浪潮英信服务器

BIOS 用户手册

文档版本 V1.1

发布日期 2021-05-25

版权所有 © 2021 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。

环境保护

请将我方产品的包装物交废品收购站回收利用，以利于污染预防，共同营造绿色家园。

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。

安全声明

服务器产品安全一直是浪潮关注的焦点，保障产品安全是浪潮的关键战略之一。为使您更清晰地了解服务器产品，请注意如下安全风险声明。

a. 在调整用途或淘汰服务器时，为了保护数据隐私，允许从 BIOS、BMC 中恢复固件出厂设置、删除信息、清除日志。同时，建议采用第三方安全擦除工具对硬盘数据进行全面安全擦除。

b. 您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如告警邮件接收地址、IP 地址），故您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施，以确保用户的个人数据受到充分的保护。

c. 服务器开源软件声明的获取，请直接联系浪潮客户服务人员咨询。

d. 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。

e. 浪潮建立了产品安全漏洞应急和处理机制，保证第一时间及时处理产品安全问题。若您在浪潮产品中发现任何安全问题，或者寻求有关产品安全漏洞的必要支持，可以直接联系浪潮客户服务人员。

浪潮将一如既往的严密关注产品与解决方案的安全性，为客户提供更满意的服务。

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。

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　　箱：lckf@inspur.com

邮　　编：250101

浪潮专有 翻印必究

前言

摘要

本手册介绍本服务器软件设置的相关内容。

目标受众

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

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

- 如您未采购装机服务，请在设备开箱前自行检查外包装箱。如发现包装箱严重损坏、水浸、封条或压敏胶带已开封，请视购机方式进行问题反馈。供应商渠道购入设备，请直接与您的供应商联系；浪潮直营渠道购入设备，请直接拨打服务电话4008600011，联系浪潮技术支持处理。
- 请不要随意拆装服务器组件、请不要随意扩配及外接其它设备。如需操作，请务必在浪潮的官方授权和指导下进行。
- 在拆装服务器组件前，请务必断开服务器连接的所有电缆。
- 请使用浪潮认证的驱动程序进行 OS 环境搭建。您可访问浪潮官网进行驱动下载，进入浪潮官网首页，顶部导航栏选择支持下载 > 产品支持 > 驱动下载，根据页面提示查找产品对应的驱动程序。如使用非浪潮认证的驱动程序，可能会引起兼容性问题并影响产品的正常使用，对此浪潮将不承担任何责任或义务。
- BIOS、BMC 的设置对配置您的服务器至关重要，如果没有特殊的需求，请您使用系统出厂时的默认值，请勿随意更改参数设置。首次登录时，请及时修改 BMC 用户密码。

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。

图标	说明
 危险	如不当操作，可能会导致死亡或严重的人身伤害。
 警告	如不当操作，可能会导致中度或轻微的人身伤害。
 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	对手册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	2021-04-19	首版发布
V1.1	2021-05-25	优化文档描述

目 录

1 概述

1.1 BIOS 简介

BIOS（基本输入输出系统）是计算机硬件系统上最基本的软件代码。BIOS 程序嵌入在计算机主板 SPI 芯片中，它的主要功能是上电自检、CPU 及内存初始化、检测输入输出设备以及可启动设备并最终引导操作系统启动，其在系统中的位置如图 1-1 所示。

图 1-1 BIOS 在系统中的位置

浪潮 M6 服务器 BIOS 是以 AMI 的 Codebase 为基础开发,支持 Legacy 和 UEFI 环境操作，具有丰富的带内带外配置功能和丰富的可扩展特性，可满足不同客户定制化需求。

1.2 适用产品

本手册适用于以下产品：

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 SN5160FM6	●			

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 SN5264FM6	●			
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	●			
浪潮英信服务器 NF5260FM6	●			
浪潮英信服务器 NF5466M6	●			
浪潮英信服务器 NF5266M6	●			
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i24LM6	●			●
浪潮英信服务器I48M6	●			●

1.3 注意事项

1. 由于产品版本升级或其他原因，本文档内容会不定期进行更新。如需查看最新的 BIOS 界面，建议从 Inspur 官网获取最新 BIOS 固件版本。
2. 本文为通用产品资料，所列出的选项名和默认值均以 Inspur M6 通用两路和四路服务器为基准。对于定制化产品，请用户以产品实际情况为准。图片仅供参考，具体请以实际页面为准。

3. 在改变服务器 BIOS 设置前，请记录下相应的初始设置，以便在因修改选项而出现系统工作异常时，可以根据记录的初始设置重新恢复。

4. 通常系统出厂默认设置都是最优化设置。在未理解各参数表示的意义前，请勿试图进行更改。

5. 本文档主要对常用设置作详细说明。使用过程中较少涉及的选项仅作简单说明或未作说明。

2 常用操作

2.1 进入 BIOS Setup 界面

功能描述

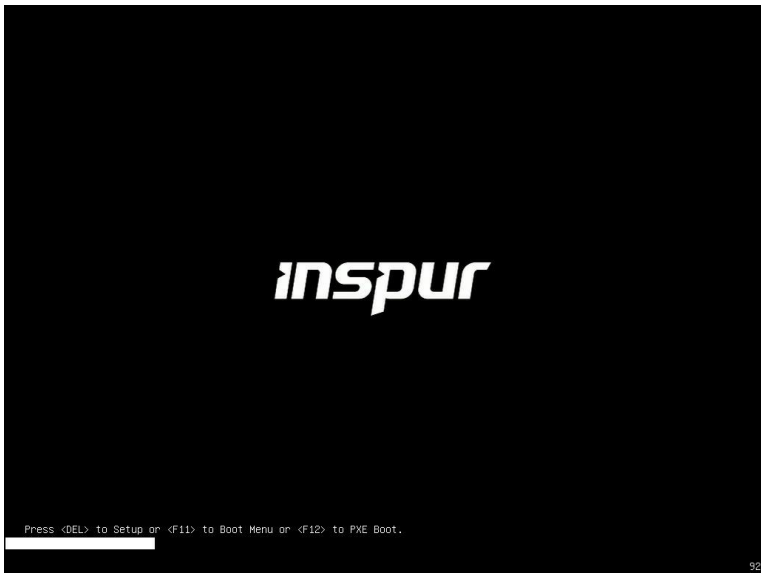
该操作指导用户进入 BIOS Setup 界面。

操作说明

1. 连接好电源并外接键盘、鼠标、显示器或者进入 BMC Web 的远程控制台操作机器。进入 BMC Web 的远程控制台的具体操作步骤请参考 BMC 用户手册。
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，如图 2-1 所示，按下“DEL”，稍后会进入 BIOS Setup 界面。

   图 2-1 BIOS Logo 界面



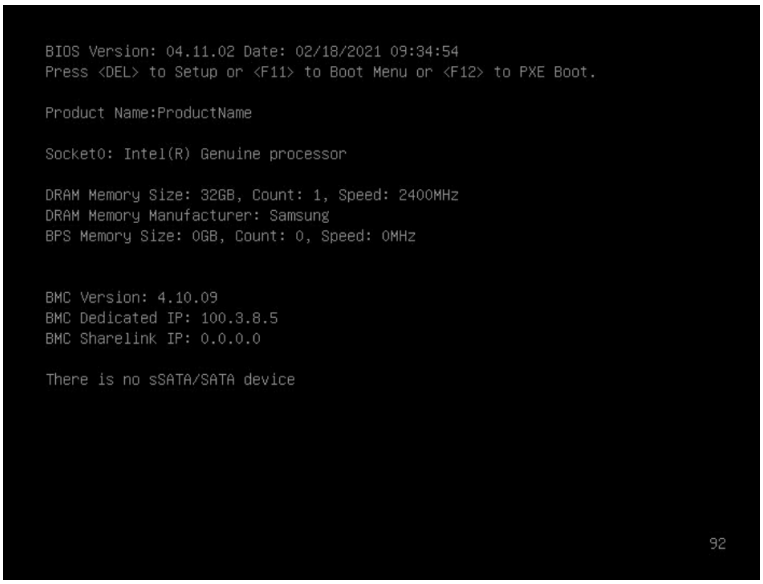
说明

- 按“F11”，可进入启动管理界面。
- 按“F12”，进入网络 PXE 预引导环境。
- 具体 Logo 显示会有差异，请以实际显示为准。
- 如果服务器的 System TF Card 插槽安装了 TF 卡，还会显示“Press <F7> to TF Card Boot.”。

4. 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，如图 2-2 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 2-2 BIOS 启动界面



   BIOS 菜单控制键说明见表 2-1。

   表 2-1 BIOS Setup 界面控制键说明表

按键	功能
<Esc>	退出或是从子菜单返回主菜单
<← >或<→ >	选择菜单
< ↑ >或< ↓ >	移动光标到上或下
<Home>或<End>	移动光标到屏幕顶部或是底部
<+>或<->	当前项的前一个或后一个数值
<F1>	快捷键的帮助信息

按键	功能
<F2>	恢复上次设置值
<F9>	恢复默认设置
<F10>	保存并退出
<Enter>	执行命令或选择子菜单
<K>或<M>	向上/下滚动帮助信息区域

