FusionServer Pro 机架服务器 iBMC V250 至 V259

用户指南

文档版本	24
发布日期	2021-06-07

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

前言

概述

本文档为服务器底层管理软件iBMC（Intelligence 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。
- Web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华为服务器进行网络部署及维护时，需要使用的命令。

对用于生产、装备、返厂检测维修的命令，不在本资料中说明。

部分仅用于工程实施或定位故障的高级命令，如使用不当，将可能导致设备异常或者业务中断。此部分命令的资料不在本文档中提供，如您需要，请向华为公司申请。

本文档适用于以下FusionServer Pro机架服务器：

- RH1288A V2和RH2288A V2
- 5288 V3、RH1288 V3、RH2288 V3、RH2288H V3、RH5885 V3、RH5885H V3和RH8100 V3
- 1288H V5、2288 V5、2288C V5、2288H V5、2488 V5、2488H V5、5885H V5和8100 V5

读者对象

本文档主要适用于以下人员：

- 服务器产品安装工程师
- 服务器产品维护工程师

华为认为您是专业的服务器设备服务人员，且经过识别设备危险的培训，能识别危险等级。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

修改记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本	发布日期	修改说明
24	2021-06-07	更新了**3.8.6 固件升级**。
23	2021-04-21	更新了**6.3 恢复iBMC默认配置**。
22	2021-03-17	更新了**3.7.6 服务配置**和**3.10.1 无法启动Java集成远程控制台**。
21	2020-11-15	更新了**3.7.10 导入导出**、**3.9 远程控制**、**4.2.2 确认管理网口IP**、**6.10 配置iBMC Syslog日志上报功能**和**6.11 使用VNC登录服务器实时桌面**。
20	2019-11-11	更新了**3.8.6 固件升级**、**4.3.28 挂载文件到虚拟光驱（vmm -d connect）**和**4.8.19 查询和设置带内用户管理使能状态（user -d usermgmtbyhost）**。
19	2019-07-30	手册更名。
18	2019-05-30	更新了**4.3.28 挂载文件到虚拟光驱（vmm -d connect）**、**4.7.9 查询服务器的设备序列号（serialnumber）**和**4.8.17 导入弱口令字典（weakpwddic -v import）**。

文档版本	发布日期	修改说明
17	2019-02-22	更新了**4.5.1 查询和设置syslog使能状态（syslog -d state）**。
16	2018-11-05	更新了**3.8.6 固件升级**、**3.9.1 Java远程虚拟控制台**、**7 独立远程控制台**。
15	2018-08-08	• 更新了**3.1 登录iBMC WebUI**、**3.9.1 Java远程虚拟控制台**。 • 新增**6.12 为iBMC导入信任证书和根证书**。
14	2018-07-05	更新了**3.4.3 告警设置**、**3.9 远程控制**。
13	2018-06-07	新增章节**7.5 （Redhat）使用独立远程控制台登录服务器实时桌面**。
12	2018-05-30	更新了**3.7.7 系统配置**、**3.11 一键收集信息说明**。
11	2018-05-03	更新了**3.9 远程控制**。
10	2018-03-29	更新了**3.6.1 电源控制**、**3.6.3 节能设置**和**4.10.3 设置硬盘locate指示灯状态（locate）**。
09	2018-02-11	更新了**表3-40**。
08	2018-01-31	• 更新了**表3-3**中产品资产标签的描述。 • 更新了**表3-67**中的兼容性列表。
07	2017-12-28	更新了**表3-37**的描述。
06	2017-11-13	更新了**3.5.3 黑匣子**章节中黑匣子的安装和使用方法介绍。
05	2017-10-12	更新了**3.7.2 LDAP配置**功能介绍的描述。
04	2017-09-30	更新了**表3-38**中权限组的描述。
03	2017-09-12	更新了**表3-67**中的兼容性列表。
02	2017-07-25	第二次正式发布。
01	2017-06-30	第一次正式发布。

目 录

前言 ii
1 iBMC 管理软件概述 1
1.1 iBMC 简介 1
1.2 安全特性 2
1.3 常用接口操作 3
1.3.1 iBMC Web 界面 3
1.3.2 iBMC CLI 3
1.3.3 Redfish 接口 3
1.3.4 iBMC 移动应用程序 3
2 用户必读 4
2.1 iBMC 使用准则 4
2.2 获取 iBMC 版本信息 4
2.3 默认参数 5
2.4 登录须知 6
3 Web 界面介绍 9
3.1 登录 iBMC WebUI 9
3.2 新手入门 12
3.2.1 基础操作 12
3.3 信息 13
3.3.1 信息概况 13
3.3.2 系统信息 19
3.3.3 实时监控 38
3.3.4 传感器 40
3.4 告警与事件 42
3.4.1 当前告警 42
3.4.2 系统事件 43
3.4.3 告警设置 45
3.5 诊断 54
3.5.1 录像回放 54
3.5.2 屏幕截图 57
3.5.3 黑匣子 59
3.5.4 串口数据 61

3.5.5 故障诊断日志 62
3.5.6 内存热插拔（RH8100 V3 服务器特有功能） 63
3.6 电源与能耗 64
3.6.1 电源控制 64
3.6.2 功率 69
3.6.3 节能设置 74
3.7 配置 79
3.7.1 本地用户 79
3.7.2 LDAP 配置 90
3.7.3 双因素认证 100
3.7.4 安全增强 103
3.7.5 网络配置 107
3.7.6 服务配置 117
3.7.7 系统配置 122
3.7.8 系统启动项 135
3.7.9 SSL 证书 136
3.7.10 导入导出 140
3.8 系统管理 142
3.8.1 操作日志 142
3.8.2 运行日志 144
3.8.3 安全日志 145
3.8.4 工作记录 146
3.8.5 在线用户 147
3.8.6 固件升级 148
3.8.7 语言更新 153
3.9 远程控制 155
3.9.1 Java 远程虚拟控制台 163
3.9.2 HTML5 集成远程控制台 173
3.10 远程虚拟控制台异常问题帮助 181
3.10.1 无法启动 Java 集成远程控制台 181
3.10.2 Google Chrome 不支持该插件 182
3.10.3 Linux 系统下 Firefox 插件版本过旧无法启动远程虚拟控制台 182
3.10.4 打开远程虚拟控制台时鼠标键盘失效 183
3.10.5 只能看到 Java web start 图标无法打开 KVM 183
3.10.6 打开 KVM 后显示非法用户 184
3.10.7 打开 KVM 后显示与管理系统连接失败 185
3.10.8 打开 HTML5 集成远程控制台后显示设置信任证书超时 186
3.11 一键收集信息说明 187
4 命令行介绍 207
4.1 命令行说明 207
4.1.1 格式说明 207
4.1.2 帮助 208

4.2 登录命令行 211
4.2.1 通过 BIOS 修改 iBMC 默认用户密码 211
4.2.2 确认管理网口 IP 218
4.2.3 登录 iBMC 命令行 222
4.3 iBMC 命令 224
4.3.1 查询 iBMC 管理网口的 IP 信息（ipinfo） 224
4.3.2 设置 iBMC 网口的 IPv4 信息（ipaddr） 226
4.3.3 设置 iBMC 网口的 IPv4 模式（ipmode） 227
4.3.4 设置 iBMC 网口的 IPv4 网关（gateway） 228
4.3.5 设置 iBMC 网口的 IPv6 信息（ipaddr6） 228
4.3.6 设置 iBMC 网口的 IPv6 模式（ipmode6） 230
4.3.7 设置 iBMC 网口的 IPv6 网关（gateway6） 231
4.3.8 设置网口模式（netmode） 232
4.3.9 设置激活端口（activeport） 233
4.3.10 设置网口 VLAN（vlan） 234
4.3.11 查询和设置串口方向（serialdir） 235
4.3.12 重启 iBMC 管理系统（reset） 236
4.3.13 固件升级（upgrade） 236
4.3.14 截屏命令（printscreen） 237
4.3.15 iBMC 软件回滚（rollback） 238
4.3.16 查询软件回滚状态（rollbackstatus） 239
4.3.17 设置服务状态（service -d state） 239
4.3.18 设置指定服务的端口号（service -d port） 240
4.3.19 查询服务状态（service -d list） 241
4.3.20 设置登录安全性信息功能的使能状态（securitybanner -d state） 242
4.3.21 定制登录安全信息（securitybanner -d content） 242
4.3.22 查询登录安全信息（securitybanner -d info） 243
4.3.23 导入 SSL 证书（certificate -d import） 244
4.3.24 查询 SSL 证书信息（certificate -d info） 245
4.3.25 导出配置文件（config -d export） 245
4.3.26 导入配置文件（config -d import） 246
4.3.27 导入 CRL 文件（crl） 247
4.3.28 挂载文件到虚拟光驱（vmm -d connect） 249
4.3.29 中断虚拟光驱的连接（vmm -d disconnect） 250
4.3.30 查询虚拟媒体信息（vmm -d info） 250
4.3.31 查询和设置散热功率模式（coolingpowermode） 251
4.4 Trap 命令 251
4.4.1 查询和设置 SNMP trap 状态（trap -d state） 251
4.4.2 设置 SNMP trap 上报端口号（trap -d port） 252
4.4.3 设置 SNMP trap 团体名称（trap -d community） 253
4.4.4 设置 SNMP trap 目的 IP 地址（trap -d address） 254
4.4.5 查询 Trap 上报目的地址信息（trap -d trapiteminfo） 254

4.4.6 查询和设置 SNMP trap 版本信息（trap -d version） 255
4.4.7 查询和设置 SNMP trap 告警发送级别（trap -d severity） 256
4.4.8 查询和设置 SNMP trap V3 用户（trap -d user） 257
4.4.9 查询和设置 SNMP trap V3 鉴权和加密协议（trap -d protocol） 257
4.4.10 查询和设置 SNMP trap 模式（trap -d mode） 258
4.5 Syslog 命令 259
4.5.1 查询和设置 syslog 使能状态（syslog -d state） 259
4.5.2 查询和设置证书认证方式（syslog -d auth） 260
4.5.3 查询和设置 syslog 主机标识（syslog -d identity） 261
4.5.4 查询和设置传输协议类型（syslog -d protocol） 261
4.5.5 查询和设置上报日志的级别（syslog -d severity） 262
4.5.6 查询和上传服务器根证书（syslog -d rootcertificate） 263
4.5.7 查询和上传本地证书（syslog -d clientcertificate） 264
4.5.8 设置 syslog 服务器地址（syslog -d address） 265
4.5.9 设置 syslog 服务器端口号（syslog -d port） 266
4.5.10 设置上报日志类型（syslog -d logtype） 266
4.5.11 测试 syslog 服务器是否可连接（syslog -d test） 267
4.5.12 查询所有 syslog 上报通道配置信息（syslog -d iteminfo） 268
4.6 服务器命令 268
4.6.1 查询和设置启动设备（bootdevice） 268
4.6.2 设置服务器重启方式（frucontrol） 269
4.6.3 查询和设置服务器上下电状态（powerstate） 270
4.6.4 查询和设置服务器的下电时限（shutdowntimeout） 271
4.6.5 查询服务器板载网卡 MAC 地址（macaddr） 272
4.6.6 查询系统可用网口（ethport） 272
4.6.7 清除 BIOS Flash（clearcmos） 273
4.6.8 查询 RAID 控制器信息（ctrlinfo） 273
4.6.9 查询逻辑盘信息（ldinfo） 275
4.6.10 查询物理盘信息（pdinfo） 277
4.6.11 查询磁盘组信息（arrayinfo） 279
4.6.12 创建逻辑盘（createld） 281
4.6.13 添加逻辑盘（addld） 284
4.6.14 删除逻辑盘（deleteld） 286
4.6.15 修改逻辑盘属性（ldconfig） 286
4.6.16 修改 RAID 控制器属性（ctrlconfig） 288
4.6.17 修改物理盘属性（pdconfig） 289
4.7 系统命令 290
4.7.1 查询系统名称（systemname） 290
4.7.2 设置 iBMC 时区（timezone） 291
4.7.3 查询 iBMC 时间（time） 292
4.7.4 查询设备的版本信息（version） 292
4.7.5 查询 FRU 信息（fruinfo） 294

4.7.6 查询系统的健康状态（health） 295
4.7.7 查询系统的健康事件信息（healthevents） 295
4.7.8 查询 80 口信息（port80） 296
4.7.9 查询服务器的设备序列号（serialnumber） 296
4.7.10 查询和清除系统 SEL 信息（sel） 297
4.7.11 查询系统操作日志（operatelog） 298
4.7.12 下载系统串口数据（systemcom） 299
4.7.13 下载黑匣子数据（blackbox） 299
4.7.14 下载 BIOS（download） 300
4.7.15 升级 BIOS（upgradebios） 301
4.7.16 设置 iBMC 网口状态（ethlink） 302
4.7.17 一键收集信息（diaginfo） 302
4.7.18 恢复 iBMC 出厂设置（restore） 303
4.7.19 设置 CLP notimeout 功能状态（notimeout） 303
4.7.20 更新系统工作密钥（workkey） 304
4.7.21 查询和设置自动发现配置（autodiscovery） 304
4.7.22 查询和设置受控上电配置（poweronpermit） 305
4.7.23 查询和清除上电锁的锁定状态（poweronlock） 306
4.7.24 查询和设置 BIOS 全打印开关状态（biosprint） 307
4.7.25 重启 iME（resetiME） 307
4.8 用户管理命令 308
4.8.1 查询所有用户信息（userlist/list） 308
4.8.2 添加新用户（adduser） 309
4.8.3 修改用户密码（password） 311
4.8.4 删除用户（deluser） 312
4.8.5 设置用户权限（privilege） 312
4.8.6 查询和设置密码检查功能（passwordcomplexity） 313
4.8.7 锁定用户（user -d lock） 315
4.8.8 解除用户锁定状态（user -d unlock） 315
4.8.9 查询和设置密码最短使用期（minimumpasswordage） 316
4.8.10 设置紧急用户（emergencyuser） 316
4.8.11 为用户添加 SSH 公钥（addpublickey） 317
4.8.12 删除用户的 SSH 公钥（delpublickey） 318
4.8.13 查询和设置 SSH 用户密码认证使能状态（sshpasswordauthentication） 318
4.8.14 设置用户登录 iBMC 的接口类型（interface） 319
4.8.15 设置弱口令字典认证使能状态（weakpwddic） 320
4.8.16 导出弱口令字典（weakpwddic -v export） 321
4.8.17 导入弱口令字典（weakpwddic -v import） 322
4.8.18 设置 SNMPv3 用户的加密密码（snmpprivacypassword） 324
4.8.19 查询和设置带内用户管理使能状态（user -d usermgmtbyhost） 325
4.9 NTP 命令 325
4.9.1 查询 NTP 信息（ntpinfo） 326

4.9.2 设置 NTP 状态（ntp -d status） 326
4.9.3 设置 NTP 信息获取方式（ntp -d mode） 327
4.9.4 设置首选 NTP 服务器地址（ntp -d preferredserver） 328
4.9.5 设置备用 NTP 服务器地址（ntp -d alternativeserver） 328
4.9.6 设置服务器身份认证状态（ntp -d authstatus） 329
4.9.7 上传 NTP 组密钥（ntp -d groupkey） 330
4.10 指示灯命令 331
4.10.1 查询服务器指示灯信息（ledinfo） 331
4.10.2 设置 UID 指示灯状态（identify） 332
4.10.3 设置硬盘 locate 指示灯状态（locate） 332
4.11 风扇命令 333
4.11.1 设置风扇运行速度（fanlevel） 333
4.11.2 设置风扇运行模式（fanmode） 334
4.11.3 查询风扇工作状态（faninfo） 335
4.12 传感器命令 335
4.12.1 查询所有传感器的所有信息（sensor -d list） 335
4.12.2 传感器测试命令（sensor -d test） 342
4.13 电源命令 342
4.13.1 设置电源工作模式（psuworkmode） 342
4.13.2 查询电源具体信息（psuinfo） 343
4.14 U-Boot 命令 344
4.14.1 登录 U-Boot 344
4.14.2 U-Boot 命令参考 345
4.15 SOL 命令 346
4.15.1 建立 SOL 会话（sol -d activate） 346
4.15.2 注销 SOL 会话（sol -d deactivate） 347
4.15.3 设置 SOL 会话超时时间（sol -d timeout） 348
4.15.4 查询 SOL 会话列表（sol -d session） 349
4.15.5 查询 SOL 会话配置信息（sol -d info） 349
5 常用维护命令 350
5.1 查看帮助信息（help） 350
5.2 断开连接（exit） 352
5.3 检查网络连通性（ping、ping6） 352
5.4 free 命令（free） 353
5.5 ps 命令（ps） 353
5.6 netstat 命令（netstat） 354
5.7 df 命令（df） 354
5.8 ifconfig 命令（ifconfig） 355
5.9 route 命令（route） 355
5.10 top 命令（top） 356
5.11 禁止 CLP 超时（notimeout） 357
6 常用操作 358

6.1 使用 PuTTY 登录服务器（串口方式）..... 358
6.2 使用 PuTTY 登录服务器（网口方式）..... 360
6.3 恢复 iBMC 默认配置..... 362
6.4 配置 iBMC WebUI Trap..... 365
6.5 配置 iBMC WebUI SMTP..... 367
6.6 配置 LDAP 功能..... 368
6.6.1 搭建 LDAP 服务器..... 368
6.6.2 在 iBMC 侧配置 LDAP 功能..... 385
6.7 配置 iBMC WebUI DNS（手动）..... 387
6.8 配置 SSH 用户密钥登录 iBMC 命令行..... 388
6.9 配置 iBMC SSL 证书..... 392
6.10 配置 iBMC Syslog 日志上报功能..... 394
6.11 使用 VNC 登录服务器实时桌面..... 396
6.12 为 iBMC 导入信任证书和根证书..... 399
7 独立远程控制台..... 409
7.1 简介..... 409
7.2 （Windows）使用独立远程控制台登录服务器实时桌面..... 410
7.3 （Ubuntu）使用独立远程控制台登录服务器实时桌面..... 413
7.4 （Mac）使用独立远程控制台登录服务器实时桌面..... 415
7.5 （Redhat）使用独立远程控制台登录服务器实时桌面..... 418
8 配置文件说明..... 421
9 FAQ..... 436
9.1 V5 服务器安装 Windows 后出现未知设备..... 436

1 iBMC 管理软件概述

1.1 iBMC简介
1.2 安全特性
1.3 常用接口操作

1.1 iBMC 简介

iBMC智能管理系统（以下简称iBMC）是服务器的远程管理系统，提供了丰富的管理功能。

- 丰富的管理接口

  提供标准的DCMI1.5/IPMI1.5/IPMI2.0接口、命令行接口、Redfish接口、超文本传输安全协议（HTTPS，Hypertext Transfer Protocol Secure）和简单网络管理协议（SNMP，Simple Network Management Protocol），满足多种方式的系统集成需求。
- 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功能，支持基于部件的精准故障诊断，方便部件故障定位和更换。
  - 支持Syslog报文、Trap报文、电子邮件上报告警，方便上层网管收集服务器故障信息。
  - 支持LCD直接从iBMC获取设备信息。
- 安全管理手段
  - 通过软件镜像备份，提高系统的安全性，即使当前运行的软件完全崩溃，也可以从备份镜像启动。
  - 多样化的用户安全控制接口，保证用户登录安全性。
  - 支持多种证书的导入替换，保证数据传输的安全性。
- 系统维护接口
  - 支持虚拟KVM（Keyboard, Video, and Mouse）和虚拟媒体功能，提供方便的远程维护手段。

  - 支持RAID的带外监控和配置，提升了RAID配置效率和管理能力。
- 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。

1.2 安全特性

- NCSI

  服务器管理平面与业务平面分离。iBMC可以通过NCSI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 Web 界面

iBMC 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。WebUI的顶层分支包括信息、告警与事件、诊断、电源与能耗、配置、系统管理、远程控制等几个大的节点，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 Web界面介绍**。

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。

关于服务器支持的Redfish接口的详细说明，请参考服务器的**iBMC Redfish 接口说明**。

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。移动应用程序直接与iBMC进行交互，对服务器进行常规的配置和监控。

关于SmartServer Mobile的详细说明，请参考服务器的**SmartServer 用户指南**。

2 用户必读

2.1 iBMC使用准则
2.2 获取iBMC版本信息
2.3 默认参数
2.4 登录须知

2.1 iBMC 使用准则

- 使用专用网络或者具有防火墙的安全网络对iBMC进行配置，避免被攻击。
- 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版本*X.XX*即*VXXX*。例如，“2.50”即“V250”。

