浪潮英信服务器

CMC 配置手册

文档版本 1.1

发布日期 2021-10-29

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	2021-06-04	首版发布
V1.1	2021-10-29	优化格式

目 录

1 概述

1.1 文档用途

本文档详细介绍 CMC 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。

说明

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 适用范围

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 i24M6	●			●
浪潮英信服务器 i48M6	●			●

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

CMC 支持通过专用口进行访问。在使用前需要先知道 CMC 管理口的 IP 地址。管理网口的 IP 可以在 BIOS Setup 界面下查看。

2.2 BIOS 下获取管理网口 IP

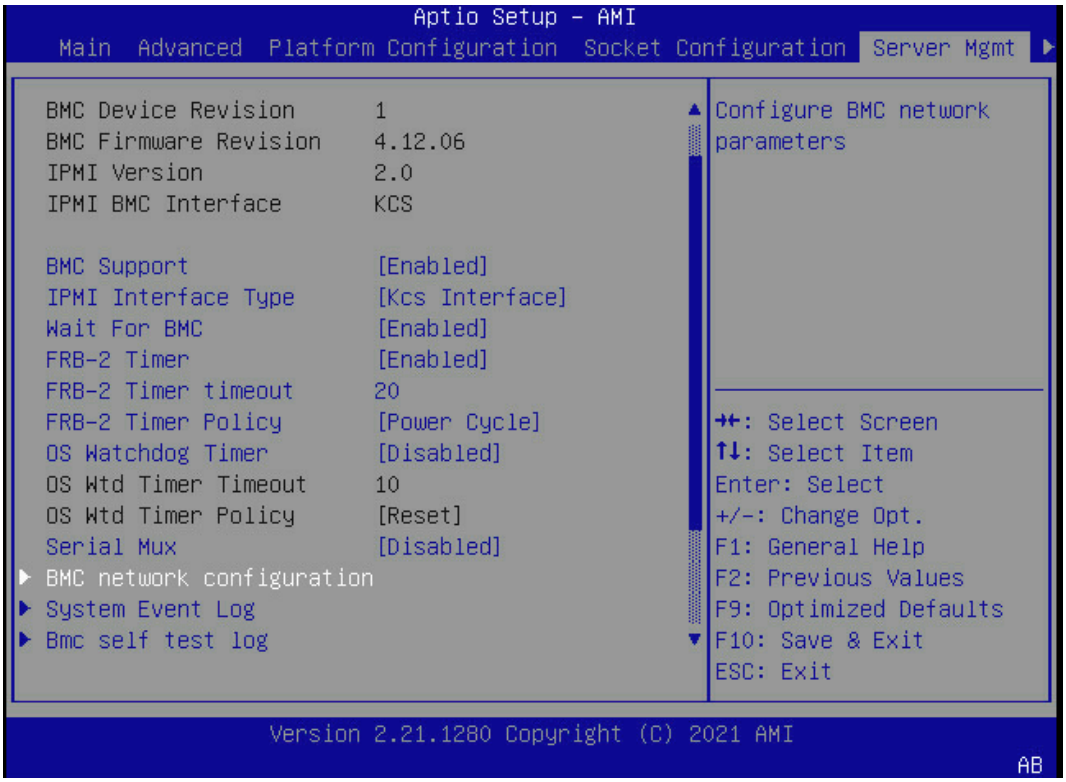
操作场景

通过 BIOS 获取管理网口的 IP。

操作步骤

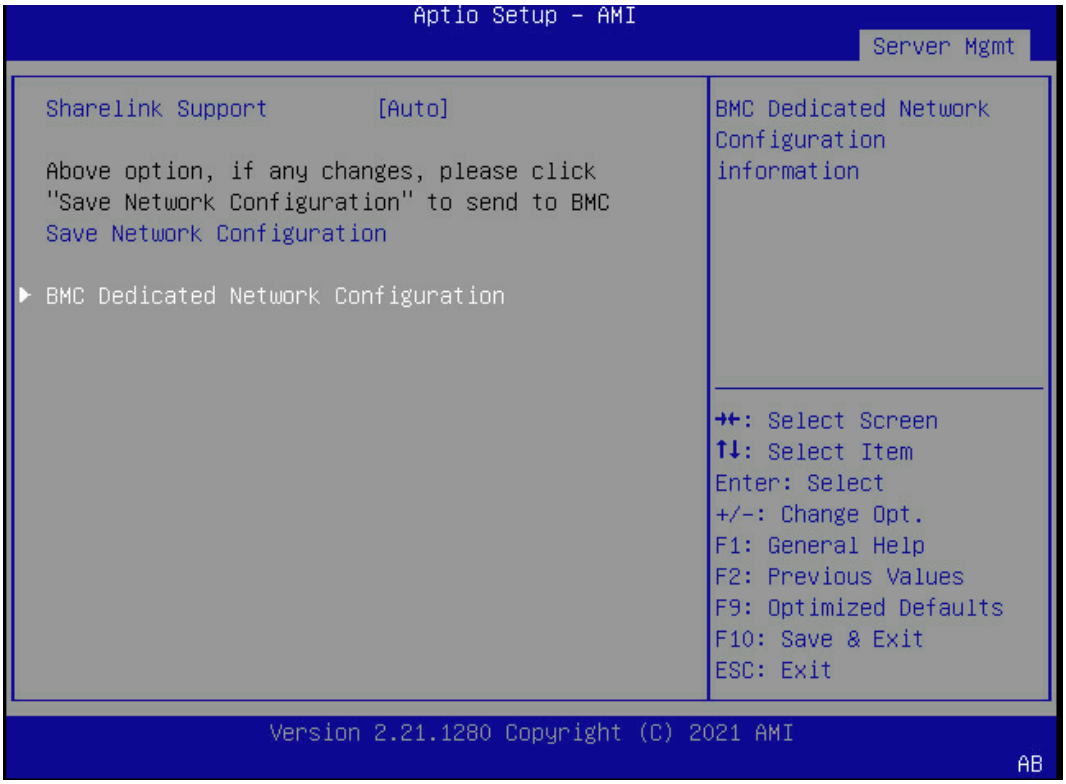
1. 进入 BIOS Setup 界面，具体操作说明请参见 14.2 本地进入 BIOS 系统界面。
2. 选择 Server Mgmt 界面，如下图所示。

图 2-1 Server Mgmt 界面



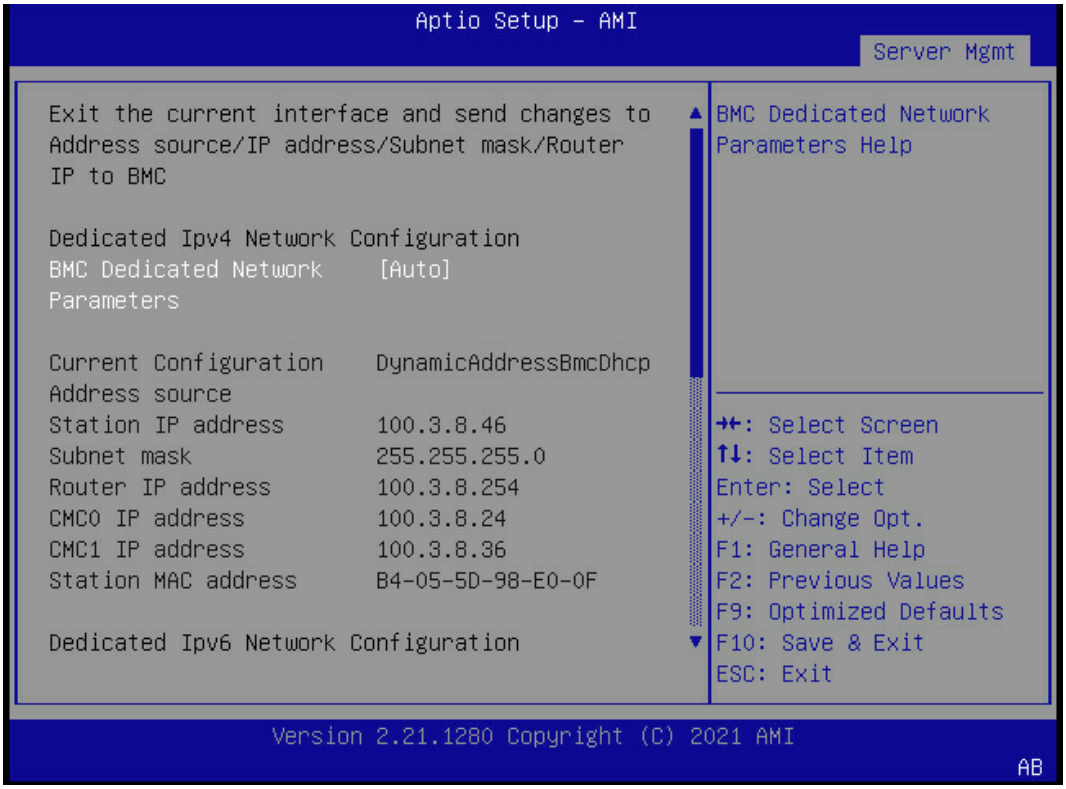
3. 选择“BMC network configuration”，按“Enter”进入，如下图所示。

