bar to adjust the CPU operating frequency or duty cycle.

    For details about the parameters, see **Table 3-37**.

    📖 NOTE

    ● Drag one slider bar at a time.

    ● Adjusting the maximum CPU operating frequency has greater impact on power consumption and smaller impact on system performance than adjusting the CPU duty cycle. Therefore, adjust the maximum CPU operating frequency first.

4. Click **Save**.

    The following information is displayed:

    Are you sure you want to perform this operation?

5. Click **Yes**.

    If "Operation Successful" is displayed, the setting is complete.

Setting the PSU Working Mode (Unsupported by RH8100 V3)

1. On the menu bar, choose **Power**.

2. In the navigation tree, choose **Energy Saving Settings**.

   The **Energy Saving Settings** page is displayed.

3. In the **Predicted PSU Status** area, set the PSU working mode and active PSU and whether to enable deep hibernation.

   For details about the parameters, see **Table 3-38**.

   📖 NOTE

   - The deep hibernation setting is available only for the 1288H V5, 2288H V5, 2488 V5, 2488H V5, and 5885H V5 servers.
   - If deep hibernation is enabled, the PSUs will be in hibernation after the OS is powered off.

4. Click **Save**.

   The following information is displayed:

   Are you sure you want to perform this operation?

5. Click **Save**.

   If "Operation Successful" is displayed, the setting is complete.

3.6.4 Smart Cooling

Function Description

Smart cooling implements automatic adjustment of the fan speed based on the CPU or memory temperature, ensuring nornal running of server compoents.

The **Smart Cooling** page allows you to query and set the fan speed adjustment policy for a server.

GUI

Choose **Power** from the main menu, and select **Smart Cooling** from the navigation tree.

Parameter Description

lists intelligent speed adjustment modes supported by each server. lists related parameters.

Table 3-39 Intelligent speed adjustment modes supported by each server

Type	Model	iBMC Version	Supported Intelligent Speed Adjustment Modes
Air-cooled server	2288H V5	V260 and later	- Energy saving mode - Low noise mode - High performance mode - Custom mode Energy saving mode is the default setting.

Table 3-40 Smart Cooling parameters

Parameter	Description
Energy saving mode	Default speed adjustment mode for air-cooled systems. Adjusts the server fans to operate at a certain speed based on the system load and heat dissipation to minimize the power consumption.
Low noise mode	Enables the fans to operate at the minimum speed that meets heat dissipation requirements to reduce noise.
High performance mode	Enables the fans to operate at high speed to ensure optimal cooling of the key components and achieve high system performance.

Parameter	Description
Custom mode	Allows users to set the target CPU temperature and the fan speeds corresponding to different inlet temperature ranges. ● The **CPU Target Temperature**, **Air Outlet Target Temperature**, and **Fan Speed** parameters are available only when **Custom mode** is selected. ● The system provides the value range of **CPU Target Temperature** and **Air Outlet Target Temperature** based on the current load and heat dissipation of the server. Set this parameter based on the value range displayed. ● The **Fan Speed** value range is 20 to 100. The fan speed corresponding to a higher temperature range must be greater than the fan speed corresponding to a lower temperature range. **NOTE** During CPU replacement, if the highest operating temperature of the new CPU is lower than the current value of **CPU Target Temperature**, the iBMC automatically changes the value of **CPU Target Temperature** to the maximum temperature allowed by the new CPU.
NOTE ● If the fan adjustment mode is **Manual**, all the settings on the **Smart Cooling** page will take effect only when the fan adjustment mode changes to **Auto**. ● You can also set the fan speed adjustment on the BIOS. For details, see the *BIOS Parameter Reference* of the server you use.	

Procedure

📖 **NOTE**

For example, to set the smart cooling mode to **Custom mode**, perform the following steps:

1. Select **Custom mode**.

2. Set **CPU Target Temperature** based on the value range displayed.

3. Set the fan speeds corresponding to the inlet temperature ranges.

4. Click **Save**.

   The system displays "Specifying custom parameter values may result in insufficient heat dissipation."

5. Click **Yes**.

   If "Operation successful" is displayed, the smart cooling mode is set successfully.

3.7 Configuration

3.7.1 Local Users

Function Description

The **Local Users** page allows you to view and manage the users of the iBMC.

The iBMC supports a maximum of 16 users. You can add, modify, and delete users on the **Local Users** page.

GUI

Choose **Configuration** from the main menu, and select **Local Users** from the navigation tree.

The **Local Users** page is displayed. The page consists of three areas.

- Local user list: lists iBMC users.
- User rights: lists the rights assigned to **Administrator**, **Operator**, **Common User**, and four custom roles.
- SSH public key management: lists the SSH users configured with public keys. The SSH public keys can be added or deleted.

Figure 3-20 Local Users page

Parameter Description

Table 3-41 Parameters related to local users

Parameter	Description
Add	Adds a local user.
✏	Changes information about a local user.
✖	Deletes a local user. **NOTE** ● All local users, including the administrators, operators, common users, and custom users, can be deleted. ● In iBMC V357 and later versions, if the iBMC has multiple enabled administrators, the roles of the default users can be modified. If there is only one administrator enabled, this administrator cannot disabled or deleted and the administrator role cannot be modified. ● You can restore the administrator by restoring the iBMC default settings. For details, see **Common Operations** > **Restoring Default iBMC Settings** in the iBMC user guide. ● If **User Management** is enabled under **OS User Management** on the **Configuration** > **System** page, you can also add iBMC users by sending standard IPMI commands from the OS.
Save	Saves the configuration of a local user.
User Name	User name for logging in to the iBMC. By default, the user name is **root** for V3 servers and **Administrator** for V5 servers, and the password is on the product nameplate. For security purposes, change the default password upon the first login, and periodically change the password.
Role	Role assigned to the user. The user role specifies the operations that can be performed by the user.
Password Validity (Days)	Validity period of the user password.
Status	User status, which can be enabled or disabled.
Rule	Login rules that apply to the user.
Login Interface	Interfaces through which the user can log in to the iBMC.
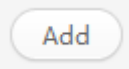
Table 3-42 Parameters related to privilege

Parameter	Description
Administrator	User who can perform all operations. The permissions of **Administrator** cannot be changed.
Operator	User who can perform basic management, KVM management, VMM management, and power control, query information, and configure their own passwords. The permissions of **Operator** cannot be changed.
Common User	User who can query information and configure their own passwords. The permissions of **Common User** cannot be changed.
Custom Role 1 to 4	User who can perform the specified operations.
User Mgmt	Perform user and password configuration. **User Mgmt** includes the following: ● Configuration of local, online, and LDAP users ● Configuration of two-factor authentication ● Restoration of factory settings
Basic Mgmt	Perform basic configuration of server out-of-band management. **Basic Mgmt** includes the following: ● Network configuration ● Alarm report configuration ● Server identification ● Firmware upgrade ● Download and deletion of system logs ● Setting of the boot device ● Configuration of storage devices ● Language update On the **Alarm Settings**, **Network**, **System**, **System Info**, and **Language Update** pages, unauthorized users can only query data.
KVM	Perform remote management using the Java or HTML5 integrated remote console or independent remote console, and perform VNC configuration (only available to V5 servers) and serial port redirection.
VMM	Use the virtual media function.

Parameter	Description
Security Mgmt	Perform configuration and query of security features. **Security Mgmt** includes the following: ● Query of operation logs and security logs ● Selection of algorithms and protocols ● SSL certificate management ● Service configuration ● One-click data collection ● Import and export of configuration files ● Configuration of login security banner On the **Services**, **SSL Certificate**, and **Import/Export** pages, unauthorized users can only query data.
Power Control	Perform power-on/off and restart operations, and power and energy-saving configuration. On the **Power Control**, **Power Capping**, and **Energy Saving Settings** pages, unauthorized users can only query data.
Diagnostics	Perform field fault locating and commissioning operations. **Diagnostics** includes the following: ● Access to the maintenance and commissioning interface ● Sensor simulation ● Configuration of automatic video recording ● Manual and automatic screenshot ● Serial port data ● Black box
Query	Query information excepting security settings, user settings, and system information.
Own password & SSH	Configure their own passwords and manage the SSH public key. System default users have this permission by default. Custom users can be assigned with this permission.

Table 3-43 SSH Public Key Management

Parameter	Description
User Name	User with an SSH public key.
Public Key Hash	String converted from an SSH public key through hash algorithms.
✖	Deletes the public key of an SSH user.

Parameter	Description
Add	Imports a public key for an SSH user.

Procedure

Viewing User Information

1. On the menu bar, choose **Configuration**.

2. In the navigation tree, choose **Local Users**.

   The **Local Users** page is displayed.

3. View information about the local users.
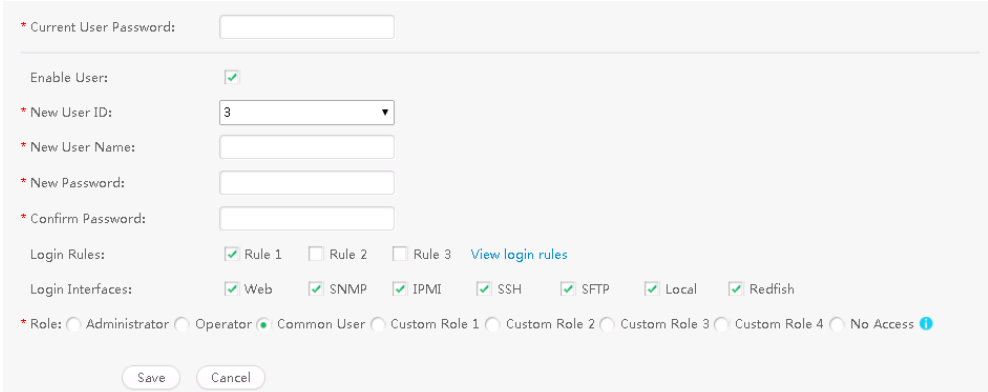
Adding Users

You can add a maximum of 15 users for the iBMC.
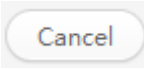
1. Click **Add**.

   The page for adding a user is displayed, as shown in **Figure 3-21**. For details about the parameters, see **Table 3-44**.

Figure 3-21 Adding a user

Table 3-44 Parameters for adding a user

Parameter	Description
Cancel	Exits the page for setting a local user without saving the settings.
Save	Saves the information.
Current User Password	Password of the user for logging in to the iBMC.

Parameter	Description
Enable User	Status of the user.
New User ID	ID of the user to be added. Value range: 3 to 17
New User Name	Name of the user to be added. Value: a string of 1 to 16 characters The user name must meet the following requirements: ● Allow letters, digits, and special characters (excluding :<>&,'"/\%). ● Cannot contain spaces or start with **#**, **+**, or **-**.
New Password	Password for logging in to the iBMC. For security purposes, enable password complexity check and periodically change your password. **NOTE** Only the administrators can enable or disable the password complexity check. Value: ● If password complexity check is disabled, the password cannot be empty or exceed 20 characters. ● If password complexity check is enabled, the password must meet the following requirements: – Contain 8 to 20 characters – Contain at least a space or one of the following special characters: `` `~!@#$%^&*()-_=+|[{}];:'",<.>/? `` – Contain at least two types of the following characters: – Uppercase letters A to Z – Lowercase letters a to z – Digits 0 to 9 – Cannot be the same as the user name or the user name in reverse order. – Have at least two new characters when compared with the previous password. ● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)
Confirm Password	Password for logging in to the iBMC. This value must be the same as **New Password**.

Parameter	Description
Login Rules	Login rules that apply for the user. Click **View login rules** to view the login rules configured.
Login Interfaces	Interfaces through which the user can log in to the iBMC. Values: ● **Web**: The user can use a web browser to log in to the iBMC WebUI. ● **SNMP**: The user can use an SNMP tool (such as MIB Browser) to log in to iBMC. ● **IPMI**: The user can use an IPMI tool (such as IPMItool) to log in to the iBMC CLI. ● **SSH**: The user can use an SSH tool (such as PuTTY) to log in to the iBMC CLI. ● **SFTP**: The user can use an SFTP tool (such as Xftp) to log in to the iBMC file system. ● **Local**: The user can use the serial port on the server to log in to the iBMC CLI or use an LCD to log in to the iBMC management interface. ● **Redfish**: The user can use a Redfish tool to log in to iBMC. **NOTE** By default, all login interfaces are selected for a new user.
Role	Role assigned to a user. The user role specifies the operations that can be performed by a user. Value: ● **Administrator**: Users assigned the **Administrator** role can perform all operations. ● **Operator**: Users with the **Operator** role can perform basic management, remote control, remote media, power control, query information, and configure their own data. ● **Common User**: Users assigned with the **Common User** role can query information and configure their own data. ● **Custom Role**: Users assigned **Custom Role 1** to **Custom Role 4** can perform the specified operations. ● **No Access**: Users assigned **No Access** role cannot perform any operation. **NOTE** The default role is **No Access** for new users.

2. Set user parameters. For details about the parameters, see **Table 3-44**.

📖 **NOTE**

- The user with ID 1 is a reserved user defined in the IPMI standard. This user is not allowed to log in to the iBMC.
- The user with ID 2 is **root** for V3 servers and **Administrator** for V5 servers.

3. Click **Save**.
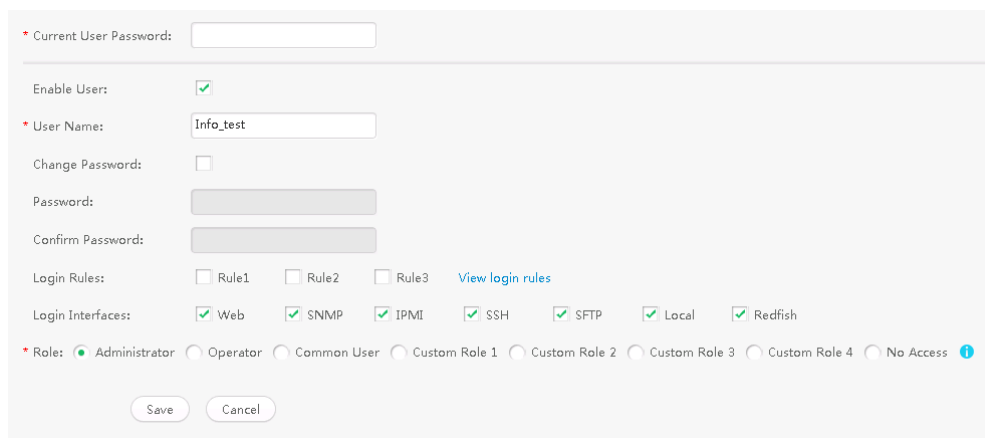
   The information about the new user is displayed in the user list.

Modifying User Information

1. In the local user list, locate the user to be modified and click 🖉.

   The page for modifying user information is displayed, as shown in **Figure 3-22**. For details about the parameters, see **Table 3-45**.

Figure 3-22 Modifying user information

Table 3-45 Parameters related to editing a user

Parameter	Description
Cancel	Exits the page for setting a local user without saving the settings.
Save	Saves the information. **NOTE** Changing the user name, password, or user role will forcibly log out the user.
Current User Password	Password of the user for logging in to the iBMC.
Enable User	Status of the user.
User Name	Name of the user to be modified.

Parameter	Description
Change Password	Specifies whether to change the user password. Select the check box and enter the new password in **Password** and **Confirm Password**. ● If password complexity check is disabled, the password cannot be empty or exceed 20 characters. ● If password complexity check is enabled, the password must meet the following requirements: – Contain 8 to 20 characters – Contain at least a space or one of the following special characters: `` `~!@#$%^&*()-_=+|[{}];:'",<.>/? `` – Contain at least two types of the following characters: – Uppercase letters A to Z – Lowercase letters a to z – Digits 0 to 9 – Cannot be the same as the user name or the user name in reverse order. – Have at least two new characters when compared with the previous password. ● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)
Login Rules	Login rules that apply for the user. Click **View login rules** to view the login rules configured.

Parameter	Description
Login Interfaces	Interfaces through which the user can log in to the iBMC. Values: ● **Web**: The user can use a web browser to log in to the iBMC WebUI. ● **SNMP**: The user can use an SNMP tool (such as MIB Browser) to log in to iBMC. ● **IPMI**: The user can use an IPMI tool (such as IPMItool) to log in to the iBMC CLI. ● **SSH**: The user can use an SSH tool (such as PuTTY) to log in to the iBMC CLI. ● **SFTP**: The user can use an SFTP tool (such as Xftp) to log in to the iBMC file system. ● **Local**: The user can use the serial port on the server to log in to the iBMC CLI or use an LCD to log in to the iBMC management interface. ● **Redfish**: The user can use a Redfish tool to log in to iBMC.
Role	Role assigned to a user. The user role specifies the operations that can be performed by a user.

2. Enter the current password of the user, and modify the user information.

   For details about the parameters, see **Table 3-45**.

3. Click **Save**.

   The user information is modified successfully.

Deleting a User

1. In the local user list, locate the user to be deleted and click ✖.

   A confirmation dialog box is displayed, prompting you to enter the current user password.

2. Enter the current user password and click **OK**.

   The user is deleted from the user list.

Configuring Custom Roles

The operation permissions of the default roles (**Administrator**, **Operator**, and **Common User**) cannot be modified, but the administrator can set the operation permissions for custom roles.

1. In the function list, select modules for the custom roles.

   Table 3-42 describes the permissions.

2. Click **Save**.

   A dialog box is displayed, prompting you to enter the current user password.

3. Enter the current user password and click **OK**.

Importing an SSH Public Key
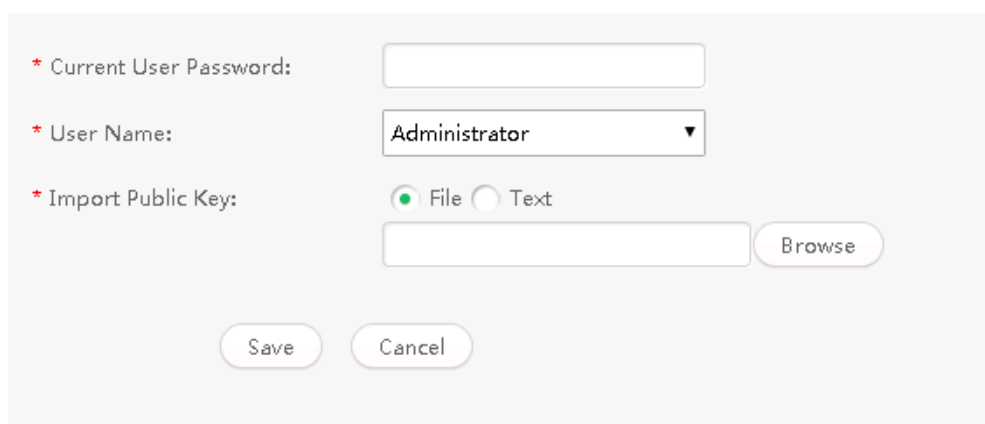
◻ **NOTE**

- After a private key is generated on a client, import the corresponding public key into the iBMC to ensure secure access of SSH users to the iBMC.
- Each user has only one public key. The newly imported public key will replace the old one.
- Public keys can be in the RFC 4716 or OpenSSH format. The public key type is RSA or DSA. An RSA key contains 2048 or 4096 bits, and a DSA key contains 1024 or 2048 bits.

1. Under **SSH Public Key Management**, click **Add**.

   The related parameters are displayed, as shown in **Figure 3-23**. **Table 3-46** describes the parameters.

   Figure 3-23 Importing an SSH public key

   Table 3-46 Parameters related to importing SSH public keys

Parameter	Description
Current User Password	Password of the user for logging in to the iBMC.
User Name	User for which you want to import an SSH public key.
Import Public Key	Mode of importing an SSH public key. Value: • **File**: Import an SSH public key file from the local client. • **Text**: Enter SSH public key information in the text box.

2. Set the parameters. For details about the parameters, see **Table 3-46**.
3. Click **Save**.

   If "Public key imported successfully" is displayed, the SSH public key is imported.

3.7.2 LDAP

Function Description

The **LDAP** page allows you to view and configure Lightweight Directory Access Protocol (LDAP) user information.

The iBMC provides an access function for LDAP users. An LDAP user can log in to the iBMC WebUI or uses an SSH tool to log to in the iBMC

NOTICE

On the LDAP server, **DisplayName** and **CN** must be the same.

The iBMC supports a maximum of six domain servers. During the login to the iBMC WebUI, the domain server can be manually specified or automatically searched. During the login to the iBMC CLI, the domain server is automatically searched.

NOTE

The iBMC supports Windows Active Directory (AD) and Linux OpenLDAP.

GUI

Choose **Configuration** from the main menu, and select **LDAP** from the navigation tree.

The **LDAP** page is displayed.
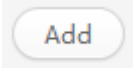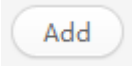
Figure 3-24 LDAP page

Parameter Description

Table 3-47 Parameters on the LDAP page

Parameter	Description	
LDAP	The LDAP function enables domain users to access the iBMC. Click [OFF] or [ON], and click **Save**. ● [ON]: enables the LDAP function. ● [OFF]: disables the LDAP function.	
Domain Controller 1 The iBMC supports a maximum of six domain controllers (servers). When a user attempts to log in to iBMC WebUI through LDAP, the user can select the domain controller or **Automatic matching**. Domain controllers 1 to 6 have the same parameters. NOTE 　Parameters with asterisks (*) are mandatory.		
Basic Parameters	Certificate Verification	Certificate verification of the LDAP server, which can be enabled or disabled. Enable certificate verification for security purposes. After certificate verification is enabled, you need to import the LDAP root certificate, install the AD, DNS, and CA certificate issuer on the LDAP server, and import the CA certificate into the LDAP server and iBMC.
	LDAP Server Address	LDAP server IP address. Format: IPv4 or IPv6 address. After certificate verification is enabled, set this parameter to the LDAP server FQDN (*Host name.Domain name*), and configure DNS address information on the **Network** page.
	LDAPS Port	Port number for the LDAP service. Value: an integer ranging from 1 to 65535 Default value: **636** NOTE 　The iBMC supports LDAPS, but it does not support LDAP without SSL (port number: 389), so the LDAP server must have a trusted server certificate to prove its identity.

Paramet er	Description	
	Domain	User domain to which an LDAP user defined in the domain controller belongs. Value: a string of up to 255 characters The value can contain letters, digits, and special characters.
	Bind DN	Distinguished name (DN) of an LDAP proxy user. For example, **CN=username,OU=company,DC=domain,DC=com**, which must be the same as the DN set on the LDAP server. Value range: a string of 255 bytes (64 to 255 characters). The specific length varies with the number of bytes of each character.
	Bind Password	Authentication password for the LDAP proxy user.
	Base DN	Directory on the LDAP server of the LDAP user who can log in to the iBMC. If the default user folder is not configured on the LDAP server, set this parameter on the iBMC to specify the search scope of LDAP users. If the default user folder is configured on the LDAP server, this parameter is optional. ● If this parameter is not set, LDAP users will be searched from the default user folder of the LDAP server. ● If this parameter is set, LDAP users will be searched from the path specified by this parameter. Format: "CN=xxx,CN=xxx,..." or "OU=xxx,OU=xxx,..." The upper-level node follows the lower-level node. For example, if the user infotest is in **\testusers\part1** on the LDAP server, enter **OU=part1,OU=testusers**. NOTE For details about the difference between CN and OU, see the detailed description of the LDAP protocol. For example, in Windows AD, the attribute of ☐ is CN, and the attribute of ☐ is OU. Value range: a string of 255 bytes (64 to 255 characters). The specific length varies with the number of bytes of each character.
	Current User Password	Password of the user for logging in to the iBMC.

Paramet er	Description	
Root Certificat e	Certificat e	LDAP root certificate in .cer, .pem, .cert, or .crt format. **NOTE** The system takes longer to upload certificate files that exceed 100 MB in size. Refresh the page for the latest status.
	Certificat e Status	Status of the LDAP root certificate, which can be imported or not imported.
	Certificat e Info	Certificate information.
LDAP Groups	Add	Adds an LDAP group. Click Add to add an LDAP group.
	✏️	Displays the region for configuring an existing LDAP group.
	✖️	Modifies an LDAP group.
	LDAP Group	Name of the LDAP group to which an LDAP user belongs. Value range: a string of 255 bytes (64 to 255 characters). The specific length varies with the number of bytes of each character.
	LDAP Group Folder	Directory on the LDAP server of the LDAP group that can log in to the iBMC. Format: "CN=xxx,CN=xxx,..." or "OU=xxx,OU=xxx,..." The upper-level node follows the lower-level node. For example, if the LDAP group **grouptest** is in **\testgroups\part1** on the LDAP server, enter **OU=part1,OU=testgroups**. **NOTE** For details about the difference between CN and OU, see the detailed description of the LDAP protocol. For example, in Windows AD, the attribute of 📁 is CN, and the attribute of 🗂️ is OU. Value range: a string of 255 bytes (64 to 255 characters). The specific length varies with the number of bytes of each character.
	Role	Role assigned to an LDAP group. Value: **Administrator**, **Operator**, **Common user**, or **Custom Role**.
	Login Rule	Login rules that apply to the LDAP group.

Paramet er	Description	
	Login Interface	Interfaces through which the LDAP group members can log in to iBMC. Values: **Web**: Users can user a web browser to log in to the iBMC WebUI. **SSH**: Users can use an SSH tool (such as PuTTY) to log in to the iBMC CLI. **Redfish**: Users can use a Redfish tool to log in to iBMC.

Procedure

Enable LDAP and set LDAP controller parameters.

1. On the menu bar, choose **Configuration**.

2. In the navigation tree, choose **LDAP**.

   The **LDAP** page is displayed.

3. Set **LDAP Function** to [ON].

4. Set LDAP controller parameters.

5. Click **Save**.

   The message "Operation Successful" is displayed.

Import an LDAP root certificate.

1. In the **Root Certificate** area, click **Browse** next to **Certificate** and select an LDAP root certificate.

2. Click **Upload**.

   If the certificate is uploaded successfully, **Certificate Status** changes to **The certificate has been uploaded**, and the information about the imported certificate is displayed. For details about the parameters, see **Table 3-48**.

Table 3-48 Parameters in the Import LDAP Root Certificate area

Parameter	Description
Issued By	Issuer of the LDAP certificate. **Issued By** and **Issued To** have the same parameters.

Parameter	Description
Issued To	User (current server) of an LDAP certificate, including: ● **CN**: user name. ● **OU**: department of the user. ● **O**: company to which the user belongs. ● **L**: city of the user. ● **S**: state or province of the user. ● **C**: country of the user.
Valid From	Date from which the LDAP certificate is valid.
Valid To	Date when the LDAP certificate will expire.
Serial Number	Serial number of the LDAP certificate, used for identifying and migrating the certificate.

Add an LDAP group.

You can add a maximum of five LDAP groups for the iBMC.

1. In the **LDAP Group** area, click **Add**.

   The page for adding an LDAP group is displayed, as shown in **Figure 3-25**.

   Figure 3-25 Adding an LDAP group

   Table 3-49 Parameters for adding an LDAP group

Parameter	Description
Current User Password	Password of the user for logging in to the iBMC.
LDAP Group	Name of the LDAP group to which an LDAP user belongs. Value range: a string of 255 bytes (64 to 255 characters). The specific length varies with the number of bytes of each character.

Parameter	Description
LDAP Group Folder	Directory on the LDAP server of the LDAP group that can log in to the iBMC. Format: "CN=xxx,CN=xxx,..." or "OU=xxx,OU=xxx,..." The upper-level node follows the lower-level node. For example, if the LDAP group grouptest is in **\testgroups\part1** on the LDAP server, enter **OU=part1,OU=testgroups**. **NOTE** For details about the difference between CN and OU, see the detailed description of the LDAP protocol. For example, in Windows AD, the attribute of ![folder] is CN, and the attribute of ![folder] is OU. Value range: a string of 255 bytes (64 to 255 characters). The specific length varies with the number of bytes of each character.
Login Rules	Login rules that apply to the LDAP group.
Login Interface	Interfaces through which the LDAP group members can log in to iBMC. Values: ● **Web**: Users can user a web browser to log in to the iBMC WebUI. ● **SSH**: Users can use an SSH tool (such as PuTTY) to log in to the iBMC CLI. ● **Redfish**: Users can use a Redfish tool to log in to iBMC.
Role	Role assigned to an LDAP group. Value: **Administrator**, **Operator**, **Common user**, or **Custom Role**.

2. Set the LDAP group parameters.
3. Click **Save**.

   Information about the new LDAP group is displayed in the LDAP group list.

Delete an LDAP group.

1. In the LDAP group area, click ❌ for the LDAP group to be deleted.

   A dialog box is displayed, prompting you to enter the current user password.
2. Enter the current user password.

Edit an LDAP group.

1. In the LDAP group area, click ✏️ for the LDAP group to be edited.
2. Enter the current user password and modify the LDAP group parameters. For details about the parameters, see **Table 3-49**.

3. Click **Save**.

3.7.3 Two-Factor Authentication

Function Description

Two-factor authentication allows user access only after both the client certificate and password are correct. It provides more security than the conventional authentication of only the account password.

You can upload the root and client certificates issued by the CA to the iBMC to implement secure connection between the client and the iBMC WebUI.

GUI

Choose **Configuration**, and select **Two-Factor Authentication** from the navigation tree.

The **Two-Factor Authentication** page is displayed.
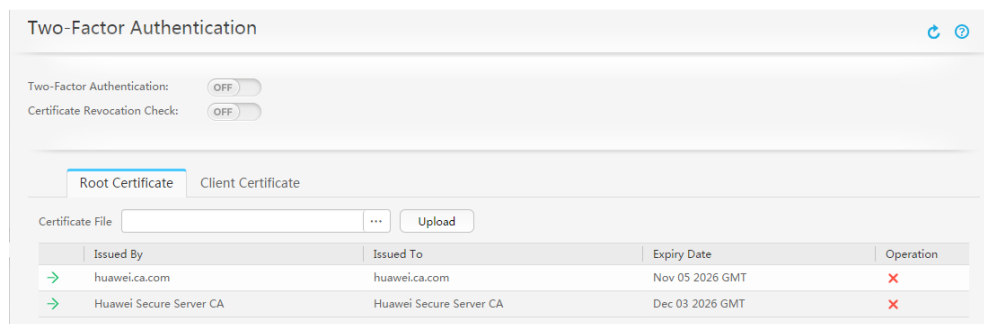
Description

Table 3-50 Two-Factor Authentication

Paramet er	Description
Two-Factor Authenti cation	Two-factor authentication allows users to log in to the iBMC WebUI only after the certificate and password are correct. • ![ON]: enables two-factor authentication. • ![OFF]: disables two factor authentication. **NOTE** • After two-factor authentication is enabled, import the root and client certificates. Otherwise, authentication failures may occur in subsequent logins. • After two-factor authentication is enabled, the SSH service will be automatically disabled and cannot be enabled manually.

Paramet er	Description
Certificat e Revocati on Check	Certificate revocation check verifies the validity of the client certificate during authentication. If the client certificate is invalid, the user cannot log in to the iBMC WebUI. • [ON]: enables certificate validity check. • [OFF]: disables certificate validity check. **NOTE** The certificate revocation check uses Online Certificate Status Protocol (OCSP). Before enabling the certificate revocation check, ensure that communication between the iBMC and the OCSP server is normal. Otherwise, the web service may become unavailable.
Root Certificat e	Root certificates that have been uploaded to the iBMC and their information. The iBMC supports a maximum of 16 root certificates.
Client Certificat e	Client certificates that have been uploaded to the iBMC and their information, such as the user name, role, client certificate fingerprint (hash value of the client certificate file) and status. The iBMC supports client certificates of a maximum of 16 users.

Procedure

Enabling Two-Factor Authentication and Uploading Certificates to the iBMC

◫ NOTE

● Before the operation, apply for the root and client certificates from a formal CA.

● Base64-coded root and client certificates can be uploaded. Valid root and client certificate formats include *.cer, *.crt, and *.pem.

1. On the menu bar, choose **Configuration**.

2. Select **Two-Factor Authentication** from the navigation tree.

   The **Two-Factor Authentication** page is displayed.

3. Set **Two-Factor Authentication** to [ON].

4. Select the **Root Certificate** tab, click [...] next to **Certificate**, and select the root certificate to be uploaded.

5. Click **Upload**.

   If the certificate is uploaded successfully, **Imported successfully** will be displayed.

6. Select the **Client Certificate** tab, click [...] next to the user name, and select the client certificate to be uploaded.

7. Click **Upload**.

If the certificate is uploaded successfully, **Imported successfully** will be displayed.

Enabling Certificate Revocation Check

1. Set **Certificate Revocation Check** to .

Enabling Certificate Authentication for Accessing the iBMC

☐ NOTE

After uploading certificates, perform the following operations to enable certificate authentication for users who attempt to log in to the iBMC WebUI.

1. On the client, open your browser, for example, Google Chrome.

2. Click at the upper right corner and select **Settings**.

3. On the **Settings** window, click **Manage certificates** under **HTTPS/SSL**.

4. Import the client certificate.

5. Enter the iBMC login address in the address box of the browser.

6. Select the client certificate as instructed.

   Login to the iBMC WebUI is successful.

Deleting a Root Certificate

1. On the **Root Certificate** tab page, click next to the root certificate to be deleted.

   A confirmation dialog box is displayed.

2. Click **Yes**.

Deleting a Client Certificate

1. On the **Client Certificate** page, click next to the user whose client certificate is to be deleted.

   A confirmation dialog box is displayed.

2. Click **Yes**.

Viewing Root Certificate Details

1. On the **Root Certificate** tab page, click before the certificate.

   Detailed information about the certificate is displayed.

3.7.4 Security

Function Description

The **Security** page allows you to view and configure user security hardening rules for iBMC.

GUI

Choose **Configuration** from the main menu, and select **Security** from the navigation tree.

The **Security** page is displayed.

Figure 3-26 Security page

Parameter Description

Table 3-51 Password parameters

Parameter	Description

Password Complexity Check	Password complexity check verifies whether the passwords meet complexity requirements. It is enabled by default.
	
	Password complexity check applies to local user passwords, trap community names, SNMPv1/v2c community names, SNMPv3 encryption passwords, and VNC passwords. The password requirements include the following:
	
	● **Local user password requirements**
	● **Trap community name requirements**
	● **SNMPv1/v2c read-only community name requirements**
	● **SNMPv1/v2c read/write community name requirements**
	● **SNMPv3 encryption password requirements**
	● **VNC password requirements**
	
	NOTICE
	  ● For security purposes, enable password complexity check.
	  ● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)

SSH Password Authentication	SSH password authentication allows users to log in to the iBMC over SSH by using the password or public key. Value: ● **Disable**: allows users to log in over SSH by using only public keys. ● **Enable**: allows users to log in over SSH by using passwords or public keys. It is enabled by default.
Password Validity (Days)	Validity period (in days) of a user password. Value range: 0 to 365 The value **0** indicates that the password never expires. Default value: 0 **NOTE** For security purposes, set a proper password validity period and change the password periodically.

Parameter	Description
Minimum Password Age (Days)	Minimum time (in days) for which the password must be used. The password cannot be changed during this period.
	Value range: 0 to 365
	The value **0** indicates that the passwords do not have a minimum password age.
	Default value: 0
	NOTE
	The minimum password age must be at least ten days earlier than the password expiration day.
	● If **Password Expiration (Days)** is **10** or less, **Minimum Password Age (Days)** can only be **0**.
	● If **Minimum Password Age (Days)** is **355** or more, **Password Expiration (Days)** can only be **0**.
Inactive Timelimit (Days)	Maximum idle period (in days) after which the user account will be disabled.
	Value:
	● 0
	● 30 to 365
	The value **0** indicates unlimited time, that is, idle user accounts will never be disabled.
	Default value: 0
Emergency Login User	User name for logging in to the iBMC in emergencies.
	This user is not restricted by any login rules or login interfaces, and the password of this user will never expire.
	NOTE
	Only an administrator can be set as the emergency login user.
Previous Passwords Disallowed	Number of previous passwords that cannot be reused as a new password.
	Value range: 0 to 5
	The value **0** indicates that all previous passwords are allowed.
	Default value: 0

Parameter	Description
User Lockout Policy	Maximum number of consecutive invalid login attempts allowed and the account locking duration. ● The maximum number of consecutive invalid login attempts allowed is an integer ranging from 1 to 5 or **Unlimited** (account locking disabled), and the default value is 5. ● The account locking duration (in minutes) is an integer ranging from 1 to 5, and the default value is 5. After a user account is locked, the user can attempt to log in only after the account locking duration expires. **NOTE** ● For security purposes, enable the account lock function. ● To unlock a user account in emergencies, run the **unlock** command on the CLI. For details, see the *iBMC User Guide* of the server.

Table 3-52 Parameters in the **Login Rules** area

Parameter	Description
Time	**NOTICE** ● The start and end years cannot be later than 2050. ● The start and end time for a login rule must be in the same format. Time period in which users are allowed to log in. The value can be in one of the following formats: ● *YYYY-MM-DD*: Example value: **2013-08-30** to **2013-12-30** ● *HH:MM*: Example value: **08:30** to **20:30** ● *YYYY-MM-DD HH:MM*: Example value: **2013-08-30 08:30** to **2013-12-30 20:30**
IP	IP address or IP address range allowed for login. The value can be in one of the following formats: ● IPv4 (*xxx.xxx.xxx.xxx*) address: indicates an IP address. ● IPv4/subnet mask (*xxx.xxx.xxx.xxx*/*mask*): indicates an IP address segment.
MAC	MAC address or MAC address range allowed for login. The value can be in one of the following formats: ● *xx:xx:xx:xx:xx:xx*: indicates a MAC address. ● *xx:xx:xx*: indicates a MAC address segment.

Table 3-53 Parameters in the login security banner settings area

Parameter	Description
Login Security Banner	Login security banner, which can be enabled or disabled. ● ON : enables the login security banner. The security banner will be displayed on the login page. ● OFF : disables the login security banner.
Security Banner	Security banner text to be displayed on the login page. Value: a string of up to 1600 characters.

Procedure

Configuring Password Rules

1. On the menu bar, choose **Configuration**.
2. In the navigation tree, choose **Security**.

   The **Security** page is displayed.
3. Set parameters as required. For details about the parameters, see **Table 3-51**.
4. Click **Save**.

   A confirmation dialog box is displayed.
5. Click **Yes**.

Configuring Login Rules

The iBMC supports up to three login rules. Users who comply with any one of the three rules can log in to the iBMC.

A login rule is effective for local users, LDAP groups, SNMPv3 services or interfaces of CLP (ssh), KVM_VMM, RMCP, and Redfish interfaces only when it meets the following two conditions:

● The login rule is configured and enabled in the **Login Rules** area.

● The login rule is selected in the configuration area.

   📖 **NOTE**

   Each login rule contains three conditions: login duration, source IP address segment, and source MAC address segment. When setting a login rule, you do not need to specify all of the three conditions.

1. In the **Login Rules** area, set login rules.

   For details about the parameters, see **Table 3-52**.
2. Set the login rules to ON .
3. Click **Save**.

   A confirmation dialog box is displayed.
4. Click **Yes**.

Setting the Login Security Banner

1. In the **Login Security Banner** area, set **Security Banner** to ⬤ **ON** .

2. Enter a message in the **Security Banner Text** box.

3. Click **Save**.

   A confirmation dialog box is displayed.

4. Click **Yes**.

Restoring the Default Login Security Message

1. In the **Login Security Banner** area, set **Security Banner** to ⬤ **ON** .

2. Click **Restore Defaults**.

3. Click **Save**.

   A confirmation dialog box is displayed.

4. Click **Yes**.

3.7.5 Network

Function Description

The **Network** page allows you to perform the following operations:

- Set a host name for the server.
- Set the mode and IP address of the management network port for the server.

> **NOTICE**
>
> Changing the IP address of the management network port will cause network disconnection. Change the IP address only when necessary.

- Set the mode for obtaining domain name system (DNS) information.

  > **NOTE**
  >
  > DNS supports both IPv4 and IPv6 addresses.
  >
  > When the RH8100 V3 or 8100 V5 server is in single-system mode, the LAN on motherboard (LOM) on HFC-1 cannot provide the Network Controller Sideband Interface (NC-SI) function. Therefore, the network ports on the LOM of HFC-1 are not displayed in the **LOM** area.

- Set VLANs.
- Set NTP information.
- Set the time zone.

  > **NOTE**
  >
  > When the server is powered off and then powered on or is loading a driver, the network port is reconnected due to the power-saving feature of the X540 or BCM5719 NIC. In this scenario, the NC-SI function is temporarily unavailable.

GUI

Choose **Configuration** from the main menu, and select **Network** from the navigation tree.

The **Network** page is displayed.

Figure 3-27 Network page of the RH8100 V3

Figure 3-28 Network page of other rack servers

Parameter Description

Table 3-54 Parameters on the **Network** page

Parameter	Description
Host Name	iBMC host name. Value: a string of 1 to 64 characters The value can contain letters, digits, and hyphens (-), but cannot start or end with a hyphen. Default value: huawei

Parameter	Description

Mode	Type of the server management network port, that is, the iBMC network port.
	
	Value:
	
	• **Fixed**: Uses a dedicated network port, LOM port, LOM2, or PCIe expansion port as the iBMC port.
	
	   – **Dedicated Port**: dedicated iBMC port (that is, the Mgmt port of the server).
	
	   – **LOM**: a service network port on an LOM.
	     NOTE
	       • For V3 servers, **LOM** indicates a flexible NIC, and **LOM2** does not exist.
	       • For V5 servers, **LOM** indicates a NIC integrated on the mainboard, and **LOM2** indicates a flexible NIC.
	
	   – **LOM2**: a port on a flexible NIC (that is, the flexible NIC of V5 servers).
	
	   – **PCIe port** (not for RH8100 V3, 8100V5, RH5885 V3, RH5885H V3, 2488 V5, and 2488H V5 servers): a port on a PCIe card (that is, a PCIe card that supports NC-SI and is connected with an NC-SI cable).
	
	• **Automatic**: If you select this option, the iBMC automatically selects the iBMC port based on port status. You also need to select the ports involved in the auto-selection. If multiple ports are available, the iBMC selects a port based on the following priority:
	
	dedicated port > LOM port > LOM2 > external PCIe port (not for RH8100 V3, 8100V5, RH5885 V3, RH5885H V3, 2488 V5, and 2488H V5 servers)
	
	The iBMC automatically selects the iBMC port based on the following priority.
	
	   – V3 servers
	
	   Dedicated port > LOM port (port 1 to 2 or port 1 to 4) > PCIe port (port 1 to 2 or port 1 to 4)
	
	   – V5 servers
	
	   Dedicated port > LOM port (port 1 to 2 or port 1 to 4) > PCIe port (port 1 to 2 or port 1 to 4) or
	
	   Dedicated port > LOM port (port 1 to 2 or port 1 to 4) > LOM2 port (port 1 to 2 or port 1 to 4
	
	   The LOM2 ports and PCIe ports are mutually exclusive. If the PCIe NIC is connected to an NC-SI cable, the PCIe NIC ports can be used to access the iBMC, but the LOM2 ports cannot. If the PCIe NIC is not connected to an NC-SI cable, the LOM2 ports can be used to access the iBMC, but the PCIe NIC ports cannot.

Parameter	Description
	NOTE ● If a network port on a PCIe card is selected as the iBMC network port, only the PCIe card connected with NC-SI cables can be used. ● If an LOM port or flexible NIC port is set as the iBMC port, the LOM or the flexible NIC must support NC-SI. ● If an LOM port, LOM2 port, or a PCIe port is selected manually or automatically, the same physical port serves as a management port and a service network port. For security purposes, configure VLAN for the management port if the **Fixed** or **Automatic** mode involves the LOM, LOM2, or PCIe ports. ● If a network port is selected as the iBMC management network port, ✓ will display behind the network port. Default value: **Fixed**
iBMC Management Network Port	If **Mode** is set to **Fixed**, specify a management network port. If **Mode** is set to **Automatic**, select the network ports for auto-negotiation.
IP Version	IP versions that can be enabled: ● IPv4 ● IPv6 ● IPv4/IPv6 Default value: **IPv4/IPv6**
IPv4	
Automatically obtain IP address	Click this option to allow an IPv4 address to be automatically allocated for the iBMC network port.
Manually set IP address	Click this option to manually set an IPv4 address for the iBMC network port. The IPv4 address information includes **IP Address**, **Subnet Mask**, **Gateway**, and **MAC Address**. NOTE **MAC Address** specifies the physical address of a network interface card (NIC).
IPv6	
Automatically obtain IP address	Click this option to allow an IPv6 address to be automatically allocated for the iBMC network port.
Manually set IP address	Click this option to manually set an IPv6 address for the iBMC network port. The IPv6 address information includes **IP Address**, **IPv6 Prefix**, **Gateway**, **Local Link** and **IP Address2**. NOTE ● **Local Link** is used for local link communication. ● **IP Address2** supports a maximum of fifteen IPv6 addresses when stateless address autoconfiguration (SLAAC) is used.

Parameter	Description
DNS	
Automatically obtain DNS IPv4 address	Click this option to allow an IPv4 address to be allocated for the DNS server.
Automatically obtain DNS IPv6 address	Click this option to allow an IPv6 address to be allocated for the DNS server.
Manually set DNS address	Click this option to manually set the DNS information. The DNS address information includes **Domain**, **Preferred Server**, and **Alternate Server**. **NOTICE** If the IP address of the iBMC network port is set manually, the DNS information must also be set manually.
Domain	Domain name for the server. Value: a string of 0 to 67 characters The value can contain letters, digits, and special characters including spaces.
Preferred Server	IP address of the preferred DNS server. Value: an IPv4 or IPv6 address or leave it empty.
Alternate Server	IP address of the alternate DNS server. Value: an IPv4 or IPv6 address or leave it empty.
NTP	
NTP	NTP allows the server to synchronize time with the NTP server. Click ⬭OFF or ⬭ON, and click **Save**. Value: ● ⬭ON: enables NTP. ● ⬭OFF: disables NTP.
Automatically obtain NTP information using DHCPv4	Click this option to allow IPv4 address to be automatically allocated for the NTP server. **NOTE** If this option is selected, time zone information need not be manually configured.
Automatically obtain NTP information using DHCPv6	Click this option to allow IPv6 address to be automatically allocated for the NTP server.
Manually set NTP information	Click this option to manually set the preferred and alternate NTP servers.

Parameter	Description
Preferred NTP server	IP address of the preferred NTP server. Value: an IPv4 or IPv6 address or a domain name **NOTE** • The iBMC versions earlier than V312 support only the Linux NTP servers. • The iBMC supports Linux and Windows NTP servers from V312.
Alternate NTP server	IP address of the alternate NTP server. Value: an IPv4 or IPv6 address or a domain name **NOTE** • The iBMC versions earlier than V312 support only the Linux NTP servers. • The iBMC supports Linux and Windows NTP servers from V312.
Server Authentication	Authentication, which can be enabled or disabled, for communication between the server and the NTP server. Default value: Disabled
NTP Time Synchronization Interval	Interval at which the system synchronizes time from the NTP server. The system automatically adjusts the time synchronization interval based on the network status. If the network status is in good condition, the time synchronization interval is adjusted toward the maximum value.
Upload NTP Secure Group Key	Private key to be uploaded to the iBMC for identity authentication if **Server Authentication** is enabled. **NOTE** You can download a key generator (for example, ntp-keygen) to generate private keys.
VLAN	

Parameter	Description
VLAN	Setting of VLAN. Click (OFF) or (ON), and click **Save**. Value: ● (ON) indicates the VLAN is enabled. ● (OFF) indicates the VLAN is disabled. **NOTE** ● VLAN setting is not supported when a dedicated network port is used under the **Fixed** mode. ● You are advised to enable VLAN and set VLAN IDs to implement isolation between the service network and management network. ● If **Dedicated Port** is selected as the iBMC management network port, the VLAN configuration is invalid. If any other value except **Dedicated Port** is selected as the iBMC management network port, the VLAN configuration is valid. Default value: (OFF)
VLAN ID	VLAN to which the iBMC network port belongs.
VLAN	
VLAN	Setting of VLAN. Click (OFF) or (ON), and click **Save**. Value: ● (ON) indicates the VLAN is enabled. ● (OFF) indicates the VLAN is disabled. **NOTE** ● VLAN setting is not supported when a dedicated network port is used under the **Fixed** mode. ● You are advised to enable VLAN and set VLAN IDs to implement isolation between the service network and management network. ● If **Dedicated Port** is selected as the iBMC management network port, the VLAN configuration is invalid. If any other value except **Dedicated Port** is selected as the iBMC management network port, the VLAN configuration is valid. Default value: (OFF)
VLAN ID	VLAN to which the iBMC network port belongs.

Parameter	Description
Time Zone	Time zone for the iBMC. You can set the time zone in either of the following ways: ● Select **Others** from **Time Zone** and choose the time offset **GMT-**_hh:mm_ or **GMT+**_hh:mm_. The time offset ranges from **GMT-12:00** to **GMT+14:00**. ● Select the area name: _Global time zone name+City name_ **NOTE** ● The time zone information is automatically obtained if **Automatically obtain NTP information through DHCPv4** is selected. ● In the time zones that use daylight saving time (DST), the iBMC automatically adjusts the time one hour forward when the DST starts and adjusts the time backward to standard time when the DST ends. Default value: **Others**+**GMT**

Procedure

Setting a Host Name

1. On the **Network** page, set a host name for the server.

   For details about this parameter, see **Table 3-54**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

3. Click **Restart Now** to restart the iBMC immediately or click **Restart Later** to restart the iBMC later.

   NOTE

   Resetting the iBMC will automatically generate an SSL certificate.

Selecting the Management Network Port

1. On the **Network** page, select the type of the management network port and set the network port.

   For details about the parameters, see **Table 3-54**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting an IPv4 Address for the Management Network Port

1. In the **IPv4** area of the **Network** page, set IPv4 information for the management network port.

   For details about the parameters, see **Table 3-54**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting an IPv6 Address for the Management Network Port

1. In the **IPv6** area of the **Network** page, set IPv6 information for the management network port.

   For details about the parameters, see **Table 3-54**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Automatically Obtaining DNS Information

1. Click **Automatically obtain DNS IPv4 address** if the management network port uses an IPv4 address or click **Automatically obtain DNS IPv6 address** if the management network port uses an IPv6 address.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Manually Setting DNS Information

1. Click the **Manually set DNS address** option button.

2. Set **Domain**, **Preferred Server**, and **Alternate Server**. For details about the parameters, see **Table 3-54**.

3. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting a VLAN ID for the Management Network Port

> 📖 **NOTE**
>
> The specified VLAN ID takes effect only to the shared management network port.

1. In the **VLAN** area of the **Network** page, set a VLAN ID for the management network port. For details about the parameters, see **Table 3-54**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting NTP Information

1. In **NTP**, set parameters based on service requirements.

   For details about the parameters, see **Table 3-54**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting the Time Zone

1. In **Time zone**, select the time zone.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

   > 📖 **NOTE**
   >
   > When performing time synchronization on the OS, run the **hwclock --utc -w** command. This command can ensure consistency between the OS time and the iBMC time.

3.7.6 Services

Function Description

The **Services** page allows you to view and set system service information.

GUI

Choose **Configuration** from the main menu, and select **Services** from the navigation tree.

The **Services** page is displayed.
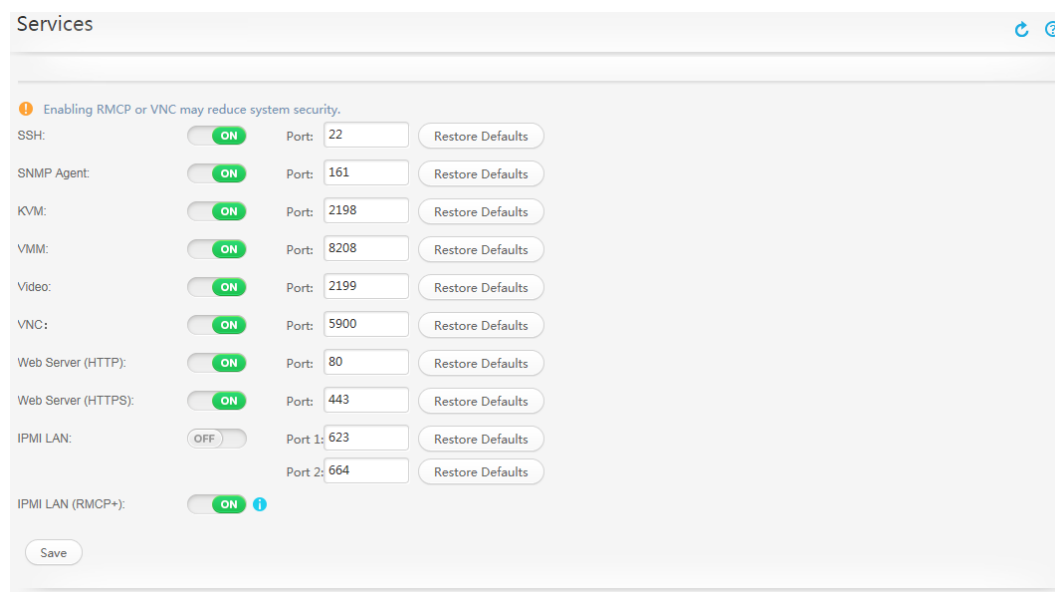
Parameter Description

Table 3-55 Parameters on the Port Settings page

Parameter	Description
Services	System services that can be enabled or disabled: ● **SSH**: allows a secure channel to be established between a local computer and the server. The iBMC supports a maximum of five concurrent SSH connections. **NOTE** SSH supports encryption algorithms **AES128-CTR**, **AES192-CTR**, and **AES256-CTR**. Use a supported encryption algorithm when logging in to iBMC over SSH. ● **SNMP Agent**: translates and transfers requests between management devices and managed devices. ● **KVM**: allows users to remotely control a server by using the local keyboard, video, and mouse (KVM). The iBMC supports a maximum of two concurrent users. ● **VMM**: allows a user to use a virtual DVD-ROM drive or floppy disk drive (FDD) to access and control a server. The iBMC supports only one user at a time. **NOTE** VMM stands for Virtual Media Manager. ● **Video**: allows users to use the video playback function. For details about this function, see **3.5.2 Playback**. The iBMC supports only one user at a time. ● **VNC**: allows users to remotely control a server by using the local keyboard, video, and mouse. (VNC stands for Virtual Network Console.) A maximum of five concurrent users are allowed. **NOTE** Only V5 servers support the VNC service. ● **Web Server (HTTP)**: supports Internet browsing and translates Hypertext Transfer Protocol (HTTP) pages. The Web Server (HTTP) service is enabled by default to establish a connection between the browser and iBMC. After the connection is set up, the secure protocol HTTPS is used. ● **Web Server (HTTPS)**: supports Internet browsing and translates Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) pages or Redfish Protocol. The iBMC supports a maximum of four concurrent HTTPS connections. ● **IPMI LAN (RMCP)**: stands for Intelligent Platform Management Interface (IPMI) over LAN, and supports the Remote Management Control Protocol (RMCP). Using the IPMI LAN (RMCP) service may pose security risks. For security purposes, use the IPMI LAN (RMCP+)

Parameter	Description
	service instead. The IPMI LAN (RMCP) service is disabled by default. ● **IPMI LAN (RMCP+)**: stands for Intelligent Platform Management Interface (IPMI) over LAN and supports RMCP+. **NOTE** The RMCP+ protocol has security vulnerabilities (CVE-2013-4786), and using RMCP+ poses security risks. Refer to **Risk Prevention Measures**. Click <kbd>OFF</kbd> or <kbd>ON</kbd>, and click **Save**. ● <kbd>ON</kbd>: enables the server. ● <kbd>OFF</kbd>: disables the server
Port	Port number used for a service. Value range: 1 to 65535 Default value: ● SSH: **22** ● SNMP Agent: **161** ● KVM: **2198** ● VMM: **8208** ● Video: **2199** ● VNC: **5900** ● Web Server (HTTP): **80** ● Web Server (HTTPS): **443** ● IPMI LAN (RMCP): **623** for port 1 (primary port) and **664** for port 2 (secondary port) ● IPMI LAN (RMCP+): RMCP+ and RMCP use the same port. **NOTE** ● If a Web Server (HTTP)/Web Server (HTTPS) port is configured as a non-default browser port, the Chrome or Firefox browser cannot use the port to establish a connection. To solve this problem, you need to configure the browser to allow connections to be set up over a non-default port. ● Disabling the SSH, HTTPS, RMCP, and RMCP+ services at the same time may result in network disconnection. If all the services are disabled, you can connect to the server through the serial port and enable the web service. ● Only V5 servers support the VNC service.

Procedure

Setting Port Numbers for System Services

1. On the menu bar, choose **Configuration**.
2. In the navigation tree on the left, choose **Services**.

   The **Services** page is displayed on the right.
3. Enable the required system services and set port numbers for these services.

   For details about the parameters, see **Table 3-55**.

   📖 **NOTE**

   To use the default port number for a service, click **Restore Defaults** next to the port.

Table 3-56 Setting service ports

Services	Operation
SSH	Enter a port number in the **Port** text box.
SNMP Agent	Enter a port number in the **Port** text box.
KVM	Enter a port number in the **Port** text box.
VMM	Enter a port number in the **Port** text box.
Video	Enter a port number in the **Port** text box.
VNC	Enter a port number in the **Port** text box.
Web Server (HTTP)	Enter a port number in the **Port** text box.
Web Server (HTTPS)	Enter a port number in the **Port** text box.
IPMI LAN (RMCP)	1. Enter a port number in the **Port 1** text box. 2. Enter a port number in the **Port 2** text box.
IPMI LAN (RMCP+)	RMCP+ and RMCP use the same port.

4. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Risk Prevention Measures

Do as follows to minimize the security risks caused by the vulnerability (CVE-2013-4786) of RMCP+:

● If you do not use IPMI protocol to access the iBMC:

   – Disable the IPMI service on this page.

      📖 **NOTE**

      After IPMI is disabled, other devices cannot use IPMI to access the iBMC. This setting affects the IPMI-based tools, such as IPMItool, InfoCollect, and eSight.

   – Enable password complexity check and set passwords complying with the password complexity requirements.

- If you need to use IPMI protocol to access the iBMC:
  - Set the network where the iBMC management network port is located as an independent LAN.
  - Enable password complexity check and set passwords complying with the password complexity requirements.

3.7.7 System

Function Description

The **System** page allows you to view and set:

- Simple Network Management Protocol (SNMP) information
- Transport Layer Security (TLS) versions
- User management function on the service side
- Web session timeout period and web session mode
- Device location
- CPU and memory alarm thresholds
- FusionPar
- RAID mode

GUI

Choose **Configuration** from the main menu, and select **System** from the navigation tree.

The **System** page is displayed.

Figure 3-29 System page of the 8100 V5

Figure 3-30 System page of the RH5885 V3

Figure 3-30 System page of the RH5885 V3

Figure 3-31 System page of other V3 rack servers

Figure 3-32 System page of V5 rack servers

Parameter Description

Table 3-57 Parameters on the **System** page

Parameter	Description
SNMP Version	
SNMPv1	The first official SNMP version, which is defined in Requests for Comments (RFC) 1157. Using SNMPv1 may pose security risks. For security purposes, use SNMPv3. **NOTE** If SNMPv1 is enabled, change the SNMP community name upon the first login, and change it periodically.
SNMPv2c	An enhanced version of SNMPv2. SNMPv2c is an experimental protocol defined in RFC 1901 and adopts a community-based management architecture. Using SNMPv2c may pose security risks. For security purposes, use SNMPv3. **NOTE** If the SNMPv2c service is enabled, change the SNMP community name upon the first login, and change it periodically.
Long Password	Long password function, which can be enabled or disabled. Enable this function to enforce a minimum of 16 characters for community names. Default value: OFF for V3 servers and ON for V5 servers. Click OFF or ON, and click **Save**. ● ON : enables the Long Password. ● OFF : disables the Long Password.

Parameter	Description

Read-Only Community	Read-only community name.
	
	Default value: **roAdmin12#$** for V3 servers and **roAdministrator@9000** for V5 servers.
	
	NOTE
	  This parameter is valid only when SNMPv1 or SNMPv2c is used.
	
	Value:
	
	● If password check is disabled, the community names must meet the following requirements:
	
	　– If the long password feature is enabled, the community name is a string of 16 to 32 characters without spaces.
	
	　– If the long password feature is disabled, the community name is a string of 1 to 32 characters without spaces.
	
	● If password check is enabled, the community names must meet the following requirements:
	
	　– Length:
	　　– If the long password feature is enabled, the community name is a string of 16 to 32 characters.
	　　– If the long password feature is disabled, the community name is a string of 8 to 32 characters without spaces.
	
	　– Contain at least one of the following special characters:
	　　`` `~!@#$%^&*()-_=+|[{}];:'",<.>/? ``
	
	　– Contain at least two types of the following characters:
	　　– Uppercase letters A to Z
	　　– Lowercase letters a to z
	　　– Digits 0 to 9
	
	　– Cannot contain spaces.
	
	● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)
	
	NOTE
	  Weak password check is not supported by V3 servers.

Confirm Read-Only Community	Read-only community name re-entered for confirmation.

Parameter	Description

Read/Write Community	Read-write community name.
	
	Default value: **rwAdmin12#$** for V3 servers and **rwAdministrator@9000** for V5 servers.
	
	NOTE
	  This parameter is valid only when SNMPv1 or SNMPv2c is used.
	
	Value:
	
	● If password check is disabled, the community names must meet the following requirements:
	
	  – If the long password feature is enabled, the community name is a string of 16 to 32 characters without spaces.
	
	  – If the long password feature is disabled, the community name is a string of 1 to 32 characters without spaces.
	
	● If password check is enabled, the community names must meet the following requirements:
	
	  – Length:
	
	    – If the long password feature is enabled, the community name is a string of 16 to 32 characters.
	
	    – If the long password feature is disabled, the community name is a string of 8 to 32 characters without spaces.
	
	  – Contain at least one of the following special characters:
	    `~!@#$%^&*()-_=+|[{}];:'",<.>/?
	
	  – Contain at least two types of the following characters:
	
	    – Uppercase letters A to Z
	
	    – Lowercase letters a to z
	
	    – Digits 0 to 9
	
	  – Cannot contain spaces.
	
	● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)
	
	NOTE
	  Weak password check is not supported by V3 servers.

Confirm Read/ Write Community	Read-write community name re-entered for confirmation.

Parameter	Description
Login Rules	Select the login rules applied to SNMPv1 and SNMPv2c users. The login rules are set on the **Configuration** > **Security** page. You can click Click here to ensure that log rules have been configured and enabled to view the login rules.
SNMPv3	The third official SNMP version, which enhances security and remote configuration capabilities on the basis of earlier versions. **NOTE** SNMPv3 is enabled by default and cannot be disabled.
SNMPv3 AuthProtocol	SNMPv3 authentication algorithm. Value: ● MD5 ● SHA1 Default value: **SHA1** **NOTE** ● This setting applies only to **SNMPv3** and **SNMPv3 Trap**. ● Using MD5 may pose security risks. SHA1 is recommended.
SNMPv3 PrivProtocol	SNMPv3 encryption algorithm. Value: ● DES ● AES Default value: **AES** **NOTE** ● This setting applies only to **SNMPv3** and **SNMPv3 Trap**. ● Using DES may pose security risks. AES is recommended.
SNMPv3 EngineID	Uniquely identifies the SNMP engine of the SNMP agent.
SNMPv3 AuthUser	An iBMC user who can access the iBMC using SNMPv3 after a successful authentication. **NOTE** ● This parameter is available only for V5 servers. ● You can select a local iBMC user. An iBMC user with the user management permission can set any local user for SNMPv3 authentication. An iBMC user without the user management permission can only set itself for SNMPv3 authentication.

Parameter	Description
SNMPv3 PrivPassword	Password for the SNMPv3 authentication. Default value: same as the user login password. **NOTE** This parameter is available only for V5 servers. Value: ● If password complexity check is disabled, the password cannot be empty or exceed 20 characters. ● If password complexity check is enabled, the password must meet the following requirements: – Contain 8 to 20 characters – Contain at least a space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – Contain at least two types of the following characters: – Uppercase letters A to Z – Lowercase letters a to z – Digits 0 to 9 – Cannot be the same as the user name or the user name in reverse order. – Have at least two new characters when compared with the previous password. ● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.) **NOTE** ● During the setting of the SNMP v3 encryption password, historical passwords and validity period are not checked. It is recommended that SNMPv3 encryption password and user password be set with different values. Setting these two passwords to the same value may pose security risks. ● A non-administrator user cannot manage other users.
Login Rules	Login rules applied to SNMPv3 users. The login rules configured and enabled for local users will apply to SNMPv3 users.

Table 3-58 Other parameters on the **System** page

Parameter	Description
TLS Versions	TLS protocol version used to ensure data security and integrity during communication between two applications. TLS can be enabled to ensure a secure connection between a web browser and a web server. **NOTE** ● JRE 1.8 uses TLS 1.2 by default. ● JRE 1.7 uses TLS 1.0 by default. If TLS 1.0 is disabled, the remote KVM cannot be used for JRE 1.7.
OS User Management	Function of user management on the service system. If this function is enabled, the service system can send user management commands, such as adding or deleting users, user roles, and passwords, to manage iBMC users. Default value: ON For security purposes, set this parameter to OFF. Click OFF or ON, and click **Save**. ● ON indicates the service system can manage users. ● OFF indicates the service system cannot manage users.
Web Session	
Timeout Period (min)	Maximum idle period (in minutes) after which the user will be logged out of the iBMC WebUI. Value range: 5 to 480
Session Mode	Mode in which a user account can be used to log in to the iBMC WebUI. ● **Share**: Each user account can be used to log in to the iBMC WebUI from up to four clients at the same time. ● **Exclusive**: Each user account can be used to log in to the iBMC WebUI from one client at any given time.
Device Location	
Device Location	Location information of the server. Value: a string of 0 to 64 characters, which can contain digits, letters, and following special characters: `` `~!@#$%^&*()-_=+|[{}];:'",<.>/? `` The value is left blank by default.
Alarm Thresholds	

Parameter	Description
CPU Usage (%)	Alarm threshold for CPU usage (in percentage). If the CPU usage exceeds the alarm threshold, the iBMC reports a normal event. Value range: 0 to 100 **NOTE** If CPU usage alarm threshold is not displayed, install and run iBMA 2.0.
Memory Usage (%)	Alarm threshold for memory usage (in percentage). If the memory usage exceeds the alarm threshold, the iBMC reports a normal event. Value range: 0 to 100 **NOTE** If memory usage alarm threshold is not displayed, install and run iBMA 2.0.
Network Port Bandwidth Usage (%)	Alarm threshold for the network port bandwidth usage. If the network port bandwidth usage exceeds the alarm threshold, the iBMC reports a normal event. Value range: 0 to 100 **NOTE** If network port bandwidth usage alarm threshold is not displayed, install and run iBMA 2.0.
Hard Disk Partition Usage (%)	Alarm threshold for the hard disk partition usage. If the hard disk partition usage exceeds the alarm threshold, the iBMC reports a normal event. Value range: 0 to 100 **NOTE** If hard disk partition usage alarm threshold is not displayed, install and run iBMA 2.0.

Parameter	Description
FusionPar (RH8100 V3 and 8100 V5 only)	The server can be configured to work as a single system or two independent systems. Value: ● Single-system mode ● Dual-system mode In dual-system mode, you cannot create disk partitions using the iBMC of system B. When the RH8100 V3 switches from the dual-system mode to the single-system mode, the management network port in system B will not have an IP address and the password of the **root** user will be restored to the default password (provided on the product nameplate). When the RH8100 V3 switches from the single-system mode to the dual-system mode, the IP address of the management network port in system B is restored to **192.168.2.101**. **NOTE** ● If the server is in single-system mode and the OS is started, switching from the single-system mode to the dual-system mode will fail. ● If the server is in dual-system mode and the OS of system A or B is started, switching from the dual-system mode to the single-system mode will fail.
RAID Mode (RH8100 V3 and 8100 V5 only)	The RAID can be configured as single RAID or dual-RAID. Value: ● Single RAID 　Select **Single RAID** only when slot 1 has a compute module. ● Dual RAID 　Select **Dual RAID** only when the server has two RAID controller cards and the compute modules are installed in slots 1 and 5. **NOTE** ● The **RAID Mode** function is not supported if the server is configured with front I/O module B or C. ● If front I/O module A is configured for the server working in single-system mode, **RAID Mode** can be **Single RAID** or **Dual RAID**. ● If front I/O module A is configured for the server working in dual-system mode, you can only switch the RAID mode from single-RAID to dual-RAID using system A of the iBMC. You cannot set the RAID mode using iBMC of system B. ● Before switching between the two RAID modes, ensure that the OS is started.

Procedure

Configuring the SNMP Settings

1. On the **System** page, set the SNMP parameters.

   For details about the parameters, see **Table 3-57**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting the TLS Version

1. In the **TLS Versions** area on the **System** page, select the TLS versions.

2. Click **Save**.

   📖 **NOTE**

   After modifying this setting, restart the iBMC for the changes to take effect.

Enabling the Service System to Manage iBMC Users

1. In the **OS User Management** area, set **User Management** to [ON].

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting the Timeout Period and Session Mode for the Web Server

1. In the **Web Session** page, set **Timeout Period (min)** and **Session Mode**. For details about this parameter, see **Table 3-58**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting the Device Location

1. In the **Device Location** area, enter the server location information in **Device Location**.

   For details about this parameter, see **Table 3-58**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting Alarm Thresholds

1. In the **Alarm Thresholds** area, set alarm thresholds for CPU and memory usage.

   For details about the parameters, see **Table 3-58**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting Hard Partitioning (RH8100 V3 and 8100 V5 only)

1. In the **FusionPar** area, set hard partitioning information for the server.

   For details about this parameter, see **Table 3-58**.

2. Click **Save**.

   The following information is displayed:

Before switching between the single-system mode and the dual-system mode, ensure that all service systems have been properly powered off and iBMC is not being upgraded. Are you sure to perform the switching?

If the switching is successful, the iBMC will restart. After switching is complete, the user name, password, and IP address of the standby iBMC are restored to factory settings.

3. Click **Save**.

The hard partitioning settings take effect after the iBMC restarts.

Setting the RAID Mode (RH8100 V3 and 8100 V5 only)

1. On the **System** page, set the RAID mode.

   For details about this parameter, see **Table 3-58**.

2. Click **Save**.

   The following information is displayed:

   Before switching between the single-RAID mode and the dual-RAID mode, ensure that all service systems have been properly powered on. Otherwise, the switching fails. A misoperation of switching the RAID mode will cause data loss. Remove the hard disks before switching, or switch the RAID mode after the service system have been powered on and before the operating system has started.

3. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

3.7.8 Boot Device

Function Description

The **Boot Device** page allows you to set the first boot device for the OS on the server.

GUI

Choose **Configuration** from the main menu, and select **Boot Device** from the navigation tree.

The **Boot Device** page is displayed.
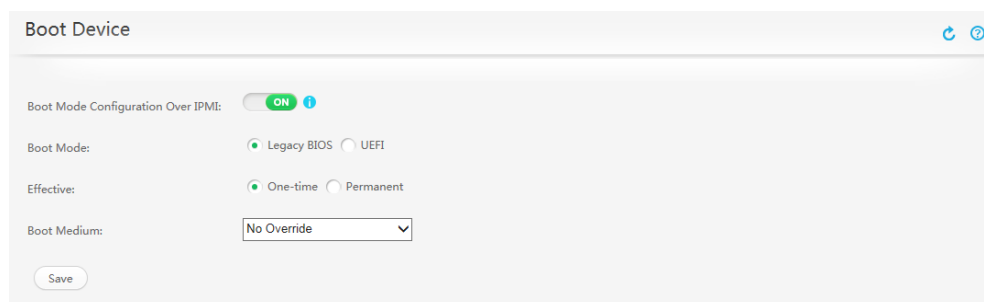
Parameter Description

Table 3-59 Parameters on the **Boot Device** page

Parameter	Description
Boot Mode Configuration Over IPMI	You can click OFF or ON to set the status. ● ON : The BIOS boot mode can be set through the IPMI interface. ● OFF : The BIOS boot mode cannot be set through the IPMI interface. **NOTE** ● Only V5 servers support this setting. ● Common users are not authorized to perform this setting.
Boot Mode	● **Legacy BIOS**: The OS starts from the BIOS. ● **UEFI**: The OS starts from the Unified Extensible Firmware Interface (UEFI). **NOTE** The **Boot Mode** parameter is only available for V5 servers.
Effective	● **One-time**: The boot device is only used for booting the next time the server is restarted. ● **Permanent**: The boot option setting takes effect permanently.
Boot Medium	**Hard Drive**: Click this option to boot the OS from the hard drive.
	DVD-ROM: Click this option to boot the OS from the CD-ROM or DVD-ROM drive.
	FDD/Removable Device: Click this option to boot the OS from a virtual floppy disk drive (FDD) or removable device.
	PXE: Click this option to boot the OS from the Preboot Execution Environment (PXE).
	BIOS Setup: Click this option to display the BIOS Setup menu upon server startup.
	No Override: Click this option to boot the OS from the default first boot device specified on the BIOS.

Procedure

1. On the menu bar, choose **Configuration**.
2. In the navigation tree, choose **Boot Device**.

   The **Boot Device** page is displayed.

3.   Set the first boot option. For details about the options, see **Table 3-59**.

4.   Click **Save**.

If the message "Save Success" is displayed, the setting is successful.

3.7.9 SSL Certificate

Function Description

The **SSL Certificate** page allows you to perform the following operation:

- View Secure Sockets Layer (SSL) certificate information, which includes information about the root certificates, intermediate certificates, and server certificates.

- Customize SSL information.

- Import new certificates.

The SSL certificate sets up an SSL security channel over HTTPS between the web browser on the client and the web server to transmit encrypted data between the client and server and prevent data disclosure. SSL ensures the security of transmitted information and is used for verifying the authenticity of the website to be accessed. Servers allow you to replace SSL certificates. For security purposes, replace the original certificate and keys with your customized certificate and public and private key pair, and promptly update the certificate.

📖 **NOTE**

- The SSL certificate can be a single SSL certificate or certificate chain that is less than 10 levels.

- MD5 poses security risks. From V360, the iBMC does not support import of certificates that use MD5.

GUI

Choose **Configuration** from the main menu, and select **SSL Certificate** from the navigation tree.

The **SSL Certificate** page is displayed.

Parameter Description

Table 3-60 Parameters in the **SSL Certificate Information** area

Parameter	Description
Issued To	Information about the user of an SSL certificate, including: ● **CN**: user name. NOTE Set **CN** to the server fully qualified domain name (FQDN), that is, *Host name.Domain name*. ● **OU**: department of the user. ● **O**: company or organization of the user. ● **L**: city of the user. ● **S**: province or state of the user. ● **C**: country of the user.

Parameter	Description
Issued By	Information about the issuer of an SSL certificate. The fields contained in **Issued By** are the same as those in **Issued To**.
Valid From	Date when the SSL certificate starts to take effect.
Valid To	Date when the SSL certificate will expire.
Serial Number	Serial number of the SSL certificate, which is used for identifying and migrating the certificate.

Procedure

Viewing Information About the Current SSL Certificate

1. In the navigation tree, choose **Configuration** > **SSL Certificate**.

   The **SSL Certificate** page is displayed.

2. In the **SSL Certificate Information** area, view information about the current SSL certificate used by the server.

Customizing SSL Certificate Information and Importing an SSL Certificate

📖 **NOTE**

   Perform this operation when you want to apply for an SSL certificate.

1. On the **SSL Certificate** page, click **Customize**.

   The page for customizing SSL certificate information is displayed.

2. In the **1. Generate CSR** area, set the parameters for customizing certificate information, and click **Save**.

   In the displayed dialog box, export the CSR file to the local PC as prompted.

   Table 3-61 describes the parameters for customizing certificate information.

Table 3-61 Parameters for customizing certificate information

Parameter	Description
Country (C)	Country of the user. This parameter is mandatory. The value can contain only two letters.
State (S)	State or province of the user. The value can contain a maximum of 128 characters, including letters, digits, hyphens (-), underscores (_), periods (.), and spaces.

Parameter	Description
City/Location (L)	City of the user.
	The value can contain a maximum of 128 characters, including letters, digits, hyphens (-), underscores (_), periods (.), and spaces.
Organization Name (O)	Company of the user.
	The value can contain a maximum of 64 characters, including letters, digits, hyphens (-), underscores (_), periods (.), and spaces.
Organizational Unit (OU)	Department of the user.
	The value can contain a maximum of 64 characters, including letters, digits, hyphens (-), underscores (_), periods (.), and spaces.
Common Name (CN)	Name of the user.
	This parameter is mandatory. The value can contain a maximum of 64 characters, including letters, digits, hyphens (-), underscores (_), periods (.), and spaces.

3. Send the exported CSR file to the SSL certificate issuer to apply for an SSL certificate.

   After obtaining the official SSL certificate, save it to the local PC.

