



浪潮英信服务器 CMC 用户手册

文档版本 V1.1

发布日期 2021-10-29

版权所有 © 2021 浪潮电子信息产业股份有限公司。保留一切权利。

未经本公司事先书面许可，任何单位和个人不得以任何形式复制、传播本手册的部分或全部内容。

内容声明

您购买的产品、服务或特性等应受浪潮集团商业合同和条款的约束。本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，浪潮集团对本文档的所有内容不做任何明示或默示的声明或保证。文档中的示意图与产品实物可能有差别，请以实物为准。本文档仅作为使用指导，不对使用我们产品之前、期间或之后发生的任何损害负责，包括但不限于利益损失、信息丢失、业务中断、人身伤害，或其他任何间接损失。本文档默认读者对服务器产品有足够的认识，获得了足够的培训，在操作、维护过程中不会造成个人伤害或产品损坏。文档所含内容如有升级或更新，恕不另行通知。

商标说明

Inspur 浪潮、Inspur、浪潮、英信是浪潮集团有限公司的注册商标。
本手册中提及的其他所有商标或注册商标，由各自的所有人拥有。

技术支持

技术服务电话：4008600011

地 址：中国济南市浪潮路 1036 号

浪潮电子信息产业股份有限公司

邮 编：250101

符号约定

在本文中可能出现下列符号，它们所代表的含义如下。

符号	说明
 危险	如不当操作，可能会导致死亡或严重的人身伤害。

符号	说明
 警告	如不当操作，可能会导致人员损伤。
 注意	如不当操作，可能会导致设备损坏或数据丢失。
 提示	为确保设备成功安装或配置，而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。

变更记录

版本	时间	变更内容
V1.0	2021-06-07	首版发布
V1.1	2021-10-29	优化描述

目 录

1	概述	1
1.1	文档用途	1
1.2	目标读者	1
1.3	适用范围	1
2	CMC 管理软件概述	2
2.1	系统简介	2
2.2	软件接口	3
2.2.1	IPMI 2.0	3
2.2.2	Web GUI	9
2.2.3	SNMP	10
2.2.4	Smashclp CLI	10
2.2.5	Redfish	11
2.3	安全管理	11
2.3.1	安全特性	11
2.3.2	总体使用原则	12
2.3.3	安全加固	12
3	CMC Web GUI 介绍	17
3.1	新手入门	17
3.1.1	基本操作	17
3.1.2	用户登录	17
3.2	系统概要	20
3.3	信息	23
3.3.1	刀片模块	23

3.3.2	刀片版本信息.....	25
3.3.3	系统信息.....	26
3.3.4	FRU 信息.....	28
3.3.5	历史曲线.....	30
3.4	远程控制.....	32
3.4.1	服务器定位 UID.....	32
3.5	日志和告警.....	33
3.5.1	系统事件日志.....	33
3.5.2	日志设置.....	35
3.5.3	审计日志.....	37
3.5.4	IDL 日志.....	38
3.5.5	一键收集日志.....	42
3.5.6	当前告警.....	45
3.5.7	SNMP Trap 设置.....	47
3.6	传感器.....	49
3.7	风扇管理.....	51
3.8	CMC 设置.....	53
3.8.1	网络.....	53
3.8.2	用户精细化管理.....	58
3.8.3	服务.....	63
3.8.4	系统防火墙.....	65
3.8.5	日期&时间.....	69
3.8.6	SSL 设置.....	70
3.8.7	BMC IP 设置.....	74

3.8.8	多机箱 CMC IP 设置.....	76
3.8.9	备份配置.....	77
3.8.10	还原配置.....	78
3.9	故障诊断.....	79
3.9.1	模块重启.....	79
3.10	系统维护.....	79
3.10.1	HPM 固件更新.....	79
3.10.2	固件镜像位置.....	95
3.10.3	固件信息.....	96
3.10.4	恢复出厂设置.....	98
4	Smashclp CLI 命令行功能介绍.....	99
4.1	命令行说明.....	99
4.1.1	命令行介绍.....	99
4.1.2	命令行格式说明.....	99
4.1.3	帮助信息.....	99
4.2	登录与退出.....	101
4.2.1	登录 Smashclp CLI.....	101
4.2.2	退出 Smashclp CLI.....	101
4.3	cmclog 命令.....	101
4.3.1	查询与清除 SEL 日志.....	101
4.4	chassis 命令.....	102
4.4.1	查询与控制 UID 灯状态.....	102
4.5	mc 命令.....	103
4.5.1	获取 CMC 系统版本.....	103

4.5.2	服务重启功能.....	104
4.5.3	恢复出厂设置.....	105
4.5.4	双镜像启动配置	106
4.6	diagnose 命令.....	107
4.6.1	列出日志文件属性	107
4.6.2	查看日志文件内容	108
4.6.3	查看最近登录的用户(last).....	109
4.6.4	查看和设置网络设备 (Ifconfig)	109
4.6.5	查看和设置网卡参数 (ethtool)	110
4.6.6	获取 CMC 系统进程(ps)	111
4.6.7	查看系统进程资源占用情况 (top)	112
4.6.8	查看内核缓冲区日志 (dmesg)	114
4.6.9	获取网络相关信息 (netstat)	115
4.6.10	CMC GPIO 设备测试	117
4.6.11	CMC I2C 设备测试	118
4.6.12	CMC PWM 风扇调控	119
4.6.13	CMC IPMI 设备访问	120
4.6.14	获取文件系统磁盘使用情况(df)	122
4.6.15	获取系统运行时间 (uptime)	123
	缩略语	124
A.1	缩略语表.....	124

1 概述

1.1 文档用途

描述了机箱管理控制器（CMC）的功能规范及其详细信息。

1.2 目标读者

本手册主要适用于以下人员：

- 技术支持工程师
- 产品维护工程师
- 服务器管理用户

建议由具备服务器知识的专业工程师参考本手册进行服务器运维操作。



说明

部分用于生产、装备、返厂检测维修的接口、命令，定位故障的高级命令，如使用不当，将可能导致设备异常或者业务中断，故不在本资料中说明。如需要，请向浪潮申请。

1.3 适用范围

本用户手册适用于以下产品：

表 1-1 适用范围

产品型号	两路服务器	四路服务器	AI服务器	多节点服务器
浪潮英信服务器 i24M6	●			●
浪潮英信服务器 i48M6	●			●



说明

因机型不同，Web 界面及个别功能或有差异，请以实际使用机型展示效果为准。

2 CMC 管理软件概述

2.1 系统简介

浪潮机箱管理系统（以下简称 CMC）是实现服务器管理的控制单元，提供丰富的管理功能。

CMC 有如下功能特点：

- 多机框管理功能
- 批量管理刀片功能
- 双 CMC 主备管理功能
- 支持 IPMI2.0, IPMI 接口包括 KCS、LANPLUS、IPMB
- 管理协议：IPMI2.0、HTTPS、SNMP、Smashclp
- Web GUI
- Redfish
- 管理网口接口：Dedicated
- 诊断日志：系统事件日志（SEL）、审计日志、浪潮故障诊断日志（IDL）和一键收集日志
- CMC 硬件看门狗，若 CMC 在 4 分钟内没有响应，风扇将拉高到安全转速以保证服务器散热正常
- 支持 Intel® Intelligent Power Node Manager 4.0
- 事件报警：SNMP Trap (v1/v2c/v3)、邮件报警、系统日志（Syslog）
- 支持 CMC 固件双 Flash
- 固件更新：CMC/BMC/BIOS/CPLD/PSU
- 设备状态监控和诊断
- 支持 IPMITool 工具管理

2.2 软件接口

2.2.1 IPMI 2.0

2.2.1.1 接口通道 ID 分配

表 2-1 接口通道 ID 分配表

通道 ID	接口	用途	支持会话管理
0x00	Primary IPMB	未用	否
0x06	Secondary IPMB	访问ME	否
0x0A	Third IPMB	未用	否
0x01	Primary LAN	专用管理口	是
0x08	Secondary LAN	复用管理口	是
0x0F	KCS/SMS	带内IPMI通信	否

2.2.1.2 LANPLUS 接口

CMC 支持 IPMI 规范 V2.0，兼容 V1.5，支持接收和发送基于 RMCP 或 RMCP+格式的 IPMI 消息。

IPMI 支持的密码套件列表：

表 2-2 IPMI 支持的密码套件

ID	认证算法	完整性算法	加密算法
1	RAKP-HMAC-SHA1	NONE	NONE
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	NONE
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC-MD5	NONE	NONE
7	RAKP-HMAC-MD5	HMAC-MD5-128	NONE
8	RAKP-HMAC-MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC-MD5	MD5-128	NONE
12	RAKP-HMAC-MD5	MD5-128	AES-CBC-128
15	RAKP_HMAC_SHA256	NONE	NONE
16	RAKP_HMAC_SHA256	HMAC-SHA256-128	NONE
17	RAKP_HMAC_SHA256	HMAC-SHA256-128	AES-CBC-128

2.2.1.3 IPMI 命令

下表定义了 CMC 支持的 IPMI 命令。

IPMI Spec 标准命令：

表 2-3 IPMI NetFn

NetFn	App	Chassis	S/E	Storage	Transport	Bridge
Value	0x06	0x00	0x04	0x0A	0x0C	0x0

表 2-4 IPMI Spec 标准命令

IPMI Device "Global" Command	NetFn	CMD	Support
Get Device ID	App	0x01	Yes
Broadcast 'Get Device ID' [1]	App	0x02	Yes
Cold Reset	App	0x03	Yes
Warm Reset	App	0x04	Yes
Get Self Test Results	App	0x05	Yes
Manufacturing Test On	App	0x06	Yes
Set ACPI Power State	App	0x07	Yes
Get ACPI Power State	App	0x08	Yes
Get Device GUID	App	0x09	Yes
Get NetFn Support	App	0x10	Yes
Get Command Support	App	0x0A	Yes
Get Command Sub-function Support	App	0x0B	Yes
Get Configurable Commands	App	0x0C	Yes
Get Configurable Command Sub-functions	App	0x0D	Yes
Set Command Enables	App	0x60	Yes
Get Command Enables	App	0x61	Yes
Set Command Sub-function Enables	App	0x62	Yes
Get Command Sub-function Enables	App	0x63	Yes
Get OEM NetFn IANA Support	App	0x64	Yes
BMC Watchdog Timer Commands	NetFn	CMD	Support
Reset Watchdog Timer	App	0x22	Yes
Set Watchdog Timer	App	0x24	Yes
Get Watchdog Timer	App	0x25	Yes
BMC Device and Messaging Commands	NetFn	CMD	Support
Set BMC Global Enables	App	0x2E	Yes
Get BMC Global Enables	App	0x2F	Yes
Clear Message Flags	App	0x30	Yes
Get Message Flags	App	0x31	Yes

Enable Message Channel Receive	App	0x32	Yes
Get Message	App	0x33	Yes
Send Message	App	0x34	Yes
Read Event Message Buffer	App	0x35	Yes
Get BT Interface Capabilities	App	0x36	Yes
Get System GUID	App	0x37	Yes
Set System Info Parameters	App	0x58	Yes
Get System Info Parameters	App	0x59	Yes
Get Channel Authentication Capabilities	App	0x38	Yes
Get Session Challenge	App	0x39	Yes
Activate Session	App	0x3A	Yes
Set Session Privilege Level	App	0x3B	Yes
Close Session	App	0x3C	Yes
Get Session Info	App	0x3D	Yes
Get AuthCode	App	0x3F	Yes
Set Channel Access	App	0x40	Yes
Get Channel Access	App	0x41	Yes
Get Channel Info Command	App	0x42	Yes
Set User Access Command	App	0x43	Yes
Get User Access Command	App	0x44	Yes
Set User Name	App	0x45	Yes
Get User Name Command	App	0x46	Yes
Set User Password Command	App	0x47	Yes
Activate Payload	App	0x48	Yes
Deactivate Payload	App	0x49	Yes
Get Payload Activation Status	App	0x4A	Yes
Get Payload Instance Info	App	0x4B	Yes
Set User Payload Access	App	0x4C	Yes
Get User Payload Access	App	0x4D	Yes
Get Channel Payload Support	App	0x4E	Yes
Get Channel Payload Version	App	0x4F	Yes
Get Channel OEM Payload Info	App	0x50	Yes
Master Write-Read	App	0x52	Yes
Get Channel Cipher Suites	App	0x54	Yes
Suspend/Resume Payload Encryption	App	0x55	Yes
Set Channel Security Keys	App	0x56	Yes
Get System Interface Capabilities	App	0x57	Yes
Firmware Firewall Configuration	App	0x60-0x64	NO
Chassis Device Commands	NetFn	CMD	Support
Get Chassis Capabilities	Chassis	0x00	Yes
Get Chassis Status	Chassis	0x01	Yes
Chassis Control	Chassis	0x02	Yes
Chassis Reset	Chassis	0x03	Yes

Chassis Identify	Chassis	0x04	Yes
Set Front Panel Button Enables	Chassis	0x0A	Yes
Set Chassis Capabilities	Chassis	0x05	Yes
Set Power Restore Policy	Chassis	0x06	Yes
Set Power Cycle Interval	Chassis	0x0B	Yes
Get System Restart Cause	Chassis	0x07	Yes
Set System Boot Options	Chassis	0x08	Yes
Get System Boot Options	Chassis	0x09	Yes
Get POH Counter	Chassis	0x0F	Yes
Event Commands	NetFn	CMD	Support
Set Event Receiver	S/E	0x00	Yes
Get Event Receiver	S/E	0x01	Yes
Platform Event (a.k.a. "Event Message")	S/E	0x02	Yes
PEF and Alerting Commands	NetFn	CMD	Support
Get PEF Capabilities	S/E	0x10	Yes
Arm PEF Postpone Timer	S/E	0x11	Yes
Set PEF Configuration Parameters	S/E	0x12	Yes
Get PEF Configuration Parameters	S/E	0x13	Yes
Set Last Processed Event ID	S/E	0x14	Yes
Get Last Processed Event ID	S/E	0x15	Yes
Alert Immediate	S/E	0x16	Yes
PET Acknowledge	S/E	0x17	Yes
Sensor Device Commands	NetFn	CMD	Support
Get Device SDR Info	S/E	0x20	Yes
Get Device SDR	S/E	0x21	Yes
Reserve Device SDR Repository	S/E	0x22	Yes
Get Sensor Reading Factors	S/E	0x23	Yes
Set Sensor Hysteresis	S/E	0x24	Yes
Get Sensor Hysteresis	S/E	0x25	Yes
Set Sensor Threshold	S/E	0x26	Yes
Get Sensor Threshold	S/E	0x27	Yes
Set Sensor Event Enable	S/E	0x28	Yes
Get Sensor Event Enable	S/E	0x29	Yes
Re-arm Sensor Events	S/E	0x2A	Yes
Get Sensor Event Status	S/E	0x2B	Yes
Get Sensor Reading	S/E	0x2D	Yes
Set Sensor Type	S/E	0x2E	Yes
Get Sensor Type	S/E	0x2F	Yes
Set Sensor Reading And Event Status	S/E	0x30	Yes
FRU Device Commands	NetFn	CMD	Support
Get FRU Inventory Area Info	Storage	0x10	Yes
Read FRU Data	Storage	0x11	Yes
Write FRU Data	Storage	0x12	Yes

SDR Device Commands	NetFn	CMD	Support
Get SDR Repository Info	Storage	0x20	Yes
Get SDR Repository Allocation Info	Storage	0x21	Yes
Reserve SDR Repository	Storage	0x22	Yes
Get SDR	Storage	0x23	Yes
Add SDR	Storage	0x24	Yes
Partial Add SDR	Storage	0x25	Yes
Delete SDR	Storage	0x26	Yes
Clear SDR Repository	Storage	0x27	Yes
Get SDR Repository Time	Storage	0x28	Yes
Set SDR Repository Time	Storage	0x29	Yes
Enter SDR Repository Update Mode	Storage	0x2A	Yes
Exit SDR Repository Update Mode	Storage	0x2B	Yes
Run Initialization Agent	Storage	0x2C	Yes
SEL Device Commands	NetFn	CMD	Support
Get SEL Info	Storage	0x40	Yes
Get SEL Allocation Info	Storage	0x41	Yes
Reserve SEL	Storage	0x42	Yes
Get SEL Entry	Storage	0x43	Yes
Add SEL Entry	Storage	0x44	Yes
Partial Add SEL Entry	Storage	0x45	Yes
Delete SEL Entry	Storage	0x46	Yes
Clear SEL	Storage	0x47	Yes
Get SEL Time	Storage	0x48	Yes
Set SEL Time	Storage	0x49	Yes
Get Auxiliary Log Status	Storage	0x5A	Yes
Set Auxiliary Log Status	Storage	0x5B	Yes
Get SEL Time UTC Offset	Storage	0x5C	Yes
Set SEL Time UTC Offset	Storage	0x5D	Yes
LAN Device Commands	NetFn	CMD	Support
Set LAN Configuration Parameters	Transport	0x01	Yes
Get LAN Configuration Parameters	Transport	0x02	Yes
Suspend BMC ARPs	Transport	0x03	Yes
Get IP/UDP/RMCP Statistics	Transport	0x04	NO
Serial/Modem Device Commands	NetFn	CMD	Support
Set Serial/Modem Configuration	Transport	0x10	Yes
Get Serial/Modem Configuration	Transport	0x11	Yes
Set Serial/Modem Mux	Transport	0x12	Yes
Get TAP Response Codes	Transport	0x13	NO
Set PPP UDP Proxy Transmit Data	Transport	0x14	NO
Get PPP UDP Proxy Transmit Data	Transport	0x15	NO
Send PPP UDP Proxy Packet	Transport	0x16	NO
Get PPP UDP Proxy Receive Data	Transport	0x17	NO

Serial/Modem Connection Active	Transport	0x18	NO
Callback	Transport	0x19	Yes
Set User Callback Options	Transport	0x1A	Yes
Get User Callback Options	Transport	0x1B	Yes
Set Serial Routing Mux	Transport	0x1C	NO
SOL Activating	Transport	0x20	NO
Set SOL Configuration Parameters	Transport	0x21	Yes
Get SOL Configuration Parameters	Transport	0x22	Yes
Command Forwarding Commands	NetFn	CMD	Support
Forwarded Command	Bridge	0x30	NO
Set Forwarded Commands	Bridge	0x31	NO
Get Forwarded Commands	Bridge	0x32	NO
Enable Forwarded Commands	Bridge	0x33	NO
Bridge Management Commands (ICMB)	NetFn	CMD	Support
Get Bridge State	Bridge	0x00	NO
Set Bridge State	Bridge	0x01	NO
Get ICMB Address	Bridge	0x02	NO
Set ICMB Address	Bridge	0x03	NO
Set Bridge ProxyAddress	Bridge	0x04	NO
Get Bridge Statistics	Bridge	0x05	NO
Get ICMB Capabilities	Bridge	0x06	NO
Clear Bridge Statistics	Bridge	0x08	NO
Get Bridge Proxy Address	Bridge	0x09	NO
Get ICMB Connector Info	Bridge	0x0A	NO
Get ICMB Connection ID	Bridge	0x0B	NO
Send ICMB Connection ID	Bridge	0x0C	NO
Discovery Commands (ICMB)	NetFn	CMD	Support
PrepareForDiscovery	Bridge	0x10	NO
GetAddresses	Bridge	0x11	NO
SetDiscovered	Bridge	0x12	NO
GetChassisDeviceId	Bridge	0x13	NO
SetChassisDeviceId	Bridge	0x14	NO
Bridging Commands (ICMB)	NetFn	CMD	Support
BridgeRequest	Bridge	0x20	NO
BridgeMessage	Bridge	0x21	NO
Event Commands (ICMB)	NetFn	CMD	Support
GetEventCount	Bridge	0x30	NO
SetEventDestination	Bridge	0x31	NO
SetEventReceptionState	Bridge	0x32	NO
SendICMBEventMessage	Bridge	0x33	NO
GetEventDestination (optional)	Bridge	0x34	NO
GetEventReceptionState (optional)	Bridge	0x35	NO

2.2.1.4 IPMI CMD Tool

通常 IPMITool 被用来发送 IPMI 命令，可以用于远程机发送 LANPLUS 接口的 IPMI 带外命令。IPMITool 有 Windows 版本和 Linux 版本。具体命令的使用方法请参考 IPMI 官方文档。

支持的接口：

- Open, Linux OpenIPMI 接口[缺省]
- LANPLUS, IPMI2.0 RMCP+ LAN 接口

图 2-1 IPMITool CMD

```
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
dcmi      Data Center Management Interface
nm        Node Manager Interface
sunoem    OEM Commands for Sun servers
kontron    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
ime       Update Intel Manageability Engine Firmware
vita      Run a VITA 46.11 extended cmd
```

2.2.2 Web GUI

支持 HTTPS (端口 443) 访问 Web GUI，HTTP 默认禁用。Web GUI 提供管理界面，用户可查看系统信息、系统事件和状态，并控制被管理的服务器。

表 2-5 支持的 OS 及浏览器

客户端 OS	浏览器版本
Windows 7.1 x64 Windows 8 x64 Windows 10 x64 Ubuntu 14.04.03 LTS x64	Windows 客户端： Edge、Firefox 43+、Chrome 47+、IE 11+ Linux客户端： Firefox 43+、Chrome 47+

关于 Web GUI 的更多说明，请参见“[第 3 章节 CMC Web GUI 介绍](#)”。

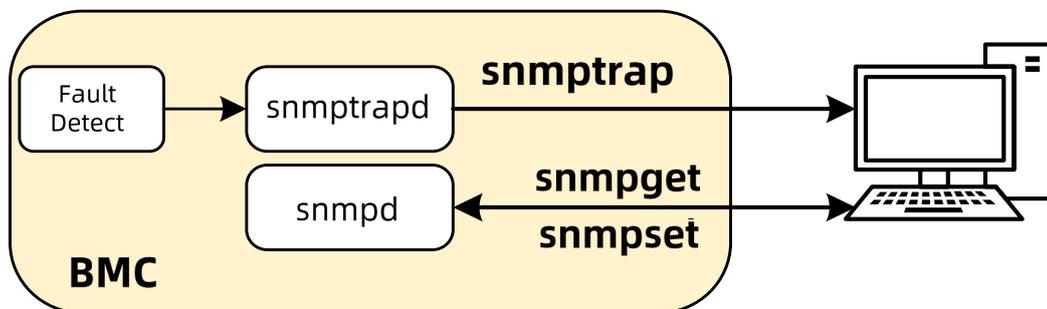
2.2.3 SNMP

SNMP 是基于 TCP/IP 协议族的网络管理标准，是一种在 IP 网络中管理网络节点（如服务器、工作站、路由器、交换机等）的标准协议。网络管理员还可以通过 SNMP 接收网络节点的通知消息以及告警事件报告等来获取网络出现的问题。

