超强 K620 V4 iBMC

用户指南

V3.01.00.00 及以上

文档版本:06
发布日期:2022-06-01

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。

目 录

前言

概述

本文档为服务器底层管理软件 iBMC（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。
- 可操作执行命令的详细解释。

说明

本文档主要介绍客户在使用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。

本文档适用于鲲鹏服务器主板。

读者对象

本文档主要适用于以下工程师：

- 服务器产品安装工程师
- 服务器产品维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
警告	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。

符号	说明
⚠ 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
06	2022-06-01	删除了清除日志功能。
05	2022-04-09	更新了 3.3 首页。
04	2022-04-01	更新了 3.3 首页。
03	2021-04-21	更新了 4.7.12 创建逻辑盘（createld）。
02	2021-04-12	更新了前言。
01	2021-02-03	第一次正式发布。

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
  - Redfish 接口
  - 超文本传输安全协议（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。
- 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 Redfish 实现 OS 部署。
  - 使能鲲鹏加速引擎，包括硬件安全加速引擎（SEC，Security Engine）、高性能 RSA 加速引擎（HPRE，High Performance RSA Engine）、RAID DIF 运算加速引擎（RDE，RAID DIF Engine）、ZIP 四个加速器。

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。

1.3.2 iBMC CLI

iBMC 将配置和查询功能封装为 **ipmcset** 和 **ipmcget** 命令。您可以通过 CLI 下的命令实现对 iBMC 的所有操作。

关于 CLI 的详细信息，请参考本文档 4 命令行介绍。

1.3.3 Redfish 接口

iBMC 支持标准的 Redfish 接口。Redfish 客户端（Redfish 接口工具，如 Chrome 的 Postman 插件）将 HTTPS 操作发送到服务器，通过 GET、PUT、PATCH、POST、DELETE 等命令对服务器进行查询、配置、监控。

1.3.4 iBMC 移动应用程序

通过使用移动应用程序 SmartServer，可以从移动设备中访问服务器的 iBMC。SmartServer 直接与 iBMC 进行交互，对服务器进行常规的配置和监控。

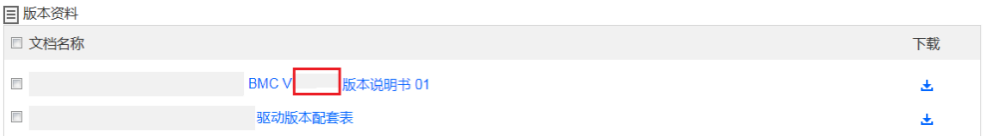
2 用户必读

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 版本说明查询。
  iBMC 版本说明，包含 iBMC 版本信息，例如：
  

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

- 通过命令行查询。

  登录 iBMC 命令行，执行 **ipmcget -d version**，在回显信息中可查看到“iBMC Version”。例如：

```
......
Active iBMC    Version:          (U68)3.01.01.00
Active iBMC      Build:          005
......
```

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 密码：Admin@9000
iBMC 管理网口 IP 地址默认获取方式	DHCP
iBMC 管理网口默认备份 IP 地址	192.168.2.100 **说明** 当管理网口切换到 NC-SI 通道时，面板的 GE 管理网口会变更成近端维护网口，其默认备份 IP 地址为 192.168.240.100。

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 iBMC CLI 修改。修改方法请参考本文档 4.3.2 设置 iBMC 网口的 IPv4 信息（ipaddr）和 4.3.6 设置 iBMC 网口的 IPv6 信息（ipaddr6）。
  - 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。
  - 上层网管可通过对接接口（例如 SNMP、Redfish 等）修改下辖服务器的地址。
- 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。
  - 通过 CLI 查询当前地址。

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 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
MAC OS X v10.7	Safari 9.0～13.1	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
	Mozilla Firefox 45.0～79.0	

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。
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

操作	说明
	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。 • “域名”选择“这台 iBMC”之外的其他选项时，支持输入

参数	描述
	的用户名的最大长度为 255 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”。 • 使用 LDAP 方式登录 iBMC 时，支持如下两种格式的用户名： – LDAP 用户名（此时“域名”可选择“自动匹配”或指定的域名）。 – LDAP 用户名@域名（此时“域名”可选择“自动匹配”或指定的域名）。 • 使用 Kerberos 方式登录 iBMC 时，支持如下两种格式的用户名： – Kerberos 用户名（此时“域名”可选择“自动匹配”或指定的域名）。 – Kerberos 用户名@域名（此时“域名”可选择“自动匹配”或指定的域名，且域名中的字母必须为大写）。 • Kerberos 用户名或 Kerberos 用户名@域名支持单点登录。
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 3-64。

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

静态 IP 地址：192.168.2.100

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。
- 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。

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
- 使用 LDAP 用户登录 WebUI
- 使用 Kerberos 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

使用 LDAP 用户登录 WebUI

在登录前，请确保以下设置满足要求：

- 网络中存在域控制器，并已在域控制器中创建了用户域、隶属于用户域的 LDAP 用户名及其密码。

说明

关于域控制器、用户域、隶属于用户域的 LDAP 用户名及其密码的创建请参见关于域控制器的相关文档。iBMC 系统仅提供 LDAP 用户的接入功能。

- 在 iBMC WebUI 的“用户&安全 > LDAP”中，已启用 LDAP 功能，并设置了用户域、隶属于用户域的 LDAP 用户名及其密码。

步骤 1 （可选）在 iBMC 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 LDAP 用户名和密码。

说明

- 使用 LDAP 方式登录 iBMC 时，支持如下两种格式的用户名：
  - LDAP 用户名（此时“域名”可选择“自动匹配”或指定的域名）。
  - LDAP 用户名@域名（此时“域名”可选择“自动匹配”或指定的域名）。
- 以 LDAP 方式登录 iBMC WebUI 时，密码最大长度为 255 个字符。

步骤 3 在域名下拉列表中，选择 LDAP 用户域。

说明

域名下拉列表中包含如下可选参数：

- “这台 iBMC”：使用本地用户登录时，可选择该参数。系统从本地用户列表中匹配对应的用户。

- 当前配置过的域服务器：使用 LDAP 用户登录时需选择对应的域服务器。系统从指定的域服务器中匹配对应的用户。
- “自动匹配”：选择该参数时，系统首先在本地用户列表中搜索，如无法匹配到对应的用户，则按照“域名”下拉列表中的顺序依次在各个域服务器中匹配。

步骤 4 单击“登录”。

成功登录后，显示“首页”界面。

----结束

使用 Kerberos 用户登录 WebUI

Kerberos 运行环境：

- 客户端支持操作系统版本为 Windows 10 64 位，浏览器版本为 Internet Explorer 11。
- Kerberos 服务器支持操作系统版本为 Windows Server 2012 R2 64 位和 Windows Server 2016 64 位。

Kerberos 用户支持两种方式登录：

- 通过 kerberos 域用户登录。
- 通过 SSO 一键登录。

在登录前，请确保以下设置满足要求：

- 在 iBMC WebUI 的“用户&安全 > Kerberos”中，已启用 Kerberos 功能，完成 Kerberos 功能及用户组配置。
- 在 Kerberos 服务器端已创建 Kerberos 用户组及用户名，并将用户加入 Kerberos 用户组。此用户为登录客户端 OS 的用户。

通过 Kerboros 域用户登录。

步骤 1 （可选）在 iBMC 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 Kerberos 用户名和密码。

步骤 3 在域名下拉列表中，选择 Kerberos 用户域（例如“ADMIN.COM(KRB)”）或“自动匹配”。

步骤 4 单击“登录”。

成功登录后，显示“首页”界面。

----结束

通过 SSO 一键登录。

步骤 1 使用已在 Kerberos 服务器配置过的 Kerberos 用户名与密码登录客户端 OS。

步骤 2 在浏览器中输入 iBMC 的 FQDN 地址，如“https://主机名.域名”。

打开 iBMC 登录界面。

步骤 3 单击“单点登录”。

成功登录后，显示“首页”界面。

----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。

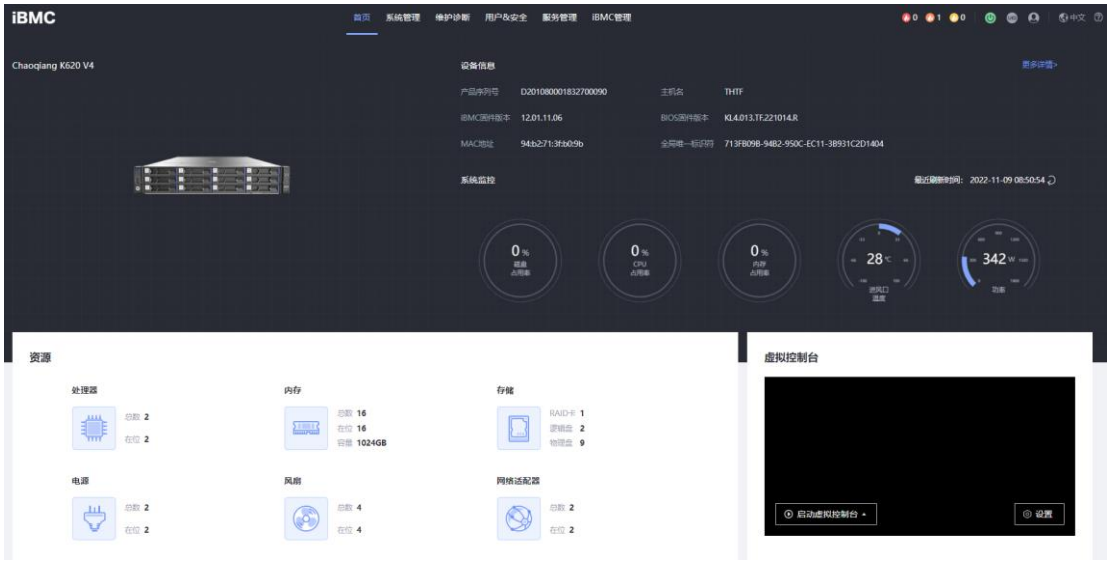
说明

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。
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

区域	展示的信息
	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
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。 • 一键收集：单击本入口可以直接下载收集到的维护相关信息，收集到信息的具体内容请参见本文档 3.11 一键收集信息说明。 • 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	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

区域	展示的信息
信息	• 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。

参数	描述
产品序列号	服务器的产品序列号。
部件编码	服务器的部件编码。
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。
BMC 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。
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。
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。
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。	

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、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、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，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。

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”	

参数	描述
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。	
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、PCIe 槽位号（PCIe 网卡独有）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

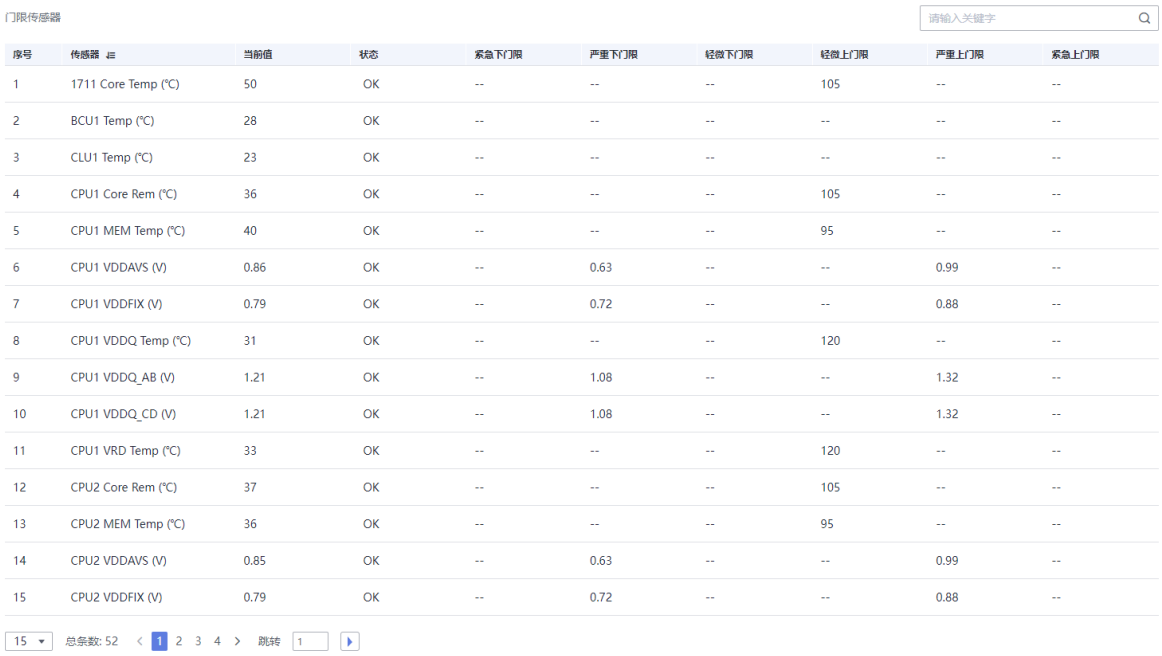
参数	描述
	支持使用 Port2，则 Port2 的网络属性显示为空。
FC 卡	显示服务器安装的 FC 卡的名称、厂商、型号、芯片型号、芯片厂商。 • 单击 FC 卡子菜单的 FC 名称，可以查看成员端口的详细信息，包括端口、FC ID、端口类型、状态。 • 单击端口属性下方的 ，可以查看指定 FC 卡的网络属性，包括速率、WWPN（World Wide Port Name）、WWNN（World Wide Node Name）、固件版本、驱动名称、驱动版本。
Team	显示汇聚网口的名称、状态、工作模式、IPv4 信息（地址/子网掩码/网关）、IPv6 信息（地址/前缀长度/网关）、MAC 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


门限传感器

请输入关键字

序号	传感器	当前值	状态	紧急下门限	严重下门限	轻微下门限	轻微上门限	严重上门限	紧急上门限
1	1711 Core Temp (℃)	50	OK	--	--	--	105	--	--
2	BCU1 Temp (℃)	28	OK	--	--	--	--	--	--
3	CLU1 Temp (℃)	23	OK	--	--	--	--	--	--
4	CPU1 Core Rem (℃)	36	OK	--	--	--	105	--	--
5	CPU1 MEM Temp (℃)	40	OK	--	--	--	95	--	--
6	CPU1 VDDAVS (V)	0.86	OK	--	0.63	--	--	0.99	--
7	CPU1 VDDFIX (V)	0.79	OK	--	0.72	--	--	0.88	--
8	CPU1 VDDQ Temp (℃)	31	OK	--	--	--	120	--	--
9	CPU1 VDDQ_AB (V)	1.21	OK	--	1.08	--	--	1.32	--
10	CPU1 VDDQ_CD (V)	1.21	OK	--	1.08	--	--	1.32	--
11	CPU1 VRD Temp (℃)	33	OK	--	--	--	120	--	--
12	CPU2 Core Rem (℃)	37	OK	--	--	--	105	--	--
13	CPU2 MEM Temp (℃)	36	OK	--	--	--	95	--	--
14	CPU2 VDDAVS (V)	0.85	OK	--	0.63	--	--	0.99	--
15	CPU2 VDDFIX (V)	0.79	OK	--	0.72	--	--	0.88	--

15 总条数: 52 1 2 3 4 跳转 1

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。

参数	描述
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 其他

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。
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。

参数	描述
	• 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。
CIC 卡	显示服务器 CIC 卡信息。 ● CIC 卡满配个数和当前在位个数。 ● CIC 卡的名称、厂商、PCB 版本、单板 ID、描述、序列号以及部件编码。
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。
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。

3.4.2 性能监控

功能介绍

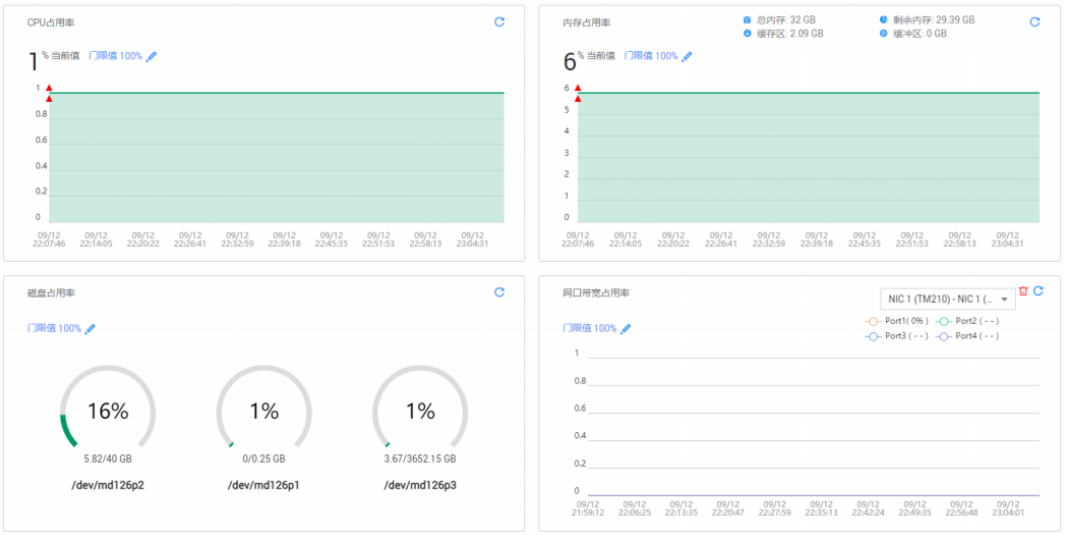
通过“性能监控”界面，您可以：

- 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** • 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 CPU 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。
内存占用率	运行的程序占用内存的比例。 **说明** • 您必须先在服务器 OS 侧安装 iBMA 2.0，并完全启动后，方可查看内存占用率信息。 • 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。
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。

参数	描述
	• 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。
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，

参数	描述
	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。
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。
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。
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。
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

配置项	说明
	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“Read Ahead”，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。
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。

配置项	说明
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 3-12 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

配置项	说明
	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
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

配置项	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。
- 查看系统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。
- 请在强制下电、下电、强制重启或强制下电再上电操作前确认无业务风险。

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


功率状态
BTU/h
W
统计开始时间：2019/12/23 11:25:59
重新统计
功率封顶配置
功率封顶功能已关闭
产生时间: 2019/12/23 12:47:20
当前功率
228 W
系统峰值功率
300 W
系统平均功率
268 W
系统累计耗电量
17.21 kWh
历史功率 (W)
选择时间段
2019/12/25 03:00 – 2019/12/26 02:50
查询
分段峰值功率： 300 W
产生时间：2019/12/25 03:16:25
下载
清空
告警门限 – (W)
300
280
260
240
220
200
180
2019/12/25 03:00
2019/12/25 05:45
2019/12/25 08:24
2019/12/25 11:00
2019/12/25 13:42
2019/12/25 16:20
2019/12/25 18:59
2019/12/25 21:38
2019/12/26 00:17
2019/12/26 02:56
平均功率
峰值功率

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。

参数	描述
当前功率	显示电源模块当前的输出功率。
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 Redfish 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 Redfish 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”。

参数	描述
	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。
功率封顶配置	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	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。
当前功率	服务器当前的功率。
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。
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，系统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。 针对支持 BBU 备电模块的服务器，当 BBU 备电模块在位时，下电时限取值范围为 180～6000；其他情况下，下电时限取值范围为 10～6000。 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。 • 启用备电功能的设备不支持强制重启操作（仅针对支持 BBU 模块的服务器）。
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。
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。

参数	描述
	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。 – 如果断电前服务器操作系统是开机状态，则通电后服务器自动开机。 – 如果断电前服务器操作系统是关机状态，则通电后服务器不上电。 默认为“保持上电”。
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”。
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

操作	操作步骤
	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”。 服务器操作系统开始强制重启。服务器操作系统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”。
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。

操作	操作步骤
	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

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”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”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。 • 如果实际温度值高于设置的目标调速温度值，iBMC 将提高风扇转

参数	描述
	速以降低温度；如果实际温度值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”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。

界面描述

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

图3-24 系统启动项

参数说明

表3-23 启动项配置

参数	描述
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。
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

参数	描述
	• 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。

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

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：

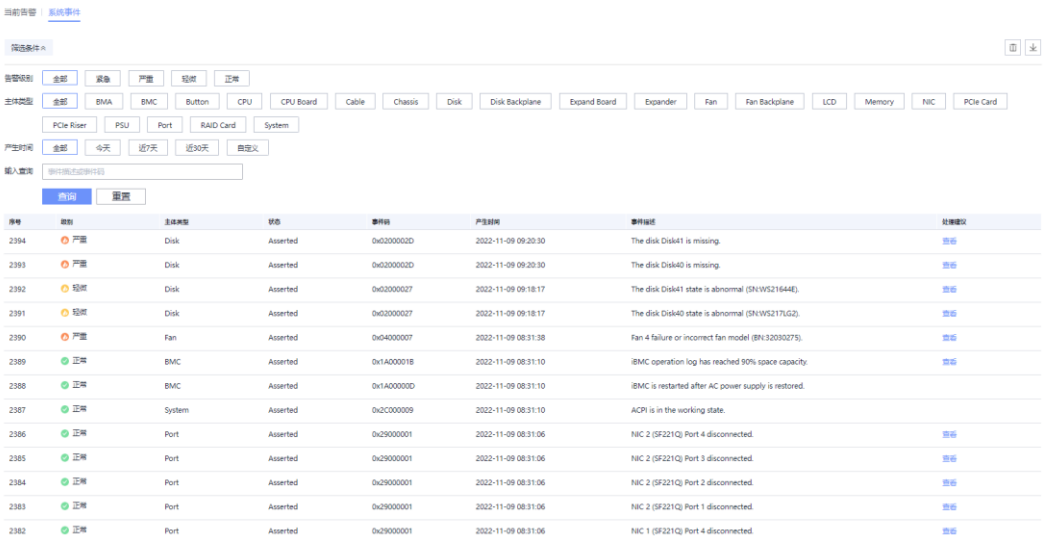
- 查看设备当前未处理的告警。
- 查看和搜索服务器产生的各种系统事件，也可以下载和清除所有系统事件。

界面描述

在导航栏中选择“维护诊断 > 告警&事件”，打开如图 3-25 和图 3-26 所示界面。

图3-25 当前告警

图3-26 系统事件



参数说明

表3-24 告警&事件

参数	描述
序号	事件的排序。
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。

参数	描述
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 3-25 提供的参数信息，设置筛选条件。

表3-25 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：

参数	描述
	• 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 3-27、图 3-28 和图 3-29 所示界面。

图3-27 Syslog 报文通知

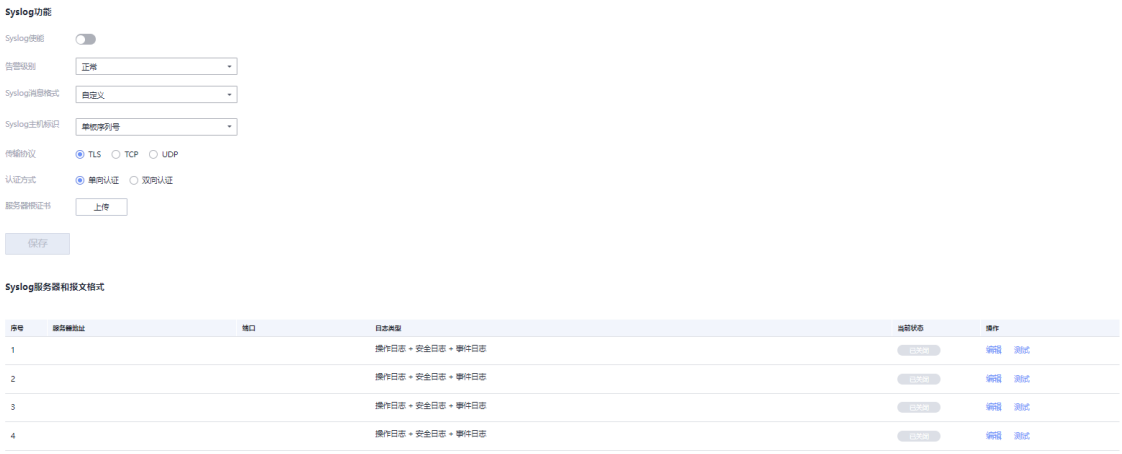


图3-28 邮件通知

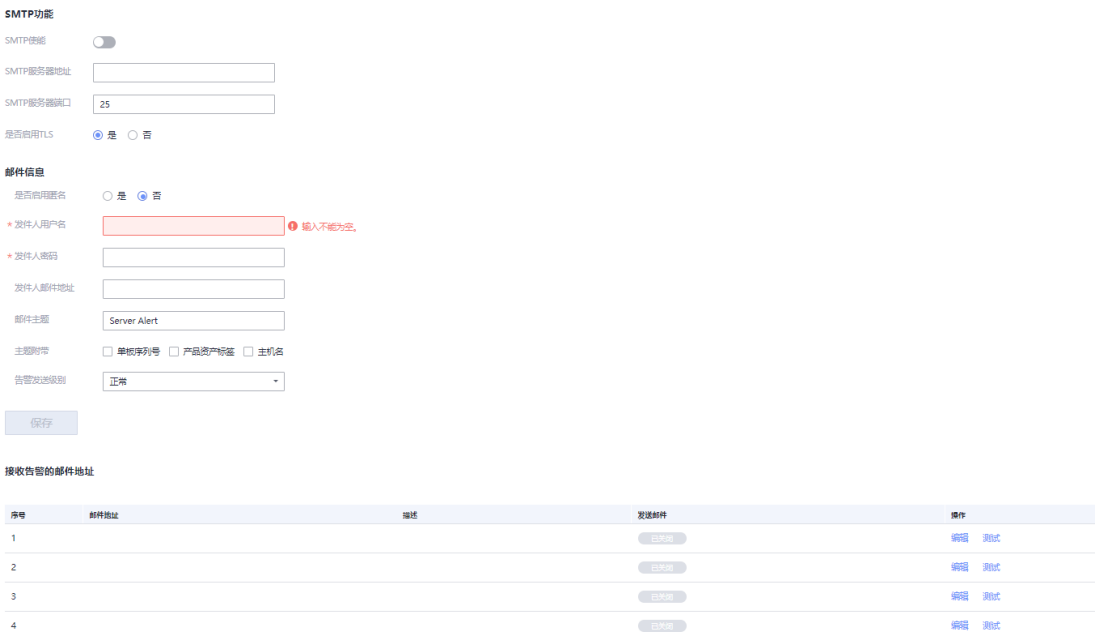
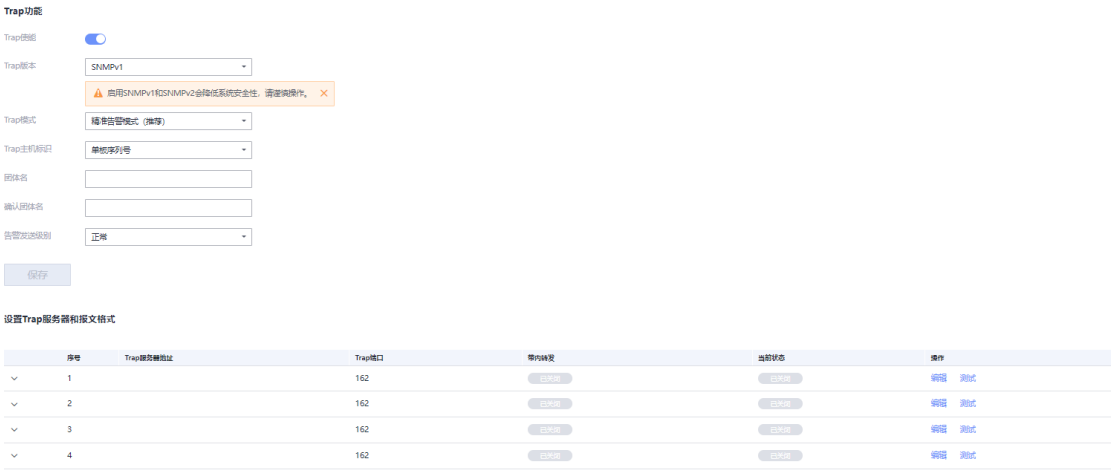


图3-29 Trap 报文通知



参数说明

表3-26 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。

参数	描述
	• 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。
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 为不安全的弱签名算法，iBMC 不支持导入弱签名算法(MD5)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。

参数	描述
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	
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3-27 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。

参数	描述
	• 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。
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3-28 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。
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

参数	描述
	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：“SNMPv1”。
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 Trap V3 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
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

参数	描述
	– 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。
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。
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”。
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。

参数	描述
	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 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 3-29 所示。

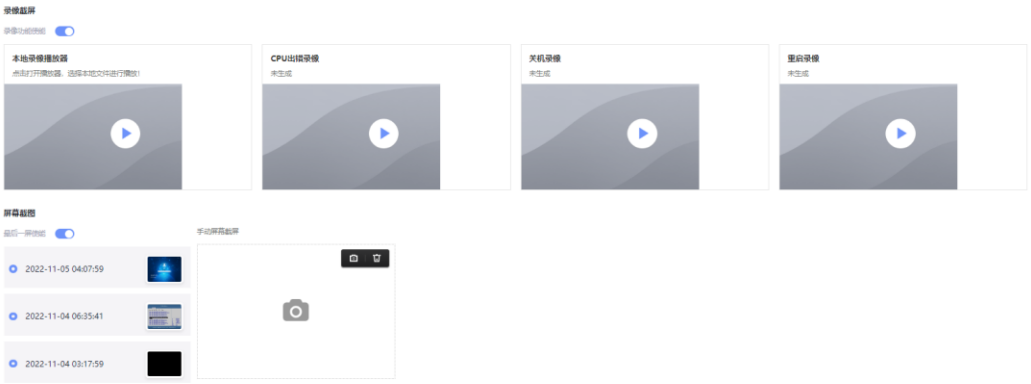
表3-29 录像回放控制窗口按钮说明

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 3-30 所示界面。

图3-30 录像截屏



操作步骤

表3-30 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。

操作	操作步骤
	播放器窗口最大化显示在屏幕上。
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3-31 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。

操作	操作步骤
	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。
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。

3.5.4 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 3-31 所示界面。

图3-31 系统日志

操作步骤

表3-32 黑匣子功能操作步骤

操作	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服务器配套的安装手册。 • 在不同浏览器下，页面提示保存文件的信息略有不同。

表3-33 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。

3.5.5 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。

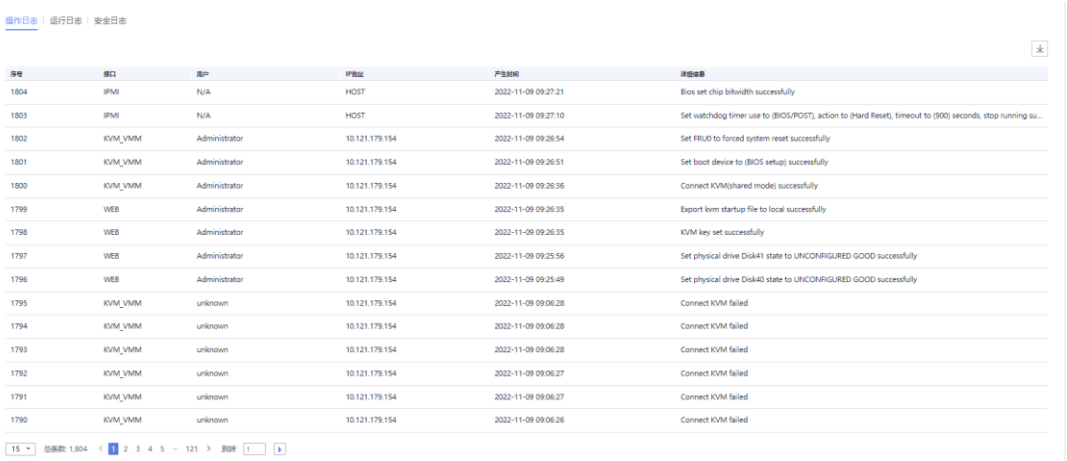
  iBMC 为安全日志提供 200KB 的存储空间，可记录约 2000 条安全日志。

  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 3-32、图 3-33、图 3-34 所示界面。

图3-32 操作日志

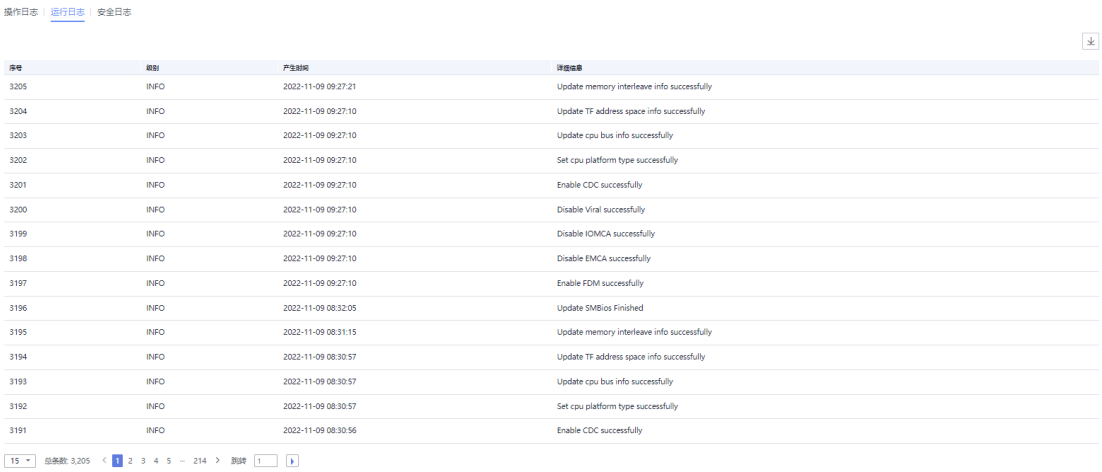


操作日志 | 运行日志 | 安全日志

序号	接口	用户	IP地址	产生时间	详细信息
1804	IPMI	N/A	HOST	2022-11-09 09:27:21	Bios set chip bitwidth successfully
1803	IPMI	N/A	HOST	2022-11-09 09:27:10	Set watchdog timer use to (BIOS/POST), action to (Hard Reset), timeout to (900) seconds, stop running su...
1802	KVM_VMM	Administrator	10.121.179.154	2022-11-09 09:26:54	Set FRU0 to forced system reset successfully
1801	KVM_VMM	Administrator	10.121.179.154	2022-11-09 09:26:51	Set boot device to (BIOS setup) successfully
1800	KVM_VMM	Administrator	10.121.179.154	2022-11-09 09:26:36	Connect KVM(shared mode) successfully
1799	WEB	Administrator	10.121.179.154	2022-11-09 09:26:35	Export kvm startup file to local successfully
1798	WEB	Administrator	10.121.179.154	2022-11-09 09:26:35	KVM key set successfully
1797	WEB	Administrator	10.121.179.154	2022-11-09 09:25:56	Set physical drive Disk41 state to UNCONFIGURED GOOD successfully
1796	WEB	Administrator	10.121.179.154	2022-11-09 09:25:49	Set physical drive Disk40 state to UNCONFIGURED GOOD successfully
1795	KVM_VMM	unknown	10.121.179.154	2022-11-09 09:06:28	Connect KVM failed
1794	KVM_VMM	unknown	10.121.179.154	2022-11-09 09:06:28	Connect KVM failed
1793	KVM_VMM	unknown	10.121.179.154	2022-11-09 09:06:28	Connect KVM failed
1792	KVM_VMM	unknown	10.121.179.154	2022-11-09 09:06:27	Connect KVM failed
1791	KVM_VMM	unknown	10.121.179.154	2022-11-09 09:06:27	Connect KVM failed
1790	KVM_VMM	unknown	10.121.179.154	2022-11-09 09:06:26	Connect KVM failed

15 总条数: 1,804 < 1 2 3 4 5 ... 121 > 到第 1

图3-33 运行日志

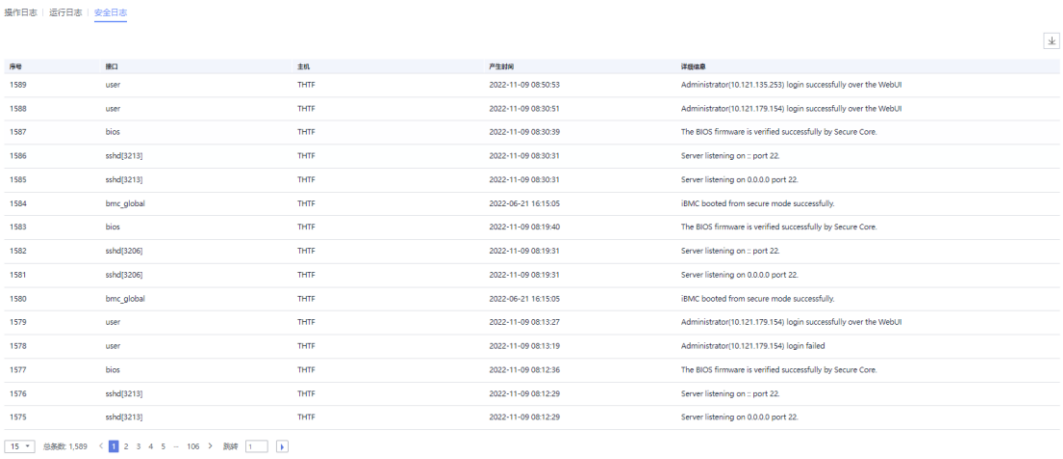


操作日志 | 运行日志 | 安全日志

序号	级别	产生时间	详细信息
3205	INFO	2022-11-09 09:27:21	Update memory interleave info successfully
3204	INFO	2022-11-09 09:27:10	Update TF address space info successfully
3203	INFO	2022-11-09 09:27:10	Update cpu bus info successfully
3202	INFO	2022-11-09 09:27:10	Set cpu platform type successfully
3201	INFO	2022-11-09 09:27:10	Enable CDC successfully
3200	INFO	2022-11-09 09:27:10	Disable Viral successfully
3199	INFO	2022-11-09 09:27:10	Disable IOMCA successfully
3198	INFO	2022-11-09 09:27:10	Disable EMCA successfully
3197	INFO	2022-11-09 09:27:10	Enable FDM successfully
3196	INFO	2022-11-09 08:32:05	Update SMBios Finished
3195	INFO	2022-11-09 08:31:15	Update memory interleave info successfully
3194	INFO	2022-11-09 08:30:57	Update TF address space info successfully
3193	INFO	2022-11-09 08:30:57	Update cpu bus info successfully
3192	INFO	2022-11-09 08:30:57	Set cpu platform type successfully
3191	INFO	2022-11-09 08:30:56	Enable CDC successfully

15 总条数: 3,205 < 1 2 3 4 5 ... 214 > 到第 1

图3-34 安全日志



参数说明

表3-34 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。
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。 • 接口为本地串口。

参数	描述
	• 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3-35 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。
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3-36 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。

参数	描述
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。

3.5.6 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。

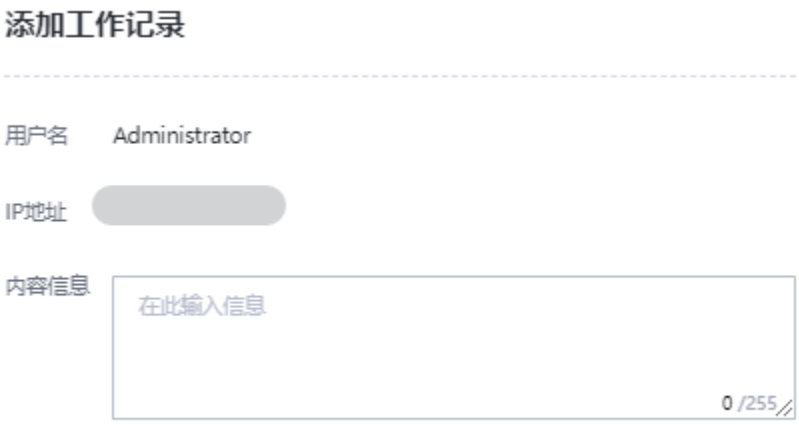
说明

- 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 3-35 所示界面。

图3-35 工作记录



操作步骤

表3-37 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 3-36 所示界面。

图3-36 本地用户

参数说明

表3-38 本地用户

参数	描述

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。
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。 • 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。 • Redfish：使能该接口后，用户可使用符合 Redfish 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。

参数	描述
	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3-39 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3-40 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：:<>&,'"/\%

参数	描述
	• 不能包含空格且首字符不能是“#”、“+”或“-”。 • 用户名不能为“.”或“..”。
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。 – 新旧口令至少在 2 个字符位上不同（iBMC V3.01.12.01 及以上版本无此要求）。 • 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。
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。

参数	描述
	• 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。 • 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。 • Redfish：使能该接口后，用户可使用符合 Redfish 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 3-40，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3-41 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。 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	修改后的用户密码，此处输入的内容需要与“密码”中相同。
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

参数	描述
	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。 • 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。 • Redfish：使能该接口后，用户可使用符合 Redfish 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。
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。

参数	描述
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 **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。 • 鲲鹏服务器主板 S920X02 和 S920X03 默认取值为 SHA，其他型号主板默认取值为 SHA256。 • 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。
取消	取消修改用户信息。

步骤 2 根据表 3-41 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

导入 SSH 公钥

说明

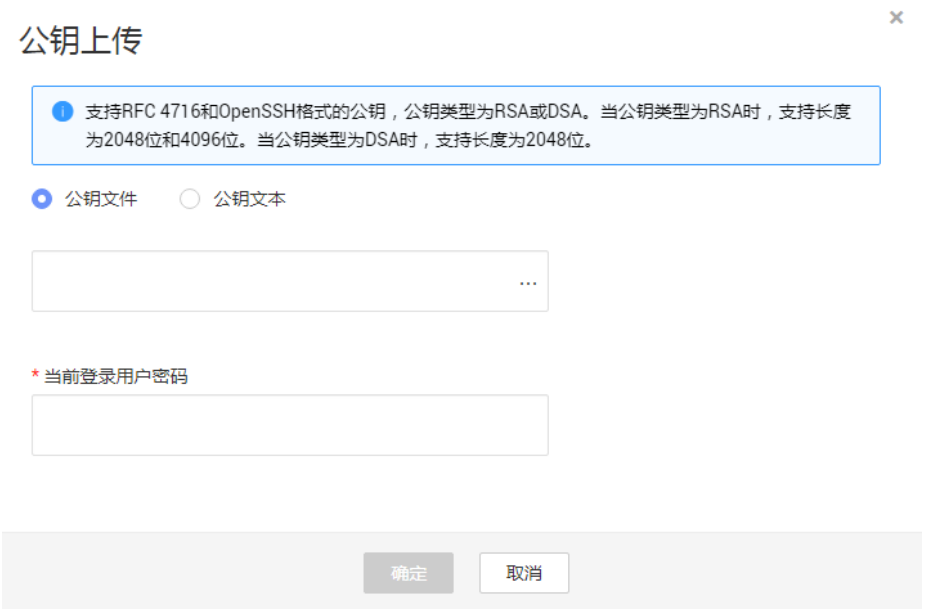
- 在客户端生成私钥后，需要在 iBMC 侧导入对应的公钥，保证用户通过 SSH 登录 iBMC 系统的安全性和唯一性。
- 每个用户只能导入一个公钥，若需要变更公钥，需要删除已导入的公钥后再导入新的公钥。
- 支持 RFC 4716 和 OpenSSH 格式的公钥，公钥类型为 RSA 或 DSA。当公钥类型为 RSA 时，支持长度为 2048 位和 4096 位。当公钥类型为 DSA 时，支持长度为 2048 位。

步骤 1 单击待导入 SSH 公钥的用户名左侧的 。

步骤 2 单击“SSH 公钥”右侧的“上传”。

弹出导入“公钥上传”窗口，如图 3-37 所示。

图3-37 公钥上传



步骤 3 选择公钥导入方式。

此处可根据实际情况选择“公钥文件”或“公钥文本”。

步骤 4 单击 选择生成的公钥。

步骤 5 输入当前登录用户密码。

步骤 6 单击“确定”。

----结束

3.6.2 LDAP

功能介绍

通过使用“LDAP”界面的功能，您可以查看和设置 LDAP 用户的信息。

iBMC 系统提供 LDAP 用户的接入功能。使用域控制器中的用户域、组域、隶属于用户域的 LDAP 用户名及其密码登录 iBMC 系统可以提高系统安全性。LDAP 用户可登录 iBMC WebUI，也可通过 SSH 方式登录 iBMC 命令行。

说明

LDAP 服务器的 DisplayName 和 CN 要保持一致。

iBMC 最多支持同时配置 6 个域服务器。

LDAP 用户登录 iBMC WebUI 时，可指定具体的域服务器，也可由系统自动匹配。LDAP 用户登录 iBMC 命令行时，无需指定域服务器，由系统自动匹配。

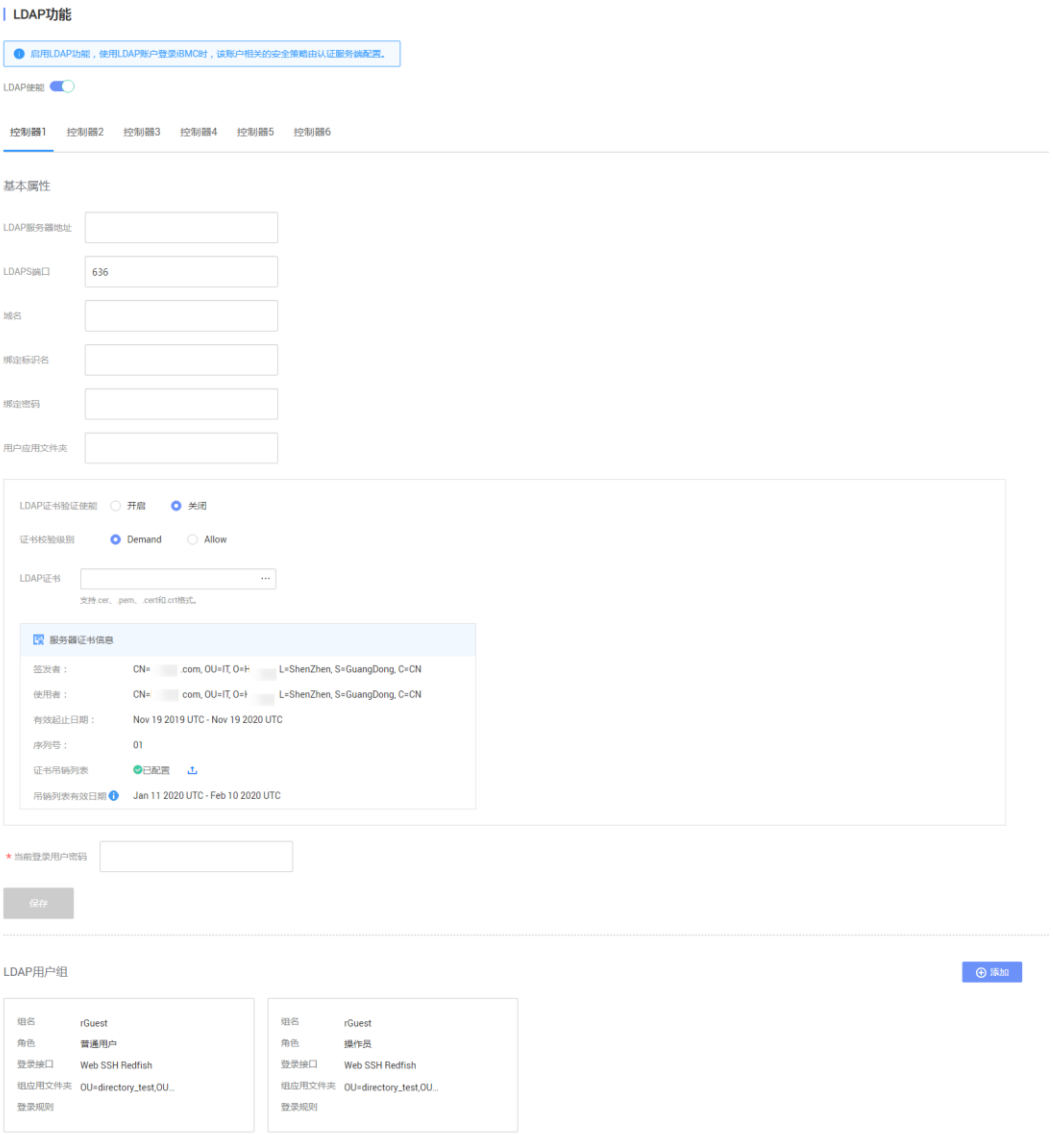
说明

iBMC 当前支持与 Windows AD 和 FreeIPA 的对接。

界面描述

在导航栏中选择“用户&安全 > LDAP”，打开如图 3-38 所示界面。

图3-38 LDAP



参数说明

表3-42 LDAP 配置

参数	描述
LDAP 使能	是否启用 LDAP 组功能。 •  表示启用 LDAP 功能。 •  表示停用 LDAP 功能。 **说明** 启用 LDAP 功能，使用 LDAP 帐户登录 iBMC 时，该帐户相关的安全策

参数	描述
	略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。
控制器 1 iBMC 可同时配置 6 个域服务器。用户使用 LDAP 方式登录 iBMC 的 WebUI 时，可指定任意一个控制器，或自动适配任意一个控制器。 控制器 2～控制器 6 的配置与控制器 1 类似，均需配置如下参数。 **说明** 带“*”的项目为必配参数。	
基本属性	
LDAP 服务器地址	LDAP 服务器的地址。 输入格式：IPv4 地址、IPv6 地址或域名。 启用证书验证功能后，该处需要配置为 LDAP 服务器的 FQDN（主机名.域名），且需要在网络配置部分配置 DNS。 **说明** 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。
LDAPS 端口	LDAP 服务的端口号。 取值范围：1～65535 默认值：636 **说明** 由于 iBMC 仅支持 LDAPS，不支持无 SSL 的 LDAP（端口号：389），所以 LDAP 服务器必须安装证明自身身份的可信任的服务器证书。
域名	域控制器中定义的 LDAP 用户所属角色组的域。 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。
绑定标识名	LDAP 代理用户标识名。 例如：“CN=username,OU=company,DC=domain,DC=com”，与 LDAP 服务器下成员标识名保持一致。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。

参数	描述
绑定密码	LDAP 代理用户的认证密码。 取值范围：1～20 个字符，由数字、英文字母和特殊字符组成。
用户应用文件夹	能够登录 iBMC 的 LDAP 用户在 LDAP 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 iBMC 的用户“infotest”在 LDAP 服务器上所属的路径为“\testusers\part1”，则此处需要输入的内容为“OU=part1,OU=testusers”。 **说明** 节点属性“CN”和“OU”的区别，请参考 LDAP 协议的详细介绍。 例如，在 Windows AD 中： • 节点的“Type”参数为“Container”时，节点属性为“CN”。 • 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
LDAP 证书验证使能	是否对远端域控制器进行证书验证。 从安全性考虑，请尽量开启证书验证。开启证书验证后需要导入 LDAP CA 证书；LDAP 服务器端需要安装 AD、DNS、CA 证书颁发机构，将 CA 证书导入 LDAP 服务器和 iBMC 系统。 默认值：关闭
证书校验级别	对 LDAP 证书进行校验的级别。 • “Demand”：证书校验过程中，当检查到客户端证书错误或没有证书时，不允许登录 iBMC。从安全性考虑，请尽量保持默认值“Demand”。 • “Allow”：证书校验过程中，当检查到客户端证书错误或没有证书时，仍允许登录 iBMC。 默认值：“Demand”
LDAP 证书	用于上传 LDAP CA 证书，支持.cer、.pem、.cert 和.crt 格式。 **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。 • 证书链的层级不得超过 10 级。
证书信息	显示证书信息。 若为证书链，显示的证书信息依次为“服务器证书 > 中间证书 > 根证书”。
当前登录用户密码	配置域控制器需要输入当前登录 iBMC 系统的用户密码。

参数	描述
LDAP 用户组	
添加	打开配置新建 LDAP 组区域框。
	打开配置已有 LDAP 组区域框。
	删除已有 LDAP 组。
组名	LDAP 用户所属角色组的名称。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
角色	LDAP 用户组的权限角色。 • 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。
登录接口	LDAP 组使能的登录接口，通过该接口，LDAP 组的成员可登录 iBMC 系统。 取值范围： • 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。 • Web：使能该接口后，用户可使用浏览器登录 iBMC WebUI。 • Redfish：使能该接口后，用户可使用符合 Redfish 协议的终端工具登录 iBMC 系统。
组应用文件夹	能够登录 iBMC 的 LDAP 组在 LDAP 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 iBMC 的用户“infotest”在 LDAP 服务器上所属的路径为“\testusers\part1”，则此处需要输入的内容为“OU=part1,OU=testusers”。 **说明** 节点属性“CN”和“OU”的区别，请参考 LDAP 协议的详细介绍。 例如，在 Windows AD 中：

参数	描述
	• 节点的“Type”参数为“Container”时，节点属性为“CN”。 • 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
登录规则	LDAP 组应用的登录规则，对已选择该登录规则的 LDAP 组进行限制。

启用 LDAP 并配置域服务器基本属性

步骤 1 单击“LDAP 使能”右侧的  ，将状态设置为  ，表示 LDAP 功能已经启用。

步骤 2 根据表 3-42 提供的参数信息，设置域服务器。

步骤 3 单击“保存”。

显示“操作成功”。

----结束

导入 LDAP 证书

单击“LDAP 证书”后的，选择要导入的 LDAP 证书。

说明

请定期更新证书，否则可能存在安全风险。

当界面提示“上传成功”后，可在下方的“证书信息”区域查看已看上传的证书的详细内容，包含内容如表 3-43 所示。

表3-43 证书信息

参数	描述
签发者	LDAP 证书的签发者信息，包含的具体参数类型与“使用者”相同。
使用者	LDAP 证书的使用者（即当前服务器）信息，包含： • CN：使用者的名称 • OU：使用者所在部门 • O：使用者所在的公司 • L：使用者所在的城市 • S：使用者所在的省份

参数	描述
	• C：使用者所在的国家
有效起止日期	LDAP 证书生效起止日期。
序列号	LDAP 证书序列号。用于证书的识别、迁移。
证书吊销列表	LDAP 证书吊销状态： • 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。
吊销列表有效日期	LDAP 证书的吊销列表有效日期。 **说明** 吊销列表过期会导致相应的认证功能失败。

配置证书吊销列表

说明

证书吊销文件的格式为“*.crl”，编码格式为 Base64，最大不超过 100KB。

步骤 1 从证书颁发机构获取证书吊销文件。

步骤 2 在“服务器证书信息”区域单击“证书吊销列表”后的 。

步骤 3 选择证书吊销文件。

步骤 4 输入当前登录用户密码并单击“确定”。

----结束

添加 LDAP 组

iBMC 系统最大可以设置 5 个 LDAP 组。

步骤 1 在“LDAP 用户组”区域中，单击“添加”。

弹出添加 LDAP 组的窗口。

表3-44 添加组

参数	描述
组名	LDAP 用户所属角色组的名称。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
组应用文件夹	能够登录 iBMC 的 LDAP 组在 LDAP 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层

参数	描述
	级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 iBMC 的用户“infotest”在 LDAP 服务器上所属的路径为“\testusers\part1”，则此处需要输入的内容为“OU=part1,OU=testusers”。 **说明** 节点属性“CN”和“OU”的区别，请参考 LDAP 协议的详细介绍。 例如，在 Windows AD 中： • 节点的“Type”参数为“Container”时，节点属性为“CN”。 • 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
角色	分配给组域的访问 iBMC 界面的权限。 取值范围：“管理员”、“操作员”、“普通用户”和“自定义”。
登录规则	LDAP 组应用的登录规则，对已选择该登录规则的 LDAP 组进行限制。
登录接口	LDAP 组使能的登录接口，通过该接口，LDAP 组的成员可登录 iBMC 系统。 取值范围： • 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。 • Web：使能该接口后，用户可使用浏览器登录 iBMC WebUI。 • Redfish：使能该接口后，用户可使用符合 Redfish 协议的终端工具登录 iBMC 系统。
当前用户登录密码	当前登录 iBMC 系统的用户密码。

步骤 2 根据表 3-44 的说明设置 LDAP 组的基本属性。

步骤 3 单击“保存”。

在 LDAP 用户组列表显示成功添加的 LDAP 组信息。

----结束

删除 LDAP 组

步骤 1 在“LDAP 用户组”区域中，单击待删除的 LDAP 组后方的 。

弹出“确认”对话框，提示输入当前登录用户的密码。

步骤 2 输入当前用户的密码。

步骤 3 单击“确定”。

界面显示“删除成功”。

----结束

修改 LDAP 组

步骤 1 在“LDAP 用户组”区域中，单击待修改的 LDAP 组右侧的 。

步骤 2 根据表 3-44 的说明修改 LDAP 组配置。

步骤 3 单击“保存”。

说明

修改 LDAP 组信息或删除 LDAP 组，已登录 KVM 用户不会自动退出登录。如需注销已登录的 KVM 用户，需要到“在线用户”页面进行操作。

----结束

3.6.3 Kerberos

功能介绍

通过使用“Kerberos”界面的功能，您可以查看和设置 Kerberos 基本属性和 Kerberos 用户组的信息。

iBMC 系统提供 Kerberos 用户的接入功能。使用 Kerberos 登录 iBMC 系统可以提高系统安全性。Kerberos 用户可登录 iBMC WebUI。

界面描述

在导航栏中选择“用户&安全 > Kerberos”，打开如图 3-39 所示界面。

图3-39 Kerberos

参数说明

表3-45 Kerberos 功能

参数	描述
Kerberos 使能	是否启用 Kerberos 功能。 •  表示启用 Kerberos 功能。 •  表示停用 Kerberos 功能。 **说明** 启用 Kerberos 功能，使用 Kerberos 帐户登录 iBMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。
基本属性 **说明** 带“*”的项目为必配参数。	
领域	Kerberos 领域。 取值范围：最大长度为 255 个字符。 取值原则：由数字、大写英文字母和特殊字符（包括空格）组成。
Kerberos 服务器地址	Kerberos 服务器的地址。 启用 Kerberos 功能后，该处需要配置为 Kerberos 服务器的 FQDN（主机名.域名），且需要在网络配置部分配置 DNS。 输入格式：IPv4 地址、IPv6 地址或域名。 域名的取值原则：

参数	描述
	• 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。
Kerberos 端口	Kerberos 服务的端口号。 取值范围：1～65535 默认值：88
密钥表	用于上传 Kerberos 密钥表，仅支持“.keytab”格式。 默认显示为空。 **说明** • 密钥表大小不可为 0KB，不能大于 1MB。 • 请定期更新密钥，否则可能存在安全风险。
当前用户登录密码	当前登录 iBMC 系统的用户密码。
Kerberos 用户组	显示所有 Kerberos 用户组的信息。 iBMC 最多支持同时添加 5 个 Kerberos 用户组。
组名	Kerberos 用户所属角色组的名称。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
SID	安全标识符（Security Identifiers）。用于 Kerberos 和用户组授权。例如，“S-1-5-21-310440588-250036847-580389505-500”。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
角色	Kerberos 用户组的权限角色。 • 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。
登录接口	Kerberos 用户组使能的登录接口，通过该接口，Kerberos 用户组

参数	描述
	的成员可登录 iBMC 系统。 使能该接口后，用户可使用浏览器登录 iBMC WebUI。 当前仅支持 WebUI 登录。
组应用文件夹	能够登录 iBMC 的 Kerberos 用户组在 Kerberos 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 iBMC 的 Kerberos 用户组“grouptest”在 Kerberos 服务器上所属的路径为“\testgroups\part1”，则此处需要输入的内容为“OU=part1,OU=testgroups”。 **说明** 节点属性“CN”和“OU”的区别，请参考 Kerberos 协议的详细介绍。 例如，在 Windows AD 中： • 节点的“Type”参数为“Container”时，节点属性为“CN”。 • 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
登录规则	Kerberos 用户组应用的登录规则，对已选择该登录规则的 Kerberos 用户组进行限制。

启用 Kerberos 认证并配置域服务器基本属性

步骤 1 单击“Kerberos 使能”右侧的  ，将状态设置为  ，表示 Kerberos 功能已经启用。

步骤 2 根据表 3-45 提供的参数信息，设置域服务器。

步骤 3 单击“保存”。

----结束

导入密钥表

步骤 1 单击“密钥表”后的，选择要导入的密钥表。

步骤 2 单击“打开”。

上传成功后，“密钥表”显示“上传成功”。

步骤 3 输入当前登录用户的密码。

说明

通过 SSO 登录的 Kerberos 用户不需要输入当前登录用户密码。

步骤 4 单击“保存”。

----结束

添加 Kerberos 用户组

iBMC 系统最大可以添加 5 个 Kerberos 用户组。

步骤 1 在“Kerberos 用户组”区域中，单击“添加”。

弹出添加 Kerberos 用户组的窗口。

表3-46 添加组

参数	描述
组名	Kerberos 用户所属角色组的名称。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
组应用文件夹	能够登录 iBMC 的 Kerberos 用户组在 Kerberos 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 iBMC 的 Kerberos 用户组“grouptest”在 Kerberos 服务器上所属的路径为“\testgroups\part1”，则此处需要输入的内容为“OU=part1,OU=testgroups”。 **说明** 节点属性“CN”和“OU”的区别，请参考 Kerberos 协议的详细介绍。 例如，在 Windows AD 中： ● 节点的“Type”参数为“Container”时，节点属性为“CN”。 ● 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
SID	安全标识符。用于 Kerberos 和用户组授权。 取值范围：iBMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64～255。
角色	分配给组域的访问 iBMC 界面的权限。 取值范围：“管理员”、“操作员”、“普通用户”和“自定义”。

参数	描述
登录规则	Kerberos 用户组应用的登录规则，对已选择该登录规则的 Kerberos 用户组进行限制。
登录接口	Kerberos 用户组使能的登录接口，通过该接口，Kerberos 用户组的成员可登录 iBMC 系统。
当前用户登录密码	当前登录 iBMC 系统的用户密码。 **说明** 通过 SSO 登录的 Kerberos 用户不需要输入当前登录用户密码。

步骤 2 根据表 3-46 的说明设置 Kerberos 用户组的基本属性。

步骤 3 单击“保存”。

在 Kerberos 用户组列表显示成功添加的 Kerberos 用户组信息。

----结束

删除 Kerberos 用户组

步骤 1 在“Kerberos 用户组”区域中，单击待删除的 Kerberos 用户组后方的 。

弹出“确认”对话框，提示输入当前登录用户的密码。

说明

通过 SSO 登录的 Kerberos 用户不需要输入当前登录用户密码。

步骤 2 输入当前用户的密码。

步骤 3 单击“确定”。

----结束

修改 Kerberos 用户组

步骤 1 在“Kerberos 用户组”区域中，单击待修改的 Kerberos 用户组右侧的 。

步骤 2 根据表 3-46 的说明修改 Kerberos 用户组配置。

步骤 3 单击“保存”。

----结束

3.6.4 双因素认证

功能介绍

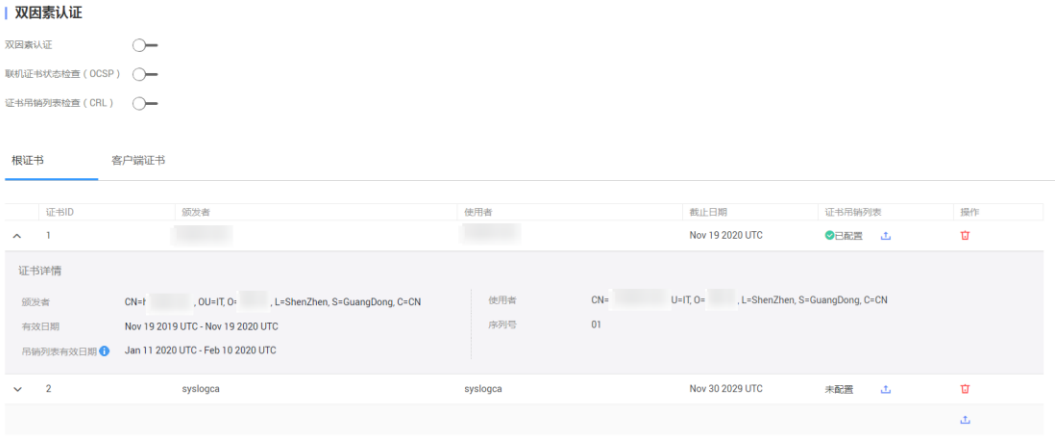
双因素认证是使用客户端证书密码以及证书来进行认证，登录时需要同时拥有客户端证书及证书密码才能认证通过，解决了传统的帐号口令认证中口令泄露导致的入侵问题。

您可以通过“双因素认证”界面将从正式的 CA 认证机构申请的根证书和客户端证书上传到 iBMC，实现客户端与 iBMC WebUI 的安全对接。

界面描述

在导航栏中选择“用户&安全 > 双因素认证”，打开如图 3-40 所示界面。

图3-40 双因素认证



参数说明

表3-47 双因素认证

参数	描述
双因素认证	是否使能双因素认证功能。使能该功能后，在客户端登录 iBMC WebUI 时，将使用证书认证登录，而不是需要输入用户名和密码的登录界面登录。 •  表示启用双因素认证功能。 •  表示停用双因素认证功能。 **说明** • 启用双因素认证功能前，必须导入有效的根证书和客户端证书。且必须存在至少一套可用证书，否则，在后续登录时会出现无法认证的情况。 • 启用双因素认证功能后，系统会自动关闭 SSH 服务，且无法手动

