

百信恒山 AI326TA 服务器 BMC V3.10.00.00 及以上 用户指南

发布日期 2023-07-27

前言

概述

本文档为服务器底层管理软件 BMC（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。

本文档主要介绍客户在使用服务器进行网络部署及维护时，需要使用的命令。不包含以下命令：

- 用于生产、装备、返厂检测维修的命令。
- 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，请联系技术支持。

说明

- 配置不同，Web 界面显示会有所不同，本文档中的 Web 界面截图仅供参考，具体以实际配置为准。
- BMC 中出现的“disk”和“drive”为同义词，泛指所有硬盘。

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

我们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	表示如不可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	表示如不可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	表示如不可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。如不可避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
 说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

文档版本	发布日期	修改说明
01	2023-07-25	第一次正式发布。

目 录

前言.....	ii
1 产品概述.....	12
2 安全特性.....	14
3 常用接口.....	16
3.1 WebUI.....	16
3.2 CLI.....	16
3.3 Redfish 接口	17
3.4 移动应用程序	17
4 用户必读.....	18
4.1 使用准则	18
4.2 获取 BMC 版本信息	18
4.3 默认参数	19
4.4 登录须知	19
4.5 安全注意事项	21
5 WebUI 介绍	22
5.1 新手入门	22
5.1.1 基础操作	22
5.1.2 用户登录	23
5.2 首页	29
5.3 系统管理	32
5.3.1 系统信息	32
5.3.1.1 产品信息	32
5.3.1.2 处理器	34
5.3.1.3 内存	35
5.3.1.4 网络适配器	36
5.3.1.5 传感器	39
5.3.1.6 其他	40
5.3.2 性能监控	41
5.3.3 存储管理	44

5.3.4 电源&功率	60
5.3.5 风扇&散热	69
5.3.6 BIOS 配置	72
5.4 维护诊断	73
5.4.1 告警&事件	73
5.4.2 告警上报	76
5.4.3 录像截屏	87
5.4.4 系统日志	91
5.4.5 BMC 日志	94
5.4.6 工作记录	98
5.5 用户&安全	99
5.5.1 本地用户	99
5.5.2 LDAP	108
5.5.3 Kerberos	117
5.5.4 双因素认证	122
5.5.5 在线用户	126
5.5.6 安全配置	127
5.5.7 证书更新	138
5.5.7.1 SSL 证书更新	138
5.6 服务管理	142
5.6.1 端口服务	142
5.6.2 Web 服务	145
5.6.3 虚拟控制台	150
5.6.4 虚拟媒体	153
5.6.5 VNC	154
5.6.6 SNMP	157
5.7 BMC 管理	161
5.7.1 网络配置	161
5.7.2 时区&NTP	166
5.7.3 固件升级	170
5.7.4 配置更新	175
5.7.5 语言管理	177
5.7.6 许可证管理	179
5.7.7 BMA 管理	181
5.7.8 SP 管理	185
5.8 虚拟控制台	186
5.8.1 虚拟控制台概述	186
5.8.2 HTML5 集成远程控制台	190
5.8.3 Java 集成远程控制台	199
5.9 远程虚拟控制台异常帮助	212

5.9.1 打开 HTML5 集成远程控制台后显示设置信任证书超时	212
5.9.2 无法启动 Java 集成远程控制台	213
5.9.3 打开远程虚拟控制台时鼠标键盘失效	214
5.9.4 打开 KVM 后显示与管理系统连接失败	214
5.10 一键收集信息说明	215
6 CLI 介绍	235
6.1 CLI 说明	235
6.1.1 格式说明	235
6.1.2 帮助	236
6.2 登录 CLI	240
6.2.1 通过管理网口登录 CLI	240
6.2.2 通过串口登录 CLI	241
6.3 BMC 命令	242
6.3.1 查询 BMC 管理网口的 IP 信息 (ipinfo)	242
6.3.2 设置 BMC 管理网口的 IPv4 信息 (ipaddr)	243
6.3.3 设置 BMC 管理网口的备份 IPv4 信息 (backupipaddr)	245
6.3.4 设置 BMC 管理网口的 IPv4 模式 (ipmode)	246
6.3.5 设置 BMC 管理网口的 IPv4 网关 (gateway)	247
6.3.6 设置 BMC 管理网口的 IPv6 信息 (ipaddr6)	248
6.3.7 设置 BMC 管理网口的 IPv6 模式 (ipmode6)	249
6.3.8 设置 BMC 管理网口的 IPv6 网关 (gateway6)	250
6.3.9 设置管理网口模式 (netmode)	251
6.3.10 设置激活端口 (activeport)	253
6.3.11 设置管理网口 VLAN (vlan)	254
6.3.12 查询和设置串口方向 (serialdir)	255
6.3.13 重启 BMC 管理系统 (reset)	256
6.3.14 固件升级 (upgrade)	257
6.3.15 截屏命令 (printscreen)	258
6.3.16 BMC 软件回滚 (rollback)	259
6.3.17 查询软件回滚状态 (rollbackstatus)	260
6.3.18 设置服务状态 (service -d state)	260
6.3.19 设置指定服务的端口号 (service -d port)	261
6.3.20 查询服务状态 (service -d list)	262
6.3.21 设置登录安全性信息功能的使能状态 (securitybanner -d state)	263
6.3.22 定制登录安全信息 (securitybanner -d content)	263
6.3.23 查询登录安全信息 (securitybanner -d info)	264
6.3.24 导入 SSL 证书 (certificate -d import)	265
6.3.25 查询 SSL 证书信息 (certificate -d info)	266
6.3.26 导出配置文件 (config -d export)	267

6.3.27 导入配置文件 (config -d import)	268
6.3.28 导入 CRL 文件 (crl)	269
6.3.29 挂载文件到虚拟光驱 (vmm -d connect)	271
6.3.30 中断虚拟光驱的连接 (vmm -d disconnect)	272
6.3.31 查询虚拟媒体信息 (vmm -d info)	272
6.3.32 将 FPGA 卡的 Golden 固件恢复出厂设置 (fpgagoldenfwrestore)	273
6.4 Trap 命令	274
6.4.1 查询和设置 SNMP trap 状态 (trap -d state)	274
6.4.2 设置 SNMP trap 上报端口号 (trap -d port)	275
6.4.3 设置 SNMP trap 团体名称 (trap -d community)	275
6.4.4 设置 SNMP trap 目的 IP 地址 (trap -d address)	277
6.4.5 查询 Trap 上报目的地址信息 (trap -d trapiteminfo)	277
6.4.6 查询和设置 SNMP trap 版本信息 (trap -d version)	278
6.4.7 查询和设置 SNMP trap 告警发送级别 (trap -d severity)	279
6.4.8 查询和设置 SNMP trap V3 用户 (trap -d user)	280
6.4.9 查询和设置 SNMP trap 模式 (trap -d mode)	280
6.5 Syslog 命令	281
6.5.1 查询和设置 syslog 使能状态 (syslog -d state)	281
6.5.2 查询和设置证书认证方式 (syslog -d auth)	282
6.5.3 查询和设置 syslog 主机标识 (syslog -d identity)	283
6.5.4 查询和设置传输协议类型 (syslog -d protocol)	284
6.5.5 查询和设置上报日志的级别 (syslog -d severity)	285
6.5.6 查询和上传服务器根证书 (syslog -d rootcertificate)	286
6.5.7 查询和上传本地证书 (syslog -d clientcertificate)	287
6.5.8 设置 syslog 服务器地址 (syslog -d address)	288
6.5.9 设置 syslog 服务器端口号 (syslog -d port)	289
6.5.10 设置上报日志类型 (syslog -d logtype)	289
6.5.11 测试 syslog 服务器是否可连接 (syslog -d test)	290
6.5.12 查询所有 syslog 上报通道配置信息 (syslog -d iteminfo)	291
6.6 VNC 命令	292
6.6.1 查询 VNC 服务信息 (vnc -d info)	292
6.6.2 设置 VNC 服务的密码 (vnc -d password)	292
6.6.3 设置 VNC 服务的超时时长 (vnc -d timeout)	293
6.6.4 设置 VNC 服务 SSL 加密功能的状态 (vnc -d ssl)	294
6.6.5 设置 VNC 服务的键盘布局 (vnc -d keyboardlayout)	294
6.7 服务器命令	295
6.7.1 查询和设置启动设备 (bootdevice)	295
6.7.2 设置服务器重启方式 (frucontrol)	296
6.7.3 查询和设置服务器上下电状态 (powerstate)	297

6.7.4 查询和设置服务器的下电时限 (shutdowntimeout)	298
6.7.5 查询服务器板载网卡 MAC 地址 (macaddr)	299
6.7.6 查询系统可用网口 (ethport)	299
6.7.7 清除 BIOS Flash (clearcmos)	300
6.7.8 查询 RAID 控制器信息 (ctrlinfo)	301
6.7.9 查询逻辑盘信息 (ldinfo)	303
6.7.10 查询物理盘信息 (pdinfo)	305
6.7.11 查询磁盘组信息 (arrayinfo)	309
6.7.12 创建逻辑盘 (createld)	311
6.7.13 添加逻辑盘 (addld)	314
6.7.14 删除逻辑盘 (deleteld)	316
6.7.15 修改逻辑盘属性 (ldconfig)	316
6.7.16 修改 RAID 控制器属性 (ctrlconfig)	318
6.7.17 修改物理盘属性 (pdconfig)	319
6.7.18 查询和设置 NPU 芯片工作模式 (npuworkmode)	321
6.8 系统命令	321
6.8.1 查询系统名称 (systemname)	322
6.8.2 设置 BMC 时区 (timezone)	322
6.8.3 查询 BMC 时间 (time)	324
6.8.4 查询设备的版本信息 (version)	324
6.8.5 查询 FRU 信息 (fruinfo)	325
6.8.6 查询系统的健康状态 (health)	326
6.8.7 查询系统的健康事件信息 (healthevents)	326
6.8.8 查询服务器的设备序列号 (serialnumber)	327
6.8.9 查询和清除系统 SEL 信息 (sel)	328
6.8.10 查询系统操作日志 (operatelog)	329
6.8.11 下载系统串口数据 (systemcom)	330
6.8.12 下载黑匣子数据 (blackbox)	331
6.8.13 下载 BIOS (download)	331
6.8.14 升级 BIOS (upgradebios)	332
6.8.15 升级主板 CPLD (upgradecpld)	333
6.8.16 设置 BMC 网口状态 (ethlink)	334
6.8.17 一键收集信息 (diaginfo)	335
6.8.18 恢复 BMC 出厂设置 (restore)	335
6.8.19 设置 CLP notimeout 功能 (notimeout)	336
6.8.20 查询 CLP notimeout 功能的配置信息 (notimeoutstate)	337
6.8.21 更新系统主密钥 (securityenhance -d updatemasterkey)	337
6.8.22 查询和设置主密钥自动更新间隔 (securityenhance -d masterkeyupdateinterval)	338
6.8.23 查询和设置自动发现配置 (autodiscovery)	339

6.8.24 查询和设置受控上电配置 (poweronpermit)	340
6.8.25 查询和清除上电锁的锁定状态 (poweronlock)	341
6.8.26 重启鲲鹏智能管理引擎 (resetiME)	341
6.9 用户管理命令	342
6.9.1 查询所有用户信息 (userlist/list)	342
6.9.2 添加新用户 (adduser)	343
6.9.3 修改用户密码 (password)	345
6.9.4 删除用户 (deluser)	347
6.9.5 设置用户权限 (privilege)	347
6.9.6 查询和设置密码检查功能 (passwordcomplexity)	348
6.9.7 锁定用户 (user -d lock)	349
6.9.8 解除用户锁定状态 (user -d unlock)	350
6.9.9 查询和设置密码最短使用期 (minimumpasswordage)	351
6.9.10 设置紧急用户 (emergencyuser)	351
6.9.11 为用户添加 SSH 公钥 (addpublickey)	352
6.9.12 删除用户的 SSH 公钥 (delpublickey)	353
6.9.13 查询和设置 SSH 用户密码认证使能状态 (sshpwordauthentication)	354
6.9.14 设置用户登录 BMC 的接口类型 (interface)	354
6.9.15 设置弱口令字典认证使能状态 (weakpwddic)	356
6.9.16 导出弱口令字典 (weakpwddic -v export)	357
6.9.17 导入弱口令字典 (weakpwddic -v import)	358
6.9.18 设置 SNMPv3 用户的加密密码 (snmpprivacypassword)	359
6.9.19 查询和设置用户不活动期限 (securityenhanc -d inactivetimetlimit)	360
6.9.20 设置用户启用状态 (user -d state)	361
6.9.21 查询和设置带内用户管理使能状态 (user -d usermgmtbyhost)	363
6.9.22 设置用户首次登录时的密码修改策略 (user -d firstloginpolicy)	363
6.10 NTP 命令	364
6.10.1 查询 NTP 信息 (ntpinfo)	364
6.10.2 设置 NTP 状态 (ntp -d status)	365
6.10.3 设置 NTP 信息获取方式 (ntp -d mode)	366
6.10.4 设置首选 NTP 服务器地址 (ntp -d preferredserver)	367
6.10.5 设置备用 NTP 服务器地址 (ntp -d alternativeserver)	368
6.10.6 设置拓展 NTP 服务器地址 (ntp -d extraserver)	369
6.10.7 设置服务器身份认证状态 (ntp -d authstatus)	370
6.10.8 上传 NTP 组密钥 (ntp -d groupkey)	371
6.11 指示灯命令	372
6.11.1 查询服务器指示灯信息 (ledinfo)	372
6.11.2 设置 UID 指示灯状态 (identify)	372
6.12 风扇命令	373

6.12.1 设置风扇运行速度 (fanlevel)	373
6.12.2 设置风扇运行模式 (fanmode)	374
6.12.3 查询风扇工作状态 (faninfo)	375
6.13 传感器命令	376
6.13.1 查询所有传感器的所有信息 (sensor -d list)	376
6.13.2 传感器测试命令 (sensor -d test)	384
6.13.3 设置传感器使能状态 (sensor -d state)	385
6.13.4 模拟事件 (precisealarm)	386
6.14 电源命令	387
6.14.1 设置电源工作模式 (psuworkmode)	387
6.14.2 查询电源具体信息 (psuinfo)	388
6.15 SOL 命令	389
6.15.1 建立 SOL 会话 (sol -d activate)	389
6.15.2 注销 SOL 会话 (sol -d deactivate)	390
6.15.3 设置 SOL 会话超时时间 (sol -d timeout)	390
6.15.4 查询 SOL 会话列表 (sol -d session)	391
6.15.5 查询 SOL 会话配置信息 (sol -d info)	392
6.16 常用维护命令	392
6.16.1 查看帮助信息 (help)	392
6.16.2 断开连接 (exit)	394
6.16.3 检查网络连通性 (ping、ping6)	394
6.16.4 free 命令 (free)	395
6.16.5 netstat 命令 (netstat)	395
6.16.6 df 命令 (df)	396
6.16.7 ifconfig 命令 (ifconfig)	397
6.16.8 route 命令 (route)	397
6.16.9 top 命令 (top)	398
6.16.10 禁止 CLP 超时 (notimeout)	399
7 常用操作.....	400
7.1 使用 PuTTY 登录服务器 (串口方式)	400
7.2 使用 PuTTY 登录服务器 (网口方式)	402
7.3 配置 WebUI Trap.....	404
7.4 配置 WebUI SMTP	406
7.5 配置目录服务功能	407
7.5.1 配置目录服务器	407
7.5.2 配置 LDAP 功能	428
7.5.3 配置 Kerberos 功能.....	430
7.6 配置 BMC WebUI DNS (手动)	433
7.7 配置 SSH 用户密钥登录 BMC CLI.....	434

7.8 配置 SSL 证书	438
7.9 配置 Syslog 日志上报功能.....	441
7.10 使用 VNC 登录服务器实时桌面	442
7.11 导入信任证书和根证书.....	446
8 FAQ.....	456
8.1 服务器安装 Windows 后出现未知设备	456
8.2 双因素认证失败后无法登录 WebUI	458
8.3 环境产生不安全协议告警	459
8.3.1 问题现象	459
8.3.2 解决方案	459
8.3.2.1 针对 SNMP 和 VNC 不安全协议	459
8.3.2.2 针对 RMCP 不安全协议	461
8.4 环境产生不安全算法告警	461
8.4.1 问题现象	461
8.4.2 解决方案	462
8.4.2.1 针对 SSH 类算法、SSL 类算法	462
8.4.2.2 针对 SNMP 类算法.....	463
8.4.2.2.1 通过 Web 接口修改算法	463
8.4.2.2.2 通过 Redfish 接口修改算法	465
8.5 IPMI RMCP 通信失败	466
8.6 使用旧版本 Edge 查看联机帮助失败	467
9 附录.....	469
9.1 确认管理网口 IP 地址	469
9.2 通过 BIOS 修改 BMC 默认用户密码.....	470
9.3 Smart Provisioning	471
9.4 独立远程控制台	471
9.4.1 简介	471
9.4.2 （Windows）使用独立远程控制台登录服务器实时桌面	472
9.4.3 （Ubuntu）使用独立远程控制台登录服务器实时桌面	475
9.4.4 （Mac）使用独立远程控制台登录服务器实时桌面	478
9.4.5 （Redhat）使用独立远程控制台登录服务器实时桌面	481
9.5 配置文件说明	484
9.6 BMC 系统默认用户	506
10 术语和缩略语.....	508

1 产品概述

BMC 智能管理系统（以下简称 BMC）提供了丰富的管理功能。

- 丰富的管理接口
提供以下标准接口，满足多种方式的系统集成需求。
 - DCMI 1.5 接口
 - IPMI 1.5/IPMI 2.0 接口
 - 命令行接口
 - Redfish 1.5 及以上版本标准接口
 - 超文本传输安全协议（HTTPS，Hypertext Transfer Protocol Secure）
 - 简单网络管理协议（SNMP，Simple Network Management Protocol）
- 故障监控与诊断
可提前发现并解决问题，保障设备 7*24 小时高可靠运行。
 - 系统崩溃时临终截屏与录像功能，使得分析系统崩溃原因不再无处下手。
 - 屏幕快照和屏幕录像，让定时巡检、操作过程记录及审计变得简单轻松。
 - FDM（Fault Diagnose Management）功能，支持基于部件的精准故障诊断，方便部件故障定位和更换。
 - 支持 Syslog 报文、Trap 报文、电子邮件上报告警，方便上层网管收集服务器故障信息。
- 安全管理手段
 - 通过软件镜像备份，提高系统的安全性，即使当前运行的软件完全崩溃，也可以从备份镜像启动。
 - 多样化的用户安全控制接口，保证用户登录安全性。
 - 支持多种证书的导入替换，保证数据传输的安全性。
- 系统维护接口
 - 支持虚拟 KVM（Keyboard, Video, and Mouse）和虚拟媒体功能，提供方便的远程维护手段。
 - 支持 RAID 的带外监控和配置，提升了 RAID 配置效率和管理能力。
 - 通过 Smart Provisioning 实现了免光盘安装操作系统、配置 RAID 以及升级等功能，为用户提供更便捷的操作接口。

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

- 智能电源管理

- 功率封顶技术助您轻松提高部署密度。
 - 动态节能技术助您有效降低运营费用。

- 许可证管理

通过管理许可证，可实现以授权方式使用高级版的特性。

BMC 高级版较标准版提供更多的高级特性，例如：

- 通过 Redfish 实现 OS 部署。
 - 通过 Redfish 收集智能诊断的原始数据。
 - 使能鲲鹏加速引擎，包括硬件安全加速引擎（SEC，Security Engine）、高性能 RSA 加速引擎（HPRE，High Performance RSA Engine）、RAID DIF 运算加速引擎（RDE，RAID DIF Engine）、ZIP 四个加速器。
 - 使能系统锁定模式。

2 安全特性

- **NC-SI**
服务器管理平面与业务平面分离。BMC 可以通过 NC-SI 边带网口功能与业务平面共享同一个网卡。在物理层，管理平面与业务平面共用接口，在软件层，通过 VLAN 实现二者隔离，互不可见。
- **协议与端口防攻击**
BMC 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**
BMC 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**
BMC 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。
BMC 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 BMC 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**
BMC 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，BMC 支持开启 KVM 加密、VNC 加密功能，实现数据的安全传输。

3 常用接口

BMC 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。

3.1 WebUI

3.2 CLI

3.3 Redfish 接口

3.4 移动应用程序

3.1 WebUI

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

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

WebUI 当前支持中文、英文、日文、法文、俄文界面，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 WebUI 的更多说明，请参考本文档 [5 WebUI 介绍](#)。

3.2 CLI

BMC 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 BMC 的所有操作。

关于 CLI 的详细信息，请参考本文档 [6 CLI 介绍](#)。

3.3 Redfish 接口

BMC 支持标准的 Redfish 1.5 及以上版本标准接口。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](#)。

3.4 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 BMC。SmartServer 直接与 BMC 进行交互，对服务器进行常规的配置和监控。

关于 SmartServer 的详细说明，请参考服务器的 [SmartServer 用户指南](#)。

4 用户必读

- [4.1 使用准则](#)
- [4.2 获取 BMC 版本信息](#)
- [4.3 默认参数](#)
- [4.4 登录须知](#)
- [4.5 安全注意事项](#)

4.1 使用准则

- 使用专用网络对 BMC 进行配置。
- BMC 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。

4.2 获取 BMC 版本信息

BMC 的版本信息的获取方式包括：

- 通过 WebUI 查询。

登录 BMC，在“首页”界面中可查看到“BMC 固件版本”，例如：



- 通过命令行查询。

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

```
.....
Active BMC   Version:      (U4282) 3.02.01.00
Active BMC   Build:       005
.....
```

4.3 默认参数

BMC 提供部分特性的默认参数如下表所示，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4-1 默认参数

参数	默认值
BMC 默认用户名和密码	Admin@100。
BMC 管理网口 IP 地址默认获取方式	DHCP
BMC 管理网口默认备份 IP 地址	192.168.2.100

4.4 登录须知

登录 IP 地址

- 首次登录时，请使用默认 IP 地址。
- 若配置了 DHCP，则 IP 地址为动态分配，使用前需要首先确认当前 IP 地址。
可通过以下方式确认：
 - 在 DHCP 服务器上通过 MAC 地址查询对应的 IP 地址。
 - 在上层网管查询下辖服务器的 BMC IP 地址。
 - PC 直连 BMC 串口，在 CLI 下查询当前地址。
- 首次登录后，请按照实际需求修改管理网口 IP 地址并进行妥善记录，方便后续产品配置及网络规划。

修改管理网口 IP 地址的方法包括：

- 直连用户可在 WebUI 修改。修改方法请参考本文档 [5.7.1 网络配置](#)。
- 直连用户可在 CLI 修改。修改方法请参考本文档 [6.3.2 设置 BMC 管理网口的 IPv4 信息（ipaddr）](#) 和 [6.3.6 设置 BMC 管理网口的 IPv6 信息（ipaddr6）](#)。
- 直连用户可在 BIOS Setup 中修改。修改方法请参考对应产品的 BIOS 参数参考手册。
- 上层网管可通过对接接口（例如 SNMP、Redfish 等）修改下辖服务器的地址。

登录用户类型

登录用户包括以下类型：

- 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 BMC 的用户个数不受常规限制。此方法适用于具有大量用户的环境。
- Kerberos 用户登录方式，支持单点登录，登录 BMC 的用户个数同样不受常规限制，且更具安全性。

客户端环境

登录 WebUI 的客户端，必须满足一定条件才能正确显示。特别是远程控制台，对浏览器及 Java 的配套关系有特殊要求，如[表 4-2 运行环境](#)所示。

为了确保您能浏览到完整的 WebUI 页面，建议使用以下屏幕分辨率：

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

说明

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

- Safari 11.0~12.0
- Microsoft Edge 12~18

表4-2 运行环境

操作系统	浏览器	Java 运行环境
Windows 7 32 位 Windows 7 64 位	• 支持 Mozilla Firefox 63.0 及以上版本，推荐 96.0~98.0 版本 • 支持 Google Chrome 70.0 及以上版本，推荐 97.0~100.0 版本	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
Windows 8 32 位 Windows 8 64 位		
Windows Server 2008 R2 64 位		
Windows Server 2012 64 位		
Windows Server 2012 R2 64		

操作系统	浏览器	Java 运行环境
位		
Windows Server 2016 64 位		
Windows 10 64 位	- 支持 Microsoft Edge, 推荐 94.0~97.0 版本 - 支持 Mozilla Firefox 63.0 及以上版本, 推荐 96~98 版本 - 支持 Google Chrome 70.0 及以上版本, 推荐 97.0~100.0 版本	
CentOS 7	支持 Mozilla Firefox 63.0 及以上版本, 推荐 96.0~98.0 版本	
MAC OS X v10.7	- 支持 Safari 11.0 及以上版本, 推荐 15.1 和 15.2 版本 - 支持 Mozilla Firefox 63.0 及以上版本, 推荐 96.0~98.0 版本	

4.5 安全注意事项

为防止中间人攻击，BMC 在发起对远程服务器的 HTTPS 连接时，增加了服务器证书校验。当证书校验开关开启时，需要导入正确的服务器 CA 证书并验证通过才能连接成功。证书校验涉及的主要场景有 Redfish 事件订阅消息上报和以 HTTPS 协议进行的文件上传或下载。

为了避免文件被替换，以及被低权限用户下载或者执行的安全风险，BMC 对文件的上传、下载及导入操作进行了文件属主判断，具体规则如下：

- A 用户上传文件后，B 用户不能上传同名文件。
- A 用户上传的文件，只有 A 用户和管理员可以导入，其他用户无法导入。
- 如果 A 用户上传文件后未导入，需要由 A 用户删除该文件后，B 用户才能导入同名文件。
- A 用户导出的文件，只有 A 用户和管理员可以下载，其他用户无法下载。
- 如果 A 用户导出的文件未下载，B 用户可以导出同名文件覆盖，覆盖后只有 B 用户和管理员用户可以下载，其他用户（包括 A 用户）无法下载。

5 WebUI 介绍

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

- 5.1 新手入门
- 5.2 首页
- 5.3 系统管理
- 5.4 维护诊断
- 5.5 用户&安全
- 5.6 服务管理
- 5.7 BMC 管理
- 5.8 虚拟控制台
- 5.9 远程虚拟控制台异常帮助
- 5.10 一键收集信息说明

5.1 新手入门

5.1.1 基础操作

WebUI 可执行的基本操作如表 5-1 基本操作所示。

表5-1 基本操作

操作	说明
切换界面语言	在 WebUI 页面右上角，鼠标移动到  , 从下拉列表中切换语言。

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

5.1.2 用户登录

功能介绍

通过使用“用户登录”界面的功能，您可以登录 WebUI。

- 通过 WebUI 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 WebUI 执行任何操作，系统将自动退出登录，此时需输入用户名和密码重新登录 WebUI。
- 连续输入错误密码的次数达到设定的失败次数后，系统将对此用户进行锁定。锁定时间达到用户设置的锁定时长后，该用户方可正常登录。

- 为保证系统的安全性，初次登录时，请及时修改初始密码，并定期更新。
- 由于网络波动导致资源获取失败，可能会导致 WebUI 显示异常，请刷新浏览器后，重新登录 WebUI。

参数说明

表5-2 用户登录

参数	描述
用户名	登录 BMC 系统的用户。 • “域名”选择“这台 BMC”时，支持输入的用户名的最大长度为 16 个字符。 • “域名”选择“这台 BMC”之外的其他选项时，支持输入的用户名的最大长度为 255 个字符。 登录时请注意以下事项： • 使用本地用户登录 BMC 时，“域名”可选择“这台 BMC”或“自动匹配”。 • 使用 LDAP 方式登录 BMC 时，支持如下两种格式的用户名： – LDAP 用户名（此时“域名”可选择“自动匹配”或指定的域名）。 – LDAP 用户名@域名（此时“域名”可选择“自动匹配”或指定的域名）。 • 使用 Kerberos 方式登录 BMC 时，支持如下两种格式的用户名： – Kerberos 用户名（此时“域名”可选择“自动匹配”或指定的域名）。 – Kerberos 用户名@域名（此时“域名”可选择“自动匹配”或指定的域名，且域名中的字母必须为大写）。 • Kerberos 用户名或 Kerberos 用户名@域名支持单点登录。
密码	登录用户的密码，为了保证安全，用户应定期修改自己的登录密码。 说明 以 LDAP 方式或 Kerberos 方式登录 WebUI 时，密码最大长度为 255 个字符。

操作步骤

本指南以 Google Chrome 为例介绍登录 WebUI 的操作步骤。

- 步骤 1** 确认使用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 4-2 运行环境](#)。
- 步骤 2** 配置客户端（例如 PC）IP 地址，使其与 BMC 管理网口网络互通。
- 步骤 3** 通过网线将 PC 连接到管理网口。
- 步骤 4** 打开 Google Chrome，在地址栏中输入管理网口地址：“https://ipaddress/”，并按“Enter”。

 说明

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

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

弹出如下图所示的安全告警窗口。

图5-1 安全告警



您的连接不是私密连接

攻击者可能会试图从  窃取您的信息（例如：密码、通讯内容或信用卡信息）。[了解详情](#)

NET::ERR_CERT_AUTHORITY_INVALID



如果您想获得 Chrome 最高级别的安全保护，请[开启增强型保护](#)

高级

返回安全连接

 说明

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

- 如果您有可信任的证书，可以为 BMC 导入信任证书和根证书。有关详细信息，请参见[7.11 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 BMC 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。

弹出如下图所示的登录界面。

图5-2 登录 BMC



The image shows the BMC login interface. At the top, it says '欢迎到访' (Welcome to visit) in orange. Below that is the 'BMC' logo in large black letters. To the right of the logo is a blurred image of a server. Below the logo, there are three input fields: '用户名' (Username) with the placeholder '请输入用户名' (Please enter username), '密码' (Password) with the placeholder '请输入密码' (Please enter password), and '域名' (Domain) with the placeholder '这台BMC' (This BMC) and a dropdown arrow. Below these fields is a large blue button labeled '登录' (Login). At the bottom, there is a link labeled '单点登录' (Single Sign-On) in blue.

步骤 6 选择其中一种方式登录 WebUI。

- [使用本地用户登录 WebUI](#)
- [使用 LDAP 用户登录 WebUI](#)
- [使用 Kerberos 用户登录 WebUI](#)

----结束

使用本地用户登录 WebUI

步骤 1 在 BMC 登录界面中，将界面切换至目标语言。

步骤 2 按照[参数说明](#)，输入登录 BMC 界面的用户名和密码。

步骤 3 在“域名”下拉列表中，选择“这台 BMC”或“自动匹配”。

步骤 4 单击“登录”。

成功登录后，显示“首页”界面。

----结束

使用 LDAP 用户登录 WebUI

在登录前，请确保以下设置满足要求：

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

说明

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

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

步骤 1 在 BMC 登录界面中，将界面切换至目标语言。

步骤 2 按照[参数说明](#)，输入登录 WebUI 界面的 LDAP 用户名和密码。

说明

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

步骤 3 在域名下拉列表中，选择 LDAP 用户域。

说明

域名下拉列表中包含如下可选参数：

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

步骤 4 单击“登录”。

成功登录后，显示“首页”界面。

----结束

使用 Kerberos 用户登录 WebUI

Kerberos 运行环境：

- 客户端支持操作系统版本为 Windows 10 64 位。
- Kerberos 服务器支持操作系统版本为 Windows Server 2012 R2 64 位和 Windows Server 2016 64 位。

Kerberos 用户支持两种方式登录：

- 通过 kerberos 域用户登录。
- 通过 SSO 一键登录。

在登录前，请确保以下设置满足要求：

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

通过 Kerberos 域用户登录。

步骤 1 在 BMC 登录界面中，将界面切换至目标语言。

步骤 2 按照[参数说明](#)，输入登录 WebUI 的 Kerberos 用户名和密码。

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

步骤 4 单击“登录”。

成功登录后，显示“首页”界面。

----结束

通过 SSO 一键登录。

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

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

打开 WebUI 登录界面。

步骤 3 单击“单点登录”。

成功登录后，显示“首页”界面。

----结束

5.2 首页

功能介绍

“首页”界面提供了：

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

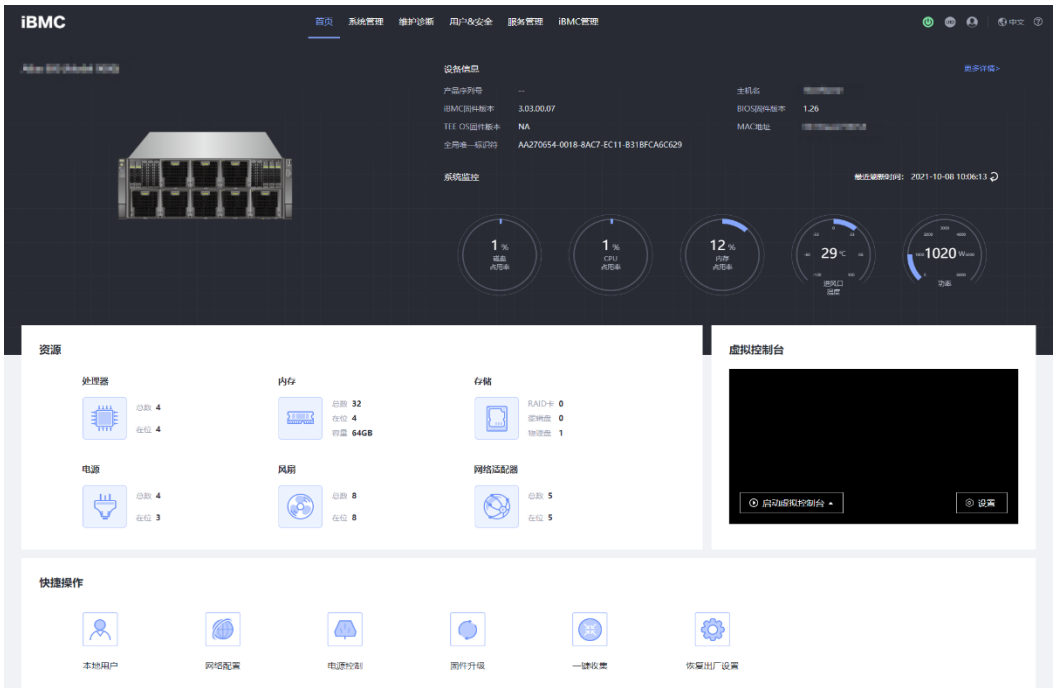
说明

本页面产品展示图仅供参考，具体以实际配置为准。

界面描述

在导航栏中选择“首页”，打开如下图所示界面。

图5-3 首页



参数说明

表5-3 基本信息

区域	展示的信息
设备信息	提供服务器的基本信息，包括： - 产品序列号：服务器的序列号。 - 系统序列号：系统的序列号。 说明 仅当产品序列号和系统序列号不一致时，支持显示系统序列号。 - 主机名：BMC 的主机名称。 - BMC 固件版本：BMC 系统的固件版本。 - BIOS 固件版本：BIOS 的固件版本。 - TEE OS 固件版本：TEE（Trusted Execution Environment）OS 版本。 - MAC 地址：管理网口物理地址。 - 全局唯一标识符：全球唯一标识。 单击“更多详情”可以跳转到“系统管理 > 系统信息 > 产品信息”界面。
系统监控	提供系统监控快捷入口，包括： - 磁盘/CPU/内存占用率：单击本入口可以直接跳转到“系统管理 > 性能监控”界面。 - 进风口温度：单击本入口可以直接跳转到“系统管理 > 风扇&散热”界面。 - 功率：单击本入口可以直接跳转到“系统管理 > 电源&功率 > 功率”界面。 说明 - 当磁盘占用率、CPU 占用率、内存占用率显示的当前值为 0%时，表示未检测到该检测项的当前值。请在 OS 侧安装并运行 BMA 2.0。 - 当磁盘占用率、CPU 占用率、内存占用率显示为 0%<当前值<门限值时，表示资源使用情况正常。 - 当磁盘占用率、CPU 占用率、内存占用率显示为门限值≤当前值≤100%时，表示资源使用情况已超出紧急预警区间，需要立即处理。 - 功率的检测情况，因服务器不同而采用不同的检测区域。 - 当进风口温度显示为当前值<一级门限值时，表示服务器温度正常。 - 当进风口温度显示为一级门限值≤当前值<二级门限值时，表示温度已超出正常范围，需要处理。 - 当进风口温度显示为当前值≥二级门限值时，表示温度已超出紧急预警区间，需要立即处理。
资源	提供资源信息快捷入口，包括： - 处理器：单击本入口可以直接跳转到“系统管理 > 系统信息 > 处理器”界面。 - 内存：单击本入口可以直接跳转到“系统管理 > 系统信息 > 内存”界

区域	展示的信息
	面。 • 存储：单击本入口可以直接跳转到“系统管理 > 存储管理”界面。 • 网络适配器：单击本入口可以直接跳转到“系统管理 > 系统信息 > 网络适配器”界面。 • 电源：单击本入口可以直接跳转到“系统管理 > 电源&功率 > 电源信息”界面。 • 风扇：单击本入口可以直接跳转到“系统管理 > 风扇&散热”界面。
虚拟控制台	从本入口可以进入 HTML5 集成远程控制台或 Java 集成远程控制台。 • 单击“启动虚拟控制台”，在弹出的列表选择独占或共享模式的 HTML5 集成远程控制台或 Java 集成远程控制台。 • 单击“设置”，可以直接跳转到“虚拟控制台”界面。 关于虚拟控制台的详细介绍和常见异常帮助请参见： • 5.8.1 虚拟控制台概述 • 5.8.2 HTML5 集成远程控制台 • 5.8.3 Java 集成远程控制台 • 5.9 远程虚拟控制台异常帮助
快捷操作	提供常用操作的快捷入口，通过以下入口可以快速跳转到相关界面，包括： • 本地用户：单击本入口可以直接跳转到“用户&安全 > 本地用户”界面。 • 网络配置：单击本入口可以直接跳转到“BMC 管理 > 网络配置”界面。 • 电源控制：单击本入口可以直接跳转到“系统管理 > 电源&功率 > 服务器上下电”界面。 • 固件升级：单击本入口可以直接跳转到“BMC 管理 > 固件升级”界面。 • 一键收集：单击本入口可以直接下载收集到的维护相关信息，收集到信息的具体内容请参见本文档 5.10 一键收集信息说明。 • 恢复出厂配置：单击本入口可以弹出“恢复默认”窗口，根据需要确定是否恢复出厂设置。 • 恢复配置操作会恢复所有用户配置的信息，例如以下配置项，但不限于这些： - 当前串口互联状态 - 功率封顶配置 - 删除用户上传的 LDAP 和 SSL 证书 - 用户名、密码、有效期、组信息、登录锁定信息 - IP 获取模式、IP 地址、掩码、默认网关 - SNMP 配置 - 告警上报的 SNMP TRAP 配置、SMTP 配置
用户	登录 BMC 后的前 10 秒会显示本用户上一次登录的信息，包括：

区域	展示的信息
上次登录信息	• 用户名 • 登录 IP 地址 • 登录时间

5.3 系统管理

5.3.1 系统信息

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

5.3.1.1 产品信息

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“产品信息”，打开如下图所示界面。

图5-4 产品信息

产品信息			
产品名称	Atlas	生产厂商	
产品序列号	111	部件编码	
资产标签	--	产品位置	--
主板信息			
iBMC固件版本	3.10.02.10(U72)	单板ID	0x0092
BIOS版本	5.28(U249)	主板厂商	
CPLD版本	0.07(U151)	主板型号	5104-00549
iBMC主UBoot版本	16.8.10.2 (21:35:00 Jun 12 2023)	主板序列号	2106411244FSP3000039
iBMC备UBoot版本	16.8.10.2 (21:35:00 Jun 12 2023)	PCB 版本	.B
部件编码			
系统软件			
❖ 您必须先在服务器OS侧安装BMA 2.0，并完全启动后，方可查询到完整的系统软件信息。			

参数说明

表5-4 产品信息

参数	描述
产品信息	
产品名称	产品名称。
生产厂商	产品的生产厂商。
资产标签	产品的资产标签。 取值范围：长度为 0~48 个字符的字符串，允许输入数字、英文字母和特殊字符。 说明 普通用户没有权限设置产品资产标签，仅管理员、操作员或具有“常规配置”权限的自定义用户可以设置产品资产标签。
产品序列号	服务器的产品序列号。
部件编码	服务器的部件编码。
产品位置	服务器的产品位置。 取值范围：长度为 0~64 个字符的字符串，允许输入数字、英文字母和特殊字符。
主板信息	
BMC 固件版本	服务器的固件的版本号。
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。
BMC 主 Uboot 版本	用于嵌入式系统的开机引导程序的主用镜像版本号。全称为 Universal Boot Loader。
BMC 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 ID。
主板厂商	主板的生产厂家。
主板型号	主板的型号。
主板序列号	主板的序列号。
部件编码	主板的部件编码。
系统软件	

参数	描述
说明	- 您必须先 在服务器 OS 侧安装 BMA 2.0 并完全启动后，方可在“系统信息”区域框中查询到完整的系统软件信息。 - 若服务器 OS 侧未安装 BMA 2.0，请获取最新的 BMA 用户文档及软件包，并参考 BMA 用户文档安装 BMA 2.0。
计算机名称	显示服务器操作系统中定义的计算机名称。
计算机描述	显示服务器操作系统的计算机描述信息。
操作系统内核版本	当操作系统改为 Linux 系统时，显示其内核版本信息。
域名/工作组	显示服务器操作系统侧的域名或所属工作组。
BMA 服务	显示服务器操作系统中安装的 BMA 版本信息。
BMA 运行状态	显示 BMA 软件的运行状态。
BMA 驱动	显示 BMA 的驱动版本信息。
操作系统版本	显示服务器操作系统的版本信息。
电子保单	
产品名称	产品名称。
产品序列号	服务器的产品序列号。
生产日期	服务器的生产日期。
UUID	服务器的全局唯一标识符（UUID，Universally Unique Identifier）。
单元类型	服务对象的单元类型。
服务起始时间	保单的服务起始时间。 默认值：服务器生产日期+100 天。
服务年限（月）	保单的服务年限，单位为月。 取值范围：1~255。 默认情况下，没有设置服务年限，此时 WebUI 不显示电子保单。

5.3.1.2 处理器

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“处理器”，打开如下图所示界面。

图5-5 处理器

CPU(2/2)
NPU(8/8)

总数 8 在位 8

名称	型号	能力规格	功率	固件版本	DIE ID
▼ NPU1			74 W	N/A	N/A
▼ NPU2			72 W	N/A	N/A
▼ NPU3			71 W	N/A	N/A
▼ NPU4			78 W	N/A	N/A
▼ NPU5			74 W	N/A	N/A
▼ NPU6			75 W	N/A	N/A
▼ NPU7			72 W	N/A	N/A
▼ NPU8			76 W	N/A	N/A

参数说明

表5-5 处理器

参数	描述
CPU 信息	显示服务器所有在位的处理器的信息。 - 处理器满配个数和当前在位个数 - 处理器的名称、厂商、型号、处理器 ID、主频 - 该型号处理器支持的核数/线程数 - 缓存：包括处理器的一级、二级、三级缓存的容量 - 状态：处理器的状态信息 - 部件编码：该处理器的部件编码 - 序列号：该处理器的序列号 - 其他参数：该处理器支持的其他技术参数
NPU 信息	显示服务器所有在位的 NPU 的信息，包括： - NPU 满配个数和当前在位个数 - 名称、厂商、型号 - 功率 - 固件版本 - DIE ID

5.3.1.3 内存

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“内存”，打开如下图所示界面。

图5-6 内存

总数 32 在位 4

名称	厂商	容量	配置速度	最大速度	类型	位置
^ DIMM000		16384 MB	2666 MT/s	2666 MT/s	DDR4	CpuBoard1
详细信息						
名称	DIMM000		位置	CpuBoard1		
厂商			容量	16384 MB		
配置速度	2666 MT/s		最大速度	2666 MT/s		
类型	DDR4		最小电压	1200 mV		
类型详细信息	Synchronous Registered (Buffered)		位宽	72 bit		
部件编码	M393A2K43BB1-CTD		Rank数	2 rank		
序列号	34F15FD3		内存温度	41 °C		
▽ DIMM001		16384 MB	2666 MT/s	2666 MT/s	DDR4	CpuBoard1
▽ DIMM100		16384 MB	2666 MT/s	2666 MT/s	DDR4	CpuBoard1
▽ DIMM101		16384 MB	2666 MT/s	2666 MT/s	DDR4	CpuBoard1

参数说明

表5-6 内存

参数	描述
基本信息	显示服务器内存信息。 - 内存满配个数和当前在位个数。 - 内存的名称、厂商、容量、配置速度、最大速度、类型以及位置。
详细信息	单击内存名称左侧的▼，显示内存的详细信息： 内存的部件编码、序列号、位宽、Rank 数、最小电压以及类型详细信息。

5.3.1.4 网络适配器

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“网络适配器”，打开如下图所示界面。

图5-7 网络适配器



参数说明

表5-7 网络适配器

参数	描述
	- 您必须先安装在服务器 OS 侧安装 BMA 2.0 并完全启动后，方可在“网络适配器”页签中查询到完整的网络信息。 - 若服务器 OS 侧未安装 BMA 2.0，请获取最新的 BMA 用户文档及软件包，并参考 BMA 用户文档安装 BMA 2.0。
以太网卡	显示服务器安装的板载网卡或 PCIe 网卡的名称、型号、芯片厂商、单板 ID、厂商、芯片型号、PCB 版本、资源归属（归属 CPU、PCH 或 PCIe Switch）、总线信息、PCIe 槽位号（PCIe 网卡独有）等信息。 - 单击以太网卡子菜单的网卡名称，可以查看成员端口的详细信息，包括端口、状态、网口类型、介质类型、速率、自动协商和全双工状态。 说明 以太网卡“端口属性”的状态含义包括以下几种： --：表示服务器未安装 BMA，并且无法获取物理连线状态。 - 连接：表示服务器未安装 BMA，物理连线状态处于连接状态。 - 断开：表示服务器未安装 BMA，物理连线状态处于断开状态。 - NoLink：表示服务器已安装 BMA，端口未连线，但端口状态为 Up。 - LinkUp：表示服务器已安装 BMA，端口已连线，且端口状态为 Up。 - LinkDown：表示服务器已安装 BMA，端口状态为 Down。 - 单击“端口属性”下方的，可查看指定网卡的网络属性，包括端口名称、固件版本、驱动名称、驱动版本、总线信息、MAC 地址、永久 MAC 地址、IPv4 信息（地址/子网掩码/网关）、IPv6 信息（地址/前缀长度/网关）、VLAN 信息（VLAN ID、VLAN 使能状态、VLAN 优先级使能状态）。 - 单击“端口属性”下方的，可查看指定网卡的连接视图，包括交换机名称、交换机连接 ID、交换机连接端口 ID 以及交换机端口 VLAN

参数	描述
	ID。 - 单击“端口属性”下方的, 可查看指定网卡的 DCB 信息和报文统计信息。 - 如果网口安装了光模块, 单击“端口属性”下方的, 可查看指定网卡的光模块信息, 包括厂商、序列号、部件名称、设备类型、设备连接类型、接收丢失状态、发送错误状态、波长、设备识别信息、当前温度、当前发送偏置电流、当前发送功率和当前接收功率。 - 如果网口插上了电缆, 单击“端口属性”下方的, 可查看指定网卡的电缆信息, 包括厂商、序列号、部件名称、设备类型以及设备连接类型。 说明 如果网卡的固件版本不支持使用某个网口, 该网口的网络属性显示为空。例如某网卡有 Port1、Port2 两个网口, 如果该网卡的固件版本不支持使用 Port2, 则 Port2 的网络属性显示为空。
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、部件编码和序列号。 - 单击 FC 卡子菜单的 FC 名称, 可以查看成员端口的详细信息, 包括端口、FC ID、端口类型、状态。 - 单击“端口属性”下方的, 可以查看指定 FC 卡的网络属性, 包括速率、WWPN (World Wide Port Name)、WWNN (World Wide Node Name)、固件版本、驱动名称、驱动版本。 - 如果网口安装了光模块, 单击“端口属性”下方的, 可查看指定网卡的光模块信息, 包括厂商、序列号、生产日期、部件名称、模块类型、传输模式、收发器类型、速率、设备类型、设备连接类型、传输距离、接收丢失状态、发送错误状态、波长、设备识别、当前温度 (°C)、当前电压 (V)、当前发送偏置电流 (mA)、当前发送功率 (mW)、当前接收功率 (mW)、严重告警阈值 (上限 下限)。 - 支持 MCTP 且芯片类型为 Hi1822 的 FC 卡支持显示以下信息: - 工作速率 - 工作模式 - 光模块开启状态 - 对端设备信用值 - 本端设备信用值 - 发送速率 - 接收速率 - 速率协商阶段
Team	显示汇聚网口的名称、状态、工作模式、IPv4 信息 (地址/子网掩码/网关)、IPv6 信息 (地址/前缀长度/网关)、MAC 地址、VLAN 信息 (VLAN ID、VLAN 使能状态、VLAN 优先级使能状态)。 单击汇聚网口子菜单的网口名称, 可以查看成员端口的详细信息, 包括网卡名称、网口名称、端口号、MAC 地址和状态。

参数	描述
Bridge	显示桥接网口的名称、状态、IPv4 信息（地址/子网掩码/网关）、IPv6 信息（地址/前缀长度/网关）、MAC 地址、VLAN 信息（VLAN ID、VLAN 使能状态、VLAN 优先级使能状态）。 • 单击桥接网口子菜单的网口名称，可以查看成员端口的详细信息，包括网口名称、端口、状态、网口类型和介质类型。 • 单击“端口属性”下方的，可以查看成员端口的网络属性。

5.3.1.5 传感器

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“传感器”，打开如下图所示界面。

图5-8 传感器

门限传感器

请输入关键字

Q

序号	传感器 名	当前值	状态	紧急下门限	严重下门限	轻度下门限	轻度上门限	严重上门限	紧急上门限
1	CPU1 Core Rem (°C)	64	OK	--	--	--	--	--	--
2	CPU1 DDR VDDQ (V)	1.22	OK	--	1.14	--	--	1.26	--
3	CPU1 DDR VDDQ2 (V)	1.22	OK	--	1.14	--	--	1.26	--
4	CPU1 DDR VPP1 (V)	2.56	OK	--	2.24	--	--	2.74	--
5	CPU1 DDR VPP2 (V)	2.56	OK	--	2.24	--	--	2.74	--
6	CPU1 DTS	-32	OK	--	--	--	-1	--	--
7	CPU1 MEM Temp (°C)	37	OK	--	--	--	95	--	--
8	CPU1 VCCIO (V)	0.99	OK	--	0.84	--	--	1.16	--
9	CPU1 VCore (V)	1.77	OK	--	1.23	--	--	2.04	--
10	CPU1 VDDQ Temp (°C)	31	OK	--	--	--	120	--	--
11	CPU1 VRD Temp (°C)	40	OK	--	--	--	120	--	--
12	CPU1 VSA (V)	0.83	OK	--	0.45	--	--	1.21	--
13	CPU2 Core Rem (°C)	58	OK	--	--	--	--	--	--
14	CPU2 DDR VDDQ (V)	1.22	OK	--	1.14	--	--	1.26	--
15	CPU2 DDR VDDQ2 (V)	1.22	OK	--	1.14	--	--	1.26	--

15

总条数: 59

1

2

3

4

跳转

1

▶

参数说明

表5-8 传感器

参数	描述
传感器	传感器是指监控服务器各类指标的模块，可以是逻辑模块或物理实体。
当前值	传感器当前监控到的指标信息。 如果显示为--，表示传感器未采集到有效数据。

参数	描述
状态	门限传感器扫描状态： • OK：表示传感器正常。 • --：表示传感器状态未知。 • NC：表示传感器检测到轻微告警。 • CR：表示传感器检测到严重告警。 • NR：表示传感器检测到紧急告警。
紧急下门限	使传感器产生紧急告警的下门限值。 如果显示为--，表示不支持此门限。
严重下门限	使传感器产生严重告警的下门限值。 如果显示为--，表示不支持此门限。
轻微下门限	使传感器产生轻微告警的下门限值。 如果显示为--，表示不支持此门限。
轻微上门限	使传感器产生轻微告警的上门限值。 如果显示为--，表示不支持此门限。
严重上门限	使传感器产生严重告警的上门限值。 如果显示为--，表示不支持此门限。
紧急上门限	使传感器产生紧急告警的上门限值。 如果显示为--，表示不支持此门限。
搜索	在搜索框中输入关键字，按“Enter”或单击  显示符合条件的传感器信息。

5.3.1.6 其他

界面描述

在导航栏中选择“系统管理 > 系统信息”，单击“其他”，打开如下图所示界面。

图5-9 其他

硬盘背板 (1/1)	名称	位置	厂商	编号	类型	PCB版本	CPLD版本	单板ID	部件编码	序列号
xPU载板 (2/2)	IT21BP8A	chassis		1	10*2.5 SAS/S...	.A	1.14	0x00c1		--
Riser卡 (2/2)										
PCIe卡 (0/4)										
安全模块 (1/1)										

参数说明

表5-9 其他

参数	描述
硬盘背板	显示服务器硬盘背板信息。 - 硬盘背板最大可扩展个数和当前在位个数。 - 硬盘背板的名称、位置、厂商、编号、类型、PCB 版本、CPLD 版本、单板 ID、部件编码以及序列号。
PCIe 卡	显示服务器 PCIe 卡信息。 - PCIe 卡满配个数和当前在位个数。 - PCIe 卡的描述、位置、厂商、槽位、制造商 ID、设备 ID、部件编码、子厂商 ID、子设备 ID 以及资源归属。
Riser 卡	显示服务器 Riser 卡信息。 - Riser 卡满配个数和当前在位个数。 - Riser 卡的名称、厂商、槽位、类型、PCB 版本、单板 ID、部件编码以及序列号。
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。
xPU 载板	显示服务器 xPU（比如 NPU 或 GPU）载板信息。 - xPU 载板满配个数和当前在位个数。 - xPU 载板的单板名称、位置、厂商、部件编码、序列号、单板 ID、槽位、PCB 版本和 CPLD 版本。
HiAM	显示服务器 HiAM 信息。 - HiAM 满配个数和当前在位个数。 - HiAM 的名称、位置、厂商、槽位、描述和 UID。

5.3.2 性能监控

功能介绍

通过“性能监控”界面，您可以：

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

界面描述

在导航栏中选择“系统管理 > 性能监控”，打开如下图所示界面。

图5-10 性能监控



参数说明

表5-10 性能监控

参数	描述
CPU 占用率	运行的程序占用 CPU 资源的比例。 说明 - 您必须先 在服务器 OS 侧安装 BMA 2.0，并完全启动后，方可查看 CPU 占用率信息。 - 若服务器 OS 侧未安装 BMA 2.0，请获取最新的 BMA 用户文档及软件包，并参考文档安装 BMA 2.0。
内存占用率	运行的程序占用内存的比例。 说明 您必须先 在服务器 OS 侧安装 BMA 2.0，并完全启动后，方可查看内存占用率信息。

参数	描述
	若服务器 OS 侧未安装 BMA 2.0，请获取最新的 BMA 用户文档及软件包，并参考文档安装 BMA 2.0。
网口带宽占用率	服务器网卡提供的所有网口的带宽占用比例。 说明 - 您必须先安装在服务器 OS 侧安装 BMA 2.0，并完全启动后，方可查看网口带宽占用率信息。 - 若服务器 OS 侧未安装 BMA 2.0，请获取最新的 BMA 用户文档及软件包，并参考文档安装 BMA 2.0。
磁盘占用率	磁盘分区中已使用的空间占整个分区空间的比例、磁盘分区路径、已使用容量及磁盘分区总容量。 说明 - 您必须先安装在服务器 OS 侧安装 BMA 2.0，并完全启动后，方可查看磁盘占用率信息。 - 若服务器 OS 侧未安装 BMA 2.0，请获取最新的 BMA 用户文档及软件包，并参考文档安装 BMA 2.0。
当前值	服务器当前 CPU 或内存的占用率。
门限值	服务器当前 CPU、内存、磁盘或网口带宽占用率的门限值，占用率超出设置的门限值后，BMC 会上报一个正常事件。 取值范围：0~100 的整数值。
	打开编辑门限的输入框。
	刷新相关性能监控项的统计信息。
	清空网口带宽占用率统计信息。

设置门限值

步骤 1 单击待设置目标区域框的 。

弹出门限值输入框。

步骤 2 根据界面提示的取值范围，在输入框中输入门限数值。

步骤 3 单击  保存设置。

设置门限值后，您可以单击  刷新占用率曲线。

---结束

5.3.3 存储管理

功能介绍

通过使用“存储管理”界面的功能，您可以查看和配置服务器当前存储设备的信息。

说明

- 不同的 RAID 控制器支持显示的存储管理信息不同，请以实际界面显示为准。
- 此页面的 RAID 控制器、逻辑驱动器、物理驱动器的信息依赖 RAID 卡的带外管理功能，并且在系统引导完成后或安装并完全启动 BMA 2.0 才能显示。
- “存储管理”中的信息在系统下电或系统未完成启动时为无效数据。服务器在每次上电并且系统完成启动后，BMC 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 link is abnormal 告警。
- 硬盘被识别并完全显示所需要的时间与逻辑盘和物理盘的数目有关，逻辑盘和物理盘的数目越多，硬盘被识别需要的时间越长。

界面描述

在导航栏中选择“系统管理 > 存储管理”，打开如下图所示界面。

图5-11 存储管理



参数说明

表5-11 存储管理

参数	描述
RAID 控制器	控制器信息： 控制器名称、类型、固件版本、是否支持带外管理、健康状态、支持的 RAID 级别、工作模式、内存大小、设备接口、SAS 地址、支持的条带大小范围、Cache Pinned 状态、

参数	描述
	物理盘故障记忆启用状态、配置版本、PCIe 带宽、启动设备、回拷启用状态、SMART 错误时回拷启用状态、JBOD 模式启用状态、一致性校验功能、一致性校验功能运行状态、校验周期、校验速率、自动修复功能、已完成数量、需要完成数量。 • BBU 名称、状态、健康状态。 说明 • RAID 控制器不支持带外管理且未安装运行 BMA 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 BMC 带外管理。 • 请不要在 RAID 卡侧将其工作模式设置为 JBOD，BMC 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。 • 一致性校验功能运行状态、校验周期、校验速率、自动修复功能、已完成数量、需要完成数量在一致性校验功能状态开启时才有效。
逻辑盘	逻辑盘信息： 名称、状态、RAID 级别、容量、条带大小、SSCD 功能启用状态、默认读策略、当前读策略、默认写策略、当前写策略、默认 IO 策略、当前 IO 策略、物理盘缓存状态、访问策略、初始化类型、后台初始化启用状态、二级缓存启用状态、一致性校验运行状态、系统盘符、启动设备、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 BMA 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 BMC 带外管理。
物理盘	物理盘信息： 接口类型、健康状态、厂商、型号、序列号、固件版本、介质类型、温度、固件状态、SAS 地址(0)、SAS 地址(1)、容量、支持的速率、协商速率、电源状态、热备状态、定位状态、剩余磨损率、通电累计时间、启动设备、转速、转速、重构状态和巡检状态。 说明 • RAID 控制器不支持带外管理且未安装运行 BMA 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 BMC 带外管理。 • 仅 SATA 硬盘及希捷 SAS 硬盘支持累计通电时间的查询。 • 对于 NVMe 硬盘，如果服务器 OS 为 Windows 或 VMware，由于其不支持 NVMe 硬盘接口的速率协商特性，此处“协商速率”显示为“NA”。 • 剩余磨损率表示 SSD 硬盘的使用寿命。剩余磨损率越大，表示硬

参数	描述
	盘的损耗越小，使用寿命越长；剩余磨损率越小，表示硬盘的损耗越大，使用寿命越短。例如剩余磨损率为 100%，表示硬盘没有损耗。 • M.2 硬盘不支持显示定位状态信息。
控制器配置项	• 工作模式 • 回拷 • SMART 错误时回拷 • JBOD 模式 • 一致性校验功能
逻辑盘配置项	• 创建逻辑盘 • 删除逻辑盘 • 修改逻辑盘属性
物理盘配置项	• 启动设备 • 定位状态 • 热备状态 • 固件状态 • 巡检开关 说明 M.2 硬盘无定位状态配置项。
日志收集	支持收集控制器日志。 • RAID 卡 AP 固件日志原始数据：“ap.bin”。 • RAID 卡 IMU 固件日志原始数据：“imu.bin”。 • RAID 卡 AP 固件日志解析字典：“ap_index.gz”。 • RAID 卡 IMU 固件日志解析字典：“imu_index.gz”。 • RAID 卡 AP 固件临终遗言原始数据：“lastword.bin”。 • RAID 卡 AP 统计计数原始数据：“dump.bin”。 • RAID 卡 AP 统计计数 flash 原始数据：“flash_dump.bin”。 • RAID 卡 nand 日志原始数据：“0nandlog.bin”和“1nandlog.bin”。

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 BMC 带外管理或已在 OS 侧安装并运行 BMA 2.0。您可以从 RAID 控制卡用户指南的“技术规格”章节中查询该 RAID 卡是否支持 BMC 带外管理。

- BIOS 启动完成。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中待查看的 RAID 控制器。

右侧区域显示 RAID 控制器的基本属性，如下图所示。

图5-12 查看控制器属性



----结束

查看 RAID 组属性

说明

执行此操作需满足以下条件：

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

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中待查看的 RAID 组。

右侧区域显示 RAID 组的基本属性，如下图所示。

图5-13 查看 RAID 组属性



----结束

查看物理盘属性

说明

执行此操作需满足以下条件：

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

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

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

其基本属性如下图所示。

图5-14 查看物理盘属性（成员盘）



图5-15 查看物理盘属性（单独物理盘）



----结束

修改 RAID 控制器属性

说明

- 执行此操作需满足以下条件：
- RAID 卡支持 BMC 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 BMC 带外管理。
 - BIOS 启动完成。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中待操作的 RAID 控制器。

步骤 3 单击“设置”。

弹出编辑界面，如下图所示。

图5-16 修改 RAID 控制器属性

×

设置

启动设备—

None

回拷

SMART错误时回拷

JBOD模式

一致性校验功能

恢复默认设置

导入Foreign配置

清除Foreign配置

确定

取消

步骤 4 参考表 5-12 控制器配置项说明的配置项说明进行配置。

表5-12 控制器配置项说明

配置项	说明
工作模式	不同类型、不同固件版本的 RAID 卡支持的工作模式不同，您可以从 RAID 控制卡用户指南查询到相关信息。 说明 物理盘的固件状态为“UNCONFIGURED GOOD”时，才能切换工作模式。
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

配置项	说明
	盘。
恢复默认设置	单击“恢复默认配置”，可将 RAID 控制器的属性恢复为默认值。
导入 Foreign 配置	单击“导入 Foreign 配置”，可以导入 Foreign 磁盘包含的 RAID 配置信息，无需输入配置文件。
清除 Foreign 配置	单击“清除 Foreign 配置”，可以清除 Foreign 磁盘包含的 RAID 配置信息。
一致性校验功能	设置控制器一致性校验功能的配置： • 运行状态：一致性校验的运行状态 • 自动修复功能：一致性校验的自动修复配置 • 校验速率：一致性校验速率 • 校验周期：一致性校验周期 • 任务等待时间：一致性校验等待时间

步骤 5 单击“确认”。

---结束

收集 RAID 控制器日志

说明

执行此操作需满足以下条件：

- 必须为 Hi1880/Aries 类型的 RAID 控制器
- 带外功能正常
- BIOS 启动完成

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中待操作的 RAID 控制器。

步骤 3 单击“日志收集”。

图5-17 日志收集



----结束

创建逻辑盘

说明

- 执行此操作需满足以下条件：
- 必须为 RAID 控制卡管理的硬盘且 RAID 控制卡需支持创建逻辑盘功能。
 - 加入逻辑盘的物理盘状态为 UNCONFIGURED GOOD。
 - RAID 卡支持 BMC 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 BMC 带外管理。
 - 当前 RAID 控制卡下的逻辑盘数量未达到 RAID 控制卡所支持的最大数量。
 - BIOS 启动完成。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中待操作的 RAID 控制器。

步骤 3 单击“添加”。

打开创建逻辑盘区域，如下图所示。

图5-18 创建逻辑盘

创建逻辑盘

名称

☐ 二级缓存

条带大小

16 KB

初始化类型

No Init

* RAID级别

0

子组的成员盘数

* 物理盘

☐ Disk0

☐ Disk1

☐ Disk2

☐ Disk3

☐ Disk4

☐ Disk5

☒ Disk6

☐ Disk7

容量

TB

加速方法

保存

取消

步骤 4 参考表 5-13 创建逻辑盘配置项说明的配置项说明进行配置。

表5-13 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。 默认为。
读策略	逻辑盘的数据读策略，包括： Read Ahead：使能预读取功能。控制器可以预读

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

配置项	说明
初始化类型	创建逻辑盘后，对其采用的初始化方式，包括： • No Init：不进行初始化。 • Quick Init：只把逻辑盘的前 100MByte 空间进行全写 0 操作，随后此逻辑盘的状态就变为“Optimal”。 • Full Init：需要把整个逻辑盘都初始化为 0，才会结束初始化过程，整个过程中，逻辑盘的状态始终为“Optimal”。 • Front：前台初始化。 • Background：后台初始化。 默认为“No Init”。
RAID 级别	逻辑盘的 RAID 级别。 默认为“0”。 说明 RAID 级别为 1 时，仅支持选择 2 个物理盘配置为 RAID1。
子组的成员盘数	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。
可用容量	逻辑盘的可用容量。
容量	逻辑盘的容量。

步骤 5 单击“保存”。

----结束

删除逻辑盘

说明

执行此操作需满足以下条件：

- 必须为 RAID 卡管理的硬盘。
- RAID 卡支持 BMC 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 BMC 带外管理。
- BIOS 启动完成。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 删除逻辑盘。

- 单击待删除的逻辑盘右侧的，可单独删除指定逻辑盘。

- 单击 RAID 控制器右侧的“编辑”后，勾选要删除的逻辑盘并单击“删除”，可批量删除多个逻辑盘。

弹出操作确认对话框。

步骤 3 单击“确定”。

----结束

修改逻辑盘属性

说明

执行此操作需满足以下条件：

- 必须为 RAID 卡管理的硬盘。
- RAID 卡支持 BMC 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 BMC 带外管理。
- BIOS 启动完成。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中待操作的逻辑盘。

步骤 3 单击“设置”。

打开逻辑盘编辑菜单。

图5-19 修改逻辑盘

×

设置

名称

123456789

启动设备

Primary

条带大小

64 KB

加速方法

maxCache

容量

199.996

GB

确定

取消

步骤 4 参考表 5-14 修改逻辑盘配置项说明的配置项说明进行配置。

表5-14 修改逻辑盘配置项说明

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

配置项	说明
	保护机制，数据会丢失。 • Disabled: 读写过程中数据不经过物理盘写 Cache，当系统意外掉电时，数据不会丢失。 • Disk's default: 保持默认的缓存策略。
是否为启动设备	是否设置该逻辑盘为系统启动设备。
SSCD 缓存功能	是否使用 CacheCade 逻辑盘做缓存。

步骤 5 单击“确认”。

----结束

修改物理盘属性

说明

执行此操作需满足以下条件：

- 必须为 RAID 卡管理的硬盘。
- RAID 卡支持 BMC 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 BMC 带外管理。
- BIOS 启动完成。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 选中要操作的物理盘，可以是 RAID 组中逻辑盘下的的成员盘，也可以是 RAID 组中独立的物理盘。

步骤 3 单击物理盘后的“设置”。

弹出物理盘编辑窗口。

图5-20 修改物理盘属性

×

设置

定位状态 ☐

热备状态 ☒ 无 ☐ 全局 ☐ 专用

巡检开关 ☐ 开启 ☒ 关闭

确定取消

步骤 4 参考表 5-15 物理盘配置项说明的配置项说明进行配置。

表5-15 物理盘配置项说明

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

配置项	说明
	说明 • RAID 组成员盘支持。 • 物理盘 HDD 介质支持。 • RAID0 不支持。 • 热备空闲盘不支持。 • 成员盘为故障盘不支持。 • RAID 组状态为 fault 不支持。

步骤 5 单击“确认”。

----结束

擦除物理盘数据

说明

- 只有加密盘支持擦除数据操作。
- 数据擦除后将无法恢复，请谨慎操作。

步骤 1 在导航栏中选择“系统管理 > 存储管理”。

步骤 2 鼠标移至待操作的物理盘名称。

步骤 3 单击.

步骤 4 根据实际需要在弹出的提示框中单击“是”。

----结束

5.3.4 电源&功率

功能介绍

通过使用“电源&功率”界面的功能，您可以：

- 查看服务器的电源信息。
- 查看服务器的功率信息。
- 设置是否开启功率封顶功能，限制服务器的封顶功率。
- 查看系统近一周或近一天的历史平均功率和峰值功率曲线，以及每个采样时间点获取的服务器功率，也可以重新统计功率。
系统的采样时间间隔为 10 分钟。
- 对服务器操作系统进行上电、下电或重启操作。
- 设置服务器面板电源按钮。
- 设置服务器操作系统的通电开机策略。
- 设置服务器延迟上电。

须知

- 设置封顶功率时，请谨慎操作。如果封顶功率过低，系统性能和服务器上的业务运营会受到影响。
- 请在强制下电、下电、强制重启或强制下电再上电操作前确认无业务风险。

界面描述

在导航栏中选择“系统管理 > 电源&功率”，打开如下图所示界面。

图5-21 电源信息



图5-22 功率



图5-23 服务器上下电

系统状态

上电

虚拟按键

下电

☒ 下电时限 (秒)

10

[↗](#)

强制下电

?

强制下电可能会损坏用户的程序或者未保存的数据!

强制重启

?

强制重启可能会损坏用户的程序或者未保存的数据!

强制下电再上电

?

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!

面板电源按钮

屏蔽面板电源按钮

☐

?

