

鲲鹏服务器主板

Toolkit 用户指南

发布日期 2023-01-13

概述

Kunpeng Toolkit是一款以华为厂商信息进行配置的工具，提供给合作厂商的研发人员使用。合作厂商研发人员需要根据自己鲲鹏产品的定制情况对Kunpeng Toolkit进行适配开发和验证产品兼容性。适配开发请参见《鲲鹏服务器主板 Toolkit 接口定制说明》。合作厂商研发团队对Kunpeng Toolkit进行适配开发和验证后，再提供新版本工具给现场工程师使用。现场工程师使用工具过程中遇到问题，先联系合作厂商研发人员支撑。如果合作厂商研发人员确认问题是华为提供的原始版本工具的问题，再联系华为技术工程师。

说明

不允许现场工程师直接使用华为提供的原始版本Kunpeng Toolkit在客户环境上进行运维操作。

本文档介绍了如何使用工具进行开局交付、例行维护、故障处理、升级/补丁等操作，供合作厂商研发人员参考。

读者对象

本文档主要适用于合作厂商研发人员。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

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

符号	说明
 说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

文档版本	发布日期	修改说明
06	2023-01-13	<ul style="list-style-type: none">• 更新3 介绍工具箱• 更新4 使用工具箱• 更新5 常见操作
05	2022-02-18	更新4.1.1 BMC配置。
04	2021-09-17	<ul style="list-style-type: none">• 更新前言。• 新增4.8 拷机章节。
03	2021-04-20	更新前言。
02	2020-12-31	更新1 概述。
01	2020-08-28	第一次正式发布。

目 录

前言	ii
1 概述	1
2 安装工具箱	3
3 介绍工具箱	4
3.1 首页.....	4
3.2 设备列表.....	5
3.3 功能分布.....	8
4 使用工具箱	9
4.1 硬件配置.....	9
4.1.1 BMC 配置.....	9
4.1.1.1 配置流程.....	9
4.1.1.2 使用前准备.....	10
4.1.1.3 选择设备.....	10
4.1.1.4 配置 BMC.....	12
4.1.1.4.1 配置 BMC.....	13
4.1.1.4.2 BMC 配置项清单.....	18
4.1.1.5 常见问题处理.....	28
4.1.2 BIOS 配置.....	31
4.1.2.1 配置流程.....	31
4.1.2.2 使用前准备.....	32
4.1.2.3 选择设备.....	32
4.1.2.4 配置 BIOS.....	34
4.1.2.5 常见问题处理.....	39
4.1.3 RAID 配置.....	41
4.1.3.1 配置流程.....	41
4.1.3.2 使用前准备.....	41
4.1.3.3 选择设备.....	42
4.1.3.4 配置 RAID.....	44
4.2 OS 部署.....	52
4.2.1 操作流程.....	52
4.2.2 使用前准备.....	53
4.2.3 选择设备.....	54

4.2.4 OS 部署.....	56
4.2.5 设置参数.....	61
4.2.6 执行部署.....	62
4.3 IP 配置.....	62
4.3.1 配置流程.....	62
4.3.2 使用前准备.....	62
4.3.3 IP 配置.....	63
4.4 健康检查.....	67
4.4.1 兼容性列表.....	67
4.4.2 流程图.....	69
4.4.3 使用前准备.....	69
4.4.4 选择设备.....	70
4.4.5 健康检查.....	72
4.4.6 巡检项统计表.....	77
4.5 电源控制.....	78
4.5.1 配置流程.....	78
4.5.2 使用前准备.....	78
4.5.3 选择设备.....	78
4.5.4 电源控制.....	81
4.5.5 常见问题处理.....	84
4.6 配置检查.....	86
4.6.1 配置流程.....	86
4.6.2 使用前准备.....	86
4.6.3 选择设备.....	87
4.6.4 检查配置.....	89
4.6.5 常见问题处理.....	94
4.7 日志收集.....	95
4.7.1 兼容性列表.....	96
4.7.2 批量服务器日志收集使用指导.....	98
4.7.2.1 日志收集流程.....	98
4.7.2.2 使用前准备.....	98
4.7.2.3 选择设备.....	99
4.7.2.4 日志收集.....	101
4.7.3 单机 OS 日志收集使用指导.....	104
4.7.3.1 收集 Linux 操作系统日志.....	104
4.7.4 日志收集项清单.....	108
4.8 拷机.....	141
4.8.1 拷机流程.....	141
4.8.2 使用前准备.....	142
4.8.3 选择设备.....	142
4.8.4 拷机.....	144
4.8.4.1 S920 服务器拷机测试.....	147

4.8.4.2 S916 服务器拷机测试.....	151
4.9 固件升级.....	154
4.9.1 升级固件.....	154
4.9.1.1 固件升级流程.....	154
4.9.1.2 使用前准备.....	155
4.9.1.3 选择设备.....	155
4.9.1.4 升级服务器固件.....	158
4.9.1.4.1 单部件升级服务器固件.....	158
4.9.1.4.2 多部件升级服务器固件.....	166
4.9.1.4.3 升级 Smart Provisioning.....	173
4.9.1.5 常见问题处理.....	179
4.9.1.5.1 操作系统侧的看门狗异常问题.....	179
4.9.1.5.2 下电失败导致升级 BIOS 或 CPLD 失败问题.....	182
4.9.1.5.3 sp 升级使用 cifs/nfs 服务搭建方法.....	182
4.9.1.5.4 其他问题.....	190
4.9.2 升级 PCIe 卡/硬盘固件.....	195
4.9.2.1 升级流程.....	195
4.9.2.2 使用前准备.....	196
4.9.2.3 选择设备.....	196
4.9.2.4 升级 PCIe 卡/硬盘固件.....	198
4.9.2.5 常见问题处理.....	202
4.10 设备变更.....	205
4.10.1 设备变更流程.....	205
4.10.2 使用前准备.....	205
4.10.3 选择设备.....	206
4.10.4 设备变更.....	208
4.10.5 常见问题处理.....	212
5 常见操作.....	216
5.1 查看 RAID 卡信息.....	216
5.2 查看 BMC 固件版本信息.....	217
5.3 查看 BMC 端口信息.....	219
5.4 查看 BMC 的 SNMP 协议.....	221
5.5 开启和配置 IPv6 功能.....	223

1 概述

工具箱中包含了对服务器设备进行批量部署、维护、升级等操作所需的各类工具，能够帮助服务工程师、维护工程师在上述过程中对设备进行精准操作，降低操作难度、提升工作效率。您可以通过本操作指导书了解详细的场景任务操作方式。

工具箱集成的服务器领域的场景任务见表1-1。

表 1-1 服务器领域下场景任务说明

场景任务	任务描述	参考
BMC配置	支持服务器批量配置BMC功能	4.1.1 BMC配置
BIOS配置	支持服务器批量配置BIOS功能	4.1.2 BIOS配置
RAID配置	支持服务器批量配置RAID功能	4.1.3 RAID配置
OS 部署	支持服务器批量部署操作系统及驱动安装	4.2 OS部署
IP配置	支持服务器批量设置BMC IP地址	4.3 IP配置
健康检查	提供批量巡检设备功能，呈现可视化健康检查报告，实时掌握设备运行状态	4.4 健康检查
电源控制	提供设备电源控制功能，支持批量重启BMC、系统上下电、重启等操作	4.5 电源控制
配置检查	支持批量检查服务器的BMC、BIOS、RAID配置	4.6 配置检查
日志收集	支持批量一键式收集服务器硬件及操作系统日志信息	4.7 日志收集
拷机	支持用户使用拷机功能对服务器的CPU、内存、硬盘进行性能测试	4.8 拷机
固件升级	支持批量升级服务器的BMC、BIOS、CPLD、SP等固件	4.9.1 升级固件
升级PCIe卡/硬盘固件	通过挂载虚拟媒体升级PCIe卡/硬盘固件	4.9.2 升级PCIe卡/硬盘固件

场景任务	任务描述	参考
设备变更	通过自定义的程序自动执行特定功能	4.10 设备变更

2 安装工具箱

本章主要介绍如何安装工具箱。

操作步骤

步骤1 将工具箱软件包，解压至自定义位置。

说明

解压路径中不能有“-”等特殊字符。

步骤2 修改解压后软件包所在文件夹的名称，不能包含“-”。

步骤3 打开修改后的文件夹，双击“start.exe”，即可使用该工具。

----结束

3 介绍工具箱

本章主要介绍工具箱的工具界面以及各项功能。通过本章您可以了解工具箱的主要功能特点以及使用方法。

3.1 首页

工具首页界面及各区域功能描述如图3-1所示，首页界面功能描述如表3-1所示。

图 3-1 首页

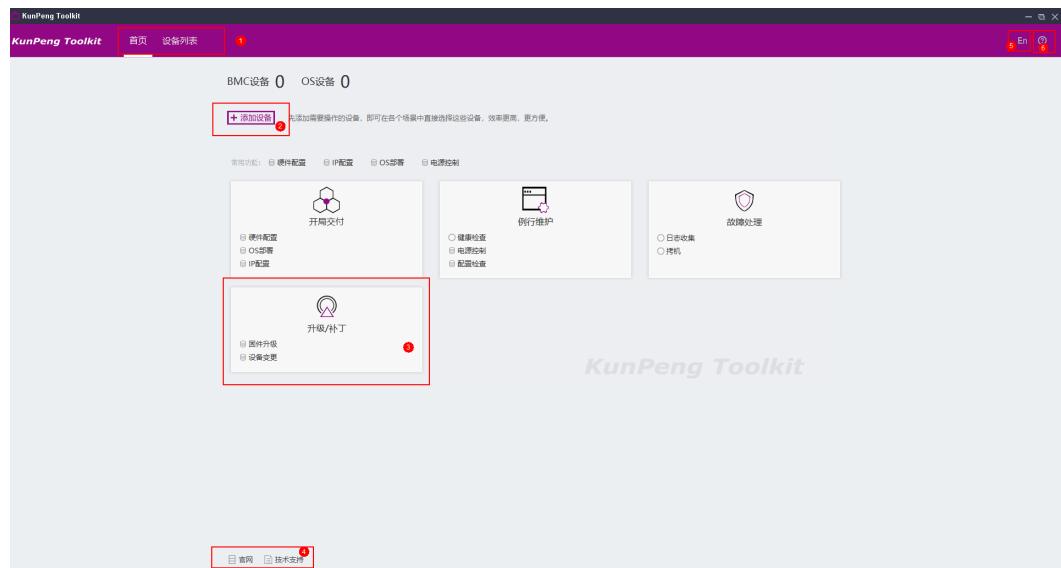


表 3-1 首页界面功能描述

区域	功能描述
1	功能导航栏：通过此导航栏可以选择功能类别。

区域	功能描述
2	增加操作设备。
3	场景化入口：单击此入口，可以使用相应的场景化功能。
4	链接（官网） 链接（技术支持）
5	语言切换
6	帮助 关于

3.2 设备列表

在“设备列表”界面，您可以添加需要维护和管理的设备，并对已添加的设备进行修改、移除、更新等操作。

该界面如图3-2所示，各区域功能描述和表3-2所示。

图 3-2 设备列表

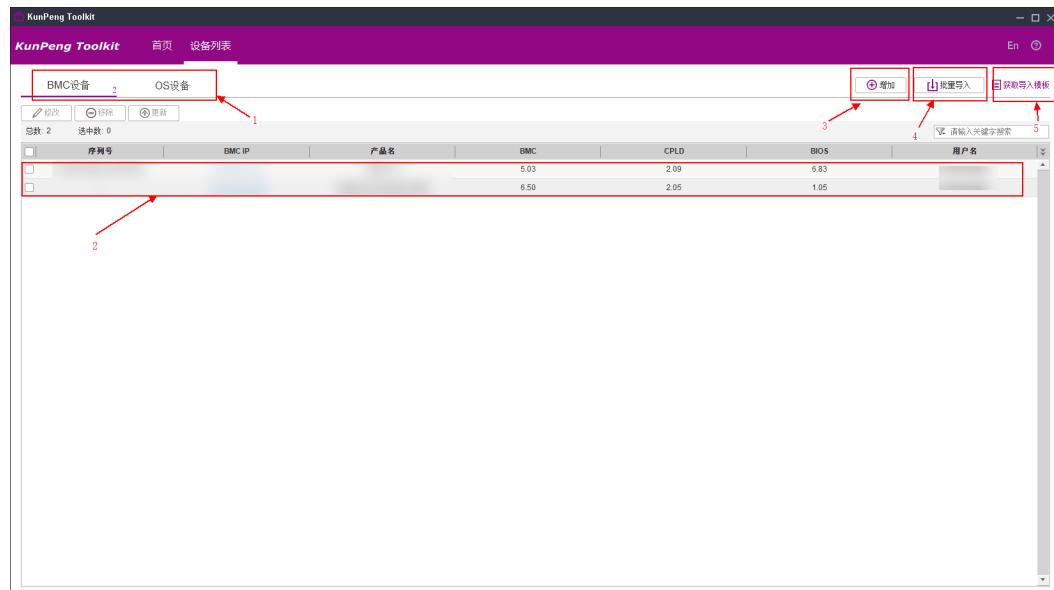


表 3-2 设备列表界面功能描述

区域	功能描述
1	BMC：服务器管理软件 OS：操作系统
2	显示已添加设备的详细信息。
3	增加单台设备。

区域	功能描述
4	批量导入设备：将“获取导入模板”批量填写设备信息后，从此入口导入。
5	获取批量导入设备模板。

- 添加设备界面，如图3-3所示，各参数说明，如表3-3所示。

图 3-3 增加设备



- 批量导入设备界面，如图3-4所示。选择设备列表文件“ServerDeviceList_Template.xls”，单击“确定”即可完成批量导入设备。模板文件内的相关参数说明如表3-3所示。

图 3-4 批量导入

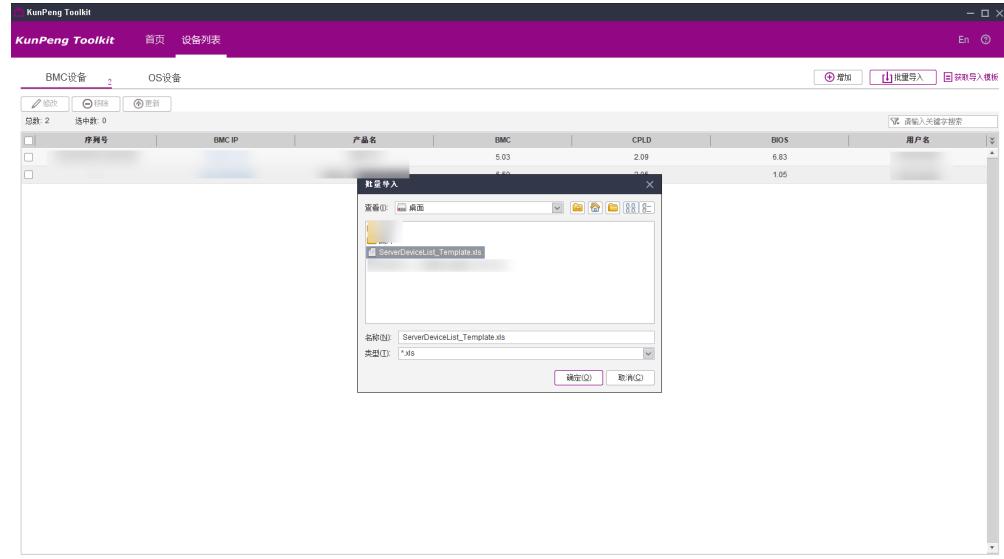


表 3-3 参数说明

类型	名称	说明	备注
-	起始IP	起始IP地址。	此处IP地址仅支持IPv4或IPv6。
	结束IP	结束IP地址。	<ul style="list-style-type: none"> • 此处IP地址仅支持IPv4或IPv6。 • 单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f434 • 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f439 • 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。
	用户名	管理员用户名。	-
	密码	管理员密码。	-
高级设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	默认值是8208，以设备实际启用的端口号为准。

类型	名称	说明	备注
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。
OS选项	root密码	root用户密码。	非root用户操作Linux操作系统时需要输入root用户密码。

3.3 功能分布

工具箱集成的服务器领域的场景功能如表3-4所示。

表 3-4 支持场景功能分布表

功能模块	子功能	场景	子场景
开局交付	硬件配置	硬件配置	BMC配置
			BIOS配置
			RAID配置
	电源控制	-	-
		-	-
		-	-
OS部署	OS部署	-	-
	IP配置	IP配置	-
	健康检查	健康检查	-
		日志收集	-
例行维护	电源控制	电源控制	-
	配置检查	配置检查	-
	日志收集	-	-
故障处理		-	-
拷机	拷机	-	
升级/补丁	固件升级	升级固件	-
		升级PCIe卡/硬盘固件	-
	设备变更	设备变更	-

4 使用工具箱

本章主要介绍工具箱在服务器领域支持的场景任务和相关的操作指导。

□ 说明

- Toolkit适配鲲鹏服务器主板V586及以上的BMC版本。
- 运行环境若选择最低硬件配置系统，工具使用过程中速度会相对较慢，支持的服务器也会相应减少，建议配置CPU8核3Ghz以上，可用内存4GB以上，硬盘空间8GB以上。

4.1 硬件配置

4.2 OS部署

4.3 IP配置

4.4 健康检查

4.5 电源控制

4.6 配置检查

4.7 日志收集

4.8 捷机

4.9 固件升级

4.10 设备变更

4.1 硬件配置

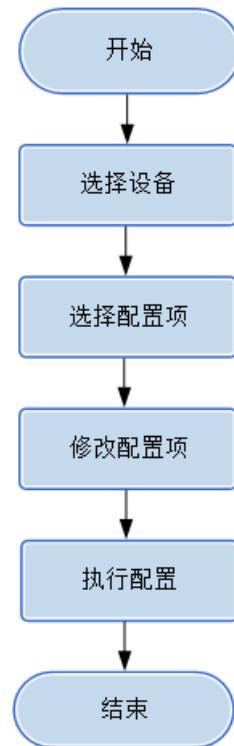
4.1.1 BMC 配置

本节指导用户使用工具箱进行BMC配置。

4.1.1.1 配置流程

BMC配置流程如图4-1所示。

图 4-1 BMC 配置流程



4.1.1.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH通信端口连通，保证能ping通服务器BMC的IP地址。

确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC的IP地址。
- 服务器BMC管理员用户名和密码。

4.1.1.3 选择设备

在硬件配置向导的“选择设备”界面中，可以选择需要进行配置的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“开局交付>硬件配置”。

系统进入“硬件配置”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要BMC配置的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

□ 说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如表4-1所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考表4-1，手工输入参数。

表 4-1 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none">单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f434多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f439多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-

类型	名称	说明	备注
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	默认值是8208，以设备实际启用的端口号为准。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要BMC配置的设备。单击“确定”，返回向导界面。

----结束

4.1.1.4 配置 BMC

在BMC配置界面中，可以对所选择的设备进行BMC配置。

□ 说明

- 批量配置要求为同机型的服务器，建议先配置一台服务器，待没有问题后，再进行批量配置，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 支持的BMC配置项请参考[4.1.1.4.2 BMC配置项清单](#)。
- 若需要批量配置LDAP，则服务器BMC需满足以下任意条件：
 - BMC版本同为2.01及以上，且低于2.50。
 - BMC版本同为2.50及以上。

4.1.1.4.1 配置 BMC

操作步骤

步骤1 在硬件配置向导界面单击“硬件配置”。

系统弹出“配置BMC、BIOS、RAID”选择框。

步骤2 单击“BMC配置”。

系统进入BMC配置向导“欢迎”界面，查看可以操作的配置项，如图4-2所示。

图 4-2 欢迎



说明

参见[4.1.1.4.2 BMC配置项清单](#)，查看详细信息。

步骤3 单击“下一步”。

进入“获取设备信息”界面，如图4-3所示。

图 4-3 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤4 在设备列表中选择需要配置BMC的设备。如果批量配置BMC，建议选择型号和BMC版本都相同的设备。

步骤5 单击“下一步”。

进入发现服务器界面，发现服务器后系统自动进入选择服务器界面。

说明

- 单击“停止”可终止此次任务。
- 单击“日志目录”可进入服务器发现结果文件“output.xml”的保存目录。
- 单击“导出”可将此界面的配置结果保存至本地（默认保存“.xls”格式）

步骤6 选择需要进行BMC配置的服务器，单击“下一步”。

进入“选择项目”界面，如图4-4所示。

图 4-4 选择项目



说明

- 单击“所有设置”可选中或取消选中所有的配置项。
- 网络设置不能批量配置，只有选择一台服务器时，才能被选择。
- 网络设置及批量修改密码不能和其他配置项同时配置。
- 如需配置批量安装license，请先联系技术支持获取license。
- 如果在“选择项目”界面勾选了“用户设置”，执行下一步“更改设置”时，必须要勾选一个用户进行配置，否则无法进行下一步。
- 如果在“选择项目”界面勾选了“BMC许可证”，执行下一步“更改设置”时，必须导入许可证文件，否则无法进行下一步。

步骤7 选择需要配置的配置项，单击“下一步”。

进入“更改设置”界面，如图4-5所示。

图 4-5 更改设置



步骤8 根据4.1.1.4.2 BMC配置项清单，修改所选配置。

须知

用户配置完成后，需要等待30秒后再进行其他操作，以免出现错误。

- 如果选择了“系统设置”

说明

工具会自动过滤掉不支持的设置项。

- 如果选择了“安全设置”

说明

配置KVM、VMM配置项时，需保证待配置服务器KVM连接已关闭。

- 如果选择了“端口设置”

说明

修改端口（IPMI、SNMP、SSH）使能状态或端口号后，需要重新发现服务器，以免出现错误。

- 如果选择了“BMC许可证”

- 单击“保存”，获取服务器的ESN列表。
- 单击“选择”，选择需要导入的License的zip包。

说明

BMC从V316版本开始，采用License文件方式控制版本功能。

- 如果选择了“批量修改密码”

a. 单击“导出配置模板”，导出.xls文件，如图4-6所示。

图 4-6 .xls 文件

```
StartIPAddress,EndIPAddress,UserName,UserPassword,  
192.168.2.35,192.168.2.37,root,*****  
192.168.2.35,192.168.2.35,test1,*****  
192.168.2.35,192.168.2.35,test2,*****
```

b. 按照.xls文件中示例的格式输入起始IP地址、结束IP地址、用户名和密码，保存文件。
c. 在界面单击“选择”后，选择编辑好后的.xls文件导入。

说明

- BMC密码复杂度要求如下：
 - 长度为8 ~ 20个字符。
 - 至少包含一个空格或者以下特殊字符：`~!@#\$%^&*()_-+=\|[{}]:;'"<.>/?
 - 至少包含以下字符中的两种：小写字母：a ~ z；大写字母：A ~ Z；数字：0 ~ 9
 - 密码不能是用户名或用户名的倒序。
 - 新旧口令至少在2个字符位上不同。

步骤9 完成配置项修改后，单击“下一步”。

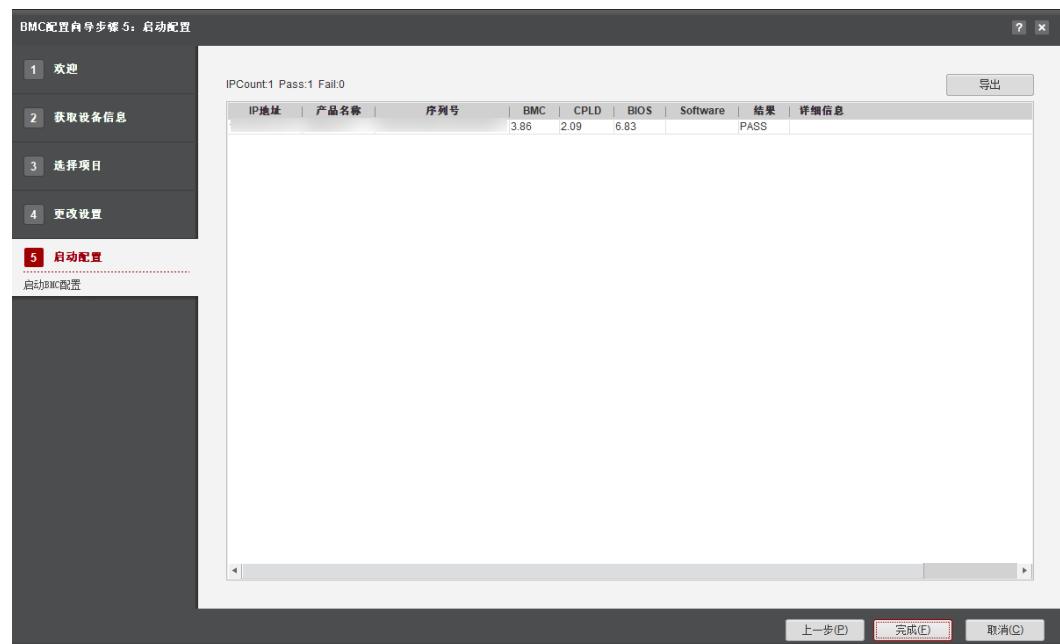
弹出“此操作可能会中断服务，请确认是否要继续”的提示框。

步骤10 如果继续执行，则在输入框中输入“yes”后单击“确定”。

进入“启动配置”界面。

步骤11 配置完成后自动进入配置结果界面，如图4-7所示。

图 4-7 启动配置



说明

单击“导出”可将此界面的配置结果保存至本地（默认保存“.xls”格式）。

步骤12 在配置结果界面，“结果”列表示配置结果。

单击“完成”退出，向导界面显示成功和未执行的服务器台数，以及总用时。

----结束

4.1.1.4.2 BMC 配置项清单

BMC配置项清单，如[表4-2](#)所示。

表 4-2 BMC 配置项清单

参数	配置项	子配置项	取值范围	备注
NTP设置	是否使能	-	<ul style="list-style-type: none">使能不使能	-
	工作模式	-	<ul style="list-style-type: none">自动手工	
	首选NTP服务器	-	IP地址（IPv4或IPv6）或域名，域名最大长度为255个字符。	
	备选NTP服务器	-		
LDAP组设置	是否使能	-	<ul style="list-style-type: none">使能不使能	勾选复选框为使能，不勾选为不使能
	LDAP服务器地址	-	0~255位的字符串，由数字、英文字母和特殊字符（包括空格）组成。	-
	域名	-	0~255位的字符串，由数字、英文字母和特殊字符组成。	-
	LDAP分组	组名	0~32位的字符串，由数字、英文字母和特殊字符组成。	最多可设置5组 <ul style="list-style-type: none">若需要批量配置LDAP，则服务器BMC需满足以下任意要求：<ul style="list-style-type: none">BMC版本同为2.01及以上，且低于2.50。
		LDAP组应用文件夹	0~255位的字符串，由数字、英文字母和特殊字符组成。	

参数	配置项	子配置项	取值范围	备注
		组权限	管理员、操作员、普通用户、自定义（单选）	- BMC版本同为2.50及以上。
启动选项 [Note1]	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/可插拔移动设备	-	-	表示强制从软驱或可插拔移动设备启动系统。
	PXE	-	-	表示强制从预启动执行环境（PXE, Pre-boot Execution Environment）启动系统。
	BIOS设置	-	-	表示服务器启动后直接进入BIOS菜单中。
	未配置	-	-	表示不设置第一启动设备，按BIOS中设置的默认方式启动操作系统。
系统设置	时区	-	GMT-12:00 ~ GMT+14:00	-
	上电策略	上电	-	服务器的电源模块通电后系统自动开机。
		保持上一次状态	-	<p>服务器的电源模块通电后保持断电前状态：</p> <ul style="list-style-type: none"> 若断电前服务器是开机状态，则通电后系统自动开机。 若断电前服务器是关机状态，则通电后系统不上电。

参数	配置项	子配置项	取值范围	备注
		保持下电	-	服务器的电源模块通电后系统不上电。
下电超时设置	是否使能	• 使能 • 不使能		勾选复选框为使能, 不勾选为不使能。
	下电超时时间	10~6540 (秒)	-	
功率封顶	是否使能	• 使能 • 不使能		勾选复选框为使能, 不勾选为不使能。
	封顶值	1~9999 (瓦)	-	
	封顶后是否下电	• 下电 • 不下电		勾选复选框为下电, 不勾选为不下电。
Web Server超时时长设置	-	5~480 (分钟)	-	
远程控制台超时时长设置	-	0~480 (分钟)	0表示不超时。	
HostName同步至SysName	-	• 使能 • 不使能		• 勾选复选框表示主机名同步到系统名, 不勾选表示关闭同步功能。 • BMC 3.34及之后的版本支持该功能。
告警电子邮件设置	是否使能	-	• 使能 • 不使能	勾选复选框为使能, 不勾选为不使能。
	服务器地址	-	IP地址	-
	TLS使能	-	• 使能 • 不使能	勾选复选框为使能, 不勾选为不使能。
	匿名使能	-	• 使能 • 不使能	勾选复选框为使能, 不勾选为不使能。

参数	配置项	子配置项	取值范围	备注
	设置电子邮件信息	用户名	1~64位的字符串,由数字、英文字母和特殊字符组成。	-
		密码	0~50位的字符串(密码为该用户在对应SMTP服务器上的用户密码)。	-
		地址	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	0~255位的字符串,由数字、英文字母和特殊字符组成。	主题附带(可选): <ul style="list-style-type: none">● 主机名● 单板序列号● 产品资产标签
	告警级别	紧急	-	仅发送紧急级别的告警信息。
		严重及以上	-	发送包括严重、紧急级别的告警信息。
		轻微及以上	-	发送包括轻微、严重、紧急级别的告警信息。
		正常及以上	-	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。
	设置用于接收警报的电子邮件地址	是否使能	<ul style="list-style-type: none">● 使能● 不使能	可设置4组。
		地址	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,式必须为“xx@xxx.xx”。	
		描述	0~255位的字符串,由数字、英文字母和特殊字符组成。	

参数	配置项	子配置项	取值范围	备注
告警上报设置	是否使能	-	<ul style="list-style-type: none"> 使能 不使能 	勾选复选框为使能, 不勾选为不使能。
	SNMP模式	V1	-	默认支持V1版本, 建议用户使用V3版本。
		V2C	-	
		V3	-	
	选择Trap v3用户	-	在“选择Trap v3用户”下拉列表中, 选择Trap V3协议使用的BMC用户。	-
	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	-	以SNMP节点的OID作为Trap事件的标识。
		事件码	-	以产生事件的事件码作为Trap事件的标识。
	Trap主机标识	单板序列号	-	-
		产品资产标签	-	-
		主机名	-	-
	团体名	-	SNMP使用的共同体名称, 团体名为Trap方式的口令。“版本”设置为“V1”或“V2C”时才能设置“团体名”。	团体名取值原则, 请根据服务器型号的BMC版本参考对应的BMC 用户指南。
	告警级别	紧急	-	仅发送紧急级别的告警信息。
		严重及以上	-	发送包括严重、紧急级别的告警信息。

参数	配置项	子配置项	取值范围	备注
系统日志设置		轻微及以上	-	发送包括轻微、严重、紧急级别的告警信息。
		正常及以上	-	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。
	服务器地址	是否使能	<ul style="list-style-type: none"> 使能 不使能 	可设置4组。
		地址	IPv4、IPv6或域名	
		Trap端口号	1~65535， 默认为：“162”	
	是否使能	-	<ul style="list-style-type: none"> 使能 不使能 	勾选复选框为使能，不勾选为不使能。
	主机标识	单板序列号	-	-
		产品资产标签	-	-
		主机名	-	-
	告警级别	紧急	-	仅发送紧急级别的告警信息。
		严重及以上	-	发送包括严重、紧急级别的告警信息。
		轻微及以上	-	发送包括轻微、严重、紧急级别的告警信息。
		正常及以上	-	发送包括轻微、严重、紧急级别的告警信息，以及正常事件信息。
	传输协议	TLS	-	可选认证类型： <ul style="list-style-type: none"> 单向认证 双向认证
		TCP	-	-
		UDP	-	-

参数	配置项	子配置项	取值范围	备注
	服务器地址	是否使能	<ul style="list-style-type: none"> 使能 不使能 	可设置4组。
		地址	0~255位的字符串，由数字、英文字母和特殊字符（包括空格）组成。	
		端口号	1~65535	
		日志类型	操作日志、安全日志、事件日志（多选）	
	用户设置	用户名	- 1~16位的字符串：由特殊符号、英文字母和数字组成，不能包含空格且首字符不能是“#”。特殊字符不包括：:<>&,""/\%	可设置16个用户。
		密码	- 最大为20位的字符串： <ul style="list-style-type: none"> 若启用了密码复杂度检查功能，则设置和修改的密码必须遵循密码复杂度的规则。 若未启用密码复杂度检查功能，则设置和修改的密码可为任意字符。 	
		权限组	管理员 操作员 普通用户 自定义 1~自定义4 无权限	
		Vlan	是否使能 <ul style="list-style-type: none"> 使能 不使能 	
		Vlan ID	1~4094	-
		IPV4	自动获取地址 手工获取地址	- -

参数	配置项	子配置项	取值范围	备注
		IP地址	IPv4地址	-
		子网掩码	-	-
		网关	-	-
		MAC地址	-	不可修改。
	DNS	自动获取	-	-
		手工设置	-	-
		域名	0~67位的字符串：由数字、英文字母和特殊字符（包括空格）组成	-
		主服务器	IP地址	-
		从服务器	IP地址	-
DNS设置	自动获取	-	-	-
	手工设置	-	-	-
	域名	-	0~67位的字符串：由数字、英文字母和特殊字符（包括空格）组成	-
	首选服务器	-	IP地址	-
	备用服务器	-	IP地址	-
IP模式设置	IP地址模式	-	<ul style="list-style-type: none"> • dhcp • static 	<ul style="list-style-type: none"> 当IP模式为“dhcp”时，支持自动获取DNS IPV4地址，也支持手动配置DNS地址。 当IP模式为“static”时，不支持自动获取DNS IPV4地址，仅支持手动配置DNS地址。
BMC主机名	BMC主机名	产品序列号	-	将产品序列号配置为BMC主机名。
		单板序列号	-	将单板序列号配置为BMC主机名。

参数	配置项	子配置项	取值范围	备注
		手动配置	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。	将输入内容配置为BMC主机名。
安全设置	密码复杂度检查	-	<ul style="list-style-type: none"> • 使能 • 不使能 	-
	密码超时时长	-	0~365（天），0表示无限期。	
	禁用历史密码	-	0~5（0表示不禁用）	
	登录失败锁定	-	0~5（0表示关闭登录失败锁定功能）	
	锁定时长	-	1~5（分钟）	
	KVM加密	-	<ul style="list-style-type: none"> • 使能 • 不使能 	
	VMM加密	-	<ul style="list-style-type: none"> • 使能 • 不使能 	
端口设置	FTP	-	1~65535， 默认为：“21”	-
	SSH	-	1~65535， 默认为：“22”	
	Telnet	-	1~65535， 默认为：“23”	
	SNMP Agent	-	1~65535， 默认为：“161”	
	KVM	-	1~65535， 默认为：“2198”	
	VMM	-	1~65535， 默认为：“8208”	
	Video	-	1~65535， 默认为：“2199”	
	Web Server (http)	-	1~65535， 默认为：“80”	
	Web Server (https)	-	1~65535， 默认为：“443”	

参数	配置项	子配置项	取值范围	备注
	IPMI LAN (RMCP)	-	1~65535 Port 1为主用端口， 默认为“623”； Port 2为备用端口， 默认为“664”	<ul style="list-style-type: none"> 修改配置项“IPMI LAN (RMCP)”与“IPMI LAN (RMCP+)”后，需要重启BMC才能使其生效。
	IPMI LAN (RMCP+)	-	RMCP+和RMCP端口共用，设置RMCP端口时RMCP+也使用相同的端口。	
BMC许可证	ESN	-	-	用于申请许可证的ESN，由主板的序列号生成。
	许可证	-	-	BMC从V316版本开始，采用License文件方式控制版本功能。
批量修改密码	配置文件	-	-	根据模板示例的格式编辑配置文件。
批量安装license	批量安装license	-	-	<ul style="list-style-type: none"> 服务器已预置TrustZone套件（预装iTrustee安全OS及配套的BMC和BIOS固件）。 要求BMC版本为3.01.12.49及以上，且BIOS版本为1.83及以上。
批量修改电子保单信息	批量修改电子保单信息	-	-	导出配置模板，按要求填写后，导入工具进行配置。
智能调速	节能模式	-	-	-
	低噪声模式	-	-	
	高性能模式	-	-	
	液冷模式	-	-	

参数	配置项	子配置项	取值范围	备注
	用户自定义模式	-	<ul style="list-style-type: none"> • CPU目标调速温度值 • 进风口温度区间 • 转速值 	-
Note1. BMC V236之前版本，系统启动项的配置均为单次有效（即仅下一次服务器启动有效，下同）；BMC V236及之后版本，系统启动项配置支持设置引导介质有效期，包含单次有效和永久有效两种选择项，默認為单次有效，如引导介质有效期被修改为永久生效，则系统启动项的修改为永久生效。				

□ 说明

不同服务器和BMC版本支持的配置项会有差异。

4.1.1.5 常见问题处理

表 4-3 常见问题

错误描述	原因	解决建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
Cannot login by SSH or SFTP	无法通过SSH或SFTP方式登录服务器。	<ol style="list-style-type: none"> 1. 查看SSH端口是否打开，端口号与工具配置的是否一致，详细请参考5.3 查看BMC端口信息。 2. 使用Xshell软件或者其他软件尝试通过SSH及SFTP方式登录服务器，查看是否可正常登录。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。

错误描述	原因	解决建议
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none"> SNMP配置错误或服务器不支持SNMP命令。 SNMP未响应。 	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看BMC端口信息、5.4 查看BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none"> 确认该操作是否符合规范。 重新执行该操作。
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合SNMP要求。	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查密码是否满足SNMP V3的要求，如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3协议不一致或用户名/密码不一致，引起巡检（升级）串行。	<ol style="list-style-type: none"> 检查所有服务器配置的SNMP V3协议是否一致，并将其调整一致。 检查所有服务器的用户名、密码是否一致，并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话，IPMI命令执行失败。	<ol style="list-style-type: none"> 手工执行IPMI命令，检查是否存在问题。 待问题解决后，重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 检查网络是否有异常。 重新执行任务。
User must be an administrator.	使用非管理员账户执行该操作。	<ol style="list-style-type: none"> 检查用户是否为管理员账户。 使用管理员账户重新执行该操作。

错误描述	原因	解决建议
Cannot login by SSH or SFTP, please execute with the manual mode.	无法通过SSH及SFTP登录服务器。	通过手工方式完成操作。
The current version of BMC does not support Boot Option settings,please upgrade to the latest version	当前BMC版本不支持Boot Option配置。	升级BMC版本至最新版本后再进行配置。
The current version of BMC does not support LDAP settings,please upgrade to the latest version	当前BMC版本不支持LDAP配置。	升级BMC版本至最新版本后再进行配置。
This device does not support NTP settings	当前服务器不支持NTP配置。	查看服务器是否支持运行工具： • 在，需要升级BMC版本后重试。 • 不在，不支持配置。
The current version of BMC does not support Network settings,please upgrade to the latest version	当前BMC版本不支持网络配置。	升级BMC版本至最新版本后再进行配置。
This device does not support port settings	当前服务器不支持端口号配置。	查看服务器是否支持运行工具： • 在，需要升级BMC版本后重试。 • 不在，不支持配置。
The current version of BMC does not support Alarm Email settings,please upgrade to the latest version	当前BMC版本不支持邮件配置。	升级BMC版本至最新版本后再进行配置。
This device does not support local user security settings	当前服务器不支持安全配置。	查看服务器是否支持运行工具： • 在，需要升级BMC版本后重试。 • 不在，不支持配置。

错误描述	原因	解决建议
The current version of BMC does not support Time Zone settings,please upgrade to the latest version	当前BMC版本不支持时区配置。	升级BMC版本至最新版本后再进行配置。
The current version of BMC does not support System settings,please upgrade to the latest version	当前BMC版本不支持系统配置。	升级BMC版本至最新版本后再进行配置。
The current version of BMC does not support Alarm Trap settings,please upgrade to the latest version	当前BMC版本不支持Trap配置。	升级BMC版本至最新版本后再进行配置
The current version of BMC does not support User settings,please upgrade to the latest version	当前BMC版本不支持用户配置。	升级BMC版本至最新版本后再进行配置。
The current version of BMC does not support Alarm Syslog settings, please upgrade to the latest version	当前BMC版本不支持Syslog配置。	升级BMC版本至最新版本后再进行配置。
Please turn off the KVM connection, then try again	未关闭远程虚拟控制台。	关闭远程虚拟控制台后再进行配置。

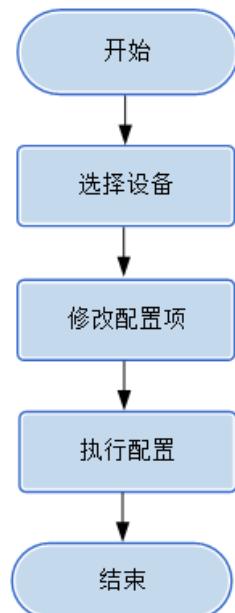
4.1.2 BIOS 配置

本节指导用户使用工具箱进行BIOS配置。

4.1.2.1 配置流程

BIOS配置流程如图4-8所示。

图 4-8 BIOS 配置



4.1.2.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH通信端口连通，保证能ping通服务器BMC的IP地址。

确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC的IP地址。
- 服务器BMC用户名和密码。

4.1.2.3 选择设备

在硬件配置向导的“选择设备”界面中，可以选择需要进行配置的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“开局交付>硬件配置”。

系统进入“硬件配置”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要BIOS配置的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明书

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如表4-4所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考表4-4，手工输入参数。

表 4-4 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none">单台设备时，和“起始IP”相同，如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.2.2 IPv6： 起始IP：2017::f434 结束IP：2017::f434多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.5.254 IPv6： 起始IP：2017::f434 结束IP：2017::f439多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-

类型	名称	说明	备注
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	请忽略该参数，或者保持默认值。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要BIOS配置的设备。单击“确定”，返回向导界面。

----结束

4.1.2.4 配置BIOS

在BIOS配置界面中，可以对所选择的设备进行BIOS配置。

□ 说明

- 批量配置要求为同机型的服务器，建议先配置一台服务器，待没有问题后，再进行批量配置，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 操作过程中遇到的问题请参考[4.1.2.5 常见问题处理](#)解决。

须知

- 操作过程中，请勿对服务器进行系统上下电及重启等操作。
- BIOS配置成功后，需要使用工具或手工将系统复位，才可使BIOS配置生效。

操作步骤

步骤1 在硬件配置向导界面上单击“硬件配置”。

系统弹出“配置BMC、BIOS、RAID”选择框。

步骤2 单击“BIOS配置”。

系统进入BIOS配置向导“欢迎”界面，如图4-9所示，查看可以执行的配置项清单。

图 4-9 欢迎



步骤3 单击“下一步”。

进入“获取设备信息”界面，如图4-10所示。

图 4-10 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤4 在设备列表中勾选需要配置BIOS的设备。