在 CMC 中，远端代理可以通过 SNMP 访问 CMC 获取网络信息、用户信息、温度、电压、扇速度等服务器信息，同时可以通过 SNMP 进行 CMC 参数配置、管理服务器。

- 支持 SNMP Get/Set/Trap。
- 支持 V1/V2C/V3 版本。
- SNMPv3 支持认证算法 MD5 或者 SHA，加密算法为 DES 或 AES。
- SNMP 支持查询系统健康状况、传感器状态、硬件状态、设备资产信息等。
- SNMP Set 支持大部分 CMC 参数设置。
- SNMP Trap，CMC 将告警信息通过 Trap 消息发送到远端 Trap 接收。

图 2-2 SNMP 原理图



2.2.4 Smashclp CLI

Smashclp CLI 是一个命令行工具，您可以通过 CLI 下的命令实现对 CMC 的部分操作。

关于 Smashclp CLI 的详细信息，请参见“[第 4 章节 Smashclp CLI 命令行功能介绍](#)”。关于 Smashclp 的字面意义，请参见“[第 5 章节 术语和缩略语](#)”。

2.2.5 Redfish

Redfish 是一种新的管理标准，它使用超媒体 RESTful 接口来表示数据。它面向模型，能够表达现代系统构件与服务、构件语义之间的关系，易于扩展。对于提供 Redfish 的服务器，客户端可以通过发送 HTTPS 请求来获取 CMC 信息，并指定 CMC 的操作。客户端可以通过 HTTPS 客户端访问 Redfish 服务。通常的请求操作是“GET”、“PUT”、“POST”、“PATCH”、“DELETE”。发送和接收数据都是 json 格式。

CMC Redfish 具体操作请参考文档《浪潮英信服务器 Redfish 用户手册》，如您需要使用此文档请联系浪潮技术服务人员获取。

2.3 安全管理

2.3.1 安全特性

- 多机箱管理密码

多机箱管理功能需要所有机箱的 admin 用户密码保持一致，这存在一定的风险性，密码泄漏会影响所有机器，提醒多机箱管理人员使用时及时修改默认密码，定期进行密码更新，保护好密码以防泄露。

- 用户账号安全管理

CMC 账号安全包括密码长度及复杂度、密码有效期、禁用历史密码重复次数和登录失败锁定等功能，还包含修改口令时验证旧口令、首次登录时提示修改默认口令等措施保证账号安全。

- 安全协议及安全端口防攻击

CMC 按照最小化原则对外开放网络服务端口，关闭不使用的服务；默认使用安全协议，默认关闭不安全协议的端口。

- 基于角色的权限管理

CMC 支持多种类型的用户，包括 IPMI、Web、SSH 和 SNMP 用户，各类用户按照不同角色分配不同权限，实现用户的权限分立，且仅授予所需的最小访问权限。

- 安全更新及安全启动

CMC 镜像文件采用安全长度的密钥加密算法进行数字签名，在更新及启动时对镜像文件的数字签名进行校验，校验通过才允许固件更新及启动，防止镜像被恶意篡改。同时提供防错刷机制，防止不同厂商、不同产品型号、不同固件类型的镜像文件之间互相刷新。

- 镜像安全备份

CMC 支持双 Flash，每个 Flash 上存储一份镜像文件，支持双镜像升级，确保镜像文件的可用性。

- 基于场景的登录限制

基于安全考虑，从 IP 地址、端口、时间段、MAC 等多个维度将服务器管理接口访问控制在最小范围。用户可根据使用场景，创建白名单访问控制规则，防止非法访问。

- 日志管理

CMC 记录所有接口的非查询操作，记录内容应包括事件发生时间、操作接口、操作源 IP、操作源用户、执行动作等。支持通过 Web 导出日志，支持日志循环记录及 Syslog 外发，防止日志空间记录满时造成日志丢失。故障诊断日志 IDL 是浪潮 CMC 独有的日志类型，用于记录 CMC 设备上基于 IPMI 传感器的事件历史记录，每条日志都有相应的处理建议，能更有效的帮助用户进行日志诊断和分析。

- 数据加密存储及传输

CMC 中的敏感数据在日志、文件或 cookie 中使用安全算法进行加密存储，默认使用 HTTPS 进行通信，LDAP、AD、Radius 及 Syslog 等均支持 OVER SSL，以保证数据传输的安全性。

- 证书管理

CMC 支持 SSL 证书生成及证书替换功能，为提高安全性，建议替换成自己的证书和公私钥对，并及时更新证书，保证证书的有效性。CMC 还支持 LDAP 证书的导入功能，为数据传输提供鉴权加密功能，提高系统安全性。

2.3.2 总体使用原则

- 使用业务网络外的内部专用网络对 CMC 进行管理及配置。
- 关闭不使用的服务端口，使用安全的协议进行通信。
- 定期审计 CMC 操作日志，更新固件安全补丁。

2.3.3 安全加固

2.3.3.1 默认用户/密码

为了方便用户首次操作，[表 2-6](#) 描述了 CMC 系统默认口令。

表 2-6 默认用户/密码

默认用户/密码	M6平台的默认值	备注
CMC默认用户名/ 密码	用户名：admin 密码：admin	用户admin拥有最高权限，属于角色 administrator。

默认用户/密码	M6平台的默认值	备注
		默认密码修改，请遵循密码复杂度要求。
Uboot密码	inspur@u600t	U-Boot命令主要用于加载底层软件、调试底层设备，属于调试命令，如需更改密码，请参考《浪潮英信服务器CMC配置手册》。
CMC串口用户/密码	用户名：sysadmin 密码：superuser	仅限CMC调测串口登陆，进行CMC调试和维护。



说明

为保证系统的安全性，建议您在首次操作时修改默认值。

2.3.3.2 用户管理

CMC 采用基于角色的本地用户精细化管理。系统权限类型被划分为用户配置、常规配置、电源控制、安全配置、调试诊断、查询功能、配置自身这九种类型。默认支持“管理员”、“操作员”、“普通用户”角色，不允许配置修改其权限。另外还支持最大 4 个自定义角色组 OEM1、OEM2、OEM3、OEM4，系统管理员可灵活地根据业务维护需求将这九类权限配置给一个自定义角色。

建议系统管理员创建审计角色和维护角色，其中审计角色拥有安全配置和查询功能权限；维护角色拥有调试诊断和查询功能。建议创建审计员，拥有审计角色；创建维护员，拥有维护角色。用户创建、分配角色及权限设置方法请参见“[3.8.2 用户精细化管理](#)”。

2.3.3.3 认证管理

CMC 支持本地认证和第三方远程认证两种认证模式。第三方远程认证支持 LDAP、AD、Radius。

本地认证方式适合小型组网环境，如中小型企业。本地认证支持用户名密码认证，另外本地自动化采用 SSH 方式登录 CMC 命令行，建议采用公钥认证。

LDAP 等第三方远程认证方式，由于其数量和权限均在服务端设置，不受 16 个本地用户限制，因此适用于具有大量用户的环境。使用域控制器中的用户域、组域、隶属于用户域的 LDAP 用户名及其密码登录 CMC 系统，可以提高系统安全性。LDAP 用户可登录 CMC Web 界面，也可通过 SSH 方式登录 CMC 命令行和 Redfish 接口访问 CMC 系统。为了保护用户认证鉴权数据的传输安全和防止 LDAP 服务端被仿冒，建议配置 LDAP over SSL，并启用“远端域控制器证书验证”。

2.3.3.4 服务管理

CMC 服务按照最小化原则对外开放网络服务端口，即调试使用的网络服务端口在正式使用的时候必须关闭，不安全协议的端口默认关闭，不使用的网络服务必须关闭。服务及端口如下：

表 2-7 服务及端口

服务	非安全端口	安全端口
Web	TCP/80	TCP/443
SSH	NA	TCP/22
Solssh	NA	NA
smux	SNMP Multiplexer	启用
srvloc	Sever Location	启用
DHCP V6 Client	DHCP V6 Client	启用
IPMI	IPMI	启用

基于最小化原则，不安全协议的端口默认关闭，CMC 目前支持非安全端口服务包括 Web、SSH 以及 Solssh，建议关闭非安全端口。

基于最小化原则，不使用的服务建议关闭。必须使用这些服务时，建议开启安全配置，包括会话超时和会话限制。目前 Web、SSH、Solssh 等支持会话超时配置，会话超时可根据不同应用场景设置不同值，建议会话超时设置不超过 300 秒。

可在“CMC 设置>服务”进行设置，设置方法请参见“[3.8.3 服务](#)”章节。

2.3.3.5 密码策略

CMC 密码策略包括：密码复杂度、密码有效期、历史密码记录和登录失败锁定。为了防止密码猜测和暴力破解，密码复杂度建议设置密码长度至少 8 位以上，字符类型包含 3 种及以上；本地用户建议开启密码有效期和历史密码记录检查；建议开启密码登录失败锁定配置。

可在“CMC 设置>用户精细化管理”进行设置，设置方法请参见“[3.8.2 用户精细化管理](#)”。

2.3.3.6 访问控制

CMC 访问控制主要通过系统防火墙，包括一般防火墙、IP 地址防火墙、端口防火墙和 MAC 防火墙，从而减少攻击来源。基于安全考虑从时间、地点(IP/端口/MAC)、行为三个维度将服务器管理接口访问控制在最小范围，建议用户根据需要设置登录规则的白名单。

可在“CMC 设置>系统防火墙”进行设置，设置方法请参见“[3.8.4 系统防火墙](#)”。

2.3.3.7 加密认证

- LDAP

CMC 支持 LDAP 证书的导入功能，为提高系统安全性，建议启用 LDAP/E-Directory 认证，选择 SSL 或 StartTLS 加密类型，从而为数据传输提供鉴权加密功能。

- SSL

证书管理是指对 SSL 证书的各种管理操作。SSL 证书默认使用自签名 SSL 证书，证书的签名算法为 SHA-256、RSA-2048。从安全考虑，建议客户在首次使用时导入自己的证书来替换系统中默认的自定义证书，从而以安全的模式访问 CMC。具体设置方法可参见“[3.8.6 SSL 设置](#)”。

- Syslog over SSL

Syslog 系统日志支持传输过程中的加密功能，为了保证数据传输的安全性，建议 Syslog 配置使用 TLS 传输协议，具体配置请参见“[3.5.2 日志设置](#)”。

- SNMP

CMC 支持 SNMP set/get，建议配置 SNMP V3，认证算法 SHA，保密算法为 AES。CMC 支持 SNMP Trap，用户打开 Trap 接收器，在 CMC Web GUI 中设置 Trap 目标 IP，当 CMC 检测到事件发生时，CMC 将自动发送事件给 Trap 接收器，具体设置方法可参见“[3.5.7 SNMP Trap 设置](#)”。

- SSH

CMC 支持 Smash-Lite CLI，用户可以通过 SSH 登录 CMC 并进入 Smash-Lite CLI。使用 SSH 登录到 CMC 的命令行。登录后，即可进入命令行操作界面。

2.3.3.8 系统擦除

当服务器设备需要报废，或者设备需要回收再利用时，为了保证数据安全及个人隐私，需要进行系统擦除操作，主要有以下场景：

- 恢复出厂设置

CMC 支持在 Web 管理界面中恢复出厂设置。具体为：登录 Web 页面，进入“系统维护>恢复出厂设置”进行恢复出厂设置。

- 日志清除

系统事件日志清除：登录到 Web 管理界面，进入“日志和告警>系统事件日志”页面，点击“清除事件日志”选项后，将删除所有现有的传感器日志记录。

IDL 日志清除：进入“日志和告警>IDL 日志”页面，点击“清除 IDL 日志”选项后，将清除该 CMC 上所有 IDL 日志信息。

告警日志清除：当系统日志中产生告警信息时，会添加告警日志，在“日志和告警>当前告警”页面显示系统中未解除的告警信息，当故障解除时告警日志会自动清除。

- 屏幕截图清除

登录 Web 管理界面，进入“故障诊断>屏幕截图”页面，此页面显示已有的屏幕截图，点击“删除截图”选项后会清除截图文件。

2.3.3.9 系统恢复

- 自动恢复

看门狗机制：CMC 支持自身代码执行异常情况下的自动恢复功能，当出现 CMC 内核崩溃、资源耗尽、无法刷写等异常情况时，通过硬件看门狗的超时重置机制，可使 CMC 自动恢复到正常状态。另外，CMC 通过软件看门狗定期检测内部服务的工作状态，出现异常时会自动重启 IPMI 服务，使进程自动恢复正常。

双镜像机制：CMC 支持双 Flash，每个 Flash 存储一份镜像文件，当其中一个镜像损坏后可以自动切换到另外一个 Flash，从而确保镜像文件的可用性。

- 手动恢复

CMC 支持对现有系统的各项配置进行还原，还原配置时手动选择已备份好的配置文件。具体为：登录到 CMC Web 管理界面，进入“CMC 设置>还原配置”页面，选择待恢复的配置文件后进行还原配置操作，配置操作可参见“[3.8.10 还原配置](#)”。

CMC 支持固件刷新失败后的回滚功能，当固件更新失败时，通过备份区的镜像文件进行回滚操作，确保固件的可用性。

此外，在出现异常情况时，用户可以通过 Web 或 IPMI 命令进行 CMC 任务重启，恢复 CMC，具体操作方法参见“[3.9.1 模块重启](#)”。

2.3.3.10 日志审计

使用 SNMP Trap 功能将 CMC 告警信息发送到远端 Trap 接收端时，为了传输安全，建议 Trap 接收端使用 SNMP V3 版本协议，配置认证协议选择“SHA”，加密协议使用“AES”，且认证密码、加密密码遵循密码复杂度要求，SNMP Trap CMC 发送端根据接收端各参数进行相应设置，配置方法请参见“[3.5.7 SNMP Trap 设置](#)”。

由于 CMC 本地存储空间有限，为保证日志信息正常记录，建议将事件日志设置为循环策略（默认即为循环策略），同时使用 Syslog 功能将 CMC 的事件日志及审计日志发送到远端 Syslog 服务器进行保存，目的是为了传输安全，建议 Syslog 配置使用 TLS 传输协议。

2.3.3.11 其他

公司针对内部发现或外部爆出的产品安全漏洞，会不定期发布安全公告及升级补丁包（具体可见公司官网 <https://www.inspur.com> 安全通告模块）。请您根据自身实际使用场景评估风险后，按需升级 CMC 固件版本。

3 CMC Web GUI 介绍

3.1 新手入门

3.1.1 基本操作

Web GUI 通过可视化、友好的界面来帮助用户完成服务器管理，Web GUI 配有联机帮助。

CMC Web GUI 可执行的基本操作如表 3-1 所示。

表 3-1 基本操作

操作	说明
切换界面语言	在登录界面或其他界面中，从下拉列表中切换语言。支持中文和英文。
查看刀片模块信息	选择“首页>信息  >刀片模块”。 “刀片模块”界面刀片信息，包括刀片在位、开关机状态、UID 状态、BMC IP 等信息。
查看联机帮助	在 CMC Web GUI 页面中，点击  查看帮助信息。
刷新页面	在 CMC Web GUI 页面中，点击  刷新当前页面。
查看和注销当前用户	在 CMC Web GUI 页面中，点击  显示当前登录用户的用户名，点击右侧下拉箭头可查看该用户及其权限组以及注销当前用户。

3.1.2 用户登录

功能描述

通过使用“用户登录”界面的功能，您可以登录 CMC Web GUI。

- 通过 Web GUI 进行界面操作，最多只能有 20 个用户同时登录。
- 默认情况下，系统超时时间为 3 分钟，即在 3 分钟内，如果您未在 Web GUI 上执行任何操作，系统将自动登出，此时需输入用户名和密码重新登录 Web GUI。
- 连续输入错误密码的次数达到设定的失败次数后，系统将对此用户进行锁定。锁定时间达到用户设置的锁定时长后，该用户方可正常登录。

- 为保证系统的安全性，初次登录时，请及时修改初始密码，并定期更新。

参数说明

表 3-2 用户登录

参数	描述
用户名	登录CMC系统的用户名。
密码	登录用户的密码。
语言	Web GUI界面的语言。

操作步骤

本文档以 Chrome 浏览器为例介绍 CMC Web GUI 的操作步骤。

1. 在浏览器地址栏输入 `https://CMC_IP`，并按“Enter”，打开如下图 3-1 所示界面。

图 3-1 用户登录



说明

端口号是可修改的（请参阅 [3.8.3 服务](#) 章节），HTTP 端口号是 80（默认禁用），HTTPS 端口号是 443。如果修改了端口号，则需要在登录时指定端口号，例如

https://CMC_IP:sslport。

2. 输入登录 CMC 的用户名称和密码。
3. 选择 Web GUI 界面语言。
4. 点击“登录”。
5. 登录成功后，显示“系统概要”界面。

说明

1. 输入 IPv6 地址时，必须使用[]将其括起来，而 IPv4 地址无此限制。例如：
 - IPv4 地址：“100.3.8.100”
 - IPv6 地址：“[fc00::64]”
 2. 第一次登陆 CMC Web GUI，网页会弹出安全提醒，请点击“高级”，然后选择“继续前往”，继续登录，出现登录界面后输入用户名密码，点击“登录”即可登录。
-

图 3-2 安全提醒

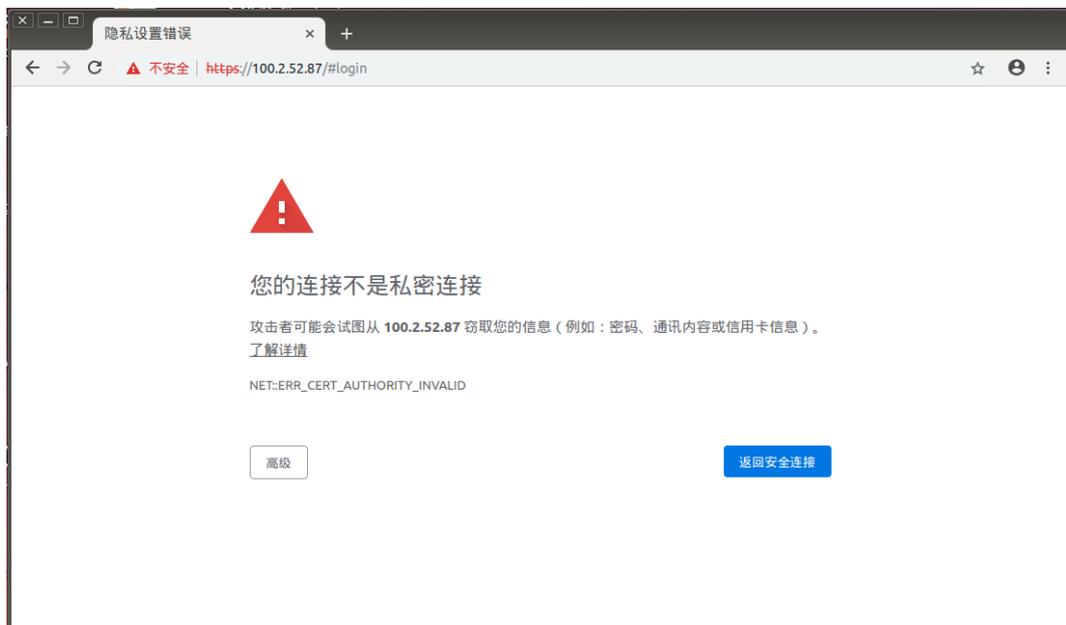
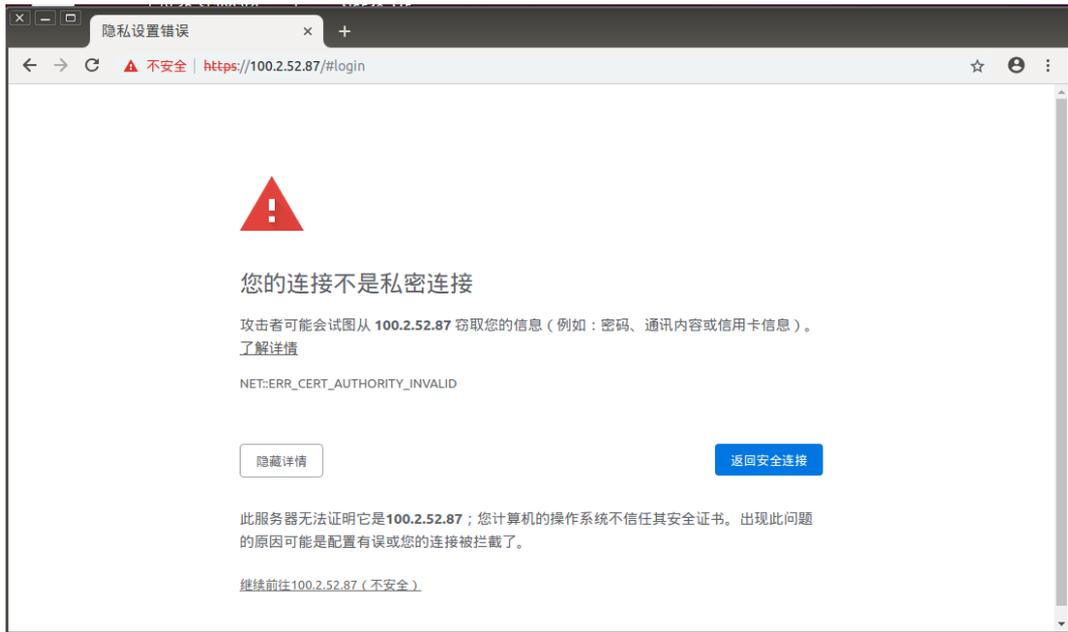


图 3-3 安全提醒_继续前往



3.2 系统概要

功能描述

“系统概要”界面提供了：

- 服务器信息
- 服务器运行状况信息
- 固件版本信息
- 在线用户信息
- 快速启动任务
- 近期事件日志列表

界面展示

登录 Web GUI 后，即为系统概要页面，在导航栏中选择“系统概要”也可以进入系统概要页面，如下图 3-4 所示。

图 3-4 系统概要



参数说明

表 3-3 系统概要

区域	展示的信息
服务器信息	<p>提供服务器的基本信息，包括：</p> <ul style="list-style-type: none"> ● 产品类型：服务器的产品类型。 ● 产品名称：服务器的产品名称。 ● 制造商：服务器的制造商。 ● 产品序号：服务器的产品序号。 ● 资产编号：服务器的资产编号。 ● System UUID：服务器的 System UUID 信息。 ● Device UUID：服务器的 Device UUID 信息。

