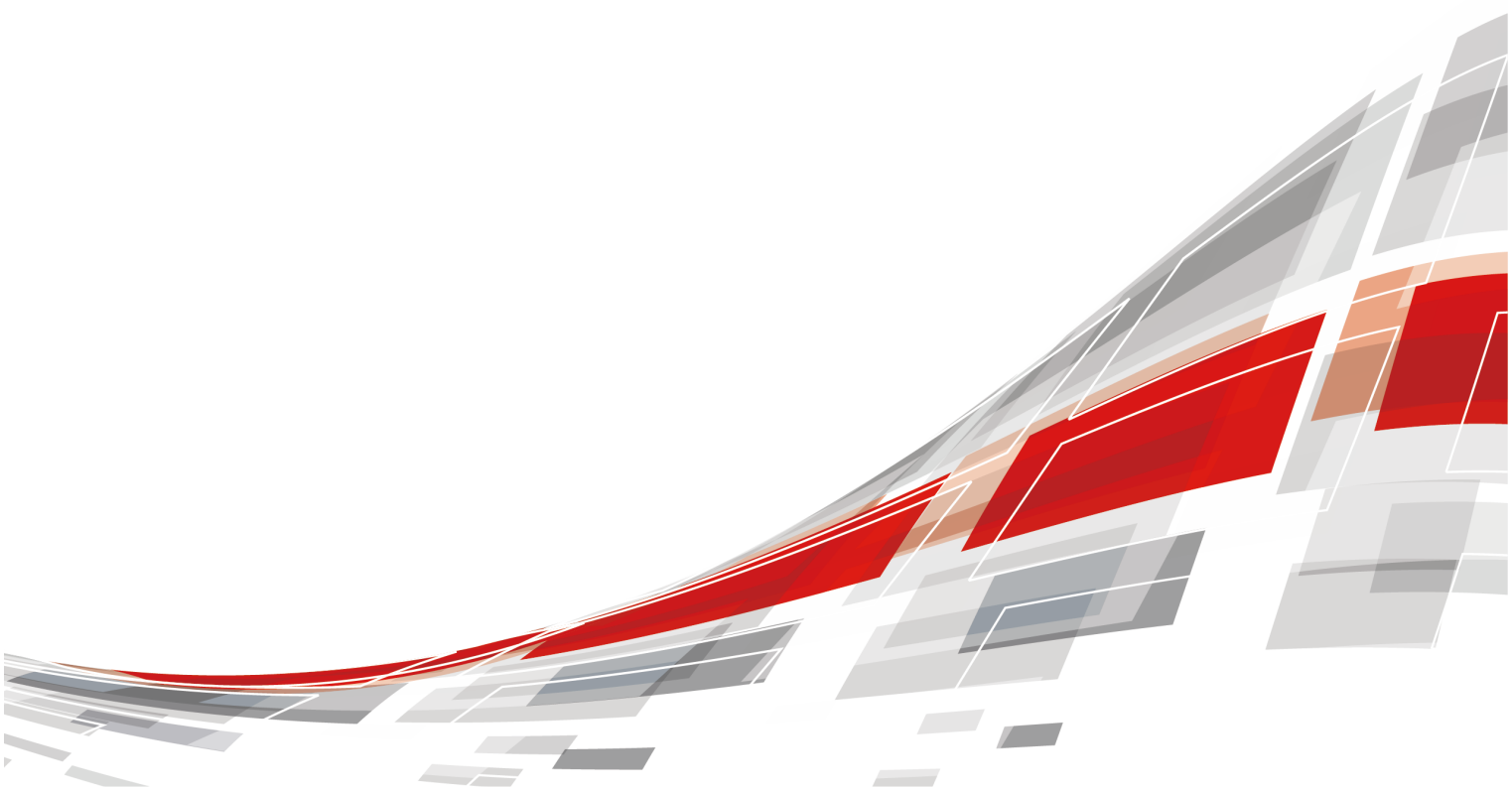
服务器 iBMC 智能管理系统

白皮书

文档版本 14

发布日期 2026-03-17



超聚变数字技术股份有限公司

商标声明

注意

本文中，只是为了描述的简洁和方便理解，用“xFusion”指代“xFusion Digital Technologies Co., Ltd.”，这并不代表“xFusion”还可以具备其它含义。基于本文中单独提及或描述的“xFusion”，不能用于“xFusion Digital Technologies Co., Ltd.”之外的理解或表达，超聚变数字技术股份有限公司也不承担因单独使用“xFusion”所带来的其它任何法律责任。

您购买的产品、服务或特性等应受超聚变数字技术股份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，超聚变数字技术股份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。

超聚变数字技术股份有限公司

地址： 河南自贸试验区郑州片区（郑东）龙湖内环北路99号 邮编：450000

网址： https://www.xfusion.com

前言

概述

本文档详细的描述了服务器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：

- 服务器厂家售前工程师。
- 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
14	2026-03-17	新增： • **3.9.21 邮件随机令牌双因素认证**章节。 • **3.9.22 BIOS固件实时完整性扫描**章节。 • **3.9.23 网卡固件实时完整性扫描**章节。
13	2025-12-16	更新**2 支持产品范围**。
12	2025-09-22	更新**3.9.8 安全配置**。 新增**3.9.20 FIPS 140-3认证**章节。
11	2025-02-20	更新**3.1.3 Redfish管理接口**。
10	2024-09-04	更新**3.2.1 故障检测**。
09	2024-07-18	新增**3.19 RADIUS身份认证**章节。
08	2023-12-14	新增**3.9.19 中国CC EAL4认证**章节。
07	2023-09-04	支持的产品范围增加5885H V6。
06	2023-06-25	新增**3.18 液冷监控管理**章节。
05	2023-04-20	• 优化支持机型描述。 • 补充安全认证等相关说明。
04	2022-12-22	支持的产品范围增加G5500 V6。
03	2022-09-13	新增**3.12.2 BIOS配置**章节。
02	2022-06-27	优化描述。
01	2021-10-27	第一次正式发布。

目 录

前言 ii
1 产品简介 1
1.1 概述 1
1.2 系统架构 2
2 支持产品范围 4
3 支持功能 5
3.1 丰富的管理接口 6
3.1.1 IPMI 管理接口 8
3.1.2 SNMP 管理接口 10
3.1.3 Redfish 管理接口 11
3.1.4 CLI 管理接口 13
3.1.5 Web 管理接口 13
3.1.6 手机 APP 管理接口 16
3.2 故障诊断与管理（FDM） 31
3.2.1 故障检测 31
3.2.2 故障诊断 34
3.2.3 FDM PFAE 35
3.2.4 系统运行记录仪 35
3.2.5 开机自检代码 36
3.2.6 系统事件管理 37
3.2.7 故障上报 38
3.2.8 宕机截屏 39
3.2.9 宕机录像 40
3.2.10 屏幕快照 40
3.2.11 屏幕录像 41
3.2.12 部件更换记录 43
3.2.13 Bom 编码管理 43
3.2.14 系统看门狗 43
3.3 虚拟 KVM 和虚拟媒体 43
3.3.1 虚拟 KVM 48
3.3.2 虚拟媒体 49
3.4 基于 HTTPS 的可视化管理接口 51

3.4.1 查看系统总体概况 51
3.4.2 查看系统信息 52
3.4.3 性能监控 54
3.4.4 设备定位 56
3.5 域管理和目录服务 56
3.5.1 域管理 56
3.5.2 目录服务 57
3.6 固件管理 59
3.6.1 固件双镜像 59
3.6.2 固件升级 60
3.6.3 BMC 升级与生效分离 60
3.7 智能电源及调速管理 60
3.7.1 电源控制 60
3.7.2 功率封顶 62
3.7.3 功率统计和历史曲线 63
3.7.4 电源主备 64
3.7.5 智能调速 65
3.8 系统串口重定向及运行记录 66
3.8.1 系统串口重定向 66
3.8.2 系统串口信息记录 66
3.9 安全管理 67
3.9.1 账号安全 67
3.9.2 认证管理 68
3.9.3 授权管理 69
3.9.4 证书管理 70
3.9.5 会话管理 71
3.9.6 安全协议 71
3.9.7 数据保护 72
3.9.8 安全配置 72
3.9.9 秘钥管理 73
3.9.10 系统加固 74
3.9.11 日志审计 74
3.9.12 DICE 74
3.9.13 安全启动 75
3.9.14 PFR 75
3.9.15 不安全版本吊销 75
3.9.16 电子保单管理 75
3.9.17 PCI DSS 认证 75
3.9.18 国际 CC EAL4+认证 75
3.9.19 中国 CC EAL4 认证 75
3.9.20 FIPS 140-3 认证 75
3.9.21 邮件随机令牌双因素认证 76

3.9.22 BIOS 固件实时完整性扫描 76
3.9.23 网卡固件实时完整性扫描 76
3.10 管理接入 76
3.10.1 管理网口自适应 76
3.10.2 边带管理 77
3.10.3 IPv6 78
3.10.4 SSO 79
3.10.5 近端运维 80
3.10.6 SSDP 80
3.10.7 固件联盟 BMC 标准符合性测试认证 80
3.11 统一用户管理 80
3.12 配置管理 81
3.12.1 配置导入导出 81
3.12.2 BIOS 配置 82
3.13 存储管理 82
3.13.1 内置 SD 卡 82
3.13.2 RAID 与硬盘管理 83
3.14 时间管理 87
3.15 SP 管理 88
3.15.1 概述 88
3.15.2 系统设计 89
3.15.3 固件升级 89
3.15.4 Smart Provisiong 升级 91
3.15.5 PCIe 卡资源查询 91
3.15.6 硬盘擦除 92
3.16 iBMA 管理 92
3.16.1 概述 92
3.16.2 支持能力 93
3.16.3 板载 iBMA 94
3.16.4 升级接口 96
3.17 Kerberos 认证 98
3.17.1 iBMC 单点登录方案概述 98
3.17.2 环境配置 99
3.17.3 系统兼容 100
3.18 液冷监控管理 100
3.18.1 服务器液冷监控 100
3.18.2 机柜液冷监控 100
3.19 RADIUS 身份认证 101
3.19.1 认证方案概述 101
3.19.2 环境配置 101

1 产品简介

1.1 概述
1.2 系统架构

1.1 概述

服务器iBMC智能管理系统（以下简称iBMC）是具有完全自主知识产权的服务器远程带外管理软件，可实现服务器远程监测及操作。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、支持硬件部件状态信息查询、硬件日志收集及查询等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，支持KVM over IP、虚拟光驱等。
- 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/LLDP
  域管理、目录服务、管理网口链路层发现协议报文发送，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。

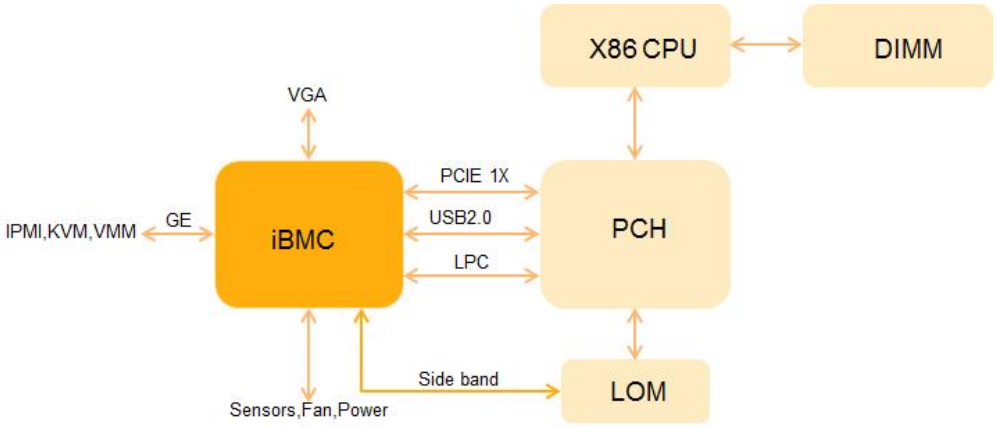
1.2 系统架构

如图1-1所示，iBMC硬件芯片采用Hi1710/Hi1711芯片，Hi1710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；Hi1711是一款针对 X86 CPU 平台的板级管理 BMC 芯片，包括一个最高主频最为1.0 GHz 的四核 A55 CPU，一个协处理 M3（主频 200MHz ）及安全核 M3 （主频200MHz，支持安全启动）。芯片支持eFuse、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LPC/eSPI系统接口与x86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



2 支持产品范围

组件	规格
支持的产品	● 机架服务器：RH1288 V3、RH2288 V3、RH2288H V3、RH5885 V3、RH5885H V3、RH8100 V3、1288H V5、1288X V5、2288 V5、2288C V5、2288H V5、2288X V5、2298 V5、2488 V5、2488H V5、5288 V5、5288X V5、5885H V5、8100 V5、1288H V6、2288H V6、2288E V6、5288 V6、2488H V6、5885H V6、1288H V7、2288 V7、2288H V7、5288 V7、5298 V7、2488H V7、5885H V7、1158H V7、1258H V7、2258 V7、2258H V7、1288 V8、2288 V8、2258H V8、2158H V8 ● 刀片服务器：CH121 V3、CH121H V3、CH121L V3、CH140 V3、CH140L V3、CH220 V3、CH222 V3、CH225 V3、CH226 V3、CH242 V3、CX710、CX220、CX620、CX320、CX318、CX920、CH121 V5、CH121L V5、CH221 V5、CH225 V5、CH242 V5 ● 高密服务器：XH310 V3、XH321 V3、XH620 V3、XH622 V3、XH628 V3、XH321 V5、XH321L V5、XH628 V5、XH321 V6、XH321C V6 ● 关键业务服务器：9008 V5、9008、9016、9032 ● AI服务器：G560、G2500、G5500（G560 V5、G530 V5）、G5500 V6、CX5200 V5、G5200 V7、G5500 V7、G8600 V7、G8600E V7 ● FusionPoD服务器：FusionPoD 600（DH120 V5、DH140CV6、DH120C V5、DH120C V6、DH121C V6）、FusionPoD 700（DH141C V5）、FusionPoD 710（DH140C V6）、FusionPoD 720（DH122E V6、DH120E V7）、FusionPoD for AI（GN560E V7）

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是独立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
3.2 故障诊断与管理（FDM）
3.3 虚拟KVM和虚拟媒体
3.4 基于HTTPS的可视化管理接口
3.5 域管理和目录服务
3.6 固件管理
3.7 智能电源及调速管理
3.8 系统串口重定向及运行记录
3.9 安全管理
3.10 管理接入
3.11 统一用户管理
3.12 配置管理

3.13 存储管理

3.14 时间管理

3.15 SP管理

3.16 iBMA管理

3.17 Kerberos认证

3.18 液冷监控管理

3.19 RADIUS身份认证

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

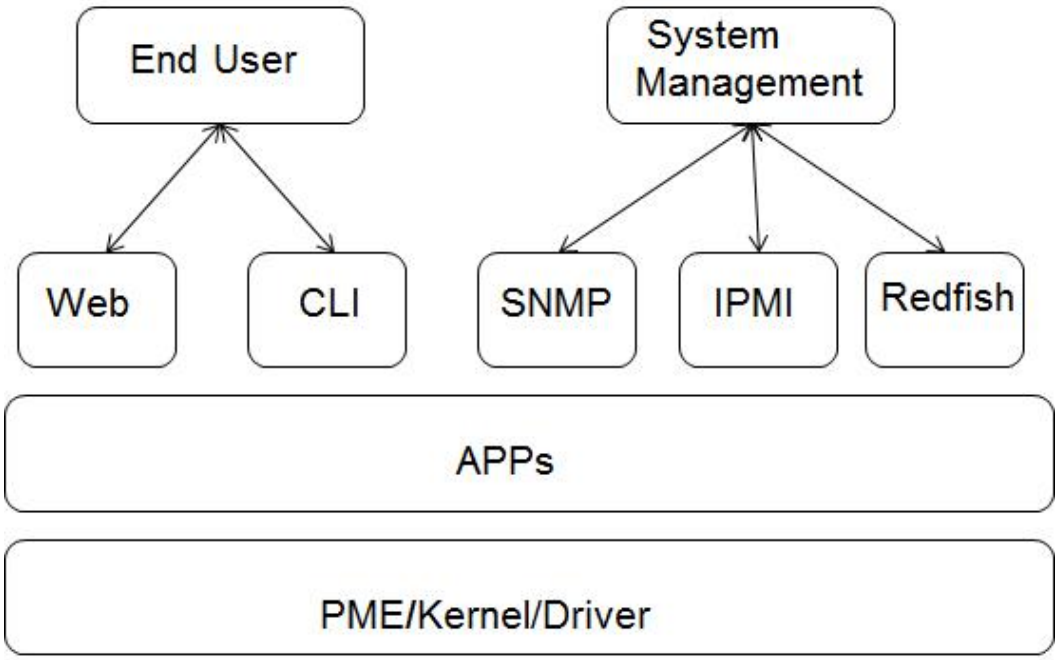


表 3-1 主要集成接口对比

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255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/eSPI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/eSPI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/eSPI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/eSPI

  ipmitool user list

  基于LAN

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

说明

- 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、SHA256、SHA384、SHA512，加密算法支持选择DES或AES、AES256，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。

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. 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。

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

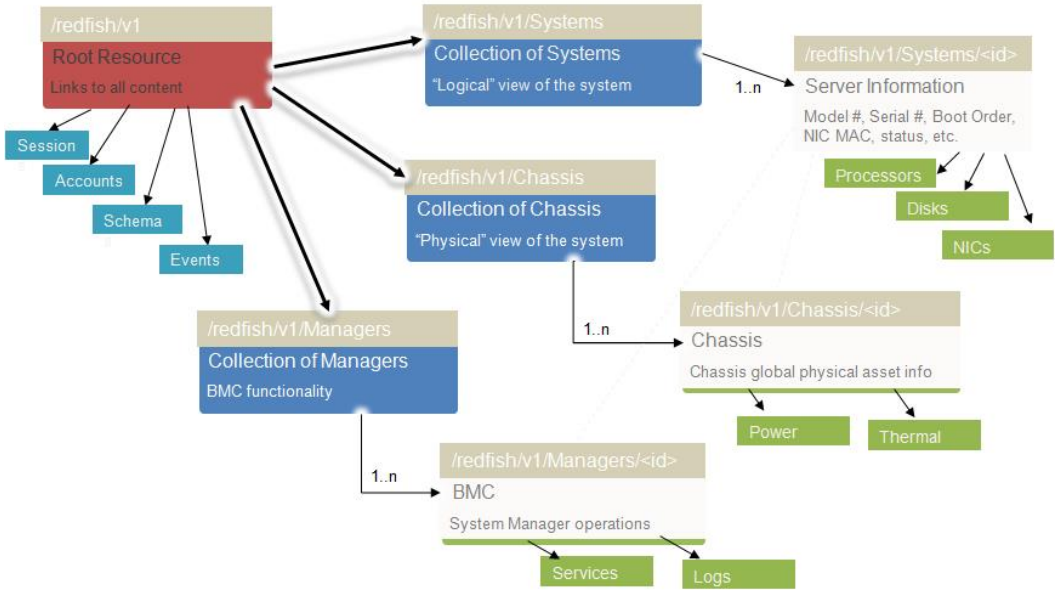
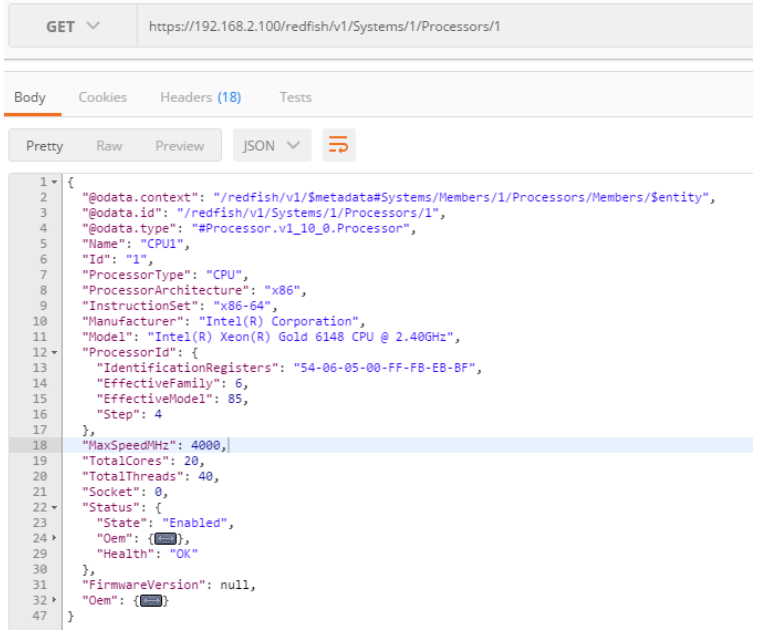