参数	描述
	开启。 • 启用再禁用双因素认证功能后，SSH 服务不会自动开启，若需要使用 SSH 服务，请手动开启。 • 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。
联机证书状态检查（OCSP）	须知 • 联机证书状态检查采用 OCSP（Online Certificate Status Protocol）进行验证，启用前请确认与 OCSP 服务器通信良好，否则可能导致 Web 服务不可用。 • 请确保根证书中已写入 OCSP 地址信息，否则开启此功能后，双因素认证可能失败。 认证过程中，是否检查证书的合法性。使能该功能后，在登录 iBMC WebUI 过程中，会检查当前客户端证书的合法性，若其为已过期或已撤销的证书，则无法通过认证，即无法登录 iBMC WebUI。 •  表示启用联机证书状态检查功能。 •  表示停用联机证书状态检查功能。
证书吊销列表检查（CRL）	认证过程中，检查证书是否已被吊销。使能该功能后，在登录 iBMC WebUI 过程中，会检查当前客户端证书是否已被吊销，若其为已被吊销的证书，则无法通过认证，即无法登录 iBMC WebUI。 说明 请确保已导入证书吊销列表，否则开启此功能后，双因素认证可能失败。
根证书	iBMC 上已存在的根证书列表，并显示每个根证书的颁发者、使用者、截止日期、证书吊销列表以及吊销列表有效日期。 iBMC 最多支持 16 个根证书。 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。 • 吊销列表过期会导致相应的认证功能失败。
客户端证书	iBMC 上已存在的客户端证书列表，并显示每个客户端证书绑定的用户名、角色、根证书上传状态、吊销状态和吊销时间以及客户端证书指纹（即客户端证书文件的哈希值）。 iBMC 最多支持 16 个用户对应的客户端证书。 说明 客户端证书有以下几种吊销状态： • 已吊销 • 未吊销

参数	描述
	• 未上传

启用双因素认证并上传证书到 iBMC

- 在此操作之前，请通过正式的 CA 证书颁发机构申请根证书和客户端证书（包括公钥证书和私钥证书）。

  说明

  - 私钥证书的常见格式为.pem、.p12、.pdx。相关操作请查询该证书机构的操作说明。
  - 请定期更新证书，否则可能存在安全风险。

- 支持上传 Base64 编码的根证书和客户端证书（公钥证书），证书格式包括：*.cer、*.crt、*.pem。

步骤 1 单击 。

选择待上传的证书文件。在“根证书”页签中上传的是根证书文件，在“客户端证书”页签中为指定用户上传客户端公钥证书。

步骤 2 单击“打开”。

界面提示“操作成功”。

步骤 3 将“双因素认证使能”右侧的状态设置为 。

----结束

为指定证书配置证书吊销列表

说明

证书吊销文件的格式为“*.crl”，编码格式为 Base64，最大不超过 100KB。

步骤 1 从证书颁发机构获取证书吊销文件。

步骤 2 单击指定证书对应的“证书吊销列表”的 。

步骤 3 选择证书吊销文件。

----结束

使用证书认证方式登录 iBMC

在“双因素认证”页面完成证书导入后，您可以通过如下的设置实现对 iBMC WebUI 的证书登录。

步骤 1 在客户端打开浏览器，例如 Google Chrome（例如 Google Chrome 81.0.4044.138，不同类型和版本的浏览器操作方法略有差异）。

步骤 2 单击浏览器右上角的 ，并打开“隐私设置和安全性”区域的隐私配置项。

步骤 3 单击“管理证书”。

步骤 4 在证书管理窗口中，导入客户端私钥证书。

说明

导入过程中需要输入的密码，为申请证书时设置的密码。

步骤 5 重新在 Chrome 的地址栏中输入 iBMC 地址登录。

步骤 6 按照提示信息选择当前客户端证书。

可成功登录 iBMC WebUI。

----结束

删除根证书

说明

只有双因素认证功能处于停用状态，才能成功删除根证书。

步骤 1 在“根证书”页签中，单击指定根证书后的 。

弹出操作确认对话框。

步骤 2 单击“确认”。

----结束

删除客户端证书

步骤 1 在“客户端证书”页签中，单击指定根证书后的 。

弹出操作确认对话框。

步骤 2 单击“确认”。

----结束

3.6.5 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 3-41 所示界面。

图3-41 在线用户

参数说明

表3-48 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。 • “Redfish”表示用户通过 Redfish 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。
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。

3.6.6 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

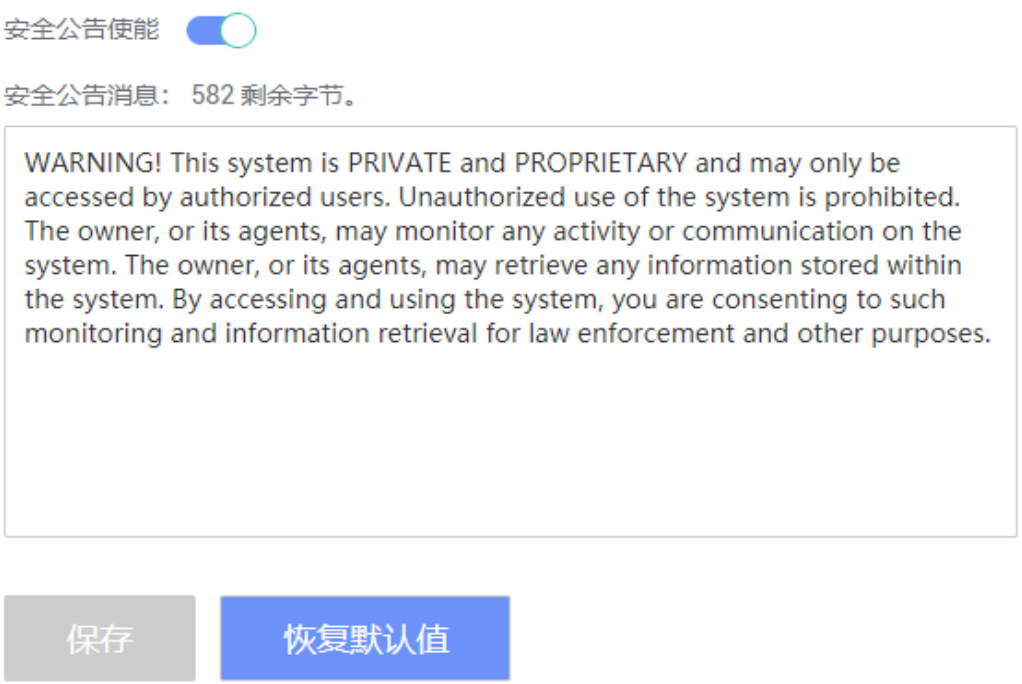
在导航栏中选择“用户&安全 > 安全配置”，打开如图 3-42、图 3-43、图 3-44 和图 3-45 所示界面。

图3-42 安全增强

图3-43 登录规则

图3-44 权限管理

图3-45 安全公告



参数说明

表3-49 安全增强

参数	描述

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。
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。

参数	描述
	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”。
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。

参数	描述
	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3-50 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。
MAC 段	规则允许的用户的具体 MAC 地址或 MAC 地址头。支持如下

参数	描述
	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3-51 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）

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
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

参数	描述
	• 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3-52 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 3-49 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、Redfish 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 3-50 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。

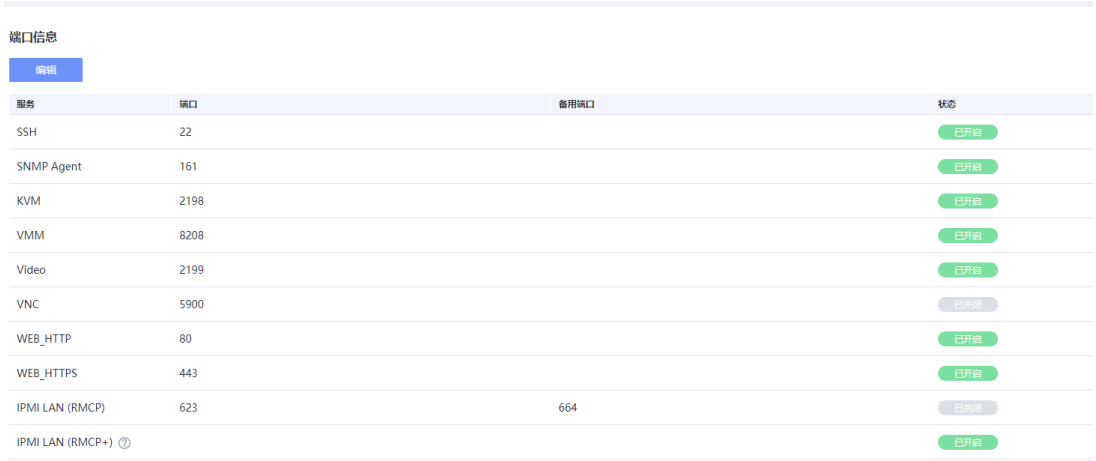
说明

- 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 3-46 所示界面。

图3-46 端口服务



参数说明

表3-53 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 3.5.3 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 Redfish 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 为不安全的弱签名算法，iBMC 不支持导入弱签名算法(MD5)证书。

界面描述

在导航栏中选择“服务管理 > Web 服务”，打开如图 3-47 所示界面。

图3-47 Web 服务

参数说明

表3-54 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 Redfish 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 3-48 所示。

图3-48 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 为不安全的弱签名算法，iBMC 不支持导入弱签名算法(MD5)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 为不安全的弱签名算法，iBMC 不支持导入弱签名算法(MD5)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 3-49 所示界面。

图3-49 虚拟控制台

参数说明

表3-55 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

参数	说明
	此参数不允许设置为空。
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。
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

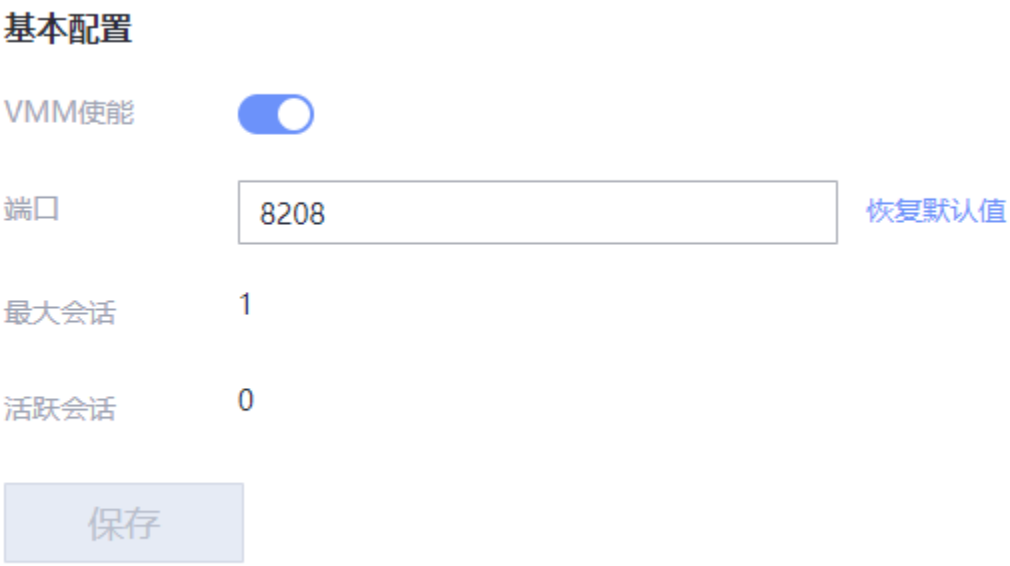
从远端控制服务器实时桌面时需要用到的 VMM（Virtual Media Manager）服务，开启后可使用虚拟光驱、虚拟软驱等功能。

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 3-50 所示界面。

图3-50 虚拟媒体



参数说明

表3-56 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。
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 3-51 所示界面。

图3-51 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3-57 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。

参数	说明
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。
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 3-52 所示界面。

图3-52 SNMP 功能

参数说明

表3-58 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

参数	说明
	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。	
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。 默认取值：**roAdministrator@9000** 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** <*filepath* | *file_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。
读写团体名	SNMP 协议读写团体名。 默认取值：**rwAdministrator@9000**

参数	说明
	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** <*filepath* | *file_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。	
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**

参数	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
- NCSI VLAN 属性
- LLDP 属性

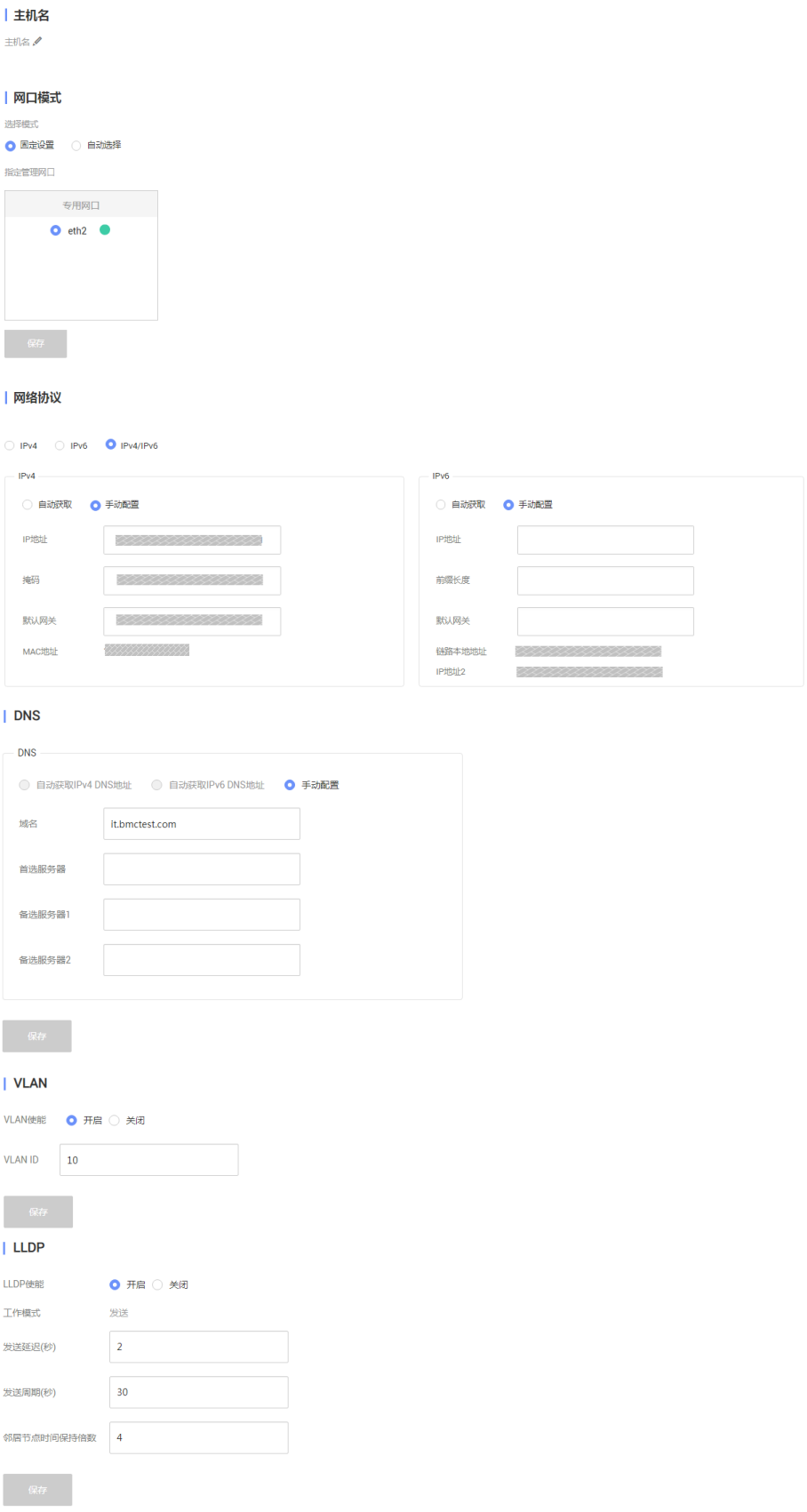
须知

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 3-53 所示界面。

图3-53 网络配置


主机名
主机名
网口模式
选择模式
固定设置
自动选择
指定管理网口
专用网口
eth2
保存
网络协议
IPv4
IPv6
IPv4/IPv6
IPv4
自动获取
手动配置
IP地址
掩码
默认网关
MAC地址
IPv6
自动获取
手动配置
IP地址
前缀长度
默认网关
链路本地地址
IP地址2
DNS
DNS
自动获取IPv4 DNS地址
自动获取IPv6 DNS地址
手动配置
域名
it.bmctest.com
首选服务器
备选服务器1
备选服务器2
保存
VLAN
VLAN使能
开启
关闭
VLAN ID
10
保存
LLDP
LLDP使能
开启
关闭
工作模式
发送
发送延迟(秒)
2
发送周期(秒)
30
邻居节点时间保持倍数
4
保存

参数说明

表3-59 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、OCP 扩展网口或 PCIe 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） ● 专用网口 > OCP 扩展网口（Port1～Port2 或 Port1～Port4） **说明** 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。
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。

参数	说明
	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 Autoconfiguration）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。
	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

参数	说明
	• 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 **说明** 仅在专用网口作为 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。
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	若邻居节点在指定时间内（发送周期×邻居节点时间保持倍

参数	说明
倍数	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：

- 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 3-54 所示界面。

图3-54 NTP&时区

参数说明

表3-60 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。

参数	描述
	• 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，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。
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

参数	描述
	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	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
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 MD5 和 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 3-60 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。
- 进行主备分区镜像倒换。
- 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。
- 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 3-55 所示界面。

图3-55 固件升级

参数说明

表3-61 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。
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”。

界面提示“主备分区镜像倒换成功”。

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 配置更新

功能介绍

您可以通过“配置更新”界面实现服务器 iBMC、BIOS 和 RAID 控制器配置文件的导入和导出。

详细配置文件请参见 8 配置文件说明章节。

说明

- 仅管理员用户可进行配置导入或配置导出操作。
- 在 KVM 开启的情况下，不支持导入关于 KVM 加密功能的设置。仅 KVM 加密功能的设置受此条件限制，不影响其他特性配置的导入。
- RAID 控制器配置需在系统 POST 完成之后导出才有效。

- 当导入配置项涉及修改 TLS 版本、网络配置时，可能导致 Web 连接断开，Web 提示“导入失败”，此时需重新登录 iBMC 查看操作日志确认是否导入成功。
- 在导出的配置文件中，如果某个配置项默认为密文，在导入其他服务器时无法生效。若需要在其他服务器上导入该配置项信息，则需要将配置文件中对应信息修改为明文，并删除该行注释符后才能支持导入生效。
- 导出的配置文件不体现 iBMC 管理网口的 IP 地址信息。
- 仅支持导入导出 iBMC 配置、BIOS 配置和部分的 RAID 控制器配置。

界面描述

在导航栏中选择“iBMC 管理 > 配置更新”，打开如图 3-56 所示界面。

图3-56 配置更新

导入配置文件

步骤 1 （可选）编辑配置文件。

1. 使用文本工具打开待导入的配置文件并找到需要编辑的配置项。
2. 编辑配置项信息。

   下面以“SenderName”为例进行说明，如图 3-57 所示。将“SenderName”的值由“******”改为实际的字符串，例如“Sendertext123456789012@xxx.com”。

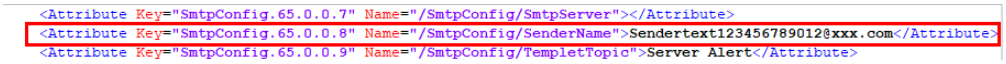
   图3-57 编辑前的配置文件

```
<Attribute Key="SmtpConfig.65.0.0.7" Name="/SmtpConfig/SmtpServer"></Attribute>
<!--<Attribute Key="SmtpConfig.65.0.0.8" Name="/SmtpConfig/SenderName">******</Attribute>-->
<Attribute Key="SmtpConfig.65.0.0.9" Name="/SmtpConfig/TempletTopic">Server Alert</Attribute>
```

3. 将“SenderName”参数前后的注释标识“<!--”和“-->”删除。

   修改后的配置文件如图 3-58 所示。

图3-58 编辑后的配置文件



4. 保存修改。

步骤 2 单击"配置导入"区域的 ，并选择要上传的配置文件。

文件上传后，显示在"配置导入"区域。

步骤 3 单击“导入”。

导入成功后，弹出对话框提示以下信息：

```
导入成功，BIOS 配置需要重启业务系统生效。
```

- iBMC 配置项和 RAID 控制器配置项导入后立即生效。
- BIOS 配置项导入后，需要重启服务器操作系统才能生效。
  - 若选择“稍后重启”，您可以在合适的时间重启服务器操作系统。
  - 若选择“立即重启”，则将跳转到服务器上下电界面，您可以根据实际情况选择合适的方式重启服务器操作系统。

说明

RAID 控制器配置项中，仅支持“回拷”、“SMART 错误时回拷”和“JBOD 模式”三个参数项的配置导入。不包括逻辑盘和物理盘等其他参数的配置导入。

----结束

导出配置文件

步骤 1 单击“配置更新”页面中的“导出”。

文件开始导出并自动保存到本地 PC 默认路径。

----结束

3.8.5 语言管理

功能介绍

通过使用“语言管理”界面的功能，您可以安装和卸载语言包以及将 iBMC 系统界面的语言更改为选定的支持语言。

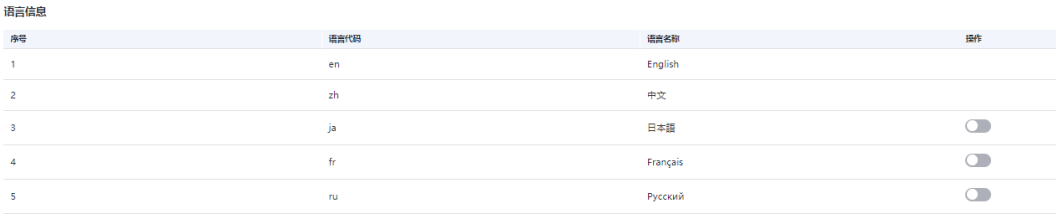
说明

- 仅管理员及具有常规设置类权限的用户有权限安装和卸载语言包。
- 当前仅支持中、英、日、法四种语言：
- 仅日文和法文语言包可升级和卸载。
- 英语和中文语言包不支持升级或卸载。
- 升级语言包操作需在“iBMC 管理 > 固件升级”页面进行。

界面描述

在导航栏中选择“iBMC 管理 > 语言管理”，打开如图 3-59 所示界面。

图3-59 语言管理



参数说明

表3-62 语言更新

参数	描述
语言代码	某种语言的代码。例如“en”代表英语，“zh”代表中文，“ja”代表日文，“fr”代表法文。
语言名称	显示语言代码代表的语种名称。
操作	单击  可以卸载对应的语言包。

查看已安装的语言

步骤 1 选择“iBMC 管理”。

步骤 2 在左侧导航树中，选择“语言管理”。

右侧显示“语言管理”界面，可查看到当前已安装的语言。

----结束

安装或升级语言包

步骤 1 下载待升级的目标语言包。

步骤 2 升级语言包。

1. 登录 iBMC WebUI。
2. 在导航栏中选择“iBMC 管理 > 固件升级”。
3. 单击固件升级区域框的 并选择待上传的文件。
4. 单击“升级”。

iBMC 系统开始执行升级操作。

升级完成后，可在界面右上角将 iBMC 系统界面的语言更改为选定的支持语言。

----结束

卸载语言包

步骤 1 在“语言管理”界面中，单击需要卸载的语言右侧的  。

弹出确认删除对话框。

步骤 2 单击“确认”。

卸载完成后“语言管理”界面将显示“操作成功”提示信息。

----结束

3.8.6 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。

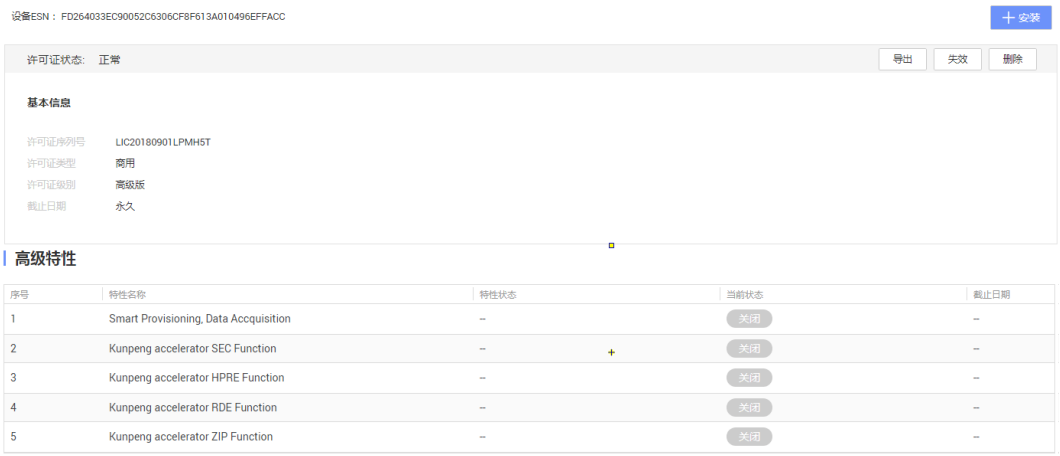
iBMC 高级版较标准版提供更多的高级特性，例如：

- 通过 Redfish 实现 OS 部署。
- 使能加速引擎，包括硬件安全加速引擎（SEC，Security Engine）、高性能 RSA 加速引擎（HPRE，High Performance RSA Engine）、RAID DIF 运算加速引擎（RDE，RAID DIF Engine）、ZIP 四个加速器。

界面描述

在导航栏中选择“iBMC 管理 > 许可证管理”，打开如图 3-60 所示界面。

图3-60 许可证管理



参数说明

表3-63 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。
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。

参数	描述
	• 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。

3.8.7 iBMA 管理

功能介绍

iBMA（Baseboard Management Agent）为带内管理代理软件，以下简称 iBMA。

通过“iBMA 管理”界面，可实现通过远程控制台将 iBMA 安装到操作系统中。iBMA 安装成功后，此界面将显示 iBMA 的基本信息，包括版本号、运行状态和驱动版本。

界面描述

在导航栏中选择“iBMC 管理 > iBMC 管理”，打开如图 3-61 所示界面。

图3-61 BMA 管理

参数说明

表3-64 iBMA 管理

参数	描述
可安装的 iBMA 版本	当前对应操作系统下，可安装的 iBMA 版本。 如显示 Linux 和 1.10，表示当前 Linux 操作系统下，可安装的 iBMA 版本为 1.10。
安装程序状态	可安装的 iBMA 连接服务器操作系统的状态。 ● “未就绪”表示未连接服务器操作系统或连接服务器操作系统失败。 ● “已就绪”表示连接服务器操作系统成功。
iBMA 状态	
iBMA 版本	显示服务器操作系统中安装的 iBMA 版本信息。 此参数项显示为“--”时，表示 iBMA 未安装或 iBMA 已安装但未运行。
iBMA 运行状态	显示 iBMA 软件的运行状态。 ● 此参数项显示为“--”时，表示 iBMA 未安装或 iBMA 已安装但未运行。 ● 此参数项显示为“Running”时，表示 iBMA 已安装且正

参数	描述
	在运行。
iBMA 驱动版本	显示 iBMA 的驱动版本信息。 此参数项显示为“--”时，表示 iBMA 未安装或 iBMA 已安装但未运行。

安装 iBMA

说明

- 当前仅 Linux 系统的客户端，可通过本界面安装 iBMA。
- 需要远程媒体权限才能挂载 iBMA 驱动盘。
- 需要远程控制权限才能启动远程控制台。
- 需要同时具有远程媒体和远程控制权限才能点击“安装 iBMA”。

步骤 1 单击“安装 iBMA”。

iBMA 将连接服务器操作系统。连接成功后，弹出“安装说明”页面。

步骤 2 单击“安装说明”页面的“启动远程控制台”。

将启动远程控制台。

步骤 3 在打开的远程控制台界面以管理员身份登录服务器操作系统，输入服务器操作系统的用户名和密码。

步骤 4 在服务器操作系统的设备列表中找到标签为“iBMA”的驱动盘。若操作系统图形界面没有显示 iBMA，请先挂载该设备后，继续执行步骤 5。挂载 iBMA 驱动盘的步骤请参见挂载 iBMA 驱动盘。

步骤 5 打开 Linux 下的“README.TXT”文件，查看“Supported Operating Systems in this Release”中列出的 Linux 系统版本信息。

1. 在服务器操作系统界面空白处单击鼠标右键，打开菜单。
2. 单击菜单中的 Open Terminal。打开服务器操作系统命令行界面。
3. 依次执行 cd Linux 和 ls，查看 Linux 下的“README.TXT”文件信息。

```
[root@localhost ~]# cd Linux
[root@localhost Linux]# ls
app config drivers install.sh README.TXT script
```

4. 执行 cat README.TXT。

```
[root@localhost ~]# cat README.TXT
iBMA on-board installation package
Version 2.1.3.020

*********************************************************************
Installation
*********************************************************************

* On the Linux operating systems, execute "sh install.sh -s" from the "Linux" directory to install iBMA
silently and execute "sh install.sh -u" to upgrade iBMA.

For more information on installation instructions, includingsilent installation options, see the "iBMA
2.0 User Guide".

*********************************************************************
Supported Operating Systems in this Release
*********************************************************************

* EulerOS 2.0 SP8
* CentOS 7.6 on aarch64
--More details on limitations and supported Operating Systems can be located in the "iBMA 2.0 User
Guide".
```

- 如果当前已安装 Linux 版本与“Supported Operating Systems in this Release”中列出的任意一个 Linux 系统版本相同，执行步骤 6。
- 如果当前已安装 Linux 版本与“Supported Operating Systems in this Release”中列出的 Linux 系统版本都不同，请将当前 Linux 系统版本更新至与“README.txt”文件中显示的任意一个 Linux 系统版本相同后，执行步骤 6。

步骤 6 根据表 3-65 所示信息并参阅最新版本的 iBMA 用户指南，进行安装 iBMA 操作。

关于安装 iBMA 的详细操作步骤，请获取并参阅最新版本的 iBMA 用户指南。

表3-65 操作系统与安装文件路径关系表

操作系统	安装文件路径
Linux	Linux/install.sh

----结束

挂载 iBMA 驱动盘

步骤 1 在服务器操作系统界面空白处单击鼠标右键，打开菜单。

步骤 2 单击菜单中的 Open Terminal。打开服务器操作系统命令行界面。

步骤 3 执行 lsscsi 命令查询 iBMA 驱动盘的属性。

```
[root@localhost ~]# lsscsi
[0:0:0:0]    disk    ATA     ST4000NM0033-9ZM SN06  -
[0:0:1:0]    disk    ATA     ST4000NC001-1FS1 CN02  -
[0:0:2:0]    disk    ATA     WDC WD6000F9PZ-3 0R01  /dev/sdc
[0:0:3:0]    disk    ATA     WDC WD6000F9PZ-3 0R01  /dev/sdd
[0:0:4:0]    disk    HGST     HUS726060AL4210  A523  -
[0:0:5:0]    disk    HGST     HUS726060AL4210  A7MH  -
[0:0:6:0]    disk    ATA     SSDSC2BB016T7H   0121  /dev/sde
```

```
[0:0:7:0]    disk    HGST     HUS726060AL4210  A523  /dev/sdf
[0:1:0:0]    disk    LSI      Logical Volume   3000  /dev/sdb
[0:1:1:0]    disk    LSI      Logical Volume   3000  /dev/sda
[19:0:0:0]   disk    SERVER   iBMA USB Device   225  /dev/sdv
```

命令回显“disk SERVER iBMA USB Device 225 /dev/sdv”中，iBMA USB Device 表示 iBMA 驱动盘节点名称，/dev/sdv 表示操作系统分配给 iBMA 驱动盘的盘符。

步骤 4 执行 mount /dev/sdv /home/file 将 iBMA 驱动盘挂载到/home/file 路径下。

/home/file 为实际挂载 iBMA 驱动盘时的挂载文件存放路径，请根据实际操作需要创建 路径。此处创建的路径中，文件夹名称支持的字符包括数字、字母、下划线（_）、中 横线（-）和点号（.）。

```
[root@localhost ~]# mount /dev/sdv /home/file
#
```

步骤 5 执行 ls/home/file 检查 iBMA 驱动盘是否已挂载成功。

```
[root@localhost ~]# ls /home/file
Linux
```

命令回显返回 Linux 表示 iBMA 驱动盘已挂载成功。

----结束

3.8.8 SP 管理

功能介绍

SP（Smart Provisioning）为服务器智能部署工具软件，以下简称 SP。

通过“SP 管理”界面，您可以配置设备信息收集功能。

参数说明

表3-66 SP 管理

参数	描述
设备信息收集使能	开启或禁止设备信息收集功能。 该功能开启后，服务器电源模块通电后，带内系统首次上电时，带内系统会先进入 SP 收集设备信息，然后再按照“BIOS 设置”中“优先引导介质”和“启动顺序”的配置来启动服务器。

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 3-62 所示界面进入虚拟控制台。

图3-62 虚拟控制台

参数说明

表3-67 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

参数	描述
	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。
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 3-68 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3-68 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 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
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

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。
- 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 IE 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://*IP address*/remoteconsole?openWay=html5”或“https://*IP address*/remoteconsole?openway=html5”
      - “https://*IP address*/remote_access.asp?authParam=*key*&lp=*lang*&openWay=html5”或“https://*IP address*/remote_access.asp?authParam=*key*&lp=*lang*&openway=html5”
    - Java 集成远程控制台推荐登录方式：
      - “https://*IP address*/remoteconsole”或“https://*IP address*/remoteconsole?openWay=jre”或“https://*IP address*/remoteconsole?openway=jre”
      - “https://*IP address*/remote_access.asp?authParam=*key*&lp=*lang*&openWay=jre”或“https://*IP address*/remote_access.asp?authParam=*key*&lp=*lang*&openway=jre”

说明

- *key* 可通过 Redfish 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://*IP address*/kvmvmm.asp”
  - 方式三：“https://*IP address*/login.html?redirect_type=1”

说明

“*IP address*”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 3-69 所示。

表3-69 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
	“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。

按钮	说明
	• 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。
	“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。

按钮	说明
	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 3-70 所示。

图3-63 HTML5 KVM

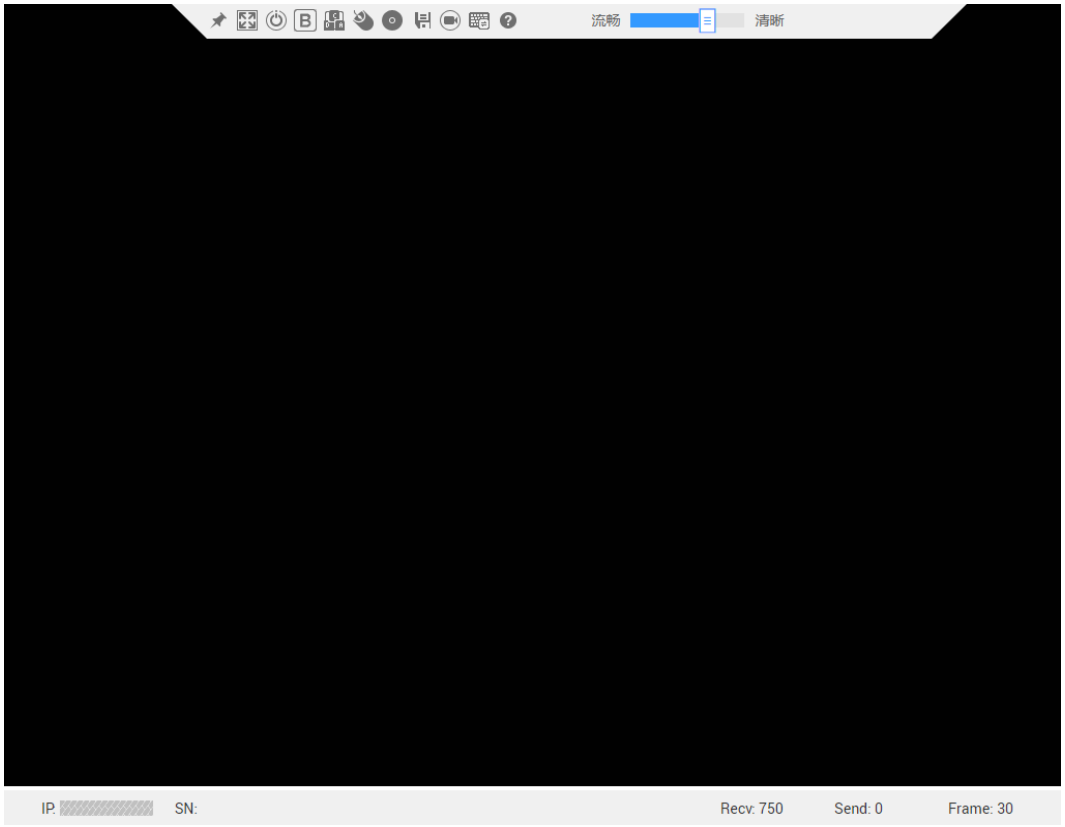


表3-70 HTML5 KVM

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。

----结束

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。

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 3-69 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 3-69 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 3-64 的界面。

图3-64 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 3-64 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 3-65 的界面。

图3-65 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 3-65 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 3-66 所示的界面。

图3-66 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 3-66 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 3-71 所示。

表3-71 按钮说明

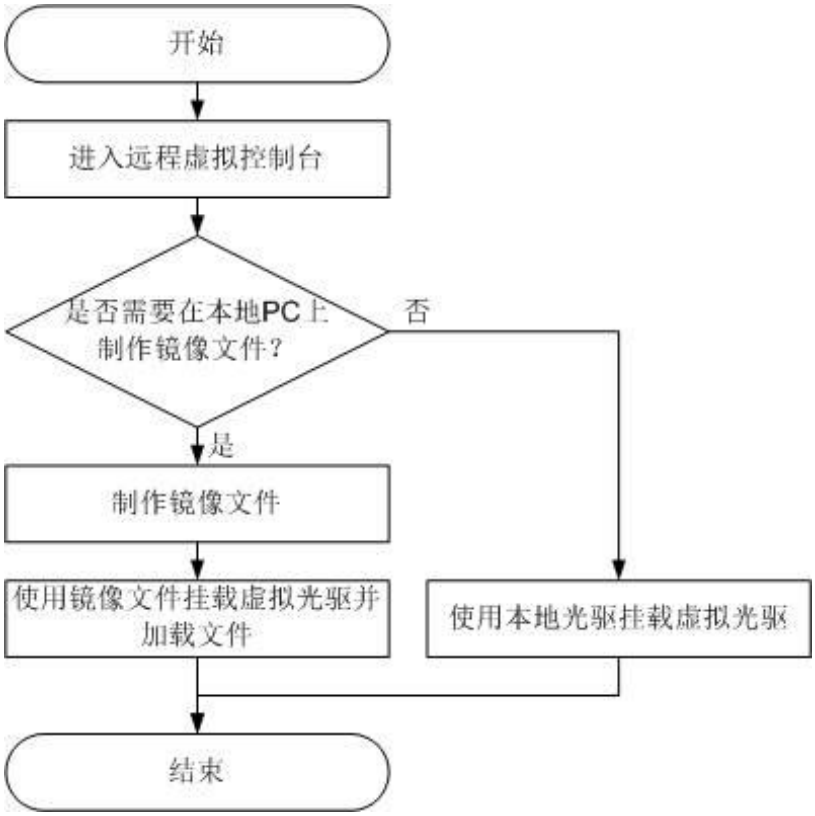
按钮	说明
	浮动按钮。表示当前工具栏被固定。
	浮动按钮。表示当前工具栏被隐藏。
	“全屏”按钮。表示全屏显示服务器的实时桌面。 **说明** 在全屏显示实时桌面时，鼠标移动到屏幕上方会显示工具栏。
	“鼠标同步”按钮。表示纠正鼠标位置。 **说明** 在全屏显示实时桌面且“鼠标控制”为“单鼠标”模式时，此时单击“切换鼠标模式”后，该按钮才可用。
	“切换鼠标模式”按钮。表示切换鼠标模式。 **说明** 在全屏显示实时桌面且在“单鼠标”模式下时，该按钮才可用。
	“返回”按钮。表示返回合适的屏幕显示服务器的实时桌面。 **说明** 只有全屏显示服务器的实时桌面时，工具栏中才会出现该按钮。
	“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

按钮	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。
	“光驱”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。
	“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。

按钮	说明
num	“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	“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	“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 3-67 所示。

图3-67 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 3-72 所示。

图3-68 Java KVM

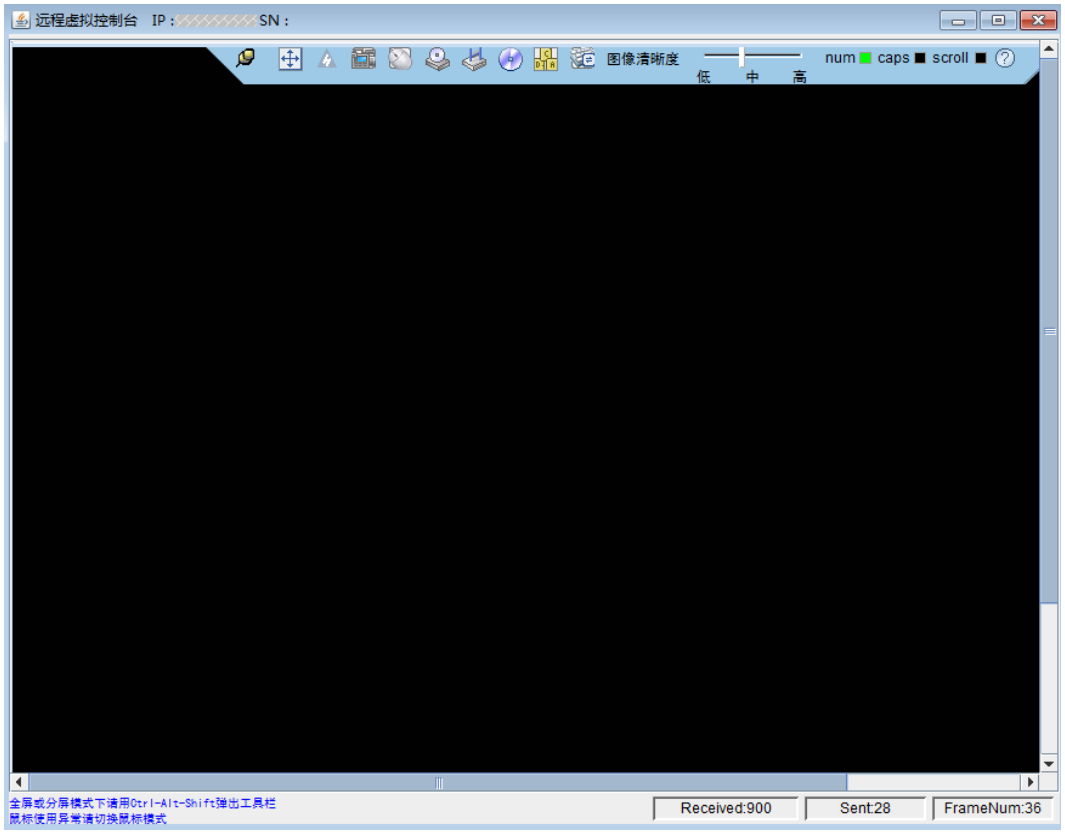


表3-72 Java KVM

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。

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 3-71 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。

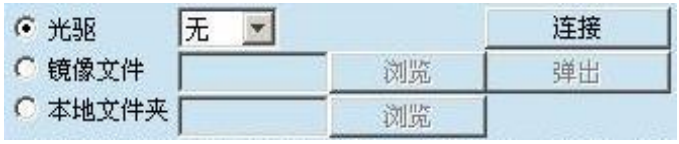
挂载虚拟光驱

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 3-69 所示的界面。

图3-69 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 3-69 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 3-69 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 3-70 所示的界面。

图3-70 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 3-70 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 3-70 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

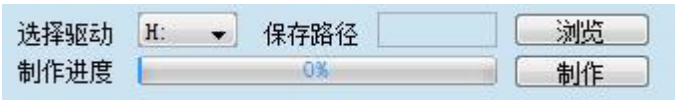
本操作使用软驱或光驱中的软盘或光盘制作镜像文件。制作成功的镜像文件保存在本地 PC 上。它可以用于挂载和加载虚拟软驱或光驱。

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 3-71 所示的界面。

图3-71 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 3-71 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。

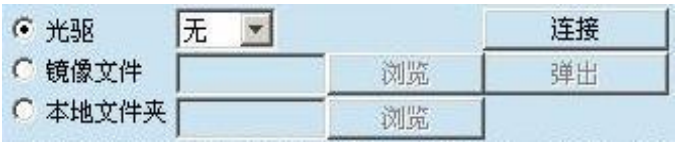
须知

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 3-72 所示的界面。

图3-72 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	KVM 客户端与服务端建立连接前，需要进行

问题描述	可能原因
示“设置信任证书超时，无法开启 KVM”。	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

3.10.4 打开 KVM 后显示与管理系统连接失败

问题现象

问题描述	可能原因
打开 KVM 后，KVM 界面显示“与管理系统连接失败，管理系统的 IP 为 xx.xx.xx.xx”。	KVM 服务默认端口为 2198，当该服务端口未开启或端口不通时，会出现此错误。

解决方案

步骤 1 打开 iBMC WebUI 中的“服务管理 > 端口服务”页面，查看“KVM”服务是否已开启。

- 是=> 步骤 2
- 否=> 步骤 3

步骤 2 打开本地命令提示符（CMD），运行 **telnet**，例如 telnet *xx.xx.xx.xx 2198*，测试 KVM 服务端口是否可以访问。

xx.xx.xx.xx 表示 IP 地址，**2198** 为 KVM 默认端口号，实际端口号以步骤 1 中查询到的端口号为准。

- 是=> 步骤 5
- 否=> 步骤 4

步骤 3 开启 KVM 服务，并重新连接 KVM 查看是否可以连接。

- 是=> 处理完毕
- 否=> 步骤 2

步骤 4 联系网络管理员开启 KVM 所需的端口，确保端口可以访问。确认端口可以访问后，重新连接 KVM，查看是否可以连接成功。

- 是=> 处理完毕
- 否=> 步骤 5

步骤 5 请联系技术支持处理。

----结束

3.11 一键收集信息说明

说明

iBMC V3.01.12.20 及以上版本不支持 MD5 类型的完整性校验码。

表3-73 一键收集信息说明

目录	子目录	文件名	文件内容说明
-	-	dump_app_log	iBMC 收集结果列表
		dump_log	一键收集结果列表
AppDump	User	User_dfl.log	User 模块管理对象的信息
	card_manage	card_manage_dfl.log	Card_Manage 模块管理对象的信息
		card_info	当前服务器在位板卡的信息
		sdi_card_cpld_info	SDI V3 卡的 CPLD 寄存器信息 说明 只有适配且已正确安装了 SDI V3 卡的产品支持收集此信息。
	BMC	BMC_dfl.log	iBMC 模块管理对象的信息
		fruinfo.txt	FRU 电子标签信息
		lldp_info.txt	LLDP 配置及报文统计信息
		nandflash_info.txt	NAND flash 信息
		net_info.txt	网口配置信息
		ntp_info.txt	NTP 同步失败时的错误信息
		psu_info.txt	服务器上配置的电源信息
		time_zone.txt	iBMC 时区信息
	PowerMgnt	PowerMgnt_dfl.log	PowerMgnt 模块管理对象的信息
		power_statistics.csv	功率统计信息
		power_bbu_info.log	BBU 模块日志（仅针对支持 BBU 模块的服务器）
	UPGRADE	UPGRADE_dfl.log	Upgrade 模块管理对象的信息
		upgrade_info	iBMC 相关器件的版本信息
	BIOS	BIOS_dfl.log	BIOS 模块管理对象的信息
		bios_info	BIOS 配置信息
		registry.json	BIOS 的注册文件，显示所有的 BIOS 项信息
		currentvalue.json	当前设置的 BIOS 项
		setting.json	通过 redfish 设置但尚未生效的 BIOS 项

目录	子目录	文件名	文件内容说明
		result.json	通过 redfish 设置的 BIOS 项结果
	discovery	discovery_dfl.log	Discovery 模块管理对象的信息
	agentless	agentless_dfl.log	Agentless 模块管理对象的信息
	ddns	ddns_dfl.log	Ddns 模块管理对象的信息
	diagnose	diagnose_dfl.log	Diagnose 模块管理对象的信息
		diagnose_info	Port 80 的故障诊断信息以及 IFMM 模块内存占用信息 **说明** 当前暂不支持收集此项信息。
	Snmp	Snmp_dfl.log	Snmp 模块管理对象的信息
	cooling_app	cooling_app_dfl.log	Cooling 模块管理对象的信息
		fan_info.txt	风扇型号、转速等详细信息
	CpuMem	CpuMem_dfl.log	CpuMem 模块管理对象的信息
		cpu_info	服务器配置的 CPU 参数的详细信息
		mem_info	服务器配置的内存参数的详细信息
	kvm_vmm	kvm_vmm_dfl.log	KVM_VMM 模块管理对象的信息
	ipmi_app	ipmi_app_dfl.log	IPMI 模块管理对象的信息
		ipmbeth_info.txt	管理系统的 IPMI 通道状态
	LicenseMgnt	alm_protected.persist	License 管理组件 ALM 的持久化文件
		LicenseMgnt_dfl.log	管理对象信息
		first_protected.persist	License 管理组件 ALM 的持久化文件
		second_protected.persist	License 管理组件 ALM 的持久化文件
		lm_info	License 的状态、设备 ESN 等信息
	Dft	Dft_dfl.log	DFT 模块管理对象的信息
	net_nat	net_nat_dfl.log	Net_NAT 模块管理对象的信息
	PcieSwitch	PcieSwitch_dfl.log	PCIeSwitch 模块管理对象的信息
		RetimerRegInfo	Retimer 芯片寄存器信息
		pcieswitch_info	PCIeSwitch 模块的固件版本说明
	sensor_alarm	sensor_alarm_dfl.log	Sensor_Alarm 模块管理对象的信息

目录	子目录	文件名	文件内容说明
		sensor_info.txt	服务器所有传感器信息列表
		current_event.txt	服务器当前健康状态和告警事件
		sel.tar	当前 sel 信息和历史 sel 信息打包文件
		sensor_alarm_sel.bin.md5	sel 原始记录文件完整性校验码
		sensor_alarm_sel.bin.bak.md5	sel 原始记录备份文件完整性校验码
		sensor_alarm_sel.bin.sha256	sel 原始记录文件完整性校验码
		sensor_alarm_sel.bin.bak.sha256	sel 原始记录备份文件完整性校验码
		sensor_alarm_sel.bin.bak	sel 原始记录备份文件
		sensor_alarm_sel.bin	sel 原始记录文件
		sel.db	sel 数据库文件
		LedInfo	服务器当前 LED 灯的显示状态
		sensor_alarm_sel.bin.tar.gz	sel 历史记录打包文件
	MaintDebug	MaintDebug_dfl.log	MaintDebug 模块管理对象的信息
	MCTP	mctp_info	MCTP 配置信息
		MCTP_dfl.log	MCTP 模块管理对象的信息
	FileManage	FileManage_dfl.log	FileManage 模块管理对象的信息
	switch_card	switch_card_dfl.log	Switch_Card 模块管理对象的信息
		phy_register_info	后插板 phy 寄存器信息
		port_adapter_info	后插板接口器件信息
	StorageMgnt	StorageMgnt_dfl.log	StorageMgnt 模块管理对象的信息
		RAID_Controller_Info.txt	当前 RAID 控制器/逻辑盘/硬盘的信息
	rimm	rimm_dfl.log	RIMM 模块管理对象的信息
	redfish	redfish_dfl.log	Redfish 模块管理对象的信息
		component_uri.json	部件 URI 列表
	dfm	dfm.log	DFM 模块管理对象的信息

目录	子目录	文件名	文件内容说明
		dfm_debug_log dfm_debug_log.1	PME 框架调试日志
3rdDump	-	error_log	Apache 错误日志
		access_log	Apache 访问日志
		error_log.1	Apache 错误日志备份文件
		access_log.1	Apache 访问日志备份文件
		httpd.conf	Apache http 配置文件
		httpd-port.conf	Apache http 端口配置文件
		httpd-ssl.conf	Apache https 配置文件
		httpd-ssl-port.conf	Apache https 端口配置文件
		httpd-ssl-protocol.conf	Apache https 协议版本配置文件
		httpd-ssl-ciphersuite.conf	Apache https 协议加密套件配置文件
BMALogDump	-	bma_debug_log bma_debug_log.1.gz bma_debug_log.2.gz bma_debug_log.3.gz	iBMA 日志
CoreDump	-	core-*（以“core-”开头的文件）	内存转储文件，根据系统运行情况可能产生一个或者多个文件，为应用程序 core dump 文件。
RTOSDump	sysinfo	cmdline	iBMC 内核的命令行参数
		cpuinfo	iBMC 内核的 CPU 芯片信息
		devices	iBMC 系统的设备信息
		df_info	iBMC 分区空间的使用信息
		diskstats	iBMC 的磁盘信息
		filesystems	iBMC 的文件系统信息
		free_info	iBMC 的内存使用概况
		interrupts	iBMC 的中断信息
		ipcs_q	iBMC 的进程队列信息
		ipcs_q_detail	iBMC 的进程队列详细信息
		ipcs_s	iBMC 的进程信号量信息

目录	子目录	文件名	文件内容说明
		ipcs_s_detail	iBMC 的进程信号量详细信息
		loadavg	iBMC 系统运行负载情况
		locks	iBMC 内核锁住的文件列表
		meminfo	iBMC 的内存占用详细信息
		modules	iBMC 的模块加载列表
		mtd	iBMC 的配置分区信息
		partitions	iBMC 所有设备分区信息
		ps_info	ps -elf iBMC 进程详细信息
		slabinfo	iBMC 内核内存管理 slab 信息
		stat	iBMC 的 CPU 利用率
		top_info	top -bn 1 显示当前 iBMC 进程运行情况
		uname_info	uname -a 显示当前 iBMC 内核版本
		uptime	iBMC 系统运行时间
		version	iBMC 当前的 RTOS 版本
		vmstat	iBMC 虚拟内存统计信息
	versioninfo	ibmc_revision.txt	iBMC 版本编译节点信息
		app_revision.txt	iBMC 版本信息
		build_date.txt	iBMC 版本构建时间
		fruinfo.txt	FRU 电子标签信息
		RTOS-Release	RTOS 版本信息
		RTOS-Revision	RTOS 版本标记号
		server_config.txt	服务器当前的配置信息
	networkinfo	ifconfig_info	网络信息，执行 ifconfig 的结果
		ipinfo_info	iBMC 配置的网络信息
		_data_var_dhcp_dhclient.leases	DHCP 租约文件
		dhclient.leases	DHCP 租约文件

目录	子目录	文件名	文件内容说明
		dhclient6.leases	DHCP 租约文件
		dhclient6_eth0.leases	DHCP 租约文件
		dhclient6_eth1.leases	DHCP 租约文件
		dhclient6_eth2.leases	DHCP 租约文件
		dhclient.conf	DHCP 配置文件
		dhclient_ip.conf	DHCP 配置文件
		dhclient6.conf	DHCP 配置文件
		dhclient6_ip.conf	DHCP 配置文件
		resolv.conf	DNS 配置文件
		netstat_info	netstat -a 显示当前网络端口、连接使用情况
		route_info	route 显示当前路由信息
		services	服务端口信息
	other_info	extern.conf	BMC 日志文件配置
		remotelog.conf	syslog 定制配置文件
		ssh	SSH 服务配置
		sshd_config	SSHD 服务配置文件
		logrotate.status	logrotate 状态记录文件
		login	login PAM 登录规则
		sshd	SSH PAM 登录规则
		pam_tally2	登录 iBMC 失败的锁定规则
		datafs_log	data 检测日志
		ntp.conf	NTP 服务配置
		vsftpd	FTP PAM 登录规则
	driver_info	dmesg_info	系统启动信息，执行 dmesg 的结果
		lsmod_info	当前加载驱动模块信息
		kbox_info	kbox 信息
		edma_drv_info	edma 驱动信息

目录	子目录	文件名	文件内容说明
		cdev_drv_info	字符设备驱动信息
		veth_drv_info	虚拟网卡驱动信息
SpLogDump	-	config	配置导出备份文件 说明 • SP 运行过程中无法收集此日志。 • SP 运行配置导出功能后可收集该日志。
		deviceinfo.json	服务器资产信息 说明 SP 运行过程中无法收集此日志。
		diagnose	硬件诊断日志 说明 • SP 运行过程中无法收集此日志。 • SP 运行硬件诊断功能后可收集该日志。
		DriveErase	硬盘擦除功能日志 说明 • SP 运行过程中无法收集此日志。 • SP 运行硬盘擦除功能后可收集该日志。
		iBMALogDump	iBMA 运行日志 说明 SP 运行过程中无法收集此日志。
		dmesg.log dmesg.tar.gz	小系统 dmesg 日志 说明 SP 运行过程中无法收集此日志。
		filepatchup_debug.log	极速部署文件打包日志 说明 • SP 运行过程中无法收集此日志。 • SP 运行极速部署功能后可收集该日志。
		images.log	极速部署克隆日志 说明 • SP 运行过程中无法收集此日志。 • SP 运行极速部署功能后可收集该日志。
		images_restore.log	极速部署还原日志 说明

目录	子目录	文件名	文件内容说明
			• SP 运行过程中无法收集此日志。 • SP 运行极速部署还原功能后可收集该日志。
		maintainlog.csv maintainlog.tar.gz	SP 维护日志。带时间戳的 maintainlog 文件为之前收集的日志。 **说明** SP 运行过程中无法收集此日志。
		operatelog.csv operatinglog.tar.gz	SP 运行日志。带时间戳的 operatinglog 文件为之前收集的日志。 **说明** SP 运行过程中无法收集此日志。
		ping6.log ping6.tar.gz	网络通信日志 **说明** SP 运行过程中无法收集此日志。
		quickdeploy_debug.log	极速部署日志 **说明** • SP 运行过程中无法收集此日志。 • SP 运行极速部署功能后可收集该日志。
		varmesg.log syslog.tar.gz	小系统信息日志 **说明** SP 运行过程中无法收集此日志。
		sp_upgrade_info.log	SP 自升级日志 **说明** • SP 运行过程中无法收集此日志。 • SP 运行自升级功能后可收集该日志。
		upgrade	SP 固件升级日志 **说明** SP 运行过程中无法收集此日志。
		version.json	SP 版本配置文件 **说明** SP 运行过程中无法收集此日志。
		version.json.*.sha	SP 版本配置文件的校验文件 **说明** SP 运行过程中无法收集此日志。
LogDump	netcard	netcard_info.txt netcard_info_bk.txt	网卡配置信息
	-	arm_fdm_log	FDM 日志

目录	子目录	文件名	文件内容说明
		arm_fdm_log.tar.gz	
		LSI_RAID_Controller_Log LSI_RAID_Controller_Log.1.gz LSI_RAID_Controller_Log.2.gz	LSI RAID 控制器的日志
		PD_SMART_INFO_C*	硬盘的 SMART 日志，*为 RAID 控制器的编号
		linux_kernel_log linux_kernel_log.1	Linux 内核日志
		operate_log operate_log.tar.gz mass_operate_log mass_operate_log.tar.gz	用户操作日志
		remote_log remote_log.1.gz	syslog test 操作日志、sel 日志
		security_log security_log.1	安全日志
		strategy_log strategy_log.tar.gz	运行日志
		fdm.bin fdm.bin.tar.gz	FDM 原始故障日志
		fdm_me_log fdm_me_log.tar.gz	ME 运行日志
		fdm_pfae_log	FDM 预告警日志
		fdm_mmio_log fdm_mmio_log.tar.gz	FDM 板卡配置日志
		maintenance_log maintenance_log.tar.gz	维护日志
		imu_log imu_log.tar.gz	IMU 运行日志（仅针对支持 IMU 模块的服务器）
		cpu1_m7_log cpu1_m7_log.tar.gz	CPU1 的 M7 协处理器运行日志（仅针对支持 M7 协处理器的服务器）
		cpu2_m7_log	CPU2 的 M7 协处理器运行日志（仅

目录	子目录	文件名	文件内容说明
		cpu2_m7_log.tar.gz	针对支持 M7 协处理器的服务器）
		ipmi_debug_log ipmi_debug_log.tar.gz	IPMI 模块日志
		ipmi_mass_operate_log ipmi_mass_operate_log.tar.gz	IPMI 模块运行日志
		app_debug_log_all app_debug_log_all.1.gz app_debug_log_all.2.gz app_debug_log_all.3.gz	所有应用模块调试日志
		agentless_driver_log agentless_driver_log.1.gz agentless_driver_log.2.gz agentless_driver_log.3.gz	agentless 驱动的日志文件
		kvm_vmm_debug_log kvm_vmm_debug_log.tar.gz	KVM 模块日志
		ps_black_box.log ps_black_box.log.1.gz ps_black_box.log.2.gz ps_black_box.log.3.gz	电源黑匣子日志
		third_party_file_bak.log	第三方文件备份日志记录
	storage	*_com_log *_com_log.1.gz ...	RAID 扣卡串口日志，如“RAID_Card1_com_log”
		drivelog	所有 SAS 和 SATA 硬盘的日志信息文件夹，其子目录根据硬盘名称命名，如：

目录	子目录	文件名	文件内容说明
			Disk0 ● SATA 盘的日志文件，如“SATA_Log”、“SMARTAttribute”、“SeagateFARMLog”、SeagateFARMLog.bin。 说明 SeagateFARMLog.bin 为 FARMlog 日志原始数据，iBMC V3.01.12.31 及以上版本不支持收集该日志文件。 ● SAS 盘的日志文件，如“SAS_Log”、“SAS_Log.1”。
		phy	所有 RAID 卡和该卡下 Expander 的 PHY 误码日志信息文件夹，其子目录根据 RAID 卡名称命名，如： RAID_Card1 ● RAID 卡 PHY 误码日志文件，如“RAID_Card1_PHY_Error_Count.csv”。 ● Expander 的 PHY 误码日志文件，如“RAID_Card1_Expander1_PHY_Error_Count.csv”。
	pciecard	PCIe 卡日志文件夹，命名格式为“PCIe 卡名称及其槽位号”_“网卡对外名称”。如：“PCIeCard6_SP570”。	所有网卡的日志，包括临终遗言、错误日志和巡检日志。如： ● “last_word_20160211182849” ● “error_log_20160211182532” ● “running_log_20160211183202”
	Retimer	Retimer 日志文件夹，以 Retimer 对象名命名。如：“Cdr5902H_Obj_1-10”。	Retimer 日志信息，包括： ● PCIe：PCIe 命令回显信息 ● RAMLog：SRAM 导出的日志 ● SerDes：SerDes 相关信息
OSDump	-	systemcom.tar	SOL 串口信息
		img*.jpeg	业务侧最后一屏图像
		*.rep	业务侧屏幕自动录像文件
		video_caterror_rep_is_deleted.info	删除过大的 caterror 录像的提示
Devic	i2c_info	*_info	I2C 设备的寄存器/存储区信息

目录	子目录	文件名	文件内容说明
eDump			
Register	-	cpld_reg_info	CPLD 寄存器信息
OptPme	pram 说明 本文件夹的文件来源于/opt/pme/pram目录，如果出现没有记录在此的文件，为程序运行过程中产生的中间文件，不存在信息安全问题。	filelist	“/opt/pme/pram”目录下文件列表
		BIOS_FileName	SMBIOS 信息
		BIOS_OptionFileName	BIOS 配置信息
		BMC_dhclient.conf	DHCP 配置文件
		BMC_dhclient.conf.md5	完整性校验码
		BMC_dhclient.conf.sha256	完整性校验码
		BMC_dhclient6.conf	DHCP 配置文件
		BMC_dhclient6.conf.md5	完整性校验码
		BMC_dhclient6.conf.sha256	完整性校验码
		BMC_dhclient6_ip.conf	DHCP 配置文件
		BMC_dhclient6_ip.conf.md5	完整性校验码
		BMC_dhclient6_ip.conf.sha256	完整性校验码
		BMC_dhclient_ip.conf	DHCP 配置文件
		BMC_dhclient_ip.conf.md5	完整性校验码
		BMC_dhclient_ip.conf.sha256	完整性校验码
		BMC_HOSTNAME	iBMC 主机名
		BMC_HOSTNAME.md5	完整性校验码
		BMC_HOSTNAME.sha256	完整性校验码
		CpuMem_cpu_utilise	服务器 CPU 利用率
		CpuMem_mem_utilis	服务器内存利用率

目录	子目录	文件名	文件内容说明
		e	
		cpu_utilise_webview.dat	CPU 利用率曲线数据
		env_web_view.dat	环境温度曲线数据
		fsync_reg.ini	文件同步配置文件
		lost+found	文件夹
		md_so_maintenance_log md_so_maintenance_log.tar.gz	维护日志
		md_so_operate_log md_so_operate_log.tar.gz md_so_mass_operate_log md_so_mass_operate_log.tar.gz	操作日志
		md_so_operate_log.md5	完整性校验码
		md_so_operate_log.sha256	完整性校验码
		md_so_strategy_log md_so_strategy_log.tar.gz	策略日志
		md_so_strategy_log.md5	完整性校验码
		md_so_strategy_log.sha256	完整性校验码
		memory_webview.dat	管理对象运行信息
		per_config.ini	iBMC 配置持久化文件
		per_config.ini.md5	完整性校验码
		per_config.ini.sha256	完整性校验码
		per_config_permanent.ini	iBMC 配置持久化文件
		per_config_permanent.ini.md5	完整性校验码
		per_config_permanen	完整性校验码