注意

灰色的选项表示在当前状态下不可被选中。带有“▶”符号的项目，有子菜单。

2.2 设置 BIOS 系统语言

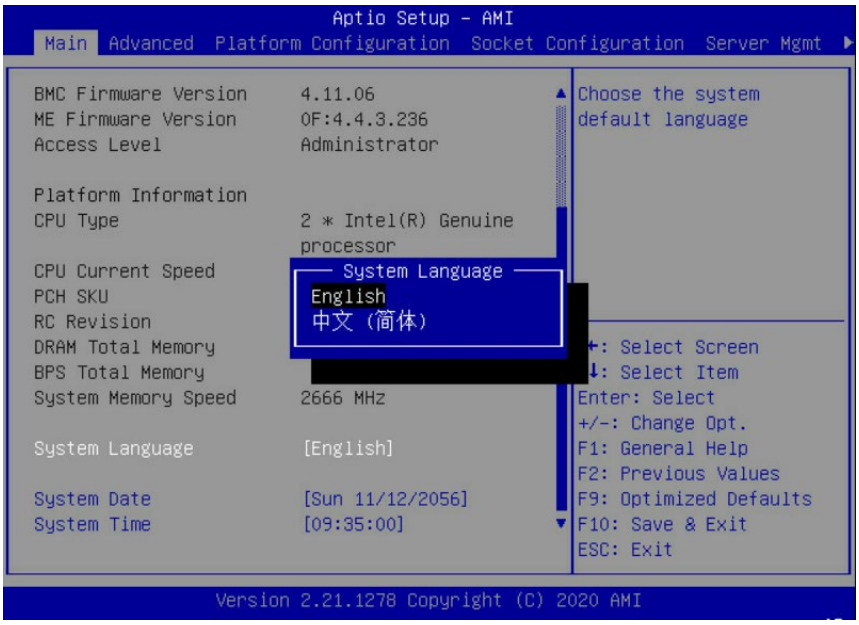
功能描述

该操作指导用户在 BIOS 下进行系统语言的设置。

操作说明

1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Main 界面，如图 2-3 所示。

图 2-3 Main 界面



3. 选择“System Language”，按“Enter”。

4. 根据需要在弹出的菜单选项对话框中选择“English”或“中文（简体）”，按“Enter”。

5. 设置完成后，按“F10”，然后单击“Yes”保存重启生效。

2.3 设置 BIOS 系统日期和时间

功能描述

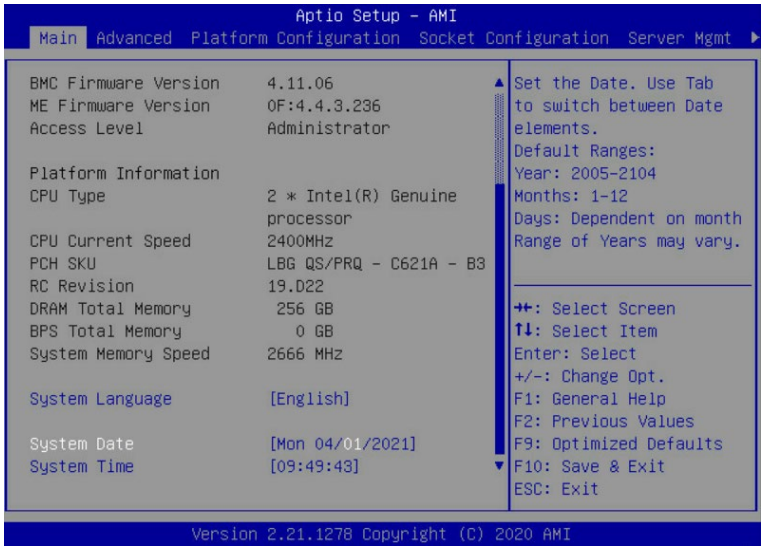
该操作指导用户在 BIOS 下进行系统日期和时间的设置。

操作说明

1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。

2. 选择 Main 界面，如图 2-4 所示。

图 2-4 Main 界面



3. 选择“System Date”或“System Time”，按照格式设置所需的日期/时间。

说明

- 系统日期的格式为“月/日/年”，按“Enter”或’“Tab”键在月、日、年之间切换。
- 系统时间是 24 小时制，格式为“时/分/秒，按“Enter”或’“Tab”键在时、分、秒之间切换。
- 按“+”：数值增加 1。
- 按“-”：数值减少 1。
- 按数字键：直接更改为相应数值。

4. 设置完成后，按“F10”，然后单击“Yes”保存重启生效。

2.4 设置 PCIE 端口

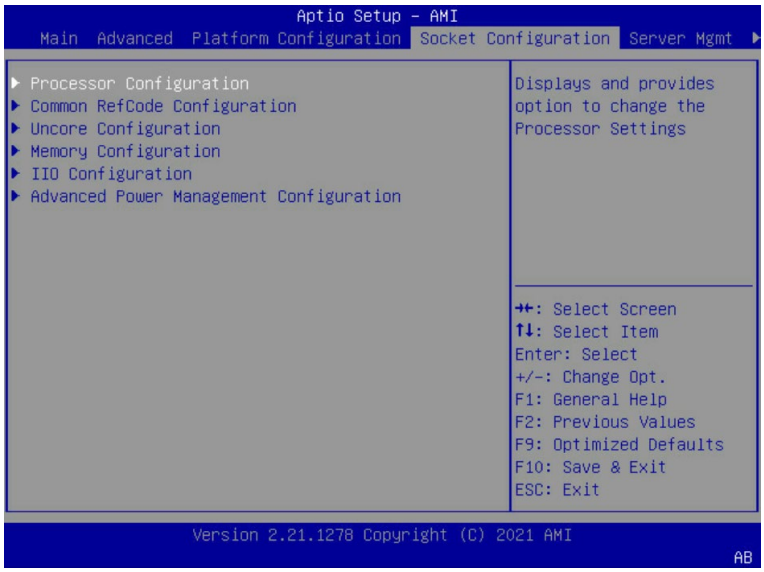
功能描述

该操作指导用户在 BIOS 下进行 PCIE 端口的设置。

操作说明

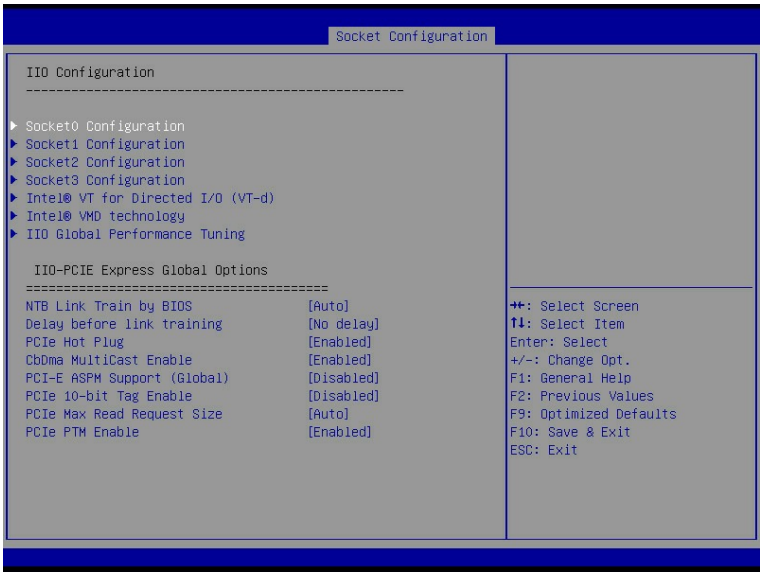
1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Socket Configuration 界面，如图 2-5 所示。

图 2-5 Socket Configuration 界面



3. 选择“IIO Configuration”，按”Enter”进入，如图 2-6 所示。

图 2-6 IIO Configuration 界面

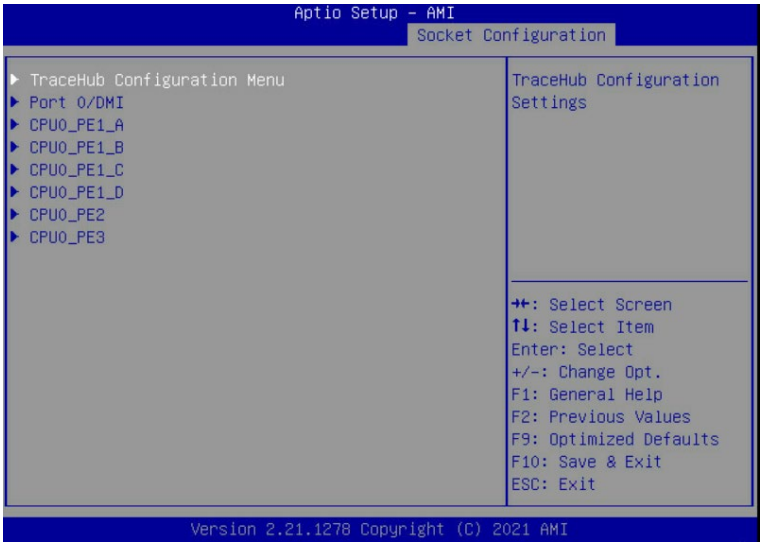


说明

Socket 的个数与 CPU 个数一致，请以实际机型为准。

4. 选择对应的 CPU 配置界面，如“Socket0 Configuration”代表 CPU0 的配置界面，按”Enter”进入，如图 2-7 所示。

图 2-7 Socket0 Configuration 界面

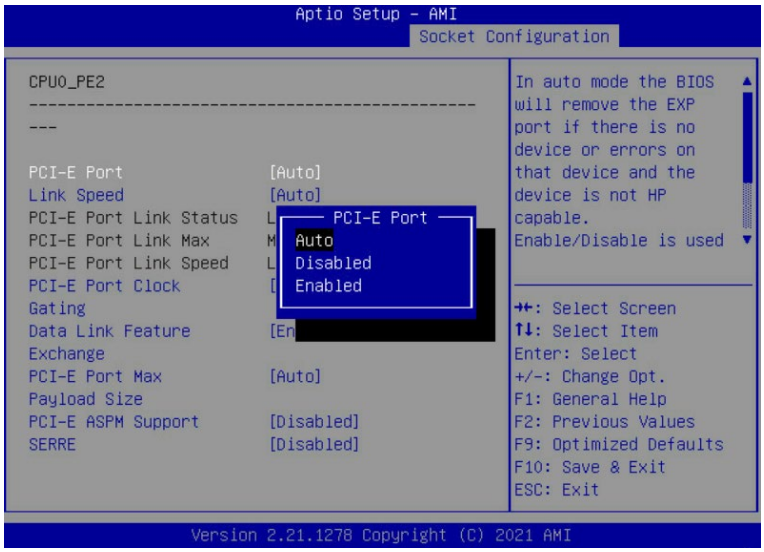


说明

根据服务器带宽配置以及使用端口的不同，该界面显示会有差异，请以实际显示为准。

5. 选择对应的端口，如“CPU0_PE2 “，按”Enter”进入，如图 2-8 所示。

图 2-8 CPU0_PE2 界面



6. 选择”PCI-E Port”，按“Enter” 。
7. 根据需要在在弹出的菜单选项对话框中选择“Auto”、“Disabled”或“Enabled”，按“Enter”。其中，“Auto”/“Enabled”都表示开启 PCIE 端口。
8. 设置完成后，按“F10” ，然后单击“Yes”保存重启生效。