图 3-3 Redfish 接口操作示例(查询处理器资源)



iBMC支持Redfish 1.20.1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. 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。

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. 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。

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所示。

表 3-2 客户端环境要求

操作系统	浏览器	Java运行环境
Windows 7 32位 Windows 7 64位	Internet Explorer 11.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	
	Google Chrome 70.0及以上	
Windows 8 32位 Windows 8 64位	Internet Explorer 11.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	
	Google Chrome 70.0及以上	
Windows 10 64位	Internet Explorer 11.0及以上 Microsoft Edge	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	
Windows Server 2008 R2 64位	Internet Explorer 11.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	
	Google Chrome 70.0及以上	
Windows Server 2012 64位	Internet Explorer 11.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	
	Google Chrome 70.0及以上	
Windows Server 2012 R2 64位	Internet Explorer 11.0及以上	AdoptOpenJDK 8u222 JRE

操作系统	浏览器	Java运行环境
	Mozilla Firefox 63.0及以上	AdoptOpenJDK 11.0.6 JRE
Windows Server 2016 64位	Internet Explorer 11.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	
CentOS 7	Mozilla Firefox 63.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
MAC OS X v10.7	Safari 11.0及以上	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 63.0及以上	

iBMC支持更安全的SSL协议版本：

支持安全的TLS 1.2/1.3协议，TLS 1.3仅支持开启状态，TLS 1.2支持开启/关闭状态。TLS 1.2/1.3均默认开启。

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（优先引导介质、开机启动顺序等）、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。
26. Syslog消息上报配置。

3.1.6 手机 APP 管理接口

iBMC提供了基于手机APP的可视化管理接口，采用安全的HTTPS协议与后台交互，使用户可以方便快捷的开展远程运维，安装要求和支持的服务器请参见**表3-3**和**表3-4**。

安装要求

表 3-3 安装要求

移动端系统	支持版本
Android	Android 8.0及以上版本
IOS	IOS 12.0及以上版本
HarmonyOS	HarmonyOS 2.0及以上版本

支持的服务器列表

表 3-4 支持的服务器列表

服务器类型	服务器型号
机架服务器	1288H V6
	2288H V6
	2488H V6
	5288 V6
	5885H V6
	1288H V7
	2288 V7
	2288H V7
	2488H V7

服务器类型	服务器型号
	5288 V7
	5885H V7
X6000 V6	XH321 V6
	XH321C V6
GPU服务器	G5200 V7
	G5500 V7
	G8600 V7

支持的功能

- 设备管理，包含添加设备，编辑设备及删除设备，可以通过局域网WIFI及Type-C类型USB线直连设备（不支持IOS版本）。

  图 3-4 添加设备界面

- 登录设备，通过手机端保存的设备连接信息来登录设备，添加设备时选择了“记住密码”选项则可直接连接设备，否则需要重新输入密码才能登录。
- 查询设备概况信息。

图 3-5 设备概览界面

- 查询设备告警信息。

图 3-6 设备告警界面

- 对设备主机名设置

图 3-7 设备主机名设置界面

- 对设备进行网口模式及端口设置。

图 3-8 设备网口设置界面

- 对设备进行网络协议及IPv4、IPv6设置。

图 3-9 设备网络设置界面

- 对设备进行VLAN开关及属性设置。

图 3-10 设备 VLAN 设置页面

- 对设备进行区域及时区信息设置。

图 3-11 区域及时区设置界面

- 查看硬件信息，包含内存、处理器、电源、网卡、存储等信息。

图 3-12 硬件信息查看界面

- 对设备进行位置信息设置。

图 3-13 设备位置设置界面

- 查看设备功耗信息，包含系统平均功率、系统累计耗电量、系统峰值功率及部件功耗信息。

图 3-14 设备功耗查看界面

- 对服务器设置启动介质及启动模式。

图 3-15 设备启动设置界面

- 对设备进行上下电操作。

图 3-16 设备上下电界面

- 对设备进行点灯操作。

图 3-17 设备点灯界面

- 查看设备固件信息。

  图 3-18 查看设备固件信息界面

- 导出设备综合信息报告。

图 3-19 设备汇总信息导出报告界面

- 对设备进行一键日志收集。

图 3-20 日志收集提示界面

- 日志管理及一键上传日志。

图 3-21 日志管理界面

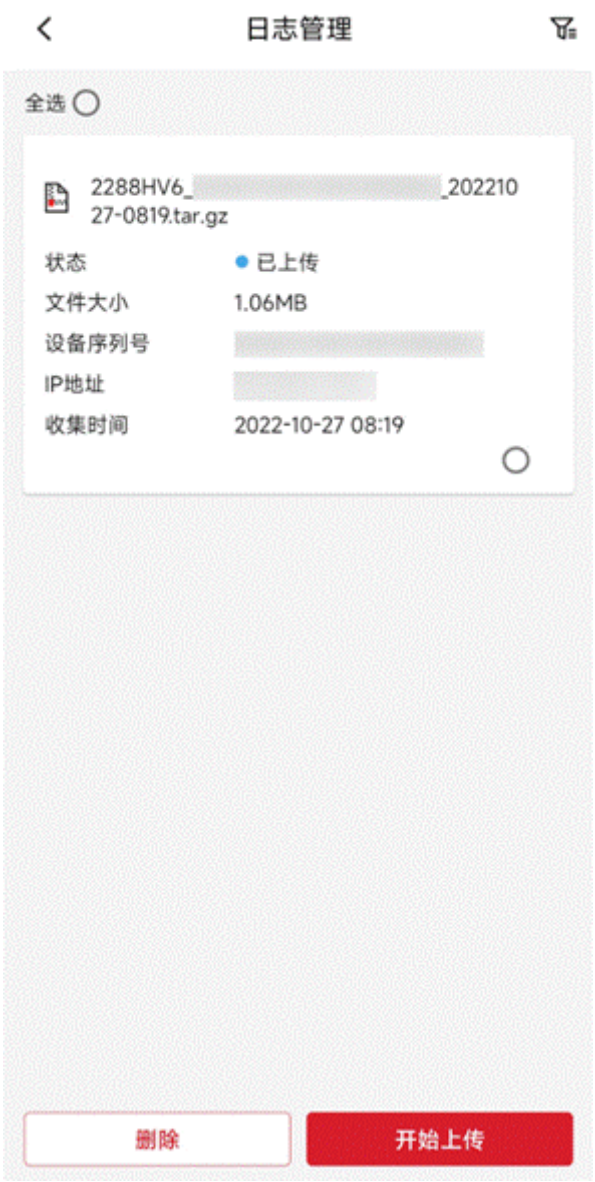
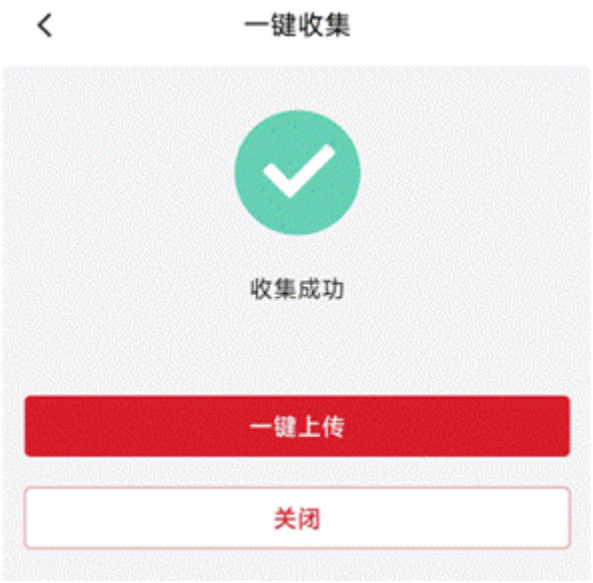


图 3-22 日志收集完成界面



- 查看设备维保信息。
- 查看设备3D图信息。

3.2 故障诊断与管理（FDM）

故障诊断与管理（FDM）是iBMC面向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告警机制，以及针对硬盘、内存和CPU等服务器组件，支持预故障告警。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）；支持CPU CE风暴检测，产生CPU健康状态降级预故障告警
- 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，支持检测风扇转速偏差大并产生预故障告警
- 网卡MCE/AER错误故障
- PCIe标卡（网卡、RAID卡、GPU卡等）UCE故障精准告警功能，能够触发告警并明确指示具体的故障部件位置；支持PCIe CE风暴检测，产生PCIe标卡健康状态降级预故障告警
- 系统电源故障（AC/DC输入丢失、高温、电源风扇故障、过压、过流），支持电源温度偏高预故障告警
- 总线故障（I2C、IPMB、QPI/UPI/HCCS），支持QPI/UPI CE风暴检测，产生QPI/UPI健康状态降级预故障告警
- DDR3/DDR4/DDR5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），针对内存UCE Non-Fatal等故障能够触发告警并明确指示具体的故障内存位置。可支持内存故障预测隔离功能，提前识别内存CE错误并针对风险区域实施隔离操作，降低业务宕机率

- 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计数超门限预故障、NVRAM错误计数非0、BMC访问失败）、硬盘故障告警精细化（物理故障、硬盘固件状态异常、硬盘有外部配置、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、黑屏/蓝屏故障
- 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 3-5 iBMA 获取的 RAID 卡和硬盘故障及故障定位信息

获取信息描述	LSI2208	LSI2308	LSI3008	LSI3108	SAS34/35/38/39系列	软RAID	PCH硬盘	NVMe	备注
RAID降级	支持	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	不支持	NA	NA	NA	iBMC呈现告警
硬盘Offline	支持	支持	支持	支持	不支持	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	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	不支持	支持	支持	支持	iBMC呈现告警
硬盘Sense Code错误	不支持	不支持	支持	支持	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
硬盘性能下降	不支持	不支持	支持	支持	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	不支持	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

获取信息描述	LSI2208	LSI2308	LSI3008	LSI3108	SAS34/35/38/39系列	软RAID	PCH硬盘	NVMe	备注
expander误码	不支持	不支持	支持	支持	不支持	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	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	不支持	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	不支持	支持	支持	不支持	iBMC呈现告警
硬盘IO异常检测	不支持	不支持	支持	支持	支持	支持	支持	不支持	iBMC呈现告警

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 3-6 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系统检测
	OAM链路故障	iBMC呈现告警，支持Linux系统检测
	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
HBA卡	链路状态（LinkDown）	iBMC记录提示级别SEL日志

类型	状态描述	备注
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

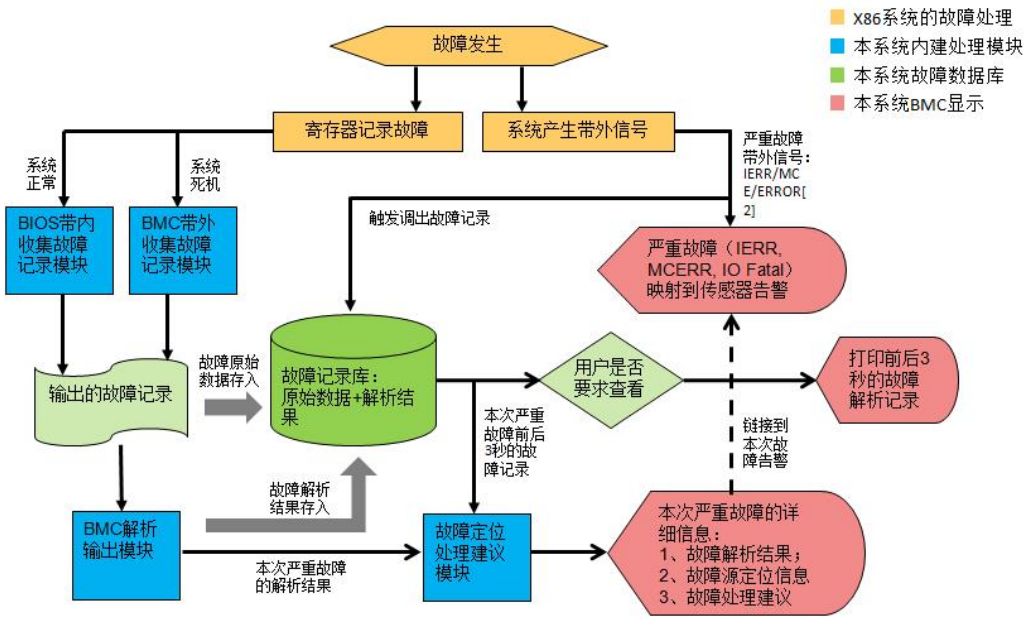
3.2.2 故障诊断

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 3-23 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

