



# 浪潮英信服务器 BMC 配置手册

文档版本 V2.8

发布日期 2022-10-27

版权所有© 2021-2022 浪潮电子信息产业股份有限公司。保留一切权利。

未经本公司事先书面许可，任何单位和个人不得以任何形式复制、传播本手册的部分或全部内容。

## 内容声明

您购买的产品、服务或特性等应受浪潮集团商业合同和条款的约束。本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，浪潮集团对本文档的所有内容不做任何明示或默示的声明或保证。文档中的示意图与产品实物可能有差别，请以实物为准。本文档仅作为使用指导，不对使用我们产品之前、期间或之后发生的任何损害负责，包括但不限于利益损失、信息丢失、业务中断、人身伤害，或其他任何间接损失。本文档默认读者对服务器产品有足够的认识，获得了足够的培训，在操作、维护过程中不会造成个人伤害或产品损坏。文档所含内容如有升级或更新，恕不另行通知。

## 商标说明

Inspur 浪潮、Inspur、浪潮、英信是浪潮集团有限公司的注册商标。  
本手册中提及的其他所有商标或注册商标，由各自的所有人拥有。

## 技术支持

技术服务电话：4008600011


地 址：中国济南市浪潮路 1036 号





浪潮电子信息产业股份有限公司

邮 编：250101

## 符号约定

在本文中可能出现下列符号，它们所代表的含义如下。

符号	说明
 危险	如不当操作，可能会导致死亡或严重的人身伤害。

符号	说明
 警告	如不当操作，可能会导致人员损伤。
 注意	如不当操作，可能会导致设备损坏或数据丢失。
 提示	为确保设备成功安装或配置，而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。

## 变更记录

版本	时间	变更内容
V1.0	2021-02-07	首版发布。
V2.0	2021-06-25	格式内容整体优化。
V2.1	2021-09-01	增加因机型不同，Web界面及个别功能或有差异的说明。
V2.2	2021-09-20	新增4款产品型号到表格1-1产品型号列表。
V2.3	2021-11-15	新增2款产品型号到表格1-1产品型号列表。
V2.4	2022-01-21	更新扉页和前言的内容。
V2.5	2022-03-05	统一所有表格的宽度。
V2.6	2022-06-06	新增2款产品型号到表格1-1产品型号列表。
V2.7	2022-09-24	更新2.3章节标题的名字。
V2.8	2022-10-27	优化部分表格内文字的格式。

# 目 录

1	概述 .....	1
1.1	文档用途 .....	1
1.2	目标读者 .....	1
1.3	适用范围 .....	1
2	管理网口 IP 地址查询 .....	3
2.1	功能特性 .....	3
2.2	BIOS 下获取管理网口 IP .....	3
2.3	Linux 下获取管理网口 IP .....	5
3	用户管理 .....	7
3.1	功能特性 .....	7
3.2	用户精细化配置 .....	7
3.3	获取用户列表 .....	10
3.4	增加用户 .....	10
3.5	更改用户 .....	13
3.6	删除用户 .....	15
4	网络设置 .....	17
4.1	功能特性 .....	17
4.2	获取网络配置 .....	17
4.3	共享网卡配置 .....	19
4.4	网络 IP 设置 .....	21
4.5	VLAN 设置 .....	23
4.6	DNS 设置 .....	23

5	风扇管理.....	26
5.1	功能特性.....	26
5.2	风扇自动设置.....	26
5.3	风扇手动设置.....	27
6	日志收集.....	28
6.1	功能特性.....	28
6.2	操作指导.....	28
6.3	Syslog 日志设置.....	28
7	BMC 时间设置.....	31
7.1	功能特性.....	31
7.2	NTP 自动同步.....	31
8	SNMP Trap 告警设置.....	34
8.1	功能特性.....	34
8.2	SNMP Trap 设置.....	34
9	邮箱告警.....	36
9.1	功能特性.....	36
9.2	邮箱告警设置.....	36
10	BMC 服务设置.....	39
10.1	功能特性.....	39
10.2	服务设置.....	39
11	存储管理.....	42
11.1	功能特性.....	42
11.2	逻辑盘的创建.....	42
11.3	逻辑盘的其他操作.....	44

12	固件升级.....	45
12.1	功能特性.....	45
12.2	操作指导.....	45
13	恢复出厂设置.....	46
13.1	功能特性.....	46
13.2	恢复出厂设置.....	46
14	SSL 设置.....	48
14.1	功能特性.....	48
14.2	在线生成 SSL 凭证.....	48
14.3	生成 SSL 凭证并上传.....	50
15	Redfish.....	53
15.1	概述.....	53
15.2	操作指导.....	53
16	进入 BIOS 系统.....	54
16.1	功能特性.....	54
16.2	本地进入 BIOS 系统.....	54
17	设置 U-Boot 密码.....	56
17.1	功能特性.....	56
17.2	Linux 下修改 U-Boot 密码.....	56
18	常用工具.....	57
18.1	IPMITOOL 介绍.....	57
18.1.1	用途及使用场景.....	57
18.1.2	Linux 下 IPMITOOL 的安装与使用.....	57
18.2	openssl 介绍.....	58

18.2.1 用途及使用场景 .....	58
18.2.2 Linux 下的 openssl 安装和使用 .....	58

# 1 概述

## 1.1 文档用途

本文档详细介绍 BMC 的相关功能的配置流程和方法, 相关技术人员能够通过此文档清楚相关功能的具体配置流程和方法。

## 1.2 目标读者

本手册主要适用于以下人员:

- 技术支持工程师
- 产品维护工程师
- 服务器管理用户

建议由具备服务器知识的专业工程师参考本手册进行服务器运维操作。



注意

部分用于生产、装备、返厂检测维修的接口、命令, 定位故障的高级命令, 如使用不当, 将可能导致设备异常或者业务中断, 故不在本资料中说明。如需要, 请向浪潮申请。

---

## 1.3 适用范围

本手册适用于以下产品:

表 1-1 产品型号列表

产品型号	两路服务器	四路服务器	AI服务器	多节点服务器
浪潮英信服务器NF8260M6		●		
浪潮英信服务器NF8480M6		●		
浪潮英信服务器NF5280M6	●			
浪潮英信服务器NF5180M6	●			
浪潮英信服务器NF5270M6	●			
浪潮英信服务器NF5260M6	●			



产品型号	两路服务器	四路服务器	AI服务器	多节点服务器
浪潮英信服务器NF5466M6	●			
浪潮英信服务器NF5266M6	●			
浪潮英信服务器NF5468M6	●		●	
浪潮英信服务器NF5488M6	●		●	
浪潮英信服务器NF5688M6	●		●	
浪潮英信服务器i24M6	●			●
浪潮英信服务器i48M6	●			●
浪潮英信服务器SA5280M6	●			
浪潮英信服务器SA5112M6	●			
浪潮英信服务器SA5270M6	●			
浪潮英信服务器SA5212M6	●			
浪潮英信服务器SN5160FM6	●			
浪潮英信服务器SN5264FM6	●			
浪潮英信服务器i24LM6	●			●
浪潮英信服务器NF5260FM6	●			



### 说明

因机型不同，Web 界面及个别功能或有差异，请以实际使用机型展示效果为准。

---

# 2 管理网口 IP 地址查询

## 2.1 功能特性

BMC 支持通过专用口以及共享口进行访问。在使用前需要先知道 BMC 管理口的 IP 地址。管理网口的 IP 可以通过在 BIOS Setup 界面下查看,也可以通过在 Linux 系统下,通过 ipmitool 进行查看。

## 2.2 BIOS 下获取管理网口 IP

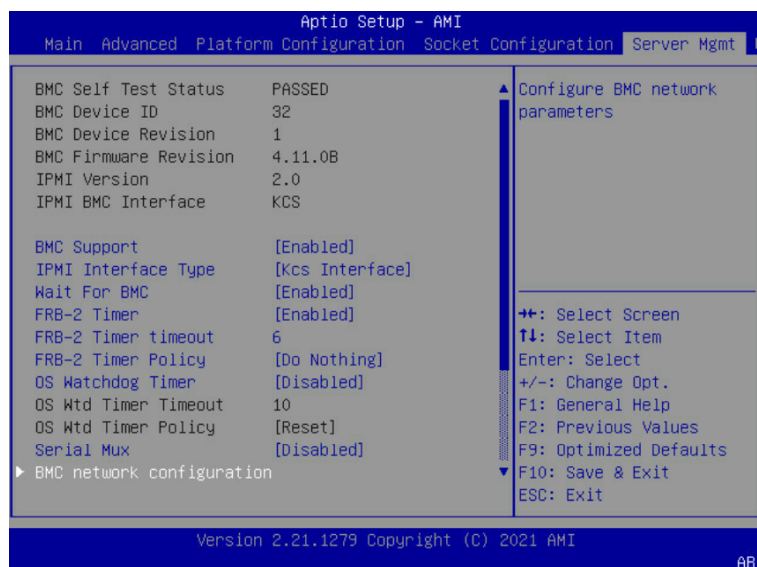
操作场景:

指导您通过 BIOS 获取管理网口的 IP。

操作步骤:

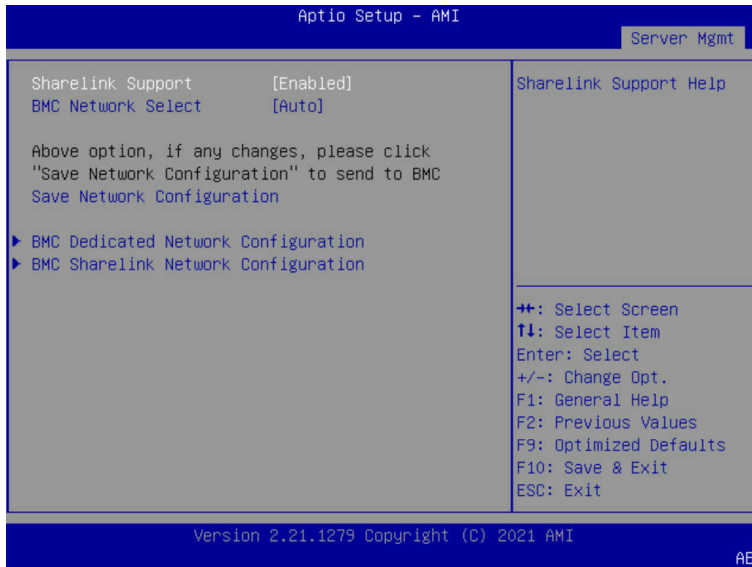
1. 进入 BIOS Setup 界面,具体操作说明请参见 [16.2 进入 BIOS Setup 界面](#)。
2. 选择 Server Mgmt 界面,如下图所示。

图 2-1 Server Mgmt 界面



3. 选择“BMC network configuration”,按“Enter”进入,如下图所示。

图 2-2 BMC network configuration 界面



4. 选择“BMC Dedicated Network Configuration”或“BMC Sharelink Network Configuration”，按“Enter”进入，可查看当前 BMC Dedicated 和 BMC Sharelink 网络参数的配置情况，如图 2-3、图 2-4 所示。通过这个界面就能够看到管理网口目前的 IP 地址。