区域	展示的信息
	<ul style="list-style-type: none"> ● 专用管理口 0：服务器的专用管理口 IP 地址。
服务器运行状况	<p>提供服务器的运行状况，包括：</p> <ul style="list-style-type: none"> ● 整体状态：服务器整体状态。 ● 风扇：风扇健康状态。 ● 网络：网络健康状态。 ● 电源：电源健康状态。 <p>说明：各模块健康状态可包含为：</p> <ul style="list-style-type: none"> ● 正常/在位 ● 灯亮 ● 警告 ● 严重 ● 不在位/灯灭
固件版本信息	<p>固件版本信息，包括：</p> <ul style="list-style-type: none"> ● CMC 版本。 ● PSU 版本。
在线用户信息	<p>当前登录本CMC Web的用户信息，包括：</p> <ul style="list-style-type: none"> ● 类型：登录类型，如 HTTPS、CLI 等。 ● 用户名：登录 CMC 的用户名。 ● 用户组：登录 CMC 的用户对应的用户组信息。 ● IP 地址：登录 CMC 的用户所在机器 IP 地址信息。
快速启动任务	<p>可进行相应的快捷操作，到达指定页面，包括：</p> <ul style="list-style-type: none"> ● 用户管理：点击本入口可以直接跳转到“CMC 设置>用户精细化管理”界面。 ● 网络管理：点击本入口可以直接跳转到“CMC 设置>网络”界面。

区域	展示的信息
	<ul style="list-style-type: none"> ● 系统信息：点击本入口可以直接跳转到“信息>系统信息”界面。 ● 固件更新：点击本入口可以直接跳转到“系统维护>HPM 固件更新”界面。
近期事件日志	<p>显示最近的10条事件日志信息，包含：</p> <ul style="list-style-type: none"> ● 事件 ID：事件日志的 ID 信息。 ● 时间戳：事件日志发生的时间。 ● 传感器名称：触发事件日志的传感器名称。 ● 传感器类型：IPMI2.0 中定义的传感器类型，包含： <ul style="list-style-type: none"> - Temperature //温度传感器。 - Voltage //电压传感器。 - Power Unit //PSU 状态传感器。 ● 描述：事件日志的描述信息。 <p>说明：如需查询更多事件日志，可查看“日志和告警>系统事件日志”页面。</p>

3.3 信息

3.3.1 刀片模块

功能描述

通过“刀片模块”界面的功能，您可以：

- 切换被管理的 CMC。
- 获取被管理 CMC 相应的 BMC 刀片信息，包括刀片在位、开关机状态、共享口 IP 地址和专口 IP 地址。
- 对被管理的 BMC 节点进行开机、关机、强制关机、循环开机、重启 BMC 等操作。
- 对选中的 BMC 节点进行批量开机、关机、强制关机或重启操作。

界面展示

在导航栏中选择“信息>刀片模块”，打开如下图 3-5 所示界面。

图 3-5 刀片模块



参数说明

表 3-4 刀片模块

参数	描述
选中	指示当前的BMC节点行是否被选中。
编号	编号。
状态	BMC节点的状态，包括： <ul style="list-style-type: none"> ● 在位/正常 ● 不在位/灯灭 ● 警告 ● 严重
类型	BMC节点类型，包括： <ul style="list-style-type: none"> ● 半宽 ● 半宽存储 ● 全宽存储 ● 不可用 说明：对于半宽存储和全宽存储节点，只占用节点刀片位置，不能执行各

参数	描述
	种电源操作。各种电源操作可由其所属的半宽节点来执行。
UID状态	当前BMC节点UID状态，包括： <ul style="list-style-type: none"> ● UID灯亮 ● UID灯灭
开关机状态	当前BMC节点开关机状态，包括： <ul style="list-style-type: none"> ● 开机 ● 关机 ● 不可用
操作	对当前BMC节点可执行的操作，点击相应的按钮可执行对应的操作。包括： <ul style="list-style-type: none"> ● 开机 ● 关机 ● 强制关机 ● 重启 ● 循环开机 ● 重启BMC
BMC eth0	显示当前BMC节点的专用管理口IP地址。
BMC eth1	显示当前BMC节点的共享管理口IP地址。

3.3.2 刀片版本信息

功能描述

通过“刀片版本信息”界面的功能，您可以：

- 切换被管理的 CMC。
- 获取被管理 CMC 上的各个 BMC 节点的 BMC 版本、BIOS 版本和 CPLD 版本。

界面展示

在导航栏中选择“信息>刀片版本信息”，打开如下图 3-6 所示界面。

图 3-6 刀片版本信息



参数说明

表 3-5 刀片版本信息

参数	描述
CMC IP	下拉选择当前被管理机箱的IP。
编号	编号。
BMC镜像1版本	当前BMC节点的BMC镜像1版本。
BMC镜像2版本	当前BMC节点的BMC镜像2版本。
BIOS版本	当前BMC节点的BIOS版本。
CPLD版本	当前BMC节点的CPLD版本。

3.3.3 系统信息

功能描述

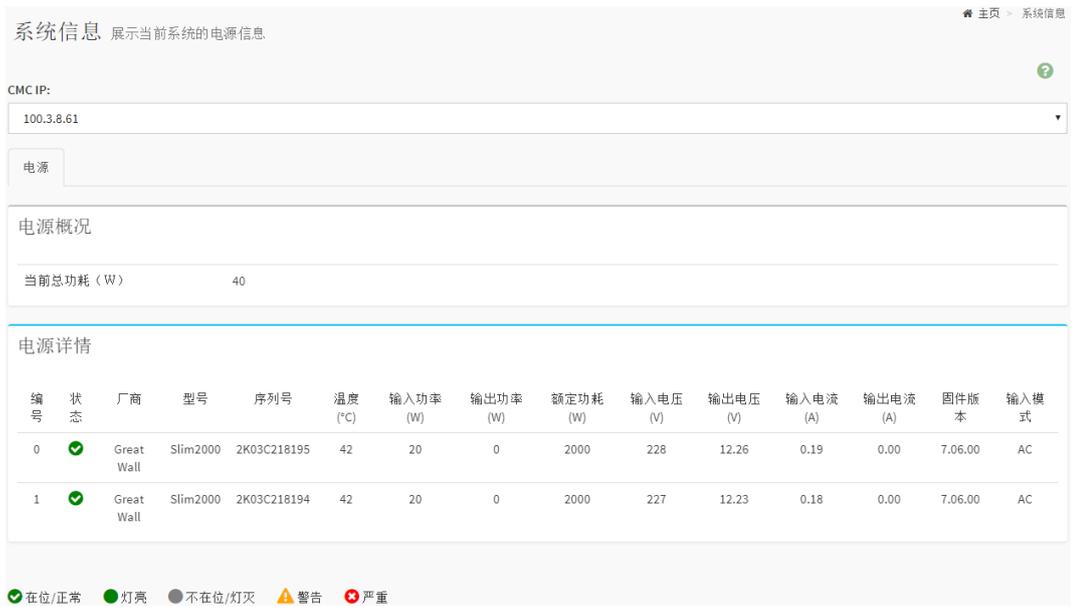
通过“系统信息”界面的功能，您可以获取当前 CMC 系统的：

- 电源概况
- 电源详情

界面展示

在导航栏中选择“信息>系统信息”，打开如下图 3-7 所示界面。

图 3-7 系统信息



参数说明

表 3-6 电源概况

参数	描述
当前总功耗(W)	电源总功耗。

表 3-7 电源详情

参数	描述
编号	电源编号。
状态	电源状态, 包含: <ul style="list-style-type: none"> ● 在位/正常 ● 灯亮 ● 不在位/灯灭 ● 警告 ● 严重
厂商	电源厂商。
型号	电源型号。

参数	描述
序列号	电源序列号。
温度(°C)	电源温度。
输入功率(W)	电源输入功率。
输出功率(W)	电源输出功率。
额定功耗(W)	电源额定功耗。
输入电压(V)	电源输入电压。
输出电压(V)	电源输出电压。
输入电流(A)	电源输入电流。
输出电流(A)	电源输出电流。
固件版本	电源固件版本。
输入模式	电源输入模式，包含： <ul style="list-style-type: none"> ● AC ● DC

3.3.4 FRU 信息

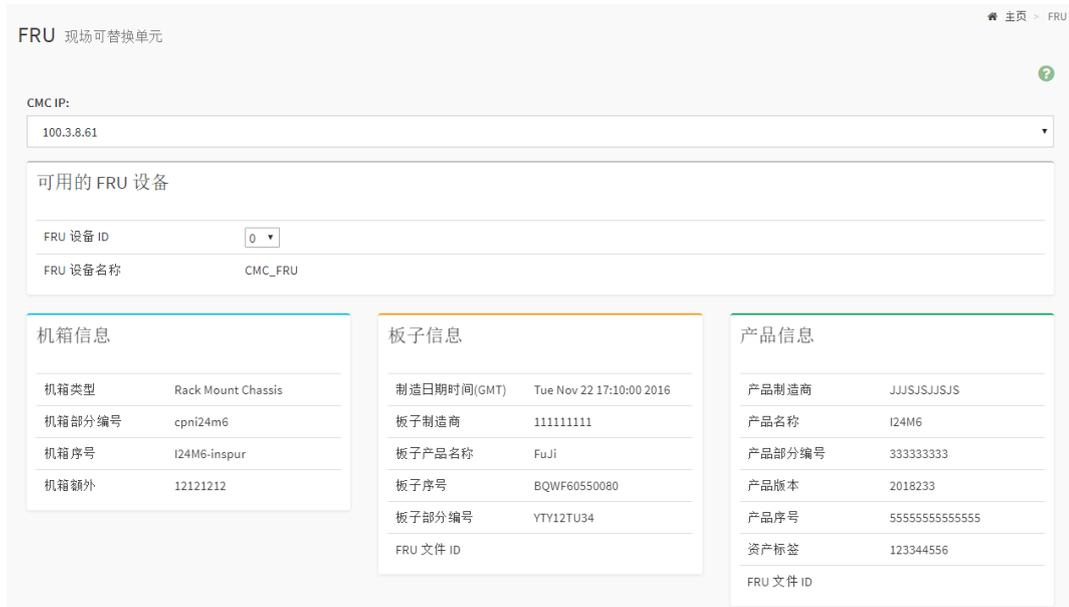
功能描述

通过“FRU 信息”界面的功能，您可以获取服务器的 FRU（可替换单元）设备信息。

界面展示

在导航栏中选择“信息>FRU 信息”，打开如下图 3-8 所示界面，包括可用的 FRU 设备、机箱信息、板子信息和产品信息。CMC 固件升级不会导致 FRU 信息丢失。

图 3-8 FRU 信息



参数说明

表 3-8 FRU 信息

类别	参数
CMC IP	显示当前被管理的CMC IP地址。 下拉选择其他CMC IP地址。
可用的FRU设备	FRU设备ID，下拉可选。 FRU设备名称，例如：CMC_FRU。
机箱信息	机箱类型，例如：塔式。 机箱部分编号。 机箱序号。 机箱额外。
板子信息	制造日期时间（GMT）。 板子制造商：Inspur。 板子产品名称。 板子序号。 板子部分编号。 FRU文件ID。

类别	参数
产品信息	产品制造商：Inspur。 产品名称。 产品部分编号。 产品版本。 产品序号。 资产标签。 FRU文件ID。

3.3.5 历史曲线

功能描述

CMC 提供“历史曲线”功能，管理员可以通过能源监控曲线了解电力和散热资源的实际使用情况，用户可以查看历史数据。

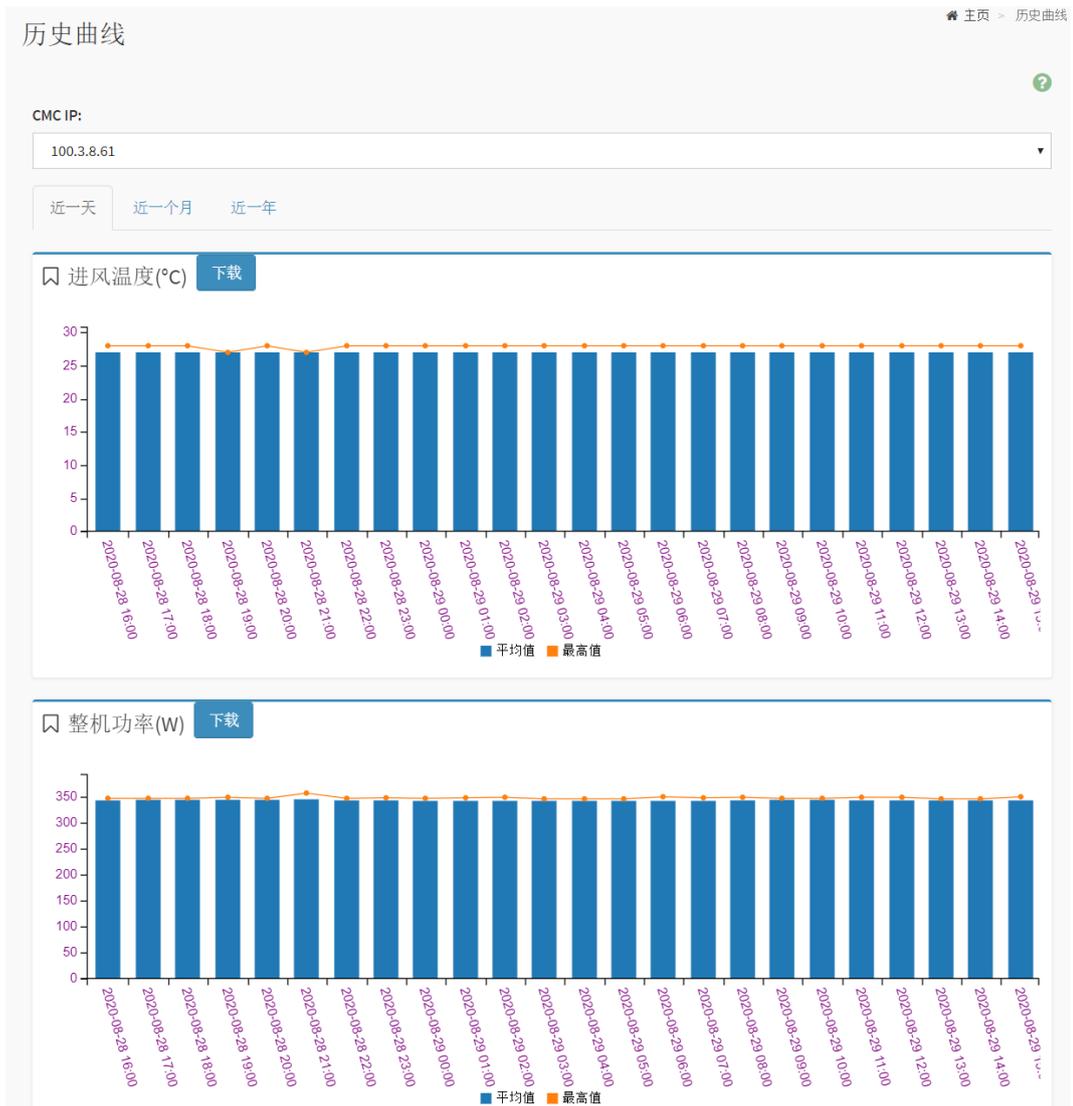
通过“历史曲线”界面的功能，您可以：

- 查看进风温度近一天/近一个月/近一年的曲线。
- 下载进风温度近一天/近一个月/近一年的数据。
- 查看整机功率近一天/近一个月/近一年的曲线。
- 下载整机功率近一天/近一个月/近一年的数据。
- 查看风扇转速近一天/近一个月/近一年的曲线。
- 下载风扇转速近一天/近一个月/近一年的数据。
- 查看 PSU0/PSU1/PSU2/PSU3 输入功耗近一天/近一个月/近一年的曲线。
- 下载 PSU0/PSU1/PSU2/PSU3 输入功耗近一天/近一个月/近一年的数据。

界面展示

在导航栏中选择“信息>历史曲线”，打开如下[图 3-9](#)所示界面。

图 3-9 历史曲线



参数说明

表 3-9 历史曲线

参数	描述
近一天	该页签显示近一天的进风温度曲线、整机功率曲线、风扇转速曲线、PSU*输入功耗曲线。
近一个月	该页签显示近一个月的进风温度曲线、整机功率曲线、风扇转速曲线、PSU*输入功耗曲线。
近一年	该页签显示近一年的进风温度曲线、整机功率曲线、风扇转速曲线、PSU*输入功耗曲线。

参数	描述
下载	点击“下载”按钮，可以下载进风温度/整机功率/风扇转速/PSU*输入功耗对应的历史数据。

3.4 远程控制

3.4.1 服务器定位 UID

功能描述

通过“服务器定位 UID”界面的功能，您可以执行点亮和熄灭定位灯操作来定位服务器。

界面展示

在导航栏中选择“远程控制>服务器定位 UID”，打开如下[图 3-10](#)所示界面。

图 3-10 服务器定位



参数说明

表 3-10 服务器定位 UID

参数	描述
UID灯状态	<ul style="list-style-type: none">• 当前服务器UID灯亮。• 当前服务器UID灯灭。
点亮UID灯	点亮当前服务器UID灯。
熄灭UID灯	熄灭当前服务器UID灯。

3.5 日志和告警

功能描述

日志和告警提供主要设备状态变化的历史记录以及当前系统的告警情况，用于故障诊断和分析。

3.5.1 系统事件日志

功能描述

通过“系统事件日志”界面的功能，您可以查看 CMC 系统事件日志、下载系统事件日志和清除系统事件日志。系统事件日志特性如下：

- 最多支持 3639 个条目。
- 支持循环模式。当 SEL 已满时，最旧的日志将被丢弃，新产生的日志被保留。
- 操作清除 SEL 时，1 条“SEL 被清除”的日志将被记录在 SEL 中。
- 支持通过 Web 或 IPMI CMD 导出 SEL。
- 支持通过 SNMP Trap、Syslog 通知事件到远程客户端。

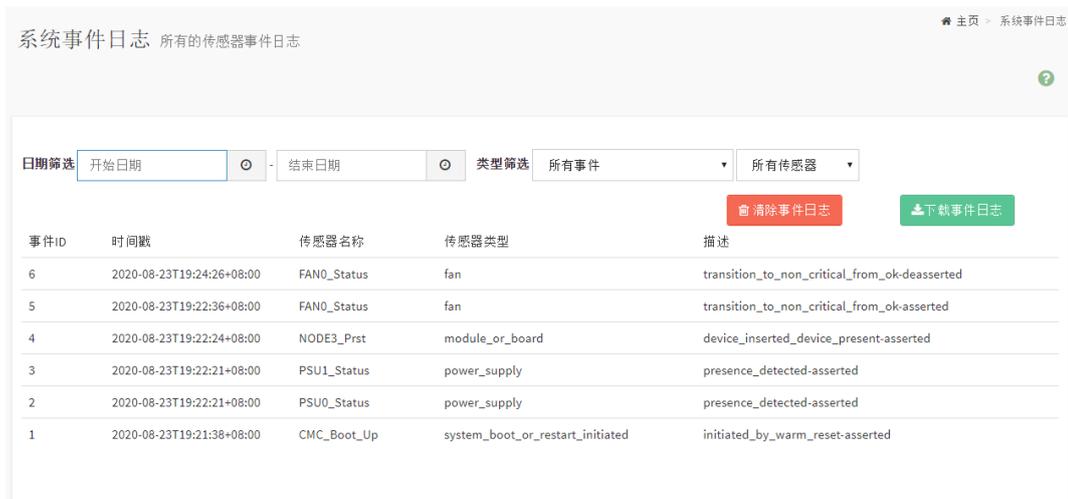


用户也可以通过 IPMI CMD 获取系统事件日志。

界面展示

在导航栏中选择“日志和告警>系统事件日志”，打开如下[图 3-11](#)所示界面。

图 3-11 系统事件日志



参数说明

表 3-11 SEL 特性

参数	描述
事件ID	SEL中的事件ID。
时间戳	事件日志生成时间。
传感器名称	传感器名称，可通过ipmitool sdr elist查看该设备上所有传感器名称。
传感器类型	IPMI2.0中定义的传感器类型，包含： <ul style="list-style-type: none"> ● Temperature //温度传感器。 ● Voltage //电压传感器。 ● Power Unit //PSU状态传感器。
描述	事件详细信息。

表 3-12 系统事件日志操作说明

参数	描述
过滤	选择事件类型、传感器和起止日期以进行过滤搜索。 动作：您可以用过滤器选项（事件类型、传感器名称、起止时间），查看设备中记录的特定事件。
下载事件日志	点击该按钮可下载事件日志到本地。
清除事件日志	点击该按钮将删除所有现有传感器日志记录。

3.5.2 日志设置

功能描述

通过“日志设置”界面的功能，您可以配置 Syslog 日志设置，使 CMC 系统向第三方服务器以 Syslog 报文方式发送日志。

界面展示

在导航栏中选择“日志和告警>日志设置”，打开如下图 3-12 所示界面，点击“Syslog 日志设置”，打开如下图 3-13 所示界面。

图 3-12 日志设置

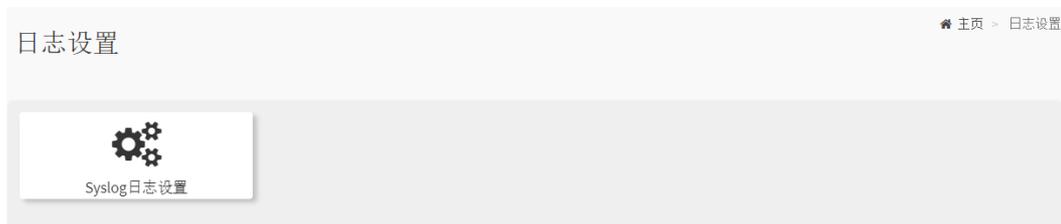


图 3-13 Syslog 设置



参数说明

表 3-13 Syslog 设置

参数	描述
远程日志	Syslog告警日志存储位置，可选择是否存储远程日志。 使用远程日志时，CMC将日志存放在远程Syslog服务器中和本地日志文件中。不使用远程日志时，仅会存放在本地日志文件中。
告警级别	高于此告警级别的事件将被发送，可选为： <ul style="list-style-type: none">● Info：发送 Info、Warning 和 Critical 级别的告警信息。● Warning：发送 Warning、Critical 级别的告警信息。● Critical：仅发送 Critical 级别的告警信息。
传输协议	Syslog报文在CMC系统和Syslog服务器之间传输时使用的传输协议，可选为： <ul style="list-style-type: none">● UDP：面向非连接的协议，在正式收发数据前，收发方不建立连接，直接传输正式的数据。● TCP：面向连接的协议，在正式收发数据前，必须在收发方建立可靠的连接。

表 3-14 Syslog 服务器和报文格式

参数	描述
序号	序号。
启用	启用或关闭自动上报Syslog报文功能。
服务器地址	Syslog服务器地址信息。
端口	Syslog服务器端口号。
日志类型	需要使用Syslog报文上报的日志类型。可选为：Idl日志，audit日志中的一项或多项。
操作	保存，保存该Syslog服务器和报文相关信息。 测试，测试已设置的Syslog通道是否可以成功发送报文。