步骤5 单击“下一步”。

进入发现服务器界面，发现服务器后系统自动进入选择服务器界面。

说明

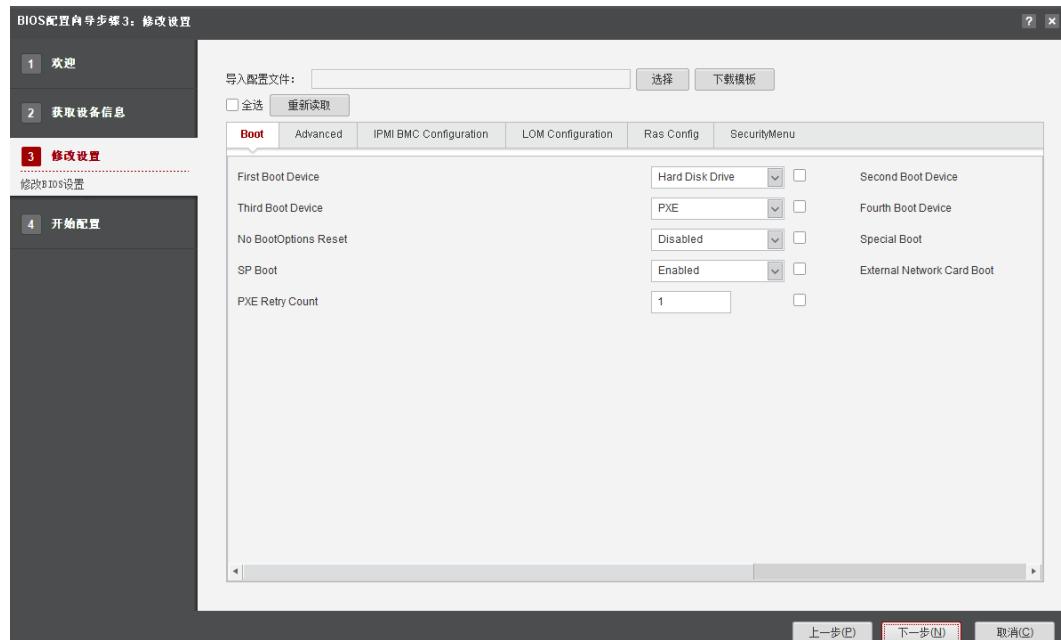
单击“停止”可终止此次任务。

步骤6 可选: 单击“过滤设备”下拉框，可对发现的服务器进行筛选，快速选择需要进行配置的一类服务器。

步骤7 勾选需要进行BIOS配置的服务器，单击“下一步”。

进入“修改设置”界面，如图4-11所示。

图 4-11 修改设置



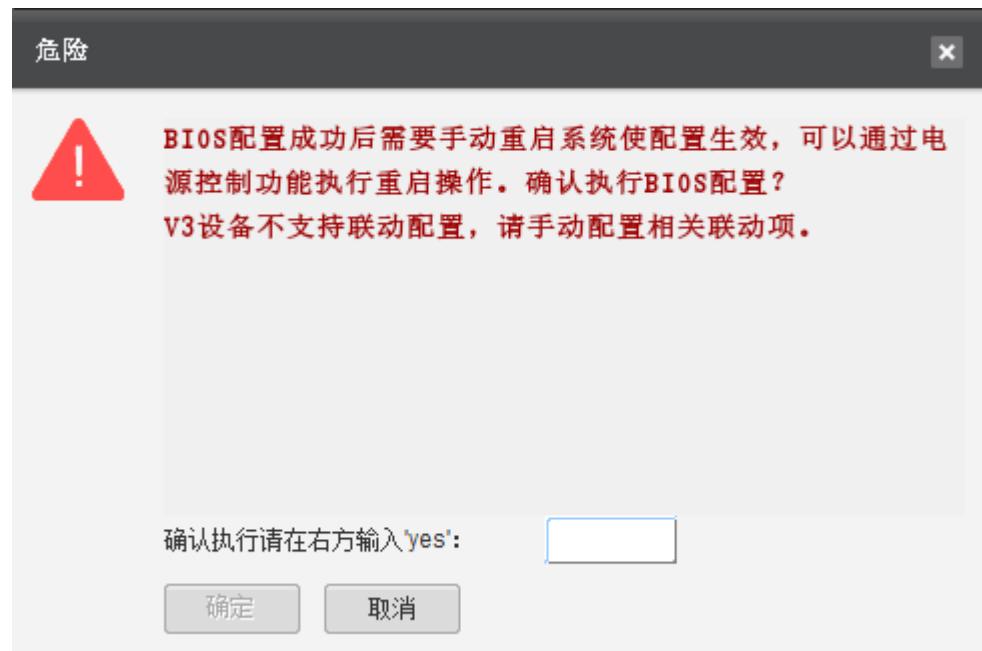
步骤8 根据需要对配置项进行修改，在此界面可进行如下操作：

- 单击界面左上方的“全选”复选框，将会选中或取消选中所有的配置项，单击每个配置项后面的复选框只选中或取消选中这一项，软件只会对选中的配置项进行配置。
- 保存模板。
单击“下载模板”，将当前的配置项保存成模板文件（“.ini”格式），默认保存在“根目录\tools\ServerMain\template\BIOSConfig”目录下。
- 导入模板。
单击“选择”，选择已经保存的模板文件，界面将会根据模板文件来显示配置项。
- 重新读取。
单击“重新读取”，修改过的配置将被恢复为修改前状态。

步骤9 修改配置项并选中配置项后面的复选框，单击“下一步”。

弹出“BIOS配置成功后需要手动重启系统使配置生效，可以通过电源控制功能执行重启操作。确认执行BIOS配置？V3设备不支持联动配置，请手动配置相关联动项”的提示框，如图4-12所示。

图 4-12 提示框



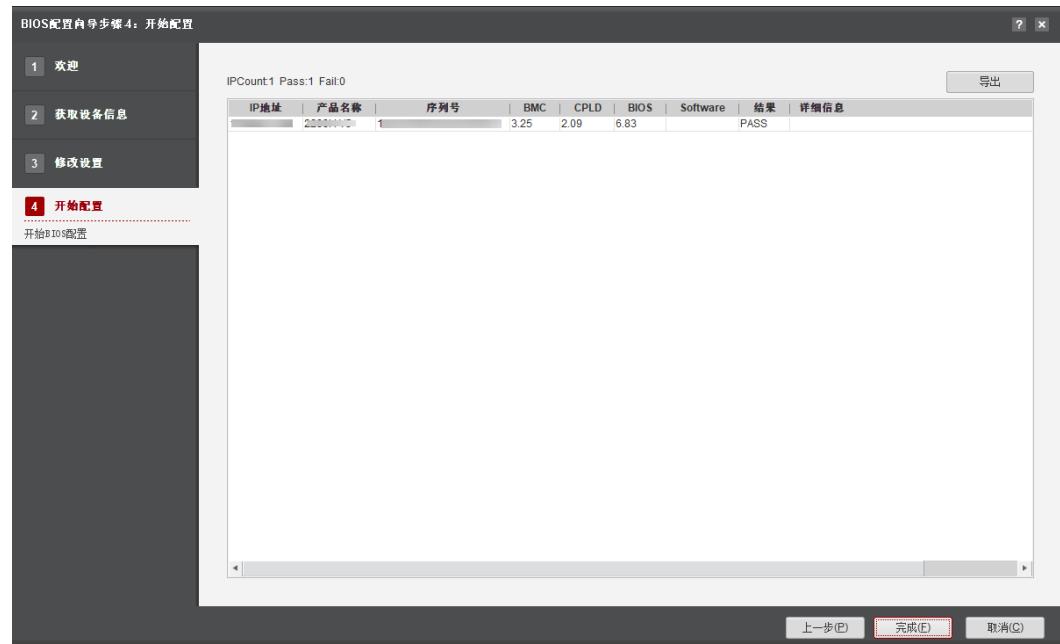
步骤10 如果继续执行BIOS配置, 则在输入框中输入“yes”后单击“确定”。

进入“开始配置”界面。

步骤11 BIOS配置完成后自动进入BIOS配置结果界面。

步骤12 在BIOS配置结果界面, “结果”列表示配置结果, 如图4-13所示。

图 4-13 开始配置



说明书

- 单击“完成”退出，向导界面显示成功和未执行的服务器台数，以及总用时。
- 单击“导出”可将此界面的设备信息保存至本地（默认保存“.xls”格式）。

----结束

4.1.2.5 常见问题处理

表 4-5 常见问题

错误描述	原因	解决建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
Cannot login by SSH or SFTP	无法通过SSH或SFTP方式登录服务器。	<ol style="list-style-type: none">1. 查看SSH端口是否打开，端口号与工具配置的是否一致，详细请参考5.3 查看 BMC端口信息。2. 使用Xshell软件或者其他软件尝试通过SSH及SFTP方式登录服务器，查看是否可正常登录。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none">• SNMP配置错误或服务器不支持SNMP命令。• SNMP未响应。	<ol style="list-style-type: none">1. 查看服务器是否支持运行工具。2. 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。3. 检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看 BMC端口信息、5.4 查看 BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none">1. 确认该操作是否符合规范。2. 重新执行该操作。

错误描述	原因	解决建议
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合SNMP要求。	<ol style="list-style-type: none"> 1. 查看服务器是否支持运行工具。 2. 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 3. 检查密码是否满足SNMP V3的要求，如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3协议不一致或用户名/密码不一致，引起巡检（升级）串行。	<ol style="list-style-type: none"> 1. 检查所有服务器配置的SNMP V3协议是否一致，并将其调整一致。 2. 检查所有服务器的用户名、密码是否一致，并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话，IPMI命令执行失败。	<ol style="list-style-type: none"> 1. 手工执行IPMI命令，检查是否存在问题。 2. 待问题解决后，重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 1. 检查网络是否有异常。 2. 重新执行任务。
User must be an administrator.	使用非管理员账户执行该操作。	<ol style="list-style-type: none"> 1. 检查用户是否为管理员账户。 2. 使用管理员账户重新执行该操作。
Cannot login by SSH or SFTP, please execute with the manual mode.	无法通过SSH及SFTP登录服务器。	通过手工方式完成操作。
Download BIOS file from device failed, please try again later	下载BIOS配置文件失败。	稍后重新执行BIOS配置。
The selected template does not support this device	选择的BIOS配置模板不支持当前服务器。	选择自己作为模板或者同类型的服务器作为模板。
Upload changed file to device failed, please try it again later	上传BIOS配置文件失败。	稍后重新执行BIOS配置。

错误描述	原因	解决建议
Effective BIOS configuration failed, please try again later	使能BIOS配置失败。	
BIOS configuration item values do not match, this device does not support the BIOS configuration	当前服务器不支持BIOS配置。	查看服务器是否支持运行工具。
BIOS config items init failed, please try again later	当前BIOS版本低于1.00。	升级BIOS版本至1.00及以上版本再进行配置。

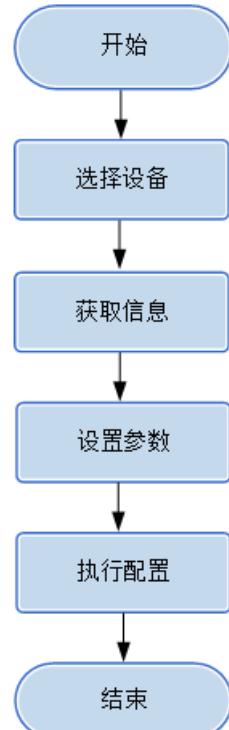
4.1.3 RAID 配置

本节指导用户使用工具进行RAID配置。

4.1.3.1 配置流程

RAID配置流程如图4-14所示。

图 4-14 RAID 配置



4.1.3.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

- PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH、VMM通信端口连通，保证能ping通服务器BMC的IP地址。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

4.1.3.3 选择设备

在硬件配置向导的“选择设备”界面中，可以选择需要进行配置的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“开局交付>硬件配置”。

系统进入“硬件配置”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要RAID配置的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-6](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-6](#)，手工输入参数。

表 4-6 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: fc00::1 结束 IP: fc00::1 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: fc00::1 结束 IP: fc00::6 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	BMC管理员用户名。	-
	密码	BMC管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级设置	SNMP端口	SNMP端口号。	请忽略该参数，或者保持默认值。
	IPMI端口	IPMI端口号。	请忽略该参数，或者保持默认值。
	SSH/SFTP端口	SSH/SFTP端口号。	请忽略该参数，或者保持默认值。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

说明书

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要RAID配置的设备。单击“确定”，返回向导界面。

----结束

4.1.3.4 配置 RAID

在RAID配置界面中，可以对所选择的设备进行RAID配置。

须知

- 建议先配置一台服务器，待没有问题后，再进行批量配置，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具对同一台设备同时进行操作。
- 配置RAID会丢失硬盘原有的数据，请在执行配置前备份硬盘里的数据。
- 批量配置选择的RAID卡型号必须相同。
- 服务器的BMC版本要求在2.32及以上或V3.01.00.00及以上。
- 服务器必须为上电状态才能进行RAID配置。
- 服务器必须支持redfish接口才能进行RAID配置。
- RAID卡必须支持带外管理才能进行RAID配置。
- 请勿对升级过程中的设备进行RAID配置。

操作步骤

步骤1 在硬件配置向导界面单击“硬件配置”。

系统弹出“配置BMC、BIOS、RAID”选择框。

步骤2 单击“RAID配置”。

系统进入RAID配置向导“欢迎”界面，查看支持的RAID卡和注意事项，如图4-15所示。

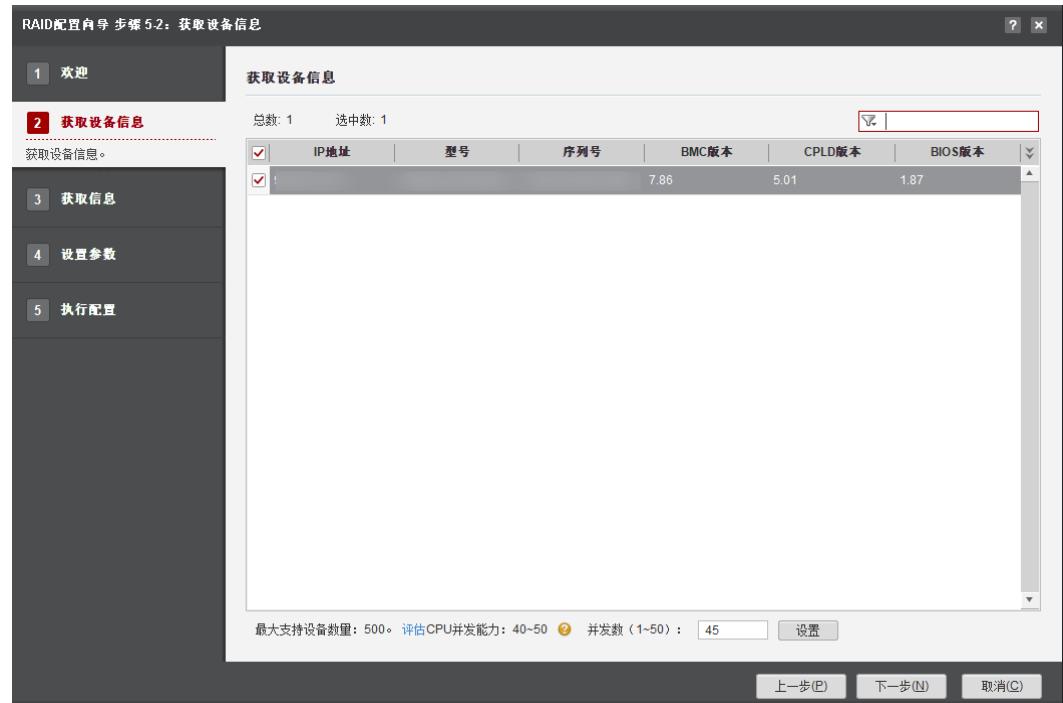
图 4-15 欢迎



步骤3 单击“下一步”。

进入“获取设备信息”界面，如图4-16所示。

图 4-16 获取设备信息



□ 说明

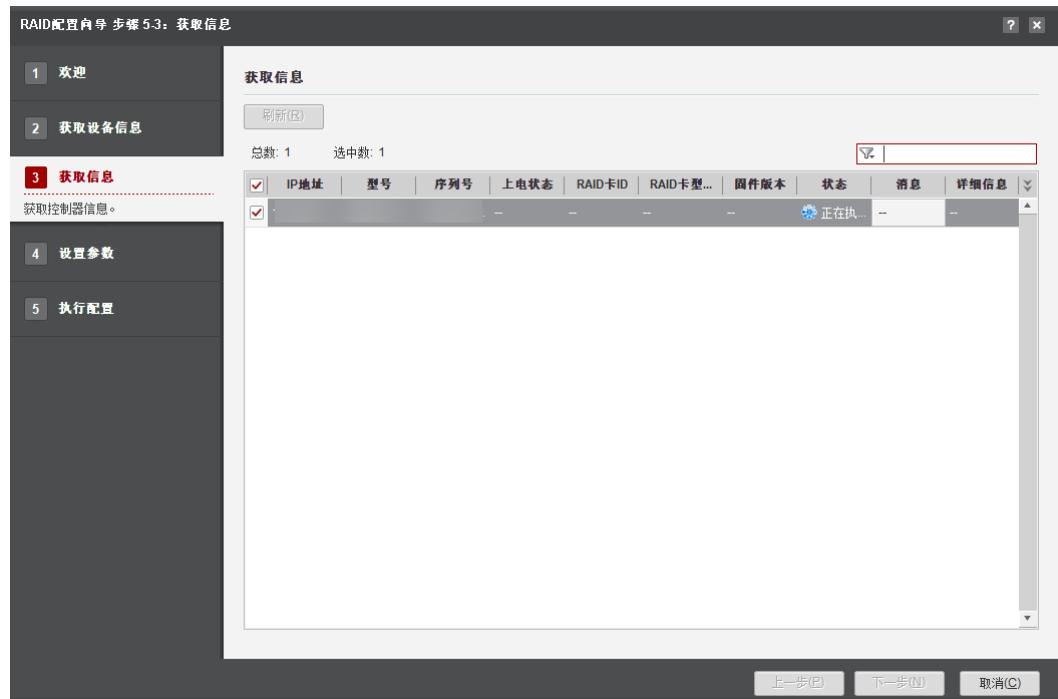
- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤4 在设备列表中勾选需要配置RAID的设备。

步骤5 单击“下一步”。

进入“获取信息”界面，系统自动评估该设备是否支持RAID配置，如图4-17所示。

图 4-17 获取信息



步骤6 在“状态”为“支持”的设备中单击“RAID卡ID”下拉框，选择要配置的RAID卡。

□ 说明

- 单击“刷新”可以刷新当前设备列表显示的信息。
- 单击“控制器信息”，可以显示当前RAID卡的详细硬件信息。
- 服务器BMC版本在2.32及以上或V3.01.00.00及以上，状态为上电，且RAID卡支持带外管理，才能支持RAID配置。

步骤7 单击“下一步”。

进入“设置参数”界面，如图4-18所示。参考表4-7，设置控制器相关参数。

图 4-18 设置参数

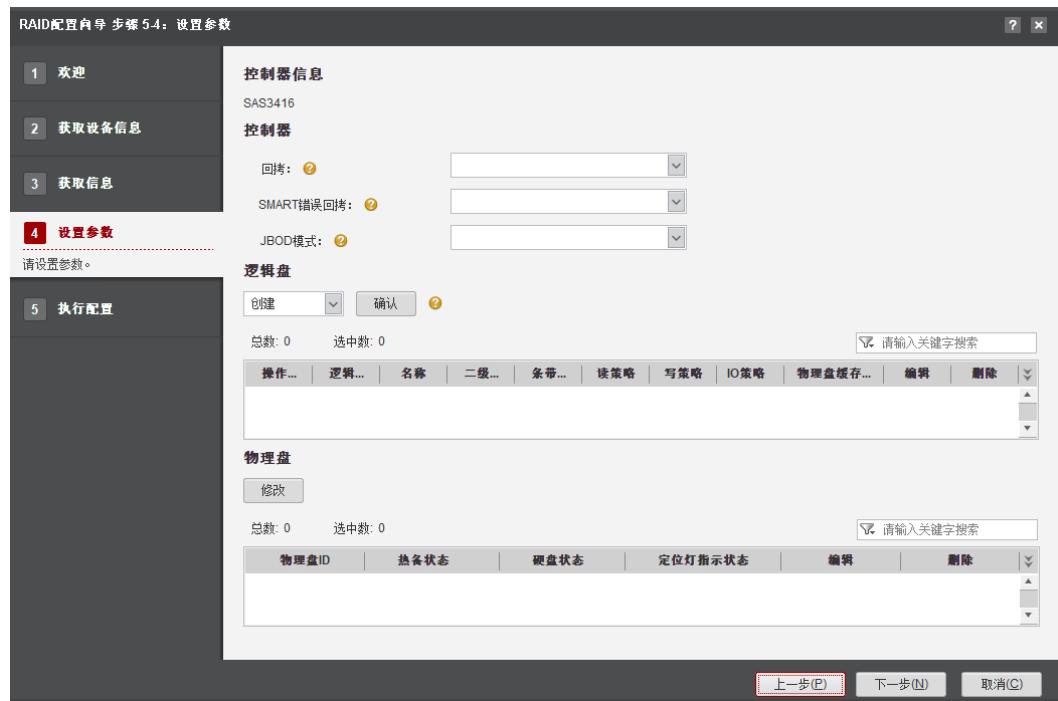


表 4-7 控制器参数说明

参数	说明	取值
回拷	回拷功能使能状态	启用/禁用 (默认为启用)
Smart错误回拷	SMART错误回拷功能的使能状态	启用/禁用 (默认为启用)
JBOD模式	驱动器直通功能的使能状态 说明 启动之后将不能创建逻辑盘，物理盘的固件状态只能选JBOD或Unconfigured Good。	启用/禁用 (默认为禁用)

说明

- 当“JBOD模式”开启时，未进行组RAID操作的物理盘固件状态才可以修改为“JBOD”。
- 当“回拷”设置为“禁用”时，“Smart错误回拷”默认设置为“禁用”。

步骤8 在逻辑盘下拉列表中选择创建、修改或者删除操作配置逻辑盘。

- 如果选择创建逻辑盘
 - 单击“确认”，弹出“创建逻辑盘”界面。参考表4-8设置相关参数。
 - 单击“保存”完成配置。
 - 如果需要创建多个逻辑盘，请重新执行**步骤8.a**和**步骤8.b**。

说明书

- 请确定勾选的物理盘ID在设备上是存在的，设备物理盘ID查询方式请参考[5.1 查看RAID卡信息](#)。
- 在已有的磁盘阵列上添加逻辑盘，RAID级别和成员盘数在下拉列表选“空”。
- 只有选择的物理盘有SSD固态硬盘才可以设置二级缓存。
- 支持RAID组数量和单个RAID组下最多创建的逻辑盘数量请参见[表4-9](#)。如果需要了解更多关于RAID控制卡的信息，请参见对应版本的RAID控制卡 用户指南。

表 4-8 创建逻辑盘

参数	说明	取值
物理盘	成员盘列表，为必选参数。	Disk0-Disk63
名称	逻辑盘名称	由0-9、a-z、A-Z组成，不超过15个字符
二级缓存	是否创建为CacheCade逻辑盘（仅SAS 3108支持）	yes/no
条带大小	逻辑盘条带大小	64/128/256/512/1024
读策略	逻辑盘默认的读策略	ReadAhead/ NoReadAhead
写策略	逻辑盘默认的写策略	WriteThrough/ WriteBackWithBBU/ WriteBack
IO策略	逻辑盘默认的Cache策略	CachedIO/DirectIO
物理盘缓存策略	成员盘的缓存策略	Unchanged/Enabled/ Disabled
访问策略	逻辑盘的访问策略	ReadWrite/ReadOnly/ Blocked
初始化类型	逻辑盘初始化模式	UnInit/QuickInit/FullInit
级别	逻辑盘的RAID级别，为必选参数（在已有的磁盘阵列上添加逻辑盘，该参数选“空”）	RAID0/RAID1/RAID5/ RAID6/RAID10/RAID50/ RAID60/“空”
成员盘数	逻辑盘子组个数（在已有的磁盘阵列上添加逻辑盘，该参数选“空”）	创建RAID0/RAID1/RAID5/ RAID6时，此参数为1 创建RAID10/RAID50/ RAID60时，此参数可设置为2~8 在已有的磁盘阵列上添加逻辑盘，此参数设置为“空”

参数	说明	取值
容量	逻辑盘容量	整数, 单位为MB

表 4-9 RAID 卡的基本参数

RAID卡	支持的RAID组数量	单个RAID组下最多创建的逻辑盘数量
LSI SAS3008IT	NA	NA
LSI SAS3108	64	16
Avago SAS3408iMR	32	16
Avago SAS3508	64	16
Avago SAS3416iMR	32	16
Avago SAS3416IT	NA	NA
Avago SAS3004iMR	32	16
Avago SAS3516	64	16
Avago SAS3408IT	NA	NA
Avago MegaRAID SAS 9460-8i	64	32
Avago MegaRAID SAS 9440-8i	32	32
Avago MegaRAID SAS 9460-16i	64	32

- 如果选择修改逻辑盘
 - 单击“确认”，弹出“如果选择修改，已存在的创建或者删除命令将会被清除，是否确定执行”提示框。
 - 单击“确定”，弹出“修改逻辑盘”界面。参考[表4-10](#)设置相关参数。
 - 单击“保存”完成配置。
 - 如果需要修改多个逻辑盘，请重新执行[9.a-9.c](#)。

说明

- 请确定输入的逻辑盘ID在设备上是存在的，设备逻辑盘ID查询方式请参考[5.1 查看RAID卡信息](#)。
- SSCD缓存功能，需要有设置了二级缓存的逻辑盘。

表 4-10 修改逻辑盘

配置项	说明	取值
逻辑盘ID	要修改的逻辑盘的ID	0-N 只能输入整数
名称	逻辑盘名称	由0-9、a-z、A-Z组成，不超过15个字符
读策略	逻辑盘默认的读策略	ReadAhead/NoReadAhead
写策略	逻辑盘默认的写策略	WriteThrough/WriteBackWithBBU/WriteBack
IO策略	逻辑盘默认的Cache策略	CachedIO/DirectIO
物理盘缓存策略	成员盘的缓存策略	Unchanged/Enabled/Disabled
访问策略	逻辑盘的访问策略	ReadWrite/ReadOnly/Blocked
BGI状态	是否使能后台初始化	yes/no
SSCD缓存功能	是否使用CacheCade逻辑盘做缓存	yes/no
是否为启动盘	是否为启动盘	yes

- 如果选择删除逻辑盘

- 单击“确认”，弹出“如果选择删除，已存在的创建或者删除命令将被清除，是否要执行”提示框。
- 单击“确定”，弹出“删除逻辑盘”界面。输入逻辑盘ID。
- 单击“保存”，弹出“是否确定执行删除逻辑盘操作”提示框，点击“确定”，完成配置。
- 如果需要删除多个逻辑盘，请重新执行9.a-9.c。

 说明

请确定输入的逻辑盘ID在设备上是存在的。

步骤9 单击物理盘配置下的“修改”，弹出“修改物理盘”界面，参考表4-11设置物理盘参数，单击“保存”完成配置。

 说明

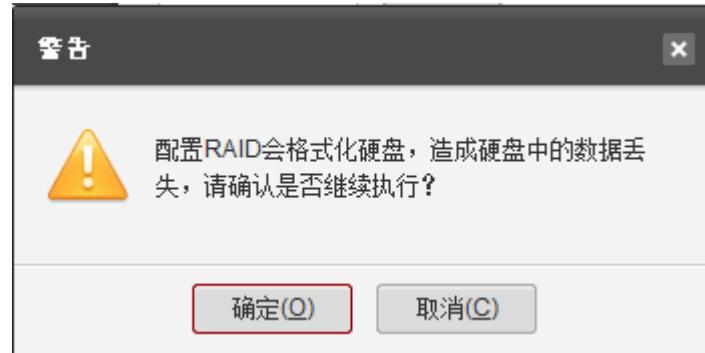
- 请确定输入的物理盘ID在设备上是存在的。
- 物理盘的热备状态设置需要有未进行组RAID操作的闲置物理盘。
- 选择“局部热备”状态时，需要输入一个要配置局部热备的逻辑盘ID（需要查询并确定当前ID是否存在），同时该逻辑盘的RAID级别需要为RAID1及以上。
- “硬盘状态”的选项值为2对互相更改，Online和Offline相互更改，UnconfigGood和JBOD相互更改，请参考5.1 查看RAID卡信息确定当前状态后，进行对应的修改。（创建了逻辑盘的物理盘固件状态为Online和Offline，未创建逻辑盘的物理盘固件状态为UnconfigGood和JBOD）

表 4-11 修改物理盘

配置项	说明	取值
物理盘ID	要修改的物理盘的ID	Disk0-Disk63
定位灯指示状态	定位指示灯状态	Off/Blinking
硬盘状态	驱动器状态	驱动器状态可在如下状态之间切换： <ul style="list-style-type: none">• Online：为某个虚拟磁盘的成员盘，可正常使用，处于在线状态。• Offline：为某个虚拟磁盘的成员盘，不可正常使用，处于离线状态。• Unconfigured Good：磁盘状态正常，但不是虚拟磁盘的成员盘或热备盘。• JBOD：硬盘直通
热备状态	驱动器的热备状态	None/Global/Dedicated
请输入逻辑盘ID	驱动器设置为局部热备盘时，所关联的逻辑盘访问路径（选择局部热备“Dedicated”后显示）	0-N 逻辑盘ID，只能为整数

步骤10 单击“下一步”，弹出“配置RAID会格式化硬盘，造成硬盘中的数据丢失，请确认是否继续执行？”提示框，如图4-19所示。

图 4-19 提示框



步骤11 单击“确定”。

进入“执行配置”界面，如图4-20所示。

图 4-20 执行配置



说明

单击“终止”可终止此次任务。

步骤12 当进度条到100%时表示配置完成。

说明

单击“继续配置”，返回到“获取信息”界面重新进行RAID配置。

----结束

4.2 OS 部署

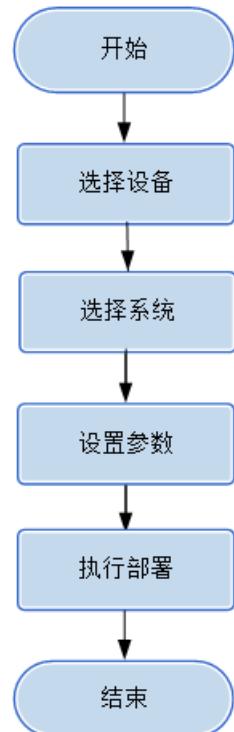
OS部署工具支持BMC服务器进行批量部署操作。

4.2.1 操作流程

介绍OS部署的操作流程。

操作流程如[4.2.1 操作流程](#)所示。

图 4-21 操作流程



4.2.2 使用前准备

必备事项

前提条件

- PC机和待操作的服务器BMC网络相通，保证SNMP和VMM通信端口连通，保证能ping通服务器BMC。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。
- 确保服务器的Smart Provisioning是使用Recover方式升级。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

安装准备

使用OS部署工具安装操作系统前，需做好以下几方面的准备工作：

- 查询服务器的当前配置是否支持待安装的操作系统。
- 待安装操作系统的ISO镜像文件。
- 待安装操作系统的服务器已设置启动盘，对于支持带外管理的RAID卡您可以使用工具的RAID配置功能进行设置。

须知

- 使用OS部署工具安装操作系统时，必须将操作系统安装在启动盘上。
- 使用OS部署工具安装操作系统时，需要格式化待安装操作系统的硬盘，请在安装操作系统前备份硬盘数据。
- 在Legacy模式下安装操作系统时，请使用容量在2TB以下的硬盘。
- 使用OS部署工具安装操作系统时，若当前环境上有多个RAID卡，不支持在不同的RAID卡上安装操作系统。
- Legacy和UEFI模式下工具会将系统安装在设置的启动盘上。

4.2.3 选择设备

在“选择设备”界面中，可以选择需要进行OS部署的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“开局交付>OS部署”。

系统进入“OS部署”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要部署的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-12](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-12](#)，手工输入参数。

表 4-12 参数说明

类型	名称	说明	备注
-	起始 IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束 IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: fc00::1 结束 IP: fc00::1 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: fc00::1 结束 IP: fc00::6 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	BMC的管理员用户名。	-
	密码	BMC的系统管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	请忽略该参数，或者保持默认值。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器。

步骤6 勾选需要部署的设备。单击“确定”，返回向导界面。

----结束

4.2.4 OS 部署

在执行部署前，需选择执行部署的系统类型和版本。

操作步骤

步骤1 在OS部署向导界面单击“OS部署”。

系统进入“OS部署工具”界面，勾选服务器设备，如图4-22所示。

图 4-22 OS 部署工具



□ 说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤2 单击“设置参数”。

选择系统界面，如图4-23所示，界面参数说明请参见表4-13。选择需要部署的系统类型和版本，如表4-14所示。

图 4-23 选择系统

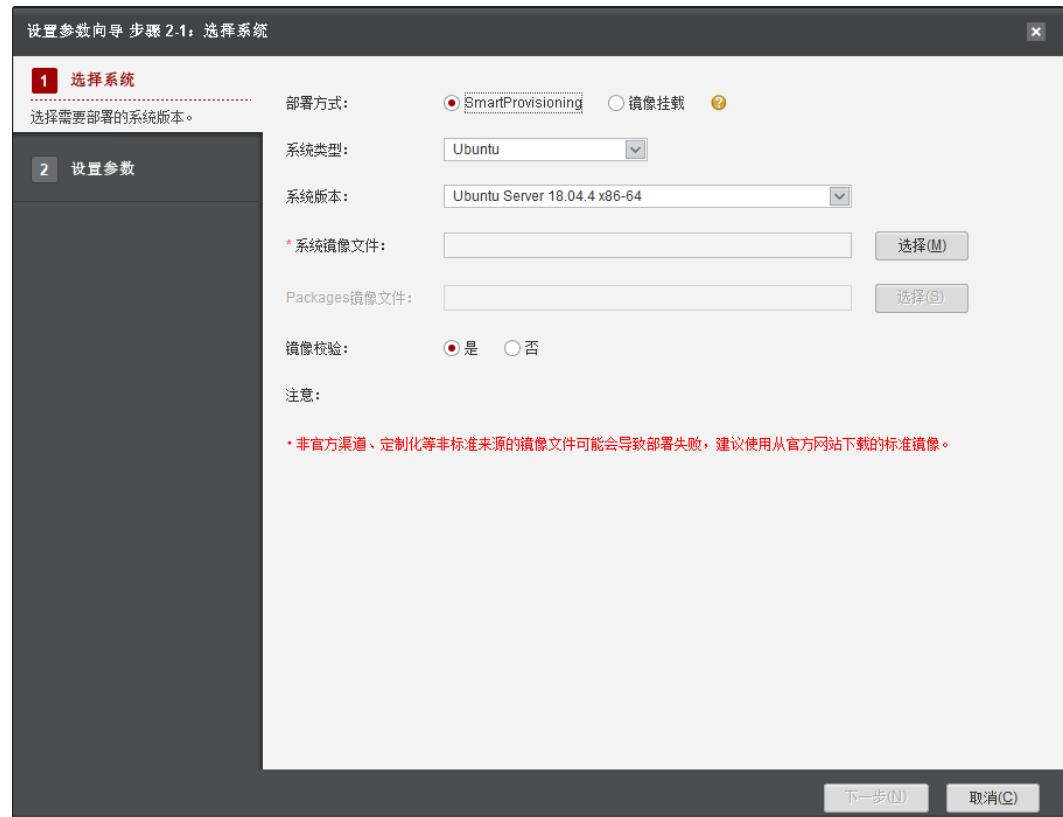


表 4-13 选择系统

参数	说明
部署方式	<ul style="list-style-type: none">SmartProvisioning方式通过服务器板载SmartProvisioning部署操作系统；镜像挂载方式通过挂载操作系统镜像部署系统。
系统类型	选择需要部署的操作系统。 说明 如果选择通过“镜像挂载”方式部署SUSE 12.x和SUSE 15.x，部署前，请登录到BIOS界面，选择“Advanced > MISC Config”，将“Support SPCR”设置为“Disabled”。
系统版本	选择需要部署的操作系统版本。
系统镜像文件	在本地选择需要部署的系统的镜像文件。
Packages镜像文件	仅部署SUSE系统时可选择该参数。 说明 部署SUSE系统时，不选择Packages镜像文件会导致专有参数无法配置。

参数	说明
镜像校验	<p>选择是否镜像校验</p> <ul style="list-style-type: none"> 是：进行镜像校验，如果镜像文件有误或者和所选系统版本不一致，会弹出提示信息。 否：不校验镜像文件的版本和所选择的系统是否一致以及镜像文件是否正确。

表 4-14 支持的系统类型和版本

操作系统	版本	部署方式	是否支持在安全模式下安装
CentOS	CentOS Linux 8 Update 2 Server for ARM	镜像挂载	否
	CentOS Linux 7 Update 8 Server for ARM	镜像挂载	否
	CentOS Linux 8.1 aarch64	SmartProvisioning	否
	CentOS Linux 8 aarch64	SmartProvisioning	否
	CentOS Linux 7.7 aarch64	SmartProvisioning	否
	CentOS Linux 7.6 aarch64	SmartProvisioning	否
EulerOS	EulerOS V2 SP8	SmartProvisioning	否
Ubuntu	Ubuntu 20.04.1 LTS Server Edition for ARM	SmartProvisioning	否
	Ubuntu 18.04.4 LTS Server Edition for ARM	SmartProvisioning	否
	Ubuntu Server 18.04.3 LTS Server Edition aarch64	SmartProvisioning	否
	Ubuntu Server 18.04.1 LTS Server Edition aarch64	SmartProvisioning	否
BCLinux	Big Cloud Linux 7.6 aarch64	SmartProvisioning	否
OpenEulerOS	openEuler 20.03 aarch64	SmartProvisioning	否
SUSE	SUSE Linux Enterprise Server 15 Service Pack 2 for ARM	镜像挂载	否

操作系统	版本	部署方式	是否支持在安全模式下安装
	SUSE Linux Enterprise Server 15 Service Pack 1 for ARM	镜像挂载	否
	SUSE Linux Enterprise Server 12 Service Pack 5 for ARM	镜像挂载	否
Kylin	NeoKylin Server V7.0 U6 for ARM	镜像挂载	否

步骤3 单击“下一步”，进入“设置参数”界面，如图4-24所示。参数填写请参考表4-15。

图 4-24 设置参数

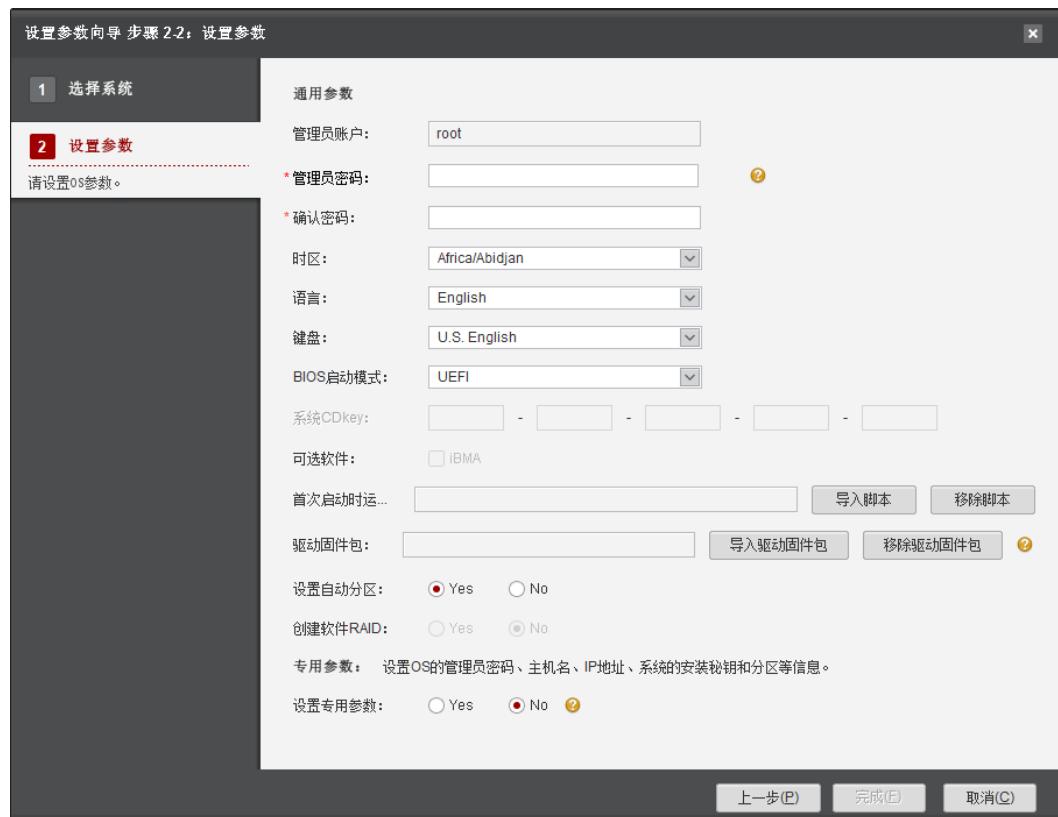


表 4-15 通用参数

参数名称	说明
管理员账户	-
管理员密码	<ul style="list-style-type: none"> SUSE系统密码长度最少为6位。 CentOS、EulerOS、OpenEulerOS、Kylin、BCLinux系统密码长度最少为6位，且不可包含# \$和空格。

参数名称	说明
确认密码	<ul style="list-style-type: none"> SUSE系统密码长度最少为6位。 CentOS、EulerOS、OpenEulerOS、Kylin、BCLinux系统密码长度最少为6位，且不可包含# \$和空格。
时区	-
语言	-
键盘	-
BIOS启动模式	-
系统CDKey	-
可选软件	iBMA可以支持服务器CPU、内存、硬盘、网卡、PCIe卡、RAID卡等各个组件的状态监控、性能监控、事件监控。
首次启动时运行脚本	<p>以下情况不支持启动脚本：</p> <ul style="list-style-type: none"> Smart Provisioning版本小于V123。 SUSE: 11.4 x86操作系统。 <p>说明 仅部署方式选择“Smart Provisioning”时，支持此功能。</p>
驱动固件包	<p>此功能将在部署OS前，升级固件包。部署成功后，安装驱动。</p> <ul style="list-style-type: none"> 仅支持ARM架构。 要求Smart Provisioning版本为1.2.1及以上。 驱动固件包文件夹存放的路径只能包含数字，字母，中划线，下划线和点号。 驱动固件包文件夹仅由driver和firmware两个文件夹组成。 <ul style="list-style-type: none"> driver文件夹用于存放驱动包（格式为.zip）和对应的签名文件，此文件夹可为空或存放一个驱动包和对应的签名文件。 firmware文件夹用于存放固件包（格式为.zip）和对应的签名文件，此文件夹可为空，也可存放一个或多个固件包和对应的签名文件。 请确保driver和firmware文件夹，至少一个不为空。 Smart Provisioning 1.6.0以下版本签名文件仅支持.asc格式，Smart Provisioning 1.6.0及以上版本支持.asc和.p7s两种格式的签名文件。 <p>说明</p> <ul style="list-style-type: none"> 仅部署方式选择“Smart Provisioning”时，支持此功能。 若导入驱动固件包文件夹中，driver和firmware文件夹均有升级包，请确保driver文件中的驱动包和firmware文件夹中的固件包兼容，否则执行部署过程中，上传驱动固件文件时会提示“存在不兼容的驱动或固件”。查看驱动包和固件包是否兼容，请参考驱动配套表。
设置自动分区	部署OS时，设置了专有参数则不是自动分区，否则是自动分区。
创建软件RAID	-

参数名称	说明
设置专有参数	<p>设置OS的管理员密码、主机名、IP地址、系统的安装密钥和分区等信息。</p> <ul style="list-style-type: none"> 设置参数界面，选择设置专有参数为yes，在下方配置文件项一栏，点击下载模板，模板为.xls文件。根据模板要求填写参数，再点击导入参数将填写好的参数文件导入工具，即可进行专有参数配置。 专有参数设置支持Linux系统。 通过SP方式部署OS时，若要配置网络信息，相应网口必须连通网络。

步骤4 单击“完成”，待部署设备的状态栏由“未设置参数”成为“已设置参数”，单击“参数详情”按钮，可查看参数详情。

步骤5 返回“OS部署工具”界面，单击“执行部署”，弹出“警告”提示框。

步骤6 勾选提示框中的注意事项和确认已识别以上风险，单击“确定”，开始执行部署。

步骤7 在下方列表中查看部署详情，如表4-16所示。

表 4-16 详情列表

列名	说明
IP	服务器的IP。
型号	服务器的型号。
BMC版本	服务器的BMC版本。
SP版本 (APP/OS/ Data)	服务器的Smart Provisioning版本。
OS版本	待安装操作系统的版本。
架构	ARM服务器。
进度	部署过程进度实时刷新，部署完成显示100%。
状态	部署状态分为“运行中”和“待运行”。
参数详情	显示参数详情。