4. In the **Import Server Certificate** area, click **Browse**, select the SSL certificate file, and click **Import**.

   The certificate is successfully uploaded to the server if the following information is displayed:

   Certificate imported successfully. The new certificate takes effect after the iBMC is restarted.

   Click **Restart Now** to restart the iBMC immediately or click **Restart Later** to restart the iBMC later.

   ☐ NOTE

   - The certificate file to be imported must be in *.crt, *.cer, or *.pem format and cannot exceed 1 MB.
   - A CSR file correlates with the server certificate applied from the CA organization. Do not generate a new CSR file before importing the server certificate. Otherwise, the original CSR file is overwritten by the new CSR file and cannot be recovered. You have to use the new CSR file to apply for a new server certificate from the CA organization.

Importing an 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 SSL certificate.

1. On the **SSL Certificate** page, click **Customize**.

   The page for customizing SSL certificate information is displayed.

2. In the **Import Custom Certificate (Optional)** area, import an SSL certificate.

    a. Click **Browse** next to **Certificate**, and select the SSL certificate file to be imported.

       The certificate must be in the format of .pfx and .p12 and cannot exceed 100 KB in size.

    b. In the **Certificate Password** text box, enter a password to ensure certificate security during transmission.

       If the certificate is protected by a password, you must enter the password. Otherwise, the certificate cannot be uploaded.

    c. Click **Import**.

       ◫ 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.

       The certificate is successfully uploaded to the server if the following information is displayed:

       Certificate imported successfully. The new certificate takes effect after the iBMC is restarted.

       Click **Restart Now** to restart the iBMC immediately or click **Restart Later** to restart the iBMC later.

Adding the Root Certificate to the Browser

◫ NOTE

If the SSL certificate is self-generated (not obtained from a CA organization), check whether the browser has the root certificate.

The following uses Internet Explorer as an example to describe how to view and add a root certificate in the browser.

1. Open Internet Explorer.

2. On the toolbar, choose **Tools** > **Internet Options**.

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

3. On the **Content** tab page, click **Certificates**.

   The **Certificates** dialog box is displayed.

4. On the **Trusted Root Certification Authorities** tab page, check whether the SSL certificate issuer is listed.

   – If yes, go to **5**.

   – If no, go to **6**.

5. Check whether the SSL certificate has expired.

   – If yes, go to **6**.

   – If no, go to **7**.

6. On the **Trusted Root Certification Authorities** tab page, click **Import**.

   Import the root certificate as prompted.

7. Open Internet Explorer again, and check whether the 🔒 icon is displayed on the address bar.

   – If yes, no further action is required.

   – If no, contact technical support.

3.7.10 Import/Export

Function Description

On the **Import/Export** page, you can import and export iBMC, BIOS, and RAID controller card configuration files.

For details about the configuration file, see **9 Configuration File Description**.

> 📖 **NOTE**
>
> - If KVM is enabled, the KVM encryption settings cannot be imported. There is no such restriction on other features.
> - RAID controller card configurations take effect only after the system power-on self-test (POST) is complete.
> - If the configuration items imported involve change of the TLS version or network configuration, the established web connections will be disconnected. If "Import failed" is displayed, log in to the iBMC WebUI again and check the operation log to determine whether the import is successful.
> - In the exported configuration file, the passwords are encrypted by default. The passwords do not take effect when the configuration file is imported to another server. If you need to import the password information to another server, change the passwords in the configuration file to plaintext and delete the comment tags in the password lines before importing the file.
> - In the configuration file exported, the iBMC management network port IP address is commented out.
> - The iBMC configuration, BIOS configuration, and some RAID controller configuration can be imported and exported.

Only the administrator can information and export configuration files.

GUI

Choose **Configuration** from the menu, and select **Import/Export** from the navigation tree.
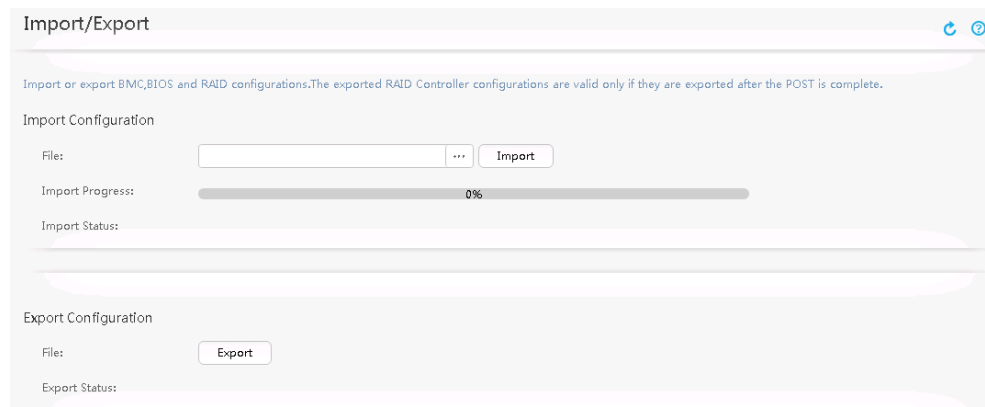
Procedure

Importing a Configuration File

In the configuration file exported through the iBMC WebUI, the password information is in ciphertext by default.

- If you want to import the configuration file to the same server, you do not need to reconfigure the passwords.
- If you want to import the configuration file to another server, change the passwords in plaintext and delete the comment tags in the password lines before importing the file.

1. (Optional) Configure the password in the configuration file to be imported.

   a. Use a text editor to open the configuration file to be imported, and locate the user name.

   b. Add the use password.

   For example, locate the user name **mytest**, as shown in **Figure 3-33**, and change ****** in **PassWord** to **Info@9000**.

   Figure 3-33 Configuration file before editing

   c. Delete the **<!--** and **-->** comment tags before and after the **PassWord**, **IsUserEnable**, and **IsUserLocked** parameters.

   Figure 3-34 shows the configuration file after editing.

   Figure 3-34 Configuration file after editing

   d. Save and close the configuration file.

2. In the **Import Configuration** area, click [...] next to **File** and select the configuration file to be imported.

3. Click **Import**.

   The configuration is successfully imported if "File imported successfully. The configuration will take effect after iBMC is restarted." is displayed.

4. The configuration file is successfully uploaded to the server if the following information is displayed:

File imported successfully. The configuration will take effect after iBMC is restarted.

Click **Restart Now** to restart the iBMC immediately or click **Restart Later** to restart the iBMC later.

📖 **NOTE**

- After importing the BIOS configuration, you need to restart the OS for the configuration to take effect.
- Of the RAID controller configuration, only the configuration of **Copyback State**, **Copyback on SMART error State**, and **JBOD State** can be imported. The configuration of the logical and physical drives cannot be imported.

Exporting Configuration Files

1. Click **Export** in the **Export Configuration** area, specify the directory for saving the file to be exported, and click **OK**.

   The configuration is successfully exported if "File exported successfully" is displayed.

3.8 System

3.8.1 Operation Logs

Function Description

The **Operation Logs** page allows you to view and download logs recorded during system operation, including information about system startup, status transition, and configuration performed by users on iBMC.

The iBMC provides 200 KB capacity for storing up to 2000 operation log records.

When the operation log reaches 200 KB, it will be automatically compressed. When a new compressed package is generated, the old compressed package will be automatically deleted.

📖 **NOTE**

Operation logs that record successful power-on, power-off, and reset operations indicate that the iBMC has successfully triggered the operations, but do not necessarily mean that these operations were successfully executed on the hardware.

GUI

On the menu bar, choose **System**. In the navigation tree, choose **Operation Logs**. The **Operation Logs** page is displayed.

Parameter Description

Table 3-62 Parameters on the **Operation Logs** page

Parameter	Description
ID	ID of an operation. The latest operation is listed first.
Time	Time when the operation was performed.
Interface	Interface over which the operation was performed.
User	User who performed the operation. The value of **User** is displayed as **N/A** (the user name is not displayed) in one of the following scenarios: ● The UID button or power button is pressed. ● The interface is SNMPv1 or SNMPv2c. ● The interface is IPMI and the IP address is **HOST** or **HMM**. (The log records an IPMI message sent from the service system.) ● For V3 servers, the iBMC IP address and the password of the **root** user were changed by using a jumper. For V5 servers, the iBMC IP address and the password of the **Administrator** were changed by using a jumper. ● A component was hot-swapped. NOTE 　From iBMC V350, the BMC default settings cannot be restored by using a jumper.

Parameter	Description
IP Address	IP address from which the operation was performed. - The value **HMM** indicates that the operation was triggered by the management module. - The value **HOST** indicates that the operation was triggered by the service system. - The value **127.0.0.1** indicates that the operation was triggered by the local host in one of the following scenarios: - The UID button, memory riser button, or power button is pressed. - The interface is the LCD or local serial port. - For V3 servers, the iBMC IP address and the password of the **root** user were changed by using a jumper. For V5 servers, the iBMC IP address and the password of the **Administrator** were changed by using a jumper. - A component was hot-swapped. **NOTE** From iBMC V350, the BMC default settings cannot be restored by using a jumper.
Details	Details about the operation. If the iBMC restarts after an upgrade was performed using the iBMC WebUI or CLI or over IPMI, the operation is logged in the following format: - Interface: N/A - User: N/A - IP address: 127.0.0.1 - Details: The iBMC was successfully reset due to an upgrade.
Note: If the values of **User** and **IP address** cannot be parsed, they are displayed as **unknown**.	

Procedure

Viewing Operation Logs

1. On the menu bar, choose **System**.

2. In the navigation tree, choose **Operation Logs**.

   The **Operation Logs** page is displayed.

Downloading Operation Logs

1. Click **Download Logs**.

   The **Save** dialog box is displayed.

2. Select a local directory for saving the downloaded operation log file.

3. Click **Save**.

The downloaded file is saved to the specified directory.

3.8.2 Run Logs

Function Description

The **Run Logs** page allows you to view the RAS logs.

iBMC provides 200 KB capacity for storing up to 2000 Run Log entries.

When the log reaches 200 KB, it will be automatically compressed. When a new compressed package is generated, the old compressed package will be automatically deleted.

GUI

Choose **System** from the main menu, and select **Run Logs** from the navigation tree.

The **Run Logs** page is displayed.

Parameter Description

Table 3-63 Parameters on the **Run Logs** page

Parameter	Description
Time	Time when the runtime error occurred.
Level	Severity of the alarm caused by the runtime error.
Details	Details about the runtime error.

Procedure

1. On the menu bar, choose **System**.
2. In the navigation tree, choose **Run Logs**.

   The **Run Logs** page is displayed.
3. View all run logs.

3.8.3 Security Logs

Function Description

The **Security Logs** page allows you to perform the following:

- View logs about iBMC login and logout over a serial port Secure Shell (SSH) and about setting operations.
- View logs about query and set operations performed over SNMP.
- Download security logs.

iBMC provides 200 KB capacity for storing up to 2000 security log entries.

When the log reaches 200 KB, it will be automatically compressed. When a new compressed package is generated, the old compressed package will be automatically deleted.

GUI

Choose **System** from the main menu, and select **Security Logs** from the navigation tree.

The **Security Logs** page is displayed.

ID	Time	Interface	Host	Details
553	2019-12-04 19:52:26	xinetd[1913]	huawei	EXIT: ssh pid=6033 duration=1021(sec)
552	2019-12-04 19:52:26	sshd[6033]	huawei	pam_unix(sshd:session): session closed for user Administrator
551	2019-12-04 19:52:26	sshd[6045]	huawei	Timeout, client not responding.
550	2019-12-04 19:35:27	sshd[6046]	huawei	error: open /dev/tty failed - could not set controlling tty: Permission denied
549	2019-12-04 19:35:27	sshd[6033]	huawei	pam_unix(sshd:session): session opened for user Administrator by (uid=0)
548	2019-12-04 19:35:27	sshd[6033]	huawei	Accepted password for Administrator from 172.234.5.161 port 64330 ssh2
547	2019-12-04 19:35:26	sshd[6033]	huawei	reprocess config line 47: Deprecated option RhostsRSAAuthentication
546	2019-12-04 19:35:26	sshd[6033]	huawei	reprocess config line 40: Deprecated option RSAAuthentication
545	2019-12-04 19:35:25	sshd[6033]	huawei	/etc/ssh/sshd_config line 47: Deprecated option RhostsRSAAuthentication
544	2019-12-04 19:35:25	sshd[6033]	huawei	/etc/ssh/sshd_config line 40: Deprecated option RSAAuthentication

Total Records: 553   < 1 2 3 4 5 ... 56 >   Go 1 ▶

Parameter Description

Table 3-64 Parameters on the **Security Logs** page

Parameter	Description
ID	Operation ID. The latest operation is listed first.
Time	Time when the operation was performed.
Interface	Interface over which the operation was performed.
Host	Host name of the iBMC.
Details	Details about the operation.

Procedure

Viewing Security Logs

1. On the **Security Logs** page, view logs about iBMC login and logout.

Downloading Security Logs

1. On the **Security Logs** page, click **Download Logs**.

   The **Save** dialog box is displayed.

2. Specify a directory for saving the downloaded file.

3. Click **Save**.

   The downloaded file is saved to the specified directory.

3.8.4 Work Records

Function Description

The **Work Records** page allows you to add and view work records. iBMC provides 200 KB capacity for storing up to 2000 Run Log entries.

> 📖 **NOTE**
>
> - A work record can contain a maximum of 255 characters. You can add a maximum of 20 work records. If the number of work records exceeds 20, new work records will overwrite the earliest ones.
>
> - Work records are visible to all users and editable by all users.

GUI

Choose **System** from the main menu, and select **Work Records** from the navigation tree.

The **Work Records** page is displayed.
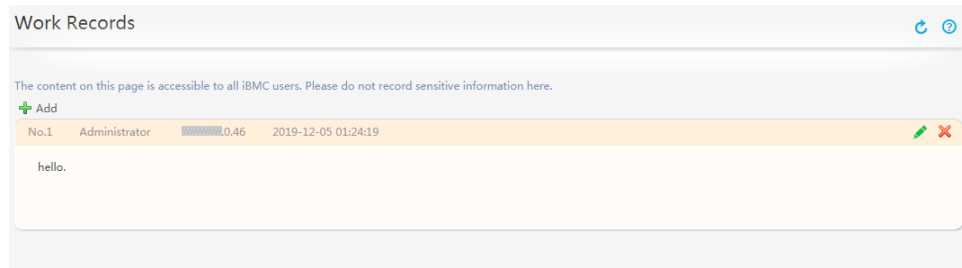
Procedure

Adding a Work Record

1. On the menu bar, choose **System**.
2. In the navigation tree, choose **Work Records**.
   The **Work Records** page is displayed.
3. Click **Add**, and add a work record in the displayed text box.
4. Click **Save**.

Modifying a Work Record

1. Click and modify the work record in the text box.
2. Click **Save**.

Deleting a Work Record

1. Click to delete the work record.
   The following information is displayed:
   Are you sure you want to perform this operation?
2. Click **Yes**.

3.8.5 Online Users

Function Description

The **Online Users** page allows you to perform the following operations:

- View the users who have logged in to the iBMC.
- Forcibly log out online users.

Only an administrator can forcibly log out users.

GUI

Choose **System** from the main menu, and select **Online Users** from the navigation tree.

The **Online Users** page is displayed.

Parameter Description

Table 3-65 Parameters on the **Online Users** page

Parameter	Description
User Name	Name of the user who has logged in to the iBMC or KVM.
Login Method	Mode for a user to log in. The options are as follows: ● **GUI**: A user has logged in to the iBMC over the WebUI. ● **CLI**: A user has logged in to the iBMC over the command-line interface (CLI). ● **KVM**: A user has logged in to the OS over the Remote Virtual Console. ● **Redfish**: A user has logged in to the iBMC over the Redfish interface. ● **VNC**: A user logs in to operating system (OS) over the Virtual Network Console. Only V5 servers support this login method.
IP Address	IP address for connecting to and logging in to the iBMC. Value: IP address or **COM** **NOTE** The value **COM** indicates that the user logs in to the iBMC over the serial port.
Login Time	Time when the user logged in to iBMC.
Operation	Forcibly logs out a user.

Procedure

Viewing Online Users

1. On the menu bar, choose **System**.

2. In the navigation tree, choose **Online Users**.

   The **Online Users** page is displayed.

3. On the **Online Users** page, view information about all users who have logged in to the iBMC.

Logging Out a User

1. On the **Online Users** page, click ✖ next to a user.

   A confirmation dialog box is displayed.

2. Click **OK**.

   The user is forcibly logged out, and information about the user is no longer displayed on the **Online Users** page.

3.8.6 Firmware Upgrade

Function Description

The **Firmware Upgrade** page allows you to perform the following operations:

- View firmware version information of the server.
- Restart the iBMC.
- Switch between the active and standby iBMC images.
- Upgrade the server firmware.

The iBMC has two images deployed in active/standby mode. Upgrade the standby image and then the active image. After the standby image is upgraded, the iBMC restarts and automatically switches to the standby image file. If an automatic switchover is not performed, manually switch over services to the standby image.

> **NOTICE**

- During the upgrade process, do not power off the server or restart the iBMC.
- After upgrading the iBMC firmware, restart the iBMC for the new version to take effect. However, you do not need to restart the server. Therefore, the services running on the server will not be affected.
- For the iBMC earlier than V312, if you need to upgrade the mainboard BIOS and component CPLDs, upgrade the CPLDs only after the BIOS upgrade takes effect. Otherwise, the BIOS upgrade may fail and the system may become abnormal.
- You do not need to restart the server after the LCD and PSU firmware is upgraded. However, you need to restart the server for the new versions to take effect after upgrading the following firmware:
  - BIOS firmware
  - Complex programmable logical device (CPLD) firmware of the mainboard
  - CPLD firmware of the CPU board (firmware exclusive to RH8100 V3 and 8100 V5)
  - CPLD firmware of the front I/O board (firmware exclusive to RH8100 V3 and 8100 V5)
  - CPLD firmware of the rear I/O board (firmware exclusive to RH8100 V3 and 8100 V5)
  - CPLD firmware of the hard disk backplane
  - CPLD firmware of the hot-swappable PCIe riser card

  Before upgrading the firmware, stop the services running on the server. This prevents service interruption when the server is restarted.
- To upgrade the CPLD firmware of the front I/O board in the dual-system mode, log in to the iBMC system B first, and then log in to the iBMC system A to upgrade the CPLD firmware of the rear I/O board.
- iBMC Version Requirements for Upgrading the current drive backplane's part number (P/N) is 03029JRX, 03029JRY, 03029JSA, check whether the iBMC version is V520 or later. If not, upgrade the iBMC version to V520 or later.
- If you need to upgrade the iBMC from a version earlier than an intermediate version to a version later than the intermediate version, upgrade the iBMC to the intermediate version and then to the target version. If the upgrade to the intermediate version fails, restart the iBMC and try again. **Table 3-66** lists the server models and their intermediate versions. For example, if the iBMC source version of an RH1288 V3 is earlier than V257 and the target version is later than V257, you need to upgrade the iBMC to V257 and then to the target version. If the upgrade to V257 fails, restart the iBMC and try again.

Table 3-66 iBMC intermediate versions and compute node models

Intermediate Version	Model
257	RH1288 V3/RH2288H V3/RH5288 V3
260	RH5885H V3

Intermediate Version	Model
262	RH2288 V3
270	RH5885 V3
276	RH8100 V3

The iBMC Help describes only how to upgrade firmware on the iBMC WebUI. For details about how to obtain the firmware upgrade packages and reference documents and verify the upgrade, see the upgrade guide delivered with the server you use.

Figure 3-35 shows the firmware upgrade process.

Figure 3-35 Firmware upgrade process

GUI
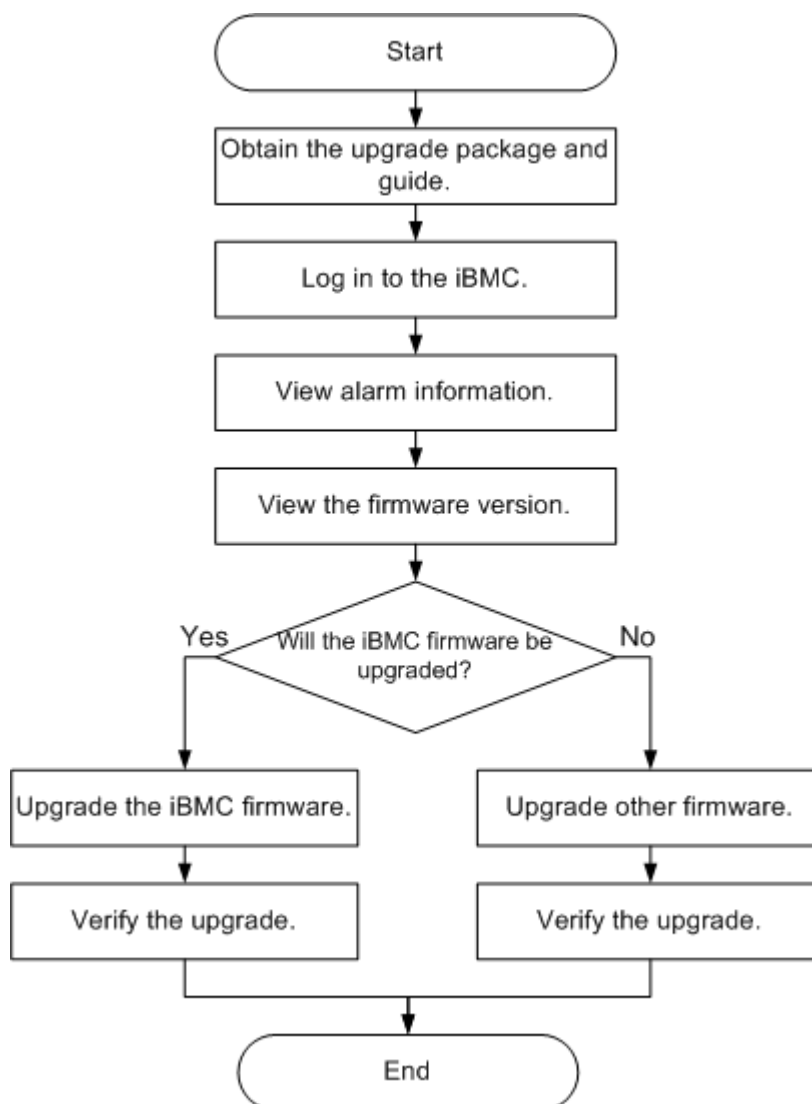
Choose **System** from the main menu, and select **Firmware Upgrade** from the navigation tree.

The **Firmware Upgrade** page is displayed.
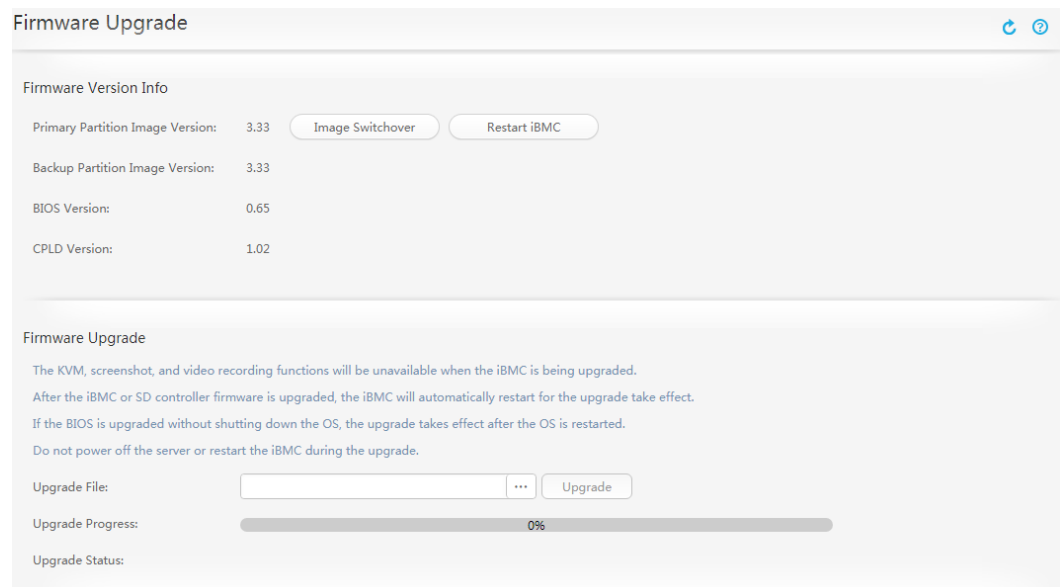
Parameter Description

Table 3-67 Parameters on the Firmware Upgrade page

Parameter	Description
Firmware Version Info	
Primary Partition Image Version	Version number of the iBMC firmware in the primary partition.
Backup Partition Image Version	Version number of the iBMC firmware in the backup partition.
BIOS Version	BIOS version number.
CPLD Version	CPLD firmware version.
Image Switchover	Switches between the iBMC images in the primary and backup partitions.
Restart iBMC	Restarts the iBMC for the upgrade to take effect.

Parameter	Description
Firmware Upgrade NOTE ● During the upgrade of the iBMC firmware of V3 servers, the KVM, screenshot, and video functions are not available. ● The iBMC will reboot to apply the firmware after upgrading the iBMC or SD card controller. ● If the BIOS is upgraded without shutting down the OS, the upgrade takes effect after the OS is restarted. ● Do not power off the server or restart iBMC during the upgrade. ● V5 servers do not support SD controllers.	
Upgrade File	Selects the local directory where the firmware upgrade package is stored. The firmware upgrade package to be uploaded must be an *.hpm file. Setting method: 1. Click [···]. Select the local directory where the firmware upgrade package is stored. Click **Open**. The **Firmware Upgrade** page is displayed. 2. Click **Upgrade**. The following information is displayed: Are you sure you want to perform this operation? 3. Click **Yes**. The iBMC starts the upgrade.
Upgrade Progress	Displays the firmware upgrade progress.
Upgrade Status	Displays the firmware upgrade status.

Procedure

Viewing Firmware Versions

1. On the menu bar, choose **System**.
2. In the navigation tree, choose **Firmware Upgrade**.

   The **Firmware Upgrade** page is displayed.
3. View the iBMC, BIOS, and CPLD versions.

Upgrading iBMC firmware.

1. On **Firmware Upgrade**, select the upgrade package from **Upgrade File** based on the methods provided in **Table 3-67**.
2. Click **Upgrade**.

   The following information is displayed:

   Are you sure you want to perform this operation?
3. Click **Yes**.

   The iBMC starts the upgrade, and **Upgrade Progress** displays the upgrade progress.

After the upgrade is complete, the following information is displayed under **Upgrade Status**:

The upgrade is complete.

4. Repeat **1** to **3** to upgrade the active image of the iBMC.

Upgrading Other Firmware

1. On **Firmware Upgrade**, select the upgrade package from **Upgrade File** based on the methods provided in **Table 3-67**.

2. Click **Upgrade**

   The following information is displayed:

   Are you sure you want to perform this operation?

3. Click **Yes**.

   The iBMC starts the upgrade, and **Upgrade Progress** displays the upgrade progress.

   After the upgrade is complete, the following information is displayed under **Upgrade Status**:

   The upgrade is complete.

   After the BIOS firmware is upgraded, the following information is displayed in **Upgrade Status**:

   File upload successfully. The upgrade takes effect automatically after the next power-off or restart

Performing an Image Switchover for the iBMC Firmware

Perform an image switchover for the iBMC firmware only when necessary. The image switchover is optional during the upgrade.

1. On the **Firmware Upgrade** page, click **Image Switchover**.

   The following information is displayed:

   iBMC will restart after the switchover is complete. Continue?

2. Click **Yes**.

   The originally backup partition image file of the iBMC firmware is in use.

   The login page is displayed, and the following information is displayed:

   iBMC is restarting. Please wait a few minutes.

   After the iBMC is restarted, the login page is displayed.

Restart iBMC

Restart the iBMC as required. This operation is not mandatory during the upgrade.

1. On **Firmware Upgrade**, click **Restart iBMC**.

   The following information is displayed:

   Are you sure you want to perform this operation?

2. Click **Yes**. The iBMC restarts.

   The login page is displayed, and the following information is displayed:

   iBMC is restarting. Please wait a few minutes.

   After the iBMC is restarted, the login page is displayed.

3.8.7 Language Update

Function Description

The **Language Update** page allows you to install and uninstall language packs and change the language used on the iBMC.

☐ NOTE

- Only the administrators and the users authorized for common settings can install or uninstall language packs.
- Only the Japanese and France pack can be uninstalled and updated.
- The English and Chinese packs cannot be uninstalled or updated.

GUI

Choose **System** from the main menu, and select **Language Update** from the navigation tree.

The **Language Update** page is displayed.
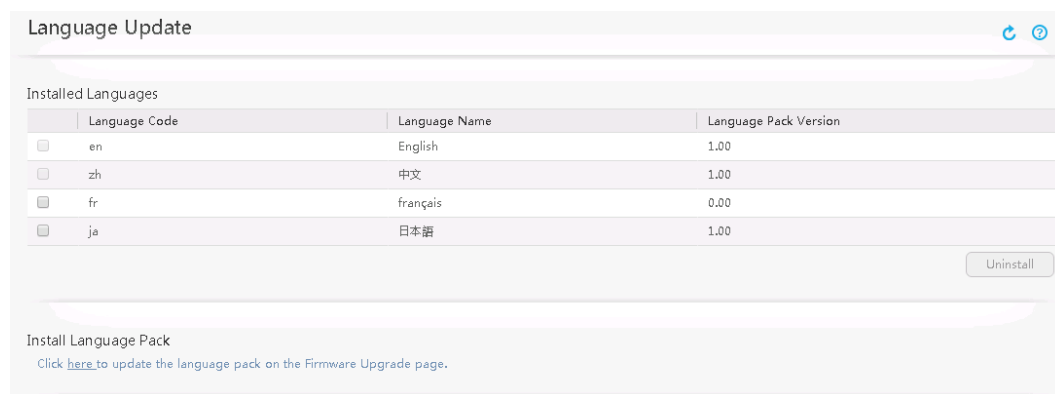
Parameters

Table 3-68 Language Update page

Parameter	Description
Installed Languages	
Language Code	Code of a language. For example, **en** stands for English, **zh** for Chinese, **ja** for Japanese, and **fr** for French.
Language Name	Language corresponding to the code.
Language Pack Version	Version of the language pack installed on the iBMC.
here	Click **here** to switch to the **Firmware Upgrade** page to update the language pack.

Procedure

Querying Installed Language Packs

1. Choose **System** from the main menu.
2. Select **Language Update** from the navigation tree.

   The **Language Update** page is displayed.

   The installed language packs are listed under **Installed Languages**.

Installing or Updating a Language Pack

1. Upload the target language pack, for example *XXX*-**iBMC-LANG-JA-V***XXX***.zip**.
2. Update the language pack.

   a. Log in to the iBMC WebUI.

   b. Choose **System** > **Firmware Upgrade**.

   The **Firmware Upgrade** page is displayed.

   c. Select the target language pack from **Upgrade File**.

   d. Click **Upgrade**.

   The following information is displayed:

   Are you sure you want to perform this operation?

   e. Click **Yes**.

   The iBMC starts to update the language pack, and **Upgrade Progress** displays the update progress.

   After the update is complete, the following information is displayed under **Upgrade Status**:

   The upgrade is complete.

   You can select the language to be used from the language drop-down list at the upper right corner of the page.

Uninstalling a Language Pack

1. On the **Language Update** page, select the language pack to be uninstalled under **Installed Languages**.
2. Click **Uninstall**.

   If "Operation Successful" is displayed, the language pack is uninstalled.

3.9 Remote Console

Function Description

The **Remote Console** page allows you to view the maximum number of sessions and the number of active sessions of the remote console, virtual media, and VNC service, and access the server operating system (OS) by using the Remote Virtual Console.

> ☐ **NOTE**
>
> Only V5 servers support the VNC service.

GUI

Choose **Remote Console** from the main menu.

The **Remote Console** page is displayed.

Parameter Description

Table 3-69 Parameters on the **Remote Console** page

Parameter	Description
Integrated Remote Console	

Parameter	Description
Java Integrated Remote Console	The Java integrated remote console provides two access modes: ● The private mode allows only one local user or VNC user to access and perform operations on the server through the iBMC. ● The shared mode allows two local users or up to 5 VNC users to simultaneously access and perform operations on the server through the iBMC. Each user can view the operations performed by the other user. The Integrated Remote Console allows you to: ● Adjust screen to your preferences using the floating buttons, screen zoom buttons, mouse buttons, and **Image Clarity** slider. ● Set the input device using the combination key button, keyboard indicators and layout buttons. ● Control the server OS using the power control buttons and records operations performed on the OS using the video recording button. ● Mount a physical DVD drive, FDD, image file, or local folder. ● Make a DVD or software image file using the image creation button. **NOTE** The Java integrated remote console requires Java Runtime Environment (JRE) to be installed. Click **here** to download it. Click **More information** for information about how to rectify common problems of the remote console.

Parameter	Description
HTML5 Integrated Remote Console	The HTML5 integrated remote console provides two access modes: ● The private mode allows only one local user or VNC user to access and perform operations on the server through the iBMC. ● The shared mode allows two local users or up to 5 VNC users to simultaneously access and perform operations on the server through the iBMC. Each user can view the operations performed by the other user. The HTML5 Integrated Remote Console allows you to: ● Adjust screen to your preferences using the floating buttons, screen zoom buttons, mouse buttons, and **Image Clarity** slider. ● Set the input device using the combination key button and keyboard layout buttons. ● Control the server OS using the power control buttons and records operations performed on the OS using the video recording button. ● Mount an image file or local folder using the DVD and FDD buttons. **NOTE** Only V5 servers support the HTML5 Integrated Remote Console.
Independent Remote Console	
Download	Independent Remote Console (IRC) allows users to access and manage the server in real time. The IRC does not depend on the browser, OS, or JRE version. If the **Download** button is unavailable on the page, contact the supplier.
Remote Console Settings	
Timeout Period (min)	Maximum idle time (in minutes) after the last operation (including data read operations on the virtual CD-ROM drive) on the remote console. If no operation is performed within the specified time, the system automatically disconnects from the remote console. Value range: 0 to 480 The value **0** indicates unlimited time. ● The default timeout period is 60 minutes for iBMC V328 and later. ● The default timeout period is **0** for the iBMC versions earlier than V328. This parameter cannot be empty.

Parameter	Description
Maximum Sessions	Maximum number of users who are allowed to use the remote console to connect to the server system. This parameter has a fixed value of **2**.
Active Sessions	Number of users who are concurrently connected to the server by using the remote console. You can click the number to switch to the **Online Users** page and view information about the users.
Encryption	Function for encrypting KVM data before transmission. If this function is enabled, KVM data is encrypted by using the AES128 algorithm before being transmitted between the server and the client. By default, KVM data encryption is disabled. For security purposes, enable this function. **NOTE** KVM encryption can be disabled only after VMM encryption is disabled and saved.
Enable local KVM	Function for enabling or disabling the local KVM. ● If **Enable local KVM** is selected, both an external monitor connected through a VGA port and the Remote Virtual Console can be used to access the server. ● If **Enable local KVM** is not selected, the external monitor cannot be used to access the server. You can use only the Remote Virtual Console to access the server. By default, **Enable local KVM** is selected.
Persistent Virtual Keyboard and Mouse	Function for enabling or disabling persistent keyboard and mouse connections. ● If this function is enabled, the iBMC virtual keyboard and mouse are always connected to the iBMC UHCI USB controller. ● If this function is disabled, the iBMC virtual keyboard and mouse are dynamically connected to the iBMC UHCI controller only when a Remote Console application is started and connected to the iBMC. This allows energy savings when the server OS is idle and no virtual USB keyboard and mouse are connected. By default, **Persistent Virtual Keyboard and Mouse** is selected.
Virtual Media	
Maximum Sessions	Maximum number of concurrent users who are allowed to use the virtual media (virtual DVD-ROM drive or floppy disk drive) of the Remote Virtual Console. This parameter has a fixed value of **1**.

Parameter	Description
Active Sessions	Number of users who are using the virtual media (virtual DVD-ROM drive or floppy disk drive) of the Remote Virtual Console. You can click the number to switch to the **Online Users** page and view information about the users.
Encryption	Function for encrypting virtual media data before transmission. If this function is enabled, virtual media data is encrypted by using the AES128 algorithm before being transmitted between the server and the client. By default, virtual media encryption is disabled. For security purposes, enable this function. **NOTE** 　VMM encryption can be enabled only after KVM encryption is enabled and saved.
VNC Service The VNC service allows you to connect to the server OS and perform operations on the keyboard, video, and mouse of the server. **NOTE** 　Only V5 servers support the VNC service.	
Timeout Period (min)	Maximum idle time (in minutes) after the last operation on the VNC interface. If no operation is performed within the specified time, the system automatically disconnects from the VNC interface. Value range: 0 to 480 ● The default timeout period is 60 minutes for iBMC V328 and later. ● The default timeout period is **0** for the iBMC versions earlier than V328. The value **0** indicates unlimited time.
Keyboard Layout	Keyboard layout of the OS controlled by the VNC. Value: ● Japanese ● English Default value: **Japanese**

Parameter	Description

VNC Password	Password for logging in to the VNC interface.
	
	Value:
	
	● If password complexity check is disabled, the VNC password is a string of 1 to 8 characters.
	
	● If password complexity check is enabled, the VNC password must meet the following requirements:
	
	  – Contain 8 characters.
	
	  – Meet the following complexity requirements:
	
	    – Contain at least one space or one of the following special characters:
	    `~!@#$%^&*()-_=+|[{}];:'",<.>/?
	
	    – Contain at least two of the following:
	
	      – Uppercase letters A to Z
	
	      – Lowercase letters a to z
	
	      – Digits 0 to 9

Confirm Password	Enter the community name again for consistency. **NOTE** After you click **Save**, the **User Password** dialog box is displayed. The VNC password can be set successfully only after you enter the password for logging in to the iBMC.
Password Validity (Days)	Validity period of the VNC password.
Login Rules	Login rules applied to VNC users. Click **View login rules** to view the login rules configured.
SSL Encryption	Function for enabling or disabling SSL encryption. Enable this function for security purposes. If SSL encryption is disabled, the VNC client starts the Remote Frame Buffer (RFB) process. **NOTE** If SSL encryption is enabled, only the VNC clients with SSL encryption enabled can connect to the server OS. If the VNC client does not provide the SSL encryption option, use an SSL tunneling application to implement SSL encryption. By default, **SSL Encryption** is selected.
Maximum Sessions	Maximum number of users who are allowed to access the VNC interface. This parameter has a fixed value of **5**.
Active Sessions	Number of users who are concurrently accessing the VNC interface. You can click the number to switch to the **Online Users** page and view information about the users.

Table 3-70 lists the operating systems (OSs), web browsers, and Java running environment (JRE) required for using the Remote Virtual Console.

☐ NOTE

- If the language of the browser you use to log in to the iBMC WebUI is not Chinese, English, or Japanese, upgrade the iBMC to V260 or later. Otherwise, the login page may fail to display.
- To download the JRE of a required version, visit the official website of the software.
- If the JRE version is 1.7 or 1.8 and the remote console application is stopped when you attempt to start it, refer to **3.10.1 Failed to Open the Remote Virtual Console**.

Table 3-70 Running environment

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	

OS	Browser	JRE
Windows Server 2008 R2 64-bit	Internet Explorer 9.0 to 11.0 **NOTE** HTML5 supports only Internet Explorer 10.0 or later.	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0 to 54.0	
	Google Chrome 21.0 to 44.0	
Windows Server 2012 64-bit	Internet Explorer 10.0 to 11.0	JRE 1.7 U45 JRE 1.8 U45 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 OS 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	

Procedure

Opening the Remote Virtual Console

☐ NOTE

When entering the OS or BIOS password on the Virtual Remote Console:

- If the keyboard in use complies with the OS keyboard setting, use the actual keyboard.
- If the keyboard in use does not comply with the OS keyboard setting, use the OS keyboard.

If a website security alert is displayed, you can ignore this message or perform any of the following to shield this alert:

- Import a trust certificate and a root certificate to the iBMC. For details, see **6.12 Importing the iBMC Trust and Root Certificates**.
- If no trust certificate is available, add the iBMC to the **Exception Site List** on **Java Control Panel**. This operation, however, poses security risks.

You can open the Remote Console in any of the following ways:

- On the **Remote Console** page, click **Java Integrated Remote Console (Shared)**, **Java Integrated Remote Console (Private)**, **HTML5 Integrated Remote Console (Shared)** or **HTML5 Integrated Remote Console (Private)**.

The shared mode allows two users to simultaneously use the remote console to access and perform operations on the server. Each user can view the operations performed by the other user.

The private mode allows only one user to use the remote console to access and perform operations on the server. If you select this mode, the manual screenshot function is unavailable.

- Open the browser and enter:
  - **https://IPaddress/remoteconsole** (recommended)
  - https://*IPaddress*/kvmvmm.asp
  - https://*IPaddress*/bmc/pages/remote/kvm.php
  - https://*IPaddress*/login.html?redirect_type=1

☐ NOTE

IPaddress indicates the iBMC IP address.

The iBMC WebUI login page is displayed. Perform the following operations:

a. Select the language to be used.

b. Enter the user name and password.

The default user name and password of V3 servers are **root** and **Huawei12#$** respectively. The default user name and password of V5 servers are **Administrator** and **Admin@9000** respectively.

c. Select **Local iBMC** or **LDAP** as required.

d. Click **Log In**.

Viewing the Number of Sessions

1. Choose **Remote Console** from the main menu.

   The **Remote Console** page is displayed.

2. View the maximum number of sessions and the number of active sessions for the remote console, virtual media, and VNC service.

3. Click the session number to switch to the **Online Users** and view information about the users.

Configuring Remote Console Settings

1. On the **Remote Console** page, set parameters in the **Remote Console Settings** area.

   For details about the parameters, see **Table 3-69**.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Enabling Virtual Media Communication Encryption

1. On the **Remote Console** page, select **Encryption** in the **Virtual Media** area.

2. Click **Save**.

   If "Operation Successful" is displayed, the setting is successful.

Setting the VNC Service

1. On the **Remote Console** page, set the parameters in the **VNC Service** area.

   For details about the parameters, see **Table 3-69**.

---

2. Click **Save**.

If "Operation Successful" is displayed, the setting is successful.

3.9.1 Java Integrated Remote Console

Function Description

With the Java Integrated Remote Console, you can access and manage a server remotely, install or repair the OS, and install drivers on the server.

With the Integrated Remote Console:

- You can use the keyboard and mouse of the local PC to remotely manage the server.
- You can enable the server to remotely access the local PC over a network using a virtual floppy disk drive (FDD) or DVD-ROM drive. To the server, the use of the virtual FDD or virtual DVD-ROM drive is the same as the user of a physical USB device.

  ☐ **NOTE**

  The media on the local PC can be a local FDD or DVD-ROM drive, or a floppy disk or DVD image file stored on the local PC or network drive.

Table 3-71 describes the icons on the KVM screen.

Table 3-71 Icons on the KVM screen

Icon	Description
📝	Locks the toolbar.
📌	Hides the toolbar.
⬌	Shows the server desktop in full-screen mode. **NOTE** To switch from full-screen mode to windowed mode, move the pointer to the top of the full-screen or press **Ctrl+Alt+Shift** to display the tool bar and press ↩.
🖱	Synchronizes the mouse location. **NOTE** This button is available on the toolbar only when the server desktop is displayed in full screen mode.
🖱	Changes the mouse mode. **NOTE** This button is available on the toolbar only when the server desktop is displayed in full screen mode.
↩	Returns to the server desktop in windowed mode. **NOTE** This button is available on the toolbar only when the server desktop is displayed in full screen mode.

Icon	Description
	Displays the power control menu, which includes the following: ● Power On ● Forced Power Off ● Power Off ● Forced System Reset ● Forced Power Cycle
	Records a video for the operations performed on the server.
	Controls the server mouse. The control operations include the following: ● **Mouse Acceleration** Accelerates the mouse on the server desktop to synchronize it with the mouse on the local PC. **NOTE** The SUSE versions earlier than SUSE 12 do not support mouse acceleration. ● **Single Mouse** Hides the mouse on the local PC and displays only the mouse on the server desktop. ● **Mouse & Key Reset** Simulates the removal and installation of a USB keyboard and mouse. When the keyboard and mouse on the server desktop stop responding, you can click **Mouse & Key Reset** to restore them. Default setting: **Mouse Acceleration** **NOTE** If **Mouse Acceleration** and **Single Mouse** are not selected, the mouse of the server desktop and the mouse of the local PC will be displayed and are not synchronized.
	Selects and uses a virtual DVD-ROM drive.
	Selects and uses a virtual FDD.
	Uses a DVD-ROM drive or FDD to create an image file.

Icon	Description
[icon: CTRL ALT DEL keys]	Sends or customizes combination keys. The combination keys are described as follows: ● **Ctrl+Shift**: switches between input methods. ● **Ctrl+Esc**: expands or collapses the **Start** menu. ● **Ctrl+Alt+Del**: locks the OS window, logs out a user, changes the password, opens Task Manager, or restarts the server. ● **Alt+Tab**: switches between running applications. ● **Ctrl+Space**: enables or disables an input method. ● **ResetKeyboad**: simulates the release of a key on the keyboard.
Image Clarity	Adjusts the image clarity of the server desktop.
num ■	Indicates the status of the **Num Lock** key on the server.
caps ■	Indicates the status of the **Caps Lock** key on the server.
scroll ■	Indicates the status of the **Scroll Lock** key on the server. If you press **Ctrl+S** by mistake after entering the Linux character mode, the screen is locked. Press **Scroll Lock** to unlock the screen. **NOTE** If a keyboard input error occurs when you manage the server using the Remote Virtual Console, check the status of the num ■, caps ■, and scroll ■ icons first.
(?)	Displays help information.
Note: The icons on the Remote Virtual Console screen and their functions vary according to the server model.	

Figure 3-36 shows the process for using a virtual DVD-ROM drive on the toolbar. The process for using an image file or virtual FDD is similar to this process.

Figure 3-36 Process

GUI
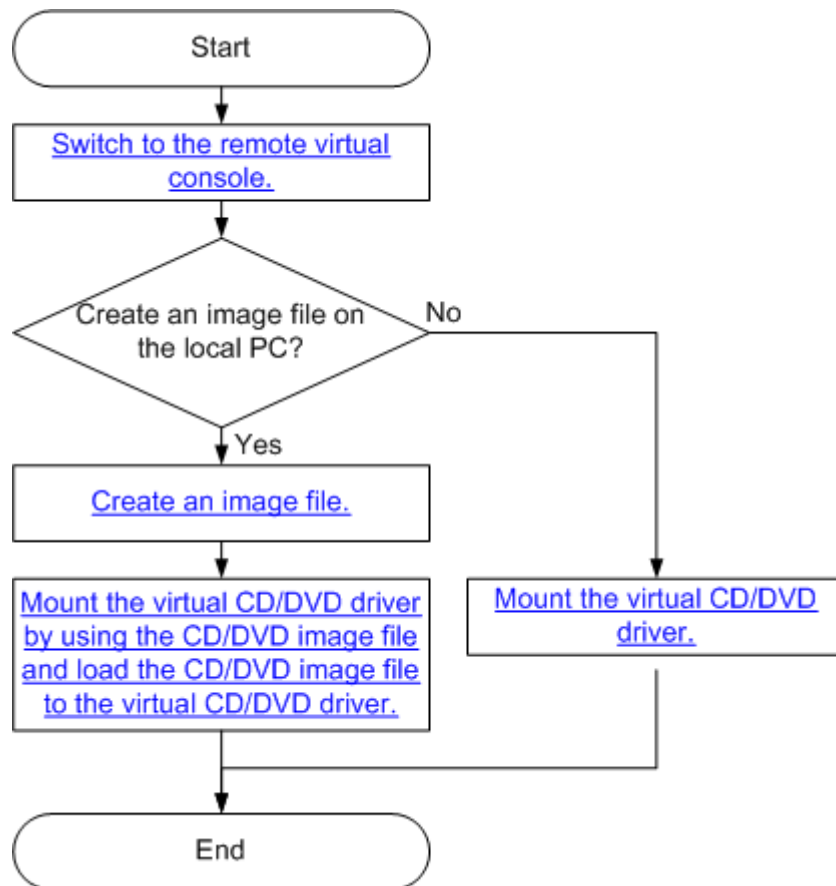
Choose **Remote Console** from the main menu, and click **Java Integrated Remote Console (Shared)** or **Java Integrated Remote Console (private)**.

The KVM screen is displayed.

☐ **NOTE**

If you click **Java Integrated Remote Console (Shared)**, two users are allowed to simultaneously access and perform operations on the server. Each user can view the operations performed by the other user, which causes security risks.

Table 3-72 describes the areas.

Figure 3-37 KVM screen
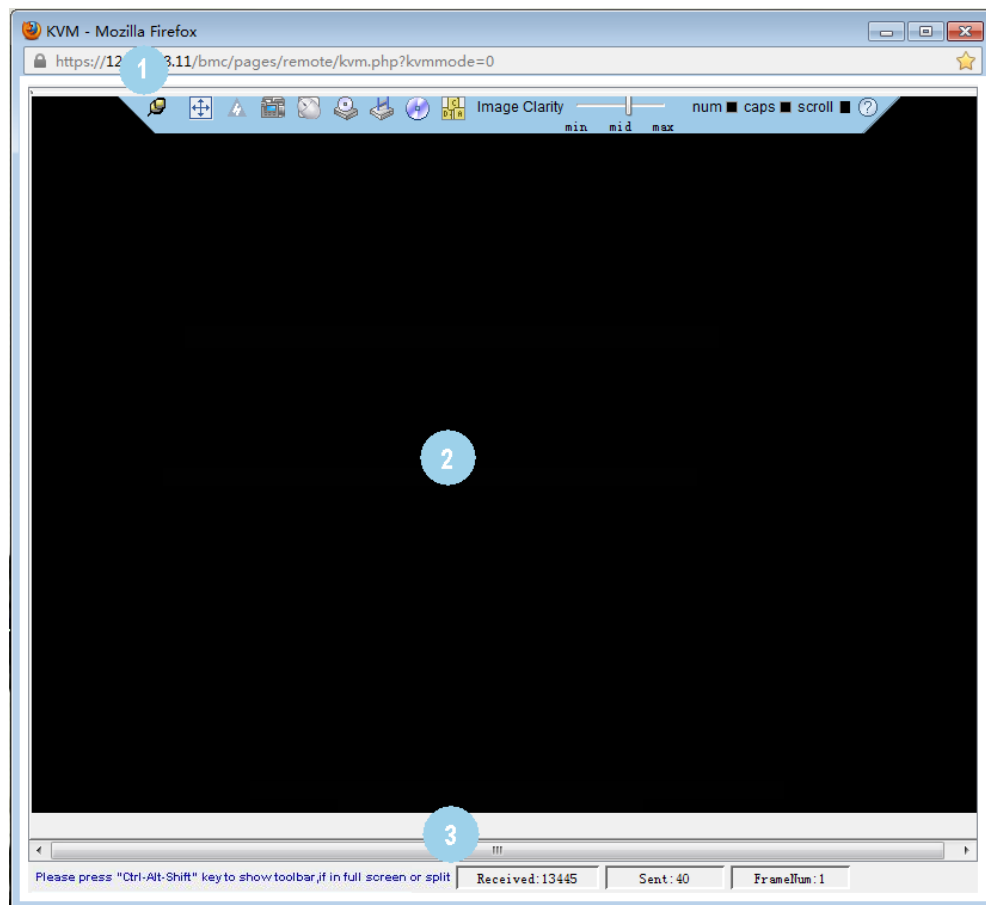
Table 3-72 Areas on the KVM screen

Area	Function
Toolbar (top)	The icons on the toolbar can be used to remotely manage the server.
Server desktop (middle)	You can use the mouse and keyboard on your local PC to manage the server on a real-time basis.
Status bar (bottom)	Displays tips for the server desktop and data about communication between the server and the local PC on a real-time basis.

Procedure

Sending a Combination Key

1. On the KVM screen, click ⌨ on the toolbar.

   The combination key dialog box is displayed.

2. Click a combination key.

   The server performs the operation defined for the combination key.

📖 **NOTE**

If you want to customize a combination key, enter the keys in the text box next to **Custom** and click **Send**.

Mounting a DVD-ROM Drive

Mount the DVD-ROM drive on the local PC to the server.

1. On the KVM screen, click 💿 on the toolbar.

   The dialog box shown in **Figure 3-38** is displayed.

   Figure 3-38 Mounting a virtual DVD-ROM drive

⦿ CD/DVD	G: ▾		Connect
◯ Image File		Browse	Eject
◯ Directory		Browse	
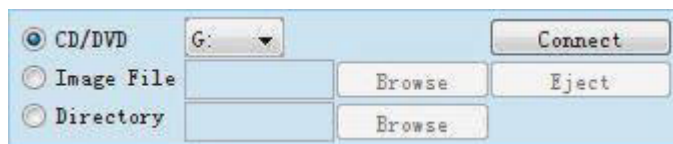
2. Select **CD/DVD**.

3. Select the drive letter of the DVD-ROM drive on the local PC from the drop-down list, for example, **G:**.

4. Click **Connect**.

   The DVD-ROM drive of the local PC is mounted to the server.

   📖 **NOTE**

   To dismount the DVD-ROM drive, click **Disconnect**. Then, click **Yes** in the **Confirm** dialog box displayed.

Loading an Image File from the Local PC Through the Virtual DVD-ROM Drive

Mount the DVD-ROM drive on the local PC and load an image file from the local PC to the server.

1. On the KVM screen, click 💿 on the toolbar.

   The dialog box shown in **Figure 3-38** is displayed.

2. Select **Image File**.

3. Click **Browse**.

   The **Open** dialog box is displayed.

4. Select the image file on the local PC, and click **Open**.

   The dialog box shown in **Figure 3-38** is displayed.

5. Click **Connect**.

   The virtual DVD-ROM drive is successfully mounted to the server and the image file is successfully loaded.

📖 **NOTE**

- To load another image file, click **Eject** to eject the existing DVD image file, select the new DVD image file, and click **Insert**.
- To dismount the virtual DVD-ROM drive, click **Disconnect**. Then, click **Yes** in the **Confirm** dialog box.

Mounting a Virtual FDD

Mount the FDD on the local PC to the server.

1. On the KVM screen, click 🖳 on the toolbar.

   The dialog box shown in **Figure 3-39** is displayed.

   Figure 3-39 Mounting a virtual FDD
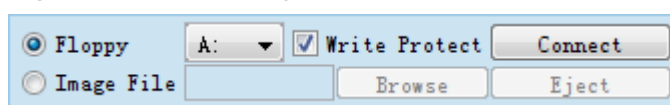
2. Select **Floppy**.
3. Select the drive letter of the FDD on the local PC from the drop-down list, for example, **A:**.
4. Select the **Write Protect** check box.

   📖 **NOTE**

   Write Protect is a mechanism that prevents alteration or erasure of important data. If **Write Protect** is selected, data cannot be written to the specified FDD.

5. Click **Connect**.

   The FDD is mounted to the server.

   📖 **NOTE**

   To dismount the FDD, click **Disconnect**. Then, click **Yes** in the **Confirm** dialog box.

Loading an Image File from the Local PC Through the Virtual FDD

Mount the FDD of the local PC and load an image file from the local PC to the server.

1. On the KVM screen, click 🖳 on the toolbar.

   The dialog box shown in **Figure 3-39** is displayed.

2. Select **Image File**.
3. Click **Browse**.

   The **Open** dialog box is displayed.

4. Select the image file on the local PC, and click **Open**.

   The dialog box shown in **Figure 3-39** is displayed.

5. Click **Connect**.

   The image file is successfully loaded to the server.

- To load another image file, click **Eject** to eject the existing virtual FDD, select the new image file, and click **Insert**.
- To dismount the virtual FDD, click **Disconnect**. Then, click **Yes** in the **Confirm** dialog box.

Creating an Image File

Create an image file with the help of the floppy disk on the FDD or DVD-ROM on the DVD-ROM drive of the local PC. The created image file is stored on the local PC.

Before performing this operation, ensure that a floppy disk has been inserted into the FDD or a DVD-ROM has been inserted into the DVD-ROM drive of the local PC.

1. On the KVM screen, click 🕹 on the toolbar.

   The dialog box shown in **Figure 3-40** is displayed.

   Figure 3-40 Creating an image file

Driver	G: ▼	Path		Browse
Progress		0%		Make
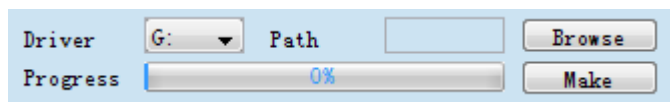
2. Select the drive letter of the FDD or DVD-ROM drive on the local PC from the **Driver** drop-down list.
3. Click **Browse**. The **Save** dialog box is displayed.
4. Specify a directory for saving the image file, and enter the file name in the **File Name** text box.

   📖 **NOTE**

   You can create only *.iso image files using the DVD-ROM drive and *.img image files using the FDD.

5. Click **Save**.

   The dialog box shown in **Figure 3-40** is displayed.

6. Click **Make**.

   Progress indicates the progress of the image file creation.

   📖 **NOTE**

   To stop creating an image file, click **Stop**.

Mounting a Virtual Directory

Mount the directories on the local PC to the server so that the server can access the local directories in read-only mode.

NOTICE

Before mounting a directory, copy the required files to the directory. After the directory is mounted, you cannot add files to the directory or delete files from it.

1. On the KVM screen, click 🖳 from the toolbar.

   The dialog box shown in **Figure 3-41** is displayed.

   Figure 3-41 Mounting a virtual directory
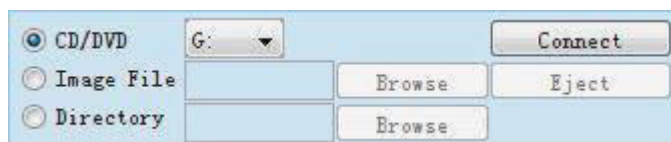
2. Click the **Directory** option button.

3. Click **Browse**.

   The dialog box for selecting a local directory is displayed.

4. Select the directory and click **Open**.

5. Click **Connect**.

   NOTE

   ● If the connection is successful, the virtual directory is displayed in the server OS list. You can copy files from this directory.

   ● To dismount the virtual directory, click **Disconnect**.

Powering On the Server

1. On the KVM screen, click ⚠ on the toolbar, and choose **Power On** from the menu.

   The **Confirm** dialog box is displayed.

2. Click **Yes**.

   The server is powered on.

   NOTE

   The server power-on time varies depending on the server configuration.

Powering Off the Server

NOTICE

● Before powering off the server, ensure that all services are stopped.

● Select a power-off mode based on your requirements. For details about the difference between the power-off modes, see **Power Control** in the *iBMC User Guide*.

1. On the KVM screen, click ⚠ on the toolbar, and choose **Power Off** from the menu.

   The **Confirm** dialog box is displayed.

2. Click **Yes**.

   The server is powered off.

Forcibly Resetting or Power Cycling the Server

NOTICE

- A forced reset or power cycle may damage user programs or unsaved data.
- Before forcefully resetting the system or forcefully power cycling the server, ensure that no service risk exists.
- Select a reset mode (**Forced System Reset** or **Forced Power Cycle**) based on service requirements. For details about the difference between the two modes, see **Power Control** in the *iBMC User Guide*.

---

1. On the KVM screen, click ⚠ on the toolbar, and choose **Forced System Reset** or **Forced Power Cycle** from the menu.

   The **Confirm** dialog box is displayed.

2. Click **Yes**.

   The server starts to reset or powers off and then powers on.

   📖 **NOTE**

   The reset or power cycle duration varies depending on the server configuration.

Resetting the Keyboard and Mouse

Simulate the removal and installation of a USB keyboard and mouse when the keyboard and mouse on the server desktop stop responding.

1. On the KVM screen, click 🖱 on the toolbar, and choose **Mouse & Key Reset** from the menu.

   The **Confirm** dialog box is displayed.

2. Click **Yes**.

   The USB keyboard and mouse are reset.

Recording a Video of the Server Desktop

Record a video of the desktop displayed on the Remote Virtual Console.

1. On the KVM screen, click 🖥 on the toolbar.

   The **Confirm** dialog box is displayed.

2. Click **Yes**.

   The **Save** dialog box is displayed.

3. Select a directory for saving the video file to be recorded, and enter a file name in the **File Name** text box.

---

4. Click **Save**.

The KVM screen is displayed, and the video recording starts.

5. After the video is recorded, click .

The **Confirm** dialog box is displayed.

6. Click **Yes**.

The video file is saved to the specified directory.

The video file is a .rep file. You can play the video file on the **Play Back** page.

Using a Single Mouse

If the mouse on the local PC is not synchronized with the server desktop, use the single-mouse function to hide the mouse on the local PC and display only the mouse of the server desktop on the

1. On the KVM screen, click on the toolbar, and choose **Single Mouse** from the menu.

The **Confirm** dialog box is displayed.

2. Click **Yes**.

Only the mouse on the server desktop is displayed on the KVM screen.

Accelerating the Remote Mouse

Accelerate the mouse on the server desktop to synchronize it with the mouse on the local PC.

1. On the KVM screen, click on the toolbar, and choose **Mouse Acceleration** from the menu.

The **Confirm** dialog box is displayed.

2. Click **Yes**.

The server mouse is synchronized with the mouse on the local PC.

3.9.2 HTML5 Integrated Remote Console

Function Description

With the HTML5 Integrated Remote Console, you can access and manage a server remotely, install or repair the OS, and install drivers on the server.

☐ **NOTE**

Only V5 servers support the HTML5 Integrated Remote Console.

With the Integrated Remote Console:

- You can use the keyboard and mouse of the local PC to remotely manage the server.
- You can enable the server to remotely access the local PC over a network using a virtual floppy disk drive (FDD) or DVD-ROM drive. To the server, the use of the virtual FDD or virtual DVD-ROM drive is the same as the user of a physical USB device.

📖 **NOTE**

The media on the local PC can be a local FDD or DVD-ROM drive, or a floppy disk or DVD image file stored on the local PC or network drive.
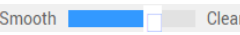
Table 3-73 describes the icons on the KVM screen.

Table 3-73 Icon description

Icon	Description
📌	Locks the toolbar.
📌	Hides the toolbar.
⛶	Shows the server desktop in full-screen mode.
⛶	Cancels the full-screen display of the server desktop.
⏻	Displays the power control menu, which includes the following: ● Power On ● Forced Power Off ● Power Off ● Forced System Reset ● Forced Power Cycle
B	Sets the first boot device for the OS. It provides the following options: ● **No Override**: Click this option to boot the OS from the default first boot device specified on the BIOS. ● **Hard Drive**: Click this option to boot the OS from the hard drive. ● **DVD-ROM**: Click this option to boot the OS from the CD-ROM or DVD-ROM drive. ● **FDD/Removable Device**: Click this option to boot the OS from a virtual floppy disk drive (FDD) or removable device. ● **PXE**: Click this option to boot the OS from the Preboot Execution Environment (PXE). ● **BIOS Setup**: Click this option to display the BIOS Setup menu upon server startup.

Icon	Description
	Sends or customizes combination keys. The combination keys are described as follows: ● **Alt+Tab**: switches between running applications. ● **Ctrl+Esc**: expands or collapses the **Start** menu. ● **Ctrl+Shift**: switches between input methods. ● **Ctrl+Space**: enables or disables an input method. ● **Ctrl+Alt+Del**: locks the OS window, logs out a user, changes the password, opens Task Manager, or restarts the server.
	Controls the server mouse. The control operations include the following: ● **Mouse Acceleration** ● Accelerates the mouse on the server desktop to synchronize it with the mouse on the local PC. **NOTE** The SUSE versions earlier than SUSE 12 do not support mouse acceleration. ● **Single Mouse** ● Hides the mouse on the local PC and displays only the mouse on the server desktop. ● **Mouse & Key Reset** ● Simulates the removal and installation of a USB keyboard and mouse. When the keyboard and mouse on the server desktop stop responding, you can click **Mouse & Key Reset** to restore them. Default setting: **Mouse Acceleration** **NOTE** If **Mouse Acceleration** and **Single Mouse** are not selected, the mouse of the server desktop and the mouse of the local PC will be displayed and are not synchronized.
	Selects and uses a virtual DVD-ROM drive.
	Selects and uses a virtual FDD.
	Records a video for the operations performed on the server.

Icon	Description
(keyboard icon)	Customizes the client keyboard. By default, the iBMC automatically selects the type of the client keyboard to be used. If the keyboard automatically selected does not function well, you can manually specify the keyboard type. ● **English (US)**: Use the English (US) keyboard. ● **Japanese**: Use the Japanese keyboard. ● **French**: Use the French keyboard. ● **Italian**: Use the Italian keyboard. ● **German**: Use the German keyboard. NOTE 　● Only iBMC V298 and later versions support this button and related settings. 　● From iBMC V350, the keyboard can be forcibly set to Italian keyboard.
(help icon)	Displays help information.
Smooth ▬▬▬ Clear	Adjusts the image clarity of the server desktop.

GUI

Choose **Remote Console** from the main menu, and click **HTML5 Integrated Remote Console (private)** or **HTML5 Integrated Remote Console (Shared)**.

The KVM screen is displayed.

📖 **NOTE**

If you click **HTML5 Integrated Remote Console (Shared)**, two users are allowed to simultaneously access and perform operations on the server. Each user can view the operations performed by the other user, which causes security risks.

Table 3-74 describes the areas.

Figure 3-42 KVM screen
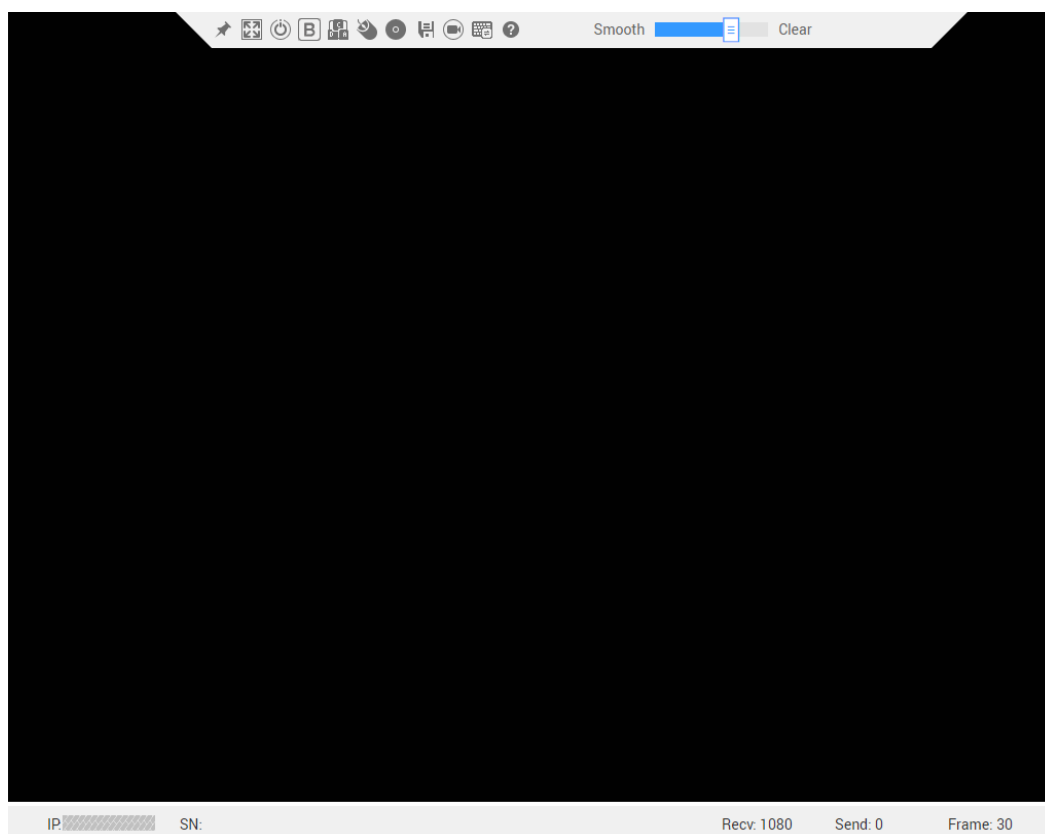
Table 3-74 Areas on the KVM screen

Area	Function
Toolbar (top)	The icons on the toolbar can be used to remotely manage the server.
Server desktop (middle)	You can use the mouse and keyboard on your local PC to manage the server on a real-time basis.
Status bar (bottom)	Displays the prompt information of the real-time desktop as well as the communication data between the server and the local PC, IP address, and product serial number of the server.

Procedure

Powering On the Server

On the **KVM** screen, click on the toolbar and choose **Power On** from the menu.

The server is powered on.

> **NOTE**
>
> The server power-on time varies depending on the server configuration.

Powering Off the Server

> **NOTICE**
>
> ● Before powering off the server, ensure that all services are stopped.
> ● Select a power-off mode based on your requirements. For details about the difference between the power-off modes, see **Power Control** in the *iBMC User Guide*.

On the **KVM** screen, click on the toolbar and choose **Forced Power Off** or **Power Off**.

The server is powered off.

Forcibly Resetting or Power Cycling the Server

> **NOTICE**
>
> ● A forced reset or power cycle may damage user programs or unsaved data.
> ● Before forcefully resetting the system or forcefully power cycling the server, ensure that no service risk exists.
> ● Select a reset mode (**Forced System Reset** or **Forced Power Cycle**) based on service requirements. For details about the difference between the two modes, see **Power Control** in the *iBMC User Guide*.

On the **KVM** screen, click on the toolbar and choose **Forced System Reset** or **Forced Power Cycle**.

The server starts to reset or powers off and then powers on.

> **NOTE**
>
> The reset or power cycle duration varies depending on the server configuration.

Setting the First Boot Device for the OS

Step 1 On the **KVM** screen, click on the toolbar.

The boot device options are displayed.

Step 2 Choose the first boot device as required.

For details about the options, see **Table 3-73**.

----End

Sending a Combination Key

Step 1 On the **KVM** screen, click [icon] on the toolbar.

The combination key dialog box is displayed.

Step 2 Click a combination key.

The server performs the operation defined for the combination key.

◯ **NOTE**

If you want to customize a combination key, enter the keys in the text box next to **Custom** and click **Send**.

----End

Accelerating the Remote Mouse

Accelerate the mouse on the server desktop to synchronize it with the mouse on the local PC.

On the **KVM** screen, click [icon] on the toolbar and choose **Mouse Acceleration**.

The server mouse is synchronized with the mouse on the local PC.

Using a Single Mouse

If the mouse on the local PC is not synchronized with the server desktop, use the single-mouse function to hide the mouse on the local PC and display only the mouse of the server desktop on the

On the **KVM** screen, click [icon] on the toolbar and choose **Single Mouse**.

Resetting the Keyboard and Mouse

Simulate the removal and installation of a USB keyboard and mouse when the keyboard and mouse on the server desktop stop responding.

On the **KVM** screen, click [icon] on the toolbar and choose **Mouse & Key Reset**.

The USB keyboard and mouse are reset.

Specifying the Client Keyboard

On the KVM screen, click [icon] on the toolbar and select the keyboard to be used.

Mounting a DVD-ROM Drive

Mount the DVD-ROM drive on the local PC to the server.

Step 1 On the **KVM** screen, click [icon] on the toolbar.

The screen shown in **Figure 3-43** is displayed.

Figure 3-43 Mounting a DVD-ROM drive

Step 2 Select **Image File**.

Step 3 Click [...].

The **Open** dialog box on the local PC is displayed.

Step 4 Select the *.iso file and click **Connect**.

The screen shown in **Figure 3-43** is displayed.

The image file is successfully loaded to the server.

☐ NOTE

- To load another image file, click **Eject**, select the *.iso file to be loaded, and click **Insert**.
- To dismount the DVD-ROM drive, click **Disconnect**.

----End

Mounting a File

Mount a file on the local PC to the server so that the server can access the file in read-only mode.

Step 1 On the **KVM** screen, click [○] on the toolbar.

The screen shown in **Figure 3-44** is displayed.

Figure 3-44 Mounting a file on the local PC

Step 2 Select **Local File**.

Step 3 Click [...].

The **Open** dialog box on the local PC is displayed.

Step 4 Select the file to be mounted.

The screen shown in **Figure 3-44** is displayed.

Step 5 Click **Connect**.

The file on the PC is successfully mounted to the server.

📖 NOTE

- After the file is successfully mounted, you can open and view the file on the server OS.
- To dismount the file, click **Disconnect**.

----End

Loading an Image File from the Local PC Through the Virtual FDD

Mount the FDD of the local PC and load an image file from the local PC to the server.

Step 1 On the **KVM** screen, click 💾 on the toolbar.

The screen shown in **Figure 3-45** is displayed.

Figure 3-45 Mounting an Image file through the virtual FDD
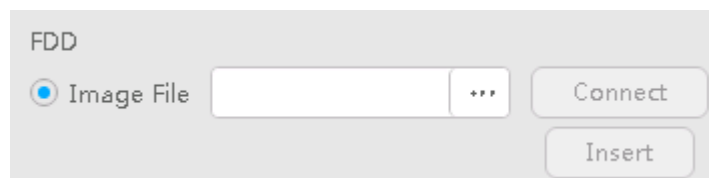
Step 2 Click ⋯ .

The **Open** dialog box on the local PC is displayed.

Step 3 Select the ***.img** file and click **Connect**.

The screen shown in **Figure 3-45** is displayed.

Step 4 Click **Connect**.

The image file is successfully mounted to the server.

📖 NOTE

- To load another image file, click **Eject** to eject the existing virtual FDD, select the new image file, and click **Insert**.
- To dismount the virtual FDD, click **Disconnect**.

----End

Recording a Video of the Server Desktop

Record a video of the desktop displayed on the Remote Virtual Console.

Step 1 On the **KVM** screen, click 🎥 on the toolbar.

When the icon changes to 🔴 , the video recording starts.

Step 2 Click 🔴 to stop the recording.

The video file is automatically downloaded and saved to the local PC.

----End

The video file is a .rep file. You can play the video file on the **Play Back** page.

3.10 Troubleshooting Remote Virtual Console Problems

3.10.1 Failed to Open the Remote Virtual Console

Symptom

Symptom	Possible Causes
The Remote Virtual Console cannot be opened.	- The JRE version is not correct. - The JRE version is incompatible with the iBMC.

Solution

Step 1 Check whether the JRE version installed is supported by the iBMC.

The iBMC supports JRE 1.7 and JRE 1.8.

- If yes, go to **Step 3**.
- If no, go to **Step 2**.

Step 2 Install a JRE version supported by the iBMC.

Install JRE 1.7 or 1.8, and go to **Step 3**.

Step 3 Modify Java security configuration.

1. Check the Java version of the client.

   On the Windows command line interface (CLI) or Linux terminal, run the **java –version** command.

2. Open Java Control Panel.

   – In Windows, open Java Control Panel through the Control Panel.

   – In Linux:

     i. Open the client.

     ii. Access the Java installation directory, for example, **/usr/java/jre1.7/ bin**.

     iii. Run the Java Control Panel.

3. Solve the incompatibility issue between JRE and the iBMC.

   You can solve the incompatibility issue by modifying the Java security configuration.

   – If the Java version is JRE 1.7, perform the following:

i. On the Java Control Panel, set the security level to **Medium** and click **OK**.

ii. Restart the web browser.

– If the Java version is JRE 1.8, perform the following:

i. On the **Security** tab page, click **Edit Site List**.

ii. Add the iBMC IP address and the port number (443 by default), for example, *https://192.168.2.10:443/*, to the list.

iii. Save the settings and restart the browser.

iv. Log in to the Remote Virtual Console again and ignore any security information displayed.

----End

3.10.2 Failed to Open the Remote Virtual Console Using Google Chrome

Symptom

Symptom	Possible Causes
The Remote Virtual Console cannot be opened in Google Chrome, and a message is displayed indicating that the plug-in is not supported.	The Netscape Plugin Application Programming Interface (NPAPI) is not enabled or supported by Google Chrome.

 NOTE

A Java plug-in complying with NPAPI is required to run the Remote Virtual Console. Before opening the Remote Virtual Console using Google Chrome, ensure that the NPAPI is enabled.

Solution

Google Chrome 45 and later versions no longer support the NPAPI.

1. Check the Google Chrome version.

   – If the Google Chrome version is 42, 43, or 44, go to **2**.

   – If the Google Chrome version is 45 or later, use other web browsers.

2. Enable NPAPI for Google Chrome.

   a. Enter **chrome://flags/#enable-npapi** in the address box of Google Chrome and press **Enter**.

   b. Restart Google Chrome.

3.10.3 Failed to Open the Remote Virtual Console Due to an Old Firefox Plug-In in Linux

Symptom

Symptom	Possible Causes
When the Remote Virtual Console is started using Firefox in Linux, a message is displayed indicating that the Firefox plug-in needs to be upgraded.	The Firefox plug-in version is too old.

Solution

Step 1 Access the Firefox plug-in directory.

