iBMC Intelligent Management System

White Paper

Issue 08

Date 2023-12-14

xFusion Digital Technologies Co., Ltd.

Trademarks and Permissions

xFUSION and other xFusion trademarks are trademarks of xFusion Digital Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

In this document, "xFusion" is used to refer to "xFusion Digital Technologies Co., Ltd." for concise description and easy understanding, which does not mean that "xFusion" may have any other meaning. Any "xFusion" mentioned or described hereof may not be understood as any meaning other than "xFusion Digital Technologies Co., Ltd.", and xFusion Digital Technologies Co., Ltd. shall not bear any liability resulting from the use of "xFusion".

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

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

xFusion Digital Technologies Co., Ltd.

Address: 9th Floor, Building 1, Zensun Boya Square, Longzihu Wisdom Island
Zhengdong New District 450046
Zhengzhou, Henan Province
People's Republic of China

Website: https://www.xfusion.com

About This Document

Purpose

This document describes the features of the intelligent Baseboard Management Controller (iBMC).

Intended Audience

This document is intended for:

- Presales engineers of server vendor
- Presales engineers of channel partners
- Enterprise presales engineers

Symbol Conventions

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

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

Issue	Date	Description
08	2023-12-14	Added **3.9.19 China CC EAL4 Certification**.
07	2023-09-04	5885H V6 is added to the supported product range.
06	2023-06-25	Added **3.18 Liquid Cooling Monitoring Management**.
05	2023-04-20	● Optimized the description of supported models. ● Added descriptions about security authentication.
04	2022-12-22	G5500 V6 is added to the supported product range.
03	2022-09-13	Added **3.12.2 BIOS Configuration**.
02	2022-06-27	The description is optimized.
01	2021-10-27	This issue is the first official release.

Contents

About This Document....ii

1 Overview....1

1.1 Introduction to iBMC....1

1.2 System Architecture....2

2 Supported Servers....4

3 Functions....5

3.1 Diversified Management Interfaces....6

3.1.1 IPMI....8

3.1.2 SNMP Interface....10

3.1.3 Redfish Interface....12

3.1.4 CLI....14

3.1.5 Web Interface....15

3.1.6 Mobile Application Management Interface....18

3.1.6.1 Installation Requirements....18

3.1.6.2 Supported Servers....18

3.1.6.3 Supported Functions....19

3.2 Fault Diagnosis and Management....33

3.2.1 Fault Detection....33

3.2.2 Fault Diagnosis....37

3.2.3 Proactive Failure Analysis....38

3.2.4 System Running Recorder....39

3.2.5 Startup Self-Check Code....40

3.2.6 Event Management....40

3.2.7 Fault Reporting....42

3.2.8 Breakdown Screenshot....43

3.2.9 Breakdown Video....44

3.2.10 Screen Snapshot....44

3.2.11 Screen Video....45

3.2.12 Parts Replacement Records....47

3.2.13 BOM Code Management....47

3.2.14 System Watchdog....47

3.3 Virtual KVM and Virtual Media....48

3.3.1 Virtual KVM....52
3.3.2 Virtual Media....53
3.4 HTTPS-based Intuitive Management Interface....55
3.4.1 Viewing System Information....56
3.4.2 Querying System Information....56
3.4.3 Performance Monitoring....58
3.4.4 Device Location....60
3.5 Domain Management and Directory Service....60
3.5.1 Domain Management....60
3.5.2 Directory Service....61
3.6 Firmware Management....63
3.6.1 Firmware Dual-image Backup....63
3.6.2 Firmware Upgrade....64
3.6.3 Separated BMC Upgrade and Validation....65
3.7 Intelligent Power Management and Smart Cooling....65
3.7.1 Power Control....65
3.7.2 Power Capping....66
3.7.3 Power Statistics and Power History Line....68
3.7.4 Active and Standby PSUs....69
3.7.5 Smart Cooling....70
3.8 SOL and System Serial Port Running Information Record....71
3.8.1 SOL....71
3.8.2 Recording System Serial Port Data....71
3.9 Security Management....72
3.9.1 Account Security....72
3.9.2 Authentication Management....73
3.9.3 Authorization Management....75
3.9.4 Certificate Management....75
3.9.5 Session Management....77
3.9.6 Security Protocols....77
3.9.7 Data Protection....78
3.9.8 Security Configuration....78
3.9.9 Key Management....79
3.9.10 System Hardening....80
3.9.11 Log Audit....80
3.9.12 DICE....80
3.9.13 Secure Boot....80
3.9.14 PFR....81
3.9.15 Revocation of Insecure Versions....81
3.9.16 E-Warranty Management....81
3.9.17 PCI DSS Certification....81
3.9.18 International CC EAL4+ Certification....81

3.9.19 China CC EAL4 Certification....81
3.10 Access Management.... 82
3.10.1 Management Network Port Auto-Adaptation.... 82
3.10.2 NC-SI.... 83
3.10.3 IPv6....84
3.10.4 SSO.... 84
3.10.5 Local O&M.... 86
3.10.6 SSDP.... 86
3.10.7 Firmware Alliance BMC Standard Compliance Test Certification.... 86
3.11 Unified User Management.... 86
3.12 Configuration Management....87
3.12.1 Configuration Import and Export....87
3.12.2 BIOS Configuration....87
3.13 Storage Management.... 88
3.13.1 Built-in SD Cards.... 88
3.13.2 RAID and Drive Management....88
3.14 Time Management.... 93
3.15 Smart Provisioning....95
3.15.1 Overview....95
3.15.2 System Design....95
3.15.3 Firmware Update.... 96
3.15.4 Smart Provisioning Upgrade....97
3.15.5 PCIe Card Resources Collected....97
3.15.6 Erasing Drives....98
3.16 iBMA Management.... 98
3.16.1 Overview....98
3.16.2 Supported Features.... 99
3.16.3 Onboard iBMA.... 100
3.16.4 Upgrade Interface.... 101
3.17 Kerberos Authentication....104
3.17.1 iBMC SSO Solution Overview....104
3.17.2 Environment Configuration.... 106
3.17.3 System Compatibility.... 106
3.18 Liquid Cooling Monitoring Management.... 107
3.18.1 Server Liquid Cooling Monitoring....107
3.18.2 Cabinet Liquid Cooling Monitoring.... 107

1 Overview

1.1 Introduction to iBMC

1.2 System Architecture

1.1 Introduction to iBMC

The Intelligent Baseboard Management Controller (iBMC) is a proprietary out-of-band management software of the remote server management system, which provides remote server monitoring and operations. The iBMC complies with Intelligent Platform Management Interface (IPMI) standards, Simple Network Management Protocol (SNMP), and Redfish interfaces. It provides various functions, including keyboard, video, and mouse (KVM) redirection, text console redirection, remote virtual media, hardware component status information query, hardware log collection and query, and reliable hardware monitoring and management. The iBMC provides the following features:

- Various management interfaces

  The iBMC provides IPMI, command-line interface (CLI), Hypertext Transfer Protocol Secure (HTTPS), SNMP, and Redfish interfaces, meeting various system integration requirements.

- Compliance with DCMI1.5, IPMI 1.5, and IPMI 2.0

  The iBMC provides standard IPMI management interfaces, which allow integration with standard management systems.

- Fault detection and alarm management

  The iBMC implements fault detection and alarm management, ensuring stable uninterrupted 24/7 system operation.

- Virtual KVM and virtual media

  The iBMC provides virtual KVM and virtual media, facilitating remote maintenance; supports KVM over IP and virtual CD/DVD-ROM drives.

- Web-based user interface (WebUI)

  The iBMC provides the web-based UI, helping you rapidly set and query device information.

- Breakdown screenshots and videos

The iBMC allows screenshots and videos to be created when the system collapses. The screenshots and videos help to identify the cause of system breakdown.

- Screen snapshots and videos

  The iBMC offers screen snapshots and videos, which simplify routine preventive maintenance, recording, and auditing.

- DNS, LDAP, and LLDP

  The iBMC supports domain name system (DNS), Lightweight Directory Application Protocol (LDAP), and Link Layer Discovery Protocol (LLDP).This feature simplifies the server management network.

- Dual-image backup

  The iBMC provides software dual-image backups, which allows software to restart from the backup image when a failure occurs. This feature enhances system security.

- Out-of-band RAID management

  The iBMC supports out-of-band RAID monitoring and configuration to improve RAID configuration efficiency and management capabilities.

- Fault diagnostic management (FDM)

  The iBMC supports component-based FDM, which helps locate and replace the faulty component rapidly.

- Network Time Protocol (NTP)

  The iBMC supports NTP to ensure time synchronization of network devices.

- Asset management

  The iBMC facilitates asset management.

- Intelligent power management

  The iBMC uses the power capping technology to improve deployment density and uses dynamic power saving to reduce the operational expenditure (OPEX).

- Security management

  The iBMC implements security management from access, accounts, transmission, and storage. This feature ensures the server security.

1.2 System Architecture

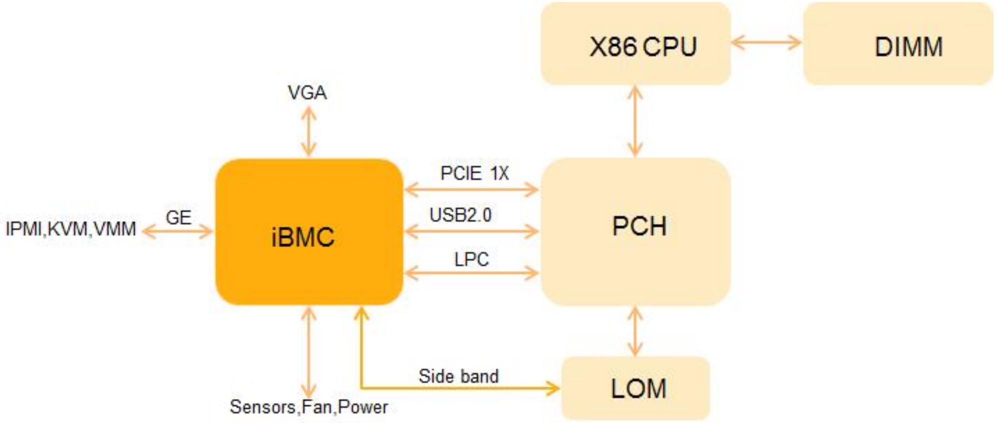
Figure 1-1 shows the iBMC system architecture. The iBMC uses the proprietary Hi1710 or Hi1711 chip. Hi1710 is developed for board-level management of computing or switching. It consists of a single-core A9 CPU with a maximum frequency of 800 MHz, an 8051 single-chip microcomputer, and a co-processor with a frequency of 200 MHz. It also supports remote KVM, IPMI, and PCIe for receiving and transmitting MCTP packets, and provides the local VGA, GE, and RMII ports, and a wide variety of board management ports and peripheral ports. Hi1711 is developed for board-level management of x86 CPU platforms.

It consists of a quad-core A55 CPU with a maximum frequency of 1 GHz, an M3 co-processor (200 MHz frequency) and an M3 security core (200 MHz frequency). Hi1711 also supports remote KVM, IPMI, and PCIe for receiving and transmitting MCTP packets, and provides the local VGA, GE, and RMII ports, and a wide variety of board management ports and peripheral ports.

More details are as follows:

- The KVM module implements remote keyboard and mouse control. When the KVM module receives video data from the OS over the video graphics array (VGA) port, it compresses the video data and sends the compressed data to a remote KVM client over the network. When the KVM module receives keyboard and mouse data from the remote KVM client, it transmits the data to the OS by using a simulated USB keyboard and mouse device.
- The VMM mounts DVD-ROM drive on a local PC as its USB flash drive.
- The iBMC receives the system running track information from the OS over a Peripheral Component Interconnect Express (PCIe) interface and provides an interface for exporting the system running information.
- The iBMC communicates with the agentless inband system intelligent baseboard management agent (iBMA) through the PCIe interface to manage inband components (such as the NICs) and obtain OS information.
- The iBMC communicates with the x86 system through a local PC (LPC) interface to implement IPMI management.
- The iBMC provides GE interfaces to facilitate remote management over IPMI and HTTPS.
- The iBMC uses sensors to monitor the server temperature and voltage. It also intelligently manages the fan modules and power supply units (PSUs) of the server.
- The iBMC supports the network controller sideband interface (NC-SI) technology and VLAN function, allowing more flexible management networking.

Figure 1-1 iBMC architecture (x86)



2 Supported Servers

Category	Servers
Supported servers	● Rack servers: RH1288 V3, RH2288 V3, RH2288H V3, RH5885 V3, RH5885H V3, RH8100 V3, 1288H V5, 1288X V5, 2288 V5, 2288C V5, 2288H V5, 2288X V5, 2298 V5, 2488 V5, 2488H V5, 5288 V5, 5288X V5, 5885H V5, 8100 V5, 1288H V6, 2288H V6, 2288E V6, 5288 V6, 2488H V6, 5885H V6, 1288H V7, 2288 V7, 2288H V7, 5288 V7, 2488H V7, 5885H V7, 1258H V7 ● Blade servers: CH121 V3, CH121H V3, CH121L V3, CH140 V3, CH140L V3, CH220 V3, CH222 V3, CH225 V3, CH226 V3, CH242 V3, CX710, CX220, CX620, CX320, CX318, CX920, CH121 V5, CH121L V5, CH221 V5, CH225 V5, CH242 V5 ● High-density servers: XH310 V3, XH321 V3, XH620 V3, XH622 V3, XH628 V3, XH321 V5, XH321L V5, XH628 V5, XH321 V6, XH321C V6, XH321 V7, XH321E V7 ● Mission-critical servers: 9008 V5, 9008, 9016, 9032 ● GPU servers: G560, G2500, G5500 (G560 V5, G530 V5), G5500 V6, CX5200 V5, G5200 V7, G5500 V7, G8600 V7, G8600E V7 ● FusionPoD servers: FusionPoD 600 (DH120 V5, DH140CV6, DH120C V5, DH120C V6, DH121C V6), FusionPoD 700 (DH141C V5), FusionPoD 710 (DH140C V6), FusionPoD 720 (DH122E V6, DH120E V7)

3 Functions

The iBMC provides diversified functions to improve management efficiency and reduce the OPEX.

- The iBMC is a proprietary intelligent management system that remotely manages servers. It supports KVM redirection, text console redirection, remote virtual media (mounting the DVD-ROM drive, floppy disk drive, or folder from a local PC to the server), and hardware monitoring and management based on IPMI and Redfish interfaces. The iBMC employs dual-image backups for software to provide carrier-class reliability.

  The iBMC provides a variety of user interfaces, such as the CLI, WebUI, IPMI, SNMP, and Redfish interface, to facilitate system integration. All the user interfaces use authentication mechanisms and highly secure encryption algorithms to ensure access and transmission security.
- The iBMC not only monitors servers, but also provides alarms and detailed logs. The iBMC provides alarms for mainboard power supply faults, CPU core temperature, voltage, drive faults, fan speed and temperature faults, NIC MCE/AER errors, system power supply faults, bus faults, and system breakdown. It also provides basic information about components, such as CPUs, memory, NICs, and drives. In addition, it supports one-click collection of alarm logs, error logs, and component information for fault locating.
- When a server breaks down, the iBMC automatically saves the last information displayed on the screen. The iBMC allows a third-party program to set scheduled tasks to capture screenshots. These features help rapidly restore the system from failures and save manpower in maintenance.

3.1 Diversified Management Interfaces

3.2 Fault Diagnosis and Management

3.3 Virtual KVM and Virtual Media

3.4 HTTPS-based Intuitive Management Interface

3.5 Domain Management and Directory Service

3.6 Firmware Management

3.7 Intelligent Power Management and Smart Cooling

3.8 SOL and System Serial Port Running Information Record

3.9 Security Management
3.10 Access Management
3.11 Unified User Management
3.12 Configuration Management
3.13 Storage Management
3.14 Time Management
3.15 Smart Provisioning
3.16 iBMA Management
3.17 Kerberos Authentication
3.18 Liquid Cooling Monitoring Management

3.1 Diversified Management Interfaces

The iBMC is a standalone out-of-band management system complying with the industry management standards. As a node on the data center management network, the iBMC monitors and manages servers, and performs fault diagnosis for servers. It is required to provide a variety of man-machine and machine-machine interfaces to meet different server management and system integration requirements.

The iBMC architecture consists of three layers:

- Interface layer

  The interface layer provides a variety of interfaces, including user interfaces (WebUI and CLI) and machine-machine interfaces (SNMP, IPMI, and Redfish interface).
- Application layer

  The application layer incorporates all the management features and functions.
- Framework layer

  The framework layer consists of the platform management engine (PME), Linux kernel, and driver.

Figure 3-1 iBMC management interfaces

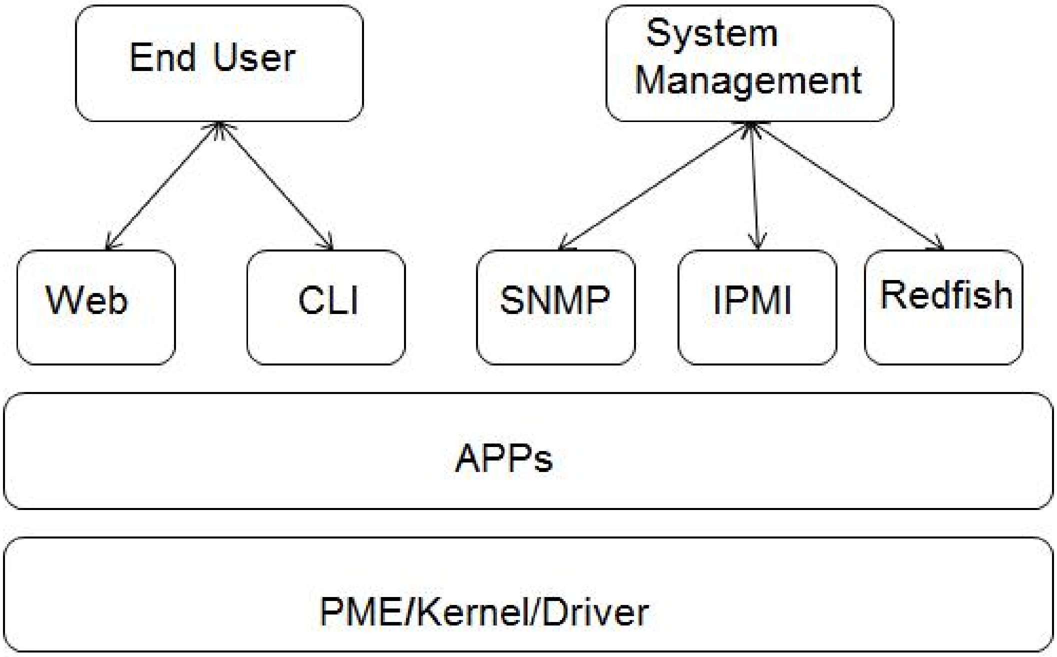


Table 3-1 System integration interfaces

Interface	Difficulty	Integration Workload	Compatibility	Security	Performance	Architecture Advantage	Application
Redfish	Redfish uses the most popular Python programming language and JavaScript object notation (JSON) for data input and output.	Data input and output in JSON does not require parsing.	Redfish offers high compatibility and is developed to replace IPMI.	It is based on HTTPS and supports various security encryption, integrity, and authentication algorithms.	Entire resources can be obtained through one interaction.	All things are abstracted as resources, with unique URI. The architecture is object-oriented.	It is widely used in Internet and network management scenarios. REST and Python are also commonly used.
SNMP	The management information base (MIB), OID, and SNMP specifications must be mastered.	Data needs to be parsed based on the MIB.	SNMP defines standard network nodes and offers poor compatibility.	It supports only MD5 and SHA1 authentication algorithms and DES and AES128 encryption algorithms. It does not support domain account access.	Only one piece of data (max. 4 KB) can be obtained at a time.	The architecture is node-oriented, which lacks hierarchy and association.	It is commonly used in management of network switching devices. The overall popularity is not very high.

Interface	Difficulty	Integration Workload	Compatibility	Security	Performance	Architecture Advantage	Application
IPMI	IPMI uses the C programming language, which is difficult to master.	Binary output is not user-friendly and has a large workload for parsing.	IPMI offers poor compatibility and has not been updated for a long time.	It supports limited security algorithms, has security vulnerabilities, and does not support domain account access.	Only one piece of data (max. 255 bytes in the inband channel) can be obtained at a time.	The architecture is command-oriented, which lacks hierarchy and association.	It is commonly used in server management. The overall popularity is not very high.

NOTE

Based on the above analysis, the Redfish interface will be the major external interface integrated by the iBMC. iBMC will proactively follow up the DMTF Redfish specifications in a timely manner.

3.1.1 IPMI

The iBMC supports IPMI 1.5 and IPMI 2.0 standards. It effectively manages servers by using third-party tools, such as IPMItool, through a LPC-based Block Transfer (BT) or local area network (LAN) User Datagram Protocol (UDP) or Internet Protocol (IP). If LPC-based BT is used, the third-party tools must run on the server OS. If LAN channels are used, the third-party tools can remotely manage servers. The iBMC supports AES-CBC-128 encryption algorithm, HMAC-SHA1 and HMAC-SHA256 algorithms for authentication and integrity verification, and third-party tools running on Windows or Linux.

IPMI is widely used in server management, especially in the early inband management scenarios due to its support for authentication-free internal channel communication. The servers from all vendors support it.

If the management network needs to be isolated from the service network, the iBMC supports the blacklist and whitelist mechanism to shield IPMI commands issued through the in-band LPC channels. Users can add, delete, and query the whitelist and blacklist, which include the channel ID, network function code, command words, subcommands, and parameters. When the whitelist and blacklist function is disabled, the inband and outband communication is normal. When the whitelist is enabled, only the commands in the whitelist can be issued through the inband channels. When the blacklist is enabled, the commands in the blacklist cannot be issued through the inband channels. By default, the blacklist is enabled. You can switch to the whitelist mode as required.

The iBMC provides the following capabilities through IPMI interfaces:

1. Upgrade firmware, such as the iBMC, BIOS, CPLD, and PSU firmware.
2. Manage user accounts, including adding users, changing passwords, modifying user permissions, and deleting users.
3. Start and stop services and modify ports.
4. Configure power capping settings.
5. Perform RAID out-of-band configuration, including viewing the information about hard drives and RAID cards, creating RAID, setting attributes, and deleting RAID.
6. Configure network settings, including the IP address, subnet mask, gateway, and DNS.
7. Configure system startup settings, including setting the boot device, boot mode, and effective mode.
8. Query the system event log (SEL).
9. Query sensor information, such as temperature and voltage.
10. Perform power control, including powering on or powering off and restarting the server.
11. Query field replaceable unit (FRU) information, including the asset label, product name, and product serial number.
12. Support the Serial Over LAN (SOL) function.

The following uses the IPMItool as an example:

- IPMItool command syntax: **ipmitool [interface] [parameter] <command>**
- The IPMItool command can be used to set the following interfaces:

```
Interfaces:
open            Linux OpenIPMI Interface [default]
imb             Intel IMB Interface
lan             IPMI v1.5 LAN Interface
lanplus         IPMI v2.0 RMCP+ LAN Interface
```

- The IPMItool parameters include the following:

```
Parameters:
-h              This help
-V              Show version information
-v              Verbose (can use multiple times)
-c              Display output in comma separated format
-d  N           Specify a /dev/ipmiN device to use (default=0)
-I  intf        Interface to use
-H  hostname    Remote host name for LAN interface
-p  port        Remote RMCP port [default=623]
-U  username    Remote session username
-f  file        Read remote session password from file
-S  sdr         Use local file for remote SDR cache
-a              Prompt for remote password
-e  char        Set SOL escape character
-C  ciphersuite Cipher suite to be used by lanplus interface
-k  key         Use Kg key for IPMIv2 authentication
-y  hex_key     Use hexadecimal-encoded Kg key for IPMIv2 authentication
-L  level       Remote session privilege level [default=ADMINISTRATOR] Append a '+' to use name/privilege
lookup in RAKP1
-A  authtype    Force use of auth type NONE, PASSWORD, MD2, MD5 or OEM
-P  password    Remote session password
-E              Read password from IPMI_PASSWORD environment variable
-K              Read kgkey from IPMI_KGKEY environment variable
-m  address     Set local IPMB address
-b  channel     Set destination channel for bridged request
-t  address     Bridge request to remote target address
```

```
-B  channel        Set transit channel for bridged request (dual bridge)
-T  address        Set transit address for bridge request (dual bridge)
-l  lun            Set destination lun for raw commands
-o  oemtype        Setup for OEM (use 'list' to see available OEM types)
-O  seloem         Use file for OEM SEL event descriptions
```

- The IPMItool tool can be used to perform the following operations:

```
Commands:
raw              Send a RAW IPMI request and print response
i2c             Send an I2C Master Write-Read command and print response
spd              Print SPD info from remote I2C device
lan             Configure LAN Channels
chassis          Get chassis status and set power state
power            Shortcut to chassis power commands
event            Send pre-defined events to MC
mc               Management Controller status and global enables
sdr             Print Sensor Data Repository entries and readings
sensor           Print detailed sensor information
fru             Print built-in FRU and scan SDR for FRU locators
gendev           Read/Write Device associated with Generic Device locators sdr
sel             Print System Event Log (SEL)
pef             Configure Platform Event Filtering (PEF)
sol             Configure and connect IPMIv2.0 Serial-over-LAN
tsol            Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol            Configure IPMIv1.5 Serial-over-LAN
user             Configure Management Controller users
channel          Configure Management Controller channels
session          Print session information
sunoem           OEM Commands for Sun servers
kontronoem       OEM Commands for Kontron devices
picmg            Run a PICMG/ATCA extended cmd
fwum             Update IPMC using Kontron OEM Firmware Update Manager
firewall        Configure Firmware Firewall
delloem          OEM Commands for Dell systems
shell            Launch interactive IPMI shell
exec             Run list of commands from file
set             Set runtime variable for shell and exec
hpm              Update HPM components using PICMG HPM.1 file
ekanalyzer       Run FRU-Ekeying analyzer using FRU files
```

- For example, to query all the local users on iBMC, run the following ipmitool command:

  LPC-based IPMItool command:

  ipmitool user list

  LAN-based IPMItool command:

  ipmitool -H *.*.*.* -I lanplus -U <*user name*> -P <*password*> user list 1

  NOTE

  - **H**: Enter the IP address of the iBMC network port after **H**.
  - **I**: Enter a transmission protocol after **I**. **lan** indicates non-encryption. **lanplus** indicates encryption.
  - **U**: Enter the local user name after **U**.
  - **P**: Enter the password for a local user after **P**.

3.1.2 SNMP Interface

The SNMP is a protocol used for communication between the network management services (NMSs) and Agents. It defines the standard management framework, common languages in communication, and security and access control mechanisms used for monitoring and managing devices on a network.

The iBMC provides simple SNMP programming interfaces and supports SNMP Get, Set, and Trap operations. Users can easily manage the server by using a third-party management software that invokes the SNMP interface. The SNMP agent supports SNMPv1, SNMPv2c, and SNMPv3, and SNMPv3 is enabled by default for security purposes. The Get and Set operations of SNMPv1 and v2c support different community names. The SNMPv3 supports authentication algorithm MD5 and SHA and encryption algorithms DES and AES, and the security user name is the same as the login user name. The same user account can be used for SNMPv3 and other interfaces (such as WebUI, CLI, and IPMI LAN).

The SNMP interface applies to the following scenarios:

- Management based on open-source tools

  In testing or temporary remote O&M of servers, a third-party MIB tool (for example MG-SOFT MIB Browser) or a CLI tool can be used to manage MIB nodes over SNMP.

- Simple integration management

  Network management software can be used to compile and import SNMP MIB definition files so that users can manage servers, configure trigger scripts for important information, and re-map trap events over SHMP. The iBMC supports mainstream network management software, such as CA, IBM System Director, and HP SIM.

- In-depth integration management

  Integrated management plug-ins are developed for NMSs of different server vendors. The plug-in receives operation commands from the NMS, communicates with the iBMC through the SNMP interface, and sends information in the format defined by the interface to the NMS. Plug-ins for VMware vCenter and Microsoft System Center has been developed.

The iBMC provides the following capabilities through the SNMP interfaces:

1. Upgrade firmware, such as the iBMC, BIOS, CPLD, and PSU firmware.
2. Manage user accounts, including adding users, changing passwords, modifying user permissions, and deleting users.
3. Configure power capping settings.
4. Perform RAID out-of-band configuration, including viewing the information about hard drives and RAID cards, creating RAID, setting attributes, and deleting RAID.
5. Configure network settings, including the IP address, subnet mask, gateway, and DNS.
6. Configure system startup settings, including setting the boot device, boot mode, and effective mode.
7. Query system resource performance information, including CPU, memory, and drive partition usage.
8. Configure stateless computing settings.
9. Query the current health events, history events, system health status, and clear events.
10. Perform certificate management, including querying certificate information, generating and exporting a CSR, and importing certificate, certificate chain, and dual-factor certificate.
11. Configure active/standby PSUs.

12. Configure NTP and time zone settings.
13. Configure LDAP settings.
14. Query temperature and voltage information.
15. Perform power control, including powering on or powering off and restarting the server.
16. Query system information, including the asset label, product name, and product serial number.
17. Query CPU and memory information.
18. Query power supply and fan information.
19. Query NIC and port information.
20. Configure SNMP Trap settings.
21. Configure alarm email notification settings.

3.1.3 Redfish Interface

Representational State Transfer (REST) is a simple stateless architecture used for designing and developing network applications. It simplifies development complexity and improves system scalability.

REST has the following design concepts and criteria:

- Everything on the network is abstracted as a resource expressed in JSON format.
- Each resource is addressed by a uniform resource identifier (URI).
- Resources are managed by HTTP interfaces including GET, PATCH, POST, and DELETE.
- Operations on resources will not change their URIs.
- All operations are stateless.

The Redfish Scalable Platforms Management API (Redfish) is a new HTTPS-based specification that uses the data model representation inside hypermedia RESTful interfaces.

Redfish = REST API + software-defined server (data model). It is maintained by Distributed Management Task Force (DMTF, **www.dmtf.org**).

Figure 3-2 Redfish schema architecture:

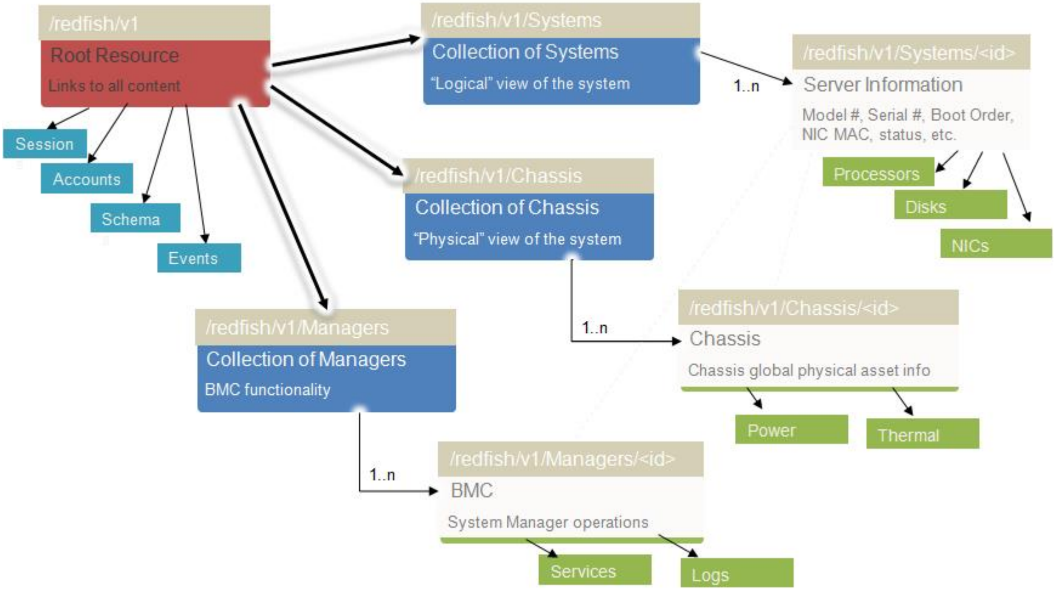
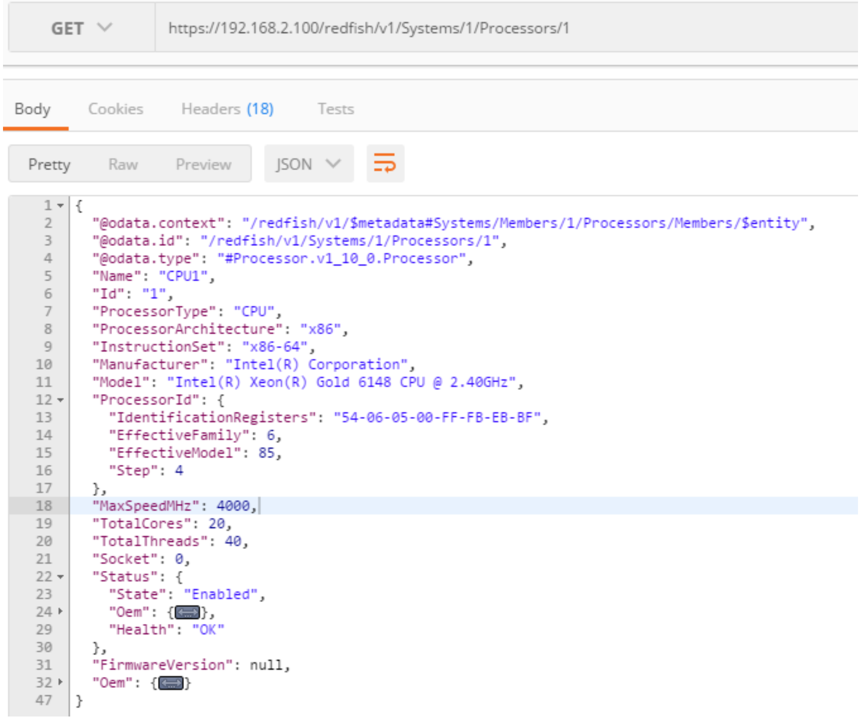


Figure 3-3 Redfish operation example (querying processor resources)



https://192.168.2.100/redfish/v1/Systems/1/Processors/1

```
{
  "@odata.context": "/redfish/v1/$metadata#Systems/Members/1/Processors/Members/$entity",
  "@odata.id": "/redfish/v1/Systems/1/Processors/1",
  "@odata.type": "#Processor.v1_10_0.Processor",
  "Name": "CPU1",
  "Id": "1",
  "ProcessorType": "CPU",
  "ProcessorArchitecture": "x86",
  "InstructionSet": "x86-64",
  "Manufacturer": "Intel(R) Corporation",
  "Model": "Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz",
  "ProcessorId": {
    "IdentificationRegisters": "54-06-05-00-FF-FB-EB-BF",
    "EffectiveFamily": 6,
    "EffectiveModel": 85,
    "Step": 4
  },
  "MaxSpeedMHz": 4000,
  "TotalCores": 20,
  "TotalThreads": 40,
  "Socket": 0,
  "Status": {
    "State": "Enabled",
    "Oem": {↔},
    "Health": "OK"
  },
  "FirmwareVersion": null,
  "Oem": {↔}
}
```

The iBMC supports Redfish 1.0.4. The iBMC implements the following through the Redfish interface:

1. Upgrade firmware, such as the iBMC, BIOS, CPLD, and PSU firmware.
2. Upgrade the NIC and RAID card drivers.
3. Manage user accounts, including adding users, changing passwords, modifying user rights, and deleting users.

4. Import and export the BMC, BIOS, and RAID controller configurations in XML files.
5. Query and configure BIOS settings.
6. Query the software resource list.
7. Start and stop services and modify ports.
8. Configure power capping settings.
9. Perform RAID out-of-band configuration, including viewing the information about hard drives and RAID cards, creating RAID, setting attributes, and deleting RAID.
10. Configure network settings, including the IP address, subnet mask, gateway, and DNS.
11. Configure system startup settings, including setting the boot device, boot mode, and effective mode.
12. Query system resource performance information, including CPU, memory, and drive partition usage.
13. Query system information, including the host name, domain name (oem), computer description (oem), OS major and minor version information, and patch major and minor version information.
14. Configure stateless computing settings.
15. Query the current health events, history events, system health status, and clear events.
16. Manage event subscription.
17. Query remote virtual media attributes, and mount and unmount virtual media.
18. Perform certificate management, including querying certificate information, generating and exporting a CSR, and importing certificate, certificate chain, and dual-factor certificate.
19. Configure active/standby PSUs.
20. Configure NTP and time zone settings.
21. Configure LDAP settings.
22. Query temperature and voltage information.
23. Perform power control, including powering on or powering off and restarting the server.
24. Query system information, including the asset label, product name, and product serial number.
25. Query CPU and memory information.
26. Query power supply and fan information.
27. Query NIC and port information.
28. Configure SNMP Trap settings.
29. Configure alarm email notification settings.

3.1.4 CLI

The iBMC provides a private command line interface (CLI), which includes two basic commands: **ipmcget** and **ipmcset**. Users can access the iBMC CLI over SSH to implement remote server management.

The CLI provides a man-machine interface that does not rely on an extra tool, and is easy to be integrated. It is more lightweight than the WebUI and is more user-friendly than some interfaces.

The iBMC provides the following capabilities through the CLI:

1. Upgrade firmware, such as the iBMC, BIOS, CPLD, and PSU firmware.
2. Manage user accounts, including adding users, changing passwords, modifying user rights, and deleting users.
3. Import and export the BMC, BIOS, and RAID controller configurations in XML files.
4. Start and stop services and modify ports.
5. Configure power capping settings.
6. Perform RAID out-of-band configuration, including viewing the information about hard drives and RAID cards, creating RAID, setting attributes, and deleting RAID.
7. Configure network settings, including the IP address, subnet mask, gateway, and DNS.
8. Configure system startup settings, including setting the boot device, boot mode, and effective mode.
9. Configure stateless computing settings.
10. Query the current health events, history events, system health status, and clear events.
11. Query remote virtual media attributes, and mount and unmount virtual media.
12. Perform certificate management, including querying certificate information, generating and exporting a CSR, and importing certificate, certificate chain, and dual-factor certificate.
13. Configure active/standby PSUs.
14. Configure NTP and time zone settings.
15. Configure LDAP settings.
16. Query temperature and voltage information.
17. Perform power control, including powering on or powering off and restarting the server.
18. Query system information, including the asset label, product name, and product serial number.
19. Query power supply and fan information.
20. Configure SNMP Trap settings.
21. Support the Serial Over LAN (SOL) function.

3.1.5 Web Interface

The iBMC provides an intuitive management interface based on HTTPS. Through this web interface, users can perform the following operations:

- Configure parameter settings and query information quickly.
- Monitor the OS startup process, perform operations on the OS, mount or unmount the DVD-ROM drive or FDD through the remote console.

Users can enter the iBMC IPv4 or IPv6 address or domain name in the address box of a browser and log in to the iBMC WebUI using a local user account or domain user account.

Table 3-2 lists the OS, browser, and Java runtime environment (JRE) versions supported by the iBMC WebUI.