部署完成后，选择设备列表中已经完成部署的设备，单击列表下方的任意部署项，在弹出的“详细信息”窗口中，可查看该部署项的详细信息。

----结束

4.2.5 设置参数

4.2.6 执行部署

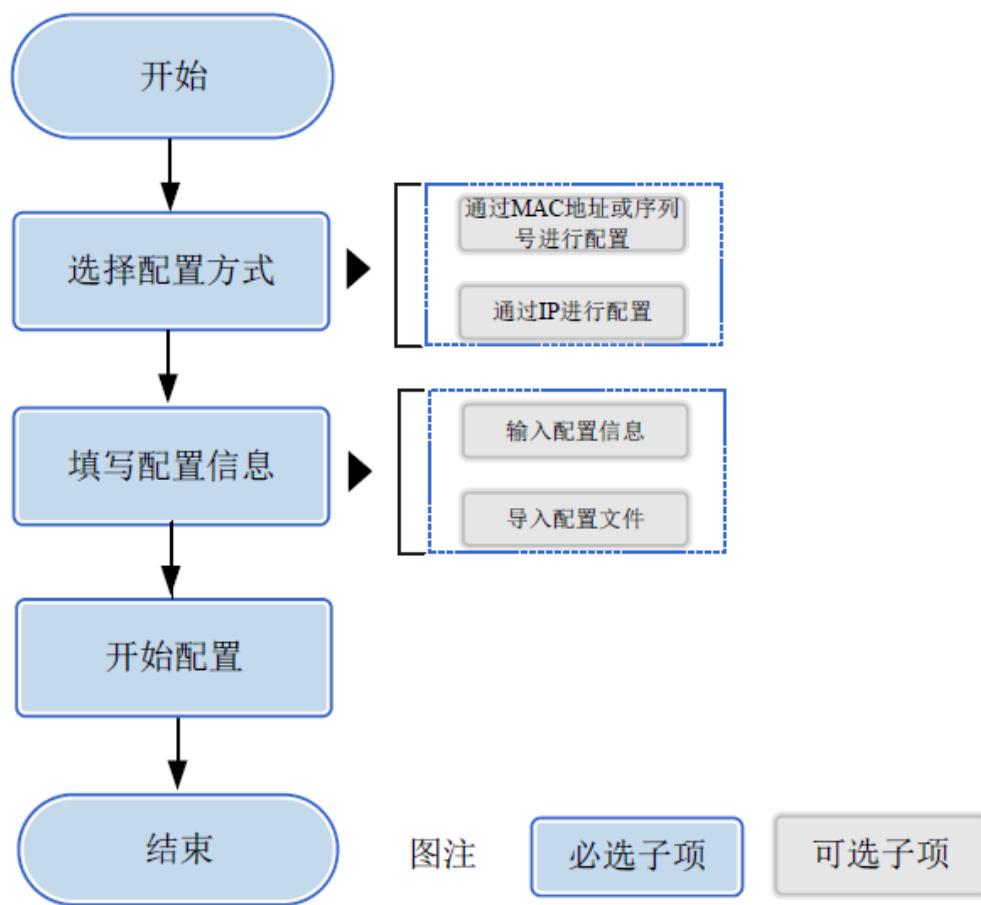
4.3 IP 配置

本节主要指导用户使用IP配置功能对服务器的IP地址信息进行修改。

4.3.1 配置流程

IP配置流程如图4-25所示。

图 4-25 流程图



4.3.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

- 通过MAC地址、序列号或者当前IPv6地址进行配置时，PC机需开启IPv6功能，以下场景要求PC机在开启IPv6功能的同时还要配置IPv6地址。开启和配置方法参见[5.5 开启和配置IPv6功能](#)。
 - 服务器已经配置了IPv6地址且使用序列号查找设备。

- 用户通过填写服务器IPv6地址查找设备。

□ 说明

- IP配置功能有三种查找设备方式：
 - 通过BMC的MAC地址查找：首先通过BMC的MAC地址计算出IPv6链路本地地址，再通过IPv6链路本地地址进行IP配置。
 - 通过服务器的序列号查找：发送IPv6的SSDP组播报文，该报文中包含序列号和IPv6地址。当前网段内的所有BMC版本大于2.90的服务器都会回复报文，通过序列号和IPv6地址进行匹配，匹配成功则进行IP配置。
 - 通过IP地址查找：直接通过用户填写的IPv4或者IPv6地址进行IP配置。
- PC机配置的IPv6地址需和待配置IP地址信息的BMC网络相通，保证IPMI通信端口连通，并且能ping通服务器BMC的IP地址。请确保BMC已开启SNMP、HTTPS、IPMI协议，查看和开启协议的方式请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址或MAC地址或者SN号。
- 服务器BMC用户名和密码。

4.3.3 IP 配置

□ 说明

BMC的版本需大于2.90。

操作步骤

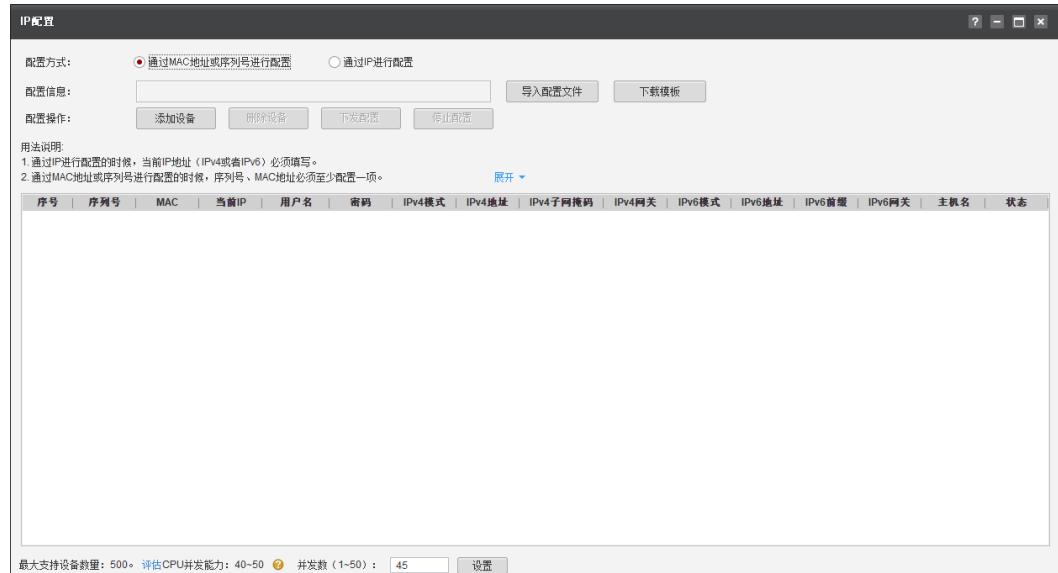
步骤1 在工具首页选择“开局交付>IP配置”。

系统进入“IP配置”向导界面。

步骤2 单击“IP配置”。

进入配置主界面，如[图4-26](#)所示。

图 4-26 IP 配置



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤3 参数说明和配置参数取值说明，如表4-17和表4-18所示。

说明

- IPv4（包含IPv4模式、IPv4地址、IPv4网关、IPv4子网掩码）、IPv6（包含IPv6模式、Pv6地址、IPv6前缀、IPv6网关）或主机名三者必须选择填写一个。
- 如果选择填写IPv4或IPv6，则IP模式必须是“Static”或“DHCP”。如果填写为“Static”，则必须输入IP地址、掩码、前缀和网关。

表 4-17 参数说明

名称	说明	取值	备注
配置方式	支持两种配置方式	通过MAC地址或序列号进行配置。	<ul style="list-style-type: none">通过MAC地址或序列号进行配置适用于初始配置。运行工具的主机必须配置本地IPv6，且和设备处于同一局域网。当通过MAC地址或序列号进行配置时，必须填写MAC或序列号，如果都填写，则优先通过MAC地址进行配置。

名称	说明	取值	备注
		通过IP进行配置。	<ul style="list-style-type: none"> 通过IP进行配置适用于一般配置。只要填写的IP可以连接就能进行配置。 “当前IP地址”（IPv4或IPv6）必须填写。 如果存在IP冲突，有如下要求： <ul style="list-style-type: none"> 必须填写待配置服务器的序列号或MAC地址（序列号/MAC地址输入其中一个即可）。 IP冲突的服务器用户名和密码必须相同。 对相同IP的配置，工具只能串行执行。
配置信息	配置信息可直接输入也可手动导入。	<ul style="list-style-type: none"> 直接输入：单击“添加”，在下方列表中输入配置信息。 手动导入：如果没有可用的模板文件，可单击“下载模板”，保存至本地，编辑完成后，单击“导入配置文件”。 	<ul style="list-style-type: none"> 配置文件支持格式为.xls。 导入配置文件会覆盖下方表格中已有的配置信息。
配置操作	可对配置内容进行相关操作。	<ul style="list-style-type: none"> 添加设备：增加一条配置记录。 删除设备：删除一条或多条配置记录。 下发配置：启动配置。 停止配置：停止或中断配置。 	增加或删除后可在下方列表中查看结果。

表 4-18 配置项取值说明

配置项	取值说明
序列号	由数字与字母组成。

配置项	取值说明
MAC	此处的MAC地址是指唯一网卡的地址， 6个字节48位，十六进制组成。
当前IP	IPv6或者IPv4： <ul style="list-style-type: none"> IPv4：长度为32位，采用十进制格式表示。 IPv6：长度为128位，由八个16位字段组成，相邻字段用冒号分隔， IPv6地址中的每个字段都必须包含一个十六进制数字。为了简化其表示法，每段中前面的0可以省略，连续的0可省略为“::”，但只能出现一次。
用户名	必填项。
密码	必填项。
IPv4模式	下拉框选择： 静态 (Static)：手动配置一个固定的IP，长期不变。 动态 (DHCP)：自动获取IP。
IPv4地址	长度为32位，采用十进制格式表示。
IPv4子网掩码	用来给IP地址划分子网，长度32位。
IPv4网关	和IPv4地址规则一致。
IPv6模式	下拉框选择： 静态 (Static)：手动配置一个固定的IP，长期不变。 动态 (DHCP)：自动获取IP。
IPv6地址	IPv6 地址的长度为128位，由八个16位字段组成，相邻字段用冒号分隔， IPv6地址中的每个字段都必须包含一个十六进制数字。为了简化其表示法，每段中前面的0可以省略，连续的0可省略为“::”，但只能出现一次。
IPv6前缀	1-124数字组成。
IPv6网关	和IPv6地址规则一致。
主机名	由数字和字母，“-”组成。
状态	-

步骤4 单击“下发配置”，执行配置。

步骤5 系统弹出“配置结果”信息框，显示成功、失败、总共执行的服务器台数。

说明

IP配置失败的原因详情可在配置项最后一栏“状态”里面查看。

步骤6 单击“确定”，配置完成。

----结束

4.4 健康检查

健康检查工具是可定制策略的工具，对设备进行检查，并导出设备运行详细信息。整个工具按照向导式的操作流程设计，导出的巡检报告以图表的形式展现，具有较强的可读性。

4.4.1 兼容性列表

健康检查支持的操作系统列表如[表4-19](#)所示。

表 4-19 健康检查支持的操作系统

操作系统	版本
SLES	SLES 11.1
	SLES 11.2
	SLES 11.3
	SLES 11.4
	SLES 12.0
	SLES 12.2
	SLES 12.3
	SLES 15
	SLES 15.1
	SLES 12 SP3 ARM
	SLES 12 SP4 ARM
RHEL	SLES 15 ARM
	SLES 15 SP1 ARM
	RHEL 5.8
	RHEL 5.9
	RHEL 5.10
	RHEL 6.1
	RHEL 6.2
	RHEL 6.3
	RHEL 6.4
	RHEL 6.5
	RHEL 6.6

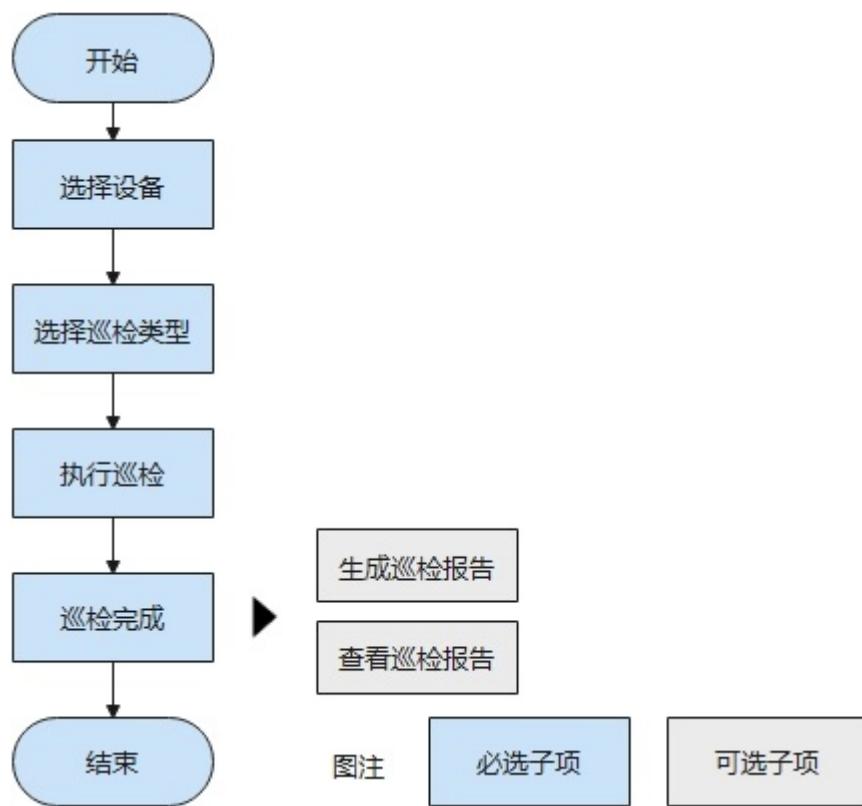
操作系统	版本
RHEL	RHEL 6.7
	RHEL 7.0
	RHEL 7.1
	RHEL 7.2
	RHEL 7.3
	RHEL 7.4
	RHEL 7.5
	RHEL 7.6
CentOS	CentOS 5.8
	CentOS 5.9
	CentOS 5.10
	CentOS 6.1
	CentOS 6.2
	CentOS 6.3
	CentOS 6.4
	CentOS 6.5
	CentOS 6.6
	CentOS 6.7
	CentOS 7.0
	CentOS 7.1
	CentOS 7.2
	CentOS 7.3
	CentOS 7.4
	CentOS 7.5
Ubuntu	CentOS 7.6
	CentOS 7.4 ARM
	CentOS 7.5 ARM
	CentOS 7.6 ARM
	Ubuntu 16.04.3 LTS ARM
	Ubuntu 16.04.4 LTS ARM

操作系统	版本
	Ubuntu 16.04.5 LTS ARM
	Ubuntu 18.04 LTS ARM
	Ubuntu 18.04.1 LTS ARM

4.4.2 流程图

健康检查流程如图4-27所示。

图 4-27 流程图



4.4.3 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

必备事项

前提条件

- PC机和待操作的服务器BMC网络相通，SNMP、IPMI、SSH/SFTP、HTTPS通信端口连通，保证能ping通服务器BMC的IP地址。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)、[5.4 查看BMC的SNMP协议](#)。

- PC机和待巡检操作系统网络相通，保证能ping通操作系统的IP地址，保证SSH、SFTP通讯端口连通。

数据

巡检服务器时需要准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

巡检操作系统时需要准备以下数据：

- 操作系统IP地址。
- 操作系统用户名和密码。

4.4.4 选择设备

在健康检查功能向导的“选择设备”界面中，可以选择需要进行健康检查的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“例行维护>健康检查”。

系统进入“健康检查”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要健康检查的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明

批量导入设备方法：

1. 工具界面上单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如表4-20所示。
3. 工具界面上单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考表4-20，手工输入参数。

表 4-20 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.2.2 IPv6： 起始IP：fc00::1 结束IP：fc00::1 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.5.254 IPv6： 起始IP：fc00::1 结束IP：fc00::6 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	请忽略该参数，或者保持默认值。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 (可选) 单击“浏览”，选择任务结果保存路径，单击“保存”。

步骤7 勾选需要健康检查的设备。单击“确定”，返回向导界面。

----结束

4.4.5 健康检查

在健康检查功能向导的“健康检查”界面中，可以对已选择的设备进行健康检查。

须知

健康检查过程中，会通过工具纳管的账户上传业务脚本到服务器，并在服务器上执行。

操作步骤

步骤1 在健康检查向导界面单击“健康检查”。

系统进入健康检查向导“欢迎”界面，查看注意事项和健康检查项，如图4-28所示。

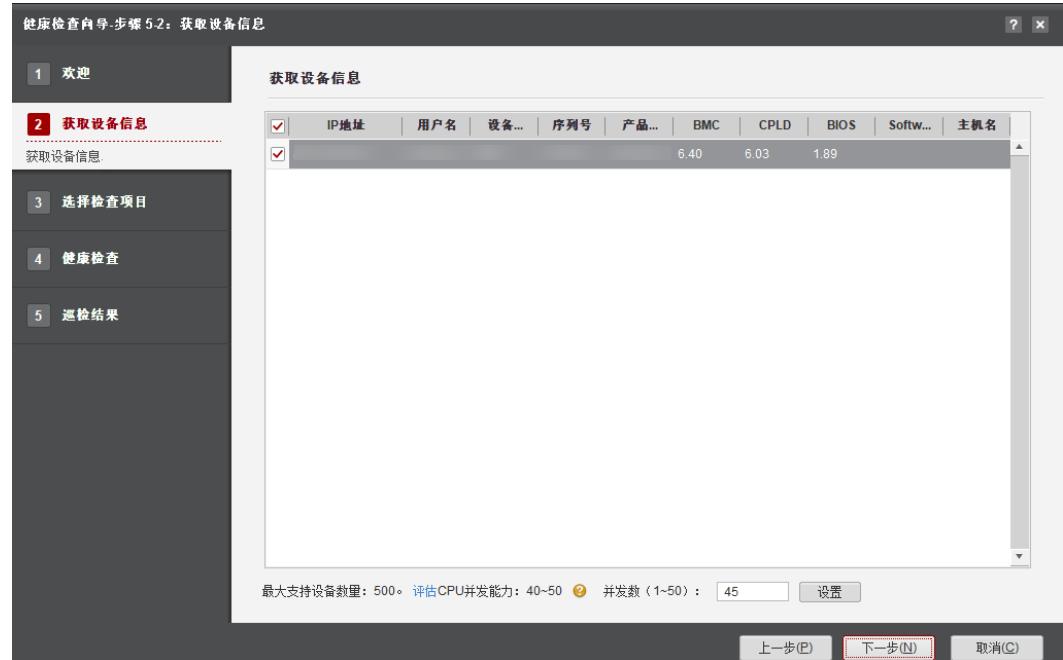
图 4-28 欢迎



步骤2 单击“下一步”。

进入“获取设备信息”界面，如图4-29所示。

图 4-29 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤3 勾选需要健康检查的设备，单击“下一步”，进入“选择检查项目”界面。

步骤4 点击“场景选择”的下拉框，选择健康检查类型，如图4-30所示。

图 4-30 选择检查项目



表 4-21 参数说明

参数	参数及说明
场景选择	<ul style="list-style-type: none">自定义：不选中任何健康检查项，由用户自己选择，建议选择“健康检查”、“配置检查”、“版本兼容性检查”、“版本风险检查”、“资产信息收集”和“安全配置检查”。常规检查：选中“健康检查”、“配置检查”、“版本兼容性检查”、“版本风险检查”和“资产信息收集”。日志收集：只选中“日志收集”。资产收集：只选中“资产信息收集”。安全配置：只选中“安全配置检查”。硬件信息收集：选中“健康检查”和“资产信息收集”。
健康检查	详细，请参考巡检项统计表。
配置检查	详细，请参考巡检项统计表。
版本兼容性检查	详细，请参考巡检项统计表。
版本风险检查	详细，请参考巡检项统计表。
资产信息收集	详细，请参考巡检项统计表。

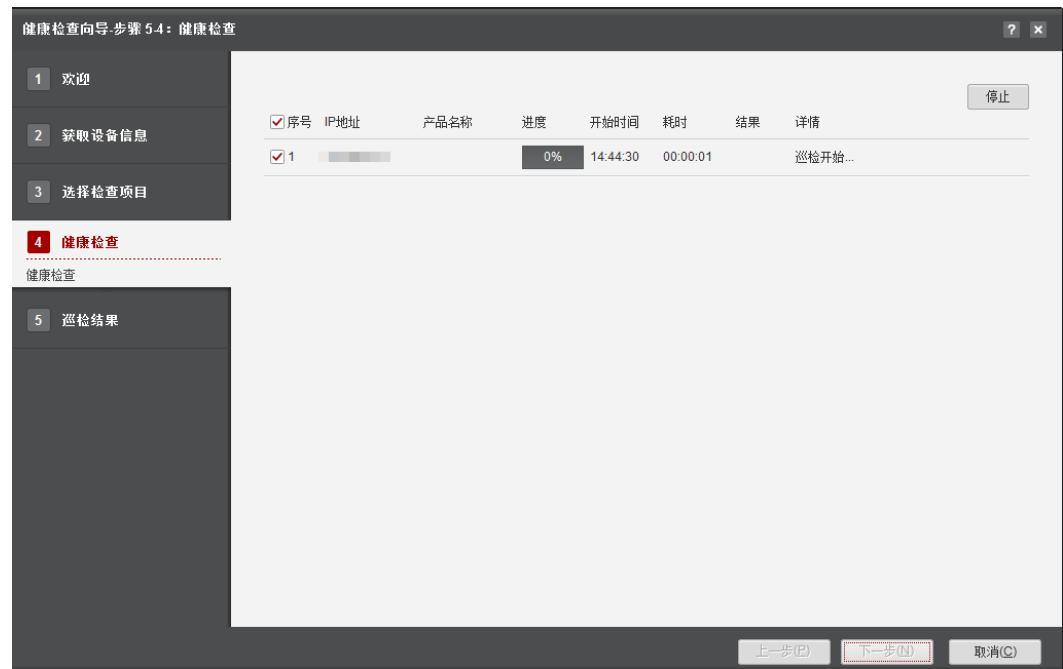
参数	参数及说明
安全配置检查	<p>详细, 请参考《SmartKit Computing 服务器巡检项》。</p> <p>说明</p> <ul style="list-style-type: none"> 此功能仅适用于Hi1711芯片设备。 查询服务器BMC中是否包含Hi1711的命令为“ipmcget -d v”。 如果不勾选或服务器类型不支持此检测项, 巡检结果不显示关于安全配置检查内容。 如果已勾选且服务器类型支持此检查项, 但服务器未包含Hi1711芯片, 巡检结果显示为不涉及。
日志收集	收集硬件BMC和操作系统日志。
基线版本检查	<ul style="list-style-type: none"> 可检查服务器或操作系统组件的版本与基线版本间的版本高低差异, 用于批量排查哪些组件需要升级至基线版本。 仅在选择“资产信息收集”后才可选择“基线版本检查”。
预警整改检查规则	健康检查工具支持载入和还原多个预警整改检查规则配置文件, 并展示载入的多个配置文件的文件名、各个文件对应的更新时间、预警整改规则的统计信息。
从本地导入配置文件	勾选后可从本地导入配置文件, 导入的检查规则配置文件将在巡检工具本地路径持久化保存。
请选择配置文件	选择导入健康检查工具的本地配置文件。
统计信息	展示预警整改规则的统计信息。包括预警整改规则库中已载入的可检查的问题风险数量, 按检查规则格式的版本统计各个版本的问题风险检查规则的数量。
还原	执行还原操作将清除现有已载入的预警整改规则, 还原后将无法恢复。
当前预警整改规则版本	健康检查工具当前支持的最高预警整改规则版本。载入的预警整改检查规则版本高于工具所支持的版本时, 部分预警整改将无法检查。
可预警风险问题数量	按检查规则可支持检查的风险数量。
文件名	<p>预警整改规则配置文件的文件名。</p> <p>说明</p> <p>工具本地路径下没有配置文件时, 无此参数。</p>
更新时间	<p>预警整改规则配置文件的更新时间。</p> <p>说明</p> <p>工具本地路径下没有配置文件时, 无此参数。</p>

步骤5 选择巡检项目。

步骤6 (可选) 勾选“从本地导入配置文件”, 单击“导入”选择本地配置文件。

步骤7 单击“下一步”，进入“健康检查”界面，开始执行健康检查，如图4-31所示。

图 4-31 健康检查



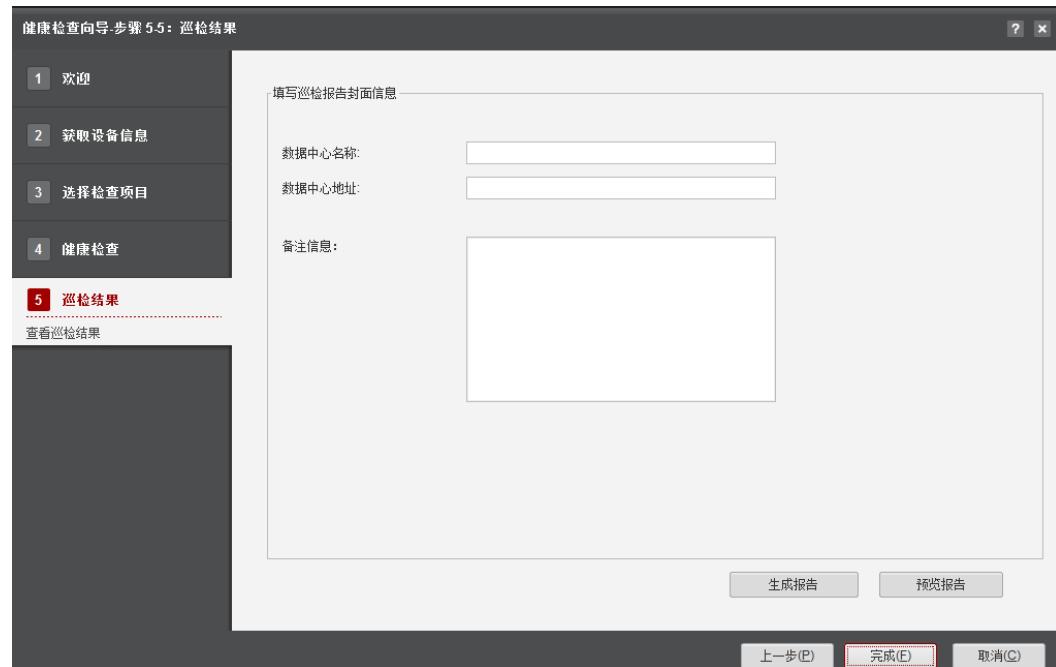
说明书

- 单击“停止”可终止此次任务。
- 单击服务器后的“详情”，可查看该服务器的健康检查结果。

步骤8 勾选需要导出健康检查报告的服务器，单击“下一步”。

进入“巡检结果”界面，填写巡检报告封面信息：数据中心名称、数据中心地址、备注信息，如图4-32所示。

图 4-32 巡检结果



步骤9 单击“预览报告”可查看批量健康检查报告。

说明书

建议使用Chrome浏览器或者IE9及以上版本的浏览器查看健康检查报告。

在批量健康检查报告中：

- 单击“统计总览”可查看服务器的检查总结。
- 单击“资产巡检信息”可查看所有服务器的资产信息。
- 单击“版本检查信息”可查看所有服务器的版本信息。
- 单击“基线版本检查”可查看基线版本检查报告。
- 单击“巡检详情”可查看各个服务器的详细健康检查报告。
- 单击“附录”可查看其他信息。

步骤10 单击“生成报告”，将巡检报告导出至本地。

单击“报告目录”可定位到巡检报告导出的具体的地址。

步骤11 完成后单击“完成”退出。向导界面显示设备执行结果，成功/失败/未执行的台数、以及总用时。

----结束

4.4.6 巡检项统计表

巡检项统计表在下载文档得到的压缩包中的resource文件夹查看。

4.5 电源控制

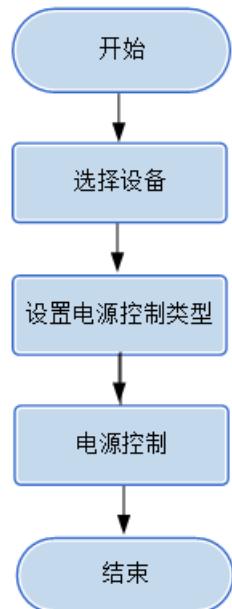
本节指导用户使用工具箱控制服务器电源，如复位BMC，系统下电、上电、复位、先下电再上电。

4.5.1 配置流程

介绍电源控制的配置流程。

电源控制流程如图4-33所示。

图 4-33 电源控制流程



4.5.2 使用前准备

前提条件

PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH通信端口连通，保证能ping通服务器BMC的IP地址。确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

4.5.3 选择设备

在电源控制向导的“选择设备”界面中，可以选择需要进行配置的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“例行维护>电源控制”。

系统进入“电源控制”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要电源控制的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-22](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-22](#)，手工输入参数。

表 4-22 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f434 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f439 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	默认值是8208，以设备实际启用的端口号为准。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

 **说明**

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要电源控制的设备。单击“确定”，返回向导界面。

----结束

4.5.4 电源控制

在电源控制界面中，可以对所选择的设备进行电源控制。

 **说明**

- 操作过程中遇到的问题请参考[4.5.5 常见问题处理](#)解决。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。

须知

- 控制服务器电源可能会影响业务，请先关闭业务后再执行操作。
- 系统下电、复位可能会损坏操作系统文件，请谨慎操作。

操作步骤

步骤1 在电源控制向导界面单击“电源控制”。

系统进入电源控制向导“欢迎”界面，查看可以执行的电源控制类型，如[图4-34](#)所示。

图 4-34 欢迎



步骤2 单击“下一步”。

进入“获取设备信息”界面，如图4-35所示。

图 4-35 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤3 在设备列表中勾选勾选一台或者多台设备需要电源控制的设备。

步骤4 单击“下一步”。

进入发现服务器界面。

□ 说明

单击“停止”可终止此次任务。

步骤5 发现服务器后系统自动进入选择服务器界面。

□ 说明

- 单击“日志目录”可进入服务器发现结果文件“output.xml”的保存目录。
- 单击“导出”可将此界面的设备信息保存至本地（默认保存“.xls”格式）。

步骤6 勾选需要进行电源设置的服务器，单击“下一步”。

进入“设置类型”界面，如图4-36所示。

图 4-36 设置类型



步骤7 选择电源控制类型，单击“下一步”。

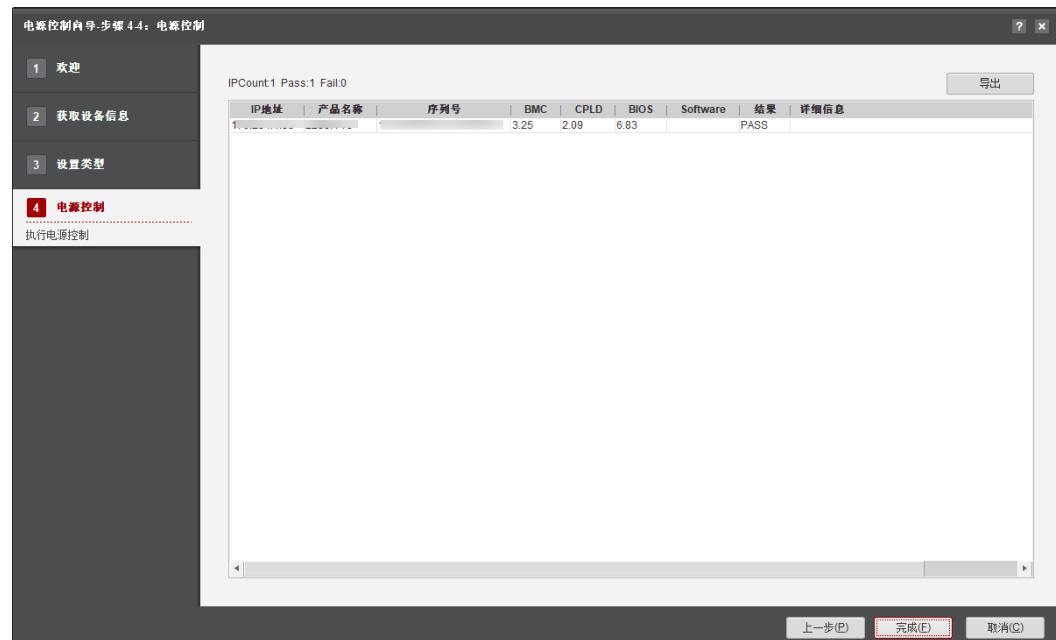
弹出“确认是否执行电源控制操作”的提示框。

步骤8 若确认要执行电源控制，则在输入框中输入“yes”后单击“确定”。

进入“电源控制”界面。

步骤9 电源控制完成后系统会自动进入电源控制完成界面，如图4-37所示。

图 4-37 电源控制



步骤10 在电源控制结果界面，“结果”列表示配置结果。

单击“完成”退出，向导界面显示设备执行结果，成功/失败/未执行的台数、以及总用时。

----结束

4.5.5 常见问题处理

表 4-23 常见问题

错误描述	原因	解决建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
Cannot login by SSH or SFTP	无法通过SSH或SFTP方式登录服务器。	1. 查看SSH端口是否打开，端口号与工具配置的是否一致，详细请参考 5.3 查看 BMC端口信息 。 2. 使用Xshell软件或者其他软件尝试通过SSH及SFTP方式登录服务器，查看是否可正常登录。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。

错误描述	原因	解决建议
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none"> SNMP配置错误或服务器不支持SNMP命令。 SNMP未响应。 	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看BMC端口信息、5.4 查看BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none"> 确认该操作是否符合规范。 重新执行该操作。
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合SNMP要求。	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查密码是否满足SNMP V3的要求，如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3协议不一致或用户名/密码不一致，引起巡检（升级）串行。	<ol style="list-style-type: none"> 检查所有服务器配置的SNMP V3协议是否一致，并将其调整一致。 检查所有服务器的用户名、密码是否一致，并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话，IPMI命令执行失败。	<ol style="list-style-type: none"> 手工执行IPMI命令，检查是否存在问题。 待问题解决后，重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 检查网络是否有异常。 重新执行任务。

错误描述	原因	解决建议
User must be an administrator.	使用非管理员账户执行该操作。	1. 检查用户是否为管理员账户。 2. 使用管理员账户重新执行该操作。

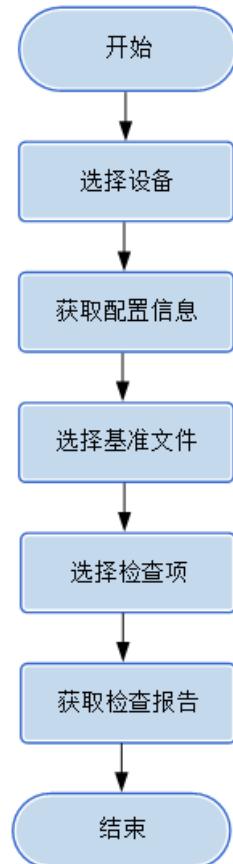
4.6 配置检查

本节指导用户使用工具箱检查服务器的BMC、BIOS、RAID配置。

4.6.1 配置流程

检查服务器配置流程如图4-38所示。

图 4-38 检查服务器配置流程



4.6.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH通信端口连通，保证能ping通服务器BMC的IP地址。

确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC的IP地址。
- 服务器BMC用户名和密码。

4.6.3 选择设备

在配置检查的“选择设备”界面中，可以选择需要进行配置的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“例行维护>配置检查”。

系统进入“配置检查”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要检查配置的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-24](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-24](#)，手工输入参数。

表 4-24 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4: 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6: 起始 IP: 2017::f434 结束 IP: 2017::f434 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4: 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6: 起始 IP: 2017::f434 结束 IP: 2017::f439 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要检查配置的设备。单击“确定”，返回向导界面。

----结束

4.6.4 检查配置

在配置检查界面中，可以对所选择的设备进行BMC、BIOS、RAID配置检查。

□ 说明

- 建议先检查一台服务器的配置，待没有问题后，再进行批量配置检查，批量操作的服务器数量建议不超过200台。
- 操作过程中遇到的问题请参考[4.6.5 常见问题处理](#)解决。

步骤1 在配置检查向导界面单击“配置检查”。

系统进入检查配置向导“欢迎”界面，查看可以操作的配置检查清单，如[图4-39](#)所示。

图 4-39 欢迎



步骤2 单击“下一步”。

进入“获取设备信息”界面，如[图4-40](#)所示。

图 4-40 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤3 在设备列表中选择需要检查配置的设备。

步骤4 单击“下一步”。

进入发现服务器界面。

说明

单击“停止”可终止此次任务。

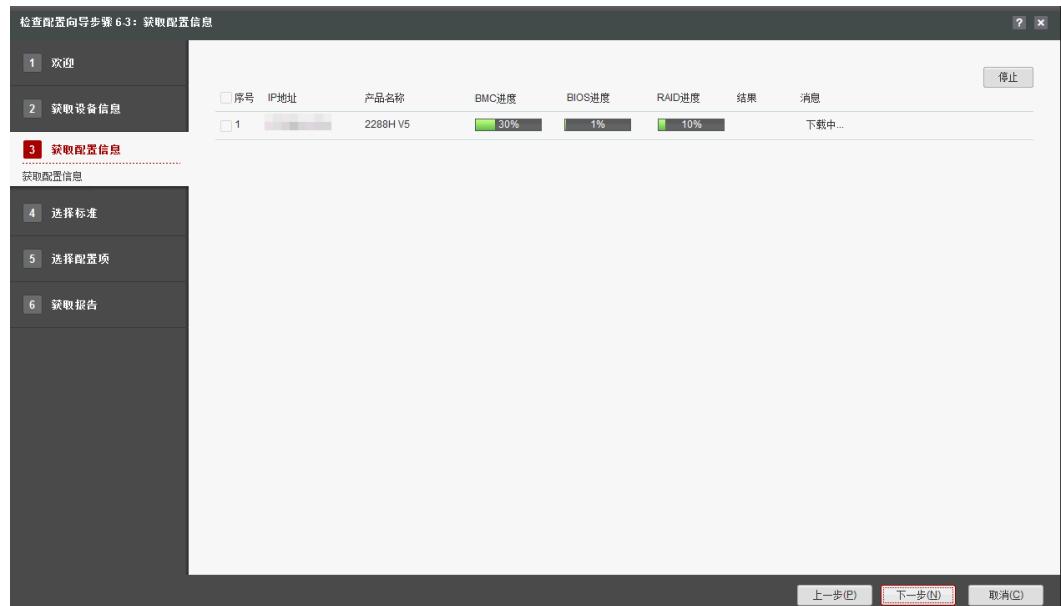
步骤5 成功发现服务器之后自动进入选择服务器界面，勾选获取配置信息的服务器和配置模块，单击“下一步”。

说明

- 至少勾选一台服务器和其对应的一个配置模块。各配置模块说明如下：
 - BMC：获取当前服务器的BMC配置信息。
 - BIOS：获取当前服务器的BIOS配置信息。
 - RAID：获取当前服务器的RAID配置信息，勾选此项前，请先确认服务器上是否存在RAID卡，否则获取配置信息时会提示：当前服务器无RAID卡，不需要检查。

步骤6 进入“获取配置信息”界面，如图4-41所示。

图 4-41 获取配置信息



步骤7 服务器配置信息获取完成后，勾选一台或多台配置模块的执行进度是100%的服务器，单击“下一步”。

进入“选择标准”界面，如图4-42所示。

图 4-42 选择标准



步骤8 选择BMC、BIOS、RAID标准文件。

只能选择导入标准配置文件或标准设备其中之一作为BMC、BIOS、RAID的检查标准。

- 勾选“选择标准设备”，选择一台配置信息已获取成功的服务器作为标准服务器。

说明

使用此方式为标准时，探测成功的服务器至少为两台。

- 勾选“导入标准配置文件”，选择导入文件作为标准文件。

说明

使用此方式为标准时，探测成功的服务器至少为一台。

各模块导入的文件说明如下：

- BMC:
导入标准配置文件：单击“选择”，导入标准文件config.xml。
- BIOS:
导入标准配置文件：单击“选择”，导入标准文件currentvalue.json或options0.ini。
导入模板文件：单击“选择”，导入模板文件registry.json或display0.ini。
- RAID:
导入标准配置文件：单击“选择”，导入标准文件currentRaidvalue.json。

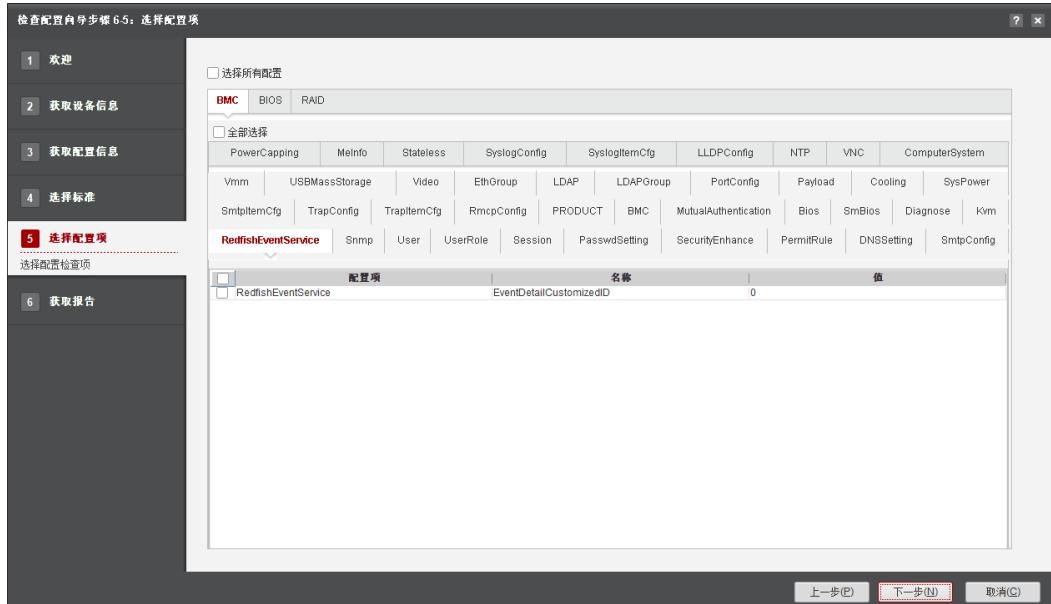
说明

- 标准文件获取地址：根目录\tools\ServerMain\work\ConfigCheck。
- 为确保数据唯一性，请不要修改导入标准文件中配置项的格式。
- 至少选择一种标准类型。
- 根据设备实际使用的标准文件和配置文件格式进行导入，具体配置文件格式可从设备导出。

步骤9 单击“下一步”。

进入“选择配置项”界面，可根据需要选择检查项，如图4-43所示。

图 4-43 选择配置项



- 单击“选择所有配置”，可进行全量对比，即BMC、BIOS和RAID的所有配置项都被勾选作对比。
- 单击“全部选择”，可分别对BMC、BIOS和RAID下的所有配置项进行对比。