2288H V5等V5系列服务器BMC提供故障分析功能（部分机型支持），支持CPU、内存、硬盘、RAID卡、网卡的故障日志，主要支持的能力如下：

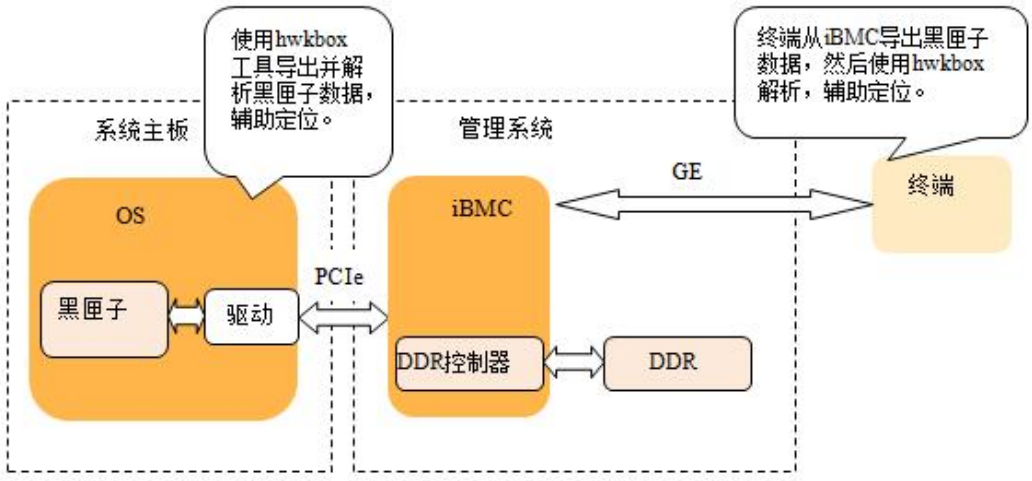
故障预警历史事件的查询

图 3-24 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（iBMA中hwkbox组件）三个模块协同完成，默认关闭。按照如图3-25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 3-25 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3-26）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 3-26 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，如下所示，[]内数字表示本次系统启动的故障码。

```
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

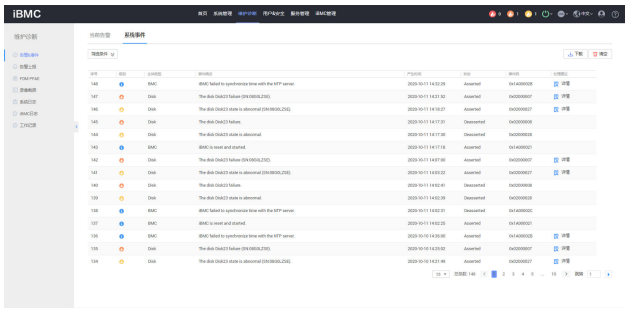
在可靠的故障检测基础上，iBMC智能管理控制器还实现了丰富的告警管理功能。

- 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、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3-27**所示。

图 3-27 系统事件界面



系统事件参数说明如**表3-7**所示。

表 3-7 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。

参数	说明
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

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3-28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3-29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 3-28 SNMP TRAP 配置界面

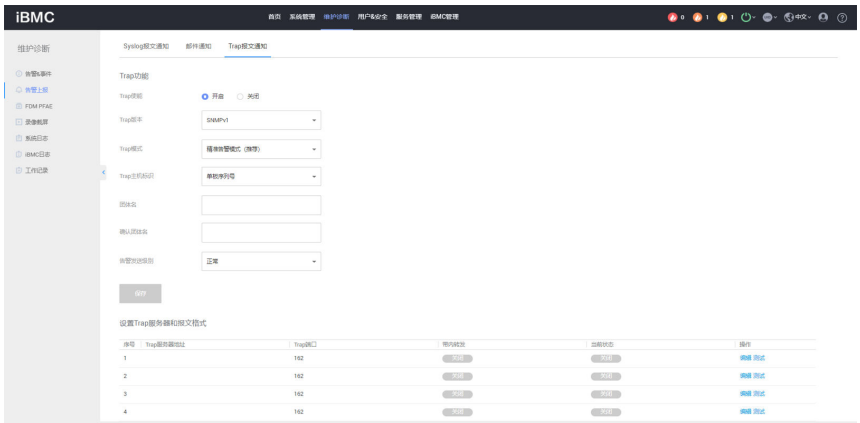


图 3-29 SMTP 配置界面

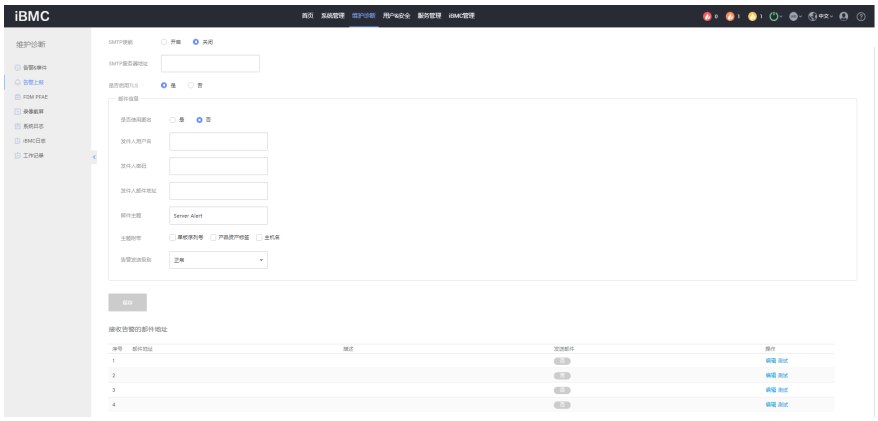
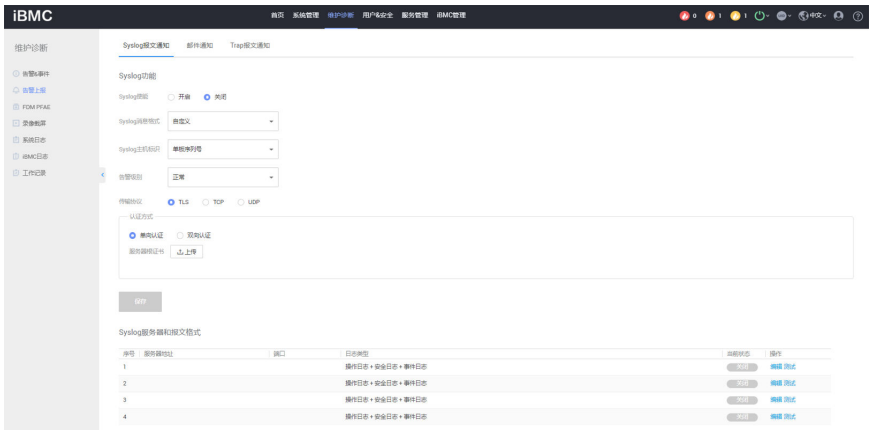


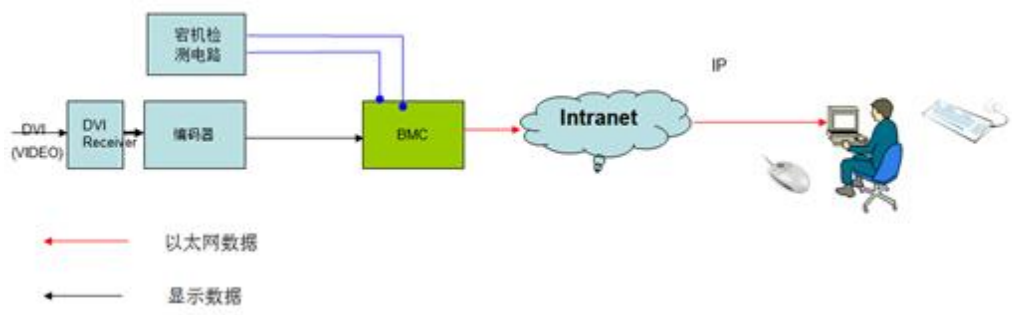
图 3-30 Syslog 配置界面



3.2.8 宕机截屏

如图3-31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。

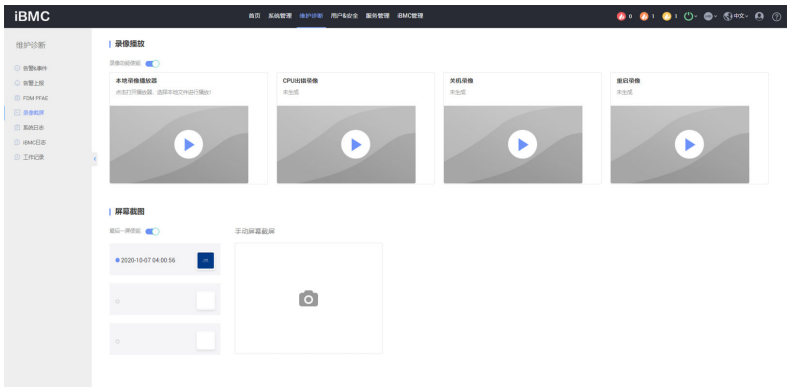
图 3-31 宕机截屏原理



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3-32所示。

图 3-32 宕机截屏界面

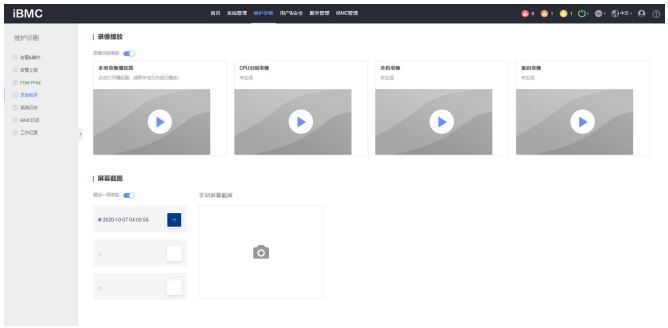


3.2.9 宕机录像

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3-33所示。

图 3-33 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。

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。

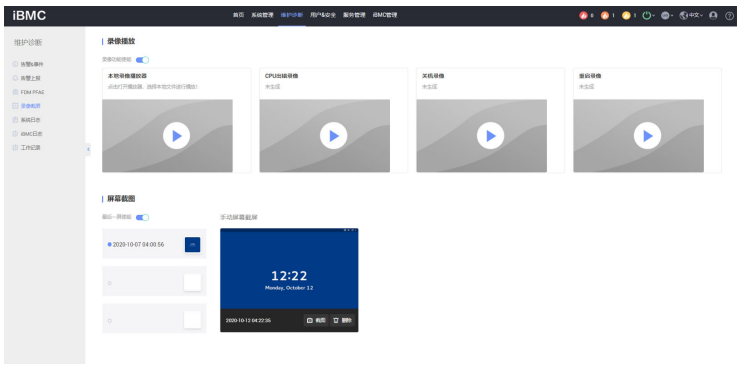
- 使用指南

  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。

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3-34所示。

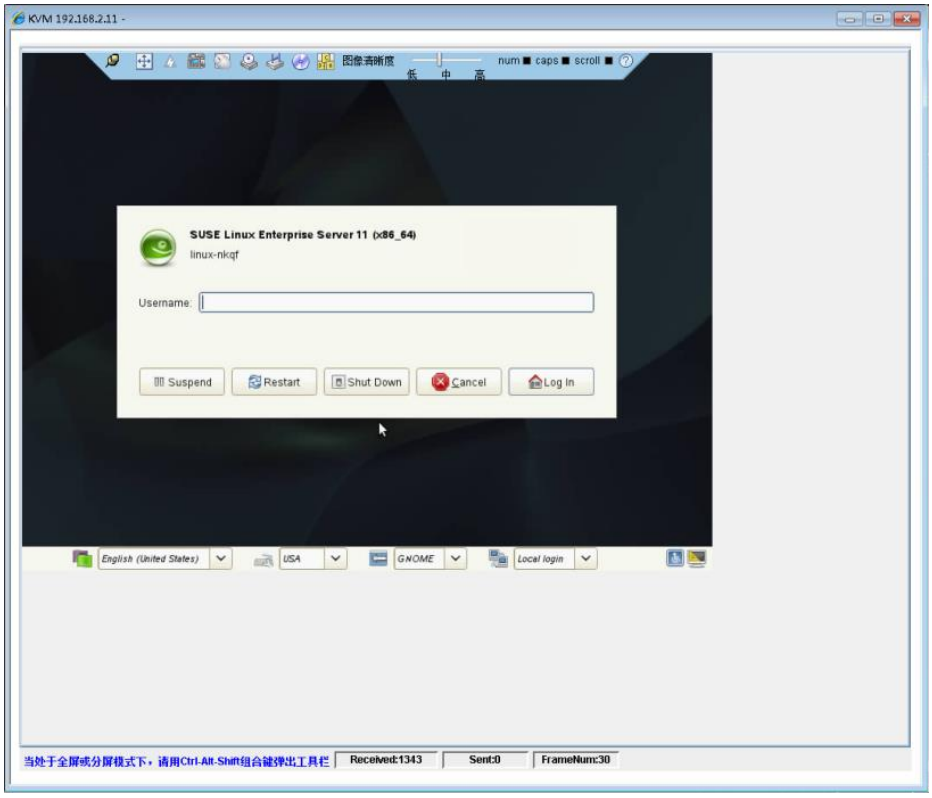
图 3-34 手动截屏界面



3.2.11 屏幕录像

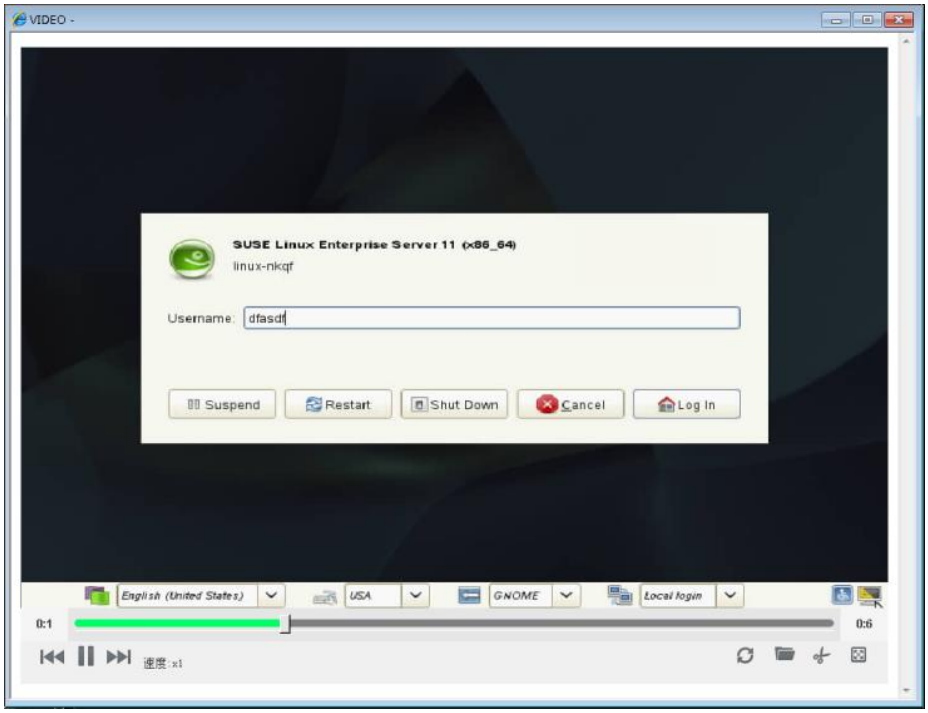
屏幕录像是虚拟KVM控制台上提供的一项远程KVM录像功能，需手动启动，录像格式为自定义，录像数据保存在本地(打开KVM控制台的计算机)；当用户出于安全或者其他需要，要将虚拟KVM操作过程记录下来时，可以通过启动屏幕录像功能来实现。屏幕录像功能启动后，虚拟KVM控制台会自动将屏幕上的所有显示和操作都记录到自定义视频格式文件中。

图 3-35 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 3-36 录像回放控制台



3.2.12 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。故iBMC新增部件更换记录的功能，仅V5及以上系列产品支持此功能。

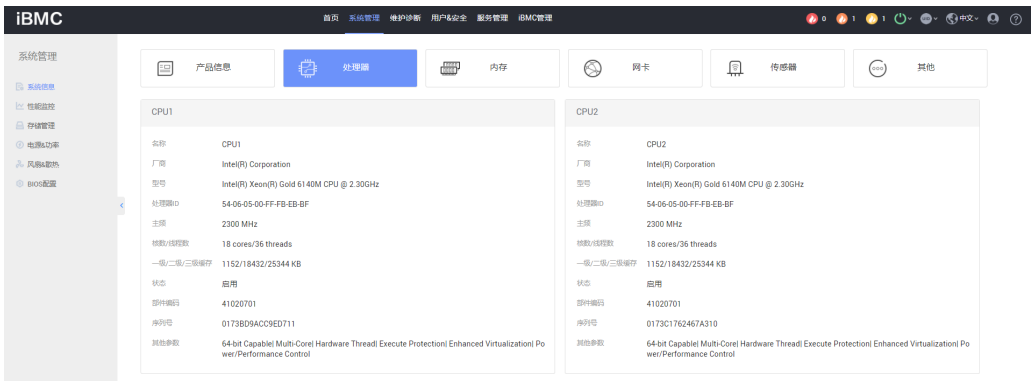
服务器的CPU、内存、硬盘进行更换，在服务器重新上电后，iBMC会产生一条部件更换事件，事件描述信息中会包含更换前后部件的SN信息。对于硬盘，只有支持带外管理的硬盘和NVME盘才能支持部件更换记录。以内存为例，在内存被更换服务器上电后会产生如下事件：

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

3.2.13 Bom 编码管理

Bom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。Bom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Bom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Bom编码如下：

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

3.2.14 系统看门狗

iBMC支持IPMI规范定义的标准看门狗定时器功能，可以通过OS内系统管理软件或BIOS配合实现OS或BIOS运行状态的监控和异常恢复处理措施。iBMC支持提供设置看门狗超时时间及超时后处理动作的IPMI命令，以及重置看门狗的命令。在设置的看门狗超时时间内没有收到重置看门狗命令的场景下，BMC可以执行用户设置的恢复动作（No Action、Power Off、Hard Reset、Power Cycle）尝试恢复系统。

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3-37**所示，HTML5控制台界面如**图3-38**。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。

远程控制台支持退出后触发系统自动锁定，有效防止系统信息泄露或入侵。

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3-39**。
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3-40**，仅支持V5及以上系列服务器。
4. iBMC Web和URL方式打开HTML5控制台，通过HTML JS加载控制台，仅支持V5及以上系列服务器。

表 3-8 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。	仅V5及以上系列产品支持。
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。	仅V5及以上系列产品支持。
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 3-37 JAVA 远程控制台(嵌入 Web)

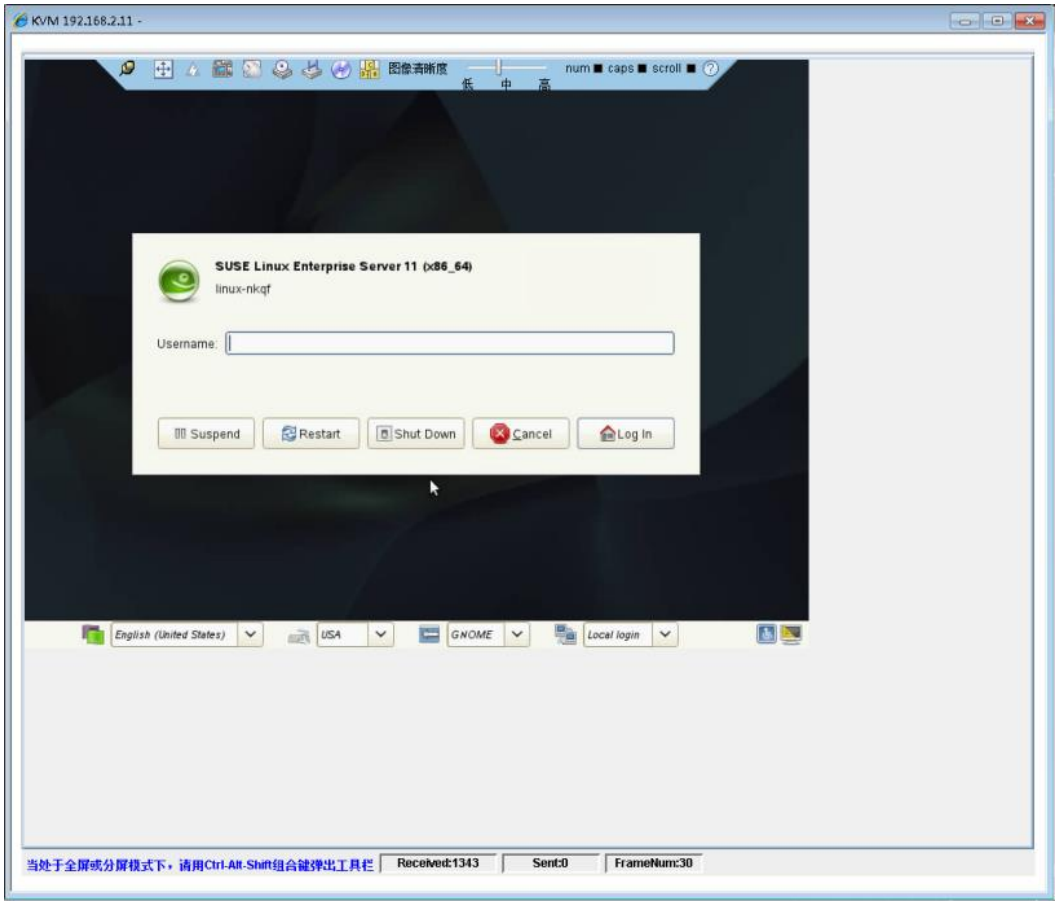
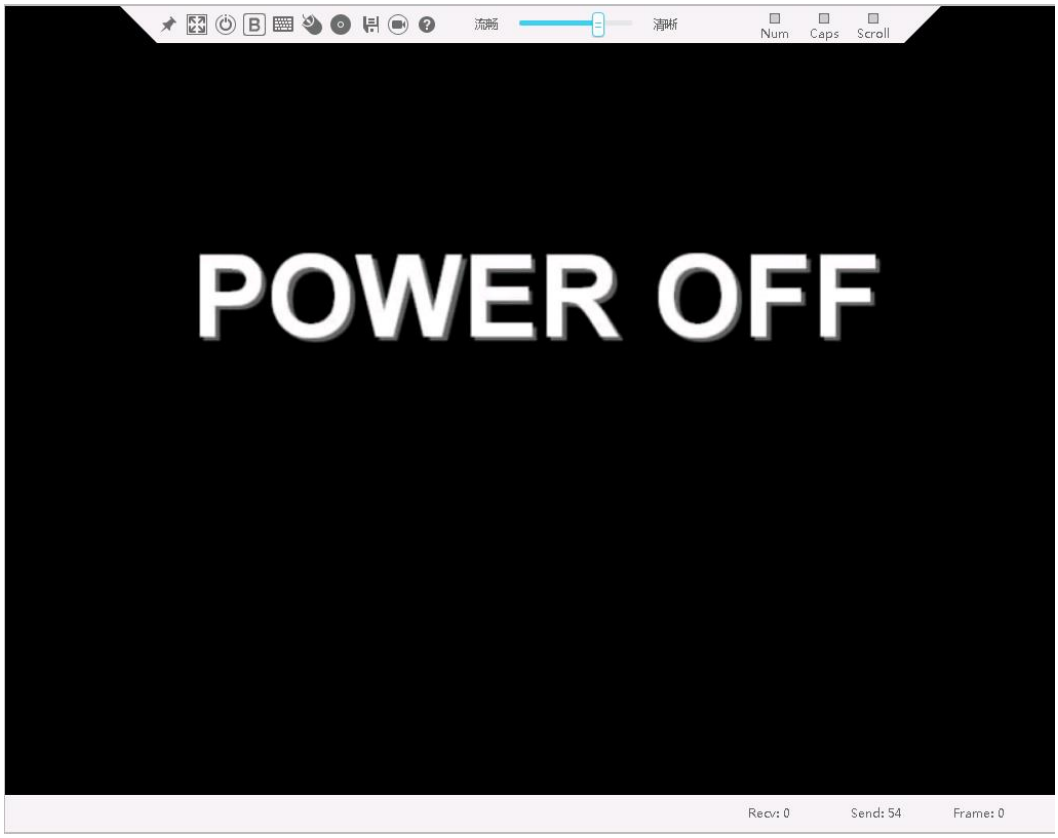


图 3-38 HTML5 远程控制台（嵌入 Web）



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：IE11.0及以上、Firefox 63.0及以上和Chrome 70.0及以上。

图 3-39 JAVA 控制台登录界面（独立）

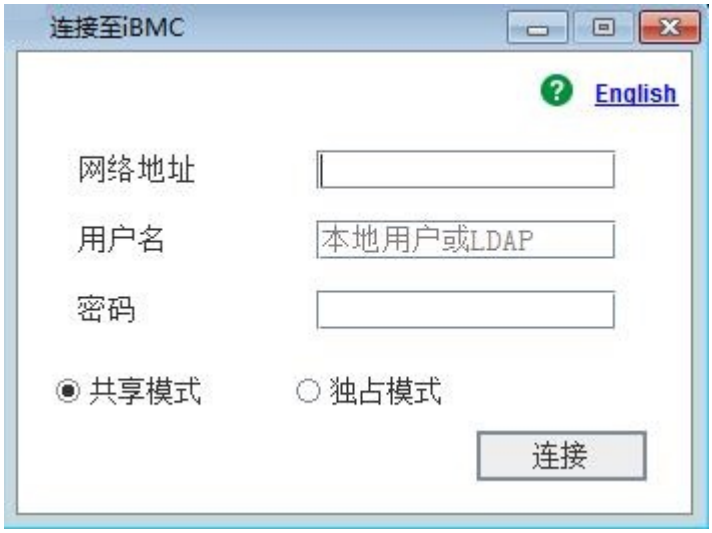
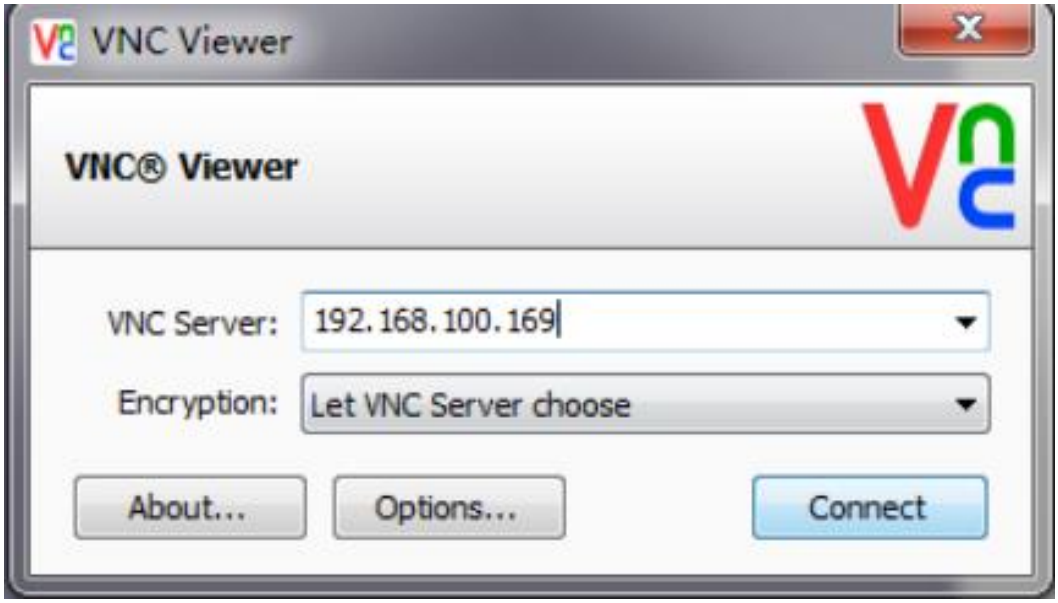


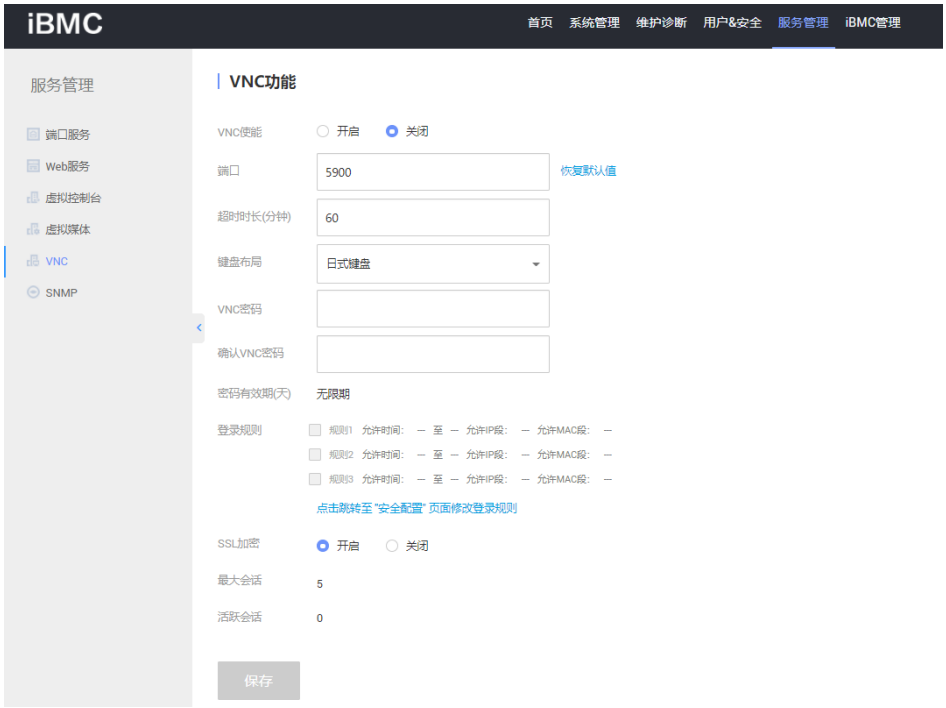
图 3-40 VNC 客户端（独立）



VNC协议具有如下特点：

1. VNC仅提供KVM功能，不支持虚拟媒体。
2. VNC遵循标准协议，能与第三方VNC客户端对接。
3. 仅提供密码认证，有自己独立的密码。
4. 使用跟键盘布局有关，支持美式键盘和日式键盘。