iBMC的版本信息的获取方式包括：

- 通过iBMC版本说明查询。

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

- 通过Web界面查询。

登录iBMC，在“信息概况”页面的“基本信息”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:        (U4282)2.50
Active iBMC    Build:          002
......
```

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	V3服务器默认值	V5服务器默认值
iBMC默认用户名和密码	用户名：**root** 密码：**Huawei12#$**	用户名：**Administrator** 密码：**Admin@9000**
iBMC管理网口默认IP地址	• RH8100 V3/8100 V5： – 8P单系统：192.168.2.100 – 4P双系统： – 主管理网口：192.168.2.100 – 从管理网口：192.168.2.101 • 其他机架服务器：192.168.2.100	• RH8100 V3/8100 V5： – 8P单系统：192.168.2.100 – 4P双系统： – 主管理网口：192.168.2.100 – 从管理网口：192.168.2.101 • 其他机架服务器：192.168.2.100
U-Boot密码	Huawei12#$	Admin@9000
SNMP只读团体名	roAdmin12#$	roAdministrator@9000
SNMP读写团体名	rwAdmin12#$	rwAdministrator@9000
Trap团体名	TrapAdmin12#$	TrapAdmin12#$

2.4 登录须知

iBMC 管理网口地址

- 首次登录时，请使用iBMC默认地址。
  默认地址可从产品铭牌或**2.3 默认参数**获取。
- 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 Web界面介绍**。
  - 直连用户可在iBMC CLI修改。修改方法请参考本文档**4 命令行介绍**。
  - 直连用户可在BIOS Setup中修改。修改方法请参考BIOS参数参考。
  - 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DNS/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。
  - PC直连iBMC串口，在CLI下查询当前地址。
  - 使用物理KVM，重启服务器并登录BIOS查询。

登录用户类型

iBMC登录用户包括本地用户、LDAP用户。

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。

客户端环境

登录iBMC Web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IE及Java的配套关系有特殊要求。

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 9.0～11.0 **说明** HTML5仅支持Internet Explorer 10.0及以上版本的浏览器。	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144

操作系统	浏览器	Java运行环境
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Windows 8 32位 Windows 8 64位	Internet Explorer 10.0～11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Windows 10 64位	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
Windows 2012 R2 64位	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
Windows 2016 64位	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
Windows Server 2008 R2 64位	Internet Explorer 9.0～11.0 **说明** HTML5仅支持Internet Explorer 10.0及以上版本的浏览器。	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Windows Server 2012 64位	Internet Explorer 10.0～11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Red Hat 6.0 64位	Mozilla Firefox 39.0～54.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144

操作系统	浏览器	Java运行环境
MAC OS X v10.7	Safari 8.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	

3 Web 界面介绍

3.1 登录iBMC WebUI
3.2 新手入门
3.3 信息
3.4 告警与事件
3.5 诊断
3.6 电源与能耗
3.7 配置
3.8 系统管理
3.9 远程控制
3.10 远程虚拟控制台异常问题帮助
3.11 一键收集信息说明

3.1 登录 iBMC WebUI

本指南以IE 11.0浏览器为例介绍登录iBMC Web管理界面的操作步骤。

说明

- 通过Web进行界面操作，最多只能有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Web界面执行任何操作，系统将自动登出。
- 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，亦可通过管理员用户在命令行下解锁。
- 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。

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3-67**。

步骤2 为PC配置与iBMC管理网口同一网段的IP地址，并保证PC能够ping通iBMC管理网口的IP地址。

- 单系统机架服务器的iBMC管理网口默认IP地址为“192.168.2.100”。
- 双系统机架服务器的主iBMC管理网口默认IP地址为“192.168.2.100”，从iBMC管理网口默认IP地址为“192.168.2.101”。

步骤3 通过网线将PC连接到iBMC管理网口。

步骤4 打开IE浏览器，并在地址栏中输入“https://ipaddress/”。（其中ipaddress为iBMC管理网口的IP地址，IP地址的具体确认方法请参见**4.2.2 确认管理网口IP**。）

弹出如**图3-1**所示的安全告警窗口。

图 3-1 安全告警

说明

- 如果需要使用非中、英、日语的浏览器登录iBMC，则需要将iBMC升级至V260及以上版本，否则可能无法正常显示登录页面。
- 登录时可能会弹出“安全告警”界面，您可以选择忽略此告警信息或根据需要执行以下操作屏蔽该界面：
  - 如果您有可信任的证书，可以为iBMC导入信任证书和根证书。有关详细信息，请参考**6.12 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 选择一种方式登录iBMC界面。

说明

- “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”之外的其它选项时，支持输入的用户名的最大长度为255个字符。
- 以LDAP方式登录iBMC WebUI时，密码最大长度在V294之前版本为20个字符，在V294及之后版本为255个字符。

使用本地用户登录iBMC界面。

1. 选择界面语言。
2. 输入用户名和密码。

   说明

   - V3服务器的iBMC默认用户为**root**，默认密码为**Huawei12#$**。
   - V5服务器的iBMC默认用户为**Administrator**，默认密码为**Admin@9000**。
3. 在“域名”下拉列表中，选择“这台iBMC”或“自动匹配”。
4. 单击“登录”。成功登录，显示“信息概况”界面。界面右上角将显示登录的用户名。

   说明

   - 如果使用IE浏览器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，无法登录，同时按下“Ctrl”+“Shift”+“DEL”键，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的Web界面。
   - 如果使用IE浏览器无法登录iBMC的Web界面，在IE浏览器中打开“工具 > Internet 选项 > 高级”页面，单击“重置”后，可以正常登录。

使用LDAP用户登录iBMC 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考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。具体操作请参考“LDAP配置”界面。

  a. 选择界面语言。

  b. 输入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”仅可选择“自动匹配”）。

  以LDAP方式登录iBMC WebUI时，密码最大长度在之前版本为20个字符，在V294及之后版本为255个字符。

  c. 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。

  d. 单击“登录”。

  成功登录，显示“信息概况”界面。界面右上角将显示登录的用户名。

----结束

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	在登录界面中，从下拉列表中切换语言。

操作	说明
查看信息概况	选择“信息 > 信息概况”。 “信息概况”界面显示如下信息： • 产品名称 • 产品序列号 • iBMC的IP地址 • iBMC固件版本 • BIOS固件版本 • GUID • Web最大会话数 • 在线用户数 • 告警和指示灯状态
查看联机帮助	在系统界面中，单击  。
查看用户信息	在登录iBMC界面后，单击右上角  后的用户名，例如“test”。 弹出“当前用户信息”窗口。该窗口显示用户所属的用户组、登录的IP地址和时间。
查看告警信息	在登录iBMC界面后，单击右上角的告警图标，跳转至“当前告警”页面，显示当前存在的告警的级别、描述、事件码、产生时间、以及处理建议。
退出系统	单击右上角的“退出”
刷新界面信息	单击界面右侧的  。

3.3 信息

3.3.1 信息概况

功能介绍

通过使用“信息概况”界面的功能，您可以获取服务器的基本信息，虚拟按键和常用操作快捷入口。

界面描述

在上方标题栏中，选择“信息”，在左侧导航树中选择“信息概况”，显示“信息概况”界面。

“信息概况”界面各区域如**图3-3**、**图3-4**和**图3-5**所示。

各区域展示的信息如**表3-2**所示。

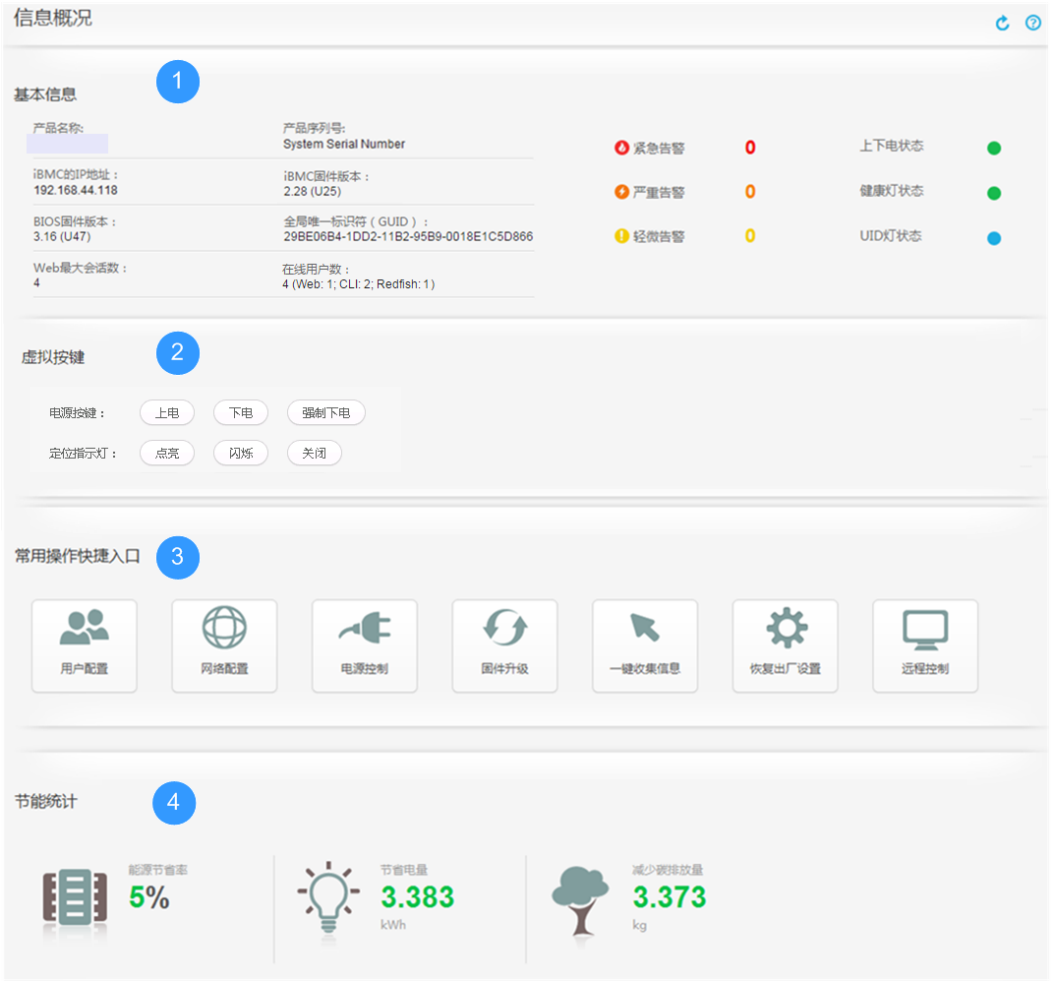
说明

RH8100 V3和8100 V5服务器的单系统模式下和双系统模式下的“信息概况”界面有区别，双系统模式多了VGA/USB/DVD切换和节点跳转功能。

图 3-3 8100 V5 服务器单系统模式下“信息概况”界面

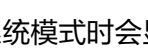
图 3-4 8100 V5 服务器双系统模式下“信息概况”界面

图 3-5 其他服务器的“信息概况”界面（产品型号以实际界面为准）



参数说明

表 3-2 “信息概况”

序号	区域	展示的信息
1	基本信息	提供服务器的基本信息，包括： ● 产品名称：服务器的型号。 ● 产品序列号：服务器的序列号。 ● iBMC的IP地址：iBMC系统的IP地址，通过此地址可以登录iBMC系统。 ● iBMC固件版本：iBMC系统的固件版本。 ● BIOS固件版本：BIOS的固件版本。 ● 全局唯一标识符（GUID）：全球唯一标识。 ● Web最大会话数：可同时登录本iBMC系统Web的最大用户数。 ● 在线用户数：在线用户的数量。 例如：“4 (Web: 1; CLI: 2; Redfish: 1)”表示此时在线用户有4人，通过Web界面登录iBMC系统的用户有1人，通过命令行登录iBMC系统的用户有2人，通过Redfish登录iBMC系统的用户有1人。 ● 上下电状态：绿色表示操作系统已经上电，灰色表示操作系统已经下电。 ● 健康灯状态：与服务器自身健康灯状态一致，通过本界面即可查看服务器的健康灯，不需要去机房查看。 ● 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。 ● 紧急告警：紧急告警总数目。（Critical，紧急告警可能会使单板下电，系统中断，需要马上采取相应的措施进行处理。） ● 严重告警：严重告警总数目。（Major，严重告警会对系统产生较大的影响，有可能中断部分系统的正常运行，导致业务中断。） ● 轻微告警：轻微告警总数目。（Minor，轻微告警不会对系统产生大的影响，需要尽快采取相应的措施，防止故障升级。）
2	虚拟按键	提供服务器的常用按钮，包括： ● 电源按键：包括上电、下电、强制下电。 ● 定位指示灯：包括点亮、关闭、闪烁（闪烁255秒）。 ● VGA/USB/DVD（RH8100 V3和8100 V5服务器特有按钮）：当服务器为双系统模式时会显示本功能，单击“  ”，此按钮变为“  ”，表示服务器的VGA接口、USB接口及DVD与本节点连接，与另一节点断开连接。

序号	区域	展示的信息
3	常用操作快捷入口	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“配置 > 本地用户”界面中的“本地用户”及“LDAP组”。 ● 网络配置：单击本入口可以直接跳转到“配置 > 网络配置”界面中的“网络”。 ● 电源控制：单击本入口可以直接跳转到“电源与能耗 > 电源控制”界面。 ● 固件升级：单击本入口可以直接跳转到“系统管理 > 固件升级”界面。 ● 一键收集信息：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考**3.11 一键收集信息说明**。 ● 恢复出厂设置：单击本入口可以弹出“恢复出厂设置”窗口，根据需要确定是否恢复出厂设置。 恢复出厂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 ● 远程控制：单击本入口可以进入“远程控制”界面。 ● 设置硬分区（RH8100 V3和8100 V5服务器特有功能）：单击本入口可以直接跳转到“配置 > 系统配置”界面中的“硬分区设置”。 ● 节点跳转（RH8100 V3和8100 V5服务器特有功能）：当服务器为双系统模式时会显示节点跳转，单击本入口可以弹出另一个节点的iBMC登录界面。

序号	区域	展示的信息
4	节能统计	显示服务器的节能信息，包括： ● “能源节省率”：显示本服务器相比于其他厂商同类设备节省能源的比例。 ● “节省电量”：显示本服务器节省的电量。 ● “减少碳排放量”：显示本服务器减少的碳排放量。 **说明** ● 节能统计计算方法： ● 节能率为综合指标(默认是5%) ● 节能能耗=实际能耗*(1/(1- 节能率) -1) ● 节约1度电(1KWh)=减排0.997千克二氧化碳 ● 节能率算法根据服务器节能菜单的开关情况计算得出。每个节能菜单对应一个节能效率值，不同菜单的权重不同。 单击“电源与能耗 > 功率”界面中的“重新统计”，节能统计信息会重新统计。

3.3.2 系统信息

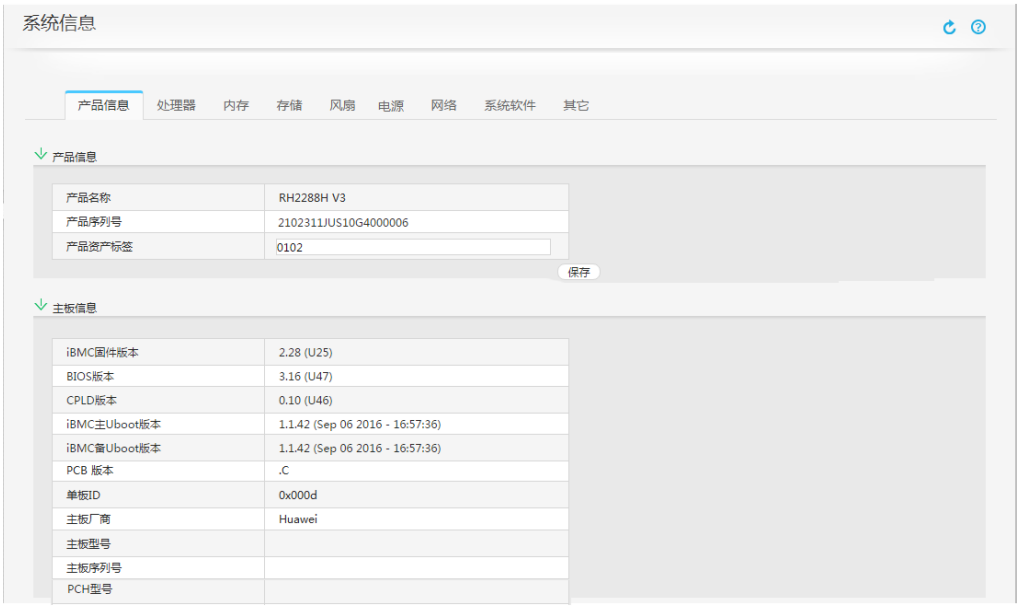
功能介绍

通过使用“系统信息”界面的功能，您可以查看服务器系统信息，并对RAID控制器进行配置和管理。

界面描述

在上方标题栏中，选择“信息”，在左侧导航树中选择“系统信息”，显示“系统信息”界面。

图 3-6 “系统信息”界面



参数说明

表 3-3 “产品信息”页签

参数	描述
产品信息	
产品名称	产品名称。
产品序列号	服务器的产品序列号。
产品资产标签	产品的资产标签。 取值范围：最多可包含48个字节，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。
主板信息	
iBMC固件版本	服务器的iBMC固件的版本号。
BIOS版本	BIOS的版本号。
CPLD版本	复杂可编程逻辑器件（CPLD，Complex Programmable Logical Device）的版本号。
iBMC主Uboot版本	用于嵌入式系统的开机引导程序的主镜像版本号。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。
PCB版本	印刷电路板（PCB，Printed Circuit Board）的版本号。
单板ID	单板的Board ID。
主板厂商	主板的生产厂家。
主板型号	主板的型号。
主板序列号	主板的序列号。
PCH型号	PCH芯片的型号。 **说明** 只有V5服务器显示PCH芯片型号。
部件编码	部件的编码。

表 3-4 “处理器”页签

参数	描述
处理器	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、主频以及部件编码。 ● 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。

表 3-5 “内存”页签

参数	描述
内存	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、位置、厂商、容量、主频、序列号、内存类型、最小电压、RANK数量、位宽、支持的技术以及部件编码。

表 3-6 “存储”页签

参数	描述
视图	通过导航树的方式展示了服务器当前存储设备的归属状态。 **说明** 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。
	单击RAID控制器，显示的信息包括： ● 控制器信息：名称、类型、驱动名称、驱动版本、固件版本、支持带外管理、健康状态、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使能状态、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信息：名称、状态、健康状况。 **说明** ● RAID控制器不支持带外管理且未安装运行iBMA 2.0的情况下，仅显示控制器名称、类型、固件版本以及是否支持带外管理。 ● 您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。 ● 请不要在RAID卡侧将其工作模式设置为JBOD，iBMC无法识别该模式下的RAID卡。详细信息请参考各服务器的RAID控制卡用户指南。

参数	描述
	单击逻辑盘，显示逻辑盘信息： 名称、状态、RAID级别、容量、条带大小、SSCD功能启用状态、默认读策略、当前读策略、默认写策略、当前写策略、默认IO策略、当前IO策略、物理盘缓存状态、访问策略、初始化类型、后台初始化启用状态、二级缓存启用状态、一致性校验运行状态、系统盘符、是否为启动盘。 **说明** ● RAID控制器不支持带外管理且未安装运行iBMA 2.0的情况下，无法显示RAID控制器下的逻辑盘信息。 ● 您可以从RAID控制卡用户指南的“技术规格”章节中查询该RAID卡是否支持iBMC带外管理。
	单击物理盘，显示物理盘信息： 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、最大速率、链接速率、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、剩余寿命、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“链接速率”显示为“NA”。
配置	提供RAID控制器的配置接口。
	控制器设置接口包括： ● 回拷 ● SMART错误时回拷 ● JBOD模式 单击“恢复默认配置”，可将RAID控制器的属性恢复为默认值。
	逻辑盘设置接口包括： ● 创建逻辑盘 ● 删除逻辑盘 ● 修改逻辑盘属性 **说明** RAID卡模式为JBOD时，不支持查询和配置逻辑盘信息。

参数	描述
	物理盘设置接口包括： ● 热备状态 ● 固件状态 ● 定位状态

说明

“存储”页签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。

表 3-7 “风扇”页签

参数	描述
风扇	显示服务器风扇信息。 ● 风扇满配个数和当前在位个数。 ● 风扇的名称、型号、转速、速率比以及部件编码。 **说明** 当服务器配置了不匹配的风扇或故障风扇时，“型号”会显示为“FAULT”。 RH8100 V3和8100 V5的双系统模式下，从系统中不显示风扇信息。

表 3-8 “电源”页签

参数	描述
电源	显示服务器电源信息。 ● 电源满配个数和当前在位个数。 ● 电源的槽位、厂商、类型、序列号、固件版本、额定功率、输入模式以及部件编码。 **说明** RH8100 V3和8100 V5的双系统模式下，从系统中不显示电源信息。

表 3-9 “网络”页签

参数	描述
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“网络”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，并参考文档安装iBMA 2.0。	
网卡	显示服务器安装的板载网卡或PCIe网卡的名称、厂商、型号、芯片型号、芯片厂商、PCB版本、单板ID、资源归属（归属CPU、PCH或PCIe Switch）、固件版本、驱动名称和驱动版本。 **说明** • 单击网卡前方的  ，可以查看成员端口的详细信息。展开网口列表，显示的网口信息包括网口名称、端口、状态、IPv4信息、IPv6信息、MAC地址、VLAN状态及网口类型。 • 如果网卡的固件版本不支持使用某个网口，该网口的网络属性显示为空。例如某网卡有Port1、Port2两个网口，如果该网卡的固件版本不支持使用Port2，则Port2的网络属性显示为空。
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、固件版本、驱动名称和驱动版本。 单击FC卡前方的  ，可以查看成员端口的详细信息。 iBMC V328及以上版本起，支持MCTP的FC卡支持显示以下信息： • 工作速率 • 工作模式 • 光模块开启状态 • 对端设备信用值 • 本端设备信用值、 • 发送速率 • 接收速率 • 速率协商阶段
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）。 **说明** 单击桥接网口前方的  ，可以查看成员端口的详细信息。
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）。 **说明** 单击汇聚网口前方的  ，可以查看成员端口的详细信息。

表 3-10 “系统软件”页签

参数	描述
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“系统软件”页签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，并参考文档安装iBMA 2.0。	
计算机名称	显示服务器操作系统中定义的计算机名称。
计算机描述	显示服务器操作系统的计算机描述信息。
操作系统版本	显示服务器操作系统的版本信息。
操作系统内核版本	当操作系统改为Linux系统时，显示其内核版本信息。
域名/工作组	显示服务器操作系统侧的域名或所属工作组。
iBMA服务	显示服务器操作系统中安装的iBMA版本信息。
iBMA运行状态	显示iBMA软件的运行状态。
iBMA驱动	显示iBMA的驱动版本信息。

表 3-11 “其它”页签

参数	描述
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、厂商、槽位、制造商ID、设备ID以及资源归属。 **说明** 单击PCIe卡前方的  ，可以查看PCIe卡的子卡信息。
PCIe转接卡	显示服务器PCIe转接卡的名称、描述、槽位、PCB版本以及单板ID。
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、厂商、类型、PCB版本、CPLD版本以及单板ID。

参数	描述
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、类型以及单板ID。 **说明** RH8100 V3和8100 V5不单独显示Riser卡信息，使用PCIe卡满配个数表示Riser卡的配置情况。 ● PCIe卡满配个数为10，表示未配置Riser卡。 ● PCIe卡满配个数为13，表示配置1张Riser卡。 ● PCIe卡满配个数为16，表示配置2张Riser卡。
SD卡	显示服务器SD卡信息。 ● SD卡满配个数和当前在位个数。 ● SD卡的厂商、序列号以及容量。 **说明** ● V5服务器不支持SD卡。 ● RH8100 V3服务器在单系统模式下，只显示主iBMC侧的SD卡；双系统模式下，显示所有分区的SD卡。
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。
RAID卡	显示服务器RAID控制器信息。 ● RAID控制器满配个数和当前在位个数。 ● RAID控制器的名称、位置、厂商、编号、类型、支持的RAID级别、PCB版本、CPLD版本、单板ID以及资源归属。
SD控制器	显示服务器SD控制器信息。 ● SD控制器满配个数和当前在位个数。 ● SD控制器的厂商以及固件版本。 **说明** V5服务器不支持SD控制器。
LCD固件版本	显示服务器LCD固件信息。 **说明** RH5885 V3不支持LCD，不显示LCD相关信息。RH5885H V3支持LCD，此处可查询LCD信息。
处理器板	显示服务器处理器板信息。 ● 处理器板满配个数和当前在位个数。 ● 处理器板的名称、厂商、槽位号、类型、PCB版本、CPLD版本、单板ID以及功率。 **说明** 仅8100 V5支持显示处理器板的功率。

参数	描述
内存板	显示服务器内存板信息。 ● 内存板满配个数和当前在位个数。 ● 内存板的名称、厂商、槽位号、类型、PCB版本以及单板ID。 **说明** RH5885 V3不支持内存板，不显示内存板相关信息。RH5885H V3支持内存板，此处可查询内存板信息。
IO板	显示服务器IO板信息。 ● IO板满配个数和当前在位个数。 ● IO板的名称、厂商、类型、PCB版本、CPLD版本、单板ID以及功率。 **说明** 仅8100 V5支持显示IO板的功率。
M.2转接卡	显示服务器M.2转接卡信息，包括M.2转接卡的名称、厂商、描述、PCB版本以及单板ID。 **说明** 当前仅RH2288 V3、RH2288H V3、1288H V5和2288H V5支持M.2转接卡。

查看系统信息

1. 在上方标题栏中选择“信息”。
2. 在左侧导航树中，选择“系统信息”。
   右侧显示“系统信息”界面。
3. 在“系统信息”界面中，查看产品信息及各部件的信息。

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iBMA2.0。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。

1. 在“系统信息”页面单击“存储”页签。
2. 在“视图”子页签左侧选中要查看的RAID控制器。
   右侧区域显示RAID控制器的基本属性，如图3-7所示。

图 3-7 查看控制器属性

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iBMA2.0。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。

1. 在“系统信息”页面单击“存储”页签。
2. 在“视图”子页签左侧选中要查看的RAID组。
   右侧区域显示RAID组的基本属性，如图3-8所示。

图 3-8 查看 RAID 组属性

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控制卡管理的硬盘且RAID控制卡需支持创建逻辑盘功能。
- RAID卡支持iBMC带外管理或已在OS侧安装并运行iBMA2.0。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。

1. 在“系统信息”页面单击“存储”页签。
2. 在“视图”子页签左侧选中要查看的物理磁盘（可以是RAID组中的成员盘，也可以是独立的磁盘）。

   右侧区域显示磁盘的基本属性，如图3-9和图3-10所示。

图 3-9 查看物理磁盘属性（成员盘）

图 3-10 查看物理磁盘属性（单独磁盘）

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。

1. 在“系统信息”页面单击“存储”页签。
2. 单击“配置”子页签。
   打开RAID配置界面。
3. 在RAID控制器列表的下拉菜单中选中要操作的RAID控制器。
4. 单击“控制器”后的 。
   展开控制器设置区域，界面中各配置项的含义如表3-12所示。

图 3-11 修改控制器属性

表 3-12 控制器配置项说明

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

5. 参考表3-12的说明进行配置，并单击“保存”。

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。

1. 在“系统信息”页面单击“存储”页签。
2. 单击“配置”子页签。
   打开RAID配置界面。

3. 在RAID控制器列表的下拉菜单中选中要操作的RAID控制器。
4. 单击“逻辑盘”后的 。
   打开逻辑盘配置菜单。
5. 单击“创建”前的单选按钮。
   打开创建逻辑盘区域，如图3-12所示，界面中各配置项的含义如表3-13所示。

图 3-12 创建逻辑盘

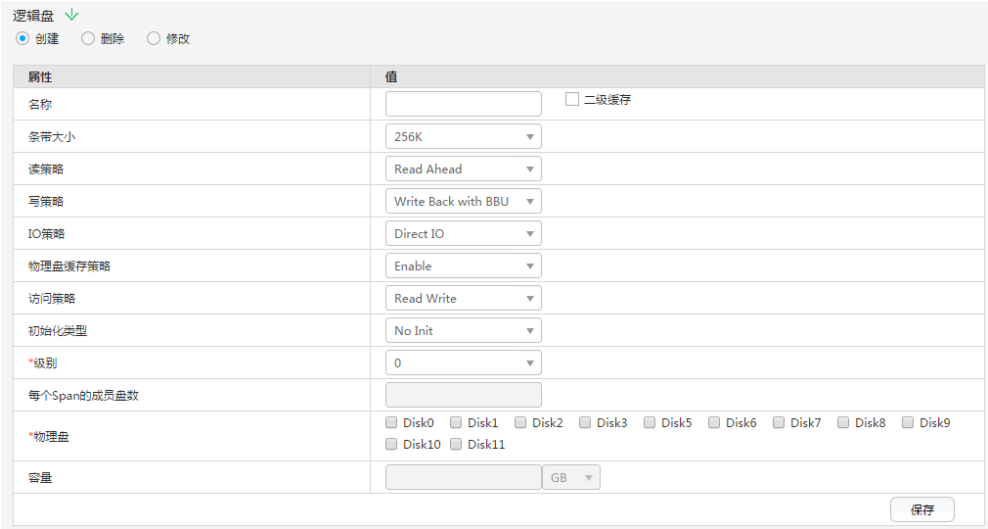


表 3-13 创建逻辑盘配置项说明

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。

配置项	说明
写策略	逻辑盘的数据写策略，包括： ● Write Through：当磁盘子系统接受到所有传输数据后，控制器将给主机返回数据传输完成信号。 ● Write Back with BBU：在控制器无BBU或BBU损坏的情况下，控制器将自动切换到Write Through模式。 ● Write Back：当控制器Cache收到所有的传输数据后，将给主机返回数据传输完成信号。
IO策略	应用于特殊的逻辑盘读取，不影响预读取Cache。包括： ● Cached IO：所有读和写均经过RAID控制器Cache处理。仅在配置CacheCade 1.1时需要设置为此参数值，其他场景不推荐。 ● Direct IO：在读、写场景中的定义不同： – 在读场景中，直接从物理盘读取数据。（如果“读策略”被设置为“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。）
磁盘缓存策略	物理盘Cache策略，包括： ● Enable：读写过程中数据经过物理盘写Cache，使写性能提升，但当系统意外掉电时，如果没有保护机制，数据会丢失。 ● Disable：读写过程中数据不经过物理盘写Cache，当系统意外掉电时，数据不会丢失。 ● Disk's default：保持默认的缓存策略。
访问策略	逻辑盘的访问策略，包括： ● Read Write：可读可写。 ● Read Only：只读访问。 ● Blocked：禁止访问。

配置项	说明
初始化操作	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”。
级别	逻辑盘的RAID级别。
每个Span的成员盘数	当RAID级别配置为10、50、60时，需要设置子组中物理盘个数。
物理盘	要加入逻辑盘的物理盘。
容量	逻辑盘的容量。

6. 参考表3-13的说明进行配置，并单击“保存”。

删除逻辑盘

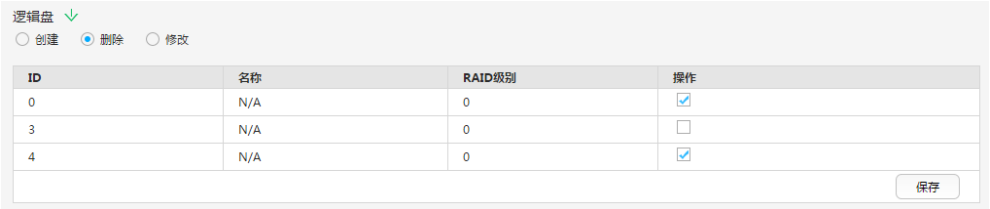
说明

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。
- 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。

1. 在“系统信息”页面单击“存储”页签。
2. 单击“配置”子页签。
   打开RAID配置界面。
3. 在RAID控制器列表的下拉菜单中选中要操作的RAID控制器。
4. 单击“逻辑盘”后的 。
   打开逻辑盘配置菜单。
5. 单击“删除”前的单选按钮。
   打开删除逻辑盘区域，如图3-13所示。

图 3-13 删除逻辑盘



6. 勾选待删除逻辑盘，并单击“保存”。

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控制卡管理的硬盘且RAID控制卡需支持创建逻辑盘功能。
- 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。

1. 在“系统信息”页面单击“存储”页签。
2. 单击“配置”子页签。
   打开RAID配置界面。
3. 在RAID控制器列表的下拉菜单中选中要操作的RAID控制器。
4. 单击“逻辑盘”后的 → 。
   打开逻辑盘配置菜单。
5. 单击“修改”前的单选按钮。
   打开修改逻辑盘属性区域，如图3-14所示，界面中各配置项的含义如表3-14所示。

图 3-14 修改逻辑盘

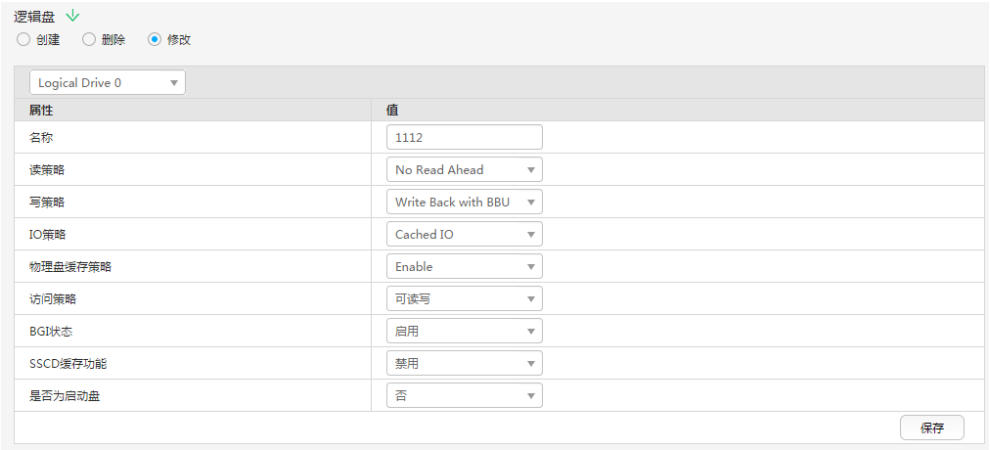


表 3-14 修改逻辑盘配置项说明

配置项	说明
名称	逻辑盘的名称。

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

配置项	说明
SSCD缓存功能	是否使用CacheCade逻辑盘做缓存。
是否为启动盘	是否设置该逻辑盘为系统启动盘。

6. 在逻辑盘列表的下拉框中选择要操作的逻辑盘。
7. 参考表3-14的说明进行配置，并单击“保存”。

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控制卡管理的硬盘且RAID控制卡需支持创建逻辑盘功能。
- 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。

1. 在“系统信息”页面单击“存储”页签。
2. 单击“配置”子页签。
   打开RAID配置界面。
3. 在RAID控制器列表的下拉菜单中选中要操作的RAID控制器。
4. 单击“物理盘”后的 。
   展开物理盘设置区域，如图3-15所示，界面中各配置项的含义如表3-15所示。

图 3-15 修改物理盘属性

表 3-15 物理盘配置项说明

配置项	说明
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

配置项	说明
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）
定位状态	物理盘是否已开启定位指示灯。

5. 在成员盘列表的下拉框中选择要操作的成员盘。
6. 参考表3-15的说明进行配置，并单击“保存”。

3.3.3 实时监控

功能介绍

通过“实时监控”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。
- 查看所有磁盘分区的占用率及磁盘容量信息。
- 查看进风口温度历史数据。

界面描述

在上方标题栏中，选择“信息”，在左侧导航树中选择“实时监控”，显示“实时监控”界面。

参数说明

表 3-16 “处理器”区域框

参数	描述
CPU占用率（%）	运行的程序占用CPU资源的比例。 **说明** • 服务器OS侧在安装iBMA 2.0并完全启动后，CPU占用率数据从iBMA 2.0获取，与OS侧统计的CPU占用率一致。 • 服务器OS侧未安装iBMA 2.0或iBMA 2.0未完全启动时，CPU占用率数据从Intel ME（Management Engine）获取，是由CPU内部模块计算出的所有核的每秒计算利用率。 • 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考文档安装iBMA 2.0。

表 3-17 “内存”区域框

参数	描述
内存占用率（%）	运行的程序占用内存的比例。 **说明** • 服务器OS侧在安装iBMA 2.0并完全启动后，内存占用率数据从iBMA 2.0获取，与OS侧统计的内存占用率一致。 • 服务器OS侧未安装iBMA 2.0或iBMA 2.0未完全启动时，内存占用率数据从Intel ME（Management Engine）获取，表示内存带宽占用率，与OS侧统计的内存容量占用率不同。 • 若服务器OS侧未安装iBMA 2.0，请获取最新的iBMA用户文档及软件包，并参考文档安装iBMA 2.0。

表 3-18 “磁盘分区”区域框

参数	描述
磁盘分区占用率（%）	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** 如果没有显示磁盘分区占用率，请在OS侧安装并运行iBMA 2.0。

表 3-19 “进风口温度”区域框

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）。

操作步骤

1. 在上方标题栏中选择“信息”，并在左侧导航树中选择“实时监控”。
   右侧显示“实时监控”界面。
2. 在“实时监控”界面中，单击 ，可以查看到每个监控项的更多相关信息。
   单击 可以收起信息。

   说明

   单击“进风口温度（℃）”区域框中的“清空历史记录”按钮可以清除统计的数据。

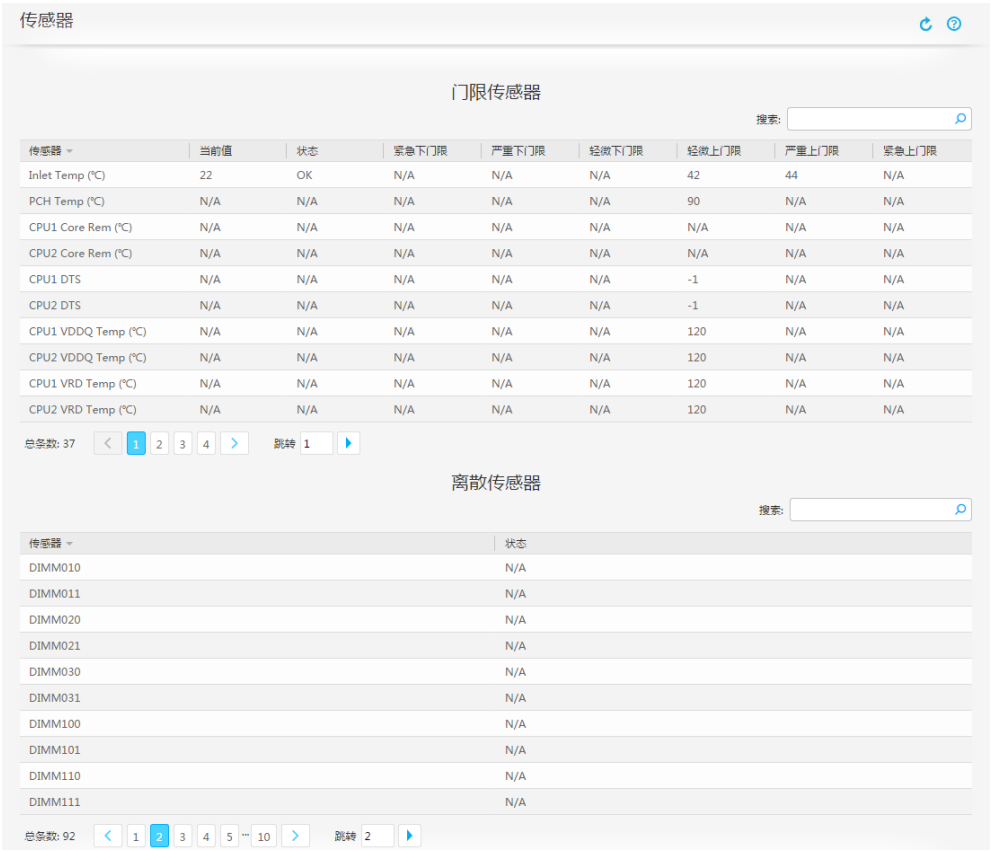
3.3.4 传感器

功能介绍

通过使用“传感器”界面的功能，您可以查看所有传感器的信息。

界面描述

在上方标题栏中，选择“信息”，在左侧导航树中选择“传感器”，显示“传感器”界面。



参数说明

表 3-20 “传感器”界面

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。
当前值	传感器当前监控到的指标信息。 如果显示为N/A，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。 ● N/A：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。 离散传感器扫描状态： ● N/A：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。 ● 0xXXXX：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，具体含义请参考具体产品的告警文档。
紧急下门限	使传感器产生紧急告警的下门限值。
严重下门限	使传感器产生严重告警的下门限值。
轻微下门限	使传感器产生轻微告警的下门限值。
轻微上门限	使传感器产生轻微告警的上门限值。
严重上门限	使传感器产生严重告警的上门限值。
紧急上门限	使传感器产生紧急告警的上门限值。

操作步骤

1. 在上方标题栏中选择“信息”。
2. 在左侧导航树中，选择“传感器”。
   右侧显示“传感器”界面。
3. 在“传感器”界面中，查看服务器的所有传感器，及其监控指标的当前值和门限值。

   说明

   在“搜索”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 告警与事件

3.4.1 当前告警

功能介绍

通过“当前告警”界面，您可以查看到设备当前未处理的告警。

界面描述

在上方标题栏中，选择“告警与事件”，在左侧导航树中选择“当前告警”，显示“当前告警”界面。

参数说明

表 3-21 当前告警列表

参数	描述
级别	告警的级别。 取值范围：“紧急”、“严重”和“轻微”。 ● ：紧急级别的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。 ● ：严重级别的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。 ● ：轻微级别的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。
主体类型	产生告警的部件类型。
事件描述	告警的描述信息。
产生时间	告警的产生时间。
事件码	告警在iBMC系统中的唯一标识。
处理建议	对告警的简要处理方法。 获取方法：单击。

操作步骤

1. 在上方标题栏中选择“告警与事件”，并在左侧导航树中，选择“系统事件”。右侧显示“系统事件”界面。
2. 在“当前告警”界面中，单击各主体类型左侧的  可以查看到详细的告警信息，单击  可以收起告警信息。

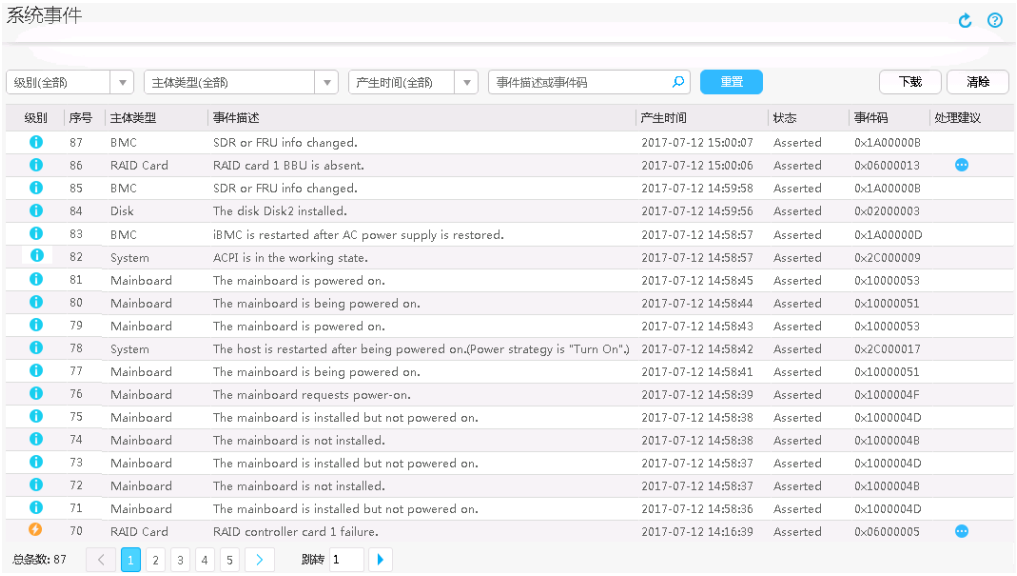
3.4.2 系统事件

功能介绍

通过使用“系统事件”界面的功能，您可以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

在上方标题栏中，选择“告警与事件”，在左侧导航树中选择“系统事件”，显示“系统事件”界面。



参数说明

表 3-22 系统事件列表

参数	描述
级别	系统事件的级别。 取值范围：“全部”、“紧急”、“严重”、“轻微”和“正常”。
序号	系统事件的排序。
主体类型	产生系统事件的部件类型。

参数	描述
事件描述	系统事件的描述信息。
产生时间	系统事件的产生时间。
状态	系统事件的状态。 取值范围： ● Asserted：表示系统事件已产生。 ● Deasserted：表示系统事件已恢复。
事件码	系统事件在iBMC系统中的唯一标识。
处理建议	对故障类事件的简要处理方法。 单击。

操作步骤

搜索系统事件

1. 在上方标题栏中选择“告警与事件”。
2. 在左侧导航树中，选择“系统事件”。
   右侧显示“系统事件”界面。
3. 根据表3-23提供的参数信息，设置搜索条件并进行搜索。

表 3-23 搜索条件说明

参数	描述
级别	系统事件的级别。 取值范围：“全部”、“紧急”、“严重”、“轻微”和“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：“今天”、“近7天”、“近30天”和“特定日期的范围”。 **说明** 当选择“特定日期的范围”时，需要在弹出的窗口中设置起止时间。
事件描述或事件码	系统事件的描述信息或事件码。 取值范围： ● 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”。 在文本框中输入后，单击或按“Enter”。

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。

1. 在“系统事件”界面中，单击“清除”。
   弹出操作确认对话框。
2. 单击“确定”。
   清除所有系统事件信息。

下载所有系统事件

在“系统事件”界面中，单击“下载”。下载文件成功保存到本地PC的默认路径。您可以在本地打开文件并查看事件日志。

3.4.3 告警设置

功能介绍

通过使用“告警设置”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。
- 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。
- 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。

界面描述

在上方标题栏中，选择“告警与事件”，在左侧导航树中选择“告警设置”，显示“告警设置”界面。

参数说明

表 3-24 “告警 Syslog 报文通知设置”区域框

参数	描述
Syslog功能	设置自动上报Syslog报文。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示Syslog功能正在启用。 • “  ”表示Syslog功能已经停用。
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：“紧急”、“严重”、“轻微”和“正常”。 **说明** 各告警发送级别的含义为： • 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。
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。

参数	描述
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。 设置方法：单击“浏览”选择客户端保存的服务器根证书文件。
服务器根证书信息	显示上传的服务器根证书信息，包括签发者、使用者、有效期、序列号。
本地证书	在建立数据连接时，iBMC向Syslog服务器发送报文时会携带本地证书信息，用于Syslog服务器对Syslog客户端（即iBMC系统）的验证。 设置方法：单击“浏览”选择客户端保存的本地证书文件。
证书密码	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。
本地证书信息	显示上传的本地证书信息，包括签发者、使用者、有效期、序列号。
设置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。
当前状态	当前通道的启用状态。
服务器地址	Syslog服务器地址信息。
端口	Syslog服务器的端口号。
日志类型	Syslog报文包含的日志类型。
操作	单击  ，显示以下内容。
当前状态	设置某个通道的启用状态。 单击“  ”或“  ”并单击“保存”，可切换状态。 ● “  ”表示通道正在启用。 ● “  ”表示通道已经停用。
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“配置 > 网络配置”页面配置正确的DNS信息。
端口	Syslog服务器的端口号。 取值范围：1～65535

参数	描述
日志类型	需要使用Syslog报文上报的日志类型。 取值范围：“全选”、“操作日志”、“安全日志”、“事件日志”。
测试	测试设置的Syslog通道是否可用。 设置方法：单击“测试”，显示“操作成功”表示该通道可用。

表 3-25 “告警 Trap 报文通知设置”区域框

参数	描述
Trap功能	设置自动上报Trap报文。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示Trap功能正在启用。 • “  ”表示Trap功能已经停用。
Trap版本	以Trap方式上报事件需遵循的SNMP Trap协议版本。 取值范围： • “SNMPv1”：SNMP Trap协议的V1版本是简单网络管理协议的第一个正式版本，在RFC（Request For Comments）1157中定义。 • “SNMPv2c”：V2C版本是针对V2的改进版。SNMP Trap协议的V2C版本是基于共同体（Community-Based）的管理架构，在RFC1901中定义的一个实验性协议。 • “SNMPv3”：SNMP协议的V3版本由RFC 3411-RFC 3418定义，主要在安全性和远程配置方面进行强化。 **说明** • “SNMPv1”和“SNMPv2c”版本由于自身机制而存在安全隐患，请尽量避免使用。建议使用“SNMPv3”版本的SNMP Trap。 • “SNMPv3”的鉴权加密算法可在**3.7.7 系统配置**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，V3服务器使用的是**root**用户，V5服务器使用的是**Administrator**用户。

参数	描述
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：V3服务器默认为“事件码模式”，V5服务器默认为“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	SNMP使用的共同体名称。团体名是用作认证Trap方式的口令。“版本”设置为“SNMPv1”或“SNMPv2c”时才能设置“团体名”。 不开启密码检查时的取值原则：1～18位的字符串，由数字、英文字母和除空格外的特殊字符组成。 开启密码检查时的取值原则： ● 长度为8～18位的字符。 ● 至少包含以下字符中的两种： – 大写字母：A～Z – 小写字母：a～z – 数字：0～9 – 至少包含以下特殊字符： `~!@#$%^&*()-_=+\\|[{}];:'",<.>/? ● 新旧团体名至少在2个字符位上不同。 ● 不能包含空格。 默认取值：“TrapAdmin12#$”
确认团体名	SNMP使用的共同体名称。此处输入的内容需要与“团体名”中相同。

参数	描述
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：“紧急”、“严重”、“轻微”和“正常”。 **说明** 各告警发送级别的含义为： • 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。
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。
操作	单击  ，显示以下内容。
当前状态	设置启用某个通道。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示通道正在启用。 • “  ”表示通道已经停用。
Trap服务器IP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和IPv6。
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”。
报文分隔符格式选择	选择Trap格式中每个关键字段之间的分隔符，例如“;”。
报文显示内容选择	选择需要上报的关键字。
在发送报文中显示关键字	显示Trap格式中每个关键字的名称。 **说明** 本行右侧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。
测试	测试设置的Trap通道是否可用。 单击“测试”，显示“操作成功”表示该通道可用。

表 3-26 “告警邮件通知设置”区域框

参数	描述
SMTP功能	设置启用SMTP服务。 单击“  ”或“  ”并单击“保存”，可切换状态。 ● “  ”表示SMTP功能正在启用。 ● “  ”表示SMTP功能已经停用。
SMTP服务器地址	SMTP服务器的IPv4或IPv6地址。 **说明** 系统不支持域名解析，因此在“SMTP服务器地址”文本框中，您只能输入SMTP服务器的IP地址，而不能输入SMTP服务器的域名。
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。
设置邮件信息	
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。 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。 取值原则： ● 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。 **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。 取值原则：由英文字母、数字、“@”和其他特殊字符组成。格式必须为“*xx@xxx.xx*”。

参数	描述
邮件主题	电子邮件的标题。 取值范围：0～255位的字符串。 取值原则：由数字、英文字母和特殊字符组成。
邮件附带	在电子邮件标题中可附带的关键信息，可以是“主机名”、“单板序列号”和“产品资产标签”。
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：“紧急”、“严重”、“轻微”和“正常”。 **说明** 各告警发送级别的含义为： • 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。
接收告警的邮件地址	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。 取值原则：由英文字母、数字、“@”和其他特殊字符组成。格式必须为“*xx@xxx.xx*”。
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。 取值原则：由数字、英文字母和特殊字符组成。
测试	验证目标邮箱地址是否可达。
启用	设置启用某个接收地址。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示该接收地址正在启用。 • “  ”表示该接收地址已经停用。

操作步骤

设置告警Syslog报文通知参数

1. 在上方标题栏中选择“告警与事件”，并在左侧导航树中，选择“告警设置”。
   右侧显示“告警设置”界面。
2. 根据表3-24提供的参数信息，设置告警Syslog报文通知参数。
3. 单击“保存”。
   显示“操作成功”表示该功能设置成功。

设置告警Trap报文通知参数

1. 根据表3-25提供的参数信息，设置告警Trap报文通知功能。
2. 单击“保存”。
   显示“操作成功”表示该功能设置成功。

设置告警邮件通知参数

1. 根据表3-26提供的参数信息，设置告警邮件通知功能。
2. 单击“保存”。
   显示“操作成功”表示该功能设置成功。

3.5 诊断

3.5.1 录像回放

功能介绍

通过使用“录像回放”界面的功能，您可以进行如下操作：

- 播放本地PC上存放的服务器实时桌面的视频文件。
- 播放服务器自动录制的视频文件。
- 对某时刻的视频文件进行截图。

说明

- 播放的视频文件格式为“*.rep”。
- 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。

录像回放控制窗口中的按钮及其作用如表3-27所示。

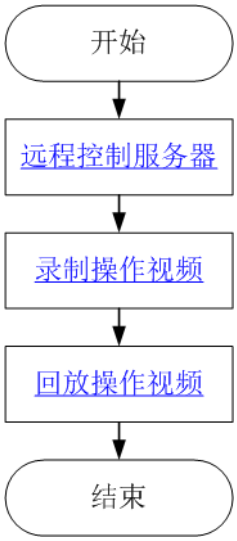
表 3-27 按钮说明

按钮	说明
	“播放”按钮。表示开始播放视频文件。
	“暂停”按钮。表示暂停视频文件的播放。
	“快进”按钮。表示加速播放视频文件。播放速度可以选择1倍、2倍或4倍。
	“慢进”按钮。表示减速播放视频文件。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** 在全屏或满屏播放视频文件时，单击右键可以弹出快捷菜单。

按钮	说明
	“打开”按钮。表示导入“*.rep”格式的视频文件。 本地播放录像时才能使用本功能。
	“截屏”按钮。表示截取视频文件中的某一帧画面。
	播放进度条。表示视频文件的播放进度。
	“循环”按钮。表示循环播放视频文件。 本地播放录像时才能使用本功能。

您可以将iBMC系统提供的录像和录像回放功能配合使用，进行服务器维护和设备故障定位。任务操作流程如图3-16所示。

图 3-16 录像功能使用流程



界面描述

在上方标题栏中，选择“诊断”，在左侧导航树中选择“录像回放”，显示“录像回放”界面。

操作步骤

播放本地视频文件

1. 在“录像回放”页面中，单击“本地录像回放控制台”右侧的“打开”按钮，进入“Video Player”。

   说明

   如果打开“Video Player”窗口前弹出安全警告，请单击“继续”，并继续进行操作。

2. 在“Video Player”窗口中，单击，选择本地PC上存放的视频文件。
3. 单击“打开”。
   返回“Video Player”窗口并开始播放该视频文件。
   - 单击，以正常速度的1倍、2倍或4倍快速播放视频文件。
   - 单击，以正常速度的1倍、0.5倍或0.25倍缓慢播放视频文件。
   - 向左或向右拖动，控制视频文件的播放进度。
   - 单击。
     系统循环播放该视频文件。
   - 单击。
     “Video Player”窗口最大化显示在屏幕上。

开启或关闭录像功能

说明

默认为开启状态。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。

执行以下步骤开启录像功能：

1. 在“录像回放”界面中，将“录像使能”右侧的按钮设置为“ON”
   界面弹出窗口提示：
   是否确定执行该操作?

2. 单击“确定”。

开启录像功能后，在下述情况中，服务器将自动录制视频文件并保存到/tmp下：

- 关机、重启时，会自动录制视频文件。
- 系统产生“CPU CAT ERROR”故障时，会自动录制视频文件。

服务器恢复正常后，可以在“录像回放”界面中播放或下载上述文件，分析故障原因。

说明

将“录像使能”右侧的按钮设置为“ OFF ”时，可关闭录像功能。

播放或下载录像

- 在“录像回放”界面中，单击“播放”可播放CPU出错录像、关机录像或重启录像。
- 在“录像回放”界面中，单击“播放”可下载CPU出错录像、关机录像或重启录像到本地。

如果其他人正在播放在线录像，需要单击“删除当前连接”右侧的“删除”，断开其他人的连接，自己才能播放在线录像。

截取视频图像

1. 在视频播放过程中，单击  。
   弹出“保存”窗口。
2. 选择视频图像在本地PC上的存放路径，单击“保存”。
   视频图像成功保存到指定的路径。图像格式为“*.jpg”。

3.5.2 屏幕截图

功能介绍

通过使用屏幕截图功能，您可以：

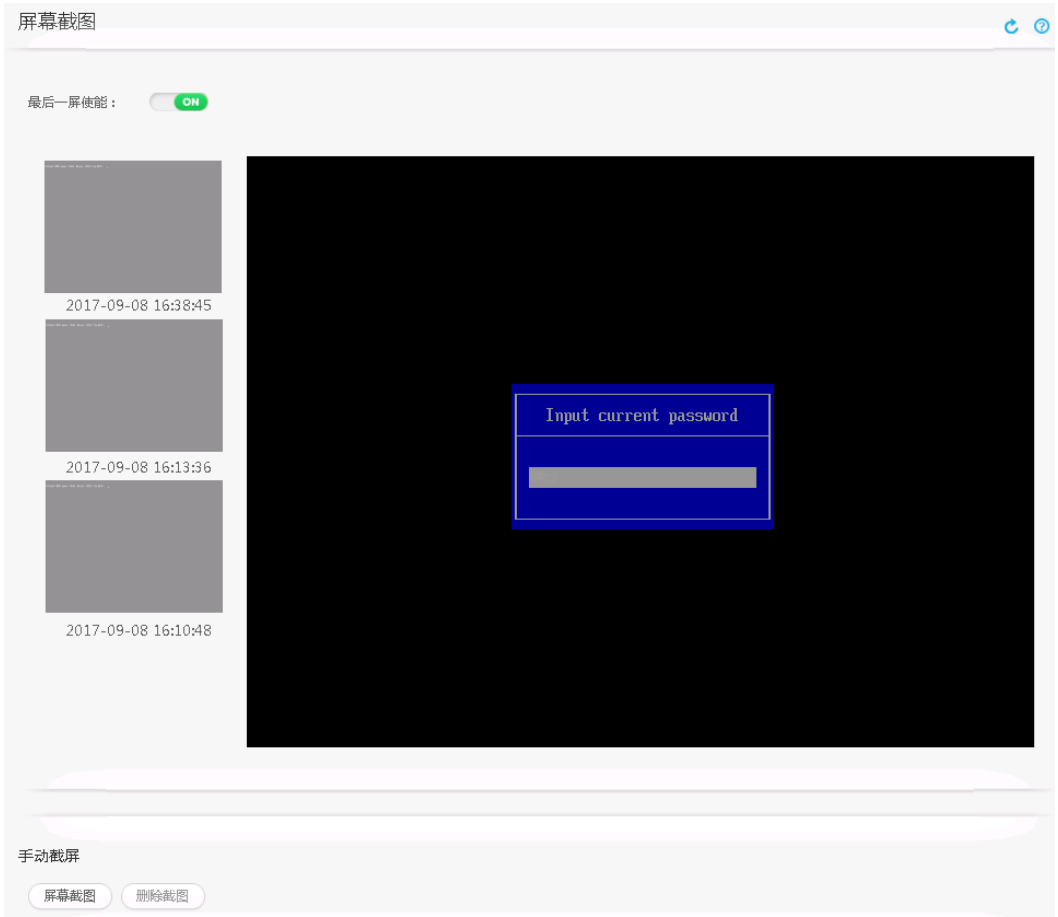
- 在服务器重启或下电时，将自动保存屏幕最后的显示信息。
- 随时对实时桌面进行屏幕截图。

说明

默认为开启状态。开启最后一屏功能后，自动截屏功能有可能录制到业务侧的敏感信息。

界面描述

在上方标题栏中，选择“诊断”，在左侧导航树中选择“屏幕截图”，显示“屏幕截图”界面。



操作步骤

开启或关闭屏幕截图功能

1. 将“最后一屏使能”右侧的按钮设置为“ON”，开启屏幕截图功能。将按钮设置为“OFF”，关闭屏幕截图功能。

   单击按钮“ON”或“OFF”，界面弹出窗口提示以下信息：

   是否确定执行该操作?
2. 单击“确定”。

   操作完成后“屏幕截图”界面将显示“操作成功”提示信息。

查看最后一屏截图

1. 在上方标题栏中选择“诊断”。
2. 在左侧导航树中，选择“屏幕截图”。

   右侧显示“屏幕截图”界面。
3. 查看截图。
   - 单击缩略图可以查看大图，默认显示最近一次服务器重启或者下电前的系统画面。
   - 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“屏幕截图”。

   显示iBMC系统截取的服务器实时桌面的图片。在图片的左上方显示图片截取时间。

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

删除前，请确保“手动截屏”区域框中存在屏幕图。

1. 单击“删除截图”。

   弹出确认对话框。
2. 在弹出的确认对话框中，单击“确定”。

3.5.3 黑匣子

功能介绍

通过使用“黑匣子”界面的功能，您可以启用或关闭黑匣子功能，并在开启功能时将黑匣子存储器中的数据下载到本地。

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V5服务器未安装黑匣子驱动，则可能在OS侧出现未知设备。

界面描述

在上方标题栏中，选择“诊断”，在左侧导航树中选择“黑匣子”，显示“黑匣子”界面。

参数说明

表 3-28 “黑匣子”界面

参数	描述
黑匣子功能	启用黑匣子功能。默认为关闭状态。 设置方法：单击“  ”，此按钮变为“  ”，表示黑匣子功能已经启用。
文件名	黑匣子监控到的服务器数据文件的名称。
大小	黑匣子数据文件的大小。

操作步骤

启用黑匣子功能

当启用黑匣子功能后，需重新启动服务器才能使其工作。

1. 在上方标题栏中选择“诊断”。
2. 在左侧导航树中，选择“黑匣子”。
   右侧显示“黑匣子”界面。
3. 单击“  ”，此按钮变为“  ”，表示黑匣子功能已经启用。
4. 重启服务器。

说明

启用或禁用黑匣子功能都需要重启服务器方可生效。

关闭黑匣子功能

关闭黑匣子功能前，请确保已经启用该功能。

1. 单击“  ”，此按钮变为“  ”，表示黑匣子功能已经关闭。
2. 重启服务器。

下载黑匣子数据文件

说明

请确认黑匣子功能已启用。

1. 单击IE的“工具 > Internet选项”。
   弹出“Internet选项”窗口。
2. 将“安全 > Internet > 自定义级别 > 下载 > 文件下载的自动提示”设置为“启用”。
3. 登录iBMC WebUI后，在导航栏中选择“诊断”，并在左侧导航树中选择“黑匣子”。
4. 单击“下载”。
   弹出“保存”提示信息。

5. 选择黑匣子数据文件在本地PC上的保存路径。
6. 单击“保存”。

   黑匣子数据文件成功保存到指定的路径。iBMC仅将黑匣子数据文件从服务器拷贝到iBMC并下载到本地。

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。

3.5.4 串口数据

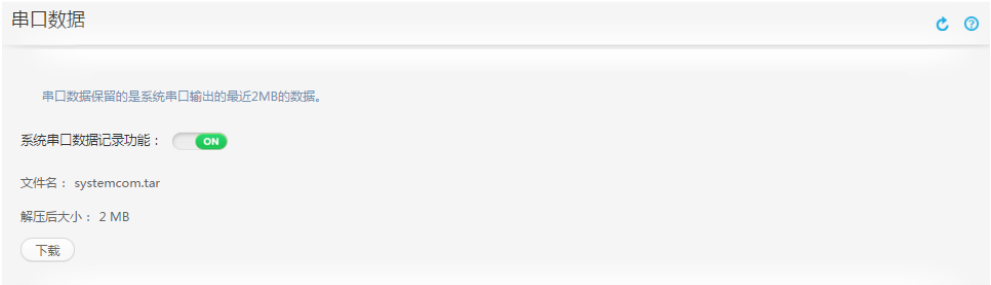
功能介绍

通过使用“串口数据”界面的功能，您可以启用或关闭串口数据下载记录功能，开启时您可以下载系统串口最近2MB的数据。

默认为开启状态。

界面描述

在上方标题栏中，选择“诊断”，在左侧导航树中选择“串口数据”，显示“串口数据”界面。



操作步骤

1. 单击IE的“工具 > Internet选项”。

   弹出“Internet选项”窗口。
2. 将“安全 > Internet > 自定义级别 > 下载 > 文件下载的自动提示”设置为“启用”。
3. 在iBMC上方标题栏中选择“诊断”。
4. 在左侧导航树中，选择“串口数据”。

   右侧显示“串口数据”界面。
5. 单击 

，此按钮变为 

，表示开启了串口数据下载记录功能。
6. 单击“下载”。

   弹出“保存”窗口。
7. 选择下载文件在本地PC上的保存路径。
8. 单击“保存”。

下载文件成功保存到指定的路径。您可以在本地打开文件并查看串口最近2MB的数据。

3.5.5 故障诊断日志

功能介绍

通过使用“故障诊断日志”界面的功能，您可以下载处理器上报的故障记录。

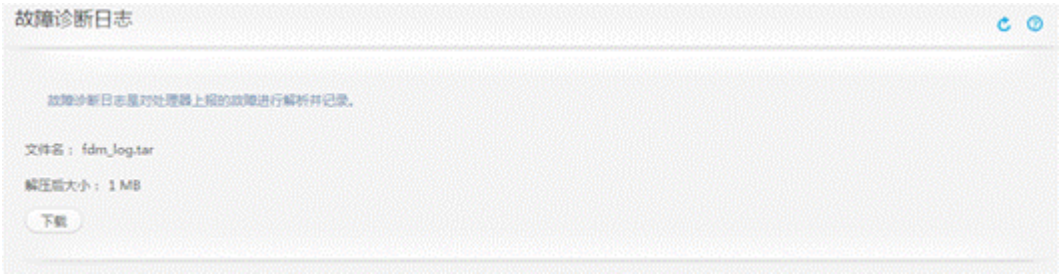
默认为开启状态。可以将BIOS里面的FDM参数设置为开启或者关闭来开启或关闭故障诊断日志功能。

不同平台的BIOS中，FDM参数所在路径不同：

- Romley平台的BIOS：Advanced > RAS Configuration > FDM
- Brickland平台的BIOS：Advanced > Runtime Error Logging > FDM
- Grantley平台的BIOS：Advanced > System Event Log > FDM
- Purley平台的BIOS：Advanced > System Event Log > FDM

界面描述

在上方标题栏中，选择“诊断”，在左侧导航树中选择“故障诊断日志”，显示“故障诊断日志”界面。



操作步骤

步骤1 单击IE的“工具 > Internet选项”。

弹出“Internet选项”窗口。

步骤2 将“安全 > Internet > 自定义级别 > 下载 > 文件下载的自动提示”设置为“启用”。

步骤3 在iBMC上方标题栏中选择“诊断”。

步骤4 在左侧导航树中，选择“故障诊断日志”。

右侧显示“故障诊断日志”界面。

步骤5 单击“下载”。

弹出“保存”窗口。

步骤6 选择下载文件在本地PC上的保存路径。

步骤7 单击“保存”。

下载文件成功保存到指定的路径。您可以在本地打开文件并查看处理器上报的故障记录。

----结束

3.5.6 内存热插拔（RH8100 V3 服务器特有功能）

功能介绍

通过使用“内存热插拔”界面的功能，您可以通过该页面操作内存热插拔并进行迁移过程状态监控。

说明

当配置Broadwell处理器时，RH8100 V3服务器不支持内存板热插拔，WebUI中无此页面。

界面描述

在上方标题栏中，选择“诊断”，在左侧导航树中选择“内存热插拔”，显示“内存热插拔”界面。

操作步骤

1. 在iBMC上方标题栏中选择“诊断”。
2. 在左侧导航树中，选择“内存热插拔”。
   右侧显示“内存热插拔”界面。
3. 单击绿色或橙色标签的内存板。
4. 单击“迁移数据”。
   开始内存迁移，进度条会显示迁移进度。

3.6 电源与能耗

3.6.1 电源控制

功能介绍

通过使用“电源控制”界面的功能，您可以：

- 对服务器操作系统进行上电、下电或重启，以及触发操作系统产生一个不可屏蔽中断（NMI，Non-maskable Interrupt）操作。
- 设置服务器操作系统的开机策略。

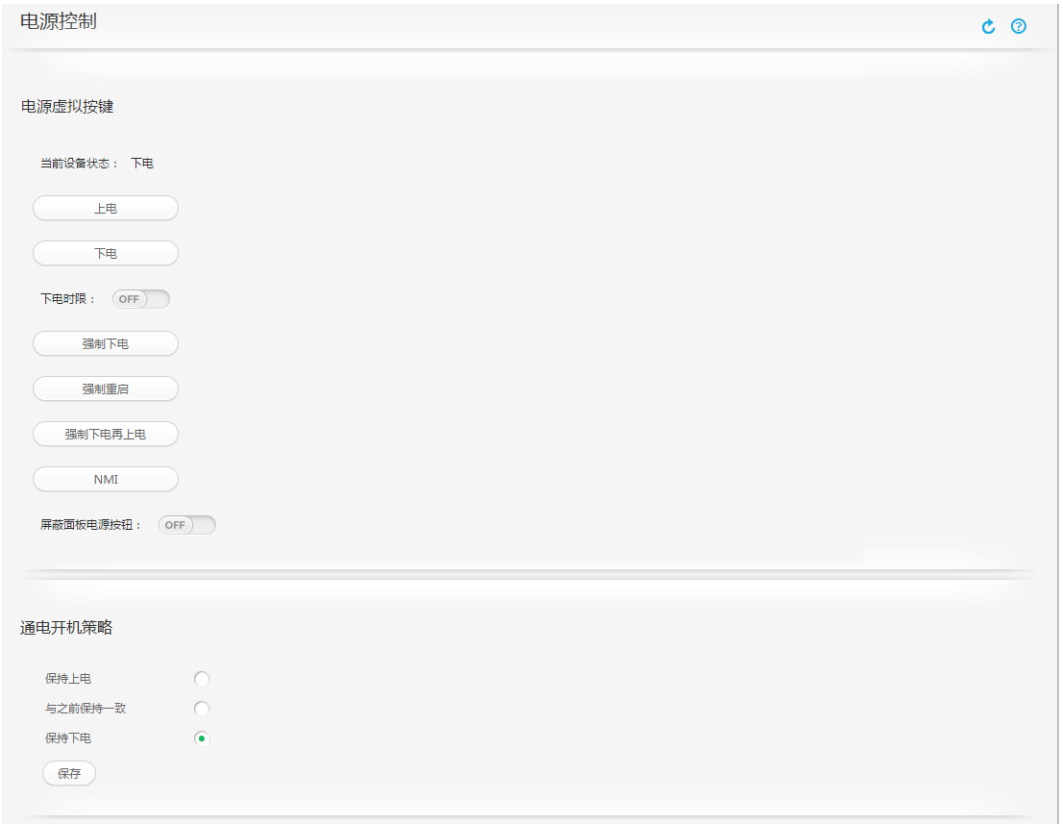
NMI是一种不能被标准屏蔽中断技术忽略的特殊中断。不可屏蔽中断特别用于不可恢复硬件错误的信号提示。通过使用特殊方法，某些不可屏蔽中断也能够被屏蔽。

须知

请在强制下电、下电、强制重启、强制下电再上电或NMI操作前确认无业务风险。

界面描述

在上方标题栏中，选择“电源与能耗”，在左侧导航树中选择“电源控制”，显示“电源控制”界面。



参数说明

表 3-29 “电源控制”区域框

参数	描述
当前设备状态	显示服务器操作系统是否上电。
上电	对服务器操作系统执行上电操作。
下电	对服务器操作系统执行下电操作。

参数	描述
下电时限	对服务器操作系统执行下电操作后，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，如果操作系统无法在指定时间内下电，iBMC会对操作系统执行强制下电。 ● 关闭“下电时限”时，iBMC不会干涉操作系统的下电过程。 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。 ● 单击“ON”或“OFF”并单击“保存”，可切换状态。单击“”，在文本框中修改下电时限，完成修改后单击“保存”。 ● 设置为OFF时，表示关闭下电时限功能。 **说明** 当前仅TaiShan 200服务器2280和5280型号支持BBU备电模块。
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。 对服务器操作系统执行强制下电，服务器操作系统将在6秒内完成下电操作。
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。 对服务器操作系统执行强制重启操作，操作系统会立即重新启动。 **说明** ● 在操作系统下电状态下，“强制重启”操作无效。 ● 该操作会影响正在执行的下电操作。
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。 对服务器操作系统执行强制下电，等待约6秒后，服务器操作系统直接上电。
NMI	触发服务器产生一个不可屏蔽中断。 该功能主要在无法再使用操作系统的情况下使用。在服务器操作系统正常运行期间，不应使用该功能。 **须知** NMI仅用于内部调测，使用时需要操作系统中有对应的NMI中断处理程序，否则可能引起系统崩溃。请谨慎使用。

参数	描述
屏蔽面板电源按钮	开启本功能后服务器面板上的电源按钮将失效。 单击“ OFF ”或“ ON ”并单击“保存”，可切换状态。 默认状态： OFF ● “ ON ”表示此功能已开启，此时电源按钮已失效。 ● “ OFF ”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。

表 3-30 “通电开机策略”区域框

参数	描述
保持上电	服务器的电源模块通电后操作系统自动开机。
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，则通电后操作系统自动开机。 ● 如果断电前服务器操作系统是关机状态，则通电后操作系统不上电。
保持下电	服务器的电源模块通电后操作系统不上电。

操作步骤

表 3-31 电源控制操作步骤

操作	操作步骤
为服务器操作系统上电	1. 在“电源控制”页面，单击“电源虚拟按键”区域框中的“上电”按钮。 弹出对话框提示以下信息： 是否确定执行该操作? 2. 单击“确定”。 服务器操作系统开始上电。服务器操作系统上电的时间根据服务器的配置不同。操作完成后“电源控制”界面将显示“操作成功”提示信息。 服务器操作系统成功上电后，“当前设备状态”显示为“上电”。

操作	操作步骤
将服务器操作系统正常下电	1. 在“电源控制”页面，单击“电源虚拟按键”区域框中的“下电”按钮。 弹出对话框提示以下信息： 是否确定执行该操作? 2. 单击“确定”。 服务器操作系统开始正常下电。操作完成后“电源控制”界面将显示“操作成功”提示信息。 服务器操作系统成功正常下电后，“当前设备状态”显示为“下电”。
将服务器操作系统强制下电	1. 在“电源控制”页面，单击“电源虚拟按键”区域框中的“强制下电”按钮。 弹出对话框提示以下信息： 是否确定执行该操作? 2. 单击“确定”。 服务器操作系统开始强制下电。操作完成后“电源控制”界面将显示“操作成功”提示信息。 服务器操作系统成功强制下电后，“当前设备状态”显示为“下电”。
强制重启服务器操作系统	1. 在“电源控制”页面，单击“电源虚拟按键”区域框中的“强制重启”按钮。 弹出对话框提示以下信息： 是否确定执行该操作? 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“电源控制”界面将显示“操作成功”提示信息。
强制下电再上电	1. 在“电源控制”页面，单击“电源虚拟按键”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： 是否确定执行该操作? 2. 单击“确定”。 服务器操作系统开始强制下电再上电。服务器操作系统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“电源控制”界面将显示“操作成功”提示信息。 服务器操作系统成功强制下电再上电后，“当前设备状态”由“上电”变为“下电”，最后显示为“上电”。

操作	操作步骤
触发NMI	**须知** 该功能主要在无法再使用操作系统的情况下使用。在服务器正常运行期间，不应使用此功能，否则可能造成系统崩溃。 1. 在“电源控制”页面，单击“电源虚拟按键”区域框中的“NMI”按钮。 弹出对话框提示以下信息： 向操作系统发送不可屏蔽中断可能导致数据丢失和数据损坏！你确定执行这个操作吗? 2. 单击“确定”。 操作系统产生一个不可屏蔽中断。操作完成后“电源控制”界面将显示“操作成功”提示信息。
设置通电开机策略	1. 在“电源控制”页面，选中“通电开机策略”区域框中的“保持上电”。 弹出对话框提示以下信息： 是否确定执行该操作? 根据表3-30提供的参数信息，设置服务器的开关机策略。 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“电源控制”页面，请将“下电时限”右侧的按钮设置为“ ON ”。 2. 单击 输入超时时长。 取值范围：单击 后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。 默认取值为“600”。 3. 单击“保存”。 显示“操作成功”表示成功设置下电时限。
查看下电时限	在“电源控制”页面的“电源虚拟按键”区域框中，查看下电时限。“超时时长（秒）”文本框中的数值为设置的时间。

3.6.2 功率

功能介绍

通过使用“功率”界面的功能，您可以:

- 查看服务器的功率信息。
- 设置是否开启功率封顶功能，限制服务器的封顶功率，以及超过封顶功率后的进一步动作。
- 查看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。

  系统的采样时间间隔为10分钟。

须知

- 在设置封顶功率时，请谨慎操作。如果封顶功率过低，系统性能和服务器上的业务运营会受到影响。
- 请谨慎选择封顶失败后的“关机”动作，避免对业务造成影响。（RH5885 V3、RH5885H V3、RH8100 V3和8100 V5无此功能。）
- RH8100 V3 和8100 V5的双系统模式下，从系统-B侧的iBMC没有该功能页面。

界面描述

在上方标题栏中，选择“电源与功耗”，在左侧导航树中选择“功率”，显示“功率”界面。

图 3-17 “功率”界面

参数说明

表 3-32 “功率”页面

参数	描述
功率封顶使能状态	开启功率封顶功能的开关。 **说明** 使用本功能前，需要进入BIOS菜单，完成以下操作： • 将“EIST Support”（部分产品此参数显示为“EIST”）设置为“Enabled”。 • V2服务器Romley平台下，将“ACPI 3.0 T-States”设置为“Enabled”。 • V3服务器Brickland平台下，将“ACPI T-States”（V3服务器Grantley平台不支持此参数）设置为“Enabled”。 • V5服务器Purley平台下，将“Software Controlled T-States”设置为“Enabled”。“T-State Throttle Level”建议保持默认值，默认值为“Disabled”。 双系统工作模式下，只有功率统计，没有功率封顶功能，这里的功率统计是整个服务器的功率，和单系统工作模式一样。 单击“OFF”或“ON”并单击“保存”，可切换状态。 • “ON”表示功率封顶功能正在启用。 • “OFF”表示功率封顶功能已经停用。
功率封顶值（W）	限制服务器可运行的最大功率。 双系统工作模式下，没有此功能。 取值范围：单击后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系统给出的下限值。
功率封顶失效自动关机 （RH5885 V3、RH5885H V3、RH8100 V3、8100 V5无此功能）	当服务器功率封顶失败时，服务器将在15秒后自动关机。 单击“OFF”或“ON”并单击“保存”，可切换状态。 • “ON”表示系统自动关机功能正在启用。 • “OFF”表示系统自动关机功能已经停用。

表 3-33 “当前状态”页面

参数	描述
选择使用的功率单位	选择“功率”页面中功率的单位。 设置方法：单击“W”或“BTU/h”单选按钮。 **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。
当前功率读数	服务器当前的功率。
系统平均功率	从服务器首次上电或重新统计起始时间，系统功率的平均值。
系统累计耗电量	从服务器首次上电或重新统计起始时间，系统耗电量的累计值。
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，系统出现过的最大功率值。
峰值产生时间	从服务器首次上电或重新统计起始时间到当前时刻，系统出现过最大功率值的时间。
CPU当前功耗	服务器当前在位的CPU的功率。
Memory当前功耗	服务器当前在位的内存的功率。

表 3-34 “历史功率”区域框

参数	描述
历史功率曲线	
平均功率	服务器最近一周或一天或从统计时间起到当前每十分钟内的平均功率。
峰值功率	服务器最近一周或一天或从统计时间起到当前每十分钟内的最大功率。

操作步骤

查看系统功率

1. 在上方标题栏中选择“电源与能耗”。
2. 在左侧导航树中，选择“功率”。
   右侧显示“功率”界面。
3. 在“当前状态”区域框中，查看服务器的功率信息。

重新统计功率

1. 单击“重新统计”。
   弹出对话框提示以下信息：

是否确定执行该操作?

2. 单击“确定”。

清除所有统计信息，并从当前时刻开始重新统计。“功率”界面显示重新统计的功率信息。

设置功率封顶

1. 单击“功率封顶使能状态”右侧的“  ”。

弹出对话框提示以下信息:

是否确定执行该操作?

2. 单击“确定”，显示“操作成功”，并且“  ”变为“  ”，表示功率封顶功能已经启用。

3. 单击  ，在“功率封顶值（W）”文本框中，输入需要设置的功率封顶值。

输入的值需要满足文本框右侧括号中给定的功率范围，例如，括号内容为（105--750），输入的功率封顶值范围是105～750。

4. 单击“保存”。

显示“操作成功”表示成功开启并设置功率封顶值。

禁用功率封顶功能

1. 单击“功率封顶使能状态”右侧的“  ”。

弹出对话框提示以下信息:

是否确定执行该操作?

2. 单击“确定”。

显示“操作成功”，并且“  ”变为“  ”表示成功禁用功率封顶功能。

设置功率封顶失效自动关机

1. 单击“功率封顶失效自动关机”右侧的“  ”。

弹出对话框提示以下信息:

是否确定执行该操作?

2. 单击“确定”。

系统显示“操作成功”，并且“  ”变为“  ”，表示功率封顶失效时，15秒后系统自动关机功能已经启用。

清空历史功率数据

1. 单击“清空历史功率数据”。

弹出对话框提示以下信息:

是否确定执行该操作?

2. 单击“确定”。

清除所有历史功率数据，并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。

下载历史功率数据

单击“下载”。

历史功率数据文件将自动保存到本地PC。

查看最近一周的功率曲线

1. 在“历史功率”区域框中，单击“近一周”。
   可以查看最近一周系统的峰值功率曲线和平均功率曲线。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。

查看最近一天的功率曲线

1. 在“历史功率”界面中，单击“近一天”。
   可以查看最近一天系统的峰值功率曲线和平均功率曲线。

3.6.3 节能设置

功能介绍

通过使用“节能设置”界面的功能，您可以设置服务器的节能策略。

须知

节能策略可能会影响系统性能，请根据实际情况谨慎使用。

使用本功能前，需要进入BIOS菜单，完成以下操作：

- 将“EIST Support”（部分产品此参数显示为“EIST”）设置为“Enabled”。
- V2服务器Romley平台下，将“ACPI 3.0 T-States”设置为“Enabled”。
- V3服务器Brickland平台下，将“ACPI T-States”（V3服务器Grantley平台不支持此参数）设置为“Enabled”。
- V5服务器Purley平台下，将“Software Controlled T-States”设置为“Enabled”。“T-State Throttle Level”建议保持默认值，默认值为“Disabled”。

界面描述

在上方标题栏中，选择“电源与能耗”，在左侧导航树中选择“节能设置”，显示“节能设置”界面。

“节能设置”界面分为“调节列表”和“供电设置”两个区域。

图 3-18 RH8100 V3 服务器的“节能设置”界面

图 3-19 其他机架服务器的“节能设置”界面

参数说明

表 3-35 “调节列表”

参数	描述
调节CPU的最高工作频率	通过调整CPU的最高工作频率的方式调整系统能耗。不同类型CPU支持的P-State节能策略的状态数量不同。 取值说明： ● 设置为P0状态时，CPU最高频率为当前支持的最大值。 ● 设置为P1、P2、P3等状态时，CPU最高频率依次递减，功耗和性能也随之递减。 **说明** ● 当功率封顶使能时，在手动设置P-State/T-State状态值后，如果电源实时功率值超过功率封顶值，会导致手动设置的P-State/T-State状态值失效，P-State/T-State会自动调节至正常值。 ● 只有在OS启动后设置此状态，才能生效。
调节CPU的空闲工作时间	通过调整CPU工作时间占空比的方式调整系统能耗。不同类型CPU支持的T-State节能策略的状态数量不同。 取值说明： ● 设置为T0状态时，CPU工作时间占空比为当前支持的最大值。 ● 设置为T1、T2、T3等状态时，CPU工作时间占空比依次递减，功耗和性能也随之递减。 **说明** ● 当功率封顶使能时，在手动设置P-State/T-State状态值后，如果电源实时功率值超过功率封顶值，会导致手动设置的P-State/T-State状态值失效，P-State/T-State会自动调节至正常值。 ● 只有在OS启动后设置此状态，才能生效。

表 3-36 “供电设置”（ RH8100 V3 无此功能 ）

参数	描述
电源实际状态	
系统功率	服务器当前功率。
电源功率	服务器所有电源模块当前的功率。
工作模式	服务器电源模块当前的工作模式。
主用电源	服务器当前主用电源模块。 **说明** 当工作模式为“负载均衡”时，此处显示所有在位的电源模块。
电源预期状态	

参数	描述
工作模式	服务器电源模块的工作模式，分为： ● 负载均衡：多个电源模块同时为系统供电，均摊系统所需功耗。 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，为系统供电，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，降低服务器功耗，延长电源模块使用寿命，但是供电能力低。 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，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。 ● 目前仅支持在配置2个电源时开启主备供电功能（1+1冗余）。
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。 是否启用深度休眠。开启深度休眠，系统下电后，进入深度休眠模式的电源会关闭输出；关闭深度休眠或系统上电后，进入深度休眠模式的电源会恢复输出。 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** ● 仅1288H V5、2288H V5、2488 V5、2488H V5和5885H V5支持开启或关闭深度休眠功能。 ● 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。

操作步骤

CPU节能设置

1. 在上方标题栏中选择“电源与能耗”。
2. 在左侧导航树中，选择“节能设置”。
   右侧显示“节能设置”界面。

3. 根据表3-35提供的参数信息，拖动节能策略下方的游标标签选择节能状态。

   说明

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

4. 单击“保存”。

   弹出对话框提示以下信息：

   是否确认执行该操作?

5. 单击“确定”。

   系统显示“操作成功”表示设置成功。

电源工作模式设置（RH8100 V3服务器无此功能）

1. 在上方标题栏中选择“电源与能耗”。
2. 在左侧导航树中，选择“节能设置”。

   右侧显示“节能设置”界面。

3. 在“电源预期状态”区域框中，根据表3-36提供的参数信息，设置服务器电源工作模式和主用电源以及开启或关闭深度休眠。

   说明

   - 仅1288H V5、2288H V5、2488 V5、2488H V5和5885H V5支持开启或关闭深度休眠功能。
   - 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。

4. 单击“保存”。

   弹出对话框提示以下信息：

   是否确认执行该操作?

5. 单击“确定”。

   系统显示“操作成功”表示设置成功。

3.7 配置

3.7.1 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添加、配置和删除。

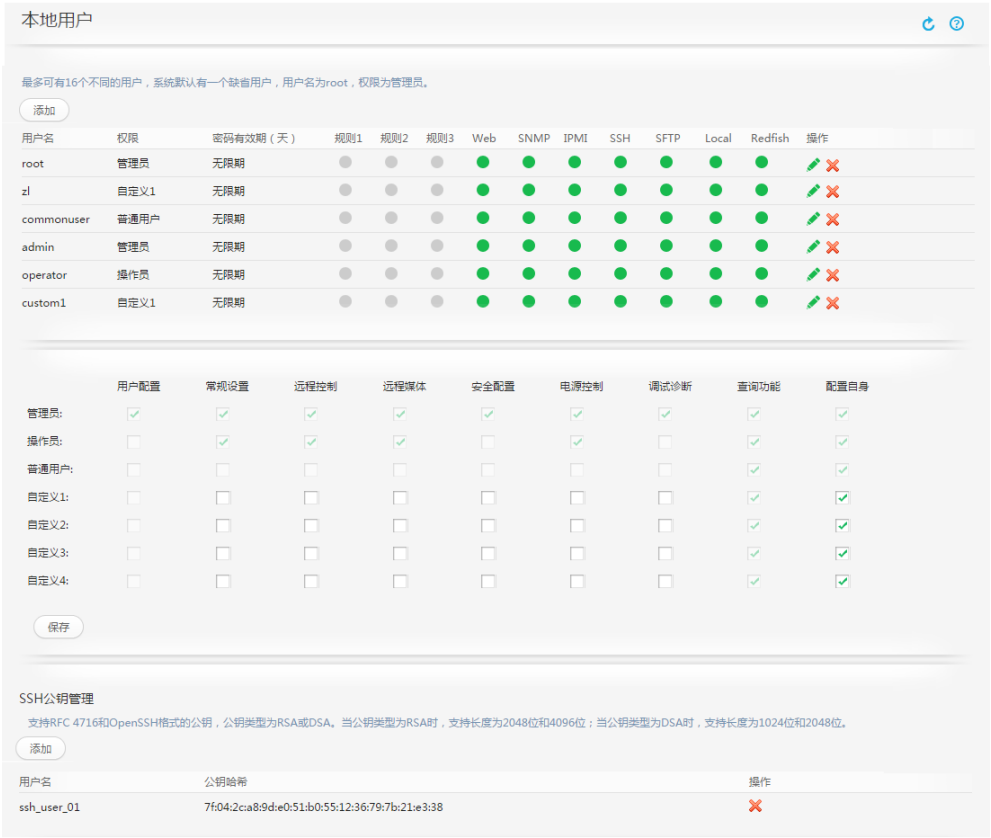
界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“本地用户”，显示“本地用户”界面，分为三个区域：

- 本地用户列表：列出当前存在的本地用户，并提供用户操作接口。

- 权限信息：列出“管理员”、“操作员”、“普通用户”以及4个“自定义用户”具备的不同权限。
- SSH公钥管理：列出已配置公钥的SSH用户，并提供SSH公钥的添加和删除接口。

图 3-20 “本地用户”界面



参数说明

表 3-37 本地用户列表区域

参数	描述
添加	打开配置新建本地用户区域框。
	打开配置已有本地用户区域框。

参数	描述
	删除已有本地用户。 **说明** • 包括管理员、操作员、普通用户、自定义用户在内的所有本地用户均可删除。 • iBMC V357及以上版本，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。 • 通过恢复iBMC默认配置恢复管理员用户，具体操作请参考iBMC用户指南中的“常用操作 > 恢复iBMC默认配置”章节。 • 若已在“配置 > 系统配置 > 设置业务侧用户管理使能状态”开启了“用户管理功能”，可在OS侧通过发送标准的IPMI命令为iBMC添加本地用户。
	保存当前权限配置。
用户名	登录iBMC系统的用户名称。 系统有1个默认用户，V3服务器中用户名为“root”，V5服务器中用户名为“Administrator”，默认密码请参考产品的铭牌，建议首次登录后修改此默认密码。
权限	用户所属的权限分组。
密码有效期（天）	用户密码的使用期限。
规则	是否启用对应的登录规则，对已选择该登录规则的本地用户进行限制。
登录接口	是否使能对应的登录接口，可通过使能的接口登录iBMC系统。

表 3-38 权限列表区域

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。

参数	描述
用户配置	用户和密码相关的配置。 用户配置包括： ● 本地用户 ● 在线用户 ● LDAP用户的配置 ● 双因素认证以及恢复出厂设置
常规设置	服务器带外管理基本配置。 常规设置包括： ● 网络配置 ● 告警上报配置 ● 服务器识别 ● 固件升级 ● 系统日志下载/删除 ● 启动设备配置 ● 存储设备配置 ● 语言更新 没有此权限的用户进入“告警设置”、“网络配置”、“系统配置”、“系统信息”、“语言更新”界面后只能查看，不能设置。
远程控制	Java集成远程控制台、HTML5集成远程控制台、独立远程控制台、VNC配置（V5服务器支持）、串口重定向功能。
远程媒体	虚拟媒体功能。
安全配置	安全性的查询和配置。 安全配置包括： ● 查看操作日志 ● 安全日志 ● 算法选择 ● 协议切换 ● SSL证书管理 ● 服务配置 ● 一键收集 ● 配置文件导入导出 ● 登录安全信息配置 没有此权限的用户进入“服务配置”、“SSL证书”、“导入导出”界面后只能查看，不能设置。

参数	描述
电源控制	上下电、重启、功率、节能配置。 没有此权限的用户进入“电源控制”、“功率”、“节能设置”界面后只能查看，不能设置。
调试诊断	现场定位、调试操作。 调试诊断包括： ● 进入维护调测接口 ● 传感器模拟 ● 自动录像配置 ● 手动/自动截屏 ● 串口重定向记录 ● 黑匣子
查询功能	可以登录以及查看除安全配置、用户配置和系统相关以外的信息。
配置自身	可以配置帐户自身的密码以及管理SSH公钥。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 3-39 SSH 公钥管理区域

参数	描述
用户名	启用SSH公钥管理的用户。
公钥哈希	导入的SSH公钥经过哈希算法转换后得到的字符串。
	删除SSH用户的公钥。
	为SSH用户导入公钥。

操作步骤

查看用户信息

1. 在上方标题栏中选择“配置”。
2. 在左侧导航树中，选择“本地用户”。
   右侧显示“本地用户”界面。
   显示所有本地用户信息。

添加用户

iBMC系统最多可添加15个不同名称的用户。

1. 单击“添加”。
   弹出添加用户的窗口，如图3-21所示，界面参数说明如表3-40所示。

图 3-21 添加用户

表 3-40 添加用户所需参数

参数	描述
取消	取消对新建用户的配置。
保存	保存对新建用户的配置。
请输入您的密码	新建用户前需要输入当前登录iBMC系统的用户密码。
新用户ID	新建用户的编号。 设置方法：在下拉列表中选择，ID取值范围为3～17。
新用户名	新建用户的名称。 取值范围：1～16位的字符串。 取值原则： ● 由特殊符号、英文字母和数字组成，特殊字符不包括：:<>&,'"/\% ● 不能包含空格且首字符不能是“#”、“+”或“-”。

参数	描述
新密码	新建用户登录iBMC系统的用户密码，为了保证安全，用户应定期修改自己的登录密码。 **说明** • 只有管理员可以设置密码检查功能的开启状态。 • 禁用密码检查功能会降低系统安全性，请尽量启用此功能。 取值范围： • 关闭密码检查功能后，密码不能为空，可以是任意字符组成的长度不大于20的字符串。 • 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。 • 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** • V3服务器不支持弱口令检查规则。 • V5服务器的默认密码“Admin@9000”在弱口令字典中。
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。
登录规则	是否启用对应的登录规则，对已选择该登录规则的本地用户进行限制。 规则查询和设置方法：单击请确认登录规则已配置并启用，点此查看。

参数	描述
登录接口	是否使能对应的登录接口，用户可通过使能的登录接口登录iBMC系统。 取值范围： ● Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 ● 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。 ● 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。 ● 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。 ● 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。 ● Local：使能该接口后，用户可通过服务器的串口登录iBMC命令行，或通过LCD登录iBMC管理界面。 ● 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。
权限	用户所属的权限分组。 取值范围：“管理员”、“操作员”、“普通用户”、“自定义”和“无权限用户”。 ● 属于“管理员”组的用户拥有权限规则中定义的所有权限。 ● 属于“操作员”组的用户拥有权限规则中定义的“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”等权限。 ● 属于“普通用户”组的用户只拥有权限规则中定义的“查询功能”和“配置自身”权限。 ● 属于“自定义1”~“自定义4”组的用户拥有权限规则中设置的权限。 ● 属于“无权限用户”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”。

2. 根据表3-40所述参数信息，设置用户的基本属性。

说明

- 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。
- V3服务器中ID为2的用户为“root”，V5服务器中ID为2的用户为“Administrator”用户。

3. 单击“保存”。
   在用户列表中显示成功添加的用户信息。

修改用户信息

1. 在本地用户列表中，选择需要修改的用户并单击  。
   弹出修改用户信息的窗口，如图3-22所示，界面参数说明如表3-41所示。

图 3-22 修改用户信息

表 3-41 修改用户信息所需参数

参数	描述
	取消修改用户信息。
	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。
请输入您的密码	修改用户信息前需要输入当前登录iBMC系统的用户密码。
用户名	待修改用户的名称。

参数	描述
修改密码	是否修改指定用户的密码。 设置方法：勾选复选框后，在“密码”和“密码确认”文本框中输入修改后的密码。 ● 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。 ● 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。 ● 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** ● V3服务器不支持弱口令检查规则。 ● V5服务器的默认密码“Admin@9000”在弱口令字典中。
登录规则	是否启用对应的登录规则，对已选择该登录规则的本地用户进行限制。 规则查询和设置方法：单击请确认登录规则已配置并启用，点此查看。

参数	描述
登录接口	是否使能对应的登录接口，用户可通过使能的登录接口登录iBMC系统。 取值范围： • Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 • 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。 • 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。 • 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。 • 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。 • Local：使能该接口后，用户可通过服务器的串口登录iBMC命令行，或通过LCD登录iBMC管理界面。 • 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。
权限	用户所属的权限分组。

2. 根据表3-41提供的参数信息，输入当前用户密码并修改指定用户的基本属性。
3. 单击“保存”。
   成功修改用户信息。

删除用户

1. 在本地用户列表中，选择需要删除的用户并单击  。
   弹出“确认删除”对话框，提示“请输入您的密码”。
2. 输入当前用户密码，单击“确定”。
   用户列表中该用户信息已消失。

设置自定义用户权限

iBMC系统提供的默认分组“管理员”、“操作员”和“普通用户”的权限信息不能修改。您可以根据实际使用需求定制其他权限分组。

仅管理员可设置自定义用户权限。

1. 在功能模块分组列表中，为自定义权限组勾选可操作的功能模块。
   各种功能模块的详细信息如表3-38所示。
2. 单击“保存”。
   弹出“确认修改”对话框，提示“请输入您的密码”。
3. 输入当前用户密码，单击“确定”。

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，可导入新的公钥进行替换。
- 支持RFC 4716和OpenSSH格式的公钥，公钥类型为RSA或DSA。
  - 当公钥类型为RSA时，支持长度为2048位和4096位。
  - 当公钥类型为DSA时，支持长度为1024位和2048位。

1. 在“SSH公钥管理”区域单击“添加”。
   打开导入SSH公钥的区域，如图3-23所示，界面参数说明如表3-42所示。

图 3-23 导入 SSH 公钥

表 3-42 导入 SSH 公钥所需信息

参数	描述
请输入您的密码	当前登录iBMC系统的用户密码。
用户名	要导入SSH公钥的SSH用户。
公钥导入方式	导入SSH公钥的方法。 取值范围： • 文件导入：选择客户端上保存的SSH公钥文件进行导入。 • 文本输入：在文本框中输入SSH公钥的具体内容进行导入。

2. 按照表3-42所示进行配置。
3. 单击“保存”。
   提示“公钥导入成功”。

3.7.2 LDAP 配置

功能介绍

通过使用“LDAP配置”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 Web界面，也可通过SSH方式登录iBMC命令行。

须知

LDAP服务器的DisplayName和CN要保持一致。

iBMC同时支持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。

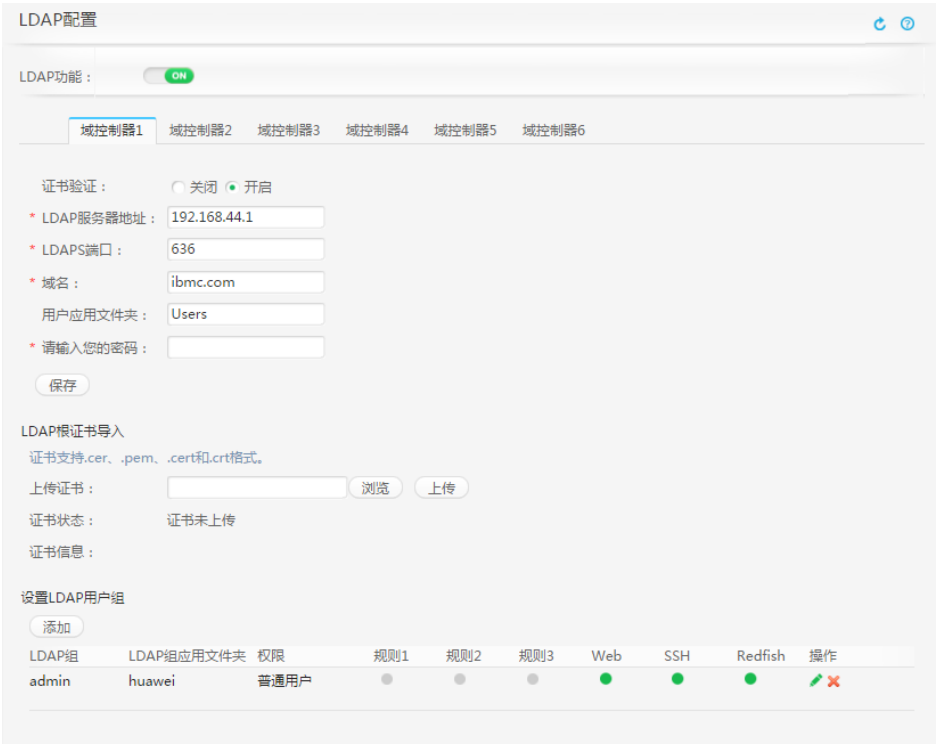
说明

iBMC当前支持与Windows AD和Linux OpenLDAP的对接。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“LDAP配置”，显示“LDAP配置”界面。

图 3-24 “LDAP 配置”界面



参数说明

表 3-43 “LDAP 配置”界面

参数	描述	
LDAP功能	是否启用LDAP组功能。 单击“  ”或“  ”并单击“保存”，可切换状态。 ● “  ”表示LDAP功能正在启用。 ● “  ”表示LDAP功能已经停用。	
域控制器1 iBMC可同时配置6个域服务器。用户使用LDAP方式登录iBMC的Web界面时，可指定任意一个域控制器，或自动适配任意一个域控制器。 域控制器2～域控制器6的配置与域控制器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	证书验证	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。
	LDAP服务器地址	LDAP服务器的IP地址。 输入格式：IPv4地址或IPv6地址。 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。
	LDAPS端口	LDAP服务的端口号。 取值范围：1 ～ 65535 默认值：636 **说明** iBMC仅支持使用加密传输的LDAP服务，LDAP服务端需要做相应的配置。
	域名	域控制器中定义的LDAP用户所属角色组的域。 取值范围：最大长度为255个字符。 取值原则：由数字、英文字母和特殊字符组成。
	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。
	绑定密码	LDAP代理用户的认证密码。

参数	描述	
	用户搜索文件夹	能够登录iBMC的LDAP用户在LDAP服务器上所属的目录。 若LDAP服务器上未配置默认用户文件夹，则iBMC侧必须通过此参数指定搜索范围。 若LDAP服务器上已配置默认用户文件夹，则该参数为选配。 ● 不配置此参数的情况下，搜索范围为LDAP服务器的默认用户文件夹。 ● 配置此参数的情况下，搜索范围为iBMC指定的路径。 格式为：“CN=xxx,CN=xxx,...”或“OU=xxx,OU=xxx,...”，下级节点在前，上级节点在后。 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** 目录属性“CN”和“OU”的区别，请参考LDAP协议的详细介绍。例如，在Windows AD中，  样式的文件夹属性为“CN”；  样式的文件夹属性为“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。
	请输入您的密码	配置域控制器需要输入当前登录iBMC系统的用户密码。
LDAP根证书导入	上传证书	用于上传，支持.cer、.pem、.cert和.crt格式。
	证书状态	显示是否已导入服务器。
	证书信息	显示证书信息。
设置LDAP用户组		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。
	LDAP组	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。

参数	描述	
	LDAP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。 格式为：“CN=xxx,CN=xxx,...”或“OU=xxx,OU=xxx,...”，下级节点在前，上级节点在后。 例如，可登录iBMC的LDAP组“grouptest”在LDAP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** 目录属性“CN”和“OU”的区别，请参考LDAP协议的详细介绍。例如，在Windows AD中，  样式的文件夹属性为“CN”；  样式的文件夹属性为“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。
	权限	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”。
	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： • Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 • 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。 • 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。

表 3-44 “LDAP 配置”界面

参数	描述
LDAP功能	是否启用LDAP组功能。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示LDAP功能正在启用。 • “  ”表示LDAP功能已经停用。

参数		描述
域控制器1 iBMC可同时配置6个域服务器。用户使用LDAP方式登录iBMC的Web界面时，可指定任意一个域控制器，或自动适配任意一个域控制器。 域控制器2～域控制器6的配置与域控制器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	证书验证	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根证书；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。
	LDAP服务器地址	LDAP服务器的IP地址。 输入格式：IPv4地址或IPv6地址。 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。
	LDAPS端口	LDAP服务的端口号。 取值范围：1 ~ 65535 默认值：636 **说明** iBMC仅支持使用加密传输的LDAP服务，LDAP服务端需要做相应的配置。
	域名	域控制器中定义的LDAP用户所属角色组的域。 取值范围：最大长度为255个字符。 取值原则：由数字、英文字母和特殊字符组成。

参数	描述	
	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。 若LDAP服务器上未配置默认用户文件夹，则iBMC侧必须通过此参数指定搜索范围。 若LDAP服务器上已配置默认用户文件夹，则该参数为选配。 ● 不配置此参数的情况下，搜索范围为LDAP服务器的默认用户文件夹。 ● 配置此参数的情况下，搜索范围为iBMC指定的路径。 格式为：“CN=xxx,CN=xxx,...”或“OU=xxx,OU=xxx,...”，下级节点在前，上级节点在后。 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** 目录属性“CN”和“OU”的区别，请参考LDAP协议的详细介绍。例如，在Windows AD中，  样式的文件夹属性为“CN”；  样式的文件夹属性为“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。
	请输入您的密码	配置域控制器需要输入当前登录iBMC系统的用户密码。
LDAP根证书导入	上传证书	用于上传LDAP根证书，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。
	证书状态	显示LDAP根证书是否已导入服务器。
	证书信息	显示证书信息。
设置LDAP用户组		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。
	LDAP组	LDAP用户所属角色组的名称。 取值范围：最多可包含255个字节。由于不同字符占用的字节数可能不同，最多可以输入64到255个字符。

参数	描述	
	LDAP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。 格式为：“CN=xxx,CN=xxx,...”或“OU=xxx,OU=xxx,...”，下级节点在前，上级节点在后。 例如，可登录iBMC的LDAP组“grouptest”在LDAP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** 目录属性“CN”和“OU”的区别，请参考LDAP协议的详细介绍。例如，在Windows AD中，  样式的文件夹属性为“CN”；  样式的文件夹属性为“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。
	权限	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”。
	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： ● Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 ● 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。 ● 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。

操作步骤

启用LDAP并配置域服务器基本属性

1. 在上方标题栏中选择“配置”。
2. 在左侧导航树中，选择“LDAP配置”。
   右侧显示“LDAP配置”界面。
3. 单击“LDAP功能”后的“ 

”，此按钮变为“ 

”，表示LDAP功能已经启用。
4. 根据参数信息，设置域服务器。
5. 单击“保存”。
   显示“操作成功”。

导入LDAP根证书

1. 在“LDAP根证书导入”区域，单击“上传证书”后的“浏览”，选择要导入的LDAP根证书。
2. 单击“上传”。
   证书上传成功后，“证书状态”显示“证书已上传”，并显示上传的证书信息，包含内容如表3-45所示。

表 3-45 “证书信息”区域框

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 ● C：使用者所在的国家
有效日期从	LDAP证书生效起始日期。
到	LDAP证书生效结束日期。
序列号	LDAP证书序列号。用于证书的识别、迁移。

添加LDAP组

iBMC系统最大可以设置5个LDAP组。

1. 在“LDAP用户编辑”区域中，单击“ 添加 ”。
   弹出添加LDAP组的窗口，如图3-25所示，界面参数说明如表3-46所示。

图 3-25 添加 LDAP 组

表 3-46 添加 LDAP 组

参数	描述
请输入您的密码	当前登录iBMC系统的用户密码。
LDAP组	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。
LDAP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。 格式为：“CN=xxx,CN=xxx,...”或“OU=xxx,OU=xxx,...”，下级节点在前，上级节点在后。 例如，可登录iBMC的LDAP组“grouptest”在LDAP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** 目录属性“CN”和“OU”的区别，请参考LDAP协议的详细介绍。例如，在Windows AD中，  样式的文件夹属性为“CN”；  样式的文件夹属性为“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。
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： ● Web：使能该接口后，用户可使用浏览器登录iBMC Web界面。 ● 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。 ● 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。
权限	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”。

2. 设置LDAP组的基本属性。
3. 单击“保存”。
   在该行显示成功添加的LDAP组信息。

删除LDAP组

1. 在“LDAP组”区域中，单击待删除的LDAP组后方的  。
   弹出“确认删除”对话框，提示“请输入您的密码”。

2. 输入当前用户的密码。

修改LDAP组

1. 在“LDAP用户编辑”区域中，单击待修改的LDAP组后方的  。
2. 在显示的界面中输入当前用户的密码，并按照**表3-46**的说明修改LDAP组配置。
3. 单击“保存”。

3.7.3 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 Web的安全对接。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“双因素认证”，显示“双因素认证”界面。

参数说明

表 3-47 “双因素认证”界面

参数	描述
双因素认证使能	是否使能双因素认证功能。使能该功能后，在客户端登录iBMC Web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。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”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后，必须导入根证书和客户端证书，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，且无法手动开启。
证书撤销检查	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 Web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 Web。 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示启用证书撤销检查功能。 • “  ”表示停用证书撤销检查功能。 **说明** 证书撤销检查采用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。
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、使用者以及截止日期。 iBMC最多支持16个根证书。