□ 说明

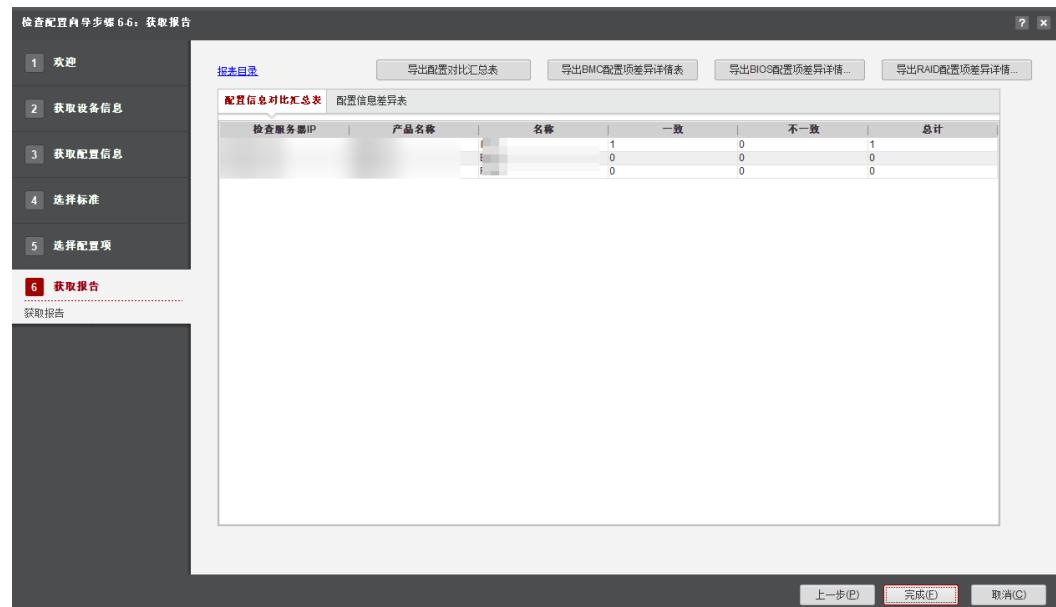
- 单击“下一步”后可能需等待几秒。
- 至少选择一个配置项做对比。

步骤10 单击“下一步”。

进入“获取报告”界面。

默认展示“配置信息对比汇总表”，如果需要查看详情，可单击“详细信息表”页签，如图4-44所示。

图 4-44 获取报告



□ 说明

在“详细信息表”中，如果“服务器值”为“--”，表示该服务器没有此配置项。

- 单击“报表目录”超链接，将弹出根目录\tools\ServerMain\work\ConfigCheck目录，可查看到自动生成的配置对比汇总结果表Summary Table.csv，配置项对比详细信息表BMC Table.csv，BIOS Table.csv，RAID Table.csv。
- 单击“导出配置对比汇总表”，导出配置对比汇总结果表。
- 单击“导出BMC配置项差异详情”，导出BMC配置项差异详细信息表。
- 单击“导出BIOS配置项差异详情”，导出BIOS配置项差异详细信息表。
- 单击“导出RAID配置项差异详情”，导出RAID配置项差异详细信息表。

步骤11 单击“完成”退出，向导界面显示设备执行结果，成功/失败/未执行的台数、以及总用时。

----结束

4.6.5 常见问题处理

表 4-25 常见问题

错误描述	原因	解决建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
Cannot login by SSH or SFTP	无法通过SSH或SFTP方式登录服务器。	<ol style="list-style-type: none">查看SSH端口是否打开，端口号与工具配置的是否一致，详细请参考5.3 查看BMC端口信息。使用Xshell软件或者其他软件尝试通过SSH及SFTP方式登录服务器，看是否可正常登录。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none">SNMP配置错误或服务器不支持SNMP命令。SNMP未响应。	<ol style="list-style-type: none">查看服务器是否支持运行工具。参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看BMC端口信息、5.4 查看BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none">确认该操作是否符合规范。重新执行该操作。
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。

错误描述	原因	解决建议
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合 SNMP 要求。	<ol style="list-style-type: none"> 1. 查看服务器是否在支持的服务器列表中。 2. 参考5.4 查看BMC的SNMP协议查看服务器是否支持 SNMP 协议。 3. 检查密码是否满足 SNMP V3 的要求, 如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3 协议不一致或用户名/密码不一致, 引起巡检(升级)串行。	<ol style="list-style-type: none"> 1. 检查所有服务器配置的 SNMP V3 协议是否一致, 并将其调整一致。 2. 检查所有服务器的用户名、密码是否一致, 并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话, IPMI命令执行失败。	<ol style="list-style-type: none"> 1. 手工执行IPMI命令, 检查是否存在故障。 2. 待问题解决后, 重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 1. 检查网络是否有异常。 2. 重新执行任务。
User must be an administrator.	使用非管理员账户执行该操作。	<ol style="list-style-type: none"> 1. 检查用户是否为管理员账户。 2. 使用管理员账户重新执行该操作。
Cannot login by SSH or SFTP, please execute with the manual mode.	无法通过SSH及SFTP登录服务器。	通过手工方式完成操作。
Download BIOS file from device failed, please try again later	下载BIOS配置文件失败。	稍后重新执行BIOS配置。
The selected template does not support this device	选择的BIOS配置模板不支持当前服务器。	选择自己作为模板或者同类型的服务器作为模板。

4.7 日志收集

日志收集工具是一键式收集服务器日志信息的工具, 具有批量收集、进度显示等特点。

4.7.1 兼容性列表

日志收集支持的操作系统列表如表4-26所示。

表 4-26 日志收集支持的操作系统

操作系统	版本
SLES	SLES 11.1
	SLES 11.2
	SLES 11.3
	SLES 11.4
	SLES 12.0
	SLES 12.2
	SLES 12.3
	SLES 15
	SLES 15.1
	SLES 12 SP3 ARM
	SLES 12 SP4 ARM
RHEL	SLES 15 ARM
	SLES 15 SP1 ARM
	RHEL 5.8
	RHEL 5.9
	RHEL 5.10
	RHEL 6.1
	RHEL 6.2
	RHEL 6.3
	RHEL 6.4
	RHEL 6.5
	RHEL 6.6
	RHEL 6.7
	RHEL 7.0
RHEL	RHEL 7.1
	RHEL 7.2
RHEL	RHEL 7.3

操作系统	版本
	RHEL 7.4
	RHEL 7.5
	RHEL 7.6
CentOS	CentOS 5.8
	CentOS 5.9
	CentOS 5.10
	CentOS 6.1
	CentOS 6.2
	CentOS 6.3
	CentOS 6.4
	CentOS 6.5
	CentOS 6.6
	CentOS 6.7
	CentOS 7.0
	CentOS 7.1
	CentOS 7.2
	CentOS 7.3
	CentOS 7.4
	CentOS 7.5
	CentOS 7.6
	CentOS 7.4 ARM
	CentOS 7.5 ARM
	CentOS 7.6 ARM
Ubuntu	Ubuntu 16.04.3 LTS ARM
	Ubuntu 16.04.4 LTS ARM
	Ubuntu 16.04.5 LTS ARM
	Ubuntu 18.04 LTS ARM
	Ubuntu 18.04.1 LTS ARM

4.7.2 批量服务器日志收集使用指导

4.7.2.1 日志收集流程

介绍日志收集的配置流程。

日志收集流程如图4-45所示。

图 4-45 日志收集



4.7.2.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

应用说明

- 使用此工具前，应事先向客户主动提供该工具的说明。
- 任何维护操作必须得到客户的授权，禁止进行超出客户审批范围的任何操作。
- 将问题定位数据传出客户网络前必须得到客户的授权。
- 使用此工具时需要遵从当地适用的法律法规。
- 问题定位完后，服务工程师必须删除本地日志文件。
- 使用此工具前，建议做好关键数据备份。

必备事项

前提条件

- PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH、VMM通信端口连通，保证能ping通服务器BMC的IP地址。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)、[5.4 查看BMC的SNMP协议](#)。

数据

收集服务器日志时需要准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

4.7.2.3 选择设备

在日志收集功能向导的“选择设备”界面中，可以选择需要收集日志的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“故障处理>日志收集”。

系统进入“日志收集”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要日志收集的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

□ 说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-27](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-27](#)，手工输入参数。

表 4-27 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.2.2 IPv6： 起始IP：2017::f434 结束IP：2017::f434 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.5.254 IPv6： 起始IP：2017::f434 结束IP：2017::f439 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	请忽略该参数，或者保持默认值。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	非root用户操作Linux操作系统时需要输入root用户密码。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6（可选）单击“浏览”，选择任务结果保存路径，单击“确定”保存。

步骤7 勾选需要收集日志的设备。单击“确定”，返回向导界面。

----结束

4.7.2.4 日志收集

在日志收集功能向导的“日志收集”界面中，可以对所选择的设备进行BMC、OS日志收集。

□ 说明

不支持在不同PC上运行工具，对同一台设备同时进行操作。

须知

日志收集过程中，会通过工具纳管的账户上传业务脚本到服务器，并在服务器上执行。

操作步骤

步骤1 在日志收集向导界面单击“日志收集”。

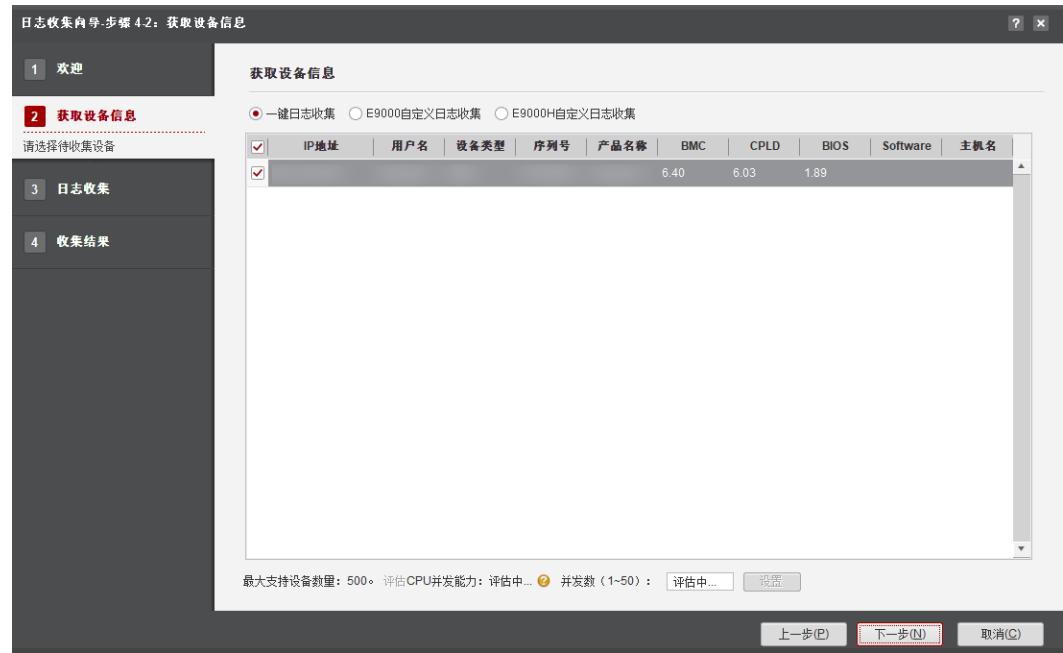
系统进入日志收集向导“欢迎”界面，查看注意事项和日志收集项，如图4-46所示。

图 4-46 欢迎



步骤2 单击“下一步”，进入“获取设备信息”界面。收集BMC、操作系统、请选择“一键日志收集”如图4-47所示。

图 4-47 获取设备信息



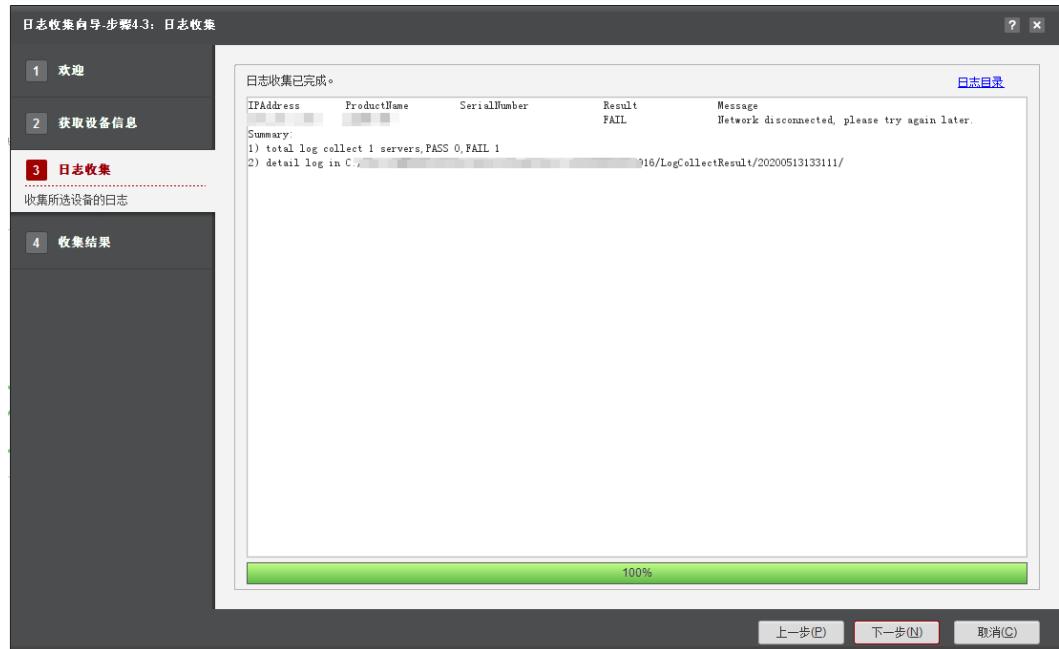
说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。
- 并发数超过20可能导致工具运行效率变低系统卡顿，日志收集因为命令执行超时而失败，请确认后再操作。

步骤3 勾选需要收集日志的设备。

单击“下一步”，进入“日志收集”界面，如图4-48所示。

图 4-48 日志收集

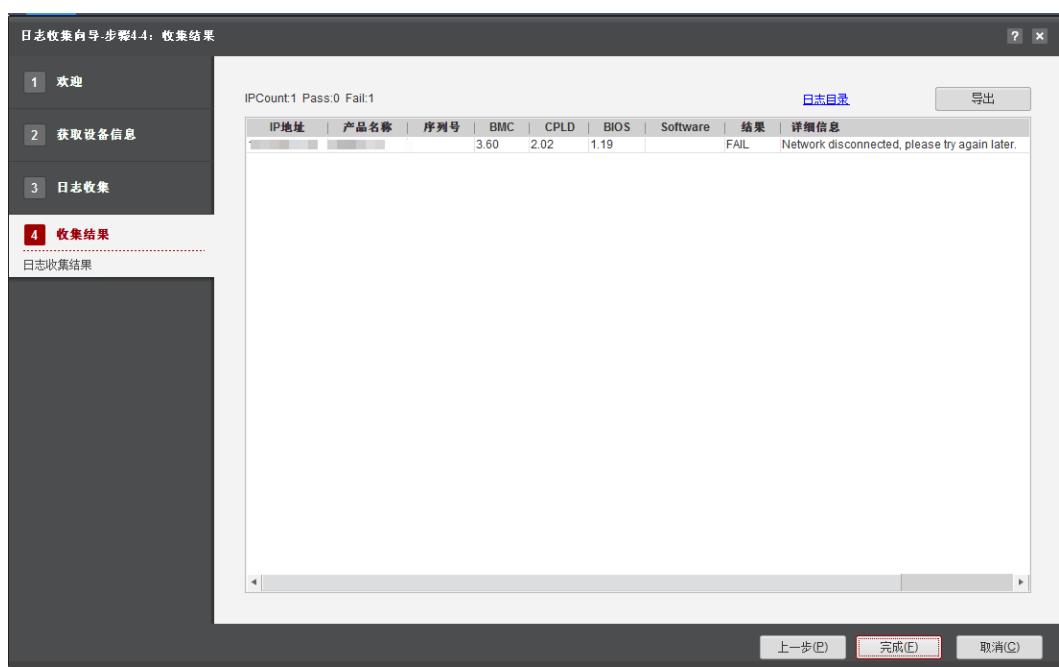


说明书

单击“停止”可终止此次任务。

步骤4 日志收集结束后，单击“下一步”，进入“收集结果”界面。如图4-49所示。

图 4-49 收集结果



BOOK 说明

- 单击“日志目录”，可打开收集的日志存放目录，可通过IP地址查看各个设备的详细日志信息。
- 单击“导出”可将此界面的结果保存至本地（默认保存“.xls”格式）。
- 服务器日志收集后，可发给服务器维护工程师分析。

步骤5 单击“完成”，弹出“当前场景整个流程已成功执行”提示框。

步骤6 单击“确认”，向导界面显示设备执行结果，成功/失败/未执行的台数、以及总用时。

----结束

4.7.3 单机 OS 日志收集使用指导

4.7.3.1 收集 Linux 操作系统日志

操作场景

收集服务器Linux操作系统日志。

必备事项

前提条件

- 登录用户ID为“0”的用户，如root。
- 已提前备份好关键数据。
- CPU使用率不超过90%，磁盘空余容量500MB以上，内存容量1GB以上且使用率不超过95%。

操作步骤

步骤1 将工具安装目录\tools\ServerInspect\tools\InfoCollect\tools下的“InfoCollect_Linux.tar.gz”文件，上传到服务器Linux操作系统。

步骤2 执行以下命令，进入“InfoCollect_Linux.tar.gz”文件所在的路径，如图4-50所示。

```
cd /home
```

图 4-50 进入文件所在的路径

```
linux:~ # cd home
linux:~/home # ls
InfoCollect_Linux.tar.gz
```

步骤3 执行以下命令，解压收集工具包，如图4-51和图4-52所示。

```
tar -zvxf InfoCollect_Linux.tar.gz
```

图 4-51 解压收集工具包

```
linux:~/home # tar -zxf InfoCollect_Linux.tar.gz
InfoCollect_Linux/
InfoCollect_Linux/infoCollect.sh
InfoCollect_Linux/modules/
InfoCollect_Linux/modules/lib/
InfoCollect_Linux/modules/lib/timeout.ini
InfoCollect_Linux/modules/lib/log.sh
InfoCollect_Linux/modules/memory/
InfoCollect_Linux/modules/memory/logCollect.cfg
InfoCollect_Linux/modules/cpu/
InfoCollect_Linux/modules/cpu/logCollect.cfg
InfoCollect_Linux/modules/driver/
InfoCollect_Linux/modules/driver/logCollect.cfg
InfoCollect_Linux/modules/mainboard/
InfoCollect_Linux/modules/mainboard/logCollect.cfg
InfoCollect_Linux/modules/bmc/
InfoCollect_Linux/modules/bmc/logCollect.cfg
InfoCollect_Linux/modules/nic/
InfoCollect_Linux/modules/nic/logCollect.cfg
InfoCollect_Linux/modules/nic/mezz_tool/
InfoCollect_Linux/modules/nic/mezz_tool/x86healthcheck.tar.gz
InfoCollect_Linux/modules/nic/mezz_collect.sh
InfoCollect_Linux/modules/raid/
InfoCollect_Linux/modules/raid/logCollect.cfg
InfoCollect_Linux/modules/raid/RAIDtool/
InfoCollect_Linux/modules/raid/RAIDtool/2308/
InfoCollect_Linux/modules/raid/RAIDtool/2308/hbacli
InfoCollect_Linux/modules/raid/RAIDtool/2308/sas2ircu
InfoCollect_Linux/modules/raid/RAIDtool/2308/sas2flash
InfoCollect_Linux/modules/raid/RAIDtool/3008/
InfoCollect_Linux/modules/raid/RAIDtool/3008/hbacli
```

图 4-52 解压收集工具包

```
InfoCollect_Linux/modules/raid/RAIDtool/3008/sas3ircu
InfoCollect_Linux/modules/raid/RAIDtool/3008/sas3flash
InfoCollect_Linux/modules/raid/RAIDtool/2208/
InfoCollect_Linux/modules/raid/RAIDtool/3108/
InfoCollect_Linux/modules/raid/RAIDtool/3108/storcli-1.15.04-1.tar.gz
InfoCollect_Linux/modules/bios/
InfoCollect_Linux/modules/bios/logCollect.cfg
InfoCollect_Linux/modules/disk/
InfoCollect_Linux/modules/disk/logCollect.cfg
InfoCollect_Linux/modules/disk/cmdlist.ini
InfoCollect_Linux/modules/system/
InfoCollect_Linux/modules/system/logCollect.cfg
InfoCollect_Linux/modules/hba/
InfoCollect_Linux/modules/hba/logCollect.cfg
InfoCollect_Linux/config.ini
InfoCollect_Linux/version.ini
linux:~/home # ls
InfoCollect_Linux  InfoCollect_Linux.tar.gz
```

步骤4 执行以下命令，进入“InfoCollect_Linux”目录，如图4-53所示。

```
cd InfoCollect_Linux/
```

图 4-53 进入 InfoCollect_Linux 目录

```
linux:~/home # cd InfoCollect_Linux/
linux:~/home/InfoCollect_Linux # ls
config.ini  infoCollect.sh  modules  version.ini
```

步骤5 执行以下命令，给用户增加“InfoCollect_Linux”目录下所有文件的操作权限。

```
chmod +x -R *
```

步骤6 (可选) 执行以下命令，修改“config.ini”文件，指定需要收集的日志，如图4-54所示。

```
vi config.ini
```

图 4-54 修改 config.ini 文件

```
#####
#Introduction:Config.ini file is used to specify the log files to be collected.
#File format:
# -- Module:Log file module
# -- filename:Log file name
# -- flag: yes:collect no:not collect
#Description:A brief description of the log file.More detail please refer to user guide
#Recommendation:users edit the flag column, specify the logs you want to collect.
#####
Module      filename          flag    description
-----+-----+-----+-----+
bios      |version_bios.txt      |yes    |BIOS version
bmc       |fru.txt              |yes    |FRU list
bmc       |mc_info.txt          |yes    |BMC version
bmc       |sensor.csv            |yes    |BMC sensor list
bmc       |sdr.csv               |yes    |BMC sdr list
bmc       |sel.csv               |yes    |BMC sel list
bmc       |time.txt              |yes    |The time information of bios bmc and os
bmc       |version_cpld.txt      |yes    |CPLD version
bmc       |bmc_lan.txt            |yes    |BMC nic info
disk      |sys_block.txt          |yes    |Hard disk names
disk      |parted_disk.txt        |yes    |All disks partition
disk      |hwdiag_hdd.txt          |yes    |All disks diagnose collected by BMA
disk      |disk_smart.txt          |yes    |All disk SMART information collected by BMA
disk      |es3000_v2.txt            |yes    |All ES3000 V2 PCIe SSD information
disk      |es3000_v3.txt            |yes    |All ES3000 V3 NVMe PCIe SSD information
cpu       |cpuinfo.txt            |yes    |CPU model and frequency
cpu       |cpu_dmidecode.txt       |yes    |CPU information collected by dmidecode
mainboard |dmidecode.txt          |yes    |All hardware information collected by dmidecode
mainboard |lspci.txt              |yes    |Detail pci devices information
driver    |lsmod.txt              |yes    |The status of modules in the Linux Kernel
driver    |modinfo.txt             |yes    |All modules driver list
hba       |lspci_fc.txt            |yes    |PCI information of FC model
hba       |firmware_fc.txt          |yes    |FC HBA firmware information
hba       |driver_fc.txt            |yes    |FC HBA driver information
hba       |wwpn.txt                |yes    |FC HBA wwpn information
nic       |lspci_eth.txt            |yes    |NIC list
nic       |/etc/sysconfig/network-scripts/* |yes    |NIC configuration files
"config.ini" 106L, 8536C
```

说明

编辑“flag”列，可设置需要收集的日志文件，“yes”表示收集，“no”表示不收集。部分收集项未设置为默认收集，例如：/var/log/message*，请根据实际需求修改。

步骤7 执行以下命令，收集日志，如图4-55所示。

```
./infoCollect.sh
```

图 4-55 Linux 收集脚本执行

说明

整个日志收集过程持续几分钟, 请耐心等待。

步骤8 日志收集完成后，提示信息如图4-56所示，表示操作成功。

图 4-56 提示

```
==[ DONE ]=====
Log file Dir: /home/InfoCollect_Linux/localhost.localdomain_20220801_151731.tar.gz
Log file size: 28M
Please collect crash files[/var/crash] manually.
```

说明书

- 如图4-56中的: /home/InfoCollect_Linux/localhost.localdomain_20220801_151731.tar.gz 为日志文件目录。
 - /home为InfoCollect_Linux.tar.gz文件存放的位置。
 - /localhost.localdomain_20220801_151731.tar.gz为日志文件压缩包。日志文件压缩包的名称,请以实际收集完成后Log file Dir显示为准。
- 进入日志文件目录,打开日志文件压缩包中的“filelist.txt”文件可查看日志收集清单。
- 可对收集到的日志文件进行筛选再压缩打包。
- crash文件较大,若需要通过此文件定位故障,则需要用户手动收集。
- 收集系统日志默认的最大收集时间为20分钟。

----结束

4.7.4 日志收集项清单

受服务器环境或配置影响,日志收集项会存在差异,以下收集项清单,仅供参考。

- BMC日志收集项清单如表4-28所示。
- Linux操作系统日志收集项清单如表4-29所示。

表 4-28 BMC 日志收集项清单

目录	子目录	文件名	文件内容说明
/	/	dump_app_log	App信息收集结果列表
		dump_log	一键收集结果列表
App Dump	Lcd	Lcd_dfl.log	管理对象信息
	User	User_dfl.log	管理对象信息
	card_manage	card_manage_dfl.log	管理对象信息
		card_info	扣卡信息
	BMC	BMC_dfl.log	管理对象信息
		fruinfo.txt	fru电子标签信息
		net_info.txt	网口配置信息
	PowerMgmt	PowerMgmt_dfl.log	管理对象信息
	UPGRADE	UPGRADE_dfl.log	管理对象信息
		upgrade_info	升级信息
	BIOS	BIOS_dfl.log	管理对象信息
		bios_info	BIOS配置信息
		ClpConfig0.ini	BIOS配置信息
		ClpResponse0.ini	BIOS配置信息

目录	子目录	文件名	文件内容说明
		options0.ini	BIOS配置信息
		changed0.ini	BIOS配置信息
		display0.ini	BIOS配置信息
diagnose		diagnose_dfl.log	管理对象信息
		diagnose_info	Port 80信息
Snmp		Snmp_dfl.log	管理对象信息
cooling_app		cooling_app_dfl.log	管理对象信息
		fan_info.txt	风扇信息
CpuMem		CpuMem_dfl.log	管理对象信息
		cpu_info	CPU信息
		mem_info	内存条信息
kvm_vmm		kvm_vmm_dfl.log	管理对象信息
ipmi_app		ipmi_app_dfl.log	管理对象信息
Dft		Dft_dfl.log	管理对象信息
sensor_alarm		sensor_alarm_dfl.log	管理对象信息
		sensor_info.txt	传感器列表
		current_event.txt	当前健康事件
		sel.tar	当前sel信息和历史sel信息打包文件
		sensor_alarm_sel.bin.md5	sel原始记录文件完整性校验码
		sensor_alarm_sel.bin.back.md5	sel原始记录备份文件完整性校验码
		sensor_alarm_sel.bin.back	sel原始记录备份文件
		sensor_alarm_sel.bin	sel原始记录文件
		sel.db	sel数据库文件
		sensor_alarm_sel.bin.tar.gz	sel历史记录打包文件
MaintDebug		MaintDebug_dfl.log	管理对象信息
FileManage		FileManage_dfl.log	管理对象信息

目录	子目录	文件名	文件内容说明	
3rdDump	switch_card	switch_card_dfl.log	管理对象信息	
		phy_register_info	phy寄存器信息	
		port_adapter_info	接口器件信息	
	StorageMgnt	StorageMgnt_dfl.log	管理对象信息	
		RAID_Controller_Info.txt		
	rimm	rimm_dfl.log	管理对象信息	
	dfm	dfm.log	管理对象信息、模块信息	
		dfm_debug_log	框架调试日志	
		dfm_debug_log.1		
	-	error_log	Apache错误日志	
Core Dump	-	access_log	Apache访问日志	
		httpd.conf	Apache http配置文件	
RTOS Dump		httpd-port.conf	Apache http端口配置文件	
		httpd-ssl.conf	Apache https配置文件	
		httpd-ssl-port.conf	Apache https端口配置文件	
		httpd-ssl-protocol.conf	Apache https协议版本配置文件	
		core-*	内存转储文件	
sysinfo	cmdline	内核的命令行参数		
	cpuinfo	cpu信息		
	devices	设备信息		
	df_info	分区空间使用信息		
	diskstats	分区信息		
	filesystems	文件系统信息		
	free_info	内存使用情况		
	interrupts	中断信息		
	ipcs_q	进程队列信息		
	ipcs_q_detail	进程队列详细信息		
	ipcs_s	进程信号量信息		
	ipcs_s_detail	进程信号量详细信息		

目录	子目录	文件名	文件内容说明
		loadavg	系统运行负载情况
		locks	内核锁住的文件列表
		meminfo	内存使用信息
		modules	模块加载列表
		mtd	分区信息
		partitions	分区信息
		ps_info	ps -elf 显示进程信息
		slabinfo	内核内存管理slab信息
		stat	CPU利用率
		top_info	top -bn 1 显示当前进程运行情况
		uname_info	uname -a 显示当前内核版本
		uptime	BMC系统运行时间
		version	RTOS版本
		vmstat	虚拟内存统计信息
	versioninfo	BMC_revision.txt	编译节点信息
		app_revision.txt	BMC版本信息
		build_date.txt	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
	networkinfo	ifconfig_info	ifconfig信息
		ipinfo_info	ip配置信息
		_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

目录	子目录	文件名	文件内容说明
		dhclient6_eth2.leases	dhcp租约文件
		dhclient.conf	dhcp配置文件
		dhclient_ip.conf	dhcp配置文件
		dhclient6.conf	dhcp配置文件
		dhclient6_ip.conf	dhcp配置文件
		resolv.conf	dns配置文件
		ipinfo.sh	BMC网络配置脚本
		netstat_info	netstat -a 显示当前网络端口、连接使用情况
		route_info	route 显示当前路由信息
		services	服务端口信息
	other_info	extern.conf	log文件配置
		remotelog.conf	syslog定制配置文件
		ssh	ssh服务配置
		sshd_config	sshd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
		sfcb	CIM pam登录规则
		datafs_log	data检测日志
		ntp.conf	NTP服务配置
	driver_info	dmesg_info	dmesg信息
		lsmod_info	当前加载驱动模块信息
		kbox_info	kbox信息
		edma_drv_info	edma驱动的统计信息
		cdev_drv_info	字符设备驱动的统计信息
		veth_drv_info	虚拟网卡驱动的统计信息
LogDump	-	app_debug_log app_debug_log.tar.gz	应用模块调试日志

目录	子目录	文件名	文件内容说明
		linux_kernel_log linux_kernel_log.1	Linux内核日志
		card_mmio_log card_mmio_log.tar.gz	外设卡各槽位的MMIO、MMCFG的配置信息
		diagnose_log.tar.gz diagnose_log	FDM2.0诊断结果日志
		remote_log remote_log.1.gz	syslog test操作日志、sel日志
		operate_log operate_log.tar.gz	用户操作日志
		security_log security_log.1	安全日志
		strategy_log strategy_log.tar.gz	策略日志
		fdm_log fdm_log.tar.gz	故障解析日志文件
		maintenance_log	维护日志
		ipmi_debug_log ipmi_debug_log.tar.gz	IPMI模块日志
		ipmi_mass_operation_log ipmi_mass_operation_log.tar.gz	IPMI模块运行日志
		app_debug_log_all app_debug_log_all.1.gz app_debug_log_all.2.gz app_debug_log_all.3.gz	所有应用模块调试日志
		kvm_vmm_debug_log kvm_vmm_debug_log.tar.gz	KVM模块日志
		reg_info_log reg_info_log.tar.gz	BIOS上报的原始寄存器信息

目录	子目录	文件名	文件内容说明
		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
OSD ump	-	systemcom.tar	SOL串口信息
		img*.jpeg	最后一屏图像
		*.rep	屏幕自动录像文件
DeviceDump	i2c_info	*_info	I2C设备的寄存器/存储区信息
Register	-	cpld_reg_info	cpld寄存器信息
OptP me	pram	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.md 5	完整性校验码
		BMC_dhclient.conf.sha 256	完整性校验码
		BMC_dhclient6.conf	dhcp配置文件
		BMC_dhclient6.conf.m d5	完整性校验码
		BMC_dhclient6.conf.sh a256	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.s ha256	完整性校验码
		BMC_dhclient6_ip.conf	dhcp配置文件
		BMC_dhclient6_ip.conf. md5	完整性校验码

目录	子目录	文件名	文件内容说明
		BMC_dhclient6_ip.conf.sha256	完整性校验码
		BMC_HOSTNAME	主机名
		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
		cpu_utilise_webview.dat	管理对象运行信息
		env_web_view.dat	管理对象运行信息
		fsync_reg.ini	文件同步配置文件
		HwScan_EnvRecWave	管理对象运行信息
		lost+found	文件夹
		mdio_lock_file	mdio文件锁
		md_so_app_debug_log	app调试日志
		md_so_app_debug_log.tar.gz	app调试日志打包
		md_so_ipmi_debug_log	ipmi调试日志
		md_so_ipmi_debug_log.tar.gz	ipmi调试日志打包
		md_so_maintenance_log	维护日志
		md_so_maintenance_log.tar.gz	维护日志打包
		md_so_mass_operate_log	操作日志
		md_so_mass_operate_log.tar.gz	操作日志打包
		md_so_operate_log	操作日志
		md_so_operate_log.md5	完整性校验码
		md_so_operate_log.tar.gz	操作日志打包

目录	子目录	文件名	文件内容说明
		md_so_strategy_log	策略日志
		md_so_strategy_log.md5	完整性校验码
		md_so_operate_log.sha256	完整性校验码
		md_so_strategy_log.tar.gz	策略日志打包
		memory_webview.dat	管理对象运行信息
		NetConfig_dhclient.conf	dhcp配置文件
		NetConfig_dhclient.conf.md5	完整性校验码
		md_so_strategy_log.sha256	完整性校验码
		NetConfig_dhclient_ip.conf	dhcp配置文件
		NetConfig_dhclient_ip.conf.md5	完整性校验码
		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.back	BMC配置持久化文件
		per_config_reset.ini.back.md5	完整性校验码
		per_config_reset.ini.back.sha256	完整性校验码
		per_config_reset.ini.md5	完整性校验码

目录	子目录	文件名	文件内容说明
		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

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

目录	子目录	文件名	文件内容说明
		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服务配置文件
		User_sshd_config.md5	完整性校验码
		User_sshd_config.sha256	完整性校验码
		User_vsftp	ftp pam登录规则
		User_vsftp.md5	完整性校验码
		User_vsftp.sha256	完整性校验码
		eo.db	sel数据库
	save	filelist	/opt/pme/pram目录下文件列表
	save	BIOS_FileName	SMBIOS信息
	save	BMC_dhclient.conf.bak	dhcp配置文件
	save	BMC_dhclient.conf.bak.md5	完整性校验码
	save	BMC_dhclient.conf.bak.sha256	完整性校验码
	save	BMC_dhclient.conf.md5	完整性校验码
	save	BMC_dhclient.conf.sha256	完整性校验码
	save	BMC_dhclient6.conf.bak	dhcp配置文件
	save	BMC_dhclient6.conf.bak.md5	完整性校验码
	save	BMC_dhclient6.conf.bak.sha256	完整性校验码
	save	BMC_dhclient6.conf.md5	完整性校验码

目录	子目录	文件名	文件内容说明
		BMC_dhclient6.conf.sh.a256	完整性校验码
		BMC_dhclient_ip.conf.bak	dhcp配置文件
		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_ip.conf.bak	dhcp配置文件
		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
		BMC_HOSTNAME.bak.md5	完整性校验码
		BMC_HOSTNAME.bak.sha256	完整性校验码
		BMC_HOSTNAME.bak.md5	完整性校验码
		BMC_HOSTNAME.sha256	完整性校验码
		BMC_HOSTNAME.md5	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
		HwScan_EnvRecWave	管理对象运行信息
		md_so_operate_log.bak	操作日志

目录	子目录	文件名	文件内容说明
		md_so_operate_log.bak.md5	完整性校验码
		md_so_operate_log.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
		NetConfig_dhclient.conf.bak	dhcp配置文件
		NetConfig_dhclient.conf.bak.md5	完整性校验码
		NetConfig_dhclient.conf.md5	完整性校验码
		NetConfig_dhclient_ip.conf.bak	dhcp配置文件
		NetConfig_dhclient_ip.conf.bak.md5	完整性校验码
		NetConfig_dhclient_ip.conf.md5	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

目录	子目录	文件名	文件内容说明
		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
		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
		PowerMgnt_record	管理对象运行信息
		sensor_alarm_sel.bin	sel原始记录文件
		sensor_alarm_sel.bin.bak	sel原始记录文件
		sensor_alarm_sel.bin.bak.md5	完整性校验码
		sensor_alarm_sel.bin.bak.sha256	完整性校验码
		sensor_alarm_sel.bin.md5	完整性校验码
		sensor_alarm_sel.bin.sha256	完整性校验码
		sensor_alarm_sel.bin.tar.gz	sel历史记录打包文件
		Snmp_http_configure.bak	HTTP Server配置文件
		Snmp_http_configure.bak.md5	完整性校验码

目录	子目录	文件名	文件内容说明
		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	HTTP Server配置文件
		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	HTTP Server配置文件
		Snmp_https_tsl.bak.md5	完整性校验码
		Snmp_https_tsl.bak.sha256	完整性校验码
		Snmp_https_tsl.md5	完整性校验码
		Snmp_https_tsl.sha256	完整性校验码
		Snmp_snmpd.conf.bak	snmp配置文件
		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

目录	子目录	文件名	文件内容说明
		User_login.sha256	完整性校验码
		User_sshd.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服务配置文件
		User_sshd_config.bak.md5	完整性校验码
		User_sshd_config.bak.sha256	完整性校验码
		User_sshd_config.md5	完整性校验码
		User_sshd_config.sha256	完整性校验码
		User_vsftp.bak	ftp pam登录规则
		User_vsftp.bak.md5	完整性校验码
		User_vsftp.bak.sha256	完整性校验码
		User_vsftp.md5	完整性校验码
		User_vsftp.sha256	完整性校验码
		eo.db	sel数据库
		eo.db.md5	完整性校验码
		eo.db_backup	sel数据库
		eo.db.md5_backup	完整性校验码

表 4-29 Linux 操作系统日志收集项清单

模块	文件名称	收集命令	文件说明
公共	version.txt	-	工具版本和发布时间
	filelist.txt	-	收集到的文件清单
BIOS	version_bios.txt	dmidecode -t bios	BIOS版本信息

模块	文件名称	收集命令	文件说明
BigData	selfdiag_log.txt	/opt/DA200/compress_tools/tools/dcadm selfdiag	DA200 selfdiag信息 (需要安装DA200工具)
	Lspci_log.txt	lspci grep d501	型号信息
	/var/log/DA200/	cp /var/log/DA200/	DA200卡日志信息
	/var/log/bigdata/	cp /var/log/bigdata/	DA200卡日志信息
BMC	fru.txt	ipmitool fru list	FRU部件信息
	bmc_lan.txt	ipmitool lan print 1	BMC网卡信息
	mc_info.txt	ipmitool mc info	BMC版本信息
	sensor.csv	ipmitool sensor list	所有传感器信息
	sdr.csv	ipmitool sdr elist	SDR日志
	sel.csv	ipmitool sel elist	BMC SEL日志
	version_cpld.txt	ipmitool raw0x30 0x90 0x08 0 2 0x00 0x10	CPLD版本信息
	time.txt	ipmitool sel time get date hwclock	BMC、BIOS、OS时间
iBMA	common.log	cat /opt/huawei/ibma/log/common.log	通用日志
	http_server.log	cat /opt/huawei/ibma/log/http_server.log	http服务器日志
	BMC_event.log	cat /opt/huawei/ibma/log/BMC_event.log	BMC事件日志
	nicErrorStatistics.log	cat /opt/huawei/ibma/log/nicErrorStatistics.log	网卡故障数据
	runlog	cat /opt/huawei/ibma/log/runlog	操作相关运行日志
	service.log	cat /opt/huawei/ibma/log/service.log	iBMA服务相关日志
CPU	cpuinfo.txt	cat /proc/cpuinfo	CPU型号、频率等信息
	cpu_dmidecode.txt	dmidecode -t processor	执行 dmidecode 命令获取到的CPU信息
	cpu_usage.txt	top -b -n 60	CPU占用率

模块	文件名称	收集命令	文件说明
硬盘	disk_smart.txt	<pre>smartctl -a /dev/sd* smartctl -a --device=sat +megaraid,0 /dev/sd* smartctl -a -- device=megaraid, 0 /dev/sd* hwdiag -t disk -s nvme -smart-log /dev/ nvmeXX nvme intel smart-log- add /dev/nvmeXX nvmecli -smart- log /dev/nvmeXX</pre>	硬盘的SMART信息（需要安装smartctl工具，NVMe盘需安装nvme、nvmecli工具）
	phy_info.txt	ls -l /dev/disk/by-path	硬盘phy信息
	sys_block.txt	ls -l /sys/block/sd*	硬盘名称
	parted_disk.txt	parted /dev/sda print	物理硬盘的分区信息
	hwdiag_hdd.txt	hwdiag -t disk -d	通过iBMA硬盘的打分数据（适用于系统已经安装iBMA）
	es3000_v2.txt	<pre>hio_info -d -- device=hioa,/dev/hio* hio_label -d -- device=hioa,/dev/hio* hio_log -d -- device=hioa,/dev/hio* hio_temperature -d -- device=hioa,/dev/hio*</pre>	ES3000 V2 PCIe SSD信息
	es3000.txt	<pre>modinfo nvme hioadm info -d device=nvme0/pd0/ sda,hioadm info hioadm info -d device=nvme/pd/ sd,hioadm info -s hioadm info -d device=nvme/pd/ sd,hioadm info -a hioadm log -d device=nvme0/pd0/ sda,hioadm info -a</pre>	ES3000 V3/V5/V6 SAS SSD和NVME PCIE SSD日志信息
	udisk.txt	./udisk -v	查询uDisk版本

模块	文件名称	收集命令	文件说明
磁盘		./udisk -l all ./udisk -s all ./udisk -m all ./udisk -d all ./udisk -p al	查询硬盘的基本信息 查询硬盘的健康状态 查询硬盘的事件 查询硬盘的smart信息 查询硬盘的phy信息
	scheduler.txt	cat /sys/block/*/queue/scheduler	操作系统的硬盘I/O调度器信息
	blktrace/\${disk}/blktrace_log.txt	blktrace -d /dev/\${disk} -w 30 -D logPath blkparse -i \${disk} -D logPath -d logPath/blktrace.bin cd logPath && btt -i blktrace.bin -l d2c_latency -q q2c_latency -B offset > blktrace.txt	磁盘blktrace信息
	disk_other_info.txt	sg_logs -a /dev/sd* sg_modes -a -a /dev/sd* lspci -vvvxxx -s \$BDF	硬盘其他信息收集
	/opt/hio/operationLogs/operations.log	cp /opt/hio/operationLogs/operations.log	hioadm工具运行日志
	dmidecode.txt	dmidecode	硬件信息
	lspci.txt	lspci	PCI设备列表
		lspci -xxx -vvv -t	详细PCI设备信息
		lspci -xxxx -vvv -b	以总线为中心查看PCI和IRQ设备信息
网卡	lspci_eth.txt	lspci grep Ethernet	网卡清单
	/etc/modprobe.d	cp /etc/modprobe.d/	网卡的配置文件
	/etc/sysconfig/network/*	cp /etc/sysconfig/network/*	SLES系统下的网卡配置文件
	/etc/sysconfig/network-scripts/*	cp /etc/sysconfig/network-scripts/*	RHEL、CentOS和Euler系统下的网卡配置文件

模块	文件名称	收集命令	文件说明
	mezz_info.tar.gz	<pre>/bin/date /usr/bin/uptime dmidecode biosdecode lspci -tv ifconfig -a /sbin/ip link show /sbin/route -n ethtool -i ethX ethtool ethX ethtool -a ethX ethtool -l ethX ethtool -d ethX ethtool -e ethX ethtool -S ethX ethtool -g ethX ethtool -k ethX /sbin/lspci -xxx -s XX:XX.X lspci -vvv -xxx -s XX:XX.X /bin/netstat -nlp /bin/netstat -nr /bin/netstat -i /sbin/arp -v /usr/sbin/iptables -t filter -nvL x86tool -r pci/ bXX:XX.X-0xXXXXXX+4-bX</pre>	collect_info/network.txt: 网卡信息 mezz.log: 收集脚本自身运行日志文件
	bonding.txt	cp /proc/net/bonding/	网卡绑定信息
	bdf.txt	ls -l /sys/class/net	网卡BDF信息

