iBMC
用户指南

文档版本 v1.0
发布日期 2023-06-01

深圳市兰盾技术有限公司

注意

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。

前言

概述

本文档为服务器底层管理软件iBMC（Intelligent Baseboard Management Controller)进行全面的介绍和说明，包含以下信息：

- 各个模块提供的详细功能。
- 各个模块之间的关系。
- WebUI界面的详细介绍。

说明

本文档主要介绍客户在使用玄昊服务器进行网络部署及维护时，需要使用的命令。用于生产、装备、返厂检测维修的命令，不在本资料中说明。

读者对象

本文档主要适用于以下人员：

- 企业管理员
- 企业终端用户

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
v1.0	2023-06-01	第一次正式发布

目录

1 iBMC 管理软件概述

1.1 系统简介

iBMC智能管理系统(以下简称iBMC)提供了丰富的管理功能。

- 丰富的管理接口
  提供以下标准接口，满足多种方式的系统集成需求。
  - DCMI 1.5接口
  - IPMI 1.5/IPMI 2.0接口
  - 命令行接口
  - Redish接口
  - Web管理接口(HTTPS， Hypertext Transfer Protocol Secure)
  - 简单网络管理协议(SNMP， Simple Network Management Protocol)
- 故障监控与诊断
  可提前发现并解决问题，保障设备7*24小时高可靠运行。
  - 系统崩溃时临终截屏与录像功能，使得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。
  - FDM（Fault Diagnose Management)功能，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Syslog报文、 Trap报文、电子邮件上报告警，方便上层网管收集服务器故障信息。
  - 支持LCD直接从iBMC获取设备信息。
- 安全管理手段
  - 通过软件镜像备份，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。
  - 多样化的用户安全控制接口，保证用户登录安全性。
  - 支持多种证书的导入替换，保证数据传输的安全性。
- 系统维护接口
  - 支持虚拟KVM（Keyboard, Video, and Mouse)和虚拟媒体功能，提供方便的远程维护手段。

- 支持RAID的带外监控和配置，提升了RAID配置效率和管理能力。
- 通过Smart Provisioning实现了免光盘安装操作系统、配置RAID以及升级等功能，为用户提供更便捷的操作接口。

- 多样化的网络协议
  - 支持NTP ，提升设备时间配置能力，用于同步网络时间。
  - 支持域管理和目录服务，简化服务器管理网络。
- 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费用。
- 许可证管理

  通过管理许可证，可实现以授权方式使用iBMC高级版的特性。

  iBMC高级版较标准版提供更多的高级特性，例如：
  - 通过Redish实现OS部署。
  - 通过Redish收集智能诊断的原始数据。

1.2 安全特性

- NC-SI

  服务器管理平面与业务平面分离。 iBMC可以通过NC-SI边带网口功能与业务平面共享同一个网卡。在物理层，管理平面与业务平面共用接口，在软件层，通过VLAN实现二者隔离，互不可见。
- 协议与端口防攻击

  iBMC按照最小化原则对外开放网络服务端口：即不使用的网络服务必须关闭，调试使用的网络服务端口在正式使用的时候必须关闭，不安全协议的端口默认处于关闭状态。
- 基于场景的登录限制

  基于安全考虑，从时间、地点(IP/MAC)、用户三个维度将服务器管理接口访问控制在最小范围；目前该特性只针对Web接口进行登录限制。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。
- 用户帐号安全管理

  iBMC通过密码复杂度、弱口令字典、密码有效期、密码最短使用期、不活动期限、紧急登录用户、禁用历史密码重复次数、登录失败锁定等功能保证帐号安全。
- 证书管理

  iBMC支持SSL证书加密及证书替换功能。证书替换功能可以通过Web界面进行操作。

  为提高安全性，建议替换成自己的证书和公私钥对，并及时更新证书，确保证书的有效性。

  iBMC还支持LDAP证书的导入功能，为数据传输提供鉴权加密功能，提高系统安全性。
- 操作日志管理

  记录了iBMC所有接口的非查询操作。操作日志分两类，一类是Linux系统进程的日志，另一类是用户进程日志。用户进程记录的日志包括时间、操作接口、操作源IP、操作源用户、执行动作。

- 数据传输加密
  iBMC支持电子邮件传输时启用TLS加密功能和SMTP登录认证功能，保证数据传输的安全性。
  在使用远程控制台时， iBMC支持开启KVM加密、 VNC加密功能，实现数据的安全传输。

1.3 常用接口操作

iBMC支持多种操作接口，其中IPMI接口主要用于内部通信、 SNMP接口主要用于与上层网管的信息交互。单机常用到的操作接口主要包括下述接口。

1.3.1 iBMC WebUI

WebUI为服务器提供直观便捷的配置查询接口，并将相关任务划分到相同或邻近的页面中。 Web的顶层分支包括首页、系统管理、维护诊断、用户&安全、服务管理、iBMC管理等几个大的节点，而页面左侧的导航树，将每个大节点做了细化拆分。

在使用WebUI时，您可以随时单击页面右上角的  获取对应页面的帮助信息，协助您可以理解对应参数，并对相关操作做出指导。

iBMC WebUI当前支持中文、英文、日文、法文界面，您可以通过右上角的语言切换按钮切换到所需语言环境。

关于iBMC WebUI的更多说明，请参考本文档**3 iBMC WebUI介绍**。

2 用户必读

2.1 iBMC 使用准则

- 使用专用网络对iBMC进行配置。
- iBMC不接入因特网。
- 关闭不使用和不安全的协议、端口。
- 及时修改默认用户名和密码，并妥善保管。
- 定期审计操作日志。

2.2 获取 iBMC 版本信息

iBMC的版本信息的获取方式包括：

- 通过iBMC版本说明书查询。
  进入指定服务器当前版本软件下载页面，可查看到iBMC版本说明，包含iBMC版本信息，例如：

- 通过WebUI查询。
  登录iBMC，在“首页”界面中可查看到“iBMC固件版本”，例如：

2.3 默认参数

iBMC提供部分特性的默认参数如**表2-1**，方便用户首次操作。为保证系统的安全性，建议您在首次操作时修改初始参数值，并定期更新。

表 2-1 默认参数

参数	默认值
iBMC默认用户名和密码	用户名：Administrator 默认密码：Admin@9000
iBMC管理网口默认IP地址	192.168.2.100

2.4 登录须知

iBMC 管理网口地址

- 首次登录时，请使用iBMC默认IP地址。
- 首次登录后，请按照实际需求修改iBMC地址并进行妥善记录，方便后续产品配置及网络规划。
  修改iBMC地址的方法包括：
  - 直连用户可在iBMC WebUI修改。修改方法请参考本文档**3.8.1 网络配置**。
  - 直连用户可在BIOS Setup中修改。修改方法请参考对应产品的BIOS参数参考手册。
- 若iBMC配置了DHCP，则iBMC地址为动态分配。使用前需要首先确认当前地址。
  可通过下述方式获取：
  - 在DHCP服务器上通过iBMC的MAC查询对应的IP地址。
  - 在上层网管查询下辖服务器的iBMC地址。

登录用户类型

iBMC登录用户包括以下类型：

- iBMC最多支持16个本地用户。本地用户登录方式适合小型环境，例如实验室、中小型企业等。
- LDAP用户登录方式，由于其数量和权限均在LDAP服务器侧设置，使得登录iBMC的用户个数不受常规限制。此方法适用于具有大量用户的环境。
- Kerberos用户登录方式，支持单点登录，登录iBMC的用户个数同样不受常规限制，且更具安全性。

客户端环境

登录iBMC WebUI的客户端，必须满足一定条件才能正确显示。特别是远程控制台，对Internet Explorer及Java的配套关系有特殊要求，如表2-2所示。

为了确保您能浏览到完整的iBMC WebUI页面，建议使用以下屏幕分辨率：

- 1280 × 800
- 1366 × 768
- 1440 × 900
- 1600 × 900
- 1600 × 1200
- 1680 × 1050
- 1920 × 1080
- 1920 × 1200

说明

当在“用户&安全 > 安全配置”界面将TLS版本配置为“仅限TLS 1.3协议”时， iBMC运行环境不支持以下浏览器版本：

- Internet Explorer所有版本
- Safari 9.0 ~ 12.0
- Microsoft Edge 12 ~ 18
- Mozilla Firefox 45.0 ~ 62.0
- Google Chrome 55.0 ~ 69.0

表 2-2 运行环境

操作系统	浏览器	Java运行环境
Windows 7 32位 Windows 7 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows 8 32位 Windows 8 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE

操作系统	浏览器	Java运行环境
	Mozilla Firefox 45.0 ~ 79.0	AdoptOpenJDK 11.0.6 JRE
	Google Chrome 55.0 ~ 84.0	
Windows 10 64位	Internet Explorer 11.0 Microsoft Edge	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2008 R2 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2012 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2012 R2 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2016 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
CentOS 7	Mozilla Firefox 45.0 ~ 79.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
MAC OS X v10.7	Safari 9.0 ~ 13.1	AdoptOpenJDK 8u222 JRE

操作系统	浏览器	Java运行环境
	Mozilla Firefox 45.0 ~ 79.0	AdoptOpenJDK 11.0.6 JRE

3 iBMC WebUI 介绍

3.1 欢迎使用 iBMC 智能管理系统联机帮助

iBMC智能管理系统(以下简称iBMC系统)是一款针对服务器的系统监测和管理软件。iBMC系统的主要特点如下:

- 为您提供优异的用户体验。
  iBMC系统提供可视化易操作的图形界面，便于您对服务器进行交互式操作。
- 为您提供高效的管理维护。
  iBMC系统提供远程管理和硬件监测功能，便于您随时接入、监测并管理服务器的运行状态。
- 为您提供高安全性的系统接入。
  iBMC系统提供丰富的管理接口，并对所有接口采用高度安全的加密算法。

本文档为您提供在iBMC系统中进行服务器告警监测、故障定位、系统管理和数据配置的方法以及参数说明。对于数据单位是TB 、GB 、MB 、KB或B的数值，统一采用1024进制进行单位换算。

3.2 新手入门

3.2.1 基础操作

iBMC WebUI可执行的基本操作如**表3-1**所示。

表 3-1 基本操作

操作	说明
切换界面语言	在登录界面或其他界面中，从下拉列表中切换语言。
查看系统信息	选择“首页 > 更多详情 > 系统信息”。 “系统信息”界面显示服务器的基本信息，包括产品信息、处理器、内存、网络适配器、传感器和其他部件的信息。

操作	说明
查看联机帮助	在iBMC WebUI页面中，单击  。
查看用户信息	在登录iBMC界面后，鼠标移至界面右上角  后的用户名，例如“test”。 弹出当前用户信息窗口，显示用户所属的用户名、角色、 IP和时间。
退出系统	鼠标移动至界面顶部的用户名，单击下拉菜单的“退出登录”。
对操作系统上下电	单击  ，可以对操作系统进行上下电操作。 绿色表示操作系统已经上电，黄色表示操作系统已经下电。
设置服务器面板的UID灯状态	与服务器自身UID灯状态一致，通过本界面即可查看服务器的UID灯，不需要去机房查看。 鼠标移至iBMC界面右上角的  可以从列表中选“点亮”、“关闭”或“闪烁”。 “闪烁”时长为255秒。
查看服务器当前告警个数和级别	单击告警个数或告警级别，可以跳转到“维护诊断 > 告警&事件 > 当前告警”页面。 ●  ：表示紧急告警，可能会使设备下电、系统中断。因此需要您马上采取相应的措施进行处理。 ●  ：表示严重告警，会对系统产生较大的影响，有可能中断系统的正常运行，导致业务中断。 ●  ：表示轻微告警，不会对系统产生大的影响，但需要您尽快采取相应的措施，防止故障升级。

3.2.2 用户登录

功能介绍

通过使用“用户登录”界面的功能，您可以登录iBMC WebUI。

- 通过WebUI进行界面操作，最多支持4个用户同时登录。
- 默认情况下，系统超时时间为5分钟，即在5分钟内，如果您未在WebUI执行任何操作，系统将自动登出，此时需输入用户名和密码重新登录WebUI。
- 连续输入错误密码的次数达到设定的失败次数后，系统将对此用户进行锁定。锁定时间达到用户设置的锁定时长后，该用户方可正常登录。
- 为保证系统的安全性，初次登录时，请及时修改初始密码，并定期更新。
- 由于网络波动导致资源获取失败，可能会导致iBMC WebUI显示异常，请刷新浏览器后，重新登录iBMC WebUI。

说明

如果使用Internet Explorer登录iBMC WebUI，需要先开启兼容视图和勾选“使用TLS 1.2”，操作步骤如下：

- 开启兼容视图：
  1. 单击浏览器右上角的。
  2. 在弹出的快捷菜单中，单击“兼容性视图设置”。
  3. 在弹出的“兼容性视图设置”窗口中的“添加此网站”中输入iBMC的IP地址，并单击“添加”。
  4. 去掉“使用Microsoft兼容性列表”的勾选。
     开启兼容视图可以解决使用Internet Explorer登录iBMC WebUI后显示不正常的问题。
- 勾选“使用TLS 1.2”：
  1. 选择“Internet选项 > 高级”。
  2. 确保“安全”区域中已勾选“使用TLS 1.2”。

参数说明

表 3-2 用户登录

参数	描述
用户名	登录iBMC系统的用户。 ● “域名”选择“这台iBMC”时，支持输入的用户名的最大长度为20个字符。 登录时请注意以下事项： ● 使用本地用户登录iBMC时，“域名”可选择“这台iBMC”或“自动匹配”。
密码	登录用户的密码，为了保证安全，用户应定期修改自己的登录密码。 **说明** 以LDAP方式或Kerberos方式登录iBMC WebUI时，密码最大长度为255个字符。

操作步骤

本指南以Internet Explorer 11为例介绍登录iBMC WebUI的操作步骤。

步骤1 确认使用iBMC系统的客户端需具备可用版本的操作系统、浏览器，如果需要使用远程控制功能，则需同时具备可用版本的Java运行环境，具体版本要求请参考**表3-72**。

步骤2 配置客户端(例如PC) IP地址，使其与iBMC管理网口网络互通。

步骤3 通过网线将PC连接到iBMC管理网口。

步骤4 打开Internet Explorer，在地址栏中输入iBMC管理网口地址：“https://ipaddress/”，并按“Enter”。

说明

输入IPv6地址时，必须使用[ ]将其括起来，而IPv4地址无此限制。例如：

- IPv4地址：“192.168.100.1 ”。
- IPv6地址：“[fc00::64]”。

弹出如**图3-1**所示的安全告警窗口。

图 3-1 安全告警

说明

登录时可能会弹出“安全告警”界面，您可以选择忽略此告警继续浏览此网站

步骤5 单击“继续浏览此网站”。

弹出登录界面，如**图3-2**所示。

图 3-2 登录 iBMC

步骤6 选择其中一种方式登录iBMC WebUI。

- **使用本地用户登录WebUI**

----结束

使用本地用户登录 WebUI

步骤1 (可选)在登录界面中，将界面切换至目标语言。

步骤2 按照**参数说明**，输入登录iBMC WebUI的用户名和密码。

说明

iBMC默认用户名为**Administrator**，默认密码为**Admin@9000**。

步骤3 在“域名”下拉列表中，选择“这台iBMC”或“自动匹配”。

步骤4 单击“登录”。

成功登录后，显示“首页”界面。

说明

- 如果使用Internet Explorer且升级后第一次登录iBMC WebUI，界面可能会提示用户名或密码错误且无法登录，同时按下“Ctrl”+“Shift”+“DEL”，在弹出的窗口中单击删除，这样可以清除浏览器缓存中的内容。再次尝试登录，可以进入iBMC WebUI。
- 如果使用Internet Explorer无法登录iBMC WebUI，在Internet Explorer中打开“工具 > Internet选项 > 高级”页面，单击“重置”后，可以正常登录。

----结束

3.3 首页

功能介绍

“首页”界面提供了：

- 服务器的基本信息。
- 虚拟控制台。
- 服务器关键部件的信息及其快捷入口。
- 系统监控项信息及其快捷入口。
- 其他常用操作的快捷入口。

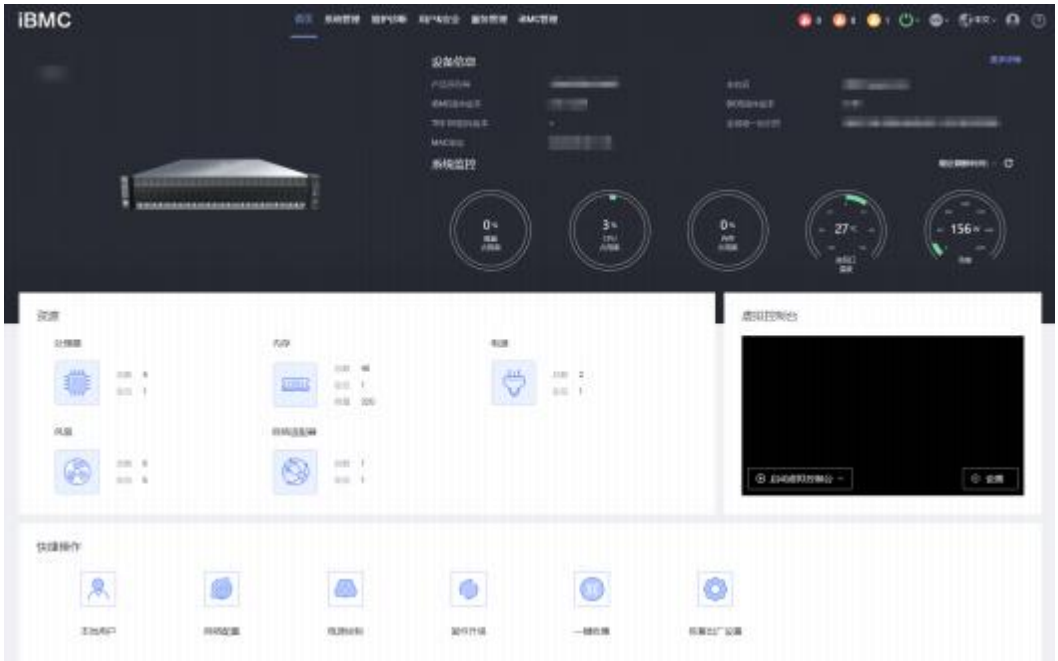
说明

本页面产品展示图仅供参考，具体以实际配置为准。

界面描述

在导航栏中选择“首页”，打开如图3-3所示界面。

图 3-3 首页



参数说明

表 3-3 基本信息

区域	展示的信息
设备信息	提供服务器的基本信息，包括： ● 产品序列号：服务器的序列号。 ● 主机名： iBMC的主机名称。 ● iBMC固件版本： iBMC系统的固件版本。 ● BIOS固件版本： BIOS的固件版本。 ● TEE OS固件版本： TEE (Trusted Execution Environment) OS版本。 ● MAC地址： iBMC管理网口物理地址。 ● 全局唯一标识符：全球唯一标识。 单击“更多详情”可以跳转到“系统管理 > 系统信息 > 产品信息”界面。
系统监控	提供系统监控快捷入口，包括： ● 磁盘/CPU/内存占用率：单击本入口可以直接跳转到“系统管理> 性能监控”界面。 ● 进风口温度：单击本入口可以直接跳转到“系统管理 > 风扇&散热”界面。 ● 功率：单击本入口可以直接跳转到“系统管理 > 电源&功率> 功率”界面。 **说明** ● 当磁盘占用率、 CPU占用率、内存占用率显示的当前值为0%时，表示未检测到该检测项的当前值。请在OS侧安装并运行iBMA 2.0。 ● 当磁盘占用率、 CPU占用率、内存占用率显示为0%<当前值<门限值时，表示资源使用情况正常。 ● 当磁盘占用率、 CPU占用率、内存占用率显示为门限值≤当前值≤100%时，表示资源使用情况已超出紧急预警区间，需要立即处理。 ● 功率的检测情况，因服务器不同而采用不同的检测区域。 ● 当进风口温度显示为当前值<一级门限值时，表示服务器温度正常。 ● 当进风口温度显示为一级门限值≤当前值<二级门限值时，表示温度已超出正常范围，需要处理。 ● 当进风口温度显示为当前值≥二级门限值时，表示温度已超出紧急预警区间，需要立即处理。

区域	展示的信息
资源	提供资源信息快捷入口，包括： ● 处理器：单击本入口可以直接跳转到“系统管理 > 系统信息 > 处理器”界面。 ● 内存：单击本入口可以直接跳转到“系统管理 > 系统信息 > 内存”界面。 ● 存储：单击本入口可以直接跳转到“系统管理 > 存储管理”界面。 ● 电源：单击本入口可以直接跳转到“系统管理 > 电源&功率> 服务器上下电”界面。 ● 风扇：单击本入口可以直接跳转到“系统管理 > 风扇&散热”界面。 ● 网络适配器：单击本入口可以直接跳转到“系统管理 > 系统信息 > 网络适配器”界面。
虚拟控制台	从本入口可以进入HTML5集成远程控制台或Java集成远程控制台。 单击“启动虚拟控制台”，在弹出的列表选择独占或共享模式的HTML5集成远程控制台或Java集成远程控制台。 单击“设置”，可以直接跳转到“虚拟控制台”界面。 关于虚拟控制台的详细介绍和常见异常帮助请参见： ● **3.9 虚拟控制台** ● **3.9.1 HTML5集成远程控制台** ● **3.9.2 Java集成远程控制台** ● **3.10 远程虚拟控制台异常帮助**

区域	展示的信息
快捷操作	提供常用操作的快捷入口，通过以下入口可以快速跳转到相关界面，包括: ● 本地用户：单击本入口可以直接跳转到“用户&安全> 本地用户”界面。 ● 网络配置：单击本入口可以直接跳转到“iBMC管理 > 网络配置”界面。 ● 电源控制：单击本入口可以直接跳转到“系统管理 > 电源&功率> 服务器上下电”界面。 ● 固件升级：单击本入口可以直接跳转到“iBMC管理 > 固件升级”界面。 ● 恢复出厂配置：单击本入口可以弹出“恢复默认”窗口，根据需要确定是否恢复出厂设置。 恢复配置操作会恢复所有用户配置的信息，例如以下配置项，但不限于这些: – 当前串口互联状态 – 功率封顶配置 – 删除用户上传的LDAP和SSL证书 – 用户名、密码、有效期、组信息、登录锁定信息 – IP获取模式、 IP地址、掩码、默认网关 – SNMP配置 – 告警上报的SNMP TRAP配置、 SMTP配置
用户上次登录信息	登录iBMC后的前十秒会显示本用户上一次登录的信息，包括: ● 用户名 ● 登录IP地址 ● 登录时间

3.4 系统管理

3.4.1 系统信息

通过“系统信息”界面的功能，您可以获取服务器的基本信息，包括产品信息、处理器、内存、网络适配器、传感器和其他部件的信息。

3.4.1.1 产品信息

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“产品信息”，打开如图3-4所示界面。

图 3-4 产品信息

参数说明

表 3-4 产品信息

参数	描述
产品信息	
产品名称	产品名称。
生产厂商	产品的生产厂商。
资产标签	产品的资产标签。 取值范围：长度为0 ~ 48个字符的字符串，允许输入数字、英文字母和特殊字符。 **说明** iBMC的普通用户没有权限设置产品资产标签，仅管理员、操作员或具有“常规配置”权限的自定义用户可以设置产品资产标签。
产品序列号	服务器的产品序列号。
产品位置	服务器的产品位置。 取值范围：长度为0 ~ 64个字符的字符串，允许输入数字、英文字母和特殊字符。
部件编码	服务器的部件编码。
主板信息	
iBMC固件版本	服务器的iBMC固件的版本号。
BIOS版本	BIOS的版本号。
CPLD版本	复杂可编程逻辑器件(CPLD ， Complex Programmable Logical Device)的版本号。
iBMC主Uboot版本	用于嵌入式系统的开机引导程序的主用镜像版本号。全称为Universal Boot Loader。

参数	描述
iBMC备Uboot版本	用于嵌入式系统的开机引导程序的备用镜像版本号。全称为Universal Boot Loader。
PCH型号	PCH芯片的型号。
PCB版本	印刷电路板(PCB ， Printed Circuit Board)的版本号。
单板ID	单板的ID。
主板厂商	主板的生产厂家。
主板型号	主板的型号。
主板序列号	主板的序列号。
部件编码	主板的部件编码。
系统软件 **说明** ● 您必须先在服务器OS侧安装iBMA 2.0并完全启动后，方可在“系统信息”区域框中查询到完整的系统软件信息。 ● 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考iBMA用户文档安装iBMA 2.0。	
计算机名称	显示服务器操作系统中定义的计算机名称。
计算机描述	显示服务器操作系统的计算机描述信息。
操作系统内核版本	当操作系统改为Linux系统时，显示其内核版本信息。
域名/工作组	显示服务器操作系统侧的域名或所属工作组。
iBMA服务	显示服务器操作系统中安装的iBMA版本信息。
iBMA运行状态	显示iBMA软件的运行状态。
iBMA驱动	显示iBMA的驱动版本信息。
操作系统版本	显示服务器操作系统的版本信息。
电子保单	
产品名称	产品名称。
产品序列号	服务器的产品序列号。
生产日期	服务器的生产日期。
UUID	服务器的全局唯一标识符(UUID ， Universally Unique Identiier) 。
单元类型	服务对象的单元类型。
服务起始时间	保单的服务起始时间。 默认值：服务器生产日期+100天。

参数	描述
服务年限(月)	保单的服务年限，单位为月。 取值范围： 1 ~ 255。 默认情况下，没有设置服务年限，此时WebUI不显示此参数。

3.4.1.2 处理器

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“处理器”，打开如图3-5所示界面。

图 3-5 处理器

参数说明

表 3-5 处理器

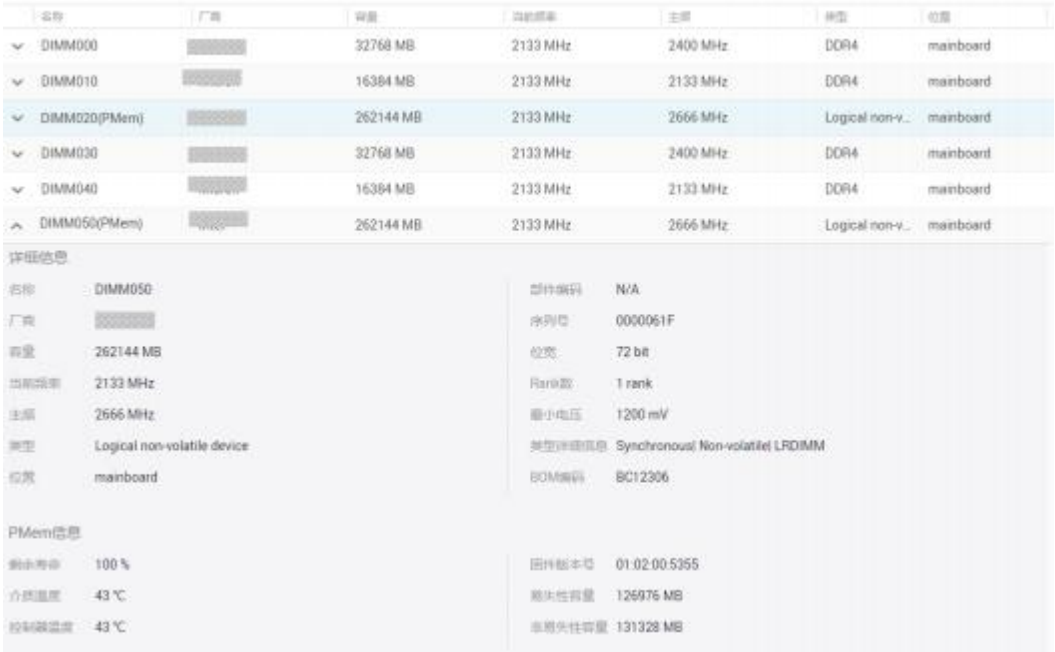
参数	描述
基本信息	显示服务器所有在位的处理器的信息。 ● 处理器的名称、厂商、型号、处理器ID 、主频、部件编码、序列号。 ● 该型号CPU支持的核数/线程数。 ● 缓存：包括CPU的一级、二级、三级缓存的容量。 ● 状态： CPU的状态信息。 ● 其他参数：该CPU支持的其他技术参数。

3.4.1.3 内存

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“内存”，打开如图3-6所示界面。

图 3-6 内存



参数说明

表 3-6 内存

参数	描述
基本信息	显示服务器内存信息。 ● 内存满配个数和当前在位个数。 ● 内存的名称、厂商、容量、当前频率、主频、类型以及位置。
详细信息	单击内存名称左侧的 ，显示内存的详细信息。 ● 展示内存的其他信息，包括内存的部件编码、序列号、位宽、 Rank数量、最小电压、类型详细信息以及BOM编码。 ● 展示PMem内存信息，包括内存的剩余寿命、介质温度、控制器温度、固件版本号、易失性容量和非易失性容量。

3.4.1.4 网络适配器

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“网络适配器”，打开如图3-7所示界面。

图 3-7 网络适配器

参数说明

表 3-7 网络适配器

参数	描述
	● 您必须先在服务器OS侧安装iBMA 2.0并完全启动后，方可在“网络适配器”页签中查询到完整的网络信息。 ● 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考iBMA用户文档安装iBMA 2.0。

参数	描述
以太网卡	显示服务器安装的板载网卡或PCIe网卡的名称、型号、芯片厂商、单板ID 、厂商、芯片型号、 PCB版本、资源归属(归属CPU 、PCH或PCIe Switch)、总线信息等信息。 ● 单击以太网卡子菜单的网卡名称，可以查看成员端口的详细信息，包括端口、状态、网口类型、介质类型、速率、自动协商和全双工状态。 **说明** 以太网卡“端口属性”的状态含义包括以下几种： ● --：表示服务器未安装iBMA，并且无法获取物理连线状态。 ● 连接：表示服务器未安装iBMA，物理连线状态处于连接状态。 ● 断开：表示服务器未安装iBMA，物理连线状态处于断开状态。 ● NoLink：表示服务器已安装iBMA，端口未连线，但端口状态为Up。 ● LinkUp：表示服务器已安装iBMA，端口已连线，且端口状态为Up。 ● LinkDown：表示服务器已安装iBMA，端口状态为Down。 ● 单击“端口属性”下方的，可查看指定网卡的网络属性，包括端口名称、固件版本、驱动名称、驱动版本、总线信息、 MAC地址、永久MAC地址、 IPv4信息(地址/子网掩码/网关)、 IPv6信息(地址/前缀长度/网关)、 VLAN信息(VLAN ID 、VLAN使能状态、 VLAN优先级使能状态) 。 ● 单击“端口属性”下方的，可查看指定网卡的连接视图，包括交换机名称、交换机连接ID 、交换机连接端口 ID以及交换机端口VLAN ID。 ● 单击“端口属性”下方的，可查看指定网卡的DCB信息和报文统计信息。 ● 如果网口安装了光模块，单击“端口属性”下方的，可查看指定网卡的光模块信息，包括厂商、序列号、部件名称、设备类型、设备连接类型、接收丢失状态、发送错误状态、波长、设备识别信息、当前温度、当前发送偏置电流、当前发送功率和当前接收功率。 ● 如果网口插上了电缆，单击“端口属性”下方的，可查看指定网卡的电缆信息，包括厂商、序列号、部件名称、设备类型以及设备连接类型。 **说明** ● 如果网卡的固件版本不支持使用某个网口，该网口的网络属性显示为空。例如某网卡有Port1 、Port2两个网口，如果该网卡的固件版本不支持使用Port2，则Port2的网络属性显示为空。 ● BIOS V672及以上版本，芯片类型为X710 ， 5719 ， 82599 ， CX4，I350，X540和X550的PCIe标卡支持上报端口MAC地址。

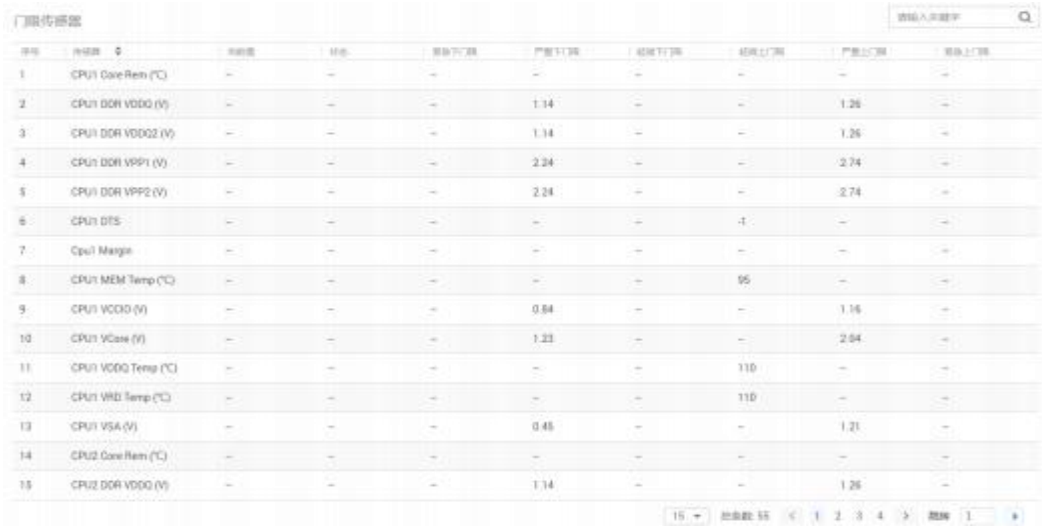
参数	描述
FC卡	显示服务器安装的FC卡的名称、厂商、型号、芯片型号、芯片厂商。 ● 单击FC卡子菜单的FC名称，可以查看成员端口的详细信息，包括端口、 FC ID 、端口类型、状态。 ● 单击端口属性下方的，可以查看指定FC卡的网络属性，包括速率、 WWPN (World Wide Port Name)、 WWNN （ World Wide Node Name)、固件版本、驱动名称、驱动版本。 ● 支持MCTP的FC卡支持显示以下信息： – 工作速率 – 工作模式 – 光模块开启状态 – 对端设备信用值 – 本端设备信用值 – 发送速率 – 接收速率 – 速率协商阶段
Team	显示汇聚网口的名称、状态、工作模式、 IPv4信息(地址/子网掩码/网关)、 IPv6信息(地址/前缀长度/网关)、 MAC地址、 VLAN信息(VLAN ID 、VLAN使能状态、 VLAN优先级使能状态)。 单击汇聚网口子菜单的网口名称，可以查看成员端口的详细信息，包括网卡名称、网口名称、端口号、 MAC地址和状态。
Bridge	显示桥接网口的名称、状态、 IPv4信息(地址/子网掩码/网关)、 IPv6信息(地址/前缀长度/网关)、 MAC地址、 VLAN信息(VLAN ID 、VLAN使能状态、 VLAN优先级使能状态)。 ● 单击桥接网口子菜单的网口名称，可以查看成员端口的详细信息，包括网口名称、端口、状态、网口类型和介质类型。 ● 单击端口属性下方的，可以查看成员端口的网络属性。

