KunTai 服务器

iBMC 智能管理系统白皮书

文档版本 **1.0**

发布日期 **2021.1.25**

商标声明

神州数码 Digital China和其他北京神州数码云科信息技术有限公司商标均为北京神州数码云科信息技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受北京神州数码云科信息技术有限公司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，北京神州数码云科信息技术有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

北京神州数码云科信息技术有限公司

地址： 北京市海淀区上地九街 9 号数码科技广场

网址： www.yunke-china.com

客户服务邮箱： yunkechina@digitalchina.com

客户服务电话： 400-810-9119

前言

概述

本文档详细的描述了鲲泰服务器 iBMC 智能管理系统的主要特性，让用户对 iBMC 有一个 深入细致的了解。

读者对象

本文档主要适用于以下人员：

- 神州数码售前工程师。
- 渠道伙伴售前工程师。
- 企业售前工程师。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
警告	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
注意	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

文档版本	发布日期	修改说明
01	2021-01-25	第一次发布。

目 录

1 产品简介

1.1 概述

鲲泰服务器 iBMC 智能管理系统（以下简称 iBMC）是国产开发的具有完全自主知识产权的服务器远程管理系统。iBMC 兼容服务器业界管理标准 IPMI 、SNMP、Redfish、支 持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件 监控和管理功能。iBMC 提供了丰富的特性支持。其主要特性有：

- 丰富的管理接口 提供 IPMI/CLI/HTTPS/SNMP/Redfish 管理接口，满足多种方式的系统集成需求。
- 兼容 DCMI1.5/IPMI1.5/ IPMI2.0
  提供标准的管理接口，可被标准管理系统集成。
- 故障监控和诊断 故障监控和诊断，提前发现并解决问题，保障设备 7*24 小时高可靠运行。
- 虚拟 KVM 和虚拟媒体 提
  供方便的远程维护手段。
- 基于 Web 界面的用户接口 可以通过简单的界面操
  作快速完成设置和查询任务。
- 系统崩溃时临终截屏与录像 分析
  系统崩溃原因不再无处下手。
- 屏幕快照和屏幕录像 让定时巡检、操作过程记录
  及审计变得简单轻松。
- 支持 DNS/LDAP 域管理和目录服务，简
  化服务器管理网络。
- 软件双镜像备份 提高系统的安全性，即使当前运行的软件完全崩溃，也可以从备份镜像启动。
- RAID 带外管理

支持 RAID 的带外监控和配置，提升了 RAID 配置效率和管理能力。

- 支持 FDM 支持基于部件的精准故障诊断，方便部件故障定位和更换。
- 支持 NTP 提升设备时间配置能力，用于同步网络时间。
- 设备资产管理 让资产盘点不再困难。
- 支持智能电源管理 功率封顶技术助您轻松提高部署密度；动态节能技术助您有效降低运营成本。
- 安全管理 从接入、账号、传输、存储四个维度保障服务器管理的安全，让您用得放心。

1.2 系统架构

如**图 1-1** 和**图 1-2** 所示，iBMC 硬件芯片采用华为研发的海思芯片 Hi1710/Hi1711，Hi1710/Hi1711 是一 款针对计算/交换平台的板级管理 BMC 芯片，包括一个最高主频为 800MHz 的单核 A9 CPU，一个 8051 单片机及主频 200MHz 的协处理器，支持远程 KVM，支持 IPMI 管理接 口，支持 PCIe 收发 MCTP 报文，支持本地显示 VGA，GE 网口、RMII 接口，以及其它丰 富的板级管理和外设接口；具体如下：

- iBMC 的 KVM 模块通过 VGA 接口接收来自业务系统的视频信息，经过压缩后再通过 网络将压缩数据传输到远程 KVM 客户端进行解压还原。此外 KVM 模块接收远程 KVM 客户端的键盘鼠标数据，通过模拟的 USB 键盘鼠标设备将数据传输到业务系 统，实现远程的键盘鼠标控制。
- iBMC 的 VMM 模块将光驱等本地资源虚拟为服务器的 USB 设备。
- iBMC 的系统运行记录仪模块通过 PCIe 接口接收来自业务系统写入的运行轨迹信息（黑匣子数据），并提供记录信息的导出接口。
- iBMC 的 agentless 特性是通过 PCIe 接口与带内 iBMA 交互对网卡等带内部件管理和 OS 信息查询。
- iBMC 提供传统的 LPC 系统接口与 x86 系统或 Kunpeng 系统通信，支持标准的 IPMI 管理。
- iBMC 对外提供 GE 以太网络接口，支持通过网络使用 IPMI，HTTPS 等协议进行远程 管理操作。
- iBMC 通过传感器实现了对服务器的温度、电压状态全面监控，并且提供对服务器 的风扇和电源的智能管理。
- iBMC 支持最新的边带网络技术（Side band，如：NCSI）以及 VLAN 网络功能，通 过边带网络可以支持更加灵活的管理组网。

图 1-1 iBMC 系统架构-x86

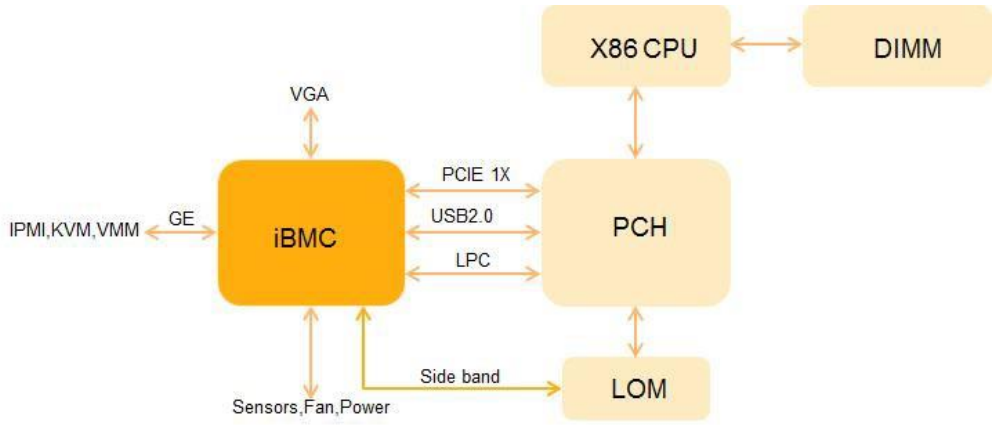
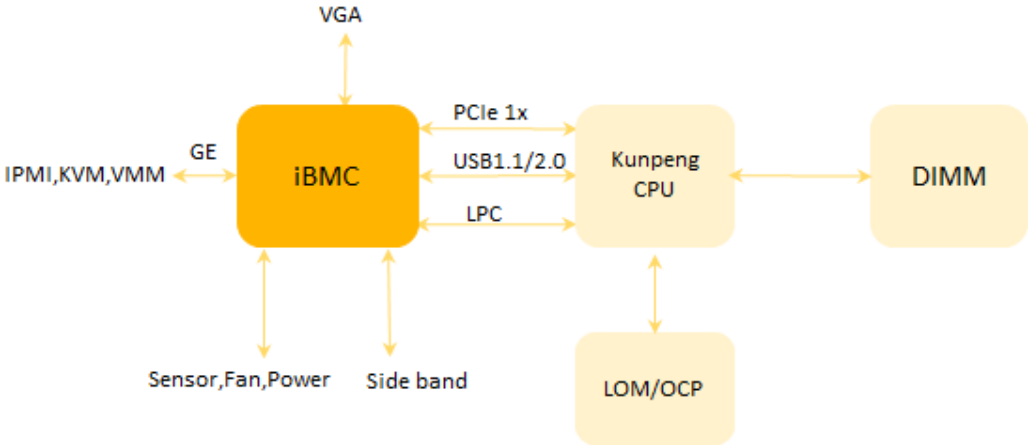


图 1-2 iBMC 系统架构-Kunpeng



2 支持产品范围

组件	规格
支持的产品 （包括但不限于）	机架服务器：KunTai R522、KunTai R722、KunTai R524、KunTai R724、KunTai R822、KunTai R722-E、KunTai R2260、KunTai R2280 AI 服务器：KunTai A722

3 支持功能

iBMC 以其丰富的特性支持，提升管理效率，有效降低运营成本。

- iBMC 是国产开发的具有完全自主知识产权的高级服务器远程管理软件。它支持键 盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体（可将终端的光 驱、软驱、文件夹映射到服务器）和基于 IPMI/Redfish 的硬件监控和管理功能。 是按照电信级的可靠性要求而设计的，支持双镜像备份的软件。

  iBMC 提供了丰富的用户接口，如命令行、基于 Web 界面的用户接口、IPMI 集成接 口、SNMP 集成接口、Redfish 集成接口，并且所有用户接口都采用了认证机制和 高度安全的加密算法，保证接入和传输的安全性。

- iBMC 对服务器进行了全面精细的监控，并且提供了丰富的告警和详细的日志。能 够独立显示主板电源故障、CPU 的内核温度、电压、硬盘故障、风扇转速及温度 故障、网卡 MCE/AER 错误、系统电源故障、总线故障、系统宕机故障等。同时还 提供了 CPU、内存、网卡和硬盘等各类部件信息的查询。同时支持对告警日志、 错误日志、部件信息等实现一键收集辅助问题定位。

- iBMC 能够在服务器宕机的时候自动保存宕机之前屏幕上输出的最后的信息，用于 故障的定位。还支持即时的屏幕快照，第三方程序可以设置定时或周期性的进行 屏幕截屏，不需要手工定时去查看服务器，为维护人员节省大量时间。

3.1 丰富的管理接口

iBMC 是一个遵循行业管理规范的带外单机管理系统，是数据中心管理网络中的一个子 节点，承载着管理、控制和诊断服务器的任务，需要对外提供各种人机接口和机机接 口，以满足各种服务器管理场景的应用和集成需求。

iBMC 的框架分三层，即：接口层、应用层和框架层，接口层主要提供各种接口，包括 用户接口（Web 和 CLI）和机机接口（SNMP、IPMI 和 Redfish）；应用层是所有特性功 能的集合；框架层主要包括 PME（Platform Management Engine）、linux 内核和驱 动。

图 3-1 iBMC 管理接口图

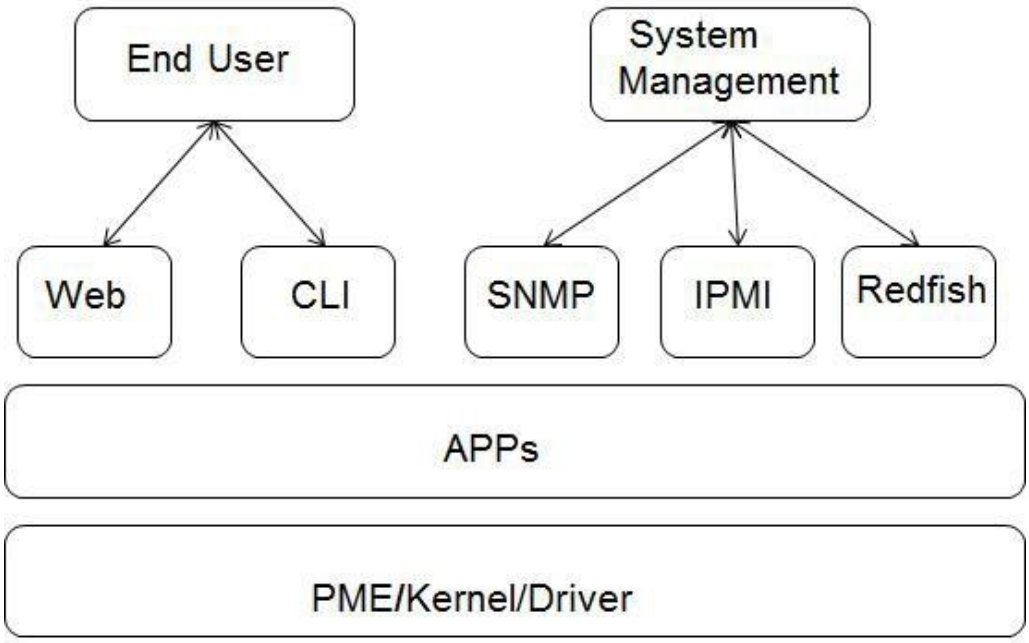


表 3-1 主要集成接口对比

接口	难度	集成工作量	兼容性	安全性	性能	架构先进性	应用
Redfish	易，使用最流行 python解析型语言编程，json格式输入输出	较小，json输入输出，不用额外解析	好，规范定义较全，意在替代IPMI	高，基于HTTPS协议，支持各种安全的加密、完整性、鉴权算法	好，一次交互可以获取整个资源	好，所有事物都抽象为资源，有唯一URI，面向对象架构	业界互联网/网管都选择或准备选择REST+Python，应用广泛
SNMP	中，需要理解MIB库和OID、SNMP规范	中，依赖MIB库进行解析	较差，规范定义较少，基本都是网络相关标准节点	低，支持的安全算法有限，目前仅支持鉴权算法MD5和SHA1，加密算法仅支持DES和AES128，不支持域账号访问	较差，每次交互只能获取一个信息，最大限制为4K字节	较差，面向节点，缺乏层次和关联	在网络交换设备管理领域比较流行，总体占有率一般
IPMI	难，C语言编程，掌握难度大	大，二进制输出，不友好且解析工作量大	较差，规范定义较少且很久未更新	低，支持的安全算法有限，出现过安全漏洞，不支持域账号访问	较差，每次交互只能获取一个信息，带内通道最大限制为字节	较差，面向命令，缺乏层次和关联	仅服务器行业比较流行，总体占有率不高

说明：基于上述优劣对比，后续鲲泰服务器管理软件对外集成接口以 redfish 接口为

主，主动规划并及时跟进 DMTF 的 redfish 规范更新。

3.1.1 IPMI 管理接口

iBMC 兼容 IPMI 1.5/IPMI 2.0 规范，使用第三方工具（如：ipmitool），通过基于 LPC 通道的 BT 协议或 LAN 通道的 UDP/IP 协议实现对服务器的有效管理。基于 LPC 时，ipmitool

等工具必须运行在服务器本机的操作系统上；而基于 LAN 时，ipmitool 等工具可以远程管理服务器，iBMC 支持 AES-CBC-128 加密算法，以及 HMAC-SHA1/HMAC-SHA256 鉴权和完整性校验算法。支持 Windows 和 Linux 系统下第三方工具。

IPMI 规范所有服务器厂商都支持，并且由于支持本机内部通道通讯，本机内部通道通讯时支持免鉴权，在服务器管理行业应用较广泛，特别是早期的带内管理场景。

对于管理网络和业务网络具有隔离诉求的场景，iBMC 支持配置黑名单和白名单机制屏蔽带内 LPC 通道的 IPMI 命令下发。白名单和黑名单的配置范围包括通道号、网络功能码、命令字、子命令、参数等选项，支持添加、删除和查询。功能禁用时带内和带外正常通信，启动白名单时仅允许白名单中配置的命令在带内通道下发；启动黑名单时禁止黑名单中配置的命令在带内通道下发。默认启用为黑名单模式，支持切换为白名单模式。

iBMC 的 IPMI 接口能力：

1. iBMC、BIOS、CPLD、电源 FW 等固件升级。
2. 用户管理(新增用户/修改密码/修改权限/删除用户)。
3. 服务启停及端口修改。
4. 功率封顶配置。
5. RAID 带外配置(查看硬盘和 RAID 卡信息、创建 RAID、设置属性、删除 RAID)。
6. 管理网络配置(IP/掩码/网关、DNS)。
7. 系统启动(系统启动设备、启动模式、是否单次生效)。
8. SEL 查看。
9. 传感器查询（温度、电压等查询）。
10. 电源控制(上下电、重启)。
11. 查看 FRU 信息(资产标签/产品名称/产品序列号等)。
12. SOL 功能。

以下以 ipmitool 工具举例说明：

- ipmitool 命令格式：ipmitool [interface] [parameter] <command>
- ipmitool 命令可设置的接口包括：

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

- ipmitool 命令可设置的参数包括：

```
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
```

- ipmitool 可执行的操作包括：

```
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
```

- ipmitool 命令举例：查询 iBMC 上所有本地用户

  基于 LPC：ipmitool user list

  基于 LAN：ipmitool -H *.*.*.* -I lanplus -U <用户名> -P <密码> user list 1

  – H：iBMC 网口 IP 地址

  – I：传输协议，lan：不加密，lanplus：加密

  – U：iBMC 本地用户名

  – P：iBMC 本地用户密码

3.1.2 SNMP 管理接口

简单网络管理协议（以下简称 SNMP）是管理进程（NMS）和代理进程（Agent）之间 的通信协议。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信 的公共语言、相应的安全和访问控制机制。

iBMC 提供了 SNMP 的编程接口，支持 SNMP Get/Set/Trap 操作。通过第三方管理软件 调用 SNMP 接口可以方便地对服务器集成管理。SNMP 代理支持 V1/V2C/V3 版本，出厂 默认只启用 V3 版本。SNMP V1/V2C 的 Get/Set 操作可以使用不同的团体名；SNMP V3 的鉴权算法支持选择 MD5 或 SHA，加密算法支持选择 DES 或 AES，安全用户名与登录用 户名相同。SNMP V3 安全用户与其他接口（Web、CLI、IPMI LAN）共用一套本地用 户。

SNMP 接口应用场景：

- 场景 1——基于开源工具的管理

直接使用第三方的 MIB 图形工具（如 MG-SOFT MIB Browser）和命令行工具基于 SNMP 协议对每个 MIB 节点进行操作，通常用于测试或临时的服务器远程管理和维护。

- 场景 2——简单集成管理

网管软件将 SNMP MIB 定义文档编译后导入，即可通过 SNMP 接口管理服务器，并可对 重要的信息配置触发脚本以及对 Trap 事件进行重新映射；目前已和业界常用的 CA、 IBM System Director、HP SIM 网管软件进行了对接验证。

- 场景 3——深度集成管理

网管支持插件方式，针对不同服务器厂商开发不同的集成管理插件，插件接收网管的操作命令并通过 SNMP 接口与 iBMC 交互进行查询和设置信息，然后按照网管与插件接 口格式返回给网管进行展示；目前已为业界常用的 Vmware Vcenter、微软 System Center 网管软件开发了插件，具体参考：**http://support.huawei.com/enterprise/zh/index.html**。

iBMC 的 SNMP 接口能力：

1. iBMC、BIOS、CPLD、电源 FW 等固件升级。
2. 用户管理(新增用户/修改密码/修改权限/删除用户)。
3. 功率封顶配置。
4. RAID 带外配置(查看硬盘和 RAID 卡信息、创建 RAID、设置属性、删除 RAID)。
5. 管理网络配置(IP/掩码/网关、DNS)。
6. 系统启动(系统启动设备、启动模式、是否单次生效)。
7. 系统资源性能(CPU、内存、磁盘分区使用率)。
8. eSight 无状态计算配置。
9. 查看当前健康事件/历史事件/系统健康状态、清除事件。
10. 证书管理(查看、CSR 生成和导出、证书/证书链导入、双因子证书)。
11. 电源主备配置。
12. NTP 配置/时区配置。
13. LDAP 配置。
14. 温度、电压查询。
15. 电源控制(上下电、重启)。
16. 查看整机系统信息(资产标签/产品名称/产品序列号等)。
17. 查看 CPU/内存信息。
18. 查看系统电源、风扇信息。
19. 查看网卡及网口信息。
20. SNMP TRAP 及配置。
21. E-mail 上报配置。

具体接口定义参考：http://support.huawei.com/enterprise/zh/server/ibmc- pid-8060757

3.1.3 Redfish 管理接口

REST（Representational State Transfer）是一种针对网络应用的设计和开发方式，可 以降低开发的复杂性，提高系统的可伸缩性。

REST 提出的设计概念和准则有：

- 网络上的所有事物都被抽象为资源，以 JSON 格式表示。
- 每个资源对应一个唯一的资源标识 URI。
- 通过通用的 HTTP 接口（GET/PATCH/POST/DELETE）对资源进行操作。
- 对资源的各种操作不会改变资源标识。
- 所有的操作都是无状态的（stateless）。

Redfish 可扩展平台管理编程接口，是一个管理标准，它基于 HTTPS 协议，使用内置于超媒体 RESTful 接口的数据模型展现。

Redfish = REST API + 软件定义的服务器(数据模型)，当前由标准组织 DMTF（www.dmtf.org）负责维护。

图 3-2 Redfish Schema 框架

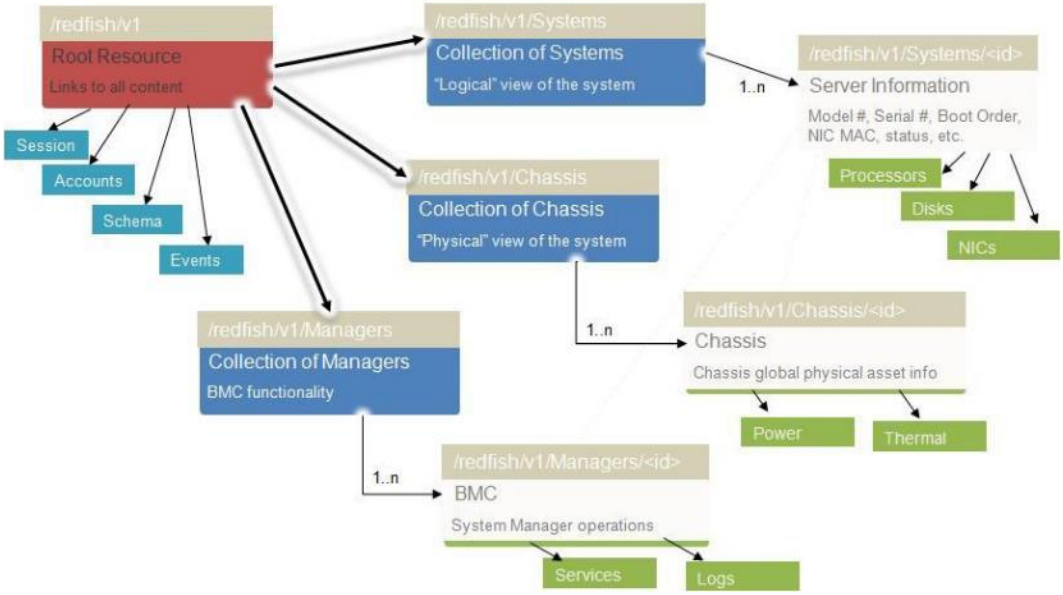
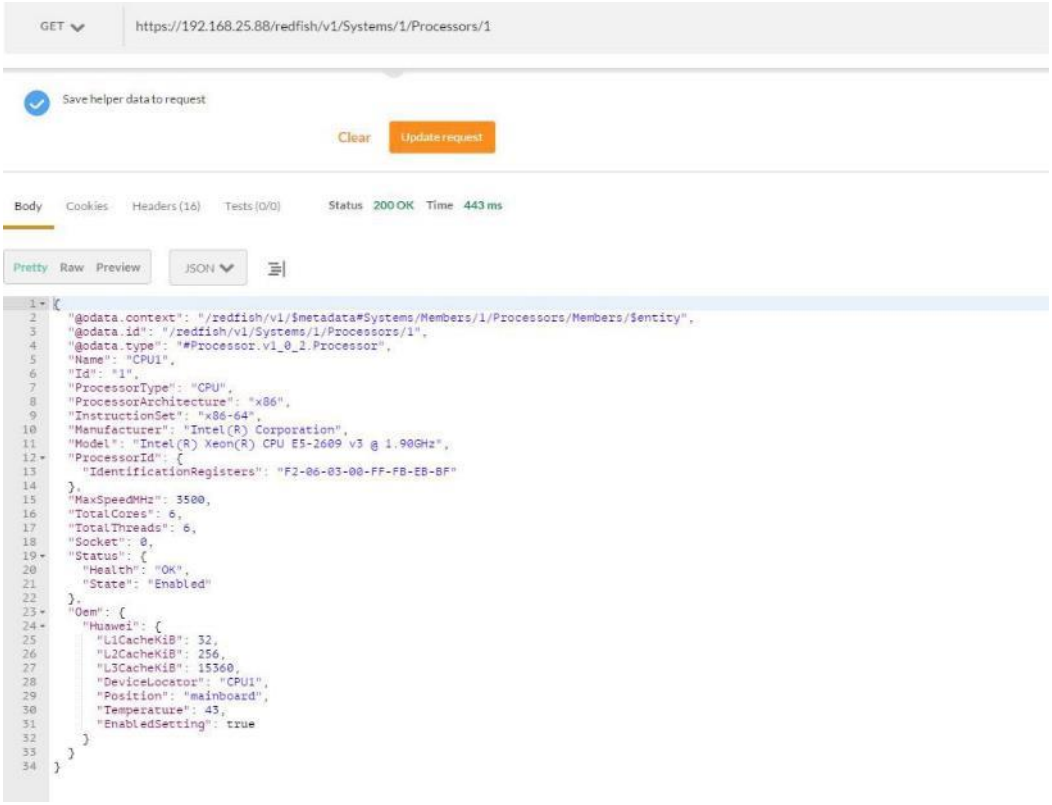