图 2-3 BMC Dedicated Network Configuration 界面

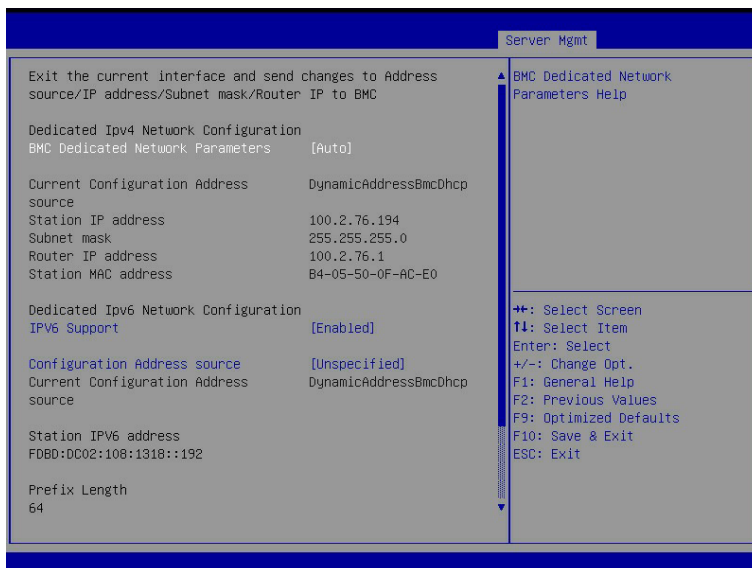
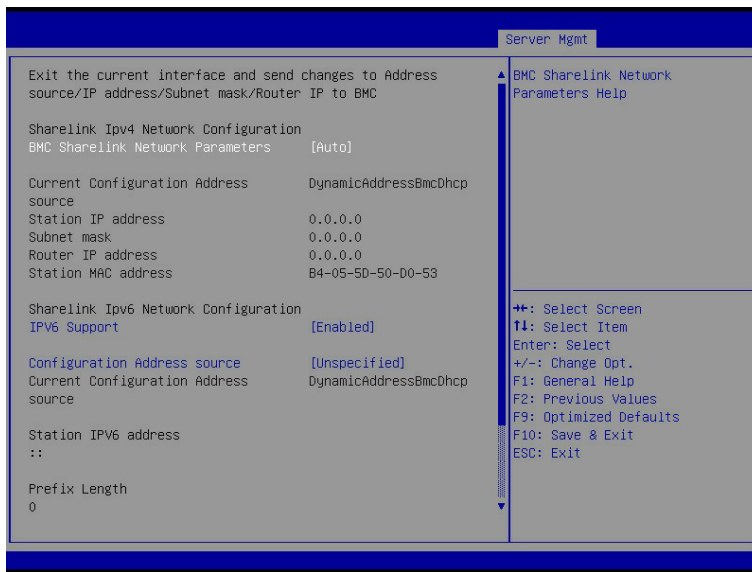


图 2-4 BMC Sharelink Network Configuration 界面



## 2.3 Linux 下获取管理网口 IP

操作场景：

指导您在 Linux 系统下获取 BMC 管理口的 IP 地址。

操作步骤：

1. 安装 ipmitool 工具，具体操作说明请参见 [18.1 IPMITOOL 介绍](#)。
2. 使用命令 “ipmitool lan print 1” 返回专用口的 IP 地址，使用命令 “ipmitool lan print 8” 返回共享口的 IP 地址。如下图所示，为获取专用口 IP 地址的命令截图。

图 2-5 获取 BMC 专用口的 IP 地址

```
[root@localhost ~]# ipmitool lan print 1
Set in Progress      : Set Complete
Auth Type Support   :
Auth Type Enable    : Callback :
                   : User      :
                   : Operator :
                   : Admin   :
                   : OEM     :
IP Address Source   : DHCP Address
IP Address          : 100.2.76.64
Subnet Mask         : 255.255.255.0
MAC Address        : 6c:92:bf:56:2c:9c
SNMP Community String : AMI
IP Header           : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control     : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Interval : 0.0 seconds
Default Gateway IP  : 100.2.76.1
Default Gateway MAC : 00:74:9c:e5:d7:4f
Backup Gateway IP   : 0.0.0.0
Backup Gateway MAC  : 00:00:00:00:00:00
B02.1q VLAN ID     : Disabled
B02.1q VLAN Priority : 0
RMCP+ Cipher Suites : 0,1,2,3,6,7,8,11,12,15,16,17
Cipher Suite Priv Max : caaaaaaaaaXX
                   : X=Cipher Suite Unused
                   : c=CALLBACK
                   : u=USER
                   : o=OPERATOR
                   : a=ADMIN
                   : 0=OEM
Bad Password Threshold : 3
Invalid password disable: yes
Attempt Count Reset Int.: 200
User Lockout Interval  : 300
[root@localhost ~]#
```

# 3 用户管理

## 3.1 功能特性

用户管理功能主要用来展示 BMC 所有用户信息，包括用户名、用户组、用户操作权限等等，并提供用户增删、修改信息等操作。

## 3.2 用户精细化配置

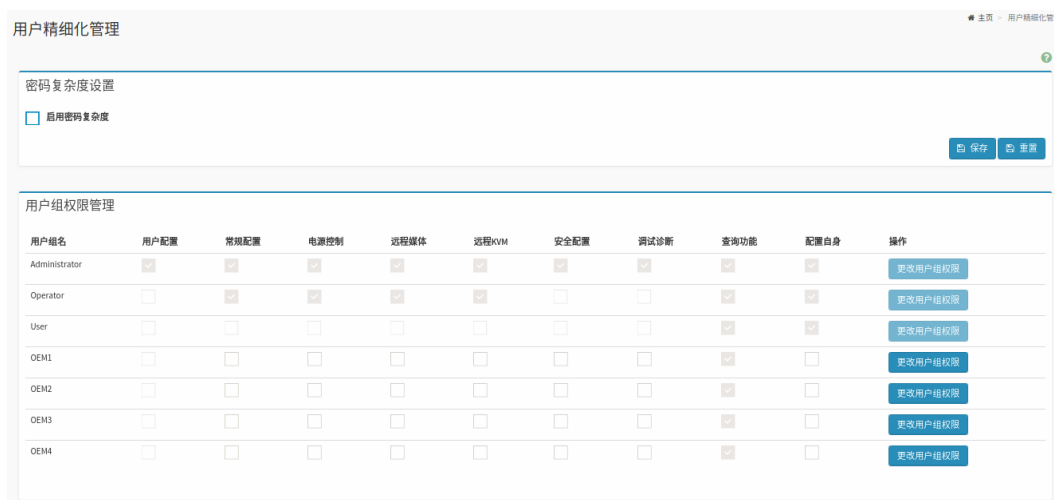
操作场景：

指导您通过 Web 界面进行用户精细化管理配置。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>用户精细化管理”页面，如下图所示。系统提供对不同用户组的精细化配置管理，用户可以对不同的用户组设置相应的操作权限。

图 3-1 用户精细化管理



2. 如果需要启用复杂密码，请勾选“启用密码复杂度”复选框；如果不需要启用，则不勾选这个复选框，然后点击保存按钮。对于表格的字段描述，可以参考[表格 3-1](#) 密码复杂度设置。点击启用复选框后，会弹出如下图所示的页面。

图 3-2 用户精细化管理密码复杂度设置页面

## 用户精细化管理 ?

🏠 主页 > 用户精细化管理

启用密码复杂度

密码最小长度  8~16

启用复杂度

密码有效期(天)  取值范围(0-90),单位(天),0表示无期限

历史密码记录  0~5

登录失败重试次数  0~5

锁定时长(分钟)  (5~60 min)

保存
重置

3. 系统缺省用户组 Administrator、Operator 和 User 无法进行用户权限修改。其它四个定制化用户组 OEM1、OEM2、OEM3、OEM4，可以进行权限修改。选择需要的权限，然后点击“更改用户组权限”按钮生效。用户组的权限以及权限描述请参考[表格 3-2](#)和[表格 3-3](#)。

精细化用户管理相关权限配置参数如下表所示：

表 3-1 密码复杂度设置

参数	描述
启用密码复杂度	<ul style="list-style-type: none"> <li>勾选，启用密码复杂度</li> <li>不勾选，不启用密码复杂度限制</li> </ul>
密码最小长度	默认为8，可设置8~16之间的数字。
启用复杂度	<ul style="list-style-type: none"> <li>勾选，启用复杂度可设置密码复杂度的细节，可选择大写字母、小写字母、数字、特殊字符。如需要密码中必须包含大写字母时，勾选大写字母即可</li> </ul>

参数	描述
	<ul style="list-style-type: none"> <li>不勾选，不启用密码复杂度限制</li> </ul>
密码有效期（天）	可设置密码的生效时间，超过生效时间用户将禁止登录。单位：天。
历史密码记录	可设置历史密码记录中保存的条数，最多5条，历史密码将被禁止重新使用。历史密码记录0~5。
登录失败重试次数	可设置用户登录失败时重试的最多次数，最多5次，登录失败后用户将被锁定。登录失败重试次数0~5。
锁定时长（分钟）	默认为5。可设置5~60。锁定时长结束后方可再次登录。

表 3-2 用户组权限管理

用户组	权限
管理员	用户配置、常规配置、电源控制、远程媒体、远程KVM、安全配置、调试诊断、查询功能、配置自身。
操作员	常规配置、电源控制、远程媒体、远程KVM、查询功能、配置自身。
用户	查询功能、配置自身。
OEM*	OEM1、OEM2、OEM3、OEM4用户是预留给自定义权限的用户组，默认具有查询功能和配置自身权限，其他权限可通过勾选进行配置。

表 3-3 权限对应功能描述

权限	描述
用户配置	用户组权限管理、用户管理、服务会话、一般LDAP设定、角色群组。
常规配置	DNS配置、密码复杂度设置、IDL日志清除、系统事件日志清除、服务配置、一般防火墙设置、IP地址防火墙规则、端口防火墙规则、日期&时间、PAM顺序、保存配置、SEL日志设置策略、Syslog日志设置、SNMP trap设置、SNMP set/get设置、邮箱告警、传感器阈值、HPM固件更新、固件镜像位置、恢复出厂设置、还原配置、前控制面板电源键设置、风扇管理、网络自适应配置、共享网卡配置、网络绑定配置、网络IP设置、BIOS启动选项。
电源控制	电源控制。
远程媒体	KVM鼠标设置、本地镜像、远程镜像、一般设置、VMedia实体装置设置、远程会话、VNC、主动重定向。



权限	描述
远程KVM	H5Viewer, JViewer。
安全配置	生成SSL凭证、上传SSL凭证、系统管理员、审计日志。
调试诊断	宕机截屏、手动截屏、视频触发设置、视频远程存储、Pre-Event视频录制、模块重启、一键收集日志。
查询功能	可以登录以及查看除安全配置外的其他信息。
配置自身	可以配置账户自身的密码、电子邮箱以及管理ssh公钥。