Table 3-2 Operating environment of clients

OS	Web Browser	Java Runtime Environment (JRE)
Windows 7 32-bit Windows 7 (64-bit)	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	
	Google Chrome 55.0 to 73.0	
Windows 8 (32-bit) Windows 8 (64-bit)	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	
	Google Chrome 55.0 to 73.0	
Windows 10 (64-bit)	Internet Explorer 11.0 Internet Explorer Edge	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	
Windows Server 2008 R2 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	
	Google Chrome 55.0 to 73.0	
Windows Server 2012 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	
	Google Chrome 55.0 to 73.0	
Windows Server 2012 R2 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	
Windows Server 2016 64-bit	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE

OS	Web Browser	Java Runtime Environment (JRE)
	Mozilla Firefox 45.0 to 67.0	AdoptOpenJDK 11.0.6 JRE
CentOS 7	Mozilla Firefox 45.0 to 67.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
MAC OS X v10.7	Safari 9.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 to 67.0	

The iBMC supports secure TLS protocols:

- The iBMC supports TLS 1.2 and 1.3.
- TLS 1.2 can be enabled or disabled, while TLS 1.3 can only be in the enabled state.
- TLS 1.2 and TLS 1.3 are enabled by default.

The iBMC provides the following capabilities through the WebUI:

1. Upgrade firmware, such as the iBMC, BIOS, CPLD, and PSU firmware.
2. Manage user accounts, including adding users, changing passwords, modifying user rights, and deleting users.
3. Import and export the BMC, BIOS (referred boot medium and boot sequence), and RAID controller configurations in XML files.
4. Start and stop services and modify ports.
5. Configure power capping settings.
6. Perform RAID out-of-band configuration, including viewing the information about hard drives and RAID cards, creating RAID, setting attributes, and deleting RAID.
7. Configure network settings, including the IP address, subnet mask, gateway, and DNS.
8. Configure system boot options, including the boot device, boot mode, and effective mode.
9. Query system resource performance information, including CPU, memory, and drive partition usage.
10. Query system information, including the host name, domain name (oem), computer description (oem), OS major and minor version information, and patch major and minor version information.
11. Query the current health events, history events, system health status, and clear events.
12. Query remote virtual media attributes, and mount and unmount virtual media.

13. Support the remote KVM function.
14. Perform certificate management, including querying certificate information, generating and exporting a CSR, and importing certificate, certificate chain, and dual-factor certificate.
15. Configure active/standby PSUs.
16. Configure NTP and time zone settings.
17. Configure LDAP settings.
18. Query temperature and voltage information.
19. Perform power control, including powering on or powering off and restarting the server.
20. Query system information, including the asset label, product name, and product serial number.
21. Query CPU and memory information.
22. Query power supply and fan information.
23. Query NIC and port information.
24. Configure SNMP Trap settings.
25. Configure alarm email notification settings.

3.1.6 Mobile Application Management Interface

The iBMC provides a visualized management interface based on the mobile applications and uses the secure HTTPS protocol to interact with the background. This enables users to perform remote O&M quickly and conveniently. For details about the installation requirements and supported servers, see Table 3-3 and Table 3-4.

3.1.6.1 Installation Requirements

Table 3-3 Installation requirements

Mobile OS	Version Supported
Android	Android 8.0 and later
IOS	IOS 12.0 and later
HarmonyOS	HarmonyOS 2.0 and later

3.1.6.2 Supported Servers

Table 3-3 List of the supported servers

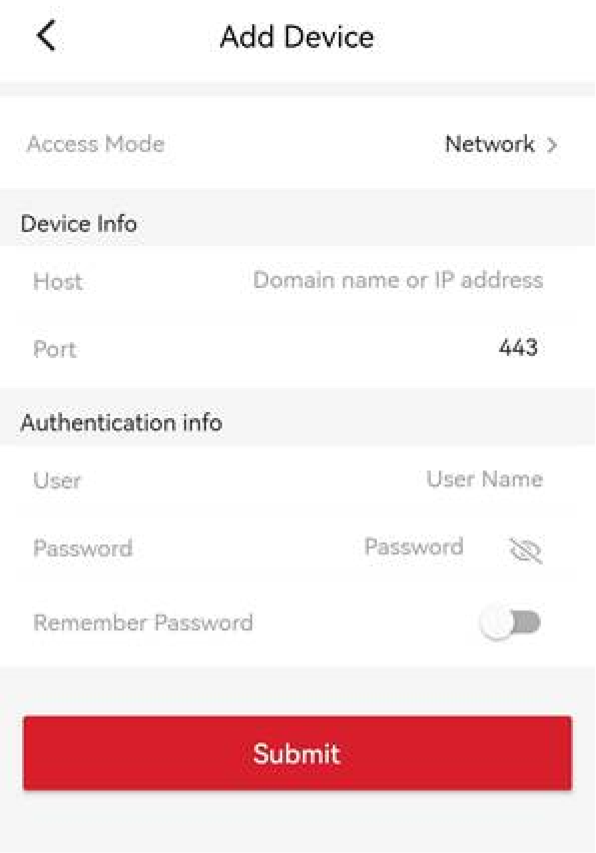
Type	Model
Rack servers	1288H V6
	2288H V6

Type	Model
	2488H V6
	5288 V6
	5885H V6
	1288H V7
	2288 V7
	2288H V7
	2488H V7
	5288 V7
	5885H V7
X6000 V6	XH321 V6
	XH321C V6
GPU servers	G5200 V7
	G5500 V7
	G8600 V7

3.1.6.3 Supported Functions

- Manage devices, which is used to add, edit, and delete devices. Devices can be directly connected through LAN Wi-Fi and Type-C USB cables (IOS versions are not supported).

  Figure 3-4 Add Device screen



Access Mode Network >

Device Info

Host Domain name or IP address

Port 443

Authentication info

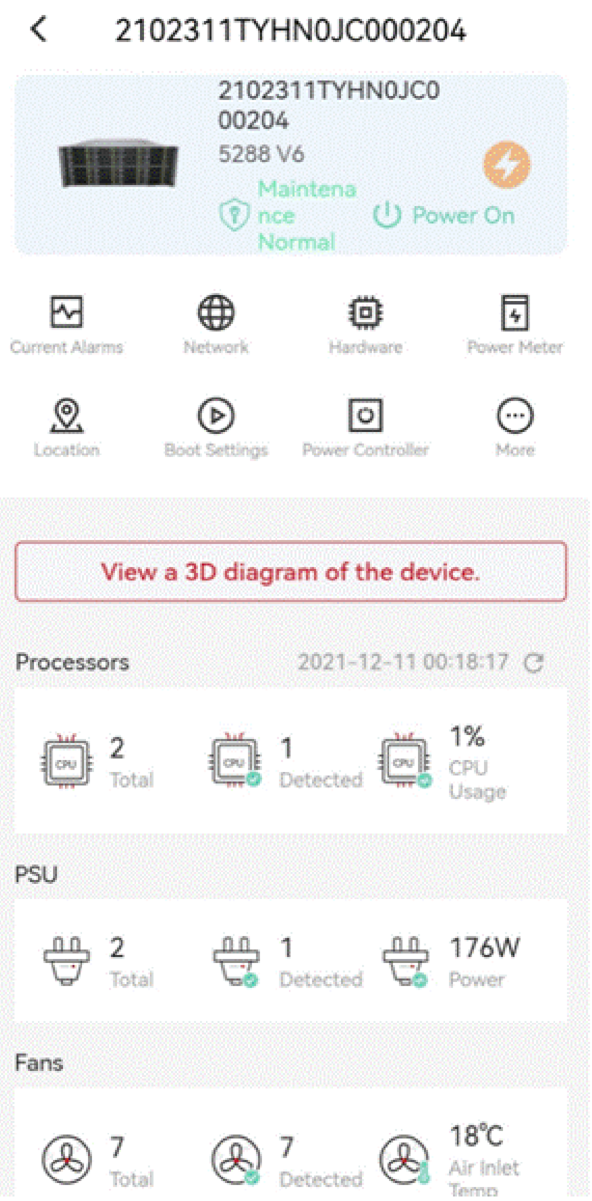
User User Name

Password Password

Remember Password

- Log in to a device. You users log in to a device using the connection information saved on the mobile phone. If users select **Remember Password** when adding a device, the device can be directly connected. Otherwise, users need to enter the password again to log in to the devic.
- Query the basic information of a device.

  Figure 3-5 Device basic information



2102311TYHN0JC000204

2102311TYHN0JC0
00204
5288 V6

Maintenance Normal

Power On

Processors 2021-12-11 00:18:17

2 Total
1 Detected
1% CPU Usage

PSU

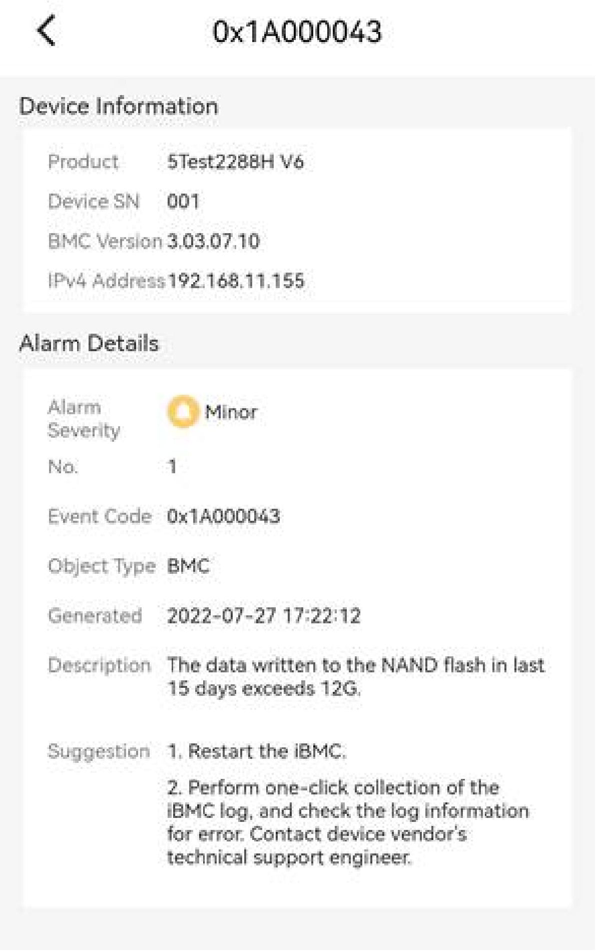
2 Total
1 Detected
176W Power

Fans

7 Total
7 Detected
18℃ Air Inlet Temp

- Query the device alarm information.

Figure 3-6 Device alarm



0x1A000043

Device Information

Product 5Test2288H V6

Device SN 001

BMC Version 3.03.07.10

IPv4 Address 192.168.11.155

Alarm Details

Alarm Severity ● Minor

No. 1

Event Code 0x1A000043

Object Type BMC

Generated 2022-07-27 17:22:12

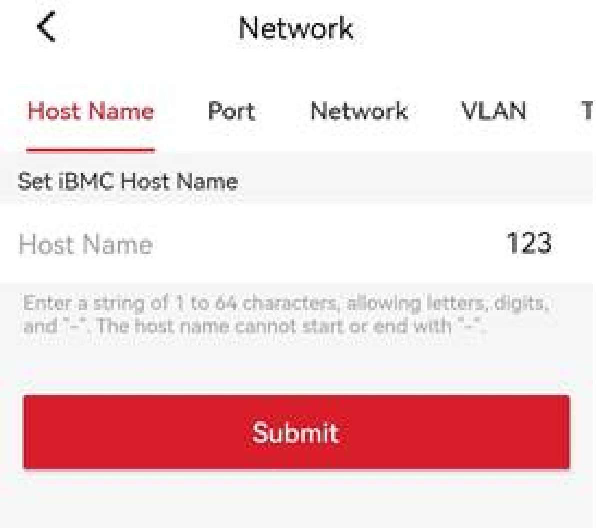
Description The data written to the NAND flash in last 15 days exceeds 12G.

Suggestion 1. Restart the iBMC.

2. Perform one-click collection of the iBMC log, and check the log information for error. Contact device vendor's technical support engineer.

- Set the host name for a device.

Figure 3-7 Setting the host name for a device



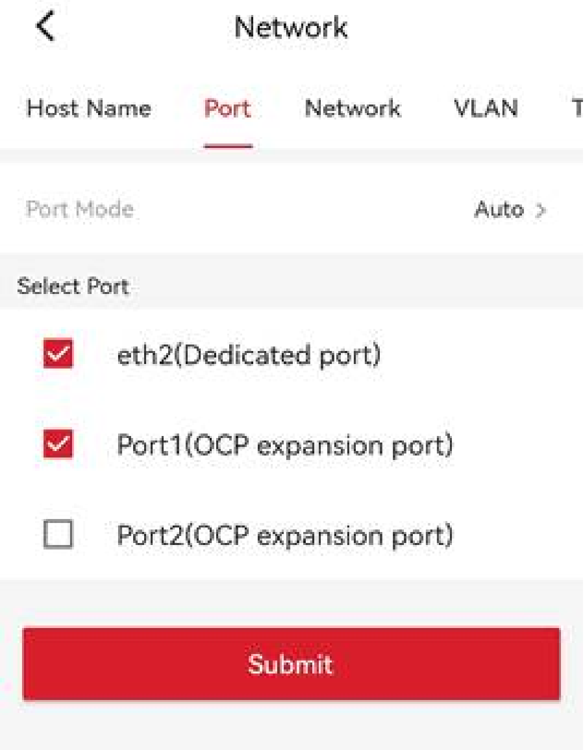
Set iBMC Host Name

Host Name 123

Enter a string of 1 to 64 characters, allowing letters, digits, and "-". The host name cannot start or end with "-".

- Set the network port mode and port for a device.

Figure 3-8 Setting the network port for a device



Port Mode: Auto

Select Port

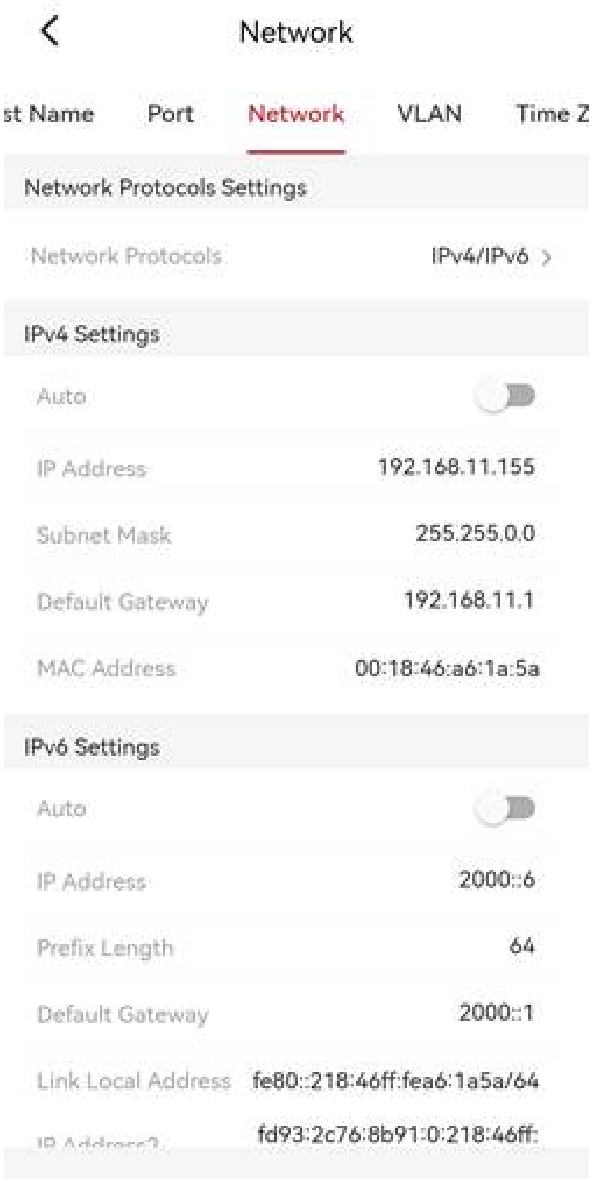
☑ eth2(Dedicated port)

☑ Port1(OCP expansion port)

□ Port2(OCP expansion port)

- Set the network protocol, IPv4, and, IPv6 for a device.

Figure 3-9 Network screen



Network Protocols Settings

Network Protocols IPv4/IPv6 >

IPv4 Settings

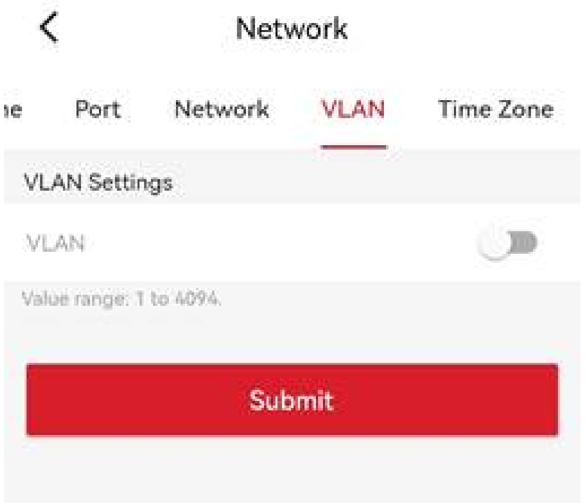
Auto	
IP Address	192.168.11.155
Subnet Mask	255.255.0.0
Default Gateway	192.168.11.1
MAC Address	00:18:46:a6:1a:5a

IPv6 Settings

Auto	
IP Address	2000::6
Prefix Length	64
Default Gateway	2000::1
Link Local Address	fe80::218:46ff:fea6:1a5a/64
IP Address2	fd93:2c76:8b91:0:218:46ff:

- Set the VLAN switch and attributes of a device.

  Figure 3-10 VLAN Setting screen



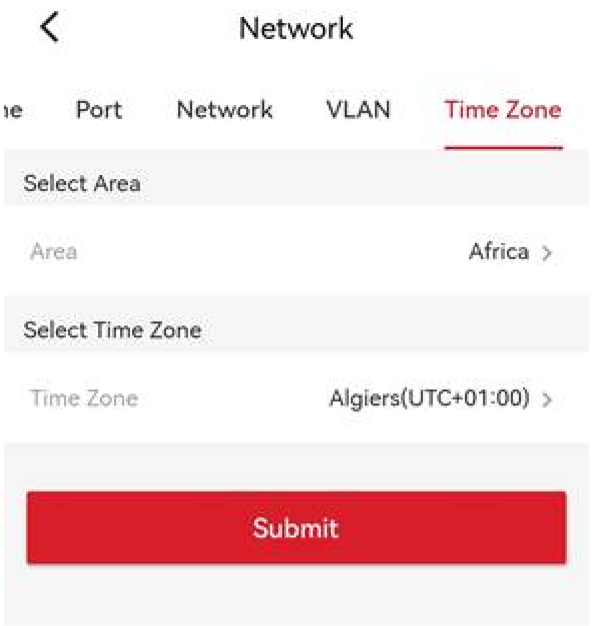
VLAN Settings

VLAN

Value range: 1 to 4094.

- Set the area and time zone for a device.

  Figure 3-11 Setting the area and the time zone



Select Area

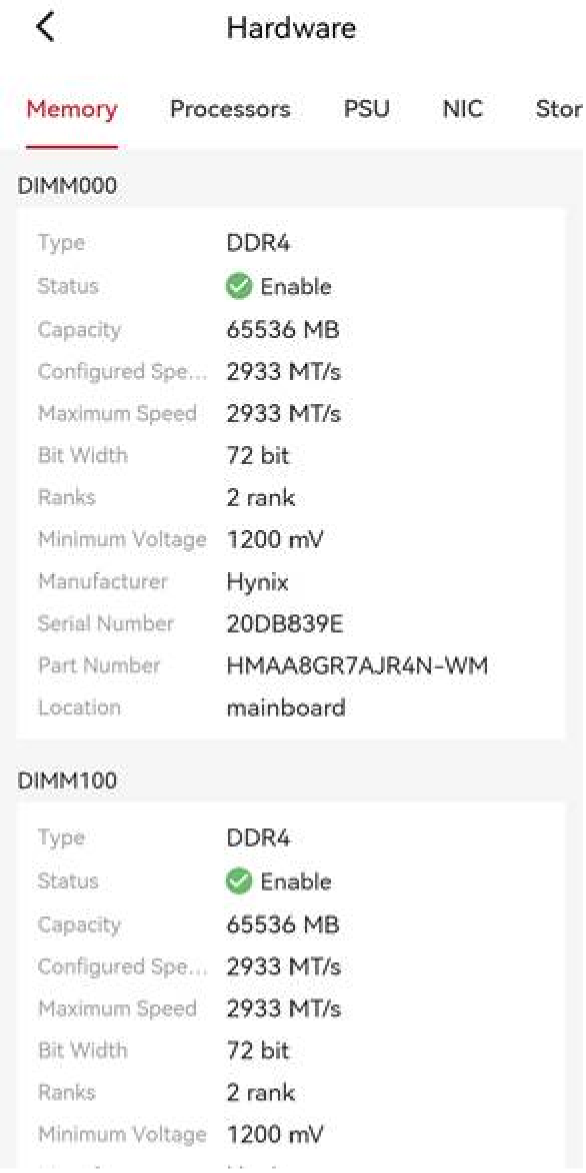
Area Africa

Select Time Zone

Time Zone Algiers(UTC+01:00)

- Display hardware information, including memory, processor, PSU, NIC, and storage.

  Figure 3-12 Hardware information



DIMM000

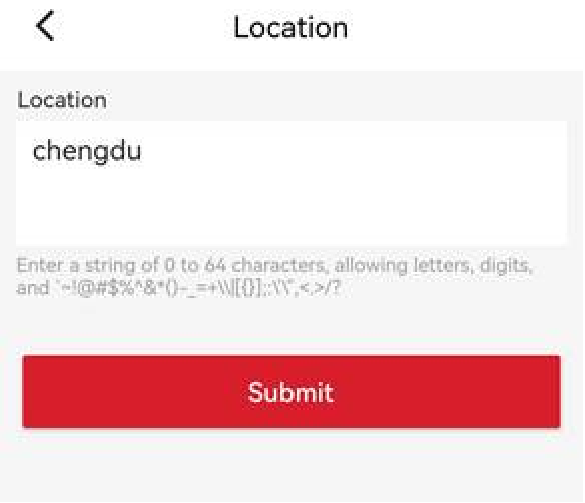
Type	DDR4
Status	✓ Enable
Capacity	65536 MB
Configured Spe...	2933 MT/s
Maximum Speed	2933 MT/s
Bit Width	72 bit
Ranks	2 rank
Minimum Voltage	1200 mV
Manufacturer	Hynix
Serial Number	20DB839E
Part Number	HMAA8GR7AJR4N-WM
Location	mainboard

DIMM100

Type	DDR4
Status	✓ Enable
Capacity	65536 MB
Configured Spe...	2933 MT/s
Maximum Speed	2933 MT/s
Bit Width	72 bit
Ranks	2 rank
Minimum Voltage	1200 mV

- Set the location of a device.

Figure 3-13 Setting the location for a device



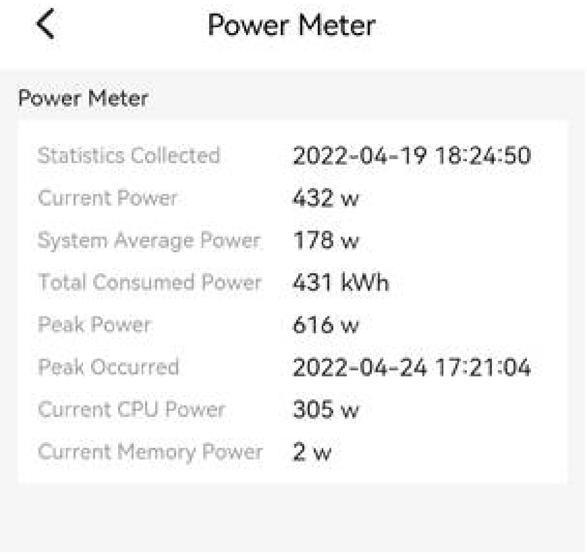
Location

chengdu

Enter a string of 0 to 64 characters, allowing letters, digits, and `~!@#$%^&*()-_=+\|[{}];:'",<.>/?

- Display device power consumption information, including the average system power, accumulated system power consumption, peak system power consumption, and component power consumption.

Figure 3-14 Power Meter screen

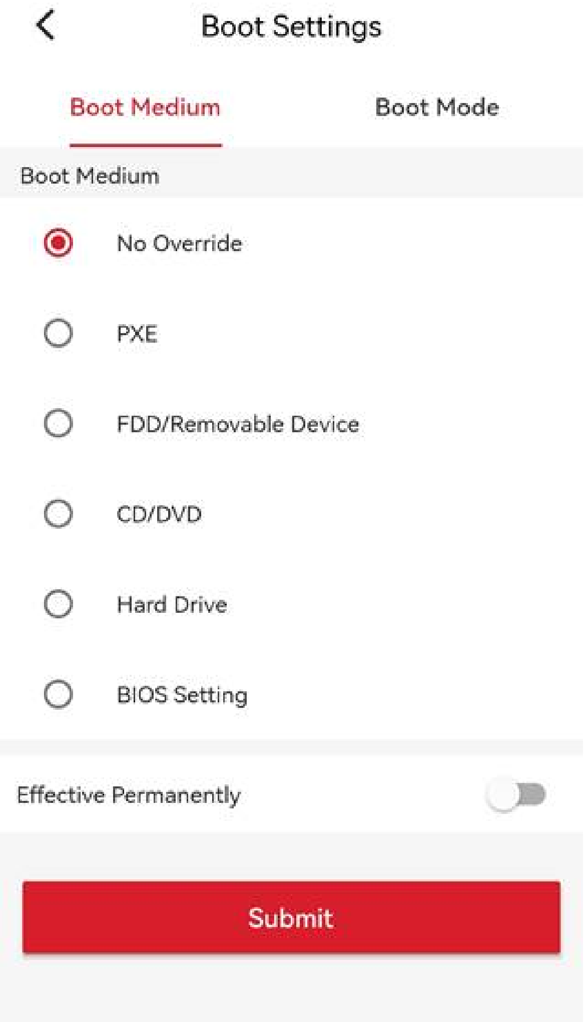


Power Meter

Statistics Collected	2022-04-19 18:24:50
Current Power	432 w
System Average Power	178 w
Total Consumed Power	431 kWh
Peak Power	616 w
Peak Occurred	2022-04-24 17:21:04
Current CPU Power	305 w
Current Memory Power	2 w

- Set the boot medium and boot mode for a server.

Figure 3-15 Boot Settings screen



Boot Settings

Boot Medium | Boot Mode

Boot Medium

● No Override

○ PXE

○ FDD/Removable Device

○ CD/DVD

○ Hard Drive

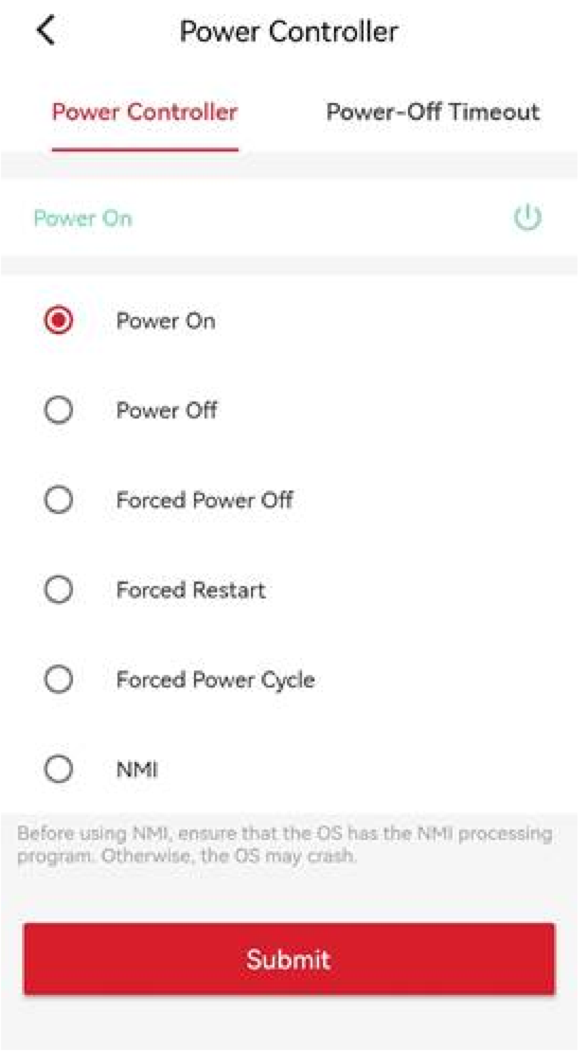
○ BIOS Setting

Effective Permanently

Submit

- Power on/off a device

Figure 3-16 Powering on/off a device



◉ Power On

○ Power Off

○ Forced Power Off

○ Forced Restart

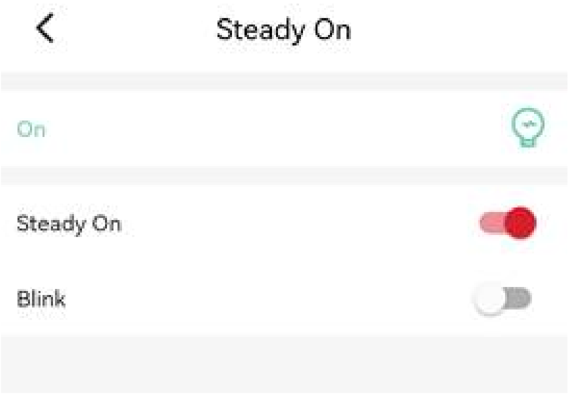
○ Forced Power Cycle

○ NMI

Before using NMI, ensure that the OS has the NMI processing program. Otherwise, the OS may crash.

- Light up the UID on a device.

Figure 3-17 Lighting up the UID on a device

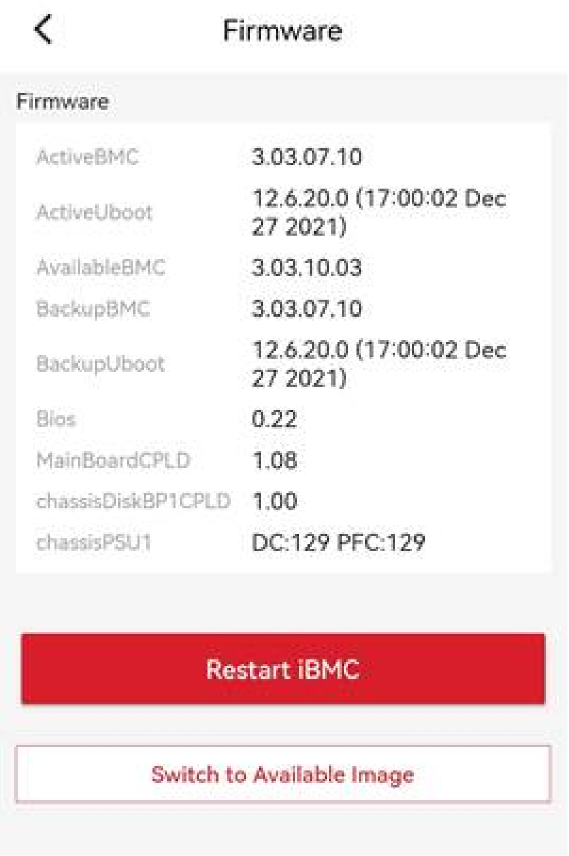


Steady On: on

Blink: off

- Display the firmware information.

Figure 3-18 Firmware information of a device



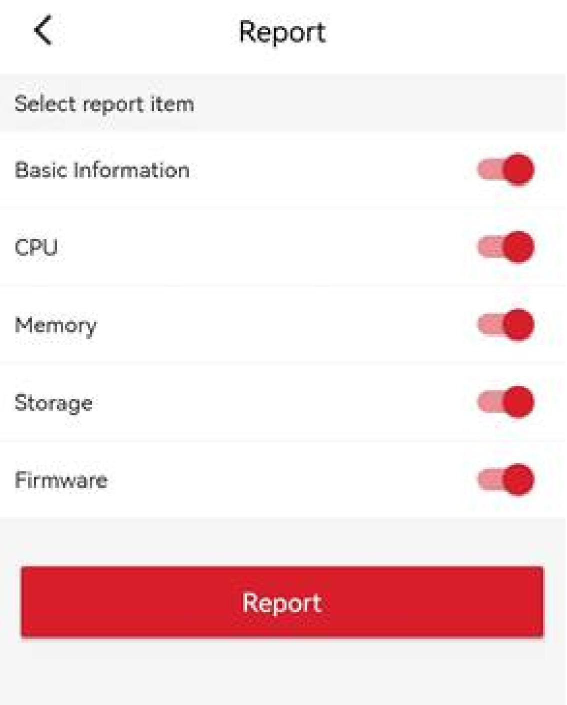
Firmware

Firmware

ActiveBMC	3.03.07.10
ActiveUboot	12.6.20.0 (17:00:02 Dec 27 2021)
AvailableBMC	3.03.10.03
BackupBMC	3.03.07.10
BackupUboot	12.6.20.0 (17:00:02 Dec 27 2021)
Bios	0.22
MainBoardCPLD	1.08
chassisDiskBP1CPLD	1.00
chassisPSU1	DC:129 PFC:129

- Output the comprehensive information report of a device.

Figure 3-19 Outputting the comprehensive information report of a device



Report

Select report item

Basic Information ●

CPU ●

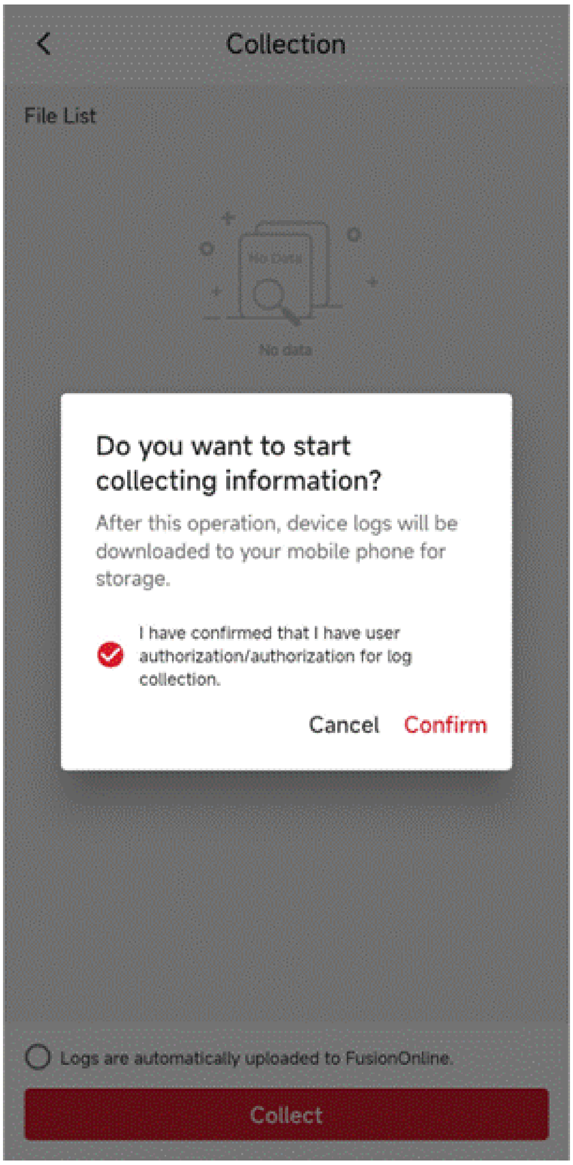
Memory ●

Storage ●

Firmware ●

- One-click to collect logs of a device.

Figure 3-20 Log collection prompt



Do you want to start collecting information?

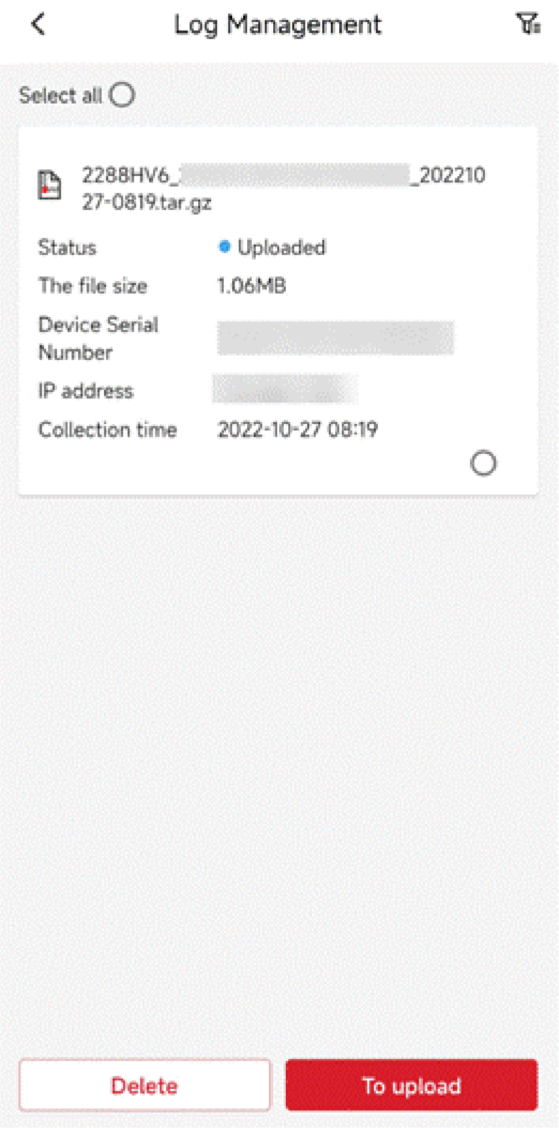
After this operation, device logs will be downloaded to your mobile phone for storage.

☑ I have confirmed that I have user authorization/authorization for log collection.

○ Logs are automatically uploaded to FusionOnline.

- Manage logs and one-click to upload logs.

Figure 3-21 Log Management screen



Log Management

Select all ○

2288HV6_[redacted]_20221027-0819.tar.gz

Status ● Uploaded

The file size 1.06MB

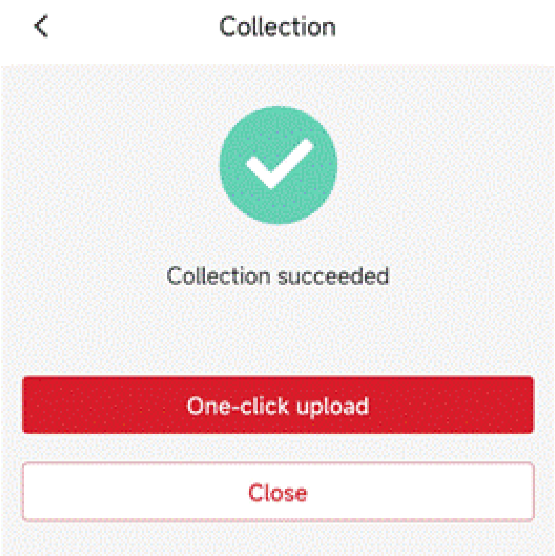
Device Serial Number [redacted]

IP address [redacted]

Collection time 2022-10-27 08:19

○

Figure 3-22 Log collection success



Collection

Collection succeeded

- Display the maintenance information of a device.
- Display the 3D image of a device.

3.2 Fault Diagnosis and Management

The iBMC provides server fault diagnosis and management (FDM), which incorporates fault detection, diagnostics, alarm reporting, and diagnosis auxiliary functions.