图 3-41 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3-9**。
- 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。

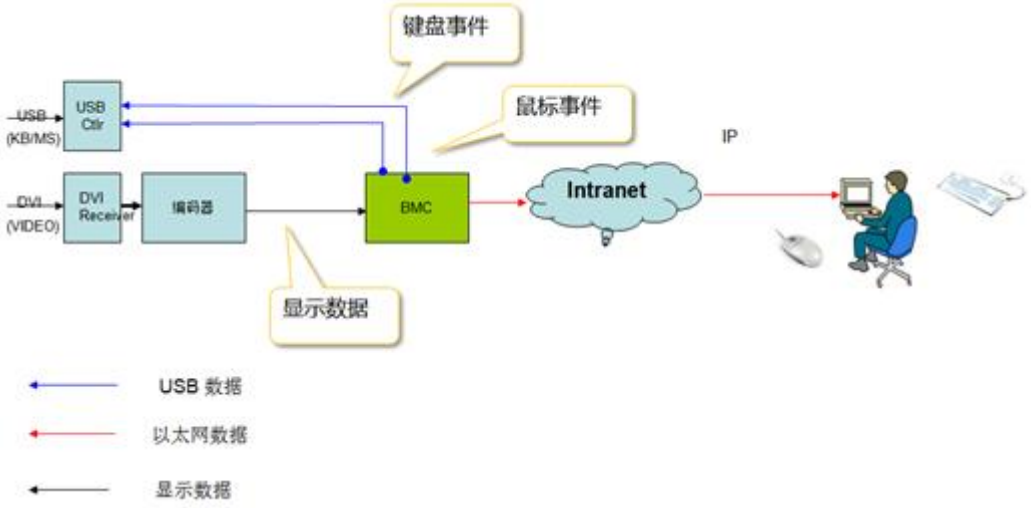
表 3-9 不支持鼠标同步功能的 OS 列表(包括但不限于)

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3-42**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 3-42 虚拟 KVM 实现原理



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3-43**所示。

图 3-43 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24 Mbit/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。

3.4 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3-44**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 3-44 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3-45**所示。

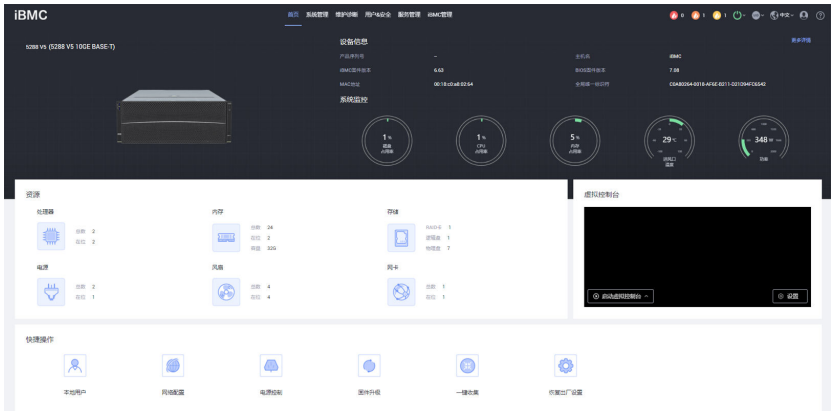
图 3-45 登录 iBMC Web

----结束

3.4.1 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、虚拟按钮和虚拟控制台链接信息，并提供常见操作接口链接，如**图3-46**所示

图 3-46 总体概况界面



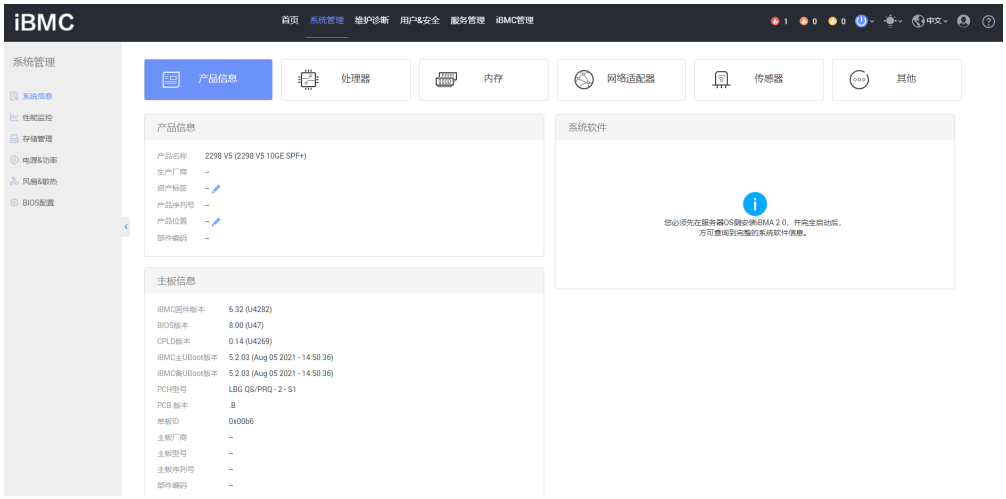
3.4.2 查看系统信息

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部件信息。

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3-47所示。

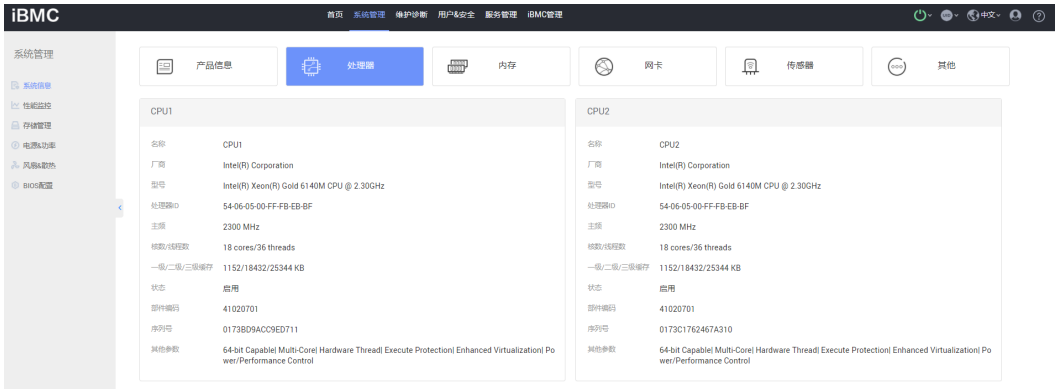
图 3-47 固件版本界面

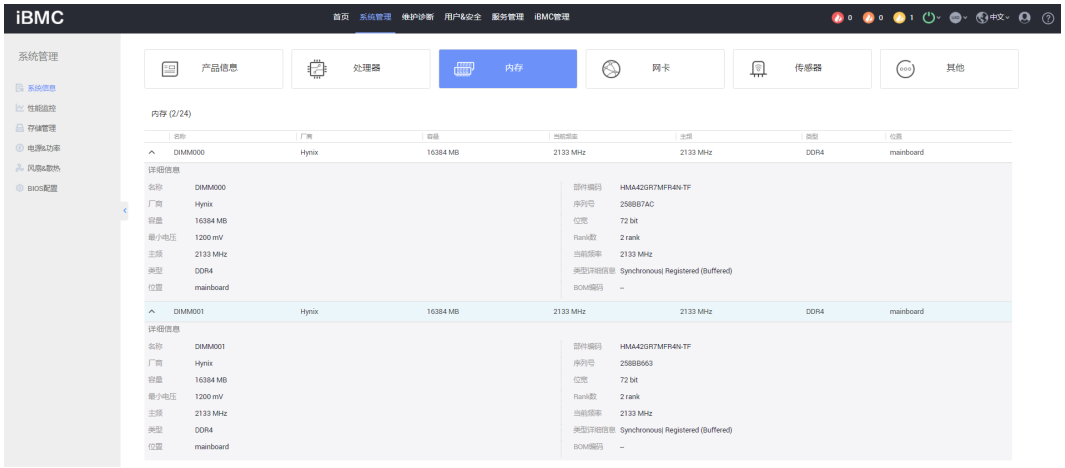


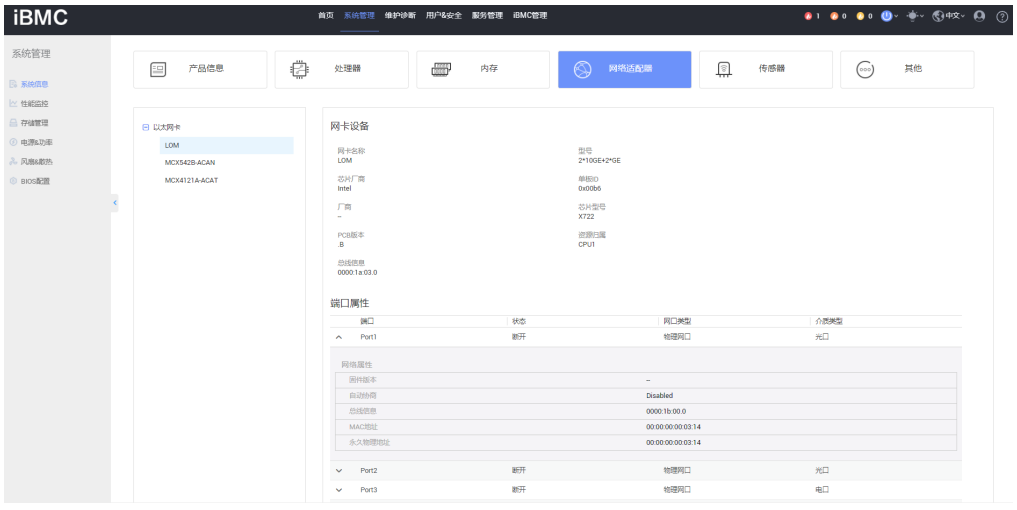
整机硬件

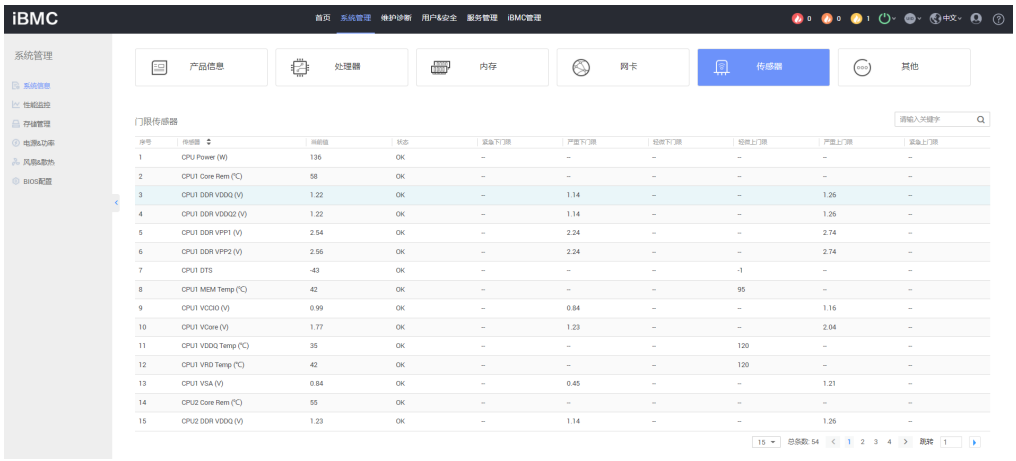
整机硬件信息包括系统主要部件的最大配置数、当前配置数和型号，其中“网络”和“系统软件”部分需要安装iBMA2.0软件，如下图所示。

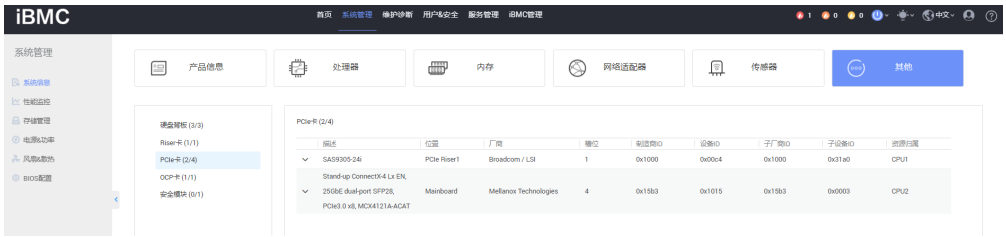
图 3-48 整机硬件界面

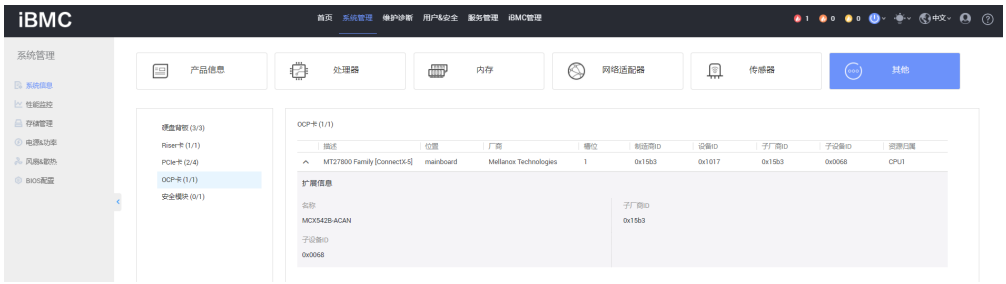












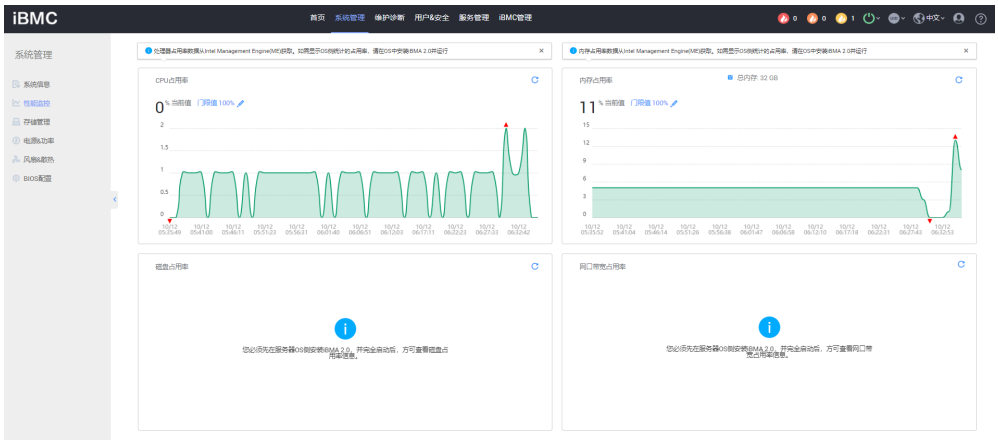
3.4.3 性能监控

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。

实时数据

如图3-49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 3-49 实时数据界面



传感器

传感器界面显示设备所有传感器信息，如**图3-50**所示，相关的参数如**表3-10**所示。

图 3-50 传感器界面示例

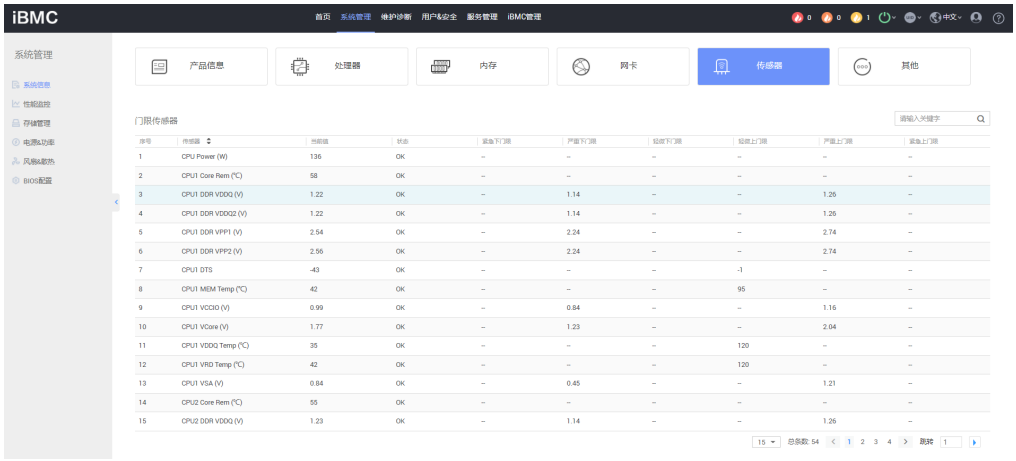


表 3-10 门限传感器界面各参数说明

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。

参数	说明
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。

3.4.4 设备定位

如图3-51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 3-51 设备定位界面

3.5 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。

3.5.1 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。

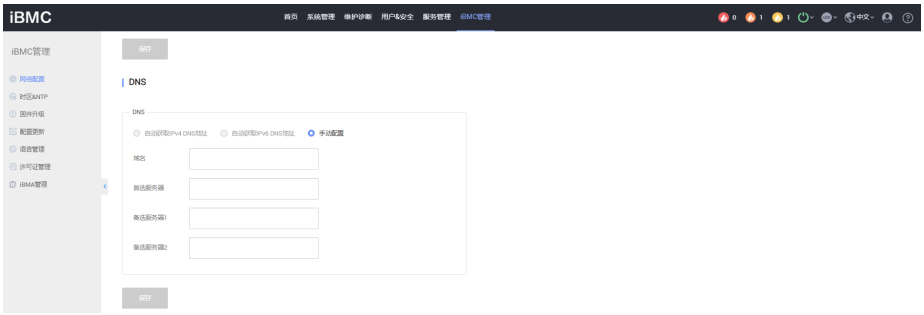
1. 在iBMC的Web中打开“网络配置”界面，如图3-52所示。

   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3-52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 3-52 DNS 配置界面



步骤2 在如图3-53所示界面中设置主机名。

图 3-53 主机名配置界面

----结束

3.5.2 目录服务

按照如图3-54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。

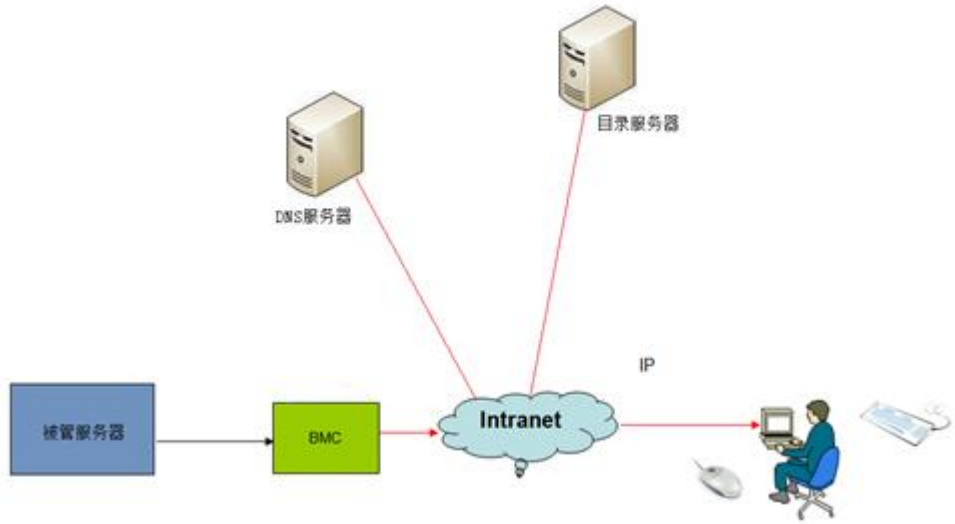
LDAP标准优点：

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 3-54 目录服务原理



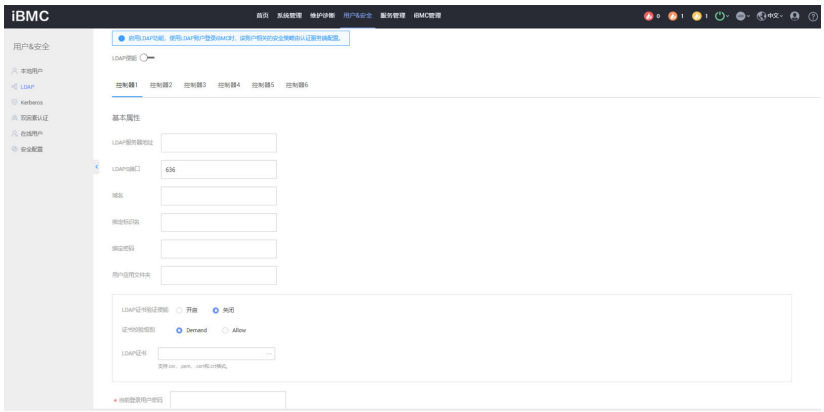
打开“LDAP用户”界面，如图3-55所示。

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3-55中，可以显示或配置LDAP用户的相关信息。

图 3-55 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。

3.6 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。

3.6.1 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。

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3-56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 3-56 固件升级界面

3.6.2 固件升级

支持对iBMC固件、BIOS、CPLD（主板\背板\扣卡\扩展板）、LCD固件、电源固件的远程升级；其中iBMC固件支持主备镜像倒换回滚和本地固件更新，如图3-57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，支持固件合法性和完整性校验。

图 3-57 固件升级界面

支持对RAID卡、网卡、硬盘固件的远程升级，升级文件必须和同名的asc格式签名文件同时上传，执行升级操作时会设置OS从SP启动，SP启动完成后执行固件升级生效。

3.6.3 BMC 升级与生效分离

基于Hi1711芯片的iBMC，支持iBMC固件升级与生效分离的能力，默认升级后立即复位生效，支持用户选择下次复位时生效。

3.7 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。

3.7.1 电源控制

电源控制界面提供对服务器的远程开关机等电源控制方式，如图3-58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 3-58 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：

- 默认延迟：0～2秒内随机延迟。通电后在0～2秒内随机延迟上电。
- 二分延迟：50%概率延迟。通电后有50%的概率按照已设定的时间（0~120s）延迟上电。
- 固定延迟：固定时间延迟。通电后按照已设定的固定时间延迟（0~120s）上电。
- 随机延迟：0～M秒内随机延迟，延迟上限为M秒（0~120s）。通电后在0～M秒内随机延迟上电。
- 刀片类产品(包括高密度产品)，支持根据槽位顺序延迟上电，每槽位至少延时500ms。

3.7.2 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3-59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3-59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”。

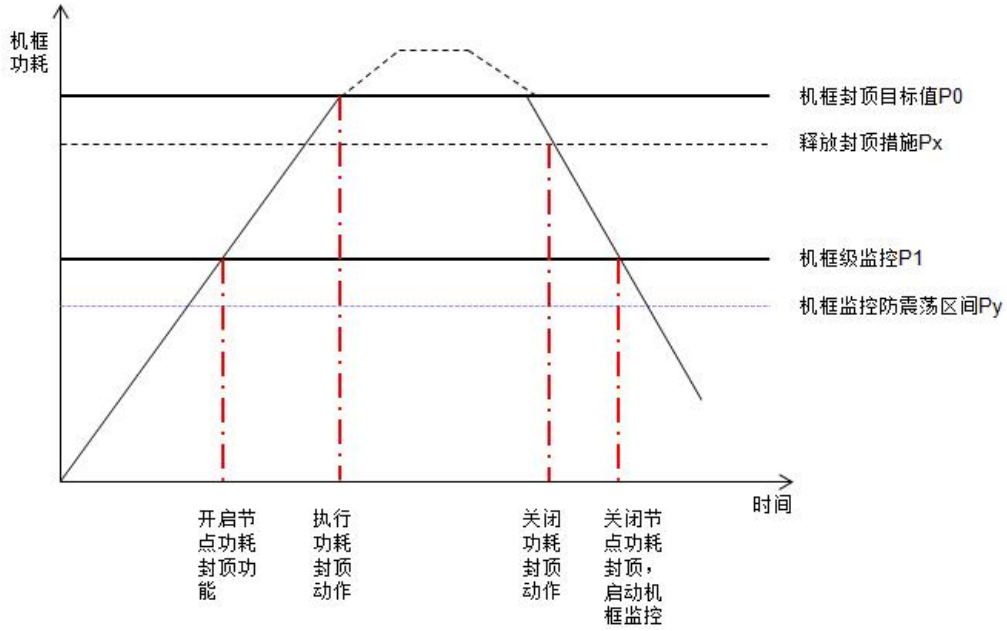
封顶失败进一步动作包括：

- 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 3-59 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 3-60 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 3-61 整框功率封顶信息