图 3-3 Redfish 接口操作示例(查询处理器资源)：



iBMC 支持 Redfish 1.0.4 规范，具体支持的 Redfish 接口能力：

1. iBMC、BIOS、CPLD、电源 FW 等固件升级。
2. 网卡、RAID 卡驱动升级。
3. 用户管理(新增用户/修改密码/修改权限/删除用户)。
4. BMC 和 BIOS 配置、RAID 控制器配置以 XML 文件导入导出。
5. BIOS 菜单项查看及配置。
6. 软件资源列表查看。
7. 服务启停及端口修改。
8. 功率封顶配置。
9. RAID 带外配置(查看硬盘和 RAID 卡信息、创建 RAID、设置属性、删除 RAID)。
10. 管理网络配置(IP/掩码/网关、DNS)。
11. 系统启动(系统启动设备、启动模式、是否单次生效)。
12. 系统资源性能(CPU、内存、磁盘分区使用率)。
13. 系统信息(主机名称、域名称(oem)、计算机描述(oem)、操作系统(OS 主版本、OS 次版本、补丁主版本、补丁次版本))。
14. eSight 无状态计算配置。
15. 查看当前健康事件/历史事件/系统健康状态、清除事件。
16. 事件订阅。
17. 远程虚拟媒体(属性查看、挂载、断开)。
18. 证书管理(查看、CSR 生成和导出、证书/证书链导入、双因子证书)。
19. 电源主备配置。
20. NTP 配置/时区配置。

21. LDAP 配置。
22. 温度、电压查询。
23. 电源控制(上下电、重启)。
24. 查看整机系统信息(资产标签/产品名称/产品序列号等)。
25. 查看 CPU/内存信息。
26. 查看系统电源、风扇信息。
27. 查看网卡及网口信息。
28. SNMP TRAP 配置。
29. E-mail 上报配置。

具体接口定义参考接口手册：http://support.huawei.com/enterprise/zh/server/ ibmc-pid-8060757 。

3.1.4 CLI 管理接口

CLI 是 iBMC 提供的一个私有命令行接口，包含两个基本命令程序：ipmcget 和 ipmcset，通过这两个命令程序就能实现对服务器的远程管理。可通过 SSH 方式登录 iBMC 后执行此命令。
CLI 接口不仅提供了不依赖额外工具的人机操作界面，也能用于被集成，比 Web 更轻量，比部分集成接口更友好。

iBMC 的 CLI 接口能力：

1. iBMC、BIOS、CPLD、电源 FW 等固件升级。
2. 用户管理(新增用户/修改密码/修改权限/删除用户)。
3. BMC 和 BIOS 配置、RAID 控制器配置以 XML 文件导入导出。
4. 服务启停及端口修改。
5. 功率封顶配置。
6. RAID 带外配置(查看硬盘和 RAID 卡信息、创建 RAID、设置属性、删除 RAID)。
7. 管理网络配置(IP/掩码/网关、DNS)。
8. 系统启动(系统启动设备、启动模式、是否单次生效)。
9. eSight 无状态计算配置。
10. 查看当前健康事件/历史事件/系统健康状态、清除事件。
11. 远程虚拟媒体(属性查看、挂载、断开)。
12. 证书管理(查看、CSR 生成和导出、证书/证书链导入、双因子证书)。
13. 电源主备配置。
14. NTP 配置/时区配置。
15. LDAP 配置。
16. 传感器查询（温度、电压等查询）。
17. 电源控制(上下电、重启)。
18. 查看整机系统信息(资产标签/产品名称/产品序列号等)。
19. 查看系统电源、风扇信息。
20. SNMP TRAP 配置。
21. SOL 功能。

具体命令定义参考用户指南：

http://support.huawei.com/enterprise/zh/server/ ibmc-pid-8060757 。

3.1.5 Web 管理接口

iBMC 提供了基于 HTTPS 的 Web 可视化管理接口，使用户可以：

- 通过简单的界面操作快速完成设置和查询任务。
- 通过远程控制台可以对服务器进行 OS 启动全程监控、OS 操作、以及光驱/软驱映 射等。

可以在浏览器地址栏输入 iBMC 的网口 IP 地址（IPv4 或 IPv6）或域名称打开 iBMC Web
的登录界面，输入本地账号或 LDAP 域账号登录到 iBMC Web。

Web 接口支持的 OS 和浏览器、JRE 如**表 3-2** 示。

表 3-2 客户端环境要求

运行环境	配置要求
	Windows 8 32 位/64 位
	Windows 10 32 位/64 位
	Windows Server 2012 64 位
	Windows Server 2012 R2 64 位
	Windows Server 2016 64 位
	Redhat 6.0 64 位
	Mac OS X v10.12
浏览器	Internet Explorer 9/10/11（仅适用于 Windows 操作系统）
	Mozilla Firefox 39/54
	Chrome 21/43（仅适用于 Windows 操作系统）
	Safari 5.1（仅适用于 MAC 操作系统）
Java 运行环境	JRE 1.7.0 U40/1.8.0U45/1.8.0U144/1.9.0U1

iBMC 支持更安全的 SSL 协议版本：

- 支持 TLS 1.0/1.1/1.2，TLS 1.2 仅支持开启状态，TLS 1.0/1.1 支持开启/关闭状态。 为兼容较低版本的浏览器，TLS 1.1 默认开启，TLS 1.0 默认关闭。

iBMC 的 Web 接口能力：

1. iBMC、BIOS、CPLD、电源 FW 等固件升级。
2. 用户管理(新增用户/修改密码/修改权限/删除用户)。
3. BMC 和 BIOS 配置、RAID 控制器配置以 XML 文件导入导出。
4. 服务启停及端口修改。
5. 功率封顶配置。
6. RAID 带外配置(查看硬盘和 RAID 卡信息、创建 RAID、设置属性、删除 RAID)。
7. 管理网络配置(IP/掩码/网关、DNS)。
8. 系统启动项配置(系统启动设备、启动模式、是否单次生效)。
9. 系统资源性能展示(CPU、内存、磁盘分区使用率)。
10. 系统信息(主机名称、域名称(oem)、计算机描述(oem)、操作系统(OS 主版本、OS 次版本、补丁主版本、补丁次版本))。
11. 查看当前健康事件/历史事件/系统健康状态、清除事件。
12. 远程虚拟媒体及配置(属性查看、挂载、断开)。
13. 远程 KVM。
14. 证书管理(查看、CSR 生成和导出、证书/证书链导入、双因子证书)。
15. 电源主备配置。
16. NTP 配置/时区配置。
17. LDAP 配置。
18. 温度、电压查询。
19. 电源控制(上下电、重启)。
20. 查看整机系统信息(资产标签/产品名称/产品序列号等)。
21. 查看 CPU/内存信息。
22. 查看系统电源、风扇信息。
23. 查看网卡及网口信息。
24. SNMP TRAP 配置。
25. E-mail 上报配置。

具体功能参考用户指南：

http://support.huawei.com/enterprise/zh/server/ibmc- pid-8060757 。

3.2 故障诊断与管理（FDM）

故障诊断与管理（FDM）是 iBMC 面向鲲泰服务器提供一系列诊断能力和工具，包括故 障检测、诊断、上报以及诊断辅助功能。

3.2.1 故障检测

iBMC 对服务器进行全面的监控，并且提供了可靠的故障检测和故障预测机制。能检测 到的故障包括（不同产品支持情况存在差异）：

- CPU 硬件故障（CAT ERROR、自检失败、配置错误）

- 超温告警（进风口、CPU、内存、系统电源、硬盘、RAID 卡）
- 主板各电源（含电池）和板卡电源故障
- 风扇故障
- 网卡 MCE/AER 错误故障
- 系统电源故障（AC/DC 输入丢失、高温、电源风扇故障、过压、过流）
- 总线故障（I2C、IPMB、QPI/UPI/HCCS）
- DDR3/DDR4 内存故障（可纠正 ECC 错误超门限、不可纠正 ECC 错误、高温、配置 和初始化错误、CE 溢出监控）
- 存储故障，包括 RAID 控制器故障（内部故障、内存 UCE 计数非 0、内存 ECC 计数超 门限、NVRAM 错误计数非 0、BMC 访问失败）、硬盘故障（故障、预故障、重构 失败、盘在位但 RAID 卡不能识别、SSD 剩余寿命监控）、逻辑盘异常（Offline、 Degraded）、BBU 电压低或故障、链路误码（RAID 扣卡、硬盘背板 expander 链 路误码、SAS 盘和 SATA 盘内部故障的 smart 信息收集）
- 系统宕机故障
- 配合 iBMA 软件，可以增强 iBMC 软件故障识别能力，主要体现在 RAID 卡，硬盘，

PCIe 卡和操作系统方面，详情参见下表：

表 3-3 iBMA 获取的 RAID 卡和硬盘故障及故障定位信息

获取信息描述	LSI 2200	LSI 2300	LSI3008	LSI 3108	软 RAID	PCH 硬盘	NVMe	备注
RAID 降级	支持	支持	支持	支持	支持	NA	NA	
RAID 卡 BBU 异常	不支持	不支持	NA	支持	NA	NA	NA	iBMC 呈现告警
硬盘 Offline	支持	支持	支持	支持	支持	支持	不支持	iBMC 呈现告警，PCH 硬盘支持 Linux，Windows 系统下检测
硬盘容量为 0	支持	支持	支持	支持	支持	支持	不支持	不支持 iBMC 带外 管理的 RAID 卡呈现 告警
SSD 硬盘使用 寿命	支持	支持	支持	支持	支持	支持	支持	iBMC 呈现告警
硬盘 Sense Code 错误	不支持	不支持	直通硬盘支持	JBOD 硬盘支持	不支持	支持	不支持	iBMC 呈现告警，PCH 硬盘支持 Linux，VMware 系 统下检测

获取信息描述	LSI 2200	LSI 2300	LSI3008	LSI 3108	软 RAID	PCH 硬盘	NVMe	备注
硬盘性能下降	不支持	不支持	直通硬盘支持	JBOD 硬盘支持	不支持	支持	不支持	iBMC 记录日志，支持 Linux 系统下性能检测
硬盘 SMART 信息	支持	支持	支持	支持	支持	支持	支持	数据可用于分析硬盘状态，iBMC 根据分析结果记录日志
expander 误码	不支持	不支持	支持	支持	NA	NA	NA	增长过快 iBMC 记录 SEL 日志，用于 辅助分析链路故障
硬盘日志	不支持	不支持	支持	支持	不支持	不支持	不支持	iBMC 用于日志收集分析
硬盘丢盘	不支持	不支持	支持	支持	支持	支持	不支持	iBMC 呈现告警
硬盘闪断	不支持	不支持	支持	支持	支持	支持	不支持	iBMC 呈现告警

说明

KunTai 服务器只支持软 RAID，PCH 硬盘，NVMe 硬盘功能；

配合 iBMA 软件，可以增强 iBMC 管理的 PCIe 卡和操作系统相关监管功能，实现对 PCIe 卡和操作系统故障识别能力，详情参见下表：

表 3-4 iBMA 获取的 PCIE 卡和操作系统故障信息

类型	状态描述	备注
CPU	CPU 占用率	iBMC 呈现告警，需要配置告警门限
内存	内存占用率	iBMC 呈现告警，需要配置告警门限
硬盘	硬盘分区使用率	iBMC 呈现告警，需要配置告警门限
以太网卡	光模块故障	iBMC 呈现告警，支持 Linux 系统检
	OAM 链路故障	iBMC 呈现告警，支持 Linux 系统检
	链路状态（LinkDown，NoLink）	iBMC 记录提示级别 SEL 日志
	物理网口带宽占用率	iBMC 呈现告警，需要配置告警门限

类型	状态描述	备注
HBA 卡	链路状态（LinkDown）	iBMC 记录提示级别 SEL 日志
CNA 卡	链路状态（LinkDown）	iBMC 记录提示级别 SEL 日志
IB 卡	链路状态（Disable）	iBMC 记录提示级别 SEL 日志，支持 Linux 系统检测
文件系统	Linux 文件系统只读	iBMC 呈现告警

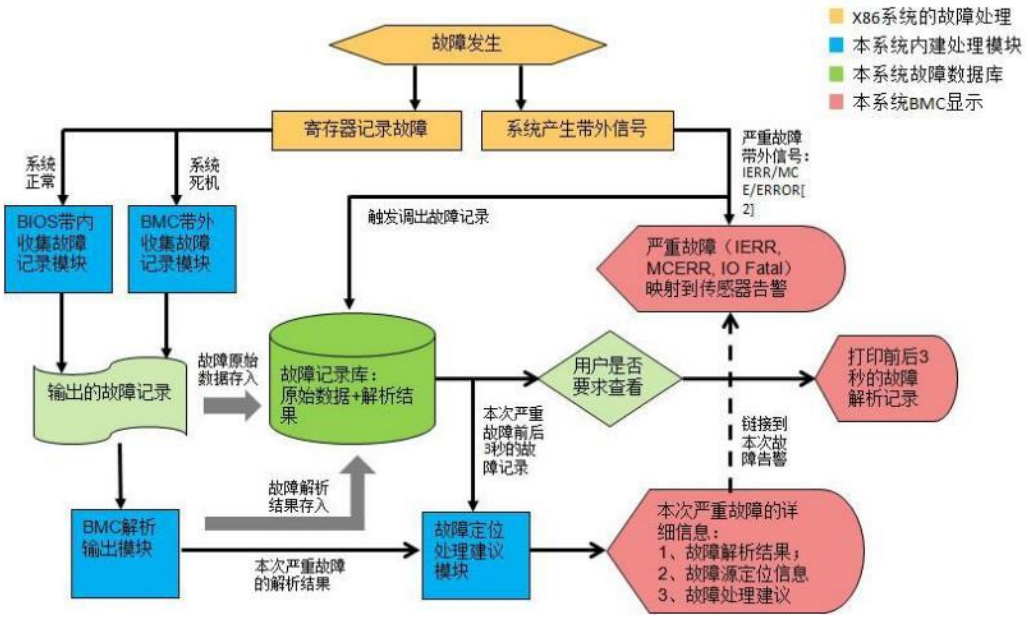
3.2.2 故障诊断

iBMC 集成了 MCE 故障处理系统，该系统建立了一套通用的以 iBMC 为管理中心的带外 的系统硬件故障处理系统，实现对硬件故障进行数据收集、记录、诊断、告警、日志 导出等功能。告警事件在 WEB 界面，通过部件健康树非常清晰的展示每个部件的故障 信息。

故障处理系统的使用场景：

1. 数据中心服务器运行过程中突然宕机，系统黑屏/无响应，由于 OS 不支持等原因没有记录下产生的 MCE 码，只有 iBMC 记录到 CAT ERROR 事件发生，无法获取更进 一步的信息判断问题所在。
2. 服务器长时间运行，整体上虽然未发生崩溃，但内部其实已经存在的大量的可恢 复/纠正的故障（如 ECC 等）。虽然这些故障暂时不影响业务，但也需要提前发现 和处理，避免发生灾难性故障。
3. 硬件故障出现概率低，难复现，主要靠人工经验判断，多次插拔/更换，效率低，对客户的影响大。
4. 故障发生后没有完整的故障记录。

图 3-4 x86 MCE 故障处理系统模块功能



故障处理系统的主要技术点：

- 实现了全方位自动的故障数据的抓取 通过带内带外不

同的故障数据收集技术的整合与自动切换。

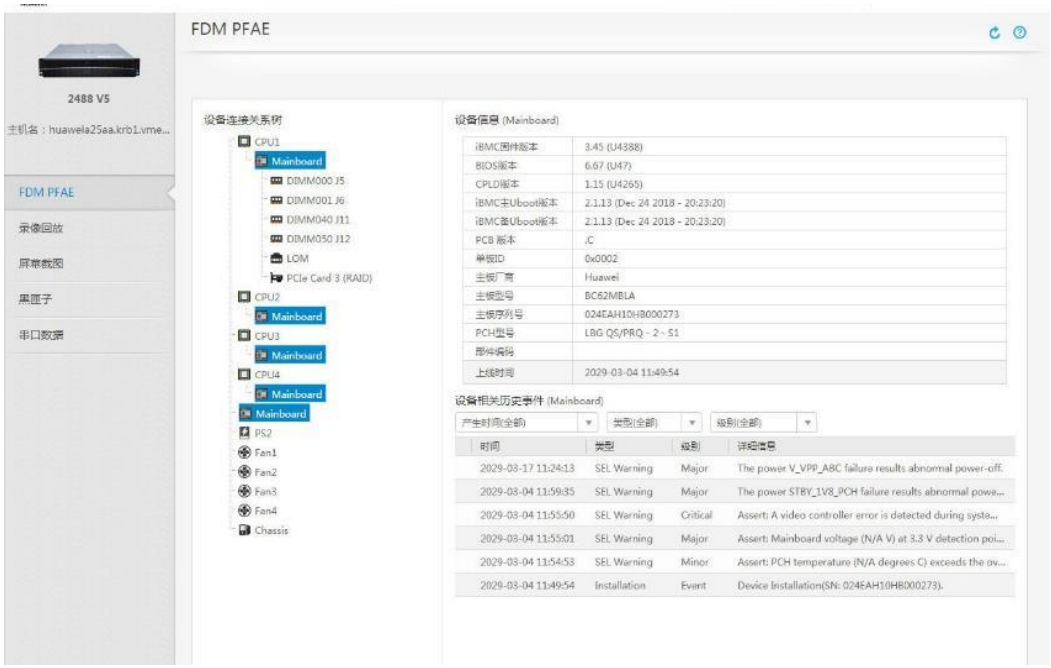
- 实现一个以 iBMC 为中心的完整可持续发展的带外故障处理系统
- 把所有的故障数据汇聚到 iBMC，由 iBMC 在带外做更进一步的记录、故障分析、 告警、日志导出等功能，克服了 OS 作为故障处理中心的能力不足、不可控、影响 系统性能等难题；故障支持定位到具体部件丝印。

3.2.3 FDM PFAE

BMC 提供故障分析功能，支持 CPU、内存、硬盘、RAID 卡、自研网卡的故障日志，主 要支持的能力如下：

- 故障预警历史事件的查询

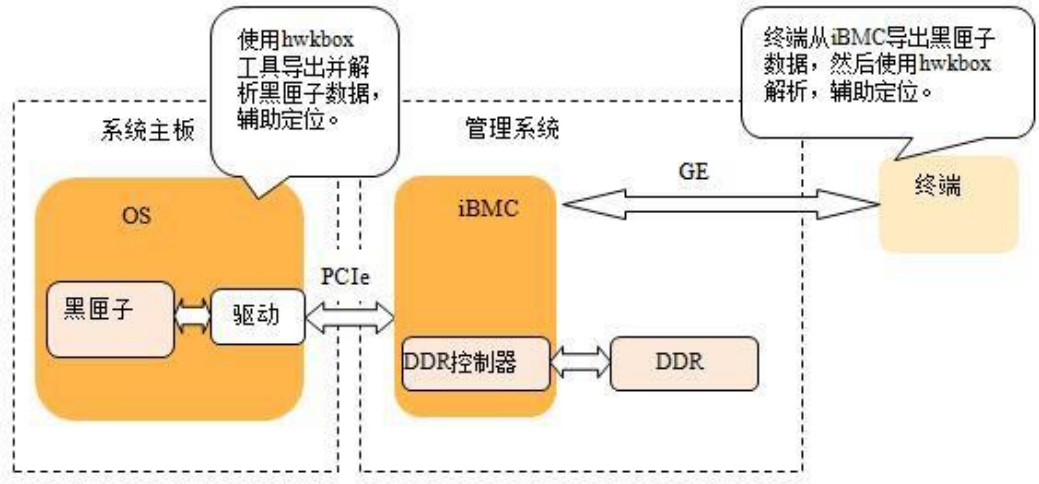
图 3-5 FDM PFAE



3.2.4 系统运行记录仪

iBMC 提供了系统运行记录仪功能，该功能由黑匣子（KBox）模块、iBMC、解析工具（hwkbox）三个模块协同完成，默认关闭。按照如图 3-6 所示，系统运行记录仪主要 实现了 linux 系统内核 panic 时的内核栈信息记录和导出，以及提供给第三方应用的读写接口，便于第三方应用记录自定义信息；记录的系统故障数据（也称黑匣子数据）不 会因系统重启和上下电而丢失，但 AC 掉电会丢失。

图 3-6 系统运行记录仪原理



应用场景一： 在内核 panic 触发时，注册的黑匣子模块自动抓取内核栈信息，并写

PCIe 设备，通过
DDR 控制器将定位信息保存到 DDR 中，最多 4M 字节数据。待系统重启后， 通过对
PCIe 设备读操作，系统侧定位工具把保存在 DDR 中的定位信息读取并解析，辅助定 位。 即使系统无法正常启动， DDR 内的信息，也可以通过 iBMC（如**图 3-7**）导出并使用专门工具解析(目前只能导入到系统 OS 下使用 hwkbox 工具解析)。

应用场景二：

系统第三方应用调用黑匣子模块写接口将运行日志记录到 iBMC 的 DDR 中，最多 4M 字 节数据；当应用异常时，系统侧调用黑匣子模块读接口或通过 iBMC 将运行日志读取并 解析以辅助问题定位。

图 3-7 黑匣子数据下载界面

3.2.5 开机自检代码

开机自检代码记录系统开机自检结果信息，表示当前自检通过还是发生具体故障，不 同的代码表示不同故障含义，通过查询故障代码表可定位到系统启动具体故障，如**图 3-8** 所示，[]内数字表示本次系统启动的故障码。

图 3-8 开机自检代码界面

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 系统事件管理

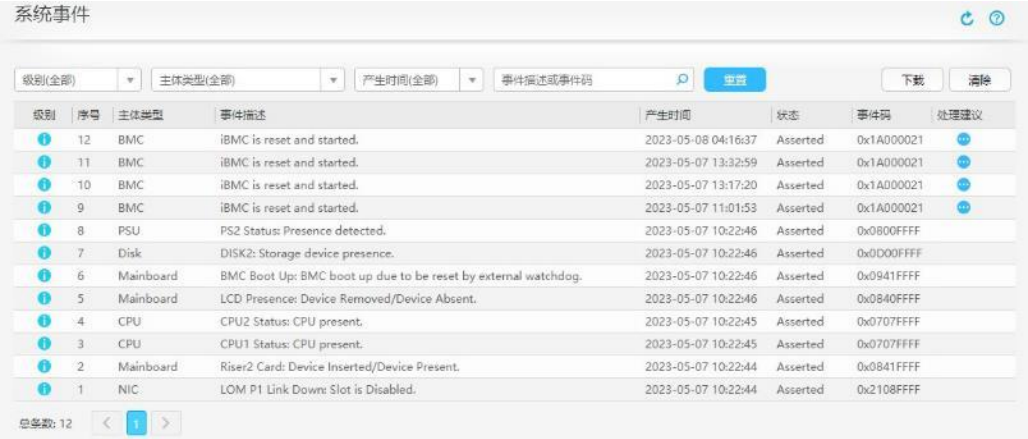
在可靠的故障检测基础上，iBMC 智能管理控制器还实现了丰富的告警管理功能。

- 告警监控覆盖全部硬件
- 日志描述详细
- 支持本地存储和归档
- 支持人性化的日志管理：可视化、过滤、排序、下载
- 支持多种方式(SNMP TRAP 和电子邮件、Syslog、Redfish Event)远程上报告警
- 支持多目的地上报告警
- 支持告警处理建议和事件码显示

系统事件实时写文件，当达到 2000 条事件记录后自动备份，最多备份 1 份文件，超过 1 份后自动将旧的备份文件删除。

系统事件界面可以查询所有系统事件并可以对其进行排序，过滤，清空等操作，如**图 3-9** 所示。

图 3-9 系统事件界面



系统事件参数说明如**表 3-5** 所示。

表 3-5 系统事件各参数说明

参数	说明
级别	事件的健康状态级别，包括：正常、轻微、严重、紧急。
序号	事件产生的顺序编号
产生时间	事件产生的时间。
事件描述	事件的描述。
事件主体	产生事件的部件
状态	事件的当前结果，包括：产生、恢复。
事件码	事件唯一识别码
处理建议	事件的指导处理建议

详细告警（级别为轻微、严重、紧急的事件）清单参考：**http://** support.huawei.com/enterprise/zh/server/ibmc-pid-8060757

3.2.7 故障上报

iBMC 支持实时监测硬件、系统的故障状态并通过 SNMP （Simple Network Management Protocol）TRAP、电子邮件、syslog、redfish event 方式上报到远程接收服务器。

如**图 3-10** 所示，SNMP Trap 支持 4 个接收目标，每个接收目标可配置接收地址、端口 号、启用状态和告警格式；支持根据严重性级别对事件上报过滤；支持 V1/V2C/V3 版 本，默认为 V1 版本，选择 V3 安全版本时需要从本地用户中选择一个 Trap V3 安全用户 以及配置 V3 鉴权和加密算法；Trap 消息中会携带主机标识和位置信息，主机标识可指 定单板序列号、产品资产标签、主机名中任意一个；支持对接收目标发送测试信息。

如**图 3-11** 所示，SMTP（Simple Mail Transfer Protocol）支持 4 个接收目标，每个接收目标可配置接收邮箱、邮箱描述和启用状态，支持对接收目标发送测试信息，

支持匿 名或用户验证登录 SMTP 服务器，支持启用 TLS 对邮件加密，支持邮件模板主题和发件 人定制。

如**图 3 Syslog 配置界面**所示，Syslog 功能支持开启/关闭，支持日志级别过滤，支持 4 个接收目标，每个接收目标可配置接收服务器地址（IPv4/IPv6/FQDN）、端口号、日 志类型和启用状态，支持对接收目标发送测试信息；上报日志支持安全日志、操作日 志和系统事件三种类型可配置，上报时携带主机标识；从安全考虑，Syslog 上报日志 支持 TLS 加密，也支持基于导入证书对 Syslog 收发两端进行合法性双向认证。