2.5 设置串口重定向功能

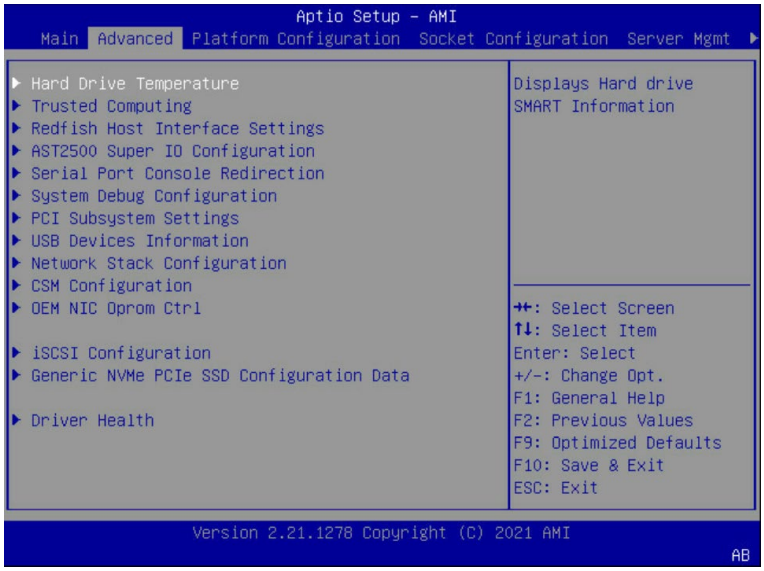
功能描述

该操作指导用户在 BIOS 下进行串口重定向的设置。

操作说明

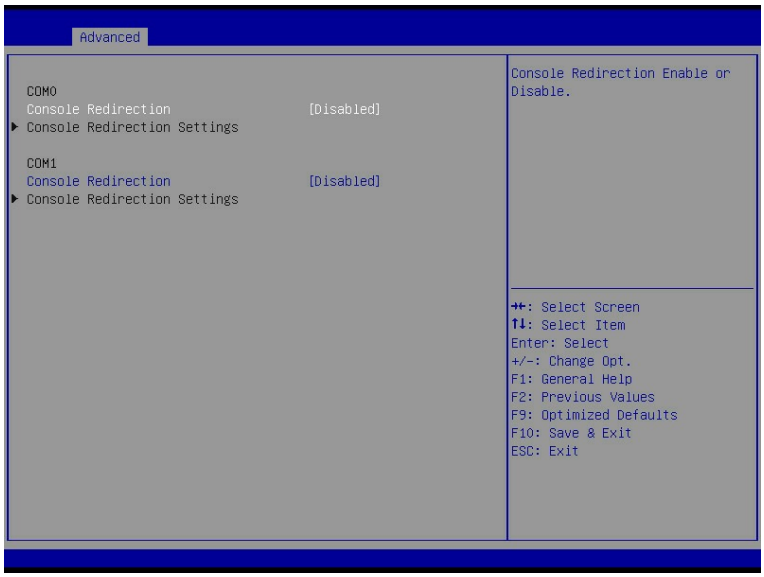
1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Advanced 界面，如图 2-9 所示。

图 2-9 Advanced 界面



3. 选择“Serial Port Console Redirection”，按“Enter”进入，如图 2-10 所示。

图 2-10 Serial Port Console Redirection 界面

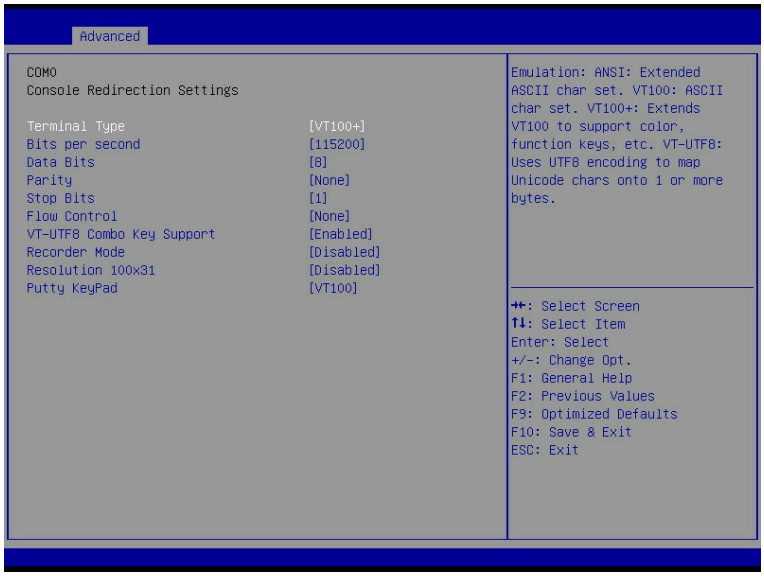


4. 可以设置串口重定向功能是通过“COM0”或“COM1”来实现，默认是通过“COM0”。选择“Console Redirection”，按“Enter”。

5. 根据需要在弹出的菜单选项对话框中选择“Disabled”或“Enabled”，按“Enter”。其中，“Disabled”表示关闭相应 COM 口的串口重定向功能，“Enabled”表示开启相应 COM 口的串口重定向功能。

6. 当“Console Redirection”设置为“Enabled”时，选择“Console Redirection Settings”，按“Enter”，可以设置串口重定向具体参数，如图 2-11 所示。

图 2-11 Console Redirection Settings 界面



说明

- 当“Console Redirection”设置为“Disabled”时，“Console Redirection Settings”选项是灰色的，无法选中。
- 串口重定向具体参数设置请参见 3.2.5 Serial Port Console Redirection。

7. 设置完成后，按“F10”，然后单击“Yes”保存重启生效。

2.6 设置服务器启动模式

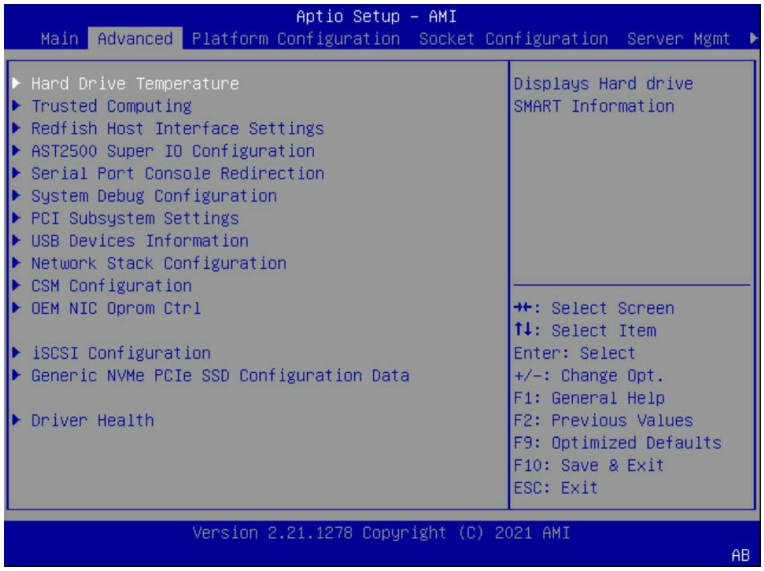
功能描述

该操作指导用户在 BIOS 下进行 UEFI/Legacy 启动模式切换。

操作说明

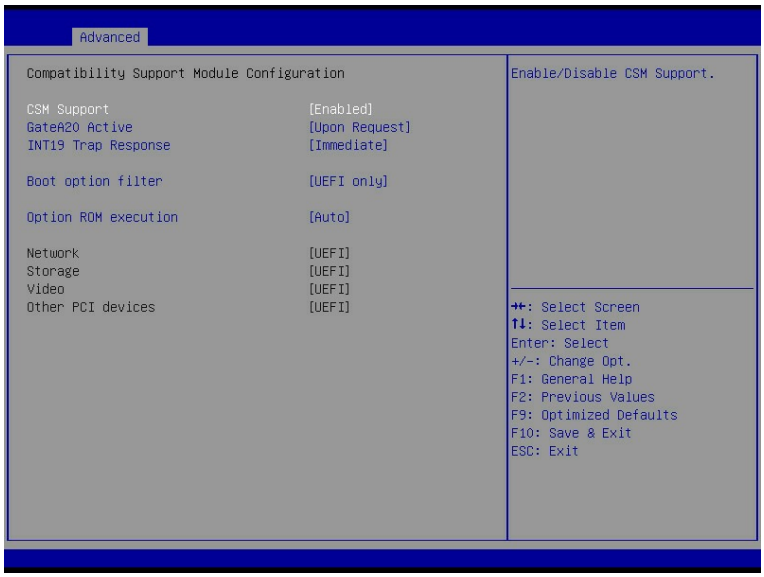
1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Advanced 界面，如图 2-12 所示。

图 2-12 Advanced 界面



3. 选择“CSM Configuration”，按“Enter”进入，如图 2-13 所示。

图 2-13 CSM Configuration 界面



4. 选择“Boot option filter”，按“Enter”。

5. 根据需要在弹出的菜单选项对话框中选择“Legacy only”或“UEFI only”，按“Enter”。

6. 按“F10”，然后单击“Yes”保存重启生效。

说明

- 目前服务器默认设置为 UEFI only，该项可根据客户实际情况进行设置。
- Option ROM execution 设置为 Auto，Network，Storage，Video，Other PCI devices 的 Option ROM 的执行方式会与 Boot option filter 选项联动。
- Option ROM execution 设置为 Manual，可以对 Network，Storage，Video，Other PCI devices 的 Option ROM 的执行方式进行设置。
- 相较于 Legacy 模式，UEFI 模式有很多优势：可以支持从大于 2.2T 的 GPT 格式硬盘引导，支持 IPv6/IPv4 网络 PXE 引导，提供 UEFI Shell 环境等。且由于不再支持 Legacy 的 SATA RAID 模式，当服务器需要配置硬盘组 Raid 环境，在 Legacy 模式下会出现无法成功组 SATA Raid，建议使用 UEFI 模式。

注意

如果 Option ROM execution 设置为 Manual，Network 的 Option ROM 的执行方式须与 Boot option filter 选项设置一致。

2.7 设置服务器启动顺序

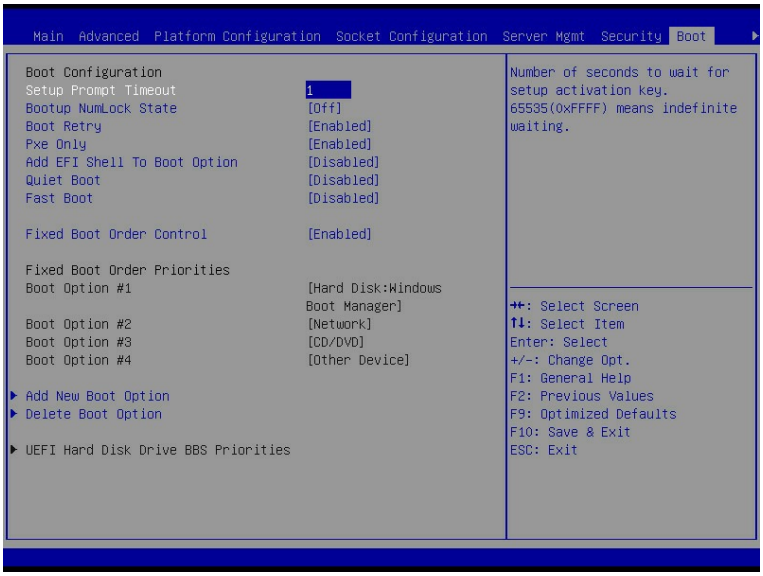
功能描述

该操作指导用户在 BIOS 下进行服务器启动顺序的设置。

操作说明

1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Boot 界面，如图 2-14 所示。

图 2-14 Boot 界面



3. 选择“Fixed Boot Order Control”，按“Enter”，在弹出的菜单选项对话框中选择“Disabled”，按”Enter”。
4. “Boot Option #1/2/3/4”变为可选状态，选择“Boot Option #1”，按“Enter”，根据需要在弹出的菜单选项对话框中选择“Hard Disk”或“Network”或“CD/DVD”或“Other Device”为第一启动项。
5. “Boot Option #2/3/4”与“Boot Option #1”设置相同，不再赘述。
6. 设置完成后，按“F10”，然后单击“Yes”保存重启生效。