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、客户端证书指纹（即客户端证书文件的哈希值）、对应的根证书上传状态。 iBMC最多支持16个用户对应的客户端证书。

操作步骤

启用双因素认证并上传证书到iBMC

说明

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

1. 在上方标题栏中选择“配置”。

2. 在左侧导航树中，选择“双因素认证”。
   右侧显示“双因素认证”界面。
3. 单击“双因素认证使能”后的“  ”，此按钮变为“  ”，表示双因素认证功能已经启用。
4. 在“根证书”页签中单击“证书文件”后的  ，并选择根证书文件。
5. 单击“上传”。
   显示“上传成功”。
6. 在“客户端证书”页签中单击指定用户名后的  ，并选择客户端证书文件。
7. 单击“上传”。
   显示“上传成功”。

启用证书撤销检查功能

1. 单击“证书撤销检查”后的“  ”，此按钮变为“  ”，表示证书撤销检查功能已经启用。

使用证书认证方式登录iBMC

说明

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 Web的证书登录。

1. 在客户端打开浏览器，例如Google Chrome。
2. 单击浏览器右上角的  ，并选择“设置”。
3. 在Chrome的设置页面中，单击“HTTPS/SSL”下的“管理证书”。
4. 在证书管理窗口中，导入客户端证书。
5. 重新在Chrome的地址栏中输入iBMC地址登录。
6. 按照提示信息选择当前客户端证书。
   可成功登录iBMC Web。

删除根证书

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。
2. 单击“确定”。

删除客户端证书

1. 在“客户端证书”页签中，单击指定用户后的  。
   弹出操作确认对话框。
2. 单击“确定”。

查看根证书详细信息

1. 在“根证书”页签中，单击指定证书前的  。
   展开证书的信息介绍页面。

3.7.4 安全增强

功能介绍

通过使用“安全增强”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。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“安全增强”，显示“安全增强”界面。

图 3-26 “安全增强”界面

参数说明

表 3-48 密码设定区域

参数	描述
密码检查	是否开启针对每个用户的密码复杂度检查功能。 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、SNMP v1/v2c团体名、SNMP v3加密密码和VNC密码的复杂度检查。其检查规则分别为： • **本地用户密码检查原则** • **Trap团体名检查原则** • **SNMP v1/v2c只读团体名检查原则** • **SNMP v1/v2c读写团体名检查原则** • **SNMPv3加密密码检查原则** • **VNC密码检查原则** **须知** • 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	是否开启SSH密码认证功能。 取值范围： • 关闭：通过SSH登录iBMC时，只能使用公钥认证。 • 启用：通过SSH登录iBMC时，可使用密码认证，可以使用公钥认证。 默认为开启状态。
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。

参数	描述
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。 设置方法：在下拉列表框中选择。 **说明** 仅管理员用户可以被设置为“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。 默认值：0
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1～5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1～5，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。详情请参考各服务器的iBMC用户指南。

表 3-49 “登录规则”区域框

参数	描述
时间段	**须知** ● 起始年份和结束年份最多只能设置为2050。 ● 同一条规则的起始时间和结束时间的格式必须保持一致。 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。
IP段	规则允许的用户的具体IP地址或IP网段。支持如下两种格式： ● xxx.xxx.xxx.xxx：允许登录服务器的单个用户的IP地址。 ● xxx.xxx.xxx.xxx/mask：允许登录服务器的用户IP网段，其中“mask”为子网掩码长度，取值范围为1～32。

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

表 3-50 “登录安全性信息配置”区域框

参数	描述
登录安全性信息	是否开启登录安全性信息配置功能。 将开关状态设置为“ ON ”后，此处设置的安全警示信息将显示在登录界面的“安全公告”区域。 系统默认开启登录安全性信息配置功能。
安全消息	显示在登录界面的具体信息。 取值范围：最大1600字节的字符串。

操作步骤

启用安全增强功能

1. 在上方标题栏中选择“配置”。
2. 在左侧导航树中，选择“安全增强”。
   右侧显示“安全增强”界面。
3. 根据表3-48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。
4. 单击“保存”。
   弹出“确认修改”对话框。
5. 单击“确定”。

设置登录规则

iBMC同时支持三组登录规则。

说明

- 登录规则对服务器的本地用户、LDAP组、SNMPv3服务、CLP（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：
  1. 该登录规则已在“登录规则”区域框中启用。
  2. 该登录规则已在对应配置区域框中勾选。
- 某条登录规则为空时，开关状态为“  ”并保存后，将导致登录无限制。
- 满足任意一条启用的登录规则即可登录。
- 登录规则输入框为空时表示此项无限制。

1. 在“登录规则”区域中，单击待启用的规则后方的“  ”，使之变为“  ”。
2. 根据表3-49提供的参数信息，设置服务器登录规则。
3. 单击“保存”。
   弹出“确认修改”对话框。
4. 单击“确定”。

设置登录安全性信息

1. 在“登录安全性信息配置”区域中单击“  ”使之变为“  ”。
2. 在“安全消息”文本框中输入待设置的信息。
3. 单击“保存”。
   弹出“确认修改”对话框。
4. 单击“确定”。

恢复默认登录安全性信息

1. 在“登录安全性信息配置”区域中单击“  ”使之变为“  ”。
2. 单击“恢复默认值”。
3. 单击“保存”。
   弹出“确认修改”对话框。
4. 单击“确定”。

3.7.5 网络配置

功能介绍

通过使用“网络配置”界面的功能，您可以：

- 设置服务器的主机名称。
- 配置服务器管理网口的模式和IP地址。

须知

变更管理网口地址会导致网络连接断开，请谨慎操作。

- 设置DNS信息获取方式。

  说明

  DNS支持基于IPv4和IPv6协议的地址信息。

  RH8100 V3和8100 V5服务器的单系统模式下，插在HFC–1上的板载网卡无法提供NCSI功能，所以不会在板载网口的框内显示HFC–1上的板载网卡的port。

- 设置VLAN。
- 设置NTP配置信息。
- 设置系统时区。

说明

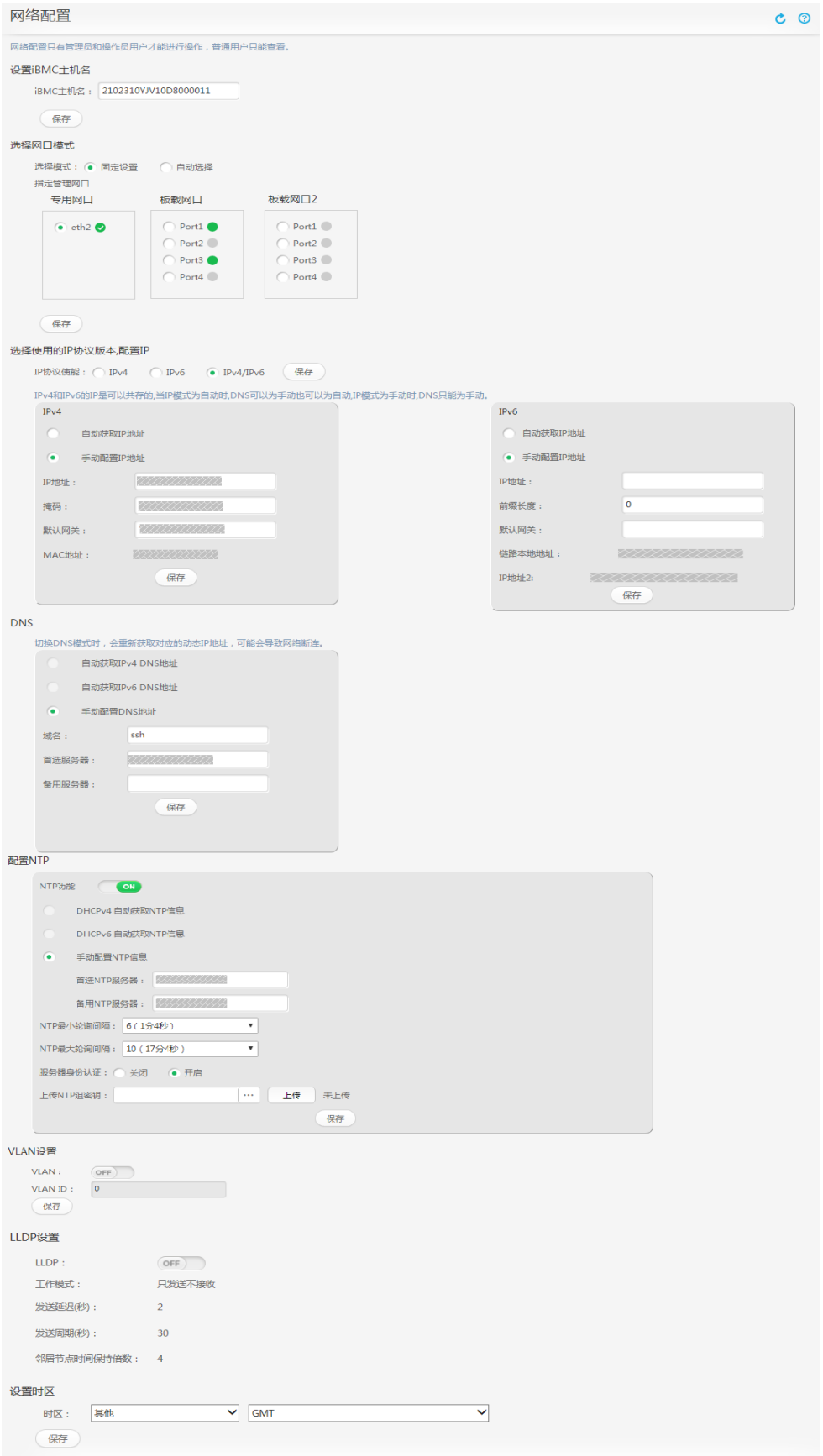
由于X540、BCM5719网卡的节能特性，在服务器上下电、加载驱动时网口会重新连接，此时NCSI功能会短暂中断。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“网络配置”，显示“网络配置”界面。

图 3-27 RH8100 V3 服务器的“网络配置”界面

图 3-28 其他机架服务器的“网络配置”界面



参数说明

表 3-51 “网络配置”界面

参数	描述
iBMC主机名	iBMC的主机名称。 取值范围：1～64位的字符串。 取值原则：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。 默认值：huawei

参数	描述
选择模式	网口模式包括： ● 固定设置：指定专用网口、板载网口、板载网口2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）。 – 板载网口：板载网卡的业务网口。 **说明** ● 对于V3服务器，“板载网口”指灵活网卡插卡，没有“板载网口2”。 ● 对于V5服务器，“板载网口”指主板集成的网卡，“板载网口2”指灵活网卡插卡。 – 板载网口2：灵活网卡插卡的业务网口（即V5服务器的灵活网卡插卡）。 – PCIE扩展网口（此网口不能作为RH8100 V3、8100V5、RH5885 V3、RH5885H V3、2488 V5和2488H V5服务器的iBMC管理网口）：PCIe卡的业务网口（即支持NCSI且已连接NCSI线缆的PCIe扩展网卡）。 ● 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根据专用网口、板载网口、板载网口2、PCIe扩展网口（此网口不能作为RH8100 V3、8100V5、RH5885 V3、RH5885H V3、2488 V5和2488H V5服务器的iBMC管理网口）的顺序选择管理网口。 iBMC根据各物理网口的连接状态来选择所使用的物理网口。 – V3服务器按照以下优先级顺序连接： 专用网口>板载网口（Port1～Port2或Port1～Port4）>PCIe扩展网口（Port1～Port2或Port1～Port4） – V5服务器按照以下优先级顺序连接： 专用网口>板载网口（Port1～Port2或Port1～Port4）>PCIe扩展网口（Port1～Port2或Port1～Port4），或专用网口>板载网口（Port1～Port2或Port1～Port4）>板载网口2（Port1～Port2或Port1～Port4）。 服务器同时配置灵活网卡插卡（即板载网口2）和PCIe网卡时，两者存在互斥机制。当PCIe网卡连接了NCSI线缆，PCIe网卡网口可用于访问iBMC，灵活网卡插卡网口不能访问iBMC；当PCIe网卡未连接NCSI线缆时，PCIe网卡网口不能访问iBMC，灵活网卡插卡网口可用于访问iBMC。

参数	描述
	说明 • 如果PCIe扩展网口要作为iBMC的管理网口，其所属的PCIe扩展网卡仅支持已连接NCSI线缆的网卡。 • 如果将板载网口或灵活网卡插卡设置为iBMC的管理网口，其对应的板载网卡或灵活网卡插卡需要支持NCSI。 • 当手动或自动选择板载网口、板载网口2或PCIe扩展网口时，管理网口与业务网口共用同一个物理网口。为安全起见，建议在“固定设置”或“自动选择”模式包含了板载网口、板载网口2或PCIe扩展网口时，为管理网口配置VLAN。 • 如果某个网口此时作为iBMC的管理网口，网口右侧会出现 标识。 默认值：“固定设置”
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。
IP协议使能	可以使能的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。 设置方法：选中单选按钮。
手动配置IP地址	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。
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IP地址	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”和“IP地址2”。 **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。
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。

参数	描述
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DNS地址	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。 **须知** 服务器管理网口的IP地址获取模式为手动时，DNS信息获取方式也必须选择手动。
域名	服务器的域名称。 取值范围：0～67位的字符串。 取值原则：由数字、英文字母和特殊字符（包括空格）组成。
首选服务器	优先选择的DNS服务器。 取值原则：IPv4地址、IPv6地址或为空
备用服务器	第二选择的DNS服务器。 取值原则：IPv4地址、IPv6地址或为空
配置NTP	
NTP功能	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。 单击“  ”或“  ”并单击“保存”，可切换状态。 ● “  ”表示NTP功能正在启用。 ● “  ”表示NTP功能已经停用。
DHCPv4自动获取NTP信息	无需手动操作，系统自动获取基于IPv4的NTP信息。 **说明** 选择该方式时，不需要手动配置时区信息。
DHCPv6自动获取NTP信息	无需手动操作，系统自动获取基于IPv6的NTP信息。
手动配置NTP信息	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。
首选NTP服务器	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** ● iBMC V312以下版本仅支持Linux NTP服务器。 ● iBMC V312及以上版本，支持Linux NTP服务器和Windows NTP服务器。

参数	描述
备用NTP服务器	第二选择的NTP服务器的地址。 取值范围：IPv4地址、IPv6地址和域名 **说明** • iBMC V312以下版本仅支持Linux NTP服务器。 • iBMC V312及以上版本，支持Linux NTP服务器和Windows NTP服务器。
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
NTP时间同步周期	系统从NTP服务器进行时间同步的周期。 系统根据网络状态自动动态调整同步周期，网络状态良好时，同步周期值朝最大值调整。
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。
VLAN设置	
VLAN	使能或禁止管理网口的VLAN属性。 单击“OFF”或“ON”并单击“保存”，可切换状态。 • “ON”表示VLAN正在启用。 • “OFF”表示VLAN已经停用。 **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；若选择了除“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。 默认值：“OFF”
VLAN ID	管理网口所属VLAN。

参数	描述
设置时区	iBMC系统的时区。 取值范围： ● 时间偏移：“其他”+“GMT-hh:mm”或“其他”+“GMT+hh:mm”，选择范围为GMT-12:00～GMT+14:00。 ● 时区名称：“全球地区名”+“城市”。 **说明** ● 当选择“DHCPv4自动获取NTP信息”时，不需要设置时区信息。 ● 在支持夏令时的时区，iBMC时间会在每年开始夏令时时自动调快1小时，结束夏令时时自动调慢1小时。 默认值：“其他”+“GMT”

操作步骤

设置iBMC主机名

1. 在“网络配置”页面中，根据表3-51提供的参数，设置服务器的主机名。
2. 单击“保存”。
   显示“操作成功”表示成功设置服务器的主机名。
3. 若选择“稍后重启”，您可以在合适的时间重启iBMC来生成新的SSL证书。若选择“立即重启”，则将立即重启iBMC。

   说明

   设置主机名成功后，复位iBMC将重新生成SSL证书。

选择网口模式

1. 在“网络配置”页面中，根据表3-51提供的参数信息，选择网口模式并指定管理网口。
2. 单击“保存”。
   显示“操作成功”表示管理网口的网口模式和主机端口设置成功。

设置管理网口的IPv4地址

1. 在“网络配置”页面的“配置IPv4”区域框中，根据表3-51提供的参数信息，设置IPv4地址。
2. 单击“保存”。
   显示“操作成功”表示管理网口的IPv4地址设置成功。

设置管理网口的IPv6地址

1. 在“网络配置”页面的“配置IPv6”区域框中，根据表3-51提供的参数信息，设置IPv6地址。
2. 单击“保存”。
   显示“操作成功”表示管理网口的IPv6地址设置成功。

自动获取DNS信息

1. 根据管理网口的IP类型，选择“自动获取IPv4 DNS地址”或“自动获取IPv6 DNS地址”单选按钮。

   说明

   自动获取DNS信息的IP类型包括IPv4和IPv6。

2. 单击“保存”。

   显示“操作成功”表示成功设置DNS属性。

手动配置DNS信息

1. 选中“手动配置DNS地址”单选按钮。
2. 根据表3-51提供的参数，设置服务器的“域名”、“首选服务器”和“备用服务器”。
3. 单击“保存”。

   显示“操作成功”表示成功设置DNS信息。

设置管理网口的VLAN信息

说明

VLAN仅对共享模式的管理网口生效，不对专有模式的管理网口生效。

1. 在“网络配置”页面的“VLAN设置”区域框中，根据表3-51提供的参数信息，设置管理网口的VLAN信息。
2. 单击“保存”。

   显示“操作成功”表示管理网口的VLAN设置成功。

配置NTP信息

1. 在“配置NTP”区域框中，根据表3-51提供的参数信息，设置NTP信息。
2. 单击“保存”。

   显示“操作成功”表示设置成功。

设置时区

1. 在“设置时区”区域框中，选择要设置的时区。
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，为了保证系统时间与iBMC时间一致，请执行命令**hwclock --utc -w**。

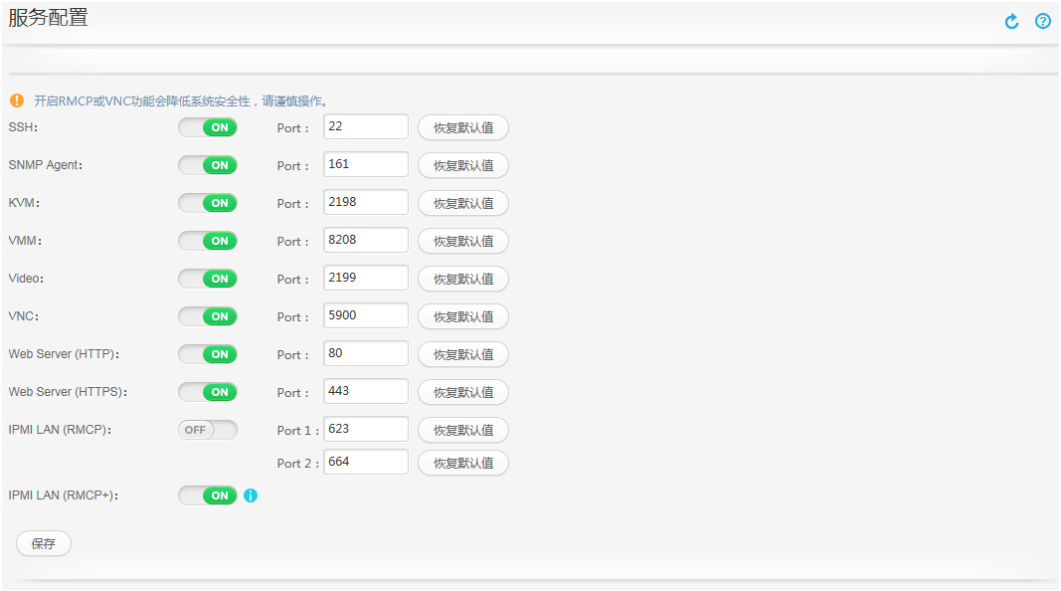
3.7.6 服务配置

功能介绍

通过使用“服务配置”界面的功能，您可以查看和设置系统服务信息。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“服务配置”，显示“服务配置”界面。



参数说明

表 3-52 “服务配置”界面

参数	描述
服务	系统服务的名称。系统服务包括： • “SSH”：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”：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”：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”：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。 • “Video”：从远端控制服务器时需要用到的Video服务，开启后可使用3.5.1 录像回放功能。 同一时间只允许1个用户使用。 • “VNC”：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。 **说明** 仅V5服务器支持VNC服务。 • “Web Server(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。 • “Web Server(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。 最多允许4个用户同时使用该服务登录iBMC。 • “IPMI LAN(RMCP)”：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

参数	描述
	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+)”：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。 单击“OFF”或“ON”并单击“保存”，可切换状态。 ● “ON”表示该服务正在启用。 ● “OFF”表示该服务已经停用。
端口号	系统服务占用的端口号。 取值范围：1～65535之间的数字。 默认取值： ● SSH：“22” ● SNMP Agent：“161” ● KVM：“2198” ● VMM：“8208” ● Video：“2199” ● VNC：“5900” ● Web Server(HTTP)：“80” ● Web Server(HTTPS)：“443” ● IPMI LAN(RMCP)：Port 1为主用端口，默认“623”；Port 2为备用端口，默认“664” ● IPMI LAN(RMCP+)：RMCP+和RMCP端口共用，设置RMCP端口时RMCP+也使用相同的端口。 **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。 ● 仅V5服务器支持VNC服务。

操作步骤

设置服务端口

1. 在上方标题栏中选择“配置”。

2. 在左侧导航树中，选择“服务配置”。
   右侧显示“服务配置”界面。
3. 根据表3-52提供的参数信息，设置需要开启的系统服务及其端口号。

   说明

   单击各端口右侧的“恢复默认值”后，该端口号变为默认值。

   表 3-53 服务端口设置

选项	操作
SSH	在“Port”文本框中，输入端口号。
SNMP Agent	在“Port”文本框中，输入端口号。
KVM	在“Port”文本框中，输入端口号。
VMM	在“Port”文本框中，输入端口号。
Video	在“Port”文本框中，输入端口号。
VNC	在“Port”文本框中，输入端口号。
Web Server(HTTP)	在“Port”文本框中，输入端口号。
Web Server(HTTPS)	在“Port”文本框中，输入端口号。
IPMI LAN(RMCP)	1. 在“Port 1”文本框中，输入端口号。 2. 在“Port 2”文本框中，输入端口号。
IPMI LAN(RMCP+)	RMCP+和RMCP端口共用，设置RMCP端口时RMCP+也使用相同的端口。

4. 单击“保存”。
   显示“操作成功”表示完成设置。

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。

3.7.7 系统配置

功能介绍

通过使用“系统配置”界面的功能，您可以：

- 查看和设置SNMP信息。
- 查看和设置TLS版本。
- 设置业务侧用户管理使能状态。
- 查看和设置Web Server超时时长和Web会话模式。
- 查看和设置设备位置。
- 查看和设置告警门限。
- 查看和设置硬分区。
- 查看和设置RAID工作模式。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“系统配置”，显示“系统配置”界面。

图 3-29 8100 V5 的“系统配置”界面

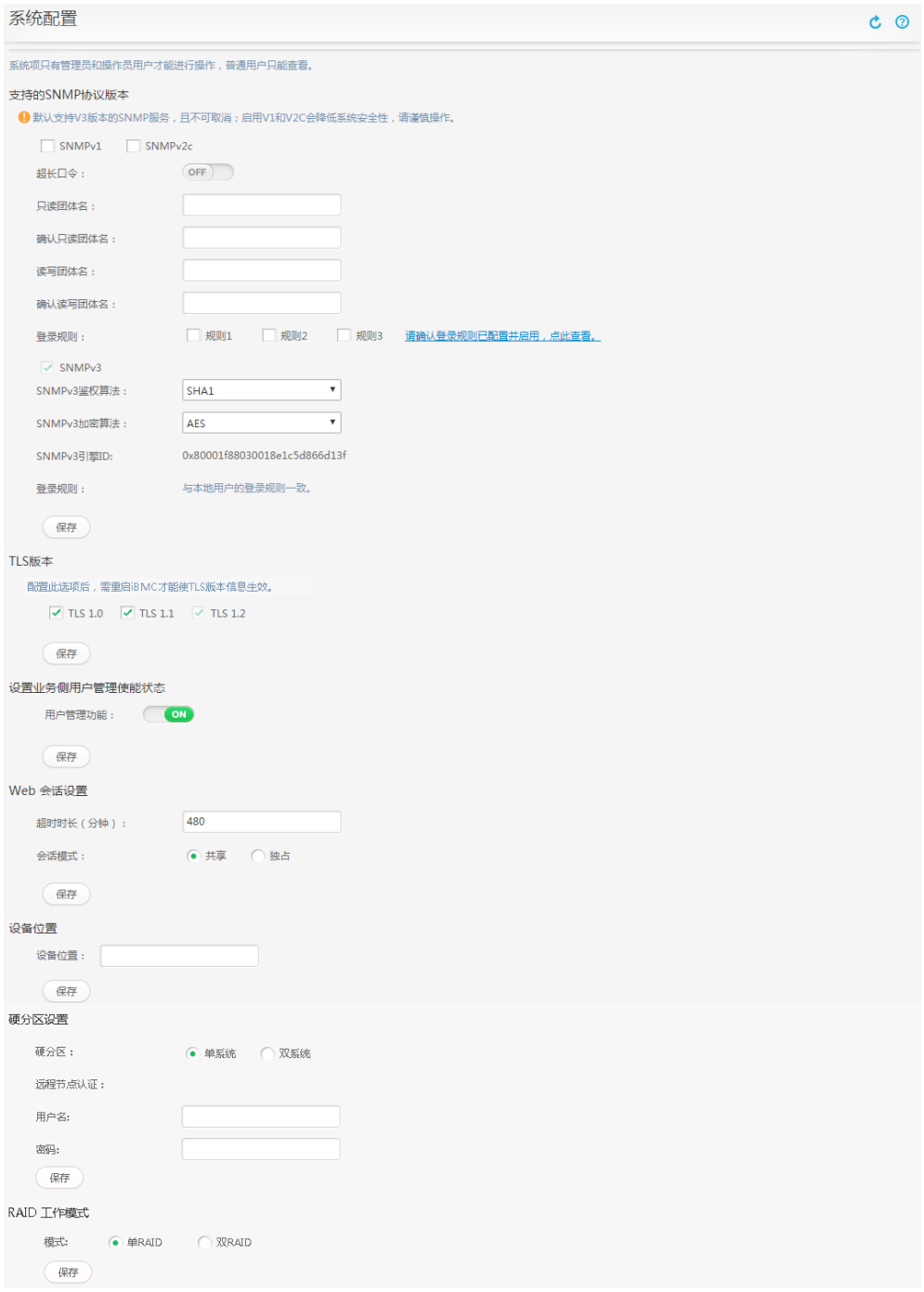


图 3-30 RH5885 V3 的“系统配置”界面

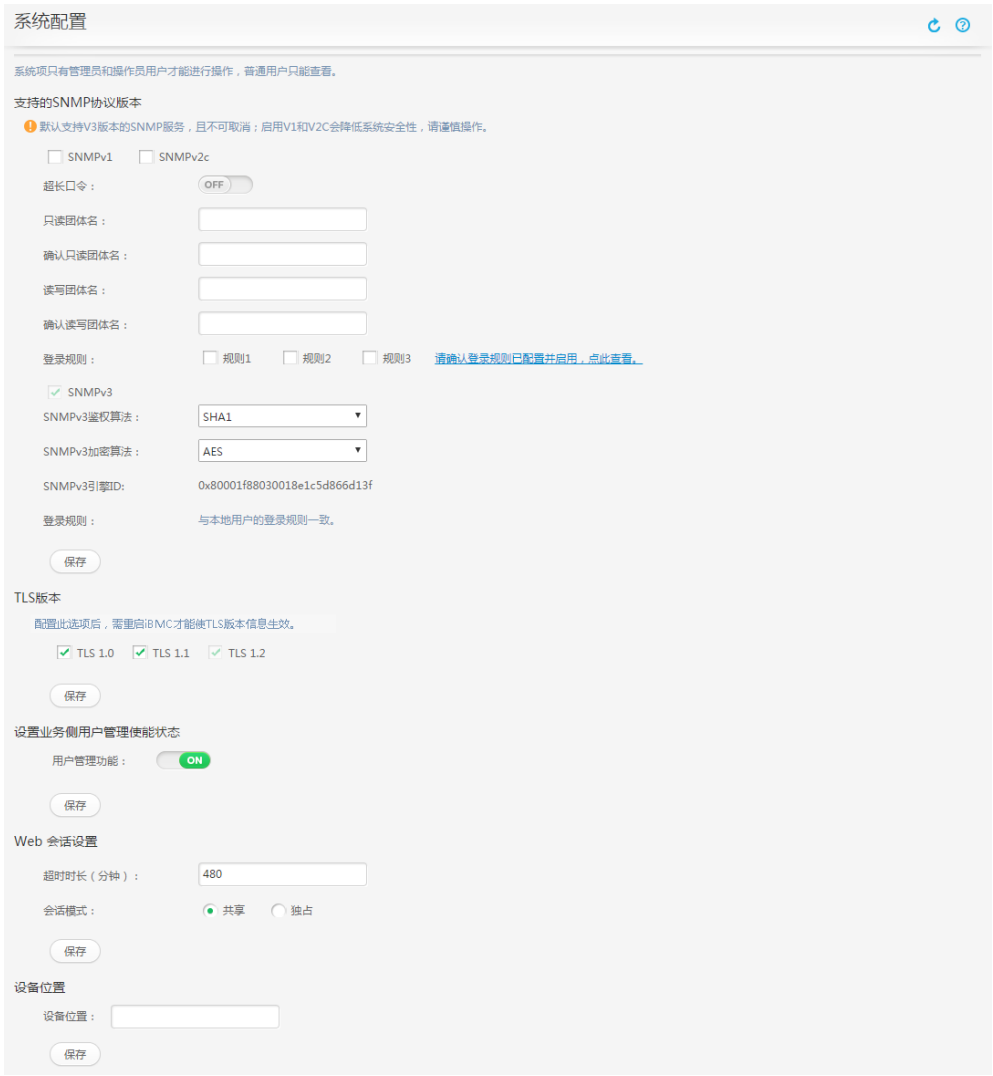


图 3-31 其他 V3 机架服务器的“系统配置”界面

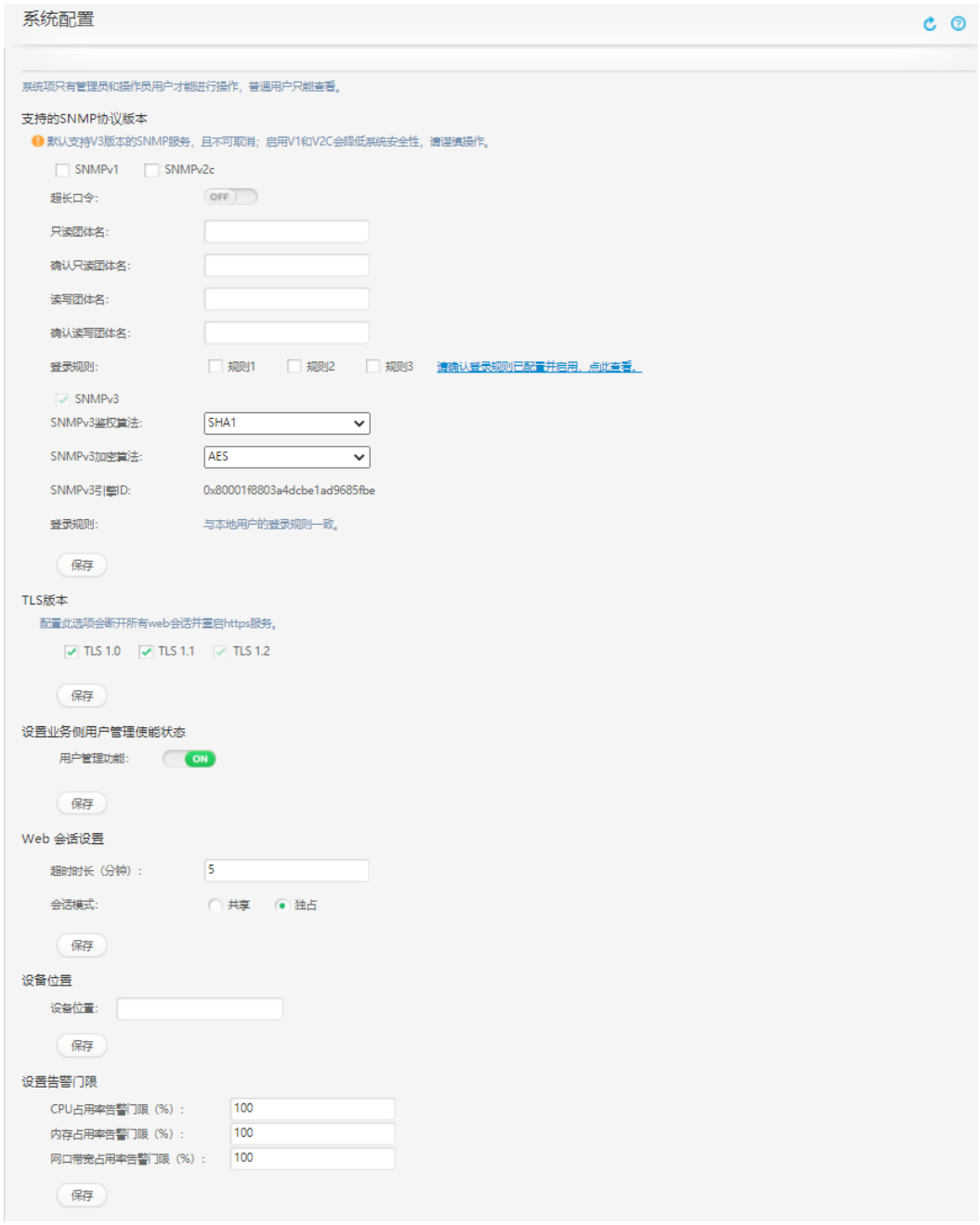


图 3-32 V5 机架服务器的“系统配置”界面

参数说明

表 3-54 “系统配置”SNMP 区域界面

参数	描述
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。 **说明** 如果启用该版本的SNMP服务，请及时修改SNMP的团体名。
SNMPv2c	针对SNMP V2的改进版本。SNMPv2c版本是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。 **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	设置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：V3服务器的默认值为“OFF”，V5服务器的默认值为“ON”。 单击“OFF”或“ON”并单击“保存”，可切换状态。 ● “ON”表示已启用超长口令。 ● “OFF”表示已停用超长口令。

参数	描述
只读团体名	SNMP协议只读团体名，V3服务器默认为**roAdmin12#$**，V5服务器默认为**roAdministrator@9000**。 **说明** 该参数仅在SNMPv1和SNMPv2c版本生效。 取值原则： ● 关闭密码检查功能时： – 若已启用超长口令，则团体名可设置为长度为16～32个字符的字符串，字符串不能包含空格。 – 若已禁用超长口令，则团体名可设置为长度为1～32个字符的字符串，字符串不能包含空格。 ● 开启密码检查功能时： – 长度要求： – 若已启用超长口令，则团体名可设置为长度为16～32个字符的字符串。 – 若已禁用超长口令，则团体名可设置为长度为8～32个字符的字符串。 – 至少包含以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/? – 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**获取。 **说明** V3服务器不支持弱口令检查规则。
确认只读团体名	重复输入上一步的只读团体名，确认输入是否正确。

参数	描述
读写团体名	SNMP协议读写团体名，V3服务器默认为**rwAdmin12#$**，V5服务器默认为**rwAdministrator@9000**。 **说明** 该参数仅在SNMPv1和SNMPv2c版本生效。 取值原则： ● 关闭密码检查功能时： – 若已启用超长口令，则团体名可设置为长度为16～32个字符的字符串，字符串不能包含空格。 – 若已禁用超长口令，则团体名可设置为长度为1～32个字符的字符串，字符串不能包含空格。 ● 开启密码检查功能时： – 长度要求： – 若已启用超长口令，则团体名可设置为长度为16～32个字符的字符串。 – 若已禁用超长口令，则团体名可设置为长度为8～32个字符的字符串。 – 至少包含以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/? – 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**获取。 **说明** V3服务器不支持弱口令检查规则。
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SNMPv2c是否启用对应的登录规则，对已选择该登录规则的本地用户进行限制。 规则查询和设置方法：单击请确认登录规则已配置并启用，点此查看。
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** iBMC系统默认支持V3版本的SNMP服务，且不可取消。

参数	描述
SNMPv3鉴权算法	SNMPv3采用的鉴权算法。 可选取值：MD5、SHA1 默认取值：SHA1 **说明** ● 该设置对“SNMPv3”和“SNMP Trap V3”都有效。 ● “MD5”算法存在安全隐患，建议使用“SHA1”算法。
SNMPv3加密算法	SNMPv3采用的加密算法。 可选取值：DES、AES 默认取值：AES **说明** ● 该设置对“SNMPv3”和“SNMP Trap V3”都有效。 ● “DES”算法存在安全隐患，建议使用“AES”算法。
SNMPv3引擎ID	SNMPv3引擎ID属于SNMP代理实体的SNMP引擎的唯一标识符。
SNMPv3鉴权用户	选择某个iBMC用户用于该用户通过SNMPv3协议连接iBMC时进行鉴权。 **说明** ● 仅V5服务器支持选择用户或设置该用户使用SNMPv3连接时的加密密码。 ● 此处可以选择iBMC所有本地用户。具有用户管理权限的iBMC用户可设置任意一个本地用户用于SNMPv3鉴权，不具有用户管理权限的iBMC用户只能设置自身用于SNMPv3鉴权。

参数	描述
SNMPv3加密密码	设置被用于SNMPv3鉴权的用户的加密密码。 默认取值：用于SNMPv3鉴权的用户的登录密码一致。 **说明** 仅V5服务器支持选择用户或设置该用户使用SNMPv3连接时的加密密码。 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： – 长度要求： – 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**获取。 **说明** ● 设置SNMPv3加密密码时，不检查历史密码和有效期。建议将SNMPv3加密密码设置成与用户密码不同的密码，若两者相同，会有安全风险。 ● 非管理员用户只能对自身进行操作。
登录规则	SNMPv3启用的登录规则，与本地用户的登录规则一致。

表 3-55 “系统配置”其他区域界面

参数	描述
TLS版本	在两个通信应用程序通信时，TLS（Transport Layer Security）协议保证其保密性和数据完整性。 浏览器与Web服务器通讯时，需要建立安全链接。此处可设置建立安全链接所使用过的TLS协议版本。 设置方法：勾选复选框。 **说明** • JRE1.8默认使用TLS 1.2协议。 • JRE1.7默认使用TLS 1.0协议。若禁用TLS 1.0，则在JRE1.7的环境下，无法使用KVM。
设置业务侧用户管理使能状态	设置业务侧是否能对用户进行管理，业务侧的用户管理功能禁止时，业务侧发送过来的用户管理相关的IPMI命令无效，主要包括用户添加/删除、权限设置、密码设置等IPMI命令。 默认取值：“  ” 单击“  ”或“  ”并单击“保存”，可切换状态。 • “  ”表示业务侧可以对用户进行管理。 • “  ”表示业务侧不能对用户进行管理。 建议设置为“  ”，否则业务侧可以对iBMC用户进行管理，产生安全隐患。
Web会话设置	
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。 取值原则：由数字组成，不能为空。单位为分钟。
会话模式	使用同一帐号登录Web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 Web。 • 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 Web。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。
设备位置	
设备位置	设置本机的位置信息。 信息数据类型为字符型，长度范围：0～64字节，默认为空。 可包含数字、字母以及以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/?

参数	描述
设置告警门限	
CPU占用率告警门限（%）	设置CPU占用率的告警门限，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。 **说明** 如果没有显示CPU占用率告警门限，请在OS侧安装并运行iBMA 2.0。
内存占用率告警门限（%）	设置内存占用率的告警门限，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。 **说明** 如果没有显示内存占用率告警门限，请在OS侧安装并运行iBMA 2.0。
硬分区设置（RH8100 V3和8100 V5特有功能）	将服务器配置成一个单系统或2个独立的双系统硬分区。 取值范围：单系统或双系统。 双系统工作模式下不能通过系统B的iBMC进行硬分区设置。 双系统工作模式切换为单系统工作模式的时候，系统B的管理网口的IP地址为无，默认用户的密码会恢复成产品铭牌上的默认密码；单系统工作模式切换为双系统工作模式的时候，系统B的管理网口的IP地址会恢复成192.168.2.101。 **说明** ● 单系统工作模式下，如果操作系统处于上电状态，进行单双系统切换会出现切换失败提示。 ● 双系统工作模式下，如果系统A或系统B的操作系统处于上电状态，进行单双系统切换会出现切换失败提示。
RAID工作模式（RH8100 V3和8100 V5特有功能）	将RAID配置成单RAID模式或者双RAID模式。 取值范围： ● 单RAID：单RAID模式下1号槽位的计算模块必须在位且安装了CPU，双RAID模式下1号槽位和5号槽位的计算模块必须都在位且都安装了CPU。 ● 双RAID：双RAID模式下必须保证服务器有两张RAID卡，进行单双RAID模式切换必须保证操作系统已经上电。 **说明** ● 如果服务器配置B型或C型前IO模块，无“RAID工作模式”功能。 ● 服务器配置A型前IO模块的单系统工作模式下可以配置成单RAID或双RAID模式。 ● 服务器配置A型前IO模块的双系统工作模式下通过系统A的iBMC可以从单RAID模式切换到双RAID模式，不能从双RAID模式切换到单RAID模式。 ● 服务器配置A型前IO模块的双系统工作模式下不能通过系统B的iBMC配置RAID工作模式。

操作步骤

设置SNMP服务

1. 在“系统配置”界面中，根据表3-54提供的参数信息，设置需要启用的SNMP信息。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

设置TLS版本

1. 在“系统配置”界面的“TLS版本”区域，勾选要配置的TLS版本。
2. 单击“保存”。

说明

配置此选项后，需重启iBMC才能使TLS版本信息生效。

设置业务侧用户管理使能状态

1. 在“系统配置”界面中，根据表3-55提供的参数信息，设置业务侧用户管理使能状态。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

设置Web Server服务的超时时间和会话模式

1. 在“系统配置”界面中，根据表3-55提供的参数信息，设置两次会话之间的最大时间间隔以及会话模式。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

设置设备位置

1. 在“系统配置”界面中，根据表3-55提供的参数信息，设置本机的位置信息。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

设置告警门限

1. 在“系统配置”界面中，根据表3-55提供的参数信息，设置告警门限。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

设置硬分区（RH8100 V3和8100 V5特有功能）

1. 在“系统配置”界面中，根据表3-55提供的参数信息，设置硬分区。
2. 单击“保存”。
   弹出提示窗口，提示：切换前应确保当前所有分区的业务已经安全下电，iBMC未处于升级状态。您是否要进行硬分区切换，如果切换成功，iBMC将会重启（如果主从iBMC版本或CPLD版本不一致，会导致切换不成功）！切换后从iBMC的用户名，密码和IP地址将恢复到出厂设置。
3. 单击“确定”。
   iBMC开始重启，重启后完成硬分区的切换。

设置RAID工作模式（RH8100 V3和8100 V5特有功能）

1. 在“系统配置”界面中，根据表3-55提供的参数信息，设置RAID工作模式。

2. 单击“保存”。

   弹出提示窗口，提示切换前请确保业务已经正常上电，否则会导致切换不成功！RAID模式切换操作不当会引起数据丢失，请在切换前拔出硬盘或者在业务上电之后且操作系统运行之前进行切换操作。

3. 单击“确定”。

   显示“操作成功”表示完成切换。

3.7.8 系统启动项

功能介绍

通过使用“系统启动项”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

在上方标题栏中，选择“配置”，在左侧导航树中选择“系统启动项”，显示“系统启动项”界面。

参数说明

表 3-56 “系统启动选项”界面

参数	描述
启动模式是否可切换	切换启动模式。 单击“OFF”或“ON”并单击“保存”，可切换状态。 • “ON”表示“启动模式”可切换，实际的启动模式以iBMC设置的启动模式为准。 • “OFF”表示“启动模式”不可切换，实际的启动模式以BIOS设置的启动模式为准。 **说明** • 仅V5服务器支持“启动模式是否可切换”。 • 普通用户没有权限切换启动模式。

参数	描述
启动模式	• 传统BIOS：BIOS从legacy模式启动。 • 统一可扩展固件接口（UEFI）：BIOS从UEFI模式启动。 **说明** 仅V5服务器有“启动模式”参数。
引导介质有效期	• 单次有效：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。 • 永久有效：系统启动项的设置永久有效。
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中设置的默认方式启动操作系统。

操作步骤

1. 在上方标题栏中选择“配置”。
2. 在左侧导航树中，选择“系统启动项”。
   右侧显示“系统启动项”界面。
3. 根据表3-56提供的参数信息，设置操作系统的第一启动设备。
4. 单击“保存”。
   显示“操作成功”表示成功设置启动设备。

3.7.9 SSL 证书

功能介绍

通过使用“SSL证书”界面的功能，您可以查看当前SSL（Secure Sockets Layer）证书信息，包括根证书信息、中间证书信息、以及服务器证书信息，并自定义SSL信息或导入新证书。

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，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。
- MD5为不安全的弱加密算法，V360及以上版本，iBMC不支持导入MD5加密的证书。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“SSL证书”，显示“SSL证书”界面。

参数说明

表 3-57 “当前证书信息”区域框

参数	描述
使用者	SSL证书的使用者（即当前服务器）信息，包含： • CN：使用者的名称 **说明** 使用者名称CN需要配置为服务器的FQDN（主机名.域名）。 • 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 • C：使用者所在的国家
签发者	SSL证书的签发者信息，包含的具体参数类型与“使用者”相同。
有效日期从	SSL证书生效起始日期。
到	SSL证书生效结束日期。
序列号	SSL证书序列号。用于证书的识别、迁移。

操作步骤

查看当前SSL证书信息

1. 在左侧导航树中，选择“配置 > SSL证书”。
   显示“SSL证书”界面。
2. 在“当前证书信息”区域框中，可查看到服务器当前使用的SSL证书信息。

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。

1. 在“SSL证书”界面中单击“自定义”。
   显示自定义SSL信息的界面。
2. 在“步骤一：生成CSR”区域框中，输入自定义的证书请求信息，并单击“保存”。
   按照弹出的对话框的提示信息导出CSR文件到客户端。
   自定义的证书参数如表3-58所示。

表 3-58 自定义证书参数

参数	描述
国家(C)	使用者所在的国家。 支持字母，长度为2个字符，为必填项。
省份(S)	使用者所在的省份。 支持字母、数字、连字符、下划线、句点和空格，最大长度128个字符。
城市(L)	使用者所在的城市。 支持字母、数字、连字符、下划线、句点和空格，最大长度128个字符。
公司(O)	使用者所在的公司。 支持字母、数字、连字符、下划线、句点和空格，最大长度64个字符。
部门(OU)	使用者所在部门。 支持字母、数字、连字符、下划线、句点和空格，最大长度64个字符。
常用名(CN)	使用者的名称。 支持字母、数字、连字符、下划线、句点和空格，最大长度64个字符，为必填项。

3. 将导出的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。
4. 在“步骤二：导入服务器证书”区域框中，单击“浏览”，选中SSL证书文件，并单击“导入”。
   证书成功上传到服务器后，弹出对话框提示以下信息：
   证书导入成功,复位iBMC后生效

若选择“稍后重启”，您可以在合适的时间重启iBMC使之生效。若选择“立即重启”，则将立即重启iBMC。

说明

- 导入的证书文件不得大于1MB，支持的格式为*.crt、*.cer、*.pem。
- 步骤一中生成的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。

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。

1. 在“SSL证书”界面中单击“自定义”。
   显示自定义SSL信息的界面。
2. 在“导入自定义证书”区域框中进行现有证书的导入。
   a. 单击“证书文件”后的“浏览”，选择现有的SSL证书文件（证书格式支持.pfx、.p12，不大于100KB）。
   b. 在“证书密码”后的文本框中输入传输过程中采用的密码，保证证书传输的安全性。
      如果证书受密码保护，此处必须填写所需的密码，否则无法上传。
   c. 单击“导入”。

      说明

      上传的文件如果超过100M会引起页面请求失败，刷新页面可恢复。

      证书成功上传到服务器后，弹出对话框提示以下信息：

      证书导入成功,复位iBMC后生效

      若选择“稍后重启”，您可以在合适的时间重启iBMC使之生效。若选择“立即重启”，则将立即重启iBMC。

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。

1. 打开浏览器。
2. 在工具栏中选择“工具 > Internet选项”。
   弹出“Internet选项”窗口。
3. 在“内容”页签中单击“证书”。
   打开“证书”窗口。
4. 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 => **5**
   - 否 => **6**
5. 查看证书是否过期。

- 是 => **6**
- 否 => **7**

6. 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。
7. 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

3.7.10 导入导出

功能介绍

您可以通过“导入导出”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。

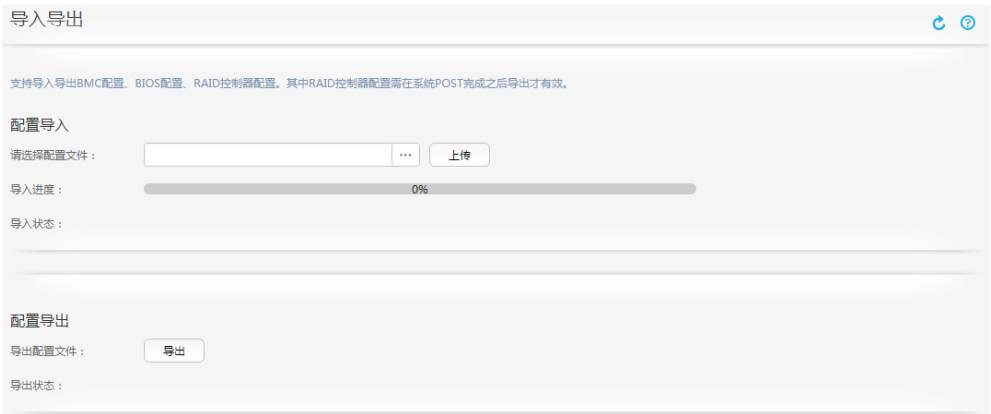
说明

- 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，密码信息默认为密文，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密码信息，则需要将配置文件中对应的密码修改为明文，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。

仅管理员用户可进行配置导入导出操作。

界面描述

在上方标题栏中，选择“配置”，在左侧导航树中选择“导入导出”，显示“导入导出”界面。



操作步骤

导入配置文件

说明

通过iBMC WebUI的“导入导出”界面导出的配置文件中，密码信息默认为密文。

- 如果使用该文件在本服务器上执行导入操作，不需要针对用户密码重新编辑配置文件。
- 如果使用该文件在其他服务器上执行导入操作，请重新编辑配置文件，将配置文件中对应的密码修改为明文，并删除该行注释符。

1. （可选）编辑配置文件。
   a. 使用文本工具打开待导入的配置文件并找到需要编辑的用户。
   b. 编辑指定用户的密码。
      下面以“mytest”用户为例进行说明，如图3-33所示。将此用户的“PassWord”的值由“******”改为实际的字符串，例如“Info@9000”。

      图 3-33 编辑前的配置文件

   c. 将“PassWord”、“IsUserEnable”、“IsUserLocked”参数前后的注释标识“<!--”和“-->”删除。
      修改后的配置文件如图3-34所示。

      图 3-34 编辑后的配置文件

   d. 保存修改。

2. 在“配置导入”区域中，单击“请选择配置文件”后的  ，选择要上传的配置文件。
3. 单击“上传”。
   上传完成后，“导入状态”一栏显示“导入成功，重启后生效”。
4. 上传成功后，弹出对话框提示以下信息：

导入成功，重启后生效

若选择“稍后重启”，您可以在合适的时间重启iBMC使之生效。若选择“立即重启”，则将立即重启iBMC。

说明

- BIOS配置项导入后，需要重启OS才能生效。
- 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。

导出配置文件

1. 单击“配置导出”区域中的“导出”，设置配置文件导出路径，并开始导出。
   导出完成后，显示“导出成功”。

3.8 系统管理

3.8.1 操作日志

功能介绍

通过该界面可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。

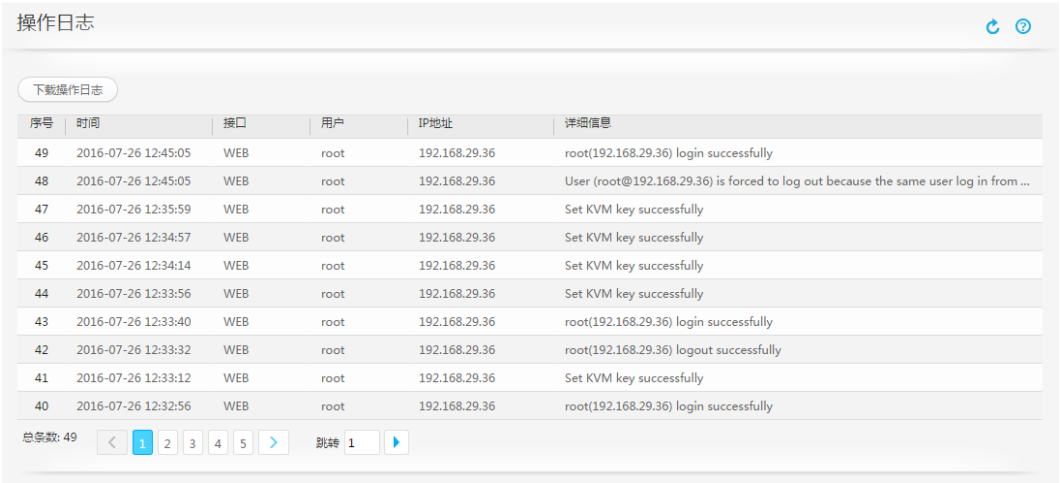
操作日志达到200KB时会自动压缩成1个压缩包，当有新的压缩包生成，会自动删除旧的压缩包。

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。

界面描述

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“操作日志”，显示“操作日志”界面。



参数说明

表 3-59 “操作日志”界面

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。 ● V3服务器跳帽重置IP和**root**密码，V5服务器跳帽重置IP和**Administrator**密码。 ● 部件热插拔。 **说明** iBMC V350及以上版本，iBMC不支持通过跳线恢复默认配置。
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。 ● 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、内存板按钮或电源按钮被按下。 – 接口为LCD或本地串口。 – V3服务器跳帽重置IP和**root**密码，V5服务器跳帽重置IP和**Administrator**密码。 – 部件热插拔。 **说明** iBMC V350及以上版本，iBMC不支持通过跳线恢复默认配置。
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
注：“用户名”和“IP地址”如果不满足上述情况，无法解析时显示为“unknown”。	

操作步骤

查看操作日志

1. 在上方标题栏中选择“系统管理”。
2. 在左侧导航树中，选择“操作日志”。
   右侧显示“操作日志”界面。

下载操作日志

1. 单击“下载操作日志”。
   弹出“保存”窗口。
2. 选择操作日志文件在本地PC上的保存路径。
3. 单击“保存”。
   操作日志文件成功保存到指定的路径。

3.8.2 运行日志

功能介绍

通过该界面，可查看服务器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。

界面描述

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“运行日志”，显示“运行日志”界面。

参数说明

表 3-60 “运行日志”界面

参数	描述
时间	运行错误发生的时间。
级别	运行错误的告警级别。
详细信息	运行错误的详细描述信息。

操作步骤

查看运行日志

1. 在上方标题栏中选择“系统管理”。
2. 在左侧导航树中，选择“运行日志”。
   右侧显示“运行日志”界面。
3. 在“运行日志”界面中，查看当前所有的运行日志。

3.8.3 安全日志

功能介绍

通过使用“安全日志”界面的功能，您可以：

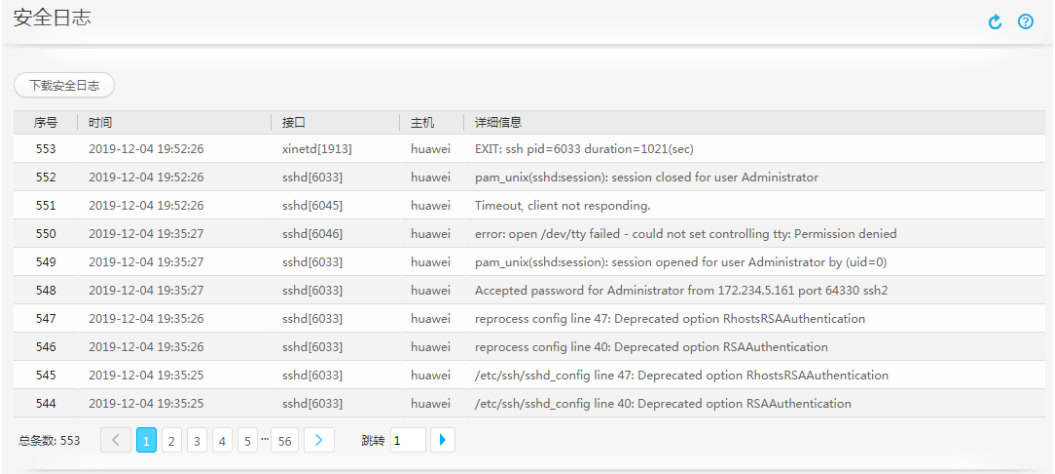
- 查看用户通过串口、SSH接口登录、退出iBMC系统以及设置类操作的日志。
- 查看用户通过SNMP接口执行的查询类和设置类操作的日志。
- 下载安全日志。

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

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“安全日志”，显示“安全日志”界面。



参数说明

表 3-61 “安全日志”区域框

参数	描述
序号	操作发生的顺序，ID越小的操作发生越早。
时间	操作发生的时间。
接口	操作接口。
主机	iBMC系统的主机名。
详细信息	显示用户的登录、退出操作详情。

操作步骤

查看所有日志

1. 在“安全日志”界面下的表格中，查看iBMC系统的所有登录、退出日志。

下载安全日志

1. 在“安全日志”界面中，单击“下载安全日志”。
   弹出“保存”窗口。
2. 选择下载文件在本地PC上的保存路径。
3. 单击“保存”。
   下载文件成功保存到指定的路径。您可以在本地打开文件并查看安全日志。

3.8.4 工作记录

功能介绍

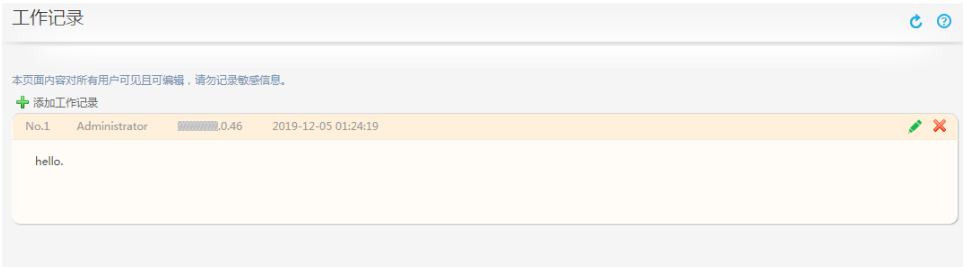
通过使用“工作记录”界面的功能，您可以在本界面记录自己的工作内容，方便以后查看。

说明

- 工作记录单条最大允许输入长度为255，最多20条，超过20条后新增的工作记录将覆盖最早的记录。
- 工作记录的内容是所有用户可见、可修改的。

界面描述

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“工作记录”，显示“工作记录”界面。



操作步骤

添加工作记录

1. 在上方标题栏中选择“系统管理”。
2. 在左侧导航树中，选择“工作记录”。
   右侧显示“工作记录”界面。
3. 单击“添加工作记录”，在弹出的文本框中记录工作内容。
4. 单击“保存”。

修改工作记录

1. 单击“ ”，修改工作记录。
2. 单击“保存”。

删除工作记录

1. 单击“ ”，删除工作记录。
   弹出对话框提示以下信息：
   是否确定执行该操作?
2. 单击“确定”。

3.8.5 在线用户

功能介绍

通过使用“在线用户”界面的功能，您可以查看已登录iBMC系统的用户信息，也可以注销已登录的用户。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

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“在线用户”，显示“在线用户”界面。

参数说明

表 3-62 “在线用户”界面

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。

参数	描述
登录方式	用户登录的方式。 取值范围： ● “GUI”表示用户通过WEB界面登录iBMC系统。 ● “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。仅V5服务器支持此登录方式。
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。
注销	强制其他用户退出登录。

操作步骤

查看在线用户

1. 在上方标题栏中选择“系统管理”。
2. 在左侧导航树中，选择“在线用户”。
   右侧显示“在线用户”界面。
3. 在“在线用户”界面中，查看当前所有登录iBMC系统的用户信息。

注销在线用户

1. 在“在线用户”界面中，单击某行用户信息的“”。
   弹出确认对话框。
2. 单击“确定”。
   成功注销该用户，“在线用户”界面不再显示该用户的相关信息。

3.8.6 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并进行固件升级。

iBMC系统存在主备2个镜像，每次升级只能升级1个镜像，所以iBMC固件升级必须执行2次升级操作。您访问的iBMC界面使用的是主用系统镜像。iBMC固件升级会先对备用镜像进行升级。备用镜像升级完成后，iBMC系统重新启动会注销当前登录的用户，

并自动切换镜像文件到已升级的备用系统镜像。如果系统没有自动切换镜像文件，您可以手动执行切换镜像文件的操作。

须知

- 若iBMC为V256之前版本，使用该界面升级固件（iBMC/CPLD/BIOS）之前，请先重启iBMC。
- 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。
- 在iBMC V312之前版本中，如需要升级主板BIOS和各部件CPLD时，请务必先升级BIOS且升级生效后再升级CPLD，否则可能导致BIOS升级失败，系统异常。
- 升级LCD固件和电源固件无需重新启动服务器；升级以下固件需要重新启动服务器才能生效：
  - BIOS固件
  - 主板CPLD固件
  - 处理器板CPLD固件（RH8100 V3和8100 V5特有固件）
  - 前IO板CPLD固件（RH8100 V3和8100 V5特有固件）
  - 后IO板CPLD固件（RH8100 V3和8100 V5特有固件）
  - 硬盘背板CPLD固件
  - 热插拔PCIe Riser卡CPLD固件

  升级以上固件前，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。
- RH8100 V3或8100 V5服务器在双系统工作模式时，要升级前IO模块的CPLD，需要登录“系统-B”的iBMC来进行升级，要升级后IO模块的CPLD，需要登录“系统-A”的iBMC来进行升级。
- 升级特定硬盘背板CPLD的iBMC版本要求：升级1288H V5、2288H V5、2288C V5或5288 V5服务器的硬盘背板CPLD时，如果当前配置的硬盘背板的部件编码（即P/N编码）为03029JRX、03029JRY、03029JSA、03029TDR、03029TDQ 、03029TDH或03029TDE，请检查iBMC版本是否为V520及以上。如果不是，请将iBMC版本升级到V520及以上。
- 执行升级时，如果需要从iBMC中间版本的以下版本升级到中间版本的以上版本，需要先将iBMC升级到中间版本，然后再升级到目标版本。若升级到中间版本失败，可对iBMC重启后再次尝试。服务器型号与iBMC中间版本关系如表3-63所示。例如，执行升级的服务器是RH1288 V3，需要从iBMC V257以下版本升级到V257以上版本，需要先将iBMC升级到V257版本，然后再升级到目标版本。若升级到V257版本失败，可对iBMC重启后再次尝试。

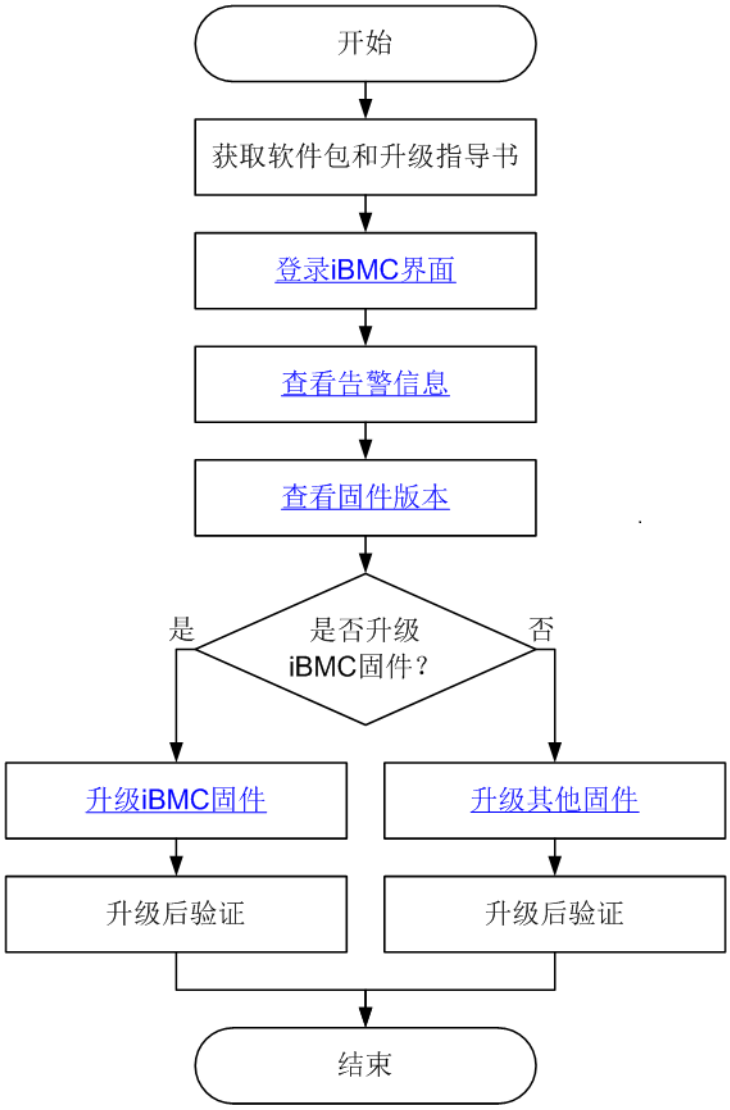
表 3-63 iBMC 中间版本与服务器型号关系表

中间版本	型号
257	RH1288 V3/RH2288H V3/RH5288 V3
260	RH5885H V3

中间版本	型号
262	RH2288 V3
270	RH5885 V3
276	RH8100 V3

升级固件的流程如图3-35所示。

图 3-35 升级固件的流程



界面描述

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“固件升级”，显示“固件升级”界面。

参数说明

表 3-64 “固件升级”界面

参数	描述
固件版本信息	
iBMC主分区镜像版本	iBMC固件主分区镜像的版本号。
iBMC备分区镜像版本	iBMC固件备分区镜像的版本号。
BIOS版本	BIOS固件当前的版本号。
CPLD版本	CPLD固件当前的版本号。
主备分区镜像倒换	将iBMC固件主分区的镜像文件切换到备分区的镜像文件。当系统没有自动切换镜像文件时用户可以执行此操作。 设置方法：单击“主备分区镜像倒换”。
重启iBMC	重新启动iBMC系统使设置生效。 设置方法：单击“重启iBMC”。
固件升级 **说明** ● V3服务器升级iBMC固件时，KVM、截屏和录像功能暂不可用。 ● 在iBMC或SD卡控制器固件升级完成之后，iBMC会自动重启，使升级的固件生效。 ● 如果在OS上电状态时启动BIOS升级，则下次OS下电或重启生效。 ● 升级过程中请勿断电，请勿重启iBMC。 ● V5服务器不支持SD控制器。	

参数	描述
升级文件	固件的升级包名称。升级文件的格式必须为“*.hpm”。 设置方法： 1. 单击  。选择升级包存放在本地PC上的路径。单击“打开”，返回“固件升级”界面。 2. 单击“开始升级”。弹出对话框提示以下信息： 是否确定执行该操作? 3. 单击“确定”，iBMC系统开始执行升级操作。
升级进度	显示固件升级的进度。
升级状态	显示固件升级的状态。

操作步骤

查看固件版本

1. 在上方标题栏中选择“系统管理”。
2. 在左侧导航树中，选择“固件升级”。
   右侧显示“固件升级”界面。
3. 在“固件升级”界面中，查看iBMC、BIOS和CPLD的版本信息。

升级iBMC固件

1. 在“固件升级”界面中，根据表3-64提供的方法，在“升级文件”一行选择升级包的存放路径。
2. 单击“开始升级”。
   弹出对话框提示以下信息：
   是否确定执行该操作?
3. 单击“确定”。
   iBMC系统开始执行升级操作。“升级进度”显示升级操作的进度。
   升级成功后，“升级状态”一行显示以下信息：
   升级完成
4. 重复执行1到3，升级iBMC系统的原主用镜像。

升级其他固件

1. 在“固件升级”界面中，根据表3-64中提供的方法，在“升级文件”一行选择升级包的存放路径。
2. 单击“开始升级”。
   弹出对话框提示以下信息：
   是否确定执行该操作?
3. 单击“确定”。
   iBMC系统开始执行升级操作。“升级进度”显示升级操作的进度。
   升级成功后，“升级状态”一行显示以下信息：
   升级完成

升级BIOS固件成功后，“升级状态”一行显示以下信息：

上传升级文件成功，下次系统下电或重启生效

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。

1. 在“固件升级”界面中，单击“主备分区镜像倒换”。
   弹出对话框提示以下信息：
   您是否要进行主备分区镜像倒换，如果倒换，iBMC将会重启!
2. 单击“确定”。
   将iBMC固件主分区的镜像文件切换为备分区的镜像文件。
   页面将跳转至登录页面并提示以下信息：
   设备正在重启中，请稍等几分钟。
   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。

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。

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：
   是否确定执行该操作?
2. 单击“确定”。将重启iBMC。
   页面将跳转至登录页面并提示以下信息：
   设备正在重启中，请稍等几分钟。
   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。

3.8.7 语言更新

功能介绍

通过使用“语言更新”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iBMC V256及以上版本支持安装和卸载语言包。
- 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。
- 当前仅支持升级和卸载日文和法文语言包。
- 不支持升级或卸载英语和中文语言包。

界面描述

在上方标题栏中，选择“系统管理”，在左侧导航树中选择“语言更新”，显示“语言更新”界面。

参数说明

表 3-65 “语言更新”界面

参数	描述
安装的语言	
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。
语言包版本	显示当前iBMC系统的语言包版本。
点击这里跳转	单击“点击这里跳转”后跳转到“固件升级”页面，可进行升级语言包操作。

操作步骤

查看已安装的语言

1. 在上方标题栏中选择“系统管理”。
   右侧显示“语言更新”界面。
2. 在“语言更新”界面中，查看当前iBMC已安装的语言。

安装或升级语言包

1. 下载待升级的目标语言包（例如“*XXX*-iBMC-LANG-JA-V*XXX*.zip”）。
2. 升级语言包。
   a. 登录iBMC WebUI。
   b. 在导航栏中选择“系统管理 > 固件升级”。
      右侧显示“固件升级”界面。
   c. 在“固件升级”界面中，在“升级文件”一行选择获取的安装包。
   d. 单击“开始升级”。
      弹出对话框提示以下信息：
      是否确认执行该操作?

e. 单击“确定”。

iBMC系统开始执行升级操作。“升级进度”显示升级操作的进度。

升级成功后，“升级状态”一行显示以下信息：

升级完成

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。

卸载语言包

1. 在“语言更新”界面中，勾选需要卸载的语言。
2. 单击“卸载”。

卸载完成后“语言更新”界面将显示“操作成功”提示信息。

3.9 远程控制

功能介绍

通过使用“远程控制”界面的功能，您可以查看远程控制台、虚拟媒体和VNC服务的最大会话数和激活的会话数，也可以使用远程虚拟控制台接入服务器的操作系统进行操作。

说明

仅V5服务器支持VNC服务。

界面描述

在上方标题栏中，选择“远程控制”，在左侧导航树中选择“远程控制”，显示“远程控制”界面。

参数说明

表 3-66 “远程控制”界面

参数	描述
集成远程控制台	

参数	描述
Java集成远程虚拟控制台	Java集成远程虚拟控制台支持以下两种模式： ● 独占模式下只能有1个本地用户或VNC用户通过iBMC连接到服务器操作系统。 ● 共享模式下可以让2个本地用户或5个VNC用户同时通过iBMC连接到服务器操作系统，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。 Java控制台提供功能如下： ● 通过浮动按钮、屏幕缩放按钮、多种鼠标按钮、图像清晰度游标，提供便捷的屏幕显示设定功能。 ● 通过组合键按钮、键盘指示灯、键盘布局按钮，提供输入设备查询和设定功能。 ● 通过电源控制按钮、录像按钮，提供服务器操作系统控制功能。 ● 通过光驱、软驱按钮，提供物理光驱、物理软驱、镜像文件的挂载功能，以及本地文件夹挂载功能。 ● 通过镜像文件制作按钮，提供光驱、软件的镜像文件的制作接口。 **说明** 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。
HTML5集成远程控制台	HTML5集成远程控制台支持以下两种模式： ● 独占模式下只能有1个本地用户或VNC用户通过iBMC连接到服务器操作系统。 ● 共享模式下可以让2个本地用户或5个VNC用户同时通过iBMC连接到服务器操作系统，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。 HTML5控制台提供功能如下： ● 通过浮动按钮、屏幕缩放按钮、多种鼠标按钮、图像清晰度游标，提供便捷的屏幕显示设定功能。 ● 通过组合键按钮、键盘布局按钮，提供输入设备设定功能。 ● 通过电源控制按钮、录像按钮，提供服务器操作系统控制功能。 ● 通过光驱、软驱按钮，提供镜像文件挂载功能，以及本地文件挂载功能。 **说明** 仅V5服务器支持HTML5集成远程控制台。
独立远程控制台	

参数	描述
下载	独立远程控制台是可独立运行的服务器实时桌面登录工具，不依赖浏览器、Java、操作系统的配套关系。若界面中无“下载”按钮，可联系供应商获取。
远程控制台配置	
超时(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。 ● iBMC V328及之后版本，默认超时时间为60分钟。 ● iBMC V328之前版本，默认为不超时。 此参数不允许设置为空。
最大会话	允许使用KVM连接系统的最大用户数量，固定为2。
活跃会话	当前使用KVM连接系统的用户数量。单击活跃会话数，可跳转至“在线用户”页面，查看当前使用KVM连接服务器OS的用户信息。
通信加密	启用数据传输加密功能。KVM数据在客户端与服务器之间传输时采用AES128算法加密。默认未开启KVM加密，出于安全考虑，建议用户开启KVM加密。 设置方法：选中“通信加密”，并单击“保存”。 **说明** 关闭并保存VMM加密后才能关闭KVM加密。
本地KVM使能	设置本地KVM的使能状态。 ● 选中“本地KVM使能”时，可同时使用VGA外接显示器和远程虚拟控制台连接到服务器实时桌面。 ● 未选中“本地KVM使能”时，VGA外接显示器不可用，仅可通过远程虚拟控制台连接到服务器实时桌面。 默认取值：选中“本地KVM使能”。
虚拟键盘、鼠标持续连接	此功能用于设置鼠标、键盘是否持续连接。 ● 选中“虚拟键盘、鼠标持续连接”时，iBMC的虚拟鼠标、键盘将一直连接到业务侧的USB控制器。 ● 未选中“虚拟键盘、鼠标持续连接”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。 默认取值：选中“虚拟键盘、鼠标持续连接”。
虚拟媒体	
最大会话	允许使用远程虚拟控制台的虚拟设备（虚拟光驱、虚拟软驱）的最大用户数量，固定为1。

参数	描述
活跃会话	当前使用远程虚拟控制台的虚拟设备（虚拟光驱、虚拟软驱）的用户数量。单击活跃会话数，可跳转至“在线用户”页面，查看当前使用远程虚拟控制台的虚拟设备（虚拟光驱、虚拟软驱）的用户信息。
通信加密	启用虚拟媒体加密功能。开启KVM加密后才能开启VMM加密。VMM数据在客户端与服务器之间传输时采用AES128算法加密。默认未开启VMM加密，从安全考虑，建议用户开启VMM加密。 **说明** 开启并保存KVM加密后才能开启VMM加密。
VNC服务 通过“VNC服务”可以连接到服务器上的操作系统，并提供对主机服务器的键盘、视频和鼠标的访问权限以执行必要的措施。 **说明** 仅V5服务器支持VNC服务。	
超时(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。 ● iBMC V328及之后版本，默认超时时间为60分钟。 ● iBMC V328之前版本，默认为不超时。 此参数不允许设置为空。
键盘布局	VNC控制的操作系统的键盘布局。 取值范围：“日式键盘”和“美式键盘”。 默认取值：“日式键盘”
VNC密码	用于设置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。 ● 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

参数	描述
确认密码	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。 **说明** 确认VNC密码时，单击“确认”将弹出“请输入您的密码”对话框，此时输入当前iBMC用户的登录密码并确认后，方能成功设置VNC密码。
密码有效期(天)	VNC密码的剩余有效期。
登录规则	是否启用对应的登录规则，VNC用户登录时将受到已选择登录规则的限制。
SSL加密	启用SSL加密。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。 默认取值：选中“SSL加密”
最大会话	允许通过VNC服务登录服务器OS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OS的用户数量。单击活跃会话数，可跳转至“在线用户”页面，查看当前通过VNC服务登录服务器OS的用户信息。

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3-67所示。

说明

- 如果需要使用非中、英、日语的浏览器登录iBMC，则需要将iBMC升级至V260及以上版本，否则可能无法正常显示登录页面。
- 如果Java运行环境不符合要求，可登录该软件的官方网站进行下载。
- 打开远程虚拟控制台时，如果Java运行环境为JRE 1.7或JRE 1.8，显示“应用程序已被阻止”或者“已阻止Java应用程序”，请参考3.10.1 无法启动Java集成远程控制台。

表 3-67 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 9.0～11.0 **说明** HTML5仅支持Internet Explorer 10.0及以上版本的浏览器。	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	

操作系统	浏览器	Java运行环境
	Google Chrome 21.0～44.0	
Windows 8 32位 Windows 8 64位	Internet Explorer 10.0～11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Windows 10 64位	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
Windows 2012 R2 64位	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
Windows 2016 64位	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
Windows Server 2008 R2 64位	Internet Explorer 9.0～11.0 **说明** HTML5仅支持Internet Explorer 10.0及以上版本的浏览器。	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Windows Server 2012 64位	Internet Explorer 10.0～11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0～54.0	
	Google Chrome 21.0～44.0	
Red Hat 6.0 64位	Mozilla Firefox 39.0～54.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
MAC OS X v10.7	Safari 8.0	JRE 1.7 U45 JRE 1.8 U45

操作系统	浏览器	Java运行环境
	Mozilla Firefox 39.0～54.0	JRE 1.8 U144

操作步骤

进入集成远程控制台

说明

在远程虚拟控制台中输入OS或BIOS密码时：

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

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

- 如果您有可信任的证书，可以为iBMC导入信任证书和根证书。有关详细信息，请参考**6.12 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“远程控制”界面中，单击“Java集成远程控制台(共享)”、“Java集成远程控制台(独占)”、“HTML5集成远程控制台(独占)”或“HTML5集成远程控制台(共享)”链接。

  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。选择独占模式方式进入实时桌面后，“诊断 > 屏幕截图”界面中的“手动截图”区域框中的“屏幕截图”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：“https://IPaddress/remoteconsole”（推荐登录方式。）
  - 方式二：“https://IPaddress/kvmvmm.asp”
  - 方式三：“https://IPaddress/bmc/pages/remote/kvm.php”
  - 方式四：“https://IPaddress/login.html?redirect_type=1”

  说明

  “IPaddress”为iBMC管理网口的IP地址。

  弹出登录界面：

  a. 选择界面语言。
  b. 输入用户名和密码。

     V3服务器的系统提供一个管理员用户组的缺省用户“root”，缺省密码为“Huawei12#$”；V5服务器的系统提供一个管理员用户组的缺省用户“Administrator”，缺省密码为“Admin@9000”。
  c. 在“域名”下拉列表中，选择“这台iBMC”或“LDAP用户域”。
  d. 单击“登录”，即可跳转至“Java集成远程控制台(独占)”或“HTML5集成远程控制台(独占)”。

查看会话数量

1. 在上方标题栏中选择“远程控制”。
   右侧显示“远程控制”界面。
2. 在“远程控制”界面中，查看远程控制台、虚拟媒体和VNC服务的最大会话数和激活的会话数。
3. 单击活跃会话数，跳转至“在线用户”页面，查看当前登录服务器OS的用户信息。

配置远程控制台

1. 在“远程控制”界面的“远程控制台配置”区域框中，根据参数说明提供的信息进行配置。
   相关参数的详细信息请参考**表3-66**。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

启用虚拟媒体通信加密

1. 在“远程控制”界面中，选中“虚拟媒体 > 通信加密”右侧的单选框。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

配置VNC服务

1. 在“远程控制”界面中的“VNC服务”区域框设置VNC服务的参数。
   相关参数的详细信息请参考**表3-66**。
2. 单击“保存”。
   显示“操作成功”表示完成设置。

3.9.1 Java 远程虚拟控制台

功能介绍

通过使用Java远程虚拟控制台提供的功能，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。

  说明

  本地PC的媒体可以是本地的软驱或光驱，也可以是保存在本地PC上或网络驱动器上的软盘或光盘的镜像文件。

“KVM”窗口中的按钮及其作用如**表3-68**所示。

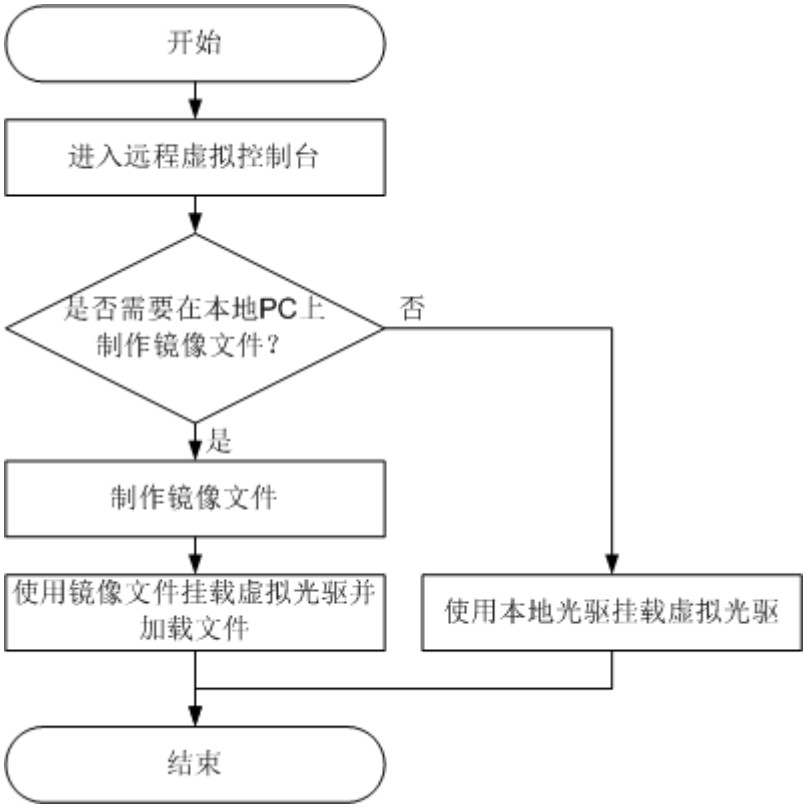
表 3-68 按钮说明

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时，工具栏才会出现该按钮。
	“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时，工具栏才会出现该按钮。
	“返回”按钮。表示返回合适的屏幕显示服务器的实时桌面。 **说明** 只有全屏显示服务器的实时桌面时，工具栏中才会出现该按钮。
	“控制”按钮。表示控制服务器电源。操作包括： • 上电 • 强制下电 • 下电 • 强制重启 • 强制下电再上电
	“录像”按钮。表示对远程实时操作进行录像。
	“鼠标控制”按钮。表示控制服务器鼠标。操作包括： • 鼠标加速 加速服务器实时桌面上的鼠标，使其与本地PC上的鼠标同步。 **说明** 低于SUSE 12版本的SUSE操作系统不支持鼠标加速功能。 • 单鼠标 隐藏本地PC上的鼠标，只显示服务器实时桌面上的鼠标。 • 键鼠复位 模拟插拔USB键盘和USB鼠标，服务器实时桌面上的键盘鼠标出现异常停滞时单击此按钮可以恢复。 默认的操作：鼠标加速 **说明** 鼠标加速和单鼠标均未勾选时，服务器实时桌面鼠标和本地PC鼠标同时显示，且服务器实时桌面鼠标不跟随本地PC鼠标。

按钮	说明
	“光驱”按钮。表示选择并使用虚拟光驱。
	“软驱”按钮。表示选择并使用虚拟软驱。
	“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。
图像清晰度	“图像清晰度”游标标签。表示调节远程实时图像的清晰度。
	“Num Lock”（数字键盘开关）键的指示灯。表示当前服务器上“Num Lock”键的指示灯状态。
	“Caps Lock”（键盘大写锁定）键的指示灯。表示当前服务器上“Caps Lock”键的指示灯状态。
	“Scroll Lock”（键盘滚动锁定）键的指示灯。表示当前服务器上“Scroll Lock”键的指示灯状态。进入Linux字符模式，如果按下了Ctrl+s（大多数情况下属于误摁），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。
	“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3-36所示。

图 3-36 使用流程



界面描述

在上方标题栏中选择“远程控制”，在“远程控制”界面中单击“Java集成远程控制台(共享)”或“Java集成远程控制台(独占)”链接，弹出“KVM”窗口。

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。

各区域的功能介绍如表3-69所示。

图 3-37 KVM 窗口

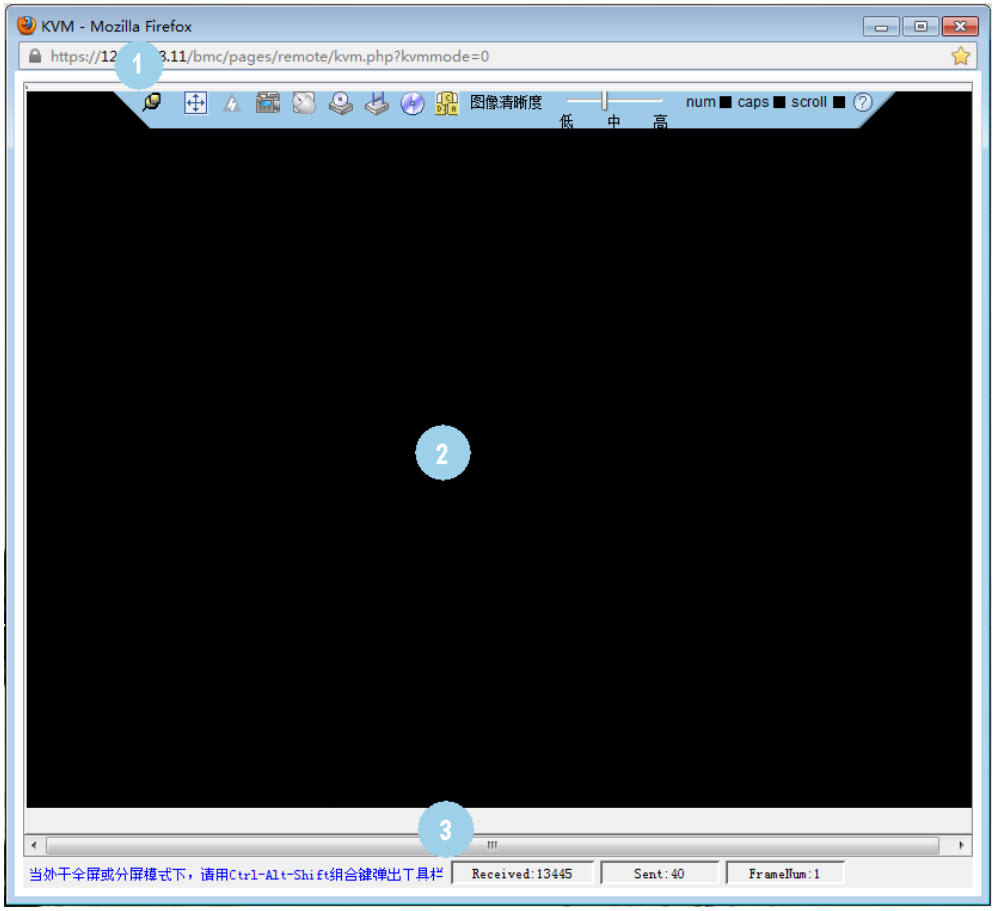


表 3-69 KVM 界面

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。

操作步骤

发送特殊组合键

1. 在“KVM”界面中，单击工具栏上的  。
   弹出组合键窗口。

2. 根据表3-68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

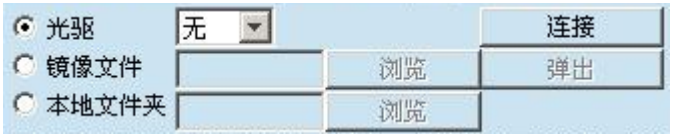
如果您需要自定义组合键，请在“自定义”后的文本框中依次输入按键，然后单击“发送”。

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。

1. 在“KVM”界面中，单击工具栏上的  。
   弹出如图3-38所示的界面。

图 3-38 挂载虚拟光驱



2. 选中“光驱”单选按钮。
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:”。
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。

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。

1. 在“KVM”界面中，单击工具栏上的  。
   弹出如图3-38所示的界面。
2. 选中“镜像文件”单选按钮。
3. 单击“浏览”。
   弹出“打开”窗口。
4. 选择本地PC上存放的光盘镜像文件，单击“打开”。
   返回如图3-38所示的界面。
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。

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。

1. 在“KVM”界面中，单击工具栏上的。
   弹出如图3-39所示的界面。

   图 3-39 挂载虚拟软驱

2. 选中“软驱”单选按钮。
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:”。
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。
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。

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。

1. 在“KVM”界面中，单击工具栏上的。
   弹出如图3-39所示的界面。
2. 选中“镜像文件”单选按钮。
3. 单击“浏览”。
   弹出“打开”窗口。
4. 选择本地PC上存放的软盘镜像文件，单击“打开”。
   返回如图3-39所示的界面。
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。

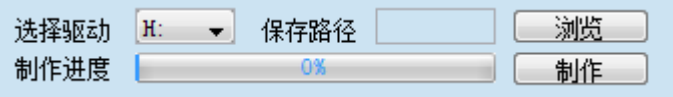
制作镜像文件

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。

1. 在“KVM”界面中，单击工具栏上的。
   弹出如图3-40所示的界面。

   图 3-40 制作镜像文件

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。
3. 单击“浏览”。弹出“保存”窗口。
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。
5. 单击“保存”。
   返回如图3-40所示的界面。
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。

挂载虚拟文件夹

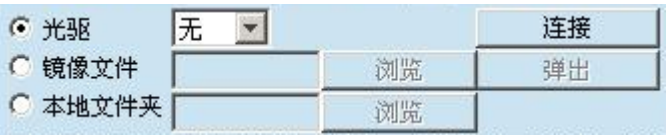
本操作将本地PC上的文件夹挂载到服务器，使服务器系统可以以只读方式访问本地文件夹。

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。

1. 在“Remote Control”界面中，单击工具栏上的。
   弹出如图3-41所示的界面。

   图 3-41 挂载虚拟文件夹

2. 选中“本地文件夹”单选按钮。
3. 单击“浏览”。
   打开本地文件夹选择窗口。
4. 选择要挂载的本地文件夹，单击“打开”。
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。

为服务器上电

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。
2. 单击“是”。
   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。

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“电源与能耗 > 电源控制”，详见3.6.1 电源控制。

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。
2. 单击“是”。
   服务器开始下电。

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“电源与能耗 > 电源控制”，详见iBMC用户指南的“电源控制”章节。

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。
2. 单击“是”。
   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。

键鼠复位

本操作模拟插拔USB键盘和USB鼠标。

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。
2. 单击“是”。
   服务器开始执行USB复位操作。

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视频录像。

1. 在“KVM”界面中，单击工具栏上的  。
   弹出“选择一个选项”对话框。
2. 单击“是”。
   弹出“保存”窗口。
3. 选择将要录制的视频文件在PC上的保存路径，并在“文件名：”文本框中输入视频文件的名称。
4. 单击“保存”。
   返回“KVM”界面并开始录制视频。
5. 录制完成后，单击  。
   弹出“选择一个选项”对话框。
6. 单击“是”。
   视频文件被保存到指定的路径。
   录制的视频文件格式为“*.rep”。可在“录像回放”界面中播放视频文件。

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。

1. 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。
2. 单击“是”。
   “KVM”界面中只显示实时桌面上的鼠标。

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。

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。
2. 单击“是”。
   同步本地PC与服务器的鼠标。

3.9.2 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。

说明

仅V5服务器支持HTML5集成远程控制台。

- 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。

  说明

  本地PC的媒体可以是本地的软驱或光驱，也可以是保存在本地PC上或网络驱动器上的软盘或光盘的镜像文件。

“KVM”窗口中的按钮及其作用如表3-70所示。

表 3-70 按钮说明

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

按钮	说明
	“系统启动项”按钮。表示设置操作系统的第一启动设备。操作包括： ● 未配置：表示不设置第一启动设备，按BIOS中设置的默认方式启动操作系统。 ● 硬盘：表示强制从硬盘启动系统。 ● 光驱：表示强制从CD/DVD启动系统。 ● 软驱/可拔插移动设备：表示强制从软驱或可拔插移动设备启动系统。 ● PXE：表示强制从预启动执行环境（PXE，Pre-boot Execution Environment）启动系统。 ● BIOS设置：表示服务器启动后直接进入BIOS菜单中。
	“键盘组合键”按钮。表示发送或自定义特殊组合键。该窗口中的组合键及其含义包括： ● Alt+Tab：在打开的项目中进行切换。 ● Ctrl+Esc：显示或收起“开始”菜单。 ● Ctrl+Shift：切换输入法。 ● Ctrl+Space：开启或关闭输入法。 ● Ctrl+Alt+Del：锁定操作系统界面、注销用户、更改密码和打开任务管理器、重新启动服务器等。
	“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。
	“软驱”按钮。表示选择并使用虚拟软驱。
	“录像”按钮。表示对远程实时操作进行录像。

按钮	说明
	“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。 **说明** ● 仅iBMC V298及以上版本支持选择客户端的键盘类型。 ● iBMC V350及以上版本支持强制指定键盘类型为意式键盘。
	“帮助”按钮。表示查看KVM页面联机帮助。
	“图像清晰度”游标标签。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“远程控制”，在“远程控制”界面中选择“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。

各区域的功能介绍如表3-71所示。

图 3-42 KVM 窗口

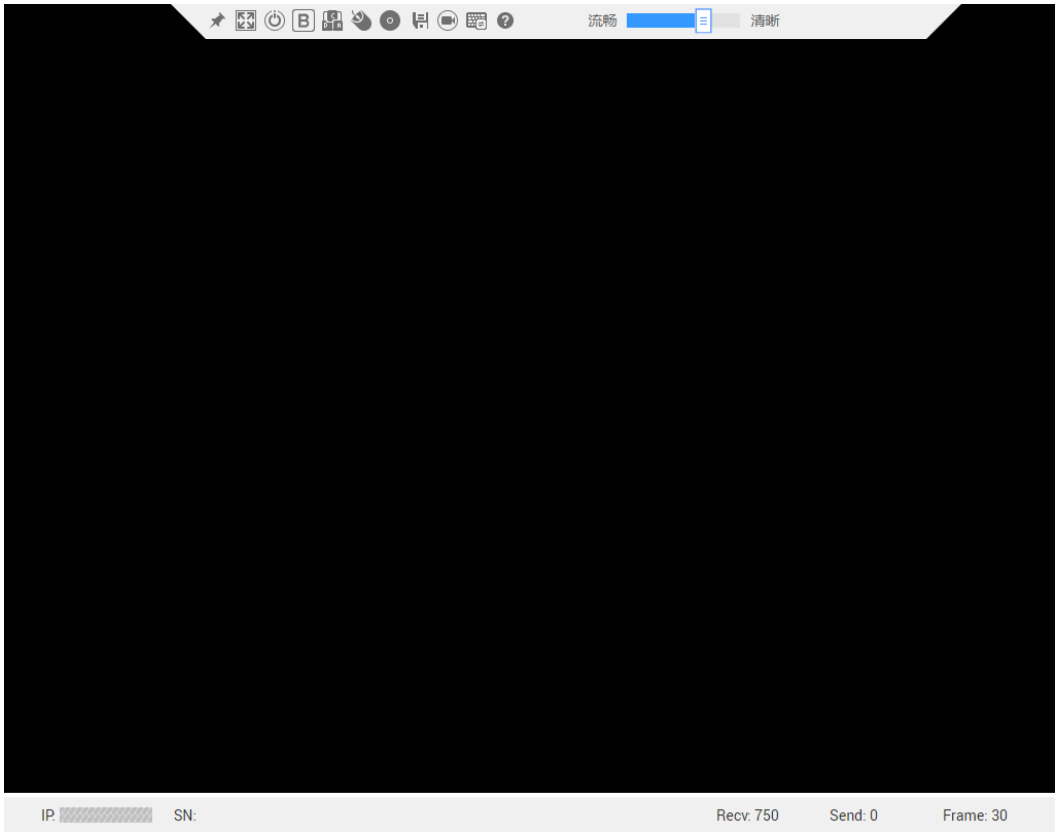


表 3-71 KVM

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

在“KVM”界面中，单击工具栏上的  ，在快捷菜单中选择“上电”。

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。

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“电源与能耗 > 电源控制”，详见iBMC用户指南的“电源控制”章节。

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“正常下电”。

服务器开始下电。

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“电源与能耗 > 电源控制”，详见iBMC用户指南的“电源控制”章节。

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”。

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。

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3-70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3-70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

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。

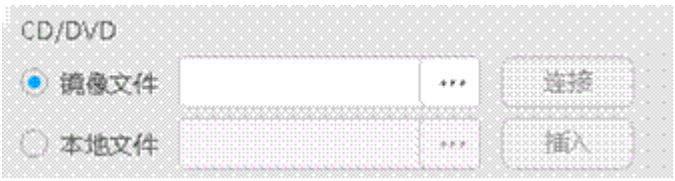
通过虚拟光驱挂载镜像文件

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3-43的界面。

图 3-43 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3-43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

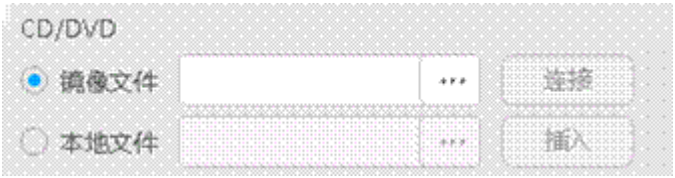
挂载本地文件

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3-44的界面。

图 3-44 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3-44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。

步骤1 在“KVM”界面中，单击工具栏上的  。

弹出如图3-45所示的界面。

图 3-45 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3-45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视频录像。

录制的视频文件格式为“*.rep”。可在“录像回放”界面中播放视频文件和对视频进行截图。

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  。

视频文件将自动被下载并保存到本地PC。

录制的视频文件格式为“*.rep”。可在“录像回放”界面中播放视频文件和对视频进行截图。

----结束

3.10 远程虚拟控制台异常问题帮助

3.10.1 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或者JRE与iBMC不兼容。

解决方案

步骤1 确认是否已安装iBMC支持的JRE版本。

iBMC支持的JRE版本为：JRE 1.7/JRE 1.8。

- 是，执行**步骤3**。
- 否，执行**步骤2**。

步骤2 安装iBMC支持的JRE版本。

安装JRE 1.7或1.8，执行**步骤3**。

步骤3 修改Java安全配置。

1. 查看客户端Java版本。
   在Windows的cmd或Linux的终端中输入：**java -version**。
2. 进入Java控制面板。
   - Windows：通过“控制面板”进入。
   - Linux：
     i. 打开终端。
     ii. 进入Java安装目录（例如：/usr/java/jre1.7/bin）。
     iii. 运行“ControlPanel”。
3. 修改Java安全配置。
   - 如果java版本为JRE 1.7
     i. 在“java控制面板”，将安全级别调为“中”。
     ii. 单击“确定”后并重启浏览器。
   - 如果java版本为JRE 1.8
     i. 打开“java控制面板 > 安全”“编辑站点列表”。
     ii. 在列表中添加iBMC的IP地址及其端口号（默认为443），例如“https://192.168.2.10:443/”。
     iii. 保存并重启浏览器。
     iv. 重新登录远程控制台，在此过程中忽略一切安全提示。

----结束

3.10.2 Google Chrome 不支持该插件

问题现象

问题描述	可能原因
在Google Chrome下启动远程虚拟控制台，显示不支持此插件。	Google Chrome没有开启或不支持NPAPI插件。

说明

启动远程虚拟控制台需要运行JAVA插件，此插件遵守NPAPI。在使用Google Chrome启动远程虚拟控制台之前，请确认NPAPI已开启，否则会出现启动异常。

解决方案

- 手动启用NPAPI插件。

  Google Chrome 42/43/44，需要手动启用NPAPI插件。

  启用方法：

  - 在Google Chrome地址栏输入：**chrome://flags/#enable-npapi**
  - 重启Google Chrome。
- 选择其他浏览器启动远程虚拟控制台。

  Google Chrome 45及以上版本将不再支持NPAPI，建议使用其他浏览器启动远程虚拟控制台。

----结束

3.10.3 Linux 系统下 Firefox 插件版本过旧无法启动远程虚拟控制台

问题现象

问题描述	可能原因
在Linux系统下，使用Firefox启动远程虚拟控制台，显示需要更新插件。	插件版本过旧，导致无法启动。

解决方案

步骤1 进入Firefox插件目录。

例如：cd /usr/lib/mozilla/plugins。

步骤2 建立软连接到java安装目录下的libnpjp2.so。

例如：ln -s /usr/java/jre1.6.0_25/lib/libnpjp2.so。

步骤3 重启Firefox。

----结束

3.10.4 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“虚拟键盘、鼠标持续连接设置”。

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”界面的“虚拟键盘、鼠标持续连接设置”是否开启。

- 是 => **步骤4**
- 否 => **步骤3**

步骤3 使能“虚拟键盘、鼠标持续连接设置”，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 请联系技术支持工程师处理。

----结束

3.10.5 只能看到 Java web start 图标无法打开 KVM

问题现象

问题描述	可能原因
打开远程虚拟控制台时，只能看到Java Web的启动界面。启动界面消失后，KVM未打开。	Java web start方式启动KVM时，需要启用java的临时文件设置。客户端未设置此配置项。

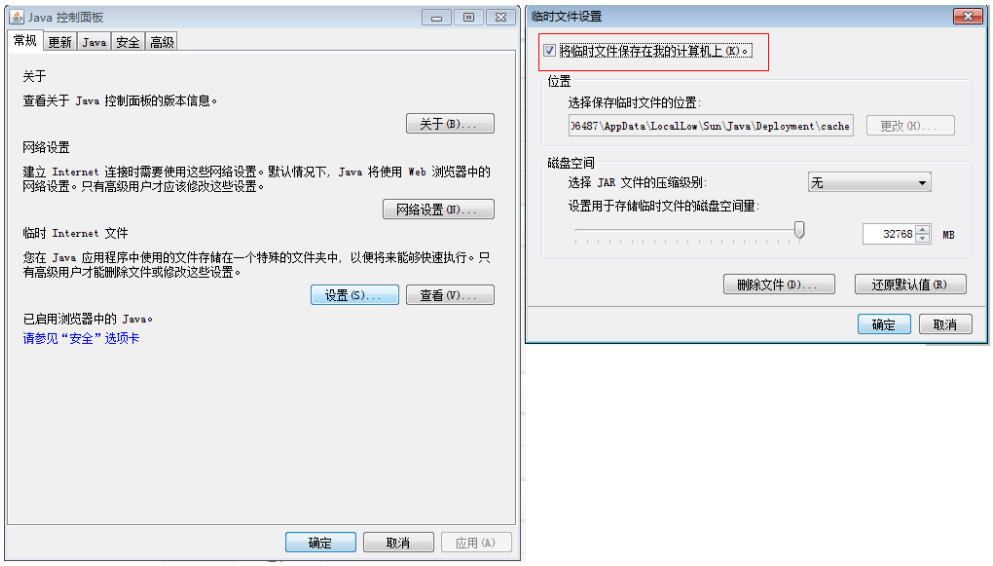
解决方案

步骤1 在客户端控制面板中打开Java控制面板。

步骤2 单击“常规”页签中的“设置”。

步骤3 在“临时文件设置”窗口中勾选“将临时文件保存在我的计算机上”并单击“确定”，如图3-46所示。

图 3-46 设置历史文件处理方式



步骤4 保存退出后重启浏览器。

----结束

3.10.6 打开 KVM 后显示非法用户

问题现象

问题描述	可能原因
1. 打开远程虚拟控制台时，出现Java web start图标。 2. 图标消失后，经过很长时间才会打开KVM。 3. 打开KVM后，显示“非法用户”。	KVM启动时校验需要在联网环境下进行，未联网时可能会出现校验超时，导致启动失败。

解决方案

方案一:

将使用KVM的客户端连接到互联网。

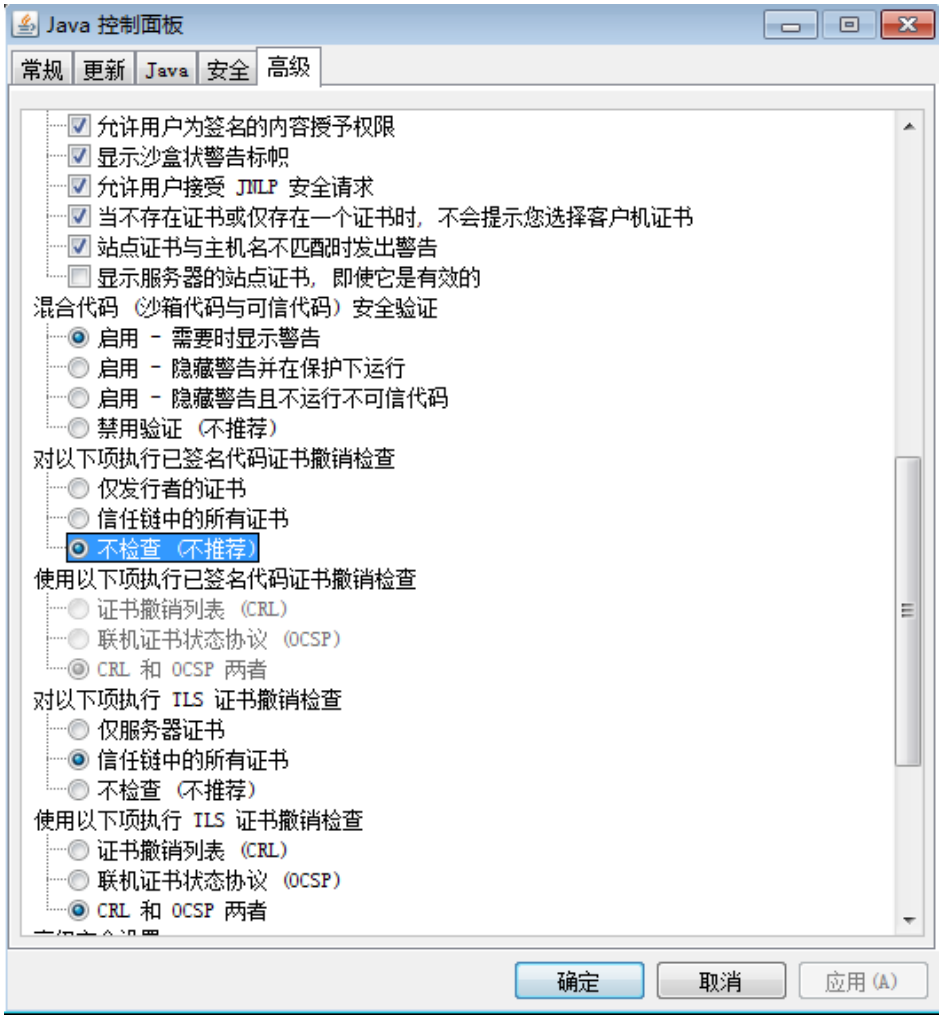
方案二:

重新设置Java参数。

1 在客户端控制面板中打开Java控制面板。

2 勾选“高级”页签中“对以下项执行已签名代码证书撤销检查”的“不检查”，如图3-47所示。

图 3-47 修改 Java 参数



3 保存退出后重启浏览器。

----结束

3.10.7 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“配置 > 服务配置”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 请联系技术支持工程师处理。

----结束

3.10.8 打开 HTML5 集成远程控制台后显示设置信任证书超时

问题现象

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

解决方案

步骤1 打开iBMC WebUI中的“配置 > SSL证书”页面，在“服务器证书信息”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 请联系技术支持工程师处理。

----结束

3.11 一键收集信息说明

表 3-72 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
3rdDump	-	error_log	Apache错误日志
		access_log	Apache访问日志
		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
AppDump	Lcd	Lcd_dfl.log	LCD模块管理对象的信息
	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	服务器上配置的扣卡信息
	BMC	BMC_dfl.log	iBMC模块管理对象的信息
		fruinfo.txt	FRU电子标签信息
		net_info.txt	网口配置信息

目录	子目录	文件名	文件内容说明
		psu_info.txt	服务器上配置的电源信息
	PowerMgnt	PowerMgnt_dfl.log	PowerMgnt模块管理对象的信息
	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
		options0.ini	BIOS配置信息对照表 **说明** 仅V3服务器支持收集此日志信息。
		changed0.ini	BIOS配置变更项列表 **说明** 仅V3服务器支持收集此日志信息。
		display0.ini	BIOS显示信息对照表 **说明** 仅V3服务器支持收集此日志信息。
		registry.json	BIOS的注册文件，显示所有的BIOS项信息 **说明** 仅V5服务器支持收集此日志信息。
		currentvalue.json	当前设置的BIOS项 **说明** 仅V5服务器支持收集此日志信息。
		setting.json	通过redfish设置但尚未生效的BIOS项 **说明** 仅V5服务器支持收集此日志信息。

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 **说明** 仅V5服务器支持收集此日志信息。
	discovery	discovery_dfl.log	Discovery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
	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
	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
	sensor_alarm	sensor_alarm_dfl.log	Sensor_Alarm模块管理对象的信息
		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

目录	子目录	文件名	文件内容说明
		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
	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	StorageMgnt模块管理对象的信息
	redfish	redfish_dfl.log	Redfish模块管理对象的信息

目录	子目录	文件名	文件内容说明
		component_uri.json	部件URI列表
	dfm	dfm.log	DFM模块管理对象的信息
		dfm_debug_log dfm_debug_log.1	PME框架调试日志
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
		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

目录	子目录	文件名	文件内容说明
		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

目录	子目录	文件名	文件内容说明
		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
		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
		ipinfo.sh	iBMC网络配置脚本
		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

目录	子目录	文件名	文件内容说明
		sfcb	CIM pam登录规则
		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
		cdev_drv_info	字符设备驱动信息
		veth_drv_info	虚拟网卡驱动信息
LogDump	-	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	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故障日志

目录	子目录	文件名	文件内容说明
		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
		ipmi_debug_log ipmi_debug_log.tar.gz	IPMI模块日志
		ipmi_mass_operation_log ipmi_mass_operation_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	电源黑匣子日志
OSDump	-	systemcom.tar	SOL串口信息
		img*.jpeg	业务侧最后一屏图像

目录	子目录	文件名	文件内容说明
		*.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
DeviceDump	i2c_info	*_info	I2C设备的寄存器/存储区信息
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

目录	子目录	文件名	文件内容说明
		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_utilise	服务器内存利用率
		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	维护日志
		md_so_maintenance_log.tar.gz	维护日志打包
		md_so_operate_log	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_operate_log.tar.gz	操作日志打包
		md_so_strategy_log	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
		md_so_strategy_log.tar.gz	策略日志打包
		memory_webview.dat	管理对象运行信息

目录	子目录	文件名	文件内容说明
		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_permanent.ini.sha256	完整性校验码
		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

目录	子目录	文件名	文件内容说明
		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
		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

目录	子目录	文件名	文件内容说明
		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.sha256	完整性校验码
		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

目录	子目录	文件名	文件内容说明
		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，*.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。）	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
		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

目录	子目录	文件名	文件内容说明
		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.bak.md5	完整性校验码
		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

目录	子目录	文件名	文件内容说明
		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
		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

目录	子目录	文件名	文件内容说明
		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
		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

目录	子目录	文件名	文件内容说明
		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
		User_login.bak	login pam登录规则
		User_login.bak.md5	完整性校验码

目录	子目录	文件名	文件内容说明
		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.md5	完整性校验码
		eo.db_backup	SEL数据库
		eo.db.md5_backup	完整性校验码

4 命令行介绍

4.1 命令行说明
4.2 登录命令行
4.3 iBMC命令
4.4 Trap命令
4.5 Syslog命令
4.6 服务器命令
4.7 系统命令
4.8 用户管理命令
4.9 NTP命令
4.10 指示灯命令
4.11 风扇命令
4.12 传感器命令
4.13 电源命令
4.14 U-Boot命令
4.15 SOL命令

4.1 命令行说明

4.1.1 格式说明

iBMC管理软件常用命令有以下2类：

- 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考**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
      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>
    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 inforamtion
    ldinfo                   Deprecated. Please use 'ipmcget -t storage ...' to get more inforamtion
    pdinfo                   Deprecated. Please use 'ipmcget -t storage ...' to get more inforamtion
    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
    storage                  Configure storage device
    config                   Operate configuration
    vmm                      Operate virtual media
    certificate              Operate certificate
    sol                      Operate SOL
    securityenhance          Operate security enhance

  -d <dataitem>
    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
    ipconfig                Set ip address mask gateway
    ipmode                    Set ip mode
    gateway                   Set gateway
    ipaddr6                 Set ipv6 address
    ipmode6                   Set ipv6 mode
    gateway6                  Set ipv6 gateway
    ipv6config              Set ipv6 fix 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 ...'.
    psuworkmode               Set PSU work mode
```