图 3-10 SNMP TRAP 配置界面

图 3-11 SMTP 配置界面

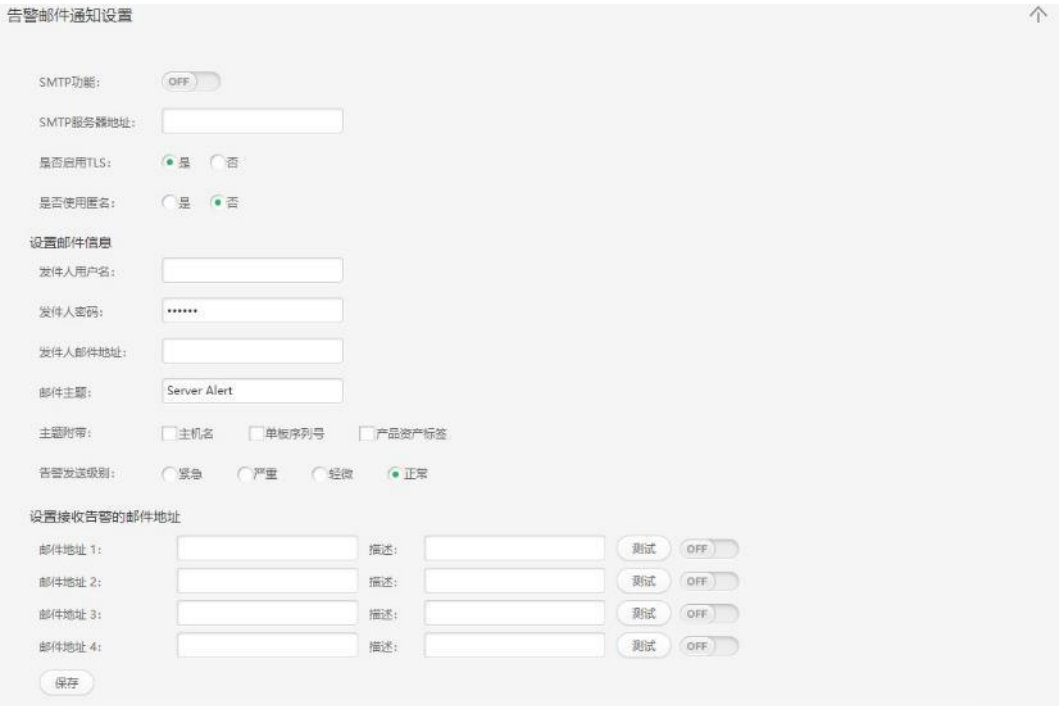
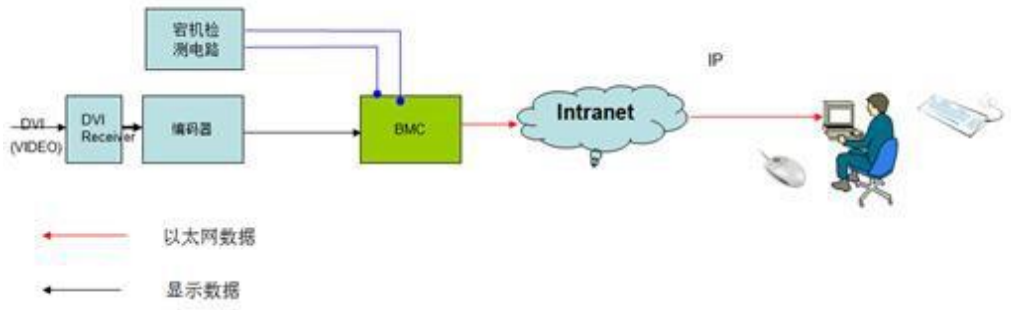


图 3-12 Syslog 配置界面

3.2.8 宕机截屏

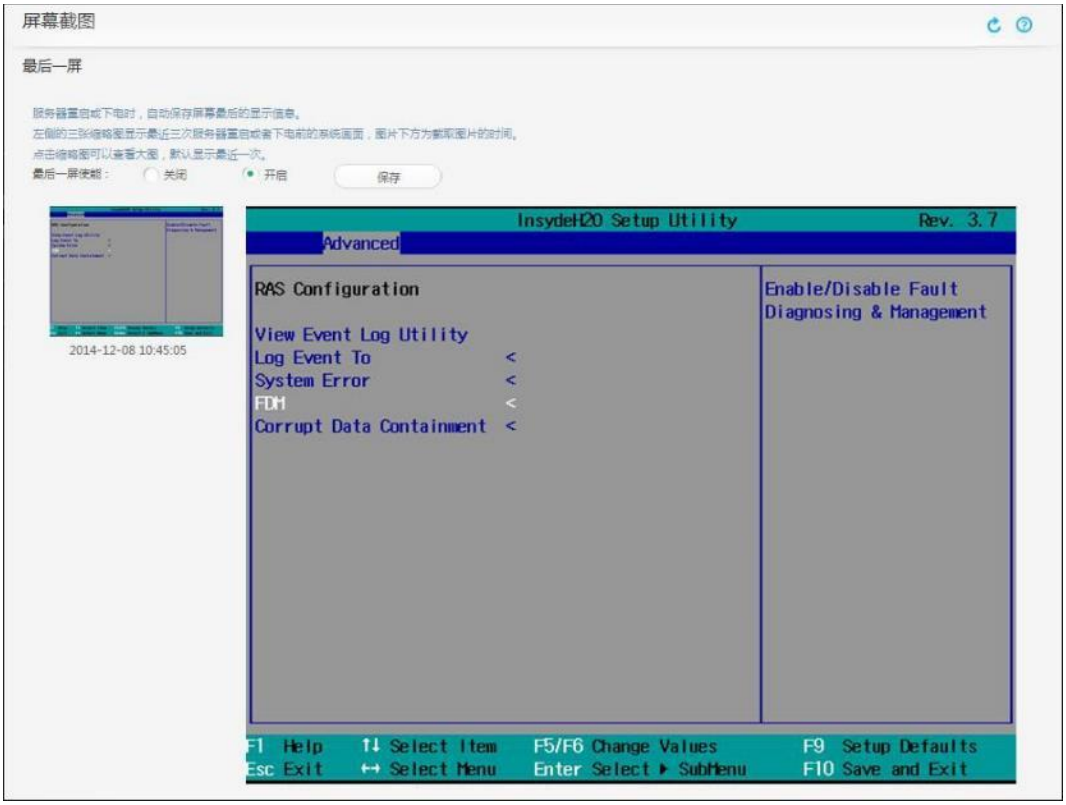
如**图 3-13** 所示，宕机截屏是 iBMC 在检测到宕机发生时将系统临终时刻的屏幕以指定的 格式保存在 iBMC 的存储空间内。当用户发现系统宕机后，可以通过网络登录 iBMC 查看 宕机屏幕进行故障定位或者远程将宕机屏幕获取到本地进行查看。

图 3-13 宕机截屏原理



iBMC 最多支持保存 3 个宕机截屏，并在下一次宕机时自动覆盖最旧的一次截屏数据。 可以参考“系统屏幕”通过 Web 查看宕机截屏，如**图 3-14** 所示。

图 3-14 宕机截屏界面



3.2.9 宕机录像

iBMC 在检测到系统宕机发生时会自动将宕机时刻前约一分钟的屏幕显示以压缩格式保 存到外部存储器中，支持 Host CAT Error、下电、重启场景的自动录像，其中 Host CAT Error 场景的录像文件保存在 iBMC 的 FLASH，其它两种场景的录像文件保存到 iBMC 的内存中。当用户发现系统宕机时，可以先将宕机录像文件导出到本地，然后再 打开 iBMC 的录像回放控制台在线播放，以帮助精确定位系统故障。

可以在“录像回放”页面中打开录像回放控制台，如**图 3-15** 所示。

图 3-15 录像回放控制台

3.2.10 屏幕快照

屏幕快照是 iBMC 提供的一项方便系统巡检的功能，用户可以通过远程命令行（CLI）和 Web 界面控制 iBMC 对当前系统的屏幕输出进行截取并保存。当用户需要查看时可以 通过远程 SFTP 将文件获取到本地使用图片查看软件浏览所有被巡检服务器的当前屏幕。

屏幕快照与虚拟 KVM 相比，省去了 HTTPS 登录过程，支持命令行接口，方便脚本集成 实现服务器巡检自动化。此外通过 Web 页面也可以获取当前系统屏幕快照。

3.2.11 通过命令行方式获取屏幕快照

命令格式

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

参数说明 加参数 wakeup 时该命令截取屏幕图片并唤醒

系统屏保。 使用指南

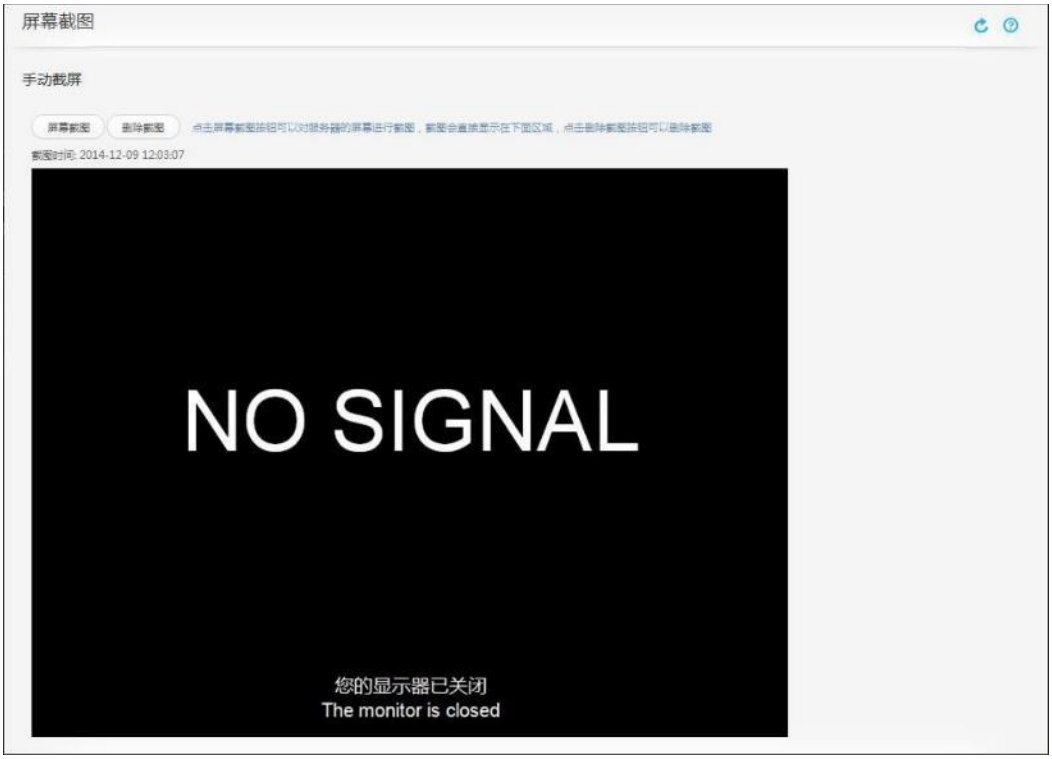
执行 printscreen 命令后，iBMC 将自动把截图文件保存至 tmp 文件夹下，文件名为 screen.jpg，查看此文件需要把图片文件通过 SFTP 传到可以查看.jpg 文件的客户端中

。

3.2.12 通过 Web 界面获取屏幕快照

通过 Web 界面，可以在“屏幕截图”的手动截屏页面下进行“截屏”操作获取当前的 系统屏幕快照，如**图 3-16** 所示。

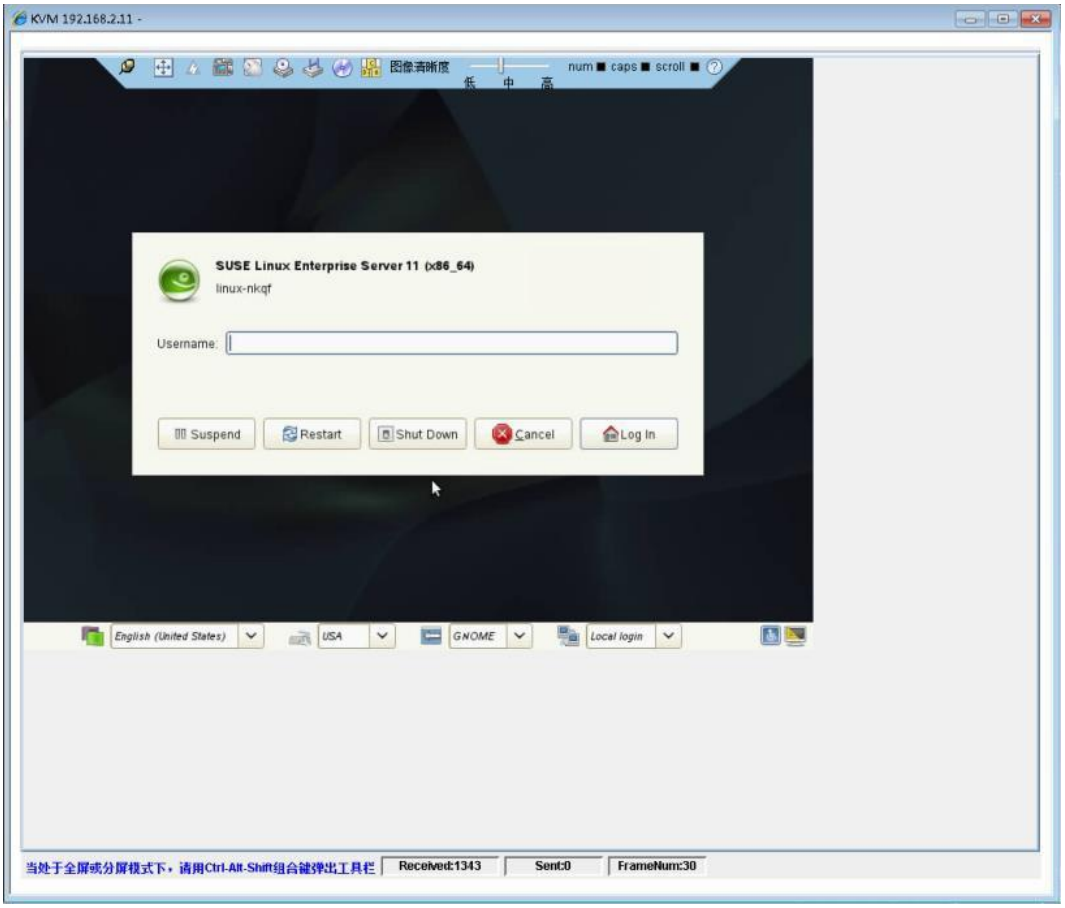
图 3-16 手动截屏界面



3.2.13 屏幕录像

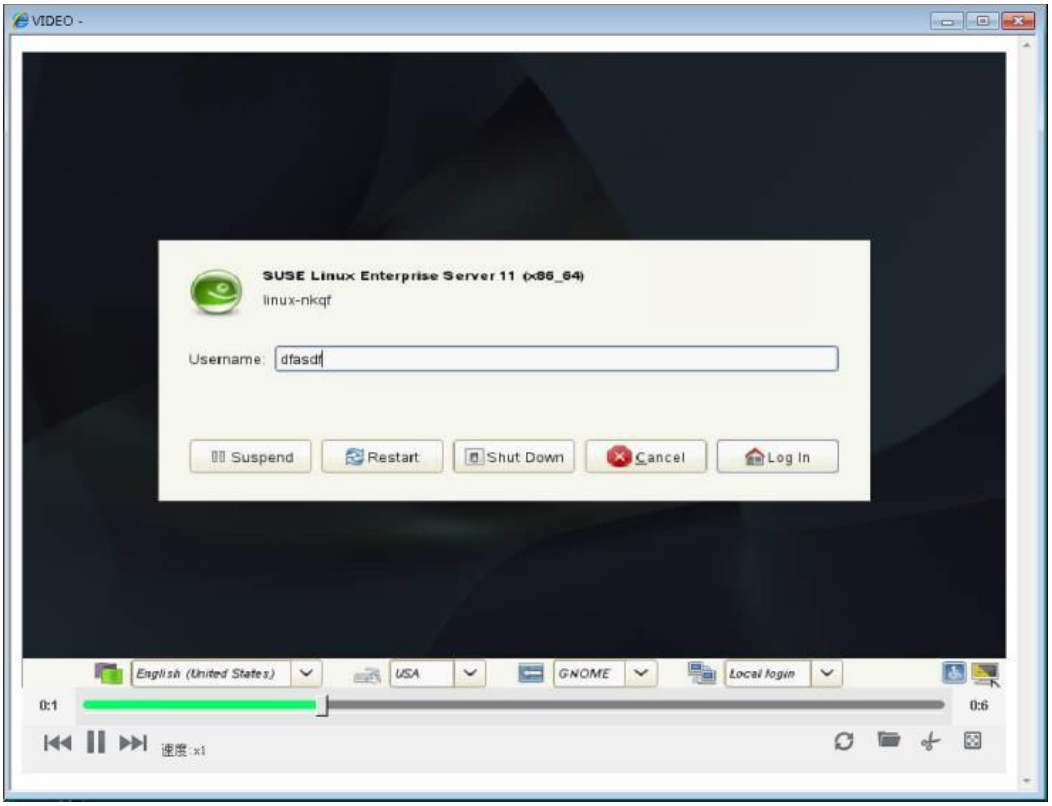
屏幕录像是虚拟 KVM 控制台上提供的一项远程 KVM 录像功能，需手动启动，录像格式 为自定义，录像数据保存在本地(打开 KVM 控制台的计算机)；当用户出于安全或者其 他需要，要将虚拟 KVM 操作过程记录下来时，可以通过启动屏幕录像功能来实现。屏 幕录像功能启动后，虚拟 KVM 控制台会自动将屏幕上的所有显示和操作都记录到自定 义视频格式文件中。

图 3-17 手动录像开启/关闭



iBMC WEB 界面集成了录像文件播放工具用于录像回放。

图 3-18 录像回放控制台



3.2.14 部件更换记录

在现网维护的过程经常遇到 CPU、内存、硬盘的故障，部分故障是由于部件被更换为不兼容部件从而产生故障，由于没有记录部件的历史信息，导致定位难度增大。对于概率性出现的故障，由于无法追溯到部件历史信息，不能做问题重现只能做理论分 析，导致故障不能定位到根因。

服务器的 CPU、内存、硬盘进行更换，在服务器重新上电后，iBMC 会产生一条部件更 换事件，事件描述信息中会包含更换前后部件的 SN 信息。对于硬盘，只有支持带外管 理的硬盘和 NVME 盘才能支持部件更换记录。以内存为例，在内存被更换服务器上电 后会产生如下事件：

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

3.2.13 部件编码管理

部件编码是在生产系统中唯一识别部件的编码信息，用于现网部件出现故障后需要更换新部件的场景，通过部件编码可以在生产系统中精确查询到新部件的信息，避免部件更换错误。部件编码可以在通过 WEB、REDFISH、告警日志以及一键收集里面查询，支持部件编码查询的部件为主板、电源、风扇、CPU、内存。

以内存为例，WEB 页面部件编码展示如下：

以内存为例，在内存出现故障后，告警描述展示的部件编码如下：

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

3.3 虚拟 KVM 和虚拟媒体

通过远程控制台界面可以使用虚拟 KVM、虚拟媒体和手动录像功能以及对系统上下 电、重启操作；远程控制台支持 JAVA 和 HTML5 两种技术实现，远程控制台 JAR 包默认 使用 CA 签名，控制台界面如**图 3-19** 所示，HTML5 控制台界面如**图 3-20**。HTML5 的远 程控制台支持美式、日式、意大利键盘。

远程控制台支持工作在窗口模式和全屏模式，当处于全屏或分屏模式下，同时按下 Ctrl Alt Shift 组合键可弹出工具栏。

远程控制台支持如下四种启动方式：

1. iBMC Web 或 URL 启动 JAVA 控制台，基于 JNLP 方式启动，避免 Chrome 版本 45 及 以上不支持 NPAPI 启动带来的影响。
2. 控制台独立启动，免装 JRE 环境，不依赖浏览器，支持 WINDOWS 7 32 位 /64 位，
   WINDOWS 8 32 位/64 位，WINDOWS 10 32 位/64 位，WINDOWS SERVER 2008
   R2 32 位/64 位，WINDOWS SERVER 2012 64 位，ubuntu 14.04 LTS，ubuntu 16.04 LTS，如**图 3-21**。
3. VNC 客户端启动，支持标准 VNC 协议及 RealVNC、TightVNC、UltraVNC、 TigerVNC 四款主流 VNC 客户端，如**图 3-22**。
4. iBMC Web 和 URL 方式打开 HTML5 控制台，通过 HTML JS 加载控制台。

表 3-6 各种启动方式对比

分类	优点	缺点	备注
嵌入 HTML5 控制台	1、无需安装 JRE，也不依赖 JRE。 2、无需下载程序包，HTML JS 加载	1、对浏览器版本有要求。 2、不支持虚拟文件夹功能。	

分类	优点	缺点	备注
嵌入 JAVA 控制台	1、支持全功能。	1、需安装 JRE。 2、高版本浏览器不支持 applet 启动，需要 切换为 JNLP 启动	
VNC 控制台	1、标准协议，兼容第三方客户端。 2、无需安装 JRE。	1、不支持虚拟媒体功能。 2、仅口令认证，无法按账号控制权限。	
独立 JAVA 控制台	1、自带 JRE，无需安装 JRE。	1、依赖 JRE。 2、工具太大，且携带不便。	

图 3-19 JAVA远程控制台(嵌入Web)

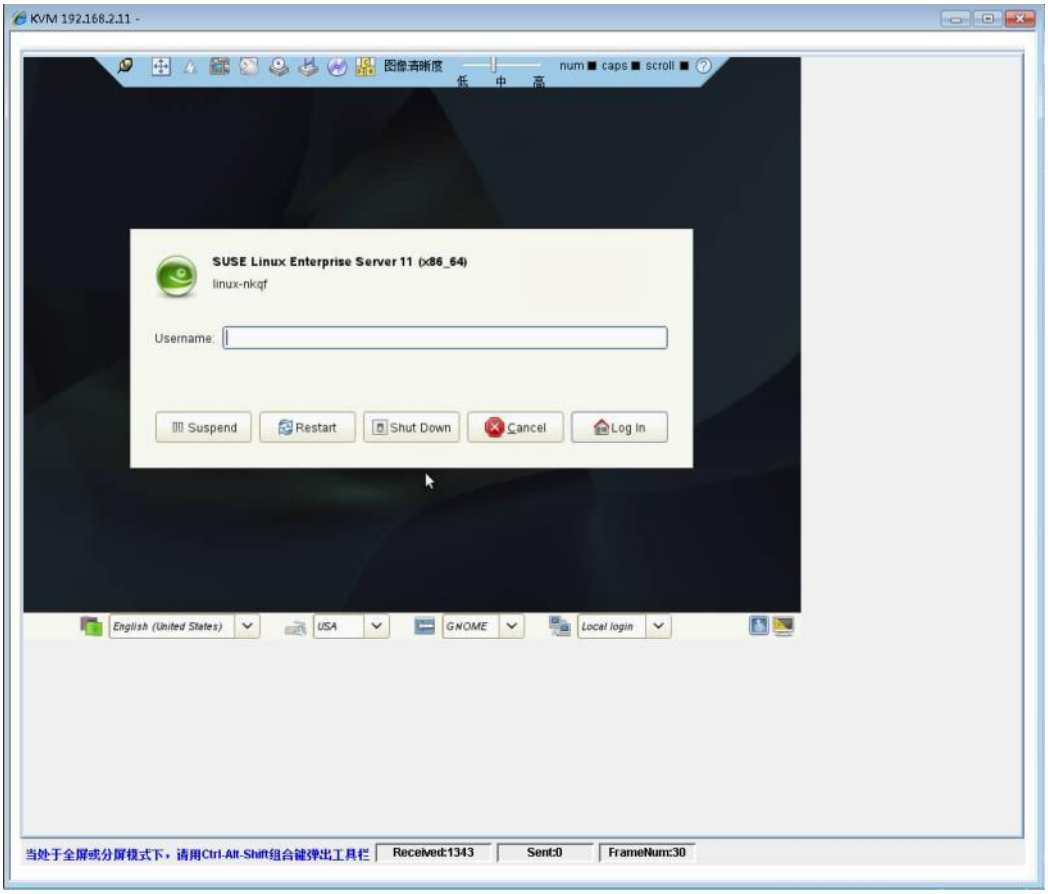
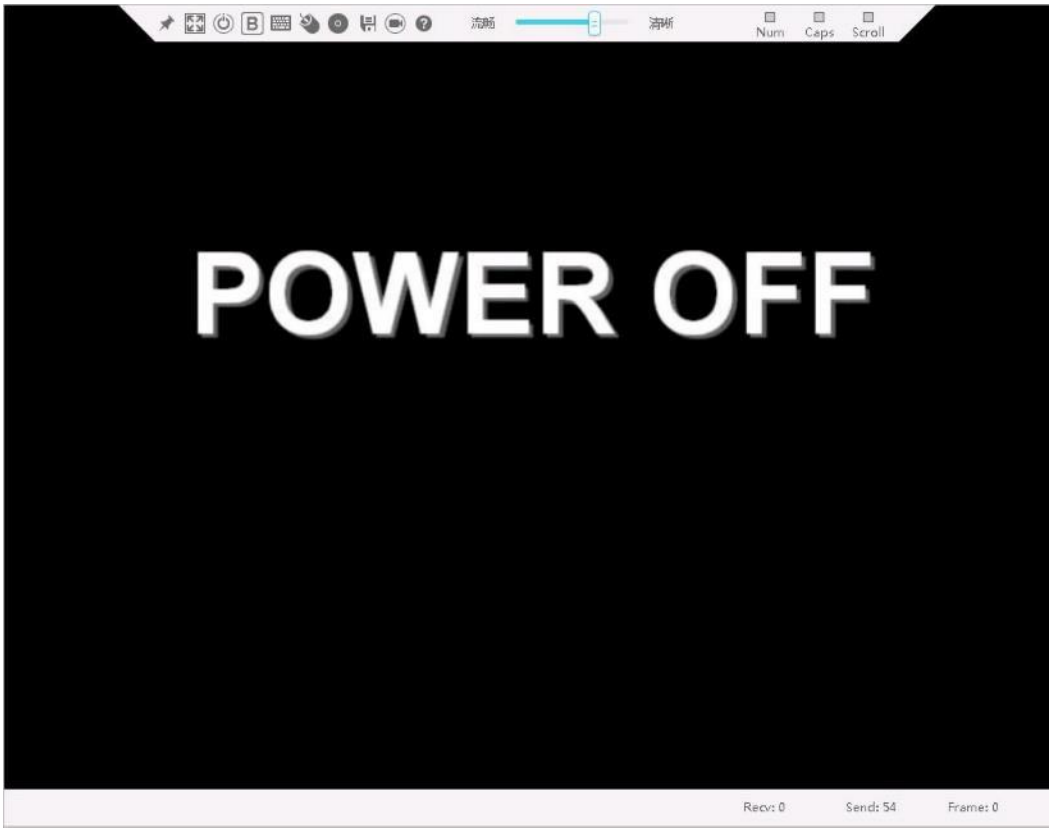