图 2-2 BMC network configuration 界面



4. 选择“BMC Dedicated Network Configuration”，按“Enter”进入，可查看当前 BMC Dedicated 网络参数的配置情况，如图 2-3 所示。通过这个界面就能够看到 CMC 管理网口目前的 IP 地址：CMC0 IP address 和 CMC1 IP address。

图 2-3 BMC Dedicated Network Configuration 界面



3 用户管理

3.1 功能特性

用户管理功能主要用来展示 CMC 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

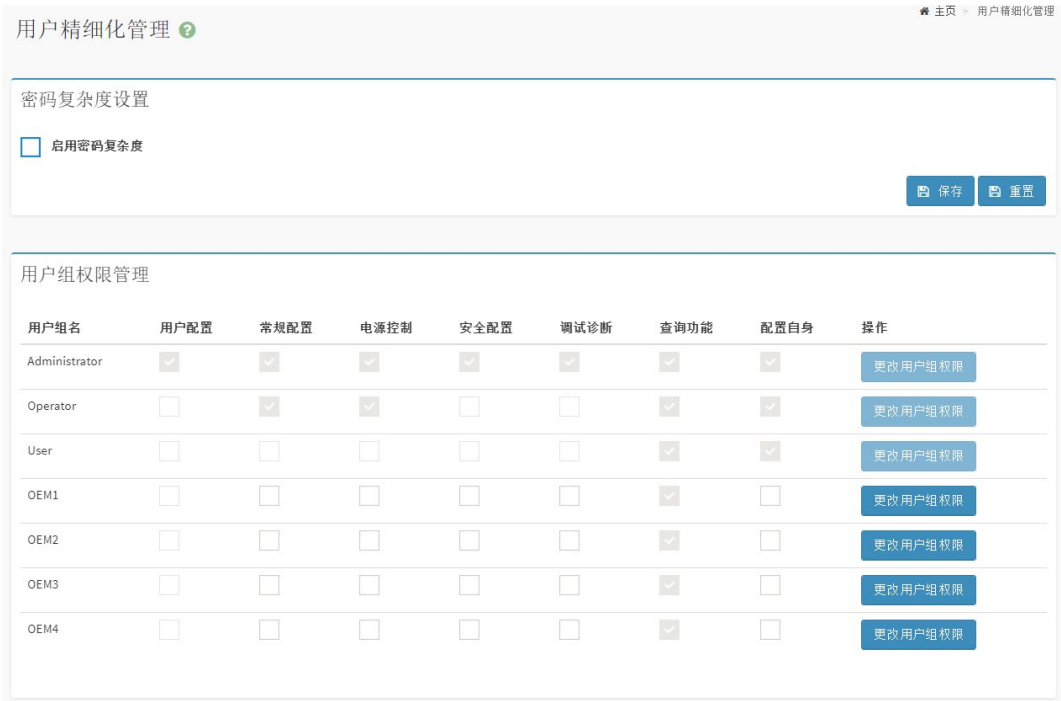
操作场景

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“CMC 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，请选中“启用密码复杂度”复选框，如果不需要启用，则取消这个复选框，然后点击保存按钮。对于表格的字段描述，可以参考表 3-1。点击启用复选框后，会弹出如下图所示的对话框。

图 3-2 用户精细化管理密码复杂度设置对话框

3. 系统缺省用户组 Administrator、Operator 和 User 无法进行用户权限修改。其它的四个定制化用户在 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 3-2 和表 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	• 勾选，启用密码复杂度。 • 不勾选，不启用密码复杂度限制。
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	• 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、

参数	描述
	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。 • 不勾选，不启用密码复杂度限制。
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5~60min。

表 3-2 用户权限管理

用户组	权限
管理员	用户配置、常规配置、电源控制、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、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、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IP设置、节点开关机以及UID定位操作、节点BMC IP设置、多机箱CMC IP设置。
电源控制	电源控制。
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	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、用户配置外的其他信息。
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

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“CMC 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