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
    ipconfig                Set ip address mask gateway
    ipmode                    Set ip mode
    gateway                   Set gateway
    ipaddr6                 Set ipv6 address
    ipmode6                   Set ipv6 mode
    gateway6                  Set ipv6 gateway
    ipv6config              Set ipv6 fix 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 ...'.
psuworkmode                Set PSU work mode
```

4.2 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：

- “ftp”：系统内部网络运行ftp服务时使用。
- “root”：系统运行app进程时使用。
- “sshd”：系统运行ssh服务时使用。
- “nobody”：系统运行vsftpd进程时使用。
- “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。

说明

- 此处关于系统默认用户“root”的说明仅适用于V5服务器。
- 此处关于系统默认用户“ftp”和“nobody”的说明仅适用于V3服务器。
- 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。

4.2.1 通过 BIOS 修改 iBMC 默认用户密码

须知

- V3服务器BIOS系统的默认密码为“Huawei12#$”，V5服务器BIOS系统的默认密码为“Admin@9000”。
- BIOS系统只能修改默认iBMC用户的密码。V3服务器的iBMC默认用户为**root**，默认密码为**Huawei12#$**；V5服务器的iBMC默认用户为**Administrator**，默认密码为**Admin@9000**。
- 通过BIOS系统设置的iBMC默认用户密码最大长度为16个字符。
- 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。
- 如果iBMC Web中“配置 > 系统配置”页面的“设置业务侧用户管理使能状态”设置为关闭，BIOS的“Server Mgmt”页面中的“BMC User Name”显示为NA，此时不能通过BIOS修改iBMC的默认用户密码。

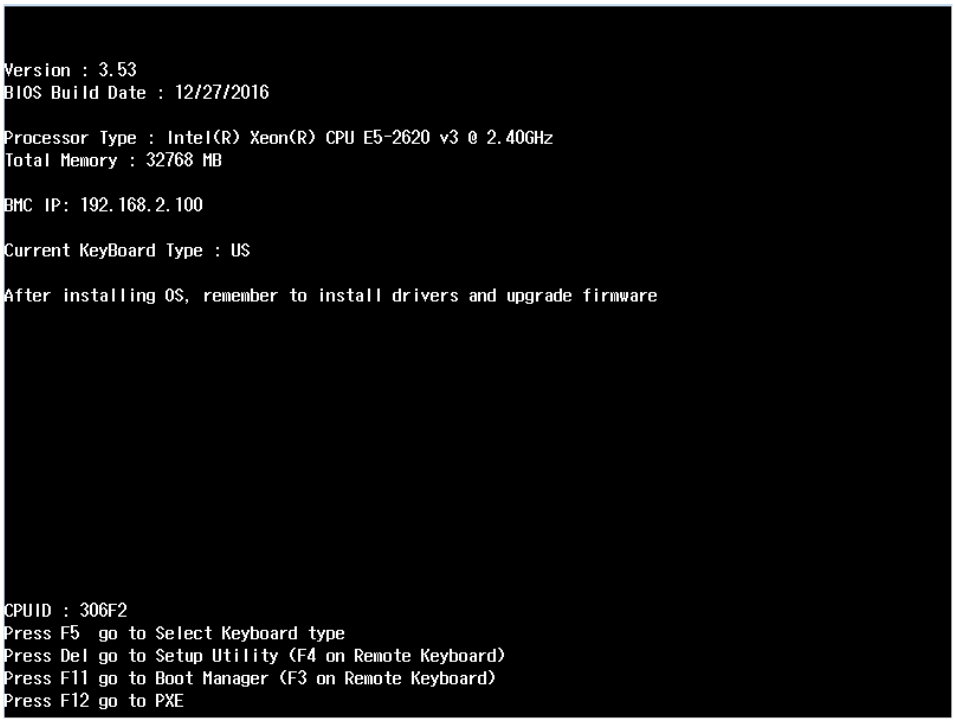
Grantley 平台下操作

不同平台的BIOS界面不同，下面以Grantley平台为例进行介绍。

步骤1 重启服务器。

步骤2 服务器重启时，当出现如下界面时，重复按“Delete”。进入BIOS界面

图 4-1 BIOS 启动界面

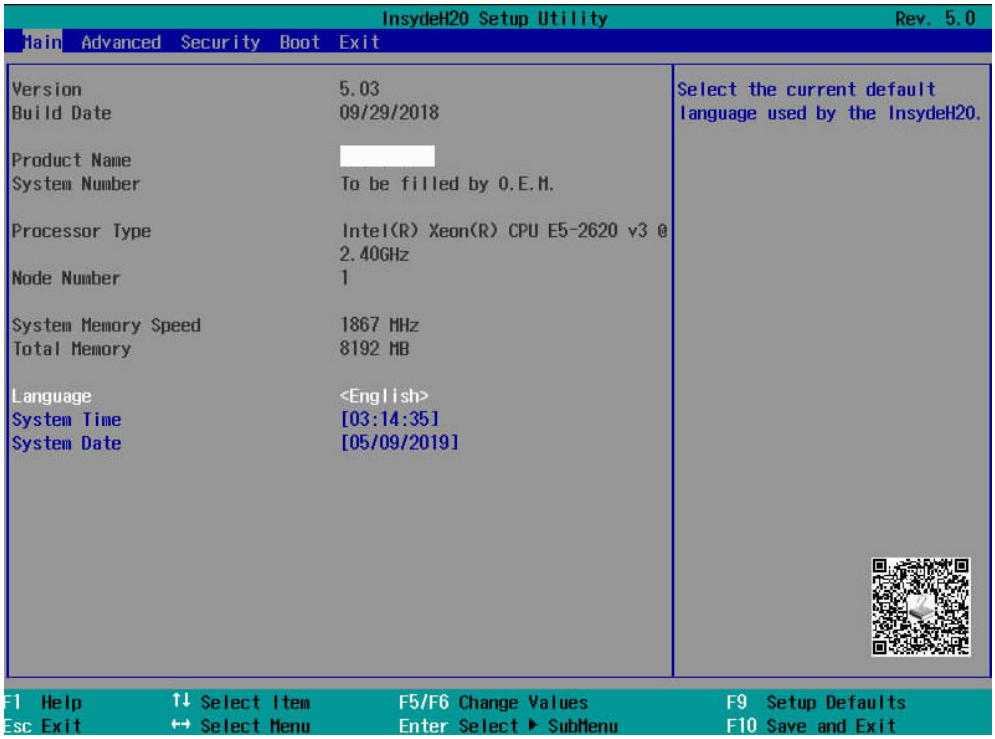


步骤3 如果在启动过程中出现输入密码对话框，请在对话框中输入BIOS密码，如图4-2所示。

图 4-2 输入密码

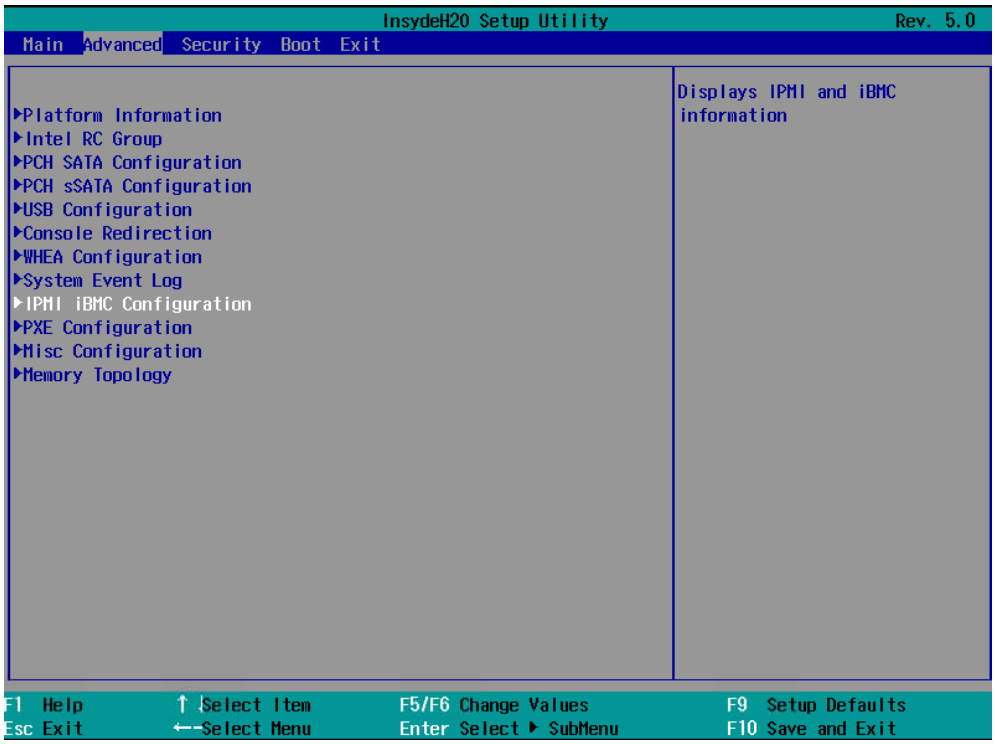
进入BIOS，如图4-3所示。

图 4-3 BIOS Main 界面



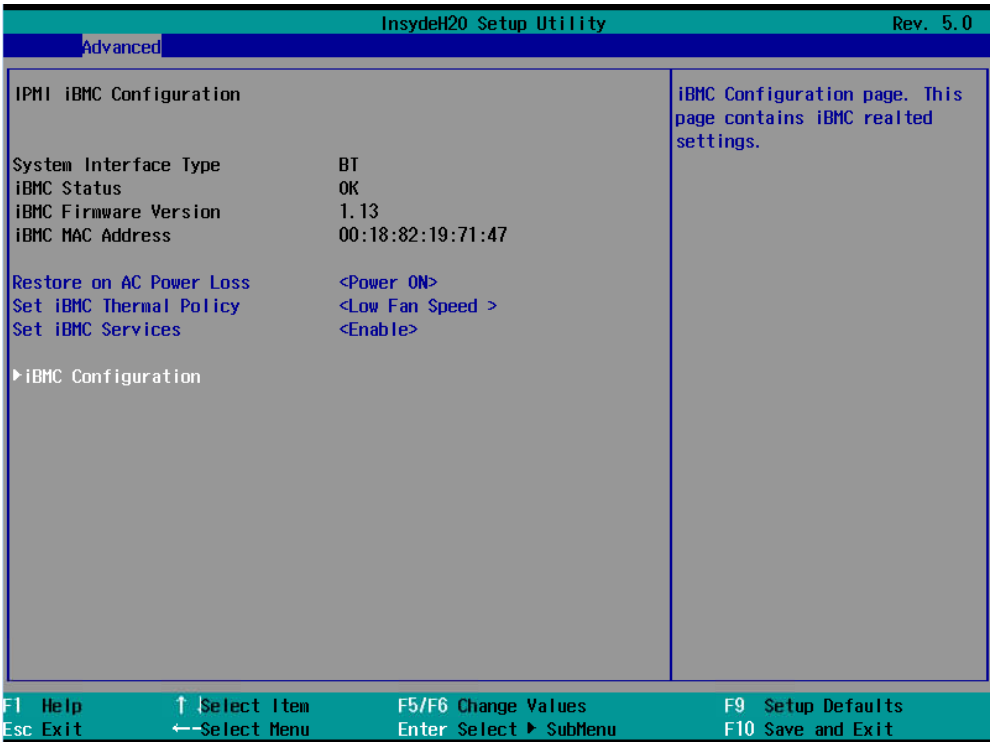
步骤4 用方向键选择“Advanced”页签，如图4-4所示。

图 4-4 BIOS Advanced 界面



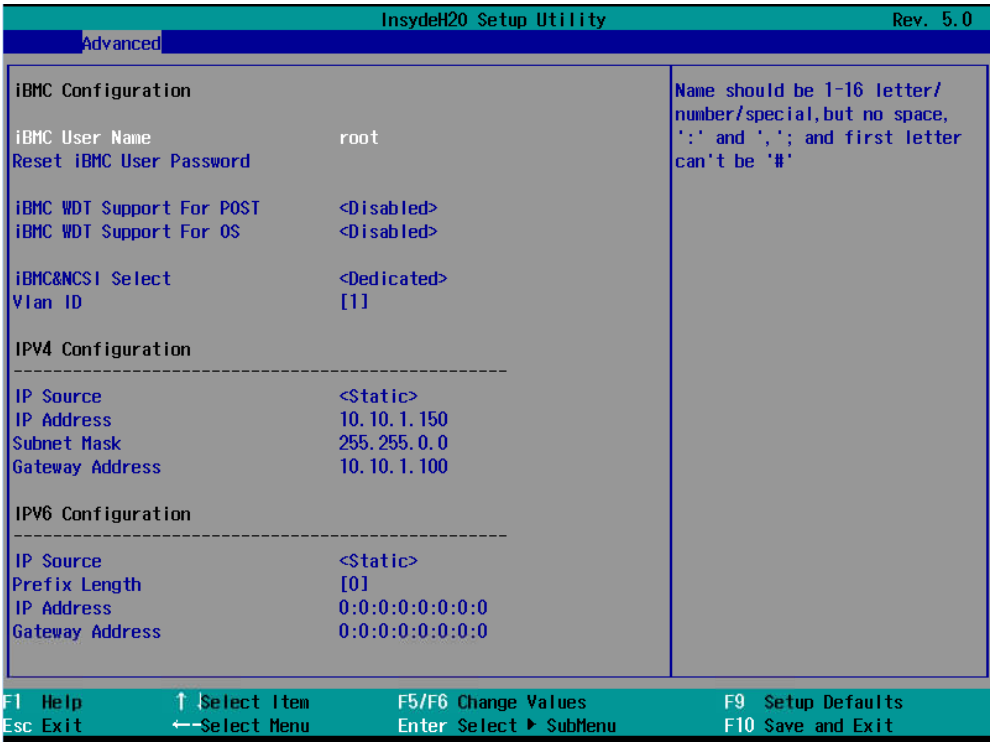
步骤5 在“Advanced”界面，用方向键选择“IPMI iBMC Configuration”界面，按“Enter”，如图4-5所示。

图 4-5 “IPMI iBMC Configuration”界面



步骤6 在“IPMI iBMC Configuration”界面，用方向键选择“iBMC Configuration”界面，按“Enter”，如图4-6所示。

图 4-6 “iBMC Configuration”界面



该界面中显示服务器的IP地址信息。

步骤7 选择“Reset iBMC User Password”，按“Enter”。

弹出“Reset iBMC User Password”对话框。

步骤8 输入iBMC用户密码，按“Enter”。

- 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。
- 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。
- 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

- V3服务器不支持弱口令检查规则。
- V5服务器的默认密码“Admin@9000”在弱口令字典中。

步骤9 重复输入设置的密码，按“Enter”。

弹出“Changes have been saved”对话框。

步骤10 按“Enter”。

保存配置。

----结束

Brinkland 平台下操作

不同平台的BIOS界面不同，下面以Brinkland平台为例进行介绍。

步骤1 重启服务器。

说明

不同配置下，服务器启动时间不同。满配时重启时间为20分钟，请耐心等待。

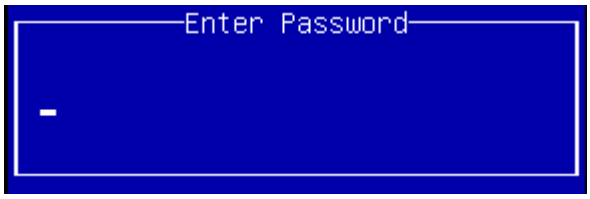
步骤2 在启动过程中，根据界面提示信息按“Del”。进入BIOS设置界面。

步骤3 如果在启动过程中出现输入密码对话框，请在对话框中输入密码，如图4-7所示。

说明

- 第一次进入后请立即修改密码，为提高安全性，建议定期修改BIOS密码。
- 如果连续三次输入错误的BIOS密码，BIOS会锁定，可按“Ctrl+Alt+Del”重启BIOS解锁。

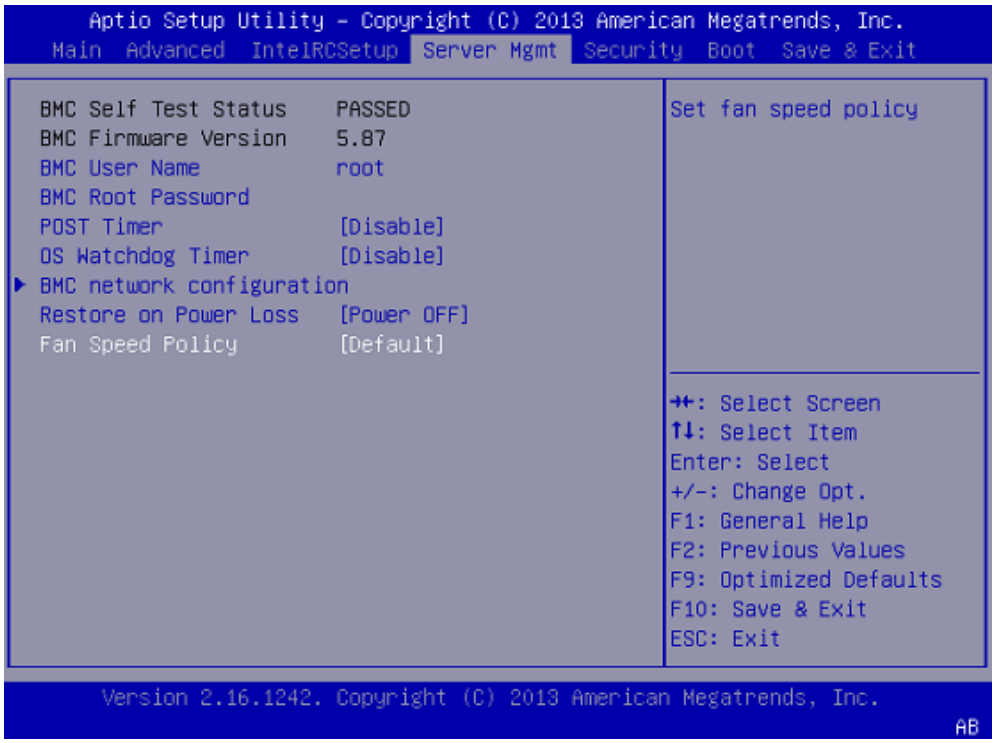
图 4-7 输入密码



步骤4 选择“Server Mgmt”，按“Enter”。

进入“Server Mgmt”界面，如图4-8所示。

图 4-8 Server Mgmt 界面



步骤5 选择“BMC Root Password”，按“Enter”。

步骤6 修改iBMC用户密码，按“Enter”。

- 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。
- 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。
- 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

  - V3服务器不支持弱口令检查规则。
  - V5服务器的默认密码“Admin@9000”在弱口令字典中。

步骤7 重复输入设置的密码，按“Enter”。

弹出“Changes have been saved”对话框。

步骤8 按“Enter”。

保存配置。

----结束

4.2.2 确认管理网口 IP

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

默认 IP 地址

表 4-2 默认 IP

产品类型	槽位	IP
RH8100 V3/8100 V5	8P单系统	192.168.2.100
	4P双系统	• 主管理网口：192.168.2.100 • 从管理网口：192.168.2.101
其它机架服务器	–	192.168.2.100

RH8100 V3 通过 BIOS 查询和设置

步骤1 重启服务器。

说明

不同配置下，服务器启动时间不同。满配时重启时间为20分钟，请耐心等待。

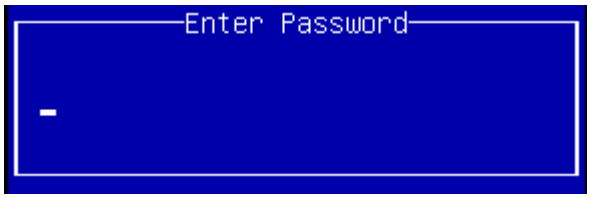
步骤2 在启动过程中，根据界面提示信息按“Del”。进入BIOS设置界面。

步骤3 如果在启动过程中出现输入密码对话框，请在对话框中输入密码，如图4-9所示。

说明

- BIOS默认密码为Huawei12#$，第一次进入后请立即修改密码，为提高安全性，建议定期修改BIOS密码。
- 如果连续三次输入错误的BIOS密码，BIOS会锁定，可按“Ctrl+Alt+Del”重启BIOS解锁。

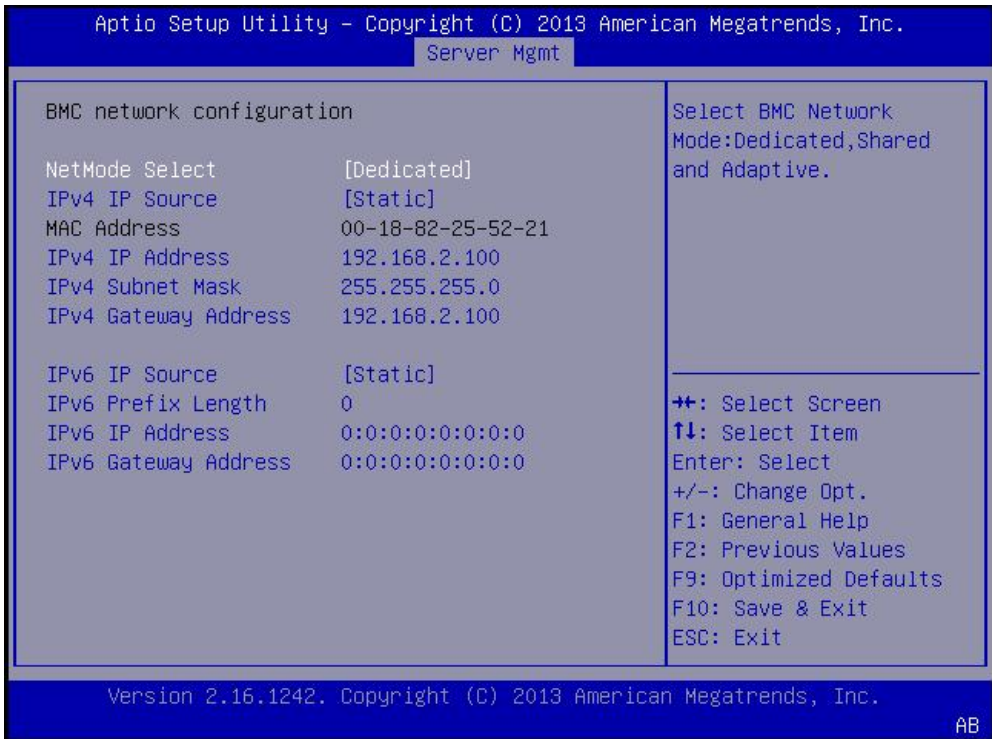
图 4-9 输入密码



步骤4 选择“Server Mgmt > BMC network configuration”，按“Enter”。

进入“BMC network configuration”界面，显示BMC IP信息，如图4-10所示。

图 4-10 BMC network configuration 界面



步骤5 选中待修改的配置项，按“Enter”。

在弹出的对话框中可对配置项进行修改。

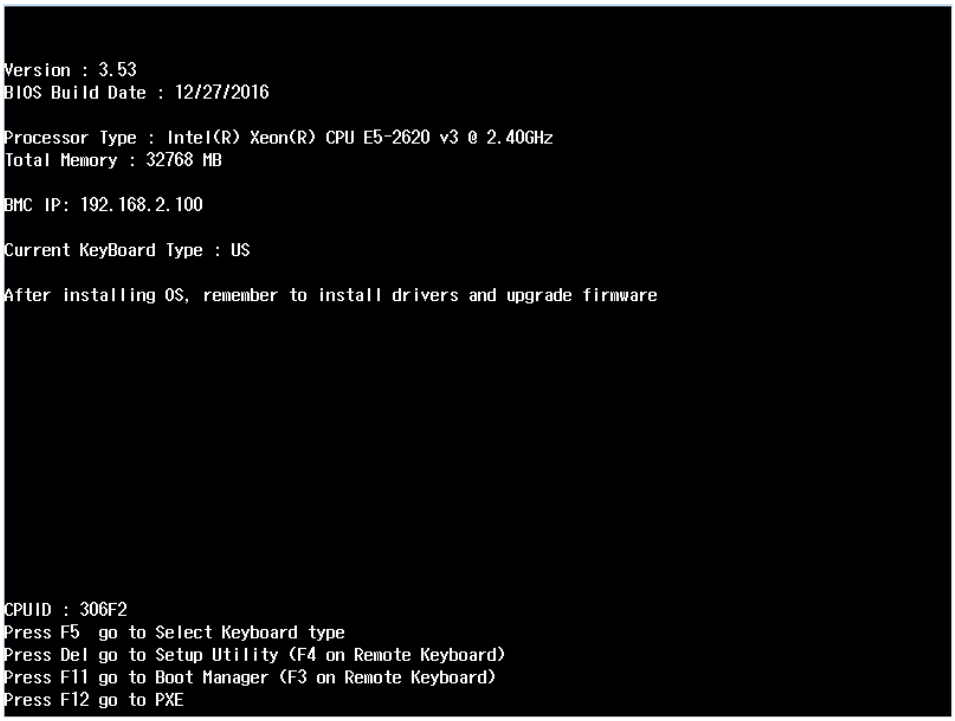
----结束

其他机架服务器通过 BIOS 查询和设置

步骤1 重启服务器。

步骤2 服务器重启时，当出现如下界面时，重复按“Delete”。进入BIOS界面

图 4-11 BIOS 启动界面



步骤3 如果在启动过程中出现输入密码对话框，请在对话框中输入密码，如图4-12所示。

图 4-12 输入密码

步骤4 选择“Advanced > IPMI BMC Configuration”，按“Enter”。

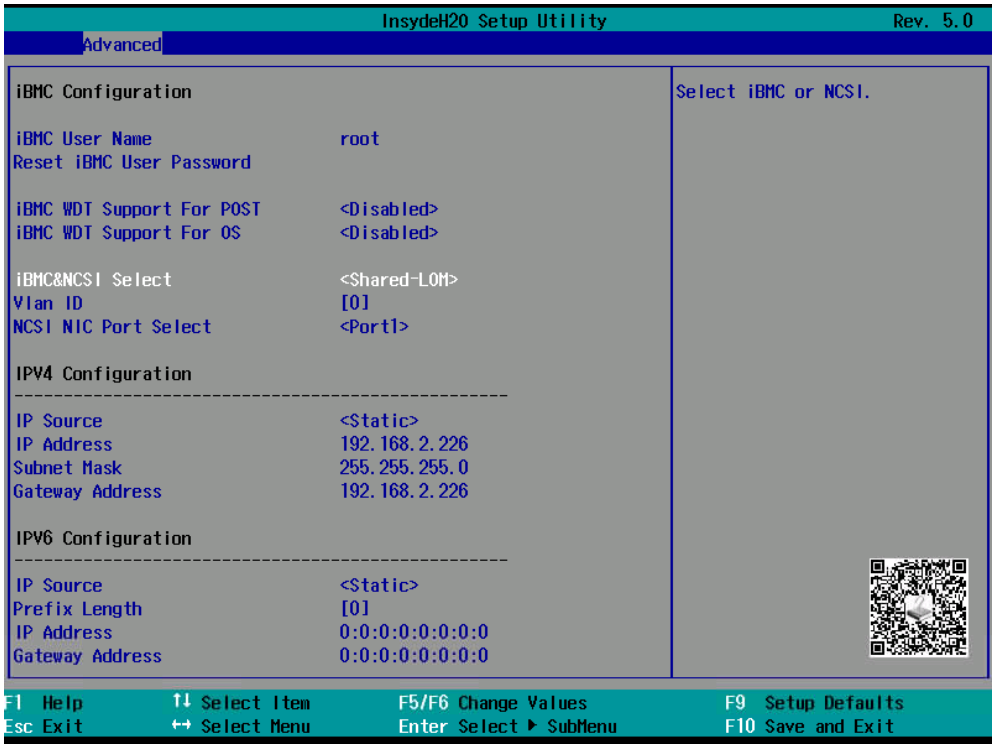
进入“IPMI BMC Configuration”界面。

步骤5 选择“iBMC Configuration”，按“Enter”。

进入“iBMC Configuration”界面，如图4-13所示。

界面中显示管理网口当前IP地址信息。

图 4-13 “iBMC Configuration”界面



步骤6 选中待修改的配置项，按“Enter”。

在弹出的对话框中可对配置项进行修改。

----结束

通过本地串口登录

须知

通过串口登录iBMC命令行，必须保证机箱的系统串口已经切换为iBMC串口。可以通过SSH登录命令行，执行**serialdir**切换串口。

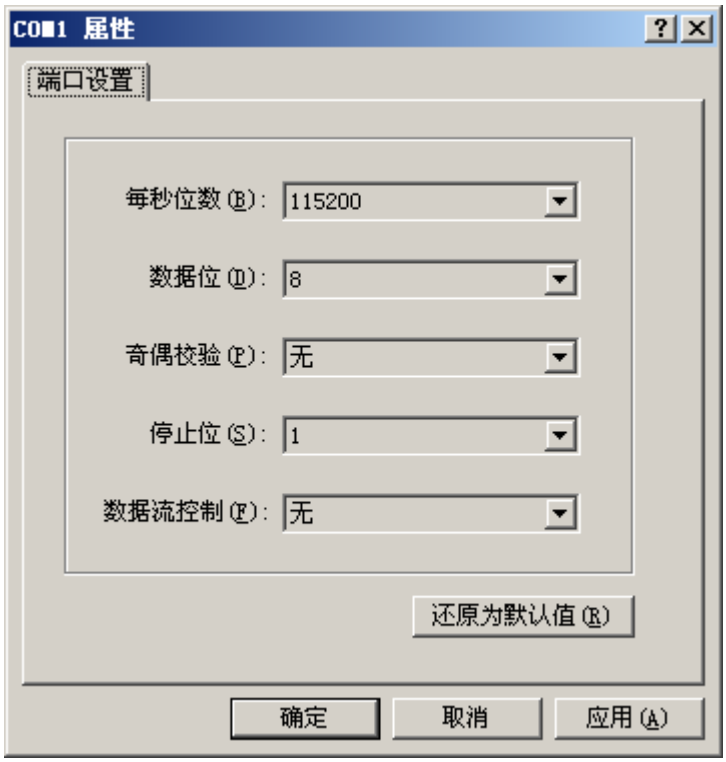
步骤1 连接串口线。

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4-14**所示。

图 4-14 超级终端属性设置



步骤3 呼叫成功后输入用户名和密码。

----结束

4.2.3 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

- V3服务器提供1个iBMC默认用户“root”，默认密码为“Huawei12#$”；V5服务器提供1个iBMC默认用户“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。

  说明

  请勿同时连接2个管理网口，连接任一管理网口均可登录iBMC。

- 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。

对于机架服务器来说，机箱面板上有1000M自适应管理网口。直接用网线相连即可。

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命令行。
- 使用LDAP用户登录iBMC命令行时，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。

通过本地串口登录

须知

通过串口登录iBMC命令行，必须保证机箱的系统串口已经切换为iBMC串口。可以通过SSH登录命令行，执行**serialdir**切换串口。

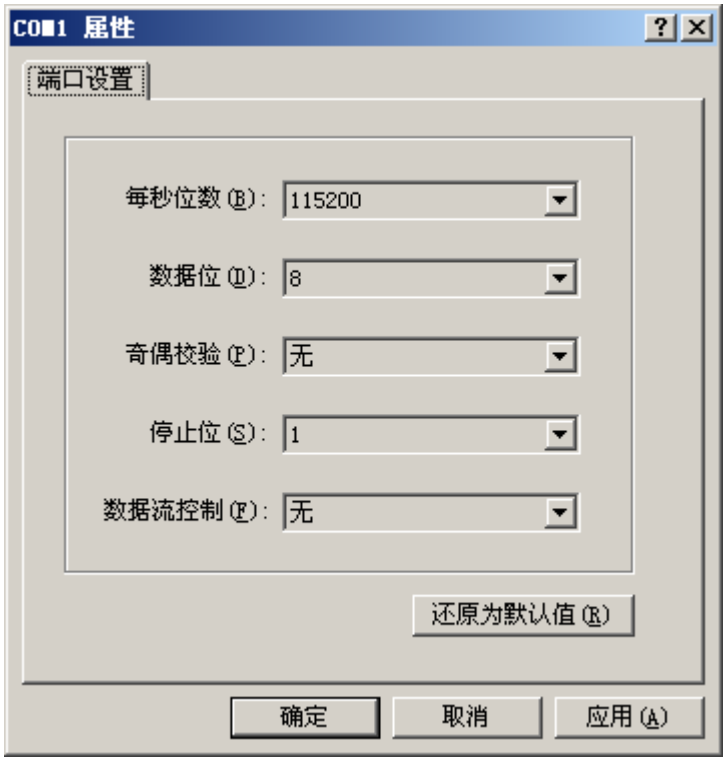
步骤1 连接串口线。

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4-15**所示。

图 4-15 超级终端属性设置



步骤3 呼叫成功后输入用户名和密码。

----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
```