For example, run the command **cd /usr/lib/mozilla/plugins**.

Step 2 Create a soft link to the **libnpjp2.so** file in the java installation directory.

For example, run the command **ln -s /usr/java/jre1.6.0_25/lib/libnpjp2.so**.

Step 3 Restart Firefox.

----End

3.10.4 Mouse and Keyboard Unavailable on the Remote Virtual Console

Symptom

Symptom	Possible Causes
The mouse and keyboard do not work on the Remote Virtual Console.	The LSISAS3108 RAID controller card is configured and persistent keyboard and mouse connection is disabled.

Solution

Step 1 Check whether the server is configured with the LSISAS3108 RAID controller card on the **Component Info** page.

- If yes, go to **Step 2**.
- If no, go to **Step 4**.

Step 2 On the **Remote Console** page, check whether persistent keyboard and mouse connection is enabled.

- If yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Enable persistent keyboard and mouse connection and restart the server. After the server is restarted, check whether the problem is solved.

- If yes, no further action is required.

- If no, go to **Step 4**.

Step 4 Contact technical support.

----End

3.10.5 Failed to Open the Remote Virtual Console After Java Web Start Icon Is Displayed

Symptom

Symptom	Possible Causes
After the Java web start page is displayed and closed, the Remote Virtual Console is not opened.	Temporary files are not available when Remote Virtual Console is started in Java web start mode.

Solution

Step 1 Open the Java Control Panel on the local PC.

Step 2 Click **Settings** on the **General** tab page.

Step 3 In the **Temporary Files Settings** window, select **Keep temporary files on my computer** and click **OK**, as shown in **Figure 3-46**.

Figure 3-46 Setting the historical file processing mode
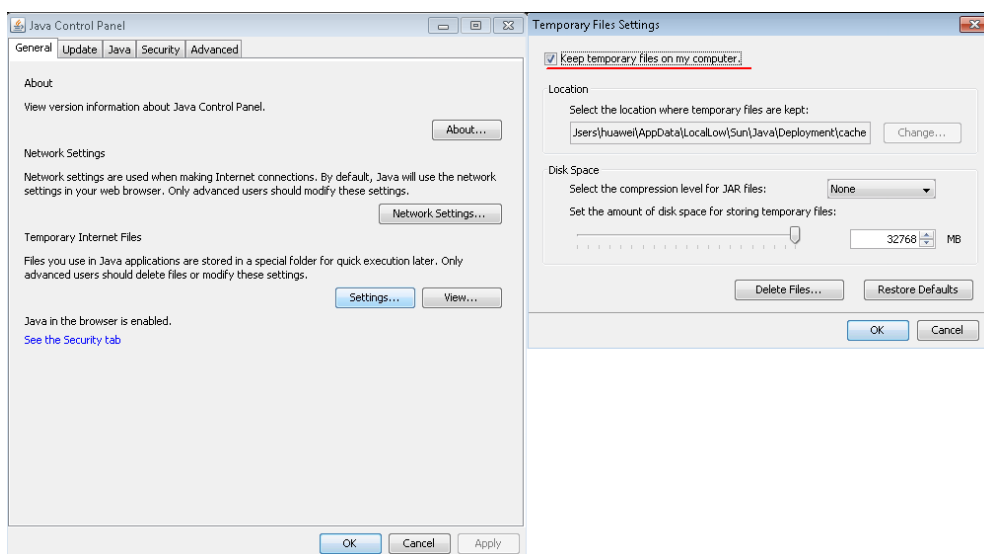
Step 4 Save the settings and restart the browser.

----End

3.10.6 Unauthorized User on the Remote Virtual Console

Symptom

Symptom	Possible Causes
1. The Java web start icon is displayed when a user attempts to open the Remote Virtual Console. 2. The Remote Virtual Console is opened after a very long time as the Java web start icon is no longer displayed. 3. After the Remote Virtual Console is displayed, the message "Unauthorized User" is displayed.	The authentication during the KVM startup needs to be performed when the client is connected to the Internet. If the client network is offline, the authentication may time out, which results in startup failure.

Solution

You can solve the problem by using any of the following methods:

- Connect the client used for accessing the Remote Virtual Console to the Internet.
- Set the Java parameters.

    a. Open the Java Control Panel on the local PC.

    b. On the **Advanced** tab page, select **Do not check** for **Perform signed code certificate revocation checks on**, as shown in **Figure 3-47**.

Figure 3-47 Modifying Java parameters
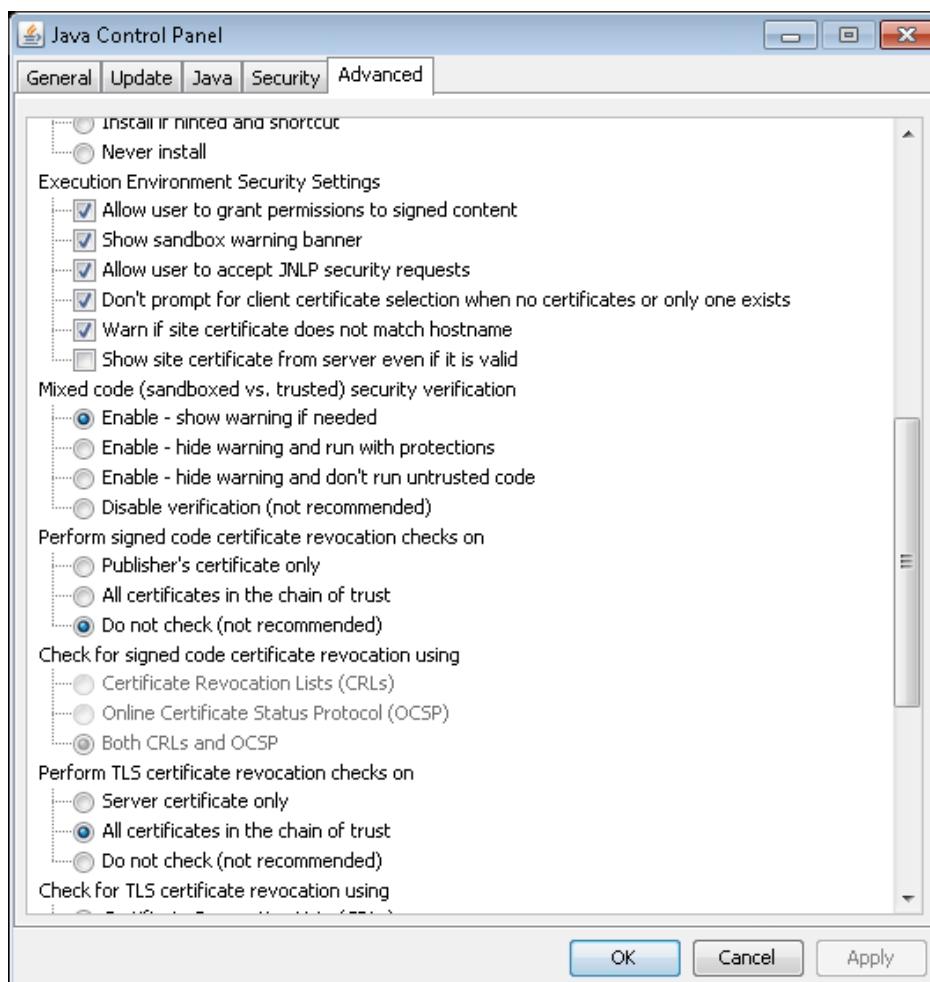
c. Save the settings and restart the browser.

3.10.7 Failed to Connect to the Management System After the KVM Is Open

Symptom

Symptom	Possible Causes
After the KVM is open, "Failed to connect to the management system. The management system IP address is xx.xx.xx.xx."	The default port number of the KVM service is 2198. This error occurs when the KVM service port is not enabled or is unavailable.

Solution

Step 1 On the iBMC WebUI, choose **Configuration** > **Services**, and check whether the KVM service is enabled.

- If yes, go to **Step 2**.

- If no, go to **Step 3**.

Step 2 Open the CLI (by using the **cmd** command), and run the **telnet** command, for example **telnet xx.xx.xx.xx 2198**, to check whether the KVM service port is reachable.

xx.xx.xx.xx indicates the IP address, *and 2198 indicates the default* KVM port No. Use the actual KVM port No. obtained in **Step 1**.

- If yes, go to **Step 5**.

- If no, go to **Step 4**.

Step 3 Enable the KVM service, and connect to the KVM. Then, check whether the problem is resolved.

- If yes, no further action is required.

- If no, go to **Step 2**.

Step 4 Contact the network administrator to enable the port required for the KVM. After checking that the port is reachable, connect to the KVM and check whether the problem is resolved.

- If yes, no further action is required.

- If no, go to **Step 5**.

Step 5 Contact technical support.

----End

3.10.8 Setting the Trusted Certificate Timed Out After the HTML5 Integrated Remote Console Is Open

Symptom

Symptom	Possible Causes
"Failed to open the KVM because setting the trust certificate timed out." is displayed on the HTML5 Integrated Remote Console.	The SSL certificate will be verified before the KVM client establishes a connection with the server. If the verification fails, the connection with the HTML5 Integrated Remote Console cannot be created.

Solution

Step 1 On the iBMC WebUI, choose **Configuration** > **SSL Certificate**, and check whether the server certificate has expired in the **Server Certificate Information** area.

- If yes, go to **Step 2**.

- If no, go to **Step 3**.

Step 2 Generate a new certificate and replace the expired certificate.

Step 3 Restart the iBMC.

Step 4 Open the HTML5 Integrated Remote Console and check whether the connection is successful.

- If yes, no further action is required.
- If no, go to **Step 5**.

Step 5 Contact technical support.

----End

3.11 One-Click Information Collection

Table 3-75 One-click information collection

Directory	Subdirectory	File Name	File Content
-	-	dump_app_log	List of information collected by the iBMC.
		dump_log	List of one-click information collecting result.
3rdDump	-	error_log	Apache error log.
		access_log	Apache access log.
		httpd.conf	Apache HTTP configuration file.
		httpd-port.conf	Apache HTTP port configuration file.
		httpd-ssl.conf	Apache HTTPS configuration file.
		httpd-ssl-port.conf	Apache HTTPS port configuration file.
		httpd-ssl-protocol.conf	Apache HTTPS protocol version configuration file.
AppDump	Lcd	Lcd_dfl.log	Information about the LCD module.
	User	User_dfl.log	Information about the User module.

Directory	Subdirectory	File Name	File Content
	card_manage	card_manage_dfl.log	Information about the Card_Manage module.
		card_info	Information about the cards configured on the server.
	BMC	BMC_dfl.log	Information about the BMC module.
		fruinfo.txt	Information about asset tag.
		net_info.txt	Information about network interface configuration
		psu_info.txt	Information about the PSUs of the server.
	PowerMgnt	PowerMgnt_dfl.log	Information about the PowerMgnt module.
		power_statistics.csv	Power statistic information.
	UPGRADE	UPGRADE_dfl.log	Information about the Upgrade module.
		upgrade_info	Version information about the devices related to the BMC.
	BIOS	BIOS_dfl.log	Information about the BIOS.
		bios_info	BIOS configuration information.

Directory	Subdirectory	File Name	File Content
		ClpConfig0.ini	Information about the iBMC configuration on the BIOS. **NOTE** This type of logs can be collected only when stateless computing is enabled for V3 servers.
		ClpResponse0.ini	Information about the iBMC response information configured on the BIOS. **NOTE** This type of logs can be collected only when stateless computing is enabled for V3 servers.
		options0.ini	BIOS configuration information. **NOTE** Only V3 servers support collecting of this type of logs.
		changed0.ini	List of changed BIOS configuration items. **NOTE** Only V3 servers support collecting of this type of logs.
		display0.ini	BIOS display information. **NOTE** Only V3 servers support collecting of this type of logs.

Directory	Subdirectory	File Name	File Content
		registry.json	BIOS registration file, containing BIOS configuration information. **NOTE** Only V5 servers support collection of this type of logs.
		currentvalue.json	Information about current BIOS configuration. **NOTE** Only V5 servers support collection of this type of logs.
		setting.json	Information about the BIOS settings configured using Redfish that have not take effect. **NOTE** Only V5 servers support collection of this type of logs.
		result.json	Result of the BIOS settings configured using Redfish. **NOTE** Only V5 servers support collection of this type of logs.
	discovery	discovery_dfl.log	Information about the Discovery module.
	diagnose	diagnose_dfl.log	Information about the Diagnose module.
		diagnose_info	Fault diagnosis information over port 80.
	Snmp	Snmp_dfl.log	Information about the Snmp module.

Directory	Subdirectory	File Name	File Content
	cooling_app	cooling_app_dfl.log	Information about the Cooling module.
		fan_info.txt	Information about the fan models and rotation speed.
	CpuMem	CpuMem_dfl.log	Information about the CpuMem module.
		cpu_info	Detailed information about the CPUs configured for the server.
		mem_info	Detailed information about the DIMMs configured for the server.
	kvm_vmm	kvm_vmm_dfl.log	Information about the KVM_VMM module.
	ipmi_app	ipmi_app_dfl.log	Information about the IPMI module.
	Dft	Dft_dfl.log	Information about the DFT module.
	net_nat	net_nat_dfl.log	Information about the Net_NAT module.
	PcieSwitch	PcieSwitch_dfl.log	Information about the PcieSwitch module.
		RetimerRegInfo	Retimer chip registry information.
	sensor_alarm	sensor_alarm_dfl.log	Information about the Sensor_Alarm module.
		sensor_info.txt	List of all sensors of the server.

Directory	Subdirectory	File Name	File Content
		current_event.txt	Current health status and alarms of the server.
		sel.tar	Compressed package of current and historical system event logs (SELs).
		sensor_alarm_sel.bin.md5	Integrity check code for original SELs.
		sensor_alarm_sel.bin.bak.md5	Integrity check code for the backup of original SELs.
		sensor_alarm_sel.bin.sha256	Integrity check code for original SELs.
		sensor_alarm_sel.bin.bak.sha256	Integrity check code for the backup of original SELs.
		sensor_alarm_sel.bin.bak	Original backup information and check value of the current SELs.
		sensor_alarm_sel.bin	Original information and check value of the current SELs.
		sel.db	Database information of the current SELs.
		LedInfo	Current indicator status of the server.
		sensor_alarm_sel.bin.tar.gz	Compressed package of historical SELs.
	MaintDebug	MaintDebug_dfl.log	Information about the MaintDebug module.

Directory	Subdirectory	File Name	File Content
	FileManage	FileManage_dfl.log	Information about the FileManage module.
	switch_card	switch_card_dfl.log	Information about the Switch_Card module.
		phy_register_info	Information about the PHY registry of the rear boards.
		port_adapter_info	Information about the interface device of the rear boards.
	StorageMgnt	StorageMgnt_dfl.log	Information about the StorageMgnt module.
		RAID_Controller_Info.txt	Information about the RAID controller card, logical disk, and hard disk.
	rimm	rimm_dfl.log	Information about the StorageMgnt module.
	redfish	redfish_dfl.log	Information about the Redfish module.
		component_uri.json	Component URI list.
	dfm	dfm.log	Information about the objects managed by the DFM.
		dfm_debug_log dfm_debug_log.1	PME frame debugging log.

Directory	Subdirectory	File Name	File Content
CoreDump	-	core-* (files starting with "core-".)	Memory dump file. It is the core dump file of an application program. One or more files are generated, depending on the system running status.
RTOSDump	sysinfo	cmdline	Kernel command line parameters.
		cpuinfo	Information about the CPU chip of the iBMC kernel.
		devices	iBMC device information.
		df_info	Information about the usage of the iBMC partitions.
		diskstats	Information about the iBMC disk status.
		filesystems	iBMC file system information.
		free_info	Information about available iBMC memory.
		interrupts	iBMC interrupt information.
		ipcs_q	iBMC process queue information.
		ipcs_q_detail	Detailed information about the iBMC process queue.
		ipcs_s	iBMC process semaphore information.

Directory	Subdirectory	File Name	File Content
		ipcs_s_detail	Detailed information about the iBMC process semaphore.
		loadavg	iBMC system workload information.
		locks	List of iBMC kernel lock files.
		meminfo	iBMC memory usage information.
		modules	List of iBMC modules.
		mtd	Information about the iBMC configuration partition.
		partitions	Information about the iBMC partitions.
		ps_info	ps -elf Displays detailed information about iBMC processes.
		slabinfo	Information about the iBMC slab information.
		stat	CPU usage of the iBMC.
		top_info	top -bn 1 Displays the current process running information.
		uname_info	uname -a Displays current status of the iBMC processes.
		uptime	iBMC system operating time

Directory	Subdirectory	File Name	File Content
		version	Real-time operating system (RTOS) version of the iBMC.
		vmstat	iBMC virtual memory statistical information.
	versioninfo	ibmc_revision.txt	iBMC revision information.
		app_revision.txt	iBMC version information.
		build_date.txt	Time when the iBMC version was built.
		fruinfo.txt	FRU electronic label information.
		RTOS-Release	RTOS release information.
		RTOS-Revision	RTOS version markup.
		server_config.txt	Current configuration information of the server.
	networkinfo	ifconfig_info	Network information. You can run the **ifconfig** command to obtain it.
		ipinfo_info	iBMC network configuration information.
		_data_var_dhcp_dhclient.leases	DHCP lease file.
		dhclient.leases	DHCP lease file.
		dhclient6.leases	DHCP lease file.
		dhclient6_eth0.leases	DHCP lease file.

Directory	Subdirectory	File Name	File Content
		dhclient6_eth1.leases	DHCP lease file.
		dhclient6_eth2.leases	DHCP lease file.
		dhclient.conf	DHCP configuration file.
		dhclient_ip.conf	DHCP configuration file.
		dhclient6.conf	DHCP configuration file.
		dhclient6_ip.conf	DHCP configuration file.
		resolv.conf	DNS configuration file.
		ipinfo.sh	iBMC network configuration script.
		netstat_info	netstat -a Displays the current network ports and connection status.
		route_info	route Displays the current routing information.
		services	Service port information.
	other_info	extern.conf	iBMC log file configuration.
		remotelog.conf	Syslog configuration file.
		ssh	SSH service configuration.
		sshd_config	SSHD service configuration file.
		logrotate.status	File recording the logrotate status.

Directory	Subdirectory	File Name	File Content
		login	Login pam login rules.
		sshd	SSH pam login rules.
		sfcb	CIM pam login rules.
		datafs_log	The data check log.
		ntp.conf	NTP service configuration.
		vsftpd	FTP pam login rules.
	driver_info	dmesg_info	System startup information (execution result of **dmesg**).
		lsmod_info	Information about loaded drivers.
		kbox_info	kbox information.
		edma_drv_info	The statistics of edma driver.
		cdev_drv_info	The statistics of character device driver.
		veth_drv_info	The statistics of virtual network card driver.
LogDump	-	LSI_RAID_Controller_Log LSI_RAID_Controller_Log.1.gz LSI_RAID_Controller_Log.2.gz	Logs of the LSI RAID controller.
		PD_SMART_INFO_C*	SMART log of hard disks. * indicates the serial number of the RAID controller.

Directory	Subdirectory	File Name	File Content
		linux_kernel_log linux_kernel_log.1	Linux kernel logs.
		operate_log operate_log.tar.gz	User operation log.
		remote_log remote_log.1.gz	Operation logs and SEL logs for Syslog test.
		security_log security_log.1	Security logs.
		strategy_log strategy_log.tar.gz	System running logs.
		fdm.bin fdm.bin.tar.gz	Log of FDM original faults.
		fdm_me_log fdm_me_log.tar.gz	Log of ME faults.
		fdm_pfae_log	Log of FDM perwarnings.
		fdm_mmio_log fdm_mmio_log.tar.gz	FDM board configuration logs.
		maintenance_log maintenance_log.tar.gz	Maintenance logs.
		ipmi_debug_log ipmi_debug_log.tar.gz	IPMI module logs.
		ipmi_mass_operation_log ipmi_mass_operation_log.tar.gz	IPMI module operation logs.
		app_debug_log_all app_debug_log_all.1.gz app_debug_log_all.2.gz app_debug_log_all.3.gz	App Debug logs.

Directory	Subdirectory	File Name	File Content
		agentless_driver_log agentless_driver_log.1.gz agentless_driver_log.2.gz agentless_driver_log.3.gz	Agentless driver debug logs.
		kvm_vmm_debug_log kvm_vmm_debug_log.tar.gz	KVM module logs.
		ps_black_box.log	Power supply black box logs.
OSDump	-	systemcom.tar	SOL serial port information.
		img*.jpeg	Image of the last screenshot of the server OS.
		*.rep	Video files automatically recorded.
		video_caterror_rep_is_deleted.info	Information prompting users to delete oversized caterror video files.
DeviceDump	i2c_info	*_info	I2C device memory or storage area information.
Register	-	cpld_reg_info	Complex programmable logical device (CPLD) register information.
OptPme	pram	filelist	List of files in the **/opt/pme/pram** directory.
		BIOS_FileName	SMBIOS information.

Directory	Subdirectory	File Name	File Content
	NOTE This folder contains files from the **/opt/pme/ pram** directory. The files that are not included in this folder are intermediate files generated during the running of the program and have no information security issues.	BIOS_OptionFileName	BIOS configuration information.
		BMC_dhclient.conf	DHCP configuration file.
		BMC_dhclient.conf.md5	Integrity check code.
		BMC_dhclient.conf.sha256	Integrity check code.
		BMC_dhclient6.conf	DHCP configuration file.
		BMC_dhclient6.conf.md5	Integrity check code.
		BMC_dhclient6.conf.sha256	Integrity check code.
		BMC_dhclient6_ip.conf	DHCP configuration file.
		BMC_dhclient6_ip.conf.md5	Integrity check code.
		BMC_dhclient6_ip.conf.sha256	Integrity check code.
		BMC_dhclient_ip.conf	DHCP configuration file.
		BMC_dhclient_ip.conf.md5	Integrity check code.
		BMC_dhclient_ip.conf.sha256	Integrity check code.
		BMC_HOSTNAME	Host name.
		BMC_HOSTNAME.md5	Integrity check code.
		BMC_HOSTNAME.sha256	Integrity check code.
		CpuMem_cpu_utilise	Server CPU usage.
		CpuMem_mem_utilise	Server memory usage.
		cpu_utilise_webview.dat	CPU usage curve data.

Directory	Subdirectory	File Name	File Content
		env_web_view.dat	Ambient temperature curve data.
		fsync_reg.ini	File synchronization configuration file.
		lost+found	Folder.
		md_so_maintenance_log	Maintenance log.
		md_so_maintenance_log.tar.gz	Maintenance log package.
		md_so_operate_log	User operation log.
		md_so_operate_log.md5	Integrity check code.
		md_so_operate_log.sha256	Integrity check code.
		md_so_operate_log.tar.gz	User operation log package.
		md_so_strategy_log	Policy log.
		md_so_strategy_log.md5	Integrity check code.
		md_so_strategy_log.sha256	Integrity check code.
		md_so_strategy_log.tar.gz	Policy log package.
		memory_webview.dat	Managed object operating information.
		per_config.ini	iBMC configuration persistence file.
		per_config.ini.md5	Integrity check code.
		per_config.ini.sha256	Integrity check code.

Directory	Subdirectory	File Name	File Content
		per_config_permanent.ini	iBMC configuration persistence file.
		per_config_permanent.ini.md5	Integrity check code.
		per_config_permanent.ini.sha256	Integrity check code.
		per_config_reset.ini	iBMC configuration persistence file.
		per_config_reset.ini.bak	iBMC configuration persistence file.
		per_config_reset.ini.bak.md5	Integrity check code.
		per_config_reset.ini.bak.sha256	Integrity check code.
		per_config_reset.ini.md5	Integrity check code.
		per_config_reset.ini.sha256	Integrity check code.
		per_def_config.ini	iBMC configuration persistence file.
		per_def_config.ini.md5	Integrity check code.
		per_def_config.ini.sha256	Integrity check code.
		per_def_config_permanent.ini	iBMC configuration persistence file.
		per_def_config_permanent.ini.md5	Integrity check code.
		per_def_config_permanent.ini.sha256	Integrity check code.
		per_def_config_reset.ini	iBMC configuration persistence file.

Directory	Subdirectory	File Name	File Content
		per_def_config_re set.ini.bak	iBMC configuration persistence file.
		per_def_config_re set.ini.bak.md5	Integrity check code.
		per_def_config_re set.ini.bak.sha256	Integrity check code.
		per_def_config_re set.ini.md5	Integrity check code.
		per_def_config_re set.ini.sha256	Integrity check code.
		per_power_off.ini	iBMC configuration persistence file.
		per_power_off.ini. md5	Integrity check code.
		per_power_off.ini. sha256	Integrity check code.
		per_reset.ini	iBMC configuration persistence file.
		per_reset.ini.bak	iBMC configuration persistence file.
		per_reset.ini.bak. md5	Integrity check code.
		per_reset.ini.bak.s ha256	Integrity check code.
		per_reset.ini.md5	Integrity check code.
		per_reset.ini.sha25 6	Integrity check code.
		pflash_lock	Flash file lock.
		PowerMgnt_recor d	Managed object operating information.
		powerview.txt	Power statistic file.

Directory	Subdirectory	File Name	File Content
		proc_queue	Process queue ID folder.
		ps_web_view.dat	Managed object operating information.
		sel.db	SEL database.
		sel_db_sync	SEL database synchronization lock.
		semid	Process semaphore ID folder.
		sensor_alarm_sel. bin	Original SEL file.
		sensor_alarm_sel. bin.md5	Integrity check code.
		sensor_alarm_sel. bin.sha256	Integrity check code.
		sensor_alarm_sel. bin.tar.gz	Historical SEL package folder.
		Snmp_snmpd.conf	SNMP configuration file.
		Snmp_snmpd.conf .md5	Integrity check code.
		Snmp_snmpd.conf .sha256	Integrity check code.
		Snmp_http_config ure	HTTP configuration folder.
		Snmp_http_config ure.md5	Integrity check code.
		Snmp_http_config ure.sha256	Integrity check code.
		Snmp_https_confi gure	HTTPS configuration folder.
		Snmp_https_confi gure.md5	Integrity check code.

Directory	Subdirectory	File Name	File Content
		Snmp_https_configure.sha256	Integrity check code.
		Snmp_https_tsl	HTTPS TLS configuration folder.
		Snmp_https_tsl.md5	Integrity check code.
		Snmp_https_tsl.sha256	Integrity check code.
		up_cfg	Upgrade configuration folder.
		User_login	Login pam login rules.
		User_login.md5	Integrity check code.
		User_login.sha256	Integrity check code.
		User_sshd	SSH pam login rules.
		User_sshd.md5	Integrity check code.
		User_sshd.sha256	Integrity check code.
		User_sshd_config	SSH configuration file.
		User_sshd_config.md5	Integrity check code.
		User_sshd_config.sha256	Integrity check code.
		User_vsftp	FTP pam login rules.
		User_vsftp.md5	Integrity check code.
		User_vsftp.sha256	Integrity check code.
		eo.db	SEL database.

Directory	Subdirectory	File Name	File Content
	save **NOTE** This folder contains files from the **/opt/pme/save** directory. The *.md5 file contains integrity check code. The *.sha256 file contains the integrity check code. The *.bak file is the backup file. The *.tar.gz file is a decompressed file package. The per_*.ini file is a configuration persistence file. The *sel.* is a system event log file. (The files that are not included in this folder are intermediate files generated during the running of the program and have no information security issues.)	filelist	List of files in the **/opt/pme/pram** directory.
		BIOS_FileName	SMBIOS information.
		BMC_dhclient.conf.bak	DHCP configuration backup file.
		BMC_dhclient.conf.bak.md5	Integrity check code.
		BMC_dhclient.conf.bak.sha256	Integrity check code.
		BMC_dhclient.conf.md5	Integrity check code.
		BMC_dhclient.conf.sha256	Integrity check code.
		BMC_dhclient6.conf.bak	DHCP configuration backup file.
		BMC_dhclient6.conf.bak.md5	Integrity check code.
		BMC_dhclient6.conf.bak.sha256	Integrity check code.
		BMC_dhclient6.conf.md5	Integrity check code.
		BMC_dhclient6.conf.sha256	Integrity check code.
		BMC_dhclient6_ip.conf.bak	DHCP configuration backup file.
		BMC_dhclient6_ip.conf.bak.md5	Integrity check code.
		BMC_dhclient6_ip.conf.bak.sha256	Integrity check code.
		BMC_dhclient6_ip.conf.md5	Integrity check code.
		BMC_dhclient6_ip.conf.sha256	Integrity check code.

Directory	Subdirectory	File Name	File Content
		BMC_dhclient_ip.conf.bak	DHCP configuration backup file.
		BMC_dhclient_ip.conf.bak.md5	Integrity check code.
		BMC_dhclient_ip.conf.bak.sha256	Integrity check code.
		BMC_dhclient_ip.conf.md5	Integrity check code.
		BMC_dhclient_ip.conf.sha256	Integrity check code.
		BMC_HOSTNAME.bak	Host name configuration backup file.
		BMC_HOSTNAME.bak.md5	Integrity check code.
		BMC_HOSTNAME.bak.sha256	Integrity check code.
		BMC_HOSTNAME.md5	Integrity check code.
		BMC_HOSTNAME.sha256	Integrity check code.
		CpuMem_cpu_utilise	Managed object operating information.
		CpuMem_mem_utilise	Managed object operating information.
		md_so_operate_log.bak	User operation log
		md_so_operate_log.bak.md5	Integrity check code.
		md_so_operate_log.md5	Integrity check code.
		md_so_operate_log.bak.sha256	Integrity check code.
		md_so_strategy_log.bak	Policy log.

Directory	Subdirectory	File Name	File Content
		md_so_operate_log.sha256	Integrity check code.
		md_so_strategy_log.bak.md5	Integrity check code.
		md_so_strategy_log.bak.sha256	Integrity check code.
		md_so_strategy_log.md5	Integrity check code.
		md_so_strategy_log.sha256	Integrity check code.
		per_config.ini	iBMC configuration persistence file.
		per_config.ini.bak	iBMC configuration persistence file.
		per_config.ini.bak.md5	Integrity check code.
		per_config.ini.bak.sha256	Integrity check code.
		per_config.ini.md5	Integrity check code.
		per_config.ini.sha256	Integrity check code.
		per_def_config.ini	iBMC configuration persistence file.
		per_def_config.ini.bak	iBMC configuration persistence file.
		per_def_config.ini.bak.md5	Integrity check code.
		per_def_config.ini.bak.sha256	Integrity check code.
		per_def_config.ini.md5	Integrity check code.
		per_def_config.ini.sha256	Integrity check code.

Directory	Subdirectory	File Name	File Content
		per_power_off.ini	iBMC configuration persistence file.
		per_power_off.ini.bak	iBMC configuration persistence file.
		per_power_off.ini.bak.md5	Integrity check code.
		per_power_off.ini.bak.sha256	Integrity check code.
		per_power_off.ini.md5	Integrity check code.
		per_power_off.ini.sha256	Integrity check code.
		PowerMgnt_record	Managed object operating information.
		sensor_alarm_sel.bin	Original SEL file.
		sensor_alarm_sel.bin.bak	Original SEL file.
		sensor_alarm_sel.bin.bak.md5	Integrity check code.
		sensor_alarm_sel.bin.bak.sha256	Integrity check code.
		sensor_alarm_sel.bin.md5	Integrity check code.
		sensor_alarm_sel.bin.sha256	Integrity check code.
		sensor_alarm_sel.bin.tar.gz	Historical SEL package.
		Snmp_http_configure.bak	HTTP configuration backup file.
		Snmp_http_configure.bak.md5	Integrity check code.
		Snmp_http_configure.bak.sha256	Integrity check code.

Directory	Subdirectory	File Name	File Content
		Snmp_http_configure.md5	Integrity check code.
		Snmp_http_configure.sha256	Integrity check code.
		Snmp_https_configure.bak	HTTPS configuration backup file.
		Snmp_https_configure.bak.md5	Integrity check code.
		Snmp_https_configure.bak.sha256	Integrity check code.
		Snmp_https_configure.md5	Integrity check code.
		Snmp_https_configure.sha256	Integrity check code.
		Snmp_https_tsl.bak	HTTPS TLS configuration backup file.
		Snmp_https_tsl.bak.md5	Integrity check code.
		Snmp_https_tsl.bak.sha256	Integrity check code.
		Snmp_https_tsl.md5	Integrity check code.
		Snmp_https_tsl.sha256	Integrity check code.
		Snmp_snmpd.conf.bak	Snmp configuration backup file.
		Snmp_snmpd.conf.bak.md5	Integrity check code.
		Snmp_snmpd.conf.bak.sha256	Integrity check code.
		Snmp_snmpd.conf.md5	Integrity check code.
		Snmp_snmpd.conf.sha256	Integrity check code.
		User_login.bak	Login pam login rules

Directory	Subdirectory	File Name	File Content
		User_login.bak.md5	Integrity check code.
		User_login.bak.sha256	Integrity check code.
		User_login.md5	Integrity check code.
		User_login.sha256	Integrity check code.
		User_sshd.bak	SSH pam login rules
		User_sshd.bak.md5	Integrity check code.
		User_sshd.bak.sha256	Integrity check code.
		User_sshd.md5	Integrity check code.
		User_sshd.sha256	Integrity check code.
		User_sshd_config.bak	SSH configuration folder.
		User_sshd_config.bak.md5	Integrity check code.
		User_sshd_config.bak.sha256	Integrity check code.
		User_sshd_config.md5	Integrity check code.
		User_sshd_config.sha256	Integrity check code.
		User_vsftp.bak	FTP pam login rules
		User_vsftp.bak.md5	Integrity check code.
		User_vsftp.bak.sha256	Integrity check code.
		User_vsftp.md5	Integrity check code.
		User_vsftp.sha256	Integrity check code.

Directory	Subdirectory	File Name	File Content
		eo.db	SEL database.
		eo.db.md5	Integrity check code.
		eo.db_backup	SEL database.
		eo.db.md5_backup	Integrity check code.

4 iBMC CLI

4.1 CLI Overview

4.1.1 Syntax

The iBMC commands can be classified into two types:

- Query command **ipmcget**

  Syntax:

  ipmcget [**-t** *target*] **-d** *dataitem* [**-v** *value*]

- Set command **ipmcset**

  Syntax:

  ipmcset [**-t** *target*] **-d** *dataitem* [**-v** *value*]

The parameters of **ipmcget** and **ipmcset** are described as follows:

- [ ]: includes optional parameter of a command.

- **-t** *target*: indicates the object to be queried or set.

- **-d** *dataitem*: indicates the specific properties of the object to be queried or set.

- **-v** *value*: indicates a parameter value of the object.

Table 4-1 lists the conventions for the command line formats.

Table 4-1 Conventions for the command line formats

Format	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.

Format	Description
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One or no item can be selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

4.1.2 Help

The iBMC CLI provides information about how to use the commands. To obtain help information, enter part of a command and press **Enter**.

Examples:

Query command:

```
iBMC:/->ipmcget
Usage: ipmcget [-t target] -d dataitem [-v value]
  -t <target>
    fru0              Get the information of the fru0
    sensor            Print detailed sensor information
    smbios            Get the information of smbios
    trap              Get SNMP trap status
    service           Get service information
    maintenance       Get maintenance information
    syslog            Get syslog status
    user              Get the information of user
    securitybanner    Get login security banner information
    storage           Get storage device information
    config            Get configuration information
    vmm               Get virtual media information
    certificate       Get SSL certificate information
    sol               Get SOL information
    securityenhance   Get security enhance information

  -d <dataitem>
    faninfo           Get fan mode and the percentage of the fan speed
    port80            Get the diagnose code of port 80
    diaginfo          Get diagnostic info of management subsystem
    systemcom         Get system com data
    blackbox          Get black box data
    bootdevice        Get boot device
    shutdowntimeout   Get graceful shutdown timeout state and value
    powerstate        Get power state
    health            Get health status
    healthevents      Get health events
    sel               Print System Event Log (SEL)
    operatelog        Print operation log
    version           Get iBMC version
    serialnumber      Get system serial number
    userlist          List all user info
    fruinfo           Get fru information
    time              Get system time
    macaddr           Get mac address
```

```
serialdir            Get currently connected serial direction
rollbackstatus          Get rollback status
passwordcomplexity         Get password complexity check enable status
ledinfo              Get led information
ipinfo               Get ip information
ethport              Get usable eth port
psuinfo              Get PSU component information
autodiscovery          Get autodiscovery configuration
poweronpermit           Get poweronpermit configuration
raid                 Deprecated. Please use 'ipmcget -t storage ...' to get more inforamtion
ldinfo               Deprecated. Please use 'ipmcget -t storage ...' to get more inforamtion
pdinfo               Deprecated. Please use 'ipmcget -t storage ...' to get more inforamtion
minimumpasswordage        Get minimum password age configuration
ntpinfo              Get NTP information
```

Set command:

```
iBMC:/->ipmcset
Usage: ipmcset [-t target] -d dataitem [-v value]
  -t <target>
    fru0              Operate with fru0
    trap              Operate SNMP trap
    service           Operate with service
    user              Operate with user
    maintenance          Operate with maintenance
    sensor            Operate with sensor
    securitybanner        Operate login security banner information
    syslog            Operate syslog
    ntp               Operate ntp
    storage           Configure storage device
    config            Operate configuration
    vmm               Operate virtual media
    certificate          Operate certificate
    sol               Operate SOL
    securityenhance       Operate security enhance

  -d <dataitem>
    fanmode             Set fan mode,you can choose manual or auto
    fanlevel            Set fan speed percent
    reset             Reboot iBMC system
    identify            Operate identify led
    upgrade             Upgrade component
    clearcmos           Clear CMOS
    bootdevice          Set boot device
    shutdowntimeout        Set graceful shutdown timeout state and value
    frucontrol          Fru control
    powerstate          Set power state
    sel               Clear SEL
    adduser             Add user
    password            Modify user password
    deluser             Delete user
    privilege           Set user privilege
    serialdir           Set serial direction
    printscreen          Print current screen to iBMC
    rollback            Perform a manual rollback
    timezone            Set time zone
    passwordcomplexity       Set password complexity check enable state
    ipaddr             Set ip address
    ipconfig            Set ip address mask gateway
    ipmode             Set ip mode
    gateway             Set gateway
    ipaddr6             Set ipv6 address
    ipmode6             Set ipv6 mode
    gateway6            Set ipv6 gateway
    ipv6config           Set ipv6 fix gateway
    netmode             Set net mode
    activeport           Set EthGroup active port
    vlan              Set sideband vlan
    restore             Restore factory setting
    notimeout           Set no timeout state
```

```
    emergencyuser          Set emergency user
    autodiscovery          Set autodiscovery configuration
    poweronpermit          Set poweronpermit configuration
    workkey                Update system workkey
    minimumpasswordage        Set minimum password age configuration
    locate                 Deprecated. Please use 'ipmcset -t storage ...'.
    psuworkmode            Set PSU work mode
```

If an incorrect parameter is entered, the help information prompts the correct optional parameters.

The following is an example:

```
iBMC:/->ipmcget -d inff
Input parameter[-d] error
   -d <dataitem>
    fanmode                Set fan mode,you can choose manual or auto
    fanlevel               Set fan speed percent
    reset                  Reboot iBMC system
    identify               Operate identify led
    upgrade                Upgrade component
    clearcmos              Clear CMOS
    bootdevice             Set boot device
    shutdowntimeout           Set graceful shutdown timeout state and value
    frucontrol             Fru control
    powerstate             Set power state
    sel                    Clear SEL
    adduser                Add user
    password               Modify user password
    deluser                Delete user
    privilege              Set user privilege
    serialdir              Set serial direction
    printscreen            Print current screen to iBMC
    rollback               Perform a manual rollback
    timezone               Set time zone
    passwordcomplexity        Set password complexity check enable state
    ipaddr                 Set ip address
    ipconfig               Set ip address mask gateway
    ipmode                 Set ip mode
    gateway                Set gateway
    ipaddr6                Set ipv6 address
    ipmode6                Set ipv6 mode
    gateway6               Set ipv6 gateway
    ipv6config             Set ipv6 fix gateway
    netmode                Set net mode
    activeport             Set EthGroup active port
    vlan                   Set sideband vlan
    restore                Restore factory setting
    notimeout              Set no timeout state
    emergencyuser          Set emergency user
    autodiscovery          Set autodiscovery configuration
    poweronpermit          Set poweronpermit configuration
    workkey                Update system workkey
    minimumpasswordage        Set minimum password age configuration
    locate                 Deprecated. Please use 'ipmcset -t storage ...'.
    psuworkmode            Set PSU work mode
```

4.2 Accessing the CLI

In addition to the default user, the iBMC has the following default users:

- **ftp**: a user for the FTP service.
- **root**: a user for running an app.
- **sshd**: a user for the Secure Shell (SSH) service.

- **nobody**: a user for the vsftpd process.

- **apache**: a user for the httpd service.

- **snmpd_user**: a user for the SNMP service.

- **ipmi_user**: a user for the IPMI service.

- **kvm_user**: a user for the remote console service.

📖 **NOTE**

- For V5 servers, user **root** is used only to run an app. It is not used for login.
- The description of the default users **ftp** and **nobody** applies only to V3 servers.
- These users cannot log in to the iBMC and have no impact on the system.
- These user roles are used for system management and not presented to end users.

4.2.1 Changing the iBMC Password on the BIOS

NOTICE

- The default BIOS password of V3 servers is **Huawei12#$**, and **Admin@9000** for V5 servers.

- On the BIOS, you can change only the password of the default iBMC user. The default iBMC user name is **root**, and default password is **Huawei12#$** for V3 servers. The default iBMC user name is **Administrator**, and default password is **Admin@9000** for V5 servers.

- The password of the default iBMC user specified on the BIOS can contain a maximum of 16 characters.

- For security purposes, change the initial password upon the first login, and change your password periodically.

- If **OS User Management** is disabled on the page displayed after you choose **Configuration** > **System** in the iBMC WebUI and the value of **BMC User Name** is displayed as **NA** on the **Server Mgmt** screen of the BIOS, you cannot change the password of the default iBMC user on the BIOS.

Operations for Grantley Platform

The BIOS screen varies depending on the server platform. This section uses the BIOS based on the Grantley platform as an example.

Step 1 Restart the server.

Step 2 During the startup process, press **Delete** repeatedly when the following screen is displayed.

Figure 4-1 BIOS startup screen

Version : 3.53
BIOS Build Date : 12/27/2016

Processor Type : Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz
Total Memory : 32768 MB

BMC IP: 192.168.2.100

Current KeyBoard Type : US

After installing OS, remember to install drivers and upgrade firmware

CPUID : 306F2
Press F5 go to Select Keyboard type
Press Del go to Setup Utility (F4 on Remote Keyboard)
Press F11 go to Boot Manager (F3 on Remote Keyboard)
Press F12 go to PXE

Step 3 Enter the BIOS password as prompted.

Figure 4-2 Entering the password

Enter Current Password:
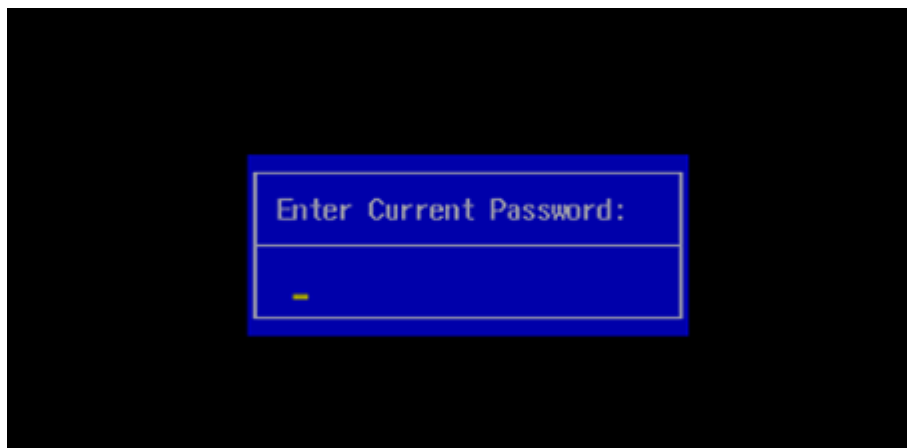
The BIOS Setup Utility screen is displayed, as shown in **Figure 4-3**.

Figure 4-3 BIOS main screen
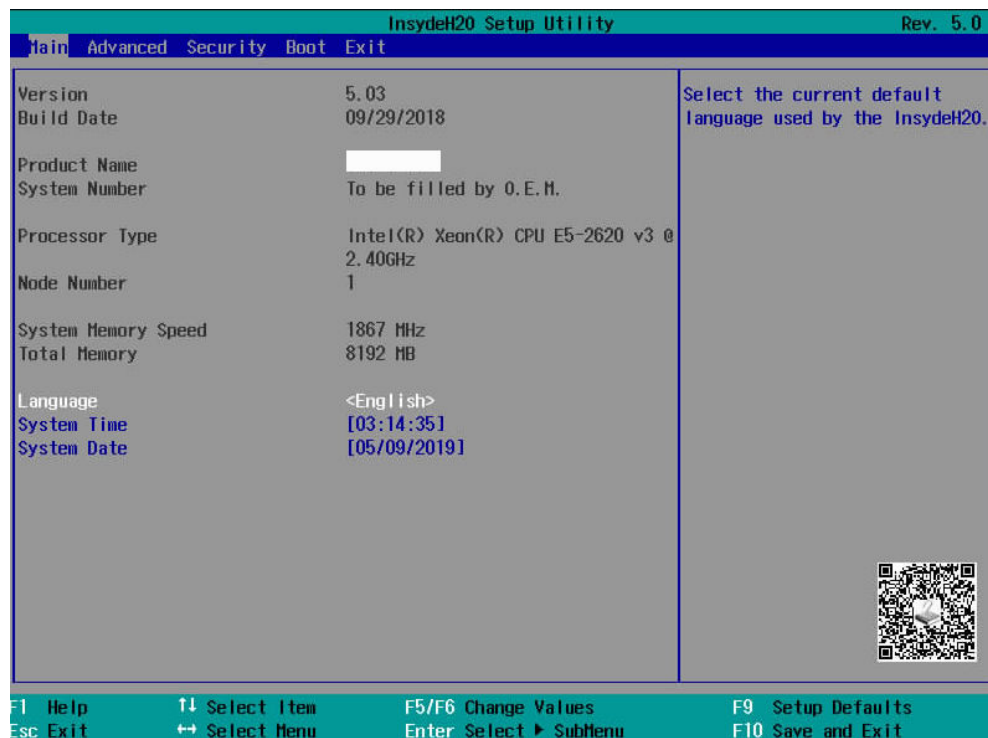
Step 4 Use arrow keys to select **Advanced**.

The **Advanced** screen is displayed, as shown in **Figure 4-4**.

Figure 4-4 Advanced screen
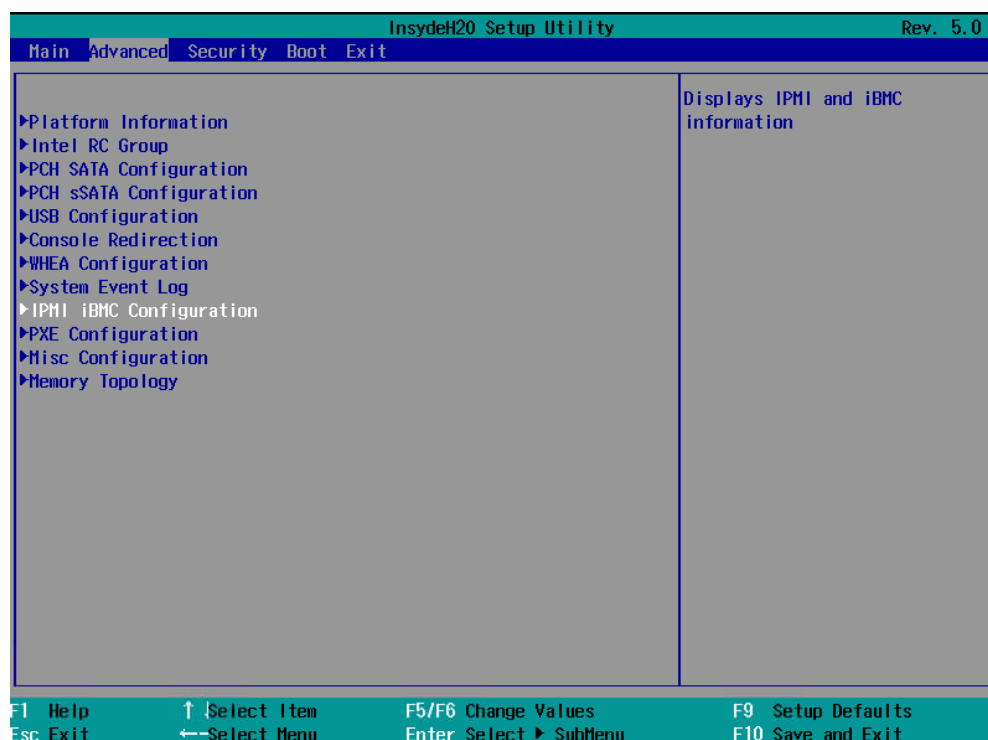
Step 5 On the **Advanced** screen, select **IPMI iBMC Configuration** using arrow keys and press **Enter**.

The **IPMI iBMC Configuration** screen is displayed, as shown in **Figure 4-5**.

Figure 4-5 IPMI iBMC Configuration screen
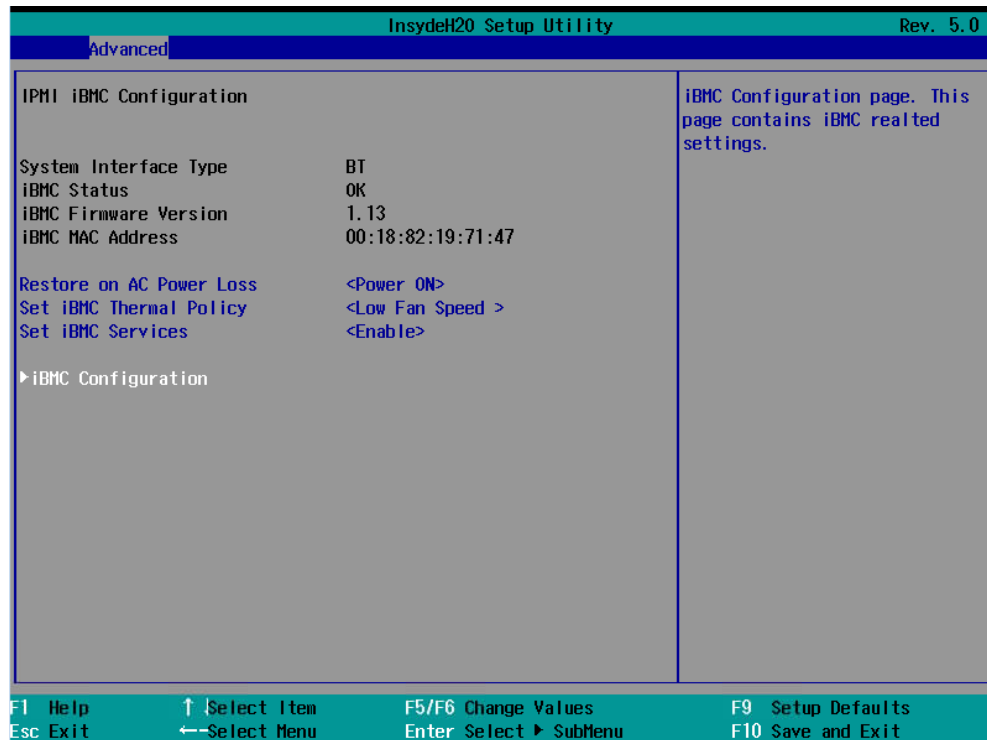
Step 6 On the **IPMI iBMC Configuration** screen, select **iBMC Configuration** using arrow keys and press **Enter**.

The **iBMC Configuration** screen is displayed, as shown in **Figure 4-6**.

Figure 4-6 iBMC Configuration screen

```
                        InsydeH20 Setup Utility                    Rev. 5.0
        Advanced

iBMC Configuration                                    Name should be 1-16 letter/
                                                      number/special,but no space,
iBMC User Name              root                      ':' and ','; and first letter
Reset iBMC User Password                              can't be '#'

iBMC WDT Support For POST   <Disabled>
iBMC WDT Support For OS     <Disabled>

iBMC&NCSI Select            <Dedicated>
Vlan ID                     [1]

IPV4 Configuration
-----------------------------------------------------
IP Source                   <Static>
IP Address                  10.10.1.150
Subnet Mask                 255.255.0.0
Gateway Address             10.10.1.100

IPV6 Configuration
-----------------------------------------------------
IP Source                   <Static>
Prefix Length               [0]
IP Address                  0:0:0:0:0:0:0:0
Gateway Address             0:0:0:0:0:0:0:0


F1  Help         ↑ Select Item      F5/F6 Change Values      F9  Setup Defaults
Esc Exit         ←—Select Menu      Enter Select ▶ SubMenu   F10 Save and Exit
```

Step 7 Select **Reset iBMC User Password** and press **Enter**.

The **Reset iBMC User Password** dialog box is displayed.

Step 8 Enter the new password and press **Enter**.

The password must meet the following requirements:

- If password complexity check is disabled, the password cannot be empty or exceed 20 characters.
- If password complexity check is enabled, the password must meet the following requirements:
  - Contain 8 to 20 characters
  - Contain at least a space or one of the following special characters: `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Contain at least two types of the following characters:
    - Uppercase letters A to Z
    - Lowercase letters a to z
    - Digits 0 to 9
  - Cannot be the same as the user name or the user name in reverse order.
  - Have at least two new characters when compared with the previous password.
- If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the

ipmcset -t user -d weakpwddic -v export command to export the weak passwords from the weak password dictionary.)

Step 9 Enter the password again for confirmation and press **Enter**.

The **Changes have been saved** dialog box is displayed.

Step 10 Press **Enter**.

The password is changed successfully.

----End

Operations for Brinkland Platform

The BIOS screen varies depending on the server platform. This section uses the BIOS based on the Brinkland platform as an example.

Step 1 Restart the server.

◫ NOTE

The server startup time varies depending on its configuration. It takes 20 minutes to start a fully configured server.

Step 2 During the startup process, press **Del** when the BIOS startup screen is displayed.

Step 3 Enter the password as prompted, as shown in **Figure 4-7**.

◫ NOTE

- For security purposes, change the default password upon the first login and change the password periodically.
- If an incorrect BIOS password is entered for three consecutive times, the BIOS is locked. You can press **Ctrl+Alt+Del** to restart the BIOS.

Figure 4-7 Entering the password
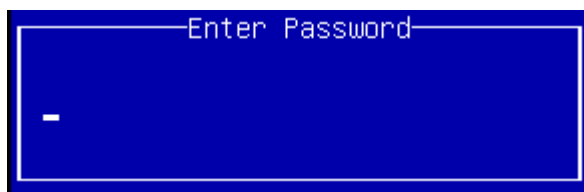
Step 4 On the BIOS Setup Utility, select **Server Mgmt** and press **Enter**.

The **Server Mgmt** screen is displayed, as shown in **Figure 4-8**.

Figure 4-8 Server Mgmt screen

Step 5 Select **BMC Root Password** and press **Enter**.

Step 6 Enter the new password and press **Enter**.

- If password complexity check is disabled, the password cannot be empty or exceed 20 characters.

- If password complexity check is enabled, the password must meet the following requirements:

  - Contain 8 to 20 characters

  - Contain at least a space or one of the following special characters:

    `` `~!@#$%^&*()-_=+\|[{}];:'",<.>/? ``

  - Contain at least two types of the following characters:

    - Uppercase letters A to Z

    - Lowercase letters a to z

    - Digits 0 to 9

  - Cannot be the same as the user name or the user name in reverse order.

  - Have at least two new characters when compared with the previous password.

- If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)

Step 7 Enter the password again for confirmation and press **Enter**.

The **Changes have been saved** dialog box is displayed.

Step 8 Press **Enter**.

The password is changed successfully.

----End

4.2.2 Querying the IP Address of the Management Network Port

You can query and set the IP address of the management network port by using:

- Basic input/output system (BIOS)
- iBMC CLI over the serial port

Default IP Addresses

Table 4-2 Default IP address

Product Type	Slot No.	IP Address
RH8100 V3/8100 V5	8-socket single system	192.168.2.100
	4-socket dual systems	• Primary management network port: 192.168.2.100 • Secondary management network port: 192.168.2.101
Other rack servers	-	192.168.2.100

Querying and Setting the IP Address on the BIOS (RH8100 V3)

Step 1 Restart the server.

📖 **NOTE**

The startup time of a server varies depending on its configuration. It takes 20 minutes to start a fully configured server.

Step 2 During the startup process, press **Del** when the BIOS startup screen is displayed.

Step 3 Enter the password and press **Enter**, as shown in **Figure 4-9**.

📖 **NOTE**

- The default BIOS password is **Huawei12#$**. For security purposes, change the default password upon the first login and change the password periodically.
- If an incorrect BIOS password is entered for three consecutive times, the BIOS will be locked. You can press **Ctrl+Alt+Del** to unlock the BIOS.

Figure 4-9 Entering the password
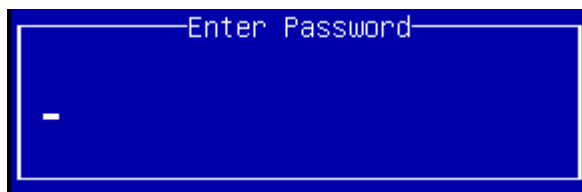
Step 4 Choose **Server Mgmt** > **BMC network configuration**, and press **Enter**.

The **BMC network configuration** screen is displayed, as shown in **Figure 4-10**.

Figure 4-10 BMC network configuration screen
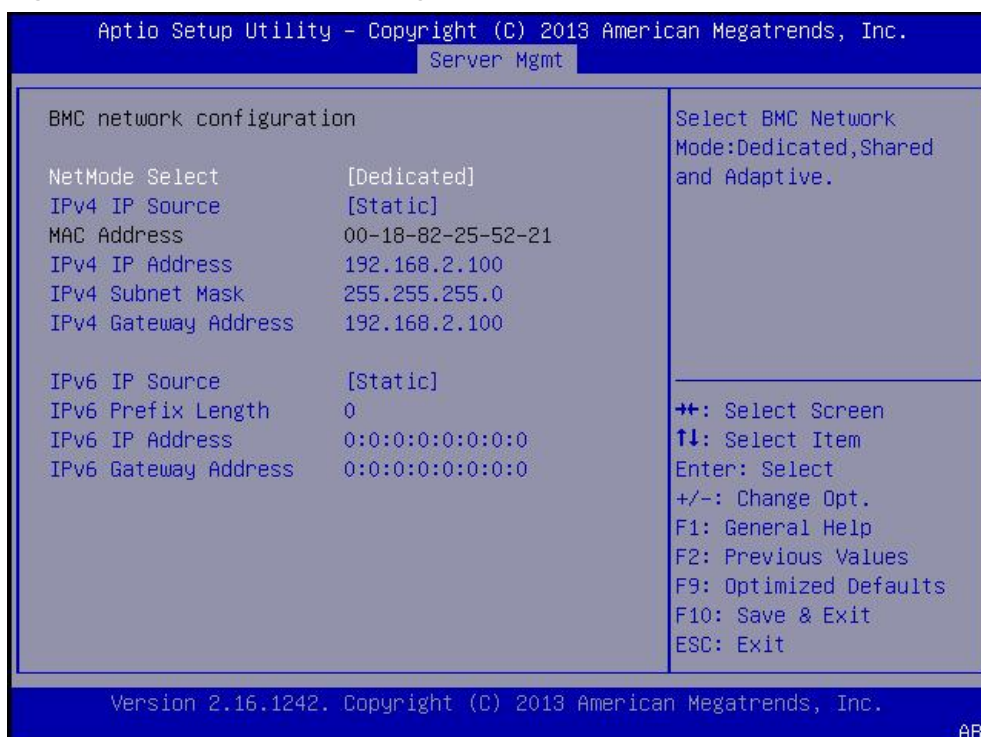
You can obtain the IP address information on this screen.

Step 5 (Optional) Change the IP address.

1. Select the IP address to be changed, and press **Enter**.
2. Enter the new IP address in the displayed dialog box, and press **Enter**.

----End

Querying and Setting the IP Address on the BIOS (Other Rack Servers)

Step 1 Restart the server.

Step 2 During the startup process, press **Delete** repeatedly when the following screen is displayed.

Figure 4-11 BIOS startup screen
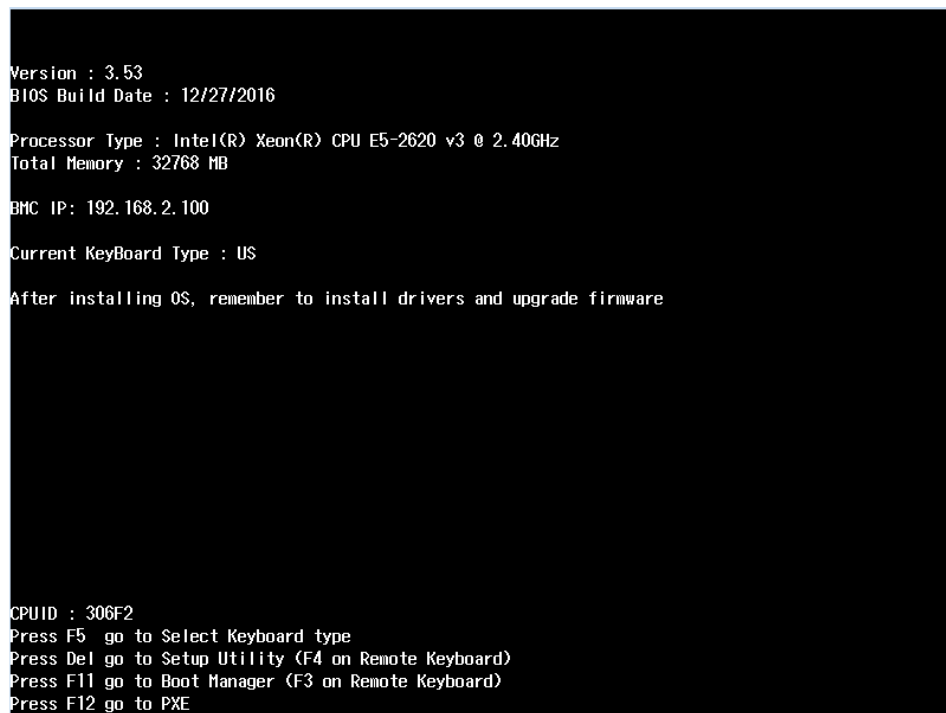
Step 3 Enter the password and press **Enter**, as shown in **Figure 4-12**.

Figure 4-12 Entering the password
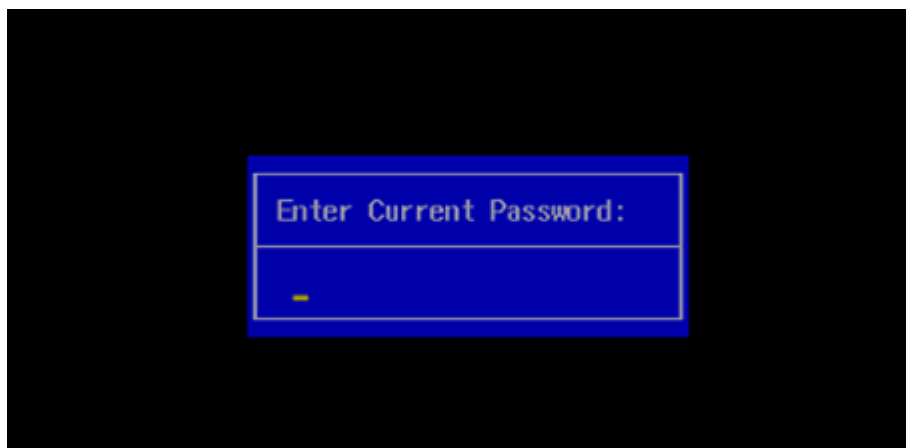
Step 4 Choose **Advanced** > **IPMI iBMC Configuration**, and press **Enter**.

The **IPMI iBMC Configuration** screen displayed.

Step 5 Select **iBMC Configuration** and press **Enter**.

The **iBMC Configuration** screen is displayed, as shown in **Figure 4-13**.

You can obtain the management port IP address on this screen.

Figure 4-13 BMC Configuration screen

```
                        InsydeH20 Setup Utility                      Rev. 5.0
      Advanced

 iBMC Configuration                                       Select iBMC or NCSI.

 iBMC User Name                   root
 Reset iBMC User Password

 iBMC WDT Support For POST        <Disabled>
 iBMC WDT Support For OS          <Disabled>

 iBMC&NCSI Select                 <Shared-LOM>
 Vlan ID                          [0]
 NCSI NIC Port Select             <Port1>

 IPV4 Configuration
 -------------------------------------------------
 IP Source                        <Static>
 IP Address                       192.168.2.226
 Subnet Mask                      255.255.255.0
 Gateway Address                  192.168.2.226

 IPV6 Configuration
 -------------------------------------------------
 IP Source                        <Static>
 Prefix Length                    [0]
 IP Address                       0:0:0:0:0:0:0:0
 Gateway Address                  0:0:0:0:0:0:0:0

 F1  Help         ↑↓ Select Item    F5/F6 Change Values      F9  Setup Defaults
 Esc Exit         ↔ Select Menu     Enter Select ▶ SubMenu   F10 Save and Exit
```

Step 6 (Optional) Change the IP address.

1. Select the IP address to be changed, and press **Enter**.

2. Enter the new IP address in the displayed dialog box, and press **Enter**.

----End

Query Through the Serial Port

Step 1 Log in to the iBMC CLI through the serial port.

For details, see **Accessing the iBMC CLI over the Serial Port**.

Step 2 Run the **ipmcget -d ipinfo** command.

The command output contains the IP address of the iBMC management network port.

----End

4.2.3 Accessing the iBMC CLI

You can log in to the iBMC CLI using any of the following methods:

- SSH

  Secure Shell (SSH) is a network protocol that allows data to be exchanged over a secure channel between two computers. A maximum of five users can access the iBMC CLI over SSH at the same time.

☐ **NOTE**

> SSH supports AES128-CTR, AES192-CTR, and AES256-CTR encryption algorithms. Use an appropriate encryption algorithm when accessing the iBMC over SSH.

- Local serial port

☐ **NOTE**

- The default iBMC user is **root** for V3 servers, and the default password is **Huawei12#$**. The default user is **Administrator** for V5 servers and the default password is **Admin@9000**.

- The system locks a user account if the user enters incorrect passwords for consecutive five times. The user account is automatically unlocked five minutes later. The administrator can also unlock the user account using the command line.

- For security purposes, change the initial password upon the first login and change your password periodically.

- The default operation timeout period on the CLI is 15 minutes.

Prerequisites

- To open the CLI over the network port, you must connect the network interface of the configuration terminal to the network interface of the server by using a network cable, and ensure that the IP addresses of the two network interfaces are on the same network segment.

  ☐ **NOTE**

  > Do not connect to the two management ports at the same time. Access the iBMC through only one management port.

- Before accessing the iBMC CLI through the serial port, use a serial cable to connect the serial port of the configuration terminal to the serial port of the server.

The rack server provides the adaptive management network interface of 1000 Mbit/s on the rear panel of the chassis. You can connect the network interface by using a network cable.

Accessing the iBMC CLI over SSH

1. Download an SSH communication tool on the local PC.
2. Connect the local PC to the server management network port directly or over the network.
3. Configure an IP address for the local PC to enable communication between the local PC and the iBMC management network port.
4. On the local PC, use the SSH tool to connect to the iBMC.
5. Enter the user name and password to access the iBMC.

☐ **NOTE**

- Both local and LDAP users can access the iBMC CLI over SSH. The LDAP user can access the iBMC CLI without entering the domain server information.

- Before logging in to the iBMC CLI as an LDAP user, ensure that the connection between the iBMC and the LDAP server is normal.

Accessing the iBMC CLI over the Serial Port

> **NOTICE**
>
> Before accessing the iBMC CLI over the serial port, ensure that the system serial port of the chassis is switched to the iBMC serial port. You can switch over the serial port by using the **serialdir** command on the CLI.

Step 1 Connect the local PC and the server using a serial cable.

Step 2 Open HyperTerminal and set the following parameters:

- Bits per second: 115200

- Data bits: 8

- Parity: None

- Stop bits: 1

- Flow control: None

For details on how to set the parameters, see **Figure 4-14**.

Figure 4-14 HyperTerminal properties
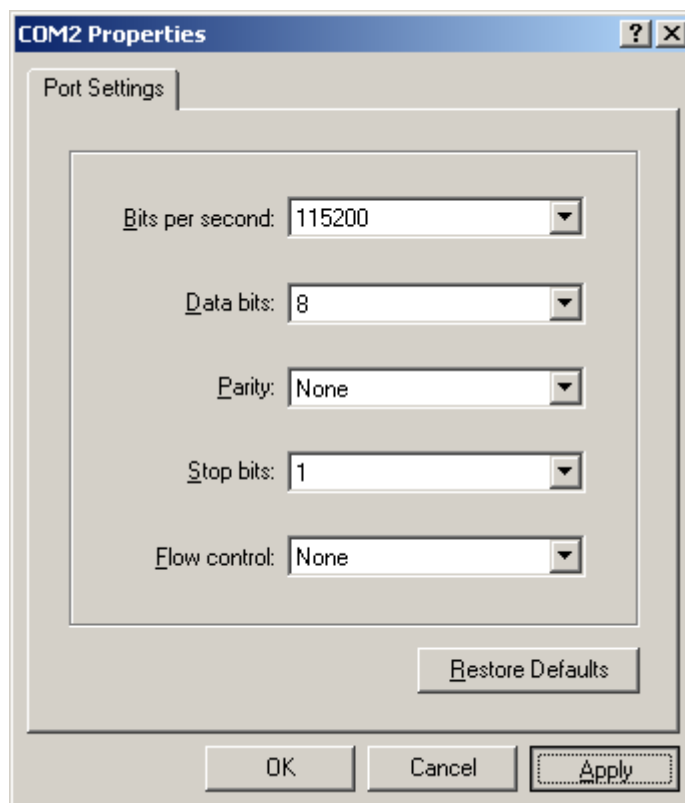
Step 3 Click **Apply**.

Step 4 Enter the user name and password to access the CLI.

----End

4.3 iBMC Commands

4.3.1 Querying iBMC IP Information (ipinfo)

Function

The **ipinfo** command is used to query the IP address of the iBMC management network port.

Format

ipmcget -d ipinfo

Parameters

None.

Usage Guidelines

None

Example

Query the iBMC IP address.

iBMC:/->**ipmcget -d ipinfo**

The System return information of RH8100 V3:

```
EthGroup ID        : 1
Net Mode           :  Manual
Net Type           :  Dedicated
IPv4 Information    :
IP Mode            :  static
IP Address         :  192.168.2.100
Subnet Mask        :  255.255.0.0
Default Gateway     :  192.168.2.25
MAC Address        :  00:18:e1:c5:d8:26
IPv6 Information    :
IPv6 Mode          :  static
IPv6 Address       :  fc00::2001/15
Default Gateway IPv6 :  fc00::2003
Link-Local Address   :  fe80::218:e1ff:fec5:d826/64
VLAN Information    :
VLAN State         :  disabled

EthGroup ID        :  2
Net Mode           :  Manual
Net Type           :  Dedicated
IPv4 Information    :
IP Mode            :  static
IP Address         :  10.0.0.1
Subnet Mask        :  255.255.255.252
Default Gateway     :
```

```
MAC Address        :
IPv6 Information    :
IPv6 Mode          : static
IPv6 Address 1        : fc00::2001/15
Default Gateway IPv6  : fc00::2003
Link-Local Address   : fe80::218:e1ff:fec5:d826/64
IPv6 Address 1        : fc00::db8:1:0:218:e1ff:fec5:d826/64
VLAN Information    :
VLAN State         : enabled
VLAN ID            : 4094
```

☐ NOTE

- GROUP1 is used for external access.

- GROUP2 is used for internal data communication.

The System return information of other rack servers:

```
EthGroup ID        : 1
Net Mode           : Manual
Net Type           : Dedicated
IPv4 Information    :
IP Mode            : static
IP Address         : 172.33.13.104
Subnet Mask        : 255.255.0.0
Default Gateway    : 172.33.0.1
MAC Address        : 00:18:ac:21:0d:68
IPv6 Information    :
IPv6 Mode          : static
IPv6 Address 1        :
Default Gateway IPv6 :
Link-Local Address   : fe80::218:acff:fe21:d68/64
VLAN Information    :
VLAN State         : enabled
VLAN ID            : 4093
```

4.3.2 Setting iBMC IPv4 Address (ipaddr)

Function

The **ipaddr** command is used to set the IPv4 address, subnet mask, and the gateway address for the iBMC.

Format

ipmcset -d ipaddr -v *<ipaddr> <mask>* [*gateway*]

Parameters

Parameter	Description	Value
ipaddr	Indicates the IPv4 address to be set for the iBMC.	An IPv4 address in the *xxx.xxx.xxx.xxx.* format.
mask	Indicates the subnet mask to be set for the iBMC.	An IPv4 address in the *xxx.xxx.xxx.xxx.* format.
gateway	Indicates the gateway address to be set for the iBMC.	An IPv4 address in the *xxx.xxx.xxx.xxx.* format.

Usage Guidelines

After the IP address is changed, the new IP address takes effect immediately, and you must use the new IP address to log in again.

Do not set *ipaddr* to a value from **10.0.0.0** to **10.0.0.3**, because these IP addresses are reserved for internal communication.

Example

Set the IP address of the iBMC management network interface to **192.168.0.25**, the subnet mask to **255.255.255.0**, and the gateway to **192.168.0.25**.

```
iBMC:/->ipmcset -d ipaddr -v 192.168.0.25 255.255.255.0 192.168.0.25
Set IP address successfully.
Set MASK address successfully.
Set GATEWAY successfully.
```

Query the changed IP address of the iBMC management network interface.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         : 1
Net Mode            : Manual
Net Type            : Dedicated
IPv4 Information     :
IP Mode             : static
IP Address          : 192.168.0.25
Subnet Mask         : 255.255.255.0
Default Gateway     : 192.168.0.25
MAC Address         : 00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           : dhcp
IPv6 Address        :
Default Gateway IPv6 :
Link-Local Address  : fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          : disabled
VLAN ID             : 1
```

4.3.3 Setting the IPv4 Mode of the iBMC (ipmode)

Function

The **ipmode** command is used to specify how the iBMC IPv4 address is allocated.

Format

ipmcset -d ipmode -v <dhcp | static>

Parameters

Parameter	Description	Value
dhcp	The DHCP server dynamically allocates an IP address to the iBMC.	–
static	The iBMC uses a static IP address.	–

Usage Guidelines

After the IPv4 mode is changed, the new configuration takes effect immediately.

Example

Enable the iBMC to use an IPv4 address dynamically allocated by the DHCP server.

```
iBMC:/->ipmcset -d ipmode -v dhcp
```

Query the iBMC IP address.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID        : 1
Net Mode           : Manual
Net Type        : Dedicated
IPv4 Information    :
IP Mode            : static
IP Address         : 192.168.0.25
Subnet Mask        : 255.255.255.0
Default Gateway     : 192.168.0.25
MAC Address         : 00:18:e1:c5:d8:66
IPv6 Information    :
IPv6 Mode          : dhcp
IPv6 Address       :
Default Gateway IPv6 :
Link-Local Address   : fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          : disabled
VLAN ID             : 1
```

📖 **NOTE**

You can run the **ipinfo** command to view that the new IP address that the iBMC management network interface obtained from the DHCP server is 192.168.0.12.

4.3.4 Setting the IPv4 Gateway Address of the iBMC (gateway)

Function

The **gateway** command is used to set the IPv4 gateway address of the iBMC.

Format

ipmcset -d gateway -v *<gateway>*

Parameters

Parameter	Description	Value
gateway	Indicates the IPv4 gateway address of the iBMC.	An IPv4 in the *xxx.xxx.xxx.xxx* format.

Usage Guidelines

After the gateway address is changed, the new gateway address takes effect immediately.