3.4 添加用户

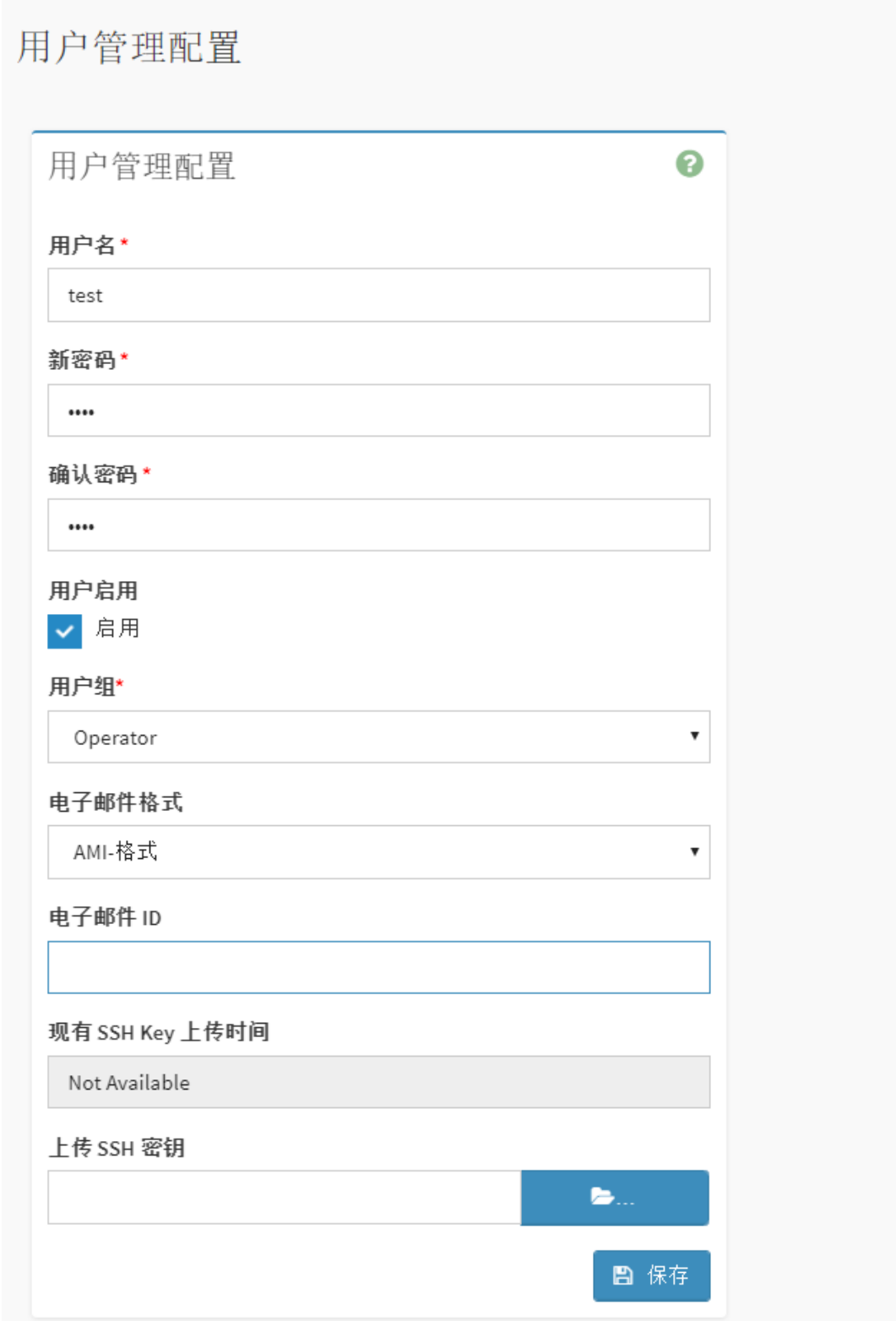
操作场景

通过 Web 管理界面添加用户。

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



添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	输入新用户的用户名。 • 用户名是一个1到16个字母和数字的字符串，包括'-'、'_'、'@'，必须以字母开头，区分大小写。 • 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。 • sshd、ntp、stunnel4、sysadmin、daemon是保留用户名，不能使用。
密码长度	可以选择16字节或者20字节密码，默认选择16字节密码。 如果选择16字节密码，最大可以输入16个字符。如果选择20字节密码，最大可以输入20个字符。 提示：20字节密码，LAN会话将无法建立。
新密码	输入并确认新密码。 • 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。 • 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。 提示：不允许密码长度超过16个字符。
确认密码	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	• AMI格式。 • FixedSubject格式。
电子邮件ID	输入用户的电子邮箱ID，如果用户忘记了密码，新密码会发送到此处配置的电子邮件ID中。 提示：必须配置SMTP服务器，才能发送电子邮件。
现有SSH Key上传时间	将显示已上传的SSH密钥信息（只读）。
上传SSH密钥	使用“  ”按钮导航到SSH的公共密钥文件。 • SSH密钥文件应该是.pub类型。

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

3.5 更改用户

操作场景

通过 Web 管理界面更改用户。

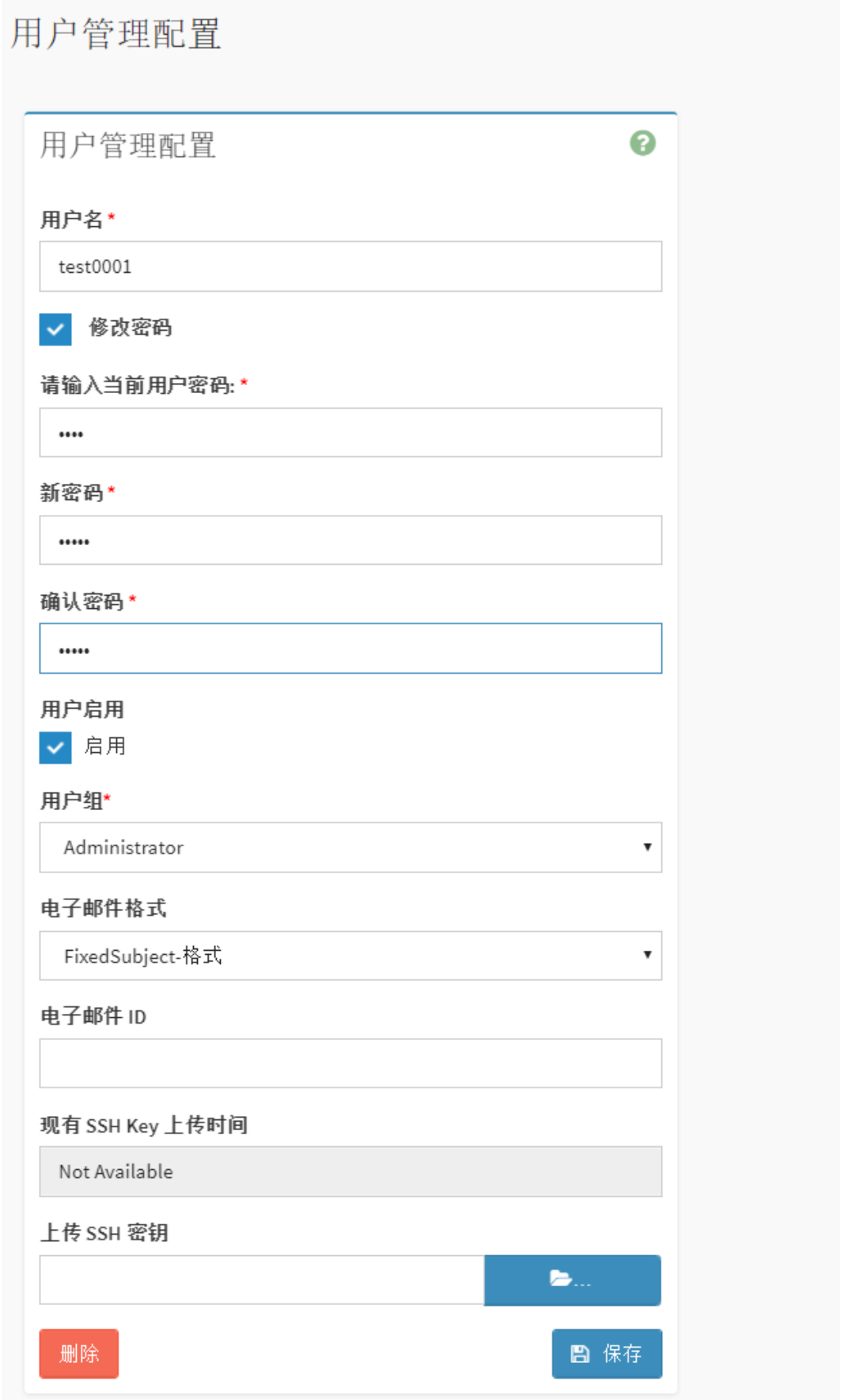
操作步骤

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

2. 页面显示当前用户相关配置信息，可在页面上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
FixedSubject-格式
电子邮件 ID
现有 SSH Key 上传时间
Not Available
上传 SSH 密钥
删除
保存

3.6 删除用户

操作场景

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

2. 点击“删除用户”按钮后，页面会弹出窗口询问是否确认要删除此用户，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

4 网络设置

4.1 功能特性

网络设置模块主要提供获取 CMC 网络配置信息、配置 CMC 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