### 3.3 获取用户列表

操作场景：

指导您通过 Web 管理界面获取用户列表。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>用户精细化管理”页面，当前存在用户将在用户精细化管理界面显示出来，如下图所示。对于已经存在的用户，点击操作栏的“更改用户”按钮或“删除用户”按钮可进行相应操作。空白行右侧操作栏点击“添加用户”按钮可添加用户。

图 3-3 用户列表

用户管理						
用户ID	用户名	用户组	用户权限	IPMI权限	电子邮箱ID	操作
1	admin	Administrator	已启用	administrator		更改用户 删除用户
2						添加用户
3						添加用户
4						添加用户
5						添加用户
6						添加用户
7						添加用户
8						添加用户
9						添加用户
10						添加用户
11						添加用户
12						添加用户
13						添加用户
14						添加用户
15						添加用户
16						添加用户

### 3.4 增加用户

操作场景：

指导您通过 Web 管理界面增加用户。

操作步骤：

1. 在用户精细化管理界面中，点击空白行右侧“添加用户”按钮，进入新增用户配置界面，如下图所示。

图 3-4 添加用户配置页面

The screenshot shows a web form titled "用户管理配置" (User Management Configuration). The form contains the following fields and controls:

- 用户名 \*** (Username): A text input field containing "test".
- 新密码 \*** (New Password): A password input field with masked characters "\*\*\*\*".
- 确认密码 \*** (Confirm Password): A password input field with masked characters "\*\*\*\*".
- 用户启用** (User Enabled): A checkbox labeled "启用" (Enabled), which is currently unchecked.
- 用户组 \*** (User Group): A dropdown menu with "Operator" selected.
- 电子邮件格式** (Email Format): A dropdown menu.
- 电子邮件 ID** (Email ID): A text input field.
- 现有的 SSH Key** (Existing SSH Key): A text area containing "Not Available".
- 上传 SSH 密钥** (Upload SSH Key): A text input field with a file upload icon and "..." next to it.
- 保存** (Save): A blue button at the bottom right.

增加用户配置参数表如下所示：

表 3-4 用户配置参数

参数	描述
用户名	<p>输入新用户的用户名。</p> <ul style="list-style-type: none"> <li>用户名由1-16个字符组成，包括字母、数字、“-”、“_”、“@”，必须以字母开头，区分大小写。</li> <li>不允许出现特殊字符，例如“,”(逗号)、“.”(句号)、“:”(冒号)、“;”(分号)、“ ”(空格)、“/”(斜线)、“\”(反斜线)、“(”(左括号)和“)”(右括号)等。</li> <li>sshd、ntp、stunnel4、sysadmin、daemon是保留用户名，不能使用。</li> </ul>
新密码	<p>输入并确认新密码。</p> <ul style="list-style-type: none"> <li>密码复杂度检查禁用时，密码至少1个字符，并且不允许有空格。</li> <li>密码复杂度检查启用时，密码必须包含特殊字符，大写字母，小写字母和数字，至少8个字符，并且不允许有空格。</li> </ul> <p>提示：不允许密码长度超过16个字符。</p>
密码确认	重新输入新密码。
用户启用	选择复选框，启动用户访问权限。
用户组	选择一个用户组，为用户分配权限。
电子邮件格式	<p>指定电子邮件格式。此格式将会在传送电子邮件时使用。两种格式皆可使用：</p> <ul style="list-style-type: none"> <li>AMI-格式：电子邮件格式标题为“Alert from (your Hostname)”。此封邮件会显示传感器信息，例如：传感器类型和描述</li> <li>FixedSubject-格式：此格式根据用户的设置显示消息。您必须设置电子邮件通知的主题和消息</li> </ul>
电子邮件ID	<p>输入用户的电子邮箱ID，如果用户忘记了密码，新密码会发送到处配置的电子邮箱ID中。</p> <p>提示：必须配置SMTP服务器，才能发送电子邮件。</p>
现有的SSH Key	将显示已上传的SSH密钥信息（只读）。
上传SSH密钥	<p>使用“浏览”按钮导航到SSH的公共密钥文件。</p> <p>SSH密钥文件是.pub类型。</p>

2. 填写完相应的用户配置信息之后，点击“保存”按钮；添加成功后返回到用户列表页面，可以查看用户列表中已经显示刚添加的用户信息，如下图所示。

图 3-5 新用户信息展示

用户ID	用户名	用户组	用户启用	IPMI权限	电子邮箱ID	操作
1	admin	Administrator	已启用	administrator		<a href="#">更改用户</a> <a href="#">删除用户</a>
2	test	Operator	未启用	operator		<a href="#">更改用户</a> <a href="#">删除用户</a>
3						<a href="#">添加用户</a>
4						<a href="#">添加用户</a>
5						<a href="#">添加用户</a>
6						<a href="#">添加用户</a>
7						<a href="#">添加用户</a>
8						<a href="#">添加用户</a>
9						<a href="#">添加用户</a>
10						<a href="#">添加用户</a>
11						<a href="#">添加用户</a>
12						<a href="#">添加用户</a>
13						<a href="#">添加用户</a>
14						<a href="#">添加用户</a>
15						<a href="#">添加用户</a>
16						<a href="#">添加用户</a>

## 3.5 更改用户

操作场景：

指导您通过 Web 管理界面更改用户。

操作步骤：

1. 在用户列表展示页面点击要更改的用户信息行并点击右侧“更改用户”按钮，如下图所示。

图 3-6 选定需要修改的用户信息

用户管理						
用户ID	用户名	用户组	用户启用	IPMI权限	电子邮箱ID	操作
1	admin	Administrator	已启用	administrator		<a href="#">更改用户</a> <a href="#">删除用户</a>
2	test	Operator	未启用	operator		<a href="#">更改用户</a> <a href="#">删除用户</a>
3						<a href="#">添加用户</a>
4						<a href="#">添加用户</a>
5						<a href="#">添加用户</a>
6						<a href="#">添加用户</a>
7						<a href="#">添加用户</a>
8						<a href="#">添加用户</a>
9						<a href="#">添加用户</a>
10						<a href="#">添加用户</a>
11						<a href="#">添加用户</a>
12						<a href="#">添加用户</a>
13						<a href="#">添加用户</a>
14						<a href="#">添加用户</a>
15						<a href="#">添加用户</a>
16						<a href="#">添加用户</a>

2. 页面显示当前用户相关配置信息，可在页面对相关信息进行修改，点击“保存”按钮进行保存，如下图所示。返回用户列表页面可以查看修改是否生效。

图 3-7 修改用户信息

用户管理配置 ?

用户名 \*

test0001

修改密码

请输入当前用户密码: \*

\*\*\*\*\*

新密码 \*

\*\*\*\*\*

确认密码 \*

\*\*\*\*\*

用户启用

启用

用户组 \*

Administrator

电子邮件格式

AMI-格式

电子邮件 ID

\*\*\*\*\*

现有的 SSH Key

Not Available

上传 SSH 密钥

.....

删除

保存

## 3.6 删除用户

操作场景：

指导您通过 Web 管理界面删除用户。

操作步骤：

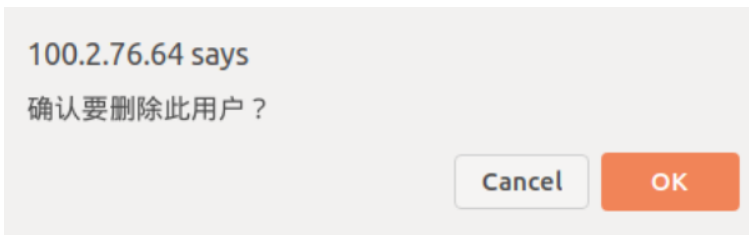
1. 首先在用户列表页面选择需要删除的用户信息行，再点击右侧“删除用户”按钮，如下图所示。

图 3-8 删除指定用户

用户管理						
用户ID	用户名	用户组	用户启用	IPMI权限	电子邮箱ID	操作
1	ADMIN	Administrator	已启用	administrator		<a href="#">更改用户</a> <a href="#">删除用户</a>
2	test0001	Administrator	已启用	administrator		<a href="#">更改用户</a> <a href="#">删除用户</a>
3						<a href="#">添加用户</a>
4						<a href="#">添加用户</a>

2. 点击“删除”按钮后，页面会弹出窗口询问确认要删除此用户，选择“Cancel”取消删除动作，选择“OK”确认删除。如下图所示。

图 3-9 确认删除用户



3. 点击“OK”后会提示操作成功。如下图所示，点击“OK”按钮后，可看到用户列表中该用户已经被删除。

图 3-10 删除完成

用户管理						
用户ID	用户名	用户组	用户启用	IPMI权限	电子邮箱ID	操作
1	ADMIN	Administrator	已启用	administrator		<a href="#">更改用户</a> <a href="#">删除用户</a>
2						<a href="#">添加用户</a>
3						<a href="#">添加用户</a>
4						<a href="#">添加用户</a>

# 4 网络设置

## 4.1 功能特性

网络设置模块主要提供获取 BMC 网络配置信息、配置 BMC 局域网接口、IPv4/IPv6 动态或静态地址配置等功能，支持 VLAN 设置。

## 4.2 获取网络配置

操作场景：

指导您通过 Web 管理界面获取网络配置信息。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>网络”页面，点击“网络设置”TAB 页，此页面用于共享网卡配置、网络绑定和网络 IP 设置，如下图所示：



图 4-1 共享网卡配置、网络绑定配置和网络 IP 设置

The screenshot displays the BMC network configuration interface, divided into three main sections:

- 共享网卡(NC-SI)配置 (NC-SI Configuration):**
  - NCSI 模式 (NC-SI Mode):** Radio buttons for "自动故障切换模式" (Automatic failover mode, selected) and "手动切换模式" (Manual failover mode).
  - NCSI 网卡 (NC-SI Network Card):** Dropdown menu set to "OCP".
  - 端口 (Port):** Dropdown menu set to "0".
  - 保存 (Save):** Button at the bottom right.
- 网络绑定配置 (Network Bonding Configuration):**
  - 启用绑定 (Enable Bonding):** Checked checkbox.
  - 绑定接口 (Bonding Interface):** Dropdown menu set to "eth0".
  - 绑定模式 (Bonding Mode):** Text field set to "active-backup".
  - 保存 (Save):** Button at the bottom right.
- 网络 IP 设置 (Network IP Settings):**
  - 启用 LAN (Enable LAN):** Checked checkbox.
  - LAN 界面 (LAN Interface):** Dropdown menu set to "bond0".
  - MAC 地址 (MAC Address):** Read-only field showing "B4:05:5D:4F:1B:76".
  - IPv4 配置 (IPv4 Configuration):**
    - 启用 IPv4 (Enable IPv4): Checked checkbox.
    - 启用 IPv4 DHCP (Enable IPv4 DHCP): Checked checkbox.
    - IPv4 地址 (IPv4 Address): Text field "100.2.76.125".
    - IPv4 子网掩码 (IPv4 Subnet Mask): Text field "255.255.255.0".
    - IPv4 默认网关 (IPv4 Default Gateway): Text field "100.2.76.1".
  - IPv6 配置 (IPv6 Configuration):**
    - 启用 IPv6 (Enable IPv6): Checked checkbox.
    - 启用 IPv6 DHCP (Enable IPv6 DHCP): Checked checkbox.
    - IPv6 索引 (IPv6 Index): Dropdown menu set to "0".
    - IPv6 地址 (IPv6 Address): Text field "2001:db8:1:0:b605:5dffe4f:1b76".
    - 子网掩码前缀长度 (Subnet Mask Prefix Length): Text field "64".
    - IPv6 网关 (IPv6 Gateway): Text field "::".
  - 其他选项 (Other Options):**
    - 启用 VLAN (Enable VLAN): Unchecked checkbox.
    - VLAN ID: Text field "0".
    - VLAN 优先权 (VLAN Priority): Text field "0".
    - 保存 (Save):** Button at the bottom right.