说明

- “Fixed Boot Order Control”为“Enabled”时，“Boot Option #1/2/3/4”不可选，默认启动顺序设置为：Hard Disk->Network->CD/DVD->Other Device。
- Fixed Boot Order Control”为“Disabled”时，如果要设置启动顺序为：Network->Hard Disk->CD/DVD-> Other Device，则 Boot Option #1 选择“Network”, Boot Option #2 选择“Hard Disk”, Boot Option #3 选择“CD/DVD”, Boot Option #4 选择“Other Device”。
- 设置启动顺序可以在服务器开机过程中自动进入所设置的第一启动项，而不需要手动按键。
- 服务器启动项的其他选项设置请参见 3.7 Boot。

2.8 恢复 BIOS 选项默认值

功能描述

该操作指导用户恢复 BIOS Setup 选项默认值。

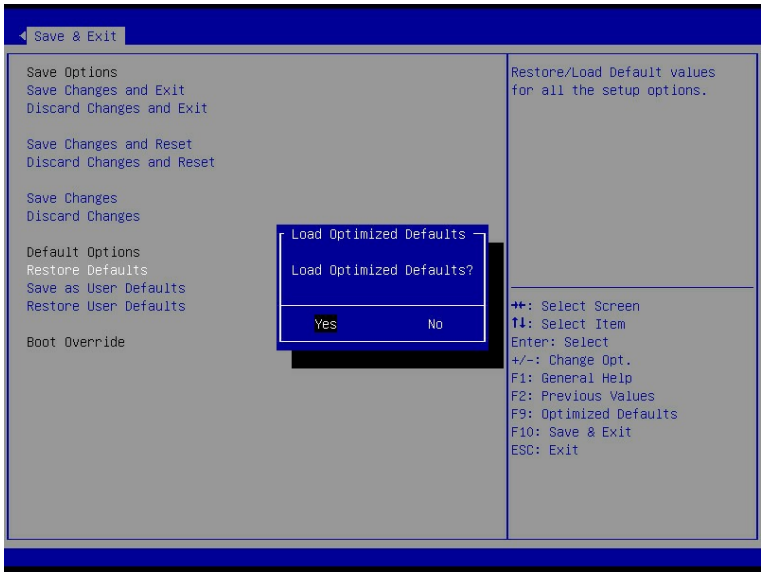
操作说明

常用恢复 BIOS 默认值的方法有四种：Setup 选项、快捷键、Clear CMOS 和 IPMI 命令行。

Setup 选项

1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Save&Exit 界面，显示“Default Options”相关选项，如图 2-15 所示。

图 2-15 Save&Exit 界面



3. 选择“Restore Defaults”，按“Enter“。
4. 点击“Yes“。
5. 按“F10“，然后单击“Yes”保存重启生效。

说明

如果有保存用户默认值，选择“Restore User Defaults”，按“Enter”，单击“Yes”，按“F10” 然后单击“Yes”保存重启后设置生效，恢复为用户默认值。

Setup 快捷键：

1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 按“F9“，单击“Yes”。
3. 按“F10“，然后单击“Yes”保存重启生效，即可恢复默认值。

Clear CMOS

Clear CMOS 可以通过两种方式实现：

1. **操作 1** 将服务器断电，取下 CMOS 电池，等电池放电后，再安装上，上电开机，即可恢复选项的默认值。
2. **操作 2** 将服务器断电，将主板上的 RTC Jumper 跳线接 2、3 引脚或将 BIOS_LOAD_DEFAULT 对应的拨码开关打开，完成 CMOS 放电，即可恢复大部分选项的默认值。操作完成后，将跳帽或拨码开关恢复原始状态。

说明

部分选项无法恢复，如：“Restore AC Power Loss”、“Console Redirection”、“System Debug Level”等选项默认值无法通过 Clear CMOS 恢复。

IPMI 命令行

1. 将服务器上电开机，确保 BMC IP 连接正常。
2. 运行 IPMI Tool 工具，在命令行中输入 ipmitool.exe -H <bmcip> -I lanplus -U <username> -P <password> raw 0x3c 0x31 0x10 0x01，可实现 BIOS Setup 菜单选项值恢复默认，重启生效。

说明

上述命令中的<bmcip>为服务器 BMC IP，<username>和<password>分别为 BMC 的用户名和密码，设置 BMC IP 具体操作步骤请参见 2.13 BMC 网络参数查看与设置。

注意

该操作会将 BIOS 选项恢复为当前 BIOS 版本默认值，如需对 BIOS 参数特殊配置，必须重新进行相应选项的修改，请谨慎操作！

2.9 查看系统配置信息

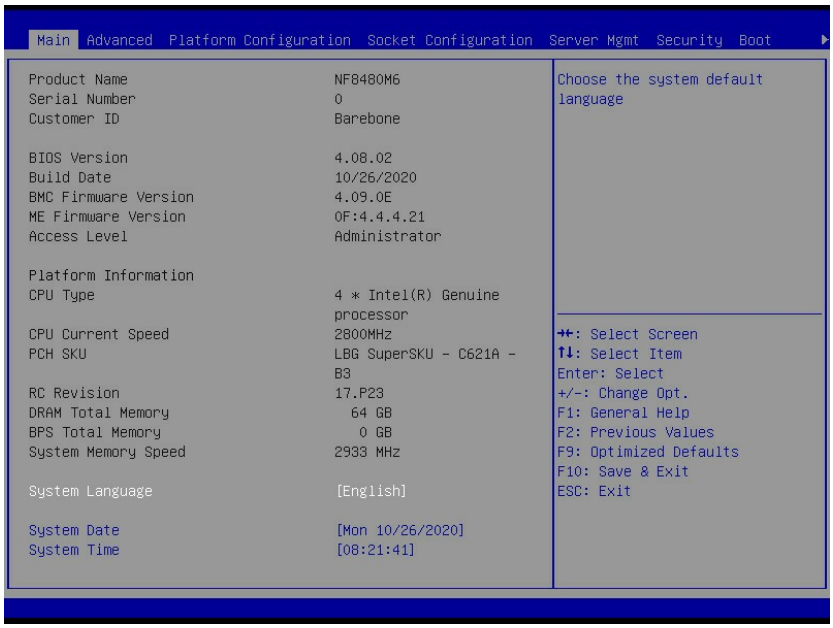
功能描述

该操作指导用户通过 BIOS 查看服务器的各项配置信息。

操作说明

1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. “Main”界面将显示当前系统系统信息概要，显示 BIOS、BMC 和 ME 的版本信息，以及 CPU、PCH、RC 版本、内存等概要信息，如图 2-16 所示。

图 2-16 Main 界面



2.10 查看 CPU 详细信息

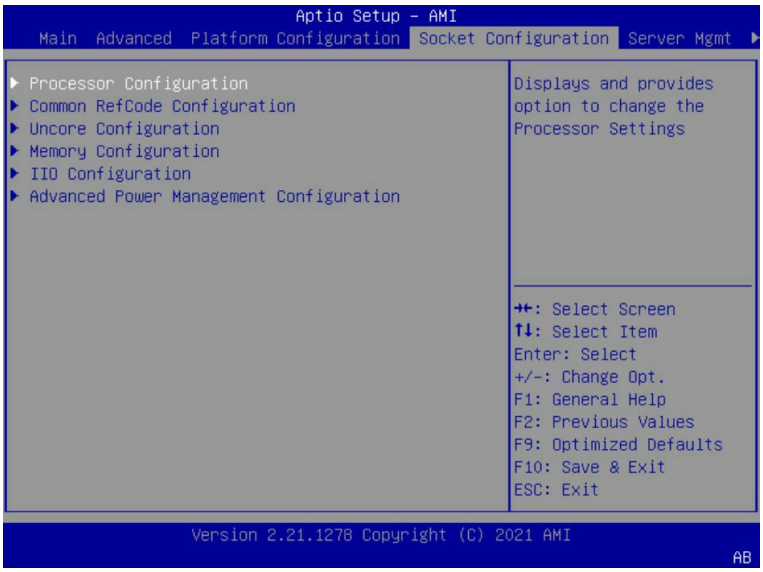
功能描述

该操作指导用户通过 BIOS 查看服务器配置的 CPU 详细信息。

操作说明

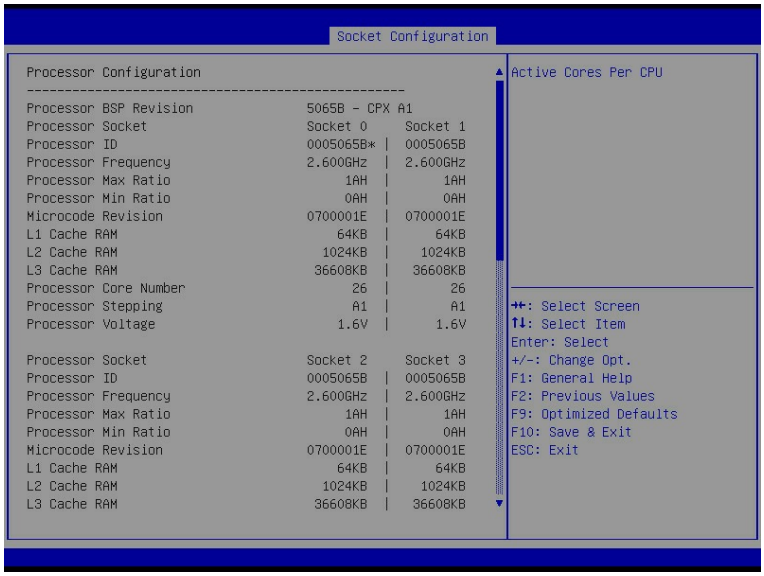
1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Socket Configuration 界面，如图 2-17 所示。