3.4.1.5 传感器

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“传感器”，打开如图3-8所示界面。

图 3-8 传感器



参数说明

表 3-8 传感器

参数	描述
传感器	传感器是指监控服务器各类指标的模块，可以是逻辑模块或物理实体。 **说明** 在搜索框中设置搜索条件后，系统将自动显示符合条件的传感器信息。
当前值	传感器当前监控到的指标信息。 **说明** 如果显示为--，表示传感器无法监控到指标。
状态	门限传感器扫描状态： ● OK：表示传感器正常。 ● --：传感器无法监控到指标。 ● NC：表示传感器检测到轻微告警。 ● CR：表示传感器检测到严重告警。 ● NR：表示传感器检测到紧急告警。
紧急下门限	使传感器产生紧急告警的下门限值。
严重下门限	使传感器产生严重告警的下门限值。
轻微下门限	使传感器产生轻微告警的下门限值。
轻微上门限	使传感器产生轻微告警的上门限值。
严重上门限	使传感器产生严重告警的上门限值。
紧急上门限	使传感器产生紧急告警的上门限值。
搜索	在搜索框中设置搜索条件后，系统自动显示符合条件的传感器信息。

3.4.1.6 其他界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“其他”，打开如图3-9所示界面。

图3-9 其它

参数说明

表 3-9 其他

参数	描述
硬盘背板	显示服务器硬盘背板信息。 ● 硬盘背板满配个数和当前在位个数。 ● 硬盘背板的名称、位置、厂商、编号、类型、 PCB版本、CPLD版本、单板ID 、部件编码以及序列号。
风扇背板	显示服务器风扇背板信息，包括风扇背板的名称、位置、厂商、类型、 PCB版本以及单板ID。
电源背板	显示服务器电源背板信息，包括电源背板的名称、类型、 PCB版本以及单板ID。
处理器板	显示服务器处理器板信息。 ● 处理器板满配个数和当前在位个数。 ● 处理器板的名称、厂商、槽位号、类型、 PCB版本、 CPLD版本、单板ID以及功率。 **说明** 仅2488H V6支持处理器板。
Riser卡	显示服务器Riser卡信息。 ● Riser卡满配个数和当前在位个数。 ● Riser卡的名称、厂商、槽位、类型、 PCB版本、单板ID、部件编码以及序列号。
RAID卡	显示服务器RAID卡信息。 ● RAID卡满配个数和当前在位个数。 ● RAID卡的名称、位置、厂商、编号、类型、 PCB版本、CPLD版本、单板ID 、资源归属、部件编码以及序列号。
PCIe卡	显示服务器PCIe卡信息。 ● PCIe卡满配个数和当前在位个数。 ● PCIe卡的描述、位置、厂商、槽位、制造商ID、设备ID、子厂商ID、子设备ID以及资源归属。
OCP卡	显示服务器OCP卡信息(仅针对支持OCP卡的服务器)。 ● OCP卡满配个数和当前在位个数。 ● OCP卡的描述、位置、厂商、槽位、制造商ID、设备ID、子厂商ID、子设备ID以及资源归属。
LCD	显示服务器LCD固件信息。

参数	描述
BBU模块	显示服务器BBU模块信息(仅针对支持BBU模块的服务器)。 ● BBU模块满配个数和当前在位个数。 ● BBU模块的名称、 ID 、固件版本、剩余容量、工作状态、电池型号、序列号、厂商以及M.2卡的在位状态。
安全模块	显示服务器安全模块信息。 ● 安全模块满配个数和当前在位个数。 ● 安全模块的协议类型、协议版本、厂商、厂商版本以及自检状态。
M.2转接卡	显示服务器M.2转接卡信息，包括M.2转接卡的名称、厂商、描述、 PCB版本、单板ID 、部件编码以及序列号(仅针对支 M.2转接卡的服务器)。

3.4.2 性能监控

功能介绍

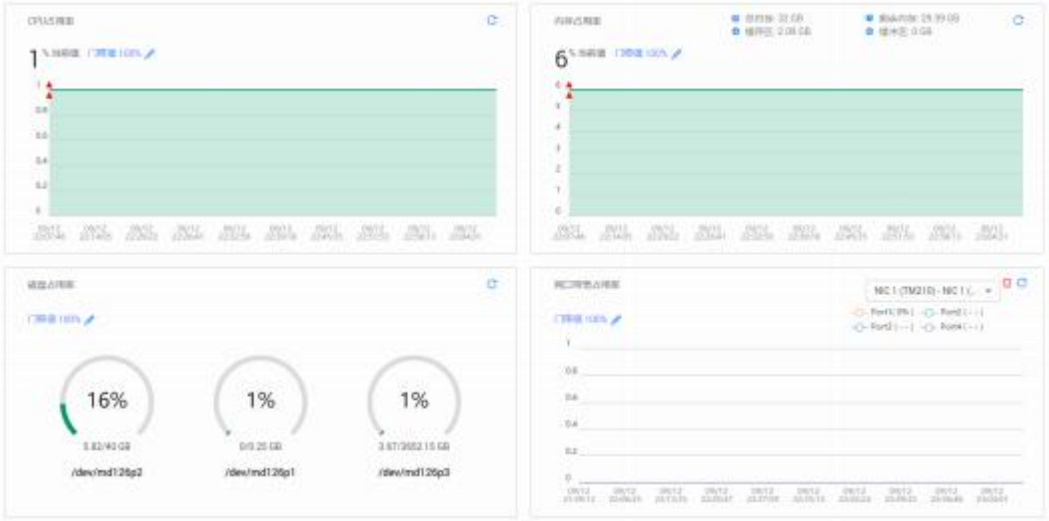
通过“性能监控”界面，您可以：

- 查看CPU最近一小时的占用率。
- 查看内存最近一小时的占用率。
- 查看所有磁盘的占用率及磁盘容量信息。
- 查看所有网口的带宽占用率。

界面描述

在导航栏中选择“系统管理 > 性能监控”，打开如图3-10所示界面。

图 3-10 性能监控



参数说明

表 3-10 性能监控

参数	描述
CPU占用率	运行的程序占用CPU资源的比例。 **说明** ● 服务器OS侧在安装iBMA 2.0并完全启动后， CPU占用率数据从iBMA 2.0获取，与OS侧统计的CPU占用率一致。 ● 服务器OS侧未安装iBMA 2.0或iBMA 2.0未完全启动时， CPU占用率数据从Intel ME（Management Engine)获取，是由CPU内部模块计算出的所有核的每秒计算利用率。 ● 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考文档安装iBMA 2.0。
内存占用率	运行的程序占用内存的比例。 **说明** ● 服务器OS侧在安装iBMA 2.0并完全启动后，内存占用率数据从iBMA 2.0获取，与OS侧统计的内存占用率一致。 ● 服务器OS侧未安装iBMA 2.0或iBMA 2.0未完全启动时，内存占用率数据从Intel ME（Management Engine)获取，表示内存带宽占用率，与OS侧统计的内存容量占用率不同。 ● 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考文档安装iBMA 2.0。
磁盘占用率	磁盘分区中已使用的空间占整个分区空间的比例、磁盘分区路径、已使用容量及磁盘分区总容量。 **说明** ● 您必须先在服务器OS侧安装iBMA 2.0，并完全启动后，方可查看磁盘占用率信息。 ● 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考文档安装iBMA 2.0。
网口带宽占用率	服务器网卡提供的所有网口的带宽占用比例。 **说明** ● 您必须先在服务器OS侧安装iBMA 2.0，并完全启动后，方可查看网口带宽占用率信息。 ● 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考文档安装iBMA 2.0。
当前值	服务器当前CPU、内存、磁盘或网口带宽的占用率。
门限值	服务器当前CPU、内存、磁盘或网口带宽占用率的门限值，占用率超出设置的门限值后， iBMC会上报一个正常事件。 取值范围： 0 ~ 100的整数值。
	打开编辑门限值的输入框。
	刷新相关性能监控项的统计信息。
	清空网口带宽占用率统计信息。

设置门限值

步骤1 单击待设置目标区域框的。

弹出门限值输入框。

步骤2 根据界面提示的取值范围，在输入框中输入门限数值。

步骤3 单击保存设置。

设置门限值后，您可以单击刷新占用率曲线。

----结束

3.4.3 存储管理

功能介绍

通过使用“存储管理”界面的功能，您可以查看和配置服务器当前存储设备的信息。

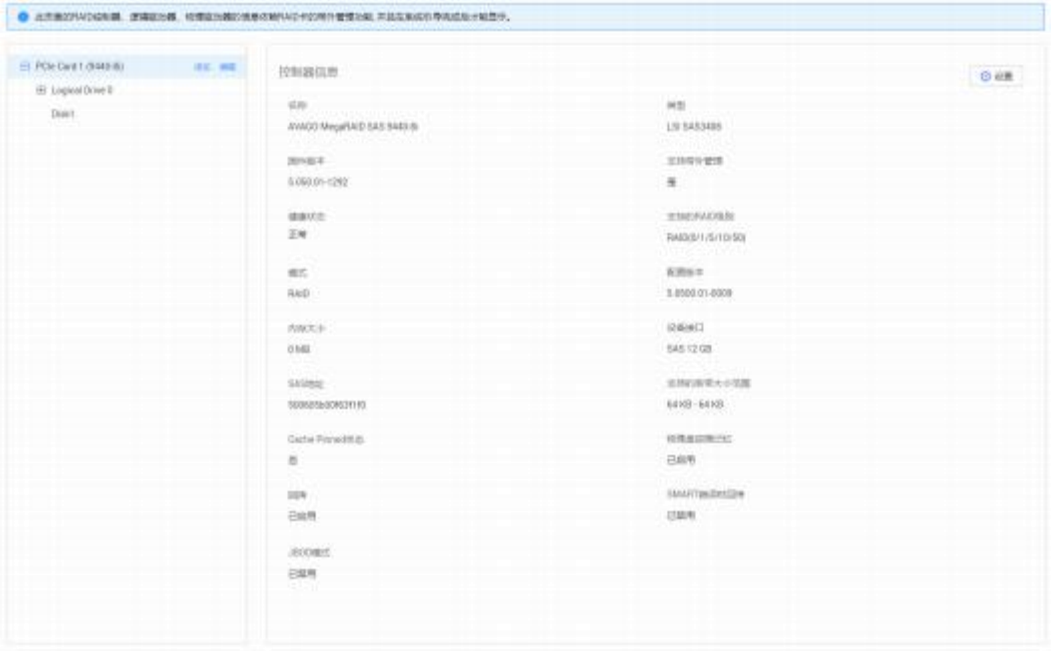
说明

- 此页面的RAID控制器、逻辑驱动器、物理驱动器的信息依赖RAID卡的带外管理功能，并且在系统引导完成后或安装并完全启动iBMA 2.0才能显示。
- “存储管理”中的信息在系统下电或系统未完成启动时为无效数据。服务器在每次上电并且系统完成启动后， iBMC会重新识别所有物理盘。如果此时物理盘正在重构，则此物理盘会延迟识别，在完成识别之前，物理盘的信息为无效数据；如果物理盘识别失败，对应的传感器（DISKN)会产生Drive Fault告警。
- 硬盘被识别并完全显示所需要的时间与逻辑盘和物理盘的数目有关，逻辑盘和物理盘的数目越多，硬盘被识别需要的时间越长。

界面描述

在导航栏中选择“系统管理 > 存储管理”，打开如图3-11所示界面。

图 3-11 存储管理



参数说明

表 3-11 存储管理

参数	描述
RAID控制器	RAID控制器信息： ● 控制器名称、类型、固件版本、是否支持带外管理、健康状态、支持的RAID级别、模式、配置版本、内存大小、设备接口、 SAS地址、支持的条带大小范围、 Cache Pinned状态、物理盘故障记忆启用状态、回拷启用状态、 SMART错误时回拷启用状态、 JBOD模式启用状态。 ● BBU名称、状态、健康状态。 **说明** ● RAID控制器不支持带外管理且未安装运行iBMA 2.0的情况下，仅显示控制器名称、类型、固件版本以及是否支持带外管理。 ● 您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。 ● 请不要在RAID卡侧将其工作模式设置为JBOD，iBMC无法识别该模式下的RAID卡。详细信息请参考各服务器的RAID控制卡用户指南。

参数	描述
逻辑盘	逻辑盘信息： 名称、状态、 RAID级别、容量、条带大小、 SSCD功能启用状态、默认读策略、当前读策略、默认写策略、当前写策略、默认IO策略、当前IO策略、物理盘缓存状态、访问策略、初始化类型、后台初始化启用状态、二级缓存启用状态、一致性校验运行状态、系统盘符、是否为启动盘。 **说明** ● RAID控制器不支持带外管理且未安装运行iBMA 2.0的情况下，无法显示RAID控制器下的逻辑盘信息。 ● 您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
物理盘	物理盘信息： 厂商、容量、型号、序列号、固件版本、固件状态、介质类型、接口类型、支持的速率、协商速率、 SAS地址(0) 、SAS地址(1)、电源状态、温度、热备状态、重构状态、巡检状态、健康状态、剩余磨损率、定位状态和累计通电时间。 **说明** ● RAID控制器不支持带外管理且未安装运行iBMA 2.0的情况下，RAID控制器下挂载的物理盘仅显示接口类型。 ● 直通硬盘仅支持显示健康状态、定位状态和接口类型，且接口类型显示为“SAS/SATA”。 ● 您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。 ● 仅SATA硬盘及希捷SAS硬盘支持累计通电时间的查询。 ● 对于NVMe硬盘，如果服务器OS为Windows或VMware，由于其不支持NVMe硬盘接口的速率协商特性，此处“协商速率”显示为“NA”。 ● 剩余磨损率表示SSD硬盘的使用寿命。剩余磨损率越大，表示硬盘的损耗越小，使用寿命越长；剩余磨损率越小，表示硬盘的损耗越大，使用寿命越短。例如剩余磨损率为100%，表示硬盘没有损耗。 ● M.2硬盘不支持显示定位状态信息。
控制器配置项	● 回拷 ● SMART错误时回拷 ● JBOD模式
逻辑盘配置项	● 创建逻辑盘 ● 删除逻辑盘 ● 修改逻辑盘属性 **说明** RAID卡模式为JBOD时，不支持查询和配置逻辑盘信息。

参数	描述
物理盘配置项	• 定位状态 • 热备状态 • 固件状态 **说明** M.2硬盘无定位状态配置项。

查看控制器属性

说明

执行此操作需满足以下条件：

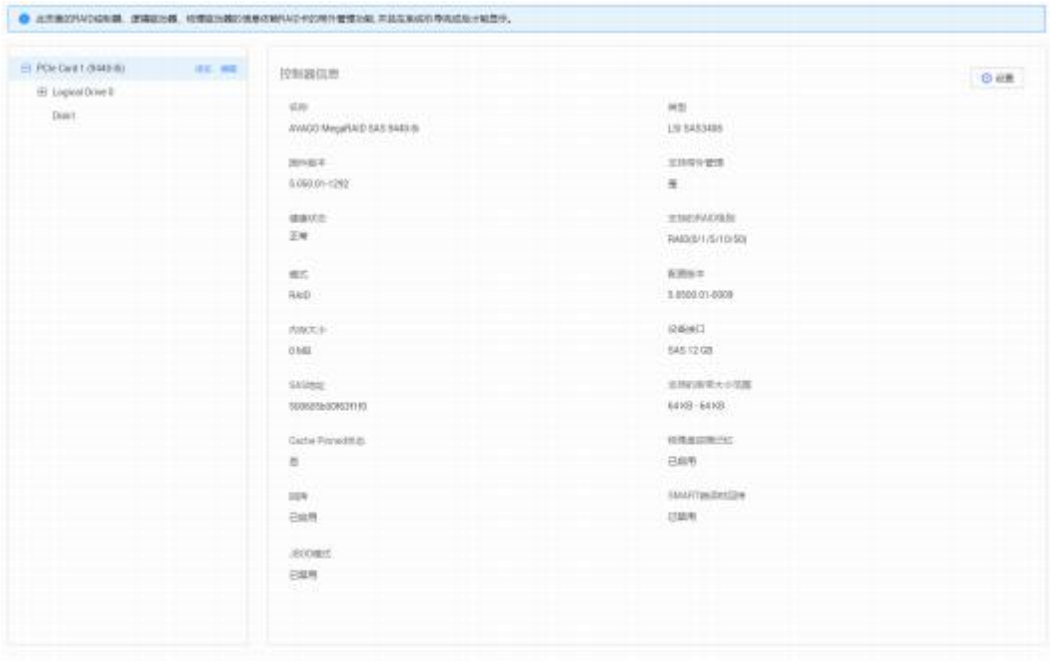
- RAID卡支持iBMC带外管理或已在OS侧安装并运行iBMA 2.0。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待查看的RAID控制器。

右侧区域显示RAID控制器的基本属性，如图3-12所示。

图 3-12 查看控制器属性



----结束

查看 RAID 组属性

说明

执行此操作需满足以下条件：

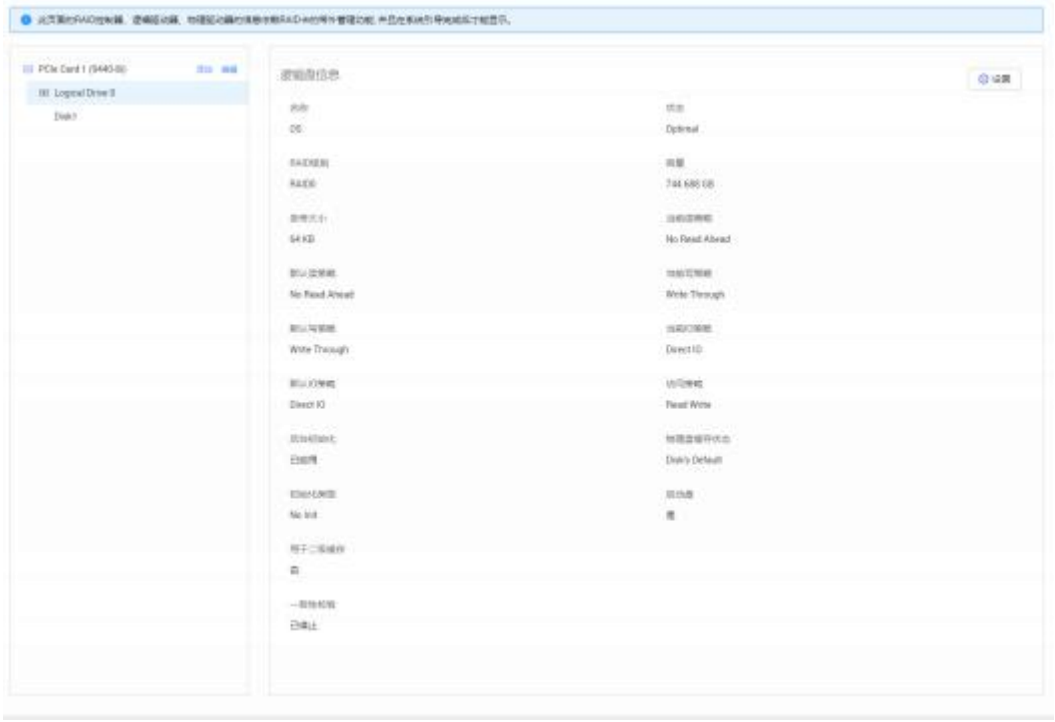
- RAID卡支持iBMC带外管理或已在OS侧安装并运行iBMA 2.0。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待查看的RAID组。

右侧区域显示RAID组的基本属性，如图3-13所示。

图 3-13 查看 RAID 组属性



----结束

查看物理磁盘属性

说明

执行此操作需满足以下条件：

- 必须为RAID卡管理的硬盘。
- RAID卡支持iBMC带外管理或已在OS侧安装并运行iBMA 2.0。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待查看的物理磁盘，可以是RAID组中的成员盘，也可以是独立的磁盘。

其基本属性如图3-14和图3-15所示。

图 3-14 查看物理磁盘属性(成员盘)

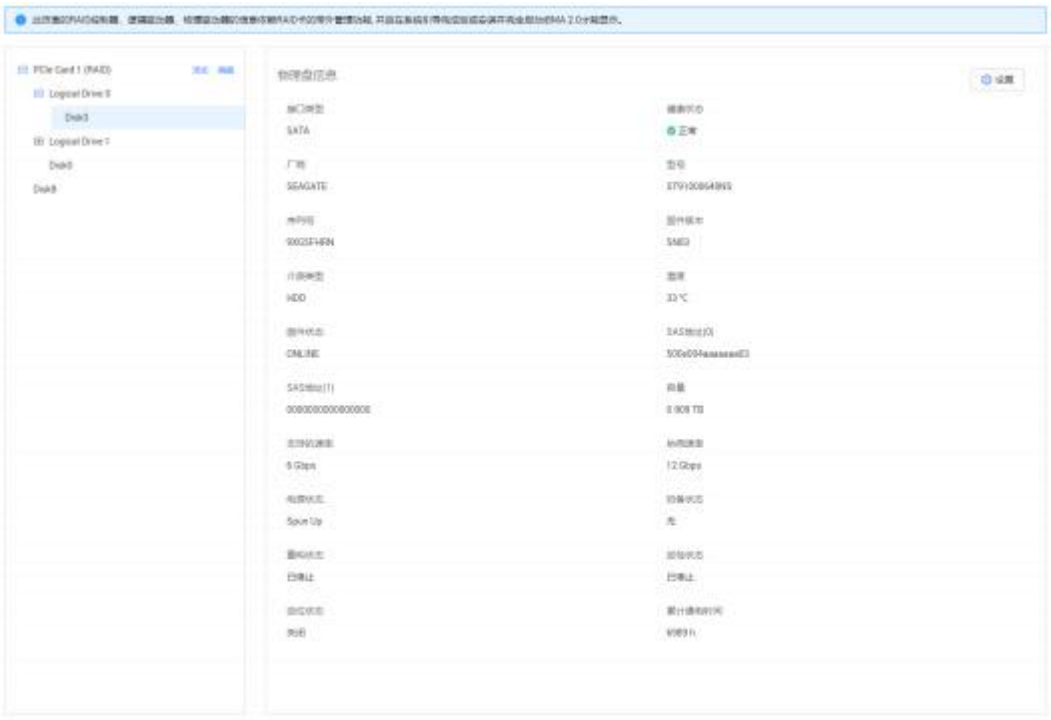
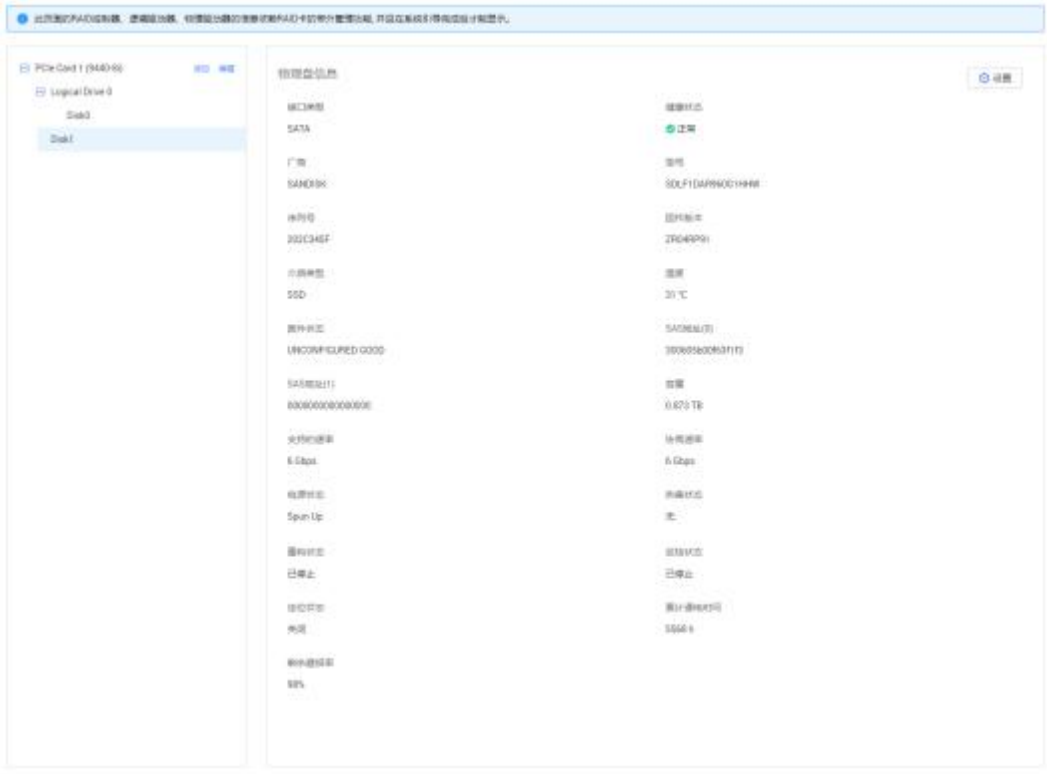


图 3-15 查看物理磁盘属性(单独磁盘)



----结束

修改 RAID 控制器属性

说明

执行此操作需满足以下条件：

- RAID卡支持iBMC带外管理。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待操作的RAID控制器。

步骤3 单击“设置”。

如图3-16所示，界面中各配置项的含义如表3-12所示。

图 3-16 修改 RAID 控制器属性

表 3-12 控制器配置项说明

配置项	说明
回拷	具备冗余功能的RAID的一块成员盘故障之后，热备盘自动替换故障数据盘并开始同步。当更换新的数据盘之后，热备盘中的数据会回拷至新数据盘，回拷完毕后，原热备盘会恢复其热备状态。
SMART错误时回拷	当控制器检测到SMART错误时，执行回拷操作。
JBOD模式	控制器可对所连接的物理盘进行指令透传，在不配置逻辑盘的情况下，用户指令可以直接透传到物理盘，方便上层业务软件或管理软件访问控制物理盘。
恢复默认设置	单击“恢复默认配置”，可将RAID控制器的属性恢复为默认值。

配置项	说明
导入Foreign配置	单击“导入Foreign配置”，可以导入Foreign磁盘包含的RAID配置信息，无需输入配置文件。

步骤4 参考**表3-12**的说明进行配置，并单击“确认”。

----结束

创建逻辑盘

说明

执行此操作需满足以下条件：

- 必须为RAID控制卡管理的硬盘且RAID控制卡需支持创建逻辑盘功能。
- 加入逻辑盘的物理盘固件状态为UNCONFIGURED GOOD。
- RAID卡支持iBMC带外管理。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- 当前RAID控制卡下的逻辑盘数量未达到RAID控制卡所支持的最大数量。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待操作的RAID控制器。

步骤3 单击“添加”。

打开创建逻辑盘区域，如**图3-17**所示，界面中各配置项的含义如**表3-13**所示。

图 3-17 创建逻辑盘

表 3-13 创建逻辑盘配置项说明

配置项	说明
名称	逻辑盘的名称。

配置项	说明
二级缓存	是否使能CacheCade。
条带大小	每个物理盘上的数据条带的大小。
读策略	逻辑盘的数据读策略，包括： ● Read Ahead：使能预读取功能。控制器可以预读取顺序数据或预测需要即将使用到的数据并存储在Cache中。 ● No Read Ahead：关闭预读取功能。
写策略	逻辑盘的数据写策略，包括： ● Write Through：当磁盘子系统接受到所有传输数据后，控制器将给主机返回数据传输完成信号。 ● Write Back with BBU：在控制器无BBU或BBU损坏的情况下，控制器将自动切换到Write Through模式。 ● Write Back：当控制器Cache收到所有的传输数据后，将给主机返回数据传输完成信号。
IO策略	应用于特殊的逻辑盘读取，不影响预读取Cache。包括： ● Cached IO：所有读和写均经过RAID控制器Cache处理。仅在配置CacheCade 1.1时需要设置为此参数值，其他场景不推荐。 ● Direct IO：在读、写场景中的定义不同： – 在读场景中，直接从物理盘读取数据。(如果“读策略”被设置为“ReadAhead”，此时读数据经过RAID控制器的Cache处理。) – 在写场景中，写数据经过RAID控制器的Cache处理。(如果“写策略”被设置为“Write Through”，此时写数据不经过RAID控制器的Cache处理，直接写入物理盘。)
物理盘缓存策略	物理盘Cache策略，包括： ● Enable：读写过程中数据经过物理盘写Cache，使写性能提升，但当系统意外掉电时，如果没有保护机制，数据会丢失。 ● Disable：读写过程中数据不经过物理盘写Cache，当系统意外掉电时，数据不会丢失。 ● Disk's default：保持默认的缓存策略。
访问策略	逻辑盘的访问策略，包括： ● Read Write：可读可写。 ● Read Only：只读访问。 ● Blocked：禁止访问。

配置项	说明
初始化类型	创建逻辑盘后，对其采用的初始化方式，包括： ● No Init：不进行初始化。 ● Quick Init：只把逻辑盘的前100MByte空间进行全写0操作，随后此逻辑盘的状态就变为“Optimal”。 ● Full Init：需要把整个逻辑盘都初始化为0，才会结束初始化过程，在此之前逻辑盘状态为“initialization”。
RAID级别	逻辑盘的RAID级别。 **说明** RAID级别为1时，仅支持选择2个物理盘配置为RAID1。
每个Span的成员盘数	当RAID级别配置为50 、60时，需要设置子组中物理盘个数。 **说明** 当RAID级别配置为10时，“每个Span的成员盘数”默认为2，且不支持修改。
物理盘	要加入逻辑盘的物理盘。
可用容量	逻辑盘的可用容量。
容量	逻辑盘的容量。

步骤4 参考**表3-13**的说明进行配置，并单击“保存”。

----结束

删除逻辑盘

说明

执行此操作需满足以下条件：

- 必须为RAID卡管理的硬盘。
- RAID卡支持iBMC带外管理。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 删除逻辑盘。

- 单击待删除的逻辑盘右侧的  ，可单独删除指定逻辑盘。
- 单击RAID控制器右侧的“编辑”后，勾选要删除的逻辑盘并单击“删除”，可批量删除多个逻辑盘。

弹出操作确认对话框。

步骤3 单击“确定”。

----结束

修改逻辑盘属性

说明

执行此操作需满足以下条件：

- 必须为RAID卡管理的硬盘。
- RAID卡支持iBMC带外管理。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待操作的逻辑盘。