通电开机策略

☒ 保持上电

☐ 保持下电

☐ 与之前保持一致

延迟上电设置

☒ 默认延迟

0 ~ 2秒随机延迟

☐ 二分延迟

50%概率延迟, 延迟时长 (秒) : --

☐ 固定延迟

固定时间延迟, 延迟时长 (秒) : --

☐ 随机延迟

0 ~ M秒内随机延迟, M为延迟上限 (秒) : --

保存

漏液自动下电:

☐

漏液检测卡在位时生效。

参数说明

表5-16 电源信息

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

参数	描述
当前功率	显示电源模块当前的输出功率。
工作模式	显示电源模块当前的工作模式，包括： ● 负载均衡：多个电源模块同时为系统供电，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，延长电源模块使用寿命。 默认取值：负载均衡 说明 ● 在系统功耗较小的情况下，主备供电模式更为节能。 ● 主备供电模式下，若系统功耗大于等于主用电源模块额定功率的 75%时，会自动切换为负载均衡模式。 ● 开启主备供电功能，主用电源个数必须大于或等于备用电源个数。
主用电源	“主备供电”工作模式下的主用电源模块。
深度休眠	须知 开启深度休眠模式，系统下电后，如果所有主用电源被拔掉或者发生故障导致输出关闭，整机会掉电 10 秒左右，然后处于深度休眠模式的电源会自动打开输出。 开启深度休眠，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。 ●  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。 默认为关闭状态。

表5-17 功率

参数	描述
功率单位	设置“功率”页面中功率的单位，可以设置为“BTU/h”或“W”。 说明 1 BTU/h = 0.293 W
统计开始时间	开始统计功率相关参数的时间。

参数	描述
重新统计	清空当前统计记录，重新开始统计。
功率封顶配置	使用本功能前，需要进入 BIOS 菜单，将“电源策略”设置为“性能”。 功耗封顶下限是实现功耗封顶的最低建议值，设置较低封顶值可能导致封顶失败。例如，当系统中含有 GPU，SSD 等高功率的 PCIe 设备时，如果设置的封顶值接近下限值，可能导致封顶失败。
功率封顶使能状态	使用本功能前，需要进入 BIOS 菜单，将“电源策略”设置为“性能”。 开启或关闭功率封顶功能。 默认为关闭状态。
功率封顶值	限制服务器可运行的最大功率。 取值范围：开启功率封顶使能后，单击“功率封顶值”后的输入框可以查看到取值范围，不同产品取值范围不相同，以界面提示为准。 取值原则：最小可设置的功率不小于系统给出的下限值。
当前功率	服务器当前的功率。
系统峰值功率	从服务器首次上电或重新统计起始时间到当前时刻，系统出现过的最大功率值。
系统平均功率	从服务器首次上电或重新统计起始时间，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。
历史功率	系统最近一周内任意时间段（精确到 10 分钟）内的峰值功率和平均功率统计数据。 选择最近一周内的任意时间段，单击“查询”，可查看到该时间段内的峰值功率和平均功率曲线，以及分段峰值功率及产生时间。 说明 如果自重新统计时间起到当前还不足一周，只能查看自重新统计时间起到当前的功率曲线。
告警门限	实时功率的告警门限。请参照界面提示的取值范围设置告警门限。 实时功率超过设置的阈值时，BMC 将产生告警。
下载	单击  , 可以下载历史功率数据文件到本地 PC。
清空	单击, 可以清除所有历史功率数据。 清除所有历史功率数据后，系统从当前时刻开始重新统计。 “历史功率”区域框显示重新统计的功率信息。

表5-18 服务器上下电

参数	描述
系统状态	显示服务器操作系统上下电状态。
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。
下电时限（秒）	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，BMC 会对操作系统执行强制下电。 - 关闭“下电时限”时，BMC 不会干涉操作系统的下电过程。 说明 启用下电时限后，对服务器操作系统执行下电操作，在下电时限内，如果在操作系统取消下电，超过下电时限后，操作系统仍会执行强制下电。 不同设备的取值范围和默认取值不同，以 WebUI 提示为准，单位为秒。 选中“下电时限”左侧的复选框，表示启用“下电时限”。 单击 ，在文本框中修改下电时限，完成修改后单击  保存设置。
强制下电	须知 强制下电可能会损坏用户的程序或者未保存的数据，请根据操作系统实际情况谨慎选择操作方式。 对服务器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。

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  或  并根据提示保存，可切换状态。 默认状态：   表示此功能已开启，此时电源按钮已失效。  表示此功能已关闭，此时电源按钮处于激活状态，可控制服务器上下电。
通电开机策略	服务器电源模块通电后，操作系统的开机策略包括： - 保持上电：服务器的电源模块通电后操作系统自动开机。 - 保持下电：服务器的电源模块通电后操作系统不上电。 - 与之前保持一致：服务器的电源模块通电后保持断电前状态。 - 如果断电前服务器操作系统是开机状态，则通电后操作系统自动开机。 - 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。 默认为“保持上电”。
延迟上电设置	在前级供电设备通断电从而引起大批量服务器同时上电时，瞬间的上电峰值电流过大会对供电设备产生冲击。为避免这种情况导致的设备故障，可设置服务器延迟上电，以减小上电峰值电流，降低设备损害风险。 服务器延迟上电设置生效需同时满足以下条件： - 通电开机策略为上电状态。 - 受控上电开关为关闭状态。 服务器的延迟上电模式包括： - 默认延迟：0~2 秒内随机延迟。通电后在 0~2 秒内随机延迟上电。 - 二分延迟：50%概率延迟。通电后有 50%的概率按照已设定的时间延迟上电。 取值范围为 0~120，精度为 0.1，单位为秒。 - 固定延迟：固定时间延迟。通电后按照已设定的固定时间延迟上电。 取值范围为 0~120，精度为 0.1，单位为秒。 - 随机延迟：0~M 秒内随机延迟，延迟上限为 M 秒。通电后在 0~M 秒内随机延迟上电。 取值范围为 0~120，精度为 0.1，单位为秒。 默认为“默认延迟”。

参数	描述
漏液自动下电	此功能开启时，若 BMC 检测到漏液告警，操作系统将自动下电（仅针对支持漏液检测卡的服务器）。 单击  或  并根据提示保存，可切换状态。  表示此功能已开启。  表示此功能已关闭。 默认状态：

操作步骤

表5-19 电源&功率操作步骤

操作	操作步骤
设置电源模块工作模式	- 在“电源信息”页签，单击“电源设置”。 - 根据实际情况，设置电源模块的工作模式。 （可选）当工作模式为主备供电时，设置主用电源模块。 （可选）单击  使之变为 ，开启深度休眠功能。 说明 - 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。 - 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。 - 单击“保存”。
为服务器操作系统上电	- 在“服务器上下电”页签，单击“虚拟按键”区域框中的“上电”按钮。 弹出对话框提示以下信息： 是否确认执行该操作？ - 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，“系统状态”显示为“上电”。
将服务器操作系统正常下电	在“服务器上下电”页签，单击“虚拟按键”区域框中的“下电”按钮。 弹出对话框提示以下信息： 是否确认执行该操作？

操作	操作步骤
	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&功率”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，“系统状态”显示为“下电”。
将服务器操作系统强制下电	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“强制下电”按钮。 弹出对话框提示以下信息： 确定要进行强制下电操作吗？强制下电可能会损坏用户的程序或者未保存的数据！ 2. 单击“确定”。 服务器操作系统开始强制下电。操作完成后“电源&功率”界面将显示“操作成功”提示信息。 服务器操作系统成功强制下电后，“系统状态”显示为“下电”。
强制重启服务器操作系统	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“强制重启”按钮。 弹出对话框提示以下信息： 确定要进行强制重启操作吗？强制重启可能会损坏用户的程序或者未保存的数据！ 2. 单击“确定”。 服务器操作系统开始强制重启。服务器操作系统强制重启的时间根据服务器配置所不同。操作完成后“电源&功率”界面将显示“操作成功”提示信息。
强制下电再上电	1. 在“服务器上下电”页签，单击“虚拟按键”区域框中的“强制下电再上电”按钮。 弹出对话框提示以下信息： 确定要进行强制下电再上电操作吗？强制下电再上电可能会损坏用户的程序或者未保存的数据！ 2. 单击“确定”。 服务器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&功率”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，“系统状态”由“上电”变为“下电”，最后显示为“上电”。
设置通电开机策略	1. 在“服务器上下电”页签，设置服务器的通电开关机策略。 2. 单击“保存”。 显示“操作成功”表示成功设置开关机策略。
设置下电时限	1. 在“服务器上下电”页签，勾选“下电时限”。

操作	操作步骤
	- 单击  输入超时时长。 不同产品取值范围不相同，以界面提示为准。 - 单击  保存设置。 显示“操作成功”表示成功设置下电时限。
查看下电时限	在“服务器上下电”页签的“虚拟按键”区域中，查看下电时限。
设置延迟上电	- 在“服务器上下电”页签，在“延迟上电设置”区域框选择延迟上电的模式。 - 单击  输入延迟时长。 延迟时间的取值范围为 0~120，精度为 0.1，单位为秒。默认延迟模式不支持设置延迟时长。 - 单击 ，保存延迟时间设置。 - 单击“保存”完成设置。 显示“操作成功”表示成功设置延迟上电。 说明 单击“保存”后，2 中设置的延迟时长将同步到另外两种可设置延迟时长的模式。

5.3.5 风扇&散热

功能介绍

通过使用风扇&散热界面的功能，您可以：

- 查看服务器进风口温度历史数据。
- 实现对服务器风扇调速方式的查询和设置。

说明

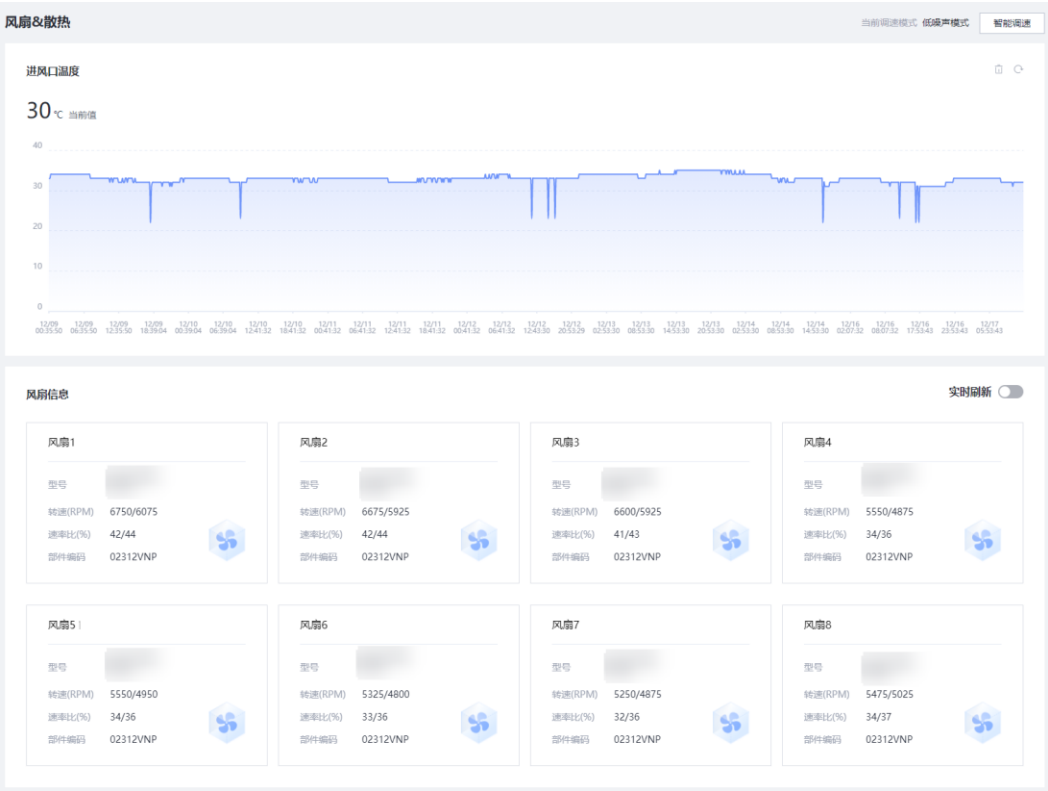
当服务器风扇调速模式为手动调速模式时，在“智能调速”区域框中所作的配置不立即生效。当风扇调速模式切换为自动调速模式后，之前的配置才能生效。

- 查看服务器的在位风扇信息。

界面描述

在导航栏中选择“系统管理 > 风扇&散热”，打开如下图所示界面。

图5-24 风扇&散热



参数描述

表5-20 进风口温度

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

表5-21 风扇模块

参数	描述
基本信息	显示服务器在位风扇模块的基本信息，包括风扇模块槽位号、名称、型号、转速、速率比以及部件编码。
实时刷新	开启或关闭实时刷新风扇信息的功能。

参数	描述
	开启后，风扇“转速”和“速率比”每秒自动刷新。 默认为关闭状态。 说明 开启“实时刷新”功能后，刷新、切换到其他页面或关闭页面会自动关闭该功能。

表5-22 智能调速（风冷系统）

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

5.3.6 BIOS 配置

功能介绍

通过使用“BIOS 配置”界面的功能，您可以设置操作系统第一选择从哪种设备进行启动。

界面描述

在导航栏中选择“系统管理 > BIOS 配置”，打开如下图所示界面。

图5-25 系统启动项

优先引导介质

未配置

☒ 单次有效 ☐ 永久有效

启动顺序

硬盘设备

光盘装置

其他

PXE

保存

参数说明

表5-23 启动项配置

参数	描述
优先引导介质	- 硬盘：表示强制从硬盘启动系统。 - 光驱：表示强制从 CD/DVD 启动系统。 - 软驱/可拔插移动设备：表示强制从软驱或可拔插移动设备启动系统。 - PXE：表示强制从预启动执行环境（PXE，Pre-boot Execution Environment）启动系统。 - BIOS 设置：表示服务器启动后直接进入 BIOS 菜单中。 - 未配置：表示不设置第一启动盘，按 BIOS 中设置的方式启动操作系统。 - 单次有效：优先引导介质的设置仅在下一次重启时生效，重启完成后，优先引导介质自动恢复为“未配置”。 - 永久有效：优先引导介质的设置永久有效。 默认为“未配置”和“单次有效”。

参数	描述
启动顺序	“优先引导介质”为“未设置”时，按照“启动顺序”中的启动方式启动 OS 系统。 单击▲表示上移，单击▼表示下移。 说明 - 在 BIOS 侧，设置启动顺序后立即生效。重启 OS 将触发 BMC 启动顺序与 BIOS 侧启动顺序同步。 - 在 BMC 侧，设置启动顺序后重启 OS 生效。重启 OS 将触发 BIOS 启动顺序与 BMC 侧启动顺序同步。

设置系统启动项

- 步骤 1 在“系统启动项”页签中，根据表 5-23 启动项配置提供的参数信息，设置操作系统的第一启动盘启动设备。
- 步骤 2 单击“保存”。
- 显示“保存成功”表示设置成功。
- 结束

5.4 维护诊断

5.4.1 告警&事件

功能介绍

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

界面描述

在导航栏中选择“维护诊断 > 告警&事件”，打开如下图所示界面。

图5-26 当前告警

序号	级别	主体类型	事件码	产生时间	事件描述	处理建议
4	轻微	PSU	0x03000013	2020-12-17 10:50:36	BMC cannot communicate with PSU 4 (SN:2102312HGYHVL3020179, BN:023...	查看
3	轻微	PSU	0x03000013	2020-12-17 10:50:36	BMC cannot communicate with PSU 3 (SN:2102312HGYHVK8012438, BN:02...	查看
2	轻微	PSU	0x03000013	2020-12-17 10:50:35	BMC cannot communicate with PSU 1 (SN:2102312HGYHVL4022846, BN:023...	查看
1	轻微	PSU	0x03000013	2020-12-17 10:50:35	BMC cannot communicate with PSU 2 (SN:2102312HGYWOL4014704, BN:02...	查看

图5-27 系统事件

筛选条件 条

告警级别

全部紧急严重轻微正常

主体类型

全部BIMABMCCPUCPU BoardCableChassisDiskDisk BackplaneExpanderFanI/O BoardLCDMainboardMemoryNICPCHPCIe CardPHYPSUPSU BackplanePortRAID CardSystem

产生时间

全部今天近7天近30天自定义

输入查询

事件描述或事件码

查询重置

序号	图标	主体类型	状态	事件码	产生时间	事件描述	处理建议
50	正常	BMC	Asserted	0x1A000021	2020-12-28 19:03:09	BMC is reset and started.	
49	正常	BMC	Asserted	0x1A000021	2020-12-28 17:46:15	BMC is reset and started.	
48	正常	BMC	Asserted	0x1A000029	2020-12-28 17:27:39	BMC time is stepped by more than 9 minutes.	查看
47	正常	RAID Card	Asserted	0x06000015	2020-12-28 17:30:38	FIO RAID card 1 BBU is present (SN:023XNBCNL4006425).	
46	正常	Port	Deasserted	0x29000002	2020-12-28 17:27:56	LOM Port 4 disconnected.	
45	正常	System	Asserted	0x2C00000F	2020-12-28 17:27:50	The host was restarted due to unrecognized reason.	
44	正常	RAID Card	Asserted	0x06000013	2020-12-28 17:27:49	FIO RAID card 1 BBU is absent (SN:023XNBCNL4006425).	查看
43	正常	Port	Asserted	0x29000001	2020-12-28 17:27:48	LOM Port 4 disconnected.	查看
42	正常	BMC	Asserted	0x1A000021	2020-12-28 17:26:11	BMC is reset and started.	
41	正常	RAID Card	Asserted	0x06000015	2020-12-28 17:01:12	FIO RAID card 1 BBU is present (SN:023XNBCNL4006425).	
40	正常	BMC	Asserted	0x1A000021	2020-12-28 17:00:36	BMC is reset and started.	
39	正常	RAID Card	Asserted	0x06000015	2020-12-11 15:55:26	FIO RAID card 1 BBU is present (SN:023XNBCNL4006425).	
38	正常	RAID Card	Asserted	0x06000013	2020-12-11 15:54:58	FIO RAID card 1 BBU is absent (SN:023XNBCNL4006425).	查看
37	正常	System	Asserted	0x2C00000F	2020-12-11 15:52:35	The host was restarted due to unrecognized reason.	
36	正常	RAID Card	Asserted	0x06000015	2020-12-11 15:34:00	FIO RAID card 1 BBU is present (SN:023XNBCNL4006425).	

15

总条数: 50

1234>

跳转

1

参数说明

表5-24 当前告警&系统事件

参数	描述
序号	事件的排序。
级别	事件的级别。 ：表示紧急告警，可能会使设备下电、系统中断。因此需要您马上采取相应的措施进行处理。 ：表示严重告警，会对系统产生较大的影响，有可能中断系统的正常运行，导致业务中断。 ：表示轻微告警，不会对系统产生大的影响，但需要您尽快采取相应的措施，防止故障升级。 ：表示正常事件，系统的正常运行记录。
主体类型	产生系统事件的部件类型。
状态	系统事件的状态。

参数	描述
	取值范围： - Asserted：表示系统事件已产生。 - Deasserted：表示系统事件已恢复。
事件码	系统事件管理软件系统中的唯一标识。
产生时间	系统事件的产生时间。
事件描述	系统事件的描述信息。
处理建议	对故障类事件的简要处理建议。

搜索系统事件

- 步骤 1 在“告警&事件”页面单击“系统事件”页签。
- 步骤 2 单击“筛选条件”。
- 打开筛选条件设置区域。
- 步骤 3 根据表 5-25 搜索条件说明提供的参数信息，设置筛选条件。单击“重置”，可以全部清除设置好的筛选条件，重新设置。

表5-25 搜索条件说明

参数	描述
告警级别	系统事件的级别。 取值范围： - 全部 - 紧急 - 严重 - 轻微 - 正常
主体类型	产生系统事件的部件类型。 取值范围：不同服务器的事件源不同，以实际情况为准。
产生时间	产生系统事件的时间。 取值范围： - 全部 - 今天 - 近 7 天 - 近 30 天 - 自定义

参数	描述
	说明 当选择“自定义”时，需要在弹出的输入框中设置起止时间。
输入查询	系统事件的描述信息或事件码。 您可以在“输入查询”右侧的文本框中输入以下内容： - 事件描述中任意连续的字符串。 - 完整的事件码，可带“0x”或不带“0x”。

步骤 4 单击“查询”。

页面将显示符合筛选条件的事件列表。

----结束

清除所有系统事件

须知

系统不能恢复被清除的系统事件，请谨慎操作。

步骤 1 在“告警&事件”页面单击“系统事件”页签。

步骤 2 单击页面右上角的。

将清除所有系统事件。

----结束

下载所有系统事件

步骤 1 在“告警&事件”页面单击“系统事件”页签。

步骤 2 单击页面右上角的。

下载的文件将自动保存到本地 PC 的默认路径。

----结束

5.4.2 告警上报

功能介绍

通过使用“告警上报”界面的功能，您可以：

- 设置 BMC 系统向第三方服务器以 Syslog 报文方式发送日志。

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

 说明

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

界面描述

在导航栏中选择“维护诊断 > 告警上报”，打开如下图所示界面。

图5-28 Syslog 报文通知

Syslog功能

Syslog使能

告警级别

正常

Syslog消息格式

自定义

Syslog主机标识

单板序列号

传输协议

TLS

TCP

UDP

认证方式

单向认证

双向认证

服务器根证书

上传

本地证书

上传

证书信息

签发者

CN=H3CComSec, O=H3C, OU=H3C, C=CN

使用者

CN=H3CComSec, O=H3C, OU=H3C, C=CN

有效起止日期

Jun 18 2021 UTC - Jun 18 2026 UTC

序列号

01

证书吊销列表

已配置 上传 删除

吊销列表有效日期

Jun 18 2021 UTC - Jun 18 2026 UTC

证书信息

签发者

CN=H3CComSec, O=H3C, OU=H3C, C=CN

使用者

CN=H3CComSec, O=H3C, OU=H3C, C=CN

有效起止日期

Nov 22 2021 UTC Nov 22 2026 UTC

序列号

02

保存

Syslog服务器和报文格式

序号	服务器地址	端口	日志类型	当前状态	操作
1			操作日志 + 安全日志 + 事件日志	已配置	编辑 测试
2			操作日志 + 安全日志 + 事件日志	已配置	编辑 测试
3			操作日志 + 安全日志 + 事件日志	已配置	编辑 测试
4			操作日志 + 安全日志 + 事件日志	已配置	编辑 测试

2023-07-27

77

图5-29 邮件通知

SMTP功能

SMTP使能

SMTP服务器地址

SMTP服务器端口

25

是否启用TLS

是

否

校验端服务器证书

端服务器证书

上传

邮件信息

是否启用匿名

是

否

* 发件人用户名

输入不能为空。

* 发件人密码

发件人邮件地址

邮件主题

Server Alert

主题附带

☐ 单板序列号

☐ 产品资产标签

☐ 主机名

告警发送级别

正常

保存

接收告警的邮件地址

序号	邮件地址	描述	发送邮件	操作
1			已关闭	编辑 测试
2			已关闭	编辑 测试
3			已关闭	编辑 测试
4			已关闭	编辑 测试

图5-30 Trap 报文通知

Trap功能

Trap使能

Trap版本

SNMPv3

选择V3用户

Administrator

Trap模式

精准告警模式 (推荐)

Trap主机标识

单板序列号

告警发送级别

正常

保存

设置Trap服务器和报文格式

序号	Trap服务器地址	Trap端口	带内转发	当前状态	操作
1	192.168.1.1	162	已关闭	已开启	编辑 测试
2		162	已关闭	已关闭	编辑 测试
3		162	已关闭	已关闭	编辑 测试
4		162	已关闭	已关闭	编辑 测试

参数说明

须知

启用 TCP 或 UDP 传输协议会降低系统安全性，请谨慎操作。

表5-26 Syslog 报文通知

参数	描述
Syslog 功能	
Syslog 使能	设置开启或关闭自动上报 Syslog 报文。 默认为关闭状态。
告警级别	以 Syslog 方式上报给第三方服务器的事件信息级别。 取值范围： • [NULL]：不发送告警信息或正常事件信息。 • 紧急：仅发送紧急级别的告警信息。 • 严重：发送包括严重、紧急级别的告警信息。 • 轻微：发送包括轻微、严重、紧急级别的告警信息。 • 正常：发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。 默认为“正常”。
Syslog 消息格式	选择 Syslog 报文上报信息的格式。 • 自定义：Syslog 报文上报的信息包括 Syslog 消息的优先级、产品名称、Syslog 主机标识、设备位置以及日志类型。 • RFC3164：Syslog 报文消息的格式遵循 RFC3164 规范，上报的信息包括 Syslog 消息的优先级、时间戳、主机名称、进程名称以及日志类型。 默认为“自定义”。 说明 设置为“RFC3164”消息格式时，“Syslog 主机标识”不支持设置，默认为“主机名”。
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 默认为“单板序列号”。
传输协议	Syslog 报文在 BMC 系统和 Syslog 服务器之间传输时，使用的传输协议。 取值范围：

参数	描述
	• 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。 默认为“TLS”。
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。 默认为“单向认证”。
服务器根证书	在建立数据连接时, 使用此处上传的服务器根证书对 Syslog 服务器发送来的报文进行验证。 说明 • 支持导入服务器根证书文件的格式为“.crt”、“.cer”和“.pem”, 最大不超过 100KB。 • 请定期更新证书, 否则可能存在安全风险。
本地证书	在建立数据连接时, BMC 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 BMC 系统) 的验证。 说明 • 支持导入本地证书文件的格式为“.pfx”和“.p12”, 最大不超过 1MB。 • 请定期更新证书, 否则可能存在安全风险。
证书信息	显示上传的服务器根证书信息, 包括: • 签发者 • 使用者 • 有效起止日期 • 序列号 • 证书吊销列表 • 吊销列表有效日期 说明 • 证书吊销列表表示证书吊销的状态: • 已配置: 表示该证书的吊销文件已上传, 在 TLS 连接时, 会进行证书吊销校验。 • 未配置: 表示该证书的吊销文件未上传。 • 证书吊销文件的格式为“*.crl”, 编码格式为 Base64, 最大不超过 100KB。 • 吊销列表过期会导致相应的认证功能失败。

参数	描述
	证书吊销列表设置方法：单击“上传”选择客户端保存的证书吊销文件。单击“删除”删除证书吊销列表。 说明 删除证书吊销列表，可能会导致使用过期的证书，请注意安全风险。
Syslog 服务器和报文格式	
序号	Syslog 报文发送通道。您最多可以定义四个通道。
服务器地址	Syslog 服务器地址信息。 取值范围： - IPv4 地址 - IPv6 地址 - 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“BMC 管理 > 网络配置”页面配置正确的 DNS 信息。 - 如果域名的 IP 地址发生变化，请手动关闭 Syslog 服务后再重新打开。 - 域名的取值原则： - 最大长度为 255 个字符。 - 可由数字、大小写英文字母和连接号 (-)，点号 (.) 组成。 - 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 - 任意两个点号之间的字符长度不允许超过 63。
端口	Syslog 服务器的端口号。 取值范围：1~65535。
日志类型	需要使用 Syslog 报文上报的日志类型。 取值范围：您可以勾选“操作日志”、“安全日志”或“事件日志”中的一项或多项。 默认为全选。
当前状态	设置某个通道的启用状态。 默认为关闭状态。
操作	- 单击“编辑”，Syslog 服务器和报文格式处于可编辑状态。 - 单击“测试”，可以测试已设置的 Syslog 通道是否可用。显示“操作成功”表示该通道可用。 说明 如果修改了“Syslog 功能”区域的参数，请务必单击“Syslog 功能”区域的“保存”按钮后再进行测试，否则修改后的参数不能生效。

表5-27 邮件通知

参数	描述
SMTP 功能	
SMTP 使能	设置开启或关闭 SMTP 服务。 默认为关闭状态。
SMTP 服务器地址	SMTP 服务器的 IPv4、IPv6 地址或域名。 域名的取值原则： - 最大长度为 255 个字符。 - 可由数字、大小写英文字母和连接号 (-)，点号 (.) 组成。 - 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 - 任意两个点号之间的字符长度不允许超过 63。
SMTP 服务器端口	SMTP 服务器的端口号。 取值范围：1~65535。 默认值：25。
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。 默认为“是”。 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。 - 当前 BMC 不支持 TLS 1.0 协议。
校验端服务器证书	启用 TLS 加密传输时，设置开启或关闭校验端服务器证书。 默认为关闭状态。
端服务器证书	在建立数据连接时，使用此处上传的端服务器证书对 SMTP 服务器发送来的报文进行验证。 说明 - 支持导入端服务器证书文件的格式为“.crt”、“.cer”和“.pem”，最大不超过 100KB。 - 请定期更新证书，否则可能存在安全风险。
证书信息	显示上传的端服务器证书信息，包括： - 签发者 - 使用者 - 有效起止日期 - 序列号

参数	描述
邮件信息	
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 BMC 系统向 SMTP 服务器发送告警信息邮件时使用。 默认为“否”。 说明 默认情况下，SMTP 服务器不使用匿名，从安全性考虑，请尽量不要使用匿名。
发件人用户名及密码	通过邮箱发送告警信息时使用的发件人用户名和密码。 用户名可以由数字、英文字母或特殊字符中的 1 种或几种组成，且不能为空。 密码为该用户在对应 SMTP 服务器上的用户密码。 取值范围： • 用户名必须是长度为 1~64 之间字符串。 • 密码必须是长度为 1~50 之间的字符串。
发件人邮件地址	通过邮箱发送告警信息时使用的邮件地址。 取值范围：最大为 255 位的字符串。 由英文字母、数字和其他特殊字符组成。格式必须为“xx@xxx.xx”。
邮件主题/主题附带	电子邮件的标题。 取值范围：0~255 位的字符串，由数字、英文字母和特殊字符组成。默认为“Server Alert”。 在电子邮件标题中可附带关键信息，可以是“主机名”、“单板序列号”或“产品资产标签”。
告警发送级别	通过 SMTP 服务器发送的告警信息的级别。 取值范围： • [NULL]：不发送告警信息或正常事件信息。 • 紧急：仅发送紧急级别的告警信息。 • 严重：发送包括严重、紧急级别的告警信息。 • 轻微：发送包括轻微、严重、紧急级别的告警信息。 • 正常：发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。 默认为“正常”。
接收告警的邮件地址	

参数	描述
序号	告警邮件的发送通道。您最多可以定义四个通道。
邮件地址	接收电子邮件的邮箱地址。该地址必须已在 SMTP 服务器上进行了注册。 取值范围：最大为 255 位的字符串，格式必须为“xx@xxx.xx”。 由英文字母、数字和其他特殊字符组成。
描述	对接收电子邮件的邮箱的相关描述。 取值范围：0~255 位的字符串，由数字、英文字母和特殊字符组成。
发送邮件	设置 BMC 是否向该接收地址发送邮件。 默认为关闭状态。
操作	- 单击“编辑”，接收告警的邮件地址处于可编辑状态。 - 单击“测试”，可以测试已设置的目标邮箱地址是否可达。 说明 如果修改了“SMTP 功能”区域的参数，请务必单击“SMTP 功能”区域的“保存”按钮后再进行测试，否则修改后的参数不能生效。

表5-28 Trap 报文通知

参数	描述
Trap 功能	
Trap 使能	设置开启或关闭自动上报 Trap 报文。 默认为开启状态。
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。

参数	描述
	“SNMPv3”的鉴权算法和加密算法可在“用户&安全 > 本地用户”中设置。 默认取值：“SNMPv1”。
选择 V3 用户	Trap 版本选择“SNMPv3”时，需要同时设置协议所需的用户名。 默认情况下，使用 BMC 提供的默认用户作为 Trap V3 用户。
Trap 模式	Trap 信息上报时采用的模式。 取值范围： “精准告警模式(推荐)”：以与事件一一对应的 SNMP 节点 OID 作为 Trap 事件的标识，相较“OID 模式”和“事件码模式”，可提供更为精准的定位信息。 “OID 模式”：以 SNMP 节点的 OID 作为 Trap 事件的标识。 “事件码模式”：以产生事件的事件码作为 Trap 事件的标识。 默认取值：“精准告警模式(推荐)”
Trap 主机标识	Trap 信息上报时，用于标识信息来源。 取值范围： - 单板序列号 - 产品资产标签 - 主机名 默认取值：“单板序列号”。
团体名	团体名为 Trap 方式的口令。“版本”设置为“SNMPv1”或“SNMPv2c”时才能设置“团体名”。 - 不开启密码检查时的取值原则： - 长度为 1~32 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 8~32 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： ~!@#\$%^&*()-_+=+\\[{}];:","<.>/? - 不能包含空格。
确认团体名	此处输入的内容需要与“团体名”中相同。

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： • [NULL]：不发送告警信息或正常事件信息。 • 紧急：仅发送紧急级别的告警信息。 • 严重：发送包括严重、紧急级别的告警信息。 • 轻微：发送包括轻微、严重、紧急级别的告警信息。 • 正常：发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。 默认为“正常”。
设置 Trap 服务器和报文格式	
序号	自定义以 Trap 发送告警的通道。您最多可以定义四个通道。
Trap 服务器地址	接收 Trap 方式发送的告警信息的服务器地址。服务器地址支持 IPv4、IPv6 和域名。 域名的取值原则： • 最大长度为 255 个字符。 • 可由数字、大小写英文字母和连接号 (-)，点号 (.) 组成。 • 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 • 任意两个点号之间的字符长度不允许超过 63。
Trap 端口	接收 Trap 方式发送的告警信息的端口号。 取值范围：1~65535。 默认取值：162。 说明 单击“重置”，接收 Trap 端口号改为默认的“162”。
带内转发	设置开启或关闭 Trap 信息带内转发。带内转发功能指将 Trap 信息通过 OS 侧转发至 Trap 服务器。 默认为关闭状态。 说明 • 当 BMC 无法连接到 Trap 服务器时，若此时服务器 OS 可与 Trap 服务器连通，则可启用带内转发，将 Trap 信息通过 OS 侧转发至 Trap 服务器。 • 需在服务器 OS 侧安装 BMA 2.0 并完全启动后，才能使通道处于可用状态。
当前状态	设置启用某个通道的启用状态。 默认为关闭状态。
报文分隔符	选择 Trap 格式中每个关键字段之间的分隔符，例如“;”。

参数	描述
	说明 仅在“事件码模式”下可设置此参数。
报文显示内容	选择需要上报的关键字。 说明 仅在“事件码模式”下可设置此参数。
显示关键字	显示 Trap 格式中每个关键字的名称。 说明 仅在“事件码模式”下可设置此参数。
样例	根据您选择的分隔符、显示内容以及显示的关键字名称给出示例。
操作	- 单击“编辑”，Trap 服务器和报文格式处于可编辑状态。 - 单击“测试”，可以测试已设置的 Trap 通道是否可用。显示“操作成功”表示该通道可用。 说明 如果修改了“Trap 功能”区域的参数，请务必单击“Trap 功能”区域的“保存”按钮后再进行测试，否则修改后的参数不能生效。

5.4.3 录像截屏

功能介绍

通过使用“录像播放”功能，您可以：

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

 说明

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

通过使用“屏幕截图”功能，您可以：

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

 说明

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

录像回放控制窗口中的按钮及其作用如表 5-29 录像回放控制窗口按钮说明所示。

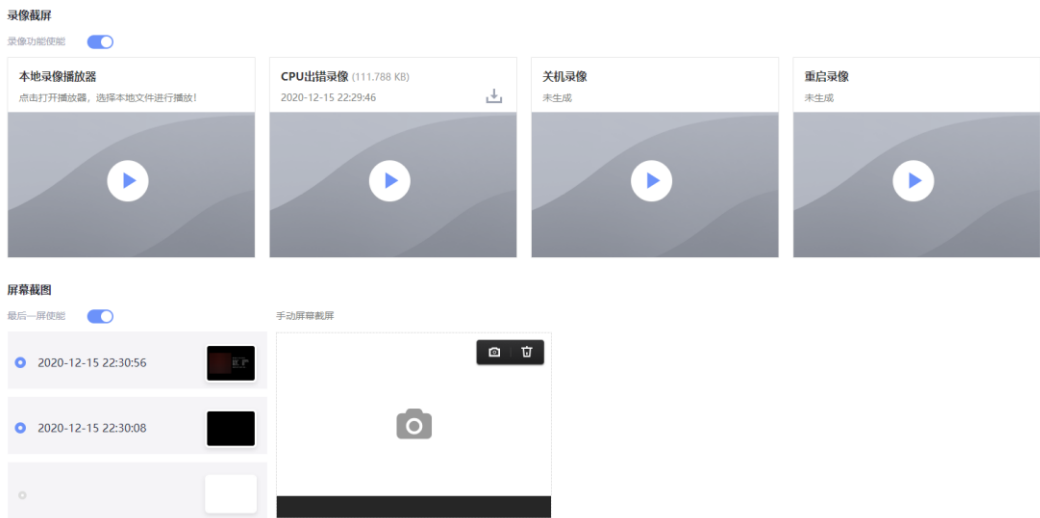
表5-29 录像回放控制窗口按钮说明

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

界面描述

在导航栏中选择“维护诊断 > 录像截屏”，打开如下图所示界面。

图5-31 录像截屏



操作步骤

表5-30 录像播放功能操作步骤

操作	操作步骤
录像功能使能	开启或关闭录像功能。 单击  或  并根据提示保存，可切换状态。  表示开启录像功能。  表示关闭录像功能。 默认状态： 
下载 Java 播放器	- 单击 。 - 单击“Java 播放器”。 - 根据页面提示信息保存文件。 将自动保存播放器文件到本地 PC 的默认路径。播放器文件的格式为“.jnlp”。 说明 HTML5 播放器可以直接使用，不需要下载。
下载录像	单击“CPU 出错录像”、“关机录像”或“重启录像”右侧的 ，将下载录像文件，并自动保存到本地 PC 的默认路径。 说明 如果录像文件大小超过 10MB，建议下载并保存到本地 PC。否则，在进行一键收集信息时，BMC 会删除超过 10MB 的录像文件。
播放本地录像文件	选择以下任意一种播放器播放本地录像文件：

操作	操作步骤
	• 打开“本地录像播放器”区域框中的 HTML5 播放器。 • 打开从“本地录像播放器”区域框中下载的 Java 播放器。 2. 在播放器中，单击 ，选择本地 PC 上存放的录像文件。 3. 单击“打开”。 将返回播放器窗口并开始播放该录像文件。 4. (可选) 根据实际需要调整录像播放状态。 • 单击 ，以正常速度的 1 倍、2 倍或 4 倍快速播放录像文件。 • 单击 ，以正常速度的 1 倍、0.5 倍或 0.25 倍缓慢播放录像文件。 • 向左或向右拖动 ，控制录像文件的播放进度。 • 单击 。 系统循环播放该录像文件。 • 单击 。 播放器窗口最大化显示在屏幕上。
播放在线录像文件	1. 选择以下任意一种播放器播放在线录像文件： • 打开“CPU 出错录像”、“关机录像”或“重启录像”区域框中的 HTML5 播放器。 • 打开从“CPU 出错录像”、“关机录像”或“重启录像”区域框中下载的 Java 播放器。 2. (可选) 根据实际需要调整录像播放状态。 • 单击 ，以正常速度的 1 倍、2 倍或 4 倍快速播放录像文件。 • 单击 ，以正常速度的 1 倍、0.5 倍或 0.25 倍缓慢播放录像文件。 • 向左或向右拖动 ，控制录像文件的播放进度。 • 单击 。 播放器窗口最大化显示在屏幕上。
截取录像图像	在录像播放过程中，单击 。 将剪切到的图像保存到客户端，图像格式为“*.jpg”。

表5-31 屏幕截图功能操作步骤

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

5.4.4 系统日志

功能介绍

通过使用“PCIe 接口”，您可以开启或关闭 PCIe 接口。开启该功能时，PCIe 接口可以用于 MCTP 通信、带内带外系统通信和黑匣子数据收集。

通过使用“黑匣子功能”，您可以开启或关闭黑匣子数据下载功能，开启该功能时，您可以下载黑匣子存储器中的数据到本地。

黑匣子包含一个存储器和一款故障监控软件：

- 黑匣子存储器是系统内置的用于故障信息记录的存储芯片。它不依赖于服务器的硬盘。
黑匣子存储器的最大容量为 4MB，用于记录操作系统崩溃时的内核信息。
- 故障监控软件记录服务器操作系统崩溃时的内核信息。

在使用黑匣子功能前，服务器上必须已安装黑匣子的故障监控软件（例如 BMA，其安装和使用方法可参考 BMA 用户指南）。

- 在开启黑匣子功能的情况下，如果服务器上未安装黑匣子驱动，则可能在 OS 侧出现未知设备。

通过使用“系统串口数据记录功能”区域框的功能，您可以开启或关闭串口数据下载记录功能，开启该功能时您可以下载系统串口最近的数据到本地。

界面描述

在导航栏中选择“维护诊断 > 系统日志”，打开如下图所示界面。

图5-32 系统日志



操作步骤

表5-32 黑匣子功能操作步骤

操作	操作步骤
开启或关闭 PCIe 接口	1. 将“PCIe 接口”右侧的按钮设置为, 表示开启 PCIe 接口。将按钮设置为, 表示关闭 PCIe 接口。单击或, 可切换状态。 2. 重启服务器。 须知 - PCIe 接口默认为开启状态。 - 开启或关闭 PCIe 接口都需要重启服务器后才能生效。
下载黑匣子数据文件	请在“黑匣子功能”为状态下下载黑匣子数据文件。 单击“黑匣子功能”区域框的.

操作	操作步骤
	黑匣子数据文件将自动保存到本地 PC 的默认地址。 说明 “黑匣子功能”默认为开启状态。 - BMC 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 BMA 用户指南。 - 在不同浏览器下，页面提示保存文件的信息略有不同。

表5-33 系统串口数据记录功能操作步骤

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

表5-34 NPU 日志功能操作步骤

操作	操作步骤
下载 NPU 日志文件	单击“NPU 日志”区域框的. NPU 日志文件自动保存到本地 PC 的默认路径。 说明 - 同一时间仅支持下载一个 NPU 的日志。 - 在不同浏览器下，页面提示保存文件的信息略有不同。

5.4.5 BMC 日志

功能介绍

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

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

说明

上下电及重启记录的成功操作日志，只表示软件触发动作成功，不代表硬件真正成功。

- 通过“运行日志”区域框，您可以查看服务器 RAS 相关日志。

BMC 为运行日志提供 200KB 的存储空间，可记录约 2000 条运行日志，运行日志达到 200KB 时会自动压缩成 1 个压缩包，当有新的压缩包生成，会自动删除旧的压缩包。
- 通过“安全日志”区域框，您可以：
 - 查看用户通过串口、SSH 接口登录、退出 BMC 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。

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

界面描述

在导航栏中选择“维护诊断 > BMC 日志”，打开如下图所示界面。

图5-33 操作日志

↓

序号	接口	用户	IP地址	产生时间	详细信息
311	WEB	Administrator		2020-06-29 17:08:45	Set power off timeout to (enable) successfully
310	WEB	Administrator		2020-06-29 16:24:58	Administrator() login successfully over the WebUI
309	WEB	Administrator		2020-06-29 16:12:16	Set web session mode to (share) successfully
308	WEB	Administrator		2020-06-29 16:12:10	Administrator() login successfully over the WebUI
307	WEB	Administrator		2020-06-29 16:12:10	User (Administrator@) is forced to log out because the same u...
306	WEB	Administrator		2020-06-29 16:02:53	Administrator() login successfully over the WebUI
305	WEB	Administrator		2020-06-29 16:02:53	User (Administrator@) is forced to log out because the same us...
304	WEB	Administrator		2020-06-29 16:02:33	Administrator() login successfully over the WebUI
303	WEB	Administrator		2020-06-29 16:02:33	User (Administrator@) is forced to log out because the same u...
302	WEB	Administrator		2020-06-29 15:59:53	Administrator() login successfully over the WebUI
301	WEB	Administrator		2020-06-29 15:59:53	User (Administrator@) is forced to log out because the same us...
300	WEB	Administrator		2020-06-29 15:26:46	Set web session timeout to (50) minutes successfully
299	WEB	Administrator		2020-06-29 15:26:39	Administrator() login successfully over the WebUI
298	WEB	Administrator		2020-06-29 15:25:44	Administrator() logout by session timeout
297	WEB	Administrator		2020-06-29 15:18:32	Administrator() login successfully over the WebUI

15 总条数: 311 1 2 3 4 5 - 21 跳转 1

图5-34 运行日志

↓

序号	级别	产生时间	详细信息
264	WARN	2020-12-16 07:19:08	Nand Flash, close nand flash write protection.
263	WARN	2020-12-16 07:12:27	Nand Flash, close nand flash write protection.
262	WARN	2020-12-16 07:10:07	Nand Flash, close nand flash write protection.
261	WARN	2020-12-14 04:15:31	Nand Flash, close nand flash write protection.
260	WARN	2020-12-14 04:08:28	Nand Flash, close nand flash write protection.
259	WARN	2020-12-14 02:08:03	Nand Flash, close nand flash write protection.
258	WARN	2020-12-14 02:00:51	Nand Flash, close nand flash write protection.
257	WARN	2020-12-11 14:45:02	Nand Flash, close nand flash write protection.
256	WARN	2020-12-11 14:38:37	Nand Flash, close nand flash write protection.
255	WARN	2020-12-11 13:06:58	Nand Flash, close nand flash write protection.
254	WARN	2020-12-11 13:00:28	Nand Flash, close nand flash write protection.
253	WARN	2020-12-11 12:54:03	Nand Flash, close nand flash write protection.
252	WARN	2020-12-11 12:09:35	Nand Flash, close nand flash write protection.
251	WARN	2020-12-11 12:02:58	Nand Flash, close nand flash write protection.
250	WARN	2020-12-11 10:42:00	Nand Flash, close nand flash write protection.

15 总条数: 264 1 2 3 4 5 - 18 跳转 1

图5-35 安全日志

↓

序号	接口	主机	产生时间	详细消息
1016	sshd[30233]		2020-12-16 22:27:29	pam_unix(sshd:session): session closed for user Administrator
1015	sshd[30266]		2020-12-16 22:09:53	error: open /dev/tty failed - could not set controlling tty: Permission denied
1014	sshd[30260]		2020-12-16 22:09:52	error: setlogin failed: Function not implemented
1013	sshd[30233]		2020-12-16 22:09:52	pam_unix(sshd:session): session opened for user Administrator(uid=502) by ...
1012	sshd[30233]		2020-12-16 22:09:52	Accepted password for Administrator from: port 58618 ssh2
1011	sshd[22990]		2020-12-16 21:28:30	pam_unix(sshd:session): session closed for user Administrator
1010	sshd[23123]		2020-12-16 21:28:30	Disconnected from user Administrator: port 56757
1009	sshd[23123]		2020-12-16 21:28:30	error: Received disconnect from: port 56757:0:
1008	sshd[23129]		2020-12-16 21:25:32	error: open /dev/tty failed - could not set controlling tty: Permission denied
1007	sshd[23123]		2020-12-16 21:25:32	error: setlogin failed: Function not implemented
1006	sshd[22990]		2020-12-16 21:25:32	pam_unix(sshd:session): session opened for user Administrator(uid=502) by ...
1005	sshd[22990]		2020-12-16 21:25:32	Accepted password for Administrator from: port 56757 ssh2
1004	sshd[22990]		2020-12-16 21:25:26	Failed password for Administrator from: port 56757 ssh2
1003	sshd[22990]		2020-12-16 21:24:53	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ss...
1002	sshd[30496]		2020-12-16 19:18:43	pam_unix(sshd:session): session closed for user Administrator

15 总条数: 1,016 1 2 3 4 5 ... 68 跳转 1

参数说明

表5-35 操作日志

参数	描述
序号	操作发生的顺序，ID 越小的操作发生越早。
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）。 - 跳帽重置 IP 和默认用户密码。 - 部件热插拔。
IP 地址	进行操作的终端 IP。 “IP 地址”显示为“HOST”表示操作由业务侧执行。 “IP 地址”显示为“X.X.X.X”表示由登录设备的客户端执行。 以下情况中，“IP 地址”显示为“127.0.0.1”表示本操作由本机执行。 - 定位按钮或电源按钮被按下。 - 接口为本地串口。

参数	描述
	- 跳帽重置 IP 和默认用户密码。 - 部件热插拔。
产生时间	操作发生的时间。
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 BMC 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 BMC caused by upgrade successfully
下载	单击  ，操作日志文件将自动保存到本地 PC 的默认路径。
注：“用户”和“IP 地址”如果不满足上述情况，无法解析时显示为“unknown”。	

表5-36 运行日志

参数	描述
序号	操作发生的顺序，ID 越小的操作发生越早。
级别	运行错误的告警级别。 - ERROR - WARN - INFO
产生时间	运行错误发生的时间。
详细信息	运行错误的详细描述信息。
下载	下载运行日志。 单击 ，运行日志文件将自动保存到本地 PC 的默认路径。

表5-37 安全日志

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

参数	描述
主机	系统的主机名。
产生时间	操作发生的时间。
详细信息	显示用户的登录、退出操作详情。
下载	下载安全日志。 单击  , 安全日志文件将自动保存到本地 PC 的默认路径。

5.4.6 工作记录

功能介绍

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

说明

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

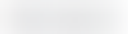
界面描述

在导航栏中选择“维护诊断 > 工作记录”，打开如下图所示界面。

图5-36 工作记录

 添加工作记录

本页面内容对所有用户可见且可编辑，请勿记录敏感信息。

	工作记录1	 
用户名	Administrator	
IP地址		
添加时间	2020/12/17 11:14:48	
内容信息	AAAAAAA	

操作步骤

表5-38 工作记录功能操作步骤

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

5.5 用户&安全

5.5.1 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 BMC 系统的本地用户。

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

界面描述

在导航栏中选择“用户&安全 > 本地用户”，打开如下图所示界面。

图5-37 本地用户

添加用户						
ID	用户名	角色	登录接口		操作	
2	Administrator	管理员	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
3		操作员	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
4		自定义用户4	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
5		管理员	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
6		普通用户	Web	SNMP SSH SFTP Local Redfish	编辑	禁用 删除
7		普通用户	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
8		管理员	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
9		管理员	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除
10		普通用户	Web	SNMP IPMI SSH SFTP Local Redfish	编辑	禁用 删除

参数说明

表5-39 本地用户

参数	描述
添加用户	打开配置新建本地用户的区域框。
ID	用户在 BMC 系统内的编号，用于唯一标识一个用户。
用户名	登录 BMC 系统的用户名称。
角色	用户所属的权限分组。 • 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 • 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 • 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 • 自定义用户：管理员可为自定义用户指定可操作的功能模块。 • 无权限用户：该权限组的用户，不拥有任何权限，常用于定义搁置的用户。
登录接口	用户登录 BMC 的接口，用户可通过已使能的接口登录 BMC 系统。 • SNMP：使能该接口后，用户可使用符合 SNMP 协议的终端工具（例如 MIB Browser）登录 BMC 系统。 • SSH：使能该接口后，用户可使用符合 SSH 协议的终端工具（例如 PuTTY）登录 BMC 命令行。 • IPMI：使能该接口后，用户可使用符合 IPMI 协议的终端工具（例如 IPMI Tool）登录 BMC 命令行。 • Local：使能该接口后，用户可通过服务器的串口登录 BMC 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 BMC 文件系统。 • Web：使能该接口后，用户可使用浏览器登录 BMC Web 界面。 • Redfish：使能该接口后，用户可使用符合 Redfish 协议的终端工具登录 BMC 系统。
操作	• 编辑：打开编辑已有本地用户信息的区域框。 • 禁用：设置用户状态为停用状态。

参数	描述
	• 启用：设置用户状态为启用状态。 • 删除：删除已有本地用户。 说明 • 包括管理员、操作员、普通用户、自定义用户在内的所有本地用户均可删除。 • 当 BMC 中存在多个启用的管理员时，可以修改默认用户的权限。当仅有一个启用的管理员用户时，该管理员用户不能被修改权限、禁用或删除。 • 若已在“用户&安全 > 安全增强”页面开启了“业务侧用户管理使能”，可在 OS 侧通过发送标准的 IPMI 命令为 BMC 添加本地用户。
有效期（天）	用户密码的使用期限。
登录规则	用户需要遵循的登录规则，用户登录时，受已选择的登录规则限制。

表5-40 SSH 公钥

参数	描述
上传	为 SSH 用户导入公钥。
公钥文件	选择客户端上保存的 SSH 公钥文件进行上传。 公钥文件的格式为“.pub”，最大不超过 2KB。
公钥文本	在文本框中输入 SSH 公钥的具体内容进行上传。
登录密码	当前正在进行该操作的用户的登录密码。

添加用户

BMC 系统最多可添加 15 个不同名称的用户。

步骤 1 单击页面左上角的“添加用户”。

弹出添加用户的窗口。

步骤 2 根据表 5-41 添加用户所需参数设置用户的基本属性。

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

表5-41 添加用户所需参数

参数	描述
用户 ID	新添加用户的 ID，取值范围：3～17。
用户名	新建用户的名称。 取值范围：1～16 位的字符串。 取值原则： - 由特殊符号、英文字母和数字组成，特殊字符不包括： :;<>,&,"'\^% - 不能包含空格且首字符不能是“#”、“+”或“-”。 - 用户名不能为“.”或“..”。
用户密码	新建用户登录 BMC 系统的用户密码。为了保证安全，用户应定期修改自己的登录密码。 说明 - 只有管理员可以设置密码检查功能的开启状态。 - 禁用密码检查功能会降低系统安全性，请尽量启用此功能。 取值范围： - 关闭密码检查功能后，密码不能为空，可以是数字、英文字母和特殊字符组成的长度不大于 20 的字符串。如果密码长度小于 8 个字符，该用户将无法使用 SNMPv3 接口。 - 启用密码检查功能后，密码复杂度要求： - 长度为 8～20 个字符。 - 至少包含一个空格或者以下特殊字符： `~!@#\$%^&*()-_+=+ {[]};:~",<.>/? - 至少包含以下字符中的两种： - 小写字母：a～z - 大写字母：A～Z - 数字：0～9 - 密码不能是用户名或用户名的倒序。 - 弱口令字典认证功能使能的情况下，密码不能在弱口令字典中。（弱口令可通过导出弱口令字典命令 ipmcset -t user -d weakpwddic -v export 获取。） 说明 使用完全由重复子串构成的口令可能会有安全风险，例如 aa、abababab 或 abcdabcd 等，请尽量避免。
确认密码	新建用户的用户密码，此处输入的内容需要与“用户密码”中相同。
首次登录策略	首次登录时的密码修改策略。 可选取值： 强制修改密码

参数	描述
	提示修改密码 默认取值：强制修改密码
角色	设置新建用户所属的权限分组。 - 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 - 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 - 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 - 自定义用户：管理员可为自定义用户指定可操作的功能模块。 - 无权限用户：该权限组的用户，不拥有任何权限，常用于定义搁置的用户。 说明 - 新建用户默认权限为“无权限用户”。 - 巡检用户设置为仅拥有“查询功能”、“配置自身”、“调试诊断”、“安全配置”模块的操作权限的自定义用户。
登录规则	用户需要遵循的登录规则，用户登录时，受已选择的登录规则限制。
登录接口	用户登录 BMC 的接口，用户可通过已使能的接口登录 BMC 系统。 - SNMP：使能该接口后，用户可使用符合 SNMP 协议的终端工具（例如 MIB Browser）登录 BMC 系统。 - SSH：使能该接口后，用户可使用符合 SSH 协议的终端工具（例如 PuTTY）登录 BMC 命令行。 - IPMI：使能该接口后，用户可使用符合 IPMI 协议的终端工具（例如 IPMI Tool）登录 BMC 命令行。 - Local：使能该接口后，用户可通过服务器的串口登录 BMC 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 BMC 文件系统。 - Web：使能该接口后，用户可使用浏览器登录 BMC Web 界面。 - Redfish：使能该接口后，用户可使用符合 Redfish 协议的终端工具登录 BMC 系统。 说明 新建用户默认支持所有登录接口。

参数	描述
登录密码	当前正在进行该操作的用户的登录密码。
保存	保存对新建用户的配置。
取消	取消对新建用户的配置。

步骤3 单击“保存”。

用户列表中将显示新添加用户的信息。

 说明

创建用户成功之后，需等待约 5 秒之后才能生效。

-----结束

修改用户信息

步骤1 在本地用户列表中，选择需要修改的用户并单击“编辑”。

弹出编辑用户信息的窗口。

步骤 2 根据表 5-42 修改用户信息所需参数提供的信息，修改指定用户的基本信息。

表5-42 修改用户信息所需参数

参数	描述
用户 ID	待修改用户的用户 ID。
用户名	待修改用户的名称。
用户密码	待修改用户的新密码。 • 关闭密码检查功能后，密码不能为空，可以是数字、英文字母和特殊字符组成的长度不大于 20 的字符串。如果密码长度小于 8 个字符，该用户将无法使用 SNMPv3 接口。 • 启用密码检查功能后，密码复杂度要求： – 长度为 8~20 个字符。 – 至少包含一个空格或者以下特殊字符： `~!@#\$%^&*()-_+=~\ {}];:~",<.>/? – 至少包含以下字符中的两种： – 小写字母：a~z – 大写字母：A~Z – 数字：0~9 – 密码不能是用户名或用户名的倒序。 • 弱口令字典认证功能使能的情况下，密码不能在弱口令字

参数	描述
	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 使用完全由重复子串构成的口令可能会有安全风险，例如 aa、abababab 或 abcdabcd 等，请尽量避免。
确认密码	修改后的用户密码，此处输入的内容需要与“用户密码”中相同。
首次登录策略	修改用户密码后首次登录时的密码修改策略。 可选取值： • 强制修改密码 • 提示修改密码
角色	用户所属的权限分组。 • 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 • 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 • 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 • 自定义用户：管理员可为自定义用户指定可操作的功能模块。 • 无权限用户：该权限组的用户，不拥有任何权限，常用于定义搁置的用户。
登录规则	用户需要遵循的登录规则，用户登录时，受已选择的登录规则限制。
登录接口	用户可用于登录的接口，用户可通过已启用的接口登录 BMC 系统。 • SNMP：使能该接口后，用户可使用符合 SNMP 协议的终端工具（例如 MIB Browser）登录 BMC 系统。 • SSH：使能该接口后，用户可使用符合 SSH 协议的终端工具（例如 PuTTY）登录 BMC 命令行。 • IPMI：使能该接口后，用户可使用符合 IPMI 协议的终端工具（例如 IPMI Tool）登录 BMC 命令行。 • Local：使能该接口后，用户可通过服务器的串口登录 BMC 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 BMC 文件系统。 • Web：使能该接口后，用户可使用浏览器登录 BMC Web 界

参数	描述
	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 BMC 系统。 说明 • 开启某个用户的 IPMI 登录接口，需要重置该用户的登录密码。 • 更改某个用户的 SNMP 鉴权算法，需要重置该用户的登录密码和 SNMPv3 加密密码。
加密密码	当登录接口勾选“SNMP”时，需要同时设置此参数。 使用指定用户进行 SNMP 通信时，可为其设置独立的加密密码来保障通信的安全性。其密码规则与本地用户的密码规则一致。 默认取值：与该用户的登录密码一致。 说明 • 未独立设置 SNMPv3 加密密码时，该密码与用户登录密码同步，存在安全隐患，建议尽快修改并妥善保存。独立设置 SNMPv3 加密密码后，该密码不再与用户登录密码同步。 • 使用完全由重复子串构成的口令可能会有安全风险，例如 aa、abababab 或 abcdabcd 等，请尽量避免。
确认密码	与“SNMPv3 加密密码”保持一致。
鉴权算法	SNMPv3 采用的鉴权算法。 可选取值： • MD5 • SHA • SHA256 • SHA384 • SHA512 默认取值：SHA256 说明 • 该设置对“SNMPv3”和“SNMP Trap V3”都有效。 • MD5 算法和 SHA 算法存在安全隐患，建议使用 SHA256、SHA384 或 SHA512 算法。 • 当与上层网管对接时，当前鉴权算法类型需要与网管侧保持一致。
加密算法	SNMPv3 的安全保障之一，采用指定的算法来保障信息传输的安全性。 可选取值： • DES • AES • AES256 默认取值：AES

参数	描述
	说明 • DES 算法存在安全隐患，建议使用 AES 或 AES256 算法。 • 加密算法 AES256 只能与鉴权算法 SHA256、SHA384 或 SHA512 搭配使用。
登录密码	当前正在进行该操作的用户的登录密码。
保存	保存对指定用户的修改。 说明 修改用户名、密码、权限会导致该用户被强制下线。
取消	取消修改用户信息。

步骤 3 单击“保存”。

成功修改用户信息。

 说明

修改用户密码成功之后，需等待约 5 秒之后才能生效。

----结束

删除用户

步骤 1 在本地用户列表中，在待删除的用户列表右侧单击“删除”。

弹出操作确认对话框。

步骤 2 输入当前用户的登录密码并单击“确定”。

显示“操作成功”，用户列表中该用户信息将消失。

----结束

导入 SSH 公钥

 说明

- 在客户端生成私钥后，需要在 BMC 侧导入对应的公钥，保证用户通过 SSH 登录 BMC 系统的安全性和唯一性。
- 每个用户只能导入一个公钥，若需要变更公钥，需要删除已导入的公钥后再导入新的公钥。
- 支持 RFC 4716 和 OpenSSH 格式的公钥，公钥类型为 RSA 或 DSA。当公钥类型为 RSA 时，支持长度为 2048 位和 4096 位。当公钥类型为 DSA 时，支持长度为 2048 位。
- 公钥文件的格式为“.pub”，最大不超过 2KB。

步骤 1 单击待导入 SSH 公钥的用户名左侧的.

步骤 2 单击“SSH 公钥”右侧的“上传”。

弹出导入“公钥上传”窗口，如下图所示。

图5-38 公钥上传

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

☒ 公钥文件

☐ 公钥文本

选择公钥文件

添加文件

★ 登录密码

保存

取消

步骤 3 选择公钥导入方式。

此处可根据实际情况选择“公钥文件”或“公钥文本”。

步骤 4 单击“添加文件”选择生成的公钥。

步骤 5 输入当前登录用户密码。

步骤 6 单击“保存”。

----结束

5.5.2 LDAP

功能介绍

通过使用“LDAP”界面的功能，您可以查看和设置 LDAP 用户的信息。

BMC 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 BMC 系统可以提高系统安全性。LDAP 用户可登录 BMC WebUI，也可通过 SSH 方式登录 BMC 命令行。

说明

LDAP 服务器的 DisplayName 和 CN 要保持一致。

BMC 最多支持同时配置 6 个域服务器。

LDAP 用户登录 BMC 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 BMC 命令行时，无需指定域服务器，由系统自动匹配。

说明

BMC 当前支持与 Windows AD、Linux OpenLDAP 和 FreeIPA 的对接。

界面描述

在导航栏中选择“用户&安全 > LDAP”，打开如下图所示界面。

图5-39 LDAP

LDAP功能

LDAP使能 ⑦ ☒

控制器 1 | 控制器 2 | 控制器 3 | 控制器 4 | 控制器 5 | 控制器 6

基本属性

LDAP服务器地址

LDAP端口

域名

绑定标识名

绑定密码

用户应用文件夹

证书验证

LDAP证书验证使能 ☐

证书校验级别 ☐ Demand ☒ Allow

LDAP证书

支持.cer、.pem、.cert和.crt格式，且文件名不能为空。

服务器证书信息

签发者

CN=, OU=, O=, L=, S=, C=cn

使用者

CN=, OU=, O=, L=, S=, C=cn

有效起止日期

Dec 23 2022 UTC - Dec 23 2032 UTC

序列号

7a 2a 93 11 49 28 04 9f

证书吊销列表

已配置

吊销列表有效日期 ⑦

Jan 03 2023 UTC - Feb 02 2023 UTC

★ 登录密码

保存

LDAP用户组

序号	组名	角色	登录接口	组应用文件夹	登录策略	操作
1	asdf	普通用户	Web SSH Redfish	sdf		编辑 删除

参数说明

表5-43 LDAP 配置

参数	描述
LDAP 使能	开启或关闭 LDAP 组功能。 默认为关闭状态。 说明 启用 LDAP 功能，使用 LDAP 帐户登录 BMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。

参数	描述
控制器 1 BMC 可同时配置 6 个域服务器。用户使用 LDAP 方式登录 BMC 的 WebUI 时，可指定任意一个控制器，或自动适配任意一个控制器。 控制器 2～控制器 6 的配置与控制器 1 类似，均需配置如下参数。 说明 带“*”的项目为必配参数。	
基本属性	
LDAP 服务器地址	LDAP 服务器的地址。 输入格式：IPv4 地址、IPv6 地址或域名。 启用证书验证功能后，该处需要配置为 LDAP 服务器的 FQDN（主机名.域名），且需要在网络配置部分配置 DNS。 说明 域名的取值原则： • 最大长度为 255 个字符。 • 可由数字、大小写英文字母和连接号（-），点号（.）组成。 • 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 • 任意两个点号之间的字符长度不允许超过 63。
LDAPS 端口	LDAP 服务的端口号。 取值范围：1～65535 默认值：636 说明 由于 BMC 仅支持 LDAPS，不支持无 SSL 的 LDAP（端口号：389），所以 LDAP 服务器必须安装证明自身身份的可信任的服务器证书。
域名	域控制器中定义的 LDAP 用户所属角色组的域。 域名的取值原则： • 最大长度为 255 个字符。 • 可由数字、大小写英文字母和连接号（-），点号（.）组成。 • 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 • 任意两个点号之间的字符长度不允许超过 63。
绑定标识名	LDAP 代理用户标识名。 例如： “CN=username,OU=company,O=organization,DC=domain,DC=com”，与 LDAP 服务器下成员标识名保持一致。 取值范围：BMC 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
	取值范围：1~20 个字符，由数字、英文字母和特殊字符组成。
用户应用文件夹	能够登录 BMC 的 LDAP 用户在 LDAP 服务器上所属的目录。 输入节点的格式为：“CN=xxx”、“OU=xxx”或“O=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 BMC 的用户“infotest”在 LDAP 服务器上所属的路径为“\testusers\part1”，则此处需要输入的内容为“OU=part1,OU=testusers”。 说明 节点属性“CN”、“OU”和“O”的区别，请参考 LDAP 协议的详细介绍。例如： - 在 Windows AD 中，节点的“Type”参数为“Container”时，节点属性为“CN”；节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 - 在 OpenLDAP 中，节点的“objectClass”参数为“Organization”时，节点属性为“O”。 取值范围：BMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64~255。
LDAP 证书验证使能	是否对远端域控制器进行证书验证。 从安全性考虑，请尽量开启证书验证。开启证书验证后需要导入 LDAP CA 证书；LDAP 服务器端需要安装 AD、DNS、CA 证书颁发机构，将 CA 证书导入 LDAP 服务器和 BMC 系统。 默认值：关闭
证书校验级别	对 LDAP 证书进行校验的级别。 “Demand”：证书校验过程中，当检查到客户端证书错误或没有证书时，不允许登录 BMC。从安全性考虑，请尽量保持默认值“Demand”。 “Allow”：证书校验过程中，当检查到客户端证书错误或没有证书时，仍允许登录 BMC。 默认值：“Demand”
LDAP 证书	用于上传 LDAP CA 证书，支持.cer、.pem、.cert 和.crt 格式。 说明 - 上传的文件如果超过 1MB 会引起页面请求失败，刷新页面可恢复。 - 证书链的层级不得超过 10 级。
证书信息	显示证书信息。 若为证书链，显示的证书信息依次为“服务器证书 > 中间证书 > 根证书”。
登录密码	配置域控制器需要输入当前登录 BMC 系统的用户密码。

参数	描述
LDAP 用户组	
添加组	打开配置新建 LDAP 组区域框。
组名	LDAP 用户所属角色组的名称。 取值范围：BMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64~255。
角色	LDAP 用户组的权限角色。 - 管理员：该权限组的用户，拥有所有功能模块的操作权限，其支持的功能模块不可更改。 - 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 - 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 - 自定义用户：管理员可为自定义用户指定可操作的功能模块。 说明 新建 LDAP 用户组默认权限为“普通用户”。
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 BMC 系统。 取值范围： - SSH：使能该接口后，用户可使用符合 SSH 协议的终端工具（例如 PuTTY）登录 BMC 命令行。 - Web：使能该接口后，用户可使用浏览器登录 BMC WebUI。 - Redfish：使能该接口后，用户可使用符合 Redfish 协议的终端工具登录 BMC 系统。 说明 新建 LDAP 用户组默认支持所有登录接口。
组应用文件夹	能够登录 BMC 的 LDAP 组在 LDAP 服务器上所属的目录。 输入节点的格式为：“CN=xxx”、“OU=xxx”或“O=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 BMC 的用户“infotest”在 LDAP 服务器上所属的路径为“\testusers\part1”，则此处需要输入的内容为“OU=part1,OU=testusers”。 说明 节点属性“CN”“OU”和“O”的区别，请参考 LDAP 协议的详细介绍。例如： 在 Windows AD 中，节点的“Type”参数为“Container”时，节点属性为

参数	描述
	“CN”；节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 在 OpenLDAP 中，节点的“objectClass”参数为“Organization”时，节点属性为“O”。 取值范围：BMC 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。
编辑	打开配置已有 LDAP 组区域框。
删除	删除已有 LDAP 组。

启用 LDAP 并配置域服务器基本属性

- 步骤 1 单击“LDAP 使能”右侧的 ，将状态设置为 ，表示 LDAP 功能已经启用。
- 步骤 2 根据[表 5-43 LDAP 配置](#)提供的参数信息，设置域服务器。
- 步骤 3 单击“保存”。
- 显示“操作成功”。
- 结束

导入 LDAP 证书

单击“LDAP 证书”后的“添加文件”，选择要导入的 LDAP 证书。

 说明

- 支持导入证书文件的格式为 .cer、.pem、.cert 和 .crt 格式，最大不超过 1MB。
- 请定期更新证书，否则可能存在安全风险。

当界面提示“上传成功”后，可在下方的“证书信息”区域查看已看上传的证书的详细内容，包含内容如[表 5-44 证书信息](#)所示。

表5-44 证书信息

参数	描述
签发者	LDAP 证书的签发者信息，包含的具体参数类型与“使用者”相同。
使用者	LDAP 证书的使用者（即当前服务器）信息，包含： - CN：使用者的名称 - OU：使用者所在部门

参数	描述
	• 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
有效起止日期	LDAP 证书生效起止日期。
序列号	LDAP 证书序列号。用于证书的识别、迁移。
证书吊销列表	LDAP 证书吊销状态: • 已配置: 表示该证书的吊销文件已上传, 在 TLS 连接时, 会进行证书吊销校验。 • 未配置: 表示该证书的吊销文件未上传。 说明 证书吊销文件的格式为“*.crl”, 编码格式为 Base64, 最大不超过 100KB。
吊销列表有效日期	LDAP 证书的吊销列表有效日期。 说明 吊销列表过期会导致相应的认证功能失败。

配置证书吊销列表

说明

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

- 步骤 1 从证书颁发机构获取证书吊销文件。
- 步骤 2 在“服务器证书信息”区域单击“证书吊销列表”后的“上传”。
- 步骤 3 选择证书吊销文件。
- 步骤 4 输入当前登录用户密码并单击“保存”。

---结束

删除证书吊销列表

说明

删除证书吊销列表, 可能会导致使用过期的证书, 请注意安全风险。

- 步骤 1 在“服务器证书信息”区域单击“证书吊销列表”后的“删除”。
- 步骤 2 输入当前登录用户密码并单击“确定”。

---结束

添加 LDAP 组

BMC 系统最大可以设置 5 个 LDAP 组。

步骤 1 在“LDAP 用户组”区域中，单击“添加组”。

弹出添加 LDAP 组的窗口。

步骤 2 根据表 5-45 添加组的说明设置 LDAP 组的基本属性。

表5-45 添加组

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

参数	描述
	• 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 BMC 命令行。 • Web: 使能该接口后, 用户可使用浏览器登录 BMC WebUI。 • Redfish: 使能该接口后, 用户可使用符合 Redfish 协议的终端工具登录 BMC 系统。 说明 新建 LDAP 用户组默认支持所有登录接口。
登录密码	当前登录 BMC 系统的用户密码。