3.5.3 审计日志

功能描述

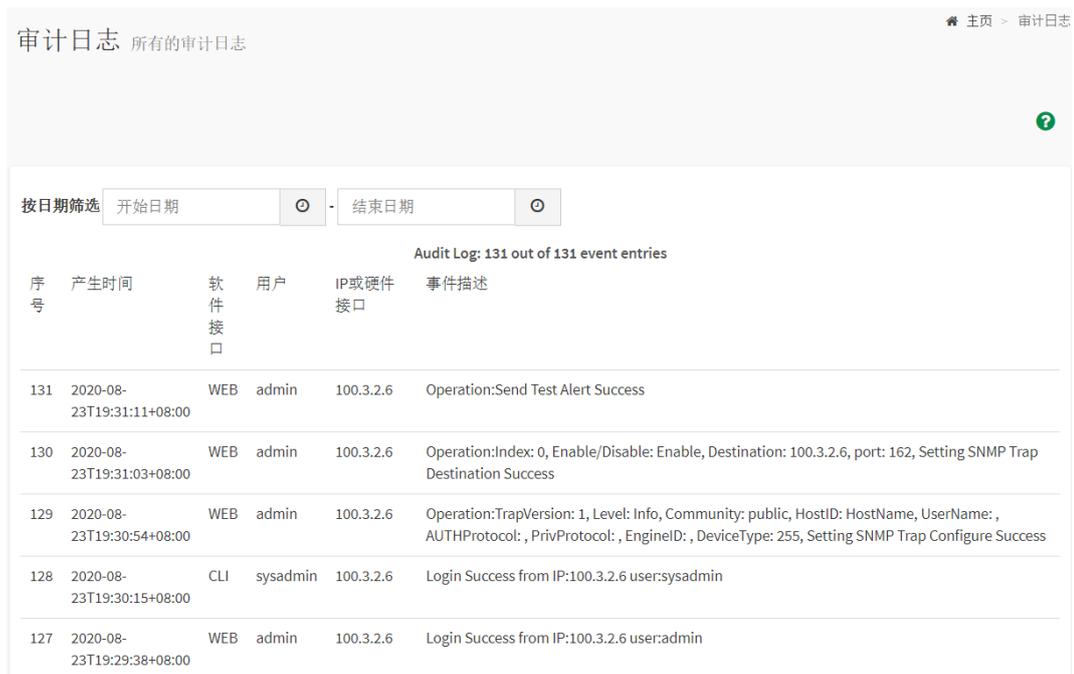
通过“审计日志”界面的功能，您可以查看系统审计日志。CMC 审计日志特性如下：

- 通过 SSH、Web、IPMI、Redfish 接口登陆系统进行管理的关键行为会被记录，其范围包括但不限于登录、注销、用户管理、口令管理、授权管理、核心安全配置（如访问控制策略、自动更新策略、安全监控策略、审计功能等）的变更、固件更新和恢复等。
- 审计日志支持的大小是 200K，如果超过 200K，较老的日志将会被备份到 CMC 中。当前的审计日志可通过 Web 进行查看，较老的审计日志可通过一键收集日志功能下载。

界面展示

在导航栏中选择“日志和告警>审计日志”，打开如下图 3-14 所示界面。

图 3-14 审计日志



参数说明

表 3-15 审计日志特性

参数	描述
序号	审计日志序号，序号越小的操作发生越早。
产生时间	审计日志产生时间。

参数	描述
软件接口	软件接口，包括： <ul style="list-style-type: none"> ● Web ● CLI ● IPMI ● Redfish ● RESTful
用户	用户，记录日志事件操作用户，如admin、sysadmin或者NA等。 说明：当硬件接口显示为HOST时，用户显示为NA。
IP或硬件接口	IP或硬件接口，硬件接口包括Serial、HOST、IPMB、USB和SSIF。
事件描述	事件详细信息。

表 3-16 审计日志和系统日志具体配置参数

参数	描述
过滤	选择起止日期以进行过滤搜索。 动作：您可以用过滤器选项（起止时间），查看设备中记录的特定事件。

3.5.4 IDL 日志

功能描述

浪潮故障诊断日志 IDL 是浪潮 CMC 独有的日志类型，用于记录 CMC 设备上基于 IPMI 传感器的事件历史记录。IDL 日志信息与系统事件日志信息一一对应，相比于系统日志信息而言，IDL 信息提供的信息更多、更全，每条日志都有相应的处理建议，能更有效的帮助用户进行日志诊断和分析。IDL 日志可以按照日期、严重性、设备、关键字等方式进行过滤，可执行日志下载和日志清除操作，点击每条日志后侧  按钮可获取关于本条日志的处理建议以及相应的操作步骤。

通过“IDL 日志”界面的功能，您可以查看此设备上的 CMC IDL 日志列表。通过点击相应告警事件右侧的处理建议按钮，可以查看对该告警事件的处理建议。

界面展示

在导航栏中选择“日志和告警>IDL 日志”，打开如下图 3-15 所示界面，点击界面上  可打开如下图 3-16 所示告警事件处理建议界面。

图 3-15 IDL 日志

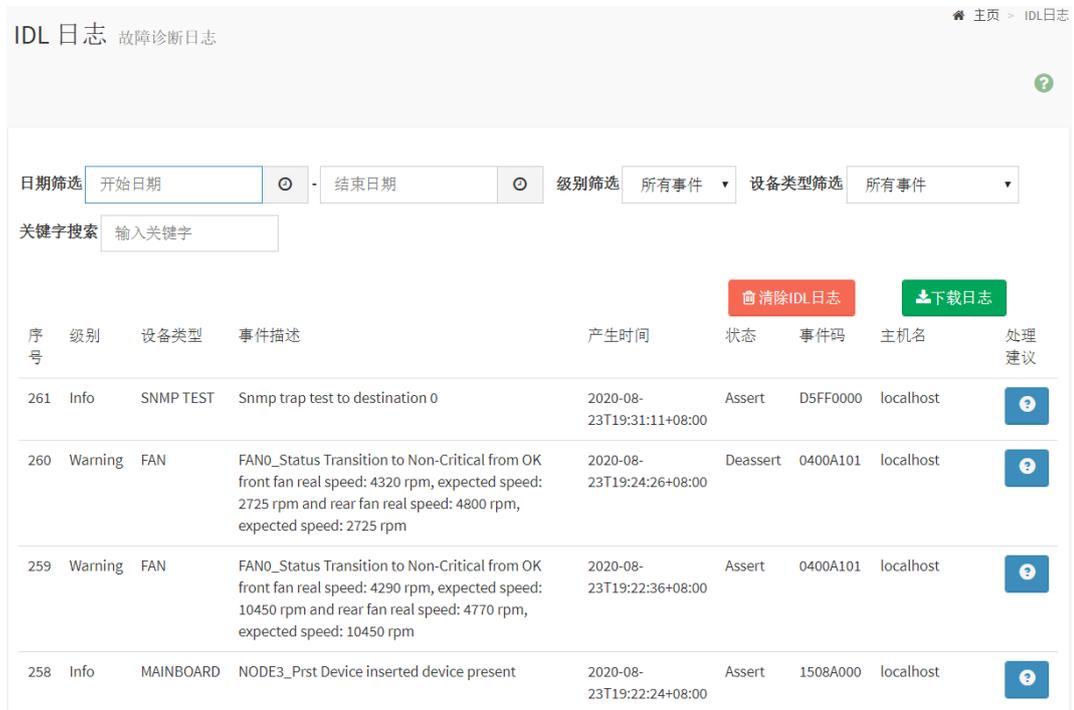


图 3-16 IDL 告警事件处理建议

处理建议

- Step1:Check whether the alarmed fan module is pulled out.
- Step2:Reset the related fan module, check whether the alarm disappears.
- Step3:Replace the failed fan, check whether the alarm disappears.
- Step4:Please contact inspur FAE.

确定

参数说明

表 3-17 IDL 日志配置参数

参数	描述
序号	IDL日志中的事件ID。

参数	描述
级别	事件错误等级, 包括Info、Warning和Critical。
设备类型	<p>告警事件关联的实体部件, 部件类型如下:</p> <ul style="list-style-type: none"> ● FAN ● INTRUSION ● CPU ● PSU ● ADDIN CARD ● MEMORY ● DISK ● SYS FW PROGRESS ● EVENT LOG ● WATCHDOG1 ● SYSTEM EVENT ● POWER BUTTON ● MAINBOARD ● PCIE ● BMC ● PCH ● CABLE ● SYS RESTART ● BOOT ERROR ● BIOS BOOT ● OS STATUS ● ACPI STATUS ● IPMI WATCHDOG ● LAN ● SUB SYSTEM ● BIOS OPTIONS ● GPU

参数	描述
	<ul style="list-style-type: none"> ● RAID ● FW UPDATE ● SYSTEM ● SNMP TEST ● SMTP TEST
事件描述	告警事件的详细描述。
产生时间	IDL日志产生时间。
状态	显示日志的状态，触发日志或解除日志。
事件码	告警事件的唯一故障编码，长度为8个字节。参考表3-19 IDL事件码说明。
主机名	服务器系统主机名。
处理建议	针对此告警事件的处理建议。

表 3-18 IDL 日志操作说明

参数	描述
过滤	<p>选择严重性和起止日期以进行过滤搜索。</p> <p>动作：您可以用过滤器选项（事件严重性级别、时间、关键字），查看设备中记录的特定事件。</p>
下载日志	下载IDL日志到本地。
清除IDL日志	点击“清除IDL日志”按钮将清除该CMC上所有IDL日志信息。

表 3-19 IDL 事件码说明

字节	含义
6-7	<p>部件类型。</p> <p>16进制数与部件对应关系，例如：</p> <ul style="list-style-type: none"> ● 04: FAN ● 05: INTRUSION ● 07: CPU ● 08: PSU ● 0B: ADDIN_CARD ● 0C: MEMORY

字节	含义
	<ul style="list-style-type: none"> ● 0D: DISK
4-5	部件的序号, 指在此部件类型中的序号。
2-3	事件的偏移量, 表示事件类型。
0-1	告警级别。 16进制数与告警级别对应关系: <ul style="list-style-type: none"> ● 00: INFO ● 01: WARNING ● 02: CRITICAL

3.5.5 一键收集日志

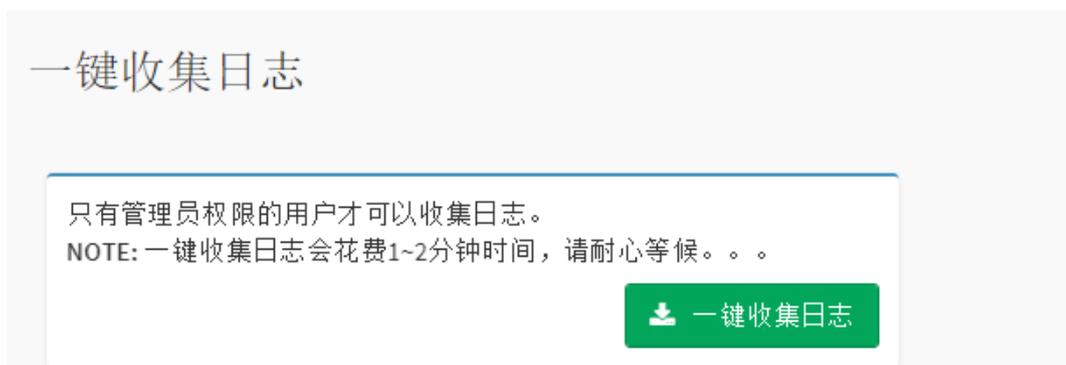
功能描述

通过“一键收集日志”界面的功能, 您可以一键收集所有故障诊断分析需要的信息, 包括日志、运行数据、CMC 配置、部件等。点击一键收集日志按钮后, 大概需要 1~2 分钟时间完成日志收集。

界面展示

在导航栏中选择“日志和告警>一键收集日志”, 打开如下[图 3-17](#)所示界面。

图 3-17 一键收集日志



等日志收集结束后, 下载的内容如下, 包括日志、运行数据、配置和部件。

表 3-20 一键收集日志内容列表

分类	信息项	一键日志文件中的路径
日志	SEL日志	onekeylog/log/selelist.csv
	审计日志	onekeylog/log/audit.log, audit.log1
	IDL日志	onekeylog/log/idl.log
	系统日志	onekeylog/log/info.log, info.log1 onekeylog/log/warning.log, warning.log1 onekeylog/log/err.log, onekeylog/log/err.log.1 onekeylog/log/crit.log onekeylog/log/alert.log onekeylog/log/emerg.log
	调试日志	onekeylog/log/inspur_debug.log, inspur_debug.log.1
	维护日志	onekeylog/log/maintenance.log, maintenance.log.1
	电源黑匣子	onekeylog/log/psuFaultHistory.log
	BMC Uart日志	onekeylog/sollog/BMCUart.log, onekeylog/sollog/BMCUart.log.1
	网卡日志	onekeylog/sollog/NetCard.log, onekeylog/sollog/NetCard.log.1
	Linux内核日志	onekeylog/log/dmesg
	BMC SEL日志	onekeylog/log/BMC1/SEL.dat
	Flash状态日志	onekeylog/log/flash_status
	SNMP Trap统计日志	onekeylog/log/index.log
Notice日志	onekeylog/log/notice.log, onekeylog/log/notice.log.1	
运行数据	CMC时间	onekeylog/runningdata/rundatainfo.l og
	CMC Flash使用率	onekeylog/runningdata/rundatainfo.l og
	电压、温度、电流、转速、功率	onekeylog/runningdata/rundatainfo.l og
	传感器信息	onekeylog/runningdata/rundatainfo.l og
	进程信息	onekeylog/runningdata/rundatainfo.l og
	风扇信息	onekeylog/runningdata/faninfo.log

分类	信息项	一键日志文件中的路径
	I2C通道信息	onekeylog/runningdata/rundatainfo.log
	I2C从设备EEPROM、寄存器实时数据	onekeylog/runningdata/rundatainfo.log
	功率统计	onekeylog/runningdata/rundatainfo.log
	运行中创建的文件	onekeylog/runningdata/var/
	在线会话信息	onekeylog/runningdata/racsessioninfo
	当前CMC网络信息	onekeylog/runningdata/rundatainfo.log
	当前CMC路由信息	onekeylog/runningdata/rundatainfo.log
	网口收发包信息	onekeylog/runningdata/rundatainfo.log
	CMC累计运行时间	onekeylog/runningdata/rundatainfo.log
	驱动信息	onekeylog/runningdata/rundatainfo.log
配置	用户信息	onekeylog/configuration/config.log
	DNS	onekeylog/configuration/conf/dns.conf
	BMC网络	onekeylog/configuration/config.log
	sshd配置	onekeylog/configuration/conf/ssh_server_config
	服务（SSH/Web/IPMI LAN等）配置	onekeylog/configuration/conf/ncml.conf
	BIOS菜单项配置	onekeylog/configuration/conf/redfish/bios/BiosAttributeRegistry0.24.00.0.24.0.json
	功率封顶配置	onekeylog/configuration/conf/redfish/bios/bios_current_settings.json
	Email配置	onekeylog/configuration/conf/redfish/bios/bios_future_settings.json
	SNMP Trap配置	onekeylog/configuration/conf/SnmTrapCfg.json
	SMTP配置文件	onekeylog/configuration/conf/SmtpCfg.json
Syslog配置	onekeylog/configuration/conf/Syslog.conf	

分类	信息项	一键日志文件中的路径
部件	电源	onekeylog/component/component.log
	风扇	onekeylog/component/component.log
	网卡	onekeylog/component/component.log
	CMC	onekeylog/component/component.log
	主板	onekeylog/component/component.log
	硬盘背板	onekeylog/component/component.log
	PCIe Riser卡	onekeylog/component/component.log
	固件版本信息	onekeylog/component/component.log



说明

更详细内容可联系 CMC 开发人员获取，一键收集日志包含内容可因机型差别存在差异。

3.5.6 当前告警

功能描述

当系统日志中产生告警信息，会添加告警日志。通过“当前告警”界面的功能，您可以查看该系统中的未解除告警信息，点击每条日志后侧  按钮可获取关于本条日志的处理建议以及相应的操作步骤。

界面展示

在导航栏中选择“日志和告警>当前告警”，打开如下 [图 3-18](#) 所示界面。

图 3-18 当前告警

级别	序号	设备类型	事件描述	产生时间	事件码	处理建议
Warning	1	PSU	PSU_Redundant Redundancy Lost	2000-08-21T01:12:15+08:00	08112201	

参数说明

表 3-21 当前告警

参数	描述
级别	告警级别，包括Info、Warning和Critical。
序号	告警序号。
设备类型	告警事件关联的实体部件，部件类型如下： <ul style="list-style-type: none"> ● FAN ● INTRUSION ● CPU ● PSU ● ADDIN CARD ● MEMORY ● DISK ● SYS FW PROGRESS ● EVENT LOG ● WATCHDOG1 ● SYSTEM EVENT ● POWER BUTTON ● MAINBOARD ● PCIE ● BMC ● PCH

参数	描述
	<ul style="list-style-type: none"> ● CABLE ● SYS RESTART ● BOOT ERROR ● BIOS BOOT ● OS STATUS ● ACPI STATUS ● IPMI WATCHDOG ● LAN ● SUB SYSTEM ● BIOS OPTIONS ● GPU ● RAID ● FW UPDATE ● SYSTEM ● SNMP TEST ● SMTP TEST
事件描述	告警事件的详细描述。
产生时间	告警信息的产生时间。
事件码	告警事件的唯一故障编码。可参考表格3-19 IDL事件码说明。
处理建议	针对此告警事件的处理建议。

3.5.7 SNMP Trap 设置

功能描述

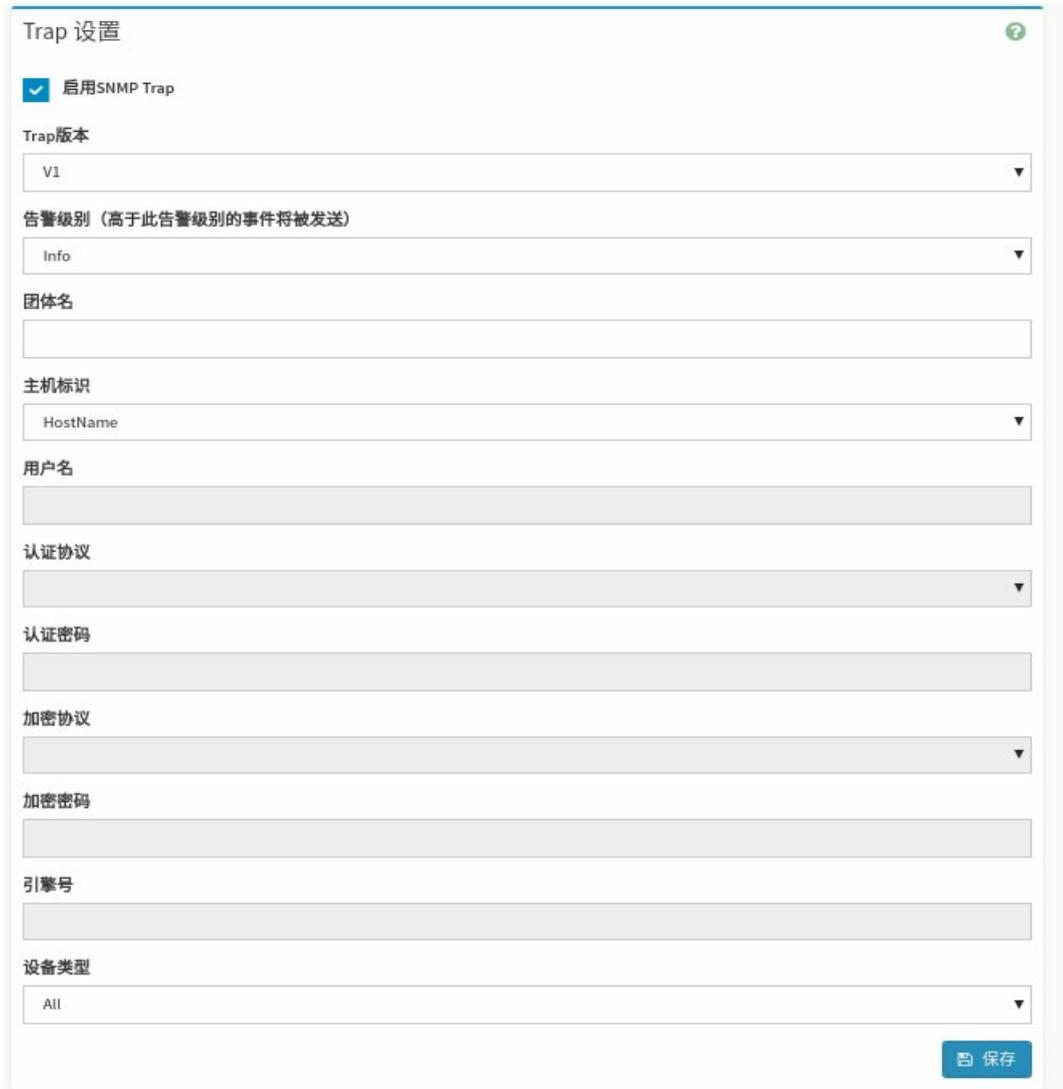
通过“SNMP Trap 设置”界面的功能，您可以：

- 启用 SNMP Trap。
- 设置告警策略。

操作步骤

1. 在导航栏中选择“日志和告警>SNMP Trap设置”，打开如下图3-19所示界面。

图 3-19 SNMP Trap 设置



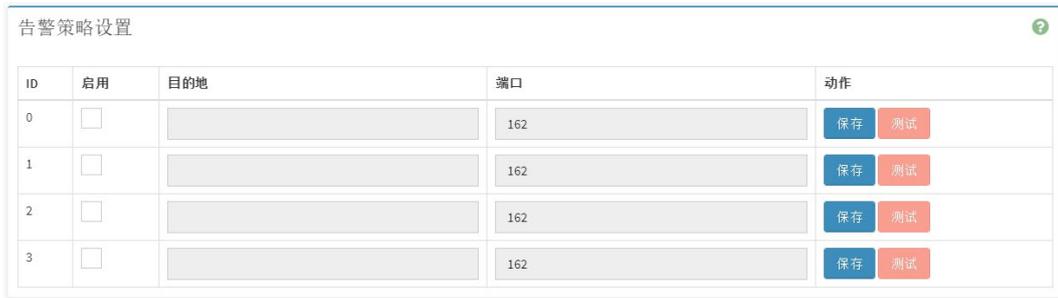
The image shows a web-based configuration interface for SNMP Trap settings. The title is "Trap 设置" (Trap Settings). At the top right, there is a green help icon. The main content area contains several configuration options:

- 启用SNMP Trap (Enable SNMP Trap)
- Trap版本 (Trap Version): A dropdown menu with "V1" selected.
- 告警级别 (高于此告警级别的事件将被发送) (Alert Level (Events above this alert level will be sent)): A dropdown menu with "Info" selected.
- 团体名 (Community Name): An empty text input field.
- 主机标识 (Host Identifier): A dropdown menu with "HostName" selected.
- 用户名 (Username): An empty text input field.
- 认证协议 (Authentication Protocol): A dropdown menu.
- 认证密码 (Authentication Password): An empty text input field.
- 加密协议 (Encryption Protocol): A dropdown menu.
- 加密密码 (Encryption Password): An empty text input field.
- 引擎号 (Engine ID): An empty text input field.
- 设备类型 (Device Type): A dropdown menu with "All" selected.