目录	子目录	文件名	文件内容说明
		t.ini.sha256	
		per_config_reset.ini	iBMC 配置持久化文件
		per_config_reset.ini.bak	iBMC 配置持久化文件
		per_config_reset.ini.bak.md5	完整性校验码
		per_config_reset.ini.bak.sha256	完整性校验码
		per_config_reset.ini.md5	完整性校验码
		per_config_reset.ini.sha256	完整性校验码
		per_def_config.ini	iBMC 配置持久化文件
		per_def_config.ini.md5	完整性校验码
		per_def_config.ini.sha256	完整性校验码
		per_def_config_permanent.ini	iBMC 配置持久化文件
		per_def_config_permanent.ini.md5	完整性校验码
		per_def_config_permanent.ini.sha256	完整性校验码
		per_def_config_reset.ini	iBMC 配置持久化文件
		per_def_config_reset.ini.bak	iBMC 配置持久化文件
		per_def_config_reset.ini.bak.md5	完整性校验码
		per_def_config_reset.ini.bak.sha256	完整性校验码
		per_def_config_reset.ini.md5	完整性校验码
		per_def_config_reset.ini.sha256	完整性校验码
		per_power_off.ini	iBMC 配置持久化文件
		per_power_off.ini.md5	完整性校验码

目录	子目录	文件名	文件内容说明
		per_power_off.ini.sha256	完整性校验码
		per_reset.ini	iBMC 配置持久化文件
		per_reset.ini.bak	iBMC 配置持久化文件
		per_reset.ini.bak.md5	完整性校验码
		per_reset.ini.bak.sha256	完整性校验码
		per_reset.ini.md5	完整性校验码
		per_reset.ini.sha256	完整性校验码
		pflash_lock	flash 文件锁
		PowerMgnt_record	管理对象运行信息
		powerview.txt	功率统计文件
		proc_queue	进程队列 id 文件夹
		ps_web_view.dat	管理对象运行信息
		sel.db	SEL 数据库
		sel_db_sync	SEL 数据库同步锁
		semid	进程信号量 id 文件夹
		sensor_alarm_sel.bin	SEL 原始记录文件
		sensor_alarm_sel.bin.md5	完整性校验码
		sensor_alarm_sel.bin.sha256	完整性校验码
		sensor_alarm_sel.bin.tar.gz	SEL 历史记录打包文件
		Snmp_snmpd.conf	Snmp 配置文件
		Snmp_snmpd.conf.md5	完整性校验码
		Snmp_snmpd.conf.sha256	完整性校验码
		Snmp_http_configure	HTTP 配置文件
		Snmp_http_configure.md5	完整性校验码
		Snmp_http_configure.	完整性校验码

目录	子目录	文件名	文件内容说明
		sha256	
		Snmp_https_configure	HTTPS 配置文件
		Snmp_https_configure.md5	完整性校验码
		Snmp_https_configure.sha256	完整性校验码
		Snmp_https_tsl	HTTPS TLS 配置文件
		Snmp_https_tsl.md5	完整性校验码
		Snmp_https_tsl.sha256	完整性校验码
		up_cfg	升级配置文件夹
		User_login	login PAM 登录规则
		User_login.md5	完整性校验码
		User_login.sha256	完整性校验码
		User_sshd	SSH PAM 登录规则
		User_sshd.md5	完整性校验码
		User_sshd.sha256	完整性校验码
		User_sshd_config	SSH 配置文件
		User_sshd_config.md5	完整性校验码
		User_sshd_config.sha256	完整性校验码
		User_vsftp	FTP PAM 登录规则
		User_vsftp.md5	完整性校验码
		User_vsftp.sha256	完整性校验码
		eo.db	SEL 数据库
	save 说明 本文件夹的文件来源于/opt/pme/save目录，*.md5文件为完整性校验码，	filelist	“/opt/pme/pram”目录下文件列表
		BIOS_FileName	SMBIOS 信息
		BMC_dhclient.conf.bak	DHCP 配置备份文件
		BMC_dhclient.conf.bak.md5	完整性校验码

目录	子目录	文件名	文件内容说明
	.sha256 文件为完整性校验码，.bak 文件为备份文件，*.tar.gz 为打包保存文件，per_*.ini 为配置持久化文件，*sel.*为系统事件记录文件（如果出现没有记录在此的文件，为程序运行过程中产生的中间文件，不存在信息安全问题。）	BMC_dhclient.conf.bak.sha256	完整性校验码
		BMC_dhclient.conf.md5	完整性校验码
		BMC_dhclient.conf.sha256	完整性校验码
		BMC_dhclient6.conf.bak	DHCP 配置备份文件
		BMC_dhclient6.conf.bak.md5	完整性校验码
		BMC_dhclient6.conf.bak.sha256	完整性校验码
		BMC_dhclient6.conf.md5	完整性校验码
		BMC_dhclient6.conf.sha256	完整性校验码
		BMC_dhclient6_ip.conf.bak	DHCP 配置备份文件
		BMC_dhclient6_ip.conf.bak.md5	完整性校验码
		BMC_dhclient6_ip.conf.bak.sha256	完整性校验码
		BMC_dhclient6_ip.conf.md5	完整性校验码
		BMC_dhclient6_ip.conf.sha256	完整性校验码
		BMC_dhclient_ip.conf.bak	DHCP 配置备份文件
		BMC_dhclient_ip.conf.bak.md5	完整性校验码
		BMC_dhclient_ip.conf.bak.sha256	完整性校验码
		BMC_dhclient_ip.conf.md5	完整性校验码
		BMC_dhclient_ip.conf.sha256	完整性校验码
		BMC_HOSTNAME.bak	主机名配置备份文件
		BMC_HOSTNAME.	完整性校验码

目录	子目录	文件名	文件内容说明
		bak.md5	
		BMC_HOSTNAME.bak.sha256	完整性校验码
		BMC_HOSTNAME.md5	完整性校验码
		BMC_HOSTNAME.sha256	完整性校验码
		CpuMem_cpu_utilise	管理对象运行信息
		CpuMem_mem_utilise	管理对象运行信息
		md_so_operate_log.bak	操作日志
		md_so_operate_log.bak.md5	完整性校验码
		md_so_operate_log.md5	完整性校验码
		md_so_operate_log.bak.sha256	完整性校验码
		md_so_strategy_log.bak	策略日志
		md_so_operate_log.sha256	完整性校验码
		md_so_strategy_log.bak.md5	完整性校验码
		md_so_strategy_log.bak.sha256	完整性校验码
		md_so_strategy_log.md5	完整性校验码
		md_so_strategy_log.sha256	完整性校验码
		per_config.ini	iBMC 配置持久化文件
		per_config.ini.bak	iBMC 配置持久化文件
		per_config.ini.bak.md5	完整性校验码
		per_config.ini.bak.sha256	完整性校验码
		per_config.ini.md5	完整性校验码

目录	子目录	文件名	文件内容说明
		per_config.ini.sha256	完整性校验码
		per_def_config.ini	iBMC 配置持久化文件
		per_def_config.ini.bak	iBMC 配置持久化文件
		per_def_config.ini.bak.md5	完整性校验码
		per_def_config.ini.bak.sha256	完整性校验码
		per_def_config.ini.md5	完整性校验码
		per_def_config.ini.sha256	完整性校验码
		per_power_off.ini	iBMC 配置持久化文件
		per_power_off.ini.bak	iBMC 配置持久化文件
		per_power_off.ini.bak.md5	完整性校验码
		per_power_off.ini.bak.sha256	完整性校验码
		per_power_off.ini.md5	完整性校验码
		per_power_off.ini.sha256	完整性校验码
		PowerMgnt_record	管理对象运行信息
		sensor_alarm_sel.bin	SEL 原始记录文件
		sensor_alarm_sel.bin.bak	SEL 原始记录文件
		sensor_alarm_sel.bin.bak.md5	完整性校验码
		sensor_alarm_sel.bin.bak.sha256	完整性校验码
		sensor_alarm_sel.bin.md5	完整性校验码
		sensor_alarm_sel.bin.sha256	完整性校验码
		sensor_alarm_sel.bin.tar.gz	SEL 历史记录打包文件

目录	子目录	文件名	文件内容说明
		Snmp_http_configure.bak	HTTP 配置备份文件
		Snmp_http_configure.bak.md5	完整性校验码
		Snmp_http_configure.bak.sha256	完整性校验码
		Snmp_http_configure.md5	完整性校验码
		Snmp_http_configure.sha256	完整性校验码
		Snmp_https_configure.bak	HTTPS 配置备份文件
		Snmp_https_configure.bak.md5	完整性校验码
		Snmp_https_configure.bak.sha256	完整性校验码
		Snmp_https_configure.md5	完整性校验码
		Snmp_https_configure.sha256	完整性校验码
		Snmp_https_tsl.bak	HTTPS TLS 配置备份文件
		Snmp_https_tsl.bak.md5	完整性校验码
		Snmp_https_tsl.bak.sha256	完整性校验码
		Snmp_https_tsl.md5	完整性校验码
		Snmp_https_tsl.sha256	完整性校验码
		Snmp_snmpd.conf.bak	Snmp 配置备份文件
		Snmp_snmpd.conf.bak.md5	完整性校验码
		Snmp_snmpd.conf.bak.sha256	完整性校验码
		Snmp_snmpd.conf.md5	完整性校验码
		Snmp_snmpd.conf.sha256	完整性校验码

目录	子目录	文件名	文件内容说明
		User_login.bak	login PAM 登录规则
		User_login.bak.md5	完整性校验码
		User_login.bak.sha256	完整性校验码
		User_login.md5	完整性校验码
		User_login.sha256	完整性校验码
		User_sshd.bak	SSH PAM 登录规则
		User_sshd.bak.md5	完整性校验码
		User_sshd.bak.sha256	完整性校验码
		User_sshd.md5	完整性校验码
		User_sshd.sha256	完整性校验码
		User_sshd_config.bak	SSH 配置文件
		User_sshd_config.bak.md5	完整性校验码
		User_sshd_config.bak.sha256	完整性校验码
		User_sshd_config.md5	完整性校验码
		User_sshd_config.sha256	完整性校验码
		User_vsftp.bak	FTP PAM 登录规则
		User_vsftp.bak.md5	完整性校验码
		User_vsftp.bak.sha256	完整性校验码
		User_vsftp.md5	完整性校验码
		User_vsftp.sha256	完整性校验码
		eo.db	SEL 数据库
		eo.db.sha256	完整性校验码
		eo.db_backup	SEL 数据库
		eo.db.sha256_backup	完整性校验码

4 命令行介绍

关于本章

介绍如何登录 iBMC 命令行，以及 iBMC 支持的命令。

4.1 命令行说明

介绍命令行的格式约定和功能。

4.1.1 格式说明

iBMC 管理软件常用命令有以下命令：

- 查询命令 **ipmcget**
  查询命令 **ipmcget** 的格式如下：
  ipmcget [**-t** *target*] **-d** *dataitem* [**-v** *value*]
- 设置命令 **ipmcset**
  设置命令 **ipmcset** 的格式如下：
  ipmcset [**-t** *target*] **-d** *dataitem* [**-v** *value*]

查询命令 **ipmcget** 和设置命令 **ipmcset** 的参数说明如下：

- [ ]：表明该内容不是每条命令都包含的部分。
- **-t** *target*：查询、设置操作设备上的对象。
- **-d** *dataitem*：查询、设置操作设备或操作设备上部件的特定属性。
- **-v** *value*：查询、设置操作设备上部件的参数值。

对命令行格式的约定请参见表 4-1。

表4-1 命令行格式的约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。

4.1.2 帮助

iBMC 命令行具有帮助功能，使用过程中可以在不完全输入的情况下直接按“Enter”，命令行将会自动提示命令的参数以及格式，帮助您完成命令操作。

例如：

查询命令：

```
iBMC:/->ipmcget
Usage: ipmcget [-t target] -d dataitem [-v value]
```

```
   -t <target>
      fru0                        Get the information of the fru0
      sensor                      Print detailed sensor information
      smbios                      Get the information of smbios
      trap                        Get SNMP trap status
      service                     Get service information
      maintenance                  Get maintenance information
      syslog                      Get syslog status
      user                        Get the information of user
      securitybanner               Get login security banner information
      vnc                         Get VNC information
      storage                     Get storage device information
      config                      Get configuration information
      vmm                         Get Virtual Media information
      certificate                  Get SSL certificate information
      sol                         Get SOL information
      securityenhance              Get security enhance information

   -d <dataitem>
      faninfo                     Get fan mode and the percentage of the fan speed
      port80                      Get the diagnose code of port 80
      diaginfo                    Get diagnostic info of management subsystem
      systemcom                   Get system com data
      blackbox                    Get black box data
      bootdevice                  Get boot device
      shutdowntimeout              Get graceful shutdown timeout state and value
      powerstate                  Get power state
      health                      Get health status
      healthevents                 Get health events
      sel                         Print System Event Log (SEL)
      operatelog                   Print operation log
      version                     Get iBMC version
      serialnumber                 Get system serial number
      userlist                    List all user info
      fruinfo                     Get fru information
      time                        Get system time
      macaddr                     Get mac address
      serialdir                   Get currently connected serial direction
      rollbackstatus               Get rollback status
      passwordcomplexity           Get password complexity check enable status
      ledinfo                     Get led information
      ipinfo                      Get ip information
      ethport                     Get usable eth port
      psuinfo                     Get PSU component information
      autodiscovery                Get autodiscovery configuration
      poweronpermit                Get poweronpermit configuration
      raid                        Deprecated. Please use 'ipmcget -t storage ...' to
get more information
      ldinfo                      Deprecated. Please use 'ipmcget -t storage ...' to
get more information
      pdinfo                      Deprecated. Please use 'ipmcget -t storage ...' to
get more information
      minimumpasswordage           Get minimum password age configuration
      ntpinfo                     Get NTP information
```

设置命令：

```
iBMC:/->ipmcset
Usage: ipmcset [-t target] -d dataitem [-v value]
   -t <target>
      fru0                      Operate with fru0
      trap                      Operate SNMP trap
      service                    Operate with service
      user                      Operate with user
      maintenance                Operate with maintenance
      sensor                    Operate with sensor
      securitybanner             Operate login security banner information
      syslog                    Operate syslog
      ntp                       Operate ntp
      vnc                       Operate vnc
      storage                    Configure storage device
      config                    Operate configuration
      vmm                       Operate virtual media
      certificate                Operate certificate
      sol                       Operate SOL
      securityenhance             Operate security enhance
      precisealarm               Operate with precise alarm

   -d <dataitem>
      fanmode                    Set fan mode,you can choose manual or auto
      fanlevel                   Set fan speed percent
      reset                     Reboot BMC system
      identify                   Operate identify led
      upgrade                   Upgrade component
      clearcmos                  Clear CMOS
      bootdevice                 Set boot device
      shutdowntimeout             Set graceful shutdown timeout state and value
      frucontrol                 Fru control
      powerstate                 Set power state
      sel                       Clear SEL
      adduser                    Add user
      password                   Modify user password
      deluser                    Delete user
      privilege                  Set user privilege
      serialdir                  Set serial direction
      printscreen                Print current screen to BMC
      rollback                   Perform a manual rollback
      timezone                   Set time zone
      passwordcomplexity           Set password complexity check enable state
      ipaddr                    Set ip address
      backupipaddr               Set backup ip address
      ipmode                    Set ip mode
      gateway                    Set gateway
      ipaddr6                    Set ipv6 address
      ipmode6                    Set ipv6 mode
      gateway6                   Set ipv6 gateway
      netmode                    Set net mode
      activeport                 Set EthGroup active port
      vlan                      Set sideband vlan
      restore                    Restore factory setting
      notimeout                  Set no timeout state
      emergencyuser               Set emergency user
```

```
      autodiscovery              Set autodiscovery configuration
      poweronpermit              Set poweronpermit configuration
      minimumpasswordage          Set minimum password age configuration
      crl                       Upload CRL file
      psuworkmode                Set PSU work mode
      clearlog                  Clear Log
      fpgagoldenfwrestore          FPGA golden firmware restore
```

在输入错误参数的情况下，帮助信息会提示可选的正确参数。

例如：

```
iBMC:/->ipmcset -d inff
Input parameter[-d] error
-d <dataitem>
      fanmode                    Set fan mode,you can choose manual or auto
      fanlevel                   Set fan speed percent
      reset                     Reboot iBMC system
      identify                   Operate identify led
      upgrade                   Upgrade component
      clearcmos                  Clear CMOS
      bootdevice                 Set boot device
      shutdowntimeout             Set graceful shutdown timeout state and value
      frucontrol                 Fru control
      powerstate                 Set power state
      sel                       Clear SEL
      adduser                    Add user
      password                   Modify user password
      deluser                    Delete user
      privilege                  Set user privilege
      serialdir                  Set serial direction
      printscreen                Print current screen to iBMC
      rollback                   Perform a manual rollback
      timezone                   Set time zone
      passwordcomplexity           Set password complexity check enable state
      ipaddr                    Set ip address
      backupipaddr               Set backup ip address
      ipmode                    Set ip mode
      gateway                   Set gateway
      ipaddr6                   Set ipv6 address
      ipmode6                   Set ipv6 mode
      gateway6                  Set ipv6 gateway
      netmode                   Set net mode
      activeport                 Set EthGroup active port
      vlan                      Set sideband vlan
      restore                    Restore factory setting
      notimeout                  Set no timeout state
      emergencyuser              Set emergency user
      autodiscovery              Set autodiscovery configuration
      poweronpermit              Set poweronpermit configuration
      workkey                   Update system workkey
      minimumpasswordage          Set minimum password age configuration
      locate                    Deprecated. Please use 'ipmcset -t storage ...'.
      crl                       Upload CRL file
      psuworkmode                Set PSU work mode
```

```
clearlog                Clear Log
fpgagoldenfwrestore       FPGA golden firmware restore
```

4.2 登录 CLI

介绍如何登录命令行。

除默认用户和用户自行添加的用户外，iBMC 还有如下系统默认用户用于某些服务：

- “root”：系统运行 app 进程时使用。
- “sshd”：系统运行 ssh 服务时使用。
- “apache”：系统运行 httpd 服务时使用。
- “snmpd_user”：系统运行 snmp 服务时使用。
- “ipmi_user”：系统运行 ipmi 服务时使用。
- “kvm_user”：系统运行远程控制台服务时使用。
- “discovery_user”：系统运行 SSDP 服务时使用。
- “comm_user”：系统运行 mctp 进程、rimm 进程以及 DDNS 服务时使用。
- “redfish_user”：系统运行 redfish 进程时使用。

说明

- 系统默认用户不能用于登录 iBMC，也不会对系统造成影响。
- 系统默认用户为系统管理使用，不对外呈现。
- 通过按↑键可以显示输入的历史命令，系统会将用户名、口令、密钥等敏感信息脱敏处理，显示为*。

4.2.1 确认管理网口 IP 地址

方法介绍

管理网口的 IP 地址确认方法有以下几种：

- 管理网口默认 IP 地址。
- 通过 BIOS 系统查询和设置管理网口 IP 地址。
- 通过串口登录管理软件命令行查询和设置管理网口 IP 地址。

默认 IP 地址

表4-2 默认 IP

槽位	IP
-	192.168.2.100

通过 BIOS 查询和设置

服务器支持通过 BIOS 查询和设置 iBMC 的 IP 地址，具体请参见相应的 BIOS 参数参考。

通过串口登录

说明

通过串口登录 iBMC CLI，必须保证机箱的系统串口已经切换为 iBMC 串口。可以通过 SSH 登录 iBMC CLI，执行 4.3.12 查询和设置串口方向（serialdir）切换串口。

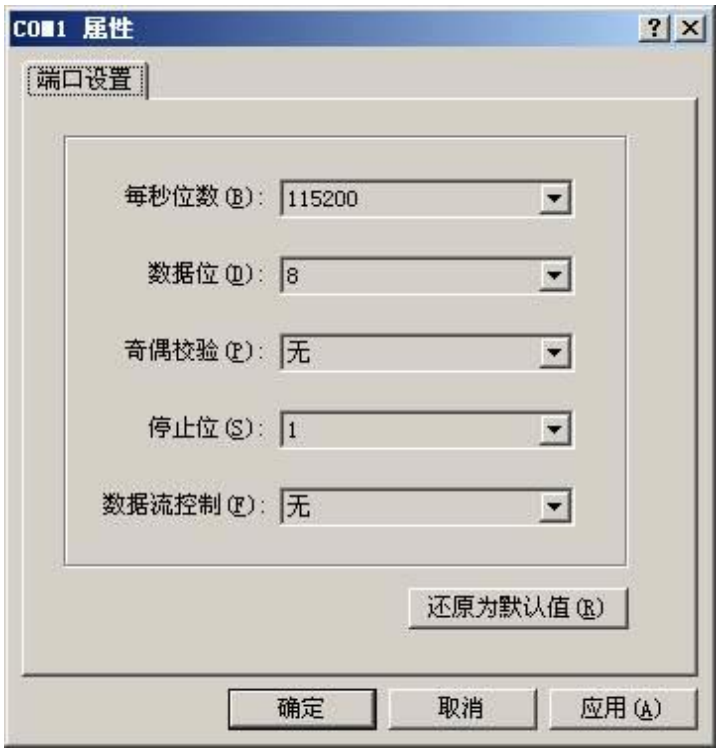
步骤 1 连接串口线。

步骤 2 通过超级终端登录串口命令行，需要设置的参数有：

- 波特率：115200
- 数据位：8
- 奇偶校验：无
- 停止位：1
- 数据流控制：无

参数设置如图 4-1 所示。

图4-1 超级终端属性设置



步骤 3 连接成功后输入用户名和密码。

说明

iBMC 提供 1 个默认用户为 **Administrator**，默认密码为 **Admin@9000**。

步骤 4 执行 **ipmcget -d ipinfo** 命令可获取管理网口 IP 地址信息。

----结束

4.2.2 登录 iBMC 命令行

您可以通过以下方式登录 iBMC 命令行：

- SSH

  通过 SSH 方式登录命令行，最多允许 5 个用户同时登录。

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。

- 本地串口

说明

- iBMC 提供 1 个默认用户为 **Administrator**，默认密码为 **Admin@9000**。
- 连续 5 次输入错误的密码后，系统将对此用户进行锁定。等待 5 分钟后，方可重新登录，亦可通过管理员在命令行下解锁。
- 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。
- 默认情况下，命令行超时时间为 15 分钟。

前提条件

- 通过网口登录管理软件命令行，必须保证配置终端已经通过网线和服务器管理网口相连，并且配置终端的网口和管理网口 IP 地址在同一网段。
- 通过串口登录管理软件命令行，必须事先通过串口线缆连接配置终端串口和服务器串口。

通过 SSH 登录

1. 在客户端下载符合 SSH 协议的通讯工具。
2. 将客户端连接（直连或通过网络连接）到服务器管理网口。
3. 配置客户端地址，使其可与服务器 iBMC 管理网口互通。
4. 在客户端打开 SSH 工具并配置相关参数（如 IP 地址）。
5. 连接到 iBMC 后，输入用户名和密码。

说明

- 本地用户和 LDAP 用户均可通过 SSH 方式登录 iBMC CLI。
- 使用 LDAP 用户登录 iBMC CLI 时，需要保证 iBMC 与 LDAP 服务器的连通性。
- LDAP 用户登录时，不需要输入域服务器信息，由系统自动匹配。

通过串口登录

说明

通过串口登录 iBMC CLI，必须保证机箱的系统串口已经切换为 iBMC 串口。可以通过 SSH 登录 iBMC CLI，执行 4.3.12 查询和设置串口方向（serialdir）切换串口。

步骤 1 连接串口线。

步骤 2 通过超级终端登录串口命令行，需要设置的参数有：

- 波特率：115200
- 数据位：8
- 奇偶校验：无
- 停止位：1
- 数据流控制：无

参数设置如图 4-2 所示。

图4-2 超级终端属性设置

步骤 3 连接成功后输入用户名和密码。

说明

iBMC 提供 1 个默认用户为 **Administrator**，默认密码为 **Admin@9000**。

步骤 4 执行 **ipmcget -d ipinfo** 命令可获取管理网口 IP 地址信息。

----结束

4.3 iBMC 命令

4.3.1 查询 iBMC 管理网口的 IP 信息（ipinfo）

命令功能

ipinfo 命令用来查询 iBMC 管理网口的 IP 信息。

命令格式

ipmcget -d ipinfo

参数说明

无

使用指南

无

使用实例

查询 iBMC 管理网口的 IP 信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID          :  1
Net Mode             :  Manual
Net Type             :  Dedicated
IPv4 Information     :
IP Mode              :  static
IP Address           :  90.90.184.128
Subnet Mask          :  255.255.252.0
Default Gateway      :  90.90.184.1
Backup IP Address    :  192.168.0.25 (Deactivated)
Backup Subnet Mask   :  255.255.255.0 (Deactivated)
MAC Address          : 20:20:06:27:10:46
IPv6 Information     :
IPv6 Mode            :  static
IPv6 Address 1       :  fc00::6516/64
Default Gateway IPv6  :  fc00::1
Link-Local Address   :  fe80::2220:6ff:fe27:1046/64
IPv6 Address 2       :  fc00:225::1a3d:5eff:febe:bc35/64
VLAN Information     :
VLAN State           :  disabled
```

说明

Backup IP Address 和 **Backup Subnet Mask** 字段中，状态为 **Activated** 表示 IP 已激活，状态为 **Deactivated** 表示该 IP 未激活。

4.3.2 设置 iBMC 网口的 IPv4 信息（ipaddr）

命令功能

ipaddr 命令用于设置 iBMC 网口的 IPv4 地址、掩码、网关。

命令格式

ipmcset -d ipaddr -v <*ipaddr*> <*mask*> [*gateway*]

参数说明

参数	参数说明	取值
ipaddr	表示要设置的 iBMC 网口的 IPv4 地址。	数据类型为 IPv4，表示形式为 xxx.xxx.xxx.xxx。
mask	表示要设置的 iBMC 网口的子网掩码。	数据类型为 IPv4，表示形式为 xxx.xxx.xxx.xxx。
gateway	表示要设置的 iBMC 网口的网关地址。	数据类型为 IPv4，表示形式为 xxx.xxx.xxx.xxx。

使用指南

重新设置 IP 地址后，新的设置立刻生效，需按照新设置重新登录。

请勿将 *ipaddr* 设置为 10.0.0.0~10.0.0.3（内部通信预留地址）。

使用实例

设置 iBMC 管理网口的 IP 地址为 192.168.0.25，子网掩码为 255.255.255.0，网关地址为 192.168.0.25。

```
iBMC:/->ipmcset -d ipaddr -v 192.168.0.25 255.255.255.0 192.168.0.25
Set IP address successfully.
Set MASK address successfully.
Set GATEWAY successfully.
```

查询修改后的 iBMC 管理网口的 IP 信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         : 255.255.255.0
Default Gateway      : 192.168.0.25
Backup IP Address    :  192.168.2.100  (Deactivated)
```

```
Backup Subnet Mask    : 255.255.255.0 (Deactivated)
MAC Address          :  20:20:06:27:10:46
IPv6 Information      :
IPv6 Mode            :  static
IPv6 Address 1       :  fc00::6516/64
Default Gateway IPv6  : fc00::1
Link-Local Address    :  fe80::2220:6ff:fe27:1046/64
IPv6 Address 2       :  fc00:225::1a3d:5eff:febe:bc35/64
VLAN Information      :
VLAN State           :  disabled
```

4.3.3 设置 iBMC 管理网口的备份 IPv4 信息（backupipaddr）

命令功能

backupipaddr 命令用于设置 iBMC 管理网口的备份 IPv4 地址。

在 DHCP 功能开启时：

- 若 iBMC 管理网口未分配到 IP 地址，此时您可以使用备份 IP 地址登录 iBMC 系统进行配置。
- 若 iBMC 管理网口已分配到 IP 地址，但用户无法确认分配的具体地址时，您可以使用备份 IP 地址登录 iBMC 系统进行查询。（前提条件为通过 DHCP 服务器分配的地址与当前备份地址分布在不同网段，否则无法登录。）

在 DHCP 功能未开启时：备份 IP 地址不生效，不可使用。

命令格式

ipmcset -d backupipaddr -v <*ipaddr*> <*mask*>

参数说明

参数	参数说明	取值
ipaddr	表示要设置的 iBMC 网口的备份 IPv4 地址。	数据类型为 IPv4，表示形式为 xxx.xxx.xxx.xxx。
mask	表示要设置的备份 IPv4 地址的子网掩码。	数据类型为 IPv4，表示形式为 xxx.xxx.xxx.xxx。

使用指南

设置备份 IP 地址后，可以通过 **ipmcget -d ipinfo** 查看“Backup IP Address”字段的状态判断备份 IP 地址是否生效。

- Activated：表示该备份 IP 地址已生效，可以使用。
- Deactivated：表示该备份 IP 地址未生效，不可使用。

请勿将备份 IP 地址设置为 10.0.0.0~10.0.0.3（内部通信预留地址）。

备份 IP 地址不支持跨网段跳转连接，因此，在使用备份 IP 地址登录 iBMC 时，客户端的 IP 地址必须与备份 IP 在同一网段，双方设备必须在同一局域网内。

使用实例

设置 iBMC 管理网口的备份 IP 地址为 192.168.0.25，子网掩码为 255.255.255.0。

```
iBMC:/->ipmcset -d backupipaddr -v 192.168.0.25 255.255.255.0
Set backup IP address successfully.
Set backup MASK address successfully.
```

查询 iBMC 管理网口的 IP 信息。

```
iBMC:/->ipmcget -d ipinfo
ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.255.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.25 (Deactivated)
Backup Subnet Mask   :  255.255.255.0 (Deactivated)
MAC Address         :
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address 1       :  fc00::6516/64
Default Gateway IPv6  :  fc00::1
Link-Local Address   :  fe80::2220:6ff:fe27:1046/64
VLAN Information     :
VLAN State          :  disabled
```

4.3.4 设置 iBMC 网口的 IPv4 模式（ipmode）

命令功能

ipmode 命令用于设置 iBMC 网口的 IPv4 模式。

命令格式

ipmcset -d ipmode -v <dhcp | static>

参数说明

参数	参数说明	取值
dhcp	表示地址模式为 dhcp	-
static	表示地址模式为 static	-

使用指南

重新设置地址模式后，新的设置立刻生效，需按照新设置重新登录。

使用实例

设置 iBMC 管理网口为 dhcp 模式。

```
iBMC:/->ipmcset -d ipmode -v dhcp
Set dhcp mode successfully.
```

查询修改后的 iBMC 管理网口 IP 信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  dhcp
IP Address          :  192.168.0.12
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.25 (Activated)
Backup Subnet Mask   :  255.255.255.0 (Activated)
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address         :
Default Gateway IPv6  :
Link-Local Address   :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             : 1
```

说明

由 **ipinfo** 命令可以查询到 iBMC 管理网口从 DHCP 服务器获得新的 IP 地址为 192.168.0.12。

4.3.5 设置 iBMC 网口的 IPv4 网关（gateway）

命令功能

gateway 命令用来设置 iBMC 网口的 IPv4 网关地址。

命令格式

ipmcset -d gateway -v <*gateway*>

参数说明

参数	参数说明	取值
gateway	表示 iBMC 网口的 IPv4 网关地址。	数据类型为 IPv4，表示形式为 xxx.xxx.xxx.xxx。

使用指南

重新设置网关地址后，新的设置立刻生效。

使用实例

设置 iBMC 管理网口的网关为 192.168.0.1。

```
iBMC:/->ipmcset -d gateway -v 192.168.0.1
Set GATEWAY successfully.
```

查询设置后的网关地址信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.255.0
Default Gateway      :  192.168.0.1
Backup IP Address    :  192.168.0.144 (Activated)
Backup Subnet Mask   :  255.255.255.0 (Activated)
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address         :
Default Gateway IPv6  :
Link-Local Address   :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             : 1
```

4.3.6 设置 iBMC 网口的 IPv6 信息（ipaddr6）

命令功能

ipaddr6 命令用于设置 iBMC 网口的 IPv6 地址、前缀长度和网关地址。

命令格式

ipmcset -d ipaddr6 -v <*ipaddr6*/*prefixlen*> [*gateway6*]

参数说明

参数	参数说明	取值
ipaddr6	表示要设置的 iBMC 网口的 IPv6 地址。	数据类型为 IPv6，表示形式为 *xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*。当多个 *xxxx* 连续为 0 时，表现形式可缩写为

参数	参数说明	取值
		xxxx::xxxx。例如：*fc00::0000:000:0000:0000:0000:0000:0001* 可缩写为 *fc00::0001*。 在一个 IPv6 地址中，只能使用一个缩写。
prefixlen	表示要设置的 iBMC 网口的子网前缀长度。	0～128。
gateway6	表示要设置的 iBMC 网口的 IPv6 网关地址。	数据类型为 IPv6，表示形式为 *xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*。当多个 *xxxx* 连续为 0 时，表现形式可缩写为 *xxxx::xxxx*。例如：*fc00::0000:000:0000:0000:0000:0000:0001* 可缩写为 *fc00::0001*。 在一个 IPv6 地址中，只能使用一个缩写。

使用指南

- 通过 ipmcget 获取 IPV6 的 Link-Local Address 信息，客户可通过这个地址访问 iBMC。
- 重新设置 IP 地址后，新的设置立刻生效，需按照新设置重新登录。

使用实例

设置 iBMC 管理网口的 IPv6 地址为 fc00::6516，子网前缀为 64，网关地址为 fc00::1。

```
iBMC:/->ipmcset -d ipaddr6 -v fc00::6516/64 fc00::1
Set IPV6 address successfully.
Set IPV6 prefix successfully.
Set IPv6 GATEWAY6 successfully.
```

查询修改后的 iBMC 管理网口的 IP 信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.255.0
Default Gateway      : 192.168.0.25
Backup IP Address    :  192.168.0.25 (Deactivated)
Backup Subnet Mask   :  255.255.255.0 (Deactivated)
MAC Address         :  20:20:06:27:10:46
IPv6 Information     :
IPv6 Mode           :  static
```

```
IPv6 Address 1        :  fc00::6516/64
Default Gateway IPv6  :  fc00::1
Link-Local Address    :  fe80::2220:6ff:fe27:1046/64
VLAN Information      :
VLAN State           :  disabled
```

4.3.7 设置 iBMC 网口的 IPv6 模式（ipmode6）

命令功能

ipmode6 命令用于设置 iBMC 网口的 IPv6 模式。

命令格式

ipmcset -d ipmode6 -v <dhcp | static>

参数说明

参数	参数说明	取值
dhcp	表示地址模式为 dhcp	-
static	表示地址模式为 static	-

使用指南

重新设置地址模式后，新的设置立刻生效，需按照新设置重新登录。

使用实例

设置 iBMC 管理网口为 dhcp 模式。

```
iBMC:/->ipmcset -d ipmode6 -v dhcp
Set dhcp mode successfully.
```

查询修改后的 iBMC 管理网口 IP 信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID          :  1
Net Mode             :  Manual
Net Type             :  Dedicated
IPv4 Information     :
IP Mode              :  dhcp
IP Address           :  192.168.0.12
Subnet Mask          :  255.255.0.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.144 (Activated)
Backup Subnet Mask   :  255.255.255.0 (Activated)
MAC Address          :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode            :  dhcp
IPv6 Address         :
```

```
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information      :
VLAN State           :  disabled
VLAN ID             : 1
```

4.3.8 设置 iBMC 网口的 IPv6 网关（gateway6）

命令功能

gateway6 命令用来设置 iBMC 网口的 IPv6 网关地址。

命令格式

ipmcset -d gateway6 -v <*gateway6*>

参数说明

参数	参数说明	取值
gateway6	表示 iBMC 网口的 IPv6 网关地址。	数据类型为 IPv6，长度为 128bit，包含 8 个 16bit 的字段。表示形式为 *xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*。 当多个 *xxxx* 连续为 0 时，表现形式可缩写为 *xxxx::xxxx*。在一个 IPv6 地址中，只能使用一个缩写。 例如，“fc00:0db8:3c4d:0015:0000:0000:1a2f:1a2b”可以缩写为“fc00:db8:3c4d:15::1a2f:1a2b”。

使用指南

重新设置网关地址后，新的设置立刻生效。

使用实例

设置 iBMC 管理网口的 IPv6 网关为 fc00::1。

```
iBMC:/->ipmcset -d gateway6 -v fc00::1
Set GATEWAY6 successfully.
```

查询设置后的网关地址信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
```

```
IP Address          : 192.168.0.25
Subnet Mask         : 255.255.255.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.25 (Deactivated)
Backup Subnet Mask   :  255.255.255.0 (Deactivated)
MAC Address         :  20:20:06:27:10:46
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address         :  fc00::6516/64
Default Gateway IPv6  :  fc00::1
Link-Local Address   : fe80::2220:6ff:fe27:1046/64
VLAN Information     :
VLAN State          :  disabled
```

4.3.9 设置网口模式（netmode）

命令功能

netmode 命令用于设置网口模式。

命令格式

ipmcset -d netmode -v <*option*>

参数说明

参数	参数说明	取值
option	网口模式	• 1：表示 Manual 模式 • 2：表示 Adaptive 模式 默认取值：“1”

使用指南

- Manual 模式：选择此模式时，用户可以指定使用哪个网络设备端口作为管理网口。（出厂默认配置）
- Adaptive 模式：选择此模式时，需要设置参与自适应的网口，网络设置优先对专有网口生效。即网络设置首先对 iBMC 专有网口进行适配，如果 iBMC 专有网口链路异常，网络设置再对主机端口进行适配。

使用实例

设置网口模式为 Manual 模式。

```
iBMC:/->ipmcset -d netmode -v 1
Set net mode Manual successfully.
```

查询网口模式。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID          :  1
Net Mode             :  Manual
Net Type             :  Dedicated
IPv4 Information     :
IP Mode              :  dhcp
IP Address           :  192.168.0.12
Subnet Mask          :  255.255.0.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.144 (Activated)
Backup Subnet Mask   :  255.255.255.0 (Activated)
MAC Address          :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode            :  static
IPv6 Address         :  fc00::65
Default Gateway IPv6  :  fc00::1
Link-Local Address   :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State           :  disabled
VLAN ID              : 1
```

4.3.10 设置激活端口（activeport）

命令功能

activeport 命令用于设置 iBMC 管理网口的激活端口。

命令格式

ipmcset -d activeport -v <*option*> [*portid*]

参数说明

参数	参数说明	取值
option	激活端口类型	• 0：专用网口 • 2：PCIe 扩展网口 • 5：OCP 扩展网口 **说明** 不同服务器的参数取值范围不同，具体取值以实际产品为准。
portid	激活端口编号	配置双端口网卡时，取值为 0、1；配置四端口网卡时，取值为 0~3。

使用指南

设置激活端口为专用网口时，不需要带参数 *portid*。

使用实例

设置 iBMC 激活端口为专用网口。

```
iBMC:/->ipmcset -d activeport -v 0
Set active port successfully.
```

查询 iBMC 端口信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  dhcp
IP Address          :  192.168.0.12
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.144 (Activated)
Backup Subnet Mask   :  255.255.255.0 (Activated)
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address         :  fc00::65
Default Gateway IPv6  :  fc00::1
Link-Local Address   :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             : 1
```

4.3.11 设置网口 VLAN（vlan）

命令功能

vlan 命令用于设置网口的 VLAN 信息。

命令格式

ipmcset -d vlan -v <off | *id*>

参数说明

参数	参数说明	取值
off	禁止 VLAN	-
id	网口所属 VLAN	1 ～ 4094

使用指南

无

使用实例

#设置网口 VLAN 为 405。

```
iBMC:/->ipmcset -d vlan -v 405
Set vlan state successfully.
```

查询网口 VLAN 信息。

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  dhcp
IP Address          :  192.168.0.12
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.25
Backup IP Address    :  192.168.0.144 (Activated)
Backup Subnet Mask   :  255.255.255.0 (Activated)
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address         :  fc00::65
Default Gateway IPv6  :  fc00::1
Link-Local Address   :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  enabled
VLAN ID             :  405
```

4.3.12 查询和设置串口方向（serialdir）

命令功能

serialdir 命令用来查询和设置串口方向。

命令格式

ipmcget -d serialdir

ipmcset -d serialdir -v <*option*>

参数说明

参数	参数说明	取值
<*option*>	串口方向	• 0：表示将服务器面板串口切换为操作系统串口 • 1：表示将服务器面板串口切换为 iBMC 串口 • 2：表示将服务器 SOL 串口切换为操作系统串

参数	参数说明	取值
		口 • 3：表示将服务器 SOL 串口切换为 iBMC 串口 • 4：表示将 SDI V3 卡面板串口切换为 SCCL 串口 • 5：表示将 SDI V3 卡面板串口切换为 IMU 串口 • 6：表示将 SDI V3 卡面板串口切换为 SCCL 串口 • 7：表示将 SDI V3 卡面板串口切换为 IMU 串口 不同服务器的参数取值及串口的连接方向可能不同，建议执行 **ipmcget -d serialdir** 命令查看参数取值及串口的连接方向。 **说明** • 服务器未安装 SDI V3 卡时，<*option*>仅支持 0、1、2 和 3。 • 服务器只安装了一张 SDI V3 卡时，<*option*>可支持 4 和 5，用于设置 IO 模组 1 或 IO 模组 2 中安装的 SDI V3 卡。 • 服务器安装了两张 SDI V3 卡时，<*option*>可支持 4、5、6 和 7，其中，4 和 5 表示设置 IO 模组 1 中安装的 SDI V3 卡，6 和 7 表示设置 IO 模组 2 中安装的 SDI V3 卡。

使用指南

- 设置 SOL 串口为系统串口或者 iBMC 串口时，如果当前面板串口是系统串口或者 iBMC 串口，会暂时使面板串口悬空，在 SOL 串口断开后恢复原来的面板串口方向。
- 当串口（面板串口或 SOL 串口）方向设置为系统串口时，在 OS 启动过程中按“Del”可通过串口进入 BIOS Setup 界面。

使用实例

将面板串口设置为 iBMC 串口。

```
iBMC:/->ipmcset -d serialdir -v 1
Set serial port direction successfully.
```

查询当前已连接的串口方向，其中 Num 值表示所设置的<*option*>值。

```
iBMC:/->ipmcget -d serialdir
Currently connected serial direction :
Num         Source               Destination
1           PANEL COM            BMC COM
4           SD100 PANEL COM5       SCCL COM5
```

4.3.13 重启 iBMC 管理系统（reset）

命令功能

reset 命令用来重启 iBMC 管理系统。

命令格式

ipmcset -d reset

参数说明

无

使用指南

无

使用实例

重新启动 iBMC 管理系统。

```
iBMC:/->ipmcset -d reset
This operation will reboot iBMC system. Continue? [Y/N]:y
Resetting...
```

4.3.14 固件升级（upgrade）

命令功能

upgrade 命令用于升级固件。

命令格式

ipmcset -d upgrade -v <*filepath*> *[option]*

参数说明

参数	参数说明	取值
filepath	表示将要升级的目标文件的绝对路径。 说明 该参数只支持“xxx.hpm”格式的文件。	例如：“*/tmp/image.hpm*”
option	表示升级完成后是否立即自动重启 iBMC。	● 1：表示升级完成后立即自动重启 iBMC。 ● 0：表示升级完成后将不会自动重启 iBMC。 默认值：1

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将升级的目标文件上传到 iBMC 文件系统的指定目录（例如“/tmp”）。

说明

文件上传时，不同用户上传的文件不能相互覆盖，即 A 用户删除其上传的文件后，B 用户才能上传同名文件。

升级 iBMC 或 SD 卡控制器后，需重启 iBMC 才能使升级的固件生效。

升级 iBMC 或 SD 卡控制器后：

- *option* 为 1 表示升级完成后立即重启 iBMC。
- *option* 为 0 表示升级完成后将不会自动重启 iBMC，如需使升级的固件生效，请重启 iBMC。

升级 iBMC 时会同时升级主、备分区镜像。

使用实例

升级软件。

```
iBMC:/->ipmcset -d upgrade -v /tmp/image.hpm 1
Please make sure the iBMC is working while upgrading!
Updating...
100%
Update successfully.
```

或

```
iBMC:/->ipmcset -d upgrade -v /tmp/image.hpm 0
Please make sure the iBMC is working while upgrading!
Updating...
```

```
100%
Upgrade successfully and need to reboot the BMC to active the upgrade.
```

4.3.15 截屏命令（printscreen）

命令功能

printscreen 命令用于截取服务器当前所显示的屏幕图片。

命令格式

ipmcset -d printscreen [-v wakeup]

参数说明

参数	参数说明	取值
wakeup	截取屏幕图片的同时唤醒系统屏保	-

使用指南

执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/dev/shm/web”路径下的“manualscreen.jpeg”文件下载到支持查看“.jpeg”文件的客户端（例如 PC）。

说明

多次执行 printscreen 命令时，系统只保存最后一次截屏数据。

使用实例

截取当前服务器操作系统的屏幕。

```
iBMC:/->ipmcset -d printscreen
Download print screen image to /tmp/manualscreen.jpeg successfully.
```

4.3.16 iBMC 软件回滚（rollback）

命令功能

rollback 命令用来将主用 iBMC 固件当前版本的镜像文件切换到可用版本的镜像文件。

命令格式

ipmcset -d rollback

参数说明

无

使用指南

该命令生效后，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。

使用实例

回滚 iBMC 软件。

```
iBMC:/->ipmcset -d rollback
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Set rollback successfully, system will reboot soon!
```

4.3.17 查询软件回滚状态（rollbackstatus）

命令功能

rollbackstatus 命令用来查询软件回滚状态。

命令格式

ipmcget -d rollbackstatus

参数说明

无

使用指南

无

使用实例

查询 iBMC 软件回滚状态。

```
iBMC:/->ipmcget -d rollbackstatus
Last rollback success!
```

4.3.18 设置服务状态（service -d state）

命令功能

service -d state 命令用于设置 iBMC 的服务状态。

命令格式

ipmcset -t service -d state -v <*option*> <**enabled** | **disabled**>

参数说明

参数	参数说明	取值
option	服务类型	• SSH • SNMP • KVM • VNC • VMM • Video • HTTP • HTTPS • RMCP • RMCP+ • SSDP
enabled	启用服务	-
disabled	禁用服务	-

使用指南

输入 *option* 参数时，大小写均支持。

使用实例

启用 HTTP 服务。

```
iBMC:/->ipmcset -t service -d state -v http enabled
WARNING: Enabling the http functions may reduce system security. Exercise caution
when enabling these functions.
Do you want to continue?[Y/N]:y
Set http service state(enabled) successfully.
```

说明

开启 http 服务有安全隐患。

4.3.19 设置指定服务的端口号（service -d port）

命令功能

service -d port 命令用于设置 iBMC 指定服务的端口号。

命令格式

ipmcset -t service -d port -v <*option*> <*port1value*> [*port2value*]

参数说明

参数	参数说明	取值
option	服务类型	• SSH • SNMP • KVM • VNC • VMM • Video • HTTP • HTTPS • RMCP
port1value	服务的端口号	1～65535
port2value	服务的端口号，只有RMCP 服务可以设置此端口	1～65535

使用指南

Web Server(HTTP)/Web Server(HTTPS)端口修改为 65535 时，Chrome 浏览器无法通过该端口建立会话。

使用实例

设置 HTTPS 服务的端口号为 443。

```
iBMC:/->ipmcset -t service -d port -v https 443
Set https service port to 443 successfully.
```

4.3.20 查询服务状态（service -d list）

命令功能

service -d list 命令用于查询服务状态。

命令格式

ipmcget -t service -d list

参数说明

无

使用指南

无

使用实例

查询服务状态。

```
iBMC:/->ipmcget -t service -d list
service name    | state          | port
SSH             | Enabled        | 22
SNMP            | Enabled        | 161
KVM             | Enabled        | 2198
VNC             | Disabled       | 5900
VMM             | Enabled        | 8208
Video           | Enabled        | 2199
HTTP            | Enabled        | 80
HTTPS           | Enabled        | 443
RMCP            | Disabled       | 623,664
RMCP+           | Enabled        | 623,664
SSDP            | Disabled       | 1900
```

4.3.21 设置登录安全性信息功能的使能状态（securitybanner -d state）

命令功能

securitybanner -d state 命令用于设置是否在 iBMC 登录界面显示安全信息。

命令格式

ipmcset -t securitybanner -d state -v <enabled | disabled>

参数说明

参数	参数说明	取值
enabled	表示在登录界面显示安全信息。	-
disabled	表示不在登录界面显示安全信息。	-

使用指南

无

使用实例

设置在 iBMC 登录界面显示安全信息。

```
iBMC:/->ipmcset -t securitybanner -d state -v enabled
Enable login security banner state successfully.
```

4.3.22 定制登录安全信息（securitybanner -d content）

命令功能

securitybanner -d content 命令用于设置在 iBMC 登录界面显示的安全信息的具体内容。

命令格式

ipmcset -t securitybanner -d content -v < **default** | *“option”* >

参数说明

参数	参数说明	取值
default	表示使用默认的安全信息，不做修改。	-
option	表示安全信息的具体内容	0 ~ 1024 个字符组成的字符串

使用指南

无

使用实例

设置登录安全信息为默认内容。

```
iBMC:/-> ipmcset -t securitybanner -d content -v default
Set login security banner content successfully.
```

4.3.23 查询登录安全信息（securitybanner -d info）

命令功能

securitybanner -d info 命令用于查询 iBMC 登录界面显示的安全信息的详细内容。

命令格式

ipmcget -t securitybanner -d info

参数说明

无

使用指南

无

使用实例

查询登录安全信息。

```
iBMC:/-> ipmcget -t securitybanner -d info
Login security banner information state: enabled.

Login security banner information:
WARNING! This system is PRIVATE and PROPRIETARY and may only be accessed by
authorized users. Unauthorized use of the system is prohibited. The owner, or its
agents, may monitor any activity or communication on the system. The owner, or its
agents, may retrieve any information stored within the system. By accessing and
using the system, you are consenting to such monitoring and information retrieval
for law enforcement and other purposes.
```

4.3.24 导入 SSL 证书（certificate -d import）

命令功能

certificate -d import 命令用于导入 SSL 证书到 iBMC 系统。

命令格式

ipmcset -t certificate -d import -v <*filepath* | *file_URL*> <*type*> [*passphrase*]

参数说明

参数	参数说明	取值
filepath	待导入的 SSL 证书的路径 说明 支持“*.pfx”、“*.p12”格式，且不大于 100KB 的证书。	证书在 iBMC 上的绝对路径，例如：“/*tmp*/*test.pfx*”。
file_URL	待导入的远程 SSL 证书文件的 URL	格式为： *protocol*://*username*:*password@IP:[port]*/*directory/filename* 其中： • *protocol*：必须为“https”、“sftp”、“cifs”和“scp”中的一种。

参数	参数说明	取值
		说明 • iBMC 当前仅支持 SMB V1.0 版本。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp 或 scp 协议。 • *username*：登录目标服务器所需的用户名。 • *password*：登录目标服务器所需的密码。 • *IP:[port]*：目标服务器的 IP 地址和端口号。 • *directory/filename*：远程 SSL 证书在目标服务器上的绝对路径。 例如： https://root:Admin12#$@10.10.10.1:443/tmp/test.pfx
type	SSL 证书类型	固定为 1。
passphrase	生成 SSL 证书时的密码	密码为空时，此参数可为空。

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将准备好的 SSL 证书上传到 iBMC 文件系统的指定目录下（例如"/tmp"）。

使用实例

导入 SSL 证书。

```
iBMC:/-> ipmcset -t certificate -d import -v /tmp/test-01.pfx 1 Admin12#$
Import certificate successfully
```

4.3.25 查询 SSL 证书信息（certificate -d info）

命令功能

certificate -d info 命令用于查询 SSL 证书的信息。

命令格式

ipmcget -t certificate -d info

参数说明

无

使用指南

无

使用实例

查询 SSL 证书信息。

```
iBMC:/-> ipmcget -t certificate -d info
SSL Certificate Information:
Issued    To: CN=Server, OU=IT, O=Mytest, L=ShenZhen, S=GuangDong, C=CN
Issued    By: CN=Server, OU=IT, O=Mytest, L=ShenZhen, S=GuangDong, C=CN
Valid   From: Jul 25 2014 UTC
Valid     To: Jul 22 2024 UTC
Serial Number: 0
```

4.3.26 导出配置文件（config -d export）

命令功能

config -d export 命令用于导出 iBMC、BIOS 和 RAID 控制器当前配置文件。

命令格式

ipmcget -t config -d export -v <*filepath* | *file_URL*>

参数说明

参数	参数说明	取值
filepath	配置文件导出后的本地存放路径	iBMC 系统中的路径，例如：“/tmp/config.xml”。
file_URL	配置文件导出后的远程存放路径	格式为： *protocol*://*[username*:*password@]IP:[port]/directory/filename* 其中： • *protocol*：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 • iBMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含 *username*:*password*@字段；使用其它协议时，存放路径中必须包含 *username*:*password*@字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • *username*：登录目标服务器所需的用户名。 • *password*：登录目标服务器所需的密码。

参数	参数说明	取值
		• *IP:[port]*：目标服务器的 IP 地址和端口号。 • *directory/filename*：配置文件在目标服务器上的绝对路径。 例如： https://root:Admin12#$@10.10.10.1:443/tmp/config.xml

使用指南

执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/tmp/config.xml”路径下的配置文件（例如“config.xml”）下载到客户端（例如 PC）。

使用实例

导出配置文件。

```
iBMC:/-> ipmcget -t config -d export -v /tmp/config.xml
NOTE: The exported RAID Controller configurations are valid only if they are
exported after the POST is complete.
Collecting configuration...
100%
Export configuration successfully.
```

4.3.27 导入配置文件（config -d import）

命令功能

config -d import 命令用于导入 iBMC、BIOS 和 RAID 控制器配置文件。

命令格式

ipmcset -t config -d import -v <*filepath* | *file_URL*>

参数说明

参数	参数说明	取值
filepath	待导入的配置文件所在本地路径。	配置文件在 iBMC 系统上的绝对路径，例如：“*/tmp/config.xml*”。
file_URL	待导入的配置文件所在远程路径。	格式为： *protocol*://[*username*:*password*@]*IP:[port]*/*directory/filename* 其中：

参数	参数说明	取值
		• *protocol*：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 • iBMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含 *username*:*password*@字段；使用其它协议时，存放路径中必须包含 *username*:*password*@字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • *username*：登录目标服务器所需的用户名。 • *password*：登录目标服务器所需的密码。 • *IP:[port]*：目标服务器的 IP 地址和端口号。 • *directory/filename*：配置文件在目标服务器上的绝对路径。 例如： https://root:Admin12#$@10.10.10.1:443/tmp/config.xml

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将准备好的配置文件上传到 iBMC 文件系统的指定目录下（例如"/tmp"）。

使用实例

导入配置文件。

```
iBMC:/-> ipmcset -t config -d import -v /tmp/testconfig.xml
Setting configuration...
100%
Import configuration successfully.
Reset OS for the BIOS config to take effect.
```

4.3.28 导入 CRL 文件（crl）

命令功能

crl 命令用于导入升级包完整性校验所使用的证书撤销列表文件。

命令格式

ipmcset -d crl –v *<localpath | URL> <type>*

参数说明

参数	参数说明	取值
localpath	待导入的 CRL 文件的路径 说明 支持*.crl 格式，且不大于 100KB 的文件。	CRL 文件在 iBMC 上的绝对路径，例如：“/tmp/cms.crl”。
URL	待导入的远程 CRL 文件的 URL	格式为： *protocol*://*[username*:*password@]IP[:port]*/*directory/filename* 其中： • *protocol*：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 • iBMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含 *username*:*password*@字段；使用其它协议时，存放路径中必须包含 *username*:*password*@字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • *username*：登录目标服务器所需的用户名。 • *password*：登录目标服务器所需的密码。 • *IP[:port]*：目标服务器的 IP 地址和端口号。 • *directory/filename*：远程 CRL 文件在目标服务器上的绝对路径。 例如： “https://Administrator:Admin@9000@10.10.10.1:443/tmp/ cms.crl”
type	CRL 文件类型	固定为 1。

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将待导入的文件上传到 iBMC 文件系统的指定目录下（例如“/tmp”）。

使用实例

导入 CRL 文件。

```
iBMC:/-> ipmcset -d crl -v /tmp/cms.crl 1
Import CRL file successfully.
```

4.3.29 挂载文件到虚拟光驱（vmm -d connect）

命令功能

vmm -d connect 命令用于挂载文件到虚拟光驱。

命令格式

ipmcset -t vmm -d connect -v <*file_URL*>

参数说明

参数	参数说明	取值
file_URL	待挂载的文件所在的远程路径。	格式为： *protocol*://*[username*:*password@]IP[:port]*/*directory/filename* 其中： • *protocol*：必须为“nfs”、“cifs”或“https”。 说明 • iBMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含 *username*:*password*@字段；使用其它协议时，存放路径中必须包含 *username*:*password*@字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https 或 nfs 协议。 • *username*：登录目标服务器所需的用户名。 • *password*：登录目标服务器所需的密码。 • *IP[:port]*：目标服务器的 IP 地址和端口号。 • *directory/filename*：待挂载的文件在目标服务器上的绝对路径。 例如： nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso 或 nfs://[fc00::64]/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso 说明 file_URL 的最大长度为 255 个字符。

使用指南

无

使用实例

挂载文件到虚拟光驱。

```
iBMC:/-> ipmcset -t vmm -d connect -v
nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso

Connect virtual media...
.............
Connect virtual media successfully.
```

4.3.30 中断虚拟光驱的连接（vmm -d disconnect）

命令功能

vmm -d disconnect 命令用于断开虚拟光驱的连接。

命令格式

ipmcset -t vmm -d disconnect

参数说明

无

使用指南

无

使用实例

中断虚拟光驱的连接。

```
iBMC:/-> ipmcset -t vmm -d disconnect
Disconnect virtual media...
.....
Disconnect virtual media successfully.
```

4.3.31 查询虚拟媒体信息（vmm -d info）

命令功能

vmm -d info 命令用于查询 iBMC 虚拟媒体信息。

命令格式

ipmcget -t vmm -d info

参数说明

无

使用指南

无

使用实例

查询虚拟媒体信息。

```
iBMC:/-> ipmcget -t vmm -d info
Virtual Media Information:
Maximum Number of Virtual Media Sessions:    1
Number of Activated Sessions          :    0
Activated Sessions URL                :
```

4.3.32 将 FPGA 卡的 Golden 固件恢复出厂设置（fpgagoldenfwrestore）

命令功能

fpgagoldenfwrestore 命令用于 FPGA 卡无法正常工作时，将 FPGA 卡的 Golden 固件恢复出厂设置。

命令格式

ipmcset -d fpgagoldenfwrestore -v <*slotid*> [*position*]

参数说明

参数	参数说明	取值
slotid	FPGA 卡的槽位号	1~16
position	FPGA 卡所处的位置	0

使用指南

FPGA 卡为正常状态时执行此命令，OS 将会重启。请谨慎操作。

使用实例

将 FPGA 卡的 Golden 固件恢复出厂设置。

```
iBMC:/-> ipmcset -d fpgagoldenfwrestore -v 6
WARNING: This operation may cause unexpected reset of the OS and affect services.
Do you want to continue?[Y/N]:y
The restore of the Golden firmware of the FPGA card is starting.
100%
The restore of the Golden firmware of the FPGA card is successful.
```

或

```
iBMC:/-> ipmcset -d fpgagoldenfwrestore -v 6 0
WARNING: This operation may cause unexpected reset of the OS and affect services.
Do you want to continue?[Y/N]:y
The restore of the Golden firmware of the FPGA card is starting.
100%
The restore of the Golden firmware of the FPGA card is successful.
```

4.4 Trap 命令

介绍服务器 trap 相关命令的查询和设置方法。

4.4.1 查询和设置 SNMP trap 状态（trap -d state）

命令功能

trap -d state 命令用于查询和设置 iBMC 的 SNMP trap 功能的使能和禁止状态。

命令格式

ipmcget -t trap -d state [-v *destination*]

ipmcset -t trap -d state -v [*destination*] <**disabled** | **enabled**>

参数说明

参数	参数说明	取值
destination	表示 SNMP trap 目标项。	• 1~4 • 不输入该参数时，表示启用或禁用 trap 功能。
disabled	表示禁用 SNMP trap 功能。	-
enabled	表示启用 SNMP trap 功能。	-

使用指南

- 需要对相应编号的通道进行操作时，设置 *destination* 参数，取值范围为 1~4。
- 需要对 trap 功能操作，即启用或禁用 trap 功能时，不需要-v [*destination*]字段。

使用实例

禁用 iBMC 的 SNMP trap 目标 1。

```
iBMC:/->ipmcset -t trap -d state -v 1 disabled
Set trap dest1 disabled successfully.
```

查询当前 SNMP trap 目标 1 的使能状态。

```
iBMC:/->ipmcget -t trap -d state -v 1
trap dest1 state : disabled
```

4.4.2 设置 SNMP trap 上报端口号（trap -d port）

命令功能

trap -d port 命令用于设置 iBMC 的 SNMP trap 上报端口号。

命令格式

ipmcset -t trap -d port -v <*destination*> <*portvalue*>

参数说明

参数	参数说明	取值
destination	表示 SNMP trap 目标项。	1 ~ 4
portvalue	表示 SNMP trap 端口号。	SNMP trap 端口号的默认值是 162，取值范围是 1 ~ 65535。

使用指南

无

使用实例

设置 SNMP trap 目标 1 的端口号为 1024。

```
iBMC:/->ipmcset -t trap -d port -v 1 1024
Set trap dest1 port successfully.
```

4.4.3 设置 SNMP trap 团体名称（trap -d community）

命令功能

trap -d community 命令用于设置 iBMC 的 SNMP trap 团体名称。

命令格式

ipmcset -t trap -d community

参数说明

参数	参数说明	取值

参数	参数说明	取值
Community	表示 SNMP trap 团体名称。	默认取值：“TrapAdmin12#$” 关闭密码检查时的取值原则：1～18 位的字符串，由数字、英文字母和除空格外的特殊字符组成。 开启密码检查时的取值原则： • 长度为 8～18 位的字符。 • 至少包含以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/? • 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。

使用指南

无

使用实例

设置 SNMP trap 的团体名称为 mytrap。

```
iBMC:/->ipmcset -t trap -d community
New Community:
Confirm Community:
Set SNMP trap community successfully.
```

4.4.4 设置 SNMP trap 目的 IP 地址（trap -d address）

命令功能

trap -d address 命令用于设置 SNMP trap 上报信息的目的 IP 地址。

命令格式

ipmcset -t trap -d address -v <*destination*> <*ipaddr*>

参数说明

参数	参数说明	取值
destination	表示 SNMP trap 目标项。	1~4
ipaddr	表示接收事件信息上报的 IP 地址。	数据类型为 IPv4（格式为“xxx.xxx.xxx.xxx”）、IPv6（格式为“xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx”）或为空（格式为""）。

使用指南

ipaddr 设置为空时表示清除 IP 地址。

使用实例

设置 SNMP trap 目标 1 接收事件上报信息的 IP 地址为 10.10.10.10。

```
iBMC:/->ipmcset -t trap -d address -v 1 10.10.10.10
Set trap dest1 address successfully.
```

清除 SNMP trap 目标 1 接收事件上报信息的 IP 地址。

```
iBMC:/->ipmcset -t trap -d address -v 1 ""
Set trap dest1 address successfully.
```

4.4.5 查询 Trap 上报目的地址信息（trap -d trapiteminfo）

命令功能

trap -d trapiteminfo 命令用于查询 SNMP trap 上报信息的目的 IP 地址、上报端口、使能状态。

命令格式

ipmcget -t trap -d trapiteminfo

参数说明

无

使用指南

无

使用实例

查询 SNMP Trap 上报目的地址信息。

```
iBMC:/->ipmcget -t trap -d trapiteminfo

TrapItem Num    | state     | port      | alert address
1             | enabled   | 1024      |
2             | disabled  | 162       |
3             | disabled  | 162       |
4             | disabled  | 162       |
```

4.4.6 查询和设置 SNMP trap 版本信息（trap -d version）

命令功能

trap -d version 命令用于查询和设置 SNMP trap 版本信息。

命令格式

ipmcget -t trap -d version

ipmcset -t trap -d version -v <*V1* | *V2C* | *V3*>

参数说明

参数	参数说明	取值
V1	表示 SNMP trap 版本号为 V1。	-
V2C	表示 SNMP trap 版本号为 V2C。	-
V3	表示 SNMP trap 版本号为 V3。	-

使用指南

SNMP trap 默认版本为 V1。

使用实例

设置 SNMP trap 版本为 V2C。

```
iBMC:/->ipmcset -t trap -d version -v V2C
Set trap V2C success.
```

说明

V1 和 V2C 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 V3 版本的 SNMP Trap。

查询 SNMP trap 版本信息。

```
iBMC:/->ipmcget -t trap -d version
Trap version : V2C
```

4.4.7 查询和设置 SNMP trap 告警发送级别（trap -d severity）

命令功能

trap -d severity 命令用于查询和设置 SNMP trap 的告警发送级别。

命令格式

ipmcget -t trap -d severity

ipmcset -t trap -d severity -v <*level*>

参数说明

参数	参数说明	取值
level	表示 SNMP trap 的告警发送级别。	• none：表示不发送告警。 • all：表示发送的告警包含所有故障和日志告警。 • normal：表示发送的告警仅包括日志告警。 • minor：表示发送的告警为轻微故障告警。 • major：表示发送的告警为严重故障告警。 • critical：表示发送的告警为紧急故障告警。