3.2.1 Fault Detection

The iBMC implements comprehensive monitoring of a server and provides reliable fault detection and prediction mechanisms. The iBMC can detect the following faults (the specific faults detected vary depending on the server model):

- CPU hardware faults (CAT ERROR, self-check failures, and configuration errors)
- Overtemperature alarms for air inlets, CPUs, DIMMs, power supply units (PSUs), hard drives, and RAID controller cards
- Mainboard power supply (including battery) and board power supply faults
- Fan faults
- NIC MCE/AER errors
- Precise alarm function of UCE faults for standard PCIe cards. PCIe faults will trigger alarms to specify the locations of faulty components.
- System power supply faults (AC/DC input lost, overtemperature, PSU fan faults, overvoltage, and overcurrent)
- Bus (I2C, IPMB, QPI/UPI/HCCS) faults
- DDR3/DDR4 DIMM faults (correctable and uncorrectable ECC errors, overtemperature, and configuration and initialization errors, CE overflow)
- Storage faults, including: 1) RAID controller faults (internal errors, memory UCE errors, memory ECC errors, NVRAM errors, BMC access failures). 2) Hard drive fault alarm refinement (physical faults, hard drive firmware exceptions, external hard drive configurations, pre-fault, data rebuild failures, hard drives detected but unrecognized by RAID controller cards, and SSD remaining lifespan monitoring). 3) Logical drive faults (offline, degraded). 4) BBU undervoltage or faults. 5) Link bit error (RAID controller card and drive backplane expander link bit errors, and collection of the SMART information about internal SAS and SATA drives)
- System breakdowns, black screen, and blue screen.
- The iBMA enhances the iBMC software fault identification of RAID controller cards, drives, PCIe cards, and OSs.

Table 3-4 RAID controller card and drive faults and fault locating information obtained by the iBMA

Information	LSI2208	LSI2308	LSI3008	LSI3108	SAS34/35/38/39 Series	Soft RAID	PCH Drive	NVMe	Remarks
RAID degradation	Supported	Supported	Supported	Supported	Supported	Supported	NA	NA	-
BBU fault on the RAID controller card	Not supported	Not supported	NA	Supported	Not supported	NA	NA	NA	The iBMC provides alarm information.
Drive offline	Supported	Supported	Supported	Supported	Not supported	Supported	Supported	Not supported	The iBMC provides alarm information, and supports monitoring of PCH drives on Linux and Windows.
Zero drive capacity	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Not supported	The iBMA collects alarm information about the RAID controller cards that do not support iBMC out-of-band management.
SSD life span	Supported	Supported	Supported	Supported	Not supported	Supported	Supported	Supported	The iBMC provides alarm information.

Information	LSI2208	LSI2308	LSI3008	LSI3108	SAS34/35/38/39 Series	Soft RAID	PCH Drive	NVMe	Remarks
Drive Sense Code error	Not supported	Not supported	Supported	Supported	Supported	Not supported	Supported	Not supported	The iBMC provides alarm information, and supports monitoring of PCH drives on Linux and VMware OSs.
Drive performance deterioration	Not supported	Not supported	Supported	Supported	Supported	Not supported	Supported	Not supported	The iBMC records logs and supports drive performance monitoring on Linux.
Drive SMART information	Supported	Supported	Supported	Supported	Not supported	Supported	Supported	Supported	The SMART data can be used to analyze the drive status. The iBMC records logs based on the analysis result.
Expander error code	Not supported	Not supported	Supported	Supported	Not supported	NA	NA	NA	When detecting fast increase of the expander error code, the iBMC records SELs, which help analyze link faults.
Drive log	Not supported	Not supported	Supported	Supported	Not supported	Not supported	Not supported	Not supported	The iBMC collects and analyzes drive logs.

Information	LSI2208	LSI2308	LSI3008	LSI3108	SAS34/35/38/39 Series	Soft RAID	PCH Drive	NVMe	Remarks
Drive lost	Not supported	Not supported	Supported	Supported	Not supported	Supported	Supported	Not supported	The iBMC provides alarm information.
Intermittent drive disconnection	Not supported	Not supported	Supported	Supported	Not supported	Supported	Supported	Not supported	The iBMC provides alarm information.
Drive I/O abnormality detection	Not supported	Not supported	Supported	Supported	Supported	Supported	Supported	Not supported	The iBMC provides alarm information.

The iBMA enhances the iBMC capability in monitoring the PCIe cards and OS, improving identification of PCIe card and OS faults

Table 3-5 PCIe card and OS fault information obtained by the iBMA

Category	Status Detected	Remarks
CPU	CPU usage	The iBMC provides alarm information, and alarm thresholds need to be set.
Memory	Memory usage	The iBMC provides alarm information, and alarm thresholds need to be set.
Drive	Partition usage	The iBMC provides alarm information, and alarm thresholds need to be set.
Ethernet NIC	Optical module fault	The iBMC provides alarm information, and supports detection on Linux.
	Link OAM fault	The iBMC provides alarm information, and supports detection on Linux.

Category	Status Detected	Remarks
	Link status (LinkDown, NoLink)	The iBMC records SELs of the informational level.
	Physical network port bandwidth usage	The iBMC provides alarm information, and alarm thresholds need to be set.
HBA card	Link status (LinkDown)	The iBMC records SELs of the informational level.
CNA card	Link status (LinkDown)	The iBMC records SELs of the informational level.
IB card	Link status (Disable)	The iBMC records SELs of the informational level, and supports checks on Linux.
File system	Linux file system read-on	The iBMC provides alarm information.

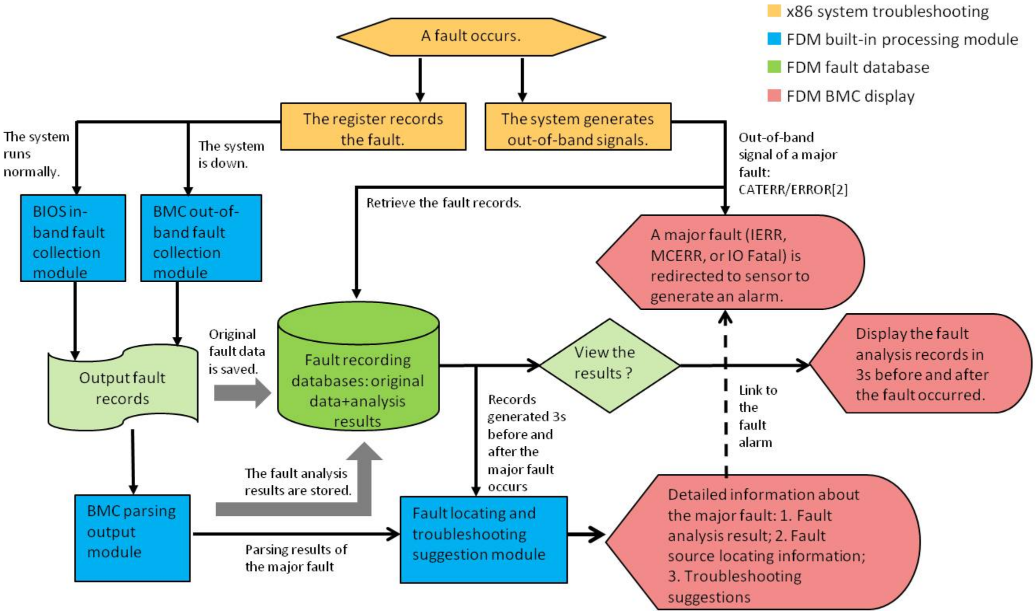
3.2.2 Fault Diagnosis

The iBMC integrates a machine check exception (MCE) fault handling system, which uses the iBMC to implement out-of-band management of hardware faults. The fault management includes data collection, logging, fault diagnosis, alarm reporting, and log export. The component health tree on the iBMC WebUI visually displays fault information about each component.

The fault handling system applies to the following scenarios:

1. A black screen is displayed on a server or the system stops responding when the server is running. No MCE data is recorded. Only CAT ERROR event is reported by the iBMC. No further information is available for locating the fault.
2. The server does not break down, but has lots of recoverable or correctable faults, for example, error-correcting codes (ECCs). You need to handle those faults promptly although they do not affect services temporarily.
3. As hardware faults hardly occur and are identified mainly based on maintenance personnel's experience, multiple insertion-removal or replacement operations cause low efficiency in fault diagnosis, which causes trouble for customers.
4. Insufficient fault information is recorded after a fault occurs.

Figure 3-4 Functions of the x86 MCE fault handling system


x86 system troubleshooting
FDM built-in processing module
FDM fault database
FDM BMC display
A fault occurs.
The register records the fault.
The system generates out-of-band signals.
The system runs normally.
The system is down.
Out-of-band signal of a major fault: CATERR/ERROR[2]
BIOS in-band fault collection module
BMC out-of-band fault collection module
Retrieve the fault records.
A major fault (IERR, MCERR, or IO Fatal) is redirected to sensor to generate an alarm.
Output fault records
Original fault data is saved.
Fault recording databases: original data+analysis results
View the results ?
Display the fault analysis records in 3s before and after the fault occurred.
Records generated 3s before and after the major fault occurs
Link to the fault alarm
The fault analysis results are stored.
BMC parsing output module
Parsing results of the major fault
Fault locating and troubleshooting suggestion module
Detailed information about the major fault: 1. Fault analysis result; 2. Fault source locating information; 3. Troubleshooting suggestions

The fault handling system has the following technical features:

- Captures complete fault data automatically.

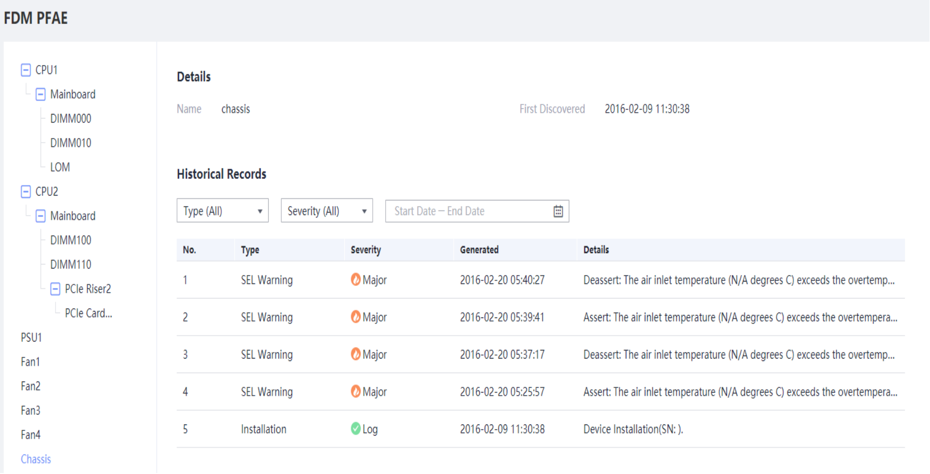
  The iBMC integrates in-band and out-of-band fault data collection technologies.
- Provides an iBMC-centered out-of-band fault handling system with sustainable development.
- After collecting fault data, iBMC analyzes them, reports alarms, generates logs through out-of-band interfaces, preventing problems caused by using the OS as the troubleshooting center, for example, insufficient processing capability, uncontrollable management, and reduced system performance. iBMC can locate faults on components of specific silkscreen markings.

3.2.3 Proactive Failure Analysis

The iBMC of V5 servers, such as the 2288H V5 server, supports the Proactive Failure Analysis Engine (PFAE) and provides warning for CPUs, DIMMs, hard drives, RAID controller cards, and NICs.

The iBMC WebUI supports query of historical PFA events.

Figure 3-5 FDM PFAE



FDM PFAE

Details

Name chassis First Discovered 2016-02-09 11:30:38

Historical Records

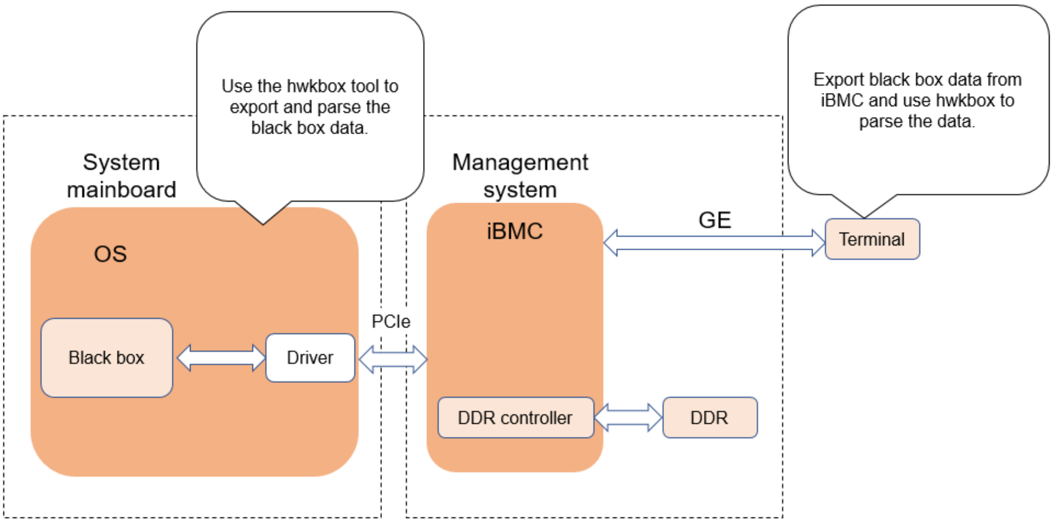
Type (All) ▾ Severity (All) ▾ Start Date – End Date

No.	Type	Severity	Generated	Details
1	SEL Warning	Major	2016-02-20 05:40:27	Deassert: The air inlet temperature (N/A degrees C) exceeds the overtemp...
2	SEL Warning	Major	2016-02-20 05:39:41	Assert: The air inlet temperature (N/A degrees C) exceeds the overtempera...
3	SEL Warning	Major	2016-02-20 05:37:17	Deassert: The air inlet temperature (N/A degrees C) exceeds the overtemp...
4	SEL Warning	Major	2016-02-20 05:25:57	Assert: The air inlet temperature (N/A degrees C) exceeds the overtempera...
5	Installation	✓ Log	2016-02-09 11:30:38	Device Installation(SN:).

3.2.4 System Running Recorder

The iBMC provides the system running recorder function. The system running recorder consists of a black box (KBox) module, iBMC, and analysis tool (hwkbox). The function is disabled by default. Figure 3-6 shows how the Linux system running recorder works. The system running recorder records the kernel stack information when kernel panic occurs, and exports and provides the information to the third party. The third party defines the information itself. The fault data (black box data) cannot be lost upon system startup and power-on or power off, but can be lost only at AC power failure.

Figure 3-6 System running recorder



Use the hwkbox tool to export and parse the black box data.
Export black box data from iBMC and use hwkbox to parse the data.
System mainboard
OS
Black box
Driver
PCIe
Management system
iBMC
GE
Terminal
DDR controller
DDR

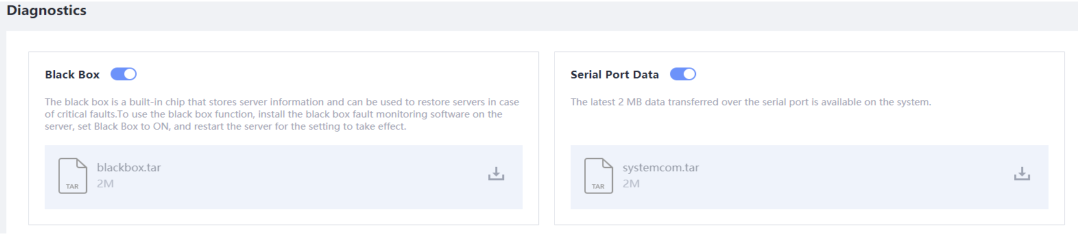
Application scenario 1

When kernel panic occurs, the registered black box automatically records the kernel stack information and saves the location information to a DDR using a DDR controller over a PCIe interface. Only 4 MB data can be saved. After the system restarts, a system-side location tool reads and analyzes the location information in the DDR over the PCIe interface. Even if the system cannot be started, iBMC can export the information from the DDR (as shown in **Figure 3-7**) and analyzes the information using a dedicated analysis tool. Currently, the location information can be exported only to the OS and analyzed using the hwkbox analysis tool.

Application scenario 2

The third-party application records a maximum of 4 MB run logs to the iBMC DDR memory using a write interface of the black box. When the application is faulty, the system reads and analyzes the run logs using a read interface on the black box or iBMC. This facilitates fault location.

Figure 3-7 Downloading black box data



Diagnostics

Black Box

The black box is a built-in chip that stores server information and can be used to restore servers in case of critical faults.To use the black box function, install the black box fault monitoring software on the server, set Black Box to ON, and restart the server for the setting to take effect.

blackbox.tar
2M

Serial Port Data

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

systemcom.tar
2M

3.2.5 Startup Self-Check Code

A startup self-check code records information about the self-check performed upon system startup. The information indicates whether a specific fault occurs. Different codes indicate different faults. You can locate the startup faults by querying the fault code table, as shown in the following. Digits in the square brackets indicate the fault code.

```
iBMC:/->ipmcget -d port80
port80 diagnose code:
02-03-06-70-74-76-7C-A1-A3-A3-A7-A9-A7-A7-A7-A8
A9-A9-A9-AA-AA-AA-AE-AF-B0-B1-B4-B2-B3-B6-B7-B8
B9-BA-B7-BB-BC-BF-83-4B-52-4D-4B-59-5A-A2-10-11
12-13-15-FF-20-1A-1A-16-17-18-1D-26-16-17-18-16
17-18-27-28-F9-[59]-5A-A2-10-11-12-13-15-FF-20-1A
1A-16-17-18-1D-26-16-17-18-16-17-18-27-28-F9-7B
C5-C3-25-2F-F8-E0-60-FB-D0-41-E0-8B-13-CA-13-EC
91-39-2D-AD-FE-6E-E4-12-F3-D9-64-DB-02-14-CD-78
E5-CF-A9-2E-34-25-2B-5A-57-18-17-F5-5E-0C-D5-BC
D0-E7-FB-E0-41-4C-FE-52-46-B5-41-BA-90-85-1B-54
D2-C2-E6-61-DA-EA-B9-58-4D-2F-09-84-93-F1-3A-0B
25-E2-1E-0D-8E-17-0A-F2-57-6B-A2-97-3A-53-1F-D5
8B-6B-F6-CD-D5-BB-C6-18-E8-85-5C-D7-68-68-52-9A
B1-67-47-A2-EC-CB-52-F9-D8-D4-74-0A-E9-23-7A-C4
FE-28-74-A7-1C-F3-C2-0C-E5-BF-D0-BC-88-05-22-1B
71-E9-AE-F1-E3-0C-BB-83-FD-10-BA-53-3B-86-B0-40
```

3.2.6 Event Management

iBMC provides the following alarm management functions:

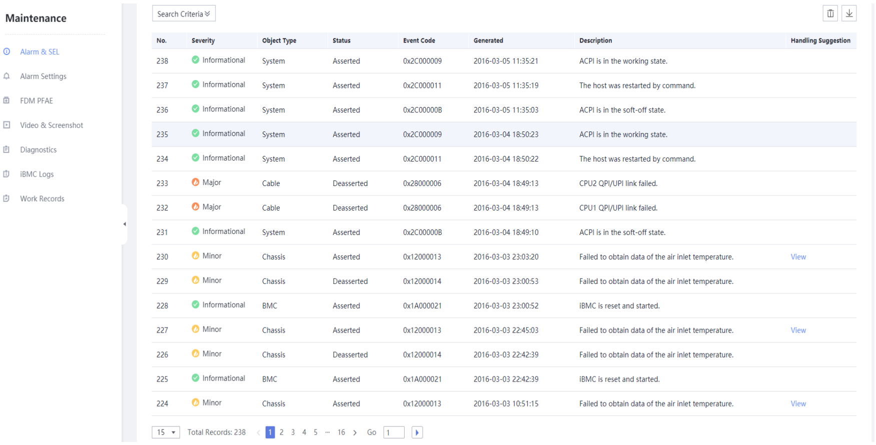
- Monitoring and alarm management for all hardware
- Detailed log description
- Local storage and archiving
- Log management based on visualization, filtering, sorting, and downloading
- Remote alarm reporting over SNMP trap, and emails, syslogs, and Redfish events

- Alarm reporting to multiple destinations
- Display of alarm handling suggestions and event codes

System events are recorded in files in real time. When 2000 events are recorded, automatic backup occurs. Only one backup file can be saved. If there are more than one file, the earlier backup file is automatically deleted.

The page displaying system events allows you to query, sort, filter, and clear all system events, as shown in **Figure 3-8**.

Figure 3-8 Page displaying system events



No.	Severity	Object Type	Status	Event Code	Generated	Description	Handling Suggestion
238	Informational	System	Asserted	0x2C000009	2016-03-05 11:35:21	ACPI is in the working state.	
237	Informational	System	Asserted	0x2C000011	2016-03-05 11:35:19	The host was restarted by command.	
236	Informational	System	Asserted	0x2C00000B	2016-03-05 11:35:03	ACPI is in the soft-off state.	
235	Informational	System	Asserted	0x2C000009	2016-03-04 18:50:23	ACPI is in the working state.	
234	Informational	System	Asserted	0x2C000011	2016-03-04 18:50:22	The host was restarted by command.	
233	Major	Cable	Deasserted	0x28000006	2016-03-04 18:49:13	CPU2 QPI/UPI link failed.	
232	Major	Cable	Deasserted	0x28000006	2016-03-04 18:49:13	CPU1 QPI/UPI link failed.	
231	Informational	System	Asserted	0x2C00000B	2016-03-04 18:49:10	ACPI is in the soft-off state.	
230	Minor	Chassis	Asserted	0x12000013	2016-03-03 23:03:20	Failed to obtain data of the air inlet temperature.	View
229	Minor	Chassis	Deasserted	0x12000014	2016-03-03 23:00:53	Failed to obtain data of the air inlet temperature.	
228	Informational	BMC	Asserted	0x1A000021	2016-03-03 23:00:52	iBMC is reset and started.	
227	Minor	Chassis	Asserted	0x12000013	2016-03-03 22:45:03	Failed to obtain data of the air inlet temperature.	View
226	Minor	Chassis	Deasserted	0x12000014	2016-03-03 22:42:39	Failed to obtain data of the air inlet temperature.	
225	Informational	BMC	Asserted	0x1A000021	2016-03-03 22:42:39	iBMC is reset and started.	
224	Minor	Chassis	Asserted	0x12000013	2016-03-03 10:51:15	Failed to obtain data of the air inlet temperature.	View

Table 3-6 describes the system event parameters.

Table 3-6 System event parameters

Parameter	Description
Severity	Indicates the severity level of the event. Values: **Informational**, **Minor**, **Major**, and **Critical**
No.	Serial number of a system event.
Generated	Date and time when the system event was generated.
Description	Supplementary information about the system event.
Object Type	Component for which the system event was generated.
Status	Indicates the current status of the event. Values: **Asserted** and **Deasserted**
Event Code	Uniquely identifies the system event.
Handling Suggestion	Suggestions on how to clear the system event.

3.2.7 Fault Reporting

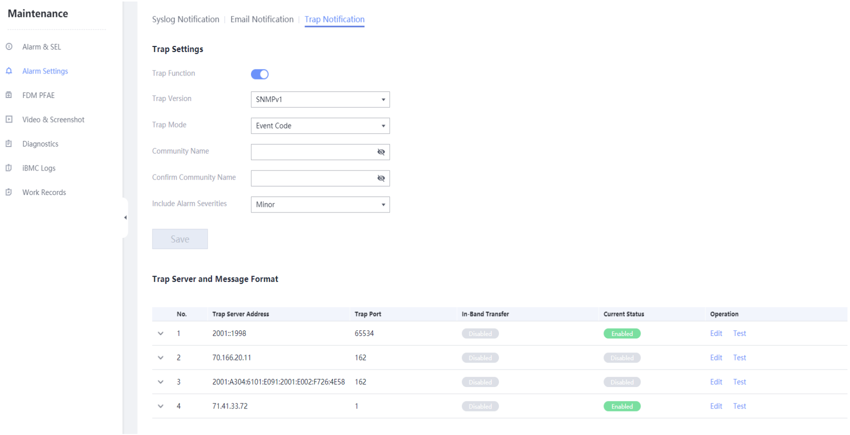
The iBMC monitors hardware and system status in real time and reports alarms to remote destination servers over SNMP trap, email, syslog, and Redfish events.

SNMP trap supports the following features: A maximum of four destinations. You can set status, IP addresses, ports, and alarm formats for the destinations. Event reporting based on severity. Versions of v1, v2c, and v3. SNMPv1 is enabled by default. If you use SNMPv3, select a trap v3 security user from local users and configure v3 authentication and encryption algorithms. Host identifiers and location contained in trap messages. A host identifier can be a board SN, product asset label, or host name. Test messages can be sent to the destinations. See **Figure 3-9**.

SMTP supports a maximum of four destinations. The following operations are supported: Set the addresses and states of the mail boxes that receive logs and alarms. Send test mails to the destinations. Log in to the SMTP server with or without authentication. Enable TLS to encrypt mails. Configure the title and mail sender of the email template. See **Figure 3-10**.

Syslog supports the following functions: enabling or disabling syslog notifications; log-level filtering; a maximum of four receiving destinations, each can be configured with a server address (IPv4, IPv6, or FQDN), a port number, the log type, and status (enabled or disabled); sending test information to the receiving destination; reporting of three types of logs (security logs, operation logs, and system events); carrying host ID when logs are reported; Encrypting reported logs by TLS; two-way authentication for the sending and receiving ends based on the imported certificate.

Figure 3-9 SNMP trap configuration page



Trap Settings

Trap Function: ●

Trap Version: SNMPv1

Trap Mode: Event Code

Community Name:

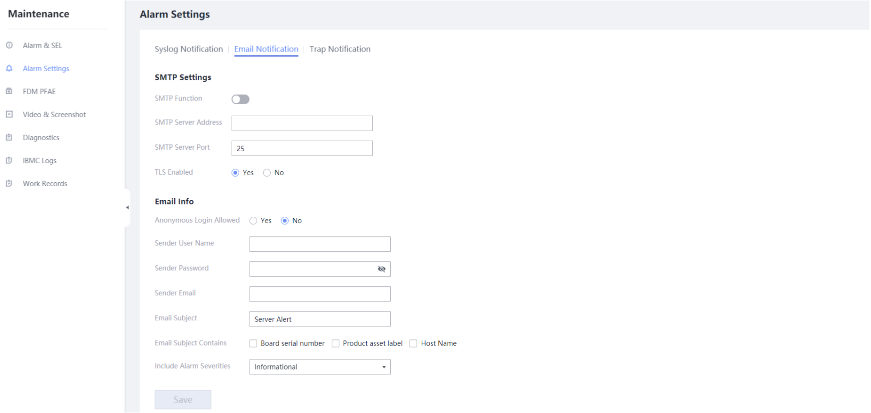
Confirm Community Name:

Include Alarm Severities: Minor

Trap Server and Message Format

No.	Trap Server Address	Trap Port	In-Band Transfer	Current Status	Operation
1	2001::1998	65534	Disabled	Enabled	Edit Test
2	70.166.20.11	162	Disabled	Disabled	Edit Test
3	2001:A304:6101:E091:2001:E002:F726:4E58	162	Disabled	Disabled	Edit Test
4	71.41.33.72	1	Disabled	Enabled	Edit Test

Figure 3-10 SMTP configuration page



SMTP Settings

SMTP Function

SMTP Server Address

SMTP Server Port: 25

TLS Enabled: ● Yes ○ No

Email Info

Anonymous Login Allowed: ○ Yes ● No

Sender User Name

Sender Password

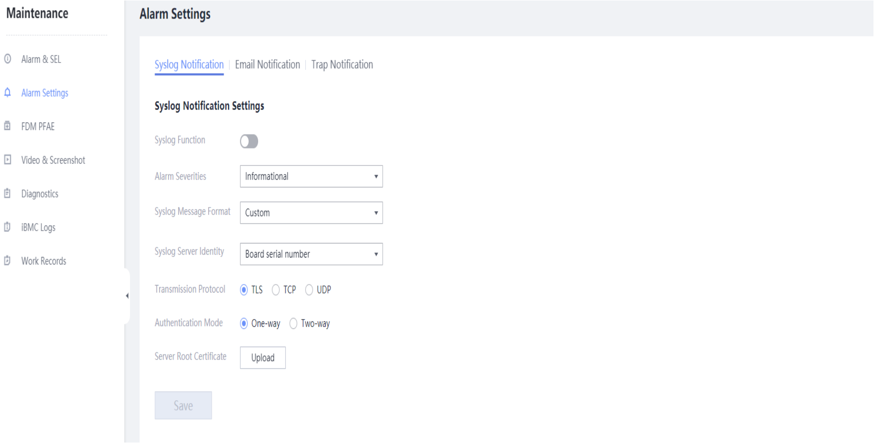
Sender Email

Email Subject: Server Alert

Email Subject Contains: □ Board serial number □ Product asset label □ Host Name

Include Alarm Severities: Informational

Figure 3-11 Syslog configurations page



Syslog Notification Settings

Syslog Function

Alarm Severities: Informational

Syslog Message Format: Custom

Syslog Server Identity: Board serial number

Transmission Protocol: ● TLS ○ TCP ○ UDP

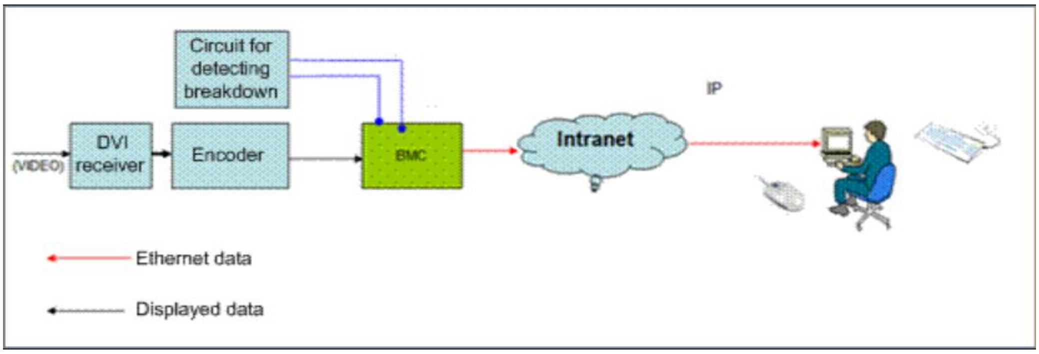
Authentication Mode: ● One-way ○ Two-way

Server Root Certificate

3.2.8 Breakdown Screenshot

When detecting a system breakdown, the iBMC stores the last screenshot in the specified format in the iBMC storage space, as shown in **Figure 3-12**. You can log in to iBMC to view the screenshot or remotely download the screenshot to a local folder to locate a fault.

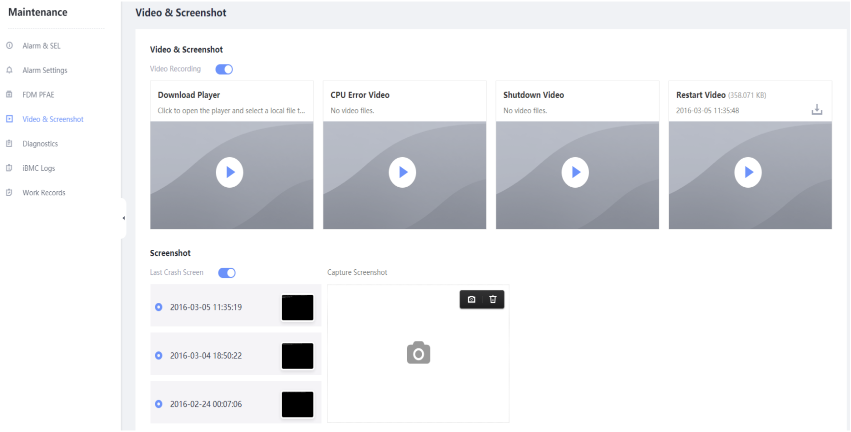
Figure 3-12 Rule of the breakdown screenshot



The iBMC supports a maximum of three breakdown screenshots. The earliest screenshot will be overwritten when a new screenshot is created.

You can log in to the WebUI to check the created screenshots. For details, see **Figure 3-13**.

Figure 3-13 Breakdown screenshot

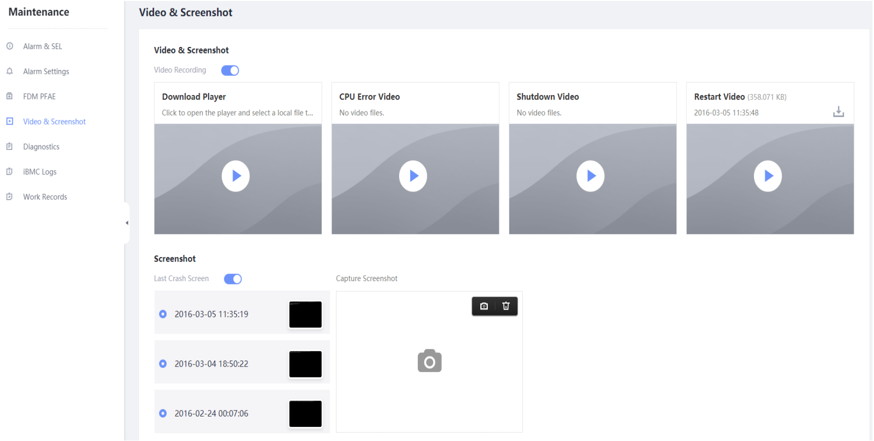


3.2.9 Breakdown Video

When the iBMC detects a system breakdown, it records the screen output that was displayed 1 minute before the breakdown and stores the compressed screen video to an external storage device. the iBMC supports automatic video recording when the host CAT error, system power-off, or system restart occurs. For the host CAT error, the video files are stored in the iBMC flash memory, and for the other two situations, the video files are stored in the iBMC memory. When a server breaks down, you can log in to iBMC to export the video file to a local folder and view the video using the video playback console for fault location.

Figure 3-14 shows the video playback console.

Figure 3-14 Video playback console



3.2.10 Screen Snapshot

The screen snapshot function is designed for system inspection. You can capture and save the screen outputs of the system using the CLI and WebUI. You can remotely obtain screen outputs from a local client and view screens of all inspected servers using Secure File Transfer Protocol (SFTP).

Compared with the virtual KVM, the screen snapshot does not need login over HTTPS. You can obtain screen snapshots by using the CLI. The CLI allows scripts to be executed, which facilitates automatic server inspection. You can also obtain current system screen snapshots on the WebUI.

Obtaining Screen Snapshots Using the CLI

- Syntax

```
ipmcset -d printscreen -v wakeup
```

- Parameter description

  When the **wakeup** parameter is used, the system takes a screenshot for the current information and is woken up from the Screen Saver mode.

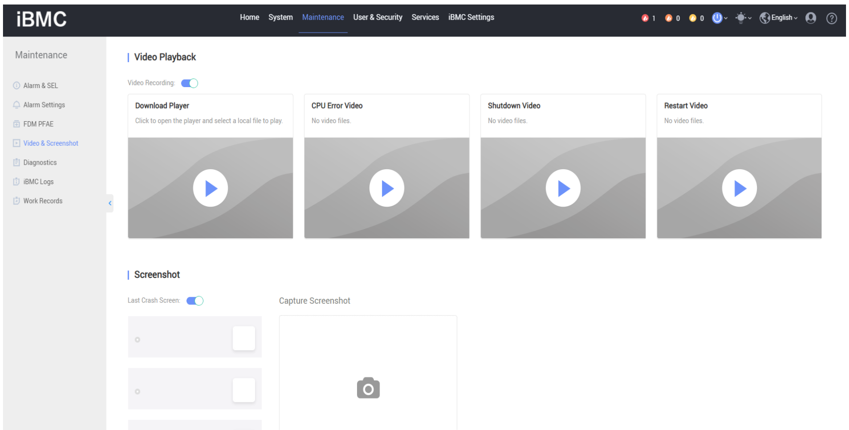
- Usage guidelines

  After the **printscreen** command is executed, iBMC automatically saves the screenshot as the **screen.jpg** file to the **tmp** directory. You need to load the file to a client that supports viewing **.jpg** files over SFTP before viewing the screenshot.

Obtaining Screen Snapshots from the Web Page

On the iBMC WebUI, you can choose **Events and Logs** > **Remote System Screen** > **Manual** to obtain the screen snapshot, as shown in **Figure 3-15**.

Figure 3-15 Obtaining screen snapshots



Video Recording: on

Download Player: Click to open the player and select a local file to play.

CPU Error Video: No video files.

Shutdown Video: No video files.

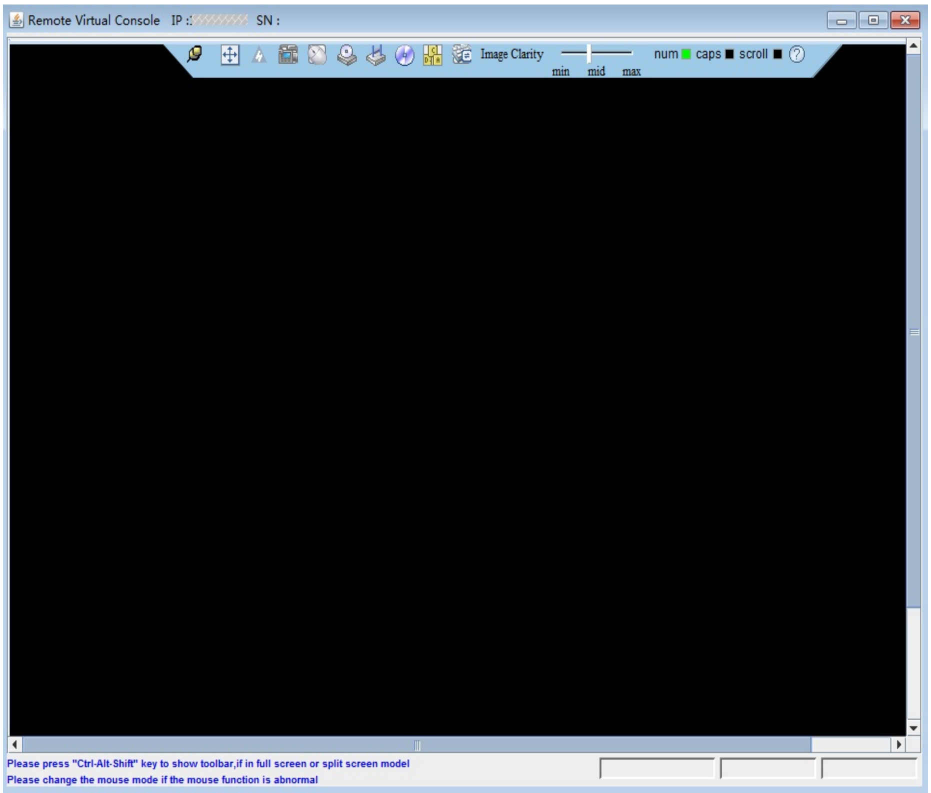
Restart Video: No video files.

Last Crash Screen: on

3.2.11 Screen Video

The screen video is a remote KVM recording function provided by the remote console, and can be enabled. The video format is defined by a user and the video file is saved in the local (the KVM console is opened). It records virtual KVM operations to ensure security or meet other special requirements. When the screen video function is enabled, the virtual KVM console automatically records all information displayed on the screen and all operations that have been performed to a self-defined video file.