BMC 网络具体配置参数如下表所示：

表 4-1 网络 IP 设置参数

参数	描述
启用 LAN	勾选，启用 LAN 对所选接口的支持。
LAN 界面	选择专口和共享口。可选项为：eth0 和 eth1。
MAC 地址	此字段显示选定的接口（只读）的 MAC 地址。

参数	描述
IPv4配置	
启用IPv4	选中此选项来启用所选接口的IPv4支持。
启用IPv4 DHCP	勾选“启用IPv4 DHCP”，则使用动态主机配置协议（DHCP）分配IPv4地址。
IPv4地址	<p>如果禁用DHCP，为选定的接口配置指定一个静态IPv4地址，子网掩码和默认网关。</p> <ul style="list-style-type: none"> <li>IP地址包含以点隔开的4组数字“xxx.xxx.xxx.xxx”。</li> <li>每组数字范围0到255。</li> <li>第一组数字不能为0。</li> </ul>
IPv4子网掩码	指定IPv4设置的默认子网掩码。
IPv4默认网关	指定IPv4设置的默认网关。
IPv6配置	
启用IPv6	选中此选项来启用所选接口的IPv6支持。
启用IPv6 DHCP	勾选“启动IPv6 DHCP”，则使用动态主机配置协议（DHCP）分配IPv6地址。
IPv6索引	选择IPv6索引。
IPv6地址	指定被选定的接口配置静态IPv6地址。
子网掩码前缀长度	指定IPv6设置的子网前缀长度。
IPv6网关	<p>设置IPv6的默认网关。</p> <p>数值范围0到128。</p>
VLAN配置	
启用VLAN	选择此选项以启用VLAN选定接口的支持。
VLAN ID	<p>指定VLAN配置的ID。</p> <p>数值范围1到4094。</p> <p>提示：VLAN ID更新后必须要进行重启。</p>
VLAN优先权	<p>指定VLAN配置的优先级。</p> <p>数值范围0到7。</p> <p>提示：7是VLAN配置的最高优先级。</p>

## 4.3 共享网卡配置

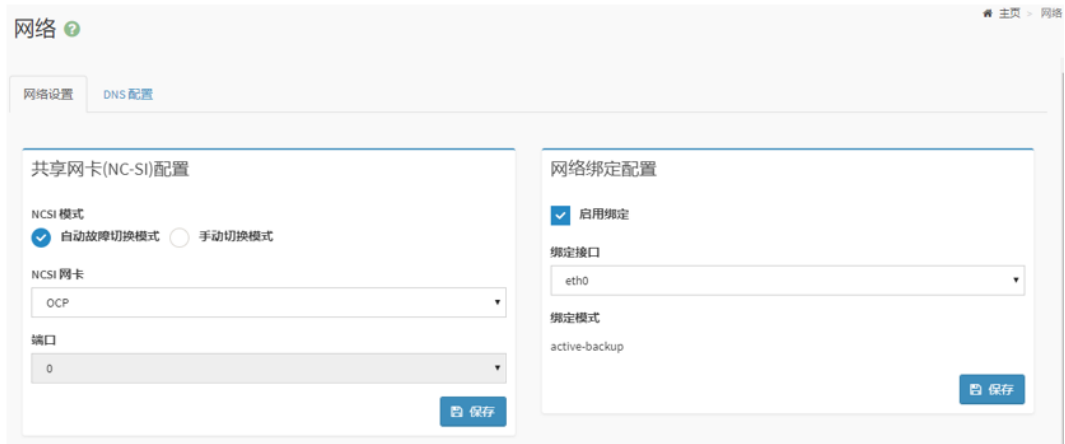
操作场景：

指导您通过 Web 管理界面进行共享网卡设置。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>网络”页面，点击“网络设置”TAB 页，此页面用于共享网卡配置，如下图所示。

图 4-2 共享网卡配置和网络绑定配置



2. 选择 NCSI 模式、NCSI 网卡类型。如果选择了“手动切换模式”，则需要选择端口。点击保存按钮。

BMC 共享网卡配置参数如下表所示：

表 4-2 共享网卡配置参数

参数	描述
NCSI模式	<ul style="list-style-type: none"><li>• 自动故障切换模式</li><li>• 手动切换模式</li></ul>
NCSI网卡	选择网卡的接口类型。可选项为：OCP和PCIe。
端口	为已选择的网卡选择端口。可选项目：0、1、2、3。

BMC 网络绑定配置参数如下表所示：

表 4-3 网络绑定配置参数

参数	描述
启用绑定	选中此选项以启用网络接口的网络连接。

参数	描述
	注意：如果启用VLAN接口，则绑定无法启用。VLAN可以在本页面中禁用。
绑定接口	本选项用来配置网络接口中的网络绑定。默认为启用。 注意：最少需要两个网络接口才可启用装置的网络绑定。eth0是专用管理口，eth1是共享管理口。
绑定模式	此栏位显示网络绑定模式状态。 注意：本栏位不可配置。绑定后使用eth0的MAC地址。

## 4.4 网络 IP 设置

操作场景：

指导您通过 Web 管理界面设置 IP 地址。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>网络”页面，点击“网络设置”标签页。
2. 首先选择 LAN 界面，选择需要配置的网络接口。
3. 选中或者取消启用 LAN 按钮，以确认这个网口是否启用。
4. 选中或者取消 IPv4、IPv6 按钮，以确认是否启用 IPv4、IPv6。
5. 如果启用了 IPv4，则可以再选中或者取消 IPv4 DHCP。如果不启用 IPv4 DHCP，则手动进行 IPv4 相关设置，包括地址、子网掩码、默认网关。
6. 如果启用了 IPv6，则可以再选中或者取消 IPv6 DHCP。如果不启用 IPv6 DHCP，则手动进行 IPv6 相关设置，包括索引、地址、子网掩码长度、默认网关。

图 4-3 IP 设置



网络 IP 设置

启用 LAN

LAN 界面  
eth0

MAC 地址  
6C:92:BF:56:2C:9C

启用 IPv4  启用 IPv6

启用 IPv4 DHCP  启用 IPv6 DHCP

IPv4 地址  
100.2.76.64

IPv4 子网掩码  
255.255.255.0

IPv4 默认网关  
100.2.76.1

IPv6 索引  
0

IPv6 地址  
2001:db8::6e92:bfff:fe56:2c9c

子网掩码前缀长度  
64

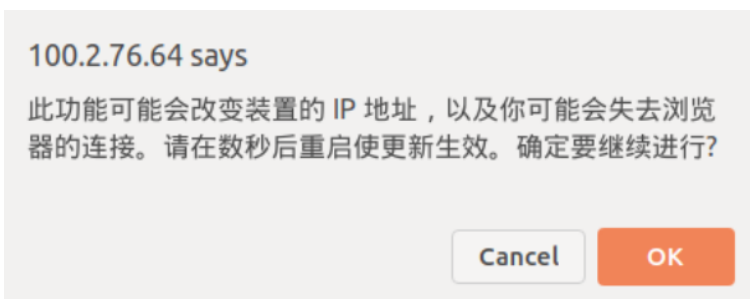
IPv6 网关  
fe80::271:c2ff:fe2a:7f08

7. 点击“保存”按钮，保存设置，会弹出如下提示框。



IP 地址变化后，需要使用新的 IP 地址来访问 BMC。

图 4-4 IP 设置提示对话框



## 4.5 VLAN 设置

操作场景：

指导您通过 Web 管理界面设置 VLAN。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>网络”页面，点击“网络设置标签页”，在 VLAN 配置选项中选中“启用 VLAN”，启用 VLAN 功能，并填写 VLAN ID、VLAN 优先级信息，如下图所示。填写完成后，点击“保存”按钮。

图 4-5 VLAN 配置



启用 VLAN

VLAN ID

0

VLAN 优先级

0

保存

## 4.6 DNS 设置

操作场景：

指导您通过 Web 管理界面进行 DNS 设置。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>网络”页面，点击“DNS 配置”标签页，此页面用来进行主机配置、域名配置以及域名服务器配置。
2. 用户可以通过选中或者取消“DNS 已启用”选项来启用或者关闭 DNS 功能。另外，页面提供“主机名称设置”、“BMC 注册设置”、“网域设置”、“域名服务器设置”和“IP 优先级”等配置选项，用户可以手动配置各参数，也可以使用自动模式，BMC 自动配置相关参数。

图 4-6 DNS 设置

网络 ?

网络设置 DNS 配置

DNS 已启用

mDNS 启用

主机名称设置

自动  手动

主机名称

qasdjkdslkjljk

BMC 注册设置

BMC 界面:

bond0

注册 BMC

注册方法:

名字服务器  DHCP 客户端 FQDN  主机名称

网域设置

自动  手动

网域界面

bond0\_v4

域名服务器设置

自动  手动

DNS 界面

bond0

IP 优先权

IPv4  IPv6

保存

3. 设置完成后，点击“保存”按钮保存配置。

DNS 具体配置参数如下表所示：

表 4-4 DNS 配置参数

参数	描述
DNS设置	
DNS已启用	<ul style="list-style-type: none"> <li>• 勾选：启用所有的DNS服务</li> <li>• 不勾选：不启用DNS服务</li> </ul>
mDNS启用	<ul style="list-style-type: none"> <li>• 勾选：启用所有的mDNS服务</li> <li>• 不勾选：不启用mDNS服务</li> </ul>
主机设置	
主机名称设置	选择自动或手动设置。
主机名称	它显示设备的主机名。如果主机设置为手动选择，则要指定该设备的主机名，IPv6服务器只能显示以字母开头的主机名。
BMC注册设置	
BMC界面	bond0
注册BMC	<ul style="list-style-type: none"> <li>• 勾选：注册BMC</li> <li>• 不勾选：不注册BMC</li> </ul>
注册方法	可选择：名字服务器，DHCP客户端FQDN或者主机名称。 名字服务器：使用名字服务器应用程序向DNS服务器来注册。 DHCP客户端FQDN：使用DHCP选项81来向DNS服务器注册。 主机名称：使用DHCP选项12来向DNS服务器注册。
网域设置	可以选择自动或者手动。
网域界面	可以选择eth0_v4或者eth1_v4。
域名服务器设置	可以选择自动或者手动。
DNS界面	显示eth0或者eth1。
IP优先级	可以选择IPv4或者IPv6。