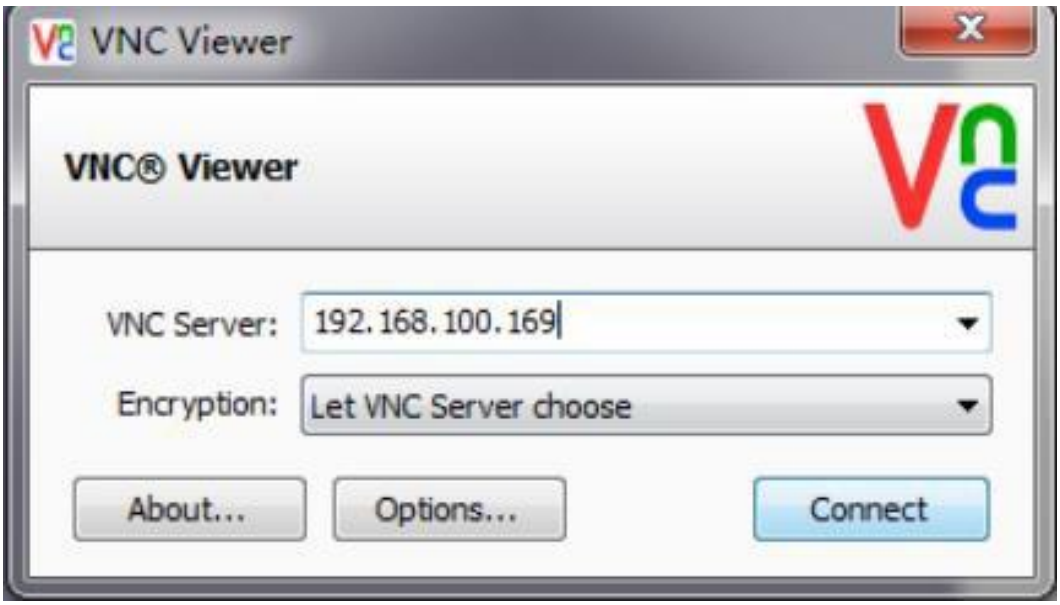
图 3-20 HTML5 远程控制台（嵌入 Web）



说明：基于 HTML5 的控制台，无需安装额外软件，支持的浏览器版本：IE10 及以上、Firefox 39 及以上和 Chrome 21 及以上。

图 3-21 JAVA 控制台登录界面（独立）

图 3-22 VNC 客户端（独立）



VNC 协议具有如下特点：

a. VNC 仅提供 KVM 功能，不支持虚拟媒体。

b. VNC 遵循标准协议，能与第三方 VNC 客户端对接。

c. 仅提供密码认证，有自己独立的密码。

d. 使用跟键盘布局有关，支持美式键盘和日式键盘。

图 3-23 VNC配置界面

3.3.1 虚拟 KVM

虚拟 KVM 是指用户在客户端利用本地的视频、键盘、鼠标对远程的设备进行监视和控 制，提供实时操作异地设备的管理方式；主要特点如下：

- 分辨率：最高分辨率为 1920*1280（实际能支持的最大分辨率跟 OS 有关），最低 分辨率为 640*480。
- 鼠标同步：远程服务器鼠标跟随本地鼠标移动，该功能需要远端服务器 OS 支

持，见**表 3-7**。

- 鼠标模式：支持绝对、相对和单鼠标三种模式。
- 工作模式：支持独占和共享模式，共享模式下，协同双方可以同时操作远端服务 器；独占模式下，同一时间只有一个会话。
- 运行环境：使用虚拟 KVM 功能，客户端需具备相应版本的浏览器、OS 和 Java 运行 环境，如**表 3-2** 所示。
- 色彩位：支持 32 位真彩色，最多 1677 万种色彩。
- 组合键：支持最多可发送 6 个键的组合键。
- 加密：视频、键盘和控制命令数据支持 AES 128 CBC 算法加密传输。

由于鼠标同步功能取决于 OS 是否支持提供绝对鼠标位置信息，所以对于不能提供绝对 鼠标位置信息的 OS，KVM 不支持鼠标同步功能。

表 3-7 不支持鼠标同步功能的 OS 列表(包括但不限于)

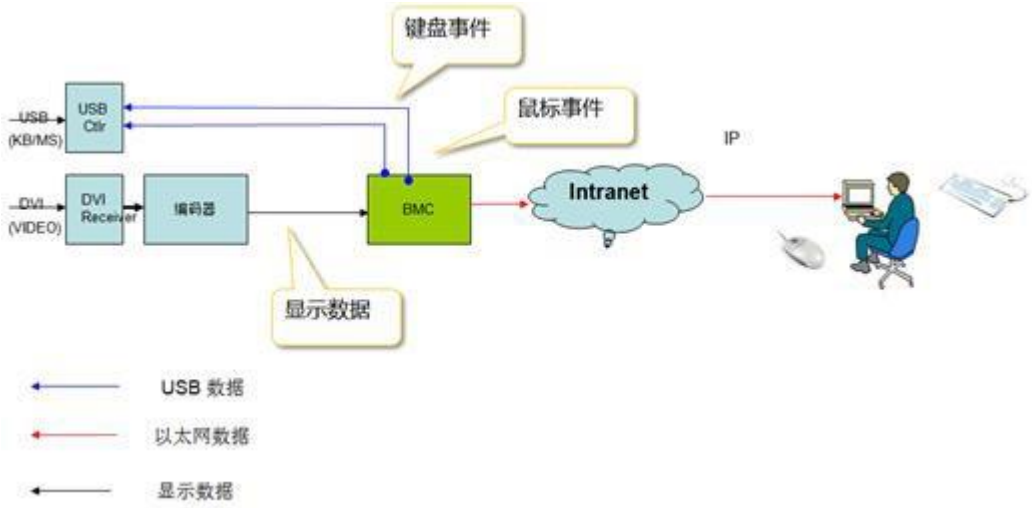
不支持鼠标同步功能的 OS 列表
SUSE Linux Enterprise Server 11 Service Pack 1 for x86(32Bit)
SUSE Linux Enterprise Server 11 Service Pack 1 for Intel EM64T(64Bit)

虚拟 KVM 的实现原理如**图 3-24** 所示：

- iBMC 将远端的显示数据压缩编码后通过网络传输到用户所在的客户端主机，由客 户端主机控制台解码解压缩后恢复显示。

- 虚拟 KVM 的控制台会将用户所在的客户端主机的鼠标事件和键盘事件捕获，通过 网络传输到远端，由 iBMC 智能管理控制器模拟远端的键盘鼠标将事件经由 USB 通 道输入到远端服务器业务系统上。

图 3-24 虚拟 KVM实现原理



3.3.2 3.3.2 虚拟媒体

虚拟媒体即通过网络在服务器上以虚拟 USB 光盘驱动器和软盘驱动器的形式提供对本 地媒体（光盘驱动器、软盘驱动器或光/软盘的镜像文件，硬盘文件夹和 USB Key）的 远程访问方式；虚拟媒体数据支持 AES 128 CBC 算法加密传输。使用虚拟媒体功能， 客户端需具备相应版本的操作系统和 Java 运行环境如**表 3-2** 所示。

虚拟媒体的实现原理是将客户所在的本地主机的媒体设备通过网络虚拟为远端服务器 主机的媒体设备，如**图 3-25** 所示。

图 3-25 虚拟媒体实现原理

iBMC 与服务器主机的数据通道采用 USB2.0 协议。目前 iBMC 的虚拟媒体具有以下功能 特性：

- 虚拟设备

  虚拟设备即将客户端的 PC 设备或者镜像文件映射到建立连接的服务器上，使得该服务器检测到一个 USB 设备。

  虚拟设备包括如下多种情况：

  -虚拟一个软驱设备

  -虚拟一个光驱设备

  -虚拟一个文件夹，包括本地和网络上的文件夹

  -虚拟软驱可以和其它虚拟设备同时使用

- 虚拟媒体性能

-虚拟光驱支持的最大传输速率为 32 Mbit/s，VLAN 时支持的最大传输速率为 24Mbit/s

-虚拟软驱支持的最大传输速率为 4M bit/s

- 制作镜像文件 将软盘或者光盘的内容制作成镜像文件并保存在硬盘上。
- CLI 挂载虚拟媒体
  在 CLI 中输入远程服务器的 IP、端口、文件路径、挂载协议及用户密码可以挂载虚拟媒体。基于 HTTPS 的可视化管理接口

iBMC 提供了基于 HTTPS 的 Web 可视化管理接口，可以实现通过简单的界面操作快速完 成设置和查询任务，支持的具体浏览器和 OS 版本如**表 3-2** 所示，以下图示以华为 2288H V5 产品为例，其它不同形态产品的界面可能存在差异。Web 界面支持中文、英文、日 文、法文四种语言，并支持在四种语言之间切换，默认与浏览器的语言一致。

可按照如下方式登录 iBMC Web：

步骤 1 在浏览器 URL 地址栏输入 https:// iBMC IP[:sslport]，如**图 3-26** 所示。

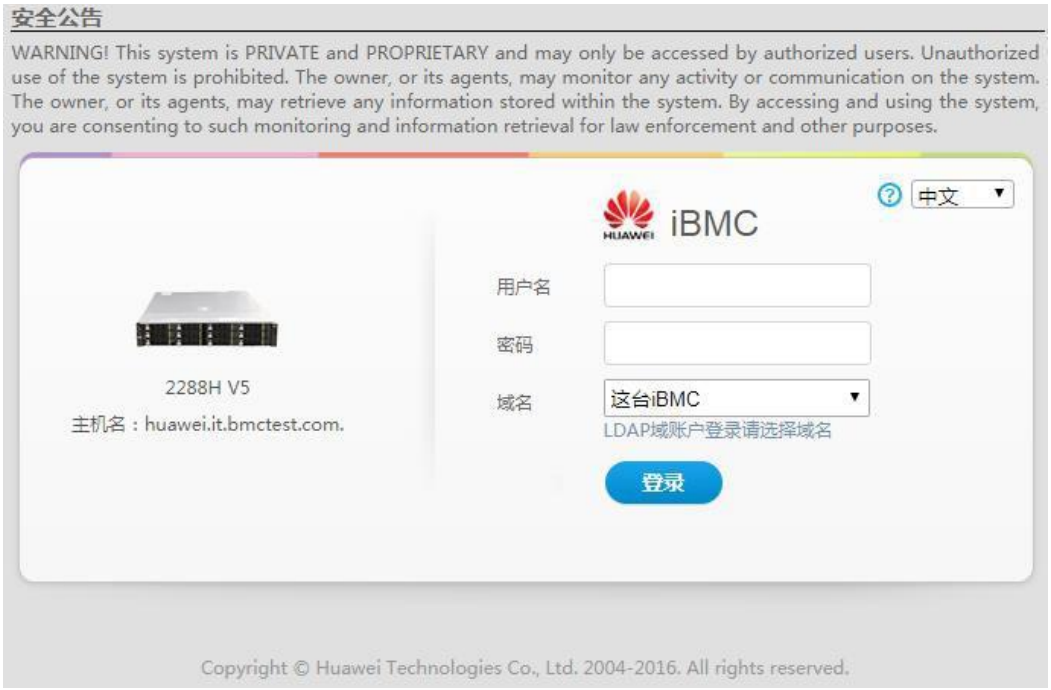
说明

端口号是可选的，若 port 不为 80 或 sslport 不为 443 则 IP 地址后面必须要带上端口号，端口号修改 方法参考 **3.9.4 证书管理**。

图 3-26 输入 iBMC地址

步骤 2 在用户登录界面中输入用户名和密码，若是域账号登录则选择登录到具体的域，然后 单击下方的“登录”按钮登录，如**图 3-27** 所示。

图 3-27 登录 iBMC Web



----结束

3.3.3 查看系统总体概况

总体概况界面显示系统当前基本情况，包括系统状态、iBMC 信息、系统配置信息、虚 拟按钮和节能统计信息，并提供常见操作接口链接，如**图 3-28** 所示。

图 3-28 总体概况界面

3.3.4 查看系统信息

系统信息界面详细显示当前系统的固件版本、资产信息和整机硬件信息。

3.3.4.1 固件版本

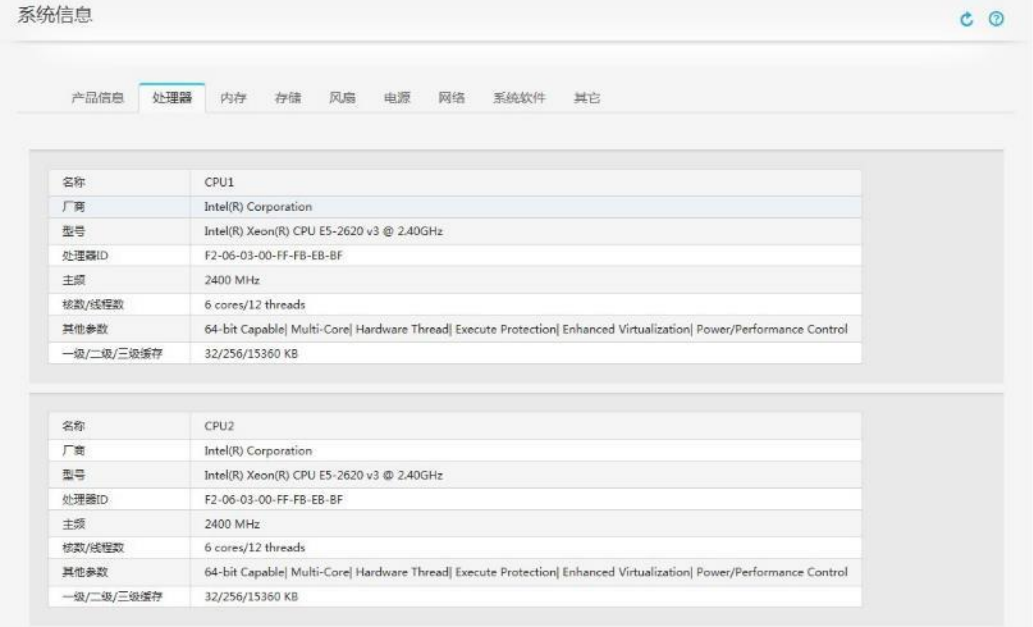
固件版本包括 iBMC 固件、BIOS、Uboot、CPLD 的版本，以及底板的 PCB、单板 ID、制 造厂商、型号和序列号，如**图 3-29** 所示。

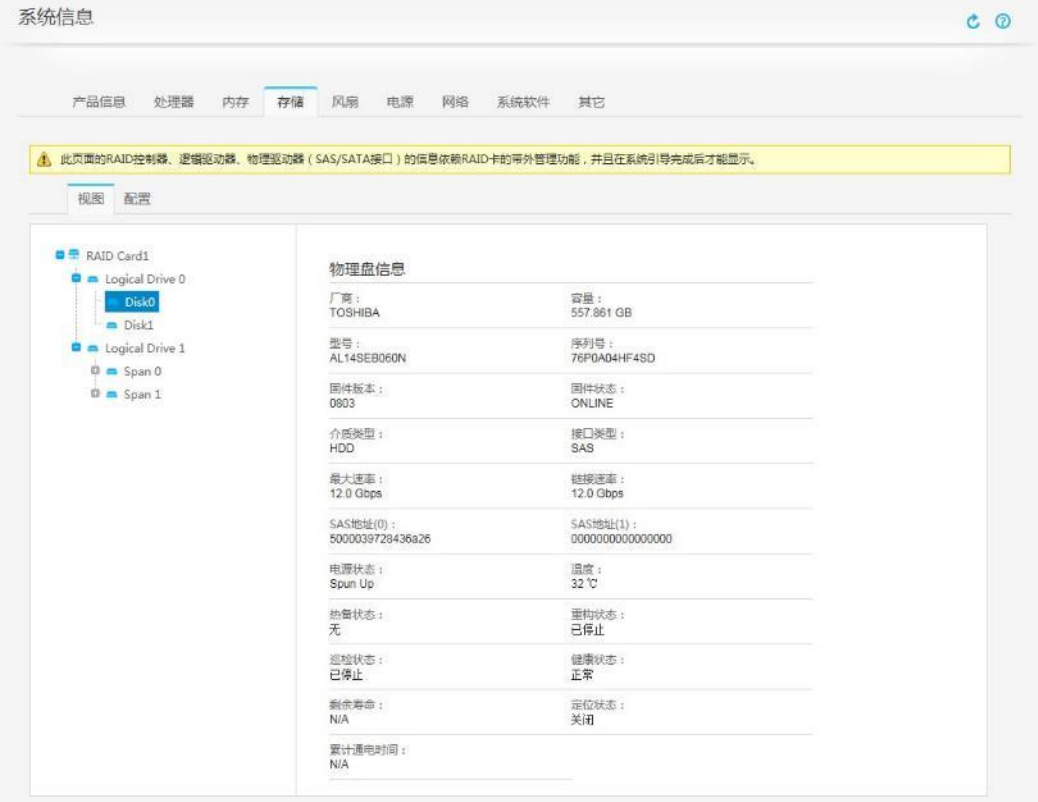
图 3-29 固件版本界面

3.3.4.2 整机硬件

整机硬件信息包括系统主要部件的最大配置数、当前配置数和型号，其中“网络”和 “系统软件”部分需要安装 iBMA2.0 软件，如**图 3-30** 所示。

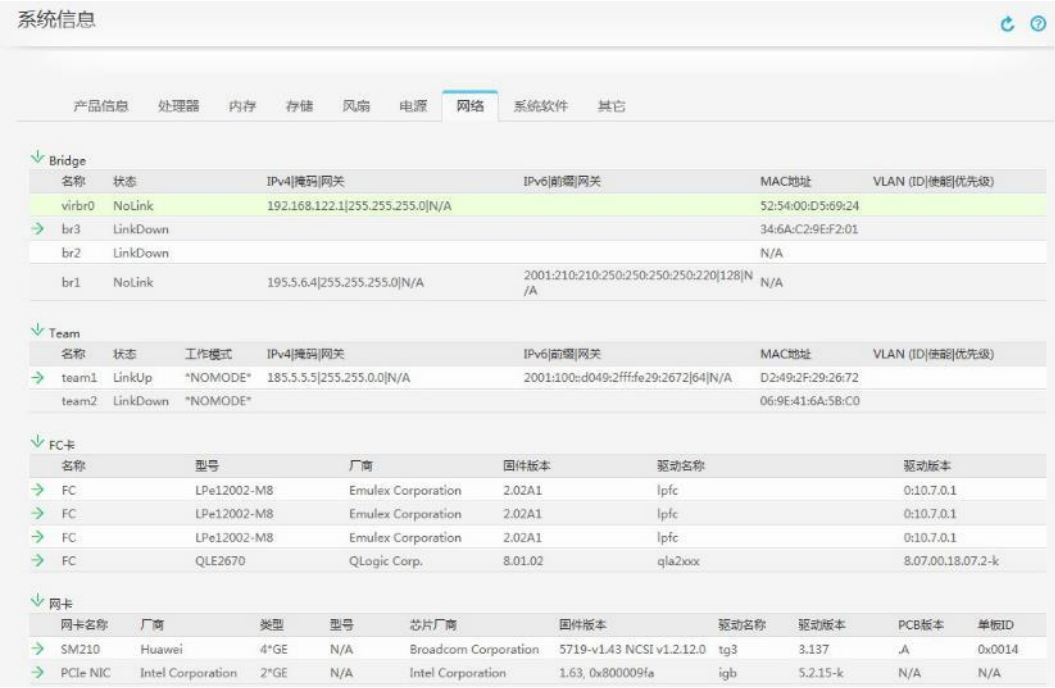
图 3-30 整机硬件界面



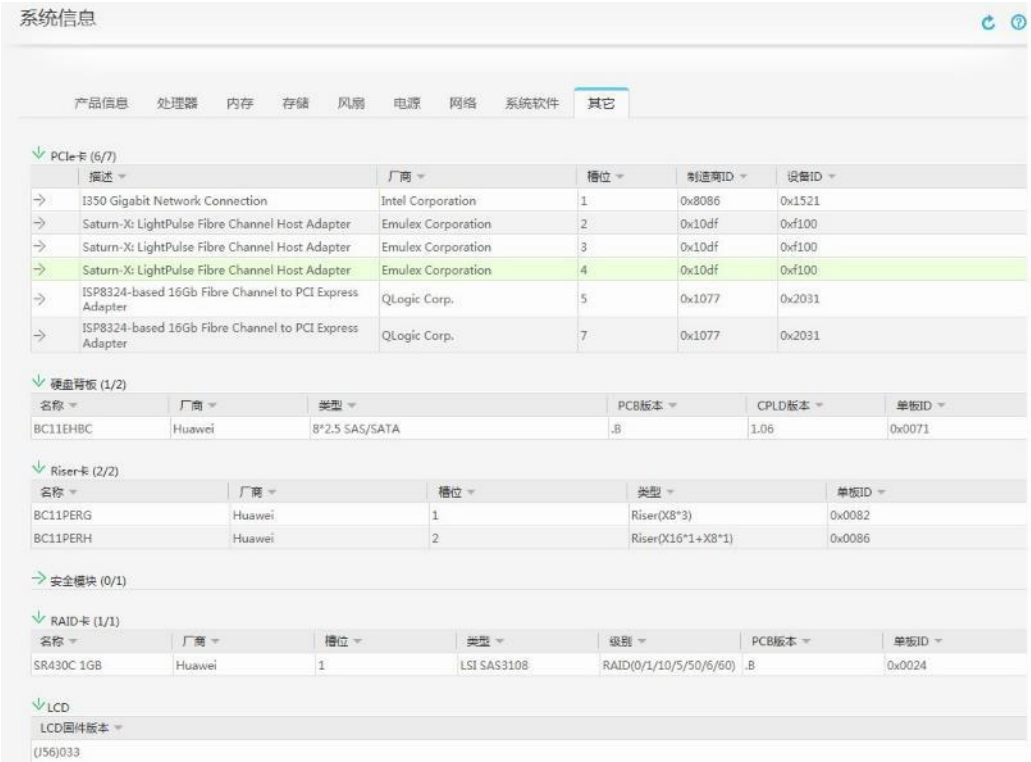

系统信息
产品信息 处理器 内存 存储 风扇 电源 网络 系统软件 其它
此页面的RAID控制器、逻辑驱动器、物理驱动器（SAS/SATA接口）的信息依赖RAID卡的带外管理功能，并且在系统引导完成后才能显示。
视图 配置
RAID Card1
Logical Drive 0
Disk0
Disk1
Logical Drive 1
Span 0
Span 1
物理盘信息
厂商：TOSHIBA
容量：557.861 GB
型号：AL14SEB060N
序列号：76P0A04HF4SD
固件版本：0803
固件状态：ONLINE
介质类型：HDD
接口类型：SAS
最大速率：12.0 Gbps
链接速率：12.0 Gbps
SAS地址(0)：5000039728436a26
SAS地址(1)：0000000000000000
电源状态：Spun Up
温度：32 ℃
热备状态：无
重构状态：已停止
巡检状态：已停止
健康状态：正常
剩余寿命：N/A
定位状态：关闭
累计通电时间：N/A


系统信息
产品信息 处理器 内存 存储 风扇 电源 网络 系统软件 其它
名称 (4/4) 型号 转速(RPM) 速率比(%)
风扇1 前/后 02310YKP 8056+ 3000/2640 27/26
风扇2 前/后 02310YKP 8056+ 2880/2640 26/26
风扇3 前/后 02310YKP 8056+ 2880/2640 26/26
风扇4 前/后 02310YKP 8056+ 2880/2640 26/26


系统信息
产品信息 处理器 内存 存储 风扇 电源 网络 系统软件 其它
槽位 (1/2) 厂商 类型 固件版本 额定功率 输入模式
2 HUAWE HUAWE 750W PLATINUM PS DC: 114 PFC: 114 750 AC/DC