   图 2-17 Socket Configuration 界面



3. 选择“Processor Configuration”，按“Enter“。如图 2-18 所示，查看 CPU 详细信息。

图 2-18 Processor Configuration 界面



2.11 查看内存信息

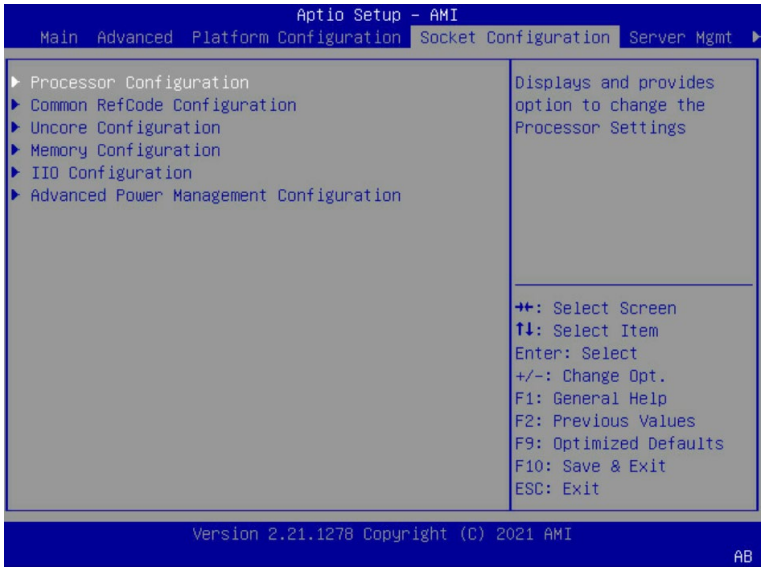
功能描述

该操作指导用户通过 BIOS 查看服务器配置的内存详细信息。

操作说明

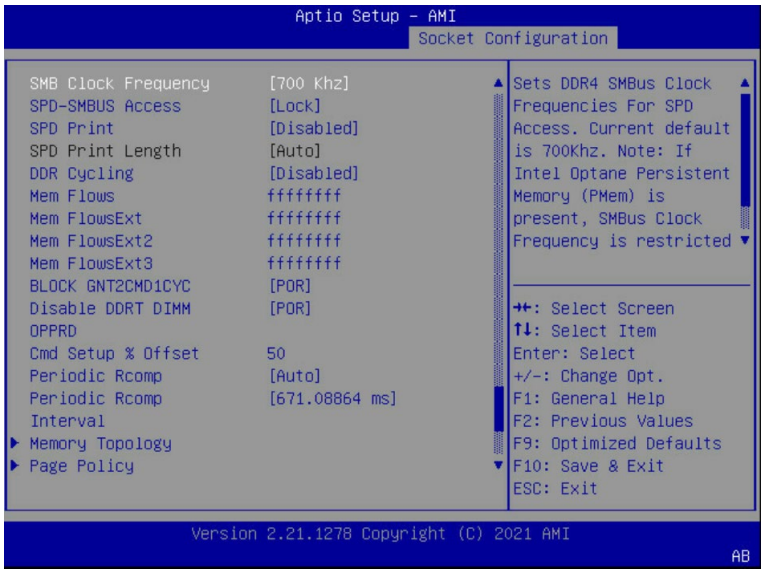
1. 进入 BIOS Setup 界面，具体操作步骤请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Socket Configuration 界面，如图 2-19 所示。

图 2-19 Socket Configuration 界面



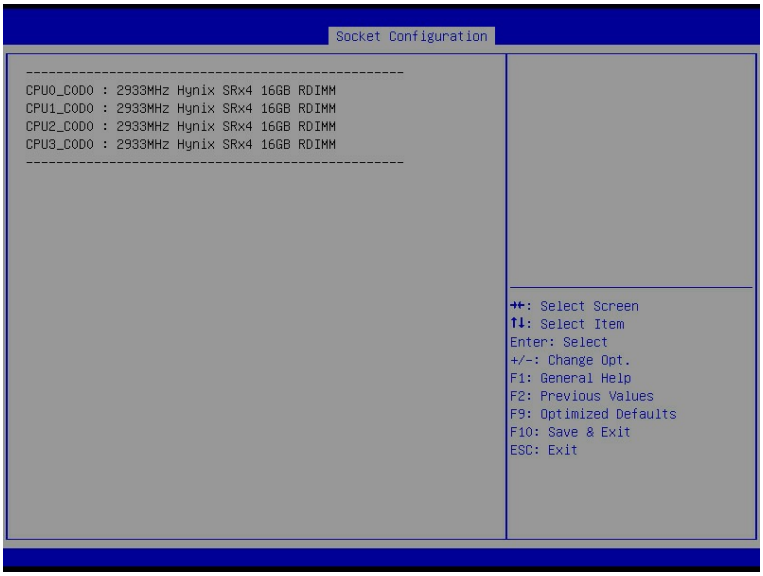
3. 选择“Memory Configuration”，按“Enter”进入，如图 2-20 所示。

图 2-20 Memory Configuration 界面



4. 在界面下方找到“Memory Topology”，按“Enter”进入，如图 2-21 所示，查看所插内存的厂商、速率、容量等详细信息。

图 2-21 Memory Topology 界面



说明

- 根据服务器实际配置的不同，界面显示会有所差异，请以实际显示为准。
- CPUx_CyDz 表示第（x+1）个 CPU 的第（y+1）个 Channel 的第（z+1）根 DIMM。

2.12 查看硬盘信息及 RAID 配置

2.12.1 查看硬盘信息

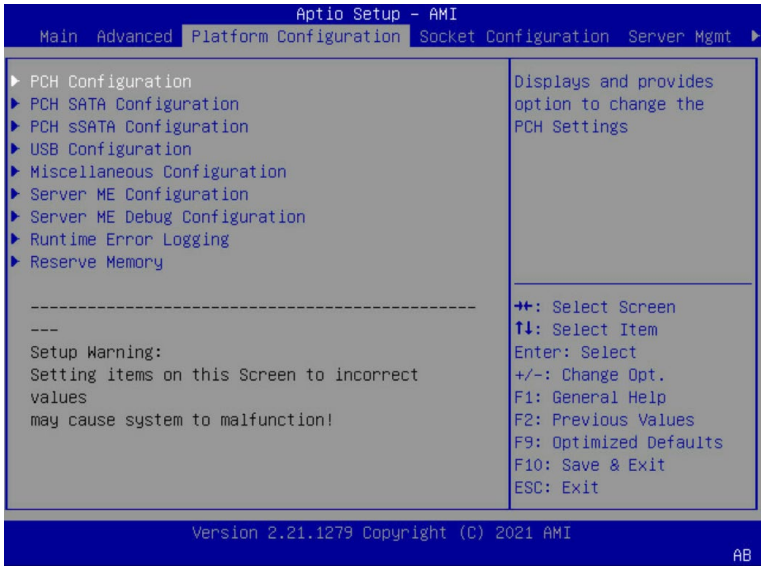
功能描述

该操作指导用户通过 BIOS 查看服务器 PCH 直连硬盘的详细信息。

操作说明

1. 进入 BIOS Setup 界面，具体操作说明请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Platform Configuration 界面，如图 2-22 所示。

图 2-22 Platform Configuration 界面



3. 选择“PCH SATA Configuration”或“PCH sSATA Configuration”，按“Enter”进入，如图 2-23 及图 2-24 所示，查看当前板载 SATA 端口或 sSATA 端口的硬盘详细信息。

图 2-23 PCH SATA Configuration 界面

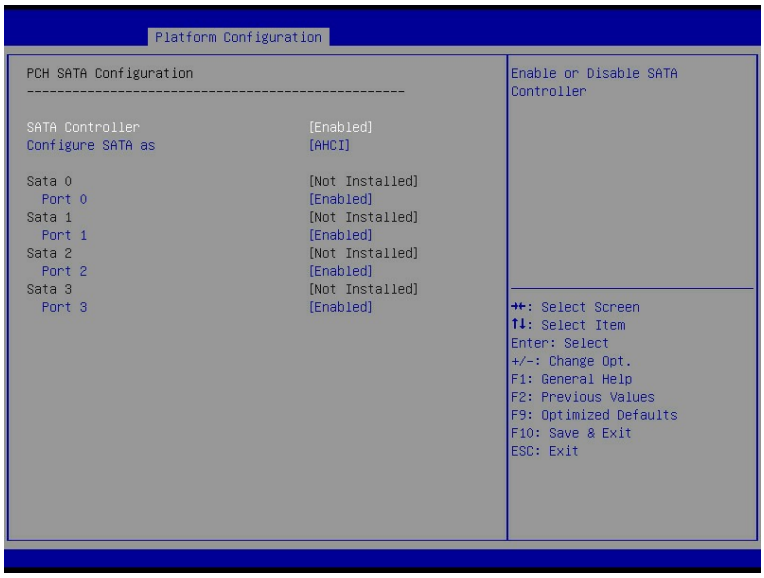
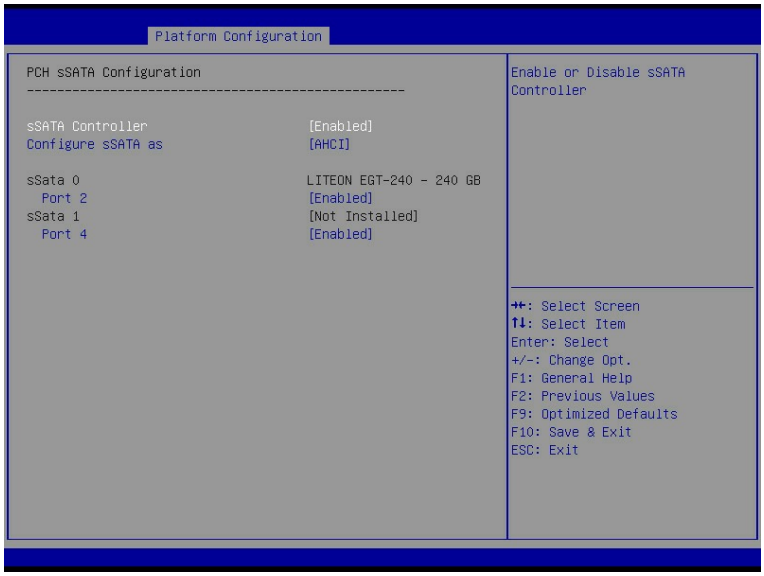