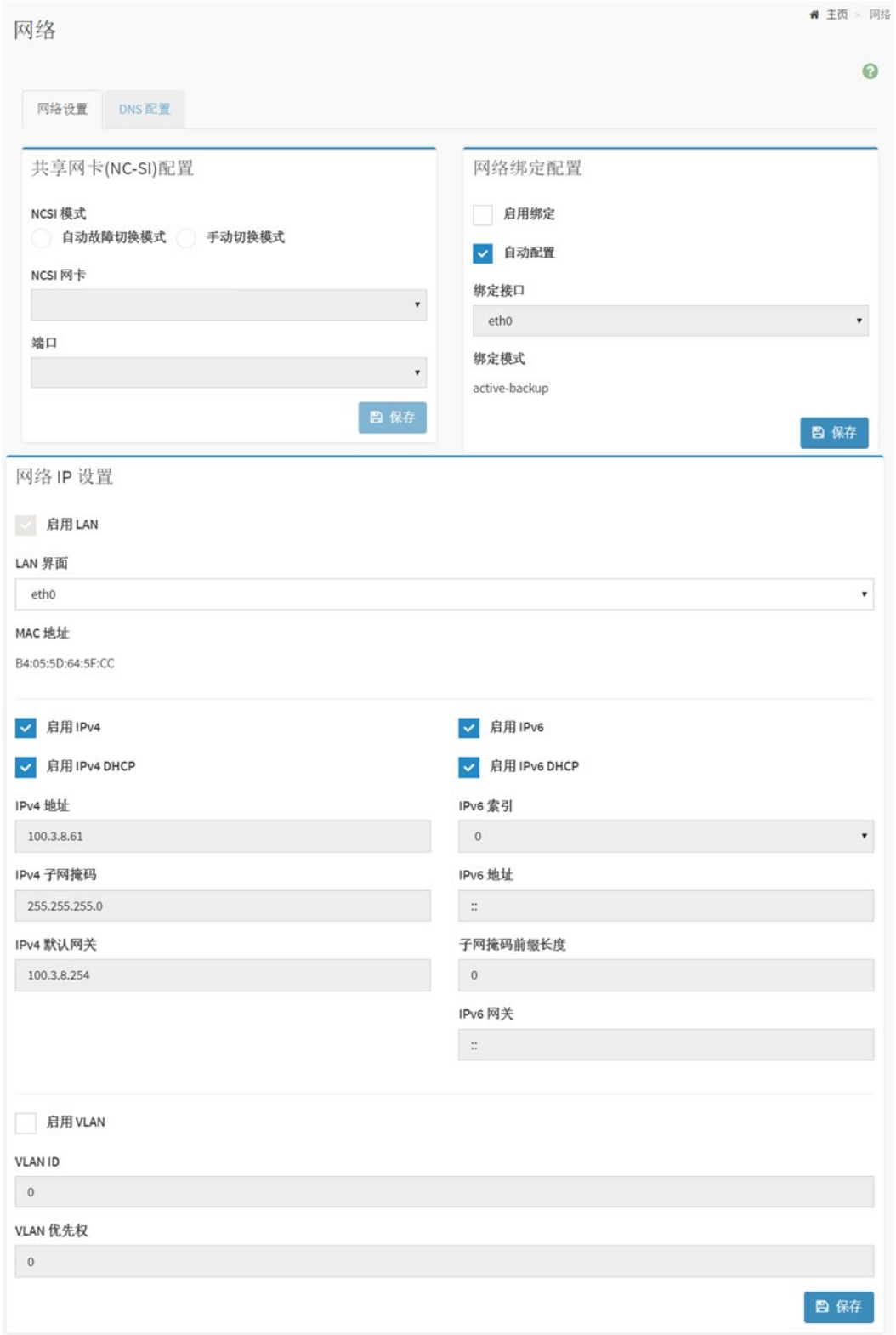
操作场景

通过 Web 管理界面删除用户。

操作步骤

1. 登录到 Web GUI，进入“CMC 设置>网络”页面，点击“网络设置”TAB 页，此页面用于网络 IP 设置，如下图 4-1 所示。

图 4-1 网络 IP 设置



CMC 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。可选项为：eth0。
MAC地址	此字段显示选定的接口（只读）的MAC地址。
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	启用“启用IPv4 DHCP”，IPv4地址使用动态主机配置协议（DHCP）。
IPv4地址	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。 • IP地址包含以逗点隔开的4组数字"xxx.xxx.xxx.xxx"。 • 每组数字范围0到255。 • 第一组数字不能为0。
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	启用“启用IPv6 DHCP”，IPv6地址使用动态主机配置协议（DHCP）。
IPv6索引	选择IPv6索引。
IPv6地址	为选定的接口配置指定一个静态IPv6地址。
子网掩码前缀长度	指定IPv6设置的子网掩码前缀长度。
IPv6网关	设置IPv6的默认网关。 • 数值范围0到128。
VLAN配置	
启用VLAN	选择此选项以启用VLAN选定接口的支持。
VLAN ID	指定VLAN配置的ID。 • 数值范围1到4094。 提示：VLAN ID更新后必须要进行重启。
VLAN优先权	指定VLAN配置的优先级。 • 数值范围0到7。 提示：7是VLAN配置的最高优先级。

4.3 网络 IP 设置

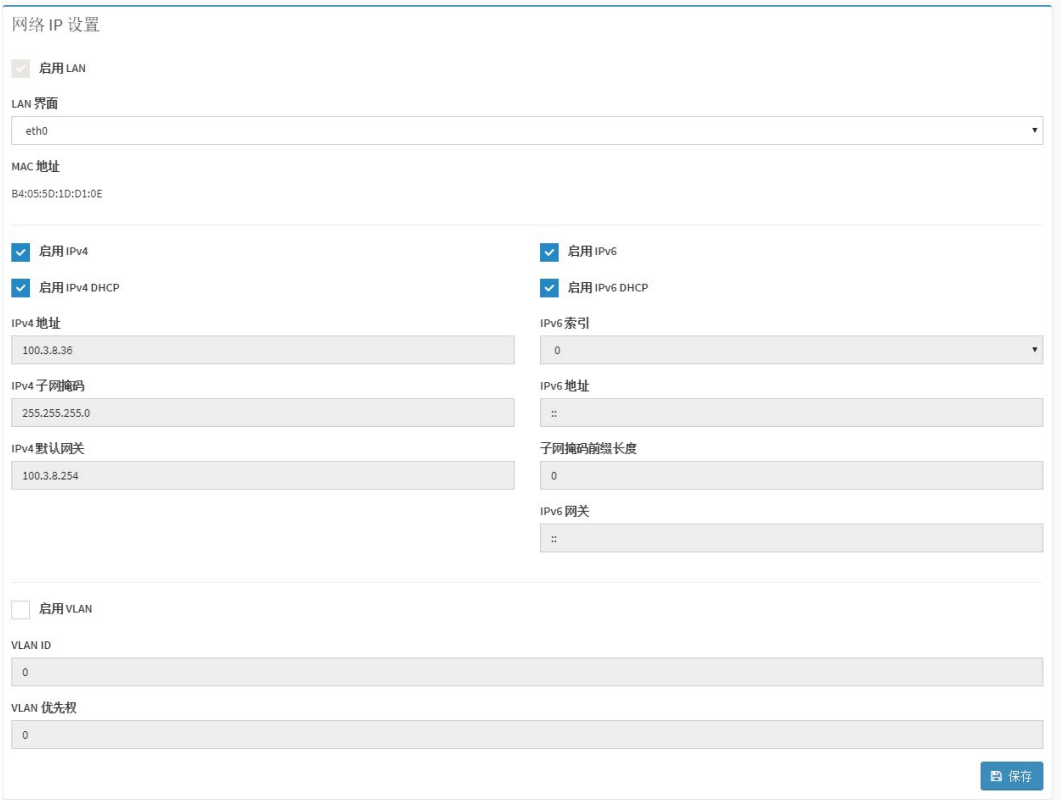
操作场景

通过 Web 管理界面设置 IP 地址。

操作步骤

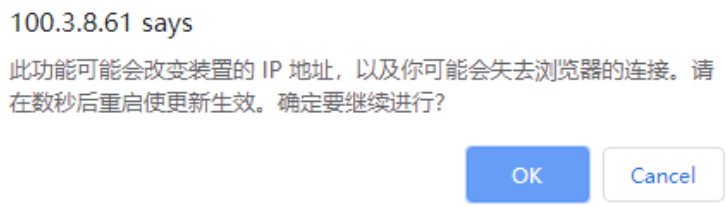
1. 登录到 Web GUI，进入“CMC 设置>网络”页面，点击“网络设置”标签页。
2. 首先选择 LAN 界面，选择需要配置的网络接口。
3. 选中或者取消启用 LAN 按钮，以确认这个网口是否启用。
4. 选中或者取消 IPv4、IPv6 按钮，以确认是否启用 IPv4、IPv6。
5. 如果启用了 IPv4,再选中或者取消 IPv4 DHCP;如果不启用 IPv4 DHCP,则手动进行 IPv4 相关设置，包括地址、子网掩码、默认网关。
6. 如果启用了 IPv6,再选中或者取消 IPv6 DHCP;如果不启用 IPv6 DHCP,则手动进行 IPv6 相关设置，包括索引、地址、子网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

图 4-2 IP 设置



7. 点击“保存”按钮，保存设置，会弹出如下提示框。选择“Cancel”取消网络 IP 设置动作；选择“OK”确认修改网络 IP 设置。如下图所示。IP 地址变化后，需要使用新的 IP 地址来访问 CMC。

图 4-3 IP 设置提示对话框



4.4 VLAN 设置

操作场景

通过 Web 管理界面设置 VLAN。

操作步骤

1. 登录到 Web GUI，进入“CMC 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 优先权信息，如下图所示。
2. 填写完成后，点击“保存”按钮。