系统信息
产品信息 处理器 内存 存储 风扇 电源 网络 系统软件 其它
Bridge
名称 状态 IPv4|掩码|网关 IPv6|前缀|网关 MAC地址 VLAN (ID|使能|优先级)
virbr0 NoLink 192.168.122.1|255.255.255.0|N/A 52:54:00:D5:69:24
br3 LinkDown 34:6A:C2:9E:F2:01
br2 LinkDown N/A
br1 NoLink 195.5.6.4|255.255.255.0|N/A 2001:210:210:250:250:250:250:220|128|N/A N/A
Team
名称 状态 工作模式 IPv4|掩码|网关 IPv6|前缀|网关 MAC地址 VLAN (ID|使能|优先级)
team1 LinkUp *NOMODE* 185.5.5.5|255.255.0.0|N/A 2001:100:d049:2fff:fe29:2672|64|N/A D2:49:2F:29:26:72
team2 LinkDown *NOMODE* 06:9E:41:6A:5B:C0
FC卡
名称 型号 厂商 固件版本 驱动名称 驱动版本
FC LPe12002-M8 Emulex Corporation 2.02A1 lpfc 0:10.7.0.1
FC LPe12002-M8 Emulex Corporation 2.02A1 lpfc 0:10.7.0.1
FC LPe12002-M8 Emulex Corporation 2.02A1 lpfc 0:10.7.0.1
FC QLE2670 QLogic Corp. 8.01.02 qla2xxx 8.07.00.18.07.2-k
网卡
网卡名称 厂商 类型 型号 芯片厂商 固件版本 驱动名称 驱动版本 PCB版本 单板ID
SM210 Huawei 4*GE N/A Broadcom Corporation 5719-v1.43 NCSI v1.2.12.0 tg3 3.137 .A 0x0014
PCIe NIC Intel Corporation 2*GE N/A Intel Corporation 1.63, 0x800009fa igb 5.2.15-k N/A N/A


系统信息
产品信息 处理器 内存 存储 风扇 电源 网络 系统软件 其它
计算机名称 redhat7
计算机描述 N/A
操作系统版本 Red Hat Enterprise Linux Server release 7.2 (Maipo)
操作系统内核版本 3.10.0-327.el7.x86_64
域名 (none)
iBMA版本 1.06
iBMA运行状态 Running
iBMA驱动版本 0.2.4
iBMA网卡驱动版本 0.2.4
iBMA设备驱动版本 0.2.4
黑匣子驱动版本 0.2.4



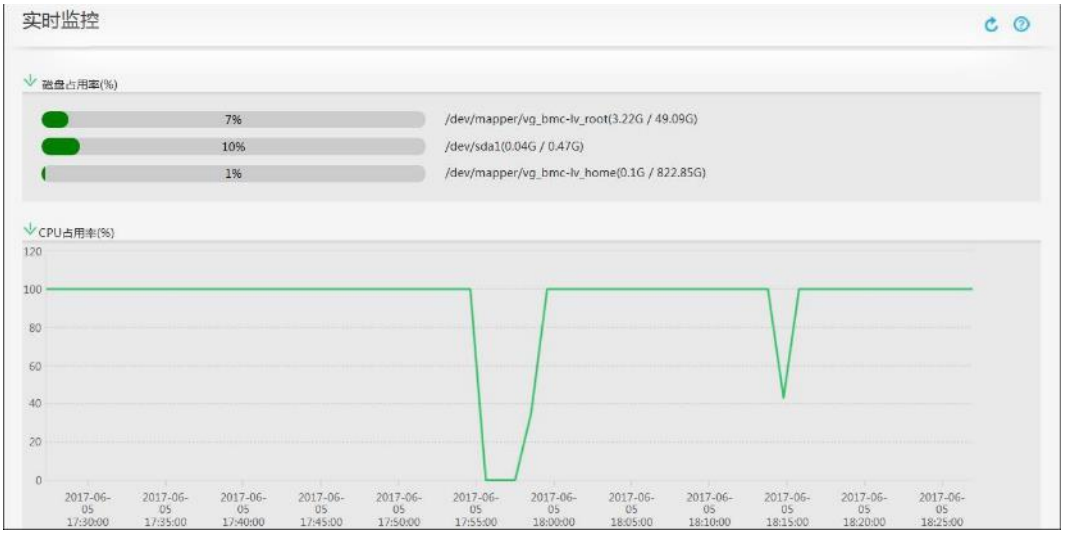
3.3.5 实时监控

实时监控包含部件、传感器、指示灯三个方面的信息和操作接口。

3.3.5.1 实时数据

如**图 3-31** 所示，该界面显示部件的实时数据的历史曲线图，目前主要展示了磁盘分区占用率、CPU 占用率、内存占用率和进风口温度，其中 CPU 占用率和内存占用率趋势图每 1 分钟采样一次，而进风口温度趋势图每 10 分钟采样一次，便于用户观察实时数据的趋势，以了解业务运行状况，CPU 占用率、内存占用率和硬盘分区占用率需要在 OS 侧安装 iBMA2.0 软件才能显示。

图 3-31 实时数据界面



3.3.5.2 传感器

传感器界面显示设备所有传感器信息，如**图 3-32** 所示，相关的参数如**表 3-8** 所示。

图 3-32 传感器界面示例

表 3-8 门限传感器界面各参数说明

参数	说明
传感器	传感器的名称。
当前值	传感器的当前值。
单位	传感器的取值单位。
紧急下门限	传感器值低于此下限值时，系统会产生紧急告警。
严重下门限	传感器值低于此下限值时，系统会产生严重告警。
轻微下门限	传感器值低于此下限值时，系统会产生轻微告警。
轻微上门限	传感器值高于此上限值时，系统会产生轻微告警。
严重上门限	传感器值高于此上限值时，系统会产生严重告警。
紧急上门限	传感器值高于此上限值时，系统会产生紧急告警。

3.3.6 设备定位

如图 3-33 所示，在设备定位界面，可以根据实际需要设置定位指示灯状态，通过点亮 定位指示灯，使用户可以在机房的大量设备中，快速定位到需要执行现场操作的设 备。

图 3-33 设备定位界面

3.4 域管理和目录服务

随着企业应用的发展，IT 基础架构的容量也越来越大，带来的资产管理和日常管理工 作量也呈数量级增长。为了应对越来越繁重的 IT 基础架构管理工作，iBMC 智能管理系 统提供了域管理和目录服务。

3.4.1 域管理

用户可以将所有被管理服务器加入一个统一的管理域并使用域名来访问被管服务器的 iBMC。如果在加入域的同时使用被管服务器的资产编号作为域名，还可以通过域控制 器实现自动资产盘点，大大降低 IT 资产管理的成本。

步骤 1 加入域。

1. 在 iBMC 的 Web 中打开“网络配置”界面，如图 3-34 所示。

   说明

   DNS（Domain Name System）是因特网的一项核心服务，将域名和 IP 地址相互映射，使用户可以通过域名直接访问网络，而不必去记住对应的 IP 地址。

2. 在图 3-34 中，用户可以配置 DNS 绑定网口及 DNS 信息获取模式。设置完毕后单击 “保存”执行操作。
3. 当用户选择“手动配置 DNS 信息”时，需要同时配置域名以及相应的首选、备用 DNS 服务器。

图 3-34 DNS 配置界面

步骤 2 在如图 3-35 所示界面中设置主机名。

图 3-35 主机名配置界面

----结束

3.4.2 目录服务

按照如图 3-36 所示原理，启用 iBMC 的目录服务，可以将所有 iBMC 的用户管理，权限 分配，有效期管理都集中到目录服务器上，避免大量的重复性用户配置任务，提高管 理效率。另外将用户集中到目录服务器上，也能大大提高 iBMC 智能管理系统的安全 性。

LDAP 标准优点：

1、可扩展性：可以在所有 iBMC 上同时动态支持 LDAP 服务器上新增账户的管理。

2、安全性：用户密码策略都在 LDAP 服务器上实施。

3、实时性：LDAP 服务器上账户的任何更新都将立即应用到所有的 iBMC。

4、高效性：可以将所有 iBMC 智能管理系统的用户管理，权限分配，有效期管理都集中到目录服务器上，避免大量的重复性用户配置任务，提高管理效率。

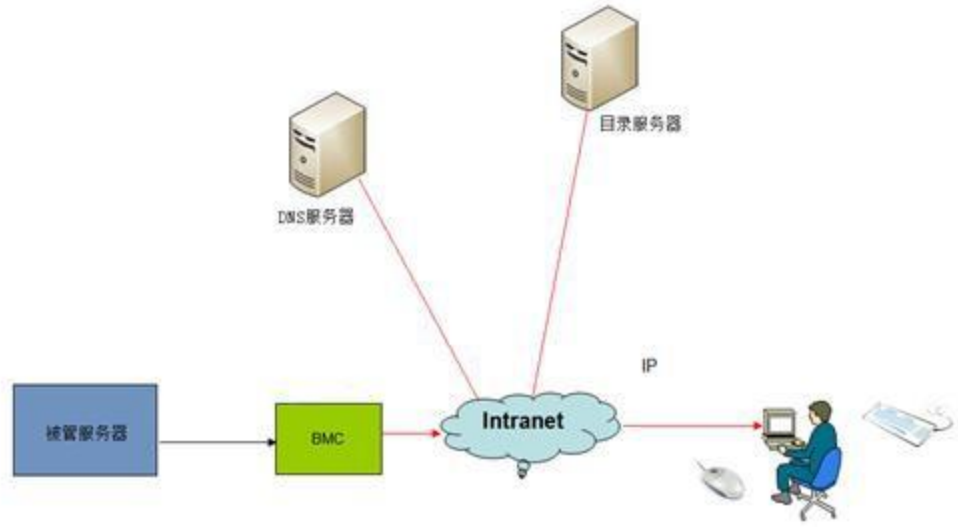
5、支持性：支持 Active Directory 和 openldap，支持 NTLM 认证机制

。 iBMC LDAP 特点：

- 从安全考虑，iBMC 只支持 LDAPS，支持 NTLM 鉴权机制
- 为了确保 LDAP 服务器的真实性，LDAP 支持对服务器合法性验证功能，该功能开 启后必须将 LDAP 服务器的根 CA 证书导入到 iBMC 才能使用 LDAP 功能，且域控制器地址必须配置为与根 CA 证书里的证书使用者通用名称一致，因为在验证服务器合法性时会匹配域控制器地址与根 CA 证书的使用者名称是否完全一致
- 支持多域功能，可配置最多 6 个域服务器，可指定登录到哪个域或自动匹配域。

- 支持在登录 Web 或通过 SSH 方式登录 CLI 时，使用 LDAP 账号。
- 支持微软 AD 和 OpenLDAP 的 LDAP 服务端。

图 3-36 目录服务原理



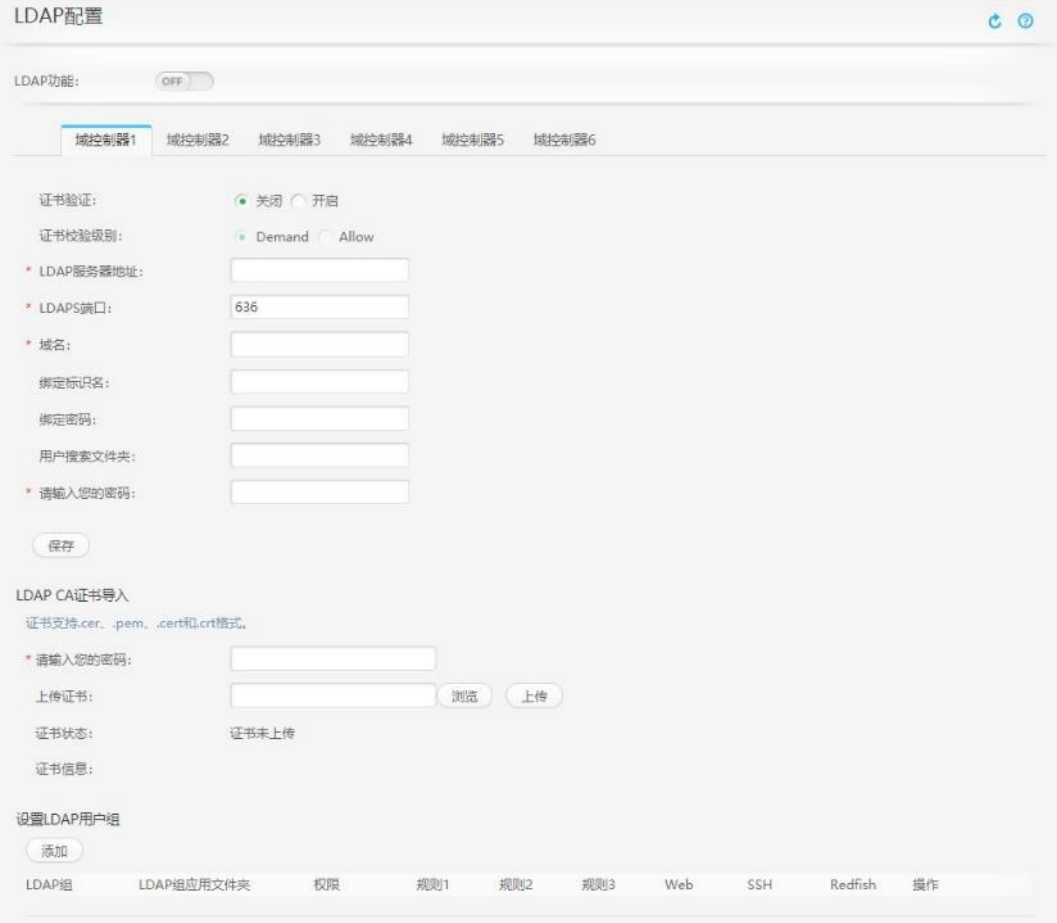
打开“LDAP 用户”界面，如**图 3-37** 所示。

说明

LDAP（Lightweight Directory Access Protocol）是一个访问在线目录服务的协议。LDAP 目录 中可以存储例如电子邮件地址、邮件路由信息等各种类型的数据，为用户提供更集中、更便捷的 查询。

在**图 3-37** 中，可以显示或配置 LDAP 用户的相关信息。

图 3-37 LDAP用户界面



通过 LDAP 用户界面可以完成的设置有：

- 启动或者禁止 LDAP。
- 启用证书验证。
- 设置 LDAPS 的端口号，默认为 636。
- LDAP 服务器 CA 根证书导入。
- 设置域控制器地址。

  域控制器地址为活动目录 active directory 所在服务器的 IP 地址或域名。域控制器 地址最大长度为 255 个字符。
- 设置用户角色组名。

  组名为配置活动目录 active directory 中登录 iBMC Web 界面的用户角色组的名称。组名最大长度为 32 个字符。
- 设置用户角色组域。

  组域为配置活动目录 active directory 中登录 iBMC Web 界面的用户角色组的域。组域最大长度为 255 个字符。
- 设置用户角色组特权。

  组特权为配置活动目录 active directory 中登录 iBMC Web 界面的用户角色组的特权。包括：规则 1、规则 2、规则 3、web、ssh、redfish 权限。

3.5 固件管理

iBMC 可管理的固件包括 iBMC 固件、BIOS、CPLD、LCD、电源，支持固件版本查询、固件升级、双镜像切换。

3.5.1 固件双镜像

为了提升系统可靠性，iBMC 使用了固件双镜像备份技术。当在网运行过程中出现 flash 误操作或者存储块损坏时，系统会自动切换到备份镜像运行，并通过告警提醒镜像冗 余降级。

3.5.2 通过 Web 切换镜像

在导航树上选择“系统管理 > 固件升级”，打开“固件升级”界面。如**图 3-38** 所示。

在固件版本视图窗口中，显示 iBMC 固件及 BIOS 固件的当前版本信息，并可进行镜像切 换和重启 iBMC 操作。

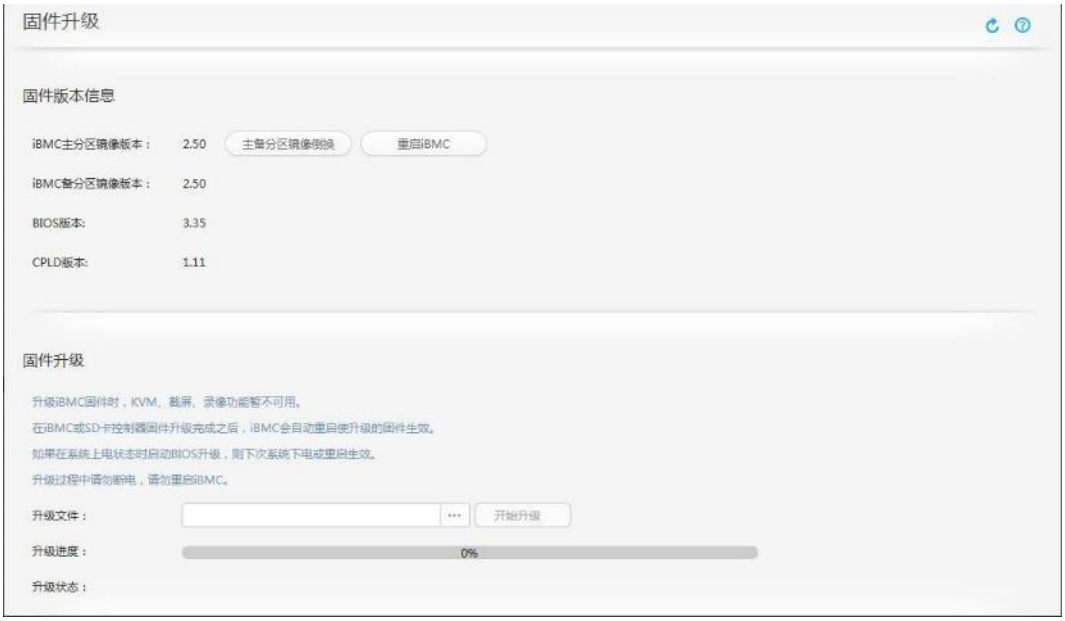
图 3-38 固件升级界面

3.5.3 固件升级

支持对 iBMC 固件、BIOS、CPLD（主板\背板\扣卡\扩展板）、LCD 固件、电源固件的 升级；其中 iBMC 固件支持主备镜像倒换回滚和本地固件更新，如**图 3-39** 所示。从兼容 性考虑，建议用户将 iBMC 主备镜像更新到同一个版本。

固件升级包都经过 RSA 2048 位算法数字签名和 AES128-CBC 算法加密。

图 3-39 固件升级界面



3.6 智能电源及调速管理

为了降低运营 TCO，iBMC 智能管理系统提供了多种智能电源管理功能。

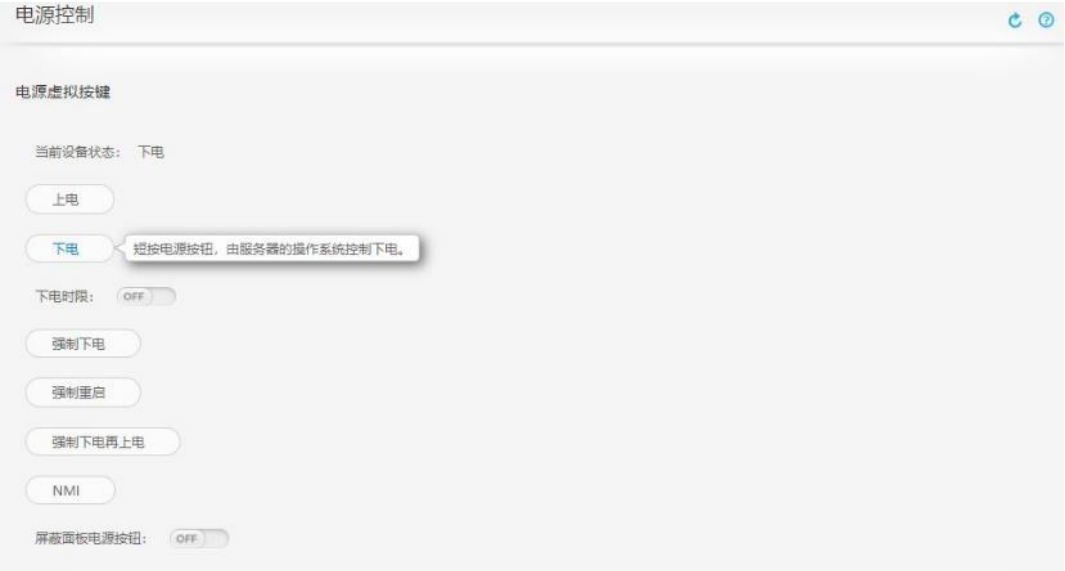
3.6.1 电源控制

电源控制界面提供对服务器的电源控制方式，如**图 3-40** 所示。 服务器电源控制方式

包括：上电、下电、强制下电、强制重启、强制下电再上电。

- 上电：表示对服务器进行上电。
- 下电：表示对服务器进行安全下电，iBMC 向 OS 发送 ACPI 中断，若 OS 支持 ACPI 服 务，则先走正常的操作系统关闭(将所有运行进程关闭)后下电，否则，只能等到 超过下电超时时间后，iBMC 将系统强制下电；效果相当于短按服务器面板上的电 源按钮。
- 强制下电：表示对服务器进行下电，无需等待 OS 响应，绕过正常的操作系统关闭 流程，效果相当于长按服务器面板上的电源按钮。
- 强制重启：表示对服务器进行冷复位，即：iBMC 直接拉南桥使系统复位，绕过正 常的操作系统关闭流程。
- 强制下电再上电：表示对服务器先安全下电再上电，实现按序重启，即：先走正 常的操作系统关闭流程并下电，若设置的安全下电超时时间内不能完成下电则强 制下电，最后再上电。
- NMI：表示向 OS 触发一个 NMI 中断，以收集内核堆栈信息并输出到控制台，便于 系统异常时定位。
- 屏蔽面板电源按钮：从安全和避免现场误操作考虑，支持对服务器面板电源按钮 禁用功能。

图 3-40 电源控制



在集群管理中，为避免多台服务器同时上电产生过流冲击，支持错峰上电：

- 机架服务器，2 秒内随机控制主机上电
- 刀片类产品(包括高密度产品)，根据槽位顺序延迟上电，每槽位至少延时 500ms

3.6.2 功率封顶

现代数据中心一直面临的一项挑战是企业正在消耗大量的电源、空间和冷却成本。而随着能源需求以及能源和冷却成本的大幅度上涨，日益增长的可用能源的容量预计在未来几年里将跟不上需求的增长。对于当前的数据中心来说，最急需解决的问题就是通过技术创新实现节能降耗。在传统的数据中心中，客户为保证数据中心无间断运 行，往往要耗费巨资来建设一套额外的电力基础设施。此外，IT 管理员通常会以过度 能源供应，来确保电力供应。iBMC 提供的功率封顶技术可以通过有效地对每一台服务 器能耗的准确控制，避免了能源的过度供应，有效地将能源中过度供应的部分能源用 于数据中心扩容。

在导航树上选择“电源与能耗 > 功率”，打开“功率”界面，如**图 3-41** 所示。

功率封顶功能通过设置系统的功率预期上限，当系统功率超过此上限值后，引导特定动作发生，从而保证机箱整体功率的合理分配。

系统启动过程中，iBMC 每隔 1 秒采集一次系统功率，总共采集 40 次或更多，去除无效 值，然后计算出平均值并乘以一个系数(每个产品可能不同)作为功率封顶下限参考值。

在**图 3-41** 中，根据实际需要设置功率封顶使能状态、封顶功率、封顶失败进一步动作，单击“保存”按钮。设置成功后，界面将提示“操作成功”。

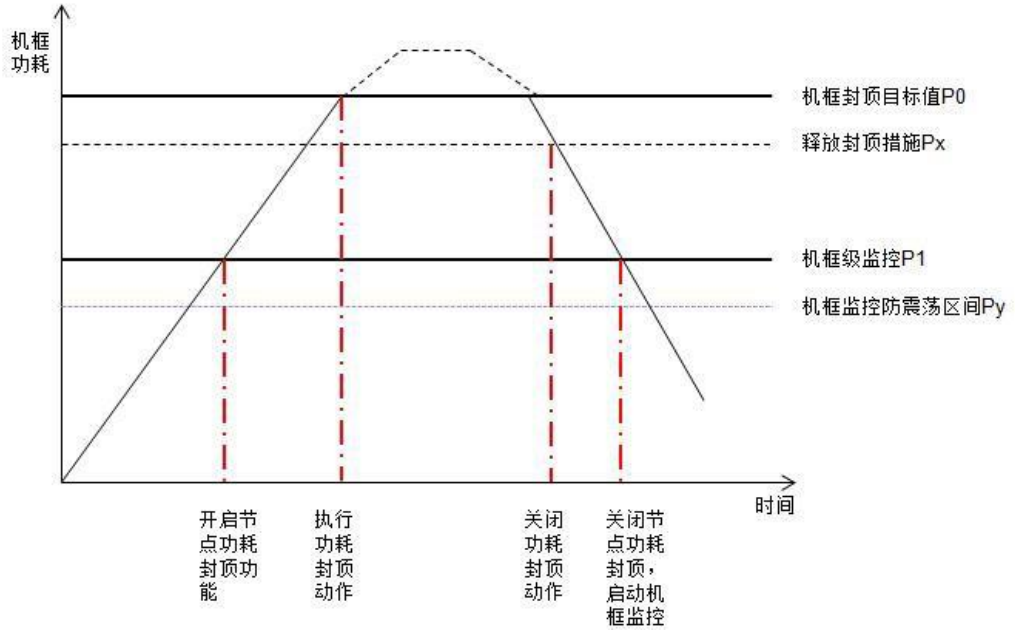
封顶失败进一步动作包括：

- 记录事件：封顶失败后在系统事件文件中记录一条日志，默认执行。
- 关机：封顶失败后，系统将在 15 秒内执行强制下电操作。

图 3-41 功率封顶界面

X 系列整框功率封顶功能是基于节点功率封顶实现的，目的在于控制整框（包括节点、电源、风扇等）的功耗。

图 3-42 功率封顶示意图



说明：

- 节点功率分配模式分为：均分模式(默认)、自动按比例、手动设置
- 开启门限值默认为 70%
- 定期获取机框功耗，当整框功耗超过 P1 值时（按照封顶目标值 P0*开启门限值计算），开启计算节点封顶，向 BMC 下发节点的功率封顶值
- 实时监控输入功耗，根据变化，重新调整各个节点的封顶值