Example

Set the gateway address of the iBMC to **192.168.0.1**.

```
iBMC:/->ipmcset -d gateway -v 192.168.0.1
Set GATEWAY successfully.
```

Query the new gateway address of the iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID        : 1
Net Mode           : Manual
Net Type           : Dedicated
IPv4 Information    :
IP Mode            : static
IP Address         : 192.168.0.25
Subnet Mask        : 255.255.255.0
Default Gateway    : 192.168.0.25
MAC Address        : 00:18:e1:c5:d8:66
IPv6 Information    :
IPv6 Mode          : dhcp
IPv6 Address       :
Default Gateway IPv6 :
Link-Local Address : fe80::218:e1ff:fec5:d866/64
VLAN Information    :
VLAN State         : disabled
VLAN ID            : 1
```

4.3.5 Setting iBMC IPv6 Address (ipaddr6)

Function

The **ipaddr6** command is used to set the IPv6 address, prefix length, and gateway address of the iBMC.

Format

ipmcset -d ipaddr6 -v <*ipaddr6*|*prefixlen*> [*gateway6*]

Parameters

Parameter	Description	Value
ipaddr6	Indicates the IPv6 address to be set for the iBMC.	An IP address that is 128 bits in length consisting of eight 16-bit fields: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**. However, most IPv6 addresses do not occupy all 128 bits and can be abbreviated. In addition, the two-colon (::) notation can be used to represent contiguous 16-bit fields of zeros, and leading zeroes in a field can be omitted. For example, the IPv6 address **fc00:0db8:3c4d:0015:0000:0000:1a2f:1a2b** can be abbreviated as **fc00:db8:3c4d:15::1a2f:1a2b**.
prefixlen	Indicates the prefix length to be set for the iBMC.	0 to 128
gateway6	Indicates the IPv6 gateway address to be set for the iBMC.	An IP address that is 128 bits in length consisting of eight 16-bit fields: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**. However, most IPv6 addresses do not occupy all 128 bits and can be abbreviated. In addition, the two-colon (::) notation can be used to represent contiguous 16-bit fields of zeros, and leading zeroes in a field can be omitted. For example, the IPv6 address **fc00:0db8:3c4d:0015:0000:0000:1a2f:1a20** can be abbreviated as **fc00:db8:3c4d:15::1a2f:1a20**.

Usage Guidelines

- After an IPv6 address is changed, the new IP address takes effect immediately.
- In addition to the IPv6 address, **Link-Local Address** can be used to access the iBMC. You can run the **ipmcget** command to obtain **Link-Local Address**.

Example

Set the IPv6 address of the iBMC to **fc00::6516**, prefix length to **64**, and IPv6 gateway to **fc00::1**.

```
iBMC:/->ipmcset -d ipaddr6 -v fc00::6516/64 fc00::1
Set IPV6 address successfully.
Set IPV6 prefix successfully.
Set IPv6 GATEWAY6 successfully.
```

Query the changed IP address of the iBMC management network interface.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID          : 1
Net Mode             : Manual
Net Type           : Dedicated
IPv4 Information      :
IP Mode            : static
IP Address         : 192.168.0.25
Subnet Mask          : 255.255.0.0
Default Gateway      : 192.168.0.1
MAC Address          : 00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode          : static
IPv6 Address       : fc00::6516
Default Gateway IPv6  : fc00::1
Link-Local Address   : fe80::218:e1ff:fec5:d866/64
VLAN Information      :
VLAN State         : disabled
VLAN ID              : 1
```

4.3.6 Setting the IPv6 Mode of the iBMC (ipmode6)

Function

The **ipmode6** command is used to specify how the iBMC IPv6 address is allocated.

Format

ipmcset -d ipmode6 -v <dhcp | static>

Parameters

Parameter	Description	Value
dhcp	The DHCP server dynamically allocates an IP address to the iBMC.	-
static	The iBMC uses a static IP address.	-

Usage Guidelines

After the IPv6 mode is changed, the new configuration takes effect immediately.

Example

Enable the iBMC to use an IPv6 address dynamically allocated by the DHCP server.

```
iBMC:/->ipmcset -d ipmode6 -v dhcp
Set dhcp mode successfully.
```

Query the iBMC IP address.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID          : 1
Net Mode             : Manual
Net Type           : Dedicated
IPv4 Information      :
```

```
                IP Mode           : static
                IP Address        : 192.168.0.25
                Subnet Mask        : 255.255.0.0
                Default Gateway     : 192.168.0.1
                MAC Address        : 00:18:e1:c5:d8:66
                IPv6 Information    :
                IPv6 Mode         : static
                IPv6 Address       : fc00::6516
                Default Gateway IPv6 : fc00::1
                Link-Local Address  : fe80::218:e1ff:fec5:d866/64
                VLAN Information     :
                VLAN State        : disabled
                VLAN ID           : 1
                EthGroup ID        : 1
                Net Mode          : Manual
                Net Type          : Dedicated
                IPv4 Information    :
                IP Mode           : static
                IP Address        : 192.168.0.25
                Subnet Mask        : 255.255.0.0
                Default Gateway     : 192.168.0.1
                MAC Address        : 00:18:e1:c5:d8:66
                IPv6 Information    :
                IPv6 Mode         : static
                IPv6 Address       : fc00::6516
                Default Gateway IPv6 : fc00::1
                Link-Local Address   : fe80::218:e1ff:fec5:d866/64
                VLAN Information     :
                VLAN State        : disabled
                VLAN ID           : 1
```

4.3.7 Setting the IPv6 Gateway Address of the iBMC (gateway6)

Function

The **gateway6** command is used to set the IPv6 gateway address of the iBMC management network port.

Format

ipmcset -d gateway6 -v *<gateway6>*

Parameters

Parameter	Description	Value
gateway6	Indicates the IPv6 gateway address of the iBMC management network port.	An IP address that is 128 bits in length consisting of eight 16-bit fields: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**. However, most IPv6 addresses do not occupy all 128 bits and can be abbreviated. In addition, the two-colon (::) notation can be used to represent contiguous 16-bit fields of zeros, and leading zeroes in a field can be omitted. For example, the IPv6 address **fc00:0db8:3c4d:0015:0000:0000:1a2f:1a2b** can be abbreviated as **fc00:db8:3c4d:15::1a2f:1a2b**.

Usage Guidelines

After the gateway address is changed, the new gateway address takes effect immediately.

Example

Set the IPv6 gateway address of the iBMC to **fc00::1**.

```
iBMC:/->ipmcset -d gateway6 -v fc00::1
Set GATEWAY6 successfully.
```

Query the new gateway address of the iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID        : 1
Net Mode          : Manual
Net Type          : Dedicated
IPv4 Information    :
IP Mode           : static
IP Address         : 192.168.0.25
Subnet Mask        : 255.255.0.0
Default Gateway      : 192.168.0.1
MAC Address        : 00:18:e1:c5:d8:66
IPv6 Information    :
IPv6 Mode          : static
IPv6 Address       : fc00::6516
Default Gateway IPv6  : fc00::1
Link-Local Address    : fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State         : disabled
VLAN ID           : 1
```

4.3.8 Setting the Network Port Mode (netmode)

Function

The **netmode** command is used to set how the iBMC network port is specified.

Format

ipmcset -d netmode -v <*option*>

Parameters

Parameter	Description	Value
option	Indicates how the iBMC network port is specified.	• **1**: **Manual** • **2**: **Adaptive** Default value: **1**

Usage Guidelines

- If *option* is **1**, you need to manually set the iBMC management network port.
- If *option* is **2**, you need to specify the network ports for auto-negotiation. The dedicated iBMC port takes precedence over other network ports specified. If the dedicated iBMC network port is unavailable, a network port will be selected from the other network ports available.

Example

Enable the iBMC network port to be manually specified.

```
iBMC:/->ipmcset -d netmode -v 1
Set net mode Manual successfully.
```

Query the iBMC network port mode.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID        : 1
Net Mode           : Manual
Net Type         : Dedicated
IPv4 Information     :
IP Mode          : dhcp
IP Address       : 192.168.0.12
Subnet Mask        : 255.255.0.0
Default Gateway     : 192.168.0.25
MAC Address        : 00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode        : static
IPv6 Address       : fc00::65
Default Gateway IPv6  : fc00::1
Link-Local Address   : fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State       : disabled
VLAN ID          : 1
```

4.3.9 Setting the Active iBMC Port (activeport)

Function

The **activeport** command is used to set the active iBMC management network port.

Format

ipmcset -d activeport -v <*option*> [*portid*]

Parameters

Parameter	Description	Value
option	Port type	- **0**: dedicated network port - **1**: port on an LOM - **2**: port on a PCIe card **NOTE** The value range varies with the server model.
portid	Port number	The value range is 0 and 1 for a dual-port NIC, and 0 to 3 for a four-port NIC.

Usage Guidelines

You do not need to specify *portid* for a dedicated iBMC network port.

Example

Set the dedicated network port as the iBMC port.

```
iBMC:/->ipmcset -d activeport -v 0
Set active port successfully.
```

Query information about the iBMC port.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID        : 1
Net Mode           : Manual
Net Type           : Dedicated
IPv4 Information    :
IP Mode            : dhcp
IP Address         : 192.168.0.12
Subnet Mask        : 255.255.0.0
Default Gateway     : 192.168.0.25
MAC Address         : 00:18:e1:c5:d8:66
IPv6 Information    :
IPv6 Mode          : static
IPv6 Address        : fc00::65
Default Gateway IPv6 :  fc00::1
Link-Local Address   : fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State         : disabled
VLAN ID            : 1
```

4.3.10 Setting a VLAN ID for a Network Port (vlan)

Function

The **vlan** command is used to set a VLAN ID for a network controller sideband interface (NC-SI) port of the iBMC. NC-SI allows a network port to serve as an iBMC port.

Format

ipmcset -d vlan -v <off | *id*>

Parameters

Parameter	Description	Value
off	Disables VLAN.	-
vlanid	Identifies the VLAN to which the network port belongs.	● For RH8100 V3 and 8100 V5:1 to 4093 ● For other rack servers: 1 to 4094

Usage Guidelines

None

Example

#Set the VLAN ID of the iBMC management network port to **405**.

```
iBMC:/->ipmcset -d vlan -v 405
Set vlan state successfully.
```

Query VLAN information of the iBMC management network port.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID        : 1
Net Mode           : Manual
Net Type        : Dedicated
IPv4 Information      :
IP Mode           : dhcp
IP Address         : 192.168.0.12
Subnet Mask         : 255.255.0.0
Default Gateway       : 192.168.0.25
MAC Address         : 00:18:e1:c5:d8:66
IPv6 Information      :
IPv6 Mode          : static
IPv6 Address        : fc00::65
Default Gateway IPv6  : fc00::1
Link-Local Address   : fe80::218:e1ff:fec5:d866/64
VLAN Information      :
VLAN State         : enabled
VLAN ID           : 405
```

4.3.11 Querying and Redirecting the Serial Port (serialdir)

Function

The **serialdir** command is used to query and set serial port redirection.

Format

ipmcget -d serialdir

ipmcset -d serialdir -v *<option>*

Parameters

Parameter	Description	Value
<option>	Indicates the serial port to be used.	**0**: sets the serial port on the server panel as the system serial port. **1**: sets the serial port on the server panel as the iBMC serial port. **2**: sets the SOL port as the system serial port. **3**: sets the SOL port as the iBMC serial port. **4**: sets the serial port on the SDI V3 card panel as an SCCL port. **5**: sets the serial port on the SDI V3 card panel as an IMU port. **6**: sets the serial port on the SDI V3 card panel as an SCCL port. **7**: sets the serial port on the SDI V3 card panel as an IMU port. The value range of this parameter varies with the server model. Before setting the serial port, run the **ipmcget -d serialdir** command to query the value range of this parameter. **NOTE** - If no SDI V3 is installed in a server, *<option>* can be **0** to **3** only. - If one SDI V3 card is installed, the values **4** and **5** are available for setting the ports on the SDI V3 in I/O module 1 or 2. - If two SDI V3 cards are installed, the values **4** to **7** are available. The values **4** and **5** are used for setting the ports on the SDI V3 in I/O module 1, while the values **6** and **7** are for the ports on the SDI V3 in I/O module 2.

Usage Guidelines

- The redirection setting of the SOL port takes precedence over the setting of the serial port on the server panel. If you redirect the SOL port to the system or iBMC serial port that is currently redirected from the serial port on the server panel, the serial port on the server panel will become unavailable temporarily. The serial port on the server panel will restore its original setting only after the SOL port is disconnected.

- If the serial port (serial port on the panel or SOL serial port) is set as the system serial port, you can press **Del** during the OS startup process to enter the BIOS Setup screen.

Example

Set the serial port on the server panel as the iBMC serial port.

```
iBMC:/->ipmcset -d serialdir -v 1
Set serial port direction successfully.
```

Query the serial ports connected. The values of **Num** indicate the *<option>* *values.*

```
iBMC:/->ipmcget -d serialdir
Currently connected serial direction :
Num          Source              Destination
1            PANEL COM           BMC COM
4            SD100 PANEL COM5    SCCL COM5
```

4.3.12 Restarting the iBMC (reset)

Function

The **reset** command is used to restart the iBMC system.

Format

ipmcset -d reset

Parameters

None

Usage Guidelines

- In single-system mode, running the **restart** command on the primary iBMC will restart the primary iBMC and secondary iBMC simultaneously.

- In dual-system mode, the **restart** command will restart only the iBMC on which the command is executed.

Example

Restart the iBMC system.

```
iBMC:/->ipmcset -d reset
This operation will reboot iBMC system. Continue? [Y/N]:y
Resetting...
```

4.3.13 Upgrading the Firmware (upgrade)

Function

The **upgrade** command is used to upgrade the server firmware, which includes the iBMC, BIOS, SD card firmware, and complex programmable logic device (CPLD).

Format

ipmcset -d upgrade -v *<filepath>*

Parameters

Parameter	Description	Value
filepath	Specifies the absolute path of the upgrade file. **NOTE** Only the **xxx.hpm** file is supported.	Example value: **/tmp/image.hpm**.

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the upgrade file to the specified directory (for example **/tmp**) of the iBMC file system.

After the iBMC or SD card controller upgrade is complete, the iBMC restarts automatically for the upgrade to take effect.

- In single-system mode, running the **upgrade** command on the primary iBMC will upgrade the primary iBMC and secondary iBMC simultaneously.

- In dual-system mode, the **upgrade** command will upgrade only the iBMC on which the command is executed.

If you need to upgrade the iBMC from a version earlier than an intermediate version to a version later than the intermediate version, upgrade the iBMC to the intermediate version and then to the target version. If the upgrade to the intermediate version fails, restart the iBMC and try again. **Table 4-3** lists the server models and their intermediate versions. For example, if the iBMC source version of an RH1288 V3 is earlier than V257 and the target version is later than V257, you need to upgrade the iBMC to V257 and then to the target version. If the upgrade to V257 fails, restart the iBMC and try again.

Table 4-3 iBMC intermediate versions and compute node models

Intermediate Version	Model
257	RH1288 V3/RH2288H V3/RH5288 V3
260	RH5885H V3
262	RH2288 V3
270	RH5885 V3
276	RH8100 V3

Example

Upgrade the firmware.

```
iBMC:/->ipmcset -d upgrade -v /tmp/image.hpm
Please make sure the iBMC is working while upgrading!
```

```
Updating...
100%
Update successfully.
```

4.3.14 Capturing the Screen (printscreen)

Function

The **printscreen** command is used to capture a screenshot of the server screen.

Format

ipmcset -d printscreen [-v wakeup]

Parameters

Parameter	Description	Value
wakeup	Wakes up the system from sleep mode.	-

Usage Guidelines

To view the screenshot, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the **manualscreen.jpeg** from the **/tmp/web** directory to the local PC that supports the **.jpeg** files.

📖 **NOTE**

Only the last screenshot is saved if you run the **printscreen** command multiple times.

Example

Capture a screenshot of the server screen.

```
iBMC:/->ipmcset -d printscreen
Download print screen image to /tmp/manualscreen.jpeg successfully.
```

4.3.15 Rolling Back the iBMC Software (rollback)

Function

The **rollback** command is used to switch the iBMC firmware from the image file in the primary partition to the image file in the secondary partition.

Format

ipmcset -d rollback

Parameters

None

Usage Guidelines

- In single-system mode, run the **rollback** command on the primary iBMC will roll back the primary iBMC and secondary iBMC simultaneously.
- In dual-system mode, the **rollback** command will roll back only the iBMC on which the command is executed.
- This command switches the iBMC firmware from the image file in the primary partition to the image file in the secondary partition. If the image files in the primary and secondary partitions have the same version, the version does not change after this command is executed.

Example

Roll back the iBMC software.

```
iBMC:/->ipmcset -d rollback
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Set rollback successfully, system will reboot soon!
```

4.3.16 Querying the Result of Rolling Back the iBMC Software (rollbackstatus)

Function

The **rollbackstatus** command is used to query the result of rolling back the iBMC software.

Format

ipmcget -d rollbackstatus

Parameters

None

Usage Guidelines

None

Example

Query the result of rolling back the iBMC software.

```
iBMC:/->ipmcget -d rollbackstatus
Last rollback success!
```

4.3.17 Setting Service State (service -d state)

Function

The **service -d state** command is used to set service state for the iBMC.

Format

ipmcset -t service -d state -v *<option>* **<enabled | disabled>**

Parameters

Parameter	Description	Value
option	Indicates the service type.	• SSH • SNMP • KVM • VNC • VMM • Video • HTTP • HTTPS • RMCP • RMCP+ • SSDP
enabled	Enables a service	-
disabled	Disables a service	-

Usage Guidelines

The value of *option* is not case-sensitive.

Only V5 servers support the VNC service.

Example

Enable the HTTP service.

```
iBMC:/->ipmcset -t service -d state -v http enabled
Set http service state(enabled) successfully.
```

☐ **NOTE**

Enabling the HTTP service may pose security risks.

4.3.18 Setting the Service Port Number (service -d port)

Function

The **service -d port** command is used to set the port number for a service.

Format

ipmcset -t service -d port -v *<option>* *<port1value>* [*port2value*]

Parameters

Parameter	Description	Value
option	Service type	- SSH - SNMP - KVM - VNC - VMM - Video - HTTP - HTTPS - RMCP
port1value	Port number	1 to 65535
port2value	Service port number. This port number is available only for the RMCP service.	1 to 65535

Usage Guidelines

- If the web server (HTTP) or (HTTPS) port number is set to **65535**, Google Chrome cannot set up a session over this port.

- Only V5 servers support the VNC service.

Example

Set the HTTPS port to **443**.

```
iBMC:/->ipmcset -t service -d port -v https 443
Set https service port to 443 successfully.
```

4.3.19 Querying Service Information (service -d list)

Function

The **service -d list** command is used to query information about the services.

Format

ipmcget -t service -d list

Parameters

None

Usage Guidelines

Only V5 servers support the VNC service.

Example

Query service information.

```
iBMC:/->ipmcget -t service -d list
service name    | state        | port
SSH        | Enabled     | 22
SNMP       | Enabled     | 161
KVM        | Enabled     | 2198
VNC        | Disabled    | 5900
VMM        | Enabled     | 8208
Video      | Enabled     | 2199
HTTP       | Enabled     | 80
HTTPS      | Enabled     | 443
RMCP       | Disabled    | 623,664
RMCP+      | Enabled     | 623,664
SSDP       | Disabled    | 1900
```

4.3.20 Setting the Enablement Status of the Login Security Message (securitybanner -d state)

Function

The **securitybanner -d state** is used to set whether to display the login security message on the iBMC login page.

Format

ipmcset -t securitybanner -d state -v <**enabled** | **disabled**>

Parameters

Parameter	Description	Value
enabled	Indicates that the security message will be displayed on the login page.	–
disabled	Indicates that no security message will be displayed on the login page.	–

Usage Guidelines

None

Example

Configure iBMC to display the security message on the login page.

```
iBMC:/->ipmcset -t securitybanner -d state -v enabled
Enable login security banner state successfully.
```

4.3.21 Customizing the Login Security Message (securitybanner -d content)

Function

The **securitybanner -d content** command is used to set the security message displayed on the iBMC login page.

Format

ipmcset -t securitybanner -d content -v <**default** | *"option"*>

Parameters

Parameter	Description	Value
default	Indicates that the default security message is used.	-
option	Specifies the customized security message.	A string of 0 to 1600 characters

Usage Guidelines

None

Example

Set the login security message to the default message.

```
iBMC:/-> ipmcset -t securitybanner -d content -v default
Set login security banner content successfully.
```

4.3.22 Querying the Login Security Message (securitybanner -d info)

Function

The **securitybanner -d info** command is used to query the security message displayed on the iBMC login page.

Format

ipmcget -t securitybanner -d info

Parameters

None

Usage Guidelines

None

Example

Query the login security message.

```
iBMC:/-> ipmcget -t securitybanner -d info
Login security banner information state: enabled.

Login security banner information:
WARNING! This system is PRIVATE and PROPRIETARY and may only be accessed by authorized users.
Unauthorized use of the system is prohibited. The owner, or its agents, may monitor any activity or
communication on the system. The owner, or its agents, may retrieve any information stored within the
system. By accessing and using the system, you are consenting to such monitoring and information retrieval
for law enforcement and other purposes.
```

4.3.23 Importing an SSL Certificate (certificate -d import)

Function

The **certificate -d import** command is used to import a Secure Sockets Layer (SSL) certificate to the iBMC.

Format

ipmcset -t certificate -d import -v <*filepath | file_URL*> <*type*> [*passphrase*]

Parameters

Parameter	Description	Value
filepath	Specifies the directory in which the SSL certificate is to be imported. **NOTE** The certificate must be in the *.pfx or *.p12 format and cannot exceed 100 KB.	Absolute path of the certificate on the iBMC, for example, **/tmp/test.pfx**.

Parameter	Description	Value

file_URL	Specifies the URL of the SSL certificate to be imported.	Format:
		 protocol://username:password@IP:[port]/ directory/filename
		 Where:
		 • *protocol* must be **https**, **sftp**, **cifs**, or **scp**.
		   NOTE
		     The iBMC supports only Server Message Block (SMB) V1.0.
		 • *username* indicates the user name used to log in to the target server.
		 • *password* indicates the password used to log in to the target server.
		 • *IP:[port]* indicates the IP address and port number of the target server.
		 • *directory/filename* indicates the absolute path of the SSL certificate on the target server.
		 For example, **https://root:Test12# $@10.10.10.1:443/tmp/test.pfx**.

type	Specifies the type of the SSL certificate.	It has a fixed value of **1**.
passphrase	Specifies the password for the SSL certificate.	This password can be empty.

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the SSL certificate to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Import an SSL certificate.

```
iBMC:/-> ipmcset -t certificate -d import -v /tmp/test-01.pfx 1 Test12#$
Import certificate successfully
Reset iBMC for the certificate to take effect.
```

4.3.24 Querying SSL Certificate Information (certificate -d info)

Function

The **certificate -d info** command is used to query SSL certificate information.

Format

ipmcget -t certificate -d info

Parameters

None

Usage Guidelines

None

Example

Query SSL certificate information.

```
iBMC:/-> ipmcget -t certificate -d info
SSL Certificate Information:
Issued     To: CN=Server, OU=IT, O=Test, L=ShenZhen, S=GuangDong, C=CN
Issued     By: CN=Server, OU=IT, O=Test, L=ShenZhen, S=GuangDong, C=CN
Valid   From: Jul 25 2014 GMT
Valid     To: Jul 22 2024 GMT
Serial Number: 07
```

4.3.25 Exporting the Configuration File (config -d export)

Function

The **config -d export** command is used to export iBMC, BIOS, and RAID controller card configuration files.

Format

ipmcget -t config -d export -v *<filepath | file_URL>*

Parameters

Parameter	Description	Value
filepath	Specifies the directory to which the configuration file is to be exported.	Absolute path of the configuration file on the iBMC. Example value: **/tmp/config.xml**

Parameter	Description	Value
file_URL	Specifies the URL of the configuration file to be exported.	Format: *protocol://username:password@IP:[port]/directory/filename* Where: • *protocol* must be **https**, **sftp**, **cifs**, **scp**, or **nfs**. **NOTE** • The iBMC supports only Server Message Block (SMB) V1.0. • When the NFS protocol is used, the storage path cannot contain the *username:password@* field. When the HTTPS is used, the *username:password@* field is optional in the storage path. When the CIFS protocol is used, the storage path must contain the *username:password@* field. • If the NFS protocol is used, the path cannot contain **username:password@**. If other protocols are used, the path must contain **username:password@**. • *username* indicates the user name for logging in to the target server. • *password* indicates the password for logging in to the target server. • *IP:[port]* indicates the IP address and port number of the target server. • *directory/filename* indicates the absolute path of the configuration file on the target server. Example value: **https://root:Test12#$@10.10.10.1:443/tmp/config.xml**

Usage Guidelines

To view the weak password dictionary, use a file transfer tool supporting SFTP (for example WinSCP) to transfer the file (for example **config.xml**) from **/tmp/config.xml** to the local PC.

Example

Export the configuration file.

```
iBMC:/-> ipmcget -t config -d export -v /tmp/config.xml
NOTE: The exported RAID Controller configurations are valid only if they are exported after the POST is complete.
Collecting configuration...
100%
Export configuration successfully.
```

4.3.26 Importing the Configuration File (config -d import)

Function

The **config -d import** command is used to import the iBMC, BIOS, and RAID controller card configuration files.

Format

ipmcset -t config -d import -v *<filepath | file_URL>*

Parameters

Parameter	Description	Value
filepath	Specifies the directory to which the configuration file is to be imported.	Absolute path of the configuration file on the iBMC. Example value: **/tmp/config.xml**

Parameter	Description	Value

file_URL	Specifies the URL of the configuration file to be imported.	Format:
		protocol://username:password@IP:[port]/ directory/filename
		Where:
		
		• *protocol* must be **https**, **sftp**, **cifs**, **scp**, or **nfs**.
		   NOTE
		    • The iBMC supports only Server Message Block (SMB) V1.0.
		    • When the NFS protocol is used, the storage path cannot contain the *username:password@* field. When the HTTPS is used, the *username:password@* field is optional in the storage path. When the CIFS protocol is used, the storage path must contain the *username:password@* field.
		    • If the NFS protocol is used, the path cannot contain **username:password@**. If other protocols are used, the path must contain **username:password@**.
		• *username* indicates the user name for logging in to the target server.
		• *password* indicates the password for logging in to the target server.
		• *IP:[port]* indicates the IP address and port number of the target server.
		• *directory/filename* indicates the absolute path of the configuration file on the target server.
		Example value: **https://root:Test12# $@10.10.10.1:443/tmp/config.xml**

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the configuration file to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Import the configuration file.

```
iBMC:/-> ipmcset -t config -d import -v /tmp/testconfig.xml
Setting configuration...
100%
Import configuration successfully.
Reset OS for the BIOS config to take effect.
```

4.3.27 Importing the CRL File (crl)

Function

The **crl** command is used to import the certificate revocation list (CRL) file, which is used to verify the integrity of the upgrade package.

Format

ipmcset -d crl -v *<localpath|URL> <type>*

Parameters

Parameter	Description	Value
localpath	Specifies the directory in which the CRL file is imported on the iBMC. **NOTE** The file must be in the ***.crl** format and smaller than 100 KB.	Absolute directory on the iBMC, for example, **/tmp/cms.crl**.

Parameter	Description	Value

URL	Specifies the URL of the CRL file to be imported.	The format is as follows:
		
		protocol://username:password@IP:[port]/directory/filename
		
		Where,
		
		● *protocol* must be **https**, **sftp**, **cifs**, **scp**, or **nfs**.
		NOTE
		   ● The iBMC supports only Server Message Block (SMB) V1.0.
		   ● When the NFS protocol is used, the storage path cannot contain the *username:password@* field. When the HTTPS is used, the *username:password@* field is optional in the storage path. When the CIFS protocol is used, the storage path must contain the *username:password@* field.
		   ● If the NFS protocol is used, the path cannot contain **username:password@**. If other protocols are used, the path must contain **username:password@**.
		● *username* indicates the user name for logging in to the target server.
		● *password* indicates the password for logging in to the target server.
		● *IP:[port]* indicates the IP address and port number of the target server.
		● *directory/filename* indicates the absolute directory in which the CRL file is stored on the target server.
		
		Example value: **https://root:Test12#$@10.10.10.1:443/tmp/cms.crl**

type	Specifies the CRL file type.	It has a fixed value of **1**.

Usage Guidelines

This command is available only for V5 servers.

Before running this command, use a file transfer tool supporting SFTP (for example WinSCP) to transfer the file to be imported to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Import the CRL file.

```
iBMC:/-> ipmcset -d crl -v /tmp/cms.crl 1
Import CRL file successfully.
```

4.3.28 Mounting a File to the Virtual CD-ROM Drive (vmm -d connect)

Function

The **vmm -d connect** command is used to mount a file to the virtual CD-ROM drive.

Format

ipmcset -t vmm -d connect -v *<file_URL>*

Parameters

Parameter	Description	Value
file_URL	Specifies the source directory of the file to be mounted.	Format: *protocol://[username:password@]IP:[port]/directory/filename* Where: • *protocol* must be **nfs**, **cifs**, or **https**. **NOTE** • Only iBMC V300 and later versions support **https**. • The iBMC supports only Server Message Block (SMB) V1.0. • If the NFS protocol is used, the path cannot contain ***username:password@***. If other protocols are used, the path must contain ***username:password@***. • *username* indicates the user name used to log in to the target server. • *password* indicates the password used to log in to the target server. • *IP:[port]* indicates the IP address and port number of the target server. • *directory/filename* indicates the absolute directory in which the file is to be stored on the target server. For example, nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso. **NOTE** The file_URL can contain up to 255 characters.

Usage Guidelines

None

Example

Mount **rhel-server-6.3-x86_64-dvd.iso** to the virtual CD-ROM drive.

iBMC:/-> **ipmcset -t vmm -d connect -v nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso**

Connect virtual media...

....

Connect virtual media successfully.

4.3.29 Disconnecting the Virtual CD-ROM Drive (vmm -d disconnect)

Function

The **vmm -d disconnect** command is used to disconnect the virtual CD-ROM drive.

Format

ipmcset -t vmm -d disconnect

Parameters

None

Usage Guidelines

None

Example

Disconnect the virtual CD-ROM drive.

iBMC:/-> **ipmcset -t vmm -d disconnect**
Disconnect virtual media...

.....

Disconnect virtual media successfully.

4.3.30 Querying Virtual Media Information (vmm -d info)

Function

The **vmm -d info** command is used to query the iBMC virtual media information.

Format

ipmcget -t vmm -d info

Parameters

None

Usage Guidelines

None

Example

Query virtual media information.

```
iBMC:/-> ipmcget -t vmm -d info
Virtual Media Information:
Maximum Number of Virtual Media Sessions:     1
Number of Activated Sessions          :    0
Activated Sessions URL              :
```

4.3.31 Querying and Setting the Cooling Power Mode (coolingpowermode)

Function

The **coolingpowermode** command is used to set and query the server cooling power mode.

Format

ipmcget -t maintenance -d coolingpowermode

ipmcset -t maintenance -d coolingpowermode -v *<option>*

Parameters

Parameter	Parameter Description	Value
option	Indicates the server cooling power mode.	• **0**: indicates the low cooling power mode. • **1**: indicates the high cooling power mode.

Usage Guidelines

This command can be used only on the RH8100 V3 and 8100 V5. In dual-system mode, the fan cooling power mode can be set only on the active system.

Example

Set the server cooling power mode to the low cooling power mode.

```
iBMC:/-> ipmcset -t maintenance -d coolingpowermode -v 0
Set cooling power mode to [Power saving mode] successfully.
```

Query the current cooling power mode.

```
iBMC:/-> ipmcget -t maintenance -d coolingpowermode
Power saving mode
```

4.4 Trap Commands

4.4.1 Querying and Setting the SNMP Trap State (trap -d state)

Function

The **trap -d state** command is used to query and set the SNMP trap state.

Format

ipmcget -t trap -d state [-v *destination*]

ipmcset -t trap -d state -v [*destination*] <**disabled** | **enabled**>

Parameters

Parameter	Description	Value
destination	Identifies an SNMP trap destination.	- Value range: 1 to 4 - If this parameter is not specified, the command is used to set the trap function.
disabled	Disables SNMP trap.	-
enabled	Enables SNMP trap.	-

Usage Guidelines

- To set trap for a specific channel, specify *destination*. The value range of *destination* is 1 to 4.
- To enable or disable the trap function, leave *destination* unspecified.

Example

Disable SNMP trap destination 1.

```
iBMC:/->ipmcset -t trap -d state -v 1 disabled
Set trap dest1 disabled successfully.
```

Query the state of SNMP trap destination 1.

```
iBMC:/->ipmcget -t trap -d state -v 1
trap dest1 state : disabled
```

4.4.2 Setting the SNMP Trap Port Number (trap -d port)

Function

The **trap -d port** command is used to set the SNMP trap port number of the iBMC.

Format

ipmcset -t trap -d port -v <*destination*> <*portvalue*>

Parameters

Parameter	Description	Value
destination	Identifies an SNMP trap destination.	Value range: 1 to 4
portvalue	Specifies the SNMP trap port number.	Value range: 1 to 65535 Default value: **162**

Usage Guidelines

None

Example

Set the port number for SNMP trap destination 1 to **1024**.

```
iBMC:/->ipmcset -t trap -d port -v 1 1024
Set trap dest1 port successfully.
```

4.4.3 Setting the SNMP Trap Community Name (trap -d community)

Function

The **trap -d community** command is used to set the SNMP trap community name.

Format

ipmcset -t trap -d community

Parameters

Parameter	Description	Value

Community	Specifies the SNMP trap community string.	Default value: **TrapAdmin12#$**
		
		The value range varies depending on whether password complexity check is enabled.
		
		● If password complexity check is disabled, the value is a string of 1 to 18 characters consisting of letters, digits, and special characters (excluding spaces).
		
		● If password complexity check is enabled, the value must meet the following requirements:
		
		  – Contain 8 to 18 characters
		
		  – Contain at least two of the following: uppercase letters A to Z, lowercase letters a to z, digits 0 to 9
		
		  – Contain at least one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/?
		
		  – Cannot contain spaces.

Usage Guidelines

None

Example

Set the SNMP trap community name to **mytrap**.

```
iBMC:/->ipmcset -t trap -d community
New Community:
Confirm Community:
Set SNMP trap community successfully.
```

4.4.4 Setting the SNMP Trap IP Address (trap -d address)

Function

The **trap -d address** command is used to set the SNMP trap IP address.

Format

ipmcset -t trap -d address -v *<destination> <ipaddr>*

Parameters

Parameter	Description	Value
destination	Identifies an SNMP trap destination.	1 to 4
ipaddr	Specifies the IP address for receiving SNMP trap messages.	It can be an IPv4 address (in **xxx.xxx.xxx.xxx** format), an IPv6 address (in **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx** format), or empty (in ""format).

Usage Guidelines

If *ipaddr* is empty, this command is used to clear the IP address.

Example

Set the IP address for receiving SNMP trap messages to **10.10.10.10**.

```
iBMC:/->ipmcset -t trap -d address -v 1 10.10.10.10
Set trap dest1 address successfully.
```

Clear the IP address of SNMP trap destination 1.

```
iBMC:/->ipmcset -t trap -d address -v 1 ""
Set trap dest1 address successfully.
```

4.4.5 Querying SNMP Trap Destination Information (trap -d trapiteminfo)

Function

The **trap -d trapiteminfo** command is used to query SNMP trap destination information, which includes the SNMP trap state, IP address, and port number.

Format

ipmcget -t trap -d trapiteminfo

Parameters

None

Usage Guidelines

None

Example

Query SNMP trap destination information.

```
iBMC:/->ipmcget -t trap -d trapiteminfo

TrapItem Num   | state    | port    | alert address
1              | enabled  | 1024    | 10.10.10.10
2              | disabled | 162     |
3              | disabled | 162     |
4              | disabled | 162     |
```

4.4.6 Querying and Setting the SNMP Trap Version (trap -d version)

Function

The **trap -d version** command is used to query and set the SNMP trap version.

Format

ipmcget -t trap -d version

ipmcset -t trap -d version -v *<V1 | V2C | V3>*

Parameters

Parameter	Description	Value
V1	Indicates SNMPv1.	-
V2C	Indicates SNMPv2c.	-
V3	Indicates SNMPv3.	-

Usage Guidelines

The default value is *V1*. However, *V3* is recommended. Exercise caution when using *V1* and *V2C*, because they pose security risks.

Example

Set the SNMP trap version to SNMPv2c.

```
iBMC:/->ipmcset -t trap -d version -v V2C
Set trap V2C success.
```

Query the SNMP trap version.

```
iBMC:/->ipmcget -t trap -d version
Trap version : V2C
```

4.4.7 Querying and Setting the SNMP Trap Alarm Severities (trap -d severity)

Function

The **trap -d severity** command is used to query and set the severities of alarms to be sent through SNMP trap messages.

Format

ipmcget -t trap -d severity

ipmcset -t trap -d severity -v *<level>*

Parameters

Parameter	Description	Value
level	Specifies the severities of alarms to be sent through SNMP trap messages.	• **none**: No alarm is sent. • **all**: All alarms and events are sent. • **normal**: Only events are sent. • **minor**: Only minor alarms are sent. • **major**: Only major alarms are sent. • **critical**: Only critical alarms are sent.

Usage Guidelines

Multiple severities can be specified, for example, **ipmcset -t trap -d severity -v normal minor**.

Example

Enable minor alarms to be sent through SNMP trap messages.

```
iBMC:/->ipmcset -t trap -d severity -v minor
Set trap severity successfully.
```

Query the severity of the alarms sent through SNMP trap messages.

```
iBMC:/->ipmcget -t trap -d severity
Trap severity :  minor
```

4.4.8 Querying and Setting the SNMPv3 Trap User (trap -d user)

Function

The **trap -d user** command is used to query and set the SNMPv3 trap user.

Format

ipmcget -t trap -d user

ipmcset -t trap -d user -v *<username>*

Parameters

Parameter	Description	Value
username	Indicates the SNMPv3 trap user.	It must be a user name that has been defined already.

Usage Guidelines

The same user name and password must be configured on the SNMP network management station (NMS).

By default, the trap V3 user name is **root** for V3 servers and **Administrator** for V5 servers.

Example

\# Set the SNMPv3 trap user to **root**.

```
iBMC:/->ipmcset -t trap -d user -v root
Set trap user root successfully.
```

\# Query the SNMPv3 trap user.

```
iBMC:/->ipmcget -t trap -d user
Trap user : root
```

4.4.9 Querying and Setting SNMPv3 Authentication and Privacy Protocols (trap -d protocol)

Function

The **trap -d protocol** command is used to query and set the authentication and privacy protocols for SNMPv3 trap.

Format

ipmcget -t trap -d protocol

ipmcset -t trap -d protocol -v *<option>*

Parameters

Parameter	Description	Value
option	Specifies the authentication and privacy protocols for SNMPv3 trap.	Value: ● **1**: The authentication protocol is MD5, and the privacy protocol is DES. ● **2**: The authentication protocol is MD5, and the privacy protocol is AES. ● **3**: The authentication protocol is SHA, and the privacy protocol is DES. ● **4**: The authentication protocol is SHA, and the privacy protocol is AES. Default value: **4**

Usage Guidelines

● The same authentication and privacy protocols must be configured on the SNMP server.

● The configured authentication and privacy protocols also apply to SNMPv3 at the same time.

● Using **MD5** and **DES** may pose security risks. You are advised to use **SHA** and **AES**.

Example

Set the SNMPv3 trap authentication and privacy protocols.

```
iBMC:/->ipmcset -t trap -d protocol -v 4
Set SNMP trap authentication and privacy protocol successfully.
```

Query the SNMPv3 trap authentication and privacy protocols.

```
iBMC:/->ipmcget -t trap -d protocol
Trap protocol     :
  Authentication  : SHA
  Privacy         : AES
```

4.4.10 Querying and Setting the SNMP Trap Mode (trap -d mode)

Function

The **trap -d mode** command enables you to query and set the SNMP trap mode.

Format

ipmcget -t trap -d mode

ipmcset -t trap -d mode -v *<option>*

Parameters

Parameter	Description	Value
option	Indicates the SNMP trap mode.	● **0** indicates the SNMP trap mode is Event Code. ● **1** indicates the SNMP trap mode is OID. ● **2** indicates the SNMP trap mode is Precise Alarm (recommended).

Usage Guidelines

Precise Alarm (recommended) provides more accurate information than **OID** and **Event Code**. For details, see the iBMC SNMP API description.

Example

Set the SNMP trap mode to Event Code.

```
iBMC:/->ipmcset -t trap -d mode -v 0
Set trap mode Event Code success.
```

Query the current SNMP trap mode.

```
iBMC:/->ipmcget -t trap -d mode
Trap mode: Event Code
```

4.5 Syslog Commands

4.5.1 Querying and Setting Syslog (syslog -d state)

Function

The **syslog -d state** command is used to query and set the syslog feature for the iBMC.

Format

ipmcget -t syslog -d state [-v *destination*]

ipmcset -t syslog -d state -v [*destination*] <**disabled** | **enabled**>

Parameters

Parameter	Description	Value
destination	Identifies the channel sending syslog messages.	• Value range: 1 to 4 • If this parameter is not specified, the command is used to set the syslog function.
disabled	Disables syslog.	-
enabled	Enables syslog.	-

Usage Guidelines

- To set syslog for a specific channel, enable the syslog function first.
- To set syslog for a specific channel, specify *destination*. The value range of *destination* is 1 to 4.

Example

Enables syslog.

```
iBMC:/->ipmcset -t syslog -d state -v enabled
Set syslog enabled successfully.
```

Query the syslog status.

```
iBMC:/->ipmcget -t syslog -d state
syslog state: enabled
```

Disable syslog for channel 1.

```
iBMC:/->ipmcset -t syslog -d state -v 1 disabled
Set syslog dest1 disabled successfully.
```

Query the syslog status of channel 1.

```
iBMC:/-> ipmcget -t syslog -d state -v 1
syslog dest1 state: disabled
```

4.5.2 Querying and Setting the Certificate Authentication Mode (syslog -d auth)

Function

The **syslog -d auth** is used to query and set the certificate authentication mode.

Format

ipmcget -t syslog -d auth

ipmcset -t syslog -d auth -v *<option>*

Parameters

Parameter	Description	Value
option	Specifies the certificate authentication mode.	• **1**: one-way authentication • **2**: mutual authentication

Usage Guidelines

- One-way authentication: Only the syslog server certificate is authenticated.
- Mutual authentication: Certificates of both the syslog server and the client are authenticated.

Example

Set the certificate authentication mode to mutual authentication.

```
iBMC:/->ipmcset -t syslog -d auth -v 2
Set syslog auth type successfully.
```

Query the current certificate authentication mode.

```
iBMC:/-> ipmcget -t syslog -d auth
Syslog auth type: mutual authentication
```

4.5.3 Querying and Setting the Syslog Host Identifier (syslog -d identity)

Function

The **syslog -d identity** command is used to query and set the host identifier used for syslog reporting.

Format

ipmcget -t syslog -d identity

ipmcset -t syslog -d identity -v *<option>*

Parameters

Parameter	Description	Value
option	Specifies the host identifier to be used.	• **1**: board serial number • **2**: product asset tag • **3**: host name

Usage Guidelines

None

Example

Set the syslog host identifier to the host name.

```
iBMC:/-> ipmcset -t syslog -d identity -v 3
Set syslog identity successfully.
```

Query the syslog host identifier.

```
iBMC:/-> ipmcget -t syslog -d identity
Syslog identity: host name
```

4.5.4 Querying and Setting the Protocol Type (syslog -d protocol)

Function

The **syslog -d protocol** command is used to query and set the protocol used to send syslog messages.

Format

ipmcget -t syslog -d protocol

ipmcset -t syslog -d protocol -v <*option*>

Parameters

Parameter	Description	Value
option	Specifies the protocol used.	**1**: UDP UDP is a connectionless protocol that does not set up a dedicated end-to-end connection before data is transmitted. **2**: TCP TCP is a connection-oriented protocol that sets up a reliable end-to-end connection before data is transmitted. **3**: TLS TLS is a connection-oriented protocol that ensures confidentiality and integrity of the data transmitted.

Usage Guidelines

None

Example

Use TLS to transfer syslog messages.

```
iBMC:/-> ipmcset -t syslog -d protocol -v 3
Set syslog protocol successfully.
```

Query the protocol used to transfer syslog messages.

```
iBMC:/-> ipmcget -t syslog -d protocol
Syslog protocol: TLS
```

4.5.5 Querying and Setting the Log Levels (syslog -d severity)

Function

The **syslog -d severity** command is used to query and set the levels of the logs reported over syslog.

Format

ipmcget -t syslog -d severity

ipmcset -t syslog -d severity -v *<level>*

Parameters

Parameter	Description	Value
level	Specifies the levels of logs to be reported.	• **none**: no alarms will be reported. • **normal**: reports alarms and event logs. • **minor**: reports minor, major, and critical alarms. • **major**: reports major and critical alarms. • **critical**: reports critical alarms.

Usage Guidelines

None.

Example

Set the log level to **critical** for syslog reporting.

```
iBMC:/->ipmcset -t syslog -d severity -v critical
Set syslog severity successfully.
```

Query the levels of logs to be sent over syslog.

```
iBMC:/-> ipmcget -t syslog -d severity
Syslog severity:  critical
```

4.5.6 Querying and Uploading the Server Root Certificate (syslog -d rootcertificate)

Function

The **syslog -d rootcertificate** command is used to upload the syslog server root certificate to iBMC or query the current root certificate information.

Format

ipmcget -t syslog -d rootcertificate

ipmcset -t syslog -d rootcertificate -v *<filepath>*

Parameters

Parameter	Description	Value
filepath	Specifies the absolute path of the syslog server root certificate on the iBMC.	For example, */tmp/rootcertificate.cer*

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the custom root certificate to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Upload the server root certificate.

```
iBMC:/-> ipmcset -t syslog -d rootcertificate -v /tmp/rootcertificate.cer
Set syslog root certificate successfully.
```

Query the server root certificate information.

```
iBMC:/-> ipmcget -t syslog -d rootcertificate
Server Root Certificate:
Issued    To: CN=SERVER, OU=IT, O=Test, L=, S=GD, C=CH
Issued    By: CN=Test, OU=IT, O=Test, L=ShenZhen, S=GuangDong, C=CN
Valid   From: Mar 24 2016 GMT
Valid    To: Mar 24 2017 GMT
Serial Number: 0b
```

4.5.7 Querying and Uploading the Local Certificate (syslog -d clientcertificate)

Function

The **syslog -d clientcertificate** command is used to upload the syslog client (local) certificate to iBMC or query the current local certificate information.

Format

ipmcget -t syslog -d clientcertificate

ipmcset -t syslog -d clientcertificate -v *<filepath> <password>*

Parameters

Parameter	Description	Value
filepath	Specifies the absolute path of the client certificate on the iBMC.	For example, **/tmp/rootcertificate.cer**
password	Specifies the password used to decrypt the client certificate.	The password is automatically generated when the certificate server is used to generate a local certificate.

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the local certificate to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Upload the local certificate.

```
iBMC:/-> ipmcset -t syslog -d client -v /tmp/clientcertificate.pfx syslogpw
Set syslog client certificate successfully.
```

Query local certificate information.

```
iBMC:/-> ipmcget -t syslog -d clientcertificate
Syslog Client Certificate Information:
Issued    To: CN=Server, OU=IT, O=it, L=ShenZhen, S=GuangDong, C=CN
Issued    By: CN=Administrator, OU=it3, O=it3, L=, S=guangdong2, C=cn
Valid   From: Feb 17 2015 GMT
Valid     To: Feb 17 2016 GMT
Serial Number: 25
```

4.5.8 Setting the Syslog Server Address (syslog -d address)

Function

The **syslog -d address** command is used to set the syslog server address.

Format

ipmcset -t syslog -d address -v *<destination> <ipaddr>*

Parameters

Parameter	Description	Value
destination	Specifies the number of a syslog reporting channel.	1 to 4

Parameter	Description	Value
ipaddr	Specifies the syslog server address.	It can be an IPv4 or IPv6 address, a domain name, or empty.

Usage Guidelines

If *ipaddr* is empty, this command is used to clear the IP address.

Example

Set the syslog server address to **host** for channel 1.

```
iBMC:/-> ipmcset -t syslog -d address -v 1 host
Set syslog dest1 address successfully.
```

Query the syslog server address.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num      | state    | port    | dest address       | log type
1             | disabled | 0       | host               | operationlogs securitylogs eventlogs
2             | disabled | 0       |                    | operationlogs securitylogs eventlogs
3             | disabled | 0       |                    | operationlogs securitylogs eventlogs
4             | disabled | 0       |                    | operationlogs securitylogs eventlogs
```

Clear the IP address of the syslog server of channel 1.

```
iBMC:/-> ipmcset -t syslog -d address -v 1 ""
Set syslog dest1 address successfully.
```

4.5.9 Setting the Syslog Server Port Number (syslog -d port)

Function

The **syslog -d port** command is used to set the syslog server port number.

Format

ipmcset -t syslog -d port -v *<destination> <portvalue>*

Parameters

Parameter	Description	Value
destination	Specifies the number of a syslog reporting channel.	1 to 4
portvalue	Specifies the syslog server port number.	1 to 65535

Usage Guidelines

None

Example

Set the syslog server port number to **65535** for channel 1.

```
iBMC:/-> ipmcset -t syslog -d port -v 1 65535
Set syslog dest1 port successfully.
```

Query the syslog server port numbers.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num     | state    | port     | dest address     | log type
1            | disabled | 65535    | host             | operationlogs securitylogs eventlogs
2            | disabled | 0        |                  | operationlogs securitylogs eventlogs
3            | disabled | 0        |                  | operationlogs securitylogs eventlogs
4            | disabled | 0        |                  | operationlogs securitylogs eventlogs
```

4.5.10 Setting Logs Types for Reporting (syslog -d logtype)

Function

The **syslog -d logtype** command is used to set the types of logs to be reported as syslog packets.

Format

ipmcset -t syslog -d logtype -v *<destination> <type>*

Parameters

Parameter	Description	Value
destination	Specifies the number of a syslog reporting channel.	1 to 4
type	Specifies the types of logs to be reported.	**none**: No logs will be reported. **all**: All logs will be reported. **operationlogs**: Operations logs will be reported. **securitylogs**: Security logs will be reported. **eventlogs**: Event logs will be reported.

Usage Guidelines

None

Example

Set the log types for channel 4 to operation and event logs.

```
iBMC:/-> ipmcset -t syslog -d logtype -v 4 operationlogs eventlogs
Set syslog log type successfully.
```

Query the types of logs reported through channel 4.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num    | state    | port     | dest address     | log type
1           | disabled | 65535    | host             | operationlogs securitylogs eventlogs
2           | disabled | 0        |                  | operationlogs securitylogs eventlogs
3           | disabled | 0        |                  | operationlogs securitylogs eventlogs
4           | disabled | 0        |                  | operationlogs eventlogs
```

4.5.11 Testing Reachability of the Syslog Server (syslog -d test)

Function

The **syslog -d test** command is used to test whether the syslog server is reachable.

Format

ipmcset -t syslog -d test -v <*destination*>

Parameters

Parameter	Description	Value
destination	Specifies the number of a syslog reporting channel.	1 to 4

Usage Guidelines

None

Example

Test whether the syslog server for channel 1 is reachable.

```
iBMC:/-> ipmcset -t syslog -d test -v 1
Test syslog dest1 successfully.
```

4.5.12 Querying Configuration Information of All Syslog Reporting Channels (syslog -d iteminfo)

Function

The **syslog -d iteminfo** command is used to query configuration information of the four syslog reporting channels.

Format

ipmcget -t syslog -d iteminfo

Parameters

None

Usage Guidelines

None

Example

Query configuration information of iBMC syslog reporting channels.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num      | state    | port     | dest address      | log type
1             | disabled | 65535    | host              | operationlogs securitylogs eventlogs
2             | disabled | 0        |                   | operationlogs securitylogs eventlogs
3             | disabled | 0        |                   | operationlogs securitylogs eventlogs
4             | disabled | 0        |                   | operationlogs eventlogs
```

4.6 Server Commands

4.6.1 Querying and Setting the Boot Device (bootdevice)

Function

The **bootdevice** command is used to query and set the boot device.

Format

ipmcget -d bootdevice

ipmcset -d bootdevice -v <*option*> [*once* | *permanent*]

Parameters

Parameter	Description	Value
option	Indicates the number of the booting device.	**0**: cancels the forcible boot. **1**: boots from the PXE. **2**: boots from the default hard disk. **5**: boots from the default CD/DVD. **6**: accesses the BIOS Setup menu upon server startup. **0xF**: boots from the FDD or the first mobile medium.
once	The setting is effective only once upon the next startup. After that, the default boot device set on the BIOS is used.	-

Parameter	Description	Value
permanent	The setting is effective permanently.	-

Usage Guidelines

None.

Example

Configure the system to boot from the default hard disk. The setting is effective only once upon the next startup.

```
iBMC:/->ipmcset -d bootdevice -v 2 once
Set boot device successfully.
```

Query the boot device.

```
iBMC:/->ipmcget -d bootdevice
Boot    device:  Force boot from default Hard-drive
Effective  type:  Once
```

If Boot device is "Unspecied", parameters related to forced boot are not set.

4.6.2 Setting the Server Reset Mode (frucontrol)

Function

The **frucontrol** command is used to specify how the server is reset.

Format

ipmcset [-t fru0] **-d frucontrol** -v <*option*>

Parameters

Parameter	Description	Value
option	Specifies the reset mode.	**0**: Forcibly restarts the server. **2**: Forcibly power cycle (power off and power on) the server.

Usage Guidelines

This command is invalid to a server in power-off state.

Example

Forcibly reset the server.

```
iBMC:/->ipmcset -d frucontrol -v 0
```

```
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced system reset) successfully.
```

Forcibly power cycle the server.

```
iBMC:/->ipmcset -d frucontrol -v 2
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced power cycle) successfully.
```

4.6.3 Querying and Setting the Server Power State (powerstate)

Function

The **powerstate** command is used to query and set the power state of the server.

Format

ipmcget [-t fru0] **-d powerstate**

ipmcset [-t fru0] **-d powerstate -v** <*option*>

Parameters

Parameter	Description	Value
option	Indicates the operation to be performed on the server.	**0**: powers off the server safely **1**: powers on the server **2**: powers off the server forcibly

Usage Guidelines

The power-off command is invalid for a server in power-off state.

Example

Power on the server.

```
iBMC:/->ipmcset -d powerstate -v 1
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Control fru0 power on successfully.
```

Query the power state of the server.

```
iBMC:/->ipmcget -d powerstate
Power state   : On
Hotswap state : M4
```

4.6.4 Querying and Setting the Server Power-Off Timeout Period (shutdowntimeout)

Function

The **shutdowntimeout** command is used to query and set the power-off timeout period for the server.

After a power-off operation is performed, the iBMC waits for the OS to shut down. If the OS fails to shut down within the specified time, the iBMC will forcibly power off the server.

Format

ipmcget [-t fru0] **-d shutdowntimeout**

ipmcset [-t fru0] **-d shutdowntimeout -v** <*time*>

Parameters

Parameter	Description	Value
time	Specifies the maximum time (in seconds) for shutting down the OS.	Value range: 0, 10 to 6000 The value **0** indicates that the shutdown timeout is disabled.

Usage Guidelines

- If **Power-off Timeout Period** is set to ON on the iBMC WebUI, you can use this command to disable shutdown timeout or set the shutdown timeout period as required.

- If **Power-off Timeout Period** is set to OFF on the iBMC WebUI, you can use this command to set the shutdown timeout period. After the setting, **Power-off Timeout Period** changes to ON on the iBMC WebUI.

Example

Set the shutdown timeout period to 600 seconds for the server.

```
iBMC:/->ipmcset -d shutdowntimeout -v 600
Set shutdown timeout successfully.
```

Query the shutdown timeout period.

```
iBMC:/->ipmcget -d shutdowntimeout
Graceful shutdown timeout state:    enabled
Graceful shutdown timeout value:    600 s
```

Query the shutdown timeout period (**power-off timeout period** is set to **OFF** on the iBMC WebUI).

```
iBMC:/->ipmcget -d shutdowntimeout
Graceful shutdown timeout state:    disabled
```

Disable shutdown timeout for the server.

iBMC:/->**ipmcset -d shutdowntimeout -v 0**
Set shutdown timeout successfully.

4.6.5 Querying the MAC Address of the Network Interface on the Main Board (macaddr)

Function

The **macaddr** command is used to query the MAC address of the network interface on the main board.

Format

ipmcget -d macaddr

Parameters

None

Usage Guidelines

None

Example

Query the MAC address of network interface on the main board.

iBMC:/->**ipmcget -d macaddr**
Type | Name | Mac Address
LOM | Port1 | 20:0b:c7:2a:e6:0b
LOM | Port2 | 20:0b:c7:2a:e6:0c
LOM | Port3 | 20:0b:c7:2a:e6:0d
LOM | Port4 | 20:0b:c7:2a:e6:0e

4.6.6 Querying the Available Network Port (ethport)

Function

The **ethport** command is used to query the information of the available network port.

Format

ipmcget -d ethport

Parameters

None

Usage Guidelines

None

Example

Query the available network port.

```
iBMC:/->ipmcget -d ethport
Type      | Name      | Port ID | Link Status
Dedicated | eth2      | na      | Link_Up
LOM       | Port1     | 1       | Link_Down
LOM       | Port2     | 2       | Link_Down
LOM       | Port3     | 3       | Link_Down
LOM       | Port4     | 4       | Link_Down
```

4.6.7 Clearing the BIOS Flash (clearcmos)

Function

The **clearcmos** command is used to delete all user-defined information from the BIOS flash.

Format

ipmcset -d clearcmos

Parameters

None

Usage Guidelines

None

Example

Clear the BIOS flash.

```
iBMC:/->ipmcset -d clearcmos
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Clear CMOS successfully.
```

4.6.8 Querying RAID Controller Card Information (ctrlinfo)

Function

The **ctrlinfo** command is used to query RAID controller card information.

Format

ipmcget -t storage -d ctrlinfo -v <*option*>

Parameters

Parameter	Description	Value
option	Specifies the ID of a RAID controller card.	**0** to **255**: indicates a specific RAID controller card. **all**: indicates all RAID controller cards.

Usage Guidelines

This command can be used only when either of the following conditions is met:

- The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

- The iBMA 2.0 has started on the OS.

Example

Query information about RAID controller card 0.

```
iBMC:/->ipmcget –t storage -d ctrlinfo –v 0
RAID Controller #0 Information
----------------------------------------------------------------------
Controller Name                  : SAS3108
Controller Type                  : LSI SAS3108
Component Name                     : RAID Card1
Support Out-of-Band Management          : Yes
Controller Mode                  : RAID
Controller Health                : Normal
Firmware Version                 : 4.650.00-6121
NVDATA Version                    : 3.1602.00-0002
Memory Size                      : 1024 MB
Device Interface                 : SAS 12G
SAS Address                      : 5e00000157737cd6
Minimum Strip Size Supported          : 64 KB
Maximum Strip Size Supported          : 1 MB
Controller Cache Is Pinned          : No
Maintain PD Fail History across Reboot    : Yes
Copyback Enabled                 : No
Copyback on SMART error Enabled       : No
JBOD Enabled                     : No
DDR ECC Count                    : 0

BBU Status                       : Present
BBU Type                         : CVPM02
BBU Health                       : Normal


PHY Status                       :
  PHY #0 :
     Invalid Dword Count        : 0
     Loss Dword Sync Count      : 0
     PHY Reset Problem Count    : 0
     Running Disparity Error Count : 0

  PHY #1 :
     Invalid Dword Count        : 0
     Loss Dword Sync Count      : 0
     PHY Reset Problem Count    : 0
     Running Disparity Error Count : 0
```

```
    PHY #2 :
      Invalid Dword Count        : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count      : 0
      Running Disparity Error Count : 0

    PHY #3 :
      Invalid Dword Count        : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count      : 0
      Running Disparity Error Count : 0

    PHY #4 :
      Invalid Dword Count        : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count      : 0
      Running Disparity Error Count : 0

    PHY #5 :
      Invalid Dword Count        : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count      : 0
      Running Disparity Error Count : 0

    PHY #6 :
      Invalid Dword Count        : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count      : 0
      Running Disparity Error Count : 0

    PHY #7 :
      Invalid Dword Count        : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count      : 0
      Running Disparity Error Count : 0
    ---------------------------------------------------------------------
```

4.6.9 Querying Logical Disk Information (ldinfo)

Function

The **ldinfo** command is used to query information about logical disks managed by a RAID controller card.

Format

ipmcget -t storage -d ldinfo -v *<ctrlid> <option>*

Parameters

Parameter	Description	Value
ctrlid	Specifies the ID of the RAID controller that manages the target logical disk.	**0** to **255**

Parameter	Description	Value
option	Specifies the ID of a logical disk.	• **0** to **255**: indicates a specific logical disk. • **all**: indicates all logical disks managed by a RAID controller.

Usage Guidelines

This command can be used only when either of the following conditions is met:

- The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
- The iBMA 2.0 has started on the OS.

Example

Query information about logical disk 0 managed by RAID controller 0.

```
iBMC:/->ipmcget –t storage -d ldinfo –v 0 0
Logical Drive Information
----------------------------------------------------------------------
Target ID                      : 0
Name                           : example1
Type                           : RAID1
State                          : Optimal
Default Read Policy               : Read Ahead
Default Write Policy              : Write Back with BBU
Default Cache Policy              : Direct IO
Current Read Policy               : Read Ahead
Current Write Policy              : Write Back with BBU
Current Cache Policy              : Direct IO
Access Policy                  : Read Write
Span depth                     : 1
Number of drives per span         : 2
Strip Size                     : 256 KB
Total Size                     : 100.234 GB
Disk Cache Policy                 : Enabled
Init State                     : No Init
Consistency Checking              : No
BGI Enabled                    : Yes
Bootable                       : No
Used for Secondary Cache          : No
SSCD Caching Enable               : No
PD participating in LD (ID#)       : 0,1
Dedicated Hot Spare PD (ID#)       : N/A
----------------------------------------------------------------------
```

Query information about all logical disks managed by RAID controller 0.

```
iBMC:/->ipmcget –t storage -d ldinfo –v 0 all
Logical Drive Information
----------------------------------------------------------------------
Target ID                      : 0
Name                           : example1
Type                           : RAID1
State                          : Optimal
Default Read Policy               : Read Ahead
Default Write Policy              : Write Back with BBU
```

```
Default Cache Policy           : Direct IO
Current Read Policy            : Read Ahead
Current Write Policy           : Write Back with BBU
Current Cache Policy           : Direct IO
Access Policy               : Read Write
Span depth                  : 1
Number of drives per span      : 2
Strip Size                : 256 KB
Total Size                : 100.234 GB
Disk Cache Policy            : Enabled
Init State                : No Init
Consistency Checking           : No
BGI Enabled               : Yes
Bootable                 : No
Used for Secondary Cache        : No
SSCD Caching Enable           : No
PD participating in LD (ID#)      : 0,1
Dedicated Hot Spare PD (ID#)     : N/A
-----------------------------------------------------------------------

Logical Drive Information

-----------------------------------------------------------------------
Target ID                 : 1
Name                   : example2
Type                   : RAID0
State                  : Optimal
Default Read Policy           : Read Ahead
Default Write Policy           : Write Back with BBU
Default Cache Policy           : Direct IO
Current Read Policy            : Read Ahead
Current Write Policy           : Write Back with BBU
Current Cache Policy           : Direct IO
Access Policy               : Read Write
Span depth                  : 1
Number of drives per span      : 5
Strip Size                : 256 KB
Total Size                : 1.149 TB
Disk Cache Policy            : Enabled
Init State                : No Init
Consistency Checking           : No
BGI Enabled               : Yes
Bootable                 : No
Used for Secondary Cache        : No
SSCD Caching Enable           : No
PD participating in LD (ID#)      : 2,8,9,10,11
Dedicated Hot Spare PD (ID#)     : N/A
-----------------------------------------------------------------------
```

4.6.10 Querying Physical Disk Information (pdinfo)

Function

The **pdinfo** command is used to query information about physical disks.

Format

ipmcget -t storage -d pdinfo -v *<option>*

Parameters

Parameter	Description	Value
option	Specifies the ID of a physical disk.	● **0** to **255**: indicates a specific physical disk. ● **all**: indicates all physical disks.

Usage Guidelines

This command can be used only when either of the following conditions is met:

● The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

● The iBMA 2.0 has started on the OS.

Example

Query information about physical disk 2.

```
iBMC:/->ipmcget –t storage -d pdinfo –v 2
Physical Drive Information
---------------------------------------------------------------------
ID                       : 2
Device Name              : Disk2
Manufacturer             : TOSHIBA
Serial Number            : EB00PC208N0R
Model                    : MBF2300RC
Firmware Version         : 0109
Health Status            : Normal
Firmware State           : UNCONFIGURED GOOD
Power State              : Spun Up
Media Type               : HDD
Interface Type           : SAS
Interface Speed          : 6.0Gbps
Link Speed               : 6.0Gbps
Drive Temperature        : 62(Celsius)
Capacity                 : 278.465 GB
Hot Spare                : None
Rebuild in Progress      : No
Patrol Read in Progress  : No
Remnant Media Wearout    : N/A
SAS Address(0)           : 50000393d84baa46
SAS Address(1)           : 0000000000000000
Location State           : Off

Media Error Count        : 0
Prefail Error Count      : 0
Other Error Count        : 0
---------------------------------------------------------------------
```

Query information about all physical disks.

```
iBMC:/->ipmcget –t storage -d pdinfo –v all
Physical Drive Information
---------------------------------------------------------------------
ID                       : 0
Device Name              : Disk0
Manufacturer             : TOSHIBA
Serial Number            : EB00PC208KL3
```

```
                           Model                       : MBF2300RC
                           Firmware Version              : 0109
                           Health Status               : Normal
                           Firmware State                : ONLINE
                           Power State                 : Spun Up
                           Media Type                  : HDD
                           Interface Type              : SAS
                           Interface Speed               : 6.0Gbps
                           Link Speed                  : 6.0Gbps
                           Drive Temperature             : 53(Celsius)
                           Capacity                    : 278.465 GB
                           Hot Spare                   : None
                           Rebuild in Progress           : No
                           Patrol Read in Progress         : No
                           Remnant Media Wearout              : N/A
                           SAS Address(0)                : 50000393d84b6f92
                           SAS Address(1)                : 0000000000000000
                           Location State              : Off

                           Media Error Count             : 0
                           Prefail Error Count           : 0
                           Other Error Count               : 0
                           ------------------------------------------------------------------

                           Physical Drive Information

                           ------------------------------------------------------------------
                           ID                          : 1
                           Device Name                 : Disk1
                           Manufacturer                : TOSHIBA
                           Serial Number               : EB72PC600G1C
                           Model                       : MBF2300RC
                           Firmware Version              : 0109
                           Health Status               : Normal
                           Firmware State                : ONLINE
                           Power State                 : Spun Up
                           Media Type                  : HDD
                           Interface Type              : SAS
                           Interface Speed               : 6.0Gbps
                           Link Speed                  : 6.0Gbps
                           Drive Temperature             : 69(Celsius)
                           Capacity                    : 278.465 GB
                           Hot Spare                   : None
                           Rebuild in Progress           : No
                           Patrol Read in Progress         : No
                           Remnant Media Wearout              : N/A
                           SAS Address(0)                : 5000039418218546
                           SAS Address(1)                : 0000000000000000
                           Location State              : Off

                           Media Error Count             : 0
                           Prefail Error Count           : 0
                           Other Error Count               : 0
                           ------------------------------------------------------------------

                           Physical Drive Information

                           ------------------------------------------------------------------
                           ID                          : 2
                           Device Name                 : Disk2
                           Manufacturer                : TOSHIBA
                           Serial Number               : EB00PC208N0R
                           Model                       : MBF2300RC
                           Firmware Version              : 0109
                           Health Status               : Normal
                           Firmware State                : ONLINE
                           Power State                 : Spun Up
                           Media Type                  : HDD
                           Interface Type              : SAS
                           Interface Speed               : 6.0Gbps
                           Link Speed                  : 6.0Gbps
```

```
Drive Temperature              : 62(Celsius)
Capacity                      : 278.465 GB
Hot Spare                     : None
Rebuild in Progress           : No
Patrol Read in Progress        : No
Remnant Media Wearout          : N/A
SAS Address(0)                : 50000393d84baa46
SAS Address(1)                : 0000000000000000
Location State                : Off

Media Error Count             : 0
Prefail Error Count           : 0
Other Error Count             : 0
--------------------------------------------------------------------
```

4.6.11 Querying Disk Array Information (arrayinfo)

Function

The **arrayinfo** command is used to query disk array information.

Format

ipmcget -t storage -d arrayinfo -v *<control_id> <option>*

Parameters

Parameter	Description	Value
control_id	Specifies the ID of the RAID controller to which the disk array belongs.	0 to 255
option	Specifies the disk array to be queried.	● **all**: Query information about all disk arrays. ● 0 to 255: Query information about the specified disk array.

Usage Guidelines

This command can be used only when either of the following conditions is met:

● The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.

● The iBMA 2.0 has started on the OS.

Example

Query information about disk array 1 of RAID controller 0.

```
iBMC:/->ipmcget –t storage -d arrayinfo –v 0 1
Disk Array Information
```

```
-------------------------------------------------------------------
Array ID                    : 1
Used Space                    : 1.149 TB
Free Space                   : 215.749 GB
Logcial Drive(s) ID            : 1
Physical Drive(s) ID           : 2,8,9,10,11
-------------------------------------------------------------------
```

Query information about all disk arrays of RAID controller 0.

```
iBMC:/->ipmcget –t storage -d arrayinfo –v 0 all
Disk Array Information

-------------------------------------------------------------------
Array ID                    : 0
Used Space                    : 200.469 GB
Free Space                   : 356.461 GB
Logcial Drive(s) ID            : 0
Physical Drive(s) ID           : 0,1
-------------------------------------------------------------------

Disk Array Information

-------------------------------------------------------------------
Array ID                    : 1
Used Space                    : 1.149 TB
Free Space                   : 215.749 GB
Logcial Drive(s) ID            : 1
Physical Drive(s) ID           : 2,8,9,10,11
-------------------------------------------------------------------

Disk Array Information

-------------------------------------------------------------------
Array ID                    : 2
Used Space                    : 446.103 GB
Free Space                   : 0 MB
Logcial Drive(s) ID            : 2
Physical Drive(s) ID           : 7
-------------------------------------------------------------------
```

4.6.12 Creating a Logical Drive (createld)

Function

The **createld** command is used to create a logical drive from an idle physical disk.

Format

ipmcset -t storage -d createld -v <*control_id*> **-rl** <*raidlevel*> **-pd** <*pd_id*> **[-cachecade] [-sc** <*span_num*>**] [-name** <*ldname*>**] [-size** <*capative*>{m|g|t} **] [-ss** <*stripesize*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-dcp** <*dcpvalue*>**] [-init** <*initmode*>**]**

Parameters

Parameter	Description	Value
control_id	Specifies the ID of the RAID controller.	0 to 255

Parameter	Description	Value
raidlevel	Specifies the RAID level of the logical drive.	**r0**: RAID 0 **r1**: RAID 1 **r5**: RAID 5 **r6**: RAID 6 **r10**: RAID 10 **r50**: RAID 50 **r60**: RAID 60 **NOTE** If the command contains **-cachecade**, this parameter must be **r0** or **r1**.
pd_id	Specifies the member disk IDs of the logical drive.	Use a comma (,) to separate multiple disk IDs, for example, **0,1,2**. **NOTE** If the command contains **-cachecade**, the member disks must be SSDs.
span_num	Specifies the number of spans of the logical drive.	- You do not need to set this parameter if the RAID level is 0, 1, 5 or 6. - Set this parameter when the RAID level is 10, 50, or 60. The default value is 2. **NOTE** If the command contains **-cachecade**, this parameter is invalid.
ldname	Specifies the name of the logical drive to be created.	The parameter value cannot exceed 15 characters.
capative	Specifies the capacity of the logical drive to be created.	The unit of the logical drive capacity can be: **m**: MB **g**: GB **t**: TB **NOTE** - If the command contains **-cachecade**, this parameter is invalid. - If the command does not contain **-cachecade** and this parameter is not set, the system sets the logical drive capacity based on the maximum capacity of the member drive.

Parameter	Description	Value
stripesize	Specifies the stripe size (in bytes) of the logical drive.	The stripe size can be: ● 64K ● 128K ● 256K ● 512K ● 1M **NOTE** ● If the command contains **-cachecade**, this parameter is invalid. The default strip size of the logical drive is **1M**. ● If the command does not contain **-cachecade** and this parameter is not set, the default stripe size of the logical drive is **256K**.
rpvalue	Specifies the read policy of the logical drive.	● **ra**: sets the read policy of the logical drives to **Read Ahead**. ● **nra**: sets the read policy of the logical drives to **No Read Ahead**. **NOTE** ● If the command contains **-cachecade**, this parameter is invalid. The default read policy of the logical drives is **nra**. ● If the command does not contain **-cachecade** and this parameter is not set, the default read policy of the logical drives is **ra**.
wpvalue	Specifies the write policy of the logical drive.	● **wt**: sets the write policy of the logical drives to **Write Through**. ● **wb**: sets the write policy of the logical drives to **Write Back**. ● **wbwithbbu**: sets the write policy of the logical drives to **Write Back with BBU**. The default value is **wbwithbbu**.
iopvalue	Specifies the IO policy of the logical drive.	● **cio**: sets the I/O policy of the logical drives to **Cached IO**. ● **dio**: sets the I/O policy of the logical drives to **Direct IO**. The default value is **dio**. **NOTE** If the command contains **-cachecade**, this parameter is invalid.

Parameter	Description	Value
apvalue	Specifies the access policy of the logical drive.	**rw**: sets the access policy of the logical drives to read/write. **ro**: sets the access policy of the logical drives to read-only. **blocked**: sets the access policy of the logical drives to blocked. The default value is **rw**. **NOTE** If the command contains **-cachecade**, this parameter is invalid.
dcpvalue	Specifies the cache policy of the logical drive.	**enabled**: enables cache for logical drives. **disabled**: disables cache for logical drives. **default**: uses the default policy, which is determined by the cache policy of the member drives. **NOTE** - If the command contains **-cachecade**, this parameter is invalid. The default drive cache policy of the logical drives is **default**. - If the command does not contain **-cachecade** and this parameter is not set, the default drive cache policy of the logical drives is **enabled**.
initmode	Specifies the initialization mode of the logical drive.	**no**: no initialization. **quick**: performs a quick initialization. **full**: performs a full initialization. The default value is **no**. **NOTE** If the command contains **-cachecade**, this parameter is invalid.

Usage Guidelines

If the command contains **-cachecade**, a CacheCade drive is to be created.

This command can be used only when the following conditions is met:The RAID controller card supports iBMC out-of-band management. You can refer to the Technical Specifications section in the RAID controller card user guide to determined whether the RAID card supports the iBMC out-of-band management.

Example

Create a common logical drive under RAID controller 0.

```
iBMC:/-> ipmcset -t storage -d createld -v 0 -rl r1 -pd 0,1 -name example -size 100g -ss 512k -rp ra -
wp wb -ap rw -iop cio -dcp enabled -init quick
```

> WARNING: The operation may have many adverse effects.
> Do you want to continue?[Y/N]:**y**

Create a Cachecade drive under RAID controller 0.

```
iBMC:/-> ipmcset -t storage -d createld -v 0 -rl r0 -pd 0,1,2 -name cachecade -cachecade -wp wb
```
> WARNING: The operation may have many adverse effects.
>   Do you want to continue?[Y/N]:**y**

4.6.13 Adding a Logical Drive (addld)

Function

The **addld** command is used to add a logical drive to a disk array.

Format

ipmcset -t storage -d addld -v *<control_id>* **-array** *<arrayid>* **[-name** *<ldname>*]
[-size *<capative>*{m|g|t} **] [-ss** *<stripesize>*] **[-rp** *<rpvalue>*] **[-wp** *<wpvalue>*] **[-iop** *<iopvalue>*] **[-ap** *<apvalue>*] **[-dcp** *<dcpvalue>*] **[-init** *<initmode>*]

Parameters

Parameter	Description	Value
control_id	Specifies the ID of the RAID controller.	0 to 255
arrayid	Specifies the ID of the disk array to be added with the logical drive.	0 to 255
ldname	Specifies the name of the logical drive to be added.	The parameter value cannot exceed 15 characters.
capative	Specifies the capacity of the logical drive to be added.	The unit of the logical drive capacity can be: ● **m**: MB ● **g**: GB ● **t**: TB **NOTE** If this parameter is not set, the system sets the logical drive capacity based on the maximum capacity provided by the disk array.

Parameter	Description	Value
stripesize	Specifies the stripe size (in bytes) of the logical drive.	The stripe size can be: ● 64K ● 128K ● 256K ● 512K ● 1M The default value is **256K**.
rpvalue	Specifies the read policy of the logical drive.	● **ra**: sets the read policy of the logical drives to **Read Ahead**. ● **nra**: sets the read policy of the logical drives to **No Read Ahead**. The default value is **ra**.
wpvalue	Specifies the write policy of the logical drive.	● **wt**: sets the write policy of the logical drives to **Write Through**. ● **wb**: sets the write policy of the logical drives to **Write Back**. ● **wbwithbbu**: sets the write policy of the logical drives to **Write Back with BBU**. The default value is **wbwithbbu**.
iopvalue	Specifies the IO policy of the logical drive.	● **cio**: sets the I/O policy of the logical drives to **Cached IO**. ● **dio**: sets the I/O policy of the logical drives to **Direct IO**. The default value is **dio**.
apvalue	Specifies the access policy of the logical drive.	● **rw**: sets the access policy of the logical drives to read/write. ● **ro**: sets the access policy of the logical drives to read-only. ● **blocked**: sets the access policy of the logical drives to blocked. The default value is **rw**.
dcpvalue	Specifies the cache policy of the logical drive.	● **enabled**: enables cache for logical drives. ● **disabled**: disables cache for logical drives. ● **default**: uses the default policy, which is determined by the cache policy of the member drives. The default value is **enabled**.

Parameter	Description	Value
initmode	Specifies the initialization mode of the logical drive.	• **no**: no initialization. • **quick**: performs a quick initialization. • **full**: performs a full initialization. The default value is **no**.

Usage Guidelines

This command can be used only when the following conditions is met:The RAID controller card supports iBMC out-of-band management. You can refer to the Technical Specifications section in the RAID controller card user guide to determined whether the RAID card supports the iBMC out-of-band management.

Example

Add a logical drive to disk array 1 of RAID controller 0.