图 4-4 VLAN 配置

4.5 DNS 设置

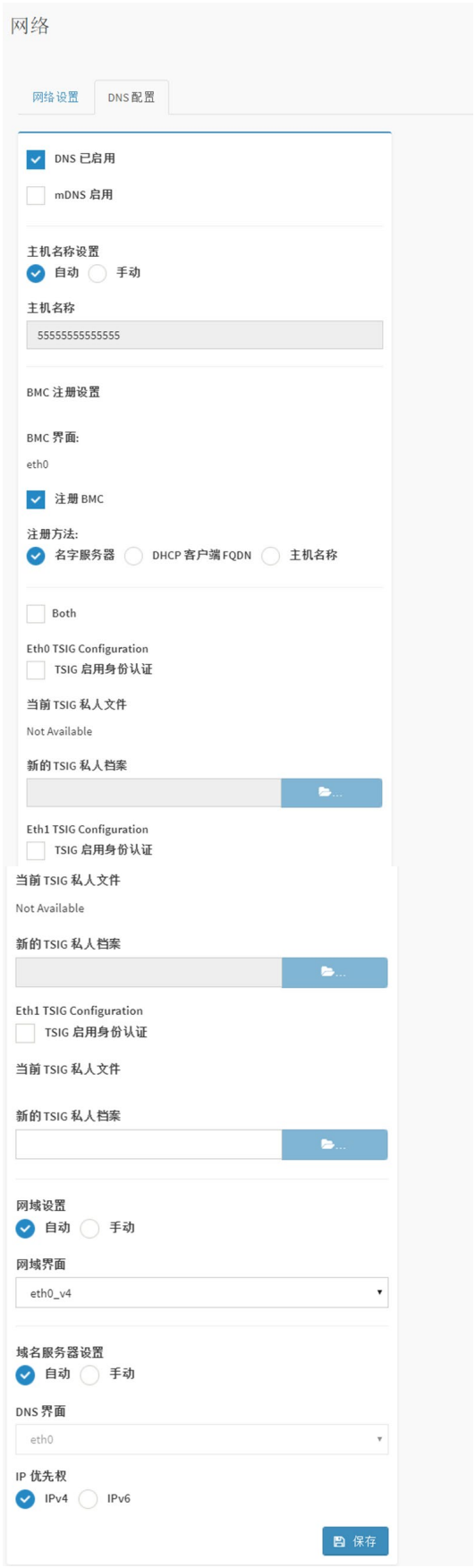
操作场景

通过 Web 管理界面进行 DNS 设置。

操作步骤

1. 登录到 Web GUI，进入“CMC 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 优先权”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，CMC 自动配置相关参数。

图 4-5 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
555555555555
BMC 注册设置
BMC 界面:
eth0
注册 BMC
注册方法:
名字服务器
DHCP 客户端 FQDN
主机名称
Both
Eth0 TSIG Configuration
TSIG 启用身份认证
当前 TSIG 私人文件
Not Available
新的 TSIG 私人档案
Eth1 TSIG Configuration
TSIG 启用身份认证
当前 TSIG 私人文件
Not Available
新的 TSIG 私人档案
Eth1 TSIG Configuration
TSIG 启用身份认证
当前 TSIG 私人文件
新的 TSIG 私人档案
网域设置
自动
手动
网域界面
eth0_v4
域名服务器设置
自动
手动
DNS 界面
eth0
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 4-2 DNS 配置参数

参数	描述
DNS设置	
DNS已启用	• 勾选：启用所有的DNS服务。 • 不勾选：不启用DNS服务。
mDNS启用	• 勾选：启用所有的mDNS服务。 • 不勾选：不启用mDNS服务。
主机名称设置	
主机设置	选择自动或手动设置。
主机名称	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	eth0
注册BMC	• 勾选：注册BMC。 • 不勾选：不注册BMC。
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来向DNS服务器注册。 • 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。
Both	点击复选框来启用TSIG身份认证（只在通过名字服务器来注册DNS时）。
Eth0 TSIG Configuration	• 勾选：TSIG启用身份认证。 • 不勾选：TSIG不启用身份认证。
当前TSIG私人文件	显示当前TSIG私人文件的日期（只读）。
新的TSIG私人档案	浏览一个新的TSIG私人档案来上传。
网域设置	

参数	描述
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	
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优先权	
IP优先权	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