步骤 3 单击“保存”。

在 LDAP 用户组列表显示成功添加的 LDAP 组信息。

----结束

删除 LDAP 组

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

弹出“确认”对话框, 提示输入当前登录用户的密码。

步骤 2 输入当前用户的密码。

步骤 3 单击“确定”。

界面显示“删除成功”。

----结束

修改 LDAP 组

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

步骤 2 根据表 5-45 添加组的说明修改 LDAP 组配置。

步骤 3 单击“保存”。

说明

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

----结束

5.5.3 Kerberos

功能介绍

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

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

界面描述

在导航栏中选择“用户&安全 > Kerberos”，打开如下图所示界面。

图5-40 Kerberos

Kerberos功能

Kerberos使能 

基本属性

领域

Kerberos服务器地址

Kerberos端口

88

* 密钥表

添加文件

仅支持.keytab格式。

* 登录密码

请输入当前登录用户密码

保存

Kerberos用户组

添加组

序号	组名	SID	角色	登录接口	组应用文件夹	登录规则	操作
1	g1	12	自定义用户1	Web	CN=0toki	规则2 规则3	编辑 删除
2	bhy	4	普通用户	Web	OU=pocli	规则2 规则3	编辑 删除

参数说明

表5-46 Kerberos 功能

参数	描述
Kerberos 使能	开启或关闭 Kerberos 功能。 默认为关闭状态。 说明 启用 Kerberos 功能，使用 Kerberos 帐户登录 BMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。
基本属性	
说明	带“*”的项目为必配参数。

参数	描述
领域	Kerberos 领域。 取值范围：最大长度为 255 个字符。 取值原则：由数字、英文字母（推荐使用大写字母）和特殊字符（包括空格）组成。
Kerberos 服务器地址	Kerberos 服务器的地址。 启用 Kerberos 功能后，该处需要配置为 Kerberos 服务器的 FQDN（主机名.域名），且需要在网络配置部分配置 DNS。 输入格式：IPv4 地址、IPv6 地址或域名。 域名的取值原则： - 最大长度为 255 个字符。 - 可由数字、大小写英文字母和连接号（-），点号（.）组成。 - 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 - 任意两个点号之间的字符长度不允许超过 63。
Kerberos 端口	Kerberos 服务的端口号。 取值范围：1~65535 默认值：88
密钥表	用于上传 Kerberos 密钥表，仅支持 “.keytab” 格式。 默认显示为空。 说明 - 密钥表大小不可为 0KB，不能大于 1MB。 - 请定期更新密钥，否则可能存在安全风险。
登录密码	当前登录 BMC 系统的用户密码。
Kerberos 用户组	显示所有 Kerberos 用户组的信息。 BMC 最多支持同时添加 5 个 Kerberos 用户组。
添加组	打开配置新建 Kerberos 组区域框。
组名	Kerberos 用户所属角色组的名称。 取值范围：BMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64~255。
SID	安全标识符（Security Identifiers）。用于 Kerberos 和用户组授权。例如，“S-1-5-21-310440588-250036847-580389505-500”。 取值范围：BMC 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，不能包含空格。
角色	Kerberos 用户组的权限角色。

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，其支持的功能模块不可更改。 - 操作员：该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 - 普通用户：该权限组的用户，拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其支持的功能模块不可更改。 - 自定义用户：管理员可为自定义用户指定可操作的功能模块。 说明 新建 Kerberos 用户组默认权限为“普通用户”。
登录接口	Kerberos 用户组使能的登录接口。 - Web 使能后，Kerberos 用户组的成员可通过 WebUI 登录 BMC 系统。新建 Kerberos 用户组默认支持 WebUI 登录。 - Redfish 使能后，Kerberos 用户组的成员可通过 Redfish 登录 BMC 系统。新建 Kerberos 用户组默认支持 Redfish 登录。 说明 仅 BMC V3.05.10.01 及以上版本支持 Redfish 登录。
组应用文件夹	能够登录 BMC 的 Kerberos 用户组在 Kerberos 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 BMC 的 Kerberos 用户组“grouptest”在 Kerberos 服务器上所属的路径为“\testgroups\part1”，则此处需要输入的内容为“OU=part1,OU=testgroups”。 说明 节点属性“CN”和“OU”的区别，请参考 Kerberos 协议的详细介绍。 例如，在 Windows AD 中： - 节点的“Type”参数为“Container”时，节点属性为“CN”。 - 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：BMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64~255。
登录规则	Kerberos 用户组应用的登录规则，对已选择该登录规则的 Kerberos 用户组进行限制。
编辑	打开配置已有 Kerberos 组区域框。

参数	描述
删除	删除已有 Kerberos 组。

启用 Kerberos 认证并配置域服务器基本属性

- 步骤 1 单击“Kerberos 使能”右侧的 ，将状态设置为 ，表示 Kerberos 功能已经启用。
- 步骤 2 根据表 5-46 Kerberos 功能提供的参数信息，设置域服务器。
- 步骤 3 单击“保存”。

----结束

导入密钥表

说明

密钥表文件的格式为“.keytab”。密钥表大小不可为 0KB，不能大于 1MB。

- 步骤 1 单击“密钥表”后的“添加文件”，选择要导入的密钥表。
- 步骤 2 单击“打开”。
- 上传成功后，“密钥表”显示“上传成功”。
- 步骤 3 输入当前登录用户的密码。

说明

通过 SSO 登录的 Kerberos 用户不需要输入当前登录用户密码。

- 步骤 4 单击“保存”。

----结束

添加 Kerberos 用户组

BMC 系统最大可以添加 5 个 Kerberos 用户组。

- 步骤 1 在“Kerberos 用户组”区域中，单击“添加组”。
- 弹出添加 Kerberos 用户组的窗口。

表5-47 添加组

参数	描述
组名	Kerberos 用户所属角色组的名称。 取值范围：BMC 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

参数	描述
	为 64~255。
组应用文件夹	能够登录 BMC 的 Kerberos 用户组在 Kerberos 服务器上所属的目录。 输入节点的格式为：“CN=xxx”或“OU=xxx”，当存在多层级节点时，下级节点在前，上级节点在后，依次排列，用半角逗号隔开。 例如，可登录 BMC 的 Kerberos 用户组“grouptest”在 Kerberos 服务器上所属的路径为“\testgroups\part1”，则此处需要输入的内容为“OU=part1,OU=testgroups”。 说明 节点属性“CN”和“OU”的区别，请参考 Kerberos 协议的详细介绍。 例如，在 Windows AD 中： - 节点的“Type”参数为“Container”时，节点属性为“CN”。 - 节点的“Type”参数为“Organizational Unit”时，节点属性为“OU”。 取值范围：BMC 为此参数分配了 255 字节的空间。由于不同编码格式下字符所占字节数不同，此处支持的最大字符串长度为 64~255。
组 SID	安全标识符。用于 Kerberos 和用户组授权。 取值范围：BMC 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，不能包含空格。
角色	分配给组域的访问 BMC 界面的权限。 取值范围：“管理员”、“操作员”、“普通用户”和“自定义”。 说明 新建 Kerberos 用户组默认权限为“普通用户”。
登录规则	Kerberos 用户组应用的登录规则，对已选择该登录规则的 Kerberos 用户组进行限制。
登录接口	Kerberos 用户组使能的登录接口。 - Web 使能后，Kerberos 用户组的成员可通过 WebUI 登录 BMC 系统。新建 Kerberos 用户组默认支持 WebUI 登录。 - Redfish 使能后，Kerberos 用户组的成员可通过 Redfish 登录 BMC 系统。新建 Kerberos 用户组默认支持 Redfish 登录。 说明 仅 BMC V3.05.10.01 及以上版本支持 Redfish 登录。
登录密码	当前登录 BMC 系统的用户密码。

参数	描述
	说明 通过 SSO 登录的 Kerberos 用户不需要输入当前登录用户密码。

步骤 2 根据表 5-47 添加组的说明设置 Kerberos 用户组的基本属性。

步骤 3 单击“保存”。

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

----结束

删除 Kerberos 用户组

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

弹出“确认”对话框，提示输入当前登录用户的密码。

说明

通过 SSO 登录的 Kerberos 用户不需要输入当前登录用户密码。

步骤 2 输入当前用户的登录密码。

步骤 3 单击“确定”。

----结束

修改 Kerberos 用户组

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

弹出“修改组”窗口。

步骤 2 根据表 5-47 添加组的说明修改 Kerberos 用户组配置。

步骤 3 单击“保存”。

----结束

5.5.4 双因素认证

功能介绍

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

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

界面描述

在导航栏中选择“用户&安全 > 双因素认证”，打开如下图所示界面。

图5-41 双因素认证



参数说明

表5-48 双因素认证

参数	描述
双因素认证	开启或关闭双因素认证功能。开启该功能后，在客户端登录 BMC WebUI 时，将使用证书认证登录，而不是需要输入用户名和密码的登录界面登录。 默认为关闭状态。 说明 - 启用双因素认证功能前，必须导入有效的根证书和客户端证书。且必须存在至少一套可用证书，否则，在后续登录时会出现无法认证的情况。 - 启用双因素认证功能后，系统会自动关闭 SSH 服务，且无法手动开启。 - 启用再禁用双因素认证功能后，SSH 服务不会自动开启，若需要使用 SSH 服务，请手动开启。 - 如果安全配置项中仅开启 TLS 1.3 协议，则无法开启双因素认证。
联机证书状态检查（OCSP）	须知 - 联机证书状态检查采用 OCSP（Online Certificate Status Protocol）进行验证，启用前请确认与 OCSP 服务器通信良好，否则可能导致 Web 服务不可用。 - 请确保根证书中已写入 OCSP 地址信息，否则开启此功能后，双因素认证可能失败。 认证过程中，是否检查证书的合法性。开启该功能后，在登录 BMC WebUI 过程中，会检查当前客户端证书的合法性，若其为已过期或已撤销的证书，则无法通过认证，即无法登录

参数	描述
	BMC WebUI。 默认为关闭状态。
证书吊销列表检查 (CRL)	认证过程中，检查证书是否已被吊销。开启该功能后，在登录 BMC WebUI 过程中，会检查当前客户端证书是否已被吊销，若其为已被吊销的证书，则无法通过认证，即无法登录 BMC WebUI。 默认为关闭状态。 说明 请确保已导入证书吊销列表，否则开启此功能后，双因素认证可能失败。
根证书	BMC 上已存在的根证书列表，并显示每个根证书的颁发者、使用者、截止日期、证书吊销列表以及吊销列表有效日期。 BMC 最多支持 16 个根证书。 说明 - 支持上传 Base64 编码的根证书，证书格式包括：*.cer、*.crt、*.pem，最大不超过 1MB。 - 证书吊销列表表示证书吊销的状态： - 已配置：表示该证书的吊销文件已上传，在 TLS 连接时，会进行证书吊销校验。 - 未配置：表示该证书的吊销文件未上传。 - 吊销列表过期会导致相应的认证功能失败。
客户端证书	BMC 上已存在的客户端证书列表，并显示每个客户端证书绑定的用户名、角色、根证书上传状态、吊销状态和吊销时间以及客户端证书指纹（即客户端证书文件的哈希值）。 BMC 最多支持 16 个用户对应的客户端证书。 说明 - 支持上传 Base64 编码的客户端证书（公钥证书），证书格式包括：*.cer、*.crt、*.pem，最大不超过 1MB。 - 客户端证书有以下几种吊销状态： - 已吊销 - 未吊销

启用双因素认证并上传证书到 BMC

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

说明

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

- 支持上传 Base64 编码的根证书和客户端证书（公钥证书），证书格式包括：
.cer、.crt、*.pem，最大不超过 1MB。

步骤 1 单击“证书上传”。

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

步骤 2 单击“打开”。

界面提示“操作成功”。

步骤 3 将“双因素认证使能”右侧的状态设置为 。

---结束

为指定证书配置证书吊销列表

说明

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

步骤 1 从证书颁发机构获取证书吊销文件。

步骤 2 单击指定证书对应的“证书吊销列表”的“上传”。

步骤 3 选择证书吊销文件。

---结束

使用证书认证方式登录 BMC

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 BMC WebUI 的证书登录。

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

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

步骤 3 单击“管理证书”。

步骤 4 在证书管理窗口中，导入客户端私钥证书。

说明

导入过程中需要输入的密码，为申请证书时设置的密码。

步骤 5 重新在 Chrome 的地址栏中输入 BMC 地址登录。

步骤 6 按照提示信息选择当前客户端证书。

可成功登录 BMC WebUI。

---结束

删除根证书

说明

只有双因素认证功能处于停用状态，才能成功删除根证书。

步骤 1 在“根证书”页签中，单击指定根证书后的“删除”。

弹出操作确认对话框。

步骤 2 单击“确认”。

----结束

删除客户端证书

步骤 1 在“客户端证书”页签中，单击指定根证书后的“删除”。

弹出操作确认对话框。

步骤 2 单击“确认”。

----结束

删除证书吊销列表

说明

删除证书吊销列表，可能会导致使用过期的证书，请注意安全风险。

步骤 1 单击指定证书对应的“证书吊销列表”的“删除 CRL”。

弹出操作确认对话框。

步骤 2 单击“确认”。

----结束

5.5.5 在线用户

功能介绍

通过使用“在线用户”界面的功能，您可以执行以下操作：

- 查看已登录 BMC 系统的用户信息。
- 注销已登录的用户。

只有隶属于管理员组的用户可以注销其他已登录的用户。

界面描述

在导航栏中选择“用户&安全 > 在线用户”，打开如下图所示界面。

图5-42 在线用户

在线用户					
用户信息					
序号	用户名	登录方式	登录IP	登录时间	操作
1	Administrator	GUI	192.168.1.100	2020-12-16 20:13:45	注销
2	Administrator	GUI	192.168.1.100	2020-12-16 19:57:20	注销
3	Administrator	GUI	192.168.1.100	2020-12-16 19:50:10	
4	Administrator	GUI	192.168.1.100	2020-12-16 15:14:50	注销

参数说明

表5-49 在线用户

参数	描述
序号	在线用户的序号。
用户名	登录 BMC 系统或使用 KVM 远程虚拟控制台的用户名称。
登录方式	用户登录的方式。 取值范围： “GUI(SSO)”表示用户通过单点登录方式登录 BMC WebUI。 “GUI”表示用户通过非单点登录方式登录 BMC WebUI。 “CLI”表示用户通过命令行视图登录 BMC 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 BMC 系统。 “VNC”表示用户通过 VNC 客户端登录服务器操作系统。
登录 IP	连接并登录 BMC 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 BMC 系统。
登录时间	用户登录 BMC 系统的时间。
操作	强制其他用户退出登录。单击某行用户信息的“注销”可以注销该用户。

5.5.6 安全配置

功能介绍

通过使用“安全配置”界面的功能，您可以：

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

界面描述

在导航栏中选择“用户&安全 > 安全配置”，打开如下图所示界面。

图5-43 安全增强

系统锁定模式	☐
业务侧用户管理使能	☒
密码检查	☒
SSH密码认证	☒
防DNS重绑定	☐
TLS版本	TLS 1.2及更高版本 ▼
密码有效期(天)	0
密码最小长度配置	8
密码最短使用期(天)	0
不活动期限(天)	0
紧急登录用户	10001 ▼
禁用历史密码	5 ▼
	失败次数 锁定时长(分钟)
登录失败锁定	5 ▼ 1
证书过期提前告警时间(天)	80
保存	

图5-44 登录规则

名称	时间段 ①	IP段 ②	MAC段 ③	状态	操作
规则1				已禁用	编辑
规则2				已禁用	编辑
规则3				已禁用	编辑

图5-45 权限管理

角色名称	用户配置	常规设置	远程控制	远程媒体	安全配置	电源控制	调试诊断	查询功能	配置自身	操作
管理员	✓	✓	✓	✓	✓	✓	✓	✓	✓	
操作员		✓	✓	✓		✓		✓	✓	
普通用户								✓	✓	
自定义用户1								✓	✓	编辑
自定义用户2							✓	✓	✓	编辑
自定义用户3							✓	✓	✓	编辑
自定义用户4								✓	✓	编辑

图5-46 安全公告

安全公告使能

安全公告消息

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.

442 /1024

保存

恢复默认值

参数说明

表5-50 安全增强

参数	描述
系统锁定模式	开启或关闭 BMC 系统的锁定模式。 默认为关闭状态。 若开启此功能，可以确保系统在根据实际需要配置后，以下等更改系统配置的尝试都将被阻止： - 配置导入 - BMA 管理 - BIOS 启动项设置 - 固件升级-重启、镜像倒换、更新 - 常规设置-存储管理、网络配置、产品信息、SP 管理、监控门限、语言、时区及 NTP - 电源控制-电源设置、功率重新统计及清空、风扇智能调速 - 用户基础配置-许可证管理、SNMP 相关配置 - web 服务、VNC 功能基础配置 - 虚拟控制台、虚拟媒体基础设置 - 安全基础配置（不包括系统锁定模式本身） - 调试诊断-系统日志、录像截屏、告警上报基础设置 说明 仅当许可证级别为高级版时，才能显示此功能。只有拥有管理员权限的用户有权限设置。
业务侧用户管理使能	开启或关闭业务侧对用户的管理功能。 关闭业务侧用户管理功能时，业务侧发送过来的用户管理相关的 IPMI 命令无效，例如用户添加/删除、权限设置、密码设置等 IPMI 命令。 默认为开启状态。 - 开启：表示业务侧可以对用户进行管理。 - 关闭：表示业务侧不能对用户进行管理。 建议关闭业务侧用户管理功能，否则业务侧可以对 BMC 用户进行管理，产生安全隐患。
密码检查	针对每个用户的密码进行复杂度检查。 系统默认启用密码检查功能。该选项同时适用于： - 本地用户密码、Trap 团体名、SNMPv1/v2c 团体名、SNMPv3 加密密码、VNC 密码的复杂度检查。 - 本地用户密码和 SNMPv3 加密密码的最小长度检查。 说明 - 禁用密码检查功能会降低系统安全性，请尽量启用此功能。

参数	描述
	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 <code>ipmcset -t user -d weakpwddic -v export</code> 获取。)
SSH 密码认证	开启或关闭 SSH 密码认证功能。 - 关闭：表示通过 SSH 登录 BMC 时，只能使用公钥认证。 - 开启：表示通过 SSH 登录 BMC 时，可使用密码认证，也可以使用公钥认证。 默认为开启状态。
防 DNS 重绑定	开启或关闭防 DNS 重绑定功能。 开启防 DNS 重绑定功能后，只能通过 BMC 上配置的主机名、FQDN 或 IP 地址访问 BMC。 默认为关闭状态。
TLS 版本	在两个通信应用程序通信时，TLS (Transport Layer Security) 协议保证其保密性和数据完整性。 浏览器与 Web 服务器通讯时，需要建立安全链接。 - TLS 1.2 及更高版本：表示支持使用 TLS 1.2 协议或 TLS 1.3 协议。 - 仅限 TLS 1.3：表示仅支持使用 TLS 1.3 协议。 默认为“TLS 1.2 及更高版本”。 说明 - 如果安全配置项中仅开启 TLS 1.3 协议，则无法开启双因素认证。 - 仅开启 TLS 1.3 时，访问 Java 集成控制台需要的 JRE 版本为 AdoptOpenJDK 11 JRE。 - 该选项仅对 BMC 的 Web 和 Redfish 服务生效。
密码有效期 (天)	用户密码的使用期限。 取值范围为 0~365，单位为天，取值为 0 时表示密码为无限期。 默认值：0 说明 为保障系统安全性，建议设置合适的密码有效期，并定期更新密码。
密码最小长度配置	本地用户密码和 SNMPv3 加密密码的最小长度限制。 该参数仅在开启密码检查时生效。 取值范围为 8~20。 默认值：8
密码最短使用期 (天)	设置一个密码后，要使用的最短时间。在此时间内不能修改密码。 取值范围为 0~365，单位为天，取值为 0 时表示密码最短使用期无限期。

参数	描述
	默认值：0 说明 密码最短使用期必须比密码有效期小 10 天以上。 - 如果密码有效期设置为≤ 10 天，密码最短使用期则只能设置为 0。 - 如果密码最短使用期设置为≥ 355 天，则密码有效期只能设置为 0。
不活动期限（天）	超过设定期限内未活动的用户会被禁用。 取值范围 0 或者 30~365，单位为天，取值为 0 时表示不限制，用户不会因为长时间不活动而被禁止。 默认值：0
紧急登录用户	不受密码有效期、登录规则和登录接口限制的用户，用于紧急情况下登录 BMC。 默认为“NULL”。 说明 - 只有管理员用户可以被设置为“紧急登录用户”。 - 只有管理员用户才能看到“紧急登录用户”。
禁用历史密码	用户修改密码时，禁止使用设置次数内的历史密码。 取值范围为 0~5，取值为 0 时，表示不限制使用历史密码。 默认值：5
登录失败锁定	可设置用户触发登录失败锁定的登录失败次数以及锁定的时长。 - 登录失败次数取值范围为 1~6 以及不限制（即关闭登录失败锁定功能），默认值为 5。 - 登录失败锁定时长取值范围为 1~30，单位为分钟，默认值为 5。 用户被锁定后，在锁定时长内不能继续登录。 说明 - 关闭登录失败锁定功能会降低系统安全性，请尽量启用此功能。 - 紧急情况下需要解锁时，可在命令行下执行 unlock 命令。详情请参见各服务器的 BMC 用户指南。
证书过期提前告警时间(天)	BMC 证书过期提前上报告警的时间，单位为天。例如证书过期提前告警时间设置为 7，表示当 BMC 中有证书距离过期时间还有小于或等于 7 天时，上报告警。 取值范围为 7~180。 默认值：90

表5-51 登录规则

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

表5-52 权限管理

参数	描述
管理员	该权限组的用户，拥有所有功能模块的操作权限，其权限不可更改。
操作员	该权限组的用户，拥有“常规设置”、“远程控制”、“远程媒体”、“电源控制”、“查询功能”和“配置自身”模块的操作权限，其权限不可更改。
普通用户	该权限组的用户，拥有与自身相关的“查询功能”和“配置自

参数	描述
	身”模块的操作权限，其权限不可更改。
自定义用户 1~自定义用户 4	管理员可为自定义权限组指定可操作的功能模块。 默认拥有与自身相关的“查询功能”和“配置自身”模块的操作权限，其中“查询功能”权限不可更改。自定义用户无“用户配置”模块的权限。
用户配置	用户和密码相关的配置。 可配置的项目包括： • 本地用户、在线用户、LDAP 用户、Kerberos 用户 • 双因素认证、SSH 密码认证 • 许可证管理 • 权限管理 • SNMP v1/v2c/v3 相关配置 • 业务侧用户管理使能 • KVM/VMM 界面的在线用户跳转 • 恢复出厂设置
常规设置	服务器带外管理基本配置。 可操作的项目包括： • 产品信息配置 • 性能监控配置 • 存储管理、网络配置、固件升级、语言管理 • NTP、时区配置 • 智能调速 • 告警、事件 • Web 服务超时时长、会话模式配置 • 告警上报（SMTP/Trap 配置） • SP 管理
远程控制	• 通过 HTML5 集成远程控制台、Java 集成远程控制台、独立远程控制台和 VNC 客户端访问服务器实时桌面 • 设置 KVM 超时时长、通信加密、本地 KVM、虚拟键鼠持续连接、最大会话、活跃会话 • 设置 VNC 超时时长、键盘布局、VNC 密码、登录规则、SSL 加密 • 配置串口重定向 • BMA 管理
远程媒体	• 设置 VMM 通信加密、注销会话 • 虚拟媒体的挂载和使用

参数	描述
	• BMA 管理
安全配置	安全性的查询和配置。 安全配置包括： • 操作日志 • 安全日志 • 安全增强 • 登录规则 • 登录安全信息配置 • 端口服务 • Web 服务（设置 HTTP 及端口、HTTPS 及端口、服务器证书信息） • KVM（可以设置 KVM 使能、端口） • VMM（可以设置 VMM 使能、端口） • VNC（可以设置 VNC 使能、端口） • SNMP（设置 SNMP 使能、端口） • 告警上报（syslog 配置） • 一键收集
电源控制	• 电源设置 • 功率设置 • 服务器上下电设置
调试诊断	现场定位、调试操作。 调试诊断包括： • FDM 故障预测诊断 • 系统日志 • 进入维护调测接口 • 传感器模拟 • 自动录像配置 • 手动/自动截屏 • 串口重定向记录 • 黑匣子
查询功能	可以登录以及查看除安全配置、调试诊断、双因素认证、在线用户和常规设置以外的信息。
配置自身	可以配置帐户自身的密码以及管理 SSH 公钥、SNMPv3 加密密码、SNMPv3 加密算法和鉴权算法。 预置角色默认拥有此权限，自定义角色的配置自身权限可设置。

参数	描述
操作	单击“编辑”，权限管理的“常规设置”、“远程控制”、“远程媒体”、“安全配置”、“电源配置”、“调试诊断”和“配置自身”处于可编辑状态。

表5-53 安全公告

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

启用安全增强功能

步骤 1 根据表 5-50 安全增强提供的参数信息，设置服务器密码检查、SSH 密码认证功能、密码有效期、不活动期限、紧急登录用户、禁用历史密码、登录失败锁定等安全增强功能。

步骤 2 单击“保存”。

界面提示“保存成功”。

---结束

设置登录规则

BMC 同时支持三组登录规则，满足任意一条启用的登录规则即可登录。

登录规则对服务器的本地用户、LDAP 组、SNMPv3 服务、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：

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

说明

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

步骤 1 在“登录规则”页签中，单击待启用的规则右侧的“编辑”。

步骤 2 单击 ，将规则状态设置为 。

步骤 3 根据表 5-51 [登录规则](#)提供的参数信息，设置服务器登录规则。

步骤 4 单击“保存”。

----结束

设置自定义用户权限

BMC 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。

步骤 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 5-52 [权限管理](#)所示。

步骤 2 单击“保存”。

弹出确认对话框，输入当前用户密码，单击“确定”。

----结束

设置安全公告消息

步骤 1 在“安全公告”页签中，单击 ，将状态设置为 。

步骤 2 在安全公告消息文本框中输入待设置的信息。

步骤 3 单击“保存”。

----结束

恢复默认安全公告消息

步骤 1 在“安全公告”页签中，单击 ，将状态设置为 。

步骤 2 单击“恢复默认值”。

步骤 3 单击“保存”。

----结束

5.5.7 证书更新

5.5.7.1 SSL 证书更新

功能介绍

通过使用“SSL 证书更新”界面的功能，您可以：

- 设置 SSL 证书更新。

- 配置 CA 服务器。
- 自定义证书主题。

界面描述

在导航栏中选择“用户&安全 > 证书更新”，单击“SSL 证书更新”，打开如下图所示界面。

图5-47 SSL 证书更新

SSL证书更新

自动更新使能

证书更新

CA服务器配置

* 服务器地址

* 端口

25803

* 路径

/cmp/BMC

证书主题

* 国家(C)

VN

省份(S)

城市(L)

公司(O)

部门(OU)

* 常用名(CN)

ZZZ

内部名(IN)

邮件地址(E)

服务器根证书

上传

客户端证书

上传

证书信息

签发者

颁发给

使用者

有效起止日期

序列号

证书吊销列表

吊销列表有效日期

证书信息

签发者

颁发给

使用者

有效起止日期

序列号

保存

参数说明

表5-54 SSL 证书更新

参数	描述
SSL 证书更新	
说明	● 当系统锁定模式关闭、用户具有安全配置权限和 CA 服务器完成配置时，支持 SSL 证书更新。 ● SSL 证书更新功能需要同时导入服务器根证书和客户端证书，否则会导致认证失败。

2023-07-27

139

参数	描述
自动更新使能	开启或关闭证书自动更新功能。 开启“自动更新使能”后，SSL 证书支持自动刷新，自动刷新时间间隔为 1 小时。 默认为关闭状态。
证书更新	单击“证书更新”，更新 SSL 证书。
CA 服务器配置	
服务器地址	CA 服务器的地址。 取值原则：IPv4 地址、IPv6 地址或域名，且最大长度为 67 个字符。
端口	CA 服务器的端口号。 取值范围：1~65535。
路径	CA 服务器的路径。 取值原则：长度为 1~128 个字符，以斜线 (/) 开头，由数字 (0-9)，字母 (a-z, A-Z)，下划线 (_)，斜线 (/) 组成。
证书主题	
国家 (C)	证书所属的国家。 取值原则：包含所有英文字母，且长度必须为两字符。
省份 (S)	证书所属的省份。 取值原则：长度为 0~128 个字符，可由数字 (0-9)、字母 (a-z, A-Z)、中划线 (-)、下划线 (_)、点 (.)、空格符号组成。
城市 (L)	证书所属的城市。 取值原则：长度为 0~128 个字符，可由数字 (0-9)、字母 (a-z, A-Z)、中划线 (-)、下划线 (_)、点 (.)、空格符号组成。
公司 (O)	证书所属的公司。 取值原则：长度为 0~64 个字符，可由数字 (0-9)、字母 (a-z, A-Z)、中划线 (-)、下划线 (_)、点 (.)、空格符号组成。
部门 (OU)	证书所属的部门。 取值原则：长度为 0~64 个字符，可由数字 (0-9)、字母 (a-z, A-Z)、中划线 (-)、下划线 (_)、点 (.)、空格符号组成。
常用名 (CN)	证书所属的常用名。 取值原则：长度为 1~64 个字符，可由数字 (0-9)、字母 (a-z, A-Z)、中划线 (-)、下划线 (_)、点 (.)、空格符号组

参数	描述
	成。
内部名 (IN)	证书的内部名。 取值原则：长度为 0~64 个字符，可由数字 (0-9)、字母 (a-z, A-Z)、中划线 (-)、下划线 (_)、点 (.)、空格符号组成。
邮件地址 (E)	证书的邮件地址。 取值原则：长度为 0~255 个字符，符合邮箱地址规则。
服务器根证书	通过正式的 CA 证书颁发机构申请的服务器根证书。在建立数据连接时，使用此处上传的服务器根证书对 CA 服务器发送来的服务器证书报文进行“TLS”验证。 说明 - 支持上传服务器根证书文件的格式为“.crt”、“.cer”和“.pem”，*.cer 格式的证书的编码为 Base64，最大不超过 100KB，且不支持上传相同的证书。 - 请定期更新证书，否则可能存在安全风险。
客户端证书	通过正式的 CA 证书颁发机构申请的客户端证书。 说明 - 支持上传客户端证书格式为*.p12 和*.pfx，最大不超过 100KB。 - 请定期更新证书，否则可能存在安全风险。
证书信息	显示上传的证书信息，包括： - 签发者 - 使用者 - 有效起止日期 - 序列号 - 证书吊销列表，状态为： - 已配置：表示该证书的吊销文件已上传，在 TLS 连接时，会进行证书吊销校验。 - 未配置：表示该证书的吊销文件未上传。 说明 - 证书吊销文件的格式为“*.crl”，文件名不能为空，最大不超过 100KB。 - 吊销列表过期会导致相应的认证功能失败。 - 客户端证书不支持证书吊销列表。

上传证书

步骤 1 单击“服务器根证书”或“客户端证书”后的“上传”。

弹出本地文件选择器或者出现客户端证书上传弹窗。

说明

- 服务器根证书支持*.cer、*.crt、*.pem 格式，*.cer 格式的证书的编码为 Base64，最大不超过 100KB，且不支持上传相同的证书。
- 客户端证书支持*.p12 和*.pfx 格式，最大不超过 100KB。

步骤 2 选择正确格式文件。

步骤 3 单击“确定”。

----结束

配置证书吊销列表

说明

证书吊销文件的格式为“*.crl”，文件名不能为空，最大不超过 100KB。

步骤 1 从证书颁发机构获取证书吊销文件。

步骤 2 在“服务器证书信息”区域单击“证书吊销列表”后的“上传”。

步骤 3 选择证书吊销文件。

步骤 4 输入当前登录用户密码并单击“保存”。

----结束

删除证书吊销列表

说明

删除证书吊销列表，可能会导致使用过期的证书，请注意安全风险。

步骤 1 单击指定证书对应的“证书吊销列表”的“删除 CRL”。

弹出操作确认对话框。

步骤 2 单击“确认”。

----结束

5.6 服务管理

5.6.1 端口服务

功能介绍

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

说明

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

界面描述

在导航栏中选择“服务管理 > 端口服务”，打开如下图所示界面。

图5-48 端口服务

端口信息

编辑

服务	端口	备用端口	状态
SSH	22		已开启
SNMP Agent	161		已开启
KVM	219		已开启
VMM	8209		已开启
Video	2199		已开启
VNC	5900		已开启
WEB_HTTP	80		已开启
WEB_HTTPS	443		已开启
IPMI LAN (RMCP)	623	664	已开启
IPMI LAN (RMCP+) ⓘ			已开启

参数说明

表5-55 端口服务

服务	默认端口号	说明
SSH	22	安全外壳（SSH，Secure Shell）是允许在本地计算机和远程计算机之间建立安全渠道的一套标准和网络协议。 BMC 最多允许 10 个 SSH 用户同时登录。 默认为开启状态。 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 BMC 时，请使用正确的加密算法。
SNMP Agent	161	SNMP 代理服务是用于翻译和传递管理设备和被管设备之间的请求。 默认为开启状态。
KVM	2198	从远端控制服务器时需要用到的 KVM（keyboard，video，and mouse）服务，开启后可用本地鼠标、键盘对服务器进

服务	默认端口号	说明
		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。 默认为开启状态。
VMM	8208	从远端控制服务器时需要用到的 VMM（Virtual Media Manager）服务，开启后可使用虚拟光驱、虚拟软驱等功能。 同一时间只允许 1 个用户使用。 默认为开启状态。
Video	2199	从远端控制服务器时需要用到的 Video 服务，开启后可使用 5.4.3 录像截屏 功能。 同一时间只允许 1 个用户使用。 默认为开启状态。
VNC	5900	从远端控制服务器时需要用到的 VNC（Virtual Network Console）服务，开启后可用本地鼠标、键盘对服务器进行操作，可用本地显示器查看服务器。 最多允许 5 个用户同时使用。 默认为关闭状态。
WEB_HTTP	80	提供网上信息浏览服务的服务器，可以解析超文本传输协议（HTTP，Hypertext Transfer Protocol）。系统默认启用该服务是为了支持输入 IP 默认跳转的功能，建立连接后将默认跳转到 HTTPS 这个安全协议。 默认为开启状态。
WEB_HTTPS	443	提供网上信息浏览服务的服务器，可以解析安全超文本传输协议（HTTPS，Hypertext Transfer Protocol over Secure Socket Layer）及 Redfish 协议。 最多允许 4 个用户同时使用该服务登录 BMC。 默认为开启状态。
IPMI LAN (RMCP)	默认主用端口 Port1 为 623，备用端口 Port2 为 664。	基于局域网（LAN，Local Area Network）方式的 IPMI，支持远程管理控制协议（RMCP，Remote Management Control Protocol）。该服务由于自身机制而存在安全隐患，请尽量避免使用。建议使用 IPMI LAN(RMCP+)服务代替 IPMI LAN(RMCP)服务。 默认为关闭状态。 说明 RMCP 和 RMCP+支持 SHA1 加密算法，存在安全风险，建议关闭该算法，关闭方法请参见《 iBMCBMC Redfish 接口说明 》。
IPMI LAN (RMCP+)	端口与 RMCP 服	基于局域网（LAN，Local Area Network）方式的 IPMI，支持远程管理控制协议。

服务	默认端口号	说明
	务共用。	默认为开启状态。 说明 RMCP+由于协议自身的漏洞（CVE-2013-4786），存在安全隐患，建议参考 风险规避措施 进行处理。

修改服务和端口属性

步骤 1 单击“编辑”。

步骤 2 设置指定服务的使能状态。

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

步骤 3 设置服务的端口。

步骤 4 单击“保存”。

----结束

风险规避措施

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

- 如果不需要使用 IPMI 协议访问 BMC：
 - 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 BMC，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 BMC：
 - 将 BMC 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。

5.6.2 Web 服务

功能介绍

在“Web 服务”页面，您可以：

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

SSL 证书通过在客户端浏览器和 Web 服务器之间建立一条 SSL 安全通道（访问方式为 HTTPS），实现数据信息在客户端和服务端之间的加密传输，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。

 说明

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

界面描述

在导航栏中选择“服务管理 > Web 服务”，打开如图 5-49 所示界面。

图5-49 Web 服务

基本配置

HTTP

端口

80

恢复默认值

HTTPS

端口

443

恢复默认值

超时时长(分钟)

50

会话模式

共享独占

保存

SSL证书

自定义

 证书信息

签发者	CN= IT Product CA, OU= , O= , L= , S= , C=CN
使用者	CN= OU=IT, O= , L=ShenZhen, S=GuangDong, C=CN
有效起止日期	Nov 07 2018 UTC 到 Nov 04 2028 UTC
序列号	5b dc 00 0b ba 50 e7 a7

参数说明

表5-56 Web 服务

区域	参数	说明
基本配置	HTTP	提供网上信息浏览服务的服务器，可以解析超文本传输协议（HTTP，Hypertext Transfer Protocol）。系统默认启用该服务是为了支持输入 IP 默认跳转的功能，建立连接后将默认跳转到 HTTPS 这个安全协议。 默认端口为“80”。 说明 停用 HTTP 服务后，在浏览器中输入“<i>http:BMC 管理网口地址</i>”后，将无法自动跳转至 HTTPS 服务，影响正常使用。
	HTTPS	提供网上信息浏览服务的服务器，可以解析安全超文本传输协议（HTTPS，Hypertext Transfer Protocol over Secure Socket Layer）及 Redfish 协议。 默认端口为“443”。 说明 停用 HTTPS 服务后，将无法登录 BMC WebUI。
	端口	系统服务占用的端口号。 取值范围：1～65535
	超时时长（分钟）	任意连续两次操作 BMC 界面的最大时间间隔。若连续两次操作的时间间隔超过了最大值，Web 页面将自动返回到登录界面。 取值范围：5～480 之间的数字。 默认值：5
	会话模式	使用同一帐号登录 BMC 界面时采用的模式。 - 共享：用户可同时在多个（≤4）客户端使用同一帐号登录 BMC WebUI。 - 独占：一个帐户在同一时间只允许一个客户端使用其登录 BMC WebUI。建立连接后，若用户在其他客户端使用该帐号进行登录，系统会自动终止之前的连接，重新与新的客户端建立连接。 默认为“独占”。
SSL 证书	签发者	SSL 证书的签发者信息，包括： - CN：签发者的名称 - OU：签发者所在部门 - O：签发者所在的公司 - L：签发者所在的城市 - S：签发者所在的省份

区域	参数	说明
		C: 签发者所在的国家
	使用者	SSL 证书的使用者（即当前 BMC）信息，包含的具体参数类型与“签发者”相同。 说明 使用者名称 CN 需要配置为服务器 BMC 的 FQDN（主机名.域名）。
	有效起止日期	SSL 证书生效起始日期和结束日期。
	序列号	SSL 证书序列号。用于证书的识别、迁移。

自定义服务器证书信息并导入

 说明

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

步骤 1 在“SSL 证书”区域单击“自定义”。

显示“自定义”窗口，如下图所示。

图5-50 自定义

☒ 生成CSR文件 ☐ 导入SSL证书

* 国家(C)

省份(S)

城市(L)

公司(O)

部门(OU)

* 常用名(CN)

步骤 2 选择“生成 CSR 文件”，输入自定义的证书请求信息，并单击“生成”。

步骤 3 将生成的 CSR 文件发往 SSL 证书颁发机构，并申请 SSL 证书。

获取到正式的 SSL 证书后，保存到客户端。

步骤 4 在“自定义”窗口选择“导入 SSL 证书”。

步骤 5 选中待上传的 SSL 证书。

说明

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

步骤 6 单击“打开”。

步骤 7 在“证书密码”编辑框输入证书密码。

步骤 8 单击“保存”。

证书导入成功后，立即生效。

说明

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

步骤 9 重新登录 BMC WebUI。

---结束

导入现有 SSL 证书

说明

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

步骤 1 在“SSL 证书”区域单击“自定义”。

显示“自定义”窗口。

步骤 2 选择“导入 SSL 证书”。

步骤 3 选择现有的 SSL 证书文件。

说明

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

步骤 4 单击“打开”。

步骤 5 在“证书密码”编辑框输入证书密码。

步骤 6 单击“确定”。

证书导入成功后，立即生效。

说明

上传的文件如果超过 1MB 会引起页面请求失败，刷新页面可恢复。

步骤 7 重新登录 BMC WebUI。

---结束

5.6.3 虚拟控制台

功能介绍

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

在“虚拟控制台”页面，您可以查看和设置 KVM 功能的开启情况及相关配置项目。

界面描述

在导航栏中选择“服务管理 > 虚拟控制台”，打开如下图所示界面。

图5-51 虚拟控制台

基本配置

KVM使能

端口

2198

恢复默认值

超时时长(分钟)

60

本地KVM

虚拟键鼠持续连接

系统自动锁定

系统自动锁定方式

自定义

Windows

自定义快捷键

+

+

+

清空

最大会话

2

活跃会话

0

保存

参数说明

表5-57 虚拟控制台

参数	说明
KVM 使能	KVM 服务的使能状态。 默认为开启状态。
端口	KVM 服务使用的端口号，默认为 2198。 取值范围：1~65535

参数	说明
超时时长 (分钟)	任意连续两次操作 KVM 界面的最大时间间隔（包括虚拟光驱读取数据的时间间隔，单位为分钟）。若连续两次操作的时间间隔超过了最大值，系统将自动断开与 KVM 界面的连接。 取值范围：0~480 之间的数字。 取值为“0”时，表示永不过时。 默认取值：60 此参数不允许设置为空。
本地 KVM	设置本地 KVM 的使能状态，默认开启。 - 开启时，可同时使用本地 KVM 和远程虚拟控制台连接到服务器实时桌面。 - 关闭时，本地 KVM 不可用，仅可通过远程虚拟控制台连接到服务器实时桌面。
虚拟键鼠持续连接	设置鼠标、键盘是否持续连接，默认开启。 - 开启时，BMC 的虚拟鼠标、键盘将一直连接到业务侧的 USB 控制器。 - 关闭时，只有当使用远程连接功能时，虚拟鼠标、键盘才动态连接到 USB 控制器，否则将断开此连接。当服务器操作系统空闲并且没有虚拟鼠标、键盘连接的时候，会有一定的节能效果。
系统自动锁定	设置系统自动锁定使能状态，默认关闭。 - 开启时，支持最后一个远程登录用户离开时，业务侧 OS 自动锁定。 - 关闭时，不支持业务侧 OS 自动锁定。 说明 该配置项仅在 OS 启动后生效。如果在 BIOS 界面，退出远程虚拟控制台前需手动退出 BIOS。
系统自动锁定方式	在系统自动锁定使能状态为开启时，设置系统自动锁定方式。 - 自定义 - Windows 默认为“自定义”。
自定义快捷键	系统自动锁定自定义快捷键，在系统自动锁定方式为自定义时可设置。 支持的字符串可以是：0~9、a~z、部分特殊字符以及功能键。 说明 支持以下特殊字符： `-/*+.[\];\`,
最大会话	允许使用 KVM 的最大用户数量，固定为 2。
活跃会话	当前使用 KVM 的用户数量。

5.6.4 虚拟媒体

功能介绍

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

在“虚拟媒体”页面，您可以查看和设置 VMM 功能的开启情况及相关配置项目。

界面描述

在导航栏中选择“服务管理 > 虚拟媒体”，打开如下图所示界面。

图5-52 虚拟媒体

基本配置

VMM使能

端口

8208

恢复默认值

最大会话

1

活跃会话

0

保存

参数说明

表5-58 虚拟媒体

参数	说明
VMM 使能	VMM 服务的使能状态。 默认为开启状态。
端口	VMM 服务使用的端口号，默认为 8208。 取值范围：1～65535 说明 浏览器出于安全问题，会禁止一些网络浏览以外的端口，设置这些端口将导致

参数	说明
	HTML5 集成远程控制台的虚拟媒体功能不能使用。
最大会话	允许使用 VMM 连接系统的最大用户数量，固定为 1。
活跃会话	当前使用 VMM 连接系统的用户数量。

5.6.5 VNC

功能介绍

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

在“VNC”页面，您可以查看和设置 VNC 功能的开启情况及相关配置项目。

界面描述

在导航栏中选择“服务管理 > VNC”，打开如下图所示界面。

图5-53 VNC

VNC功能

VNC使能

端口

33821

[恢复默认值](#)

超时时长(分钟)

66

键盘布局

日式键盘

VNC密码

确认VNC密码

密码有效期(天)

187

登录规则

规则 1

允许时间:

至

允许IP段:

允许MAC段:

规则 2

允许时间:

至

允许IP段:

允许MAC段:

规则 3

允许时间:

至

允许IP段:

允许MAC段:

[点击跳转至 "安全配置" 页面修改登录规则](#)

SSL加密

最大会话

5

活跃会话

0

保存

参数说明

表5-59 VNC

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

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

5.6.6 SNMP

功能介绍

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

在“SNMP”页面，您可以查看和设置 SNMP 功能的开启情况及相关配置项目。

BMC 支持多个版本的 SNMP：

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

说明

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

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

界面描述

在导航栏中选择“服务管理 > SNMP”，打开如下图所示界面。

图5-54 SNMP 功能

SNMP功能

SNMP使能

端口

161

恢复默认值

联系人

位置

SNMP选择

☐ SNMPv1

☐ SNMPv2

超长口令

☐ 删除只读团体名

只读团体名

确认只读团体名

☐ 删除读写团体名

读写团体名

确认读写团体名

登录规则

规则 1

允许时间:

至

允许IP段:

允许MAC段:

规则 2

允许时间:

至

允许IP段:

允许MAC段:

规则 3

允许时间:

至

允许IP段:

允许MAC段:

点击跳转至“安全配置”页面修改登录规则

☒ SNMPv3

引擎ID

0x80001f88030018e1c5d8669e93

保存

参数说明

表5-60 SNMP 功能

参数	说明
SNMP 使能	SNMP 服务的启用状态。

2023-07-27

158

参数	说明
	默认为开启状态。
端口	SNMP 服务使用的端口号，默认为 161。 取值范围：1～65535
联系人	服务器的管理人员。 取值范围：0～255 个字符组成的字符串，由数字、英文字母和特殊字符组成。
位置	服务器的物理位置。 取值范围：0～255 个字符组成的字符串，由数字、英文字母和特殊字符组成。
SNMP 选择	选择 SNMP 服务。
SNMPv1/SNMPv2 说明 - SNMPv1 和 SNMPv2 服务默认为关闭状态。 - 如果启用该版本的 SNMP 服务，请及时修改 SNMP 的团体名。	
超长口令	超长口令的启用状态。 启用超长口令后，设置的团体名长度必须大于等于 16 个字符。 默认取值：开启。
只读团体名	SNMP 协议只读团体名。 取值原则： - 关闭密码检查功能时： - 若已启用超长口令，则团体名可设置为长度为 16～32 个字符的字符串，字符串不能包含空格。 - 若已禁用超长口令，则团体名可设置为长度为 1～32 个字符的字符串，字符串不能包含空格。 - 开启密码检查功能时： - 若已启用超长口令，则团体名可设置为长度为 16～32 个字符的字符串。 - 若已禁用超长口令，则团体名可设置为长度为 8～32 个字符的字符串。 - 至少包含以下特殊字符： `~!@#\$%^&*()-_+=+ [{ }];:","<.>/? - 至少包含以下字符中的两种： - 大写字母：A～Z - 小写字母：a～z - 数字：0～9 - 不能包含空格。 - 弱口令字典认证功能使能的情况下，团体名不能在弱口令字典

参数	说明
	中。（弱口令可通过导出弱口令字典命令 ipmcset -t user -d weakpwddic -v export <filepath file_URL> ）获取。
确认只读团体名	重复输入上一步的只读团体名，确认输入是否正确。
删除只读团体名	删除已配置的只读团体名。 说明 - 勾选“删除只读团体名”时，无法同时设置“只读团体名”。 - 建议在不使用 SNMPv1、SNMPv2 时将已配置的只读团体名删除。
读写团体名	SNMP 协议读写团体名。 取值原则： - 关闭密码检查功能时： - 若已启用超长口令，则团体名可设置为长度为 16~32 个字符的字符串，字符串不能包含空格。 - 若已禁用超长口令，则团体名可设置为长度为 1~32 个字符的字符串，字符串不能包含空格。 - 开启密码检查功能时： - 若已启用超长口令，则团体名可设置为长度为 16~32 个字符的字符串。 - 若已禁用超长口令，则团体名可设置为长度为 8~32 个字符的字符串。 - 至少包含以下特殊字符： `~!@#%\$^&*()_-+=\ [{ }];: ",<.>/? - 至少包含以下字符中的两种： - 大写字母：A~Z - 小写字母：a~z - 数字：0~9 - 不能包含空格。 - 弱口令字典认证功能使能的情况下，团体名不能在弱口令字典中。（弱口令可通过导出弱口令字典命令 ipmcset -t user -d weakpwddic -v export <filepath file_URL>）获取。
确认读写团体名	重复输入上一步的读写团体名，确认输入是否正确。
删除读写团体名	删除已配置的读写团体名。 说明 - 勾选“删除读写团体名”时，无法同时设置“读写团体名”。 - 建议在不使用 SNMPv1、SNMPv2 时将已配置的读写团体名删除。
登录规则	SNMPv1 和 SNMPv2 用户对应的登录规则，对已选择该登录规则的本地用户进行限制。

参数	说明
SNMPv3 说明	BMC 系统支持开启或关闭 SNMPv3 服务，SNMPv3 服务默认为开启状态。
引擎 ID	SNMP 代理实体的 SNMP 引擎的唯一标识符。

5.7 BMC 管理

5.7.1 网络配置

功能介绍

在“网络配置”界面，您可以查询和设置 BMC 管理网口的网络配置情况，包括：

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

须知

变更管理网口地址会导致网络连接断开，请谨慎操作。

界面描述

在导航栏中选择“BMC 管理 > 网络配置”，打开如下图所示界面。

图5-55 网络配置

主机名

主机名

网口模式

选择模式

固定设置

自动选择

NCSI模式

自动故障切换模式

手动切换模式

指定管理网口

专用网口

Mgmt

板载网口

Port1

Port2

Port3

Port4

保存

网络协议

选择网络协议

IPv4

IPv6

IPv4/IPv6

IPv4

自动获取

手动配置

IP地址

掩码

默认网关

MAC地址

20:20:05:13:08:42

IPv6

自动获取

手动配置

IP地址

前缀长度

默认网关

链路本地地址

fe80::220:5ff:fe13:842/64

保存

DNS

DNS信息

自动获取IPv4 DNS地址

自动获取IPv6 DNS地址

手动配置

域名

首选服务器

备选服务器1

备选服务器2

保存

NCSI VLAN

VLAN使能

VLAN ID

保存

LLDP

LLDP使能

工作模式

发送延迟(秒)

发送周期(秒)

邻居节点时间保持倍数

保存

参数说明

表5-61 网络配置

参数	说明
主机名	BMC 的主机名称。

参数	说明
	取值范围：1~64 位的字符串。 可由数字、英文字母和连字符（-）组成，且连字符不能出现在开头和结尾。
选择模式	BMC 管理网口的选择模式。 默认值为“固定设置”。
固定设置	指定 BMC 的管理网口。 - 专用网口：专用的 BMC 管理网口（即服务器 Mgmt 网口）。 - PCIe 扩展网口：PCIe 卡的业务网口（即支持 NC-SI 且已连接 NC-SI 线缆的 PCIe 扩展网卡）。 默认为“专用网口”。
自动选择	依据网口连接状态，BMC 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，BMC 根据如下顺序选择管理网口： 专用网口 > PCIe 扩展网口（Port1~Port2 或 Port1~Port4） 说明 如果某个网口此时作为 BMC 的管理网口，网口右侧会出现  标识。
NCSI 模式	选择模式设置“自动选择”下的 NCSI 网口切换模式。 默认值为“手动切换模式”。
自动故障切换模式	根据扩展网口连接状态自动切换到优先级更高的扩展网口。在遵循自动选择规则下，BMC 的扩展网口根据如下顺序选择： port1>port2 或 port1>port2>port3>port4
手动切换模式	手动切换到优先级更高的扩展网口。
指定管理网口	“固定设置”模式下，选中单选按钮指定管理网口。 “自动选择”模式下，勾选复选框设置参与自动选择的网口。
网络协议	支持的 IP 协议包括： - IPv4：只使能 IPv4 协议，此时只能配置 IPv4。 - IPv6：只使能 IPv6 协议，此时只能配置 IPv6。 - IPv4/IPv6：既使能 IPv4 协议又使能 IPv6 协议，此时既能配置 IPv4 又能配置 IPv6。 默认值：IPv4/IPv6
IPv4	- 自动获取：服务器自动获取管理网口的 IPv4 地址。 - 手动配置：自定义管理网口的 IPv4 地址。管理网口的 IPv4 地址信息包括：“IP 地址”、“掩码”、“默认网关”和

参数	说明
	“MAC 地址”。 默认为“手动配置”。 说明 “MAC 地址”是网卡的硬件地址。 - 如果不使用默认网关，网关地址可以配置为同一网段的任一 IP 地址。
IPv6	- 自动获取：服务器自动获取管理网口的 IPv6 地址。 - 手动配置：自定义管理网口的 IPv6 地址。管理网口的 IP 地址信息包括“IP 地址”、“前缀长度”、“默认网关”、“链路本地地址”。 默认为“手动配置”。 说明 “链路本地地址”用于本地链路通讯。 “IP 地址 2”列出了通过 SLAAC (Stateless Address Autoconfiguration) 协议获取到的 IPv6 地址，最多可以获取到 15 个。 - 如果不使用默认网关，网关地址可以配置为同一网段的任一 IP 地址。
DNS	- 自动获取 IPv4 DNS 地址：无需手动操作，系统自动获取基于 IPv4 的 DNS 信息。 - 自动获取 IPv6 DNS 地址：无需手动操作，系统自动获取基于 IPv6 的 DNS 信息。 - 手动配置：选择手动设置 DNS 信息后，用户可以手动配置 DNS 服务器的域名、首选 DNS 服务器地址和备选 DNS 服务器地址。 默认为“手动配置”。 须知 - BMC 管理网口的 IP 地址获取模式为自动获取时，DNS 信息获取方式可以选择自动获取或者手动配置，建议选择自动获取。 - BMC 管理网口的 IP 地址获取模式为手动配置时，DNS 信息获取方式也必须选择手动配置。 域名：服务器的域名称。 取值原则： - 最大长度为 67 个字符。 - 可由数字、大小写英文字母和连接号 (-)，点号 (.) 组成。 - 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 - 任意两个点号之间的字符长度不允许超过 63。 首选服务器：优先选择的 DNS 服务器。

参数	说明
	取值原则：IPv4 地址、IPv6 地址或为空 • 备选服务器 1：第二选择的 DNS 服务器。 • 备选服务器 2：第三选择的 DNS 服务器。 取值原则：IPv4 地址、IPv6 地址或为空
VLAN 使能	使能或禁止 NCSI 网口的 VLAN 属性。 默认关闭。 说明 • 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 BMC 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 BMC 管理网口，则当前配置的 VLAN 信息有效。
VLAN ID	NCSI 网口所属 VLAN。 取值范围：1~4094 的整数。 说明 VLAN ID 配置保存后，需要几秒钟之后功能才会生效。
LLDP 说明 仅在专用网口作为 BMC 的管理网口场景下支持 LLDP 功能。	
LLDP 使能	开启 LLDP 后，BMC 可将自身设备的 MAC 地址通过标准报文发送给直连设备，方便网络管理系统查询及判断链路通信状况。 默认值：关闭
工作模式	BMC 当前仅支持发送 LLDP 报文，不接收 LLDP 报文。
发送延迟(秒)	在当前工作模式下，BMC 本地配置（主要为切换管理网口或插拔管理网口网线）发生变化时，会发送 LLDP 报文通知邻居设备。 为防止本地信息频繁变化而引起 LLDP 报文的大量发送，LLDP 服务定义了一个延迟时间（单位为秒），在延迟时间内，检测到 BMC 本地配置有变化时，则重新计时，到达延迟时间后，再发送下一个 LLDP 报文。 取值范围：1~8192 默认值：2
发送周期(秒)	当前工作模式下，若本地信息无变化，BMC 会周期性地向邻居发送 LLDP 报文，单位为秒。 取值范围：5~32768 默认值：30
邻居节点时间保持	若邻居节点在指定时间内（发送周期×邻居节点时间保持倍

参数	说明
倍数	数) 未收到 BMC 的 LLDP 报文，则自动清除之前保留的报文信息。 取值范围：2~10 默认值：4

5.7.2 时区&NTP

功能介绍

通过使用“时区&NTP”界面，您可以：

- 查询和设置系统时区。
- 查询和设置 NTP 功能。

界面描述

在导航栏中选择“BMC 管理 > 时区&NTP”，打开如下图所示界面。

图5-56 NTP&时区

时区

地区

亚洲

时区

上海(UTC+08:00)

NTP功能

NTP使能

DHCP获取

DHCPv4 自动获取

DHCPv6 自动获取

手动配置

服务器一

服务器二

服务器三

最小轮询间隔

10 (17分4秒)

最大轮询间隔

12 (1时8分16秒)

服务器身份认证

上传NTP组密钥

上传

保存

参数说明

表5-62 时区&NTP

参数	描述
时区	BMC 系统的时区。 时区信息由“地区”和“时区”组成。 默认值：“其他”+“UTC” 说明 当选择“DHCPv4 自动获取 NTP 信息”时，不需要设置时区信息。

参数	描述
	- 在支持夏令时的时区，BMC 时间会在每年开始夏令时时自动调快 1 小时，结束夏令时时自动调慢 1 小时。 - 在操作系统中执行时间同步时，为了保证操作系统时间与 BMC 时间一致，请执行命令 hwclock --utc -w。
NTP 功能	
NTP 使能	使能或禁止 BMC 的 NTP 功能。使能 NTP 服务后，BMC 系统时间可从 NTP 服务器同步。 默认为关闭状态。
DHCP 获取	- DHCPv4 自动获取：无需手动操作，系统自动获取基于 IPv4 的 NTP 信息。 - DHCPv6 自动获取：无需手动操作，系统自动获取基于 IPv6 的 NTP 信息。 - 手动配置：选择手动设置 NTP 信息后，用户可以手动配置 NTP 服务器地址。 默认为“手动配置”。 须知 - BMC 管理网口的 IP 地址获取模式为自动获取时，NTP 信息获取方式可以选择自动获取或者手动配置，建议选择自动获取。 - BMC 管理网口的 IP 地址获取模式为手动配置时，NTP 信息获取方式也必须选择手动配置。
- 服务器一～三 - 首选服务器一～三或备选服务器一～三	优先选择的 NTP 服务器的地址。 取值范围：IPv4 地址、IPv6 地址和域名 说明 域名的取值原则： - 最大长度为 67 个字符。 - 可由数字、大小写英文字母和连接号 (-)，点号 (.) 组成。 - 连接号不能作为域名的开头或结尾，点号不能作为域名的开头。 - 任意两个点号之间的字符长度不允许超过 63。 提供两种选择方案。具体方案请以实际界面为准。 - 服务器一～三：提供三个 NTP 服务器。实际使用时，三个服务器地址同时生效。 - 首选服务器一～三或备选服务器一～三：提供三组 NTP 服务器，每组服务器中，左侧为首选服务器，右侧为备选服务器。实际使用时，按照以下优先级规则选择服务器地址： - 分别从每组中选择一个服务器地址。 - 当某组两个服务器地址均无效时，放弃选择该组服务器地址。 - 当某组只有一个服务器地址有效时，选择有效服务器地址。

参数	描述
	– 当某组两个服务器地址均有效时，优先选择 IPv6 地址。如果均为 IPv4 或 IPv6 地址，则优先选择首选服务器地址。 说明 NTP 主备服务器的切换与 BMC 和 NTP 服务器之间的同步时间间隔（最小轮询间隔 ≤ 同步时间间隔 ≤ 最大轮询间隔）有关，当 BMC 多次与主用服务器同步无响应时，NTP 服务器将切换为备用服务器。
最小轮询间隔	BMC 系统从 NTP 服务器进行时间同步的最小周期，即 NTP 报文的最小轮询间隔时间。 如最小轮询间隔为 6，表示间隔时间为 2 的 6 次方秒，即 1 分 4 秒。 取值范围：3~17 默认为“6（1 分 4 秒）”。
最大轮询间隔	BMC 系统从 NTP 服务器进行时间同步的最大周期，即 NTP 报文的最大轮询间隔时间。 如最大轮询间隔为 6，表示间隔时间为 2 的 6 次方秒，即 1 分 4 秒。 取值范围：3~17 默认为“10（17 分 4 秒）”。
服务器身份认证	BMC 系统与 NTP 服务器通信时，是否需要进行身份认证。 默认为关闭状态。
上传 NTP 组密钥	当开启服务器身份认证时，需要上传密钥到 BMC，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，密钥文件的格式为“.keys”，最大不超过 2MB。 - 仅支持上传 SHA256 和 SHA512 算法生成的秘钥文件。 - 请定期更新密钥，否则可能存在安全风险。

设置时区

- 步骤 1 在“地区”和“时区”下拉列表中，根据表 5-62 时区&NTP 提供的参数信息，选择要设置的参数。
- 步骤 2 单击“保存”。
- 显示“操作成功”表示设置成功。

 说明

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

- 当修改时区后，BMC 页面上 CPU 占用率、内存占用率、网口带宽占用率、磁盘占用率、历史功率、进风口温度等曲线涉及的时间，需要重启 BMC 后生效。

----结束

配置 NTP 信息

步骤 1 在“NTP 功能”区域框中，根据表 5-62 时区&NTP 提供的参数信息，设置 NTP 信息。

步骤 2 单击“保存”。

显示“操作成功”表示设置成功。

----结束

5.7.3 固件升级

功能介绍

通过“固件升级”功能，您可以：

- 查看版本信息。
- 重启 BMC 系统。
- 进行可用分区镜像倒换。
- 通过带外通道升级服务器固件。
- 通过带内通道升级服务器固件。

BMC 系统存在以下 3 个分区镜像：

- 主用分区镜像：BMC 当前生效的分区。
- 备用分区镜像：主用分区镜像的备份，当主用分区镜像异常时，备用分区镜像自动切换为主用分区镜像，原主用分区镜像降为备用分区，并同步当前主用分区镜像的版本，使得主用和备用分区镜像的版本保持一致。升级 BMC 时会同时升级主用和备用分区镜像。
- 可用分区镜像：用作 BMC 储备版本的承载，您可以通过“可用分区镜像倒换”功能，生效可用分区镜像的版本。此时，原可用分区镜像切换为主用分区镜像，原主用分区同步新主用分区镜像后切为备用分区镜像，原备用分区镜像自动切换为可用分区镜像。

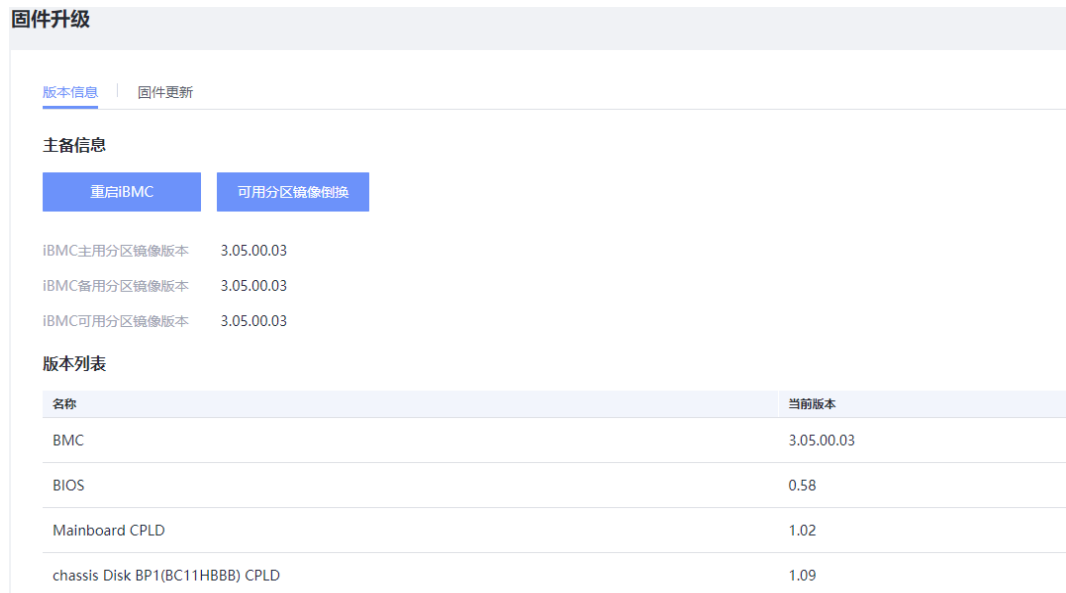
须知

- 在操作系统启动过程中，请不要重启 BMC、镜像倒换或升级 BMC 固件。
- 为确保升级成功，升级过程中不允许断电、不允许重启 BMC 系统。
- 升级 BMC 固件需要重启 BMC 系统使功能生效。但您不需要重启操作系统。因此，服务器上运行的业务不会受到影响。
- 升级电源固件无需重启服务器。
- 在 BMC 和 SD 卡固件升级完成之后，BMC 会自动重启，使升级的固件生效。
- 升级 BIOS 或 CPLD 前，建议先关闭服务器上运行的业务，避免服务器重启时中断业务。
- 如果在操作系统上电状态时升级 BIOS 或 CPLD，则 BIOS 在操作系统下电再上电或重启后生效，CPLD 在操作系统下电后生效。
- 如果在操作系统下电状态时升级 BIOS 或 CPLD，则 BIOS 和 CPLD 在操作系统上电后生效。
- 通过带内通道升级固件前，建议先关闭服务器上运行的业务，避免服务器自动重启时中断业务。
- 当 BMC 可用分区镜像与主分区镜像的版本不一致时，单击“可用分区镜像倒换”可能会对服务器上运行的业务产生影响，请谨慎操作。

界面描述

在导航栏中选择“BMC 管理 > 固件升级”，打开如下图所示界面。

图5-57 固件升级



参数说明

表5-63 版本信息

参数	描述
主备信息	
重启 BMC	重启 BMC 系统使设置生效。
可用分区镜像倒换	将 BMC 固件主用分区的镜像文件切换到可用分区的镜像文件。
BMC 主用分区镜像版本	BMC 固件主用分区镜像的版本号。
BMC 备用分区镜像版本	BMC 固件备用分区镜像的版本号。
BMC 可用分区镜像版本	BMC 固件可用分区镜像的版本号。
版本列表	
名称	固件的名称。
当前版本	固件当前的版本号。

表5-64 固件更新

参数	描述
带外通道	
升级文件	升级文件的格式为“.hpm”，最大不超过 90MB。 升级文件的命名规则：可由数字、大小写英文字母、圆括号（）、点号（.），下划线（_）和连接号（-）组成。
生效分离	BMC 固件升级完成后是否立即重启 BMC，使升级的固件生效。 默认勾选。 说明 本选项仅适用于 BMC 升级操作。
带内通道	
升级文件	升级文件的格式为“.zip”，最大不超过 499MB。
签名文件	签名文件的格式为“.asc”（pgp）或“.p7s”（cms），最大不超过 90MB。
ID	上传的升级文件的序号。

参数	描述
名称	上传的升级文件的名称。

查看固件版本

步骤 1 在上方标题栏中选择“BMC 管理”。

步骤 2 在左侧导航树中，选择“固件升级”。

右侧显示“版本信息”界面，界面中显示服务器固件的名称和版本信息。

----结束

升级固件（带外通道）

以下操作以升级 BMC 为例，同时适用于升级其他固件，详细操作请参见各服务器对应的升级指导书。

步骤 1 选择“固件更新 > 带外通道”。

步骤 2 单击“添加文件”并选择待上传的文件。

说明

- 升级文件的格式为“.hpm”，最大不超过 90MB。
- 升级文件的命名规则：可由数字、大小写英文字母、圆括号（）、点号（.），下划线（_）和连接号（-）组成。

步骤 3（可选）勾选“升级完成后立即重启 BMC，使升级的固件生效”前方的复选框。

说明

本选项仅适用于 BMC 升级操作。

步骤 4 单击“开始升级”。

弹出对话框提示以下信息：

是否确定执行此操作？

步骤 5 单击“确定”。

BMC 系统开始执行升级操作。

升级成功后，BMC 将进入自动重启并跳转至登录页面。

请耐心等待几分钟，重启完成后将自动恢复到 BMC 正常的登录页面。

----结束

升级固件（带内通道）

以下操作适用于支持通过 SP 升级的固件（例如网卡、RAID 卡和硬盘固件），升级前，需要先下载固件升级包和签名文件。

步骤 1 选择“固件更新 > 带内通道”。

步骤 2 分别单击“升级文件”和“签名文件”后面的“添加文件”选择并上传升级文件和签名文件。

说明

- 升级文件的格式为“.zip”，最大不超过 499MB。
- 签名文件的格式为“.asc”（pgp）或“.p7s”（cms），最大不超过 90MB。

步骤 3 单击“上传”。

弹出对话框提示以下信息：

是否立即到 SP 管理界面设置下次 OS 从 SP 启动？

说明

- 如果需要上传其他固件升级包，单击“取消”，重复 [步骤 2](#) 和 [步骤 3](#) 继续上传固件升级包和签名文件。
- 如果需要清除已上传的固件升级包，单击“取消”，然后单击“清除”，清除所有已上传的文件。

步骤 4 单击“确认”。

进入“SP 管理”界面。

步骤 5 将“OS 从 SP 启动”设置为开启状态，并在弹出的操作确认对话框中单击“确认”。

步骤 6 重启服务器进入 SP 升级固件。

详细操作请参见对应版本的 Smart Provisioning 用户指南。

---结束

切换 BMC 固件的镜像文件

请您根据需要切换 BMC 固件的镜像文件。此操作不是升级过程中的必做操作。

步骤 1 在“版本信息”界面中，单击“可用分区镜像倒换”。

弹出对话框提示以下信息：

是否确定可用分区镜像倒换？

步骤 2 单击“确定”。

界面提示“可用分区镜像倒换成功”。

切换成功后，BMC 将进入自动重启并跳转至登录页面。

请耐心等待几分钟，重启完成后将自动恢复到 BMC 正常的登录页面。

----结束

重启 BMC

请您根据需要重启 BMC。此操作不是升级过程中的必做操作。

步骤 1 在“版本信息”界面中，单击“重启 BMC”。

弹出对话框提示以下信息：

是否确定重启BMC？

步骤 2 单击“确定”。

BMC 开始重启并跳转至登录页面。

请耐心等待几分钟，重启完成后将自动恢复到 BMC 正常的登录页面。

----结束

5.7.4 配置更新

功能介绍

您可以通过“配置更新”界面实现服务器 BMC、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 BMC 用户指南的[配置文件说明](#)章节。

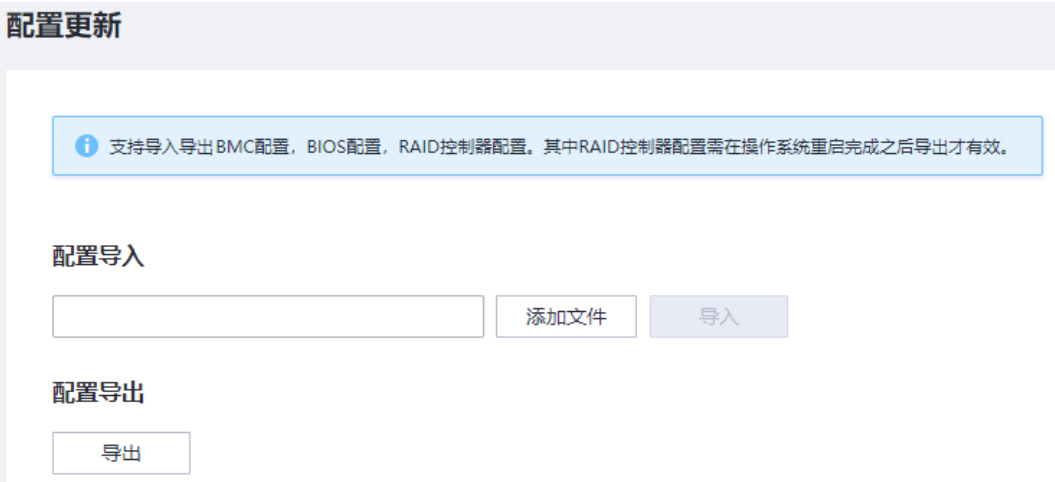
说明

- 仅管理员用户可进行配置导入或配置导出操作，导入或导出的配置文件格式为“.xml”，最大不超过 1MB。
- 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 BMC 查看操作日志确认是否导入成功。
- 在导出的配置文件中，如果某个配置项默认为密文，在导入其他服务器时无法生效。若需要在其他服务器上导入该配置项信息，则需要将配置文件中对应信息修改为明文，并删除该行注释符后才能支持导入生效。
- 导出的配置文件不体现 BMC 管理网口的 IP 地址信息。
- 仅支持导入导出 BMC 配置、BIOS 配置和部分的 RAID 控制器配置。

界面描述

在导航栏中选择“BMC 管理 > 配置更新”，打开如[图 5-58](#) 所示界面。

图5-58 配置更新



导入配置文件

须知

配置文件导入属于高危操作，请谨慎处理。

- 步骤 1 （可选）编辑配置文件。
- 1. 使用文本工具打开待导入的配置文件并找到需要编辑的配置项。
 - 2. 编辑配置项信息。
- 下面以“SenderName”为例进行说明，如图 5-59 所示。将“SenderName”的值由“*****”改为实际的字符串，例如“Sendertext123456789012@example.com”。

图5-59 编辑前的配置文件

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

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

图5-60 编辑后的配置文件

```
<Attribute Key="SmtpConfig.65.0.0.7" Name="/SmtpConfig/SmtpServer"></Attribute>
<Attribute Key="SmtpConfig.65.0.0.8" Name="/SmtpConfig/SenderName">Sendertext123456789012@xxx.com</Attribute>
<Attribute Key="SmtpConfig.65.0.0.9" Name="/SmtpConfig/TempletTopic">Server Alert</Attribute>
```

- 4. 保存修改。

步骤 2 单击“配置导入”区域的“添加文件”，并选择要上传的配置文件。

文件上传后，显示在“配置导入”区域。

说明

支持导入的配置文件格式为“.xml”，最大不超过 1MB。

步骤 3 单击“导入”。

弹出操作确认对话框。

步骤 4 输入当前用户的登录密码并单击“确定”。

导入成功后，弹出对话框提示以下信息：

导入成功，BIOS 配置需要重启业务系统生效。

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

说明

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

----结束

导出配置文件

步骤 1 单击“配置更新”页面中的“导出”。

文件开始导出并自动保存到本地 PC 默认路径。

----结束

5.7.5 语言管理

功能介绍

通过使用“语言管理”界面的功能，您可以开启和关闭 BMC 支持的语言。

说明

- 仅管理员及具有常规设置类权限的用户有开启和关闭语言的权限。
- 当前仅支持中、英、日、法、俄五种语言，中英文默认为开启状态。其中日语、法语、俄语可根据实际需要开启或关闭。

界面描述

在导航栏中选择“BMC 管理 > 语言管理”，打开如图 5-61 所示界面。

图5-61 语言管理

语言信息			
序号	语言代码	语言名称	操作
1	en	English	
2	zh	中文	
3	ja	日本語	
4	fr	Français	
5	ru	Русский	

参数说明

表5-65 语言管理

参数	描述
序号	某种语言的序号。
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，“ru”代表俄语。
语言名称	显示语言代码代表的语种名称。
操作	根据实际需要开启或关闭目标语言。  表示开启目标语言。  表示关闭目标语言。

查看已开启的语言

- 步骤 1 选择“BMC 管理”。
- 步骤 2 在左侧导航树中，选择“语言管理”。
- 右侧显示“语言管理”界面，可查看到当前已开启的语言。
- 结束

开启目标语言

- 步骤 1 在“语言管理”界面中，单击目标语言右侧的。
- 步骤 2 单击“确认”。
- 开启完成后界面将显示“操作成功”提示信息。
- 结束

5.7.6 许可证管理

功能介绍

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

BMC 高级版较标准版提供更多的高级特性，例如：

- 通过 Redfish 实现 OS 部署。
- 通过 Redfish 收集智能诊断的原始数据。
- 使能鲲鹏加速引擎，包括硬件安全加速引擎（SEC，Security Engine）、高性能 RSA 加速引擎（HPRE，High Performance RSA Engine）、RAID DIF 运算加速引擎（RDE，RAID DIF Engine）、ZIP 四个加速器。
- 使能系统锁定模式。

界面描述

在导航栏中选择“BMC 管理 > 许可证管理”，打开如下图所示界面。

图5-62 许可证管理

许可证管理

许可证信息

安装

设备ESN: 1FB811FE20CA8B952718A5CE66C28790CA41A2F6

许可证状态: 正常

删除

失效

导出

基本信息

许可证序列号LIC20180820LDM5C

许可证类型商用

许可证级别高级版

截止日期永久

高级特性

序号	特性名称	特性状态	当前状态	截止日期
1	Smart Provisioning, Data Acquisition	正常	已开启	永久
2	Kunpeng accelerator SEC Function	--	已关闭	--
3	Kunpeng accelerator HPRE Function	--	已关闭	--
4	Kunpeng accelerator RDE Function	--	已关闭	--
5	Kunpeng accelerator ZIP Function	--	已关闭	--

参数说明

表5-66 许可证管理

参数	描述
设备 ESN	用于申请许可证的 ESN，由主板的序列号生成。
安装	安装许可证。

参数	描述
	说明 - 许可证的格式为“.xml”，最大不超过 1MB。 - 不能安装已经执行过“失效”操作的许可证，安装时会提示安装失败。
删除	删除许可证。
失效	使许可证失效。 许可证失效后进入宽限期并且可以从界面获得许可证的失效码。例如用户需要更换备件，您需要执行“失效”操作来获取失效码，凭此失效码申请新的许可证后，将许可证安装到备件。 说明 不能安装已经执行过“失效”操作的许可证，请谨慎操作。
导出	导出已经安装的许可证。 用户可以导出许可证并进行备份。
许可证状态	许可证的状态包括： - 正常状态：已安装商用许可证，许可证未过期，所有授权特性为正常状态。 - 调测状态：已安装调测许可证，许可证未过期，所有授权特性为正常状态。 - 宽限状态：已安装商用或调测许可证，许可证已过期且在宽限期内，所有授权特性进入宽限状态。 - 默认状态：已安装商用或调测许可证，但是许可证已过期且已过宽限期。
失效码	在已安装许可证的情况下，执行许可证“失效”操作后生成的失效凭证，用户可以凭此失效码申请新的许可证。
许可证信息	许可证的信息包括： - 许可证序列号 - 许可证类型：提供两种许可证类型。 - 商用：基于合同发放给客户的正式许可证，所有授权特性的截止日期一致，授权特性截止日期为永久或某个具体时间，过期后自动进入宽限期，宽限天数为 60 天。 - 试用：用于新特性试用、客户现场设备调测或品牌展览的临时许可证，有效使用时间根据实际情况而定，过期后自动进入宽限期，宽限天数为 60 天。 - 许可证级别： - 标准版（默认）：默认版本，无需用户自行购买。 - 高级版：以授权方式提供较标准版更多的特性，需要用户自行购买。 - 截止日期：授权特性授权截止的日期，可以是永久或某个

参数	描述
	具体时间。 说明 许可证过期后的宽限期表示许可证过期后，仍可以使用 BMC 的天数。 宽限天数固定为 60 天。
高级特性	显示许可证高级特性，包括序号、特性名称、特性状态、当前状态和使用截止日期。

5.7.7 BMA 管理

功能介绍

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

通过“BMA”管理界面，可实现通过远程控制台将 BMA 安装到操作系统中。

BMA 安装成功后，此界面将显示 BMA 的基本信息，包括版本号、运行状态和驱动版本。

界面描述

在导航栏中选择“BMC 管理 > BMA 管理”，打开如下图所示界面。

图5-63 BMA 管理



参数说明

表5-67 BMA 管理

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

参数	描述
	- 此参数项显示为“--”时，表示 BMA 未安装或已安装但未运行。 - 此参数项显示为“Running”时，表示 BMA 已安装且正在运行。 - 此参数项显示为“Unhealthy”时，表示 BMA 已安装且不能正常运行。
BMA 驱动版本	显示 BMA 的驱动版本信息。 此参数项显示为“--”时，表示 BMA 未安装或已安装但未运行。

安装 BMA

说明

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

步骤 1 单击“安装 BMA”。

BMA 将连接服务器操作系统。连接成功后，弹出“安装说明”页面。

步骤 2 单击“安装说明”页面的“启动远程控制台”。

将启动远程控制台。

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

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

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

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

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

- 执行 **cat README.TXT**。

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

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

For more information on installation instructions, including silent installation
options, see the "BMA 2.0 User Guide".