图 2-24 PCH sSATA Configuration 界面



2.12.2 硬盘 RAID 模式配置

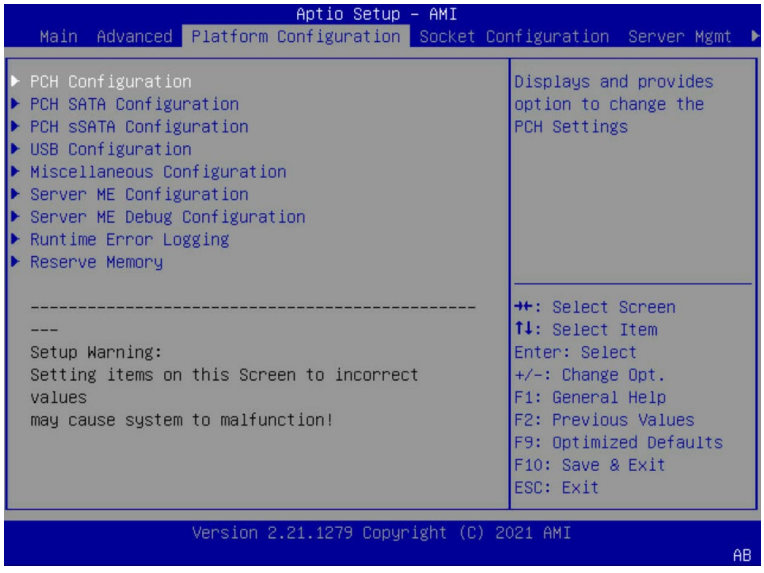
功能描述

该操作指导用户进行硬盘组 RAID 模式配置。

操作说明

1. 进入 BIOS Setup 界面，具体操作说明请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Platform Configuration 界面，如图 2-25 所示。

图 2-25 Platform Configuration 界面



3. 选择“PCH SATA Configuration”或“PCH sSATA Configuration”，按“Enter”进入，如图 2-26 及图 2-27 所示。

图 2-26 PCH SATA Configuration 界面

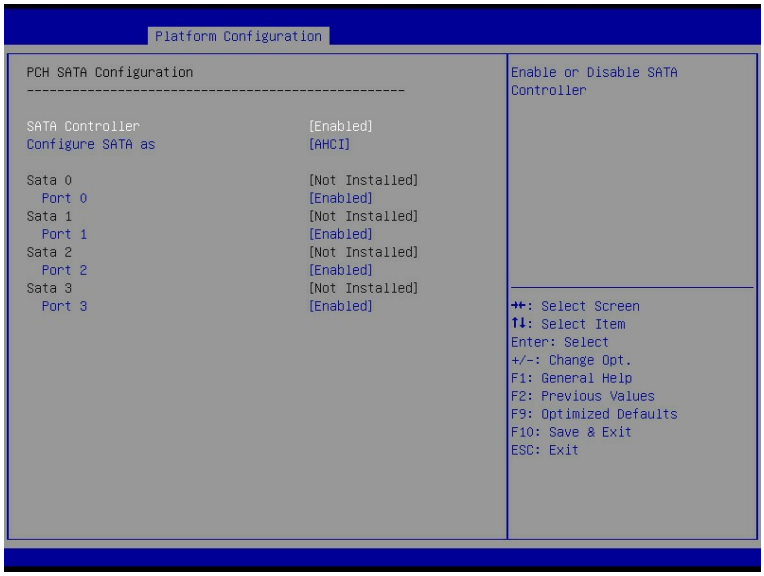
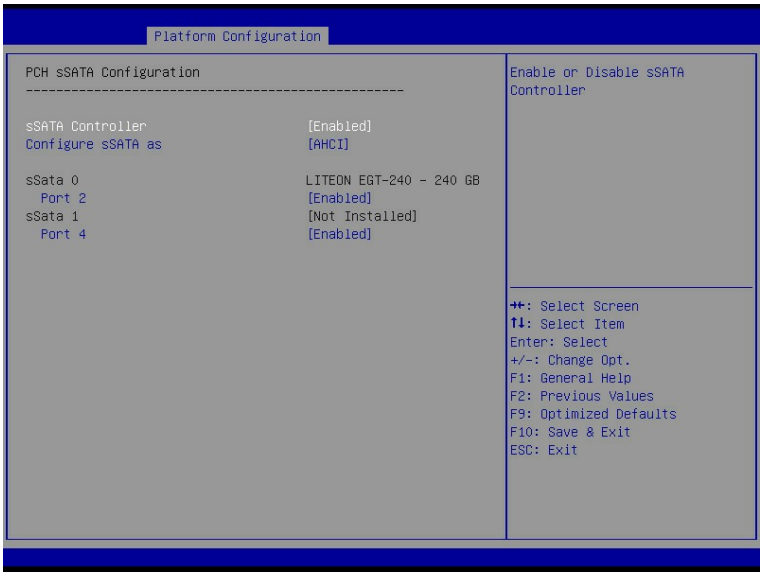


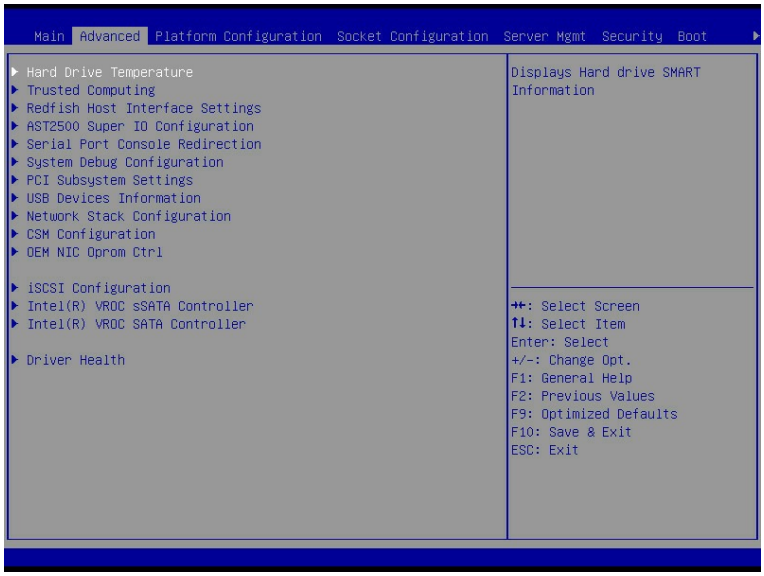
图 2-27 PCH sSATA Configuration 界面



4. 选择“Configure SATA as”或“Configure sSATA as”选项，按“Enter”，在弹出的菜单选项对话框中选择“RAID”，按“F10”，单击“Yes”保存重启生效。

5. 服务器重启进入 BIOS Setup 界面，当选项“Boot option filter”为“UEFI Only”模式，在 Advanced 界面，会出现“Intel(R) VROC SATA Controller”或“Intel(R) VROC sSATA Controller”选项，如图 2-28 所示。

图 2-28 Advanced 界面

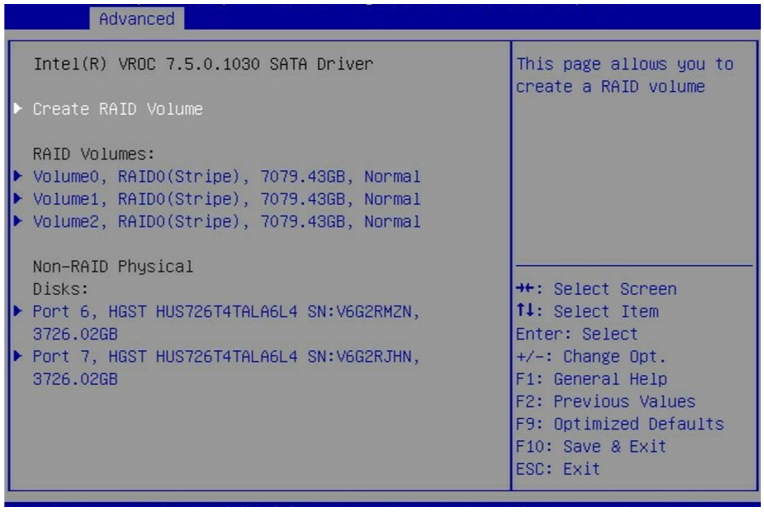


说明

由于不再支持 Legacy 的 SATA RAID 模式,当服务器需要配置硬盘组 Raid 环境,在 Legacy 模式下会出现无法成功组 SATA Raid，请使用 UEFI 模式。

6. 选择“Intel(R) VROC SATA Controller”或“Intel(R) VROC sSATA Controller”，按“Enter”进入，显示可执行操作及当前的硬盘信息，如图 2-29 所示。

图 2-29 Intel(R) VROC SATA Controller 界面



创建 RAID 模式

选择“Create RAID Volume”选项，按“Enter”进入，如图 2-30 所示，具体选项操作说明请参考表 2-2。

图 2-30 Create RAID Volume 界面

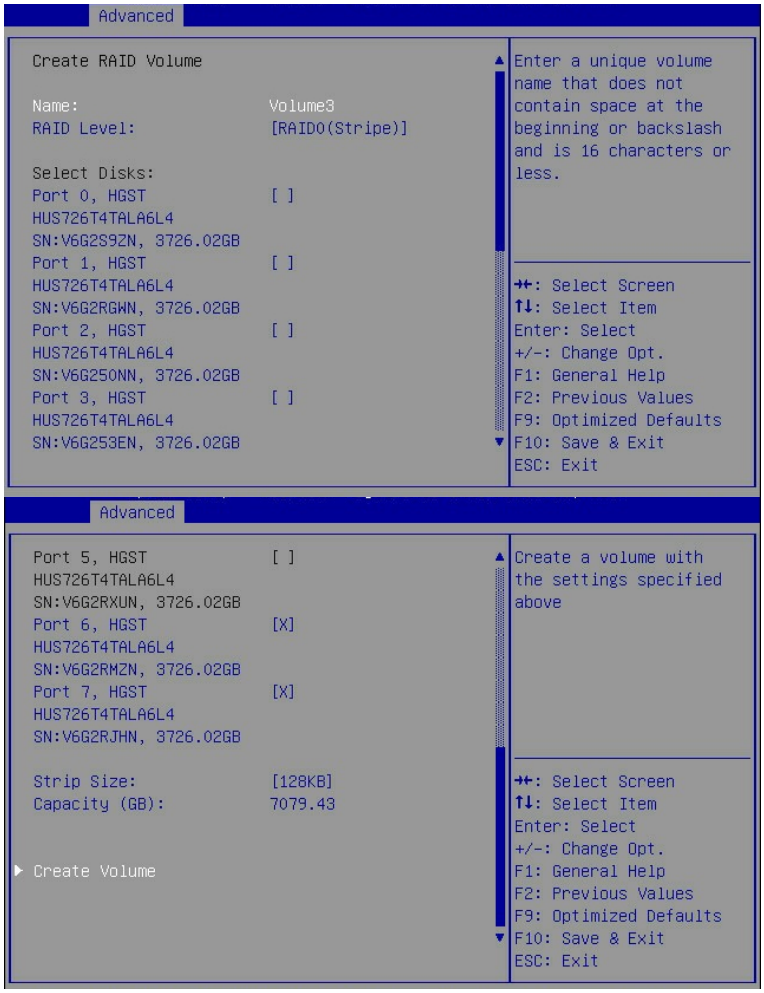


表 2-2 Create RAID 选项操作说明表

界面参数	功能说明
Name	请输入少于16个不包含特殊字符的名称。
RAID Level	请选择RAID模式级别，如果目前还没有创建任何RAID，在此有RAID0(Stripe)、RAID1(Mirror)，RAID5(Parity)和RAID10(RAID0+1)四个级别可供选择，请根据实际需求选择级别。其中，RAID5(Parity)和RAID10(RAID0+1)只有在服务器上插入RAID Key时才会显示。 • RAID0：RAID0