At the bottom right of the form, there is a blue button labeled "保存" (Save).

2. 勾选“启用SNMP Trap”选项，选择Trap版本、告警级别和团体名等。
3. 设置告警策略，点击启用按钮，设置SNMP Trap服务器的IP为目的地、端口，点击“保存”。

图 3-20 告警策略设置



告警策略设置

ID	启用	目的地	端口	动作
0	<input type="checkbox"/>		162	保存 测试
1	<input type="checkbox"/>		162	保存 测试
2	<input type="checkbox"/>		162	保存 测试
3	<input type="checkbox"/>		162	保存 测试

说明

- SNMP 默认端口号为 162。
- CMC 支持 SNMP Trap。用户需打开 Trap 接收器，在 CMC Web GUI 中设置 Trap 目标 IP，当 CMC 检测到事件发生时，CMC 将自动发送事件给 Trap 接收器。

3.6 传感器

功能描述

通过“传感器”界面的功能，您可以查看当前系统支持的所有传感器的相关信息，并可以通过双击门限传感器界面中的传感器行跳转到修改传感器阈值界面进行设置。传感器界面包含门限传感器页签和离散传感器页签。

界面展示

在导航栏中选择“传感器”，选择“门限传感器”页签，打开如下[图 3-21](#)所示界面。

图 3-21 门限传感器

传感器读数 活动中传感器状态读取 ? 主页 > 传感器

门限传感器 离散传感器

门限传感器

名称	当前值	状态	不可逆低阈	严重低阈	非严重低阈	非严重高阈	严重高阈	不可逆高阈	单位
Inlet_Temp	28	✔	NA	NA	NA	NA	40	45	deg_c
Outlet_Temp	28	✔	NA	NA	NA	75	NA	NA	deg_c
CMC_Temp	34	✔	NA	NA	NA	NA	80	85	deg_c
PSU0_Inlet_Temp	29	✔	NA	NA	NA	NA	NA	NA	deg_c
PSU1_Inlet_Temp	31	✔	NA	NA	NA	NA	NA	NA	deg_c
PSU2_Inlet_Temp	Disabled	●	NA	NA	NA	NA	NA	NA	deg_c

参数说明

表 3-22 门限传感器

参数	描述
名称	传感器名称。
当前值	传感器当前读值。
状态	传感器状态。
不可逆低阈	传感器不可逆低阈值。
严重低阈	传感器严重低阈值。
非严重低阈	传感器非严重低阈值。
非严重高阈	传感器非严重高阈值。
严重高阈	传感器严重高阈值。
不可逆高阈	传感器不可逆高阈值。
单位	传感器读值单位。

界面展示

在导航栏中选择“传感器”，选择“离散传感器”页签，打开如下图 3-22 所示界面。

图 3-22 离散传感器



参数说明

表 3-23 离散传感器

参数	描述
名称	传感器名称。
状态	传感器状态。

3.7 风扇管理

功能描述

通过“风扇管理”界面的功能，您可以查看风扇模块的在位情况、状态、当前转速、占空比等信息，可以设置风扇控制模式，手动控制风扇模式下还可以为每个风扇模块预定义转速。

界面展示

在导航栏中选择“风扇管理”，打开如下[图 3-23](#)所示界面。

图 3-23 风扇管理



说明

MCU 或 CPLD 将通过接收 CMC 看门狗信号来监控 CMC 风扇控制任务。如果 MCU 或 CPLD 在 4 分钟内不能收到看门狗信号，说明风扇控制任务异常，所有风扇都将被设置为安全转速以避免系统过热。

参数说明

表 3-24 风扇管理

参数	描述
控制模式	手动控制风扇或自动控制风扇。 手动控制风扇模式下，您可以手动调节每颗风扇的转速。
编号	风扇编号。

参数	描述
规格	风扇硬件规格，如8056、8038等。
状态	风扇状态，包括： <ul style="list-style-type: none"> ● 在位/正常 ● 警告 ● 不在位/灯灭
当前转速(rpm)	当前风扇转速。
占空比	当前风扇占空比。
转速控制	手动控制风扇模式下，可以设置转速，可设置为： <ul style="list-style-type: none"> ● 低速(20%) ● 中速(50%) ● 高速(75%) ● 满速(100%)

3.8 CMC 设置

3.8.1 网络

3.8.1.1 网络设置

功能描述

通过“网络设置”界面的功能，您可以查询和设置 CMC 管理网络配置情况，包括：

- NCSI 模式。
- 网络绑定的接口和模式。
- 网络 IP 设置。
- VLAN 属性。

网络设置相关特性如下：

- CMC 支持 CMC 专用 LAN 控制器。
- 最大带宽：专用网卡--1000M。

- CMC 网络接口兼容支持 IPv4 和 IPv6，支持 DHCP 或手动设置 IP 地址。
- MAC 地址保存在 EEPROM 中。
- 支持 VLAN。
- CMC 网络为专口独立模式。
- 默认情况下，IPMI LAN 通道分配如下：

表 3-25 CMC LAN 接口

通道ID	接口	支持会话
0x01	Primary LAN(dedicated)	Yes

界面展示

在导航栏中选择“CMC 设置>网络”，点击“网络设置”页签，打开如下[图 3-24](#)，[图 3-25](#) 所示界面。

图 3-24 网络

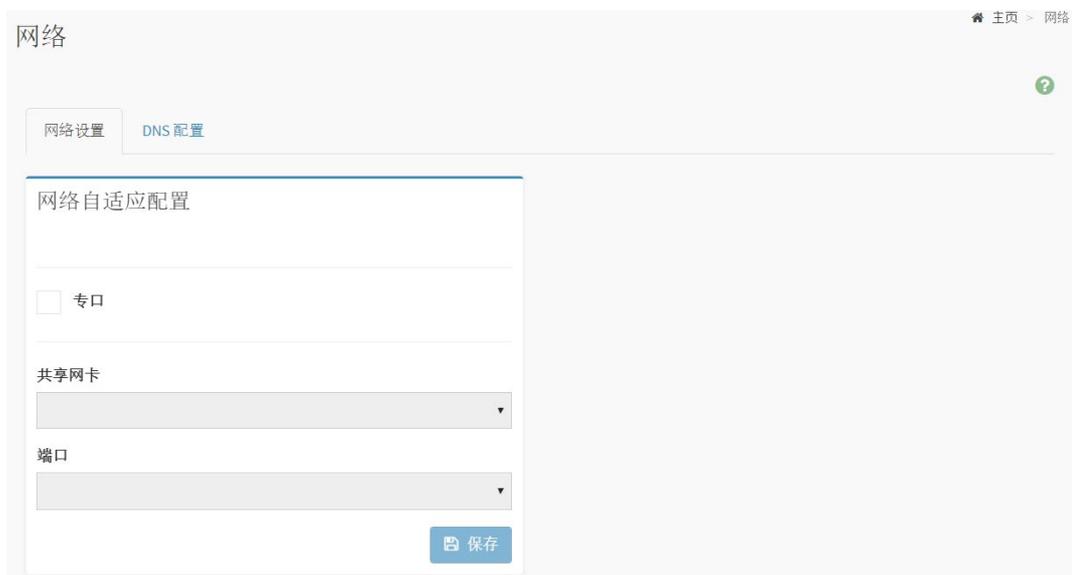


图 3-25 网络 IP 设置

网络 IP 设置

启用 LAN

LAN 界面
eth0

MAC 地址
B4:05:5D:1D:D1:0E

启用 IPv4

启用 IPv4 DHCP

IPv4 地址
100.3.8.36

IPv4 子网掩码
255.255.255.0

IPv4 默认网关
100.3.8.254

启用 IPv6

启用 IPv6 DHCP

IPv6 索引
0

IPv6 地址
::

子网掩码前缀长度
0

IPv6 网关
::

启用 VLAN

VLAN ID
0

VLAN 优先级
0

[保存](#)

参数说明

表 3-26 网络设置

参数	描述
共享网卡（NC-SI）配置。 注：NCSI模式不能进行配置。	
NCSI模式	自动故障切换模式和手动切换模式。
NCSI网卡	显示NCSI网卡。
端口	显示端口信息。
网络绑定配置	
启用绑定	勾选，启用绑定。
自动配置	启用此选项来自动配置接口。

参数	描述
绑定接口	显示绑定接口，eth0（专用管理口）。
绑定模式	显示网络绑定模式，不可配置。
网络IP设置	
启用LAN	勾选，启用LAN。
LAN界面	可选为eth0（专用管理口）或eth1（共享管理口）。
MAC地址	显示MAC地址。
启用IPv4	选中此选项，为选定的接口上启用IPv4支持。
启用IPv4 DHCP	勾选，使用DHCP动态配置IPv4地址。 不勾选，需指定静态IPv4地址信息，包括：“IPv4地址”、“IPv4子网掩码”、“IPv4默认网关”。
启用IPv6	选中此选项，为选定的接口上启用IPv6支持。
启用IPv6 DHCP	勾选，使用DHCP动态配置IPv6地址。 不勾选，需指定静态IPv6地址信息，包括：“IPv6索引”、“IPv6地址”、“子网掩码前缀长度”、“IPv6网关”。
启用VLAN	使能或禁止管理网口的VLAN属性。 默认关闭。 注：VLAN更改后必须要进行重启。
VLAN ID	管理网口所属VLAN。 取值范围0~7。
VLAN优先权	VLAN优先权。

3.8.1.2 DNS 配置

功能描述

通过“DNS 配置”界面的功能，您可以查询和设置 DNS，包括：

- 主机配置。
- 域名配置。
- 域名服务器配置。

界面展示

在导航栏中选择“CMC 设置>网络”，点击“DNS 配置”页签，打开如下图 3-26 所示界面。

图 3-26 DNS 配置

网络

网络设置 DNS 配置

DNS 已启用
 mDNS 启用

主机名称设置
 自动 手动

主机名称
AMIB4055D2F07C2

BMC 注册设置

BMC 界面:
eth0

注册 BMC

注册方法:
 名字服务器 DHCP 客户端 FQDN 主机名称

BMC 界面:
eth1

注册 BMC

注册方法:
 名字服务器 DHCP 客户端 FQDN 主机名称

Both

Eth0 TSIG Configuration
 TSIG 启用身份认证

当前 TSIG 私人文件
Not Available

新的 TSIG 私人档案
[File Selection]

Eth1 TSIG Configuration
 TSIG 启用身份认证

当前 TSIG 私人文件
Not Available

新的 TSIG 私人档案
[File Selection]

网域设置
 自动 手动

网域界面
eth1_v4

域名服务器设置
 自动 手动

DNS 界面
eth1

IP 优先权
 IPv4 IPv6

保存

参数说明

表 3-27 DNS 配置

参数	描述
DNS已启用	启用DNS。
mDNS启用	启用mDNS。
主机名称设置	主机名称设置，可选为自动或手动。 自动会显示默认主机名称。 手动需输入主机名称。
BMC注册设置	注册BMC： 勾选，注册BMC。 注册方法，可选为： <ul style="list-style-type: none">● 名字服务器● DHCP 客户端 FQDN● 主机名称 默认名字服务器。
TSIG配置	TSIG启用身份认证： 勾选，启用TSIG启用身份认证。 默认不启用。 当前TSIG私人文件： 显示当前TSIG私人文件。 新的TSIG私人档案： 浏览上传一个新的TSIG私人档案。
网域设置	自动或手动。 网域界面，可选为bond0_v4或bond0_v6。
域名服务器设置	自动或手动。 DNS界面，自动显示。 选择为手动时，需填写DNS服务器地址。
IP优先级	IPv4或IPv6。

3.8.2 用户精细化管理

功能描述

通过“用户精细化管理”界面的功能，您可以：

- 启用密码复杂度。
- 更改用户组权限。
- 添加用户。
- 删除用户。
- 更改用户。

CMC 用户管理相关特性如下：

- CMC 支持统一的用户管理机制，管理 IPMI、Web、SSH 和 Redfish 用户。由 IPMI 或 Web 创建的用户将具有 IPMI、Web、Redfish 和 SSH 用户权限。通过 SSH，用户可以访问 Smash-Lit CLI。
- Sysadmin 是用于访问 CMC 诊断串口，不能访问 IPMI、Web、Redfish 和 SSH。
- CMC 支持 IPMI 2.0 用户模型。统一用户可以通过 IPMI 命令或 Web GUI 创建。
- 最多支持 16 个用户。
- 16 个用户可以分配到任意通道，包括专用 LAN。
- 所有创建的用户都可以同时登录。
- 可用的用户权限级别有管理员、操作员、用户、无权限。IPMI 用户权限、Web GUI 用户权限和 Smash-Lite CLI 用户权限如下表 3-28、表 3-29、表 3-30 所示。

表 3-28 IPMI 用户权限

用户权限	支持的操作
管理员	读/写
操作员	读
用户	读

表 3-29 Web GUI 用户权限

用户组	权限
管理员	用户配置、常规配置、电源控制、安全配置、调试诊断、查询功能、配置自身。
操作员	常规配置、电源控制、查询功能、配置自身。
用户	查询功能、配置自身。

表 3-30 Smash-Lite CLI 用户权限

命令	子命令	用户	操作员	管理员
bmclog	get	是	是	是
	set	否	否	是
chassis	get	是	是	是
	set	否	否	是
mc	get	是	是	是
	set	否	否	是
diagnose	ls	否	否	是
	cat			
	last			
	ifconfig			
	ethtool			
	ps			
	top			
	dmesg			
	netstat			
	gpiotool			
	i2c-test			
	pwmtachtool			
	ipmitool			
df				
uptime				

界面展示

在导航栏中选择“CMC 设置>用户精细化管理”，打开如下[图 3-27](#)、[图 3-28](#)所示界面。

图 3-27 用户密码复杂度设置&权限管理

用户精细化管理 ?
主页 > 用户精细化管理

密码复杂度设置

启用密码复杂度

保存
重置

用户组权限管理

用户组名	用户配置	常规配置	电源控制	安全配置	调试诊断	查询功能	配置自身	操作
Administrator	▼	▼	▼	▼	▼	▼	▼	更改用户组权限
Operator	<input type="checkbox"/>	▼	▼	<input type="checkbox"/>	<input type="checkbox"/>	▼	▼	更改用户组权限
User	<input type="checkbox"/>	▼	▼	更改用户组权限				
OEM1	<input type="checkbox"/>	▼	<input type="checkbox"/>	更改用户组权限				
OEM2	<input type="checkbox"/>	▼	<input type="checkbox"/>	更改用户组权限				
OEM3	<input type="checkbox"/>	▼	<input type="checkbox"/>	更改用户组权限				
OEM4	<input type="checkbox"/>	▼	<input type="checkbox"/>	更改用户组权限				

图 3-28 用户管理

用户管理

用户ID	用户名	用户组	用户启用	IPMI权限	电子邮箱ID	操作
1	admin	Administrator	已启用	administrator		更改用户 删除用户
2						添加用户
3						添加用户
4						添加用户

参数说明

表 3-31 密码复杂度设置

参数	描述
启用密码复杂度	勾选，启用密码复杂度。 不勾选，不启用密码复杂度。

参数	描述
密码最小长度	默认为8，可设置8~16之间的数字。
启用复杂度	勾选，启用复杂度可设置密码复杂度的细节，可选择大写字母、小写字母、数字、特殊字符。如需要密码中必须包含大写字母时，勾选大写字母即可。 不勾选，不启用密码复杂度限制。
密码有效期（天）	可设置密码的生效时间，超过生效时间用户将禁止登录。单位：天。
历史密码记录	可设置历史密码记录中保存的条数，最多5条，历史密码将被禁止重新使用。历史密码记录0~5。
登录失败重试次数	可设置用户登录失败时重试的最多次数，最多5次，登录失败后用户将被锁定。登录失败重试次数0~5。
锁定时长（分钟）	默认为5。可设置5~60min。

表 3-32 用户组权限管理

用户组	权限
管理员	用户配置、常规配置、电源控制、安全配置、调试诊断、查询功能、配置自身。
操作员	常规配置、电源控制、查询功能、配置自身。
用户	查询功能、配置自身。
OEM*	OEM1、OEM2、OEM3、OEM4用户是预留给自定义权限的用户组，默认具有查询功能和配置自身权限，其他权限可通过勾选进行配置。

表 3-33 用户组权限对应功能

权限	描述
用户配置	用户组权限管理、用户管理、服务会话、一般LDAP设定、角色群组。
常规配置	DNS配置、密码复杂度设置、IDL日志清除、系统事件日志清除、服务配置、一般防火墙设置、IP地址防火墙规则、端口防火墙规则、日期&时间、保存配置、SEL日志设置策略、Syslog日志设置、SNMP Trap设置、SNMP set/get设置、邮箱告警、传感器阈值、HPM固件更新、固件镜像位置、恢复出厂设置、还原配置、前控制面板电源键设置、风扇管理、网络自适应配置、共享网卡配置、网络绑定配置、网络IP设置、BIOS启动选项。
电源控制	电源控制。
安全配置	生成SSL凭证、上传SSL凭证、系统管理员、审计日志。

权限	描述
调试诊断	宕机截屏、手动截屏、视频触发设置、视频远程存储、Pre-Event视频录制、模块重启、一键收集日志。
查询功能	可以登录以及查看除安全配置、用户配置外的其他信息。
配置自身	可以配置账户自身的密码、电子邮箱以及管理SSH公钥。

表 3-34 用户管理

参数	描述
用户ID	用户ID
用户名	用户名
用户组	用户组
用户权限	用户是否已启用，包括： <ul style="list-style-type: none"> ● 已启用 ● 未启用
IPMI权限	用户对应IPMI权限
电子邮箱ID	用户电子邮箱地址
操作	可执行的用户操作，包括： <ul style="list-style-type: none"> ● 添加用户 ● 更改用户 ● 删除用户

3.8.3 服务

功能描述

通过“服务”界面的功能，您可以查看和修改 CMC 运行中的服务的基本信息，包括：服务的状态、非安全端口、安全端口、超时时间以及最大会话数。

说明

- 修改服务信息，用户必须是管理员。
- 为保证系统的安全性，建议禁用不需要的服务，并关闭其端口。

- 除可修改的服务外，CMC 还使用了一些固定协议的端口，可参考表 3-36 固定协议。固定协议是不可配置的。

界面展示

在导航栏中选择“CMC 设置>服务”，打开如下图 3-29 所示界面。

图 3-29 协议和端口

服务	状态	非安全端口	安全端口	超时	最大会话数
web	活动的	80	443	1800	20
ssh	活动的	N/A	22	600	N/A
solssh	非活动的	N/A	N/A	60	N/A

参数说明

表 3-35 服务

参数	描述
服务	显示服务名称。
状态	活动的或非活动的。
非安全端口	非安全端口。
安全端口	安全端口。
超时	超时时长。单位：秒
最大会话数	显示各服务支持的最大会话数，不可更改。

表 3-36 固定协议

服务	用途	状态	端口号	TCP/UDP
smux	SNMP Multiplexer	启用	199	TCP
srvloc	Sever Location	启用	427	TCP、UDP
DHCP V6 Client	DHCP V6 Client	启用	546	UDP

服务	用途	状态	端口号	TCP/UDP
IPMI	IPMI	启用	623	UDP

3.8.4 系统防火墙

功能描述

通过“系统防火墙”界面的功能，您可以查看和修改防火墙规则，包括：

- IP 地址防火墙规则。
- 端口防火墙规则。
- MAC 防火墙规则。

界面展示

在导航栏中选择“CMC 设置>系统防火墙”，打开如下[图 3-30](#)、[图 3-31](#)、[图 3-32](#)、[图 3-33](#)所示界面。

图 3-30 系统防火墙



图 3-31 添加 IP 规则

添加 IP 规则



(单个/范围) IP 开始

IP 范围结束

启用超时

规则

 保存

图 3-32 添加 MAC 规则

添加 MAC 规则



单个MAC

启用超时

规则

 保存

图 3-33 添加端口规则

添加端口规则

单个/范围 端口开始

端口范围结束

协议

网络类型

启用超时

规则

保存

参数说明

表 3-37 系统防火墙

参数	描述
现有IP规则	显示现有IP规则。
添加新的IP规则	添加新的IP规则，需指定如下参数： <ul style="list-style-type: none">● IP 开始。● IP 范围结束。● 启用超时：

参数	描述
	<ul style="list-style-type: none"> a. 不勾选，立即生效且一直有效。 b. 勾选，需指定起止时间日期，在设定期间规则有效。 <ul style="list-style-type: none"> ● 规则：允许或阻挡。
当前的端口规则	显示当前的端口规则。
添加新的端口规则	添加新的端口规则，需指定如下参数： <ul style="list-style-type: none"> ● 单个/范围 端口开始。 ● 端口范围结束。 ● 协议：TCP、UDP 或 Both。 ● 网络类型：IPv4、IPv6 或 Both。 ● 启用超时： <ul style="list-style-type: none"> a. 不勾选，立即生效且一直有效。 b. 勾选，需指定起止时间日期，在设定期间规则有效。 ● 规则：允许或阻挡。
现有MAC规则	显示现有MAC规则。
添加新的MAC规则	添加新的MAC规则，需指定如下参数： <ul style="list-style-type: none"> ● 单个 MAC。 ● 启用超时： <ul style="list-style-type: none"> a. 不勾选，立即生效且一直有效。 b. 勾选，需指定起止时间日期，在设定期间规则有效。 ● 规则：允许或阻挡。

3.8.5 日期&时间

功能描述

通过“日期&时间”界面的功能，您可以查询和设置：

- CMC 系统时区。
- NTP 信息。

CMC 时间同步规则如下：

- CMC 运行后，CMC 会给 ME 发送请求获取系统 RTC 时间。
- 如果启用 NTP，并且 NTP 服务器是通的，则 CMC 将按照时间同步设置周期与 NTP 服务器同步时间。

界面展示

在导航栏中选择“CMC 设置>日期&时间”，打开如下[图 3-34](#)所示界面。

图 3-34 日期&时间

日期 & 时间 主页 > 日期 & 时间

CMC 日期 & 时间

Aug 27, 2000 11:57:19 AM (GMT+08:00 CST) - Asia/Shanghai

配置日期 & 时间

请选择时区

NTP 自动刷新日期 & 时间 NTP DHCP4 刷新日期 & 时间 NTP DHCP6 刷新日期 & 时间

NTP 服务器 1: pool.ntp.org

NTP 服务器 2: time.nist.gov

NTP 服务器 3: NTP 服务器名称

NTP 服务器 4: NTP 服务器名称

NTP 服务器 5: NTP 服务器名称

NTP 服务器 6: NTP 服务器名称

保存

时间同步设置

同步周期: 60

最大跳变时间: 5

保存

参数说明

表 3-38 日期&时间

参数	描述
CMC日期&时间	显示CMC日期&时间。
配置日期&时间	选择时区。 选择NTP刷新日期和时间的模式，可选为： <ul style="list-style-type: none">● NTP 自动刷新日期&时间。● NTP DHCP4 刷新日期&时间。● NTP DHCP6 刷新日期&时间。 填写NTP服务器地址。
时间同步设置	同步周期（最小值5分钟,最大值1440分钟）。 跳变时间(最小值1分钟，最大值60分钟)。

3.8.6 SSL 设置

功能描述

SSL 证书通过在客户端浏览器和 Web 服务器之间建立一条 SSL 安全通道（访问方式为 HTTPS），实现数据信息在客户端和服务端之间的加密传输，可以防止数据信息的泄漏。SSL 保证了双方传递信息的安全性，而且用户可以通过服务器证书验证所访问的网站是否可靠。产品支持 SSL 证书替换功能，为提高安全性，建议替换成自己的证书和公私钥对，并及时更新证书，保证证书的有效性。

通过“SSL 设置”界面的功能，您可以：

- 查看 SSL 认证。
- 产生 SSL 认证。
- 上传 SSL 认证。

界面展示

在导航栏中选择“CMC 设置>SSL 设置”，打开如下[图 3-35](#)、[图 3-36](#)、[图 3-37](#)、[图 3-38](#)所示界面。

图 3-35 SSL 设置



图 3-36 查看 SSL 凭证

查看 SSL 凭证

当前凭证信息 ?