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

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

步骤 6 根据[表 5-68 操作系统与安装文件路径关系表](#)所示信息并参阅最新版本的 BMA 用户指南，进行安装 BMA 操作。

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

表5-68 操作系统与安装文件路径关系表

操作系统	安装文件路径
Linux	Linux/install.sh

----结束

挂载 BMA 驱动盘

- 步骤 1 在服务器操作系统界面空白处单击鼠标右键，打开菜单。
- 步骤 2 单击菜单中的 **Open Terminal**。打开服务器操作系统命令行界面。
- 步骤 3 执行 **ls SCSI** 命令查询 BMA 驱动盘的属性。

```
[root@localhost ~]# lsscsi
[0:0:0:0]    disk    ATA      ST4000NM0033-9ZM  SN06  -
[0:0:1:0]    disk    ATA      ST4000NC001-1FS1  CN02  -
[0:0:2:0]    disk    ATA      WDC WD6000F9PZ-3  0R01  /dev/sdc
[0:0:3:0]    disk    ATA      WDC WD6000F9PZ-3  0R01  /dev/sdd
[0:0:4:0]    disk    HGST     HUS726060AL4210   A523  -
[0:0:5:0]    disk    HGST     HUS726060AL4210   A7MH  -
[0:0:6:0]    disk    ATA      SSDSC2BB016T7H    0121  /dev/sde
[0:0:7:0]    disk    HGST     HUS726060AL4210   A523  /dev/sdf
[0:1:0:0]    disk    LSI      Logical Volume     3000  /dev/sdb
[0:1:1:0]    disk    LSI      Logical Volume     3000  /dev/sda
[19:0:0:0]   disk    SERVER   BMA USB Device     225   /dev/sdv
```

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

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

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

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

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

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

命令回显返回 **Linux** 表示 BMA 驱动盘已挂载成功。

----结束

5.7.8 SP 管理

功能介绍

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

通过“SP 管理”界面，您可以：

- 配置设备信息收集功能。
- 配置 OS 从 SP 启动功能。

界面描述

在导航栏中选择“BMC 管理 > SP 管理”，打开如图 5-64 所示界面。

图5-64 SP 管理



参数说明

表5-69 SP 管理

参数	描述
设备信息收集使能	该功能开启后，服务器电源模块通电后，带内系统首次上电时，带内系统会先进入 SP 收集设备信息，然后再按照“BIOS 设置”中“优先引导介质”和“启动顺序”的配置来启动服务器。 默认为关闭状态。
OS 从 SP 启动	该功能开启后，重启服务器时，带内系统会先进入 SP。 默认为关闭状态。 说明 仅在下次重启时生效，进入 SP 后，自动恢复为关闭状态。

5.8 虚拟控制台

5.8.1 虚拟控制台概述

功能介绍

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

界面描述

在导航栏中选择“首页”，从如图 5-65 所示界面进入虚拟控制台。

图5-65 虚拟控制台

虚拟控制台



参数说明

表5-70 虚拟控制台

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

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

运行环境

使用远程虚拟控制台需要具备以下版本的操作系统、浏览器和 Java 运行环境，如表 5-71 运行环境所示。

说明

- 如果 Java 运行环境不符合要求，可登录 AdoptOpenJDK 的官方网站进行下载。
- 当在“用户&安全 > 安全配置”界面将 TLS 版本配置为“仅限 TLS 1.3 协议”时，BMC 运行环境不支持以下浏览器版本：
- Safari 11.0~12.0
- Microsoft Edge 12~18

表5-71 运行环境

操作系统	浏览器	Java 运行环境
Windows 7 32 位 Windows 7 64 位	• 支持 Mozilla Firefox 63.0 及以上版本，推荐 96.0~98.0 版本 • 支持 Google Chrome 70.0 及以上版本，推荐 97.0~100.0 版本	AdoptOpenJDK 8u222 JRE AdoptOpenJDK 11.0.6 JRE
Windows 8 32 位 Windows 8 64 位		
Windows Server 2008 R2 64 位		

操作系统	浏览器	Java 运行环境
Windows Server 2012 64 位		
Windows Server 2012 R2 64 位		
Windows Server 2016 64 位		
Windows 10 64 位	- 支持 Microsoft Edge, 推荐 94.0~97.0 版本 - 支持 Mozilla Firefox 63.0 及以上版本, 推荐 96~98 版本 - 支持 Google Chrome 70.0 及以上版本, 推荐 97.0~100.0 版本	
CentOS 7	支持 Mozilla Firefox 63.0 及以上版本, 推荐 96.0~98.0 版本	
MAC OS X v10.7	- 支持 Safari 11.0 及以上版本, 推荐 15.1 和 15.2 版本 - 支持 Mozilla Firefox 63.0 及以上版本, 推荐 96.0~98.0 版本	

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 BMC 导入信任证书和根证书。有关详细信息, 请参见[表 5-71 运行环境](#)。
- 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 BMC 添加为例外站点或降低 Java 安全级别。由于该操作可能降低用户的安全性, 请谨慎使用。
- (常规入口)** 在“首页”界面中, 单击“启动虚拟控制台”区域框, 从弹出的下拉列表中选择“Java 集成远程控制台”或“HTML5 集成远程控制台”。

共享模式可以让 2 个用户连接到服务器, 并同时服务器进行操作。本用户可以看到对方用户的操作, 对方用户也能看到本用户的操作。

独占模式只能有 1 个用户连接到服务器进行操作。选择独占模式方式进入实时桌面后，“维护诊断 > 录像截屏”界面中的“屏幕截图”区域框中的“手动屏幕截屏”按钮无法使用，自己或其他人此时均不能截图。

- （快捷入口）打开浏览器，并在地址栏中输入：
 - 方式一：
 - HTML5 集成远程控制台推荐登录方式：
 - “https://IP address/remoteconsole?openWay=html5” 或 “https://IP address/remoteconsole?openway=html5”
 - “https://IP address/remote_access.asp?authParam=key&lp=lang&openWay=html5” 或 “https://IP address/remote_access.asp?authParam=key&lp=lang&openway=html5”
 - Java 集成远程控制台推荐登录方式：
 - “https://IP address/remoteconsole” 或 “https://IP address/remoteconsole?openWay=jre” 或 “https://IP address/remoteconsole?openway=jre”
 - “https://IP address/remote_access.asp?authParam=key&lp=lang&openWay=jre” 或 “https://IP address/remote_access.asp?authParam=key&lp=lang&openway=jre”

说明

- key 可通过 Redfish 接口设置，使用 key 可直接进行 KVM 连接。
- lp 表示控制台使用的语言类别。
- openWay 参数仅支持“openway”和“openWay”两种式样，若使用其余写法，会跳转至 Java 控制台。
- 方式二：“https://IP address/kvmvmm.asp”
- 方式三：“https://IP address/login.html?redirect_type=1”

说明

“IP address”为 BMC 管理网口的 IP 地址。

5.8.2 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。

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

“KVM”窗口中的按钮及其作用如表 5-72 按钮说明所示。

表5-72 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 不支持平铺显示。
	“退出全屏”按钮。表示取消全屏显示服务器的实时桌面。
	“控制”按钮。表示控制服务器电源。操作包括： • 上电 • 强制下电 • 下电 • 强制重启 • 强制下电再上电
	“系统启动项”按钮。表示设置操作系统的第一启动设备。操作包括： • 未配置：表示不设置第一启动设备，按 BIOS 中设置的默认方式启动操作系统。 • 硬盘：表示强制从硬盘启动系统。 • 光驱：表示强制从 CD/DVD 启动系统。 • 软驱/可拔插移动设备：表示强制从软驱或可拔插移动设备启动系统。 • PXE：表示强制从预启动执行环境（PXE，Pre-boot Execution Environment）启动系统。 • BIOS 设置：表示服务器启动后直接进入 BIOS 菜单中。
	“键盘组合键”按钮。表示发送或自定义特殊组合键。该窗口中的组合键及其含义包括： • Alt+Tab：在打开的项目中进行切换。 • Ctrl+Esc：显示或收起“开始”菜单。 • Ctrl+Shift：切换输入法。 • Ctrl+Space：开启或关闭输入法。 • Ctrl+Alt+Del：锁定操作系统界面、注销用户、更改密码和打开任务管理器、重新启动服务器等。 • 自定义按键：如果您需要自定义组合键，请在“自定义按键”后的文本框中依次输入按键，然后单击“确定”。

按钮	说明
	说明 在不同的操作系统中，操作系统各自定义的组合键及其含义不同。该窗口中的组合键及其含义仅适用于 Windows 操作系统。
	“鼠标控制”按钮。表示控制服务器鼠标。操作包括： - 鼠标加速 加速服务器实时桌面上的鼠标，使其与本地 PC 上的鼠标同步。 说明 低于 SUSE 12 版本的 SUSE 操作系统不支持鼠标加速功能。 - 单鼠标 隐藏本地 PC 上的鼠标，只显示服务器实时桌面上的鼠标。 - 键鼠复位 模拟插拔 USB 键盘和 USB 鼠标，服务器实时桌面上的键盘鼠标出现异常停滞时单击此按钮可以恢复。 默认的操作：鼠标加速 说明 - 鼠标加速和单鼠标均未勾选时，服务器实时桌面鼠标和本地 PC 鼠标同时显示，且服务器实时桌面鼠标不跟随本地 PC 鼠标。 - BMA 驱动盘连接状态下，执行鼠标控制操作会中断此连接。请先断开 BMA 驱动盘连接，再执行鼠标控制操作。
	“CD/DVD”按钮。表示选择并使用虚拟光驱。 说明 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟光驱时，服务器会同时识别到一个无介质的虚拟软驱设备。按照正常操作方式可继续使用虚拟软驱功能。
	“软驱”按钮。表示选择并使用虚拟软驱。 说明 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟软驱时，服务器会同时识别到一个无介质的虚拟光驱设备。按照正常操作方式可继续使用虚拟光驱功能。
	“录像”按钮。表示对远程实时操作进行录像。 说明 开启录像功能后，自动录像功能有可能录制到业务侧的敏感信息，请注意安全风险。
	“键盘布局”按钮。表示客户端的键盘类型。默认情况下，BMC 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。

按钮	说明
	“意式键盘”：强制指定键盘类型为意式键盘。 “德式键盘”：强制指定键盘类型为德式键盘。
	“帮助”按钮。表示查看 KVM 页面联机帮助。
	“图像清晰度”游标图标。表示调节远程实时图像的清晰度。

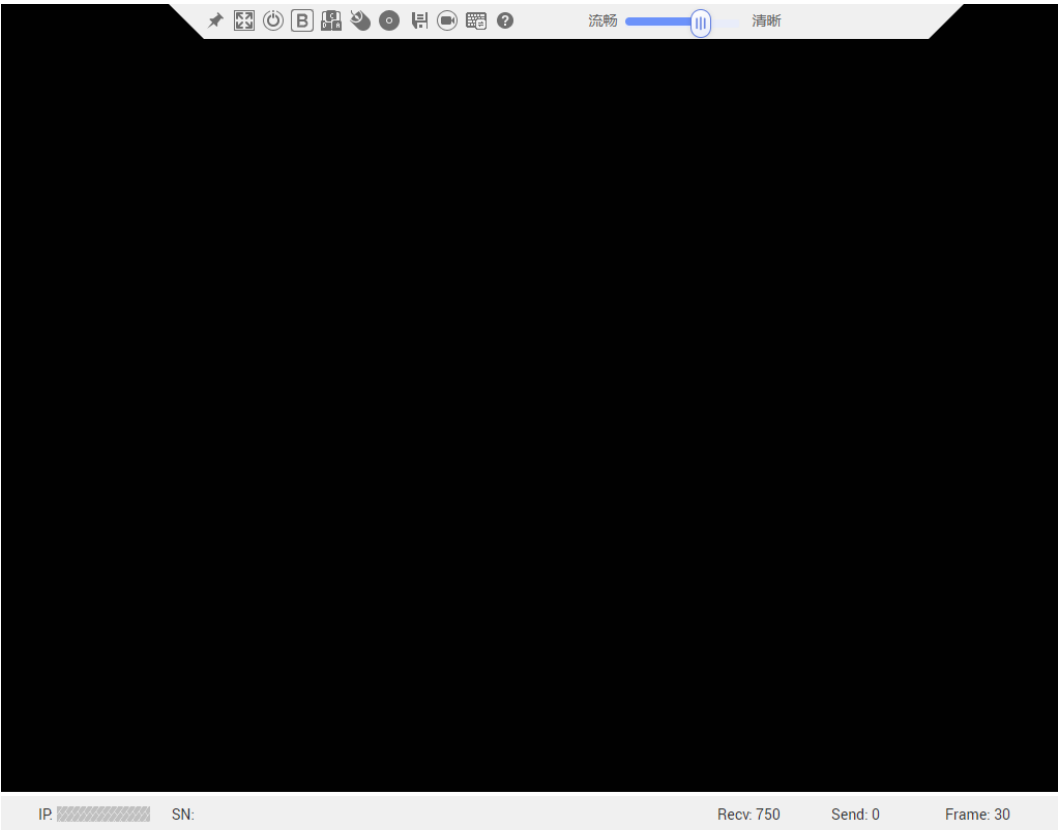
界面描述

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

 说明

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

图5-66 HTML5 KVM



HTML5 KVM 窗口各区域的功能介绍如[表 5-73 HTML5 KVM](#) 所示。

表5-73 HTML5 KVM

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

操作步骤

为服务器上电

- 步骤 1 在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“上电”。
- 步骤 2 单击“确定”。
- 服务器开始上电。

 说明

服务器上电的时间根据服务器配置所不同。

----结束

为服务器下电

须知

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

- 步骤 1 在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“强制下电”或“下电”。
- 步骤 2 单击“确定”。
- 服务器开始下电。
- 结束

强制重启或强制下电再上电

须知

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

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

步骤 2 单击“确定”。

服务器开始强制重启或强制下电再上电。

----结束

说明

服务器强制重启或强制下电再上电的时间根据服务器配置所不同。

设置操作系统的第一启动设备

步骤 1 在“KVM”界面中，单击工具栏上的 。

弹出启动设备列表。

步骤 2 根据表 5-72 按钮说明提供的参数信息，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 5-72 按钮说明提供的参数信息，单击需要发送的组合键。

服务器将执行组合键对应的操作。

说明

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

----结束

加速远程鼠标

本操作对实时桌面上的鼠标进行加速，使其与本地 PC 上的鼠标同步。

在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“鼠标加速”。

同步本地 PC 与服务器的鼠标。

使用单鼠标

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

在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“单鼠标”。

“KVM”界面中只显示实时桌面上的鼠标。

键鼠复位

本操作模拟插拔 USB 键盘和 USB 鼠标。

在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“键鼠复位”。

服务器开始执行 USB 复位操作。

指定客户端的键盘类型

在“KVM”界面中，单击工具栏上的。

从下拉列表中选择目标键盘类型，则成功强制指定键盘类型。

通过虚拟光驱挂载镜像文件

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

步骤 1 在“KVM”界面中，单击工具栏上的。

弹出如图 5-67 的界面。

图5-67 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 5-67 所示的界面。

图5-68 通过虚拟光驱挂载镜像文件



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 5-69 的界面。

图5-69 挂载本地文件



步骤 2 选中 “本地文件” 单选按钮。

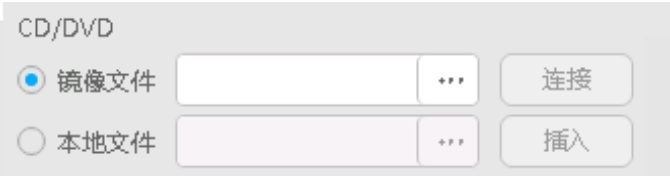
步骤 3 单击 .

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 5-70 所示的界面。

图5-70 挂载本地文件



步骤 5 单击“插入”。

服务器上成功挂载本地文件。

 说明

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

----结束

通过虚拟软驱挂载镜像文件

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

 说明

挂载的镜像文件大小必须为 1.44MB，否则会导致挂载失败。

步骤 1 在“KVM”界面中，单击工具栏上的 。

弹出如图 5-71 所示的界面。

图5-71 通过虚拟软驱挂载镜像文件



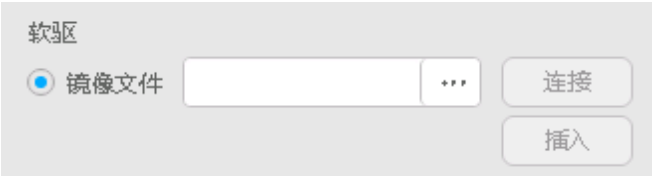
步骤 2 单击 。

打开本地文件夹选择窗口。

步骤 3 选择本地 PC 上存放的“*.img”格式镜像文件，单击“连接”。

返回如图 5-72 所示的界面。

图5-72 通过虚拟软驱挂载镜像文件



步骤 4 单击“连接”。

服务器上成功挂载镜像文件。

说明

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

----结束

为实时桌面录像

本操作对当前远程虚拟控制台显示的画面进行录像。

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

说明

开启录像功能后，自动录像功能有可能录制到业务侧的敏感信息，请注意安全风险。

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

步骤 2 录制完成后，单击 。

录像文件将自动被下载并保存到本地 PC。

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

----结束

5.8.3 Java 集成远程控制台

功能介绍

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

- 您可以在本地 PC 上利用键盘和鼠标对远程的服务器进行远程实时操作。

- 您可以通过网络使服务器以虚拟软驱或光驱的形式实现对本地 PC 的远程访问。从服务器一侧看，虚拟软驱或光驱与实际插入服务器的（USB，Universal Serial Bus）设备的使用方法相同。

“KVM”窗口中的按钮及其作用如表 5-74 按钮说明所示。

表5-74 按钮说明

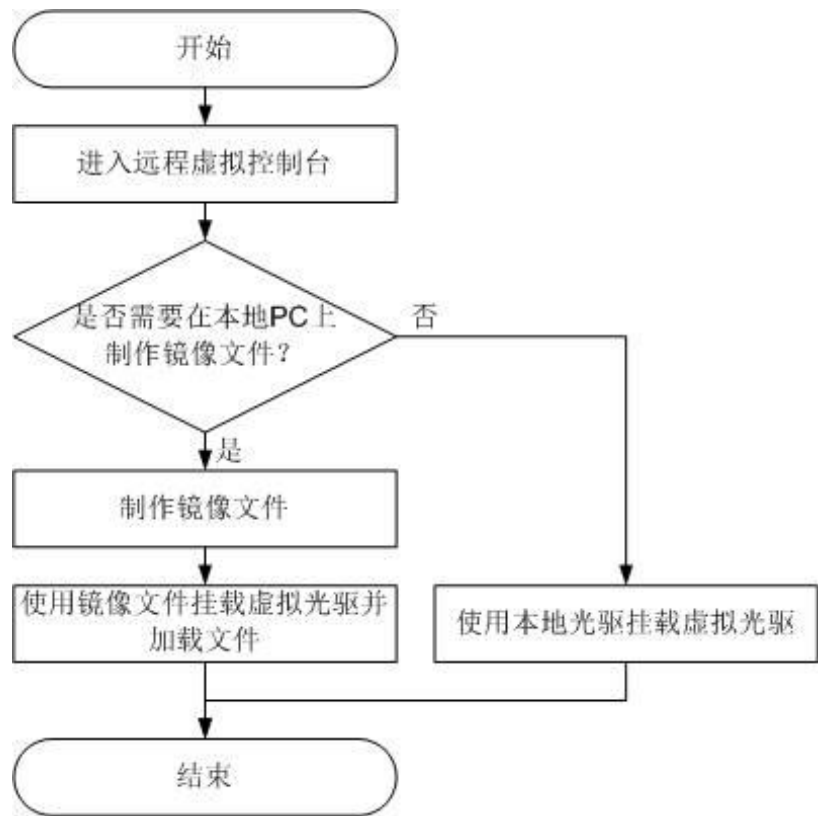
按钮	说明
	浮动按钮。表示当前工具栏被固定。
	浮动按钮。表示当前工具栏被隐藏。
	“全屏”按钮。表示全屏显示服务器的实时桌面。 说明 - 在全屏显示实时桌面时，鼠标移动到屏幕上方会显示工具栏。 - 不支持平铺显示。
	“鼠标同步”按钮。表示纠正鼠标位置。 说明 在全屏显示实时桌面且“鼠标控制”为“单鼠标”模式时，此时单击“切换鼠标模式”后，该按钮才可用。
	“切换鼠标模式”按钮。表示切换鼠标模式。 说明 在全屏显示实时桌面且在“单鼠标”模式下时，该按钮才可用。
	“返回”按钮。表示返回合适的屏幕显示服务器的实时桌面。 说明 只有全屏显示服务器的实时桌面时，工具栏中才会出现该按钮。
	“控制”按钮。表示控制服务器电源。操作包括： - 上电 - 强制下电 - 下电 - 强制重启 - 强制下电再上电
	“录像”按钮。表示对远程实时操作进行录像。 说明 开启录像功能后，自动录像功能有可能录制到业务侧的敏感信息，请注意安全风险。
	“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。

按钮	说明
	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。 • BMA 驱动盘连接状态下，执行鼠标控制操作会中断此连接。请先断开 BMA 驱动盘连接，再执行鼠标控制操作。
	“光驱”按钮。表示选择并使用虚拟光驱。 说明 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟光驱时，服务器会同时识别到一个无介质的虚拟软驱设备。按照正常操作方式可继续使用虚拟软驱功能。
	“软驱”按钮。表示选择并使用虚拟软驱。 说明 虚拟光驱和虚拟软驱属于复合设备，当连接虚拟光驱时，服务器会同时识别到一个无介质的虚拟软驱设备。按照正常操作方式可继续使用虚拟光驱功能。
	“制作镜像文件”按钮。表示使用光驱或软驱制作镜像文件。
	“键盘组合键”按钮。表示发送或自定义特殊组合键。该窗口中的组合键及其含义包括： • Ctrl+Shift：切换输入法。 • Ctrl+Esc：显示或收起“开始”菜单。 • Ctrl+Alt+Del：锁定操作系统界面、注销用户、更改密码和打开任务管理器、重新启动服务器等。 • Alt+Tab：在打开的项目中进行切换。 • Ctrl+Space：开启或关闭输入法。 • ResetKeyboard：模拟弹起键盘上的按键。 • 自定义：如果您需要自定义组合键，请在“自定义”后的文本框中依次输入按键，然后单击“发送”。 说明 在不同的操作系统中，操作系统各自定义的组合键及其含义不同。该窗口中的组合键及其含义仅适用于 Windows 操作系统。
	“键盘布局”按钮。表示客户端的键盘类型。默认情况下，BMC 自动适配客户端的键盘类型。当自适应模式下键盘适配

按钮	说明
	情况不理想时，请强制指定目标键盘类型。 “美式键盘”：强制指定键盘类型为美式键盘。 “日式键盘”：强制指定键盘类型为日式键盘。 “法式键盘”：强制指定键盘类型为法式键盘。 “意式键盘”：强制指定键盘类型为意式键盘。 “德式键盘”：强制指定键盘类型为德式键盘。
图像清晰度	“图像清晰度”游标图标。表示调节远程实时图像的清晰度。
	“Num Lock”（数字键盘开关）键的指示灯。表示当前服务器上“Num Lock”键的指示灯状态。
	“Caps Lock”（键盘大写锁定）键的指示灯。表示当前服务器上“Caps Lock”键的指示灯状态。
	“Scroll Lock”（键盘滚动锁定）键的指示灯。表示当前服务器上“Scroll Lock”键的指示灯状态。进入 Linux 字符模式，如果按下了 Ctrl+s（大多数情况下属于误按），此时屏幕会锁住，按下键盘上的“Scroll Lock”键可以解锁屏幕。 说明 - 通过 KVM 操作服务器时，如果键盘输入异常，请先检查 KVM 中服务器键盘指示灯状态是否正确。 “Scroll Lock”键的指示灯需要操作系统支持才能点亮，某些操作系统可能无法点亮。
	“帮助”按钮。表示查看 KVM 页面联机帮助。
注：不同型号的服务器，提供的功能不完全相同，请以实际界面为准。	

以光驱为例，工具栏中的镜像文件、虚拟光驱和虚拟软驱的使用流程如图 5-73 所示。

图5-73 使用流程



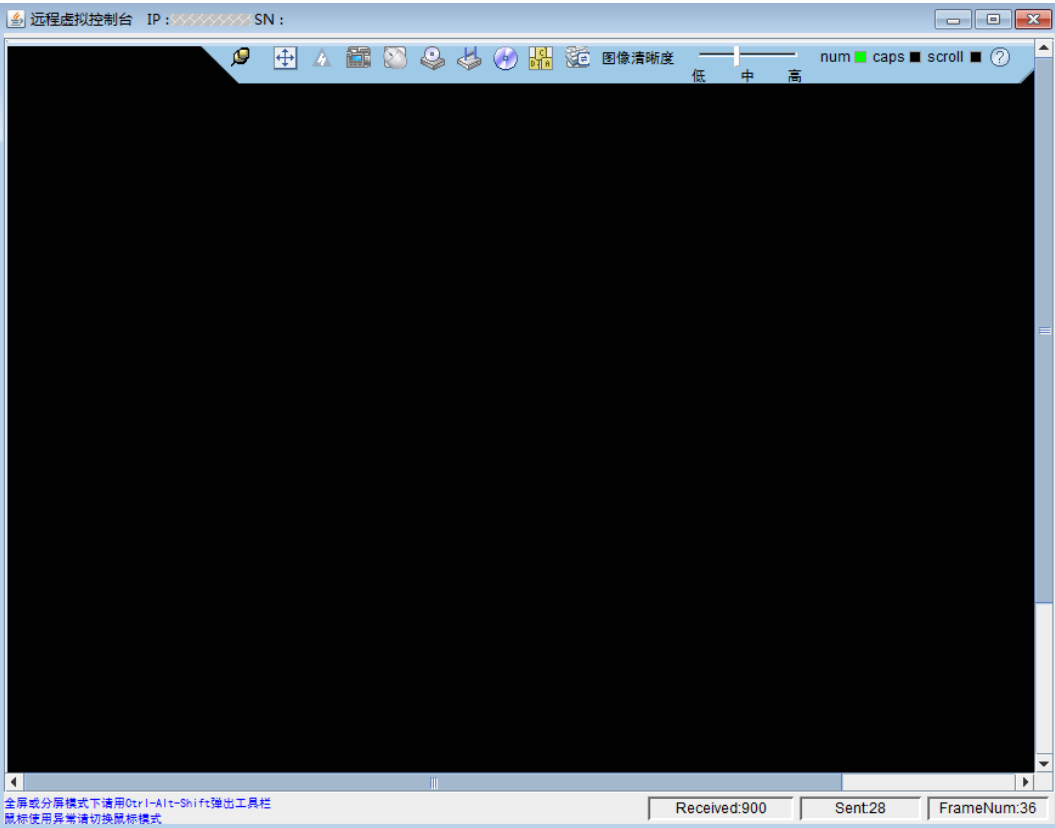
界面描述

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

说明

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

图5-74 Java KVM



Java KVM 窗口各区域的功能介绍如表 5-75 Java KVM 所示。

表5-75 Java KVM

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

操作步骤

发送特殊组合键

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出组合键窗口。

步骤 2 根据表 5-74 按钮说明提供的参数信息，单击需要发送的组合键。

服务器将执行组合键对应的操作。

说明

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

----结束

指定客户端的键盘类型

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

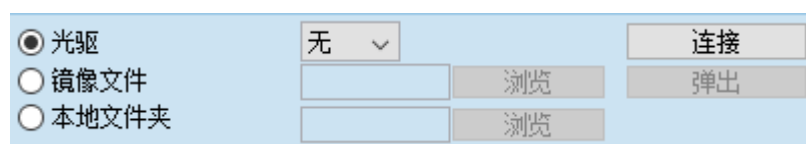
挂载虚拟光驱

本操作使用本地 PC 上的光盘驱动器虚拟出另一个光盘驱动器提供给服务器。

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出如图 5-75 所示的界面。

图5-75 挂载虚拟光驱



步骤 2 选中“光驱”单选按钮。

步骤 3 在下拉列表中，选择本地 PC 上待虚拟的光盘驱动器，例如“G:”。

步骤 4 单击“连接”。

服务器上成功挂载虚拟光驱。

说明

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

----结束

通过虚拟光驱挂载镜像文件

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

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出如图 5-76 所示的界面。

图5-76 挂载虚拟光驱



步骤 2 选中“镜像文件”单选按钮。

步骤 3 单击“浏览”。

弹出“打开”窗口。

步骤 4 选择本地 PC 上存放的光盘镜像文件，单击“打开”。

返回如图 5-76 所示的界面。

步骤 5 单击“连接”。

服务器上成功挂载镜像文件。

 说明

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

----结束

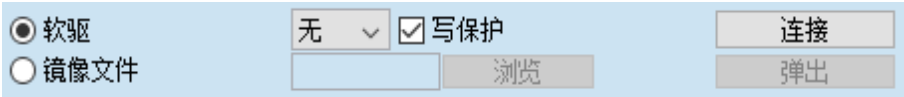
挂载虚拟软驱

本操作使用本地 PC 上的软驱或软盘镜像文件虚拟出另一个软驱提供给服务器。

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出如图 5-77 所示的界面。

图5-77 挂载虚拟软驱



步骤 2 选中“软驱”单选按钮。

步骤 3 在下拉列表中，选择本地 PC 上待虚拟的软盘驱动器，例如“A:”。

步骤 4 勾选“写保护”复选框。

说明

写保护是指软驱禁止写入数据。它是一种防止重要数据被更改或被删除的保护机制。

步骤 5 单击“连接”。

服务器上成功挂载虚拟软驱。

说明

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

----结束

通过虚拟软驱挂载镜像文件

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

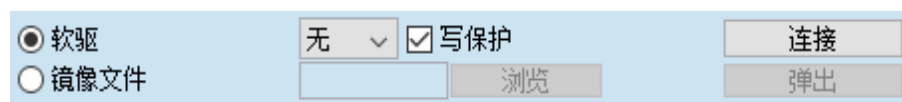
说明

挂载的镜像文件大小必须为 1.44MB，否则会导致挂载失败。

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出如图 5-78 所示的界面。

图5-78 挂载虚拟软驱



步骤 2 选中“镜像文件”单选按钮。

步骤 3 单击“浏览”。

弹出“打开”窗口。

步骤 4 选择本地 PC 上存放的软盘镜像文件，单击“打开”。

返回如图 5-78 所示的界面。

步骤 5 单击“连接”。

服务器上成功挂载镜像文件。

说明

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

----结束

制作镜像文件

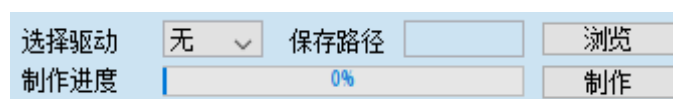
本操作使用软驱或光驱中的软盘或光盘制作镜像文件。制作成功的镜像文件保存在本地 PC 上。它可以用于挂载和加载虚拟软驱或光驱。

执行本操作前请确保本地 PC 上的软驱或光驱中已插入了软盘或光盘。

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出如图 5-79 所示的界面。

图5-79 制作镜像文件



步骤 2 在“选择驱动”下拉列表中，选择客户端的软盘驱动器或光盘驱动器。

步骤 3 单击“浏览”。弹出“保存”窗口。

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

说明

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

步骤 5 单击“保存”。

返回如图 5-79 所示的界面。

步骤 6 单击“制作”。

制作完成后，系统弹出窗口提示成功制作镜像文件。

在“制作进度”一栏将显示镜像文件的制作百分比。

说明

制作过程中，单击“停止”可以终止制作镜像文件。

----结束

挂载虚拟文件夹

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

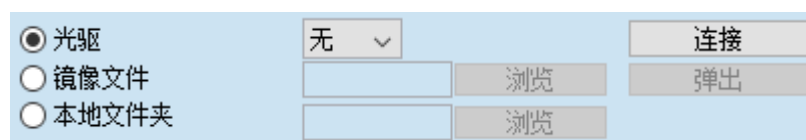
须知

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

步骤 1 在“KVM”界面中，单击工具栏上的。

弹出如图 5-80 所示的界面。

图5-80 挂载虚拟文件夹



步骤 2 选中“本地文件夹”单选按钮。

步骤 3 单击“浏览”。

打开本地文件夹选择窗口。

步骤 4 选择要挂载的本地文件夹，单击“打开”。

步骤 5 单击“连接”。

说明

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

---结束

为服务器上电

步骤 1 在“KVM”界面中，单击工具栏上的，在快捷菜单中选择“上电”。

弹出“选择一个选项”对话框。

步骤 2 单击“确定”。

服务器开始上电。

说明

服务器上电的时间根据服务器配置所不同。

---结束

为服务器下电

须知

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

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

弹出“选择一个选项”对话框。

步骤 2 单击“确定”。

服务器开始下电。

----结束

强制重启或强制下电再上电

须知

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

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

弹出“选择一个选项”对话框。

步骤 2 单击“确定”。

服务器开始强制重启或强制下电再上电。

说明

服务器强制重启或强制下电再上电的时间根据服务器配置所不同。

----结束

键鼠复位

本操作模拟插拔 USB 键盘和 USB 鼠标。

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

弹出“选择一个选项”对话框。

步骤 2 单击“确定”。

服务器开始执行 USB 复位操作。

----结束

为实时桌面录像

本操作对当前远程虚拟控制台显示的画面进行录像。

说明

开启录像功能后，自动录像功能有可能录制到业务侧的敏感信息，请注意安全风险。

步骤 1 在“KVM”界面中，单击工具栏上的.

弹出“选择一个选项”对话框。

步骤 2 单击“确定”。

弹出“保存”窗口。

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

步骤 4 单击“保存”。

返回“KVM”界面并开始录制录像。

步骤 5 录制完成后，单击.

弹出“选择一个选项”对话框。

步骤 6 单击“确定”。

录像文件被保存到指定的路径。

录制的录像文件格式为“*.rep”。可在“录像回放”界面中播放录像文件。

----结束

使用单鼠标

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

步骤 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。

步骤 2 单击“确定”。

“KVM”界面中只显示实时桌面上的鼠标。

----结束

加速远程鼠标

本操作对实时桌面上的鼠标进行加速，使其与本地 PC 上的鼠标同步。

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

弹出“选择一个选项”对话框。

步骤 2 单击“确定”。

同步本地 PC 与服务器的鼠标。

----结束

5.9 远程虚拟控制台异常帮助

5.9.1 打开 HTML5 集成远程控制台后显示设置信任证书超时

问题现象

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

解决方案

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

- 是=> [步骤 2](#)
- 否=> [步骤 3](#)

步骤 2 重新生成证书并替换原有证书。

步骤 3 重启 BMC。

步骤 4 重新打开 HTML5 集成远程控制台，查看是否可以正常开启。

- 是=> 处理完毕
- 否=> [步骤 5](#)

步骤 5 请联系技术支持处理。

----结束

5.9.2 无法启动 Java 集成远程控制台

问题现象

问题描述	可能原因
无法启动 Java 集成远程控制台。	- 没有正确安装 JRE。 - JRE 版本与 BMC 不兼容。

解决方案

步骤 1 确认客户端 JRE 已正确安装。

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

- 若 JRE 版本正确，请联系技术支持定位。
- 若 JRE 版本不正确，执行[步骤 2](#)。

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

步骤 3 安装 AdoptOpenJDK。

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

步骤 4 登录 BMC WebUI，在“首页”的“虚拟控制台”区域，单击“启动虚拟控制台 > Java 集成远程控制台(独占)或 Java 集成远程控制台(共享)”。

在此过程中，会自动下载 .jnlp 文件。

步骤 5 打开 .jnlp 文件。

说明

.jnlp 文件具有时效性，如果无法使用请参见[步骤 4](#)重新下载 .jnlp 文件。

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

----结束

5.9.3 打开远程虚拟控制台时鼠标键盘失效

问题现象

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

解决方案

步骤 1 检查服务器是否配置了 LSISAS3108 RAID 控制卡。

可通过“部件信息”界面查询。

- 是 => [步骤 2](#)
- 否 => [步骤 4](#)

步骤 2 检查“远程控制台”界面的“虚拟键鼠持续连接”是否开启。

- 是 => [步骤 4](#)
- 否 => [步骤 3](#)

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

- 是 => 处理完毕
- 否 => [步骤 4](#)

步骤 4 请联系技术支持处理。

---结束

5.9.4 打开 KVM 后显示与管理系统连接失败

问题现象

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

解决方案

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

- 是=> [步骤 2](#)
- 否=> [步骤 3](#)

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

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

- 是=> [步骤 5](#)
- 否=> [步骤 4](#)

步骤 3 开启 KVM 服务，并重新连接 KVM 查看是否可以连接。

- 是=> 处理完毕
- 否=> [步骤 2](#)

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

- 是=> 处理完毕
- 否=> [步骤 5](#)

步骤 5 请联系技术支持处理。

----结束

5.10 一键收集信息说明

说明

BMC V3.02.00.03 及以上版本不支持 MD5 类型的完整性校验码。

表5-76 一键收集信息说明

收集项文件	收集项文件内容说明
dump\dump_info	
dump_app_log	BMC 收集结果列表
dump_log	一键收集结果列表
dump\dump_info\3rdDump	
access_log	Nginx 访问日志
access_log.1	Nginx 访问日志备份文件
error_log	Nginx 错误日志
error_log.1	Nginx 错误日志备份文件
nginx.conf	Nginx 基础配置文件

收集项文件	收集项文件内容说明
nginx_http_server.conf	Nginx http server 配置文件
nginx_https_server.conf	Nginx https server 配置文件
nginx_https_server_ext.conf	Nginx 扩展配置文件
nginx_https_default_server_ext.conf	Nginx https default server 扩展配置文件
nginx_ssl_ciphersuite.conf	Nginx https 协议加密套件配置文件
nginx_ssl_protocol.conf	Nginx https 协议版本配置文件
nginx_ssl_verify_client.conf	Nginx 双因素认证配置文件
dump\dump_info\AppDump	
agentless	
agentless_dfl.log	Agentless 模块管理对象的信息
BIOS	
BIOS_dfl.log	BIOS 模块管理对象的信息
bios_info	BIOS 配置信息
currentvalue.json	当前设置的 BIOS 项
registry.json	BIOS 的注册文件，显示所有的 BIOS 项信息
result.json	通过 redfish 设置的 BIOS 项结果
setting.json	通过 redfish 设置但尚未生效的 BIOS 项
BMC	
BMC_dfl.log	BMC 模块管理对象的信息
fruinfo.txt	FRU 电子标签信息
lldp_info.txt	LLDP 配置及报文统计信息
nandflash_info.txt	NAND flash 信息
net_info.txt	网口配置信息
ntp_info.txt	NTP 同步失败时的错误信息
psu_info.txt	服务器上配置的电源信息
time_zone.txt	BMC 时区信息
card_manage	
card_info	服务器上配置的扣卡信息
card_manage_dfl.log	Card_Manage 模块管理对象的信息

收集项文件	收集项文件内容说明
sdi_card_cpld_info	SDI V3 卡 的 CPLD 寄存器信息 说明 只有适配且已正确安装了 SDI V3 卡的产品支持收集此信息。
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	
cpu_info	服务器配置的 CPU 参数的详细信息
CpuMem_dfl.log	CpuMem 模块管理对象的信息
mem_info	服务器配置的内存参数的详细信息
npu_info	服务器配置的 NPU 参数的详细信息
npu_ecc_info.json	服务器配置的 NPU ECC（Error Correcting Code）的详细信息
ddns	
ddns_dfl.log	Ddns 模块管理对象的信息
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
Dft	
Dft_dfl.log	DFT 模块管理对象的信息
diagnose	
diagnose_dfl.log	Diagnose 模块管理对象的信息
diagnose_info	Port 80 的故障诊断信息以及 IFMM 模块内存占用信息 说明 当前暂不支持收集此项信息。
discovery	
discovery_dfl.log	Discovery 模块管理对象的信息
FileManage	

收集项文件	收集项文件内容说明
FileManage_dfl.log	FileManage 模块管理对象的信息
ipmi_app	
ipmbeth_info.txt	管理系统的 IPMI 通道状态
ipmi_app_dfl.log	IPMI 模块管理对象的信息
kvm_vmm	
kvm_vmm_dfl.log	KVM_VMM 模块管理对象的信息
LicenseMgnt	
alm_protected.persist	License 管理组件 ALM 的持久化文件
first_protected.persist	License 管理组件 ALM 的持久化文件
LicenseMgnt_dfl.log	管理对象信息
lm_info	License 的状态、设备 ESN 等信息
second_protected.persist	License 管理组件 ALM 的持久化文件
MaintDebug	
MaintDebug_dfl.log	MaintDebug 模块管理对象的信息
net_nat	
net_nat_dfl.log	Net_NAT 模块管理对象的信息
PcieSwitch	
PcieSwitch_dfl.log	PCieSwitch 模块管理对象的信息
RetimerRegInfo	Retimer 芯片寄存器信息
PowerMgnt	
power_statistics.csv	功率统计信息
PowerMgnt_dfl.log	PowerMgnt 模块管理对象的信息
redfish	
component_uri.json	部件 URI 列表
redfish_dfl.log	Redfish 模块管理对象的信息
rimm	
rimm_dfl.log	RIMM 模块管理对象的信息
sensor_alarm	
current_event.txt	服务器当前健康状态和告警事件

收集项文件	收集项文件内容说明
LedInfo	服务器当前 LED 灯的显示状态
sel.db	sel 数据库文件
sel.tar	当前 sel 信息和历史 sel 信息打包文件
sensor_alarm_dfl.log	Sensor_Alarm 模块管理对象的信息
sensor_alarm_sel.bin	sel 原始记录文件
sensor_alarm_sel.bin.bak	sel 原始记录备份文件
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.bak.sha256	sel 原始记录备份文件完整性校验码
sensor_alarm_sel.bin.md5	sel 原始记录文件完整性校验码
sensor_alarm_sel.bin.sha256	sel 原始记录文件完整性校验码
sensor_alarm_sel.bin.tar.gz	sel 历史记录打包文件
sensor_info.txt	服务器所有传感器信息列表
Snmp	
Snmp_dfl.log	Snmp 模块管理对象的信息
StorageMgnt	
RAID_Controller_Info.txt	当前 RAID 控制器/逻辑盘/硬盘的信息
StorageMgnt_dfl.log	StorageMgnt 模块管理对象的信息
switch_card	
phy_register_info	后插板 phy 寄存器信息
port_adapter_info	后插板接口器件信息
switch_card_dfl.log	Switch_Card 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	BMC 相关器件的版本信息
User	
User_dfl.log	User 模块管理对象的信息
dump\dump_info\BMALogDump	
bma_debug_log bma_debug_log.1.gz bma_debug_log.2.gz	BMA 日志

收集项文件	收集项文件内容说明
bma_debug_log.3.gz	
dump\dump_info\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。
dump\dump_info\RTOSDump	
sysinfo	
cmdline	BMC 内核的命令行参数
cpuinfo	BMC 内核的 CPU 芯片信息
devices	BMC 系统的设备信息
df_info	BMC 分区空间的使用信息
diskstats	BMC 的磁盘信息
filesystems	BMC 的文件系统信息
free_info	BMC 的内存使用概况
interrupts	BMC 的中断信息
ipcs_q	BMC 的进程队列信息
ipcs_q_detail	BMC 的进程队列详细信息
ipcs_s	BMC 的进程信号量信息
ipcs_s_detail	BMC 的进程信号量详细信息
loadavg	BMC 系统运行负载情况
locks	BMC 内核锁住的文件列表
meminfo	BMC 的内存占用详细信息
modules	BMC 的模块加载列表
mtd	BMC 的配置分区信息
partitions	BMC 所有设备分区信息
ps_info	ps -elf BMC 进程详细信息
slabinfo	BMC 内核内存管理 slab 信息
stat	BMC 的 CPU 利用率
top_info	top -bn 1

收集项文件	收集项文件内容说明
	显示当前 BMC 进程运行情况
uname_info	uname -a 显示当前 BMC 内核版本
uptime	BMC 系统运行时间
version	BMC 当前的 RTOS 版本
vmstat	BMC 虚拟内存统计信息
versioninfo	
bmc_revision.txt	BMC 版本编译节点信息
app_revision.txt	BMC 版本信息
build_date.txt	BMC 版本构建时间
fruinfo.txt	FRU 电子标签信息
RTOS-Release	RTOS 版本信息
RTOS-Revision	RTOS 版本标记号
server_config.txt	服务器当前的配置信息
networkinfo	
ifconfig_info	网络信息，执行 ifconfig 的结果
ipinfo_info	BMC 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
netstat_info	netstat -an

收集项文件	收集项文件内容说明
	显示当前网络端口、连接使用情况
route_info	route 显示当前路由信息
services	服务端口信息
other_info	
extern.conf	BMC 日志文件配置
remotelog.conf	syslog 定制配置文件
ssh	SSH 服务配置
sshd_config	SSHD 服务配置文件
logrotate.status	logrotate 状态记录文件
login	login PAM 登录规则
sshd	SSH PAM 登录规则
pam_tally2	登录 BMC 失败的锁定规则
datafs_log	data 检测日志
ntp.conf	NTP 服务配置
vsftpd	FTP PAM 登录规则
driver_info	
dmesg_info	系统启动信息，执行 dmesg 的结果
lsmod_info	当前加载驱动模块信息
kbox_info	kbox 信息
edma_drv_info	edma 驱动信息
cdev_drv_info	字符设备驱动信息
veth_drv_info	虚拟网卡驱动信息
dump\dump_info\DeviceDump	
i2c_info	
*_info	I2C 设备的寄存器/存储区信息
dump\dump_info\LogDump	
M3LogDump	
m3_log m3_log.1	M3 安全启动及校验日志

收集项文件	收集项文件内容说明
.....	
netcard	
netcard_info.txt netcard_info_bk.txt	网卡配置信息
pciecard	
dump\dump_info\LogDump	
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
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
pid_log.txt pid_log1.tar.gz pid_log2.tar.gz	所有 pid 调试日志
bmccom.dat	BMC 串口日志
cpu1_m7_log cpu1_m7_log.tar.gz	CPU1 的 M7 协处理器运行日志（仅针对支持 M7 协处理器的服务器）
kunpeng_dfx_reg_log kunpeng_dfx_reg_log.tar.gz acsend_dfx_reg_log ascend_dfx_reg_log.tar.gz	dfx 寄存器信息
cpu2_m7_log cpu2_m7_log.tar.gz	CPU2 的 M7 协处理器运行日志（仅针对支持 M7 协处理器的服务器）
fdm.bin fdm.bin.tar.gz	FDM 原始故障日志
fdm_log fdm_log.tar.gz	FDM 日志
fdm_me_log fdm_me_log.tar.gz	ME 故障日志
fdm_mmio_log	FDM 板卡配置日志

收集项文件	收集项文件内容说明
fdm_mmio_log.tar.gz	
fdm_output fdm_output.1.gz fdm_output.2.gz fdm_output.3.gz	FDM 故障诊断日志
fdm_pfae_log	FDM 预告警日志
imu_log imu_log.tar.gz	IMU 运行日志（仅针对支持 IMU 模块的服务器）
ipmi_debug_log ipmi_debug_log.tar.gz	IPMI 模块日志
ipmi_mass_operate_log ipmi_mass_operate_log.tar.gz	IPMI 模块运行日志
kvm_vmm_debug_log kvm_vmm_debug_log.tar.gz	KVM 模块日志
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
maintenance_log maintenance_log.tar.gz	维护日志
mass_operate_log mass_operate_log.tar.gz operate_log operate_log.tar.gz	用户操作日志
ps_black_box.log ps_black_box.log.1.gz ps_black_box.log.2.gz ps_black_box.log.3.gz	电源黑匣子日志
remote_log remote_log.1.gz	syslog test 操作日志、sel 日志
security_log security_log.1	安全日志

收集项文件	收集项文件内容说明
strategy_log strategy_log.tar.gz	运行日志
third_party_file_bak.log	第三方文件备份日志记录
dump\dump_info\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_dhclient_ip.conf	DHCP 配置文件
BMC_dhclient_ip.conf.md5	完整性校验码
BMC_dhclient_ip.conf.sha256	完整性校验码
BMC_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.md5	完整性校验码
BMC_dhclient6_ip.conf.sha256	完整性校验码
BMC_HOSTNAME	BMC 主机名
BMC_HOSTNAME.md5	完整性校验码
BMC_HOSTNAME.sha256	完整性校验码
cpu_utilise_webview.dat	CPU 利用率曲线数据
CpuMem_cpu_utilise	服务器 CPU 利用率
CpuMem_mem_utilise	服务器内存利用率
env_web_view.dat	环境温度曲线数据
eo.db	SEL 数据库

收集项文件	收集项文件内容说明
fsync_reg.ini	文件同步配置文件
lost+found	文件夹
md_so_maintenance_log md_so_maintenance_log.tar.gz	维护日志
md_so_operate_log md_so_operate_log.tar.gz md_so_mass_operate_log md_so_mass_operate_log.tar.gz	操作日志
md_so_operate_log.sha256	完整性校验码
md_so_strategy_log md_so_strategy_log.tar.gz	策略日志
md_so_strategy_log.md5	完整性校验码
md_so_strategy_log.sha256	完整性校验码
memory_webview.dat	管理对象运行信息
NPU1-1_hbm_webview.dat NPU1-2_hbm_webview.dat NPU2-1_hbm_webview.dat NPU2-2_hbm_webview.dat NPU3-1_hbm_webview.dat NPU3-2_hbm_webview.dat NPU4-1_hbm_webview.dat NPU4-2_hbm_webview.dat	NPU 温度曲线数据
per_config.ini	BMC 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	BMC 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	BMC 配置持久化文件
per_config_reset.ini.bak	BMC 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

收集项文件	收集项文件内容说明
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	BMC 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	BMC 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	BMC 配置持久化文件
per_def_config_reset.ini.bak	BMC 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	BMC 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	BMC 配置持久化文件
per_reset.ini.bak	BMC 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
PowerMgmt_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

收集项文件	收集项文件内容说明
sel_db_sync	SEL 数据库同步锁
semid	进程信号量 id 文件夹
sensor_alarm_sel.bin	SEL 原始记录文件
sensor_alarm_sel.bin.md5	完整性校验码
sensor_alarm_sel.bin.sha256	完整性校验码
sensor_alarm_sel.bin.tar.gz	SEL 历史记录打包文件
Snmp_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
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
up_cfg	升级配置文件夹
User_login	login PAM 登录规则
User_login.md5	完整性校验码
User_login.sha256	完整性校验码
User_sshd	SSH PAM 登录规则
User_sshd.md5	完整性校验码
User_sshd.sha256	完整性校验码
User_sshd_config	SSH 配置文件
User_sshd_config.md5	完整性校验码
User_sshd_config.sha256	完整性校验码
User_vsftpd	FTP PAM 登录规则

收集项文件	收集项文件内容说明
User_vsftp.md5	完整性校验码
User_vsftp.sha256	完整性校验码
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_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_dhclient6.conf.bak	DHCP 配置备份文件
BMC_dhclient6.conf.bak.md5	完整性校验码
BMC_dhclient6.conf.bak.sha256	完整性校验码
BMC_dhclient6.conf.md5	完整性校验码
BMC_dhclient6.conf.sha256	完整性校验码
BMC_dhclient6_ip.conf.bak	DHCP 配置备份文件
BMC_dhclient6_ip.conf.bak.md5	完整性校验码
BMC_dhclient6_ip.conf.bak.sha256	完整性校验码
BMC_dhclient6_ip.conf.md5	完整性校验码
BMC_dhclient6_ip.conf.sha256	完整性校验码
BMC_HOSTNAME.bak	主机名配置备份文件

收集项文件	收集项文件内容说明
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
eo.db	SEL 数据库
eo.db.sha256	完整性校验码
eo.db.sha256_backup	完整性校验码
eo.db_backup	SEL 数据库
md_so_operate_log.bak	操作日志
md_so_operate_log.bak.md5	完整性校验码
md_so_operate_log.bak.sha256	完整性校验码
md_so_operate_log.md5	完整性校验码
md_so_operate_log.sha256	完整性校验码
md_so_strategy_log.bak	策略日志
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	BMC 配置持久化文件
per_config.ini.bak	BMC 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	BMC 配置持久化文件
per_def_config.ini.bak	BMC 配置持久化文件
per_def_config.ini.bak.md5	完整性校验码

收集项文件	收集项文件内容说明
per_def_config.ini.bak.sha256	完整性校验码
per_def_config.ini.md5	完整性校验码
per_def_config.ini.sha256	完整性校验码
per_power_off.ini	BMC 配置持久化文件
per_power_off.ini.bak	BMC 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
PowerMgmt_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
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

收集项文件	收集项文件内容说明
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
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
dump\dump_info\OSDump	

收集项文件	收集项文件内容说明
*.rep	业务侧屏幕自动录像文件 说明 如果录像文件大小超过 21MB，建议下载并保存到本地 PC。否则，在进行一键收集信息时，BMC 会删除超过 21MB 的录像文件。
img*.jpeg	业务侧最后一屏图像
systemcom.tar	SOL 串口信息
video_catererror_rep_is_deleted.info	删除过大的 catererror 录像的提示
dump\dump_info\Register	
cpld_reg_info	CPLD 寄存器信息
cpu_reg_info	CPU 寄存器信息
vrld_reg_info	VRD 寄存器信息
dump\dump_info\SpLogDump	
config	配置导出备份文件 说明 - SP 运行过程中无法收集此日志。 - SP 运行配置导出功能后可收集该日志。
deviceinfo.json	服务器资产信息 说明 SP 运行过程中无法收集此日志。
diagnose	硬件诊断日志 说明 - SP 运行过程中无法收集此日志。 - SP 运行配置导出功能后可收集该日志。
dmesg.log	小系统 dmesg 日志 说明 SP 运行过程中无法收集此日志。
filepatchup_debug.log	极速部署文件打包日志 说明 - SP 运行过程中无法收集此日志。 - SP 运行极速部署功能后可收集该日志。
images.log	极速部署克隆日志 说明 - SP 运行过程中无法收集此日志。 - SP 运行极速部署功能后可收集该日志。

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

6 CLI 介绍

介绍如何登录 BMC 命令行，以及 BMC 支持的命令。

- 6.1 CLI 说明
- 6.2 登录 CLI
- 6.3 BMC 命令
- 6.4 Trap 命令
- 6.5 Syslog 命令
- 6.6 VNC 命令
- 6.7 服务器命令
- 6.8 系统命令
- 6.9 用户管理命令
- 6.10 NTP 命令
- 6.11 指示灯命令
- 6.12 风扇命令
- 6.13 传感器命令
- 6.14 电源命令
- 6.15 SOL 命令
- 6.16 常用维护命令

6.1 CLI 说明

6.1.1 格式说明

BMC 管理软件常用命令有以下命令：

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

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

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

对命令行格式的约定请参见表 6-1 命令行格式的约定。

表6-1 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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 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。

6.1.2 帮助

BMC 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。

说明

通过按 **↑** 键可以显示输入的历史命令，系统会将用户名、口令、密钥等敏感信息脱敏处理，显示为*。

例如：

查询命令：


```

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

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

  -d <dataitem>
    faninfo             Get fan mode and the percentage of the fan speed
    port80              Get the diagnose code of port 80
    diaginfo            Get diagnostic info of management subsystem
    systemcom           Get system com data
    blackbox            Get black box data
    bootdevice          Get boot device
    shutdowntimeout     Get graceful shutdown timeout state and value
    powerstate          Get power state
    health              Get health status
    healthevents        Get health events
    sel                 Print System Event Log (SEL)
    operatelog          Print operation log
    version             Get BMC 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
    minimumpasswordage  Get minimum password age configuration
    ntpinfo             Get NTP information
    npuworkmode         Get NPU work mode
    npustatus           Get NPU isolation status
    notimeoutstate      Get CLI session notimeout state
    lldpinfo            Get LLDP information

```

设置命令:

```

BMC:/->ipmcset
Usage: ipmcset [-t target] -d dataitem [-v value]

  -t <target>
    fru0                Operate with fru0
    trap                Operate SNMP trap
    service             Operate with service
    user                Operate with user
    maintenance         Operate with maintenance
    sensor              Operate with sensor
    securitybanner      Operate login security banner information
    syslog              Operate syslog
    ntp                 Operate ntp
    vnc                 Operate vnc
    storage             Configure storage device
    config              Operate configuration
    vmm                 Operate virtual media
    certificate         Operate certificate
    sol                 Operate SOL
    securityenhance     Operate security enhance
    precisealarm        Operate with precise alarm
    lldp                Operate lldp

  -d <dataitem>
    fanmode             Set fan mode,you can choose manual or auto
    fanlevel            Set fanlevel
    reset               Reboot BMC system
    identify            Operate identify led
    upgrade             Upgrade component
    clearcmos           Clear CMOS
    bootdevice          Set boot device
    shutdowntimeout     Set graceful shutdown timeout state and value
    frucontrol          Fru control
    powerstate          Set power state
    sel                 Clear SEL
    adduser             Add user
    password            Modify user password
    deluser             Delete user
    privilege           Set user privilege
    npuworkmode         Set NPU work mode
    npuisolation        Set NPU isolation status
    serialdir           Set serial direction
    printscreen         Print current screen to BMC
    rollback            Perform a manual rollback
    timezone            Set time zone
    passwordcomplexity  Set password complexity check enable state
    ipaddr              Set ip address
    backupipaddr        Set backup ip address
    ipmode              Set ip mode
    gateway             Set gateway
    ipaddr6             Set ipv6 address
    ipmode6             Set ipv6 mode
    gateway6            Set ipv6 gateway
    netmode             Set net mode
    activeport          Set EthGroup active port
    vlan                Set sideband vlan

```

restore	Restore factory setting
notimeout	Set no timeout state
emergencyuser	Set emergency user
autodiscovery	Set autodiscovery configuration
poweronpermit	Set poweronpermit configuration
minimumpasswordage	Set minimum password age configuration
crl	Upload CRL file
psuworkmode	Set PSU work mode
fpgagoldenfwrestore	FPGA golden firmware restore

在输入错误参数的情况下，帮助信息会提示可选的正确参数。

例如：

```
BMC:/->ipmcset -d inff
Usage: ipmcset [-t target] -d dataitem [-v value]

-t <target>
    fru0          Operate with fru0
    trap          Operate SNMP trap
    service       Operate with service
    user          Operate with user
    maintenance   Operate with maintenance
    sensor        Operate with sensor
    securitybanner Operate login security banner information
    syslog        Operate syslog
    ntp           Operate ntp
    vnc           Operate vnc
    storage       Configure storage device
    config        Operate configuration
    vmm           Operate virtual media
    certificate    Operate certificate
    sol           Operate SOL
    securityenhance Operate security enhance
    precisealarm  Operate with precise alarm

-d <dataitem>
    fanmode       Set fan mode,you can choose manual or auto
    fanlevel      Set fan speed percent
    reset         Reboot BMC system
    identify      Operate identify led
    upgrade       Upgrade component
    clearcmos     Clear CMOS
    bootdevice    Set boot device
    shutdowntimeout Set graceful shutdown timeout state and value
    frucontrol    Fru control
    powerstate    Set power state
    sel           Clear SEL
    adduser       Add user
    password      Modify user password
    deluser       Delete user
    privilege     Set user privilege
    npuworkmode   Set NPU work mode
    serialdir     Set serial direction
    printscreen   Print current screen to BMC
    rollback      Perform a manual rollback
    timezone      Set time zone
```

passwordcomplexity	Set password complexity check enable state
ipaddr	Set ip address
backupipaddr	Set backup ip address
ipmode	Set ip mode
gateway	Set gateway
ipaddr6	Set ipv6 address
ipmode6	Set ipv6 mode
gateway6	Set ipv6 gateway
netmode	Set net mode
activeport	Set EthGroup active port
vlan	Set sideband vlan
restore	Restore factory setting
notimeout	Set no timeout state
emergencyuser	Set emergency user
autodiscovery	Set autodiscovery configuration
poweronpermit	Set poweronpermit configuration
minimumpasswordage	Set minimum password age configuration
crl	Upload CRL file
psuworkmode	Set PSU work mode
fpgagoldenfwrestore	FPGA golden firmware restore

6.2 登录 CLI

6.2.1 通过管理网口登录 CLI

本地用户和 LDAP 用户均可通过网口使用 SSH 方式登录 CLI。使用 LDAP 用户登录 CLI 时，需要保证 BMC 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。

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 CLI 时，请使用正确的加密算法。
- 系统最多允许 5 个用户同时登录 CLI。

前提条件

通过管理网口登录 CLI 之前，请使用网线将配置终端网口和服务器管理网口相连，并确保配置终端和服务器管理网口网络互通。

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 BMC。

操作步骤

- 步骤 1 在客户端下载符合 SSH 协议的通讯工具。
- 步骤 2 将客户端连接（直连或通过网络连接）到服务器管理网口。
- 步骤 3 配置客户端地址，使其可与服务器 BMC 管理网口互通。

步骤 4 在客户端打开 SSH 工具并配置相关参数（如 IP 地址）。

说明

- 系统缺省的 IP 地址为 192.168.2.100。
- 可通过 BIOS 系统查询和设置管理网口 IP 地址，具体请参见 [9.1 确认管理网口 IP 地址](#)。

步骤 5 连接到 BMC 后，输入用户名和密码。

如果用户首次登录 CLI，系统会强制用户修改登录密码，请妥善保管并定期更新登录密码。

----结束

6.2.2 通过串口登录 CLI

前提条件

通过串口登录 CLI 之前，请先通过串口线缆连接配置终端串口和服务器串口。

操作步骤

须知

通过串口登录 BMC CLI，必须保证机箱的系统串口已经切换为 BMC 串口。可以通过 SSH 登录命令行，执行 **ipmcset -d serialdir -v <option>** 命令切换串口。