RH8100 V3 服务器的系统返回信息如下所示：

```
EthGroup ID          : 1
Net Mode             : Manual
Net Type             : Dedicated
IPv4 Information     :
IP Mode              : static
IP Address           : 192.168.2.100
Subnet Mask          : 255.255.0.0
Default Gateway      : 192.168.2.25
MAC Address          : 00:18:e1:c5:d8:26
IPv6 Information     :
IPv6 Mode            : static
IPv6 Address         : fc00::2001/15
Default Gateway IPv6 : fc00::2003
Link-Local Address   : fe80::218:e1ff:fec5:d826/64
VLAN Information     :
VLAN State           : disabled

EthGroup ID          : 2
Net Mode             : Manual
Net Type             : Dedicated
IPv4 Information     :
IP Mode              : static
IP Address           : 10.0.0.1
Subnet Mask          : 255.255.255.252
Default Gateway      :
MAC Address          :
IPv6 Information     :
IPv6 Mode            : static
IPv6 Address 1       : fc00::2001/15
Default Gateway IPv6 : fc00::2003
Link-Local Address   : fe80::218:e1ff:fec5:d826/64
IPv6 Address 1       : fc00:db8:1:0:218:e1ff:fec5:d826/64
VLAN Information     :
VLAN State           : enabled
VLAN ID              : 4094
```

说明

- GROUP1用于对外访问。
- GROUP2用于内部数据通信。

其他机架服务器系统返回信息如下所示：

```
EthGroup ID          : 1
Net Mode             : Manual
Net Type             : Dedicated
IPv4 Information     :
IP Mode              : static
IP Address           : 172.33.13.104
Subnet Mask          : 255.255.0.0
Default Gateway      : 172.33.0.1
MAC Address          : 00:18:ac:21:0d:68
IPv6 Information     :
IPv6 Mode            : static
IPv6 Address 1       :
Default Gateway IPv6 :
Link-Local Address   : fe80::218:acff:fe21:d68/64
VLAN Information     :
VLAN State           : enabled
VLAN ID              : 4093
```

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
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
```

4.3.3 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
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。

4.3.4 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
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
```

4.3.5 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*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          : 255.255.0.0
Default Gateway      : 192.168.0.1
MAC Address          : 00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode            : static
```

```
IPv6 Address          : fc00::6516
Default Gateway IPv6  : fc00::1
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 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               : static
IP Address            : 192.168.0.25
Subnet Mask           : 255.255.0.0
Default Gateway       : 192.168.0.1
MAC Address           : 00:18:e1:c5:d8:66
IPv6 Information      :
IPv6 Mode             : static
IPv6 Address          : fc00::6516
Default Gateway IPv6  : fc00::1
Link-Local Address    : fe80::218:e1ff:fec5:d866/64
VLAN Information      :
VLAN State            : disabled
VLAN ID               : 1
EthGroup ID           : 1
Net Mode              : Manual
Net Type              : Dedicated
```

```
IPv4 Information      :
IP Mode             : static
IP Address          : 192.168.0.25
Subnet Mask         : 255.255.0.0
Default Gateway     : 192.168.0.1
MAC Address         : 00:18:e1:c5:d8:66
IPv6 Information      :
IPv6 Mode           : static
IPv6 Address        : fc00::6516
Default Gateway IPv6  : fc00::1
Link-Local Address    : fe80::218:e1ff:fec5:d866/64
VLAN Information      :
VLAN State          : disabled
VLAN ID             : 1
```

4.3.7 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           : 255.255.0.0
Default Gateway       : 192.168.0.1
MAC Address           : 00:18:e1:c5:d8:66
IPv6 Information      :
IPv6 Mode           : static
IPv6 Address        : fc00::6516
Default Gateway IPv6  : fc00::1
Link-Local Address    : fe80::218:e1ff:fec5:d866/64
VLAN Information      :
VLAN State          : disabled
VLAN ID             : 1
```

4.3.8 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
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
```

4.3.9 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 • 1：板载网口 • 2：PCIe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
```

```
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	• RH8100 V3、8100 V5的取值范围：1 ~ 4093 • 其它机架服务器的取值范围：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
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
```

4.3.11 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
```

4.3.12 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

- 单系统模式下，在主iBMC执行该命令会触发主从iBMC同步重启。
- 双系统模式下，该命令只对当前操作的iBMC生效。

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...
```

4.3.13 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*>

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*”

使用指南

iBMC为V256之前版本，使用该命令升级固件（iBMC/CPLD/BIOS）之前，请先使用**ipmcset -d reset**命令重启iBMC。

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”）。

升级iBMC或SD卡控制器后，iBMC自动重启，使升级的固件生效。

- 单系统模式下，在主iBMC执行该命令会触发主从iBMC同步升级。
- 双系统模式下，该命令只对当前操作的iBMC生效。

执行升级时，如果需要从iBMC中间版本的以下版本升级到中间版本的以上版本，需要先将iBMC升级到中间版本，然后再升级到目标版本。若升级到中间版本失败，可对iBMC重启后再次尝试。服务器型号与iBMC中间版本关系如**表4-3**所示。例如，执行升级的服务器是RH1288 V3，需要从iBMC V257以下版本升级到V257以上版本，需要先将iBMC升级到V257版本，然后再升级到目标版本。若升级到V257版本失败，可对iBMC重启后再次尝试。

表 4-3 iBMC 中间版本与服务器型号关系表

中间版本	型号
257	RH1288 V3/RH2288H V3/RH5288 V3
260	RH5885H V3
262	RH2288 V3
270	RH5885 V3
276	RH8100 V3