```
iBMC:/-> ipmcset -t storage -d addld -v 0 -array 1 -name example -size 500g -ss 256k -rp ra -wp wb -ap rw -iop cio -dcp enabled -init quick
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.14 Deleting a Logical Drive (deleteld)

Function

The **deleteld** command is used to delete a logical drive managed by a RAID controller.

Format

ipmcset -t storage -d deleteld -v *<control_id> <ldid>*

Parameters

Parameter	Description	Value
control_id	Specifies the ID of the RAID controller.	0 to 255
ldid	Specifies the ID of a logical disk to be deleted.	0 to 255

Usage Guidelines

This command can be used only when the following conditions is met:The RAID controller card supports iBMC out-of-band management. You can refer to the

Technical Specifications section in the RAID controller card user guide to determined whether the RAID card supports the iBMC out-of-band management.

Example

Delete logical drive 1 managed by RAID controller 0.

```
iBMC:/-> ipmcset -t storage -d deleteld -v 0 0
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.15 Modifying Logical Drive Properties (ldconfig)

Function

The **ldconfig** command is used to modify properties of a logical drive.

Format

ipmcset -t storage -d ldconfig -v <*control_id*> <*ldid*> <[**-name** <*ldname*>] [**-rp** <*rpvalue*>] [**-wp** <*wpvalue*>] [**-iop** <*iopvalue*>] [**-ap** <*apvalue*>] [**-dcp** <*dcpvalue*>] [**-bgi** <*bgistate*>] [**-boot**] [**-sscd** <*sscdstate*>]

Parameters

Parameter	Description	Value
control_id	Specifies the ID of the RAID controller.	0 to 255
ldid	Specifies the ID of the logical drive to be modified.	0 to 255
ldname	Specifies the name of the logical drive to be modified.	The parameter value cannot exceed 15 characters.
rpvalue	Specifies the read policy of the logical drive.	• **ra**: sets the read policy of the logical drives to **Read Ahead**. • **nra**: sets the read policy of the logical drives to **No Read Ahead**. NOTE This parameter is not supported if the logical drive type is **CacheCade**.
wpvalue	Specifies the write policy of the logical drive.	• **wt**: sets the write policy of the logical drives to **Write Through**. • **wb**: sets the write policy of the logical drives to **Write Back**. • **wbwithbbu**: sets the write policy of the logical drives to **Write Back with BBU**.

Parameter	Description	Value
iopvalue	Specifies the IO policy of the logical drive.	● **cio**: sets the I/O policy of the logical drives to **Cached IO**. ● **dio**: sets the I/O policy of the logical drives to **Direct IO**. **NOTE** This parameter is not supported if the logical drive type is **CacheCade**.
apvalue	Specifies the access policy of the logical drive.	● **rw**: sets the access policy of the logical drives to read/write. ● **ro**: sets the access policy of the logical drives to read-only. ● **blocked**: sets the access policy of the logical drives to blocked. **NOTE** This parameter is not supported if the logical drive type is **CacheCade**.
dcpvalue	Specifies the cache policy of the logical drive.	● **enabled**: enables cache for logical drives. ● **disabled**: disables cache for logical drives. ● **default**: uses the default policy, which is determined by the cache policy of the member drives. **NOTE** This parameter is not supported if the logical drive type is **CacheCade**.
bgistate	Specifies the BGI status of the logical drive.	● **enabled**: enables the background initialization function for the logical drives. ● **disabled**: disables the background initialization function for the logical drives. **NOTE** This parameter is not supported if the logical drive type is **CacheCade**.
sscdstate	Specifies the setting of SSD Caching (whether to use the CacheCade drive as the cache).	● **enabled**: enables the SSD caching function for the logical drives. ● **disabled**: disables the SSD caching function for the logical drives. **NOTE** ● The current RAID controller card must have a CacheCade logical drive available. ● This parameter is unavailable when the logical drive type is **CacheCade**.

Usage Guidelines

If the command contains **-boot**, the logical drive is the boot device.

This command can be used only when the following conditions is met:The RAID controller card supports iBMC out-of-band management. You can refer to the Technical Specifications section in the RAID controller card user guide to determined whether the RAID card supports the iBMC out-of-band management.

Example

Modify the properties of logical drive 1 under RAID controller 0.

```
iBMC:/-> ipmcset -t storage -d ldconfig -v 0 1 -name example -rp ra -wp wb -ap rw -iop cio -dcp
enabled –bgi enabled -boot
WARNING: The operation may have many adverse effects.
   Do you want to continue?[Y/N]:y
```

4.6.16 Modifying RAID Controller Properties (ctrlconfig)

Function

The **ctrlconfig** command is used to modify RAID controller properties.

Format

ipmcset -t storage -d ctrlconfig -v *<control_id>* **<[-cb** *<cbstate>*] [**-smartercb** *<smartercbstate>*] [**-jbod** *<jbodstate>*] [**-restore**]

Parameters

Parameter	Description	Value
control_id	Specifies the ID of the RAID controller.	0 to 255
cbstate	Specifies the setting of copyback of the RAID controller.	- enabled - disabled
smartercbstate	Specifies whether copyback is enabled when a SMART error is detected on a member disk of the RAID controller.	- enabled - disabled
jbodstate	Specifies the setting of JBOD of the RAID controller.	- enabled - disabled

Usage Guidelines

If the command contains **-restore**, the RAID controller properties will be restored to default values.

This command can be used only when the following conditions is met:The RAID controller card supports iBMC out-of-band management. You can refer to the Technical Specifications section in the RAID controller card user guide to determined whether the RAID card supports the iBMC out-of-band management.

Example

Enable copyback for RAID controller 0.

```
iBMC:/-> ipmcset -t storage -d ctrlconfig -v 0 -cb enabled
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.17 Modifying Physical Drive Properties (pdconfig)

Function

The **pdconfig** command is used to modify properties of a physical drive managed by a RAID controller.

Format

ipmcset -t storage -d pdconfig -v *<pdid>* **[-state** *<pdstate>*] **[-hotspare** *<hotsparetype>* **[-ld** *<ldid>*]] **[-locate** *<locatestate>*]

Parameters

Parameter	Description	Value
pdid	Specifies the ID of the physical drive.	0 to 255
pdstate	Specifies the status of the physical drive.	• **online**: The drive is online. • **offline**: The drive is offline. • **ug**: The drive is idle. • **jbod**: The drive is a JBOD disk.
hotsparetype	Specifies the hot spare status of the physical drive.	• **none**: It is not a hot spare disk • **global**: It is a global spare hot disk. • **dedicated**: It is a dedicated spare hot disk.

Parameter	Description	Value
ldid	Specifies the ID of the logical drive. If **hotsparetype** is **dedicated**, you need to set the logical drive associated with this physical drive.	0~255
locatestate	Specifies the status of the location indicator of the physical drive.	• **start**: The location indicator is flashing. • **stop**: The location indicator is off.

Usage Guidelines

This command can be used only when the following conditions is met:The RAID controller card supports iBMC out-of-band management. You can refer to the Technical Specifications section in the RAID controller card user guide to determined whether the RAID card supports the iBMC out-of-band management.

Example

Set the status of physical drive 1 to **online**.

```
iBMC:/-> ipmcset -t storage -d pdconfig -v 1 -state online
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7 System Commands

4.7.1 Querying the System Name (systemname)

Function

The **systemname** command is used to query the system name.

Format

ipmcget -t smbios -d systemname

Parameters

None

Usage Guidelines

None

Example

Query the system name.

```
iBMC:/->ipmcget -t smbios -d systemname
System name is: xxxxx
```

4.7.2 Setting the Time Zone (timezone)

Function

The **timezone** command is used to set the time zone.

Format

ipmcset -d timezone -v <*timezone*>

Parameters

Parameter	Description	Value

timezone	Time zone.	You can set the time zone by specifying either of the following:
		
		● Time offset
		Value range:
		  – -12:00 to +14:00. For example, **+8:00** or **-4:30**.
		  – GMT-12:00 to GMT+14:00. For example, **GMT +8:00** or **GMT-4:30**.
		● Area name
		Value range: Global time zone area names. For example, **Asia/Shanghai** or **America/New_York**.
		● Default value: **GMT**
		
		You can run the **ipmcset -d timezone -v** <*a*> command to query the time zones supported.

Usage Guidelines

In the time zones that use daylight saving time (DST), the iBMC automatically adjusts the time one hour forward when the DST starts and adjusts the time backward to standard time when the DST ends.

Example

Set the iBMC time zone to **+8:00**.

```
iBMC:/->ipmcset -d timezone -v +8:00
Set time zone successfully.
```

Set the iBMC time zone to **GMT+8:00**.

```
iBMC:/->ipmcset -d timezone -v GMT+8:00
Set time zone successfully.
```

Query the iBMC time zone.

```
iBMC:/->ipmcget -d time
2014-06-28 Saturday 16:43:51 GMT+08:00
```

Set the iBMC time zone to **Asia/Shanghai**.

```
iBMC:/->ipmcset -d timezone -v Asia/Shanghai
Set time zone successfully.
```

Query the iBMC time zone.

```
iBMC:/->ipmcget -d time
2017-09-06 Wednesday 16:43:51 Asia/Shanghai(GMT+08:00)
```

4.7.3 Querying the iBMC Time (time)

Function

The **time** command is used to query the iBMC time.

Format

ipmcget -d time

Parameters

None

Usage Guidelines

None

Example

Query the iBMC time.

```
iBMC:/->ipmcget -d time
2014-06-28 Saturday 16:43:51 GMT+08:00
```

or

```
iBMC:/->ipmcget -d time
2017-09-06 Wednesday 16:43:51 Asia/Shanghai(GMT+08:00)
```

4.7.4 Querying Device Version Information (version)

Function

The **version** command is used to query the version information about the device.

Format

ipmcget -d version

Parameters

None

Usage Guidelines

None

Example

Query version information about device.

iBMC:/->**ipmcget -d version**

The System return information of RH8100 V3:

```
------------------- iBMC INFO -------------------
IPMC          CPU:        Hi1710
IPMI        Version:      2.0
CPLD        Version:     (U6029)1.04
Active iBMC   Version:      (U6005)5.30
Active iBMC    Build:      001
Active iBMC    Built:      10:56:13 Aug  1 2014
Backup iBMC   Version:       5.30
SDK         Version:      1.36
SDK          Built:      15:07:46 Jul 30 2014
Active Uboot  Version:        1.1.26 (Jun 20 2014 - 14:28:52)
Backup Uboot  Version:        1.1.26 (Jun 20 2014 - 14:28:52)
IPMB        Address:       0x20
----------------- Product INFO -----------------
Product        ID:        0x0008
Product       Name:       RH8100 V3
BIOS        Version:      (U6145)V019
-------------- Mother Board INFO --------------
RH8100        BoardID:        0x005b
RH8100         PCB:         .A
---------------- Raid Card INFO ----------------
SR130        BoardID:        0x002c
SR130         PCB:         .A
--------------- Riser Card INFO ----------------
BC61PRBA      BoardID:         0x0080
-------------- HDD Backplane INFO --------------
BC11THBG      BoardID:        0x007a
BC11THBG       PCB:         .A
---------------- CPU Board INFO ----------------
CpuBoard      BoardID:        0x0090
CpuBoard        PCB:         .A
CpuBoard  CPLD Version:       (U1028)1.04
CpuBoard      BoardID:        0x0090
CpuBoard        PCB:         .A
CpuBoard  CPLD Version:       (U1028)1.04
CpuBoard      BoardID:        0x0090
CpuBoard        PCB:         .A
CpuBoard  CPLD Version:       (U1028)1.04
CpuBoard      BoardID:        0x0090
CpuBoard        PCB:         .A
CpuBoard  CPLD Version:       (U1028)1.04
-------------- Memory Board INFO --------------
MemoryBoard    BoardID:        0x0094
MemoryBoard       PCB:         .A
MemoryBoard    BoardID:        0x0094
MemoryBoard       PCB:         .A
---------------- IO Board INFO ----------------
BioBoard      BoardID:        0x005a
BioBoard        PCB:         .A
BioBoard  CPLD Version:       (U1044)1.04
------------------- LCD INFO -------------------
LCD         Version:      (J7)1.00
```

Command output of other rack servers:

```
------------------- iBMC INFO -------------------
IPMC          CPU:        Hi1710
IPMI        Version:      2.0
```

```
CPLD         Version:        (U4269)2.02
Active iBMC   Version:        (U4282)2.92
Active iBMC    Build:         002
Active iBMC    Built:         21:09:56 Feb 11 2018
Backup iBMC   Version:        2.97
SDK          Version:        3.10
SDK          Built:         17:16:44 Feb  6 2018
Active Uboot  Version:        2.1.07 (Dec 21 2017 - 18:01:59)
Backup Uboot  Version:        2.1.07 (Dec 21 2017 - 18:01:59)
----------------- Product INFO -----------------
Product        ID:           0x0001
Product        Name:         1288H V5
BIOS         Version:        (U47)0.60
-------------- Mother Board INFO ---------------
Mainboard     BoardID:        0x0019
Mainboard     PCB:           .B
--------------- Riser Card INFO ----------------
BC11PERY      BoardID:        0x0091
-------------------- PS INFO -------------------
PS1          Version:        DC: 02e  PFC: 018
```

4.7.5 Querying FRU Information (fruinfo)

Function

The **fruinfo** command is used to query information about the FRUs except the PSUs, which include the mainboard, RAID controller card, mezzanine card, hard disk backplane, PCIe riser card, and GPU board.

Format

ipmcget [-t fru0] **-d fruinfo**

Parameters

None

Usage Guidelines

None

Example

Query the information about the FRUs.

```
iBMC:/->ipmcget -d fruinfo
FRU Device Description : Builtin FRU Device (ID 0, Mainboard)
 Board Mfg. Date      : 2014/04/03 Thu 16:12:00
 Board Manufacturer   :
 Board Product Name   : board
 Board Serial Number  : 022HLV10E3000003
 Board FRU File ID    : 1.17
 Product Manufacturer :
 Product Name         : pname
 Product Serial Number : serialnumber
 Product FRU File ID   : 1.17
```

4.7.6 Querying System Health Status (health)

Function

The **health** command is used to query the health status of the system.

Format

ipmcget [-t fru0] **-d health**

Parameters

None

Usage Guidelines

None

Example

Query the health status of the system.

iBMC:/->**ipmcget -d health**
System in health state.

4.7.7 Querying System Health Event Information (healthevents)

Function

The **healthevents** command is used to query the health event information about the system.

Format

ipmcget [-t fru0] **-d healthevents**

Parameters

None

Usage Guidelines

None

Example

Query health event information about the system.

iBMC:/->**ipmcget -d healthevents**
Event Num | Event Time | Alarm Level | Event Code | Event Description
1 | 2016-10-17 06:27:14 | Minor | 0x01000021 | Failed to obtain data of the CPU 1 DIMM
VDDQ2 voltage.
2 | 2016-10-17 10:24:43 | Critical | 0x01000015 | DIMM020 DIMM configuration error or

training failed.
3 | 2016-10-17 10:24:43 | Major | 0x01000017 | DIMM012 DIMM triggered an uncorrectable
error, .
4 | 2016-10-17 10:24:43 | Critical | 0x01000015 | DIMM001 DIMM configuration error or
training failed.
5 | 2016-10-17 08:47:27 | Major | 0x03000009 | [Mock]PSU 1 failure.
6 | 2016-10-17 07:40:57 | Minor | 0x0D000003 | The NIC 1 temperature (150 degrees C)
exceeds the overtemperature threshold (100 degrees C).
7 | 2016-10-17 07:04:47 | Major | 0x2100000B | Data rebuild failed at SD card 2.
8 | 2016-10-17 06:33:21 | Major | 0x2C000029 | The OS is forcibly powered off and on due to
the watchdog timeout.

4.7.8 Querying the Information of Port 80 (port80)

Function

The **port80** command is used to query the current and history information of port 80.

Format

ipmcget -d port80

Parameters

None

Usage Guidelines

None

Example

Query the current and history information of port 80. The value in square brackets is the current value.

```
iBMC:/->ipmcget -d port80
port80 diagnose code:
[00]-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
```

4.7.9 Querying the Serial Number of the Server (serialnumber)

Function

The **serialnumber** command is used to query the serial number of the server.

Format

ipmcget [-t smbios] **-d serialnumber**

Parameters

None

Usage Guidelines

None

Example

Query the server SN.

```
iBMC:/->ipmcget -d serialnumber
System SN is:444444444444444444444
```

4.7.10 Querying and Clearing SEL Information (sel)

Function

The **sel** command is used to query and clear system event log (SEL) information.

Format

ipmcget -d sel -v <*option*> [*sel_id*]

ipmcset [-t fru0] **-d sel -v clear**

Parameters

Parameter	Description	Value
option	Specifies the operation to be performed.	**list**: lists all SEL records. **info**: queries the usage of SEL records. **suggestion**: queries the handling suggestion of a specified SEL. NOTE A maximum of 4000 SEL records can be stored. If more SEL records are generated, the system automatically deletes the earliest 2000 SEL records and numbers the new SEL records from 2001.

Parameter	Description	Value
sel_id	Identifies an SEL.	This parameter is valid only when the **suggestion** operation is to be performed. You can perform the **list** operation to obtain the *sel_id*.
clear	Clears all SELs. **NOTE** Cleared SELs cannot be restored.	-

Usage Guidelines

None

Example

Query SEL records.

```
iBMC:/->ipmcget -d sel -v info
SEL Information
Version            :1.0.0
Current Event Number  :  147
Max Event Number      :  4000
```

Query the handling suggestion of SEL 146.

```
iBMC:/->ipmcget -d sel -v suggestion 146
ID              :  146
Generation Time    :  2016-10-26 03:26:23
Severity        :  Minor
Event Code        :  0x12000013
Status          :  Asserted
Event Description  :  [Mock]Failed to obtain data of the air inlet temperature
Suggestion        :  1. Restart the iBMC.
                     2. Remove and reconnect power cables or remove and reinstall the board in the chassis.
```

clear SEL information

```
iBMC:/->ipmcset -t fru0 -d sel -v clear
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
Clear SEL records successfully.
```

4.7.11 Querying Operation Logs (operatelog)

Function

The **operatelog** command is used to query the system operation log.

Format

ipmcget -d operatelog

Parameters

None

Usage Guidelines

When the operation log reaches 200 KB, it will be automatically compressed. When a new compressed package is generated, the old compressed package will be automatically deleted.

Example

Query the operation log.

```
iBMC:/->ipmcget -d operatelog
2018-06-19 15:42:08 MAINT,Administrator@192.168.124.103:62541,cooling_app,Set debug log output type
to (local) successfully
2018-06-19 15:41:58 MAINT,Administrator@192.168.124.103:62541,cooling_app,Set debug log output level
to (debug) successfully
2018-06-19 15:41:52 MAINT,Administrator@192.168.124.103:62541,cooling_app,Set debug log output level
failed
2018-06-19 15:41:48 MAINT,Administrator@192.168.124.103:62541,cooling_app,Attach (cooling_app)
successfully
2018-06-19 15:39:25 IPMI,N/A@HOST,BMC,Set FRU0 MAC1 address(00:00:00:00:00:00) successfully
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set bios setting file changed flag to (no changed) successfully
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set PCIePortDisable3 from [Disabled] to [Disabled]
success,EvtCode:21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set PStateDomain from [One] to [One] success,EvtCode:
21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set TurboMode from [Enabled] to [Enabled] success,EvtCode:
21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set CustomPowerPolicy from [Efficiency] to [Efficiency]
success,EvtCode:21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set QuietBoot from [Disabled] to [Disabled] success,EvtCode:
21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set QuickBoot from [Enabled] to [Enabled] success,EvtCode:
21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set BootType from [LegacyBoot] to [LegacyBoot]
success,EvtCode:21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set boot flags to (RAW:00-00-00-00-00) successfully
2018-06-19 15:38:35 IPMI,N/A@HOST,BMC,Set watchdog timer to (RAW:02-00-00-00-e0-2e) successfully
2018-06-19 15:38:30 IPMI,N/A@HOST,BMC,Set watchdog timer to (RAW:02-00-00-00-e0-2e) successfully
Input 'q' to quit:
```

4.7.12 Downloading the Systemcom Data (systemcom)

Function

The **systemcom** command is used to download the serial over LAN (SOL) file.

Format

ipmcget -d systemcom

Parameters

None

Usage Guidelines

Before running this command, ensure that **Serial Port Data** is set to [ON] on the **Diagnosis** > **Serial Port Data** page of the iBMC WebUI.

To view the Systemcom data, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the serial port data (for example **systemcom.tar**) from the **/tmp** directory to the local PC.

Example

Download the SOL file.

```
iBMC:/->ipmcget -d systemcom
Download System Com data to /tmp/systemcom.tar successfully.
```

4.7.13 Downloading the Black Box File (blackbox)

Function

The **blackbox** command is used to download the black box file.

Format

ipmcget -d blackbox

Parameters

None

Usage Guidelines

- The black box stores the kernel information of the server before a critical fault such as OS breakdown occurs.

- The black box function can be used only after the fault monitoring software (for example, iBMA) is installed on the server. For details about how to parse black box data, see the iBMA user guide.

- Before running this command, ensure that the black box function is enabled on the **Diagnosis** > **Black Box** page of the iBMC WebUI. For more details, see **Black Box**.

- To view the black box file, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the **blackbox.tar** file from the **/tmp** directory to the local PC.

Example

Download black box data.

```
iBMC:/->ipmcget -d blackbox
Downloading...
100%
Download Black Box data to /tmp/blackbox.tar successfully.
```

4.7.14 Downloading the BIOS (download)

Function

The **maintenance -d download** command is used to download the BIOS file **bios.bin** to **/tmp**.

The **bios.bin** file helps locate OS startup exceptions and BIOS faults.

Format

ipmcset -t maintenance -d download –v *<option>*

Parameters

Parameter	Description	Value
option	Specifies the destination directory to which the BIOS data is downloaded.	The value must be **1**, which indicates **/tmp**.

Usage Guidelines

When a fault occurs, download the **bios.bin** file and contact technical support.

To prevent timeout, disable the CLP timeout feature before downloading BIOS data. For details, see **Disabling the CLP Timeout Feature (notimeout)**.

To view the BIOS data, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the file (for example **bios.bin**) from the **/tmp** directory to the local PC.

Example

Download the BIOS file **bios.bin** to **/tmp**.

```
iBMC:/->ipmcset -t maintenance -d download –v 1
Download /tmp/bios.bin.
Downloading BIOS...
Download BIOS successfully.
```

4.7.15 Upgrading the BIOS (upgradebios)

Function

The **maintenance -d upgradebios** command is used to upgrade the BIOS.

Format

ipmcset -t maintenance -d upgradebios -v *filepath*

Parameters

Parameter	Description	Value
filepath	Specifies the path of the BIOS upgrade file.	For example, */tmp/biosimage.hpm*.

Usage Guidelines

- Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the upgrade file to the specified directory (for example **/tmp**) of the iBMC file system.

- Both the **maintenance -d upgradebios** and **upgrade** commands can be used to upgrade the BIOS. The difference of the two commands is as follows:

  - Before using the **maintenance -d upgradebios** command, you need to power off the OS. You do not need to power off the OS before using the **upgrade** command.

  - If the **maintenance -d upgradebios** command is used to upgrade the BIOS, the default BIOS password will be changed to the default password of the target version after the upgrade. Exercise caution when performing this operation.

    □ NOTE

    After the BIOS is upgraded on the iBMC WebUI, the following information is the same as that before the upgrade:

    - Date, time, and language information on the **Main** page

    - BIOS password and startup logo

    - All parameters except watchdog parameters on the **IPMI iBMC Configuration** page of the **Advanced** screen

  - If the **upgrade** command is used, system settings will not be changed. For details, see **4.3.13 Upgrading the Firmware (upgrade)**.

Example

Upgrade the BIOS using the **/tmp/biosimage.hpm** file.

```
iBMC:/->ipmcset -t maintenance -d upgradebios -v /tmp/biosimage.hpm
Please make sure the iBMC is working while upgrading.
Updating...
System needs two minutes time to prepare.
<100%>
Update successfully.
```

4.7.16 Setting the iBMC Network Port State (ethlink)

Function

The **maintenance -d ethlink** command is used to set the state of the iBMC network port.

Format

ipmcset -t maintenance -d ethlink -v *<ethname> <action>*

Parameters

Parameter	Description	Value
ethname	Specifies the iBMC network port to be set.	- eth0 - eth1 - eth2 - eth3 The number of iBMC network ports varies with the server model.
action	Specifies the network port state.	- enable - disable

Usage Guidelines

None

Example

\# Enable iBMC network port **eth2**.

```
iBMC:/->ipmcset -t maintenance -d ethlink -v eth2 enable
WARNING: This operation will enable eth2.
Do you want to continue?[Y/N]:y
Enable eth2 successfully.
```

4.7.17 Performing One-Click Information Collection (diaginfo)

Function

The **diaginfo** command is used to perform one-click information collection. For more details, see **One-Click Information Collection**.

Format

ipmcget -d diaginfo

Parameters

None

Usage Guidelines

To view the collected information, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the file (for example **dump_info.tar.gz**) from the **/tmp** directory to the local PC.

Example

Perform one-click information collection.

```
iBMC:/->ipmcget -d diaginfo
Download diagnose info to /tmp/ successfully.
```

4.7.18 Restoring the iBMC Factory Settings (restore)

Function

The **restore** command is used to restore the iBMC factory settings. The iBMC restarts after this command is executed.

Format

ipmcset -d restore

Parameters

None

Usage Guidelines

None

Example

Restore the iBMC factory settings.

```
iBMC:/->ipmcset -d restore
WARNING: The iBMC will automatically restart and restore factory settings. Continue? [Y/N]:Y
Restore factory setting successfully.
```

4.7.19 Enabling or Disabling the CLP Notimeout Function

Function

The **notimeout** command is used to enable or disable the CLP notimeout function. The setting takes effect only after you exit and log in to iBMC CLI again.

By default, the CLP notimeout function is disabled.

Format

ipmcset -d notimeout -v <enabled | disabled>

Parameters

Parameter	Description	Value
enabled	Enables the CLP notimeout function.	–

Parameter	Description	Value
disabled	Disables the CLP notimeout function.	-

Usage Guidelines

None

Example

\# Enable the CLP notimeout function.

iBMC:/->**ipmcset -d notimeout -v enabled**
Set no timeout state successfully.

\# Disable the CLP notimeout function.

iBMC:/->**ipmcset -d notimeout -v disabled**
Set no timeout state successfully.

4.7.20 Updating the System Workkey (workkey)

Function

The **workkey** command is used to update the system workkey.

Format

ipmcset -d workkey

Parameters

None

Usage Guidelines

None

Example

\# Update the system workkey.
iBMC:/->**ipmcset -d workkey**
Update system workkey successfully.

4.7.21 Querying and Setting Automatic Discovery Configuration (autodiscovery)

Function

The **autodiscovery** command is used to query and set the automatic discovery function.

Format

ipmcget -d autodiscovery

ipmcset -d autodiscovery -v <enable>/<disable> [option(0/1)] [netport]

Parameters

Parameter	Description	Value
enabled/disable	Enables or disables the automatic discovery function.	• **enable**: Enables automatic discovery. • **disable**: Disables automatic discovery.
option	Specifies a network segment.	• **0**: Broadcasts to 255.255.255.255 • **1**: Subnet broadcast address
netport	Specifies the port number.	0 to 65535

Usage Guidelines

None

Example

Query configuration of the automatic discovery function.

```
iBMC:/->ipmcget -d autodiscovery
State       : disabled
Broadcast   : 255.255.255.255
NetPort     : 26957
```

Enable the automatic discovery function.

```
iBMC:/->ipmcset -d autodiscovery -v enable 0 26957
Set state to (enable) successfully.
Set broadcast to (255.255.255.255) successfully.
Set netport to (26957) successfully.
```

4.7.22 Querying and Setting Controlled Power-on Configuration (poweronpermit)

Function

The **poweronpermit** command is used to query and set the controlled power-on function.

Format

ipmcget -d poweronpermit

ipmcset -d poweronpermit -v <**enable** | **disable**> [*ip*] [*netport*]

Parameters

Parameter	Description	Value
enable	Enables the controlled power-on function.	-
disable	Disables the controlled power-on function.	-
ip	Specifies the server IP address.	-
netport	Specifies the port number.	0 to 65535

Usage Guidelines

None

Example

Query configuration of the controlled power-on function.

```
iBMC:/->ipmcget -d poweronpermit
State        : enabled
ManagerIP    : 192.168.1.1
ManagerPort  : 26957
```

Enable the controlled power-on function.

```
iBMC:/->ipmcset -d poweronpermit -v enable 192.168.1.1 26957
Set poweronpermit successfully.
```

4.7.23 Querying and Clearing the Power-On Lock (poweronlock)

Function

By default, if the server is not powered on within the specified time, the function of powering on the server through the iBMC will be locked. As a result, the server cannot be powered on through the iBMC.

The **poweronlock** command is used to query the status of the power-on lock.

The **poweronlock -v clear** command is used to clear the lock.

Format

ipmcget -t maintenance -d poweronlock

ipmcset -t maintenance -d poweronlock -v clear

Parameters

None

Usage Guidelines

The iBMC supports this command from version V338.

Example

Query the power-on lock status.

```
iBMC:/->ipmcget -t maintenance -d poweronlock
Power on lock state: Locked
```

Clear the power-on lock.

```
iBMC:/->ipmcset -t maintenance -d poweronlock -v clear
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:Y
Clear power on lock successfully.
```

4.7.24 Querying and Setting BIOS Print Enablement Status (biosprint)

Function

The **biosprint** command is used to query and set BIOS debug. If BIOS debug is enabled, debug information will be sent to the serial port during the POST process.

Format

ipmcget -t maintenance -d biosprint

ipmcset -t maintenance -d biosprint -v *<option>*

Parameters

Parameter	Description	Value
<option>	Specifies the operation to be performed.	• **1**: forcibly enables BIOS debug. • **2**: applies the setting on the BIOS.

Usage Guidelines

The RH1288A V2 and RH2288A V2 do not support the command.

Example

Enable BIOS print.

```
iBMC:/->ipmcset -t maintenance -d biosprint -v 1
WARNING: Setting BIOS debug info enbale will make system start slow. Do you want to continue?[Y/N]y
Set BIOS debug info enable successfully
```

Query the BIOS print status.

```
iBMC:/->ipmcget -t maintenance -d biosprint
BIOS debug info enable
```

4.7.25 Restarting the iME (resetiME)

Function

The **resetiME** command is used to restart the Intel Management Engine (iME). When the iME cannot run properly, you can run this command to reset it.

Format

ipmcset -t maintenance -d resetiME

Parameters

None

Usage Guidelines

None

Example

Restart the iME.

```
iBMC:/->ipmcset -t maintenance -d resetiME
WARNING:
 The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
Reset iME successfully, the iME will restart soon.
```

4.8 User Management Commands

4.8.1 Querying the Information About All Users (userlist/list)

Function

The **userlist** command is used to query the information about all the users.

Format

ipmcget -d userlist

ipmcget -t user -d list

Parameters

None

Usage Guidelines

None

Example

Query the information about all the users.

```
iBMC:/->ipmcget -t user -d list
ID      Name          Privilege      Interface                      PublicKeyHash
State
2       root          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
3       test1         CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
4       test2         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
5       test3         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
6       test4         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
7       test5         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
8       test6         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
9       test7         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
10      test8         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
11      test9         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
12      test10        ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
13      test11        ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
14      test12        ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
15      test13        ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
16      test14        ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Disabled
17      test15        ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                   Enabled
```

4.8.2 Adding a User (adduser)

Function

The **adduser** command is used to add a user.

Format

ipmcset [-t user] -d adduser -v *<username>*

Parameters

Parameter	Description	Value
username	Specifies the user to be added.	A string of up to 16 characters meeting the following requirements ● Allow digits, letters, special characters. ● Avoid the following special characters: :<>&,'"/\% ● Avoid number sign (#) at the beginning.

Usage Guidelines

Only administrators can add users, and the administrator's password is required.

A maximum of 15 users can be added. The default permission of a newly added user is **No Access**, which supports access to all login interfaces.

A password must be set for the newly added user. The password setting rules vary depending on whether password complexity check and weak password check are enabled. To check whether password complexity check is enabled, run the **passwordcomplexity** command. To check whether weak password check is enabled, run the **weakpwddic** command.

● If password complexity check is disabled, the password cannot be empty or exceed 20 characters.

● If password complexity check is enabled, the password must meet the following requirements:

    – Contain 8 to 20 characters

    – Contain at least a space or one of the following special characters: `~!@#$%^&*()-_=+\|[{}];:'",<.>/?

    – Contain at least two types of the following characters:

        ■ Uppercase letters A to Z

        ■ Lowercase letters a to z

        ■ Digits 0 to 9

    – Cannot be the same as the user name or the user name in reverse order.

    – Have at least two new characters when compared with the previous password.

● If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)

Example

Add user **test**.

```
iBMC:/->ipmcset -d adduser -v test
```

Input your password:
Password:
Confirm password:
Add user successfully.

Query user information.

```
iBMC:/->ipmcget -d userlist
ID     Name          Privilege     Interface                     PublicKeyHash
State
2      root          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                  Enabled
3      test          NO ACCESS      Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                  Enabled
4                    NO ACCESS                    NA
Disabled
5                    NO ACCESS                    NA
Disabled
6                    NO ACCESS                    NA
Disabled
7                    NO ACCESS                    NA
Disabled
8                    NO ACCESS                    NA
Disabled
9                    NO ACCESS                    NA
Disabled
10                   NO ACCESS                    NA
Disabled
11                   NO ACCESS                    NA
Disabled
12                   NO ACCESS                    NA
Disabled
13                   NO ACCESS                    NA
Disabled
14                   NO ACCESS                    NA
Disabled
15                   NO ACCESS                    NA
Disabled
16                   NO ACCESS                    NA
Disabled
17                   NO ACCESS                    NA
Disabled
```

The user **test** is added successfully.

4.8.3 Changing the User Password (password)

Function

The **password** command is used to change the user password.

Format

ipmcset [-t user] -d password -v *username*

Parameters

Parameter	Description	Value
username	Specifies the user whose password needs to be changed.	-

Usage Guidelines

Administrators can change the password of any user. Operators and common users can only change their own passwords. The password of the current user is required.

The password setting rules vary depending on whether password complexity check and weak password check are enabled. To check whether password complexity check is enabled, run the **passwordcomplexity** command. To check whether weak password check is enabled, run the **weakpwddic** command.

- If password complexity check is disabled, the password cannot be empty or exceed 20 characters.
- If password complexity check is enabled, the password must meet the following requirements:
  - Contain 8 to 20 characters
  - Contain at least a space or one of the following special characters:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Contain at least two types of the following characters:
    - Uppercase letters A to Z
    - Lowercase letters a to z
    - Digits 0 to 9
  - Cannot be the same as the user name or the user name in reverse order.
  - Have at least two new characters when compared with the previous password.
- If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)

Example

Change the password of **user**.

```
iBMC:/->ipmcset -d password -v user
Input your password:
New password:
Confirm password:
Set user password successfully.
```

4.8.4 Deleting a User (deluser)

Function

The **deluser** command is used to delete a user.

Format

ipmcset [-t user] -d deluser -v *username*

Parameters

Parameter	Description	Value
username	Specifies the user to be deleted.	-

Usage Guidelines

- Only administrators can delete users, and the administrator's password is required.
- From iBMC V357, if there is only one administrator enabled in the iBMC system, the administrator cannot be deleted.

Example

Delete user **test**.

```
iBMC:/->ipmcset -d deluser -v test
Input your password:
Delete user successfully.
```

4.8.5 Setting User Rights (privilege)

Function

The **privilege** command is used to set user rights.

Format

ipmcset [-t user] -d privilege -v *<username> <privalue>*

Parameters

Parameter	Description	Value
username	Specifies the user to be set.	-
privalue	Specifies user rights.	• **15**: No Access • **2**: User • **3**: Operator • **4**: Administrator • **5**: Custom Role 1 • **6**: Custom Role 2 • **7**: Custom Role 3 • **8**: Custom Role 4

Usage Guidelines

- Only administrators can set user rights, and the administrator's password is required.

- In versions earlier than iBMC V357, the rights of the default users cannot be set. From iBMC V357, if the iBMC has multiple enabled administrators, the roles of the default users can be modified. If there is only one administrator enabled, this administrator cannot disabled or deleted and the administrator role cannot be modified.

  📖 **NOTE**

  The default user is **root** for V3 servers, and **Administrator** for V5 servers.

- In versions earlier than iBMC V357, user rights cannot be set for the users in SSH login mode. From iBMC V357, user rights can be set for such users.

Example

Grant user **test** with the **Administrator** rights.

```
iBMC:/->ipmcset -d privilege -v test 4
Input your password:
Set user privilege successfully.
```

4.8.6 Querying and Setting the Status of the Password Complexity Check Function (passwordcomplexity)

Function

The **passwordcomplexity** command is used to query and set the status of the password complexity check function.

Format

ipmcget [-t user] -d passwordcomplexity

ipmcset [-t user] -d passwordcomplexity -v <**enabled** | **disabled**>

Parameters

Parameter	Description	Value
enabled	Enables the password complexity check function.	-
disabled	Disables the password complexity check function.	-

Usage Guidelines

NOTICE

- The password complexity check function is enabled by default.
- Disabling the password complexity check function reduces the system security. Set the parameter with caution.

- If password complexity check is disabled, the password cannot be empty or exceed 20 characters.

- If password complexity check is enabled, the password must meet the following requirements:
  - Contain 8 to 20 characters
  - Contain at least a space or one of the following special characters:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Contain at least two types of the following characters:
    - Uppercase letters A to Z
    - Lowercase letters a to z
    - Digits 0 to 9
  - Cannot be the same as the user name or the user name in reverse order.
  - Have at least two new characters when compared with the previous password.

☐ **NOTE**

In addition to the password complexity check, the iBMC also checks for weak passwords for security purposes. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)

Only the administrators can set the status of the password complexity check function.

Example

Query the status of the password complexity check function.

```
iBMC:/->ipmcget -d passwordcomplexity
Password complexity check state : enabled
```

Enable the password complexity check function.

```
iBMC:/->ipmcset -d passwordcomplexity -v enabled
Set password complexity check state successfully.
```

4.8.7 Locking a User (user -d lock)

Function

The **lock** command is used to lock a specified user. The locked user cannot log in to the system.

Format

ipmcset -t user -d lock -v *username*

Parameters

Parameter	Description	Value
username	Specifies the name of the user to be locked.	-

Usage Guidelines

Only administrators have the permission to lock a user.

Enter the password of the current administrator when locking a user.

Example

lock user **admin**.

```
iBMC:/->ipmcset -t user -d lock -v admin
Input your password:
Lock user:admin successfully.
```

4.8.8 Unlocking a User (user -d unlock)

Function

The **unlock** command is used to unlock a user in locked state.

Format

ipmcset -t user -d unlock -v *username*

Parameters

Parameter	Description	Value
username	Specifies the user to be unlocked.	-

Usage Guidelines

Only administrators can perform this operation, and the administrator's password is required.

Example

Unlock user **root**.

```
iBMC:/->ipmcset -t user -d unlock -v root
Input your password:
Set user:root unlock status successfully.
```

4.8.9 Querying and Setting the Minimum Password Age (minimumpasswordage)

Function

The **minimumpasswordage** command is used to query or set the minimum password age.

The minimum password age is the shortest time period for which a password must be used after it was set. During this period, the password cannot be changed.

Format

ipmcget -d minimumpasswordage

ipmcset -d minimumpasswordage -v *time*

Parameters

Parameter	Description	Value
time	Specifies the minimum password age.	Value range: 0 to 365 The value **0** indicates that the passwords do not have a minimum password age.

Usage Guidelines

Only the system administrator can set the minimum password age.

Example

Set the minimum password age to one day.

```
iBMC:/->ipmcset -d minimumpasswordage -v 1
Set minimum password age successfully, minimumpasswordage(1) days.
```

Query the minimum password age.

```
iBMC:/->ipmcget -d minimumpasswordage
Minimum password age: 1
```

4.8.10 Setting an Emergency User (emergencyuser)

Function

The **emergencyuser** command is used to set an emergency user, which is not restricted by any login rule.

Format

ipmcset [-t user] -d emergencyuser -v *username*

Parameters

Parameter	Description	Value
username	Emergency user name.	-

Usage Guidelines

Only an administrator can set an emergency user.

Example

Set **root** as an emergency user.

```
iBMC:/->ipmcset -d emergencyuser -v root
Set emergency user to (root) successfully.
```

4.8.11 Importing an SSH Public Key for a User (addpublickey)

Function

The **addpublickey** command is used to import an SSH public key for a user.

Format

ipmcset -t user -d addpublickey -v *username <filepath|file_URL>*

Parameters

Parameter	Description	Value
username	Specifies the user for whom the SSH public key is to be imported.	An existing user name.
filepath	Specifies the path from which the public key will be imported.	The value must be in the **/Path/File name** format. For example, **/tmp/id_dsa_1024.key**
file_URL	Specifies the URL of the public key file to be imported.	A value in the following format: *protocol://username:password*@IP:[port]/ *directory/filename* Where: *protocol* must be **https** or **http**. *username* and *password* are the user name and password for accessing the target server. *directory/filename* is the path of the public key file on the target server.

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the SSH public key file to the specified directory (for example **/tmp**) of the iBMC file system.

The administrators can import SSH public keys for all users. Common users can import only their own SSH public keys.

Example

Import an SSH public key for user **ssh_user**.

```
iBMC:/->ipmcset -t user -d addpublickey -v ssh_user /tmp/id_dsa_1024.key
Input your password:
Add user public key successfully.
```

4.8.12 Deleting the SSH Public Key of a User (delpublickey)

Function

The **delpublickey** command is used to delete the SSH public key of a user.

Format

ipmcset -t user -d delpublickey -v *username*

Parameters

Parameter	Description	Value
username	Specifies the user whose SSH public key is to be deleted.	–

Usage Guidelines

The administrators can delete the SSH public keys of all users. Common users can delete only their own SSH public keys.

Example

Delete the public key of user **ssh_user_01**.

```
iBMC:/->ipmcset -t user -d delpublickey -v ssh_user_01
Input your password:
Delete user public key successfully.
```

4.8.13 Querying and Setting the SSH User Password Authentication Enablement Status (sshpasswordauthentication)

Function

The **sshpasswordauthentication** command is used to enable or disable SSH user password authentication.

Format

ipmcget -t user -d sshpasswordauthentication

ipmcset -t user -d sshpasswordauthentication -v <**enabled** | **disabled**>

Parameters

Parameter	Description	Value
enabled	Indicates that SSH user password authentication will be enabled.	–
disabled	Indicates that SSH user password authentication will be disabled.	–

Usage Guidelines

None

Example

\# Enable SSH user password authentication.

```
iBMC:/->ipmcset -t user -d sshpasswordauthentication -v enabled
Set SSH password authentication successfully.
```

\# Query the enablement status of SSH user password authentication.

```
iBMC:/-> ipmcget -t user -d sshpasswordauthentication
SSH Password Authentication : enabled
```

4.8.14 Setting the User Interfaces for Logging to iBMC (interface)

Function

The **interface** command is used to set the user interfaces that can be used by specified users to log in to iBMC.

Format

ipmcset -t user -d interface -v *username* <**enabled** | **disabled**> <*option1 option2 … optionN*>

Parameters

Parameter	Description	Value
username	Name of the user to be configured.	–
enabled	Indicates that the interfaces will be enabled.	–
disabled	Indicates that the interfaces will be disabled.	–

Parameter	Description	Value
option1 *option2 ...* *optionN*	Indicates the interface types to be configured.	You can set multiple interface types at a time. The options are: • **1**: Web • **2**: SNMP • **3**: IPMI • **4**: SSH • **5**: SFTP • **7**: Local • **8**: Redfish

Usage Guidelines

None

Example

Enable the iBMC login interfaces **Web, SNMP, IPMI, SSH, SFTP, Local** for the **test** user.

```
iBMC:/->ipmcset -t user -d interface -v test enabled 1 2 3 4 5 7
Input your password:
Set user login interface successfully.
```

Query information about the **ssh_user_01** user.

```
iBMC:/->ipmcget -t user -d list
ID    Name          Privilege    Interface                            PublicKeyHash
2     root          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish       NA
3     xxx           CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish       NA
4     commonuser    USER         Web,SNMP,IPMI,SSH,SFTP,Local,Redfish       NA
5     admin         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish        NA
6     operator      OPERATOR       Web,SNMP,IPMI,SSH,SFTP,Local,Redfish       NA
7     custom1       CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish        NA
8     test          USER         Web,SNMP,IPMI,SSH,SFTP,Local                NA
9                   NO ACCESS                                        NA
10                  NO ACCESS                                        NA
11                  NO ACCESS                                        NA
12                  NO ACCESS                                        NA
13                  NO ACCESS                                        NA
14                  NO ACCESS                                        NA
15                  NO ACCESS                                        NA
16                  NO ACCESS                                        NA
17                  NO ACCESS
```

4.8.15 Setting Weak Password Check State (weakpwddic)

Function

The **weakpwddic** command can be used to enable or disable weak password check.

The password in the weak password dictionary cannot be used as any of the following:

- Local user password

- SNMPv1/v2c read-only or read/write community name

- SNMPv3 encryption password

Format

ipmcset -t user -d weakpwddic -v <**enabled** | **disabled**>

Parameters

Parameter	Description	Value
enabled	Enables weak password check.	–
disabled	Disables weak password check.	–

Usage Guidelines

This command is available only for V5 servers.

Example

Enable weak password check.

```
iBMC:/-> ipmcset -t user -d weakpwddic -v enabled
Enable weak password dictionary check successfully.
```

4.8.16 Exporting the Weak Password Dictionary (weakpwddic -v export)

Function

The **weakpwddic -v export** command is used to export the weak password dictionary of the iBMC.

Format

ipmcset -t user -d weakpwddic -v export <*filepath* | *file_URL*>

Parameters

Parameter	Description	Value
filepath	Specifies the local directory in which the weak password dictionary is stored.	Absolute directory on the iBMC, for example, **/tmp/weakpwddictionary**.

Parameter	Description	Value

file_URL	Specifies the remote path of the weak password dictionary.	The format is as follows: *protocol://username:password@IP:[port]/directory/filename* Where,
		
		 • *protocol* must be **https**, **sftp**, **cifs**, **scp**, or **nfs**.
		 NOTE
		   • The iBMC supports only Server Message Block (SMB) V1.0.
		   • When the NFS protocol is used, the storage path cannot contain the *username:password@* field. When the HTTPS is used, the *username:password@* field is optional in the storage path. When the CIFS protocol is used, the storage path must contain the *username:password@* field.
		   • If the NFS protocol is used, the path cannot contain **username:password@**. If other protocols are used, the path must contain **username:password@**.
		
		 • *username* indicates the user name for logging in to the target server.
		
		 • *password* indicates the password for logging in to the target server.
		
		 • *IP:[port]* indicates the IP address and port number of the target server.
		
		 • *directory/filename* indicates the absolute directory in which the weak password dictionary is stored on the target server.
		
		 Example value: **https://root:Test12#$@10.10.10.1:443/tmp/weakpwddictionary**

Usage Guidelines

This command is available only for V5 servers.

To view the weak password dictionary, use a file transfer tool supporting SFTP (for example WinSCP) to transfer the **weakpwddictionary** file from **/tmp** to the local PC.

Example

Export the weak password dictionary.

iBMC:/-> **ipmcset -t user -d weakpwddic -v export /tmp/weakpwddictionary**
Export weak password dictionary successfully.

4.8.17 Importing the Weak Password Dictionary (weakpwddic -v import)

Function

The **weakpwddic -v import** command is used to import the weak password dictionary to the iBMC.

Format

ipmcset -t user -d weakpwddic -v import <*filepath* | *file_URL*>

Parameters

Parameter	Description	Value
filepath	Specifies the directory in which the weak password dictionary is imported on the iBMC.	Absolute directory on the iBMC, for example, **/tmp/weakpwddictionary**.

Parameter	Description	Value
file_URL	Specifies the remote path of the weak password dictionary.	The format is as follows: *protocol://username:password@IP: [port]/directory/filename* Where, ● *protocol* must be **https**, **sftp**, **cifs**, **scp**, or **nfs**. NOTE ● The iBMC supports only Server Message Block (SMB) V1.0. ● When the NFS protocol is used, the storage path cannot contain the *username:password@* field. When the HTTPS is used, the *username:password@* field is optional in the storage path. When the CIFS protocol is used, the storage path must contain the *username:password@* field. ● If the NFS protocol is used, the path cannot contain **username:password@**. If other protocols are used, the path must contain **username:password@**. ● *username* indicates the user name for logging in to the target server. ● *password* indicates the password for logging in to the target server. ● *IP:[port]* indicates the IP address and port number of the target server. ● *directory/filename* indicates the absolute directory in which the weak password dictionary is stored on the target server. Example value: **https://root:Test12# $@10.10.10.1:443/tmp/ weakpwddictionary**

Usage Guidelines

This command is available only for V5 servers.

Before running this command, use a file transfer tool supporting SFTP (for example WinSCP) to transfer the file to be imported to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Import the weak password dictionary.

iBMC:/-> **ipmcset -t user -d weakpwddic -v import /tmp/weakpwddictionary**
Import weak password dictionary successfully.

4.8.18 Setting the SNMPv3 User Encryption Password (snmpprivacypassword)

Function

The **snmpprivacypassword** command is used to set the data encryption password for a user who uses SNMPv3 to connect to the iBMC.

Format

ipmcset -t user -d snmpprivacypassword -v *username*

Parameters

Parameter	Description	Value
username	Indicates the existed user whose password is to be changed.	-

Usage Guidelines

This command is available only for V5 servers.

Administrators can change the password of any user. Operators and common users can only change their own passwords. The password of the current user is required.

The password setting rules vary depending on whether password complexity check and weak password check are enabled. To check whether password complexity check is enabled, run the **passwordcomplexity** command. To check whether weak password check is enabled, run the **weakpwddic** command.

- If password complexity check is disabled, the password cannot be empty or exceed 20 characters.
- If password complexity check is enabled, the password must meet the following requirements:
  - Contain 8 to 20 characters
  - Contain at least a space or one of the following special characters:
    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Contain at least two types of the following characters:
    - Uppercase letters A to Z
    - Lowercase letters a to z
    - Digits 0 to 9
  - Cannot be the same as the user name or the user name in reverse order.
  - Have at least two new characters when compared with the previous password.

- If weak password check is enabled, the password cannot be the same as the passwords contained in the weak password dictionary. (You can run the **ipmcset -t user -d weakpwddic -v export** command to export the weak passwords from the weak password dictionary.)

Example

Set the password for the SNMPv3 user.

```
iBMC:/->ipmcset -t user -d snmpprivacypassword -v Administrator
Input your password:
Password:
Confirm password:
Set snmp privacy password successfully.
```

4.8.19 Querying and Setting User Inactive Period (securityenhance -d inactivetimelimit)

Function

The **securityenhance -d inactivetimelimit** command is used to query and set the user inactive period. If a user does not perform any operation during the specified period, the user will be disabled.

Format

ipmcset -t securityenhance -d inactivetimelimit -v *<value>*

ipmcget -t securityenhance -d inactivetimelimit

Parameters

Parameter	Description	Value
value	Inactive period (in days).	0 30 to 365 The value **0** indicates unlimited time, that is, the user will never be disabled.

Usage Guidelines

None.

Example

Set the user inactive period to 30 days.

```
iBMC:/-> ipmcset -t securityenhance -d inactivetimelimit -v 30
WARNING: This operation could lead to iBMC users be disabled when users' inactive time is overdue.
Do you want to continue?[Y/N]y
Set inactive user timelimit successfully.
```

Query the user inactive period.

4.8.20 Setting User Status (user -d state)

Function

The **user -d state** command is used to enable or disable a user.

Format

ipmcset -t user -d state -v <*username*> [**enabled** | **disabled**]

ipmcget -d userlist

Parameters

Parameter	Description	Value
username	Name of the user.	An existing user name.
enabled	Enables the user.	-
disabled	Disables the user.	-

Usage Guidelines

If there is only one administrator enabled in the iBMC system, the administrator cannot be disabled.

Example

Enable user **test15**.

```
iBMC:/-> ipmcset -t user -d state -v test15 enabled
Input your password:
Enable user:test15 successfully.
```

Query the status of user **test15**.

```
iBMC:/-> ipmcget -d userlist
ID     Name          Privilege    Interface                      PublicKeyHash
State
2      root          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 Enabled
3      test1         CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 Enabled
4      test2         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 Enabled
5      test3         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 Enabled
6      test4         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 disabled
7      test5         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 Enabled
8      test6         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                 Enabled
9      test7         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
```

NA			disabled	
10	test8	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			Enabled	
11	test9	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			disabled	
12	test10	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			disabled	
13	test11	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			disabled	
14	test12	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			disabled	
15	test13	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			disabled	
16	test14	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			disabled	
17	**test15**	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	
NA			**Enabled**	

4.8.21 Querying and Setting the In-Band User Management Status (user -d usermgmtbyhost)

Function

The **user -d usermgmtbyhost** command is used to enable or disable in-band user management or query the in-band user management settings.

Format

ipmcset -t user -d usermgmtbyhost -v *<option>*

ipmcget -t user -d usermgmtbyhost

Parameters

Parameter	Description	Value
<option>	Status of in-band user management.	● **0**: disables in-band user management. ● **1**: enables in-band user management.

Usage Guidelines

If in-band user management is disabled, user management cannot be performed through the BIOS or by using the IPMI commands sent in in-band mode.

Example

Disable in-band user management.

iBMC:/->**ipmcset -t user -d usermgmtbyhost -v** 0
The BMC user management function is successfully disabled on the host side.

Query the in-band user management settings.

iBMC:/->**ipmcget -t user -d usermgmtbyhost**
Disable

4.9 NTP Commands

4.9.1 Querying NTP Information (ntpinfo)

Function

The **ntpinfo** command is used to query Network Time Protocol (NTP) information about the iBMC.

Format

ipmcget -d ntpinfo

Parameters

None

Usage Guidelines

None

Example

Query iBMC NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status            : enabled
Mode              : manual
Preferred Server  : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.9.2 Setting NTP State (ntp -d status)

Function

The **ntp -d status** command is used to enable or disable the NTP function.

Format

ipmcset -t ntp -d status -v *status*

Parameters

Parameter	Description	Value
status	Indicates the NTP status.	● enabled ● disabled

Usage Guidelines

None

Example

Enable the NTP function.

```
iBMC:/->ipmcset -t ntp -d status -v enabled
Set NTP enable status (enabled) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status             : enabled
Mode               : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server       : 192.168.2.2
Synchronize        : successful
Auth Enable        : enabled
Group Key          : imported
```

4.9.3 Setting the Method for Obtaining NTP Information (ntp -d mode)

Function

The **ntp -d mode** command is used to set how to obtain NTP information.

Format

ipmcset -t ntp -d mode –v *mode*

Parameters

Parameter	Description	Value
mode	Indicates how to obtain NTP information.	• **manual**: Manually set NTP information. • **dhcpv4**: Automatically obtain NTP information using DHCPv4. • **dhcpv6**: Automatically obtain NTP information using DHCPv6.

Usage Guidelines

If *mode* is **DHCPv4**, you do not need to set the time zone data.

Example

Enable NTP information to be manually set.

```
iBMC:/->ipmcset -t ntp -d mode -v manual
Set NTP mode (manual) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status            : enabled
Mode              : manual
Preferred Server  : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.9.4 Setting an Address for the Preferred NTP Server (ntp -d preferredserver)

Function

The **ntp -d preferredserver** command is used to set an address for the preferred NTP server.

Format

ipmcset -t ntp -d preferredserver –v *addr*

Parameters

Parameter	Description	Value
addr	Indicates the IP address of the preferred NTP server.	The value can be any of the following: ● IPv4 address ● IPv6 address ● Domain name

Usage Guidelines

- The iBMC versions earlier than V312 support only the Linux NTP servers.
- The iBMC supports Linux and Windows NTP servers from V312.

Example

Set the preferred NTP server address to **dhcp1.com**.

```
iBMC:/->ipmcset -t ntp -d preferredserver -v dhcp1.com
Set NTP preferred server (dhcp1.com) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status            : enabled
Mode              : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server       : 192.168.2.2
Synchronize        : successful
Auth Enable        : enabled
Group Key          : imported
```

4.9.5 Setting an Address for the Alternative NTP Server (ntp -d alternativeserver)

Function

The **ntp -d alternativeserver** command is used to set an address for the alternative NTP server.

Format

ipmcset -t ntp -d alternativeserver –v *addr*

Parameters

Parameter	Description	Value
addr	Indicates the address of the alternative NTP server.	The value can be any of the following: ● IPv4 address ● IPv6 address ● Domain name

Usage Guidelines

- The iBMC versions earlier than V312 support only the Linux NTP servers.
- The iBMC supports Linux and Windows NTP servers from V312.

Example

Set the alternative NTP server address to **fc00::1234**.

```
iBMC:/-> ipmcset -t ntp -d alternativeserver -v fc00::1234
Set NTP alternative server (fc00::1234) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.9.6 Setting an Address for an Extra NTP Server (ntp -d extraserver)

Function

The **ntp -d extraserver** command is used to set an address for an extra NTP server.

Format

ipmcset -t ntp -d extraserver -v *addr*

Parameters

Parameter	Description	Value
addr	Specifies the address of the extra NTP server.	The value can be any of the following: ● IPv4 address ● IPv6 address ● Domain name **NOTE** The value **0.0.0.0** indicates that the address of the extra NTP server is deleted.

Usage Guidelines

- iBMC V505 and later support this command.
- The iBMC versions earlier than V312 support only the Linux NTP servers.
- The iBMC supports Linux and Windows NTP servers from V312.

Example

Set an extra NTP server with IP address of **192.168.2.2**.

```
iBMC:/->ipmcset -t ntp -d extraserver -v 192.168.2.2
Set NTP extraserver server (192.168.2.2) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status            : enabled
Mode              : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server       : 192.168.2.2
Synchronize        : successful
Auth Enable        : enabled
Group Key          : imported
```

4.9.7 Setting NTP Server Authentication (ntp -d authstatus)

Function

The **ntp -d authstatus** command is used to set the NTP server authentication status.

- If authentication is enabled, an authentication is performed before communication between the iBMC and the NTP server.
- If authentication is disabled, no authentication is required before communication between the iBMC and the NTP server.

Format

ipmcset -t ntp -d authstatus -v *status*

Parameters

Parameter	Description	Value
status	Indicates whether an authentication is required.	• enabled • disabled

Usage Guidelines

If authentication is enabled, you must upload the group key to the iBMC.

Example

Enable authentication for NTP servers.

```
iBMC:/->ipmcset -t ntp -d authstatus -v enabled
Set NTP enable status (enabled) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status             : enabled
Mode               : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server       : 192.168.2.2
Synchronize        : successful
Auth Enable        : enabled
Group Key          : imported
```

4.9.8 Uploading the NTP Group Key (ntp -d groupkey)

Function

The **ntp -d groupkey** command is used to upload the NTP group key to the iBMC. The NTP group key is used in identity authentication for communication between the iBMC and the NTP server.

Format

ipmcset -t ntp -d groupkey -v *filepath*

Parameters

Parameter	Description	Value
filepath	Specifies the file that contains the group key.	In the **/file path/file name** format. For example, **/tmp/ntp.keys**.

Usage Guidelines

Before running this command, use a file transfer tool that supports SFTP, for example WinSCP, to transfer the key file to the specified directory (for example **/tmp**) of the iBMC file system.

Example

Upload the NTP group key to the iBMC.

```
iBMC:/->ipmcset -t ntp -d groupkey -v /tmp/ntp.keys
Set NTP group key (/tmp/ntp.keys) successfully.
```

Query NTP information.

```
iBMC:/->ipmcget -d ntpinfo
Status            : enabled
Mode              : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10 Indicator Commands

4.10.1 Querying the State of the Current Indicator (ledinfo)

Function

The **ledinfo** command is used to query the state of the current indicator.

Format

ipmcget -d ledinfo

Parameters

None

Usage Guidelines

None

Example

Query the status of the indicator.

```
iBMC:/->ipmcget -d ledinfo
LED Name          : SysHealLed
LED Mode          : Local Control
LED State         : BLINKING
Off Duration      : 100 ms
On Duration       : 100 ms
LED Color         : RED
```

```
LED Color Capabilities : RED GREEN
Default LED Color in
    Local Control    : GREEN
    Override State   : GREEN

LED Name             : UIDLed
LED Mode             : Local Control
LED State            : OFF
LED Color            : BLUE
LED Color Capabilities : BLUE
Default LED Color in
    Local Control    : BLUE
    Override State   : BLUE
```

4.10.2 Setting the UID Indicator (identify)

Function

The **identify** command is used to set the UID indicator.

Format

ipmcset -d identify [**-v** {*time* | **force** }]

Parameters

Parameter	Description	Value
time	Specifies the time (in seconds) for which the UID indicator blinks.	Value range: 0 to 255 The value **0** indicates that the UID indicator is off.
force	Forces the UID indicator to be steady on.	-

Usage Guidelines

If *time* is not set, the UID indicator blinks for 15 seconds by default.

Example

Turn on the UID indicator permanently.

```
iBMC:/->ipmcset -d identify -v force
Identify UID led successfully.
```

4.10.3 Setting the UID Indicator Status (locate)

Function

The **locate** command is used to set the Unit Identification (UID) indicator status of a hard disk. The UID indicator helps locate a hard disk in a chassis.

Format

ipmcset -d locate -v <*ID*> <*Action*>

Parameters

Parameter	Description	Value
ID	Specifies the ID of a hard disk.	**0** to **255**
Action	Specifies the UID indicator status.	**start**: turns on the UID indicator of a hard disk. **stop**: turns off the UID indicator of a hard disk.

Usage Guidelines

Before running this command, ensure that the following conditions are met:

- The hard disk is managed by a RAID controller card.
- The RAID controller card supports iBMC out-of-band management. You can refer to the **Technical Specifications** section in the RAID controller card user guide to determine whether the RAID card supports the iBMC out-of-band management.
- The BIOS has started.

If **Action** is **start**, the UID indicator of the hard disk will keep blinking.

Example

Turn on the UID indicator of hard disk 5.

```
iBMC:/->ipmcset -d locate -v 5 start
start locating physical drive (ID:5) successfully
```

4.11 Fan Commands

4.11.1 Setting the Fan Speed (fanlevel)

Function

The **fanlevel** command is used to set the fan speed.

Format

ipmcset -d fanlevel -v <*fanlevel*> [*fanid*]

Parameters

Parameter	Description	Value
fanlevel	Indicates the percentage of the current fan speed to the full fan speed.	The value is an integer. The value range varies with the server model.
fanid	Indicates the ID of the fan.	The value range varies with the server model.

Usage Guidelines

- If the fan ID is not specified, the command sets the fan rotation speed for all fans.
- This command is valid only when the fan runs in the manual mode.

  For details about how to configure the fan mode, see **4.11.2 Setting the Fan Mode (fanmode)**.

Example

Set the speed of fan 2 to 50% of the full speed.

```
iBMC:/->ipmcset -d fanlevel -v 50 2
Set fan(2) level to (50%) successfully.
Current Mode        :   Auto
iBMC:/->ipmcset -d fanlevel -v 50
Set fan level successfully.
Current Mode        :   Auto
Global Manual Fan Level:   50%
```

4.11.2 Setting the Fan Mode (fanmode)

Function

The **fanmode** command is used to set the fan mode.

Format

ipmcset -d fanmode -v *<mode>* [*timeout*]

Parameters

Parameter	Description	Value
mode	Specifies the fan mode.	- **0**: automatic mode In this mode, *timeout* need not be specified. - **1**: manual mode In this mode, *timeout* must be specified.

Parameter	Description	Value
timeout	Specifies the time period (in seconds) after which a manual-to-automatic switchover is triggered.	Default value: **30** The value **0** indicates that the fan mode will not be switched over.

Usage Guidelines

The fan work mode changes to automatic in any of the following scenarios:

- The iBMC restarts.
- The server is powered off.
- The switchover from the manual to automatic mode times out.

Example

Set the fan mode to manual and the timeout period to 60 seconds.

```
iBMC:/->ipmcset -d fanmode -v 1 60
Set fan mode successfully.
Current Mode:      manual
Time out   :      60 seconds
```

4.11.3 Querying the Fan State (faninfo)

Function

The **faninfo** command is used to query the fan state.

Format

ipmcget -d faninfo

Parameters

None

Usage Guidelines

None

Example

Query the fan state.

```
iBMC:/->ipmcget -d faninfo
Get fan mode and fan level successfully!
Current mode: manual,timeout 297 seconds.
Manual fan level is 80.
```

4.12 Sensor Commands

4.12.1 Querying All Sensor Information (sensor -d list)

Function

The **sensor -d list** command is used to query information about all the sensors.

Format

ipmcget -t sensor -d list

Parameters

None

Usage Guidelines

None

Example

Query information about all the sensors. (The sensors vary with the server mode.)

```
iBMC:/->ipmcget -t sensor -d list
sensor id  | sensor name   | value     | unit       | status | lnr      | lc       | lnc      | unc     | uc      |
unr     | phys  | nhys
0x1      | Inlet Temp    | 24.000    | degrees C   | ok    | na      | na      | na      | 42.000  | 44.000
| na      | 2.000  | 2.000
0x2      | Outlet Temp   | 30.000    | degrees C   | ok    | na      | na      | na      | na      | na      |
na      | 2.000  | 2.000
0x3      | PCH Temp      | 32.000    | degrees C   | ok    | na      | na      | na      | 90.000  | na
| na      | 3.000  | 3.000
0x4      | CPU1 Core Rem | 30.000    | degrees C   | ok    | na      | na      | na      | na      | na
| na      | 0.000  | 0.000
0x5      | CPU2 Core Rem | 30.000    | degrees C   | ok    | na      | na      | na      | na      | na
| na      | 0.000  | 0.000
0x6      | CPU1 DTS      | -65.000   | unspecified | ok    | na      | na      | na      | -1.000  | na
| na      | 3.000  | 3.000
0x7      | CPU2 DTS      | -66.000   | unspecified | ok    | na      | na      | na      | -1.000  | na
| na      | 3.000  | 3.000
0x8      | CPU1 Prochot  | 30.000    | degrees C   | ok    | na      | na      | na      | na      | 90.000
| na      | 0.000  | 0.000
0x9      | CPU2 Prochot  | 30.000    | degrees C   | ok    | na      | na      | na      | na      | 90.000
| na      | 0.000  | 0.000
0xa      | CPU1 VDDQ Temp | 32.000    | degrees C   | ok    | na      | na      | na      | 120.000 |
na      | na      | 3.000  | 3.000
0xb      | CPU2 VDDQ Temp | 32.000    | degrees C   | ok    | na      | na      | na      | 120.000 |
na      | na      | 3.000  | 3.000
0xc      | CPU1 VRD Temp | 33.000    | degrees C   | ok    | na      | na      | na      | 120.000 |
na      | na      | 3.000  | 3.000
0xd      | CPU2 VRD Temp | 31.000    | degrees C   | ok    | na      | na      | na      | 120.000 |
na      | na      | 3.000  | 3.000
0xe      | CPU1 MEM Temp | 27.000    | degrees C   | ok    | na      | na      | na      | 90.000  |
na      | na      | 3.000  | 3.000
0xf      | CPU2 MEM Temp | 27.000    | degrees C   | ok    | na      | na      | na      | 90.000  |
na      | na      | 3.000  | 3.000
0x10     | +3.3V         | 3.260     | Volts      | ok    | na      | 2.980    | na      | na      | 3.620   |
na      | 0.160  | 0.160
0x11     | +5.0V         | 4.980     | Volts      | ok    | na      | 4.530    | na      | na      | 5.490   |
na      | 0.240  | 0.240
0x12     | +12.0V        | 12.120    | Volts      | ok    | na      | 10.800   | na      | na      | 13.200  |
na      | 0.480  | 0.480
```

0x13	+1.8V CPU1	1.800	Volts	ok	na	1.470	na	na	1.850	na	0.020	0.020
0x14	+1.8V CPU2	1.790	Volts	ok	na	1.470	na	na	1.850	na	0.020	0.020
0x15	+1.2V VDDQ1	1.180	Volts	ok	na	1.140	na	na	1.260	na	0.020	0.020
0x16	+1.2V VDDQ2	1.180	Volts	ok	na	1.140	na	na	1.260	na	0.020	0.020
0x17	+1.2V VDDQ3	1.180	Volts	ok	na	1.140	na	na	1.260	na	0.020	0.020
0x18	+1.2V VDDQ4	1.180	Volts	ok	na	1.140	na	na	1.260	na	0.020	0.020
0x19	FAN1 F Speed	6720.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x1a	FAN1 R Speed	6720.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x1b	FAN2 F Speed	6600.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x1c	FAN2 R Speed	6600.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x1d	FAN3 F Speed	6720.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x1e	FAN3 R Speed	6720.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x1f	FAN4 F Speed	6600.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x20	FAN4 R Speed	6600.000	RPM	ok	na	na	na	na	na	na	0.000	0.000
0x21	RearDisk1 Temp	26.000	degrees C	ok	na	na	na	53.000	na	na	2.000	2.000
0x22	Power1	124.000	Watts	ok	na	na	na	na	na	na	0.000	0.000
0x23	Power2	52.000	Watts	ok	na	na	na	na	na	na	0.000	0.000
0x24	CPU1 Status	0x0	discrete	0x8080	na	na	na	na	na	na	na	na
0x25	CPU2 Status	0x0	discrete	0x8080	na	na	na	na	na	na	na	na
0x26	CPU1 Memory	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x27	CPU2 Memory	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x28	FAN1 F Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x29	FAN1 R Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x2a	FAN2 F Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x2b	FAN2 R Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x2c	FAN3 F Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x2d	FAN3 R Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x2e	FAN4 F Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x2f	FAN4 R Status	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x30	PS1 Presence	0x0	discrete	0x8002	na	na	na	na	na	na	na	na
0x31	PS2 Presence	0x0	discrete	0x8002	na	na	na	na	na	na	na	na
0x32	DIMM000	0x0	discrete	0x8040	na	na	na	na	na	na	na	na
0x33	DIMM001	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x34	DIMM002	0x0	discrete	0x8000	na	na	na	na	na	na	na	na
0x35	DIMM010	0x0	discrete	0x8040	na	na	na	na	na	na	na	na

na	na	na								
0x36	DIMM011	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x37	DIMM012	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x38	DIMM020	0x0	discrete	0x8040	na	na	na	na	na	
na	na	na								
0x39	DIMM021	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x3a	DIMM022	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x3b	DIMM030	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x3c	DIMM031	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x3d	DIMM032	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x3e	DIMM100	0x0	discrete	0x8040	na	na	na	na	na	
na	na	na								
0x3f	DIMM101	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x40	DIMM102	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x41	DIMM110	0x0	discrete	0x8040	na	na	na	na	na	
na	na	na								
0x42	DIMM111	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x43	DIMM112	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x44	DIMM120	0x0	discrete	0x8040	na	na	na	na	na	
na	na	na								
0x45	DIMM121	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x46	DIMM122	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x47	DIMM130	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x48	DIMM131	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x49	DIMM132	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x4a	AreaIntrusion	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x4b	RTC Battery	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x4c	PCIE Status	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x4d	ACPI State	0x0	discrete	0x8001	na	na	na	na	na	
na	na	na								
0x4e	SysFWProgress	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x4f	Power Button	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x50	SysRestart	0x0	discrete	0x8080	na	na	na	na	na	
na	na	na								
0x51	Boot Error	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x52	Watchdog2	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x53	Mngmnt Health	0x0	discrete	0x8000	na	na	na	na		
na	na	na	na							
0x54	UID Button	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x55	PwrOk Sig. Drop	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								
0x56	PwrOn TimeOut	0x0	discrete	0x8000	na	na	na	na		
na	na	na	na							
0x57	PwrCap Status	0x0	discrete	0x8000	na	na	na	na	na	
na	na	na								

0x58	HDD Backplane	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x59	HDD BP Status	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x5a	Riser1 Card	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x5b	Riser2 Card	0x0	discrete	0x8002	na	na	na	na	na	na	na
0x5c	SAS Cable	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x5d	FAN1 F Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x5e	FAN1 R Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x5f	FAN2 F Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x60	FAN2 R Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x61	FAN3 F Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x62	FAN3 R Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x63	FAN4 F Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x64	FAN4 R Presence	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x65	RAID Presence	0x0	discrete	0x8002	na	na	na	na	na	na	na
0x66	CPU Usage	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x67	Memory Usage	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x68	LCD Status	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x69	LCD Presence	0x0	discrete	0x8001	na	na	na	na	na	na	na
0x6a	RAID Status	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x6b	DISK0	0x0	discrete	0x8001	na	na	na	na	na	na	na
0x6c	DISK1	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x6d	DISK2	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x6e	DISK3	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x6f	DISK4	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x70	DISK5	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x71	DISK6	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x72	DISK7	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x73	DISK8	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x74	DISK9	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x75	DISK10	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x76	DISK11	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x77	DISK12	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x78	DISK13	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x79	DISK14	0x0	discrete	0x8000	na	na	na	na	na	na	na
0x7a	DISK15	0x0	discrete	0x8000	na	na	na	na	na	na	na

na		na		na					
0x7b		DISK16		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x7c		DISK17		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x7d		DISK18		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x7e		DISK19		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x7f		DISK20		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x80		DISK21		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x81		DISK22		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x82		DISK23		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x83		DISK24		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x84		DISKA		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x85		DISKB		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x86		DISKC		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x87		DISKD		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x88		Eth1 Link Down		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x89		Eth2 Link Down		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x8a		Eth3 Link Down		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x8b		Eth4 Link Down		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x8c		PS1 Status		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x8d		PS1 Fan Status		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x8e		PS2 Status		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x8f		PS2 Fan Status		0x0		discrete		0x8000	na		na		na		na		na	
na		na		na					
0x90		PCIE SW1 Temp		na		degrees C		na		na		na		na		100.000	
na		na		2.000		2.000			
0x91		PCIE SW2 Temp		na		degrees C		na		na		na		na		100.000	
na		na		2.000		2.000			
0x93		LOM P1 Link Down	0x0		discrete		0x8100	na		na		na		na		
na		na		na		na			
0x94		LOM P2 Link Down	0x0		discrete		0x8100	na		na		na		na		
na		na		na		na			
0x95		LOM P3 Link Down	0x0		discrete		0x8100	na		na		na		na		
na		na		na		na			
0x96		LOM P4 Link Down	0x0		discrete		0x8100	na		na		na		na		
na		na		na		na			

📖 **NOTE**

The command output is for reference only. The actual sensor thresholds may vary from the preceding command output.

Table 4-4 Field description of sensor information

Field	Description	Example	Remarks
sensor name	Name of the sensor	**CPU1 Core Rem**: indicates the core temperature sensor of CPU 1.	-
value	Current value	**35.000**	**na**: The device monitored by this sensor is not installed.
unit	Unit of the current value	**degrees C**: indicates that the unit is degree Celsius.	**discrete**: indicates a discrete sensor. Discrete sensors have no unit.
status	State	**ok**: The sensor works properly. **nc**: The sensor detects a minor alarm. **cr**: The sensor detects a major alarm. **nr**: The sensor detects a critical alarm.	**na**: The device monitored by this sensor is not installed. The sensor value is displayed in hexadecimal system, for example **0x8000**, as defined by IPMI specifications. For details, see **Generic Offset** in table 42-2 Generic Event/ Reading Type Codes and **Sensor specific Offset** in table 42-3 Sensor Type Codes of the IPMI specifications.
lnr	Lower threshold for critical alarms	na	**na**: The sensor does not support the threshold.
lc	Lower threshold for major alarms	na	**na**: The sensor does not support the threshold.
lnc	Lower threshold for minor alarms	na	**na**: The sensor does not support the threshold.