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

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

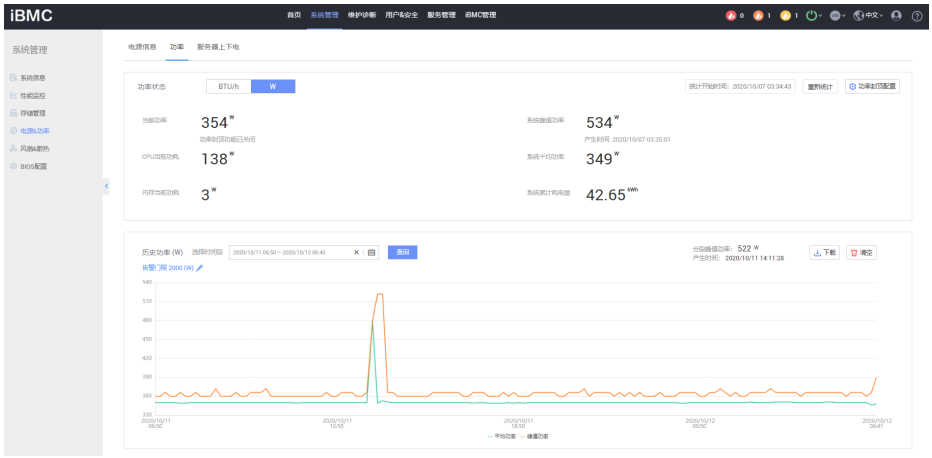
3.7.3 功率统计和历史曲线

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3-62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 3-62 功率统计界面

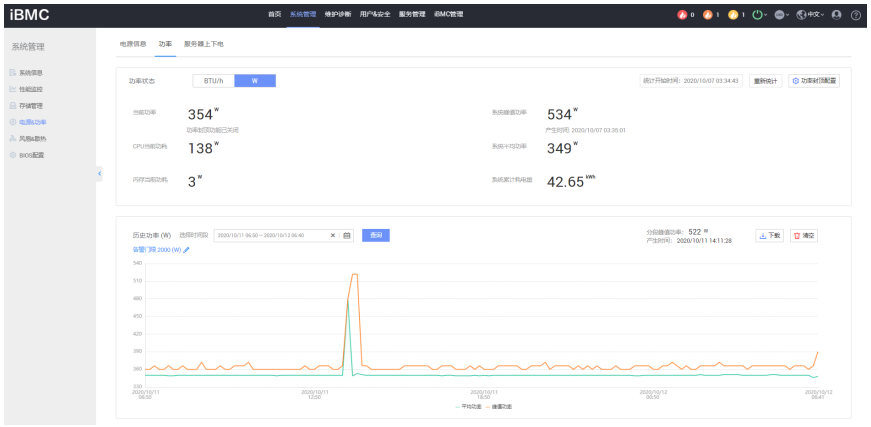


在导航树上选择“电源管理 > 历史功率”，打开“历史功率”界面，如图3-63所示。

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 3-63 历史功率界面



3.7.4 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（仅V5及以上产品且系统下电状态支持），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。

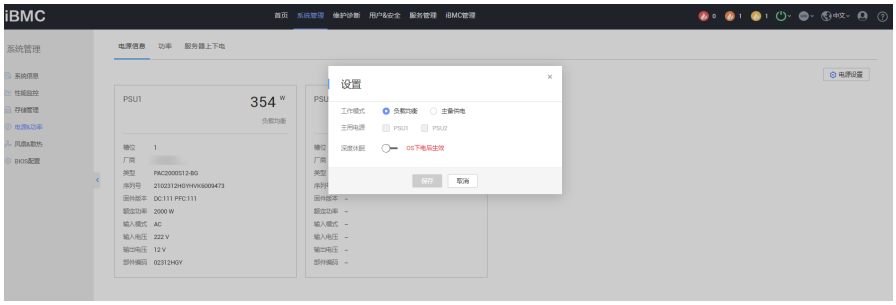
备用电源投入供电条件(主备模式切换为负载均衡模式)：

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3-64**所示，提供电源供电总体工作模式、主用电源的设置接口。

针对深度休眠功能，当开启深度休眠后，系统下电后，进入深度休眠模式的电源会关闭输出；关闭深度休眠或系统上电后，进入深度休眠模式的电源会恢复输出。开启深度休眠模式，系统下电后，如果所有主用电源被拔掉或者发生故障导致输出关闭，整机会掉电10秒左右，然后处于深度休眠模式的电源会自动打开输出。

图 3-64 主备供电界面



3.7.5 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3-65**，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。

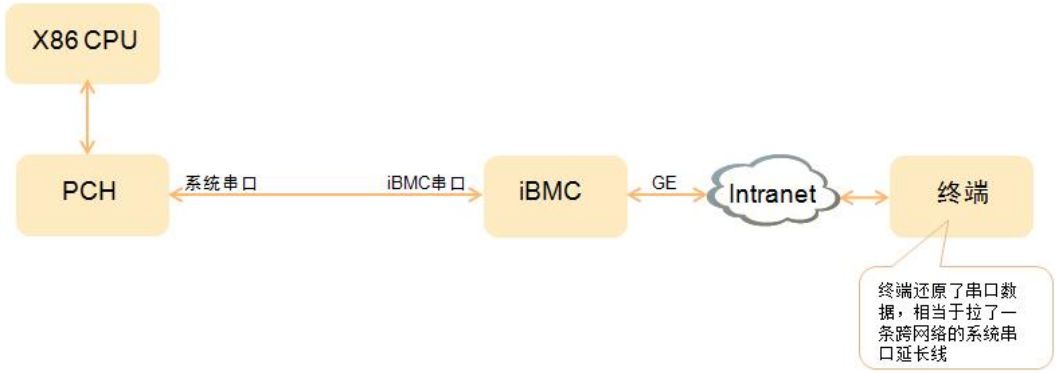
图 3-65 智能调速配置界面

3.8 系统串口重定向及运行记录

3.8.1 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3-66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。

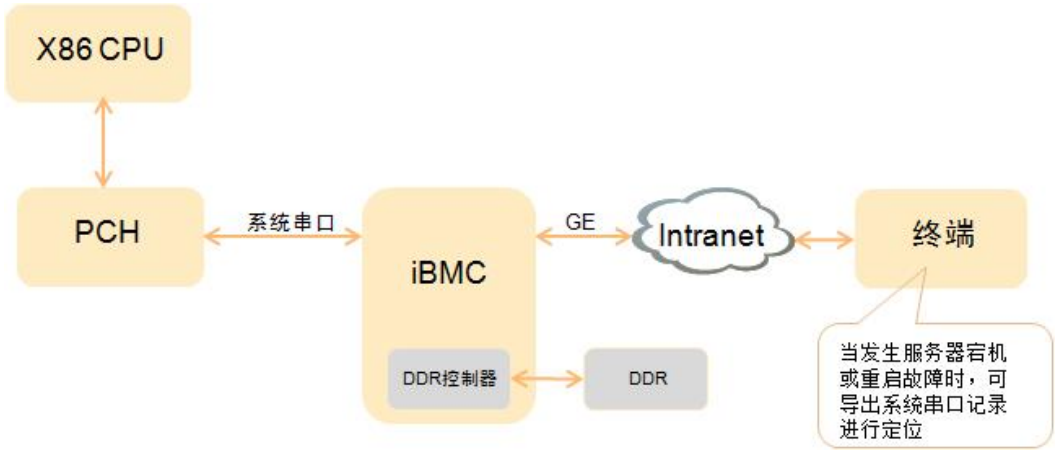
图 3-66 系统串口重定向原理-x86



3.8.2 系统串口信息记录

iBMC提供系统串口信息记录功能。如图3-67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 3-67 系统串口信息记录原理-x86



web展示界面

图 3-68 Web 展示界面

3.9 安全管理

3.9.1 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、弱口令字典、禁用历史密码、密码有效期、密码最短使用期、不活动期限、紧急登录用户、账号防暴力破解（登录失败锁定）、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录；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。

不活动期限：超过设定期限内未活动的用户会被禁用。

紧急登录用户：不受密码有效期、登录规则和登录接口限制的用户，用于紧急情况下登录iBMC，默认为空。

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。

弱口令字典：支持CLI接口设置弱口令字典认证使能状态和导入、导出弱口令字典，在密码复杂度检查和弱口令字典认证功能使能的情况下，所设置密码不能在弱口令字典中。

在线用户：支持查看已登录iBMC系统的用户信息，并支持注销已登录的用户。

3.9.2 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，用户口令采用PBKDF2算法计算口令单向哈希，可有效防止密码被明文破解。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。

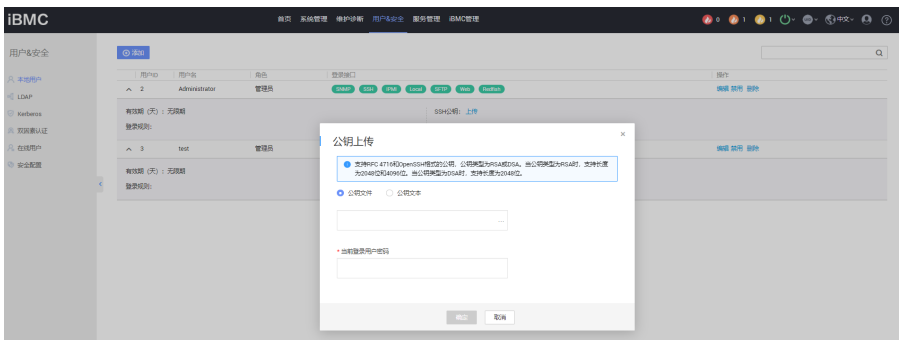
SSH公钥认证：SSH支持用户名、密码和公钥方式认证，公钥方式适合于自动配置工具，无需输入密码的交互步骤。

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，主要特性如下：

- 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。

3.9.3 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 3-69 自定义角色应用

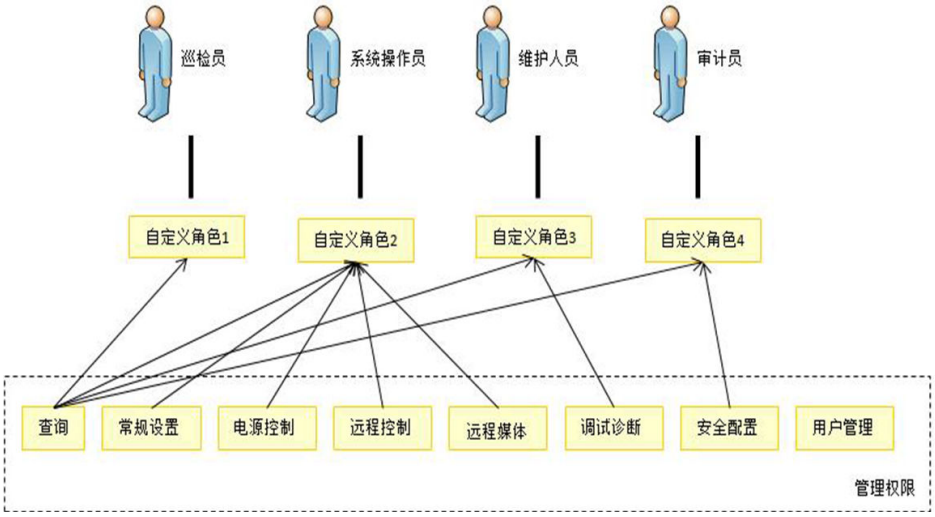
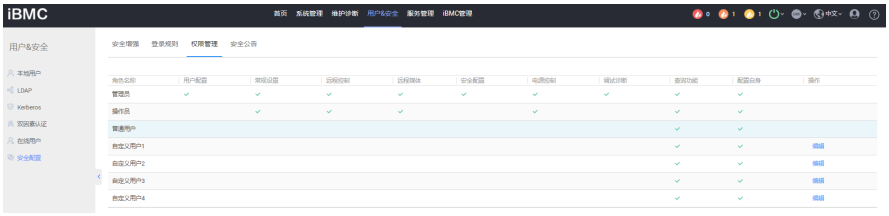


图 3-70 角色自定义界面



3.9.4 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，同时支持证书过期前告警提示。

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。

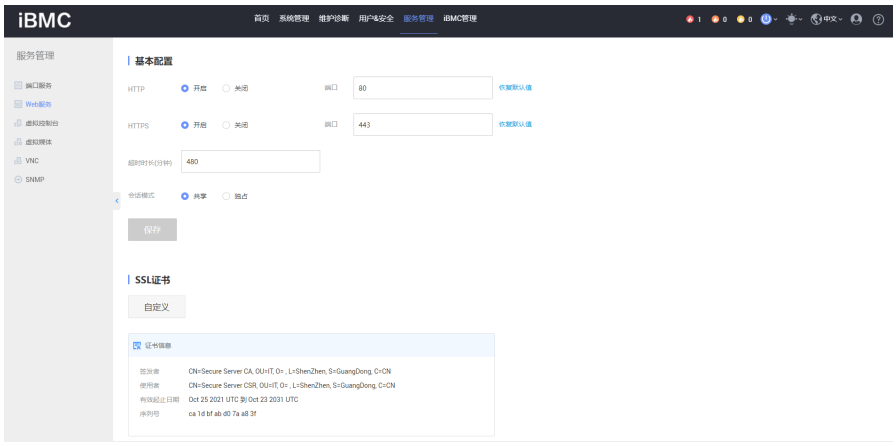
说明

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。

图 3-71 SSL 证书管理界面



针对Redfish等接口涉及访问远程共享路径的场景，访问远程HTTPS共享路径前支持校验对端服务器证书，在iBMC中导入远程共享文件服务器证书对应的根证书，在访问远程路径时iBMC支持校验对端服务器证书，从而避免文件共享服务器被伪造，能有效保证共享文件的合法性。

3.9.5 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

- 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。
- 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。

3.9.6 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TLS1.2及以上版本。为保持浏览器兼容性，默认开启TLS1.2/TLS1.3，用户可以登录iBMC禁用TLS1.2。

SNMPv3：

1. 认证算法支持MD5、SHA、SHA256、SHA384、SHA512，支持用户配置。
2. 加密算法支持DES、AES、AES256，支持用户配置。

3.9.7 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 3-11 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	PBKDF2
SNMP V3用户密码	MD5、SHA-1、SHA-256、SHA-512
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。

3.9.8 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地址黑/白名单，黑名单可以设置阻止访问，白

名单可以设置允许访问，规则重叠时黑名单的优先级高于白名单，仅允许符合规则的设备访问系统，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；

由用户根据需要可设置登录规则黑名单和白名单各三组，同一用户登录时，仅设置了白名单规则且匹配上任意一条白名单登录规则时，即可登录，否则拒绝登录；仅设置了黑名单规则且匹配上任意一条黑名单登录规则时，即拒绝登录，否则可登录；同时设置了黑白名单时，白名单登录规则内可登录，黑名单登录规则内拒绝登录，重叠规则内拒绝登录，未匹配到规则的部分禁止登陆；

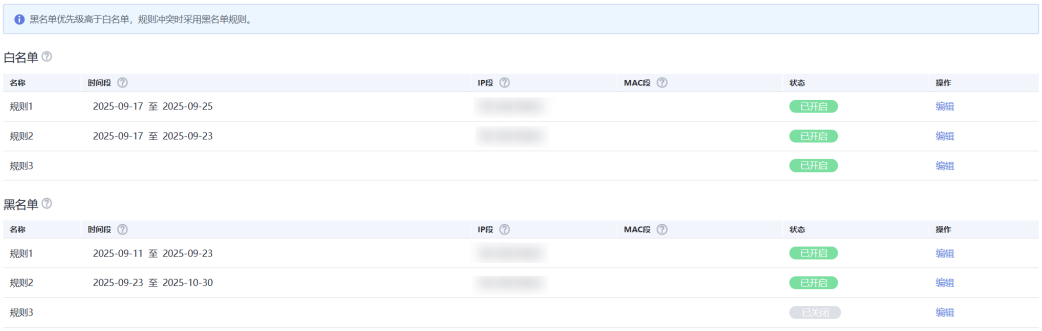
每条登录规则包括时间段、登录用户的源IP段和MAC段，这三个条件必须同时满足才认为匹配到一条登录规则；登录规则可应用于所有本地用户和LDAP用户组；

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。

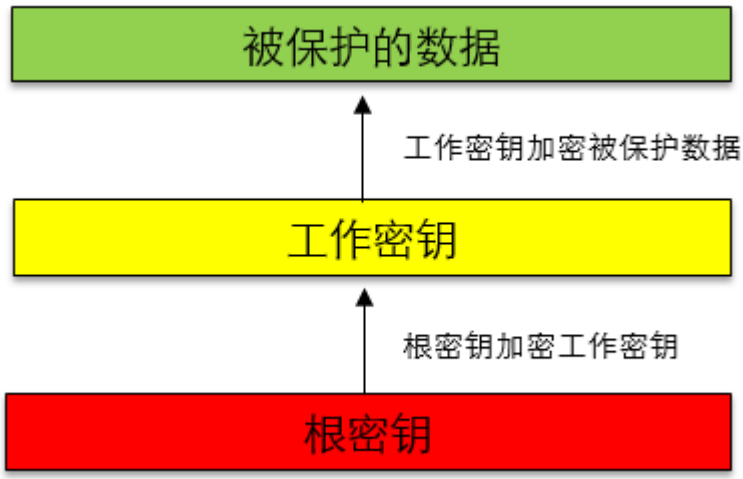
2. 系统锁定

   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。