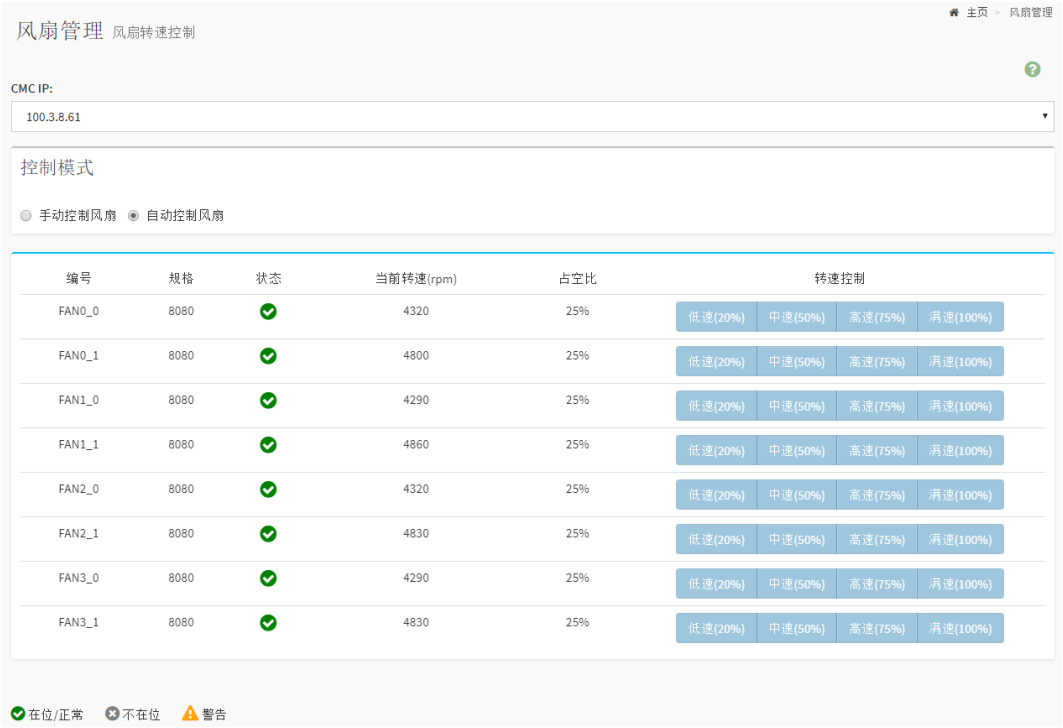
操作场景

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

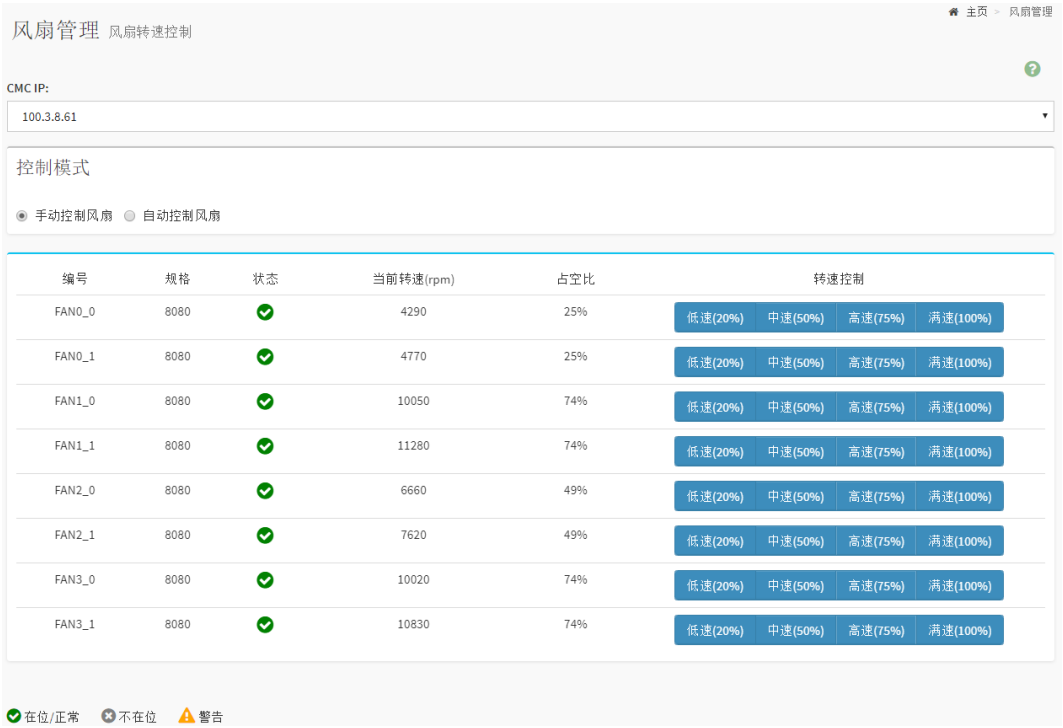
通过 Web 管理界面设置风扇控制模式为手动。

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%，可以在第一行点击“中速”按钮。

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 CMC 日志收集和分析指南》。

6.3 Syslog 日志设置

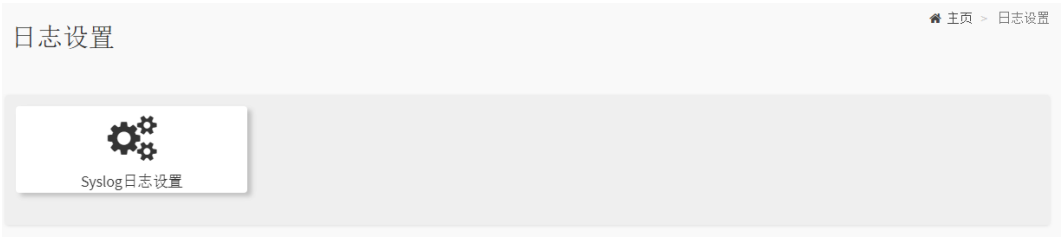
操作场景

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”、“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： • 本地日志 • 远程日志
Syslog主机标识	Syslog主机标识，可选为： • 主机名 • 单板序列号 • 产品资产标签
告警级别	高于此告警级别的事件将被发送，可选为： • warning • info • critical

参数	描述
传输协议	传输协议，可选为： • UDP • TCP • TLS（单项认证，双向认证） 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 设置 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，也可多选。
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 CMC 时间设置

7.1 功能特性

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

7.2 NTP 自动同步

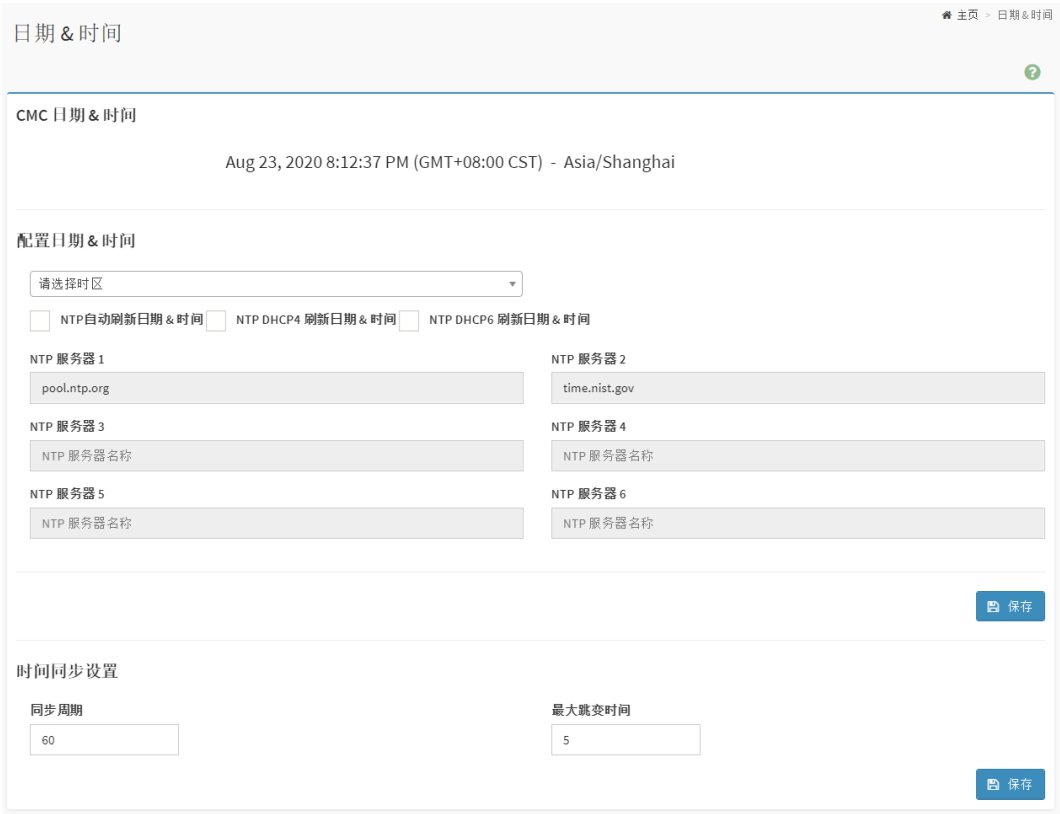
操作场景

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“CMC 设置>日期&时间”页面，此页面显示当前的 CMC 时间和 NTP 设置。如下图所示：

图 7-1 NTP 自动同步配置页面



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 服务器以及 NTP 同步周期和最大跳变进行设置，实现 NTP 自动同步配置，点击“OK”按钮，保存配置。

图 7-2 NTP 配置确认对话框

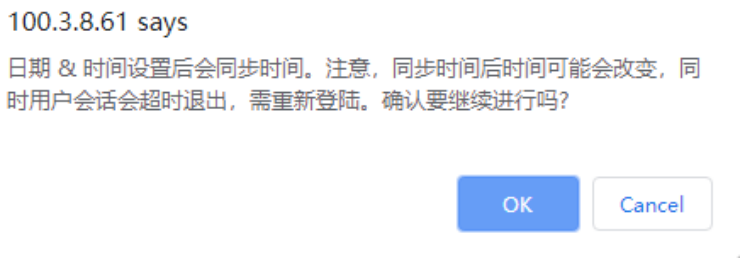
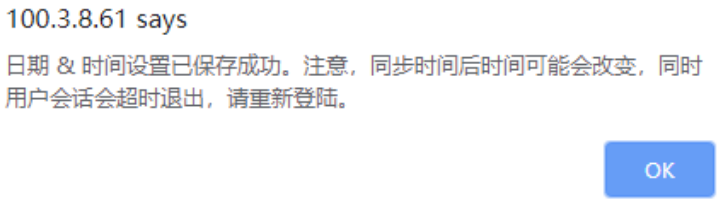


图 7-3 NTP 配置成功提示框



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

通过 Web 管理界面进行 SNMP Trap 设置。

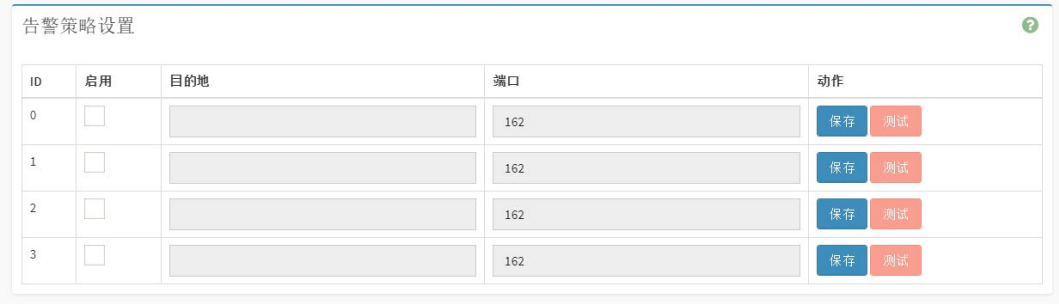
操作步骤

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

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，端口号为端口，点击“保存”。保存后，点击“测试”按钮，在 SNMP Trap 的接收端可以得到一条测试消息。