# 5 风扇管理

## 5.1 功能特性

风扇控制模块主要用于手动或者自动控制风扇转速，设置完成后立即生效。

## 5.2 风扇自动设置

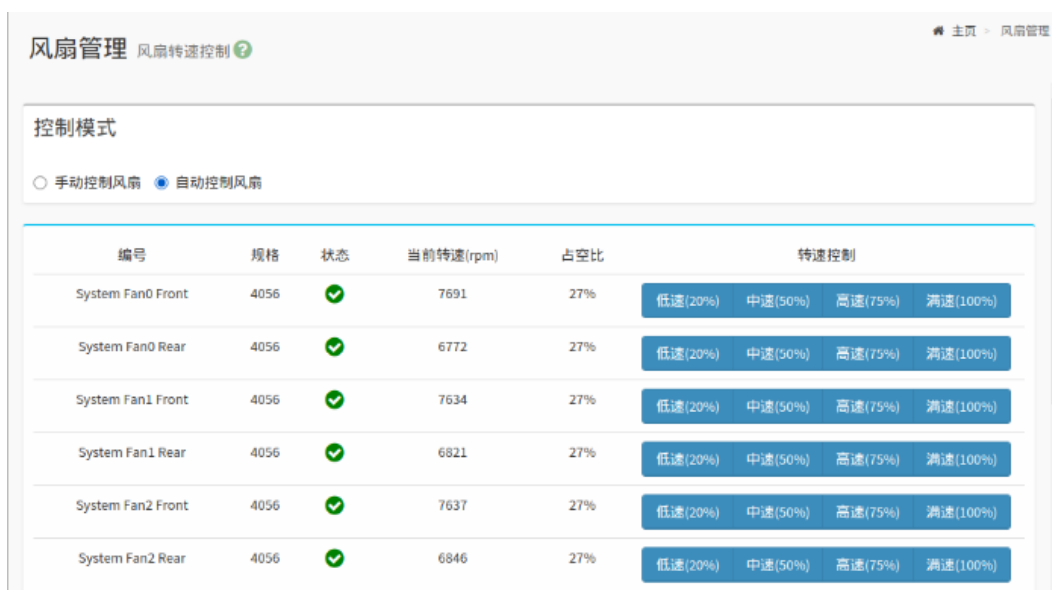
操作场景：

指导您通过 Web 管理界面设置风扇控制模式为自动。

操作步骤：

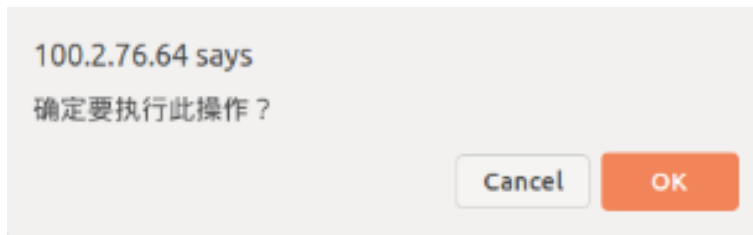
1. 登录到 Web GUI，进入“风扇管理”页面，此页面用于风扇控制模式的设置以及风扇转速的控制。点击页面左上方“自动控制风扇”选项。如下图所示：

图 5-1 自动风扇控制



2. 点击自动控制风扇，会弹出以下提示框，点击“OK”按钮完成设置。

图 5-2 自动风扇控制确认对话框



## 5.3 风扇手动设置

操作场景：

指导您通过 Web 管理界面设置风扇控制模式为手动。

操作步骤：

1. 登录到 Web GUI，进入“风扇管理”页面，此页面用于风扇控制模式的设置以及风扇转速的控制。点击页面左上方“手动控制风扇”选项，改为手动控制风扇。
2. 找到需要手动配置的风扇编号，点击转速控制“低速”、“中速”、“高速”、“满速”四个选项完成手动配置风扇转速。如下图所示，设置 Fan0 为中速 50%。

图 5-3 手动风扇控制



# 6 日志收集

## 6.1 功能特性

日志模块主要支持系统事件日志、审计日志、IDL 日志和一键收集日志，可以在页面中展示日志信息，提供日期以及日志等级等选项进行日志筛选，提供日志下载、日志清除功能。

## 6.2 操作指导

请参考《浪潮英信服务器 BMC 日志收集和分析指南》。

## 6.3 Syslog 日志设置

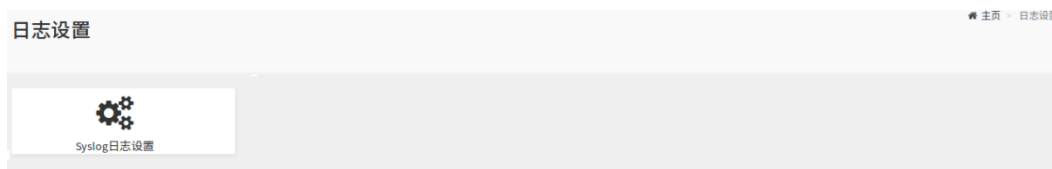
操作场景：

指导您通过 Web 管理界面进行 Syslog 设置。

操作步骤：

1. 登录到 Web GUI，进入“日志和告警>日志设置”页面。

图 6-1 日志设置



2. 点击 Syslog 日志设置，如下图，可设置 Syslog 告警设置、Syslog 主机标识、告警级别以及传输协议和 Syslog 服务器和报文格式。用户可以对 IDL 日志或者审计日志系统记录选择开启或关闭，并在启用时选择记录类型为本地日志信息或者远程日志信息。当选择远程日志信息时，需填写服务器地址、服务器端口和协议类型。

图 6-2 Syslog 设置

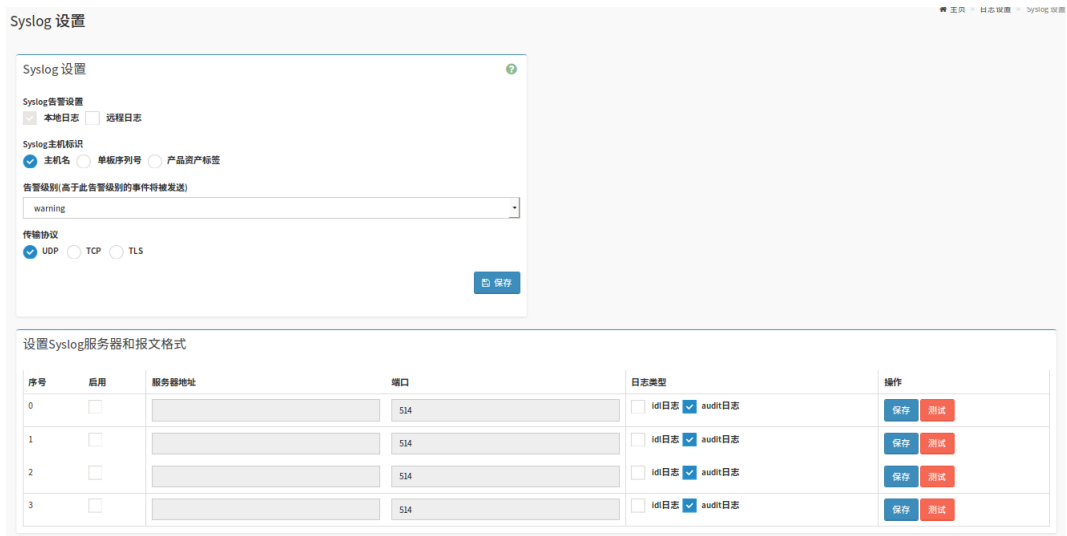


表 6-1 Syslog 设置

参数	描述
Syslog 告警设置	Syslog 告警日志存储位置，可多选，选项为： <ul style="list-style-type: none"> <li>本地日志</li> <li>远程日志</li> </ul>
Syslog 主机标识	Syslog 主机标识，可选为： <ul style="list-style-type: none"> <li>主机名</li> <li>单板序列号</li> <li>产品资产标签</li> </ul>
告警级别	高于此告警级别的时间将被发送，可选为： <ul style="list-style-type: none"> <li>Warning</li> <li>Info</li> <li>Critical</li> </ul>
传输协议	传输协议，可选为： <ul style="list-style-type: none"> <li>UDP</li> <li>TCP</li> </ul>

参数	描述
	<ul style="list-style-type: none"> <li>TLS（单项认证，双向认证）</li> </ul> 注：选择TLS协议时，需上传对应的服务器证书或认证文件。

表 6-2 Syslog 服务器和报文格式

参数	描述
序号	序号。
启用	启用或不启用。
服务器地址	Syslog服务器地址。
端口	Syslog服务器端口。
日志类型	IDL日志、audit日志。可单选，可多选。
操作	保存，保存该Syslog服务器信息。 测试，测试该Syslog服务器报文是否可以成功发送。

# 7 BMC 时间设置

## 7.1 功能特性

BMC 时间设置模块提供配置 BMC 时间的方法：通过配置 NTP 服务器，同步周期等参数，实现 BMC 自动同步 NTP 服务器的时间。

## 7.2 NTP 自动同步

操作场景：

指导您通过 Web 管理界面进行 NTP 自动同步设置。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>日期&时间”页面，此页面显示当前的 BMC 时间和 NTP 设置。如下图所示。

图 7-1 NTP 自动同步配置页面

日期 & 时间 ?

浏览器本地时区时间

Apr 27, 2020 2:55:23 AM ( GMT+8) - Broswer Timezone/GMT+8

配置 BMC 日期 & 时间

请选择时区

NTP 自动刷新日期 & 时间  NTP DHCP4 刷新日期 & 时间  NTP DHCP6 刷新日期 & 时间

NTP 服务器 1  
pool.ntp.org

NTP 服务器 2  
time.nist.gov

NTP 服务器 3  
NTP 服务器名称

NTP 服务器 4  
NTP 服务器名称

NTP 服务器 5  
NTP 服务器名称

NTP 服务器 6  
NTP 服务器名称

保存

2. 在页面中选中“NTP 自动刷新日期&时间”选项、“NTP DHCP4 刷新日期&时间”或“NTP DHCP6 刷新日期&时间”，并对 NTP 服务器进行设置，实现 NTP 自动同步配置，点击“保存”按钮，保存配置。

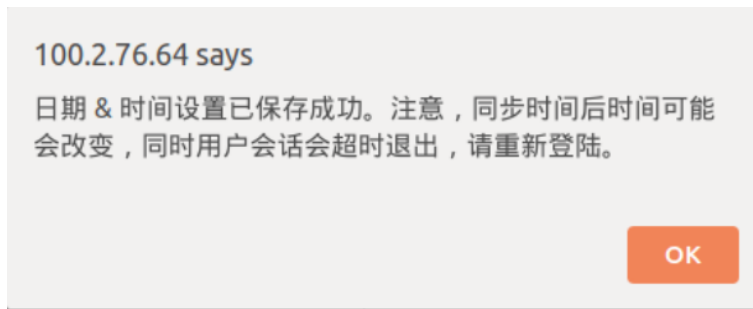
图 7-2 NTP 配置确认对话框

100.2.76.64 says

日期 & 时间设置后会同步时间。注意，同步时间后时间可能会改变，同时用户会话会超时退出，需重新登陆。确认要继续进行吗?