使用指南

可同时设置多种告警级别，如 **ipmcset -t trap -d severity -v normal minor**。

使用实例

设置 SNMP trap 发送告警的级别为 minor。

```
iBMC:/->ipmcset -t trap -d severity -v minor
Set trap severity successfully.
```

查询当前 SNMP trap 发送告警的级别。

```
iBMC:/->ipmcget -t trap -d severity
Trap severity :  minor
```

4.4.8 查询和设置 SNMP trap V3 用户（trap -d user）

命令功能

trap -d user 命令用于查询和设置 SNMP trap V3 用户。

命令格式

ipmcget -t trap -d user

ipmcset -t trap -d user -v <*username*>

参数说明

参数	参数说明	取值
username	表示 SNMP trap V3 用户。	已存在的用户名。

使用指南

需要管理工作站配置相同用户名、密码的用户。

默认情况下，Trap V3 使用“Administrator”用户。

使用实例

设置 SNMP trap V3 用户。

```
iBMC:/->ipmcset -t trap -d user -v root
Set trap user root successfully.
```

查询 SNMP trap V3 用户。

```
iBMC:/->ipmcget -t trap -d user
Trap user : root
```

4.4.9 查询和设置 SNMP trap 模式（trap -d mode）

命令功能

trap -d mode 命令用于查询和设置 SNMP trap 模式。

命令格式

ipmcget -t trap -d mode

ipmcset -t trap -d mode -v <*option*>

参数说明

参数	参数说明	取值
option	表示 SNMP trap 模式类型。	• “0”，表示 trap 模式是 Event Code。 • “1”，表示 trap 模式是 OID。 • “2”，表示 trap 模式是 Precise Alarm (recommended)。

使用指南

上报告警时，“精准告警模式(推荐)”相较“OID 模式”和“事件码模式”，可提供更为精准的定位信息。

使用实例

设置 SNMP trap 模式为 Event Code。

```
iBMC:/->ipmcset -t trap -d mode -v 0
Set trap mode Event Code success.
```

查询 SNMP trap 模式信息。

```
iBMC:/->ipmcget -t trap -d mode
Trap mode: Event Code
```

4.5 Syslog 命令

介绍服务器 syslog 相关命令的查询和设置方法。

4.5.1 查询和设置 syslog 使能状态（syslog -d state）

命令功能

syslog -d state 命令用于查询和设置 iBMC 的 syslog 上报功能的使能状态。

命令格式

ipmcget -t syslog -d state [-v *destination*]

ipmcset -t syslog -d state -v [*destination*] <**disabled** | **enabled**>

参数说明

参数	参数说明	取值

参数	参数说明	取值
destination	表示 syslog 上报通道的编号。	• 1~4 • 不输入该参数时，表示启用或禁用 syslog 功能。
disabled	表示禁用 syslog 上报功能。	-
enabled	表示启用 syslog 上报功能。	-

使用指南

- 需要对相应编号的通道进行操作时，请先启用 syslog 功能。
- 需要对相应编号的通道进行操作时，设置 *destination* 参数，取值范围为 1~4。

使用实例

启用 syslog 上报功能。

```
iBMC:/->ipmcset -t syslog -d state -v enabled
Set syslog enabled successfully.
```

查询 syslog 上报功能的使能状态。

```
iBMC:/->ipmcget -t syslog -d state
syslog state: enabled
```

禁用通道 1 的 syslog 上报功能。

```
iBMC:/->ipmcset -t syslog -d state -v 1 disabled
Set syslog dest1 disabled successfully.
```

查询通道 1 的 syslog 上报功能的使能状态。

```
iBMC:/-> ipmcget -t syslog -d state -v 1
syslog dest1 state: disabled
```

4.5.2 查询和设置证书认证方式（syslog -d auth）

命令功能

syslog -d auth 命令用于查询和设置证书认证方式。

命令格式

ipmcget -t syslog -d auth

ipmcset -t syslog -d auth -v <*option*>

参数说明

参数	参数说明	取值
option	表示证书认证方式。	• 1：单向认证 • 2：双向认证

使用指南

- 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。

使用实例

设置证书认证方式为双向认证。

```
iBMC:/->ipmcset -t syslog -d auth -v 2
Set syslog auth type successfully.
```

查询当前证书认证方式。

```
iBMC:/-> ipmcget -t syslog -d auth
Syslog auth type: mutual authentication
```

4.5.3 查询和设置 syslog 主机标识（syslog -d identity）

命令功能

syslog -d identity 命令用于查询和设置 syslog 日志上报时使用的主机标识。

命令格式

ipmcget -t syslog -d identity

ipmcset -t syslog -d identity -v <*option*>

参数说明

参数	参数说明	取值
option	表示要设置的主机标识	• 1：单板序列号 • 2：产品资产标签 • 3：主机名

使用指南

无

使用实例

设置 syslog 主机标识为主机名。

```
iBMC:/-> ipmcset -t syslog -d identity -v 3
Set syslog identity successfully.
```

查询 syslog 主机标识。

```
iBMC:/-> ipmcget -t syslog -d identity
Syslog identity: host name
```

4.5.4 查询和设置传输协议类型（syslog -d protocol）

命令功能

syslog -d protocol 命令用于查询和设置上报 syslog 日志时采用的传输协议类型。

命令格式

ipmcget -t syslog -d protocol

ipmcset -t syslog -d protocol -v <*option*>

参数说明

参数	参数说明	取值
option	表示采用的协议类型。	• 1：UDP • 2：TCP • 3：TLS

使用指南

- 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。

使用实例

设置 syslog 上报时采用的协议类型为“TLS”。

```
iBMC:/-> ipmcset -t syslog -d protocol -v 3
Set syslog protocol successfully.
```

查询当前 syslog 上报时采用的协议类型。

```
iBMC:/-> ipmcget -t syslog -d protocol
Syslog protocol: TLS
```

4.5.5 查询和设置上报日志的级别（syslog -d severity）

命令功能

syslog -d severity 命令用于查询和设置通过 syslog 上报的日志的级别。

命令格式

ipmcget -t syslog -d severity

ipmcset -t syslog -d severity -v <*level*>

参数说明

参数	参数说明	取值
level	表示上报日志的级别。	• none：表示不发送告警。 • all：表示发送的告警包含所有故障和日志告警。 • normal：表示发送的告警包含所有故障和日志告警。 • minor：表示发送的告警为轻微、严重、紧急故障告警。 • major：表示发送的告警为严重、紧急故障告警。 • critical：表示发送的告警为紧急故障告警。

使用指南

无

使用实例

设置 syslog 上报日志的级别为“critical”。

```
iBMC:/->ipmcset -t syslog -d severity -v critical
Set syslog severity successfully.
```

查询 syslog 上报日志的级别。

```
iBMC:/-> ipmcget -t syslog -d severity
Syslog severity:  critical
```

4.5.6 查询和上传服务器根证书（syslog -d rootcertificate）

命令功能

syslog -d rootcertificate 命令可将 syslog 服务器的根证书上传到 iBMC，或查询当前根证书信息。

命令格式

ipmcget -t syslog -d rootcertificate

ipmcset -t syslog -d rootcertificate -v <*filepath*>

参数说明

参数	参数说明	取值
filepath	表示待上传的根证书在 iBMC 上的绝对路径。	绝对路径，例如：“*/tmp/rootcertificate.cer*”。

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将用户自行生成的根证书文件上传到 iBMC 文件系统的指定目录（例如“/tmp”）。

说明

请定期更新证书，否则可能存在安全风险。

使用实例

上传服务器根证书。

```
iBMC:/-> ipmcset -t syslog -d rootcertificate -v /tmp/rootcertificate.cer
Set syslog root certificate successfully.
```

查询服务器根证书信息。

```
iBMC:/-> ipmcget -t syslog -d rootcertificate
Server Root Certificate:
Issued    To: CN=SERVER, OU=IT, O=TS, L=, S=GD, C=CH
Issued    By: CN=Info, OU=IT, O=Mytest, L=ShenZhen, S=GuangDong, C=CN
Valid   From: Mar 24 2016 UTC
Valid     To: Mar 24 2017 UTC
Serial Number: 0b
```

4.5.7 查询和上传本地证书（syslog -d clientcertificate）

命令功能

syslog -d clientcertificate 命令可将 syslog 客户端证书上传到 iBMC，或查询本地证书信息。

命令格式

ipmcget -t syslog -d clientcertificate

ipmcset -t syslog -d clientcertificate -v <*filepath*> <*password*>

参数说明

参数	参数说明	取值
filepath	表示待上传的本地证书在 iBMC 上的绝对路径。	绝对路径，例如：“*/tmp/rootcertificate.cer*”。
password	表示用于解密本地证书的密码。	该密码在使用证书服务器生成本地证书时同步生成。

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将用户自行生成的本地证书文件上传到 iBMC 文件系统的指定目录（例如“/tmp”）。

说明

请定期更新证书，否则可能存在安全风险。

使用实例

上传本地证书。

```
iBMC:/-> ipmcset -t syslog -d client -v /tmp/clientcertificate.pfx syslogpw
Set syslog client certificate successfully.
```

查询本地证书信息。

```
iBMC:/-> ipmcget -t syslog -d clientcertificate
Syslog Client Certificate Information:
Issued    To: CN=Server, OU=IT, O=Mytest, L=ShenZhen, S=GuangDong, C=CN
Issued    By: CN=Administrator, OU=it3, O=ts3, L=, S=guangdong2, C=cn
Valid From   : Feb 17 2015 UTC
Valid     To: Feb 17 2016 UTC
Serial Number: 25
```

4.5.8 设置 syslog 服务器地址（syslog -d address）

命令功能

syslog -d address 命令用于设置 syslog 服务器地址。

命令格式

ipmcset -t syslog -d address -v <*destination*> <*ipaddr*>

参数说明

参数	参数说明	取值
destination	表示 syslog 上报通道的编号。	1 ~ 4
ipaddr	表示 syslog 服务器地址。	可以为 IPv4 地址、IPv6 地址、域名地址或为空。

使用指南

ipaddr 设置为空时表示清除 IP 地址。

使用实例

设置通道 1 的 syslog 服务器地址为“host”。

```
iBMC:/-> ipmcset -t syslog -d address -v 1 host
Set syslog dest1 address successfully.
```

查询 syslog 服务器地址。

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1              | disabled  | 0         | host                | operationlogs
securitylogs eventlogs
2              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
3              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
4              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
```

清除通道 1 的 syslog 服务器地址。

```
iBMC:/-> ipmcset -t syslog -d address -v 1 ""
Set syslog dest1 address successfully.
```

4.5.9 设置 syslog 服务器端口号（syslog -d port）

命令功能

syslog -d port 命令用于设置 syslog 服务器端口号。

命令格式

ipmcset -t syslog -d port -v <*destination*> <*portvalue*>

参数说明

参数	参数说明	取值
destination	表示 syslog 上报通道的编号。	1 ~ 4
portvalue	表示 syslog 服务器端口号。	1 ~ 65535

使用指南

无

使用实例

设置通道 1 的 syslog 服务器端口号为“65535”。

```
iBMC:/-> ipmcset -t syslog -d port -v 1 65535
Set syslog dest1 port successfully.
```

查询 syslog 服务器端口。

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1              | disabled  | 65535     | host                | operationlogs
securitylogs eventlogs
2              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
3              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
4              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
```

4.5.10 设置上报日志类型（syslog -d logtype）

命令功能

syslog -d logtype 命令用于设置通过 syslog 报文上报的日志的类型。

命令格式

ipmcset -t syslog -d logtype -v *<destination> <type>*

参数说明

参数	参数说明	取值
destination	表示 syslog 上报通道的编号。	1 ~ 4
type	表示上报日志类型。	• none：不上报 • all：上报所有日志 • operationlogs：上报操作日志 • securitylogs：上报安全日志 • eventlogs：上报事件日志

使用指南

无

使用实例

设置通道 4 上报的日志类型为操作日志和事件日志。

```
iBMC:/-> ipmcset -t syslog -d logtype -v 4 operationlogs eventlogs
Set syslog log type successfully.
```

查询通道 4 上报的日志类型。

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1              | disabled  | 65535     | host                | operationlogs
securitylogs eventlogs
2              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
3              | disabled  | 0         |                     | operationlogs
securitylogs eventlogs
4              | disabled  | 0         |                     | operationlogs eventlogs
```

4.5.11 测试 syslog 服务器是否可连接（syslog -d test）

命令功能

syslog -d test 命令用于测试配置的 syslog 服务器是否可连接。

命令格式

ipmcset -t syslog -d test -v <*destination*>

参数说明

参数	参数说明	取值
destination	表示 syslog 上报通道的编号。	1 ~ 4

使用指南

无

使用实例

测试通道 1 配置的 syslog 服务器是否可连接。

```
iBMC:/-> ipmcset -t syslog -d test -v 1
Test syslog dest1 successfully.
```

4.5.12 查询所有 syslog 上报通道配置信息（syslog -d iteminfo）

命令功能

syslog -d iteminfo 命令用于查询 4 条 syslog 日志上报通道的配置情况。

命令格式

ipmcget -t syslog -d iteminfo

参数说明

无

使用指南

无

使用实例

查询 iBMC syslog 日志上报通道的配置情况。

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1              | disabled  | 65535     | host                | operationlogs
securitylogs eventlogs
2              | disabled  | 0         |                     | operationlogs
```

```
securitylogs eventlogs
3             | disabled   | 0        |                  | operationlogs
securitylogs eventlogs
4             | disabled   | 0        |                  | operationlogs eventlogs
```

4.6 VNC 命令

介绍服务器 VNC 相关命令的查询和设置方法。

4.6.1 查询 VNC 服务信息（vnc -d info）

命令功能

vnc -d info 命令用于查询 VNC 服务的信息。

命令格式

ipmcget -t vnc -d info

参数说明

无

使用指南

无

使用实例

查询 VNC 服务的信息。

```
iBMC:/->ipmcget -t vnc -d info
Timeout Period(Min)       :   60
SSL Encryption           :   enabled
Active Sessions          :   0
Keyboard Layout          :   jp
Password Validity(Days)    :   Indefinite
```

4.6.2 设置 VNC 服务的密码（vnc -d password）

命令功能

vnc -d password 命令用于设置 VNC 服务的密码。

命令格式

ipmcset -t vnc -d password

参数说明

无

使用指南

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

使用实例

设置 VNC 服务的密码。

```
iBMC:/->ipmcset -t vnc -d password
Input your password:
Incorrect password or locked account.
```

4.6.3 设置 VNC 服务的超时时长（vnc -d timeout）

命令功能

vnc -d timeout 命令用于设置 VNC 服务的超时时长。

命令格式

ipmcset -t vnc -d timeout -v <*value*>

参数说明

参数	参数说明	取值
value	表示 VNC 服务的超时时长	• 0：永不超时 • 1~480：超时时长，单位为分钟

使用指南

无

使用实例

设置 VNC 服务超时的时长。

```
iBMC:/->ipmcset -t vnc -d timeout -v 0
Set VNC timeout period successfully.
```

4.6.4 设置 VNC 服务 SSL 加密功能的状态（vnc -d ssl）

命令功能

vnc -d ssl 命令用于设置 VNC 服务 SSL 加密功能的状态。

命令格式

ipmcset -t vnc -d ssl -v <*enabled*|*disabled*>

参数说明

参数	参数说明	取值
enabled	表示启用 SSL 加密功能	-
disabled	表示禁止 SSL 加密功能	-

使用指南

无

使用实例

设置 VNC 服务 SSL 加密功能为启用状态。

```
iBMC:/->ipmcset -t vnc -d ssl -v enabled
Set VNC SSL encryption state (enabled) successfully.
```

4.6.5 设置 VNC 服务的键盘布局（vnc -d keyboardlayout）

命令功能

vnc -d keyboardlayout 命令用于设置 VNC 服务的键盘布局。

命令格式

ipmcset -t vnc -d keyboardlayout -v <*en*|*jp*|*de*>

参数说明

参数	参数说明	取值
en	表示美式键盘	-
jp	表示日式键盘	-
de	表示德式键盘	-

使用指南

无

使用实例

设置 VNC 服务的键盘布局为日式键盘。

```
iBMC:/->ipmcset -t vnc -d keyboardlayout -v jp
Set VNC keyboard layout to (jp) successfully.
```

4.7 服务器命令

4.7.1 查询和设置启动设备（bootdevice）

命令功能

bootdevice 用来查询和设置启动设备。

命令格式

ipmcget -d bootdevice

ipmcset -d bootdevice -v <*option*> [*once* | *permanent*]

参数说明

参数	参数说明	取值
option	设置的启动设备编号。	• 0：取消强制启动。 • 1：从 PXE 启动。 • 2：从默认的硬盘启动。 • 5：从默认的 CD/DVD 启动。

参数	参数说明	取值
		• 6：启动后进入 BIOS 菜单。 • 0xF：从软驱或第一个移动介质启动。
once	系统启动项的设置仅在下一次重启时生效，重启完成后，系统启动项自动恢复为 BIOS 中设置的默认方式。	-
permanent	系统启动项的设置永久有效。	-

使用指南

无

使用实例

说明

如果打印信息中的提示是“Unspecified”，表示未设置设备强制启动参数。

设置启动设备从默认的硬盘启动，仅生效一次。

```
iBMC:/->ipmcset -d bootdevice -v 2 once
```

查询修改后的启动设备。

```
iBMC:/->ipmcget -d bootdevice
Boot    device:  Force boot from default Hard-drive
Effective  type:  Once
```

4.7.2 设置服务器重启方式（frucontrol）

命令功能

frucontrol 命令设置服务器的重启方式。

命令格式

ipmcset [-t fru0] **-d frucontrol** -v <*option*>

参数说明

参数	参数说明	取值
option	服务器重启方式	• 0：表示强制重启服务器

参数	参数说明	取值
		• 2：表示强制下电再上电服务器

使用指南

服务器在下电状态时不支持该命令。

使用实例

强制重启服务器。

```
iBMC:/->ipmcset -d frucontrol -v 0
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced system reset) successfully.
```

强制下电再上电服务器。

```
iBMC:/->ipmcset -d frucontrol -v 2
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced power cycle) successfully.
```

4.7.3 查询和设置服务器上下电状态（powerstate）

命令功能

powerstate 命令用于查询和控制服务器的上电和下电状态。

命令格式

ipmcget [-t fru0] **-d powerstate**

ipmcset [-t fru0] **-d powerstate -v** <*option*>

参数说明

参数	参数说明	取值
option	要对服务器进行的操作	• 0：正常下电 • 1：上电 • 2：强制下电

使用指南

服务器在下电状态时执行下电命令无效。

使用实例

对服务器执行上电命令操作。

```
iBMC:/->ipmcset -d powerstate -v 1
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Control fru0 power on successfully.
```

查询服务器上下电状态

```
iBMC:/->ipmcget -d powerstate
Power state   : On
Hotswap state : M4
```

4.7.4 查询和设置服务器的下电时限（shutdowntimeout）

命令功能

shutdowntimeout 命令用来查询和设置服务器的下电时限。

下电时限：执行下电操作后，iBMC 系统等待操作系统下电的时间。如果超过该时间操作系统仍未自动下电，iBMC 会强制执行下电操作。

命令格式

ipmcget [-t fru0] **-d shutdowntimeout**

ipmcset [-t fru0] **-d shutdowntimeout -v** <*time*>

参数说明

参数	参数说明	取值
time	• 表示要关闭服务器的下电时限功能。 • 表示要设置的时间。	数据类型为整型，单位为秒，取值范围为10~6000。 设置为“0”可以关闭服务器的下电时限功能。

使用指南

- “下电时限”设置为 

时，您可以使用此命令来关闭服务器的下电时限功能或设置服务器的下电时限。
- “下电时限”设置为 

时，您可以使用此命令来设置服务器的下电时限。此时，Web 界面中的“下电时限”功能状态变为 

。

使用实例

设置服务器的下电时限为 600s。

```
iBMC:/->ipmcset -d shutdowntimeout -v 600
Set shutdown timeout successfully.
```

查询服务器的下电时限。

```
iBMC:/->ipmcget -d shutdowntimeout
Graceful shutdown timeout state:   enabled
Graceful shutdown timeout value:   600 s
```

如果 Web 界面中的“下电时限”设置为“OFF”，此时可以查看到“下电时限”功能已经被禁止。

```
iBMC:/->ipmcget -d shutdowntimeout
Graceful shutdown timeout state:   disabled
```

关闭服务器的下电时限功能。

```
iBMC:/->ipmcset -d shutdowntimeout -v 0
Set shutdown timeout successfully.
```

4.7.5 查询服务器网口 MAC 地址（macaddr）

命令功能

macaddr 命令用于查询服务器上可被 OS 使用的网口 MAC 地址。

命令格式

ipmcget -d macaddr

参数说明

无

使用指南

无

使用实例

查询服务器可被 OS 使用的网口 MAC 地址。

```
iBMC:/->ipmcget -d macaddr
Type | Name | Mac Address
LOM | Port1 | 20:0b:c7:2a:e6:0b
LOM | Port2 | 20:0b:c7:2a:e6:0c
LOM | Port3 | 20:0b:c7:2a:e6:0d
LOM | Port4 | 20:0b:c7:2a:e6:0e
```

4.7.6 查询 iBMC 可用网口（ethport）

命令功能

ethport 命令用于查询服务器上可用作 iBMC 管理网口的接口信息。

命令格式

ipmcget -d ethport

参数说明

无

使用指南

无

使用实例

查询 iBMC 可用网口信息。

```
iBMC:/->ipmcget -d ethport
Type      | Name      | Port ID  | Link Status
Dedicated  | eth2      | na      | Link_Up
```

4.7.7 清除 BIOS Flash（clearcmos）

命令功能

clearcmos 命令用于清除 BIOS Flash 上的用户自定义信息。

命令格式

ipmcset -d clearcmos

参数说明

无

使用指南

无

使用实例

清除主板 BIOS Flash 信息。

```
iBMC:/->ipmcset -d clearcmos
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Clear CMOS successfully.
```

4.7.8 查询 RAID 控制器信息（ctrlinfo）

命令功能

ctrlinfo 用来查询 RAID 控制器信息。

命令格式

ipmcget -t storage -d ctrlinfo -v <*option*>

参数说明

参数	参数说明	取值
option	待查询的 RAID 控制器的 ID。	• 0～255：表示 RAID 控制器的 ID，即只查询指定 RAID 控制器的信息。 • all：列出所有 RAID 控制器的信息。

使用指南

必须满足如下条件方可执行此命令：

- 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。
- 服务器 OS 侧已安装并运行 iBMA 2.0。

使用实例

查询 ID 为 0 的 RAID 控制器的信息。

```
iBMC:/->ipmcget -t storage -d ctrlinfo -v 0
RAID Controller #0 Information
---------------------------------------------------------------------------
Controller Name                          : SAS3108
Controller Type                          : LSI SAS3108
Component Name                           : RAID Card1
Support Out-of-Band Management             : Yes

Controller Mode                          : RAID
Controller Health                        : Normal
Firmware Version                         : 4.650.00-6121
NVDATA Version                           : 3.1602.00-0002
Memory Size                              : 1024 MB
Device Interface                         : SAS 12G
SAS Address                              : 5e00000157737cd6
Minimum Strip Size Supported               : 64 KB
Maximum Strip Size Supported               : 1 MB
Controller Cache Is Pinned                 : No
Maintain PD Fail History across Reboot       : Yes
Copyback Enabled                         : No
```

```
Copyback on SMART error Enabled            : No
JBOD Enabled                               : No
DDR ECC Count                              : 0

BBU Status                                 : Present
BBU Type                                   : CVPM02
BBU Health                                 : Normal

PHY Status                                 :
   PHY #0 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #1 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #2 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #3 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #4 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #5 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #6 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #7 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
```

```
      Running Disparity Error Count : 0
----------------------------------------------------------------------
```

4.7.9 查询逻辑盘信息（ldinfo）

命令功能

ldinfo 用来查询 RAID 控制器所管理的逻辑盘的信息。

命令格式

ipmcget -t storage -d ldinfo -v <*ctrlid*> <*option*>

参数说明

参数	参数说明	取值
ctrlid	待查询逻辑盘所属 RAID 控制器的 ID。	0～255
option	待查询的逻辑盘的 ID。	• 0～255：表示逻辑盘的 ID，即只查询指定逻辑盘的信息。 • all：列出 RAID 控制器下所有逻辑盘的信息。

使用指南

必须满足如下条件方可执行此命令：

- 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。
- 服务器 OS 侧已安装并运行 iBMA 2.0。

使用实例

查询 ID 为 0 的 RAID 控制器下 ID 为 0 的逻辑盘的信息。

```
iBMC:/->ipmcget -t storage -d ldinfo -v 0 0
Logical Drive Information
----------------------------------------------------------------------
Target ID                          : 0
Name                               : example1
Type                               : RAID1
State                              : Optimal
Default Read Policy                  : Read Ahead
Default Write Policy                 : Write Back with BBU
Default Cache Policy                 : Direct IO
Current Read Policy                  : Read Ahead
Current Write Policy                 : Write Back with BBU
Current Cache Policy                 : Direct IO
```

```
Access Policy                        : Read Write
Span depth                           : 1
Number of drives per span             : 2
Strip Size                           : 256 KB
Total Size                           : 100.234 GB
Disk Cache Policy                     : Enabled
Init State                           : No Init
Consistency Checking                  : No
BGI Enabled                          : Yes
Bootable                             : No
Used for Secondary Cache              : No
SSCD Caching Enable                   : No
PD participating in LD (ID#)          : 0,1
Dedicated Hot Spare PD (ID#)          : N/A
------------------------------------------------------------------------
```

查询 ID 为 0 的 RAID 控制器下所有逻辑盘的信息。

```
iBMC:/->ipmcget -t storage -d ldinfo -v 0 all
Logical Drive Information
------------------------------------------------------------------------
Target ID                            : 0
Name                                 : example1
Type                                 : RAID1
State                                : Optimal
Default Read Policy                   : Read Ahead
Default Write Policy                  : Write Back with BBU
Default Cache Policy                  : Direct IO
Current Read Policy                   : Read Ahead
Current Write Policy                  : Write Back with BBU
Current Cache Policy                  : Direct IO
Access Policy                        : Read Write
Span depth                           : 1
Number of drives per span             : 2
Strip Size                           : 256 KB
Total Size                           : 100.234 GB
Disk Cache Policy                     : Enabled
Init State                           : No Init
Consistency Checking                  : No
BGI Enabled                          : Yes
Bootable                             : No
Used for Secondary Cache              : No
SSCD Caching Enable                   : No
PD participating in LD (ID#)          : 0,1
Dedicated Hot Spare PD (ID#)          : N/A
------------------------------------------------------------------------

Logical Drive Information
------------------------------------------------------------------------
Target ID                            : 1
Name                                 : example2
Type                                 : RAID0
State                                : Optimal
Default Read Policy                   : Read Ahead
Default Write Policy                  : Write Back with BBU
Default Cache Policy                  : Direct IO
```

```
Current Read Policy                    : Read Ahead
Current Write Policy                   : Write Back with BBU
Current Cache Policy                   : Direct IO
Access Policy                         : Read Write
Span depth                            : 1
Number of drives per span              : 5
Strip Size                            : 256 KB
Total Size                            : 1.149 TB
Disk Cache Policy                      : Enabled
Init State                            : No Init
Consistency Checking                   : No
BGI Enabled                           : Yes
Bootable                              : No
Used for Secondary Cache               : No
SSCD Caching Enable                    : No
PD participating in LD (ID#)           : 2,8,9,10,11
Dedicated Hot Spare PD (ID#)           : N/A
------------------------------------------------------------------------
```

4.7.10 查询物理盘信息（pdinfo）

命令功能

pdinfo 用来查询物理盘的信息。

命令格式

ipmcget -t storage -d pdinfo -v <*option*>

参数说明

参数	参数说明	取值
option	待查询的物理盘的 ID。	• 0～255：表示物理盘的 ID，即只查询指定物理盘的信息。 • all：列出所有物理盘的信息。

使用指南

必须满足如下条件方可执行此命令：

- 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。
- 服务器 OS 侧已安装并运行 iBMA 2.0。

使用实例

查询 ID 为 2 的物理盘的信息。

```
iBMC:/->ipmcget -t storage -d pdinfo -v 2
Physical Drive Information
---------------------------------------------------------------------------
ID                                : 2
Device Name                        : Disk2
Manufacturer                       : SEAGATE
Serial Number                      : 6XR1JS5H
Model                             : ST9600205SS
Firmware Version                    : B002
Health Status                      : Normal
Firmware State                     : UNCONFIGURED GOOD
Power State                       : Spun Up
Media Type                        : HDD
Interface Type                     : SAS
Capable Speed                      : 6.0 Gbps
Negotiated Speed                    : 6.0 Gbps
Drive Temperature                   : 34(Celsius)
Capacity                          : 557.861 GB
Hot Spare                         : None
Rebuild in Progress                 : No
Patrol Read in Progress             : No
Remnant Media Wearout               : N/A
Power-On Hours                     : 2217
SAS Address(0)                     : 5000c500473326b1
SAS Address(1)                     : 0000000000000000
Location State                     : Off

Media Error Count                   : 0
Prefail Error Count                 : 0
Other Error Count                   : 0
---------------------------------------------------------------------------
```

查询所有物理盘的信息。

```
iBMC:/->ipmcget -t storage -d pdinfo -v all
Physical Drive Information
---------------------------------------------------------------------------
ID                                : 0
Device Name                        : Disk0
Manufacturer                       : HGST
Serial Number                      : 2MV5YZEA
Model                             : HUSMM8080ASS204
Firmware Version                    : C210
Health Status                      : Minor
Firmware State                     : UNCONFIGURED GOOD
Power State                       : Spun Up
Media Type                        : SSD
Interface Type                     : SAS
Capable Speed                      : 12.0 Gbps
Negotiated Speed                    : 12.0 Gbps
Drive Temperature                   : 32(Celsius)
Capacity                          : 744.126 GB
Hot Spare                         : None
Rebuild in Progress                 : No
Patrol Read in Progress             : No
Remnant Media Wearout               : 99%
```

```
Power-On Hours                        : 5200
SAS Address(0)                        : 5000cca02b0ad99d
SAS Address(1)                        : 0000000000000000
Location State                        : Off

Media Error Count                     : 0
Prefail Error Count                   : 1
Other Error Count                     : 0
---------------------------------------------------------------------

Physical Drive Information
---------------------------------------------------------------------
ID                                  : 1
Device Name                           : Disk1
Manufacturer                          : SAMSUNG
Serial Number                         : S2HSNYAG400079
Model                                 : SAMSUNG MZ7KM480HAHP-00005
Firmware Version                      : 003Q
Health Status                         : Normal
Firmware State                        : UNCONFIGURED GOOD
Power State                           : Spun Up
Media Type                            : SSD
Interface Type                        : SATA
Capable Speed                         : 6.0 Gbps
Negotiated Speed                      : 6.0 Gbps
Drive Temperature                     : 38(Celsius)
Capacity                              : 446.103 GB
Hot Spare                             : None
Rebuild in Progress                   : No
Patrol Read in Progress               : No
Remnant Media Wearout                 : 99%
Power-On Hours                        : 11750
SAS Address(0)                        : 4433221101000000
SAS Address(1)                        : 0000000000000000
Location State                        : Off

Media Error Count                     : 0
Prefail Error Count                   : 0
Other Error Count                     : 0
---------------------------------------------------------------------

Physical Drive Information
---------------------------------------------------------------------
ID                                  : 2
Device Name                           : Disk2
Manufacturer                          : SEAGATE
Serial Number                         : 6XR1JS5H
Model                                 : ST9600205SS
Firmware Version                      : B002
Health Status                         : Normal
Firmware State                        : UNCONFIGURED GOOD
Power State                           : Spun Up
Media Type                            : HDD
Interface Type                        : SAS
Capable Speed                         : 6.0 Gbps
```

```
Negotiated Speed                    : 6.0 Gbps
Drive Temperature                   : 34(Celsius)
Capacity                           : 557.861 GB
Hot Spare                          : None
Rebuild in Progress                 : No
Patrol Read in Progress             : No
Remnant Media Wearout               : N/A
Power-On Hours                     : 2217
SAS Address(0)                     : 5000c500473326b1
SAS Address(1)                     : 0000000000000000
Location State                     : Off

Media Error Count                   : 0
Prefail Error Count                 : 0
Other Error Count                   : 0
---------------------------------------------------------------------------

Physical Drive Information
---------------------------------------------------------------------------
ID                                 : 3
Device Name                         : Disk3
Manufacturer                        : SEAGATE
Serial Number                       : S0M3326E
Model                              : ST600MM0006
Firmware Version                    : B001
Health Status                      : Normal
Firmware State                     : UNCONFIGURED GOOD
Power State                        : Spun Up
Media Type                         : HDD
Interface Type                      : SAS
Capable Speed                      : 6.0 Gbps
Negotiated Speed                    : 6.0 Gbps
Drive Temperature                   : 34(Celsius)
Capacity                           : 557.861 GB
Hot Spare                          : None
Rebuild in Progress                 : No
Patrol Read in Progress             : No
Remnant Media Wearout               : N/A
Power-On Hours                     : 519
SAS Address(0)                     : 5000c50076d10609
SAS Address(1)                     : 0000000000000000
Location State                     : Off

Media Error Count                   : 0
Prefail Error Count                 : 0
Other Error Count                   : 0
---------------------------------------------------------------------------

Physical Drive Information
---------------------------------------------------------------------------
ID                                 : 4
Device Name                         : Disk4
Manufacturer                        : SEAGATE
Serial Number                       : S0M31J5T
Model                              : ST600MM0006
```

```
Firmware Version                     : B001
Health Status                        : Normal
Firmware State                       : UNCONFIGURED GOOD
Power State                          : Spun Up
Media Type                           : HDD
Interface Type                       : SAS
Capable Speed                        : 6.0 Gbps
Negotiated Speed                     : 6.0 Gbps
Drive Temperature                    : 34(Celsius)
Capacity                             : 557.861 GB
Hot Spare                            : None
Rebuild in Progress                  : No
Patrol Read in Progress              : No
Remnant Media Wearout                : N/A
Power-On Hours                       : 519
SAS Address(0)                       : 5000c50076b1aa2d
SAS Address(1)                       : 0000000000000000
Location State                       : Off

Media Error Count                    : 0
Prefail Error Count                  : 0
Other Error Count                    : 0
------------------------------------------------------------------------
```

4.7.11 查询磁盘组信息（arrayinfo）

命令功能

arrayinfo 用来查询磁盘组的信息。

命令格式

ipmcget -t storage -d arrayinfo -v <*control_id*> <*option*>

参数说明

参数	参数说明	取值
control_id	磁盘组所在控制器的 ID	0～255
option	待查询的磁盘组的 ID。	• 0～255：表示磁盘组的 ID，即只查询指定磁盘组的信息。 • all：列出所有磁盘组的信息。

使用指南

必须满足如下条件方可执行此命令：

- 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。

- 服务器 OS 侧已安装并运行 iBMA 2.0。

使用实例

查询 ID 为 0 的控制器上 ID 为 1 的磁盘组的信息。

```
iBMC:/->ipmcget -t storage -d arrayinfo -v 0 1
Disk Array Information
---------------------------------------------------------------------------
Array ID                              : 1
Used Space                            : 800.000 GB
Free Space                            : 716.655 GB
Free Blocks Space                       : (0)500.000 GB
                                      : (1)216.655 GB
Logcial Drive(s) ID                     : 1,5
Physical Drive(s) ID                    : 1,2
---------------------------------------------------------------------------
```

查询 ID 为 0 的控制器上所有磁盘组的信息。

```
iBMC:/->ipmcget -t storage -d arrayinfo -v 0 all
Disk Array Information
---------------------------------------------------------------------------
Array ID                              : 0
Used Space                            : 110.000 GB
Free Space                            : 447.861 GB
Free Blocks Space                       : (0)30.000 GB
                                      : (1)417.861 GB
Logcial Drive(s) ID                     : 0,4
Physical Drive(s) ID                    : 0
---------------------------------------------------------------------------
Disk Array Information
---------------------------------------------------------------------------
Array ID                              : 1
Used Space                            : 800.000 GB
Free Space                            : 716.655 GB
Free Blocks Space                       : (0)500.000 GB
                                      : (1)216.655 GB
Logcial Drive(s) ID                     : 1,5
Physical Drive(s) ID                    : 1,2
---------------------------------------------------------------------------
Disk Array Information
---------------------------------------------------------------------------
Array ID                              : 2
Used Space                            : 300.000 GB
Free Space                            : 816.655 GB
Free Blocks Space                       : (0)400.000 GB
                                      : (1)416.655 GB
Logcial Drive(s) ID                     : 2,6
Physical Drive(s) ID                    : 3
---------------------------------------------------------------------------
```

4.7.12 创建逻辑盘（createld）

命令功能

createld 用于使用空闲物理盘创建虚拟盘。

命令格式

ipmcset -t storage -d createld -v <*control_id*> **-rl** <*raidlevel*> **-pd** <*pd_id*> **[-cachecade] [-sc** <*span_num*>**] [-name** <*ldname*>**] [-size** <*capative*>{m|g|t} **] [-ss** <*stripesize*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-dcp** <*dcpvalue*>**] [-init** <*initmode*>**]**

参数说明

参数	参数说明	取值
control_id	RAID 控制器的 ID	0～255
raidlevel	逻辑盘的 RAID 级别	• r0：RAID 0 • r1：RAID 1 • r5：RAID 5 • r6：RAID 6 • r10：RAID 10 • r50：RAID 50 • r60：RAID 60 **说明** 当命令行包含“-cachecade”时，此参数只能配置为“r0”和“r1”。
pd_id	逻辑盘的成员盘列表	物理盘的 ID，用“,”分隔。 例如：0,1,2 **说明** 当命令行包含“-cachecade”时，所选成员盘必须为 SSD。
span_num	逻辑盘的子组个数	• 创建 RAID 0/1/5/6 时不需配置此参数。 • 创建 RAID 10/50/60 是可设置此参数，默认为 2。 **说明** 当命令行包含“-cachecade”时，此参数无效。
ldname	逻辑盘名称	最大长度为 15 个字符的字符串。
capative	逻辑盘容量	逻辑盘容量的单位可以为： • m：MB • g：GB

参数	参数说明	取值
		• t：TB 说明 • 当命令行包含“-cachecade”时，此参数无效。 • 当命令中不包含“-cachecade”且不设置此参数时，系统根据成员盘所能提供的最大容量来设置逻辑盘的容量。
stripesize	逻辑盘条带大小	可选的条带大小包括： • 64K • 128K • 256K • 512K • 1M 说明 • 当命令行包含“-cachecade”时，此参数无效，逻辑盘的默认条带大小为 1M。 • 当命令中不包含“-cachecade”且不配置此参数时，逻辑盘的默认条带大小为 256K。
rpvalue	逻辑盘的读策略	• ra：设置逻辑盘读策略为“Read Ahead”。 • nra：设置逻辑盘读策略为“No Read Ahead”。 说明 • 当命令行包含“-cachecade”时，此参数无效，逻辑盘的默认读策略为 nra。 • 当命令中不包含“-cachecade”且不配置此参数时，逻辑盘的默认读策略为 ra。
wpvalue	逻辑盘的写策略	• wt：设置逻辑盘写策略为“Write Through”。 • wb：设置逻辑盘写策略为“Write Back”。 • wbwithbbu：设置逻辑盘写策略为“Write Back with BBU”。 默认为“wbwithbbu”。
iopvalue	逻辑盘的 IO 策略	• cio：设置逻辑盘 IO 策略为“Cached IO”。 • dio：设置逻辑盘 IO 策略为“Direct IO”。 默认为“dio”。 说明 当命令行包含“-cachecade”时，此参数无效。
apvalue	逻辑盘的访问策略	• rw：设置逻辑盘的访问策略为可读写。 • ro：设置逻辑盘的访问策略为只读。 • blocked：设置逻辑盘的访问策略为隐藏。

参数	参数说明	取值
		默认为“rw”。 说明 当命令行包含“-cachecade”时，此参数无效。
dcpvalue	逻辑盘的磁盘缓存策略	• enabled：允许逻辑盘使用 cache。 • disabled：禁止逻辑盘使用 cache。 • default：使用默认策略，根据成员盘自身的缓存策略决定。 说明 • 当命令行包含“-cachecade”时，此参数无效，逻辑盘的默认磁盘缓存策略为“default”。 • 当命令中不包含“-cachecade”且不配置此参数时，逻辑盘的默认磁盘缓存策略为“enabled”。
initmode	逻辑盘的初始化方式	• no：不初始化。 • quick：快速初始化。 • full：全量初始化。 默认为“no”。 说明 当命令行包含“-cachecade”时，此参数无效。

使用指南

命令行中包含“-cachecade”时，表示创建的逻辑盘为 CacheCade 逻辑盘。

必须满足如下条件方可执行此命令：

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。

使用实例

在 ID 为 0 的 RAID 控制器下创建普通逻辑盘。

```
iBMC:/-> ipmcset -t storage -d createld -v 0 -rl r1 -pd 0,1 -name example -size
100g -ss 512k -rp ra -wp wb -ap rw -iop cio -dcp enabled -init quick
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

在 ID 为 0 的 RAID 控制器下创建 Cachecade 逻辑盘。

```
iBMC:/-> ipmcset -t storage -d createld -v 0 -rl r0 -pd 0,1,2 -name cachecade -
cachecade -wp wb
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7.13 添加逻辑盘（addld）

命令功能

addld 用于在已有逻辑盘的磁盘组上添加新的逻辑盘。

命令格式

ipmcset -t storage -d addld -v <*control_id*> **-array** <*arrayid*> **[-name** <*ldname*>**] [-size** <*capative*>{m|g|t} **] [-ss** <*stripesize*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-dcp** <*dcpvalue*>**] [-init** <*initmode*>**] [-block <***blockid***>]**

参数说明

参数	参数说明	取值
control_id	RAID 控制器的 ID	0～255
arrayid	待添加逻辑盘的磁盘组的 ID	0～255
ldname	逻辑盘名称	最大长度为 15 个字符的字符串。
capative	逻辑盘容量	逻辑盘容量的单位可以为： • m：MB • g：GB • t：TB 说明 当未设置此参数时，系统根据磁盘组所能提供的最大容量来设置该逻辑盘的容量。
stripesize	逻辑盘条带大小	可选的条带大小包括： • 64K • 128K • 256K • 512K • 1M 单位为字节，默认为“256K”。
rpvalue	逻辑盘的读策略	• ra：设置逻辑盘读策略为“Read Ahead”。 • nra：设置逻辑盘读策略为“No Read Ahead”。 默认为“ra”。
wpvalue	逻辑盘的写策略	• wt：设置逻辑盘写策略为“Write Through”。 • wb：设置逻辑盘写策略为“Write Back”。 • wbwithbbu：设置逻辑盘写策略为“Write

参数	参数说明	取值
		Back with BBU”。 默认为“wbwithbbu”。
iopvalue	逻辑盘的 IO 策略	• cio：设置逻辑盘 IO 策略为“Cached IO”。 • dio：设置逻辑盘 IO 策略为“Direct IO”。 默认为“dio”。
apvalue	逻辑盘的访问策略	• rw：设置逻辑盘的访问策略为可读写。 • ro：设置逻辑盘的访问策略为只读。 • blocked：设置逻辑盘的访问策略为隐藏。 默认为“rw”。
dcpvalue	逻辑盘的磁盘缓存策略	• enabled：允许逻辑盘使用 cache。 • disabled：禁止逻辑盘使用 cache。 • default：使用默认策略，根据成员盘自身的缓存策略决定。 默认为“enabled”。
initmode	逻辑盘的初始化方式	• no：不初始化。 • quick：快速初始化。 • full：全量初始化。 默认为“no”。
blockid	待添加逻辑盘的磁盘组的空闲块 ID	0～32

使用指南

必须满足如下条件方可执行此命令：

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。

使用实例

在 ID 为 0 的 RAID 控制器下，在磁盘组 1 上添加逻辑盘。

```
iBMC:/-> ipmcset -t storage -d addld -v 0 -array 1 -name example -size 500g -ss
256k -rp ra -wp wb -ap rw -iop cio -dcp enabled -init quick -block 2
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7.14 删除逻辑盘（deleteld）

命令功能

deleteld 用于删除 RAID 卡管理的逻辑盘。

命令格式

ipmcset -t storage -d deleteld -v <*control_id*> <*ldid*>

参数说明

参数	参数说明	取值
control_id	RAID 控制器的 ID	0～255
ldid	待删除的逻辑盘的 ID	0～255

使用指南

必须满足如下条件方可执行此命令：

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。

使用实例

删除 ID 为 0 的 RAID 控制器的逻辑盘 1。

```
iBMC:/-> ipmcset -t storage -d deleteld -v 0 0
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7.15 修改逻辑盘属性（ldconfig）

命令功能

ldconfig 用于修改逻辑盘的属性。

命令格式

ipmcset -t storage -d ldconfig -v <*control_id*> <*ldid*> <**[-name** <*ldname*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-dcp <***dcpvalue*>**] [-bgi** <*bgistate*>**] [-boot] [-sscd** <*sscdstate*>**]**

参数说明

参数	参数说明	取值

参数	参数说明	取值
control_id	RAID 控制器的 ID	0～255
ldid	逻辑盘的 ID	0～255
ldname	逻辑盘名称	最大长度为 15 个字符的字符串。
rpvalue	逻辑盘的读策略	• ra：设置逻辑盘读策略为“Read Ahead”。 • nra：设置逻辑盘读策略为“No Read Ahead”。 **说明** 当逻辑盘为 CacheCade 逻辑盘时，不支持设置此参数。
wpvalue	逻辑盘的写策略	• wt：设置逻辑盘写策略为“Write Through”。 • wb：设置逻辑盘写策略为“Write Back”。 • wbwithbbu：设置逻辑盘写策略为“Write Back with BBU”。
iopvalue	逻辑盘的 IO 策略	• cio：设置逻辑盘 IO 策略为“Cached IO”。 • dio：设置逻辑盘 IO 策略为“Direct IO”。 **说明** 当逻辑盘为 CacheCade 逻辑盘时，不支持设置此参数。
apvalue	逻辑盘的访问策略	• rw：设置逻辑盘的访问策略为可读写。 • ro：设置逻辑盘的访问策略为只读。 • blocked：设置逻辑盘的访问策略为隐藏。 **说明** 当逻辑盘为 CacheCade 逻辑盘时，不支持设置此参数。
dcpvalue	逻辑盘的磁盘缓存策略	• enabled：允许逻辑盘使用 cache。 • disabled：禁止逻辑盘使用 cache。 • default：使用默认策略，根据成员盘自身的缓存策略决定。 **说明** 当逻辑盘为 CacheCade 逻辑盘时，不支持设置此参数。
bgistate	逻辑盘的 BGI 使能状态	• enabled：开启逻辑盘的后台初始化功能。 • disabled：关闭逻辑盘的后台初始化功能。 **说明** 当逻辑盘为 CacheCade 逻辑盘时，不支持设置此参数。

参数	参数说明	取值
sscdstate	逻辑盘是否开启 SSD Caching 功能（即是否使用 CacheCade 逻辑盘作为缓存）	• enabled：开启逻辑盘的 SSD Caching 功能。 • disabled：关闭逻辑盘的 SSD Caching 功能。 说明 • 当前 RAID 控制卡上必须存在可用的 CacheCade 逻辑盘。 • 当逻辑盘为 CacheCade 逻辑盘时，不支持设置此参数。

使用指南

命令行中包含“-boot”时，表示设置此逻辑盘为启动盘。

必须满足如下条件方可执行此命令：

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。

使用实例

修改 ID 为 0 的 RAID 控制器下的 ID 为 1 的逻辑盘的属性。

```
iBMC:/-> ipmcset -t storage -d ldconfig -v 0 1 -name example -rp ra -wp wb -ap rw -
iop cio -dcp enabled -bgi enabled -boot
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7.16 修改 RAID 控制器属性（ctrlconfig）

命令功能

ctrlconfig 用于修改 RAID 控制器的属性。

命令格式

ipmcset -t storage -d ctrlconfig -v <*control_id*> <**[-cb** <*cbstate*>**] [-smartercb** <*smartercbstate*>**] [-jbod** <*jbodstate*>**] [-restore]**

参数说明

参数	参数说明	取值
control_id	RAID 控制器的 ID	0～255
cbstate	RAID 控制器的 Copyback 功能使能状	• enabled • disabled

参数	参数说明	取值
	态	
smartercbstate	RAID 控制器在成员盘出现 SMART 错误时 Copyback 功能使能状态	• enabled • disabled
jbodstate	RAID 控制器 JBOD 模式使能状态	• enabled • disabled

使用指南

命令行中包含“-restore”时，表示将 RAID 控制器的属性恢复为默认值。

必须满足如下条件方可执行此命令：

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。

使用实例

设置 ID 为 0 的 RAID 控制器的 Copyback 使能状态。

```
iBMC:/-> ipmcset -t storage -d ctrlconfig -v 0 -cb enabled
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7.17 修改物理盘属性（pdconfig）

命令功能

pdconfig 用于修改 RAID 控制器所管理的物理盘的属性。

命令格式

ipmcset -t storage -d pdconfig -v <*pdid*> **[-state** <*pdstate*>**] [-hotspare** <*hotsparetype*> **[-ld** <*ldid*>**]] [-locate** <*locatestate*>] **[-cryptoerase]**

参数说明

参数	参数说明	取值
pdid	物理硬盘的 ID	0～255
pdstate	物理盘的运行状态	• online：在线 • offline：离线 • ug：空闲

参数	参数说明	取值
		• jbod：直通
hotsparetype	物理盘的热备状态	• none：取消热备 • global：全局热备 • dedicated：局部热备
ldid	逻辑盘 ID。 当物理盘热备状态为“dedicated”时，需同时设置关联的逻辑盘。	0～255
locatestate	物理盘定位指示灯状态	• start：定位指示灯闪烁 • stop：定位指示灯熄灭

使用指南

命令行中包含**-cryptoerase** 时，表示将加密盘的数据擦除。

必须满足如下条件方可执行此命令：

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。

使用实例

擦除 ID 为 1 的加密物理盘数据。

```
iBMC:/-> ipmcset -t storage -d pdconfig -v 1 -cryptoerase
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
The operation may take a few seconds, Please wait...
Cryptographically erase Physical Drive successfully.
```

4.7.18 查询和设置 RAID 扣卡日志记录功能（raidcom）

命令功能

raidcom 命令用于查询和设置要启用日志记录功能的 RAID 扣卡信息。指定了 RAID 扣卡后，可通过一键信息收集功能获取该 RAID 扣卡的日志，日志文件存放路径为“dump_info\LogDump\storage”。

命令格式

ipmcget -t maintenance -d raidcom

ipmcset -t maintenance -d raidcom -v <*value*>

参数说明

参数	参数说明	取值
<*value*>	待记录日志的 RAID 扣卡编号。	不同服务器上 RAID 扣卡的编号不同，请通过命令行自带的帮助信息获取参数取值范围。

使用指南

LSI SAS3008 IT RAID 扣卡、LSI SAS3008 IR RAID 扣卡、Avago 3416 IT RAID 扣卡不支持此命令。

使用实例

查询当前已启用日志记录功能的 RAID 扣卡。

```
iBMC:/->ipmcget -t maintenance -d raidcom
Current RAID com connected:
Com Channel    :  1
Device Name    :  RAID Card1
```

开启“RAID Card1”的日志记录功能。

```
iBMC:/->ipmcset -t maintenance -d raidcom -v
Usage: ipmcset -t maintenance -d raidcom -v <value>
Values are:
   1    RAID Card1
iBMC:/->ipmcset -t maintenance -d raidcom -v 1
Set RAID com channel to RAID Card1 successfully.
```

4.8 系统命令

4.8.1 查询系统名称（systemname）

命令功能

systemname 命令用来查询系统名称。

命令格式

ipmcget -t smbios -d systemname

参数说明

无

使用指南

无

使用实例

查询服务器系统名称。

```
iBMC:/->ipmcget -t smbios -d systemname
System name is: xxxxx
```

4.8.2 设置 iBMC 时区（timezone）

命令功能

timezone 命令用来设置 iBMC 时区。

命令格式

ipmcset -d timezone -v <*timezone*>

参数说明

参数	参数说明	取值
timezone	时区。	• 时间偏移 取值范围： – [-12:00~+14:00]，例如+8:00、-4:30。 – [UTC-12:00~UTC+14:00]，例如 UTC+8:00、UTC-4:30。 – [GMT-12:00~GMT+14:00]，例如 GMT+8:00、GMT-4:30。 • 时区名称 取值范围：全球时区地名，例如 Asia/Shanghai、America/Swift_Current。 • 默认值：UTC **说明** 当输入的是时间偏移中不带时间标准名称时，表示设置的是 UTC 时间。当输入的是时区名称时，表示设置的是

参数	参数说明	取值
		UTC 时间。

使用指南

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。

使用实例

设置 iBMC 时区为+8:00。

```
iBMC:/->ipmcset -d timezone -v +8:00
Set time zone successfully.
```

设置 iBMC 时区为 UTC+8:00。

```
iBMC:/->ipmcset -d timezone -v UTC+8:00
Set time zone successfully.
```

查询 iBMC 时间。

```
iBMC:/->ipmcget -d time
2014-06-28 Saturday 16:43:51 UTC+08:00
```

设置 iBMC 时区为 Asia/Shanghai。

```
iBMC:/->ipmcset -d timezone -v Asia/Shanghai
Set time zone successfully.
```

查询 iBMC 时间。

```
iBMC:/->ipmcget -d time
2017-09-06 Wednesday 16:43:51 Asia/Shanghai(UTC+08:00)
```

4.8.3 查询 iBMC 时间（time）

命令功能

time 命令用来查询 iBMC 时间。

命令格式

ipmcget -d time

参数说明

无

使用指南

无

使用实例

查询 iBMC 时间。

```
iBMC:/->ipmcget -d time
2014-06-28 Saturday 16:43:51 UTC+08:00
```

或

```
iBMC:/->ipmcget -d time
2017-09-06 Wednesday 16:43:51 Asia/Shanghai(UTC+08:00)
```

4.8.4 查询设备的版本信息（version）

命令功能

version 命令用来查询设备的版本信息。

命令格式

ipmcget -d version

参数说明

无

使用指南

无

使用实例

查询设备的版本信息。

```
iBMC:/->ipmcget -d version
------------------- iBMC INFO --------------------
IPMC             CPU:          Hi1711
IPMI          Version:          2.0
CPLD          Version:          (U151)0.15
Active iBMC   Version:           (U68)3.01.01.00
Active iBMC     Build:          005
Active iBMC     Built:         18:43:56 Mar 6 2020
Backup iBMC   Version:          3.01.01.00
Available iBMC Version:         3.01.01.00
Available iBMC Build:           005
SDK           Version:         5.0.80.0
SDK             Built:          21:11:10 Feb 29 2020
Active Uboot   Version:           5.0.80.0 (21:21:56 Feb 29 2020)
Backup Uboot   Version:           5.0.80.0 (21:21:56 Feb 29 2020)
Active Secure Bootloader Version: 5.0.80.0 (21:21:55 Feb 29 2020)
Backup Secure Bootloader Version: 5.0.80.0 (21:21:55 Feb 29 2020)
Active Secure Firmware Version: 5.0.80.0 (21:21:55 Feb 29 2020)
Backup Secure Firmware Version: 5.0.80.0 (21:21:55 Feb 29 2020)
----------------- Product INFO -----------------
```

```
Product           ID:         0x0007
Product         Name:         XXXXXX
BIOS         Version:         (U75)1.13
-------------- Mother Board INFO ---------------
Mainboard     BoardID:         0x0005
Mainboard        PCB:         .A
----------------- NIC INFO ----------------
NIC 1 (TM280) BoardID: 0x0067
NIC 1 (TM280) PCB: .A
--------------- Riser Card INFO ----------------
Riser1      BoardName:         BC82PRUN
Riser1      BoardID:           0x0093
Riser1      PCB:               .A
Riser2      BoardName:         BC82PRUN
Riser2      BoardID:           0x0093
Riser2      PCB:               .A
-------------- HDD Backplane INFO --------------
Disk BP0        BoardName:     BC82THBB
Disk BP0        BoardID:       0x004a
Disk BP0        PCB:           .A
Disk BP0        CPLD Version:  (U31)0.05
---------------- IO Board INFO ----------------
IOBoard0        ProductName:    BC82IOEA
IOBoard0        BoardID:        0x0063
IOBoard0        PCB:            .A
-------------------- PSU INFO --------------------
PS1            Version:          DC:113 PFC:113
PS2            Version:          DC:111 PFC:111
------------- Security Module INFO -------------
Specification Type:     TPM/TCM
Specification Version:   N/A
Manufacturer Name:      N/A
Manufacturer Version:    N/A
```

4.8.5 查询 FRU 信息（fruinfo）

命令功能

fruinfo 命令用于查询除电源模块之外的其它 FRU 的信息，包括主板、RAID 卡、Mezz 卡、硬盘背板、PCIe Rsier 卡、GPU 载板等。

命令格式

ipmcget [-t fru0] **-d fruinfo**

参数说明

无

使用指南

无

使用实例

查询 FRU 信息。

```
iBMC:/->ipmcget -d fruinfo
FRU Device Description : Builtin FRU Device (ID 0, Mainboard)
 Board Mfg. Date      : 2014/04/03 Thu 16:12:00
 Board Manufacturer   :
 Board Product Name   : board
 Board Serial Number  : 022HLV10E3000003
 Board FRU File ID    : 1.17
 Product Manufacturer  :
 Product Name         : pname
 Product Serial Number : serialnumber
 Product FRU File ID   : 1.17
```

4.8.6 查询系统的健康状态（health）

命令功能

health 命令用来查询系统的健康状态。

命令格式

ipmcget [-t fru0] **-d health**

参数说明

无

使用指南

无

使用实例

查询系统的健康状态。

```
iBMC:/->ipmcget -d health
System in health state.
```

4.8.7 查询系统的健康事件信息（healthevents）

命令功能

healthevents 命令用来查询系统的健康事件信息。

命令格式

ipmcget [-t fru0] **-d healthevents**

参数说明

无

使用指南

无

使用实例

查询系统的健康事件信息。

```
iBMC:/->ipmcget -d healthevents
Event Num  | Event Time          | Alarm Level  | Event Code   | Event Description
1          | 2016-10-17 06:27:14  | Minor       | 0x01000021   | Failed to obtain data
of the CPU 1 DIMM VDDQ2 voltage.
2          | 2016-10-17 10:24:43  | Critical    | 0x01000015   |  DIMM020 DIMM
configuration error or training failed.
3          | 2016-10-17 10:24:43  | Major       | 0x01000017   |  DIMM012 DIMM
triggered an uncorrectable error, .
4          | 2016-10-17 10:24:43  | Critical    | 0x01000015   |  DIMM001 DIMM
configuration error or training failed.
5          | 2016-10-17 08:47:27  | Major       | 0x03000009   | [Mock]PSU 1 failure.
6          | 2016-10-17 07:40:57  | Minor       | 0x0D000003   | The NIC 1 temperature
(150 degrees C) exceeds the overtemperature threshold (100 degrees C).
7          | 2016-10-17 07:04:47  | Major       | 0x2100000B   | Data rebuild failed
at SD card 2.
8          | 2016-10-17 06:33:21  | Major       | 0x2C000029   | The OS is forcibly
powered off and on due to the watchdog timeout.
```

4.8.8 查询服务器的设备序列号（serialnumber）

命令功能

serialnumber 命令用来查询服务器的设备序列号。

命令格式

ipmcget [-t smbios] **-d serialnumber**

参数说明

无

使用指南

无

使用实例

查询服务器的设备序列号。

```
iBMC:/->ipmcget -d serialnumber
System SN is:44444444444444444444
```

4.8.9 查询和清除系统 SEL 信息（sel）

命令功能

sel 命令用来查询和清除系统 SEL 信息。

命令格式

ipmcget -d sel -v <*option*> [*sel_id*]

ipmcset [-t fru0] **-d sel -v clear**

参数说明

参数	参数说明	取值
option	要进行的操作	• list：列出所有系统 SEL 记录。 • info：查询 SEL 记录的使用情况。 • suggestion：查询指定 SEL 的处理建议。 **说明** 系统最多可保留 4000 条日志信息，当产生第 4001 条日志时，系统自动删除最旧的 2000 条日志信息以释放空间。新的事件 ID 从 2001 开始。
sel_id	要获取处理建议的 SEL 的 ID。	仅当执行“suggestion”操作时，包含此参数。 可从“list”操作的回显中获取。
clear	清除所有 SEL 信息。 **说明** 清除 SEL 后无法恢复。	-

使用指南

无

使用实例

查询 SEL 记录的使用情况。

```
iBMC:/->ipmcget -d sel -v info
SEL Information
Version            :1.0.0
Current Event Number  :  147
Max Event Number      :  4000
```

查询 ID 为 146 的 SEL 的处理建议。

```
iBMC:/->ipmcget -d sel -v suggestion 146
ID               :  146
Generation Time    :  2016-10-26 03:26:23
Severity          :  Minor
Event Code         :  0x12000013
Status            :  Asserted
Event Description   :  [Mock]Failed to obtain data of the air inlet temperature
Suggestion         :  1. Restart the iBMC.
                      2. Remove and reconnect power cables or remove and reinstall the
board in the chassis.
```

清除系统 SEL 信息。

```
iBMC:/->ipmcset -t fru0 -d sel -v clear
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
Clear SEL records successfully.
```

4.8.10 查询系统操作日志（operatelog）

命令功能

operatelog 命令用来查询系统操作日志。

命令格式

ipmcget -d operatelog

参数说明

无

使用指南

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。

使用实例

查询系统操作日志。

```
iBMC:/->ipmcget -d operatelog
```

```
2018-06-19 15:42:08 MAINT,Administrator@192.168.124.103:62541,cooling app,Set debug
log output type to (local) successfully
2018-06-19 15:41:58 MAINT,Administrator@192.168.124.103:62541,cooling_app,Set debug
log output level to (debug) successfully
2018-06-19 15:41:52 MAINT,Administrator@192.168.124.103:62541,cooling_app,Set debug
log output level failed
2018-06-19 15:41:48 MAINT,Administrator@192.168.124.103:62541,cooling_app,Attach
(cooling_app) successfully
2018-06-19 15:39:25 IPMI,N/A@HOST,BMC,Set FRU0 MAC1 address(00:00:00:00:00:00)
successfully
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set bios setting file changed flag to (no
changed) successfully
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set PCIePortDisable3 from [Disabled] to
[Disabled] success,EvtCode:21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set PStateDomain from [One] to [One]
success,EvtCode: 21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set TurboMode from [Enabled] to [Enabled]
success,EvtCode: 21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set CustomPowerPolicy from [Efficiency] to
[Efficiency] success,EvtCode:21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set QuietBoot from [Disabled] to [Disabled]
success,EvtCode: 21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set QuickBoot from [Enabled] to [Enabled]
success,EvtCode: 21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set BootType from [LegacyBoot] to
[LegacyBoot] success,EvtCode:21700BE0
2018-06-19 15:39:10 IPMI,N/A@HOST,BIOS,Set boot flags to (RAW:00-00-00-00-00)
successfully
2018-06-19 15:38:35 IPMI,N/A@HOST,BMC,Set watchdog timer to (RAW:02-00-00-00-e0-2e)
successfully
2018-06-19 15:38:30 IPMI,N/A@HOST,BMC,Set watchdog timer to (RAW:02-00-00-00-e0-2e)
successfully Input 'q' to quit:

2020-09-25 23:12:09 Redfish,Administrator@192.168.1.1,User,Modify
user(wsUqLPNmYsGYOyd|user3) privilege to (Operator) successfully
2020-09-25 23:12:09 Redfish,Administrator@192.168.1.1,User,Enable
user(wsUqLPNmYsGYOyd|user3) successfully
2020-09-25 23:12:08 Redfish,Administrator@192.168.1.1,User,Modify
user(wsUqLPNmYsGYOyd|user3) password successfully
2020-09-25 23:12:08 Redfish,Administrator@192.168.1.1,User,Add user3's username
(wsUqLPNmYsGYOyd) successfully
2020-09-25 23:12:07 Redfish,Administrator@192.168.1.1,User,Set password minimum
time to (1) days successfully
2020-09-25 22:54:49 Redfish,Administrator@192.168.1.1,sensor alarm,Set syslog auth
type: mutual authentication successfully
2020-09-25 22:54:48 Redfish,Administrator@192.168.1.1,User,Delete user3's username
(DXpUpMqcHHvBodK) successfully
2020-09-25 22:54:46 Redfish,Administrator@192.168.1.1,sensor alarm,Set SNMP trap
version to (V1) successfully
2020-09-25 22:54:45 Redfish,Administrator@192.168.1.1,User,Remove exclude user
successfully
2020-09-25 22:54:42 Redfish,Administrator@192.168.1.1,User,Kick
user(username:Administrator|client type:CLI|client IP:192.168.1.1) out successfully
2020-09-25 22:54:42 Redfish,Administrator@192.168.1.1,User,Kick
user(username:Administrator|client type:GUI|client IP:192.168.1.1) out successfully
```

```
2020-09-25 22:54:42 Redfish,Administrator@192.168.1.1,User,Kick
user(username:DXpUpMqcHHvBodK|client type:GUI|client IP:192.168.1.1) out
successfully
2020-09-25 22:54:41 WEB,DXpUpMqcHHvBodK@192.168.1.1,VNC,Set VNC password
successfully
2020-09-25 22:54:39
WEB,DXpUpMqcHHvBodK@192.168.1.1,User,DXpUpMqcHHvBodK(192.168.1.1) login
successfully over the WebUI
2020-09-25 22:54:20 Redfish,Administrator@192.168.1.1,User,Set
user(DXpUpMqcHHvBodK|user3) userrole to (CustomRole1) successfully
2020-09-25 22:54:20 Redfish,Administrator@192.168.1.1,User,Modify
user(DXpUpMqcHHvBodK|user3) privilege to (CustomRole1) successfully
2020-09-25 22:54:19 Redfish,Administrator@192.168.1.1,User,Enable
user(DXpUpMqcHHvBodK|user3) successfully
2020-09-25 22:54:18 Redfish,Administrator@192.168.1.1,User,Modify
user(DXpUpMqcHHvBodK|user3) password successfully
2020-09-25 22:54:18 Redfish,Administrator@192.168.1.1,User,Add user3's username
(DXpUpMqcHHvBodK) successfully
2020-09-25 22:54:17 Redfish,Administrator@192.168.1.1,User,Disable
userrole(CustomRole1) security management state successfully
Input 'q' to quit:
```