图 8-2 告警策略设置



9 CMC 服务设置

9.1 功能特性

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

9.2 服务设置

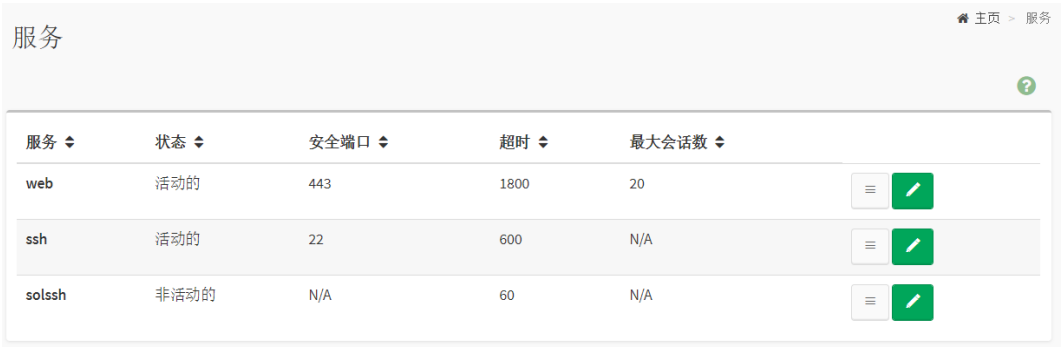
操作场景

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“CMC 设置>服务”页面，此页面显示了 CMC 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 9-1 服务设置页面



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 9-2 修改服务配置

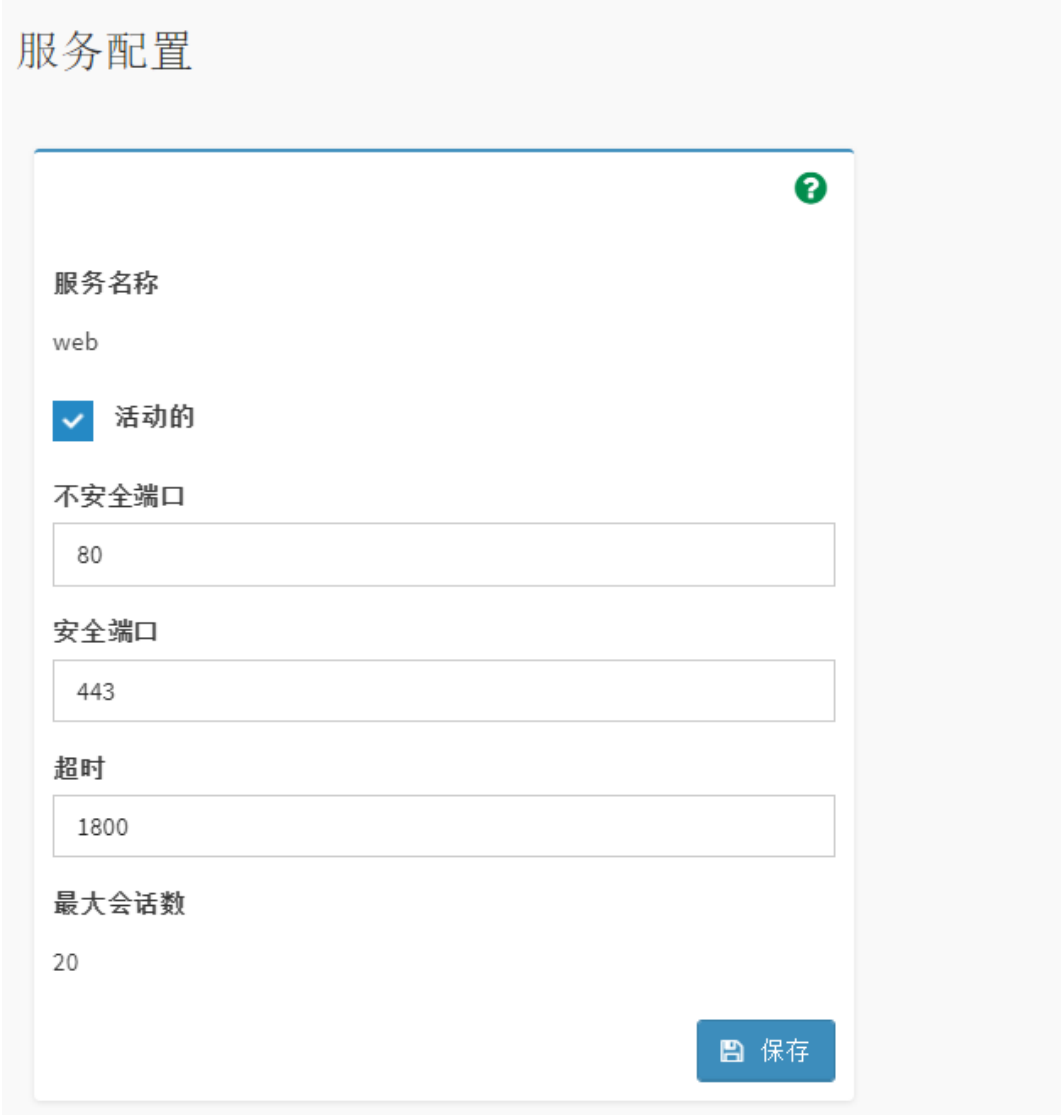
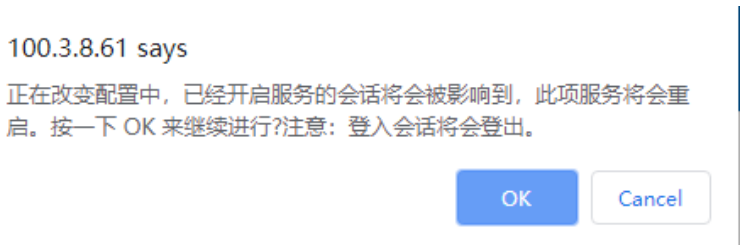


图 9-3 服务重启确认对话框



CMC 服务设置相关参数如下表所示：

表 9-1 服务设置

参数	描述

参数	描述
服务	显示选定行（只读）的服务名称。
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。
非安全端口	用于配置服务的非安全端口号。 • Web默认端口为80。 • Solssh的默认端口是N/A。 • 端口值范围从1到65535。 提示：SSH服务不支持非安全端口。
安全端口	用于配置服务的安全端口号。 • Web默认端口为443。 • SSH的默认端口是22。 • 端口值范围从1到65535。 提示：Solssh服务不支持安全端口。
超时	用于配置服务会话超时值。 • Web超时数值范围为300到1800秒。 • SSH and Solssh超时数值范围为60到1800秒。 • 超时值应该为60秒的倍数。
最大会话数	当前服务最大会话数量。

10 固件升级

10.1 功能特性

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

10.2 操作指导

请参考《浪潮英信服务器 CMC 升级手册》。

11 恢复出厂设置

11.1 功能特性

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

11.2 恢复出厂设置

操作场景

通过 Web 管理界面将 CMC 恢复到出厂设置。

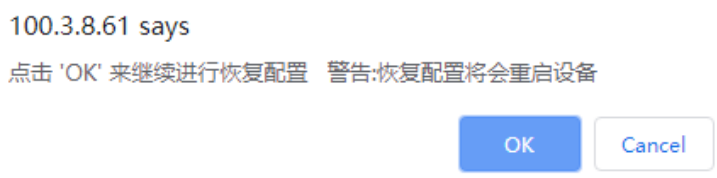
操作步骤

1. 登录 Web GUI，进入“系统维护>恢复出厂设置”。

图 11-1 恢复出厂设置页面

2. 点击“保存”按钮，会弹出以下提示框，点击“OK”按钮。

图 11-2 恢复出厂设置提示框



3. 恢复出厂设置成功。

12 SSL 设置

12.1 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。

12.2 在线生成 SSL 凭证

操作场景

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“CMC 设置>SSL 设置”，选择“产生 SSL 认证”。