步骤3 单击“设置”。

打开逻辑盘编辑菜单如**图3-18**所示，界面中各配置项的含义如**表3-14**所示。

图 3-18 修改逻辑盘

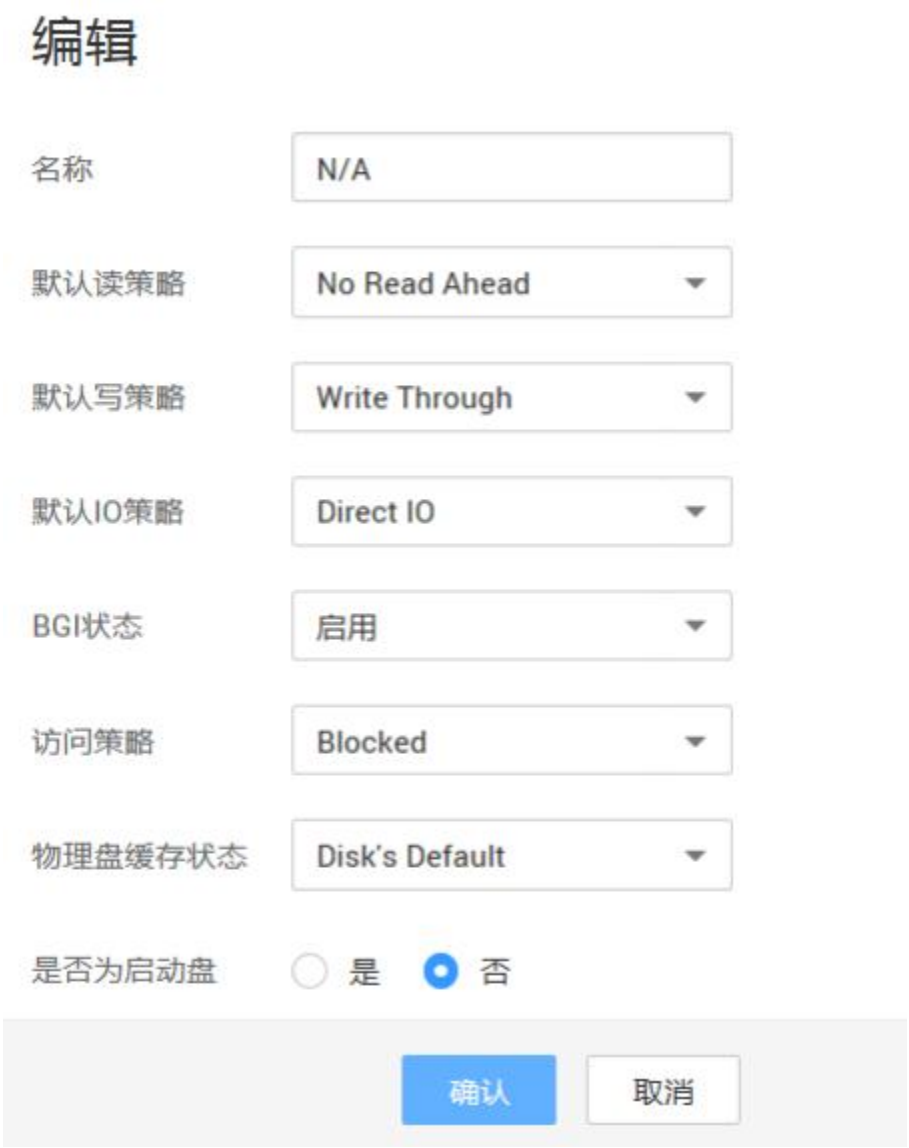


表 3-14 修改逻辑盘配置项说明

配置项	说明
名称	逻辑盘的名称。
默认读策略	逻辑盘的数据读策略，包括： ● Read Ahead：使能预读取功能。控制器可以预读取顺序数据或预测需要即将使用到的数据并存储在Cache中。 ● No Read Ahead：关闭预读取功能。
默认写策略	逻辑盘的数据写策略，包括： ● Write Through：当磁盘子系统接受到所有传输数据后，控制器将给主机返回数据传输完成信号。 ● Write Back with BBU：在控制器无BBU或BBU损坏的情况下，控制器将自动切换到Write Through模式。 ● Write Back：当控制器Cache收到所有的传输数据后，将给主机返回数据传输完成信号。
默认IO策略	应用于特殊的逻辑盘读取，不影响预读取Cache。包括： ● Cached IO：所有读和写均经过RAID控制器Cache处理。仅在配置CacheCade 1.1时需要设置为此参数值，其他场景不推荐。 ● Direct IO：在读、写场景中的定义不同： – 在读场景中，直接从物理盘读取数据。（“读策略”设置为“Read Ahead”时除外，此时读数据经过RAID控制器的Cache处理。） – 在写场景中，写数据经过RAID控制器的Cache处理。（“写策略”设置为“Write Through”时除外，此时写数据不经过RAID控制器的Cache处理，直接写入物理盘。）
BGI状态	是否启用后台初始化。
访问策略	逻辑盘的访问策略，包括： ● Read Write：可读可写 ● Read Only：只读访问 ● Blocked：禁止访问

配置项	说明
物理磁盘缓存状态	物理盘Cache策略，包括： ● Enabled：读写过程中数据经过物理盘写Cache，使写性能提升，但当系统意外掉电时，如果没有保护机制，数据会丢失。 ● Disabled：读写过程中数据不经过物理盘写Cache，当系统意外掉电时，数据不会丢失。 ● Disk's default：保持默认的缓存策略。
是否为启动盘	是否设置该逻辑盘为系统启动盘。
SSCD缓存功能	是否使用CacheCade逻辑盘做缓存。

步骤4 参考**表3-14**的说明进行配置，并单击“确认”。

----结束

修改成员盘属性

说明

执行此操作需满足以下条件：

- 必须为RAID卡管理的硬盘。
- RAID卡支持iBMC带外管理。您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
- BIOS启动完成。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 选中待操作的逻辑盘。

步骤3 单击 展开成员盘。

步骤4 选中要操作的成员盘。

步骤5 单击成员盘后的“设置”。

弹出成员盘编辑窗口，如**图3-19**所示，界面中各配置项的含义如**表3-15**所示。

图 3-19 编辑成员盘属性

表 3-15 成员盘配置项说明

配置项	说明
定位状态	物理盘是否已开启定位指示灯。 **说明** M.2硬盘无定位状态配置项。
热备状态	物理盘的热备状态，包括： ● 无：不设置 ● 全局：设置为全局热备盘 ● 局部：设置为局部热备盘
固件状态	物理盘的状态，包括： ● UNCONFIGURED BAD：不可用 ● ONLINE：在线 ● OFFLINE：离线 ● UNCONFIGURED GOOD：空闲 ● JBOD：直通(OS直接管理) **说明** RAID控制器的JBOD模式为“禁用”时，物理盘的固件状态不允许设置为“JBOD”。

步骤6 参考**表3-15**的说明进行配置，并单击“确认”。

----结束

擦除物理盘数据

说明

- 只有加密盘支持擦除数据操作。
- 数据擦除后将无法恢复，请谨慎操作。

步骤1 在导航栏中选择“系统管理 > 存储管理”。

步骤2 鼠标移至待操作的物理盘名称。

步骤3 单击 。

步骤4 根据实际需要在弹出的提示框中单击“是”。

----结束

3.4.4 电源&功率

功能介绍

通过使用“电源&功率”界面的功能，您可以：

- 查看服务器的电源信息。
- 查看服务器的功率信息。
- 设置是否开启功率封顶功能，限制服务器的封顶功率，以及超过封顶功率后的进一步动作。
- 查看服务器近一周或近一天的历史平均功率和峰值功率曲线，以及每个采样时间点获取的服务器功率，也可以重新统计功率。
  iBMC的采样时间间隔为10分钟。
- 对服务器进行上电、下电或重启，以及触发服务器产生一个不可屏蔽中断（NMI，Non-maskable Interrupt)操作。
- 设置服务器面板电源按钮。
- 设置服务器的通电开机策略。

须知

- 设置封顶功率时，请谨慎操作。如果封顶功率过低，系统性能和服务器上的业务运营会受到影响。
- 请谨慎选择封顶失败后的“功率封顶失效自动关机”动作，避免对业务造成影响。
- 请在强制下电、下电、强制重启、强制下电再上电或NMI操作前确认无业务风险。
- NMI是一种不能被标准屏蔽中断技术忽略的特殊中断。不可屏蔽中断特别用于不可恢复硬件错误的信号提示。通过使用特殊方法，某些不可屏蔽中断也能够被屏蔽。

界面描述

在导航栏中选择“系统管理 > 电源&功率”，打开如图3-20 、图3-21以及图3-22所示界面。

图 3-20 电源信息

图 3-21 功率

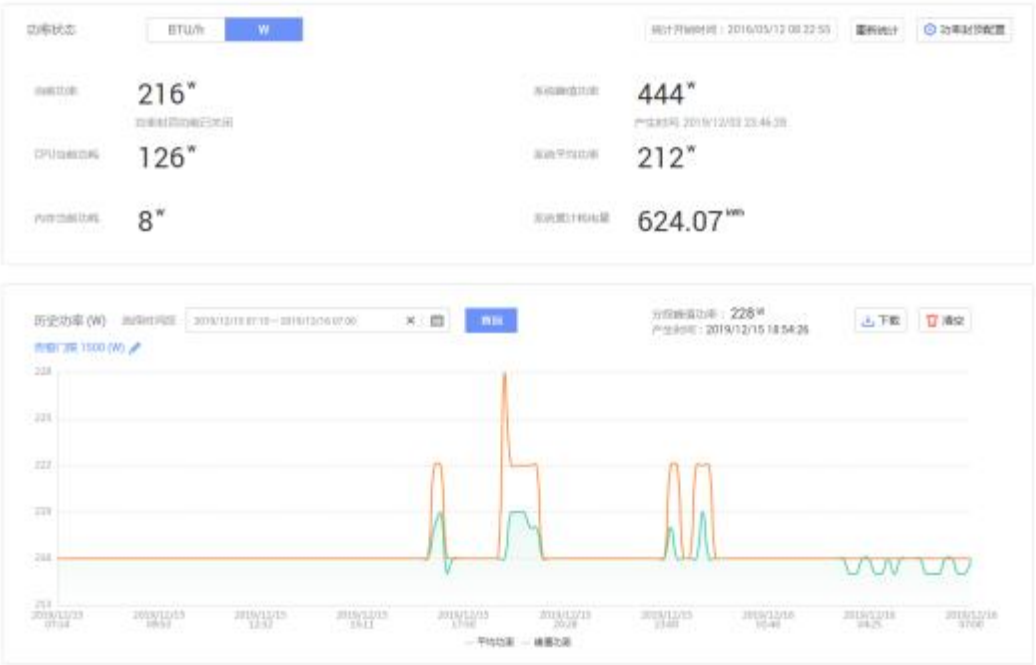


图 3-22 服务器上下电

参数说明

表 3-16 电源信息

参数	描述
基本信息	显示在位电源模块的槽位、厂商、类型、序列号、固件版本、额定功率、输入模式、输入电压、输出电压以及部件编码。
当前功率	显示电源模块当前的输出功率。

参数	描述
工作模式	显示电源模块当前的工作模式，包括： ● 负载均衡：多个电源模块同时为服务器供电，均摊服务器所需功耗。 此种工作模式整体供电能力高，单路供电故障时，对备用电源模块的冲击较小，但是电源模块供电效率低，耗电量大。 ● 主备供电：其中一个或多个电源模块为主供电模块，为服务器供电，其他电源模块作为备份。 此种工作模式能够提高电源模块供电效率，延长电源模块使用寿命。 默认取值：负载均衡 **说明** ● 在系统功耗较小的情况下，主备供电模式更为节能。 ● 主备供电模式下且Redish未开启N+R时，若系统功耗大于等于主用电源模块额定功率的75%时，会自动切换为负载均衡模式。 ● 开启主备供电功能，主用电源个数必须大于或等于备用电源个数。 ● 若已通过Redish接口开启N+R ，则不支持设置电源的工作模式。
主用电源	“主备供电”工作模式下的主用电源模块。
深度休眠	**须知** 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。 开启深度休眠，服务器下电后，进入深度休眠模式的电源会关闭输出；关闭深度休眠或服务器上电后，进入深度休眠模式的电源会恢复输出。 单击  或  并单击“保存”，可切换状态。 .  表示开启深度休眠，此操作在OS下电后生效。 .  表示关闭深度休眠，此操作在OS下电后生效。 **说明** 如果使能了深度休眠功能， OS下电后，则电源进入深度休眠状态。

表 3-17 功率

参数	描述
功率状态	设置“功率”页面中功率的单位，可以设置为“BTU/h”或“W”。 **说明** 1 BTU/h = 0.293 W
统计开始时间	开始统计功率相关参数的时间。
重新统计	清空当前统计记录，重新开始统计。

参数	描述
功率封顶配置	使用本功能前，需要进入BIOS设置菜单，完成以下操作： 1. 将“EIST Support”(部分产品此参数显示为“EIST”)设置为“Enabled”。 2. Purley平台下，将“Software Controlled T-States”设置为“Enabled”。“T-State Throttle Level”建议保持默认值，默认值为“Disabled”。 功耗封顶下限是实现功耗封顶的最低建议值，设置较低封顶值可能导致封顶失败。 例如，当系统中含有GPU，SSD等高功率的PCIe设备时，如果设置的封顶值接近下限值，可能导致封顶失败。
功率封顶使能状态	使用本功能前，需要进入BIOS设置菜单，完成以下操作： 1. 将“EIST Support”(部分产品此参数显示为“EIST”)设置为“Enabled”。 2. Purley平台下，将“Software Controlled T-States”设置为“Enabled”。“T-State Throttle Level”建议保持默认值，默认值为“Disabled”。 启用或禁用功率封顶功能。
功率封顶值	限制服务器可运行的最大功率。 取值范围：开启功率封顶使能后，单击“功率封顶值”后的输入框可以查看到取值范围，不同产品取值范围不相同，以界面提示为准。 取值原则：最小可设置的功率不小于iBMC给出的下限值。
功率封顶失效自动关机	当服务器功率封顶失败时，服务器将在15秒后自动关机。
当前功率	服务器当前的功率。
CPU当前功耗	服务器当前在位的CPU的功率。
内存当前功耗	服务器当前在位的内存的功率。
系统峰值功率	从服务器首次上电或重新统计起始时间到当前时刻，服务器出现过的最大功率值。
系统平均功率	从服务器首次上电或重新统计起始时间，服务器功率的平均值。
系统累计耗电量	从服务器首次上电或重新统计起始时间，服务器耗电量的累计值。
历史功率	服务器最近一周内任意时间段(精确到10分钟)内的峰值功率和平均功率统计数据。 选择最近一周内的任意时间段，单击“查询”，可查看到该时间段内的峰值功率和平均功率曲线，以及分段峰值功率及产生时间。 **说明** 如果自重新统计时间起到当前还不足一周，只能查看自重新统计时间起到当前的功率曲线。

参数	描述
告警门限	实时功率的告警门限。请参照界面提示的取值范围设置告警门限。 实时功率超过设置的阈值时， iBMC将产生告警。
下载	单击“下载”，可以下载历史功率数据文件到本地PC。
清空	单击“清空”，可以清除所有历史功率数据。 清除所有历史功率数据后， iBMC从当前时刻开始重新统计。“历史功率”区域框显示重新统计的功率信息。

表 3-18 服务器上下电

参数	描述
系统状态	显示服务器上下电状态。
上电	对服务器执行上电操作。
下电	对服务器执行下电操作。
下电时限(秒)	对服务器执行下电操作后，根据“下电时限”的设置情况，将进行不同的处理。 ● 启用“下电时限”时，如果服务器无法在指定时间内下电， iBMC会对服务器执行强制下电。 ● 关闭“下电时限”时， iBMC不会干涉服务器的下电过程。 **说明** 启用下电时限后，对服务器执行下电操作，在下电时限内，如果在操作系统取消下电，超过下电时限后，服务器仍会执行强制下电。 不同设备的取值范围和默认取值不同，以Web界面提示为准，单位为秒。 选中“下电时限”左侧的复选框，表示启用“下电时限”。 单击，在文本框中修改下电时限，完成修改后单击保存设置。
强制下电	**须知** 强制下电可能会损坏用户的程序或者未保存的数据，请根据操作系统实际情况谨慎选择操作方式。 对服务器执行强制下电，服务器将在6秒内完成下电操作。 该操作与长按电源按钮5s的效果相同。
强制重启	**须知** 强制重启可能会损坏用户的程序或者未保存的数据，请根据操作系统实际情况谨慎选择操作方式。 对服务器执行强制重启操作，服务器会立即重新启动。 **说明** ● 在服务器下电状态下，“强制重启”操作无效。 ● 该操作会影响正在执行的下电操作。

参数	描述
强制下电再上电	**须知** 强制下电再上电可能会损坏用户的程序或者未保存的数据，请根据操作系统实际情况谨慎选择操作方式。 对服务器执行强制下电，等待约6秒后，服务器直接上电。
NMI	**须知** NMI仅用于内部调测，使用时需要操作系统中有对应的NMI中断处理程序，否则可能引起系统崩溃。请谨慎使用。 触发服务器产生一个不可屏蔽中断。 该功能主要在服务器操作系统异常的情况下使用。在服务器操作系统正常运行期间请勿使用。
屏蔽面板电源按钮	开启本功能后服务器面板上的电源按钮将失效。 单击  或  并根据提示保存，可切换状态。 默认状态:  ●  表示此功能已开启，此时电源按钮已失效。 ●  表示此功能已关闭，此时电源按钮处于激活状态，可控制服务器上下电。
通电开机策略	服务器整机断电，电源模块通电后，服务器的开机策略包括： ● 保持上电：服务器的电源模块通电后服务器自动开机。 ● 保持下电：服务器的电源模块通电后服务器不上电。 ● 与之前保持一致：服务器的电源模块通电后保持断电前状态。 – 如果断电前服务器是开机状态，则通电后服务器自动开机。 – 如果断电前服务器是关机状态，则通电后服务器不上电。 默认为“保持上电”。

参数	描述
延迟上电设置	在前级供电设备通断电从而引起大批量服务器同时上电时，瞬间的上电峰值电流过大会对供电设备产生冲击。为避免这种情况导致的设备故障，可设置服务器延迟上电，以减小上电峰值电流，降低设备损害风险。 服务器延迟上电设置生效需同时满足以下条件： ● 通电开机策略为上电状态。 ● 受控上电开关为关闭状态。 服务器的延迟上电模式包括： ● 默认延迟：按照槽位延迟， N槽位延迟时长为N×0.5。通电后按照N×0.5延迟上电。 ● 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延迟上电。 取值范围为0 ~ 120，精度为0.1，单位为秒。 ● 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上电。 取值范围为0 ~ 120，精度为0.1，单位为秒。 ● 随机延迟： 0 ~ M秒内随机延迟，延迟上限为M秒。通电后在0 ~ M秒内随机延迟上电。 取值范围为0 ~ 120，精度为0.1，单位为秒。

操作步骤

表 3-19 电源&功率操作步骤

操作	操作步骤
设置电源模块工作模式	1. 在“电源信息”页签，单击右上角的“电源设置”。 2. 根据实际情况，设置电源模块的工作模式。 3. (可选)当工作模式为主备供电时，设置主用电源模块。 4. (可选)单击  使之变为  ，开启深度休眠功能。 **说明** ● 开启深度休眠，服务器下电后，进入深度休眠模式的电源会关闭输出；关闭深度休眠或服务器上电后，进入深度休眠模式的电源会恢复输出。 ● 开启深度休眠模式，服务器下电后，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。 5. 单击“保存”。

操作	操作步骤
为服务器上电	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“上电”按钮。 弹出对话框提示以下信息： 是否确认执行该操作? 2. 单击“确定”。 服务器开始上电。服务器上电的时间根据服务器的配置不同。操作完成后界面将显示“操作成功”提示信息。 服务器成功上电后，“系统状态”显示为“上电”。
将服务器正常下电	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“下电”按钮。 弹出对话框提示以下信息： 是否确认执行该操作? 2. 单击“确定”。 服务器开始正常下电。 操作完成后“电源&功率”界面将显示“操作成功”提示信息。 服务器成功正常下电后，“系统状态”显示为“下电”。
将服务器强制下电	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“强制下电”按钮。 弹出对话框提示以下信息： 确定要进行强制下电操作吗？强制下电可能会损坏用户的程序或者未保存的数据! 2. 单击“确定”。 服务器开始强制下电。操作完成后“电源&功率”界面将显示“操作成功”提示信息。 服务器成功强制下电后，“系统状态”显示为“下电”。
强制重启服务器	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“强制重启”按钮。 弹出对话框提示以下信息： 确定要进行强制重启操作吗？强制重启可能会损坏用户的程序或者未保存的数据! 2. 单击“确定”。 服务器开始强制重启。服务器强制重启的时间根据服务器配置所不同。操作完成后“电源&功率”界面将显示“操作成功”提示信息。
强制下电再上电	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“强制下电再上电”按钮。 弹出对话框提示以下信息： 确定要进行强制下电再上电操作吗？强制下电再上电可能会损坏用户的程序或者未保存的数据! 2. 单击“确定”。 服务器开始强制下电再上电。服务器强制下电再上电的时间根据服务器配置所不同。操作完成后“电源&功率”界面将显示“操作成功”提示信息。 服务器成功强制下电再上电后，“系统状态”由“上电”变为“下电”，最后显示为“上电”。

操作	操作步骤
触发NMI	**须知** 该功能主要在无法再使用操作系统的情况下使用。在服务器正常运行期间，不应使用此功能，否则可能造成系统崩溃。 1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“NMI”按钮。 弹出对话框提示以下信息： 确定要进行NMI操作吗？ NMI会向操作系统发送不可屏蔽中断可能导致数据丢失和数据损坏！ 2. 单击“确定”。 服务器产生一个不可屏蔽中断。操作完成后“电源&功率”界面将显示“操作成功”提示信息。
设置通电开机策略	1. 在“服务器上下电”页签，设置服务器的通电开关机策略。 2. 单击“保存”。 显示“操作成功”表示成功设置开关机策略。
设置下电时限	1. 在“服务器上下电”页签，勾选“下电时限”左侧的复选框。 2. 单击 输入超时时长。 不同产品取值范围不相同，以界面提示为准。 3. 单击 保存设置。 显示“操作成功”表示成功设置下电时限。
查看下电时限	在“服务器上下电”页签的“虚拟按键”区域中，查看下电时限。
设置延迟上电	1. 在“服务器上下电”页签，在“延迟上电设置”区域框选中延迟上电模式前方的单选框。 2. 单击 输入延迟时长。 延迟时间的取值范围为0 ~ 120，精度为0.1，单位为秒。默认延迟模式不支持设置延迟时长。 3. 单击 ，保存延迟时间设置。 4. 单击“保存”完成设置。 显示“操作成功”表示成功设置延迟上电。 **说明** 单击“保存”后， 3中设置的延迟时长将同步到另外两种可设置延迟时长的模式。

3.4.5 风扇&散热

功能介绍

通过使用风扇&散热界面的功能，您可以:

- 查看服务器进风口温度历史数据。

- 实现对服务器调速方式的查询和设置。

  说明

  当服务器风扇调速模式为手动调速模式时，在“智能调速”区域框中所作的配置不立即生效。当风扇调速模式切换为自动调速模式后，之前的配置才能生效。

- 查看服务器的在位风扇信息。

界面描述

在导航栏中选择“系统管理 > 风扇&散热”，打开如图3-23所示界面。

图 3-23 风扇&散热(以 2288H V6-32DIMM 为例)

参数描述

表 3-20 进风口温度

参数	描述
进风口温度	本服务器最近一周的进风口温度变化(每10分钟采样一次)。
当前值	显示进风口传感器最近一次检测到的温度值。
清空	单击“清空”可以清除历史数据。
刷新	单击“刷新”可以更新当前统计的数据。

表 3-21 风扇模块

参数	描述
基本信息	显示服务器在位风扇模块的基本信息，包括风扇模块槽位号、名称、型号、转速、速率比以及部件编码。

表 3-22 智能调速

参数	描述
节能模式	风冷系统默认的调速模式，评估系统当前负载及散热情况，将风扇转速控制在一个平衡点，使系统功耗达到最低。
低噪声模式	在满足散热需求的前提下，使风扇转速降至最低，降低噪声。
高性能模式	提高风扇转速，保证关键部件散热能力，使其保持较低温度，使服务器系统整体性能达到最高。
自定义模式	提供自定义接口，用户可自行设置CPU目标温度、出风口目标调速温度以及进风口各温度区域对应的风扇转速。 ● “CPU目标调速温度值”、“出风口目标调速温度值”及“温度区间对应转速值”为“用户自定义模式”下的可配置参数，其他模式下无法查看和配置此参数。 ● 设置“CPU目标调速温度值”、“出风口目标调速温度值”及“温度区间对应转速值”时，服务器会根据当前负载及散热情况，提示可设置的取值范围。请根据提示信息设置。 ● 较高温度区间对应的转速值必须大于较低温度区间对应的转速值。 **说明** ● 用户自定义模式下，不同服务器支持的参数不同，请以界面实际显示情况为准。 ● 如果任一实际温度值高于设置的目标调速温度值， iBMC将提高风扇转速以降低温度；如果所有实际温度值都低于设置的目标调速温度值， iBMC将根据“温度区间对应转速值”调节风扇转速。 ● 在CPU更换场景下，如果新CPU所允许设置的最高目标调速温度值低于当前设置的“CPU目标调速温度值”时， iBMC自动将“CPU目标调速温度值”修改为新CPU允许设置的最大温度值。

设置智能调速模式

下面以设置“自定义模式”为例说明智能调速的操作方法。

说明

设置为用户自定义模式可能导致散热能力不足，请谨慎选择。

步骤1 单击页面右上角的“智能调速”。

步骤2 选择“自定义模式”。

步骤3 在“CPU目标调速温度值”、“出风口目标调速温度值”的文本框中，根据提示信息，输入想要调节的目标温度。

步骤4 在“温度区间对应转速值”的文本框中输入各个进风口温度区域下想要实现的风扇转速。

步骤5 单击“确定”。

提示操作成功。

----结束

3.4.6 BIOS 配置

功能介绍

通过使用“BIOS配置”界面的功能，您可以：

- 设置操作系统第一选择从哪种设备进行启动。
- 设置服务器的节能策略。
  提供两种系统能耗控制方法：
  – P-State：通过调整CPU工作频率的方式调整系统能耗。
  – T-State：通过调整CPU工作时间占空比的方式调整系统能耗。
  不同类型CPU支持的P-State和T-State的可选状态数量不同。

界面描述

在导航栏中选择“系统管理 > BIOS配置”，打开如**图3-24**、**图3-25**所示界面。

图 3-24 系统启动项

图 3-25 CPU 调节

参数说明

表 3-23 启动项配置

参数	描述
支持IPMI设置启动模式	● 开启：表示支持通过IPMI接口设置BIOS启动模式。 ● 关闭：表示不支持通过IPMI接口设置BIOS启动模式。 **说明** 普通用户不支持此特性。
启动模式	● 传统BIOS： BIOS从legacy模式启动。 ● 统一可扩展固件接口(UEFI)： BIOS从UEFI模式启动。
优先引导介质	● 硬盘：表示强制从硬盘启动系统。 ● 光驱：表示强制从CD/DVD启动系统。 ● 软驱/可拔插移动设备：表示强制从软驱或可拔插移动设备启动系统。 ● PXE ：表示强制从预启动执行环境(PXE ， Pre-boot Execution Environment)启动系统。 ● BIOS设置：表示服务器启动后直接进入BIOS菜单中。 ● 未配置：表示不设置第一启动设备，按BIOS中设置的方式启动操作系统。 ● 单次有效：优先引导介质的设置仅在下一次重启时生效，重启完成后，优先引导介质自动恢复为“未配置”。 ● 永久有效：优先引导介质的设置永久有效。

参数	描述
启动顺序	“优先引导介质”为“未设置”时，按照“启动顺序”中的启动方式启动OS系统。 单击▲表示上移，单击▼表示下移。 默认启动顺序为： ● 硬盘设备 ● 光盘装置 ● PXE ● 其他 **说明** ● 在BIOS侧，设置启动顺序后立即生效。重启OS将触发iBMC启动顺序与BIOS侧启动顺序同步。 ● 在iBMC侧，设置启动顺序后重启OS生效。重启OS将触发BIOS启动顺序与iBMC侧启动顺序同步。

表 3-24 CPU 调节

参数	描述
须知 节能策略可能会影响系统性能，请根据实际情况谨慎使用。 使用本功能前，需要进入BIOS菜单： ● 将“EIST Support”(部分产品此参数显示为“EIST”或“SpeedStep”)设置为“Enabled”。 ● 将“Software Controlled T-States”设置为“Enabled”， Purley平台下，“T-State Throttle Level”建议保持默认值，默认值为“Disabled”。 Whitley平台下，将“T-State Throttle Level”设置成有效值。	
调节CPU的最高工作频率	通过调整CPU的最高工作频率的方式调整系统能耗。不同类型CPU支持的P-State节能策略的状态数量不同。 ● 设置为P0状态时， CPU最高频率为当前支持的最大值。 ● 设置为P1 、P2 、P3等状态时， CPU最高频率依次递减，功耗和性能也随之递减。 **说明** 当功率封顶使能时，在手动设置P-State/T-State状态值后，如果电源实时功率值超过功率封顶值，会导致手动设置的P-State/T-State状态值失效， P-State/T-State会自动调节至正常值。

参数	描述
调节CPU的空闲工作时间	通过调整CPU工作时间占空比的方式调整系统能耗。不同类型CPU支持的T-State节能策略的状态数量不同。 ● 设置为T0状态时， CPU工作时间占空比为当前支持的最大值。 ● 设置为T1 、T2 、T3等状态时， CPU工作时间占空比依次递减，功耗和性能也随之递减。 **说明** ● 当功率封顶使能时，如果手动设置P-State/T-State状态值后，电源实时功率值超过功率封顶值，手动设置的P-State/T-State状态值就会失效， P-State/T-State会自动调节至正常值。 ● 因内核版本过低， CenOS 7系列和Redhat 7系列的OS不支持该功能。

设置系统启动项

步骤1 在“系统启动项”页签中，根据**表3-23**提供的参数信息，设置操作系统的第一启动设备。

步骤2 单击“保存”。

显示“保存成功”表示设置成功。

----结束

CPU 节能设置

步骤1 在“CPU调节”页签中，根据**表3-24**提供的参数信息，拖动节能策略下方的游标选择节能状态。

说明

- 设置时请只选择其中一种策略。
- 与调节CPU的空闲工作时间策略相比，调节CPU的最高工作频率策略对系统能耗的调整幅度更大，同时对系统性能的影响较小。建议您首先使用调节CPU的最高工作频率对系统能耗进行调整。

步骤2 单击“保存”。

显示“保存成功”表示设置成功。

----结束

3.5 维护诊断

3.5.1 告警&事件

功能介绍

通过“告警&事件”界面，您可以：

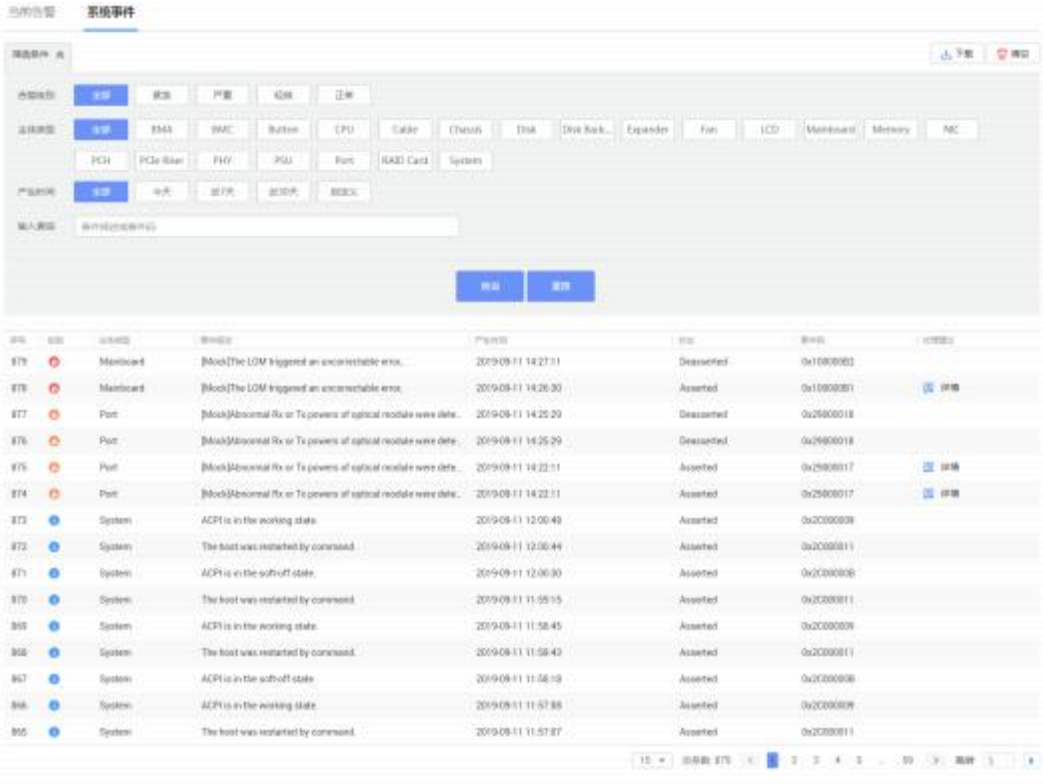
- 查看设备当前未处理的告警。
- 查看和搜索服务器产生的各种系统事件，也可以下载和清除所有系统事件。

界面描述

在导航栏中选择“维护诊断 > 告警&事件”，打开如图3-26和图3-27所示界面。

图 3-26 当前告警

图 3-27 系统事件



参数说明

表 3-25 告警&事件

参数	描述
序号	事件的排序。

参数	描述
级别	事件的级别。 ●  ：表示紧急告警，可能会使设备下电、系统中断。因此需要您马上采取相应的措施进行处理。 ●  ：表示严重告警，会对系统产生较大的影响，有可能中断系统的正常运行，导致业务中断。 ●  ：表示轻微告警，不会对系统产生大的影响，但需要您尽快采取相应的措施，防止故障升级。 ●  ：表示正常事件，系统的正常运行记录。
主体类型	产生系统事件的部件类型。
事件描述	系统事件的描述信息。
产生时间	系统事件的产生时间。
状态	系统事件的状态。 取值范围： ● Asserted：表示系统事件已产生。 ● Deasserted：表示系统事件已恢复。
事件码	系统事件管理软件系统中的唯一标识。
处理建议	对故障类事件的简要处理建议。 单击  查看事件的处理建议。

搜索系统事件

步骤1 在“告警&事件”页面单击“系统事件”页签。

步骤2 单击“筛选条件”。

打开筛选条件设置区域。

步骤3 根据**表3-26**提供的参数信息，设置筛选条件。

表 3-26 搜索条件说明

参数	描述
告警级别	系统事件的级别。 取值范围： ● 全部 ● 紧急 ● 严重 ● 轻微 ● 正常
主体类型	产生系统事件的部件类型。 取值范围：不同服务器的事件源不同，以实际情况为准。
产生时间	产生系统事件的时间。 取值范围： ● 全部 ● 今天 ● 近7天 ● 近30天 ● 自定义 **说明** 当选择“自定义”时，需要在弹出的输入框中设置起止时间。
输入查询	系统事件的描述信息或事件码。 您可以在“输入查询”右侧的文本框中输入以下内容： ● 事件描述中任意连续的字符串。 ● 完整的事件码，可带“0x”或不带“0x”。