4.8.11 下载系统串口数据（systemcom）

命令功能

systemcom 命令用来下载系统串口数据。

命令格式

ipmcget -d systemcom

参数说明

无

使用指南

需要在 iBMC Web 管理系统的“系统日志”界面开启系统串口数据下载功能。

执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/tmp”路径下的串口数据文件（如“systemcom.tar”）下载到客户端（例如 PC）。

使用实例

下载系统串口数据。

```
iBMC:/->ipmcget -d systemcom
Download System Com data to /tmp/systemcom.tar successfully.
```

4.8.12 下载黑匣子数据（blackbox）

命令功能

blackbox 命令用来下载黑匣子数据。

命令格式

ipmcget -d blackbox

参数说明

无

使用指南

- 黑匣子用于记录操作系统崩溃时的内核信息。
- 黑匣子功能必须在服务器安装黑匣子故障监控软件后才可以使用。
- 需要在 iBMC Web 管理系统的“维护诊断 > 系统日志”界面开启黑匣子功能。更多关于黑匣子的信息请参见 3.5.4 系统日志。
- 执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/tmp”路径下的“blackbox.tar”文件下载到客户端（例如 PC）。

使用实例

#下载黑匣子数据。

```
iBMC:/->ipmcget -d blackbox
Downloading...
100%
Download Black Box data to /tmp/blackbox.tar successfully.
```

4.8.13 下载 BIOS（download）

命令功能

maintenance -d download 命令用于下载 BIOS 文件“bios.bin”到“/tmp”目录下。

“bios.bin”文件可用于定位 OS 启动异常和 BIOS 异常等问题。

命令格式

ipmcset -t maintenance -d download -v <*option*>

参数说明

参数	参数说明	取值
option	表示是否下载 BIOS 到“/tmp”目录下。	“1”：表示下载 BIOS 到“/tmp”目录下。

参数	参数说明	取值
		说明 目前只支持 *option* 参数为“1”。

使用指南

当系统出现异常时，请下载“bios.bin”文件并联系技术支持工程师处理。

若下载 BIOS 出现超时，请在下载 BIOS 前执行**禁止 CLP 超时（notimeout）**命令，执行操作参见 5.11 禁止 CLP 超时（notimeout）。

执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/tmp”路径下的文件（如“bios.bin”）下载到客户端（例如 PC）。

使用实例

下载 BIOS 文件“bios.bin”到“/tmp”目录下。

```
iBMC:/->ipmcset -t maintenance -d download -v 1
Download /tmp/bios.bin.
Downloading BIOS...
Download BIOS successfully.
```

4.8.14 升级 BIOS（upgradebios）

命令功能

maintenance -d upgradebios 命令用来升级 BIOS。

命令格式

ipmcset -t maintenance -d upgradebios -v *filepath*

参数说明

参数	参数说明	取值
filepath	BIOS 升级文件的路径。	例如，“*/tmp/biosimage.hpm*”。

使用指南

- 执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将升级的目标文件上传到 iBMC 文件系统的指定目录（例如“/tmp”）。
- **maintenance -d upgradebios** 和 **upgrade** 命令均可升级 BIOS，区别为：

- 使用 **maintenance -d upgradebios** 命令升级 BIOS 时，需在 OS 下电的情况下才能升级 BIOS。使用 **upgrade** 时则没有此要求。
- 使用 **maintenance -d upgradebios** 命令升级 BIOS 时，BIOS 默认密码会变更为目标版本的默认值，请谨慎使用。

说明

在 iBMC WebUI 升级 BIOS 后，以下信息与升级前的信息保持一致：

- “Main”界面的日期、时间和语言信息。
- BIOS 密码以及 BIOS 开机 Logo。
- “Advanced”界面的“IPMI iBMC Configuration”页面所有参数项（看门狗相关参数项除外）。

- 使用 **upgrade** 命令升级 BIOS 时，BIOS 配置不变。详细信息请参考 4.3.14 固件升级（upgrade）。

使用实例

用“/tmp/biosimage.hpm”文件升级 BIOS。

```
iBMC:/->ipmcset -t maintenance -d upgradebios -v /tmp/biosimage.hpm
Please make sure the iBMC is working while upgrading.
Updating...
System needs two minutes time to prepare.
<100%>
Update successfully.
```

4.8.15 升级主板 CPLD（upgradecpld）

命令功能

maintenance -d upgradecpld 命令用来升级服务器主板 CPLD。

命令格式

ipmcset -t maintenance -d upgradecpld -v *filepath*

参数说明

参数	参数说明	取值
filepath	主板 CPLD 升级文件的路径。	例如：“/tmp/cpldimage.hpm”

使用指南

- 当服务器主板 CPLD 异常无法使用 upgrade 命令升级生效时，可使用此命令升级主板 CPLD 并强制生效。
- 执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将待升级的目标文件上传到 iBMC 文件系统的指定目录（例如“/tmp”）。

- 执行此命令升级主板 CPLD 时会强制将服务器电源复位，请谨慎使用。

使用实例

使用“/tmp/cpldimage.hpm”文件升级主板 CPLD。

```
iBMC:/->ipmcset -t maintenance -d upgradecpld -v /tmp/cpldimage.hpm
WARNING: This operation will forcibly upgrade the CPLD and reset the server, which
will interrupt services for a period of time. The OS will be powered on or off
based on the power-on policy.
Do you want to continue?[Y/N]:Y
Updating...
<100%>
Update successfully.
```

4.8.16 设置 iBMC 网口状态（ethlink）

命令功能

maintenance -d ethlink 命令用来设置 iBMC 网口的使能状态。

命令格式

ipmcset -t maintenance -d ethlink -v <*ethname*> <*action*>

参数说明

参数	参数说明	取值
ethname	待设置的网口名称	eth0、eth1、eth2、eth3 不同服务器的 iBMC 网口个数不同。
action	网口使能状态	• enable • disable

使用指南

无

使用实例

使能 iBMC 网口“eth2”。

```
iBMC:/->ipmcset -t maintenance -d ethlink -v eth2 enable
WARNING: This operation will enable eth2.
Do you want to continue?[Y/N]:y
enable eth2 successfully.
```

4.8.17 一键收集信息（diaginfo）

命令功能

diaginfo 命令用来一键收集信息，包括 iBMC 相关的配置信息、版本信息和日志等。一键收集信息的更多内容请参见 3.11 一键收集信息说明。

命令格式

ipmcget -d diaginfo

参数说明

无

使用指南

执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/tmp”路径下的一键收集信息文件（例如“dump_info.tar.gz”）下载到客户端（例如 PC）。

使用实例

一键收集信息。

```
iBMC:/->ipmcget -d diaginfo
Download diagnose info to /tmp/ successfully.
```

4.8.18 恢复 iBMC 出厂设置（restore）

命令功能

restore 命令用来恢复 iBMC 出厂设置。执行此命令后 iBMC 会重启。

命令格式

ipmcset -d restore

参数说明

无

使用指南

无

使用实例

恢复 iBMC 出厂设置。

```
iBMC:/->ipmcset -d restore
WARNING: The iBMC will automatically restart and restore factory settings. Continue?
[Y/N]:Y
Restore factory setting successfully.
```

4.8.19 设置 CLP notimeout 功能（notimeout）

命令功能

notimeout 命令用于设置 CLP notimeout 功能的使能和禁止状态，以及会话的超时时间。禁用或启用 CLP notimeout 功能后，需要退出 iBMC 后重新登录，才能实现 CLP notimeout 功能的禁用或启用。

默认为禁用状态。

命令格式

ipmcset -d notimeout -v <*enabled* | *disabled*> [*value*]

参数说明

参数	参数说明	取值
enabled	启用 CLP notimeout 功能	-
disabled	禁用 CLP notimeout 功能	-
value	会话超时时间	取值范围：1~480 默认取值：15 取值仅在禁用状态下生效。单位为分钟。

使用指南

只有管理员和具有安全配置权限的自定义用户可设置该命令，设置成功后对所有用户的会话窗口均生效。

使用实例

启用 CLP notimeout 功能。

```
iBMC:/->ipmcset -d notimeout -v enabled
Set notimeout state successfully.
```

禁用 CLP notimeout 功能。

```
iBMC:/->ipmcset -d notimeout -v disabled
Set notimeout state successfully.
```

设置会话超时时间为 30 分钟。

```
iBMC:/->ipmcset -d notimeout -v disabled 30
Set notimeout state successfully.
```

4.8.20 查询 CLP notimeout 功能的配置信息（notimeoutstate）

命令功能

notimeoutstate 命令用于查询 CLP notimeout 功能的配置信息，如查询 CLP notimeout 功能的会话超时时间。

命令格式

ipmcget -d notimeoutstate

参数说明

无

使用指南

无

使用实例

查询 CLP notimeout 功能的配置信息。

```
iBMC:/->ipmcget -d notimeoutstate
Current notimeout state: disabled
Timeout period: 15(min)
```

4.8.21 更新系统主密钥（securityenhance -d updatemasterkey）

命令功能

securityenhance -d updatemasterkey 命令用来更新系统主密钥。

命令格式

ipmcset -t securityenhance -d updatemasterkey

参数说明

无

使用指南

请定期更新密钥，否则可能存在安全风险。

使用实例

更新系统主密钥。

```
iBMC:/->ipmcset -t securityenhance -d updatemasterkey
WARNING: You are about to update the following master key:
      IPMI password master key
      SNMP community master key
      SNMP privacy password master key
      Trap community master key
      SMTP password master key
      Redfish master key
      VNC password master key
      Upgrade file master key
      SSH host key master key
      SSL master key
      LDAP bind password master key
      NTP GroupKey file master key
Do you want to continue?[Y/N]:y
Update master key begin.
Update master key successfully.
```

4.8.22 查询和设置主密钥自动更新间隔（securityenhance -d masterkeyupdateinterval）

命令功能

securityenhance -d masterkeyupdateinterval 命令用来查询和设置主密钥自动更新间隔。

命令格式

ipmcget -t securityenhance -d masterkeyupdateinterval

ipmcset -t securityenhance -d masterkeyupdateinterval -v <*interval*>

参数说明

参数	参数说明	取值
interval	表示自动更新间隔	0～365 的整数 单位为天，取值为 0 时表示不自动更新主密钥。

使用指南

无

使用实例

查询主密钥自动更新间隔。

```
iBMC:/->ipmcget -t securityenhance -d masterkeyupdateinterval
Master key update interval: 0
```

设置主密钥自动更新间隔为 365 天。

```
iBMC:/->ipmcset -t securityenhance -d masterkeyupdateinterval -v 365
WARNING: This operation enables the BMC to automatically update the master key when
the update interval is reached.
Do you want to continue?[Y/N]y
Set master key automatic update interval successfully.
```

4.8.23 查询和设置自动发现配置（autodiscovery）

命令功能

autodiscovery 命令用来查询和设置自动发现配置。

命令格式

ipmcget -d autodiscovery

ipmcset -d autodiscovery -v <enable>/<disable> [option(0/1)] [netport]

参数说明

参数	参数说明	取值
enabled/disable	使能或禁用自动发现配置功能	• “enable”：使能 • “disable”：禁用
option	网段选择	• “0”：广播到 255.255.255.255 • “1”：同网段子网广播
netport	端口	0~65535

使用指南

无

使用实例

查询自动发现配置。

```
iBMC:/->ipmcget -d autodiscovery
State        : disabled
```

```
Broadcast    : 255.255.255.255
NetPort      : 26957
```

设置自动发现配置。

```
iBMC:/->ipmcset -d autodiscovery -v enable 0 26957
Set state to (enable) successfully.
Set broadcast to (255.255.255.255) successfully.
Set netport to (26957) successfully.
```

4.8.24 查询和设置受控上电配置（poweronpermit）

命令功能

poweronpermit 命令用来查询和设置受控上电配置。

命令格式

ipmcget -d poweronpermit

ipmcset -d poweronpermit -v <**enable** | **disable**> [*ip*] [*netport*]

参数说明

参数	参数说明	取值
enable	使能受控上电配置	-
disable	禁止受控上电配置	-
ip	服务器 IP 地址	-
netport	端口号	0~65535

使用指南

无

使用实例

查询受控上电配置。

```
iBMC:/->ipmcget -d poweronpermit
State        : enabled
ManagerIP    : 192.168.1.1
ManagerPort  : 26957
```

设置受控上电配置。

```
iBMC:/->ipmcset -d poweronpermit -v enable 192.168.1.1 26957
Set poweronpermit successfully.
```

4.8.25 查询和清除上电锁的锁定状态（poweronlock）

命令功能

默认状态下，若服务器在指定时间内未完成上电，则通过 iBMC 为服务器上电的功能被锁定，服务器将无法通过 iBMC 上电。

poweronlock 命令用来查询此上电锁的锁定状态，并可清除此上电锁，取消上述限制。

命令格式

ipmcget -t maintenance -d poweronlock

ipmcset -t maintenance -d poweronlock -v clear

参数说明

无

使用指南

无

使用实例

查询上电锁的锁定状态。

```
iBMC:/->ipmcget -t maintenance -d poweronlock
Power on lock state: Locked
```

清除上电锁。

```
iBMC:/->ipmcset -t maintenance -d poweronlock -v clear
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:Y
Clear power on lock successfully.
```

4.8.26 查询和设置 BIOS 全打印开关状态（biosprint）

命令功能

biosprint 命令用于查询和设置 BIOS 全打印开关状态。

命令格式

ipmcget -t maintenance -d biosprint

ipmcset -t maintenance -d biosprint -v <*option*>

参数说明

参数	参数说明	取值

参数	参数说明	取值
<*option*>	BIOS 全打印开关状态	• 1：表示强制开启。 • 2：按照 BIOS 中本地菜单设置。系统上电时，全打印的开启和关闭取决于本地菜单设置标志位。

使用指南

无。

使用实例

设置 BIOS 全打印开关状态为开启。

```
iBMC:/->ipmcset -t maintenance -d biosprint -v 1
WARNING: Setting BIOS debug info enable will make system start slow.
Do you want to continue?[Y/N]:y
Set BIOS debug info enable successfully
```

查询 BIOS 全打印开关状态。

```
iBMC:/->ipmcget -t maintenance -d biosprint
BIOS debug info enable
```

4.8.27 重启鲲鹏智能管理引擎（resetiME）

命令功能

resetiME 命令用于重启智能管理引擎，当智能管理引擎无法正常运行时，可使用该命令将其重启。

命令格式

ipmcset -t maintenance -d resetiME

参数说明

无

使用指南

无

使用实例

重启鲲鹏智能管理引擎。

```
iBMC:/->ipmcset -t maintenance -d resetiME
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
Reset iME successfully, the iME will restart soon.
```

4.9 用户管理命令

介绍用户管理有关命令的查询和设置方法。

4.9.1 查询所有用户信息（userlist/list）

命令功能

userlist 命令用来查询所有用户信息。

命令格式

ipmcget -d userlist

ipmcget -t user -d list

参数说明

无

使用指南

无

使用实例

查询所有用户信息。

```
iBMC:/->ipmcget -t user -d list
ID     Name            Privilege     Interface
PublicKeyHash                              State
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
3      test1           CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
4      test2           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
5      test3           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
6      test4           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
7      test5           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
8      test6           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
9      test7           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
```

```
NA                                      Disabled
10     test8          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Enabled
11     test9          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Disabled
12     test10         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Disabled
13     test11         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Disabled
14     test12         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Disabled
15     test13         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Disabled
16     test14         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Disabled
17     test15         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Enabled
```

4.9.2 添加新用户（adduser）

命令功能

adduser 用于添加新用户。

命令格式

ipmcset [-t user] -d adduser -v <*username*>

参数说明

参数	参数说明	取值
username	表示待添加的用户名。	数据类型为字符型，数据范围不超过 16 个字符。 • 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“..”。

使用指南

只有管理员可以添加新用户，操作过程中需要输入当前管理员的密码。

新添加的 SSH 用户默认为禁用状态，如需启用该用户，可参考 4.9.20 设置用户启用状态（user -d state）启用用户。

最多可添加 15 个新用户，在添加用户名后要求设置新用户的密码。新建用户的默认权限为“No Access”，默认支持所有登录接口。

请根据密码复杂度检查功能的开启情况（可通过 4.9.6 查询和设置密码检查功能（passwordcomplexity）命令查询）以及弱口令认证功能的开启情况（可通过 4.9.15 设置弱口令字典认证使能状态（weakpwddic）命令查询），修改符合不同规则的密码。

- 关闭密码检查功能后，密码不能为空，可以是任意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 4.9.16 导出弱口令字典（weakpwddic -v export）获取。）

说明

默认密码“Admin@9000”在弱口令字典中。

使用实例

添加一个新用户，用户名称为 test。

```
iBMC:/->ipmcset -d adduser -v test
Input your password:
Password:
Confirm password:
Add user successfully.
```

查询添加后的用户名单。

```
iBMC:/->ipmcget -d userlist
ID     Name            Privilege     Interface
PublicKeyHash                              State
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
3      test            NO ACCESS     Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
4                      NO ACCESS                                          NA
Disabled
5                      NO ACCESS                                          NA
Disabled
6                      NO ACCESS                                          NA
Disabled
7                      NO ACCESS                                          NA
Disabled
```

```
8                    NO ACCESS                                          NA
Disabled
9                    NO ACCESS                                          NA
Disabled
10                   NO ACCESS                                          NA
Disabled
11                   NO ACCESS                                          NA
Disabled
12                   NO ACCESS                                          NA
Disabled
13                   NO ACCESS                                          NA
Disabled
14                   NO ACCESS                                          NA
Disabled
15                   NO ACCESS                                          NA
Disabled
16                   NO ACCESS                                          NA
Disabled
17                   NO ACCESS                                          NA
Disabled
```

结果显示新增用户 test 已经成功添加。

4.9.3 修改用户密码（password）

命令功能

password 命令用来修改用户密码。

命令格式

ipmcset [-t user] -d password -v *username*

参数说明

参数	参数说明	取值
username	表示已存在的待修改密码的用户名。	-

使用指南

管理员可以修改所有用户的密码，操作员和普通用户只能修改自身的密码。操作过程中需要输入当前操作用户的密码。

请根据密码复杂度检查功能的开启情况（可通过 4.9.6 查询和设置密码检查功能（passwordcomplexity）命令查询）以及弱口令认证功能的开启情况（可通过 4.9.15 设置弱口令字典认证使能状态（weakpwddic）命令查询），修改符合不同规则的密码。

- 关闭密码检查功能后，密码不能为空，可以是任意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 4.9.16 导出弱口令字典（weakpwddic -v export）获取。）

说明

默认密码“Admin@9000”在弱口令字典中。

使用实例

修改用户名称为 user 的密码。

```
iBMC:/->ipmcset -d password -v user
Input your password:
New password:
Confirm password:
Set user password successfully.
```

4.9.4 删除用户（deluser）

命令功能

deluser 用来删除用户。

命令格式

ipmcset [-t user] -d deluser -v *username*

参数说明

参数	参数说明	取值
username	表示当前存在的待删除的用户名。	-

使用指南

- 只有管理员可以删除用户，操作过程中需要输入当前管理员的密码。
- 当 iBMC 系统中仅有一个启用的管理员用户时，该管理员用户不能被删除。

使用实例

删除一个用户，用户名称为 test。

```
iBMC:/->ipmcset -d deluser -v test
Input your password:
Delete user successfully.
```

4.9.5 设置用户权限（privilege）

命令功能

privilege 命令用来设置用户权限。

命令格式

ipmcset [-t user] -d privilege -v <*username*> <*privalue*>

参数说明

参数	参数说明	取值
username	表示当前存在的待设置权限的用户名。	-
privalue	用户权限	• 15：No Access 权限 • 2：User 权限 • 3：Operator 权限 • 4：Administrator 权限 • 5：Custom Role1 权限 • 6：Custom Role2 权限 • 7：Custom Role3 权限 • 8：Custom Role4 权限

使用指南

- 只有管理员用户可以设置用户权限，操作过程中需要输入当前管理员的密码。
- 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。

说明

默认用户为 **Administrator**。

- 被设置权限的用户可以处于 SSH 登录状态。

使用实例

设置用户名称为 test 的用户权限为 Administrator。

```
iBMC:/->ipmcset -d privilege -v test 4
Input your password:
Set user privilege successfully.
```

4.9.6 查询和设置密码检查功能（passwordcomplexity）

命令功能

passwordcomplexity 命令用来查询和设置密码复杂度检查功能的启用状态。

命令格式

ipmcget [-t user] -d passwordcomplexity

ipmcset [-t user] -d passwordcomplexity -v <enabled | disabled>

参数说明

参数	参数说明	取值
enabled	启用密码复杂度检查功能	-
disabled	禁用密码复杂度检查功能	-

使用指南

只有管理员和具有安全配置权限的自定义用户可以设置密码复杂度检查功能的开启状态。

须知

- 密码检查功能的默认状态为启用。
- 禁用密码检查功能，会降低系统安全性，请谨慎使用。

- 关闭密码检查功能后，密码不能为空，可以是任意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。

说明

在弱口令字典认证功能使能的情况下，除上述复杂度检查外，iBMC 系统还会对密码进行弱口令排查，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 4.9.16 导出弱口令字典（weakpwddic -v export）获取。）

使用实例

查询密码复杂度检查功能的开启状态。

```
iBMC:/->ipmcget -d passwordcomplexity
Password complexity check state : enabled
```

开启密码复杂度检查功能。

```
iBMC:/->ipmcset -d passwordcomplexity -v enabled
Set password complexity check state successfully.
```

4.9.7 锁定用户（user -d lock）

命令功能

lock 命令用于锁定指定的用户，而用户在被锁定之后将不能登录。

命令格式

ipmcset -t user -d lock -v *username*

参数说明

参数	参数说明	取值
username	待锁定用户的用户名	-

使用指南

只有管理员可以进行锁定操作，锁定用户时需要输入当前管理员的密码。

使用实例

锁定 admin 用户。

```
iBMC:/->ipmcset -t user -d lock -v admin
Input your password:
Lock user:admin successfully.
```

4.9.8 解除用户锁定状态（user -d unlock）

命令功能

unlock 命令用于解锁被手动锁定或因密码重试次数用完而锁定的用户。

命令格式

ipmcset -t user -d unlock -v *username*

参数说明

参数	参数说明	取值
username	待解锁用户的用户名	-

使用指南

只有管理员可以进行解锁操作，解锁时需要输入当前管理员的密码。

使用实例

解锁 root 用户的锁定状态。

```
iBMC:/->ipmcset -t user -d unlock -v root
Input your password:
Set user:root unlock status successfully.
```

4.9.9 查询和设置密码最短使用期（minimumpasswordage）

命令功能

minimumpasswordage 命令用于查询和设置密码的最短使用期。

密码最短使用期，是指设置一个密码后，要使用的最短时间，在此期间不能修改此密码。

命令格式

ipmcget -d minimumpasswordage

ipmcset -d minimumpasswordage -v *time*

参数说明

参数	参数说明	取值
time	密码最短使用期	0～365，单位为天。 0 表示密码最短使用期为无限期。

使用指南

只有管理员可以进行该操作。

使用实例

设置密码最短使用期为 1 天。

```
iBMC:/->ipmcset -d minimumpasswordage -v 1
Set minimum password age successfully, minimumpasswordage(1) days.
```

查询密码最短使用期。

```
iBMC:/->ipmcget -d minimumpasswordage
Minimum password age: 1
```

4.9.10 设置紧急用户（emergencyuser）

命令功能

emergencyuser 命令用于设置不受登录规则限制的紧急用户。

命令格式

ipmcset [-t user] -d emergencyuser -v *username*

参数说明

参数	参数说明	取值
username	紧急用户的用户名	-

使用指南

只有管理员可以设置紧急用户。

使用实例

将 root 设置为紧急用户。

```
iBMC:/->ipmcset -d emergencyuser -v root
Set emergency user to (root) successfully.
```

4.9.11 为用户添加 SSH 公钥（addpublickey）

命令功能

addpublickey 命令为用户添加 SSH 公钥。

命令格式

ipmcset -t user -d addpublickey -v *username filepath|file URL*

参数说明

参数	参数说明	取值
username	待导入 SSH 公钥的用户名	已存在的 SSH 用户的用户名
filepath	待导入的保存于本地的 SSH 公钥文件路径	“*/路径/文件名*”。例如，“*/tmp/id_dsa_2048.key*”。
file URL	待导入的远程 SSH 公钥文件的 URL	格式为： protocol://username:password@IP:[port]/directory/filename 说明 • “protocol”必须为“https”或“http”。 • “username”和“password”必须为目标服务器的用户名和密码。 • “directory/filename”必须为远程公钥文件在目标服务器上的路径。

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将准备好的 SSH 公钥文件上传到 iBMC 文件系统的指定目录下（例如"/tmp"）。

管理员可为所有用户导入 SSH 公钥，普通用户只能为自身导入 SSH 公钥。

使用实例

为“ssh_user”用户导入公钥。

```
iBMC:/->ipmcset -t user -d addpublickey -v ssh_user /tmp/id_dsa_2048.key
Input your password:
Add user public key successfully.
```

4.9.12 删除用户的 SSH 公钥（delpublickey）

命令功能

delpublickey 命令为用户删除 SSH 公钥。

命令格式

ipmcset -t user -d delpublickey -v *username*

参数说明

参数	参数说明	取值
username	待删除 SSH 公钥的用户的用户名	-

使用指南

管理员可删除所有用户的 SSH 公钥，普通用户只能删除自身的 SSH 公钥。

使用实例

删除“ssh_user_01”用户的公钥。

```
iBMC:/->ipmcset -t user -d delpublickey -v ssh_user_01
Input your password:
Delete user public key successfully.
```

4.9.13 查询和设置 SSH 用户密码认证使能状态（sshpasswordauthentication）

命令功能

sshpasswordauthentication 命令用于查询和设置 SSH 用户密码认证功能的使能状态。

命令格式

ipmcget -t user -d sshpasswordauthentication

ipmcset -t user -d sshpasswordauthentication -v <enabled | disabled>

参数说明

参数	参数说明	取值
enabled	使能 SSH 用户密码认证功能	-
disabled	禁止 SSH 用户密码认证功能	-

使用指南

无

使用实例

使能 SSH 用户密码认证功能。

```
iBMC:/->ipmcset -t user -d sshpasswordauthentication -v enabled
Set SSH password authentication successfully.
```

查询 SSH 用户密码认证使能状态。

```
iBMC:/-> ipmcget -t user -d sshpasswordauthentication
SSH Password Authentication : enabled
```

4.9.14 设置用户登录 iBMC 的接口类型（interface）

命令功能

interface 命令用于设置指定用户登录 iBMC 的接口类型。

命令格式

ipmcset -t user -d interface -v *username* <**enabled** | **disabled**> <*option1 option2 ... optionN*>

参数说明

参数	参数说明	取值
username	待配置的用户	-
enabled	使能指定的接口类型	-
disabled	禁止指定的接口类型	-
option1 option2 ... optionN	可设置的接口类型	可同时设置多个接口类型，包括： • 1：Web • 2：SNMP • 3：IPMI • 4：SSH • 5：SFTP • 7：Local • 8：Redfish

使用指南

无

使用实例

设置用户“test”登录 iBMC 的接口类型为“Web,SNMP,IPMI,SSH,SFTP,Local”。

```
iBMC:/-> ipmcset -t user -d interface -v test enabled 1 2 3 4 5 7
Input your password:
Set user login interface successfully.
```

查询“ssh_user_01”的信息。

```
iBMC:/->ipmcget -t user -d list
ID     Name            Privilege     Interface
PublicKeyHash
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish    NA
3      xxx             CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
4      commonuser       USER          Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
5      admin           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
6      operator         OPERATOR      Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
7      custom1          CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
8      test            USER          Web,SNMP,IPMI,SSH,SFTP,Local                NA
9                      NO ACCESS                                                 NA
10                     NO ACCESS                                                 NA
11                     NO ACCESS                                                 NA
12                     NO ACCESS                                                 NA
13                     NO ACCESS                                                 NA
14                     NO ACCESS                                                 NA
15                     NO ACCESS                                                 NA
16                     NO ACCESS                                                 NA
17                     NO ACCESS
```

4.9.15 设置弱口令字典认证使能状态（weakpwddic）

命令功能

weakpwddic 命令用于设置弱口令字典认证功能的使能状态。

出现在弱口令字典中的字符串不能被设置为

- 本地用户的密码
- SNMP v1/v2c 的只读团体名、读写团体名
- SNMP v3 加密密码

命令格式

ipmcset -t user -d weakpwddic -v <enabled | disabled>

参数说明

参数	参数说明	取值
enabled	使能弱口令字典认证功能	-
disabled	禁止弱口令字典认证功能	-

使用指南

只有管理员和具有安全配置权限的自定义用户可以设置弱口令字典认证使能状态。

使用实例

使能弱口令字典认证功能。

```
iBMC:/-> ipmcset -t user -d weakpwddic -v enabled
Enable weak password dictionary check successfully.
```

4.9.16 导出弱口令字典（weakpwddic -v export）

命令功能

weakpwddic -v export 命令用于导出 iBMC 的弱口令字典。

命令格式

ipmcset -t user -d weakpwddic -v export <*filepath* | *file_URL*>

参数说明

参数	参数说明	取值
filepath	将弱口令字典导出到 iBMC 文件系统时，在 iBMC 件系统中的存放路径。	绝对路径，例如：“/tmp/weakpwddictionary”。
file_URL	将弱口令字典导出到远程设备时，在远程设备上的存放路径。	格式为： *protocol*://*[username*:*password@]IP*:*[port]*/*directory/filename* 其中： • *protocol*：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 **说明** • iBMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含

参数	参数说明	取值
		username:*password*@字段；使用其它协议时，存放路径中必须包含*username*:*password*@字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • *username*：登录远程设备所需的用户名。 • *password*：登录远程设备所需的密码。 • *IP:[port]*：远程设备的 IP 地址和端口号。 • *directory/filename*：弱口令字典在远程设备上的绝对路径。 例如：“https://root:Admin12#$@10.10.10.1:443/tmp/weakpwddictionary”

使用指南

只有管理员和具有安全配置权限的自定义用户可以导出弱口令字典。

执行此命令后，可以使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将保存在“/tmp”路径下的“weakpwddictionary”文件下载到客户端（例如 PC）。

使用实例

导出弱口令字典。

```
iBMC:/-> ipmcset -t user -d weakpwddic -v export /tmp/weakpwddictionary
Export weak password dictionary successfully.
```

4.9.17 导入弱口令字典（weakpwddic -v import）

命令功能

weakpwddic -v import 命令用于导入 iBMC 的弱口令字典。

命令格式

ipmcset -t user -d weakpwddic -v import <*filepath* | *file_URL*>

参数说明

参数	参数说明	取值

参数	参数说明	取值
filepath	将弱口令字典导入 iBMC 时，待导入的文件在 iBMC 文件系统中的存放路径。	对路径，例如：“/tmp/weakpwddictionary”。
file_URL	将弱口令字典导入 iBMC 时，待导入的文件在远程设备上的存放路径。	格式为： *protocol*://*[username*:*password@]IP:[port]*/*directory/filename* 其中： • *protocol*：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 • iBMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含 *username*:*password*@字段；使用其它协议时，存放路径中必须包含 *username*:*password*@字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • *username*：登录目标服务器所需的用户名。 • *password*：登录目标服务器所需的密码。 • *IP:[port]*：目标服务器的 IP 地址和端口号。 • *directory/filename*：弱口令字典在目标服务器上的绝对路径。 例如： “https://root:Admin12#$@10.10.10.1:443/tmp/weakpwddictionary”

使用指南

只有管理员和具有安全配置权限的自定义用户可以导入弱口令字典。

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将待导入的文件上传到 iBMC 文件系统的指定目录下（例如“/tmp”）。

使用实例

导入弱口令字典。

```
iBMC:/-> ipmcset -t user -d weakpwddic -v import /tmp/weakpwddictionary
Import weak password dictionary successfully.
```

4.9.18 设置 SNMPv3 用户的加密密码（snmpprivacypassword）

命令功能

snmpprivacypassword 命令用于设置指定用户使用 SNMPv3 连接 iBMC 的数据加密密码。

命令格式

ipmcset -t user -d snmpprivacypassword -v *username*

参数说明

参数	参数说明	取值
username	待配置的用户	-

使用指南

非管理员只能修改自身的密码。管理员可以修改所有用户的密码，操作员和普通用户只能修改自身的密码。操作过程中需要输入当前操作用户的密码。

请根据密码复杂度检查功能的开启情况（可通过 4.9.6 查询和设置密码检查功能（passwordcomplexity）命令查询）以及弱口令认证功能的开启情况（可通过 4.9.15 设置弱口令字典认证使能状态（weakpwddic）命令查询），修改符合不同规则的密码。

- 关闭密码检查功能后，密码不能为空，可以是任意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 4.9.16 导出弱口令字典（weakpwddic -v export）获取。）

使用实例

设置 SNMPv3 用户的加密密码。

```
iBMC:/->ipmcset -t user -d snmpprivacypassword -v Administrator
Input your password:
Password:
Confirm password:
Set snmp privacy password successfully.
```

4.9.19 查询和设置用户不活动期限（securityenhance -d inactivetimelimit）

命令功能

securityenhance -d inactivetimelimit 命令用于设置用户不活动期限。超过设定期限内未活动的用户会被禁用。

命令格式

ipmcset -t securityenhance -d inactivetimelimit -v <*value*>

ipmcget -t securityenhance -d inactivetimelimit

参数说明

参数	参数说明	取值
value	表示不活动期限	• 0 • 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。

使用指南

无

使用实例

设置和查询不活动期限。

```
iBMC:/-> ipmcset -t securityenhance -d inactivetimelimit -v 30
WARNING: This operation could lead to iBMC users be disabled when users' inactive
time is overdue.
Do you want to continue?[Y/N]y
Set inactive user timelimit successfully.
iBMC:/-> ipmcget -t securityenhance -d inactivetimelimit
User inactive timelimit: 30
```

4.9.20 设置用户启用状态（user -d state）

命令功能

user -d state 命令用于设置用户的启用状态。

命令格式

ipmcset -t user -d state -v <*username*> [**enabled** | **disabled**]

ipmcget -d userlist

参数说明

参数	参数说明	取值
username	表示待设置的用户	已存在的用户名
enabled	表示启用该用户	-
disabled	表示禁用该用户	-

使用指南

当 iBMC 系统中仅有一个启用的管理员用户时，该管理员用户不能被禁用。

使用实例

启用“test15”用户。

```
iBMC:/-> ipmcset -t user -d state -v test15 enabled
Input your password:
Enable user:test15 successfully.
```

查询“test15”的状态。

```
iBMC:/-> ipmcget -d userlist
ID     Name            Privilege     Interface
PublicKeyHash                              State
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
3      test1           CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
4      test2           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
5      test3           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
6      test4           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        disabled
7      test5           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
8      test6           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
```

```
NA                                      Enabled
9      test7          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
10     test8          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      Enabled
11     test9          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
12     test10         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
13     test11         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
14     test12         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
15     test13         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
16     test14         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                      disabled
17     test15         ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                     Enabled
```

4.9.21 查询和设置带内用户管理使能状态（user -d usermgmtbyhost）

命令功能

user -d usermgmtbyhost 命令用于查询和设置带内用户管理功能的使能状态。

命令格式

ipmcset -t user -d usermgmtbyhost -v <*option*>

ipmcget -t user -d usermgmtbyhost

参数说明

参数	参数说明	取值
<*option*>	表示待设置的带内用户管理使能状态	• 0：禁止带内用户管理功能 • 1：使能带内用户管理功能

使用指南

带内用户管理使能关闭时，用户无法通过带内发送 IPMI 命令或 BIOS 来进行用户管理。

使用实例

禁用带内用户管理功能。

```
iBMC:/->ipmcset -t user -d usermgmtbyhost -v 0
The BMC user management function is successfully disabled on the host side.
```

查询带内用户管理使能状态。

```
iBMC:/->ipmcget -t user -d usermgmtbyhost
Disable
```

4.10 NTP 命令

介绍 NTP 相关命令的查询和设置方法。

4.10.1 查询 NTP 信息（ntpinfo）

命令功能

ntpinfo 命令用于查询 iBMC 的 NTP 信息。

命令格式

ipmcget -d ntpinfo

参数说明

无

使用指南

无

使用实例

查询 iBMC 的 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10.2 设置 NTP 状态（ntp -d status）

命令功能

ntp -d status 命令用于设置 NTP 功能的使能状态。

命令格式

ipmcset -t ntp -d status -v *status*

参数说明

参数	参数说明	取值
status	表示 NTP 功能的使能状态	• enabled • disabled

使用指南

无

使用实例

使能 NTP 功能。

```
iBMC:/->ipmcset -t ntp -d status -v enabled
Set NTP enable status (enabled) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10.3 设置 NTP 信息获取方式（ntp -d mode）

命令功能

ntp -d mode 命令用于设置 NTP 信息获取方式。

命令格式

ipmcset -t ntp -d mode -v *mode*

参数说明

参数	参数说明	取值
mode	表示 NTP 信息获取方式	• manual：手动配置 NTP 信息

参数	参数说明	取值
		• dhcpv4：使用 DHCPv4 自动获取 NTP 信息 • dhcpv6：使用 DHCPv6 自动获取 NTP 信息

使用指南

当 NTP 信息获取方式为“DHCPv4”时，无需设置时区。

使用实例

设置 NTP 信息获取方式为“manual”。

```
iBMC:/->ipmcset -t ntp -d mode -v manual
Set NTP mode (manual) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10.4 设置首选 NTP 服务器地址（ntp -d preferredserver）

命令功能

ntp -d preferredserver 命令用于设置首选 NTP 服务器地址信息。

命令格式

ipmcset -t ntp -d preferredserver -v *addr*

参数说明

参数	参数说明	取值
addr	表示首选 NTP 服务器地址	可设置为： • IPv4 格式的地址 • IPv6 格式的地址 • 域名地址 说明

参数	参数说明	取值
		设置为 0.0.0.0 时表示删除首选 NTP 服务地址。

使用指南

支持 Linux NTP 服务器和 Windows NTP 服务器。

使用实例

设置首选 NTP 服务器地址为“dhcp1.com”。

```
iBMC:/->ipmcset -t ntp -d preferredserver -v dhcp1.com
Set NTP preferred server (dhcp1.com) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10.5 设置备用 NTP 服务器地址（ntp -d alternativeserver）

命令功能

ntp -d alternativeserver 命令用于设置备用 NTP 服务器地址信息。

命令格式

ipmcset -t ntp -d alternativeserver -v *addr*

参数说明

参数	参数说明	取值
addr	表示备用 NTP 服务器地址	可设置为： • IPv4 格式的地址 • IPv6 格式的地址 • 域名地址 说明 设置为 0.0.0.0 时表示删除备用 NTP 服务地址。

使用指南

支持 Linux NTP 服务器和 Windows NTP 服务器。

使用实例

设置备用 NTP 服务器地址为“fc00::1234”。

```
iBMC:/-> ipmcset -t ntp -d alternativeserver -v fc00::1234
Set NTP alternative server (fc00::1234) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10.6 设置拓展 NTP 服务器地址（ntp -d extraserver）

命令功能

ntp -d extraserver 命令用于设置拓展 NTP 服务器地址信息。

命令格式

ipmcset -t ntp -d extraserver -v *addr*

参数说明

参数	参数说明	取值
addr	表示拓展 NTP 服务器地址	可设置为： • IPv4 格式的地址 • IPv6 格式的地址 • 域名地址 说明 设置为 0.0.0.0 时表示删除拓展 NTP 服务地址。

使用指南

支持 Linux NTP 服务器和 Windows NTP 服务器。

使用实例

设置拓展 NTP 服务器地址为“192.168.2.2”。

```
iBMC:/->ipmcset -t ntp -d extraserver -v 192.168.2.2
Set NTP extraserver server (192.168.2.2) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : fc00::1234
Extra Server      : 192.168.2.2
Synchronize       : successful
Auth Enable       : enabled
Group Key         : imported
```

4.10.7 设置服务器身份认证状态（ntp -d authstatus）

命令功能

ntp -d authstatus 命令用于设置服务器身份认证状态。

- 使能身份认证后，iBMC 与 NTP 服务器通信时会进行身份校验。
- 禁用身份认证后，iBMC 与 NTP 服务器通信时无需进行身份校验。

命令格式

ipmcset -t ntp -d authstatus -v status

参数说明

参数	参数说明	取值
status	表示服务器身份认证状态	• enabled • disabled

使用指南

使能服务器身份认证时，需要上传密钥到 iBMC 后，方可与 NTP 服务器进行通信。

说明

请定期更新密钥，否则可能存在安全风险。

使用实例

使能服务器身份认证。

```
iBMC:/->ipmcset -t ntp -d authstatus -v enabled
Set NTP enable status (enabled) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status : enabled
Mode : manual
Preferred Server : dhcp1.com
Alternative Server : fc00::1234
Extra Server : 192.168.2.2
Synchronize : successful
Auth Enable : enabled
Group Key : imported
```

4.10.8 上传 NTP 组密钥（ntp -d groupkey）

命令功能

ntp -d groupkey 命令可将用户自行获取的 NTP 组密钥上传到 iBMC，此时，iBMC 与 NTP 服务器通信时将使用该密钥进行身份校验。

命令格式

ipmcset -t ntp -d groupkey -v *filepath*

参数说明

参数	参数说明	取值
filepath	密钥文件的名称	格式为“/存放目录/文件名”。例如“/tmp/ntp.keys”。

使用指南

执行此命令之前，请先使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将准备好的密钥文件上传到 iBMC 文件系统的指定目录（例如“/tmp”）。

说明

- 鲲鹏服务器主板 S920X02 和 S920X03 支持上传 MD5 和 SHA256 算法生成的秘钥文件。
- 鲲鹏服务器主板 S920X00、S920X00K、S920X01、S920X01K、S920S00、S920S00K、S920X05 和 S920X05K 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。

使用实例

上传 NTP 组密钥。

```
iBMC:/->ipmcset -t ntp -d groupkey -v /tmp/ntp.keys
Set NTP group key (/tmp/ntp.keys) successfully.
```

查询 NTP 信息。

```
iBMC:/->ipmcget -d ntpinfo
Status : enabled
Mode : manual
Preferred Server : dhcp1.com
Alternative Server : fc00::1234
Extra Server : 192.168.2.2
Synchronize : successful
Auth Enable : enabled
Group Key : imported
```

4.11 指示灯命令

4.11.1 查询服务器指示灯信息（ledinfo）

命令功能

ledinfo 命令用来查询服务器指示灯信息。

命令格式

ipmcget -d ledinfo

参数说明

无

使用指南

无

使用实例

查询服务器控制的指示灯。

```
iBMC:/->ipmcget -d ledinfo
LED Name             : SysHealLed
LED Mode             : Local Control
LED State            : BLINKING
Off Duration          : 100 ms
On Duration          : 100 ms
LED Color            : RED
```

```
LED Color Capabilities : RED GREEN
Default LED Color in
     Local Control    : GREEN
     Override State   : GREEN

LED Name             : UIDLed
LED Mode             : Local Control
LED State            : OFF
LED Color            : BLUE
LED Color Capabilities : BLUE
Default LED Color in
     Local Control    : BLUE
     Override State   : BLUE
```

4.11.2 设置 UID 指示灯状态（identify）

命令功能

identify 命令用于设置 UID 指示灯状态。

命令格式

ipmcset -d identify [**-v** {*time* | **force**}]

参数说明

参数	参数说明	取值
time	表示 UID 指示灯闪烁时长。	数据类型为整型，单位是秒。取值范围为 0~255。 取值为 0 时，表示关闭该指示灯。
force	表示永久点亮 UID 指示灯。	-

使用指南

任何参数都没有设置的情况下，UID 指示灯默认闪烁时长为 15 秒。

使用实例

永久点亮 UID 指示灯。

```
iBMC:/->ipmcset -d identify -v force
Identify UID led successfully.
```

4.12 风扇命令

介绍服务器风扇模块有关命令的查询和设置方法。

4.12.1 设置风扇运行速度（fanlevel）

命令功能

fanlevel 命令用于设置风扇运行速度。

命令格式

ipmcset -d fanlevel -v <*fanlevel*> [*fanid*]

参数说明

参数	参数说明	取值
fanlevel	表示设置当前风扇转速为全速运转时的百分比。	数据类型为整型，不同服务器取值范围不同。
fanid	表示风扇的 ID	不同服务器的取值范围不同。

使用指南

- 若执行命令行时不输入风扇 ID，则表示设置当前所有风扇的运行速度。
- 当风扇运行模式为手动模式时该命令生效。

使用实例

手动设置 ID 为 2 的风扇转速为全速运转时的 50%。

```
iBMC:/->ipmcset -d fanlevel -v 50 2
Set fan(2) level to (50%) successfully.
Current Mode         :  Auto
iBMC:/->ipmcset -d fanlevel -v 50
Set fan level successfully.
Current Mode         :  Auto
Global Manual Fan Level:  50%
```

4.12.2 设置风扇运行模式（fanmode）

命令功能

fanmode 命令用来设置风扇的运行模式。

命令格式

ipmcset -d fanmode -v <*mode*> [*timeout*]

参数说明

参数	参数说明	取值
mode	表示风扇工作模式	• 0：风扇工作模式为自动，后面不设置 *timeout* 参数。 • 1：风扇工作模式为手动，后面可设置 *timeout* 参数。
timeout	表示由手动模式转换成自动模式的超时时间。	数据类型为整型，单位为秒。设置为“0”，表示不超时。默认情况下是表示 30 秒。

使用指南

iBMC 重启、服务器掉电以及手动模式转换成自动模式的超时时间到达，风扇运行模式会恢复至自动模式。

使用实例

设置风扇当前的模式为手动模式，60 秒钟后转换成自动模式。

```
iBMC:/->ipmcset -d fanmode -v 1 60
Set fan mode successfully.
Current Mode:      manual
Time out    :      60 seconds
```

4.12.3 查询风扇工作状态（faninfo）

命令功能

faninfo 命令用来查询风扇的工作模式和当前转速。

命令格式

ipmcget -d faninfo

参数说明

无

使用指南

无

使用实例

查询风扇工作状态。

```
iBMC:/->ipmcget -d faninfo
Get fan mode and fan level successfully!
Current mode: manual,timeout 297 seconds.
Manual fan level is 80.
```

4.13 传感器命令

4.13.1 查询所有传感器的所有信息（sensor -d list）

命令功能

sensor -d list 命令用来查询所有传感器信息。

命令格式

ipmcget -t sensor -d list

参数说明

无

使用指南

无

使用实例

查询所有传感器的所有信息。（不同服务器的传感器不同）

```
iBMC:/->ipmcget -t sensor -d list
sensor id  | sensor name     | value     | unit        | status | lnr       | lc
| lnc       | unc     | uc        | unr       | phys   | nhys
0x1       | Inlet Temp      | 24.000    | degrees C   | ok     | na        | na
| na        | 42.000   | 44.000    | na        | 2.000  | 2.000
0x2       | Outlet Temp     | 30.000    | degrees C   | ok     | na        | na
| na        | na      | na        | na        | 2.000  | 2.000
0x3       | PCH Temp        | 32.000    | degrees C   | ok     | na        | na
| na        | 90.000   | na        | na        | 3.000  | 3.000
0x4       | CPU1 Core Rem   | 30.000    | degrees C   | ok     | na        | na
| na        | na      | na        | na        | 0.000  | 0.000
0x5       | CPU2 Core Rem   | 30.000    | degrees C   | ok     | na        | na
| na        | na      | na        | na        | 0.000  | 0.000
```

```
0x6       | CPU1 DTS        | -65.000    | unspecified  | ok    | na        | na
| na        | -1.000   | na        | na        | 3.000  | 3.000
0x7       | CPU2 DTS        | -66.000    | unspecified  | ok    | na        | na
| na        | -1.000   | na        | na        | 3.000  | 3.000
0x8       | CPU1 Prochot    | 30.000     | degrees C    | ok    | na        | na
| na        | na       | 90.000     | na        | 0.000  | 0.000
0x9       | CPU2 Prochot    | 30.000     | degrees C    | ok    | na        | na
| na        | na       | 90.000     | na        | 0.000  | 0.000
0xa       | CPU1 VDDQ Temp   | 32.000     | degrees C    | ok    | na        | na
| na        | 120.000  | na        | na        | 3.000  | 3.000
0xb       | CPU2 VDDQ Temp   | 32.000     | degrees C    | ok    | na        | na
| na        | 120.000  | na        | na        | 3.000  | 3.000
0xc       | CPU1 VRD Temp    | 33.000     | degrees C    | ok    | na        | na
| na        | 120.000  | na        | na        | 3.000  | 3.000
0xd       | CPU2 VRD Temp    | 31.000     | degrees C    | ok    | na        | na
| na        | 120.000  | na        | na        | 3.000  | 3.000
0xe       | CPU1 MEM Temp    | 27.000     | degrees C    | ok    | na        | na
| na        | 90.000   | na        | na        | 3.000  | 3.000
0xf       | CPU2 MEM Temp    | 27.000     | degrees C    | ok    | na        | na
| na        | 90.000   | na        | na        | 3.000  | 3.000
0x10      | +3.3V           | 3.260     | Volts        | ok    | na        | 2.980
| na        | na       | 3.620     | na        | 0.160  | 0.160
0x11      | +5.0V           | 4.980     | Volts        | ok    | na        | 4.530
| na        | na       | 5.490     | na        | 0.240  | 0.240
0x12      | +12.0V          | 12.120     | Volts        | ok    | na        | 10.800
| na        | na       | 13.200     | na        | 0.480  | 0.480
0x13      | +1.8V CPU1      | 1.800     | Volts        | ok    | na        | 1.470
| na        | na       | 1.850     | na        | 0.020  | 0.020
0x14      | +1.8V CPU2      | 1.790     | Volts        | ok    | na        | 1.470
| na        | na       | 1.850     | na        | 0.020  | 0.020
0x15      | +1.2V VDDQ1     | 1.180     | Volts        | ok    | na        | 1.140
| na        | na       | 1.260     | na        | 0.020  | 0.020
0x16      | +1.2V VDDQ2     | 1.180     | Volts        | ok    | na        | 1.140
| na        | na       | 1.260     | na        | 0.020  | 0.020
0x17      | +1.2V VDDQ3     | 1.180     | Volts        | ok    | na        | 1.140
| na        | na       | 1.260     | na        | 0.020  | 0.020
0x18      | +1.2V VDDQ4     | 1.180     | Volts        | ok    | na        | 1.140
| na        | na       | 1.260     | na        | 0.020  | 0.020
0x19      | FAN1 F Speed    | 6720.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x1a      | FAN1 R Speed    | 6720.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x1b      | FAN2 F Speed    | 6600.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x1c      | FAN2 R Speed    | 6600.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x1d      | FAN3 F Speed    | 6720.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x1e      | FAN3 R Speed    | 6720.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x1f      | FAN4 F Speed    | 6600.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x20      | FAN4 R Speed    | 6600.000   | RPM         | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x21      | RearDisk1 Temp   | 26.000     | degrees C    | ok    | na        | na
```

```
| na        | 53.000   | na        | na        | 2.000  | 2.000
0x22      | Power1          | 124.000    | Watts       | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x23      | Power2          | 52.000     | Watts       | ok    | na        | na
| na        | na       | na        | na        | 0.000  | 0.000
0x24      | CPU1 Status     | 0x0        | discrete    | 0x8080 | na        | na
| na        | na       | na        | na        | na     | na
0x25      | CPU2 Status     | 0x0        | discrete    | 0x8080 | na        | na
| na        | na       | na        | na        | na     | na
0x26      | CPU1 Memory     | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x27      | CPU2 Memory     | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x28      | FAN1 F Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x29      | FAN1 R Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x2a      | FAN2 F Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x2b      | FAN2 R Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x2c      | FAN3 F Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x2d      | FAN3 R Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x2e      | FAN4 F Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x2f      | FAN4 R Status   | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x30      | PS1 Presence    | 0x0        | discrete    | 0x8002 | na        | na
| na        | na       | na        | na        | na     | na
0x31      | PS2 Presence    | 0x0        | discrete    | 0x8002 | na        | na
| na        | na       | na        | na        | na     | na
0x32      | DIMM000         | 0x0        | discrete    | 0x8040 | na        | na
| na        | na       | na        | na        | na     | na
0x33      | DIMM001         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x34      | DIMM002         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x35      | DIMM010         | 0x0        | discrete    | 0x8040 | na        | na
| na        | na       | na        | na        | na     | na
0x36      | DIMM011         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x37      | DIMM012         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x38      | DIMM020         | 0x0        | discrete    | 0x8040 | na        | na
| na        | na       | na        | na        | na     | na
0x39      | DIMM021         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x3a      | DIMM022         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x3b      | DIMM030         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
0x3c      | DIMM031         | 0x0        | discrete    | 0x8000 | na        | na
| na        | na       | na        | na        | na     | na
```

```
0x3d      | DIMM032         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x3e      | DIMM100         | 0x0       | discrete    | 0x8040 | na        | na
| na        | na      | na        | na        | na     | na
0x3f      | DIMM101         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x40      | DIMM102         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x41      | DIMM110         | 0x0       | discrete    | 0x8040 | na        | na
| na        | na      | na        | na        | na     | na
0x42      | DIMM111         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x43      | DIMM112         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x44      | DIMM120         | 0x0       | discrete    | 0x8040 | na        | na
| na        | na      | na        | na        | na     | na
0x45      | DIMM121         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x46      | DIMM122         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x47      | DIMM130         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x48      | DIMM131         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x49      | DIMM132         | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x4a      | AreaIntrusion   | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x4b      | RTC Battery     | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x4c      | PCIE Status     | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x4d      | ACPI State      | 0x0       | discrete    | 0x8001 | na        | na
| na        | na      | na        | na        | na     | na
0x4e      | SysFWProgress   | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x4f      | Power Button    | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x50      | SysRestart      | 0x0       | discrete    | 0x8080 | na        | na
| na        | na      | na        | na        | na     | na
0x51      | Boot Error      | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x52      | Watchdog2       | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x53      | Mngmnt Health   | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x54      | UID Button      | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x55      | PwrOk Sig. Drop | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x56      | PwrOn TimeOut   | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x57      | PwrCap Status   | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x58      | HDD Backplane   | 0x0       | discrete    | 0x8000 | na        | na
```

```
| na        | na       | na         | na         | na     | na
0x59      | HDD BP Status    | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x5a      | Riser1 Card      | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x5b      | Riser2 Card      | 0x0       | discrete    | 0x8002 | na        | na
| na        | na       | na         | na         | na     | na
0x5c      | SAS Cable        | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x5d      | FAN1 F Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x5e      | FAN1 R Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x5f      | FAN2 F Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x60      | FAN2 R Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x61      | FAN3 F Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x62      | FAN3 R Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x63      | FAN4 F Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x64      | FAN4 R Presence  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x65      | RAID Presence    | 0x0       | discrete    | 0x8002 | na        | na
| na        | na       | na         | na         | na     | na
0x66      | CPU Usage        | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x67      | Memory Usage     | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x6a      | RAID Status      | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x6b      | DISK0            | 0x0       | discrete    | 0x8001 | na        | na
| na        | na       | na         | na         | na     | na
0x6c      | DISK1            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x6d      | DISK2            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x6e      | DISK3            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x6f      | DISK4            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x70      | DISK5            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x71      | DISK6            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x72      | DISK7            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x73      | DISK8            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x74      | DISK9            | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
0x75      | DISK10           | 0x0       | discrete    | 0x8000 | na        | na
| na        | na       | na         | na         | na     | na
```

```
0x76      | DISK11          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x77      | DISK12          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x78      | DISK13          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x79      | DISK14          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x7a      | DISK15          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x7b      | DISK16          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x7c      | DISK17          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x7d      | DISK18          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x7e      | DISK19          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x7f      | DISK20          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x80      | DISK21          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x81      | DISK22          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x82      | DISK23          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x83      | DISK24          | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x84      | DISKA           | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x85      | DISKB           | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x86      | DISKC           | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x87      | DISKD           | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x88      | Eth1 Link Down  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x89      | Eth2 Link Down  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x8a      | Eth3 Link Down  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x8b      | Eth4 Link Down  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x8c      | PS1 Status      | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x8d      | PS1 Fan Status  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x8e      | PS2 Status      | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x8f      | PS2 Fan Status  | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na     | na
0x90      | PCIE SW1 Temp   | na        | degrees C   | na     | na        | na
| na        | 100.000 | na        | na        | 2.000  | 2.000
0x91      | PCIE SW2 Temp   | na        | degrees C   | na     | na        | na
```

```
| na        | 100.000  | na        | na        | 2.000  | 2.000
0x93      | LOM P1 Link Down | 0x0       | discrete    | 0x8100 | na        | na
| na        | na       | na        | na        | na     | na
0x94      | LOM P2 Link Down | 0x0       | discrete    | 0x8100 | na        | na
| na        | na       | na        | na        | na     | na
0x95      | LOM P3 Link Down | 0x0       | discrete    | 0x8100 | na        | na
| na        | na       | na        | na        | na     | na
0x96      | LOM P4 Link Down | 0x0       | discrete    | 0x8100 | na        | na
| na        | na       | na        | na        | na     | na
```

表4-3 传感器信息字段说明

字段	含义	举例说明	备注
sensor name	传感器名称	CPU1 Core Rem，表示 CPU1 的核心温度传感器。	-
value	当前值	35.000，表示当前传感器的值。	na，表示当前传感器未检测到数值或状态，可能当前传感器对应的设备不在位。
unit	当前值单位	degrees C，表示单位为摄氏度。	discrete，表示对应传感器为离散传感器，没有单位。
status	状态	ok，表示传感器正常。 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。	na，表示当前传感器未检测到数值或状态，可能当前传感器对应的设备不在位。 0x*XXX*，例如，0x8000，是根据 IPMI 规范定义的，采用 16 进制数值表示当前传感器的状态，具体含义请参见 IPMI 规范中表 42-2 Generic Event/Reading Type Codes 中字段 Generic Offset 的解释和表 42-3 Sensor Type Codes 中字段 Sensor specific Offset 的解释。
lnr	紧急下门限	na	na，表示当前传感器不支持该门限值。
lc	严重下门限	na	na，表示当前传感器不支持该门限值。
lnc	轻微下门限	na	na，表示当前传感器不支持该门限值。
unc	轻微上门限	84.000，表示当前传感器正向轻微告警门限值是84。	na，表示当前传感器不支持该门限值。
uc	严重上门限	88.000，表示当前传感器正向严重告警门限值是88。	na，表示当前传感器不支持该门限值。
unr	紧急上门限	na	na，表示当前传感器不支持该门限值。
phys	正向迟滞量	3，表示当前传感	na，表示当前传感器不支持该迟滞量。

字段	含义	举例说明	备注
		器的正向迟滞量是 3。	
nhys	负向迟滞量	3，表示当前传感器的负向迟滞量是 3。	na，表示当前传感器不支持该迟滞量。

说明

传感器的门限值请参考实际列表。

4.13.2 传感器测试命令（sensor -d test）

命令功能

test 命令用于模拟传感器状态或读数。

须知

测试之前请先使用 **ipmcget -t sensor -d list** 命令查询传感器状态，确保在传感器状态正常的情况下进行测试，否则已经故障告警的传感器在测试结束后会重复上报一次故障告警。

命令格式

ipmcset -t sensor -d test -v <*sensorname*/stopall> [*value*/stop]

参数说明

参数	参数说明	取值
sensorname/stopall	传感器名称	• “sensorname”：传感器名称 • “stopall”：停止所有测试
value/stop	模拟值	• “value”：传感器的测试模拟值 说明 执行该命令时，设置的值在 iBMC 内部会进行转换，转换过程中容易造成精度丢失，故传感器的设置值与实际值之间存在误差。误差不会影响系统本身的运行，请以回显信息中的实际值为

参数	参数说明	取值
		准。 • “stop”：停止所有测试

使用指南

建议使用 4.13.3 模拟事件（precisealarm）命令模拟告警。

使用实例

模拟 CPU1 Core Rem 传感器温度当前值为 100。

```
iBMC:/->ipmcset -t sensor -d test -v "CPU1 Core Rem" 100
Sensor test successfully.
```

4.13.3 模拟事件（precisealarm）

命令功能

precisealarm 命令用于模拟 iBMC 定义的事件。

命令格式

ipmcset -t precisealarm -d mock -v {*eventcode* |**stopall**} [*subjectindex*] *eventstatus*

参数说明

参数	参数说明	取值
eventcode	要模拟事件的事件码。	• 0xffffffff：表示模拟 iBMC 定义的全部事件。 • 0x**ffffff：表示模拟事件主体类型为**的全部事件。 • 指定事件的事件码：表示模拟指定事件。 说明 • 事件码的第一个字节表示其事件主体类型。例如，事件码为“0x02000007”的告警，其事件主体类型为“02”，含义是“Disk”。 • 事件主体类型**的实际含义，可参考服务器告警处理文档中的详细描

参数	参数说明	取值
		述。
stopall	停止事件模拟动作，取消所有模拟的事件。	-
subjectindex	要模拟的指定事件的事件主体类型代表的事件序号。	与模拟事件相关的事件序号。 事件序号获取方法如下： 1. 查询指定事件码下的所有事件。 2. 从获取到的信息中查看目标事件对应的事件序号。
eventstatus	模拟告警的状态。	• assert：事件产生 • deassert：事件恢复 • stop：停止模拟

使用指南

- 当“eventcode”为“0xffffffff”和“0x**ffffff”时，不可添加“subjectindex”参数。
- 当“eventcode”为指定事件码时，添加“subjectindex”参数可对指定的事件主体进行事件模拟。

使用实例

模拟事件码为“0x2C000025”的告警。

```
iBMC:/->ipmcset -t precisealarm -d mock -v 0x2C000025 assert
Precise alarm mock successfully.
```

4.14 电源命令

介绍电源有关命令的查询和设置方法。

4.14.1 设置电源工作模式（psuworkmode）

命令功能

psuworkmode 命令用来设置电源工作模式。

命令格式

ipmcset -d psuworkmode -v <*option*> [*active_psuid*]

参数说明

参数	参数说明	取值
option	电源工作模式	• 0：负载均衡模式 • 1：主备模式 • 2：深度休眠模式
active_psuid	电源工作模式为主备模式时，主电源的 ID。	1~2

使用指南

无

使用实例

设置电源的工作模式。

```
iBMC:/->ipmcset -d psuworkmode -v 1 1
Set Power Work Mode (Active Standby) successfully
```

4.14.2 查询电源具体信息（psuinfo）

命令功能

psuinfo 命令用来获取电源信息。

命令格式

ipmcget -d psuinfo

参数说明

无

使用指南

无

使用实例

查询电源的信息。

```
iBMC:/-> ipmcget -d psuinfo
Current PSU Information :
Slot   Manufacturer    Type              SN                          Version
Rated Power   InputMode
1     HUAWEI         PAC3000S12-T1       2102312SRLBTL9000092          DC:110
```

```
PFC:110                 3000        AC
2     HUAWEI          PAC3000S12-T1       2102312SRLBTL9000004          DC:110
PFC:110                 3000        AC
3     HUAWEI          PAC3000S12-T1       00000000000000000000          DC:110
PFC:110                 3000        AC
4     HUAWEI          PAC3000S12-T1       2102312SRLBTL9000055          DC:110
PFC:110                 3000        AC

Current PSU WorkMode    :
Actual PSU Status       :
   Work Mode          : Load Balancing
Predicted PSU Status    :
   Work Mode          : Load Balancing
```

4.15 SOL 命令

介绍 SOL 有关命令的查询和设置方法。

4.15.1 建立 SOL 会话（sol -d activate）

命令功能

sol -d activate 命令用于建立 SOL 会话连接系统或 iBMC 串口。

命令格式

ipmcset -t sol -d activate -v <*option*> <*mode*>

参数说明

参数	参数说明	取值
option	表示要连接的串口，系统串口或 iBMC 串口。	• 1：系统串口 • 2：iBMC 串口
mode	表示 SOL 会话模式。	• 0：共享模式 选择共享模式时，可同时建立两路 SOL 会话，两路会话的内容共享，在任意一路 SOL 会话中的操作，对另一路会话可见。 • 1：独占模式 选择独占模式时，只允许同时存在一路 SOL 会话。