凭证版本
3

序号
5ADE171D

签名机制
sha256WithRSAEncryption

公钥
(2048 bit)

发出的通用名称 (CN)
www.ami.com

发出的组织 (O)
American Megatrends Incorporated

发出的组织单位 (OU)
Service Processors

发出的城市或地点 (L)
Norcross

发出的州或省 (ST)
Georgia

发出的国家 (C)
US

发出的电子邮件地址
support@ami.com

有效自
Apr 23 17:25:49 2018 GMT

有效至
Jun 22 17:25:49 2037 GMT

发出给通用名称 (CN)
www.ami.com

发出的组织 (O)
American Megatrends Incorporated

发出的组织单位 (OU)
Service Processors

发出的城市或地点 (L)
Norcross

发出的州或省 (ST)
Georgia

发出的国家 (C)
US

发出的电子邮件地址
support@ami.com

图 3-37 生成 SSL 凭证

生成 SSL 凭证

通用名称(CN)

组织(O)

组织单位(OU)

城市或地点(L)

州或省(ST)

国家(C)

电子邮件地址

有效自

密钥长度

 保存

图 3-38 上传 SSL 凭证

上传 SSL 凭证

当前凭证
Thu Mar 25 02:00:29 2021

新凭证

当前私钥
Thu Mar 25 02:00:29 2021

新的私钥

保存

参数说明

表 3-39 SSL 设置

参数	描述
通用名称	通用名称
组织	组织
组织单位	组织单位
城市或地点	城市或地点
州或省	州或省
国家	国家
电子邮件地址	电子邮件地址
有效自	有效自
密钥长度	密钥长度

3.8.7 BMC IP 设置

功能描述

通过“BMC IP 设置”界面的功能，您可以设置 BMC IPv4 IP。

界面展示

在导航栏中选择“CMC 设置>BMC IP 设置”，打开如下图 3-39 所示界面。

图 3-39 BMC IP 设置

编号	IP
1	不可用
2	100.3.8.29
3	不可用
4	不可用
5	不可用
6	不可用
7	100.3.8.33
8	不可用

参数说明

表 3-40 BMC IP 设置

参数	描述
编号	显示节点编号。
IP	显示节点IP。
起始刀片	设置起始刀片编号。
数量	设置IP的刀片数量。
网络模式	网络模式，包括：

参数	描述
	<ul style="list-style-type: none"> ● 静态 ● DHCP
起始IP	设置起始刀片的IP。 按照数量，其他刀片的IP依次顺延。
子网掩码	子网掩码。
网关	网关。

3.8.8 多机箱 CMC IP 设置

功能描述

通过“多机箱 CMC IP 设置”界面的功能，您可以添加和删除多机箱 CMC IP。被添加的 CMC IP 机箱，可以在刀片模块、刀片版本信息，系统信息，电源模块、FRU、风扇模块页面进行信息的查看和配置。

界面展示

在导航栏中选择“CMC 设置>多机箱 CMC IP 设置”，打开如下图 3-40 所示界面。

图 3-40 多机箱 CMC IP 设置



参数说明

表 3-41 多机箱 CMC IP 设置

参数	描述
增加机箱 CMC IP	添加被管理的 CMC IP 信息。
当前已设置的机箱 CMC IP 列表	显示当前已添加的 CMC IP 列表。

3.8.9 备份配置

功能描述

通过“备份配置”界面的功能，您可以对现有系统的各项配置进行备份并下载备份的配置文件到本地。

界面展示

在导航栏中选择“CMC 设置>备份配置”，打开如下[图 3-41](#)所示界面。

图 3-41 备份配置



参数说明

表 3-42 备份配置

参数	描述
SNMP	备份SNMP相关配置信息。
网络&服务	备份网络&服务相关配置信息。
IPMI	备份IPMI相关配置信息。
NTP	备份NTP相关配置信息。
验证	备份验证相关配置信息。
SYSLOG	备份Syslog相关配置信息。

3.8.10 还原配置

功能描述

通过“还原配置”界面的功能，您可以对现有系统的各项配置进行还原。

界面展示

在导航栏中选择“CMC 设置>还原配置”，打开如下图 3-42 所示界面。

图 3-42 还原配置



参数说明

表 3-43 还原配置

参数	描述
配置文件	浏览选择本地备份好的配置文件对当前系统配置进行还原。

3.9 故障诊断

诊断工具提供了对 CMC 或主机系统进行检查和验证的能力，以检查是否有某些功能失效或无法正常工作。

3.9.1 模块重启

功能描述

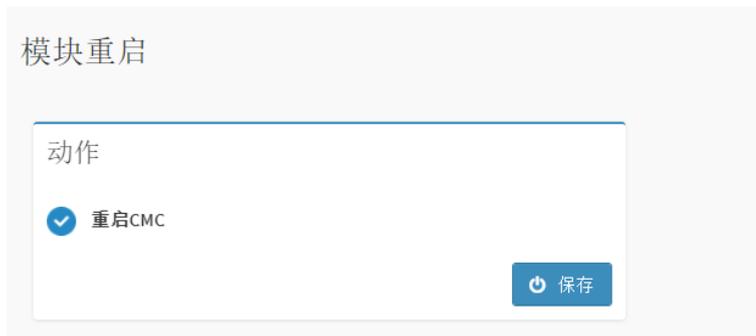
通过“模块重启”界面的功能，您可以：

- 重启 CMC。

界面展示

在导航栏中选择“故障诊断>模块重启”，打开如下[图 3-43](#)所示界面。

图 3-43 模块重启



参数说明

表 3-44 模块重启

参数	描述
重启CMC	重启CMC。

3.10 系统维护

3.10.1 HPM 固件更新

功能描述

通过“HPM 固件更新”界面的功能，您可以进行 HPM 固件更新，可更新 CMC、BIOS、BMC、CPLD、PSU。CMC 包含两个 64M 的闪存，每个闪存上存储了一个 64M 的固件镜像，CMC 支持双镜像升级。支持的升级模式包含 Web 更新和 YafuFlash 更新。升级时可选择保留配置升级和不保留配置升级。HPM 固件更新更安全，提供防错刷机制。

以下示例为 CMC 更新、BMC 更新、BIOS 更新、CPLD 更新过程详细步骤。

3.10.1.1 CMC 更新过程步骤

1. 用户登录到 Web GUI，进入“系统维护>HPM 固件更新”页面，选择 CMC 镜像文件。

图 3-44 选择镜像文件



表 3-45 选择镜像文件参数

选项	含义
本地	选择本地镜像。
远程	选择远程镜像。（protocol:nfs/sftp/scp. nfs has no username and password, use NA by default）

2. 点击解析文件。

图 3-45 解析文件



- 文件解析后，会显示对应的组件名称以及上传版本，确认无误后，选择是否保留配置、是否异步更新，点击上传镜像，等到校验成功以及上传进度 100%。

图 3-46 镜像校验

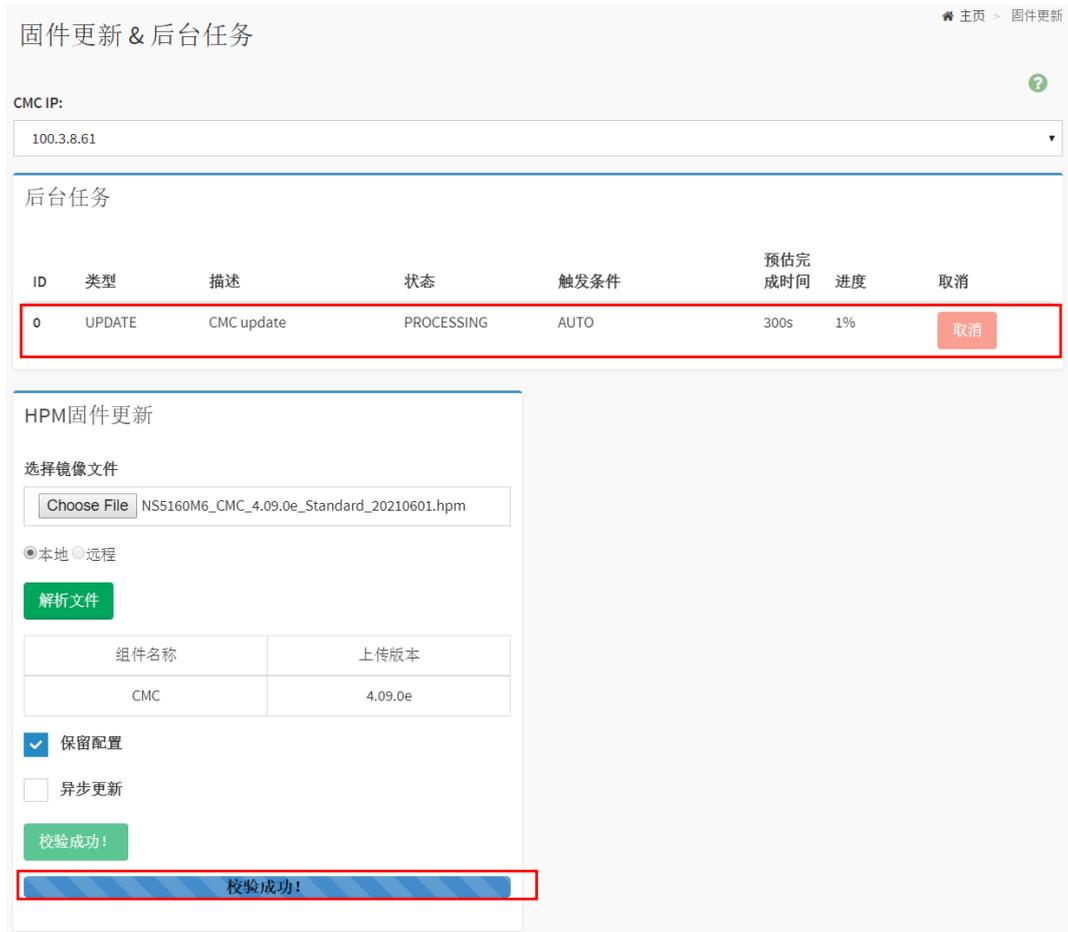


表 3-46 升级选项参数

选项	含义
保留配置	勾选：SDR、FRU、SEL策略设置、IPMI、网络配置、NTP、SNMP Set/Get设置、SSH、KVM、认证、系统日志Syslog设置、Web、Extlog以及Redfish的BIOS配置会被保存。 不勾选：所有配置信息会被恢复成出厂设置。
异步更新	勾选：升级完成后CMC暂不自动重启，等到下次手动重启之后才会切换到新的镜像版本，同时另外一个镜像版本也会被同步到最新版本。 不勾选：刷新完成后，CMC立即重启。重启之后切换到新的镜像版本，同时另外一个镜像也同步更新到最新版本。

4. 镜像上传成功会自动进入后台任务，进行更新。可在后台任务栏查看进度以及预估完成时间。等到进度 100%即为刷新成功。

图 3-47 上传镜像&自动刷新



5. 待到 CMC 重启后，查看 CMC 固件版本。重新登陆 CMC Web，检查页面左上角固件版本信息。如果升级的是 BMC、BIOS、CPLD 等，需要在“信息>刀片版本信息”页面查看对应刀片版本信息。

图 3-48 查看固件版本



3.10.1.2 BMC 更新过程步骤

1. 用户登录到 Web GUI，进入“系统维护>HPM 固件更新”页面，选择 BMC 镜像文件。

图 3-49 选择镜像文件



表 3-47 选择镜像文件参数

选项	含义
本地	选择本地镜像。
远程	选择远程镜像。 Protocol:nfs/sftp/scp. nfs没有用户名和密码，使用NA Protocol://username:password@ip/directory

2. 点击解析文件。

图 3-50 解析文件



3. 文件解析后，会显示对应的组件名称以及上传版本，确认无误后，选中待升级的 BMC 节点编号，选择是否保留配置、是否异步更新，点击上传镜像，等到校验成功。

图 3-51 选择待升级节点

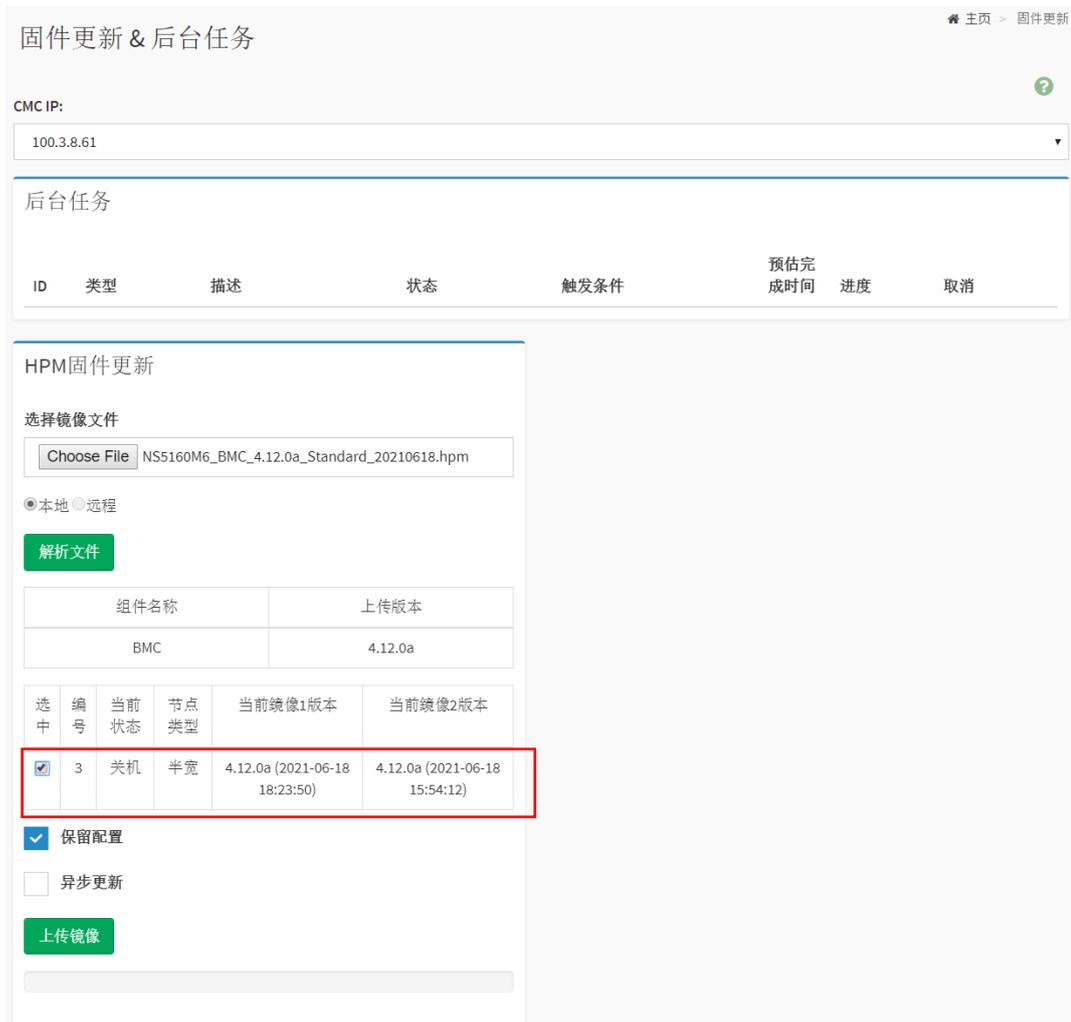


表 3-48 升级选项参数

选项	含义
保留配置	勾选：SDR、FRU、SEL策略设置、IPMI、网络配置、NTP、SNMP Set/Get设置、SSH、KVM、认证、系统日志Syslog设置、Web、Extlog以及Redfish的BIOS配置会被保存。 不勾选：所有配置信息会被恢复成出厂设置。
异步更新	勾选：升级完成后BMC暂不自动重启，等到下次手动重启之后才会切换到新的镜像版本，同时另外一个镜像版本也会被同步到最新版本。 不勾选：刷新完成后，BMC立即重启。重启之后切换到新的镜像版本，同时另外一个镜像也同步更新到最新版本。

4. 镜像上传成功会自动进入后台任务，进行更新。可在后台进度栏查看进度。等到进度100%即为刷新成功。

图 3-52 上传镜像&自动刷新

刷新进度

编号	刷新进度
3	刷新完成

HPM固件更新

选择镜像文件

Choose File NS5160M6_BMC_4.12.0a_Standard_20210618.hpm

本地 远程

解析文件

组件名称	上传版本
BMC	4.12.0a

选中	编号	当前状态	节点类型	当前镜像1版本	当前镜像2版本
<input checked="" type="checkbox"/>	3	关机	半宽	4.12.0a (2021-06-18 18:23:50)	4.12.0a (2021-06-18 15:54:12)

保留配置

异步更新

刷新完成

刷新完成

校验结果

编号	校验结果
3	校验通过

- 待 BMC 重启后，查看 BMC 固件版本。重新登陆 CMC Web，进入“信息>刀片版本信息”页面，查看对应刀片版本信息。

图 3-53 查看固件版本

刀片版本信息

主页 > 刀片版本信息

CMC IP: 100.3.8.61

编号	BMC镜像1版本	BMC镜像2版本	BIOS版本	CPLD版本
1	不可用	不可用	不可用	不可用
2	不可用	不可用	不可用	不可用
3	4.12.0a (2021-06-18 18:23:50)	4.12.0a (2021-06-18 18:23:50)	05.00.00 (05/07/2021 14:18:22)	2.3
4	不可用	不可用	不可用	不可用

3.10.1.3 BIOS 更新过程步骤

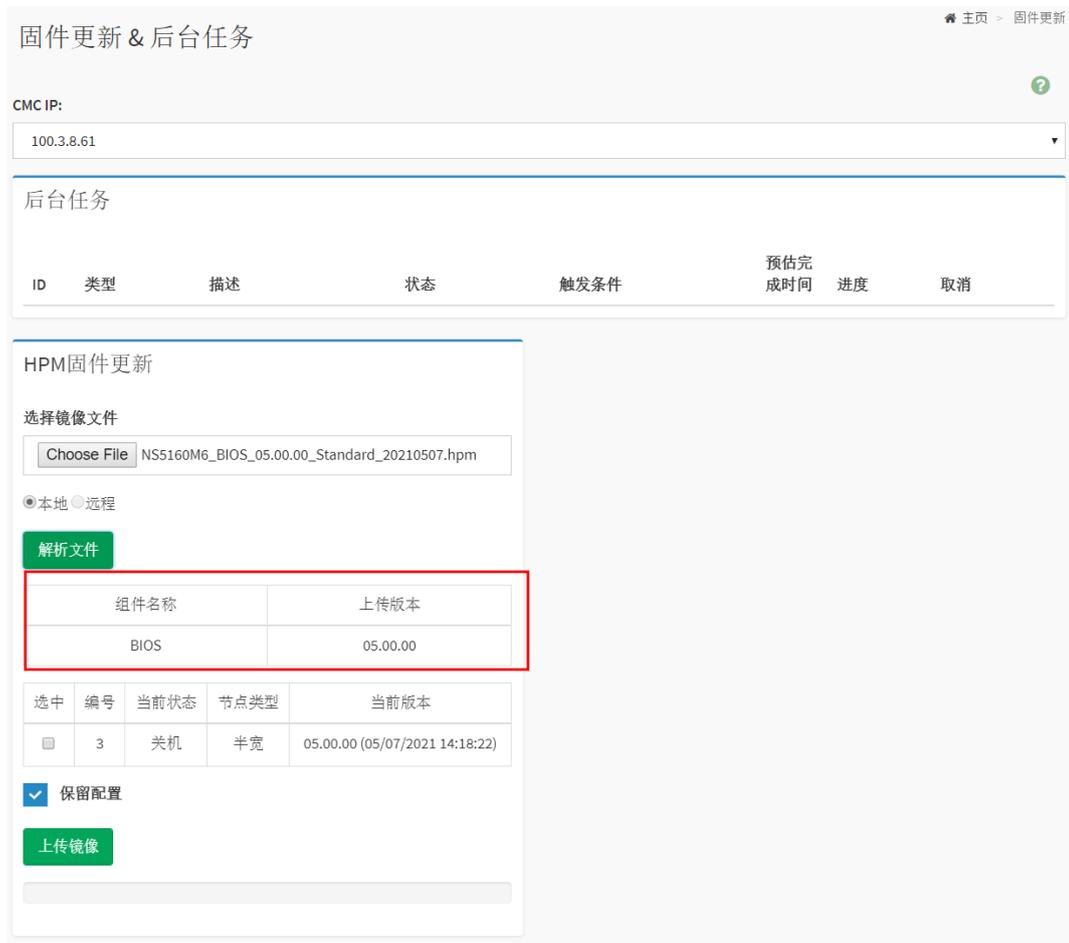
1. 用户登录到 Web GUI，进入“系统维护>HPM 固件更新”页面，选择 BIOS 镜像文件。

图 3-54 BIOS 更新_选择镜像文件



2. 点击解析文件，并选择是否保留配置。

图 3-55 BIOS 更新_解析文件



3. 文件解析后，会显示对应的组件名称以及上传版本，确认无误后，选中待升级的 BMC 节点编号，选择是否保留配置，点击上传镜像，等到校验成功。

图 3-56 BIOS 更新_镜像校验

刷新进度

编号	刷新进度
3	0%

HPM固件更新

选择镜像文件

Choose File NS5160M6_BIOS_05.00.00_Standard_20210507.hpm

本地 远程

解析文件

组件名称	上传版本
BIOS	05.00.00

选中	编号	当前状态	节点类型	当前版本
<input checked="" type="checkbox"/>	3	关机	半宽	05.00.00 (05/07/2021 14:18:22)

保留配置

开始刷新...