模块	文件名称	收集命令	文件说明
	error_frame_cr.c.txt	cat /sys/class/net/*/ statistics/rx_crc_errors cat /sys/class/net/*/ statistics/ rx_frame_errors	网卡错帧和端口误码信息
	1822_nic_info.tar.gz	./hinic_log_collect.sh -a	收集1822网卡日志信息
	routeInfo.txt	route -n	网卡路由信息
	iptablesInfo.txt	iptables -t filter -nvL	防火墙信息
	trafficControl.txt	tc -s qdisc	显示 / 维护流量控制设置
	network_adapter_numa_node.txt	cat /sys/class/net/*/ device/numa_node	网卡信息
	nic_pci_info.txt	ll /sys/class/net	网卡PCI接口信息
		cat /sys/class/net/ethX/ device/device	网卡PCI信息
		cat /sys/class/net/ethX/ device/vendor	
		cat /sys/class/net/ethX/ device/ subsystem_vendor	
		cat /sys/class/net/ethX/ device/subsystem_device	
		/var/log/boot.msg	网卡驱动日志
cna	cna_pci_info.txt	cat /sys/devices/ pci0000:xx/[root port]/ [bus/device/function]/ device cat /sys/devices/ pci0000:xx/[root port]/ [bus/device/function]/ subsystem_vendor cat /sys/devices/ pci0000:xx/[root port]/ [bus/device/function]/ subsystem_device	CNA卡PCI信息

模块	文件名称	收集命令	文件说明
	cna_fcoe_info.txt	cat /sys/devices/pci0000:xx/[root port]/[bus/device/function]/vendor	
		cat /sys/class/fc_host/hostX/symbolic_name	CNA卡firmware版本
		ethtool -i ethY	
		cat /sys/class/fc_host/hostX/port_id	CNA卡端口FC_ID信息
		cat /sys/class/fc_host/hostX/port_type	CNA卡端口类型信息
		cat /sys/class/fc_host/hostX/speed	CNA卡端口速率信息
		cat /sys/class/fc_host/hostX/fabric_name	CNA卡端口连接的Switch的WWN信息
	hba_pci_info.txt	iostat -mx [interval] [count]	磁盘/LUN性能统计信息
		cat /sys/devices/pci0000:xx/[root port]/[bus/device/function]/vendor	HBA卡PCI信息
		cat /sys/devices/pci0000:xx/[root port]/[bus/device/function]/device	
		cat /sys/devices/pci0000:xx/[root port]/[bus/device/function]/subsystem_vendor	
		cat /sys/devices/pci0000:xx/[root port]/[bus/device/function]/subsystem_device	
		rpm -qa grep lpfc (Emulex) modinfo lpfc grep version (Emulex) modinfo qla2xxx grep version (QLogic)	HBA卡驱动版本
		cat /sys/class/fc_host/hostX/port_id	HBA卡端口FC_ID信息

模块	文件名称	收集命令	文件说明
		cat /sys/class/fc_host/hostX/port_type	HBA卡端口类型信息
		cat /sys/class/fc_host/hostX/speed	HBA卡端口速率信息
		cat /sys/class/fc_host/hostX/fabric_name	HBA卡端口连接的Switch的WWN信息
		iostat -mx [interval] [count]	磁盘/LUN性能统计信息
	lspci_fc.txt	lspci grep Fibre	FC型号
	firmware_fc.txt	cat /sys/class/scsi_host/host*/fwrev cat /sys/class/scsi_host/host*/fw_version	FC HBA卡的固件信息
	driver_fc.txt	cat /sys/class/scsi_host/host*/lpfc_drvr_version cat /sys/class/scsi_host/host*/driver_version	FC HBA卡的驱动信息
	wwpn.txt	cat /sys/class/fc_host/host*/port_name cat /sys/class/fc_host/host*/node_name	FC HBA卡的WWPN和WWNN信息
	bdf.txt	ls -l /sys/class/fc_host/ ls -l /sys/class/iscsi	Iscsi和FC HBA卡的BDF信息
	error_frame_crc.txt	cat /sys/class/fc_host/host*/statistics/error_frames cat /sys/class/fc_host/host*/statistics/invalid_crc_count	FC HBA卡的端口误码和错帧信息
驱动	port_state.txt	cat /sys/class/fc_host/host*/port_state	FC HBA卡的端口状态信息
	1822_fc_info.tar.gz	./collect_log_prd.sh	收集1822FC HBA卡日志信息
内存	meminfo	/proc/meminfo	内存信息

模块	文件名称	收集命令	文件说明
	mem_ecc.txt	mcelog --client	内存ECC信息（默认为空）
	memory_dmid_ecode.txt	dmidecode -t memory	物理内存信息
	hwdiag_mem.txt	hwdiag -t mem -d	通过iBMA收集内存的诊断数据（适用于系统已经安装iBMA）
	swapon_info.txt	swapon --bytes --show	显示交换分区设备的信息
RAID	sashbalog.txt	sas3ircu_arm组合命令集	LSI SAS3008 RAID卡日志（arm）
		sas3ircu sas3flash hbacli组合命令集	LSI SAS3008 RAID卡日志（x86）
		sas2ircu sas2flash hbacli组合命令集	LSI SAS2308 RAID卡日志（x86）
	sasraidlog.txt	storcli组合命令集	LSI SAS2208、LSI SAS3108、Avago SAS3408、Avago SAS3508或Avago SAS3516 RAID卡日志
	diskmap.txt	lsscsi opt/MegaRAID/storcli/ storcli c* show	LSI SAS2208、LSI SAS3108、Avago SAS3408或Avago SAS3508 RAID卡的逻辑磁盘与物理盘的对应关系
	/md/ mdinfo.txt	-	软RAID md信息
	pmc/Support/*	arcconf savesupportarchive	收集RAID控制卡的Firmware日志
	snap_dump_result.txt snapdump*.zip	storcli64 /call show snapdump storcli64 /call get snapdump ID=all	查询Raid卡snmpdump日志信息并获取日志文件
	系统	runlog	工具运行后台记录
		/var/log/secure	安全日志
		/var/log/mcelog	定位MCE错误需要的日志信息
		/var/log/message	常规系统日志文件

模块	文件名称	收集命令	文件说明
	/var/log/cron	cp /var/log/cron*	定制任务日志文件
	/var/log/boot.log	cp /var/log/boot.log	本次启动日志, log格式
	/var/log/boot.msg	cp /var/log/boot.msg	本次启动日志, msg格式
	/var/log/boot.0msg	cp /var/log/boot.0msg	启动日志 (本次启动的前一次过程日志)
	/etc/syslog.conf	cp /etc/syslog.conf	syslogd进程的配置文件
	/etc/resolv.conf	cp /etc/resolv.conf	网络代理的配置文件
	/etc/hosts	cp /etc/hosts	主机信息
	/etc/services	cp /etc/services	启动服务
	/etc/sysctl.conf	cp /etc/sysctl.conf	系统内核参数配置文件, 涉及网络功能, 例如转发等
	/etc/inittab	cp /etc/inittab	初始化, 涉及系统配置
	/etc/ntp.conf	cp /etc/ntp.conf	NTP配置文件
	/etc/ntp/step-tickers	cp /etc/ntp/step-tickers	NTP配置文件
	/etc/ntp/ntpservers	cp /etc/ntp/ntpservers	NTP服务器列表
	/etc/yp.conf	cp /etc/yp.conf	ypbind配置文件
	/etc/fstab	cp /etc/fstab	文件系统列表
	/proc/interrupts	cp /proc/interrupts	中断数量
	/proc/filesystems	cp /proc/filesystems	当前文件系统列表
	/etc/exports	cp /etc/exports	NFS服务器配置
	/proc/self/maps	cp /proc/self/maps	查看进程的虚拟地址空间
	/proc/self/smaps	cp /proc/self/smaps	单个进程的内存查看
	/proc/self/numa_maps	cp /proc/self/numa_maps	numa进程的内存查看
	/proc/iomap	cp /proc/iomap	I/O映射内存空间

模块	文件名称	收集命令	文件说明
	/proc/ioports	cp /proc/ioports	显示当时正在使用的I/O端口资源分布
	/proc/swaps	cp /proc/swaps	交换分区信息
	/proc/slabinfo	cp /proc/slabinfo	内核信息
	/proc/locks	cp /proc/locks	查看是否有进程锁定
	/proc/modules	cp /proc/modules	显示各个模块
	/proc/mounts	cp /proc/mounts	显示当前挂载的设备
	/proc/version	cp /proc/version	查看内核版本
	/proc/stat	cp /proc/stat	内核和系统的统计信息
	/proc/schedstat	cp /proc/schedstat	内核schedstat信息
	/proc/zoneinfo	cp /proc/zoneinfo	内核时区信息
	/proc/config.gz	cp /proc/config.gz	proc文件系统配置文件集
	/proc/kallsyms	cp /proc/kallsyms	内核调试文件
	/proc/mtrr	cp /proc/mtrr	内核内存范围寄存器
	/proc/vmstat	cp /proc/vmstat	虚拟内存状态
	/proc/buddyinfo	cp /proc/buddyinfo	内存碎片信息
	/proc/cmdline	cp /proc/cmdline	内核启动的命令行
	/proc/devices	cp /proc/devices	设备驱动程序
	/proc/diskstats	cp /proc/diskstats	硬盘状态
	/proc/iomem	cp /proc/iomem	物理地址的分配情况
	/proc/dma	cp /proc/dma	DMA通道信息
	/boot/config*	cp /boot/config*	内核配置文件
	/etc/grub.conf	cp /etc/grub.conf	grub配置文件
	/boot/grub/device.map	cp /boot/grub/device.map	启动设备映射
	/boot/grub/menu.lst	cp /boot/menu.lst	启动菜单
	/boot/grub2/grub.cfg	cp /boot/grub2/grub.cfg	Grub2信息
	dump_list.txt	du -ah /var/crash/	crash文件清单

模块	文件名称	收集命令	文件说明
	dmesg.txt	dmesg	dmesg文件
	/root/.bash_history	cp /root/.bash_history	历史执行命令
	command_log.txt	df -lT df -Th mount /usr/bin/last -xF grep "reboot\ shutdown\ runlevel\ system"	查看剩余空间 文件系统挂载信息 挂载信息 重启纪录
		nfsstat -cnrs	NFS服务状态
		lsof	已打开文件列表
		ulimit -a	查看系统资源限制
		ipcs -a	显示进程间通信设施状态
		ipcs -l	查看共享信息的内存
		sysctl -a	sysctl设置和显示在“/proc/sys”目录中的内核参数
		uptime	已经运行时间
		uname -a	查看内核
		ps auwx	当前所有进程列表
		last	历史登录过的用户纪录
		hostid	登录用户的ID号
		/bin/rpm -qa	已经安装软件清单
		printenv	打印环境变量
		hostname	主机名信息
	filesystem_config_log.txt	cat /proc/sys/vm/dirty_ratio cat /proc/sys/vm/dirty_background_ratio cat /proc/sys/vm/dirty_writeback_centisecs	文件系统配置信息

模块	文件名称	收集命令	文件说明
		cat /proc/sys/vm/ dirty_expire_centisecs	
		cat /proc/sys/vm/ vfs_cache_pressure	
		cat /proc/sys/vm/ swappiness	
		cat blockdev -- getra /dev/sdx	
		cat /sys/block/sdx/ queue/scheduler	
		cat /sys/class/block/sdx/ device/block/sdx/queue/ nr_requests	
		cat /sys/class/block/sdx/ device/block/sdx/queue/ max_segments	
		cat /sys/class/block/sdx/ device/block/sdx/queue/ max_sectors_kb	
		cat /sys/class/block/sdx/ device/block/sdx/queue/ max_hw_sectors_kb	
		cat /sys/class/block/sdx/ device/block/sdx/queue/ hw_sector_size	
		cat /sys/class/block/sdx/ device/queue_depth	
	devinfo.txt	ls -l /dev	/dev文件夹下的详细信息
	/var/log/kern*	cp /var/log/kern*	Kern日志信息
	/var/log/ dmesg*	cp /var/log/dmesg*	Dmesg日志信息
	/var/log/ syslog*	cp /var/log/syslog*	Syslog日志信息
	/var/log/ {hostname}/ {date}/	cp -r /var/log/ {hostname}/{date}/	FusionSphere CNA 6.1系 统日志备份

模块	文件名称	收集命令	文件说明
	/var/backuplog/galaxenginelog/{date}/	cp -r /var/backuplog/galaxenginelog/{date}/	FusionSphere CNA6.3~6.5 系统日志备份
	/var/log/logdump/	cp -r /var/log/logdump	FusionSphere openstack 系统日志备份
	/var/log/logdump-{num}-{timestamp}.tar.gz	cp -r /var/log/logdump-{num}-{timestamp}.tar.gz	FusionSphere openstack 系统日志备份
	/var/crash/*/vmcore-dmesg.txt	-	系统错误信息
	dpkglist.txt	dpkg -l	Ubuntu系统安装的软件包信息
	vmstat.txt	vmstat 1 60	进程, 虚拟内存和CPU活动信息
	iostat.txt	iostat -xct 1 60	磁盘和CPU活动统计信息
	command_log.txt	ps -eo pid,lstart,cmd	等待资源的进程数
SLES	nts_{hostname}_{time}.tbz	supportconfig (SLES系统)	SLES系统定位用日志收集套件
	nts_{hostname}_{time}.tbz.md5	supportconfig (SLES系统)	SLES系统定位用日志收集套件的校验码
sosreport (需要安装sosreport软件)	sosreport-{hostname}_{time}.tar.xz	sosreport --batch 或者 sosreport -n networking --batch	RHEL、CentOS和Ubuntu系统定位用日志收集套件。(如果是RHEL 6且安装的sosreport版本低于3.3或者RHEL 7且安装的sosreport版本低于3.6, 请使用参数-n networking)

模块	文件名称	收集命令	文件说明
	sosreport-\$ (hostname)_\$ (time).tar.xz.m d5	sosreport --batch 或者 sosreport -n networking --batch	RHEL、CentOS和Ubuntu 系统定位用日志收集套件 的校验码。（如果是 RHEL 6且安装的 sosreport版本低于3.3或 者RHEL 7且安装的 sosreport版本低于3.6， 请使用参数-n networking）
hpc	opainfo_log.txt	opainfo	网络端口的连接状态
	opareport-v_log.txt	opareport -v	节点端口信息
	opareport-slowlinks_log.txt	opareport -o slowlinks	端口速率问题
	opareport-errors_log.txt	opareport -o errors	网口error统计数
	opareport-linear_log.txt	opareport -o linear	路由情况
	opasaquery-swinfo_log.txt	opasaquery -o swinfo	交换机信息
	opahfirev_log.txt	opahfirev	网卡SN、PCIE号等硬件信 息
	opasaquery-nodeinfo_log.txt	opasaquery -o node	节点详细信息
	ibstat_log.txt	ibstat	IB/OPA 网络设备的基本 状态
atlas	dlog/	cp /var/dlog	Atlas NPU日志
	/tmp/atlas300_smartkit.log	cp /tmp/atlas300_smartkit.log	Atlas300 OS巡检脚本执 行日志。
	ascend-dmi.txt	ascend-dmi -v ascend-dmi -i -dt ascend-dmi -topo ascend-dmi -c	Atlas NPU相关信息
	ascend-log-collect.tar.gz	ascend-dmi -c	Ascend日志收集

模块	文件名称	收集命令	文件说明
hiarm	hiarm_log_xxx.tar.gz	hiarm_log_collect.sh -a -p -l /tmp -z {log_dir}	Hi1620芯片日志及其它相关日志
block	blk_list.txt	lsblk	列出块设备
	blk_list.txt	lsblk -t	列出块设备的拓扑
	blk_list.txt	fdisk -l	列出所有块设备的分区信息(Legacy)
	initramfs.txt	lsinitrd	显示initramfs镜像的内容
	file_directory.txt	ls -lanR /boot	列出/boot目录以及子目录的文件
cgroups	/proc/cgroups	/proc/cgroups	显示当前内核支持的cgroup子系统以及是否使能
	/sys/fs/cgroup	/sys/fs/cgroup	收集所有cgroup文件系统的文件
	cgroup.txt	systemd-cgls --no-pager	递归显示 cgroup 的内容
cron	scheduled_tasks.txt	crontab -l -u <user>	列出user用户设定的定时任务
	/etc/cron.monthly	/etc/cron.monthly	每月运行一次的定时任务配置目录
	/etc/cron.weekly	/etc/cron.weekly	每周运行一次的定时任务配置目录
	/etc/cron.daily	/etc/cron.daily	每天运行一次的定时任务配置目录
	/etc/cron.hourly	/etc/cron.hourly	每小时运行一次的定时任务配置目录
	/etc/cron.d	/etc/cron.d	定时任务配置目录
	/etc/crontab	/etc/crontab	系统级定时任务，使用root权限执行
grub2	grub2.txt	grub2-mkconfig	导出当前的grub配置文件
hardware	udevadm.txt	udevadm info -e	导出udev数据库的内容
	/proc/irq	/proc/irq	每个中断的单独的信息
kernel	kpatch_list.txt	kpatch list	列出所有已安装的内核热补丁模块
last	OS_restart_info.txt	last reboot	最近一次OS重启的记录

模块	文件名称	收集命令	文件说明
	OS_shutdown_info.txt	last shutdown	最近一次OS关机的记录
sar	/var/log/sa	/var/log/sa	sa日志，用来分析性能问题
scsi	scsi_info.txt	lsscsi	列出scsi设备以及其属性
	scsi_sg_mapping.txt	sg_map -x	列出sg设备和scsi设备的映射关系
cyclicCollection	memory_free.txt	free	查看耗用和剩余的内存
	ifconfig.txt	ifconfig -a	所有网卡配置
	ethtool.txt	ethtool ethX	网卡的设置
		ethtool -i ethX	
		ethtool -S ethX	
		ethtool -g ethX	
		ethtool -k ethX	
	netstat.txt	netstat -i -n	网络端口状态
		netstat -avn	
		netstat -s	
		netstat -rvn	
	stat.txt	cat /proc/stat	系统状态
	routeInfo.txt	route -n	路由信息
	iptablesInfo.txt	iptables -t filter -nvL	iptables信息
	trafficControl.txt	tc -s qdisc	流量控制排队规则
	command_log.txt	sysctl -a	内核信息
	network_adapter_numa_node.txt	cat /sys/class/net/\${netname}/device/numa_node	网卡numa节点信息
	network_script.txt	ls /etc/sysconfig/network-scripts/ cat /etc/sysconfig/network-scripts/\${netname}	网络脚本信息

模块	文件名称	收集命令	文件说明
	interrupts.txt	cat /proc/interrupts	系统中断信息
gpu	nvidia-smi.txt	nvidia-smi -q	nvidia smi信息
	nvidia-installer.log	cp -rf /var/log/nvidia-installer.log	nvidia安装程序日志
	nvidia-uninstall.log	cp -rf /var/log/nvidia-uninstall.log	nvidia卸载日志
	Xorg.*.log	cp -rf /var/log/Xorg.*.log	Xorg日志
trustZone	/var/log/tee/*	/var/log/tee/*	TrustZone日志

说明

- 不同Linux操作系统，收集到的日志文件数量和内容会略有不同，但都在[表4-29](#)范围内。
- 工具依赖大量的系统的命令，如ipmitool、smartctl等，若系统未安装对应的软件，将无法搜集到对应日志文件。
- bash_history**会收集历史命令信息（对维护定位问题有帮助），请谨慎收集，可通过修改“config.ini”配置文件不收集，也可收集后手工删除该文件后再压缩打包。
- sosreport**和**supportconfig**命令是操作系统自带日志收集命令，收集的日志用于深层次问题定位分析，请谨慎收集，可通过修改“config.ini”配置文件不收集，也可收集后手工删除该文件后再压缩打包。
- 用户可通过编辑工具目录下的“config.ini”文件定制化日志收集的内容。
- “mezz_info.tar.gz”为OSCA要求的网卡信息，虽有重复收集，但方便OSCA操作。
- 收集trustZone日志前，请先开启trustZone特性以及执行日志生成指令tlogcat -f。具体操作方法请参考《Kunpeng BoostKit 21.0.0 机密计算TrustZone套件 特性指南》中的“TA/CA应用运行环境搭建”。

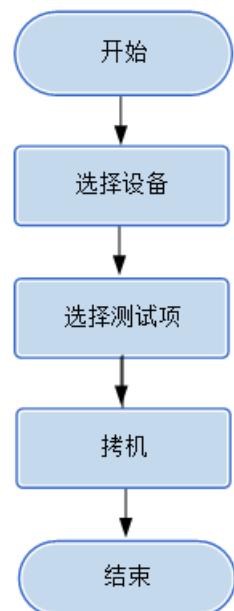
4.8 拷机

本节主要指导用户使用拷机功能对服务器的CPU、内存、硬盘进行性能测试。

4.8.1 拷机流程

拷机流程如[图4-57](#)所示。

图 4-57 拷机



4.8.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

- PC机和待操作的服务器BMC网络相通，保证SNMP、IPMI、SSH/SFTP、VMM、HTTPS通信端口连通，保证能ping通服务器BMC的IP地址。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

4.8.3 选择设备

在拷机向导的“选择设备”界面中，可以选择需要进行拷机的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“服务器>故障处理>拷机”。

系统进入“拷机”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要拷机的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明书

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如表4-30所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考表4-30，手工输入参数。

表 4-30 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务 BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和 IPv6。
	结束IP	搜索的结束服务 器BMC的IP地址。	<ul style="list-style-type: none">单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: fc00::1 结束 IP: fc00::1多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: fc00::1 结束 IP: fc00::6多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。BMC的IP地址，此处IP地址支持IPv4和 IPv6。
	用户名	BMC管理员用户名。	-
	密码	BMC管理员密码。	-

类型	名称	说明	备注
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	默认值是8208，以设备实际启用的端口号为准。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要拷机的设备。单击“确定”，返回向导界面。

----结束

4.8.4 拷机

在拷机界面中，可以对所选择的设备进行拷机测试。

□ 说明

- 建议先尝试拷机一台服务器，待没有问题后，再进行批量拷机，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 拷机不支持外接存储设备。
- 如果使用服务器自带的SmartProvisioning进行拷机，请确保BIOS配置中SP Boot配置项为Enabled状态。

须知

- 拷机过程中，手动对服务器进行系统上下电及重启等操作会导致拷机流程被中断，请谨慎操作。
- 拷机操作“设置测试项”后须自动重启系统才能使功能生效，执行前请确保服务器上业务都已停止。

操作步骤

步骤1 在拷机向导界面单击“拷机”。

系统进入拷机向导“欢迎”界面，查看可以执行的拷机测试项，如图4-58所示。

图 4-58 欢迎



步骤2 单击“下一步”。

进入“获取设备信息”界面，如图4-59所示。

图 4-59 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤3 在设备列表中勾选一台或者多台设备进行拷机。

步骤4 单击“下一步”。

进入发现服务器界面。

说明

单击“停止”可终止此次任务。

步骤5 发现服务器后系统自动进入选择服务器界面。

说明

- 如果查询到服务器版本为None，则说明Smart Provisioning没有正确安装，请先安装Smart Provisioning。
- 如果查询到Smart Provisioning版本为空值，请检查相关依赖软件版本。如：要求BMC须使用2.64及以上版本，BIOS须使用0.37及以上版本。

步骤6 单击“过滤设备”下拉框，可对发现的服务器进行筛选，快速选择需要进行操作的一类服务器。

步骤7 勾选需要进行拷机的服务器，单击“下一步”。

进入“设置测试项”界面。

- S920服务器拷机测试，请参见[4.8.4.1 S920服务器拷机测试](#)。

- S916服务器拷机测试, 请参见[4.8.4.2 S916服务器拷机测试](#)。

----结束

4.8.4.1 S920 服务器拷机测试

步骤1 S920服务器拷机测试, 如图4-60所示。参数说明请参见表4-31。

图 4-60 S920 服务器设置测试项

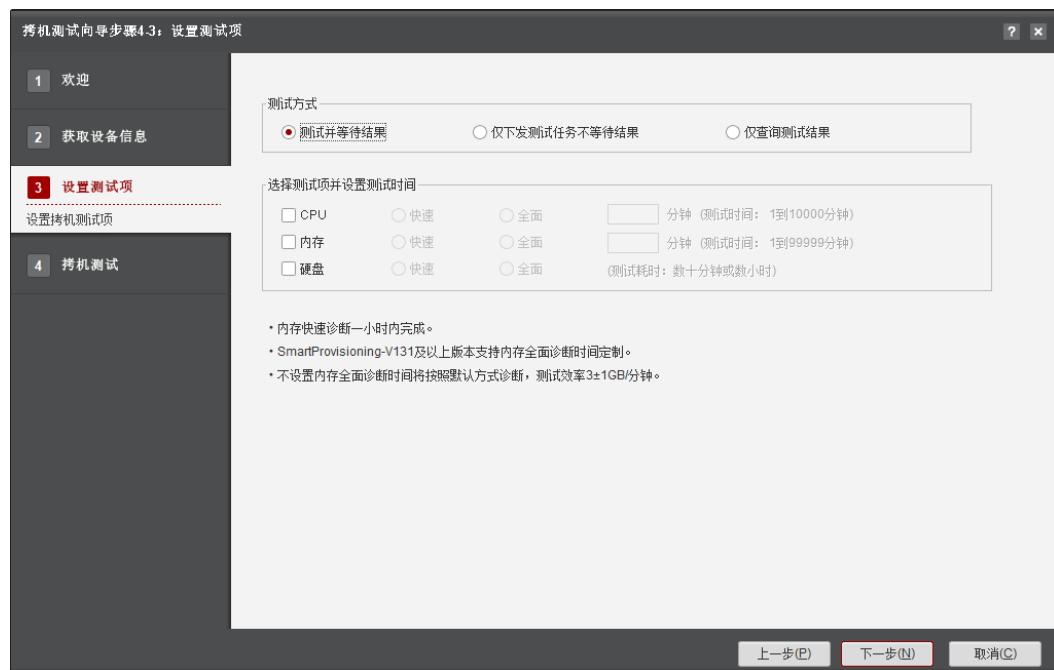


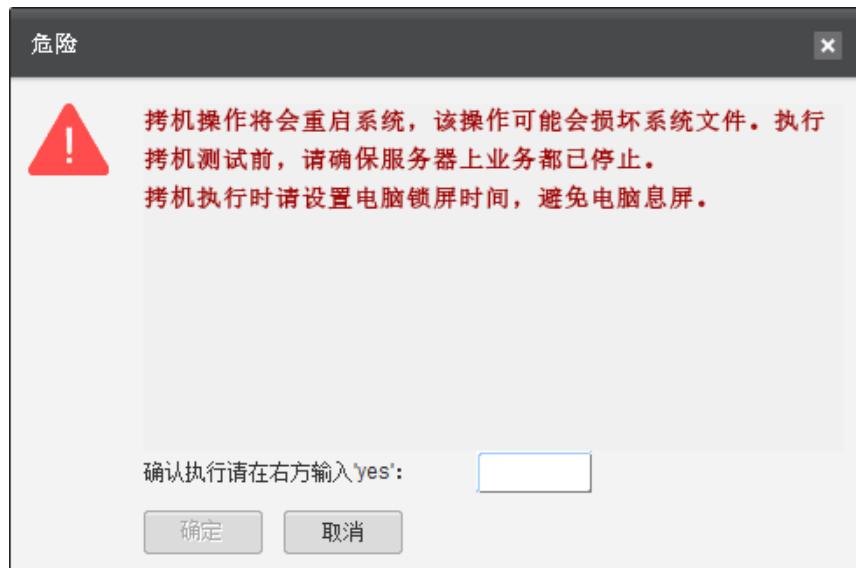
表 4-31 拷机模式说明

测试项	快速模式	全面模式	备注
CPU	执行CPU压力测试, 适合短时间测试场景。	执行CPU压力测试, 适合长时间测试场景。	测试时间: 1到10000分钟。
内存	执行算法简单的内存压力测试, 执行时间快, 包括ECC, UCNA和重传错误的检查。	执行算法复杂的内存压力测试, 执行时间慢, 更容易发现内存的错误, 包括ECC, UCNA和重传错误的检查。	测试效率: 快速诊断1小时内完成, 全量诊断3±1GB/分钟
硬盘	利用硬盘SMART的短自检程序, 诊断时间短, 适用于快速确认磁盘是否故障的场景。	利用硬盘SMART的长自检程序, 深度诊断时间较长, 测试内容和快速诊断一致, 一般先执行快速诊断, 诊断发现问题再使用深度诊断。	测试时间: 数十分钟或数小时。

步骤2 根据需求配置任务。

- 测试并等待结果, 请参见[勾选“测试并等待结果”](#)。
- 仅下发测试任务不等待结果, 请参见[勾选“仅下发测试任务不等待结果”](#)。
- 仅查询测试结果, 请参见[勾选“仅查询测试结果”](#)。
 - 勾选“测试并等待结果”。
 - 选择测试项和测试模式, 测试项包括CPU、内存、硬盘。参数说明请参见[表4-31](#)。
 - 单击“下一步”。弹出危险提示框, 如[图4-61](#)所示。

图 4-61 提示框



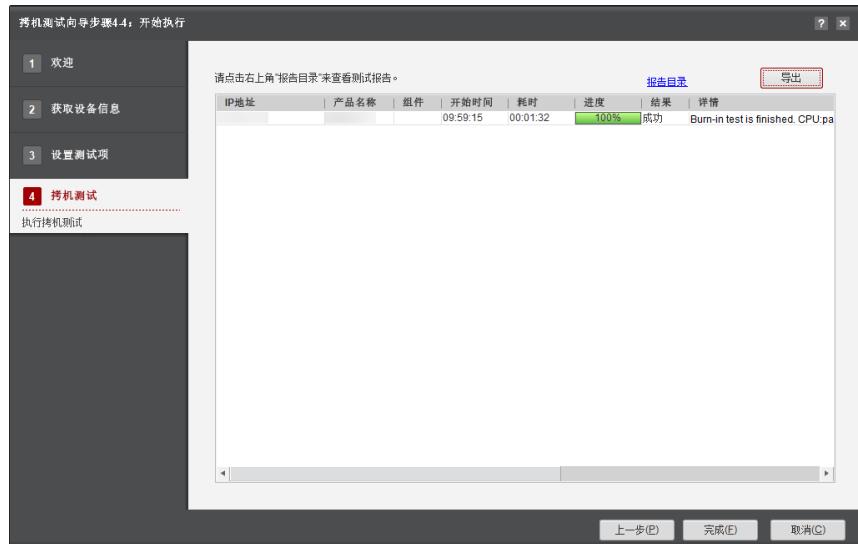
- iii. 如果已关闭服务器业务, 则在输入框中输入“yes”后单击“确定”。系统进入“拷机测试”界面, 拷机任务开始执行。

说明

拷机需要的总时间为前面设置的各项拷机时间之和。

- iv. 当进度条到100%时表示拷机完成, 如[图4-65](#)所示。
单击“完成”退出, 向导界面显示设备执行结果, 成功/失败/未执行的台数、以及总用时。

图 4-62 拷机测试



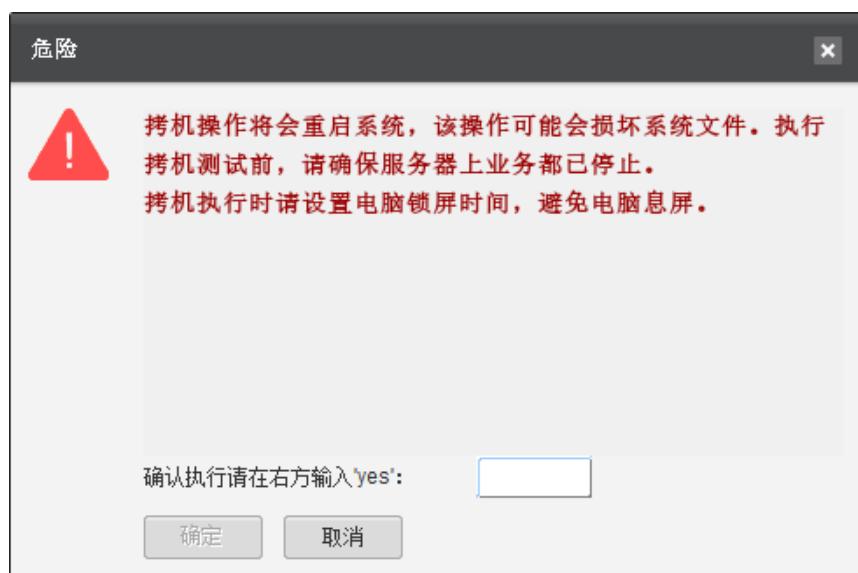
□ 说明

- 详情栏的“Disk(2/2: pass)”表示拷机成功（2/2分别表示拷机成功2个硬盘/系统内查到2个硬盘/通过BMC查到2个硬盘），若拷机结果为“failed”或者“unknown”时请通过拷机报告来查找具体原因。
- 单击右上角的“导出”，可将拷机报告导出至本地。
- 单击右上角的“报告目录”可进入拷机结果报告所在目录。

- 勾选“仅下发测试任务不等待结果”。

- i. 选择测试项和测试模式，测试项包括CPU、内存、硬盘。参数说明请参见[表4-31](#)。
- ii. 单击“下一步”。弹出危险提示框，如[图4-63所示](#)。

图 4-63 提示框



- iii. 如果已关闭服务器业务，则在输入框中输入“yes”后单击“确定”。

系统进入“拷机测试”界面，拷机任务开始执行。

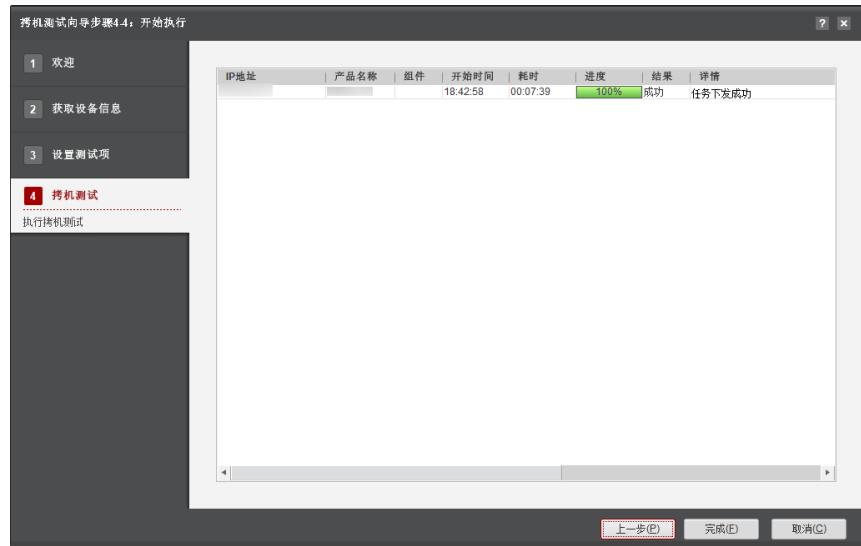
□ 说明

拷机需要的总时间为前面设置的各项拷机时间之和。

iv. 当进度条到100%时表示下发任务成功，如图4-64所示。

单击“完成”退出，向导界面显示设备执行结果，成功/失败/未执行的台数、以及总用时。

图 4-64 拷机测试



- 勾选“仅查询测试结果”。
 - 单击“下一步”，系统进入“开始执行”界面，拷机任务开始执行。

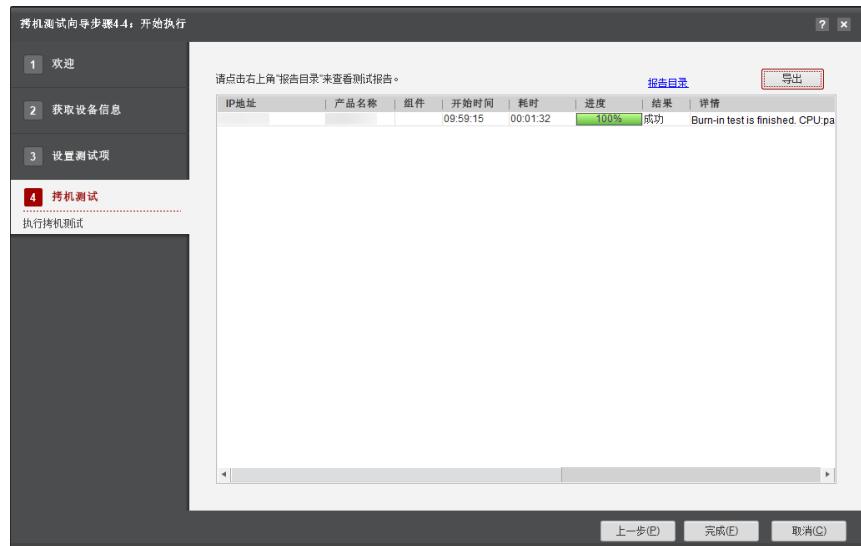
□ 说明

拷机需要的总时间为前面设置的各项拷机时间之和。

ii. 当进度条到100%时表示拷机完成，如图4-65所示。

单击“完成”退出，向导界面显示设备执行结果，成功/失败/未执行的台数、以及总用时。

图 4-65 开始执行



□ 说明

- 详情栏的“Disk(2/2/2: pass)”表示拷机成功（2/2/2分别表示拷机成功2个硬盘/系统内查到2个硬盘/通过BMC查到2个硬盘），若拷机结果为“failed”或者“unknown”时请通过拷机报告来查找具体原因。
- 单击右上角的“导出”，可将拷机报告导出至本地。
- 单击右上角的“报告目录”可进入拷机结果报告所在目录。

----结束

4.8.4.2 S916 服务器拷机测试

步骤1 S916服务器拷机测试，如图4-66所示。

图 4-66 S916 服务器设置测试项



说明

支持SmartProvisioning-V129/1.2.0.4及以上版本。

选择“SmartProvisioning iso文件”有以下两种方式：

1. 通过“选择文件”界面，手动导入“SmartProvisioning iso文件”。
 - a. 将下载的"SmartProvisioning"工具包解压至本地文件夹内。
 - b. 在“SmartProvisioning iso文件”所在行单击“选择”，选择本地的“SmartProvisioning.iso”文件。
2. 通过工具首页“服务器>功能管理>导入”的方式，直接导入已下载的"SmartProvisioning.zip"工具包。

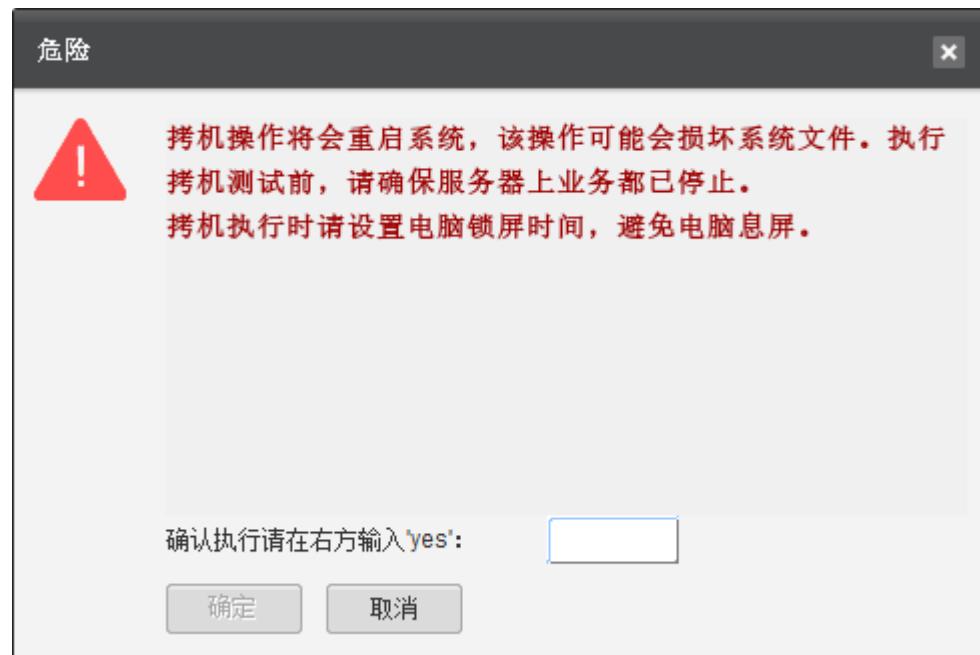
说明

通过这种方式导入工具包，工具运行到“选择文件”界面，“SmartProvisioning iso文件”会自动默认选中。

步骤2 单击“下一步”。

弹出危险提示框，如图4-67所示。

图 4-67 提示框



步骤3 如果已关闭服务器业务, 则在输入框中输入“yes”后单击“确定”。

系统进入“开始执行”界面, 拷机任务开始执行。

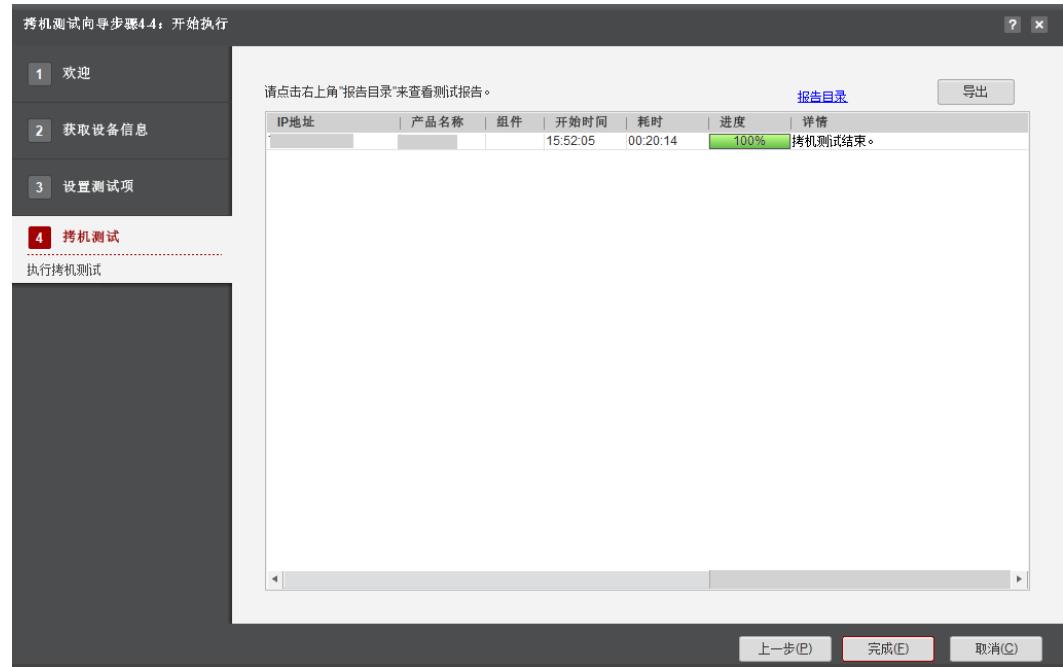
说明

拷机需要的总时间为前面设置的各项拷机时间之和。

步骤4 当进度条到100%时表示拷机完成, 如图4-68所示。

单击“完成”退出, 向导界面显示设备执行结果, 成功/失败/未执行的台数、以及总用时。

图 4-68 开始执行



□ 说明

- 单击右上角的“导出”，可将拷机报告导出至本地。
- 单击右上角的“报告目录”可进入拷机结果报告所在目录。

----结束

4.9 固件升级

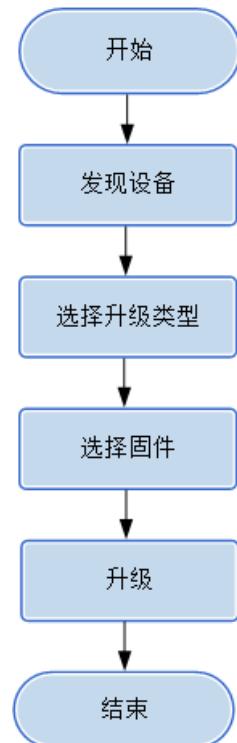
4.9.1 升级固件

本节指导用户使用工具箱对BMC、BIOS、CPLD、SP固件进行升级操作。

4.9.1.1 固件升级流程

升级服务器固件流程如图4-69所示。

图 4-69 固件升级



4.9.1.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH、HTTPS通信端口连通，保证能ping通服务器BMC的IP地址。

确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC的IP地址。
- 服务器BMC用户名和密码。

软件

- 在官网下载服务器BMC、BIOS、CPLD、PSU、CDR、Retimer固件（“.zip”格式）和对应的签名文件（“.p7s”格式）。
- 在官网下载Smart Provisioning软件包。

4.9.1.3 选择设备

在升级固件的“选择设备”界面中，可以选择需要进行升级固件的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“升级/补丁>固件升级”。