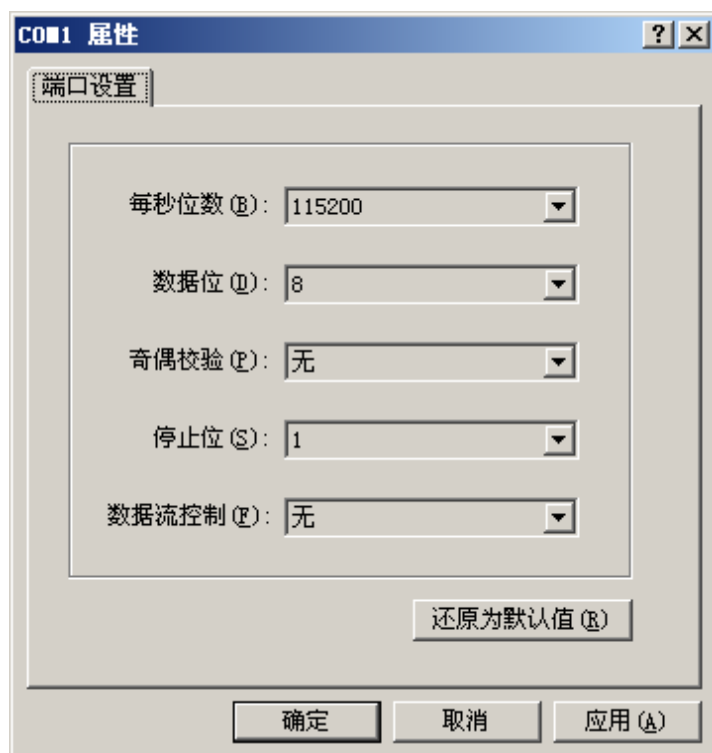
步骤 1 连接串口线。

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

参数设置如下图所示。

图6-1 超级终端属性设置



步骤 3 呼叫成功后输入用户名和密码。

说明

- 连续 5 次密码输入错误后，系统将会锁定该用户。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。
- 缺省情况下，CLI 超时时间为 15 分钟。

如果用户首次登录 CLI，系统会强制用户修改登录密码，请妥善保管并定期更新登录密码。

----结束

6.3 BMC 命令

6.3.1 查询 BMC 管理网口的 IP 信息 (ipinfo)

命令功能

ipinfo 命令用来查询 BMC 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 BMC 管理网口的 IP 信息。

```
BMC:/->ipmcget -d ipinfo
EthGroup ID      : 1
Net Mode         : Manual
Net Type         : LOM
Active Port      : eth2
IPv4 Information :
IP Mode          : static
IP Address       :
Subnet Mask      : 255.255.0.0
Default Gateway  : 192.168.0.1
Backup IP Address : 192.168.0.33 (Deactivated)
Backup Subnet Mask : 255.255.255.0 (Deactivated)
MAC Address      :
IPv6 Information :
IPv6 Mode        : static
IPv6 Address 1   : fc00:226::3:185/64
Default Gateway IPv6 : fc00:226::5
Link-Local Address : fe80::218:e1ff:fec5:d866/64
IPv6 Address 2   : fc00:226::218:e1ff:fec5:d866/64
VLAN Information :
NCSI Port VLAN State : disabled
Dedicated Port VLAN State : disabled
```

说明

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

6.3.2 设置 BMC 管理网口的 IPv4 信息（ipaddr）

命令功能

ipaddr 命令用于设置 BMC 管理网口的 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
<i>ipaddr</i>	表示要设置的 BMC 网口的 IPv4 地址。	数据类型为 IPv4，表示形式为 XXX.XXX.XXX.XXX。
<i>mask</i>	表示要设置的 BMC 网口的子网掩码。	数据类型为 IPv4，表示形式为 XXX.XXX.XXX.XXX。
<i>gateway</i>	表示要设置的 BMC 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 BMC 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。

```
BMC:/->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 BMC 管理网口的 IP 信息。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : dhcp
IPv6 Address     :
Default Gateway IPv6 :
Link-Local Address : fe80::218:e1ff:fec5:d866/64
VLAN Information  :
VLAN State       : disabled
```


6.3.3 设置 BMC 管理网口的备份 IPv4 信息 (backupipaddr)

命令功能

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

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

命令格式

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

参数说明

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

使用指南

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

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

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

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

使用实例

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

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

查询 BMC 管理网口的 IP 信息。

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

6.3.4 设置 BMC 管理网口的 IPv4 模式（ipmode）

命令功能

ipmode 命令用于设置 BMC 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
<i>dhcp</i>	表示地址模式为 dhcp	-
<i>static</i>	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 BMC 管理网口为 dhcp 模式。

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

查询修改后的 BMC 管理网口 IP 信息。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : dhcp
IPv6 Address     :
Default Gateway IPv6 :
Link-Local Address : fe80::218:elff:fec5:d866/64
VLAN Information :
VLAN State       : disabled
```

 说明

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

6.3.5 设置 BMC 管理网口的 IPv4 网关（gateway）

命令功能

gateway 命令用来设置 BMC 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
<i>gateway</i>	表示 BMC 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 BMC 管理网口的网关为 192.168.0.1。

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

查询设置后的网关地址信息。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : dhcp
IPv6 Address     :
Default Gateway IPv6 :
Link-Local Address : fe80::218:elff:fec5:d866/64
VLAN Information :
VLAN State       : disabled
```

6.3.6 设置 BMC 管理网口的 IPv6 信息（ipaddr6）

命令功能

ipaddr6 命令用于设置 BMC 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
<i>ipaddr6</i>	表示要设置的 BMC 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。
<i>prefixlen</i>	表示要设置的 BMC 网口的子网前缀长度。	0~128。
<i>gateway6</i>	表示要设置的 BMC 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。

参数	参数说明	取值
		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 BMC。
- 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 BMC 管理网口的 IPv6 地址为 `fc00::6516`，子网前缀为 `64`，网关地址为 `fc00::1`。

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

查询修改后的 BMC 管理网口的 IP 信息。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : static
IPv6 Address     : fc00::6516
Default Gateway IPv6 : fc00::1
Link-Local Address : fe80::218:elff:fec5:d866/64
VLAN Information :
VLAN State       : disabled
```

6.3.7 设置 BMC 管理网口的 IPv6 模式（ipmode6）

命令功能

ipmode6 命令用于设置 BMC 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
<i>dhcp</i>	表示地址模式为 dhcp	-
<i>static</i>	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 BMC 管理网口为 dhcp 模式。

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

查询修改后的 BMC 管理网口 IP 信息。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : dhcp
IPv6 Address     :
Default Gateway IPv6 :
Link-Local Address : fe80::218:elff:fec5:d866/64
VLAN Information  :
VLAN State       : disabled
```

6.3.8 设置 BMC 管理网口的 IPv6 网关（gateway6）

命令功能

gateway6 命令用来设置 BMC 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
<i>gateway6</i>	表示 BMC 网口的 IPv6 网关地址。	数据类型为 IPv6，表示形式为 <i>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</i> 。当多个 <i>xxxx</i> 连续为 0 时，表现形式可缩写为 <i>xxxx::xxxx</i> 。例如： <i>fc00:0000:000:0000:0000:0000:0000:0001</i> 可缩写为 <i>fc00::0001</i> 。 在一个 IPv6 中，只能使用一个缩写。

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 BMC 管理网口的 IPv6 网关为 *fc00::1*。

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

查询设置后的网关地址信息。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : static
IPv6 Address     : fc00::65
Default Gateway IPv6 : fc00::1
Link-Local Address : fe80::218:elff:fec5:d866/64
VLAN Information :
VLAN State       : disabled
```

6.3.9 设置管理网口模式（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
<i>option</i>	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 BMC 专有网口进行适配, 如果 BMC 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。

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

查询网口模式。

```
BMC:/->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      :
IPv6 Information :
IPv6 Mode        : static
IPv6 Address     : fc00::65
Default Gateway IPv6 : fc00::1
Link-Local Address : fe80::218:elff:fec5:d866/64
VLAN Information :
VLAN State       : disabled
```


6.3.10 设置激活端口（activeport）

命令功能

activeport 命令用于设置 BMC 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
<i>option</i>	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。
<i>portid</i>	激活端口编号	配置双端口网卡时，取值为 1、2；配置四端口网卡时，取值为 1~4。

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 BMC 激活端口为专用网口。

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

查询 BMC 端口信息。

```
BMC:/->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      :
IPv6 Information :
```

```
IPv6 Mode          : static
IPv6 Address       : fc00::65
Default Gateway IPv6 : fc00::1
Link-Local Address  : fe80::218:eff:fec5:d866/64
VLAN Information    :
VLAN State         : disabled
```

6.3.11 设置管理网口 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	取值范围：1~4094
port type	BMC VLAN 功能生效的网口类型。	0：NC-SI shared port 1：Dedicated port 默认值：0

使用指南

-

使用实例

#设置网口 VLAN 为 405。

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

查询网口 VLAN 信息。

```
BMC:/->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      :
IPv6 Information  :
IPv6 Mode        : static
IPv6 Address     : fc00::65
Default Gateway IPv6 : fc00::1
Link-Local Address : fe80::218:eff:fec5:d866/64
VLAN Information  :
VLAN State       : enabled
VLAN ID          : 405
```

6.3.12 查询和设置串口方向（serialdir）

命令功能

serialdir 命令用来查询和设置串口方向。

命令格式

```
ipmcget -d serialdir
ipmcset -d serialdir -v <option>
```

参数说明

参数	参数说明	取值
<option>	串口方向	• 0: 表示系统串口 • 1: 表示 BMC 串口 • 2: 表示 SOL 串口切换为系统串口 • 3: 表示 SOL 串口切换为 BMC 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

参数	参数说明	取值
		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 BMC 串口时，如果当前面板串口与 SOL 串口方向设置相同，同为系统串口或者 BMC 串口时，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

```
# 将串口设置为 BMC 串口。

BMC:/->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。

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

6.3.13 重启 BMC 管理系统（reset）

命令功能

reset 命令用来重启 BMC 管理系统。

命令格式

ipmcset -d reset

参数说明

无

使用指南

无

使用实例

重新启动 BMC 管理系统。

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

6.3.14 固件升级（upgrade）

命令功能

upgrade 命令用于升级固件。

命令格式

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

参数说明

参数	参数说明	取值
<i>filepath</i>	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”
<i>option</i>	表示升级完成后是否立即自动重启 BMC。	1：表示升级完成后立即自动重启 BMC。 0：表示升级完成后将不会自动重启 BMC。 默认值：1

使用指南

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

说明

- 文件上传时，不同用户上传的文件不能相互覆盖，即 A 用户删除其上传的文件后，B 用户才能上传同名文件。
- 如果操作系统上电，BIOS 升级文件会上传到 iBMC，并在下次操作系统下电或复位时生效。
- 文件路径的长度不应超过 255 个字符。

升级 BMC 或 SD 卡控制器后，需重启 BMC 才能使升级的固件生效。

升级 BMC 或 SD 卡控制器后：

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

升级 BMC 时会同时升级主、备分区镜像。

使用实例

升级软件。

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

或

```
BMC:/->ipmcset -d upgrade -v /tmp/image.hpm 0
Please make sure the BMC is working while upgrading!
Updating...
100%
Upgrade successfully and need to reboot the BMC to active the upgrade.
```

6.3.15 截屏命令（printscreen）

命令功能

printscreen 命令用于截取服务器当前所显示的屏幕图片。

命令格式

ipmcset -d printscreen [-v wakeup]

参数说明

参数	参数说明	取值
wakeup	截取屏幕图片的同时唤醒系统屏保	-

使用指南

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

 说明

多次执行 printscreen 命令时，BMC 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。

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

6.3.16 BMC 软件回滚（rollback）

命令功能

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

命令格式

ipmcset -d rollback

参数说明

无

使用指南

该命令生效后，原可用分区镜像切换为主分区镜像，原主分区同步新主分区镜像后切为备份分区镜像，原备分区镜像自动切换为可用分区镜像。

使用实例

回滚 BMC 软件。

```
BMC:/->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!
```

6.3.17 查询软件回滚状态（rollbackstatus）

命令功能

rollbackstatus 命令用来查询软件回滚状态。

命令格式

ipmcget -d rollbackstatus

参数说明

无

使用指南

无

使用实例

查询 BMC 软件回滚状态。

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

6.3.18 设置服务状态（service -d state）

命令功能

service -d state 命令用于设置 BMC 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
<i>option</i>	服务类型	• SSH • SNMP • KVM • VNC • VMM • Video • HTTP

参数	参数说明	取值
		• HTTPS • RMCP • RMCP+ • SSDP
enabled	启用服务	-
disabled	禁用服务	-

使用指南

输入 *option* 参数时，大小写均支持。

使用实例

启用 HTTP 服务。

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

 说明

开启 http 服务有安全隐患。

6.3.19 设置指定服务的端口号（service -d port）

命令功能

service -d port 命令用于设置 BMC 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
<i>option</i>	服务类型	• SSH • SNMP • KVM • VNC • VMM • Video

参数	参数说明	取值
		• HTTP • HTTPS • RMCP
<i>port1value</i>	服务的端口号	1~65535
<i>port2value</i>	服务的端口号，只有 RMCP 服务可以设置此端口	1~65535

使用指南

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

使用实例

设置 HTTPS 服务的端口号为 443。

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

6.3.20 查询服务状态（service -d list）

命令功能

service -d list 命令用于查询服务状态。

命令格式

```
ipmcget -t service -d list
```

参数说明

无

使用指南

无

使用实例

查询服务状态。

```
BMC:/->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

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

命令功能

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

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

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

命令功能

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

命令格式

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

参数说明

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

使用指南

无

使用实例

设置登录安全信息为默认内容。

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

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

命令功能

`securitybanner -d info` 命令用于查询 BMC 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。

```
BMC:/-> 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.
```

6.3.24 导入 SSL 证书（certificate -d import）

命令功能

certificate -d import 命令用于导入 SSL 证书到 BMC 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 BMC 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 - BMC 当前仅支持 SMB V1.0 版本。 - cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp 或 scp 协议。 - username: 登录目标服务器所需的用户名。 - password: 登录目标服务器所需的密码。 - IP:[port]: 目标服务器的 IP 地址和端口号。 - directory/filename: 远程 SSL 证书在目标服务器上的绝对路径。 例如： https://Administrator:Admin@9000@10.10.10.1:

参数	参数说明	取值
		443/tmp/test.pfx
<i>type</i>	SSL 证书类型	固定为 1。
<i>passphrase</i>	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 BMC 文件系统的指定目录下（例如"/tmp"）。

使用实例

```
# 导入 SSL 证书。

BMC:/-> ipmcset -t certificate -d import -v /tmp/test-01.pfx 1 Admin@9000
Import certificate successfully
```

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

命令功能

certificate -d info 命令用于查询 SSL 证书的信息。

命令格式

```
ipmcget -t certificate -d info
```

参数说明

无

使用指南

无

使用实例

```
# 查询 SSL 证书信息。

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

6.3.26 导出配置文件（config -d export）

命令功能

config -d export 命令用于导出 BMC、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
<i>filepath</i>	配置文件导出后的本地存放路径	BMC 系统中的路径，例如：“/tmp/config.xml”。
<i>file_URL</i>	配置文件导出后的远程存放路径	格式为： <i>protocol://[username:password@]IP:[port]/directory/filename</i> 其中： <i>protocol</i>：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 - BMC 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 <i>username:password@</i> 字段；使用其它协议时，存放路径中必须包含 <i>username:password@</i> 字段。 - cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 <i>username</i>：登录目标服务器所需的用户名。 <i>password</i>：登录目标服务器所需的密码。 <i>IP:[port]</i>：目标服务器的 IP 地址和端口号。 <i>directory/filename</i>：配置文件在目标服务器上的绝对路径。 例如： “https://Administrator:Admin@9000@10.10.10.1:443/tmp/config.xml”

使用指南

- 若设备不支持或未配置 RAID 控制器，则配置文件中不包含 RAID 控制器信息。

- 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。

```
BMC:/-> 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.
```

6.3.27 导入配置文件（config -d import）

命令功能

config -d import 命令用于导入 BMC、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 BMC 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 • BMC 当前仅支持 SMB V1.0 版本。 • 使用 nfs 协议时，存放路径中不能包含 username:password@ 字段；使用其它协议时，存放路径中必须包含 username:password@ 字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • username：登录目标服务器所需的用户名。 • password：登录目标服务器所需的密码。 • IP:[port]：目标服务器的 IP 地址和端口

参数	参数说明	取值
		号。 <i>directory/filename</i>: 配置文件在目标服务器上的绝对路径。 例如: https://Administrator:Admin@9000@10.10.10.1:443/tmp/config.xml

使用指南

- 若设备不支持或未配置 RAID 控制器，则配置文件中不包含 RAID 控制器信息。
- 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 BMC 文件系统的指定目录下（例如"/tmp"）。

使用实例

导入配置文件。

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

6.3.28 导入 CRL 文件（crl）

命令功能

crl 命令用于导入升级包完整性校验所使用的证书撤销列表文件。

命令格式

ipmcset -d crl -v <localpath/URL> <type>

参数说明

参数	参数说明	取值
<i>localpath</i>	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 BMC 上的绝对路径，例如： “/tmp/cms.crl”。
<i>URL</i>	待导入的远程 CRL 文件的 URL	格式为： <i>protocol://[username:password@]IP:[port]/directory/filename</i>

参数	参数说明	取值
		其中： • <i>protocol</i>：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 • BMC 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 <i>username:password@</i> 字段；使用其它协议时，存放路径中必须包含 <i>username:password@</i> 字段。 • cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 • <i>username</i>：登录目标服务器所需的用户名。 • <i>password</i>：登录目标服务器所需的密码。 • <i>IP:[port]</i>：目标服务器的 IP 地址和端口号。 • <i>directory/filename</i>：远程 CRL 文件在目标服务器上的绝对路径。 例如： “https://Administrator:Admin@9000@10.10.10.1:443/tmp/cms.crl”
<i>type</i>	CRL 文件类型	固定为 1。

使用指南

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

使用实例

导入 CRL 文件。

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

6.3.29 挂载文件到虚拟光驱（vmm -d connect）

命令功能

vmm -d connect 命令用于挂载文件到虚拟光驱。

命令格式

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

参数说明

参数	参数说明	取值
file_URL	待挂载的文件所在的远程路径。	格式为： protocol://[username:password@]IP[:port]/directory/filename 其中： - protocol：必须为“nfs”、“cifs”或“https”。 说明 - BMC 当前仅支持 SMB V1.0 版本。 - 使用 nfs 协议时，存放路径中不能包含 username:password@ 字段；使用其它协议时，存放路径中必须包含 username:password@ 字段。 - cifs 标准协议使用了不安全算法，建议优先选择更安全的 https 或 nfs 协议。 - username：登录目标服务器所需的用户名。 - password：登录目标服务器所需的密码。 - IP[:port]：目标服务器的 IP 地址和端口号。 - directory/filename：待挂载的文件在目标服务器上的绝对路径。 例如： nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso 或 nfs://[fc00::64]/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso 说明 - file_URL 的最大长度为 255 个字符。 - 使用 IPv6 地址挂载文件时，必须使用[]将其括起来，例如“[fc00::64]”，而 IPv4 地址无此限制。

使用指南

无

使用实例

挂载文件到虚拟光驱。

```
BMC:/-> 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.
```

6.3.30 中断虚拟光驱的连接（vmm -d disconnect）

命令功能

vmm -d disconnect 命令用于断开虚拟光驱的连接。

命令格式

ipmcset -t vmm -d disconnect

参数说明

无

使用指南

无

使用实例

中断虚拟光驱的连接。

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

6.3.31 查询虚拟媒体信息（vmm -d info）

命令功能

vmm -d info 命令用于查询 BMC 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。

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

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

命令功能

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

命令格式

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

参数说明

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

使用指南

FPGA 卡为正常状态时执行此命令，OS 将会重启。请谨慎操作。

使用实例

将 FPGA 卡的 Golden 固件恢复出厂设置。

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

```
100%
The restore of the Golden firmware of the FPGA card is successful.

或

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

6.4 Trap 命令

介绍服务器 trap 相关命令的查询和设置方法。

6.4.1 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 BMC 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
<i>destination</i>	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 BMC 的 SNMP trap 目标 1。

```
BMC:/->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。

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

6.4.2 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 BMC 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
<i>destination</i>	表示 SNMP trap 目标项。	1 ~ 4
<i>portvalue</i>	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。

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

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

命令功能

trap -d community 命令用于设置 BMC 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
<i>Community</i>	表示 SNMP trap 团体名称。	不开启密码检查时的取值原则： • 长度为 1～32 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 8～32 位的字符串。 • 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。

使用指南

无

使用实例

设置 SNMP trap 的团体名称为 mytrap。

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


6.4.4 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
<i>destination</i>	表示 SNMP trap 目标项。	1~4
<i>ipaddr</i>	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。

```
BMC:/->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。

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

6.4.5 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。

```
BMC:/->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	

6.4.6 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。

```
BMC:/->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。

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

6.4.7 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
<i>level</i>	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。

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

查询当前 SNMP trap 发送告警的级别。

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

6.4.8 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
<i>username</i>	表示 SNMP trap V3 用户。	已存在的用户名。

使用指南

需要管理工作站配置相同用户名、密码的用户。

默认情况下，Trap V3 使用“Administrator”用户。

使用实例

设置 SNMP trap V3 用户。

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

查询 SNMP trap V3 用户。

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

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

命令功能

trap -d mode 命令用于查询和设置 SNMP trap 模式。

命令格式

ipmcget -t trap -d mode

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

参数说明

参数	参数说明	取值
<i>option</i>	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，详细内容请参见随版本发布的《BMC SNMP 接口说明书》。

使用实例

设置 SNMP trap 模式为 Event Code。

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

查询 SNMP trap 模式信息。

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

6.5 Syslog 命令

介绍服务器 syslog 相关命令的查询和设置方法。

6.5.1 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 BMC 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
<i>destination</i>	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。
<i>disabled</i>	表示禁用 syslog 上报功能。	-
<i>enabled</i>	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。

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

查询 syslog 上报功能的使能状态。

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

禁用通道 1 的 syslog 上报功能。

```
BMC:/->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。

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

6.5.2 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
<i>option</i>	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。

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

查询当前证书认证方式。

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

6.5.3 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
<i>option</i>	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。

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

查询 syslog 主机标识。

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

6.5.4 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
<i>option</i>	表示采用的协议类型。	• 1: UDP • 2: TCP • 3: TLS

使用指南

- **TLS**: 面向连接的协议，并保证数据传输的保密性和数据完整性。
- **TCP**: 面向连接的协议，在正式收发数据前，必须在收发方建立可靠的连接。
- **UDP**: 面向非连接的协议，在正式收发数据前，收发方不建立连接，直接传输正式的数据。

使用实例

设置 syslog 上报时采用的协议类型为“TLS”。

```
BMC:/-> 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。

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


6.5.5 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
<i>level</i>	表示上报日志的级别。	• none: 表示不发送告警。 • all: 表示发送的告警包含所有故障和日志告警。 • normal: 表示发送的告警包含所有故障和日志告警。 • minor: 表示发送的告警为轻微、严重、紧急故障告警。 • major: 表示发送的告警为严重、紧急故障告警。 • critical: 表示发送的告警为紧急故障告警。

使用指南

无

使用实例

设置 syslog 上报日志的级别为 “critical”。

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

查询 syslog 上报日志的级别。

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

6.5.6 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 BMC，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
<i>filepath</i>	表示待上传的根证书在 BMC 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 BMC 文件系统的指定目录（例如 “/tmp”）。

说明

请定期更新证书，否则可能存在安全风险。

使用实例

上传服务器根证书。

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

查询服务器根证书信息。

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

6.5.7 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 BMC，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
<i>filepath</i>	表示待上传的本地证书在 BMC 上的绝对路径。	绝对路径，例如：“/tmp/clientcertificate”。
<i>password</i>	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 BMC 文件系统的指定目录（例如“/tmp”）。

说明

请定期更新证书，否则可能存在安全风险。

使用实例

上传本地证书。

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

查询本地证书信息。

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

6.5.8 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
<i>destination</i>	表示 syslog 上报通道的编号。	1 ~ 4
<i>ipaddr</i>	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”。

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

查询 syslog 服务器地址。

```
BMC:/-> 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。

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

6.5.9 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
<i>destination</i>	表示 syslog 上报通道的编号。	1 ~ 4
<i>portvalue</i>	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”。

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

查询 syslog 服务器端口。

```
BMC:/-> 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
```

6.5.10 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
<i>destination</i>	表示 syslog 上报通道的编号。	1 ~ 4
<i>type</i>	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。

```
BMC:/-> 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。

```
BMC:/-> 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
```

6.5.11 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
<i>destination</i>	表示 syslog 上报通道的编号。	1 ~ 4

使用指南

syslog 服务器地址和端口已配置且当前状态已开启。

使用实例

测试通道 1 配置的 syslog 服务器是否可连接。

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

6.5.12 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 BMC syslog 日志上报通道的配置情况。

```
BMC:/-> 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
```

6.6 VNC 命令

介绍服务器 VNC 相关命令的查询和设置方法。

6.6.1 查询 VNC 服务信息（vnc -d info）

命令功能

vnc -d info 命令用于查询 VNC 服务的信息。

命令格式

ipmcget -t vnc -d info

参数说明

无

使用指南

无

使用实例

查询 VNC 服务的信息。

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

6.6.2 设置 VNC 服务的密码（vnc -d password）

命令功能

vnc -d password 命令用于设置 VNC 服务的密码。

命令格式

ipmcset -t vnc -d password

参数说明

无

使用指南

设置 VNC 服务的登录密码。

取值原则：

- 关闭密码检查功能时，VNC 服务的登录密码取值长度为 1~8 个字符，可由数字、英文字母和特殊字符组成。
- 启用密码检查功能时，VNC 服务的登录密码取值规则为：
 - 长度要求：必须为 8 个字符。
 - 复杂度要求：
 - 至少包含一个空格或以下特殊字符：
`~!@#\$%^&*()-_+=\|[]{};:","<.>/?
 - 至少包含以下两种字符：
 - 大写字母：A~Z
 - 小写字母：a~z
 - 数字：0~9

使用实例

设置 VNC 服务的密码。

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

6.6.3 设置 VNC 服务的超时时长（vnc -d timeout）

命令功能

vnc -d timeout 命令用于设置 VNC 服务的超时时长。

命令格式

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

参数说明

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

使用指南

无

使用实例

设置 VNC 服务超时的时长。

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

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

命令功能

vnc -d ssl 命令用于设置 VNC 服务 SSL 加密功能的状态。

命令格式

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

参数说明

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

使用指南

无

使用实例

设置 VNC 服务 SSL 加密功能为启用状态。

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

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

命令功能

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

命令格式

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

参数说明

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

使用指南

无

使用实例

设置 VNC 服务的键盘布局为日式键盘。

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

6.7 服务器命令

6.7.1 查询和设置启动设备（bootdevice）

命令功能

bootdevice 用来查询和设置启动设备。

命令格式

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

参数说明

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

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

使用指南

无

使用实例

说明

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

设置启动设备从默认的硬盘启动，仅生效一次。

```
BMC:/->ipmcset -d bootdevice -v 2 once
Set boot device successfully.
```

查询修改后的启动设备。

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

6.7.2 设置服务器重启方式（frucontrol）

命令功能

frucontrol 命令设置服务器的重启方式。

命令格式

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

参数说明

参数	参数说明	取值
option	服务器重启方式	0: 表示强制重启服务

参数	参数说明	取值
		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。

```
BMC:/->ipmcset -d frucontrol -v 0
WARNING: A forced restart may damage programs or unsaved data of the server.
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。

```
BMC:/->ipmcset -d frucontrol -v 2
WARNING: A forced power cycle may damage programs or unsaved data of the server.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced power cycle) successfully.
```

6.7.3 查询和设置服务器上下电状态（powerstate）

命令功能

powerstate 命令用于查询和控制服务器的上电和下电状态。

命令格式

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

参数说明

参数	参数说明	取值
<i>option</i>	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。

```
BMC:/->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

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

6.7.4 查询和设置服务器的下电时限（shutdowntimeout）

命令功能

shutdowntimeout 命令用来查询和设置服务器的下电时限。

下电时限：执行下电操作后，BMC 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，BMC 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
<i>time</i>	- 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

无。

使用实例

设置服务器的下电时限为 600s。

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

查询服务器的下电时限。

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

如果 WebUI 中的“下电时限”设置为“未勾选”，此时可以查看到“下电时限”功能已经被禁止。

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

关闭服务器的下电时限功能。

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

6.7.5 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。

```
BMC:/->ipmcget -d macaddr
Type      | Name      | Mac Address
LOM       | Port1     | 
LOM       | Port2     | 
LOM       | Port3     | 
LOM       | Port4     | 
```

6.7.6 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。

```
BMC:/->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
```

6.7.7 清除 BIOS Flash（clearcmos）

命令功能

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

命令格式

ipmcset -d clearcmos

参数说明

无

使用指南

无

使用实例

清除主板 BIOS Flash 信息。

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


6.7.8 查询 RAID 控制器信息（ctrlinfo）

命令功能

ctrlinfo 用来查询 RAID 控制器信息。

命令格式

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

参数说明

参数	参数说明	取值
<i>option</i>	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 BMC 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 BMC 带外管理。
- 服务器 OS 侧已安装并运行 BMA 2.0。

使用实例

查询 ID 为 0 的 RAID 控制器的信息。

```
BMC:/->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
-----
```

6.7.9 查询逻辑盘信息 (ldinfo)

命令功能

ldinfo 用来查询 RAID 控制器所管理的逻辑盘的信息。

命令格式

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

参数说明

参数	参数说明	取值
<i>ctrlid</i>	待查询逻辑盘所属 RAID 控制器的 ID。	0~255
<i>option</i>	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 BMC 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 BMC 带外管理。
- 服务器 OS 侧已安装并运行 BMA 2.0。

使用实例

查询 ID 为 0 的 RAID 控制器下 ID 为 0 的逻辑盘的信息。

```
BMC:/->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。

```

BMC:/->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
-----
```

6.7.10 查询物理盘信息（pdinfo）

命令功能

pdinfo 用来查询物理盘的信息。

命令格式

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

参数说明

参数	参数说明	取值
<i>option</i>	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 BMC 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 BMC 带外管理。
- 服务器 OS 侧已安装并运行 BMA 2.0。

使用实例

查询 ID 为 2 的物理盘的信息。

```

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

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

```

查询所有物理盘的信息。

```

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

```

```

Remnant Media Wearout      : 99%
Power-On Hours             : 5200
SAS Address(0)             : 5000cca02b0ad99d
SAS Address(1)             : 0000000000000000
Location State             : Off

```

```

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

```

Physical Drive Information

```

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

```

```

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

```

Physical Drive Information

```

ID                          : 2
Device Name                 : Disk2
Manufacturer               : SEAGATE
Serial Number              : 6XR1JS5H
Model                     : ST9600205SS
Firmware Version           : B002
Health Status              : Normal
Firmware State             : UNCONFIGURED GOOD
Power State                : Spun Up

```

```

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

```

```

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

```

Physical Drive Information

```

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

```

```

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

```

Physical Drive Information

```

ID                          : 4

```



```
Device Name           : Disk4
Manufacturer          : SEAGATE
Serial Number         : S0M31J5T
Model                 : ST600MM0006
Firmware Version      : B001
Health Status         : Normal
Firmware State        : UNCONFIGURED GOOD
Power State           : Spun Up
Media Type             : HDD
Interface Type        : SAS
Capable Speed         : 6.0 Gbps
Negotiated Speed      : 6.0 Gbps
Drive Temperature     : 34(Celsius)
Capacity              : 557.861 GB
Hot Spare              : None
Rebuild in Progress   : No
Patrol Read in Progress : No
Remnant Media Wearout : N/A
Power-On Hours        : 519
SAS Address(0)        : 5000c50076b1aa2d
SAS Address(1)        : 0000000000000000
Location State        : Off

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

6.7.11 查询磁盘组信息（arrayinfo）

命令功能

arrayinfo 用来查询磁盘组的信息。

命令格式

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

参数说明

参数	参数说明	取值
<i>control_id</i>	磁盘组所在控制器的 ID	0~255
<i>option</i>	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 BMC 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 BMC 带外管理。
- 服务器 OS 侧已安装并运行 BMA 2.0。

使用实例

查询 ID 为 0 的控制器上 ID 为 1 的磁盘组的信息。

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

查询 ID 为 0 的控制器上所有磁盘组的信息。

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

Physical Drive(s) ID	: 3

6.7.12 创建逻辑盘（createld）

命令功能

createld 用于使用空闲物理盘创建虚拟盘。

命令格式

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

参数说明

参数	参数说明	取值
<i>control_id</i>	RAID 控制器的 ID	0~255
<i>raidlevel</i>	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”。
<i>pd_id</i>	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。
<i>span_num</i>	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 时，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。
<i>ldname</i>	逻辑盘名称	最大长度为 15 个字符的字符串。
<i>capative</i>	逻辑盘容量	逻辑盘容量的单位可以为：

参数	参数说明	取值
		• 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。
<i>stripesize</i>	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。
<i>rpvalue</i>	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。
<i>wpvalue</i>	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”。
<i>iopvalue</i>	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。
<i>apvalue</i>	逻辑盘的访问策略	• rw: 设置逻辑盘的访问策略为可读写。

参数	参数说明	取值
		- 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	逻辑盘的物理盘缓存策略	- 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，逻辑盘的默认物理盘缓存策略为“default”。 - 当命令中不包含“-cachecade”且不配置此参数时，逻辑盘的默认物理盘缓存策略为“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 BMC 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 BMC 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。

```
BMC:/-> 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。

```
BMC:/-> 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
```

6.7.13 添加逻辑盘（addld）

命令功能

addld 用于在已有逻辑盘的磁盘组上添加新的逻辑盘。

命令格式

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

参数说明

参数	参数说明	取值
<i>control_id</i>	RAID 控制器的 ID	0~255
<i>arrayid</i>	待添加逻辑盘的磁盘组的 ID	0~255
<i>ldname</i>	逻辑盘名称	最大长度为 15 个字符的字符串。
<i>capative</i>	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。
<i>stripesize</i>	逻辑盘条带大小	可选的条带大小包括： • 64K • 128K • 256K • 512K • 1M 单位为字节，默认为“256K”。
<i>rpvalue</i>	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”。
<i>wpvalue</i>	逻辑盘的写策略	• wt: 设置逻辑盘写策略为“Write Through”。

参数	参数说明	取值
		- 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”。
<i>iopvalue</i>	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”。
<i>apvalue</i>	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”。
<i>dcpvalue</i>	逻辑盘的物理盘缓存策略	- 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”。
<i>initmode</i>	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”。
<i>blockid</i>	待添加逻辑盘的磁盘组的空闲块 ID	0~32

使用指南

必须满足如下条件方可执行此命令：

RAID 卡支持 BMC 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 BMC 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。

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

6.7.14 删除逻辑盘（deleteld）

命令功能

deleteld 用于删除 RAID 卡管理的逻辑盘。

命令格式

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

参数说明

参数	参数说明	取值
<i>control_id</i>	RAID 控制器的 ID	0~255
<i>ldid</i>	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 BMC 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 BMC 带外管理。

使用实例

删除 ID 为 0 的 RAID 控制器的逻辑盘 1。

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

6.7.15 修改逻辑盘属性（ldconfig）

命令功能

ldconfig 用于修改逻辑盘的属性。

命令格式

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

参数说明

参数	参数说明	取值
<i>control_id</i>	RAID 控制器的 ID	0~255
<i>ldid</i>	逻辑盘的 ID	0~255
<i>ldname</i>	逻辑盘名称	最大长度为 15 个字符的字符串。
<i>rpvalue</i>	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。
<i>wpvalue</i>	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”。
<i>iopvalue</i>	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。
<i>apvalue</i>	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。
<i>dcpvalue</i>	逻辑盘的物理盘缓存策略	- 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。
<i>bgistate</i>	逻辑盘的 BGI 使能状态	- enabled: 开启逻辑盘的后台初始化功能。 - disabled: 关闭逻辑盘的后台初始化功能。 说明 当逻辑盘为 CacheCade 逻辑盘时, 不支持设置此参数。

参数	参数说明	取值
		数。
<i>sscdstate</i>	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 BMC 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 BMC 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。

```
BMC:/-> 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
```

6.7.16 修改 RAID 控制器属性（ctrlconfig）

命令功能

ctrlconfig 用于修改 RAID 控制器的属性。

命令格式

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

参数说明

参数	参数说明	取值
<i>control_id</i>	RAID 控制器的 ID	0~255
<i>cbstate</i>	RAID 控制器的	enabled

参数	参数说明	取值
	Copyback 功能使能状态	disabled
<i>smartercbstate</i>	RAID 控制器在成员盘出现 SMART 错误时 Copyback 功能使能状态	- enabled - disabled
<i>jbodstate</i>	RAID 控制器 JBOD 模式使能状态	- enabled - disabled
<i>mode</i>	RAID 控制器的工作模式	- RAID - JBOD

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 BMC 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 BMC 带外管理。

使用实例

设置 ID 为 0 的 RAID 控制器的 Copyback 使能状态。

```
BMC:/-> 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
```

6.7.17 修改物理盘属性（pdconfig）

命令功能

pdconfig 用于修改 RAID 控制器所管理的物理盘的属性。

命令格式

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

参数说明

参数	参数说明	取值
<i>pdid</i>	物理硬盘的 ID	0~255

参数	参数说明	取值
<i>pdstate</i>	物理盘的运行状态	• online: 在线 • offline: 离线 • ug: 空闲 • jbod: 直通
<i>hotsparetype</i>	物理盘的热备状态	• none: 取消热备 • global: 全局热备 • dedicated: 局部热备
<i>ldid</i>	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
<i>locatestate</i>	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
<i>bootparam</i>	启动盘优先级设置级别	• none: 关闭物理盘作为启动设备 • primary: 设置物理盘为第一启动项 • secondary: 设置物理盘为第二启动项 • all : 设置物理盘为第一和第二启动项

使用指南

命令行中包含 **-cryptoerase** 时，表示将加密盘的数据擦除。

必须满足如下任一条件方可执行此命令：

RAID 卡支持 BMC 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 BMC 带外管理。

使用实例

擦除 ID 为 1 的加密物理盘数据。

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

6.7.18 查询和设置 NPU 芯片工作模式（npuworkmode）

命令功能

npuworkmode 命令用于查询和设置 NPU 芯片的工作模式。

命令格式

```
ipmcget -d npuworkmode
ipmcset -d npuworkmode -v <option>
```

参数说明

参数	参数说明	取值
<i>option</i>	NPU 芯片的工作模式	0：AMP 模式 1：SMP 模式

使用指南

只有服务器操作系统在下电状态时支持执行该命令。

使用实例

设置 NPU 芯片的工作模式为 AMP 模式。

```
BMC:/->ipmcset -d npuworkmode -v 0
----- NPU BOARD WORK MODE -----
NPU BOARD ID           : 1
WORK MODE               : AMP
----- NPU BOARD WORK MODE -----
NPU BOARD ID           : 2
WORK MODE               : AMP
```

查询 NPU 芯片的工作模式。

```
BMC:/->ipmcget -d npuworkmode
----- NPU BOARD WORK MODE -----
NPU BOARD ID           : 1
WORK MODE               : AMP
----- NPU BOARD WORK MODE -----
NPU BOARD ID           : 2
WORK MODE               : AMP
```

6.8 系统命令

介绍系统有关命令的查询和设置方法。

6.8.1 查询系统名称（systemname）

命令功能

systemname 命令用来查询系统名称。

命令格式

ipmcget -t smbios -d systemname

参数说明

无

使用指南

无

使用实例

查询服务器系统名称。

```
BMC:/->ipmcget -t smbios -d systemname
System name is: xxxxxx
```

6.8.2 设置 BMC 时区（timezone）

命令功能

timezone 命令用来设置 BMC 时区。

命令格式

ipmcset -d timezone -v <timezone>

参数说明

参数	参数说明	取值
<i>timezone</i>	时区。	- 时间偏移 取值范围： - [-12:00~+14:00]，例如+8:00、-4:30。 - [UTC-12:00~UTC+14:00]，例如 UTC+8:00、UTC-4:30。 - [GMT-12:00~GMT+14:00]

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

使用指南

在支持夏令时的时区，BMC 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 BMC 时区为+8:00。

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

设置 BMC 时区为 UTC+8:00。

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

查询 BMC 时间。

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

设置 BMC 时区为 Asia/Shanghai。

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

查询 BMC 时间。

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

6.8.3 查询 BMC 时间（time）

命令功能

time 命令用来查询 BMC 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 BMC 时间。

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

或

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

6.8.4 查询设备的版本信息（version）

命令功能

version 命令用来查询设备的版本信息。

命令格式

ipmcget -d version

参数说明

无

使用指南

无

使用实例

查询设备的版本信息。


```
BMC:/->ipmcget -d version
```

服务器的系统返回信息如下所示：

```
----- BMC INFO -----
IPMC          CPU:      Hi1711
IPMI          Version:   2.0
CPLD          Version:   (U151)0.07
Active BMC Version:      (U72)3.10.02.16
Active BMC Build:        002
Active BMC Built:        21:09:56 Feb 11 2018
Backup BMC Version:      3.10.02.16
Available iBMC Version:  3.10.02.16
Available iBMC Build:    002
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:
BIOS          Version:   (U47)0.60
Backup BIOS Version:     0.60
----- Mother Board INFO -----
Mainboard     BoardID:    0x0019
Mainboard     PCB:        .B
----- Riser Card INFO -----
BC11PERY      BoardID:    0x0091
----- HDD Backplane INFO -----
Disk BP1      BoardName:   IT21BP8A
Disk BP1      BoardID:     0x00c1
Disk BP1      PCB:         .A
Disk BP1      CPLD Version: (U24)0.06
----- PSU INFO -----
PS1           Version:     DC: 02e PFC: 018
```

6.8.5 查询 FRU 信息（fruinfo）

命令功能

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

命令格式

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

参数说明

无

使用指南

无

使用实例

查询 FRU 信息。

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

6.8.6 查询系统的健康状态（health）

命令功能

health 命令用来查询系统的健康状态。

命令格式

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

参数说明

无

使用指南

无

使用实例

查询系统的健康状态。

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

6.8.7 查询系统的健康事件信息（healthevents）

命令功能

healthevents 命令用来查询系统的健康事件信息。

命令格式

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

参数说明

无

使用指南

无

使用实例

查询系统的健康事件信息。

```
BMC:/->ipmcget -d healthevents
Event Num | Event Time          | Alarm Level | Event Code | Event Description
1         | 2019-03-13 16:22:32 | Critical   | 0x01000025 | DIMM241 memory
configuration error. Error code: 0x1701.
2         | 2019-03-13 16:22:30 | Critical   | 0x01000025 | DIMM041 memory
configuration error. Error code: 0x1701.
3         | 2019-03-13 16:22:33 | Critical   | 0x01000025 | DIMM311 memory
configuration error. Error code: 0x1701.
4         | 2019-03-13 16:22:31 | Critical   | 0x01000025 | DIMM111 memory
configuration error. Error code: 0x1701.
```

6.8.8 查询服务器的设备序列号（serialnumber）

命令功能

serialnumber 命令用来查询服务器的设备序列号。

命令格式

ipmcget [-t smbios] -d serialnumber

参数说明

无

使用指南

无

使用实例

查询服务器的设备序列号。

```
BMC:/->ipmcget -d serialnumber
System SN is:44444444444444444444444444444444
```

6.8.9 查询和清除系统 SEL 信息（sel）

命令功能

sel 命令用来查询和清除系统 SEL 信息。

命令格式

```
ipmcget -d sel -v <option> [sel_id]
ipmcset [-t fru0] -d sel -v clear
```

参数说明

参数	参数说明	取值
option	要进行的操作	- list: 列出所有系统 SEL 记录。 - info: 查询 SEL 记录的使用情况。 - suggestion: 查询指定 SEL 的处理建议。 说明 系统最多可保留条日志信息，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。

```
BMC:/->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。

```
BMC:/->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 BMC.
               2. Remove and reconnect power cables or remove and reinstall the
board in the chassis.
```

清除系统 SEL 信息。

```
BMC:/->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.
```

6.8.10 查询系统操作日志（operatelog）

命令功能

operatelog 命令用来查询系统操作日志。

命令格式

ipmcget -d operatelog

参数说明

无

使用指南

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

使用实例

查询系统操作日志。

```
BMC:/->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 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:
```

6.8.11 下载系统串口数据（systemcom）

命令功能

systemcom 命令用来下载系统串口数据。

命令格式

ipmcget -d systemcom

参数说明

无

使用指南

需要在 BMC WebUI 的“维护诊断 > 系统日志”中开启系统串口数据记录功能。

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。

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

6.8.12 下载黑匣子数据（blackbox）

命令功能

blackbox 命令用来下载黑匣子数据。

命令格式

ipmcget -d blackbox

参数说明

无

使用指南

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

使用实例

#下载黑匣子数据。

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

6.8.13 下载 BIOS（download）

命令功能

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

“bios.tar.gz”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
<i>option</i>	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 <i>option</i> 参数为“1”。

使用指南

当系统出现异常时，请下载“bios.tar.gz”文件并联系技术支持工程师处理。

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

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

使用实例

下载 BIOS 文件“bios.tar.gz”到“/tmp”目录下。

```
BMC:/->ipmcset -t maintenance -d download -v 1
Download /tmp/bios.tar.gz.
Downloading BIOS...
Download BIOS successfully.
Note: Please remove /tmp/bios.tar.gz after use.
```

6.8.14 升级 BIOS（upgradebios）

命令功能

maintenance -d upgradebios 命令用来升级 BIOS。

命令格式

ipmcset -t maintenance -d upgradebios -v filepath

参数说明

参数	参数说明	取值
<i>filepath</i>	BIOS 升级文件的路径。 说明 该参数只支持“xxx.hpm”格式的文件。	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 BMC 文件系统的指定目录（例如 “/tmp”）。
- **maintenance -d upgradebios** 和 **upgrade** 命令均可升级 BIOS，区别为：
 - 使用 **maintenance -d upgradebios** 命令升级 BIOS 时，需在 OS 下电的情况下才能升级 BIOS。使用 **upgrade** 时则没有此要求。
 - 使用 **maintenance -d upgradebios** 命令升级 BIOS 时，BIOS 默认密码会变更为目标版本的默认值，请谨慎使用。

说明

在 BMC 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 BMC 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[固件升级 \(upgrade\)](#)。

使用实例

用 “/tmp/biosimage.hpm” 文件升级 BIOS。

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

6.8.15 升级主板 CPLD (upgradecpld)

命令功能

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

命令格式

ipmcset -t maintenance -d upgradecpld -v filepath

参数说明

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

使用指南

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

使用实例

使用“/tmp/cpldimage.hpm”文件升级主板 CPLD。

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

6.8.16 设置 BMC 网口状态（ethlink）

命令功能

maintenance -d ethlink 命令用来设置 BMC 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
<i>ethname</i>	待设置的网口名称	eth0、eth1、eth2、eth3 不同服务器的 BMC 网口 个数不同。
<i>action</i>	网口使能状态	• enable • disable

使用指南

无

使用实例

使能 BMC 网口“eth2”。

```
BMC:/->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.
```

6.8.17 一键收集信息（diaginfo）

命令功能

diaginfo 命令用来一键收集信息，包括 BMC 相关的配置信息、版本信息和日志等。一键收集信息的更多内容请参见本文档 [5.10 一键收集信息说明](#)。

命令格式

ipmcget -d diaginfo

参数说明

无

使用指南

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

使用实例

一键收集信息。

```
BMC:/->ipmcget -d diaginfo
Downloading...
100%
Download diagnose info to /tmp/ successfully.
```

6.8.18 恢复 BMC 出厂设置（restore）

命令功能

restore 命令用来恢复 BMC 出厂设置。执行此命令后 BMC 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 BMC 出厂设置。

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

6.8.19 设置 CLP notimeout 功能（notimeout）

命令功能

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

默认为禁用状态。

命令格式

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

参数说明

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

使用指南

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

使用实例

```
# 启用 CLP notimeout 功能。
```

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

禁用 CLP notimeout 功能。

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

设置会话超时时间为 30 分钟。

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

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

命令功能

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

命令格式

ipmcget -d notimeoutstate

参数说明

无

使用指南

无

使用实例

查询 CLP notimeout 功能的配置信息。

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

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

命令功能

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

命令格式

ipmcset -t securityenhance -d updatemasterkey

参数说明

无

使用指南

请定期更新密钥，否则可能存在安全风险。

使用实例

更新系统主密钥。

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

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

命令功能

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

命令格式

```
ipmcget -t securityenhance -d masterkeyupdateinterval
ipmcset -t securityenhance -d masterkeyupdateinterval -v <interval>
```

参数说明

参数	参数说明	取值
interval	表示自动更新间隔	0~365 的整数 单位为天，取值为 0 时表

参数	参数说明	取值
		示不自动更新主密钥。

使用指南

无

使用实例

```
# 查询主密钥自动更新间隔。

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

# 设置主密钥自动更新间隔为 365 天。

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

6.8.23 查询和设置自动发现配置（autodiscovery）

命令功能

autodiscovery 命令用来查询和设置自动发现配置。

命令格式

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

参数说明

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

使用指南

无

使用实例

```
# 查询自动发现配置。

BMC:/->ipmcget -d autodiscovery
State      : disabled
Broadcast  : 255.255.255.255
NetPort    : 26957

# 设置自动发现配置。

BMC:/->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.
```

6.8.24 查询和设置受控上电配置（poweronpermit）

命令功能

poweronpermit 命令用来查询和设置受控上电配置。

命令格式

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

参数说明

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

使用指南

无

使用实例

```
# 查询受控上电配置。
```



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

设置受控上电配置。

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

6.8.25 查询和清除上电锁的锁定状态（poweronlock）

命令功能

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

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

命令格式

```
ipmcget -t maintenance -d poweronlock
```

```
ipmcset -t maintenance -d poweronlock -v clear
```

参数说明

无

使用指南

无

使用实例

查询上电锁的锁定状态。

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

清除上电锁。

```
BMC:/->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.
```

6.8.26 重启鲲鹏智能管理引擎（resetiME）

命令功能

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

命令格式

ipmcset -t maintenance -d resetiME

参数说明

无

使用指南

无

使用实例

重启鲲鹏智能管理引擎。

```
BMC:/->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.
```

6.9 用户管理命令

介绍用户管理有关命令的查询和设置方法。

6.9.1 查询所有用户信息（userlist/list）

命令功能

userlist/list 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。

```
BMC:/->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
```

6.9.2 添加新用户（adduser）

命令功能

adduser 用于添加新用户。

命令格式

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

参数说明

参数	参数说明	取值
<i>username</i>	表示待添加的用户名。	数据类型为字符型，数据范围不超过 16 个字符。 由特殊符号、英文字母

参数	参数说明	取值
		和数字组成，特殊字符不包括： :<>&,"'\^% - 不能包含空格且首字符不能是“#”、“+”或“-”。 - 用户名不能为“.”或“..”。

使用指南

只有管理员可以添加新用户，操作过程中需要输入当前管理员的密码。

新添加的 SSH 用户默认为禁用状态，如需启用该用户，可参考 [6.9.20 设置用户启用状态（user -d state）](#) 启用用户。

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

请根据密码复杂度检查功能的开启情况（可通过 [6.9.6 查询和设置密码检查功能（passwordcomplexity）](#) 命令查询）以及弱口令认证功能的开启情况（可通过 [6.9.15 设置弱口令字典认证使能状态（weakpwddic）](#) 命令查询），修改符合不同规则的密码。

- 关闭密码检查功能后，密码不能为空，可以是任意字符组成的长度不大于 20 的字符串。如果密码长度小于 8 个字符，该用户将无法使用 SNMPv3 接口。
- 启用密码检查功能后，密码复杂度要求：
 - 长度为 8 ~ 20 个字符。
 - 至少包含一个空格或者以下特殊字符：
`~!@#%&^&()*-_=+~\[\]{};:~",<.>/?
 - 至少包含以下字符中的两种：
 - 小写字母：a ~ z
 - 大写字母：A ~ Z
 - 数字：0 ~ 9
 - 密码不能是用户名或用户名的倒序。
- 弱口令字典认证功能使能的情况下，除上述复杂度检查外，BMC 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 [6.9.16 导出弱口令字典（weakpwddic -v export）](#) 获取。）

说明

默认密码在弱口令字典中。

使用实例

添加一个新用户，用户名称为 test。

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

查询添加后的用户名单。

```
BMC:/->ipmcget -d userlist
```

ID	Name	Privilege	Interface	State
2	root	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
3	test	NO ACCESS	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
4		NO ACCESS		NA
5		NO ACCESS		NA
6		NO ACCESS		NA
7		NO ACCESS		NA
8		NO ACCESS		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		NA

结果显示新增用户 **test** 已经成功添加。

6.9.3 修改用户密码（password）

命令功能

password 命令用来修改用户密码。

命令格式

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

参数说明

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

使用指南

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

请根据密码复杂度检查功能的开启情况（可通过 [6.9.6 查询和设置密码检查功能（passwordcomplexity）](#) 命令查询）以及弱口令认证功能的开启情况（可通过 [6.9.15 设置弱口令字典认证使能状态（weakpwddic）](#) 命令查询），修改符合不同规则的密码。

- 关闭密码检查功能后，密码不能为空，可以是任意字符组成的长度不大于 20 的字符串。如果密码长度小于 8 个字符，该用户将无法使用 SNMPv3 接口。
- 启用密码检查功能后，密码复杂度要求：
 - 长度为 8 ~ 20 个字符。
 - 至少包含一个空格或者以下特殊字符：
`~!@#\$%^&\*()-\_+=\|{};:","<.>/?`
 - 至少包含以下字符中的两种：
 - 小写字母：a ~ z
 - 大写字母：A ~ Z
 - 数字：0 ~ 9
 - 密码不能是用户名或用户名的倒序。
- 弱口令字典认证功能使能的情况下，除上述复杂度检查外，BMC 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 [6.9.16 导出弱口令字典（weakpwddic -v export）](#) 获取。）

说明

默认密码在弱口令字典中。

使用实例

修改用户名称为 user 的密码。

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

6.9.4 删除用户（deluser）

命令功能

deluser 用来删除用户。

命令格式

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

参数说明

参数	参数说明	取值
<i>username</i>	表示当前存在的待删除的用户名。	-

使用指南

- 只有管理员可以删除用户，操作过程中需要输入当前管理员的密码。
- 当 BMC 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。

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

6.9.5 设置用户权限（privilege）

命令功能

privilege 命令用来设置用户权限。

命令格式

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

参数说明

参数	参数说明	取值
<i>username</i>	表示当前存在的待设置权限的用户名。	-
<i>privalue</i>	用户权限	• 15: No Access 权限

参数	参数说明	取值
		• 2: User 权限 • 3: Operator 权限 • 4: Administrator 权限 • 5: Custom Role1 权限 • 6: Custom Role2 权限 • 7: Custom Role3 权限 • 8: Custom Role4 权限

使用指南

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

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

6.9.6 查询和设置密码检查功能（passwordcomplexity）

命令功能

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

命令格式

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

参数说明

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

使用指南

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

须知

- 密码检查功能的默认状态为启用。
- 禁用密码检查功能，会降低系统安全性，请谨慎使用。
- 关闭密码检查功能后，密码不能为空，可以是任意字符组成的长度不大于 20 的字符串。如果密码长度小于 8 个字符，该用户将无法使用 SNMPv3 接口。
- 启用密码检查功能后，密码复杂度要求：
 - 长度为 8 ~ 20 个字符。
 - 至少包含一个空格或者以下特殊字符：
`~!@#\$%^&\*()-\_+=+\\[{}];:","<.>/?`
 - 至少包含以下字符中的两种：
 - 小写字母：a ~ z
 - 大写字母：A ~ Z
 - 数字：0 ~ 9
 - 密码不能是用户名或用户名的倒序。
- 弱口令字典认证功能使能的情况下，除上述复杂度检查外，BMC 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 [6.9.16 导出弱口令字典（weakpwddic -v export）](#) 获取。）

说明

默认密码在弱口令字典中。

使用实例

查询密码复杂度检查功能的开启状态。

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

开启密码复杂度检查功能。

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

6.9.7 锁定用户（user -d lock）

命令功能

lock 命令用于锁定指定的用户，而用户在被锁定之后将不能登录。

命令格式

ipmcset -t user -d lock -v username

参数说明

参数	参数说明	取值
<i>username</i>	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。

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

6.9.8 解除用户锁定状态（user -d unlock）

命令功能

unlock 命令用于解锁被手动锁定或因密码重试次数用完而锁定的用户。

命令格式

ipmcset -t user -d unlock -v username

参数说明

参数	参数说明	取值
<i>username</i>	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。

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

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

命令功能

minimumpasswordage 命令用于查询和设置密码的最短使用期。

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

命令格式

ipmcget -d minimumpasswordage

ipmcset -d minimumpasswordage -v time

参数说明

参数	参数说明	取值
<i>time</i>	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。

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

查询密码最短使用期。

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

6.9.10 设置紧急用户（emergencyuser）

命令功能

emergencyuser 命令用于设置不受登录规则限制的紧急用户。

命令格式

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

参数说明

参数	参数说明	取值
<i>username</i>	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。

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

6.9.11 为用户添加 SSH 公钥（addpublickey）

命令功能

addpublickey 命令为用户添加 SSH 公钥。

命令格式

ipmcset -t user -d addpublickey -v username <filepath|file_URL>

参数说明

参数	参数说明	取值
<i>username</i>	待导入 SSH 公钥的用户名	已存在的 SSH 用户的用户名
<i>filepath</i>	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_2048key”。
<i>file_URL</i>	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

参数	参数说明	取值
		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 BMC 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。

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

6.9.12 删除用户的 SSH 公钥（delpublickey）

命令功能

delpublickey 命令为用户删除 SSH 公钥。

命令格式

ipmcset -t user -d delpublickey -v username

参数说明

参数	参数说明	取值
<i>username</i>	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。

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

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

命令功能

sshpaswordauthentication 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 sshpaswordauthentication
ipmcset -t user -d sshpaswordauthentication -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。

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

查询 SSH 用户密码认证使能状态。

```
BMC:/-> ipmcget -t user -d sshpaswordauthentication
SSH Password Authentication : enabled
```

6.9.14 设置用户登录 BMC 的接口类型（interface）

命令功能

interface 命令用于设置指定用户登录 BMC 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
<i>username</i>	待配置的用户	-
<i>enabled</i>	使能指定的接口类型	-
<i>disabled</i>	禁止指定的接口类型	-
<i>option1 option2 ... optionN</i>	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 BMC 的接口类型为“Web,SNMP,IPMI,SSH,SFTP,Local”。

```
BMC:/-> 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。

```
BMC:/->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		NA

6.9.15 设置弱口令字典认证使能状态（weakpwddic）

命令功能

weakpwddic 命令用于设置弱口令字典认证功能的使能状态。

出现在弱口令字典中的字符串不能被设置为:

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

命令格式

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

参数说明

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

使用指南

只有管理员和具有安全配置权限的自定义用户可以设置弱口令字典认证使能状态。

使用实例

使能弱口令字典认证功能。

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


6.9.16 导出弱口令字典（weakpwddic -v export）

命令功能

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

命令格式

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

参数说明

参数	参数说明	取值
filepath	将弱口令字典导出到 BMC 文件系统时，在 BMC 件系统中的存放路径。	绝对路径，例如： “/tmp/weakpwddictionary”。
file_URL	将弱口令字典导出到远程设备时，在远程设备上的存放路径。	格式为： protocol://[username:password@]IP:[port]/directory/filename 其中： - protocol：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 - BMC 当前仅支持 SMB V1.0 版本。 - 使用 nfs 协议时，存放路径中不能包含 username:password@ 字段；使用其它协议时，存放路径中必须包含 username:password@ 字段。 - cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 - username：登录远程设备所需的用户名。 - password：登录远程设备所需的密码。 - IP:[port]：远程设备的 IP 地址和端口号。 - directory/filename：弱口令字典在远程设备上的绝对路径。 例如： “https://root:Mytest12#\$@10.10.10.1:443/tmp/weakpwddictionary”

使用指南

只有管理员和具有安全配置权限的自定义用户可以导出弱口令字典。

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

使用实例

```
# 导出弱口令字典。

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

6.9.17 导入弱口令字典（weakpwddic -v import）

命令功能

weakpwddic -v import 命令用于导入 BMC 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	将弱口令字典导入 BMC 时，待导入的文件在 BMC 文件系统中的存放路径。	对路径，例如： “/tmp/weakpwddictionary”。
file_URL	将弱口令字典导入 BMC 时，待导入的文件在远程设备上的存放路径。	格式为： protocol://[username:password@]IP:[port] /directory/filename 其中： - protocol：必须为“https”、“sftp”、“cifs”、“scp”和“nfs”中的一种。 说明 - BMC 当前仅支持 SMB V1.0 版本。 - 使用 nfs 协议时，存放路径中不能包含 username:password@ 字段；使用其它协议时，存放路径中必须包含 username:password@ 字段。 - cifs 标准协议使用了不安全算法，建议优先选择更安全的 https、sftp、scp 或 nfs 协议。 - username：登录目标服务器所需的用

参数	参数说明	取值
		户名。 <i>password</i>: 登录目标服务器所需的密码。 <i>IP:[port]</i>: 目标服务器的 IP 地址和端口号。 <i>directory/filename</i>: 弱口令字典在目标服务器上的绝对路径。 例如: “https://root:Admin12#\$@10.10.10.1:443/tmp/weakpwddictionary”

使用指南

只有管理员和具有安全配置权限的自定义用户可以导入弱口令字典。

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

使用实例

```
# 导入弱口令字典。

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

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

命令功能

snmpprivacypassword 命令用于设置指定用户使用 SNMPv3 连接 BMC 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
<i>username</i>	待配置的用户	-

使用指南

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

请根据密码复杂度检查功能的开启情况（可通过 [6.9.6 查询和设置密码检查功能（passwordcomplexity）](#) 命令查询）以及弱口令认证功能的开启情况（可通过 [6.9.15 设置弱口令字典认证使能状态（weakpwddic）](#) 命令查询），修改符合不同规则的密码。

- 关闭密码检查功能后，密码不能为空，可以是任意字符组成的长度不大于 20 的字符串。如果密码长度小于 8 个字符，该用户将无法使用 SNMPv3 接口。
- 启用密码检查功能后，密码复杂度要求：
 - 长度为 8 ~ 20 个字符。
 - 至少包含一个空格或者以下特殊字符：
'~!@#\$%^&*()-_+=\|[]{};:","<.>/?
 - 至少包含以下字符中的两种：
 - 小写字母：a ~ z
 - 大写字母：A ~ Z
 - 数字：0 ~ 9
 - 密码不能是用户名或用户名的倒序。
- 弱口令字典认证功能使能的情况下，除上述复杂度检查外，BMC 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 6.9.16 导出弱口令字典（weakpwddic -v export）获取。）

 说明

默认密码在弱口令字典中。

使用实例

```
# 设置 SNMPv3 用户的加密密码。
```

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

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

命令功能

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

命令格式

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

ipmcget -t securityenhance -d inactivetimelimit

参数说明

参数	参数说明	取值
<i>value</i>	表示不活动期限	• 0 • 30~365 单位为天，取值为 0 时表示 unlimited，用户不会因为长时间不活动而被禁止。

使用指南

无

使用实例

设置和查询不活动期限。

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

6.9.20 设置用户启用状态（user -d state）

命令功能

user -d state 命令用于设置用户的启用状态。

命令格式

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

ipmcget -d userlist

参数说明

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

使用指南

当 BMC 系统中仅有一个启用的管理员用户时，该管理员用户不能被禁用。

使用实例

启用 “test15” 用户。

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

查询 “test15” 的状态。

```
BMC:/-> ipmcget -d userlist
```

ID	Name	Privilege	Interface	State
2	root	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
3	test1	CUSTOM_ROLE1	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
4	test2	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
5	test3	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
6	test4	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
7	test5	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
8	test6	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
9	test7	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
10	test8	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled
11	test9	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
12	test10	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
13	test11	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
14	test12	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
15	test13	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
16	test14	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	disabled
17	test15	ADMINISTRATOR	Web,SNMP,IPMI,SSH,SFTP,Local,Redfish	Enabled

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

命令功能

`user -d usermgmtbyhost` 命令用于查询和设置带内用户管理功能的使能状态。

命令格式

`ipmcset -t user -d usermgmtbyhost -v <option>`

`ipmcget -t user -d usermgmtbyhost`

参数说明

参数	参数说明	取值
<i>option</i>	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。

```
BMC:/->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。

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

6.9.22 设置用户首次登录时的密码修改策略（`user -d firstloginpolicy`）

命令功能

对于新建的用户或被重置了密码的用户，其登录密码为初始状态，可能存在密码泄露的风险。

user -d firstloginpolicy 命令用于设置用户密码为初始状态的情况下，首次登录时的密码修改策略。

命令格式

ipmcset -t user -d firstloginpolicy -v <username> <option>

参数说明

参数	参数说明	取值
<i>username</i>	表示待设置的用户	已存在的用户名
<i>option</i>	表示用户密码为初始状态，首次登录时的密码修改策略	1：表示仅提示修改密码 2：表示强制修改密码

使用指南

设置的密码修改策略仅在用户密码为初始状态时生效，默认为“强制修改密码”。当新建用户或重置密码的用户由其他人使用时，建议保持“强制修改密码”的默认选项。

使用实例

新建用户或重置密码的用户由管理员自己使用，可设置首次登录时仅提示修改密码。

```
BMC:/->ipmcset -t user -d firstloginpolicy -v testuser 1
Set testuser first login policy to prompt password reset successfully.
```

新建用户或重置密码的用户由其他人使用，则设置首次登录时强制修改密码。

```
BMC:/->ipmcset -t user -d firstloginpolicy -v testuser 2
Set testuser first login policy to force password reset successfully.
```

6.10 NTP 命令

6.10.1 查询 NTP 信息（ntpinfo）

命令功能

ntpinfo 命令用于查询 BMC 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 BMC 的 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server     : 192.168.2.2
Synchronize     : successful
Auth Enable     : enabled
Group Key       : imported
```

6.10.2 设置 NTP 状态（ntp -d status）

命令功能

ntp -d status 命令用于设置 NTP 功能的使能状态。

命令格式

ipmcset -t ntp -d status -v status

参数说明

参数	参数说明	取值
status	表示 NTP 功能的使能状态	- enabled - disabled

使用指南

无

使用实例

使能 NTP 功能。

```
BMC:/->ipmcset -t ntp -d status -v enabled
Set NTP enable status (enabled) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server     : 192.168.2.2
Synchronize     : successful
Auth Enable     : enabled
Group Key       : imported
```

6.10.3 设置 NTP 信息获取方式（ntp -d mode）

命令功能

ntp -d mode 命令用于设置 NTP 信息获取方式。

命令格式

```
ipmcset -t ntp -d mode -v mode
```

参数说明

参数	参数说明	取值
<i>mode</i>	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”。

```
BMC:/->ipmcset -t ntp -d mode -v manual
Set NTP mode (manual) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
```

```
Extra Server      : 192.168.2.2
Synchronize      : successful
Auth Enable      : enabled
Group Key         : imported
```

6.10.4 设置首选 NTP 服务器地址（ntp -d preferredserver）

命令功能

ntp -d preferredserver 命令用于设置首选 NTP 服务器地址信息。

命令格式

ipmcset -t ntp -d preferredserver -v *addr*

参数说明

参数	参数说明	取值
<i>addr</i>	表示首选 NTP 服务器地址	可设置为： • IPv4 格式的地址 • IPv6 格式的地址 • 域名地址 说明 设置为 0.0.0.0 时表示删除首选 NTP 服务地址。

使用指南

支持 Linux NTP 服务器和 Windows NTP 服务器。

使用实例

设置首选 NTP 服务器地址为 “example.com”。

```
BMC:/->ipmcset -t ntp -d preferredserver -v example.com
Set NTP preferred server (example.com) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server     : 192.168.2.2
Synchronize     : successful
Auth Enable     : enabled
Group Key       : imported
```

6.10.5 设置备用 NTP 服务器地址（ntp -d alternativeserver）

命令功能

ntp -d alternativeserver 命令用于设置备用 NTP 服务器地址信息。

命令格式

ipmcset -t ntp -d alternativeserver -v addr

参数说明

参数	参数说明	取值
addr	表示备用 NTP 服务器地址	可设置为： - IPv4 格式的地址 - IPv6 格式的地址 - 域名地址 说明 设置为 0.0.0.0 时表示删除备用 NTP 服务地址。

使用指南

支持 Linux NTP 服务器和 Windows NTP 服务器。

说明

NTP 服务器切换时间请参见 [5.7.2 时区&NTP](#)。

使用实例

设置备用 NTP 服务器地址为“fc00::1234”。

```
BMC:/-> ipmcset -t ntp -d alternativeserver -v fc00::1234
Set NTP alternative server (fc00::1234) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server     : 192.168.2.2
Synchronize     : successful
Auth Enable     : enabled
Group Key       : imported
```

6.10.6 设置拓展 NTP 服务器地址（ntp -d extraserver）

命令功能

ntp -d extraserver 命令用于设置拓展 NTP 服务器地址信息。

命令格式

ipmcset -t ntp -d extraserver -v addr

参数说明

参数	参数说明	取值
addr	表示拓展 NTP 服务器地址	可设置为： - IPv4 格式的地址 - IPv6 格式的地址 - 域名地址 说明 设置为 0.0.0.0 时表示删除拓展 NTP 服务地址。

使用指南

支持 Linux NTP 服务器和 Windows NTP 服务器。

说明

NTP 服务器切换时间请参见 [5.7.2 时区&NTP](#)。

使用实例

设置拓展 NTP 服务器地址为“192.168.2.2”。

```
BMC:/->ipmcset -t ntp -d extraserver -v 192.168.2.2
Set NTP extraserver server (192.168.2.2) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status      : enabled
Mode        : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server  : 192.168.2.2
Synchronize  : successful
Auth Enable  : enabled
Group Key    : imported
```

6.10.7 设置服务器身份认证状态（ntp -d authstatus）

命令功能

ntp -d authstatus 命令用于设置服务器身份认证状态。

- 使能身份认证后，BMC 与 NTP 服务器通信时会进行身份校验。
- 禁用身份认证后，BMC 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 BMC 后，方可与 NTP 服务器进行通信。

说明

请定期更新密钥，否则可能存在安全风险。

使用实例

使能服务器身份认证。

```
BMC:/->ipmcset -t ntp -d authstatus -v enabled
Set NTP enable status (enabled) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server     : 192.168.2.2
Synchronize     : successful
Auth Enable     : enabled
Group Key       : imported
```

6.10.8 上传 NTP 组密钥（ntp -d groupkey）

命令功能

ntp -d groupkey 命令可将用户自行获取的 NTP 组密钥上传到 BMC，此时，BMC 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
<i>filepath</i>	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 BMC 文件系统的指定目录（例如“/tmp”）。

说明

请定期更新密钥，否则可能存在安全风险。

使用实例

上传 NTP 组密钥。

```
BMC:/->ipmcset -t ntp -d groupkey -v /tmp/ntp.keys
Set NTP group key (/tmp/ntp.keys) successfully.
```

查询 NTP 信息。

```
BMC:/->ipmcget -d ntpinfo
Status          : enabled
Mode            : manual
Preferred Server : example.com
Alternative Server : fc00::1234
Extra Server     : 192.168.2.2
Synchronize     : successful
Auth Enable     : enabled
Group Key       : imported
```