Cancel OK

图 7-3 NTP 配置成功提示框





# 8 SNMP Trap 告警设置

## 8.1 功能特性

SNMP Trap 告警设置模块提供发送事件日志相关的 SNMP Trap 参数配置，通过告警级别、设备类型等，对事件日志进行筛选发送。通过告警策略设置来指定事件日志的发送目的地 IP 和端口。

## 8.2 SNMP Trap 设置

操作场景：

指导您通过 Web 管理界面进行 SNMP Trap 设置。

操作步骤：

1. 登录到 Web GUI，进入“日志和告警>SNMP Trap 设置”页面，设置 SNMP Trap 相关参数，包括 Trap 版本、告警级别和团体名等，如下图所示：

图 8-1 SNMP Trap 配置页面

Trap 设置

启用SNMP Trap

Trap版本  
V1

告警级别（高于此告警级别的事件将被发送）  
Info

团体名  
[Empty text box]

主机标识  
HostName

用户名  
[Empty text box]

认证协议  
[Empty dropdown menu]

认证密码  
[Empty text box]

加密协议  
[Empty dropdown menu]

加密密码  
[Empty text box]

引擎号  
[Empty text box]

设备类型  
All

保存

2. 设置告警策略，设置安装了 Trap 接收端的客户机 IP 为目的地址，设置 Trap 接收端的端口号为端口，点击“保存”。保存后，点击“测试”按钮，在 Trap 接收端可以得到一条测试消息。

图 8-2 告警策略设置

ID	启用	目的地	端口	动作
0	<input checked="" type="checkbox"/>	100.3.7.4	162	保存 测试
1	<input type="checkbox"/>	[Empty text box]	162	保存 测试
2	<input type="checkbox"/>	[Empty text box]	162	保存 测试
3	<input type="checkbox"/>	[Empty text box]	162	保存 测试

# 9 邮箱告警

## 9.1 功能特性

邮箱告警模块需要先启用 SMTP 邮件告警功能，并配置相关信息。

## 9.2 邮箱告警设置

操作场景：

指导您通过 Web 管理界面进行邮箱告警设置。

操作步骤：

1. 在导航栏中选择“日志和告警>邮箱告警”，进入 SMTP 设置页面。

图 9-1 SMTP 设置页面

启动SMTP邮件告警

SMTP服务器地址

SMTP服务器端口

25

SMTP服务器安全端口

465

发件人身份认证

发件人电子邮件 ID

发件人用户名

发件人密码

启用SMTP SSLTLS

启用SMTP STARTTLS

邮件主题

主题附加

主机名  单板序列号  产品资产标签

告警发送级别(高于此告警级别的事件将被发送)

Info

保存

2. 输入 SMTP 服务器地址、发件人电子邮件、邮件主题等必需信息，其它信息根据需要进行输入，然后点击“保存”按钮。
3. 输入接收告警的邮件地址，点击“保存”按钮。然后再点击“测试”按钮，测试是否能够接收到测试邮件。测试邮件接收成功，则功能配置完成。

图 9-2 设置接收告警的邮件地址

设置接收告警的邮件地址

操作执行成功！

邮件地址1：	<input type="text" value="test01@test.com"/>	描述：	<input type="text" value="manager email"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input checked="" type="checkbox"/> 启用
邮件地址2：	<input type="text"/>	描述：	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/> 启用
邮件地址3：	<input type="text"/>	描述：	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/> 启用
邮件地址4：	<input type="text"/>	描述：	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="保存"/>	<input type="checkbox"/> 启用

# 10 BMC 服务设置

## 10.1 功能特性

BMC 服务设置模块主要用于展示 BMC 相关服务列表信息，并提供各服务配置信息查看、修改功能。

## 10.2 服务设置

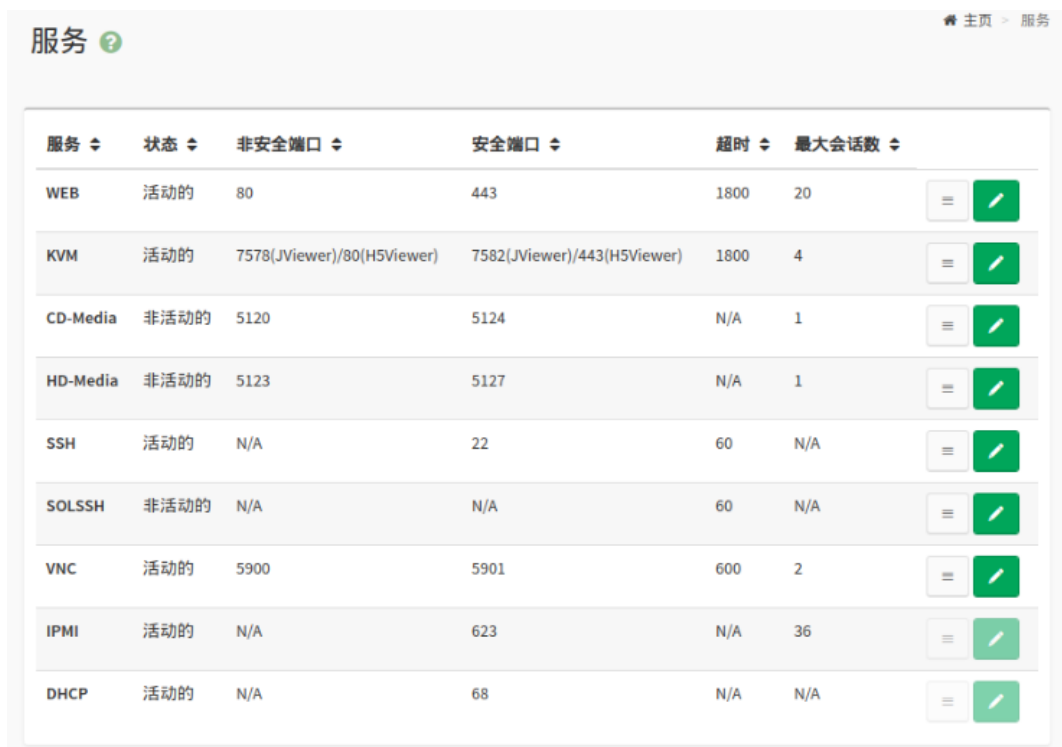
操作场景：

指导您通过 Web 管理界面对服务的端口、超时等属性进行配置。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>服务”页面，此页面显示了 BMC 运行中的服务基本信息。修改服务信息，用户必须是管理员。

图 10-1 服务设置页面



服务	状态	非安全端口	安全端口	超时	最大会话数		
WEB	活动的	80	443	1800	20	=	✎
KVM	活动的	7578(JViewer)/80(H5Viewer)	7582(JViewer)/443(H5Viewer)	1800	4	=	✎
CD-Media	非活动的	5120	5124	N/A	1	=	✎
HD-Media	非活动的	5123	5127	N/A	1	=	✎
SSH	活动的	N/A	22	60	N/A	=	✎
SOLSSH	非活动的	N/A	N/A	60	N/A	=	✎
VNC	活动的	5900	5901	600	2	=	✎
IPMI	活动的	N/A	623	N/A	36	=	✎
DHCP	活动的	N/A	68	N/A	N/A	=	✎


2. 点击需要修改的服务行右侧  按钮，进入服务配置修改页面，可对具体配置选项进行修改，点击“保存”按钮，完成修改操作。下图为 Web 服务修改示例。

图 10-2 修改服务配置

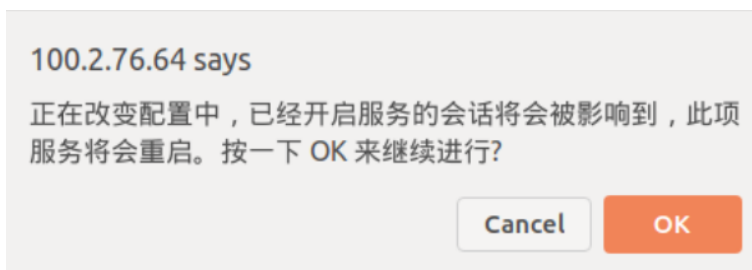


The image shows a 'Service Configuration' dialog box with the following fields and options:

- 服务名称** (Service Name): web
- 活动的** (Active)
- 不安全端口** (Insecure Port): 80
- 安全端口** (Secure Port): 443
- 超时** (Timeout): 1800
- 最大会话数** (Maximum Sessions): 20

A '保存' (Save) button is located at the bottom right of the dialog box.

图 10-3 服务重启确认对话框



The image shows a confirmation dialog box with the following text:

100.2.76.64 says  
正在改变配置中，已经开启服务的会话将会被影响到，此项服务将会重启。按一下 OK 来继续进行？

Buttons: Cancel, OK

BMC 服务设置相关参数如下表所示：

表 10-1 服务设置

参数	描述
服务	显示选定行的服务名称（只读）。
状态	显示当前的服务状态。分为活动的和非活动的两种状态。
不安全端口	<p>用于配置服务的非安全端口号：</p> <ul style="list-style-type: none"> <li>• Web默认端口为80</li> <li>• KVM默认端口为7578</li> <li>• 光盘媒体默认端口是5120</li> <li>• 硬盘媒体默认端口是5123</li> <li>• Solssh的默认端口是N/A</li> <li>• VNC的默认端口是5900</li> <li>• 端口值范围从1到65535</li> </ul> <p>提示：SSH服务不支持非安全端口。</p>
安全端口	<p>用于配置服务的安全端口号：</p> <ul style="list-style-type: none"> <li>• Web默认端口为443</li> <li>• KVM默认端口为7582</li> <li>• 光盘媒体默认端口是5124</li> <li>• 硬盘媒体默认端口是5127</li> <li>• SSH的默认端口是22</li> <li>• VNC的默认端口是5901</li> <li>• 端口值范围从1到65535</li> </ul> <p>提示：Solssh服务不支持安全端口。</p>
超时	<p>服务会话超时值。用户可以配置会话超时值：</p> <ul style="list-style-type: none"> <li>• Web、KVM和VNC超时数值范围300到1800秒</li> <li>• SSH and Solssh超时数值范围60到1800秒</li> <li>• 超时值应该为60秒的倍数</li> </ul>
最大会话数	当前服务最大会话数量。