使用指南

在建立 SOL 会话连接到系统串口之前，请先在 OS 侧配置串口重定向功能。OS 侧的串口重定向配置方法，请查看各 OS 厂商提供的操作指导。

建立连接后，可轮流按下“Esc”和“(”退出当前 SOL 会话，返回命令行。按下“Esc”和“(”的时间间隔不允许超过 1 秒。

使用实例

建立 SOL 共享模式会话，连接系统串口。

```
iBMC:/->ipmcset -t sol -d activate -v 1 0
[Connect SOL successfully! Use 'Esc(' to exit.]
Warning! The SOL session is in shared mode, the operation can be viewed on another
terminal.

sles11sp1:~ #
sles11sp1:~ # Esc( [Close SOL]

SOL connection closed.
```

4.15.2 注销 SOL 会话（sol -d deactivate）

命令功能

sol -d deactivate 命令用于强制注销 SOL 会话。

命令格式

ipmcset -t sol -d deactivate -v <*index*>

参数说明

参数	参数说明	取值
index	表示 SOL 会话序号。	• “1”：会话 1 • “2”：会话 2

使用指南

通过 IPMITOOL 建立的 SOL 会话不可注销。

使用实例

注销 SOL 会话。

```
iBMC:/->ipmcset -t sol -d deactivate -v 1
Close SOL session successfully.
```

4.15.3 设置 SOL 会话超时时间（sol -d timeout）

命令功能

sol -d timeout 命令用于设置 SOL 会话超时时间。设置超时时间后，用户在 SOL 会话中无输入并达到超时时间后，SOL 会话将退出并返回 iBMC 命令行界面。

命令格式

ipmcset -t sol -d timeout -v <*value*>

参数说明

参数	参数说明	取值
value	表示 SOL 会话用户无输入时，退出 SOL 会话的时间。	0 ~ 480，单位为分钟，取值为“0”时表示永不超时。 超时时间的默认取值为 15 分钟。

使用指南

无

使用实例

设置 SOL 会话超时时间为 20 分钟。

```
iBMC:/->ipmcset -t sol -d timeout -v 20
Set SOL timeout period successfully.
```

4.15.4 查询 SOL 会话列表（sol -d session）

命令功能

sol -d session 命令用于查询 SOL 会话列表。

命令格式

ipmcget -t sol -d session

参数说明

无

使用指南

无

使用实例

查询 SOL 会话列表。

```
iBMC:/->ipmcget -t sol -d session
Index  Type    Mode    LoginTime            IP                  Name
1      CLI     Shared  2017-09-14 11:19:55  192.168.1.40:50013  root
2      N/A     N/A     N/A                  N/A                 N/A
```

4.15.5 查询 SOL 会话配置信息（sol -d info）

命令功能

sol -d info 命令用于查询 SOL 会话配置信息，如查询 SOL 会话超时时间。

命令格式

ipmcget -t sol -d info

参数说明

无

使用指南

无

使用实例

查询 SOL 会话配置信息。

```
iBMC:/->ipmcget -t sol -d info
Timeout Period(Min)       :   20
```

5 常用维护命令

5.1 查看帮助信息（help）

命令功能

help 命令用于查看帮助信息，也可以查看某条命令的具体使用方法。

命令格式

help

[*command*] **--help**

参数说明

参数	参数说明	取值

参数	参数说明	取值
command	具体命令	-

使用指南

无

使用实例

获取当前路径下支持的命令。

```
iBMC:/->help
Commands:
help     :      Used to get context sensitive help.
exit     :      Used to terminate the CLP session.
ipmcget   :      Used to get BMC runtime status.
ipmcset   :      Used to set BMC runtime status or send control command.
notimeout :      Used to set no timeout limit to login shell.
maint debug cli : Used to maintance in debug mode.
ping     :      Used to test IPv4 network status.
ping6    :      Used to test IPv6 network status.
ifconfig  :      Used to check network device information.
ps       :      Used to check processes status.
free     :      Used to check memory status.
top      :      Used to check system resource used information. None parameter is
allowed
df       :      Used to check disk used information.
route    :      Used to check route information. None parameter is allowed
netstat   :      Used to check network port status.
```

说明

maint_debug_cli 命令主要用于现场维护定位，只允许管理员和操作员使用。

获取 ping 命令的具体使用方法。

```
iBMC:/->ping --help
BusyBox v1.31.1 (2020-07-16 00:11:18 CST) multi-call binary.

Usage: ping [OPTIONS] HOST

Send ICMP ECHO_REQUEST packets to network hosts

Options
-4,-6Force IP or IPv6 name resolution
-c CNTSend only CNT pings
-s SIZESend SIZE data bytes in packets (default:56)
-I IFACE/IP Use interface or IP address as source
-W SECSeconds to wait for the fiàäì response (default:10)
(after all -c CNT packets are sent)
-w SECSeconds until ping exits (š ž f† ñÃìó²nfin²ìž )
(can exit earlier with -c CNT)
-qQuiet, only displays output at start
```

```
and when fin²ä¯ž š
```

5.2 断开连接（exit）

命令功能

exit 命令用于断开客户端与 iBMC 的连接。

命令格式

exit

参数说明

无

使用指南

无

使用实例

断开连接。

```
iBMC:/->exit

Connection closed by foreign host.
```

5.3 检查网络连通性（ping、ping6）

命令功能

ping 或 **ping6** 命令用于检查网络是否连通。

命令格式

ping <*IPv4 Address*>

ping6 <*IPv6 Address*>

参数说明

参数	参数说明	取值
IPv4 Address	目标 IPv4 地址	-
IPv6 Address	目标 IPv6 地址	-

使用指南

更多信息可参考 Linux ping、ping6 命令使用说明。

使用实例

检查当前设备是否可与目标地址的设备连通。

```
iBMC:/->ping 192.168.44.178
PING 192.168.44.178 (192.168.44.178): 56 data bytes
64 bytes from 192.168.44.178: icmp req=1 ttl=64 time=8.19 ms
64 bytes from 192.168.44.178: icmp req=2 ttl=64 time=0.398 ms
64 bytes from 192.168.44.178: icmp req=3 ttl=64 time=0.263 ms
64 bytes from 192.168.44.178: icmp req=4 ttl=64 time=0.285 ms
64 bytes from 192.168.44.178: icmp req=5 ttl=64 time=0.418 ms
iBMC:/->ping6 fc00::39ad:9345:1a6e:d0e1
PING fc00::39ad:9345:1a6e:d0e1(fc00::39ad:9345:1a6e:d0e1) 56 data bytes
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp seq=1 ttl=64 time=0.821 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp seq=2 ttl=64 time=0.840 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp seq=3 ttl=64 time=0.843 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp seq=4 ttl=64 time=0.744 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp seq=5 ttl=64 time=0.774 ms
64 bytes from fc00::39ad:9345:1a6e:d0e1: icmp_seq=6 ttl=64 time=1.02 ms
```

5.4 free 命令（free）

命令功能

该命令用于执行 Linux 中的 free 命令。

命令格式

参考 Linux 中 free 命令的使用方法。

参数说明

支持 free 命令的所有参数。

使用指南

无

使用实例

```
iBMC:/->free
              total        used        free      shared  buff/cache   available
Mem:        1609608      334264     1227292       10200       48052     1220532
Swap:             0           0           0
```

5.5 netstat 命令（netstat）

命令功能

该命令用于执行 Linux 中的 netstat 命令。

命令格式

参考 Linux 中 netstat 命令的使用方法。

参数说明

支持 netstat 命令的所有参数。

使用指南

无

使用实例

```
iBMC:/->netstat -t
 Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp       0    116 192.168.64.110:ssh     192.168.29.200:65069   ESTABLISHED
tcp       0      0 192.168.64.110:ssh     192.168.29.200:65068   ESTABLISHED
```

5.6 df 命令（df）

命令功能

该命令用于执行 Linux 中的 df 命令。

命令格式

参考 Linux 中 df 命令的使用方法。

参数说明

支持 df 命令的所有参数。

使用指南

无

使用实例

```
iBMC:/->df
Filesystem         1K-blocks     Used Available Use% Mounted on
```

```
/dev/nvm active       364681   124710   216624  37% /
tmpfs                804804        0   804804   0% /dev
tmpfs                804804     1076   803728   0% /dev/shm
none                  98304        0    98304   0% /tmp
/dev/mmcblk0p1       967844   172664   728800  19% /data
/dev/pramdisk0        11891     3444     8447  29% /opt/pme/pram
/dev/loop0             6566     2973     3045  49% /opt/pme/extern/profile
/dev/loop1             8975     5977     2276  72% /opt/pme/extern/web
/dev/mapper/mmcblksp  3578016  2438184  1139832  68% /data/sp
```

5.7 ifconfig 命令（ifconfig）

命令功能

该命令用于执行 Linux 中的 ifconfig 命令。

命令格式

参考 Linux 中 ifconfig 命令的使用方法。

参数说明

只支持参数为“lo”、“ethn”（n 为网口索引号）或“-a”，或不带参数。

使用指南

无

使用实例

```
iBMC:/->ifconfig eth1
eth1     Link encap:Ethernet  Addr
         inet6 addr: fe80::218:82ff:fe11:321/64 Scope:Link
         UP BROADCAST DEBUG RUNNING  MTU:1500  Metric:1
         RX packets:28 errors:0 dropped:0 overruns:0 frame:0
         TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1832 (1.7 KiB)  TX bytes:2558 (2.4 KiB)
         Interrupt:28
```

5.8 route 命令（route）

命令功能

该命令用于执行 Linux 中的 route 命令。

命令格式

参考 Linux 中 route 命令的使用方法。

参数说明

-n ： 不要使用通讯协定或主机名称，直接使用 IP 或端口号。

-e ： 显示更多信息。

-A inet{6} ： 选择地址族。

使用指南

无

使用实例

```
iBMC:/->route --help
Usage: route [option]

Check kernel routing tables

Options:
-n              Don't resolve names
-e              Display other/more information
-A inet{6}       Select address family
```

5.9 top 命令（top）

命令功能

该命令用于执行 Linux 中的 top 命令。

命令格式

参考 Linux 中 top 命令的使用方法。

参数说明

不支持带参数。

使用指南

无

使用实例

```
iBMC:/->top
top - 16:26:41 up 3 days, 15:48,  3 users,  load average: 0.09, 0.08, 0.08
Tasks:  46 total,   1 running,  45 sleeping,   0 stopped,   0 zombie
```

```
Cpu(s):  2.2%us,  3.4%sy,  0.0%ni, 94.3%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:    125572k total,    94920k used,    30652k free,    14780k buffers
Swap:       0k total,       0k used,       0k free,    35916k cached

 PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
1133 root      20   0  2408  968  784 R  3.7  0.8   0:00.09 top
   1 root      20   0  1980  652  572 S  0.0  0.5   0:01.95 init
   2 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kthreadd
   3 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
   4 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 events/0
   5 root      15  -5     0    0    0 S  0.0  0.0   0:03.81 khelper
  64 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
 103 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
 104 root      20   0     0    0    0 S  0.0  0.0   0:13.65 pdflush
```

5.10 禁止 CLP 超时（notimeout）

命令功能

notimeout 命令用于禁止 CLP 超时，确保可以在 CLP 命令行进行长时间操作。

命令格式

notimeout

参数说明

无

使用指南

该命令仅对当前会话窗口生效。

使用实例

禁止 CLP 命令行超时。

```
iBMC:/->notimeout
iBMC:/->
```

6 常用操作

6.1 使用 PuTTY 登录服务器（串口方式）

操作场景

使用 PuTTY 工具，可以通过串口方式访问服务器，主要应用场景如下：

- 新建局点首次配置服务器时，本地 PC 机可以通过连接服务器的串口，登录服务器进行初始配置。
- 产品网络故障，远程连接服务器失败时，可通过连接服务器的串口，登录服务器进行故障定位。

必备事项

前提条件

- 已通过串口线缆连接 PC 与服务器。
- 已经安装 PuTTY，且 PuTTY 的版本为 0.68 及以上。

说明

低版本的 PuTTY 软件可能导致登录服务器失败，建议使用最新版本的 PuTTY 软件。

数据

登录服务器的用户名和密码。

操作步骤

步骤 1 双击“PuTTY.exe”。

弹出“PuTTY Configuration”窗口。

步骤 2 在左侧导航树中选择“Connection > Serial”。

步骤 3 设置登录参数。

参数举例如下：

- Serial Line to connect to：COM*n*
- Speed（baud）：115200
- Data bits：8
- Stop bits：1
- Parity：None
- Flow control：None

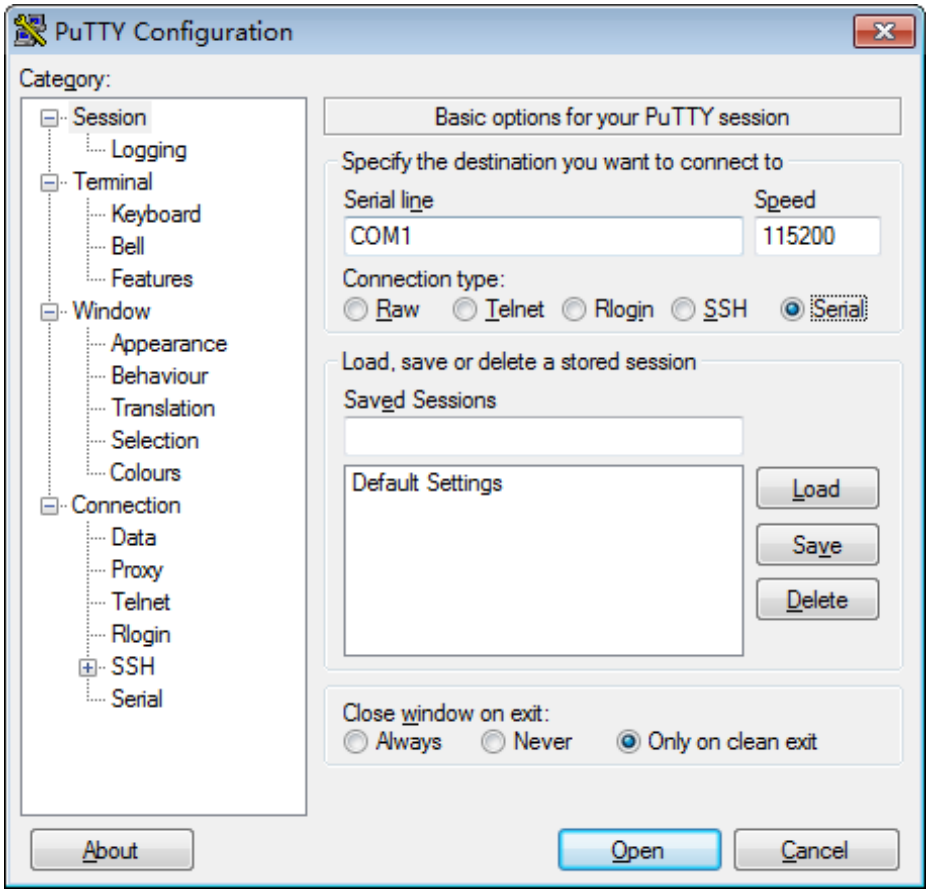
说明

n 表示不同串口的编号，取值为整数。

步骤 4 在左侧导航树中选择“Session”。

步骤 5 选择“Connection type”为“Serial”，如图 6-1 所示。

图6-1 PuTTY Configuration



步骤 6 单击“Open”。

进入“PuTTY”运行界面，提示“login as:”，等待用户输入用户名。

步骤 7 按提示分别输入用户名和密码。

登录完成后，命令提示符左侧显示出当前登录服务器的主机名。

----结束

6.2 使用 PuTTY 登录服务器（网口方式）

操作场景

使用 PuTTY 工具，可以通过局域网远程访问服务器，对服务器实施配置、维护操作。

必备事项

前提条件

- 已通过网线连接 PC 与服务器的管理网口。

- 已经安装 PuTTY，且 PuTTY 的版本为 0.68 及以上。

说明

低版本的 PuTTY 软件可能导致登录服务器失败，建议使用最新版本的 PuTTY 软件。

数据

需准备如下数据：

- 服务器的 IP 地址
- 登录服务器的用户名和密码

操作步骤

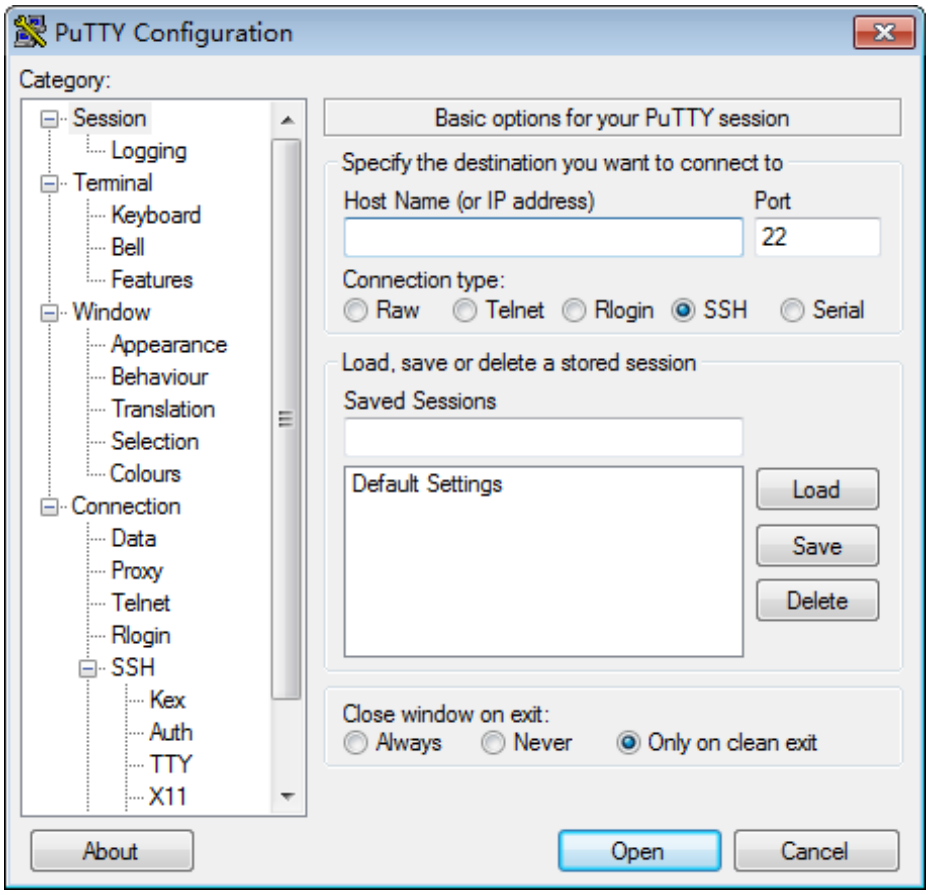
步骤 1 设置 PC 机的 IP 地址、子网掩码或者路由，使 PC 机能和服务器网络互通。

可在 PC 机的 cmd 命令窗口，通过 **Ping** ***服务器 IP 地址***命令，检查网络是否互通。

步骤 2 双击“PuTTY.exe”。

弹出“PuTTY Configuration”窗口，如图 6-2 所示。

图6-2 PuTTY Configuration



步骤 3 填写登录参数。

参数说明如下：

- Host Name（or IP address）：输入要登录服务器的 IP 地址，如“192.168.34.32”。
- Port：默认设置为“22”。
- Connection type：默认选择“SSH”。
- Close window on exit：默认选择“Only on clean exit”。

说明

配置“Host Name”后，再配置“Saved Sessions”并单击“Save”保存，则后续使用时直接双击“Saved Sessions”下保存的记录即可登录服务器。

步骤 4 单击“Open”。

进入“PuTTY”运行界面，提示“login as:”，等待用户输入用户名。

说明

- 如果首次登录该目标服务器，则会弹出“PuTTY Security Alert”窗口。单击“是”表示信任此站点，进入“PuTTY”运行界面。
- 登录服务器时，如果帐号输入错误，必须重新连接 PuTTY。

步骤 5 按提示分别输入用户名和密码。

登录完成后，命令提示符左侧显示出当前登录服务器的主机名。

----结束

6.3 配置 iBMC WebUI Trap

操作场景

iBMC WebUI 的“维护诊断 > 告警上报”提供“Trap 功能”，可以设置 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、轻微告警和事件。

必备事项

数据

进行配置之前，请先规划好配置过程中所需数据：

- 采用的 SNMP Trap 协议版本。
- 用于识别信息来源的主机标识（“单板序列号”、“产品资产标签”或“主机名”）。
- SNMP Trap 协议使用的团体名。
- 接收 Trap 方式发送的告警信息的服务器地址。

操作步骤

步骤 1 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 在 iBMC WebUI，选择“维护诊断 > 告警上报”。

步骤 3 在“Trap 报文通知”区域框，开启 Trap 功能。

步骤 4 设置 Trap 属性。

1. 在“Trap 版本”中，选择 Trap 方式上报事件需遵循的 SNMP Trap 协议版本。
   SNMP Trap 协议提供“SNMPv1”、“SNMPv2c”和“SNMPv3”三种版本。
   默认取值：“SNMPv1”。

   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。
2. （可选）在“选择 V3 用户”下拉列表中，选择 Trap V3 协议使用的 iBMC 用户。
3. 在“Trap 模式”中，选择 Trap 信息上报时，采用的 Trap 模式。
   - “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。
4. 在“Trap 主机标识”中，选择 Trap 信息上报时，识别信息来源的主机标识。
   “Trap 主机标识”提供“单板序列号”、“产品资产标签”和“主机名”三种主机标识。

步骤 5 设置告警发送级别。

步骤 6 设置 Trap 服务器和报文格式。

1. 选择发送告警通道。
   在 iBMC WebUI 中，最多可以定义四个发送告警通道。
   单击“编辑”，显示指定通道的编辑区域框。
2. 启用发送告警通道。
3. 输入接收 Trap 方式发送的告警信息的服务器地址。
   服务器地址支持 IPv4 和 IPv6。
4. 输入接收 Trap 方式发送的告警信息的端口号。
   默认取值：162。
5. 选择 Trap 格式中每个关键字段之间的分隔符。
6. 选择需要上报的关键字。
7. 选择显示 Trap 格式中每个关键字的名称。
8. 单击“保存”。
   显示“操作成功”，表示 Trap 功能及其设置正式生效。
9. 单击“测试”。

显示“操作成功”，表示该通道可用。

----结束

6.4 配置 iBMC WebUI SMTP

操作场景

iBMC WebUI 的“维护诊断 > 告警上报”提供“SMTP 功能”，可以将服务器产生的告警和事件以电子邮件方式，通过 SMTP 服务器转发到目标邮箱。

必备事项

数据

进行配置之前，请先规划好配置过程中所需数据：

- SMTP 服务器的地址。
- 发件人邮件信息。
  - 发件人用户名和密码
  - 发件人邮件地址
  - 邮件主题
- 收件人邮件信息。
  - 接收人邮件地址
  - 接收人邮件地址描述信息

操作步骤

步骤 1 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 在 iBMC WebUI，选择“维护诊断 > 告警上报”。

步骤 3 在“邮件通知”区域框，开启 SMTP 功能。

步骤 4 输入 SMTP 服务器的地址。

SMTP 服务器的 IPv4 或 IPv6 地址。

步骤 5 选择是否启用 TLS 功能。

- 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，建议启用 TLS 加密。
- 在 iBMC WebUI 启用 TLS 加密时，SMTP 服务器需要配置身份验证和配置支持 TLS 后，才能接收到邮件。

步骤 6 选择是否使用匿名。

- 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。

步骤 7 设置邮件信息。

1. 输入发件人用户名及密码。

说明

- “是否使用匿名”选择“是”时，不需要验证用户名及其密码。
- 如果使用电子邮箱服务的用户在 SMTP 服务器端修改了密码，请在登录“告警设置”界面后，在“发件人密码”文本框中重新输入修改后的密码。

2. 输入发件人邮件地址。
3. 输入邮件主题。

   SMTP 邮件主题提供主题附带功能，可以选择“主机名”、“单板序列号”和“产品资产标签”作为邮件主题的附加内容。

步骤 8 设置告警发送级别。

步骤 9 启用接收告警的邮件地址。

1. 输入接收告警邮件地址。
2. 输入接收告警邮件地址的描述信息。

步骤 10 单击“保存”。

显示“操作成功”，表示 SMTP 功能及其设置正式生效。

步骤 11 单击“测试”，显示“操作成功”。

显示“操作成功”，表示测试邮件已正常发送，请在接受告警的邮箱进行验证。

----结束

6.5 配置目录服务功能

6.5.1 配置目录服务器

配置 LDAP 功能时，iBMC 支持与 Windows AD、Linux OpenLDAP 和 FreeIPA 的对接；配置 Kerberos 功能时，iBMC 支持与 Windows AD 的对接。

此处以 Windows Server 2012 R2 Enterprise 为例说明目录服务器的简要配置过程。如果已存在可正常使用的目录服务器，请忽略此章节。

前提条件

- 用于搭建目录服务器的设备已正常运行。
- 已获取 Windows Server 2012 R2 Enterprise 安装光盘或 ISO 镜像文件。

操作步骤

步骤 1 安装操作系统。

1. 通过服务器 iBMC WebUI 设置服务器下次启动设备为光驱。
2. 将操作系统安装光盘放入光驱，或将操作系统镜像文件通过 iBMC 虚拟光驱挂载。
3. 重启服务器进入操作系统安装引导界面。
4. 在操作系统选择界面选择要安装的系统为“Windows Server 2012 R2 Datacenter”。
5. 单击“下一步”。

   跟随引导程序指引逐步完成 OS 安装。

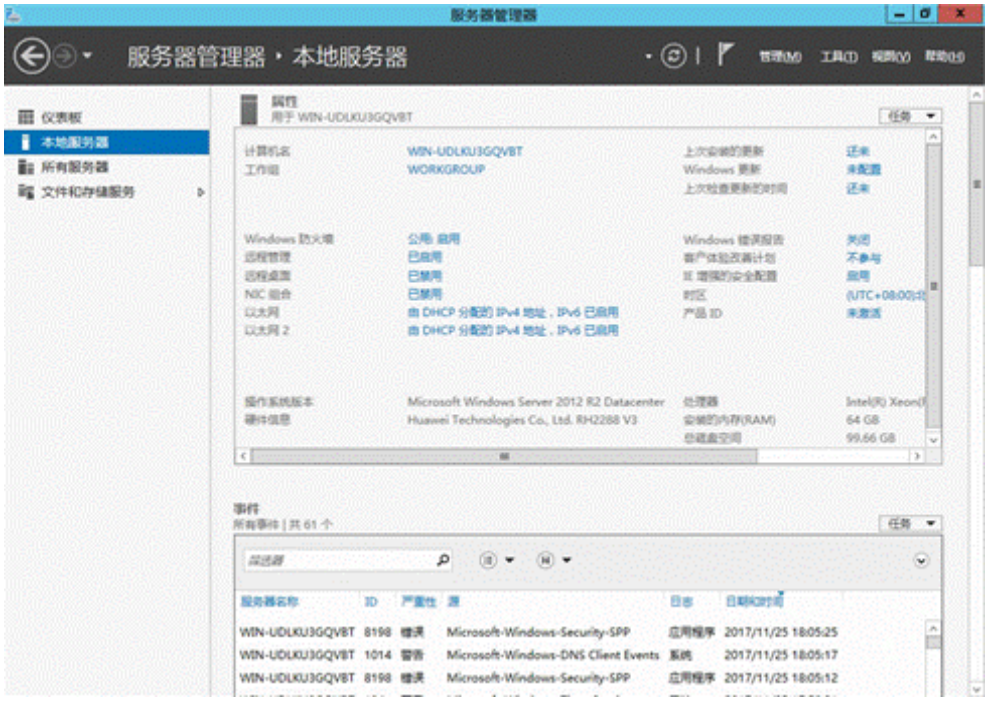
步骤 2 安装 DNS 服务。

1. 在“开始”菜单中选择服务器管理器。

   打开“服务器管理器”。
2. 在左侧导航树中选择“本地服务器”。

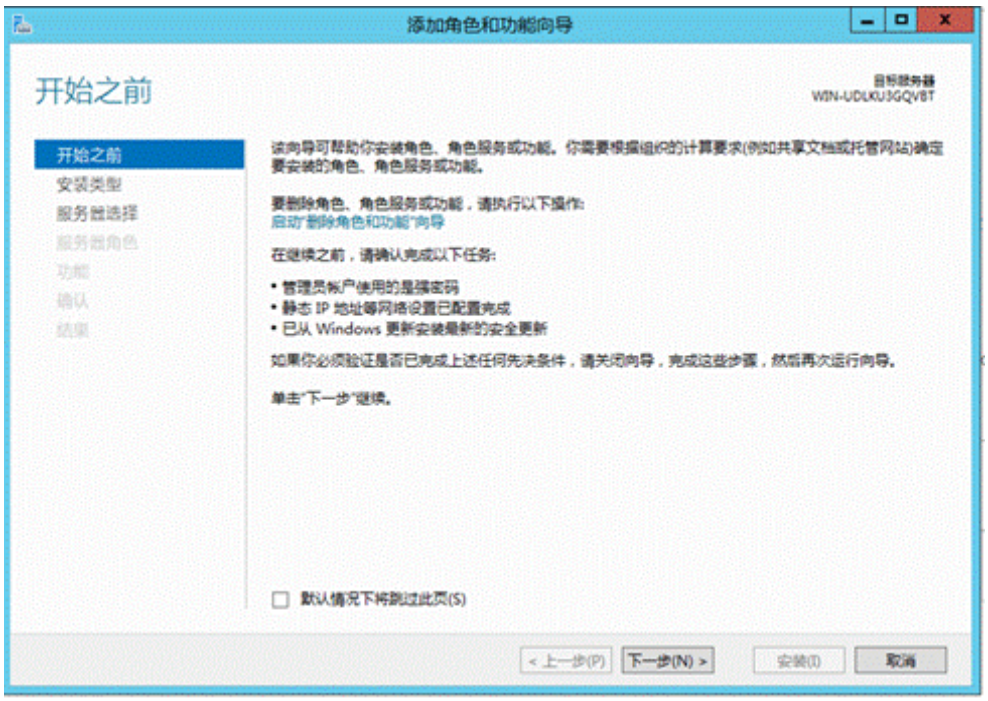
   右侧显示本地服务器的“属性”窗口，如图 6-3 所示。

图6-3 本地服务器属性



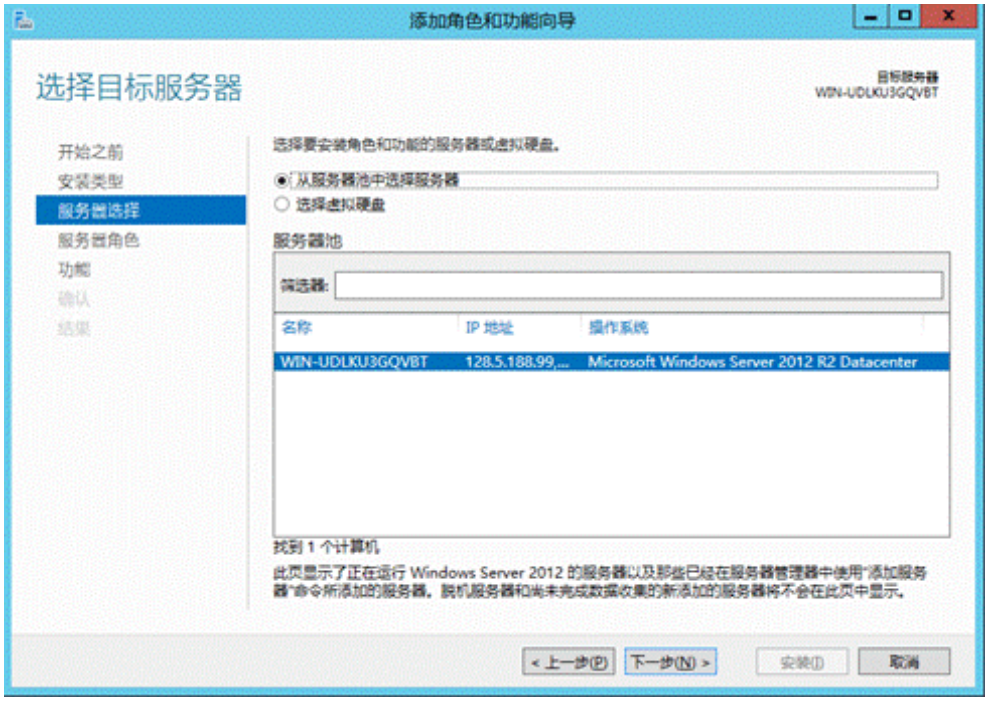
3. 在右上角的“管理”菜单中选择“添加角色和功能”。
   打开“添加角色和功能向导”，如图 6-4 所示。

图6-4 添加角色和功能向导



4. 单击“下一步”。
   进入“安装类型”选择界面。
5. 选择“基于角色或基于功能的安装”，并单击“下一步”。
   进入“服务器选择”界面，如图 6-5 所示。

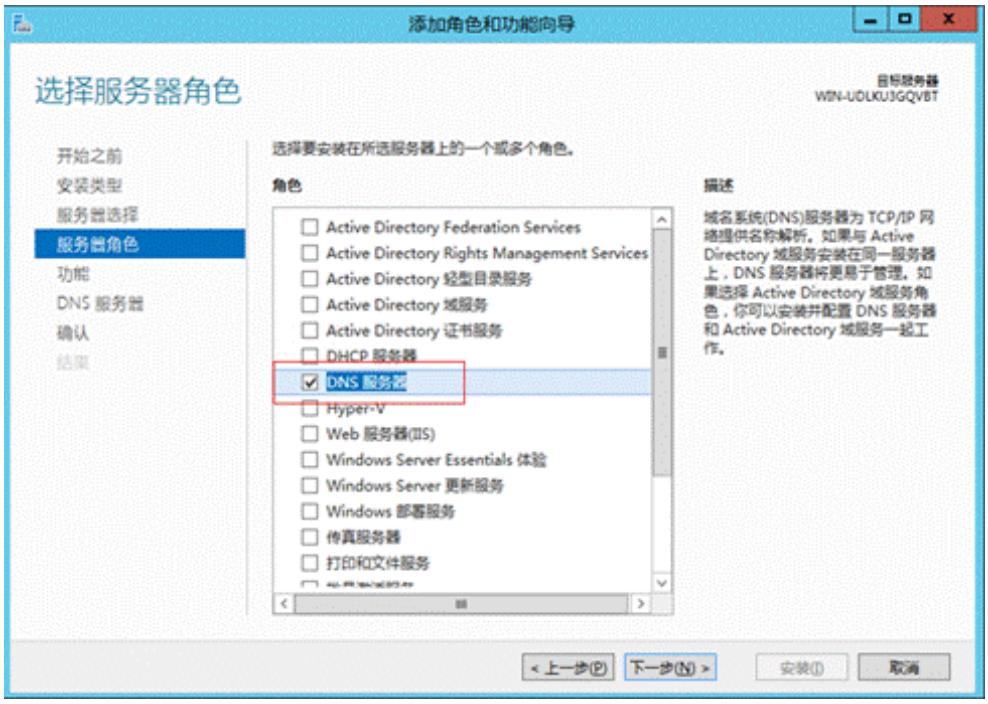
图6-5 选择目标服务器



6. 选择“从服务器池中选择服务器”，并在“服务器池”中选择本机后，单击“下一步”。

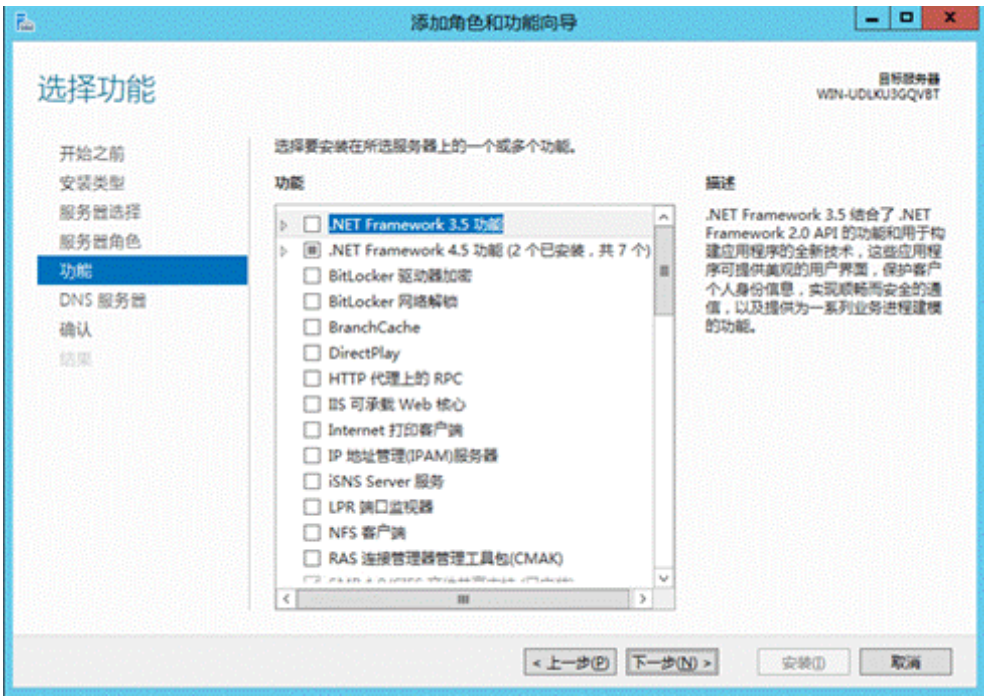
   进入“选择服务器角色”界面，如图 4 选择服务器角色所示。

图6-6 选择服务器角色



7. 在“角色”列表中勾选“DNS 服务器”。
   弹出操作确认窗口。
8. 单击“添加功能”。
   返回“选择服务器角色”界面。
9. 单击“下一步”。
   打开“选择功能”界面，如图 6-7 所示。

图6-7 选择功能



10. 勾选“.NET Framework 4.5 功能”并单击“下一步”。
    打开“DNS 服务器”界面。
11. 单击“下一步”。
    打开操作确认界面。
12. 单击“安装”。
    显示 DNS 服务安装进度条。
13. 安装完成后单击“关闭”。
    返回“本地服务器”界面。

步骤 3 安装 AD 服务。

参考步骤 2，继续添加新服务。

1. 在如图 6-7 所示界面中勾选“Active Directory 域服务”。
   弹出操作确认窗口。
2. 单击“添加功能”。

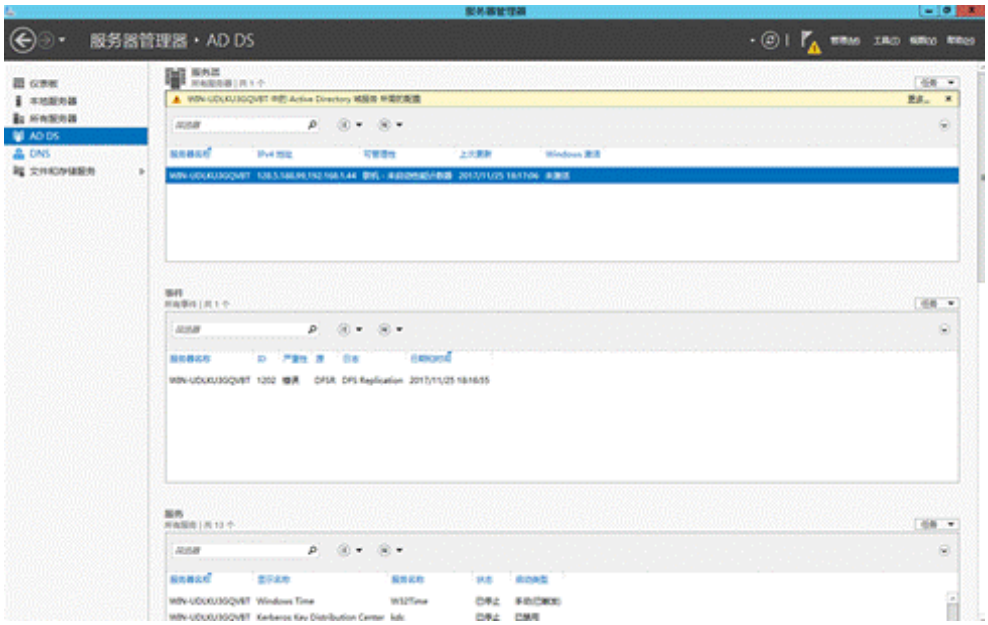
返回“选择服务器角色”界面。

3. 单击“下一步”。
   打开“选择功能”界面。
4. 勾选“.NET Framework 4.5 功能”并单击“下一步”。
   打开“Active Directory 域服务”界面。
5. 单击“下一步”。
   打开操作确认界面。
6. 单击“安装”。
   显示 Active Directory 域服务安装进度条。
7. 安装完成后单击“关闭”。
   返回“本地服务器”界面。

步骤 4 配置 AD 服务。

1. 在“服务器管理器”左侧导航树中选择“AD DS”。
   右侧显示“AD DS”属性，如图 6-8 所示。

图6-8 AD DS 属性



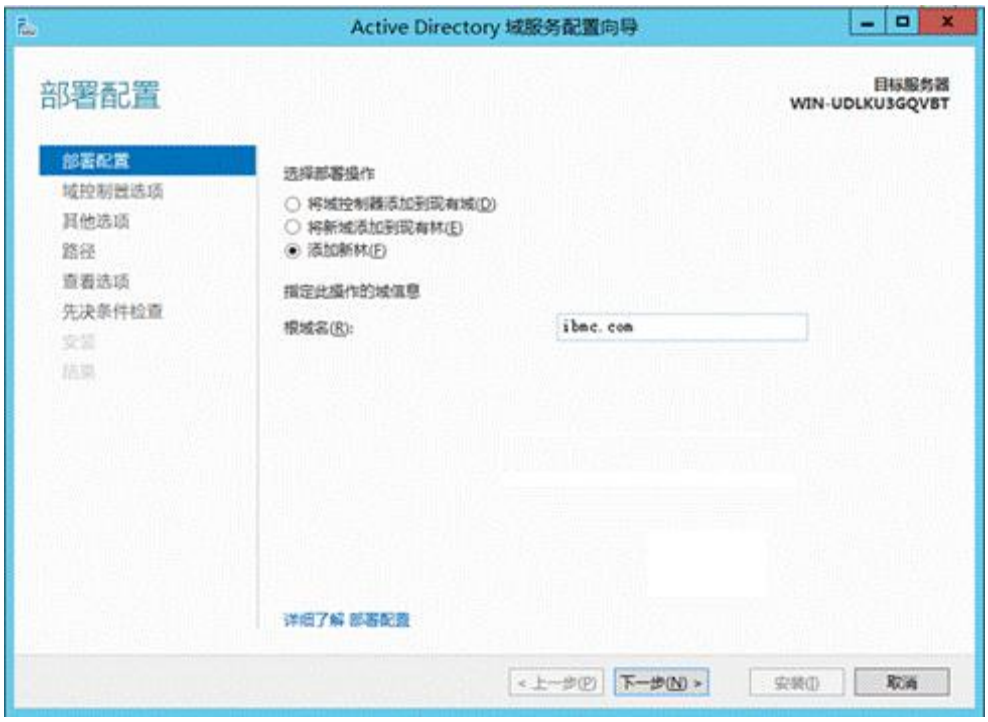
2. 单击页面右上方告警信息中的“更多...”。
   打开“所有服务器任务详细信息”窗口，如图 6-9 所示。

图6-9 所有服务器任务详细信息

3. 单击“将此服务器提升为域控制器”。

   打开“Active Directory 域服务配置向导”，如图 6-10 所示。

图6-10 Active Directory 域服务配置向导



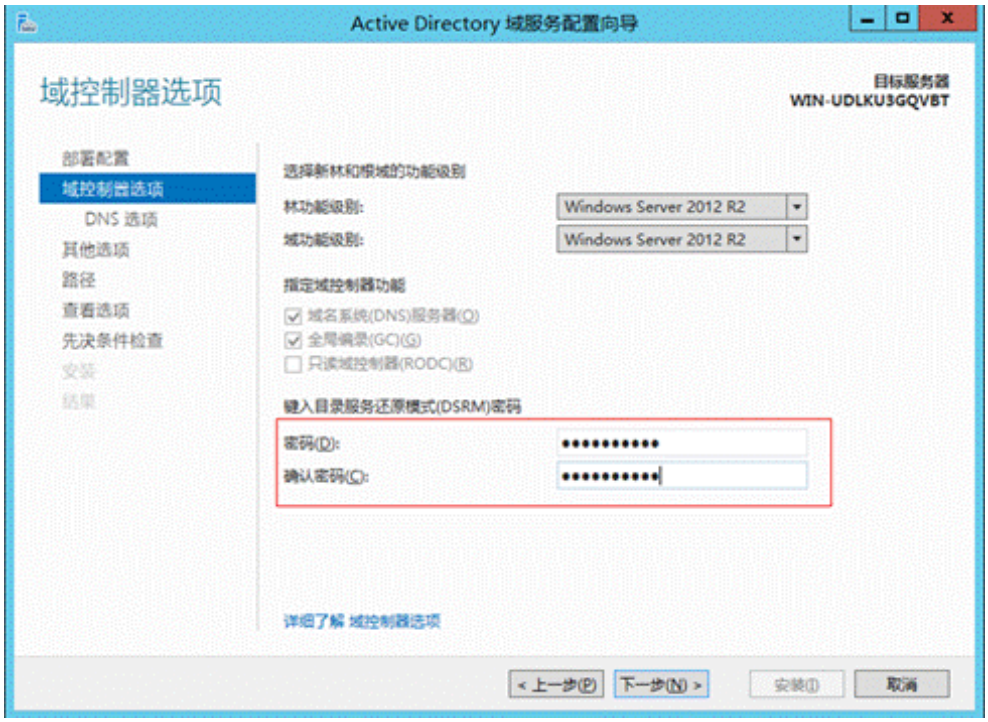
4. 选择“添加新林”并在“根域名”后的文本框中输入 AD 域名（例如“ibmc.com”），单击“下一步”。

   打开“域控制器选项”界面，如图 6-11 所示。

说明

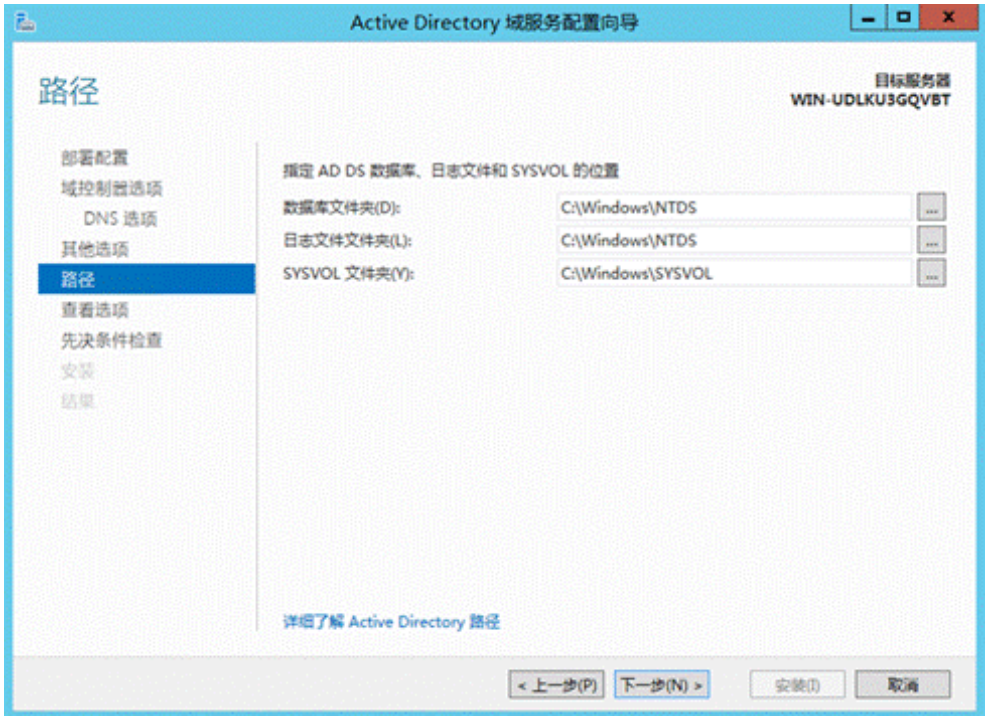
域名字符区分大小写，配置时请严格按照规划的域名来输入。

图6-11 域控制器选项



5. 按照实际需要设置 AD 域控制器的密码，单击“下一步”。
6. 按照指引继续单击“下一步”，直至出现如图 6-12 所示界面。

图6-12 域服务路径

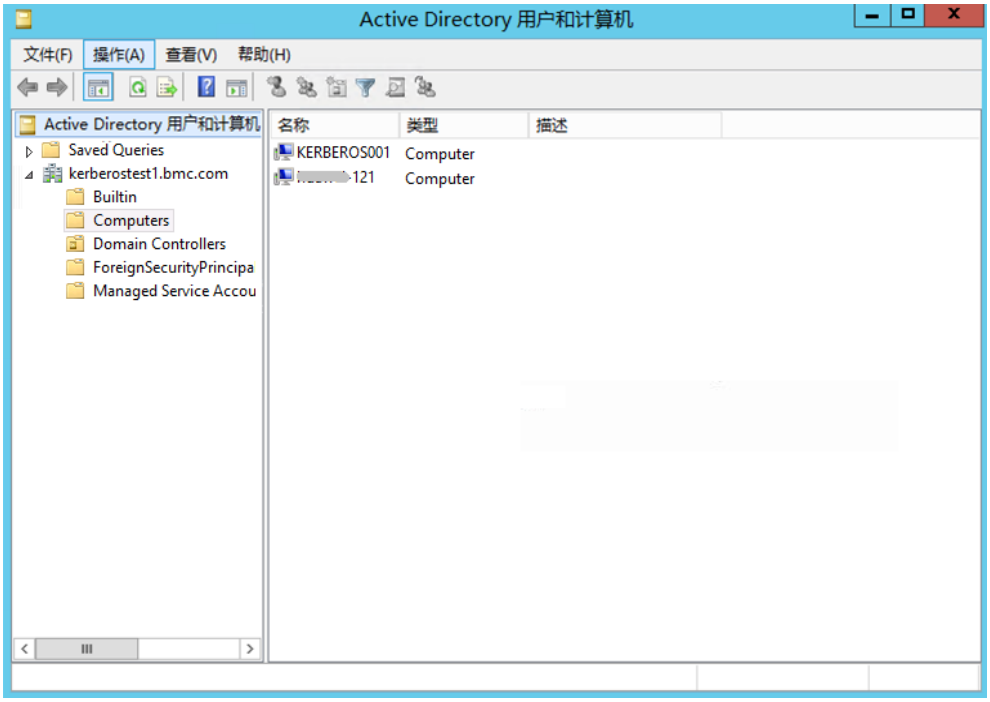


7. 按照实际需求设置 AD 域服务相关路径，单击“下一步”。
   您也可以保持默认配置，不做修改。
8. 在后续页面中依次单击“下一步”。
9. 当出现“先决条件检查”界面时，单击“安装”。
   AD 域服务配置完成后，操作系统将自动重启。

步骤 5（对于 LDAP 功能为非必选步骤）配置 AD 主机名。

1. 在“服务器管理器”页面右上方的工具栏中单击“工具”，在下拉菜单中选择“Active Directory 用户和计算机”。
2. 在“Active Directory 用户和计算机”左侧导航树中选择“Computers”。
   右侧显示主机名列表，如图 6-13 所示。

图6-13 配置 AD 主机名路径



3. 在主机名列表空白处单击鼠标右键，新建主机名，例如“host”。

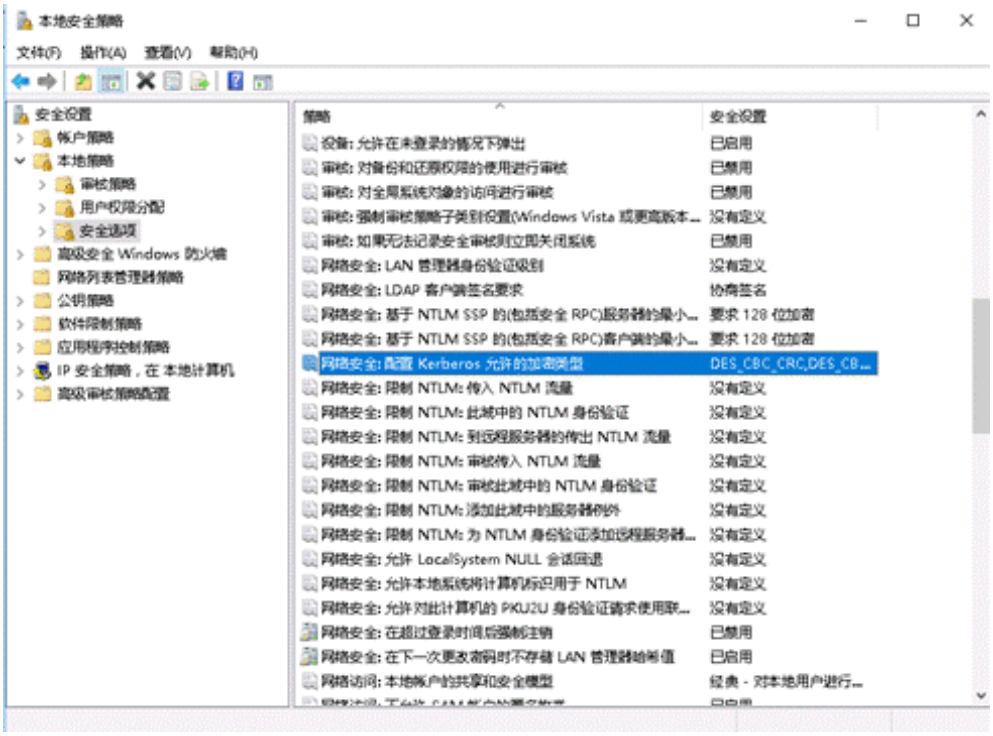
说明

此处新建的主机名为后续在 iBMC WebUI 配置主机名时可使用的主机名，请做好记录。iBMC WebUI 配置主机名步骤请参见本文档 6.6.3 在 iBMC 侧配置 Kerberos 功能章节的步骤 1。

步骤 6 （对于 LDAP 功能为非必选步骤）配置 AD 域支持的加密算法。

1. 在“服务器管理器”页面右上方的工具栏中单击“工具”，在下拉菜单中选择“本地安全策略”。
2. 在“本地安全策略”左侧导航树中选择“本地策略 > 安全选项”，右侧显示安全策略类型，如图 6-14 所示。

图6-14 配置本地安全策略



3. 在右侧安全策略类型中，选中“网络安全：配置 Kerberos 允许的加密类型”并单击鼠标右键，在下拉菜单中选择“属性”，打开属性列表。
4. 确保勾选“本地安全设置”中的以下加密算法：
   - AES128_HMAC_SHA1
   - AES256_HMAC_SHA1

说明

对于跨域场景登录，还需要配置域间的信任关系，才能确保安全的加密算法可以认证成功。

步骤 7（对于 LDAP 功能为非必选步骤）在 AD 域配置服务端支持的加密算法。

1. 在“服务器管理器”页面右上方的工具栏中单击“工具”，在下拉菜单中选择“ADSI 编辑器”。
2. 在“ADSI 编辑器”左侧导航树中选择“Computers”。

   右侧显示主机名列表。
3. 选中待操作的主机名并单击鼠标右键，在下拉菜单中选择“属性”，打开属性列表。
4. 在属性列表中选中“msDS-SupportedEncryptiontypes”。
5. 单击“编辑”，打开“整数属性编辑器”并在输入框中输入服务端支持的加密算法对应的数值。

说明

客户端支持的加密算法只有 **AES128-CTS-HMAC-SHA1-96** 和 **AES256-CTS-HMAC-SHA1-96**，根据表 6-1，分别对应取值为 **8** 和 **16**。因为服务端配置的加密算法必须与客户端支持的加密算法配置成一致才能保证协商成功，因此此处的加密算法取值根据实际情况必须配置为 **8**，**16** 或 **24**。

表6-1 加密算法取值与代表的加密算法类型关系表

加密算法取值	代表的加密算法类型
8	AES128-CTS-HMAC-SHA1-96
16	AES256-CTS-HMAC-SHA1-96
24	AES128-CTS-HMAC-SHA1-96 和 AES256-CTS-HMAC-SHA1-96

6. 单击“确认”。

步骤 8 （对于 LDAP 功能为非必选步骤）生成密钥表。

1. 在 AD 域服务中打开 cmd。
2. 使用 **ktpass** 命令生成密钥表。

说明

建议使用 **ktpass** 命令生成密钥表时，使用 **AES128-CTS-HMAC-SHA1-96** 或 **AES256-CTS-HMAC-SHA1-96** 加密算法，且使用的加密算法类型必须与服务端实际使用的加密算法类型保持一致，即：

- 若服务端加密算法取值配置为 **8**，必须使用 **AES128-CTS-HMAC-SHA1-96** 加密算法生成密钥表。
- 若服务端加密算法取值配置为 **16** 或 **24**，必须使用 **AES256-CTS-HMAC-SHA1-96** 加密算法生成密钥表。

使用示例：

```
C:\Users\Administrator>ktpass -out c:\kerberos\admin.keytab +rndPass -ptype
KRB5_NT_SRV_HST -mapuser admin$@it.software.com -princ
HTTP/admin.it.software.com@IT.SOFTWARE.COM -crypto AES128-SHA1
Targeting domain controller: WIN-D0VNHFBODLC.it.software.com
Successfully mapped HTTP/admin.it.software.com to ADMIN$.
WARNING: Account ADMIN$ is not a user account (uacflags=0x1021).
WARNING: Resetting ADMIN$'s password may cause authentication problems if
ADMIN$ is being used as a server.

Reset ADMIN$'s password [y/n]?  y
Password succesfully set!8
Key created.Output keytab to c:\kerberos\admin.keytab:
Keytab version: 0x502
keysize 86 HTTP/admin.it.software.com@IT.SOFTWARE.COM ptype 3 (KRB5 NT SRV HST)
vno 3 etype 0x11 (AES128-SHA1) keylength 16 (0xd517c317bf1a6f333a45f3282d0b69a9)
```

步骤 9 安装 CS 服务。

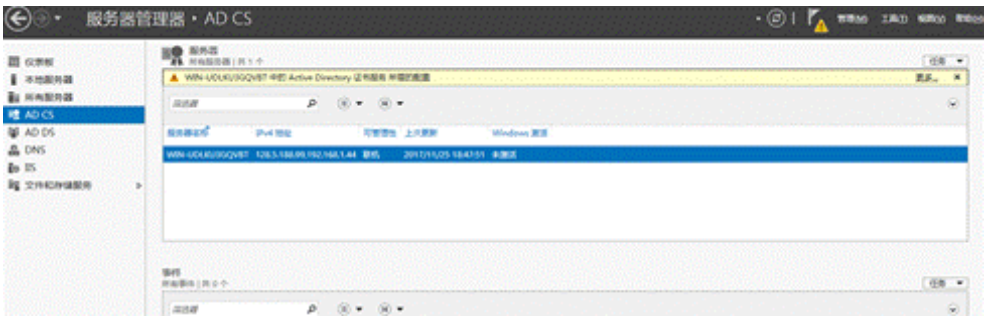
参考安装 DNS 服务，继续添加新服务。

1. 在如图 6-7 所示界面中勾选“Active Directory 证书服务”。
   弹出操作确认窗口。
2. 单击“添加功能”。
   返回“选择服务器角色”界面。
3. 单击“下一步”。
   打开“选择功能”界面。
4. 勾选“.NET Framework 4.5 功能”并单击“下一步”。
   打开“AD CS”界面。
5. 单击“下一步”。
   打开“选择角色服务”界面。
6. 勾选“证书颁发机构”和“证书颁发机构 Web 注册”并单击“下一步”。
   弹出操作确认窗口。
7. 单击“添加功能”。
   返回“选择角色服务”界面。
8. 连续单击“下一步”。
9. 在“确认安装所选内容”界面单击“安装”。
   显示 CS 服务安装进度条。
10. 安装完成后单击“关闭”。

步骤 10 配置 CS 服务。

1. 返回“服务器管理器”主界面。
2. 在左侧导航树中选择“AD CS”。
   右侧显示“AD CS”属性，如图 6-15 所示。

图6-15 AD CS 属性

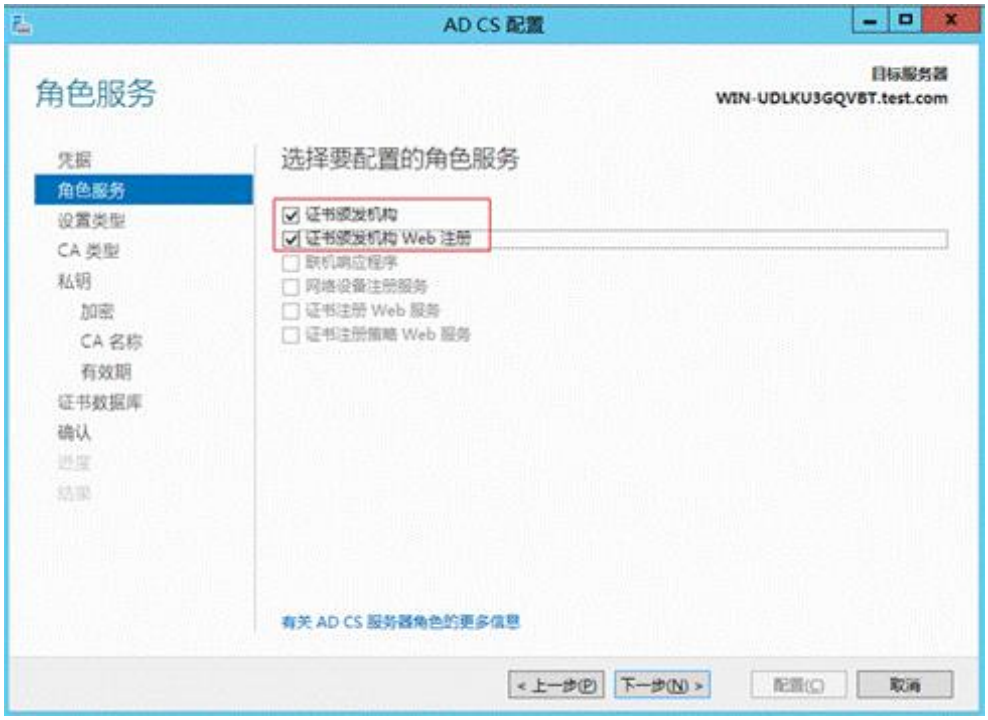


3. 单击页面右上方告警信息中的“更多...”。
   打开“所有服务器任务详细信息”窗口，如图 6-16 所示。

图6-16 所有服务器任务详细信息

4. 单击“配置目标服务器上的 Active Directory 证书服务”。
   打开“AD CS 配置”界面。
5. 单击“下一步”。
   打开“角色服务”界面，如图 6-17 所示。