图 3-43 整框功率封顶信息

```
~ # 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
```

3.6.3 功率统计和历史曲线

iBMC 可以提供准确的能耗监测并且能通过曲线提供统计，从而使管理员能够通过能耗 监测装置深入了解实际电力及散热资源的使用情况。用户可以根据历史数据对服务器 节能进行优化。

在导航树上选择“电源管理 > 功率统计”，打开“功率统计”界面，如**图 3-44** 所示。 在功率统计界面显示系统当前功率、CPU 总功率、内存总功率以及特定时间段的峰值功率、平均功率、累计耗电量。

单击“重新统计”按钮可以对系统峰值功率、系统平均功率和系统累计耗电量重新进行统计。

图 3-44 功率统计界面

在导航树上选择“电源管理 > 历史功率”，打开“历史功率”界面，如**图 3-45** 所示。

iBMC 每 10 分钟对系统功率采样一次并记录下来，在历史功率界面中，通过曲线可以显 示近期历史功率统计信息。单击“近一周”和“近一天”查看相应时间段的功率信 息；单击“重新统计”可对历史功率曲线和对应表格进行刷新；单击“下载”可以下 载历史功率信息。

通过此界面，用户可以更直观地观察到近期内设备的功率变化情况，更方便地了解到一段时间内设备的运行情况。

图 3-45 历史功率界面

3.6.4 电源主备

在满足业务功耗前提下，将部分电源设置为热备用或冷备用，提升电源功率转换效率。

- 特性原理

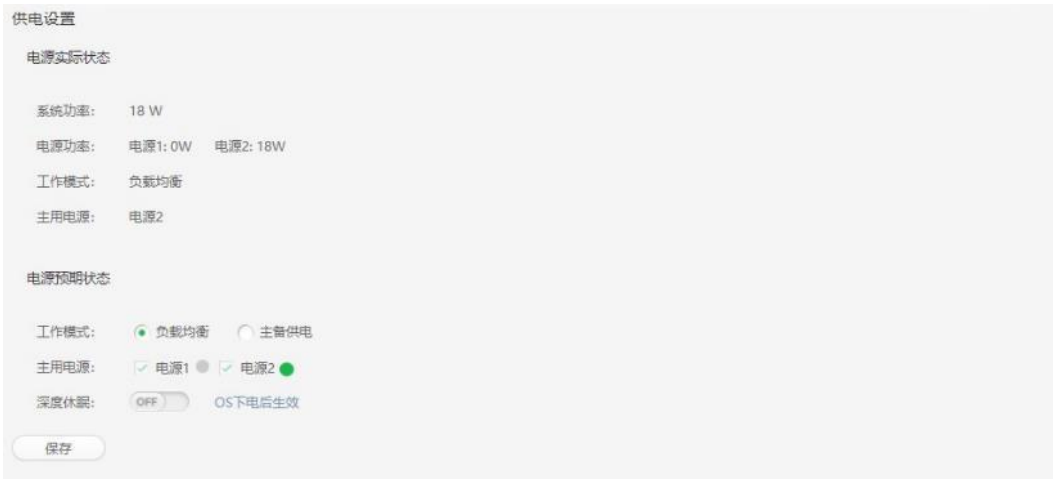
在满足业务功耗情况下，将部分电源的输出电压降低 0.3V，通过电压差抑制备用电源 电流输出，由主用电源提供系统供电；使电源处于热备用状态，一旦有主用电源异常 时，备用电源平滑切换为主用电源投入供电，不影响业务。

备用电源投入供电条件(主备模式切换为负载均衡模式)：

1. 主用电源拔出；
2. 主用电源输出电压低或无输出；
3. 主用电源温度过高、输入丢失、过流、过压；
4. 系统功率占主用电源额定功率总和的百分比达到上限(如：75%)时(注：占比小于下限，如 65%时，用户设置的备用电源切回到备用模式)，上下限值跟具体产品相 关。

主备供电界面如**图 3-46** 所示，提供电源供电总体工作模式、主用电源的设置接口。

图 3-46 主备供电界面



3.6.5 智能调速

不同客户或不同场景对服务器的性能、功耗、噪声等有不同需求，如：更高性能、更节能、更低噪音，还有客户希望能够灵活自定义。

智能调速（Smart Cooling）就是一个满足上述需求的特性。如图 3-47，四种调速模式说明如下：

- 节能模式：控制风扇转速在一个平衡点，使系统功耗达到最低。
- 低噪声模式：在满足散热前提下，降低风扇转速，使噪声最低。
- 高性能模式：提高风扇转速，控制关键部件的温度在较低水平，使系统性能最 高。
- 自定义：为满足客户特殊要求，提供对 CPU 目标温度和进风口温度区间自定义。

图 3-47 智能调速配置界面

3.7 系统串口重定向及运行记录

3.7.1 系统串口重定向

iBMC 提供系统串口重定向(SOL：Serial Over LAN)功能，即将原本只能从近端串口线输出的系统串口数据重定向到网络设备输出，并能接受远程网络设备的输入。支持 IPMI SOL 和命令行 SOL 两种方式，但这两种方式互斥，其中命令行 SOL 支持同时打开 两个 SOL 会话。如图 3-48 和图 3-49 所示原理，网管人员在远程通过网络终端就可以轻 松的查看系统串口实时输出数据，并能对系统进行操作干预，跟在近端使用系统串口 一样的效果。

图 3-48 系统串口重定向原理-x86

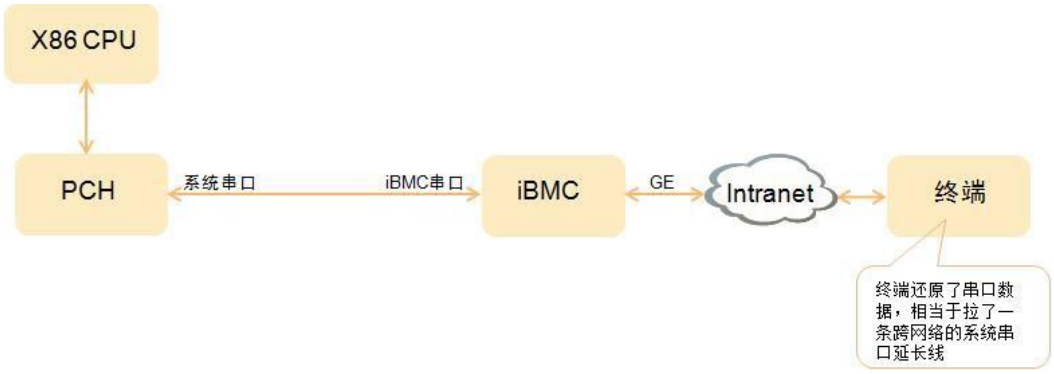
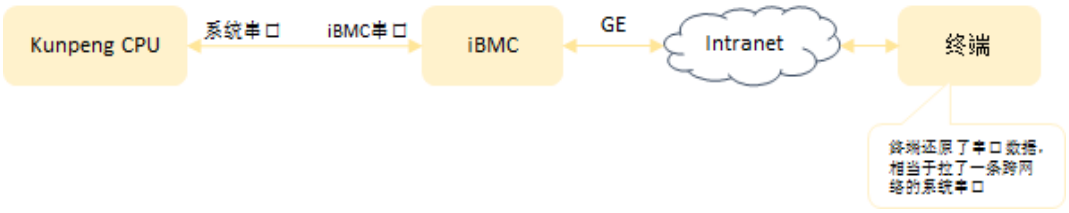


图 3-49 系统串口重定向原理-Kunpeng



3.7.2 系统串口信息记录

iBMC 提供系统串口信息记录功能。如图 3-50 和图 3-51 所示原理和展示方式，系统串口 信息记录将系统串口的实时数据记录到 DDR 中，循环覆盖，最多保留最近 2M 字节的系 统串口数据；当系统发生宕机或重启故障时，可以从 iBMC 导出信息记录并查看详细的 故障信息。

图 3-50 系统串口信息记录原理-x86

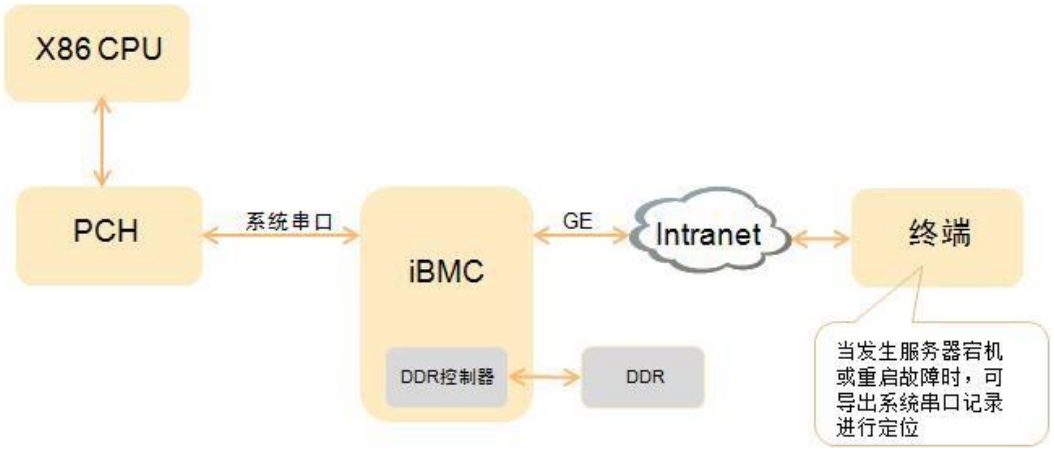
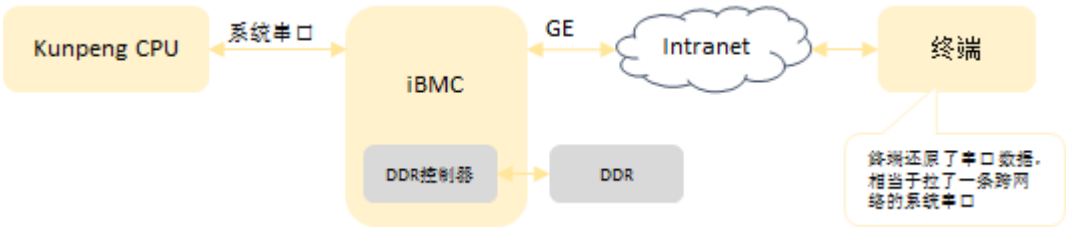
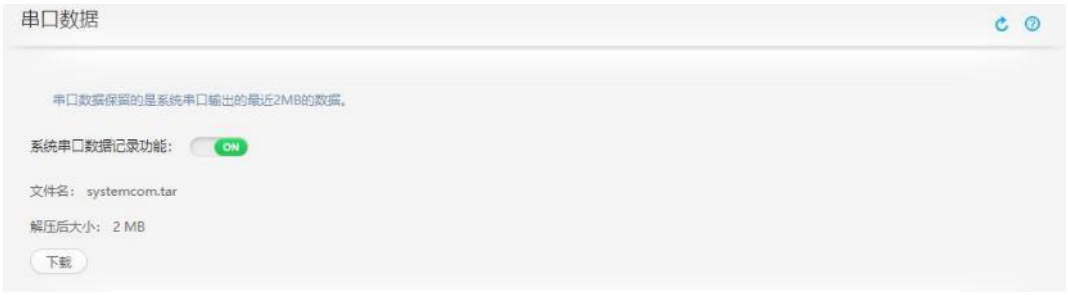


图 3-51 系统串口信息记录原理-Kunpeng



web 展示界面

图 3-52 Web 展示界面



3.8 安全管理

3.8.1 账号安全

服务器带外管理软件 iBMC 支持 CLI、SNMP、Web、IPMI、Redfish 等管理接口，并提供了统一的用户管理功能。最多支持 16 个用户，支持增加、修改和删除用 户。

账号安全包括：密码复杂度检查、禁用历史密码、密码有效期、密码最短使用 期、账号防暴力破解、账号手动锁定、在线用户注销。

密码复杂度检查：对用户配置的密码的复杂度进行校验，避免用户设置过于简单的密码。密码复杂度要求：

– 长度为 8 ~ 20 个字符。

– 至少包含一个空格或者以下特殊字符：`~!@#$%^&*()-_=+\|[{}];:'",<.>/?

– 至少包含以下字符中的两种： 小写字母：a ~ z； 大写字母：A ~ Z；数 字：0 ~ 9

– 不能是用户名或用户名的倒序。

– 新旧口令至少在两个字符位上不同。

禁用历史密码：支持用户配置保留历史密码的个数，设置的新密码不允许和历史 密码相同。

密码有效期：支持用户配置密码有效期时间，密码达到有效期后必须修改新密码 才能登陆；密码有效期小于 10 天时，系统会提示用户修改密码。

密码最短使用期：设置一个密码后，要使用的最短时间，在此时间内不能修改密 码；设置密码最短使用期的目的在于防止频繁修改密码而重复使用历史密码的风 险，确保密码安全。

账号防暴力破解：账号支持基于用户连续多次登录失败锁定，及 SNMP 超长团体 名

的防暴力破解机制；

– 登录失败锁定：支持登录失败次数，锁定时间的配置；当用户连续输入错误 密码的次数超过设置的“错误次数”时，该用户被锁定。用户被锁定后，在 锁定时长内不能继续登录，可以通过管理用户登入命令行手工解锁。如不进 行手动解锁，系统会在超过锁定时间时自动解锁。

SNMP 超长团体名：启用 SNMP 超长团体名后，设置的团体名必须大于等于 16 个字符，团体名设置也支持复杂度检查，防止设置简单团体名带来的风险。

3.8.2 认证管理

用户和上层管理系统通过 Web、CLI、SNMP、IPMI、Redfish 接口对 iBMC 的访问都需 要进行认证。认证通过后才能进行设备的管理配置和信息查询等操作。

iBMC 支持本地认证、LDAP 两种认证模式。支持“用户名 + 密码”认证、SSH 公钥认证、USB Key 证书的双因素认证以及重要操作的二次认证。

SSH 公钥认证：SSH 支持用户名、密码和公钥方式认证，公钥方式适合于自动配置工具，无需输入密码的交互步骤。

SSH 公钥认证有如下优点：

- 登录验证时无需交互密码
- 密钥长度很长，不容易被人偷窥或猜测到

支持 RFC 4716 和 OpenSSH 格式的公钥，公钥类型为 RSA 或 DSA。当公钥类型为 RSA 时，支持长度为 2048 位和 4096 位；当公钥类型为 DSA 时，支持长度为 1024 位和 2048 位。

每个账号只支持配置一个公钥，公钥导入支持文本输入和文件导入，导入后可查看该公钥的哈希值。基于更多安全考虑，启用 SSH 公钥认证后可禁用 SSH 的密码认证方式。

双因素认证：双因素认证是使用客户端证书密码以及证书来进行认证，登录时需要同时拥有客户端证书及证书密码才能认证通过，解决了传统的账号口令认证中口令泄露导致的入侵问题。双因素认证开启后，只有客户端证书被 iBMC 中导入的 CA 根证书验证 通过，且跟导入到 iBMC 中的客户端证书一致，才允许登录，当前只有 WEB 支持双因素 认证。双因素认证开启后不支持基于用户口令、LDAP 的认证，主要特性下：

- 支持基于客户端浏览器中导入证书和 USB KEY 中存储证书两种方式；
- 最多支持导入 16 个不同的 CA 根证书；
- 开启双因素认证后，不支持双因素认证所有接口会关闭，只保留 SNMP、IPMI 接 口，跟网管软件 esight 对接；双因素认证功能默认关闭，可以通过 Web、

SNMP 接 口配置开启；

- 支持证书吊销检查，默认关闭，吊销检查开启后，已被吊销的证书不允许登录；

典型应用场景：基于 USB KEY 的双因素认证解决了传统账号口令认证中口令泄露而导致的入侵问题，使用时需要同时拥有 USB KEY，且知道 USB KEY 的 Pin 码，才能登录。使用时需要先把申请的证书和 CA 导入到 BMC 中，然后在登录的客户端中插入 USB KEY，通过浏览器连接 iBMC WEB 时，需要输入 USB KEY 的 Pin 码，才能把证书导入到 浏览器发送到服务端进行验证。

二次认证：对于重要的管理操作，如用户配置、权限配置、公钥导入会对已登录用户 进行二次认证，认证通过后才能执行重要操作，防止用户登录后没有断开链接，被其 它非法用户执行恶意操作。

3.8.3 授权管理

- iBMC 中用户划分为管理员、操作员、普通用户和自定义用户等权限组，每个组的 具体权限如下：
  - 管理员 ：拥有的所有配置和控制权限。
  - 操作员：相对于管理员，拥有除用户管理、调试诊断和安全配置外的所有配 置和控制权限。
  - 普通用户：只有查看权限，除 OS 相关信息和操作日志查看外的所有查看权 限，并能修改自身密码。
  - 自定义权限组：自定义权限组允许系统管理员根据用户的实际场景自定义精 确分配用户权限。iBMC 支持最大 4 个自定义权限组。系统权限类型被划分为 用户配置、常规设置、远程控制、远程媒体、安全配置、电源控制、调试诊 断、查询功能、配置自身这几种类型，系统管理员可以灵活将这些权限类型 配置为一个自定义权限组。

图 3-53 自定义角色应用

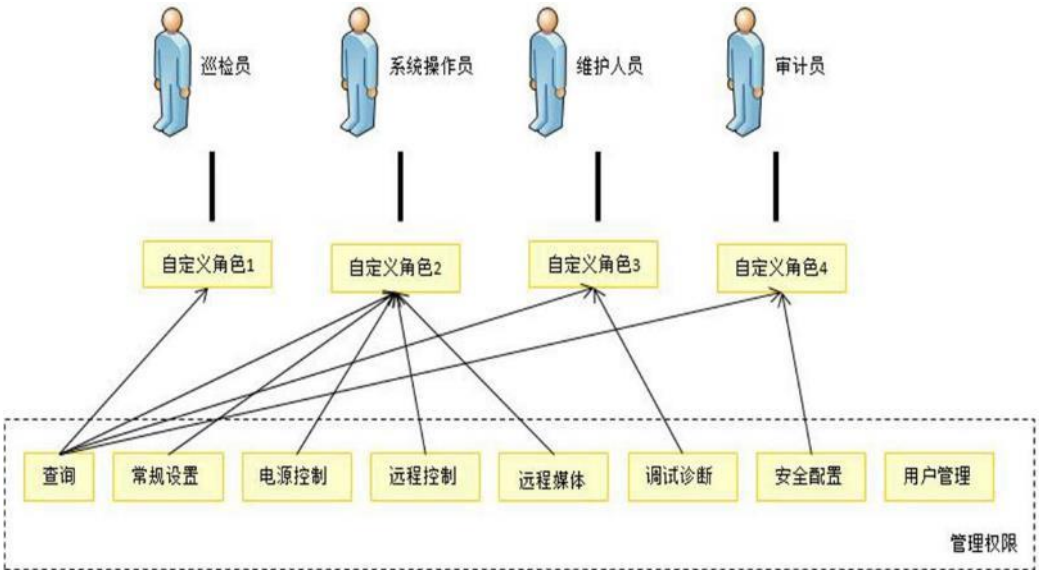


图 3-54 角色自定义界面

3.8.4 证书管理

证书是指 SSL 证书，在建立 Web HTTPS 连接时使用，用于证明 Web 站点的身份。

证书管理就是指对 SSL 证书的各种管理操作，包括查看当前证书信息（证书的使用者、 颁发者、有效期、序列号）、生成 CSR 文件、导入由 CSR 生成的签名证书（只有公钥， PKCS#7 格式）、导入自定义证书（包含公钥和私钥，pkcs#12 格式）。证书格式只支 持 X.509 格式，封装格式支持 pkcs#7 和 pkcs#12 两种，pkcs#12 格式证书支持对私钥设 置密码。

iBMC 的 SSL 证书默认使用自签名 SSL 证书，证书的签名算法使用 SHA256RSA（2048 位），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，iBMC 提供了两种替换自签名证书的方法：

第一种方法（使用 iBMC 生成的证书）：

1、登录到 iBMC Web，修改证书使用者信息；

2、生成 CSR；

3、导出 CSR；

4、将 CSR 提交给 CA 机构；

5、CA 机构生成 PKCS#7 格式签名证书；

6、将签名证书导入到 iBMC；

7、重启 iBMC 生效。

注意：签名证书必须与 CSR 配套，即：签名证书必须是通过该 CSR 申请的，否则导入证 书失败。

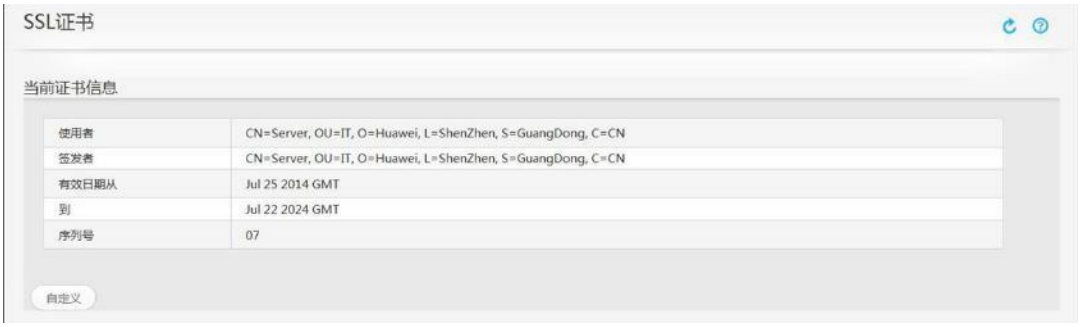
第二种方法（使用用户提供的证书）：

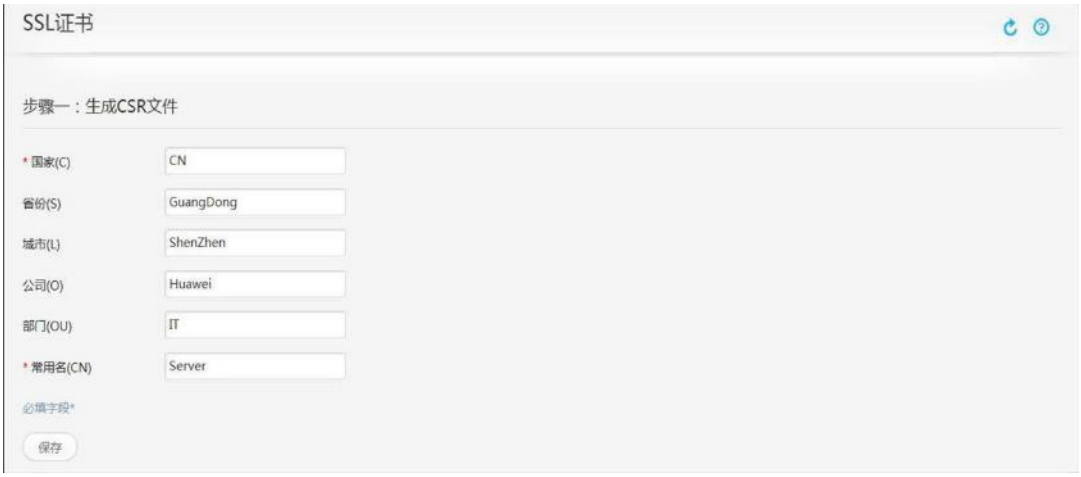
1、用户生成自定义证书或直接从 CA 购买证书；

2、登录到 iBMC　Web，将自定义证书或购买的证书导入到 iBMC；

3、重启 iBMC 生效。 SSL 证书

管理界面





3.8.5 会话管理

会话生成：会话标识使用安全随机数生成，长度为 192 bits；禁止同一个用户同时建立 多个会话；

会话销毁：有两种方式终止会话，

1）超时终止：对于 CLI、Web、SFTP 等长连接会话实现了静默超时断连机制，超过超 时时间没有操作则会自动断开会话。

2）手动终止：用户主动发起请求终止当前会话。另外，管理员可以主动终止其它会话。

3.8.6 安全协议

外部接入访问默认使用 SFTP、SSH、HTTPS、SNMPv3、RMCP+(IPMILAN)方式，传 输通道通过使用安全协议进行加密。不安全协议 HTTP、SNMP v1/v2c RMCP(IPMILAN)都默认关闭。

各种安全传输协议的特性如下：

SSH：

1）支持用户密码认证和公钥认证。

2）支持 SSH V2。

3）支持安全的加密算法 aes128-ctr、aes192-ctr、aes256-ctr、aes128-gcm、 aes256-gcm、chacha20-poly1305。

SFTP：

1）仅/tmp 目录具有上传、下载文件的权限。

2）上传到/tmp 目录的文件默认不具备可执行权限。

HTTPS：

支持 TLS1.0 及以上版本。为保持浏览器兼容性，默认开启 TLS1.1/TLS1.2，用户可以登录 iBMC 禁用 TLS1.1。

SNMPv3：

1）认证算法支持 SHA、MD5，支持用户配置。

2）加密算法支持 AES、DES，支持用户配置。

3.8.7 数据保护

iBMC 上涉及密码、密钥的所有敏感数据都进行了加密保护，防止敏感信息泄露。

iBMC 支持升级包的加密和签名保护，防止升级包内容被破解和篡改，保证升级包的机 密性和完整性。

除了加密保护，iBMC 对 linux shell 进行了封装，用户通过 SSH、串口等接口登录后无 法直接访问文件系统中的文件，防止文件被破坏及软件信息泄露。

iBMC 中支持对关键数据文件进行备份及计算并保存文件校验和，并提供了文件校验失 败的备份恢复机制，防止因系统异常掉电导致的数据文件破坏，保护数据文件的可用 性和完整性；