3.9.9 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。

3.9.10 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。

3.9.11 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。

3.9.12 DICE

基于Hi1711芯片的iBMC支持提供DICE挑战接口，接收挑战请求，返回DICE证书链。基于DICE引擎，生成固件可信启动证书链，基于证书链进行挑战验证，校验启动固件完整性。

3.9.13 安全启动

基于Hi1711芯片的iBMC，支持基于硬件可信根的安全启动，对uboot、BMC、BIOS、ME进行数字签名校验，数字签名校验通过才允许启动，防止固件被恶意篡改。同时支持PFR机制，iBMC启动完成后获取BIOS的签名校验标记，如果校验错误，则使用备份区的BIOS文件重新升级BIOS。iBMC自身三次启动失败后会从备区启动恢复管理功能。

3.9.14 PFR

基于Hi1711芯片的iBMC，支持iBMC自身3次启动失败后备区升为主区，并对校验不通过的分区固件执行恢复动作；iBMC启动完成后获取BIOS的签名校验结果，如果结果显示校验失败，则使用备份区的BIOS固件重新升级BIOS。

3.9.15 不安全版本吊销

基于Hi1711芯片的iBMC，版本支持唯一标识符来识别对应版本，可以对指定不安全版本进行吊销，吊销后指定的风险版本在升级前会被拦截阻止，避免误升风险版本。

3.9.16 电子保单管理

基于Hi1711芯片的iBMC，支持提供电子保单信息查询和设置能力，支持Redfish/Web接口查询产品名称、产品序列号、生产日期、UUID、服务起始时间、服务年限，支持配置服务起始时间和服务年限。

3.9.17 PCI DSS 认证

Payment Card Industry (PCI) Data Security Standard，第三方支付行业(支付卡行业PCI DSS)数据安全标准，是一种全球信息安全标准，力在使国际上采用一致的数据安全措施，简称PCI DSS。2288H V7、2288H V6、2488H V6服务器已获得PCI DSS 4.0标准认证。

3.9.18 国际 CC EAL4+认证

CC（Common Criteria for Information Technology Security Evaluation）标准是信息技术安全性评估标准，用来评估信息系统、信息产品的安全性。CC标准的评估分为两个方面：安全功能需求和安全保证需求。iBMC已获得国际CC EAL4增强认证。

3.9.19 中国 CC EAL4 认证

中国网络安全审查技术与认证中心开展的IT产品信息安全认证业务，是依据信息技术安全评估准则和相关技术要求，对IT产品的安全性进行评价，旨在保护用户信息安全，维护用户利益。生产企业的IT产品获得信息安全认证证书，表明该产品符合相应的标准和技术要求。iBMC已获得IT产品信息安全认证EAL4级证书。

3.9.20 FIPS 140-3 认证

加密模块是所有密码使用的基石，加密模块的FIPS模式（BMC版本为3.10.3及以上支持）遵守FIP 140-3标准设计，同时也满足ISO/IEC 19790标准。采用标准批准的密码算法，如对称密钥算法、非对称密钥算法、摘要算法、数字签名算法、密钥交换机制等。加密模块在如下方面满足标准的合规设计：

- 模块接口安全

- 角色、服务与身份验证机制
- 固件安全
- 操作环境隔离与保护
- 非侵入式安全
- 敏感安全参数（密钥）管理
- 自测试能力（上电自检、条件自检）
- 生命周期保障

3.9.21 邮件随机令牌双因素认证

支持基于邮件发送的随机令牌的简易双因素认证功能，支持针对每个本地用户开启简单双因素身份认证功能，支持配置电子邮件地址，支持当登录BMC的用户登录IP与上次登录不同时，用户登录要求输入通过邮件接收到的验证码才能登录。通过在用户名密码登录认证基础上，增加邮件收到的验证码叠加认证，全部通过验证后才能登录，进一步增强用户登录的合法性校验，提升安全性。

3.9.22 BIOS 固件实时完整性扫描

支持通过BMC在OS运行状态下执行BIOS固件实时完整性扫描，支持通过BMC Web开启BIOS实时扫描功能，并可以自由选择立即触发或定时触发模式，查看BMC安全日志可以获得BIOS固件实时扫描执行成功的结果。在OS不需重启的条件下可执行BIOS固件的完整性扫描，确保BIOS固件未遭篡改或破坏，保证业务稳定性和安全性。

3.9.23 网卡固件实时完整性扫描

支持通过BMC对BCM957508、BCM957608、LPE35002网卡固件开展基于SPDM协议的完整性扫描，通过BMC Redfish接口开启对应网卡的SPDM完整性扫描功能，并导入依赖的网卡签名根证书和固件度量值后，可通过BMC Redfish接口触发针对网卡固件的完整性扫描，并可查询到网卡固件的度量值。在OS不需重启的条件下可执行网卡固件的完整性扫描，确保网卡固件未遭篡改或破坏，保证业务稳定性和安全性。

3.10 管理接入

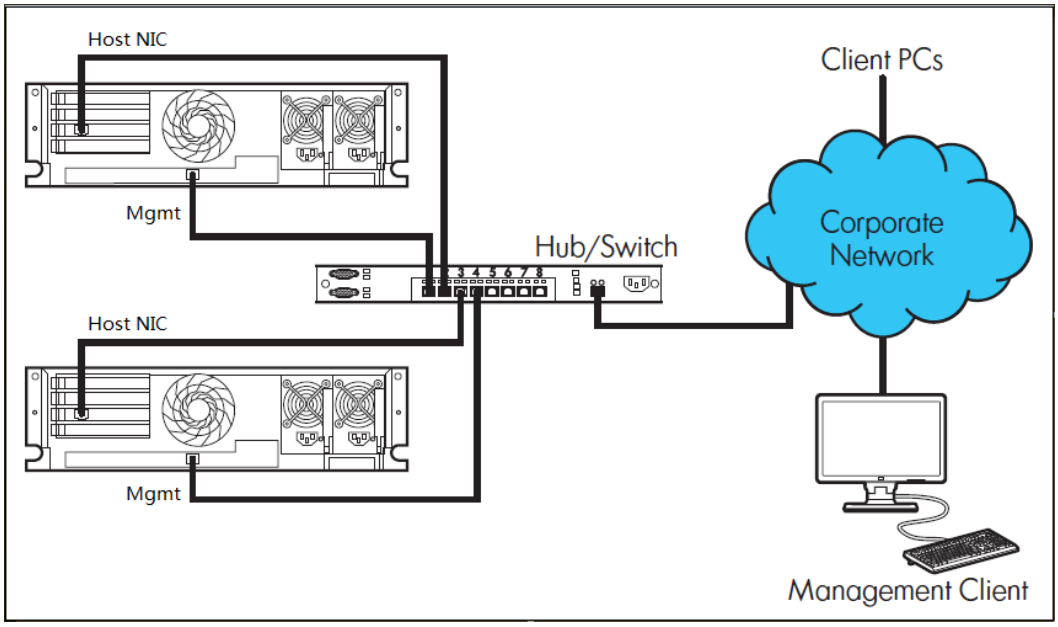
iBMC兼容支持了IPv4和IPv6两种协议版本地址，支持通过专用管理网口或共享网口(利用NCSI边带功能)接入，其中共享网口支持VLAN功能。

3.10.1 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。

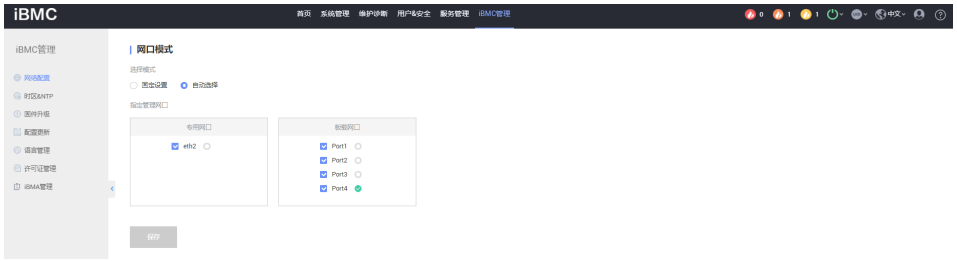
网口自适应启用后，服务器更换组网后只要专用管理网口或边带管理网口任一网口连接了网线即可访问管理界面，平滑切换，不需要再配置任何网络信息，省去繁杂的配置步骤，提升维护效率。

图 3-72 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3-73所示。

图 3-73 网口自适应配置界面



3.10.2 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 3-74 边带管理框图

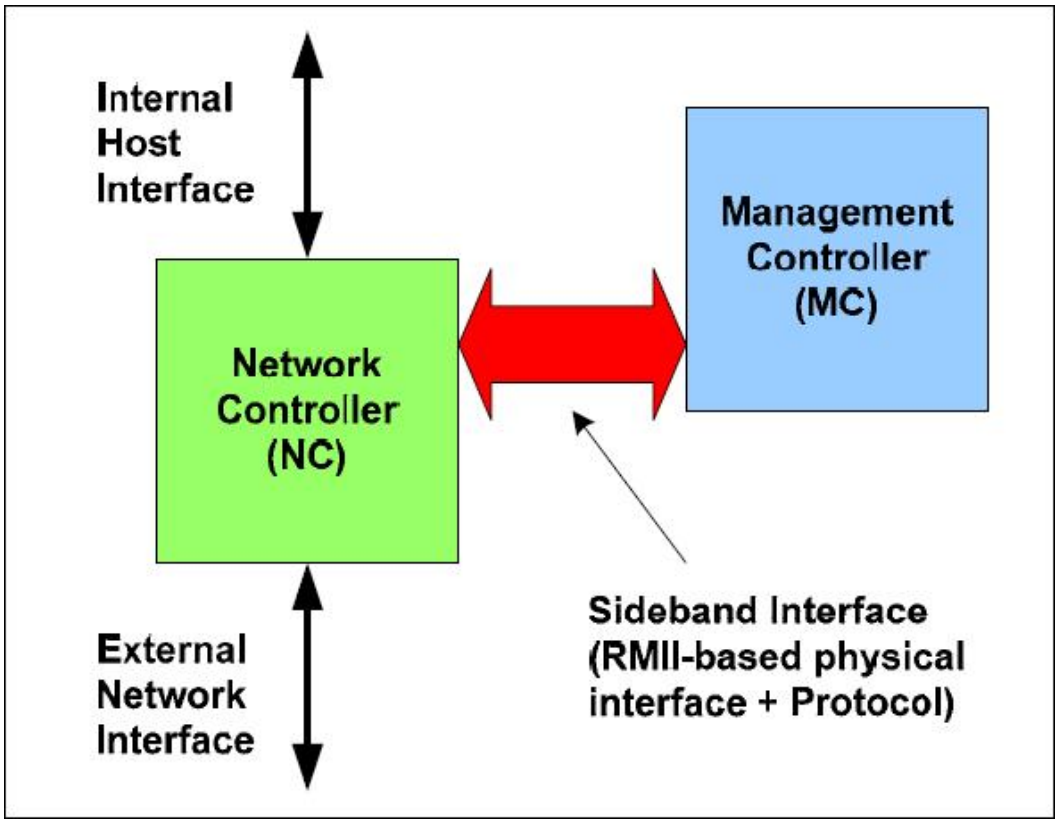
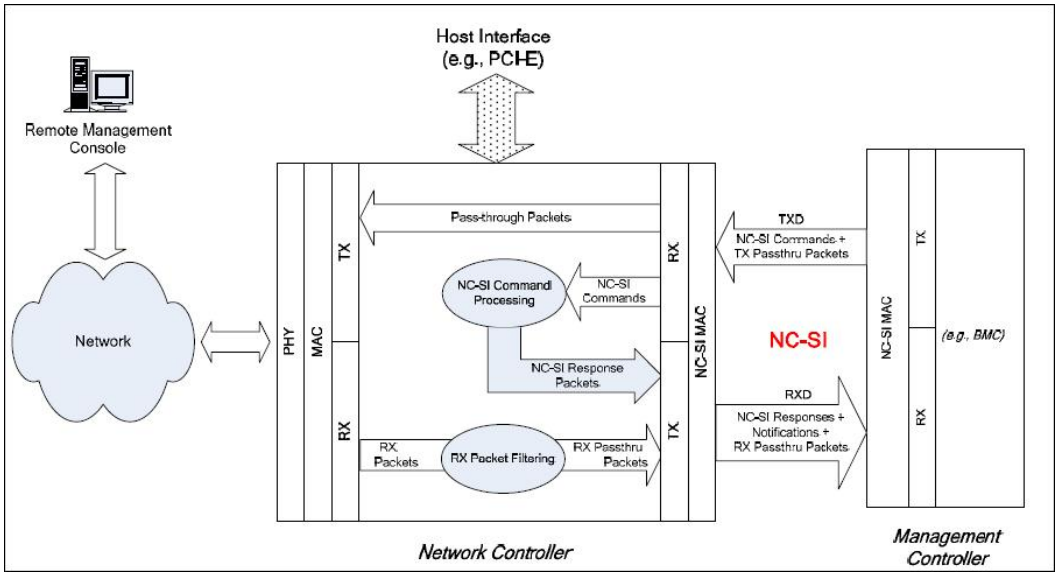


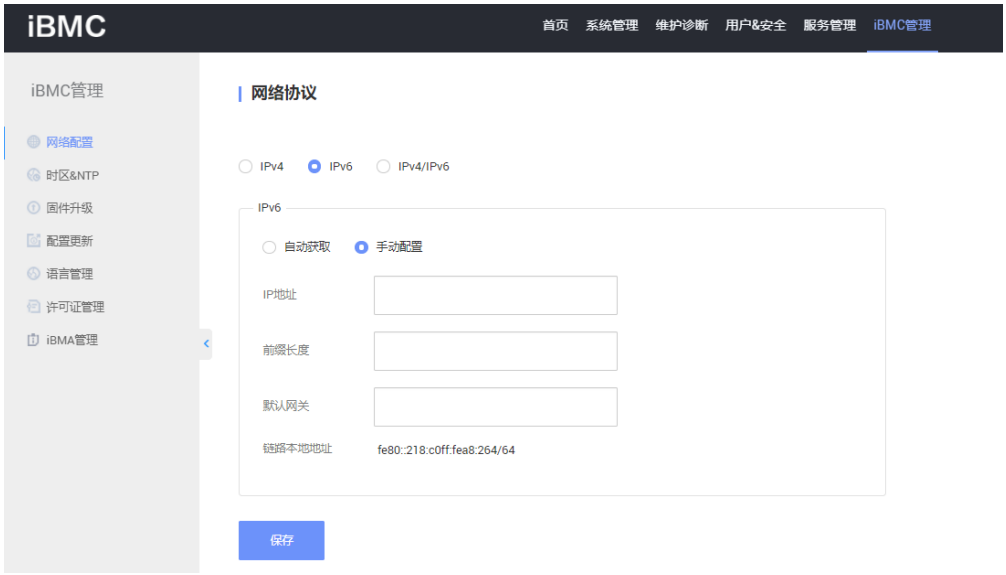
图 3-75 边带管理数据流图



3.10.3 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 3-76 IPv6 地址配置界面



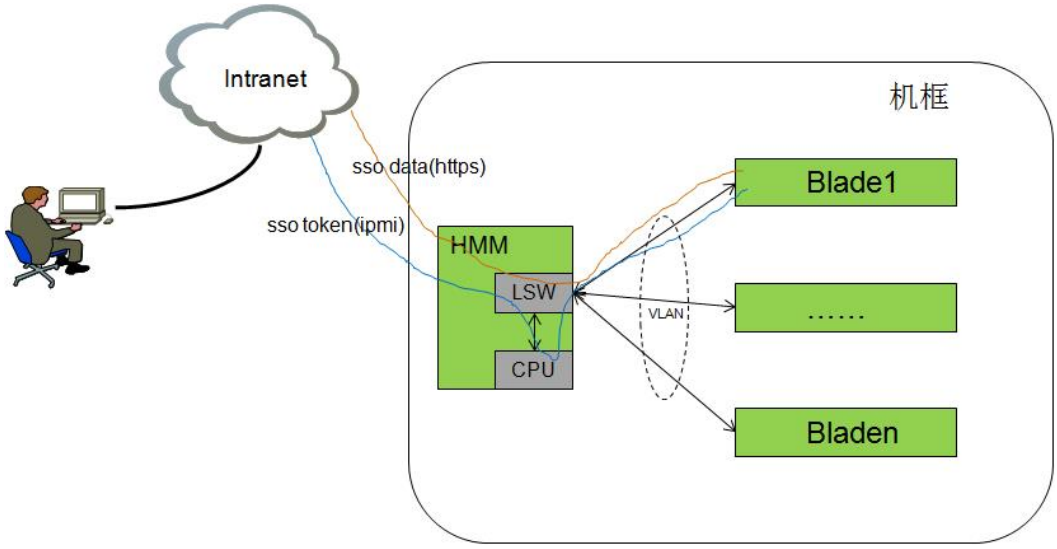
支持手动设置或DHCP获取iBMC的IPv6地址。

3.10.4 SSO

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。

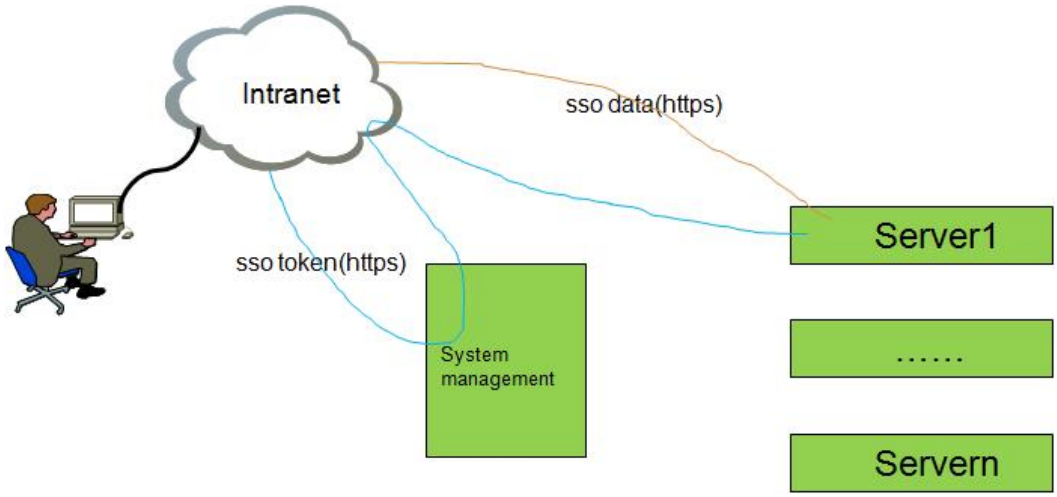
机框SSO实现原理，用户先登录HMM WEB，点击单板iBMC的SSO链接时，HMM通过内部VLAN通道发IPMI命令从iBMC获取SSO token，然后使用该token通过https协议登录iBMC WEB首页或远程控制台，跳转到iBMC上的操作权限由HMM指定，如图3-77。

图 3-77 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3-78。

图 3-78 网管 SSO 原理



3.10.5 近端运维

V6、V7系列服务器提供了通过USB管理口（Type-C）接入iBMC管理系统的能力，可以通过手机APP或笔记本对服务器信息进行查询或配置等近端维护管理动作。同时支持接入U盘执行自动导入、导出配置操作。

说明

近端运维功能依赖产品硬件包含iBMC直连管理接口，详细支持情况请参见产品的用户指南。

3.10.6 SSDP

SSDP是一个“简单服务发现协议”，即英文“Simple Service Discovery Protocol”的缩写，该协议定义了如何在网络上发现网络服务的方法。iBMC支持SSDP协议中的NOTIFY报文发送和M-SEARCH响应机制，控制点（客户端）通过SSDP报文获取到BMC的本地链路IPV6地址，通过此IP地址实现BMC的网络接入和网络配置，进一步实现纳管BMC和管理BMC的效果。

3.10.7 固件联盟 BMC 标准符合性测试认证

支持固件产业技术创新联盟T/CESA 1219-2022《服务器基板管理控制器（BMC）测试方法》标准符合性测试，并达到高级或扩展要求（level 3）。

3.11 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 3-79 用户管理界面

3.12 配置管理

3.12.1 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 3-80 WEB 接口操作界面

3.12.2 BIOS 配置

支持通过Redfish接口实现全量BIOS菜单项的远程查询和配置。

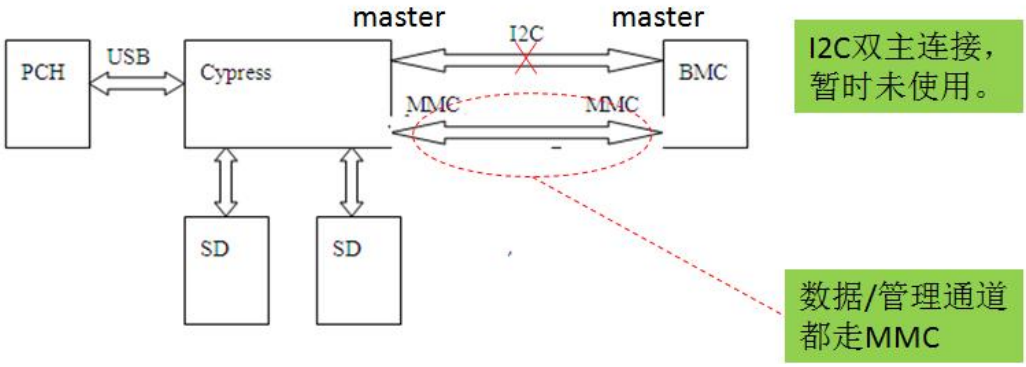
3.13 存储管理

3.13.1 内置 SD 卡

每台V3系列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 OS数据隔离