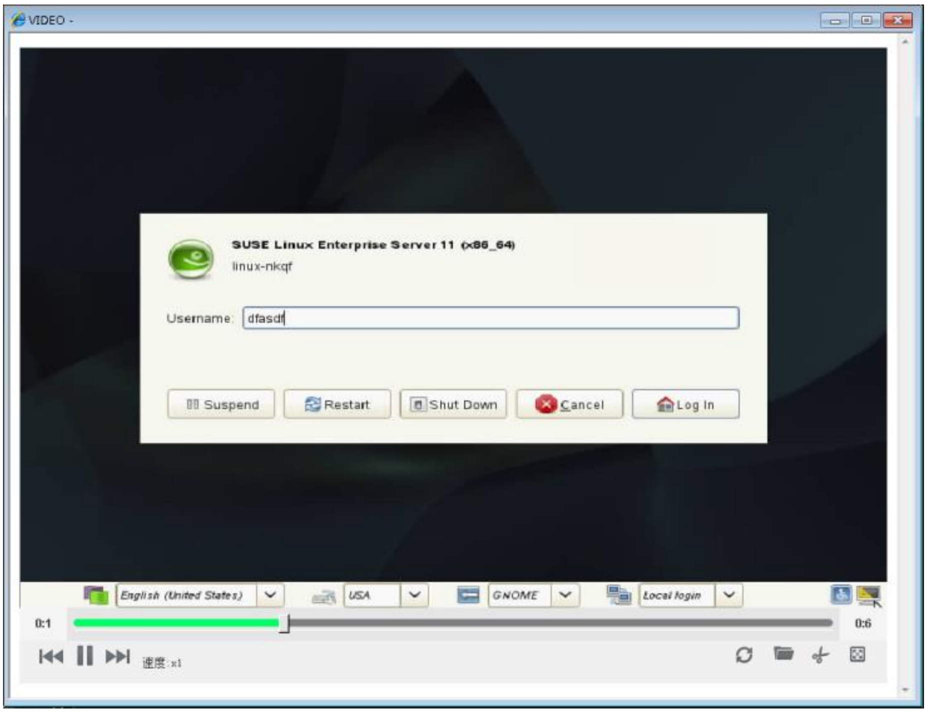
Figure 3-16 Enabling/Disabling the screen video function



Please press "Ctrl-Alt-Shift" key to show toolbar,if in full screen or split screen model
Please change the mouse mode if the mouse function is abnormal

iBMC integrates a video file playback tool for playing videos.

Figure 3-17 Video playback console



Username: dfasdf

3.2.12 Parts Replacement Records

CPU, memory, and drive faults often occur during routine maintenance. Some faults are caused by incompatible components after parts replacement. It is difficult to locate fault when there is no historical information about the component. For the faults that occur occasionally, the faults cannot be reproduced due to lack of historical information about the component, and only theoretical analysis can be performed. As a result, the root cause of the faults cannot be located. The iBMC provides parts replacement records from V5 series servers.

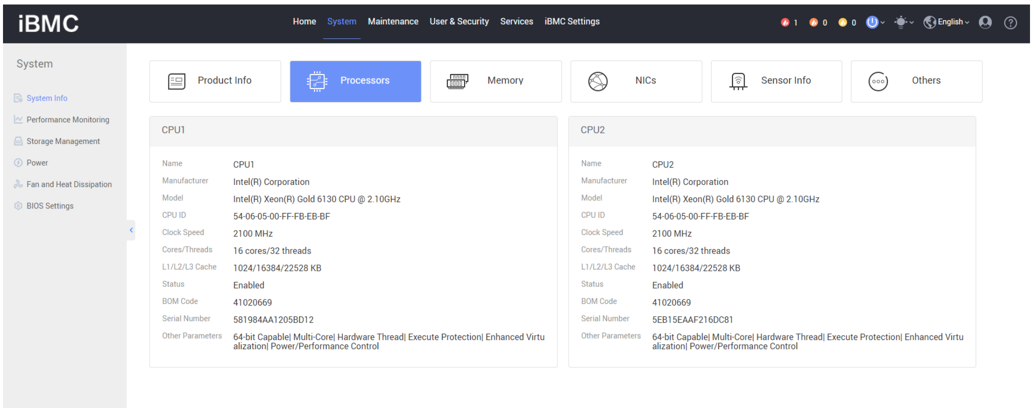
After a CPU, DIMM or drive is replaced, the iBMC generates a parts replacement event when the server is powered on again. The event information contains the SNs of the old and new components. The iBMC provides parts replacement events only for NVMe drives and the drives that support out-of-band management. For example, if a DIMM is replaced, the following event is generated after the server is powered on:

DIMM000 is replaced from SN(39D06B9B) to SN(39186EF0).

3.2.13 BOM Code Management

A BOM code refers to a part number that uniquely identifies a component in the production system. When a faulty component needs to be replaced, you can query information about the new component in the production system based on the part number. You can query part numbers on the iBMC WebUI, Redfish interface, alarm logs, and information obtained in one-click collection mode. The iBMC provides part numbers of the mainboard, PSUs, fan modules, CPUs, and DIMMs.

The following uses the memory as an example to describe the part numbers on the web page:



	CPU1	CPU2
Name	CPU1	CPU2
Manufacturer	Intel(R) Corporation	Intel(R) Corporation
Model	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
CPU ID	54-06-05-00-FF-FB-EB-BF	54-06-05-00-FF-FB-EB-BF
Clock Speed	2100 MHz	2100 MHz
Cores/Threads	16 cores/32 threads	16 cores/32 threads
L1/L2/L3 Cache	1024/16384/22528 KB	1024/16384/22528 KB
Status	Enabled	Enabled
BOM Code	41020669	41020669
Serial Number	581984AA1205BD12	5EB15EAAF216DC81
Other Parameters	64-bit Capable| Multi-Core| Hardware Thread| Execute Protection| Enhanced Virtualization| Power/Performance Control	64-bit Capable| Multi-Core| Hardware Thread| Execute Protection| Enhanced Virtualization| Power/Performance Control

If a DIMM is fault, the following alarm information is displayed:

DIMM000 configuration error or training failed(SN:39D06B9B,PN:131E9E8C).

3.2.14 System Watchdog

The iBMC supports the standard watchdog timer defined in the IPMI standards. The watchdog timer can be used together with the OS management software or the BIOS to monitor the OS or BIOS operating status and rectify faults. The iBMC provides IPMI commands for setting the watchdog timeout period and processing actions after timeout, as well as commands for resetting the watchdog. If the iBMC does not receive the command for resetting the watchdog before it times out, the iBMC can perform the user-specified actions (such as No Action, Power Off, Hard Reset and Power Cycle) to recover the system.

3.3 Virtual KVM and Virtual Media

On the remote control, you can use the virtual KVM, virtual media, and manual recording functions, and you can also power on, power off, and restart the system. The remote console supports Java and HTML5. The remote console JAR package uses CA signature by default. **Figure 3-18** shows the Java remote console, and **Figure 3-19** shows the HTML5 remote console. The HTML5 remote console supports English (American), Japanese, and Italian keyboards.

The remote console supports full-screen mode and windowed mode. You can press **Ctrl+Alt+Shift** to show the toolbar.

The remote console can trigger automatic system locking upon logout, which effectively prevents system information leakage or intrusion.

The remote console can be opened in the following ways:

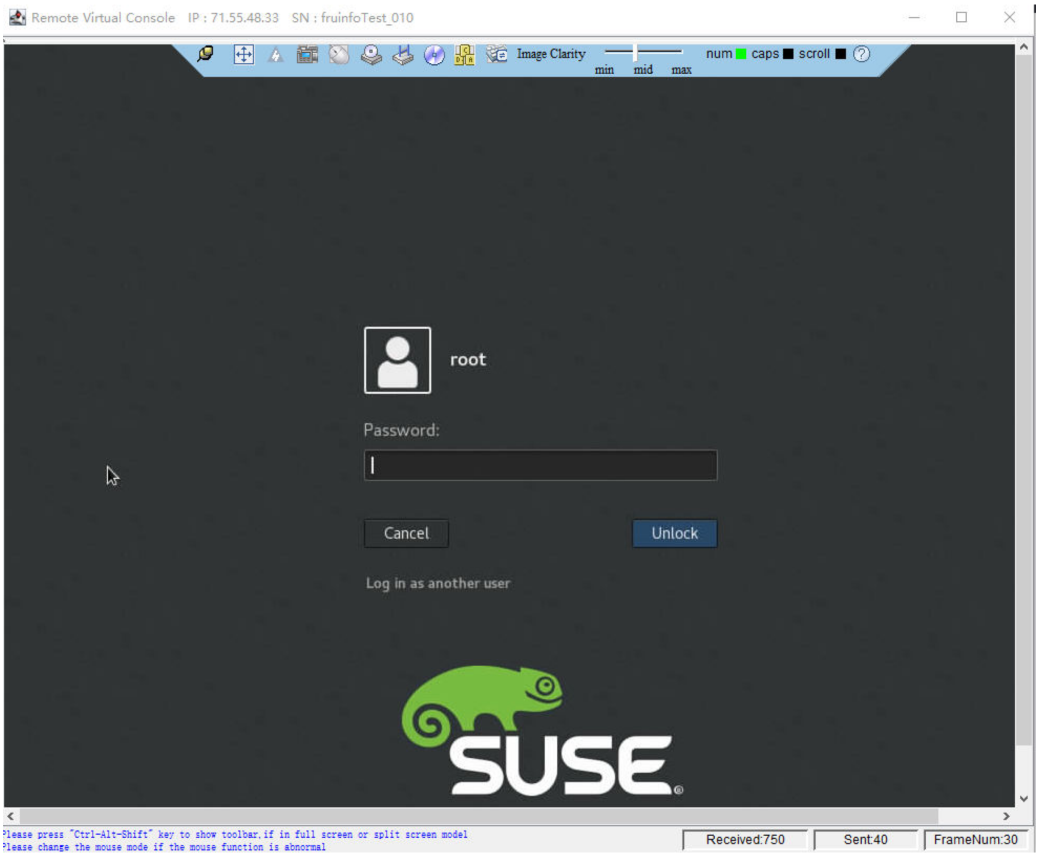
1. Open the Java remote console using the iBMC WebUI or URL. Java Network Launch Protocol (JNLP) is used instead of Netscape Plugin Application Programming Interface (NPAPI), which is not supported by Chrome 45 and later versions.
2. Open the independent remote console. The independent remote console does not depend on the browser or JRE version. It supports the following OSs: Windows 7 (32-bit/64-bit), Windows 8 (32-bit/64-bit), Windows 10 (32-bit/64-bit), Windows Server 2008 R2 (32-bit/64-bit), Windows Server 2012 (64-bit), Ubuntu 14.04 LTS, and Ubuntu 16.04 LTS. For details, see **Figure 3-20**.
3. Open the remote console from a Virtual Network Computing (VNC) client. The iBMC supports standard VNC and mainstream VNC clients, including RealVNC, TightVNC, UltraVNC, and TigerVNC. Only V5 servers support VNC clients. **Figure 3-21** shows a VNC client.
4. Open the HTML5 remote console using the iBMC WebUI or URL. HTML JS is used to load the remote console.

Table 3-7 Comparison of remote consoles

Category	Advantages	Disadvantages	Remarks
HTML5 integrated remote console	● JRE-independent ● Users do not need to download the program package.	● Used with certain browser versions ● Does not support virtual folder.	Only V5 servers support the HTML5 integrated remote console.

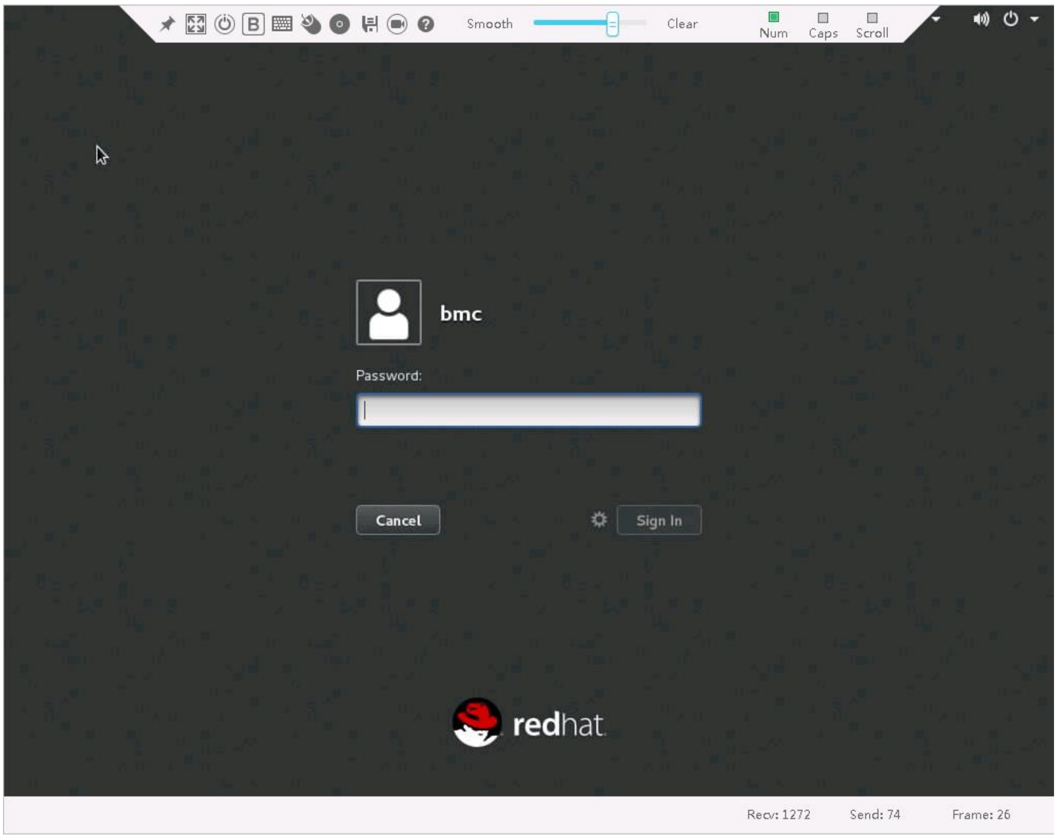
Category	Advantages	Disadvantages	Remarks
Java integrated remote console	● Supports all KVM functions.	● JRE must be installed. ● Browsers of later versions do not support applet start. JNLP start must be used.	-
VNC console	● Compatible with third-party clients ● JRE-independent	● Does not support virtual media. ● Only password-based authentication is supported.	Only V5 servers support the VNC console.
Java independent remote console	● Comes with JRE.	● JRE-dependent ● Poor portability	-

Figure 3-18 Java remote console (web integrated)



```
Please press "Ctrl-Alt-Shift" key to show toolbar,if in full screen or split screen model
Please change the mouse mode if the mouse function is abnormal
```

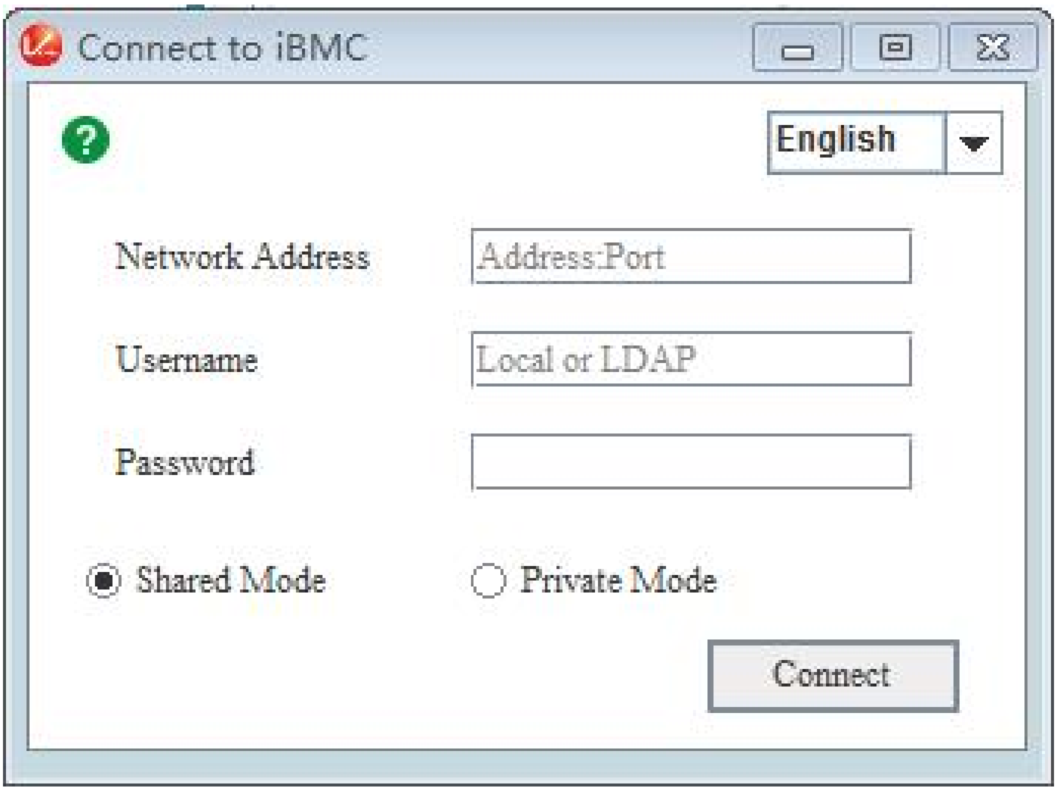
Figure 3-19 HTML5 remote console (web integrated)



NOTE

The HTML5 remote console does not require additional software. The supported browser versions are as follows: Internet Explorer 10 or later, Firefox 39 or later, and Chrome 21 or later.

Figure 3-20 Java console (independent)



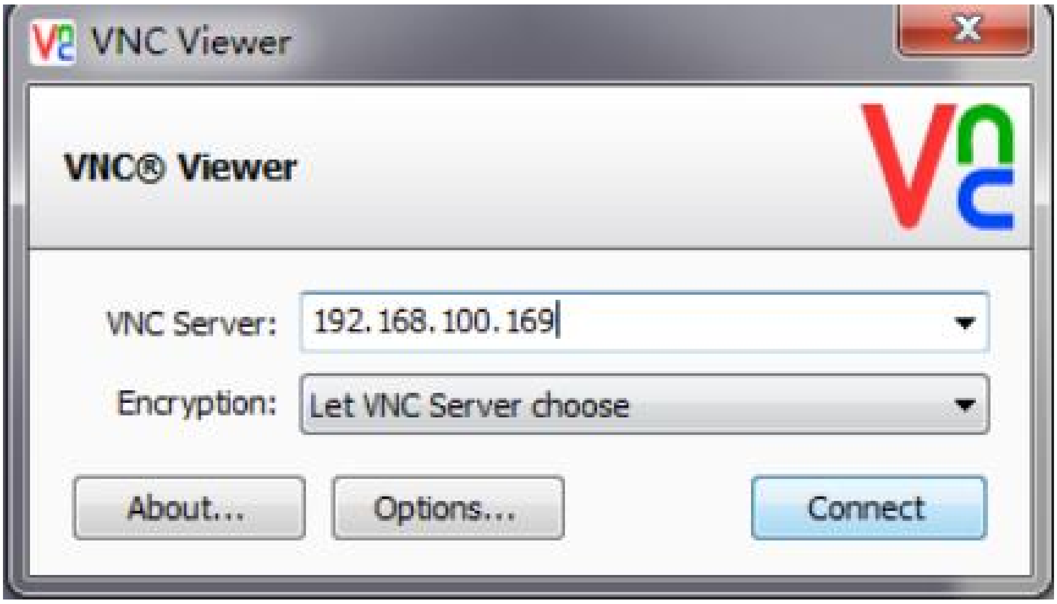
Network Address: Address:Port

Username: Local or LDAP

Password:

● Shared Mode ○ Private Mode

Figure 3-21 VNC client (independent)



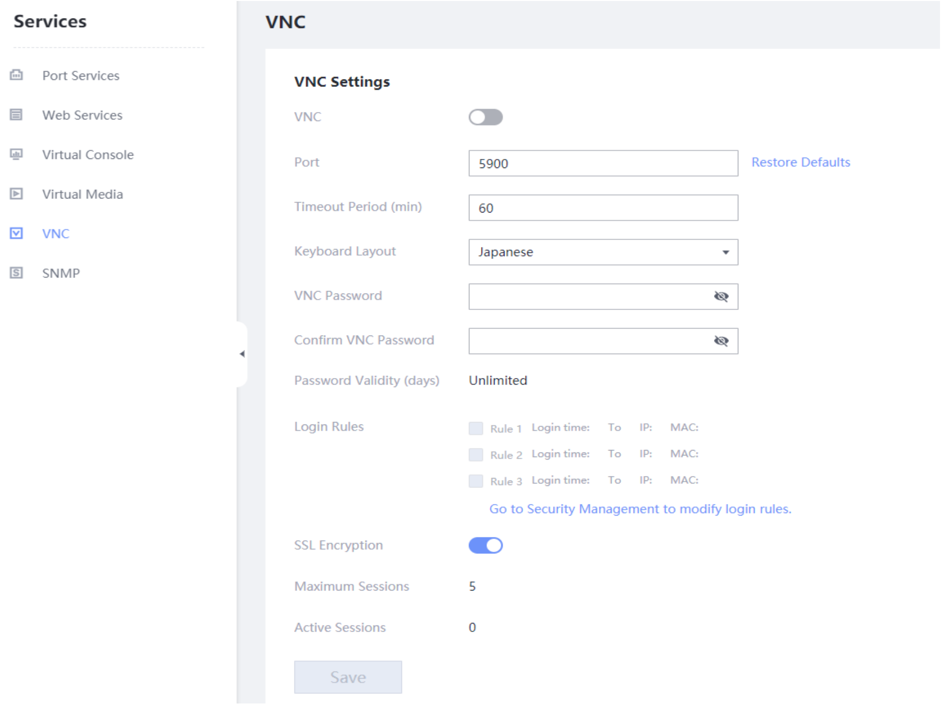
VNC Server: 192.168.100.169

Encryption: Let VNC Server choose

The VNC protocol has the following features:

1. The VNC provides only the KVM function. It does not support virtual media.
2. The VNC can interwork with a third-party VNC client.
3. Only password authentication is supported. VNC has its independent password.
4. The use of VNC client depends on the keyboard layout. The English (American) and Japanese keyboards are supported.

Figure 3-22 VNC configuration



VNC Settings

VNC	○
Port	5900
Timeout Period (min)	60
Keyboard Layout	Japanese
VNC Password	
Confirm VNC Password	
Password Validity (days)	Unlimited
Login Rules	□ Rule 1 Login time: To IP: MAC: □ Rule 2 Login time: To IP: MAC: □ Rule 3 Login time: To IP: MAC: Go to Security Management to modify login rules.
SSL Encryption	●
Maximum Sessions	5
Active Sessions	0

3.3.1 Virtual KVM

The virtual KVM function allows you to monitor and control remote devices in real time by using the local KVM. The virtual KVM provides the following features:

- Resolution
  - Maximum resolution: 1920 x 1280
  - Minimum resolution: 640 x 480

  The actual resolution varies depending on the OS.
- Mouse synchronization

  Mouse synchronization allows the mouse of the server to synchronize with the local mouse. However, this function depends on whether the OS can provide absolute mouse position. For details, see **Table 3-8**.
- Mouse mode

  Absolute, relative, and single mouse modes are available.
- Access mode
  - 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.
- Operating environment

  To use the virtual KVM function, the browser, OS, and JRE versions on the client must meet the requirements listed in **Table 3-2**.
- Color depth

  It supports 32-bit true color, providing a maximum of 16.77 million colors.

- Combination key

  It supports combination of a maximum of six keys.
- Encryption

  The AES128 CBC encryption algorithm is adopted for video, keyboard, and control command data transmission.

For OSs that cannot provide the position of the mouse in absolute mode, the virtual KVM does not support the mouse synchronization function.

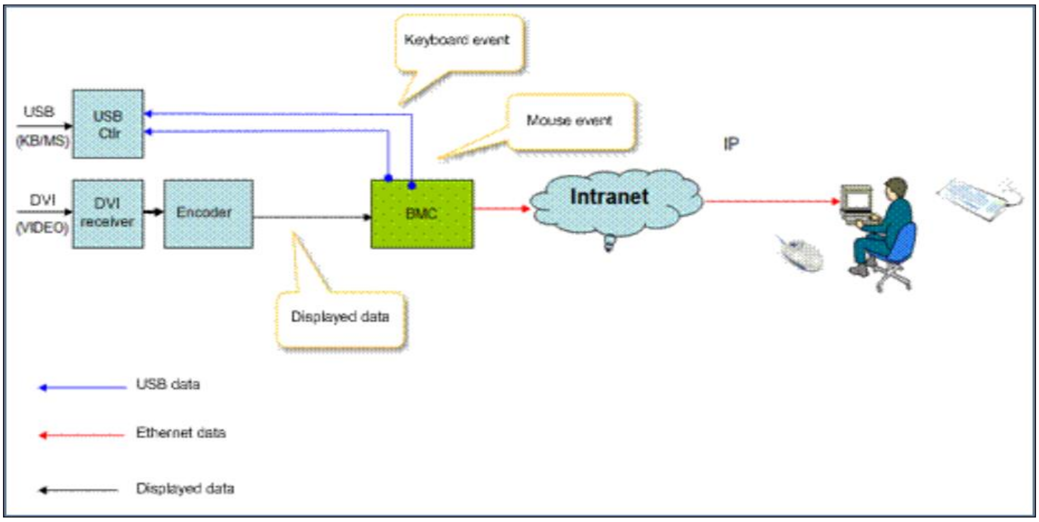
Table 3-8 OSs not supporting mouse synchronization (The OSs include, but not limited to the OSs in the table)

OS Not Supporting Mouse Synchronization
SUSE Linux Enterprise Server 11 Service Pack 1 for x86 (32-Bit)
SUSE Linux Enterprise Server 11 Service Pack 1 for Intel EM64T (64-Bit)

Figure 3-23 shows how the virtual KVM is implemented.

- When receiving data from a remote client, iBMC compresses the data and transmits the compressed data to the local client over a network. The local client console decompresses the data received and displays the data on the local client.
- The virtual KVM console captures local mouse and keyboard events and transmits the events to a remote client over a network. iBMC simulates the local keyboard and mouse to transmit the events to a remote server service system over the USB channel.

Figure 3-23 Virtual KVM in iBMC



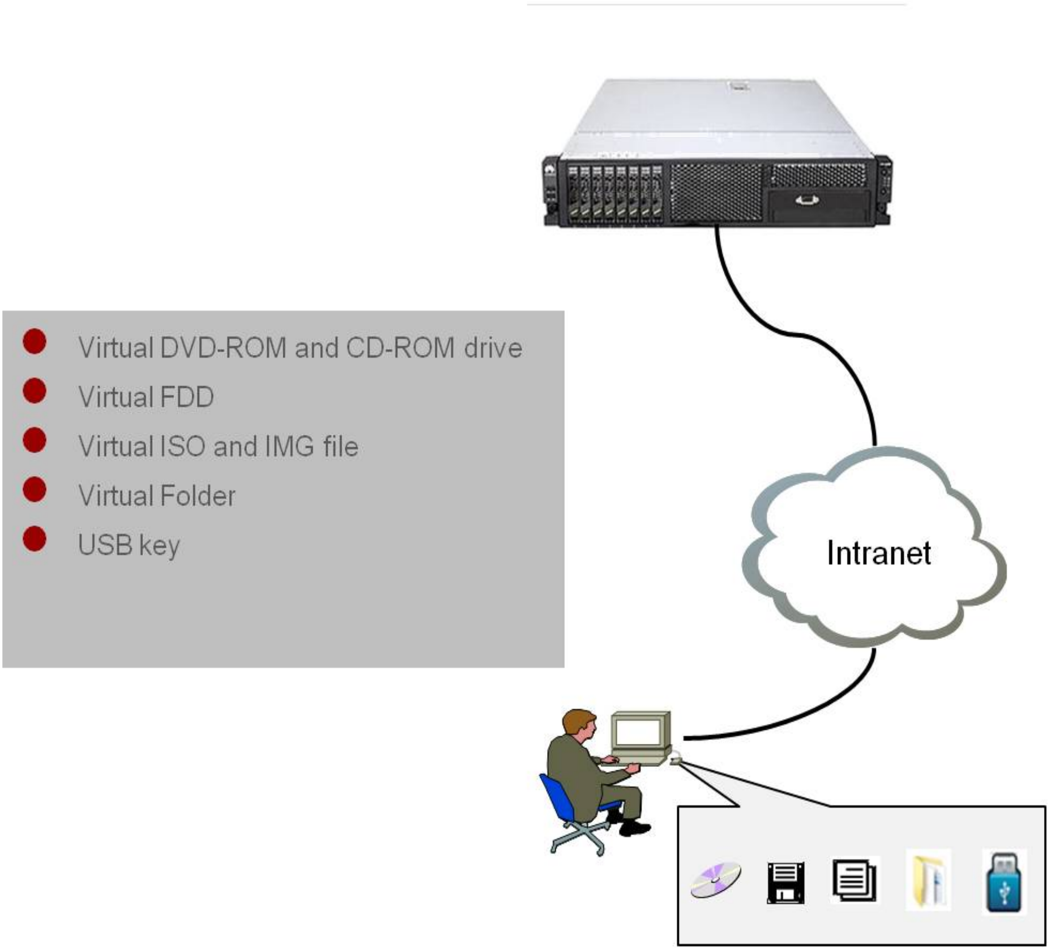
3.3.2 Virtual Media

The virtual media function allows you to use a virtual USB DVD-ROM drive or an FDD to remotely access the local media (such as the DVD-ROM drive, FDD, DVD-

ROM image file, floppy disk image file, hard disk folder, and USB key) over a network. The virtual media data is encrypted using the AES128 CBC encryption algorithm. To use the virtual media function, the client must be equipped with the OS and the JRE of proper versions. For details, see **Table 3-2**.

The purpose of virtual media is to virtualize the local media devices to the media devices on the remote client over a network. **Figure 3-24** shows how virtual media is implemented.

Figure 3-24 Virtual media in the iBMC



iBMC exchanges data with hosts through USB 2.0 protocol. iBMC provides the following virtual media features:

- Virtualizing devices

  The PC or image file on a client is mapped to a connected server. Then the server can detect the client as a USB device.

  The following can be virtualized:

  FDD

  DVD-ROM drive

  Folder (local folder or network folder)

  FDD, which can be used along with other virtual devices.

- Excellent performance

  The virtual DVD-ROM drive supports a transmission rate of up to 32 Mbit/s and 24 Mbit/s in a VLAN.

  The virtual FDD supports a maximum transmission rate of 4 Mbit/s.

- Preparing image files

  The content on a floppy disk or a DVD-ROM can be created as an image file and stored on a hard disk.

- Mounting virtual media using the CLI

  On the iBMC CLI, you can mount virtual media after entering the IP address, port number, file path, mounting protocol, and user password of the remote server.

3.4 HTTPS-based Intuitive Management Interface

The iBMC provides an intuitive web user interface based on HTTPS. You can quickly set and query information through this WebUI. **Table 3-2** shows OSs and browsers supported by the iBMC. The following uses the 2288H V5 as an example. The WebUI supports Chinese, English, Japanese, and French. You can alternate between the four languages. By default, the language to use is the same as that of the browser you use.

To log in to the iBMC Web, perform the following steps:

Step 1 Enter **https://***iBMC IP[:sslport]* in the address box of your browser, and press **Enter**. See **Figure 3-25**.

NOTE

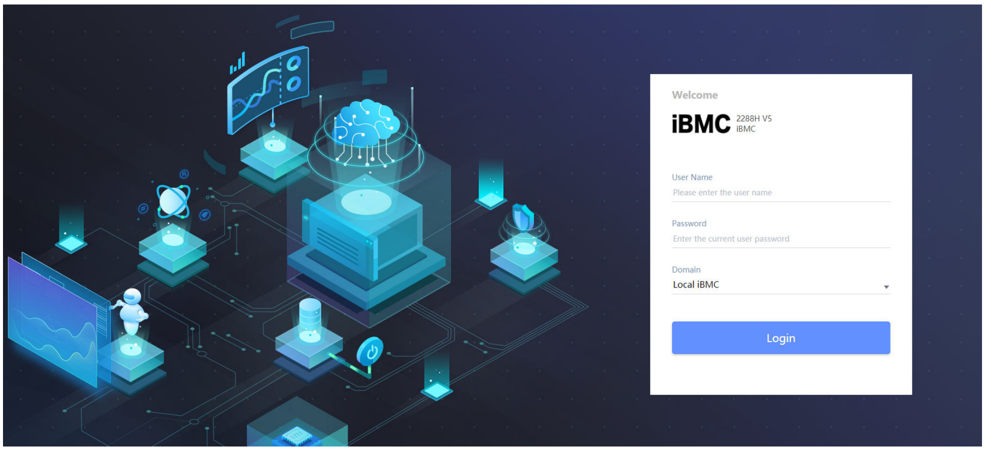
The port number is optional. If the port number is not **80** or the sslport port number is not **443**, you must enter the port number after the IP address. For a method of changing the port number, see **3.9.4 Certificate Management**.

Figure 3-25 Entering the iBMC IP address

http://192.168.2.100

Step 2 On the login page, enter the user name and password or select a domain if a domain account is used, and click **Log In**, as shown in **Figure 3-26**.

Figure 3-26 iBMC login page



Welcome

iBMC 2288H V5 iBMC

User Name: Please enter the user name

Password: Enter the current user password

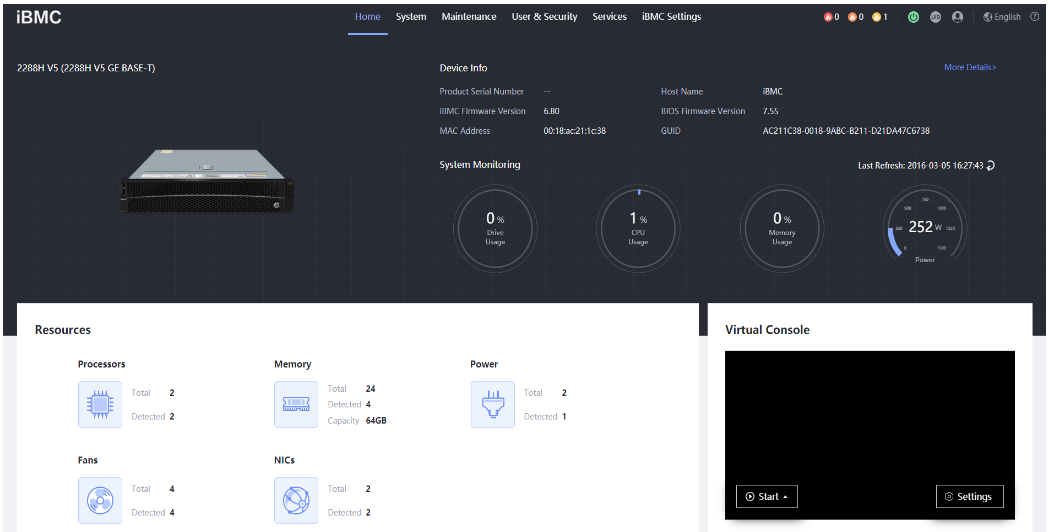
Domain: Local iBMC

----End

3.4.1 Viewing System Information

The **Overview** page displays the system information, including the system status, iBMC information, system configurations, virtual buttons, and virtual console link information, and provides links to common operations, as shown in **Figure 3-27**.

Figure 3-27 Overview page



2288H V5 (2288H V5 GE BASE-T)

Device Info

Product Serial Number --
Host Name iBMC
iBMC Firmware Version 6.80
BIOS Firmware Version 7.55
MAC Address 00:18:ac:21:1c:38
GUID AC211C38-0018-9ABC-B211-D21DA47C6738

System Monitoring

Last Refresh: 2016-03-05 16:27:43

0 % Drive Usage
1 % CPU Usage
0 % Memory Usage
252 W Power

Resources

Processors: Total 2, Detected 2
Memory: Total 24, Detected 4, Capacity 64GB
Power: Total 2, Detected 1
Fans: Total 4, Detected 4
NICs: Total 2, Detected 2

Virtual Console

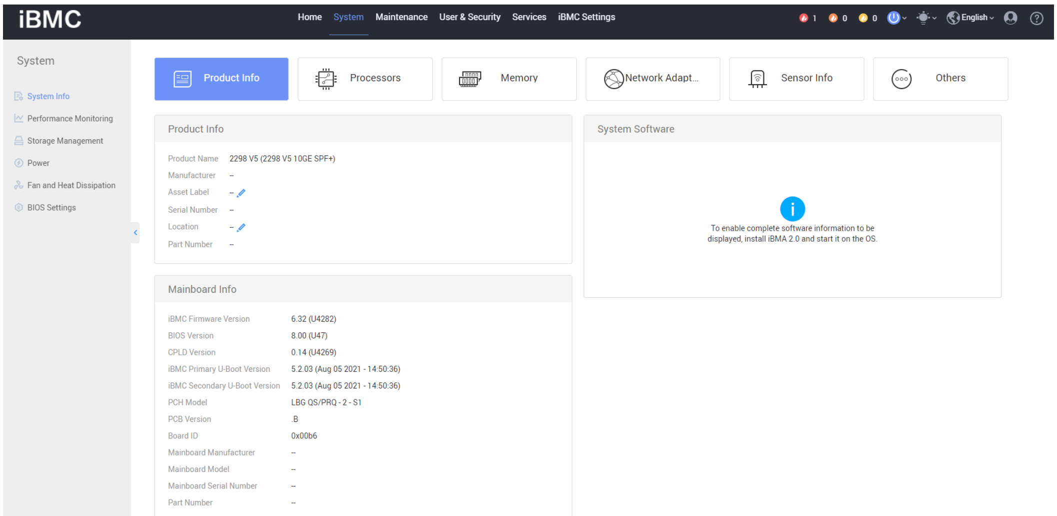
3.4.2 Querying System Information

The system information includes the firmware versions, asset information, and system hardware information.

Firmware Version

The firmware version information includes the iBMC, BIOS, U-Boot and CPLD versions, as well as baseboard PCB versions, baseboard IDs, baseboard manufacturers, baseboard models, and baseboard serial numbers. See **Figure 3-28**.

Figure 3-28 Firmware Version page



Product Info

Product Name	2298 V5 (2298 V5 10GE SPF+)
Manufacturer	--
Asset Label	--
Serial Number	--
Location	--
Part Number	--

Mainboard Info

iBMC Firmware Version	6.32 (U4282)
BIOS Version	8.00 (U47)
CPLD Version	0.14 (U4269)
iBMC Primary U-Boot Version	5.2.03 (Aug 05 2021 - 14:50:36)
iBMC Secondary U-Boot Version	5.2.03 (Aug 05 2021 - 14:50:36)
PCH Model	LBG QS/PRQ - 2 - S1
PCB Version	.B
Board ID	0x00b6
Mainboard Manufacturer	--
Mainboard Model	--
Mainboard Serial Number	--
Part Number	--

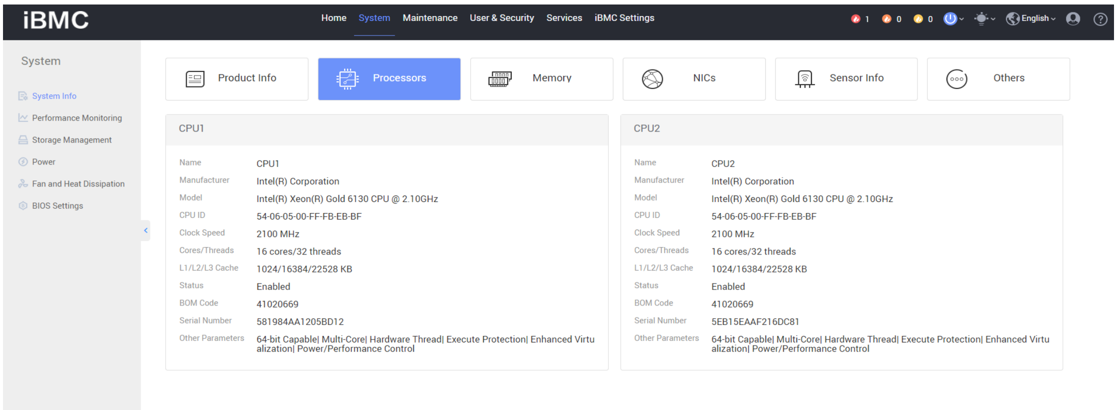
System Software

To enable complete software information to be displayed, install iBMA 2.0 and start it on the OS.