Field	Description	Example	Remarks
unc	Upper threshold for minor alarms	**84.000**: The positive minor alarm threshold of the current sensor is **84**.	**na**: The sensor does not support the threshold.
uc	Upper threshold for major alarms	**88.000**: The positive major alarm threshold of the current sensor is **88**.	**na**: The sensor does not support the threshold.
unr	Upper threshold for critical alarms	na	**na**: The sensor does not support the threshold.
phys	Positive hysteresis	**3**: The positive hysteresis of the current sensor is **3**.	**na**: The current sensor does not support the hysteresis.
nhys	Negative hysteresis	**3**: The negative hysteresis of the current sensor is **3**.	**na**: The current sensor does not support the hysteresis.

4.12.2 Sensor Test Command (sensor -d test)

Function

The **sensor -d test** command is used to simulate the sensor status or value.

Format

ipmcset -t sensor -d test -v <sensorname/stopall> [value/stop]

Parameters

Parameter	Description	Value
sensorname/ stopall	Specifies the sensor name.	*sensorname*: specifies the sensor name. **stopall**: Stops all tests.
value/stop	Specifies the analog value.	*value*: specifies the analog value of the sensor test. **stop**: Stops all tests.

Usage Guidelines

- If the iBMC version is earlier than V253, running this command will simulate the related alarm.

- If the iBMC version is V253 or later, running this command will not simulate the related alarm.

Example

Simulate a CPU1 Core Rem sensor temperature value of 100°C.

```
iBMC:/->ipmcset -t sensor -d test -v "CPU1 Core Rem" 100
Sensor test successfully.
```

4.13 PSU Commands

4.13.1 Setting the PSU Work Mode (psuworkmode)

Function

The **psuworkmode** command is used to set the PSU work mode.

Format

ipmcset -d psuworkmode -v *<option>* [*active_psuid*]

Parameters

Parameter	Description	Value
option	PSU work mode.	• **0**: load-balancing mode • **1**: active/standby mode
active_psuid	ID of the active PSU when the PSUs are working in active/standby mode.	1 or 2

Usage Guidelines

None

Example

Set the PSU work mode.

```
iBMC:/->ipmcset -d psuworkmode -v 1 1
Set Power Work Mode (Active Standby) successfully
```

4.13.2 Querying Basic PSU Information (psuinfo)

Function

The **psuinfo** command is used to query the PSU information.

Format

ipmcget -d psuinfo

Parameters

None

Usage Guidelines

None

Example

Query PSU information.

```
iBMC:/-> ipmcget -d psuinfo
Current PSU Information :
Slot  Manufacturer   Type               SN          Version      Rated power   InputMode
1            750W PLATINUM PS   N/A          07           750          AC/DC
2            750W PLATINUM PS   N/A       07         750        AC/DC

Current PSU WorkMode   :
Actual PSU Status      :
   Work Mode        : Load Balancing
Predicted PSU Status   :
   Work Mode        : Load Balancing
```

4.14 U-Boot Commands

4.14.1 Logging In to U-Boot

Scenarios

Log in to U-Boot of the iBMC over a serial port.

> **NOTICE**
>
> U-Boot commands are used to load underlying software and debug underlying devices. Only qualified maintenance engineers can use U-Boot commands.

Prerequisites

- User name and password for logging in to the iBMC

  The default user is **root** for V3 servers and **Administrator** for V5 servers, and the default password is on the product nameplate.

- Password for logging in to the iBMC U-Boot

  The default password is **Huawei12#$** for V3 servers and **Admin@9000** for V5 servers.

NOTICE

For security purposes, change the initial password after the first login and change your password periodically.

Procedure

Step 1 Log in to the iBMC CLI over the serial port.

Step 2 Restart the iBMC.

```
iBMC:/->ipmcset –d reset
This operation will reboot iBMC system. Continue? [Y/N]:
```

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

The iBMC restarts.

Step 4 Press **Ctrl+B** when the message Hit 'ctrl + b' to stop autoboot: is displayed.

The output is as follows:

```
ENTER PASSWD:
```

Step 5 Enter the password for logging in to U-Boot. The default password is **Huawei12#$** for V3 servers and **Admin@9000** for V5 servers.

The U-Boot CLI is displayed.

----End

4.14.2 U-Boot Command List

NOTE

The U-boot commands are used only for debugging. The following lists the U-boot commands. If you require information about these commands, contact technical support.

On the iBMC U-boot command-line interface (CLI), type **?** or **help** and press **Enter**. The help of all U-boot commands is displayed as follows:

NOTE

The command output varies depending on the U-Boot version. The following uses U-Boot 2.1.07 as an example.

```
Hi1710_UBOOT> help
?       - alias for 'help'
base    - print or set address offset
bdinfo  - print Board Info structure
bmc_burning- flashdata_burning
flashdata_burning  -refresh all flash data from filename (default filename is ipmc.bin)!
bmc_partition_reset- reset_bmc_partition_table
boot    - boot default, i.e., run 'bootcmd'
```

```
bootd   - boot default, i.e., run 'bootcmd'
bootm   - boot application image from memory
bootp   - boot image via network using BOOTP/TFTP protocol
cmp     - memory compare
coninfo - print console devices and information
cp      - memory copy
crc32   - checksum calculation
datafs_burning- update_datafs
datafs_reset- datafs_reset  make datafs reset
datafs_up- update_datafs
ddr_test- ddr_test
dt      - memory test
dts     - just for test
echo    - echo args to console
editenv - edit environment variable
erase   - erase FLASH memory
ext4load- load binary file from a Ext4 filesystem
ext4ls  - list files in a directory (default /)
ext4write- create a file in the root directory
false   - do nothing, unsuccessfully
flinfo  - print FLASH memory information
go      - start application at address 'addr'
help    - print command description/usage
hiddr_test- use for save ddr auto test ret
ibmc0_up- update_bmc0
ibmc1_up- update_bmc1
iminfo  - print header information for application image
itest   - return true/false on integer compare
loadb   - load binary file over serial line (kermit mode)
loads   - load S-Record file over serial line
loady   - load binary file over serial line (ymodem mode)
loop    - infinite loop on address range
lswread - read value of lsw register
lswwrite- write value to lsw register
md      - memory display
mm      - memory modify (auto-incrementing address)
mmc     - MMC sub system
mmcinfo - display MMC info
mtdparts- define flash/nand partitions
mtest   - simple RAM read/write test
mw      - memory write (fill)
nfs     - boot image via network using NFS protocol
nm      - memory modify (constant address)
passwd  - passwd -  Modify uboot passwd
phyread - read value of phy register
phywrite- write value to phy register
ping    - send ICMP ECHO_REQUEST to network host
printenv- print environment variables
protect - enable or disable FLASH write protection
rarpboot- boot image via network using RARP/TFTP protocol
reboot  - Perform RESET of the CPU
reset   - Perform RESET of the BMC
run     - run commands in an environment variable
saveenv_sfc- save environment variables to persistent storage
setenv  - set environment variables
sfc_burning- sfc_burning  copy sfc image(sfc.bin) to flash
sfc_uboot_cp0- sfc_uboot_cp0  copy uboot0 to flash
sfc_uboot_cp1- sfc_uboot_cp1  copy uboot1 to flash
sleep   - delay execution for some time
test    - minimal test like /bin/sh
tftpboot- boot image via network using TFTP protocol
true    - do nothing, successfully
uboot0_up- uboot0_up  update uboot0
uboot1_up- uboot1_up  update uboot1
version - display u-boot version
```

4.15 SOL Commands

4.15.1 Creating an SOL Session (sol -d activate)

Function

The **sol -d activate** command is used to establish a Serial Over LAN (SOL) session to the system serial port or iBMC serial port of a server.

Format

ipmcset -t sol -d activate -v *<option> <mode>*

Parameters

Parameter	Description	Value
option	Serial port to be connected.	• **1**: system serial port • **2**: iBMC serial port
mode	SOL session mode.	• **0**: shared mode The shared mode allows two SOL sessions to be established simultaneously. Each user can view the operations performed by the other user. • **1**: private mode The private mode allows only one user to set up the SOL session.

Usage Guidelines

Only iBMC V256 and later versions support this command.

Before stabling an SOL session to the system serial port, configure the serial port redirection function on the OS. For details, see the operation guide provided by the OS vendor.

You can press **Esc** and then **(** with an interval less than one second to exit from the SOL session to the command line interface.

Example

Establish an SOL session in shared mode to the system serial port.

```
iBMC:/->ipmcset -t sol -d activate -v 1 0
[Connect SOL successfully! Use 'Esc(' to exit.]
Warning! The SOL session is in shared mode, the operation can be viewed on another terminal.
```

```
sles11sp1:~ #
sles11sp1:~ # Esc( [Close SOL]

SOL connection closed.
```

4.15.2 Deactivating an SOL Session (sol -d deactivate)

Function

The **sol -d deactivate** command is used to deactivate an SOL session forcibly.

Format

ipmcset -t sol -d deactivate -v *<index>*

Parameters

Parameter	Description	Value
index	Serial number of the SOL session.	**1**: session 1. **2**: session 2.

Usage Guidelines

Only iBMC V256 and later versions support this command.

The SOL session established by using IPMItool cannot be deactivated.

Example

Deactivate SOL session 1.

```
iBMC:/->ipmcset -t sol -d deactivate -v 1
Close SOL session successfully.
```

4.15.3 Setting SOL Session Timeout Period (sol -d timeout)

Function

The **sol -d timeout** command is used to set the timeout period for SOL sessions. If no operation is performed within the specified timeout period, the SOL session will be automatically disconnected and the iBMC CLI is displayed.

Format

ipmcset -t sol -d timeout -v *<value>*

Parameters

Parameter	Description	Value
value	Maximum idle time (in minutes) after the last operation on the SOL session. If no operation is performed within the specified time, the SOL session will be automatically disconnected.	Value range: 0 to 480 The value **0** indicates unlimited time. Default value: **15**

Usage Guidelines

Only iBMC V256 and later versions support this command.

Example

Set the SOL session timeout period to 20 minutes.

```
iBMC:/->ipmcset -t sol -d timeout -v 20
Set SOL timeout period successfully.
```

4.15.4 Querying the SOL Session List (sol -d session)

Function

The **sol -d session** command is used to query the SOL session list.

Format

ipmcget -t sol -d session

Parameters

None

Usage Guidelines

Only iBMC V256 and later versions support this command.

Example

Query the SOL session list.

```
iBMC:/->ipmcget -t sol -d session
Index   Type    Mode    LoginTime           IP                  Name
1       CLI     Shared  2017-09-14 11:19:55  192.168.1.40:50013   root
2       N/A     N/A     N/A                  N/A                  N/A
```

4.15.5 Querying SOL Session Configuration Information (sol -d info)

Function

The **sol -d info** command is used to query the SOL session configuration information, such as the SOL session timeout period.

Format

ipmcget -t sol -d info

Parameters

None

Usage Guidelines

Only iBMC V256 and later versions support this command.

Example

Query SOL session configuration information.

```
iBMC:/->ipmcget -t sol -d info
Timeout Period(Min)      :  20
```

5 Common Maintenance Commands

5.1 Viewing Help Information (help)

Function

The **help** command is used to view help information.

Format

help

[*command*] **--help**

Parameters

Parameter	Description	Value
command	The command is to be queried.	-

Usage Guidelines

None

Example

View the commands supported in the current path.

```
iBMC:/->help
Commands:
help     :     Used to get context sensitive help.
exit     :     Used to terminate the CLP session.
ipmcget  :     Used to get BMC runtime status.
ipmcset  :     Used to set BMC runtime status or send control
command.
notimeout :     Used to set no timeout limit to login shell.
maint_debug_cli : Used to maintance in debug
mode.
ping     :     Used to test IPv4 network status.
ping6    :     Used to test IPv6 network status.
ifconfig :     Used to check network device information.
```

```
ps      :    Used to check processes status.
free    :    Used to check memory status.
top     :    Used to check system resource used information. None parameter is
allowed
df      :    Used to check disk used information.
route   :    Used to check route information. None parameter is
allowed
netstat :    Used to check network port status.
```

📖 NOTE

The **maint_debug_cli** command is mainly used to locate faults onsite and can be used by administrators and operators only. For details about how to use the command, see the iBMC advanced command reference.

\# View the method of using the **ping** command.

```
iBMC:/->ping --help
BusyBox v1.18.4 (2014-08-09 16:28:25 CST) multi-call binary.

Usage: ping [OPTIONS] HOST

Send ICMP ECHO_REQUEST packets to network hosts

Options:
 -4,-6  Force IP or IPv6 name resolution
 -c CNT  Send only CNT pings
 -s SIZE  Send SIZE data bytes in packets (default:56)
 -I IFACE/IP Use interface or IP address as source
 -W SEC  Seconds to wait for the first response (default:10)
   (after all -c CNT packets are sent)
 -w SEC  Seconds until ping exits (default:infinite)
   (can exit earlier with -c CNT)
 -q  Quiet, only displays output at start
   and when finished
```

5.2 Disconnecting the Client from iBMC (exit)

Function

The **exit** command is used to disconnect the client from iBMC.

Format

exit

Parameters

None

Usage Guidelines

None

Example

\# Disconnect the client from iBMC.

```
iBMC:/->exit
```

Connection closed by foreign host.

5.3 Checking the Network Connectivity (ping, ping6)

Function

The **ping** or **ping6** command is used to check the network connectivity.

Format

ping <*IPv4 Address*>

ping6 <*IPv6 Address*>

Parameters

Parameter	Description	Value
IPv4 Address	Indicates the target IPv4 address	-
IPv6 Address	Indicates the target IPv6 address	-

Usage Guidelines

For details, see the user guide of the **ping** or **ping6** command in Linux.

Example

Check the connectivity between the current device and the target device with the IP address.

```
iBMC:/->ping 192.168.44.178
PING 192.168.44.178 (192.168.44.178) 56(84) bytes of data.
64 bytes from 192.168.44.178: icmp_req=1 ttl=64 time=8.19 ms
64 bytes from 192.168.44.178: icmp_req=2 ttl=64 time=0.398 ms
64 bytes from 192.168.44.178: icmp_req=3 ttl=64 time=0.263 ms
64 bytes from 192.168.44.178: icmp_req=4 ttl=64 time=0.285 ms
64 bytes from 192.168.44.178: icmp_req=5 ttl=64 time=0.418 ms
iBMC:/->ping6 fc00::39ad:9345:1a6e:d0e1
PING fc00::39ad:9345:1a6e:d0e1(fc00::39ad:9345:1a6e:d0e1) 56 data bytes
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=1 ttl=64 time=0.821 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=2 ttl=64 time=0.840 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=3 ttl=64 time=0.843 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=4 ttl=64 time=0.744 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=5 ttl=64 time=0.774 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=6 ttl=64 time=1.02 ms
```

5.4 Checking Memory Status (free)

Function

The **free** command is used to check memory status.

Format

See the syntax of the **free** command of Linux.

Parameters

This command supports all parameters of the **free** command of Linux.

Usage Guidelines

None

Example

Check memory status.

```
iBMC:/->free
            total       used       free      shared     buffers
  Mem:      125572      94780      30792      0          14780
  Swap:     0           0          0
Total:      125572      94780      30792
```

5.5 Checking Process Status (ps)

Function

The **ps** command is used to check status of processes.

Format

See the syntax of the **ps** command of Linux.

Parameters

This command supports all parameters of the **ps** command of Linux.

Usage Guidelines

None

Example

Check status of processes.

```
iBMC:/-> ps
  PID TTY          TIME CMD
 6743 ttyAMA0  00:00:00 ps
28112 ?        00:00:00 bash
```

5.6 Checking Network Port Status (netstat)

Function

The **netstat** command is used to check network port status.

Format

See the syntax of the **netstat** command of Linux.

Parameters

This command supports all parameters for the **netstat** command.

Usage Guidelines

None

Example

Check network port status.

```
iBMC:/->netstat -t
 Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address        Foreign Address       State
tcp      0    116 192.168.64.110:ssh     192.168.29.200:65069   ESTABLISHED
tcp      0      0 192.168.64.110:ssh     192.168.29.200:65068   ESTABLISHED
```

5.7 Checking Disk Usage (df)

Function

The **df** command is used to check disk usage.

Format

See the syntax of the **df** command of Linux.

Parameters

This command supports all parameters of the **df** command of Linux.

Usage Guidelines

None

Example

Check disk usage.

```
iBMC:/->df
Filesystem        1k-blocks      Used Available Use% Mounted on
rootfs            50580     50580        0 100% /
/dev/root         50580     50580        0 100% /
/dev/mtdblock5     15872      1308    14564  8% /data
tmpfs             62784       292    62492  0% /dev/shm
tmpfs             62784       292    62492  0% /dev/shm
tmpfs             49152       160    48992  0% /tmp
tmpfs              4096        12     4084  0% /ipmc/usr
```

5.8 Checking Network Device Information (ifconfig)

Function

The **ifconfig** command is used to check network device information.

Format

See the syntax of the **ifconfig** command of Linux.

Parameters

This command supports the following parameters:

- **lo**
- **eth**n (n indicates a network port number)
- **-a**

This command can also be used without parameters.

Usage Guidelines

None

Example

```
iBMC:/->ifconfig eth1
eth1    Link encap:Ethernet  HWaddr 00:18:82:11:03:21
        inet6 addr: fe80::218:82ff:fe11:321/64 Scope:Link
        UP BROADCAST DEBUG RUNNING  MTU:1500  Metric:1
        RX packets:28 errors:0 dropped:0 overruns:0 frame:0
        TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1832 (1.7 KiB)  TX bytes:2558 (2.4 KiB)
        Interrupt:28
```

5.9 Checking Route Information (route)

Function

The **route** command is used to check route information.

Format

See the syntax of the **route** command of Linux.

Parameters

-n: uses an IP address or port number instead of a communication protocol or host name.

-e: displays more information.

-A inet{6}: selects an address family.

Usage Guidelines

None

Example

Check route information.

```
iBMC:/->route --help
Usage: route [option]

Check kernel routing tables

Options:
  -n           Don't resolve names
  -e           Display other/more information
  -A inet{6}    Select address family
```

5.10 Checking System Resource Usage (top)

Function

The **top** command is used to check system resource usage.

Format

See the syntax of the **top** command of Linux.

Parameters

None

Usage Guidelines

None

Example

Check system resource usage.

```
iBMC:/->top
top - 16:26:41 up 3 days, 15:48,  3 users,  load average: 0.09, 0.08, 0.08
Tasks:  46 total,   1 running, 45 sleeping,   0 stopped,   0 zombie
Cpu(s): 2.2%us, 3.4%sy,  0.0%ni, 94.3%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   125572k total,   94920k used,    30652k free,    14780k buffers
Swap:      0k total,       0k used,       0k free,    35916k cached

 PID USER     PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+
COMMAND
1133 root     20   0 2408 968  784 R  3.7  0.8   0:00.09
top
   1 root     20   0 1980 652  572 S  0.0  0.5   0:01.95
init
   2 root     15  -5    0    0    0 S  0.0  0.0   0:00.00
kthreadd
   3 root     15  -5    0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/
```

```
0
   4 root    15 -5   0   0   0 S 0.0 0.0  0:00.00 events/
0
   5 root    15 -5   0   0   0 S 0.0 0.0  0:03.81
khelper
  64 root    15 -5   0   0   0 S 0.0 0.0  0:00.00 kblockd/
0
 103 root    20  0   0   0   0 S 0.0 0.0  0:00.00
pdflush
 104 root    20  0   0   0   0 S 0.0 0.0  0:13.65 pdflush
```

5.11 Disabling the CLP Timeout Feature (notimeout)

Function

The **notimeout** command is used to disable the Command Line Protocol (CLP) timeout feature, and the CLP command line interface will not time out.

Format

notimeout

Parameters

None

Usage Guidelines

None

Example

Disable the CLP timeout feature.

```
iBMC:/->notimeout
iBMC:/->
```

6 Common Operations

6.1 Logging In to a Server Over the Serial Port Using PuTTY

Scenarios

Use PuTTY to log in to a server over a serial port in any of the following scenarios:

- The server is configured for the first time at a site.
- A remote connection to the server cannot be established.

Prerequisites

Conditions

- The PC is connected to the server over a serial cable.
- PuTTY 0.60 or later has been installed.

Data

User name and password for logging in to the server.

Software

PuTTY, free software available at the chiark website.

> 📖 **NOTE**
>
> The PuTTY of the latest version is recommended, because an earlier version may cause a failure in accessing the storage system.

Procedure

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

   The **PuTTY Configuration** window is displayed.

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

3 Set the login parameters.

   The following are the examples:

- Serial Line to connect to: COM*n*

- Speed (baud): 115200

- Data bits: 8

- Stop bits: 1

- Parity: None

- Flow control: None

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

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

5   Select **Serial** under **Connection type**, as shown in **Figure 6-1**.

Figure 6-1 PuTTY Configuration window
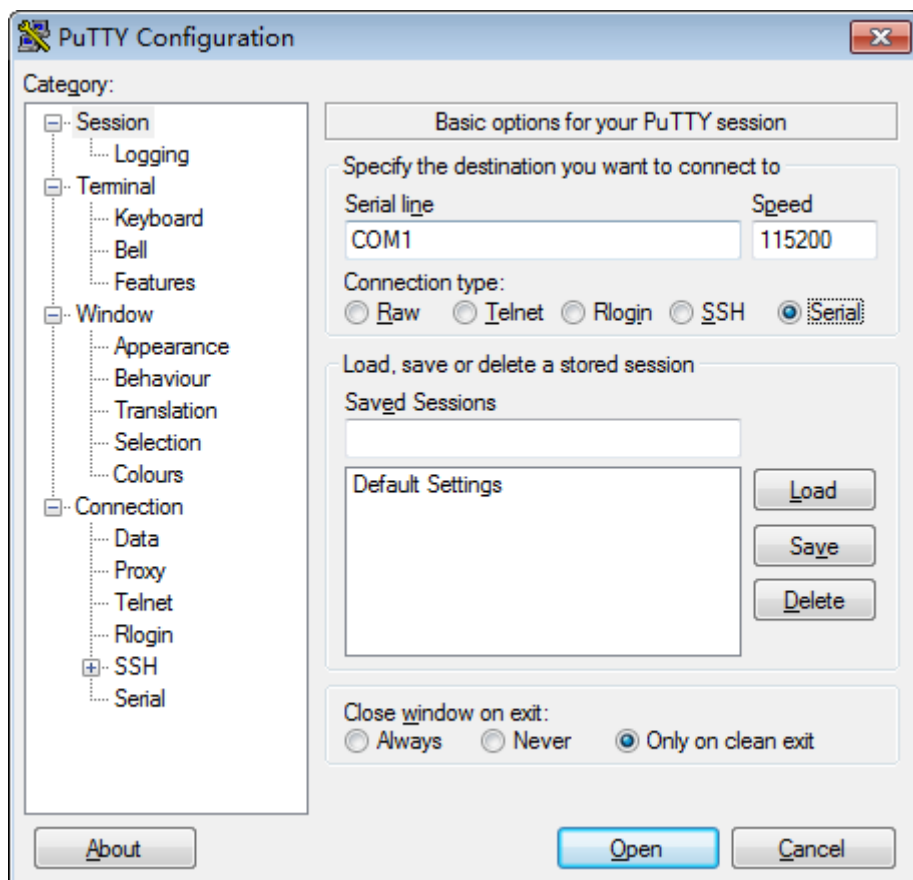
6   Click **Open**.

    The **PuTTY** login window is displayed.

7   Enter the user name and password.

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

----End

6.2 Logging In to a Server Over a Network Port Using PuTTY

Scenarios

Use PuTTY to remotely log in to a server over a local area network (LAN) and configure and maintain the server.

Prerequisites

Conditions
The local PC is connected to the management network port of the server through a network cable.

Data

- IP address of the server

- User name and password for logging in to the server

Software

PuTTY, free software available at the chiark website.

Procedure

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

2. On the PC command-line interface (CLI), run the following command to check whether the server is reachable:

    Ping *Server IP address*

3. Double-click **PuTTY.exe**.

    The **PuTTY Configuration** window is displayed, as shown in **Figure 6-2**.

Figure 6-2 PuTTY Configuration window
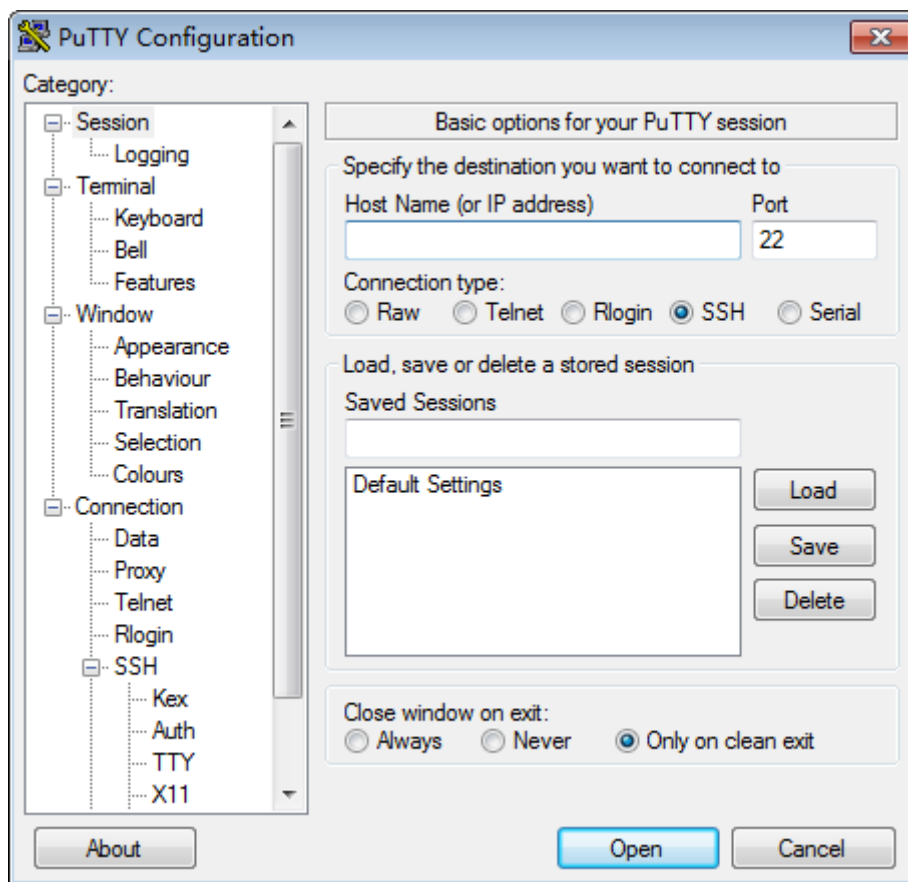
4   Set login parameters.

–   **Host Name (or IP address)**: Enter the IP address of the server to be
     logged in to. For example, **191.100.34.32**.

–   **Port**: Retain the default value **22**.

–   **Connection type**: Retain the default value **SSH**.

–   **Close window on exit**: Retain the default value **Only on clean exit**.

📖 **NOTE**

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

5   Click **Open**.

The PuTTY login window is displayed.

📖 **NOTE**

If this is your first login to the server, the **PuTTY Security Alert** dialog box is displayed.
Click **Yes** to proceed.

6   Enter the user name and password.

> If an incorrect user name or password is entered, you must set up a new PuTTY session.

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

----End

6.3 Restoring Default iBMC Settings

Scenario

Restore the default iBMC settings when the iBMC configuration data is damaged or the iBMC cannot start or be accessed.

NOTICE

- Only technical support personnel or personnel authorized can perform this operation.
- Default iBMC settings cannot be restored remotely.
- All user settings, including user names, passwords, and IP addresses, will be restored to defaults. Perform this operation with caution.
- Before using the jumper to restore the default iBMC settings, back up data and network settings and power off the server.

Default iBMC configurations can be restored using U-Boot commands or the jumper. **Table 6-1** lists the product models and supported restoration methods.

📖 NOTE

The following methods are available to restore default iBMC settings:

- Use the U-Boot commands to restore the default iBMC settings if you can log in to the U-Boot over a serial port.
- Use a jumper to restore the default iBMC settings if the U-Boot and iBMC are inaccessible.

Table 6-1 Product models and supported restoration methods

Product Model	U-Boot	Jumper
RH1288A V2	Supported	Supported
RH2288A V2	Supported	Supported
RH1288 V3	Supported	Supported
RH2288 V3	Supported	Supported
RH2288H V3	Supported	Supported

Product Model	U-Boot	Jumper
RH5885 V3	Supported	N/A
RH5885H V3	Supported	N/A
5288 V3	Supported	Supported
RH8100 V3	Supported	N/A
1288H V5	Supported	Supported
2288C V5	Supported	Supported
2288H V5	Supported	Supported
2488 V5	Supported	Supported
2488H V5	Supported	Supported
5288 V5	Supported	Supported
5885H V5	Supported	Supported
8100 V5	Supported	Supported

Procedure

- To restore iBMC default settings using U-Boot commands, perform the following steps:

  a. Connect to the serial port of iBMC using a serial cable, and use PuTTY to log in to the iBMC over the serial port.

     📖 NOTE

     Before accessing the iBMC CLI over the serial port, ensure that the system serial port of the chassis is switched to the iBMC serial port. You can switch over the serial port by using the **Querying and Redirecting the Serial Port (serialdir)** command on the CLI.

  b. Press and hold the UID button on the server for 6 seconds to restart the iBMC.

  c. When "Hit 'ctrl + b' to stop autoboot: 1" is displayed, press **Ctrl** + **B**.

  d. Enter the default U-Boot password.

     The default password of U-Boot is **Huawei12#$** for V3 servers and **Admin@9000** for V5 servers.

     If "u-boot>" is displayed, you have successfully logged in to U-Boot.

  e. Run the following command to query the U-Boot version:

     printenv ver

  f. Restore datafs.

     - If the U-Boot version is 1.1.37 or earlier, run the following commands:

       fsload /usr/upgrade/datafs.jffs2

   datafs_cp

   ▪ If the U-Boot version is later than 1.1.37, run the following
     command:

     datafs_reset

g.   Run the following command to restart the iBMC:

   reset

   The restart process takes about 3 minutes. After the iBMC restarts, the
   iBMC default settings are restored.

● To restore iBMC default settings using the jumper, perform the following
  steps:

a.   Back up data.

   NOTICE

   Back up data and network before restoring iBMC default settings.

b.   Locate the jumper.

   The jumper number varies depending on the server model. **Table 6-2**
   provides the jumper ID and silkscreen information. For details about the
   location of the jumper, see "Mainboard Layout" in the user guide of the
   server you use.

Table 6-2 Jumper ID and silkscreen

Product Model	Jumper ID	Silkscreen
RH2288A V2	J117	CLR_BMC_PW
RH1288A V2	J117	CLR_BMC_PW
RH1288 V3	J36	CLR_BMC_PW
RH2288 V3	J36	CLR_BMC_PW
RH2288H V3	J36	CLR_BMC_PW
5288 V3	J36	CLR_BMC_PW
1288H V5	J176	BMC_RCV
2288C V5	J176	BMC_RCV
2288H V5	J176	BMC_RCV
2488 V5	J93	CLEAR_BMC_PW
2488H V5	J93	CLEAR_BMC_PW
5288 V5	J176	CLR_BMC_PW
5885H V5	J93	CLEAR_BMC_PW
8100 V5	J16	CLEAR_BMC_PW

c. Use a jumper cap or a tool to short-circuit the jumper.

d. Press and hold the UID button for 6 seconds to restart the iBMC while keeping the jumper short-circuited.

The restart process takes about 3 minutes. After the iBMC restarts, the iBMC default settings are restored.

◻ NOTE

Disconnect the jumper after the iBMC default settings are restored. Otherwise, the default settings are restored each time when the iBMC restarts.

6.4 Configuring the Trap Function on the iBMC WebUI

Operation Scenario

Enable the trap function on **Alarm & SEL** > **Alarm Setting** of the iBMC WebUI.

The trap function enables the iBMC to send alarm information, event information, and trap properties to a third-party server through trap messages.

Prerequisites

Data

- SNMP trap version

- Host identifier (such as **Board Serial Number**, **Product Asset Tag**, or **Host Name**) used to identify the source of the message

- SNMP trap community name

- Address of the server receiving trap messages

Procedure

Step 1 Log in to the iBMC WebUI. For details, see **3.1 Logging In to the iBMC WebUI**.

Step 2 Choose **Alarm & SEL** > **Alarm Settings**.

Step 3 In the **Alarm Trap Notification Settings** area, click [OFF] to enable the trap function.

If [OFF] changes to [ON], the trap function is enabled.

Step 4 Set trap parameters and click **Save**.

Set the following parameters:

- **Trap Version**: Select an SNMP trap version. **SNMPv3** is recommended. Exercise caution when using **SNMPv1** and **SNMPv2c**, because they pose security risks.

- **Choose Trap SNMPv3 User**: Set this parameter only when **Trap Version** is **SNMPv3**. The default user name is **root** for V3 servers and **Administrator** for V5 servers.

- **Trap Mode**: Set the mode for reporting trap information.
    - Select **Precise Alarm (recommended)** to use the SNMP node OID that is in one-to-one mapping with the event to identify a trap event. Compared with **OID** and **Event Code**, this mode provides more accurate information.
    - −Select **OID** to use the object identifier of the SNMP node to identify a trap event.
    - −Select **Event Code** to use the event code to identify a trap event.
- **Trap Server Identity**: Set the source host of the trap message. The source host can be identified by **Board Serial Number**, **Product Asset Tag**, or **Host Name**.
- **Community Name** and **Confirm Community Name**: Set the community name only when **Trap Version** is set to **SNMPv1** or **SNMPv2c**. The community name is used for trap authentication if SNMPv1 or SNMPv2c is used. **Community Name** and **Confirm Community Name** must be the same.
- **Include Alarm Severities**: Select the severities of alarms to be reported through trap messages.

Step 5 Configure the trap server and message format.

A maximum of four channels can be specified to send alarms.

1. In the **Trap Server and Message Format** area, click ✏ under the **Operation** column of a channel.

2. Click OFF to enable the channel.

    If OFF changes to ON, the channel is enabled.

3. In the **Trap Server Address** text box, enter an IPv4 or IPv6 address for the server that receives the trap messages.

4. In the **Trap Port** text box, enter the port number for receiving trap messages.

    The default port number is **162**.

5. On the right of **Packet Delimiter**, select the delimiter used to separate the key words in trap messages.

6. In **Select Message Content**, select the content to be included in trap messages.

    The content includes time, sensor name, severity, event code, and event description.

7. Select **Display Keyword in Message** to display the keywords in trap messages. Deselect this check box if you do not want to display the keywords in trap messages.

8. Click **Save**.

    If "Operation successful" is displayed, the configuration is saved successfully.

9. Click **Test** to check whether the trap channel is available.

    If "Operation successful" is displayed, the trap channel is available.

----End

6.5 Configuring the SMTP Function on the iBMC WebUI

Operation Scenario

On the **Alarm Setting** page of the iBMC WebUI, you can configure the Simple Mail Transfer Protocol (SMTP) function to enable the iBMC to send alarms and events to specified mailboxes by email over an SMTP server.

📖 NOTE

V3 servers can be used as SMTP servers only when the SMTP port number is 25.

Prerequisites

Data

Obtain the following information:

- The address of an SMTP server
- The sender information:
  - User name and password of the sender
  - The email address of the sender
  - The email subject
- The receiving information:
  - The receiving email address
  - The description about the receiving email address

Procedure

Step 1　Log in to the iBMC WebUI. For details, see **3.1 Logging In to the iBMC WebUI**.

Step 2　Choose **Alarm & SEL** > **Alarm Setting**.

Step 3　In the **Alarm Email Notification Settings** area, click OFF to enable the SMTP function.

When OFF changes to ON, the SMTP function is enabled.

Step 4　In the **SMTP Server Address** text box, type the SMTP server address.

The address can be an IPv4 or IPv6 address.

Step 5　Set **Allows TLS Enabled** to enable or disable the Transport Layer Security (TLS) function.

- **Yes**: Enable the TLS function so that data is transmitted in ciphertext.
- **No**: Disable the TLS function so that data is transmitted in plain text.

- By default, SMTP supports TLS. You are advised to enable the TLS function for security purposes.
- After enabling the TLS function on the iBMC WebUI, you must configure the TLS function and identity authentication on the SMTP server so that the SMTP server can receive emails from the iBMC.

Step 6 Set **Allows Anonymous Login**.

- **Allows Anonymous Login** specifies whether the SMTP server supports anonymous authentication. The value **Yes** indicates that no user name or password is required for authentication when alarm emails are forwarded by the SMTP server. The anonymous authentication function requires the SMTP server to support anonymous login.

- The value **No** indicates non-anonymous authentication. If you click the **No** option button, you need to enter the user name and password registered with the SMTP server. The user name and password are required for authentication when the iBMC sends alarm emails to the SMTP server.

☐ NOTE

By default, the SMTP server does not support anonymous authentication. You are advised to set **Allows Anonymous Login** to **No** for security purposes.

Step 7 Configure email information.

1. Set **Sender's User Name** and **Sender's Password**.

   ☐ NOTE

   – If **Allows Anonymous Login** is set to **Yes**, **Sender's User Name** and **Sender's Password** do not need to be set.

   – If the password has been changed on the SMTP server, you need to open the **Alarm Setting** page and enter the new password in the **Sender's Password** text box.

2. Set **Sender's Address**.

3. Set **Email Subject**.

   You can select **Host Name**, **Board serial number**, and **Product asset tag** to specify the content to be attached to the email subject.

Step 8 Set **Select Alarm Severities**.

The iBMC can send alarms of five severities: **ALL**, **Critical**, **Major**, **Minor**, and **Normal**.

After you select an alarm severity, the iBMC sends alarms and events of the specified severity to specified email addresses over the SMTP server if there is any.

☐ NOTE

The options are described as follows:

- **All**: indicates that events and minor, major, and critical alarms are sent.
- **Critical**: indicates that only critical alarms are sent.
- **Major**: indicates that only major alarms are sent.
- **Minor**: indicates that only minor alarms are sent.
- **Normal**: indicates that only events are sent.

Step 9 Set email addresses for receiving alarms.

Click (OFF). If (OFF) changes to (ON), the address is enabled.

1. Type the alarm receiving email address.
2. Type the description of the alarm receiving email address.

Step 10 Click **Save**.

After the configuration is saved, you can click **Test** to check the email address. If **Operation succeeded** is displayed, the SMTP function and its configuration take effect.

Step 11 Click **Test** to verify the email address.

If **Operation succeeded** is displayed, a test email has been sent to the corresponding mailbox, and you need to check the email in the mailbox for verification.

----End

6.6 Configuring the LDAP Function

6.6.1 Configuring the LDAP Server

The iBMC supports Windows AD and Linux OpenLDAP. This section uses Windows Server 2012 R2 Enterprise as an example to describe how to configure the LDAP server. If an LDAP server is already available, skip this section.

Prerequisites

- The device (for example, a server) for deploying the LDAP server is available.
- The Windows Server 2012 R2 Enterprise installation CD-ROM or ISO image file is available.

Procedure

Step 1 Install the OS.

1. On the iBMC web user interface (WebUI) of the server, set the CD-ROM drive as the next boot device of the server.
2. Insert the OS installation CD-ROM into the CD-ROM drive or mount the OS image file through the iBMC virtual CD-ROM drive.
3. Restart the server to access the OS installation wizard.
4. On the OS selection page, select **Windows Server 2012 R2 Datacenter**.
5. Click **Next**.

   Complete the OS installation by following the instructions.

Step 2 Install the DNS service.

1. Select **Server Manager** in the **Start** menu.
2. Select **Local Server** in the navigation tree.

The **PROPERTIES For FusionServer** window is displayed, as shown in **Figure 6-3**.

Figure 6-3 Local server properties
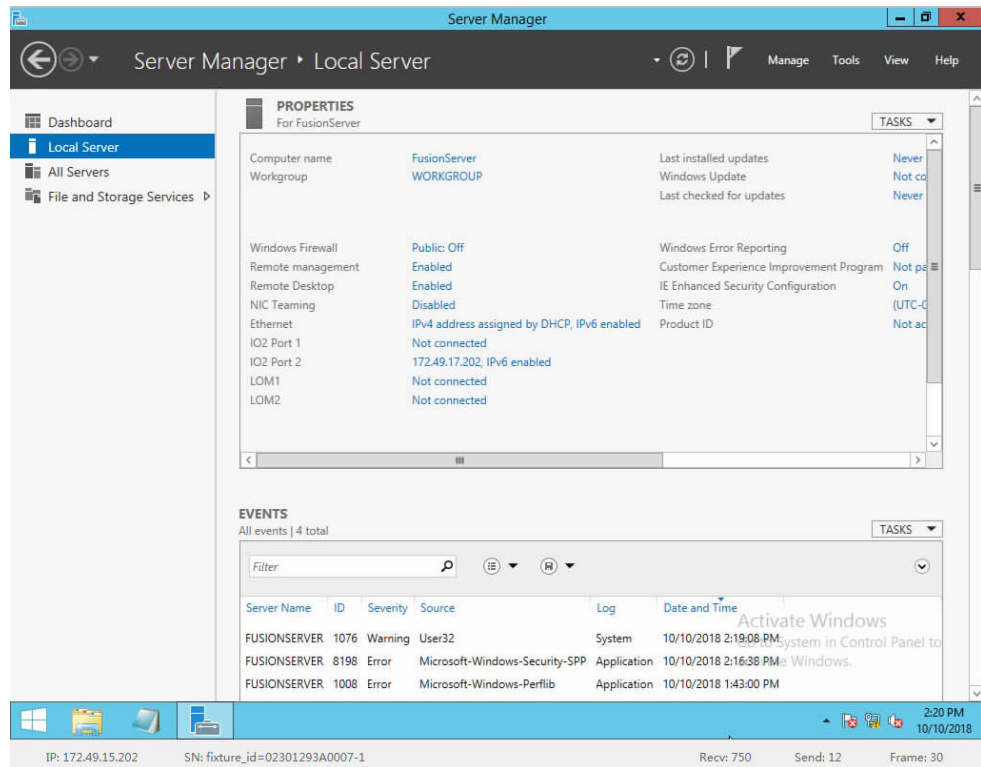
3. Select **Manage** at the top right corner and choose **Add Roles and Features**.

The **Add Roles and Features Wizard** window is displayed, as shown in **Figure 6-4**.

Figure 6-4 Add roles and features wizard
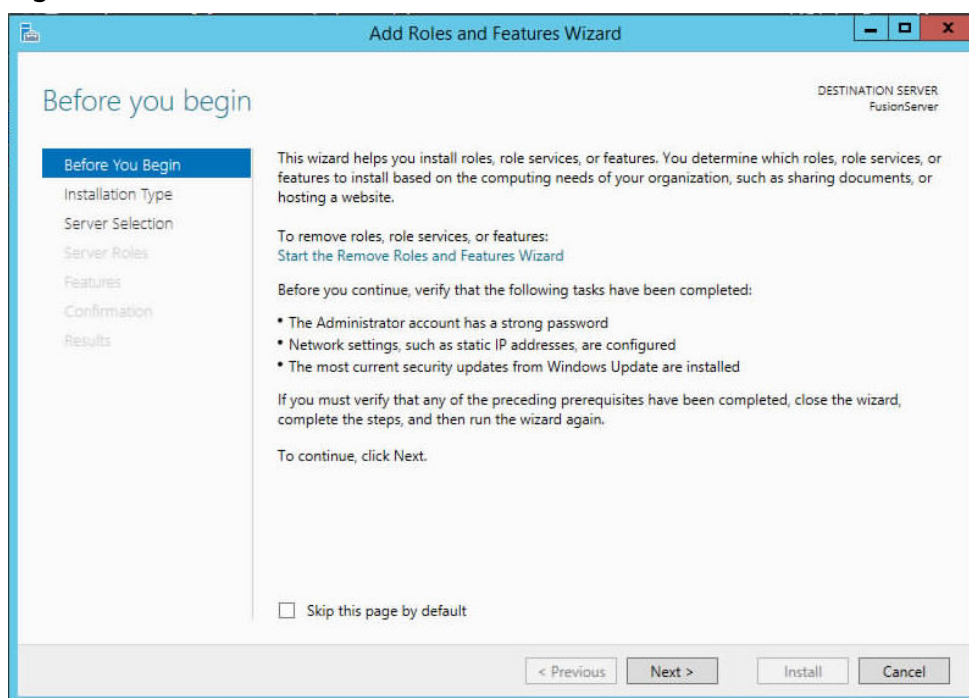
4. Click **Next**.

   The **Select installation type** window is displayed.

5. Select **Role-based or feature-based installation** and click **Next**.

   The **Select destination server** window is displayed, as shown in **Figure 6-5**.

Figure 6-5 Select destination server
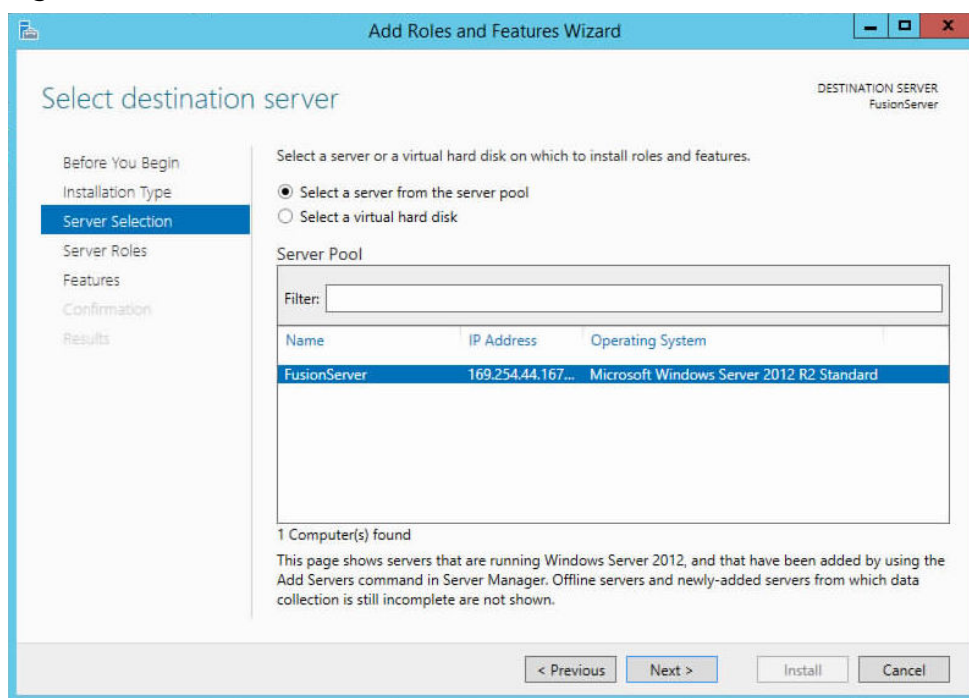
6. Choose **Select a server from the server pool**, select the server in the **Server Pool** box and click **Next**.

   The **Select server roles** page is displayed, as shown in **Figure 6-6**.

Figure 6-6 Select server roles
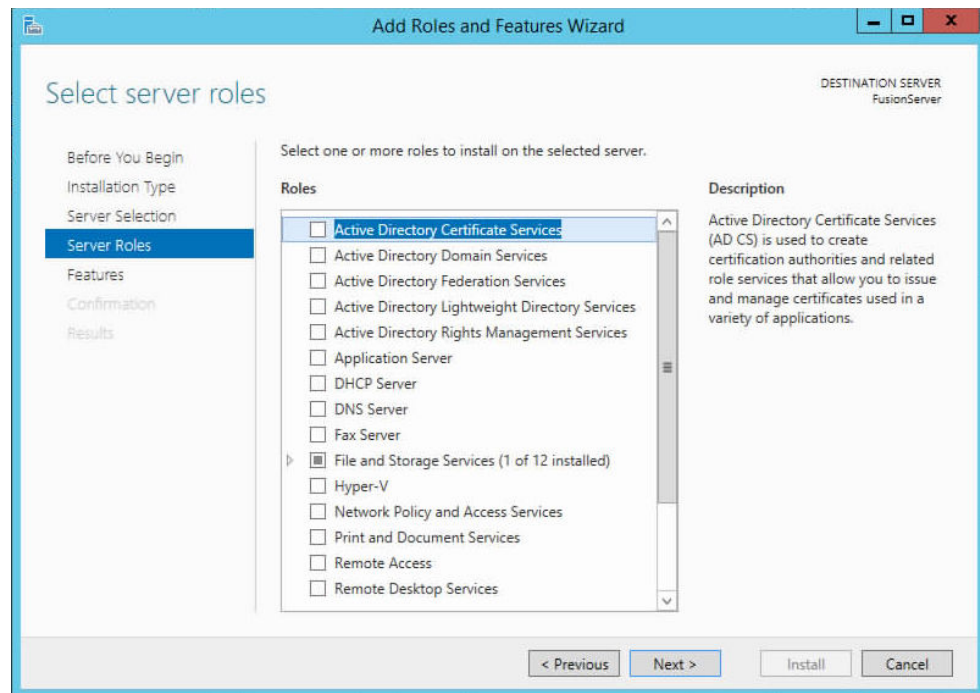
7. Select **DNS Server** in the **Roles** box.

   The confirmation window is displayed.

8. Click **Add Features**.

   The **Select server roles** window is displayed.

9. Click **Next**.

   The **Select features** window is displayed, as shown in **Figure 6-7**.

Figure 6-7 Select features
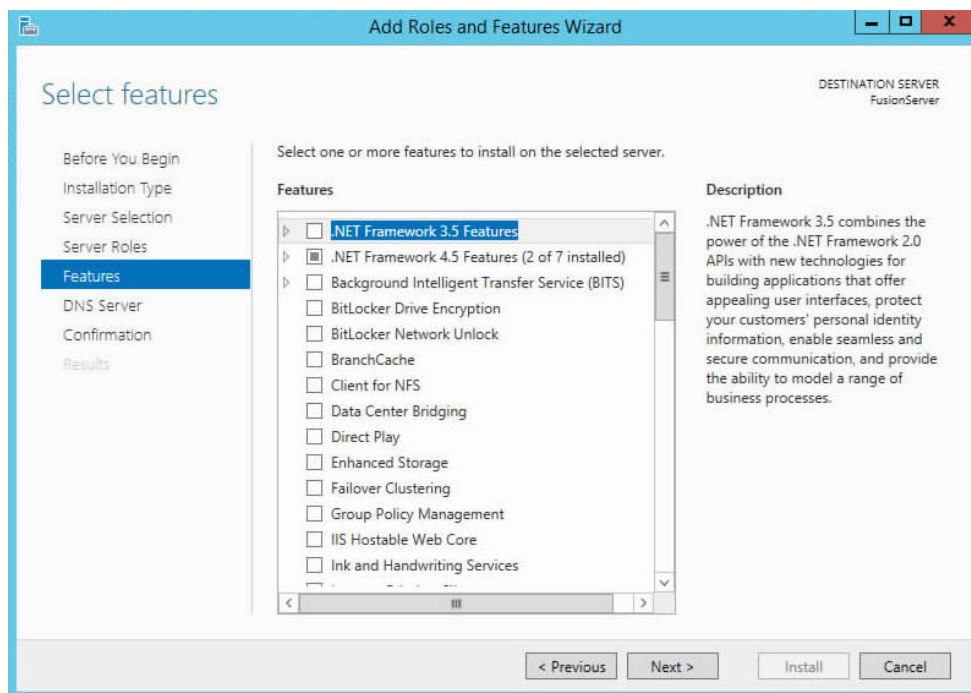
10. Select **.NET Framework 4.5 Features** and click **Next**.

    The **DNS Server** window is displayed.

11. Click **Next**.

    The confirmation window is displayed.

12. Click **Install**.

    The DNS server installation process is displayed.

13. When the installation is complete, click **Close**.

    The **Local Server** window is displayed.

Step 3 Install the AD service.

Add new services by referring to the **Install the DNS service**.

1. Select **Active Directory Domain Services** in the Roles box shown in **Figure 6-7**.

    The confirmation window is displayed.

2. Click **Add Features**.

    The **Select server roles** window is displayed.

3. Click **Next**.

    The **Select features** window is displayed.

4. Select **.NET Framework 4.5 Features** and click **Next**.

    The **Active Directory Domain Services** window is displayed.

5. Click **Next**.

The confirmation window is displayed.

6. Click **Install**.

The installation progress of the Active Directory Domain Services is displayed.

7. When the installation is complete, click **Close**.

The **Local Server** window is displayed.

Step 4 Configure the AD service.

1. Select **AD DS** in the navigation tree in the **Server Manager** window.

The AD DS properties are displayed in the right pane, as shown in **Figure 6-8**.

Figure 6-8 AD DS properties
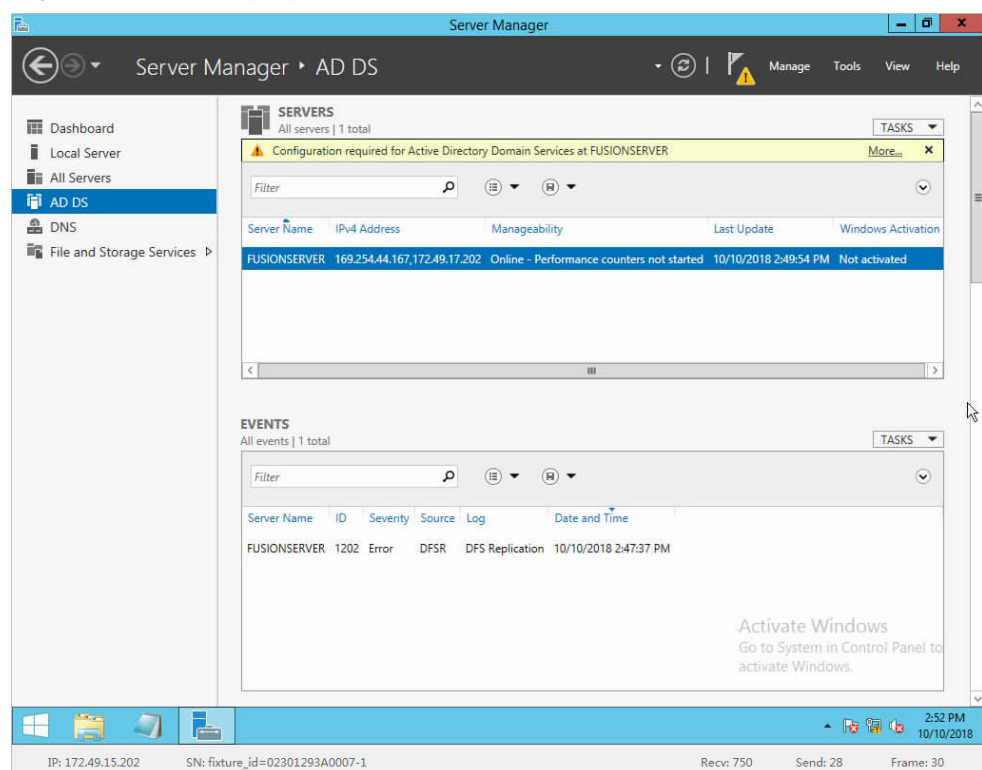
2. Click **More…** in the alarm information.

The **All Servers Task Details** window is displayed, as shown in **Figure 6-9**.

Figure 6-9 All servers task details
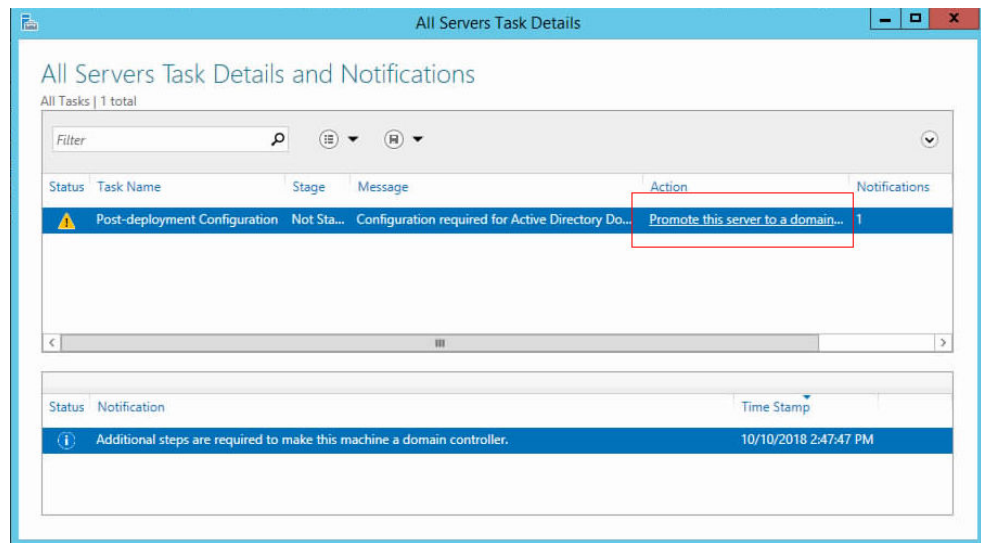
3. Click **Promote this server to a domain controller**.

The **Active Directory Domain Services Configuration Wizard** window is displayed, as shown in **Figure 6-10**.

Figure 6-10 Active Directory Domain Services Configuration Wizard
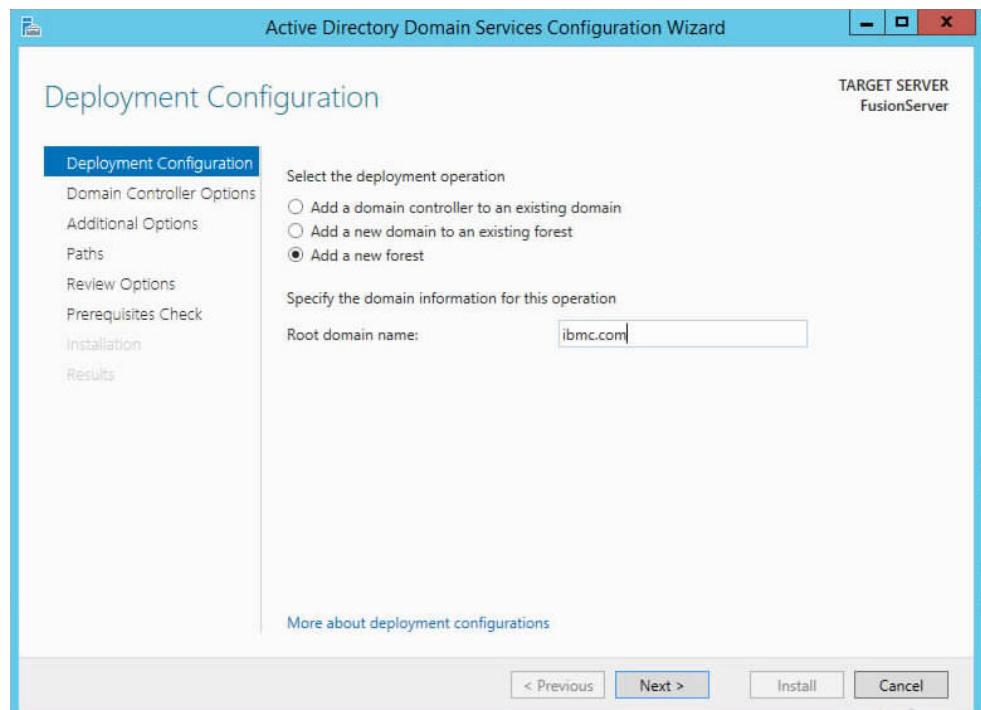
4. Select **Add a new forest**, enter the AD domain name, for example **ibmc.com**, in **Root domain name**, and click **Next**.

The **Domain Controller Options** window is displayed, as shown in **Figure 6-11**.

☐ NOTE

The domain name is case-sensitive. Set the domain name based on the planned domain name.

Figure 6-11 Domain controller options
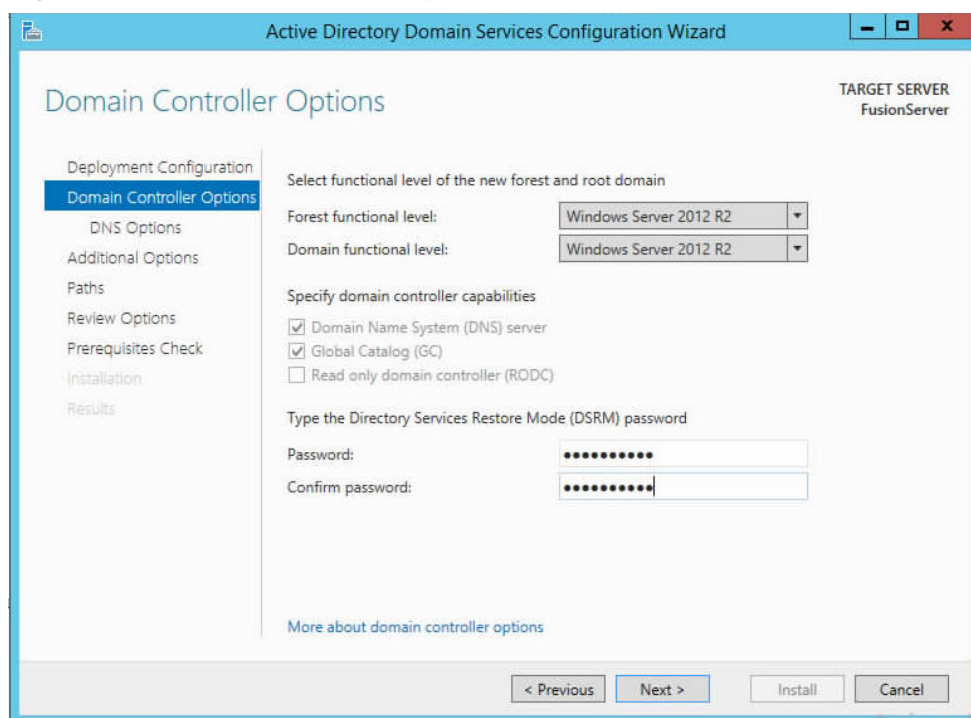
5. Set the AD domain controller password and click **Next**.
6. Click **Next** until the window in **Figure 6-12** is displayed.

Figure 6-12 Domain services paths
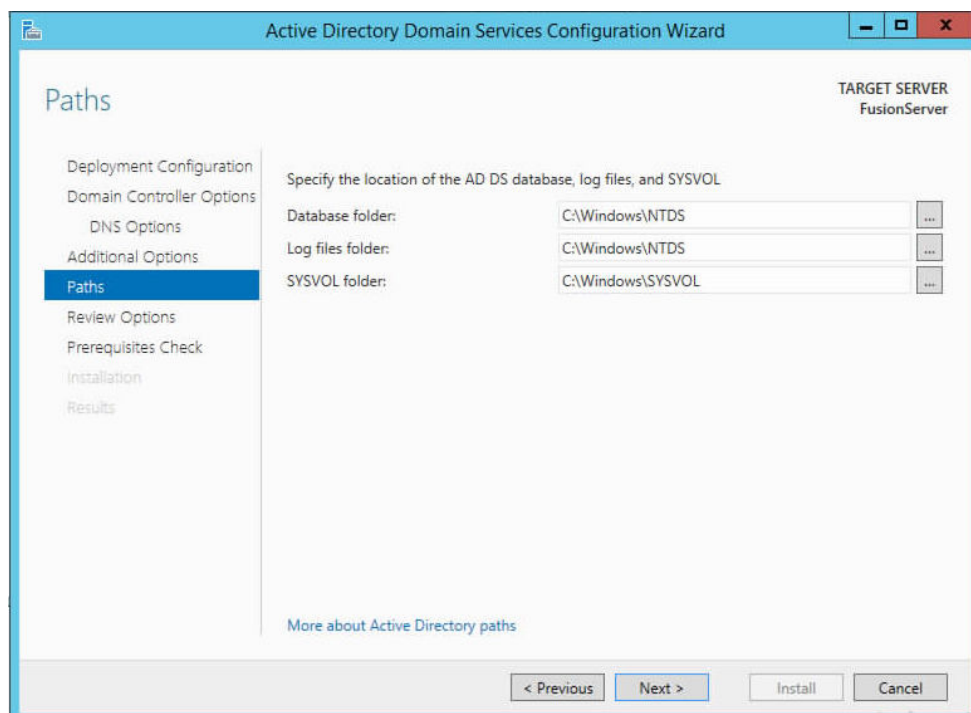
7. Set the AD domain services paths and click **Next**.

   You can also retain the default configuration.

8. Click **Next** in the following windows displayed.

9. When the **Prerequisites Check** window is displayed, click **Install**.

   The OS automatically restarts after the configuration is complete.

Step 5 Install the CS services.

Add new services by referring to **Install the DNS service**.

1. Select **Active Directory Certificate Services** in the **Roles** box shown in **Figure 6-7**.

   The confirmation window is displayed.

2. Click **Add Features**.

   The **Select server roles** window is displayed.

3. Click **Next**.

   The **Select features** window is displayed.

4. Select **.NET Framework 4.5 Features** and click **Next**.

   The **Active Directory Certificate Services** window is displayed.

5. Click **Next**.

   The **Select role services** window is displayed.

6. Select **Certification Authority** and **Certification Authority Web Enrollment**, and click **Next**.

The confirmation window is displayed.

7. Click **Add Features**.

   The **Select server roles** window is displayed.

8. Click **Next**.

9. Click **Install** in the **Confirm installation selections** window.

   The installation progress is displayed.

10. Click **Close** when the installation is complete.

Step 6 Configure the CS services.

1. Open the **Server Manager** window.

2. Select **AD CS** in the navigation tree.

   The AD CS properties are displayed in the right pane, as shown in **Figure 6-13**.

Figure 6-13 AD CS properties
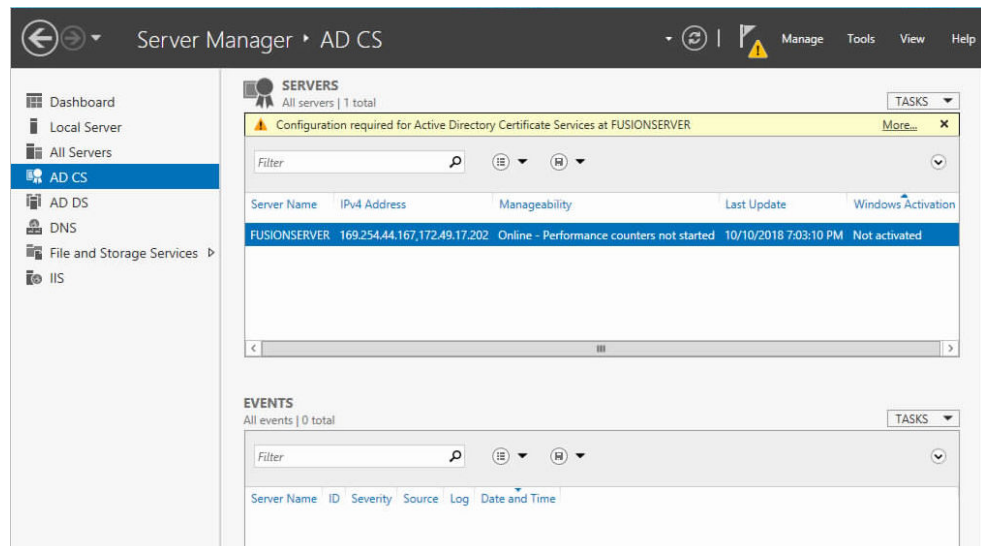
3. Click **More...** in the alarm information.

   The **All Servers Task Details** window is displayed, as shown in **Figure 6-14**.

Figure 6-14 All servers task details
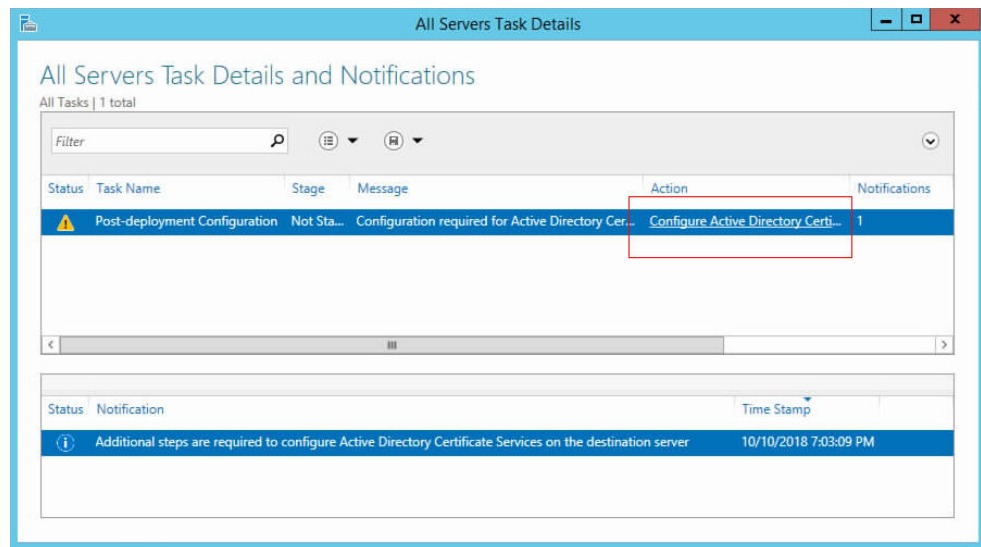
4. Click **Configure Active Directory Certificate Services on the Destination Server**.

   The **AD CS Configuration** window is displayed.

5. Click **Next**.

   The **Role Services** window is displayed, as shown in **Figure 6-15**.

Figure 6-15 Role services
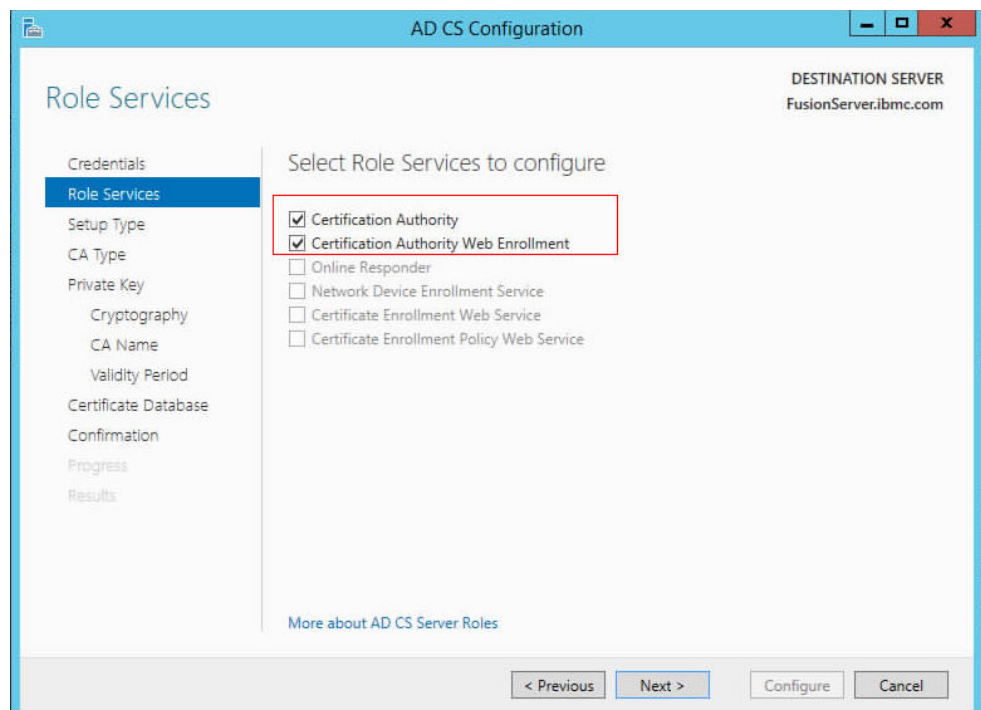
6. Select **Certification Authority** and **Certification Authority Web Enrollment**, and click **Next**.

   The **Setup Type** window is displayed.

7. Select **Enterprise CA** and click **Next**.

   The **CA Type** window is displayed.

8. Select **Root CA** and click **Next**.

   The **Private Key** window is displayed.

9. Select **Create a new private key** and click **Next**.

   The **Cryptography for CA** window is displayed, as shown in **Figure 6-16**.

Figure 6-16 Cryptography for CA
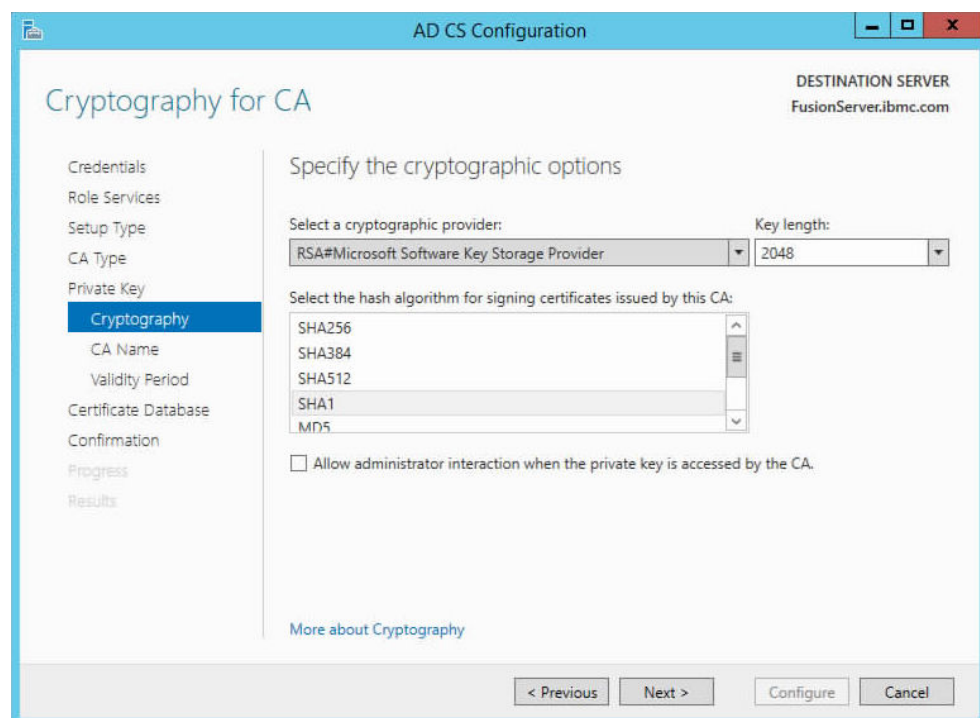
10. Select **RSA#Microsoft Software Key Storage Provider** as the cryptographic provider, **2048** in **Key length**, and **SHA1** as the hash algorithm, and click **Next**.

    The **CA Name** window is displayed, as shown in **Figure 6-17**.

Figure 6-17 CA name
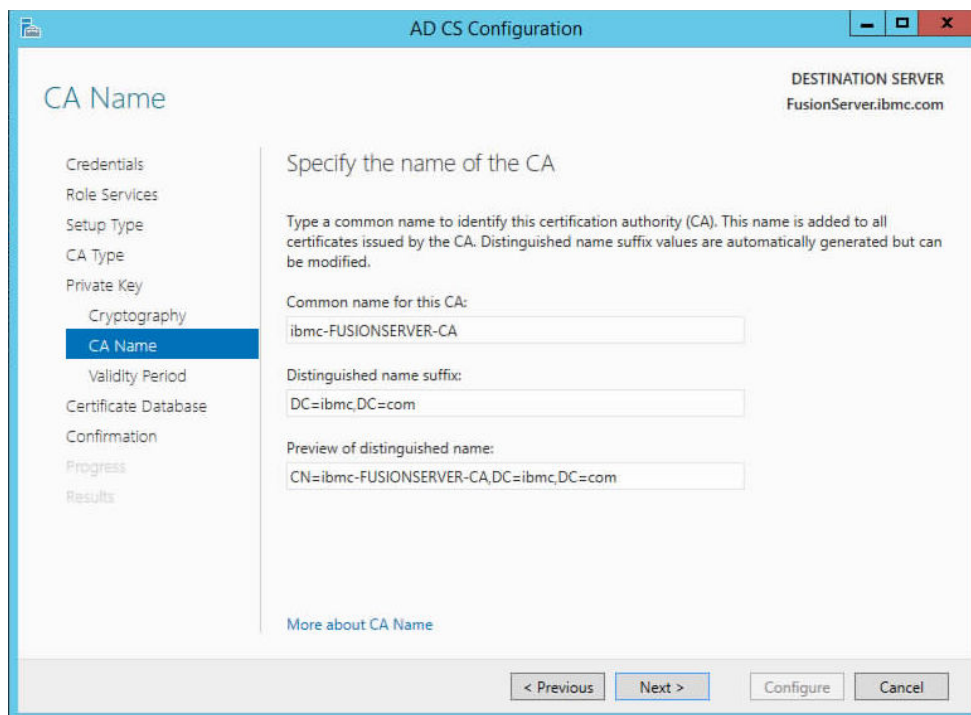
11. Set the common name for this CA and click **Next**.

   The **Validity Period** window is displayed.

12. Set the validity period and click **Next**.

   The **CA Database** window is displayed.