使用实例

升级软件。

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

4.3.14 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“/tmp/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.
```

4.3.15 iBMC 软件回滚（rollback）

命令功能

rollback命令用来将iBMC固件主分区的镜像文件切换到备分区的镜像文件。

命令格式

ipmcset -d rollback

参数说明

无

使用指南

- 单系统模式下，在主iBMC执行该命令会触发主从iBMC同步回滚。
- 双系统模式下，该命令只对当前操作的iBMC生效。
- 回滚操作是将主备iBMC的版本区域进行切换，如果主备版本一致，则回滚后的版本是一样的。

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!
```

4.3.16 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!
```

4.3.17 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。

仅V5服务器支持VNC服务。

使用实例

启用服务。

```
iBMC:/->ipmcset -t service -d state -v http enabled
Set http service state(enabled) successfully.
```

说明

开启http服务有安全隐患。

4.3.18 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。
- 仅V5服务器支持VNC服务。

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.
```

4.3.19 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

仅V5服务器支持VNC服务。

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
```

4.3.20 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.
```

4.3.21 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 ~ 1600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.
```

4.3.22 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.
```

4.3.23 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。 **说明** iBMCBMC当前仅支持SMB V1.0版本。 ● *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:Huawei12#$@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 Huawei12#$
Import certificate successfully
Reset iBMC for the certificate to take effect.
```

4.3.24 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=Huawei, L=ShenZhen, S=GuangDong, C=CN
Issued      By: CN=Server, OU=IT, O=Huawei, L=ShenZhen, S=GuangDong, C=CN
Valid    From: Jul 25 2014 GMT
Valid      To: Jul 22 2024 GMT
Serial Number: 07
```

4.3.25 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”。

参数	参数说明	取值
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** ● iBMCBMC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。 ● *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:Huawei12#$@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.
```

4.3.26 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： ● *protocol*：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 **说明** ● iBMCBMC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。 ● *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:Huawei12#$@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.
```

4.3.27 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** ● iBMCBMC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。 ● *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://root:Huawei12#$@10.10.10.1:443/tmp/cms.crl”
type	CRL文件类型	固定为1。

使用指南

仅V5服务器支持当前命令。

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.
```

4.3.28 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** ● 仅iBMC V300及以上版本支持“https”协议。 ● iBMCBMC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。 ● *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 **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.
```

4.3.29 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.
```

4.3.30 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                  :
```

4.3.31 查询和设置散热功率模式（coolingpowermode）

命令功能

coolingpowermode命令用于查询和设置服务器散热功率模式。

命令格式

ipmcget -t maintenance -d coolingpowermode

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

参数说明

参数	参数说明	取值
option	服务器散热功率模式	• 0：低散热功率模式 • 1：高散热功率模式

使用指南

该命令仅适用于RH8100 V3和8100 V5。在双系统情况下，只能由主系统设置风扇散热功率模式。

使用实例

设置服务器散热功率模式为低散热功率模式。

```
iBMC:/-> ipmcset -t maintenance -d coolingpowermode -v 0
Set cooling power mode to [Power saving mode] successfully.
```

查询服务器当前散热功率模式。

```
iBMC:/-> ipmcget -t maintenance -d coolingpowermode
Power saving mode
```

4.4 Trap 命令

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

参数	参数说明	取值
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
Community	表示SNMP trap团体名称。	默认取值：“TrapAdmin12#$” 不开启密码检查时的取值原则：1～18位的字符串，由数字、英文字母和除空格外的特殊字符组成。 开启密码检查时的取值原则： ● 长度为8～18位的字符。 ● 至少包含以下特殊字符： `~!@#$%^&*()-_=+|[{}];:'",<.>/? ● 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       | 10.10.10.10
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，V3服务器的Trap V3使用“root”用户，V5服务器的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 V3 鉴权和加密协议（trap -d protocol）

命令功能

trap -d protocol命令用于查询和设置SNMP trap V3的鉴权和加密协议。

命令格式

ipmcget -t trap -d protocol

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

参数说明

参数	参数说明	取值
option	表示SNMP trap V3采用的加密协议。	• 1：表示鉴权协议为MD5，加密协议为DES。 • 2：表示鉴权协议为MD5，加密协议为AES。 • 3：表示鉴权协议为SHA，加密协议为DES。 • 4：表示鉴权协议为SHA，加密协议为AES。 • 默认取值：“4”。

使用指南

- 需要管理工作站配置相同的鉴权、加密协议。
- 该设置同时对“SNMP V3”生效。
- “MD5”和“DES”存在安全隐患，建议使用“SHA”和“AES”。

使用实例

设置SNMP trap V3协议。

```
iBMC:/->ipmcset -t trap -d protocol -v 4
Set SNMP trap authentication and privacy protocol successfully.
```

查询SNMP trap V3协议。

```
iBMC:/->ipmcget -t trap -d protocol
Trap protocol      :
  Authentication  : SHA
  Privacy         : AES
```

4.4.10 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，详细内容请参考服务器的iBMC智能管理系统SNMP接口说明书。

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

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
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 面向连接的协议，并保证数据传输的保密性和数据完整性。 • 2：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。 • 3：TLS 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。

使用指南

无

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。 • 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”）。

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=HW, L=, S=GD, C=CH
Issued     By: CN=Huawei, OU=IT, O=Huawei, L=ShenZhen, S=GuangDong, C=CN
Valid    From: Mar 24 2016 GMT
Valid      To: Mar 24 2017 GMT
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”）。

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=Huawei, L=ShenZhen, S=GuangDong, C=CN
Issued      By: CN=Administrator, OU=it3, O=huawei3, L=, S=guangdong2, C=cn
Valid     From: Feb 17 2015 GMT
Valid       To: Feb 17 2016 GMT
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 服务器命令

4.6.1 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。 ● 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
Set boot device successfully.
```

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
```

4.6.2 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 • 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.
```

4.6.3 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
```

4.6.4 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。
“下电时限”设置为 

后，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.
```

4.6.5 查询服务器板载网卡 MAC 地址（macaddr）

命令功能

macaddr命令用来查询服务器主板上网口的MAC地址。

命令格式

ipmcget -d macaddr

参数说明

无

使用指南

无

使用实例

查询服务器主板上网口的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
```

4.6.6 查询系统可用网口（ethport）

命令功能

ethport命令用来查询服务器上可用网口信息。

命令格式

ipmcget -d ethport

参数说明

无

使用指南

无

使用实例

查询服务器可用网口。

```
iBMC:/->ipmcget -d ethport
Type       | Name       | Port ID  | Link Status
Dedicated  | eth2       | na       | Link_Up
LOM        | Port1      | 1        | Link_Down
LOM        | Port2      | 2        | Link_Down
LOM        | Port3      | 3        | Link_Down
LOM        | Port4      | 4        | Link_Down
```

4.6.7 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.
```

4.6.8 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

必须满足如下任一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iBMA2.0。

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
---------------------------------------------------------------------
```

4.6.9 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

必须满足如下任一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iBMA2.0。

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
------------------------------------------------------------------------
```

4.6.10 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

必须满足如下任一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iBMA2.0。

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                      : TOSHIBA
Serial Number                     : EB00PC208N0R
Model                             : MBF2300RC
Firmware Version                  : 0109
Health Status                     : Normal
Firmware State                    : UNCONFIGURED GOOD
Power State                       : Spun Up
Media Type                        : HDD
Interface Type                    : SAS
Interface Speed                   : 6.0Gbps
Link Speed                        : 6.0Gbps
Drive Temperature                 : 62(Celsius)
Capacity                          : 278.465 GB
Hot Spare                         : None
Rebuild in Progress               : No
Patrol Read in Progress           : No
Remnant Media Wearout             : N/A
SAS Address(0)                    : 50000393d84baa46
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                      : TOSHIBA
Serial Number                     : EB00PC208KL3
Model                             : MBF2300RC
Firmware Version                  : 0109
Health Status                     : Normal
Firmware State                    : ONLINE
Power State                       : Spun Up
Media Type                        : HDD
Interface Type                    : SAS
Interface Speed                   : 6.0Gbps
Link Speed                        : 6.0Gbps
Drive Temperature                 : 53(Celsius)
Capacity                          : 278.465 GB
Hot Spare                         : None
Rebuild in Progress               : No
Patrol Read in Progress           : No
Remnant Media Wearout             : N/A
SAS Address(0)                    : 50000393d84b6f92
SAS Address(1)                    : 0000000000000000
Location State                    : Off

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

Physical Drive Information
```

```
---------------------------------------------------------------------------
ID                              : 1
Device Name                     : Disk1
Manufacturer                    : TOSHIBA
Serial Number                   : EB72PC600G1C
Model                           : MBF2300RC
Firmware Version                : 0109
Health Status                   : Normal
Firmware State                  : ONLINE
Power State                     : Spun Up
Media Type                      : HDD
Interface Type                  : SAS
Interface Speed                 : 6.0Gbps
Link Speed                      : 6.0Gbps
Drive Temperature               : 69(Celsius)
Capacity                        : 278.465 GB
Hot Spare                       : None
Rebuild in Progress             : No
Patrol Read in Progress         : No
Remnant Media Wearout           : N/A
SAS Address(0)                  : 5000039418218546
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                    : TOSHIBA
Serial Number                   : EB00PC208N0R
Model                           : MBF2300RC
Firmware Version                : 0109
Health Status                   : Normal
Firmware State                  : ONLINE
Power State                     : Spun Up
Media Type                      : HDD
Interface Type                  : SAS
Interface Speed                 : 6.0Gbps
Link Speed                      : 6.0Gbps
Drive Temperature               : 62(Celsius)
Capacity                        : 278.465 GB
Hot Spare                       : None
Rebuild in Progress             : No
Patrol Read in Progress         : No
Remnant Media Wearout           : N/A
SAS Address(0)                  : 50000393d84baa46
SAS Address(1)                  : 0000000000000000
Location State                  : Off

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

4.6.11 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

必须满足如下任一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iBMA2.0。

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                       : 1.149 TB
Free Space                      : 215.749 GB
Logcial Drive(s) ID              : 1
Physical Drive(s) ID             : 2,8,9,10,11
---------------------------------------------------------------------
```

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                       : 200.469 GB
Free Space                      : 356.461 GB
Logcial Drive(s) ID              : 0
Physical Drive(s) ID             : 0,1
---------------------------------------------------------------------

Disk Array Information
---------------------------------------------------------------------
Array ID                        : 1
Used Space                       : 1.149 TB
Free Space                      : 215.749 GB
Logcial Drive(s) ID              : 1
Physical Drive(s) ID             : 2,8,9,10,11
---------------------------------------------------------------------

Disk Array Information
---------------------------------------------------------------------
```



```
Array ID                        : 2
Used Space                      : 446.103 GB
Free Space                      : 0 MB
Logcial Drive(s) ID             : 2
Physical Drive(s) ID            : 7
--------------------------------------------------------------------------------
```

4.6.12 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。

参数	参数说明	取值
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”。

参数	参数说明	取值
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。 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
```

4.6.13 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*>**]**

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 默认为“256K”。

参数	参数说明	取值
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 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”。

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
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.14 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
```

4.6.15 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
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。

参数	参数说明	取值
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。
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
```

4.6.16 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功能使能状态	• enabled • disabled
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
```

4.6.17 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*>]

参数说明

参数	参数说明	取值
pdid	物理硬盘的ID	0～255

参数	参数说明	取值
pdstate	物理盘的运行状态	• online：在线 • offline：离线 • ug：空闲 • 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

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1的物理盘的固件运行状态为online。

```
iBMC:/-> ipmcset -t storage -d pdconfig -v 1 -state online
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7 系统命令

4.7.1 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
```

4.7.2 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。 – [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/New_York。 • 默认值：GMT 支持的时区，请通过输入命令**ipmcset -d timezone -v** <*a*>查看。

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GMT+8:00。

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

查询iBMC时间。

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

4.7.3 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 GMT+08:00
```

或

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

4.7.4 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
```

RH8100 V3 服务器的系统返回信息如下所示：

```
------------------- iBMC INFO --------------------
IPMC               CPU:            Hi1710
IPMI            Version:           2.0
CPLD            Version:           (U6029)1.04
Active iBMC     Version:           (U6005)5.30
Active iBMC      Build:            001
Active iBMC      Built:            10:56:13 Aug  1 2014
Backup iBMC     Version:           5.30
SDK             Version:           1.36
SDK              Built:           15:07:46 Jul 30 2014
Active Uboot    Version:           1.1.26 (Jun 20 2014 - 14:28:52)
Backup Uboot    Version:           1.1.26 (Jun 20 2014 - 14:28:52)
IPMB            Address:           0x20
----------------- Product INFO -----------------
Product             ID:            0x0008
Product            Name:           RH8100 V3
BIOS            Version:           (U6145)V019
-------------- Mother Board INFO ---------------
RH8100          BoardID:           0x005b
RH8100             PCB:            .A
---------------- Raid Card INFO ----------------
SR130           BoardID:           0x002c
SR130              PCB:            .A
--------------- Riser Card INFO ----------------
BC61PRBA        BoardID:           0x0080
-------------- HDD Backplane INFO --------------
BC11THBG        BoardID:           0x007a
BC11THBG           PCB:            .A
---------------- CPU Board INFO ----------------
CpuBoard        BoardID:           0x0090
CpuBoard           PCB:            .A
CpuBoard  CPLD Version:            (U1028)1.04
CpuBoard        BoardID:           0x0090
CpuBoard           PCB:            .A
CpuBoard  CPLD Version:            (U1028)1.04
CpuBoard        BoardID:           0x0090
CpuBoard           PCB:            .A
CpuBoard  CPLD Version:            (U1028)1.04
CpuBoard        BoardID:           0x0090
CpuBoard           PCB:            .A
CpuBoard  CPLD Version:            (U1028)1.04
-------------- Memory Board INFO --------------
MemoryBoard     BoardID:           0x0094
MemoryBoard        PCB:            .A
MemoryBoard     BoardID:           0x0094
MemoryBoard        PCB:            .A
---------------- IO Board INFO -----------------
BioBoard        BoardID:           0x005a
BioBoard           PCB:            .A
BioBoard  CPLD Version:            (U1044)1.04
------------------- LCD INFO --------------------
LCD             Version:           (J7)1.00
```

其他机架服务器系统返回信息如下所示：

```
------------------- iBMC INFO -------------------
IPMC               CPU:           Hi1710
IPMI           Version:           2.0
CPLD           Version:           (U4269)2.02
Active iBMC    Version:           (U4282)2.92
Active iBMC      Build:           002
Active iBMC      Built:           21:09:56 Feb 11 2018
Backup iBMC    Version:           2.97
SDK            Version:           3.10
SDK              Built:           17:16:44 Feb  6 2018
Active Uboot   Version:           2.1.07 (Dec 21 2017 - 18:01:59)
Backup Uboot   Version:           2.1.07 (Dec 21 2017 - 18:01:59)
----------------- Product INFO -----------------
Product            ID:            0x0001
Product          Name:            1288H V5
BIOS           Version:           (U47)0.60
-------------- Mother Board INFO ---------------
Mainboard      BoardID:           0x0019
Mainboard        PCB:             .B
--------------- Riser Card INFO ----------------
BC11PERY       BoardID:           0x0091
-------------------- PS INFO --------------------
PS1            Version:           DC: 02e  PFC: 018
```

4.7.5 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    : Huawei Technologies Co., Ltd.
 Board Product Name    : board
 Board Serial Number   : 022HLV10E3000003
 Board FRU File ID     : 1.17
 Product Manufacturer  : Huawei Technologies Co., Ltd.
 Product Name          : pname
 Product Serial Number : serialnumber
 Product FRU File ID   : 1.17
```

4.7.6 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.
```

4.7.7 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.
```

4.7.8 查询 80 口信息（port80）

命令功能

port80命令用于查询80口当前和历史信息。

命令格式

ipmcget -d port80

参数说明

无

使用指南

无

使用实例

查询80口当前和历史信息。其中，方括号括起来的值为当前值。

```
iBMC:/->ipmcget -d port80
port80 diagnose code:
[00]-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
```

4.7.9 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
```

4.7.10 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.
```

4.7.11 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:
```

4.7.12 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“串口数据”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.
```

4.7.13 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（例如iBMA）后才可以使用。如何使用iBMA解析黑匣子数据请参考iBMA用户指南。
- 需要在iBMC Web管理系统的“诊断 > 黑匣子”界面开启黑匣子功能。更多关于黑匣子的信息请参考**黑匣子**。
- 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.
```

4.7.14 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。 **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”文件并联系华为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，执行操作请参考本文档**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.
```

4.7.15 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**升级时则没有此要求。
  - 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**4.3.13 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.
```

4.7.16 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.
```

4.7.17 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考**一键收集信息**。

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.
```

4.7.18 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.
```

4.7.19 设置 CLP notimeout 功能状态（notimeout）

命令功能

notimeout命令用于设置CLP notimeout功能的使能和禁止状态。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>

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	-

使用指南

无

使用实例

启用CLP notimeout功能。

```
iBMC:/->ipmcset -d notimeout -v enabled
Set no timeout state successfully.
```

#禁用CLP notimeout功能。

```
iBMC:/->ipmcset -d notimeout -v disabled
Set no timeout state successfully.
```

4.7.20 更新系统工作密钥（workkey）

命令功能

workkey命令用来更新系统工作密钥。

命令格式

ipmcset -d workkey

参数说明

无

使用指南

无

使用实例

更新系统工作密钥。

```
iBMC:/->ipmcset -d workkey
Update system workkey successfully.
```

4.7.21 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.
```

4.7.22 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	-

参数	参数说明	取值
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.
```

4.7.23 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

iBMC V338及以上版本支持此命令。

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.
```

4.7.24 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
<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

RH1288A V2、RH2288A V2不支持该命令。

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 enbalewill 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.
```

4.7.25 重启 iME（resetiME）

命令功能

resetiME命令用于重启iME（Intel Management Engine），当iME无法正常运行时，可使用该命令将其复位。

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iME。

```
iBMCBMC:/->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.
```

4.8 用户管理命令

4.8.1 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
```

4.8.2 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。 • 可包含数字、字母以及字符。 • 字符不包括： :<>&,'"/\% • 字符串首字符不能是“#”。

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。

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**passwordcomplexity**命令查询）以及弱口令认证功能的开启情况（可通过**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。

- 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。
- 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

  - V3服务器不支持弱口令检查规则。
  - V5服务器的默认密码“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。

4.8.3 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

请根据密码复杂度检查功能的开启情况（可通过**passwordcomplexity**命令查询）以及弱口令认证功能的开启情况（可通过**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。
- 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。
- 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

- V3服务器不支持弱口令检查规则。
- V5服务器的默认密码“Admin@9000”在弱口令字典中。

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。

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.
```

4.8.4 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。
- iBMC V357及以上版本起，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.
```

4.8.5 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。
- iBMC V357之前版本，不允许设置默认用户的权限；iBMC V357及以上版本，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

  V3服务器的默认用户为“root”，V5服务器的默认用户为“Administrator”。
- iBMC V357之前版本，被设置权限的用户不能处于SSH登录状态；iBMC V357及以上版本，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.
```

4.8.6 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

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。
- 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。

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**ipmcset -t user -d weakpwddic -v export**获取。）

只有管理员可以设置密码复杂度检查功能的开启状态。

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.
```

4.8.7 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.
```

4.8.8 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.
```

4.8.9 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
```

4.8.10 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.
```

4.8.11 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_1024.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_1024.key
Input your password:
Add user public key successfully.
```

4.8.12 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.
```

4.8.13 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
```

4.8.14 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	–

参数	参数说明	取值
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
```

4.8.15 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

仅V5服务器支持当前命令。

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.
```

4.8.16 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	弱口令字典导出后的本地存放路径	弱口令字典在iBMC系统中的绝对路径，例如：“/tmp/weakpwddictionary”。

参数	参数说明	取值
file_URL	弱口令字典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** ● iBMCBMC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。 ● *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:Huawei12#$@10.10.10.1:443/tmp/weakpwddictionary”

使用指南

仅V5服务器支持当前命令。

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.
```

4.8.17 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
filepath	待导入的弱口令字典所在本地路径	弱口令字典在iBMC系统上的绝对路径，例如：“/tmp/weakpwddictionary”。
file_URL	待导入的弱口令字典所在远程路径	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** ● iBMCBMC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。 ● *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:Huawei12#$@10.10.10.1:443/tmp/weakpwddictionary”

使用指南

仅V5服务器支持当前命令。

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.
```


4.8.18 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

仅V5服务器支持当前命令。

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**passwordcomplexity**命令查询）以及弱口令认证功能的开启情况（可通过**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。
- 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。
- 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

  - V3服务器不支持弱口令检查规则。
  - V5服务器的默认密码“Admin@9000”在弱口令字典中。

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.
```

4.8.19 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。

```
iBMCBMC:/->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。

```
iBMCBMC:/->ipmcget -t user -d usermgmtbyhost
Disable
```

4.9 NTP 命令

4.9.1 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
```

4.9.2 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
```

4.9.3 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 • 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
```

4.9.4 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

使用指南

- iBMC V312以下版本仅支持Linux NTP服务器。
- iBMC V312及以上版本，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
```

4.9.5 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

使用指南

- iBMC V312以下版本仅支持Linux NTP服务器。
- iBMC V312及以上版本，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
```

4.9.6 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。

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
```

4.9.7 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”）。

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
```

4.10 指示灯命令

4.10.1 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
```

4.10.2 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.
```

4.10.3 设置硬盘 locate 指示灯状态（locate）

命令功能

locate用来设置指定硬盘的定位指示灯的状态。

命令格式

ipmcset -d locate -v <*ID*> <*Action*>

参数说明

参数	参数说明	取值
ID	待设置的硬盘的ID。	0～255

参数	参数说明	取值
Action	定位指示灯的状态	• start：表示点亮硬盘定位指示灯。 • stop：表示熄灭硬盘定位指示灯。

使用指南

执行此命令需满足以下条件：

- 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。

“Action”为“start”时，硬盘的定位指示灯会一直闪烁。

使用实例

点亮ID为5的硬盘的定位指示灯。

```
iBMC:/->ipmcset -d locate -v 5 start
start locating physical drive (ID:5) successfully
```

4.11 风扇命令

4.11.1 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。
  设置方法请参考**4.11.2 设置风扇运行模式（fanmode）**章节。

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%
```

4.11.2 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
```

4.11.3 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.
```

4.12 传感器命令

4.12.1 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        | 0.000  | 0.000
0x24      | CPU1 Status      | 0x0       | discrete    | 0x8080 | na       | na        | na        | na        |
na        | na     | na
0x25      | CPU2 Status      | 0x0       | discrete    | 0x8080 | 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
0x29      | FAN1 R Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x2a      | FAN2 F Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x2b      | FAN2 R Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x2c      | FAN3 F Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x2d      | FAN3 R Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x2e      | FAN4 F Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x2f      | FAN4 R Status    | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x30      | PS1 Presence     | 0x0       | discrete    | 0x8002 | na       | na        | na        | na        |
na        | na     | na
0x31      | PS2 Presence     | 0x0       | discrete    | 0x8002 | na       | na        | na        | na        |
na        | na     | na
0x32      | DIMM000          | 0x0       | discrete    | 0x8040 | na       | na        | na        | na        |
na        | na     | na
0x33      | DIMM001          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x34      | DIMM002          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x35      | DIMM010          | 0x0       | discrete    | 0x8040 | na       | na        | na        | na        |
na        | na     | na
0x36      | DIMM011          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x37      | DIMM012          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x38      | DIMM020          | 0x0       | discrete    | 0x8040 | na       | na        | na        | na        |
na        | na     | na
0x39      | DIMM021          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x3a      | DIMM022          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x3b      | DIMM030          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x3c      | DIMM031          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x3d      | DIMM032          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x3e      | DIMM100          | 0x0       | discrete    | 0x8040 | na       | na        | na        | na        |
na        | na     | na
0x3f      | DIMM101          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x40      | DIMM102          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x41      | DIMM110          | 0x0       | discrete    | 0x8040 | na       | na        | na        | na        |
na        | na     | na
0x42      | DIMM111          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x43      | DIMM112          | 0x0       | discrete    | 0x8000 | na       | na        | na        | na        |
na        | na     | na
0x44      | DIMM120          | 0x0       | discrete    | 0x8040 | na       | na        | na        | na        |
na        | na     | na
```

```
0x45     | DIMM121          | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x46     | DIMM122          | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x47     | DIMM130          | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x48     | DIMM131          | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x49     | DIMM132          | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x4a     | AreaIntrusion    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x4b     | RTC Battery      | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x4c     | PCIE Status      | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x4d     | ACPI State       | 0x0       | discrete    | 0x8001 | na        | na        | na        | na        |
na       | na     | na
0x4e     | SysFWProgress    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x4f     | Power Button     | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x50     | SysRestart       | 0x0       | discrete    | 0x8080 | na        | na        | na        | na        |
na       | na     | na
0x51     | Boot Error       | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x52     | Watchdog2        | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x53     | Mngmnt Health    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x54     | UID Button       | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x55     | PwrOk Sig. Drop  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x56     | PwrOn TimeOut    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x57     | PwrCap Status    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x58     | HDD Backplane    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x59     | HDD BP Status    | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x5a     | Riser1 Card      | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x5b     | Riser2 Card      | 0x0       | discrete    | 0x8002 | na        | na        | na        | na        |
na       | na     | na
0x5c     | SAS Cable        | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x5d     | FAN1 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x5e     | FAN1 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x5f     | FAN2 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x60     | FAN2 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x61     | FAN3 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x62     | FAN3 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x63     | FAN4 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x64     | FAN4 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        | na        | na
| na       | na     | na
0x65     | RAID Presence    | 0x0       | discrete    | 0x8002 | na        | na        | na        | na        |
na       | na     | na
0x66     | CPU Usage        | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
na       | na     | na
0x67     | Memory Usage     | 0x0       | discrete    | 0x8000 | na        | na        | na        | na        |
```

```
na        | na         | na     | na
0x68      | LCD Status       | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x69      | LCD Presence     | 0x0       | discrete     | 0x8001 | na        | na        | na        | na        |
na        | na     | na
0x6a      | RAID Status      | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x6b      | DISK0            | 0x0       | discrete     | 0x8001 | na        | na        | na        | na        |
na        | na     | na
0x6c      | DISK1            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x6d      | DISK2            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x6e      | DISK3            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x6f      | DISK4            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x70      | DISK5            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x71      | DISK6            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x72      | DISK7            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x73      | DISK8            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x74      | DISK9            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x75      | DISK10           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x76      | DISK11           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x77      | DISK12           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x78      | DISK13           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x79      | DISK14           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x7a      | DISK15           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x7b      | DISK16           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x7c      | DISK17           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x7d      | DISK18           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x7e      | DISK19           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x7f      | DISK20           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x80      | DISK21           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x81      | DISK22           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x82      | DISK23           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x83      | DISK24           | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x84      | DISKA            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x85      | DISKB            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x86      | DISKC            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x87      | DISKD            | 0x0       | discrete     | 0x8000 | na        | na        | na        | na        |
na        | na     | na
0x88      | Eth1 Link Down   | 0x0       | discrete     | 0x8000 | na        | na        | na        | na
| na        | na     | na
0x89      | Eth2 Link Down   | 0x0       | discrete     | 0x8000 | 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
0x8d      | PS1 Fan Status   | 0x0       | discrete     | 0x8000 | na        | na        | na        | na       |
na       | na     | na
0x8e      | PS2 Status       | 0x0       | discrete     | 0x8000 | na        | na        | na        | na       |
na       | na     | na
0x8f      | PS2 Fan Status   | 0x0       | discrete     | 0x8000 | 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 4-4 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。

字段	含义	举例说明	备注
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，具体含义请参考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，表示当前传感器的正向迟滞量是3。	na，表示当前传感器不支持该迟滞量。
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。

4.12.2 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。

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 • “stop”：停止所有测试

使用指南

- 当iBMC版本为V253以下时，执行该命令，可产生对应告警信息。
- 当iBMC版本为V253及以上时，执行该命令，不产生对应告警信息。

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 电源命令

4.13.1 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
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
```

4.13.2 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           HUAWEi 750W PLATINUM PS     N/A             07               750            AC/
DC
2      HUAWEi           HUAWEi 750W PLATINUM PS     N/A             07               750            AC/
DC

Current PSU WorkMode    :
Actual PSU Status       :
   Work Mode          : Load Balancing
Predicted PSU Status    :
   Work Mode          : Load Balancing
```

4.14 U-Boot 命令

4.14.1 登录 U-Boot

操作场景

该操作指导维护工程师，通过服务器串口，登录iBMC的U-Boot。

须知

U-Boot命令主要用于加载底层软件、调试底层设备，如有需要，请联系维护工程师进行操作。

前提条件

- 登录iBMC命令行的用户名和密码。

  V3服务器的iBMC缺省用户为“root”，V5服务器的iBMC缺省用户为“Administrator”，默认密码请参考产品的铭牌。
- 登录U-Boot的密码。

  V3服务器的Uboot默认密码为“Huawei12#$”，V5服务器的Uboot默认密码为“Admin@9000”。

须知

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。

操作步骤

步骤1 通过串口登录iBMC命令行。

步骤2 重启iBMC。

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

步骤3 输入“Y”，按“Enter”。

iBMC开始重启。

步骤4 当界面提示Hit 'ctrl + b' to stop autoboot:时，按“Ctrl+B”。

屏幕回显如下：

```
ENTER PASSWD:
```

步骤5 输入登录U-Boot的密码，V3服务器的Uboot默认密码为“Huawei12#$”，V5服务器的Uboot默认密码为“Admin@9000”。

进入U-Boot操作界面。

----结束

4.14.2 U-Boot 命令参考

说明

U-Boot命令仅用于调试，此处仅给出命令列表，关于U-Boot详细的命令说明，请向华为公司申请。

在iBMC的U-Boot命令行界面输入“?”或“help”，按“Enter”，可以打印iBMC的U-Boot的所有命令帮助，如下所示：

说明

不同版本的U-Boot命令行回显略有差别，下面以U-Boot版本2.1.07为例进行说明。

```
Hi1710_UBOOT> help
?       - alias for 'help'
base    - print or set address offset
bdinfo  - print Board Info structure
bmc_burning- flashdata_burning
flashdata_burning  -refresh all flash data from filename (default filename is ipmc.bin)!
bmc_partition_reset- reset_bmc_partition_table
boot    - boot default, i.e., run 'bootcmd'
bootd   - boot default, i.e., run 'bootcmd'
bootm   - boot application image from memory
bootp   - boot image via network using BOOTP/TFTP protocol
cmp     - memory compare
coninfo - print console devices and information
cp      - memory copy
crc32   - checksum calculation
datafs_burning- update_datafs
datafs_reset- datafs_reset  make datafs reset
datafs_up- update_datafs
ddr_test- ddr_test
dt      - memory test
dts     - just for test
echo    - echo args to console
editenv - edit environment variable
erase   - erase FLASH memory
ext4load- load binary file from a Ext4 filesystem
ext4ls  - list files in a directory (default /)
ext4write- create a file in the root directory
false   - do nothing, unsuccessfully
flinfo  - print FLASH memory information
go      - start application at address 'addr'
help    - print command description/usage
hiddr_test- use for save ddr auto test ret
ibmc0_up- update_bmc0
ibmc1_up- update_bmc1
iminfo  - print header information for application image
itest   - return true/false on integer compare
loadb   - load binary file over serial line (kermit mode)
loads   - load S-Record file over serial line
loady   - load binary file over serial line (ymodem mode)
loop    - infinite loop on address range
lswread - read value of lsw register
lswwrite- write value to lsw register
md      - memory display
mm      - memory modify (auto-incrementing address)
mmc     - MMC sub system
mmcinfo - display MMC info
mtdparts- define flash/nand partitions
mtest   - simple RAM read/write test
```

```
mw      - memory write (fill)
nfs     - boot image via network using NFS protocol
nm      - memory modify (constant address)
passwd  - passwd -   Modify uboot passwd
phyread - read value of phy register
phywrite- write value to phy register
ping    - send ICMP ECHO_REQUEST to network host
printenv- print environment variables
protect - enable or disable FLASH write protection
rarpboot- boot image via network using RARP/TFTP protocol
reboot  - Perform RESET of the CPU
reset   - Perform RESET of the BMC
run     - run commands in an environment variable
saveenv_sfc- save environment variables to persistent storage
setenv  - set environment variables
sfc_burning- sfc_burning  copy sfc image(sfc.bin) to flash
sfc_uboot_cp0- sfc_uboot_cp0  copy uboot0 to flash
sfc_uboot_cp1- sfc_uboot_cp1  copy uboot1 to flash
sleep   - delay execution for some time
test    - minimal test like /bin/sh
tftpboot- boot image via network using TFTP protocol
true    - do nothing, successfully
uboot0_up- uboot0_up  update uboot0
uboot1_up- uboot1_up  update uboot1
version - display u-boot version
```

4.15 SOL 命令

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

参数	参数说明	取值
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

仅iBMC V256及以上版本支持此命令。

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

仅iBMC V256及以上版本支持此命令。

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

仅iBMC V256及以上版本支持此命令。

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

仅iBMC V256及以上版本支持此命令。

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

仅iBMC V256及以上版本支持此命令。

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

登录iBMC的CLI后，输入**clp_commands**，可进入CLP命令行，用户可以执行如下常用的维护命令。

5.1 查看帮助信息（ help ）
5.2 断开连接（ exit ）
5.3 检查网络连通性（ ping、ping6 ）
5.4 free命令（ free ）
5.5 ps命令（ ps ）
5.6 netstat命令（ netstat ）
5.7 df命令（ df ）
5.8 ifconfig命令（ ifconfig ）
5.9 route命令（ route ）
5.10 top命令（ top ）
5.11 禁止CLP超时（ notimeout ）

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
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。详细使用方法请参考服务器的iBMC高级命令参考。

获取ping命令的具体使用方法。

```
iBMC:/->ping --help
BusyBox v1.18.4 (2014-08-09 16:28:25 CST) multi-call binary.

Usage: ping [OPTIONS] HOST

Send ICMP ECHO_REQUEST packets to network hosts

Options:
   -4,-6        Force IP or IPv6 name resolution
   -c CNT       Send only CNT pings
   -s SIZE      Send SIZE data bytes in packets (default:56)
   -I IFACE/IP    Use interface or IP address as source
   -W SEC       Seconds to wait for the first response (default:10)
          (after all -c CNT packets are sent)
   -w SEC       Seconds until ping exits (default:infinite)
          (can exit earlier with -c CNT)
   -q       Quiet, only displays output at start
          and when finished
```

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(84) bytes of data.
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     buffers
 Mem:        125572       94780       30792           0       14780
 Swap:            0           0           0
Total:       125572       94780       30792
```

5.5 ps 命令（ps）

命令功能

该命令用于执行Linux中的ps命令。

命令格式

参考Linux中ps命令的使用方法。

参数说明

支持ps命令的所有参数。

使用指南

无

使用实例

```
iBMC:/-> ps
  PID TTY          TIME CMD
 6743 ttyAMA0  00:00:00 ps
28112 ?        00:00:00 bash
```

5.6 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
```

5.7 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
rootfs                 50580     50580         0 100% /
/dev/root              50580     50580         0 100% /
/dev/mtdblock5         15872      1308     14564   8% /data
tmpfs                  62784       292     62492   0% /dev/shm
tmpfs                  62784       292     62492   0% /dev/shm
tmpfs                  49152       160     48992   0% /tmp
tmpfs                   4096        12      4084   0% /ipmc/usr
```

5.8 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  HWaddr 00:18:82:11:03:21
          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
```

5.9 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
```

5.10 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
```

5.11 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

无

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）
6.2 使用PuTTY登录服务器（网口方式）
6.3 恢复iBMC默认配置
6.4 配置iBMC WebUI Trap
6.5 配置iBMC WebUI SMTP
6.6 配置LDAP功能
6.7 配置iBMC WebUI DNS（手动）
6.8 配置SSH用户密钥登录iBMC命令行
6.9 配置iBMC SSL证书
6.10 配置iBMC Syslog日志上报功能
6.11 使用VNC登录服务器实时桌面
6.12 为iBMC导入信任证书和根证书

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0.60及以上。

数据

登录待连接服务器的用户名和密码。

软件

PuTTY.exe：此工具为免费软件，您可以访问chiark网站主页下载。

说明

低版本的PuTTY软件可能导致登录存储系统失败，建议使用最新版本的PuTTY软件。

操作步骤

1 双击“PuTTY.exe”。

弹出“PuTTY Configuration”窗口。

2 在左侧导航树中选择“Connection > Serial”。

3 设置登录参数。

参数举例如下：

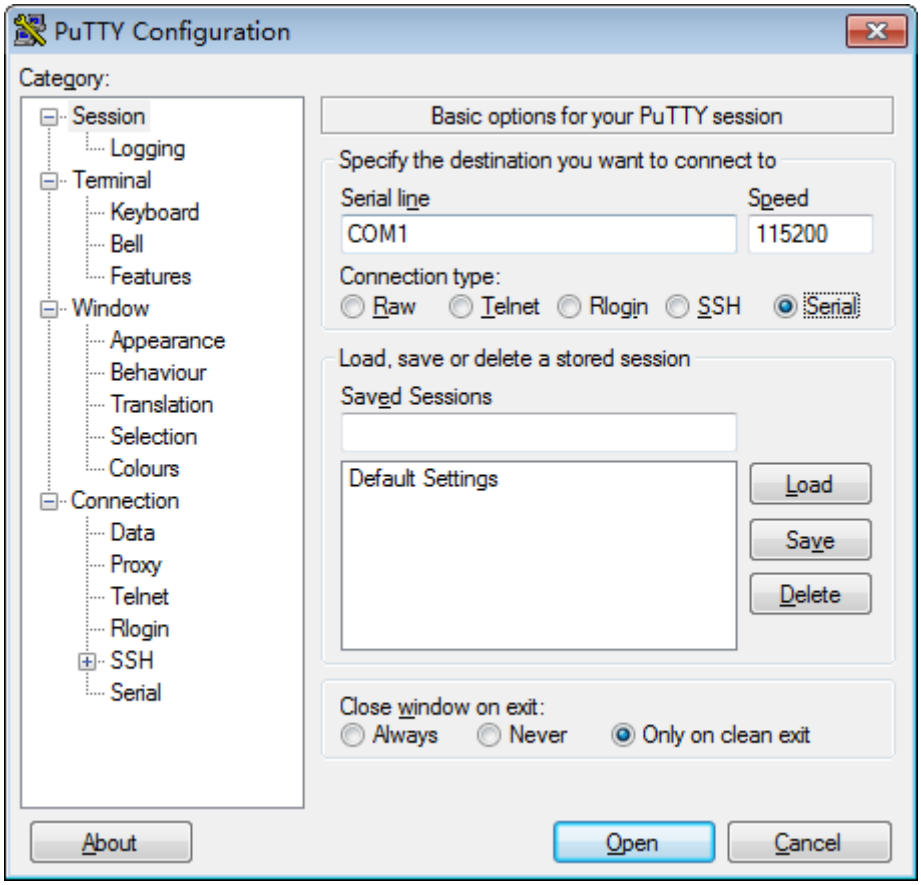
- Serial Line to connect to：COMn
- Speed（baud）：115200
- Data bits：8
- Stop bits：1
- Parity：None
- Flow control：None

*n*表示不同串口的编号，取值为整数。

4 在左侧导航树中选择“Session”。

5 选择“Connection type”为“Serial”，如图6-1所示。

图 6-1 PuTTY Configuration



6 单击“Open”。

进入“PuTTY”运行界面，提示“login as:”，等待用户输入用户名。

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。

数据

需准备如下数据：

- 待连接服务器的IP地址
- 登录待连接服务器的用户名和密码

软件

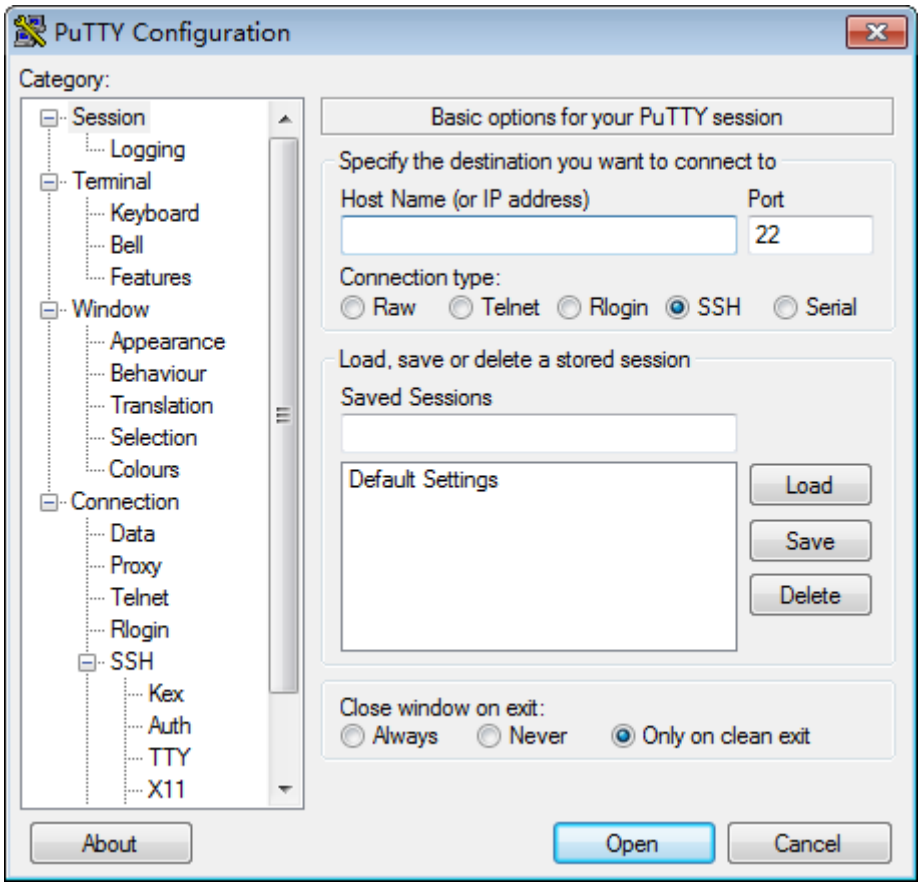
PuTTY.exe：此工具为免费软件，请用户自行获取。

操作步骤

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。

2 双击“PuTTY.exe”。
弹出“PuTTY Configuration”窗口，如图6-2所示。

图 6-2 PuTTY Configuration



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“191.100.34.32”。
- 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。

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。

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 恢复 iBMC 默认配置

操作场景

现网运行设备，当iBMC配置信息发生损坏时，可以使用恢复iBMC默认配置功能，使iBMC可以正常工作或者登录。

恢复iBMC默认配置支持U-Boot命令恢复以及跳线恢复两种方式。跳线恢复需要下电设备。

- 能通过串口线登录U-Boot时，可通过U-Boot命令恢复方式恢复iBMC默认配置。
- 无法登录U-Boot或登录iBMC网络无响应时，可通过跳线恢复方式恢复iBMC默认配置。

须知

- 此功能仅限于华为公司授权人员或华为公司技术服务人员。
- 此功能仅能在设备近端进行，不支持远程操作。
- 此功能会恢复iBMC所有的用户配置，包括用户名、密码、IP地址以及功能配置等，请谨慎操作。
- 执行跳线恢复操作前请做好数据和网络备份。
- iBMC V350及以上版本，iBMC不支持通过跳线恢复默认配置。

各产品支持的恢复方式如**表1 产品恢复方式对应关系表**所示。

表 6-1 产品恢复方式对应关系表

产品型号	U-Boot命令恢复	跳线恢复
RH1288A V2	支持	支持
RH2288A V2	支持	支持
RH1288 V3	支持	支持
RH2288 V3	支持	支持

产品型号	U-Boot命令恢复	跳线恢复
RH2288H V3	支持	支持
RH5885 V3	支持	不支持
RH5885H V3	支持	不支持
5288 V3	支持	支持
RH8100 V3	支持	不支持
1288H V5	支持	支持
2288C V5	支持	支持
2288H V5	支持	支持
2488 V5	支持	支持
2488H V5	支持	支持
5288 V5	支持	支持
5885H V5	支持	支持
8100 V5	支持	支持

操作步骤

- U-Boot命令恢复
  a. 连接串口线，使用Putty工具登录iBMC串口。

     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**查询和设置串口方向（serialdir）**切换串口。

  b. 长按UID按钮，重启iBMC。
  c. 当界面出现如下提示信息时：“Hit 'ctrl + b' to stop autoboot: 1”，立即按下“Ctrl + B”。
  d. 输入U-Boot默认密码。

     V3服务器的Uboot默认密码为“Huawei12#$”，V5服务器的Uboot默认密码为“Admin@9000”。

     显示如下信息，进入U-Boot界面。

     ```
     u-boot>
     ```

  e. 执行以下命令，查询U-Boot版本号：

     printenv ver

  f. 恢复datafs。

     - 如果U-Boot为1.1.37及以前版本，执行以下命令：

       fsload /usr/upgrade/datafs.jffs2

       datafs_cp

- 如果U-Boot为1.1.37以后版本，执行以下命令：
  datafs_reset

g. 执行以下命令，重启iBMC。
reset
等待3分钟后，iBMC重启完成，iBMC恢复默认配置。

- 跳线恢复

a. 备份数据。

须知

跳线恢复需要下电设备，执行操作前请做好数据和网络备份。

b. 找到跳线位号。
跳线位号根据服务器的型号不同而不同，表6-2提供了支持跳线恢复的服务器的跳线位号与跳线丝印关系表。跳线的实际位置请参考各产品用户指南的主板布局章节。

表 6-2 跳线位号与丝印对应关系表

产品型号	跳线位号	跳线丝印
RH2288A V2	J117	CLR_BMC_PW
RH1288A V2	J117	CLR_BMC_PW
RH1288 V3	J36	CLR_BMC_PW
RH2288 V3	J36	CLR_BMC_PW
RH2288H V3	J36	CLR_BMC_PW
5288 V3	J36	CLR_BMC_PW
1288H V5	J176	BMC_RCV
2288C V5	J176	BMC_RCV
2288H V5	J176	BMC_RCV
2488 V5	J93	CLEAR_BMC_PW
2488H V5	J93	CLEAR_BMC_PW
5288 V5	J176	CLR_BMC_PW
5885H V5	J93	CLEAR_BMC_PW
8100 V5	J16	CLEAR_BMC_PW

c. 使用跳线帽或其他工具短接跳线。
d. 保持跳线短接状态并长按UID按钮6秒，重启iBMC。
等待3分钟后，iBMC重启完成，iBMC恢复iBMC默认配置。

说明

请在合适的时机将跳线拔出，否则iBMC下次重启时恢复iBMC默认配置。

6.4 配置 iBMC WebUI Trap

操作场景

iBMC WebUI的“告警设置”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，详细操作请参考**3.1 登录iBMC WebUI**。

步骤2 在iBMC WebUI，选择“告警与事件 > 告警设置”。

步骤3 在“告警Trap报文通知设置”区域框，单击 

，使能Trap功能。

当 

按钮变为 

，表示启动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。

   默认情况下，V3服务器的Trap V3使用“root”用户，V5服务器的Trap V3使用“Administrator”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。
5. （可选）在“团体名”中，输入SNMP Trap协议使用的团体名。

   “Trap版本”设置为“SNMPv1”或“SNMPv2c”时，才需要设置“团体名”。

   团体名是用作认证Trap SNMPv1/SNMPv2c协议的口令。
6. （可选）在“确认团体名”中，重复输入上一步骤输入的“团体名”，确认团体名输入正确。

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 Web中，最多可以定义四个发送告警通道。
2. 单击  ，显示指定通道的编辑区域框。
3. 单击  ，使能发送告警通道。

   当  按钮变为  ，表示启用该发送告警通道。
4. 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。
5. 输入接收Trap方式发送的告警信息的端口号。

   默认取值：162。
6. 选择Trap格式中每个关键字段之间的分隔符。
7. 选择需要上报的关键字。
8. 选择显示Trap格式中每个关键字的名称。
9. 单击“保存”。

   显示“操作成功”，表示Trap功能及其设置正式生效。
10. 单击“测试”。

    显示“操作成功”，表示该通道可用。

----结束

6.5 配置 iBMC WebUI SMTP

操作场景

iBMC WebUI的“告警设置”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，详细操作请参考3.1 登录iBMC WebUI。

步骤2 在iBMC WebUI，选择“告警与事件 > 告警设置”。

步骤3 在“告警邮件通知设置”区域框，单击 

，使能SMTP功能。

当 

按钮变为 

，表示启用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 设置接受告警的邮件地址。

单击 

，此按钮变为 

，表示启用该接受地址。

1. 输入接受告警邮件地址。
2. 输入接受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

6.6 配置 LDAP 功能

6.6.1 搭建 LDAP 服务器

iBMC当前支持与Windows AD和Linux OpenLDAP的对接，此处以Windows Server 2012 R2 Enterprise为例说明LDAP服务器的简要配置过程。如果已存在可正常使用的LDAP服务器，请忽略此章节。

前提条件

- 用于搭建LDAP服务器的设备（如华为服务器）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。

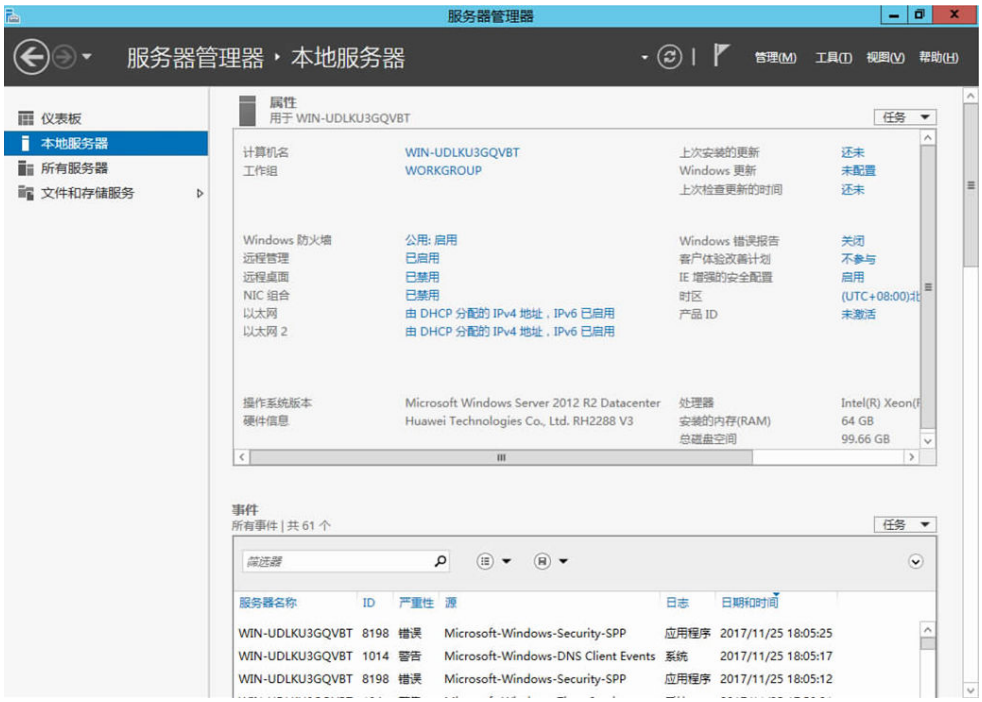
步骤2 安装DNS服务。

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。

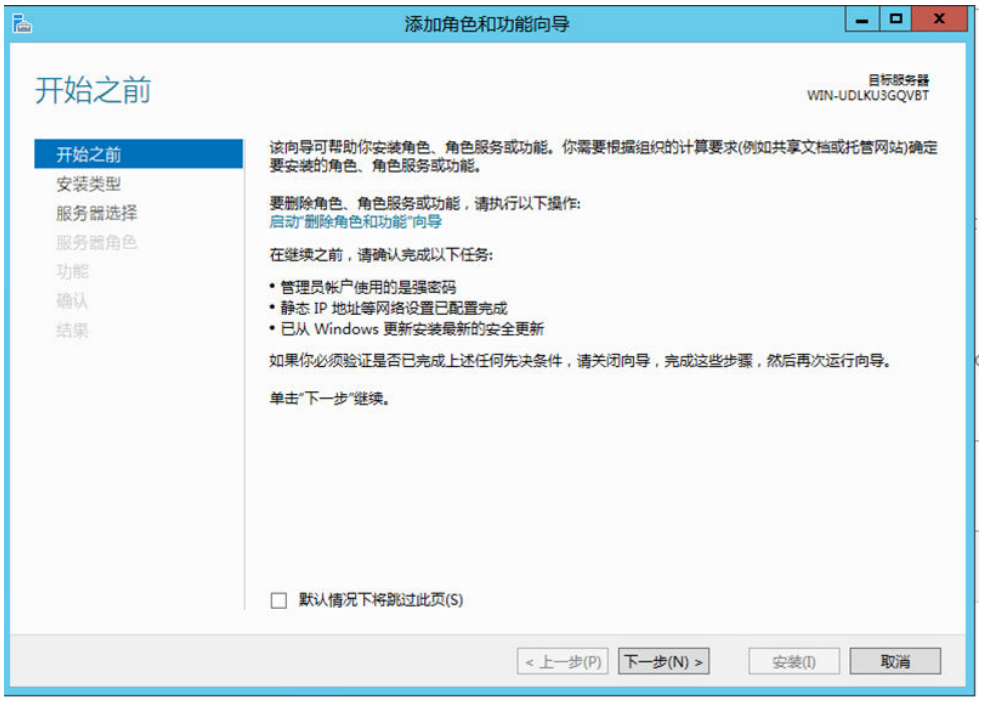
   图 6-3 本地服务器属性



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



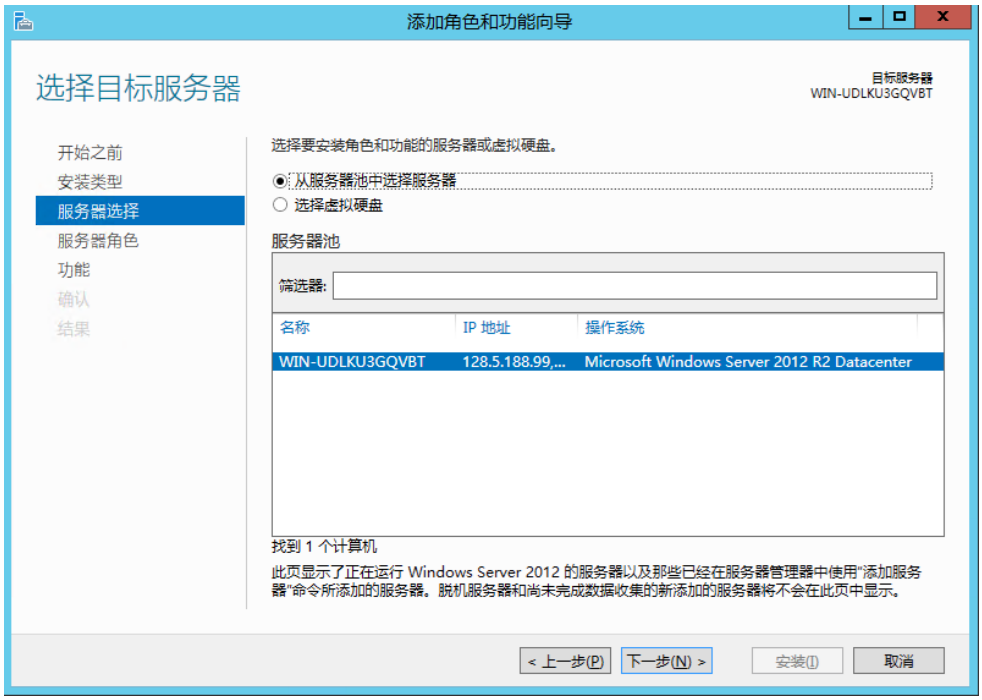
4. 单击“下一步”。

   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。

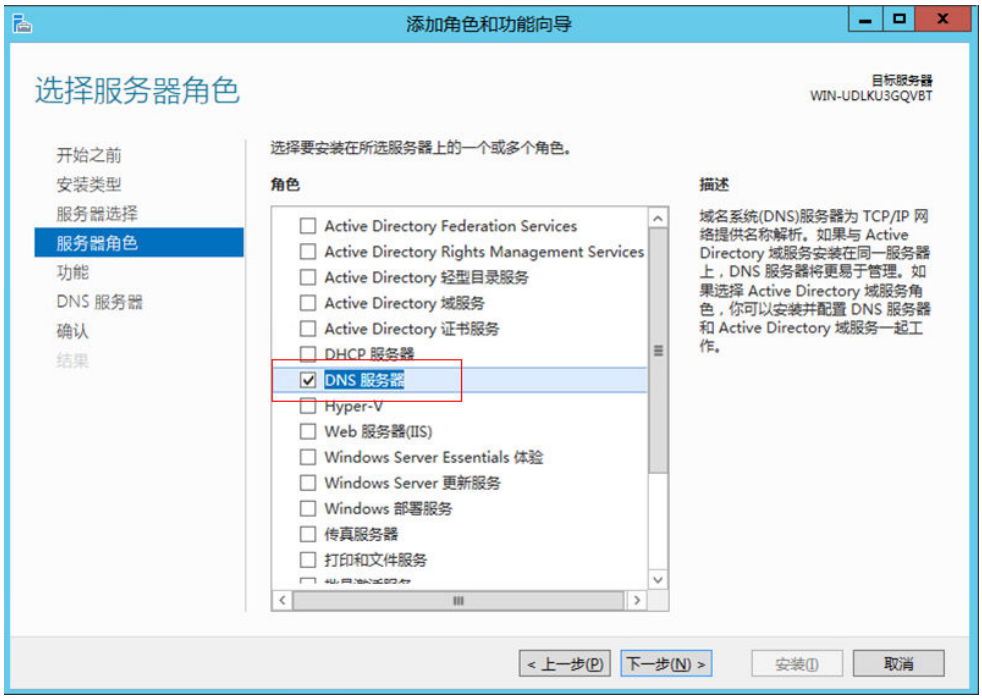
图 6-5 选择目标服务器



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6-6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。