System Hardware

The system hardware information includes the configured number and maximum number of key system components, and component models. The **Network** and **System Software** tabs are displayed only when iBMA 2.0 software is installed. For details, see the following figures:

Figure 3-29 System Hardware page

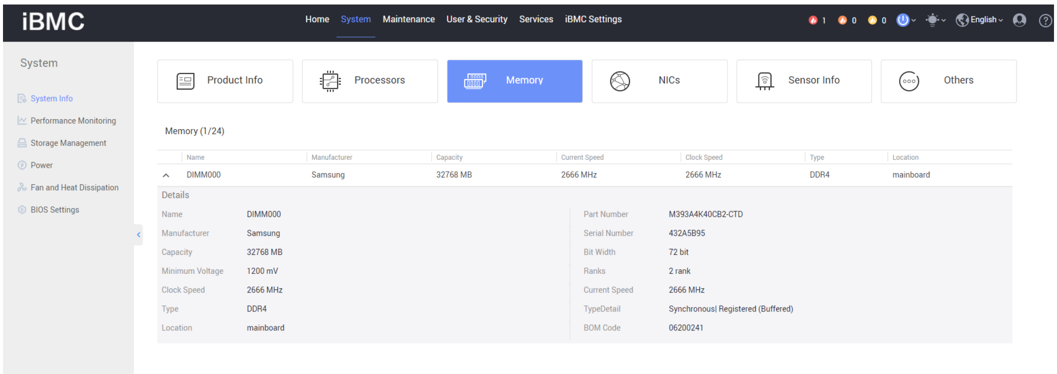


CPU1

Name	CPU1
Manufacturer	Intel(R) Corporation
Model	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
CPU ID	54-06-05-00-FF-FB-EB-BF
Clock Speed	2100 MHz
Cores/Threads	16 cores/32 threads
L1/L2/L3 Cache	1024/16384/22528 KB
Status	Enabled
BOM Code	41020669
Serial Number	581984AA1205BD12
Other Parameters	64-bit Capable| Multi-Core| Hardware Thread| Execute Protection| Enhanced Virtualization| Power/Performance Control

CPU2

Name	CPU2
Manufacturer	Intel(R) Corporation
Model	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
CPU ID	54-06-05-00-FF-FB-EB-BF
Clock Speed	2100 MHz
Cores/Threads	16 cores/32 threads
L1/L2/L3 Cache	1024/16384/22528 KB
Status	Enabled
BOM Code	41020669
Serial Number	5EB15EAAF216DC81
Other Parameters	64-bit Capable| Multi-Core| Hardware Thread| Execute Protection| Enhanced Virtualization| Power/Performance Control

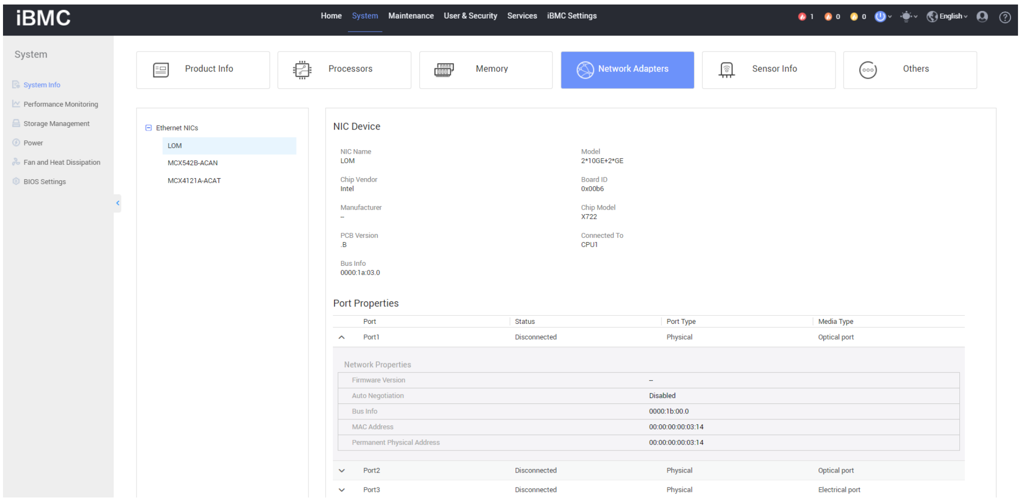


Memory (1/24)

Name	Manufacturer	Capacity	Current Speed	Clock Speed	Type	Location
DIMM000	Samsung	32768 MB	2666 MHz	2666 MHz	DDR4	mainboard

Details

Name	DIMM000	Part Number	M393A4K40CB2-CTD
Manufacturer	Samsung	Serial Number	432A5B95
Capacity	32768 MB	Bit Width	72 bit
Minimum Voltage	1200 mV	Ranks	2 rank
Clock Speed	2666 MHz	Current Speed	2666 MHz
Type	DDR4	TypeDetail	Synchronous| Registered (Buffered)
Location	mainboard	BOM Code	06200241



NIC Device

NIC Name
LOM

Model
2*10GE+2*GE

Chip Vendor
Intel

Board ID
0x00b6

Manufacturer
--

Chip Model
X722

PCB Version
.B

Connected To
CPU1

Bus Info
0000:1a:03.0

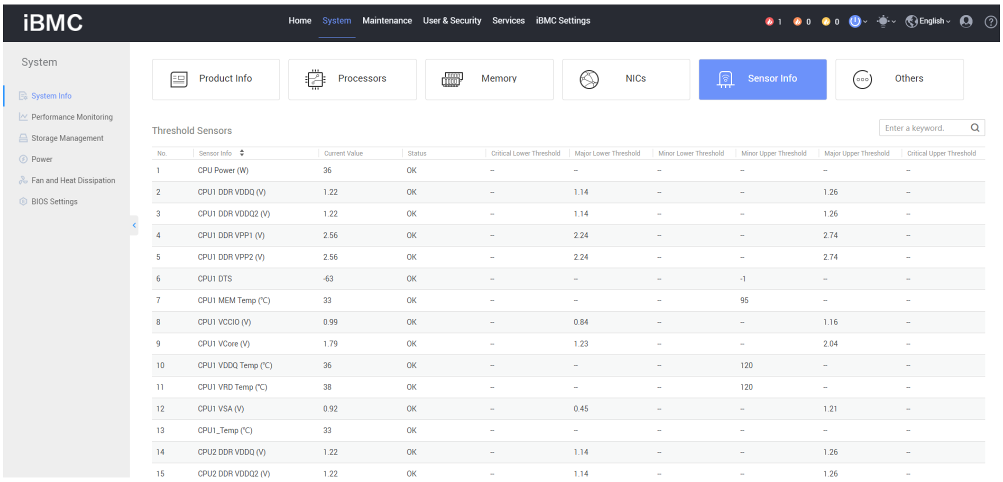
Port Properties

Port	Status	Port Type	Media Type
Port1	Disconnected	Physical	Optical port

Network Properties

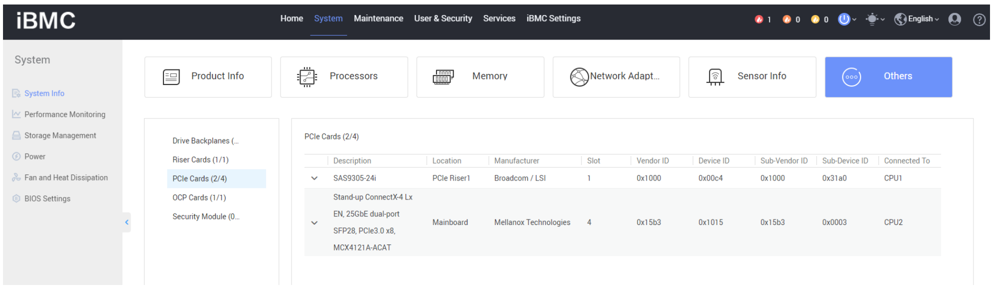
Firmware Version	--
Auto Negotiation	Disabled
Bus Info	0000:1b:00.0
MAC Address	00:00:00:00:03:14
Permanent Physical Address	00:00:00:00:03:14

Port	Status	Port Type	Media Type
Port2	Disconnected	Physical	Optical port
Port3	Disconnected	Physical	Electrical port



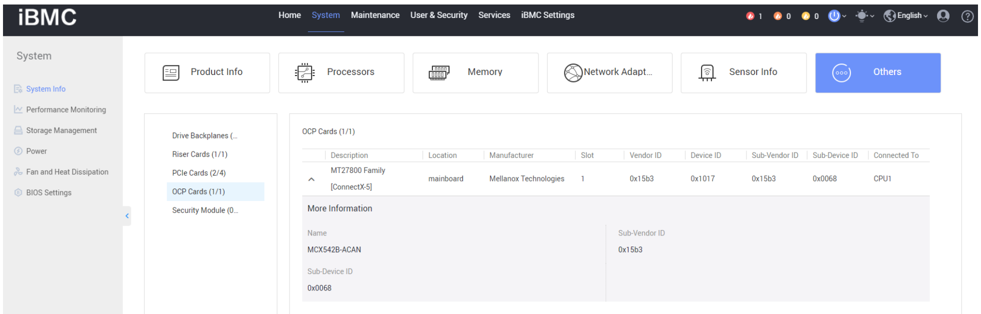
Threshold Sensors

No.	Sensor Info	Current Value	Status	Critical Lower Threshold	Major Lower Threshold	Minor Lower Threshold	Minor Upper Threshold	Major Upper Threshold	Critical Upper Threshold
1	CPU Power (W)	36	OK	--	--	--	--	--	--
2	CPU1 DDR VDDQ (V)	1.22	OK	--	1.14	--	--	1.26	--
3	CPU1 DDR VDDQ2 (V)	1.22	OK	--	1.14	--	--	1.26	--
4	CPU1 DDR VPP1 (V)	2.56	OK	--	2.24	--	--	2.74	--
5	CPU1 DDR VPP2 (V)	2.56	OK	--	2.24	--	--	2.74	--
6	CPU1 DTS	-63	OK	--	--	--	-1	--	--
7	CPU1 MEM Temp (°C)	33	OK	--	--	--	95	--	--
8	CPU1 VCCIO (V)	0.99	OK	--	0.84	--	--	1.16	--
9	CPU1 VCore (V)	1.79	OK	--	1.23	--	--	2.04	--
10	CPU1 VDDQ Temp (°C)	36	OK	--	--	--	120	--	--
11	CPU1 VRD Temp (°C)	38	OK	--	--	--	120	--	--
12	CPU1 VSA (V)	0.92	OK	--	0.45	--	--	1.21	--
13	CPU1_Temp (°C)	33	OK	--	--	--	--	--	--
14	CPU2 DDR VDDQ (V)	1.22	OK	--	1.14	--	--	1.26	--
15	CPU2 DDR VDDQ2 (V)	1.22	OK	--	1.14	--	--	1.26	--



PCIe Cards (2/4)

Description	Location	Manufacturer	Slot	Vendor ID	Device ID	Sub-Vendor ID	Sub-Device ID	Connected To
SAS9305-24i	PCIe Riser1	Broadcom / LSI	1	0x1000	0x00c4	0x1000	0x31a0	CPU1
Stand-up ConnectX-4 Lx EN, 25GbE dual-port SFP28, PCIe3.0 x8, MCX4121A-ACAT	Mainboard	Mellanox Technologies	4	0x15b3	0x1015	0x15b3	0x0003	CPU2



OCP Cards (1/1)

Description	Location	Manufacturer	Slot	Vendor ID	Device ID	Sub-Vendor ID	Sub-Device ID	Connected To
MT27800 Family [ConnectX-5]	mainboard	Mellanox Technologies	1	0x15b3	0x1017	0x15b3	0x0068	CPU1

More Information

Name
MCX542B-ACAN

Sub-Vendor ID
0x15b3

Sub-Device ID
0x0068

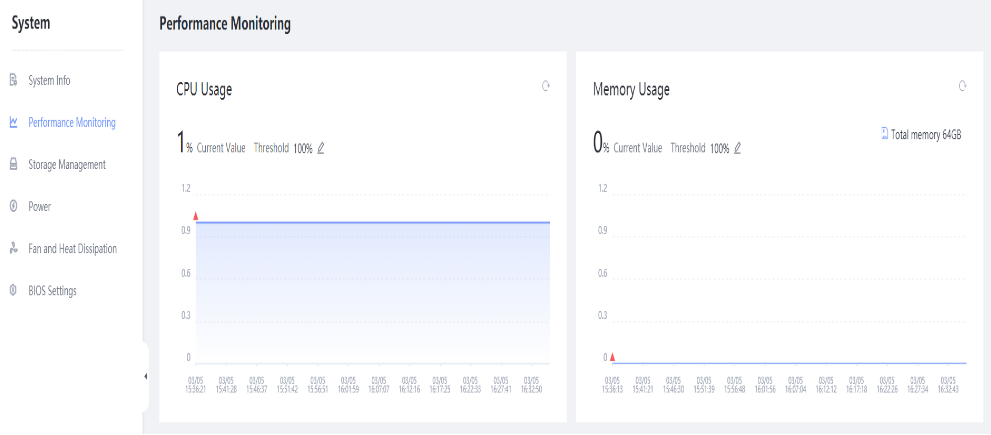
3.4.3 Performance Monitoring

Real-time monitoring involves monitoring of components, sensors, and indicators.

Real-Time Data

Figure 3-30 shows the history lines of real-time data for items including drive partition usage, CPU usage, memory usage, and air intake vent temperature. The CPU usage and memory usage are measured every minute, and the air intake vent temperature is measured every 10 minutes. This allows users to view the data in real time and understand the service running status. The CPU, memory, hard drive usage data is displayed only when iBMA 2.0 software is installed.

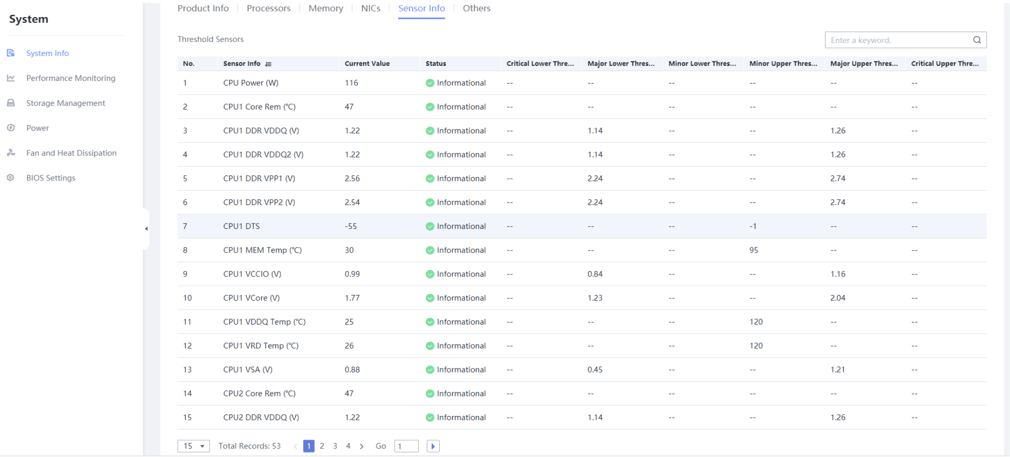
Figure 3-30 Real-time data page



Sensor

The **Sensor** page displays all sensor information, as shown in **Figure 3-31**. **Table 3-9** describes sensor parameters.

Figure 3-31 Sensor page



Threshold Sensors

No.	Sensor Info	Current Value	Status	Critical Lower Thre...	Major Lower Thres...	Minor Lower Thres...	Minor Upper Thres...	Major Upper Thres...	Critical Upper Thre...
1	CPU Power (W)	116	Informational	--	--	--	--	--	--
2	CPU1 Core Rem (°C)	47	Informational	--	--	--	--	--	--
3	CPU1 DDR VDDQ (V)	1.22	Informational	--	1.14	--	--	1.26	--
4	CPU1 DDR VDDQ2 (V)	1.22	Informational	--	1.14	--	--	1.26	--
5	CPU1 DDR VPP1 (V)	2.56	Informational	--	2.24	--	--	2.74	--
6	CPU1 DDR VPP2 (V)	2.54	Informational	--	2.24	--	--	2.74	--
7	CPU1 DTS	-55	Informational	--	--	--	-1	--	--
8	CPU1 MEM Temp (°C)	30	Informational	--	--	--	95	--	--
9	CPU1 VCCIO (V)	0.99	Informational	--	0.84	--	--	1.16	--
10	CPU1 VCore (V)	1.77	Informational	--	1.23	--	--	2.04	--
11	CPU1 VDDQ Temp (°C)	25	Informational	--	--	--	120	--	--
12	CPU1 VRD Temp (°C)	26	Informational	--	--	--	120	--	--
13	CPU1 VSA (V)	0.88	Informational	--	0.45	--	--	1.21	--
14	CPU2 Core Rem (°C)	47	Informational	--	--	--	--	--	--
15	CPU2 DDR VDDQ (V)	1.22	Informational	--	1.14	--	--	1.26	--

15 ▾ Total Records: 53 ‹ 1 2 3 4 › Go 1 ▸

Table 3-9 Threshold sensor parameters

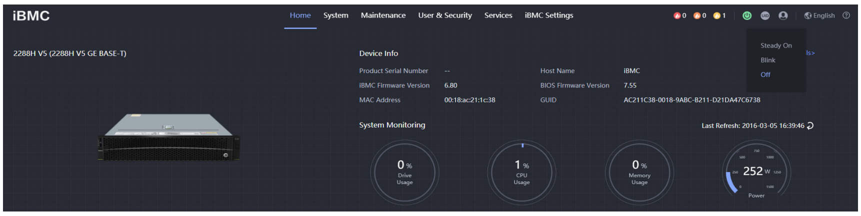
Parameter	Description
Sensor	Name of a sensor
Current value	Current value of the sensor

Parameter	Description
Unit	Unit of the sensor value
Lower critical	The system generates a critical alarm when the sensor value exceeds this threshold.
Lower major	The system generates a major alarm when the sensor value exceeds this threshold.
Lower minor	The system generates a minor alarm when the sensor value exceeds this threshold.
Upper minor	The system generates a minor alarm when the sensor value exceeds this threshold.
Upper major	The system generates a major alarm when the sensor value exceeds this threshold.
Upper critical	The system generates a critical alarm when the sensor value exceeds this threshold.

3.4.4 Device Location

The **Device Location** page allows you to set the status of the location indicator. By illuminating the UID indicator on the device panel, you can quickly locate the device to be operated among a large number of devices in the equipment room. See **Figure 3-32**.

Figure 3-32 Device Location page



2288H V5 (2288H V5 GE BASE-T)

Device Info

Product Serial Number --
iBMC Firmware Version 6.80
MAC Address 00:18:ac:21:1c:38
Host Name iBMC
BIOS Firmware Version 7.55
GUID AC211C38-0018-9ABC-B211-D21DA47C6738

System Monitoring

Last Refresh: 2016-03-05 16:39:46

3.5 Domain Management and Directory Service

With development of enterprise applications, IT infrastructure capacity is increasing, which increases workloads in asset management and daily management. The iBMC provides domain management and directory service to streamline tedious IT infrastructure management.

3.5.1 Domain Management

You can add all managed servers to a domain and access iBMC using the domain name. If the domain name is the asset number of a managed server, the domain controller can help count assets. This greatly reduces IT asset management costs.

Step 1 Add the computer to the domain.

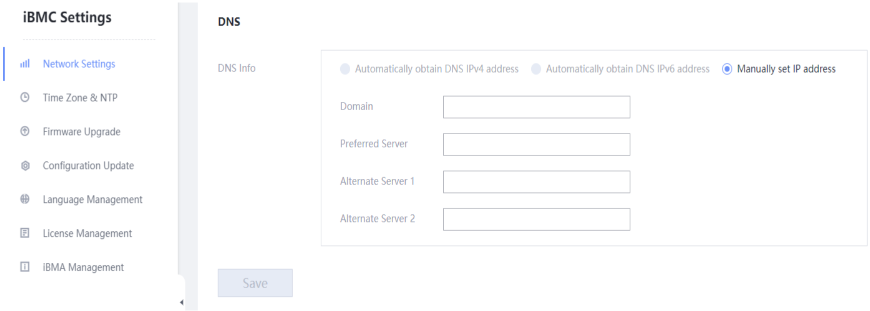
1. Log in to the iBMC WebUI using the domain name, and open the **Network Settings** tab. See **Figure 3-33**.

   NOTE

   Domain Name System (DNS) is an Internet service. The DNS maps easy-to-remember domain names and IP addresses. This helps you easily access the network.

2. The UI shown in **Figure 3-33** enables you to set DNS bound network port and methods of obtaining DNS information. Click **OK** to save the settings.
3. Set **Domain Name**, **Primary DNS Server**, and **Secondary DNS Server** if **Manually Obtain DNS Information** is selected.

Figure 3-33 Configuring DNS parameters

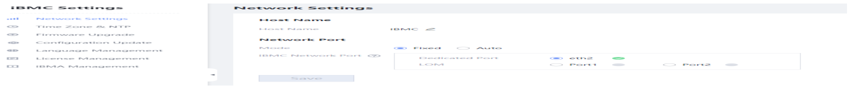


DNS Info: ○ Automatically obtain DNS IPv4 address ○ Automatically obtain DNS IPv6 address ● Manually set IP address

Domain:
Preferred Server:
Alternate Server 1:
Alternate Server 2:

Step 2 Set a host name. See **Figure 3-34**.

Figure 3-34 Host Name page



Host Name: iBMC

Mode: ● Fixed ○ Auto

iBMC Network Port: Dedicated Port ● eth2; LOM ○ Port1 ○ Port2

----End

3.5.2 Directory Service

The directory service integrates user management, rights assignment, and validity period management on iBMC into the directory server, as shown in **Figure 3-35**. This minimizes repeated user configuration tasks and improves management efficiency. In addition, centralized user management greatly enhances the security of iBMC.

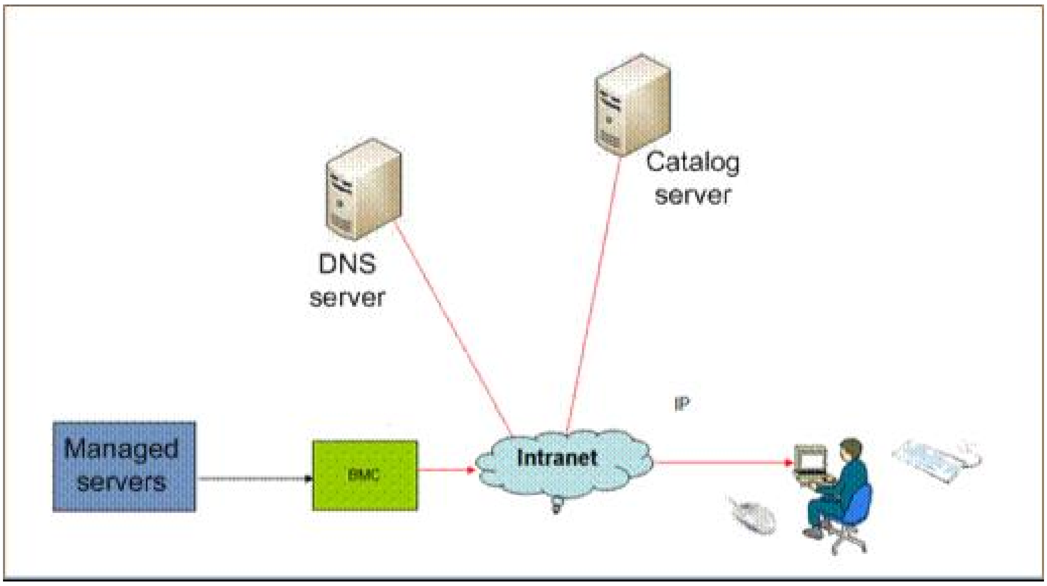
The advantages of LDAP are as follows:

1. Scalability: dynamically add users on the LDAP server in all iBMCs at the same time.
2. Security: User password policies are all implemented on the LDAP server.
3. Real-time performance: Any account update on the LDAP server takes effect immediately on all iBMCs.
4. High efficiency: integrates user management, rights assignment, and validity management on iBMC into the catalog server. This minimizes repeated user configuration tasks and improves management efficiency.
5. Supports Active Directory (AD) and OpenLDAP, and the New Technology LAN Manager (NTLM) authentication.

The iBMC LDAP provides the following features:

- For security purposes, the iBMC supports only LDAPS and supports the NTLM authentication mechanism.
- To ensure the authenticity of an LDAP server, LDAP supports certificate authentication of servers and becomes valid only when the root CA certificate of the LDAP server is imported into iBMC. In addition, the domain controller address must be the same as the user name of the root CA certificate because their consistency is checked during server authentication.
- Multiple domains are supported. Up to six domain servers can be configured. The domain to be used can be manually or automatically selected.
- LDAP accounts can be used to log in to the iBMC WebUI or the CLI over Secure Shell (SSH).
- LDAP servers deployed with AD or OpenLDAP are supported.

Figure 3-35 Directory service work process



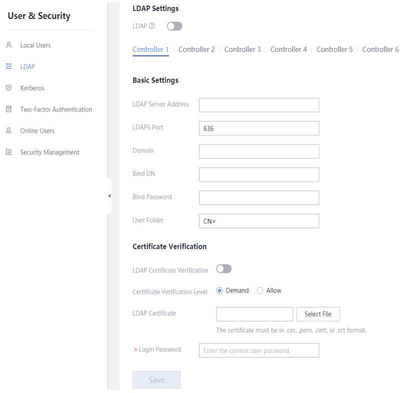
The **LDAP User** page is displayed, as shown in **Figure 3-36**.

NOTE

LDAP is a protocol for accessing online directory services over an IP network. LDAP directories can help store any types of data, such as email addresses and mail routing information, so that you can query the information conveniently.

View or set the LDAP user information on the **LDAP User** page, as shown in **Figure 3-36**.

Figure 3-36 LDAP User page



LDAP Settings

LDAP ○

Basic Settings

LDAP Server Address:

LDAPS Port: 636

Domain:

Bind DN:

Bind Password:

User Folder: CN=

Certificate Verification

LDAP Certificate Verification ○

Certificate Verification Level ● Demand ○ Allow

LDAP Certificate:

The certificate must be in .cer, .pem, .cert, or .crt format.

* Login Password: Enter the current user password.

On the **LDAP User** page, you can perform the following operations:

- Enable or disable LDAP.
- Enable certificate verification.
- Set the LADPS port number. The default value is **636**.
- Import LDAP root certificate.
- Set a domain controller address.

  The domain controller address is the IP address or domain name of the server where the active directory is located. The domain controller address consists of a maximum of 255 characters.
- Set a group name.

  The group name is the name for logging in to the iBMC page in the active directory. The group name can contain a maximum of 32 characters.
- Set a group domain.

  The group domain is the domain for logging in to the iBMC page in the active directory. The group domain name can contain a maximum of 255 characters.
- Set the group privilege.

  The group privilege is the permission for logging in to the iBMC page in the active directory. The permissions are: rule 1, rule 2, rule 3, Web, SSH, and Redfish.

3.6 Firmware Management

Firmware management involves the iBMC firmware, BIOS, CPLD, LCD, and PSU. It allows you to query firmware version, upgrade firmware, and alternate between the iBMC dual images.

3.6.1 Firmware Dual-image Backup

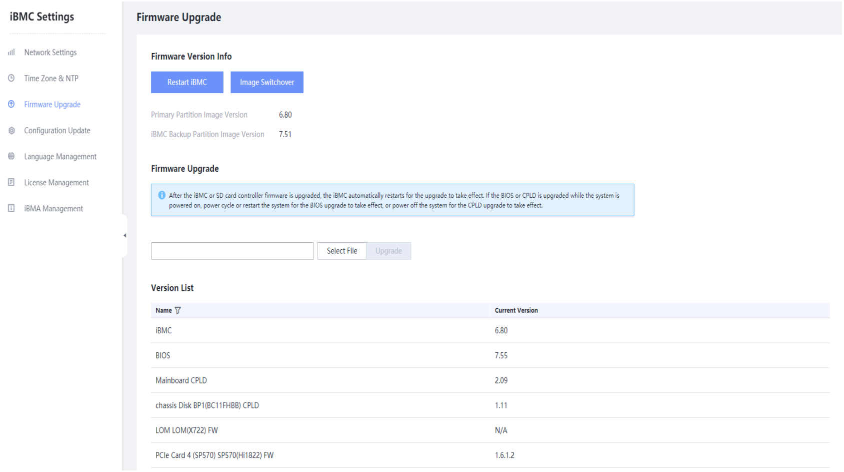
iBMC uses firmware dual-image backup to improve system reliability. When flash misoperations occur or storage modules are damaged, the system automatically switches to the backup image and generates an alarm, indicating that image redundancy becomes invalid.

Switching Over Images on the Web Page

In the navigation tree, choose **System Management** > **Firmware Upgrade**. The **Firmware Upgrade** page is displayed, as shown in **Figure 3-37**.

The iBMC and BIOS version information are displayed on this page, and a user is allowed to switch images and restart iBMC.

Figure 3-37 Firmware Upgrade page



Primary Partition Image Version 6.80
iBMC Backup Partition Image Version 7.51

After the iBMC or SD card controller firmware is upgraded, the iBMC automatically restarts for the upgrade to take effect. If the BIOS or CPLD is upgraded while the system is powered on, power cycle or restart the system for the BIOS upgrade to take effect, or power off the system for the CPLD upgrade to take effect.

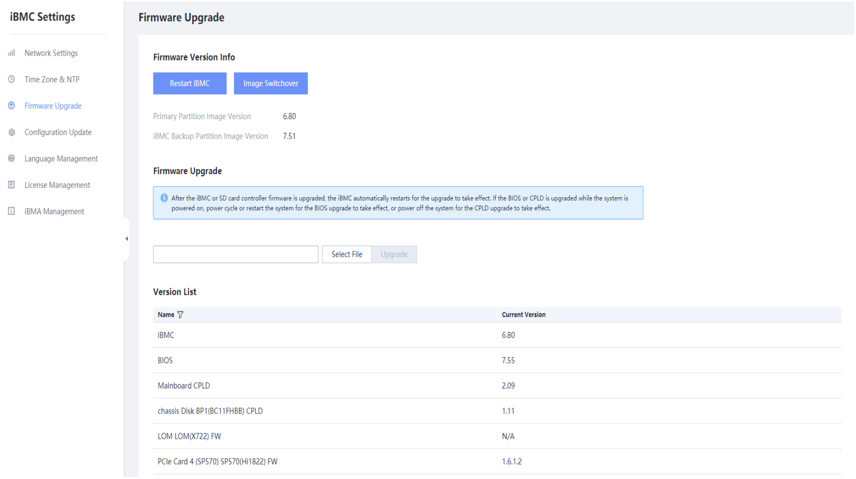
Name	Current Version
iBMC	6.80
BIOS	7.55
Mainboard CPLD	2.09
chassis Disk BP1(BC11FHBB) CPLD	1.11
LOM LOM(X722) FW	N/A
PCIe Card 4 (SP570) SP570(Hi1822) FW	1.6.1.2

3.6.2 Firmware Upgrade

The iBMC firmware, BIOS, CPLD (mainboard, backplane, mezzanine module, and expansion card), LCD firmware, and PSU firmware can be remotely upgraded. The iBMC WebUI supports switchover between primary and backup iBMC images, and upgrade and rollback of the iBMC firmware. For details, see **Figure 3-38**. For the compatibility purpose, you are advised to upgrade active and standby iBMC images to the same version.

All firmware upgrade packages have RSA-2048 digital signatures and are encrypted by using AES-128-CBC algorithms. Supports firmware validity and integrity verification.

Figure 3-38 Firmware Upgrade page

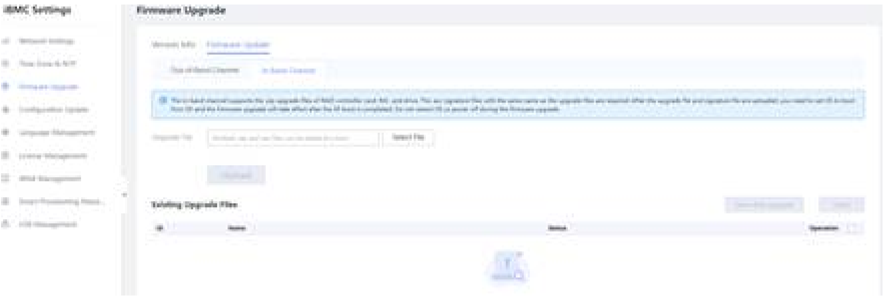


Primary Partition Image Version 6.80
iBMC Backup Partition Image Version 7.51

After the iBMC or SD card controller firmware is upgraded, the iBMC automatically restarts for the upgrade to take effect. If the BIOS or CPLD is upgraded while the system is powered on, power cycle or restart the system for the BIOS upgrade to take effect, or power off the system for the CPLD upgrade to take effect.

Name	Current Version
iBMC	6.80
BIOS	7.55
Mainboard CPLD	2.09
chassis Disk BP1(BC11FHBB) CPLD	1.11
LOM LOM(X722) FW	N/A
PCIe Card 4 (SP570) SP570(Hi1822) FW	1.6.1.2

The RAID controller card firmware, NIC firmware, and drive firmware can be remotely upgraded. The upgrade files must be uploaded together with the ASC signature files with the same name. During the upgrade, the OS is set to boot from the SP. After the SP is started, the firmware upgrade takes effect.



3.6.3 Separated BMC Upgrade and Validation

The iBMC based on the Hi1711 chip supports taking effect of upgraded BMC firmware upon the next server restart. By default, the server restarts immediately upon completion of the BMC firmware upgrade for the new version to take effect.

3.7 Intelligent Power Management and Smart Cooling

iBMC provides multiple intelligent power management methods to reduce total cost of ownership (TCO).

3.7.1 Power Control

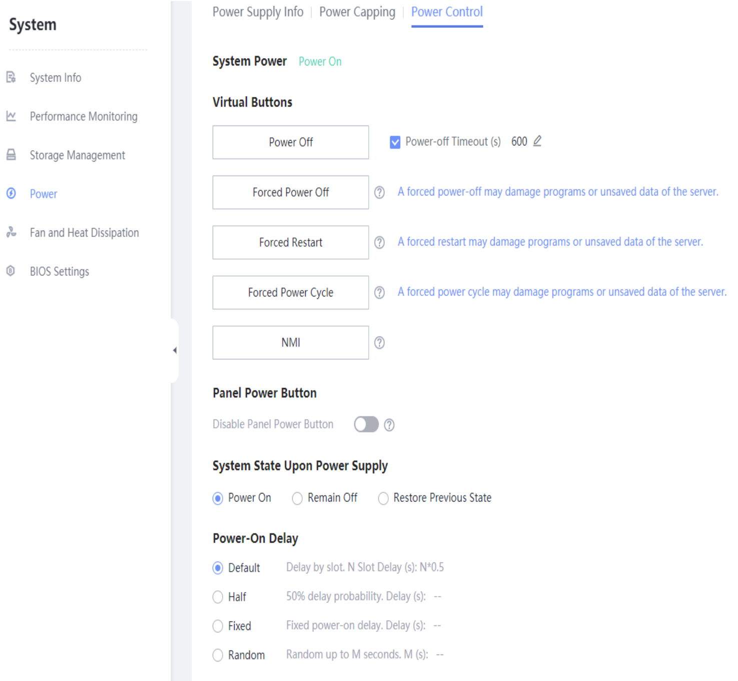
The **Power Control** page provides power control methods such as remote power-on and power-off of servers, as shown in **Figure 3-39**.

You can perform the following operations:

- **Power On**: powers on the server.
- **Power Off**: gracefully powers off a server. The iBMC sends an ACPI interrupt to the OS. If the OS supports the ACPI interrupt, the iBMC shuts down the OS (ends all running processes) and then powers off the device. If the OS does not support the ACPI interrupt, the iBMC powers off the device forcibly after the graceful power-off timeout period ends. The result is the same as the operation that you press the power button on the front panel of the server.
- **Forced Power Off**: powers off a server without waiting for the response from the OS. This option has the same result as the operation that you hold down the power button on the front panel of the server.
- **Forced System Reset**: indicates cold reset. iBMC can reset the system through the southbridge directly, without the need of powering off the OS.
- **Forced Power Cycle**: powers off and then powers on the server. iBMC shuts down the OS and then power off the server. iBMC powers off the server forcibly after the graceful power-off timeout period ends, and then powers on the server.
- **NMI**: sends a non-maskable interrupt (NMI) to the OS to collect kernel stack information and sends the information to the console, which is used for identifying the causes of system exceptions.

- **Disable Panel Power Button**: disables the power button on the server panel.

Figure 3-39 Power Control



System Power Power On

☑ Power-off Timeout (s) 600

A forced power-off may damage programs or unsaved data of the server.

A forced restart may damage programs or unsaved data of the server.

A forced power cycle may damage programs or unsaved data of the server.

Disable Panel Power Button

● Power On ○ Remain Off ○ Restore Previous State

● Default Delay by slot. N Slot Delay (s): N*0.5

○ Half 50% delay probability. Delay (s): --

○ Fixed Fixed power-on delay. Delay (s): --

○ Random Random up to M seconds. M (s): --

Servers are powered on in sequence in cluster management, because powering on multiple servers at the same time may cause overcurrent.

- Rack servers are powered on randomly during two seconds.
- Blade servers, including high-density servers, are powered on in an ascending order of slot numbers. The interval between powering on servers is at least 500 ms.

3.7.2 Power Capping

Currently, data centers are facing a challenge that enterprises consume a lot of electric power and space and have high refrigeration costs. The available resources can hardly meet ever-increasing energy and refrigeration requirements. The top priority for data centers is to save energy and reduce energy consumption using innovative technologies. In traditional data centers, customers spend enormous amounts building electric power infrastructure to ensure service continuity. In addition, IT administrators usually use excessive power supply to meet system power requirements. The power capping technology helps control energy consumption of each server, avoiding excessive energy supply. The saved energy realized by the power capping technology can be used for capacity expansion in data centers.

In the navigation tree, choose **PS Management** > **Power History**. The **Power History** page is displayed, as shown in **Figure 3-40**.

You can set the power upper limit. If the system power exceeds the upper limit, specific actions are triggered to ensure that the chassis power is properly distributed.