图6-17 角色服务



6. 勾选“证书颁发机构”和“证书颁发机构 Web 注册”，单击“下一步”。

打开“设置类型”界面。

7. 勾选“企业 CA”，单击“下一步”。

   打开“CA 类型”界面。

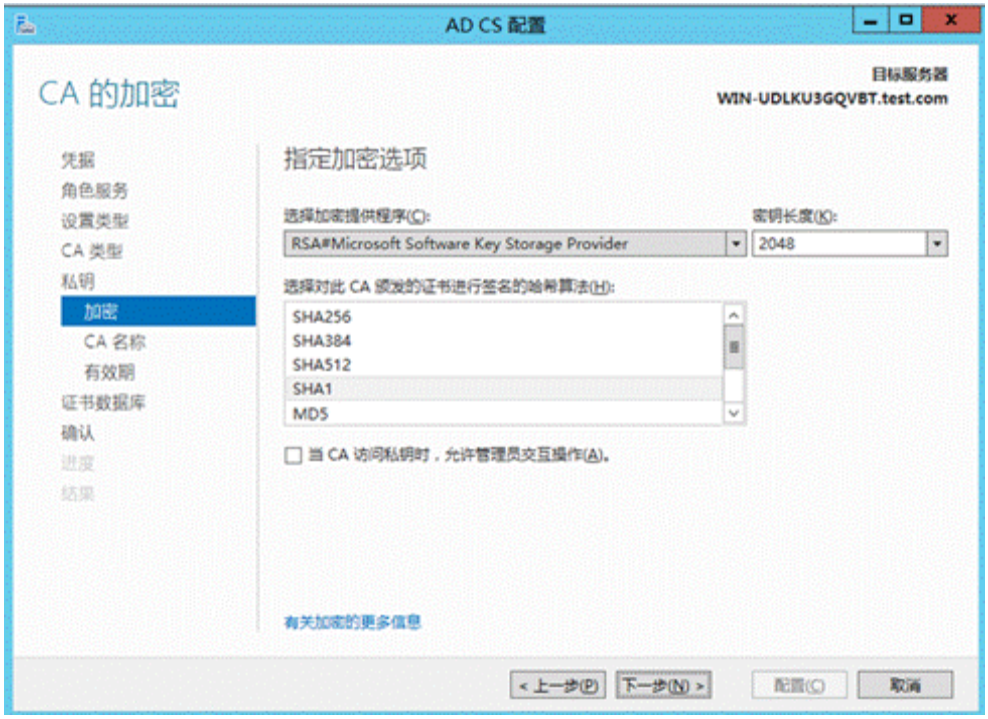
8. 勾选“根 CA”，单击“下一步”。

   打开“私钥”界面。

9. 勾选“创建新的私钥”，单击“下一步”。

   打开“CA 的加密”界面，如图 6-18 所示。

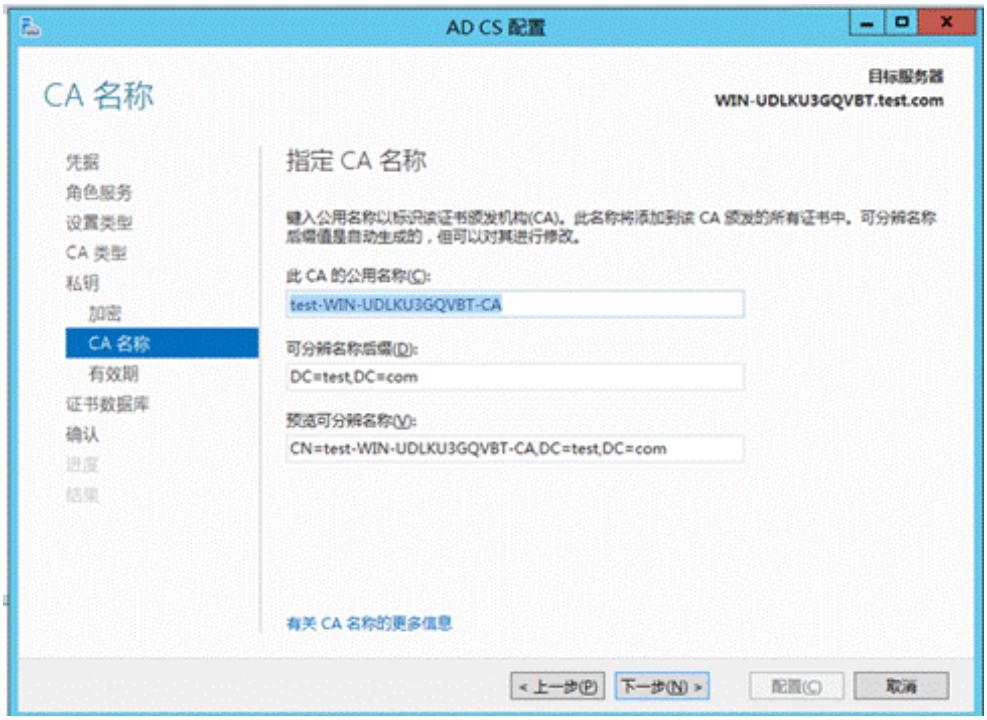
图6-18 CA 的加密



10. 指定加密提供程序为“RSA”、密钥长度为“2048”、哈希算法为“SHA1”，单击“下一步”。

    打开“CA 名称”界面，如图 6-19 所示。

图6-19 CA 名称



11. 按照规划，设置“此 CA 的公用名称”，单击“下一步”。
    打开“有效期”界面。
12. 按照实际需要设置有效期，单击“下一步”。
    打开“CA 数据库”界面。
13. 指定 CA 数据库的路径，单击“下一步”。
    打开“确认”界面。
14. 单击“配置”。
    显示 AD 证书服务配置进度条。
15. 配置完成后，单击“关闭”。

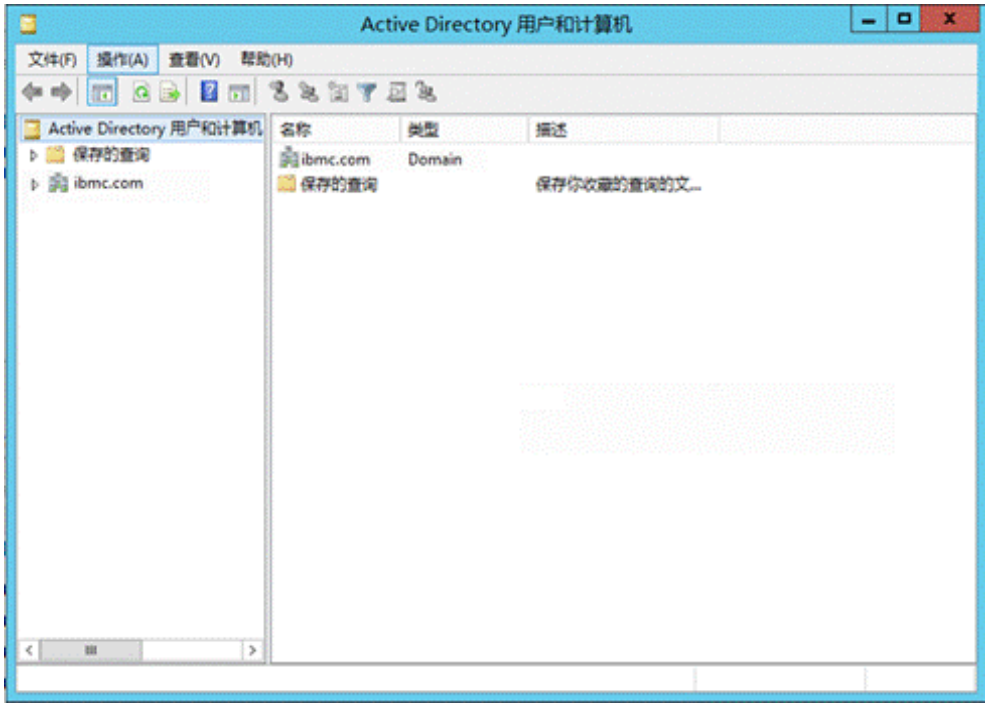
步骤 11 重启服务器使配置生效。

步骤 12 新建组织单位。

您可以根据实际需要在服务器上规划新的组织单位，可以在任意节点下新建组织单位，下面以新建一级节点及其子节点为例进行说明。

1. 登录服务器操作系统。
2. 在“服务器管理器”左侧导航树中选择“本地服务器”。
3. 在页面右上角的“任务”下拉列表中选择“Active Directory 用户和计算机”。
   打开域的服务组件，如图 6-20 所示。

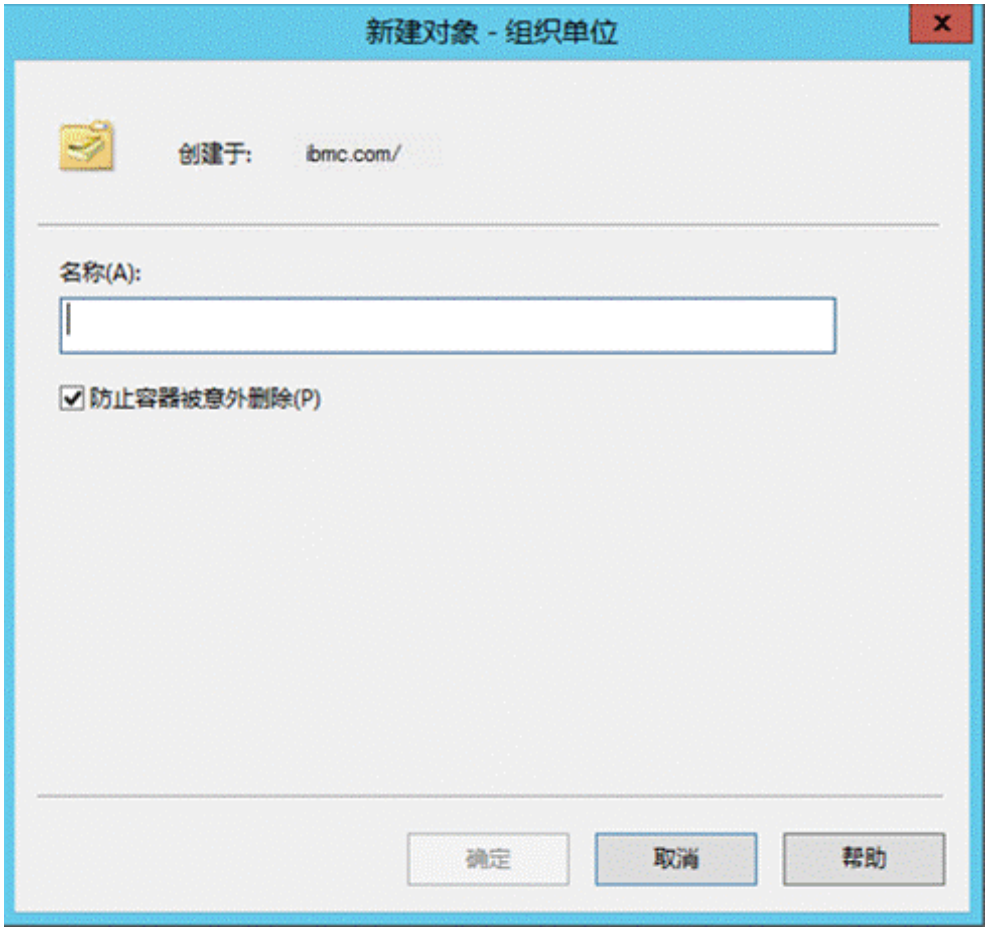
图6-20 服务器管理器



4. 右键单击服务器的顶级节点（如“ibmc.com”）打开操作菜单，并选择“新建 > 组织单位”。

   打开组织新建窗口，如图 6-21 所示。

图6-21 新建组织



5. 在“名称”文本框中输入组织名称（例如“company”），单击“确定”。

   在服务器的组织中，可看到新建的组织（例如“company”）。

6. 右键单击新创建的组织（例如“company”）打开操作菜单，并选择“新建 > 组织单位”，创建子组织（例如“department”）。

   创建完成后，可在一级节点下，看到新建的子节点。

7. 可根据实际需求，重复步骤 12.4～步骤 12.6，创建多个组织单位。

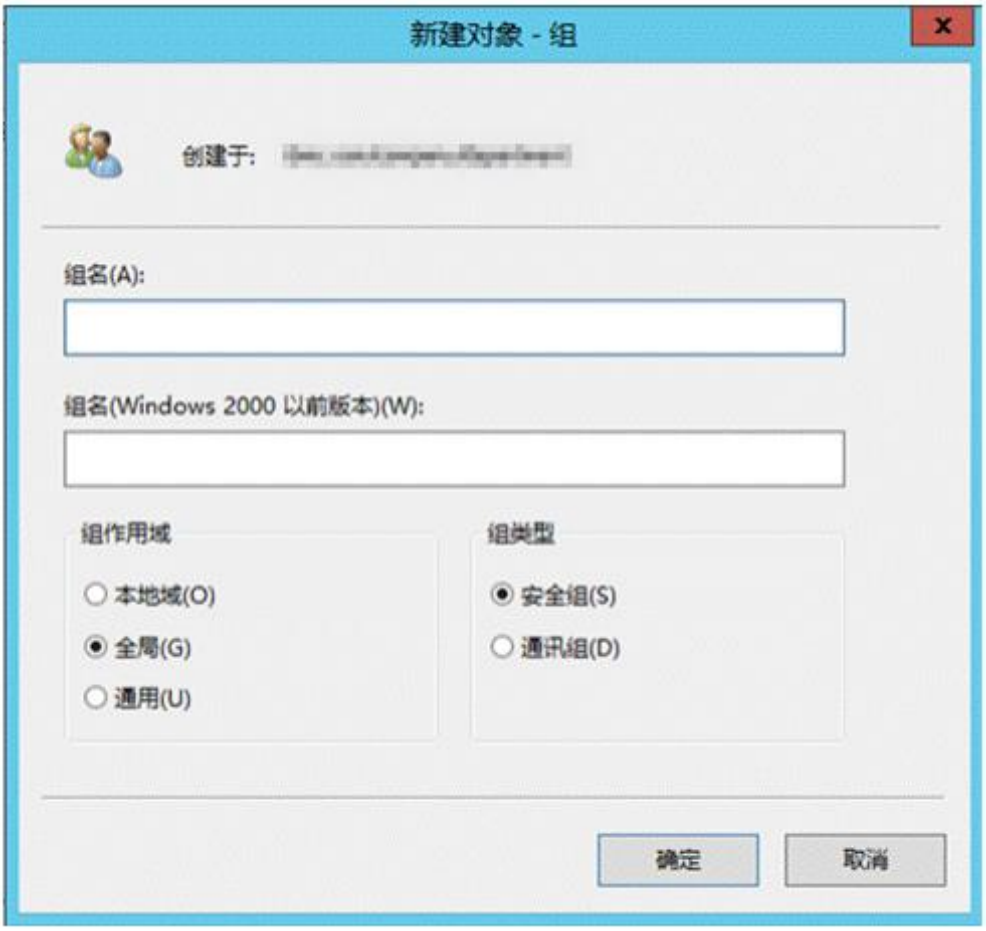
步骤 13 新建组。

您可以根据实际需求，在任意节点下新建组。

1. 右键单击要创建组的节点（例如“department”）打开操作菜单，并选择“新建 > 组”。

   打开新建组窗口，如图 6-22 所示。

图6-22 新建组



2. 在“组名”文本框中输入 LDAP 组名称（例如“info_group1”），并勾选组作用域和组类型，单击“确定”。

说明

“组名”和“组名（Windows 2000 以前版本）”建议保持一致。

在指定的组织下可以看到新建的组（例如“info_group1”）。

3. 可根据实际需要，重复 13.a～13.b，创建多个组。

步骤 14 新建用户。

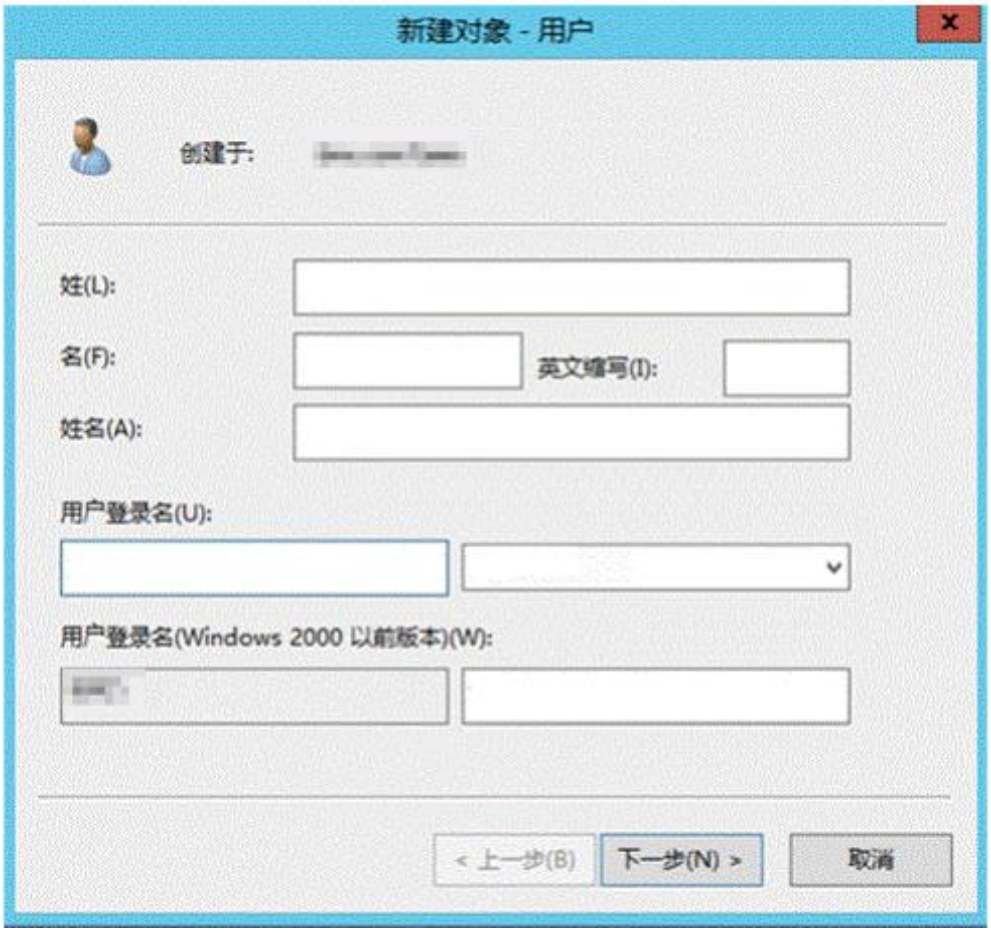
可以在所需的任何目录下新增用户。一般情况下，建议在“Users”下新建所需用户。

1. 右键单击要新建用户的节点（如“Users”）打开操作菜单，并选择“新建 > 用户”。
2. 在打开的“新建角色-用户”窗口中，输入新用户信息，如图 6-23 所示。

说明

其中，“用户登录名”为后续登录 iBMC WebUI 时可使用的域名，此处请做好记录。

图6-23 新建用户



3. 单击“下一步”。
   弹出密码设置窗口，如图 6-24 所示。

图6-24 设置密码

4. 在“密码”和“确认密码”的文本框中输入密码，并勾选下方的密码策略，然后单击“下一步”。

须知

密码策略请勿设置为“用户下次登录时须更改密码”。

弹出用户信息确认窗口。

5. 单击“完成”。

   在“Users”列表中可看到新创建的用户。

6. 重复上述操作，可在“Users”中新建更多用户。

步骤 15 将用户添加到组。

可以通过对组的操作来添加用户，也可以通过对用户操作来添加到组，此处以对用户操作为例进行说明。

1. 右键单击步骤 10 中创建的用户打开操作菜单，并选择“添加到组”。

打开选择组窗口，如图 6-25 所示。

图6-25 选择组

2. 在“输入对象名称来选择”文本框中输入要加入的组名（例如“info_group1”），单击“确定”。

   提示操作成功。

3. 可根据实际需要，重复上述操作，可将多个用户添加到组。

----结束

6.5.2 在 iBMC 侧配置 LDAP 功能

操作场景

iBMC WebUI 的“LDAP”提供“LDAP 用户组”功能，设置 LDAP 用户后，可以直接使用 LDAP 用户访问 iBMC。

说明

- LDAP（Lightweight Directory Access Protocol，轻量目录访问协议），作为一个统一认证的解决方案，主要的优点就在能够快速响应用户的查找需求。
- 关于域控制器、用户域、隶属于用户域的 LDAP 用户名及其密码的创建请参见关于域控制器的相关文档。iBMC 系统仅提供 LDAP 用户的接入功能。
- 启用 LDAP 功能，使用 LDAP 帐户登录 iBMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。

必备事项

数据

- 可用的 LDAP 服务器信息，包括 LDAP 服务器地址、域名、主机名、用户应用文件夹以及 LDAP 用户所属角色组的名称。
- iBMC 当前用户的密码。

操作步骤

步骤 1 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 配置 LDAP 服务器信息。

1. 在 iBMC WebUI，选择“用户&安全 > LDAP”。
2. 单击“LDAP 使能”后的  ，此按钮变为  ，表示 LDAP 功能已经启用。
3. 配置 LDAP 服务器参数。

   必须配置的参数包括：

   - 输入 LDAP 服务器的 IP 地址，如“192.168.66.66”。
   - 输入 LDAP 服务器端口号。
   - 输入 LDAP 服务器的域名，如“ibmc.com”，域名和 LDAP 服务器下的域名保持一致。
   - 输入当前登录 iBMC 的用户密码。

     其它参数请根据实际需要进行设置。相关参数说明请参考“LDAP”章节。
4. 单击“保存”。

步骤 3 （可选）导入 LDAP CA 证书

若开启了证书验证功能，需要导入 LDAP CA 证书。请用户自行从 CA 证书颁发机构获取证书文件。

1. 配置 iBMC WebUI DNS 地址为 LDAP 服务器地址，详细操作请参见 LDAP 章节。
2. 单击“上传证书”后的“浏览”，选择要上传的根证书，证书支持.cer、.pem、.cert 和.crt 格式。
3. 单击“上传”，上传成功后，证书状态会显示 LDAP CA 证书已上传。

说明

请定期更新证书，否则可能存在安全风险。

步骤 4 配置 iBMC LDAP 组信息

1. 在“LDAP 用户组”区域单击“添加”或  ，进入“添加组”编辑区域框。
2. 输入 iBMC 的用户密码。修改 LDAP 信息前需要输入当前登录的用户密码。
3. 配置 LDAP 组参数。
   - 输入 LDAP 用户所属角色组的名称，如“info_group1”（即 6.5.1 配置目录服务器中创建的 LDAP 组）。

- 输入 LDAP 组应用所在文件夹。

  和 LDAP 服务器下用户的组所在的组织单位名保持一致，如“company/department”（即 6.5.1 配置目录服务器中涉及的最下层组织单位），最大长度为 255。
- 选择已设定的登录规则。
- 选择登录接口。
- 选择 LDAP 组权限。

4. 单击“保存”。

步骤 5 使用域帐号登录 iBMC

1. 输入已在 LDAP 服务器生效的帐号密码。
2. 在域名下拉列表，选择对应 LDAP 服务器的域名。
3. 单击“登录”。

----结束

6.5.3 在 iBMC 侧配置 Kerberos 功能

操作场景

iBMC WebUI 的“Kerberos”提供“Kerberos 用户组”功能，设置 Kerberos 用户后，可以直接使用 Kerberos 用户访问 iBMC。

说明

- Kerberos 是一种网络认证协议，通过密钥系统为客户机或服务器应用程序提供强大的认证服务。
- iBMC 系统仅提供 Kerberos 用户的接入功能。
- 启用 Kerberos 功能，使用 Kerberos 帐户登录 iBMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。

必备事项

数据

- 可用的 Kerberos 服务器信息，包括 Kerberos 服务器地址、领域以及 Kerberos 用户所属角色组的名称。
- 在 Windows AD 中，为 iBMC 生成密钥表文件。生成密钥表的详细操作请参见本文档 6.5.1 配置目录服务器的步骤 8。
- iBMC 当前用户的密码。

操作步骤

步骤 1 配置 iBMC 主机名和域名。

说明

此处配置的主机名和域名必须与 AD 域服务中的主机名和域名相同。AD 域服务中配置主机名步骤请参见本文档 6.5.1 配置目录服务器的步骤 5。

1. 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。
2. 配置 iBMC 主机名和 DNS。详细信息请参见本文档 6.6 配置 iBMC WebUI DNS（手动）。
3. 配置 iBMC 时区与 Kerberos 服务器时区一致。
   a. 在 iBMC WebUI，选择“iBMC 管理 > 时区&NTP”。
   b. 在“地区”和“时区”下拉列表中，选择要设置的参数。
   c. 单击“保存”。
4. 开启 NTP。

说明

此步骤是为了确保 iBMC 时间与 Kerberos 服务器的时间一致。

   a. 在 iBMC WebUI，选择“iBMC 管理 > 时区&NTP”。
   b. 在“NTP 功能”区域中，选择“开启”。
   c. 单击“保存”。

步骤 2 配置 iBMC Kerberos 服务端信息。

1. 在 iBMC WebUI，选择“用户&安全 > Kerberos”。
2. 单击“Kerberos 使能”后的  ，此按钮变为  ，表示 Kerberos 功能已经启用。
3. 配置 Kerberos 服务器参数。

   必须配置的参数包括：

   - 输入 Kerberos 服务器的领域，如“ADMIN.COM”，领域和 Kerberos 服务器下的领域保持一致。
   - 输入 Kerberos 服务器的 IPv4 地址，如“192.168.66.66”。
   - 输入 Kerberos 服务器端口号。
   - 导入 Kerberos 密钥表。详细操作请参见本文档“用户&安全 > Kerberos”中的导入密钥表。
   - 输入当前登录 iBMC 的用户密码。

   其它参数请根据实际需要进行设置。相关参数说明请参考“用户&安全 > Kerberos”章节的启用 Kerberos 认证并配置域服务器基本属性。
4. 单击“保存”。

步骤 3 配置 Kerberos 用户组信息

1. 在 iBMC WebUI，选择“用户&安全 > Kerberos”。
2. 在“Kerberos 用户组”区域单击  进入“修改用户”编辑区域框，或单击“添加”进入“添加组”编辑区域框。
3. 配置 Kerberos 组参数。

- 输入 Kerberos 用户所属角色组的名称，如“info_group1”（即 6.5.1 配置目录服务器中创建的 Kerberos 组）。
- 输入 Kerberos 组应用所在文件夹。

  和 Kerberos 服务器下用户的组所在的组织单位名保持一致，如“company/department”（即 6.5.1 配置目录服务器中涉及的最下层组织单位），最大长度为 255。
- 配置 SID。
- 选择 Kerberos 组权限。
- 选择已设定的登录规则。
- 选择登录接口。

相关参数说明请参考“用户&安全 > Kerberos”章节的表 3-46。

4. 输入当前登录的用户密码。
5. 单击“保存”。

步骤 4 为支持的浏览器配置单点登录。Chrome 不需要进行配置。

在 Internet Explorer 中启用单点登录。

以下以 Internet Explorer 11 为例进行说明。其它浏览器版本可能具有不同的步骤。

1. 在 Internet Explorer 中启用身份验证。
   a. 单击  打开 Internet 选项窗口。
   b. 选择“Internet 选项 > 高级”。
   c. 勾选安全性区域的“启用集成 Windows 验证”。
   d. 单击“确定”。
2. 将 iBMC 域添加到 Internet 区域中。
   a. 选择“Internet 选项 > 安全”。
   b. 单击“高级”。
   c. 在“将该网站添加到区域框”中输入要添加的站点，例如“*.ibmc.com”。
   d. 单击“添加”。
   e. 单击“关闭”。
3. 启用“仅在 Intranet 区域中自动登录”。
   a. 选择“Internet 选项 > 安全”。
   b. 单击“自定义级别”。
   c. 滚动至用户身份验证区域，选中“仅在 Intranet 区域中自动登录”。
   d. 单击“确定”。
   e. 如需关闭“Internet 选项”对话框，单击“确定”。
4. 关闭并重启 Internet Explorer，以确保步骤 4.1~步骤 4.3 中的更改生效。

在 Firefox 中启用单点登录

以下以 Firefox 17.0 为例进行说明。其它浏览器版本可能具有不同的步骤。

1. 在浏览器地址栏中输入“about:config”，打开浏览器配置页。

2. 如果显示“这样可能会失去质保！”提示消息，请单击“我保证会小心”。
3. 在浏览器搜索框中输入“network.negotiate”。
4. 双击“network.negotiate-auth.trusted-uris”。
5. 在弹出的输入框中输入 iBMC DNS 的域名（例如“ibmc.com”）。
6. 单击“确定”。

步骤 5 使用 Kerberos 域帐户或通过 SSO 登录 iBMC

方式一：通过 Kerberos 域帐户登录

1. 输入已在 Kerberos 服务器生效的帐号密码。
2. 在域名下拉列表，选择对应 Kerberos 服务器的域名，例“ADMIN.COM(KRB)”。
3. 单击“登录”。

方式二：通过 SSO 一键登录

1. 在已完成步骤 4 配置的浏览器中输入 iBMC 的 FQDN 地址，如“https://主机名.域名”。
2. 单击“单点登录”。

----结束

6.6 配置 iBMC WebUI DNS（手动）

操作场景

iBMC WebUI 的“iBMC 管理 > 网络配置”提供“配置 DNS”功能，设置 DNS 后，用户可以直接通过域名地址访问 iBMC。

说明

- 域名地址 = 主机名 + 域名。如：主机名为“mytest”，域名为“manager.com”，那么域名地址为“mytest.manager.com”
- DNS（Domain Name System，域名系统），因特网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。

必备事项

数据

进行配置之前，请先规划好配置过程中所需数据：

- iBMC 主机名。
- 可用的 DNS 服务器信息。
  - DNS 服务器地址
  - DNS 服务器域名

操作步骤

步骤 1 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 在 iBMC WebUI，选择“iBMC 管理 > 网络配置”。

步骤 3 在“设置 iBMC 主机名”区域框，设置 iBMC 主机名，如“mytest”。

步骤 4 单击“保存”。

步骤 5 在“DNS”区域框，单击“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 服务器地址和备用 DNS 服务器地址。

步骤 6 配置 DNS 地址。

1. 输入 DNS 域名，如“manager.com”。
2. 输入 DNS 首选服务器，如“192.168.66.66”。
3. 输入 DNS 备用服务器。
4. 单击“保存”。

步骤 7 在连接 iBMC 的本地 PC 中，配置本地 DNS 地址为 DNS 服务器地址。

请保证本地 DNS 地址和 iBMC DNS 地址一致，否则本地 PC 无法通过网络访问 iBMC。

步骤 8 使用域名登录 iBMC WebUI。

说明

域名地址 = 主机名 + 域名。如：主机名为“mytest”，域名为“manager.com”，那么域名地址为“mytest.manager.com”

在浏览器输入域名地址，如“mytest.manager.com”，即可访问 iBMC WebUI。

----结束

6.7 配置 SSH 用户密钥登录 iBMC 命令行

操作场景

用户通过 SSH 方式登录 iBMC 时，有两种认证方式：

- 输入密码认证：需要每次登录时都输入密码，不但操作不便，而且存在密码泄露的隐患。
- 使用密钥认证：只需要进行一次设置，后续登录操作都不需要输入密码。且由于密钥的对称性，导致用户必须通过具有对应密钥的客户端，才能使用 SSH 方式登录 iBMC，提高了安全性。

此章节指导用户进行 SSH 密钥管理，实现 SSH 密钥认证方式登录 iBMC。

必备事项

前提条件

- 已存在可连接到服务器 iBMC 的客户端
- iBMC 上已添加接口类型为 SSH 的用户

数据

- 生成的 SSH 公钥类型：RSA 或 DSA
- iBMC 管理网口 IP 地址
- SSH 服务端口号

软件

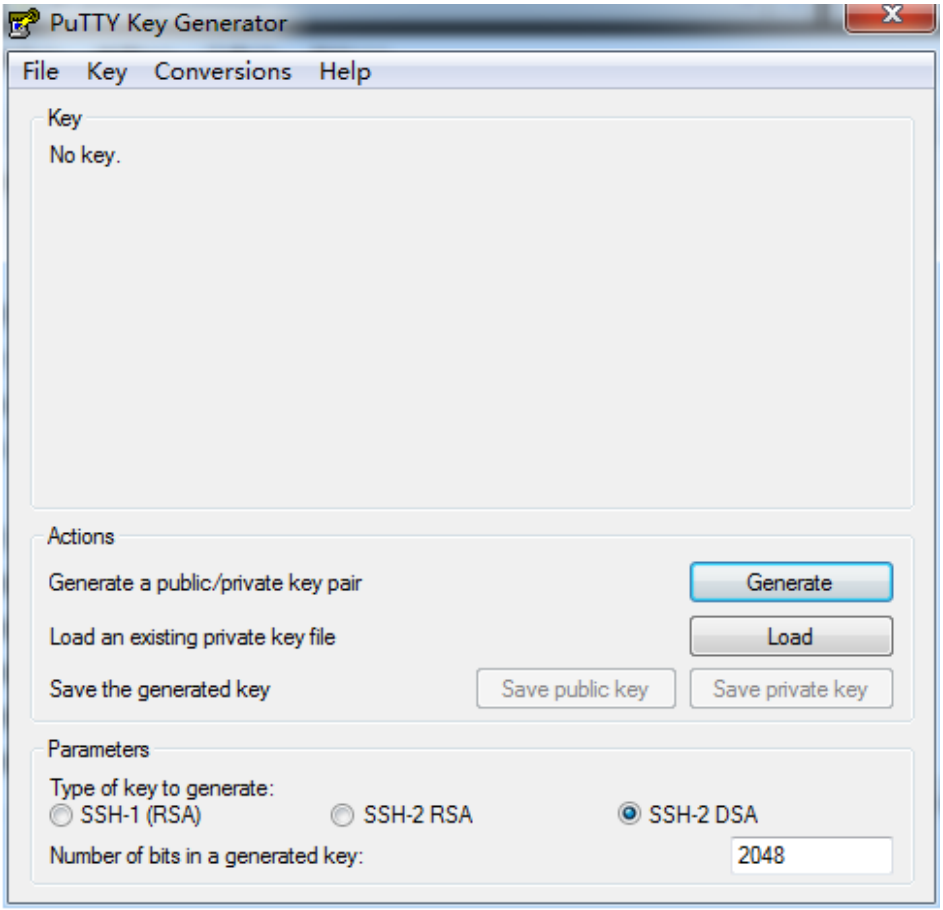
- 登录工具，例如“putty.exe”。
- 密钥生成工具，例如“puttygen.exe”。

上述工具为免费工具，请自行在互联网搜索下载。

操作步骤

- 生成 SSH 密钥
  a. 在客户端（例如 PC）打开密钥生成工具（例如“puttygen.exe”），如图 6-26 所示。

图6-26 密钥生成界面



b. 在“Parameters”区域中选择密钥类型，例如“SSH-2 DSA”。

c. 设置密钥容量。

d. 单击“Generate”生成密钥。

e. 单击“Save public key”和“Save private key”将生成的公钥、私钥保存到客户端。

- 将公钥导入 iBMC

a. 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

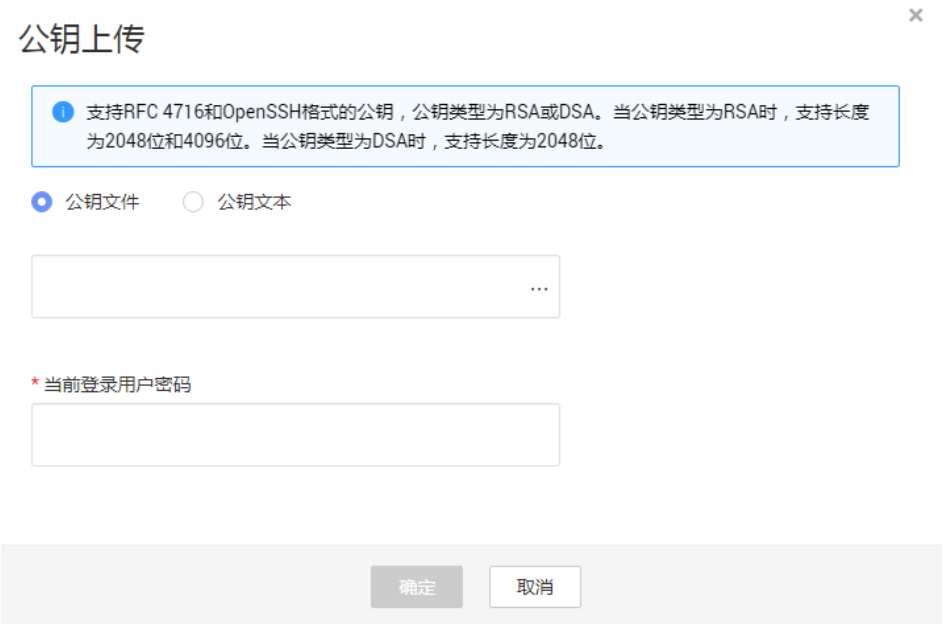
b. 在 iBMC WebUI，选择“用户&安全 > 本地用户”。

c. 单击待导入 SSH 公钥的用户名左侧的 。

d. 单击“SSH 公钥”右侧的“上传”。

弹出导入“公钥上传”窗口，如图 6-27 所示。

图6-27 公钥上传



e. 选择公钥导入方式。

此处可根据实际情况选择“公钥文件”或“公钥文本”。

f. 单击 ... 选择生成的公钥。

g. 输入当前登录用户密码。

h. 单击“确定”。

说明

请定期更新密钥，否则可能存在安全风险。

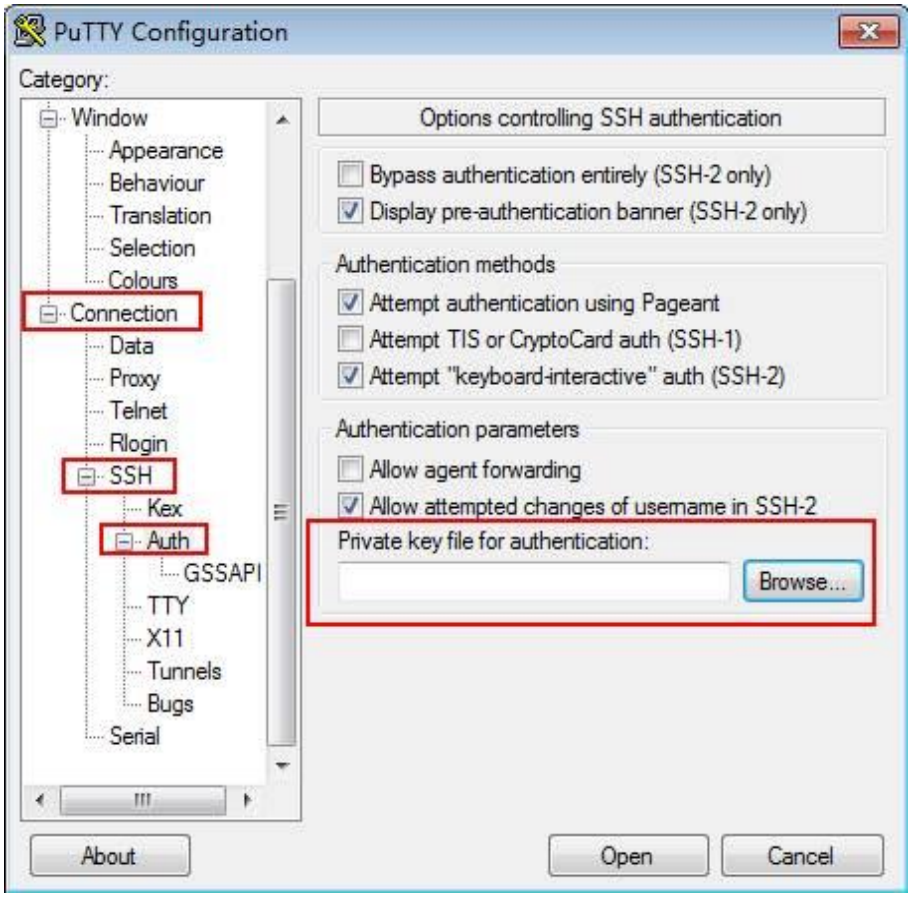
- 配置 SSH 客户端

a. 在客户端打开登录工具（例如“putty.exe”）。

b. 导入生成的私钥。

私钥导入界面如图 6-28 所示。

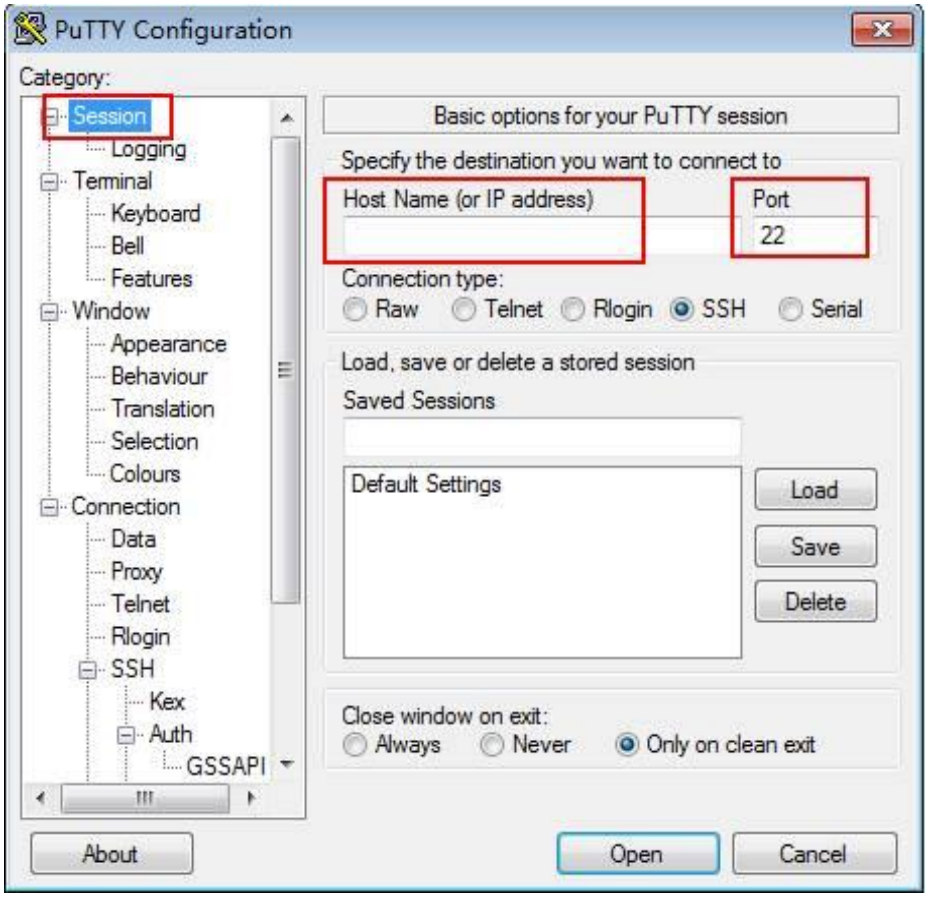
图6-28 导入私钥



c. 配置 SSH 客户端登录信息。

登录信息配置界面如图 6-29 所示，需要输入 iBMC 地址、SSH 服务端口号。

图6-29 配置登录信息



- 登录 iBMC 命令行
  a. 单击“Open”。
  b. 按提示信息输入 SSH 用户名。
     进入 iBMC 命令行。

6.8 配置 iBMC SSL 证书

操作场景

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他所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。

此章节指导用户进行 SSL 证书替换。

必备事项

前提条件

已存在可连接到服务器 iBMC 的客户端。

操作步骤

登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

请根据实际需求执行不同的操作：

- 当客户端存在正式的证书颁发机构颁发的 SSL 证书时，请执行•导入 SSL 证书。
- 当客户端存在用户手动生成的 SSL 证书时，请执行•导入 SSL 证书、•向浏览器添加根证书。
- 当用户需要自定义证书信息并使用正式的证书颁发机构颁发 SSL 证书时，请执行•申请 SSL 证书、•导入 SSL 证书、•向浏览器添加根证书。

当用户需要自定义证书信息并使用证书生成工具手动生成 SSL 证书时，请执行•自定义证书信息、•申请 SSL 证书、•导入 SSL 证书、•向浏览器添加根证书。

- 自定义证书信息
  a. 在 iBMC WebUI，选择“Web 服务 > SSL 证书”。
  b. 单击“自定义”打开自定义 SSL 信息的界面。
  c. 在“步骤一：生成 CSR”区域框中，输入自定义的证书请求信息。
     自定义信息包括：国家、省份、城市、公司、部门和常用名。
  d. 单击“保存”。
  e. 按照弹出的对话框的提示信息导出 CSR 文件到客户端。
- 申请 SSL 证书
  SSL 证书可通过如下方式获取：
  - 向正式的证书颁发机构申请 SSL 签名证书。（推荐方式）
  - 使用证书生成工具（例如 openssl）手动生成 SSL 签名证书和根证书。

  证书生成工具及其使用方法请用户自行从互联网下载。
- 导入 SSL 证书
  a. 在“SSL 证书”界面单击“自定义”。
  b. 导入 SSL 证书。
     - （使用证书颁发机构申请的 SSL 证书时）在“步骤二：导入服务器证书”区域框中，单击“浏览”，选中•申请 SSL 证书中获取的 SSL 签名证书，并单击“保存”。
     - （使用用户手动生成的 SSL 证书时）在“自定义证书”区域框中，单击“浏览”，选中•申请 SSL 证书中获取的 SSL 签名证书，在“证书密码”后的文本框中输入传输过程中采用的密码，并单击“保存”。

     导入后，会返回“操作成功”信息。
  c. 重新登录 iBMC WebUI。
- 向浏览器添加根证书

说明

导入的 SSL 证书如果不是从正式的证书颁发机构获取，而是用户自己使用工具生成，在导入该 SSL 证书后，还需要确认客户端浏览器中是否已存在对应的根证书。

下面以 IE 为例说明如何在浏览器中查看并添加认证机构的根证书。

a. 打开浏览器。

b. 在工具栏中选择“工具 > Internet 选项”。

弹出“Internet 选项”窗口。

c. 在“内容”页签中单击“证书”。

打开“证书”窗口。

d. 在“受信任的根证书颁发机构”页签中查看办理 SSL 证书的机构是否在列表中。

- 是 => e
- 否 => f

e. 查看证书是否过期。

- 是 => f
- 否 => g

f. 单击“受信任的根证书颁发机构”下方的“导入”。按照提示信息导入或重新导入根证书。

g. 重新打开浏览器，观察地址栏是否已存在  标识。

- 是 => 操作完成
- 否 => 请联系技术支持处理

6.9 配置 iBMC Syslog 日志上报功能

操作场景

iBMC WebUI 的“维护诊断 > 告警上报”提供 Syslog 日志上报配置接口，可以设置 iBMC 系统向第三方服务器以 syslog 报文方式发送日志信息。

必备事项

前提条件

已存在可连接到服务器 iBMC 的客户端。

数据

进行配置之前，请先规划好配置过程中所需数据：

- syslog 属性
  - 用于识别信息来源的主机标识（“单板序列号”、“产品资产标签”或“主机名”）。
  - 传输过程使用过的协议类型（包括“TLS”、“TCP”或“UDP”）。

  - syslog 认证方式（包括“单向认证”和“双向认证”）。
  - 传输日志的级别
- syslog 服务器和报文格式
  - 上报通道的状态
  - 服务器地址
  - 服务器端口号
  - 上报日志的类型

软件

已从互联网下载免费的证书生成工具“openssl”。

操作步骤

步骤 1 生成证书

请用户使用证书生成工具手动生成所需证书：

- 单向认证时，需要的证书包括 syslog 服务器证书和服务器根证书。
- 双向认证时，需要的证书包括 syslog 服务器证书和服务器根证书、syslog 客户端证书和客户端根证书。

操作方法可参考从互联网下载“openssl”的说明文档。

步骤 2 将证书上传到 syslog 服务器

请使用文件传输工具（支持 SFTP 协议，例如 WinSCP）将所需证书上传到 iBMC 文件系统的指定目录（例如“/tmp”）。

- 单向认证时，需要将服务器证书上传到 syslog 服务器。
- 双向认证时，需要将服务器证书和客户端根证书上传到 syslog 服务器。

说明

请定期更新证书，否则可能存在安全风险。

步骤 3 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 4 配置 syslog 属性

1. 在 iBMC WebUI，选择“维护诊断 > 告警上报”。
2. 在“Syslog 报文通知”区域框中，开启 syslog 报文上报功能。
3. 按照界面信息配置“Syslog 消息格式”、“Syslog 主机标识”、“告警级别”、“传输协议”、“认证方式”。

   详细信息请参考表 3-26。
4. 上传证书。
   - 当“认证方式”为“单向认证”时，将步骤 1 中生成的**服务器根证书**上传到 iBMC。
   - 当“认证方式”为“双向认证”时，将步骤 1 中生成的**服务器根证书**和**客户端证书**上传到 iBMC。

步骤 5 配置 syslog 服务器信息和报文格式

1. 选择 syslog 报文发送通道。
2. 单击“编辑”，显示指定通道的编辑区域框。
3. 单击  ，使能发送通道。

   当  按钮变为  ，表示启用该发送通道。
4. 按照界面信息配置“服务器地址”、“端口”、“日志类型”。
5. 单击“测试”。

   显示“操作成功”，表示该通道可用。

----结束

6.10 使用 VNC 登录服务器实时桌面

操作场景

iBMC 实现的 VNC 服务配置功能，丰富了 KVM 操作接口，提供了更灵活的 KVM 操作方式。由于 VNC 协议的开源性，当前有多种第三方 VNC 工具供您自由选择，可以根据需要从第三方获取。

VNC 服务支持 SSL 加密和不加密两种传输模式，此处以不加密传输方式为例进行说明。

必备事项

前提条件

客户端（例如 PC）已连接到服务器 iBMC 管理网口。

数据

- iBMC 管理网口的地址和端口号（即 VNC 服务端口号）
- VNC 服务密码

软件

客户端（例如 PC）已下载并安装第三方的 VNC 客户端软件，例如 TigerVNC、RealVNC。

操作步骤

步骤 1 使能 VNC 端口

iBMC 支持通过 Web、CLI、IPMI、Redfish 接口开启 VNC 服务并设置端口号，下面以在 Web UI 中的操作方法为例进行说明。

1. 登录 iBMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。
2. 在 iBMC WebUI，选择“服务管理 > VNC”。

3. 开启 VNC 服务，并设置端口号。VNC 服务默认为关闭状态。默认端口号为“5900”。

步骤 2 配置 VNC 属性

1. 在不采用 SSL 加密传输时，关闭 SSL 加密使能，设置 VNC 密码。

   密码复杂度要求：

   - 长度必须为 8 个字符。
   - 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
   - 至少包含一个以下特殊字符：

     `~!@#$%^&*()-_=+\|[{}];:'",<.>/?

   说明

   出于安全考虑，保存设置时需要输入当前登录用户密码进行身份验证。

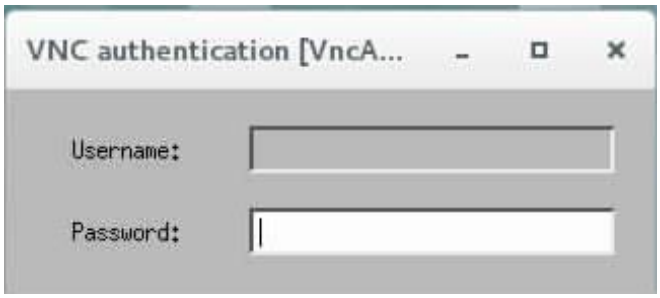
步骤 3 （可选）Linux 客户端使用 TigerVNC 登录服务器实时桌面

1. 在客户端的 TigerVNC 安装目录下，打开命令行控制台，并执行 **vncviewer ipaddress:port** 命令。

   其中，*ipaddress* 表示服务器 iBMC 管理网口 IPv4 或 IPv6 地址，*port* 表示 VNC 服务端口号。

   打开 TigerVNC 的登录窗口，如图 6-30 所示。

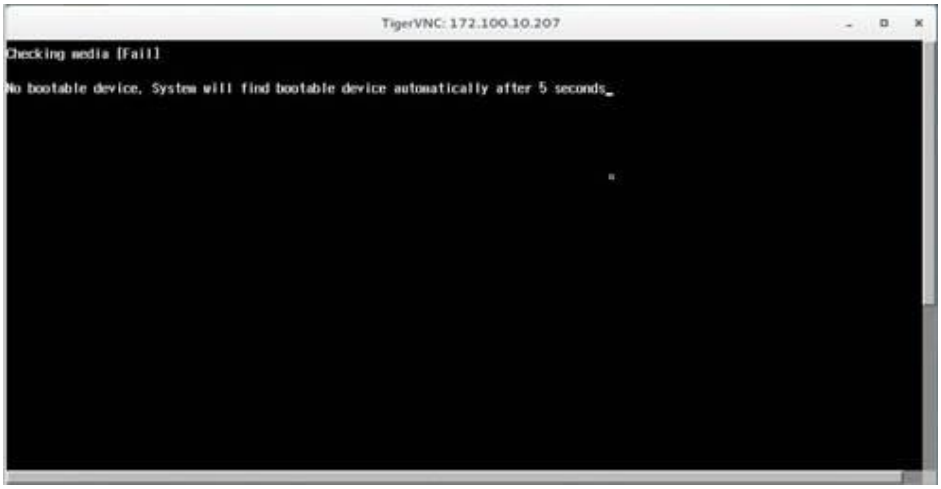
   图6-30 TigerVNC 登录窗口

2. 输入步骤 1.2 中设置的密码，并按“Enter”。

   登录服务器实时桌面，如图 6-31 所示。

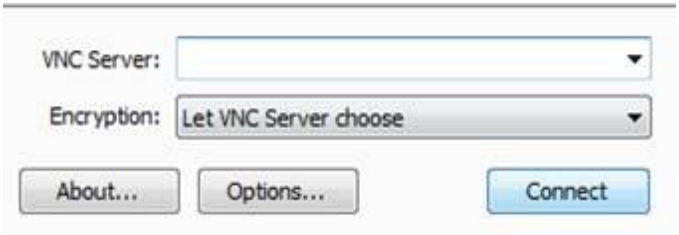
图6-31 服务器实时桌面



步骤 4 （可选）Windows 客户端使用 RealVNC 登录服务器实时桌面

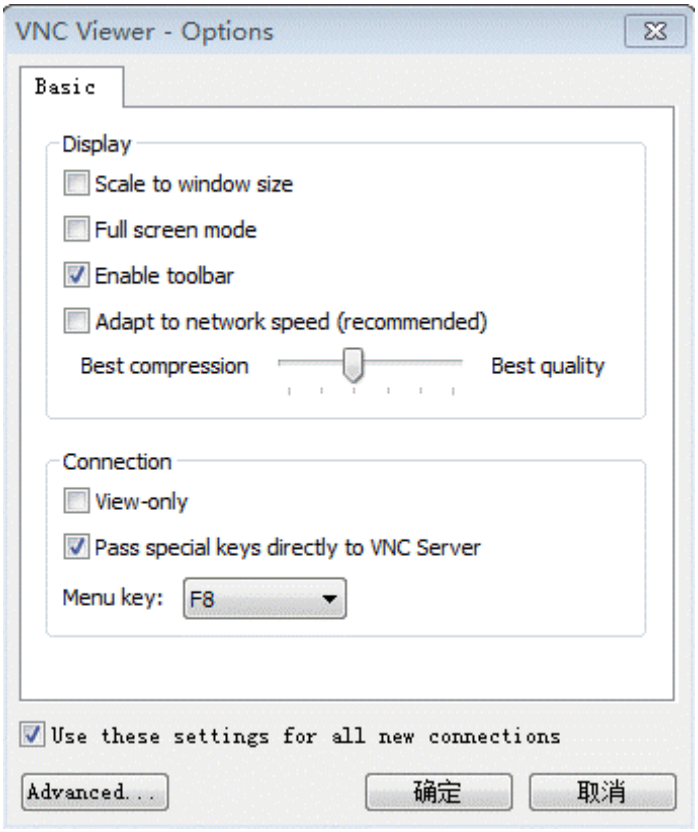
1. 在客户端双击 RealVNC 客户端软件。
   打开 RealVNC 登录窗口，如图 6-32。

图6-32 RealVNC 登录窗口



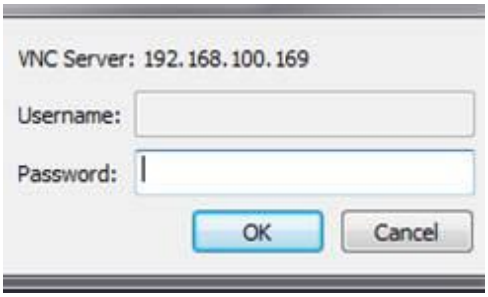
2. 单击“Options”，打开参数设置界面，如图 6-33。

图6-33 RealVNC 客户端参数设置界面



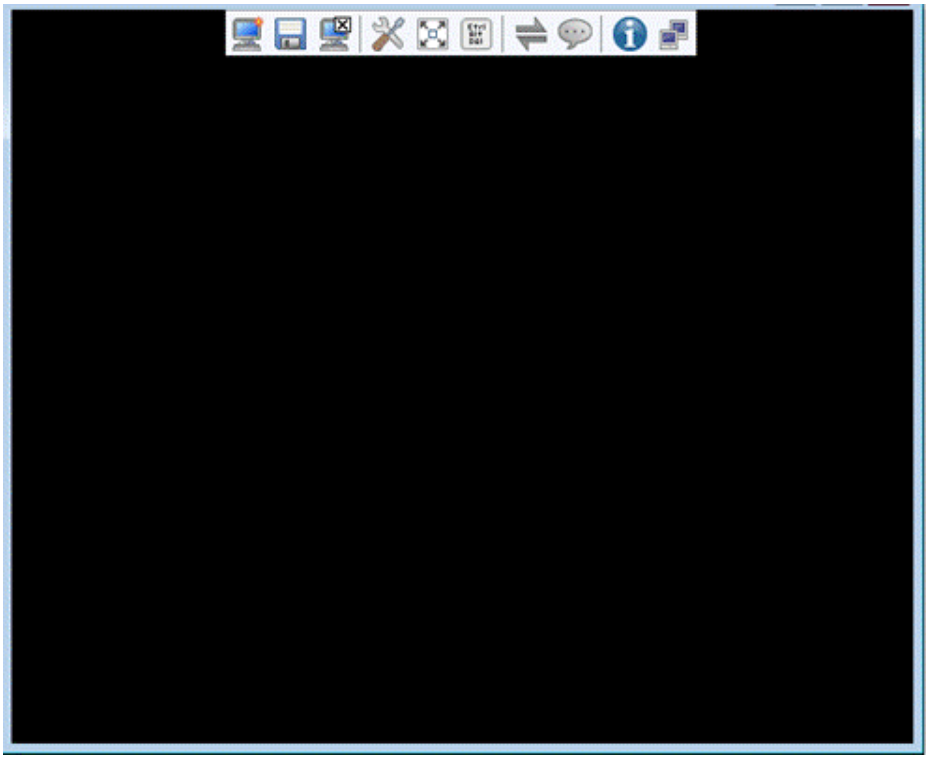
3. 按照实际需要设置显示参数，单击“确定”。
   返回图 6-30 所示的登录窗口。
4. 在“VNC Server”右侧的文本框中输入要登录的服务器 iBMC 管理网口 IP 地址。
   地址格式为“管理网口 IP 地址（IPv4 地址或 IPv6 地址）:端口号”，例如“192.168.100.169:5900”。
5. 单击“Connect”。
   若弹出数据加密提示窗口，请单击“continue”继续进行操作。
   弹出身份认证窗口，如图 6-34。

图6-34 RealVNC 客户端身份认证窗口



6. 在“Password”右侧的文本框中输入步骤 3.1 中设置的密码，并单击“OK”。
登录服务器实时桌面，如图 6-35。

图6-35 服务器实时桌面



----结束

6.11 为 iBMC 导入信任证书和根证书

操作场景

使用浏览器登录 iBMC WebUI 时，若弹出安全告警提示，可以在浏览器中为 iBMC 导入信任证书和根证书来屏蔽此安全告警提示。

本指南以 Internet Explorer 11.0 为例介绍为 iBMC 导入信任证书和根证书的操作步骤。

必备事项

前提条件

请用户自行准备好需要导入的信任证书和根证书。

数据

无

软件

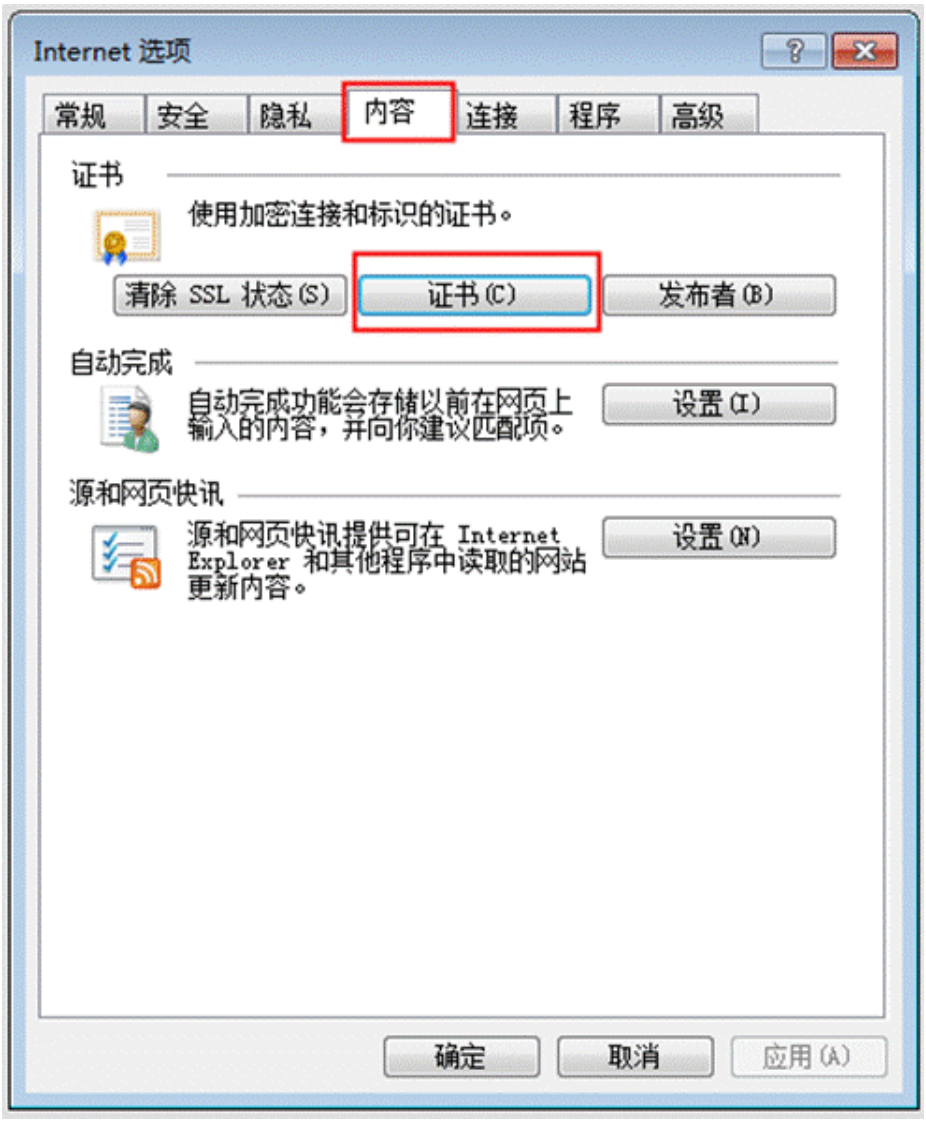
无

操作步骤

- 导入信任证书

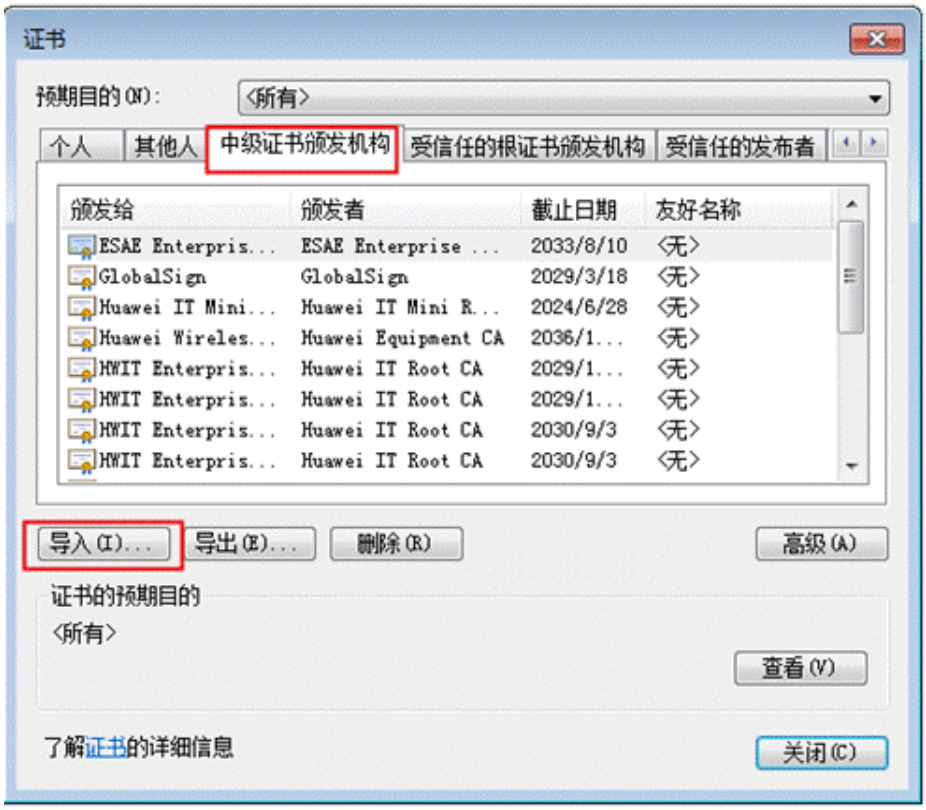
  a. 打开 IE 浏览器，单击。
  弹出 Internet 选项窗口如图 6-36。

  图6-36 Internet 选项窗口



  b. 单击“内容 > 证书”。
  弹出导入证书窗口如图 6-37。

图6-37 导入证书窗口



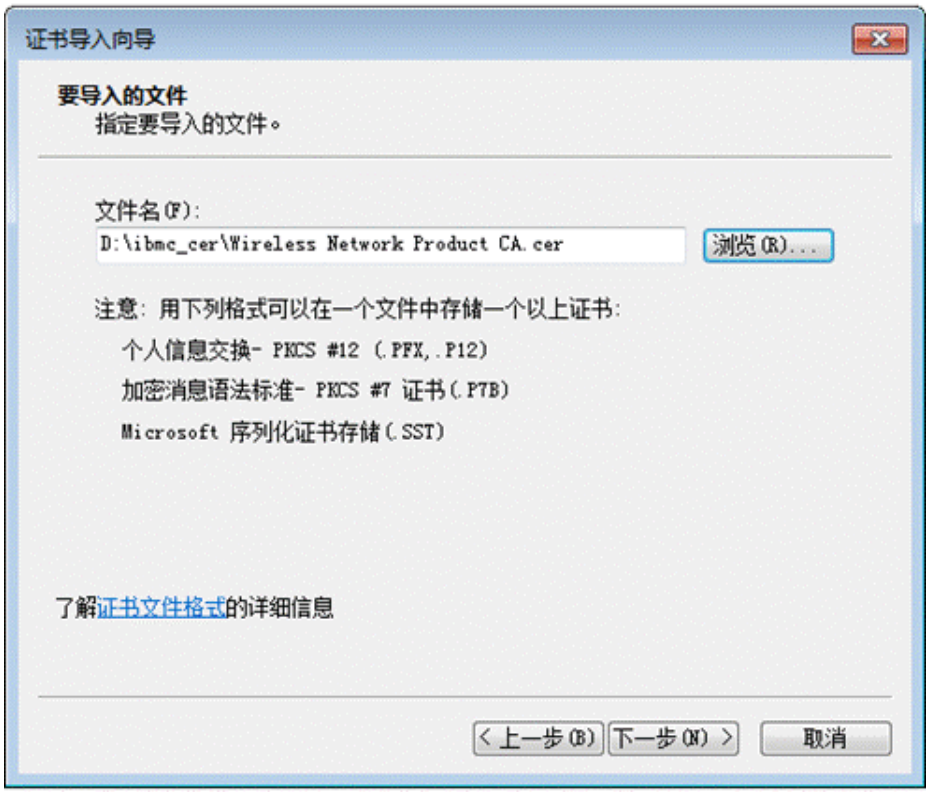
c. 单击“中级证书颁发机构 > 导入”。
弹出证书导入向导窗口如图 6-38。