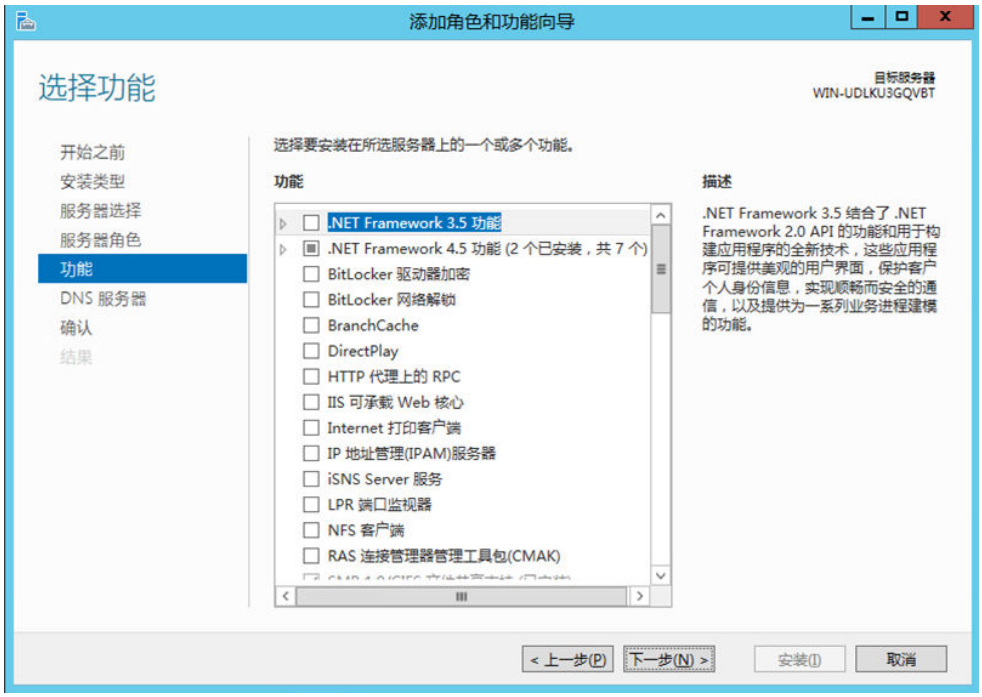
8. 单击“添加功能”。

   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**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”。

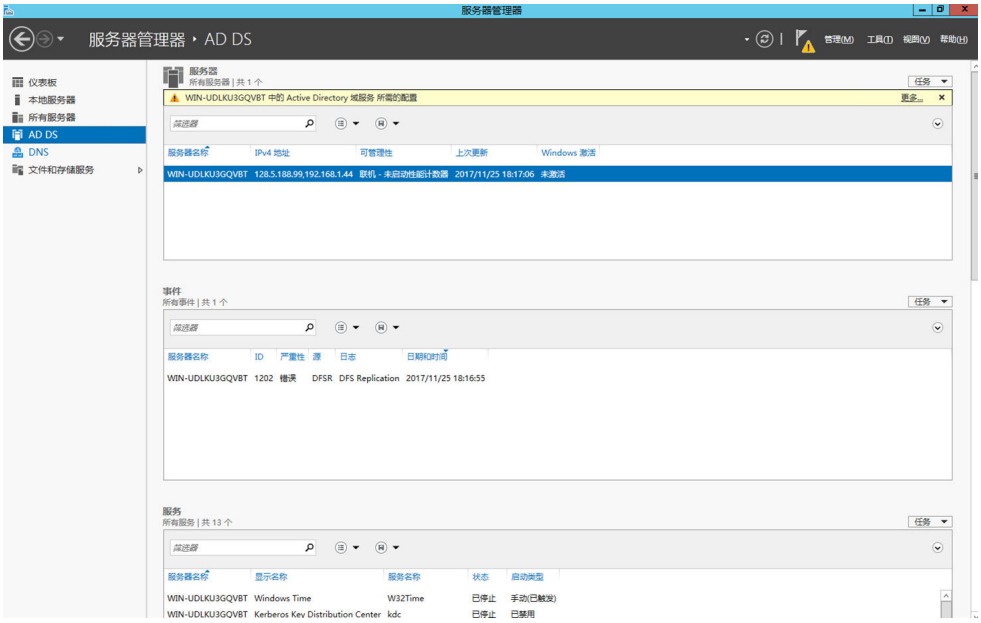
   返回“本地服务器”界面。

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...”。

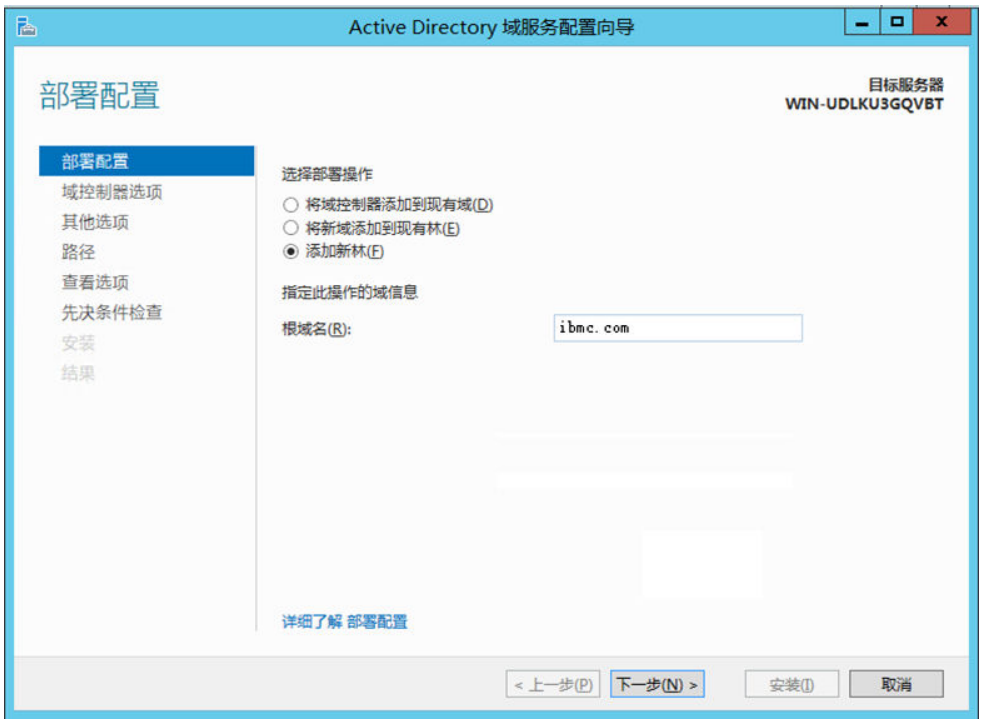
   打开“所有服务器任务详细信息”窗口，如图6-9所示。

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



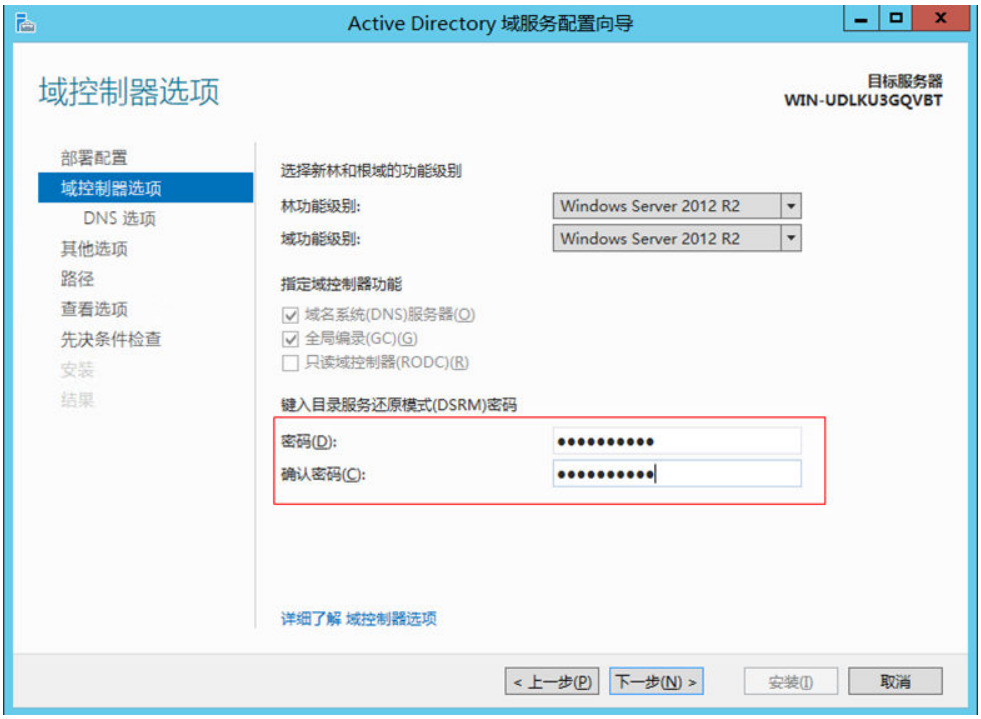
4. 选择“添加新林”并在“根域名”后的文本框中输入AD域名（例如“ibmc.com”），单击“下一步”。

   打开“域控制器选项”界面，如图6-11所示。

说明

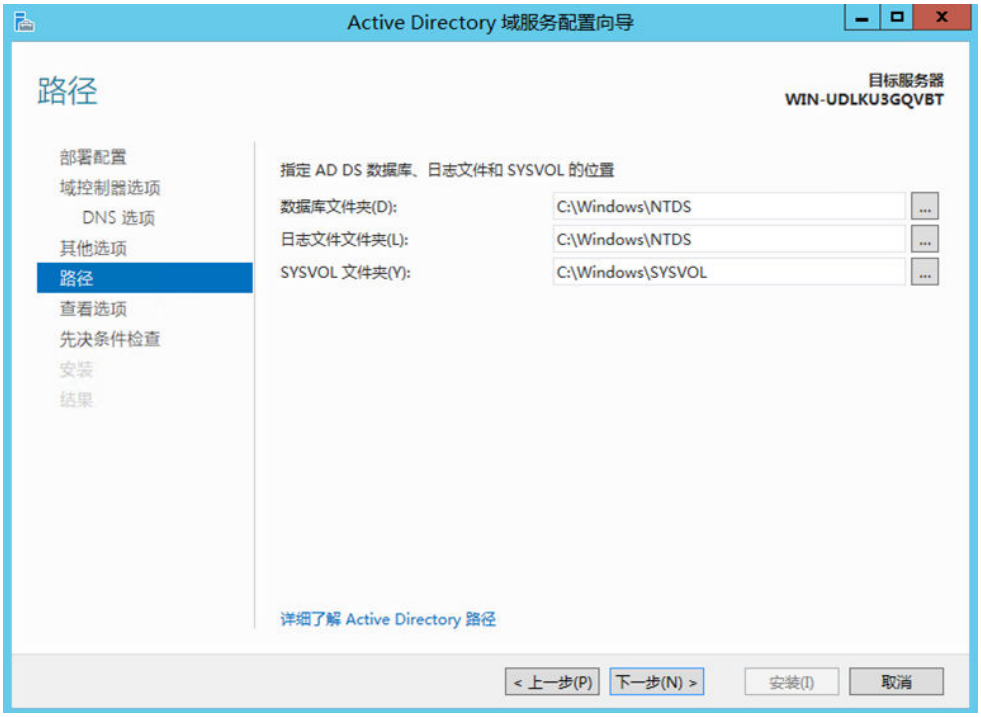
域名字符区分大小写，配置时请严格按照规划的域名来输入。

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 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。

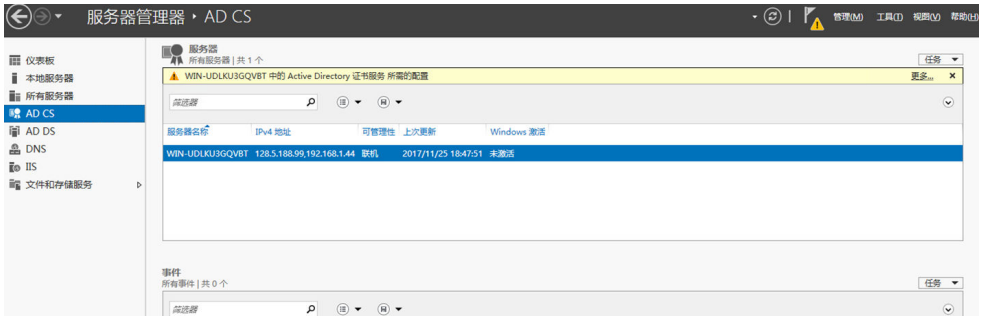
10. 安装完成后单击“关闭”。

步骤6 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6-13所示。

图 6-13 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6-14所示。

图 6-14 所有服务器任务详细信息

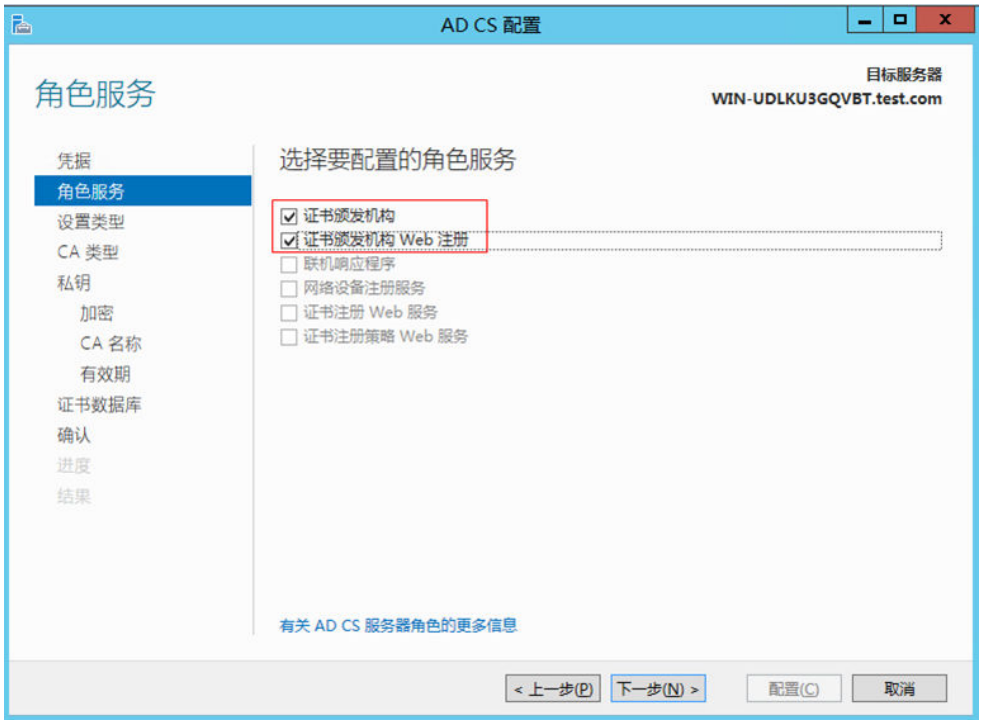
4. 单击“配置目标服务器上的Active Directory证书服务”。

   打开“AD CS配置”界面。

5. 单击“下一步”。

   打开“角色服务”界面，如图6-15所示。

图 6-15 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。

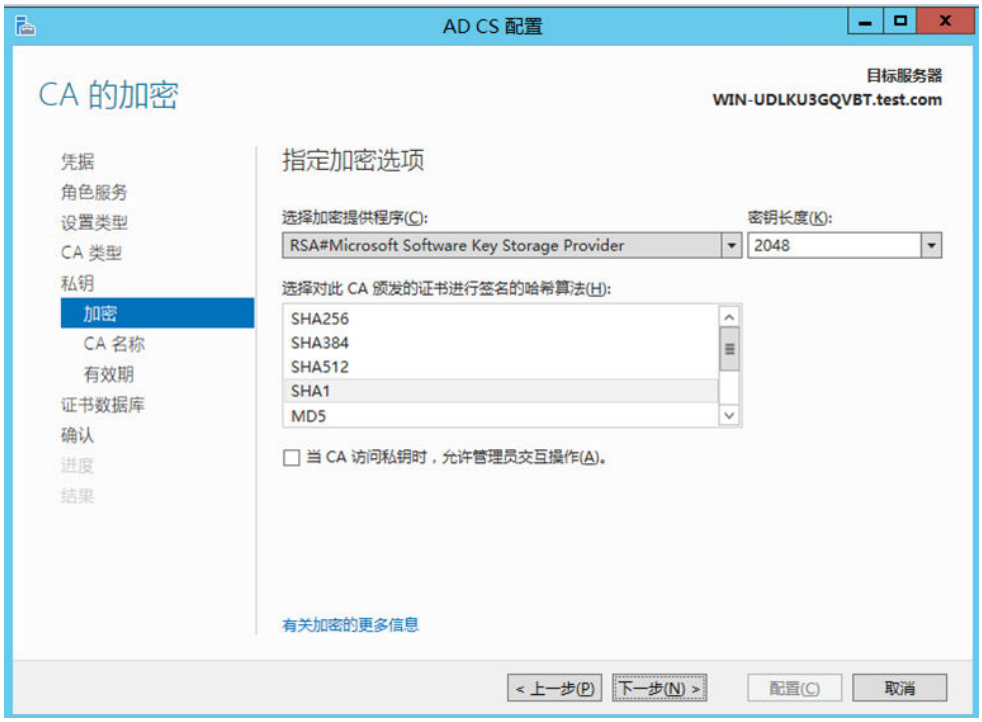
8. 勾选“根CA”，单击“下一步”。

   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6-16所示。

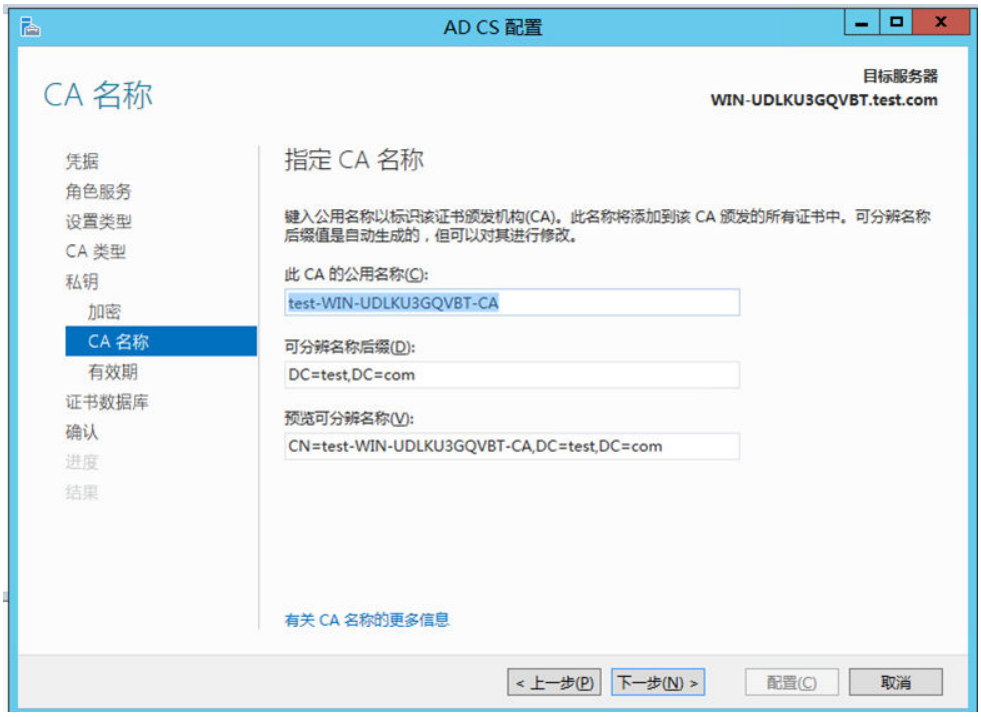
图 6-16 CA 的加密



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6-17所示。

图 6-17 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7 重启服务器使配置生效。

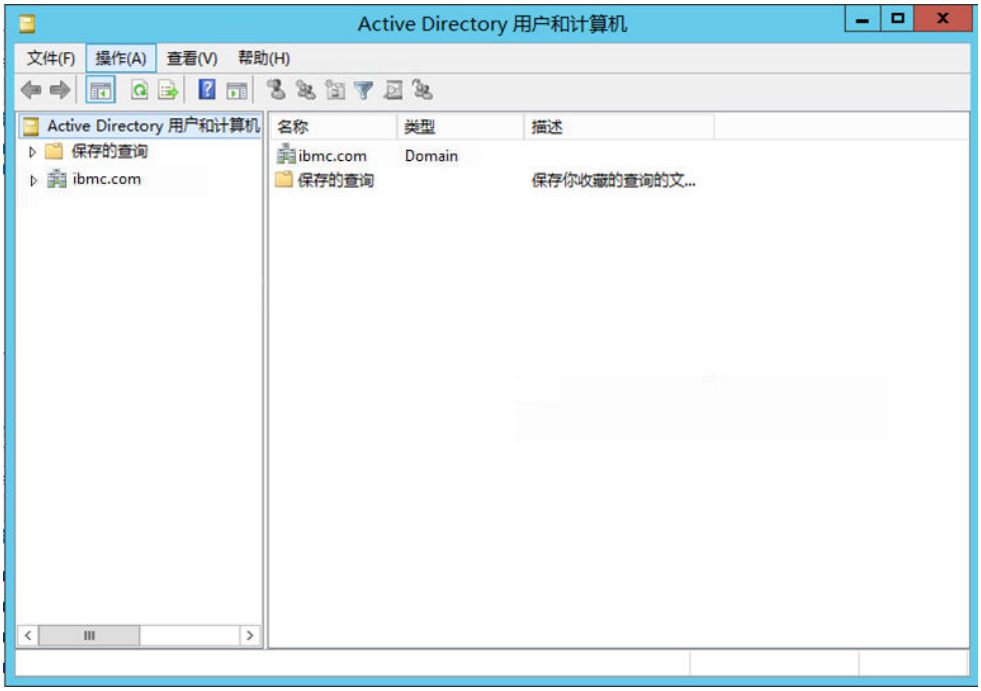
步骤8 新建组织单位。

您可以根据实际需要在LDAP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6-18所示。

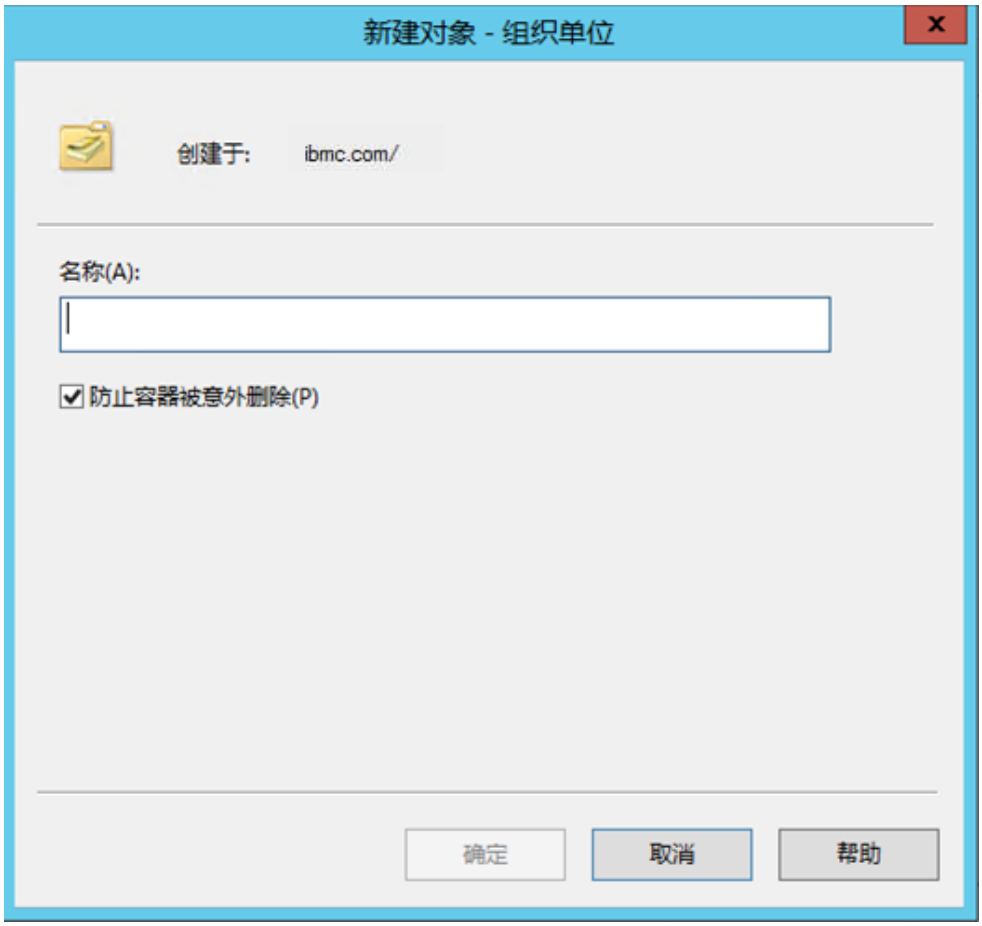
图 6-18 服务器管理器



4. 右键单击LDAP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6-19所示。

图 6-19 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LDAP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8.4**～**步骤8.6**，创建多个组织单位。

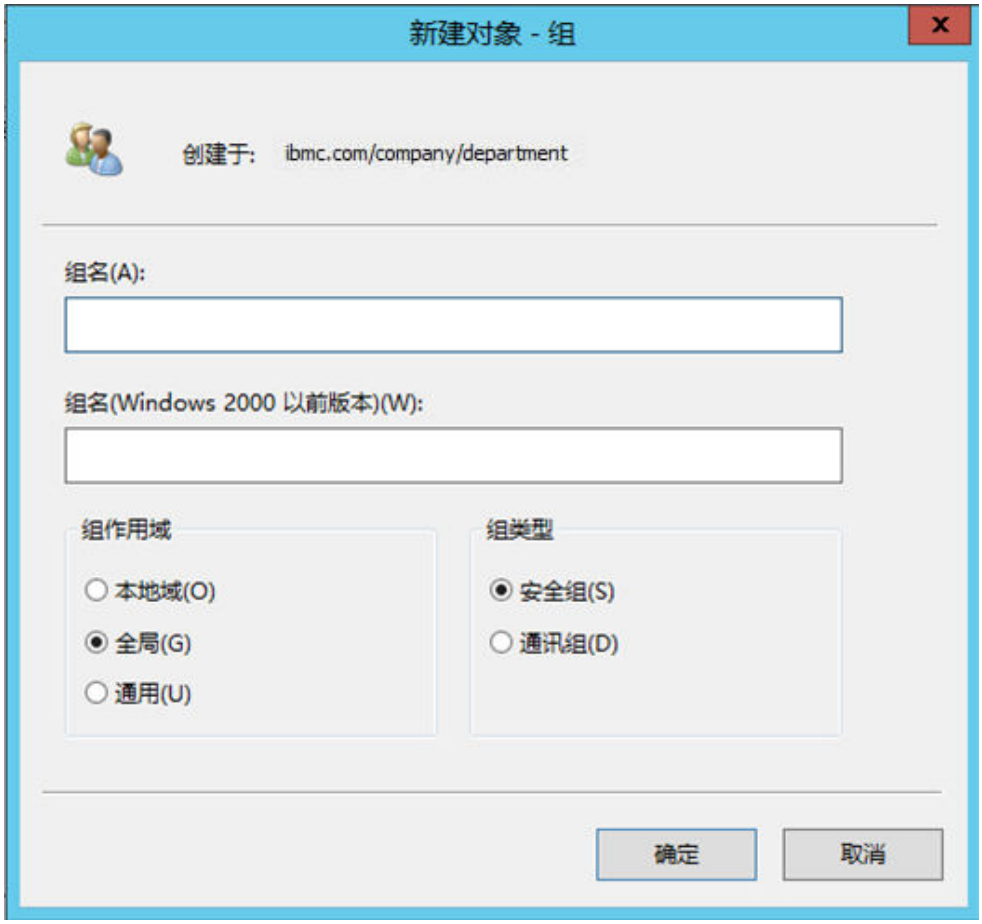
步骤9 新建LDAP组。

您可以根据实际需求，在任意节点下新建LDAP组。

1. 右键单击要创建LDAP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6-20所示。

图 6-20 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**步骤9.1**～**步骤9.2**，创建多个组。

步骤10 新建用户。

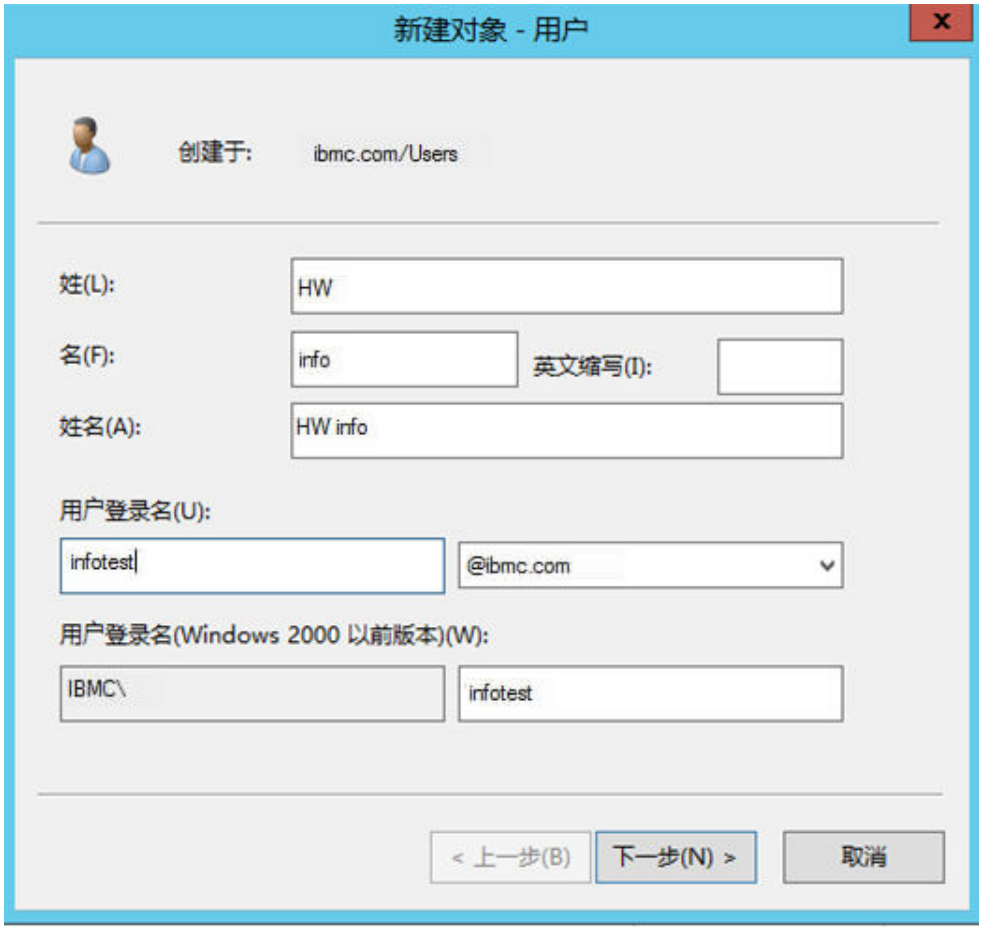
可以在所需的任何目录下新增用户。一般情况下，建议在“Users”下新建所需用户。

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6-21**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。

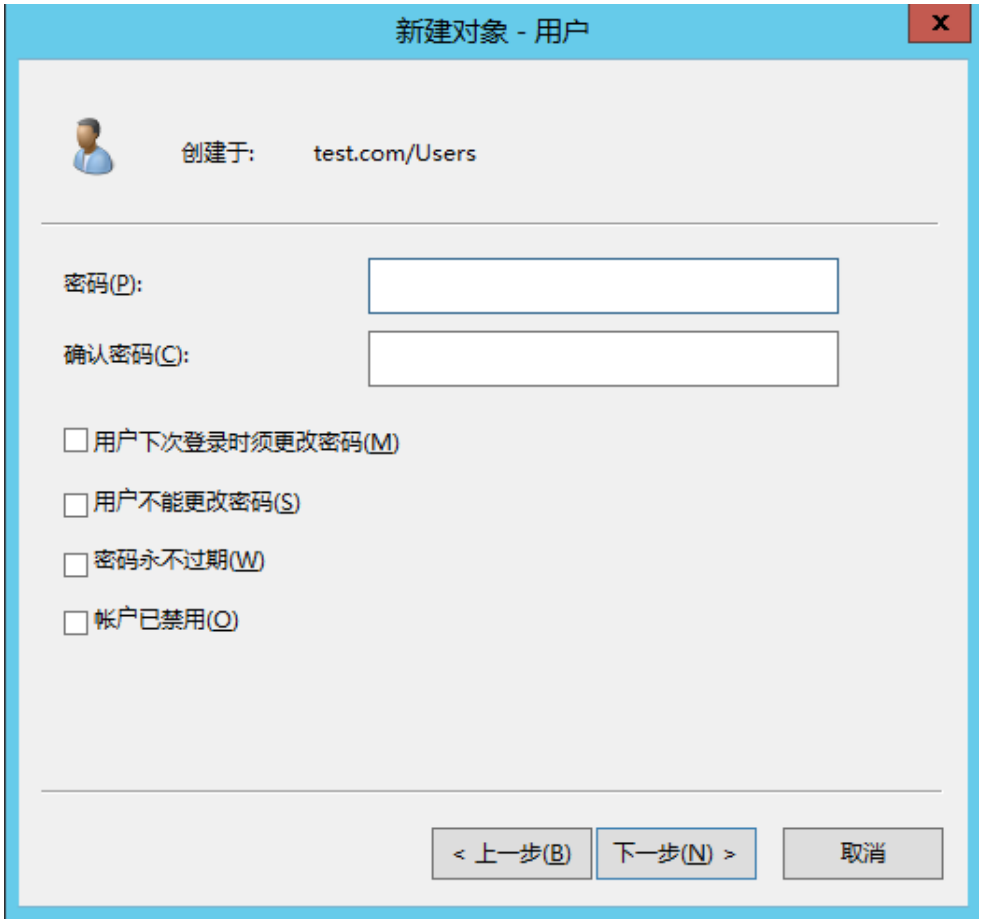
图 6-21 新建用户



3. 单击“下一步”。

   弹出密码设置窗口，如图6-22所示。

图 6-22 设置密码



4. 在“密码”和“确认密码”的文本框中输入密码（例如“Huawei12#$”），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“HWinfo”。

6. 重复上述操作，可在“Users”中新建更多用户。

步骤11 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（例如“HWinfo”）打开操作菜单，并选择“添加到组”。

打开选择组窗口，如**图6-23**所示。

图 6-23 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

6.6.2 在 iBMC 侧配置 LDAP 功能

操作场景

iBMC WebUI的“用户配置”提供“LDAP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。

必备事项

数据

- 可用的LDAP服务器信息。
  - LDAP服务器地址
  - LDAP服务器域名
  - LDAP服务器主机名

  - LDAP服务器的用户应用文件夹
- iBMC当前用户的密码。
- LDAP用户所属角色组的名称。

操作步骤

步骤1 3.1 登录iBMC WebUI。

步骤2 配置iBMC LDAP服务器信息。

1. 在iBMC WebUI，选择“配置 > LDAP配置”。
2. 单击“LDAP功能”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3.7.2 LDAP配置。
4. 单击“保存”。

步骤3 （可选）导入

1. 配置iBMC WebUI DNS地址为LDAP服务器地址，详细操作请参考6.7 配置iBMC WebUI DNS（手动）。
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。

步骤4 配置iBMC LDAP组信息

1. 在“LDAP组”区域单击  或  ，进入“LDAP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6.6.1 搭建LDAP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6.6.1 搭建LDAP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，例如“HWinfo/Huawei12#$”。
2. 在域名下拉列表，选择对应LDAP服务器的域名，例如“ibmc.com”。
3. 单击“登录”。

----结束

6.7 配置 iBMC WebUI DNS（手动）

操作场景

iBMC WebUI的“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“huawei”，域名为“manager.com”，那么域名地址为“huawei.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，详细操作请参考**3.1 登录iBMC WebUI**。

步骤2 在iBMC WebUI，选择“配置 > 网络配置”。

步骤3 在“设置iBMC主机名”区域框，设置iBMC主机名，如“huawei”。

步骤4 单击“保存”。

步骤5 在iBMC WebUI，选择“配置 > 网络配置”。

步骤6 在“配置DNS”区域框，单击“手动配置DNS地址”。

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7 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8 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9 使用域名登录iBMC WebUI。

说明

域名地址 = 主机名 + 域名。如：主机名为“huawei”，域名为“manager.com”，那么域名地址为“huawei.manager.com”

在浏览器输入域名地址，如“huawei.manager.com”，即可访问iBMC WebUI。

----结束

6.8 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”。

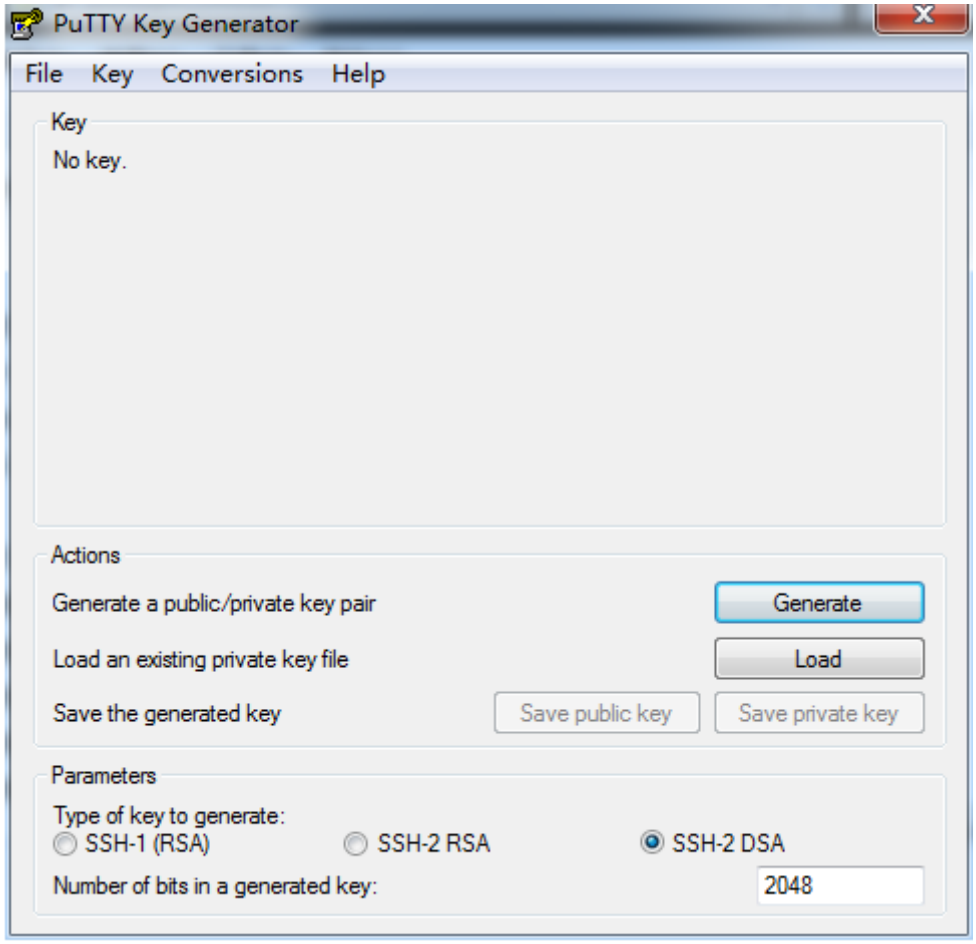
上述工具为免费工具，请自行在互联网搜索下载。

操作步骤

生成SSH密钥

1 在客户端（例如PC）打开密钥生成工具（例如“puttygen.exe”），如图6-24所示。

图 6-24 密钥生成界面



2 在“Parameters”区域中选择密钥类型，例如“SSH-2 DSA”。

3 设置密钥容量。

说明

基于安全考虑，此处建议将密钥容量设置为2048及以上。

4 单击“Generate”生成密钥。

5 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

6 登录iBMC WebUI，详细操作请参考3.1 登录iBMC WebUI。

7 在iBMC WebUI，选择“配置 > 本地用户”。

8 在“SSH公钥管理”区域单击“添加”。

弹出导入SSH公钥的窗口，如图6-25所示。

图 6-25 导入 SSH 公钥

9 输入当前用户的用户名。

10 选择要导入公钥的SSH用户名。

11 选择公钥导入方式为“文件导入”。

此处可根据实际情况调整导入方式。

12 单击“浏览”选择**生成SSH密钥**生成的公钥。

13 单击“保存”。

导入成功后，界面提示导入公钥成功。

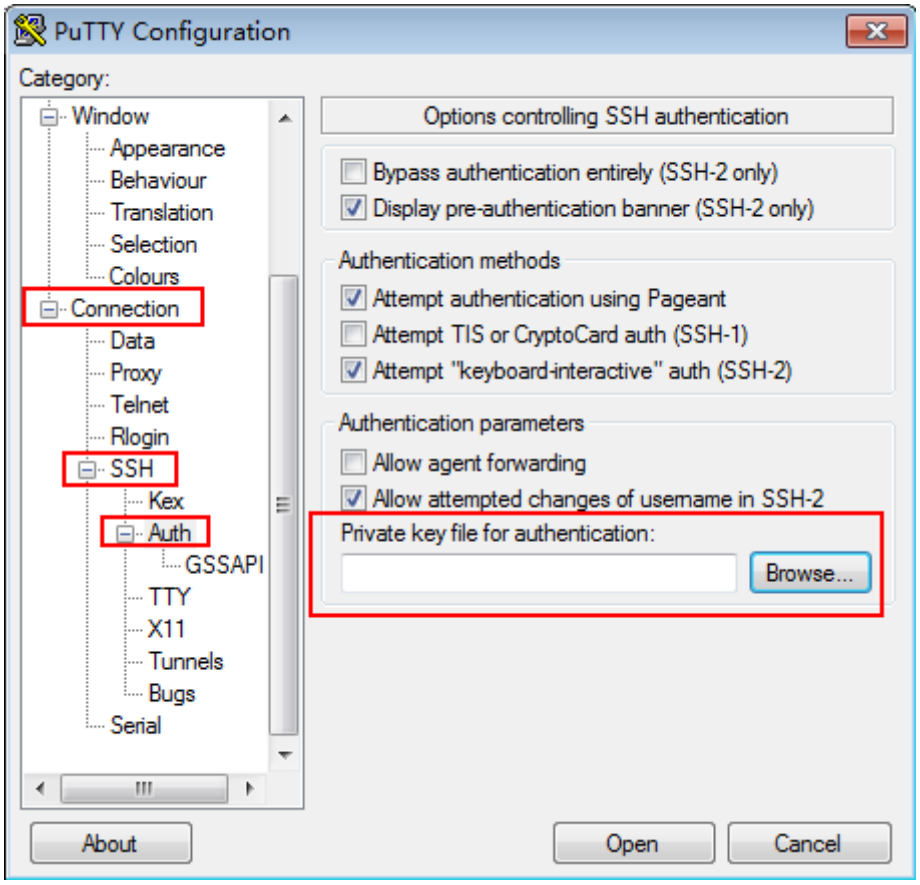
配置SSH客户端

14 在客户端打开登录工具（例如“putty.exe”）。

15 导入**生成SSH密钥**生成的私钥。

私钥导入界面如**图6-26**所示。

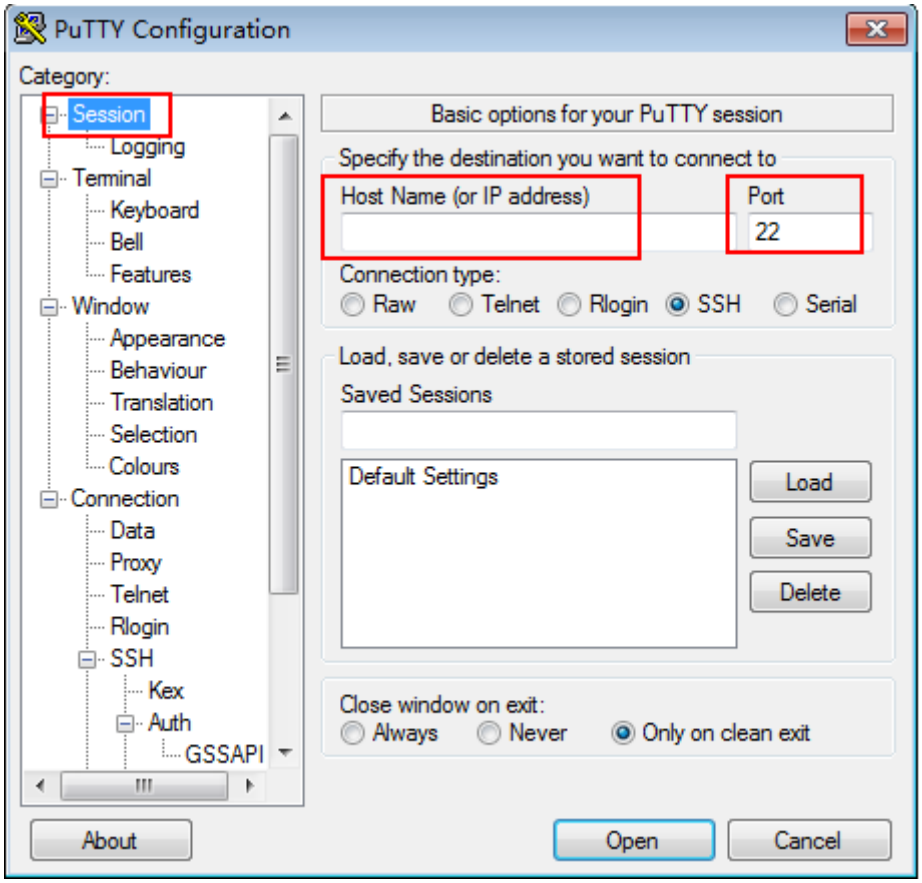
图 6-26 导入私钥



16 配置SSH客户端登录信息。

登录信息配置界面如图6-27所示，需要输入iBMC地址、SSH服务端口号。

图 6-27 配置登录信息



登录iBMC命令行

17 单击“Open”。

18 按提示信息输入SSH用户名。

进入iBMC命令行。

----结束

6.9 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

详细操作请参考**3.1 登录iBMC WebUI**。

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**自定义证书信息**、**申请SSL证书**、**导入SSL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

1 在iBMC WebUI，选择“配置 > SSL证书”。
2 单击“自定义”打开自定义SSL信息的界面。
3 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。

4 单击“保存”。
5 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

6 在“SSL证书”界面单击“自定义”。
7 （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”。

导入后，会返回“证书导入成功,复位iBMC后生效”信息。

8 （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“证书导入成功,复位iBMC后生效”信息。

9 重启iBMC。

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。

10 打开浏览器。

11 在工具栏中选择“工具 > Internet选项”。

弹出“Internet选项”窗口。

12 在“内容”页签中单击“证书”。

打开“证书”窗口。

13 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 => **14**
- 否 => **15**

14 查看证书是否过期。

- 是 => **15**
- 否 => **16**

15 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。

16 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

----结束

6.10 配置 iBMC Syslog 日志上报功能

操作场景

iBMC WebUI的“告警设置”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。

步骤3 登录iBMC WebUI

详细操作请参考**3.1 登录iBMC WebUI**。

步骤4 配置syslog属性

1. 在iBMC WebUI，选择“告警与事件 > 告警设置”。
2. 在“告警Syslog报文通知设置”区域框，单击 

，使能syslog报文上报功能。

   当 

按钮变为 

，表示启动syslog报文上报功能。
3. 按照界面信息配置“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3-24**。
4. 上传证书。
   - 当“认证方式”为“单向认证”时，将**生成证书**步骤中生成的**服务器根证书**上传到iBMC。
   - 当“认证方式”为“双向认证”时，将**生成证书**步骤中生成的**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  ，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

6.11 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

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。详细操作请参考**3.1 登录iBMC WebUI**。

2 在iBMC WebUI，选择“配置 > 服务配置”。

3 使能VNC服务，并设置端口号。VNC右侧的按钮设置为 

时为开启VNC服务。VNC服务默认为关闭状态，默认端口号为“5900”。

配置VNC属性

4 在iBMC WebUI，选择“远程控制”。

5 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。

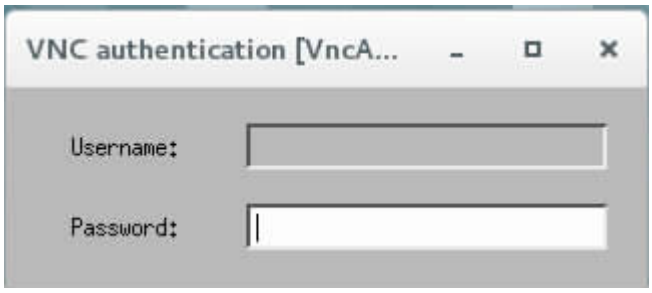
（可选）Linux客户端使用TigerVNC登录服务器实时桌面

6 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6-28所示。

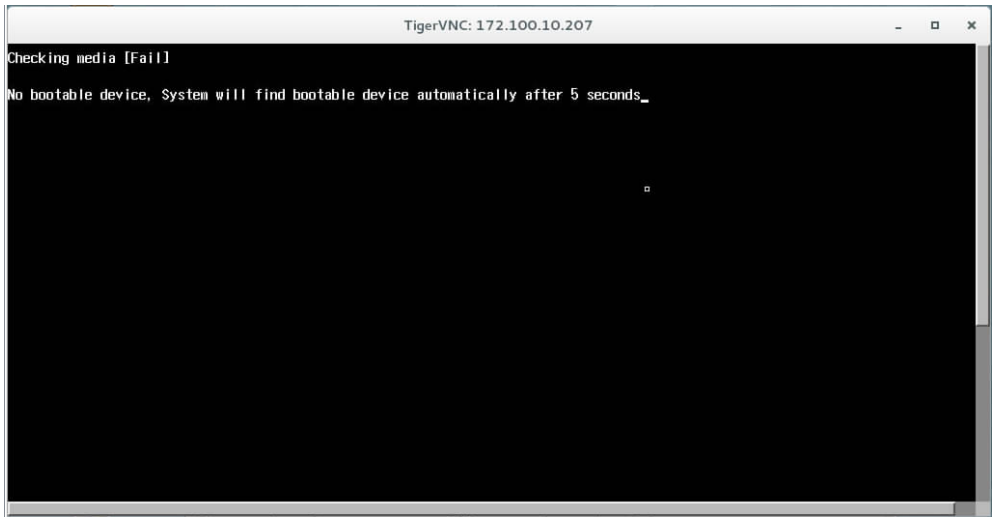
图 6-28 TigerVNC 登录窗口



7 输入5中设置的密码，并按“Enter”。

登录服务器实时桌面，如图6-29所示。

图 6-29 服务器实时桌面

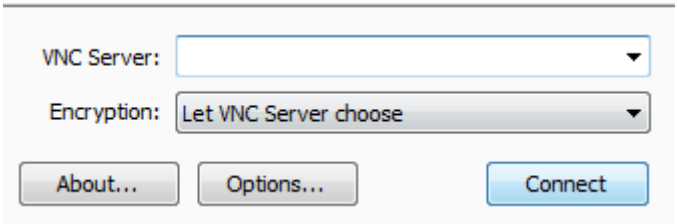


（可选）Windows客户端使用RealVNC登录服务器实时桌面

8 在客户端双击RealVNC客户端软件。

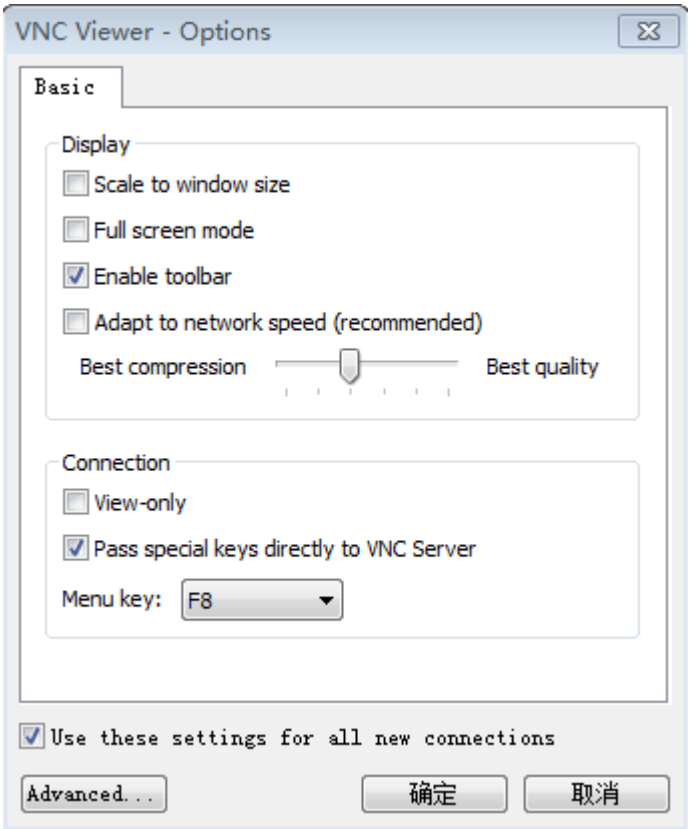
打开RealVNC登录窗口，如图6-30

图 6-30 RealVNC 登录窗口



9 单击“Options”，打开参数设置界面，如图6-31。

图 6-31 RealVNC 客户端参数设置界面



10 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。

11 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。

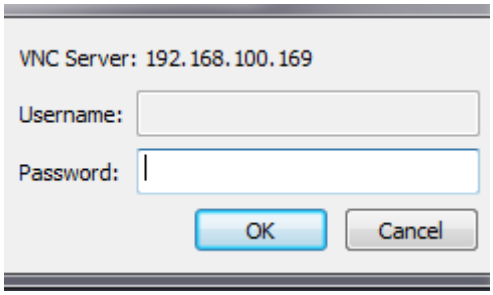
地址格式为“管理网口IP地址（IPv4地址或IPv6地址）:端口号”，例如“192.168.100.169:5900”。