开始刷新...

校验结果

编号	校验结果
3	校验通过

4. 镜像上传成功会自动进入后台任务，进行更新。可在进度栏查看进度。等到进度 100% 即为刷新成功。

注意

BIOS 更新的触发条件为 power off，如果当前电源状态为 power on，则不会触发，需要 power off 触发，可使用 ipmitool power off 命令关闭电源后，自动触发。建议升级 BIOS 前先关闭电源。

图 3-57 BIOS 更新_更新完成

刷新进度

编号	刷新进度
3	刷新完成

HPM固件更新

选择镜像文件

Choose File NS5160M6_BIOS_05.00.00_Standard_20210507.hpm

本地 远程

解析文件

组件名称	上传版本
BIOS	05.00.00

选中	编号	当前状态	节点类型	当前版本
<input checked="" type="checkbox"/>	3	关机	半宽	05.00.00 (05/07/2021 14:18:22)

保留配置

刷新完成

刷新完成

校验结果

编号	校验结果
3	校验通过

5. 待到系统重启后，查看 BIOS 固件版本。重新登陆 CMC Web，进入“信息>刀片版本信息”页面，查看对应刀片版本信息。

图 3-58 BIOS 更新_版本检查

刀片版本信息 主页 > 刀片版本信息

CMC IP: 100.3.8.61

编号	BMC镜像1版本	BMC镜像2版本	BIOS版本	CPLD版本
1	不可用	不可用	不可用	不可用
2	不可用	不可用	不可用	不可用
3	4.12.0a (2021-06-18 18:23:50)	4.12.0a (2021-06-18 18:23:50)	05.00.00 (05/07/2021 14:18:22)	2.3
4	不可用	不可用	不可用	不可用

3.10.1.4 CPLD 更新过程步骤

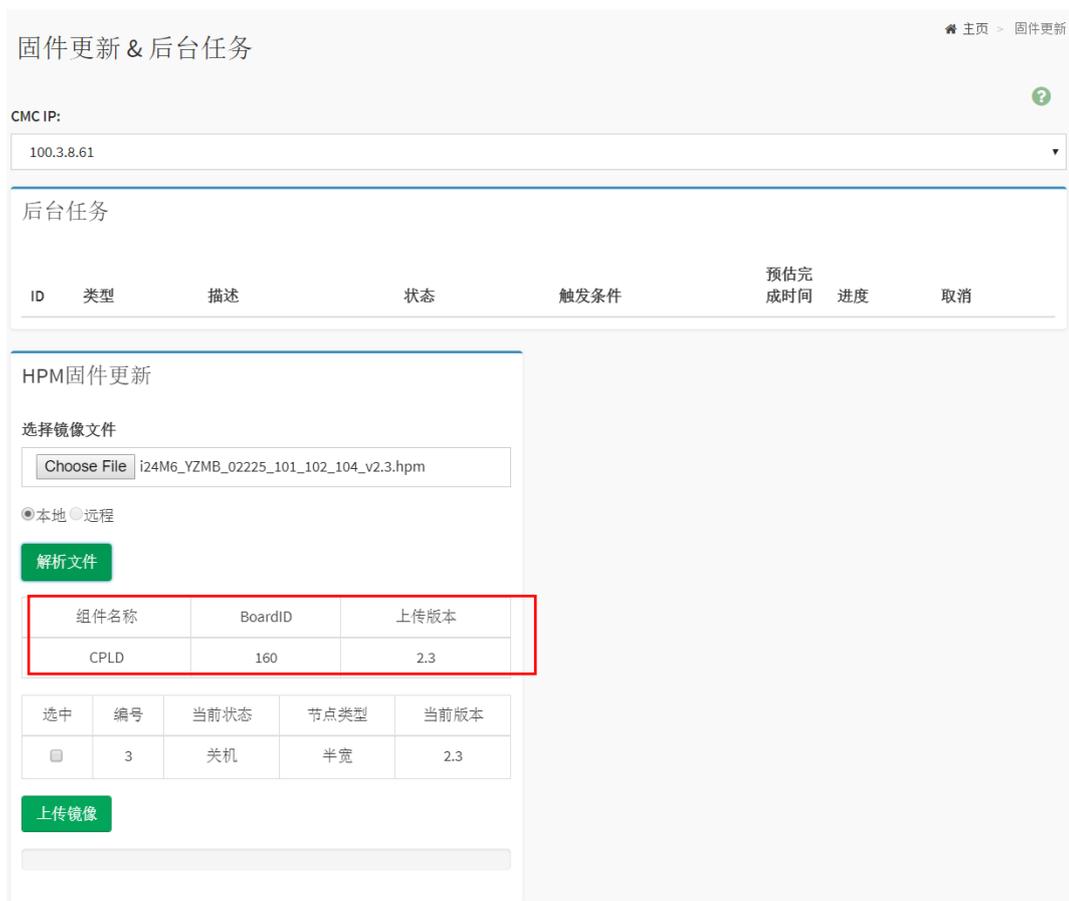
1. 用户登录到 Web GUI，进入“系统维护>HPM 固件更新”页面，选择 CPLD 镜像文件。

图 3-59 CPLD 更新_选择镜像文件



2. 点击解析文件，文件解析后，会显示对应的组件名称以及上传版本，确认无误后，点击上传镜像，等到校验成功。

图 3-60 CPLD 更新_解析文件



- 选中待刷新节点，点击上传镜像，等到校验成功以及上传进度 100%。

图 3-61 CPLD_选择待更新节点，点击上传镜像

刷新进度

编号	刷新进度
3	0%

HPM固件更新

选择镜像文件

Choose File i24M6_YZMB_02225_101_102_104_v2.3.hpm

本地 远程

解析文件

组件名称	BoardID	上传版本
CPLD	160	2.3

选中	编号	当前状态	节点类型	当前版本
<input checked="" type="checkbox"/>	3	关机	半宽	2.3

开始刷新...

开始刷新...

校验结果

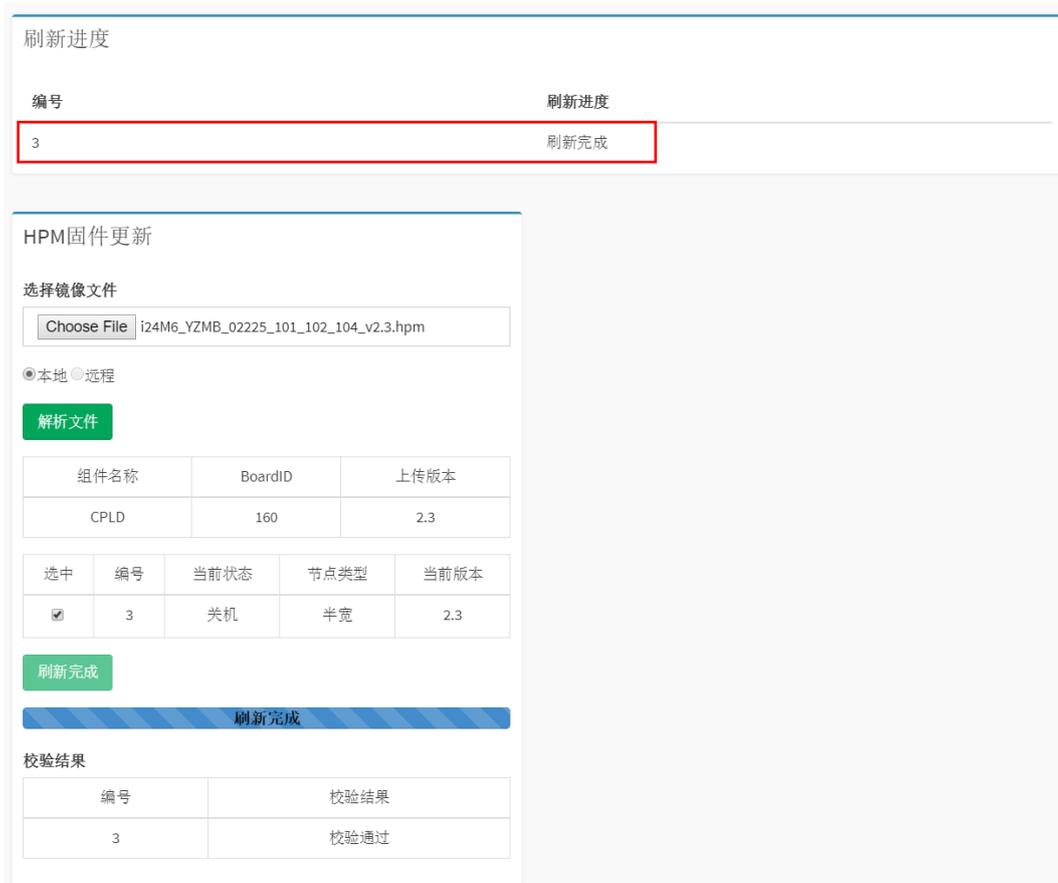
编号	校验结果
3	校验通过

4. 镜像上传成功会自动进入后台任务，进行更新。可在进度栏查看进度。等到进度 100% 即为刷新成功。

 注意

CPLD 更新的触发条件为 power off，如果当前电源状态为 power on，则不会触发，需要 power off 触发，可使用 ipmitool power off 命令关闭电源后，自动触发。建议升级 CPLD 前先关闭电源。

图 3-62 CPLD 更新完成



5. 重新登陆 CMC Web，进入“信息>刀片版本信息”页面，查看对应刀片版本信息。

图 3-63 CPLD 更新_版本检查



3.10.2 固件镜像位置

功能描述

通过“固件镜像位置”界面的功能，您可以选择将固件镜像传送到 CMC 时使用的协议，包含在网页更新期间刷新 TFTP 服务器。

界面展示

在导航栏中选择“系统维护>固件镜像位置”，打开如下图 3-64 所示界面。

图 3-64 固件镜像位置



参数说明

表 3-49 固件镜像位置

参数	描述
在网页更新期间刷新	在网页更新期间刷新。
TFTP服务器	选择TFTP服务器，固件镜像被上传到TFTP服务器。 选择TFTP服务器时，需指定TFTP服务器地址、TFTP镜像名称和TFTP重试次数。

3.10.3 固件信息

功能描述

通过“固件信息”界面的功能，您可以查看 CMC 固件信息，包括：活动中的镜像 ID、创建日期、创建时间和固件版本。

界面展示

在导航栏中选择“系统维护>固件信息”，打开如下图 3-65 所示界面。

图 3-65 固件信息



参数说明

表 3-50 固件信息

参数	描述
活动中的镜像ID	当前使用的CMC镜像ID。
创建日期	CMC镜像创建日期。
创建时间	CMC镜像创建时间。
固件版本	CMC镜像固件版本。

3.10.4 恢复出厂设置

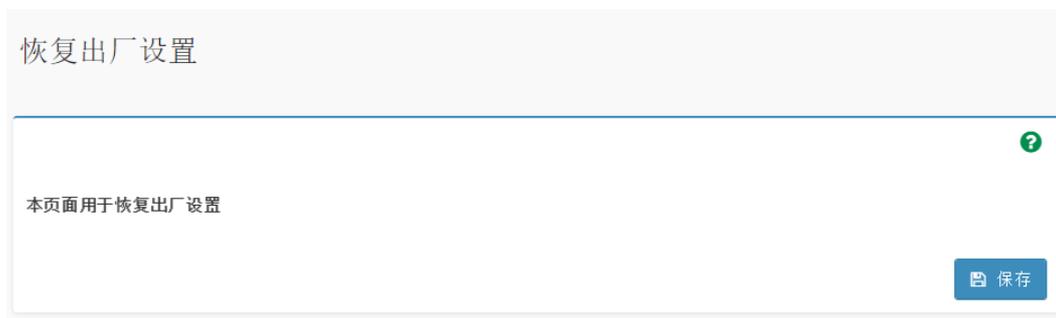
功能描述

通过“恢复出厂设置”界面的功能，您可以恢复 CMC 出厂设置。

界面展示

在导航栏中选择“系统维护>恢复出厂设置”，打开如下图 3-66 所示界面。

图 3-66 恢复出厂设置



参数说明

表 3-51 恢复出厂设置

参数	描述
保存	点击保存按钮可恢复到出厂设置。



恢复出厂设置后，用户的配置信息将丢失，请您谨慎操作。

4 Smashclp CLI 命令行功能介绍

4.1 命令行说明

4.1.1 命令行介绍

Smashclp CLI 命令行功能主要支持以下命令：

表 4-1 命令行功能

命令名称	功能概述
cmclg	获取与清除CMC的SEL日志。
chassis	对服务器机箱电源和UID灯的状态进行查询与控制。
mc	对管理控制器的状态进行查询与控制。
diagnose	各种诊断工具。

4.1.2 命令行格式说明

命令行一般为命令字再加一个或者几个命令选项，其格式一般如下：

command [<option1>] [<option2>] ...

表 4-2 命令行格式

格式	意义
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
<option>	表示从提供的参数范围中选取一个。
<x y ...>	表示从两个或多个选项中选取一个。

4.1.3 帮助信息

CLI 支持帮助信息，一种是显示命令列表，另外一种显示命令的详细帮助信息。

使用 help 命令查看命令列表：

```
/smashclp> help
Built-in command:
-----
```

```
cmclog : get or set cmclog parameters, please enter <cmclog --help> for
more information
chassis : get or set chassis parameters, please enter <chassis --help> for more
information
mc : get or set mc parameters, please enter <mc --help> for more
information
ipconfig: get or set network parameters, please enter <ipconfig --help> for
more information
service : get or set service parameters, please enter <service --help> for more
information
syscmd : get or set syscmd parameters, please enter <syscmd --help> for
more information
diagnose: CMC diagnose function, please enter <diagnose --help> for more
information
exit : exit the command line
```

在具体命令后面添加--help 查看该命令的详细信息，bmclog 的帮助信息示例如下：

```
/smashclp> cmclog --help
cmclog commands:
  cmclog <option1> [option2]
  option1:
    --help          show help information
    ?              show help information
    --get           get bmc log
    --set           set bmc log
  option2:
    sel [clear]    get SEL or clear SEL
```

在具体命令后面添加--help 查看该命令的详细信息，netstat 的帮助信息示例如下：

```
/smashclp> diagnose netstat --help
BusyBox v1.21.1 (2021-04-01 09:46:39 CST) multi-call binary.

Usage: netstat [-ral] [-tuwx] [-en]

Display networking information

-r  Routing table
-a  All sockets
-l  Listening sockets
    Else: connected sockets
-t  TCP sockets
-u  UDP sockets
-w  Raw sockets
-x  Unix sockets
```

```
Else: all socket types
-e Other/more information
-n Don't resolve names
```

4.2 登录与退出

4.2.1 登录 Smashclp CLI

用户可以通过 SSH 登录 CMC 并进入 Smash-Lite CLI。登录后，即可进入命令行操作界面。请使用 CMC 系统的用户名密码进行登录。

```
root@desktop:~# ssh admin@100.3.8.36
The authenticity of host '100.3.8.36 (100.3.8.36)' can't be established.
RSA key fingerprint is e6:eb:b1:3e:d0:b6:0a:43:ba:28:38:60:72:9e:66:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '100.3.8.36' (RSA) to the list of known hosts.
admin@100.3.8.36's password:

>> smashclp <<
////////////////////////////////////
smashclp cli tool version 1.0
Enter 'help' for a list of built-in commands
////////////////////////////////////

/smashclp>
```

4.2.2 退出 Smashclp CLI

使用 exit 命令退出登录 Smashclp CLI。

```
/smashclp> exit
Connection to 100.3.8.36 closed.
```

4.3 cmclog 命令

4.3.1 查询与清除 SEL 日志

命令功能：

sel 命令用来进行 SEL 日志的查询与清除。

命令格式：

```
cmclog --get sel
```

```
cmclog -set sel clear
```

参数说明：

无

使用指南：

无

使用示例：

#查询 SEL 日志。

```
/smashclp> cmclog --get sel
ID   |RecordTy |TimeS      |GenID   |EvmRev  |SensorT |Sensor# |Evt DT
|Data1  |Data2    |Data3
119  |0x02     |0x386ea48e |0x20    |0x04    |0x15    |0x35    |0x08
|0x01   |0000     |0000
118  |0x02     |0x386ea336 |0x20    |0x04    |0x28    |0x3d    |0xef
|0x03   |0000     |0000
117  |0x02     |0x386ea336 |0x20    |0x04    |0x15    |0x35    |0x88
|0x01   |0000     |0000
116  |0x02     |0x386ea090 |0x20    |0x04    |0x28    |0x3d    |0x6f
|0x03   |0000     |0000
```

#删除 SEL 日志，删除后再次查询会看到只有一条日志（记录删除操作）。

```
/smashclp> cmclog --set sel clear
/smeshclp> cmclog --get sel
ID   |RecordTy |TimeS      |GenID   |EvmRev  |SensorT |Sensor# |Evt DT
|Data1  |Data2    |Data3
1    |0x02     |0x60563d6a |0x20    |0x04    |0x10    |0x6f    |0x6f
|0x02   |0xff     |0xff
```

4.4 chassis 命令

4.4.1 查询与控制 UID 灯状态

命令功能：

identify 命令用来进行 UID 灯状态的查询与控制。

命令格式：

chassis --get identify status

chassis -set identify <force | value>

参数说明：

表 4-3 参数说明

参数	参数说明	取值
force	表示永久点亮UID指示灯。	无
value	表示UID指示灯闪烁时长。	数据类型为整型，单位是秒。取值范围为0~240。取值为0时，表示关闭该指示灯。

使用指南：

无

使用示例：

#查询 UID 灯状态。

```
/smashclp> chassis identify status  
The UID status is off
```

#永久点亮 UID 指示灯。

```
/smashclp> chassis --set identify force  
Identify UID successfully.
```

#打开 UID 指示灯 15 秒。

```
/smashclp> chassis --set Didentify 15  
Identify UID successfully.
```

4.5 mc 命令

4.5.1 获取 CMC 系统版本

命令功能：

用来显示当前 CMC 系统的版本。

命令格式：

mc -get version

参数说明：

无

使用指南：

无

使用示例：

#获取 CMC 系统版本。

```
/smashclp> mc --get version
Device ID           : 32
Device Revision     : 1
Firmware Revision   : 4.09.0b
IPMI Version        : 2.0
```

4.5.2 服务重启功能

命令功能：

用来对 CMC 系统或者 CMC 系统内的服务进行重启。

命令格式：

mc -set <servicename> reset

参数说明：

表 4-4 参数说明

参数	参数说明	取值
servicename	服务名称	bmc web

使用指南：

无

使用示例：

#重启 CMC 的 Web 模块。

```
/smashclp> mc --set web reset  
Web reset OK!
```

#重启 CMC 系统。

```
/smashclp> mc --set bmc reset  
  
Broadcast message from sysadmin@ProductSN (Mon Apr 13 21:56:13 2020):  
  
The system is going down for reboot NOW!  
MC reset OK!
```

4.5.3 恢复出厂设置

命令功能：

用来恢复出厂设置，执行完成后 CMC 系统会重启。

命令格式：

```
mc --set factorydefaults restore
```

参数说明：

无

使用指南：

无

使用示例：

#恢复出厂设置。

```
/smashclp> mc --set factorydefaults restore  
/smashclp>
```

4.5.4 双镜像启动配置

命令功能：

用来显示和修改当前 CMC 系统的双镜像启动配置。

命令格式：

```
mc --get dualimgconf
```

```
mc --set dualimgconf [boot_number]
```

参数说明：

表 4-5 参数说明

参数	参数说明	取值
boot_number	从哪个镜像启动	0: Higher firmware version 1: IMAGE-1 2: IMAGE-2 3: Lower firmware version 4: Newest updated firmware 5: Not newest updated firmware

使用指南：

无

使用示例：

#获取 CMC 系统的当前双镜像启动配置。

```
/smashclp> mc --get dualimgconf  
Current active image: Image2  
Current active image version: 4.9.11  
Current standby image: Image1  
Current standby image version: 4.9.11
```

#设置 CMC 系统以版本较高的版本启动。

```
/smashclp> mc --set dualimgconf 0  
Setting dual image configuration OK! The specified boot image is Higher  
firmware version
```

```
Set bmc boot image OK!
```

4.6 diagnose 命令

4.6.1 列出日志文件属性

命令功能：

用来显示某目录下的日志目录或者文件信息，使用的是 Linux 系统的 ls 命令。

命令格式：

```
diagnose ls <logfile>
```

参数说明：

表 4-6 参数说明

参数	参数说明	取值
logfile	日志文件	<ul style="list-style-type: none">● ncml bmc service configuration● log bmc system log● versioninfo bmc version info● crontab bmc crontab file

使用指南：

无

使用示例：

#显示 log 目录信息。

```
/smashclp> diagnose ls log
BMC1            audit.log        debug.log        idl.log
inspur_debug.log    notice.log      warning.log
alert.log        crit.log        err.log          info.log
maintenance.log    notice.log.1    warning.log.1
archive            crit.log.1      err.log.1        info.log.1
maintenance.log.1    psuFaultHistory.log
```

4.6.2 查看日志文件内容

命令功能：

用来显示某个日志文件的具体内容，使用的是 Linux 系统的 cat 命令。

命令格式：

```
diagnose cat <logfile>
```

参数说明：

表 4-7 参数说明

参数	参数说明	取值	
logfile	日志文件	ncml	bmc service configuration
		log	bmc system log
		versioninfo	bmc version info
		crontab	bmc crontab file

使用指南：

无

使用示例：

```
#列出 crit 日志文件的内容 crit.log
```

```
/smashclp> diagnose cat log crit.log
<130> 2000-01-04T04:59:20.750000+08:00 ProductSN inspurn_monitor_app:
[21863 : 22001 CRITICAL][libipmi_XportDevice.c:690]LIBIPMI_HL_GetIPv4Source:
Error getting LAN configuration for channel 8
<130> 2000-01-04T04:59:20.750000+08:00 ProductSN inspurn_monitor_app:
[21863 : 22001 CRITICAL][libipmi_XportDevice.c:1699]LIBIPMI, Error getting IPv4
Address Source::1cc
<130> 2000-01-04T04:59:21.040000+08:00 ProductSN inspurn_monitor_app:
[21863 : 22001 CRITICAL][libipmi_XportDevice.c:690]LIBIPMI_HL_GetIPv4Source:
Error getting LAN configuration for channel 8
<130> 2000-01-04T04:59:21.040000+08:00 ProductSN inspurn_monitor_app:
[21863 : 22001 CRITICAL][libipmi_XportDevice.c:1699]LIBIPMI, Error getting IPv4
Address Source::1cc
```

```
<130> 2000-01-04T04:59:42.370000+08:00 ProductSN inspur_monitor_app:
[21863 : 22001 CRITICAL][libipmi_XportDevice.c:690]LIBIPMI_HL_GetIPv4Source:
Error getting LAN configuration for channel 8
```