表 3-9 iBMC 数据加密情况

数据	加密算法
SSH/SFTP 用户密码	SHA512
Web 用户密码	AES128
SNMP V3 用户密码	MD5、SHA-1
SNMP V1/V2C 团体名	AES128
RMCP+用户密码	AES128
串口	SHA512
SSL 证书	AES128
升级包	AES128

除了对保存在 iBMC 中的敏感数据进行加密保护，系统运行过程中产生的敏感数据在使 用完后会使用清空内存的方式立刻清空。

3.8.8 安全配置

1. 访问策略

支持基于场景的登录限制，基于时间段、IP、MAC 的访问控制策略，通过配置登入时 间段、登入 IP 网段、登入 MAC 地址白名单，只允许满足白名单要求的用户通过管理通 道访问系统，对系统进行管理和配置，将服务器管理接口访问控制在最小范围；

由用户根据需要设置登录规则的白名单，最多支持三条登录规则，登录时只要匹配上任意一条登录规则，即可登录，否则拒绝登录；

每条登录规则包括时间段、登录用户的源 IP 段和 MAC 段，这三个条件必须同时满足才 认为匹配到一条登录规则；登录规则可应用于所有本地用户和 LDAP 用户组；

三维立体象限： 时间段：包括开始时间和结束时间，时间格式必须一致，支持

YYYY-MM-DD HH: MM、YYYY-MM-DD 和 HH:MM 三种格式，允许为空；

IP 段：支持单个 IPv4 地址或 IPv4 地址段，允许为空，目前不支持 IPv6 地址；

MAC 段：支持单个 MAC 地址或 MAC 地址段，允许为空。

登录规则应用场景：

时间段：只在特定的时间段允许登录维护，比如有些数据中心下班后不允许登录操 作，就可以通过配置登录时间来进行控制，以降低安全风险。

IP 段、MAC 段：只允许特定范围内的 IP、MAC 才能登录，防止网络上的大规模异常攻 击。

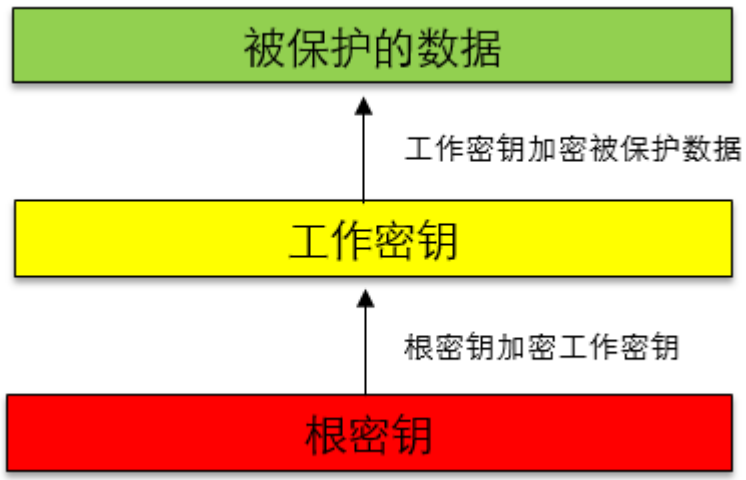
2. 系统锁定

支持系统锁定功能，系统锁定功能开启后，系统中的用户配置、常规配置、虚拟控制 台配置、安全配置都处于锁定状态不能配置，系统电源控制、虚拟媒体功能和查询功 能可以正常使用。系统锁定功能可以防止系统配置的意外或恶意更改。

只有管理员权限用户才有系统锁定功能开启和关闭的权限，开启后，WEB、CLI、SNMP、Redfish、IPMI 接口都被锁定，无法进行配置。

3.8.9 秘钥管理

- iBMC 密钥管理采用“根密钥 + 工作密钥”的“两层密钥管理结构”，根密钥用来 对工作密钥进行加密，工作密钥对被保护数据进行加密。密钥管理如下图所示：



  - 密钥生成：根密钥由安全随机数生成，分成多个组件分开保存；工作密钥使 用安全随机数生成。
  - 密钥使用：密钥用途单一，每个密钥只用于一种用途。
  - 密钥存储：根密钥分成多个组件分开保存，进行权限控制；工作密钥使用根 密钥加密后保存。

密钥更新：支持手动更新，执行更新密钥的命令，系统会随机生产新的密钥，旧密钥会被销毁。

3.8.10 系统加固

系统最小化安装，iBMC 中对嵌入式 linux 系统进行裁剪，只安装系统必须的组件，不使 用的组件和命令都被删除。

对 linux shell 命令行进行了封装加固，屏蔽了对 linux 系统命令的支持，只能执行白名单 定义的命令，降低攻击风险。

对系统中 SSH、Apache 等服务端进行安全配置加固，只支持安全的算法，不安全的协 议和端口默认关闭。

3.8.11 日志审计

iBMC 支持日志审计，日志信息中包含用户名、用户 IP 地址、操作时间、操作内容等信 息。iBMC 会记录 SEL 日志、操作日志、运行日志、安全日志，并可以通过 iBMC 提供的 接口进行查阅和审计。

iBMC 日志实时保存在 iBMC 的 Flash 文件系统中，当日志快达到最大存储容量时会产生 日志快满的日志提醒，当日志文件达到指定大小后会自动进行日志文件备份。按照最 小权限原则，非授权用户无法查看和下载日志文件。

iBMC 支持日志的 syslog 远程转储，把日志存储到远程 syslog 服务器中，防止本地日志 满后被覆盖丢失，支持对 syslog 服务器进行验证。

3.9 管理接入

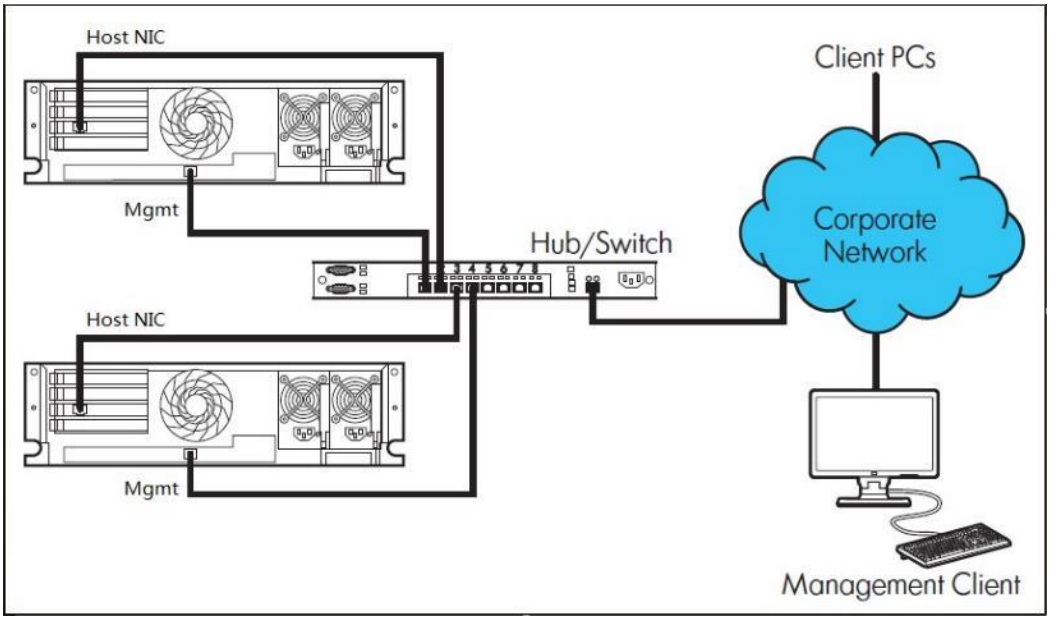
iBMC 兼容支持了 IPv4 和 IPv6 两种协议版本地址，支持通过专用管理网口或共享网口(利 用 NCSI 边带功能)接入，其中共享网口支持 VLAN 功能。

3.9.1 管理网口自适应

机架和节点服务器有两个物理管理网口：一个千兆专用管理网口和一个边带管理网口(NCSI，与主机系统共用物理网口)，此功能是根据网口 link 状态，自动将逻辑网口与其 中一个物理网口适配。

网口自适应启用后，服务器更换组网后只要专用管理网口或边带管理网口任一网口连 接了网线即可访问管理界面，平滑切换，不需要再配置任何网络信息，省去繁杂的配 置步骤，提升维护效率。

图 3-55 管理组网图



网口自适应配置界面提供了网口模式查询和设置接口，若选择自适应模式，则可指定 某个主机网口作为边带网口，默认为网口 1，如**图 3-56** 所示。

图 3-56 网口自适应配置界面

3.9.2 边带管理

边带管理(iBMC 界面称共享网口)就是利用边带(NC-SI)技术使管理系统与主机系统共用主机物理网口，通过一个网口就可以同时做管理操作和业务处理，简化组网，节省交换机端口；从业务数据优先角度考虑，管理数据最大带宽限制在 100Mb/S；从安全考虑，利用 VLAN 技术将管理与业务划分在不同网段。

图 3-57 边带管理框图

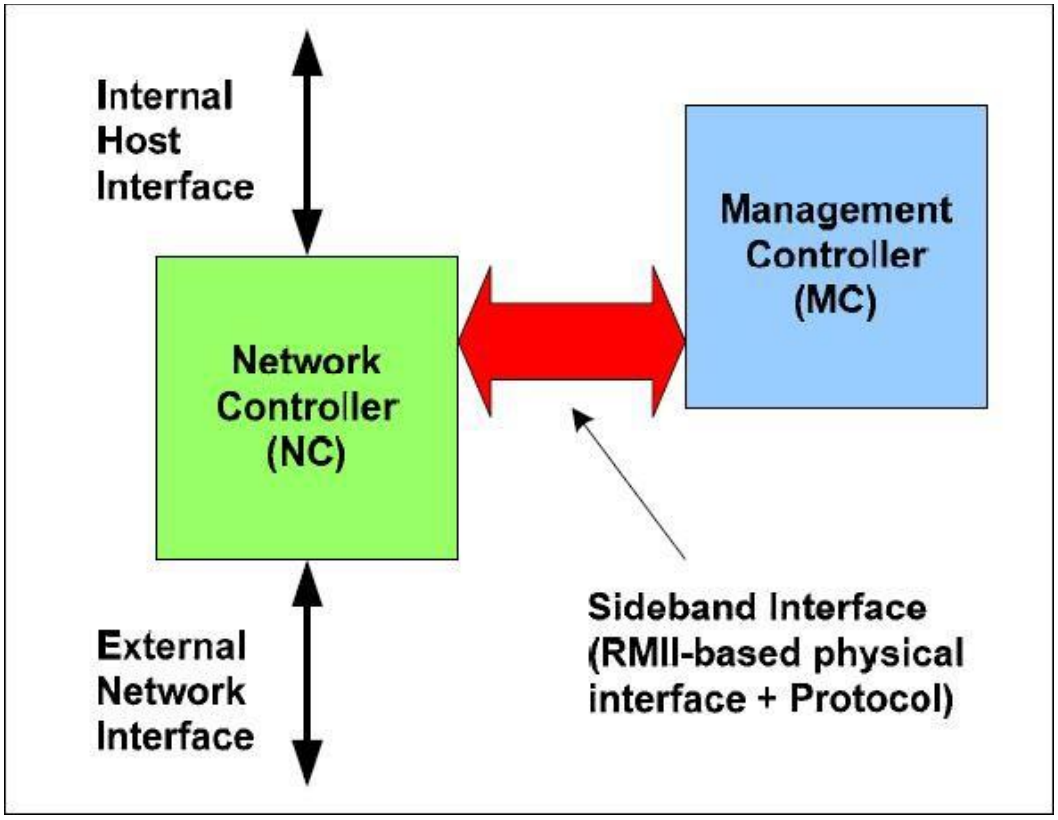
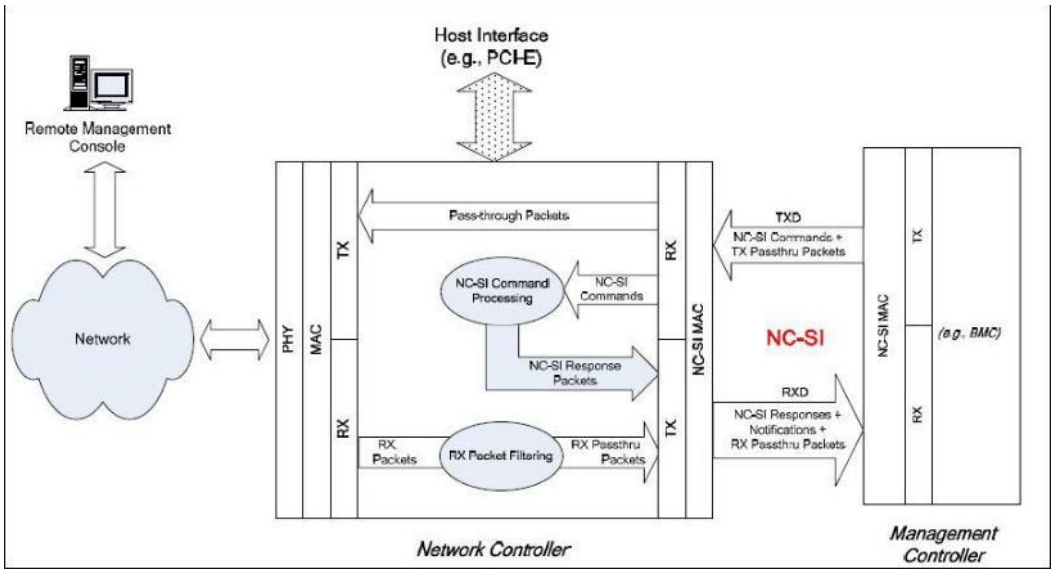


图 3-58 边带管理数据流图



3.9.3 IPv6

IPv4 地址资源很快面临枯竭，解决办法是使用 IPv6 地址，iBMC 已经正式全面支持了 IPv6 地址功能。目前 iBMC 的 WEB、SSH、SNMP、IPMI LAN、redfish 接口模块都已支 持 IPv6 地址访问，专用管理网口和共享网口(NCSI)的物理通道也都支持 IPv6 地址访 问。

图 3-59 IPv6 地址配置界面

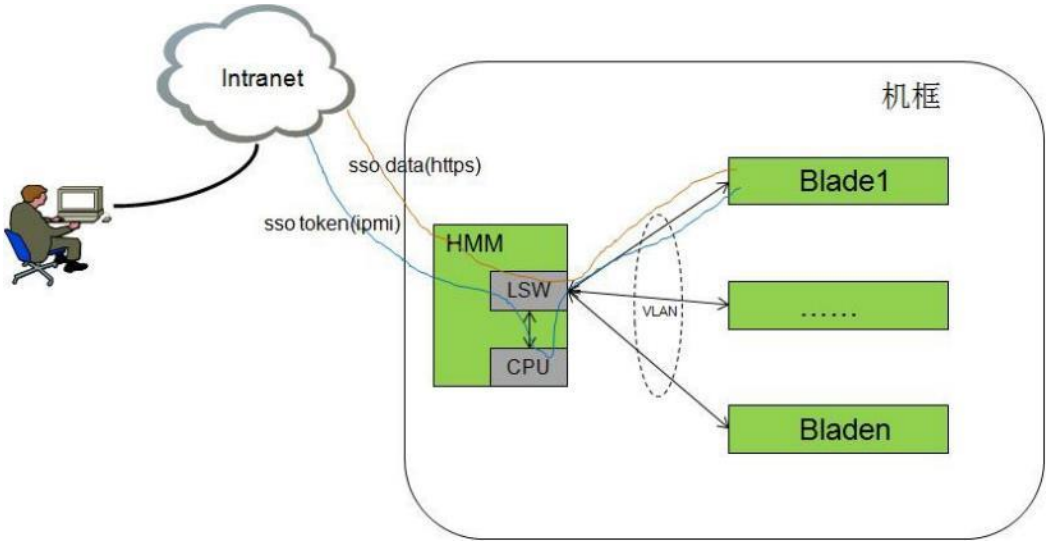
3.9.4 SSO

支持手动设置或 DHCP 获取 iBMC 的 IPv6 地址。

为了减少用户在浏览不同管理软件 WEB 界面时反复输入用户名、密码进行鉴权，iBMC 支持网管 SSO 和机框 SSO。登录网管或机框管理板的用户可以直接浏览到 iBMC WEB 或远程控制台界面，无需再输入密码。

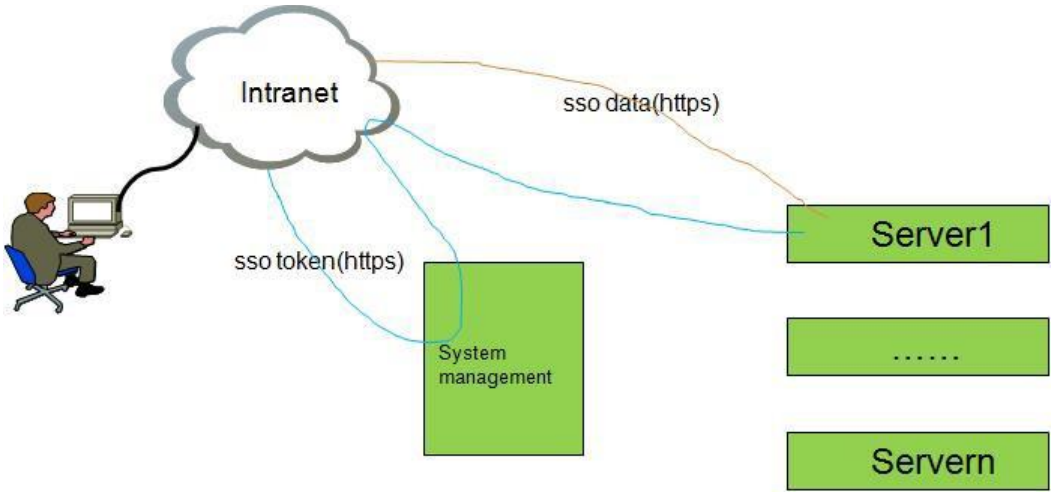
机框 SSO 实现原理，用户先登录 HMM WEB，点击单板 iBMC 的 SSO 链接时，HMM 通过内部 VLAN 通道发 IPMI 命令从 iBMC 获取 SSO token，然后使用该 token 通过 https 协议登录 iBMC WEB 首页或远程控制台，跳转到 iBMC 上的操作权限由 HMM 指定，如图 3-60。

图 3-60 机框 SSO 原理



网管 SSO 实现原理，网管预先将服务器接入管理，用户登录网管 WEB，点击服务器 iBMC 的 SSO 链接时，网管通过 https 协议从 iBMC 获取 SSO token，然后使用该 token 通 过 https 协议登录 iBMC　WEB 首页或远程控制台，如图 3-61。

图 3-61 网管 SSO 原理



3.10 统一用户管理

iBMC 是一个基于嵌入式 CPU 和 OS 的管理子系统，OS 和应用对外是一个封闭的整体， 只提供了固定的维护、集成接口。OS(CLI)、SNMP、IPMI LAN、WEB、redfish 等这 些对外接口各自都有一套独立的本地用户管理，对用户来说，要想通过这些接口都能 接入，则必须重复五遍配置用户的动作，非常繁琐。因此，我们提供了统一用户管理 的功能，只要在上述任一接口配置好用户，即可使用该用户登录 iBMC 所有接口，也就 是说所有接口呈现的本地用户是同一套；iBMC 后台自动完成了各个接口的用户同步。

本地用户最多支持 16 个用户，支持增加、修改和删除用户；所有用户划分为管理员、操作员和普通用户三个固定权限组和一个自定义权限组，每个组的具体权限如下：

管理员：拥有 iBMC 的所有配置和控制权限； 操作员：相对于管理员，拥有除用户管

理和安全配置外的所有配置和控制权限； 普通用户：只有查看权限，除 OS 相关信息

和操作日志查看外的所有查看权限。 自定义组：由用户指定该组的具体权限。

登录接口：由创建者指定新用户可以 使用

的接口类型

图 3-62 用户管理界面

3.11 配置管理

3.11.1 配置导入导出

配置导入导出，就是指把 BMC、BIOS 和 RAID 控制器的所有配置能以配置文件的方式导 出和导入，其中 RAID 控制器配置需在系统 POST 完成之后导出才有效。此功能提供了一 种方法让客户可以轻松的远程保存服务器配置，一旦设备需要更换，可以导入以前保 存的配置到新机器，快速完成新设备的配置，也可以针对同一类型机器，用同一个配 置文件进行批量配置导入，完成大规模设备的配置和部署。当前支持的接口有： SNMP、CLI、WEB 和 redfish；

WEB 接口操作界面如下图： 图 3-63

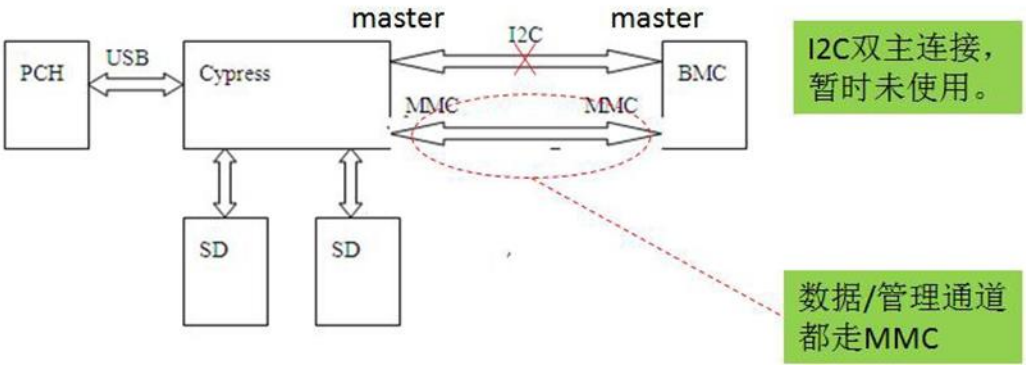
3.12 存储管理

3.12.1 内置 SD 卡

每台 V3 服务器可选配两张内置 SD 卡，当前可满足以下应用场景：

- 安装 OS，常用于无盘或全数据盘系统，安全、可靠
- 存储重要数据，重要业务数据或主机 OS 数据存储，与 Guest O 数据隔离

图 3-64 SD 卡连接图



SD 卡主要功能：

- 默认一个分区，RAID1
- 默认 Owner 为主机系统
- 支持 RAID 重构，记录开始和结束日志
- 读写错误次数越门限检测
- RAID 重构失败检测
- SD 卡容量、厂商、SN 查看

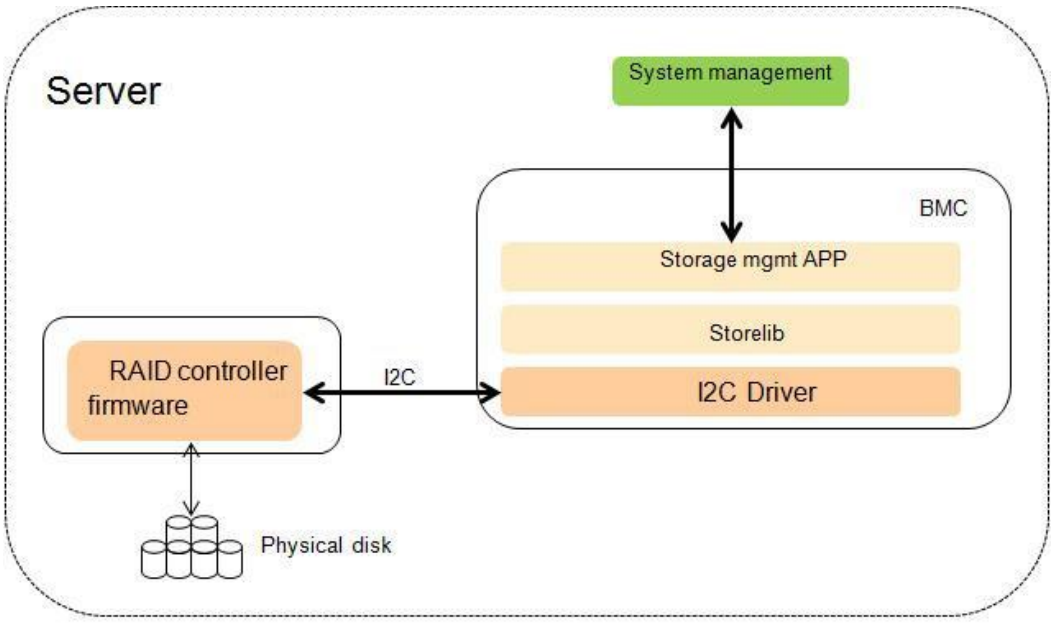
3.12.2 RAID 与硬盘管理

硬盘在服务器中扮演着非常重要的角色，上面安装了系统 OS 或存储了用户数据，因此对硬盘的管理和监控是非常必要的。

iBMC 通过与 RAID 控制器交互来对硬盘进行带外管理，依赖于 RAID 控制器 firmware 的 能力，目前只有最新硬件版本的 SAS3004iMR/LSI 3108/3008 以及 LSI 34 系列/35 系 列/LSI 93 系列等 RAID 卡支持，如**图 1 硬盘带外管理原理**。注意：产品中插多 RAID 卡场景下，若其中有 RAID 卡不支持带外管理技术，则该产品无法支持硬盘带外管理。