12 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6-32。

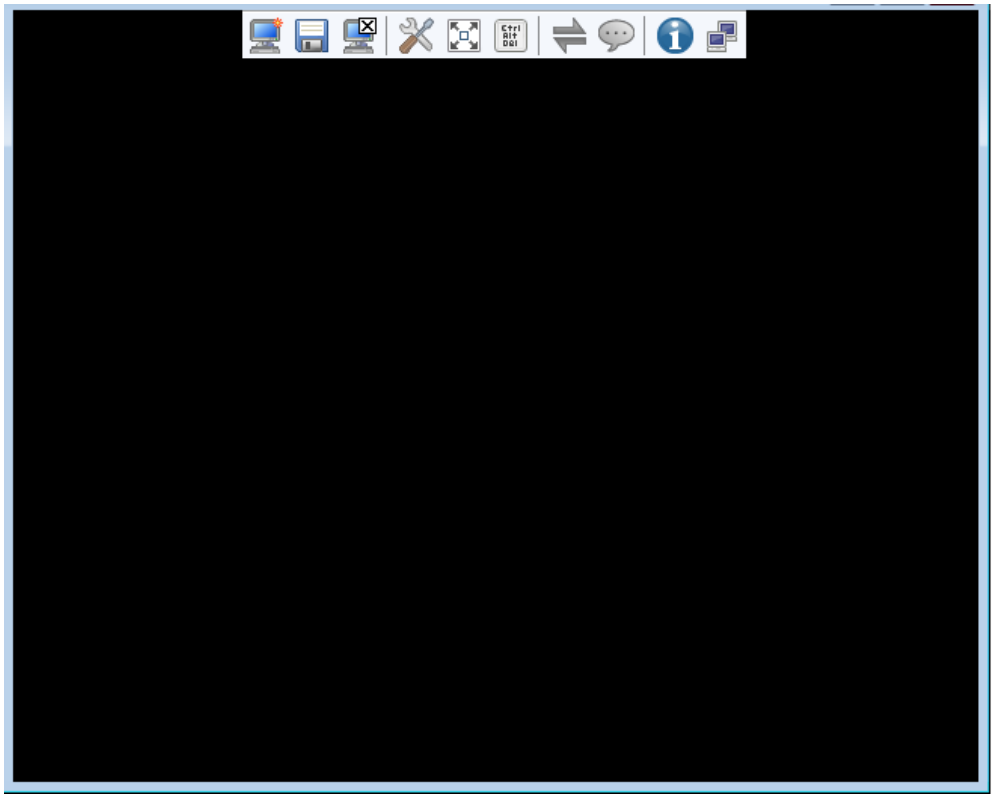
图 6-32 RealVNC 客户端身份认证窗口



13 在“Password”右侧的文本框中输入5中设置的密码，并单击“OK”。

登录服务器实时桌面，如图6-33。

图 6-33 服务器实时桌面



----结束

6.12 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

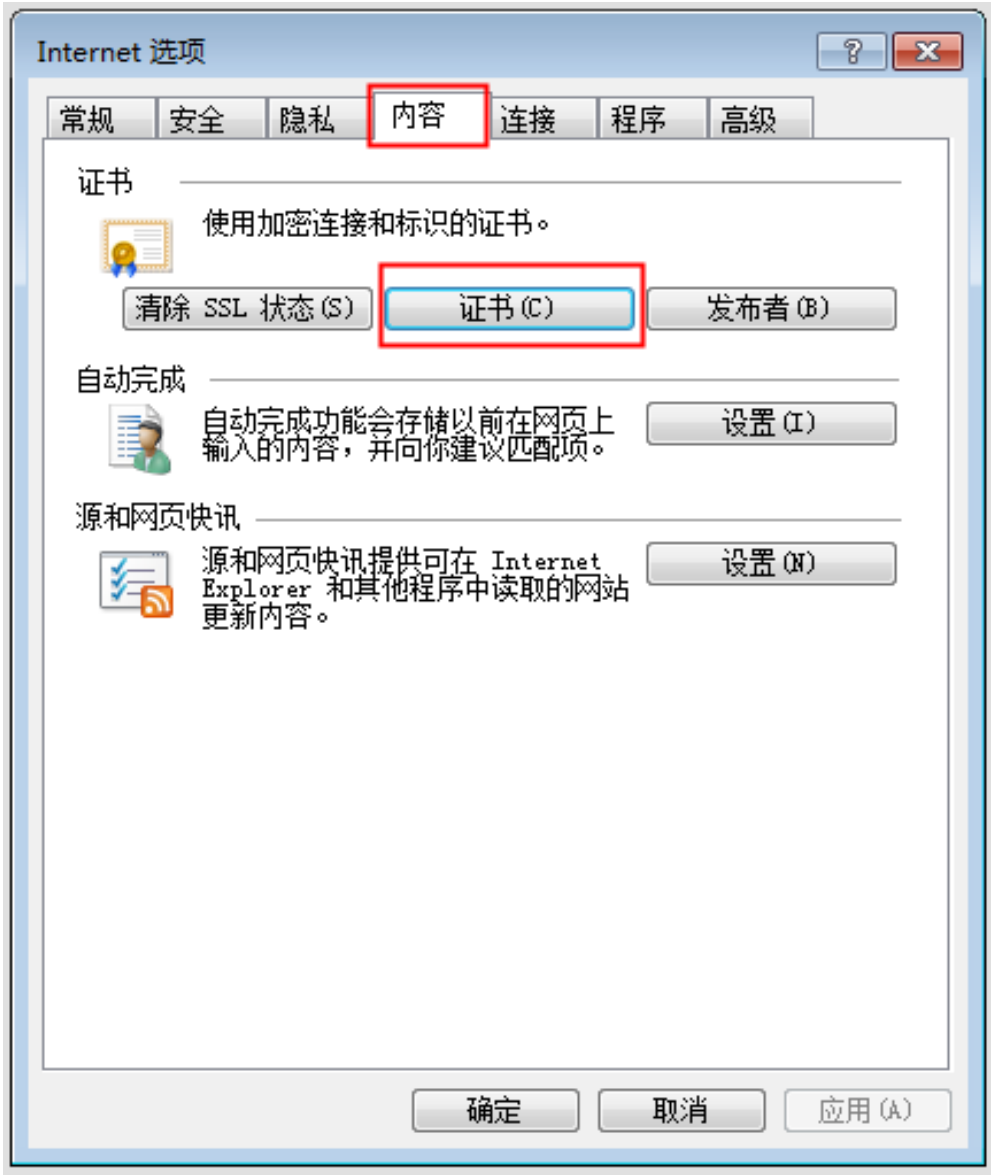
操作步骤

导入信任证书

1 打开IE浏览器，单击  。

弹出Internet选项窗口如**图6-34**。

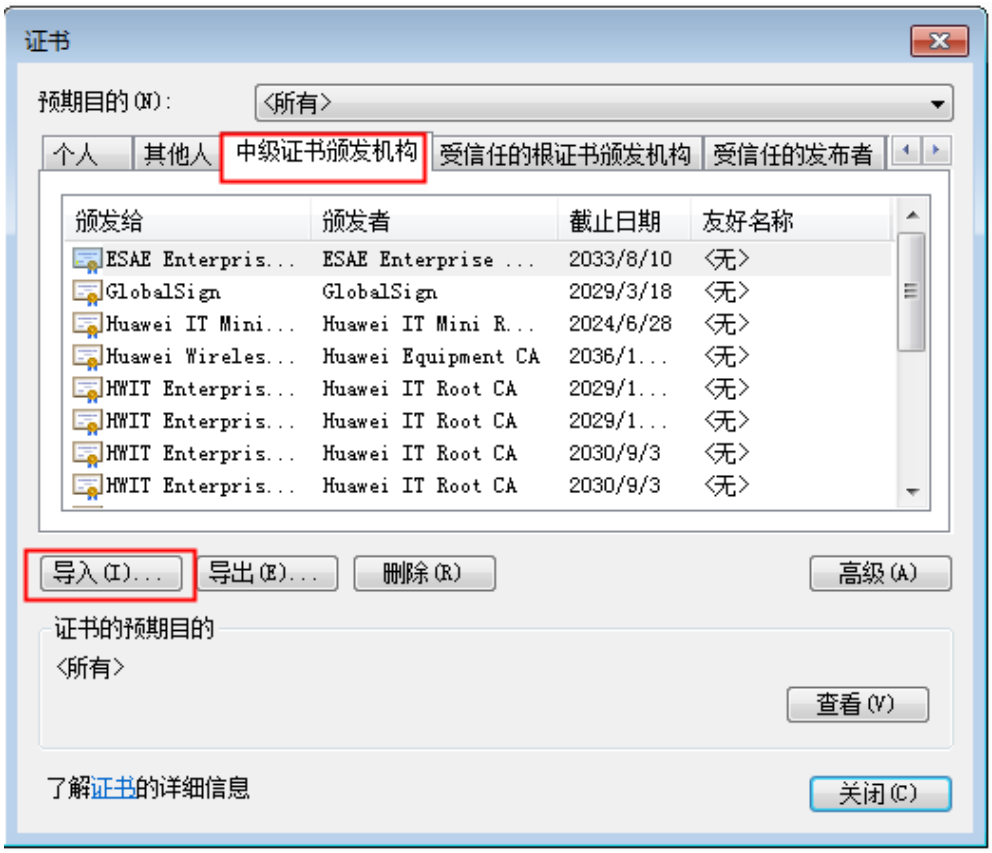
图 6-34 Internet 选项窗口



2 单击“内容 > 证书”。

弹出导入证书窗口如图6-35。

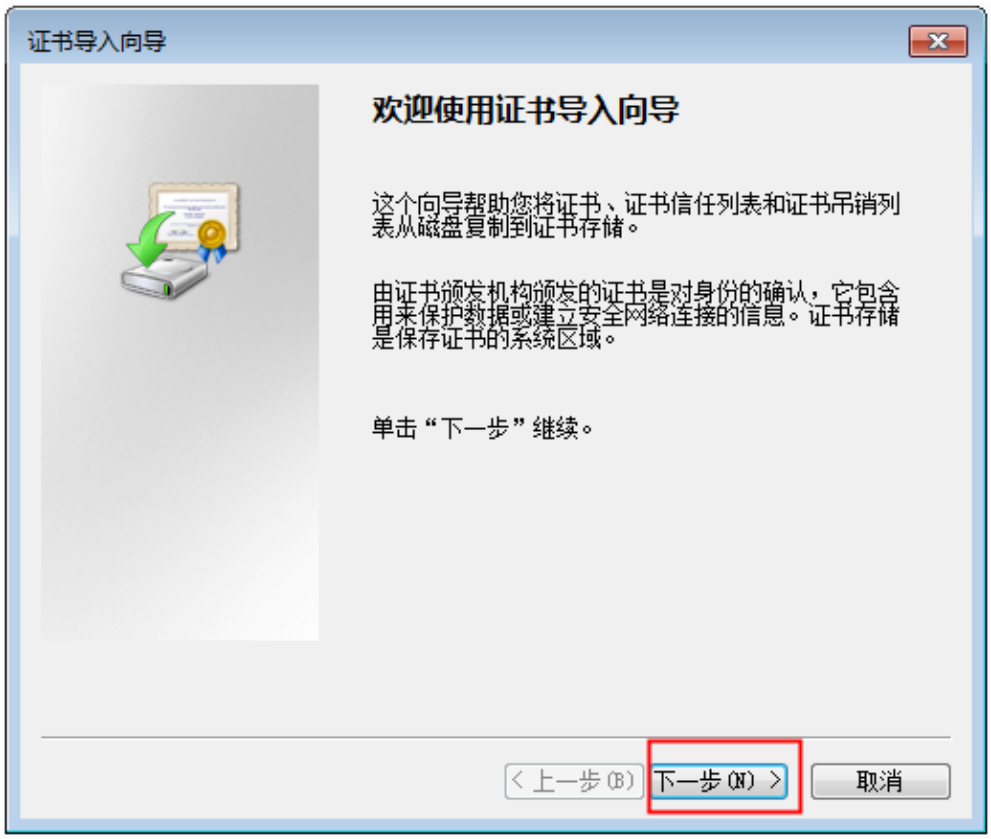
图 6-35 导入证书窗口



3 单击“中级证书颁发机构 > 导入”。

弹出证书导入向导窗口如图6-36。

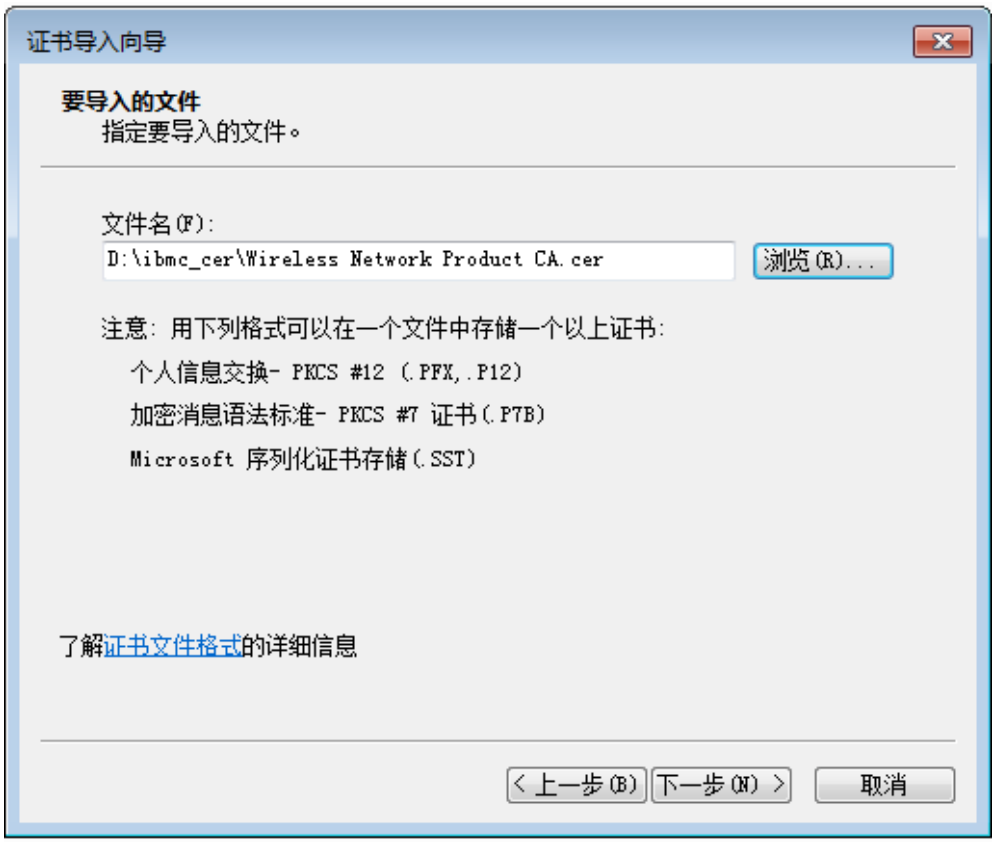
图 6-36 导入证书窗口



4 单击“下一步”继续。

弹出选择证书窗口如图6-37。

图 6-37 选择证书窗口



5 单击“浏览”，从本地PC路径中选择待上传的证书。

6 单击“下一步”继续。

在弹出的选择证书存储位置窗口图6-38中选择证书的存放位置。

图 6-38 选择证书存储位置窗口

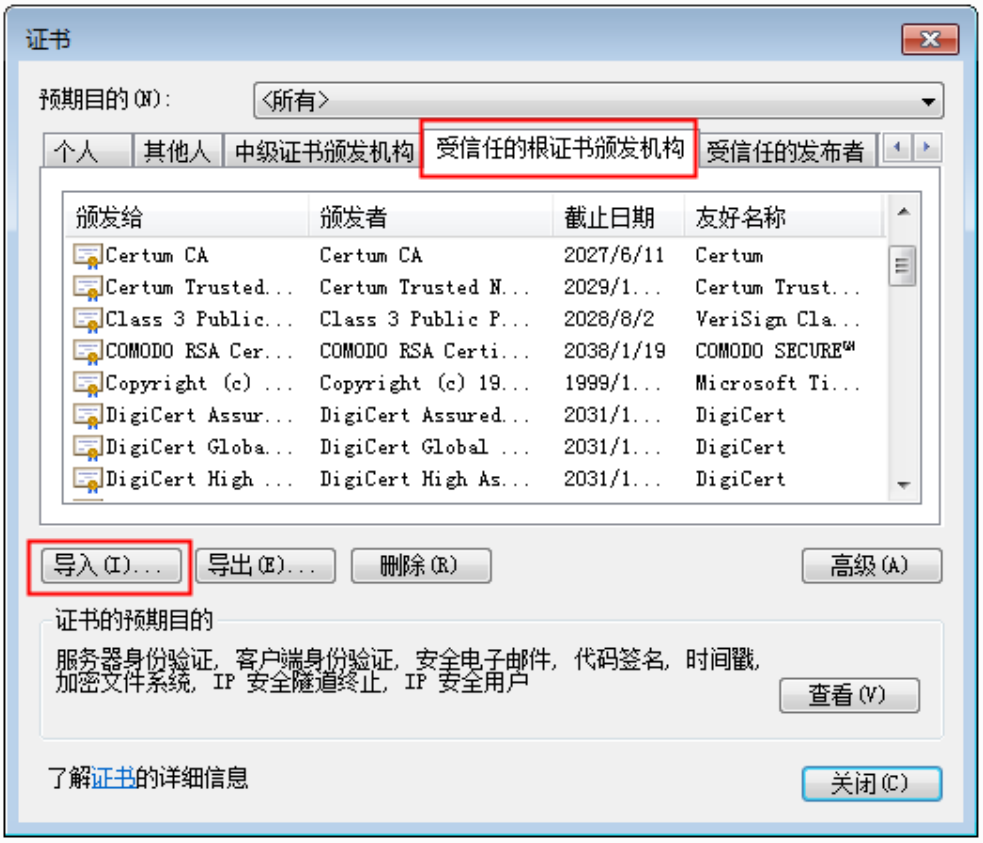
7 单击“下一步 > 完成”。
弹出“导入成功”提示框。则表示成功导入证书。

8 单击“确定”完成证书导入。

导入根证书

9 重复以上**步骤1**和**步骤2**，打开弹出导入证书窗口，如**图6-39**。

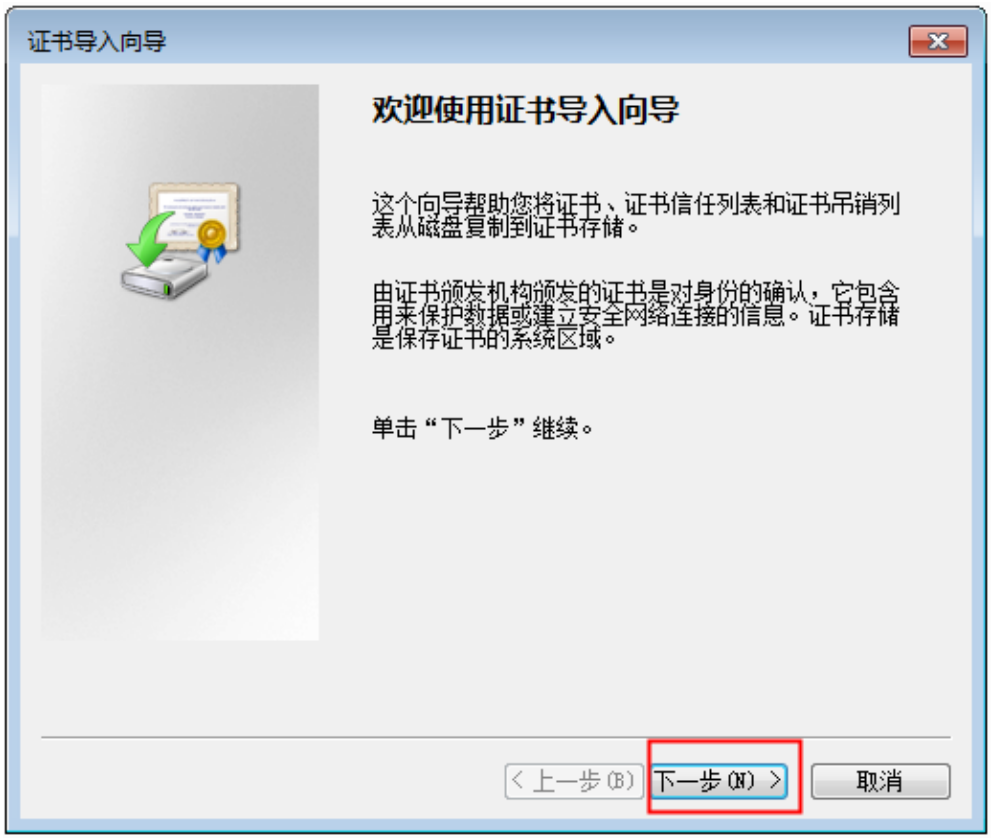
图 6-39 导入证书窗口



10 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6-40。

图 6-40 导入证书窗口



11 重复以上**步骤4** ~ **步骤8**，完成根证书导入。

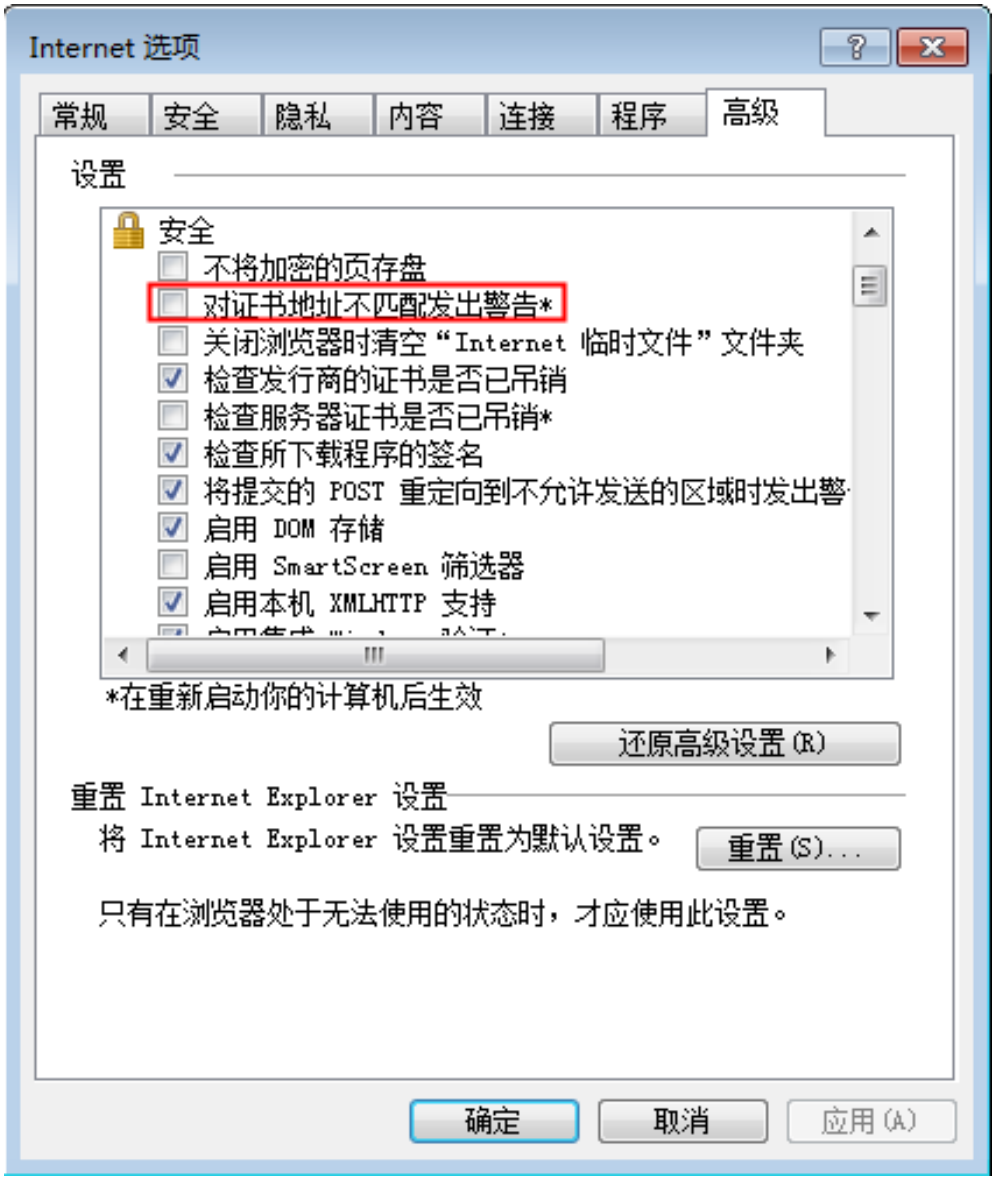
取消勾选“对证书地址不匹配发出警告”

此操作需要重启计算机后才能生效。

12 单击“ > Internet 选项 > 高级”。

弹出Internet选项窗口如**图6-41**。

图 6-41 Internet 选项窗口



13 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。

----结束

7 独立远程控制台

7.1 简介
7.2 （Windows）使用独立远程控制台登录服务器实时桌面
7.3 （Ubuntu）使用独立远程控制台登录服务器实时桌面
7.4 （Mac）使用独立远程控制台登录服务器实时桌面
7.5 （Redhat）使用独立远程控制台登录服务器实时桌面

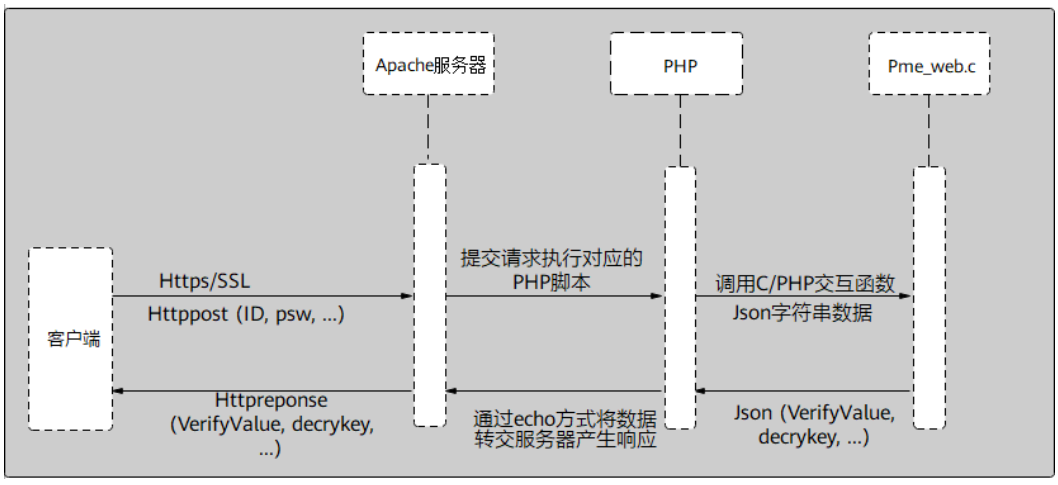
7.1 简介

独立远程控制台是基于华为服务器管理软件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

软件包	操作系统类型	版本
kvm_client_windows.zip	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
kvm_client_ubuntu.zip	Ubuntu	Ubuntu 14.04 LTS
		Ubuntu 16.04 LTS
kvm_client_mac.zip	Mac OS	Mac OS X El Capitan
kvm_client_linux.zip	Redhat	Redhat 6.9
		Redhat 7.3

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

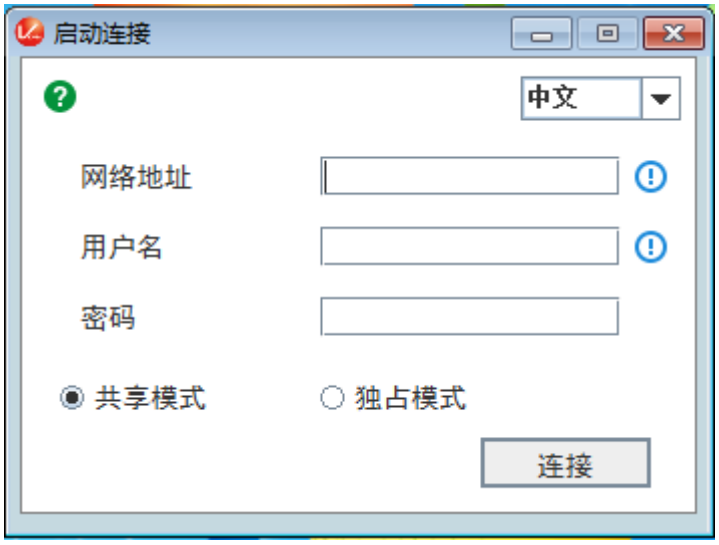
独立远程控制台软件包已下载到客户端（例如PC）并解压。

操作步骤

步骤1 配置客户端（例如PC）IP地址，使其与iBMC管理网口在同一网段。

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

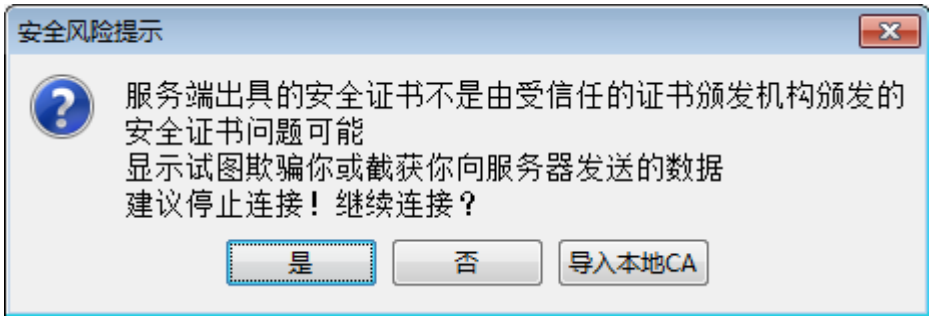
- iBMC V228之前版本仅支持本地用户登录，iBMC V228及之后版本支持本地用户及LDAP域用户登录。
- iBMC V228之前版本端口号对应RMCP+服务端口号，iBMC V228及之后版本端口号对应HTTPS服务端口号。
- 输入IPv6地址时，必须使用[ ]将其括起来，而IPv4地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认时，“网络地址”中可不加端口号。

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

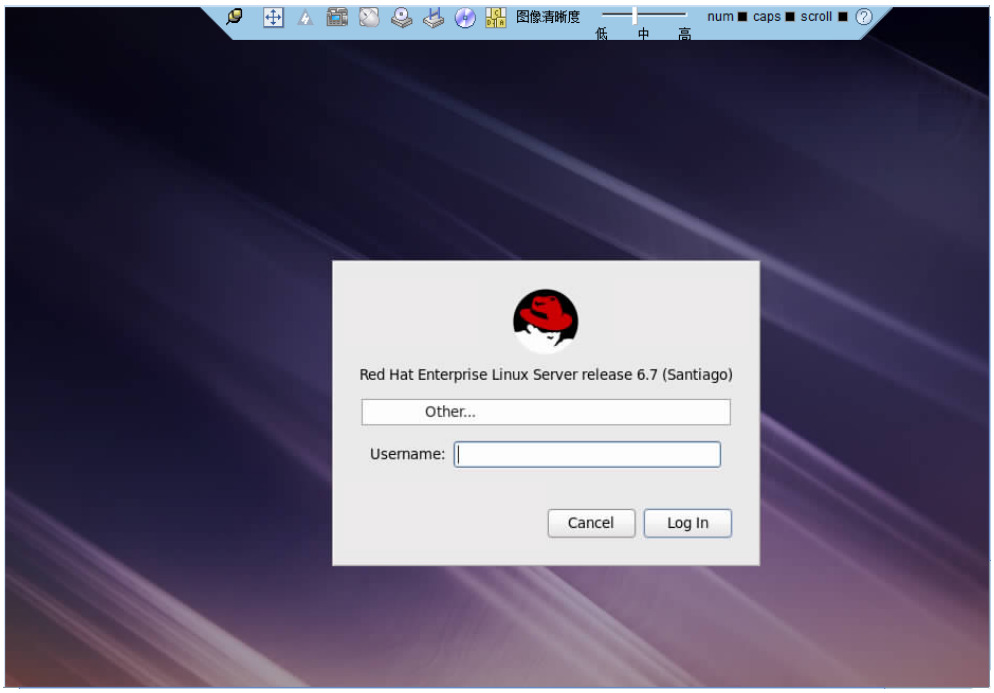


步骤5 按照实际需要单击确认按钮。

- 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。

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管理网口在同一网段。

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 777 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

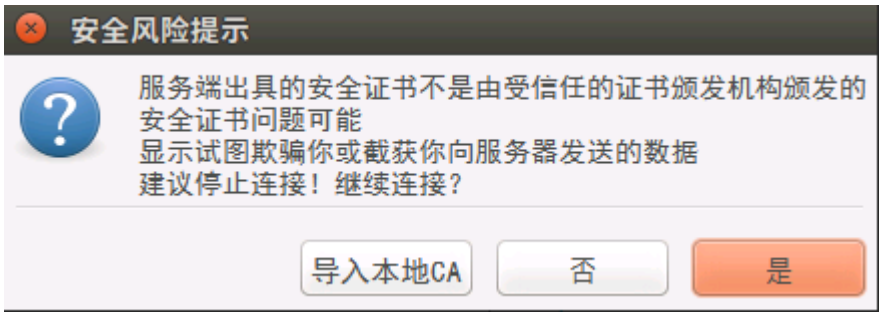
- iBMC V228之前版本仅支持本地用户登录，iBMC V228及之后版本支持本地用户及LDAP域用户登录。
- iBMC V228之前版本端口号对应RMCP+服务端口号，iBMC V228及之后版本端口号对应HTTPS服务端口号。
- 输入IPv6地址时，必须使用[ ]将其括起来，而IPv4地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认时，“网络地址”中可不加端口号。

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

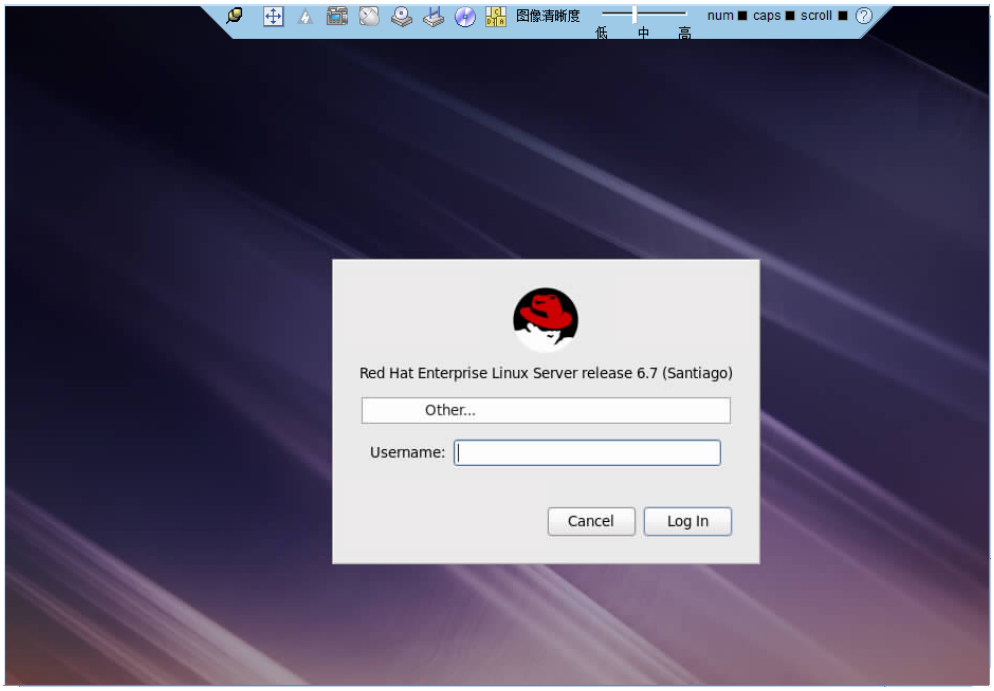


步骤7 按照实际需要单击确认按钮。

- 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。

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管理网口在同一网段。

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 777 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

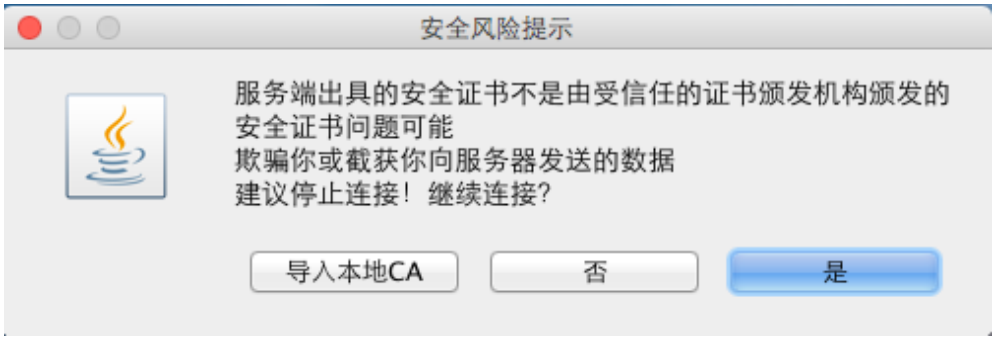
- iBMC V228之前版本仅支持本地用户登录，iBMC V228及之后版本支持本地用户及LDAP域用户登录。
- iBMC V228之前版本端口号对应RMCP+服务端口号，iBMC V228及之后版本端口号对应HTTPS服务端口号。
- 输入IPv6地址时，必须使用[ ]将其括起来，而IPv4地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认时，“网络地址”中可不加端口号。

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

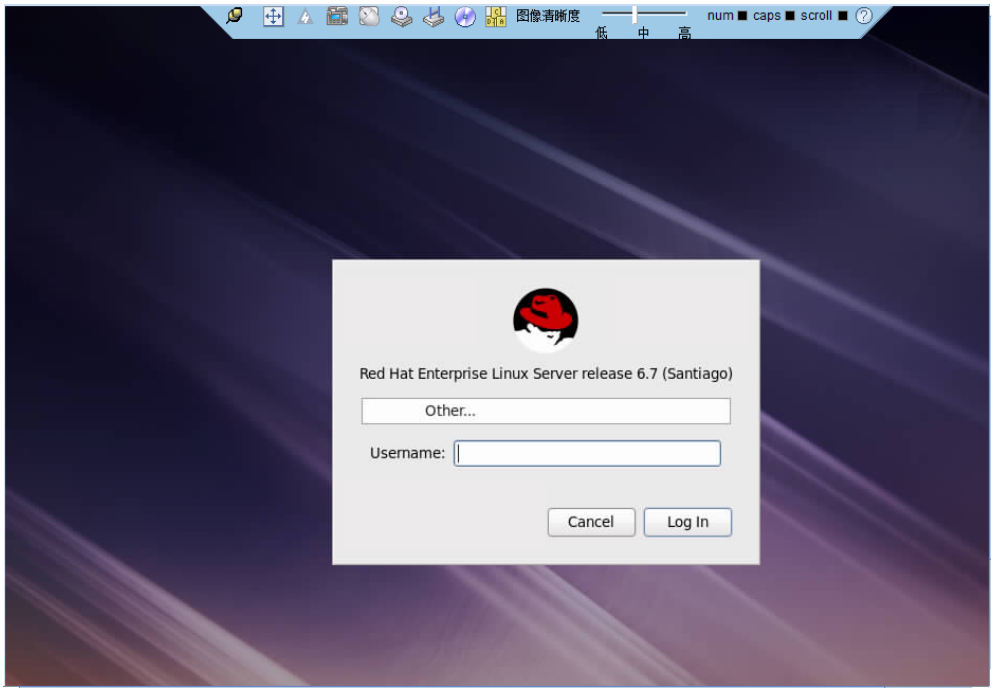


步骤7 按照实际需要单击确认按钮。

- 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。

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

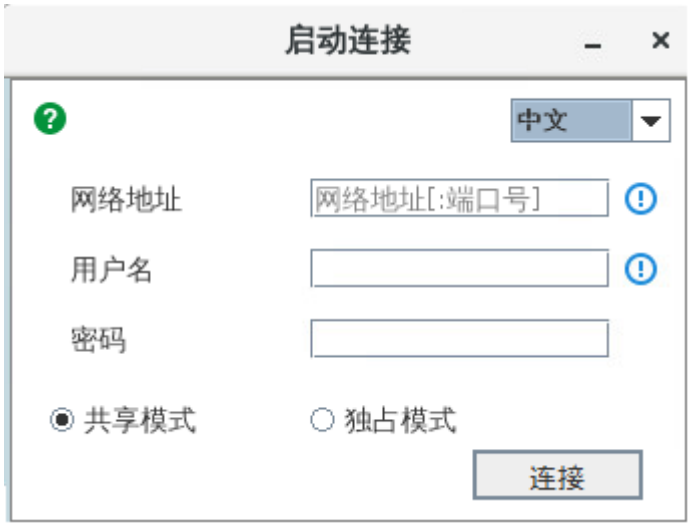
步骤1 配置客户端（例如PC）IP地址，使其与iBMC管理网口在同一网段。

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 777 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

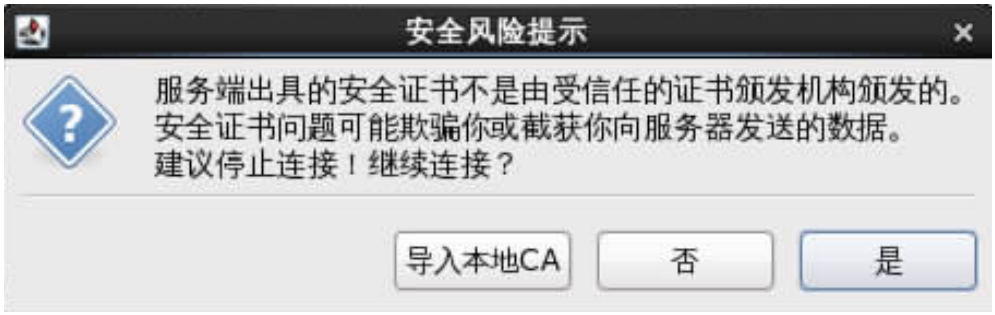
- iBMC V228之前版本仅支持本地用户登录，iBMC V228及之后版本支持本地用户及LDAP域用户登录。
- iBMC V228之前版本端口号对应RMCP+服务端口号，iBMC V228及之后版本端口号对应HTTPS服务端口号。
- 输入IPv6地址时，必须使用[ ]将其括起来，而IPv4地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认时，“网络地址”中可不加端口号。

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

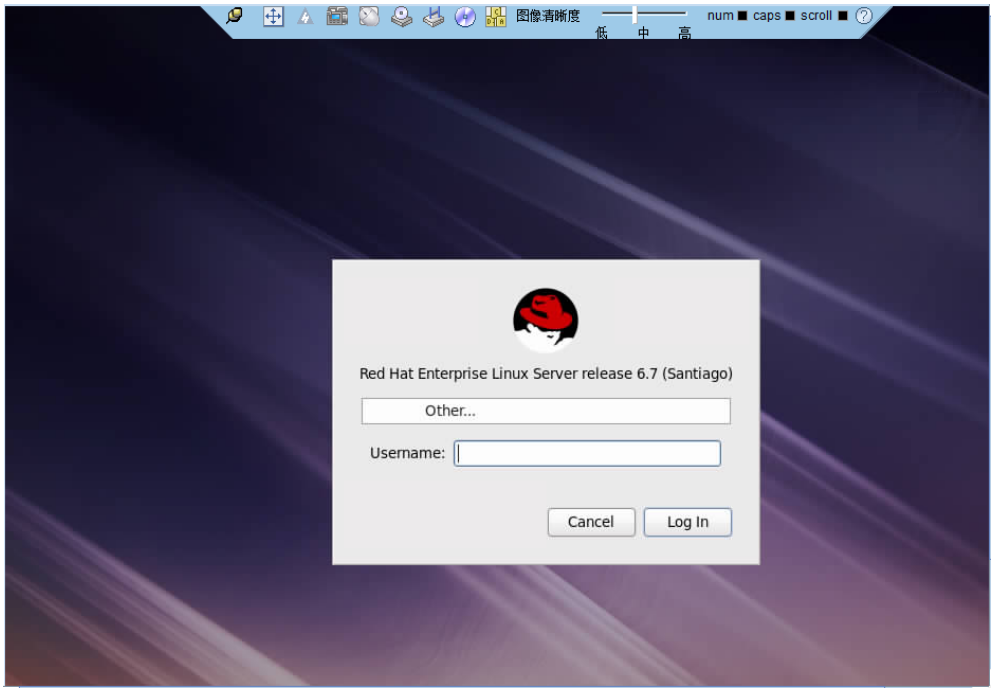


步骤7 按照实际需要单击确认按钮。

- 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。

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	是否支持配置文件生效
本地用户	User	UserName	用户名	是
	User	PassWord	用户密码	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	是
	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。

分类	导出项	导出子项	说明	是否支持配置文件生效
	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
	LDAP	Port	LDAPS端口号	是
	LDAP	UserDomain	域名	是
	LDAP	Folder	用户应用文件夹	是
	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

分类	导出项	导出子项	说明	是否支持配置文件生效
	LDAPServer	UserDomain	域名	是
	LDAPServer	Folder	用户应用文件夹	是
	LDAPGroup	GroupName	LDAP组名称	是
	LDAPGroup	GroupFolder	LDAP组应用文件夹	是
	LDAPGroup	GroupPermitRuleIds	LDAP组登录规则	是
	LDAPGroup	GroupLoginInterface	LDAP组登录接口	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	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
网络配置	BMC	HostName	iBMC主机名	否，取值在配置文件中体现。

分类	导出项	导出子项	说明	是否支持配置文件生效
	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。
	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	是
	DNSSetting	DomainName	DNS域名	是
	EthGroup	VlanState	VLAN使能	是
	EthGroup	VlanID	VLAN ID	是

分类	导出项	导出子项	说明	是否支持配置文件生效
	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	否，敏感信息在配置文件中隐藏，不能直接生效。
	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

分类	导出项	导出子项	说明	是否支持配置文件生效
	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
	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SNMP V1	是
	Snmp	V2CState	支持SNMP V2C	是
	Snmp	LongPasswordEnable	超长口令使能	是
	Snmp	ROCommunity	只读团体名	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	否，敏感信息在配置文件中隐藏，不能直接生效。
	Snmp	SNMPV1V2CPermitRuleIds	SNMP登录规则	是
	Snmp	AuthProtocol	SNMPv3鉴权算法	是
	Snmp	PrivProtocol	SNMPv3加密算法	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

分类	导出项	导出子项	说明	是否支持配置文件生效
	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
	Partition	RAIDMode	RAID工作模式（RH8100特有）	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
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
	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

分类	导出项	导出子项	说明	是否支持配置文件生效
	TrapConfig	CommunityName	Trap团体名	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
	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
	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	否，敏感信息在配置文件中隐藏，不能直接生效。
	SmtpConfig	SenderName	SMTP发件人邮箱	是
	SmtpConfig	TempletTopic	SMTP邮件主题	是

分类	导出项	导出子项	说明	是否支持配置文件生效
	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	是
	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
	PowerCapping	LimitValue	功率封顶值	是
	PowerCapping	FailAction	功率封顶失效关机使能	是
节能设置	SysPower	ExpectedMode	电源工作模式	是
	SysPower	ExpectedActive	主用电源	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
录像回放	Video	VideoSwitch	录像使能状态	是

分类	导出项	导出子项	说明	是否支持配置文件生效
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
其他	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
	Stateless	SysManagerPort	无状态计算功能受控上电服务器端口	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

表 8-2 BIOS 配置项

导出项	说明
ProcessorHyperThreadingDisable	控制超线程开关的选项。
ProcessorFlexibleRatioOverrideEnable	频率上限限制调节开关，没有开放，默认关闭。
ProcessorFlexibleRatio	频率上限，默认CPU标称频率。
MonitorMwaitEnable	控制是否开启Monitor/Mwait功能。
ProcessorVmxEnable	CPU虚拟化开关。
ProcessorLtsxEnable	Intel TXT功能开关。
MlcStreamerPrefetcherEnable	硬件预取开关，是指CPU处理指令或数据之前，它将这些指令或数据从内存预取到L2缓存中，借此减少内存读取的时间，帮助消除潜在的瓶颈，以此提高系统效能。
MlcSpatialPrefetcherEnable	相邻缓存预取功能，开启之后计算机在读取数据时，会智能的认为要读取的数据旁边或邻近的数据也是需要的，于是在处理的时候就会将这些邻近的数据预先读取出来，这样可以加快读取速度。
DCUStreamerPrefetcherEnable	DCU流预取功能可以预读取CPU的数据，从而减少数据的读取时间。
DCUIPPrefetcherEnable	DCU IP预取功能可以从历史记录中判断是否有数据需要预读取，从而减少数据的读取时间。
CustomPowerPolicy	能效模式选择菜单，不支持定制。
PowerSaving	Dynamic Energy Management Technology，华为自定义选项，合入uniBIOS自主调频算法，提高能效。
ProcessorEistEnable	Intel处理器动态调频技术，Enhanced Intel SpeedStep® Technolog，系统根据工作量动态调节CPU频率，以节能和减少发热量。
TurboMode	CPU Turbo超频开关。
PStateDomain	PStateDomain开关，core调节或者Package调节。
ProcessorCcxEnable	CPU C状态总开关。
TStateEnable	T状态开关，没有开放，会限制频率。
PackageCState	Package C状态调节开关。
C3Enable	CPU C3状态调节开关。
C6Enable	CPU C6状态调节开关。

导出项	说明
ProcessorC1eEnable	CPU C1e状态调节开关。
OSCx	ACPI C2/C3 调节。
QpiLinkSpeed	QPI LINK Speed。
ClusterOnDieEn	内存Snoop模式ClusterOnDie设置开关。
EarlySnoopEn	内存Snoop模式EarlySnoop和HomeSnoop设置开关。
DdrFreqLimit	内存频率设置开关。
RankMargin	Rank Margin Tool开关。
rmtPatternLength	RMT Pattern Length，Rank Margin Tool开启时设置。
MemTestOnFastBoot	快速启动时，内存测试开关。
ADREn	内存ADR开关。
CustomRefreshRateEn	配置内存刷新频率的开关。
CustomRefreshRate	手动配置内存刷新频率数值。
refreshMode	选择刷新模式，1表示支持2倍的刷新模式，0表示不支持2倍的刷新模式；配置成1时，当内存条温度超过85度就会将刷新频率加大到2倍，来防止高温对内存数据的影响。
mcODTOverride	内存mc ODT选择， ODT（on die termination），是一种允许DRAM控制器通过多种方式动态控制DRAM器件的DQ/DQS/DM管脚片上终结电阻值的机制，有50ohms/100ohms设置。
NumaEn	NUMA（Non Uniform Memory Access）是一种分布式存储器访问方式，多个节点上合理的进行内存分配，处理器可以同时访问不同的存储器地址，大幅度提高并行性。
IsocEn	内存访问模式有关。
RASMode	设置内存RAS模式为独立模式/镜像模式/Lockstep模式。
enableSparing	Rank Sparing特性开关。
multiSparingRanks	Haswell开始支持多Rank做备份，本菜单可配置一个channel中备份Rank的数量。
spareErrTh	内存可纠正错误门限值，达到这个阈值之后会触发SMI，在SMI里面会根据事先配置的RAS特性做相应处理。
PatrolScrub	内存engine会以一定的速度主动对内存进行巡检，发现并修正可纠正错误，防止可纠正错误积累变成不可纠正错误。本选项用于控制内存巡检开关。
PatrolScrubDuration	以小时为单位定义完整巡检一次的时间。

导出项	说明
DemandScrubMode	Demand Scrub特性指当HA主动读取内存数据时，如果发现可纠正错误，会将错误纠正并将正确数据写回到内存。本选项控制Demand Scrub特性的开关。
DeviceTaggingMode	当某个内存颗粒频繁发生错误，错误数量超过门限时，将触发SMI中断，在SMI中断处理中可以设置用奇偶校验颗粒来代替一个故障颗粒。本选项控制Device Tagging特性的开关。
thermalthrottlingsupport	CLTT（Closed Loop Thermal Throttling）适用于有温度传感器的内存条，根据传感器温度对内存进行动态调节；OLTT（Open Loop Thermal Throttling）适用于没有温度传感器的内存条，根据预先配置做静态内存调节；本选项用于选择内存温度调节模式。
PcieAcpiHotPlugEnable	该选项为开关选项，用于控制是否IIO PCI-E的Hotplug功能。
EnableAzaliaVCpOptimizationste	开关选项，控制打开或者关闭azalia_on_vcp功能。
PCIeSRIOVSupport	开关选项，用于控制打开或者关闭PCIE的虚拟化功能，设置寄存器。
VTdSupport	打开或者关闭VT-d虚拟化功能。
InterruptRemap	开启或者关闭Interrupt Remapping功能，和vtd相关。
CoherencySupport	打开或者关闭Coherency Support的功能，和vtd相关。
IsochCoherencySupport	打开或者关闭Coherency Support（Isoch）功能，和vtd相关。
IdeController	打开或关闭SATA控制器。
SataCnfigure	sata控制器模式设置。
PchsSata	打开或关闭sSATA控制器。
sSataInterfaceMode	ssata控制器模式设置。
XHCIMode	USB 3.0控制器开关。
CREnable	串口重定向开关。
CRTerminalType	串口重定向字体类型选择开关。
CRBaudRate	串口重定向波特率选择开关。
CRInfoWaitTime	串口重定向初始化信息显示时间。
CRAfterPost	串口重定向是否在BIOS POST之后生效。
PXE1setting	板载网口1 PXE开关。
PXE2setting	板载网口2 PXE开关。

导出项	说明
WheaSupport	打开或者关闭WHEA功能，故障诊断相关。
WheaEinjType	打开或者关闭故障注入功能，故障诊断相关。
SystemErrorEn	打开或者关闭故障诊断开关。
FDM	打开或者关闭故障诊断上报BMC开关。
PoisonEn	中毒位开关，故障诊断相关。
EMcaLogEn	EMCA日志记录（又称ELOG）的开关，BIOS会创建ELOG Entries，ELOG Entries中详细记录了错误信息，可供OS/VMM预测故障使用。该日志保存在BIOS提供的保留内存当中，通过Entries地址访问。与ELOG对应还有一个WHEA log，WHEA日志的结构是由ACPI规范定义。
EMcaCSmiEn	CMCI转SMI信号开关，选项关闭时内存可纠正错误只会产生CMCI，直到错误计数达到阈值之后才会产生SMI；打开后每个内存可纠正错误直接产生SMI，由BIOS处理，在SMI处理函数结尾再由BIOS决定是否发MCE信号通知OS，这样做有利于收集更多的有用信息。
PowerStateRestoreOnACLoss	在AC上电后，操作系统侧的上电策略。 ● ON：自动上电 ● OFF：保持下电 ● Last State：保持前一次配置
BmcWdtEnable	打开或关闭开机自检看门狗，即POST看门狗。
BmcWdtTimeout	POST看门狗时间设置。
BmcWdtAction	POST看门狗动作设置。
OSWdtEnable	打开或关闭OS启动看门狗，即OS看门狗。
OSWdtTimeout	OS看门狗时间设置。
OSWdtAction	OS看门狗动作设置。
SysDbgLevel	BIOS调试开关。
serialDebugMsgLvl	BISO调试打印级别。
Pci64BitResourceAllocation	4G以上MMIO开启开关。
ClkGenSpreadSpectrum	展频开关。
WakeOnPME	网络唤醒开关。
NICTrunk	打开菜单后，在进入OS前会调用DisableNic2ndhandle函数关闭82599的第二个光口，该功能产品已不使用。
Language	语言设置。

导出项	说明
ComBaseOutput	串口IO基址设置。
OemMemTurbo	内存超频开关。
SoftRaidModeSe@lect	软RAID选择开关。 **说明** V5服务器不支持软RAID选择开关。
BootType	启动模式设置，Legacy/UEFI/DUAL。
QuickBoot	快速启动设置，关闭后，每次启动到第一屏后会进行内存测试。
QuietBoot	停用或启用在出现图形之前不显示信息的功能。
PXEOnly	只支持PXE启动，跳过硬盘光驱等。
VideoSelected	板载显卡/外接显卡显示选择。
NoBootDevCtr	无启动设备是否自动复位设置。
BootTypeOrder[0]	启动顺序。
BootTypeOrder[1]	启动顺序。
BootTypeOrder[2]	启动顺序。
BootTypeOrder[3]	启动顺序。

表 8-3 RAID 控制器配置项

分类	导出项	导出子项	说明	是否支持配置文件生效
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 FAQ

9.1 V5服务器安装Windows后出现未知设备

9.1 V5 服务器安装 Windows 后出现未知设备

问题现象

问题描述	可能原因
1. 为V5服务器安装Windows系统。 2. 安装产品对应的驱动包。 3. 打开设备管理器，发现存在未知设备，如**图9-1**所示。	V5服务器的iBMC默认打开黑匣子功能，但Windows侧没有相关驱动。

图 9-1 V5 服务器 Windows 系统下的未知设备

解决方案

方法一：安装黑匣子驱动

黑匣子驱动可随iBMA一起安装生效。

1. 请参考iBMA用户指南在Windows侧正确安装iBMA。
2. BMA运行后，若仍存在上述问题，请联系华为技术支持处理。

方法二：关闭黑匣子功能

1. 在iBMC WebUI的“黑匣子”界面中关闭黑匣子功能。
2. 若仍存在上述问题，请联系华为技术支持处理。