界面参数	功能说明
	• RAID1：RAID1 • RAID5：RAID5，至少需要3块以上硬盘 • RAID10：RAID0+1，需要4块硬盘
Select Disks	选择要组建RAID模式的硬盘，按“Enter”键，选择“X”，然后按“Enter”键回到RAID模式创建界面，表示选中该硬盘。
Strip Size	请选择RAID的带大小，只有RAID0和RAID5模式才能选择该项。
Capacity(GB)	输入需要设置的RAID容量大小，在右侧Help信息中可以看到最大容量信息。
Create Volume	设置完以上参数信息后，点击该选项创建RAID。

删除 RAID 模式

选择已创建的 RAID Volume 选项,按“Enter”进入,如图 2-31、图 2-32 所示。选择“Delete”,会进入 Delete 提示菜单,提示是否要删除 RAID 模式,如图 2-33 所示。如果删除,选择“Yes”,按“Enter”，如果不删除，选择“No”，按“Enter”。

图 2-31 RAID Volume 界面

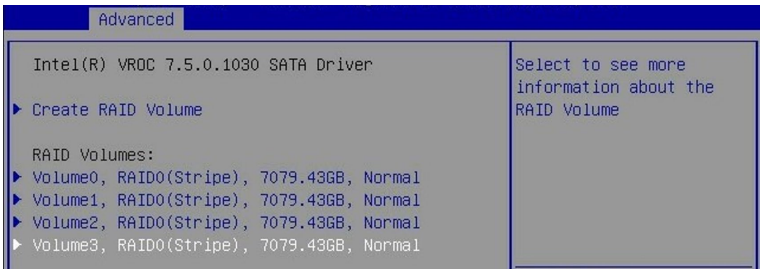


图 2-32 RAID Volume Info 界面

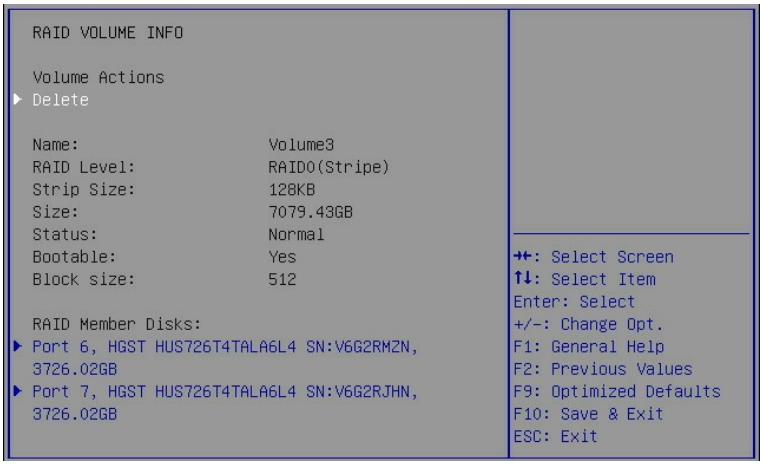
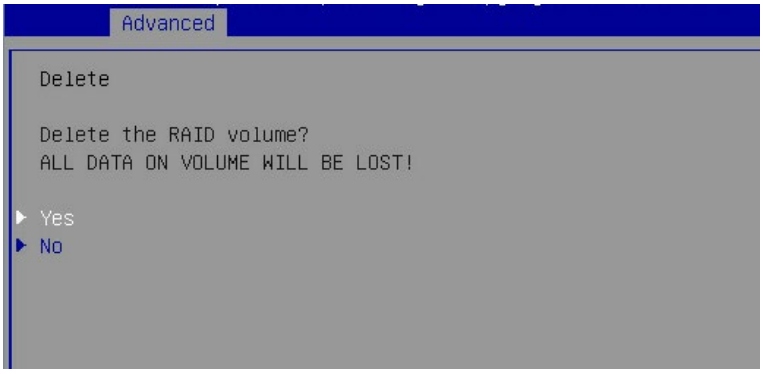


图 2-33 RAID Volume Delete 界面



注意

该操作导致 RAID 模式被删除，如果使用 RAID 功能需要重新进行设置，请谨慎操作！

2.13 BMC 网络参数查看与设置

2.13.1 查看 BMC 网络参数

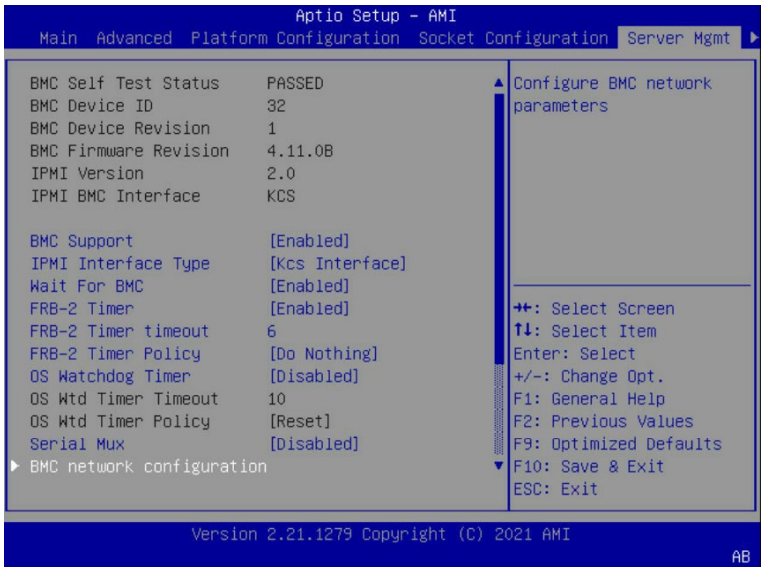
功能描述

该操作指导用户通过 BIOS 查看服务器 BMC 管理网口的 IP 信息。

操作说明

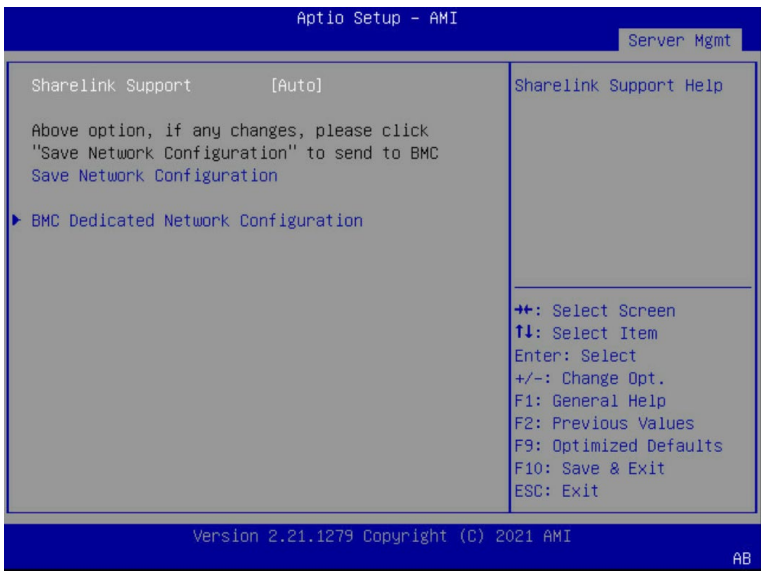
1. 进入 BIOS Setup 界面，具体操作说明请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Server Mgmt 界面，如图 2-34 所示。

图 2-34 Server Mgmt 界面



3. 选择“BMC network configuration”，按“Enter”进入，如图 2-35 所示。

图 2-35 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 2-36、图 2-37 所示。

说明

- BMC 的网络有 Dedicated Network 和 Sharelink Network。
- Dedicated Network，专有网络，该网络模式只能通过服务器 Mgmt 网口访问 BMC。
- Sharelink Network，共享网络，该网络模式可以通过 PCIE 网卡的网口访问 BMC，且只有在服务器上存在 PCIE 网卡的情况下才会显示。

图 2-36 BMC Dedicated Network Configuration 界面

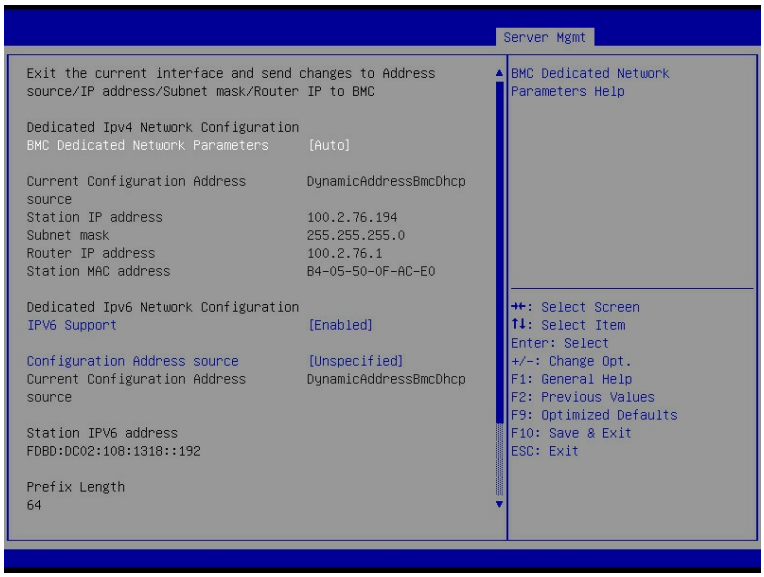
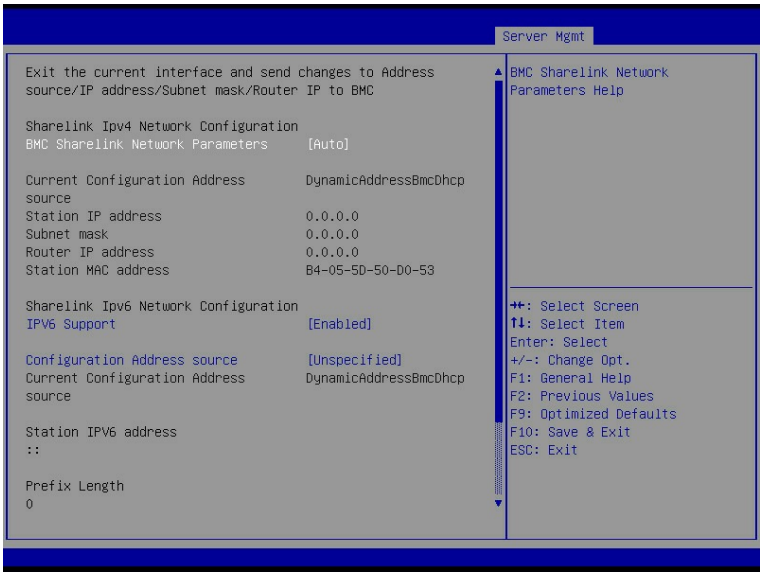