6.11 指示灯命令

介绍指示灯命令的查询和设置方法。

6.11.1 查询服务器指示灯信息（ledinfo）

命令功能

ledinfo 命令用来查询服务器指示灯信息。

命令格式

ipmcget -d ledinfo

参数说明

无

使用指南

无

使用实例

查询服务器控制的指示灯。

```
BMC:/->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
```

6.11.2 设置 UID 指示灯状态（identify）

命令功能

identify 命令用于设置 UID 指示灯状态。

命令格式

ipmcset -d identify [-v {time | force}]

参数说明

参数	参数说明	取值
<i>time</i>	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。

```
BMC:/->ipmcset -d identify -v force
Identify UID led successfully.
```

6.12 风扇命令

介绍服务器风扇模块有关命令的查询和设置方法。

6.12.1 设置风扇运行速度（fanlevel）

命令功能

fanlevel 命令用于设置风扇运行速度。

命令格式

ipmcset -d fanlevel -v <fanlevel> [fanid]

参数说明

参数	参数说明	取值
<i>fanlevel</i>	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。

参数	参数说明	取值
<i>fanid</i>	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，当风扇运行模式为自动模式时，该命令不生效。
- 设置方法请参考 [6.12.2 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%。

```
BMC:/->ipmcset -d fanlevel -v 50 2
Set fan(2) level to (50%) successfully.
Current Mode      : manual, timeout 99999998 seconds.
```

6.12.2 设置风扇运行模式（fanmode）

命令功能

fanmode 命令用来设置风扇的运行模式。

命令格式

```
ipmcset -d fanmode -v <mode> [timeout]
```

参数说明

参数	参数说明	取值
<i>mode</i>	表示风扇工作模式	• 0：风扇工作模式为自动，后面不设置 <i>timeout</i> 参数。 • 1：风扇工作模式为手动，后面可设置 <i>timeout</i> 参数。
<i>timeout</i>	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

BMC 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。

```
BMC:/->ipmcset -d fanmode -v 1 60
Set fan mode successfully.
Current Mode:      manual
Time out   :      60 seconds
```

6.12.3 查询风扇工作状态（faninfo）

命令功能

faninfo 命令用来查询风扇的工作模式和当前转速。

命令格式

ipmcget -d faninfo

参数说明

无

使用指南

无

使用实例

查询风扇工作状态。

```
BMC:/->ipmcget -d faninfo
Get fan mode and fan level successfully!
Current mode: manual, timeout 297 seconds.
Manual fan level:
Fan1: 40, Fan2: 50, Fan3: 60, Fan4: 70
Fan5: 40, Fan6: 50, Fan7: 60, Fan8: 70
```

6.13 传感器命令

6.13.1 查询所有传感器的所有信息（sensor -d list）

命令功能

sensor -d list 命令用来查询所有传感器信息。

命令格式

ipmcget -t sensor -d list

参数说明

无

使用指南

无

使用实例

查询所有传感器的所有信息。（不同服务器的传感器不同）

```
BMC:/->ipmcget -t sensor -d list
sensor id | sensor name | value | unit | status | lnr
| lc | lnc | unc | uc | unr | phys | nhys
0x1 | Inlet Temp | 25.000 | degrees C | ok |
na
| na | na | 36.000 | 38.000 | na | 2.000 | 2.000
0x2 | Outlet Temp | 35.000 | degrees C | ok |
na
| na | na | 75.000 | na | na | 2.000 | 2.000
0x28 | Power | 0.000 | Watts | ok | na
| na | na | na | na | na | 0.000 | 0.000
0x3 | Disks Temp | na | degrees C | na | na
| na | na | na | na | na | 0.000 | 0.000
0x6 | 1711 Core Temp | 37.000 | degrees C | ok |
na
| na | na | 105.000 | na | na | 2.000 | 2.000
0x7 | Power1 | na | Watts | na |
na
| na | na | na | na | na | 0.000 | 0.000
0x8 | PS1 VIN | na | Volts | na | na
| na | na | na | na | na | 0.000 | 0.000
0x9 | PS1 Inlet Temp | 0.000 | degrees C | ok | na
| na | na | na | na | na | 0.000 | 0.000
0xa | PS1 Chip Temp | 0.000 | degrees C | ok |
na
| na | na | na | na | na | 0.000 | 0.000
0x4 | CPU1 Core Rem | 39.000 | degrees C | ok |
na
```

na	na	105.000	na	na	2.000	2.000
0x5	CPU2 Core Rem	38.000	degrees C	ok	na	
na	na	105.000	na	na	2.000	2.000
0xe	CPU1 MEM Temp	37.000	degrees C	ok		
na						
na	na	95.000	na	na	2.000	2.000
0xf	CPU2 MEM Temp	37.000	degrees C	ok	na	
na	na	95.000	na	na	2.000	2.000
0xb	CPU1 VDDQ_AB	1.230	Volts	ok	na	
1.080	na	na	1.320	na	0.020	0.020
0xc	CPU1 VDDQ_CD	1.230	Volts	ok	na	
1.080	na	na	1.320	na	0.020	0.020
0xd	CPU2 VDDQ_AB	1.230	Volts	ok		
na						
1.080	na	na	1.320	na	0.020	0.020
0x10	CPU2 VDDQ_CD	1.230	Volts	ok	na	
1.080	na	na	1.320	na	0.020	0.020
0x11	CPU1 VDDQ Temp	31.000	degrees C	ok	na	
na	na	120.000	na	na	2.000	2.000
0x13	CPU2 VDDQ Temp	31.000	degrees C	ok	na	
na	na	120.000	na	na	2.000	2.000
0x14	CPU1 VRD Temp	33.000	degrees C	ok		
na						
na	na	120.000	na	na	2.000	2.000
0x15	CPU2 VRD Temp	34.000	degrees C	ok	na	
na	na	120.000	na	na	2.000	2.000
0x16	CPU1 VDDAVS	0.890	Volts	ok	na	
0.730	na	na	1.050	na	0.020	0.020
0x17	CPU2 VDDAVS	0.870	Volts	ok	na	
0.730	na	na	1.050	na	0.020	0.020
0x18	CPU1 HVCC	1.190	Volts	ok		
na						
1.080	na	na	1.320	na	0.020	0.020
0x29	CPU2 HVCC	1.190	Volts	ok	na	
1.080	na	na	1.320	na	0.020	0.020
0x2a	CPU1 N_VDDAVS	0.850	Volts	ok	na	
0.810	na	na	0.990	na	0.020	0.020
0x2b	CPU2 N_VDDAVS	0.850	Volts	ok	na	
0.810	na	na	0.990	na	0.020	0.020
0x2c	CPU1 VDDFIX	0.790	Volts	ok		
na						
0.720	na	na	0.880	na	0.020	0.020
0x2d	CPU2 VDDFIX	0.790	Volts	ok		
na						
0.720	na	na	0.880	na	0.020	0.020
0x2e	SYS 12V_2	11.880	Volts	ok	na	
10.010	na	na	13.530	na	0.440	0.440
0x2f	SYS 12V_3	11.990	Volts	ok	na	
10.010	na	na	13.530	na	0.440	0.440
0x30	SYS 12V_4	11.990	Volts	ok		
na						
10.010	na	na	13.530	na	0.440	0.440
0x31	SYS 12V_5	12.100	Volts	ok		
na						
10.010	na	na	13.530	na	0.440	0.440

0x32	SYS 12V_6	11.880	Volts	ok	na
10.010	na	na	13.530	na	0.440 0.440
0x19	FAN1 F Speed	16350.000	RPM	ok	na
na	na	na	na	na	0.000 0.000
0x1a	FAN1 R Speed	14700.000	RPM	ok	
na	na	na	na	na	0.000 0.000
0x1b	FAN2 F Speed	na	RPM	na	
na	na	na	na	na	0.000 0.000
0x1c	FAN2 R Speed	na	RPM	na	na
na	na	na	na	na	0.000 0.000
0x1d	FAN3 F Speed	16500.000	RPM	ok	na
na	na	na	na	na	0.000 0.000
0x1e	FAN3 R Speed	14850.000	RPM	ok	
na	na	na	na	na	0.000 0.000
0x1f	FAN4 F Speed	16200.000	RPM	ok	
na	na	na	na	na	0.000 0.000
0x20	FAN4 R Speed	15000.000	RPM	ok	na
na	na	na	na	na	0.000 0.000
0x21	FAN5 F Speed	16200.000	RPM	ok	na
na	na	na	na	na	0.000 0.000
0x22	FAN5 R Speed	14850.000	RPM	ok	
na	na	na	na	na	0.000 0.000
0x23	FAN6 F Speed	na	RPM	na	
na	na	na	na	na	0.000 0.000
0x24	FAN6 R Speed	na	RPM	na	na
na	na	na	na	na	0.000 0.000
0x25	FAN7 F Speed	16350.000	RPM	ok	na
na	na	na	na	na	0.000 0.000
0x26	FAN7 R Speed	14850.000	RPM	ok	
na	na	na	na	na	0.000 0.000
0x98	PCIe NIC2 Temp	53.000	degrees C	ok	
na	na	105.000	na	na	2.000 2.000
0x99	PCIe2 NIC 3.3V	3.320	Volts	ok	na
3.140	na	na	3.460	na	0.040 0.040
0x9a	PCIe2 NIC 1.2V	1.190	Volts	ok	na
1.140	na	na	1.260	na	0.020 0.020
0x9b	PCIe2 NIC 1.8V	1.800	Volts	ok	
na	1.710	na	1.890	na	0.020 0.020
0x9c	PCIe2 NIC 0.8V	0.800	Volts	ok	
na	0.760	na	0.840	na	0.020 0.020
0x93	PCIe NIC5 Temp	56.000	degrees C	ok	na
na	na	105.000	na	na	2.000 2.000
0x94	PCIe5 NIC 3.3V	3.320	Volts	ok	na
3.140	na	na	3.460	na	0.040 0.040
0x95	PCIe5 NIC 1.2V	1.190	Volts	ok	

na							
1.140	na	na	1.260	na	0.020	0.020	
0x96	PCIe5 NIC 1.8V	1.790	Volts	ok	na		
1.710	na	na	1.890	na	0.020	0.020	
0x97	PCIe5 NIC 0.8V	0.800	Volts	ok			
na							
0.760	na	na	0.840	na	0.020	0.020	
0x33	PCIE Status	0x0	discrete	0x8000			
na							
na	na	na	na	na	na	na	
0x34	ACPI State	0x0	discrete	0x8001	na		
na	na	na	na	na	na	na	
0x35	Power Button	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x36	SysRestart	0x0	discrete	0x8080			
na							
na	na	na	na	na	na	na	
0x37	Boot Error	0x0	discrete	0x8000			
na							
na	na	na	na	na	na	na	
0x38	Watchdog2	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x39	UID Button	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x3a	PwrOk Sig. Drop	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x3b	PwrOn TimeOut	0x0	discrete	0x8000			
na							
na	na	na	na	na	na	na	
0x3c	BMC Boot Up	0x0	discrete	0x8002	na		
na	na	na	na	na	na	na	
0x3d	RTC Time	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x3e	Riser1 Card	0x0	discrete	0x8002	na		
na	na	na	na	na	na	na	
0x3f	Riser2 Card	0x0	discrete	0x8002			
na							
na	na	na	na	na	na	na	
0x40	System Notice	0x0	discrete	0x8000			
na							
na	na	na	na	na	na	na	
0x41	System Error	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x42	SysFWProgress	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x43	Mngmnt Health	0x0	discrete	0x8001			
na							
na	na	na	na	na	na	na	
0x44	BMC Time Hopping	0x0	discrete	0x8000			
na							
na	na	na	na	na	na	na	
0x45	NTP Sync Failed	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	
0x46	SEL Status	0x0	discrete	0x8000	na		
na	na	na	na	na	na	na	

0x47	Op. Log Full	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x48	Sec. Log Full	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x49	Host Loss	0x0	discrete	0x8000	
na	na	na	na	na	na
0x4a	Cert OverDue	0x0	discrete	0x8000	
na	na	na	na	na	na
0x4b	PwrCap Status	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x4c	PS1 Status	0x0	discrete	0x8001	na
na	na	na	na	na	na
0x4d	PS1 Temp Status	0x0	discrete	0x8000	
na	na	na	na	na	na
0x4e	CPU1 Status	0x0	discrete	0x8080	
na	na	na	na	na	na
0x4f	CPU2 Status	0x0	discrete	0x8080	na
na	na	na	na	na	na
0x50	CPU1 Memory	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x51	CPU2 Memory	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x52	CPU1 Prochot	0x0	discrete	0x8000	
na	na	na	na	na	na
0x53	CPU2 Prochot	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x54	DIMM000	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x55	DIMM001	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x56	DIMM010	0x0	discrete	0x8040	
na	na	na	na	na	na
0x57	DIMM011	0x0	discrete	0x8000	
na	na	na	na	na	na
0x58	DIMM020	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x59	DIMM021	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x5a	DIMM030	0x0	discrete	0x8040	
na	na	na	na	na	na
0x5b	DIMM031	0x0	discrete	0x8000	
na	na	na	na	na	na
0x5c	DIMM040	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x5d	DIMM041	0x0	discrete	0x8000	na
na	na	na	na	na	na

0x5e	DIMM050	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x5f	DIMM051	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x60	DIMM060	0x0	discrete	0x8040	
na					
na	na	na	na	na	na
0x61	DIMM061	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x62	DIMM070	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x63	DIMM071	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x64	DIMM100	0x0	discrete	0x8040	
na					
na	na	na	na	na	na
0x65	DIMM101	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x66	DIMM110	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x67	DIMM111	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x68	DIMM120	0x0	discrete	0x8040	
na					
na	na	na	na	na	na
0x69	DIMM121	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x6a	DIMM130	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x6b	DIMM131	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x6c	DIMM140	0x0	discrete	0x8040	
na					
na	na	na	na	na	na
0x6d	DIMM141	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x6e	DIMM150	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x6f	DIMM151	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x70	DIMM160	0x0	discrete	0x8040	
na					
na	na	na	na	na	na
0x71	DIMM161	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x72	DIMM170	0x0	discrete	0x8040	na
na	na	na	na	na	na
0x73	DIMM171	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x74	Memory Usage	0x0	discrete	0x8000	na
na	na	na	na	na	na

0x75	DISK24	0x0	discrete	0x8001	na
na	na	na	na	na	na
0x76	RTC Battery	0x0	discrete	0x8000	
na	na	na	na	na	na
0x77	FAN1 F Status	0x0	discrete	0x8000	
na	na	na	na	na	na
0x78	FAN1 R Status	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x79	FAN2 F Status	na	discrete	na	na
na	na	na	na	na	na
0x7a	FAN2 R Status	na	discrete	na	
na	na	na	na	na	na
0x7b	FAN3 F Status	0x0	discrete	0x8000	
na	na	na	na	na	na
0x7c	FAN3 R Status	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x7d	FAN4 F Status	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x7e	FAN4 R Status	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x7f	FAN5 F Status	0x0	discrete	0x8000	
na	na	na	na	na	na
0x80	FAN5 R Status	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x81	FAN6 F Status	na	discrete	na	na
na	na	na	na	na	na
0x82	FAN6 R Status	na	discrete	na	na
na	na	na	na	na	na
0x83	FAN7 F Status	0x0	discrete	0x8000	
na	na	na	na	na	na
0x84	FAN7 R Status	0x0	discrete	0x8000	
na	na	na	na	na	na
0x85	FAN1 F Presence	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x86	FAN1 R Presence	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x87	FAN2 F Presence	0x0	discrete	0x8001	
na	na	na	na	na	na
0x88	FAN2 R Presence	0x0	discrete	0x8001	
na	na	na	na	na	na
0x89	FAN3 F Presence	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x8a	FAN3 R Presence	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x8b	FAN4 F Presence	0x0	discrete	0x8000	na
na	na	na	na	na	na

0x8c	FAN4 R Presence	0x0	discrete	0x8000	na
na	na	na	na	na	na
0x8d	FAN5 F Presence	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x8e	FAN5 R Presence	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x8f	FAN6 F Presence	0x0	discrete	0x8001	na
na	na	na	na	na	na
0x90	FAN6 R Presence	0x0	discrete	0x8001	na
na	na	na	na	na	na
0x91	FAN7 F Presence	0x0	discrete	0x8000	
na					
na	na	na	na	na	na
0x92	FAN7 R Presence	0x0	discrete	0x8000	
na					
na	na	na	na	na	na

表6-2 传感器信息字段说明

字段	含义	举例说明	备注
sensor name	传感器名称	CPU1 Core Rem, 表示 CPU1 的核心温度传感器。	-
value	当前值	35.000, 表示当前传感器的值。	na, 表示当前传感器未检测到数值或状态, 可能当前传感器对应的设备不在位。
unit	当前值单位	degrees C, 表示单位为摄氏度。	discrete, 表示对应传感器为离散传感器, 没有单位。
status	状态	ok, 表示传感器正常。 nc, 表示传感器检测到轻微告警。 cr, 表示传感器检测到严重告警。 nr, 表示传感器检测到紧急告警。	na, 表示当前传感器未检测到数值或状态, 可能当前传感器对应的设备不在位。 0xXXX, 例如, 0x8000, 是根据 IPMI 规范定义的, 采用 16 进制数值表示当前传感器的状态, 具体含义请参见 IPMI 规范中表 42-2 Generic Event/Reading Type Codes 中字段 Generic Offset 的解释和表 42-3 Sensor Type Codes 中字段 Sensor specific Offset 的解释。
lnr	紧急下门限	na	na, 表示当前传感器不支持该门限值。
lc	严重下门限	na	na, 表示当前传感器不支持该门限值。
lnc	轻微下门限	na	na, 表示当前传感器不支持该门限值。
unc	轻微上门限	84.000, 表示当	na, 表示当前传感器不支持该门限值。

字段	含义	举例说明	备注
		前传感器正向轻微告警门限值是 84。	
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。

6.13.2 传感器测试命令（sensor -d test）

命令功能

test 命令用于模拟传感器状态或读数。

须知

测试之前请先使用 **ipmcget -t sensor -d list** 命令查询传感器状态，确保在传感器状态正常的情况下进行测试，否则已经故障告警的传感器在测试结束后会重复上报一次故障告警。

命令格式

ipmcset -t sensor -d test -v <sensorname/stopall> [value/stop]

参数说明

参数	参数说明	取值
sensorname/stopall	传感器名称	“sensorname”：传感器名称 “stopall”：停止所有测试

参数	参数说明	取值
<code>value/stop</code>	模拟值	“value”：传感器的测试模拟值 说明 执行该命令时，设置的值在 BMC 内部会进行转换，转换过程中容易造成精度丢失，故传感器的设置值与实际值之间存在误差。误差不会影响系统本身的运行，请以回显信息中的实际值为准。 “stop”：停止所有测试

使用指南

建议使用 [4.13.3 模拟事件（precisealarm）](#) 命令模拟告警。

使用实例

模拟 CPU1 Core Rem 传感器温度当前值为 100。

```
BMC:/->ipmcset -t sensor -d test -v "CPU1 Core Rem" 100
Sensor test successfully.
```

6.13.3 设置传感器使能状态（sensor -d state）

命令功能

sensor -d state 命令用于设置传感器的使能状态。

 说明

该命令只支持离散型传感器，不支持门限型传感器。

命令格式

```
ipmcset -t sensor -d state -v <sensorname> <enabled | disabled>
```

参数说明

参数	参数说明	取值
<code>sensorname</code>	传感器名称	<code>sensorname</code> ：传感器名称
<code>enabled disabled</code>	启用/禁用传感器	<code>enabled</code>：启用传感器 <code>disabled</code>：禁用传感器

使用指南

传感器默认为使能状态，禁用传感器后，传感器状态更新为“na”，不再产生新告警。

使用实例

```
# 启用传感器。

BMC:/->ipmcset -t sensor -d state -v "SEL_Status" enabled
Enable sensor successfully.

# 禁用传感器。

BMC:/->ipmcset -t sensor -d state -v "SEL_Status" disabled
Disable sensor successfully.
```

6.13.4 模拟事件（precisealarm）

命令功能

precisealarm 命令用于模拟 BMC 定义的事件。

命令格式

```
ipmcset -t precisealarm -d mock -v {eventcode|stopall} [subjectindex] eventstatus
```

参数说明

参数	参数说明	取值
eventcode	要模拟事件的事件码。	0xffffffff：表示模拟 BMC 定义的全部事件。 0x**ffffff：表示模拟事件主体类型为**的全部事件。 - 指定事件的事件码：表示模拟指定事件。 说明 - 事件码的第一个字节表示其事件主体类型。例如，事件码为“0x02000007”的告警，其事件主体类型为“02”，含义是“Disk”。 - 事件主体类型**的实际含义，可参考服务器告警处理文档中的详细描述。
stopall	停止事件模拟动作，取消所有模拟的事件。	-
subjectindex	要模拟的指定事件的事件主体类型代表的事件序号。	与模拟事件相关的事件序号。

参数	参数说明	取值
		事件序号获取方法如下： 1. 查询指定事件码下的所有事件。 2. 从获取到的信息中查看目标事件对应的事件序号。
<i>eventstatus</i>	模拟告警的状态。	- assert: 事件产生 - deassert: 事件恢复 - stop: 停止模拟

使用指南

- 当“eventcode”为“0xffffffff”和“0x**fffff”时，不可添加“subjectindex”参数。
- 当“eventcode”为指定事件码时，添加“subjectindex”参数可对指定的事件主体进行事件模拟。

使用实例

模拟事件码为“0x2C000025”的告警。

```
BMC:/->ipmcset -t precisealarm -d mock -v 0x2C000025 assert
Precise alarm mock successfully.
```

6.14 电源命令

介绍电源有关命令的查询和设置方法。

6.14.1 设置电源工作模式（psuworkmode）

命令功能

psuworkmode 命令用来设置电源工作模式。

命令格式

```
ipmcset -d psuworkmode -v <option> [active_psuid]
```

参数说明

参数	参数说明	取值
<i>option</i>	电源工作模式	0: 负载均衡模式

参数	参数说明	取值
		1: 主备模式 2: 深度休眠模式
<i>active_psuid</i>	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。

BMC:/->ipmcset -d psuworkmode -v 1 1
Set Power Work Mode (Active Standby) successfully
```

6.14.2 查询电源具体信息（psuinfo）

命令功能

psuinfo 命令用来获取电源信息。

命令格式

```
ipmcget -d psuinfo
```

参数说明

无

使用指南

无

使用实例

```
# 查询电源的信息。

BMC:/-> ipmcget -d psuinfo
Current PSU Information :
Current PSU Information :
Slot  Manufacturer      Type                SN                      Version
Rated Power  InputMode
1      DELTA             DPS-550AB-23  A    021312553LH1000053    DC:01c PFC:010
550      AC
Current PSU WorkMode      :
Actual PSU Status         :
```



```
Work Mode          : Load Balancing
Predicted PSU Status :
Work Mode          : Load Balancing
Hibernate Status    : Disabled
```

6.15 SOL 命令

介绍 SOL 有关命令的查询和设置方法。

6.15.1 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 BMC 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
<i>option</i>	表示要连接的串口，系统串口或 BMC 串口。	1：系统串口 2：BMC 串口
<i>mode</i>	表示 SOL 会话模式。	0：共享模式 - 选择共享模式时，可同时建立两路 SOL 会话，两路会话的内容共享，在任意一路 SOL 会话中的操作，对另一路会话可见。 1：独占模式 - 选择独占模式时，只允许同时存在一路 SOL 会话。

使用指南

在建立 SOL 会话连接到系统串口之前，请先在 OS 侧配置串口重定向功能。OS 侧的串口重定向配置方法，请查看各 OS 厂商提供的操作指导。

建立连接后，可轮流按下“Esc”和“(”退出当前 SOL 会话，返回命令行。按下“Esc”和“(”的时间间隔不允许超过 1 秒。

使用实例

```
# 建立 SOL 共享模式会话，连接系统串口。

BMC:/->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.
```

6.15.2 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
<i>index</i>	表示 SOL 会话序号。	“1”：会话 1 “2”：会话 2

使用指南

通过 IPMITOOL 建立的 SOL 会话不可注销。

使用实例

```
# 注销 SOL 会话。

BMC:/->ipmcset -t sol -d deactivate -v 1

Close SOL session successfully.
```

6.15.3 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 BMC 命令行界面。

命令格式

ipmcset -t sol -d timeout -v <value>

参数说明

参数	参数说明	取值
value	表示 SOL 会话用户无输入时，退出 SOL 会话的时间。	0 ~ 480，单位为分钟，取值为“0”时表示永不超时。 超时时间的默认取值为 15 分钟。

使用指南

无

使用实例

设置 SOL 会话超时时间为 20 分钟。

```
BMC:/->ipmcset -t sol -d timeout -v 20
Set SOL timeout period successfully.
```

6.15.4 查询 SOL 会话列表（sol -d session）

命令功能

sol -d session 命令用于查询 SOL 会话列表。

命令格式

ipmcget -t sol -d session

参数说明

无

使用指南

无

使用实例

查询 SOL 会话列表。

```
BMC:/->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

6.15.5 查询 SOL 会话配置信息（sol -d info）

命令功能

sol -d info 命令用于查询 SOL 会话配置信息，如查询 SOL 会话超时时间。

命令格式

ipmcget -t sol -d info

参数说明

无

使用指南

无

使用实例

查询 SOL 会话配置信息。

```
BMC:/->ipmcget -t sol -d info
Timeout Period (Min)      : 20
```

6.16 常用维护命令

6.16.1 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
<i>command</i>	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。

```
BMC:/->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.

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，只允许管理员和具有调试诊断权限的自定义用户使用。详细使用方法请参考 [《iBMC 高级命令参考》](#)。

获取 ping 命令的具体使用方法。

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

6.16.2 断开连接（exit）

命令功能

exit 命令用于断开客户端与 BMC 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。

```
BMC:/->exit  
Connection closed by foreign host.
```

6.16.3 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。

```
BMC:/->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
BMC:/->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
```

6.16.4 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

```
BMC:/->free
              total        used        free      shared    buffers
Mem:      125572        94780        30792          0        14780
Swap:            0           0           0
Total:    125572        94780        30792
```

6.16.5 netstat 命令（netstat）

命令功能

该命令用于执行 Linux 中的 netstat 命令。

命令格式

参考 Linux 中 `netstat` 命令的使用方法。

参数说明

支持 `netstat` 命令的所有参数。

使用指南

无

使用实例

```
BMC:/->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
```

6.16.6 df 命令（df）

命令功能

该命令用于执行 Linux 中的 `df` 命令。

命令格式

参考 Linux 中 `df` 命令的使用方法。

参数说明

支持 `df` 命令的所有参数。

使用指南

无

使用实例

```
BMC:/->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
```


6.16.7 ifconfig 命令（ifconfig）

命令功能

该命令用于执行 Linux 中的 ifconfig 命令。

命令格式

参考 Linux 中 ifconfig 命令的使用方法。

参数说明

只支持参数为 “lo”、“ethn”（n 为网口索引号）或 “-a”，或不带参数。

使用指南

无

使用实例

```
BMC:/->ifconfig eth1
eth1      Link encap:Ethernet  Addr
          inet6 addr: fe80::218:82ff:fe11:321/64 Scope:Link
          UP BROADCAST DEBUG RUNNING MTU:1500 Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1832 (1.7 KiB) TX bytes:2558 (2.4 KiB)
          Interrupt:28
```

6.16.8 route 命令（route）

命令功能

该命令用于执行 Linux 中的 route 命令。

命令格式

参考 Linux 中 route 命令的使用方法。

参数说明

-n : 不要使用通讯协定或主机名称，直接使用 IP 或端口号。

-e : 显示更多信息。

-A inet{6} : 选择地址族。

使用指南

无

使用实例

```
BMC:/->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
```

6.16.9 top 命令 (top)

命令功能

该命令用于执行 Linux 中的 top 命令。

命令格式

参考 Linux 中 top 命令的使用方法。

参数说明

不支持带参数。

使用指南

无

使用实例

```
BMC:/->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
```

6.16.10 禁止 CLP 超时（notimeout）

命令功能

notimeout 命令用于禁止 CLP 超时，确保可以在 CLP 命令行进行长时间操作。

命令格式

notimeout

参数说明

无

使用指南

该命令仅对当前会话窗口生效。

使用实例

禁止 CLP 命令行超时。

```
BMC:/->notimeout  
BMC:/->
```

7 常用操作

- 7.1 使用 PuTTY 登录服务器（串口方式）
- 7.2 使用 PuTTY 登录服务器（网口方式）
- 7.3 配置 WebUI Trap
- 7.4 配置 WebUI SMTP
- 7.5 配置目录服务功能
- 7.6 配置 BMC WebUI DNS（手动）
- 7.7 配置 SSH 用户密钥登录 BMC CLI
- 7.8 配置 SSL 证书
- 7.9 配置 Syslog 日志上报功能
- 7.10 使用 VNC 登录服务器实时桌面
- 7.11 导入信任证书和根证书

7.1 使用 PuTTY 登录服务器（串口方式）

操作场景

使用 PuTTY 工具，可以通过串口方式访问服务器，主要应用场景如下：

- 新建局点首次配置服务器时，本地 PC 机可以通过连接服务器的串口，登录服务器进行初始配置。
- 产品网络故障，远程连接服务器失败时，可通过连接服务器的串口，登录服务器进行故障定位。

必备事项

前提条件

- 已通过串口线缆连接 PC 与服务器。

- 已经安装 PuTTY，且 PuTTY 的版本为 0.68 及以上，推荐 0.76 及以上。

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。

数据

需准备如下数据：

登录待连接服务器的用户名和密码

操作步骤

步骤 1 双击“PuTTY.exe”。

弹出“PuTTY Configuration”窗口。

步骤 2 在左侧导航树中选择“Connection > Serial”。

步骤 3 设置登录参数。

参数举例如下：

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

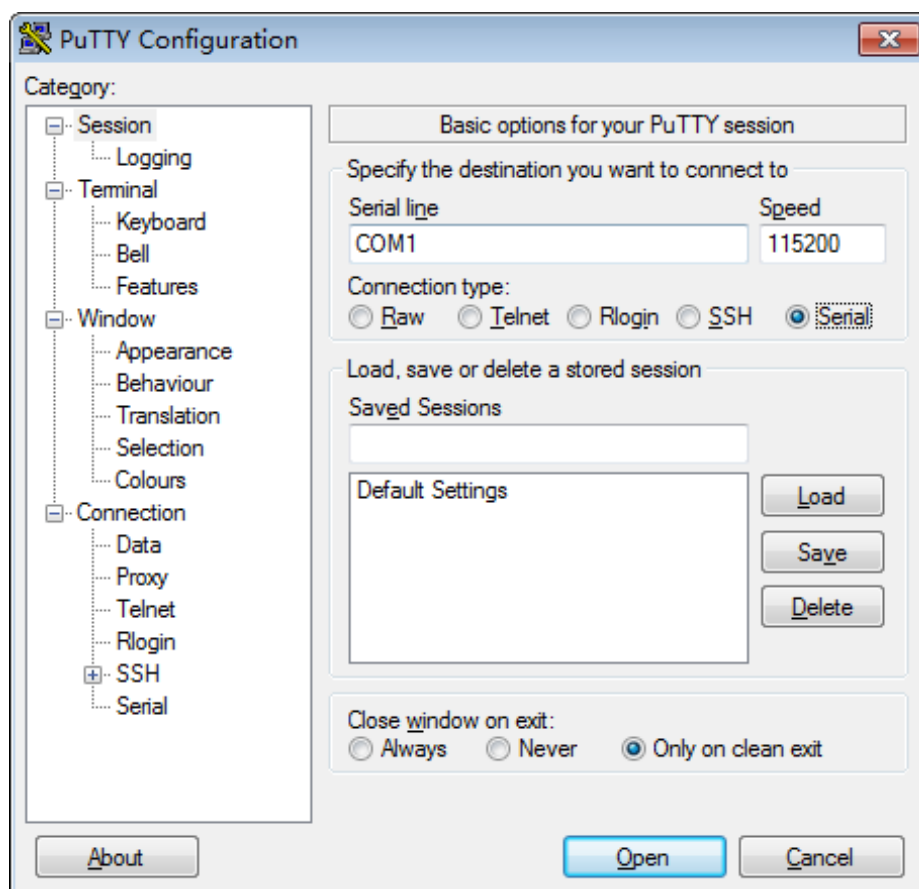
说明

n 表示不同串口的编号，取值为整数。

步骤 4 在左侧导航树中选择“Session”。

步骤 5 选择“Connection type”为“Serial”，如[图 7-1](#)所示。

图7-1 PuTTY Configuration



步骤 6 单击“Open”。

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

步骤 7 按提示分别输入用户名和密码。

登录完成后，命令提示符左侧显示出当前登录服务器的主机名。

----结束

7.2 使用 PuTTY 登录服务器（网口方式）

操作场景

使用 PuTTY 工具，可以通过局域网远程访问服务器，对服务器实施配置、维护操作。

必备事项

前提条件

- 已通过网线连接 PC 与服务器的管理网口。

- 已经安装 PuTTY，且 PuTTY 的版本为 0.68 及以上，推荐 0.76 及以上。

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。

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

操作步骤

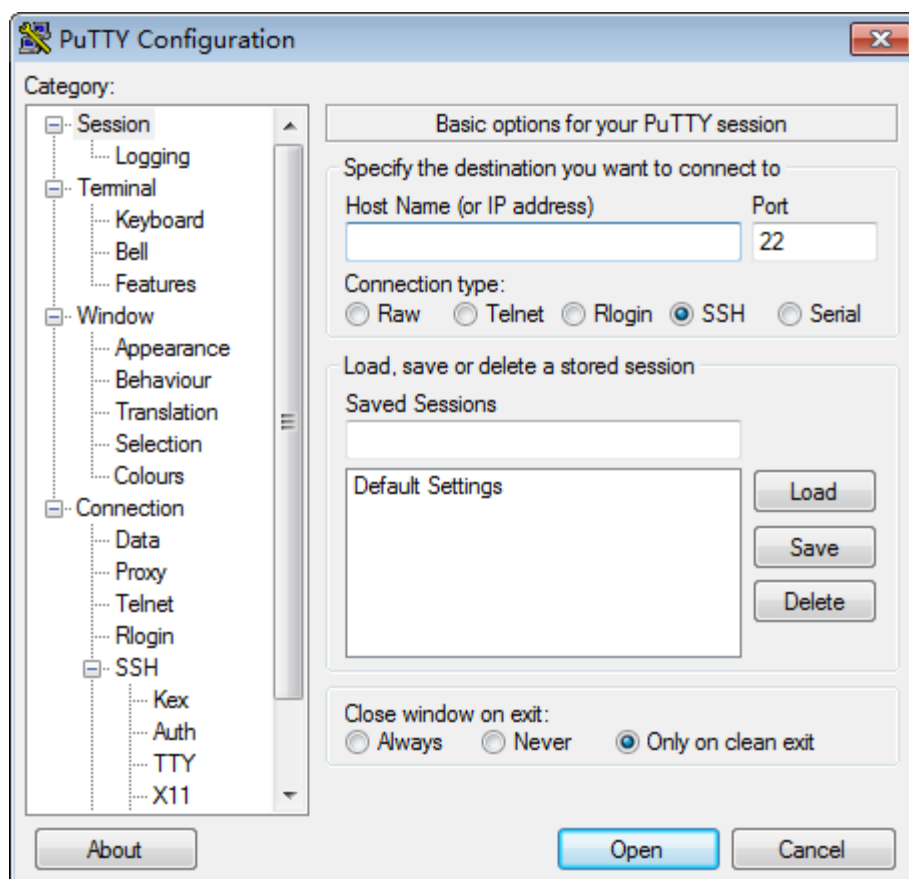
步骤 1 设置 PC 机的 IP 地址、子网掩码或者路由，使 PC 机能和服务器网络互通。

可在 PC 机的 cmd 命令窗口，通过 **Ping 服务器 IP 地址** 命令，检查网络是否互通。

步骤 2 双击“PuTTY.exe”。

弹出“PuTTY Configuration”窗口，如图 7-2 所示。

图7-2 PuTTY Configuration



步骤 3 填写登录参数。

参数说明如下：

- Host Name (or IP address): 输入要登录服务器的 IP 地址，如 “192.168.34.32”。
- Port: 默认设置为 “22”。
- Connection type: 默认选择 “SSH”。
- Close window on exit: 默认选择 “Only on clean exit”。

说明

配置 “Host Name” 后，再配置 “Saved Sessions” 并单击 “Save” 保存，则后续使用时直接双击 “Saved Sessions” 下保存的记录即可登录服务器。

步骤 4 单击 “Open”。

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

说明

- 如果首次登录该目标服务器，则会弹出 “PuTTY Security Alert” 窗口。单击 “是” 表示信任此站点，进入 “PuTTY” 运行界面。
- 登录服务器时，如果帐号输入错误，必须重新连接 PuTTY。

步骤 5 按提示分别输入用户名和密码。

登录完成后，命令提示符左侧显示出当前登录服务器的主机名。

----结束

7.3 配置 WebUI Trap

操作场景

WebUI 的 “维护诊断 > 告警上报” 提供 “Trap 功能”，可以设置 BMC 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 WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 选择“维护诊断 > 告警上报”。

步骤 3 在“Trap 报文通知”区域框，开启 Trap 功能。

步骤 4 设置 Trap 属性。

1. 在“Trap 版本”中，选择 Trap 方式上报事件需遵循的 SNMP Trap 协议版本。
SNMP Trap 协议提供“SNMPv1”、“SNMPv2c”和“SNMPv3”三种版本。
默认取值：“SNMPv1”。

说明

SNMPv1 和 SNMPv2c 版本由于自身机制而存在安全隐患，请尽量避免使用。建议使用 SNMPv3 版本的 SNMP Trap。

2. （可选）在“选择 V3 用户”下拉列表中，选择 Trap V3 协议使用的 BMC 用户。
3. 在“Trap 模式”中，选择 Trap 信息上报时，采用的 Trap 模式。
 - “精准告警模式(推荐)”：以与事件一一对应的 SNMP 节点 OID 作为 Trap 事件的标识，相较“OID 模式”和“事件码模式”，可提供更为精准的定位信息。
 - “OID 模式”：以 SNMP 节点的 OID 作为 Trap 事件的标识。
 - “事件码模式”：以产生事件的事件码作为 Trap 事件的标识。
4. 在“Trap 主机标识”中，选择 Trap 信息上报时，识别信息来源的主机标识。
“Trap 主机标识”提供“单板序列号”、“产品资产标签”和“主机名”三种主机标识。

步骤 5 设置告警发送级别。

步骤 6 设置 Trap 服务器和报文格式。

1. 选择发送告警通道。
在 WebUI 中，最多可以定义四个发送告警通道。
单击“编辑”，显示指定通道的编辑区域框。
2. 启用发送告警通道。
3. 输入接收 Trap 方式发送的告警信息的服务器地址。
服务器地址支持 IPv4 和 IPv6。
4. 输入接收 Trap 方式发送的告警信息的端口号。
默认取值：162。
5. 选择 Trap 格式中每个关键字段之间的分隔符。
6. 选择需要上报的关键字。
7. 选择显示 Trap 格式中每个关键字的名称。
8. 单击“保存”。
显示“操作成功”，表示 Trap 功能及其设置正式生效。
9. 单击“测试”。
显示“操作成功”，表示该通道可用。

----结束

7.4 配置 WebUI SMTP

操作场景

BMC WebUI 的“维护诊断 > 告警上报”提供“SMTP 功能”，可以将服务器产生的告警和事件以电子邮件方式，通过 SMTP 服务器转发到目标邮箱。

必备事项

数据

进行配置之前，请先规划好配置过程中所需数据：

- SMTP 服务器的地址。
- 发件人邮件信息。
 - 发件人用户名和密码
 - 发件人邮件地址
 - 邮件主题
- 收件人邮件信息。
 - 接收人邮件地址
 - 接收人邮件地址描述信息

操作步骤

步骤 1 登录 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 选择“维护诊断 > 告警上报”。

步骤 3 在“邮件通知”区域框，开启 SMTP 功能。

步骤 4 输入 SMTP 服务器的地址。

SMTP 服务器的 IPv4 或 IPv6 地址。

步骤 5 选择是否启用 TLS 功能。

- 设置启用 TLS（Transport Layer Security）加密传输。
- 不启用 TLS 时，采用明文传输。

说明

- 默认情况下，SMTP 支持 TLS 加密，从安全性考虑，建议启用 TLS 加密。
- 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 BMC 系统向 SMTP 服务器发送告警信息邮件时使用。

说明

默认情况下，SMTP 服务器不使用匿名，从安全性考虑，请尽量不要使用匿名。

步骤 7 设置邮件信息。

1. 输入发件人用户名及密码。

说明

- “是否使用匿名”选择“是”时，不需要验证用户名及其密码。
- 如果使用电子邮箱服务的用户在 SMTP 服务器端修改了密码，请在登录“告警设置”界面后，在“发件人密码”文本框中重新输入修改后的密码。

2. 输入发件人邮件地址。
3. 输入邮件主题。

SMTP 邮件主题提供主题附带功能，可以选择“主机名”、“单板序列号”和“产品资产标签”作为邮件主题的附加内容。

步骤 8 设置告警发送级别。

步骤 9 启用接收告警的邮件地址。

1. 输入接收告警邮件地址。
2. 输入接收告警邮件地址的描述信息。

步骤 10 单击“保存”。

显示“操作成功”，表示 SMTP 功能及其设置正式生效。

步骤 11 单击“测试”，显示“操作成功”。

显示“操作成功”，表示测试邮件已正常发送，请在接受告警的邮箱进行验证。

---结束

7.5 配置目录服务功能

7.5.1 配置目录服务器

配置 LDAP 功能时，BMC 支持与 Windows AD 和 Linux OpenLDAP 的对接；配置 Kerberos 功能时，BMC 支持与 Windows AD 的对接。

此处以 Windows Server 2012 R2 Enterprise 为例说明目录服务器的简要配置过程。如果已存在可正常使用的目录服务器，请忽略此章节。

前提条件

- 用于搭建目录服务器的设备（如服务器）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

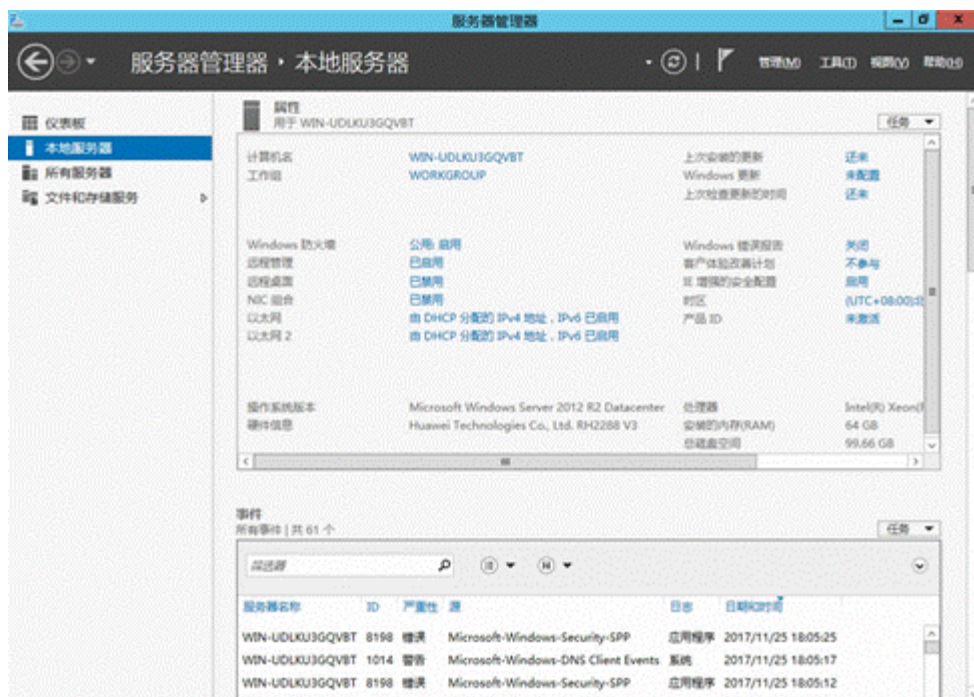
步骤1 安装操作系统。

1. 通过服务器 BMC 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 BMC 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。

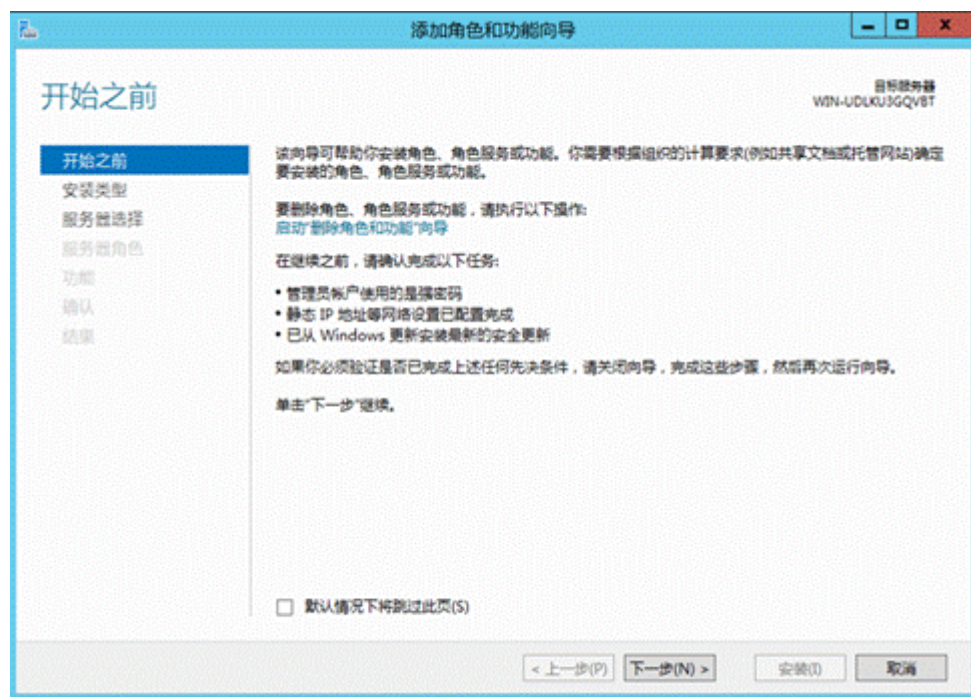
1. 在“开始”菜单中选择服务器管理器。
打开“服务器管理器”。
2. 在左侧导航树中选择“本地服务器”。
右侧显示本地服务器的“属性”窗口，如图 7-3 所示。

图7-3 本地服务器属性



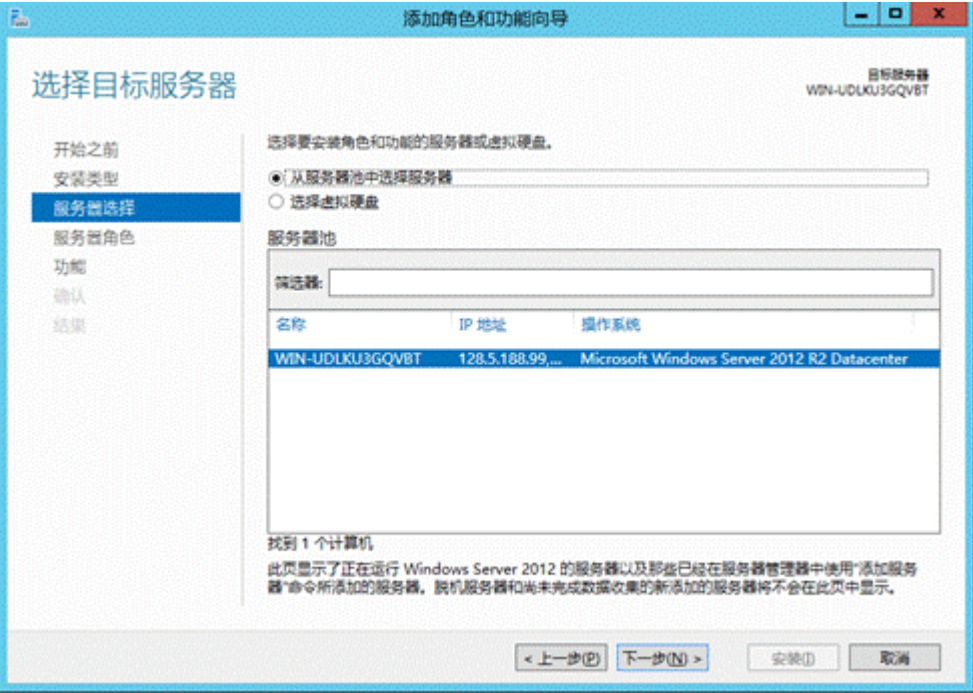
- 在右上角的“管理”菜单中选择“添加角色和功能”。
打开“添加角色和功能向导”，如图 7-4 所示。

图7-4 添加角色和功能向导



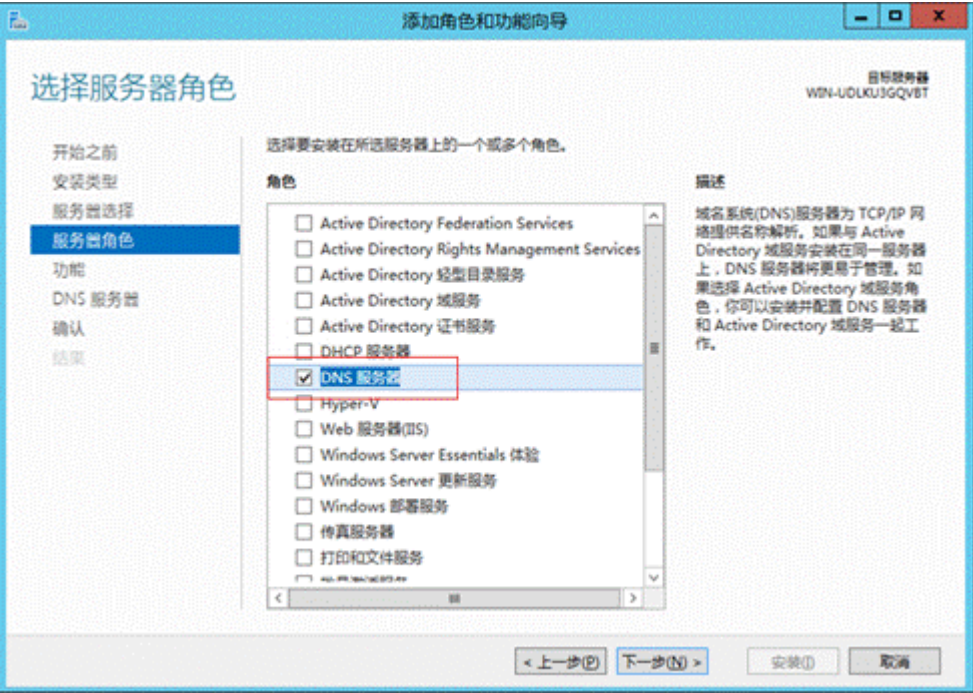
4. 单击“下一步”。
- 进入“安装类型”选择界面。
5. 选择“基于角色或基于功能的安装”，并单击“下一步”。
- 进入“服务器选择”界面，如图 7-5 所示。

图7-5 选择目标服务器



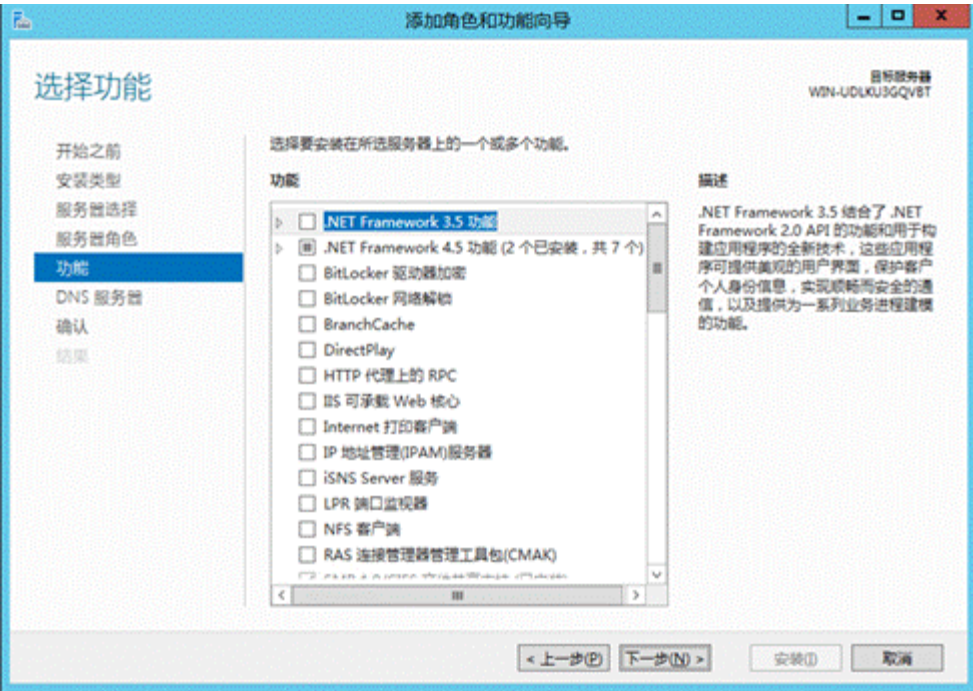
6. 选择“从服务器池中选择服务器”，并在“服务器池”中选择本机后，单击“下一步”。
- 进入“选择服务器角色”界面，如图 4 选择服务器角色所示。

图7-6 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 7-7 所示。

图7-7 选择功能



- 10. 勾选“.NET Framework 4.5 功能”并单击“下一步”。
打开“DNS 服务器”界面。
- 11. 单击“下一步”。
打开操作确认界面。
- 12. 单击“安装”。
显示 DNS 服务安装进度条。
- 13. 安装完成后单击“关闭”。
返回“本地服务器”界面。

步骤 3 安装 AD 服务。

参考步骤 2，继续添加新服务。

- 1. 在如图 6-7 所示界面中勾选“Active Directory 域服务”。
弹出操作确认窗口。
- 2. 单击“添加功能”。

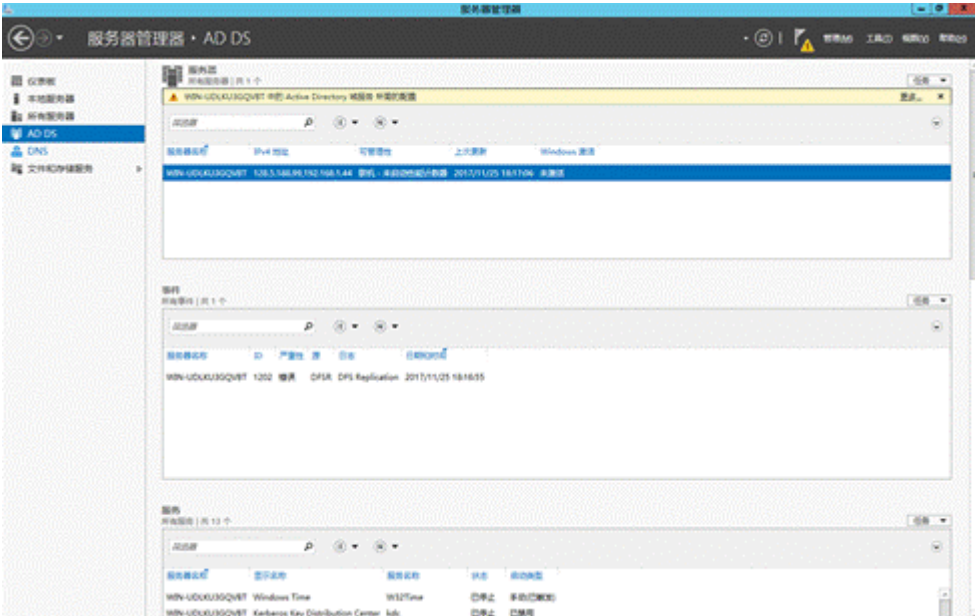
返回“选择服务器角色”界面。

3. 单击“下一步”。
打开“选择功能”界面。
4. 勾选“.NET Framework 4.5 功能”并单击“下一步”。
打开“Active Directory 域服务”界面。
5. 单击“下一步”。
打开操作确认界面。
6. 单击“安装”。
显示 Active Directory 域服务安装进度条。
7. 安装完成后单击“关闭”。
返回“本地服务器”界面。

步骤 4 配置 AD 服务。

1. 在“服务器管理器”左侧导航树中选择“AD DS”。
右侧显示“AD DS”属性，如图 7-8 所示。

图7-8 AD DS 属性



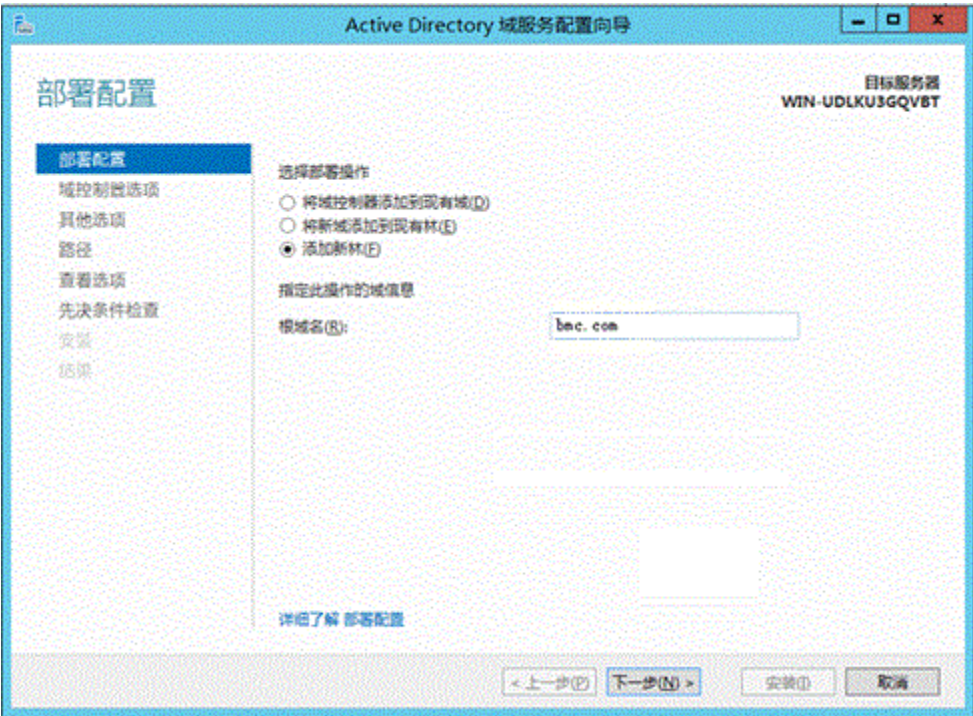
2. 单击页面右上方告警信息中的“更多...”。
打开“所有服务器任务详细信息”窗口，如图 7-9 所示。

图7-9 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 7-10 所示。

图7-10 Active Directory 域服务配置向导

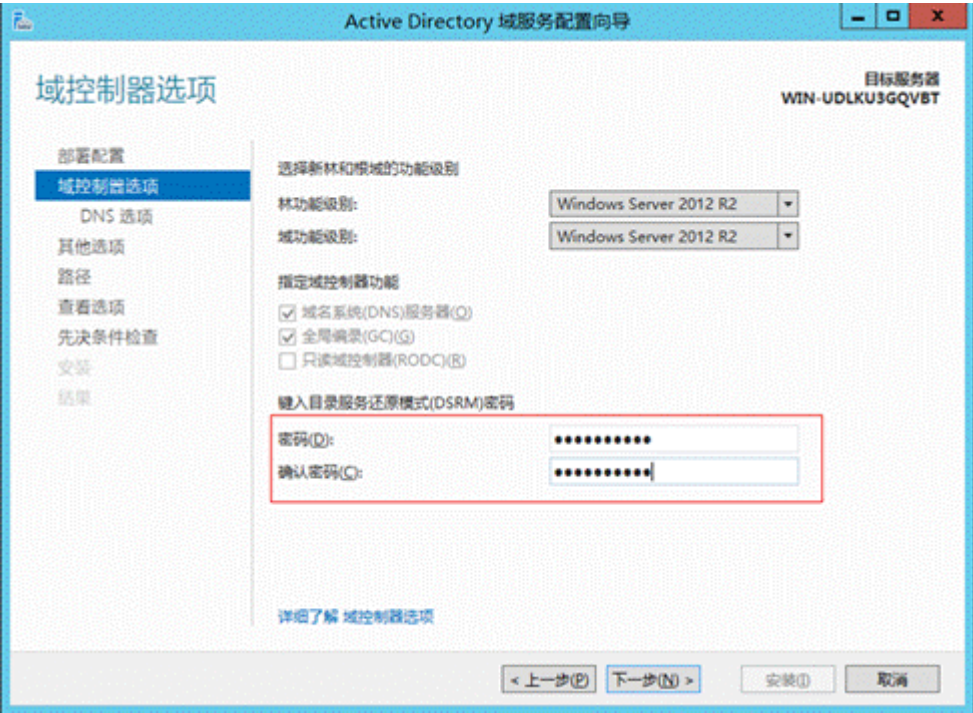


4. 选择“添加新林”并在“根域名”后的文本框中输入 AD 域名（例如“example.com”），单击“下一步”。
- 打开“域控制器选项”界面，如图 7-11 所示。

 说明

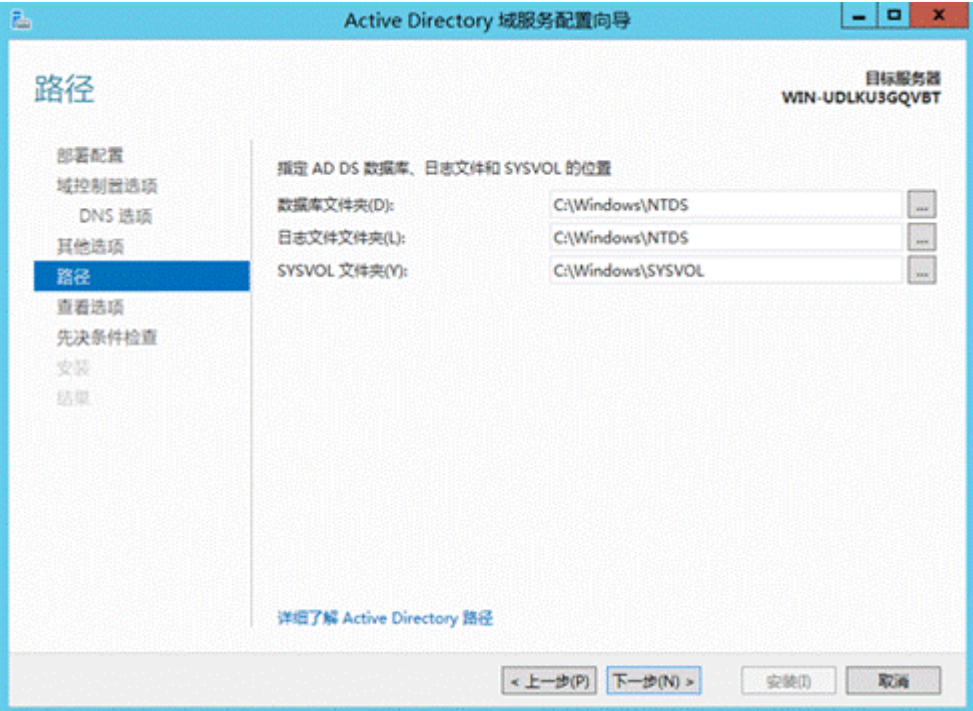
域名字符区分大小写，配置时请严格按照规划的域名来输入。

图7-11 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 7-12 所示界面。

图7-12 域服务路径

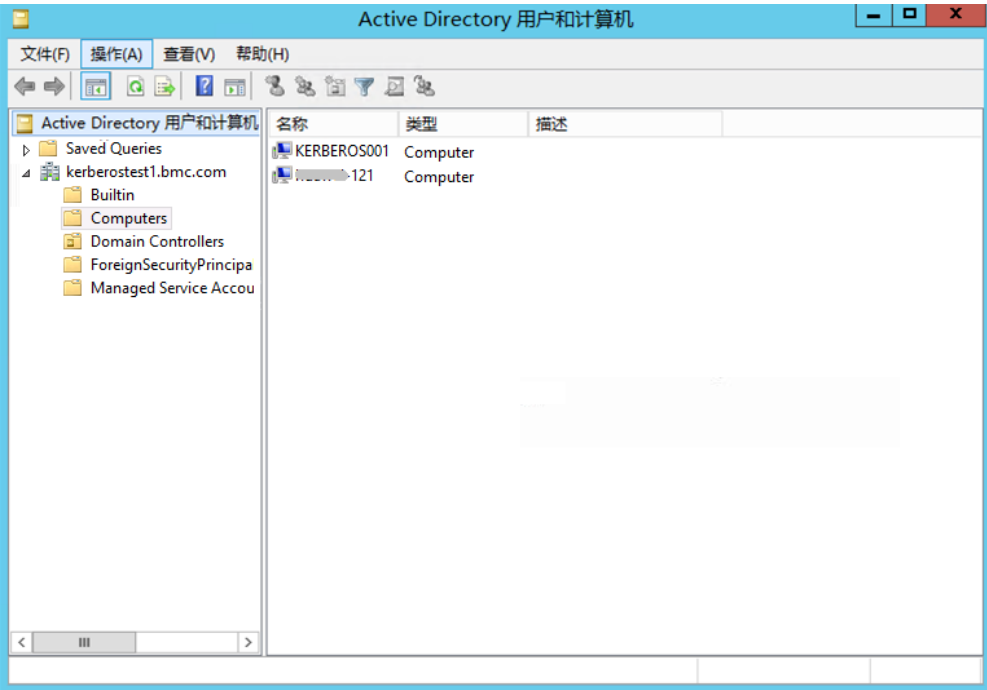


- 7. 按照实际需求设置 AD 域服务相关路径，单击“下一步”。
您也可以保持默认配置，不做修改。
- 8. 在后续页面中依次单击“下一步”。
- 9. 当出现“先决条件检查”界面时，单击“安装”。
AD 域服务配置完成后，操作系统将自动重启。

步骤 5（对于 LDAP 功能为非必选步骤）配置 AD 主机名。

- 1. 在“服务器管理器”页面右上方的工具栏中单击“工具”，在下拉菜单中选择“Active Directory 用户和计算机”。
- 2. 在“Active Directory 用户和计算机”左侧导航树中选择“Computers”。
右侧显示主机名列表，如图 7-13 所示。

图7-13 配置 AD 主机名路径



3. 在主机名列表空白处单击鼠标右键，新建主机名，例如“host”。

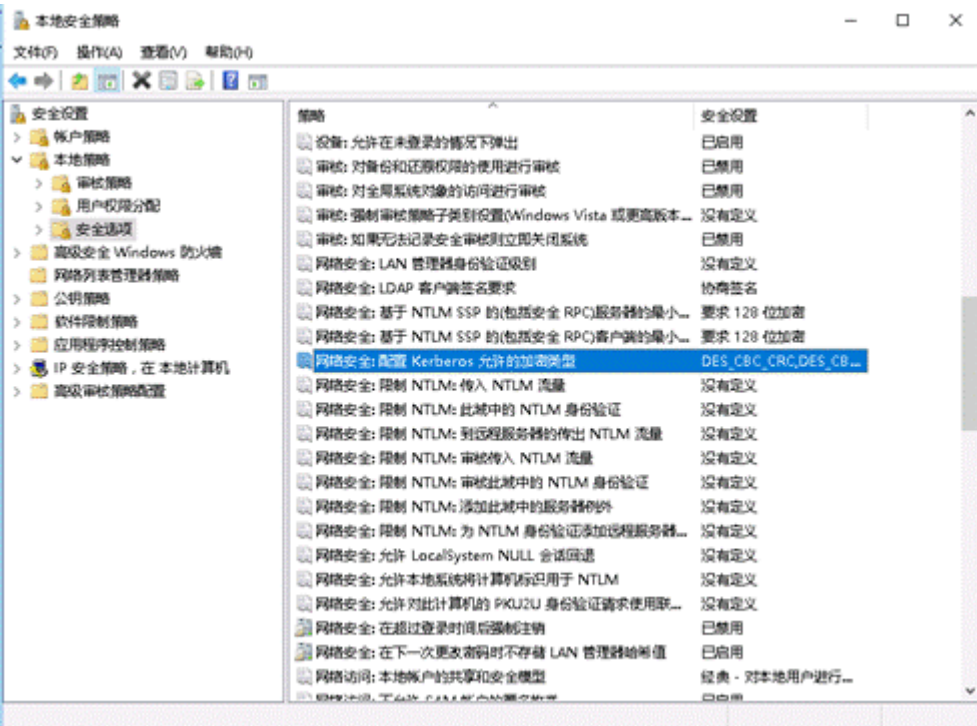
说明

此处新建的主机名为后续在 BMC WebUI 配置主机名时可使用的主机名，请做好记录。BMC WebUI 配置主机名步骤请参见本文档 7.5.3 配置 Kerberos 功能 章节的步骤 1。

步骤 6（对于 LDAP 功能为非必选步骤）配置 AD 域支持的加密算法。

- 1. 在“服务器管理器”页面右上方的工具栏中单击“工具”，在下拉菜单中选择“本地安全策略”。
- 2. 在“本地安全策略”左侧导航树中选择“本地策略 > 安全选项”，右侧显示安全策略类型，如图 7-14 所示。

图7-14 配置本地安全策略



- 3. 在右侧安全策略类型中，选中““网络安全：配置 Kerberos 允许的加密类型””并单击鼠标右键，在下拉菜单中选择“属性”，打开属性列表。
- 4. 确保勾选“本地安全设置”中的以下加密算法：
 - AES128_HMAC_SHA1
 - AES256_HMAC_SHA1

说明

对于跨域场景登录，还需要配置域间的信任关系，才能确保安全的加密算法可以认证成功。

步骤 7（对于 LDAP 功能为非必选步骤）在 AD 域配置服务端支持的加密算法。

- 1. 在“服务器管理器”页面右上方的工具栏中单击“工具”，在下拉菜单中选择“ADSI 编辑器”。
- 2. 在“ADSI 编辑器”左侧导航树中选择“Computers”。
右侧显示主机名列表。
- 3. 选中待操作的主机名并单击鼠标右键，在下拉菜单中选择“属性”，打开属性列表。
- 4. 在属性列表中选中“msDS-SupportedEncryptiontypes”。
- 5. 单击“编辑”，打开“整数属性编辑器”并在输入框中输入服务端支持的加密算法对应的数值。

 说明

客户端支持的加密算法只有 **AES128-CTS-HMAC-SHA1-96** 和 **AES256-CTS-HMAC-SHA1-96**，根据表 7-1 **加密算法取值与代表的加密算法类型关系表**，分别对应取值为 **8** 和 **16**。因为服务端配置的加密算法必须与客户端支持的加密算法配置成一致才能保证协商成功，因此此处的加密算法取值根据实际情况必须配置为 **8**、**16** 或 **24**。

表7-1 加密算法取值与代表的加密算法类型关系表

加密算法取值	代表的加密算法类型
8	AES128-CTS-HMAC-SHA1-96
16	AES256-CTS-HMAC-SHA1-96
24	AES128-CTS-HMAC-SHA1-96 和 AES256-CTS-HMAC-SHA1-96

6. 单击“确认”。

步骤 8（对于 LDAP 功能为非必选步骤）生成密钥表。

1. 在 AD 域服务中打开 cmd。
2. 使用 **ktpass** 命令生成密钥表。

 说明

建议使用 **ktpass** 命令生成密钥表时，使用 **AES128-CTS-HMAC-SHA1-96** 或 **AES256-CTS-HMAC-SHA1-96** 加密算法，且使用的加密算法类型必须与服务端实际使用的加密算法类型保持一致，即：

- 若服务端加密算法取值配置为 **8**，必须使用 **AES128-CTS-HMAC-SHA1-96** 加密算法生成密钥表。
- 若服务端加密算法取值配置为 **16** 或 **24**，必须使用 **AES256-CTS-HMAC-SHA1-96** 加密算法生成密钥表。

使用示例：

```
C:\Users\Administrator>ktpass -out c:\kerberos\admin.keytab +rndPass -ptype
KRB5_NT_SRV_HST -mapuser admin$@it.example.com -princ
HTTP/admin.it.example.com@IT.example.com -crypto AES128-SHA1
Targeting domain controller: WIN-D0VNHFBDLC.it.example.com
Successfully mapped HTTP/admin.it.example.com to ADMIN$.
WARNING: Account ADMIN$ is not a user account (uacflags=0x1021).
WARNING: Resetting ADMIN$'s password may cause authentication problems if
ADMIN$ is being used as a server.