步骤4 单击“查询”。

页面将显示符合筛选条件的事件列表。

----结束

清除所有系统事件

须知

系统不能恢复被清除的系统事件，请谨慎操作。

步骤1 在“告警&事件”页面单击“系统事件”页签。

步骤2 单击页面右上角的“清空”。

将清除所有系统事件。

----结束

下载所有系统事件

步骤1 在“告警&事件”页面单击“系统事件”页签。

步骤2 单击页面右上角的“下载”。

下载的文件将自动保存到本地PC的自定义路径。

----结束

3.5.2 告警上报

功能介绍

通过使用“告警上报”界面的功能，您可以：

- 设置iBMC系统向第三方服务器以Syslog报文方式发送日志。
- 将服务器产生的告警和事件以电子邮件方式发送到目标邮箱。带有告警和事件信息的电子邮件通过SMTP服务器转发到目标邮箱，从而通知用户。
- 设置iBMC系统向第三方服务器以Trap报文方式发送告警信息、事件信息以及Trap属性。

  说明

  Trap是系统主动向第三方服务器发送的不经请求的信息，用于报告紧急告警、严重告警、轻微告警和正常事件。

界面描述

在导航栏中选择“维护诊断 > 告警上报”，打开如图3-28 、图3-29和图3-30所示界面。

图 3-28 Syslog 报文通知

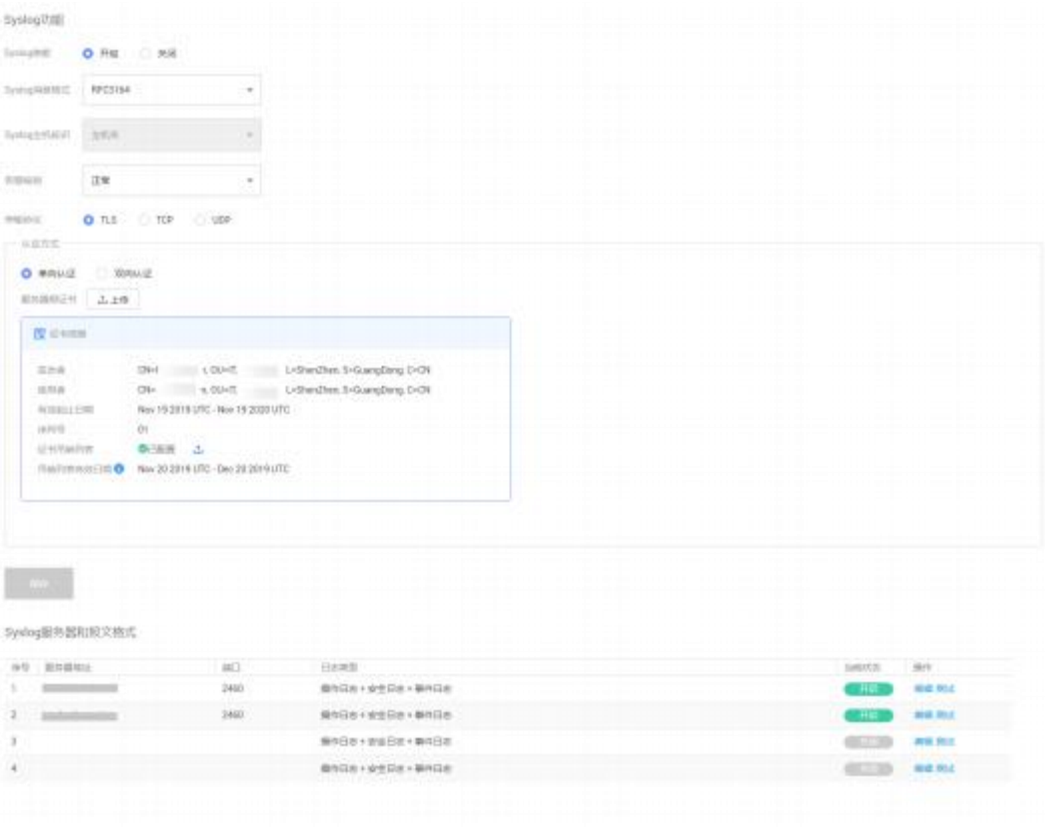


图 3-29 邮件通知

图 3-30 Trap 报文通知

参数说明

表 3-27 Syslog 报文通知

参数	描述
Syslog使能	设置开启或关闭自动上报Syslog报文。
Syslog消息格式	选择Syslog报文上报信息的格式。 ● 自定义： Syslog报文上报的信息包括Syslog消息的优先级、产品名称、 Syslog主机标识、设备位置以及日志类型。 ● RFC3164：Syslog报文消息的格式遵循RFC3164规范，上报的信息包括Syslog消息的优先级、时间戳、主机名称、进程名称以及日志类型。 **说明**
Syslog主机标识	Syslog信息上报时，用于标识信息来源。 取值范围： ● 单板序列号 ● 产品资产标签 ● 主机名
告警级别	以Syslog方式上报给第三方服务器的事件信息级别。 取值范围： ● [NULL]：不发送告警信息或正常事件信息。 ● 紧急：仅发送紧急级别的告警信息。 ● 严重：发送包括严重、紧急级别的告警信息。 ● 轻微：发送包括轻微、严重、紧急级别的告警信息。 ● 正常：发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。

参数	描述
传输协议	Syslog报文在iBMC系统和Syslog服务器之间传输时，使用的传输协议。 取值范围： ● TLS：面向连接的协议，并保证数据传输的保密性和数据完整性。 ● TCP：面向连接的协议，在正式收发数据前，必须在收发方建立可靠的连接。 ● UDP：面向非连接的协议，在正式收发数据前，收发方不建立连接，直接传输正式的数据。
认证方式	“传输协议”选择“TLS”时，采用的认证方式。 取值范围： ● 单向认证：只认证Syslog服务器端的证书。 ● 双向认证： Syslog服务器端和客户端的证书都需要认证。 **说明** MD5和SHA1为不安全的弱签名算法， iBMC不支持导入弱签名算法(MD5和SHA1)客户端证书。
服务器根证书	在建立数据连接时，使用此处上传的服务器根证书对Syslog服务器发送来的报文进行验证。 **说明** 请定期更新证书，否则可能存在安全风险。
证书信息	显示上传的服务器根证书信息，包括： ● 使用者 ● 签发者 ● 有效期 ● 序列号 ● 证书吊销列表 ● 吊销列表有效日期 **说明** ● 证书吊销列表表示证书吊销的状态： ● 已配置：表示该证书的吊销文件已上传，在TLS连接时，会进行证书吊销校验。 ● 未配置：表示该证书的吊销文件未上传。 ● 证书吊销文件的格式为“*.crl”，编码格式为Base64，最大不超过100KB。 ● 吊销列表过期会导致相应的认证功能失败。 证书吊销列表设置方法：单击 选择客户端保存的证书吊销文件。
保存	保存Syslog功能区域参数的修改。
取消	取消Syslog功能区域参数的修改。
Syslog服务器和报文格式	

参数	描述
序号	Syslog报文发送通道。您最多可以定义四个通道。
服务器地址	Syslog服务器地址信息。 取值范围：可设置为IPv4 、IPv6 、域名。 **说明** ● 当“传输协议”选择“TLS”的时候，此处必须使用域名地址。使用域名地址的时候，必须在“iBMC配置 > 网络配置”页面配置正确的DNS信息。 ● 域名的取值原则： ● 最大长度为255个字符。 ● 可由数字、大小写英文字母和连接号(-)，点号(.)组成。 ● 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 ● 任意两个点号之间的字符长度不允许超过63。
端口	Syslog服务器的端口号。 取值范围： 1 ~ 65535
日志类型	需要使用Syslog报文上报的日志类型。 取值范围：您可以勾选“操作日志”、“安全日志”或“事件日志”中的一项或多项。
当前状态	设置某个通道的启用状态。
操作	● 单击“编辑”， Syslog服务器和报文格式处于可编辑状态。 ● 单击“测试”，可以测试已设置的Syslog通道是否可用。显示“操作成功”表示该通道可用。 **说明** 如果修改了“Syslog功能”区域的参数，请务必单击“Syslog功能”区域的“保存”按钮后再进行测试，否则修改后的参数不能生效。

表 3-28 邮件通知

参数	描述
SMTP使能	设置开启或关闭SMTP服务。
SMTP服务器地址	SMTP服务器的IPv4 、IPv6地址或域名。 域名的取值原则： ● 最大长度为255个字符。 ● 可由数字、大小写英文字母和连接号(-)，点号(.)组成。 ● 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 ● 任意两个点号之间的字符长度不允许超过63。

参数	描述
是否启用TLS	设置启用TLS (Transport Layer Security)加密传输。 不启用TLS时，采用明文传输。 **说明** ● 默认情况下， SMTP支持TLS加密，从安全性考虑，请尽量不要关闭TLS加密。 ● 启用TLS加密时， SMTP服务器需要配置身份验证，配置支持TLS后，才能接收到邮件。
是否使用匿名	匿名是指通过SMTP服务器转发告警电子邮件时不需要验证用户名及其密码。 匿名认证功能需要SMTP服务器支持匿名登录。 不匿名时，认证方式为非匿名认证。非匿名认证需要输入已在SMTP服务器上注册的用户名和密码。该用户名和密码用于iBMC系统向SMTP服务器发送告警信息邮件时使用。 **说明** 默认情况下， SMTP服务器不使用匿名，从安全性考虑，请尽量不要使用匿名。
发件人用户名及密码	通过邮箱发送告警信息时使用的发件人用户名和密码。 用户名可以由数字、英文字母或特殊字符中的1种或几种组成，且不能为空。 密码为该用户在对应SMTP服务器上的用户密码。 取值范围： ● 用户名必须是长度为1 ~ 64之间字符串。 ● 密码必须是长度为1 ~ 50之间的字符串。 **说明** 停用SMTP功能时，发件人用户名和密码可以设置为空。
发件人邮件地址	通过邮箱发送告警信息时使用的邮件地址。 取值范围：最大为255位的字符串。 由英文字母、数字和其他特殊字符组成。格式必须为“*xx@xxx.xx*”。
邮件主题/主题附带	电子邮件的标题。 取值范围： 0 ~ 255位的字符串，由数字、英文字母和特殊字符组成。 在电子邮件标题中可附带关键信息，可以是“主机名”、“单板序列号”或“产品资产标签”。

参数	描述
告警发送级别	通过SMTP服务器发送的告警信息的级别。 取值范围： ● [NULL]：不发送告警信息或正常事件信息。 ● 紧急：仅发送紧急级别的告警信息。 ● 严重：发送包括严重、紧急级别的告警信息。 ● 轻微：发送包括轻微、严重、紧急级别的告警信息。 ● 正常：发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。
保存	保存SMTP功能区域参数的修改。
取消	取消SMTP功能区域参数的修改。
邮件地址	接收电子邮件的邮箱地址。该地址必须已在SMTP服务器上进行了注册。 取值范围：最大为255位的字符串，格式必须为“*xx@xxx.xx*”。 由英文字母、数字和其他特殊字符组成。
描述	对接收电子邮件的邮箱的相关描述。 取值范围： 0 ~ 255位的字符串，由数字、英文字母和特殊字符组成。
发送邮件	设置iBMC是否向该接收地址发送邮件。
操作	● 单击“编辑”，接收告警的邮件地址处于可编辑状态。 ● 单击“测试”，可以测试已设置的目标邮箱地址是否可达。 **说明** 如果修改了“SMTP功能”区域的参数，请务必单击“SMTP功能”区域的“保存”按钮后再进行测试，否则修改后的参数不能生效。

表 3-29 Trap 报文通知

参数	描述
Trap使能	设置开启或关闭自动上报Trap报文。

参数	描述
Trap版本	以Trap方式上报事件需遵循的SNMP Trap协议版本。 取值范围： ● “SNMPv1”： SNMP Trap协议的V1版本是简单网络管理协议的第一个正式版本，在RFC（Request For Comments) 1157中定义。 ● “SNMPv2c”： V2C版本是针对V2的改进版。 SNMP Trap协议的V2C版本是基于共同体(Community-Based)的管理架构，在RFC1901中定义的一个实验性协议。 ● “SNMPv3”： SNMP协议的V3版本由RFC 3411-RFC 3418定义，主要在安全性和远程配置方面进行强化。 **说明** ● “SNMPv1”和“SNMPv2c”版本由于自身机制而存在安全隐患，请尽量避免使用。建议使用“SNMPv3”版本的SNMP Trap。 ● “SNMPv3”的鉴权算法和加密算法可在“用户&安全 > 本地用户”中设置。 默认取值：“SNMPv3”。
选择V3用户	Trap版本选择“SNMPv3”时，需要同时设置协议所需的用户名。 默认情况下，使用iBMC提供的默认用户作为TrapV3用户。
Trap模式	Trap信息上报时采用的模式。 取值范围： ● “精准告警模式(推荐)”：以与事件一一对应的SNMP节点OID作为Trap事件的标识，相较“OID模式”和“事件码模式”，可提供更为精准的定位信息。 ● “OID模式”：以SNMP节点的OID作为Trap事件的标识。 ● “事件码模式”：以产生事件的事件码作为Trap事件的标识。 默认取值：“精准告警模式(推荐)”
Trap主机标识	Trap信息上报时，用于标识信息来源。 取值范围： ● 单板序列号 ● 产品资产标签 ● 主机名

参数	描述
团体名	团体名为Trap方式的口令。“版本”设置为“SNMPv1”或“SNMPv2c”时才能设置“团体名”。 ● 关闭密码检查时的取值原则： 1 ~ 18位的字符串，由数字、英文字母和除空格外的特殊字符组成。 ● 开启密码检查时的取值原则： – 长度为8 ~ 18位的字符。 – 至少包含以下字符中的两种： – 大写字母： A ~ Z – 小写字母： a ~ z – 数字： 0 ~ 9 – 至少包含以下特殊字符： `~!@#$%^&*()-_=+\|[{}];:'",<.>/? – 新旧团体名至少在2个字符位上不同。 – 不能包含空格。 默认取值： “TrapAdmin12#$”
确认团体名	此处输入的内容需要与“团体名”中相同。
告警发送级别	以Trap方式上报给第三方服务器的事件信息级别。 取值范围： ● [NULL]：不发送告警信息或正常事件信息。 ● 紧急：仅发送紧急级别的告警信息。 ● 严重：发送包括严重、紧急级别的告警信息。 ● 轻微：发送包括轻微、严重、紧急级别的告警信息。 ● 正常：发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。
保存	保存Trap功能区域参数的修改。
取消	取消Trap功能区域参数的修改。
序号	自定义以Trap发送告警的通道。您最多可以定义四个通道。
Trap服务器地址	接收Trap方式发送的告警信息的服务器地址。服务器地址支持IPv4 、IPv6和域名。 域名的取值原则： ● 最大长度为255个字符。 ● 可由数字、大小写英文字母和连接号(-)，点号(.)组成。 ● 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 ● 任意两个点号之间的字符长度不允许超过63。

参数	描述
Trap端口	接收Trap方式发送的告警信息的端口号。 取值范围： 1 ~ 65535之间的数字。 默认取值： 162。 **说明** 单击“恢复默认值”，接收Trap端口号改为默认的“162”。
带内转发	设置开启或关闭Trap信息带内转发。带内转发功能指将Trap信息通过OS侧转发至Trap服务器。 **说明** ● 当iBMC无法连接到Trap服务器时，若此时服务器OS可与Trap服务器连通，则可启用带内转发，将Trap信息通过OS侧转发至Trap服务器。 ● 需在服务器OS侧安装iBMA 2.0并完全启动后，才能使通道处于可用状态。
当前状态	设置启用某个通道的启用状态。
报文分隔符	选择Trap格式中每个关键字段之间的分隔符，例如“;”。 **说明** 仅在“事件码模式”下可设置此参数。
报文显示内容	选择需要上报的关键字。 **说明** 仅在“事件码模式”下可设置此参数。
显示关键字	显示Trap格式中每个关键字的名称。 **说明** 仅在“事件码模式”下可设置此参数。
样例	根据您选择的分隔符、显示内容以及显示的关键字名称给出示例。
操作	● 单击“编辑”， Trap服务器和报文格式处于可编辑状态。 ● 单击“测试”，可以测试已设置的Trap通道是否可用。显示“操作成功”表示该通道可用。 **说明** 如果修改了“Trap功能”区域的参数，请务必单击“Trap功能”区域的“保存”按钮后再进行测试，否则修改后的参数不能生效。

3.5.3 FDM PFAE

功能介绍

FDM（Fault Diagnose Management)提供覆盖整个系统的全自动故障处理能力，包括故障数据收集、故障数据分析、故障诊断定位等。

在日常维护中，可在界面中查看到FDM分析诊断出来的故障部件信息，以及与此相关的历史事件。您可依据此分析对故障设备做出处理。

在使用FDM故障诊断功能前，请确认已在BIOS中开启FDM功能。

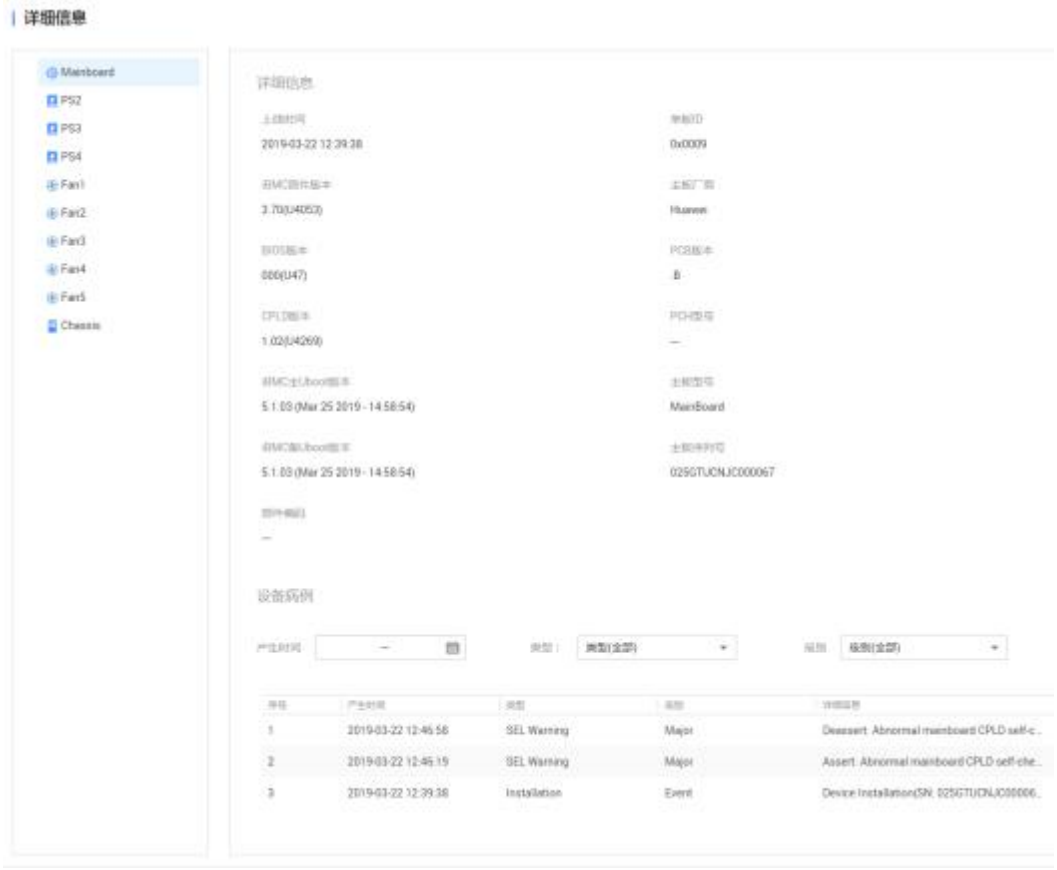
说明

在Whitley平台的BIOS中， FDM开关的路径为“Advanced > System Event Log > FDM ”。

界面描述

在导航栏中选择“维护诊断 >FDM PFAE ”，打开如图3-31所示界面。

图 3-31 FDM PFAE



参数说明

表 3-30 FDM PFAE

参数	描述
详细信息	所选择设备的详细信息。 ● CPU基本信息包括：名称、上线时间、使能状态、厂商、核数/线程数、型号、一级/二级/三级缓存、处理器ID、部件编码、主频、 PPIN以及其他参数。 ● 主板基本信息包括：上线时间、 iBMC固件版本、单板ID 、BIOS版本、主板厂商、 CPLD版本、 PCB版本、 iBMC主Uboot版本、 PCH型号、 iBMC备Uboot版本、主板型号、部件编码以及主板序列号。 ● 内存基本信息包括：名称、上线时间、序列号、厂商、类型、位置、最小电压、容量、部件编码、主频、 RANK列以及其他参数。 ● 网卡基本信息包括：名称、上线时间、厂商、型号、 PCB版本、单板ID 、芯片厂商以及芯片型号。 ● RAID卡基本信息包括：名称、上线时间、 RAID级别、位置、 PCB版本、厂商、 CPLD版本、编号、单板ID 、类型以及资源归属。 ● 电源基本信息包括：上线时间、槽位、固件版本、厂商、额定功率、类型、输入模式、序列号以及部件编码。 ● 风扇基本信息包括：名称、上线时间、转速值、型号、速率比以及部件编码。 ● 硬盘背板基本信息包括：上线时间、位置、 PCB版本、厂商、 CPLD版本、编号、单板ID以及类型。 ● 硬盘基本信息包括：上线时间、接口类型、型号、厂商、固件版本、序列号、温度、介质类型、 SAS地址、容量、支持的速率、协商速率、电源状态、巡视状态、热备状态、固件状态、定位状态、累计通电时间、剩余磨损率、重构状态、资源归属以及部件编码。 ● PCIe卡基本信息包括：上线时间、描述、厂商、槽位、制造商ID、设备ID、子厂商ID、子设备ID以及资源归属。 ● 机箱基本信息包括：名称以及上线时间。 **说明** ● 剩余磨损率表示SSD硬盘的使用寿命。剩余磨损率越大，表示硬盘的损耗越小，使用寿命越长；剩余磨损率越小，表示硬盘的损耗越大，使用寿命越短。例如剩余磨损率为100%，表示硬盘没有损耗。 ● 上线时间表示设备首次在服务器安装上电并被iBMC识别为新设备的时间。
设备病例	影响该设备健康的历史相关事件。
产生时间	事件的产生时间。

参数	描述
类型	事件的类型。 ● FDM Warning： FDM告警事件 ● SEL Warning：系统事件 ● Installation：部件安装事件
级别	事件的级别： ● 事件日志 ● 轻微告警 ● 严重告警 ● 紧急告警
详细信息	事件的具体描述。
查询	根据需要选择“产生时间”、“类型”以及“级别”后，可以查询到符合条件的事件。

3.5.4 录像截屏

功能介绍

通过使用“录像播放”功能，您可以：

- 启用或禁用录像功能。
  启用时， iBMC将自动录制CPU出错、关机和重启录像。
- 播放本地PC上存放的服务器实时桌面的录像文件。
- 播放服务器自动录制的录像文件。
- 播放录像文件时，对某时刻的录像文件进行截图。

说明

- 播放的录像文件格式为“*.rep”。
- 截取的图像格式为“*.jpg”。
- 开启录像功能后，自动录像功能有可能录制到业务侧的敏感信息，请注意安全风险。

通过使用“屏幕截图”功能，您可以：

- 启用或禁用最后一屏功能。
  启用时，在服务器重启或下电时，自动保存屏幕最后的显示信息。
- 随时对实时桌面进行屏幕截图。

说明

“最后一屏使能”默认为开启状态。开启最后一屏功能后，自动截屏功能可能会录制到业务侧的敏感信息，请注意安全风险。

录像回放控制窗口中的按钮及其作用如表3-31所示。

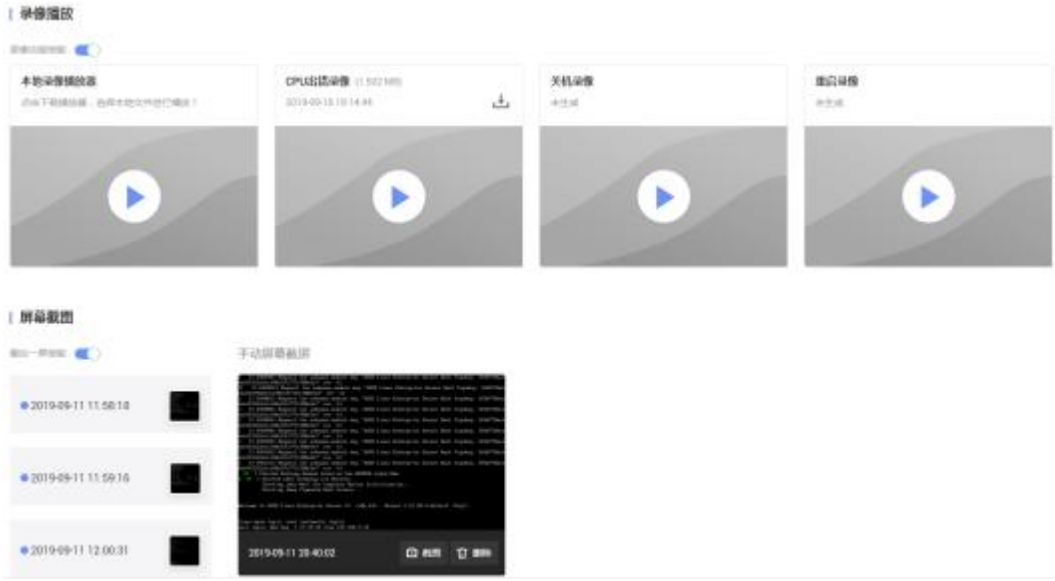
表 3-31 录像回放控制窗口按钮说明

按钮	说明
	“播放”按钮。表示开始播放录像文件。
	“暂停”按钮。表示暂停录像文件的播放。
	“快进”按钮。表示加速播放录像文件。播放速度可以选择1倍、 2倍或4倍。
	“慢进”按钮。表示减速播放录像文件。播放速度可以选择1倍、 0.5倍或0.25倍。
	“全屏”按钮。表示最大化显示录像回放控制窗口。 **说明** 在全屏或满屏播放录像文件时，单击右键可以弹出快捷菜单。
	“打开”按钮。表示导入“*.rep”格式的录像文件。 本地播放录像时才能使用本功能。
	“截屏”按钮。表示截取录像文件中的某一帧画面。
	播放进度条。表示录像文件的播放进度。
	“循环”按钮。表示循环播放录像文件。 本地播放录像时才能使用本功能。

界面描述

在导航栏中选择“维护诊断 > 录像截屏”，打开如图3-32所示界面。

图 3-32 录像截屏



操作步骤

表 3-32 录像播放功能操作步骤

操作	操作步骤
录像功能使能	开启或关闭录像功能。 单击 或 并根据提示保存，可切换状态。 ● 表示开启录像功能。 ● 表示关闭录像功能。
下载Java播放器	1. 单击。 2. 单击“Java播放器”。 3. 根据页面提示信息保存文件。 将自动保存播放器文件到本地PC的默认路径。播放器文件的格式为“.jnlp”。 **说明** HTML5播放器可以直接使用，不需要下载。
下载录像	单击“CPU出错录像”、“关机录像”或“重启录像”右侧的，将下载录像文件，并自动保存到本地PC的默认路径。
播放本地录像文件	1. 选择以下任意一种播放器播放本地录像文件： ● 打开“本地录像播放器”区域框中的HTML5播放器。 ● 打开从“本地录像播放器”区域框中下载的Java播放器。 2. 在播放器中，单击，选择本地PC上存放的录像文件。 3. 单击“打开”。 将返回播放器窗口并开始播放该录像文件。 4. (可选)根据实际需要调整录像播放状态。 ● 单击，以正常速度的 1倍、 2倍或4倍快速播放录像文件。 ● 单击，以正常速度的 1倍、 0.5倍或0.25倍缓慢播放录像文件。 ● 向左或向右拖动，控制录像文件的播放进度。 ● 单击。 系统循环播放该录像文件。 ● 单击。 播放器窗口最大化显示在屏幕上。

操作	操作步骤
播放在线录像文件	1. 选择以下任意一种播放器播放在线录像文件： ● 打开“CPU出错录像”、“关机录像”或“重启录像”区域框中的HTML5播放器。 ● 打开从“CPU出错录像”、“关机录像”或“重启录像”区域框中下载的Java播放器。 2. (可选)根据实际需要调整录像播放状态。 ● 单击  ，以正常速度的 1倍、 2倍或4倍快速播放录像文件。 ● 单击  ，以正常速度的 1倍、 0.5倍或0.25倍缓慢播放录像文件。 ● 向左或向右拖动  ，控制录像文件的播放进度。 ● 单击  。 播放器窗口最大化显示在屏幕上。
截取录像图像	在录像播放过程中，单击  。 将剪切到的图像保存到客户端，图像格式为“*.jpg”。

表 3-33 屏幕截图功能操作步骤

操作	操作步骤
开启或关闭最后一屏功能	开启或关闭最后一屏功能。 单击  或  并根据提示保存，可切换状态。 ●  表示开启最后一屏功能。 ●  表示关闭最后一屏功能。
查看最后一屏截图	单击“屏幕截图”区域框的缩略图可以查看大图。 左侧的三张小图片显示最近三次服务器重启或者下电前的系统画面。
截取屏幕图	1. 单击“手动屏幕截屏”区域框的“截图”。 弹出确认提示框。 2. 单击“确定”完成截图。 “手动屏幕截屏”区域框中将显示iBMC系统截取的服务器实时桌面的图片。图片左下方显示图片截取时间。 **说明** 对于多次截取的屏幕图，“手动截屏”区域框中只显示最近一次的图片和截取时间。

操作	操作步骤
删除屏幕图	1. 单击“手动屏幕截屏”区域框的“删除”。 弹出确认提示框。 2. 单击“确定”完成删除截图。

3.5.5 系统日志

功能介绍

- 通过使用“黑匣子功能”区域框的功能，您可以启用或关闭黑匣子功能，开启功能时您可以下载黑匣子存储器中的数据到本地。
  黑匣子包含一个存储器和一款故障监控软件：
  - 黑匣子存储器是系统内置的用于故障信息记录的存储芯片。它不依赖于服务器的硬盘。
    黑匣子存储器的最大容量为4MB，用于记录操作系统崩溃时的内核信息。
  - 故障监控软件记录服务器操作系统崩溃时的内核信息。
    在使用黑匣子功能前，服务器上必须已安装黑匣子的故障监控软件(例如iBMA，其安装和使用方法可参考**iBMA 用户指南**)。
  - 在开启黑匣子功能的情况下，如果服务器上未安装黑匣子驱动，则可能在OS侧出现未知设备。
- 通过使用“系统串口数据记录功能”区域框的功能，您可以启用或关闭串口数据下载记录功能，开启功能时您可以下载系统串口最近2MB的数据到本地。

界面描述

在导航栏中选择“维护诊断 > 系统日志”，打开如**图3-33**所示界面。

图 3-33 系统日志

操作步骤

表 3-34 黑匣子功能操作步骤

操作	操作步骤
启用或关闭黑匣子功能	1. 将“黑匣子功能”右侧的按钮设置为  ，表示开启黑匣子功能。将按钮设置为  ，表示关闭黑匣子功能。单击  或  ，可切换状态。 2. 重启服务器。 **说明** • 黑匣子功能默认为开启状态。 • 启用或禁用黑匣子功能都需要重启服务器后才能生效。
下载黑匣子数据文件	请在“黑匣子功能”为  状态下下载黑匣子数据文件。 单击“黑匣子功能”区域框的  。 黑匣子数据文件将自动保存到本地PC的默认地址。 **说明** • iBMC不提供黑匣子数据文件的解析功能。关于黑匣子数据文件的解析功能请参考**iBMA 用户指南**。 • 在不同浏览器下，页面提示保存文件的信息略有不同。

表 3-35 系统串口数据记录功能操作步骤

操作	操作步骤
启用或关闭系统串口数据记录功能	将“系统串口数据记录功能”右侧的按钮设置为  ，表示开启系统串口数据记录功能。将按钮设置为  ，表示关闭系统串口数据记录功能。单击  或  ，可切换状态。 **说明** “系统串口数据记录功能”默认为开启状态。
下载系统串口数据文件	请在“系统串口数据记录功能”为  状态下下载系统串口数据文件。 单击“系统串口数据记录功能”区域框的  。 系统串口数据文件自动保存到本地PC的默认路径。 **说明** • 下载的数据文件为系统串口最近2MB的数据。 • 在不同浏览器下，页面提示保存文件的信息略有不同。

3.5.6 iBMC 日志

功能介绍

- 通过“操作日志”区域框，您可以查看系统启动过程中的信息记录，包括启动信息和状态转移，还可以查看用户对iBMC执行的设置类操作日志，并可下载操作日志。

  iBMC为操作日志提供200KB的存储空间，可记录约2000条操作日志。
  操作日志达到200KB时会自动压缩成1个压缩包，当有新的压缩包生成，会自动删除旧的压缩包。