# 11 存储管理

## 11.1 功能特性

该模块能够查看存储相关的控制器、逻辑盘、物理盘信息，进行逻辑磁盘的创建、删除等操作。

## 11.2 逻辑盘的创建

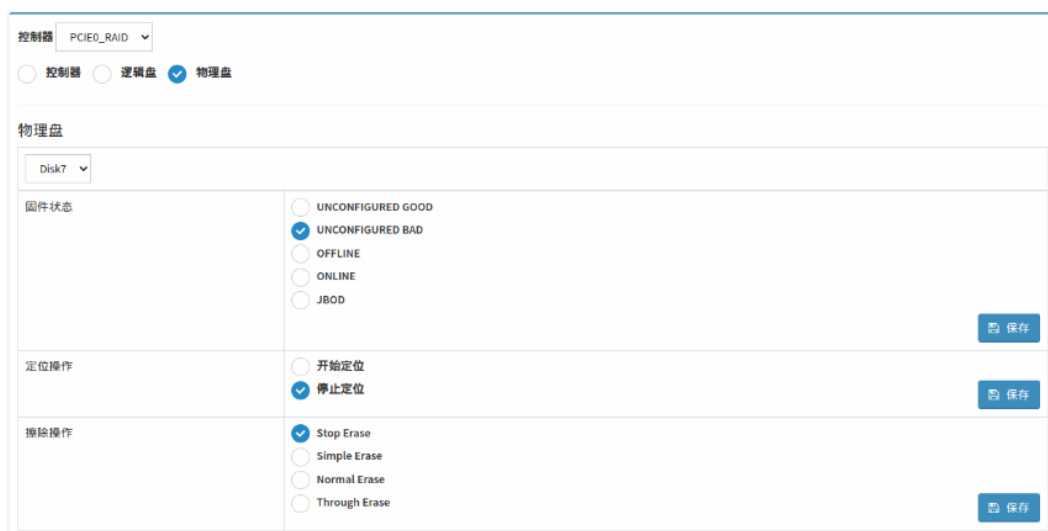
操作场景：

指导您通过 Web 管理界面进行逻辑盘的创建。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>存储”页面，点击配置标签页。只有 UNCONFIGURED GOOD 状态的物理盘才能够创建逻辑盘，当无法创建逻辑盘时，优先查看以下物理盘的状态。选择“控制器>物理盘”，查看物理盘的状态。如下图所示，物理盘状态为 UNCONFIGURED BAD，这种情况下，无法用于创建逻辑盘。

图 11-1 物理盘查看页面



2. 创建逻辑磁盘，主要选择物理盘和 RAID 级别，其它选项请根据您的实际使用需求自行选择。然后点击“保存”按钮。

图 11-2 逻辑盘创建页面

存储 ?

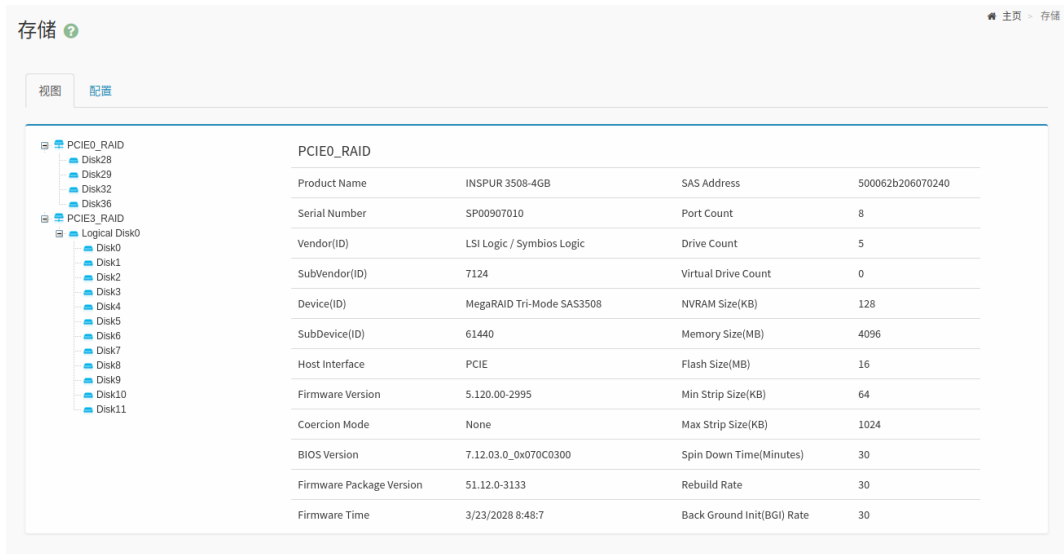
### 逻辑盘

创建虚拟硬盘	
级别	RAID0 ▾
条带大小	64K ▾
访问策略	Read Write ▾
读策略	Read Ahead ▾
写策略	Write Throgh ▾
IO策略	Direct IO ▾
缓存策略	Unchanged ▾
初始化类型	No Init ▾
所选物理盘大小	100 %
物理盘	<input type="checkbox"/> Disk6

 保存

3. 查看存储视图，查看所做修改是否已经显示。组 RAID 需要时间，需要耐心等待。如果一直没有操作成功，请使用 RAID 卡的 BIOS setup 界面或者其它工具进行 RAID 操作。

图 11-3 存储视图



## 11.3 逻辑盘的其它操作

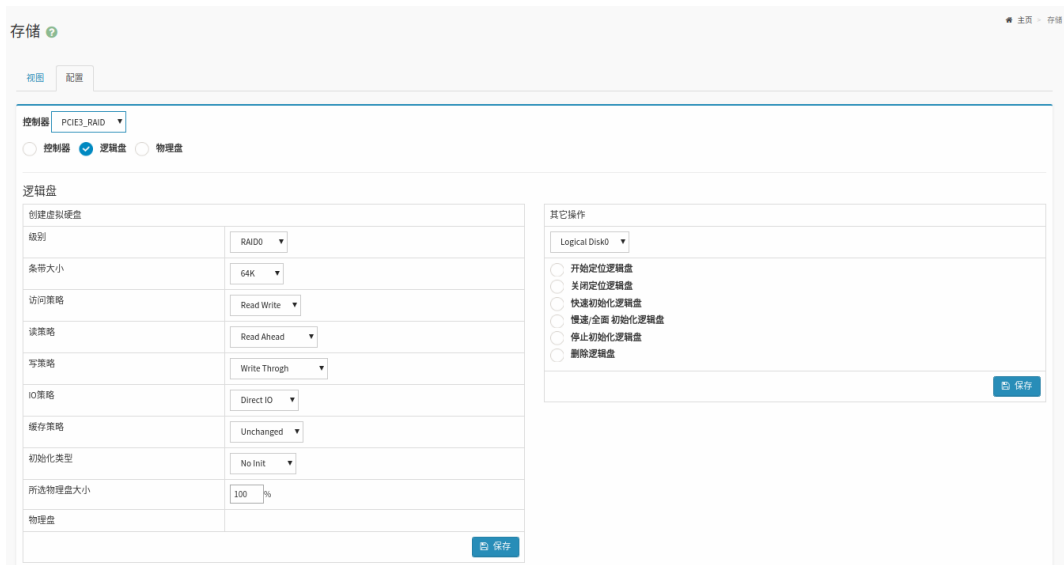
操作场景：

指导您通过 Web 管理界面进行逻辑盘的定位、关闭定位、初始化、删除等操作。

操作步骤：

1. 登录到 Web GUI，进入“BMC 设置>存储”页面，点击配置标签页，再点击逻辑盘。
2. 点击右侧其它操作的按钮，进行相关操作。

图 11-4 存储页面



# 12 固件升级

## 12.1 功能特性

提供 HPM 固件更新升级功能。可更新升级 BIOS、BMC、CPLD、PSU 和 FPGA。

## 12.2 操作指导

请参考《浪潮英信服务器 BMC 升级手册》。

# 13 恢复出厂设置

## 13.1 功能特性

该功能将使 BMC 的配置恢复到出厂设置，您在 BMC 上所做的任何配置修改都将丢失。当您发现您对 BMC 的配置修改引起了某些功能异常时，可以审慎地进行这个操作。

## 13.2 恢复出厂设置

操作场景：

指导您通过 Web 管理界面将 BMC 恢复出厂设置。

操作步骤：

1. 登录 Web GUI，进入“系统维护>恢复出厂设置”。

图 13-1 恢复出厂设置配置页面



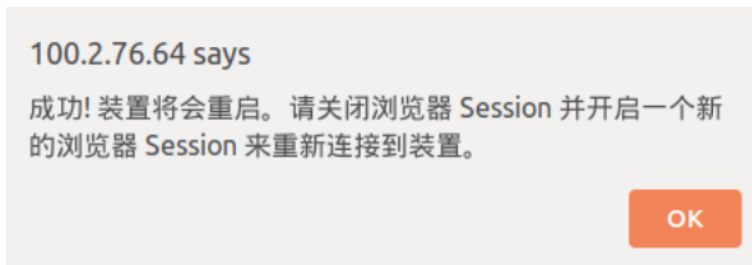
2. 点击“保存”按钮，会弹出以下提示框，点击“OK”按钮。

图 13-2 恢复出厂设置提示框



3. 恢复出厂设置成功，会弹出以下提示框。需要关闭浏览器，并开启一个新的浏览器 Session 来重新连接到装置。

图 13-3 恢复出厂设置成功提示框



# 14 SSL 设置

## 14.1 功能特性

该功能支持对 SSL 证书进行替换，为提高安全性，建议替换成您自己的证书和公私钥对，并及时更新证书，保证证书的有效性。

## 14.2 在线生成 SSL 凭证

操作场景：

指导您通过 Web 管理界面在线生成 SSL 凭证。

操作步骤：

1. 登录 Web GUI，进入“BMC 设置>SSL 设置”，选择“产生 SSL 认证”。

图 14-1 SSL 设置界面



2. 在如下图所示界面中填写信息。表格字段信息请参考[表格 14-1](#)。

图 14-2 生成 SSL 凭证界面

生成 SSL 凭证

通用名称(CN)  
testssl

组织(O)  
INSPUR

组织单位(OU)  
FW

城市或地点(L)  
JN

州或省(ST)  
SD

国家(C)  
CN

电子邮件地址  
testssl@inspur.com

有效自  
3650

密钥长度  
2048 bits

保存

表 14-1 SSL 设置

参数	描述
通用名称 (CN)	Common Name, 可以存放姓名或者用途名称, 比如 testssl。
组织 (O)	Organization Name, 组织名称或者公司名称, 比如浪潮英文缩写INSPUR。
组织单位 (OU)	Organizational Unit Name, 组织或者单位的下属单位名称, 比如固件部门缩写FW。
城市或地点	城市或地点, 比如济南市缩写JN。
州或省	州或省, 比如山东省缩写SD。
国家	国家, 比如中国china缩写CN。
电子邮件地址	电子邮件地址, 比如testssl@inspur.com。
有效自	有效时长, 365天到3650天。



参数	描述
密钥长度	密钥长度，默认密钥长度为2048bits。

## 14.3 生成 SSL 凭证并上传

操作场景：

指导您通过 openssl 工具生成 SSL 凭证，并通过 Web 管理界面上传您的 SSL 凭证。

操作步骤：

1. 安装 openssl 工具，具体操作说明请参见 [18.2 openssl 介绍](#)。本操作步骤是使用 openssl 工具生成 SSL 凭证，如果你已经有生成的证书，请直接跳至第 6 步。
2. 生成私钥，openssl genrsa -out privkey.pem 2048。
3. 生成证书请求（参考下表），openssl req -new -key privkey.pem -out cert\_req.pem

表 14-2 证书请求输入参数

<p>You are about to be asked to enter information that will be incorporated into your certificate request.</p> <p>What you are about to enter is what is called a Distinguished Name or a DN.</p> <p>There are quite a few fields but you can leave some blank</p> <p>For some fields there will be a default value,</p> <p>If you enter '.', the field will be left blank.</p> <p>-----</p> <p>Country Name (2 letter code) [AU]:CN</p> <p>State or Province Name (full name) [Some-State]:SD</p> <p>Locality Name (eg, city) []:JN</p> <p>Organization Name (eg, company) [Internet Widgits Pty Ltd]:INSPUR</p> <p>Organizational Unit Name (eg, section) []:FW</p> <p>Common Name (e.g. server FQDN or YOUR name) []:webssl</p> <p>Email Address []:webssltest@inspur.com</p>
--

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

4. 生成签名证书, `openssl x509 -req -days 365 -in cert_req.pem -signkey privkey.pem -out sign_cert.pem`。
5. 将证书合并到私钥文件 `cat privkey.pem sign_cert.pem > server.pem`。
6. 登录 Web GUI, 进入 “BMC 设置>SSL 设置”, 选择上传 SSL 凭证, 如下图。
7. 在打开的页面中, 选择新的凭证文件 `sign_cert.pem`, 选择新的私钥文件 `server.pem`, 点击保存完成设置。

图 14-3 上传 SSL 凭证界面

上传 SSL 凭证

HTTPS 凭证已更新,刷新页面后来使用新凭证!