13. Specify the CA database path and click **Next**.

   The Confirmation window is displayed.

14. Click **Configure**.

   The configuration process of AD certificate services is displayed.

15. Click **Close** when the configuration is complete.

Step 7 Restart the server to make the configuration take effect.

Step 8 Create an organizational unit.

   You can create an organizational unit in any node of the LDAP server. The following describes how to create a first-level node and its sub-nodes.

1. Log in to the server OS.

2. Open **Server Manager**, and select **Local Server** in the navigation tree.

3. Select **Active Directory Users and Computers** from the **TASKS** drop-down list at the top right corner of the window.

   The window shown in **Figure 6-18** is displayed.

Figure 6-18 Server manager
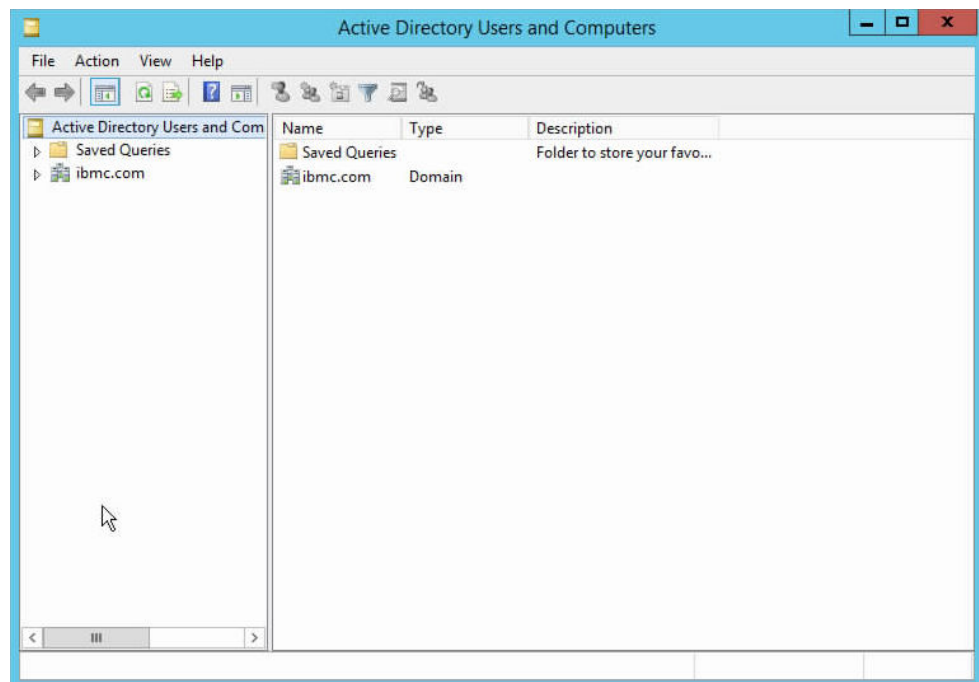
4. Right-click the first-level node (for example, **ibmc.com**) of the LDAP server, and choose **New** > **Organizational Unit**.

The window shown in **Figure 6-19** is displayed.

Figure 6-19 Adding an organizational unit
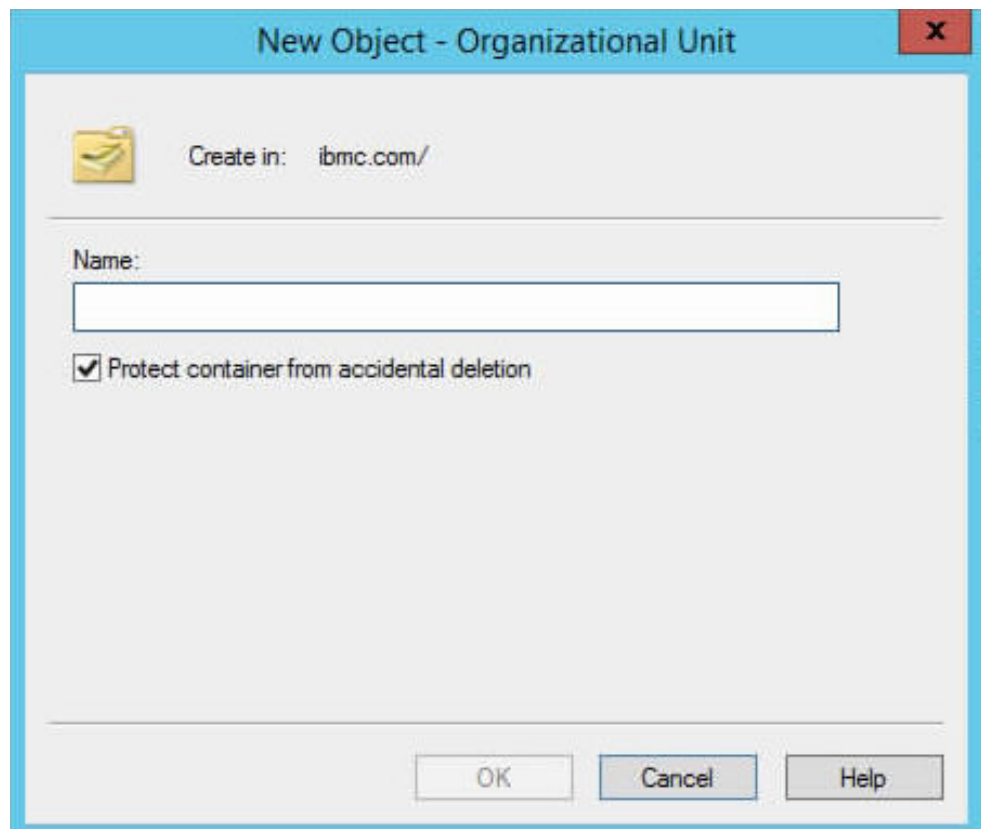
5. Enter the organization name, for example **company**, and click **OK**.

The organizational unit **company** is displayed in the LDAP server organization.

6. Right-click the newly created organizational unit (for example, **company**), and choose **New** > **Organizational Unit** to create a sub-organizational unit (for example, **department**).

The sub-node **department** is displayed under **company**.

7. Repeat **Step 8.4** to **Step 8.6** to create organizational units based on actual needs.

Step 9 Create an LDAP group.

Create an LDAP group in any node based on actual needs.

1. Right-click the node (for example, **department**), and choose **New** > **Group**.

The **New Object-Group** window is displayed, as shown in **Figure 6-20**.

Figure 6-20 Creating a group
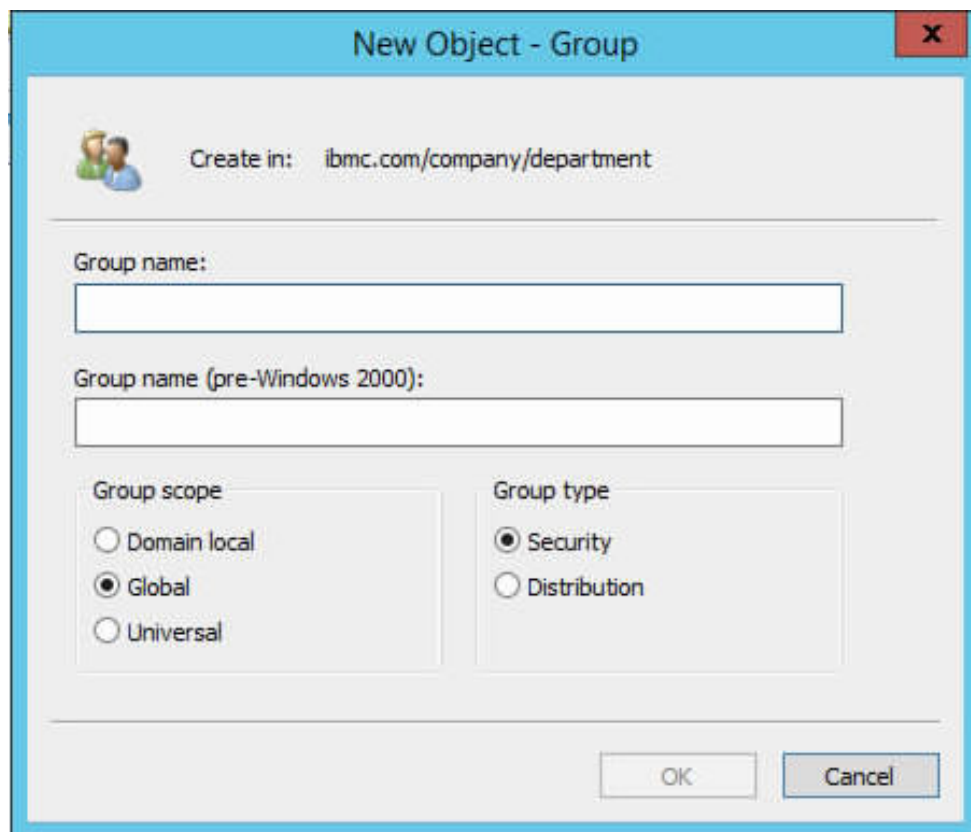
2. In the **Group name** box, enter the LADP group name, for example **info_group1**, select the group scope and the group type, and click **OK**.

   □ NOTE

   You are advised to set the same value for **Group name** and **Group name (pre-Windows 2000)**.

   The newly created group (for example, **info_group1**) is displayed in the specified organization.

3. Repeat **Step 9.1** to **Step 9.2** to create groups based on actual needs.

Step 10 Create a user.
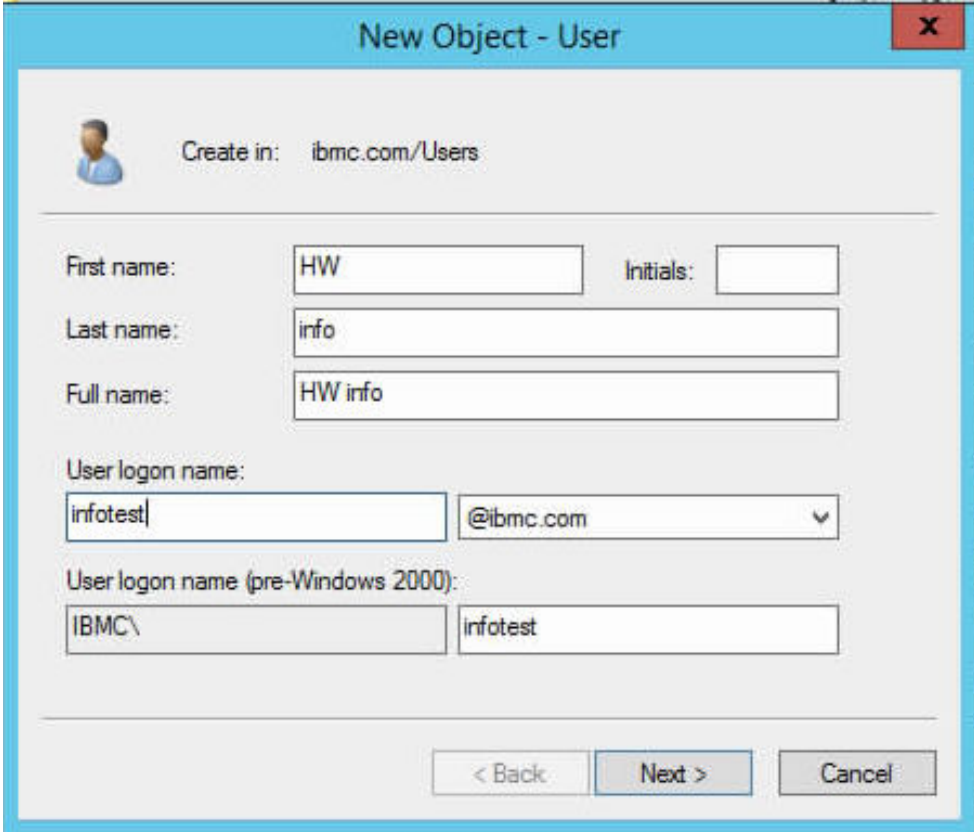
You can add users in any directory, but you are advised to add users in the **Users** directory.

1. Right-click the node (for example, **Users**) and choose **New** > **User**.

2. In the **New Object-User** window as shown in **Figure 6-21**, enter the user information and click Next.

   □ NOTE

   User login name is the domain name used to log in to the iBMC WebUI. Record the user login name.

Figure 6-21 Creating a user
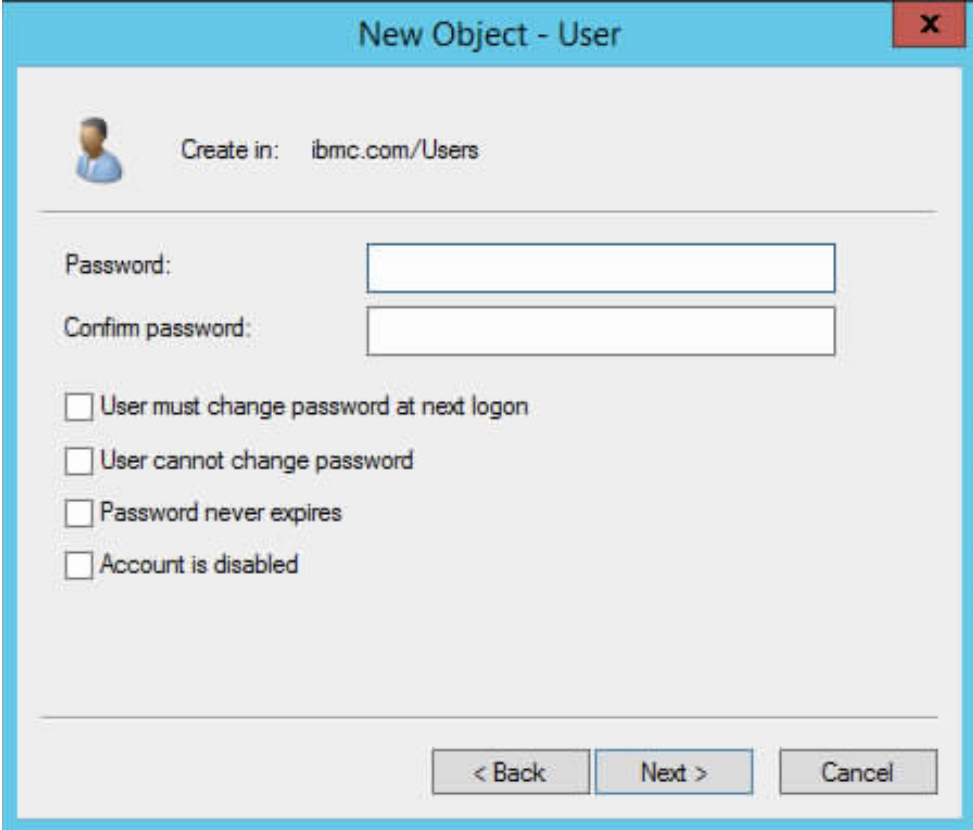
3. Click **Next**.

   The window shown in **Figure 6-22** is displayed.

Figure 6-22 Setting the password

4. Enter the password (for example, **Test12#$**) in the **Password** and **Confirm password** boxes, select the password policy, and click **Next**.

NOTICE

Do not select **User must change password at next logon** as the password policy.

The user information confirmation window is displayed.

5. Click **Finish**.

The user **HWinfo** is displayed in the **Users** list.

6. Create other users in the same way.

Step 11 Add the user to a group.

You can add a user to a group by managing the user or group. The following uses the operations on the user as an example.

1. Right-click the user created in **Step 10** (for example, **HWinfo**) and choose **Add to a group**.

The **Select Groups** window is displayed, as shown in **Figure 6-23**.

Figure 6-23 Select groups
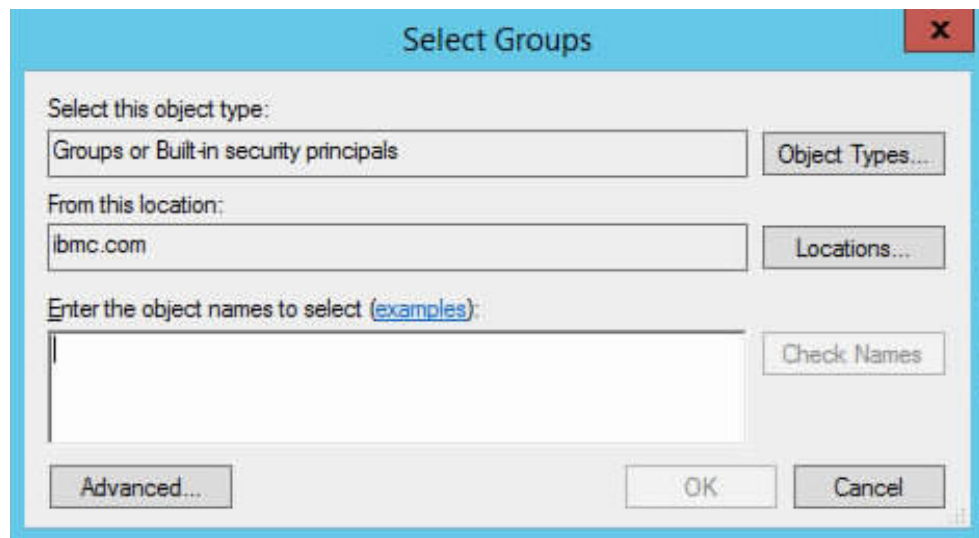
2. In **Enter the object names to select**, enter the group name (for example, **info_group1**) to which the user is to be added, and click **OK**.

A message is displayed indicating the operation is successful.

3. Repeat the steps to add users to the related groups based on actual needs.

----End

6.6.2 Configuring the LDAP Parameters on the iBMC

Scenario

Configure the Lightweight Directory Access Protocol (LDAP) function on **Configuration** > **LDAP** of the iBMC WebUI.

The LDAP function enables domain users to access the iBMC.

📖 **NOTE**

● A common function of LDAP is to provide a central repository for user names and passwords, which allows different applications and services to connect to the LDAP server to validate users.

● The iBMC only provides an access interface for LDAP users; therefore this section does not include the procedure of configuring domain controllers, user domains, and LDAP users. For details, see the user guide of the domain controller you use.

Prerequisites

Data

● LDAP server information, including the LDAP server address, domain name, host name, user application folder, and LDAP user group name

● Password for logging in to the iBMC WebUI

Procedure

Step 1 Log in to the iBMC WebUI. For details, see **3.1 Logging In to the iBMC WebUI**.

Step 2 Configure the LDAP server on the iBMC.

1. On the iBMC WebUI, choose **Configuration** > **LDAP**.

2. Set **LDAP** to [ON] to enable the LDAP function.

3. Set the LDAP server parameters.

   The following parameters must be configured.

   – **LDAP Server Address**: Enter the LDAP server IP address, for example, **192.168.66.66**.

   – **LDAPS Port**: Enter the port number of the LDAP server.

   – **Domain**: Enter the LDAP server domain name, for example, **ibmc.com**. This domain name must be the same as the domain name set on the LDAP server.

   – **Current User Password**: Enter the password for logging in to the iBMC.

   Set other parameters based on actual needs. For details about parameter description, see **3.7.2 LDAP**.

4. Click **Save**.

Step 3 (Optional) Import an LDAP root certificate.

You can choose whether to import the LDAP root certificate. For security purposes, enable certificate validation.
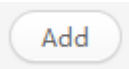
1. Set the DNS server address to the LDAP server address. For details, see **6.7 Configuring the DNS on the iBMC WebUI**.

2. On the **LDAP** page, set **Certificate Verification** to **Enable**.

3. Under **Root Certificate**, click **Browse** and select the root certificate to be uploaded.

   The root certificate must be in .cer, .pem, .cert, or .crt format.

4. Click **Upload**.

   If the root certificate is successfully uploaded, "The certificate has been uploaded" is displayed.

Step 4 Configure the LDAP group.

1. In the **LDAP Groups** area, click [Add] or [✏].

2. In **Current User Password**, enter the iBMC user password.

3. Configure LDAP group parameters.

   – **LDAP Group**: Enter the LDAP user group name, for example **info_group1** (the LDAP group name set in **6.6.1 Configuring the LDAP Server**).

   – **LDAP Group Folder**: Enter the name of the folder in which the LDAP group applications are stored.

     The LDAP group folder must be the same as the organizational unit set on the LDAP server, for example, **company/department** (the organizational unit set in **6.6.1 Configuring the LDAP Server**).

- – **Login Rules**: Set the login rules.
- – **Login Interfaces**: Set the login interfaces.
- – **Role**: Assign operation permissions to the user group.

4. Click **Save**.

Step 5 Use a domain account to log in to the iBMC.

1. On the iBMC login page, enter the user name **test** and password **HWinfo/ Huawei12#$**.

2. In **Domain**, select the LDAP server domain name, for example, **ibmc.com**.

3. Click **Log In**.

----End

6.7 Configuring the DNS on the iBMC WebUI

Scenarios

Configure the domain name system (DNS) on **Configuration** > **Network** of the iBMC WebUI.

The DNS is a distributed database that stores the mapping between domain names and IP addresses. It enables users to access the network using easily memorized domain names instead of numerical IP addresses.

Prerequisites

Data

- iBMC host name
- IP addresses and domain name of the DNS servers

Procedure

Step 1 Log in to the iBMC WebUI. For details, see **3.1 Logging In to the iBMC WebUI**.

Step 2 Choose **Configuration** > **Network**.

Step 3 In the **iBMC Host Name** area, enter the iBMC host name, for example, **test** in **Server Name**.

Step 4 Click **Save**.

Step 5 In the **DNS** area, select **Manually set DNS address**.

Step 6 Set the DNS address.

1. In **Domain**, enter the DNS server domain name, for example, **manager.com**.

2. In **Preferred Server**, enter the IP address of the preferred DNS server, for example, **192.168.66.66**.

3. In **Alternate Server**, enter the IP address of the alternate DNS server.

4. Click **Save**.

Step 7 On the PC used to connect to the iBMC, set the DNS server addresses.

Ensure that the same DNS addresses are set on the PC and the iBMC.

Step 8 Use the domain name address to log in to the iBMC WebUI.

> **NOTE**
>
> A domain name address consists of the host name and domain name. For example, if the host name is **Test** and the domain name is **manager.com**, the domain name address is **Test.manager.com**.

Open the browser of the PC, enter the domain name address, for example **Test.manager.com**, in the address box, and press **Enter**.

----End

6.8 Configuring the SSH User Private Key

Operation Scenario

Configure the SSH private key.

After the SSH private key has been loaded on the user client and the iBMC, the user can log in to the iBMC CLI over SSH without entering a password. This access mode is recommended due to higher security and easier operation.

Prerequisites

Conditions

- The client (local PC) can communicate with the server iBMC.
- The SSH interface has been enabled on the iBMC.

Data

- SSH public key type: RSA or DSA
- IP address of the iBMC management network port
- SSH service port number

Software

- A free tool, such as **putty.exe**, to log in to the iBMC
- A free tool, such as **puttygen.exe**, to generate private keys

Procedure

Generate an SSH private key.

1 On the client (such as a PC), run **puttygen.exe**.

The **PuTTY Key Generator** window is displayed, as shown in **Figure 6-24**.

Figure 6-24 Private key generation
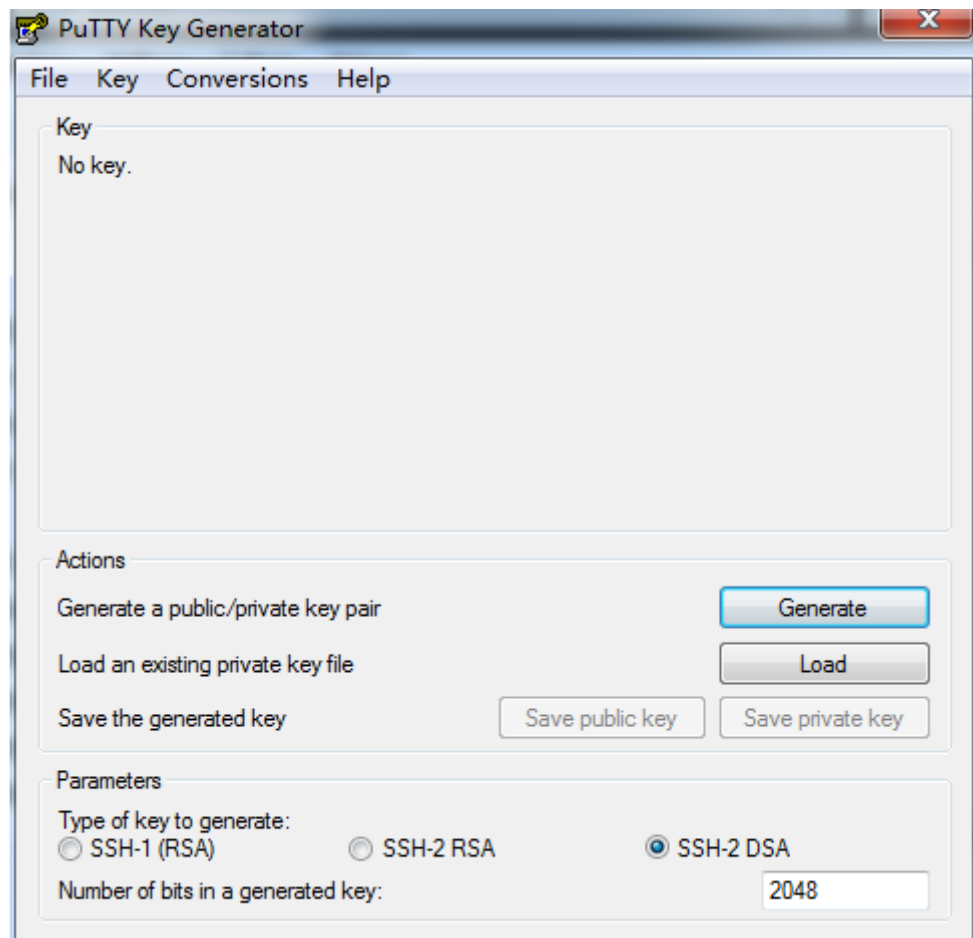
2   In the **Parameters** area, select the private key type, for example **SSH-2 DSA**.

3   Set the private key size.

📖 **NOTE**

For security purposes, set **Number of bits in a generated key** to **2048** or more.
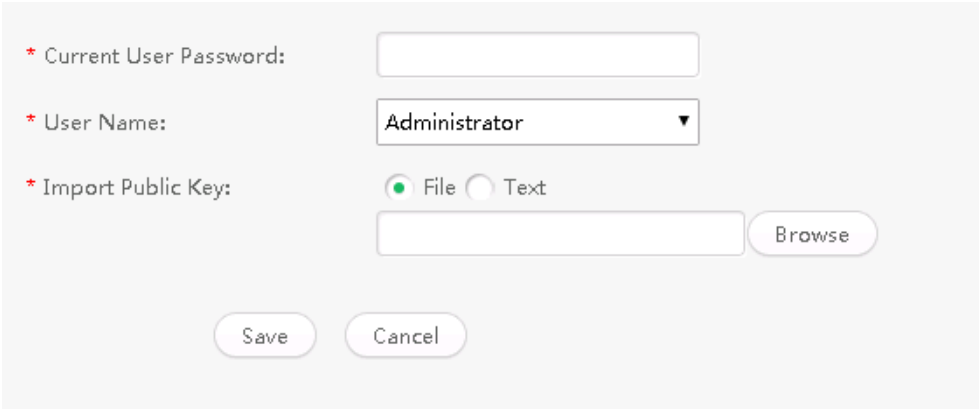
4   Click **Generate**.

5   Click **Save public key** and **Save private key** to save the generated public and private keys to the client.

Import the public key to the iBMC.

6   Log in to the iBMC WebUI. For details, see **3.1 Logging In to the iBMC WebUI**.

7   On the iBMC WebUI, choose **Configuration** > **Local Users**.

8   In the **SSH Public Key Management** area, click **Add**.

The window for importing the SSH public key is displayed, as shown in **Figure 6-25**.

Figure 6-25 Importing an SSH public key

9   Enter the name of the current user.

10   Select the SSH user for whom the SSH public key is to be imported.

11   In **Public Key Import Mode**, select **File**.

12   Click **Browse** and select the public key generated in **Generate an SSH private key**.

13   Click **Save**.

Configure the SSH client.

14   On the PC, run **putty.exe**.

15   Import the private key generated in **Generate an SSH private key**.

        Figure 6-26 shows the interface for importing a private key.

Figure 6-26 Importing a private key
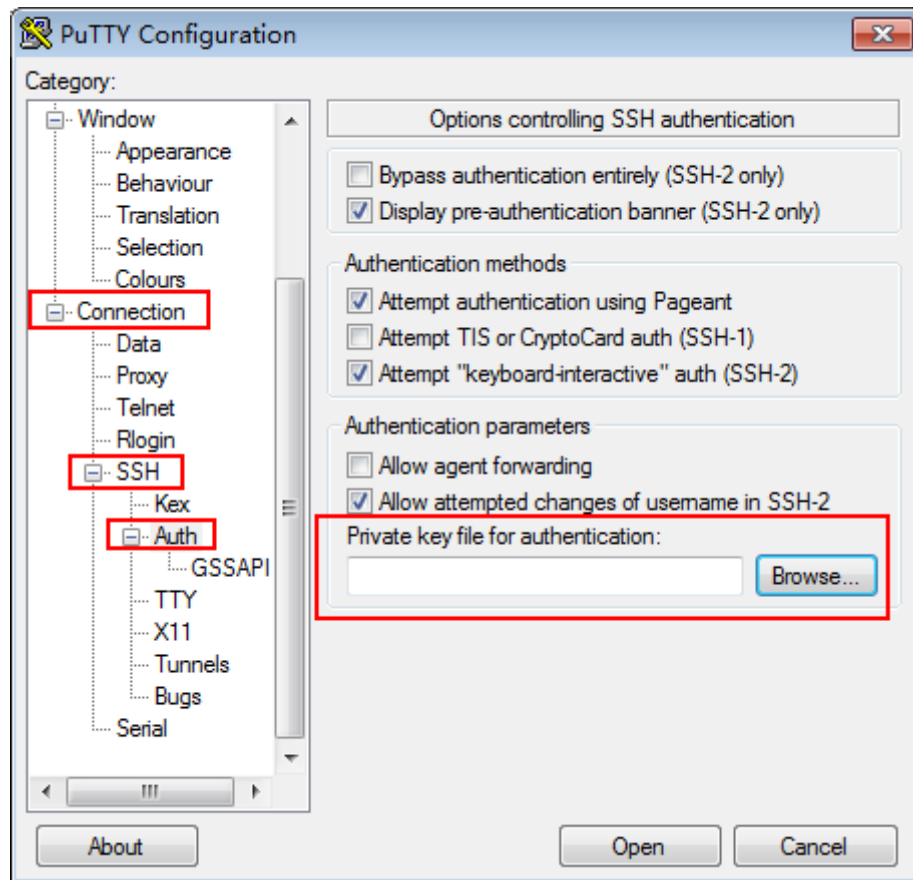
16 Set the user login information.

Enter the iBMC address and SSH port number, as shown in **Figure 6-27**.

Figure 6-27 Setting login information
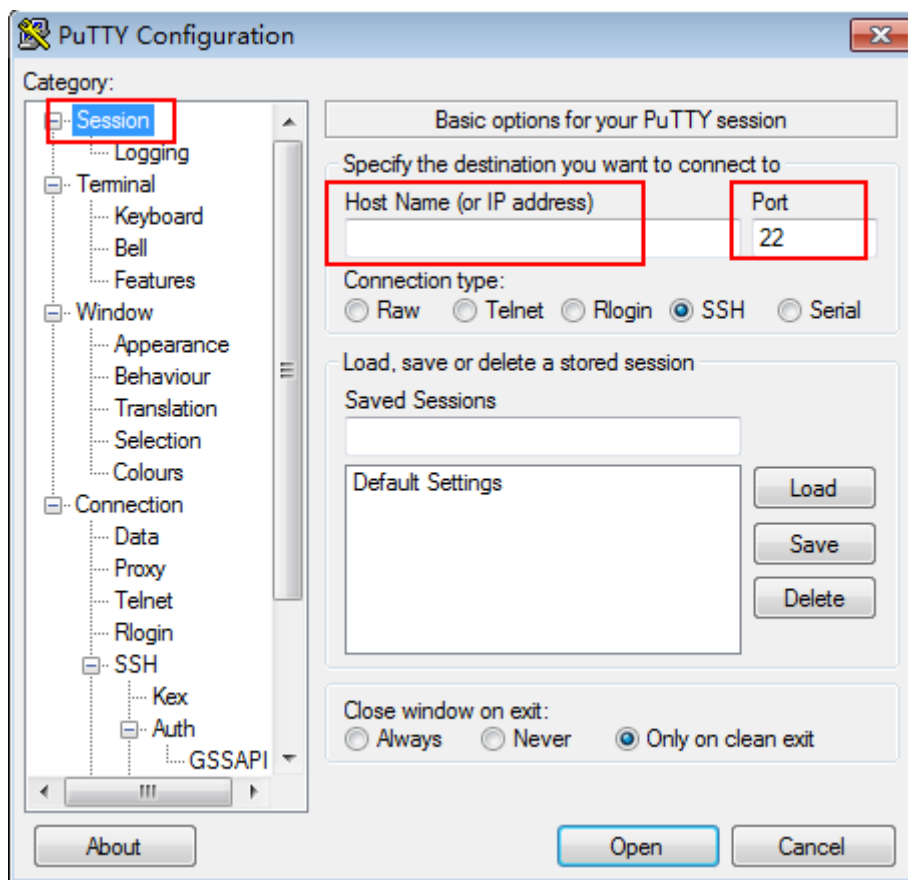
Log in to the iBMC CLI.

> 17 Click **Open**.
>
> 18 Enter the SSH user name.
>
> The iBMC CLI is displayed.
>
> **----End**

6.9 Configuring the iBMC SSL Certificate

Scenarios

Configure a Secure Sockets Layer (SSL) certificate for the iBMC.

SSL helps establish an encrypted link (accessed using HTTPS) between a web server and a browser to ensure secure data transmission. A web server requires an SSL certificate to create an SSL connection.

For security purposes, replace the original certificate and keys with a customized certificate and public and private key pairs.

Prerequisites

Conditions

The local client can communicate with the server iBMC.

Procedure

Step 1 Log in to the iBMC WebUI. For details, see **3.1 Logging In to the iBMC WebUI**.

Step 2 Perform one of the following operations based on the actual scenario:

- If the client has an SSL certificate issued by an official authority, **import the SSL certificate**.
- If the client has an SSL certificate manually generated by the user, **import the SSL certificate** and **add a root certificate to the client browser**.
- To customize an SSL certificate and use a certificate issued by an official authority, **customize certificate information**, **obtain an SSL certificate**, and **import the SSL certificate**.
- To customize an SSL certificate and use a certificate manually generated, **customize certificate information**, **obtain an SSL certificate**, **import the SSL certificate**, and **add a root certificate to the client browser**.

Step 3 Customize certificate information.

1. On the iBMC WebUI, choose **Configuration** > **SSL Certificate**.
2. Click **Customize**.
3. Under **1. Generate CSR**, set certificate information.

   Certificate information includes country, state, city/location, organization name and unit, and common name.
4. Click **Generate**.

   A certificate signing request (CSR) file is generated.
5. Save the CSR file to the client.

Step 4 Obtain an SSL certificate.

You can obtain an SSL certificate using one of the following methods:

- Apply for an SSL signature certificate from an official certificate authority. (recommended)
- Use a certificate generation tool (such as OpenSSL) to generate an SSL signature certificate and root certificate.

   You can download the certificate generation tool and its manual from the Internet.

Step 5 Import the SSL certificate.

1. On the **SSL Certificate** page, click **Customize**.
2. Import the SSL certificate.

   - To use an SSL certificate issued by a certificate authority, click **Browse** under **2. Import Server Certificate**, select the SSL signature certificate to be used, and click **Import**.
   - To use an SSL certificate manually generated, click **Browse** under **Import Custom Certificate (Optional)**, select the SSL signature certificate to be used, enter the password in **Certificate Password**, and click **Import**.

   After the certificate is imported, "Succeeded in importing the certificate. Reset iBMC for the certificate to take effect." is displayed.

3. Restart the iBMC.

Step 6 Add a root certificate to the client browser.

> 📖 **NOTE**
>
> If the imported SSL certificate is not issued by an official authority, check whether the client browser has the root certificate after the SSL certificate is imported.

The following uses Internet Explorer as an example to describe how to check and add a root certificate to the browser.

1. Open Internet Explorer.

2. On the toolbar, choose **Tools** > **Internet Options**.

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

3. On the **Content** tab page, click **Certificate**.

   The **Certificate** dialog box is displayed.

4. On the **Trusted Root Certificate Issuer** tab page, check whether the SSL certificate issuer is listed.

   – If yes, go to **Step 6.5**.

   – If no, go to **Step 6.6**.

5. Check whether the SSL certificate has expired.

   – If yes, go to **Step 6.6**.

   – If no, go to **Step 6.7**.

6. On the **Trusted Root Certificate Issuer** tab page, click **Import** and import the root certificate as instructed.

7. Open Internet Explorer again, and check whether the 🔒 icon is displayed on the address bar.

   – If yes, no further action is required.

   – If no, contact Huawei technical support.

----End

6.10 Configuring Syslog on the iBMC WebUI

Scenarios

Enable and configure the syslog function on **Alarm & SEL** > **Alarm Settings** of the iBMC WebUI.

Prerequisites

Conditions

The local client can communicate with the server iBMC.

Data

- Syslog information:

- Information used to identify the source host, for example, the board serial number, product asset tag, or host name
- Transmission protocol to be used, for example, TLS, TCP, or UDP
- Syslog authentication method, for example, one-way or two-way authentication
- Log levels
- Syslog server information and log types:
  - Channel status
  - Server address
  - Server port number
  - Types of logs to be reported

Software

A free certificate generation tool, such as **OpenSSL**, downloaded from the Internet.

Procedure

Step 1 Generate certificates.

The certificates required vary depending on the authentication mode:

- One-way authentication: requires a syslog server certificate and a server root certificate.
- Two-way authentication: requires a syslog server certificate, a server root certificate, a syslog client certificate, and a client root certificate.

For details about how to generate certificates, see the user guide of **OpenSSL**.

Step 2 Upload certificates to the syslog server.

Use a file transfer tool that supports SFTP, for example WinSCP, to transfer the certificates to the specified directory (for example **/tmp**) of the iBMC file system.

- One-way authentication: Upload the server certificate to the syslog server.
- Two-way authentication: Upload the server certificate and client root certificate to the syslog server.

Step 3 Log in to the iBMC WebUI.

For details, see **3.1 Logging In to the iBMC WebUI**.

Step 4 Configure the syslog function.

1. On the iBMC WebUI, choose **Alarm & SEL** > **Alarm Settings**.
2. In the **Syslog Notification Settings** area, set **Syslog Notifications** to
   ON.
3. Set **Syslog Server Identity**, **Alarm Severities**, **Transmission Protocol**, and **Authentication Mode**.

   For details, see **Table 3-25**.
4. Upload certificates.

- – If **Authentication Mode** is **One-way**, upload the server root certificate (generated in **Generate certificates**) to the iBMC.
- – If **Authentication Mode** is **Two-way**, upload the server root certificate and client certificate (generated in **Generate certificates**) to the iBMC.

Step 5 Configure the syslog server and message format.

1. Locate the channel for sending syslog messages, and click 🖊 in the **Operation** column.

2. Set **Current Status** to ON to enable the channel.

3. Set **Server Address**, **Syslog Port**, and **Log Type**.

4. Click **Test**.

----End

6.11 Logging In to a Server Using VNC

Scenarios

Log in to a server using the Virtual Network Computing (VNC) service.

The VNC service configuration function provided by the iBMC enriches KVM operation interfaces and provides a more flexible KVM operation mode. The VNC is an open-source protocol, and you can obtain the required VNC tool from a variety of third-party VNC tools available.

The VNC service supports data transmission with or without SSL encryption. This section uses the VNC transmission without SSL encryption as an example.

Prerequisites

Conditions

The client (local PC) is connected to the iBMC management network port of the target server.

Data

- iBMC management network port address and port number (VNC service port number)
- VNC service password

Software

A third-party VNC client, for example, TigerVNC or RealVNC, has been installed on the local PC.

Procedure

Enable the VNC service.

The VNC service can be enabled through the iBMC web, CLI, IPMI, or Redfish interface. This section uses the operations on the iBMC WebUI as an example.

1   Log in to the iBMC WebUI.

For details, see **3.1 Logging In to the iBMC WebUI**.

2   Choose **Configuration** > **Services**.

3   Set the VNC service to ![ON], set the port number, and click **Save**.

The VNC service is disabled by default. The default VNC port number is **5900**.

Configure VNC settings.

4   On the iBMC WebUI, choose **Remote Console**.

5   Set the VNC password and deselect **SSL Encryption**.

the password must meet the following requirements:

–   It must be of 8 characters

–   Contain at least a space or one of the following special characters:

`~!@#$%^&*()-_=+\|[{}];:'",<.>/?

–   Contain at least two types of the following characters:

▪   Uppercase letters A to Z

▪   Lowercase letters a to z

▪   Digits 0 to 9

📖 NOTE

For security purposes, you are required to enter the login password when saving the settings.

(Optional) Use TigerVNC to log in to the server from a Linux client.

6   In the TigerVNC installation folder on the client, open the CLI console and run the **vncviewer ipaddress:port** command.

In this command, *ipaddress* indicates the IPv4 or IPv6 address of the server iBMC network port, and *port* indicates the port number of the VNC service.

The TigerVNC login window is displayed, as shown in **Figure 6-28**.

Figure 6-28 TigerVNC login window
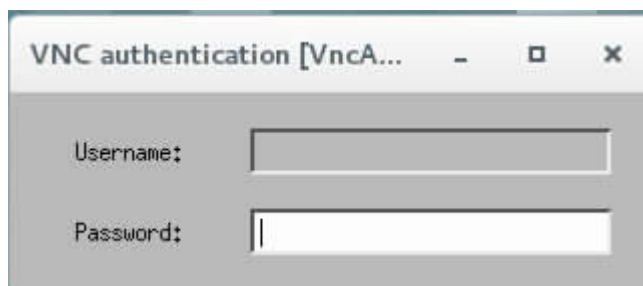
7   Enter the password set in **5**, and press **Enter**.

The server desktop is displayed, as shown in **Figure 6-29**.

Figure 6-29 Server desktop
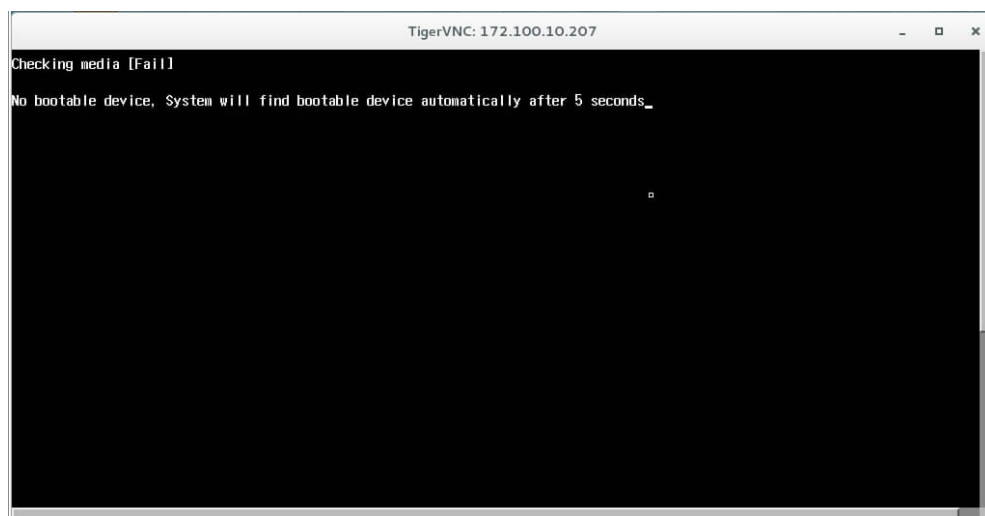
(Optional) Use RealVNC to log in to the server from a Windows client.

      8   On the client, double-click the RealVNC software.

           The RealVNC login window is displayed, as shown in **Figure 6-30**.

Figure 6-30 RealVNC login window
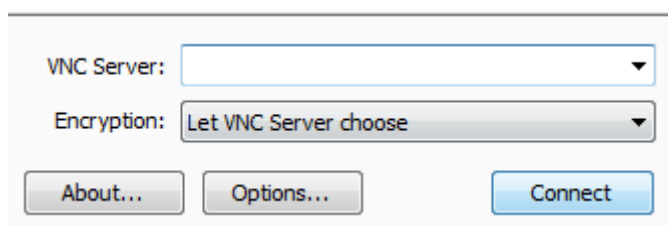
      9   Click **Options**.

           The VNC basic setting dialog box is displayed, as shown in **Figure 6-31**.

Figure 6-31 VNC client basic settings
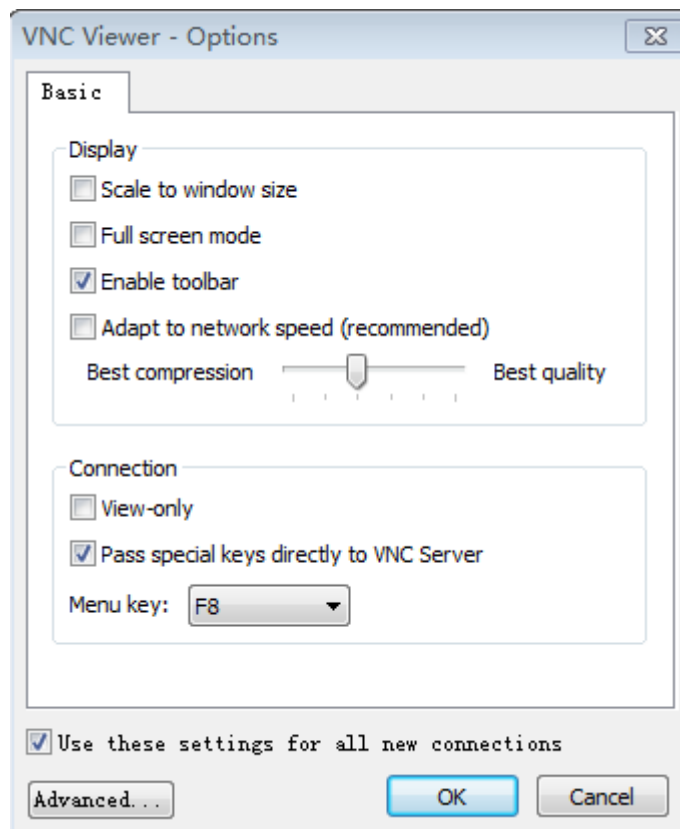
10 Set parameters based on service requirements, and click **OK**.

The login window, as shown in **Figure 6-30**, is displayed.

11 In the text box next to **VNC Server**, enter *iBMC management network port IP address*:*VNC port number*, for example, **192.168.100.169:5900**.

12 Click **Connect**.

If the **Encryption** dialog box is displayed, click **Continue**.

The dialog box shown in **Figure 6-32** is displayed.

Figure 6-32 RealVNC client authentication
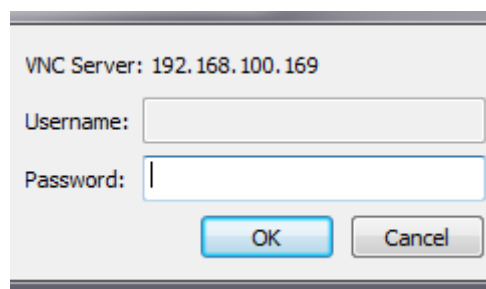
13 In the text box next to **Password**, enter the password set in **5** and click **OK**.

The server desktop is displayed, as shown in **Figure 6-33**.

Figure 6-33 Server desktop
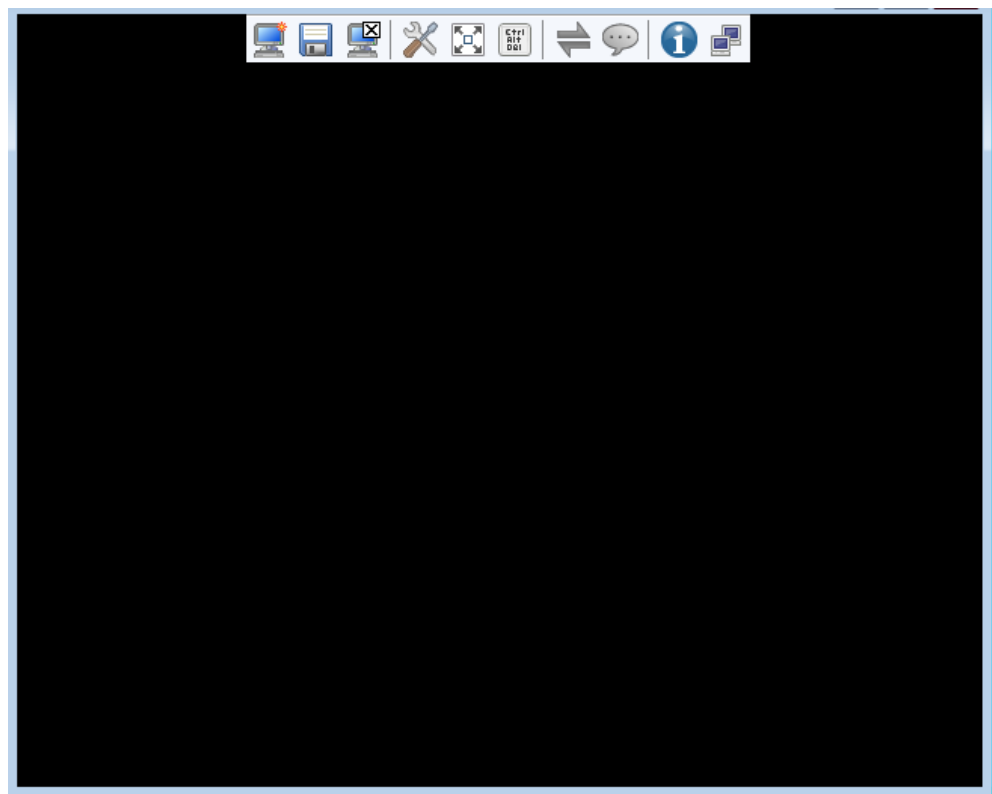
----End

6.12 Importing the iBMC Trust and Root Certificates

Scenarios

A security alert will be displayed when you log in to the iBMC WebUI using a browser. If you do not want this alert to be displayed, import the trust and root certificates of the iBMC using the browser.

This section uses Internet Explorer 11.0 as an example to describe how to import trust and root certificates of the iBMC.

Prerequisites

Conditions

The root and trust certificates to be imported are available.

Data

None.

Software

None.

Procedure

Importing a Trust Certificate

1 Open Internet Explorer, and click ⚙.

The dialog box shown in **Figure 6-34** is displayed.

Figure 6-34 Internet Options
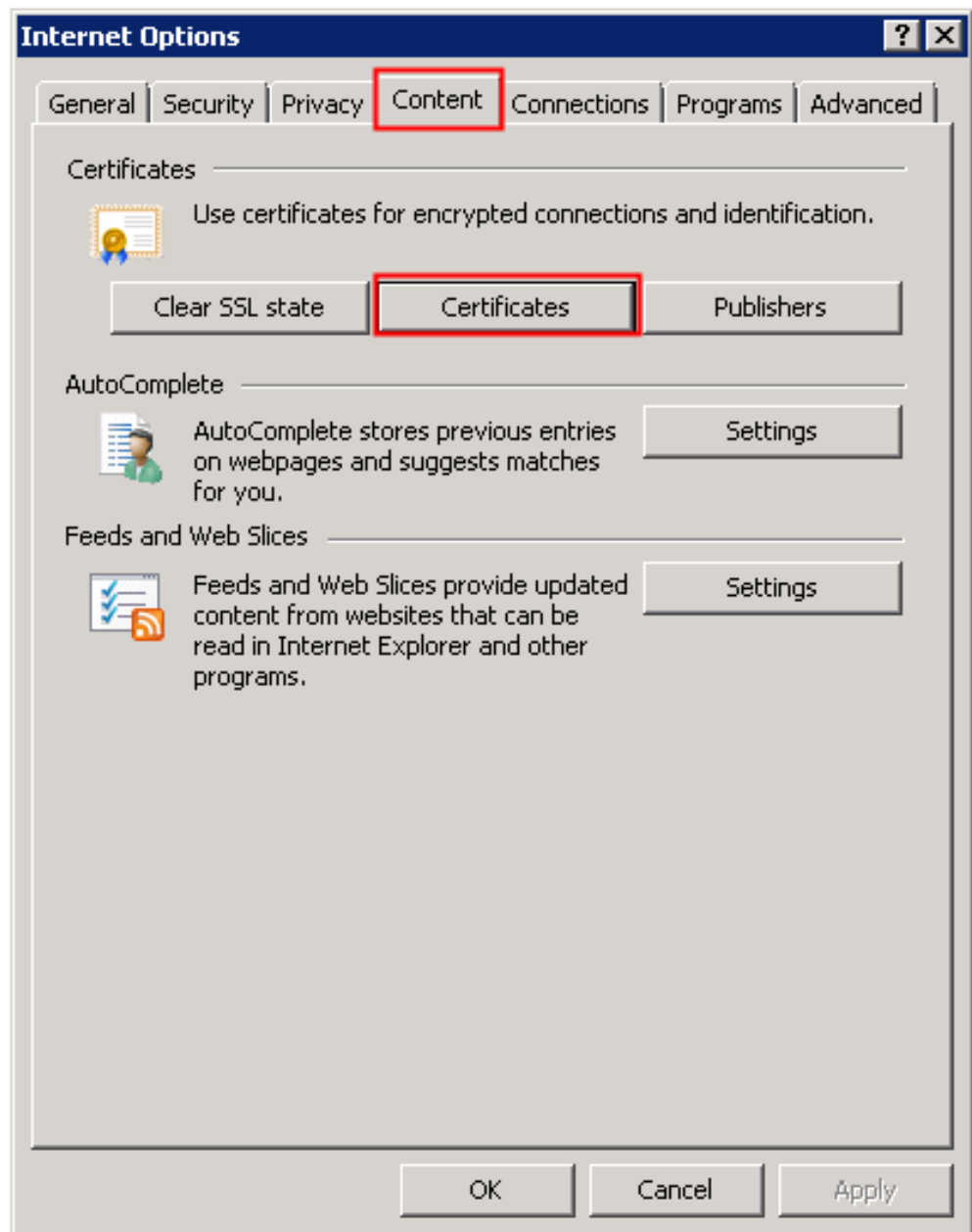
2 Click the **Content** tab and select **Certificates**.

The dialog box shown in **Figure 6-35** is displayed.

Figure 6-35 Certificates
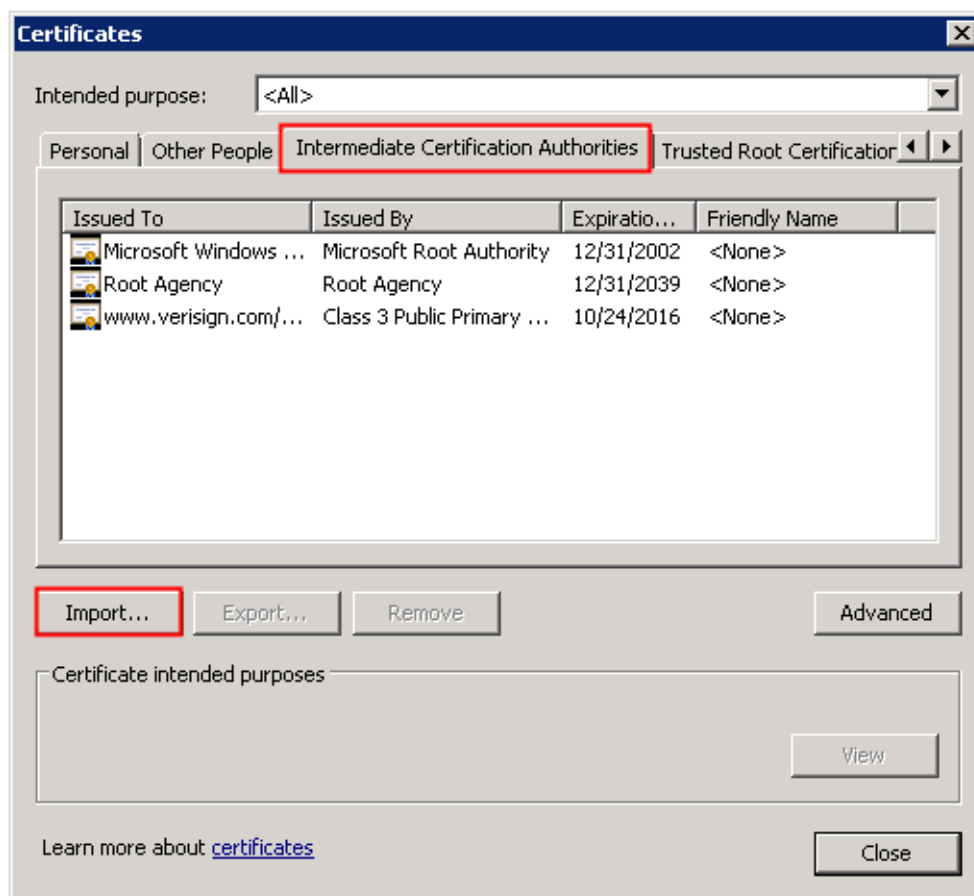
3   Choose **Intermediate Certification Authorities** > **Import**.

The dialog box shown in **Figure 6-36** is displayed.

Figure 6-36 Certificate Import Wizard
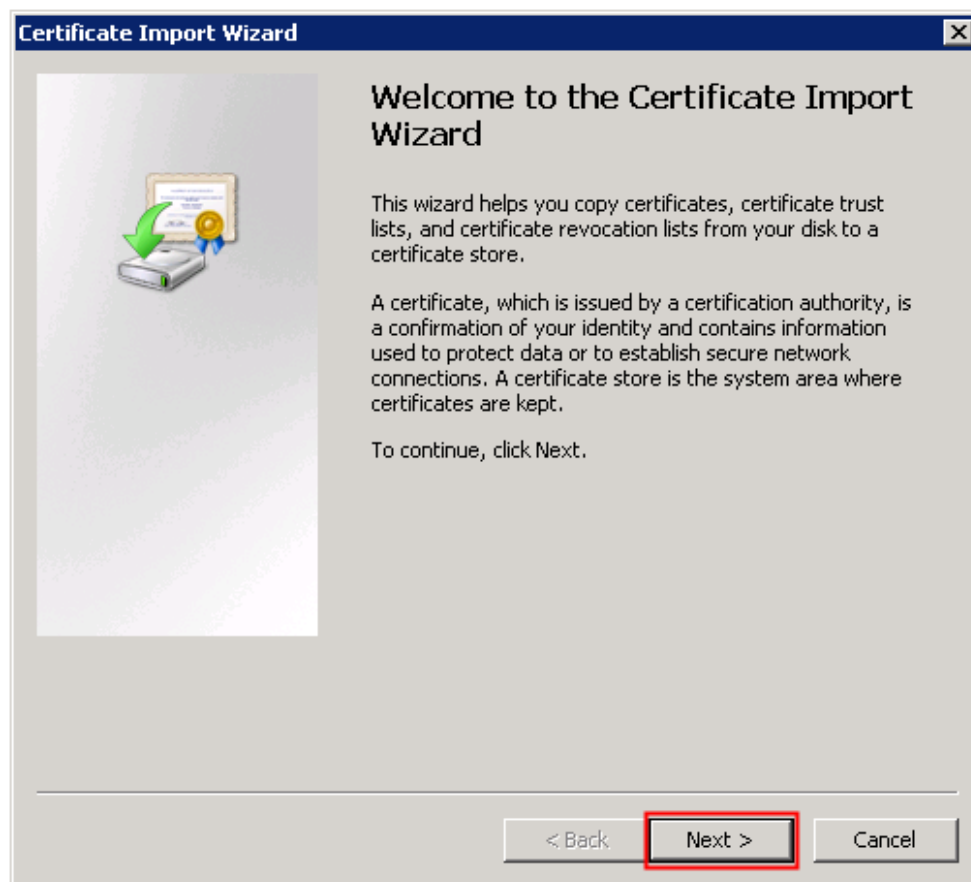
4   Click **Next**.

The dialog box shown in **Figure 6-37** is displayed.

Figure 6-37 Selecting the certificate to be imported
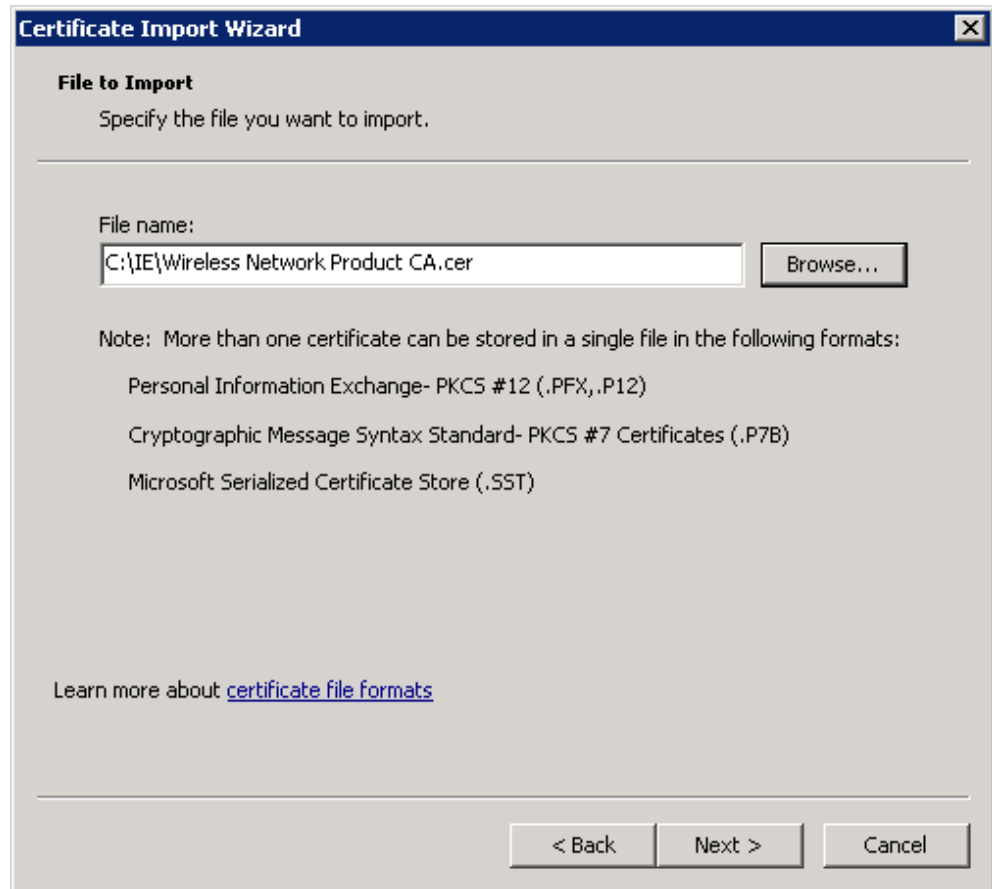
5   Click **Browse**, select the certificate to be imported from the local PC, and click
    Next.

6   In the dialog box displayed, as shown in **Figure 6-38**, select the directory in
    which the certificate is to be stored, and click **Next**.

Figure 6-38 Selecting the destination directory for the certificate
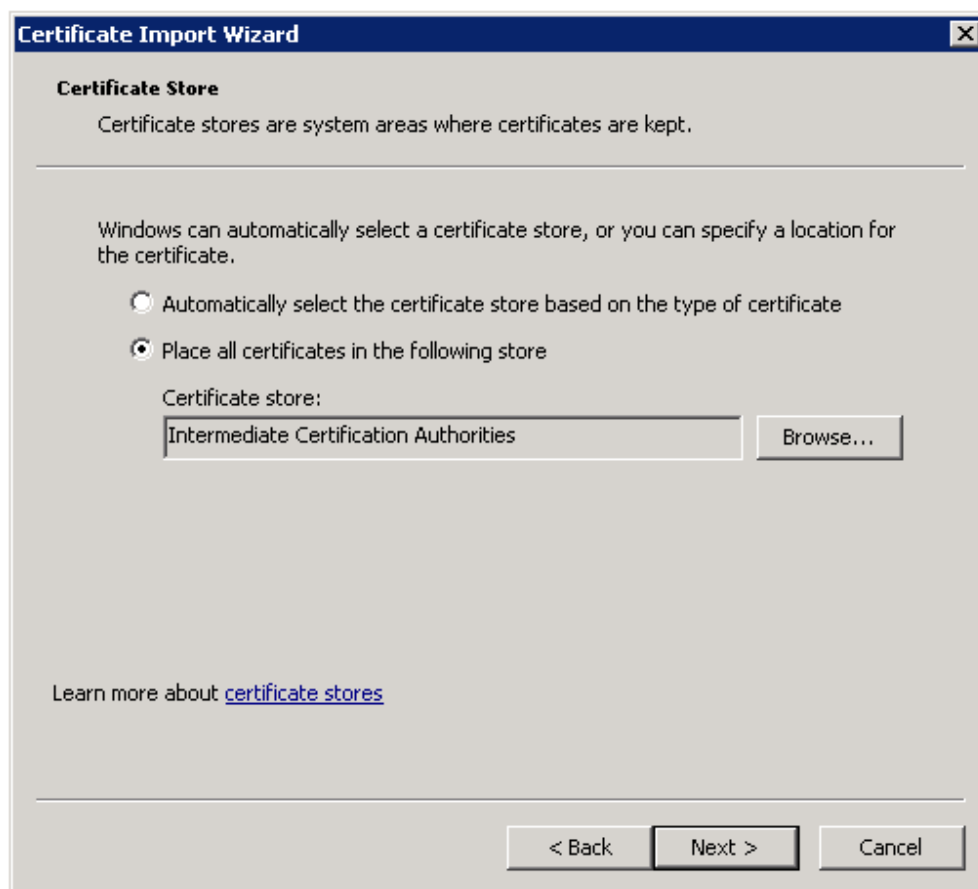
7   Click **Finish**.

If "The import was successful" is displayed, the certificate is imported successfully.

8   Click **OK**.

Importing a Root Certificate

9   Repeat **step 1** and **step 2**.

The dialog box shown in **Figure 6-39** is displayed.

Figure 6-39 Certificates
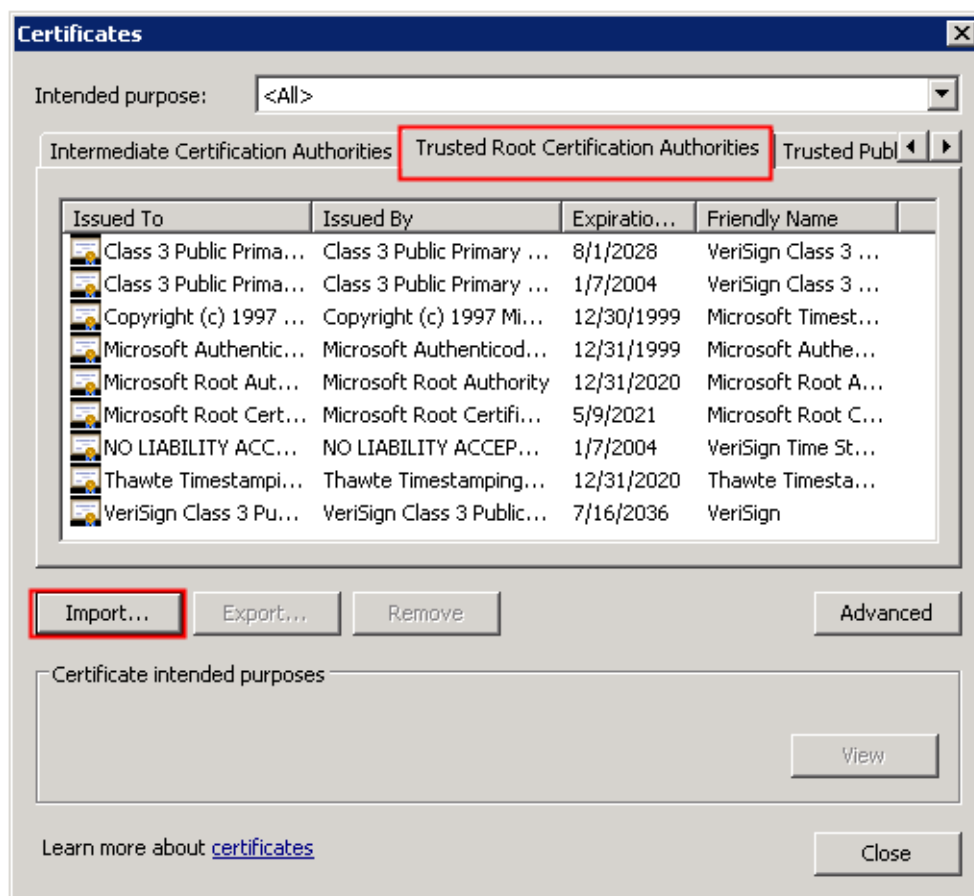
10   Choose **Trusted Root Certification Authorities** > **Import**.

The dialog box shown in **Figure 6-40** is displayed.

Figure 6-40 Certificate Import Wizard
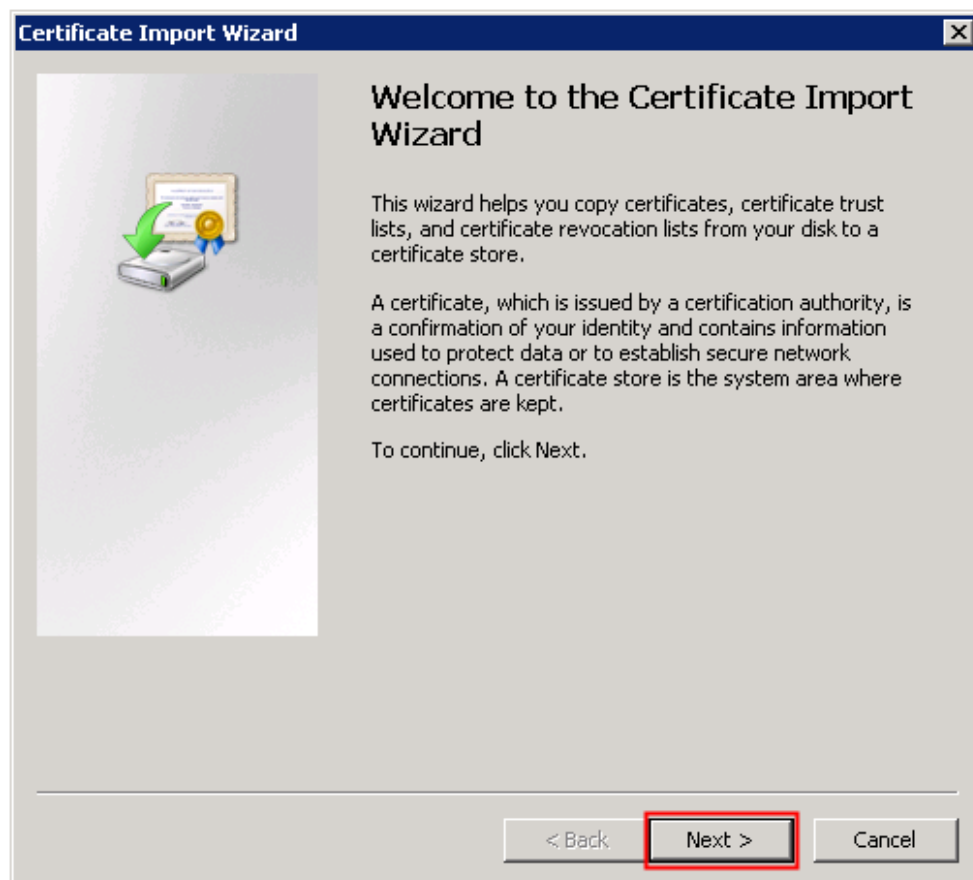
11   Repeat **step 4** to **step 8** to import the root certificate.

Deselecting Allow active content to run in files on My Computer

This operation takes effect only after you restart the server.

12   Click ⚙, and choose **Internet Options** > **Advanced**.

The **Internet Options** window is displayed, as shown in **Figure 6-41**.

Figure 6-41 Internet Options
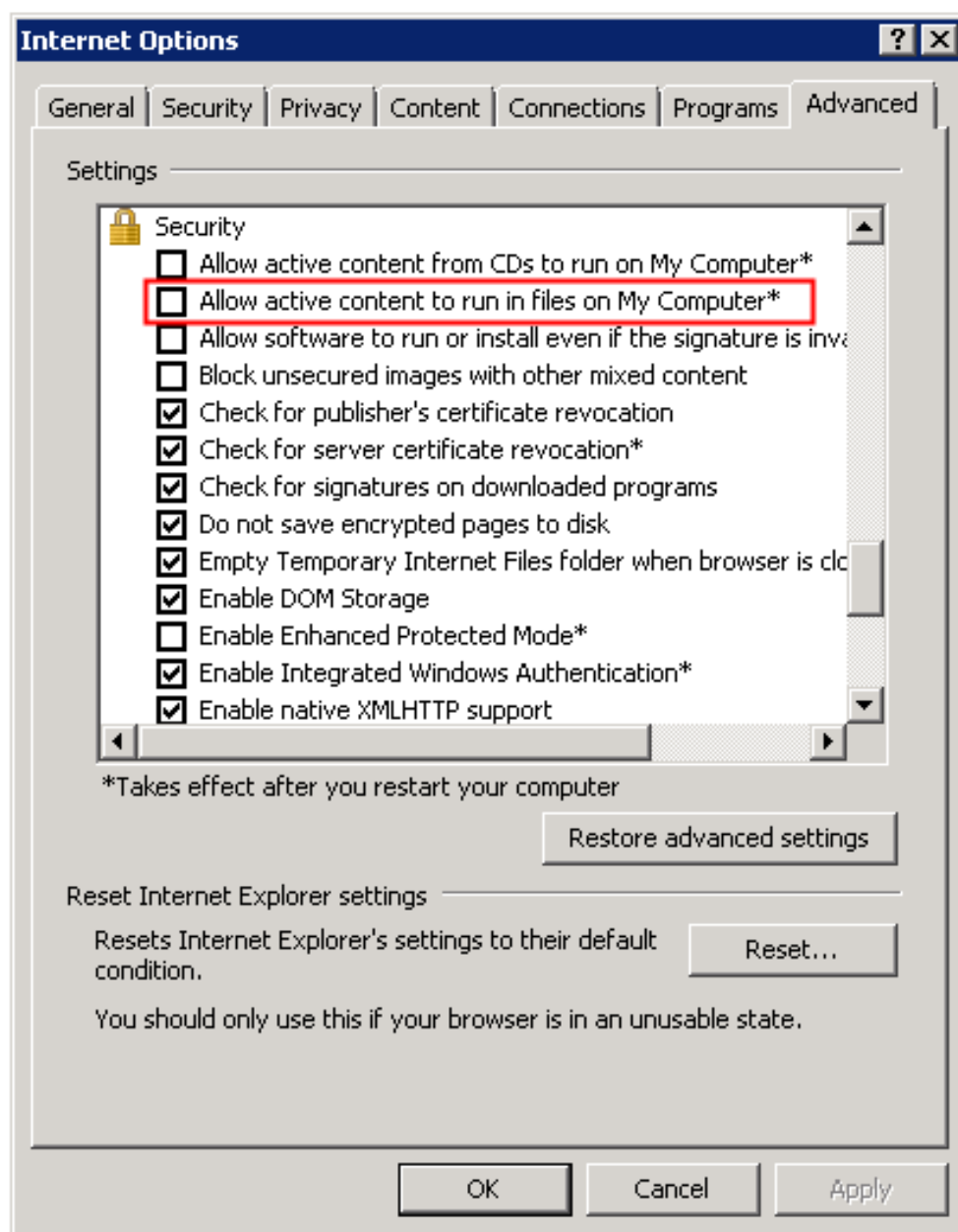
13 Deselect **Allow active content to run in files on My Computer**, and click **Apply** and then **OK**.

If the security alert is still displayed after you log in to the iBMC WebUI, restart the browser and log in to the iBMC WebUI.

☐ **NOTE**

If any other issuer is displayed in **Issued by** in the certificate error message, import the trust certificate of the issuer to shield the security alert.

----End

7 Independent Remote Console

7.1 Overview

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

Basic Principle

Figure 7-1 shows the basic principle of the independent remote console.