  说明

  上下电及重启记录的成功操作日志，只表示软件触发动作成功，不代表硬件真正成功。
- 通过“运行日志”区域框，您可以查看服务器RAS相关日志。

  iBMC为运行日志提供200KB的存储空间，可记录约2000条运行日志。
  运行日志达到200KB时会自动压缩成1个压缩包，当有新的压缩包生成，会自动删除旧的压缩包。
- 通过“安全日志”区域框，您可以：
  - 查看用户通过串口、 SSH接口登录、退出iBMC系统以及设置类操作的日志。
  - 查看用户通过SNMP接口执行的查询类和设置类操作的日志。
  - 下载安全日志。

  iBMC为安全日志提供200KB的存储空间，可记录约2000条安全日志。
  安全日志达到200KB时会自动压缩成1个压缩包，当有新的压缩包生成时，会自动删除旧的压缩包。

界面描述

在导航栏中选择“维护诊断 > iBMC日志”，打开如图3-34 、图3-35 、图3-36所示界面。

图 3-34 操作日志

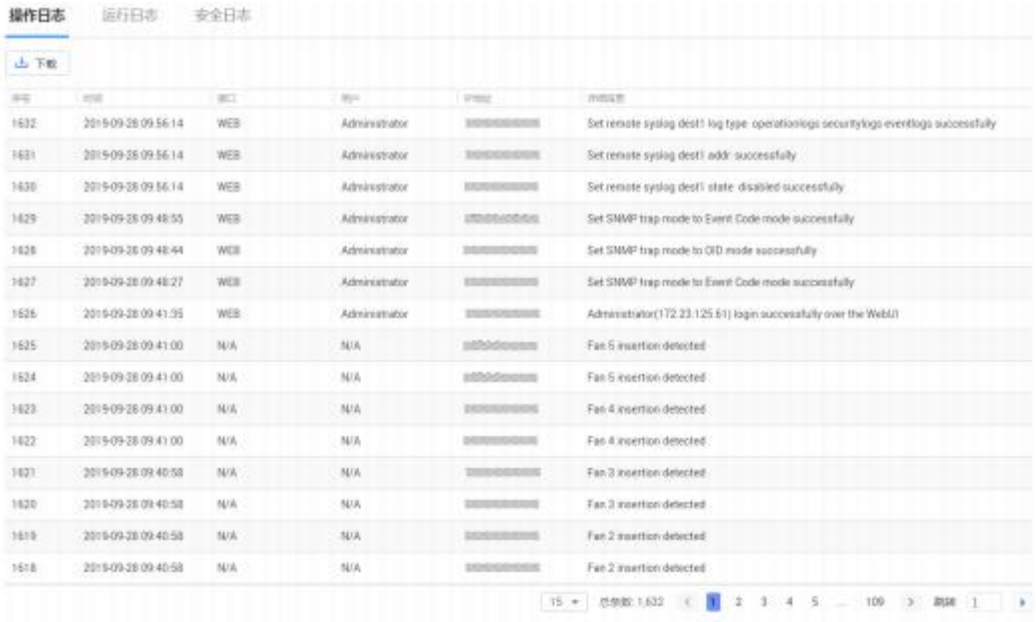


图 3-35 运行日志

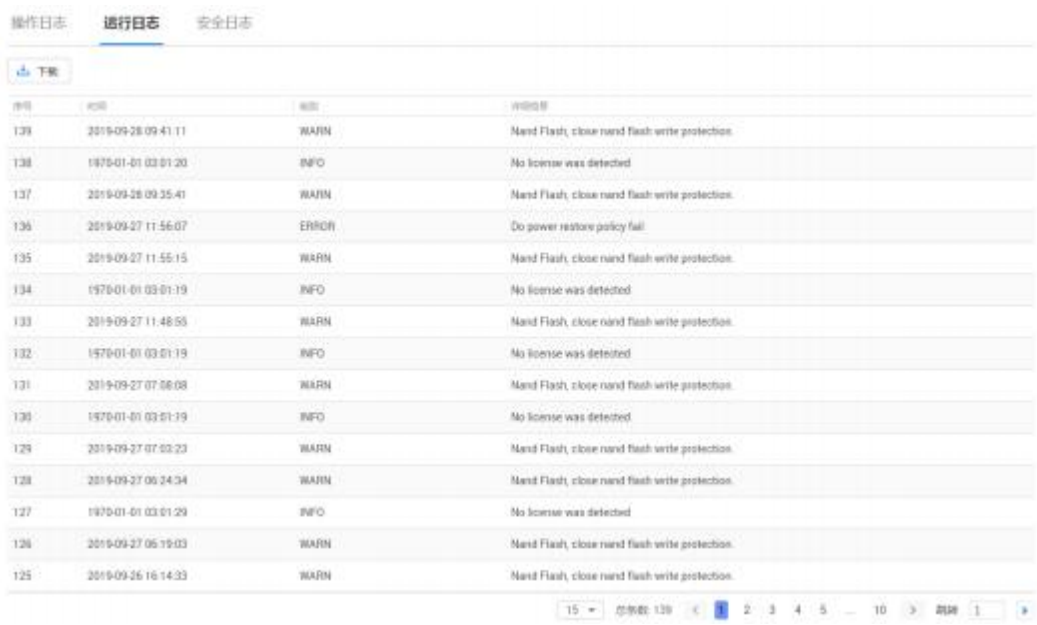
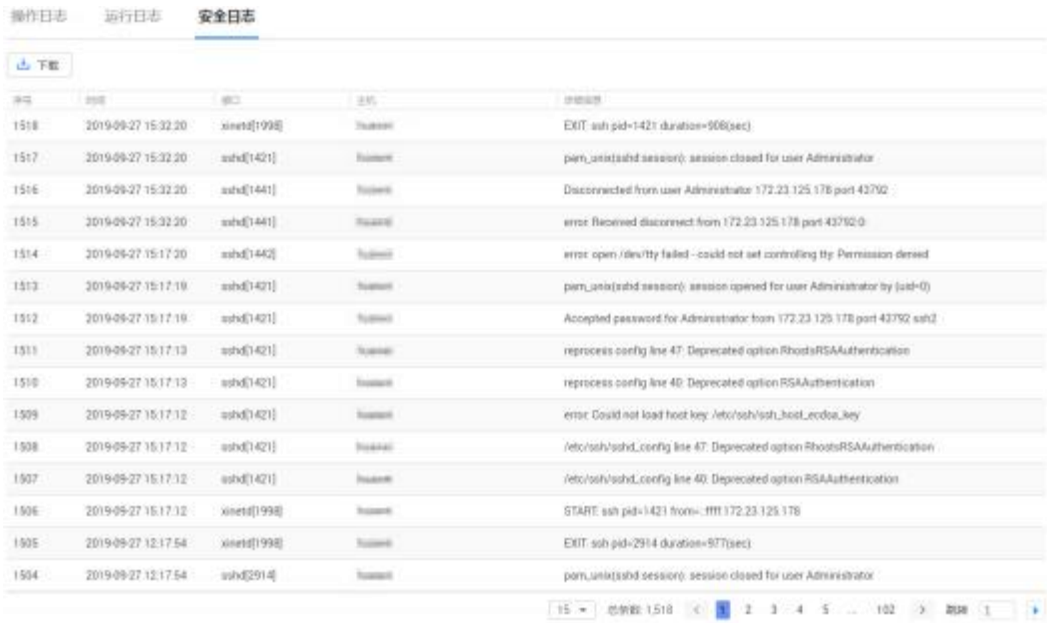


图 3-36 安全日志



参数说明

表 3-36 操作日志

参数	描述
序号	操作发生的顺序， ID越小的操作发生越早。
时间	操作发生的时间。
接口	操作接口。

参数	描述
用户	进行操作的用户。 以下情况“用户”显示为“N/A”，即不显示用户。 ● 定位按钮或电源按钮被按下。 ● 接口为SNMP且版本为v1或v2c。 ● 接口为IPMI且IP地址为HOST (此条日志记录了业务侧发来的IPMI消息)或管理板。 ● 跳帽重置IP和默认用户密码。 ● 部件热插拔。
IP地址	进行操作的终端IP。 ● “IP地址”显示为“ HMM”表示操作由管理板执行。 ● “IP地址”显示为“HOST”表示操作由业务侧执行。 ● “IP地址”显示为“X.X.X.X”表示由登录设备的客户端执行。 以下情况中，“ IP地址”显示为“ 127.0.0.1 ”表示本操作由本机执行。 ● 定位按钮或电源按钮被按下。 ● 接口为LCD或本地串口。 ● 跳帽重置IP和默认用户密码。 ● 部件热插拔。
详细信息	操作的详细描述信息。 通过WEB 、CLI或IPMI升级后，如果触发了iBMC重启，操作日志要记录，记录格式如下： ● 接口： N/A ● 用户： N/A ● IP地址： 127.0.0.1 ● 详细信息： Reset iBMC caused by upgrade successfully
下载	单击“下载”，操作日志文件将自动保存到本地PC的默认路径。
注：“用户”和“ IP地址”如果不满足上述情况，无法解析时显示为“unknown”。	

表 3-37 运行日志

参数	描述
序号	操作发生的顺序， ID越小的操作发生越早。
时间	运行错误发生的时间。

参数	描述
级别	运行错误的告警级别。 ● ERROR ● WARN ● INFO
详细信息	运行错误的详细描述信息。
下载	单击“下载”，运行日志文件将自动保存到本地PC的默认路径。

表 3-38 安全日志

参数	描述
序号	操作发生的顺序， ID越小的操作发生越早。
时间	操作发生的时间。
接口	操作接口。
主机	iBMC系统的主机名。
详细信息	显示用户的登录、退出操作详情。
下载	单击“下载”，安全日志文件将自动保存到本地PC的默认路径。

3.5.7 工作记录

功能介绍

通过使用“工作记录”界面的功能，您可以在本界面记录自己的工作内容，方便以后查看。

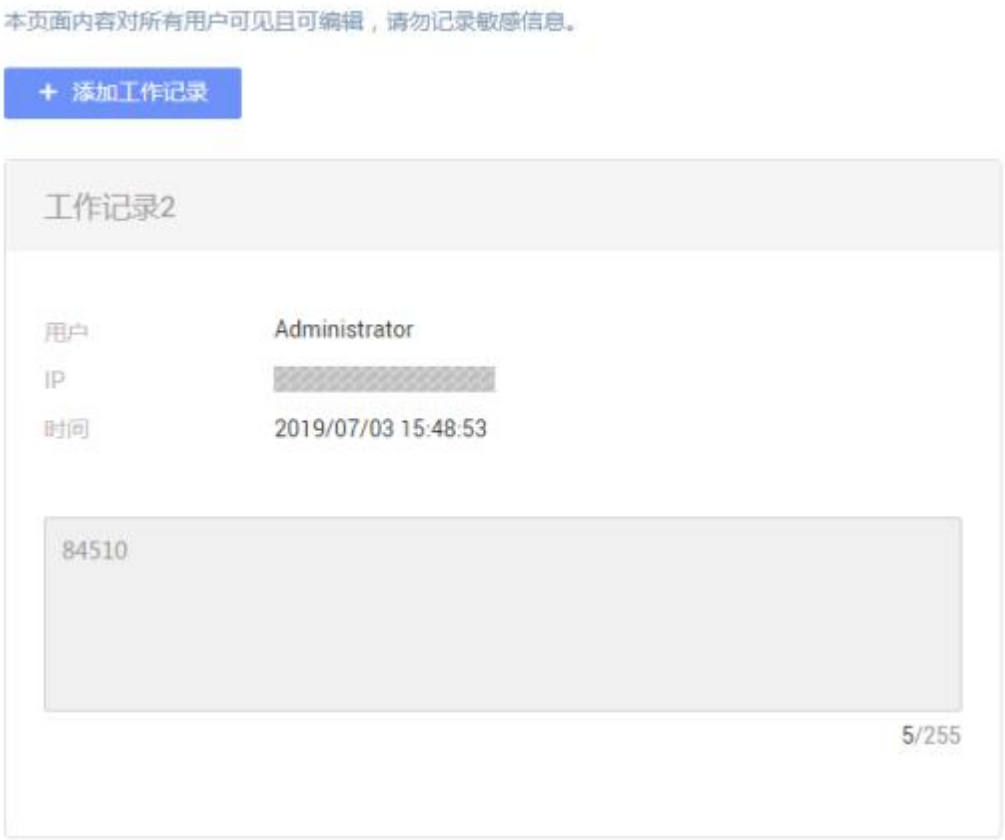
说明

- 工作记录单条最大允许输入255个字符， iBMC最多支持20条工作记录。记录满20条后，若需新增记录，需删除旧的记录以释放空间。
- 工作记录的内容是所有用户可见、所有用户可编辑的。

界面描述

在导航栏中选择“维护诊断 > 工作记录”，打开如图3-37所示界面。

图 3-37 工作记录



操作步骤

表 3-39 工作记录功能操作步骤

操作	操作步骤
添加工作记录	1. 单击“添加工作记录”。 2. 在文本框中编辑工作记录的内容，单击“确定”。
修改工作记录	1. 鼠标移至待操作的工作记录。 2. 单击，在文本框中修改工作记录的内容。 3. 单击“确定”。
删除工作记录	1. 鼠标移至待操作的工作记录。 2. 单击。 3. 在操作确认对话框中单击“是”。

3.6 用户&安全

3.6.1 本地用户

功能介绍

通过使用“本地用户”界面的功能，您可以查看并管理登录iBMC系统的本地用户。

iBMC最多支持16个不同的用户，您可以通过该界面进行用户的搜索、添加、配置和删除。

界面描述

在导航栏中选择“用户&安全> 本地用户”，打开如图3-38所示界面。

图 3-38 本地用户

参数说明

表 3-40 本地用户

参数	描述
添加	打开配置新建本地用户的区域框。
用户ID	用户在iBMC系统内的编号，用于唯一标识一个用户。
用户名	登录iBMC系统的用户名称。 系统有1个默认用户，默认用户名为**Administrator**，默认密码为**Admin@9000**。
角色	用户所属的权限分组。 ● 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 ● 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 ● 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 ● 自定义用户：管理员可为自定义用户指定可操作的功能模块。 ● 无权限用户：该权限组的用户，不拥有任何权限，常用于定义搁置的用户。

参数	描述
登录接口	用户登录iBMC的接口，用户可通过已使能的接口登录iBMC系统。 ● SNMP：使能该接口后，用户可使用符合SNMP协议的终端工具(例如MIB Browser)登录iBMC系统。 ● SSH：使能该接口后，用户可使用符合SSH协议的终端工具（例如PuTTY)登录iBMC命令行。 ● IPMI：使能该接口后，用户可使用符合 IPMI协议的终端工具(例如IPMI Tool)登录iBMC命令行。 ● Local：使能该接口后，用户可通过服务器的串口登录iBMC命令行，或通过LCD登录iBMC管理界面。 ● SFTP：使能该接口后，用户可使用符合SFTP协议的终端工具(例如Xftp)登录iBMC文件系统。 ● Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 ● Redish：使能该接口后，用户可使用符合Redish协议的终端工具登录iBMC系统。
操作	● 编辑：打开编辑已有本地用户信息的区域框。 ● 禁用：设置用户状态为停用状态。 ● 启用：设置用户状态为启用状态。 ● 删除：删除已有本地用户。 **说明** ● 包括管理员、操作员、普通用户、自定义用户在内的所有本地用户均可删除。 ● 当iBMC中存在多个启用的管理员时，可以修改默认用户的权限。当仅有一个启用的管理员用户时，该管理员用户不能被修改权限、禁用或删除。 ● 若已在“用户&安全> 安全增强”页面开启了“业务侧用户管理使能”，可在OS侧通过发送标准的IPMI命令为iBMC添加本地用户。
有效期(天)	用户密码的使用期限。
登录规则	用户需要遵循的登录规则，用户登录时，受已选择的登录规则限制。

表 3-41 SSH 公钥

参数	描述
上传	为SSH用户导入公钥。
公钥文件	选择客户端上保存的SSH公钥文件进行上传。
公钥文本	在文本框中输入SSH公钥的具体内容进行上传。
当前登录用户密码	当前正在进行该操作的用户的登录密码。

添加用户

iBMC系统最多可添加15个不同名称的用户。

步骤1 单击页面左上角的“添加”。

弹出添加用户的窗口。

表 3-42 添加用户所需参数

参数	描述
新建用户ID	新添加用户的ID，取值范围： 3 ~ 17。
新用户名	新建用户的名称。 取值范围： 1 ~ 16位的字符串。 取值原则： ● 由特殊符号、英文字母和数字组成，特殊字符不包括：:<>&,'"/\% ● 不能包含空格且首字符不能是“#”、“+”或“-”。 ● 用户名不能为“.”或“..”。

参数	描述
新密码	新建用户登录iBMC系统的用户密码。为了保证安全，用户应定期修改自己的登录密码。 **说明** ● 只有管理员可以设置密码检查功能的开启状态。 ● 禁用密码检查功能会降低系统安全性，请尽量启用此功能。 取值范围： ● 关闭密码检查功能后，密码不能为空，可以是数字、英文字母和特殊字符组成的长度不大于20的字符串。如果密码长度小于8个字符，该用户将无法使用SNMPv3接口。 ● 启用密码检查功能后，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 – 密码不能是用户名或用户名的倒序。 ● 弱口令字典认证功能使能的情况下，密码不能在弱口令字典中。(弱口令可通过导出弱口令字典命令**ipmcset -t user -d weakpwddic -v export**获取。) **说明** – 默认密码“Admin@9000”在弱口令字典中。 – 使用完全由重复子串构成的口令可能会有安全风险，例如aa、abababab或abcdabcd等，请尽量避免。
密码确认	新建用户的用户密码，此处输入的内容需要与“新密码”中相同。

参数	描述
角色	设置新建用户所属的权限分组。 用户所属的权限分组。 ● 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 ● 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 ● 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 ● 自定义用户：管理员可为自定义用户指定可操作的功能模块。 ● 无权限用户：该权限组的用户，不拥有任何权限，常用于定义搁置的用户。 **说明** 新建用户默认权限为“无权限用户”。
登录规则	用户需要遵循的登录规则，用户登录时，受已选择的登录规则限制。
登录接口	用户可用于登录的接口，用户可通过已启用的接口登录iBMC系统。 ● SNMP：使能该接口后，用户可使用符合SNMP协议的终端工具(例如MIB Browser)登录iBMC系统。 ● SSH：使能该接口后，用户可使用符合SSH协议的终端工具(例如PuTTY)登录iBMC命令行。 ● IPMI：使能该接口后，用户可使用符合 IPMI协议的终端工具(例如IPMI Tool)登录iBMC命令行。 ● Local：使能该接口后，用户可通过服务器的串口登录iBMC命令行，或通过LCD登录iBMC管理界面。 ● SFTP：使能该接口后，用户可使用符合SFTP协议的终端工具(例如Xftp)登录iBMC文件系统。 ● Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 ● Redish：使能该接口后，用户可使用符合Redish协议的终端工具登录iBMC系统。 **说明** 新建用户默认支持所有登录接口。
当前用户登录密码	当前正在进行该操作的用户的登录密码。
保存	保存对新建用户的配置。
取消	取消对新建用户的配置。

步骤2 根据表3-42，设置用户的基本属性。

- ID为1的用户为IPMI标准规范里定义的预留用户，无任何权限，也无法通过该用户登录iBMC。
- ID为2的用户为默认用户。

步骤3 单击“保存”。

用户列表中将显示新添加用户的信息。

----结束

修改用户信息

步骤1 在本地用户列表中，选择需要修改的用户并单击“编辑”。

弹出修改用户信息的窗口。

表 3-43 修改用户信息所需参数

参数	描述
用户名	待修改用户的名称。
密码	待修改用户的新密码。 ● 关闭密码检查功能后，密码不能为空，可以是数字、英文字母和特殊字符组成的长度不大于20的字符串。如果密码长度小于8个字符，该用户将无法使用SNMPv3接口。 ● 启用密码检查功能后，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 – 密码不能是用户名或用户名的倒序。 ● 弱口令字典认证功能使能的情况下，密码不能在弱口令字典中。(弱口令可通过导出弱口令字典命令**ipmcset -t user -d weakpwddic -v export**获取。) **说明** – 默认密码“Admin@9000”在弱口令字典中。 – 使用完全由重复子串构成的口令可能会有安全风险，例如aa、abababab或abcdabcd等，请尽量避免。
密码确认	修改后的用户密码，此处输入的内容需要与“密码”中相同。

参数	描述
角色	用户所属的权限分组。 ● 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 ● 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 ● 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 ● 自定义用户：管理员可为自定义用户指定可操作的功能模块。 ● 无权限用户：该权限组的用户，不拥有任何权限，常用于定义搁置的用户。
登录规则	用户需要遵循的登录规则，用户登录时，受已选择的登录规则限制。
登录接口	用户可用于登录的接口，用户可通过已启用的接口登录iBMC系统。 ● SNMP：使能该接口后，用户可使用符合SNMP协议的终端工具(例如MIB Browser)登录iBMC系统。 ● SSH：使能该接口后，用户可使用符合SSH协议的终端工具（例如PuTTY)登录iBMC命令行。 ● IPMI：使能该接口后，用户可使用符合 IPMI协议的终端工具(例如IPMI Tool)登录iBMC命令行。 ● Local：使能该接口后，用户可通过服务器的串口登录iBMC命令行，或通过LCD登录iBMC管理界面。 ● SFTP：使能该接口后，用户可使用符合SFTP协议的终端工具(例如Xftp)登录iBMC文件系统。 ● Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 ● Redish：使能该接口后，用户可使用符合Redish协议的终端工具登录iBMC系统。 **说明** ● 开启某个用户的IPMI登录接口，需要重置该用户的登录密码。 ● 更改某个用户的SNMP鉴权算法，需要重置该用户的登录密码和SNMPv3加密密码。

参数	描述
SNMPv3加密密码	当登录接口勾选“SNMP”时，需要同时设置此参数。 使用指定用户进行SNMP通信时，可为其设置独立的加密密码来保障通信的安全性。其密码规则与本地用户的密码规则一致。 默认取值：与该用户的登录密码一致。 **说明** ● 未独立设置SNMPv3加密密码时，该密码与用户登录密码同步，存在安全隐患，建议尽快修改并妥善保存。独立设置SNMPv3加密密码后，该密码不再与用户登录密码同步。 ● 使用完全由重复子串构成的口令可能会有安全风险，例如aa、abababab或abcdabcd等，请尽量避免。
确认加密密码	与“SNMPv3加密密码”保持一致。
鉴权算法	SNMPv3采用的鉴权算法。 可选取值： ● MD5 ● SHA ● SHA256 ● SHA384 ● SHA512 默认取值： SHA256 **说明** ● 该设置对“SNMPv3”和“SNMP Trap V3”都有效。 ● MD5算法和SHA算法存在安全隐患，建议使用SHA256 、SHA384或SHA512算法。 ● 当与上层网管对接时，当前鉴权算法类型需要与网管侧保持一致。
加密算法	SNMPv3的安全保障之一，采用指定的算法来保障信息传输的安全性。 可选取值： ● DES ● AES ● AES256 默认取值： AES **说明** ● DES算法存在安全隐患，建议使用AES或AES256算法。 ● 加密算法AES256只能与鉴权算法SHA256 、SHA384或SHA512搭配使用。
当前用户登录密码	当前正在进行该操作的用户的登录密码。
保存	保存对指定用户的修改。 **说明** 修改用户名、密码、权限会导致该用户被强制下线。

参数	描述
取消	取消修改用户信息。

步骤2 根据表3-43提供的信息，修改指定用户的基本信息。

步骤3 单击“保存”。

成功修改用户信息。

----结束

删除用户

步骤1 在本地用户列表中，在待删除的用户列表右侧单击“删除”。

弹出操作确认对话框。

步骤2 输入当前用户的登录密码并单击“是”。

显示“操作成功”，用户列表中该用户信息将消失。

----结束

3.6.2 在线用户

功能介绍

通过使用“在线用户”界面的功能，您可以执行以下操作：

- 查看已登录iBMC系统的用户信息。
- 注销已登录的用户。

只有隶属于管理员组的用户可以注销其他已登录的用户。

界面描述

在导航栏中选择“用户&安全> 在线用户”，打开如图3-43所示界面。

图 3-43 在线用户

参数说明

表 3-50 在线用户

参数	描述
用户名	登录iBMC系统或使用KVM远程虚拟控制台的用户名称。
登录方式	用户登录的方式。 取值范围： ● “GUI(SSO)”表示用户通过单点登录方式登录iBMC WebUI。 ● “GUI”表示用户通过非单点登录方式登录iBMC WebUI。 ● “CLI”表示用户通过命令行视图登录iBMC系统。 ● “KVM”表示用户通过远程虚拟控制台登录服务器操作系统。 ● “Redish”表示用户通过Redish接口登录iBMC系统。 ● “VNC”表示用户通过VNC客户端登录服务器操作系统。
登录IP	连接并登录iBMC系统的IP地址。 取值范围： IP地址和“COM”。 **说明** COM表示使用串口登录iBMC系统。
登录时间	用户登录iBMC系统的时间。

参数	描述
操作	强制其他用户退出登录。 单击某行用户信息的 可以注销该用户。

3.6.3 安全配置

功能介绍

通过使用“安全配置”界面的功能，您可以：

- 查看并设置iBMC系统的用户安全增强规则。
- 查看并管理iBMC系统本地用户的权限。

界面描述

在导航栏中选择“用户&安全 > 安全配置”，打开如图3-44 、图3-45 、图3-46和图3-47所示界面。

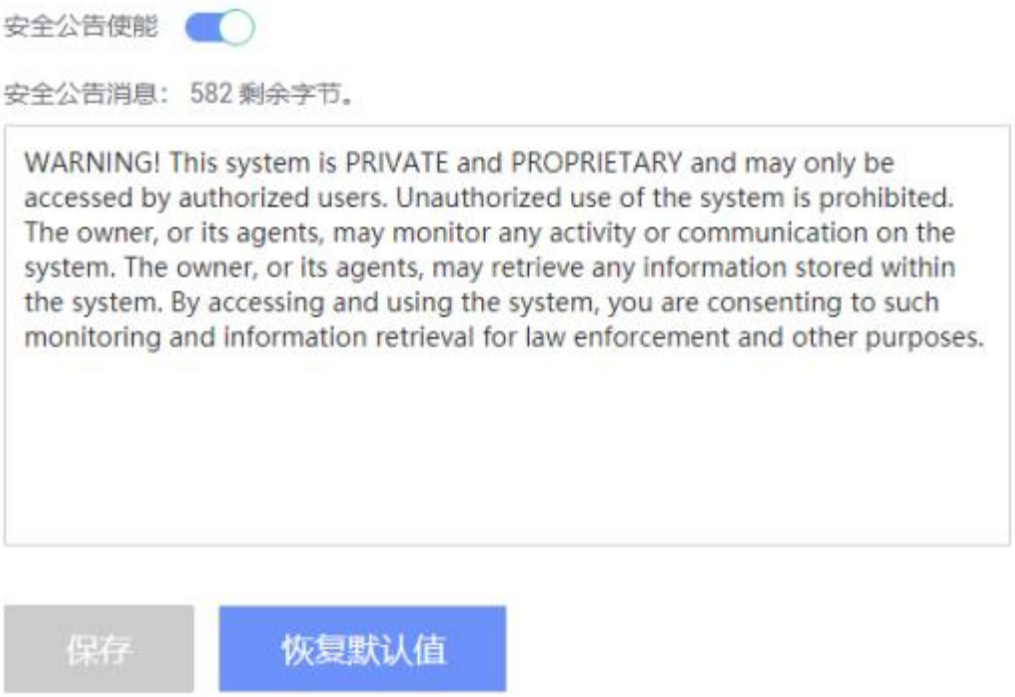
图 3-44 安全增强


系统锁定模式
开启
关闭
业务侧用户管理使能
开启
关闭
密码检查
开启
关闭
SSH密码认证
开启
关闭
TLS版本
TLS 1.2及更高版本
密码有效期(天)
0
密码最小长度配置
8
密码最短使用期(天)
0
不活动期限(天)
0
紧急登录用户
[NULL]
禁用历史密码
5
失败次数
锁定时长(分钟)
登录失败锁定
5
5
证书过期提前告警时间(天)
90
保存

图 3-45 登录规则

图 3-46 权限管理

图 3-47 安全公告



参数说明

表 3-51 安全增强

参数	描述
系统锁定模式	开启或关闭iBMC系统的锁定模式。 默认为关闭状态。 若开启此功能，可以确保系统在根据实际需要配置后，除以下操作允许执行外，其他更改系统配置的尝试都将被阻止： ● 服务器系统上下电 ● UID指示灯和硬盘指示灯的点亮、闪烁与关闭 ● HTML5集成远程控制台、 Java集成远程控制台的使用 ● 虚拟媒体的使用 ● Syslog 、SNMP和SMTP功能的测试和告警模拟 **说明** 仅当许可证级别为高级版时，才能显示此功能。只有拥有管理员权限的用户有权限设置。
业务侧用户管理使能	开启或关闭业务侧对用户的管理功能。 关闭业务侧用户管理功能时，业务侧发送过来的用户管理相关的IPMI命令无效，例如用户添加/删除、权限设置、密码设置等IPMI命令。 默认为开启状态。 ● “开启”表示业务侧可以对用户进行管理。 ● “关闭”表示业务侧不能对用户进行管理。 建议关闭业务侧用户管理功能，否则业务侧可以对iBMC用户进行管理，产生安全隐患。
密码检查	针对每个用户的密码进行复杂度检查。 系统默认启用密码检查功能。该选项同时适用于： ● 本地用户密码、 Trap团体名、 SNMPv1/v2c团体名、SNMPv3加密密码、 VNC密码的复杂度检查。 ● 本地用户密码和SNMPv3加密密码的最小长度检查。 **说明** ● 禁用密码检查功能会降低系统安全性，请尽量启用此功能。 ● 弱口令字典认证功能使能的情况下，密码不能在弱口令字典中。（弱口令可通过导出弱口令字典命令**ipmcset -t user -d weakpwddic -v export**获取。）
SSH密码认证	启用或关闭SSH密码认证功能。 ● 关闭：表示通过SSH登录iBMC时，只能使用公钥认证。 ● 启用：表示通过SSH登录iBMC时，可使用密码认证，也可以使用公钥认证。 默认为开启状态。

参数	描述
TLS版本	在两个通信应用程序通信时， TLS (Transport Layer Security)协议保证其保密性和数据完整性。 浏览器与Web服务器通讯时，需要建立安全链接。 ● TLS 1.2及更高版本：表示支持使用TLS 1.2协议或TLS 1.3协议。 ● 仅限TLS 1.3：表示仅支持使用TLS 1.3协议。 **说明** ● 如果安全配置项中仅开启TLS 1.3协议，则无法开启双因素认证。 ● 仅开启TLS 1.3时，访问Java集成控制台需要的JRE版本为AdoptOpenJDK 11 JRE。
密码有效期(天)	用户密码的使用期限。 取值范围为0 ~ 365，单位为天，取值为0时表示密码为无限期。 默认值： 0 **说明** 为保障系统安全性，建议设置合适的密码有效期，并定期更新密码。
密码最小长度配置	本地用户密码和SNMPv3加密密码的最小长度限制。 该参数仅在开启密码检查时生效。 取值范围为8 ~ 20。 默认值： 8
密码最短使用期（天）	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。 取值范围为0 ~ 365，单位为天，取值为0时表示密码最短使用期无限期。 默认值： 0 **说明** 密码最短使用期必须比密码有效期小10天以上。 ● 如果密码有效期设置为≤10天，密码最短使用期则只能设置为0。 ● 如果密码最短使用期设置为≥355天，则密码有效期只能设置为0。
不活动期限(天)	超过设定期限内未活动的用户会被禁用。 取值范围0或者30 ~ 365，单位为天，取值为0时表示不限制，用户不会因为长时间不活动而被禁止。 默认值： 0
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。 **说明** ● 只有管理员用户可以被设置为“紧急登录用户”。 ● 只有管理员用户才能看到“紧急登录用户”。

参数	描述
禁用历史密码	用户修改密码时，禁止使用设置次数内的历史密码。 取值范围为0 ~ 5，取值为0时，表示不限制使用历史密码。 默认值： 5
登录失败锁定	可设置用户触发登录失败锁定的登录失败次数以及锁定的时长。 ● 登录失败次数取值范围为1 ~ 6以及不限制(即关闭登录失败锁定功能)，默认值为5。 ● 登录失败锁定时长取值范围为1 ~ 30，单位为分钟，默认值为5。 用户被锁定后，在锁定时长内不能继续登录。 **说明** ● 关闭登录失败锁定功能会降低系统安全性，请尽量启用此功能。 ● 紧急情况下需要解锁时，可在命令行下执行**unlock**命令。详情请参见各服务器的iBMC用户指南。
证书过期提前告警时间(天)	iBMC证书过期提前上报告警的时间，单位为天。例如证书过期提前告警时间设置为7 ，表示当iBMC中有证书距离过期时间还有小于或等于7天时，上报告警。 取值范围为7 ~ 180。 默认值： 90

表 3-52 登录规则

参数	描述
时间段	规则允许用户登录服务器的时间段。支持如下三种格式： ● YYYY-MM-DD ： 规则允许用户登录的起始日期和结束日期，例如起始日期为2013-08-30，结束日期为2013-12-30。 ● HH:MM ： 规则允许用户每日登录的时间段，例如起始时间为08:30，结束时间为20:30。 ● YYYY-MM-DD HH:MM ： 规则允许用户登录的具体时间段，例如起始时间为2013-08-30 08:30，结束时间为2013-12-30 20:30。 **说明** ● 起始年份和结束年份只能在1970到2050之间。 ● 同一条规则的起始时间和结束时间的格式必须保持一致。
IP段	规则允许的用户的具体IP地址或IP网段。支持如下两种格式： ● xxx.xxx.xxx.xxx：允许登录服务器的单个用户的IP地址。 ● xxx.xxx.xxx.xxx/mask：允许登录服务器的用户IP网段，其中“mask”为子网掩码长度，取值范围为1 ~ 32。