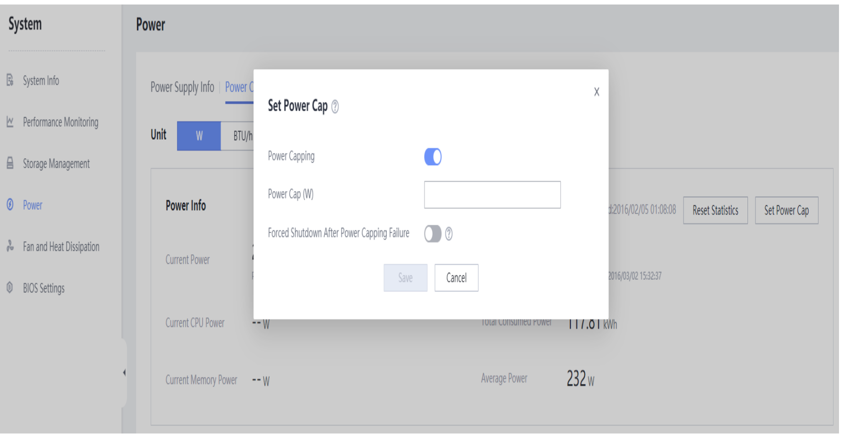
iBMC collects system power data every one second for 40 times or more during system startup. It deletes the invalid values, calculates the average value, and then multiples the value by a coefficient varying by product. The calculation result is the minimum power.

Set **Power Capping State**, **Power Limit**, and **Follow-up Action After Power Capping Fails** as required, and click **OK**, as shown in **Figure 3-40**. After the configuration, Operation performed successfully is displayed.

Follow-up Action After Power Capping Fails has the following value options:

- **Event log**: logs information about a power capping failure in the system event file. This function is enabled by default.
- **Power off**: iBMC forcibly powers off the server within 15s.

Figure 3-40 Power Capping page



Set Power Cap

Power Capping: ●

Power Cap (W):

Forced Shutdown After Power Capping Failure: ○

Current CPU Power -- W

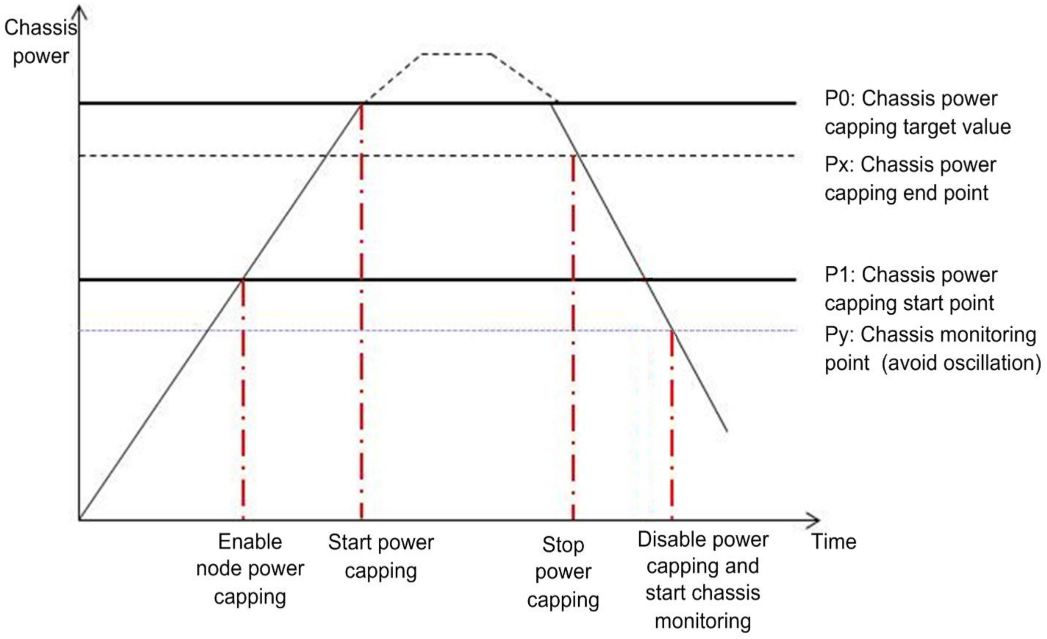
Current Memory Power -- W

Total Consumed Power 117.61 kWh

Average Power 232 W

Chassis power capping of X series servers is based on node power capping and aims to control the power consumption of the entire chassis (including the nodes, PSUs, and fan modules).

Figure 3-41 Power capping diagram

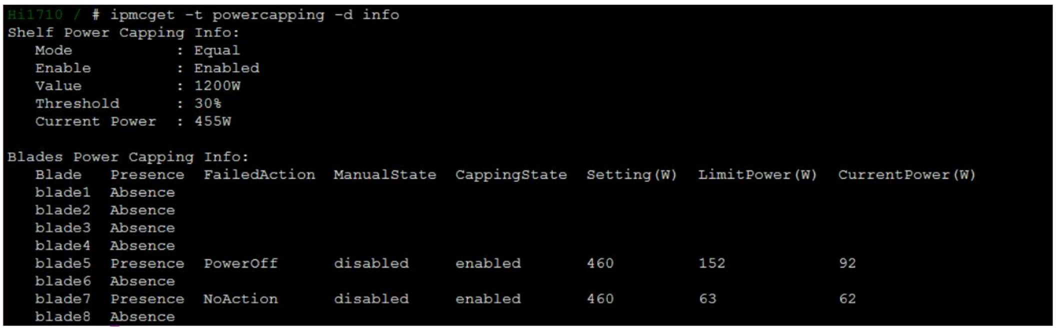


Chassis power
P0: Chassis power capping target value
Px: Chassis power capping end point
P1: Chassis power capping start point
Py: Chassis monitoring point (avoid oscillation)
Enable node power capping
Start power capping
Stop power capping
Disable power capping and start chassis monitoring
Time

NOTE

- Node power distribution modes: equal (default), automatically proportional, and manual.
- The default threshold is 70%.
- The management module periodically queries the chassis power consumption. When the chassis power consumption exceeds the P1 value (power capping target value P0 x threshold), node power capping is enabled and power cap values are sent to node BMCs.
- iBMC monitors the input power in a real-time manner and automatically adjusts the power cap values of each node.

Figure 3-42 Chassis power capping information



```
Hi1710 / # ipmcget -t powercapping -d info
Shelf Power Capping Info:
   Mode           : Equal
   Enable         : Enabled
   Value          : 1200W
   Threshold      : 30%
   Current Power  : 455W

Blades Power Capping Info:
   Blade   Presence  FailedAction  ManualState  CappingState  Setting(W)  LimitPower(W)  CurrentPower(W)
   blade1  Absence
   blade2  Absence
   blade3  Absence
   blade4  Absence
   blade5  Presence  PowerOff      disabled     enabled       460         152            92
   blade6  Absence
   blade7  Presence  NoAction      disabled     enabled       460         63             62
   blade8  Absence
```

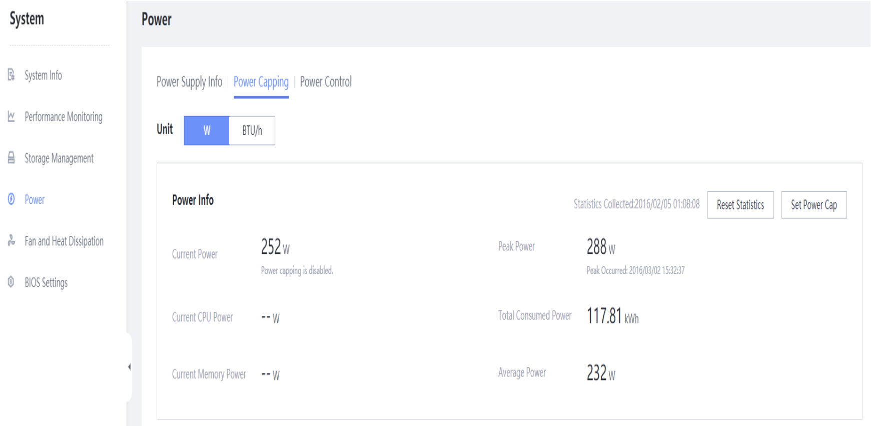
3.7.3 Power Statistics and Power History Line

iBMC provides accurate energy monitoring information and historical power statistics. This helps system administrators know about the actual usage of electric power and heat dissipation resources. You can adjust the server consumption based on historical power data.

In the navigation tree, choose **PS Management > Power Statistics**. The **Power Statistics** page is displayed, as shown in **Figure 3-43**. The page displays **Current Power**, **Total CPU Power**, **Total Memory Power**, **Peak System Power**, **Average System Power**, and **Consumed Electricity**.

Click **Recollect** to recollect information about the peak system power, average system power, and consumed electricity.

Figure 3-43 Power Statistics page



Unit: W | BTU/h

Power Info

Statistics Collected:2016/02/05 01:08:08

Current Power 252 W
Power capping is disabled.

Peak Power 288 W
Peak Occurred: 2016/03/02 15:32:37

Current CPU Power -- W

Total Consumed Power 117.81 kWh

Current Memory Power -- W

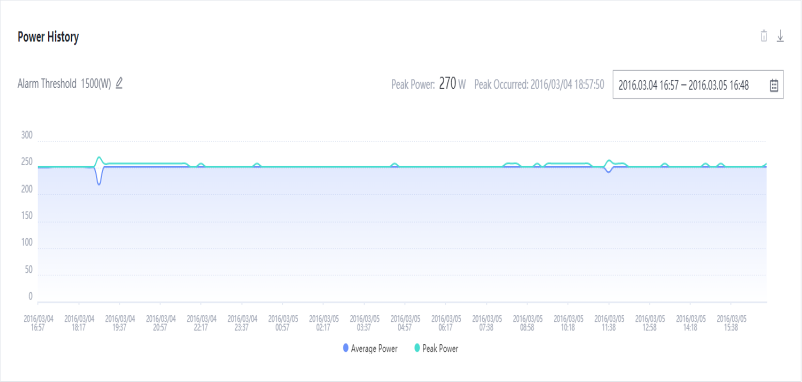
Average Power 232 W

In the navigation tree, choose **PS Management** > **Power History**. The power history user interface (UI) is displayed, as shown in **Figure 3-44**.

iBMC collects and saves the system power every 10 minutes. The **Power History** page displays the recent power history in a line chart. To view the power statistics in recent periods, click **Last Week** or **Last Day**. To refresh the line charts and tables, click Recollect. To download historical power information, click Download.

On this page, you can view the recent device power changes and understand the device running status in a certain period.

Figure 3-44 Power History page



Power History

Alarm Threshold 1500(W)

Peak Power: 270 W Peak Occurred: 2016/03/04 18:57:50

2016.03.04 16:57 – 2016.03.05 16:48

3.7.4 Active and Standby PSUs

When the service power consumption requirement is met, set some PSUs to hot standby or cold standby (only supported by V5 or later servers in power-off state) to improve the power conversion efficiency.

The feature implementation principles are described as follows:

When the service power consumption requirement is met, set the output voltage of some PSUs to 0.3 V lower than the output voltages of other PSUs to suppress the current output of the standby PSUs by using the voltage difference. The service system is powered by the active PSUs, and the PSUs with a lower output voltage work in hot standby mode. If the active PSUs are abnormal, the standby PSUs switch to the active state to supply power to the entire service system, without affecting services.

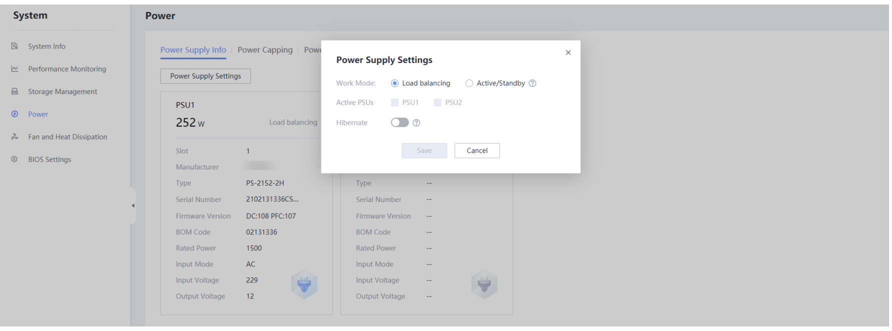
The standby PSUs switch to the active state (from the active/standby mode to the load balancing mode) when:

1. Active PSUs are removed.
2. The output voltage of active PSUs is low or active PSUs have no output.
3. Active PSUs have a high temperature, no input, overcurrent, or overvoltage.
4. The percentage of the system power to the total rated power of active PSUs reaches the upper limit (for example, 75%). (Note: If the percentage is less than the lower limit, for example, 65%, the previous standby PSUs switch to the standby state. The percentage upper limit and lower limit vary depending on products.)

The page allows you to set the PSU working mode and set active PSUs, as shown in **Figure 3-45**.

When deep hibernation is enabled, PUSs in deep hibernation mode stop power output when the system is powered off. They restore power output when deep hibernation is disabled or the system is powered on. If all active PUSs are removed or faulty when deep hibernation is enabled and the system is powered off, a power failure occurs on the device and persists for about 10 seconds. Then, PSUs in deep hibernation automatically starts output.

Figure 3-45 Active and standby PSUs page



Power Supply Settings

Work Mode: ● Load balancing ○ Active/Standby ⓘ
Active PSUs □ PSU1 □ PSU2
Hibernate ○ ⓘ

PSU1
252 W
Load balancing

Slot	1		
Manufacturer	[redacted]		
Type	PS-2152-2H	Type	--
Serial Number	2102131336CS...	Serial Number	--
Firmware Version	DC:108 PFC:107	Firmware Version	--
BOM Code	02131336	BOM Code	--
Rated Power	1500	Rated Power	--
Input Mode	AC	Input Mode	--
Input Voltage	229	Input Voltage	--
Output Voltage	12	Output Voltage	--

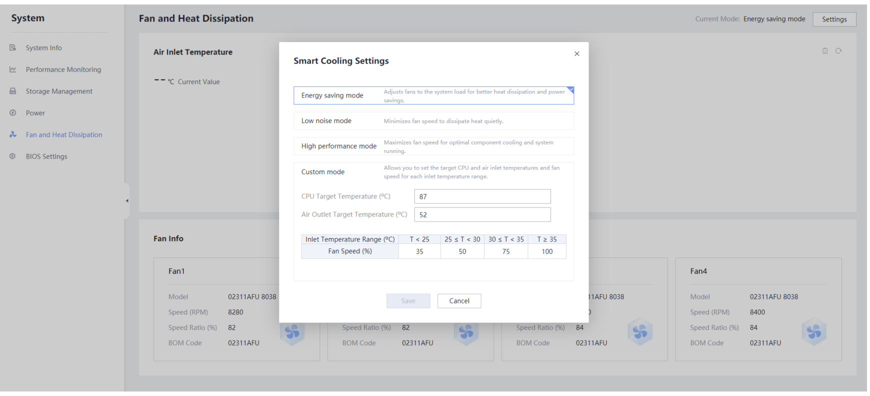
3.7.5 Smart Cooling

Different customers or scenarios have different requirements on server performance, power consumption, and noise. For example, some customers require higher performance, energy saving, and lower noise, while others require flexible customization.

The iBMC provides Smart Cooling to meet different requirements. As shown in **Figure 3-46**, Smart Cooling provides the following modes:

- Energy saving: controls the fan speed at a balance point to maintain the minimum power consumption.
- Noise reduction: reduces the fan speed to minimize the noise when the heat dissipation is satisfied.
- High performance: increases the fan speed to cool key components for optimal system performance.
- Custom: customizes the CPU target temperature and air inlet temperature range based on actual requirements.

Figure 3-46 Smart Cooling



Fan and Heat Dissipation

Current Mode: Energy saving mode

Air Inlet Temperature

-- ℃ Current Value

Smart Cooling Settings

Energy saving mode	Adjusts fans to the system load for better heat dissipation and power savings.
Low noise mode	Minimizes fan speed to dissipate heat quietly.
High performance mode	Maximizes fan speed for optimal component cooling and system running.
Custom mode	Allows you to set the target CPU and air inlet temperatures and fan speed for each inlet temperature range.

CPU Target Temperature (ºC): 87

Air Outlet Target Temperature (ºC): 52

Inlet Temperature Range (ºC)	T < 25	25 ≤ T < 30	30 ≤ T < 35	T ≥ 35
Fan Speed (%)	35	50	75	100

Fan Info

Fan1
Model 02311AFU 8038
Speed (RPM) 8280
Speed Ratio (%) 82
BOM Code 02311AFU

Speed Ratio (%) 82
BOM Code 02311AFU

1AFU 8038
Speed Ratio (%) 84
BOM Code 02311AFU

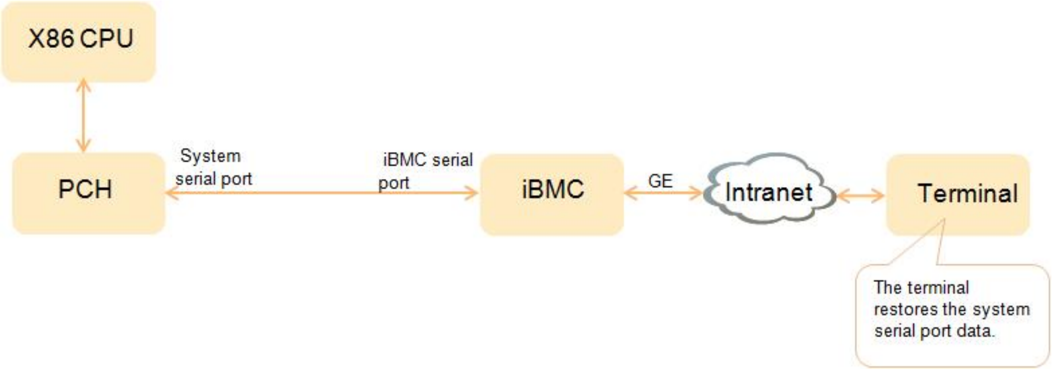
Fan4
Model 02311AFU 8038
Speed (RPM) 8400
Speed Ratio (%) 84
BOM Code 02311AFU

3.8 SOL and System Serial Port Running Information Record

3.8.1 SOL

iBMC provides the SOL function. This function redirects the serial port data, which is sent only through a serial cable originally, to the remote network devices for sending, and allows the system to receive data from remote network devices. The iBMC supports IPMI SOL and CLI SOL, which are mutually exclusive. The CLI SOL supports two SOL sessions at the same time. **Figure 3-47** shows how the SOL function is implemented. Management personnel can query the data using a network terminal sent by the serial port in real time and perform operations on the OS. The effect is the same as that a near-end serial port is used.

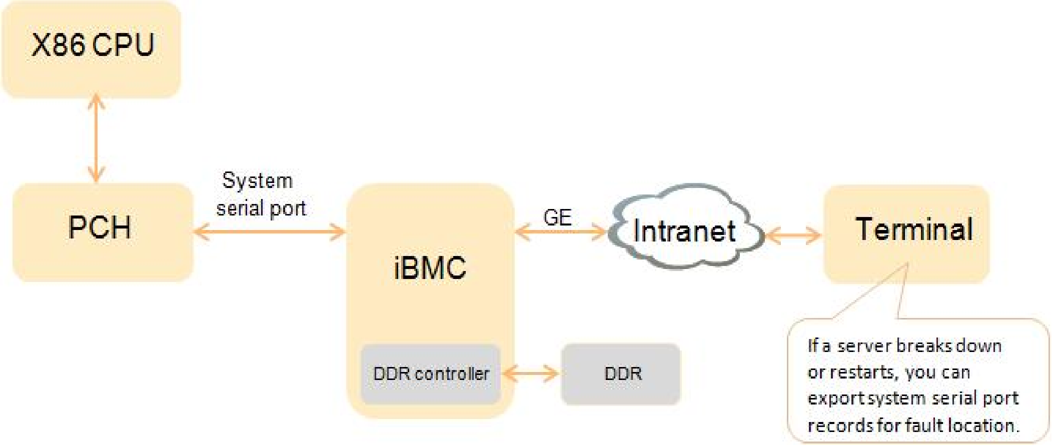
Figure 3-47 SOL (x86)



3.8.2 Recording System Serial Port Data

The iBMC records system serial port data in real time. **Figure 3-48** shows how the function is implemented. The recorded data is stored in DDR. If the data exceeds 2 MB, the earliest data will be overwritten. When the system breaks down or restarts, you can export and view the serial port data from iBMC.

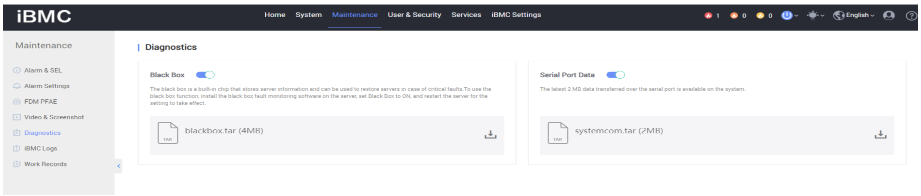
Figure 3-48 Recording system serial port data (x86)



If a server breaks down or restarts, you can export system serial port records for fault location.

Display on the WebUI

Figure 3-49 Display on the WebUI



The black box is a built-in chip that stores server information and can be used to restore servers in case of critical faults.To use the black box function, install the black box fault monitoring software on the server, set Black Box to ON, and restart the server for the setting to take effect.

blackbox.tar (4MB)

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

systemcom.tar (2MB)

3.9 Security Management

3.9.1 Account Security

- The iBMC supports CLI, SNMP, Web, IPMI, and Redfish management interfaces, and provides unified user management. A maximum of 16 users can be added. Users can be modified and deleted.

  The iBMC ensures account security by using measures, such as password complexity check, disabling of historical passwords, password validity period, minimum password validity period, anti-brute force cracking, manual account lockout, and online user logout.

  Password complexity check verifies complexity of the passwords set by users to prevent simple passwords. 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: **`~!@#$%^&*()-_=+\|[{}];:'",<.>/?**

  – Contains 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.

Disabling of historical passwords sets the number of historical passwords retained. The new password cannot be the same as the historical passwords.

Password validity period defines the validity period of a password. If a password has expired, it cannot be used to log in. Users will be prompted to change the password 10 days before the password is expired.

Minimum password validity period means that the password cannot be changed within this period. The purpose of setting the minimum password validity period is to prevent repeated use of historical passwords as the password is frequently changed.

Defense against brute force password cracking: An account will be locked if the number of consecutive invalid login attempts reaches the specified number. The iBMC also supports an anti-brute force cracking mechanism for SNMP long community names.

User lockout policy: Set the maximum number of consecutive invalid login attempts allowed and the account locking duration. After a user account is locked, the user can attempt to log in only after the account locking duration expires. The system administrator can also unlock a user account using the command line. If you do not manually unlock the system, the system automatically unlocks the user when the locking time expires.

Long SNMP community name: You can enable this function to enforce a minimum of 16 characters for community names. Complexity check also applies to community names.

3.9.2 Authentication Management

Authentication must be performed for the access to the iBMC from users or upper-layer management system through the web, CLI, SNMP, IPMI, or Redfish interface. The access is allowed only when the authentication is successful.

The iBMC supports local authentication and LDAP authentication. It supports user name + password authentication, SSH public key authentication, two-factor authentication for USB Key certificates, and secondary authentication for important operations.

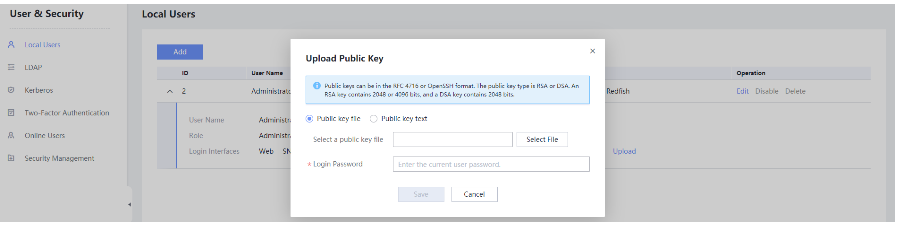
SSH public key authentication: SSH supports username + password authentication and public key authentication. The public key authentication is applicable to automatic configuration tools.

Public key authentication provides the following advantages:

- Login authentication does not need interactions.
- The private key is long and encrypted.

Public keys can be in the RFC 4716 or OpenSSH format. The public key type is RSA or DSA. An RSA public key contains 2048 or 4096 bits. A DSA public key contains 1024 or 2048 bits.

Each account supports only one public key. Public keys can be imported as text or a file. You can view the hash values of imported public keys. For security purposes, disable SSH password authentication after enabling SSH public key authentication.



Upload Public Key

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 2048 bits.

● Public key file ○ Public key text

Select a public key file

* Login Password: Enter the current user password.

ID	User Name		Operation
2	Administrato	Redfish	Edit Disable Delete

User Name: Administra
Role: Administra
Login Interfaces: Web SN

Two-Factor Authentication

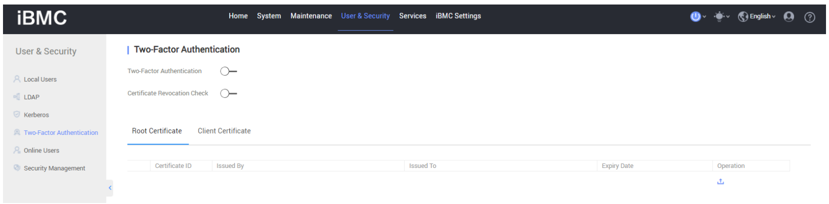
Two-factor authentication requires both the client certificate and password.

It effectively prevents attacks caused by password leakage. If two-factor authentication is enabled, login is allowed only if:

- The client's certificate passes the authentication performed by the CA root certificate imported into the iBMC.
- The client's certificate is consistent with the client certificate imported into iBMC.

Currently only iBMC WebUI supports two-factor authentication. After two-factor authentication is enabled, password and LDAP authentication modes are not supported. Two-factor authentication provides the following features:

- The client's certificate can be imported into the browser or stored in a USB key.
- A maximum of 16 different CA root certificates can be imported.
- Enabling two-factor authentication will disable all interfaces that do not support two-factor authentication, that is, only SNMP and IPMI are supported and used for interaction with the NMS. Two-factor authentication is disabled by default and can be enabled through the Web or SNMP interface.
- Certificate revocation check is supported and disabled by default. If certificate revocation check is enabled, invalid certificates cannot be used.



Two-Factor Authentication

Two-Factor Authentication ○—

Certificate Revocation Check ○—

Certificate ID	Issued By	Issued To	Expiry Date	Operation

Two-factor authentication based on the USB key eliminates password leakage in traditional account and password authentication. The login is allowed only when the user has the USB key and the PIN code. Before applying the two-factor authentication, you need to import the certificate and CA certificate to the iBMC, and insert the USB Key into the client (local PC). When connecting to the iBMC WebUI using a browser, you need to enter the PIN code of the USB Key. The certificate can be imported to the browser and sent to the server for verification only if the PIN code is correct.

Secondary Authentication

The iBMC provides a secondary authentication on login users for important management operations, such as configuration of users and permissions, and public key import operations. The operations can be performed only after the authentication is successful. Secondary authentication can prevent unauthorized users from using the login connections established by authorized users.

3.9.3 Authorization Management

- Users of the iBMC can be classified into the following types:
  - Administrator: The administrator can perform all operations.
  - Operator: The operator can perform operations excluding user management, debugging and diagnosis, and security configuration.
  - Common user: Common users can only query information excluding OS information and operation logs, and change their own passwords.
  - Custom user: A user who can perform the specified operations. The iBMC supports a maximum of four custom user roles. The system administrator can define custom roles by selecting from the **User Mgmt**, **Basic Mgmt**, **KVM**, **VMM**, **Security Mgmt**, **Power Control**, **Diagnostics**, **Query**, and **Own password & SSH** options provided on the iBMC WebUI.

Figure 3-50 Customized role application

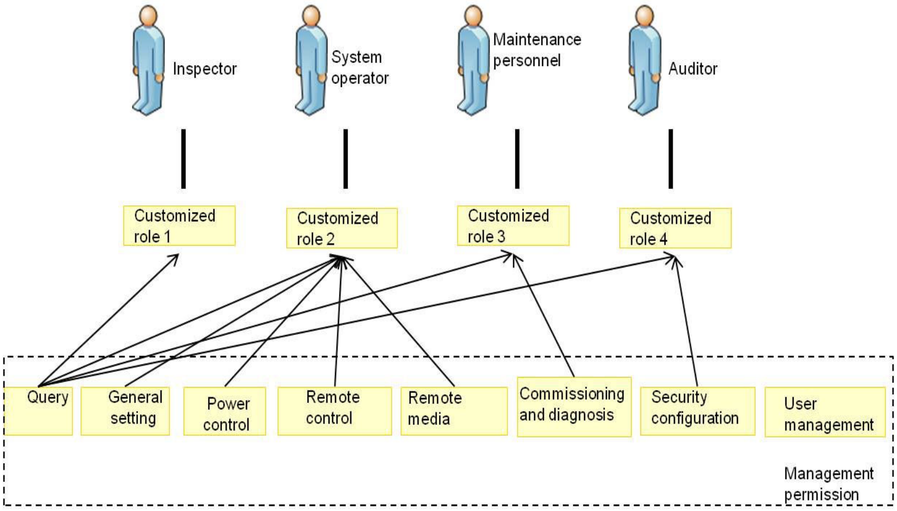
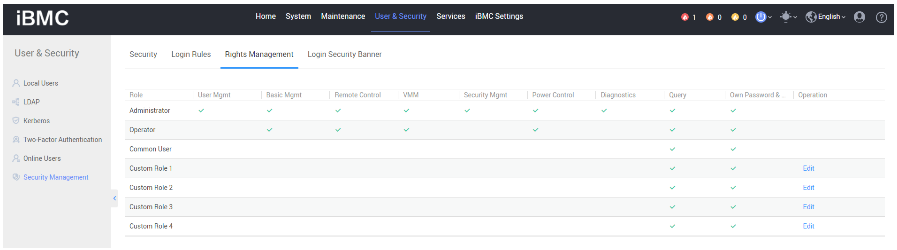


Figure 3-51 Role customization page



Role	User Mgmt	Basic Mgmt	Remote Control	VMM	Security Mgmt	Power Control	Diagnostics	Query	Own Password & ...	Operation
Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Operator		✓	✓	✓		✓		✓	✓	
Common User								✓	✓	
Custom Role 1								✓	✓	Edit
Custom Role 2								✓	✓	Edit
Custom Role 3								✓	✓	Edit
Custom Role 4								✓	✓	Edit

3.9.4 Certificate Management

The SSL certificate is used to verify the website before a web HTTPS connection is set up.

Certificate management including the following:

- Query certificate information (including the user, issuer, validity period, and serial number)
- Generate the CSR file.
- Import the signature certificate in PKCS#7 format (containing only the public key) generated by the CSR
- Import a customized certificate in PKCS#12 format (containing the public key and private key).

The certificate supports only the X.509 format. The encapsulation format can be PKCS#7 or PKCS#12. The PKCS#12 certificate supports a password set for the private key.

The iBMC uses self-signed SSL certificates by default. The SHA256RSA (2048 bits) signature algorithm is used. For security purposes, import self-signed certificate to replace the default certificate in the iBMC. Users can replace the default certificate using either of the following methods:

Method 1

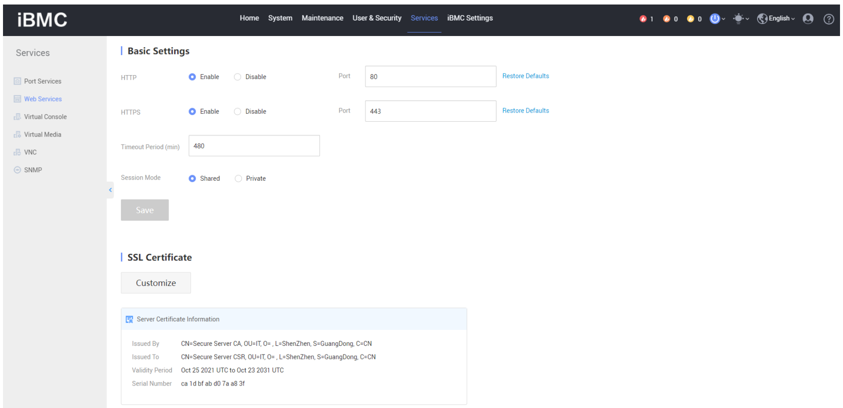
1. Log in to the iBMC WebUI, and modify the user information on the WebUI.
2. Generate a CSR file.
3. Export the CSR file.
4. Submit the CSR file to the CA organization to generate a PKCS#7 signature certificate.
5. Import the signature certificate to the iBMC.
6. Restart the iBMC for the certificate to take effect.

> NOTE
>
> The signature certificate must match the CSR. Otherwise, the certificate cannot be imported.

Method 2

1. Generate a self-defined certificate using the customer's CA server or purchase a certificate from the CA organization.
2. Log in to the iBMC WebUI and import the certificate to the iBMC.
3. Restart the iBMC for the certificate to take effect.

Figure 3-52 SSL certificate management page



Basic Settings

HTTP ● Enable ○ Disable Port 80 Restore Defaults

HTTPS ● Enable ○ Disable Port 443 Restore Defaults

Timeout Period (min) 480

Session Mode ● Shared ○ Private

SSL Certificate

Server Certificate Information

Issued By CN=Secure Server CA, OU=IT, O= , L=ShenZhen, S=GuangDong, C=CN
Issued To CN=Secure Server CSR, OU=IT, O= , L=ShenZhen, S=GuangDong, C=CN
Validity Period Oct 25 2021 UTC to Oct 23 2031 UTC
Serial Number ca 1d bf ab d0 7a a8 3f

In the scenario where interfaces such as Redfish involve accessing a remote shared path, the peer server certificate can be verified before the remote HTTPS shared path is accessed. The root certificate corresponding to the certificate of the remote server that shares files can be imported to the iBMC. The iBMC verifies the peer server certificate when the remote shared path is accessed. In this way, the file sharing server is prevented from being forged, and the validity of the shared file can be effectively ensured.

3.9.5 Session Management

When a session is established, the 192-bit session ID is generated from a secure random number. A user cannot set up multiple sessions at the same time.

A session can be terminated using either of the following methods:

- Termination due to timeout: The mechanism of disconnecting silent connections upon timeout is used for CLI, web, and SFTP sessions. If no operation is performed within the timeout period, the session will be automatically disconnected.
- Manual termination: A user can initiate a request to terminate a session. The administrator can also terminate other sessions.

3.9.6 Security Protocols

By default, SFTP, SSH, HTTPS, SNMPv3, and RMCP+(IPMILAN) are used by default to access the iBMC. Transmission channels are encrypted using security protocols. Insecure protocols HTTP and SNMPv1/v2c and RMCP (IPMILAN) are disabled by default.

The secure transmission protocols provide the following features:

SSH

1. Supports user password authentication and public key authentication.
2. Supports SSH V2.
3. Supports secure encryption algorithms AES128-CTR, AES192-CTR, and AES256-CTR, AES128-GCM, AES256-GCM, and Chacha20-Poly1305.

SFTP

1. Only the**/tmp** directory allows files to be uploaded and downloaded.
2. The files uploaded to the**/tmp** directory do not have the execute permission by default.

HTTPS

The iBMC supports TLS1.0 and later versions. TLS1.1, and TLS1.2 are enabled by default to maintain compatibility with the browser. Users can log in to the iBMC and disable TLS1.1 for security purposes.

SNMPv3

1. Authentication algorithms SHA and MD5 are supported, and can be configured by users.
2. Encryption algorithms AES and DES are supported, and can be configured by users.

3.9.7 Data Protection

All sensitive data related to passwords and keys on the iBMC is encrypted to ensure data security.

The iBMC supports encryption and signature protection of upgrade packages to prevent the content of the upgrade package from being cracked and modified and ensure confidentiality and integrity of the upgrade packages.

In addition to encryption, the iBMC encapsulates the Linux shell. After logging in to the iBMC over SSH or serial port, users cannot directly access files in the file system. This prevents file damage and software information leakage.

The iBMC supports backup of key data files and calculates and saves the file checksum. It also provides a backup and restore mechanism for file verification failures to prevent data file damage caused by abnormal power-off of the system.

Table 3-10 iBMC data encryption

Data	Encryption Algorithm
SSH/SFTP user password	SHA512
Web user password	AES128
SNMPv3 user password	MD5, SHA-1, SHA-256, SHA-512
SNMPv1/v2c communicate name	AES128
RMCP+ user password	AES128
Serial port data	SHA512
SSL certificate	AES128
Upgrade packages	AES128

Sensitive data generated during system running will be cleared immediately after being used.

3.9.8 Security Configuration

1. Access Policy

   Web access is secured by using login rules. The login rules specify the time, IP address, and MAC address allowed for access. You can configure the time, IP address segment, and MAC address whitelist to allow only users that meet the requirements to access the system through the management channel. This allows you to manage and configure the system and minimize the access to the server management interface.

   You can set the login whitelist that supports a maximum of three login rules. A user who follows any of these rules can log in to the iBMC. Otherwise, login fails.

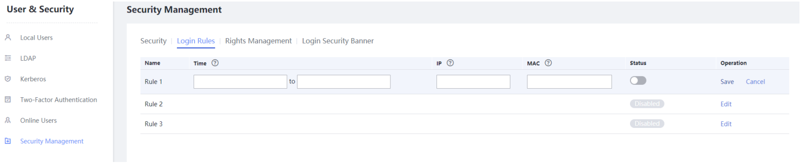
   Users who comply with any one of three rules can log in. Login rules can be applied to all local users and LDAP user groups.

   Each login rule contains the following conditions:

Time: includes the start time and end time in the format of *YYYY-MM-DD HH:MM*, *YYYY-MM-DD, or HH:MM*. The value can be empty.

IP: supports a single IPv4 address or IPv4 address segment, and does not support an IPv6 address. The value can be empty.

MAC: specifies the MAC address or MAC address range allowed for login. This parameter can be empty.


User & Security
Local Users
LDAP
Kerberos
Two-Factor Authentication
Online Users
Security Management
Security Management
Security | Login Rules | Rights Management | Login Security Banner

Name	Time	IP	MAC	Status	Operation
Rule 1	to				Save Cancel
Rule 2				Disabled	Edit
Rule 3				Disabled	Edit

Application scenarios:

Time: allows maintenance only in the specified time period. For example, if some data centers are not allowed to be accessed after work, you can configure the login time to restrict user access after work.

IP and **MAC**: allow access from specified IP addresses and MAC addresses to prevent large-scale network attacks.

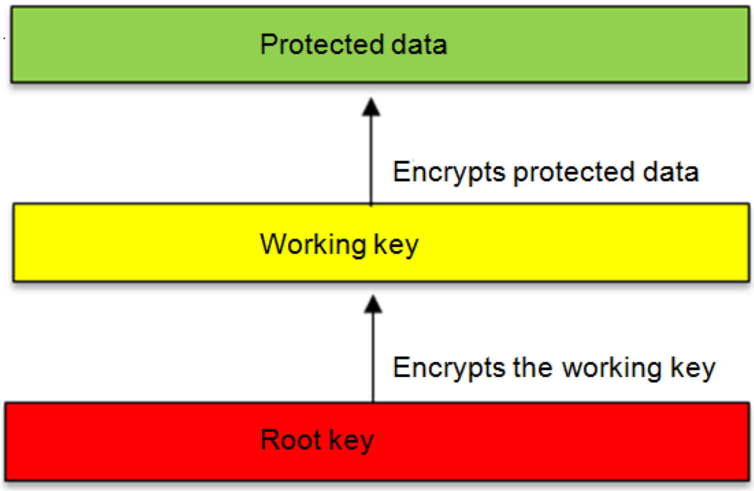
2. System Lock

   The iBMC supports the system lock function. After the system lock function is enabled, the user configuration, common configuration, virtual console configuration, and security configuration in the system are locked and cannot be changed. The power control, virtual media, and query functions are available. This function prevents the system configuration from being changed unexpected or maliciously.