图 3-81 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

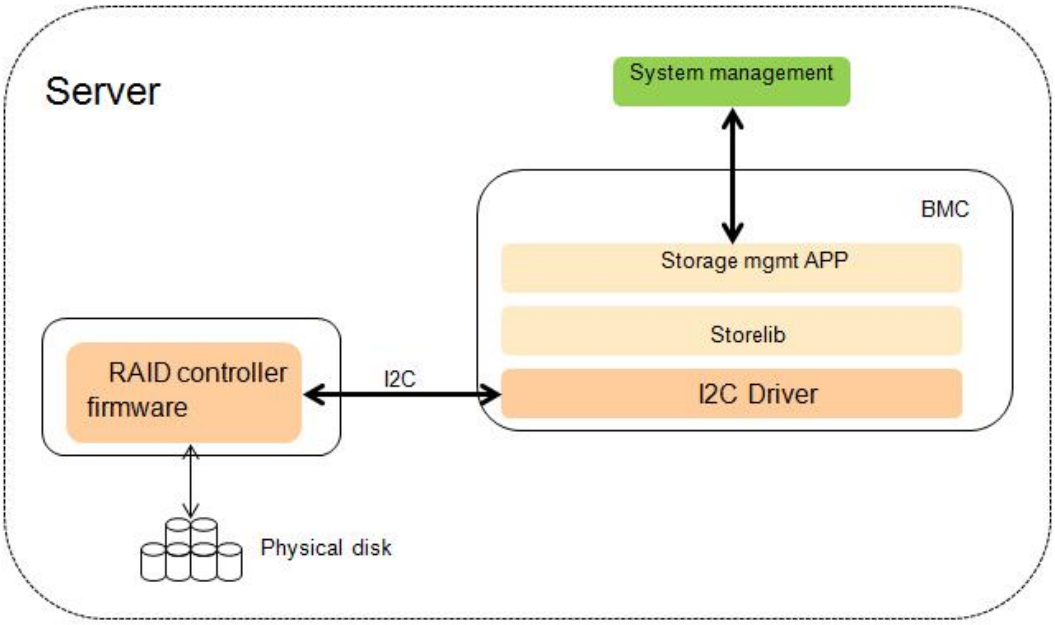
3.13.2 RAID 与硬盘管理

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 3-82 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3-12**、**表3-13**、**表3-14**：

表 3-12 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。

部件	管理属性	备注
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 of Drives 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

说明

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 3-13 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 3-14 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 3-83 RAID 控制器管理界面

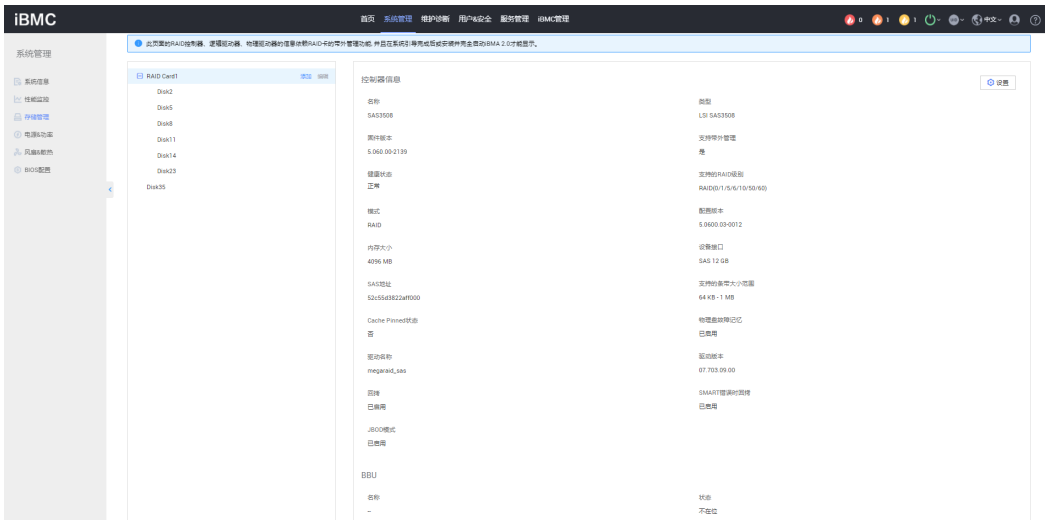


图 3-84 逻辑盘管理界面

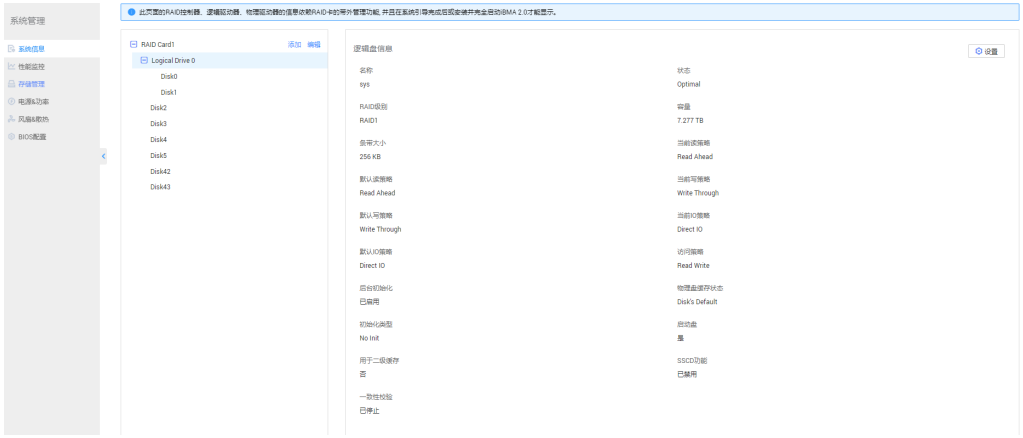


图 3-85 物理盘管理界面

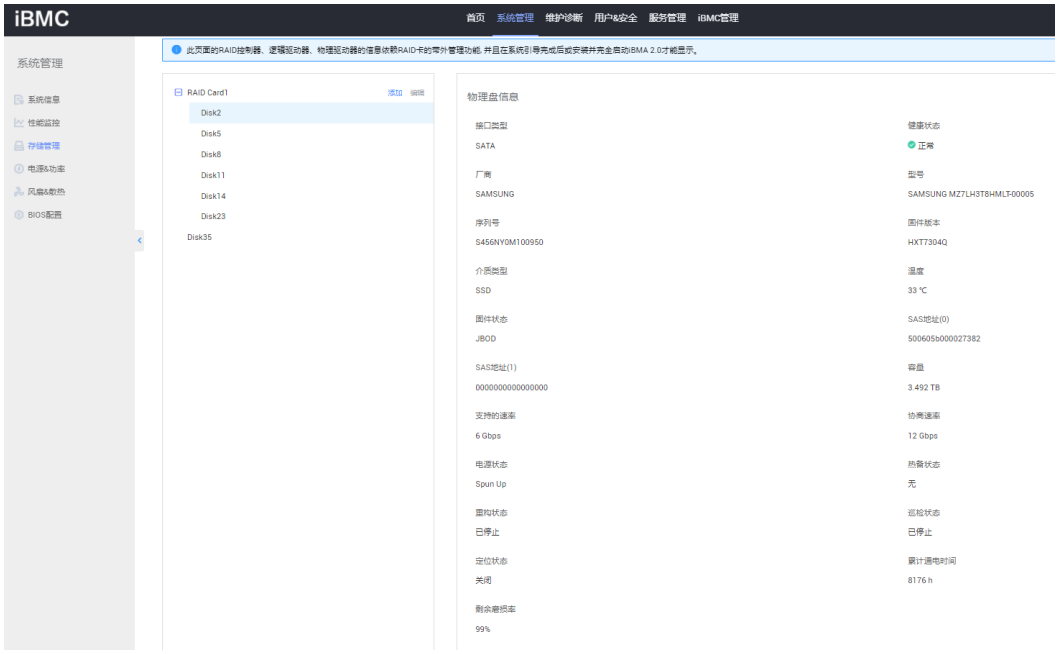


图 3-86 RAID 配置界面

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3-15**所示。

表 3-15 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 3-16 M.2/SATADOM 管理（基于 iBMA 2.0）

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。

3.14 时间管理

网络时间协议（NTP）：

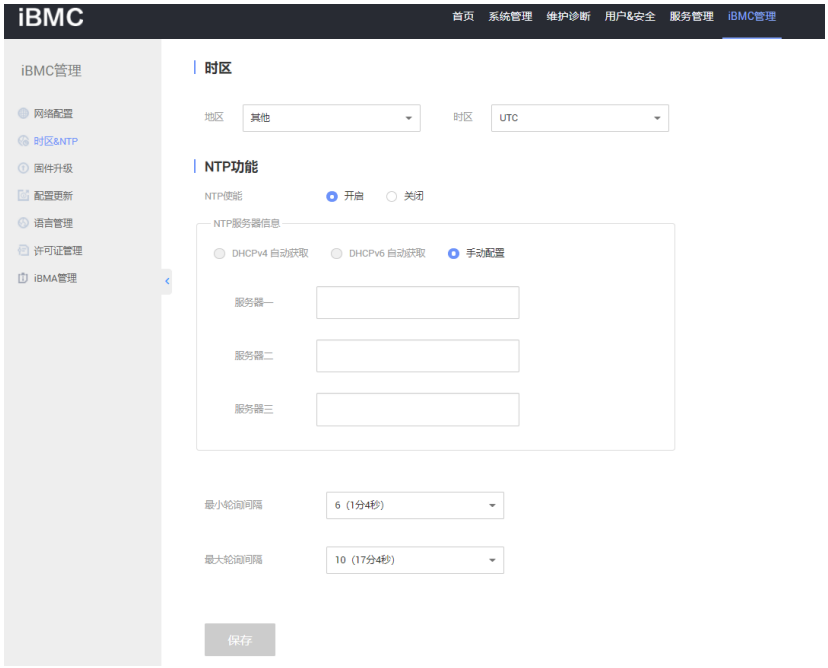
NTP(Network Time Protocol)是用来使计算机时间同步的一种协议。服务器iBMC自身没有RTC硬件，但支持从多个时间源同步时间且同一时间只能从一个时间源同步，时间源见**表3-17**。NTP功能默认关闭且支持开启，支持手动设置或自动获取首选和备用NTP服务器地址(支持IP的v4和v6版本)，手动设置时NTP服务器地址还支持FQDN域名输入；从时间获取的安全性考虑，iBMC支持对NTP服务器合法性校验。

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 3-17 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 3-87 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 3-88 夏令时配置界面

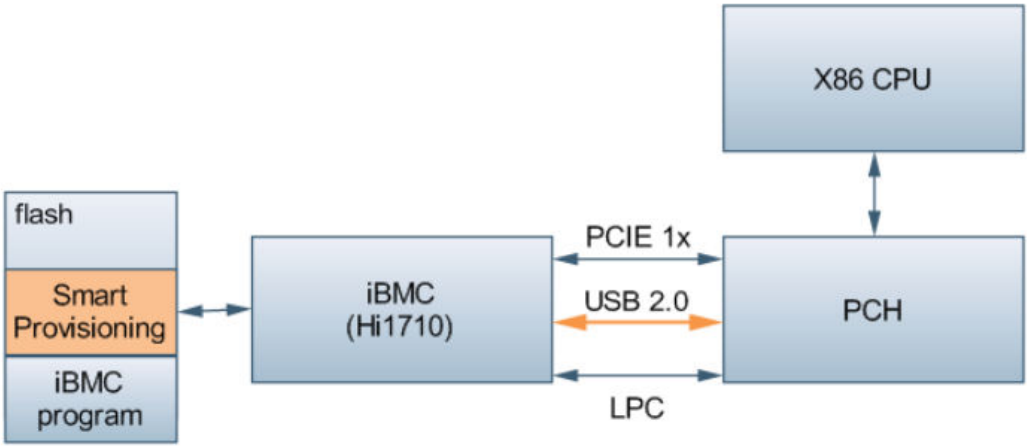
3.15 SP 管理

3.15.1 概述

智能部署工具（Smart Provisioning）是一款集成到V5及以上系列机架服务器、刀片服务器、高密服务器计算节点上的工具软件。在V3系列服务器上，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。

3.15.2 系统设计

图 3-89 Smart Provisioning 在系统中的位置-x86



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。

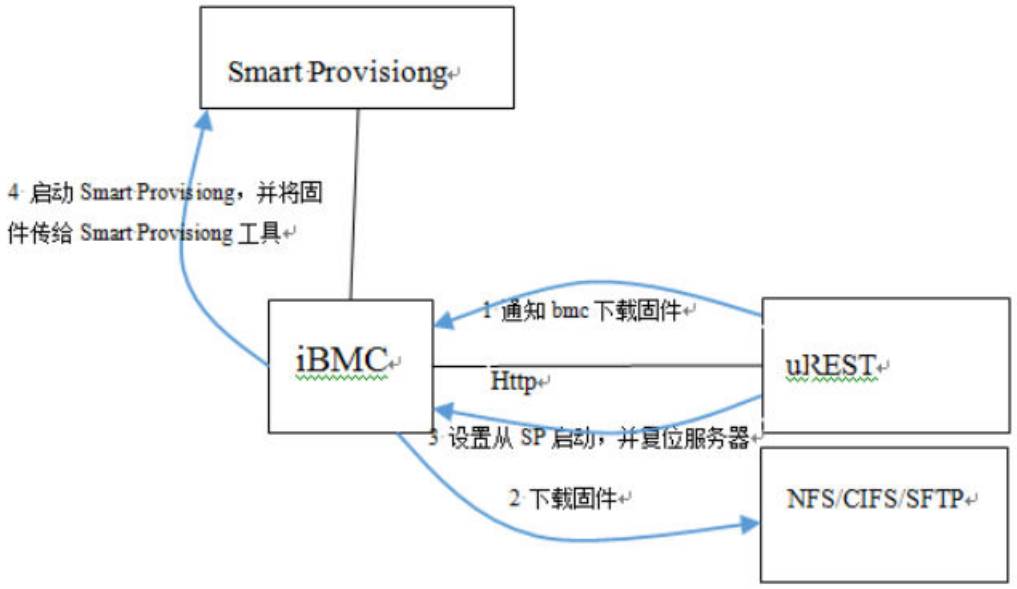
iBMC提供的redfish接口，支持的主要功能如下：

- 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
- 硬盘擦除

3.15.3 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 3-90 通过 iBMC Redfish 接口升级

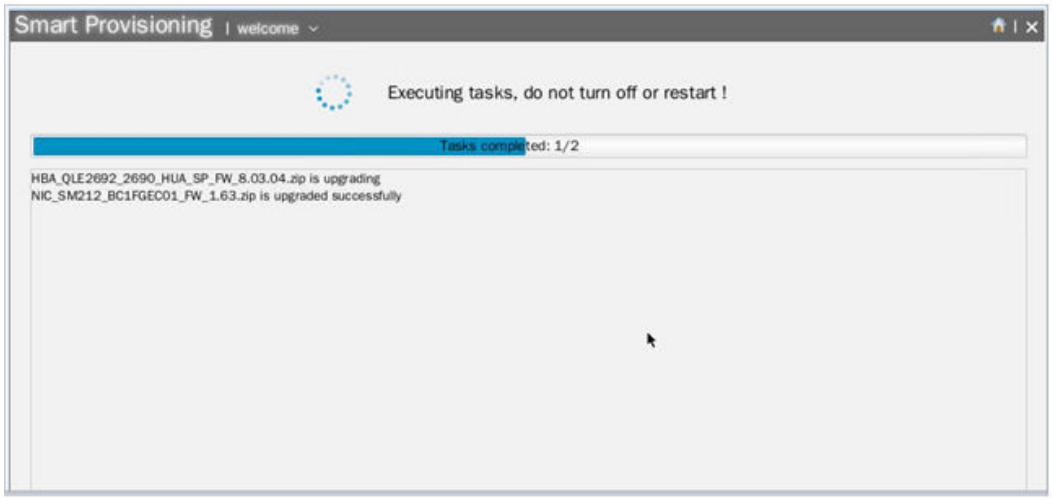


iBMC提供了Redfish接口支持升级PCIe卡和硬盘的固件，可以通过工具（比如uREST tool）下发命令给iBMC，iBMC将会从指定的文件服务器下载固件。

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。

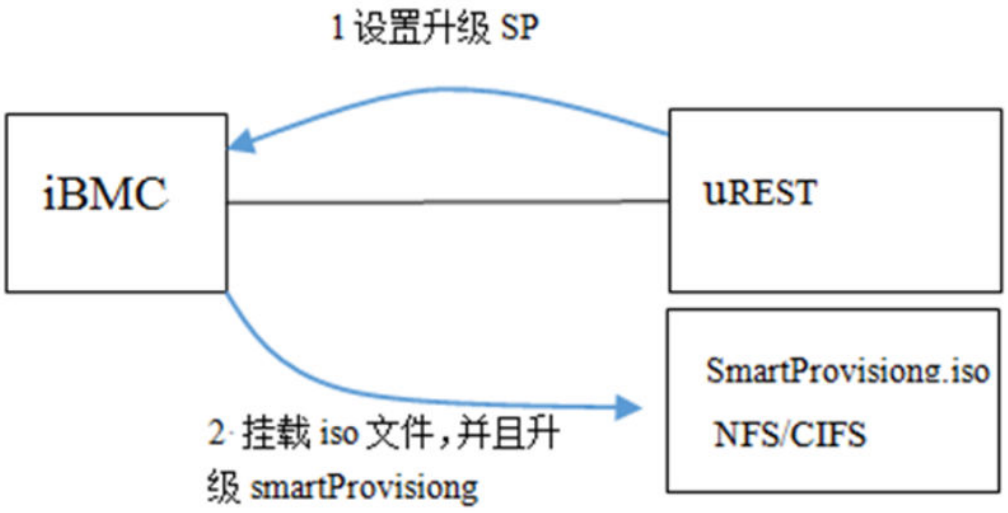
通过这种方式，可以实现对PCIe固件的上传和生效进行分离。

图 3-91 固件升级进度



3.15.4 Smart Provisiong 升级

图 3-92 通过 iBMC 升级 SmartProvisioning



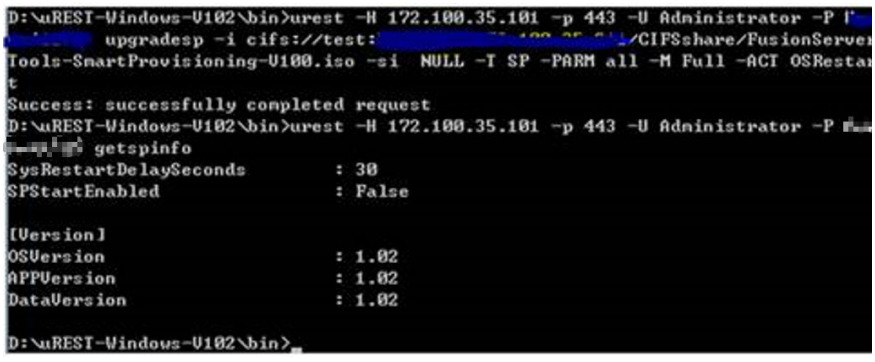
iBMC提供了Redfish接口升级或者恢复Smart Provisioning。

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《**FusionServer Tools 2.3.0 uREST 用户指南**》。

图 3-93 使用 iBMC 升级 Smart Provisioning



3.15.5 PCIe 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 3-18 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
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

3.15.6 硬盘擦除

支持硬盘的快速擦除和安全擦除；安全模式下提供支持简单（全盘擦除1次），正常（全盘擦除3次）和深度擦除（全盘擦除9次）三种模式。

3.16 iBMA 管理

3.16.1 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

3.16.2 支持能力

表 3-19 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。

部件	不安装iBMA	安装iBMA
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。

3.16.3 板载 iBMA

iBMA支持板载功能，通过iBMC界面可以将iBMA软件以U盘的形式插入到操作系统，在系统挂载USB硬盘后，即可安装iBMA软件。

当前V5及以上系列服务器支持板载iBMA，提供CentOS、Red Hat、Ubuntu等主流Linux系统安装iBMA的功能。

图 3-94 iBMA 管理界面

图 3-95 iBMA 操作说明界面

3.16.4 升级接口

iBMA 2.0通过RESTful接口提供系统软件的升级服务，同时支持升级过程中的进度查询及升级结果查询。升级总体流程如下：

- 网管获取到升级包后，通过升级服务接口下发以下参数到iBMA 2.0。

数据类型	数据项定义	数据项描述
字符串	Name	软件名称，使用半角逗号隔开，仅异步升级接口支持
字符串	ImageURI	升级包URL地址
字符串	SignalURL	升级包数字签名地址
字符串	CrlURI	升级包公钥文件地址
字符串	ImageType	升级包类型：Driver、iBMA、Software、Firmware_Shell
字符串	TransferProtocol	使用的传输协议，SFTP
字符串	User	URL访问用户名
字符串	Password	URL访问密码
字符串	Parameter	驱动升级：all表示整包升级，也可指定升级包，如“package1.rpm, package2.rpm”指定升级package1和package2； iBMA升级：NA Firmware_Shell升级：all 表示8张卡全部升级。也可指定槽位升级, 如"1, 2"指定升级1槽和2槽的FPGA卡。 软件升级：软件包升级脚本依赖的参数
字符串	ActiveMethod	包括重启OS(OSRestart)，重启服务器(ServerRestart)，升级包自己做生效动作（Immediately或null），FPGA热生效（WarmReboot），FPGA冷生效（ColdReboot）
字符串	DownloadViaiBMC	是否通过iBMC下载，仅异步升级接口支持
字符串	AllowStop	是否允许停止，仅异步升级接口支持

- iBMA 2.0解析升级服务操作命令相关参数，获取到升级包，解压并校验合法性后，调用升级包中的升级脚本进行升级操作。
- 升级过程中，通过升级脚本获取升级进度及结果供网管查询。
- 升级完成后，按照升级启动命令中指定的生效方式完成升级操作。