图6-38 导入证书窗口

d. 单击“下一步”继续。

弹出选择证书窗口如图 6-39。

图6-39 选择证书窗口

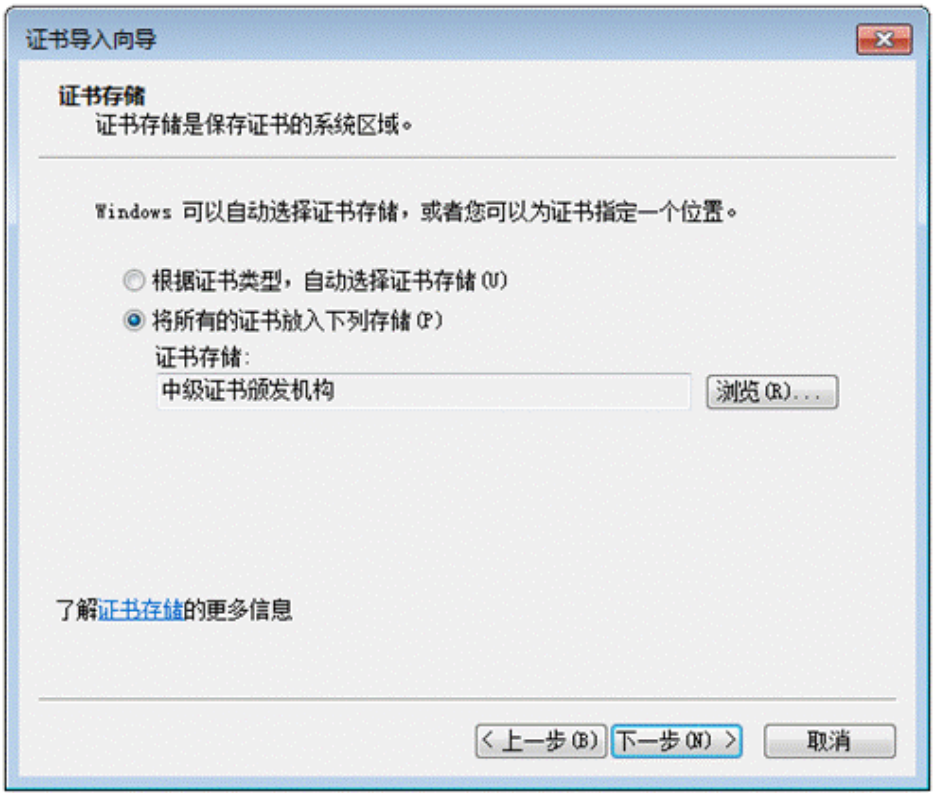


e. 单击“浏览”，从本地 PC 路径中选择待上传的证书。

f. 单击“下一步”继续。

在弹出的选择证书存储位置窗口图 6-40 中选择证书的存放位置。

图6-40 选择证书存储位置窗口



g. 单击“下一步 > 完成”。

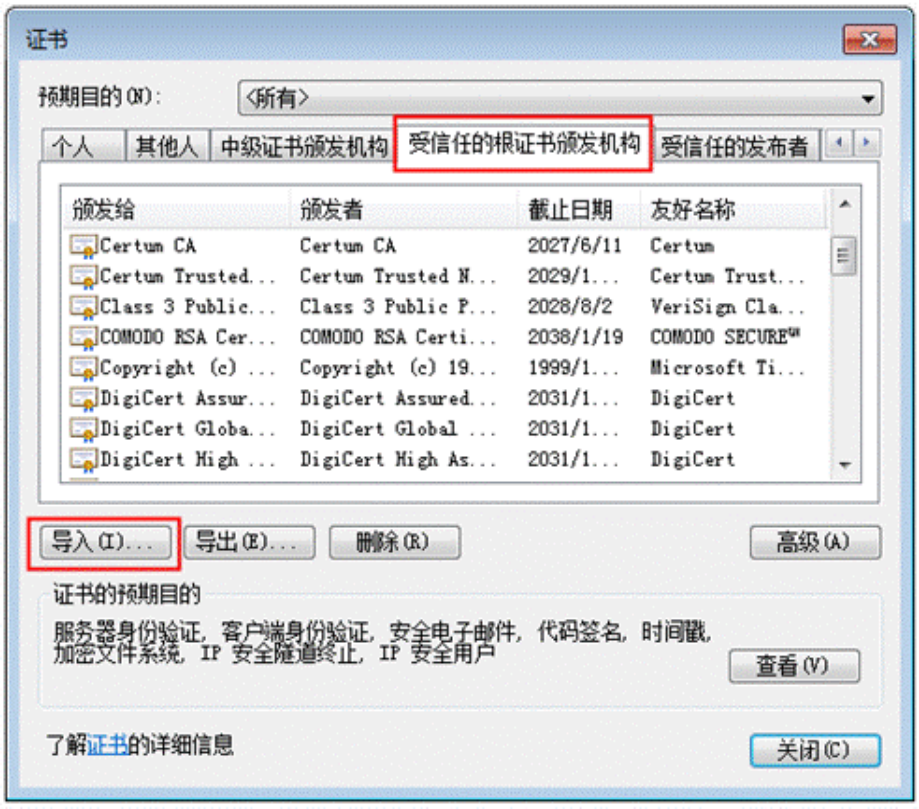
弹出“导入成功”提示框。则表示成功导入证书。

h. 单击“确定”完成证书导入。

- 导入根证书

a. 重复以上 a 和 2，打开弹出导入证书窗口，如图 6-41。

图6-41 导入证书窗口



b. 单击“受信任的根证书颁发机构 > 导入”。

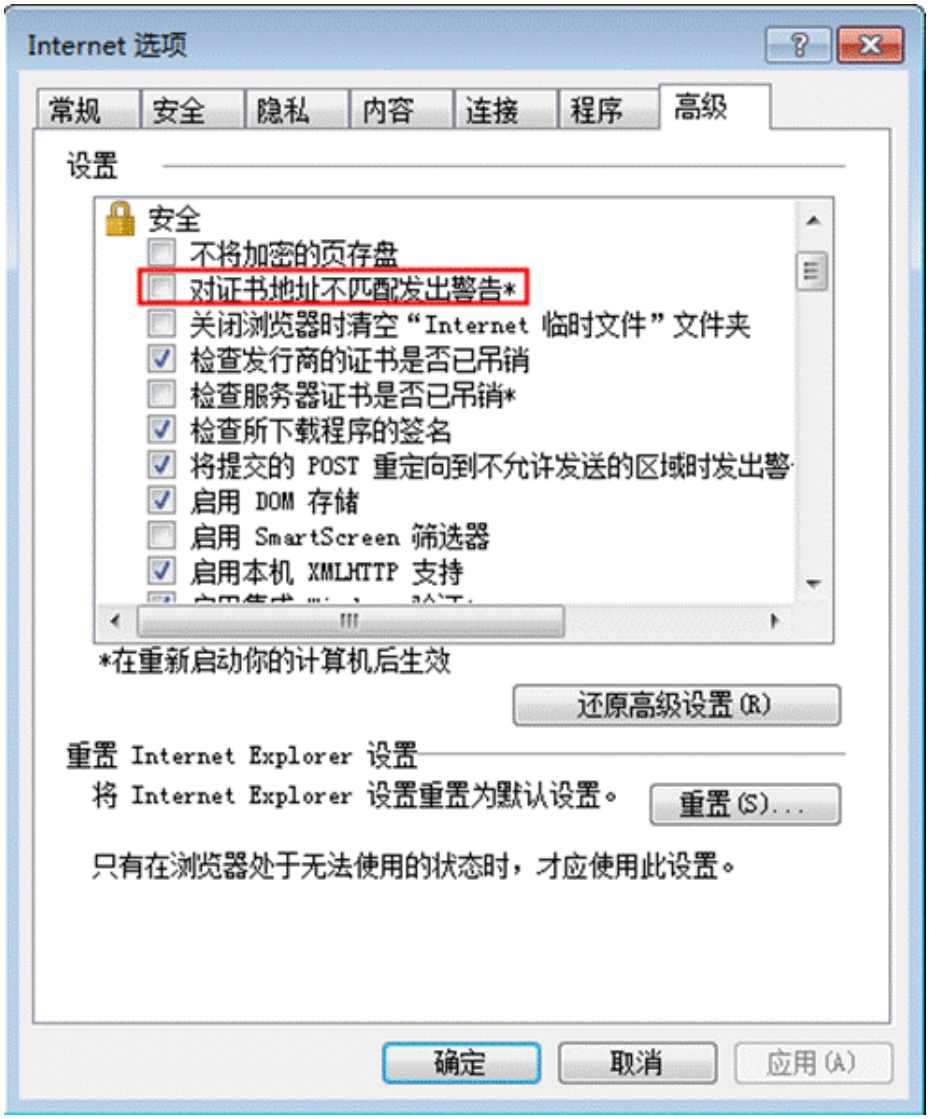
弹出证书导入向导窗口如图 6-42。

图6-42 导入证书窗口

c. 重复以上 4～8，完成根证书导入。
取消勾选“对证书地址不匹配发出警告”
此操作需要重启计算机后才能生效。

d. 单击“ > Internet 选项 > 高级”。
弹出 Internet 选项窗口如图 6-43。

图6-43 Internet 选项窗口



e. 取消勾选“对证书地址不匹配发出警告”后，单击“应用 > 确认”，保存设置。

如果保存设置后登录 iBMC，屏蔽安全告警提示操作仍未生效，请重启浏览器后再次登录。

说明

- 如果证书错误提示中显示其它的颁发者，此时导入颁发者对应的信任证书即可屏蔽安全告警提示。
- 请定期更新证书，否则可能存在安全风险。

6.12 配置 IPMI 通行名单

操作场景

服务器操作系统内可以通过发送 IPMI 命令对 iBMC 进行配置，IPMI 规范定义系统内发送到 iBMC 的 IPMI 命令是不需要认证的。为避免由此造成的安全隐患，请务必通过配置 IPMI 通行名单的方式来限制可对 iBMC 下发的 IPMI 命令，保证 iBMC 安全性。

只有通行名单中的 IPMI 命令，方可下发到 iBMC。

必备事项

前提条件

已存在可连接到服务器 iBMC 的客户端。

软件

已在客户端安装 IPMI 工具。

操作步骤

步骤 1 在客户端通过 IPMI 工具执行启动防火墙并设置通行名单的操作。

以 IPMItool 为例，可执行如下命令：

```
ipmitool.exe -I lanplus -H ibmcipaddr -U username -P password raw 0x30 0x93 0xdb
0x07 0x0 0x4a 0x01 0x01 0x01
```

说明

- ibmcipaddr：表示 iBMC 管理网口 IP 地址。
- username：表示登录 iBMC 所需的管理员用户名。
- password：表示登录 iBMC 所需的管理员密码。

步骤 2 向通行名单中添加命令。

以 IPMItool 为例，可执行如下命令：

```
ipmitool.exe -I lanplus -H ibmcipaddr -U username -P password raw 0x30 0x93 0xdb
0x07 0x0 0x3f 0x0 0x0 0x01 netfn cmd chan data
```

说明

- ibmcipaddr：表示 iBMC 管理网口 IP 地址。
- username：表示登录 iBMC 所需的管理员用户名。
- password：表示登录 iBMC 所需的管理员密码。
- netfn、cmd、han、data：表示标准 IPMI 命令中包含的字段。

----结束

7 独立远程控制台

关于本章

介绍独立远程控制台的基本信息和使用方法。

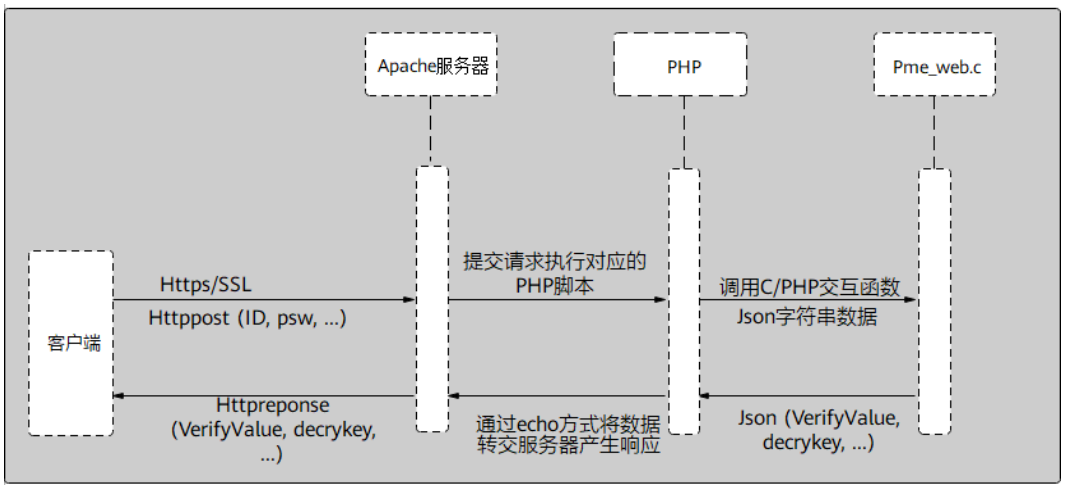
7.1 简介

独立远程控制台是基于服务器管理软件 iBMC 的远程控制工具，其实现的功能与 iBMC WebUI 的“远程控制”界面相同。用户可以使用此工具直接登录服务器实时桌面，而不需要考虑客户端浏览器与 JRE 的兼容性问题，方便您实时操作服务器。

基本原理

独立远程控制台的基本原理如图 7-1 所示。

图7-1 基本原理



兼容性

独立远程控制台可在如表 7-1 所示环境中运行。

表7-1 环境要求

客户端操作系统类型	客户端操作系统版本
Windows	Windows 7 32 位/64 位
	Windows 8 32 位/64 位
	Windows 10 32 位/64 位
	Windows Server 2008 R2 32 位/64 位
	Windows Server 2012 64 位
Redhat	Redhat 6.9
	Redhat 7.3
Ubuntu	Ubuntu 14.04 LTS
	Ubuntu 16.04 LTS
Mac OS	Mac OS X El Capitan

7.2（Windows）使用独立远程控制台登录服务器实时桌面

操作场景

当用户需要使用 iBMC 登录服务器实时桌面时，在客户端操作系统版本与 iBMC 版本均符合独立远程控制台运行要求的情况下，相较 iBMC WebUI 的“远程控制”界面，独立远程控制台可以提供更方便的操作。

下面介绍 Windows 系统下如何使用独立远程控制台登录服务器实时桌面。

必备事项

前提条件

客户端（例如 PC）已连接到服务器 iBMC 管理网口。

数据

- iBMC 管理网口的地址和端口号
- 登录 iBMC 所需的用户名和密码

软件

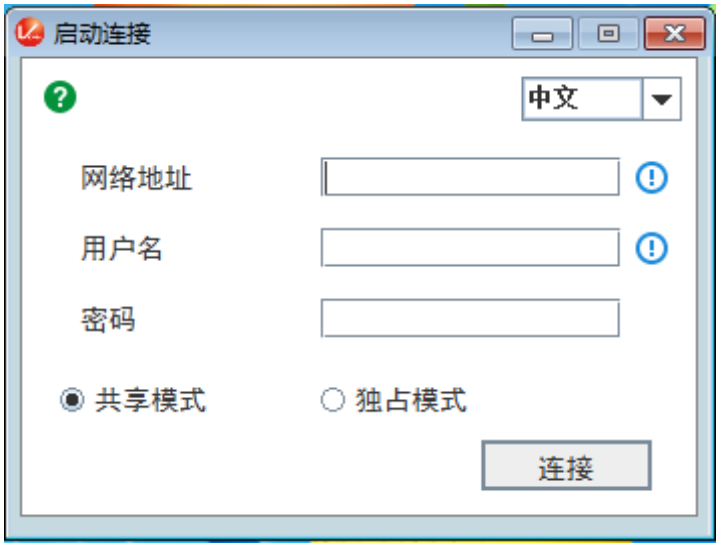
独立远程控制台软件包已下载到客户端（例如 PC）并解压。

操作步骤

步骤 1 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 2 双击“KVM.exe”打开独立远程控制台，如图 7-2 所示。

图7-2 独立远程控制台登录界面



步骤 3 按提示信息输入网络地址、用户名和密码。

网络地址有两种格式：

- iBMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- iBMC 域名地址：端口号

说明

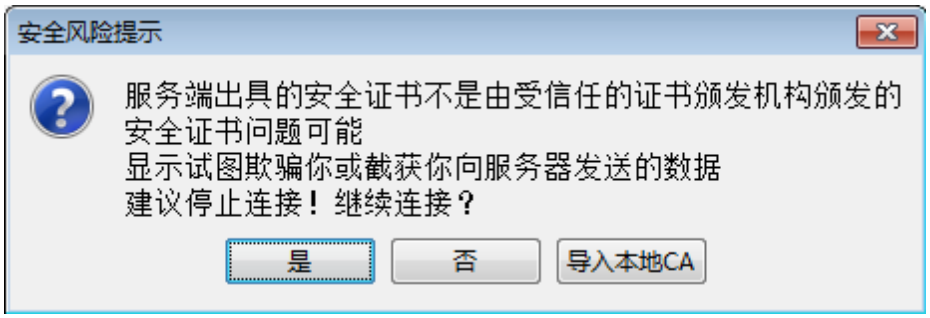
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 4 选择登录模式，并单击“连接”。

- 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。

弹出如图 7-3 所示的安全风险提示对话框。

图7-3 安全风险提示



步骤 5 按照实际需要单击确认按钮。

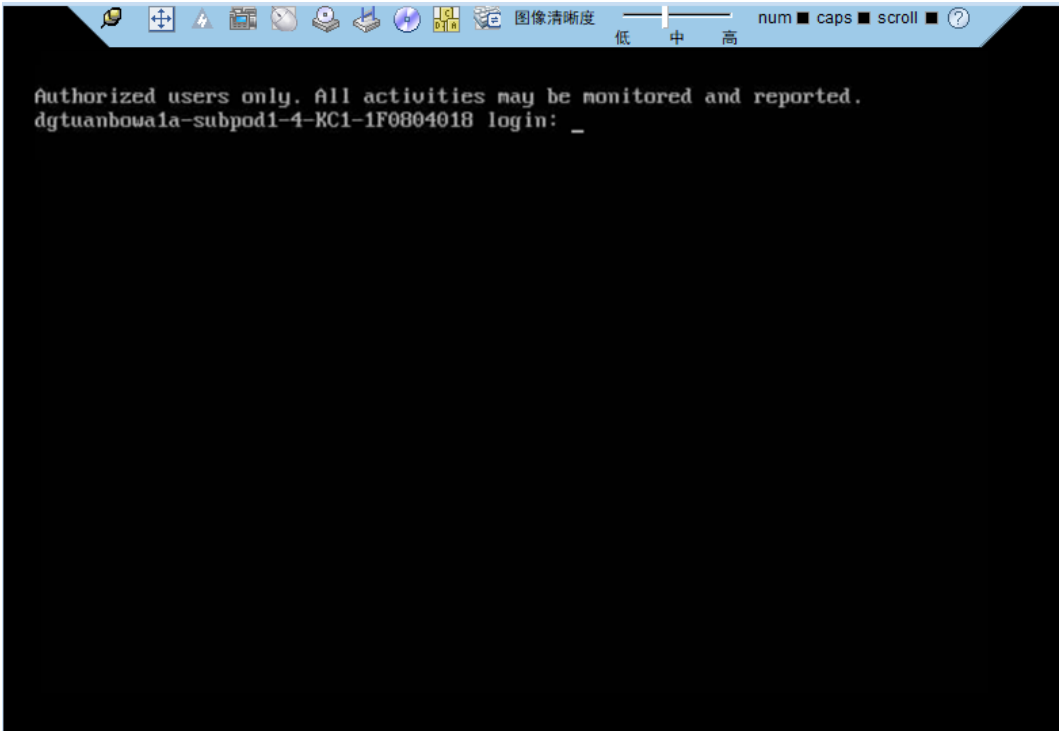
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件（“*.cer”、“*.crt”或“*.pem”），之后将不会再弹出该安全风险提示对话框。

说明

请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如图 7-4 所示。

图7-4 服务器实时桌面



----结束

7.3（Ubuntu）使用独立远程控制台登录服务器实时桌面

操作场景

当用户需要使用 iBMC 登录服务器实时桌面时，在客户端操作系统版本与 iBMC 版本均符合独立远程控制台运行要求的情况下，相较 iBMC WebUI 的“远程控制”界面，独立远程控制台可以提供更方便的操作。

下面介绍 Ubuntu 系统下如何使用独立远程控制台登录服务器实时桌面。

必备事项

前提条件

- 客户端（例如 PC）已连接到服务器 iBMC 管理网口。
- 系统已安装 ipmitool 工具，且 ipmitool 工具版本高于 1.8.14。

数据

- iBMC 管理网口的地址和端口号
- 登录 iBMC 所需的用户名和密码

软件

独立远程控制台软件包已下载到客户端（例如 PC）并解压。

操作步骤

步骤 1 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 2 打开控制台，并将独立远程控制台所在文件夹设置为工作路径。

步骤 3 执行 **chmod +x KVM.sh** 设置独立远程控制台的权限。

步骤 4 执行**./KVM.sh**，打开独立远程控制台，如图 7-5 所示。

图7-5 独立远程控制台登录界面

步骤 5 按提示信息输入网络地址、用户名和密码。

网络地址有两种格式：

- iBMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- iBMC 域名地址：端口号

说明

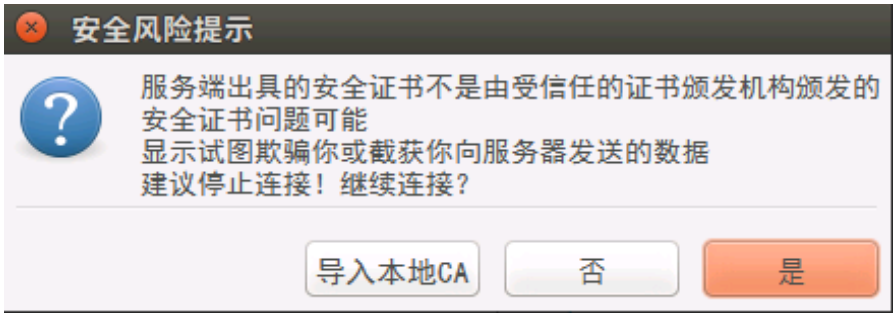
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 6 选择登录模式，并单击“连接”。

- 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。

弹出如图 7-6 所示的安全风险提示对话框。

图7-6 安全风险提示



步骤 7 按照实际需要单击确认按钮。

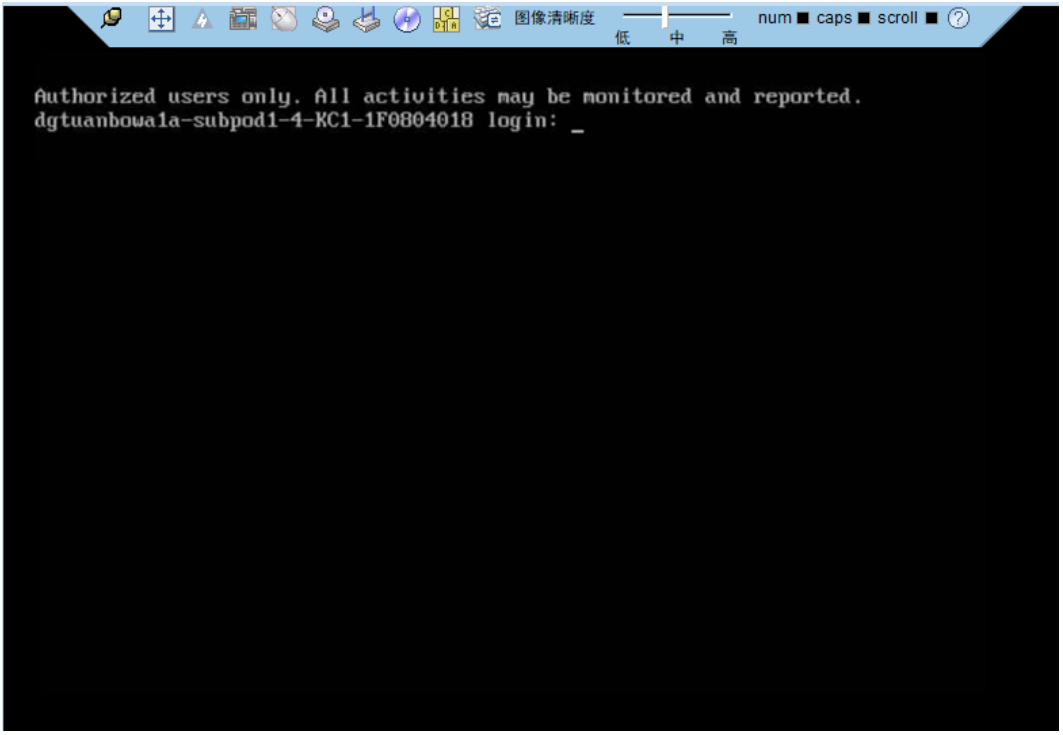
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件（“*.cer”、“*.crt”或“*.pem”），之后将不会再弹出该安全风险提示对话框。

说明

请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如图 7-7 所示。

图7-7 服务器实时桌面



----结束

7.4（Mac）使用独立远程控制台登录服务器实时桌面

操作场景

当用户需要使用 iBMC 登录服务器实时桌面时，在客户端操作系统版本与 iBMC 版本均符合独立远程控制台运行要求的情况下，相较 iBMC WebUI 的“远程控制”界面，独立远程控制台可以提供更方便的操作。

下面介绍 Mac 系统下如何使用独立远程控制台登录服务器实时桌面。

必备事项

前提条件

- 客户端（例如 PC）已连接到服务器 iBMC 管理网口。
- 系统已安装 ipmitool 工具，且 ipmitool 工具版本高于 1.8.14。

数据

- iBMC 管理网口的地址和端口号
- 登录 iBMC 所需的用户名和密码

软件

独立远程控制台软件包已下载到客户端（例如 PC）并解压。

操作步骤

步骤 1 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 2 打开控制台，并将独立远程控制台所在文件夹设置为工作路径。

步骤 3 执行 **chmod +x KVM.sh** 设置独立远程控制台的权限。

步骤 4 执行**./KVM.sh**，打开独立远程控制台，如图 7-8 所示。

图7-8 独立远程控制台登录界面

步骤 5 按提示信息输入网络地址、用户名和密码。

网络地址有两种格式：

- iBMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- iBMC 域名地址：端口号

说明

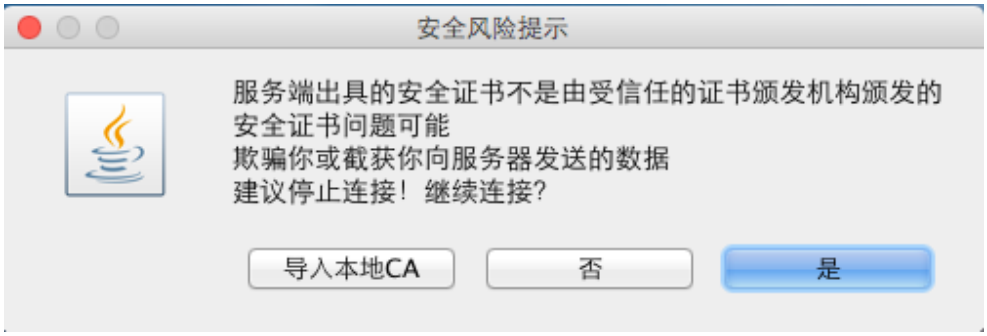
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 6 选择登录模式，并单击“连接”。

- 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。

弹出如图 7-9 所示的安全风险提示对话框。

图7-9 安全风险提示



步骤 7 按照实际需要单击确认按钮。

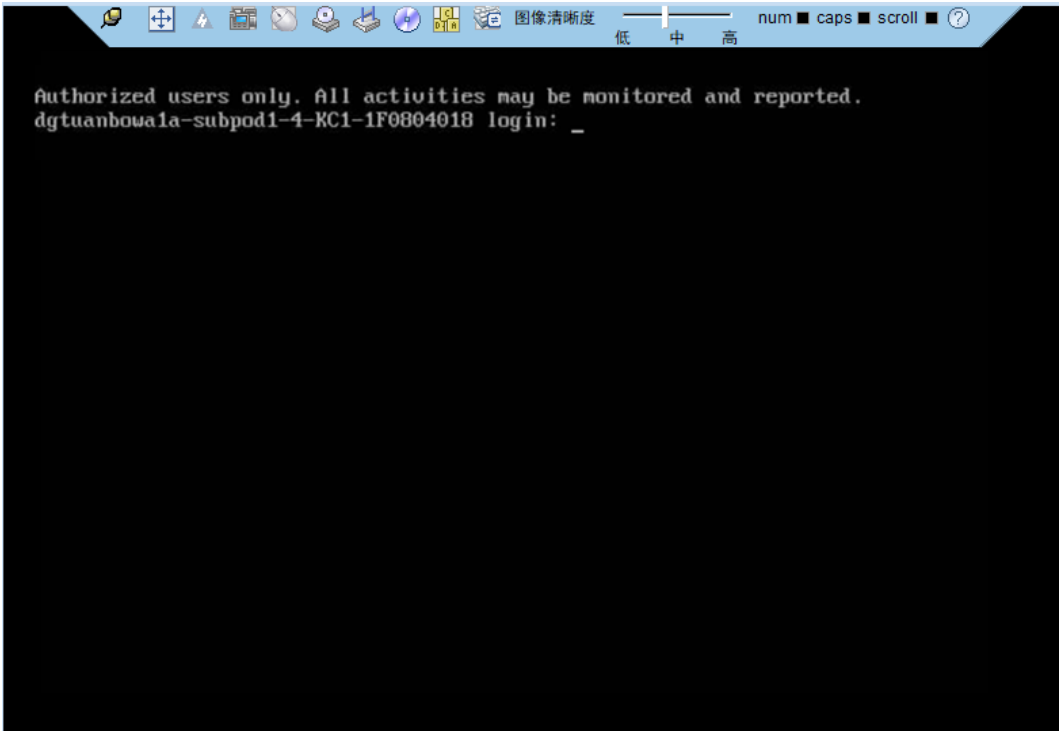
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件（“*.cer”、“*.crt”或“*.pem”），之后将不会再弹出该安全风险提示对话框。

说明

请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如图 7-10 所示。

图7-10 服务器实时桌面



----结束

7.5（Redhat）使用独立远程控制台登录服务器实时桌面

操作场景

当用户需要使用 iBMC 登录服务器实时桌面时，在客户端操作系统版本与 iBMC 版本均符合独立远程控制台运行要求的情况下，相较 iBMC WebUI 的“远程控制”界面，独立远程控制台可以提供更方便的操作。

下面介绍 Redhat 系统下如何使用独立远程控制台登录服务器实时桌面。

必备事项

前提条件

- 客户端（例如 PC）已连接到服务器 iBMC 管理网口。
- 系统已安装 ipmitool 工具，且 ipmitool 工具版本高于 1.8.14。

数据

- iBMC 管理网口的地址和端口号
- 登录 iBMC 所需的用户名和密码

软件

独立远程控制台软件包已下载到客户端（例如 PC）并解压。

操作步骤

步骤 1 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 2 打开控制台，并将独立远程控制台所在文件夹设置为工作路径。

步骤 3 执行 **chmod +x KVM.sh** 设置独立远程控制台的权限。

步骤 4 执行**./KVM.sh**，打开独立远程控制台，如图 7-11 所示。

图7-11 独立远程控制台登录界面

步骤 5 按提示信息输入网络地址、用户名和密码。

网络地址有两种格式：

- iBMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- iBMC 域名地址：端口号

说明

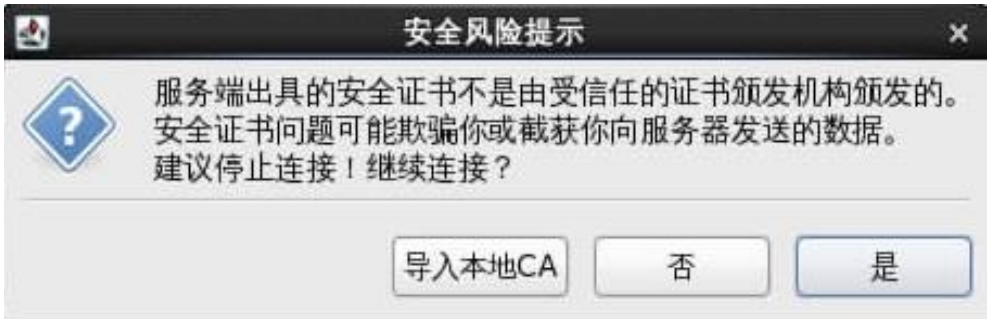
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 6 选择登录模式，并单击“连接”。

- 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。

弹出如图 7-12 所示的安全风险提示对话框。

图7-12 安全风险提示



步骤 7 按照实际需要单击确认按钮。

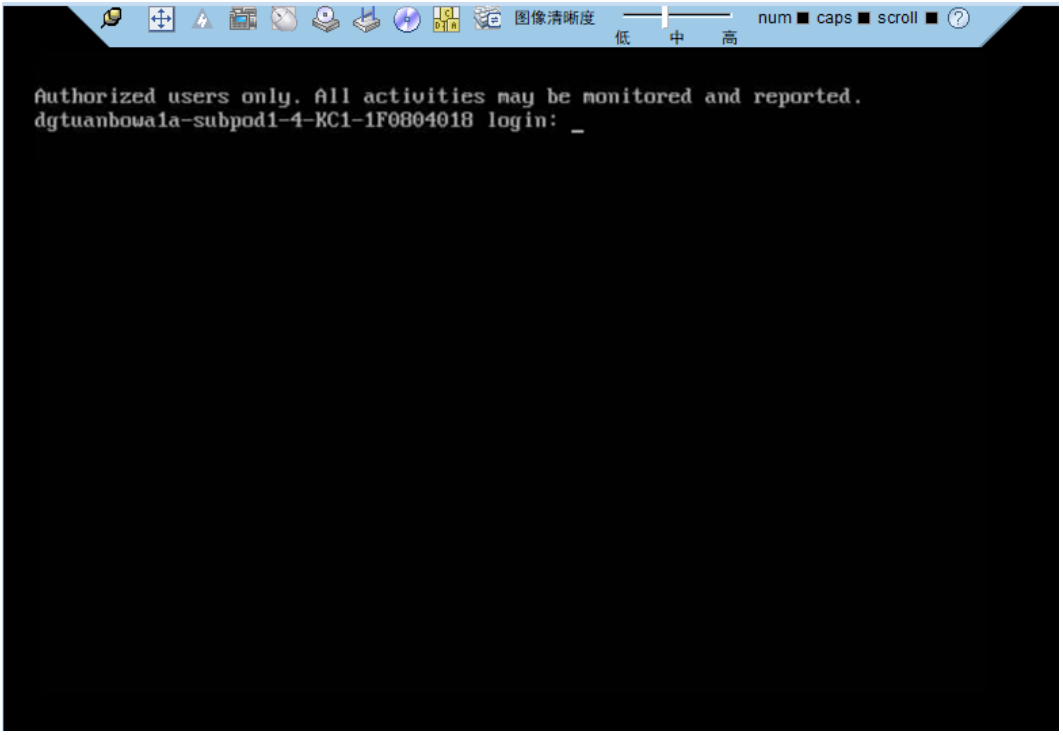
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件（“*.cer”、“*.crt”或“*.pem”），之后将不会再弹出该安全风险提示对话框。

说明

请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如图 7-13 所示。

图7-13 服务器实时桌面



----结束

8 配置文件说明

iBMC 配置文件、BIOS 配置文件和 RAID 控制器配置文件的说明如表 8-1、表 8-2 和表 8-3 所示。

为保证数据安全性，服务器更换主板后导入原配置文件时，iBMC 部分配置、RAID 控制器部分配置不随配置文件生效。

仅支持导入导出 iBMC 配置、BIOS 配置和部分的 RAID 控制器配置。

表8-1 iBMC 配置项

分类	导出项	导出子项	说明	是否支持配置文件导入生效
本地用户	User	UserName	用户名	是
	User	PassWord	用户密码 说明 iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	User	Privilege	用户权限	是
	User	UserRoleId	用户角色	是
	User	PermitRuleIds	用户登录规则	是
	User	LoginInterface	用户登录接口 说明 iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他	否

分类	导出项	导出子项	说明	是否支持配置文件导入生效
			服务器上导入了配置文件，需要管理员重新配置。	
	User	IsUserEnable	用户使能	否，取值在配置文件中体现。
	User	IsUserLocked	用户锁定	否，取值在配置文件中体现。
	UserRole	KVMMgnt	配置角色（KVM 权限）	是
	UserRole	UserMgnt	配置角色（用户管理权限）	是
	UserRole	VMMMgnt	配置角色（VMM 权限）	是
	UserRole	BasicSetting	配置角色（基本设置权限）	是
	UserRole	ReadOnly	配置角色（只读权限）	是
	UserRole	PowerMgnt	配置角色（电源控制权限）	是
	UserRole	DiagnoseMgnt	配置角色（调试诊断权限）	是
	UserRole	ConfigureSelf	配置角色（配置自身权限）	是
	UserRole	SecurityMgnt	配置角色（安全配置权限）	是
双因素认证	MutualAuthentication	MutualAuthenticationState	双因素认证使能状态	是
	MutualAuthentication	MutualAuthenticationOCSP	双因素认证证书撤销检查使能状态	是
LDAP 配置	LDAP	Enable	LDAP 使能状态	是
	LDAP	CertStatus	LDAP 证书验证使能状态	是
	LDAP	HostAddr	LDAP 服务器地址	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	LDAP	Port	LDAPS 端口号	是
	LDAP	UserDomain	域名	是
	LDAP	Folder	用户应用文件夹	是
	LDAP	BindDN	绑定标识名	是
	LDAP	BindDNPsw	绑定密码 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，取值在配置文件中体现。
	LDAPServer	Enable	LDAP 使能状态	是
	LDAPServer	CertStatus	LDAP 证书验证使能状态	是
	LDAPServer	HostAddr	LDAP 服务器地址	是
	LDAPServer	Port	LDAPS 端口号	是
	LDAPServer	UserDomain	域名	是
	LDAPServer	Folder	用户应用文件夹	是
	LDAPServer	BindDN	绑定标识名	是
	LDAPServer	BindDNPsw	绑定密码 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，取值在配置文件中体现。
	LDAPGroup	GroupName	LDAP 组名称	是
	LDAPGroup	GroupFolder	LDAP 组应用文件夹	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	LDAPGroup	GroupPermitRuleIds	LDAP 组登录规则	是
	LDAPGroup	GroupLoginInterface	LDAP 组登录接口	是
	LDAPGroup	GroupUserRoleId	LDAP 组用户角色	是
	LDAPGroup	GroupPrivilege	LDAP 组权限	是
安全增强	PasswdSetting	EnableStrongPassword	密码检查使能状态	是
	SecurityEnhance	SSHPasswordAuthentication	SSH 密码认证使能状态	是
	SecurityEnhance	UserInactTimeLimit	用户不活动期限	是
	SecurityEnhance	PwdExpiredTime	密码有效期	是
	SecurityEnhance	MinimumPwdAge	密码最短使用期	是
	SecurityEnhance	InitialPwdPrompt	密码修改提示使能状态	是
	SecurityEnhance	ExcludeUser	紧急登录用户	是
	SecurityEnhance	OldPwdCount	禁用历史密码	是
	SecurityEnhance	AuthFailMax	登录失败锁定次数	是
	SecurityEnhance	AuthFailLockTime	登录失败锁定时长	是
	PermitRule	TimeRuleInfo	时间段登录规则	是
	PermitRule	IpRuleInfo	IP 登录规则	是
	PermitRule	MacRuleInfo	MAC 登录规则	是
	SecurityEnhance	PermitRuleIds	规则使能状态	是
	SecurityEnhance	BannerState	登录安全信息配置使能状态	是
	SecurityEnhance	BannerContent	登录安全信息	是
	SecurityEnhance	CertOverdueWarnTime	证书过期告警时间	是
	SecurityEnhance	SSHCiphers	SSH 协议加密	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
			算法使能状态	
	SecurityEnhance	SSHKexs	SSH 协议密钥交换算法使能状态	是
	SecurityEnhance	SSHMACs	SSH 协议消息认证算法使能状态	是
	SecurityEnhance	SSHHostKeys	SSH 协议主机公钥算法	是
	SecurityEnhance	SSLCipherSuites	SSL 协议加密套件使能状态	是
	SecurityEnhance	RMCPCipherSuites	RMCP 协议加密套件使能状态	是
网络配置	BMC	HostName	iBMC 主机名	否，取值在配置文件中体现。
	EthGroup	NetMode	网口模式	是
	EthGroup	ActivePort	指定管理网口	是
	EthGroup	IpVersion	IP 协议使能	是
	EthGroup	IpMode	IPv4 地址获取模式	是
	EthGroup	IpAddr	IPv4 地址	否，取值在配置文件中体现。
	EthGroup	SubnetMask	IPv4 子网掩码	否，取值在配置文件中体现。
	EthGroup	DefaultGateway	IPv4 默认网关	否，取值在配置文件中体现。
	EthGroup	Ipv6Mode	IPv6 地址获取模式	是
	EthGroup	Ipv6Addr	IPv6 地址	否，取值在配置文件中体现。
	EthGroup	Ipv6Prefix	IPv6 地址前缀长度	否，取值在配置文件中体现。
	EthGroup	Ipv6DefaultGateway	IPv6 地址默认网关	否，取值在配置文件中体现。

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	DNSSetting	IPVer	DNS 绑定 IP 协议版本	是
	DNSSetting	Mode	DNS 地址获取模式	是
	DNSSetting	PrimaryDomain	DNS 首选服务器	是
	DNSSetting	BackupDomain	DNS 备用服务器 1	是
	DNSSetting	TertiaryDomain	DNS 备用服务器 2	是
	DNSSetting	DomainName	DNS 域名	是
	EthGroup	VlanState	VLAN 使能	是
	EthGroup	VlanID	VLAN ID	是
	NTP	EnableStatus	NTP 使能	是
	NTP	Mode	NTP 模式	是
	NTP	PreferredServer	NTP 首选服务器地址	是
	NTP	AlternativeServer	NTP 备用服务器地址	是
	NTP	AuthEnableStatus	NTP 服务器身份认证使能	是
	NTP	MinPollInterval	NTP 同步周期最小值	是
	NTP	MaxPollInterval	NTP 同步周期最大值	是
	VNC	EnableState	VNC 使能	是
	VNC	Password	VNC 密码 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配	否，敏感信息在配置文件中隐藏，不能直接生效。

分类	导出项	导出子项	说明	是否支持配置文件导入生效
			置。	
	VNC	Timeout	VNC 密码有效期	是
	VNC	SSLEnableState	SSL 加密使能状态	是
	VNC	Port	VNC 服务端口号	是
	VNC	KeyboardLayout	键盘布局	是
	VNC	PermitRuleIds	登录规则	是
	BMC	TimeZoneStr	时区	是
服务配置	SSH	State	SSH 使能状态	是
	SSH	Port	SSH 端口	是
	Snmp	State	SNMP Agent 使能状态	是
	Snmp	PortID	SNMP Agent 端口	是
	Kvm	State	KVM 使能状态	是
	Kvm	Port	KVM 端口	是
	Vmm	State	VMM 使能状态	是
	Vmm	Port	VMM 端口	是
	Video	State	Video 使能状态	是
	Video	Port	Video 端口	是
	WEBHTTP	State	HTTP 使能状态	是
	WEBHTTP	Port	HTTP 端口	是
	WEBHTTPS	State	HTTPS 使能状态	是
	WEBHTTPS	Port	HTTPS 端口	是
	RmcpConfig	LanState	IPMI LAN（RMCP）使能状态	是
	RmcpConfig	Port1	IPMI LAN（RMCP）端口 1	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	RmcpConfig	Port2	IPMI LAN（RMCP）端口 2	是
	RmcpConfig	LanPlusState	IPMI LAN（RMCP+）使能状态	是
系统配置	Snmp	V1State	支持 SNMPv1	是
	Snmp	V2CState	支持 SNMPv2c	是
	Snmp	V3Status	支持 SNMPv3	是
	Snmp	LongPasswordEnable	超长口令使能	是
	Snmp	ROCommunity	只读团体名 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	Snmp	RWCommunity	读写团体名 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	Snmp	RWCommunityState	读写团体名使能状态	是
	Snmp	SNMPV1V2CPermitRuleIds	SNMP 登录规则	是
	Snmp	AuthProtocol	SNMPv3 鉴权算法 **说明** iBMC V3.01.12.01 及以上版本不支持导	否

分类	导出项	导出子项	说明	是否支持配置文件导入生效
			出导入此配置项。	
	Snmp	PrivProtocol	SNMPv3 加密算法 说明 iBMC V3.01.12.01 及以上版本不支持导出导入此配置项。	否
	Snmp	sysContact	联系人	是
	Snmp	sysLocation	位置	是
	SecurityEnhance	TLSVersion	TLS 版本	是
	SecurityEnhance	EnableUserMgnt	业务侧用户管理使能状态	是
	Session	Timeout	Web 超时时间	是
	Session	Mode	Web 会话模式	是
	BMC	LocationInfo	设备位置	否，取值在配置文件中体现。
	MeInfo	CpuUtiliseThre	CPU 告警门限	是
	MeInfo	MemUtiliseThre	内存占用率告警门限	是
	MeInfo	DiskPartitionUsageThre	磁盘分区占用率告警门限	是
	PRODUCT	WOLState	网络唤醒使能状态	是
系统启动项	Bios	StartOption	第一启动设备	是
	Bios	StartOptionFlag	永久使能状态	是
	Bios	StartOptionFlagExt	系统启动项单次有效时，配置的生效状态	是
告警设置	SyslogConfig	EnableState	Syslog 使能状态	是
	SyslogConfig	MsgIdentity	Syslog 主机标识	是
	SyslogConfig	MsgSeverity	Syslog 告警级别	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	SyslogConfig	NetProtocol	Syslog 传输协议	是
	SyslogConfig	AuthType	Syslog 认证方式	是
	SyslogItemCfg	EnableState	Syslog 服务器使能	是
	SyslogItemCfg	DestAddr	Syslog 服务器地址	是
	SyslogItemCfg	DestPort	Syslog 服务器端口	是
	SyslogItemCfg	LogSrcMask	Syslog 日志类型	是
	TrapConfig	TrapEnable	Trap 使能	是
	TrapConfig	TrapVersion	Trap 版本	是
	TrapConfig	Trapv3Userid	Trap 选择使用的 V3 用户	是
	TrapConfig	TrapMode	Trap 模式	是
	TrapConfig	TrapIdentity	Trap 主机标识	是
	TrapConfig	CommunityName	Trap 团体名 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	TrapConfig	SendSeverity	Trap 告警发送级别	是
	TrapItemCfg	ItemEnable	Trap 服务器使能	是
	TrapItemCfg	DestIpAddr	Trap 服务器地址	是
	TrapItemCfg	DestIpPort	Trap 服务器端口	是
	TrapItemCfg	Separator	报文分隔符	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	TrapItemCfg	Time	报文显示内容（时间）	是
	TrapItemCfg	SensorName	报文显示内容（传感器名称）	是
	TrapItemCfg	Severity	报文显示内容（级别）	是
	TrapItemCfg	EventCode	报文显示内容（事件码）	是
	TrapItemCfg	EventDesc	报文显示内容（事件描述）	是
	TrapItemCfg	ShowKeyWord	报文显示关键字	是
	TrapItemCfg	BobEnable	带内通道上报 trap 报文使能状态	是
	TrapItemCfg	BmaVethIpAddr	通过带内上报 Trap 报文时对应的 BMA veth 网口 IP 地址	是
	TrapItemCfg	BmaVethIpPort	通过带内上报 Trap 报文时对应的 BMA veth 网口的端口号	是
	SmtpConfig	SmtpEnable	SMTP 使能	是
	SmtpConfig	SmtpServer	SMTP 地址	是
	SmtpConfig	TlsSendMode	SMTP 是否启动 tls	是
	SmtpConfig	AnonymousMode	SMTP 是否使用匿名	是
	SmtpConfig	LoginName	SMTP 发件人用户名	是
	SmtpConfig	LoginPasswd	SMTP 发件人密码 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置	否，敏感信息在配置文件中隐藏，不能直接生效。

分类	导出项	导出子项	说明	是否支持配置文件导入生效
			项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	
	SmtpConfig	SenderName	SMTP 发件人邮箱 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项。	否，敏感信息在配置文件中隐藏，不能直接生效。
	SmtpConfig	TempletTopic	SMTP 邮件主题	是
	SmtpConfig	TempletIpaddr	SMTP 主题附带主机名	是
	SmtpConfig	TempletBoardSn	SMTP 主题附带单板序列号	是
	SmtpConfig	TempletAsset	SMTP 主题附带产品资产标签	是
	SmtpConfig	SendSeverity	SMTP 设置告警发送级别	是
	SmtpItemCfg	EmailName	接收告警地址 **说明** iBMC V3.01.12.01 及以上版本不支持导出导入此配置项。	否，敏感信息在配置文件中隐藏，不能直接生效。
	SmtpItemCfg	EmailDesc	接收告警描述	是
	SmtpItemCfg	ItemEnable	接收告警使能	是
电源控制	ChassisPayload	PowerOffTimeoutEN	下电时限使能状态	是
	ChassisPayload	PowerOffTimeout	下电时限	是
	ChassisPayload	PwrButtonLock	屏蔽面板电源按钮功能使能状态	是
	ChassisPayload	PowerRestorePolicy	通电开机策略	是
功率	PowerCapping	Enable	功率封顶使能	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	PowerCapping	LimitValue	功率封顶值	是
	PowerCapping	FailAction	功率封顶失效关机使能 说明 该服务器不支持功率封顶配置，此配置项无效。	是
远程控制	Kvm	EncryptState	KVM 加密使能状态	是
	Vmm	EncryptState	VMM 加密使能状态	是
	Kvm	KeyboardMode	虚拟键盘、鼠标持续连接使能状态	是
	Kvm	KvmTimeout	远程控制台超时时长	是
	Kvm	LocalKVMState	本地 KVM 使能状态	是
	Kvm	AutoOSLockState	系统锁定状态	是
	Kvm	AutoOSLockType	系统锁定方式	是
	Kvm	AutoOSLockKey	自定义快捷键	是
录像回放	Video	VideoSwitch	录像使能状态	是
屏幕截图	Kvm	ScreenSwitch	最后一屏使能状态	是
黑匣子	Diagnose	BlackBoxState	黑匣子使能状态	是
串口数据	Diagnose	SolDataState	串口数据使能状态	是
固件升级	Upgrade	DowngradeDisabled	版本防降级功能使能状态	是
智能调速	Cooling	SmartCoolingMode	智能调速模式	是
	Cooling	CustomOutletTobj	出风口目标值	是
	Cooling	CustomCpuCoremTobj	CPU 目标值	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	Cooling	CustomDiskTobj	硬盘目标值	是
	Cooling	CustomMemoryTobj	内存目标值	是
	Cooling	CustomPCHTobj	PCH 目标值	是
	Cooling	CustomVRDTobj	VRD 目标值	是
	Cooling	CustomVDDQTobj	VDDQ 目标值	是
	Policy1Class	EnvRangeRdL	区间调速策略的温度和转速区间	是
其他	HMMSSHNAT	State	NAT 使能状态	是
	ExPortConfig	State	SSDP 使能状态	是
	HMMSSHNAT	Port	NAT 端口	是
	Bios	BiosPrintFlag	BIOS 全打印开关	是
	Cooling	Mode	风扇调速模式	否，取值在配置文件中体现。
	Cooling	PowerMode	电源模式	是
	Cooling	Level	风扇转速级别	否，取值在配置文件中体现。
	Stateless	Enable	无状态计算功能使能状态	是
	Stateless	SysManagerID	无状态计算功能远程管理 ID	是
	Stateless	AutoPowerOn	无状态计算功能是否自主上电开关	是
	Stateless	BroadcastNetSegment	无状态计算功能自动发现广播网段	是
	Stateless	BroadcastPort	无状态计算功能自动发现广播端口	是
	Stateless	SysManagerIP	无状态计算功能受控上电服务器 IP	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	Stateless	SysManagerPort	无状态计算功能受控上电服务器端口	是
	USBMassStorage	UmsMaxUpdateSpace	部件配置或升级包下发到NAND FLASH完成标识	是
	USBMassStorage	SpConfigFileReady	进入 SP 的方式	是
	USBMassStorage	SPStartmode	SP 操作完成到复位 OS 的时间间隔	是
	USBMassStorage	SysRestartDelay	OS 重启延时	是
	SmBios	Version	SMBIOS 中 Version 参数取值	是
	SmBios	SKUNumber	SMBIOS 中 SKUNumber 参数取值	是
	SmBios	Family	SMBIOS 中 Family 参数取值	是
	SMS	CdevChannelEnabled	带内字符设备通道使能状态	是

表8-2 BIOS 配置项

导出项	说明
DDRDebugLevel	内存打印级别
DDRFreqLimit	内存频率
DdrRefreshSupport	自定义刷新开关
DdrRefreshRate	自定义刷新速率
RankMargin	Rank Margin Tool 模式开关
RMTPatternLength	Rank Margin Tool 模式长度

导出项	说明
PerBITMargin	控制 Margin Test 粒度
CAMargin	控制命令线/地址线 Margin 测试开关
CAVrefMarginOption	控制命令线/地址线参考电压测试的配置
DieInterleaving	die 交织开关
ChannelInterleaving	内存通道交织开关
RankInterleaving	排列交织模式开关
NUMAEn	NUMA 开关
HWMemTest	内存测试开关
ECCSupport	ECC 和 SDEC 开关
BMCWDTEnable	POST 阶段看门狗开关
BMCWDTTimeout	设置 POST 阶段看门狗超时时长
BMCWDTAction	设置 POST 阶段看门狗超时操作
OSWDTEnable	OS 阶段开门狗开关
OSWDTTimeout	设置 OS 阶段看门狗超时时长
OSWDTAction	设置 OS 阶段看门狗超时操作
PXE1Setting	网口 NIC1 的 PXE 功能开关
PXE2Setting	网口 NIC2 的 PXE 功能开关
PXE3Setting	网口 NIC3 的 PXE 功能开关
PXE4Setting	网口 NIC4 的 PXE 功能开关
PCIEDPCSupport	DPC 开关
PCIESRIOVSupport	SRIOV 开关
PCIEPort[0]	port0 PCIe 端口开关
PCIELinkSpeedPort[0]	port0 链接速度配置
PCIELinkDeEmphasisPort[0]	port0 去加重 PCIe 端口
PCIEMaxPayloadSizePort[0]	port0 PCIe 最大有效字节
PCIEPort[8]	port8 PCIe 端口开关
PCIELinkSpeedPort[8]	port8 链接速度配置
PCIELinkDeEmphasisPort[8	port8 去加重 PCIe 端口

导出项	说明
]	
PCIEMaxPayloadSizePort[8]	port8 PCIe 最大有效字节
PCIEPort[10]	port10 PCIe 端口开关
PCIELinkSpeedPort[10]	port10 链接速度配置
PCIELinkDeEmphasisPort[10]	port10 去加重 PCIe 端口
PCIEMaxPayloadSizePort[10]	port10 PCIe 最大有效字节
PCIEPort[12]	port12 PCIe 端口开关
PCIELinkSpeedPort[12]	port12 链接速度配置
PCIELinkDeEmphasisPort[12]	port12 去加重 PCIe 端口
PCIEMaxPayloadSizePort[12]	port12 PCIe 最大有效字节
PCIEPort[16]	port16 PCIe 端口开关
PCIELinkSpeedPort[16]	port16 链接速度配置
PCIELinkDeEmphasisPort[16]	port16 去加重 PCIe 端口
PCIEMaxPayloadSizePort[16]	port16 PCIe 最大有效字节
PCIEPort[18]	port18 PCIe 端口开关
PCIELinkSpeedPort[18]	port18 链接速度配置
PCIELinkDeEmphasisPort[18]	port18 去加重 PCIe 端口
PCIEMaxPayloadSizePort[18]	port18 PCIe 最大有效字节
PCIEPort[24]	port24 PCIe 端口开关
PCIELinkSpeedPort[24]	port24 链接速度配置
PCIELinkDeEmphasisPort[24]	port24 去加重 PCIe 端口
PCIEMaxPayloadSizePort[24]	port24 PCIe 最大有效字节
PCIEPort[28]	port28 PCIe 端口开关
PCIELinkSpeedPort[28]	port28 链接速度配置

导出项	说明
PCIELinkDeEmphasisPort[28]	port28 去加重 PCIe 端口
PCIEMaxPayloadSizePort[28]	port28 PCIe 最大有效字节
PCIEPort[32]	port32 PCIe 端口开关
PCIELinkSpeedPort[32]	port32 链接速度配置
PCIELinkDeEmphasisPort[32]	port32 去加重 PCIe 端口
PCIEMaxPayloadSizePort[32]	port32 PCIe 最大有效字节
PCIEPort[34]	port34 PCIe 端口开关
PCIELinkSpeedPort[34]	port34 链接速度配置
PCIELinkDeEmphasisPort[34]	port34 去加重 PCIe 端口
PCIEMaxPayloadSizePort[34]	port34 PCIe 最大有效字节
PCIEPort[36]	port36 PCIe 端口开关
PCIELinkSpeedPort[36]	port36 链接速度配置
PCIELinkDeEmphasisPort[36]	port36 去加重 PCIe 端口
PCIEMaxPayloadSizePort[36]	port36 PCIe 最大有效字节
EnableSMMU	SMMU 开关
EnableFDTTable	DTB 表开关
EnableGOP	GOP 开关
EnableSpcr	SPCR 开关
SYSDBGLevel	系统 debug 等级设置
CPUPrefetchConfig	CPU 预取功能开关
ENRASSupport	RAS 开关
CheckAlgorithm	检查算法开关
EnPoison	损坏开关
PatrolScrub	激活巡检开关
PatrolScrubDuration	巡检周期

导出项	说明
DemandScrubMode	消极巡检开关
CorrectErrorThreshold	校正错误阈值
FunnelPeriod	每分钟漏斗周期
AdvanceDeviceCorrection	推进设备校正
RankSparing	等级保留开关
DpcFeature	DPC 需求开关
EcrcFeature	ECRC 需求开关
CompletionTimeout	完成超时开关
CompletionTimeoutValue	完成超时值
HotPlug	热插拔开关
NoBootResetSetting	无启动设备自动重启开关

表8-3 RAID 控制器配置项

分类	导出项	导出子项	说明	是否支持配置文件导入
存储	RaidController	Type	RAID 控制器类型。	否，取值在配置文件中体现。
	RaidController	CopybackEnabled	RAID 控制器回拷功能状态。	是
	RaidController	SMARTerCopybackEnabled	RAID 控制器在检测到物理盘 SMART 错误之后是否自动进行回拷。	是
	RaidController	JBODEnabled	RAID 控制器 JBOD 功能状态。	是

9 术语和缩略语

A

AC	Alternating Current（交流电）
AES	Advanced Encryption Standard（高级加密标准）

B

BBU	Backup Battery Unit（备份电池单元）
BIOS	Basic Input Output System（基本输入输出系统）

C

CA	Certificate Authority（证书颁发中心）
CD	Compact Disc（光盘）
CLI	Command-line Interface（命令行接口）
COM	Cluster Communication Port（COM 口）
CPLD	Complex Programmable Logic Device（复杂可编程逻辑器件）
CPU	Central Processing Unit（中央处理单元）
CRL	Certificate Revocation List（证书撤销列表）

D

disk	drive 的同义词，泛指所有硬盘。
drive	disk 的同义词，泛指所有硬盘。
DC	Direct Current（直流电）
DCMI 1.5	Data Center Manageability Interface Specification v1.5（数据中心管理接口）
DES	Data Encryption Standard（数据加密标准）

DNS	Domain Name Server（网域名称服务器）
DVD	Digital Video Disc（数字视频光盘）

E

EIST	Enhanced Intel SpeedStep Technology（增强型 Intel SpeedStep 技术）
ESN	Equipment Serial Number（设备序列号）

F

FDM	Fault Diagnosis & Management（故障诊断管理）
FC	Fibre Channel（光纤通道）

G

GPU	Graphics Processing Unit（图形处理器）
GUI	Graphical User Interface（图形用户界面）

H

HDD	Hard Disk Drive（硬式磁盘驱动器）
HMM	Hyper Management Module（超级管理模块）
HPRE	High Performance RSA Engine（高性能 RSA 加速引擎）
HTTP	Hypertext Transfer Protocol（超文本传输协议）
HTTPS	Hypertext Transfer Protocol Secure（HTTPS 加密协定）

I

iBMA	intelligent baseboard management agent（服务器智能板级管理代理）
iBMC	Intelligent Baseboard Management Controller（智能服务器管理控制单元）
IMU	I/O Board Management Unit（IO 板管理单元）
IO	Integrated Operation（集成运作）
IP	Internet Protocol（互联网协议）
IPMI	Intelligent Platform Management Interface（智能平台管理接口）

J

JBOD	Just a Bundle Of Disks（磁盘簇）

K

Kerberos	是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。在 Hadoop 里面用于支撑多租户的实现。
KVM	keyboard, video, and mouse（键盘，显示器，鼠标三合一）

L

LAN	Local Area Network（局域网）
LCD	Liquid Crystal Display（液晶显示器）
LDAP	Lightweight Directory Access Protocol（轻型目录访问协议）
LLDP	Link Layer Discovery Protocol（链路层发现协议）
LOM	LAN On Motherboard（板载网络）

M

MAC	Media Access Control（媒体接入控制）
MCTP	Management Component Transport Protocol（管理组件传输协议）
MD5	Message-Digest Algorithm 5（消息验证码）

N

NTP	Network Time Protocol（网络时间协议）
NMI	Non-Maskable Interrupt（不可屏蔽中断）
NCSI	Network Controller Sideband Interface（网络控制器边带接口）
NPU	Network Process Unit（网络处理单元）
NVMe	Non-Volatile Memory express（非易失性高速传输总线）

O

OS	Operating System（作业系统）
OCP	Open Compute Project（开放计算项目）
OID	Object Identifier（对象标识符）
OCSP	Online Certificate Status Protocol（在线证书状态协议）

P

PCB	Printed Circuit Board（印制电路板）
PCIe	Peripheral Component Interconnect Express（快捷外围部件互连标准）
PCH	Platform Controller Hub（平台控制单元）
PFAE	Proactive Failure Analysis Engine（主动故障分析引擎）
PXE	Pre-boot Execution Environment（预启动执行环境）
PSU	Power Supply Unit（电源模块）

R

RAID	Redundant Array of Independent Disks（独立磁盘冗余数组）
RDE	RAID DIF engine（RAID DIF 运算加速引擎模块）
Redfish	DMTF 的 Redfish™API 是一个开放的行业标准规范和模式，有助于简化和安全管理现代可扩展平台硬件。
RFC	Request For Comments（请求注解）
RMCP	Remote Management Control Protocol（远程管理控制协议）

S

SAS	Serial Attached SCSI（串行连接的 SCSI）
SATA	Serial Advanced Technology Attachment（串行高级技术附件）
SEL	System Event Log（系统事件日志）
SFTP	Secure File Transfer Protocol（安全文件传输协议）
SHA	Secure Hash Algorithm（安全散列算法）
SID	Security Identifier（安全标识号）
SMTP	Simple Mail Transfer Protocol（简单邮件传输协议）
SNMP	Simple Network Management Protocol（简单网络管理协议）
SOL	Serial Over LAN（局域网承载串行）
SSD	Solid-State Drive（固态硬盘）
SSH	Secure Shell（安全外壳）
SSL	Secure Sockets Layer（安全套接层）
SSO	Single Sign-On（单点登录）

T

TLS	Transport Layer Security（传输层安全性协议）

U

UEFI	Unified Extensible Firmware Interface（统一可扩展固件接口）
UID	Unit /Identification Light（定位指示灯）
UUID	Universally Unique /Identifier（通用唯一识别码）
USB	Universal Serial Bus（通用串行总线）

V

VGA	Video Graphics Array（视频图形阵列）
VLAN	Virtual Local Area Network（虚拟局域网）
VMM	Virtual Media Manager（虚拟媒体管理器）
VNC	Virtual Network Console（虚拟网络控制台）

W

WWPN	World Wide Port Name（全球端口名称）
WWNN	World Wide Node（全球惟一节点名字）