图 12-1 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 12-1。

图 12-2 生成 SSL 凭证界面

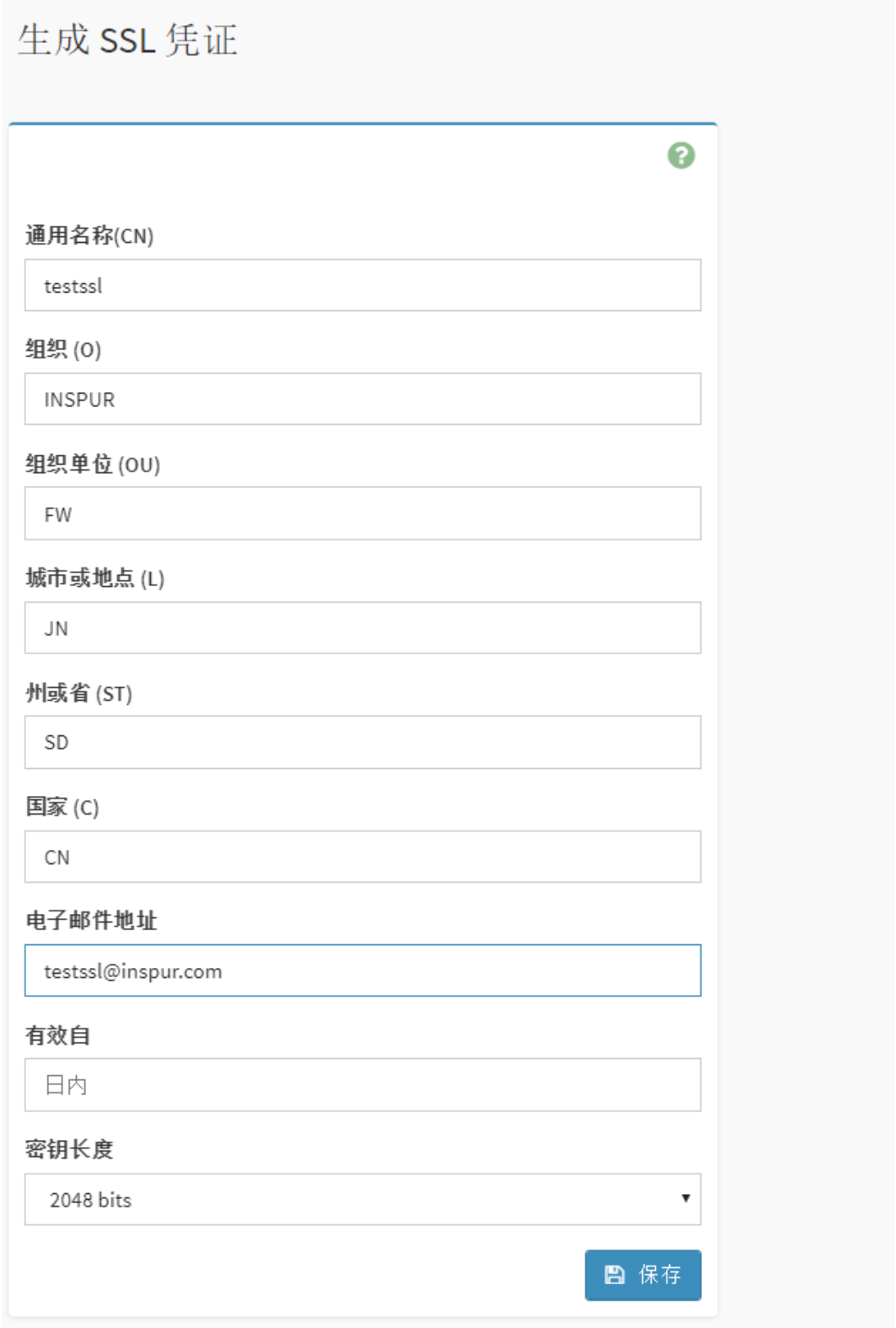


表 12-1 SSL 设置

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（L）	城市或地点，比如济南市缩写JN。
州或省（ST）	州或省，比如山东省缩写SD。
国家（C）	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。
密钥长度	密钥长度，可以使用缺省2048。

12.3 生成 SSL 凭证并上传

操作场景

自己生成 SSL 凭证，并通过 Web 管理界面上传。

操作步骤

1. 安装 OpenSSL 工具，具体操作说明请参见 15.2 OpenSSL 介绍。本操作步骤是使用 OpenSSL 工具生成证书，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（参考表 12-2），openssl req -new -key privkey.pem -out cert_req.pem。

表 12-2 证书请求输入项

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
```

```
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:SD
Locality Name (eg, city) []:JN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:INSPUR
Organizational Unit Name (eg, section) []:FW
Common Name (e.g. server FQDN or YOUR name) []:webssl
Email Address []:websstest@inspur.com

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“CMC 设置>SSL 设置”，选择“上传 SSL 认证”，如图 12-1。
7. 在弹出的对话框中，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，如图 12-3。

图 12-3 上传 SSL 凭证界面

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

图 12-4 查看 SSL 凭证界面

13 Redfish

13.1 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，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。

13.2 操作指导

CMC Redfish 具体操作请参考文档《浪潮英信服务器 Redfish 用户手册》，如您需要使用此文档请联系浪潮技术服务人员获取。

14 进入 BIOS 系统

14.1 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。有 CMC 的服务器系统，也能够通过 BIOS 看到 CMC 的网络配置信息。

14.2 本地进入 BIOS 系统

操作场景

通过本地键盘显示器，进入 BIOS 系统。

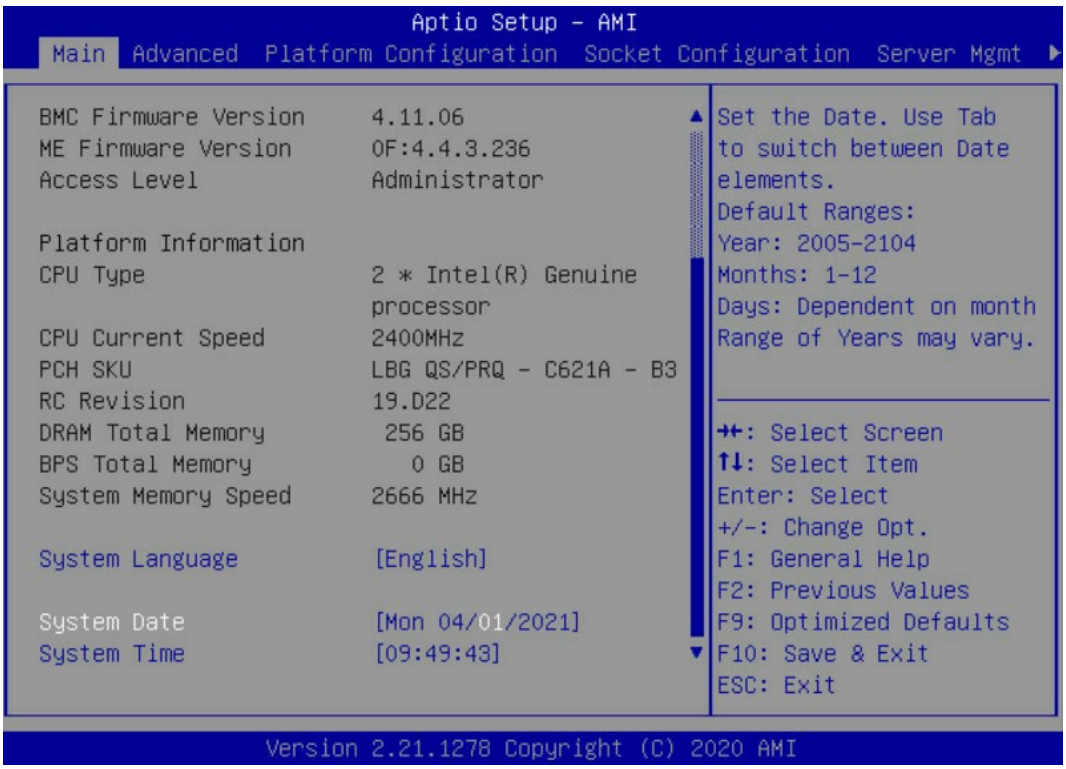
操作步骤

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. 系统开始引导，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 14-1 BIOS Logo 界面

4. 进入 BIOS 后的界面示例如下图所示。

图 14-2 BIOS Setup 界面



15 常用工具

15.1 IPMItool 介绍

15.1.1 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 KCS 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 Window 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。

15.1.2 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。在访问 CMC 时，只能使用 LANPLUS 接口。

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 帮助信息返回的部分支持命令截图。

图 15-1 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
        ekanalyzer      run FRU-Ekeying analyzer using FRU files
        ime             Update Intel Manageability Engine Firmware
        vita            Run a VITA 46.11 extended cmd
```

15.2 OpenSSL 介绍

15.2.1 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、证书封装管理功能及实现 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。

15.2.2 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 帮助信息返回的部分支持命令截图。

图 15-2 OpenSSL cmd