Reset ADMIN$'s password [y/n]? y
Password succesfully set!8
Key created.Output keytab to c:\kerberos\admin.keytab:
Keytab version: 0x502
keysize 86 HTTP/admin.it.example.com@IT.example.com ptype 3 (KRB5_NT_SRV_HST)
vno 3 etype 0x11 (AES128-SHA1) keylength 16
(0xd517c317bf1a6f333a45f3282d0b69a9)
```

步骤 9 安装 CS 服务。

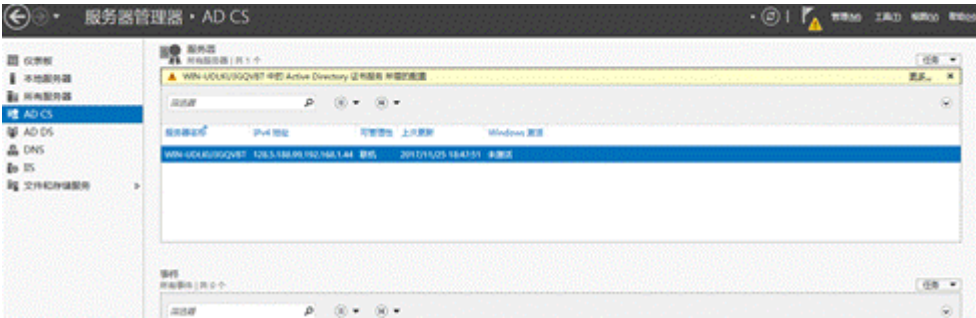
参考[安装 DNS 服务](#)，继续添加新服务。

1. 在如图 7-7 所示界面中勾选“Active Directory 证书服务”。
弹出操作确认窗口。
2. 单击“添加功能”。
返回“选择服务器角色”界面。
3. 单击“下一步”。
打开“选择功能”界面。
4. 勾选“.NET Framework 4.5 功能”并单击“下一步”。
打开“AD CS”界面。
5. 单击“下一步”。
打开“选择角色服务”界面。
6. 勾选“证书颁发机构”和“证书颁发机构 Web 注册”并单击“下一步”。
弹出操作确认窗口。
7. 单击“添加功能”。
返回“选择角色服务”界面。
8. 连续单击“下一步”。
9. 在“确认安装所选内容”界面单击“安装”。
显示 CS 服务安装进度条。
10. 安装完成后单击“关闭”。

步骤 10 配置 CS 服务。

1. 返回“服务器管理器”主界面。
2. 在左侧导航树中选择“AD CS”。
右侧显示“AD CS”属性，如图 7-15 所示。

图7-15 AD CS 属性



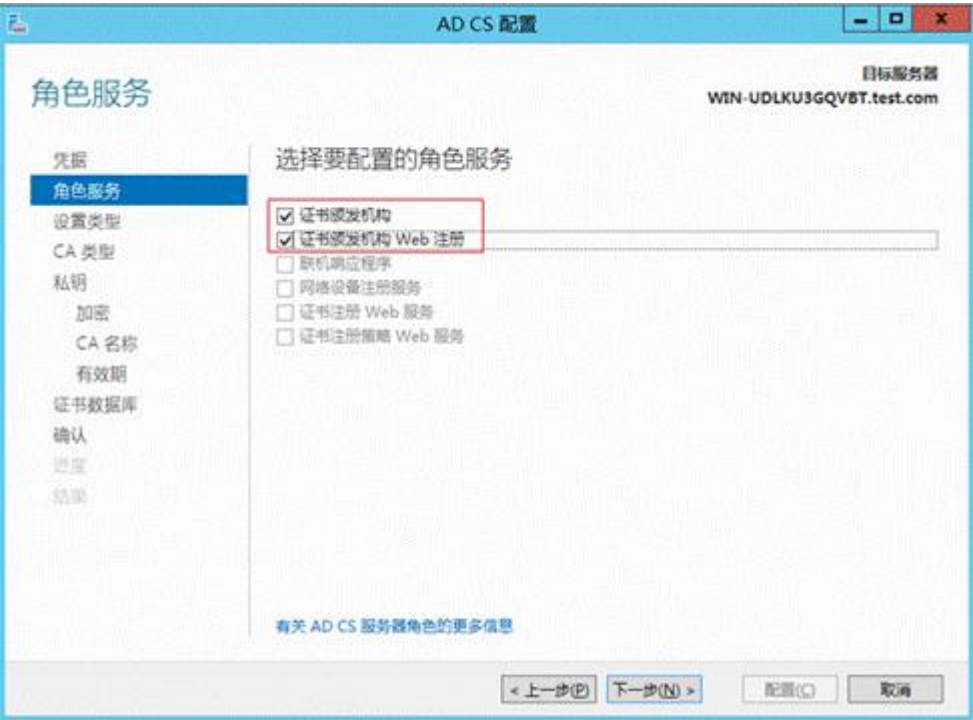
3. 单击页面右上方告警信息中的“更多...”。
打开“所有服务器任务详细信息”窗口，如图 7-16 所示。

图7-16 所有服务器任务详细信息



- 4. 单击“配置目标服务器上的 Active Directory 证书服务”。
打开“AD CS 配置”界面。
- 5. 单击“下一步”。
打开“角色服务”界面，如图 7-17 所示。

图7-17 角色服务



- 6. 勾选“证书颁发机构”和“证书颁发机构 Web 注册”，单击“下一步”。

打开“设置类型”界面。

7. 勾选“企业 CA”，单击“下一步”。

打开“CA 类型”界面。

8. 勾选“根 CA”，单击“下一步”。

打开“私钥”界面。

9. 勾选“创建新的私钥”，单击“下一步”。

打开“CA 的加密”界面，如图 7-18 所示。

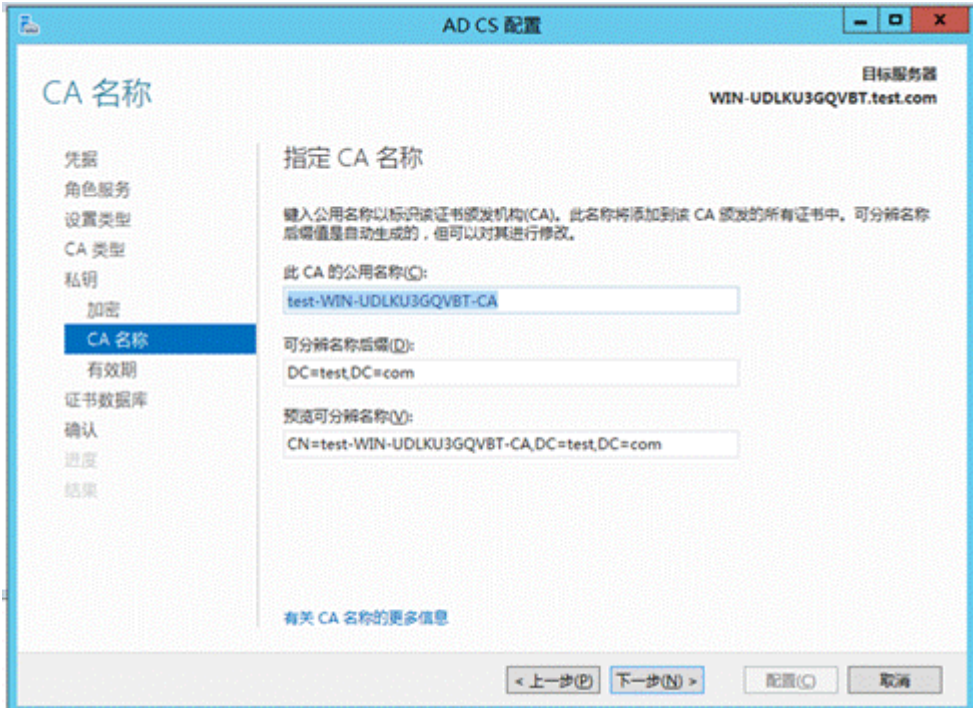
图7-18 CA 的加密



10. 指定加密提供程序为“RSA”、密钥长度为“2048”、哈希算法为“SHA1”，单击“下一步”。

打开“CA 名称”界面，如图 7-19 所示。

图7-19 CA 名称



11. 按照规划，设置“此 CA 的公用名称”，单击“下一步”。
打开“有效期”界面。
12. 按照实际需要设置有效期，单击“下一步”。
打开“CA 数据库”界面。
13. 指定 CA 数据库的路径，单击“下一步”。
打开“确认”界面。
14. 单击“配置”。
显示 AD 证书服务配置进度条。
15. 配置完成后，单击“关闭”。

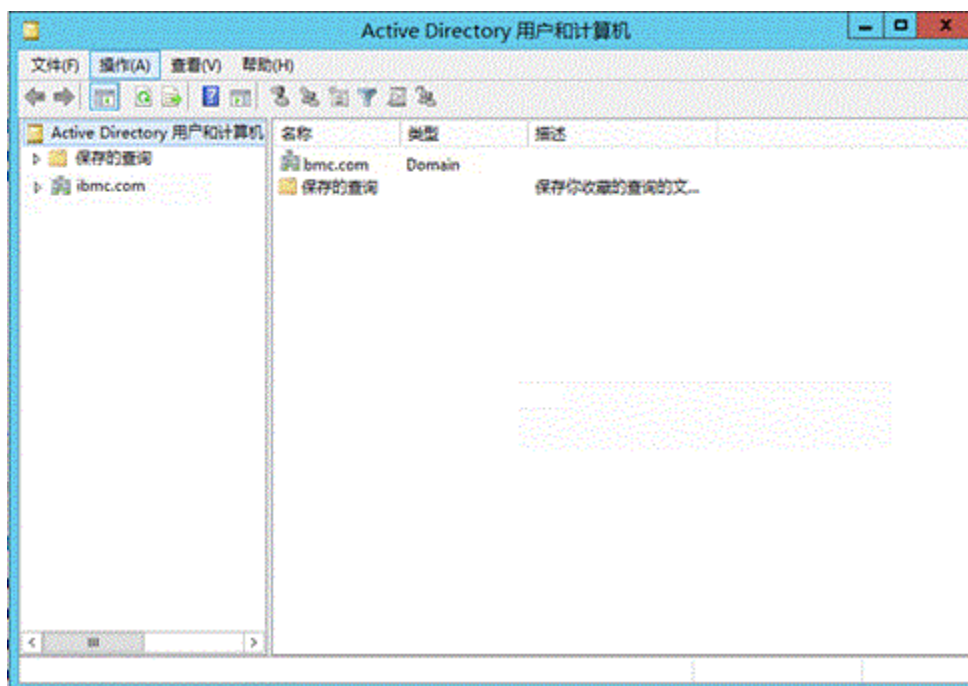
步骤 11 重启服务器使配置生效。

步骤 12 新建组织单位。

您可以根据实际需要在服务器上规划新的组织单位，可以在任意节点下新建组织单位，下面以新建一级节点及其子节点为例进行说明。

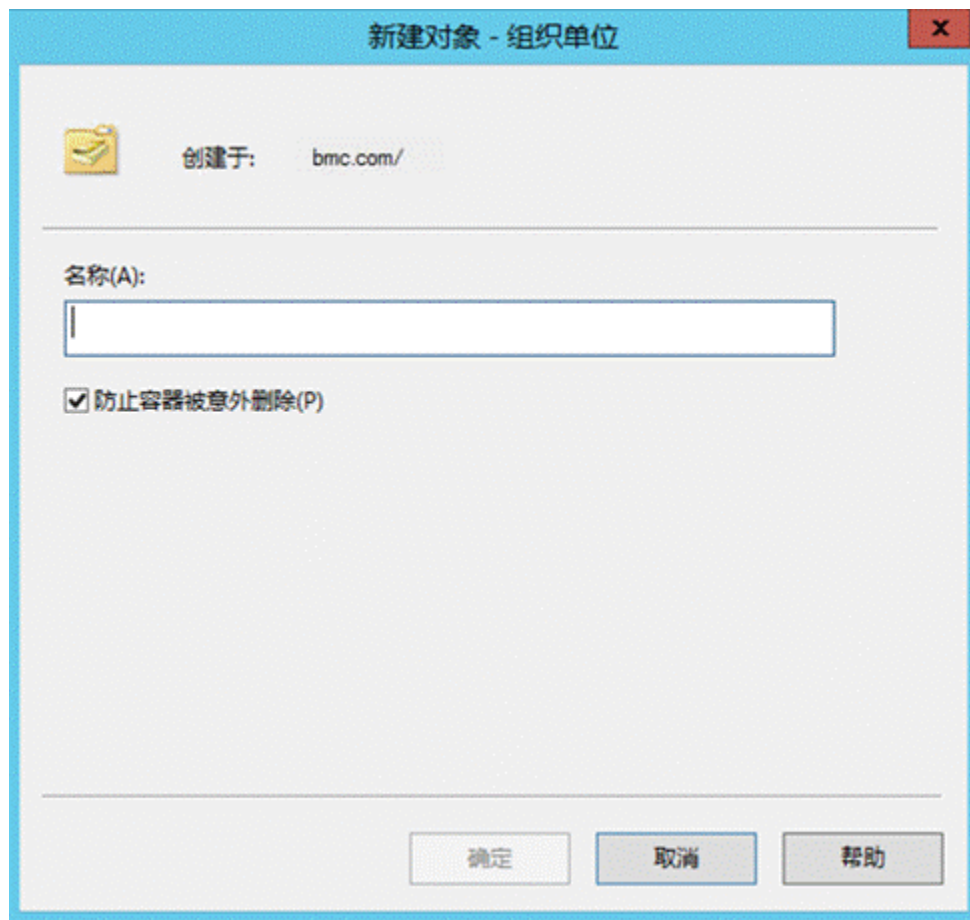
1. 登录服务器操作系统。
2. 在“服务器管理器”左侧导航树中选择“本地服务器”。
3. 在页面右上角的“任务”下拉列表中选择“Active Directory 用户和计算机”。
打开域的服务组件，如图 7-20 所示。

图7-20 服务器管理器



4. 右键单击服务器的顶级节点（如“example.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 7-21](#) 所示。

图7-21 新建组织



新建对象 - 组织单位

创建于: bmc.com/

名称(A):

☒ 防止容器被意外删除(P)

确定 取消 帮助

5. 在“名称”文本框中输入组织名称（例如“company”），单击“确定”。
在服务器的组织中，可看到新建的组织（例如“company”）。
6. 右键单击新创建的组织（例如“company”）打开操作菜单，并选择“新建 > 组织单位”，创建子组织（例如“department”）。
创建完成后，可在一级节点下，看到新建的子节点。
7. 可根据实际需求，重复[步骤 12.4](#)～[步骤 12.6](#)，创建多个组织单位。

步骤 13 新建组。

您可以根据实际需求，在任意节点下新建组。

1. 右键单击要创建组的节点（例如“department”）打开操作菜单，并选择“新建 > 组”。
打开新建组窗口，如[图 7-22](#)所示。

图7-22 新建组

新建对象 - 组

创建于: bmc.com/company/department

组名(A):

组名(Windows 2000 以前版本)(W):

组作用域

☐ 本地域(O)

☒ 全局(G)

☐ 通用(U)

组类型

☒ 安全组(S)

☐ 通讯组(D)

确定 取消

- 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”）。

- 可根据实际需要，重复步骤 13.1～步骤 13.b，创建多个组。

步骤 14 新建用户。

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

- 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”。
- 在打开的“新建角色-用户”窗口中，输入新用户信息，如图 7-23 所示。

说明

其中，“用户登录名”为后续登录 BMC WebUI 时可使用的域名，此处请做好记录。

图7-23 新建用户

新建对象 - 用户

创建于: bmc.com/Users

姓(L):

名(F): 英文缩写(I):

姓名(A):

用户登录名(U):

用户登录名(Windows 2000 以前版本)(W):

< 上一步(B) 下一步(N) > 取消

- 单击“下一步”。
- 弹出密码设置窗口，如[图 7-24](#)所示。

图7-24 设置密码

新建对象 - 用户

创建于: test.com/Users

密码(P):

确认密码(C):

☐ 用户下次登录时须更改密码(M)

☐ 用户不能更改密码(S)

☐ 密码永不过期(W)

☐ 帐户已禁用(Q)

< 上一步(B) 下一步(N) > 取消

4. 在“密码”和“确认密码”的文本框中输入密码（例如“Admin@9000”），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 15 将用户添加到组。

可以通过对组的操作来添加用户，也可以通过对用户操作来添加到组，此处以对用户操作为例进行说明。

1. 右键单击步骤 10 中创建的用户（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 7-25 所示。

图7-25 选择组



- 2. 在“输入对象名称来选择”文本框中输入要加入的组名（例如“info_group1”），单击“确定”。
- 提示操作成功。
- 3. 可根据实际需要，重复上述操作，可将多个用户添加到组。

----结束

7.5.2 配置 LDAP 功能

操作场景

BMC WebUI 的“LDAP”提供“LDAP 用户组”功能，设置 LDAP 用户后，可以直接使用 LDAP 用户访问 BMC。

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。BMC 系统仅提供 LDAP 用户的接入功能。
- 启用 LDAP 功能，使用 LDAP 帐户登录 BMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。

必备事项

数据

- 可用的 LDAP 服务器信息，包括 LDAP 服务器地址、域名、主机名、用户应用文件夹以及 LDAP 用户所属角色组的名称。
- BMC 当前用户的密码。

操作步骤

步骤 1 登录 WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 配置 LDAP 服务器信息。

1. 选择“用户&安全 > LDAP”。
2. 单击“LDAP 使能”后的 ，此按钮变为 ，表示 LDAP 功能已经启用。
3. 配置 LDAP 服务器参数。
必须配置的参数包括：
 - 输入 LDAP 服务器的 IP 地址，如“192.168.66.66”。
 - 输入 LDAP 服务器端口号。
 - 输入 LDAP 服务器的域名，如“example.com”，域名和 LDAP 服务器下的域名保持一致。
 - 输入当前登录 BMC 的用户密码。其它参数请根据实际需要进行设置。相关参数说明请参考“LDAP”章节。
4. 单击“保存”。

步骤 3（可选）导入 LDAP CA 证书

若开启了证书验证功能，需要导入 LDAP CA 证书。请用户自行从 CA 证书颁发机构获取证书文件。

1. 配置 BMC WebUI DNS 地址为 LDAP 服务器地址，详细操作请参见“LDAP”章节。
2. 单击“上传证书”后的“浏览”，选择要上传的根证书，证书支持.cer、.pem、.cert 和.crt 格式，最大不超过 1MB。
3. 单击“上传”，上传成功后，证书状态会显示 LDAP CA 证书已上传。

说明

请定期更新证书，否则可能存在安全风险。

步骤 4 配置 LDAP 组信息

1. 在“LDAP 用户组”区域单击“添加组”或“编辑”，进入“添加组”或“修改组”编辑区域框。
2. 输入 BMC 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 [7.5.1 配置目录服务器](#)中创建的 LDAP 组）。

- 输入 LDAP 组应用所在文件夹。
和 LDAP 服务器下用户的组所在的组织单位名保持一致，如“company/department”（即 [7.5.1 配置目录服务器](#)中涉及的最下层组织单位），最大长度为 255。
- 选择已设定的登录规则。
- 选择登录接口。
- 选择 LDAP 组权限。

4. 单击“保存”。

步骤 5 使用域帐号登录 BMC

1. 输入已在 LDAP 服务器生效的帐号密码，例如“info/Admin@9000”。
2. 在域名下拉列表，选择对应 LDAP 服务器的域名，例如“example.com”。
3. 单击“登录”。

---结束

7.5.3 配置 Kerberos 功能

操作场景

BMC WebUI 的“Kerberos”提供“Kerberos 用户组”功能，设置 Kerberos 用户后，可以直接使用 Kerberos 用户访问 BMC。

说明

- Kerberos 是一种网络认证协议，通过密钥系统为客户机或服务器应用程序提供强大的认证服务。
- BMC 系统仅提供 Kerberos 用户的接入功能。
- 启用 Kerberos 功能，使用 Kerberos 帐户登录 BMC 时，该帐户相关的安全策略（密码检查、密码有效期、密码最短使用期限、不活动期限、禁用历史密码、登录失败锁定）由认证服务端配置。

必备事项

数据

- 可用的 Kerberos 服务器信息，包括 Kerberos 服务器地址、领域以及 Kerberos 用户所属角色组的名称。
- 在 Windows AD 中，为 BMC 生成密钥表文件。生成密钥表的详细操作请参见本文档 [7.5.1 配置目录服务器](#)的步骤 8。
- BMC 当前用户的密码。

操作步骤

步骤 1 配置 BMC 主机名和域名。

说明

此处配置的主机名和域名必须与 AD 域服务中的主机名和域名相同。AD 域服务中配置主机名步骤请参见本文档 [7.5.1 配置目录服务器的步骤 5](#)。

1. 登录 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。
2. 配置 BMC 主机名和 DNS。详细信息请参见本文档 [7.6 配置 BMC WebUI DNS（手动）](#)。
3. 配置时区与 Kerberos 服务器时区一致。
 - a. 选择“BMC 管理 > 时区&NTP”。
 - b. 在“地区”和“时区”下拉列表中，选择要设置的参数。
 - c. 单击“保存”。
4. 开启 NTP。

说明

此步骤是为了确保 BMC 时间与 Kerberos 服务器的时间一致。

- a. 在 BMC WebUI，选择“BMC 管理 > 时区&NTP”。
- b. 在“NTP 功能”区域中，选择“开启”。
- c. 单击“保存”。

步骤 2 配置 BMC Kerberos 服务端信息。

1. 在 BMC WebUI，选择“用户&安全 > Kerberos”。
2. 单击“Kerberos 使能”后的 ，此按钮变为 ，表示 Kerberos 功能已经启用。
3. 配置 Kerberos 服务器参数。

必须配置的参数包括：

- 输入 Kerberos 服务器的领域，如“example.com”，领域和 Kerberos 服务器下的领域保持一致。
- 输入 Kerberos 服务器的 IPv4 地址，如“192.168.66.66”。
- 输入 Kerberos 服务器端口号。
- 导入 Kerberos 密钥表。详细操作请参见本文档“用户&安全 > Kerberos”中的[启用 Kerberos 认证并配置域服务器基本属性](#)。
- 输入当前登录 BMC 的用户密码。

其它参数请根据实际需要进行设置。相关参数说明请参考“用户&安全 > Kerberos”章节的 [5.5.3 Kerberos](#)。

4. 单击“保存”。

步骤 3 配置 Kerberos 用户组信息

1. 在 BMC WebUI，选择“用户&安全 > Kerberos”。
2. 在“Kerberos 用户组”区域单击“编辑”进入“修改用户”编辑区域框，或单击“添加组”进入“添加组”编辑区域框。
3. 配置 Kerberos 组参数。

- 输入 Kerberos 用户所属角色组的名称，如 “info_group1”（即 [7.5.1 配置目录服务器](#)中创建的 Kerberos 组）。
- 输入 Kerberos 组应用所在文件夹。
和 Kerberos 服务器下用户的组所在的组织单位名保持一致，如 “company/department”（即 [7.5.1 配置目录服务器](#)中涉及的最下层组织单位），最大长度为 255。
- 配置 SID。
- 选择 Kerberos 组权限。
- 选择已设定的登录规则。
- 选择登录接口。

相关参数说明请参考“用户&安全 > Kerberos”章节的[表 5-47 添加组](#)。

4. 输入当前登录的用户密码。
5. 单击“保存”。

步骤 4 为支持的浏览器配置单点登录。Chrome 不需要进行配置。

在 Firefox 中启用单点登录

以下以 Firefox 17.0 为例进行说明。其它浏览器版本可能具有不同的步骤。

1. 在浏览器地址栏中输入 “about:config”，打开浏览器配置页。
2. 如果显示 “这样可能会失去质保！” 提示消息，请单击 “我保证会小心”。
3. 在浏览器搜索框中输入 “network.negotiate”。
4. 双击 “network.negotiate-auth.trusted-uris”。
5. 在弹出的输入框中输入 BMC DNS 的域名。
6. 单击 “确定”。

步骤 5 使用 Kerberos 域帐户或通过 SSO 登录 BMC

方式一：通过 Kerberos 域帐户登录

1. 输入已在 Kerberos 服务器生效的帐号密码，例 “HWinfo/Admin@9000”。
2. 在域名下拉列表，选择对应 Kerberos 服务器的域名，例 “example.com(KRB)”。
3. 单击 “登录”。

方式二：通过 SSO 一键登录

1. 在已完成[步骤 4](#)配置的浏览器中输入 BMC 的 FQDN 地址，如 “https://主机名.域名”。
2. 单击 “单点登录”。

---结束

7.6 配置 BMC WebUI DNS（手动）

操作场景

BMC WebUI 的“BMC 管理 > 网络配置”提供“配置 DNS”功能，设置 DNS 后，用户可以直接通过域名地址访问 BMC。

说明

- 域名地址 = 主机名 + 域名。如：主机名为“mytest”，域名为“example.com”，那么域名地址为“mytest.example.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：

- BMC 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 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 选择“BMC 管理 > 网络配置”。

步骤 3 在“设置 BMC 主机名”区域框，设置 BMC 主机名，如“mytest”。

步骤 4 单击“保存”。

步骤 5 在“DNS”区域框，单击“手动配置”。

选择手动设置 DNS 信息后，用户可以手动配置 DNS 服务器的域名、首选 DNS 服务器地址和备用 DNS 服务器地址。

步骤 6 配置 DNS 地址。

1. 输入 DNS 域名，如“example.com”。
2. 输入 DNS 首选服务器，如“192.168.66.66”。
3. 输入 DNS 备用服务器。
4. 单击“保存”。

步骤 7 在连接 BMC 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 BMC DNS 地址一致，否则本地 PC 无法通过网络访问 BMC。

步骤 8 使用域名登录 BMC WebUI。

说明

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

在浏览器输入域名地址，如“mytest.example.com”，即可访问 BMC WebUI。

----结束

7.7 配置 SSH 用户密钥登录 BMC CLI

操作场景

用户通过 SSH 方式登录 BMC 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 BMC，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 BMC。

必备事项

前提条件

- 已存在可连接到服务器 BMC 的客户端
- BMC 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
- BMC 管理网口 IP 地址
- SSH 服务端口号

软件

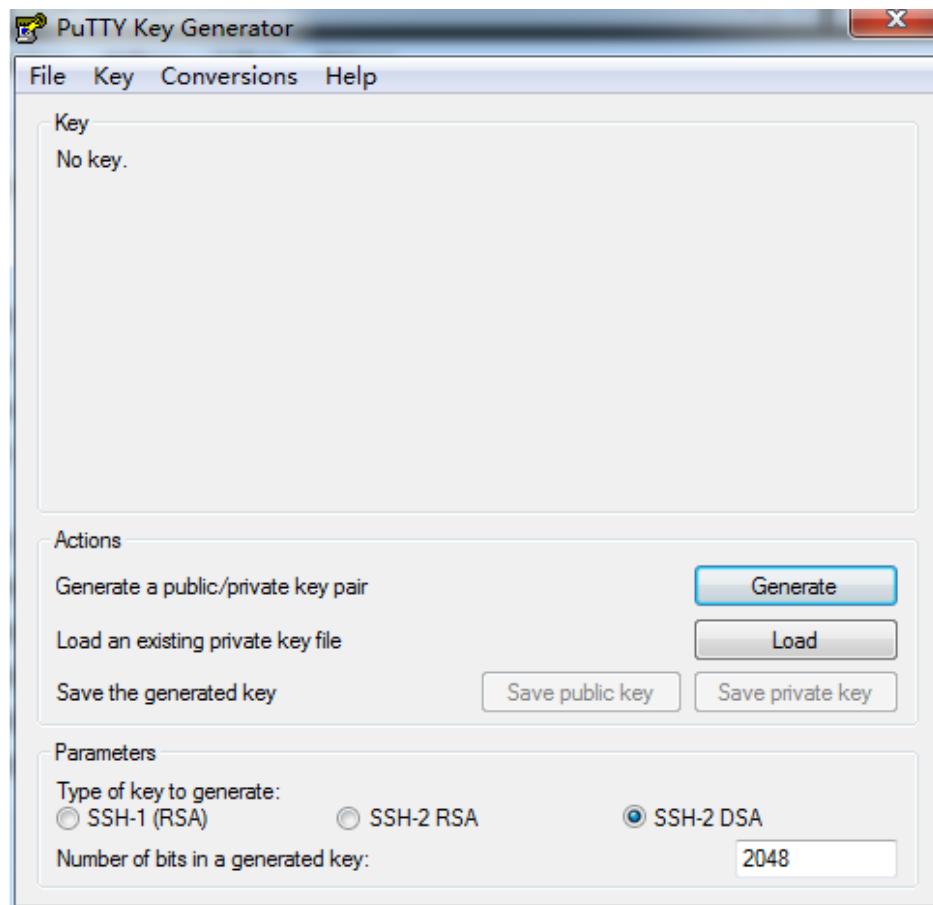
- 登录工具，例如“putty.exe”。
- 密钥生成工具，例如“puttygen.exe”。

上述工具为免费工具，请自行在互联网搜索下载。

操作步骤

- 生成 SSH 密钥
 - a. 在客户端（例如 PC）打开密钥生成工具（例如“puttygen.exe”），如图 7-26 所示。

图7-26 密钥生成界面



- b. 在“Parameters”区域中选择密钥类型，例如“SSH-2 DSA”。
 - c. 设置密钥容量。
 - d. 单击“Generate”生成密钥。
 - e. 单击“Save public key”和“Save private key”将生成的公钥、私钥保存到客户端。
 - 将公钥导入 BMC
 - a. 登录 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。
 - b. 在择“用户&安全 > 本地用户”。
 - c. 单击待导入 SSH 公钥的用户名左侧的 。
 - d. 单击“SSH 公钥”右侧的“上传”。
- 弹出导入“公钥上传”窗口，如图 7-27 所示。

图7-27 公钥上传

×

公钥上传

i

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

☒ 公钥文件

☐ 公钥文本

选择公钥文件

添加文件

★ 登录密码

请输入当前登录用户密码

保存

取消

- e. 选择公钥导入方式。
此处可根据实际情况选择“公钥文件”或“公钥文本”。

 说明

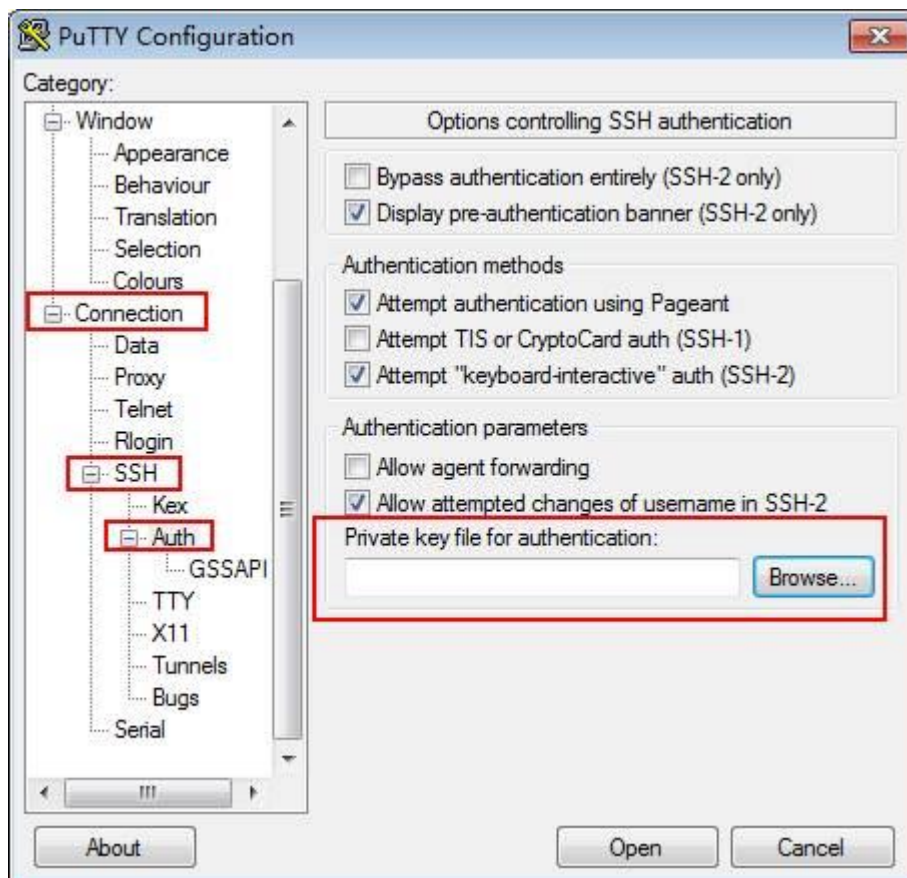
- 公钥文件的格式为“.pub”，最大不超过 2KB。
- f. 单击“添加文件”选择生成的公钥。
 - g. 输入当前登录用户密码。
 - h. 单击“保存”。

 说明

请定期更新密钥，否则可能存在安全风险。

- 配置 SSH 客户端
 - a. 在客户端打开登录工具（例如“putty.exe”）。
 - b. 导入生成的私钥。
私钥导入界面如[图 7-28](#)所示。

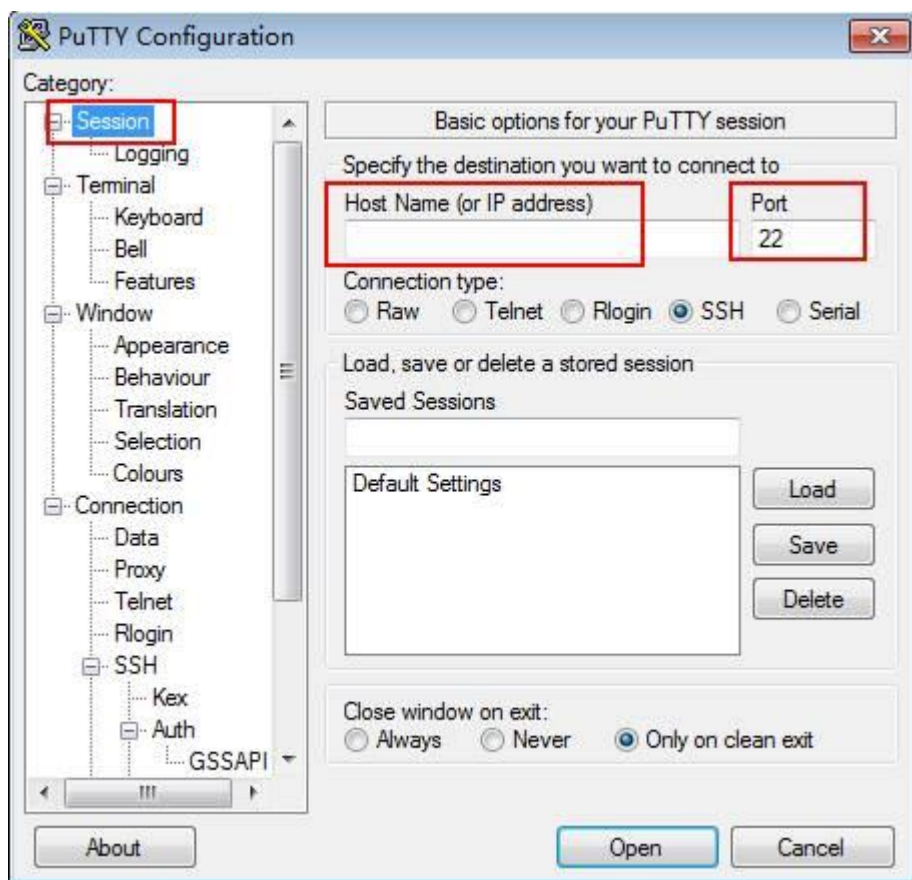
图7-28 导入私钥



c. 配置 SSH 客户端登录信息。

登录信息配置界面如图 7-29 所示，需要输入 BMC 地址、SSH 服务端口号。

图7-29 配置登录信息



- 登录 BMC CLI
 - a. 单击“Open”。
 - b. 按提示信息输入 SSH 用户名。
进入 BMC CLI。

7.8 配置 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端之间的加密传输，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。

设备出厂时默认使用的 SSL 证书为预置证书。预置证书只用于开局初始化阶段，开局后建议将使用设备预置证书的业务更改为使用自己签发的证书。证书过期后将无法访问环境或者无法安全访问环境，为保证业务不中断可以使用不安全的连接访问 BMC。

证书长有效期的安全隐患：随着技术发展，可能当前证书会被破解，一旦一台环境预置证书被破解，所有使用预置证书的环境都会被破解。

说明

- 百信预置证书仅用于部署阶段为设备接入客户网络建立初始安全通道，百信不对预置证书的安全性做承诺与保证。
- 对于将百信预置证书作为业务证书使用而导致的安全风险和安全事件，由客户自行处置并承担后果。
- 百信预置证书有效期自生产制造之日起计算，有效期为 10 年，15 年或从出厂时间到 2041 年。
- 预置证书过期后，使用预置证书的业务会中断。
- 百信建议客户通过部署 PKI 系统对现网设备、软件签发证书并做好证书的生命周期管理（为保证安全性推荐使用短有效期的证书）。

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 BMC 的客户端。

操作步骤

登录 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

请根据实际需求执行不同的操作：

- 当客户端存在正式的证书颁发机构颁发的 SSL 证书时，请执行[•导入 SSL 证书](#)。
- 当客户端存在用户手动生成的 SSL 证书时，请执行[•导入 SSL 证书](#)、[•向浏览器添加根证书](#)。
- 当用户需要自定义证书信息并使用正式的证书颁发机构颁发 SSL 证书时，请执行[•申请 SSL 证书](#)、[•导入 SSL 证书](#)、[•向浏览器添加根证书](#)。

当用户需要自定义证书信息并使用证书生成工具手动生成 SSL 证书时，请执行[•自定义证书信息](#)、[•申请 SSL 证书](#)、[•导入 SSL 证书](#)、[•向浏览器添加根证书](#)。

- 自定义证书信息
 - a. 在 BMC WebUI，选择“服务管理 > Web 服务 > SSL 证书”。
 - b. 单击“自定义”打开自定义证书的界面。
 - c. 在“步骤一：生成 CSR 文件”区域框中，输入自定义的证书请求信息。
自定义信息包括：国家、省份、城市、公司、部门和常用名。
 - d. 单击“生成”。
 - e. 按照弹出的对话框的提示信息导出 CSR 文件到客户端。
- 申请 SSL 证书
SSL 证书可通过如下方式获取：
 - 向正式的证书颁发机构申请 SSL 签名证书。（推荐方式）
 - 使用证书生成工具（例如 openssl）手动生成 SSL 签名证书和根证书。

证书生成工具及其使用方法请用户自行从互联网下载。

- 导入 SSL 证书

支持导入证书文件的格式为 .crt、.cer、.pem、.pfx 和 .p12。其中，.crt、.cer 或 .pem 格式的证书文件不得大于 1MB，.pfx 或 .p12 格式的证书文件不得大于 100KB。

在“SSL 证书”界面单击“自定义”。

- （使用证书颁发机构申请的 SSL 证书时）在“步骤二：自定义证书”区域框中，单击“添加文件”，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 BMC 后生效”信息。

- （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“添加文件”，选中 **• 申请 SSL 证书** 中获取的 SSL 签名证书，在“证书密码”后的文本框中输入传输过程中采用的密码，并单击“保存”。

导入后，会返回“操作成功”信息。

- 重启 BMC。

- 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 Google Chrome 为例说明如何在浏览器中查看并添加认证机构的根证书。

- 打开浏览器，单击  和“设置”。
弹出设置页面。
- 在设置页面，单击“隐私设置和安全性 > 安全”。
跳转到安全页面。
- 在安全页面，单击“管理证书”。
弹出证书窗口。
- 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
- 查看证书是否过期。
 - 是 => 6
 - 否 => 7
- 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。
- 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

7.9 配置 Syslog 日志上报功能

操作场景

BMC WebUI 的“维护诊断 > 告警上报”提供 Syslog 日志上报配置接口，可以设置 BMC 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 BMC 的 syslog 服务器。

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 BMC

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 BMC 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 BMC。
- 双向认证时，需要将服务器证书和客户端根证书上传到 BMC。

说明

请定期更新证书，否则可能存在安全风险。

步骤 3 登录 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 4 配置 syslog 属性

1. 在 BMC WebUI，选择“维护诊断 > 告警上报”。
2. 在“Syslog 报文通知”区域框中，开启 syslog 报文上报功能。
3. 按照界面信息配置“告警级别”、“Syslog 消息格式”、“Syslog 主机标识”、“传输协议”、“认证方式”。

详细信息请参考[表 5-26 Syslog 报文通知](#)。

4. 上传证书。
 - 当“认证方式”为“单向认证”时，将[步骤 1](#)中生成的**服务器根证书**上传到 BMC。
 - 当“认证方式”为“双向认证”时，将[步骤 1](#)中生成的**服务器根证书**和**客户端证书**上传到 BMC。

说明

支持导入服务器根证书文件的格式为“.crt”、“.cer”和“.pem”，最大不超过 100KB。支持导入本地证书文件的格式为“.pfx”和“.p12”，最大不超过 1MB。

步骤 5 配置 syslog 服务器信息和报文格式

1. 选择 syslog 报文发送通道。
2. 单击“编辑”，显示指定通道的编辑区域框。
3. 单击 ，使能发送通道。
当  按钮变为 ，表示启用该发送通道。
4. 按照界面信息配置“服务器地址”、“端口”、“日志类型”。
5. 单击“测试”。

显示“操作成功”，表示该通道可用。

---结束

7.10 使用 VNC 登录服务器实时桌面

操作场景

BMC 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 BMC 管理网口。

数据

- BMC 管理网口的地址和端口号（即 VNC 服务端口号）
- VNC 服务密码

软件

客户端（例如 PC）已下载并安装第三方的 VNC 客户端软件，例如 TigerVNC、RealVNC。

操作步骤

步骤 1 使能 VNC 端口

BMC 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 BMC WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。
2. 在 BMC WebUI，选择“服务管理 > VNC”。
3. 开启 VNC 服务，并设置端口号。VNC 服务默认为关闭状态。默认端口号为“5900”。

步骤 2 配置 VNC 属性

1. 在不采用 SSL 加密传输时，关闭 SSL 加密使能，设置 VNC 密码。

密码复杂度要求：

- 长度必须为 8 个字符。
- 至少包含以下字符中的两种：
 - 小写字母：a~z
 - 大写字母：A~Z
 - 数字：0~9
- 至少包含一个以下特殊字符：
`~!@#\$%^&*()-_+=\|[]{};:","<.>/?

说明

出于安全考虑，保存设置时需要输入当前登录用户密码进行身份验证。

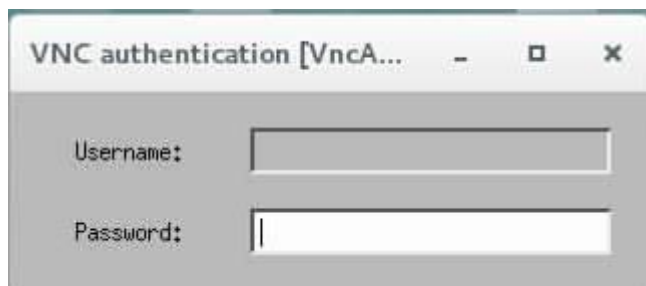
步骤 3（可选）Linux 客户端使用 TigerVNC 登录服务器实时桌面

1. 在客户端的 TigerVNC 安装目录下，打开命令行控制台，并执行 **vncviewer ipaddress:port** 命令。

其中, *ipaddress* 表示服务器 BMC 管理网口 IPv4 或 IPv6 地址, *port* 表示 VNC 服务端口号。

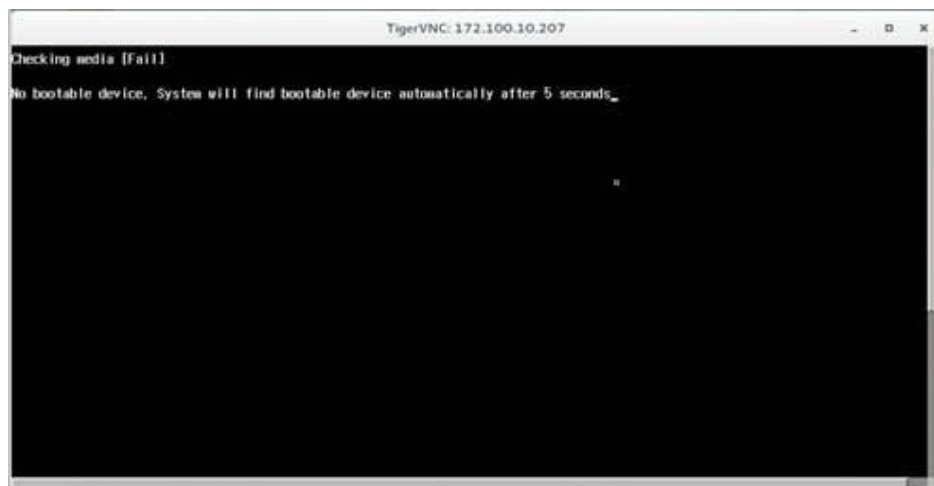
打开 TigerVNC 的登录窗口, 如图 7-30 所示。

图7-30 TigerVNC 登录窗口



2. 输入步骤 1.2 中设置的密码, 并按“Enter”。
登录服务器实时桌面, 如图 7-31 所示。

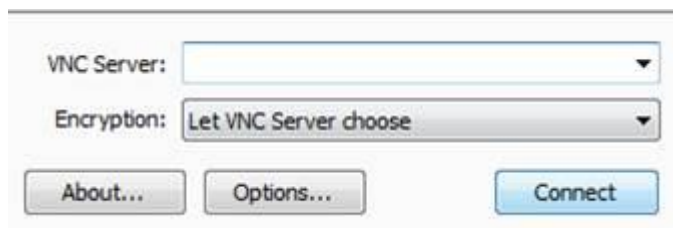
图7-31 服务器实时桌面



步骤 4（可选）Windows 客户端使用 RealVNC 登录服务器实时桌面

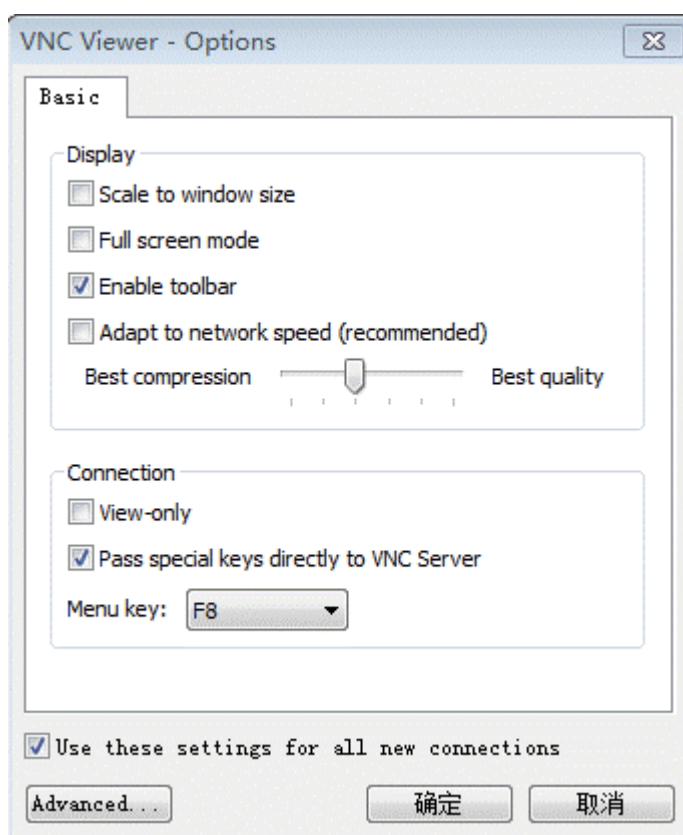
1. 在客户端双击 RealVNC 客户端软件。
打开 RealVNC 登录窗口, 如图 7-32。

图7-32 RealVNC 登录窗口



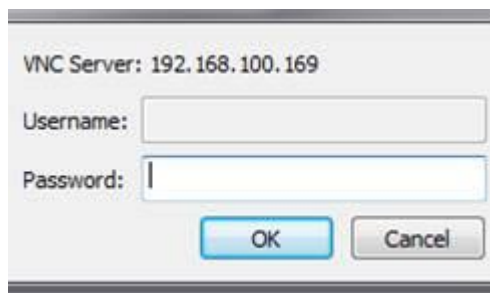
2. 单击“Options”，打开参数设置界面，如[图 7-33](#)。

图7-33 RealVNC 客户端参数设置界面



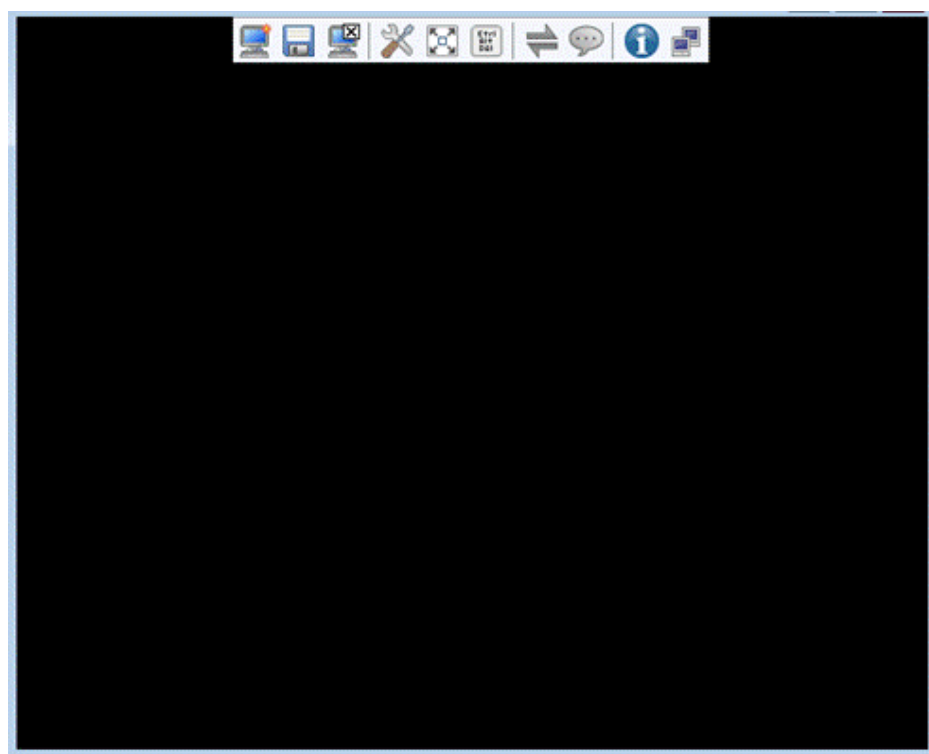
3. 按照实际需要设置显示参数，单击“确定”。
返回[图 7-30](#)所示的登录窗口。
4. 在“VNC Server”右侧的文本框中输入要登录的服务器 BMC 管理网口 IP 地址。
地址格式为“管理网口 IP 地址（IPv4 地址或 IPv6 地址）:端口号”，例如
“192.168.100.169:5900”。
5. 单击“Connect”。
若弹出数据加密提示窗口，请单击“continue”继续进行操作。
弹出身份认证窗口，如[图 7-34](#)。

图7-34 RealVNC 客户端身份认证窗口



6. 在“Password”右侧的文本框中输入[步骤 3.1](#)中设置的密码，并单击“OK”。
登录服务器实时桌面，如[图 7-35](#)。

图7-35 服务器实时桌面



----结束

7.11 导入信任证书和根证书

操作场景

使用浏览器登录 BMC WebUI 时，若弹出安全告警提示，可以在浏览器中为 BMC 导入信任证书和根证书来屏蔽此安全告警提示。

本指南以 Google Chrome 为例介绍为 BMC 导入信任证书和根证书的操作步骤。

必备事项

前提条件

请用户自行准备好需要导入的信任证书和根证书。

数据

无

软件

无

操作步骤

- 导入信任证书
 - a. 打开 Google Chrome 浏览器，单击  和“设置”。
弹出设置页面如图 7-36。

图7-36 设置页面



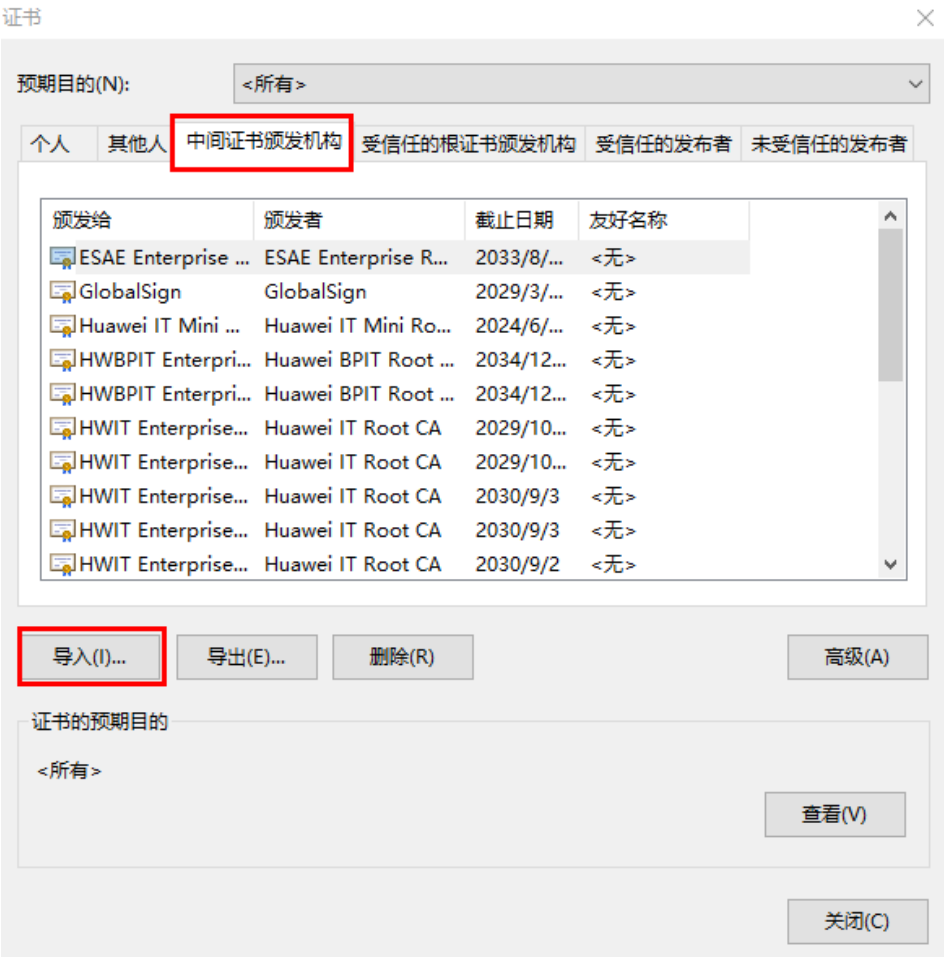
- b. 单击“隐私设置和安全性 > 安全”。
跳转到安全页面如图 7-37。

图7-37 安全页面



- c. 单击“管理证书”。
弹出证书窗口如图 7-38。

图7-38 证书窗口



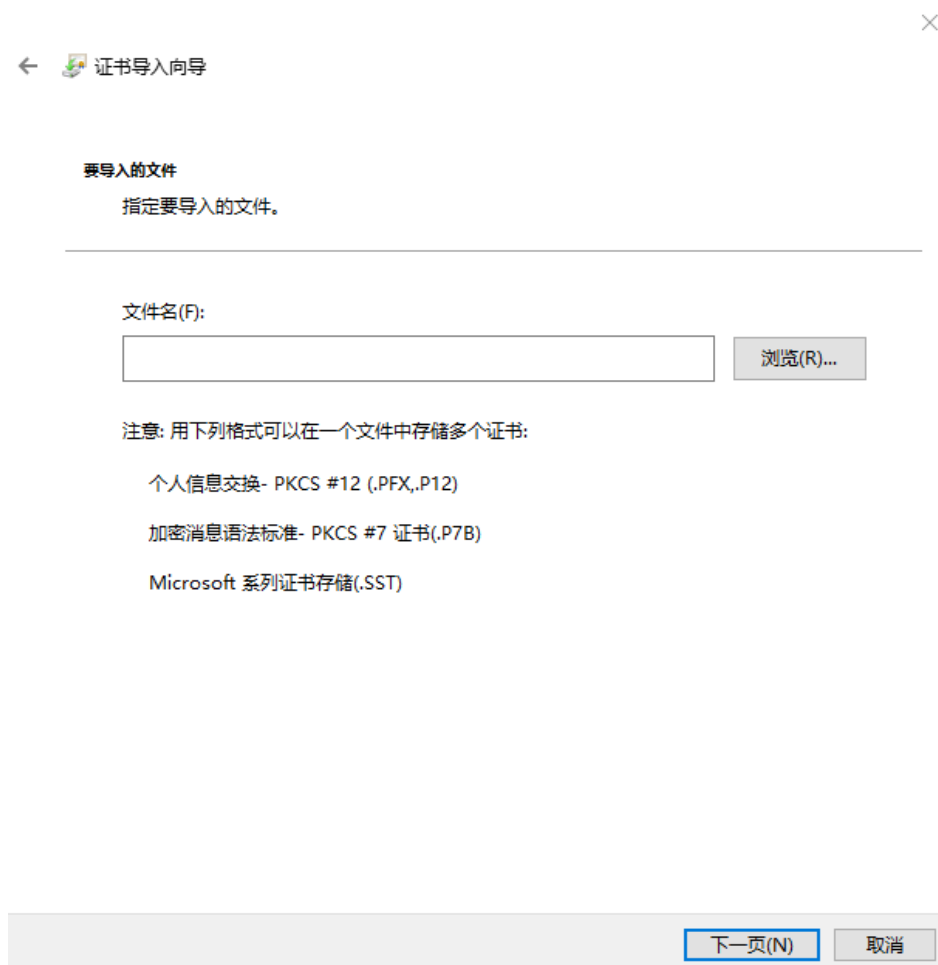
- d. 单击“中间证书颁发机构> 导入”。
弹出证书导入向导窗口如图 7-39。

图7-39 导入证书窗口



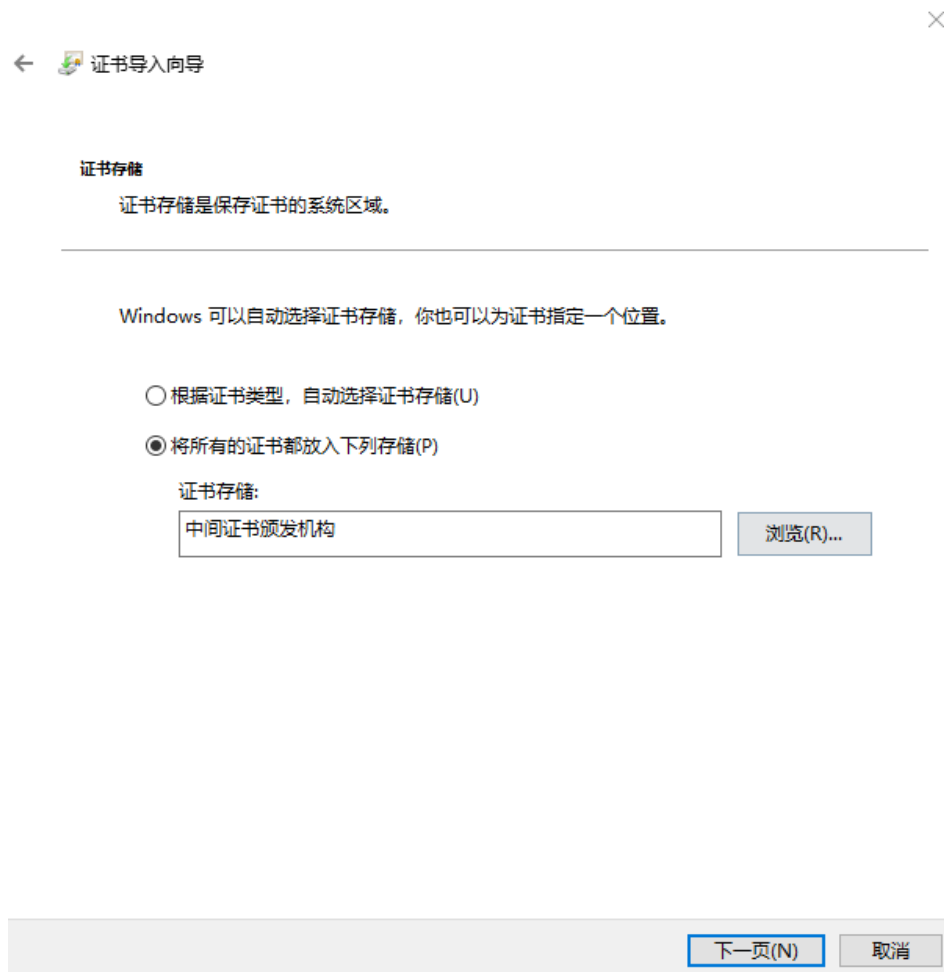
- e. 单击“下一页”继续。
弹出选择证书窗口如[图 7-40](#)。

图7-40 选择证书窗口



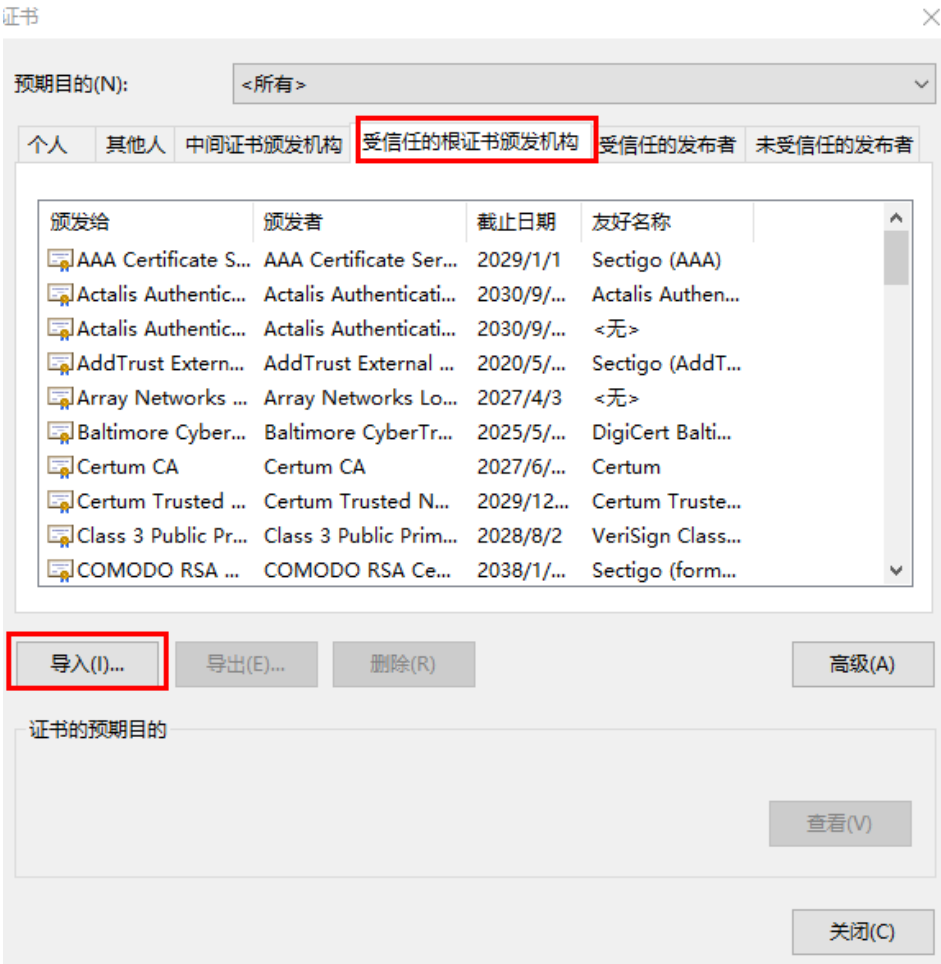
- f. 单击“浏览”，从本地 PC 路径中选择待上传的证书。
- g. 单击“下一步”继续。
在弹出的选择证书存储位置窗口如图 7-41 中选择证书的存放位置

图7-41 选择证书存储位置窗口



- h. 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。
- i. 单击“确定”完成证书导入。
- 导入根证书
 - a. 重复以上 a 和 3，打开弹出导入证书窗口，如图 7-42。

图7-42 导入证书窗口



- b. 单击“受信任的根证书颁发机构 > 导入”。
- 弹出证书导入向导窗口如[图 7-43](#)。

图7-43 导入证书窗口



c. 重复以上 5~9，完成根证书导入。

说明

- 如果证书错误提示中显示其它的颁发者，此时导入颁发者对应的信任证书即可屏蔽安全告警提示。
- 请定期更新证书，否则可能存在安全风险。

8 FAQ

- 8.1 服务器安装 Windows 后出现未知设备
- 8.2 双因素认证失败后无法登录 WebUI
- 8.3 环境产生不安全协议告警
- 8.4 环境产生不安全算法告警
- 8.5 IPMI RMCP 通信失败
- 8.6 使用旧版本 Edge 查看联机帮助失败

8.1 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 8-1 所示。	服务器的 BMC 默认打开黑匣子功能，但 Windows 侧没有相关驱动。

图8-1 服务器 Windows 系统下的未知设备



解决方案一

步骤 1 请参考 BMA 的用户指南在 Windows 侧正确安装 BMA。

📖 说明

黑匣子驱动可随 BMA 一起安装生效。

步骤 2 BMA 运行后，若仍存在上述问题，请联系技术支持处理。

----结束

解决方案二

步骤 1 在 BMC WebUI 的“黑匣子”界面中关闭黑匣子功能。

步骤 2 若仍存在上述问题，请联系技术支持处理。

----结束

8.2 双因素认证失败后无法登录 WebUI

问题现象

问题描述	可能原因
双因素认证失败，无法登录 BMC WebUI。	- BMC 开启双因素认证后，导入的证书不正确。 - BMC 开启双因素认证后，客户端浏览器无配套证书。

解决方案一

步骤 1 用户自行从因特网获取 IPMI 工具（例如 IPMITool）并安装。

步骤 2 配置客户端地址，使之可与 BMC 正常通信。

步骤 3 在客户端通过 IPMI 工具执行关闭双因素认证的操作。

以 IPMITool 为例，可执行如下命令：