iBMA升级接口如下表所示：

URI	Method	功能描述	支持的操作系统
/redfish/v1/Sms/1/UpdateService/Actions/UpdateService. SimpleUpdate	POST	下发升级参数，执行升级操作（不推荐使用）	Linux、Windows、VMware
/redfish/v1/Sms/1/UpdateService/Progress	GET	查询升级进度和结果（不推荐使用）	Linux、Windows、VMware
/redfish/v1/Sms/1/UpdateService/Actions/UpdateService.AsynchronousUpdate	POST	异步下发升级参数，执行升级操作	Linux、Windows、VMware
/redfish/v1/Sms/1/UpdateService/Actions/UpdateService.EffectiveUpdate	POST	异步生效接口	Linux、Windows、VMware
/redfish/v1/Sms/1/TaskService/Tasks/*taskid*	GET	查询指定taskid的升级或生效任务进度	Linux、Windows、VMware

iBMA当前版本支持的升级对象如下表所示：

升级对象	是否支持		
	Linux	Windows	VMware
iBMA	Y	Y	Y
网卡驱动	Y	Y	Y
RAID卡驱动	Y	Y	Y
FC驱动	Y	Y	Y
FCoE驱动	Y	Y	Y
iSCSI驱动	Y	Y	Y
FPGA 固件	Y	N	N
NVMe驱动	Y	Y	Y
IB驱动	Y	N	N
软件	Y	Y	Y

3.17 Kerberos 认证

Kerberos V5身份验证协议提供客户端和服务器端之间进行身份验证机制，BMC支持基于Kerberos的用户名密码认证和单点登录认证两种认证方式。

使用Kerberos登录iBMC系统可以提高系统安全性。Kerberos用户可登录iBMC WebUI。

Kerberos单点登录，基于Kerberos身份认证协议，指用户只需要输入一次密码就可以访问网络中的所有服务器。iBMC集成Kerberos协议，用户只需要输入一次密码登录PC（或工作站），就可以免密码登录网络内的所有iBMC。

基于Kerberos协议的单点登录，在认证过程中，秘钥不会在网络中传输，每次会话产生一个秘钥，会话结束秘钥失效，因此具有更高的安全性。Kerberos在认证过程中产生票证服务票证（TGT），用户登录某个服务时自动将服务ID和TGT一起发送到认证中心，并得到一个秘钥，通过该秘钥加密用户账户信息，登录服务器，而不必用户输入密码，因此操作更方便，由于在多个服务器之间频繁切换登录时，效果更明显。

成千上万台服务器部署在不同区域，管理员如何操作这些服务器，成为客户的困扰，基于Kerberos认证的单点登录，即可解决这一问题。下面章节简单介绍怎么部署iBMC，以支持基于Kerberos的单点登录。

3.17.1 iBMC 单点登录方案概述

BMC支持基于Kerberos认证的单点登录功能，基本配置步骤如下：

步骤1 需要一个安装Windows Server 操作系统的服务器或PC机，作为AD域控制器，并创建一个域。

- 在该域内，创建一个用户和组，将用户加入组，并获取组的SID，该SID需要配置到iBMC；
- 使用ktpass命令，生成一个keytab文件，该问题需要配置到iBMC。

步骤2 需要一个PC机，或工作站，要求工作站加入该域。

- 需要配置浏览器，以支持Kerberos认证协议；
- 将服务器的主机名配置到站点。

步骤3 一台或多台服务器，配置服务器上iBMC，将服务器加入该域，并且配置iBMC Kerberos属性。

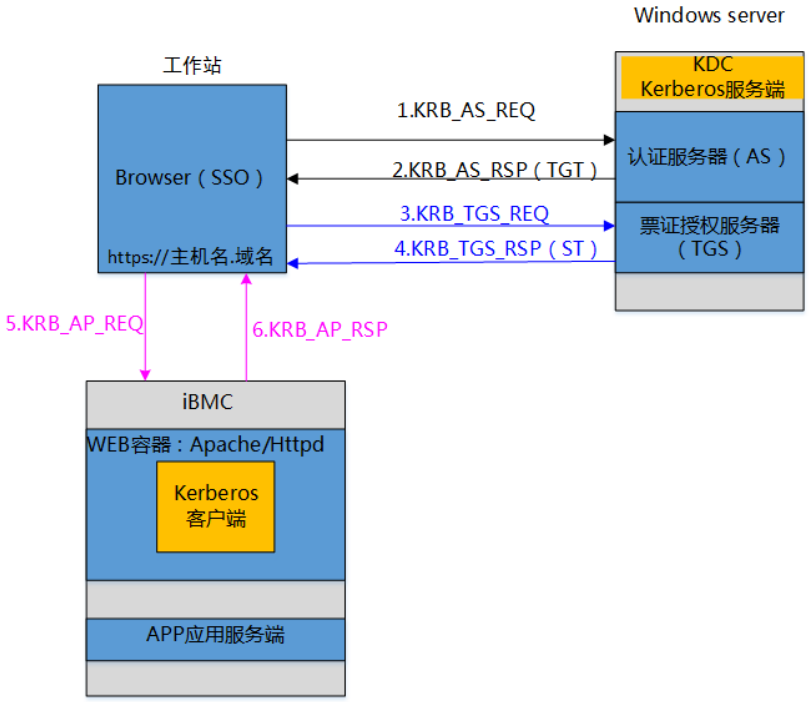
- 将SID配置到Kerberos参数页面；
- 将keytab文件配置到Kerberos参数页面

步骤4 详细的配置可以参考**3.17.3 系统兼容**章节。

----结束

上述配置完成之后，就可以在工作站上，通过浏览器登录iBMC，而不需要输入密码，框图如下：

图 3-96 基于 Kerberos 认证方式的 SSO 登录



基本的交互分为6个步骤，具体如下：

1. 用户通过已在Windows Server中创建的域用户，登录到工作站。在登录过程中，工作站（即Client）向Windows Server（即KDC）发送KRB_AS_REQ请求，以获取票证服务票证（TGT），发送报文时附带Client主体名称和预认证信息。
2. 用户认证通过后，KDC向Client发送KRB_AS_RSP响应消息，返回TGT和Client与KDC之间通信用的SessionKey1。
3. 打开Client中浏览器，输入**https://ibmc**主机名.域名，以访问iBMC。iBMC上的Kerberos 客户端检测为Kerberos登录，向浏览器返回一个特殊的https消息头，浏览器收到消息后，向KDC发送KRB_TGS_REQ请求消息，请求访问服务票证。请求消息附带TGT和认证器。
4. KDC校验TGT和认证器有效，向浏览器发送KRB_TGS_RSP响应消息，并返回服务票证。
5. 浏览器向iBMC发送KRB_AP_REQ消息，带上服务票证，iBMC认证通过之后，允许浏览器登录iBMC，sso登录成功。
6. iBMC向浏览器发送KRB_AP_RSP响应消息，登录成功。

3.17.2 环境配置

涉及到三个方面：

1. Windows Server的配置
   - 安装“Active Directory Domain Server”，并配置完成。在配置AD时，将此Windows Server提升为域控制器，添加新林，配置域名（注意大小写），完成配置重启系统。
   - 点击Tools ->Active Directory User and Computers，打开目录用户和计算机，在域下面创建用户和组，并将该用户加入组，记录用户组的SID。

- 安装“Active Directory Certificate Services”服务。选择“Certification Authority Web Enrollment” ，配置好CS服务，完成配置重启系统。
- 使用ktpass命令生成keytab文件。

2. 工作站上浏览器的配置

- Tool->Internet options ->Security->Local intranet ->Sites->Advanced，将**https://iBMC主机名.域名加入Websites**中。
- Tools->Internet options ->Security ->Trusted sites ->Sites，将**https://iBMC_IP加入Websites**中。

3. iBMC的配置

- 配置iBMC主机名，并加入上面的AD域中；
- 创建Kerberos用户组。用户组中的SID为上面第一点中创建的组SID；
- 使能Kerberos特性，配置kerberos参数；
- 上传keytab文件，并保存。

上面三个步骤完成SSO登录涉及的主要配置。

3.17.3 系统兼容

- AD域控支持的操作系统：Windows Server 2012 R2 64bit和Windows Server 2016 R2 64bit
- 工作站支持的操作系统及浏览器

操作系统	浏览器
Windows 7 32位 Windows 7 64位	Internet Explorer 11
	Google Chrome 55+
Windows 8 32位 Windows 8 64位	Internet Explorer 11
	Google Chrome 55+

3.18 液冷监控管理

针对液冷机型，iBMC支持分级的液冷监控管理：服务器液冷监控、机柜液冷监控。

3.18.1 服务器液冷监控

服务器液冷监控主要负责服务器内部的液冷监控管理。

- 支持液冷管路漏液告警
- 支持配置漏液关机策略
- 支持漏液检测部件在位监控（水浸绳、漏液检测卡等）

3.18.2 机柜液冷监控

在配置管理板的整机柜场景下支持机柜液冷监控，机柜液冷监控主要负责机柜的液冷监控管理。

- 支持机柜液冷管路漏液告警
- 支持二次管路漏液告警

3.19 RADIUS 身份认证

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证）协议是一种分布式的、客户端/服务端架构的信息交互协议，能保护网络不受未授权访问的干扰。BMC支持配置RADIUS服务器信息，用户认证信息通过RADIUS协议与服务端建立身份认证之后登录BMC。

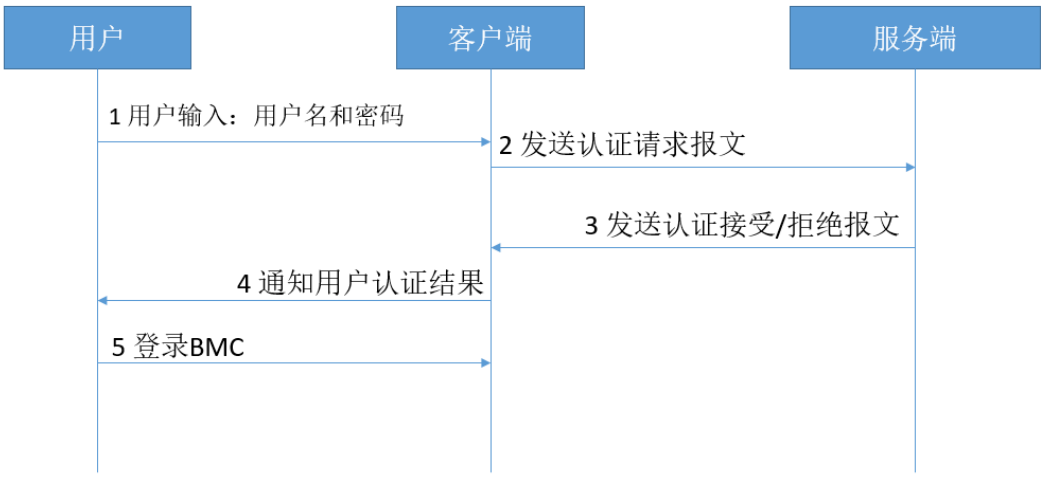
说明

iBMC 3.07.03.27及以后版本支持。

3.19.1 认证方案概述

服务器BMC作为RADIUS客户端，负责收集用户信息（例如：用户名、密码、密钥等），并将这些信息发送到RADIUS服务器。RADIUS服务器则根据这些信息完成用户身份认证以及认证通过后的用户授权。用户、RADIUS客户端和RADIUS服务器之间的交互流程如下所示：

图 3-97 基于 RADIUS 认证方式登录



3.19.2 环境配置

客户端：

通过BMC WEB或Redfish接口配置RADIUS服务端地址、端口、密钥，选择用户角色，并开启RADIUS使能，即可使用RADIUS用户登录。

服务端：

在RADIUS服务端配置用户、用户密码和密钥，并开启RADIUS服务。