参数	描述
MAC段	规则允许的用户的具体MAC地址或MAC地址头。支持如下两种格式： ● xx:xx:xx:xx:xx:xx：允许登录服务器的单个用户的MAC地址。 ● xx:xx:xx：允许登录服务器的用户MAC地址头。

表 3-53 权限管理

参数	描述
管理员	该权限组的用户，拥有所有功能模块的操作权限，其权限不可更改。
操作员	该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其权限不可更改。
普通用户	该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其权限不可更改。
自定义1 ~自定义4	管理员可为自定义权限组指定可操作的功能模块。
用户配置	用户和密码相关的配置。 可配置的项目包括： ● 本地用户、在线用户、 LDAP用户、 Kerberos用户 ● 双因素认证、 SSH密码认证 ● 许可证管理、权限管理 ● SNMP v1/v2c/v3相关配置 ● 业务侧用户管理使能 ● KVM/VMM界面的在线用户跳转 ● 恢复出厂设置
常规设置	服务器带外管理基本配置。 可操作的项目包括： ● 产品信息配置 ● 性能监控配置 ● 存储管理、网络配置、固件升级、语言管理 ● NTP、时区配置 ● 智能调速 ● 告警、事件 ● Web服务超时时长、会话模式配置 ● 告警上报(SMTP/Trap配置) ● USB管理

参数	描述
远程控制	● 通过HTML5集成远程控制台、 Java集成远程控制台、独立远程控制台和VNC客户端访问服务器实时桌面 ● 设置KVM超时时长、通信加密、本地KVM、虚拟键鼠持续连接、最大会话、活跃会话 ● 设置VNC超时时长、键盘布局、 VNC密码、登录规则、 SSL加密 ● 配置串口重定向
远程媒体	● 设置VMM通信加密、注销会话 ● 虚拟媒体的挂载和使用
安全配置	安全性的查询和配置。 安全配置包括： ● 操作日志 ● 安全日志 ● 安全增强 ● 登录规则 ● 登录安全信息配置 ● 端口服务 ● Web服务(设置HTTP及端口、 HTTPS及端口、服务器证书信息) ● KVM (可以设置 KVM使能、端口) ● VMM (可以设置VMM使能、端口) ● VNC (可以设置VNC使能、端口) ● SNMP (设置SNMP使能、端口) ● 告警上报(syslog配置) ● 一键收集
电源控制	● 电源设置 ● 功率设置 ● 服务器上下电设置 ● CPU调节设置

参数	描述
调试诊断	现场定位、调试操作。 调试诊断包括： ● FDM故障预测诊断 ● 系统日志 ● 进入维护调测接口 ● 传感器模拟 ● 自动录像配置 ● 手动/自动截屏 ● 串口重定向记录 ● 黑匣子
查询功能	可以登录以及查看除安全配置、调试诊断、双因素认证、在线用户和常规设置以外的信息。
配置自身	可以配置帐户自身的密码以及管理SSH公钥、 SNMPv3加密密码、 SNMPv3加密算法和鉴权算法。 预置角色默认拥有此权限，自定义角色的配置自身权限可设置。

表 3-54 安全公告

参数	描述
安全公告使能	开启或关闭安全公告使能。 将开关状态设置为  后，此处设置的安全公告信息将显示在登录界面的“安全公告”区域。 系统默认开启安全公告使能。
安全公告消息	显示在登录界面的具体信息。 取值范围：最大1024字节的字符串。

启用安全增强功能

步骤1 根据**表3-51**提供的参数信息，设置服务器密码检查、 SSH密码认证功能、密码有效期、不活动期限、紧急登录用户、禁用历史密码、登录失败锁定等安全增强功能。

步骤2 单击“保存”。

界面提示“保存成功”。

----结束

设置登录规则

iBMC同时支持三组登录规则，满足任意一条启用的登录规则即可登录。

登录规则对服务器的本地用户、 LDAP组、 SNMPv3服务、 CLI (SSH)接口、KVM_VMM接口、 RMCP接口、 Redish接口等生效需要满足以下两个条件:

- 该登录规则已在“登录规则”区域框中启用。
- 该登录规则已在对应配置区域框中勾选。

说明

- 某条登录规则为空，规则状态为“启用”并保存时，将导致登录无限制。
- 登录规则输入框为空时表示此项无限制。

步骤1 在“登录规则”区域中，单击待启用的规则右侧的“编辑”。

步骤2 单击  ，将规则状态设置为  。

步骤3 根据表3-52提供的参数信息，设置服务器登录规则。

步骤4 单击“保存”。

----结束

设置安全公告消息

步骤1 在“安全公告”区域中，单击  ，将状态设置为  。

步骤2 在安全公告消息文本框中输入待设置的信息。

步骤3 单击“保存”。

----结束

恢复默认安全公告消息

步骤1 在“安全公告”区域中，单击  ，将状态设置为  。

步骤2 单击“恢复默认值”。

步骤3 单击“保存”。

----结束

3.7 服务管理

3.7.1 端口服务

功能介绍

在“端口服务”页面，您可以查询和设置iBMC支持的各种服务的使能情况以及对应的端口号。

说明

- Web Server(HTTP)/Web Server(HTTPS)端口修改为非浏览器默认端口时， Chrome 、Firefox浏览器无法通过该端口建立会话。此时需要在浏览器中设置允许非默认端口建立会话。
- 同时关闭SSH 、HTTPS 、RMCP 、RMCP+服务会导致无法连接系统。如果这些服务全部关闭，用户需要通过串口连接服务器来开启Web服务。

界面描述

在导航栏中选择“服务管理 > 端口服务”，打开如图3-48所示界面。

图 3-48 端口服务

参数说明

表 3-55 端口服务

服务	默认端口号	说明
SSH	22	安全外壳(SSH ， Secure Shell)是允许在本地计算机和远程计算机之间建立安全渠道的一套标准和网络协议。 iBMC最多允许5个SSH用户同时登录。 **说明** SSH服务支持的加密算法有“AES128-CTR”、“AES192-CTR”和“AES256-CTR”。使用SSH登录iBMC时，请使用正确的加密算法。
SNMP Agent	161	SNMP代理服务是用于翻译和传递管理设备和被管设备之间的请求。
KVM	2198	从远端控制服务器时需要用到的KVM (keyboard ， video ， and mouse)服务，开启后可用本地鼠标、键盘对服务器进行操作，可用本地显示器查看服务器。 最多允许2个用户同时使用。
VMM	8208	从远端控制服务器时需要用到的VMM (Virtual Media Manager)服务，开启后可使用虚拟光驱、虚拟软驱等功能。 同一时间只允许1个用户使用。

服务	默认端口号	说明
Video	2199	从远端控制服务器时需要用到的Video服务，开启后可使用**3.5.4 录像截屏**功能。 同一时间只允许1个用户使用。
VNC	5900	从远端控制服务器时需要用到的VNC（Virtual Network Console)服务，开启后可用本地鼠标、键盘对服务器进行操作，可用本地显示器查看服务器。 最多允许5个用户同时使用。
Web Server (HTTP)	80	提供网上信息浏览服务的服务器，可以解析超文本传输协议(HTTP，Hypertext Transfer Protocol)。系统默认启用该服务是为了支持输入IP默认跳转的功能，建立连接后将默认跳转到HTTPS这个安全协议。
Web Server (HTTPS)	443	提供网上信息浏览服务的服务器，可以解析安全超文本传输协议(HTTPS，Hypertext Transfer Protocol over Secure Socket Layer)及Redish协议。 最多允许4个用户同时使用该服务登录iBMC。
IPMI LAN (RMCP)	默认主用端口Port1为623，备用端口Port2为664。	基于局域网(LAN，Local Area Network)方式的IPMI，支持远程管理控制协议（RMCP，Remote Management Control Protocol)。该服务由于自身机制而存在安全隐患，请尽量避免使用。建议使用IPMI LAN(RMCP+)服务代替IPMI LAN(RMCP)服务。系统默认禁用该服务。
IPMI LAN (RMCP+)	端口与RMCP服务共用。	基于局域网(LAN，Local Area Network)方式的IPMI，支持远程管理控制协议。 **说明** RMCP+由于协议自身的漏洞(CVE-2013-4786)，存在安全隐患，建议参考**风险规避措施**进行处理。

修改服务和端口属性

步骤1 单击“编辑”。

步骤2 设置指定服务的使能状态及端口号。

- 单击  使其变为  ，表示开启该服务。
- 单击  使其变为  ，表示关闭该服务。

步骤3 设置服务的端口。

步骤4 单击“保存”。

----结束

风险规避措施

针对RMCP+存在的安全漏洞(CVE-2013-4786)，建议按照如下方式处理：

- 如果不需要使用IPMI协议访问iBMC：
  - 请在此界面中关闭IPMI服务。

    说明

    关闭IPMI服务后，其他设备将无法通过IPMI协议访问iBMC，因此，对基于IPMI协议的工具(例如IPMItool 、InfoCollect 、eSight等)的使用产生影响。
  - 开启密码复杂度检查功能，设置符合密码复杂度要求的密码。
- 如果需要使用IPMI协议访问iBMC：
  - 将iBMC管理网口所在网络设置为独立的局域网。
  - 开启密码复杂度检查功能，设置符合密码复杂度要求的密码。

3.7.2 Web 服务

功能介绍

在“Web服务”页面，您可以：

- 查看和设置Web服务的基本属性，并对当前使用的SSL证书进行了解。
- 自定义SSL证书并进行导入。

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

说明

- 该页面涉及的SSL证书，可以是单一的SSL证书信息，也可以是证书链信息。其中证书链的层级不得超过10级。
- 支持导入证书文件的格式为.crt 、.cer 、.pem 、.pfx和.p12。其中， .crt 、.cer或.pem格式的证书文件不得大于1MB ， .pfx或 .p12格式的证书文件不得大于100KB。
- MD5和SHA1为不安全的弱签名算法， iBMC不支持导入弱签名算法(MD5和SHA1)证书。

界面描述

在导航栏中选择“服务管理 > Web服务”，打开如**图3-49**所示界面。

图 3-49 Web 服务

参数说明

表 3-56 Web 服务

区域	参数	说明
基本配置	HTTP	提供网上信息浏览服务的服务器，可以解析超文本传输协议(HTTP ， Hypertext Transfer Protocol)。系统默认启用该服务是为了支持输入IP默认跳转的功能，建立连接后将默认跳转到HTTPS这个安全协议。 **说明** 停用HTTP服务后，在浏览器中输入“*http:iBMC管理网口地址*”后，将无法自动跳转至HTTPS服务，影响正常使用。
	HTTPS	提供网上信息浏览服务的服务器，可以解析安全超文本传输协议(HTTPS ， Hypertext Transfer Protocol over Secure Socket Layer)及Redish协议。 **说明** 停用HTTPS服务后，将无法登录iBMC WebUI。

区域	参数	说明
	端口	系统服务占用的端口号。 取值范围： 1 ~ 65535
	超时时长（分钟）	任意连续两次操作iBMC界面的最大时间间隔。若连续两次操作的时间间隔超过了最大值， Web页面将自动返回到登录界面。 取值范围： 5 ~ 480之间的数字。 默认值： 5
	会话模式	使用同一帐号登录iBMC界面时采用的模式。 ● 共享：用户可同时在多个(≤4)客户端使用同一帐号登录iBMC WebUI。 ● 独占：一个帐户在同一时间只允许一个客户端使用其登录iBMC WebUI。建立连接后，若用户在其他客户端使用该帐号进行登录，系统会自动终止之前的连接，重新与新的客户端建立连接。
SSL证书	签发者	SSL证书的签发者信息，包括： ● CN：签发者的名称 ● OU：签发者所在部门 ● O：签发者所在的公司 ● L：签发者所在的城市 ● S：签发者所在的省份 ● C：签发者所在的国家
	使用者	SSL证书的使用者(即当前iBMC)信息，包含的具体参数类型与“签发者”相同。 **说明** 使用者名称CN需要配置为服务器iBMC的FQDN (主机名 .域名)。
	有效起止日期	SSL证书生效起始日期和结束日期。
	序列号	SSL证书序列号。用于证书的识别、迁移。

自定义服务器证书信息并导入

说明

- 该操作主要适用于申请和导入服务器可信证书的场景。
- 请定期更新证书，否则可能存在安全风险。

步骤1 在“SSL证书”区域单击“自定义”。

显示“自定义证书”窗口，如图3-50所示。

图 3-50 自定义证书

步骤2 选择“生成CSR服务”，输入自定义的证书请求信息，并单击“生成”。

步骤3 将生成的CSR文件发往SSL证书颁发机构，并申请SSL证书。

获取到正式的SSL证书后，保存到客户端。

步骤4 在“自定义证书”窗口选择“导入服务器证书”。

步骤5 选中待上传的SSL证书。

说明

- 支持导入证书文件的格式为.crt、.cer、.pem、.pfx和.p12。其中，.crt、.cer或.pem格式的证书文件不得大于1MB，.pfx或.p12格式的证书文件不得大于100KB。
- MD5和SHA1为不安全的弱签名算法，iBMC不支持导入弱签名算法(MD5和SHA1)证书。

步骤6 单击“打开”。

步骤7 在“证书密码”编辑框输入证书密码。

步骤8 单击“确定”。

证书导入成功后，立即生效。

说明

自定义生成的CSR文件与向CA机构申请的服务器证书是一一对应的，在导入服务器证书之前请不要再次生成新的CSR文件，否则需要向CA机构重新申请服务器证书。

步骤9 重新登录iBMC WebUI。

----结束

导入现有 SSL 证书

说明

- 该操作主要适用于客户端已具有可用SSL证书的场景。
- 如要导入自己制作的证书，在证书生成时建议采用安全性高的加密算法，例如RSA2048。
- 请定期更新证书，否则可能存在安全风险。

步骤1 在“SSL证书”区域单击“自定义”。

显示“自定义证书”窗口。

步骤2 选择“导入服务器证书”。

步骤3 选择现有的SSL证书文件。

说明

- 支持导入证书文件的格式为.crt 、.cer 、.pem 、.pfx和.p12。其中， .crt 、.cer或.pem格式的证书文件不得大于1MB ， .pfx或 .p12格式的证书文件不得大于100KB。
- MD5和SHA1为不安全的弱签名算法， iBMC不支持导入弱签名算法(MD5和SHA1)证书。

步骤4 单击“打开”。

步骤5 在“证书密码”编辑框输入证书密码。

步骤6 单击“确定”。

证书导入成功后，立即生效。

说明

上传的文件如果超过100MB会引起页面请求失败，刷新页面可恢复。

步骤7 重新登录iBMC WebUI。

----结束

3.7.3 虚拟控制台

功能介绍

从远端控制服务器实时桌面时需要用到的KVM (keyboard，video ， and mouse)服务，开启后可用本地(即用户操作所用的客户端)的鼠标、键盘、显示器对服务器进行操作管理。

在“虚拟控制台”页面，您可以查看和设置KVM功能的开启情况及相关配置项目。

界面描述

在导航栏中选择“服务管理 > 虚拟控制台”，打开如图3-51所示界面。

图 3-51 虚拟控制台

参数说明

表 3-57 虚拟控制台

参数	说明
KVM使能	KVM服务的使能状态。
端口	KVM服务使用的端口号，默认为2198。 取值范围： 1 ~ 65535
超时时长（分钟）	任意连续两次操作KVM界面的最大时间间隔(包括虚拟光驱读取数据的时间间隔，单位为分钟)。若连续两次操作的时间间隔超过了最大值，系统将自动断开与KVM界面的连接。 取值范围： 0 ~ 480之间的数字。 取值为“0”时，表示永不超时。 默认取值： 60 此参数不允许设置为空。
通信加密	数据传输加密功能的启用状态。 开启通信加密时， KVM数据在客户端与服务器之间传输时采用AES128算法加密。 默认关闭KVM通信加密，出于安全考虑，建议用户保持通信加密的开启状态。 **说明** ● 关闭并保存VMM加密后才能关闭KVM加密。 ● 通信加密仅对Java远程控制台有效。 HTML5远程控制台的通信是TLS加密的，不依赖于当前页面的通信加密。
本地KVM	设置本地KVM的使能状态。 ● 开启时，可同时使用本地KVM和远程虚拟控制台连接到服务器实时桌面。 ● 关闭时，本地KVM不可用，仅可通过远程虚拟控制台连接到服务器实时桌面。
虚拟键鼠持续连接	设置鼠标、键盘是否持续连接。 ● 开启时， iBMC的虚拟鼠标、键盘将一直连接到业务侧的USB控制器。 ● 关闭时，只有当使用远程连接功能时，虚拟鼠标、键盘才动态连接到USB控制器，否则将断开此连接。当服务器操作系统空闲并且没有虚拟鼠标、键盘连接的时候，会有一定的节能效果。
系统自动锁定	设置系统自动锁定使能状态，默认关闭。 ● 开启时，支持最后一个远程登录用户离开时，业务侧OS自动锁定。 ● 关闭时，不支持业务侧OS自动锁定。 **说明** 该配置项仅在OS启动后生效。如果在BIOS界面，退出远程虚拟控制台前需手动退出BIOS。

参数	说明
系统自动锁定方式	设置系统自动锁定方式，在系统自动锁定使能显示。 ● “Custom”：自定义。 ● “Windows”： Windows锁定方式。
自定义快捷键	系统自动锁定自定义快捷键，在系统自动锁定方式为自定义时可设置。 支持的字符串可以是： 0 ~ 9 、a ~ z 、特殊字符以及功能键。
最大会话	允许使用KVM的最大用户数量，固定为2。
活跃会话	当前使用KVM的用户数量。

3.7.4 虚拟媒体

功能介绍

从远端控制服务器实时桌面时需要用到的VMM（Virtual Media Manager)服务，开启后可使用虚拟光驱、虚拟软驱等功能。

在“虚拟媒体”页面，您可以查看和设置VMM功能的开启情况及相关配置项目。

界面描述

在导航栏中选择“服务管理 > 虚拟媒体”，打开如图3-52所示界面。

图 3-52 虚拟媒体

参数说明

表 3-58 虚拟媒体

参数	说明
VMM使能	VMM服务的使能状态。
端口	VMM服务使用的端口号，默认为8208。 取值范围： 1 ~ 65535 **说明** 浏览器出于安全问题，会禁止一些网络浏览以外的端口，设置这些端口将导致HTML5集成远程控制台的虚拟媒体功能不能使用。
通信加密	数据传输加密功能的启用状态。 开启通信加密时， VMM数据在客户端与服务器之间传输时采用AES128算法加密。 默认关闭VMM通信加密，出于安全考虑，建议用户保持通信加密的开启状态。 **说明** ● 通信加密仅对Java远程控制台有效。 HTML5远程控制台的通信是TLS加密的，不依赖于当前页面的通信加密。 ● iBMC V3.01.12.01及之后版本，虚拟媒体通信加密默认为开启状态，不再支持设置通信加密。

参数	说明
最大会话	允许使用VMM连接系统的最大用户数量，固定为1。
活跃会话	当前使用VMM连接系统的用户数量。

3.7.5 VNC

功能介绍

从远端控制服务器实时桌面时需要用到的VNC（Virtual Network Console)服务，开启后可用本地(即用户操作所用的客户端)的鼠标、键盘对服务器进行操作，可用本地显示器查看服务器。

在“VNC”页面，您可以查看和设置VNC功能的开启情况及相关配置项目。

界面描述

在导航栏中选择“服务管理 >VNC”，打开如图**3-53**所示界面。

图 3-53 VNC


VNC功能
VNC使能
开启
关闭
端口
5900
恢复默认值
超时时长(分钟)
60
键盘布局
日式键盘
VNC密码
确认VNC密码
密码有效期(天)
无限期
登录规则
规则1 允许时间： — 至 — 允许IP段： — 允许MAC段： —
规则2 允许时间： — 至 — 允许IP段： — 允许MAC段： —
规则3 允许时间： — 至 — 允许IP段： — 允许MAC段： —
点击跳转至"安全配置"页面修改登录规则
SSL加密
开启
关闭
最大会话
5
活跃会话
0
保存

参数说明

表 3-59 VNC

参数	说明
VNC使能	VNC服务的使能状态。
端口	VNC服务使用的端口号，默认为5900。 取值范围： 1 ~ 65535
超时时长（分钟）	任意连续两次操作VNC界面的最大时间间隔(包括虚拟光驱读取数据的时间间隔)。若连续两次操作的时间间隔超过了最大值，系统将自动断开与VNC界面的连接。 取值范围： 0 ~ 480之间的数字。 取值为“0”时，表示永不超时。 默认取值： 60 此参数不允许设置为空。
键盘布局	VNC控制的服务器实时桌面的键盘布局。 取值范围： ● 日式键盘 ● 美式键盘 ● 德式键盘 默认取值：日式键盘
VNC密码	设置VNC服务的登录密码。 取值原则： ● 关闭密码检查功能时， VNC服务的登录密码取值长度为1 ~ 8个字符，可由数字、英文字母和特殊字符组成。 ● 启用密码检查功能时， VNC服务的登录密码取值规则为： – 长度要求：必须为8个字符。 – 复杂度要求： – 至少包含一个空格或以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/? – 至少包含以下两种字符： 大写字母： A ~ Z 小写字母： a ~ z 数字： 0 ~ 9
确认VNC密码	确认设置的VNC服务登录密码。此处输入的内容需要与“VNC密码”中相同。
密码有效期（天）	VNC密码的剩余有效期。
登录规则	VNC用户登录规则， VNC用户登录时将受到已选择登录规则的限制。

参数	说明
SSL加密	设置SSL加密功能的启用状态。 出于安全考虑，建议用户保持SSL加密功能的开启状态。如果已禁用SSL加密，则VNC客户端将直接启动RFB进程，无需进行SSL验证。 **说明** 如果已启用SSL加密，则仅已启用SSL加密的VNC客户端可连接到服务器OS 。 如果VNC客户端没有内置的SSL加密选项，则请使用SSL隧道应用程序提供SSL加密功能。
最大会话	允许通过VNC服务登录服务器实时桌面的最大用户数量，固定为5。
活跃会话	当前通过VNC服务登录服务器实时桌面的用户数量。

3.7.6 SNMP

功能介绍

简单网络管理协议(SNMP)，由一组网络管理的标准组成，包含一个应用层协议、数据库模型和一组资源对象。该协议支持网络管理系统，用以监测连接到网络上的设备。

在“SNMP”页面，您可以查看和设置SNMP功能的开启情况及相关配置项目。

iBMC支持多个版本的SNMP：

- SNMPv1 ：简单网络管理协议的第一个正式版本，在RFC1157中定义。该版本由于自身机制而存在安全隐患，请尽量避免使用。建议使用SNMPv3版本的SNMP服务。
- SNMPv2：基于共同体的管理架构，在RFC1901中定义的一个实验性协议。该版本由于自身机制而存在安全隐患，请尽量避免使用。建议使用SNMPv3版本的SNMP服务。
- SNMPv3：简单网络管理协议的第三个正式版本。在前面的版本基础上， SNMPv3增加了安全能力和远程配置能力。

说明

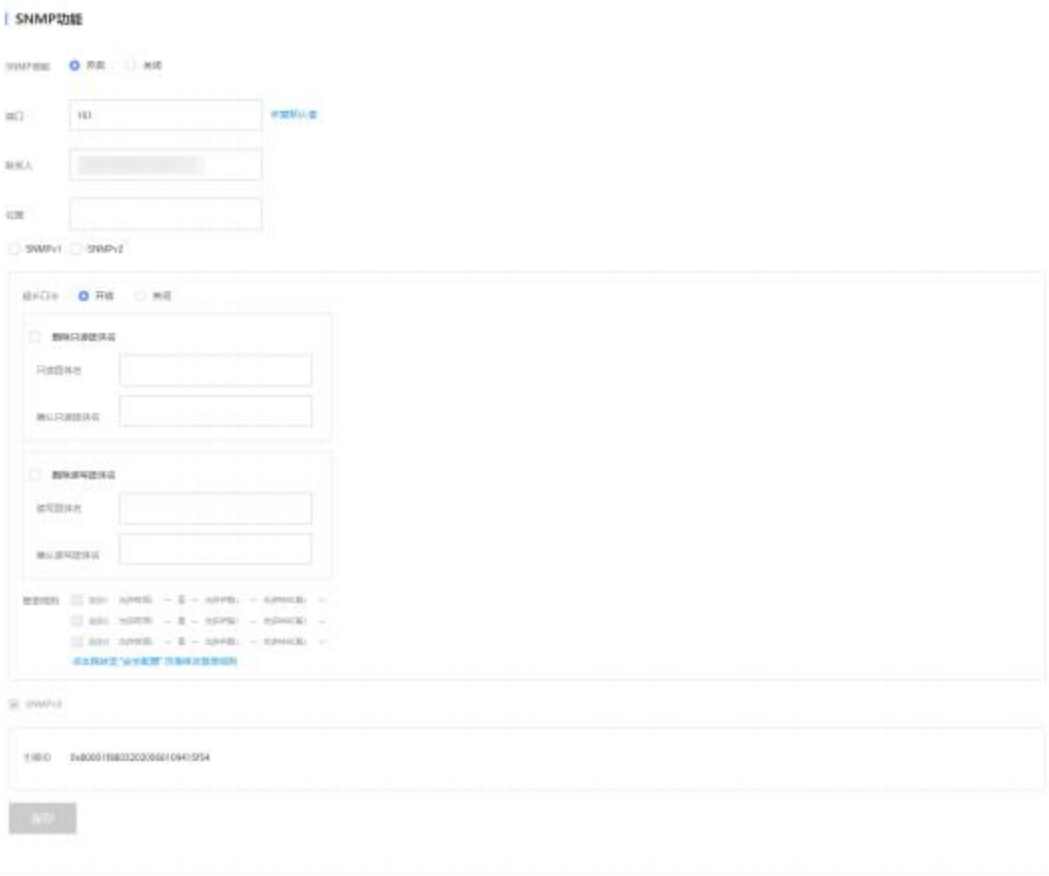
在“用户&安全 > 本地用户”界面执行以下操作后，可能会导致SNMP功能在5s~10s内不可用：

- 添加或删除用户
- 编辑用户密码、用户角色
- 设置SNMPv3加密密码、 SNMPv3算法

界面描述

在导航栏中选择“服务管理 > SNMP”，打开如图3-54所示界面。

图 3-54 SNMP 功能



参数说明

表 3-60 SNMP 功能

参数	说明
SNMP使能	SNMP服务的启用状态。
端口	SNMP服务使用的端口号，默认为161。 取值范围： 1 ~ 65535
联系人	服务器的管理人员。 取值范围： 0 ~ 255个字符组成的字符串，由数字、英文字母和特殊字符组成。
位置	服务器的物理位置。 取值范围： 0 ~ 255个字符组成的字符串，由数字、英文字母和特殊字符组成。
SNMPv1/SNMPv2 **说明** 如果启用该版本的SNMP服务，请及时修改SNMP的团体名。	

参数	说明
超长口令	超长口令的启用状态。 启用超长口令后，设置的团体名长度必须大于等于16个字符。 默认取值：开启。
只读团体名	SNMP协议只读团体名。 取值原则： ● 关闭密码检查功能时： – 若已启用超长口令，则团体名可设置为长度为16 ~ 32个字符的字符串，字符串不能包含空格。 – 若已禁用超长口令，则团体名可设置为长度为1 ~ 32个字符的字符串，字符串不能包含空格。 ● 开启密码检查功能时： – 若已启用超长口令，则团体名可设置为长度为16 ~ 32个字符的字符串。 – 若已禁用超长口令，则团体名可设置为长度为8 ~ 32个字符的字符串。 – 至少包含以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/? – 至少包含以下字符中的两种： 大写字母： A ~ Z 小写字母： a ~ z 数字： 0 ~ 9 – 不能包含空格。 ● 弱口令字典认证功能使能的情况下，团体名不能在弱口令字典中。(弱口令可通过导出弱口令字典命令**ipmcset -t user -d weakpwddic -v export** <*ilepath*| *ile-URL*>)获取。
确认只读团体名	重复输入上一步的只读团体名，确认输入是否正确。

参数	说明
读写团体名	SNMP协议读写团体名。 取值原则： ● 关闭密码检查功能时： – 若已启用超长口令，则团体名可设置为长度为16 ~ 32个字符的字符串，字符串不能包含空格。 – 若已禁用超长口令，则团体名可设置为长度为1 ~ 32个字符的字符串，字符串不能包含空格。 ● 开启密码检查功能时： – 若已启用超长口令，则团体名可设置为长度为16 ~ 32个字符的字符串。 – 若已禁用超长口令，则团体名可设置为长度为8 ~ 32个字符的字符串。 – 至少包含以下特殊字符： `~!@#$%^&*()-_=+\\|[{}];:'",<.>/? – 至少包含以下字符中的两种： 大写字母： A ~ Z 小写字母： a ~ z 数字： 0 ~ 9 – 不能包含空格。 ● 弱口令字典认证功能使能的情况下，团体名不能在弱口令字典中。(弱口令可通过导出弱口令字典命令**ipmcset -t user -d weakpwddic -v export** < *ilepath*| *ile-URL*>)获取。
确认读写团体名	重复输入上一步的读写团体名，确认输入是否正确。
登录规则	SNMPv1和SNMPv2用户对应的登录规则，对已选择该登录规则的本地用户进行限制。
SNMPv3 **说明** ● iBMC系统支持开启或关闭SNMPv3服务， SNMPv3服务默认为开启状态。 ● iBMC V3.01.12.01及以上版本，请在“用户&安全 > 本地用户 > 编辑用户”界面设置SNMPv3加密密码和SNMPv3算法。	

参数	说明
鉴权算法	SNMPv3采用的鉴权算法。 可选取值： ● MD5 ● SHA ● SHA256 ● SHA384 ● SHA512 默认取值： SHA **说明** ● 该设置对“SNMPv3”和“SNMP Trap V3”都有效。 ● iBMC V591及以上版本支持SHA256 、SHA384或SHA512算法。 ● MD5算法和SHA算法存在安全隐患，建议使用SHA256 、SHA384或SHA512算法。 ● 当与上层网管对接时，当前鉴权算法类型需要与网管侧保持一致。
加密算法	SNMPv3的安全保障之一，采用指定的算法来保障信息传输的安全性。 可选取值： DES 、AES 默认取值： AES **说明** DES算法存在安全隐患，建议使用AES算法。
引擎ID	SNMP代理实体的SNMP引擎的唯一标识符。