Figure 7-1 Basic principle
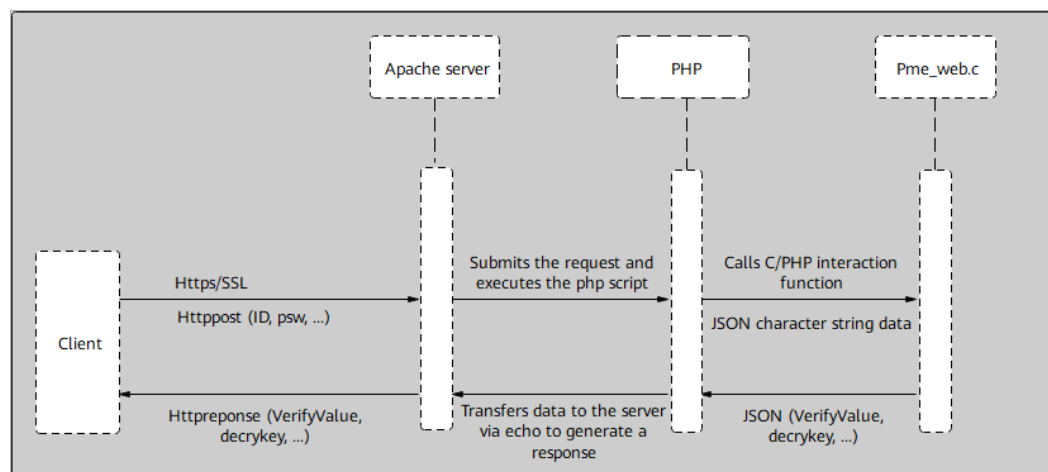
Compatibility

The independent remote console can run in an environment that meets the requirements listed in **Table 7-1**.

Table 7-1 Environmental requirements

Software Package	OS Type	Version
kvm_client_windows.zip	Windows	Windows 7 32-bit or 64-bit
		Windows 8 32-bit or 64-bit
		Windows 10 32-bit or 64-bit
		Windows Server 2008 R2 32-bit or 64-bit
		Windows Server 2012 64-bit
kvm_client_ubuntu.zip	Ubuntu	Ubuntu 14.04 LTS
		Ubuntu 16.04 LTS
kvm_client_mac.zip	Mac OS	Mac OS X El Capitan
kvm_client_linux.zip	Red Hat	Red Hat Enterprise Linux 6.9
		Red Hat Enterprise Linux 7.3

7.2 Logging In to a Server Using the Independent Remote Console (Windows)

Scenarios

Use the independent remote console to remotely access a server from a client running Windows.

Prerequisites

Conditions

The client (for example, a PC) is connected to the iBMC management network port of the server to be accessed.

Data

- iBMC management network port IP address and port number
- User name and password for logging in to the iBMC

Software

You have downloaded the independent remote console software package to the client (PC) and decompressed it.

Procedure

Step 1 Configure an IP address for the client (PC) to enable communication between the client and the iBMC. That is, the IP address configured and the iBMC management network port IP address must be in the same network segment.

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

The independent remote console interface is displayed, as shown in **Figure 7-2**.

Figure 7-2 Login interface

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

The network address can be in any of the following formats:

- iBMC [*IPv6 address*]:*Port number* or iBMC *IPv4 address*:*Port number*

  For example, **[fc00::64]:444** or **192.168.100.1:444**

- iBMC *domain name address*:*Port number*

  ☐ NOTE

  - The iBMC versions earlier than V228 only support logins of local users. The iBMC V228 and later versions support logins of local and LDAP domain users.

  - For the versions earlier than iBMC V228, *Port number* indicates the RMCP+ service port number. For iBMC V228 and later versions, *Port number* indicates the HTTPS service port number.

  - The IPv6 address must be included in square brackets ([ ]), for example, **[fc00::64]:444**. Do not include the IPv4 address, for example, **192.168.100.1:444**.

  - If the default port number is used, you do not need to enter the port number.

Step 4 Select the login mode, and click **Connect**.

- **Shared Mode**: allows two users to access and manage a server at the same time. The two users can see each other's operations.

- **Private Mode**: allows only one user to access and manage a server.

Information shown in **Figure 7-3** is displayed.

Figure 7-3 Security warning
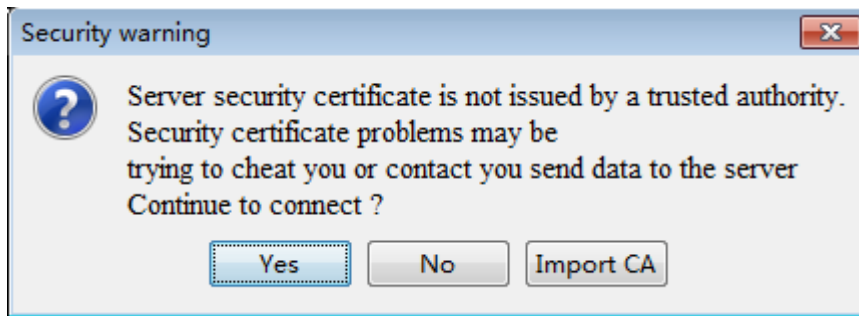
☐ **NOTE**

> If no CA certificate is installed, click **Import CA** to import a CA certificate (***.cer**, ***.crt**, or ***.pem**). After the CA certificate is imported, the security risk dialog box will no longer be displayed.

Step 5 Click **Yes** to open the remote console.

The Remote Virtual Console of the server is displayed, as shown in **Figure 7-4**.

Figure 7-4 Remote Virtual Console
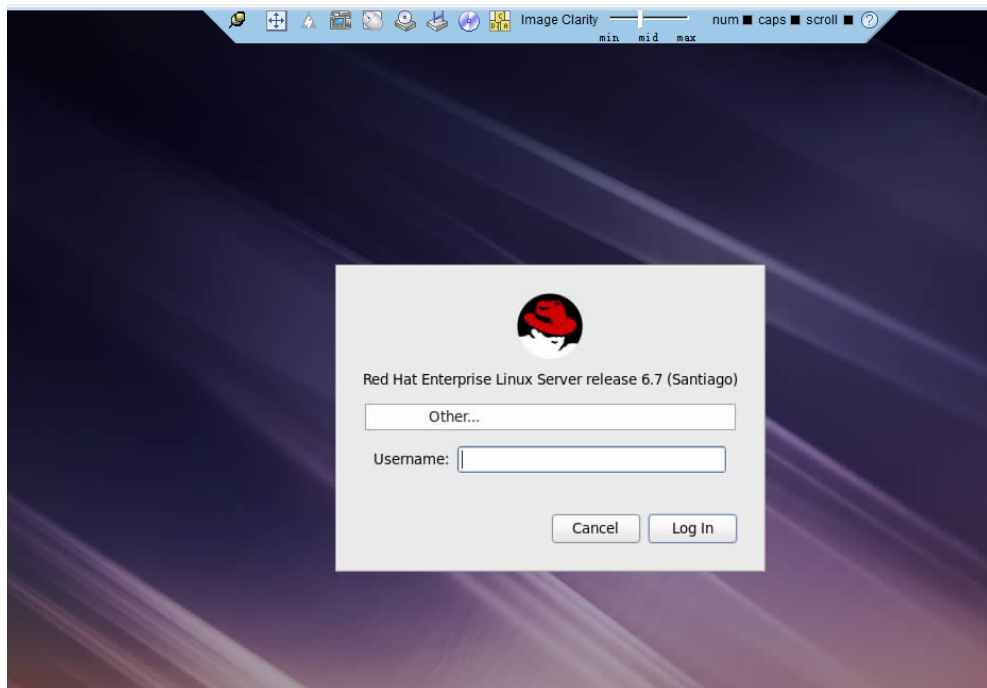
----End

7.3 Logging In to a Server Using the Independent Remote Console (Ubuntu)

Scenarios

Use the independent remote console IRC to remotely access a server from a client running Ubuntu.

Prerequisites

Conditions

- The client (for example, a PC) is connected to the iBMC management network port of the server to be accessed.
- The ipmitool later than 1.8.14 has been installed.

Data

- iBMC management network port IP address and port number
- User name and password for logging in to the iBMC

Software

You have downloaded the independent remote console software package to the client (PC) and decompressed it.

Procedure

Step 1 Configure an IP address for the client (PC) to enable communication between the client and the iBMC. That is, the IP address configured and the iBMC management network port IP address must be in the same network segment.

Step 2 Open the console and specify the folder in which the IRC is stored as the working folder.

Step 3 Run the **chmod 777 KVM.sh** command to set the permission for the independent remote console.

Step 4 Run **./KVM.sh** to start the independent remote console.

A dialog box similar to the one shown in **Figure 7-5** is displayed.

Figure 7-5 Login interface

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

The network address can be in any of the following formats:

- iBMC [*IPv6 address*]:*Port number* or iBMC *IPv4 address*:*Port number*

  For example, **[fc00::64]:444** or **192.168.100.1:444**

- iBMC *domain name address*:*Port number*

  📖 **NOTE**

  - The iBMC versions earlier than V228 only support logins of local users. The iBMC V228 and later versions support logins of local and LDAP domain users.
  - For the versions earlier than iBMC V228, *Port number* indicates the RMCP+ service port number. For iBMC V228 and later versions, *Port number* indicates the HTTPS service port number.
  - The IPv6 address must be included in square brackets ([ ]), for example, **[fc00::64]:444**. Do not include the IPv4 address, for example, **192.168.100.1:444**.
  - If the default port number is used, you do not need to enter the port number.

Step 6 Select the login mode, and click **Connect**.

- **Shared Mode**: allows two users to access and manage a server at the same time. The two users can see each other's operations.

- **Private Mode**: allows only one user to access and manage a server.

Information shown in **Figure 7-6** is displayed.

Figure 7-6 Security warning
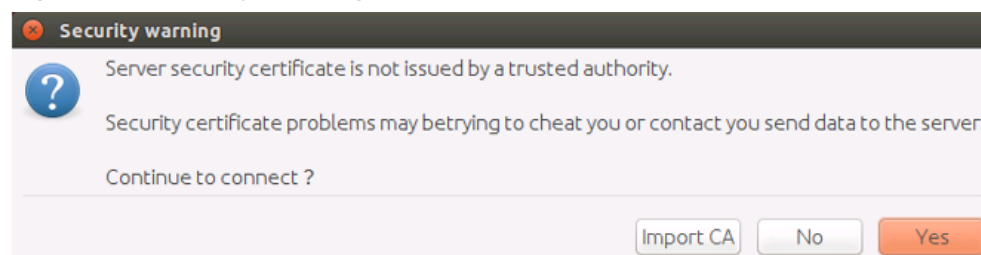
📖 **NOTE**

> If no CA certificate is installed, click **Import CA** to import a CA certificate (***.cer**, ***.crt**, or ***.pem**). After the CA certificate is imported, the security risk dialog box will no longer be displayed.

Step 7 Click **Yes** to open the remote console.

The Remote Virtual Console of the server is displayed, as shown in **Figure 7-7**.

Figure 7-7 Remote Virtual Console
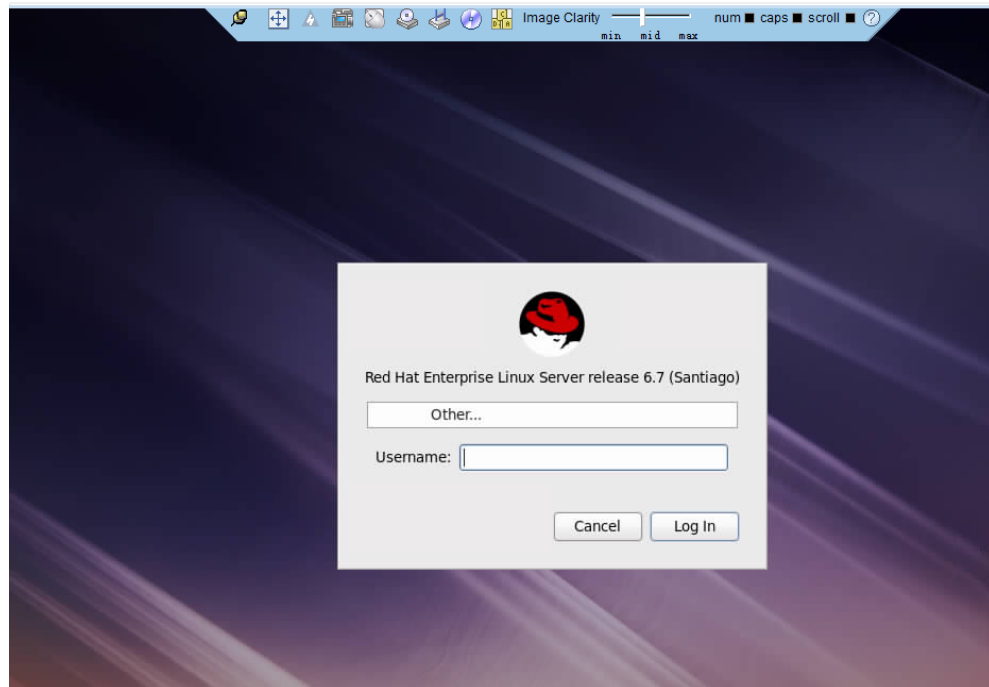
----End

7.4 Logging In to a Server Using the Independent Remote Console (macOS)

Scenarios

Use the independent remote console to remotely access a server from a client running macOS.

Prerequisites

Conditions

- The client (for example, a PC) is connected to the iBMC management network port of the server to be accessed.
- The ipmitool later than 1.8.14 has been installed.

Data

- iBMC management network port IP address and port number
- User name and password for logging in to the iBMC

Software

You have downloaded the independent remote console software package to the client (PC) and decompressed it.

Procedure

Step 1 Configure an IP address for the client (PC) to enable communication between the client and the iBMC. That is, the IP address configured and the iBMC management network port IP address must be in the same network segment.

Step 2 Open the console and specify the folder in which the IRC is stored as the working folder.

Step 3 Run the **chmod 777 KVM.sh** command to set the permission for the independent remote console.

Step 4 Run **./KVM.sh** to start the independent remote console.

A dialog box similar to the one shown in **Figure 7-8** is displayed.

Figure 7-8 Login interface

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

The network address can be in any of the following formats:

- iBMC [*IPv6 address*]:*Port number* or iBMC *IPv4 address:Port number*
  For example, **[fc00::64]:444** or **192.168.100.1:444**
- iBMC *domain name address:Port number*

- The iBMC versions earlier than V228 only support logins of local users. The iBMC V228 and later versions support logins of local and LDAP domain users.
- For the versions earlier than iBMC V228, *Port number* indicates the RMCP+ service port number. For iBMC V228 and later versions, *Port number* indicates the HTTPS service port number.
- The IPv6 address must be included in square brackets ([ ]), for example, **[fc00::64]:444**. Do not include the IPv4 address, for example, **192.168.100.1:444**.
- If the default port number is used, you do not need to enter the port number.

Step 6 Select the login mode, and click **Connect**.

- **Shared Mode**: allows two users to access and manage a server at the same time. The two users can see each other's operations.
- **Private Mode**: allows only one user to access and manage a server.

Information shown in **Figure 7-9** is displayed.

Figure 7-9 Security warning

📖 **NOTE**

If no CA certificate is installed, click **Import CA** to import a CA certificate (***.cer**, ***.crt**, or ***.pem**). After the CA certificate is imported, the security risk dialog box will no longer be displayed.

Step 7 Click **Yes** to open the remote console.

The Remote Virtual Console of the server is displayed, as shown in **Figure 7-10**.

Figure 7-10 Remote Virtual Console
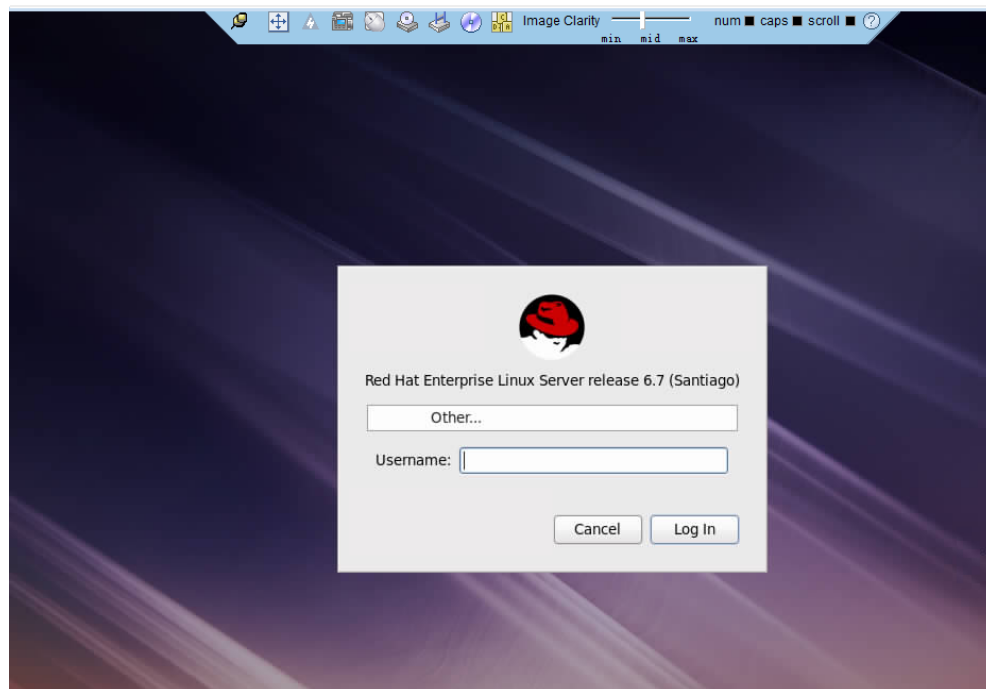
----**End**

7.5 Logging In to a Server Using the Independent Remote Console (Red Hat)

Scenarios

Use the independent remote console to remotely access a server from a client running Red Hat.

Prerequisites

Conditions

- The client (for example, a PC) is connected to the iBMC management network port of the server to be accessed.
- The ipmitool later than 1.8.14 has been installed.

Data

- iBMC management network port IP address and port number
- User name and password for logging in to the iBMC

Software

You have downloaded the independent remote console software package to the client (PC) and decompressed it.

Procedure

Step 1 Configure an IP address for the client (PC) to enable communication between the client and the iBMC. That is, the IP address configured and the iBMC management network port IP address must be in the same network segment.

Step 2 Open the console and specify the folder in which the IRC is stored as the working folder.

Step 3 Run the **chmod 777 KVM.sh** command to set the permission for the independent remote console.

Step 4 Run **./KVM.sh** to start the independent remote console.

A dialog box similar to the one shown in **Figure 7-11** is displayed.

Figure 7-11 Login interface

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

The network address can be in any of the following formats:

- iBMC [*IPv6 address*]:*Port number* or iBMC *IPv4 address:Port number*
  For example, **[fc00::64]:444** or **192.168.100.1:444**

- iBMC *domain name address:Port number*

☐ **NOTE**

- The iBMC versions earlier than V228 only support logins of local users. The iBMC V228 and later versions support logins of local and LDAP domain users.

- For the versions earlier than iBMC V228, *Port number* indicates the RMCP+ service port number. For iBMC V228 and later versions, *Port number* indicates the HTTPS service port number.

- The IPv6 address must be included in square brackets ([ ]), for example, **[fc00::64]:444**. Do not include the IPv4 address, for example, **192.168.100.1:444**.

- If the default port number is used, you do not need to enter the port number.

Step 6 Select the login mode, and click **Connect**.

- **Shared Mode**: allows two users to access and manage a server at the same time. The two users can see each other's operations.

● **Private Mode**: allows only one user to access and manage a server.

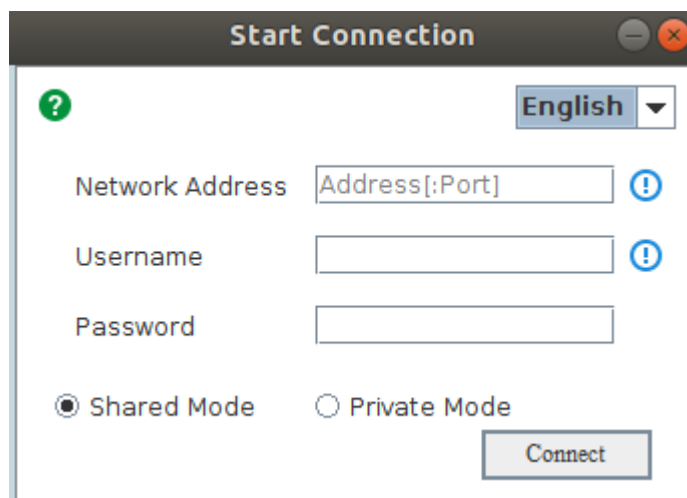Information shown in **Figure 7-12** is displayed.

Figure 7-12 Security warning
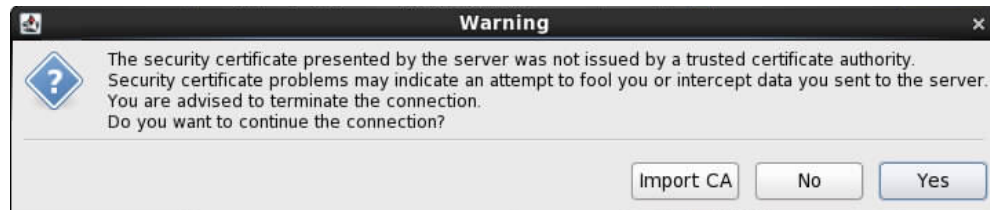
📖 **NOTE**

If no CA certificate is installed, click **Import CA** to import a CA certificate (***.cer**, ***.crt**, or ***.pem**). After the CA certificate is imported, the security risk dialog box will no longer be displayed.

Step 7 Click **Yes** to open the remote console.

The Remote Virtual Console of the server is displayed, as shown in **Figure 7-13**.

Figure 7-13 Remote Virtual Console
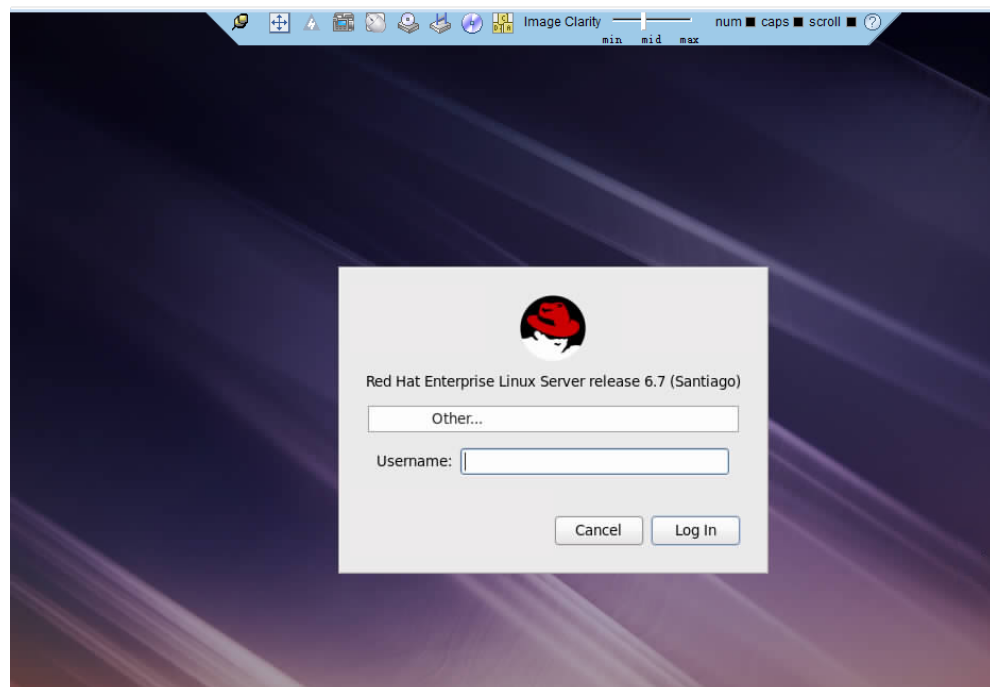
----End

8 Smart Provisioning

8.1 Overview

Smart Provisioning provides functions, such as OS installation, RAID configuration, and firmware updates. Only V5 servers, iBMC 2.64 or later versions, and BIOS 0.37 or later versions support Smart Provisioning.

Figure 8-1 shows the architecture of Smart Provisioning.

Figure 8-1 Smart Provisioning architecture
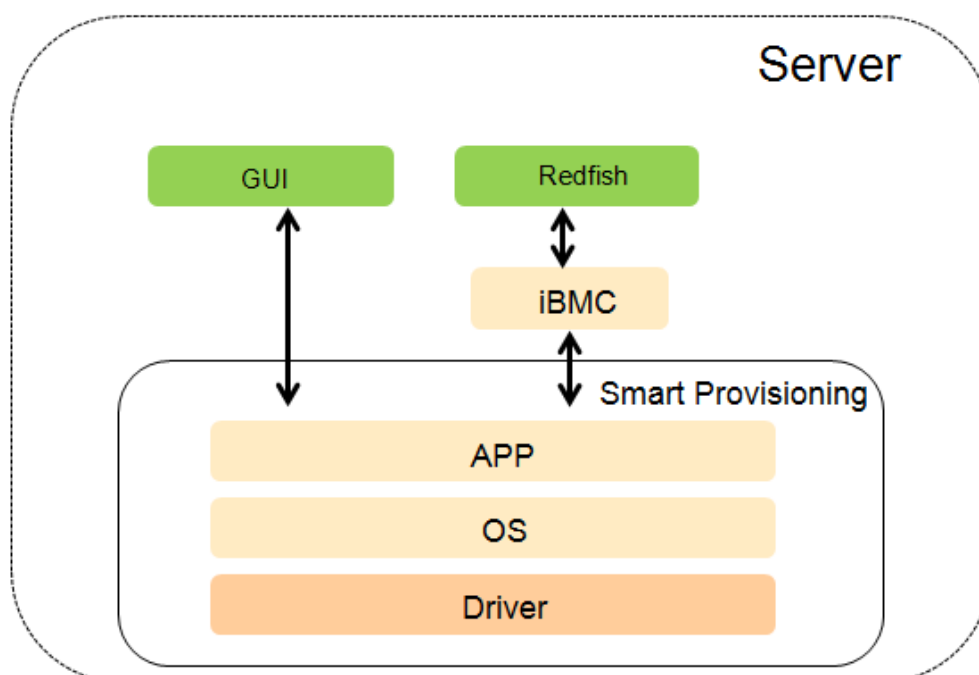
Smart Provisioning provides a GUI for single-server operation and the Redfish interface for batch operation.

Table 8-1 lists the functions provided by Smart Provisioning.

Table 8-1 Functions

Function	Description
OS installation	Supports installation of mainstream OSs, including Windows, Red Hat Enterprise Linux (RHEL), CentOS, SUSE Linux Enterprise Server (SLES), and VMware ESXi, in UEFI and Legacy modes. For details about the OSs supported, see **Table 8-2**.
RAID configuration	Smart Provisioning supports the configuration of the Avago SAS3008, Avago SAS3108, Avago SAS3004, Avago SAS3408, Avago SAS3508, and Avago SAS3416iMR RAID controller cards.
Firmware update	Supports updates of the following firmware: ● PCIe devices include firmware of RAID controller cards and NICs (mainstream Huawei-developed cards and standard cards). ● Hard disk (SAS and SATA) firmware ● Smart Provisioning

Table 8-2 Supported OSs

OS	Version
Windows	Windows Server 2012 R2, Windows Server 2016
RHEL	RHEL 6.9, RHEL 7.3, RHEL 7.4
CentOS	CentOS 6.9, CentOS 7.3, CentOS 7.4
SLES	SLES 12.2
VMware ESXi	VMware ESXi 6.5

8.2 Login Procedure

8.2.1 Logging In to the Smart Provisioning GUI

Scenarios

Log in to the Smart Provisioning GUI through the iBMC WebUI when you want to use Smart Provisioning to install OS, configure RAID, or upgrade firmware.

📖 **NOTE**

- Do not restart the iBMC during the SP startup process.
- If the iBMC is reset after SP is started, you need to log in to SP again.

Prerequisites

Conditions

You have logged in to the iBMC WebUI.

Data

None

Hardware

None

Procedure

Step 1 Choose **Remote Console** on the iBMC WebUI.

Step 2 Click **Java Integrated Remote Console** or **HTML5 Integrated Remote Console** to open the remote console.

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

- **Shared Mode**: allows two users to access and manage the server at the same time. The two users can see each other's operations.

This section uses the **Java Integrated Remote Console** as an example.

Step 3 Click 🔺 on the toolbar, and select **Forced System Reset** or **Forced Power Cycle** to restart the OS.

Step 4 During the startup process, press **F6** when the screen shown in **Figure 8-2** is displayed.

Figure 8-2 Startup screen
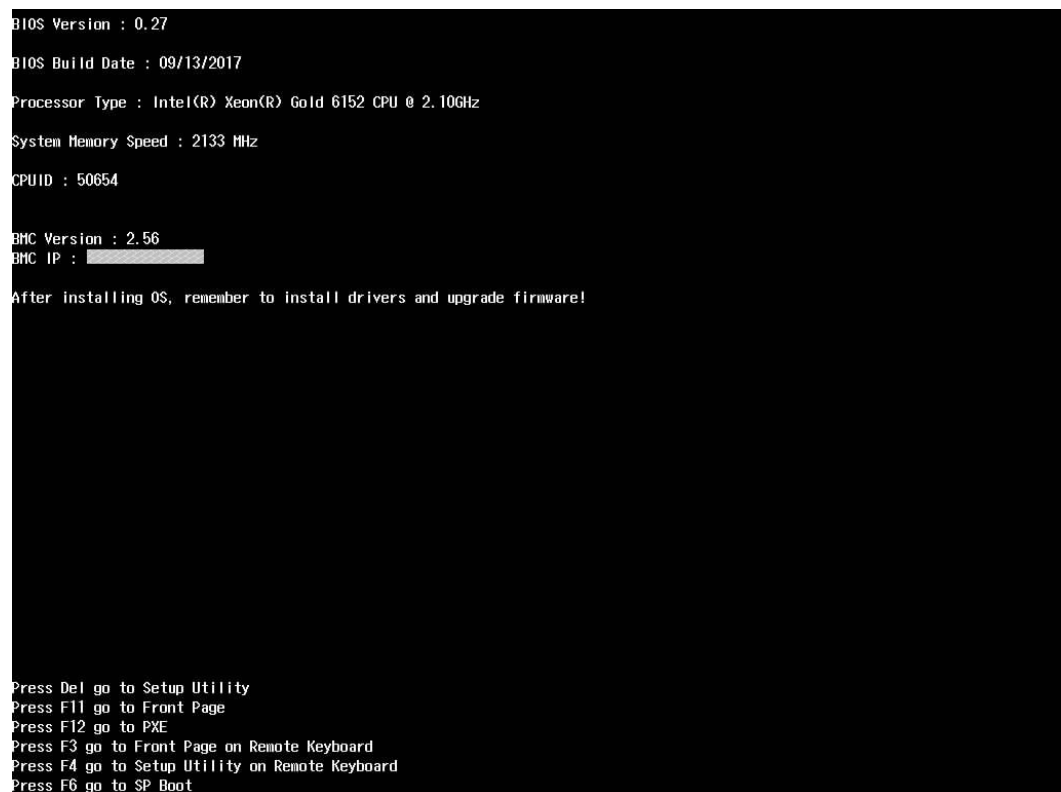
Step 5 If a dialog box prompting you to enter a password is displayed during the startup process, enter a password and press **Enter**.

The default password is **Admin@9000**.

The dialog box shown in **Figure 8-3** is displayed.

Figure 8-3 Confirm
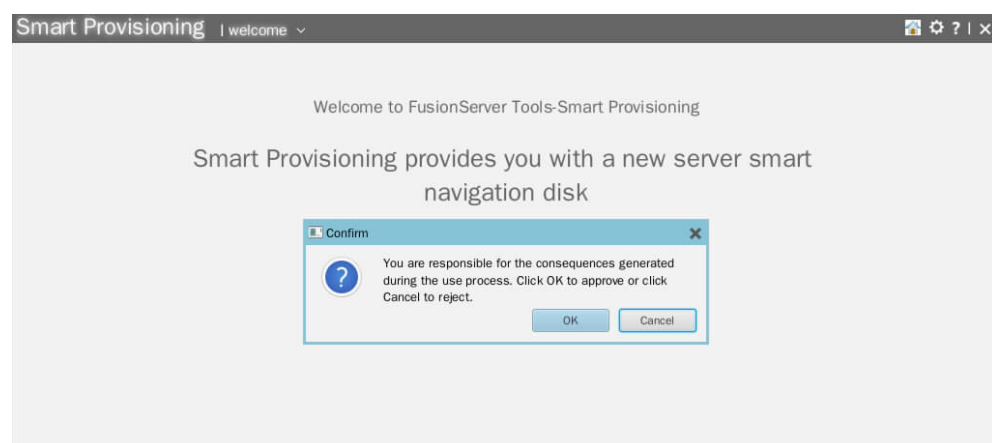
Step 6 Click **OK**.

The Smart Provisioning welcome window is displayed, as shown in **Figure 8-4**.

Figure 8-4 Smart Provisioning welcome window
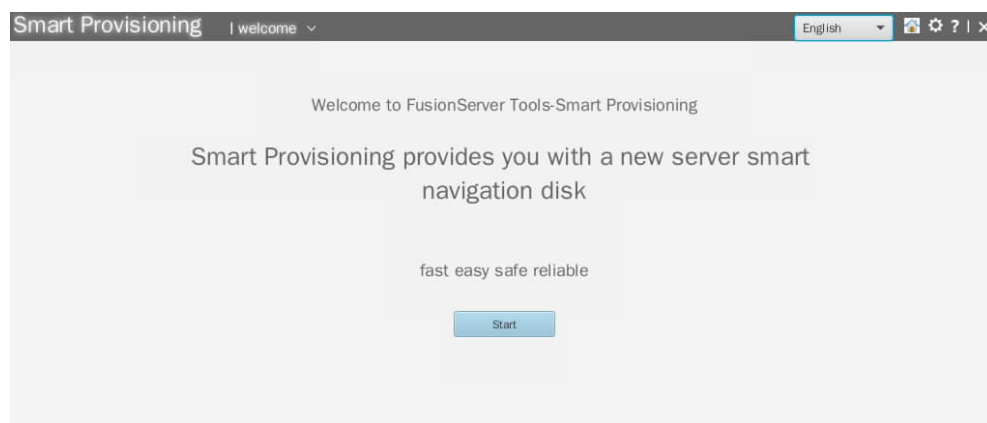
Step 7 Click **Start**.

The Smart Provisioning home page is displayed, as shown in **Figure 8-5**.

Figure 8-5 Smart Provisioning home page
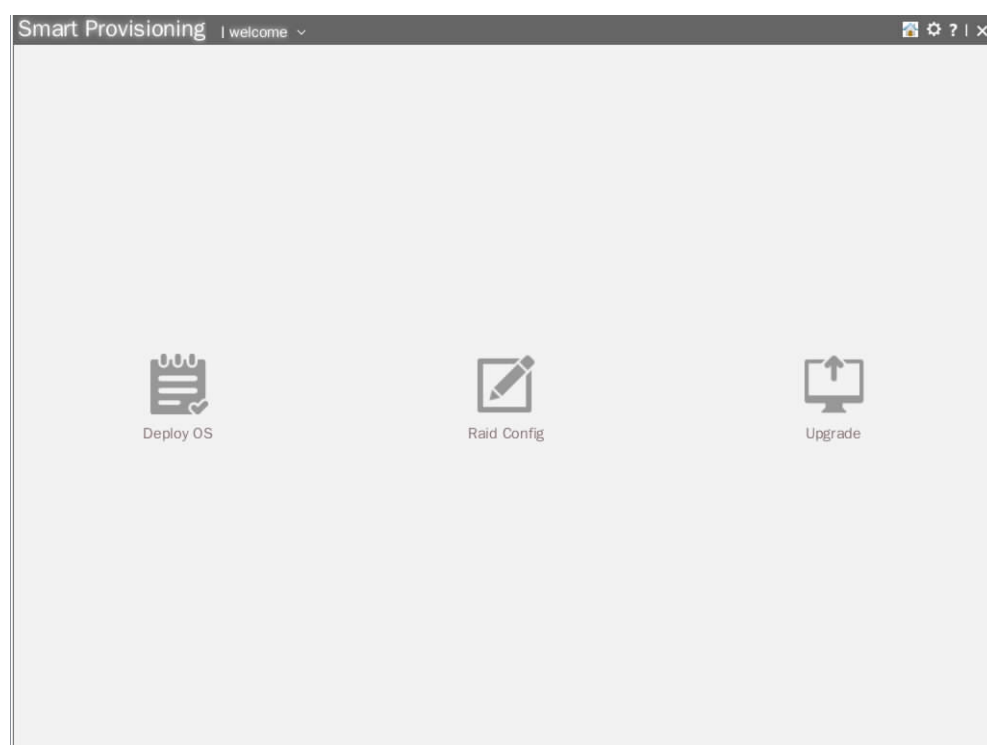
📖 **NOTE**

To return to the home page of Smart Provisioning, click 🏠 in the upper right corner.

----End

8.2.2 Logging In to the Smart Provisioning Redfish Interface

Scenarios

Log in to the Redfish interface when you want to use Smart Provisioning through the Redfish interface.

This section uses the Google Chrome Postman extension program as an example to describe how to log in to the Smart Provisioning Redfish interface.

> 📖 **NOTE**
>
> - Do not restart the iBMC during the SP startup process.
> - If the iBMC is reset after SP is started, you need to log in to SP again.

Prerequisites

Conditions

- The client (for example, local PC) is connected to the iBMC management network port.
- Postman has been installed on the client that uses the Google Chrome browser.

> 📖 **NOTE**

For details about how to install Postman, see the iBMC Redfish API description.

Data

- IP address of the iBMC management network port
- iBMC user name and password

Procedure

Step 1 Run Postman.

Step 2 Create a session.

1. Choose **POST** from the menu, as shown in **Figure 8-6**.

2. Enter **https://*.*.*.*/redfish/v1/SessionService/Sessions** in the parameter text box.

   ..*.* indicates the iBMC management network port IP address.

Figure 8-6 Setting parameters for creating a session
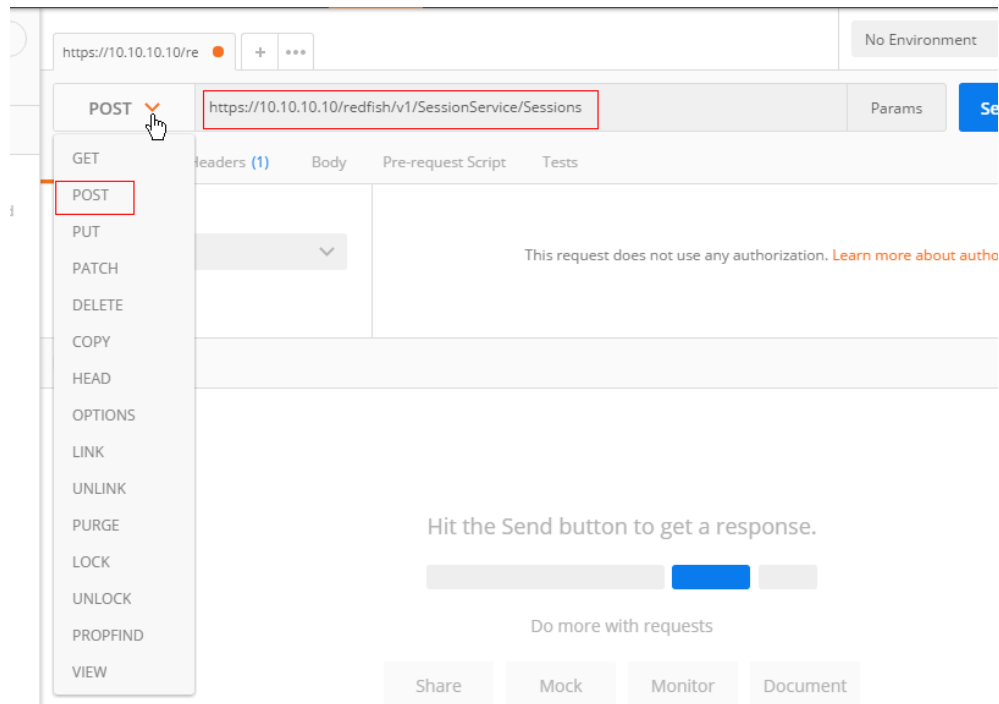
3. Click the **Body** tab, select **raw**, and choose **JSON (application/json)** from the **Text** drop-down list, as shown in **Figure 8-7**.

Figure 8-7 Setting parameters for creating a session
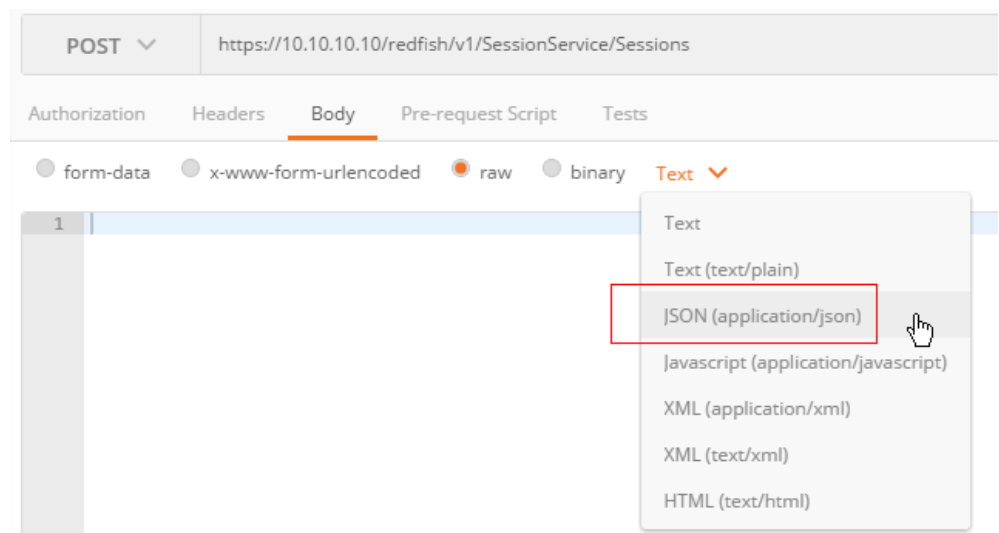
4. In the text box on the **Body** tab, enter the request body.

```
{
    "UserName": "username",
    "Password": "password"
}
```

In the request body, *username* indicates the iBMC user name, and *password* indicates the password. **Figure 8-8** shows an example.

Figure 8-8 Setting parameters for creating a session
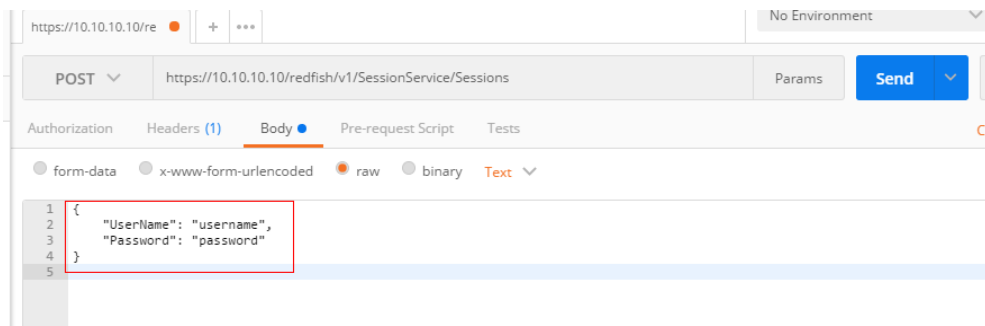
5. Click **Send**.

   If the response code obtained in the **Response** area is **201**, the session is established.

   Record the value of **X-Auth-Token** in the response message for subsequent operations.

Step 3 Perform operations on Smart Provisioning.

1. Select **Get** from the menu.

2. Enter **https://*.*.*.*/redfish/v1/Managers/1/SPService** in the parameter text box.

   ..*.* indicates the iBMC management network port IP address.

3. On the **Headers** tab, add the **X-Auth-Token** parameter and its value (obtained in **Step 2.5**), as shown in **Figure 8-9**.

Figure 8-9 Setting parameters for obtaining Smart Provisioning resources
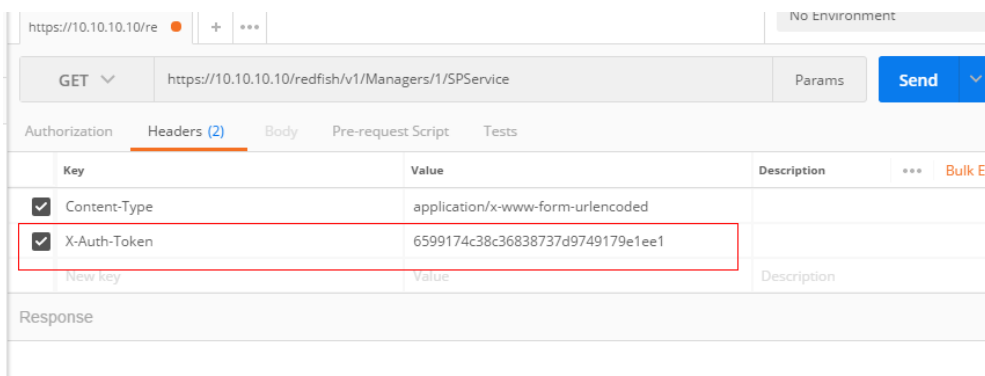
4. Click **Send**.

   If the returned response code is **200**, the operation is successful.

In the **Response** window, you can see the Smart Provisioning resources supported by the server.

----End

8.3 Operations

For details about Smart Provisioning operations, see:

- GUI: *FusionServer Tools Smart Provisioning User Guide*
- Redfish interface: *iBMC Redfish API Description*

9 Configuration File Description

Table 9-1, **Table 9-2**, and **Table 9-3** describe the parameters in iBMC, BIOS, and RAID controller card configuration files.

To ensure data security, some of the iBMC and RAID controller configuration in the configuration file imported after the mainboard replacement do not take effect.

The iBMC configuration, BIOS configuration, and some RAID controller configuration can be imported and exported.

Table 9-1 iBMC parameters

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
Local user	User	UserName	Specifies the name of a user.	Yes
	User	PassWord	Specifies the password of a user.	No Sensitive information is displayed in ciphertext in the configuration file and does not take effect after the configuration file is imported.
	User	Privilege	Specifies the rights of a user.	Yes
	User	UserRoleId	Specifies the role of a user.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	User	PermitRuleIds	Specifies the login rules for a user.	Yes
	User	LoginInterfac e	Specifies the login interface for a user.	Yes
	User	IsUserEnable	Specifies whether the user is enabled.	No The value is displayed in the configuration file.
	User	IsUserLocked	Specifies whether the user is locked.	No The value is displayed in the configuration file.
	UserRole	KVMMgnt	Specifies the KVM rights.	Yes
	UserRole	UserMgnt	Specifies the user management rights.	Yes
	UserRole	VMMMgnt	Specifies the VMM rights.	Yes
	UserRole	BasicSetting	Specifies the rights for performing basic settings.	Yes
	UserRole	ReadOnly	Specifies the read-only rights.	Yes
	UserRole	PowerMgnt	Specifies the power control rights.	Yes
	UserRole	DiagnoseMgn t	Specifies the debugging and diagnosis rights.	Yes
	UserRole	ConfigureSelf	Specifies the rights for configuring the user's own data.	Yes
	UserRole	SecurityMgnt	Specifies the security configuration rights.	Yes
Tw o-fact or aut hen	MutualAut hentication	MutualAuthe nticationState	Specifies whether two-factor authentication is enabled.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
tica tion	MutualAut hentication	MutualAuthe nticationOCS P	Specifies whether the two-factor authentication revocation check is enabled.	Yes
LD AP conf igur atio n	LDAP	Enable	Specifies whether LDAP is enabled.	Yes
	LDAP	CertStatus	Specifies whether LDAP certificate verification is enabled.	Yes
	LDAP	HostAddr	Specifies the LDAP server address.	Yes
	LDAP	Port	Specifies the LDAPS port number.	Yes
	LDAP	UserDomain	Specifies the domain name.	Yes
	LDAP	Folder	Specifies the folder for which user applications are stored.	Yes
	LDAP	BindDN	Specifies the distinguished name of an LDAP proxy user.	Yes
	LDAP	BindDNPsw	Specifies the password of the LDAP proxy user.	No The value is displayed in the configuration file.
	LDAPServer	Enable	Specifies whether LDAP is enabled.	Yes
	LDAPServer	CertStatus	Specifies whether LDAP certificate verification is enabled.	Yes
	LDAPServer	HostAddr	Specifies the LDAP server address.	Yes
	LDAPServer	Port	Specifies the LDAPS port number.	Yes
	LDAPServer	UserDomain	Specifies the domain name.	Yes

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
	LDAPServer	Folder	Specifies the user application folder.	Yes
	LDAPServer	BindDN	Specifies the distinguished name of an LDAP proxy user.	Yes
	LDAPServer	BindDNPsw	Specifies the user password.	No The value is displayed in the configuration file.
	LDAPGroup	GroupName	Specifies the LDAP group name.	Yes
	LDAPGroup	GroupFolder	Specifies the application folder for an LDAP group.	Yes
	LDAPGroup	GroupPermitRuleIds	Specifies the login rules for an LDAP group.	Yes
	LDAPGroup	GroupLoginInterface	Specifies the login interface for an LDAP group.	Yes
	LDAPGroup	GroupPrivilege	Specifies the rights of an LDAP group.	Yes
Security hardening	PasswdSetting	EnableStrongPassword	Specifies whether password complexity check is enabled.	Yes
	SecurityEnhance	SSHPasswordAuthentication	Specifies whether SSH password authentication is enabled.	Yes
	SecurityEnhance	UserInactTimeLimit	Specifies the time limit for which a user is inactive.	Yes
	SecurityEnhance	PwdExpiredTime	Specifies the validity period of a password.	Yes
	SecurityEnhance	MinimumPwdAge	Specifies the minimum validity period of a password.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	SecurityEnh ance	InitialPwdPro mpt	Specifies whether to enable the function of prompting the user to change the password.	Yes
	SecurityEnh ance	ExcludeUser	Specifies the user who can log in to the system in emergencies.	Yes
	SecurityEnh ance	OldPwdCount	Specifies the previous password that cannot be used.	Yes
	SecurityEnh ance	AuthFailMax	Specifies the maximum number of failed login attempts allowed before a user account is locked.	Yes
	SecurityEnh ance	AuthFailLockT ime	Specifies the user lockout period.	Yes
	PermitRule	TimeRuleInfo	Specifies the rules for time-based logins.	Yes
	PermitRule	IpRuleInfo	Specifies the rules for IP-based logins.	Yes
	PermitRule	MacRuleInfo	Specifies the rules for MAC-based logins.	Yes
	SecurityEnh ance	PermitRuleIds	Specifies whether rules are enabled.	Yes
	SecurityEnh ance	BannerState	Specifies whether login security information configuration is enabled.	Yes
	SecurityEnh ance	BannerConte nt	Provides the login security information.	Yes
Net wor k conf igur atio n	BMC	HostName	Specifies the iBMC host name.	No The value is displayed in the configuration file.
	EthGroup	NetMode	Specifies the network port mode.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	EthGroup	ActivePort	Specifies the management network port.	Yes
	EthGroup	IpVersion	Specifies whether IP is enabled.	Yes
	EthGroup	IpMode	Specifies how IPv4 addresses are assigned.	Yes
	EthGroup	IpAddr	Specifies an IPv4 address.	No The value is displayed in the configuration file.
	EthGroup	SubnetMask	Specifies an IPv4 subnet mask.	No The value is displayed in the configuration file.
	EthGroup	DefaultGatew ay	Specifies the default IPv4 gateway IP address.	No The value is displayed in the configuration file.
	EthGroup	Ipv6Mode	Specifies how IPv6 addresses are allocated.	Yes
	EthGroup	Ipv6Addr	Specifies an IPv6 address.	No The value is displayed in the configuration file.
	EthGroup	Ipv6Prefix	Specifies the prefix length of an IPv6 address.	No The value is displayed in the configuration file.
	EthGroup	Ipv6DefaultG ateway	Specifies the default IPv6 gateway IP address.	No The value is displayed in the configuration file.
	DNSSetting	IPVer	Specifies the IP version bound with the DNS.	Yes
	DNSSetting	Mode	Specifies how the DNS addresses are assigned.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	DNSSetting	PrimaryDoma in	Specifies the preferred DNS server.	Yes
	DNSSetting	BackupDomai n	Specifies the alternate DNS server.	Yes
	DNSSetting	DomainName	Specifies the DNS domain name.	Yes
	EthGroup	VlanState	Specifies whether VLAN is enabled.	Yes
	EthGroup	VlanID	Specifies the VLAN ID.	Yes
	NTP	EnableStatus	Specifies whether NTP is enabled.	Yes
	NTP	Mode	Specifies the NTP mode.	Yes
	NTP	PreferredServ er	Specifies the address of the preferred NTP server.	Yes
	NTP	AlternativeSer ver	Specifies the address of the alternate NTP server.	Yes
	NTP	AuthEnableSt atus	Specifies whether NTP server authentication is enabled.	Yes
	NTP	MinPollInterv al	Specifies the minimum NTP synchronization interval.	Yes
	NTP	MaxPollInterv al	Specifies the maximum NTP synchronization interval.	Yes
	VNC	EnableState	Specifies whether VNC is enabled.	Yes

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
	VNC	Password	Specifies the VNC password.	No Sensitive information is displayed in ciphertext in the configuration file and does not take effect after the configuration file is imported.
	VNC	Timeout	Specifies the validity period of the VNC password.	Yes
	VNC	SSLEnableSta te	Specifies whether the SSL is enabled.	Yes
	VNC	Port	Specifies the VNC service port number.	Yes
	VNC	KeyboardLayo ut	Specifies the keyboard layout.	Yes
	VNC	PermitRuleIds	Specifies the login rules.	Yes
	BMC	TimeZoneStr	Specifies the time zone.	Yes
Service configuration	SSH	State	Specifies whether SSH is enabled.	Yes
	SSH	Port	Specifies the SSH port number.	Yes
	Snmp	State	Specifies whether SNMP Agent is enabled.	Yes
	Snmp	PortID	Specifies the SNMP Agent.	Yes
	Kvm	State	Specifies whether KVM is enabled.	Yes
	Kvm	Port	Specifies the KVM port number.	Yes
	Vmm	State	Specifies whether VMM is enabled.	Yes

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
	Vmm	Port	Specifies the VMM port number.	Yes
	Video	State	Specifies whether Video is enabled.	Yes
	Video	Port	Specifies the Video port number.	Yes
	WEBHTTP	State	Specifies whether HTTP is enabled.	Yes
	WEBHTTP	Port	Specifies the HTTP port number.	Yes
	WEBHTTPS	State	Specifies whether HTTPS is enabled.	Yes
	WEBHTTPS	Port	Specifies the HTTPS port number.	Yes
	RmcpConfig	LanState	Specifies whether IPMI LAN (RMCP) is enabled.	Yes
	RmcpConfig	Port1	Specifies the IPMI LAN (RMCP) port 1.	Yes
	RmcpConfig	Port2	Specifies the IPMI LAN (RMCP) port 2.	Yes
	RmcpConfig	LanPlusState	Specifies whether IPMI LAN (RMCP+) is enabled.	Yes
System configuration	Snmp	V1State	Specifies whether SNMPv1 is supported.	Yes
	Snmp	V2CState	Specifies whether SNMPv2c is supported.	Yes
	Snmp	LongPasswordEnable	Specifies whether long passwords are enabled.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
Snmp	ROCommunit y	Specifies the read-only community string.	No Sensitive information is displayed in ciphertext in the configuration file and does not take effect after the configuration file is imported.
Snmp	RWCommunit y	Specifies the read-write community string.	No Sensitive information is displayed in ciphertext in the configuration file and does not take effect after the configuration file is imported.
Snmp	RWCommunit yState	Specifies whether the read/write community name is enabled.	Yes
Snmp	SNMPV1V2CP ermitRuleIds	Specifies the SNMP login rules.	Yes
Snmp	AuthProtocol	Specifies the SNMPv3 authentication algorithm.	Yes
Snmp	PrivProtocol	Specifies the SNMPv3 encryption algorithm.	Yes
SecurityEnh ance	TLSVersion	Specifies the TLS version.	Yes
SecurityEnh ance	EnableUserM gnt	Specifies whether user management on the service side is enabled.	Yes
Session	Timeout	Specifies the timeout period for a web session.	Yes
Session	Mode	Specifies the web session mode.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	BMC	LocationInfo	Specifies the equipment location.	No The value is displayed in the configuration file.
	MeInfo	CpuUtiliseThr e	Specifies the CPU usage alarm threshold.	Yes
	MeInfo	MemUtiliseTh re	Specifies the memory usage alarm threshold.	Yes
	MeInfo	DiskPartition UsageThre	Specifies the hard disk partition usage alarm threshold.	Yes
	Partition	RAIDMode	Specifies the RAID working mode (RH8100 only)	Yes
	PRODUCT	WOLState	Specifies whether Wake on LAN (WOL) is enabled.	Yes
Syst em boo t opti on	Bios	StartOption	Specifies the first boot device.	Yes
	Bios	StartOptionFl ag	Specifies whether the boot setting takes effect permanently or just for one time only.	Yes
Ala rm sett ings	SyslogConfi g	EnableState	Specifies whether Syslog is enabled.	Yes
	SyslogConfi g	MsgIdentity	Identifies the Syslog host.	Yes
	SyslogConfi g	MsgSeverity	Specifies Syslog alarm severity level.	Yes
	SyslogConfi g	NetProtocol	Specifies the Syslog transmission protocol.	Yes
	SyslogConfi g	AuthType	Specifies the Syslog authentication mode.	Yes
	SyslogItem Cfg	EnableState	Specifies whether the Syslog server is enabled.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	SyslogItem Cfg	DestAddr	Specifies the Syslog server address.	Yes
	SyslogItem Cfg	DestPort	Specifies the Syslog server port number.	Yes
	SyslogItem Cfg	LogSrcMask	Specifies the Syslog log type.	Yes
	TrapConfig	TrapEnable	Specifies whether Trap is enabled.	Yes
	TrapConfig	TrapVersion	Specifies the Trap version.	Yes
	TrapConfig	Trapv3Userid	Specifies the SNMPv3 user name.	Yes
	TrapConfig	TrapMode	Specifies Trap mode.	Yes
	TrapConfig	TrapIdentity	Identifies the Trap host.	Yes
	TrapConfig	CommunityN ame	Specifies the Trap community name.	No Sensitive information is displayed in ciphertext in the configuration file and does not take effect after the configuration file is imported.
	TrapConfig	SendSeverity	Specifies the severity level for sending a Trap alarm.	Yes
	TrapItemCf g	ItemEnable	Specifies whether the Trap server is enabled.	Yes
	TrapItemCf g	DestIpAddr	Specifies the Trap server address.	Yes
	TrapItemCf g	DestIpPort	Specifies the Trap server port number.	Yes
	TrapItemCf g	Separator	Specifies the delimiter to be used in a message.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	TrapItemCf g	Time	Specifies the message content (time).	Yes
	TrapItemCf g	SensorName	Specifies the message content (sensor name).	Yes
	TrapItemCf g	Severity	Specifies the message content (severity level).	Yes
	TrapItemCf g	EventCode	Specifies the message content (event code).	Yes
	TrapItemCf g	EventDesc	Specifies the message content (event description).	Yes
	TrapItemCf g	ShowKeyWor d	Specifies whether to display the keywords in a message.	Yes
	SmtpConfig	SmtpEnable	Specifies whether SMTP is enabled.	Yes
	SmtpConfig	SmtpServer	Specifies the SMTP address.	Yes
	SmtpConfig	TlsSendMode	Specifies whether TLS is enabled.	Yes
	SmtpConfig	AnonymousM ode	Specifies whether anonymous login is enabled.	Yes
	SmtpConfig	LoginName	Specifies the email sender name.	Yes
	SmtpConfig	LoginPasswd	Specifies the email sender password.	No Sensitive information is displayed in ciphertext in the configuration file and does not take effect after the configuration file is imported.
	SmtpConfig	SenderName	Specifies the mailbox address of the sender.	Yes

Typ e	Exported Parameter	Exported Subparamete r	Description	Valid After Imported via Configuration File
	SmtpConfig	TempletTopic	Specifies the email subject.	Yes
	SmtpConfig	TempletIpadd r	Specifies whether the email subject contains the host name.	Yes
	SmtpConfig	TempletBoard Sn	Specifies whether the email subject contains the board serial number.	Yes
	SmtpConfig	TempletAsset	Specifies whether the email subject contains the product asset tag.	Yes
	SmtpConfig	SendSeverity	Specifies the severity levels of the alarms to be sent.	Yes
	SmtpItemC fg	EmailName	Specifies the recipient address.	Yes
	SmtpItemC fg	EmailDesc	Provides information about the alarm	Yes
	SmtpItemC fg	ItemEnable	Specifies whether alarm email notifications are sent to the recipient.	Yes
Po wer con trol	ChassisPayl oad	PowerOffTim eoutEN	Specifies whether power-off timeout period is enabled.	Yes
	ChassisPayl oad	PowerOffTim eout	Specifies the power-off timeout period.	Yes
	ChassisPayl oad	PwrButtonLoc k	Specifies whether the power button on the server front panel is disabled.	Yes
	ChassisPayl oad	PowerRestore Policy	Specifies the power restore policy when the power supply is connected.	Yes
Po wer	PowerCappi ng	Enable	Specifies whether power capping is enabled.	Yes

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
	PowerCapping	LimitValue	Specifies the power cap value.	Yes
	PowerCapping	FailAction	Specifies whether to forcibly shut down the server if the power capping fails.	Yes
Energy saving settings	SysPower	ExpectedMode	Specifies the power supply working mode.	Yes
	SysPower	ExpectedActive	Specifies the active power supply.	Yes
Remote control	Kvm	EncryptState	Specifies whether KVM encryption is enabled.	Yes
	Vmm	EncryptState	Specifies whether VMM encryption is enabled.	Yes
	Kvm	KeyboardMode	Specifies whether persistent connection of the virtual keyboard and mouse is enabled.	Yes
	Kvm	KvmTimeout	Specifies the remote console timeout period.	Yes
	Kvm	LocalKVMState	Specifies whether local KVM is enabled.	Yes
Video playback	Video	VideoSwitch	Specifies whether video recording is enabled.	Yes
Screenshot	Kvm	ScreenSwitch	Specifies whether last screenshot is enabled.	Yes
Black box	Diagnose	BlackBoxState	Specifies whether black box is enabled.	Yes

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
Serial port data	Diagnose	SolDataState	Specifies whether serial port data is enabled.	Yes
Others	Bios	BiosPrintFlag	Specifies the setting of the BIOS print switch.	Yes
	Cooling	Mode	Specifies the speed adjustment mode of fans.	No The value is displayed in the configuration file.
	Cooling	PowerMode	Specifies the power supply mode.	Yes
	Cooling	Level	Specifies the fan speed level.	No The value is displayed in the configuration file.
	Stateless	Enable	Specifies whether stateless computing is enabled.	Yes
	Stateless	SysManagerID	Specifies the remote management ID. (stateless computing configuration)	Yes
	Stateless	AutoPowerOn	Specifies whether to enable self-control power-on. (stateless computing configuration)	Yes
	Stateless	BroadcastNetSegment	Specifies the broadcast network segment used for automatic discovery. (stateless computing configuration)	Yes
	Stateless	BroadcastPort	Specifies the broadcast port number used for automatic discovery. (stateless computing configuration)	Yes

Type	Exported Parameter	Exported Subparameter	Description	Valid After Imported via Configuration File
Stateless	SysManagerIP	Specifies the IP address of the server that performs power control. (stateless computing configuration)	Yes
Stateless	SysManagerPort	Specifies the port number of the server that performs power control. (stateless computing configuration)	Yes
USBMassStorage	UmsMaxUpdateSpace	Specifies the flag indicating that the component configuration or upgrade package is delivered to the NAND flash memory.	Yes
USBMassStorage	SpConfigFileReady	Specifies the mode for accessing the SP.	Yes
USBMassStorage	SPStartmode	Specifies the interval between the SP operation completion time and the OS reset time.	Yes
USBMassStorage	SysRestartDelay	Specifies the OS restart delay.	Yes

Table 9-2 BIOS parameters

Parameter	Description
ProcessorHyperThreadingDisable	Specifies whether processor hyper-threading is enabled.
ProcessorFlexibleRatioOverrideEnable	Specifies whether the feature of setting the CPU frequency upper limit is enabled. This feature is disabled by default.
ProcessorFlexibleRatio	Specifies the CPU frequency upper limit. By default, it is the nominal CPU frequency.

Parameter	Description
MonitorMwaitEnable	Specifies whether Monitor/Mwait is enabled.
ProcessorVmxEnable	Specifies whether CPU virtualization is enabled.
ProcessorLtsxEnable	Specifies whether Intel TXT is enabled.
MlcStreamerPrefetch-erEnable	Specifies whether hardware prefetcher is enabled. Before processing instructions or data, the CPU prefetches these instructions or data and saves them to the L2 cache. This reduces memory read time, eliminates potential bottlenecks, and therefore improves system performance.
MlcSpatialPrefetcher-Enable	Specifies whether adjacent cache prefetcher is enabled. This feature allows prefetch of the data adjacent to the data to be read. This improves read speed significantly.
DCUStreamerPrefetcherEnable	Specifies whether DCU streamer prefetcher is enabled. This function allows CPU data to be prefetched, which reduces data read time.
DCUIPPrefetcherEnable	Specifies whether DCU IP prefetcher is enabled. This function enables the system to check historical records for the data that must be prefetched, which reduces data read time.
CustomPowerPolicy	Menu for selecting the energy-saving mode. It does not support customization.
PowerSaving	Indicates a customized parameter for Dynamic Energy Management Technology (DEMT), integrates uniBIOS frequency adjustment algorithms developed, and improves energy efficiency.
ProcessorEistEnable	Specifies whether Enhanced Intel SpeedStep® Technology (EIST) is enabled. EIST enables CPU frequency to be dynamically adjusted based on workloads, reducing heat dissipation.
TurboMode	Specifies whether CPU Turbo mode is enabled.
PStateDomain	PStateDomain switch. PStateDomain adjusts frequencies by core or package.
ProcessorCcxEnable	CPU C-state control menu, which controls the power consumption of CPUs in idle state.
TStateEnable	CPU T-state switch. This function is not available because it limits the CPU frequency.
PackageCState	Package C state setting.
C3Enable	CPU C3 state setting switch.
C6Enable	CPU C6 state setting switch.

Parameter	Description
ProcessorC1eEnable	CPU C1e state setting switch.
OSCx	ACPI C2/C3 adjustment
QpiLinkSpeed	QPI LINK Speed
ClusterOnDieEn	Memory Snoop mode ClusterOnDie setting switch
EarlySnoopEn	Memory Snoop mode EarlySnoop and HomeSnoop setting switch
DdrFreqLimit	Memory frequency setting switch.
RankMargin	Rank Margin Tool switch.
rmtPatternLength	RMT Pattern Length, which is set when Rank Margin Tool is enabled.
MemTestOnFastBoot	Memory test switch set for fast boot.
ADREn	Memory ADR switch
CustomRefreshRa-teEn	Memory refresh rate switch.
CustomRefreshRate	Specifies the memory refresh rate.
refreshMode	Specifies the memory refresh mode. 1 indicates 2x memory self-refresh, and 0 indicates that 2x memory self-refresh is not supported. If this parameter is set to 1, the memory refresh rate will be doubled when the memory DIMM exceeds 85°C.
mcODTOverride	Memory mc on die termination (ODT) setting. ODT is a mechanism that allows the DRAM controller to dynamically control the termination resistance value of DQ/DQS/DM pins on DRAM devices in a variety of ways. The value can be 50 ohms or 100 ohms.
NumaEn	Non Uniform Memory Access (NUMA) is a distributed memory access mode. It allows reasonable memory allocation among multiple nodes and the processor to simultaneously access different memory addresses.
IsocEn	Specifies whether to enable the isochronous flow-control mode, which ensures the quality of traffic to/from PCH and impacts the memory performance because some bandwidths are reserved for DMI.
RASMode	Specifies the memory RAS mode. It can be independent mode, mirrored mode, or Lockstep mode.
enableSparing	Rank Sparing setting switch

Parameter	Description
multiSparingRanks	Haswell CPU supports multiple spare ranks. You can set the number of spare ranks for a channel.
spareErrTh	Memory correctable error threshold. When the number of correctable errors reaches this threshold, an SMI will be triggered and measures will be taken based on the RAS feature configured.
PatrolScrub	Controls the memory patrol scrub feature. The memory engine checks the memory at a certain speed and correct the correctable errors found, to prevent errors from being accumulated to uncorrectable errors.
PatrolScrubDuration	Specifies the memory patrol duration in hours.
DemandScrubMode	Controls the Demand Scrub feature. When HA reads memory data, it corrects errors found and writes correct data to the memory.
DeviceTaggingMode	Controls the Device Tagging feature. This feature allows an SMI to be triggered when the number of errors occurred on a memory chip exceeds the threshold. During the SMI processing, a parity chip can be used to replace the faulty chip.
thermalthrottlingsup-port	Specifies the memory temperature adjustment mode. Closed Loop Thermal Throttling (CLTT) applies to DIMMs with temperature sensors. It allows dynamic memory adjustment based on the sensor temperature. Open Loop Thermal Throttling (OLTT) applies to DIMMs without temperature sensor. It allows static memory adjustment based on configuration.
PcieAcpiHotPlugEna-ble	Specifies whether to enable IIO PCI-E Hotplug.
EnableAzaliaVCpOp-timizationste	Specifies whether to enable azalia_on_vcp.
PCIeSRIOVSupport	Specifies whether to enable PCIe virtualization function.
VTdSupport	Specifies whether to enable Intel VT for Directed I/O (VT-d).
InterruptRemap	Specifies whether to enable Interrupt Remapping, which is related to VT-d.
CoherencySupport	Specifies whether to enable Coherency Support, which is related to VT-d.
IsochCoherencySup-port	Specifies whether to enable Coherency Support (Isoch), which is related to VT-d.
IdeController	Specifies whether to enable SATA controller.

Parameter	Description
SataCnfigure	Specifies the SATA controller mode.
PchsSata	Specifies whether to enable sSATA controller.
sSataInterfaceMode	Specifies the sSATA controller mode.
XHCIMode	Specifies the USB 3.0 controller switch.
CREnable	Serial port redirection switch.
CRTerminalType	Font type selection switch for serial port redirection.
CRBaudRate	Baud Rate selection switch for serial port redirection.
CRInfoWaitTime	Initialization information display time for serial port redirection.
CRAfterPost	Specifies whether serial port redirection takes effect after BIOS POST.
PXE1setting	LOM 1 PXE switch
PXE2setting	LOM 2 PXE switch
WheaSupport	Specifies whether to enable WHEA for fault diagnosis.
WheaEinjType	Specifies whether to enable WHEA error injection for fault diagnosis.
SystemErrorEn	Specifies whether to enable fault diagnosis.
FDM	Specifies whether to enable reporting of fault diagnosis to the BMC.
PoisonEn	Poison bit switch.
EMcaLogEn	EMCA log (ELOG) switch. The BIOS creates ELOG entries, which record error information in detail for the OS/VMM to predict faults. The log is stored in the reserved memory provided by the BIOS and accessed through the Entry address. There is also a WHEA log corresponding to ELOG, and the structure of the WHEA log is defined by ACPI specifications.
EMcaCSmiEn	CMCI-to-SMI signal switch. If it is disabled, only CMCI will be triggered when correctable errors are found on the memory. An SMI will be triggered only when the number of errors reaches the threshold. If it is enabled, each correctable error will trigger an SMI, which is processed by the BIOS. At the end of the SMI processing function, the BIOS decides whether to send an MCE signal to the OS. This helps to collect more useful information.

Parameter	Description
PowerStateRestoreO-nACLoss	Specifies the power control policy for the operating system when the AC is powered on. ● ON: Automatic power-on ● OFF: Remain power-off ● Last State: Restore the last state
BmcWdtEnable	Specifies whether to enable the POST watch dog.
BmcWdtTimeout	Specifies the timeout period of the POST watch dog.
BmcWdtAction	Specifies the POST watch dog actions.
OSWdtEnable	Specifies whether to enable the OS watch dog.
OSWdtTimeout	Specifies the timeout period of the OS watch dog.
OSWdtAction	Specifies the OS watch dog actions.
SysDbgLevel	BIOS debugging switch
serialDebugMsgLvl	BISO debugging print level.
Pci64BitResourceAllo-cation	If this function is enabled, the PCI MMIO address space is greater than 4 GB.
ClkGenSpreadSpec-trum	Spread spectrum switch.
WakeOnPME	Wake On LAN switch.
NICTrunk	Before OS starts, the DisableNic2ndhandle function will be called to disable the second optical port of 82599. This function is not available at present.
Language	Specifies the language used.
ComBaseOutput	Serial port IO base settings.
OemMemTurbo	Memory overclock switch.
SoftRaidModeSelect	SoftRAID selection switch. **NOTE** V5 servers do not support this configuration.
BootType	Specifies the boot type, which can be Legacy, UEFI, or DUAL.
QuickBoot	Quick Boot settings. If it is disabled, a memory test will be performed after the first screen after each start.
QuietBoot	Specifies whether to display boot information before the BIOS logo appears.
PXEOnly	Specifies whether to limit the server to boot from PXE only and skip other boot options (such as a hard disk and CD-ROM).

Parameter	Description
VideoSelected	Onboard video card or external video card
NoBootDevCtr	Specifies whether the board is automatically restarted when no boot device is available.
BootTypeOrder[0]	Specifies the boot sequence.
BootTypeOrder[1]	Specifies the boot sequence.
BootTypeOrder[2]	Specifies the boot sequence.
BootTypeOrder[3]	Specifies the boot sequence.

Table 9-3 RAID controller card parameters

| Type	Export Parameter	Export Subparameter	Description	Valid After Imported via Configuration File
Storage	RaidController	Type	Specifies the controller type.	No The value is displayed in the configuration file.
	RaidController	CopybackEnabled	Specifies the copyback function status of the RAID controller card.	Yes
	RaidController	SMARTerCopybackEnabled	Specifies whether to automatically perform copyback when the RAID controller card detects a physical disk SMART error.	Yes
	RaidController	JBODEnabled	Specifies the JBOD function status of the RAID controller card.	Yes

10 FAQ

10.1 Unknown Devices Detected on V5 Servers After Windows Installed

Symptom

Symptom	Possible Cause
After Windows and related driver packages are installed on the V5 Servers, an unknown device is found in the **Device Manager** Window, as shown in **Figure 10-1**.	The black box function is enabled on the iBMC of the V5 Servers by default. However, there is no driver on the Windows.

Figure 10-1 Unknown device on the Windows of the V5 server
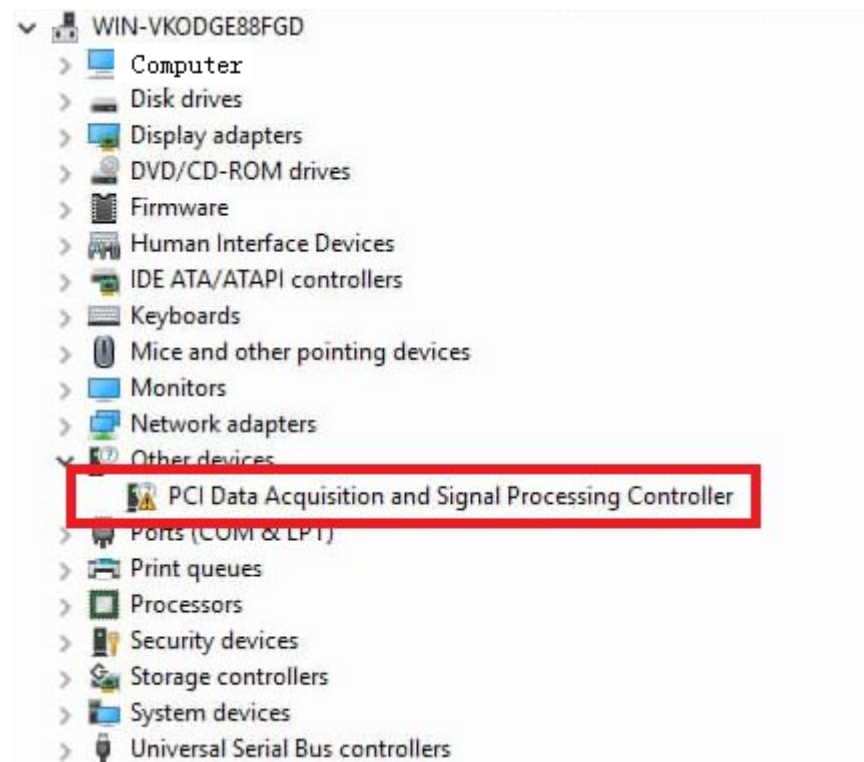
Solution

Method 1: Install the black box driver.

The black box driver is installed automatically with the iBMA.

1. Install the iBMA on the Windows. For details, see the iBMA user guide.
2. If the problem still persists after the iBMA is run, contact technical support.

Method 2: Disable the black box function.

1. Disable the black box function on the **Black Box** page of the iBMC WebUI.
2. If the problem still persists, contact technical support.