**当前凭证**  
Sat May 2 02:25:03 2020

**新凭证**  
sign\_cert.pem

**当前私钥**  
Sat May 2 02:25:03 2020

**新的私钥**  
server.pem

保存

8. 再次点击 “BMC 设置>SSL 设置”, 点击 “查看 SSL 凭证”, 确认凭证信息已经修改。如下图所示。

图 14-4 查看 SSL 凭证界面



# 15 Redfish

## 15.1 概述

Redfish 是一种基于 HTTPS 服务的管理标准，利用 RESTful 接口实现设备管理。每个 HTTPS 操作都以 UTF-8 编码的 JSON 的形式，提交或返回一个资源。就像 Web 应用程序向浏览器返回 HTML 一样，RESTful 接口会通过同样的传输机制(HTTPS)，以 JSON 的形式向客户端返回数据。

当前，整个互联网正逐渐向通用的新软件接口模式发展，Redfish 无疑契合了这一趋势。相比之前的技术，它们易于实施、易于使用而且提供了可扩展性优势。Redfish 的同一个数据模型既可以用于传统机架安装式服务器、刀片服务器，也可以用于新型系统。此优势源自于数据模型设计用来向客户端自我描述服务功能，而且从一开始便为设计灵活性预留了足够空间。

## 15.2 操作指导

具体操作请参考文档《浪潮英信服务器 Redfish 用户手册》。

# 16 进入 BIOS 系统

## 16.1 功能特性

在服务器系统中，BIOS 与 BMC 之间相互通信，进行数据交换。通过 BIOS 界面，可以查看 BMC 的网络配置信息、用户信息等。

## 16.2 本地进入 BIOS 系统

操作场景：

指导您通过本地键盘显示器，进入 BIOS 系统。

操作步骤：

1. 连接好电源并外接键盘、鼠标、显示器。
2. 将服务器上电开机。
3. 系统开始启动时，当屏幕出现 Logo 且下方提示：“Press <DEL> to SETUP or <F11> to Boot Menu or <F12> to PXE Boot.” 时，如下图所示，按下“DEL”，稍后会进入 BIOS Setup 界面。

图 16-1 BIOS Logo 界面



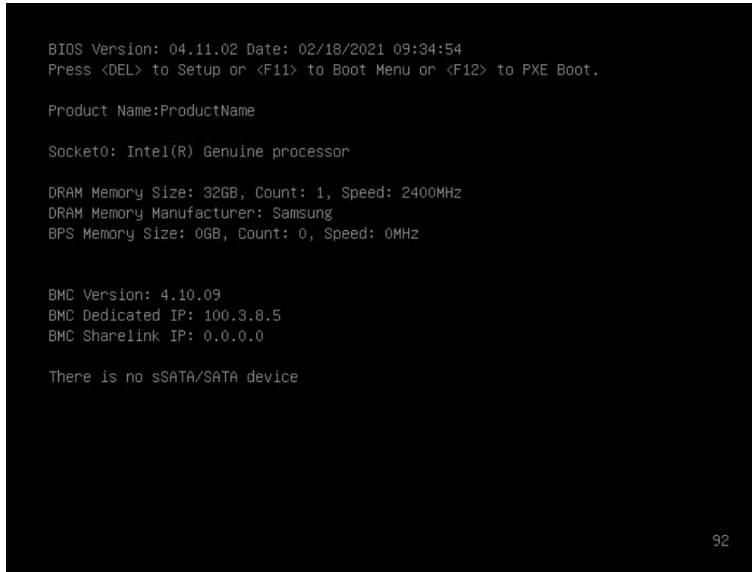


## 说明

如果当前 BIOS 版本没有放开 Logo 显示，当出现 “Press <DEL> to Setup or <F11> to Boot Menu or <F12> to PXE Boot.” 信息时，如下图所示，按下 “Del” 。

按下 “Del” 键的时间不同会看到屏幕显示信息有略微差异。

图 16-2 BIOS 启动界面



4. 进入 BIOS 后的界面示例如下图所示。

图 16-3 BIOS Main 界面



# 17 设置 U-Boot 密码

## 17.1 功能特性

U-Boot 命令主要用于加载底层软件、调试底层设备,属于调试命令。一般情况下登录 U-Boot,需要使用串口设备,这个是物理安全的。登录 U-Boot,需要输入密码,这个密码不属于 BMC 的用户管理范畴。如果需要修改这个密码,可以使用 ipmitool 工具进行修改。

## 17.2 Linux 下修改 U-Boot 密码

操作场景:

指导您在 Linux 系统下修改 U-Boot 密码。

操作步骤:

1. 安装 ipmitool 工具,具体操作说明请参见 [18.1 IPMITOOL 介绍](#)。
2. 登录 OS,使用命令“ipmitool raw 0x3c 0x18 <Length> <Password Data>”修改密码,具体参数参考下述表格。示例:如果需要将密码修改为 123456,命令为“ipmitool raw 0x3c 0x18 0x06 0x31 0x32 0x33 0x34 0x35 0x36”。

表 17-1 U-Boot 密码修改参数

Request	NetFn	0x3c	
	Command	0x18	
	Byte[1]	Length	密码长度,最大为31 (0x1FH)
	Byte[2-n]	Password Data	只支持可打印字符 (0x20-0x80),不允许密码为空,为对应密码字符的ASCII码。
Response	Byte[0]	Complete Code	0: 成功 其它: 失败

# 18 常用工具

## 18.1 IPMITOOL 介绍

### 18.1.1 用途及使用场景

通常 ipmitool 被用来发送 IPMI 命令，可以在主机 OS 上发送 Open 接口的带内命令，也可以用于远程机来发送 LAN 接口的 IPMI 带外命令。ipmitool 有 Windows 版本和 Linux 版本。在 Open 接口下，只支持 Linux 版本。

支持的接口：

- Open, Linux OpenIPMI 接口【缺省】。
- LANPLUS, IPMI v2.0 RMCP+ LAN 接口。

### 18.1.2 Linux 下 IPMITOOL 的安装与使用

在 Linux 系统下安装 ipmitool，需要安装两个软件包 openipmi 和 ipmitool。Openipmi 为 ipmitool 提供内核驱动，使得 ipmitool 能够通过 Open 接口访问本地服务器 BMC。

支持的 ipmitool 命令可参考下文，具体使用方法和参数列表可参见命令行帮助。使用“ipmitool -h”查看帮助信息，如下图所示，是 ipmitool 帮助信息返回的支持命令部分截图。



图 18-1 ipmitool cmd

```
Commands:
raw          Send a RAW IPMI request and print response
i2c         Send an I2C Master Write-Read command and print response
spd         Print SPD info from remote I2C device
lan         Configure LAN Channels
chassis     Get chassis status and set power state
power       Shortcut to chassis power commands
event       Send pre-defined events to MC
mc          Management Controller status and global enables
sdr         Print Sensor Data Repository entries and readings
sensor      Print detailed sensor information
fru         Print built-in FRU and scan SDR for FRU locators
gendev      Read/Write Device associated with Generic Device locators sdr
sel         Print System Event Log (SEL)
pef         Configure Platform Event Filtering (PEF)
sol         Configure and connect IPMIv2.0 Serial-over-LAN
tsol        Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol        Configure IPMIv1.5 Serial-over-LAN
user        Configure Management Controller users
channel     Configure Management Controller channels
session     Print session information
dcmi        Data Center Management Interface
nm          Node Manager Interface
sunoem      OEM Commands for Sun servers
kontronoem  OEM Commands for Kontron devices
picmg       Run a PICMG/ATCA extended cmd
fwum        Update IPMC using Kontron OEM Firmware Update Manager
firewall    Configure Firmware Firewall
delloem     OEM Commands for Dell systems
shell       Launch interactive IPMI shell
exec        Run list of commands from file
set         Set runtime variable for shell and exec
hpm         Update HPM components using PICMG HPM.1 file
ekalyzer    run FRU-Ekeying analyzer using FRU files
ime         Update Intel Manageability Engine Firmware
vita        Run a VITA 46.11 extended cmd
```

## 18.2 openssl 介绍

### 18.2.1 用途及使用场景

openssl 是一个安全套接字层密码库，囊括主要的密码算法、常用密钥、证书管理功能及实现 ssl 协议。openssl 整个软件包大概可以分成三个主要的功能部分：SSL 协议库 libssl、应用程序命令工具以及密码算法库 libcrypto。

### 18.2.2 Linux 下的 openssl 安装和使用

在 Linux 系统下安装 openssl，需要安装两个软件包：openssl 和 libssl-dev。具体使用方法和参数列表可参见命令行帮助。使用“openssl help”查看帮助信息，如下图所示，是 openssl 帮助信息返回的支持命令部分截图。

图 18-2 openssl cmd

```
$ openssl help
Standard commands
asn1parse      ca              ciphers         cms
crl            crl2pkcs7      dgst            dhparam
dsa           dsaparam       ec              ecpam
enc           engine         errstr         gendsa
genpkey       genrsa         help           list
nseq         ocs           passwd        pkcs12
pkcs7        pkcs8         pkey          pkeyparam
pkeyutl      prime         rand          rehash
req          rsa           rsautl        s_client
s_server     s_time        sess_id       smime
speed        spkac         srp           storeutl
ts          verify        version       x509

Message Digest commands (see the `dgst' command for more details)
blake2b512    blake2s256    gost           md2
md4           md5           rmd160        sha1
sha224       sha256        sha3-224      sha3-256
sha3-384     sha3-512      sha384        sha512
sha512-224   sha512-256    shake128       shake256
sm3

Cipher commands (see the `enc' command for more details)
aes-128-cbc   aes-128-ecb   aes-192-cbc   aes-192-ecb
aes-256-cbc   aes-256-ecb   aria-128-cbc   aria-128-cfb
```