在 OS 侧安装了 iBMA2.0 软件的情况下，即使 RAID 卡本身不支持 RAID 带外管理，iBMC 也能对硬盘进行带外管理和对 SATADOM、M.2 进行故障监控；

图 3-65 硬盘带外管理原理



硬盘带外管理包括对 RAID 控制器、物理盘和逻辑盘管理，支持的特性如**表 3-10**、**表** 3-11、表 3-12：

表 3-10 硬盘带外管理支持属性（状态监控和信息查询）

部件	管理属性	备注
RAID 控制器	名称、类型、健康状态、固件版本、配置版本、电容状态、SAS 地址、高速缓存存储器大小、SAS 速率、是否保留高速缓存、启动盘、是否打开物理盘故障记忆、DDR 可纠正 ECC 计数、PHY 误码计数、驱动名称、驱动版本	支持 Web/ SNMP/CLI/Redfish 接口和一键收集；DDR 可纠正 ECC 计数、PHY 误码计数不在 Web 显示。
物理盘	健康状态、SN、型号、容量、固件版本、介质类型、总线协议、是否热备盘、厂商、重构进度、是否在巡检、medium error 计数、prefail 计数、其它错误计数、支持速率、协商速率、SAS 地址、逻辑归属位置、电源状态、温度、SSD 盘剩余寿命、SMART 预告警状态	支持 Web/SNMP /CLI/Redfish 接口和一键收集；medium error 计数、prefail 计数、其它错误计数不在 Web 显示。
逻辑盘	运行状态、RAID 级别、读策略、写策略（默认的和当前的）、条带大小、容量、物理盘写 cache 是否使能、是否在进行数据一致性校验、成员盘列表、span depth、Number ofDrives Per Span、系统盘符	支持 Web/SNMP /CLI/Redfish 接口和一键收集
日志	RAID 卡日志导出	包含在一键收集中

注：驱动名称、驱动版本、系统盘符这些信息只有安装了 iBMA2.0 才支持。

表 3-11 配置功能点（仅 RAID 卡支持带外管理时支持）

部件类型	功能点
RAID 控制器	Copyback 设置、SMART 错误时回拷设置、JBOD 模式设置、重置 控制器；
物理盘	全局局部热备状态设置、固件状态设置、物理盘定位设置；
逻辑盘	支持逻辑盘的创建、删除和属性修改，可以修改的属性有：VD 名 称修改、读策略修改、写策略修改、IO 策略修改、访问策略修改、后台初始化使能设置、SSD Caching 使能设置，CacheCade 逻辑盘设置、Disk Cache Policy 设置、启动盘设置；

表 3-12 故障监控点

部件	故障类型及场景
RAID 控制器	内部故障、内存 UCE 计数非 0、内存 ECC 计数超门限、NVRAM 错 误计数非 0、BMC 访问失败
物理盘	故障、预故障(predictive failed error 为非 0)、重构失败、盘在位 但 RAID 卡不能识别
逻辑盘	逻辑盘状态为 offline 则该逻辑盘下不在位的物理盘报 “In Critical Array” 、逻辑盘状态为 degraded 或 partial degraded 则该逻辑盘 下不在位的物理盘报 “In Failed Array〞
BBU	电压低、BBU 故障、不在位

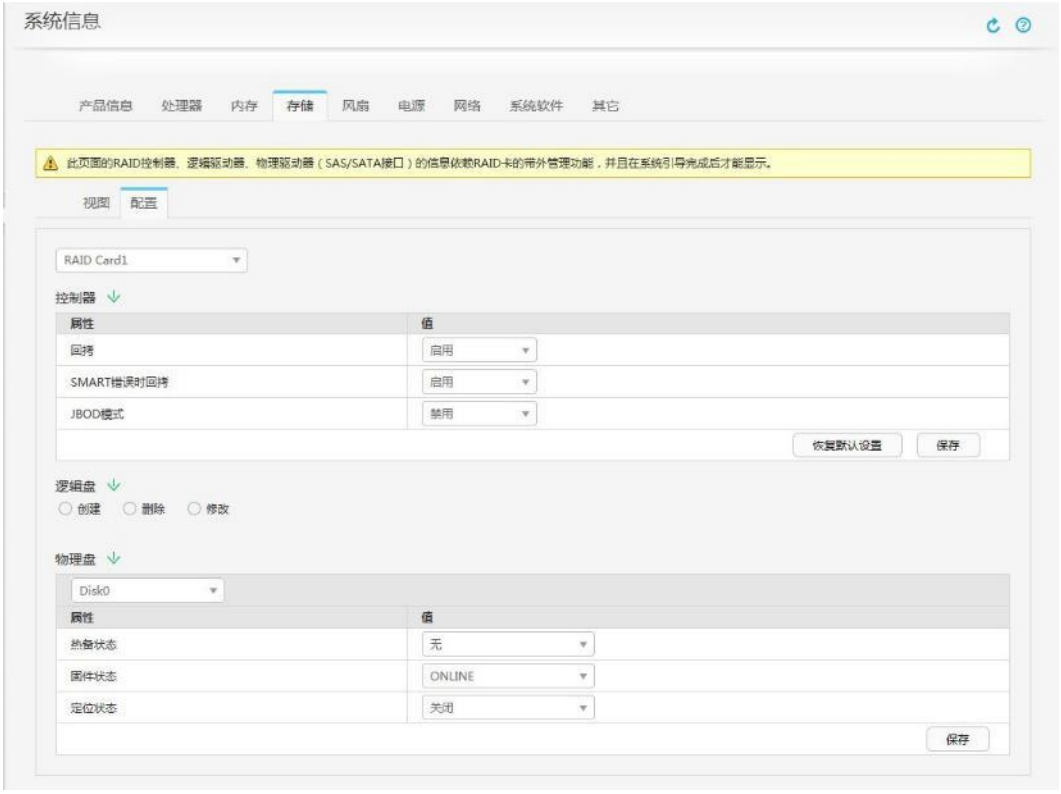
硬盘带外管理界面视图，是基于存储部件逻辑关系组织的。

图 3-66 RAID 控制器管理界面

图 3-67 逻辑盘管理界面

图 3-68 物理盘管理界面

图 3-69 RAID配置界面



说明：由于目前 RAID 控制器不支持对 NVMe 盘组 RAID，故上述管理和监控方式只适合 于 SAS/SATA 盘；对于 NVMe 盘，目前管理如**表 3-13** 所示。

表 3-13 NVMe 盘管理

项目	具体取值
信息查询	序列号、型号、接口类型、厂商、固件版本、剩余寿命百分比、基于 iBMA 2.0 获取：接口最大速率、接口协商速率、接口类型、介质类型、容量、累计通电时间
故障监控	故障、SMART 预告警、过温、剩余寿命不足

表 3-14 M.2/SATADOM 管理（基于 iBMA2.0）

项目	具体取值
信息查询	序列号、容量、厂商、温度
故障监控	容量为 0、offline、剩余寿命不足

说明：目前 M.2 出 SATA 接口，接 PCH 或 RAID 卡，上表仅适用接 PCH 场景，接 RAID 卡场 景（如 M.2 盘）归属上面的硬盘带外管理。

3.13 时间管理

网络时间协议（NTP）：

NTP(Network Time Protocol)是用来使计算机时间同步的一种协议。服务器 iBMC 自身没有 RTC 硬件，但支持从多个时间源同步时间且同一时间只能从一个时间源同步，时间 源见**表 3-15**。NTP 功能默认关闭且支持开启，支持手动设置或自动获取首选和备用 NTP 服务器地址(支持 IP 的 v4 和 v6 版本)，手动设置时 NTP 服务器地址还支持 FQDN 域名 输入；从时间获取的安全性考虑，iBMC 支持对 NTP 服务器合法性校验。

只要 NTP 功能开启了，无论时间是否同步成功，都不会自动切换到其它时间源。NTP 功 能关闭，则 iBMC 从默认时间源同步时间。时间同步失败、时间跳变都会记录事件日 志。

表 3-15 iBMC 时间源

iBMC	支持时间源	默认时间源
机架服务器	主机 RTC（BIOS/OS）、NTP	主机 RTC（BIOS/OS）
刀片服务器	机框管理板、NTP	机框管理板
高密度服务器	主机 RTC（BIOS/OS）、NTP	主机 RTC（BIOS/OS）
辅助管理板	iBMC RTC、NTP	iBMC RTC

图 3-70 NTP 配置界面

夏令时（DST）：

夏令时（Daylight Saving Time：DST），又称“日光节约时制”和“夏令时间”，是一种为节约能源而人为规定地方时间的制度，在这一制度实行期间所采用的统一时间 称为“夏令时间”。一般在天亮早的夏季人为将时间调快一小时，可以使人早起早 睡，减少照明量，以充分利用光照资源，从而节约照明用电。各个采纳夏时制的国家

具体规定不同。目前全世界有近 110 个国家每年要实行夏令时。对于未实行夏令时的国家只要配置对应时区即可。

图 3-71 夏令时配置界面

3.14 SP 管理

3.14.1 概述

智能部署工具（Smart Provisioning）是一款集成到 KunTai 服务器上的工具软件。在 V3 服务器上，维护工程师需要通过随机发放的 ServiceCD 2.0 光盘，使用物理光驱来进行 OS 的安装引导和 RAID 配置或者下载ServiceCD 的 ISO 文件，通过虚拟光驱挂载的方式完成上述功能。在集成 Smart Provisioning 工具后，在服务器上电后，就可通过 BIOS 界面进入，实现服务器 RAID 卡 的配置、OS 的安装、PCIe 卡的固件升级等功能，从而简化用户操作，提高安装效率。

3.14.2 系统设计

图 3-72 Smart Provisioning 在系统中的位置-x86

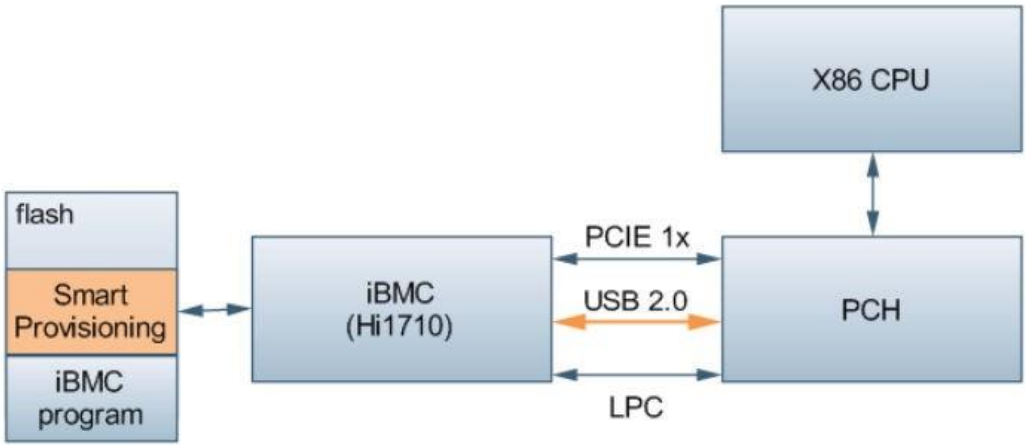
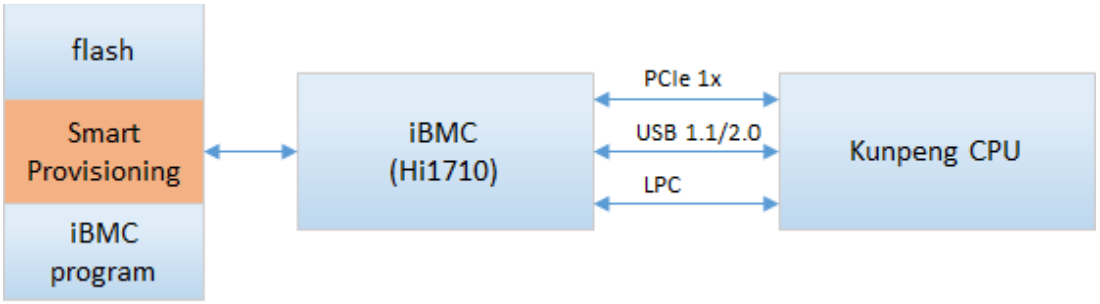


图 3-73 Smart Provisioning 在系统中的位置 - Kunpeng



Smart Provisioning 存储在服务器主板的 flash 芯片上，通过 iBMC 的 Hi1710/Hi1711 芯片接入到 服务器系统中。 Smart Provisioning 集成了一个 Linux 操作系统，因此用户在没有安装 操作系统的情况下也可以使用该工具。主板的 flash 芯片为 8GB 的 NAND Flash 芯片，存 放 iBMC 的程序和配置文件、Smart Provisioning(SP)的程序和配置文件。

用户可以使用两种方式进入 Smart Provisioning：

- 在 BIOS 启动过程中按快捷键： 适用于用户手动进入系统，进行服务器的 OS 安装、RAID 配置和固件升级的场景。
- 通过 iBMC 的 Redfish 接口设置从 Smart Provisioning 启动： 适用于通过带外管理软件来控制 Smart Provisioning 工具进行升级固件的场景。
  当系统设置为从 Smart Provisioning 启动的时候，iBMC 将 flash 中工具区域的数据 进行映射后作为 USB 盘连接到系统中，X86 系统通过该 USB 设备完成系统启动，并 加载工具进入到工具的图形界面。

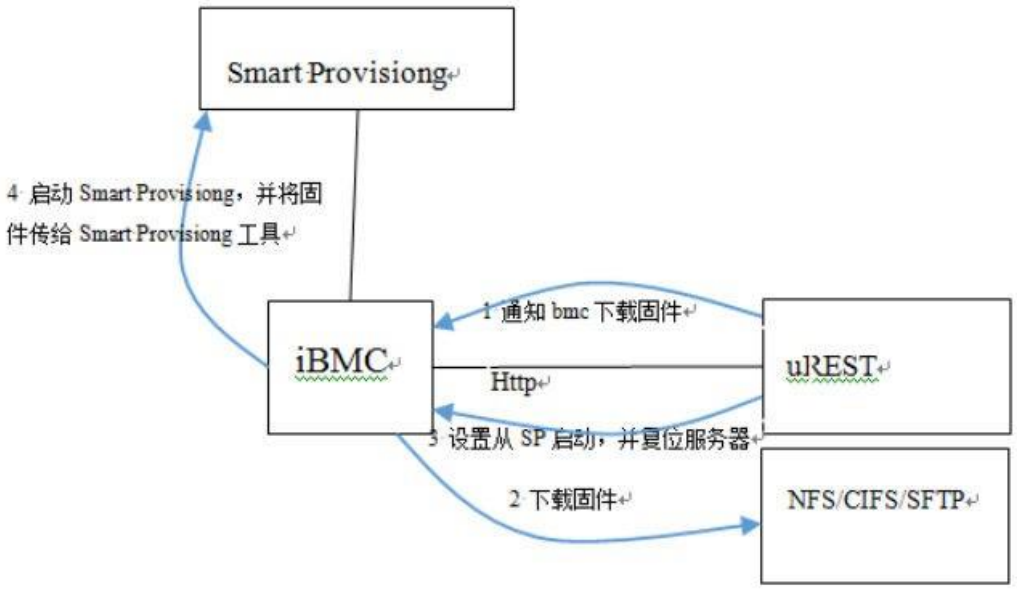
iBMC 提供的 redfish 接口，支持的主要功能如下：

- 固件升级(RAID 卡、网卡、FC 卡、SATA 盘、SAS 盘的固件升级）
- Smart Provisiong 升级
- PCIE 卡资源查询

3.14.3 固件升级

Smart Provisioning 支持通过 iBMC 的 Redfish 接口进行固件升级，管理软件或者其它工具可通过这种方式实现对多台服务器固件进行批量升级。这里以 uREST tool 工具为 例，组网方式如图所示：

图 3-74 通过 iBMC Redfish 接口升级

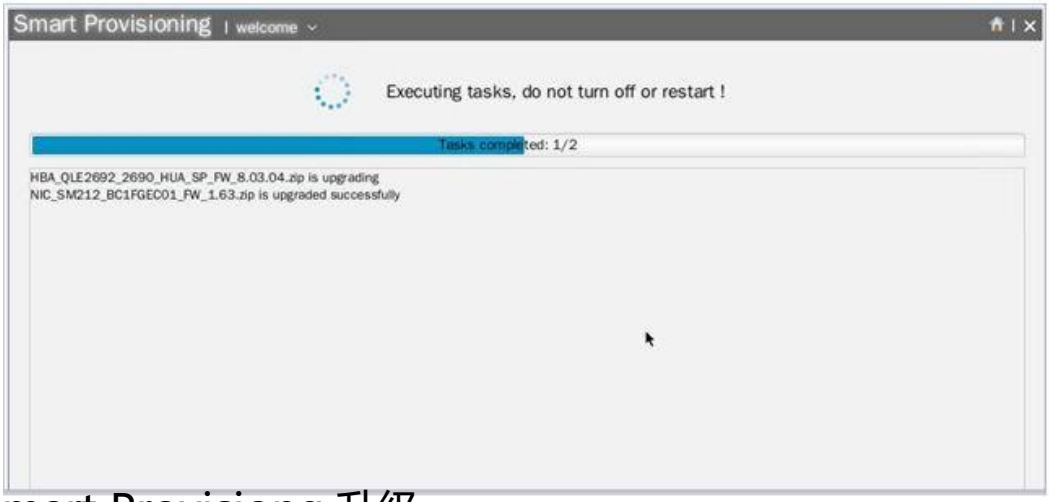


iBMC 提供了 Redfish 接口支持升级 PCIe 卡和硬盘的固件，可以通过工具（比如 uREST tool）下发命令给 iBMC，iBMC 将会从指定的文件服务器下载固件。

固件下载完成后，通过工具设置系统从 Smart Provisiong 启动，并且复位服务器。服 务器从 Smart Provisioning 启动后，将自动检测是否有固件需要升级。如果需要升级 固件则执行升级任务，并显示升级进度。升级完成后，工具将自动复位系统。

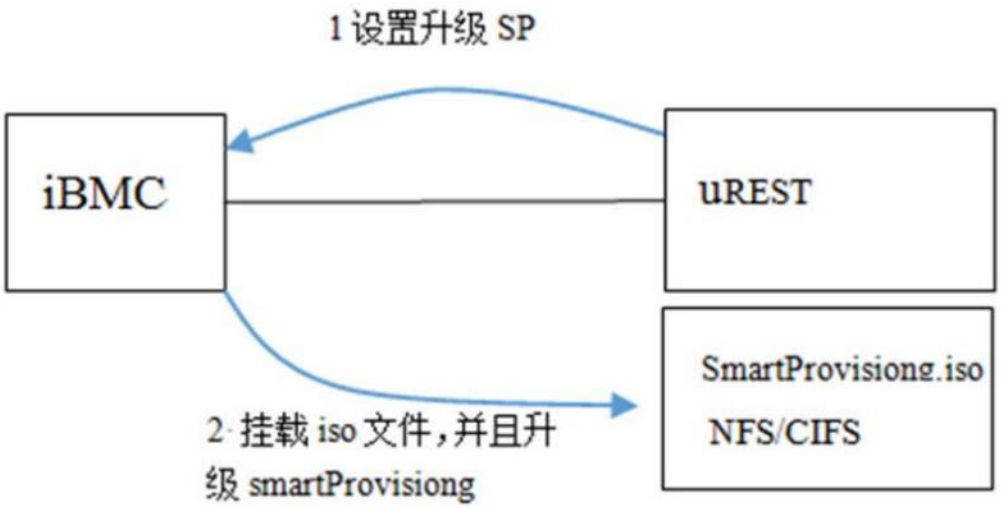
通过这种方式，可以实现对 PCIe 固件的上传和生效进行分

离。**图 3-75** 固件升级进度



3.14.4 Smart Provisiong 升级

图 3-76 通过 iBMC 升级 SmartProvisioning



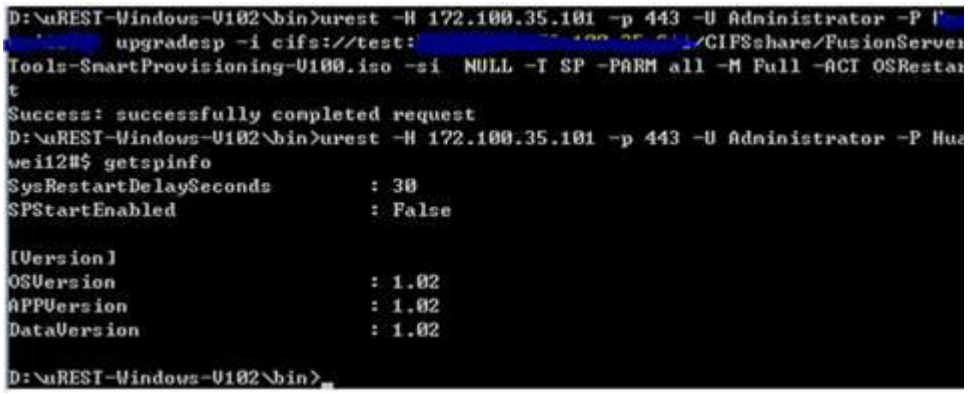
iBMC 提供了 Redfish 接口升级或者恢复 Smart Provisioning。

升级时 iBMC 通过 NFS/CIFs 协议从远端挂载 Smart Provisioning 的 ISO 文件。在对文件内容进行校验后，将光盘信息复制到 flash 上完成对工具的升级。在下次进入 Smart Provisioning 时将生效。

这种方式升级时可以不需要复位业务系统，因此不会影响业务侧的业务。通过带外管

理软件可以实现对多台服务器的批量升级。
如图使用 uREST tool 命令进行升级，并且查询升级后的版本号。更详细操作可以参考
《 uREST tool V2R2 用户指南》。

图 3-77 使用 iBMC 升级 Smart Provisioning



3.14.5 卡资源查询

Smart Provisioning 对服务器带外监控能力进行了扩展，在 Smart Provisioning 启动后把以前 iBMC 无法获取的 PCIe 卡信息提供给了 iBMC，当前能检测到的信息如下：

表 3-16 Smart Provisioning 提供 PCIe 卡的信息如下：

资源名称	资源描述
DeviceName	丝印
Controlers	控制器信息
Model	型号
Functions	功能属性信息
VendorId	厂商 id
BDFNumber	BDF 信息
BDF	BDF
Description	描述信息
MacAddress	MAC 地址
DeviceId	设备 ID

资源名称	资源描述
SubsystemId	子系统 ID
Type	卡类型
SubsystemVendorId	子系统厂商 ID
FirmwareVersion	固件版本
Manufacturer	厂商信息
DeviceLocator	丝印信息
Position	位置信息

3.15 iBMA 管理

3.15.1 概述

iBMA 2.0 对服务器带外监控能力进行了扩展，把以前 BMC 无法获取的服务器部件信息提供给了 BMC，当前能检测到的信息包括：

- OS 版本和内核版本信息
- X86 主机名称和域名称
- 网卡、RAID、硬盘、PCIE 卡的驱动和 FW 版本查询及升级
- 网卡型号、芯片型号和驱动信息，网口 link 状态、MAC 地址、IP 信息、VLAN 信 息，桥接和绑定信息查询
- FC 卡型号、芯片型号和驱动信息，端口 link 状态、FC_ID 和 WWNN、WWPN 号查询
- 网卡光模块信息查看和故障监控，需要驱动配合支持，目前支持的网卡：Intel 82599、Emulex XE102，且仅 Linux 系统支持
- 以太网卡 OAM 检测，仅 E9000 刀片支持
- RAID 卡、物理盘和逻辑盘详细信息查询
- SATADOM/M.2 卡的信息查看各故障监控
- CPU/内存/硬盘分区/网卡物理端口带宽使用率查询

3.15.2 支持能力

表 3-17 iBMA 提供的信息

部件	不安装 iBMA	安装 iBMA
网卡	网卡名称、厂商、芯片厂商、型号、芯片型号； 网卡各端口的名称(与物理丝印对应)、link 状态(板载网卡)、MAC 地 址(板载网卡)。	网卡名称、厂商、芯片厂商、型号、芯片型号、FW 版本、驱动名称、版本； 网卡各端口的名称（与物理丝印对应）、IPv4、掩码、网关和 IPv6、VLAN 信息、link 状态、MAC 地 址； 网口的 team 和 bridge 信息，含逻辑网口名称、IPv4、掩码、网关和IPv6、前缀长度、网关、MAC 地 址、link 状态、工作模式及下属成员的端口名称、MAC 地址和 link 状 态； OAM 链路检测，包括物理端口网 络链路丢包、错包。
光模块	N/A	厂家名称、厂家部件号、序列号、生产日期、光模块类型（如：10GBASE_SR）、波长、多模/单模，温度、电压、收发功率、偏置电流的当前值和门限值； 功率、电压越限监控，网卡与光模块速率不匹配检测。
FC 卡	FC 卡名称、厂商、芯片厂商、型 号、芯片型号	FC 卡名称、厂商、芯片厂商、型号、芯片型号、驱动名称，驱动版本、FW 版本、wwnn 号、wwpn 号、端口类型、速率、链接状态和 FC ID。
SATADOM、M.2（接 PCH）	N/A	信息查看：序列号、容量、厂家名称、接口类型温度 故障监控：容量为 0、offline、剩 余寿命（剩余寿命仅 SATADOM 支持）。
系统信息	N/A	iBMA2.0 版本、iBMA2.0 驱动版本、OS 版本、Kernel 版本、主机名称、域名城、计算机描述、CPU/ 内存/硬盘资源使用率及监控、网 卡物理端口带宽占用率及监控。
统一升级	N/A	升级 iBMA 软件和 PCIe 部件驱动程 序，文件传输性能可达 4MB/s。