3.8 iBMC 管理

3.8.1 网络配置

功能介绍

在“网络配置”界面，您可以查询和设置iBMC管理网口的网络配置情况，包括：

- 主机名
- 网口模式
- 网络协议及地址
- DNS信息
- VLAN属性
- LLDP属性

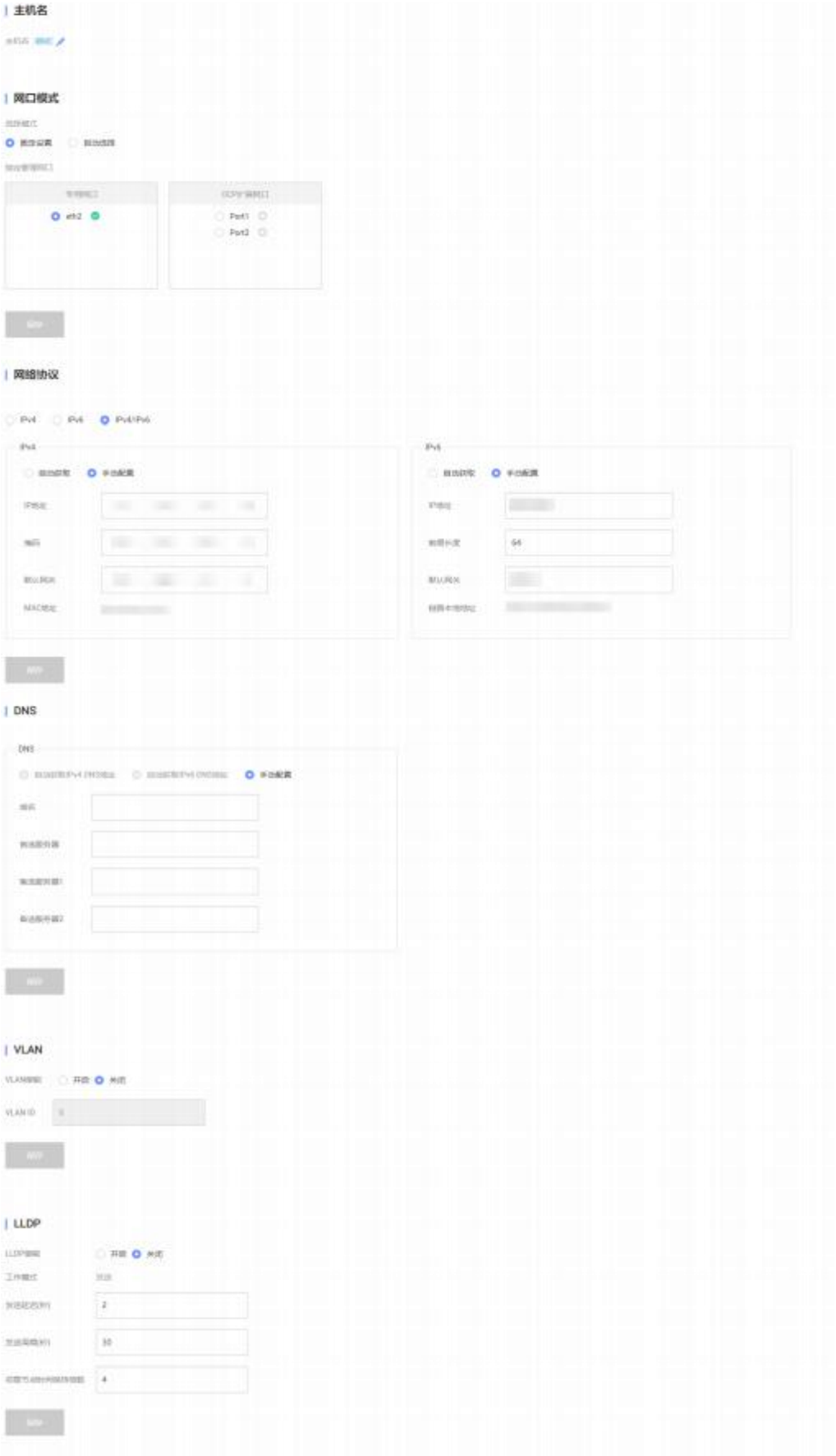
须知

变更管理网口地址会导致网络连接断开，请谨慎操作。

界面描述

在导航栏中选择“iBMC管理> 网络配置”，打开如图3-55所示界面。

图 3-55 网络配置



参数说明

表 3-61 网络配置

参数	说明
主机名	iBMC的主机名称。单击可进行修改。 取值范围： 1 ~ 64位的字符串。 可由数字、英文字母和连字符(-)组成，且连字符不能出现在开头和结尾。
选择模式	iBMC管理网口的选择模式。 默认值为“固定设置”。
固定设置	指定专用网口、 PCIe扩展网口或OCP扩展网口作为iBMC的管理网口。 ● 专用网口：专用的iBMC管理网口(即服务器Mgmt网口)。 ● PCIe扩展网口： PCIe卡的业务网口(即支持NC-SI且已连接NC-SI线缆的PCIe扩展网卡)。 ● OCP扩展网口： OCP卡的业务网口。
自动选择	依据网口连接状态， iBMC自动选择管理网口所使用的物理网口。 勾选复选框设置参与自动选择的网口，如果同时存在多个已连接的网口， iBMC根据如下顺序选择管理网口： 专用网口 > PCIe扩展网口(Port1 ~ Port2或Port1 ~ Port4) > OCP扩展网口(Port1 ~ Port2或Port1 ~ Port4)。 当服务器上同时存在OCP卡和已连接NC-SI线缆的PCIe卡时，OCP卡的业务网口不能作为管理网口使用。 服务器同时配置OCP卡和PCIe网卡时，两者存在互斥机制。当PCIe网卡连接了NC-SI线缆， PCIe网卡网口可用于访问iBMC，OCP卡网口不能访问iBMC；当PCIe网卡未连接NC-SI线缆时，PCIe网卡网口不能访问iBMC ，OCP卡网口可用于访问iBMC。 **说明** ● 如果PCIe扩展网口要作为iBMC的管理网口，其所属的PCIe扩展网卡仅支持已连接NC-SI线缆的网卡。 ● 当手动或自动选择PCIe扩展网口或OCP扩展网口时，管理网口与业务网口共用同一个物理网口。为安全起见，建议在“固定设置”或“自动选择”模式包含了PCIe扩展网口或OCP扩展网口时，为管理网口配置VLAN。 ● 如果某个网口此时作为iBMC的管理网口，网口右侧会出现标识。
指定管理网口	“固定设置”模式下，选中单选按钮指定管理网口；“自动选择”模式下，勾选复选框设置参与自动选择的网口。

参数	说明
网络协议	支持的IP协议包括： ● IPv4：只使能IPv4协议，此时只能配置IPv4。 ● IPv6：只使能IPv6协议，此时只能配置IPv6。 ● IPv4/IPv6：既使能IPv4协议又使能IPv6协议，此时既能配置IPv4又能配置IPv6。 默认值： IPv4/IPv6
IPv4	自动获取IP地址：服务器自动获取管理网口的IPv4地址。
	手动配置：自定义管理网口的IPv4地址。管理网口的IPv4地址信息包括：“IP地址”、“掩码”、“默认网关”和“MAC地址”。 **说明** ● “MAC地址”是网卡的硬件地址。 ● 如果不使用默认网关，网关地址可以配置为同一网段的任一IP地址。
IPv6	自动获取IP地址：服务器自动获取管理网口的IPv6地址。
	手动配置：自定义管理网口的IPv6地址。管理网口的IP地址信息包括“IP地址”、“前缀长度”、“默认网关”、“链路本地地址”。 **说明** ● “链路本地地址”用于本地链路通讯。 ● “IP地址2”列出了通过SLAAC (Stateless Address Autoconiguration)协议获取到的IPv6地址，最多可以获取到15个。 ● 如果不使用默认网关，网关地址可以配置为同一网段的任一IP地址。
DNS	● 自动获取IPv4 DNS地址：无需手动操作，系统自动获取基于IPv4的DNS信息。 ● 自动获取IPv6 DNS地址：无需手动操作，系统自动获取基于IPv6的DNS信息。 ● 手动配置：选择手动设置DNS信息后，用户可以手动配置DNS服务器的域名、首选DNS服务器地址和备选DNS服务器地址。 **须知** ● iBMC管理网口的IP地址获取模式为自动获取时， DNS信息获取方式也必须选择自动获取。 ● iBMC管理网口的IP地址获取模式为手动配置时， DNS信息获取方式也必须选择手动配置。

参数	说明
	域名：服务器的域名称。 取值原则： ● 最大长度为67个字符。 ● 可由数字、大小写英文字母和连接号(-)，点号(.)组成。 ● 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 ● 任意两个点号之间的字符长度不允许超过63。
	首选服务器：优先选择的DNS服务器。 取值原则： IPv4地址、 IPv6地址或为空
	● 备选服务器1 ： 第二选择的DNS服务器。 ● 备选服务器2：第三选择的DNS服务器。 取值原则： IPv4地址、 IPv6地址或为空
VLAN使能	使能或禁止管理网口的VLAN属性。 默认关闭。 **说明** ● 仅“固定设置”模式下选择“专用网口”时，不支持VLAN设置。其他模式下，支持使能和配置VLAN ID。 ● 从管理网络与业务网络隔离角度考虑，建议使能VLAN和配置VLAN ID。 ● 若选择“专用网口”作为iBMC管理网口，当前配置的VLAN信息不生效；若选择除“专用网口”外的其他网口作为iBMC管理网口，则当前配置的VLAN信息有效。
VLAN ID	管理网口所属VLAN。 取值范围： 1 ~ 4094的整数。 **说明** VLAN ID配置保存后，需要几秒钟之后功能才会生效。
LLDP 仅在专用网口或PCIe扩展网口作为iBMC的管理网口场景下支持LLDP功能。	
LLDP使能	开启LLDP后， iBMC可将自身设备的MAC地址通过标准报文发送给直连设备，方便网络管理系统查询及判断链路通信状况。 默认值：关闭
工作模式	iBMC当前仅支持发送LLDP报文，不接收LLDP报文。

参数	说明
发送延迟(秒)	在当前工作模式下， iBMC本地配置(主要为切换管理网口或插拔管理网口网线)发生变化时，会发送LLDP报文通知邻居设备。 为防止本地信息频繁变化从而引起LLDP报文的大量发送，LLDP服务定义了一个延迟时间(单位为秒)，在延迟时间内，检测到iBMC本地配置有变化时，则重新计时，到达延迟时间后，再发送下一个LLDP报文。 取值范围： 1 ~ 8192 默认值： 2
发送周期(秒)	当前工作模式下，若本地信息无变化， iBMC会周期性地向邻居发送LLDP报文，单位为秒。 取值范围： 5 ~ 32768 默认值： 30
邻居节点时间保持倍数	若邻居节点在指定时间内(发送周期×邻居节点时间保持倍数)未收到iBMC的LLDP报文，则自动清除之前保留的报文信息。 取值范围： 2 ~ 10 默认值： 4

3.8.2 时区&NTP

功能介绍

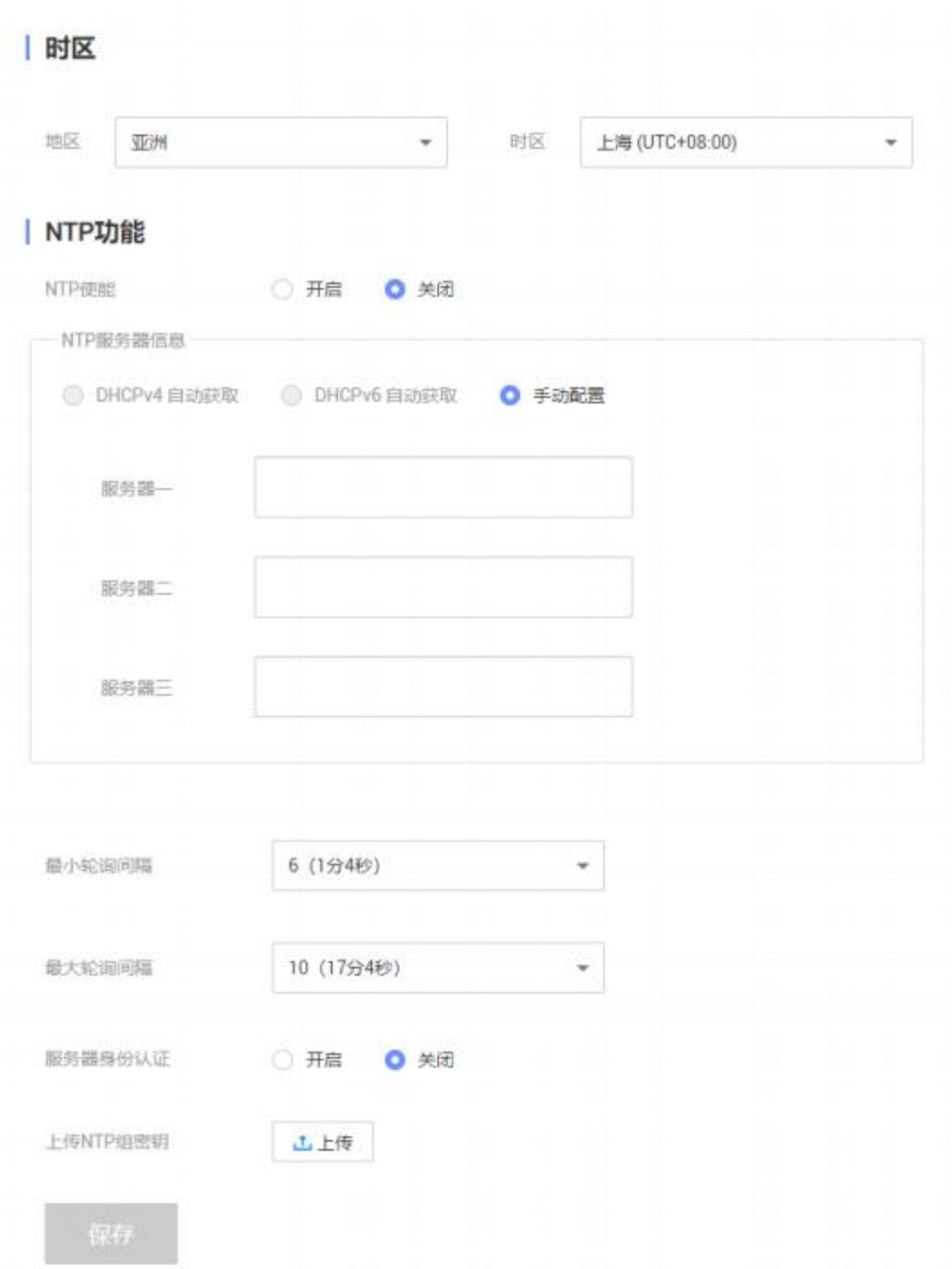
通过使用“时区&NTP”界面的功能，您可以查询和设置：

- iBMC系统时区。
- NTP信息。

界面描述

在导航栏中选择“iBMC管理 > 时区&NTP”，打开如**图3-56**所示界面。

图 3-56 NTP&时区


时区
地区
亚洲
时区
上海 (UTC+08:00)
NTP功能
NTP使能
开启
关闭
NTP服务器信息
DHCPv4 自动获取
DHCPv6 自动获取
手动配置
服务器一
服务器二
服务器三
最小轮询间隔
6（1分4秒）
最大轮询间隔
10（17分4秒）
服务器身份认证
开启
关闭
上传NTP组密钥
上传
保存

参数说明

表 3-62 时区&NTP

参数	描述
时区	iBMC系统的时区。 时区信息由“地区”和“时区”组成。 默认值：“其他”+“UTC” **说明** ● 当选择“DHCPv4自动获取“NTP信息时，不需要设置时区信息。 ● 在支持夏令时的时区， iBMC时间会在每年开始夏令时时自动调快1小时，结束夏令时时自动调慢1小时。 ● 在操作系统中执行时间同步时，为了保证操作系统时间与iBMC时间一致，请执行命令**hwclock --utc -w**。
NTP使能	使能或禁止iBMC的NTP功能。使能NTP服务后， iBMC系统时间可从NTP服务器同步。
DHCPv4自动获取	无需手动操作， iBMC系统自动获取基于IPv4的NTP信息。 **须知** iBMC管理网口的IP地址获取模式为自动获取时， NTP信息获取方式也必须选择自动获取。
DHCPv6自动获取	无需手动操作， iBMC系统自动获取基于IPv6的NTP信息。 **须知** iBMC管理网口的IP地址获取模式为自动获取时， NTP信息获取方式也必须选择自动获取。
手动配置	选择手动设置NTP信息后，用户可以手动配置首选NTP服务器地址和备用NTP服务器地址。 **须知** iBMC管理网口的IP地址获取模式为手动配置时， NTP信息获取方式也必须选择手动配置。

参数	描述
首选服务器一~三或备选服务器一~三	优先选择的NTP服务器的地址。 取值范围： IPv4地址、 IPv6地址和域名 **说明** 域名的取值原则： ● 最大长度为67个字符。 ● 可由数字、大小写英文字母和连接号(-)，点号(.)组成。 ● 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 ● 任意两个点号之间的字符长度不允许超过63。 提供两种选择方案。具体方案请以实际界面为准。 ● 方案一：提供三个NTP服务器。实际使用时，三个服务器地址同时生效。 ● 方案二：提供三组NTP服务器，每组服务器中，左侧为首选服务器，右侧为备选服务器。实际使用时，按照以下优先级规则选择服务器地址： – 分别从每组中选择一个服务器地址。 – 当某组两个服务器地址均无效时，放弃选择该组服务器地址。 – 当某组只有一个服务器地址有效时，选择有效服务器地址。 – 当某组两个服务器地址均有效时，优先选择IPv6地址。如果均为IPv4或IPv6地址，则优先选择首选服务器地址。 **说明** NTP主备服务器的切换与iBMC和NTP服务器之间的同步时间间隔(最小轮询间隔 ≤ 同步时间间隔 ≤ 最大轮询间隔)有关，当iBMC多次与主用服务器同步无响应时， NTP服务器将切换为备用服务器。
最小轮询间隔	iBMC系统从NTP服务器进行时间同步的最小周期，即NTP报文的最小轮询间隔时间。 如最小轮询间隔为6，表示间隔时间为2的6次方秒，即1分4秒。 取值范围： 3 ~ 17
最大轮询间隔	iBMC系统从NTP服务器进行时间同步的最大周期，即NTP报文的最大轮询间隔时间。 如最大轮询间隔为6，表示间隔时间为2的6次方秒，即1分4秒。 取值范围： 3 ~ 17
服务器身份认证	iBMC系统与NTP服务器通信时，是否需要进行身份认证。 默认值：关闭

参数	描述
上传NTP组密钥	当开启服务器身份认证时，需要上传密钥到iBMC，用于与NTP服务器通信时的身份认证。 **说明** • 您可以自行下载密钥生成器(例如ntp-keygen)生成所需密钥。 • 仅支持上传SHA256算法生成的秘钥文件。 • 请定期更新秘钥，否则可能存在安全风险。

设置时区

步骤1 在“地区”和“时区”下拉列表中，选择要设置的参数。

步骤2 单击“保存”。

显示“操作成功”表示设置成功。

说明

在操作系统中执行时间同步时，为了保证操作系统时间与iBMC时间一致，请执行命令**hwclock --utc -w**。

----结束

配置 NTP 信息

步骤1 在“NTP功能”区域框中，根据**表3-62**提供的参数信息，设置NTP信息。

步骤2 单击“保存”。

显示“操作成功”表示设置成功。

----结束

3.8.3 固件升级

功能介绍

通过使用“固件升级”界面的功能，您可以：

- 查看版本信息。
- 重启iBMC系统。
- 进行可用分区镜像倒换。
- 进行服务器固件升级。

iBMC系统存在以下3个分区镜像：

- 主分区镜像： iBMC当前生效的分区。
- 备分区镜像：主分区镜像的备份，当主分区镜像异常时，备分区镜像自动切换为主分区镜像，原主分区镜像降备，并同步当前主分区镜像的版本，使得主、备分区镜像的版本保持一致。升级iBMC时会同时升级主、备分区镜像。
- 可用分区镜像：用作iBMC储备版本的承载，您可以通过“可用分区镜像倒换”功能，生效可用分区镜像的版本。此时，原可用分区镜像切换为主分区镜像，原主

分区同步新主分区镜像后切为备份分区镜像，原备分区镜像自动切换为可用分区镜像。

须知

- 在操作系统启动过程中，请不要重启iBMC、镜像倒换或升级iBMC固件。
- 为确保升级成功，升级过程中不允许断电、不允许重新启动iBMC系统。
- 升级iBMC固件需要重新启动iBMC系统使功能生效。但您不需要重新启动服务器。因此，服务器上运行的业务不会受到影响。
- 升级LCD固件和电源固件无需重新启动服务器。
- 在iBMC升级时，可以选择升级完成后立即自动重启使升级的固件生效；也可以在升级完成后，由用户自行重启iBMC来使之生效。
- 在SD卡固件升级完成之后， iBMC会自动重启，使升级的固件生效。
- 升级BIOS或CPLD前，建议先关闭服务器上运行的业务，避免服务器重新启动时中断业务。
- 如果在操作系统上电状态时升级BIOS或CPLD，则BIOS在操作系统下电再上电或重启后生效， CPLD在操作系统下电后生效。
- 如果在操作系统下电状态时升级BIOS或CPLD，则BIOS和CPLD在操作系统上电后生效。
- 服务器上电状态下升级BIOS时，在服务器已安装OS且OS在正常运行状态下，若服务器安装了TPM卡，且已设置TXT功能，则禁止强制重启或强制上下电服务器，需要进入OS重启操作系统使BIOS新版本生效。
- 服务器下电状态下升级BIOS时，在服务器已安装OS且OS在正常运行状态下，若服务器安装了TPM卡，且已设置TXT功能，则确保升级前是进入OS进行的下电服务器，禁止强制下电服务器。
- 当iBMC可用分区镜像与主分区镜像的版本不一致时，单击“可用分区镜像倒换”可能会对服务器上运行的业务产生影响，请谨慎操作。

界面描述

在导航栏中选择“iBMC管理 > 固件升级”，打开如图3-57所示界面。

图 3-57 固件升级

参数说明

表 3-63 固件升级

参数	描述
重启iBMC	重新启动iBMC系统使设置生效。
可用分区镜像倒换	将iBMC固件主分区的镜像文件切换到可用分区的镜像文件。
iBMC主用分区镜像版本	iBMC固件主用分区镜像的版本号。

参数	描述
iBMC备用分区镜像版本	iBMC固件备用分区镜像的版本号。
iBMC可用分区镜像版本	iBMC固件可用分区镜像的版本号。
BIOS版本	BIOS固件当前的版本号。
CPLD版本	CPLD固件当前的版本号。

查看固件版本

步骤1 在上方标题栏中选择“iBMC管理”。

步骤2 在左侧导航树中，选择“固件升级”。

右侧显示“固件升级”界面，界面中显示iBMC 、BIOS 、CPLD的版本信息。

----结束

升级 iBMC 固件

以下操作同时适用于升级iBMC系统的原主用镜像以及其他固件。

步骤1 单击固件升级区域框的 ... 并选择待上传的文件。

步骤2 单击“开始升级”。

弹出对话框提示以下信息：

```
是否确定执行此操作?
```

步骤3 单击“确定”。

iBMC系统开始执行升级操作。

升级成功后， iBMC将进入自动重启并跳转至登录页面。

请耐心等待几分钟，重启完成后将自动恢复到iBMC正常的登录页面。

----结束

切换 iBMC 固件的镜像文件

请您根据需要切换iBMC固件的镜像文件。此操作不是升级过程中的必做操作。

步骤1 在“固件升级”界面中，单击“可用分区镜像倒换”。

弹出对话框提示以下信息：

```
是否确定可用分区镜像倒换?
```

步骤2 单击“确定”。

切换成功后， iBMC将进入自动重启并跳转至登录页面。

请耐心等待几分钟，重启完成后将自动恢复到iBMC正常的登录页面。

----结束

重启 iBMC

请您根据需要重启iBMC。此操作不是升级过程中的必做操作。

步骤1 在“固件升级”界面中，单击“重启iBMC”。

弹出对话框提示以下信息：

是否确定重启iBMC?

步骤2 单击“确定”。

iBMC开始重启并跳转至登录页面。

请耐心等待几分钟，重启完成后将自动恢复到iBMC正常的登录页面。

----结束

3.8.4 许可证管理

功能介绍

通过“许可证管理”界面，可实现以授权方式使用iBMC高级版的特性。许可证在有效期内，用户才能使用高级版的iBMC，否则只能使用默认的标准版本。

iBMC高级版较标准版提供更多的高级特性，例如：

- 通过Redish实现OS部署。
- 通过Redish收集智能诊断的原始数据。

界面描述

在导航栏中选择“iBMC管理 > 许可证管理”，打开如图3-62所示界面。

图 3-62 许可证管理

参数说明

表 3-65 许可证管理

参数	描述
设备ESN	用于申请许可证的ESN，由主板的序列号生成。
安装许可证	安装许可证。 **说明** 不能安装已经执行过“失效”操作的许可证，安装时会提示安装失败。
失效	使许可证失效。 许可证失效后进入宽限期并且可以从界面获得许可证的失效码。例如用户需要更换备件，您需要执行“失效”操作来获取失效码，凭此失效码申请新的许可证后，将许可证安装到备件。 **说明** 不能安装已经执行过“失效”操作的许可证，请谨慎操作。
导出	导出已经安装的许可证。 用户可以导出许可证并进行备份。
删除	删除许可证。

参数	描述
许可证状态	许可证的状态包括： ● 正常状态：已安装商用许可证，许可证未过期，所有授权特性为正常状态。 ● 调测状态：已安装调测许可证，许可证未过期，所有授权特性为正常状态。 ● 宽限状态：已安装商用或调测许可证，许可证已过期且在宽限期内，所有授权特性进入宽限状态。 ● 默认状态：已安装商用或调测许可证，但是许可证已过期且已过宽限期。
失效码	在已安装许可证的情况下，执行许可证“失效”操作后生成的失效凭证，用户可以凭此失效码申请新的许可证。
许可证信息	许可证的信息包括： ● 许可证序列号 ● 许可证类型：提供两种许可证类型。 – 商用：基于合同发放给客户的正式许可证，所有授权特性的截止日期一致，授权特性截止日期为永久或某个具体时间，过期后自动进入宽限期，宽限天数为60天。 – 试用：用于新特性试用、客户现场设备调测或品牌展览的临时许可证，有效使用时间根据实际情况而定，过期后自动进入宽限期，宽限天数为60天。 ● 许可证级别： – 标准版(默认)：默认版本，无需用户自行购买。 – 高级版：以授权方式提供较标准版更多的特性，需要用户自行购买。 ● 截止日期：授权特性授权截止的日期，可以是永久或某个具体时间。 **说明** 许可证过期后的宽限期表示许可证过期后，仍可以使用iBMC的天数。宽限天数固定为60天。
高级特性	显示许可证高级特性，包括序号、特性名称、特性状态、当前状态和使用截止日期。

3.9 虚拟控制台

功能介绍

通过使用虚拟控制台的功能，您可以查看HTML5集成远程虚拟控制台或Java集成远程控制台接入服务器的操作系统进行操作。

界面描述

在导航栏中选择“首页”，从如图3-67所示界面进入虚拟控制台。

图 3-67 虚拟控制台

参数说明

表 3-71 虚拟控制台

参数	描述
HTML5集成远程控制台	HTML5集成远程控制台支持以下两种模式： ● 独占模式下只能有1个本地用户或VNC用户通过iBMC连接到服务器操作系统。 ● 共享模式下可以让2个本地用户或5个VNC用户同时通过iBMC连接到服务器操作系统，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。 HTML5控制台提供功能如下： ● 通过浮动按钮、屏幕缩放按钮、多种鼠标按钮、图像清晰度游标，提供便捷的屏幕显示设定功能。 ● 通过组合键按钮、键盘布局按钮，提供输入设备设定功能。 ● 通过电源控制按钮、录像按钮，提供服务器操作系统控制功能。 ● 通过光驱、软驱按钮，提供镜像文件挂载功能，以及本地文件挂载功能。

参数	描述
Java集成远程虚拟控制台	Java集成远程虚拟控制台支持以下两种模式： ● 独占模式下只能有1个本地用户或VNC用户通过iBMC连接到服务器操作系统。 ● 共享模式下可以让2个本地用户或5个VNC用户同时通过iBMC连接到服务器操作系统，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。 Java控制台提供功能如下： ● 通过浮动按钮、屏幕缩放按钮、多种鼠标按钮、图像清晰度游标，提供便捷的屏幕显示设定功能。 ● 通过组合键按钮、键盘指示灯、键盘布局按钮，提供输入设备查询和设定功能。 ● 通过电源控制按钮、录像按钮，提供服务器操作系统控制功能。 ● 通过光驱、软驱按钮，提供物理光驱、物理软驱、镜像文件的挂载功能，以及本地文件夹挂载功能。 ● 通过镜像文件制作按钮，提供光驱、软件的镜像文件的制作接口。

运行环境

使用远程虚拟控制台需要具备以下版本的操作系统、浏览器和Java运行环境，如**表3-72**所示。

说明

- Java远程虚拟控制台依赖于Java运行环境，如未安装，可通过“下载”链接登录AdoptOpenJDK的官方网站下载安装；如安装后仍不能使用，可通过“更多信息”链接获取帮助。
- 当在“用户&安全 > 安全配置”界面将TLS版本配置为“仅限TLS 1.3协议”时， iBMC运行环境不支持以下浏览器版本：
  - Internet Explorer所有版本
  - Safari 9.0 ~ 12.0
  - Microsoft Edge 12 ~ 18
  - Mozilla Firefox 45.0 ~ 62.0
  - Google Chrome 55.0 ~ 69.0

表 3-72 运行环境

操作系统	浏览器	Java运行环境
Windows 7 32位 Windows 7 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	

操作系统	浏览器	Java运行环境
	Google Chrome 55.0 ~ 84.0	
Windows 8 32位 Windows 8 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows 10 64位	Internet Explorer 11.0 Microsoft Edge	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2008 R2 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2012 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2012 R2 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
Windows Server 2016 64位	Internet Explorer 11.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	
	Google Chrome 55.0 ~ 84.0	
CentOS 7	Mozilla Firefox 45.0 ~ 79.0	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE

操作系统	浏览器	Java运行环境
MAC OS X v10.7	Safari 9.0 ~ 13.1	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0 ~ 79.0	

进入集成远程控制台

说明

在远程虚拟控制台中输入OS或BIOS密码时：

- 如果操作系统的键盘设置与实际使用的键盘一致，则可按照实际键盘上的字符进行输入。
- 如果操作系统的键盘设置与实际使用的键盘不一致，则按照操作系统键盘设置中键盘字符进行输入。

登录时可能会弹出“安全告警”界面，您可以选择忽略此告警信息或根据需要执行以下操作屏蔽该界面：

- 如果您有可信任的证书，可以为iBMC导入信任证书和根证书。有关详细信息，请参见**6.11 为iBMC导入信任证书和根证书**。
- 如果您没有可信任的证书，且可以保证网络安全的情况下，可以在Java的安全列表中将iBMC添加为例外站点或降低Java安全级别。由于该操作可能降低用户的安全性，请谨慎使用。

- **(常规入口)** 在“首页”界面中，单击“启动虚拟控制台”区域框，从弹出的下拉列表中选择“Java集成远程控制台”或“HTML5集成远程控制台”。
  共享模式可以让2个用户连接到服务器，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。
  独占模式只能有1个用户连接到服务器进行操作。选择独占模式方式进入实时桌面后，“维护诊断 > 录像截屏”界面中的“屏幕截图”区域框中的“手动屏幕截屏”按钮无法使用，自己或其他人此时均不能截图。
- **(快捷入口)** 打开Internet Explorer浏览器，并在地址栏中输入：
  - 方式一：
    - HTML5集成远程控制台推荐登录方式：
      - “https://*IPaddress*/remoteconsole?openWay=html5”或“https://*IPaddress*/remoteconsole?openway=html5”
      - “https://*IPaddress*/remote_access.asp?authParam=*key*&lp=*lang*&openWay=html5”或“https://*IPaddress*/remote_access.asp?authParam=*key*&lp=*lang*&openway=html5”
    - Java集成远程控制台推荐登录方式：
      - “https://*IPaddress*/remoteconsole”或“https://*IPaddress*/remoteconsole?openWay=jre”或“https://*IPaddress*/remoteconsole?openway=jre”
      - “https://*IPaddress*/remote_access.asp?authParam=*key*&lp=*lang*&openWay=jre”或“https://*IPaddress*/remote_access.asp?authParam=*key*&lp=*lang*&openway=jre”

说明

- *key*可通过Redish接口设置，使用key可直接进行KVM连接。
- *lp*表示控制台使用的语言类别。
- openWay参数仅支持“openway”和“openWay”两种式样，若使用其余写法，会跳转至Java控制台。

– 方式二：“https://*IPaddress*/kvmvmm.asp”
– 方式三：“https://*IPaddress*/login.html?redirect_type=1 ”

说明

“*IPaddress*”为iBMC管理网口的IP地址。

3.9.1 HTML5 集成远程控制台

功能介绍

通过使用HTML5集成远程控制台提供的功能，您可以远程连接到服务器完成远程控制、管理服务器，安装、修复操作系统、安装设备驱动程序等操作。

- 您可以在本地PC上利用键盘和鼠标对远程的服务器进行远程实时操作。
- 您可以通过网络使服务器以虚拟软驱或光驱的形式实现对本地PC的远程访问。从服务器一侧看，虚拟软驱或光驱与实际插入服务器的(USB ， Universal Serial Bus)设备的使用方法相同。

“KVM”窗口中的按钮及其作用如**表3-73**所示。

表 3-73 按钮说明

按钮	说明
	浮动按钮。表示当前工具栏被固定。
	浮动按钮。表示当前工具栏被隐藏。
	“全屏”按钮。表示全屏显示服务器的实时桌面。
	“退出全屏”按钮。表示取消全屏显示服务器的实时桌面。
	“控制”按钮。表示控制服务器电源。操作包括： ● 上电 ● 强制下电 ● 下电 ● 强制重启 ● 强制下电再上电

按钮	说明
	“系统启动项”按钮。表示设置操作系统的第一启动设备。操作包括： ● 未配置：表示不设置第一启动设备，按BIOS中设置的默认方式启动操作系统。 ● 硬盘：表示强制从硬盘启动系统。 ● 光驱：表示强制从CD/DVD启动系统。 ● 软驱/可拔插移动设备：表示强制从软驱或可拔插移动设备启动系统。 ● PXE：表示强制从预启动执行环境(PXE，Pre-boot Execution Environment)启动系统。 ● BIOS设置：表示服务器启动后直接进入BIOS菜单中。
	“键盘组合键”按钮。表示发送或自定义特殊组合键。该窗口中的组合键及其含义包括： ● Alt+Tab：在打开的项目中进行切换。 ● Ctrl+Esc：显示或收起“开始”菜单。 ● Ctrl+Shift：切换输入法。 ● Ctrl+Space：开启或关闭输入法。 ● Ctrl+Alt+Del：锁定操作系统界面、注销用户、更改密码和打开任务管理器、重新启动服务器等。 ● 自定义按键：如果您需要自定义组合键，请在“自定义按键”后的文本框中依次输入按键，然后单击“确定”。 **说明** 在不同的操作系统中，操作系统各自定义的组合键及其含义不同。该窗口中的组合键及其含义仅适用于Windows操作系统。
	“鼠标控制”按钮。表示控制服务器鼠标。操作包括： ● 鼠标加速 加速服务器实时桌面上的鼠标，使其与本地PC上的鼠标同步。 **说明** 低于SUSE 12版本的SUSE操作系统不支持鼠标加速功能。 ● 单鼠标 隐藏本地PC上的鼠标，只显示服务器实时桌面上的鼠标。 ● 键鼠复位 模拟插拔USB键盘和USB鼠标，服务器实时桌面上的键盘鼠标出现异常停滞时单击此按钮可以恢复。 默认的操作：鼠标加速 **说明** ● 鼠标加速和单鼠标均未勾选时，服务器实时桌面鼠标和本地PC鼠标同时显示，且服务器实时桌面鼠标不跟随本地PC鼠标。 ● iBMA驱动盘连接状态下，执行鼠标控制操作会中断此连接。请先断开iBMA驱动盘连接，再执行鼠标控制操作。