   Only the system administrators can enable or disable the system lock function. After the system lock function is enabled, the web, CLI, SNMP, Redfish, and IPMI interfaces are locked and cannot be configured.

3.9.9 Key Management

The iBMC key management involves root key and working key. The root key is used to encrypt the working key, and the working key encrypts the protected data. Key management



- Key generation: A root key is generated based on a secure random number and is divided into multiple parts for storage. A working key is generated based on a secure random number.
- Key usage: Each key is used for only one purpose.
- Key storage: The root key is divided into multiple parts and stored separately. Only authorized users can manage the root keys. The working key is encrypted using the root key during storage.
- Key renewal: The keys can be manually updated. After the command for updating the key is executed, the system generates a new key randomly and the old key is destroyed.

3.9.10 System Hardening

The iBMC allows minimum OS installation. The embedded Linux system is tailored, and only mandatory components are installed. Unused components and commands are deleted.

The Linux shell commands are encapsulated and hardened, which shields the support for Linux system commands. Only the commands in the whitelist can be executed.

Security hardening has been performed on the SSH and Apache servers. Only secure algorithms are supported. Insecure protocols and ports are disabled by default.

3.9.11 Log Audit

The iBMC supports log audit. The log information includes the user name, user IP address, operation time, and specific operations. The iBMC records SELs, user operation logs, system running logs, and security logs. Users can view and audit the logs through the interface provided by the iBMC.

The iBMC logs are saved in the flash file system of the iBMC in real time. When the log files reach the maximum storage capacity, a message will be displayed to remind the user. When the size of the log file reaches the specified size, the log file will be automatically backed up. Unauthorized users cannot view or download log files.

The iBMC supports remote log dump using Syslog. The logs are stored in a remote syslog server to prevent the local logs from being overwritten by new logs when the number of logs files reaches the limit. The iBMC supports verification of the syslog server.

3.9.12 DICE

The iBMC based on the Hi1711 chip provides the DICE to receive challenge requests and return the DICE certificate chain. iBMC supports generating the trusted boot certificate chain based on the DICE. The certificate chain is used for challenge-response authentication to verify the integrity of boot firmware.

3.9.13 Secure Boot

The iBMC based on Hi1711 supports secure boot based on the processor RoT, which verifies digital signatures for the U-Boot, BMC, BIOS, and ME. The boot is allowed only after the digital signature verification is successful, preventing the firmware from being tampered with. In addition, it supports the PFR mechanism. After the iBMC is started, it obtains the BIOS signature verification flag. If the verification fails, the BIOS file in the backup area is used to upgrade the BIOS again. If the iBMC fails to start for three consecutive times, it starts from the standby area to restore the management function.

3.9.14 PFR

The iBMC based on Hi1711 allows the standby area to become the active area after the iBMC fails to be started for three times, and restores the partition firmware that fails to pass the verification. After the iBMC starts, it obtains the BIOS signature verification result. If the verification fails, it uses the BIOS file in the backup area to upgrade the BIOS again.

3.9.15 Revocation of Insecure Versions

The iBMC based on Hi1711 uses a unique version identifier. You can revoke a specified insecure version. After the revocation, the specified risky version will be blocked before the upgrade, preventing the risky version from being upgraded by mistake.

3.9.16 E-Warranty Management

The iBMC based on Hi1711 chip allows users to query and set e e-warranty information, to use the Redfish/Web interface to query the product name, product SN, production date, UUID, service start time, and service life, and to configure the service start time and service life.

3.9.17 PCI DSS Certification

PCI DSS (Payment Card Industry Data Security Standard) is a global information security standard for the third-party payment industry. It strives to adopt consistent data security measures internationally. The 2288H V7, 2288H V6, and 2488H V6 servers have obtained the PCI DSS 4.0 certification.

3.9.18 International CC EAL4+ Certification

Common Criteria for Information Technology Security Evaluation (CC) is used to evaluate the security of information systems and information products. The evaluation of CC is in respect of security function requirements and security assurance requirements. The iBMC has obtained the international CC EAL4+ certification.

3.9.19 China CC EAL4 Certification

China Cybersecurity Review Technology and Certification Center conducts information security certification for IT products based on the information technology security evaluation criteria and related technical requirements to evaluate the security of products, to protect users' information security and safeguard users' interests. The manufacturer's IT product obtains the information security certificate, which indicates that the product meets the relevant standards and technical requirements. The iBMC has obtained the IT product EAL4 certificate of information security certification.

3.10 Access Management

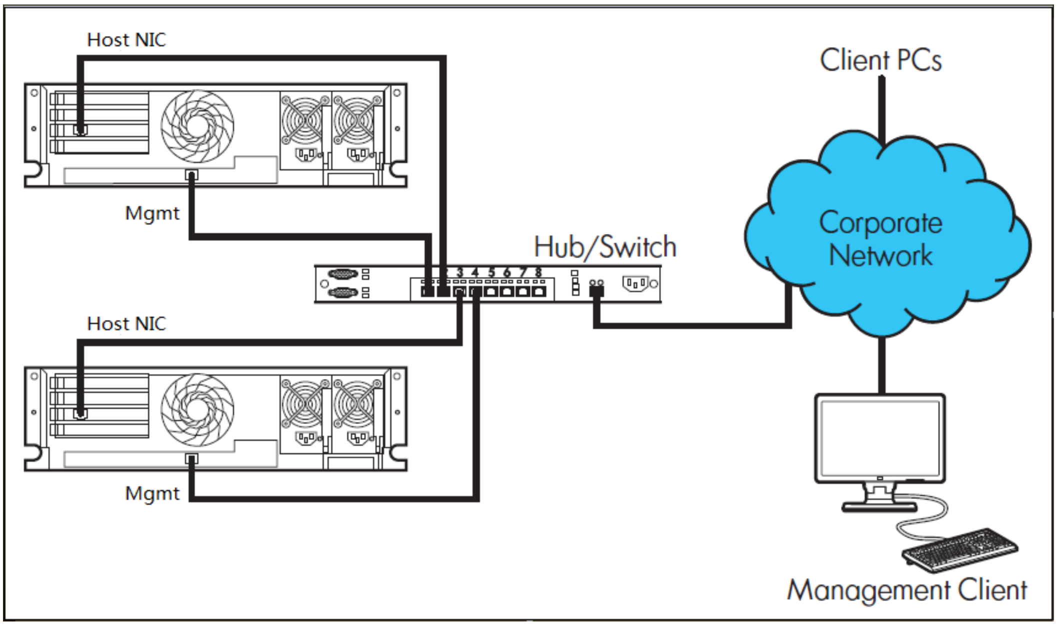
The iBMC supports both IPv4 and IPv6 addresses and access over a dedicated management port or shared network port using the NC-SI function. The shared network port supports the VLAN function.

3.10.1 Management Network Port Auto-Adaptation

A rack server or node server has two management network ports: a GE management network port and a sideband network port using NC-SI (share the physical management network port with the host). The NC-SI function automatically associates the logical network port with a physical network port based on the network port link status.

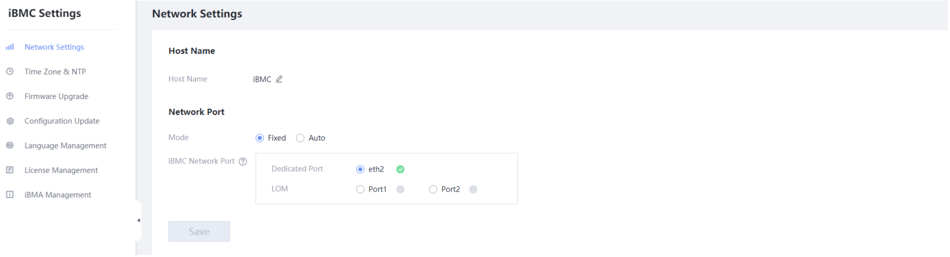
After auto-adaptation is enabled for a network port and the server network is changed, you can use a network cable to connect to the dedicated management network port or sideband management network port to access the management GUI without any new network settings and perform smooth switch. This eliminates complicated configuration and improves the maintenance efficiency.

Figure 3-53 Management network connection



You can query and set the iBMC network port data on this page. If auto-adaptation is selected, you can specify a host network port (port 1 by default) as the shared network port. For details, see **Figure 3-54**.

Figure 3-54 Configuring network port auto-adaptation



Network Settings

Host Name

Host Name: iBMC

Network Port

Mode: ● Fixed ○ Auto

iBMC Network Port:
- Dedicated Port: ● eth2
- LOM: ○ Port1 ○ Port2

3.10.2 NC-SI

NS-CI enables the management system and the host system to share a physical network port on the host using the NC-SI technology, implementing management and service handling, simplifying networking, and reducing ports on the switch. Preferentially considering the service data, the maximum bandwidth for data management is 100 Mbit/s. For the security purpose, divide the management and service in different network segments using the VLAN technology.

Figure 3-55 NS-CI framework

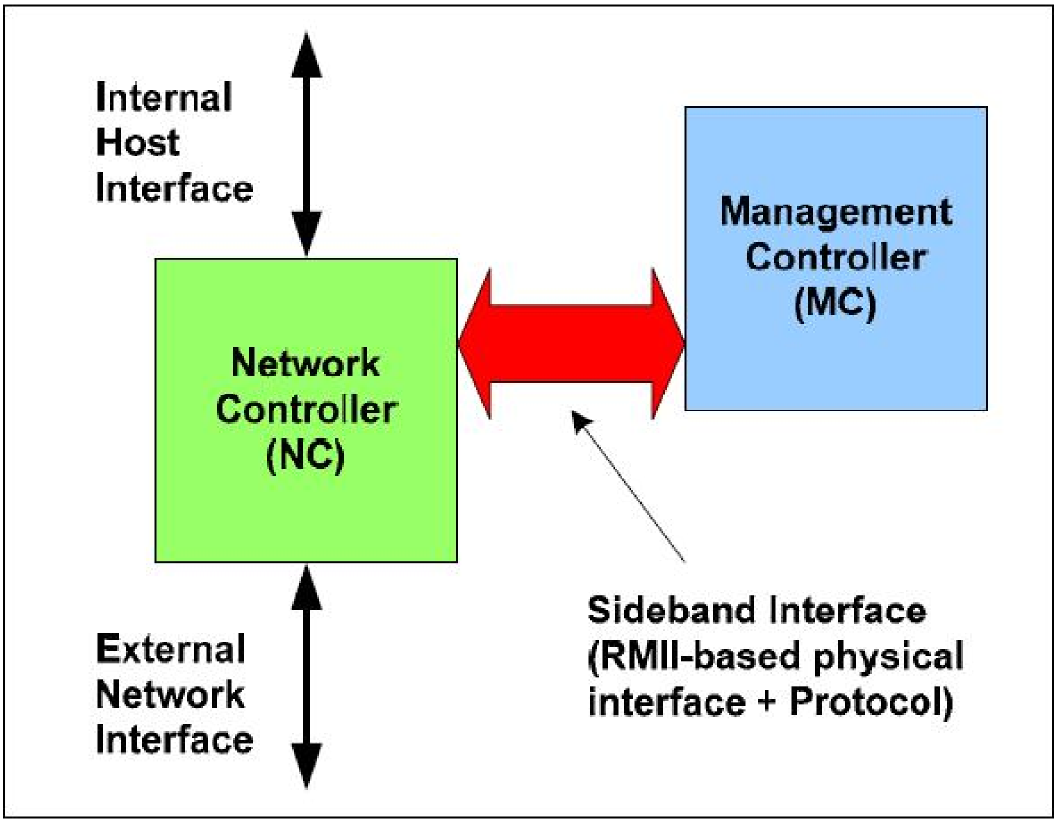
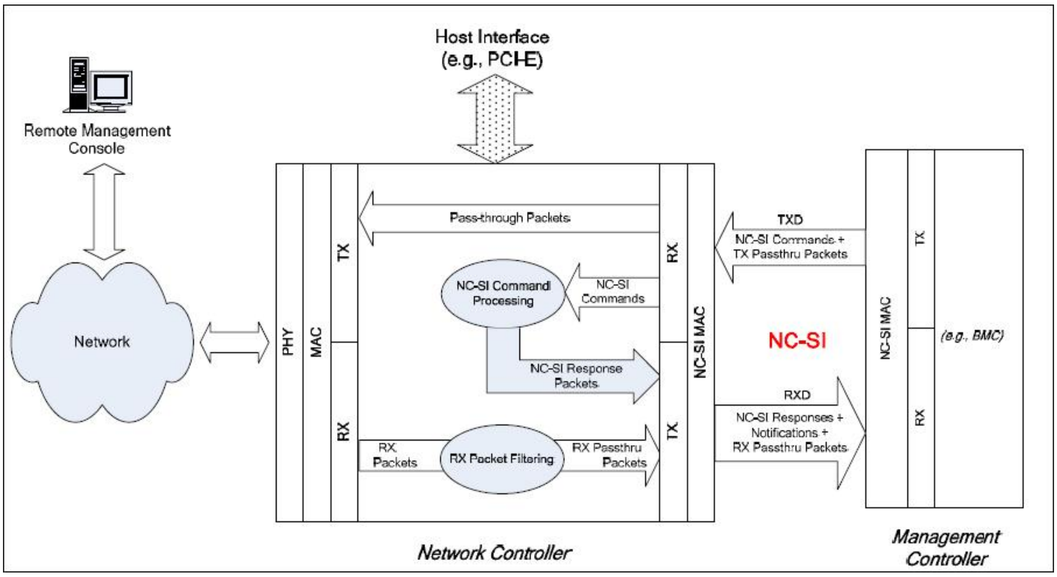

Internal Host Interface
Management Controller (MC)
Network Controller (NC)
Sideband Interface (RMII-based physical interface + Protocol)
External Network Interface

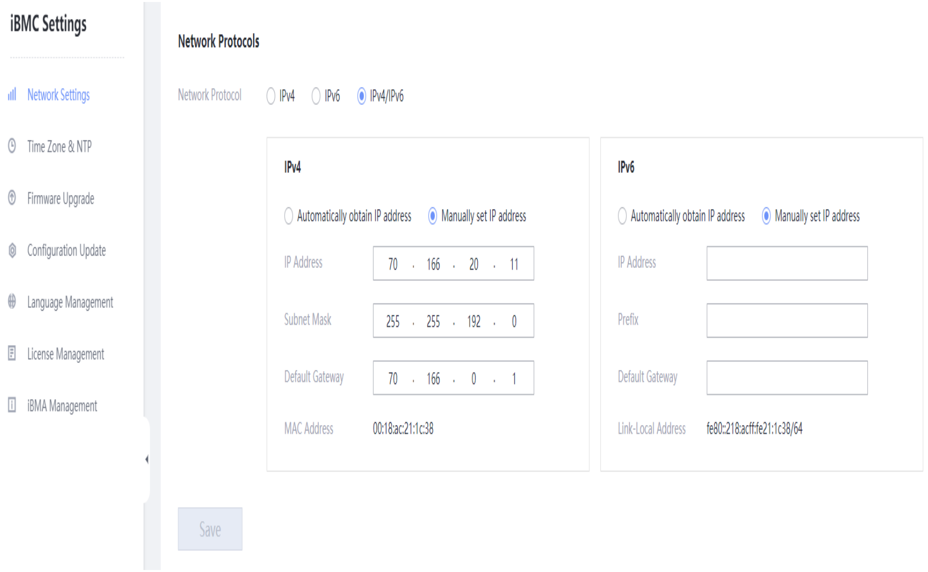
Figure 3-56 NS-CI data flow diagram



3.10.3 IPv6

iBMC supports IPv6 to ensure sufficient IP addresses because IPv4 addresses are insufficient. All the Web, SSH, SNMP, IPMI LAN, and Redfish interfaces supported by iBMC support IPv6. Physical channels of the dedicated management network port and NC-SI also support IPv6.

Figure 3-57 IPv6 address configuration screen



iBMC Settings

- Network Settings
- Time Zone & NTP
- Firmware Upgrade
- Configuration Update
- Language Management
- License Management
- iBMA Management

Network Protocols

Network Protocol ○ IPv4 ○ IPv6 ● IPv4/IPv6

IPv4

○ Automatically obtain IP address ● Manually set IP address

IP Address	70 . 166 . 20 . 11
Subnet Mask	255 . 255 . 192 . 0
Default Gateway	70 . 166 . 0 . 1
MAC Address	00:18:ac:21:1c:38

IPv6

○ Automatically obtain IP address ● Manually set IP address

IP Address	
Prefix	
Default Gateway	
Link-Local Address	fe80::218:acff:fe21:1c38/64

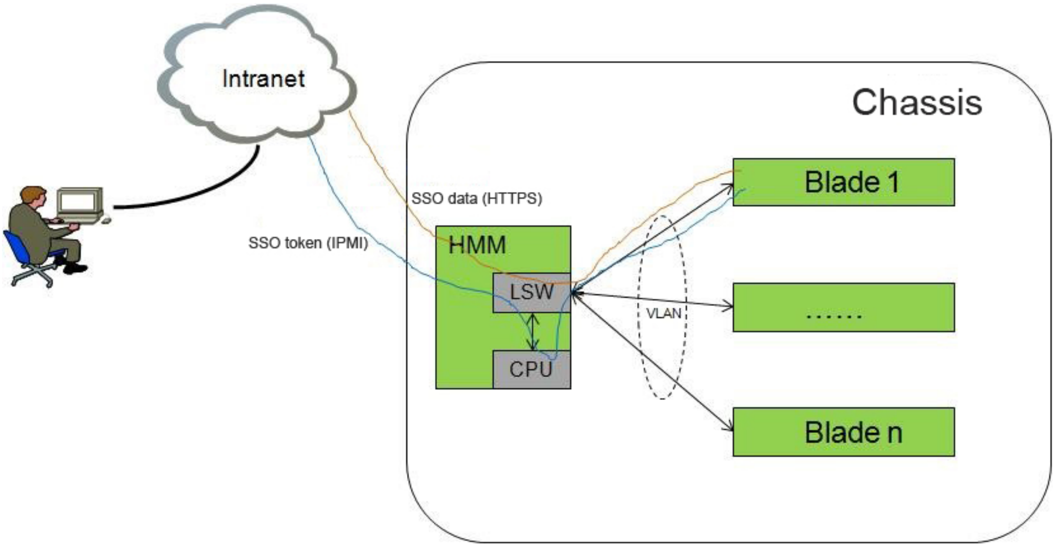
The iBMC IPv6 address can be manually set or automatically assigned by the DHCP server.

3.10.4 SSO

To prevent users from repeatedly entering user names and passwords when accessing different management WebUIs, iBMC supports the single sign-on (SSO) function of the network management system (NMS) or chassis. SSO allows users who have logged in to the NMS or chassis management module to directly access iBMC WebUIs or remote consoles without entering passwords again.

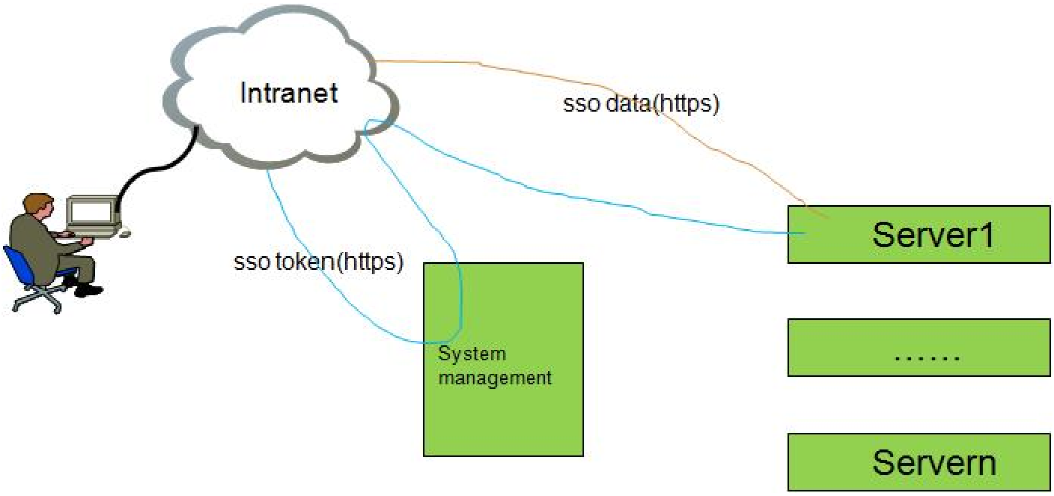
How chassis SSO works: After a user logs in to HMM WebUI and clicks the SSO link of iBMC of a blade, the HMM sends IPMI commands through the internal VLAN to obtain the SSO token from the iBMC, and uses the token to log in to the the iBMC WebUI or remote console over HTTPS. The iBMC operation permissions are specified by the HMM. For details, see **Figure 3-58**.

Figure 3-58 How chassis SSO works



How NMS SSO works: The servers are added to the NMS in advance. After a user logs in to the NMS WebUI and clicks the SSO link of iBMC of a server, the NMS obtains the SSO token from iBMC over HTTPS, and uses the token to log in to the iBMC WebUI or remote console through HTTPS. For details, see **Figure 3-59**.

Figure 3-59 How NMS SSO works



3.10.5 Local O&M

The V6 and V7 series servers can be connected to the iBMC management system through the USB management port. You can use a mobile application or a laptop to perform local maintenance and management operations, such as querying or configuring server information.

NOTE

For the local O&M, the hardware must include the iBMC direct connect management port. For details, see the user guide.

3.10.6 SSDP

SSDP is a "Simple Service Discovery Protocol", which defines how to discover network services on the network. The iBMC supports the sending of NOTIFY packets and the M-SEARCH response mechanism in the SSDP protocol. The control point (client) obtains the local link IPV6 address of the BMC through the SSDP packet, and implements the network access and network configuration of the BMC through this IP address. , to further realize the effect of managing BMC and managing BMC.

3.10.7 Firmware Alliance BMC Standard Compliance Test Certification

The iBMC has passed the compliance tests specified in the *T/CESA 1219-2022 Test Methods for Server BMC* of the Firmware Industry Technology Innovation Alliance, and met advanced or extended requirements (level 3).

3.11 Unified User Management

iBMC is a management subsystem based on the built-in CPU and the OS and provides only fixed maintenance and integration ports. The OS and applications are integrated. The OS (CLI), SNMP, IPMI LAN, Web, and Redfish interfaces are independently managed by respective local users. To access iBMC through these interfaces, users have to set each interface. However, the unified user management function enables a user to access iBMC through all those interfaces as long as one interface is set. iBMC synchronizes the setting among all interfaces.

iBMC supports a maximum of 16 users and enables you to add, modify, and delete users. The user types and user rights are as follows:

Administrator: The user has all configuration and control rights for the iBMC.

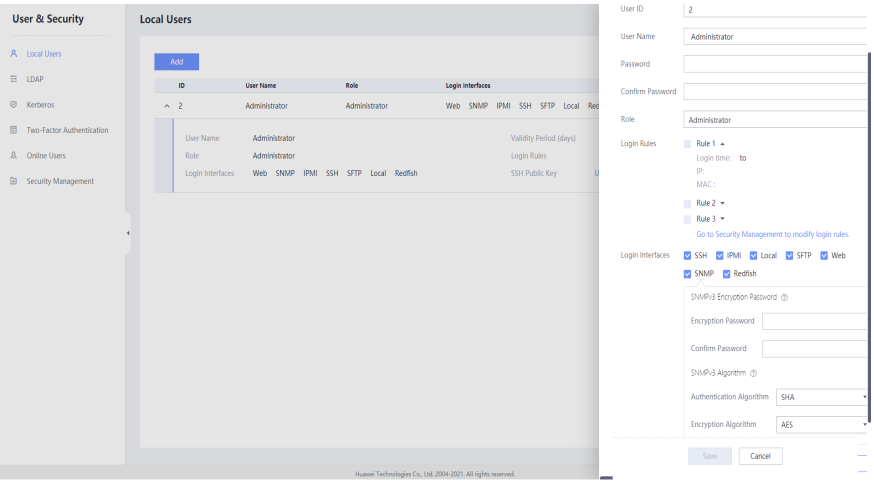
Operator: The user has all configuration and control rights, excluding user management and security configuration.

Common user: The user has only permission to view information, excluding OS information and operation logs.

Customized group: The user specifies its right.

Login interfaces: Types of interfaces through which the user can log in to the iBMC.

Figure 3-60 User management page


User & Security
Local Users
LDAP
Kerberos
Two-Factor Authentication
Online Users
Security Management
Add
Save
Cancel
Huawei Technologies Co., Ltd. 2004-2021. All rights reserved.

Local Users

	ID	User Name	Role	Login Interfaces
^	2	Administrator	Administrator	Web SNMP IPMI SSH SFTP Local Red

User Name Administrator
Role Administrator
Login Interfaces Web SNMP IPMI SSH SFTP Local Redfish
Validity Period (days)
Login Rules
SSH Public Key

User ID 2
User Name Administrator
Password
Confirm Password
Role Administrator
Login Rules □ Rule 1
Login time: to
IP:
MAC :
□ Rule 2
□ Rule 3
Go to Security Management to modify login rules.
Login Interfaces ☑ SSH ☑ IPMI ☑ Local ☑ SFTP ☑ Web ☑ SNMP ☑ Redfish
SNMPv3 Encryption Password
Encryption Password
Confirm Password
SNMPv3 Algorithm
Authentication Algorithm SHA
Encryption Algorithm AES

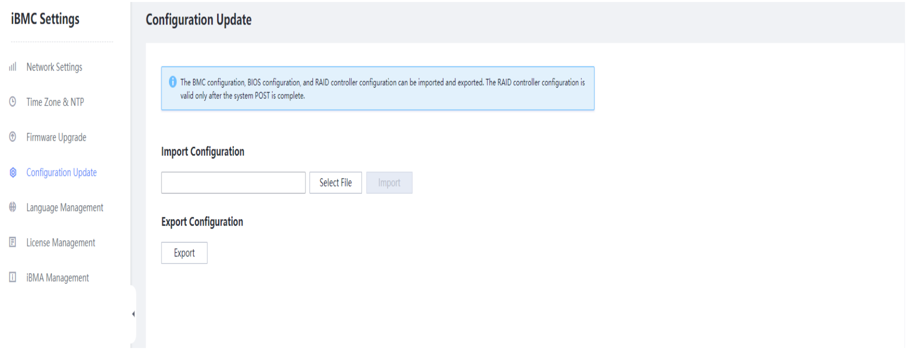
3.12 Configuration Management

3.12.1 Configuration Import and Export

The BMC, BIOS, and RAID controller configurations can be imported or exported as configuration files. Export the RAID controller configuration only when the system POST is complete. Users can remotely export server configurations. If a server is replaced, the exported configurations can be imported to the new server to quickly finish the configuration. A configuration file can also be imported to multiple servers of the same type at the same time to quickly complete the configuration of a large number of servers. Currently, the SNMP, CLI, web, and Redfish interfaces support configuration import and export.

The following figure shows the configuration import and export page on the iBMC WebUI.

Figure 3-61 Configuration import and export page



Configuration Update

The BMC configuration, BIOS configuration, and RAID controller configuration can be imported and exported. The RAID controller configuration is valid only after the system POST is complete.

Import Configuration

Export Configuration

3.12.2 BIOS Configuration

The iBMC supports remote query and configuration of all BIOS menu items through the Redfish interface.

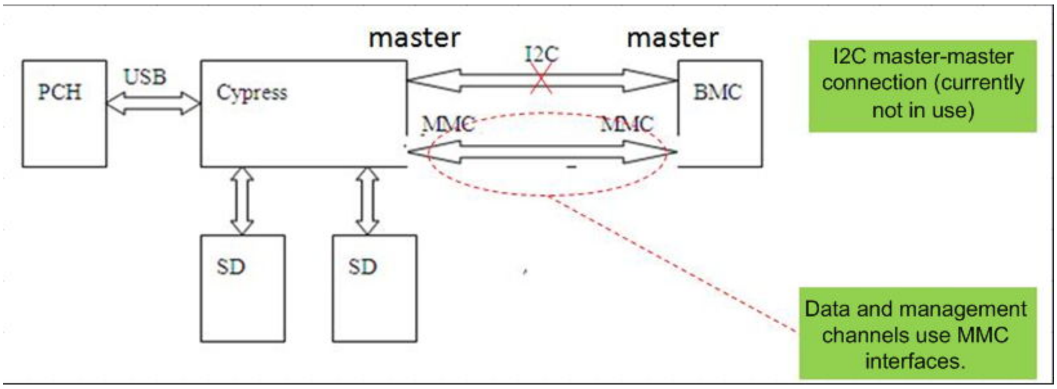
3.13 Storage Management

3.13.1 Built-in SD Cards

Each V3 server can be configured with up to two SD cards (optional) to meet the following requirements:

- Install the OS if the system has no drives or has only data drives.
- Store important data, such as important service data and host OS data, to implement isolation from guest OS data.

Figure 3-62 SD card connections


master
master
PCH
USB
Cypress
I2C
BMC
MMC
MMC
SD
SD
I2C master-master connection (currently not in use)
Data and management channels use MMC interfaces.

SD cards provide the following functions:

- By default, the two SD cards form a RAID 1 array.
- The default owner of the two SD cards is the host OS.
- RAID rebuild, with the start and end logs recorded.
- Detection of whether the number of read/write errors exceeds the threshold.
- RAID rebuild failure detection.
- Query of the SD card capacities, manufacturers, and serial numbers.

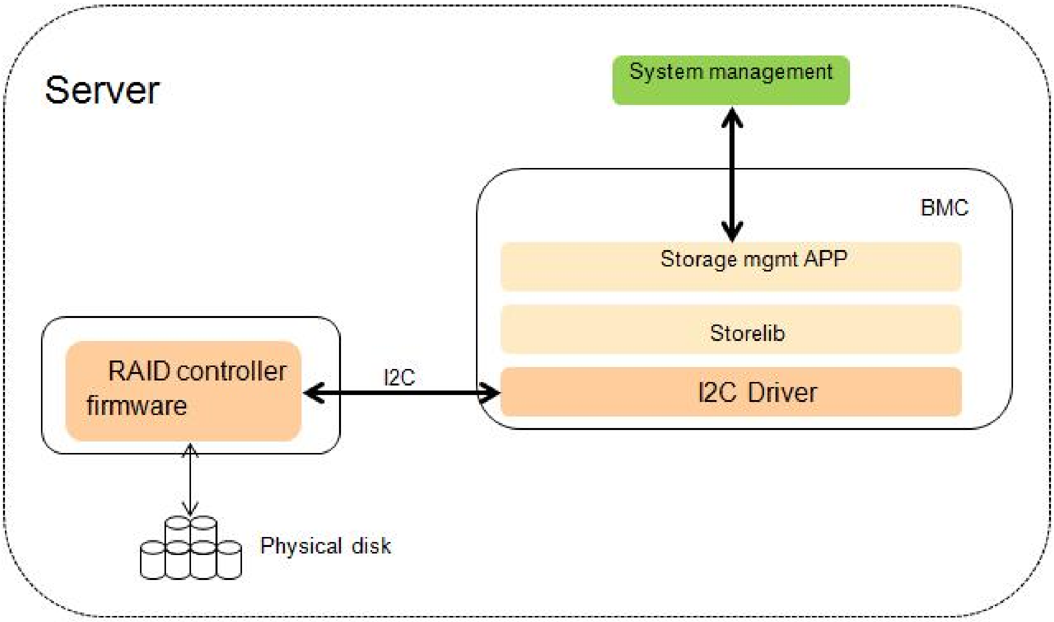
3.13.2 RAID and Drive Management

Hard drives are used to store OSs or user data. Therefore, drive management and monitoring are necessary.

The iBMC interacts with the RAID controller to implement out-of-band management of hard drives. Hard drive management relies on the RAID controller firmware. Currently, only the SAS3004iMR, LSI SAS3108, LSI SAS3008, LSI SAS 34 series, LSI SAS 35 series, and LSI SAS 93 series RAID controller cards support out-of-band hard drive management. A server does not support out-of-band hard drive management if one of the RAID controller cards on the server does not support out-of-band management.

However, if iBMA 2.0 software is installed on the OS, the iBMC can perform out-of-band management of hard drives and monitor SATADOMs and M.2 SSDs even if the RAID controller card does not support out-of-band RAID management.

Figure 3-63 Out-of-band hard drive management mechanism



Out-of-band hard drive management supports management of RAID controller cards, physical drives, and virtual drives. **Table 3-11**, **Table 3-12**, and **Table 3-13** list the supported properties.

Table 3-11 Parameters supported by out-of-band hard drive management (monitoring and query)

Component	Property	Note
RAID controller card	Name, type, health status, firmware version, driver version, capacitor status, SAS address, cache memory size, SAS rate, whether to retain the cache, boot drive, whether to enable physical drive failure history, DDR correctable ECC error count, PHY error code count, and driver name and version	Web, SNMP, Redfish, and CLI interfaces and one-click log collection are supported. The DDR correctable ECC error and PHY error code statistics are not available on the WebUI.
Physical drive	Health status, SN, model, capacity, firmware version, media type, interface type, hot spare status, manufacturer, rebuild status, patrol status, medium error count, prefailure count, other error count, maximum speed, link speed, SAS address, logical drive, power status, temperature, SSD remaining life, and SMART pre-alarm status	Web, SNMP, Redfish, and CLI interfaces and one-click log collection are supported. The medium error, prefailure, and other error statistics are not available on the WebUI.

Component	Property	Note
Logical drive	Running status, RAID level, read policies (default and current), write policies (default and current), strip size, capacity, whether physical drive write cache is enabled, consistency check status, member drive list, span depth, number of drives per span, and system drive letters	Web, SNMP, Redfish, and CLI interfaces and one-click log collection are supported.
Log	RAID controller card log export	RAID controller card logs are included in the logs collected through one-click collection.

📖 NOTE

Information about the driver name and version and system drive letters is displayed only after iBMA 2.0 has been installed.

Table 3-12 Configuration (available only when RAID card supports out-of-band management)

Component	Function
RAID controller card	RAID controller setup: ● Copyback ● Copyback on SMART error ● JBOD
Physical drive	Physical drive setup: ● Hot spare status ● Firmware status ● Location status
Logical drive	Allows you to create and delete logical disks and modify the following attributes of logical disks: VD name, read policy, write policy, I/O policy, access policy, background initialization, SSD caching, CacheCade logical disk, Disk Cache Policy, and boot disk.

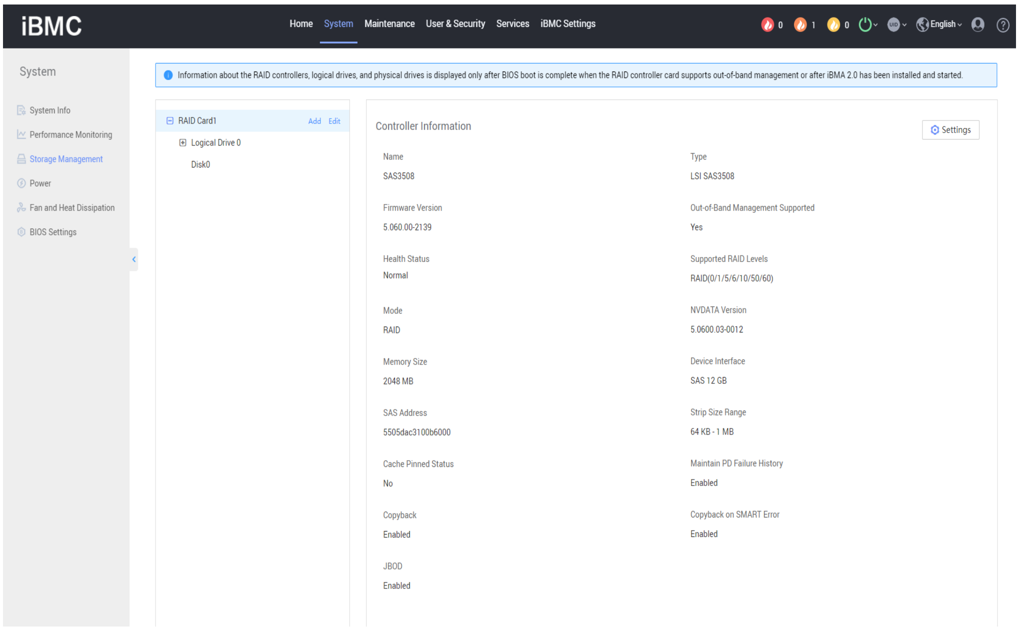
Table 3-13 Fault monitoring items

Component	Fault Types and Scenarios
RAID controller card	Internal error, non-zero memory UCE errors, memory ECC error threshold, non-zero NVRAM errors, BMC access failure

Component	Fault Types and Scenarios
Physical drive	Failure, non-zero predictive failures, rebuild failure, drive installed but not detected by the RAID controller card
Logical drive	If the logical drive is in the offline state, "In Critical Array" is reported for its absent physical member drives. If the logical drive is in the degraded or partially degraded state, "In Failed Array" is reported for its absent physical member drives.
BBU	Low voltage, BBU failure, BBU absence

The out-of-band hard drive management page displays information based on the hierarchical relationships of storage devices.

Figure 3-64 RAID controller card management



Information about the RAID controllers, logical drives, and physical drives is displayed only after BIOS boot is complete when the RAID controller card supports out-of-band management or after iBMA 2.0 has been installed and started.

Controller Information

Name
SAS3508

Type
LSI SAS3508

Firmware Version
5.060.00-2139

Out-of-Band Management Supported
Yes

Health Status
Normal

Supported RAID Levels
RAID(0/1/5/6/10/50/60)

Mode
RAID

NVDATA Version
5.0600.03-0012

Memory Size
2048 MB

Device Interface
SAS 12 GB

SAS Address
5505dac3100b6000

Strip Size Range
64 KB - 1 MB

Cache Pinned Status
No

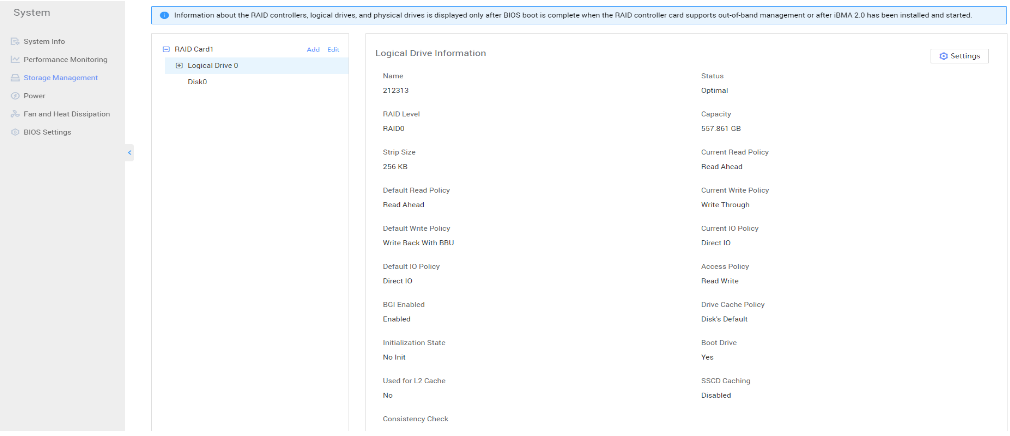
Maintain PD Failure History
Enabled

Copyback
Enabled

Copyback on SMART Error
Enabled

JBOD
Enabled

Figure 3-65 Logical drive management



Information about the RAID controllers, logical drives, and physical drives is displayed only after BIOS boot is complete when the RAID controller card supports out-of-band management or after iBMA 2.0 has been installed and started.