系统进入“固件升级”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要升级固件的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

□ 说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-32](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-32](#)，手工输入参数。

表 4-32 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4: 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6: 起始 IP: fc00::1 结束 IP: fc00::1 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4: 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6: 起始 IP: fc00::1 结束 IP: fc00::6 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	管理员用户名。	-
	密码	管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级 设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/ SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	请忽略该参数，或者保持默认值。。
	HTTPS端口	HTTPS端口号。	默认值是443，以设备实际启用的端口号为准。

类型	名称	说明	备注
OS 选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要固件升级的设备。单击“确定”，返回向导界面。

----结束

4.9.1.4 升级服务器固件

4.9.1.4.1 单部件升级服务器固件

在固件升级界面中，可以对所选择的设备使用单部件升级服务器的BMC、BIOS、CPLD、PSU、CDR、Retimer固件等。

□ 说明

- 建议先尝试升级一台服务器，待没有问题后，再进行批量升级，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 如对软件包版本无特殊要求，建议使用最新配套版本。
- 操作过程中遇到的问题请参考[4.9.1.5 常见问题处理](#)解决。
- 若发现服务器失败或者上传文件失败，请复位BMC后再重新进行升级。

须知

- 固件升级前，请检查是否配置了功率封顶，若进行了配置，请确保当功率封顶失败时不会对业务造成影响。
- 升级服务器固件和操作服务器电源可能影响业务，请确保关闭业务后再进行操作。
- 升级服务器固件过程中，请勿进行系统上下电、复位和复位BMC以及插拔单板等操作。
- 升级BIOS或者CPLD时，如果需要立即生效，建议升级前先在系统下正常关机，因为升级生效会执行强制系统下电再上电。
- BIOS和CPLD均需要升级时，请务必先升级BIOS且升级生效后再升级CPLD，否则可能导致BIOS升级失败，系统异常。
- 系统复位（PowerReset）、系统下电再上电（PowerOffThenOn）属于强制系统操作，可能会损坏操作系统文件，请谨慎操作。

步骤1 在固件升级向导界面单击“固件升级”。

系统弹出“升级固件、升级PCIe卡/硬盘固件”选择框。

步骤2 单击“升级固件”。

系统进入固件升级向导“欢迎”界面，查看可以升级的固件类型，如图4-70所示。

图 4-70 欢迎



步骤3 单击“下一步”。

进入“获取设备信息”界面，如图4-71所示。

图 4-71 获取设备信息



□ 说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。
- 设置并发数超过20时，会弹出若并发数过高可能导致工具运行效率变低系统卡顿，日志收集因为命令执行超时而失败的弹框。请确认后再操作。

步骤4 在设备列表中勾选一台或者多台需要固件升级的设备。

步骤5 单击“下一步”。

执行发现服务器操作。

□ 说明

单击“停止”可终止此次任务。

步骤6 成功发现服务器后系统自动进入“选择升级类型”界面。选择“单部件升级”，如图4-72所示。

单击“下一步”。进入“选择固件”界面。

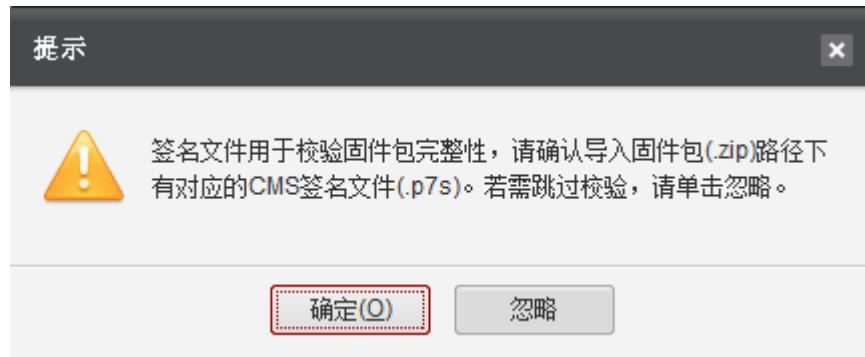
图 4-72 选择升级类型



步骤7 在“升级固件”页签中单击“选择”，弹出“签名文件用于校验固件包完整性，请确认导入固件包(zip)路径下有对应的CMS签名文件(.p7s)。若需跳过校验，请单击忽略。”提示，如图4-73所示。

- 确认导入固件包路径下有对应的签名文件，请单击“确定”。
- 如需跳过签名文件校验，请单击“忽略”。

图 4-73 提示

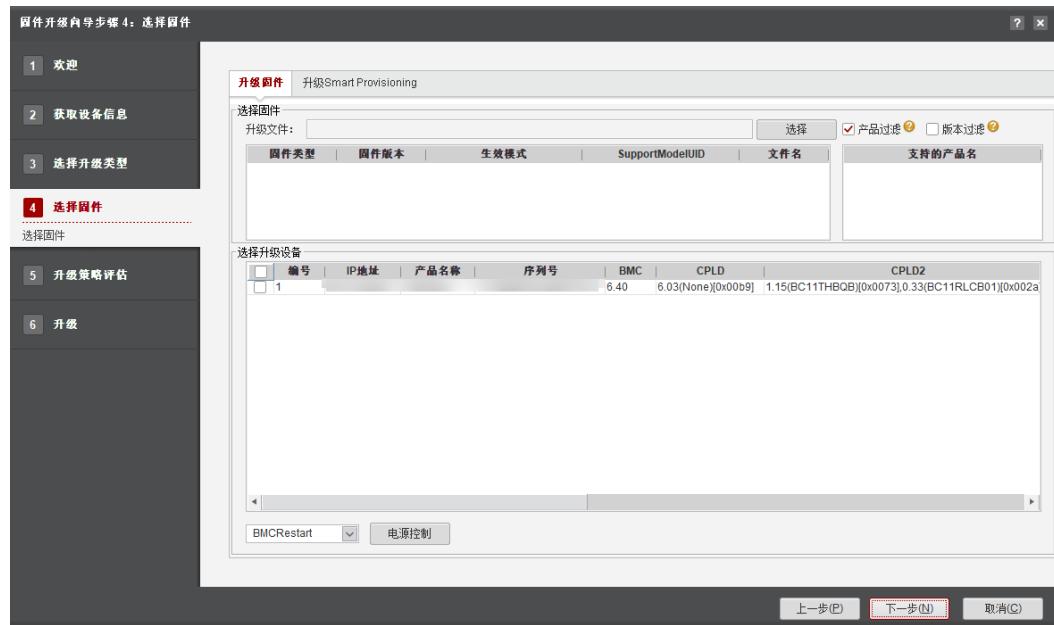


说明

如果导入的是.hpm格式升级文件，无需验证签名文件。

步骤8 选择本地的升级软件包，如图4-74所示。

图 4-74 升级固件



说明

- 如果勾选了右上角的“产品过滤”，将会过滤掉与导入固件包不匹配的服务器，若取消勾选，则强制升级。
- 如果勾选了右上角的“版本过滤”，将会过滤掉固件版本与待升级版本相同的服务器。“版本过滤”复选框只有在选中“产品过滤”复选框时才生效。
- 选择“.zip”格式的升级文件（建议使用此种升级文件）。
系统会解析软件包里的“version.xml”文件，并将解析内容展示到升级文件列表以及支持的服务器名称列表中。
- 如果无法导入.zip包，请解压.zip包，选择“.hpm”格式的升级文件（仅针对老版本的固件包可能会存在此种情况）。

- a. 系统弹出“配置升级文件”界面。
- b. 参考**表4-33**输入升级文件的相关信息，单击“确认”。

升级文件里的内容会展示到升级文件列表以及支持的服务器名称列表中。

表 4-33 升级文件信息

名称	说明	备注
文件名	升级文件名称。	不可修改。
模块	固件升级的类型：BMC、BIOS、CPLD、PSU、CDR、Retimer固件等。	-
版本	固件的版本号。	用于版本过滤。
生效模式	生效模式，分为如下几种： <ul style="list-style-type: none"> ▪ Immediately：实时生效 ▪ ResetBMC：复位BMC后生效 ▪ ResetOS：复位系统后生效 ▪ ResetServer：系统先下电再上电后生效 	<ul style="list-style-type: none"> ▪ 升级BMC选择“ResetBMC” ▪ 升级BIOS选择“ResetOS” ▪ 升级主板CPLD选择“ResetServer”

步骤9 单击“下一步”。

进入“升级策略评估”界面，如**图4-75**所示。

图 4-75 升级策略评估



1. 勾选需要评估升级策略的设备。
2. 单击“评估”。
3. 在“评估结果”列显示评估的结果。

说明

- 评估结果如：通过/不通过/不支持评估/未评估。
- 单击“导出报告”，可将升级策略评估结果报告导出至本地。
- 单击“导入”，可导入评估规则文件。
- 下方展示设备信息、各固件类型当前版本和目标版本信息、评估结果及建议详情。
- 当未进行评估或评估不通过时，单击“下一步”，弹出相应警告框。请确认风险操作及影响。

步骤10 单击“下一步”。

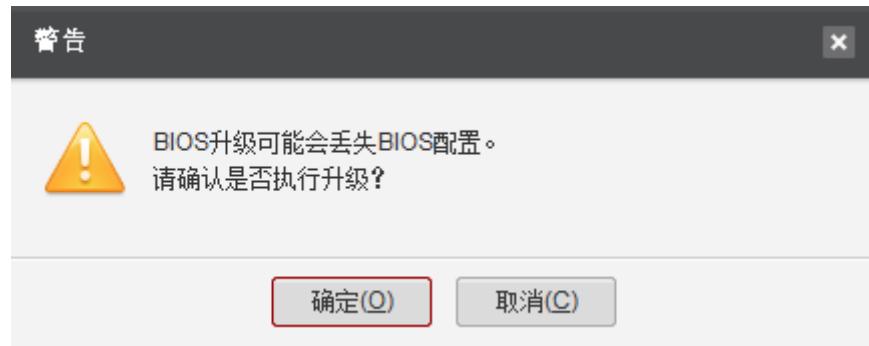
说明

当所勾选的设备看门狗状态异常时，会弹出“如下设备看门狗为开启状态，并且超时动作作为Hard Reset, Power Cycle, Power Down中的一种，可能导致服务器异常掉电或重启，请参考4.9.1.5.1 操作系统侧的看门狗异常问题，修复后重新获取设备信息”提示框。请根据实际情况，选择是否勾选“我已同意工具自动修改看门狗的超时动作作为No Action，并在升级完成后恢复初始超时动作”。

- 如果升级BIOS、CPLD、CDR或Retimer。
- 1. (仅升级BIOS时存在此步骤)，弹出“BIOS升级可能会丢失BIOS配置”提示框。如图4-76所示。

单击“确定”，继续升级；否则，单击“取消”，取消升级。

图 4-76 警告



2. 弹出“固件需要重启后才能生效，请选择：”。如图4-77所示。

图 4-77 警告提示



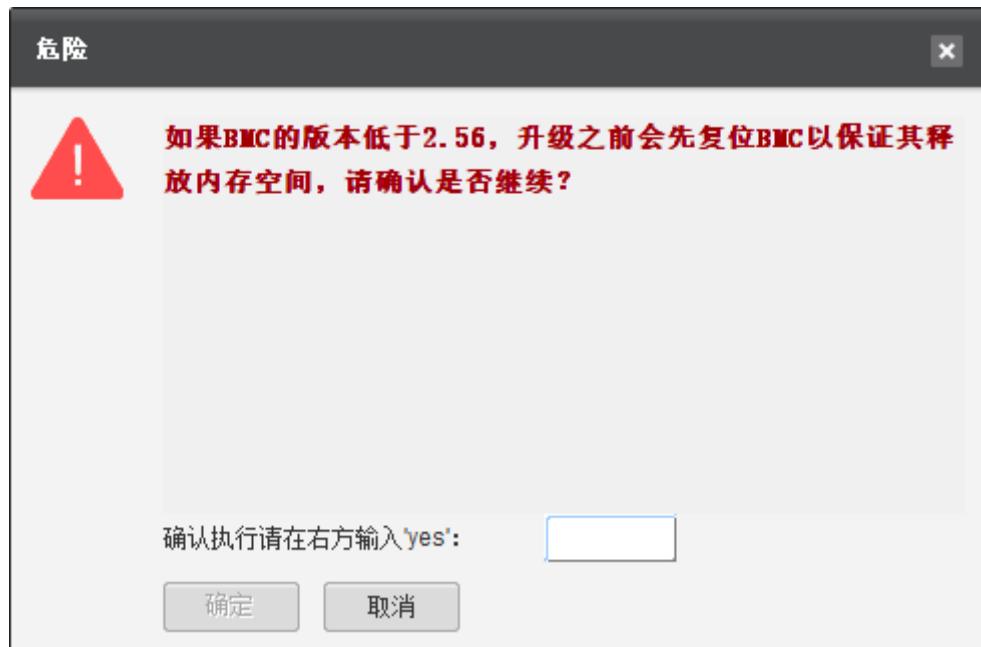
- 如果选择“仅加载固件，用户稍后自行重启生效（CPLD升级需要设备下电再上电）”，如果升级CPLD，则需要将CPLD先下电再上电，其他模块则自行重启服务器生效。

须知

升级前，请先确保服务器上不存在其他预埋任务，否者可能导致升级失败。

- 如果选择“安全下电再上电生效（业务中断）”，则服务器自动重启。
单击“确定”，继续升级；否则，单击“取消”，取消升级。
- 3. 如果选择继续升级，则弹出“如果BMC版本低于2.56，升级之前会先复位BMC以保证其释放内存空间，请确认是否继续？”提示框。如图4-78所示。
确认BMC版本不低于2.56或者设备允许重启BMC，则输入“yes”，单击“确定”，继续升级，否则单击“取消”。

图 4-78 危险提示



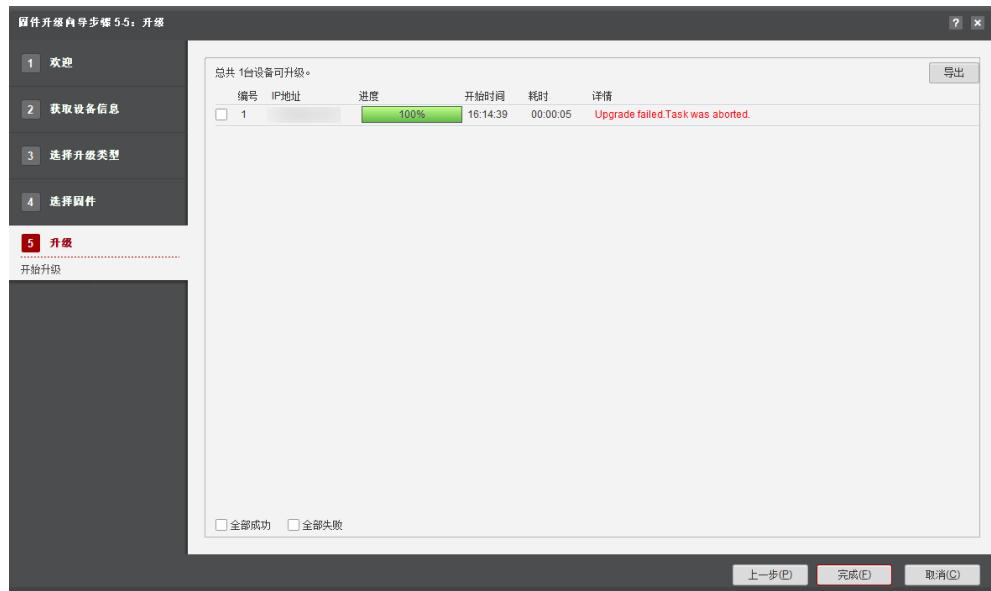
- 4. 若升级BMC，弹出“要保证BMC主备版本一致，请在升级完成界面点击“再次升级”。”提示框。单击“确定”，或  按钮。
工具自动跳转升级页面。具自动跳转升级页面。如图4-79所示。

图 4-79 提示



查看升级进度，如图4-80所示，当“进度”为100%时表示升级成功。

图 4-80 升级



说明

- 单击“停止”按钮，可终止此次升级任务。升级过程中，停止升级可能会导致设备处于异常状态，请谨慎操作。部分已经向设备下发升级命令的任务，无法停止。
- 勾选“全部成功”可查看所有升级成功的服务器。
- 勾选“全部失败”可查看所有升级失败的服务器。
- 仅在升级BMC时，工具升级界面右下角会显示“再次升级”的按钮。
- 使用单部件升级BMC时，进度条卡在90%，提示：Upgrade finished, But the version check failed, Currentversion: *****时，请单击“再次升级”按钮，确保升级成功。

步骤11 单击“完成”，完成升级。

若用户之前选择手动重启服务器生效固件，单击“上一步”，进入“选择固件”界面。

1. 确认操作系统业务允许中断的情况下，参考表4-34，在左下角电源控制下拉列表中，选择“Poweroff”，点击“电源控制”。

弹出“请确认是否要进行”提示框，请确认。

表 4-34 电源控制类型

电源控制操作	说明
BMCRestart	复位BMC
PowerOff	正常系统下电
PowerOn	正常系统上电
PowerReset	强制系统复位
PowerOffThenOn	强制系统先下电再上电

□ 说明

PowerReset和PowerOffThenOn可能损坏操作系统文件，请谨慎操作。

2. 系统下电完成后，点击“上一步”，参考步骤1，进行“PowerOn”操作。
电源控制完成后系统自动进入电源控制结果界面。

□ 说明

- 单击“导出”可将电源控制结果保存至本地（默认保存“.xls”格式）。
- 单击“日志目录”可进入电源控制结果“powerOutput.xml”的保存目录“根目录\tools\ServerMain\work\FWUpgrade\日期+时间+编号\日期+时间+编号”，如“根目录\tools\ServerMain\work\FWUpgrade\20181205143333\20181205151345”。

----结束

4.9.1.4.2 多部件升级服务器固件

在固件升级界面中，可以对所选择的设备使用多部件升级服务器的BMC、BIOS、CPLD、PSU、CDR、Retimer固件等。

□ 说明

- 建议先尝试升级一台服务器，待没有问题后，再进行批量升级，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 如对软件包版本无特殊要求，建议使用最新配套版本。
- 操作过程中遇到的问题请参考4.9.1.5 常见问题处理解决。
- 若发现服务器失败或者上传文件失败，请复位BMC后再重新进行升级。

须知

- 固件升级前, 请检查是否配置了功率封顶, 若进行了配置, 请确保当功率封顶失败时不会对业务造成影响。
- 升级服务器BIOS或者CPLD需重启系统生效, 会影响操作系统业务, 请确保关闭业务后再进行操作。
- 升级服务器固件过程中, 请勿进行系统上下电、复位以及复位BMC等操作。
- 系统复位 (PowerReset)、系统下电再上电 (PowerOffThenOn) 属于强制系统操作, 可能会损坏操作系统文件, 请谨慎操作。

操作步骤

步骤1 在固件升级向导界面单击“固件升级”。

系统弹出“升级固件、升级PCIe卡/硬盘固件”选择框。

步骤2 单击“升级固件”。

系统进入固件升级向导“欢迎”界面, 查看可以升级的固件类型, 如图4-81所示。

图 4-81 欢迎



步骤3 单击“下一步”。

进入“获取设备信息”界面, 如图4-82所示。

图 4-82 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。
- 设置并发数超过20时，会弹出若并发数过高可能导致工具运行效率变低系统卡顿，日志收集因为命令执行超时而失败的弹框。请确认后再操作。

步骤4 在设备列表中勾选一台或者多台需要固件升级的设备。

步骤5 单击“下一步”。

执行发现服务器操作。

说明

单击“停止”可终止此次任务。

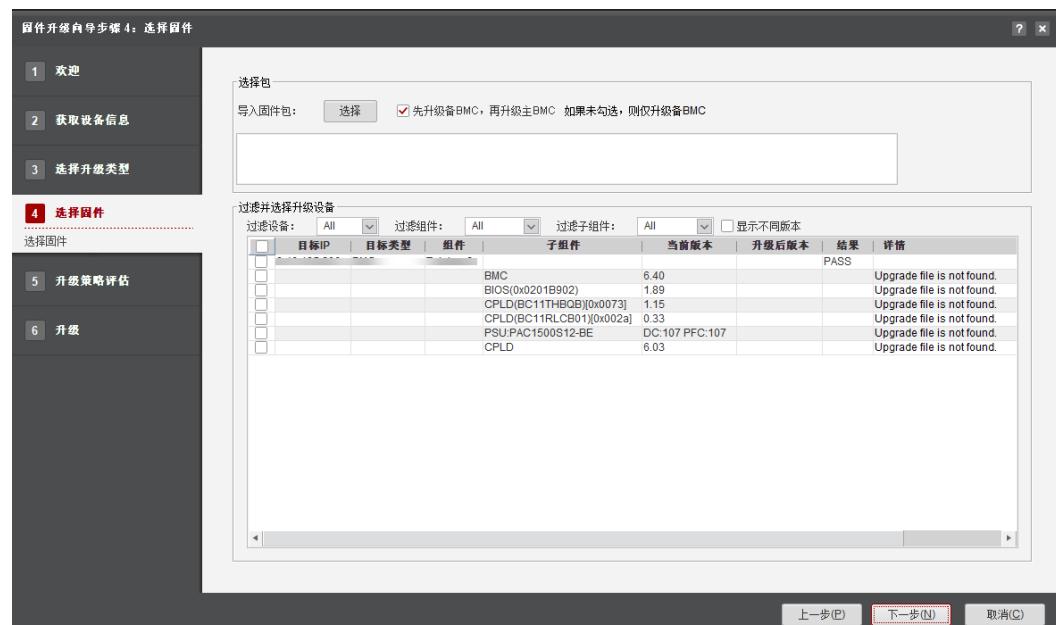
步骤6 成功发现服务器后系统自动进入“选择升级类型”界面。选择“多部件升级”，如图4-83所示。

图 4-83 选择升级类型



步骤7 单击“下一步”，进入“选择固件”界面，如图4-84所示。

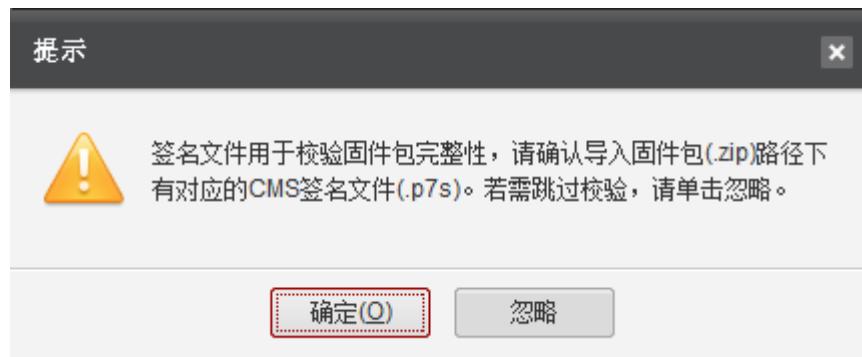
图 4-84 选择固件



步骤8 在“导入固件包”处单击“选择”，弹出“签名文件用于校验固件包完整性，请确认导入固件包(.zip)路径下有对应的CMS签名文件(.p7s)。若需跳过校验，请单击忽略。”提示，如图4-85所示。

- 确认导入固件包路径下有对应的签名文件，请单击“确定”。
- 如需跳过签名文件校验，请单击“忽略”。

图 4-85 提示



步骤9 选择本地的升级包。

导入完成后, 会弹出“固件升级包导入成功”提示框。

□□ 说明

如果需要升级多个固件, 可通过同时按“shift”+鼠标点击选择多个升级包一次导入。

步骤10 单击“确认”, 关闭导入升级固件包界面。

回到“选择固件”界面, 界面出现待升级包的信息。

□□ 说明

- 勾选“先升级备BMC, 再升级主BMC”, 不勾选则只升级备BMC。
- “过滤设备”用于过滤“目标类型”列的服务器类型。
- “过滤组件”用于过滤“组件”列的服务器。
- “过滤子组件”用于过滤“子组件”列的固件类型。
- 勾选“显示不同版本”表示过滤掉与待升级版本相同的固件, 不勾选则显示全部固件。

步骤11 勾选需要进行升级的固件。

步骤12 单击“下一步”。

进入“升级策略评估”界面, 如图4-86所示。

图 4-86 升级策略评估



1. 勾选需要评估升级策略的设备。
2. 单击“评估”。
3. 在“评估结果”列显示评估的结果。

说明

- 评估结果如：通过/不通过/不支持评估/未评估。
- 单击“导出报告”，可将升级策略评估结果报告导出至本地。
- 单击“导入”，可导入评估规则文件。
- 下方展示设备信息、各固件类型当前版本和目标版本信息、评估结果及建议详情。
- 当未进行评估或评估不通过时，单击“下一步”，弹出相应警告框。请确认风险操作及影响。

步骤13 单击“下一步”。升级BIOS、CPLD、CDR或者Retimer。

说明

当所勾选的设备看门狗状态异常时，会弹出“如下设备看门狗为开启状态，并且超时动作Hard Reset, Power Cycle, Power Down中的一种，可能导致服务器异常掉电或重启，请参考**4.9.1.5.1 操作系统侧的看门狗异常问题**，修复后重新获取设备信息”提示框。请根据实际情况，选择是否勾选“我已同意工具自动修改看门狗的超时动作No Action，并在升级完成后恢复初始超时动作”。

1. 弹出“固件需要重启后才能生效，请选择：”。如图4-87所示。

图 4-87 警告



- 如果选择“仅加载固件，用户稍后自行重启生效（CPLD升级需要设备下电再上电）”，如果升级CPLD，则需要将CPLD先下电再上电，其他模块则自行重启服务器生效。

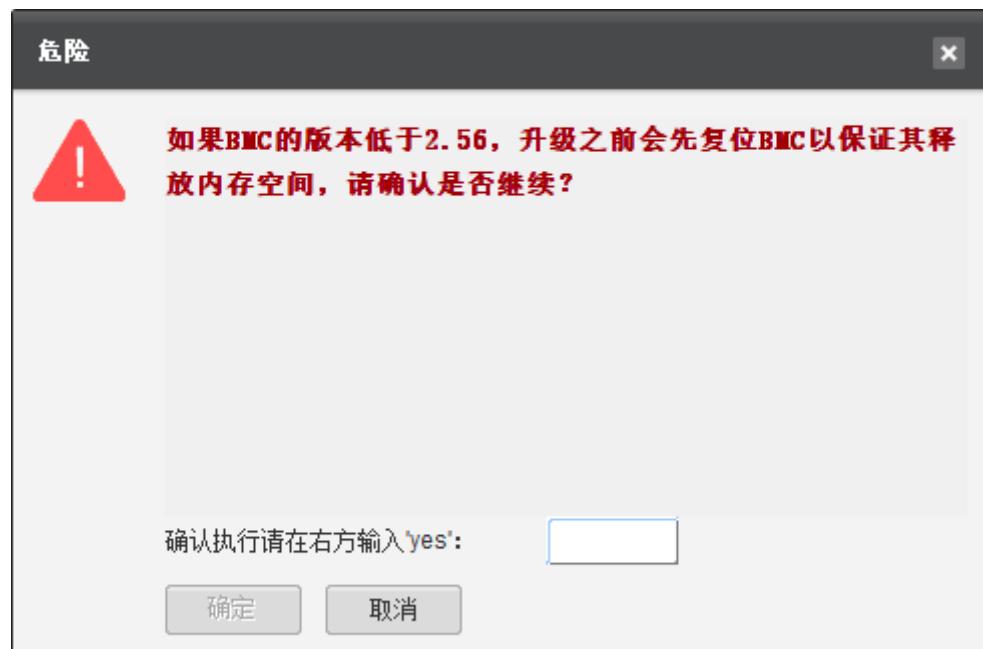
须知

升级前，请先确保服务器上不存在其他预埋任务，否者可能导致升级失败。

- 如果选择“安全下电再上电生效（业务中断）”，则服务器自动重启。
单击“确定”，继续升级；否则，单击“取消”，取消升级。

2. 如果选择继续升级，则弹出“如果BMC版本低于2.56，升级之前会先复位BMC以保证其释放内存空间，请确认是否继续？”提示框。如图4-88所示。
确认BMC版本不低于2.56或者设备允许重启BMC，则输入“yes”，单击“确定”，继续升级，否则单击“取消”。

图 4-88 危险



步骤14 查看升级进度，如图4-89所示。当“进度”为100%时表示升级成功。

图 4-89 升级



步骤15 单击“完成”退出，向导界面显示成功和未执行的服务器台数，以及总用时。

----结束

4.9.1.4.3 升级 Smart Provisioning

操作场景

在固件升级界面中，可以升级服务器的Smart Provisioning。

说明

- 建议先尝试升级一台服务器，待没有问题后，再进行批量升级，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 操作过程中遇到的问题请参考[4.9.1.5 常见问题处理](#)解决。
- 若发现服务器失败或者上传文件失败，请复位BMC后再重新进行升级。
- 在设备上电到操作系统启动期间或者Smart Provisioning启动和运行期间，不支持升级Smart Provisioning。

须知

- 升级Smart Provisioning前，请检查是否配置了功率封顶，若进行了配置，请确保当功率封顶失败时不会对业务造成影响。
- 升级Smart Provisioning可能影响业务，请确保关闭业务后再进行操作。

操作步骤

步骤1 在固件升级向导界面单击“固件升级”。

系统弹出“升级固件、升级PCIe卡/硬盘固件”选择框。

步骤2 单击“升级固件”。

系统进入固件升级向导“欢迎”界面，查看可以升级的固件类型，如图4-90所示。

图 4-90 欢迎



步骤3 单击“下一步”。

进入“获取设备信息”界面，如图4-91所示。

图 4-91 获取设备信息



□ 说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。
- 设置并发数超过20时，会弹出若并发数过高可能导致工具运行效率变低系统卡顿，日志收集因为命令执行超时而失败的弹框。请确认后再操作。

步骤4 在设备列表中勾选一台或者多台需要固件升级的设备。

步骤5 单击“下一步”。

执行发现服务器操作。

□ 说明

单击“停止”可终止此次任务。

步骤6 成功发现服务器后系统自动进入“选择升级类型”界面。选择“单部件升级”，如图4-92所示。

单击“下一步”。进入“选择固件”界面。

图 4-92 选择升级类型



步骤7 单击“升级Smart Provisioning”页签，进入升级Smart Provisioning界面，如图4-93所示。相关参数填写，请参考表4-35。

图 4-93 升级 Smart Provisioning



须知

如果协议类型选择CIFS，对应参数项填写不正确，升级时会报错：“**Upgrade Failure: The shared folder is faulty and cannot be mounted to the iBMC. Ensure that the shared folder can be accessed**”从而导致升级失败。例如：共享设备IP、用户名、密码填写错误，选择的文件路径不符合要求（文件路径下存放Smart Provisioning ISO文件的文件夹需要设置为共享，且同时要求存放Smart Provisioning ISO文件的文件夹为该路径下的第一级目录文件夹）。

说明

- 请确认服务器可以访问共享文件，Windows系统检查网络连通性命令为“**ping 服务器BMC的IP地址 -S 共享文件所在操作系统IP地址**”。
- SP升级使用cifs/nfs服务搭建方法，请参考[4.9.1.5.3 sp升级使用cifs/nfs服务搭建方法](#)。
- CIFS协议1.0版本不能使用安全算法，建议优先选择更安全的NFS协议。

表 4-35 参数列表

参数	类型	参数项	说明
协议	本地文件	Smart Provisioning ISO文件	仅Smart Provisioning_1.2.1及以上版本支持通过本地文件挂载方式升级SP，请确保iso文件的完整性。 说明 本地文件路径不能包含 &\$><及空格等特殊字符和中文。
	NFS	共享设备IP	将Smart Provisioning文件以共享的形式放在配置CIFS或NFS服务的服务器上来执行升级。

参数	类型	参数项	说明
		文件路径	SmartProvisioning镜像文件路径，格式为“shared director/SmartProvisioning-Vxxx.iso”，不能包含 &\$><@及空格等特殊字符和中文。 说明 SP镜像文件路径中不能包含“\”，可以使用“/”。
		升级文件	由协议、共享设备IP和文件路径组成。 规则请参考对应服务器的《华为服务器 iBMC Redfish 接口说明》，选择“接口介绍>Managers资源的操作>升级SP或者升级固件”，查看参数说明表格中“ImageURL_value”的参数取值。
	CIFS 1.0	共享设备IP	将Smart Provisioning文件以共享的形式放在配置CIFS或NFS服务的服务器上来执行升级。
		用户名和密码	<ul style="list-style-type: none"> 用户名：共享文件所在操作系统用户名。 密码：共享文件所在操作系统密码，不能包含 &\$><@及空格等特殊字符和中文。
		文件路径	SmartProvisioning镜像文件路径，格式为“shared director/SmartProvisioning-Vxxx.iso”，不能包含 &\$><及空格等特殊字符和中文。 说明 SP镜像文件路径中不能包含“\”，可以使用“/”。
		升级文件	由协议、共享设备IP、用户名、密码和文件路径组成。 规则请参考对应服务器的《华为服务器 iBMC Redfish 接口说明》，选择“接口介绍>Managers资源的操作>升级SP或者升级固件”，查看参数说明表格中“ImageURL_value”的参数取值。
	升级类型	Auto	- OS、APP、Driver当前版本和目标版本不同时，升级Smart Provisioning的OS、APP或Driver至目标版本。
		Recover	- 先格式化Smart Provisioning所在的分区，再升级所有OS、APP、Driver至目标版本。默认为Recover。

步骤8 在“选择升级设备”区域勾选需要升级Smart Provisioning的服务器，单击“下一步”。

进入“升级策略评估”界面，如图4-94所示。

图 4-94 升级策略评估



1. 勾选需要评估升级策略的设备。
2. 单击“评估”。
3. 在“评估结果”列显示评估的结果。

□ 说明

- 评估结果如：通过/不通过/不支持评估/未评估。
- 单击“导出报告”，可将升级策略评估结果报告导出至本地。
- 单击“导入”，可导入评估规则文件。
- 下方展示设备信息、Smart Provisioning当前版本、评估结果及建议详情。
- 当未进行评估或评估不通过时，单击“下一步”，弹出相应警告框。请确认风险操作及影响。

步骤9 单击“下一步”，弹出“SP升级可能会丢失SP配置”提示框。

□ 说明

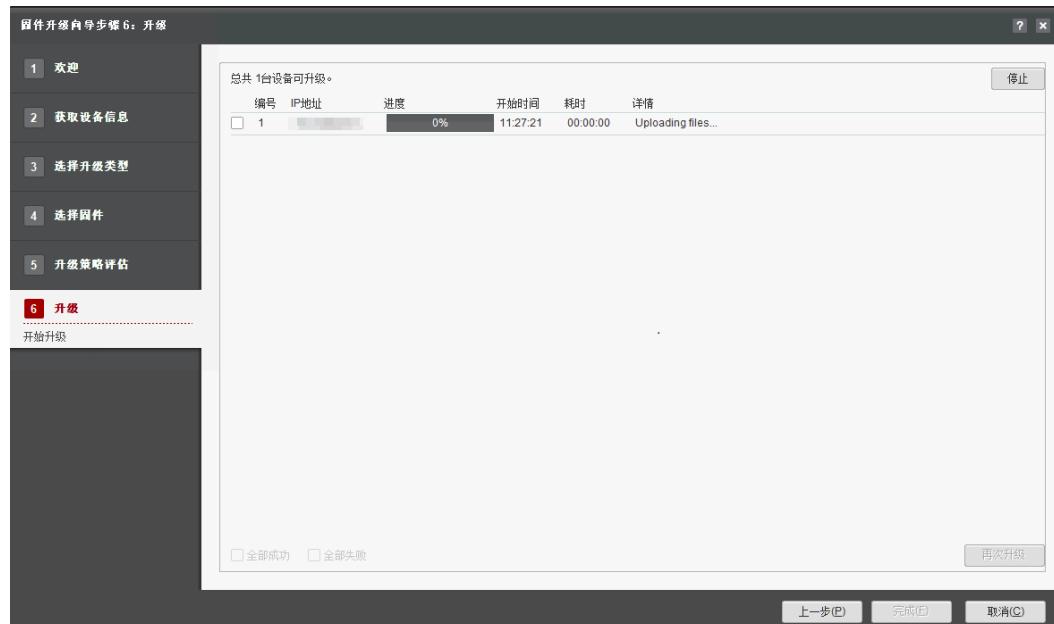
- 当所勾选的设备看门狗状态异常时，会先弹出“如下设备看门狗为开启状态，并且超时动作为Hard Reset, Power Cycle, Power Down中的一种，可能导致服务器异常掉电或重启，请参考[4.9.1.5.1 操作系统侧的看门狗异常问题](#)，修复后重新获取设备信息”提示框。请根据实际情况，选择是否勾选“我已同意工具自动修改看门狗的超时动作作为No Action，并在升级完成后恢复初始超时动作”。
- 在设备上电到操作系统启动期间或者Smart Provisioning启动和运行期间，不支持升级Smart Provisioning；如果未安装操作系统或操作系统无法正常启动，则需要对服务器下电再进行Smart Provisioning升级。

步骤10 单击“确认”。弹出“如果BMC的版本在3.30到3.50之间，该操作会重启BMC并影响业务，请确认是否继续？”。确认BMC版本不在3.30到3.50或者设备允许重启BMC，且已停止操作操作系统业务情况下，则在输入框中输入“yes”后单击“确定”。开始执行升级。否则单击“取消”，取消升级。

步骤11 查看升级进度，当进度“为100%时表示升级成功，如图4-95所示。

单击“完成”退出，向导界面显示成功和未执行的服务器台数，以及总用时。

图 4-95 升级



须知

- 单击“停止”按钮，可终止此次升级任务。
- 升级过程中，停止升级可能会导致设备处于异常状态，请谨慎操作。
- 部分已经向设备下发升级命令的任务，无法停止。
- Smart Provisioning升级成功后，若需要升级PCIe卡，升级前，请先手动登录Smart Provisioning。以避免因Smart Provisioning无法获取PCIe资源，导致无法升级。具体登录Smart Provisioning的方法，请参考《Smart Provisioning 用户指南》中“登录Smart Provisioning”。

说明

- 批量升级Smart Provisioning时，勾选“全部成功”可查看所有升级成功的服务器。
- 批量升级Smart Provisioning时，勾选“全部失败”可查看所有升级失败的服务器。

结束

4.9.1.5 常见问题处理

4.9.1.5.1 操作系统侧的看门狗异常问题

问题现象

重启或升级BMC，可能导致服务器异常重启/下电。

问题原因

当操作系统侧安装看门狗软件并使能了看门狗进程，且看门狗超时动作（Watchdog Timer Actions）为Hard Reset, Power Cycle, Power Down中的一种，则重启或升

级BMC可能会触发操作系统侧看门狗软件缺陷，导致操作系统侧看门狗软件终止喂狗，触发硬件看门狗喂狗超时动作，服务器可能异常重启/下电。

解决措施

BMC重启或升级前，建议关闭硬件看门狗进程或将硬件看门狗超时操作设置为No Action。

- 如果设置硬件看门狗超时动作作为No Action

- 进入到工具安装目录\tools\ServerMain\tools\ipmitool，通过ipmitool查询硬件看门狗当前配置，执行如下命令，查询硬件看门狗配置。

```
ipmitool -I lanplus -H 172.XX.XX.XX -U root -P Password raw 0x06 0x25
```

说明

其中-H后面的172.XX.XX.XX为BMC的IP，-U后面的root为BMC的用户名，-P后面的Password为BMC的密码，需根据实际情况进行修改。

图 4-96 查询硬件看门狗配置



```
ipmitool -I lanplus -H [REDACTED] -U root -P [REDACTED] raw 0x06 0x25
Watchdog Timer Use: SMS/OS (0x44)
Watchdog Timer Is: Started/Running
Watchdog Timer Actions: Hard Reset (0x01)
Pre-timeout interval: 0 seconds
Timer Expiration Flags: 0x00
Initial Countdown: 300 sec
Present Countdown: 298 sec
[REDACTED]
44 01 00 00 b8 0b 8d 0b
```

如图4-96所示，返回结果中的前6字节44 01 00 00 b8 0b为当前硬件看门狗的配置，其中第二字节01中的末尾数字表示硬件看门狗超时后的动作，该数值的定义如下：

- 0: No Action，表示看门狗喂狗超时后不执行任何动作。
- 1: Hard Reset，表示看门狗喂狗超时后服务器重启。
- 2: Power Down，表示看门狗喂狗超时后将服务器下电。
- 3: Power Cycle，表示看门狗喂狗超时后将服务器先下电再上电。

如果该字节值为0，超时动作作为No Action，则无需进行下一步操作。

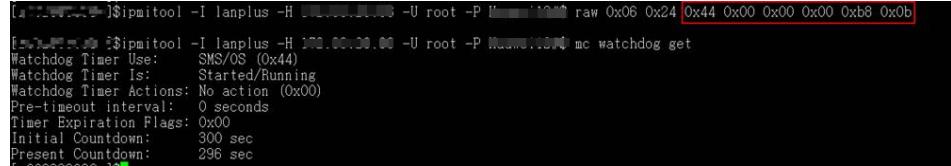
- 通过ipmitool执行如下命令，设置硬件看门狗超时动作作为No Action，如图4-97所示。

```
ipmitool -I lanplus -H 172.XX.XX.XX -U root -P Password raw 0x06 0x24 0x44 0x00 0x00 0x00 0xb8 0x0b
```

说明

其中-H后面的172.XX.XX.XX为BMC的IP，-U后面的root为BMC的用户名，-P后面的Password为BMC的密码，需根据实际情况进行修改。0x44 0x00 0x00 0x00 0xb8 0x0b为a中获取到的前6字节，仅将第二字节0x01改为0x00。

图 4-97 设置硬件看门狗超时动作作为 No Action



```
ipmitool -I lanplus -H [REDACTED] -U root -P [REDACTED] raw 0x06 0x24 0x44 0x00 0x00 0x00 0xb8 0x0b
Watchdog Timer Use: SMS/OS (0x44)
Watchdog Timer Is: Started/Running
Watchdog Timer Actions: No action (0x00)
Pre-timeout interval: 0 seconds
Timer Expiration Flags: 0x00
Initial Countdown: 300 sec
Present Countdown: 296 sec
```

须知

该命令临时生效，系统或看门狗软件重启后恢复修改前的配置。

c. 待BMC重启或升级完成后，执行如下命令，恢复硬件看门狗配置。

```
ipmitool -I lanplus -H 172.XX.XX.XX -U root -P Password raw 0x06 0x24 0x44 0x01 0x00 0x00  
0xb8 0xb
```

说明

其中-H后面的172.XX.XX.XX为BMC的IP，-U后面的root为BMC的用户名，-P后面的Password为BMC的密码，需根据实际情况进行修改。0x44 0x01 0x00 0x00 0xb8 0xb为a中获取到的前6字节。

- 如果关闭硬件看门狗

- a. 可通过如下2种方法关闭硬件看门狗：

- 通过ipmitool执行如下命令，关闭硬件看门狗，如图4-98所示。

```
ipmitool mc watchdog off
```

图 4-98 操作系统侧关闭硬件看门狗

```
[root@localhost ~]# ipmitool mc watchdog off  
Watchdog Timer Shutoff successful -- timer stopped  
[root@localhost ~]# ipmitool mc watchdog get  
Watchdog Timer Use: SMS/OS (0x04)  
Watchdog Timer Is: Stopped  
Watchdog Timer Actions: No action (0x00)  
Pre-timeout interval: 0 seconds  
Timer Expiration Flags: 0x00  
Initial Countdown: 300 sec  
Present Countdown: 0 sec  
[root@localhost ~]#
```

- 通过ipmitool执行如下命令，远程关闭硬件看门狗，如图4-99所示。

```
ipmitool -I lanplus -H 172.XX.XX.XX -U root -P Password mc watchdog off
```

说明

其中-H后面的172.XX.XX.XX为BMC的IP，-U后面的root为BMC的用户名，-P后面的Password为BMC的密码，需根据实际情况进行修改。

图 4-99 远程关闭硬件看门狗

```
[root@localhost ~]# ipmitool -I lanplus -H 172.XX.XX.XX -U root -P Password mc watchdog off  
Watchdog Timer Shutoff successful -- timer stopped  
[root@localhost ~]# ipmitool -I lanplus -H 172.XX.XX.XX -U root -P Password mc watchdog get  
Watchdog Timer Use: SMS/OS (0x04)  
Watchdog Timer Is: Stopped  
Watchdog Timer Actions: No action (0x00)  
Pre-timeout interval: 0 seconds  
Timer Expiration Flags: 0x00  
Initial Countdown: 300 sec  
Present Countdown: 300 sec
```