```
ipmitool -I lanplus -H bmcipaddr -U username -P password raw 0x30 0x93 0xdb 0x07
0x00 0x35 0x53 0x00 0x01 0x00 0x00 0x00 0xff 0xff 0x79 0x01 0x00 0x01 0x00 0x79
0x01 0x00
```

说明

- bmcipaddr*: 表示 BMC 管理网口 IP 地址。
- username*: 表示登录 BMC 所需的管理员用户名。
- password*: 表示登录 BMC 所需的管理员密码。

步骤 4 重新登录 BMC WebUI。

- 如果可以正常登录 BMC WebUI，若您仍然需要使用双因素认证登录，请参考 [5.5.4 双因素认证](#)，上传正确的证书到 BMC 和客户端浏览器后，重新验证。
- 如果仍然不能登录 BMC WebUI，请联系技术支持处理。

----结束

解决方案二

步骤 1 用户自行从因特网获取 MIB 工具（例如 MIB Browser）并安装。

步骤 2 配置客户端地址，使之可与 BMC 正常通信。

步骤 3 使用 MIB 工具连接到 BMC。

步骤 4 将“twoFactorAuthenticationEnable”（OID 为 1.3.6.1.4.1.2011.2.235.1.1.41.1）节点设置为“disable(1)”。

步骤 5 重新登录 BMC WebUI。

- 如果可以正常登录 BMC WebUI，若您仍然需要使用双因素认证登录，请参考 [5.5.4 双因素认证](#)，上传正确的证书到 BMC 和客户端浏览器后，重新验证。
- 如果仍然不能登录 BMC WebUI，请联系技术支持处理。

---结束

8.3 环境产生不安全协议告警

8.3.1 问题现象

问题描述	可能原因
BMC 上报不安全协议告警	BMC 开启不安全协议：SNMPv1/v2、RMCP、VNC

8.3.2 解决方案

8.3.2.1 针对 SNMP 和 VNC 不安全协议

步骤 1 登录 WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。

步骤 2 在导航栏中选择“服务管理 > SNMP”或“服务管理 > VNC”。

步骤 3 勾选对应的安全协议，单击“保存”。如下图所示。

说明

勾选不安全协议时会有风险提示。

图8-2 勾选 SNMP 安全协议

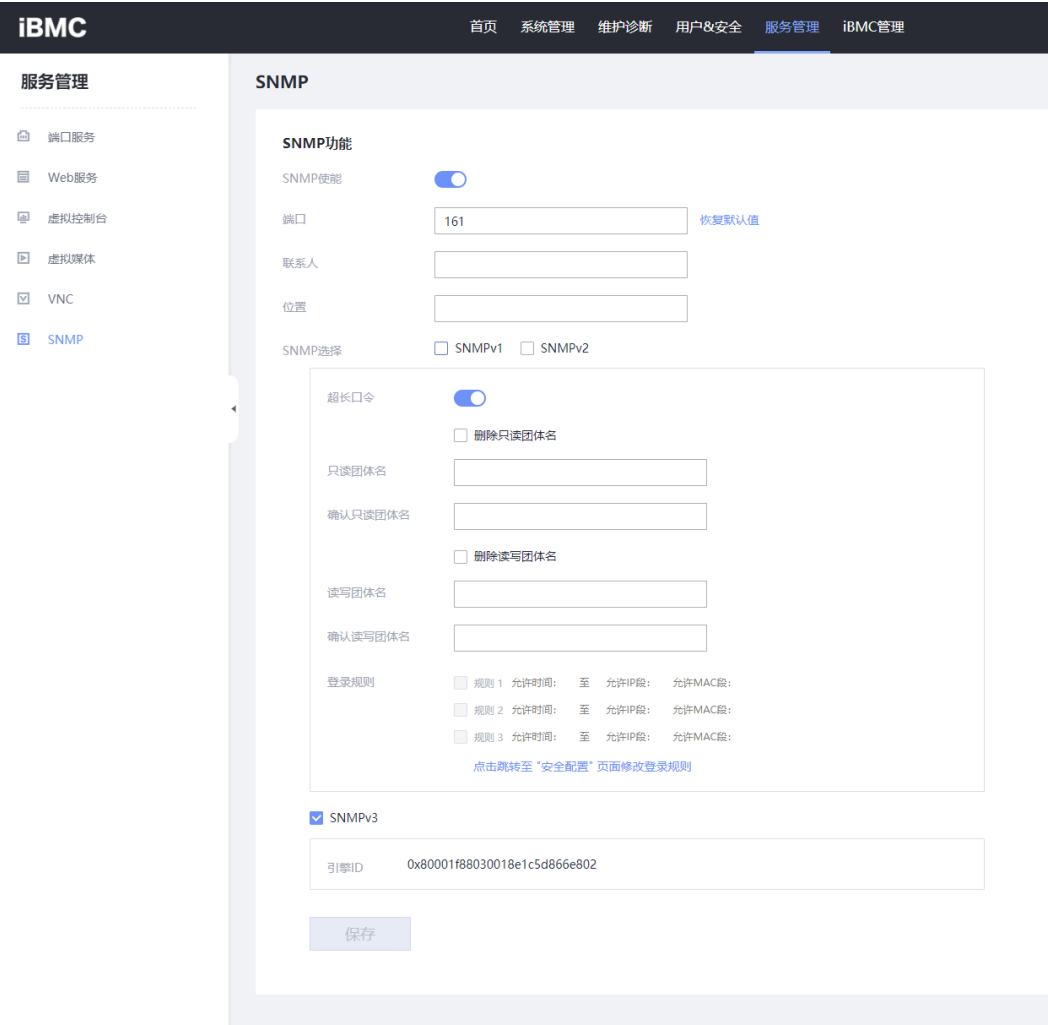


图8-3 勾选 VNC 安全协议



----结束

8.3.2.2 针对 RMCP 不安全协议

步骤 1 登录 CLI。详细信息请参见本文档“CLI 介绍 > 登录 CLI”章节。

步骤 2 执行 ipmcset -t service -d state -v rmcp disabled 命令。

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

----结束

8.4 环境产生不安全算法告警

8.4.1 问题现象

问题描述	可能原因
BMC 上报不安全算法告警	BMC 开启不安全的算法，涉及算法种类可能为 SSH 加密算法、SSH 密钥交换算法、SSH 消息认证算法、SSH 公钥算法、SSL 加密算法、SNMP 鉴权算法、SNMP 加密算法

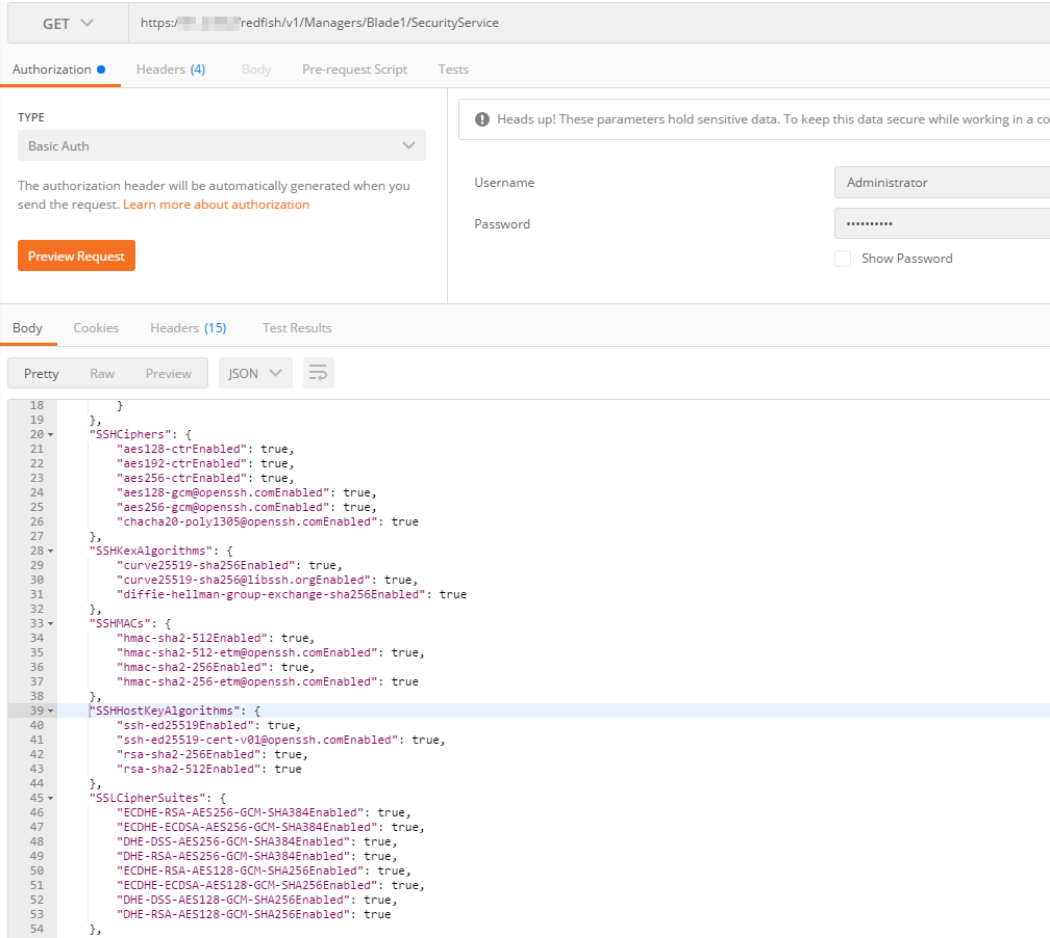
8.4.2 解决方案

8.4.2.1 针对 SSH 类算法、SSL 类算法

步骤 1 登录 Redfish 接口。

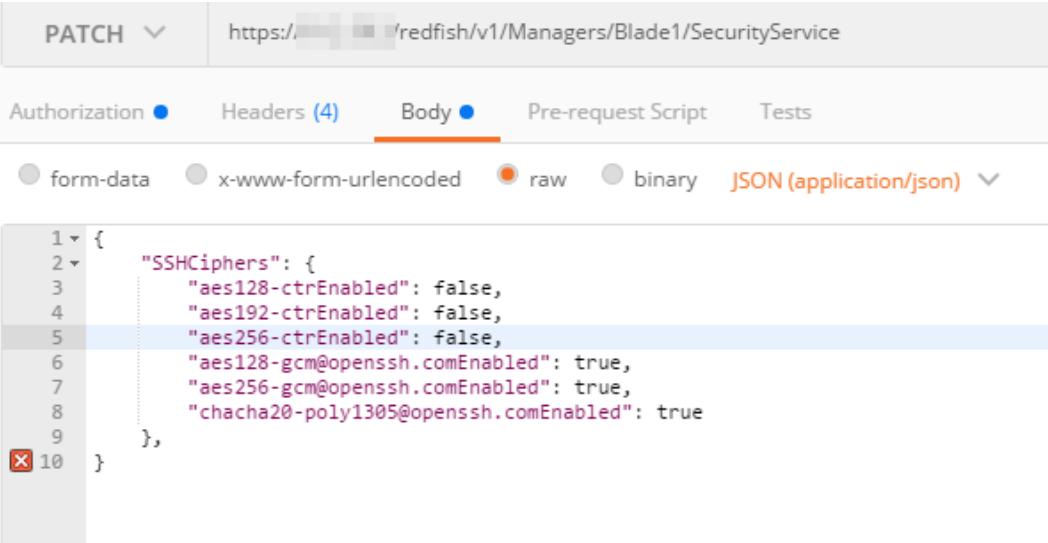
URL: “https://device_ip/redfish/v1/Managers/manager_id/SecurityService”。

图8-4 登录 Redfish 接口



步骤 2 在 PATCH 操作类型下，关闭不安全算法。

图8-5 关闭不安全算法



----结束

8.4.2.2 针对 SNMP 类算法

8.4.2.2.1 通过 Web 接口修改算法

- 步骤 1 登录 WebUI。详细信息请参见本文档“新手入门 > 用户登录”章节。
- 步骤 2 在在导航栏中选择“用户安全 > 本地用户”。
- 步骤 3 单击“编辑”，弹出编辑用户界面，如下图所示。

图8-6 编辑用户

编辑用户

用户ID

2

用户名

Administrator

用户密码

确认密码

首次登录策略

提示修改密码

角色

管理员

请至少保留一个管理员用户

登录规则

规则1

允许时间至

允许IP段

允许MAC段

规则2

规则3

点击跳转至“安全配置”页面修改登录规则

登录接口

SSH

IPMI

Local

SFTP

Web

SNMP

Redfish

SNMPv3加密密码

加密密码

确认密码

SNMPv3算法

鉴权算法

SHA256

加密算法

AES

* 登录密码

请输入当前登录用户密码

保存

取消

2023-07-27

464

步骤 4 勾选安全的 SNMP 算法（勾选不安全算法时会有风险提示）。

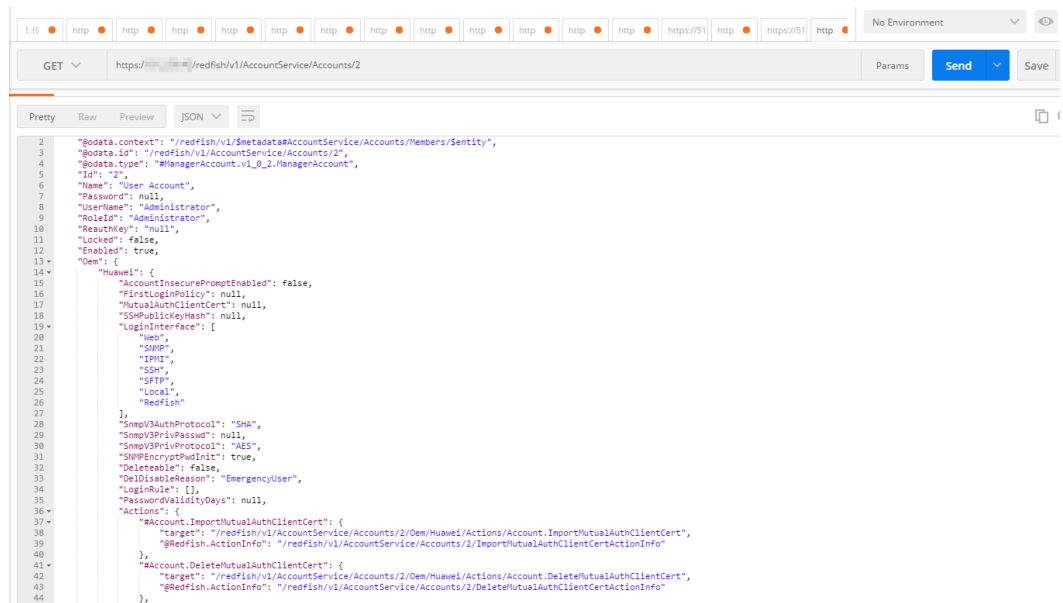
----结束

8.4.2.2.2 通过 Redfish 接口修改算法

步骤 1 登录 Redfish 接口。

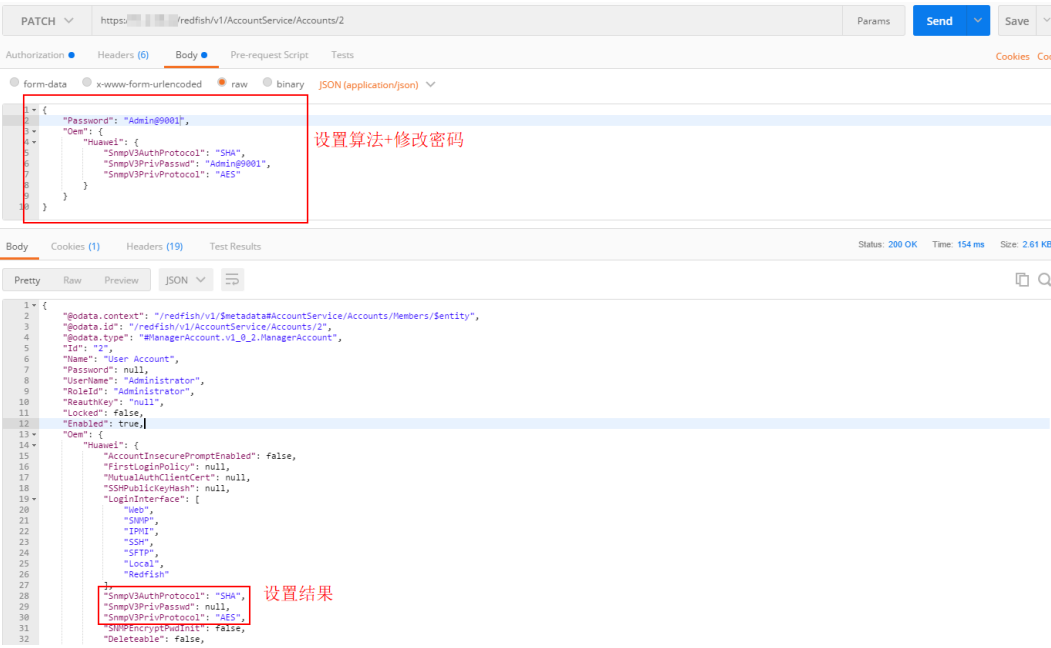
URL: “https://device_ip/redfish/v1/AccountService/Accounts/account_id”。

图8-7 登录 Redfish 接口



步骤 2 在 **PATCH** 操作类型下，关闭不安全算法。

图8-8 关闭不安全算法



----结束

8.5 IPMI RMCP 通信失败

问题现象

问题描述	可能原因
与 BMC 收发 ipmi 消息失败	BMC 默认只开启了安全加密套件，而 ipmitool 不支持此加密套件

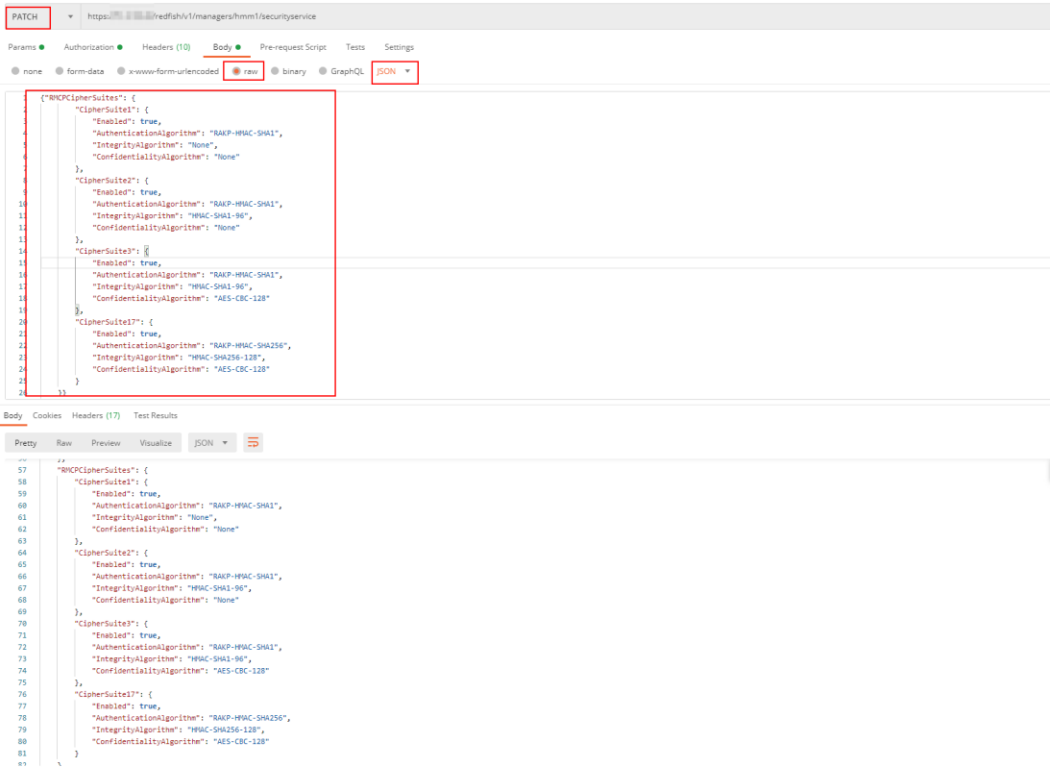
解决方案

- 步骤 1 将 ipmitool 升级到 1.8.18-6 及以上版本，并且在调用 ipmitool 命令时，追加参数“-C 17”，再与 BMC 的 IPMI 接口通信。
- 步骤 2 如果 ipmitool 无法升级到 1.8.18-6 及以上版本，或者虽然版本达到要求，但不希望追加参数，则可以登录 Redfish 接口。
- URL：“https://device_ip/redfish/v1/Managers/manager_id/SecurityService”。
- 步骤 3 在 **PATCH** 操作类型下，启用 BMC 的 RMCP 不安全加密套件。

说明

启用 BMC 的 RMCP 不安全加密套件存在一定的安全风险，请谨慎启用。

图8-9 启用 BMC 的 RMCP 不安全加密套件



----结束

8.6 使用旧版本 Edge 查看联机帮助失败

问题现象

问题描述	可能原因
1. 使用旧版本 EdgeHtml 内核的 Edge 浏览器登录 WebUI 2. 单击  查看联机帮助 3. 提示安全告警信息，继续转到页面 4. 查看联机帮助页面报错	iBMC 没有信任证书和根证书

解决方案一

如果您有可信任的证书和根证书，可以为 BMC [导入信任证书和根证书](#)。

解决方案二

步骤 1 单击“详细信息 > 继续转到网页”。

图8-10 安全告警

此站点不安全

这可能意味着，有人正在尝试欺骗你或窃取你发送到服务器的任何信息。你应该立即关闭此站点。

 [转到起始页](#)

详细信息

你的电脑不信任此网站的安全证书。
该网站的安全证书中的主机名与你正在尝试访问的网站不同。

错误代码: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

[继续转到网页](#) (不推荐)

步骤 2 刷新页面，联机帮助页面恢复正常。

---结束

9 附录

- 9.1 确认管理网口 IP 地址
- 9.2 通过 BIOS 修改 BMC 默认用户密码
- 9.3 Smart Provisioning
- 9.4 独立远程控制台
- 9.5 配置文件说明
- 9.6 BMC 系统默认用户

9.1 确认管理网口 IP 地址

BMC 管理网口的 IP 地址确认方法有以下几种：

- 通过服务器 BIOS 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。

通过 BIOS 查询和设置

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

通过串口查询和设置

须知

通过串口登录 BMC CLI，必须保证系统串口已经切换为 BMC 串口。可以通过 SSH 登录命令行，执行[查询和设置串口方向（serialdir）](#)切换串口。

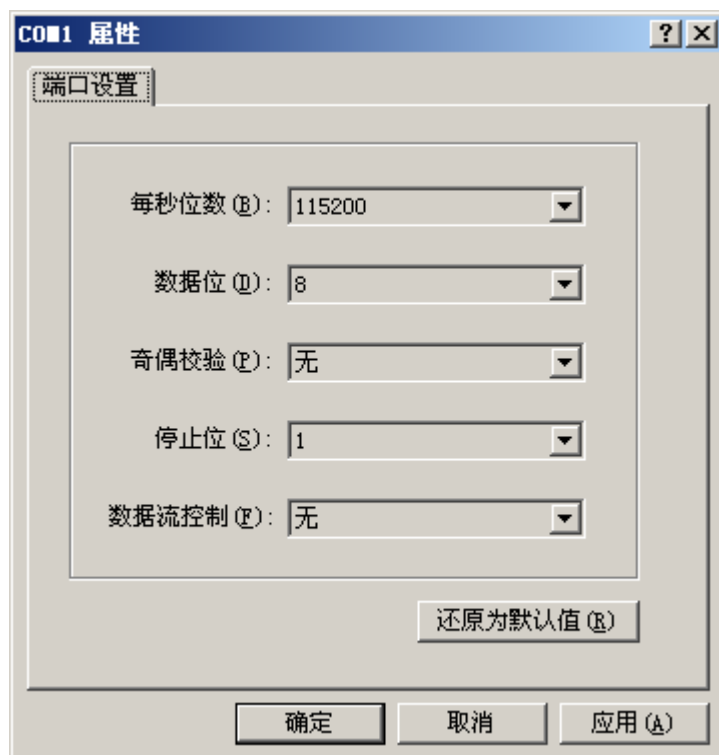
步骤 1 连接串口线。

步骤 2 通过超级终端登录串口命令行，需要设置的参数有：

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

参数设置如图 9-1 所示。

图9-1 超级终端属性设置



步骤 3 单击“应用”。

步骤 4 连接成功后输入用户名和密码。

步骤 5 执行 `ipmcget -d ipinfo` 命令可获取管理网口 IP 地址信息。

----结束

9.2 通过 BIOS 修改 BMC 默认用户密码

须知

- 通过 BIOS 系统设置的 BMC 默认用户密码最大长度为 16 个字符。
- 如果 BMC Web 中“用户&安全 > 安全配置”页面的“业务侧用户管理使能”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 BMC 的默认用户密码。

服务器支持通过 BIOS 修改 BMC 的默认用户密码，具体请参见相应的 BIOS 参数参考。

9.3 Smart Provisioning

仅 BMC V264 及以上版本和 BIOS 0.37 及以上版本支持 Smart Provisioning。

Smart Provisioning 提供 GUI 和 Redfish 两种接口，分别对应单机操作和批量操作的应用场景。

9.4 独立远程控制台

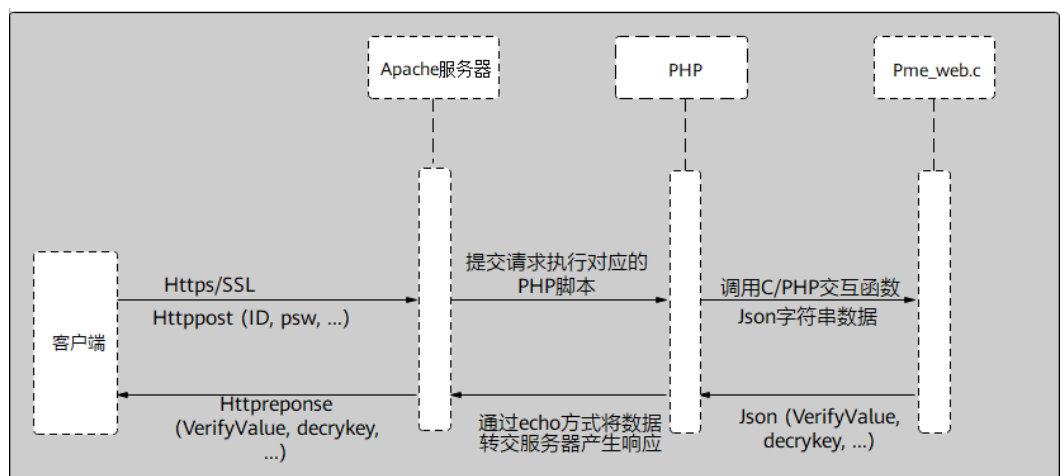
9.4.1 简介

独立远程控制台是基于服务器管理软件 BMC 的远程控制工具，其实现的功能与 BMC 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下图所示。

图9-2 基本原理



兼容性

独立远程控制台可在如下表所示环境中运行。

表9-1 环境要求

客户端操作系统类型	客户端操作系统版本
Windows	Windows 7 32 位/64 位
	Windows 8 32 位/64 位
	Windows 10 32 位/64 位
	Windows Server 2008 R2 32 位/64 位
	Windows Server 2012 64 位
Redhat	Redhat 6.9
	Redhat 7.3
Ubuntu	Ubuntu 14.04 LTS
	Ubuntu 16.04 LTS
Mac OS	Mac OS X El Capitan

下载地址

您可以单击 [SmartKit Computing 23.0.RC1](#) 来下载所需软件。

9.4.2（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 BMC 登录服务器实时桌面时，在客户端操作系统版本与 BMC 版本均符合独立远程控制台运行要求的情况下，相较 BMC 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 BMC 管理网口。

数据

- BMC 管理网口的地址和端口号
- 登录 BMC 所需的用户名和密码

软件

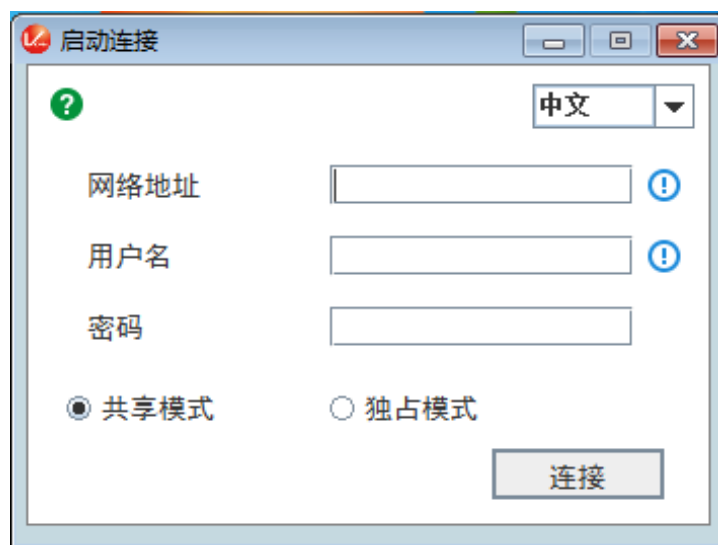
独立远程控制台软件包已下载到客户端（例如 PC）并解压。

操作步骤

步骤 1 配置客户端（例如 PC）IP 地址，使其与 BMC 管理网口网络互通。

步骤 2 双击“KVM.exe”打开独立远程控制台，如图 9-3 所示。

图9-3 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：

- BMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- BMC 域名地址：端口号

说明

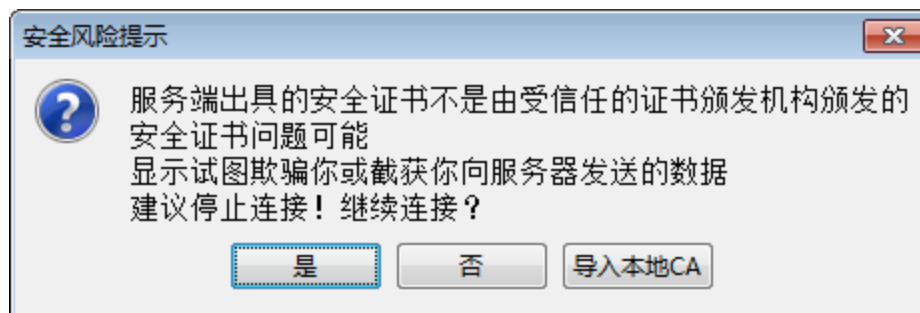
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 输入 IPv6 地址时，必须使用[]将其括起来，而 IPv4 地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 4 选择登录模式，并单击“连接”。

- 共享模式：可以让 2 个用户连接到服务器，并同时服务器进行操作。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 9-4 所示的安全风险提示对话框。

图9-4 安全风险提示



步骤 5 按照实际需要单击确认按钮。

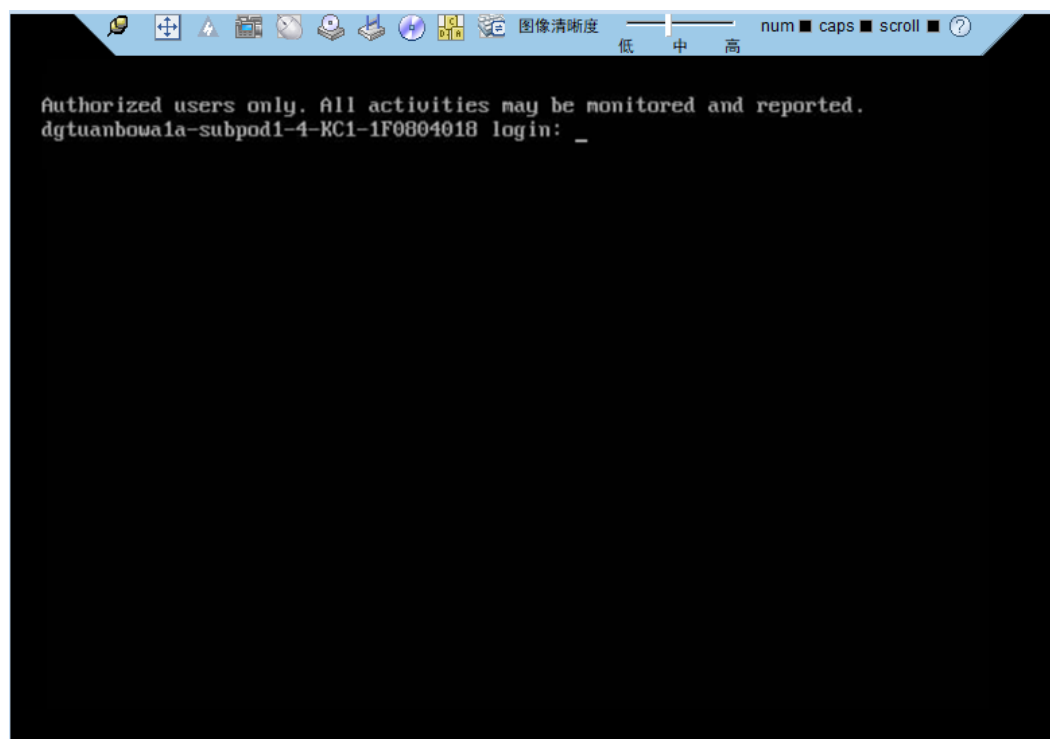
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA，之后将不会再弹出该安全风险提示对话框。

说明

- CA 证书文件格式为“*.cer”、“*.crt”或“*.pem”，最大不超过 1MB。
- 请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如图 9-5 所示。

图9-5 服务器实时桌面



----结束

9.4.3 (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 BMC 登录服务器实时桌面时，在客户端操作系统版本与 BMC 版本均符合独立远程控制台运行要求的情况下，相较 BMC 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 BMC 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

- BMC 管理网口的地址和端口号
- 登录 BMC 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 BMC 管理网口网络互通。

步骤 2 打开控制台，并将独立远程控制台所在文件夹设置为工作路径。

步骤 3 执行 **chmod +x KVM.sh** 设置独立远程控制台的权限。

步骤 4 执行 **./KVM.sh**，打开独立远程控制台，如图 9-6 所示。

图9-6 独立远程控制台登录界面

该图显示了一个名为“启动连接”的窗口。窗口顶部有一个语言选择下拉菜单，当前显示为“中文”。窗口内有三个输入框，分别用于“网络地址”、“用户名”和“密码”。每个输入框右侧都有一个蓝色的感叹号图标。在输入框下方，有两个单选按钮，分别是“共享模式”（已选中）和“独占模式”。窗口底部有一个“连接”按钮。窗口左上角有一个绿色的问号图标。

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：

- BMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- BMC 域名地址：端口号

说明

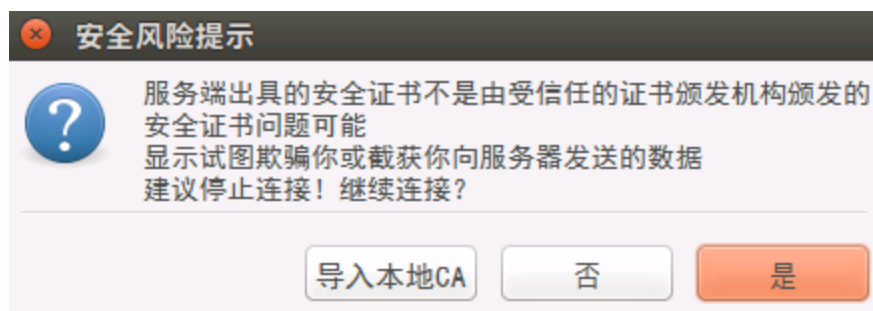
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 输入 IPv6 地址时，必须使用[]将其括起来，而 IPv4 地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 6 选择登录模式，并单击“连接”。

- 共享模式：可以让 2 个用户连接到服务器，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。
- 独占模式：只能有 1 个用户连接到服务器进行操作。

弹出如图 9-7 所示的安全风险提示对话框。

图9-7 安全风险提示



步骤 7 按照实际需要单击确认按钮。

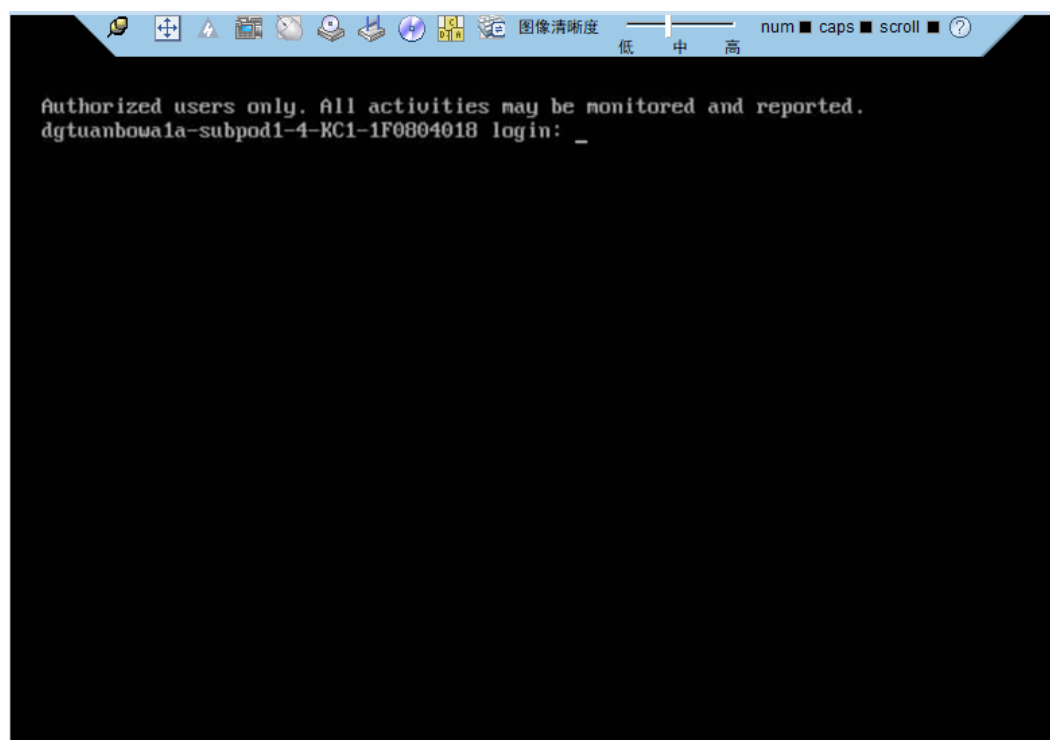
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件，之后将不会再弹出该安全风险提示对话框。

说明

- CA 证书文件格式为“*.cer”、“*.crt”或“*.pem”，最大不超过 1MB。
- 请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如[图 9-8](#) 所示。

图9-8 服务器实时桌



----结束

9.4.4 (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 BMC 登录服务器实时桌面时，在客户端操作系统版本与 BMC 版本均符合独立远程控制台运行要求的情况下，相较 BMC 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 BMC 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

- BMC 管理网口的地址和端口号
- 登录 BMC 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 BMC 管理网口网络互通。

步骤 2 打开控制台，并将独立远程控制台所在文件夹设置为工作路径。

步骤 3 执行 **chmod +x KVM.sh** 设置独立远程控制台的权限。

步骤 4 执行 **./KVM.sh**，打开独立远程控制台，如图 9-9 所示。

图9-9 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：

- BMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- BMC 域名地址：端口号

说明

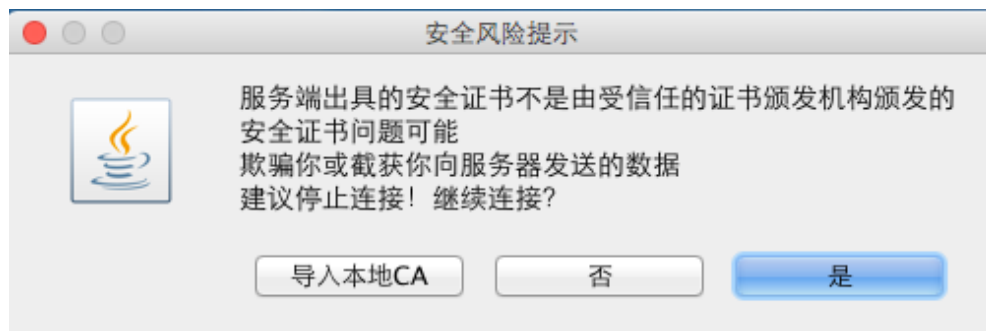
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 输入 IPv6 地址时，必须使用[]将其括起来，而 IPv4 地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 6 选择登录模式，并单击“连接”。

- 共享模式：可以让 2 个用户连接到服务器，并同时服务器进行操作。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 9-10 所示的安全风险提示对话框。

图9-10 安全风险提示



步骤 7 按照实际需要单击确认按钮。

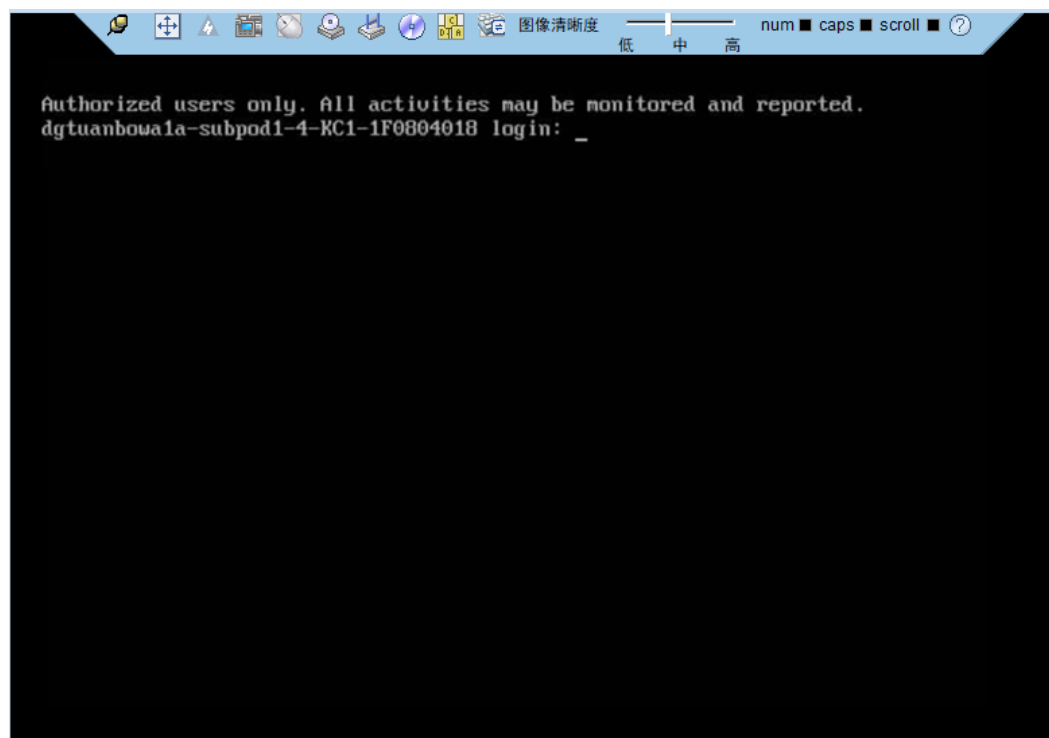
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件，之后将不会再弹出该安全风险提示对话框。

说明

- CA 证书文件格式为“*.cer”、“*.crt”或“*.pem”，最大不超过 1MB。
- 请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如图 9-11 所示。

图9-11 服务器实时桌面



----结束

9.4.5 (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 BMC 登录服务器实时桌面时，在客户端操作系统版本与 BMC 版本均符合独立远程控制台运行要求的情况下，相较 BMC 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 BMC 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

- BMC 管理网口的地址和端口号
- 登录 BMC 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 BMC 管理网口网络互通。

步骤 2 打开控制台，并将独立远程控制台所在文件夹设置为工作路径。

步骤 3 执行 **chmod +x KVM.sh** 设置独立远程控制台的权限。

步骤 4 执行 **./KVM.sh**，打开独立远程控制台，如图 9-12 所示。

图9-12 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：

- BMC 管理网口 IP 地址（IPv4 地址或 IPv6 地址）：端口号
- BMC 域名地址：端口号

说明

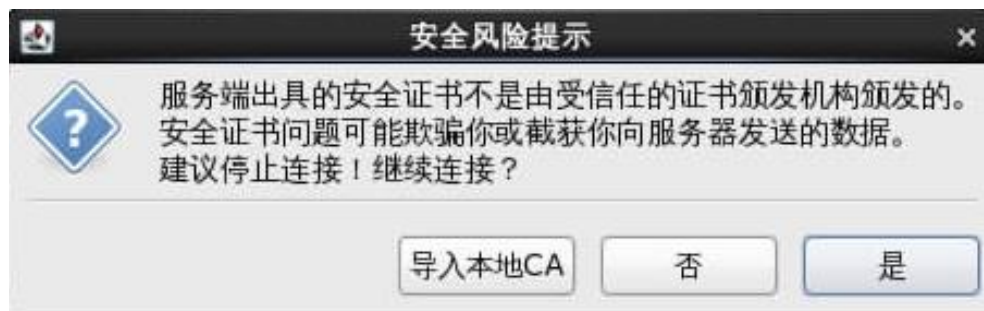
- 支持本地用户及 LDAP 域用户登录。
- 端口号优先对应 HTTPS 服务端口号，其次对应 RMCP+服务端口号。
- 输入 IPv6 地址时，必须使用[]将其括起来，而 IPv4 地址无此限制。例如：“[fc00::64]:444”、“192.168.100.1:444”。
- 当端口号为默认值时，“网络地址”中可不加端口号。

步骤 6 选择登录模式，并单击“连接”。

- 共享模式：可以让 2 个用户连接到服务器，并同时对服务器进行操作。本用户可以看到对方用户的操作，对方用户也能看到本用户的操作。
- 独占模式：只能有 1 个用户连接到服务器进行操作。

弹出如图 9-13 所示的安全风险提示对话框。

图9-13 安全风险提示



步骤 7 按照实际需要单击确认按钮。

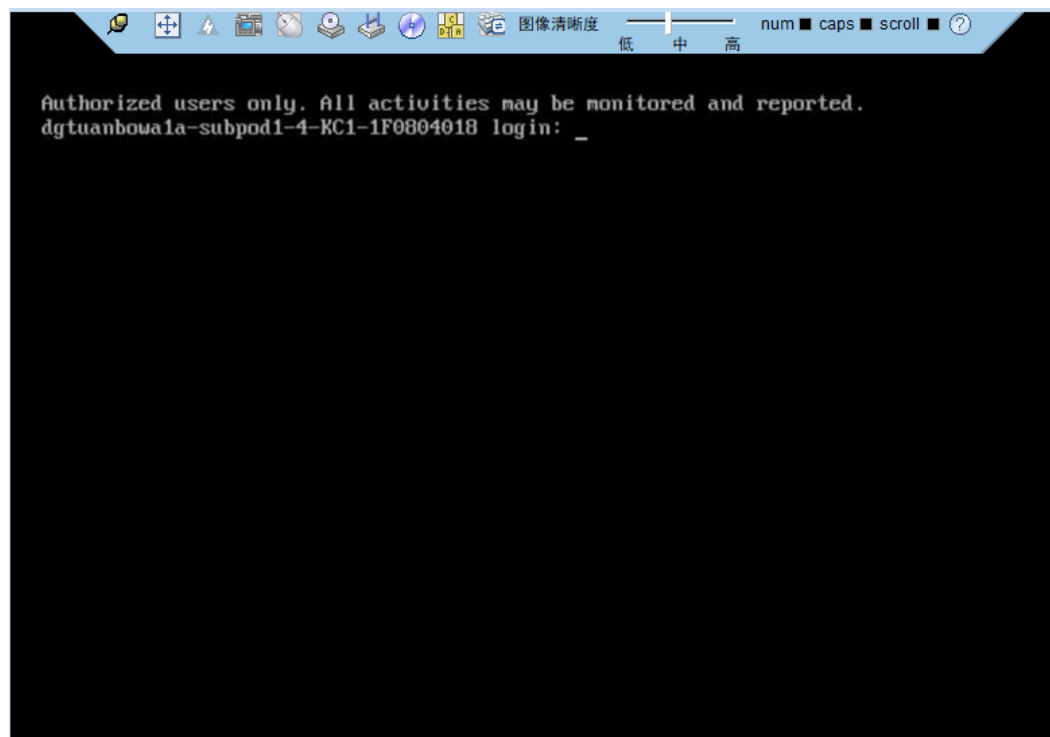
- 单击“是”：直接打开独立远程控制台，忽略证书认证错误。
- 单击“否”：回退到登录界面。
- 单击“导入本地 CA”：弹出文件选择窗口，您可以导入预先准备好的自定义 CA 证书文件，之后将不会再弹出该安全风险提示对话框。

说明

- CA 证书文件格式为“*.cer”、“*.crt”或“*.pem”，最大不超过 1MB。
- 请定期更新证书，否则可能存在安全风险。

打开服务器实时桌面，如[图 9-14](#)所示。

图9-14 服务器实时桌面



---结束

9.5 配置文件说明

BMC 配置文件、BIOS 配置文件和 RAID 控制器配置文件的说明如表 9-2 BMC 配置项、表 9-3 BIOS 配置项和表 3 RAID 控制器配置项所示。

为保证数据安全性，服务器更换主板后导入原配置文件时，BMC 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 BMC 配置、BIOS 配置和部分的 RAID 控制器配置。

表9-2 BMC 配置项

分类	导出项	导出子项	说明	是否支持配置文件导入生效
本地用户	User	UserName	用户名	是
	User	PassWord	用户密码 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	User	Privilege	用户权限	是
	User	UserRoleId	用户角色	是
	User	PermitRuleIds	用户登录规则	是
	User	LoginInterface	用户登录接口 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	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 导入生效
				现。
	UserRole	KVMMgnt	配置角色（KVM 权限）	是
	UserRole	UserMgnt	配置角色（用户管理权限）	是
	UserRole	VMMgnt	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/Kerberos 配置	LDAP	Enable	LDAP（或 Kerberos）使能状态	是
	LDAP	CertStatus	LDAP（或 Kerberos）证书验证使能状态	是
	LDAP	HostAddr	LDAP（或 Kerberos）服务器地址	是
	LDAP	Port	LDAP（或 Kerberos）端口号	是
	LDAP	UserDomain	域名	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	LDAP	Folder	用户应用文件夹	是
	LDAP	BindDN	绑定标识名	是
	LDAP	BindDNPsw	绑定密码 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	LDAP	CertificateVerificationLevel	证书校验级别	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
	LDAPServer	UserDomain	域名	是
	LDAPServer	Folder	用户应用文件夹	是
	LDAPServer	BindDN	绑定标识名	是
	LDAPServer	BindDNPsw	绑定密码 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	LDAPGroup	GroupName	LDAP（或 Kerberos）组名称	是
	LDAPGroup	SID	Kerberos 组安全标识符	是
	LDAPGroup	GroupFolder	LDAP（或 Kerberos）组应用文件夹	是
	LDAPGroup	GroupPermitRuleIds	LDAP（或	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
			Kerberos) 组登录规则	
	LDAPGroup	GroupLoginInterface	LDAP (或 Kerberos) 组登录接口	是
	LDAPGroup	GroupUserRoleId	LDAP (或 Kerberos) 组用户角色	是
	LDAPGroup	GroupPrivilege	LDAP (或 Kerberos) 组权限	是
	LDAPGroup	GroupDomain	设置 LDAP (或 Kerberos) 组域	是
	LDAPCommon	Enable	LDAP 使能	是
安全增强	PasswdSetting	EnableStrongPassword	密码检查使能状态	是
	SecurityEnhance	SSHPasswordAuthentication	SSH 密码认证使能状态	是
	SecurityEnhance	UserInactTimeLimit	用户不活动期限	是
	SecurityEnhance	PwdExpiredTime	密码有效期	是
	SecurityEnhance	MinimumPwdAge	密码最短使用期	是
	SecurityEnhance	InitialPwdPrompt	密码修改提示使能状态	是
	SecurityEnhance	ExcludeUser	紧急登录用户	是
	SecurityEnhance	OldPwdCount	禁用历史密码	是
	SecurityEnhance	AuthFailMax	登录失败锁定次数	是
	SecurityEnhance	AuthFailLockTime	登录失败锁定时长	是
	PermitRule	TimeRuleInfo	时间段登录规则	是
	PermitRule	IpRuleInfo	IP 登录规则	是
	PermitRule	MacRuleInfo	MAC 登录规则	是
	SecurityEnhance	PermitRuleIds	规则使能状态	是
	SecurityEnhance	BannerState	登录安全信息配置使能状态	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	SecurityEnhance	BannerContent	登录安全信息	是
	SecurityEnhance	CertOverdueWarnTime	证书过期告警时间	是
	SecurityEnhance	SSHCiphers	SSH 协议加密算法使能状态	是
	SecurityEnhance	SSHKexs	SSH 协议密钥交换算法使能状态	是
	SecurityEnhance	SSHMACs	SSH 协议消息认证算法使能状态	是
	SecurityEnhance	SSHHostKeys	SSH 协议主机公钥算法	是
	SecurityEnhance	SSLCipherSuites	SSL 协议加密套件使能状态	是
	SecurityEnhance	RMCPCipherSuites	RMCP 协议加密套件使能状态	是
网络配置	BMC	HostName	BMC 主机名	否，取值在配置文件中体现。
	EthGroup	NetMode	网口模式	是
	EthGroup	ActivePort	指定管理网口	是
	EthGroup	IpVersion	IP 协议使能	是
	EthGroup	IpMode	IPv4 地址获取模式	是
	EthGroup	IpAddr	IPv4 地址	否，取值在配置文件中体现。
	EthGroup	SubnetMask	IPv4 子网掩码	否，取值在配置文件中体现。
	EthGroup	DefaultGateway	IPv4 默认网关	否，取值在配置文件中体现。

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	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 1	是
	DNSSetting	TertiaryDomain	DNS 备用服务器 2	是
	DNSSetting	DomainName	DNS 域名	是
	EthGroup	VlanState	VLAN 使能	是
	EthGroup	VlanID	VLAN ID	是
	NTP	EnableStatus	NTP 使能	是
	NTP	Mode	NTP 模式	是
	NTP	PreferredServer	NTP 首选服务器地址	是
	NTP	AlternativeServer	NTP 备用服务器地址	是
	NTP	AuthEnableStatus	NTP 服务器身份认证使能	是
	NTP	MinPollInterval	NTP 同步周期最小值	是
	NTP	MaxPollInterval	NTP 同步周期最大	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
			值	
	VNC	EnableState	VNC 使能	是
	VNC	Password	VNC 密码 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	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
	SSDPConfig	Mode	SSDP 运行的模式	是
	SSDPConfig	UseInterface	使用的网口	是
	SSDPConfig	Interval	Alive 消息发送的时间间隔	是
	SSDPConfig	Port	SSDP 本地服务端端口号	是
	SSDPConfig	NotifyTTL	设置 ssdp 跳数	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
	Snmp	V3State	SNMP 服务 V3 使能状态	是
	Snmp	IsUpdateEngineID	设置引擎 ID 的 MAC 与外出网口 MAC 不一致时，是否更新引	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
			擎 ID	
	Kvm	State	KVM 使能状态	是
	Kvm	Port	KVM 端口	是
	Vmm	State	VMM 使能状态	是
	Vmm	Port	VMM 端口	是
	Video	State	Video 使能状态	是
	Video	Port	Video 端口	是
	WEBHTTP	State	HTTP 使能状态	是
	WEBHTTP	Port	HTTP 端口	是
	WEBHTTPS	State	HTTPS 使能状态	是
	WEBHTTPS	Port	HTTPS 端口	是
	RmcpConfig	LanState	IPMI LAN (RMCP) 使能状态	是
	RmcpConfig	Port1	IPMI LAN (RMCP) 端口 1	是
	RmcpConfig	Port2	IPMI LAN (RMCP) 端口 2	是
	RmcpConfig	LanPlusState	IPMI LAN (RMCP+) 使能状态	是
	RmcpConfig	ServiceFlag	设置 RMCP 服务使 能	是
系统 配置	Snmp	V1State	支持 SNMPv1	是
	Snmp	V2CState	支持 SNMPv2c	是
	Snmp	V3Status	支持 SNMPv3	是
	Snmp	LongPasswordEnable	超长口令使能	是
	Snmp	ROCommunity	只读团体名 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理	否，敏感信息在配置文件中隐藏，不能直接生效。

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
			员重新配置。	
	Snmp	RWCommunity	读写团体名 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	Snmp	RWCommunityState	读写团体名使能状态	是
	Snmp	SNMPV1V2CPermitRuleIds	SNMP 登录规则	是
	Snmp	AuthProtocol	SNMPv3 鉴权算法 说明 BMC V3.01.12.01 及以上版本，不支持明文导出此配置项。	否
	Snmp	PrivProtocol	SNMPv3 加密算法 说明 BMC V3.01.12.01 及以上版本，不支持明文导出此配置项。	否
	Snmp	sysContact	联系人	是
	Snmp	sysLocation	位置	是
	SecurityEnhance	TLSVersion	TLS 版本	是
	SecurityEnhance	EnableUserMgmt	业务侧用户管理使能状态	是
	SecurityEnhance	DoubleCertificationEnable	设置二次认证使能状态 1: 开启 0: 关闭	是
	SecurityEnhance	WeakPwdDictEnable	设置弱口令字典检查开关状态的方法	是
	SecurityEnhance	AuthFailLockTimeExCustom	设置用户锁定时长扩展，兼容旧 web 连续性白牌	是
	SecurityEnhance	AuthFailMaxExCustom	设置用户连续认证失败最大次数扩展,兼	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
			容旧 web 连续性白牌	
	Session	Timeout	Web 超时时间	是
	Session	Mode	Web 会话模式	是
	Contact	OfficalWeb	设置官网	是
	Contact	Copyright	设置版权信息	是
	Contact	SupportWeb	设置技术支持网站	是
	Contact	Email	设置技术支持邮箱	是
	Contact	Phone	设置技术支持电话	是
	Contact	DownloadKVMLink	设置独立 KVM 下载链接	是
	BMC	LocationInfo	设备位置	否，取值在配置文件中体现。
	BMC	RemoteOEMInfo	设置第三方预置信息	是
	BMC	BladeManageMode	单板管理模式，1 OSCA 单板的 HMM 管理模式, 2 OSCA 单板的 esight 扁平化管理模式, 不持久化, OSCA 专用	是
	BMC	LanguageSet	语言集	是
	BMC	CertAlgorithm	默认证书	是
	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
	MeInfo	CpuTjmax	CPU 开启节能模式的温度	是
	Partition	RAIDMode	RAID 工作模式	是
	PRODUCT	WOLState	网络唤醒使能状态	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	PRODUCT	SWRaidType	单板支持软 RAID 的类型	是
	PRODUCT	WeakPwdDictSupport	标识产品是否支持弱口令字典检查	是
	DataAcquisitionService	Enable	数据收集服务使能	是
系统 启动 项	Bios	StartOption	第一启动设备	是
	Bios	StartOptionFlag	永久使能状态	是
	Bios	BiosBootModeSw	启动模式使能开关	是
	Bios	BiosBootMode	启动模式	是
	Bios	BiosBootModeSwEnable	IPMI 设置启动模式显示开关	是
	Bios	StartOptionFlagExt	系统启动项单次有效时，配置的生效状态	是
告警 设置	SyslogConfig	EnableState	Syslog 使能状态	是
	SyslogConfig	MsgIdentity	Syslog 主机标识	是
	SyslogConfig	MsgSeverity	Syslog 告警级别	是
	SyslogConfig	NetProtocol	Syslog 传输协议	是
	SyslogConfig	AuthType	Syslog 认证方式	是
	SyslogConfig	MsgProtocol	消息协议类型 BSD:1 IETF:2	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

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	TrapConfig	TrapIdentity	Trap 主机标识	是
	TrapConfig	CommunityName	Trap 团体名 说明 BMC V3.01.12.01 及以上版本不支持导出导入此配置项，如果在其他服务器上导入了配置文件，需要管理员重新配置。	否，敏感信息在配置文件中隐藏，不能直接生效。
	TrapConfig	SendSeverity	Trap 告警发送级别	是
	TrapItemCfg	ItemEnable	Trap 服务器使能	是
	TrapItemCfg	DestIpAddr	Trap 服务器地址	是
	TrapItemCfg	DestIpPort	Trap 服务器端口	是
	TrapItemCfg	Separator	报文分隔符	是
	TrapItemCfg	Time	报文显示内容（时间）	是
	TrapItemCfg	SensorName	报文显示内容（传感器名称）	是
	TrapItemCfg	Severity	报文显示内容（级别）	是
	TrapItemCfg	EventCode	报文显示内容（事件码）	是
	TrapItemCfg	EventDesc	报文显示内容（事件描述）	是
	TrapItemCfg	ShowKeyWord	报文显示关键字	是
	TrapItemCfg	BobEnable	带内通道上报 trap 报文使能状态	是
	TrapItemCfg	BmaVethIpAddr	通过带内上报 Trap 报文时对应的 BMA veth 网口 IP 地址	是
	TrapItemCfg	BmaVethIpPort	通过带内上报 Trap 报文时对应的 BMA veth 网口的端口号	是
	Sel	QuerySelMaxNum	Sel 最大查询长度	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	SmtplibConfig	SmtplibEnable	SMTP 使能	是
	SmtplibConfig	SmtplibServer	SMTP 地址	是
	SmtplibConfig	TlsSendMode	SMTP 是否启动 tls	是
	SmtplibConfig	AnonymousMode	SMTP 是否使用匿名	是
	SmtplibConfig	LoginName	SMTP 发件人用户名	是
	SmtplibConfig	LoginPasswd	SMTP 发件人密码 说明 BMC V3.01.12.01 及以上版本，不支持明文导出此配置项。	否，敏感信息在配置文件中隐藏，不能直接生效。
	SmtplibConfig	SenderName	SMTP 发件人邮箱 说明 BMC V3.01.12.01 及以上版本，不支持明文导出此配置项。	否，敏感信息在配置文件中隐藏，不能直接生效。
	SmtplibConfig	TempletTopic	SMTP 邮件主题	是
	SmtplibConfig	TempletIpaddr	SMTP 主题附带主机名	是
	SmtplibConfig	TempletBoardSn	SMTP 主题附带单板序列号	是
	SmtplibConfig	TempletAsset	SMTP 主题附带产品资产标签	是
	SmtplibConfig	SendSeverity	SMTP 设置告警发送级别	是
	SmtplibItemCfg	EmailName	接收告警地址 说明 BMC V3.01.12.01 及以上版本，不支持明文导出此配置项。	否，敏感信息在配置文件中隐藏，不能直接生效。
	SmtplibItemCfg	EmailDesc	接收告警描述	是
	SmtplibItemCfg	ItemEnable	接收告警使能	是
	SmtplibItemCfg	Separator	内容分隔符	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	SmtpltemCfg	ShowKeyWord	是否带关键字	是
	SmtpltemCfg	Time	是否发送时间	是
	SmtpltemCfg	Severity	是否发送告警等级	是
	SmtpltemCfg	SensorName	是否发送传感器名称	是
	SmtpltemCfg	EventCode	是否发送事件码	是
	SmtpltemCfg	EventDesc	是否发送事件描述	是
	EventInformation	Enable	告警事件使能	是
	EventInformation	EventType	告警事件类型	是
	EventInformation	Severity	告警事件级别	是
	RedfishEventService	ServiceEnabled	对外消息上报使能开关	是
	RedfishEventService	ServerIdentitySource	设置主机标识源	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	PowerLimitWhenSteady	功率封顶是否需要依赖于 BMC 初始化完成	否
远程控制	Kvm	EncryptState	KVM 加密使能状态	是
	Vmm	EncryptState	VMM 加密使能状态	是
	Kvm	KeyboardMode	虚拟键盘、鼠标持续连接使能状态	是
	Kvm	KvmTimeout	远程控制台超时时长	是
	Kvm	LocalKVMState	本地 KVM 使能状态	是
	Kvm	AutoOSLockState	系统锁定状态	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	Kvm	AutoOSLockType	系统锁定方式	是
	Kvm	AutoOSLockKey	自定义快捷键	是
录像 回放	Video	VideoSwitch	录像使能状态	是
屏幕 截图	Kvm	ScreenSwitch	最后一屏使能状态	是
黑匣 子	Diagnose	BlackBoxState	黑匣子使能状态	是
串口 数据	Diagnose	SolDataState	串口数据使能状态	是
固件 升级	Upgrade	DowngradeDisabled	版本防降级功能使能 状态	是
智能 调速	Cooling	SmartCoolingMode	智能调速模式	是
	Cooling	CustomOutletTobj	出风口目标值	是
	Cooling	CustomCpuCoreTobj	CPU 目标值	是
	Cooling	CustomDiskTobj	硬盘目标值	是
	Cooling	CustomMemoryTobj	内存目标值	是
	Cooling	CustomPCHTobj	PCH 目标值	是
	Cooling	CustomVRDTobj	VRD 目标值	是
	Cooling	CustomVDDQTobj	VDDQ 目标值	是
	Cooling	CustomNpuHbmTobj	NPU HBM 目标值	是
	Cooling	CustomNpuAiCoreTobj	NPU AI Core 目标值	是
	Cooling	CustomNpuBoardTobj	NPU 板目标值	是
	Policy1Class	EnvRangeRdL	区间调速策略的温度 和转速区间	是
其他	HMMSSH NAT	State	NAT 使能状态	是
	ExPortConfig	State	SSDP 使能状态	是
	HMMSSH NAT	Port	NAT 端口	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
	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。
	ComputerSystem	HostnameSyncEnabled	BMA 上报 Hostname 同步 BMC 使能开关	是
	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
	USBMassStorage	UmsMaxUpdateSpace	部件配置或升级包下 发到 NAND FLASH 完成标识	是
	USBMassStorage	SpConfigFileReady	进入 SP 的方式	是
	USBMassStorage	SPStartmode	SP 操作完成到复位 OS 的时间间隔	是
	USBMassStorage	SysRestartDelay	OS 重启延时	是
	SmBios	Version	SMBIOS 中 Version	是

分类	导出项	导出子项	说明	是否支持 配置文件 导入生效
			参数取值	
	SmBios	SKUNumber	SMBIOS 中 SKUNumber 参数取值	是
	SmBios	Family	SMBIOS 中 Family 参数取值	是
	SMS	CdevChannelEnabled	带内字符设备通道使能状态	是
	PTAS	Enable	PTAS 特性使能	是
	PTAS	Altitude	设置海拔高度	是
	PTAS	ServerTag	机器型号	是
	Chassis	OwnerID	节点归属标识	是
	Chassis	MaxNodeIndex	框内的最大节点索引值	是
	Chassis	NodeIndex	节点在框内的索引	是
	Chassis	SyncElabel	节点是否同步机框 product SN、product AssetTag 电子标签	是
	Chassis	NodeIndexSuffix	节点在框内的后缀	是
	Chassis	AlarmPolicy	x6800mm 是否对所有节点板上报告警的属性 0: 所有节点上报 1: 只上报一个节点	是
	IpmbEthBlade	PowerCappingValue	设置封顶值方法	是
	IpmbEthBlade	PowerCappingFailAction	节点封顶失效动作	是
	Cpu	DisableCpuSw	设置禁用/启用 cpu 接口	是
	IOBoard	FirmwareVersion	设置 IO 版固件版本	是
	Warning	ImmediatelyReport	当前告警是否支持立即上报	是

分类	导出项	导出子项	说明	是否支持配置文件导入生效
	FdmConfig	IErrWarmResetEnable	ERR 收集失败时热复位使能	是
	PMEServiceConfig	CustomSNMPOID	定制化的 OID	是
	PMEServiceConfig	WOLConfigEnable	PME 是否支持 WOL(wake on lan)网络唤醒配置功能	是
	SdrDev	DynamicSensorNumBase	动态分配传感器号的起始传感器号	是
	Composition	DefaultSettingId	默认配置模式 ID	是
	StorageCfgCustomize	DiskSlotCustomId	硬盘槽位定制的类型 ID	是
	IPMIMessageFilter	FireWallStatus	IPMI 消息过滤总开关	是
	IPMIMessageFilter	FireWallMode	IPMI 消息过滤总开关开启时，启动的黑白名单模式	是

表9-3 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

导出项	说明
	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，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® Technology，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。
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。

导出项	说明
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。
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。
thermalthrottling-support	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。

导出项	说明
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。
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

导出项	说明
	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。
ComBaseOutput	串口 IO 基址设置。
OemMemTurbo	内存超频开关。
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。

导出项	说明
BootTypeOrder[1]	启动顺序。
BootTypeOrder[2]	启动顺序。
BootTypeOrder[3]	启动顺序。

表9-4 RAID 控制器配置项

分类	导出项	导出子项	说明	是否支持配置文件导入
存储	RaidController	Type	RAID 控制器类型。	否，取值在配置文件中体现。
	RaidController	CopybackEnabled	RAID 控制器回拷功能状态。	是
	RaidController	SMARTerCopybackEnabled	RAID 控制器在检测到物理盘 SMART 错误之后是否自动进行回拷。	是
	RaidController	JBODEnabled	RAID 控制器 JBOD 功能状态。	是
	RaidController	Mode	RAID 控制器的工作模式。 • 0-RAID • 1-HBA • 2-JBOD	是

9.6 BMC 系统默认用户

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

- “root”：系统运行 app 进程时使用。
- “sshd”：系统运行 ssh 服务时使用。
- “apache”：系统运行 httpd 服务时使用。
- “snmpd_user”：系统运行 snmp 服务时使用。
- “ipmi_user”：系统运行 ipmi 服务时使用。
- “kvm_user”：系统运行远程控制台服务时使用。

- “discovery_user”：系统运行 SSDP 服务时使用。
- “comm_user”：系统运行 mctp 进程、rimm 进程以及 DDNS 服务时使用。
- “redfish_user”：系统运行 redfish 进程时使用。

说明

- 系统默认用户不能用于登录 BMC，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。

10 术语和缩略语

A

AC	Alternating Current（交流电）
AES	Advanced Encryption Standard（高级加密标准）

B

BBU	Backup Battery Unit（备份电池单元）
BIOS	Basic Input Output System（基本输入输出系统）
BMA	Baseboard Management Agent（单板管理代理）
BMC	Baseboard Management Controller（主板管理控制单元）

C

CA	Certificate Authority（证书颁发中心）
CD	Compact Disc（光盘）
CLI	Command-line Interface（命令行接口）
COM	Cluster Communication Port（COM 口）
CPLD	Complex Programmable Logic Device（复杂可编程逻辑器件）
CPU	Central Processing Unit（中央处理单元）
CRL	Certificate Revocation List（证书撤销列表）

D

disk	drive 的同义词，泛指所有硬盘。
drive	disk 的同义词，泛指所有硬盘。
DC	Direct Current（直流电）
DCMI 1.5	Data Center Manageability Interface Specification v1.5 （数据中心管理接口）
DES	Data Encryption Standard（数据加密标准）
DNS	Domain Name Server（网域名称服务器）
DVD	Digital Video Disc（数字视频光盘）

E

EIST	Enhanced Intel SpeedStep Technology（增强型 Intel SpeedStep 技术）
ESN	Equipment Serial Number（设备序列号）

F

FDM	Fault Diagnosis & Management（故障诊断管理）
FC	Fibre Channel（光纤通道）

G

GPU	Graphics Processing Unit（图形处理器）
GUI	Graphical User Interface（图形用户界面）

H

HDD	Hard Disk Drive（硬式磁盘驱动器）
HMM	Hyper Management Module（超级管理模块）
HPRE	High Performance RSA Engine（高性能 RSA 加速引擎）
HTTP	Hypertext Transfer Protocol（超文本传输协议）

HTTPS	Hypertext Transfer Protocol Secure (HTTPS 加密协定)

I

IMU	I/O Board Management Unit (IO 板管理单元)
IO	Integrated Operation (集成运作)
IP	Internet Protocol (互联网协议)
IPMI	Intelligent Platform Management Interface (智能平台管理接口)

J

JBOD	Just a Bundle Of Disks (磁盘簇)

K

Kerberos	是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。在 Hadoop 里面用于支撑多租户的实现。

L

LAN	Local Area Network (局域网)
LCD	Liquid Crystal Display (液晶显示器)
LDAP	Lightweight Directory Access Protocol (轻型目录访问协议)
LLDP	Link Layer Discovery Protocol (链路层发现协议)
LOM	LAN On Motherboard (板载网络)

M

MAC	Media Access Control (媒体接入控制)
MCTP	Management Component Transport Protocol (管理组件传输协议)

MD5	Message-Digest Algorithm 5（消息验证码）

N

NTP	Network Time Protocol（网络时间协议）
NMI	Non-Maskable Interrupt（不可屏蔽中断）
NCSI	Network Controller Sideband Interface（网络控制器边带接口）
NPU	Network Process Unit（网络处理单元）
NVMe	Non-Volatile Memory express（非易失性高速传输总线）

O

OS	Operating System（作业系统）
OCP	Open Compute Project（开放计算项目）
OID	Object Identifier（对象标识符）
OCSP	Online Certificate Status Protocol（在线证书状态协议）

P

PCB	Printed Circuit Board（印制电路板）
PCIe	Peripheral Component Interconnect Express（快捷外围部件互连标准）
PCH	Platform Controller Hub（平台控制单元）
PFAE	Proactive Failure Analysis Engine（主动故障分析引擎）
PXE	Pre-boot Execution Environment（预启动执行环境）
PSU	Power Supply Unit（电源模块）

Q

-	-

R

RAID	Redundant Array of Independent Disks（独立磁盘冗余数组）
RDE	RAID DIF engine（RAID DIF 运算加速引擎模块）
Redfish	DMTF 的 Redfish™API 是一个开放的行业标准规范和模式，有助于简化和安全管理现代可扩展平台硬件。
RFC	Request For Comments（请求注解）
RMCP	Remote Management Control Protocol（远程管理控制协议）

S

SAS	Serial Attached SCSI（串行连接的 SCSI）
SATA	Serial Advanced Technology Attachment（串行高级技术附件）
SEL	System Event Log（系统事件日志）
SFTP	Secure File Transfer Protocol（安全文件传输协议）
SHA	Secure Hash Algorithm（安全散列算法）
SID	Security Identifier（安全标识号）
SMTP	Simple Mail Transfer Protocol（简单邮件传输协议）
SNMP	Simple Network Management Protocol（简单网络管理协议）
SOL	Serial Over LAN（局域网承载串行）
SSD	Solid-State Drive（固态硬盘）
SSH	Secure Shell（安全外壳）
SSL	Secure Sockets Layer（安全套接层）
SSO	Single Sign-On（单点登录）

T

TLS	Transport Layer Security（传输层安全性协议）

U

UEFI	Unified Extensible Firmware Interface（统一可扩展固件接口）
UID	Unit Identification Light（定位指示灯）
UUID	Universally Unique Identifier（通用唯一识别码）
USB	Universal Serial Bus（通用串行总线）

V

VLAN	Virtual Local Area Network（虚拟局域网）

W

WWPN	World Wide Port Name（全球端口名称）
WWNN	World Wide Node（全球唯一节点名字）

X

-	-

Y

-	-

Z

-	-