4.6.3 查看最近登录的用户(last)

命令功能：

用来显示当前 CMC 系统的最近登录的用户，使用的是 Linux 系统的 last 命令。

命令格式：

```
diagnose last
```

参数说明：

无

使用指南：

无

使用示例：

#显示 CMC 系统的最近登录用户。

```
/smashclp> diagnose last
admin pts/0 100.2.54.244 Tue Jan 4 04:45 still logged in
reboot system boot 3.14.17-ami Sat Jan 1 08:01 - 05:02 (2+21:00)

wtmp begins Sat Jan 1 08:01:44 2000
```

4.6.4 查看和设置网络设备 (Ifconfig)

命令功能：

用来显示和设置当前 CMC 系统的网络设备，使用的是 Linux 系统的 ifconfig 命令。

命令格式：

```
diagnose ifconfig [interface]
```

参数说明：

表 4-8 参数说明

参数	参数说明	取值
interface	物理网络接口	eth0

使用指南：

无

使用示例：

#列出所有网络设备的信息。

```
/smashclp> diagnose ifconfig
eth0      Link encap:Ethernet  HWaddr B4:05:5D:1D:D1:0E
          inet addr:100.3.8.36  Bcast:100.3.8.255  Mask:255.255.255.0
          inet6 addr: fe80::b605:5dff:fe1d:d10e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34875550 errors:0 dropped:99086 overruns:0 frame:0
          TX packets:350128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2220670735 (2.0 GiB)  TX bytes:144103858 (137.4 MiB)
          Interrupt:2

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:13080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13080 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2100858 (2.0 MiB)  TX bytes:2100858 (2.0 MiB)
```

4.6.5 查看和设置网卡参数 (ethtool)

命令功能：

用来显示和设置当前 CMC 系统的网卡参数，使用的是 Linux 系统的 ethtool 命令。

命令格式：

```
diagnose ethtool <interface>
```

参数说明：

表 4-9 参数说明

参数	参数说明	取值
interface	物理网络接口	eth0

使用指南：

无

使用示例：

#列出网卡 eth0 的参数。

```
/smashclp> diagnose ethtool eth0
Settings for eth0:
  Supported ports: [ TP MII ]
  Supported link modes:   10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
  Supported pause frame use: Symmetric
  Supports auto-negotiation: Yes
  Advertised link modes:  10baseT/Half 10baseT/Full
  Advertised pause frame use: No
  Advertised auto-negotiation: Yes
  Speed: 10Mb/s
  Duplex: Full
  Port: Twisted Pair
  PHYAD: 0
  Transceiver: internal
  Auto-negotiation: on
  MDI-X: Unknown
  Cannot get wake-on-lan settings: Operation not permitted
  Link detected: yes
```

4.6.6 获取 CMC 系统进程(ps)

命令功能：

用来显示当前 CMC 系统的进程信息，使用的是 Linux 系统的 ps 命令。

命令格式：

diagnose ps

参数说明：

无

使用指南：

无

使用示例：

#列出当前系统进程。

```
/smashclp> diagnose ps
PID TTY          TIME CMD
11434 pts/0        00:00:00 smashclp
23087 pts/0        00:00:00 sh
23088 pts/0        00:00:00 ps
```

4.6.7 查看系统进程资源占用情况 (top)

命令功能：

用来显示当前 CMC 系统的进程资源占用情况，使用的是 Linux 系统的 top 命令。

命令格式：

diagnose top [-b] [-nCOUNT] [-dSECONDS] [-m]

参数说明：

表 4-10 参数说明

参数	参数说明	取值
-nCOUNT	循环几次后退出	1-n
q	退出循环	无

使用指南：

无

使用示例：

#显示一次系统进程资源占用情况然后退出。

```
/smashclp> diagnose top -n 1

Mem: 143516K used, 266888K free, 0K shrd, 604680K buff, 604728K cached
CPU: 25.0% usr 16.6% sys 0.0% nic 58.3% idle 0.0% io 0.0% irq 0.0% sirq
Load average: 1.53 1.71 1.85 1/140 24460
  PID  PPID  USER    STAT   VSZ %VSZ CPU %CPU COMMAND
24458 24457 admin    R      2812 0.6  0  8.3 /usr/bin/top -n 1
   732    1 sysadmin S      381m 95.0  0  0.0 /usr/local/bin/IPMIMain --
daemonize --reg-with-procmgr
21863  681 sysadmin S      135m 33.7  0  0.0
/usr/local/bin/inspur_monitor_app --inspur-server
1840    1 sysadmin S      72056 17.5  0  0.0 /usr/local/bin/InspurDiagnose
2384    1 sysadmin S      47672 11.6  0  0.0
/usr/local/bin/InspurSelfManager
18689 18688 sysadmin S      44736 10.8  0  0.0 /usr/local/bin/spx_restservice
1075    1 sysadmin S      30744  7.4  0  0.0 /usr/sbin/rsyslogd
   681    1 sysadmin S      23728  5.7  0  0.0
/usr/local/bin/processmanager
1100    1 sysadmin S      22876  5.5  0  0.0
/usr/local/bin/inspur_poweroffprocess_app
18690 18688 sysadmin S      22824  5.5  0  0.0
/usr/local/bin/spx_restservice_ext
2239    1 sysadmin S      22592  5.5  0  0.0 ./compmanager
   679    1 sysadmin S      21692  5.2  0  0.0 /usr/local/bin/execcdaemon
   641    1 sysadmin S      15484  3.7  0  0.0
/usr/local/bin/InspurConfMonitor
2353    1 sysadmin S      15296  3.7  0  0.0 /usr/sbin/snmpd -c
/var/snmpd.conf -L udp:161,udp6:161
11385 11252 admin    S      14360  3.4  0  0.0 sshd: admin@pts/0
11252  2014 sysadmin S      14360  3.4  0  0.0 sshd: admin [priv]
2237    1 sysadmin S      14068  3.4  0  0.0 /usr/local/bin/flasher
1838    1 sysadmin S      12832  3.1  0  0.0
/usr/local/bin/network_monitor
18688    1 sysadmin S      9888  2.4  0  0.0 /usr/local/sbin/lighttpd -f
/conf/lighttpd.conf -m /usr/local/lib
1886    1 sysadmin S      8096  1.9  0  0.0 /usr/local/bin/syslogmonitord
11434 11385 admin    S      7408  1.8  0  0.0 -smashclp
1890    1 sysadmin S      6836  1.6  0  0.0 /usr/local/bin/dhcpmonitor
```

2014	1	sysadmin	S	5484	1.3	0	0.0	/usr/sbin/sshd -p 22 -f /etc/ssh/sshd_config
2192	1	sysadmin	S	5268	1.2	0	0.0	/usr/local/bin/vmapp
2135	1	messageb	S	5228	1.2	0	0.0	/usr/bin/dbus-daemon --system
2364	1	sysadmin	S	4664	1.1	0	0.0	/usr/local/bin/timeoutd
1104	1	sysadmin	S	4224	1.0	0	0.0	/usr/local/bin/pam_helperd
1	0	sysadmin	S	2992	0.7	0	0.0	init [3]
2387	1	sysadmin	S	2816	0.6	0	0.0	/sbin/getty -L console 115200 vt100
1443	1	sysadmin	S	2816	0.6	0	0.0	udhcpc -b -p /var/run/udhcpc.eth0.pid -i eth0 -t 3 -T 3 -x hostname ProductSN -O 248
669	1	sysadmin	S	2812	0.6	0	0.0	{rsyncconf.sh} /bin/sh /etc/rsyncconf.sh /conf /bkupconf
24457	11434	admin	S	2812	0.6	0	0.0	sh -c /usr/bin/top -n 1
2027	1	sysadmin	S	2064	0.5	0	0.0	dhcp6c -p /var/run/dhcp6c.eth0.pid eth0
24446	669	sysadmin	S	2044	0.5	0	0.0	[inotifywait]
2244	1	sysadmin	S	1900	0.4	0	0.0	/usr/sbin/cron
3	2	sysadmin	SW	0	0.0	0	0.0	[ksoftirqd/0]
158	2	sysadmin	SW	0	0.0	0	0.0	[kworker/0:1]
7	2	sysadmin	SW	0	0.0	0	0.0	[watchdog/0]
620	2	sysadmin	SWN	0	0.0	0	0.0	[jffs2_gcd_mtd9]
617	2	sysadmin	SWN	0	0.0	0	0.0	[jffs2_gcd_mtd7]
619	2	sysadmin	SWN	0	0.0	0	0.0	[jffs2_gcd_mtd2]
618	2	sysadmin	SWN	0	0.0	0	0.0	[jffs2_gcd_mtd1]
213	2	sysadmin	SW	0	0.0	0	0.0	[fsnotify_mark]
6	2	sysadmin	SW	0	0.0	0	0.0	[kworker/u2:0]

4.6.8 查看内核缓冲区日志 (dmesg)

命令功能:

用来显示当前 CMC 系统的 dmesg 日志，使用的是 Linux 系统的 demsg 命令。

命令格式:

```
diagnose dmesg
```

参数说明:

无

使用指南:

无

使用示例：

#显示 CMC 系统的 dmesg 日志。

```
/smashclp> diagnose dmesg
[ 1.340000] sdhci: Copyright(c) Pierre Ossman
[ 1.430000] mmc0: SDHCI controller on ast_sdhci1 [ast_sdhci1.0] using ADMA
[ 1.480000] mmc1: SDHCI controller on ast_sdhci2 [ast_sdhci2.0] using ADMA
[ 1.480000] AST SoC SD/MMC Driver Init Success
[ 1.490000] Netfilter messages via NETLINK v0.30.
[ 1.490000] nfnl_acct: registering with nfnetlink.
[ 1.500000] xt_time: kernel timezone is -0000
```

4.6.9 获取网络相关信息 (netstat)

命令功能：

用来显示当前 CMC 系统的网络相关信息，使用的是 Linux 系统的 netstat 命令。

命令格式：

```
diagnose netstat [-ral] [-tuwx] [-en]
```

参数说明：

表 4-11 参数说明

参数	参数说明	取值
-a	显示所有socket	无
-n	不进行域名解析	无

使用指南：

无

使用示例：

#显示当前系统的全部连接信息。

```

/smashclp> diagnose netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:199            0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:22             0.0.0.0:*              LISTEN
tcp      0    100 100.3.8.36:22          100.2.54.244:39243    ESTABLISHED
ESTABLISHED
tcp      0      0 0 :::623                :::*                   LISTEN
tcp      0      0 0 :::80                 :::*                   LISTEN
tcp      0      0 0 :::22                 :::*                   LISTEN
tcp      0      0 0 :::443                :::*                   LISTEN
udp      0      0 0 127.0.0.1:514         0.0.0.0:*             
udp      0      0 0 0.0.0.0:161           0.0.0.0:*             
udp      0      0 0 0.0.0.0:44769         0.0.0.0:*             
udp      0      0 0 :::546                 :::*                  
udp      0      0 0 :::623                 :::*                  
udp      0      0 0 :::161                 :::*                  

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node Path
unix  2      [ ACC ]   STREAM    LISTENING  3102
/var/run/dbus/system_bus_socket
unix  2      [ ACC ]   STREAM    LISTENING  6575658
/tmp/stateless.server
unix  2      [ ACC ]   STREAM    LISTENING  7909468
/tmp/spx_restservice.socket-0
unix  2      [ ACC ]   STREAM    LISTENING  7909471
/tmp/spx_restservice_ext.socket-0
unix  10     [ ]      DGRAM          1135 /var/syslogsock
unix  2      [ ACC ]   STREAM    LISTENING  755 /var/UDSocket1
unix  2      [ ]      STREAM    CONNECTED  7907008
unix  2      [ ]      DGRAM          2940
unix  3      [ ]      STREAM    CONNECTED  7885364
unix  3      [ ]      STREAM    CONNECTED  7885363
unix  2      [ ]      DGRAM          7909526
unix  2      [ ]      DGRAM          4102
unix  2      [ ]      DGRAM          3442
unix  2      [ ]      STREAM    CONNECTED  7909504
unix  2      [ ]      DGRAM          3820
unix  3      [ ]      STREAM    CONNECTED  3110
unix  3      [ ]      STREAM    CONNECTED  3109
unix  2      [ ]      STREAM    CONNECTED  7884941
unix  2      [ ]      DGRAM          6575673
unix  2      [ ]      DGRAM          4082806
unix  2      [ ]      STREAM    CONNECTED  7930888

```

unix	2	[]	STREAM	CONNECTED	7910393
unix	2	[]	DGRAM		7909502
unix	2	[]	STREAM	CONNECTED	7930887

4.6.10 CMC GPIO 设备测试

命令功能：

用来调试当前 CMC 系统的 GPIO 设备。

命令格式：

diagnose gpiotool <gpionumber> <option>

参数说明：

表 4-12 参数说明

参数	参数说明	取值
gpionumber	GPIO编号	0-227
option	支持命令	--get-dir --get-data

使用指南：

这个是专业的工具，非专业人士需要在指导下使用，错误的使用可能导致系统异常。

使用示例：

#获取 GPIO 10 的输入输出方向

```
/smashclp> diagnose gpiotool 10 --get-dir
Inside Get Dir

Input Pin
```

#获取 GPIO 10 的输入状态

```
/smashclp> diagnose gpiotool 10 --get-data
Inside Read gpio.

Pin is High
```

4.6.11 CMC I2C 设备测试

命令功能：

用来调试当前 CMC 系统的 I2C 设备。

命令格式：

```
diagnose i2c-test -b <bus number> --scan
```

```
diagnose i2c-test -b <bus number> -s slave -rc count -d < bytes >
```

```
diagnose i2c-test -b <bus number> -s slave -w -d < bytes >
```

参数说明：

表 4-13 参数说明

参数	参数说明	取值
bus number	bus号	0-13
slave	7位slave地址	0-0x7F
count	读取数目	缺省为1
bytes	要发送的数据	无

使用指南：

这个是专业的工具，非专业人士需要在指导下使用，错误的使用可能导致系统异常。

使用示例：

#扫描 I2C bus 1 的所有 slave 地址。

```
/smashclp> diagnose i2c-test -b 1 --scan
Scanning the I2C Bus...this may take a while...
.
.....X.....
.....
Done! Found 1 valid slave address(es)
Slave list:
0xa0
```

#从 I2C 的 bus 1 的 7 位 slave 地址 0x50 读取 32 个字节。

```
/smashclp> diagnose i2c-test -b 1 -s 0x50 -rc 32 -d 0 0
i2c_dev = /dev/i2c1
Bytes read: 32
b4 05 5d 4d f8 94 ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
Bytes written: 2
00 00
```

4.6.12 CMC PWM 风扇调控

命令功能：

用来调试 CMC 系统的 PWM 风扇。

命令格式：

```
diagnose pwmtachtool <device_id> <command-option> <fannum>
```

参数说明：

表 4-14 参数说明

参数	参数说明	取值
device_id	设备id	一般为0
command-option	支持命令	--get-fan-speed --get-pwm-dutycycle
fannum	第几个风扇	[1-n]要参考实际的风扇数目

使用指南：

这个是专业的工具，非专业人士需要在指导下使用，错误的使用可能导致系统异常。

使用示例：

#获取设备 0 下风扇 0 的转速。

```
/smashclp> diagnose pwmtachtool 0 --get-fan-speed 0
Fan 0 speed is 7498
```

#获取设备 0 下风扇 2 的 duty。

```
/smashclp> diagnose pwmtachtool 0 --get-pwm-duty-cycle 2
PWM 2 Duty-cycle is 26
```

4.6.13 CMC IPMI 设备访问

命令功能：

使用 IPMITool 工具对当前 CMC 系统进行 IPMI 相关信息的访问。

命令格式：

```
diagnose ipmitool -H 127.0.0.1 <command>
```

参数说明：

表 4-15 参数说明

参数	参数说明	取值
command	ipmitool命令	fru sensor sdr sel sel list

使用指南：

无

使用示例：

#获取 CMC 的 FRU 信息。

```
/smashclp> diagnose ipmitool -H 127.0.0.1 fru
FRU Device Description : Builtin FRU Device (ID 0)
Chassis Type           : Rack Mount Chassis
Chassis Part Number   : ChassisPN
Chassis Serial        : ChassisSN
Chassis Extra         : ChassisExtra
Board Mfg Date        : Sat Jan  1 08:02:00 2000
Board Mfg             : BoardMfr
Board Product         : BoardPN
Board Serial         : BoardSN
Board Part Number    : BoardPart
```

Board Extra	: BoardExtra1
Board Extra	: BoardExtra2
Board Extra	: BoardExtra3
Product Manufacturer	: ProductMFR
Product Name	: ProductName
Product Part Number	: ProductPN
Product Version	: ProductVer
Product Serial	: ProductSN
Product Asset Tag	: ProductAT
Product Extra	: ProductExtra1
Product Extra	: ProductExtra2

#获取 CMC 的 sdr 信息。

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sdr
Inlet_Temp      | 28 degrees C      | ok
Outlet_Temp     | 28 degrees C      | ok
CMC_Temp        | 36 degrees C      | ok
PeerCMC_Prst   | 0x02              | ok
CMC_Status      | 0x00              | ok
PeerCMC_Status | 0x00              | ok
Switch_Temp     | 0 degrees C       | ok
```

#获取 CMC 的 sensor 信息。

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sensor
Inlet_Temp      | 28.000            | degrees C | ok   | na   | na   | na
| na            | 40.000            | 45.000
Outlet_Temp     | 28.000            | degrees C | ok   | na   | na   | na
| 75.000       | na                | na
CMC_Temp        | 36.000            | degrees C | ok   | na   | na   | na
| na            | 80.000            | 85.000
PeerCMC_Prst   | 0x0               | discrete  | 0x0280| na   | na   | na
| na           | na                | na
CMC_Status      | 0x0               | discrete  | 0x0080| na   | na   | na
| na           | na                | na
PeerCMC_Status | 0x0               | discrete  | 0x0080| na   | na   | na
| na           | na                | na
Switch_Temp     | 0.000             | degrees C | ok   | na   | na   | na
| na           | 100.000           | 105.000
NODE1_Prst     | 0x0               | discrete  | 0x0180| na   | na   | na
| na           | na                | na
NODE2_Prst     | 0x0               | discrete  | 0x0280| na   | na   | na
| na           | na                | na
```

#获取 CMC 的 SEL 概要信息。

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sel
SEL Information
Version      : 1.5 (v1.5, v2 compliant)
Entries      : 119
Free Space   : 63360 bytes
Percent Used : 2%
Last Add Time : 01/02/2000 01:06:22
Last Del Time : Not Available
Overflow     : false
Supported Cnds : 'Delete' 'Partial Add' 'Reserve' 'Get Alloc Info'
# of Alloc Units : 3639
Alloc Unit Size : 18
# Free Units   : 3520
Largest Free Blk : 3520
Max Record Size : 13
```

#获取 CMC 的 SEL 的列表信息。

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sel elist
 1 | 01/01/2000 | 08:00:25 | System Boot Initiated CMC_Boot_Up | Initiated by
warm reset | Asserted
 2 | 01/01/2000 | 08:01:06 | Module/Board PeerCMC_Prst | Device Present
 3 | 01/01/2000 | 08:01:06 | Module/Board NODE2_Prst | Device Present
 4 | 01/01/2000 | 08:01:06 | Module/Board NODE7_Prst | Device Present
```

4.6.14 获取文件系统磁盘使用情况(df)

命令功能：

用来显示当前 CMC 系统的文件系统使用情况，使用的是 Linux 系统的 df 命令。

命令格式：

```
diagnose df [-Pkmhai]
```

参数说明：

无

使用指南：

无

使用示例：

#获取当前文件系统的使用情况。

```
/smashclp> diagnose df
Filesystem          1K-blocks      Used Available Use% Mounted on
/dev/root            51004          51004         0 100% /
devtmpfs            172296           0    172296   0% /dev
/dev/shm            205200          128    205072   0% /var
/dev/shm            205200           44    205156   0% /run
/dev/mtdblock7      1984           316     1668   16% /bkupsync
/dev/mtdblock1      1984           352     1632   18% /conf
/dev/mtdblock2      1984           340     1644   17% /bkupconf
/dev/mtdblock9     10176           532     9644    5% /extlog
/dev/mtdblock10    10176           388     9788    4% /usr/local/lmedia
/dev/ram3           6032           6032         0 100% /usr/local/www
/splashclp> exit
```

4.6.15 获取系统运行时间 (uptime)

命令功能：

用来显示当前 CMC 系统的运行时间，使用的是 Linux 系统的 uptime 命令。

命令格式：

```
diagnose uptime
```

参数说明：

无

使用指南：

无

使用示例：

#获取当前系统运行时间。

```
/smashclp> diagnose uptime
05:14:10 up 2 days, 21:14,  1 users,  load average: 2.58, 2.07, 1.94
```

缩略语

A.1 缩略语表

B

BIOS	Basic Input Output System	基本输入输出系统
BMC	Baseboard Management Controller	基板管理系统

C

CLI	Command-Line Interface	命令行界面
CLP	Command Line Protocol	命令行协议
CMC	Chassis Management Controller	机箱管理系统
CPU	Central Processing Unit	中央处理器

D

DHCP	Dynamic Host Configuration Protocol	动态主机设置协议
DNS	Domain Name System	域名系统

F

FMA	Failure Mode Analysis	失效模式分析
-----	-----------------------	--------

G

GUI	Graphical User Interface	图形用户界面
-----	--------------------------	--------

H

HTML	Hyper Text Markup Language	超文本标记语言
------	----------------------------	---------

I

IPMI	Intelligent Platform Management Interface	智能平台管理接口
------	--	----------

M

MLAN	Music Local Area Network	音乐局域网
------	--------------------------	-------

N

NIC	Network Interface Controller	网络接口控制器
NTP	Network Time Protocol	网络时间协议

P

PSU	Power Supply Unit	电源设备
-----	-------------------	------

R

RST	Reset	复位
-----	-------	----

S

SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SMASH	Systems Management Architecture for Server Hardware	服务器硬件系统管理架构
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳协议

T

TCO	Total Cost of Ownership	总拥有成本
-----	-------------------------	-------

U

UID	User Identification	定位指示灯
-----	---------------------	-------

UPI	Ultra Path Interconnect	超级通道互联
USB	Universal Serial Bus	通用串行总线