- b. BMC重启或升级完成后，可通过系统侧命令行进行看门狗进程开启操作或重启操作系统恢复修改前配置。

4.9.1.5.2 下电失败导致升级 BIOS 或 CPLD 失败问题

问题现象

升级界面提示固件加载成功，但生效操作失败：已下发下电命令，但设备未能下电。

问题原因

- 未配置下电超时的情况下，下电需要等待设备响应。设备响应缓慢时下电操作无法及时进行。
- 进行下电时，部分操作系统会弹出确认框。需要进行确认后设备才可以正常下电。

解决措施

- 设备已安装操作系统时，登录BMC远程虚拟控制台，在操作系统尝试下电。详细操作请参见服务器 BMC用户指南。确认下电后，请执行上电操作，并确认版本是否生效。
- 设备未安装操作系统时，请在工具“例行维护->电源控制”中尝试强制下电。确认下电后，请执行上电操作，并确认版本是否生效。
- 设备未安装操作系统时，请在设备BMC页面中尝试强制下电。详细操作请参见服务器 BMC用户指南。确认下电后，请执行上电操作，并确认版本是否生效。

说明

强制下电可能损坏操作系统文件，请谨慎操作。

4.9.1.5.3 sp 升级使用 cifs/nfs 服务搭建方法

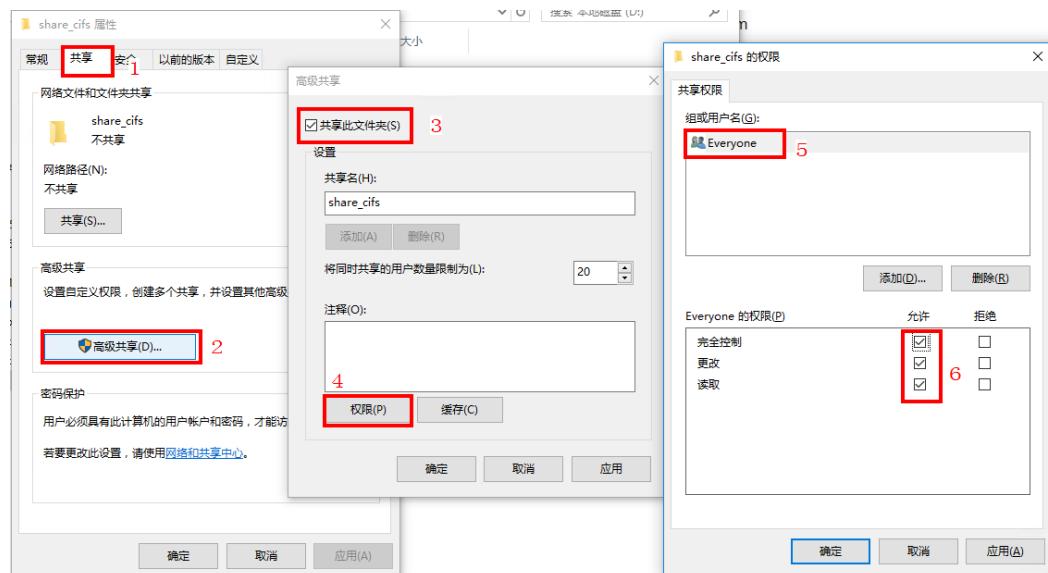
在 Windows 系统内使用 CIFS 协议共享文件

以Windows10为例：

步骤1 在系统内创建个文件夹，并将sp镜像文件拷贝至已创建的个人文件夹内。

步骤2 配置文件夹共享，如图4-100所示。

图 4-100 win10 配置文件夹共享



1. 在创建的文件夹内，单击鼠标右键，选择“属性”按钮，进入“share_cifs属性”界面。
2. 选择“共享”窗口界面。
3. 单击“高级共享”，进入“高级共享”界面。
4. 勾选“共享此文件夹”，单击“权限”，进入“共享权限”界面。
5. 根据实际情况勾选“完全控制”，“更改”，“读取”。
6. 单击“确定”完成设置。

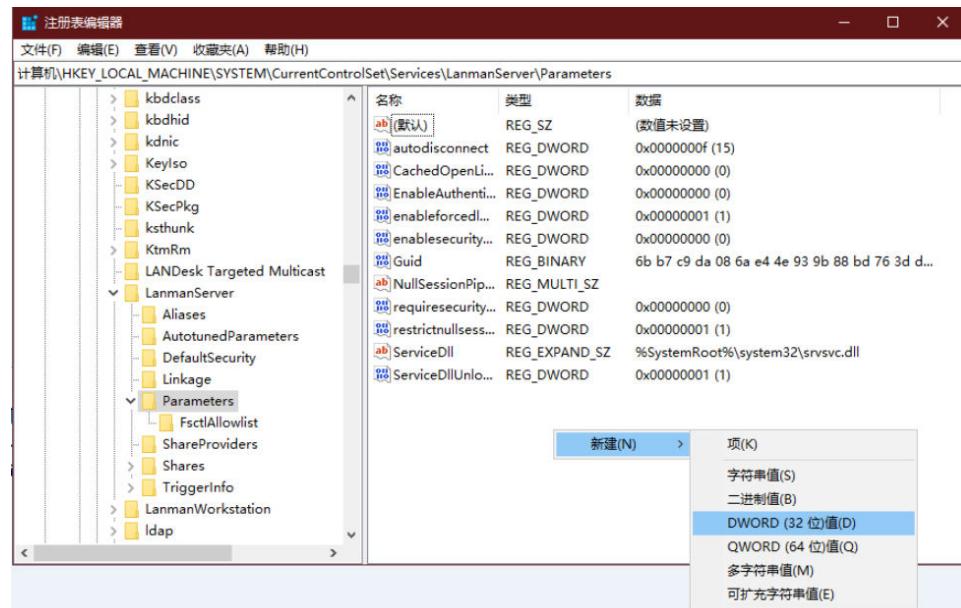
步骤3 使用其他PC机查看共享文件。

步骤4 配置注册表，启用SMB1功能。

□ 说明

- 工具只支持SMB (CIFS) 1.0版本环境下执行升级操作。
- 配置注册表前，请将注册表备份。操作方法如下：
 1. 单击电脑左下角“开始”按钮，在搜索框输入“regedit.exe”，回车，弹出注册编辑表。
 2. 在注册编辑表中，选择您需要备份的子项注册表项，单击鼠标“右键”，选择导出。
 3. 选择您需要保存备份文件的位置，在[文件名]字段中键入备份文件的名称，单击“保存”。
- 1. 打开注册表文件夹“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters”。
- 2. 查找注册表项为SMB1的文件，如果没有找到注册表项为SMB1的文件，需手动创建名为SMB1的文件，如图4-101所示。

图 4-101 创建 SMB1



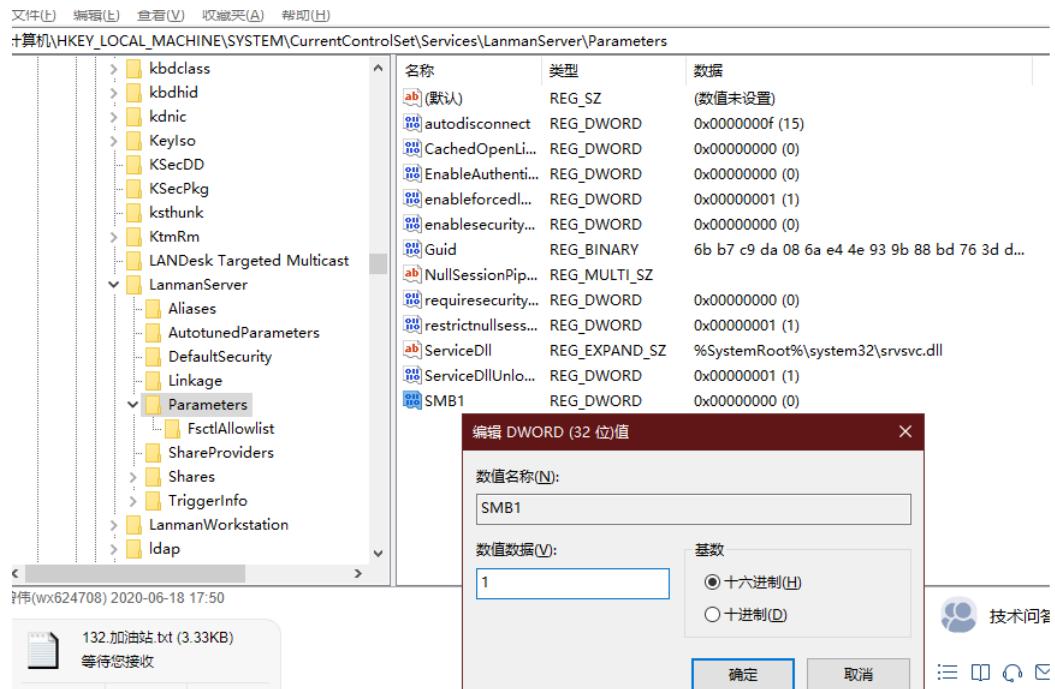
REG_DWORD: 0=已禁用

REG_DWORD: 1=已启用

默认值: 1=已启用 (未创建注册表项)

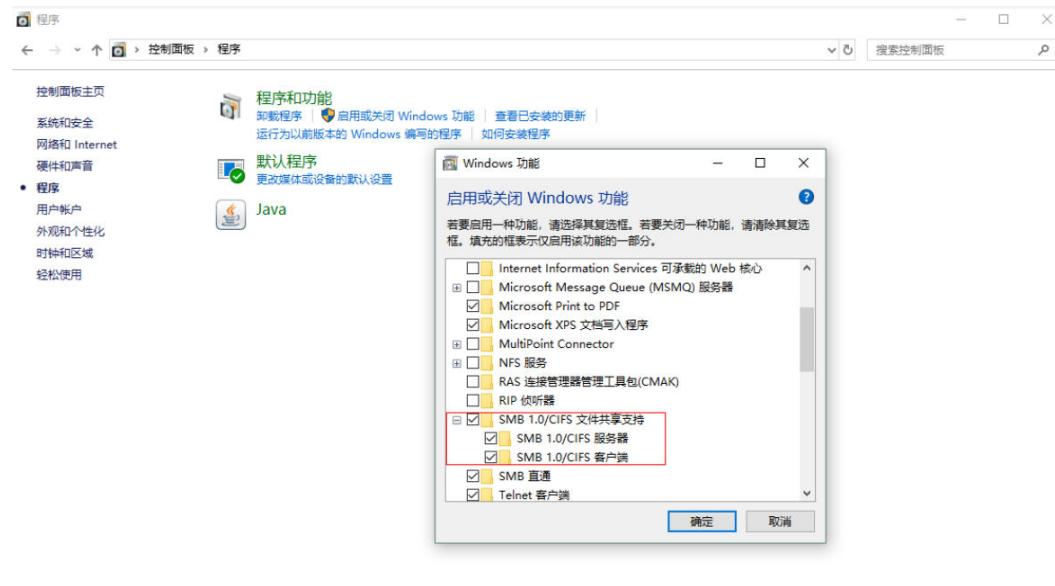
步骤5 打开SMB1文件将“REG_DWORD”值改为1，将注册表的SMB (CIFS) 的版本设置为1.0，如图4-102所示。

图 4-102 修改 SMB1



步骤6 开启SMB 1.0/CIFS文件共享，如图4-103所示。

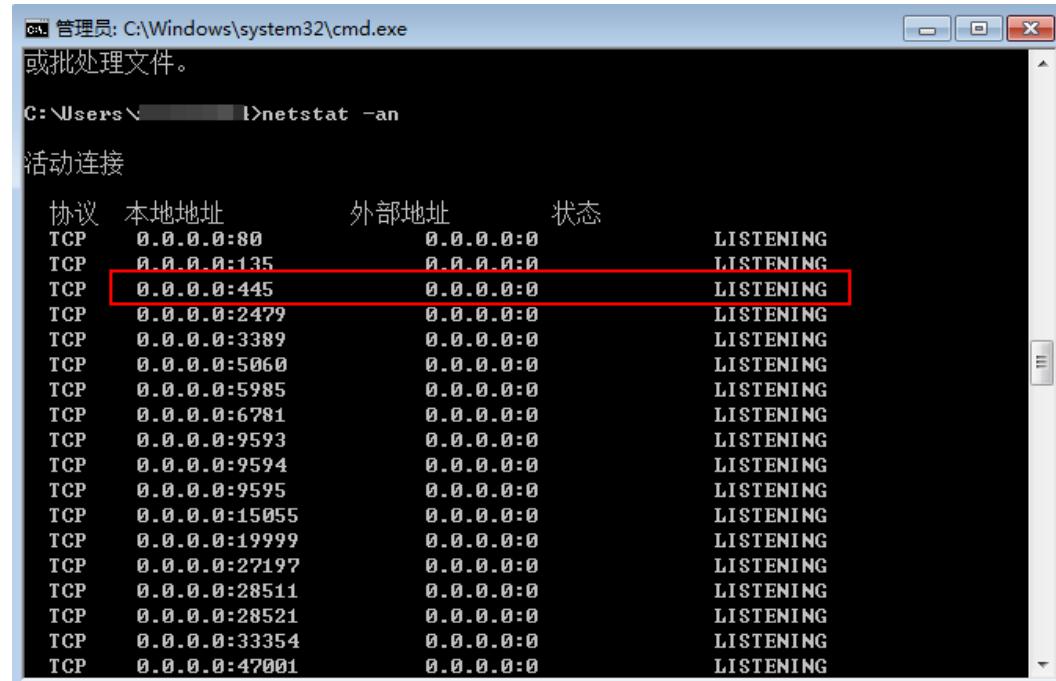
图 4-103 开启 SMB 1.0/CIFS 文件共享



步骤7 配置完成后，重启电脑生效。

步骤8 登录Windows命令窗口，使用“netstat -an”命令查询445端口是否开启（Windows CIFS需要开启445端口）。如图4-104所示，则表示445端口已开启。

图 4-104 Windows 开启 445 端口



```
管理员: C:\Windows\system32\cmd.exe
或批处理文件。

C:\Users\...> netstat -an

活动连接

协议 本地地址          外部地址          状态
TCP 0.0.0.0:80          0.0.0.0:0          LISTENING
TCP 0.0.0.0:135         0.0.0.0:0          LISTENING
TCP 0.0.0.0:445         0.0.0.0:0          LISTENING
TCP 0.0.0.0:2479        0.0.0.0:0          LISTENING
TCP 0.0.0.0:3389        0.0.0.0:0          LISTENING
TCP 0.0.0.0:5060        0.0.0.0:0          LISTENING
TCP 0.0.0.0:5985        0.0.0.0:0          LISTENING
TCP 0.0.0.0:6781        0.0.0.0:0          LISTENING
TCP 0.0.0.0:9593        0.0.0.0:0          LISTENING
TCP 0.0.0.0:9594        0.0.0.0:0          LISTENING
TCP 0.0.0.0:9595        0.0.0.0:0          LISTENING
TCP 0.0.0.0:15055       0.0.0.0:0          LISTENING
TCP 0.0.0.0:19999       0.0.0.0:0          LISTENING
TCP 0.0.0.0:27197       0.0.0.0:0          LISTENING
TCP 0.0.0.0:28511       0.0.0.0:0          LISTENING
TCP 0.0.0.0:28521       0.0.0.0:0          LISTENING
TCP 0.0.0.0:33354       0.0.0.0:0          LISTENING
TCP 0.0.0.0:47001        0.0.0.0:0          LISTENING
```

----结束

Windows 上搭建 NFS 服务器

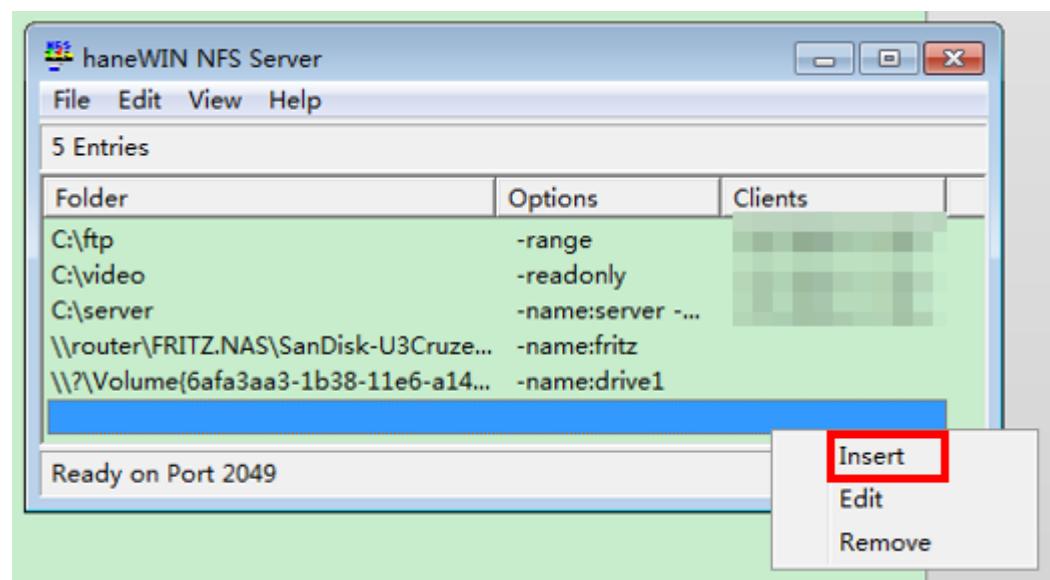
步骤1 下载“NFS”服务器软件，运行并安装，如图4-105所示。

图 4-105 安装 NFS 软件



步骤2 打开NFS Server客户端，在空白处点击右键，单击“Insert”，如图4-106所示。进入填写参数界面。

图 4-106 插入

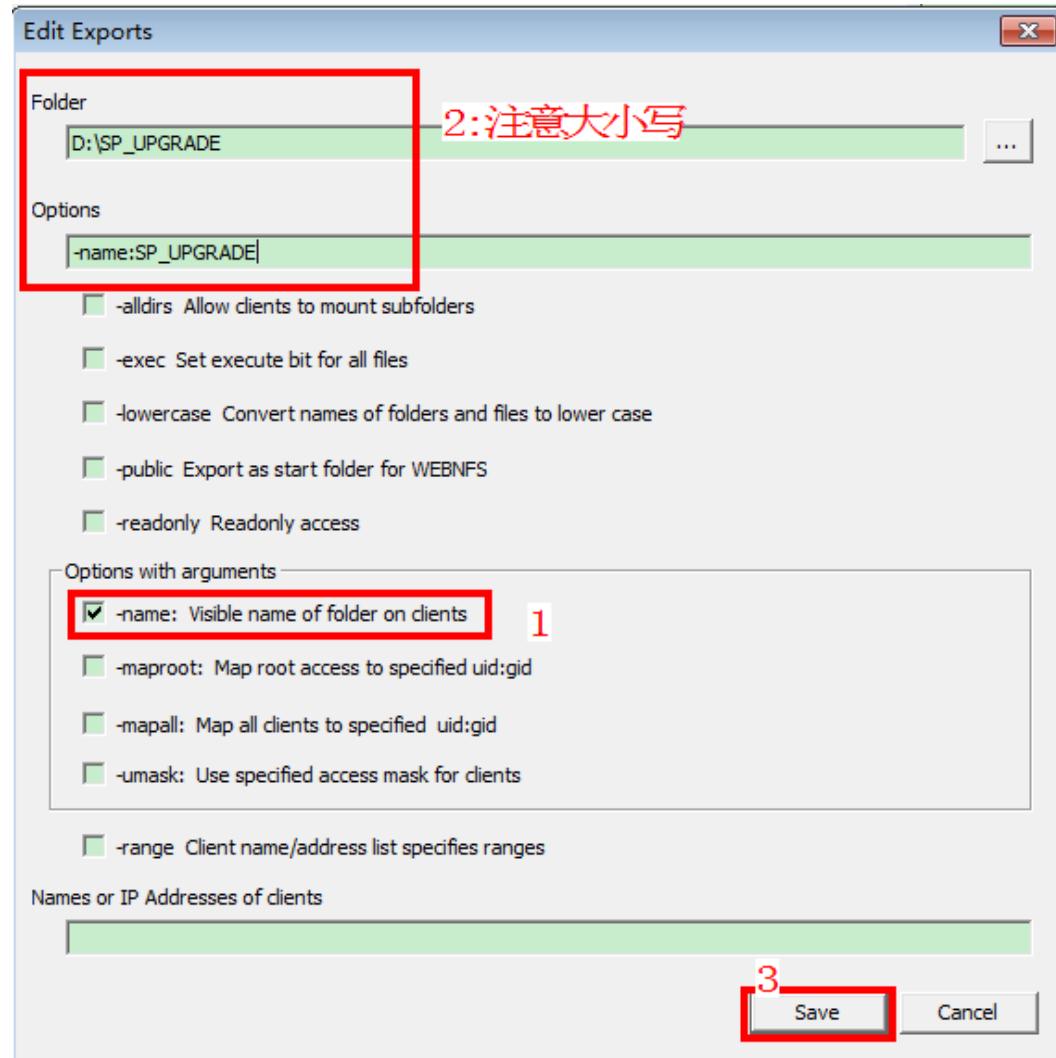


步骤3 勾选“-name: Visible name of folder on clients”，并按要求要求填写相关参数。如图4-107所示。

说明

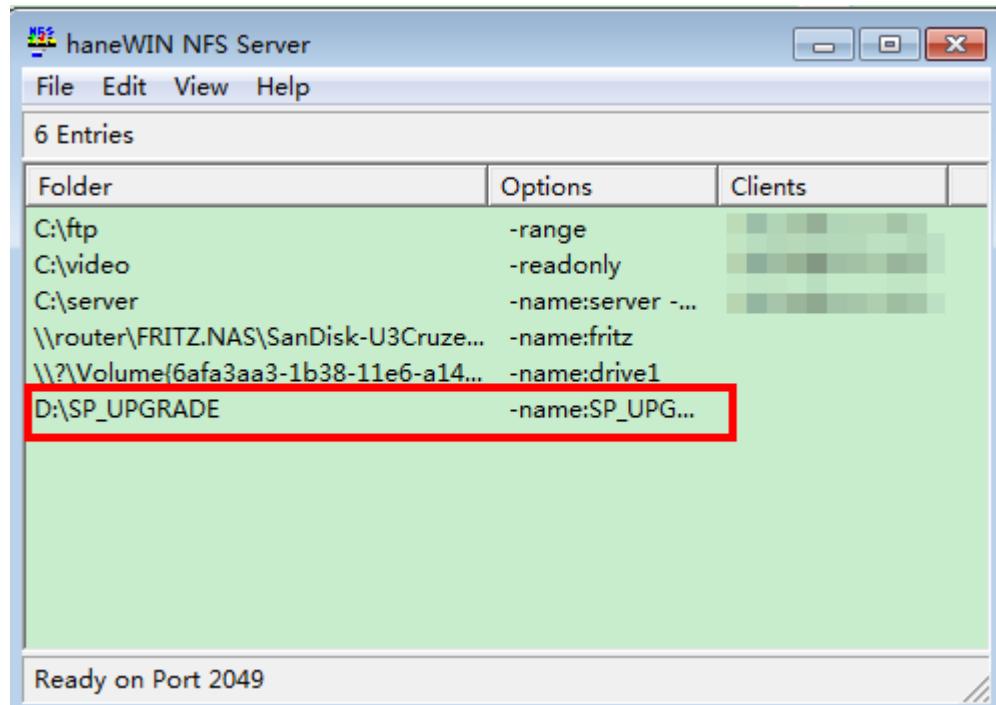
- Folder后请填写SP升级镜像文件所在目录，如：D:\SP_UPGRADE。
- -name:后请填SP_UPGRADE。

图 4-107 填写参数



步骤4 单击“Save”，如图4-108所示，表示nfs服务搭建完成。

图 4-108 nfs 服务搭建完成



----结束

在 Linux 系统中搭建 NFS 服务

在 Linux 系统中搭建 nfs 服务

以 CentOS 7.3 系统为例介绍在 Linux 系统中搭建 nfs 服务。

步骤1 执行以下命令，检查是否已经安装 nfs 服务，如图 4-109 所示，若没有安装则需要自行安装。

```
rpm -qa|grep nfs-utils
```

图 4-109 检查是否已经安装 nfs 服务

```
[root@localhost bai]# rpm -qa|grep nfs-utils
nfs-utils-1.3.0-0.33.el7.x86_64
[root@localhost bai]#
```

步骤2 关闭防火墙。

1. 执行以下命令，停止防火墙。
systemctl stop firewalld.service
2. 执行以下命令，禁止防火墙开机启动。
systemctl disable firewalld.service
3. 执行以下命令，查看防火墙状态。
firewall-cmd --state

查询结果显示“notrunning”则表示已关闭防火墙，查询结果显示“running”则表示已打开防火墙。

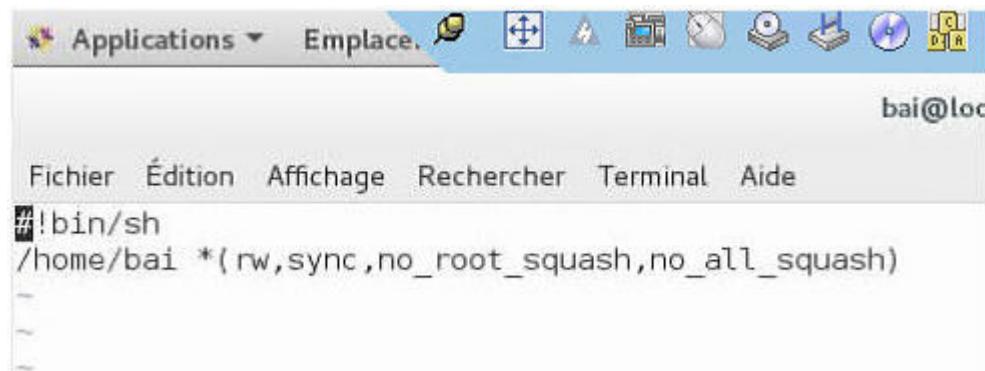
步骤3 执行以下命令，启动 nfs 服务。

```
service nfs start
```

步骤4 设置共享目录。执行vi /etc/exports命令编辑文件。

在文件中输入“/home/bai *(rw, sync, no_root_squash, no_all_squash)”。如图4-110所示。

图 4-110 编辑文件



- “/home/bai” 代表待共享出去的目录。
- “*” 表示可以访问的IP范围，这里表示所有IP地址都可以访问，也可以设置为“hostname”。
- “rw” 表示具有读写权限。
- “no_all_squash” 表示保留共享文件的UID和GID（默认）。
- “no_root_squash” 表示root用户具有根目录的完全管理访问权限。

步骤5 执行以下命令，重启nfs服务。

```
service nfs restart
```

步骤6 执行以下命令，重新激活nfs。

```
exportfs -rv
```

其中r表示重启，v表示显示“etc/exports”配置文件里的内容。

步骤7 执行以下命令，在客户端查看服务器端共享的文件。

```
showmount -e serverIP
```

其中serverIP表示nfs服务器ip。

步骤8 在服务器端执行以下命令，开放写权限给其他用户。

```
chmod 777 -R /home/bai
```

步骤9 登录Linux命令窗口，使用“netstat -an”命令查询是否已开启111端口和2049端口（Linux NFS 需要开启111端口和2049端口）。如图4-111所示，则表示111端口已开启。

图 4-111 Linux 开启 111 端口

```
linux-suse:~/www_c/BIOS # netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:111              0.0.0.0:*
tcp        0      0 0.0.0.0:50000             0.0.0.0:*
tcp        0      0 0.0.0.0:43156             0.0.0.0:*
tcp        0      0 0.0.0.0:22               0.0.0.0:*
tcp        0      0 [REDACTED]                0.0.0.0:*
tcp        0      0 127.0.0.1.128             0.0.0.0:*
tcp        0      0 [REDACTED]                [REDACTED]          ESTABLISHED
tcp        0      0 127.0.0.1.42050            [REDACTED]          ESTABLISHED
tcp        0      0 :::7072                  :::*
tcp        0      0 :::25640                 :::*
tcp        0      0 :::9099                 :::*
tcp        0      0 :::111                  :::*
tcp        0      0 :::50000                 :::*
tcp        0      0 :::9011                  :::*
tcp        0      0 :::25620                 :::*
tcp        0      0 :::22                   :::*
tcp        0      0 :::1631                 :::*
tcp        0      0 :::125                  :::*
tcp        0      0 [REDACTED]                [REDACTED]          ESTABLISHED
udp        0      0 0.0.0.0:111              0.0.0.0:*
udp        0      0 0.0.0.0:631              0.0.0.0:*
udp        0      0 0.0.0.0:828              0.0.0.0:*
udp        0      0 :::111                  :::*
udp        0      0 :::828                  :::*
```

----结束

4.9.1.5.4 其他问题

□ 说明

不在表4-36的错误信息，请联系技术支持。

表 4-36 其他问题

错误描述	原因	处理建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。

错误描述	原因	处理建议
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none"> SNMP配置错误或服务器不支持SNMP命令。 SNMP未响应。 	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看BMC端口信息、5.4 查看BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none"> 确认该操作是否符合规范。 重新执行该操作。
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合SNMP要求。	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查密码是否满足SNMP V3的要求，如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3协议不一致或用户名/密码不一致，引起巡检（升级）串行。	<ol style="list-style-type: none"> 检查所有服务器配置的SNMP V3协议是否一致，并将其调整一致。 检查所有服务器的用户名、密码是否一致，并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话，IPMI命令执行失败。	<ol style="list-style-type: none"> 手工执行IPMI命令，检查是否存在问题。 待问题解决后，重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 检查网络是否有异常。 重新执行任务。
User must be an administrator.	使用非管理员账户执行该操作。	<ol style="list-style-type: none"> 检查用户是否为管理员账户。 使用管理员账户重新执行该操作。

错误描述	原因	处理建议
version.xml was not found in the upgrade file. Please select hpm file or upgrade on BMC web	选择的升级包中未找到version.xml文件。	<ul style="list-style-type: none"> 选择hpm文件进行升级。 直接在BMC Web界面进行升级。
Upgrade file was not found, please check "FileName" node in version.xml	升级文件与“version.xml”文件中的配置不一致。	将“version.xml”文件中的升级文件名修改得与实际升级文件名一致。
Unsupported upgrade file, that cannot find upgrade file which end with ".hpm"	升级文件不是以“.hpm”结尾的。	在BMC Web界面进行升级。
Get software version error	获取固件版本失败。	重新执行发现服务器。
Upgrade abnormally, please restart BMC and try again	升级时异常关闭BMC。	复位BMC，待完全启动后，重新进行升级。
The target is in upgrading, please wait a few minutes and try again.	服务器正在进行固件升级。	等待30分钟，待固件升级完成后，重新执行升级任务。
Unknown upgrade error,please check BMC:1)network 2)ipmi service 3)BMC upgrade log.	升级时未知的错误。	重启BMC后重新升级，若还是不成功，搜集日志提供给BMC进一步分析原因。
The upgrade file does not exist.	升级文件不存在。	检查升级文件路径后，重新执行升级任务。
Upgrade file error.	升级文件错误。	检查升级文件是否有误，无误后，重新执行升级。
Failed to download the upgrade file.	下载升级文件失败。	重新执行升级任务。
The upgrade file error, Please confirms the upgrade file matches.	服务器不支持使用该升级文件进行固件升级。	<ol style="list-style-type: none"> 检查升级文件是否支持该服务器。 重新下载该服务器的固件升级包。
Insufficient BMC memory.The target may be upgrading, please wait a few minutes and try again.	固件升级时检测到内存不足。	可能正在进行升级，等待30分钟后再重新执行升级，若还是失败，建议复位BMC后再试。

错误描述	原因	处理建议
The upgrade space is insufficient. Please restart BMC and try again.	内存空间不足导致固件升级失败。	复位BMC后再重新执行升级，若还是失败，请直接在BMC Web界面上进行升级。
Does not support the Bios 8M upgrade under the condition of power on! Please power off the server and try again	服务器处于上电状态时不支持BIOS 8M模式升级。	对服务器进行下电操作后再执行升级任务。
Communication exception, please check the network or SNMP/IPMI configuration.	SNMP或IPMI配置错误。	检查是否打开SNMP和IPMI，并检查端口号是否与工具配置的一致，详细请参考 5.4 查看BMC的SNMP协议 。
The system disk has no sufficient space.	系统盘无足够的空间。	检查工具所在系统盘空间是否不足，清理后，再执行升级操作。
Unknown error.	升级时未知的错误。	复位BMC后重新执行升级任务。
Start upgrade failed. Please wait 30 minutes and try again.	可能正在进行升级导致启动升级失败。	<ul style="list-style-type: none"> 等待30分钟后再进行升级。 在BMC Web界面上进行升级。
Upgrade timeout.	升级超时。	<ol style="list-style-type: none"> 检查网络是否良好。 复位BMC后重新执行升级。 若执行以上操作后还是失败，请直接在BMC Web界面上进行升级。
The BMC upgrade process is running.	BMC板正在升级。	等待升级完成后，再重新执行升级。
Not support bundle version information.	当前BMC板的版本不支持大包版本信息的存放与获取。	需要先升级BM的版本后再执行升级。
No bundle version information.	当前BMC板的版本无大包版本信息。	需要先升级BMC的版本后再执行升级。
The current version and the bundle version(version) are not compatible.	当前固件版本与大包版本不配套。	将当前固件版本升级至提示信息括号中相同的版本。
Upgrade failed. Card not found.	未找到要升级的MEZZ卡。	检查服务器上是否存在相应槽位的MEZZ卡。

错误描述	原因	处理建议
Upgrade failed. Firmware matching the OS not found.	未找到所选操作系统对应的固件导致升级失败。	1. 检查服务器是否支持该MEZZ卡, 以及是否支持所选操作系统。 2. 检查固件升级包是否为最新版本。
Upgrade failed. Driver for this mezzanine card not found.	未找到MEZZ卡所需的固件导致升级失败。	
Upgrade failed. Firmware upgrade of this card is not supported.	不支持升级该MEZZ卡。	
Set boot from CD/DVD failed, cannot upgrade Firmware, please try again later.	设置从光驱启动失败。	查看服务器是否支持运行工具后再重新执行该操作。
Control the upgrade failed, please try again later.	控制超时。	稍后重新执行该操作。
Reset the system after upgrade failed, please do it manually.	升级完成后自动复位系统失败。	手工复位系统。
Poweron the system failed, cannot upgrade Firmware, please try again later.	系统上电失败。	请联系技术支持。
Upgrade failed. The system goes to power off status, please try upgrade again later.	固件升级过程中系统自动下电导致升级失败。	
Reset the system failed, cannot upgrade Firmware, please try again later.	复位系统失败导致不能进行固件升级。	稍后重新执行升级操作, 若还是失败, 请联系技术支持。
Mount firmware image failed.	挂载升级镜像文件失败。	1. 查看服务器是否支持运行工具。 2. 检查是否已经挂载镜像文件, 将其断掉后重新执行该操作。
Set firmware upgrade command failed, please try again later.	发送固件升级命令失败。	1. 查看服务器是否支持运行工具后再重新执行该操作。 2. 稍后重新执行该操作。
Have same connect.	交换板有相同的SOL连接。	退出交换板SOL连接后, 重新执行该操作。

错误描述	原因	处理建议
Upgrade timed out. Check your network or try again.	升级超时,请检查你的网络或者再试一次。	<ol style="list-style-type: none"> 1. 请确认是否已升级到预期版本。 <ol style="list-style-type: none"> a. 如果升级的是计算节点或管理模块,若已升级到预期版本,请忽略,继续执行未完成的升级操作。否则请参照第2条处理建议。 b. 如果升级的是交换模块,请联系技术支持。 2. 确认网络是否正常。如果网络不稳定或者网络断开,请修复网络后重新执行升级操作。 3. 如果仍无法解决问题,请联系技术支持。
Upgrade failed. This operation is not supported.	BIOS启动过程中或者启动失败等情况下导致服务器U盘被占用,升级Smart Provisioning时无法挂载镜像。	执行服务器下电操作,在下电状态下升级Smart Provisioning。
upgrade failed,message:unknown error	sp分区的文件系统被破坏。	插拔服务器电源后重试,若仍存在问题,请联系技术服务工程师处理。
unknown error	升级文件共享问题,导致服务器访问共享文件失败。	<ol style="list-style-type: none"> 1. 确认cifs/nfs协议是否正常,服务器可以访问共享文件。 2. 确认参数填写是否正确。 3. 重新执行升级操作。

4.9.2 升级 PCIe 卡/硬盘固件

本节指导用户使用工具箱升级PCIe卡。

4.9.2.1 升级流程

升级PCIe卡/硬盘固件流程如图4-112所示。

图 4-112 升级 PCIe 卡/硬盘固件



4.9.2.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

- PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH、VMM通信端口连通，保证能ping通服务器BMC的IP地址。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。
- PCIe卡/硬盘固件升级包为适配FwUpgrade V101或之后版本的zip文件（参考固件升级包说明），包含install.sh升级脚本，使用时不允许解压。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

4.9.2.3 选择设备

在固件升级向导的“选择设备”界面中，可以选择需要进行升级PCIe卡/硬盘固件的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“升级/补丁>固件升级”。

系统进入“固件升级”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要升级PCIe卡/硬盘固件的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明书

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如表4-37所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考表4-37，手工输入参数。

表 4-37 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none">单台设备时，和“起始IP”相同，如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.2.2 IPv6： 起始IP：2017::f434 结束IP：2017::f434多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始IP：192.168.2.2 结束IP：192.168.5.254 IPv6： 起始IP：2017::f434 结束IP：2017::f439多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	BMC板管理员用户名。	-

类型	名称	说明	备注
	密码	BMC板管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	默认值是8208，以设备实际启用的端口号为准。
	HTTPS端口	HTTPS端口号。	请忽略该参数，或者保持默认值。
OS选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选升级PCIe卡/硬盘固件的设备。单击“确定”，返回向导界面。

----结束

4.9.2.4 升级PCIe卡/硬盘固件

□ 说明

- 建议先尝试升级一台服务器的网卡、RAID卡、硬盘固件，待没有问题后，再进行批量挂载，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 如对软件包版本无特殊要求，建议使用最新配套版本。
- 操作过程中遇到的问题请参考[4.9.2.5 常见问题处理](#)解决。

须知

- 操作过程中, 请勿对服务器进行系统上下电及重启等操作。
- 服务器上运行的业务可能被中断, 仅限专业人士操作该功能。
- 升级PCIe卡/硬盘固件前, 请先确认BIOS和CPLD是否已经升级完成, 但实际未生效。如果是, 请先重启服务器再升级PCIe卡/硬盘固件。

操作步骤

步骤1 在固件升级向导界面上单击“固件升级”。

系统弹出“升级固件、升级PCIe卡/硬盘固件”选择框。

步骤2 单击“升级PCIe卡/硬盘固件”。系统进入升级向导“欢迎”界面, 如图4-113所示。

在升级向导“欢迎”界面, 了解该场景主要用来挂载虚拟媒体和升级PCIe固件。

图 4-113 欢迎



步骤3 单击“下一步”。

进入“获取设备信息”界面, 如图4-114所示。

图 4-114 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量，并发数可设置为1~50。
- CPU并发能力，通过简单测试CPU性能，预估建议并发能力范围值。测试结果与CPU占用率有关，测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤4 在设备列表中勾选一台或者多台需要升级的设备。

步骤5 单击“下一步”。执行发现服务器操作。

说明

单击“停止”可终止此次任务。

步骤6 发现服务器后系统自动进入选择服务器界面。单击“过滤设备”下拉框，可对发现的服务器进行筛选，快速选择需要进行操作的一类服务器。

步骤7 勾选需要升级PCIe卡/硬盘固件的服务器，单击“下一步”。

进入“选择挂载媒体”界面。, 如图4-115所示。

图 4-115 选择挂载媒体界面



1. 单击“Smart Provisioning ISO文件”所在行的“选择”，选择Smart Provisioning ISO V125/1.2.0.4及之后版本的ISO文件。
2. 单击“固件包路径”所在行的“选择”，选择适配Smart Provisioning V125/1.2.0.4及之后版本的固件包所在文件夹。

说明

- 如果选择的ISO文件类型和版本不符合要求，会弹出“该ISO/IMG不适合当前场景，请用FusionServer Tools-Smart Provisioning-V125/1.2.0.4或更高版本”的提示框。
- 如果只选择Smart Provisioning ISO文件，未选择固件包路径，会弹出“当执行PCIe升级时，固件包路径与” Smart Provisioning ISO文件都必须选择”的提示框。

步骤8 (可选) 在选项设置中手动勾选“数字签名验证”，表示验证数字证书。

须知

请确认固件包路径中包含对应的数字签名。

步骤9 单击“下一步”。

弹出“服务器将会重启，请确保已关闭服务器业务，请确认是否继续”的提示框。

步骤10 若已关闭服务器业务，则在输入框中输入“yes”后单击“确定”。

开始执行升级。

步骤11 当进度条显示“100%时”表示升级完成。如图4-116所示。

图 4-116 开始执行



步骤12 单击“完成”退出，弹出提示框“确认要退出升级PCIe卡/硬盘固件向导？”

步骤13 单击“确定”，退出该界面。”向导界面显示成功和未执行的服务器台数，以及总用时。

----结束

4.9.2.5 常见问题处理

表 4-38 其他问题

错误描述	原因	解决建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。

错误描述	原因	解决建议
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none"> SNMP配置错误或服务器不支持SNMP命令。 SNMP未响应。 	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看BMC端口信息、5.4 查看BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none"> 确认该操作是否符合规范。 重新执行该操作。
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合SNMP要求。	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查密码是否满足SNMP V3的要求，如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3协议不一致或用户名/密码不一致，引起巡检（升级）串行。	<ol style="list-style-type: none"> 检查所有服务器配置的SNMP V3协议是否一致，并将其调整一致。 检查所有服务器的用户名、密码是否一致，并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话，IPMI命令执行失败。	<ol style="list-style-type: none"> 手工执行IPMI命令，检查是否存在问题。 待问题解决后，重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 检查网络是否有异常。 重新执行任务。
User must be an administrator.	使用非管理员账户执行该操作。	<ol style="list-style-type: none"> 检查用户是否为管理员账户。 使用管理员账户重新执行该操作。

错误描述	原因	解决建议
Mount firmware image failed.	挂载升级镜像文件失败。	1. 查看服务器是否支持运行工具。 2. 检查是否已经挂载镜像文件，将其断掉后重新执行该操作。
Set firmware upgrade command failed, please try again later.	发送固件升级命令失败。	1. 查看服务器是否支持运行工具。 2. 稍后重新执行该操作。
Have same connect.	交换板有相同的SOL连接。	退出交换板SOL连接后，重新执行该操作。
Mount failed. The device is already mount, please unmount it first.	已挂载虚拟媒体导致此次挂载失败。	使用 <code>umount</code> 命令卸载已挂载的虚拟媒体后再进行挂载。
Mount media failed. Media file-path is not exists.	镜像文件的路径不存在。	检查镜像文件的路径是否存在。
Mount media failed. Media file-path can not read.	镜像文件不可读导致挂载失败。	添加镜像文件的读权限。
Unmount failed, no media was mounted.	未挂载虚拟媒体导致卸载失败。	先挂载虚拟媒体后再卸载。
Unmount media failed, the device is not found in the management list.	设备第一次添加，尚未进行过虚拟媒体挂载，不能进行卸载。	先挂载虚拟媒体后再卸载。
Query the mount status failed, the device is not found in the management list.	设备第一次添加，尚未进行过虚拟媒体挂载，不能查询挂载状态。	先挂载虚拟媒体后再查询挂载状态。
Mount media failed. The path of the image file does not exist or the image file is used by other program. Therefore, the image file cannot be opened.	镜像文件的路径不存在或文件被其他程序占用导致虚拟媒体挂载失败。	1. 检查镜像文件的路径是否存在。 2. 检查镜像文件是否被其他程序占用。 3. 检查镜像文件是否支持写入功能。