Logical Drive Information

Name
212313

Status
Optimal

RAID Level
RAID0

Capacity
557.861 GB

Strip Size
256 KB

Current Read Policy
Read Ahead

Default Read Policy
Read Ahead

Current Write Policy
Write Through

Default Write Policy
Write Back With BBU

Current IO Policy
Direct IO

Default IO Policy
Direct IO

Access Policy
Read Write

BGI Enabled
Enabled

Drive Cache Policy
Disk's Default

Initialization State
No Init

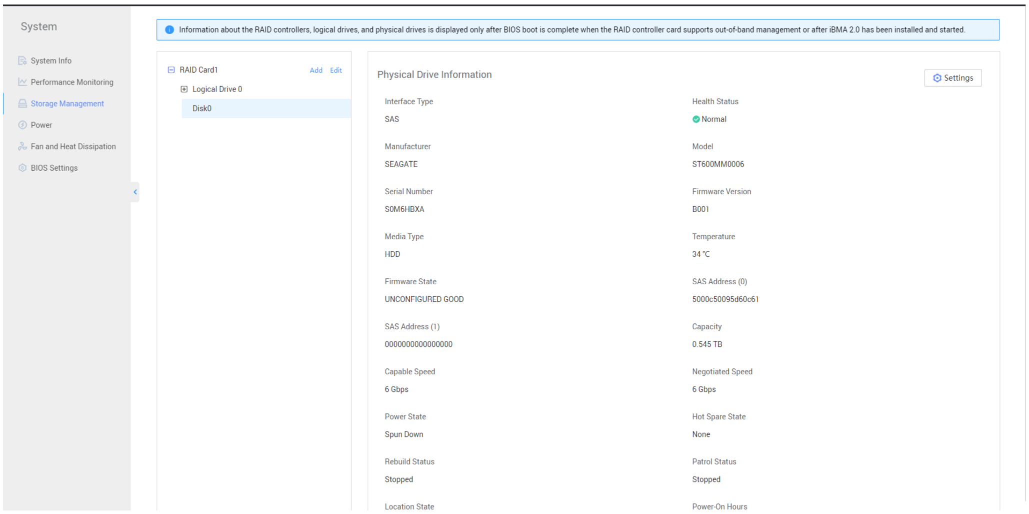
Boot Drive
Yes

Used for L2 Cache
No

SSCD Caching
Disabled

Consistency Check

Figure 3-66 Physical drive management

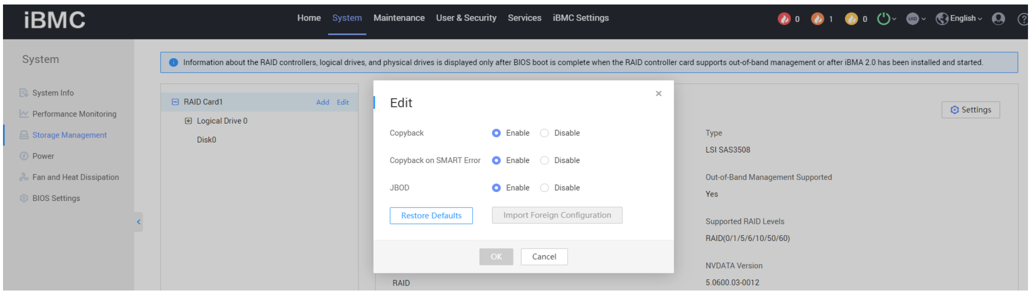


Information about the RAID controllers, logical drives, and physical drives is displayed only after BIOS boot is complete when the RAID controller card supports out-of-band management or after iBMA 2.0 has been installed and started.

Physical Drive Information

Interface Type SAS	Health Status Normal
Manufacturer SEAGATE	Model ST600MM0006
Serial Number S0M6HBXA	Firmware Version B001
Media Type HDD	Temperature 34 ℃
Firmware State UNCONFIGURED GOOD	SAS Address (0) 5000c50095d60c61
SAS Address (1) 0000000000000000	Capacity 0.545 TB
Capable Speed 6 Gbps	Negotiated Speed 6 Gbps
Power State Spun Down	Hot Spare State None
Rebuild Status Stopped	Patrol Status Stopped
Location State	Power-On Hours

Figure 3-67 RAID configuration screen



Information about the RAID controllers, logical drives, and physical drives is displayed only after BIOS boot is complete when the RAID controller card supports out-of-band management or after iBMA 2.0 has been installed and started.

Edit

Copyback ● Enable ○ Disable

Copyback on SMART Error ● Enable ○ Disable

JBOD ● Enable ○ Disable

Type
LSI SAS3508

Out-of-Band Management Supported
Yes

Supported RAID Levels
RAID(0/1/5/6/10/50/60)

NVDATA Version
5.0600.03-0012

RAID

NOTE

The RAID controller does not support RAID for NVMe drives. Therefore, the preceding management and monitoring modes apply only to SAS/SATA drives. Table 3-14 shows the management of NVMe drives.

Table 3-14 NVMe drive management items

Type	Item
Information query	Serial number, model, interface type, vendor, firmware version, remaining lifespan (%), and the following information obtained through the iBMA: maximum interface rate, negotiated interface rate, interface type, media type, capacity, and accumulated power-on time
Fault monitoring	Fault, SMART pre-alarm, overtemperature, insufficient lifespan

Table 3-15 M.2 and SATADOM management (based on iBMA 2.0)

Type	Item
Information query	Serial number, capacity, vendor, and temperature
Fault monitoring	Insufficient lifespan, 0 capacity, offline

NOTE

The M.2 provides the SATA interface to connect to the PCH or RAID controller card. The management feature listed in **Table 3-15** applies only to the scenario where the M.2 is connected to the PCH. The connection between the M.2 SSD and the RAID controller card belongs to hard drive out-of-band management.

3.14 Time Management

NTP

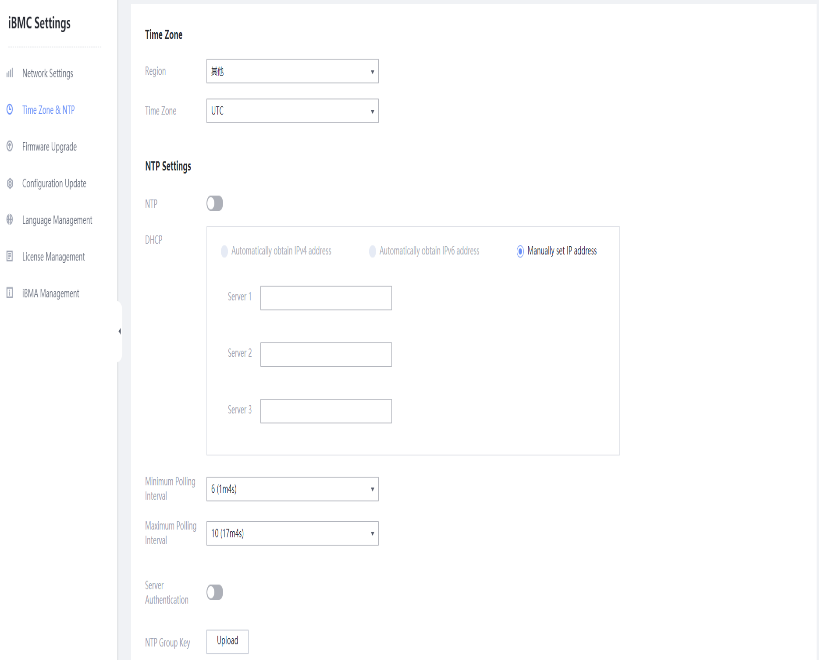
The Network Time Protocol (NTP) is used for synchronizing time for computers. The Network Time Protocol (NTP) is used for synchronizing time for computers. The server iBMC does not have the RTC hardware and supports synchronizing time from multiple time sources (one source at a time). NTP is disabled by default and can be enabled. The IPv4 or IPv6 addresses of the preferred and alternate NTP servers can be manually set or automatically obtained. If you choose to manually set IP addresses, fully qualified domain names (FQDNs) are supported. The iBMC also supports NTP server verification for security purposes.

If NTP is enabled, the iBMC does not switch to other time sources no matter whether time synchronization succeeds or not. If NTP is disabled, the iBMC synchronizes time from the default time source. Time synchronization failures and time source switching are all recorded in event logs.

Table 3-16 iBMC time sources

iBMC	Supported Time Source	Default Time Source
Rack server	Host RTC (BIOS or OS) and NTP	Host RTC (BIOS or OS)
Blade server	Chassis management module and NTP	Chassis management module
High-density server	Host RTC (BIOS or OS) and NTP	Host RTC (BIOS or OS)
Auxiliary management board	iBMC RTC and NTP	iBMC RTC

Figure 3-68 NTP configuration page



Time Zone

Region: 其他

Time Zone: UTC

NTP Settings

NTP: ○

DHCP: ○ Automatically obtain IPv4 address ○ Automatically obtain IPv6 address ● Manually set IP address

Server 1:

Server 2:

Server 3:

Minimum Polling Interval: 6 (1m4s)

Maximum Polling Interval: 10 (17m4s)

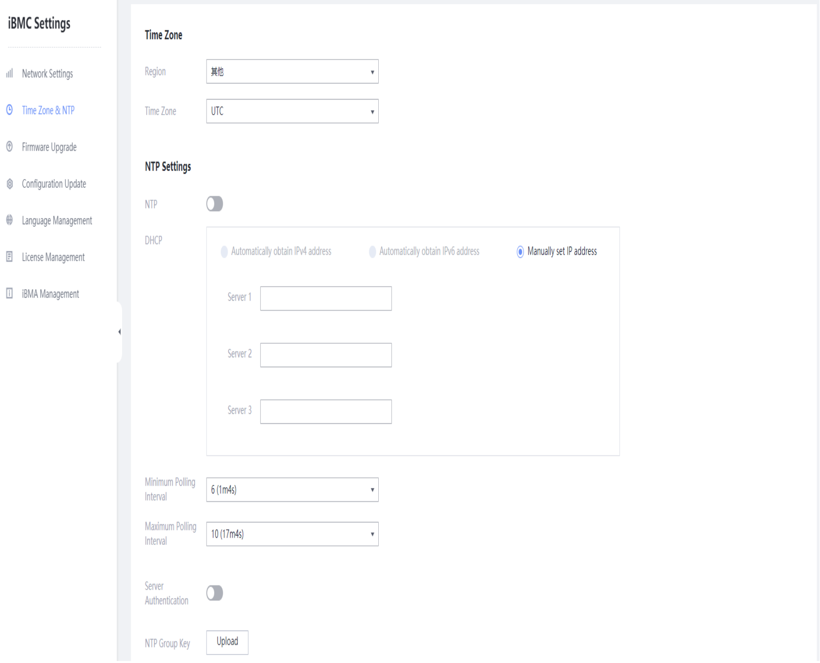
Server Authentication: ○

NTP Group Key: Upload

DST

The daylight saving time (DST), also called summer time, is a practice of regulating the local time for saving energy. Generally, clocks are adjusted forward one hour at the start of the summer to make full use of the daylight and save energy. The DST regulations vary with countries. At present, nearly 110 countries around the world use DST every year. For countries that do not use DST, configure the time zone on the iBMC WebUI.

Figure 3-69 DST Settings screen



Time Zone

Region: 其他

Time Zone: UTC

NTP Settings

NTP: ○

DHCP: ○ Automatically obtain IPv4 address ○ Automatically obtain IPv6 address ● Manually set IP address

Server 1:

Server 2:

Server 3:

Minimum Polling Interval: 6 (1m4s)

Maximum Polling Interval: 10 (17m4s)

Server Authentication: ○

NTP Group Key: Upload

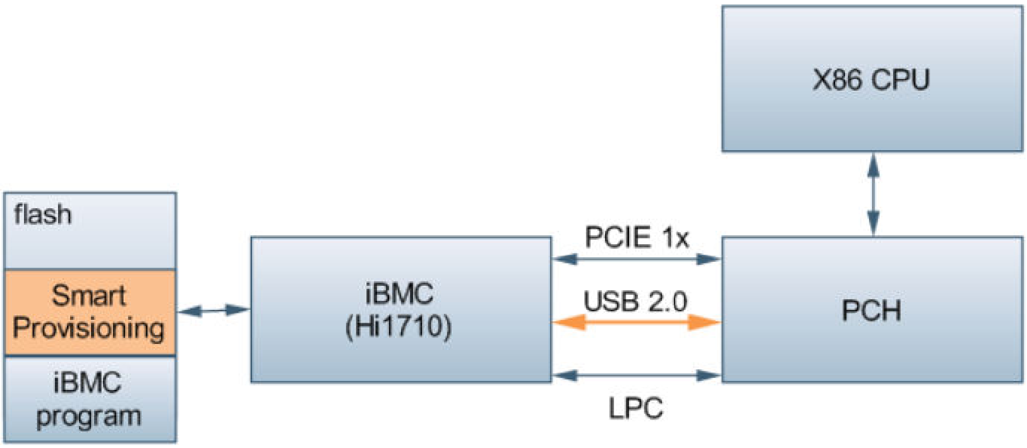
3.15 Smart Provisioning

3.15.1 Overview

Smart Provisioning is a tool software integrated into V5 or later rack servers, compute nodes of blade servers, and server nodes of high-density servers. For V3 servers, users need to use the ServiceCD 2.0 CD delivered with the servers or mount the ServiceCD ISO file using a virtual CD drive to install OS or configure RAID. With Smart Provisioning, users can access the BIOS interface to install the OS, configure RAID controller cards, and upgrade PCIe card firmware after powering on the server. Smart Provisioning simplifies user operations and increases the installation efficiency.

3.15.2 System Design

Figure 3-70 Smart Provisioning in the system (x86)



Smart Provisioning is stored on the flash chip on the mainboard and is connected to the server system through the Hi1710 chip of the iBMC. Smart Provisioning incorporates a Linux OS. Therefore, users can use it even if the OS is not installed. The Smart Provisioning program is stored on an 8 GB NAND flash chip of the server mainboard, which stores the iBMC and Smart Provisioning program and configuration files.

You can access Smart Provisioning in either of the following ways:

- Press the shortcut key during the BIOS startup process.

  This method applies to manual OS installation, RAID configuration, and firmware updates.

- Use the Redfish interface of the iBMC to enable boot from Smart Provisioning.

  This method applies when you use an out-of-band management software to control Smart Provisioning to perform firmware updates.

  When the system boots from Smart Provisioning, the iBMC maps the data in the Smart Provisioning area in the flash memory to a USB drive and connects the USB drive to the system. The OS system starts through the USB device and loads Smart Provisioning to access the graphical interface of Smart Provisioning.

The Redfish interface supports the following functions:

- Firmware updates of the RAID controller cards, NICs, FC cards, and SATA and SAS drives.
- SP upgrades
- Query of PCIe card resources

3.15.3 Firmware Update

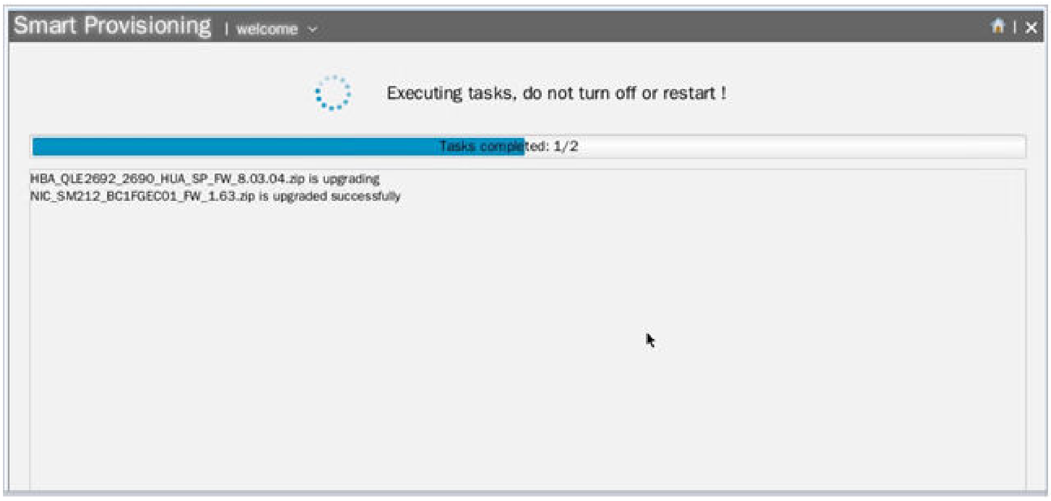
Smart Provisioning supports firmware updates through the iBMC Redfish interface. Management software or other tools can use Smart Provisioning to update firmware of multiple servers in batches. This section uses the uREST tool as an example.

The iBMC provides the Redfish interface to support firmware updates of PCIe cards and hard drives. The uREST tool sends instructions to iBMC. The iBMC downloads the firmware from the specified file server.

After the firmware is downloaded, use the tool to enable boot from Smart Provisioning and reset the server. When the server boots from Smart Provisioning, it automatically checks for new firmware versions. If a firmware update is required, Smart Provisioning performs the firmware update and displays the progress. After the firmware update is complete, Smart Provisioning automatically resets the system.

In this way, the uploading and validation of the PCIe firmware are separated.

Figure 3-71 Firmware upgrade progress



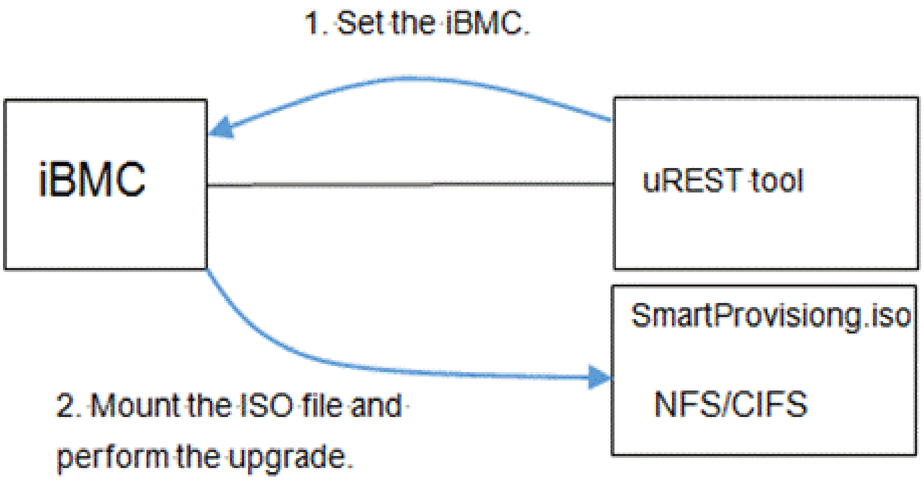
Executing tasks, do not turn off or restart !

Tasks completed: 1/2

```
HBA_QLE2692_2690_HUA_SP_FW_8.03.04.zip is upgrading
NIC_SM212_BC1FGEC01_FW_1.63.zip is upgraded successfully
```

3.15.4 Smart Provisioning Upgrade

Figure 3-72 Upgrading Smart Provisioning using the iBMC



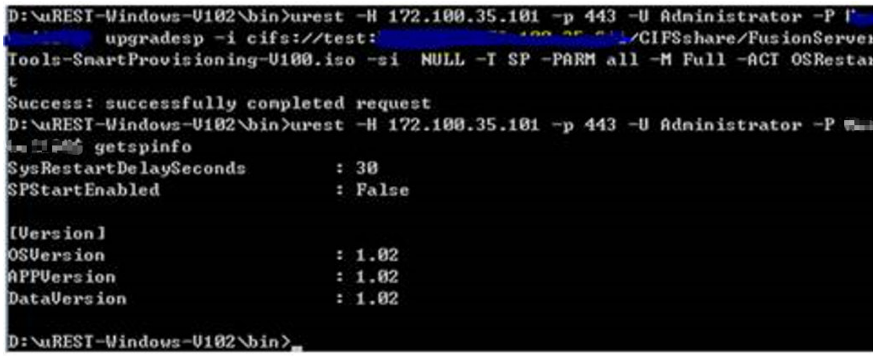
The iBMC provides the Redfish interface to upgrade or restore Smart Provisioning.

During the upgrade, the iBMC uses the NFS/CIFS protocol to mount the Smart Provisioning ISO file. After the file content is verified, the ISO file is copied to the flash memory to perform the upgrade. When Smart Provisioning starts the next time, the upgrade takes effect.

The upgrade does not need to reset the OS. Therefore, services on the OS are not affected. The out-of-band management software can use Smart Provisioning to upgrade servers in batches.

You can run the uREST tool command to perform the upgrade and query the version after the upgrade. For details, see the ***FusionServer Tools 2.3.0 uREST User Guide***.

Figure 3-73 Upgrading Smart Provisioning using the iBMC



```
D:\uREST-Windows-V102\bin>urest -H 172.100.35.101 -p 443 -U Administrator -P [redacted]
 upgradesp -i cifs://test:[redacted]/CIFSshare/FusionServer
Tools-SmartProvisioning-V100.iso -si  NULL -T SP -PARM all -M Full -ACT OSRestar
t
Success: successfully completed request
D:\uREST-Windows-V102\bin>urest -H 172.100.35.101 -p 443 -U Administrator -P [redacted]
 getspinfo
SysRestartDelaySeconds          : 30
SPStartEnabled                  : False

[Version]
OSVersion                       : 1.02
APPVersion                      : 1.02
DataVersion                     : 1.02

D:\uREST-Windows-V102\bin>_
```

3.15.5 PCIe Card Resources Collected

Smart Provisioning provides the iBMC with the PCIe information, which the iBMC cannot obtain. **Table 3-17** lists the PCIe card information collected by Smart Provisioning.

Table 3-17 PCIe card information collected by Smart Provisioning

Resource Name	Description
DeviceName	Silkscreen.
Controlers	Controller information.
Model	Model.
Functions	Function attribute information.
VendorId	Vendor ID.
BDFNumber	BDF information.
BDF	BDF
Description	Description.
MacAddress	MAC address.
DeviceId	Device ID.
SubsystemId	Subsystem ID.
Type	Card type.
SubsystemVendorId	Subsystem vendor ID.
FirmwareVersion	Firmware version.
Manufacturer	Vendor information.
DeviceLocator	Silkscreen information.
Position	Location information.

3.15.6 Erasing Drives

Quick Mode and Secure Mode are supported. Secure Mode provides Simple (erases data on a drive only one round), Normal (erases data on a drive three rounds), and Thorough (erases data on a drive nine rounds) modes.

3.16 iBMA Management

3.16.1 Overview

iBMA 2.0 extends the out-of-band monitoring capability of the server and provides the server component information that the BMC cannot obtain. iBMA 2.0 can detect the following information:

- OS version and kernel version
- x86 hostname and domain name

- NIC, RAID controller card, drive, and PCIe card driver and firmware versions
- NIC model, chip model, driver information, network port link status, MAC address, IP address, VLAN information, bridge information, and binding information
- FC card model, chip model, driver information, port link status, FC_ID, WWNN, and WWPN
- NIC optical module information and fault monitoring

  This function is implemented by the iBMA and the related driver. Only the Intel 82599 and Emulex XE102 NICs and the Linux system are supported.
- NIC OAM information for E9000 blades only
- Detailed information about RAID controller cards, physical drives, and logical drives
- SATADOM/M.2 card information and fault information
- CPU usage, memory usage, drive partition usage, and bandwidth usage of physical ports

3.16.2 Supported Features

Table 3-18 Information provided by the iBMA

Component	Without iBMA	With iBMA
NIC	NIC name, manufacturer, and model, chip manufacturer and model Port names (corresponding to the silkscreen), link status (LOM), and MAC address (LOM)	NIC name, manufacturer, and model, chip manufacturer and model, firmware version, driver name, and version; NIC port names (corresponding to the silkscreen), IPv4 addresses, subnet masks, gateway, IPv6 addresses, VLAN information, link status, and MAC addresses Teaming and bridge information of the network ports, including the logical network port names, IPv4 addresses, subnet mask, gateway and IPv6 addresses, prefix length, gateway, MAC addresses, link status, working mode, and names, MAC addresses, and link status of member ports Link OAM information, including packet loss and error packets on the physical port networks

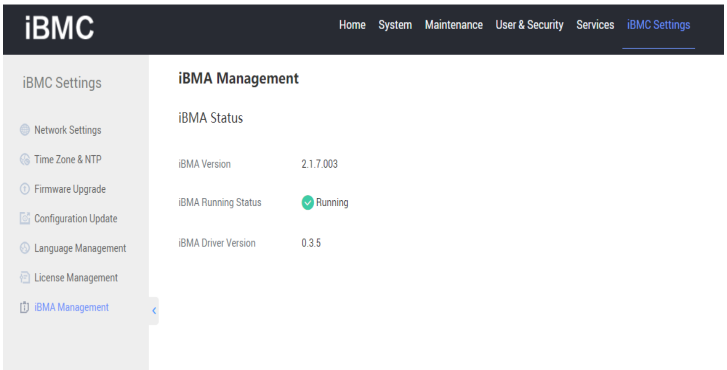
Component	Without iBMA	With iBMA
Optical module	N/A	Information collection: manufacturer, part number, serial number, production date, optical module type (for example, 10GBASE_SR), wavelength, multi-mode/single-mode, temperature, voltage, transmit/ receive power, and current value and threshold of the bias current Fault monitoring: power and voltage threshold-crossing, and rate mismatch between the NIC and optical module
FC card	● FC card name, manufacturer, and model ● Chip manufacturer and model	FC card name, manufacturer, and model, chip model and manufacturer, driver name and version, firmware version, WWNN, WWPN, port type, rate, link status, and FC ID.
SATADOM, M.2 (connected to the PCH)	N/A	Information collection: serial number, capacity, manufacturer, interface type, and temperature Fault monitoring: zero capacity, offline, and remaining service life (only for SATADOM).
System information	N/A	iBMA 2.0 version, iBMA 2.0 driver version, OS version, kernel version, hostname, domain name, computer description, CPU/ memory/drive usage and monitoring, and physical port bandwidth usage and monitoring
Unified upgrade	N/A	Upgrade the iBMA software and PCIe driver. The file transfer speed reaches 4 MB/s.

3.16.3 Onboard iBMA

The iBMA supports the onboard function. On the iBMC WebUI, you can use a USB flash drive to mount the iBMA software into the OS. After the USB drive is mounted to the OS, you can install the iBMA software.

Currently, the V5 series or later servers support onboard iBMA that can be installed on mainstream Linux OSs including CentOS, Red Hat, and Ubuntu.

Figure 3-74 iBMA management page



iBMA Management

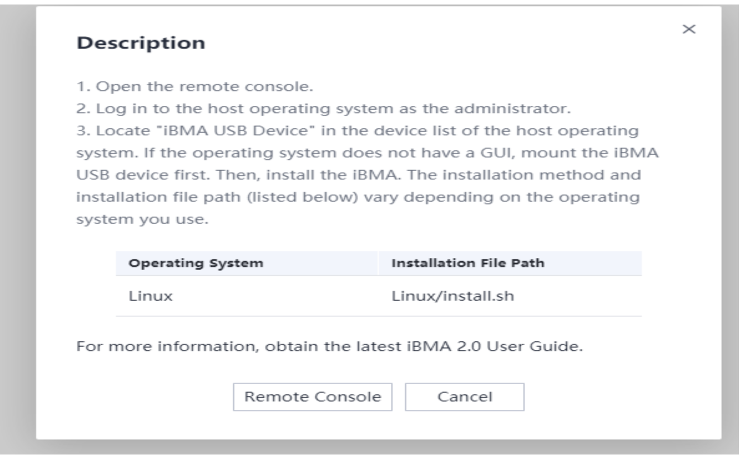
iBMA Status

iBMA Version 2.1.7.003

iBMA Running Status ✓ Running

iBMA Driver Version 0.3.5

Figure 3-75 iBMA operation description



Description

1. Open the remote console.
2. Log in to the host operating system as the administrator.
3. Locate "iBMA USB Device" in the device list of the host operating system. If the operating system does not have a GUI, mount the iBMA USB device first. Then, install the iBMA. The installation method and installation file path (listed below) vary depending on the operating system you use.

Operating System	Installation File Path
Linux	Linux/install.sh

For more information, obtain the latest iBMA 2.0 User Guide.

3.16.4 Upgrade Interface

iBMA 2.0 provides upgrade services for system software through RESTful interfaces and also supports the queries of upgrade progress and upgrade results. The overall upgrade process is as follows:

- After the NMS obtains the upgrade package, NMS sends the following parameters to iBMA 2.0 through the service upgrade interface.

Data types	Definition	Description
Character string	Name	Specifies the software name. Names need to be separated by commas (,). This parameter is supported only by asynchronous upgrade interfaces.
String	ImageURI	URI of the upgrade package.
String	SignalURL	Digital signature address of the upgrade package.
Character string	CrlURI	Address of the public key file of the upgrade package

Data types	Definition	Description
Character string	ImageType	Upgrade package types: Driver, iBMA, Software, or Firmware_Shell.
String	TransferProtocol	Specifies the transmission protocol, such as SFTP.
Character string	User	Indicates the user name for accessing the URL.
Character string	Password	Indicates the password for accessing the URL.
Character string	Parameter	Driver upgrade: all indicates that all packages are to be upgraded. You can also specify upgrade packages. For example, **package1.rpm, package2.rpm** indicates that package 1 and package 2 are to be upgraded. iBMA upgrade: N/A Firmware_Shell upgrade: all indicates that all eight cards are to be upgraded. You can also specify the slots to be upgraded. For example, **1, 2** indicates that the FPGA cards in slots 1 and 2 are to be upgraded. Software upgrade: parameters on which the software package upgrade script depends
Character string	ActiveMethod	The operations include restarting the OS (OSRestart), restarting the server (ServerRestart), making the upgrade package take effect (immediately or null), making the FPGA take effect (WarmReboot), and making the FPGA take effect (ColdReboot).
Character string	DownloadViaiBMC	Specifies whether to use the iBMC for download. This parameter is supported only by asynchronous upgrade interfaces.
Character string	AllowStop	Specifies whether to enable the stopping function. This parameter is supported only by asynchronous upgrade interfaces.

- iBMA 2.0 parses the parameters related to upgrade service commands, obtains the upgrade package, decompresses the package and checks its validity, and invokes upgrade scripts in the upgrade package to perform upgrade operations.

- During the upgrade process, iBMA 2.0 obtains the upgrade progress and results by using upgrade scripts for the NMS to query.
- After the upgrade is complete, iBMA 2.0 enables the upgrade to take effect by using the mode specified in upgrade commands.

The following table lists the iBMA upgrade interfaces.

URI	**Method**	**Overview**	**Supported OS types**
/redfish/v1/Sms/1/UpdateService/Actions/UpdateService. SimpleUpdate	POST	(Not recommended) Delivers upgrade parameters and performing the upgrade.	Linux, Windows, and VMware
/redfish/v1/Sms/1/UpdateService/Progress	GET	(Not recommended) Queries the upgrade progress and result.	Linux, Windows, and VMware
/redfish/v1/Sms/1/UpdateService/Actions/UpdateService.AsynchronousUpdate	POST	Sends upgrade parameters asynchronously and performs upgrade operations.	Linux, Windows, and VMware
/redfish/v1/Sms/1/UpdateService/Actions/UpdateService.EffectiveUpdate	POST	Enables the upgrade to take effect asynchronously.	Linux, Windows, and VMware
/redfish/v1/Sms/1/TaskService/Tasks/*taskid*	GET	Queries the progress of an upgrade or effective task of a specified task ID.	Linux, Windows, and VMware

Currently, iBMA 2.0 supports the following upgrade objects.

Upgrade object	Supported		
	Linux	Windows	VMware
iBMA	Y	Y	Y

NIC driver	Y	Y	Y
RAID controller card driver	Y	Y	Y
FC drive	Y	Y	Y
FCoE driver	Y	Y	Y
iSCSI driver	Y	Y	Y
FPGA firmware	Y	N	N
NVMe driver	Y	Y	Y
InfindBand (IB) driver	Y	N	N
Software	Y	Y	Y

3.17 Kerberos Authentication

Kerberos V5 identity authentication protocol provides an identity authentication mechanism between the client and server. The BMC supports Kerberos-based user name and password authentication and SSO authentication.

Using Kerberos to log in to the iBMC system can improve system security. Kerberos users can log in to the iBMC WebUI.

Based on the Kerberos identity authentication protocol, Kerberos SSO allows you to access all servers on the network by entering the password only once. The iBMC integrates the Kerberos protocol. You only need to enter the password once to log in to the PC (or workstation), and then you can log in to all iBMCs on the network without entering the password.

Kerberos-based SSO provides higher security, because the key is not transmitted over the network during authentication. A key is generated for each session and becomes invalid after the session ends. Kerberos generates a ticket granting ticket (TGT) during authentication. When you log in to a service, the service ID and TGT are automatically sent to the authentication center to obtain a key. The key is used to encrypt the account that logs in to the server. In this way, you do not need to enter the password. It is convenient when you need to frequently switch between multiple servers.

Managing thousands of servers deployed in different areas is always a headache of customers. Kerberos-based SSO authentication solves this problem. The following sections describe how to deploy iBMC to support Kerberos-based SSO.

3.17.1 iBMC SSO Solution Overview

The BMC supports the Kerboros-based SSO authentication. The basic configuration procedure is as follows:

Step 1 Prepare a server or PC, running the Windows Server OS, as the AD domain controller and create a domain.

- In the created domain, create a user and a group, add the user to the group, and obtain the group SID. The SID is required in the iBMC configuration.

- Run the **ktpass** command to generate a **keytab** file. This file is also needed in the iBMC configuration.

Step 2 Prepare a PC or workstation. The workstation must be added to the domain.

- Configure the browser to make it support the Kerberos authentication protocol.
- Configure the server host name at the workstation.

Step 3 Configure iBMC for servers, add the servers to this domain, and configure the iBMC to support the Kerberos authentication protocol.

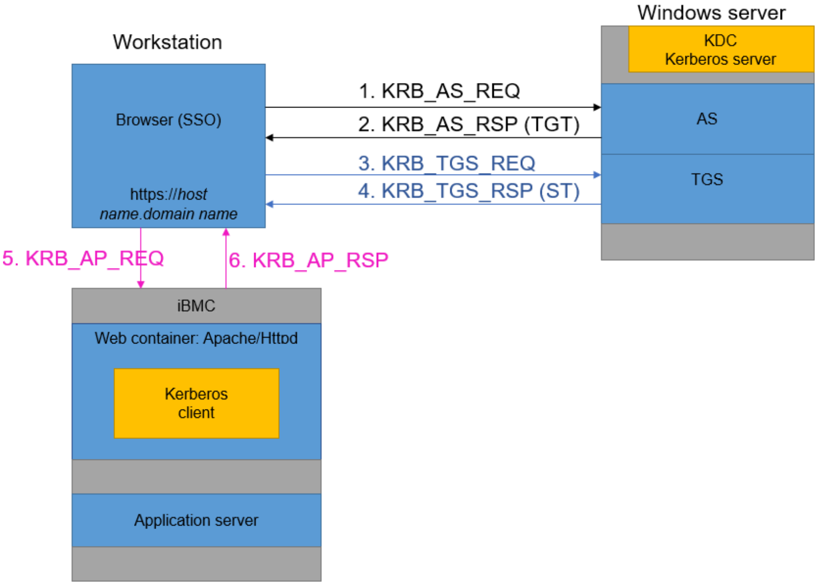
- Add SID to the Kerberos parameter page.
- Add the **keytab** file to the Kerberos parameter page.

Step 4 For details about the configuration, see **3.17.3 System Compatibility**.

----End

After completing the preceding configuration, you can log in to the iBMC WebUI through a browser on the workstation without entering the password. For details, see the following figure.

Figure 3-76 Kerberos-based SSO login



The basic interaction process is as follows:

1. Log in to the workstation as a domain user that has been created on the Windows Server OS. During the login, the workstation (client) sends a **KRB_AS_REQ** request to the Windows Server (KDC) to obtain the ticket granting ticket (TGT). The message carries the client name and pre-authentication information.
2. After the user passes the authentication, the KDC sends the **KRB_AS_RSP** response to the client. The response contains the TGT and session key 1 used for the communication between the client and the KDC.
3. Open the browser on the client and enter **https://ibmc***host name.domain name* in the address box to access the iBMC WebUI. The iBMC detects that the Kerberos client is logged in and returns a special HTTPS message header to the

browser. After receiving the message, the browser sends a **KRB_TGS_REQ** request to the KDC for accessing the service ticket. The request contains the TGT and authenticator.

4. The KDC verifies that the TGT and authenticator are valid, sends a **KRB_TGS_RSP** response to the browser, and returns the service ticket.
5. The browser sends a **KRB_AP_REQ** request carrying the service ticket to the iBMC. After the iBMC authentication is successful, the browser can access the iBMC. The SSO login is successful.
6. The iBMC sends a **KRB_AP_RSP** response to the browser, indicating that the login is successful.

3.17.2 Environment Configuration

The following aspects are involved:

1. Configuring the Windows server
   - Install **Active Directory Domain Server** and complete the configuration. When configuring the AD, use the Windows server as a domain controller, add a new forest, configure the domain name (case-sensitive), and restart the system.
   - Choose **Tools** > **Active Directory User and Computers**, open the directory users and computers, create a user and group in the domain, add the user to the group, and record the SID of the user group.
   - Install the **Active Directory Certificate Services**. Select **Certification Authority Web Enrollment**, configure the CS service, and restart the system.
   - Run the **ktpass** command to generate the **keytab** file.
2. Configuring the Browser on the Workstation

- Choose **Tools** > **Internet options** > **Security** > **Local intranet** > **Sites** > **Advanced**, and add **https://***iBMC host name*.*domain name* to the Websites.
- Choose **Tools** > **Internet options** > **Security** > **Trusted sites** > **Sites**, and add **https://***iBMC_IP* to Websites.

3. iBMC Configuration

- Configure the iBMC host name and add it to the AD domain.
- Create the Kerberos user group. The SID in the user group is the SID created in the preceding step.
- Enable the Kerberos feature and configure Kerberos parameters.
- Upload the **keytab** file and save it.

Perform the preceding steps to configure SSO login.

3.17.3 System Compatibility

- The AD domain controller supports the following operating systems: Windows Server 2012 R2 64-bit and Windows Server 2016 R2 64-bit.
- Operating systems and browsers supported by the workstation

Operating System	Web Browser

Windows 7 32-bit Windows 7 (64-bit)	Internet Explorer 11
	Google Chrome 55+
Windows 8 (32-bit) Windows 8 (64-bit)	Internet Explorer 11
	Google Chrome 55+

3.18 Liquid Cooling Monitoring Management

For liquid-cooled models, the iBMC supports layered liquid cooling monitoring and management, including server liquid cooling monitoring and cabinet liquid cooling monitoring.

3.18.1 Server Liquid Cooling Monitoring

Server liquid cooling monitoring is used for the liquid cooling monitoring and management in the server.

- Supports alarm generation in case of liquid leakage in the liquid-cooling pipes.
- Supports configuration of the power-off strategy in case of liquid leakage.
- Supports presence monitoring of liquid leakage detection components (such as water sensors and leakage detection cards).

3.18.2 Cabinet Liquid Cooling Monitoring

Supports cabinet liquid cooling monitoring when the cabinet is configured with the management module. The cabinet liquid cooling monitoring is used for the liquid cooling monitoring and management in the cabinet.

- Supports alarm generation in case of liquid leakage in the liquid cooling pipes of the cabinet.
- Supports alarm generation in case of liquid leakage in the secondary loop.