按钮	说明
	“CD/DVD”按钮。表示选择并使用虚拟光驱。 **说明** 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟光驱时，服务器会同时识别到一个无介质的虚拟软驱设备。按照正常操作方式可继续使用虚拟软驱功能。
	“软驱”按钮。表示选择并使用虚拟软驱。 **说明** 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟软驱时，服务器会同时识别到一个无介质的虚拟光驱设备。按照正常操作方式可继续使用虚拟光驱功能。
	“录像”按钮。表示对远程实时操作进行录像。
	“键盘布局”按钮。表示客户端的键盘类型。默认情况下，iBMC自动适配客户端的键盘类型。当自适应模式下键盘适配情况不理想时，请强制指定目标键盘类型。 ● “美式键盘”：强制指定键盘类型为美式键盘。 ● “日式键盘”：强制指定键盘类型为日式键盘。 ● “法式键盘”：强制指定键盘类型为法式键盘。 ● “意式键盘”：强制指定键盘类型为意式键盘。 ● “德式键盘”：强制指定键盘类型为德式键盘。
	“帮助”按钮。表示查看KVM页面联机帮助。
	“图像清晰度”游标图标。表示调节远程实时图像的清晰度。

界面描述

在上方标题栏中选择“首页”，在“启动虚拟控制台”右侧的下拉列表中选择“HTML5集成远程控制台(独占)”或“HTML5集成远程控制台(共享)”，跳转至“KVM”页面。

说明

单击“HTML5集成远程控制台(共享)”的情况下，本用户可以看到对方用户的操作，对方用户也能看到本用户的操作，有一定安全风险。

HTML5 KVM窗口各区域的功能介绍如**表3-74**所示。

图 3-68 HTML5 KVM

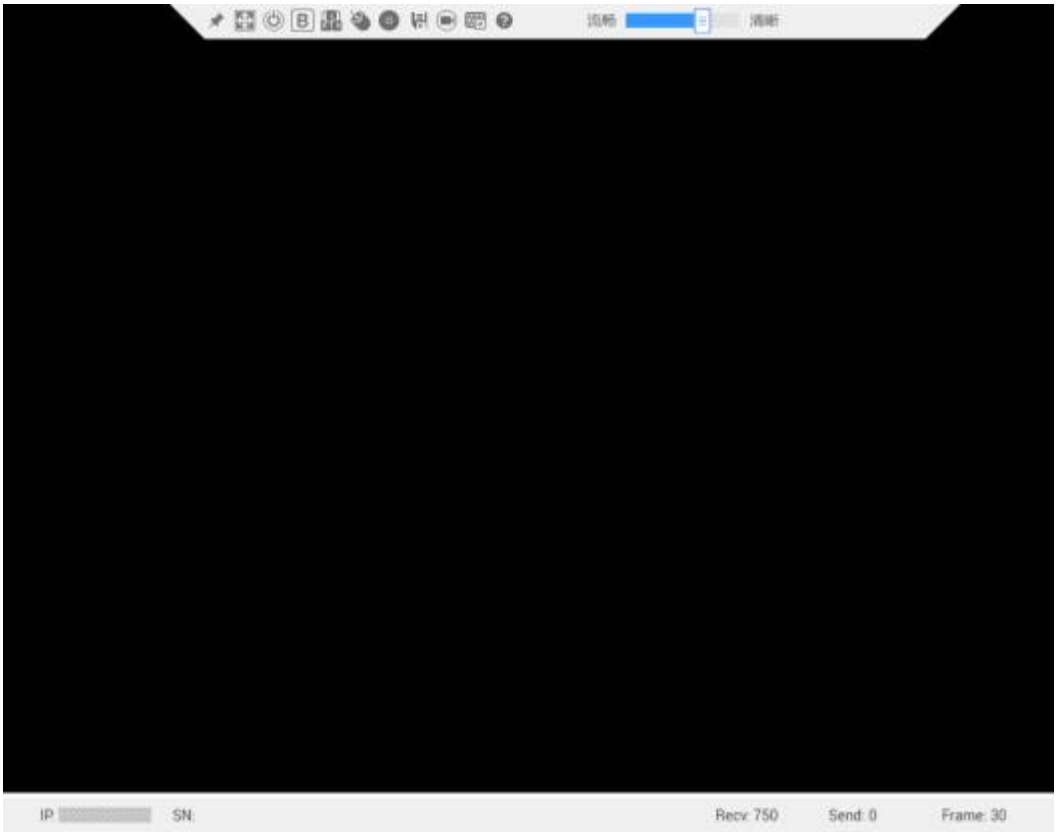


表 3-74 HTML5 KVM

区域	功能
工具栏(顶部)	显示您可以对服务器进行远程执行的所有操作。
实时桌面(中部)	显示服务器的实时桌面。您可以在实时桌面中用鼠标操作或执行命令。
状态栏(底部)	显示实时桌面的提示信息，以及服务器与本地PC之间的通信数据、 IP地址和服务器的产品序列号。

操作步骤

为服务器上电

步骤1 在“KVM”界面中，单击工具栏上的 ，在快捷菜单中选择“上电”。

步骤2 单击“确定”。

服务器开始上电。

说明

服务器上电需要的时间根据服务器配置所不同。

----结束

为服务器下电

须知

- 请在下电前确认无中断当前业务风险。
- 请根据实际情况选择下电方式，“强制下电”和“下电”的区别请参考iBMC用户指南的“系统管理 > 电源&功率”章节。

步骤1 在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“强制下电”或“下电”。

步骤2 单击“确定”。

服务器开始下电。

----结束

强制重启或强制下电再上电

须知

- 强制重启或强制下电再上电可能会损坏用户的程序或者未保存的数据，请根据操作系统实际情况谨慎选择操作方式。
- 请在强制重启或强制下电再上电前确认无中断当前业务风险。
- 请根据实际情况选择“强制重启”或“强制下电再上电”，“强制重启”和“强制下电再上电”的区别请参考iBMC用户指南的“系统管理> 电源&功率”章节。

步骤1 在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“强制重启”或“强制下电再上电”。

步骤2 单击“确定”。

服务器开始强制重启或强制下电再上电。

说明

服务器强制重启或强制下电再上电需要的时间根据服务器配置所不同。

----结束

设置操作系统的第一启动设备

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出启动设备列表。

步骤2 根据表3-73提供的参数信息，单击需要设置的启动设备。

成功设置服务器操作系统的第一启动设备。

----结束

发送特殊组合键

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出组合键快捷菜单。

步骤2 根据表3-73提供的参数信息，单击需要发送的组合键。

服务器将执行组合键对应的操作。

说明

如果您需要自定义组合键，请在“自定义按键”后的文本框中依次输入按键，然后单击“确定”。

----结束

加速远程鼠标

本操作对实时桌面上的鼠标进行加速，使其与本地PC上的鼠标同步。

在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“鼠标加速”。

同步本地PC与服务器的鼠标。

使用单鼠标

如果本地PC上的鼠标与实时桌面上的不同步，您可以使用单鼠标功能隐藏本地PC上的鼠标。“KVM”界面中只保留实时桌面上的鼠标。

在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“单鼠标”。

“KVM”界面中只显示实时桌面上的鼠标。

键鼠复位

本操作模拟插拔USB键盘和USB鼠标。

在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“键鼠复位”。

服务器开始执行USB复位操作。

指定客户端的键盘类型

在“KVM”界面中，单击工具栏上的  。

从下拉列表中选择目标键盘类型，则成功强制指定键盘类型。

通过虚拟光驱挂载镜像文件

本操作使用本地PC上的光盘镜像文件虚拟出另一个光驱提供给服务器，并将光盘镜像文件加载到该虚拟光驱中。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-69的界面。

图 3-69 通过虚拟光驱挂载镜像文件

步骤2 选中“镜像文件”单选按钮。

步骤3 单击  。

打开本地文件夹选择窗口。

步骤4 选择本地PC上存放的“*.iso”格式镜像文件，单击“连接”。

返回如图3-69所示的界面。

服务器上成功挂载镜像文件。

说明

- 挂载镜像文件成功后，单击“弹出”，弹出光盘镜像文件；弹出光盘镜像文件后，可重新选择其他“*.iso”格式的镜像文件，然后单击“插入”，挂载该镜像文件。
- 挂载镜像文件成功后，单击“断开”，卸载服务器上的虚拟光驱。

----结束

挂载本地文件

本操作将本地PC上的文件挂载到服务器，使服务器系统可以以只读方式访问本地文件。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-70的界面。

图 3-70 挂载本地文件

步骤2 选中“本地文件”单选按钮。

步骤3 单击  。

打开本地文件选择窗口。

步骤4 选择要挂载的本地文件。

返回如图3-70所示的界面。

步骤5 单击“连接”。

服务器上成功挂载本地文件。

说明

- 连接成功后，在服务器操作系统中，可以看到虚拟文件。
- 连接成功后，单击“断开”，可以卸载虚拟文件。

----结束

通过虚拟软驱挂载镜像文件

本操作使用本地PC上的软盘镜像文件虚拟出另一个软驱提供给服务器，并将软盘镜像文件加载到该虚拟软驱中。

说明

挂载的镜像文件大小必须为1.44MB，否则会导致挂载失败。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-71所示的界面。

图 3-71 通过虚拟软驱挂载镜像文件

步骤2 单击  。

打开本地文件夹选择窗口。

步骤3 选择本地PC上存放的“*.img”格式镜像文件，单击“连接”。

返回如图3-71所示的界面。

步骤4 单击“连接”。

服务器上成功挂载镜像文件。

说明

- 挂载镜像文件成功后，单击“弹出”，弹出镜像文件；弹出软盘镜像文件后，可重新选择其他“*.img”格式镜像文件，然后单击“插入”，挂载该镜像文件。
- 单击“断开”，可以卸载服务器上的虚拟软驱。

----结束

为实时桌面录像

本操作对当前远程虚拟控制台显示的画面进行录像。

录制的录像文件格式为“*.rep”。可在“录像回放”界面中播放录像文件和对录像进行截图。

步骤1 在“KVM”界面中，单击工具栏上的  ，按钮状态切换为  时，开始对实时桌面进行录像。

步骤2 录制完成后，单击  。

录像文件将自动被下载并保存到本地PC。

录制的录像文件格式为“*.rep”。可在“录像回放”界面中播放录像文件和对录像进行截图。

----结束

3.9.2 Java 集成远程控制台

功能介绍

通过使用Java集成远程控制台提供的功能，您可以远程连接到服务器完成远程控制、管理服务器，安装、修复操作系统或安装设备驱动程序等操作。

- 您可以在本地PC上利用键盘和鼠标对远程的服务器进行远程实时操作。
- 您可以通过网络使服务器以虚拟软驱或光驱的形式实现对本地PC的远程访问。从服务器一侧看，虚拟软驱或光驱与实际插入服务器的(USB， Universal Serial Bus)设备的使用方法相同。

“KVM”窗口中的按钮及其作用如**表3-75**所示。

表 3-75 按钮说明

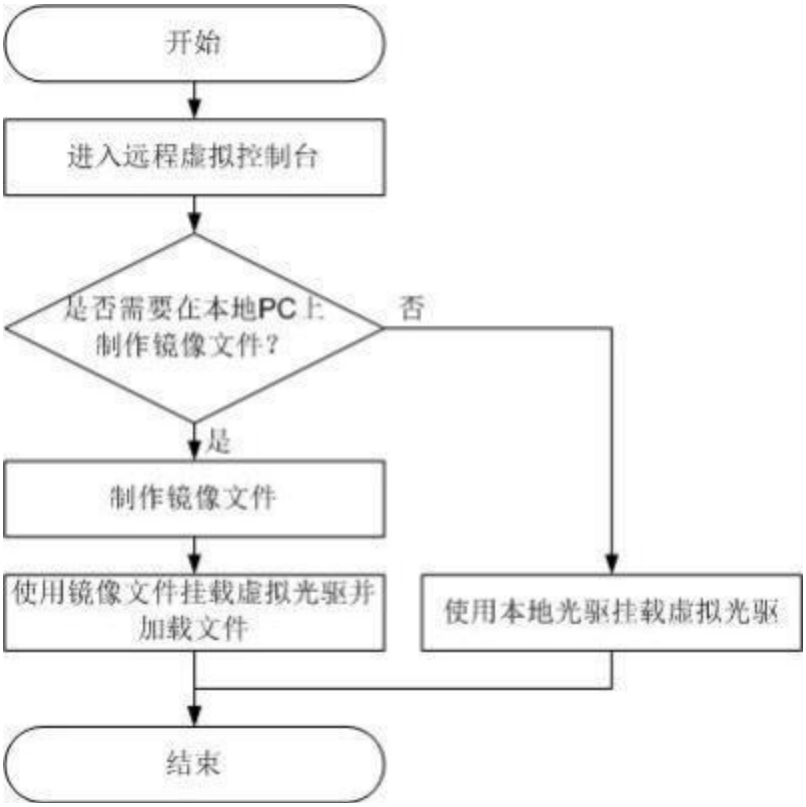
按钮	说明
	浮动按钮。表示当前工具栏被固定。
	浮动按钮。表示当前工具栏被隐藏。
	“全屏”按钮。表示全屏显示服务器的实时桌面。 **说明** 在全屏显示实时桌面时，鼠标移动到屏幕上方会显示工具栏。
	“鼠标同步”按钮。表示纠正鼠标位置。 **说明** 在全屏显示实时桌面且“鼠标控制”为“单鼠标”模式时，此时单击“切换鼠标模式”后，该按钮才可用。
	“切换鼠标模式”按钮。表示切换鼠标模式。 **说明** 在全屏显示实时桌面且在“单鼠标”模式下时，该按钮才可用。

按钮	说明
	“返回”按钮。表示返回合适的屏幕显示服务器的实时桌面。 **说明** 只有全屏显示服务器的实时桌面时，工具栏中才会出现该按钮。
	“控制”按钮。表示控制服务器电源。操作包括： ● 上电 ● 强制下电 ● 下电 ● 强制重启 ● 强制下电再上电
	“录像”按钮。表示对远程实时操作进行录像。
	“鼠标控制”按钮。表示控制服务器鼠标。操作包括： ● 鼠标加速 加速服务器实时桌面上的鼠标，使其与本地PC上的鼠标同步。 **说明** 低于SUSE 12版本的SUSE操作系统不支持鼠标加速功能。 ● 单鼠标 隐藏本地PC上的鼠标，只显示服务器实时桌面上的鼠标。 ● 键鼠复位 模拟插拔USB键盘和USB鼠标，服务器实时桌面上的键盘鼠标出现异常停滞时单击此按钮可以恢复。 默认的操作：鼠标加速 **说明** ● 鼠标加速和单鼠标均未勾选时，服务器实时桌面鼠标和本地PC鼠标同时显示，且服务器实时桌面鼠标不跟随本地PC鼠标。 ● iBMA驱动盘连接状态下，执行鼠标控制操作会中断此连接。请先断开iBMA驱动盘连接，再执行鼠标控制操作。
	“CD/DVD”按钮。表示选择并使用虚拟光驱。 **说明** 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟光驱时，服务器会同时识别到一个无介质的虚拟软驱设备。按照正常操作方式可继续使用虚拟软驱功能。
	“软驱”按钮。表示选择并使用虚拟软驱。 **说明** 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟软驱时，服务器会同时识别到一个无介质的虚拟光驱设备。按照正常操作方式可继续使用虚拟光驱功能。
	“制作镜像文件”按钮。表示使用光驱或软驱制作镜像文件。

按钮	说明
	“键盘组合键”按钮。表示发送或自定义特殊组合键。该窗口中的组合键及其含义包括： ● Ctrl+Shift：切换输入法。 ● Ctrl+Esc：显示或收起“开始”菜单。 ● Ctrl+Alt+Del：锁定操作系统界面、注销用户、更改密码和打开任务管理器、重新启动服务器等。 ● Alt+Tab：在打开的项目中进行切换。 ● Ctrl+Space：开启或关闭输入法。 ● ResetKeyboad：模拟弹起键盘上的按键。 ● 自定义：如果您需要自定义组合键，请在“自定义”后的文本框中依次输入按键，然后单击“发送”。 **说明** 在不同的操作系统中，操作系统各自定义的组合键及其含义不同。该窗口中的组合键及其含义仅适用于Windows操作系统。
	“键盘布局”按钮。表示客户端的键盘类型。默认情况下，iBMC自动适配客户端的键盘类型。当自适应模式下键盘适配情况不理想时，请强制指定目标键盘类型。 ● “美式键盘”：强制指定键盘类型为美式键盘。 ● “日式键盘”：强制指定键盘类型为日式键盘。 ● “法式键盘”：强制指定键盘类型为法式键盘。 ● “意式键盘”：强制指定键盘类型为意式键盘。 ● “德式键盘”：强制指定键盘类型为德式键盘。
图像清晰度	“图像清晰度”游标图标。表示调节远程实时图像的清晰度。
	“Num Lock”(数字键盘开关)键的指示灯。表示当前服务器上“Num Lock”键的指示灯状态。
	“Caps Lock”(键盘大写锁定)键的指示灯。表示当前服务器上“Caps Lock”键的指示灯状态。
	“Scroll Lock”(键盘滚动锁定)键的指示灯。表示当前服务器上“Scroll Lock”键的指示灯状态。进入Linux字符模式，如果按下了Ctrl+s (大多数情况下属于误按)，此时屏幕会锁住，按下键盘上的“Scroll Lock”键可以解锁屏幕。 **说明** ● 通过KVM操作服务器时，如果键盘输入异常，请先检查KVM中服务器键盘指示灯状态是否正确。 ● “Scroll Lock”键的指示灯需要操作系统支持才能点亮，某些操作系统可能无法点亮。
	“帮助”按钮。表示查看KVM页面联机帮助。
注：不同型号的服务器，提供的功能不完全相同，请以实际界面为准。	

以光驱为例，工具栏中的镜像文件、虚拟光驱和虚拟软驱的使用流程如图3-72所示。

图 3-72 使用流程



界面描述

在上方标题栏中选择“首页”，在“启动虚拟控制台”右侧的下拉列表中选择“Java集成远程控制台(独占)”或“Java集成远程控制台(共享)”，跳转至“KVM ”页面。

说明

单击“Java集成远程控制台(共享)”的情况下，本用户可以看到对方用户的操作，对方用户也能看到本用户的操作，有一定安全风险。

Java KVM窗口各区域的功能介绍如**表3-76**所示。

图 3-73 Java KVM

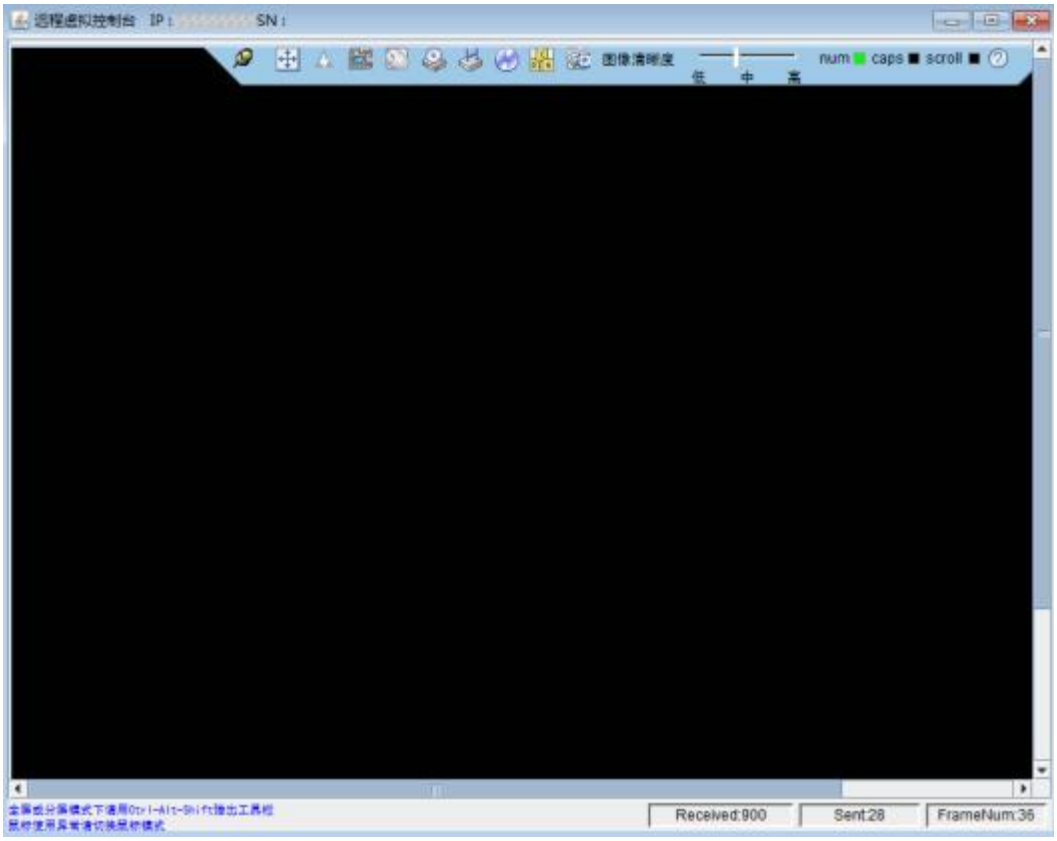


表 3-76 Java KVM

区域	功能
标题栏	KVM界面的顶部标题栏显示iBMC的IP地址和服务器的产品序列号。
工具栏(顶部)	显示您可以对服务器进行远程执行的所有操作。
实时桌面(中部)	显示服务器的实时桌面。您可以在实时桌面中用鼠标操作或执行命令。
状态栏(底部)	显示实时桌面的提示信息，以及服务器与本地PC之间的通信数据。

操作步骤

发送特殊组合键

步骤1 在“KVM”界面中，单击工具栏上的。

弹出组合键窗口。

步骤2 根据表3-75提供的参数信息，单击需要发送的组合键。

服务器将执行组合键对应的操作。

说明

如果您需要自定义组合键，请在“自定义”后的文本框中依次输入按键，然后单击“发送”。

----结束

指定客户端的键盘类型

在“KVM”界面中，单击工具栏上的  。从下拉列表中选择目标键盘类型。则成功强制指定键盘类型。

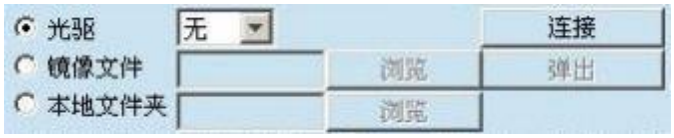
挂载虚拟光驱

本操作使用本地PC上的光盘驱动器虚拟出另一个光盘驱动器提供给服务器。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-74所示的界面。

图 3-74 挂载虚拟光驱



步骤2 选中“光驱”单选按钮。

步骤3 在下拉列表中，选择本地PC上待虚拟的光盘驱动器，例如“G:”。

步骤4 单击“连接”。

服务器上成功挂载虚拟光驱。

说明

挂载成功后，单击“断开”，在弹出的“选择一个选项”对话框中单击“是”，卸载服务器上的虚拟光驱。

----结束

通过虚拟光驱挂载镜像文件

本操作使用本地PC上的光盘镜像文件虚拟出另一个光驱提供给服务器，并将光盘镜像文件加载到该虚拟光驱中。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-74所示的界面。

步骤2 选中“镜像文件”单选按钮。

步骤3 单击“浏览”。

弹出“打开”窗口。

步骤4 选择本地PC上存放的光盘镜像文件，单击“打开”。

返回如图3-74所示的界面。

步骤5 单击“连接”。

服务器上成功挂载镜像文件。

说明

- 挂载镜像文件成功后，单击“弹出”，弹出镜像文件；弹出镜像文件后，可重新选择其他“*.iso”格式的镜像文件，然后单击“插入”，加载该镜像文件。
- 挂载镜像文件功后，单击“断开”，在弹出的“选择一个选项”对话框中单击“是”，卸载服务器上的虚拟光驱。

----结束

挂载虚拟软驱

本操作使用本地PC上的软驱或软盘镜像文件虚拟出另一个软驱提供给服务器。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-75所示的界面。

图 3-75 挂载虚拟软驱

步骤2 选中“软驱”单选按钮。

步骤3 在下拉列表中，选择本地PC上待虚拟的软盘驱动器，例如“A:”。

步骤4 勾选“写保护”复选框。

说明

写保护是指软驱禁止写入数据。它是一种防止重要数据被更改或被删除的保护机制。

步骤5 单击“连接”。

服务器上成功挂载虚拟软驱。

说明

挂载成功后，单击“断开”，在弹出的“选择一个选项”对话框中单击“是”，卸载服务器上的虚拟软驱。

----结束

通过虚拟软驱挂载镜像文件

本操作使用本地PC上的软盘镜像文件虚拟出另一个软驱提供给服务器，并将软盘镜像文件加载到该虚拟软驱中。

说明

挂载的镜像文件大小必须为1.44MB，否则会导致挂载失败。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-75所示的界面。

步骤2 选中“镜像文件”单选按钮。

步骤3 单击“浏览”。

弹出“打开”窗口。

步骤4 选择本地PC上存放的软盘镜像文件，单击“打开”。

返回如图3-75所示的界面。

步骤5 单击“连接”。

服务器上成功挂载镜像文件。

说明

- 挂载镜像文件成功后，单击“弹出”，弹出镜像文件；弹出软盘镜像文件后，可重新选择其他“*.img”格式镜像文件，然后单击“插入”，挂载该镜像文件。
- 单击“断开”，在弹出的“选择一个选项”对话框中单击“是”，卸载服务器上的虚拟软驱。

----结束

制作镜像文件

本操作使用软驱或光驱中的软盘或光盘制作镜像文件。制作成功的镜像文件保存在本地PC上。它可以用于挂载和加载虚拟软驱或光驱。

执行本操作前请确保本地PC上的软驱或光驱中已插入了软盘或光盘。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-76所示的界面。

图 3-76 制作镜像文件

步骤2 在“选择驱动”下拉列表中，选择客户端的软盘驱动器或光盘驱动器。

步骤3 单击“浏览”。弹出“保存”窗口。

步骤4 选择镜像文件在PC上的保存路径，并在“文件名：”文本框中输入镜像文件的名称。

说明

系统只支持制作“*.iso”格式的光盘镜像文件和“*.img”格式的软盘镜像文件。

步骤5 单击“保存”。

返回如图3-76所示的界面。

步骤6 单击“制作”。

制作完成后，系统弹出窗口提示成功制作镜像文件。

在“制作进度”一栏将显示镜像文件的制作百分比。

说明

制作过程中，单击“停止”可以终止制作镜像文件。

----结束

挂载虚拟文件夹

本操作将本地PC上的文件夹挂载到服务器，使服务器系统可以以只读方式访问本地文件夹。

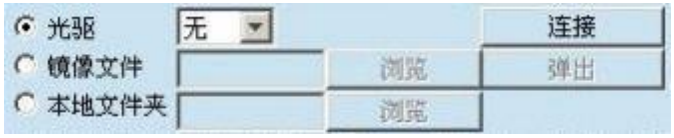
须知

在挂载虚拟文件夹之前，请先把要传输的文件拷入目标文件夹中。虚拟文件夹挂载后，不可对其进行添加或删除文件的操作。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-77所示的界面。

图 3-77 挂载虚拟文件夹



步骤2 选中“本地文件夹”单选按钮。

步骤3 单击“浏览”。

打开本地文件夹选择窗口。

步骤4 选择要挂载的本地文件夹，单击“打开”。

步骤5 单击“连接”。

说明

- 连接成功后，在服务器操作系统中，可以看到虚拟文件夹。您可以从此文件夹中直接拷贝文件。
- 连接成功后，单击“断开”，可以卸载虚拟文件夹。

----结束

为服务器上电

步骤1 在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“上电”。

弹出“选择一个选项”对话框。

步骤2 单击“确定”。

服务器开始上电。

说明

服务器上电的时间根据服务器配置所不同。

----结束

为服务器下电

须知

- 请在下电前确认无中断当前业务风险。
- 请根据实际情况选择下电方式，“强制下电”和“下电”的区别请参考iBMC用户指南的“系统管理 > 电源&功率”章节。

步骤1 在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“强制下电”或“下电”。

弹出“选择一个选项”对话框。

步骤2 单击“确定”。

服务器开始下电。

----结束

强制重启或强制下电再上电

须知

- 强制重启或强制下电再上电可能会损坏用户的程序或者未保存的数据，请根据操作系统实际情况谨慎选择操作方式。
- 请在强制重启或强制下电再上电前确认无中断当前业务风险。
- 请根据实际情况选择“强制重启”或“强制下电再上电”，“强制重启”和“强制下电再上电”的区别请参考iBMC用户指南的“系统管理> 电源&功率”章节。

步骤1 在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“强制重启”或“强制下电再上电”。

弹出“选择一个选项”对话框。

步骤2 单击“确定”。

服务器开始强制重启或强制下电再上电。

说明

服务器强制重启或强制下电再上电的时间根据服务器配置所不同。

----结束

键鼠复位

本操作模拟插拔USB键盘和USB鼠标。

步骤1 在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“键鼠复位”。

弹出“选择一个选项”对话框。

步骤2 单击“确定”。

服务器开始执行USB复位操作。

----结束

为实时桌面录像

本操作对当前远程虚拟控制台显示的画面进行录像。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出“选择一个选项”对话框。

步骤2 单击“确定”。

弹出“保存”窗口。

步骤3 选择将要录制的录像文件在PC上的保存路径，并在“文件名：”文本框中输入录像文件的名称。

步骤4 单击“保存”。

返回“KVM”界面并开始录制录像。

步骤5 录制完成后，单击  。

弹出“选择一个选项”对话框。

步骤6 单击“确定”。

录像文件被保存到指定的路径。

录制的录像文件格式为“*.rep”。可在“录像回放”界面中播放录像文件。

----结束

使用单鼠标

步骤1 如果本地PC上的鼠标与实时桌面上的不同步，您可以使用单鼠标功能隐藏本地PC上的鼠标。“KVM”界面中只保留实时桌面上的鼠标。

步骤2 在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“单鼠标”。

弹出“选择一个选项”对话框。

步骤3 单击“确定”。

“KVM”界面中只显示实时桌面上的鼠标。

----结束

加速远程鼠标

本操作对实时桌面上的鼠标进行加速，使其与本地PC上的鼠标同步。

步骤1 在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“鼠标加速”。

弹出“选择一个选项”对话框。

步骤2 单击“确定”。

同步本地PC与服务器的鼠标。

----结束

3.10 远程虚拟控制台异常帮助

3.10.1 打开 HTML5 集成远程控制台后显示设置信任证书超时

问题现象

问题描述	可能原因
打开HTML5集成远程控制台后显示“设置信任证书超时，无法开启KVM”。	KVM客户端与服务端建立连接前，需要进行SSL证书校验，若校验失败，则导致HTML5集成远程控制台无法连接。

解决方案

步骤1 打开iBMC WebUI中的“服务管理 > Web服务”页面，在“证书信息”区域中检查服务器证书是否过期。

- 是=> **步骤2**
- 否=> **步骤3**

步骤2 重新生成证书并替换原有证书。

步骤3 重启iBMC。

步骤4 重新打开HTML5集成远程控制台，查看是否可以正常开启。

- 是=>处理完毕
- 否=> **步骤5**

步骤5 请联系技术支持处理。

----结束

3.10.2 无法启动 Java 集成远程控制台

问题现象

问题描述	可能原因
无法启动远程虚拟控制台。	● 没有正确安装JRE。 ● JRE版本与iBMC不兼容。

解决方案

步骤1 确认客户端JRE已正确安装。

iBMC支持的JRE版本为： AdoptOpenJDK 8 JRE和AdoptOpenJDK 11 JRE。

- 若JRE版本正确，请联系技术支持处理。
- 若JRE版本不正确，执行**步骤2**。

步骤2 从AdoptOpenJDK官网下载适配客户端OS的JRE二进制压缩包。

步骤3 安装AdoptOpenJDK。

- 压缩包解压后需要手动配置JAVA_HOME及PATH环境变量。
- 需要从AdoptOpenJDK官网额外下载IcedTea Web并解压，然后将bin文件夹配置进PATH环境变量。

步骤4 按照正常操作方法重新打开Java集成远程控制台。

在此过程中，会自动下载.jnlp文件。

步骤5 打开.jnlp文件。

- 客户端使用Linux命令行或Windows命令行操作时，请切换至.jnlp文件所在目录，运行javaws kvm.jnlp。
- 客户端使用图形界面操作时，找到下载的.jnlp文件后，右键选择javaws打开。（若右键菜单无javaws，可至IcedTea Web安装目录中的bin目录下查找。）

----结束

3.10.3 打开远程虚拟控制台时鼠标键盘失效

问题现象

问题描述	可能原因
打开远程虚拟控制台后，鼠标、键盘失效。	服务器配置了LSISAS3108 RAID控制卡，且未使能“虚拟键鼠持续连接”。

解决方案

步骤1 检查服务器是否配置了LSISAS3108 RAID控制卡。

可通过“部件信息”界面查询。

- 是 => **步骤2**
- 否 => **步骤4**

步骤2 检查“远程控制台”界面的“虚拟键鼠持续连接”是否开启。

- 是 => **步骤4**
- 否 => **步骤3**

步骤3 使能“虚拟键鼠持续连接”，并重启服务器。重启完成后，检查故障现象是否消失。

- 是 => 处理完毕
- 否 => **步骤4**

步骤4 请联系技术支持处理。

----结束