错误描述	原因	解决建议
The firmware upgrade has been completed,please manually restart the server to make it take effect and the download log failed	FwUpgrade升级已经完成，心跳异常断开没有下发结束标志，下载日志失败	<ul style="list-style-type: none"> 打开KVM观察界面。 界面如果显示Current Progress is 100%，说明升级固件已经成功需要手动重启服务器生效。

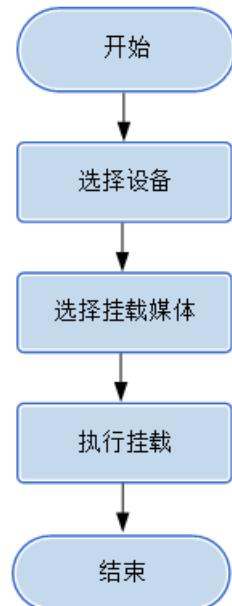
4.10 设备变更

本节指导用户使用工具箱通过自定义的程序修复服务器设备。

4.10.1 设备变更流程

设备变更流程如图4-117所示。

图 4-117 设备变更



4.10.2 使用前准备

使用工具前，您需要做以下准备工作，以保证工具的正常使用。

前提条件

- PC机和待操作的服务器BMC网络相通，保证IPMI、SNMP、SSH、VMM通信端口连通，保证能ping通服务器BMC的IP地址。
- 确保BMC已配置需使用的相关协议和端口，详细请参考[5.3 查看BMC端口信息](#)和[5.4 查看BMC的SNMP协议](#)。

数据

执行该操作前需准备以下数据：

- 服务器BMC管理网口IP地址。
- 服务器BMC用户名和密码。

4.10.3 选择设备

在设备变更向导的“选择设备”界面中，可以选择需要进行设备变更的设备，如果设备列表中不存在设备，也可以添加设备。

操作步骤

步骤1 在工具首页选择“升级/补丁>设备变更”。

系统进入“设备变更”向导界面。

步骤2 单击“选择设备”，在设备列表中选择需要变更的设备。

步骤3 如果列表中没有设备，单击“增加”进行添加。

系统弹出“增加设备”界面。

说明

批量导入设备方法：

1. 工具界面单击“设备列表>获取导入模板”，将模板文件“ServerDeviceList_Template”下载到本地。
2. 填写“ServerDeviceList_Template”内相关参数，各参数说明，如[表4-39](#)所示。
3. 工具界面单击“设备列表>批量导入”，选择设备列表文件“ServerDeviceList_Template”，单击“确定”即可完成批量导入设备。

步骤4 参考[表4-39](#)，手工输入参数。

表 4-39 参数说明

类型	名称	说明	备注
-	起始IP	搜索的起始服务器管理板IP地址或BMC的IP地址。	BMC的IP地址，此处IP地址支持IPv4和IPv6。

类型	名称	说明	备注
	结束IP	搜索的结束服务器管理板IP地址或BMC的IP地址。	<ul style="list-style-type: none"> 单台设备时，和“起始IP”相同，如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.2.2 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f434 多台连续IP地址设备时，IPv4需和“起始IP”前2个网段一致，用户名密码必须一致。IPv6需和“起始IP”前7个网段一致，用户名密码必须一致。如： IPv4： 起始 IP: 192.168.2.2 结束 IP: 192.168.5.254 IPv6： 起始 IP: 2017::f434 结束 IP: 2017::f439 多台非连续IP地址或用户名、密码不一致时，按照单台设备处理。 BMC的IP地址，此处IP地址支持IPv4和IPv6。
	用户名	BMC管理员用户名。	-
	密码	BMC板管理员密码。	-
	SNMPv3 加密密码	SNMPv3加密密码	<ul style="list-style-type: none"> 如果不填写，则使用登录设备的密码。 如果登录设备的密码和SNMPv3加密密码不一致，则必须填写此参数。 SNMPv3加密密码默认值请参考“账户清单”。
高级设置	SNMP端口	SNMP端口号。	默认值是161，以设备实际启用的端口号为准。
	IPMI端口	IPMI端口号。	默认值是623，以设备实际启用的端口号为准。
	SSH/SFTP端口	SSH/SFTP端口号。	默认值是22，以设备实际启用的端口号为准。
	VMM端口	VMM端口号。	默认值是8208，以设备实际启用的端口号为准。

类型	名称	说明	备注
	HTTPS端口	HTTPS端口号。	请忽略该参数，或者保持默认值。
OS选项	root密码	root用户密码。	请忽略该参数。

步骤5 单击“确定”，设备信息出现在列表中。

□ 说明

单击“增加”，可添加其他服务器或操作系统。

步骤6 勾选需要变更的设备。单击“确定”，返回向导界面。

----结束

4.10.4 设备变更

□ 说明

- 建议先尝试变更一台服务器，待没有问题后，再进行批量变更，批量操作的服务器数量建议不超过200台。
- 不支持在不同PC上运行工具，对同一台设备同时进行操作。
- 操作过程中遇到的问题请参考[4.10.5 常见问题处理](#)解决。

须知

- 操作过程中，请勿对服务器进行系统上下电及重启等操作。
- 请勿对升级过程中的设备进行设备变更。

操作步骤

步骤1 在设备变更向导界面单击“设备变更”。系统进入设备变更向导“欢迎”界面，如[图4-118](#)所示。

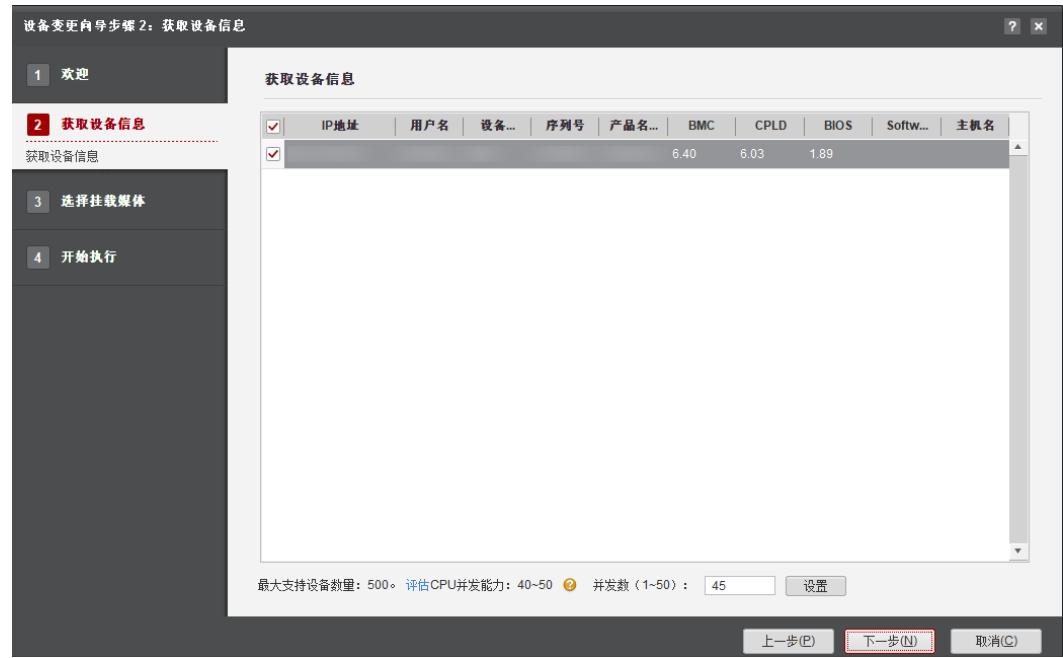
图 4-118 欢迎



步骤2 单击“下一步”。

进入“获取设备信息”界面, 如图4-119所示。

图 4-119 获取设备信息



说明

- 编辑并发数文本框可以设置在同一时刻能批量操作的服务器数量, 并发数可设置为1~50。
- CPU并发能力, 通过简单测试CPU性能, 预估建议并发能力范围值。测试结果与CPU占用率有关, 测试时间10秒。建议并发数设置在CPU并发能力评估范围内。

步骤3 在设备列表中勾选一台或者多台服务器。

步骤4 单击“下一步”。执行发现服务器操作。

□ 说明

单击“停止”可终止此次任务。

步骤5 发现服务器后系统自动进入选择服务器界面。单击“过滤设备”下拉框，可对发现的服务器进行筛选，快速选择需要进行操作的一类服务器。

步骤6 勾选需要挂载虚拟媒体的服务器，单击“下一步”。进入“选择挂载媒体”界面，如图4-120所示。

图 4-120 选择挂载媒体界面



□ 说明

- 同时挂载本地ISO文件和文件夹时，ISO文件要求Smart Provisioning版本为V125/1.2.0.4及以上。
- 请确认文件夹路径中包含对应的.asc数字签名。

步骤7 选择挂载媒体。

挂载媒体，可以单独挂载本地ISO/IMG文件或者本地文件夹，也可以同时挂载本地ISO/IMG文件和文件夹，具体操作如下：

- 如果是挂载ISO/IMG格式的文件：

单击“ISO/IMG文件”所在行的“选择”，选择本地的ISO/IMG文件，单击“下一步”。

□ 说明

- 勾选“挂载后重启服务器”，表示在虚拟媒体挂载之后服务器自动重启。
- 勾选“挂载后重启服务器”之后会自动勾选“设置从CD/DVD-ROM启动”。
- 可手动取消勾选“设置从CD/DVD-ROM启动”。
- 挂载的IMG文件需小于软驱标准容量1.44MB。

- 如果是挂载其他虚拟媒体：

单击“文件夹”所在行的“选择”，选择挂载文件所在的文件夹，单击“下一步”。

□ 说明

- 勾选“挂载后重启服务器”，表示在虚拟媒体挂载之后服务器自动重启。

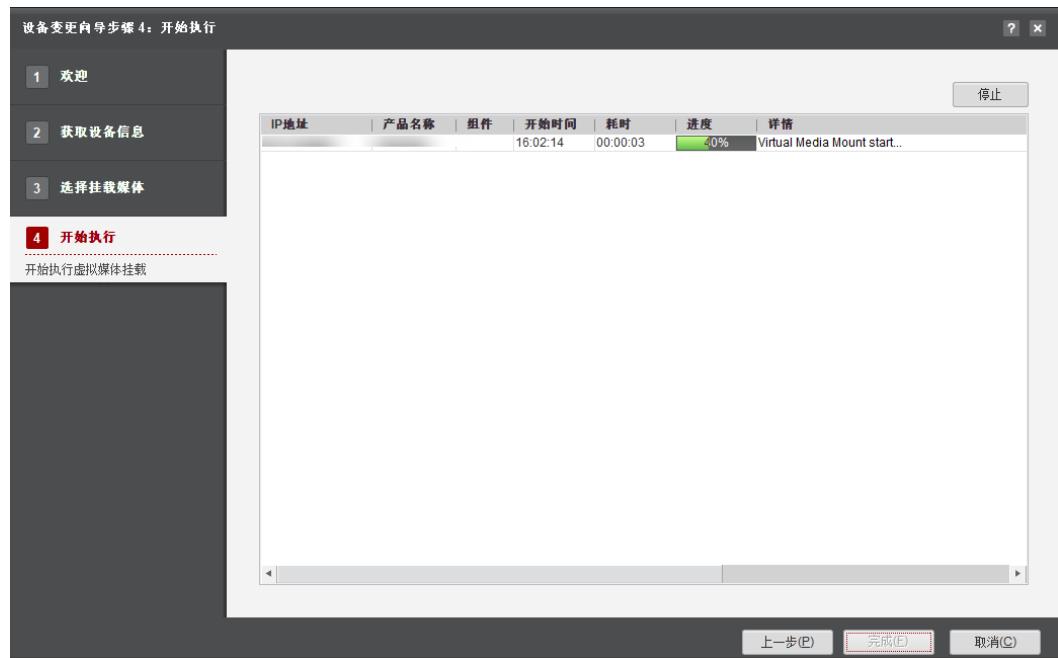
- 如果同时挂载本地ISO/IMG文件和文件夹可以用来执行自定义任务：
 - 服务器单击“ISO/IMG文件”所在行的“选择”，选择Smart Provisioning V125/1.2.0.4及以上版本的ISO文件。
 - 单击“文件夹”所在行的“选择”，选择含有task.py或者task.sh脚本的文件夹。
 - 设置任务超时时间，默认为600秒。
 - 单击“下一步”。

□ 说明

- task.py或者task.sh脚本模板获取地址：根目录\tools\ServerMain\template\VMConfig。
- 将自动勾选“挂载后重启服务器”，“设置从CD/DVD-ROM启动”和“任务完成后重启服务器”。
- 可手动勾选“数字签名验证”。

步骤8 选择挂载媒体操作结束后，单击“下一步”开始执行虚拟媒体挂载。如图4-121所示。

图 4-121 开始执行



□ 说明

单击“停止”可停止执行未开始挂载的设备。

步骤9 当进度条显示“100%”时，表示挂载完成，用户可在服务器BMC Web的远程虚拟控制台界面查看挂载的虚拟媒体。

步骤10 单击“完成”退出，向导界面显示成功和未执行的服务器台数，以及总用时。

----结束

4.10.5 常见问题处理

表 4-40 其他问题

错误描述	原因	解决建议
Host is unreachable	目标主机不可达。	检查待操作服务器的IP地址是否能ping通，或者配置文件是否写错。
User name or password error, account is locked or not an administrator.	用户名或密码错误，用户被锁定或不是管理员账户导致无法登录SSH。	检查用户名和密码是否能登录SSH；检查用户是否被锁定以及是否为管理员账户。
User name or password error	用户名或密码错误。	检查用户名和密码是否正确。
Too many authentication failures	用户被锁定导致无法登录SSH。	通过BMC Web界面查看用户状态。

错误描述	原因	解决建议
SNMP config error or unsupported server, please check the network, SNMP settings and the system configuration.	<ul style="list-style-type: none"> SNMP配置错误或服务器不支持SNMP命令。 SNMP未响应。 	<ol style="list-style-type: none"> 查看服务器是否支持运行工具。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查网络是否有异常，检查工具配置的SNMP端口及协议是否跟BMC的Web界面上一致，详细请参考5.3 查看BMC端口信息、5.4 查看BMC的SNMP协议。
SNMP command execute failed, please check support and try again later.	SNMP命令执行失败。	<ol style="list-style-type: none"> 确认该操作是否符合规范。 重新执行该操作。
Unsupported server	不支持该服务器。	查看服务器是否支持运行工具。
Username or password is invalid, can not use SNMP V3 protocol.	用户名或密码不符合SNMP要求。	<ol style="list-style-type: none"> 查看服务器是否在支持的服务器列表中。 参考5.4 查看BMC的SNMP协议查看服务器是否支持SNMP协议。 检查密码是否满足SNMP V3的要求，如长度至少8位字符。
Protocol conflict, waiting for next inspect(upgrade)...	服务器配置的SNMP V3协议不一致或用户名/密码不一致，引起巡检（升级）串行。	<ol style="list-style-type: none"> 检查所有服务器配置的SNMP V3协议是否一致，并将其调整一致。 检查所有服务器的用户名、密码是否一致，并将其调整一致。
Unable to establish LAN session, please check ipmi configuration and network.	无法建立会话，IPMI命令执行失败。	<ol style="list-style-type: none"> 手工执行IPMI命令，检查是否存在问题。 待问题解决后，重新执行该操作。
Task was aborted	任务被取消。	重新执行任务。
Activate Session command failed	启动会话命令失败。	<ol style="list-style-type: none"> 检查网络是否有异常。 重新执行任务。
User must be an administrator.	使用非管理员账户执行该操作。	<ol style="list-style-type: none"> 检查用户是否为管理员账户。 使用管理员账户重新执行该操作。

错误描述	原因	解决建议
Mount firmware image failed.	挂载升级镜像文件失败。	1. 查看服务器是否支持运行工具。 2. 检查是否已经挂载镜像文件，将其断掉后重新执行该操作。
Set firmware upgrade command failed, please try again later.	发送固件升级命令失败。	1. 查看服务器是否支持运行工具。 2. 稍后重新执行该操作。
Have same connect.	交换板有相同的SOL连接。	退出交换板SOL连接后，重新执行该操作。
Mount failed. The device is already mount, please unmount it first.	已挂载虚拟媒体导致此次挂载失败。	使用 <code>umount</code> 命令卸载已挂载的虚拟媒体后再进行挂载。
Mount media failed. Media file-path is not exists.	镜像文件的路径不存在。	检查镜像文件的路径是否存在。
Mount media failed. Media file-path can not read.	镜像文件不可读导致挂载失败。	添加镜像文件的读权限。
Unmount failed, no media was mounted.	未挂载虚拟媒体导致卸载失败。	先挂载虚拟媒体后再卸载。
Unmount media failed, the device is not found in the management list.	设备第一次添加，尚未进行过虚拟媒体挂载，不能进行卸载。	先挂载虚拟媒体后再卸载。
Query the mount status failed, the device is not found in the management list.	设备第一次添加，尚未进行过虚拟媒体挂载，不能查询挂载状态。	先挂载虚拟媒体后再查询挂载状态。
Mount media failed. The path of the image file does not exist or the image file is used by other program. Therefore, the image file cannot be opened.	镜像文件的路径不存在或文件被其他程序占用导致虚拟媒体挂载失败。	1. 检查镜像文件的路径是否存在。 2. 检查镜像文件是否被其他程序占用。 3. 检查镜像文件是否支持写入功能。
输入参数非法。	查询、设置操作时，输入的参数非法。	根据节点的参数定义，输入正确的参数。

错误描述	原因	解决建议
逻辑分区已处在下电状态, 请上电后操作。	逻辑分区处于下电状态下, 对逻辑分区进行下电、重启、强制重启、关闭等操作。	执行正确的上下电操作。
逻辑分区已处在上电状态, 请下电后操作	逻辑分区处于上电状态, 对逻辑分区进行上电操作。	执行正确的上下电操作。
逻辑分区处在上电状态, 不允许设置启动项	逻辑分区处于上电状态, 对该逻辑分区进行启动项设置操作。	逻辑分区下电状态下, 对启动项进行设置。
CD-ROM资源缺失。	挂载的ISO文件不存在。	<ol style="list-style-type: none">1. 将ISO文件上传到VMA的/temp/upgrade/clsftp/iso路径下。2. 确保输入的ISO文件名正确。
当前逻辑分区已插入光盘。	当前逻辑分区已经插入光盘, 再次执行插入光盘挂载ISO文件操作会失败。	先执行弹出光盘操作, 再重新执行插入光盘挂载ISO文件。
操作失败, 操作过于频繁, 请稍后再试。	插入弹出光盘操作过于频繁。	重新执行挂载或者重新执行卸载。
逻辑分区任务正在执行, 需要等待一段时间再操作。	执行逻辑分区相关操作后, 马上执行另一个操作。	稍后重新执行该操作。
逻辑分区当前状态不支持该操作, 请在关闭或运行状态下操作。	逻辑分区处于关闭或运行状态下执行插入光盘操作, 退出CD-ROM。	稍后重新执行该操作。

5 常见操作

- 5.1 查看RAID卡信息
- 5.2 查看BMC固件版本信息
- 5.3 查看BMC端口信息
- 5.4 查看BMC的SNMP协议
- 5.5 开启和配置IPv6功能

5.1 查看 RAID 卡信息

操作场景

本文以IE 11浏览器为例介绍在BMC Web界面中查看RAID卡信息。

必备事项

前提条件

本地电脑的IP地址与服务器BMC管理网口的IP地址在同一网段。

数据

执行该任务前需准备以下数据：

- 服务器BMC管理网口IP地址和子网掩码，此处IP地址支持IPv4和IPv6。
- 服务器BMC用户名和密码。

操作步骤

步骤1 打开IE浏览器，在地址栏中输入如下管理网口的IP地址：<https://BMC管理网口的IP地址>。

步骤2 查看BMC RAID卡信息。

1. 按“Enter”。
- 弹出安全告警窗口。

2. 单击“高级”展开“详情”。
3. 单击“继续前往*.**.**.** (不安全)”。
弹出登录界面。
4. 在BMC登录界面中，进行如下设置：
 - 选择界面语言。
 - 输入用户名和密码。
 - 选择登录到“这台BMC”。
 - 单击“登录”。
 进入BMC主界面。
5. 选择“系统管理>存储管理”。如图5-1所示。
可以查看RAID卡的逻辑ID、物理ID和对应的控制器信息。

图 5-1 存储管理界面

RAID Card1	
Disk0	添加 编辑
控制器信息	
名称	SAS3508
固件版本	5.140.00-3515
健康状态	正常
工作模式	RAID
内存大小	2048 MB
SAS地址	5440044443b6-6000
Cache Pinned状态	否
回弹	已禁用
JBOF模式	已禁用
类型	SAS3508
支持带外管理	是
支持的RAID级别	RAID0/1/5/6/10/50/60
配置版本	5.1400.00-0007
设备接口	SAS 12 Gb
支持的数据带宽大小范围	64 KB-1 MB
物理盘故障记忆	已启用
SMART错误计时回弹	已禁用

----结束

5.2 查看 BMC 固件版本信息

操作场景

本文以IE 11浏览器为例介绍在BMC Web界面中查看BMC的固件版本信息。

必备事项

前提条件

本地电脑的IP地址与服务器BMC管理网口的IP地址在同一网段。

数据

执行该任务前需准备以下数据：

- 服务器BMC管理网口IP地址和子网掩码，此处IP地址支持IPv4和IPv6。
- 服务器BMC用户名和密码。

操作步骤

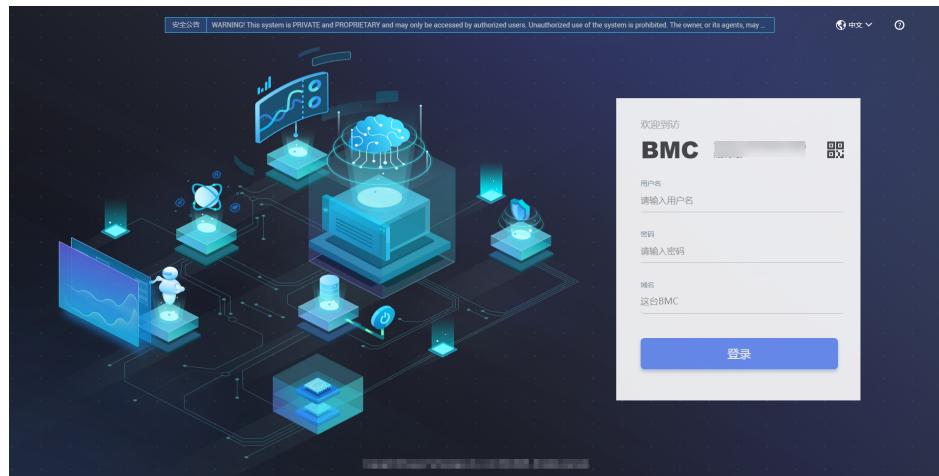
查看BMC固件版本信息。

1. 打开IE浏览器，在地址栏中输入“<https://BMC管理网口的IP地址>”。
2. 按“Enter”。

弹出安全告警窗口。

3. 单击“高级”展开“详情”。
4. 单击“继续前往*.**.**.** (不安全)”。
弹出登录界面。如图5-2所示。

图 5-2 登录 BMC



5. 在BMC登录界面中，进行如下设置：

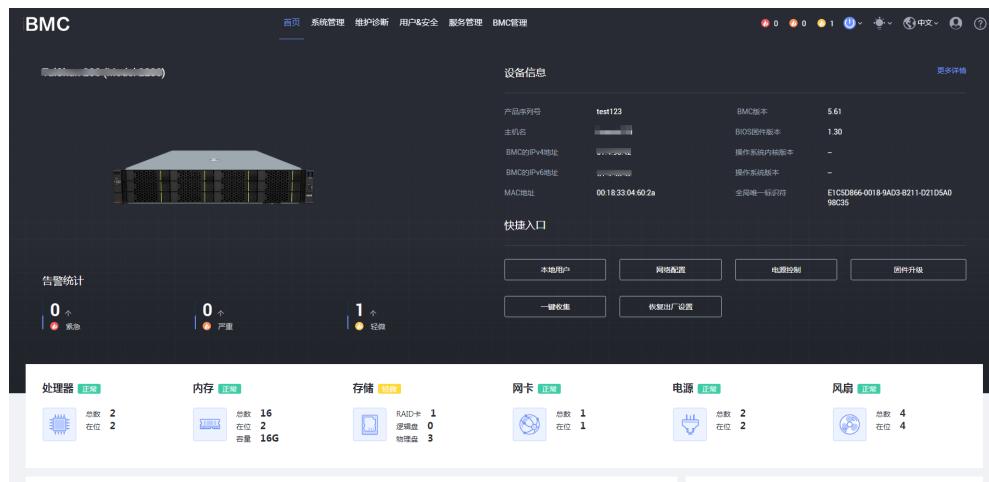
□ 说明

系统提供一个管理员用户组的缺省用户名和密码。

- 选择界面语言。
- 输入用户名和密码。
- 选择登录到“这台BMC”。
- 单击“登录”。

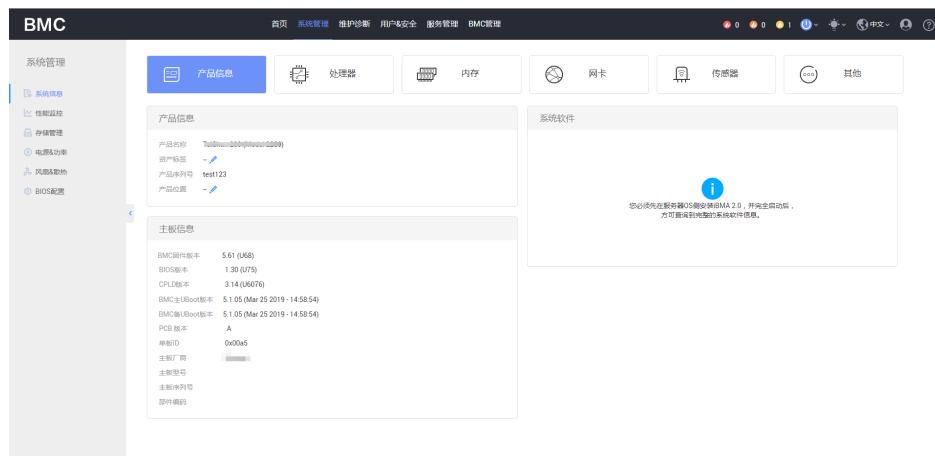
进入BMC主界面。如图5-3所示。

图 5-3 BMC 主界面



6. 选择“系统管理 > 系统信息 > 产品信息”。
进入“产品信息”界面，如图5-4所示。

图 5-4 产品信息界面



在“主板信息”栏可查看BMC的固件版本信息。

5.3 查看 BMC 端口信息

操作场景

本文以IE 11浏览器为例介绍在BMC Web界面中查看BMC的端口信息。

必备事项

前提条件

本地电脑的IP地址与服务器BMC管理网口的IP地址在同一网段。

数据

执行该任务前需准备以下数据：

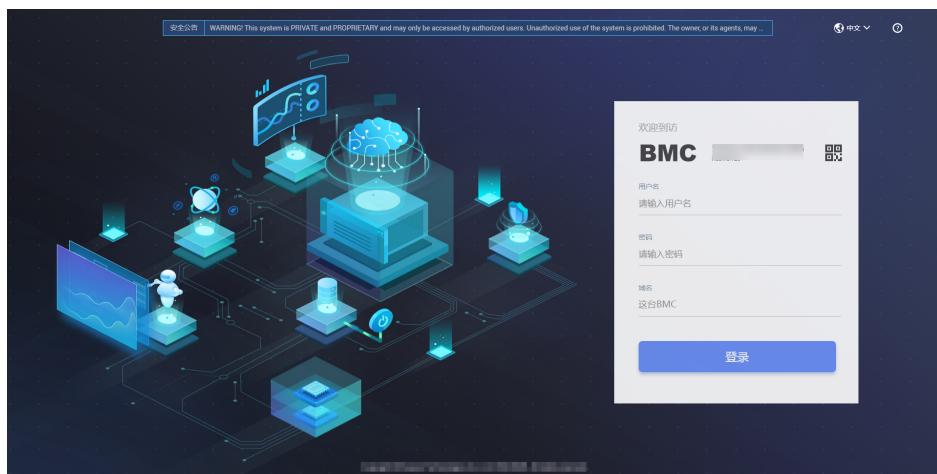
- 服务器BMC管理网口IP地址和子网掩码，此处IP地址支持IPv4和IPv6。
- 服务器BMC用户名和密码。

操作步骤

查看BMC端口信息。

1. 打开IE浏览器，在地址栏中输入“<https://BMC管理网口的IP地址>”。
2. 按“Enter”。
3. 弹出安全告警窗口。
4. 单击“高级”展开“详情”。
5. 单击“继续前往*.*.*.* (不安全)”。
弹出登录界面。如图5-5所示。

图 5-5 登录 BMC



5. 在BMC登录界面中，进行如下设置：

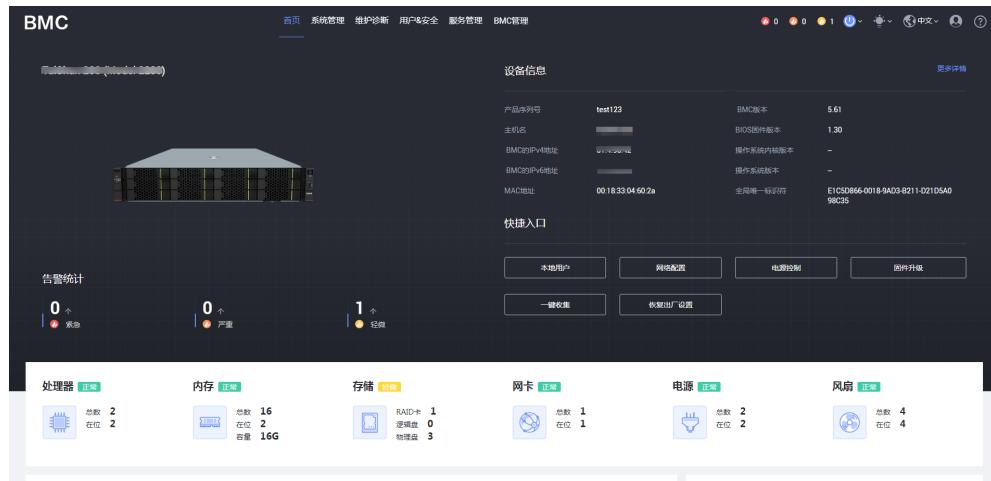
说明

系统提供一个管理员用户组的缺省用户名和密码。

- 选择界面语言。
- 输入用户名和密码。
- 选择登录到“这台BMC”。
- 单击“登录”。

进入BMC主界面。如图5-6所示。

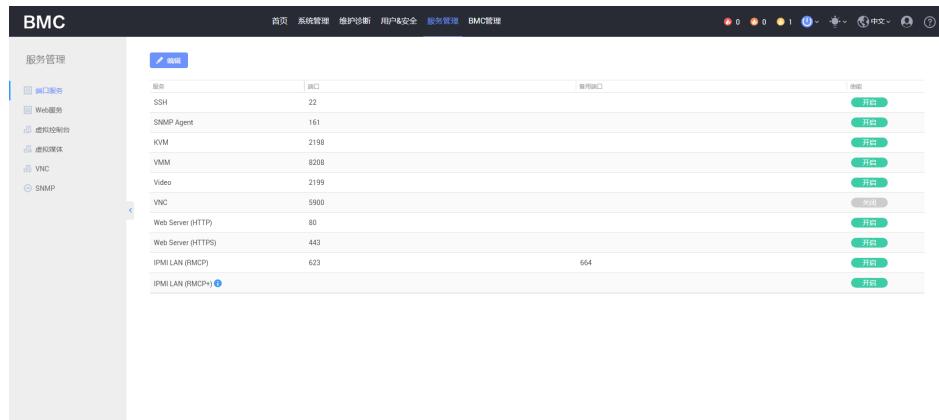
图 5-6 BMC 主界面



6. 选择“服务管理 > 端口服务”。

进入“端口服务”界面，可查看BMC端口信息，如图5-7所示。

图 5-7 BMC 端口信息



5.4 查看 BMC 的 SNMP 协议

操作场景

本文以IE 11浏览器为例介绍在BMC Web界面中查看BMC的SNMP协议。

必备事项

前提条件

本地电脑的IP地址与服务器BMC管理网口的IP地址在同一网段。

数据

执行该任务前需准备以下数据：

- 服务器BMC管理网口IP地址和子网掩码，此处IP地址支持IPv4和IPv6。

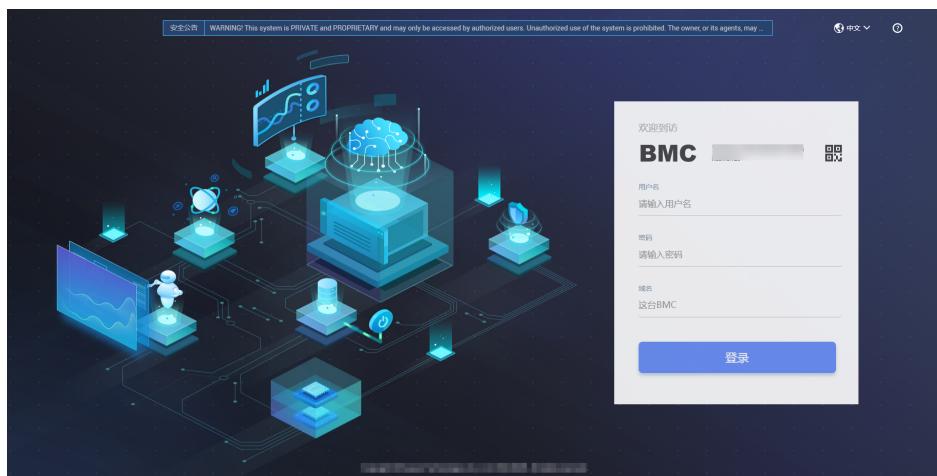
- 服务器BMC用户名和密码。

操作步骤

查看BMC的SNMP协议。

1. 打开IE浏览器，在地址栏中输入“<https://BMC管理网口的IP地址>”。
2. 按“Enter”。
3. 弹出安全告警窗口。
4. 单击“高级”展开“详情”。
5. 单击“继续前往*.*.*.* (不安全)”。
弹出登录界面。如图5-8所示。

图 5-8 登录 BMC



5. 在BMC登录界面中，进行如下设置：

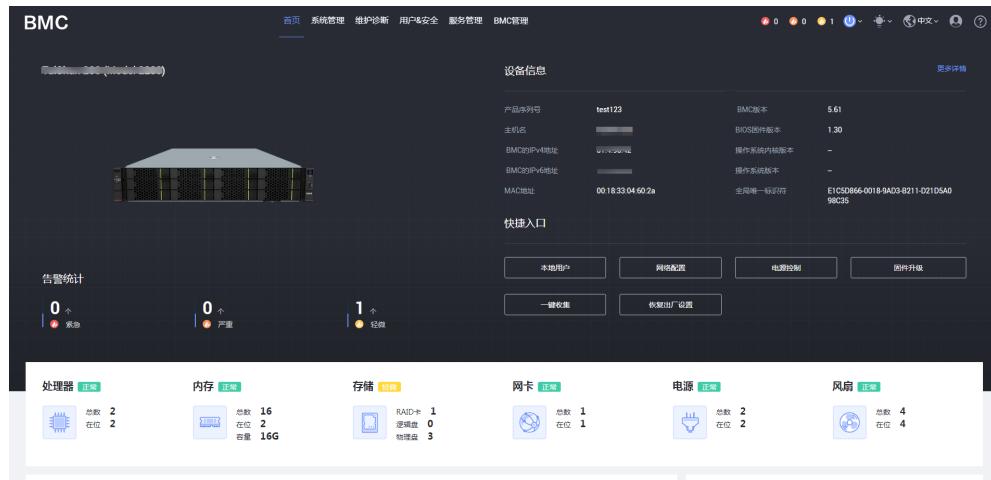
说明

系统提供一个管理员用户组的缺省用户名和密码。

- 选择界面语言。
- 输入用户名和密码。
- 选择登录到“这台BMC”。
- 单击“登录”。

进入BMC主界面。如图5-9所示。

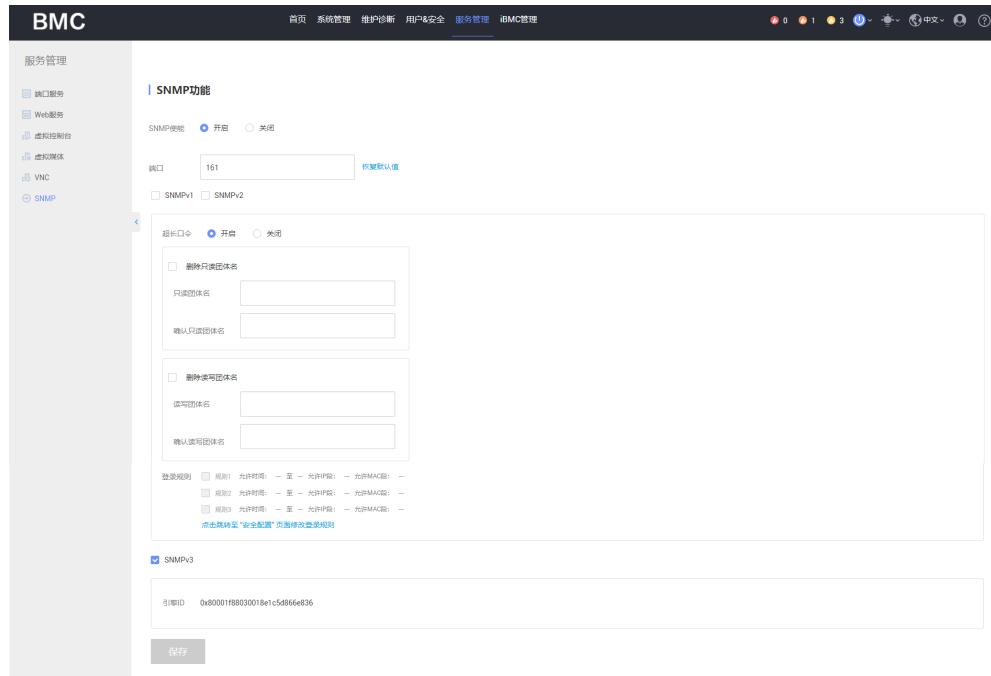
图 5-9 主界面



6. 选择“服务管理 > SNMP”。

进入“SNMP功能”界面，即可查看BMC支持的SNMP协议版本，如图5-10所示。涉及SNMP相关内容，请参见服务器 BMC用户指南。

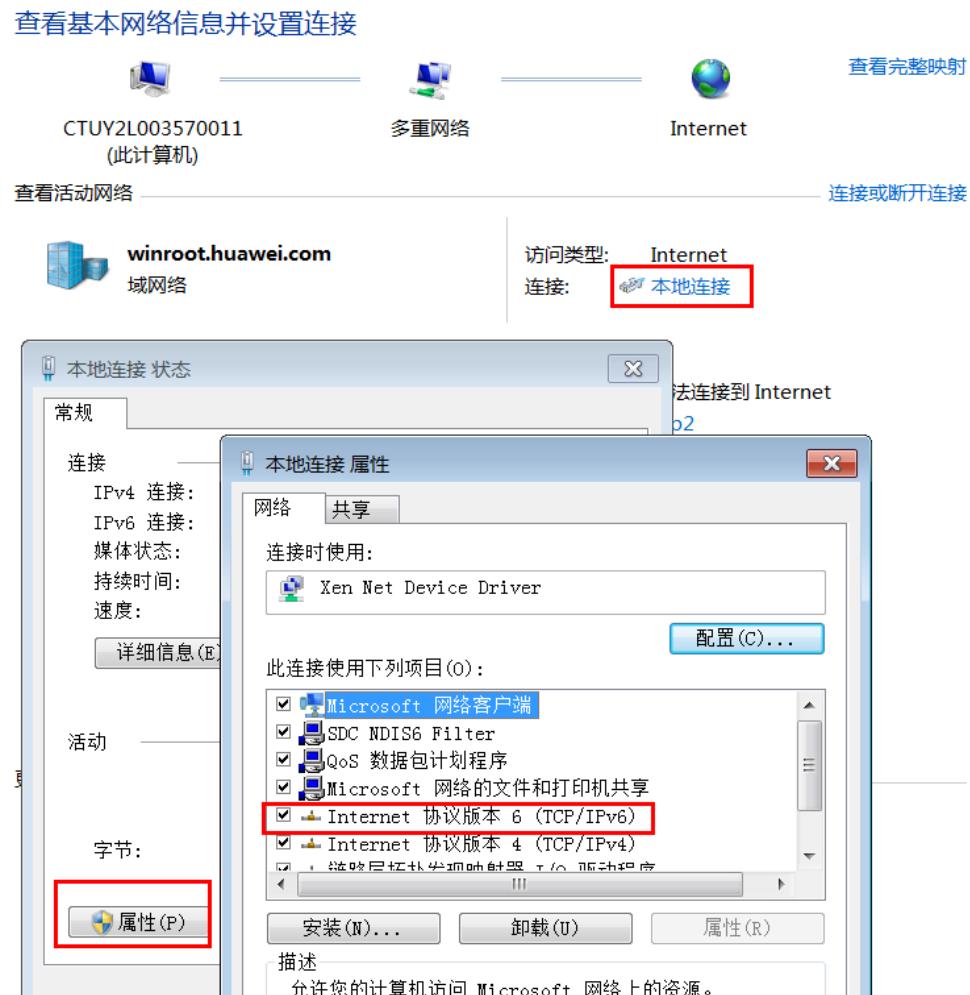
图 5-10 SNMP 功能界面



5.5 开启和配置 IPv6 功能

本节以Windows7为例进行说明如何开启和配置IPv6。

步骤1 打开网络和共享中心，选择“本地连接>属性”，确保IPv6协议已勾选。



步骤2 在cmd命令行通过“services.msc”命令，设置IP Helper的状态为“已启动”、启动类型为“自动”。

图 5-11 IP Helper



名称	描述	状态	启动类型	登录为
Google 更新服务 (gupdatem)	请确...	手动	本地系...	
Group Policy Client	该服...	已启...	自动	本地系...
HaccService		已启...	自动	本地系...
Health Key and Certificate Management	为网...	手动	本地系...	
HomeGroup Listener	使本...	手动	本地系...	
HomeGroup Provider	执行...	手动	本地服...	
Huawei HDP TraceLogC	Hua...	已启...	自动	本地系...
Huawei PV Driver Upgrade Tools	PV ...	已启...	自动	本地系...
Huawei UVP Monitor Tools	Mo...	已启...	自动	本地系...
Human Interface Device Access	启用...	手动	本地系...	
iDeskService		已启...	自动	本地系...
IdpCacheService	IDP...	已启...	自动	本地系...
IdpDataTraceService3.5		已启...	自动	本地系...
IdpUpgradeService	Idp...	已启...	自动	本地系...
IKE and AuthIP IPsec Keying Modules	IKEE...	已启...	自动	本地系...
Intel Local Scheduler Service		已启...	自动	本地系...
Intel PDS		已启...	自动	本地系...
Internet Connection Sharing (ICS)	为家...	手动	本地系...	
Internet Explorer ETW Collector Service	ET...	手动	本地系...	
IP Helper	使用...	已启...	自动	本地系...
IPsec Policy Agent	Inte...	已启...	手动	网络服...
KtmRm for Distributed Transaction Coordinator	协调...	手动		网络服...

步骤3 在cmd命令行通过“regedit”命令，找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters”。将“DisabledComponents”变量的值设置为0。

图 5-12 DisabledComponents



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
Dhcpv6DUID	REG_BINARY	00 01 00 01 1d 40
DisabledComponents	REG_DWORD	0x00000000 (0)

步骤4 重启PC。

步骤5 在cmd命令行通过“ipconfig”命令查看本地连接下是否存在IPv6地址，存在表示开启成功。

说明

如果IPv6开启后，IP配置依旧失败并且报无法连接的错误，请尝试禁用无关网络后再配置。

步骤6 开启成功后，再次打开网络和共享中心，选择“本地连接>属性>Internet 协议版本6 (TCP/IPv6) >属性”配置IPv6地址。如果PC机和服务器之间能够通信表示配置成功。

---结束