图 2-37 BMC Sharelink Network Configuration 界面



2.13.2 BMC 网络设置

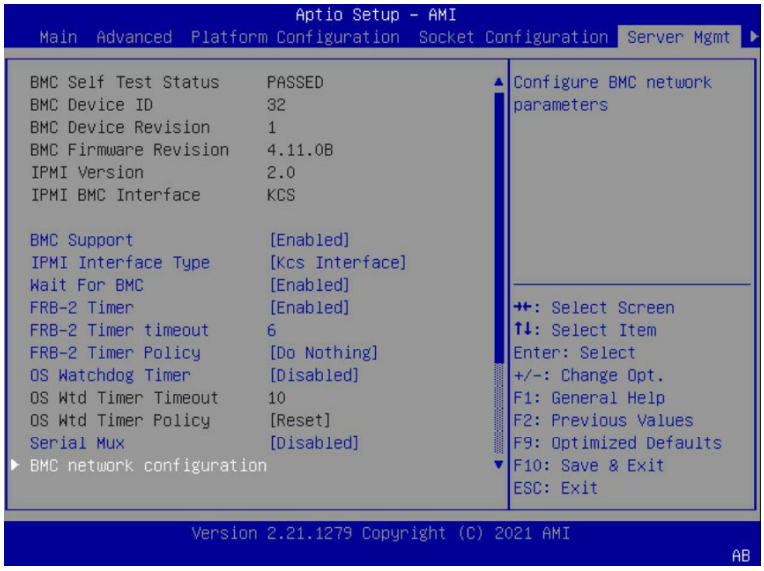
功能描述

该操作指导用户通过 BIOS 设置服务器 BMC 的网络信息,包括配置 BMC IP 地址的获取方式,配置其 IP 地址、子网掩码以及网关。

操作说明

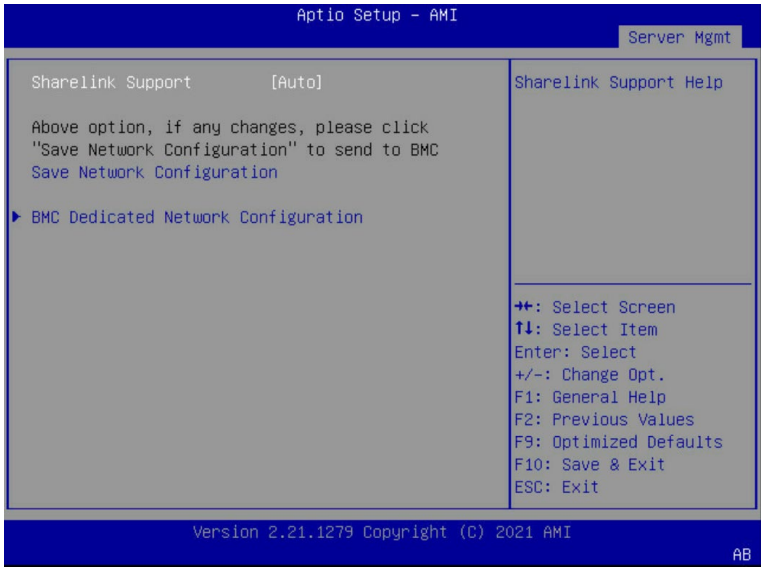
1. 进入 BIOS Setup 界面，具体操作说明请参见 2.1 进入 BIOS Setup 界面。
2. 选择 Server Mgmt 界面，如图 2-38 所示。

图 2-38 Server Mgmt 界面



3. 选择“BMC network configuration”，按“Enter”进入，如图 2-39 所示。

图 2-39 BMC network configuration 界面



说明

以 Dedicated Network 配置来介绍网络参数的设置，Sharelink Network 配置同理。

4. 选择“BMC Dedicated Network Configuration”，按“Enter”进入，如图 2-40 所示。以 BMC Dedicated 网络配置为例，介绍 BMC 网络参数的设置，具体参数设置如表 2-3 所示。

图 2-40 BMC Dedicated Network Configuration 界面

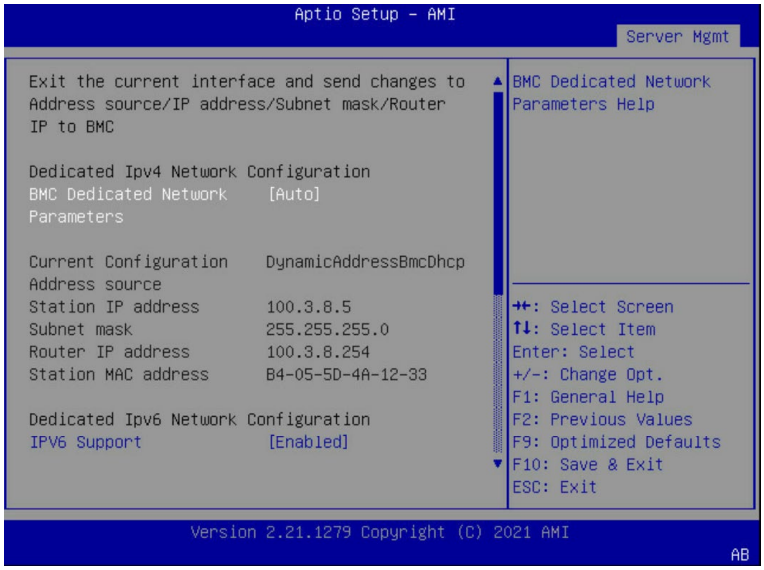


表 2-3 BMC network configuration 界面说明表

界面参数	功能说明	默认值
BMC Dedicated Network Parameters	获取BMC专口网络参数的方式设置，该选项可选值有： Auto：自动获取当前BMC网络设置参数 Manual：手动设置BMC网络设置参数	Auto
Address source	配置BMC网络状态，该选项可选值有： Unspecified：不修改BMC网络参数 Static：设置静态参数 DynamicBmcDhcp：动态获取BMC网络参数	Unspecified
Current Configuration Address source	当前BMC配置地址状态	----
Station IP address	端口的IP地址	----
Subnet mask	子网掩码	----
Router IP address	路由IP地址	----
CMC0 IP address (多节点服务器才会有此项)	从BMC获取的CMC IP0地址	----

界面参数	功能说明	默认值
CMC1 IP address (多节点服务器才会有此项)	从BMC获取的CMC IP1地址	----
Station MAC address	端口的MAC地址	----
IPV6 Support	是否支持IPV6，选项参数有： Enabled：启用 Disabled：禁用	Enabled
Configuration Address Source	配置BMC网络状态，选项参数有： Unspecified：将不修改BMC网络参数 Static：静态 DynamicBmcDhcp：动态获取BMC网络参数 参数设置成功后立即生效。	Unspecified
Current Configuration Address source	当前BMC配置地址状态	----
Station IPv6 address	端口的IPv6地址	----
Prefix Length	前缀长度	----
IPV6 Router1 IP Address	IPV6路由IP1地址	----
IPV6 address status	IPV6地址状态	----
IPV6 DHCP Algorithm	IPV6 DHCP算法	

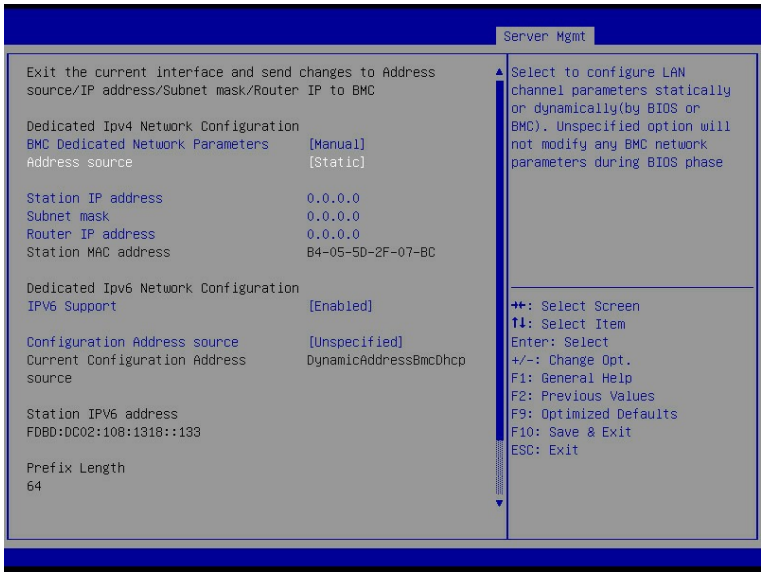
说明

- 当 BMC Dedicated Network Parameters 选项设置为 Auto，即该选项保持默认设置值时，Address source 选项联动隐藏，不需要手动设置网络参数，会自动从当前所连接的网络中获取 IP，请以实际界面显示为准。
- 当 BMC Dedicated Network Parameters 选项设置为 Manual，需要手动设置 IP，请参考以下步骤。

设置 BMC 静态网络参数

将 BMC Dedicated Network Parameters 选项设置为 Manual，此时 Address source 显示并可设置，将 Address source 选项设置为【Static】，此时 Station IP address、Subnet mask、Router IP address 可设置。如图 2-41 所示。

图 2-41 BMC Dedicated Network Configuration 界面



在 Station IP address、Subnet mask、Router IP address 设置完后，按“ESC”键，会提示“Set BMC Network Config”，点击“Yes”向 BMC 发送设置，点击”OK”键退出当前界面，设置成功如图 2-42、图 2-43 所示。

图 2-42 BMC Dedicated Network Configuration 界面

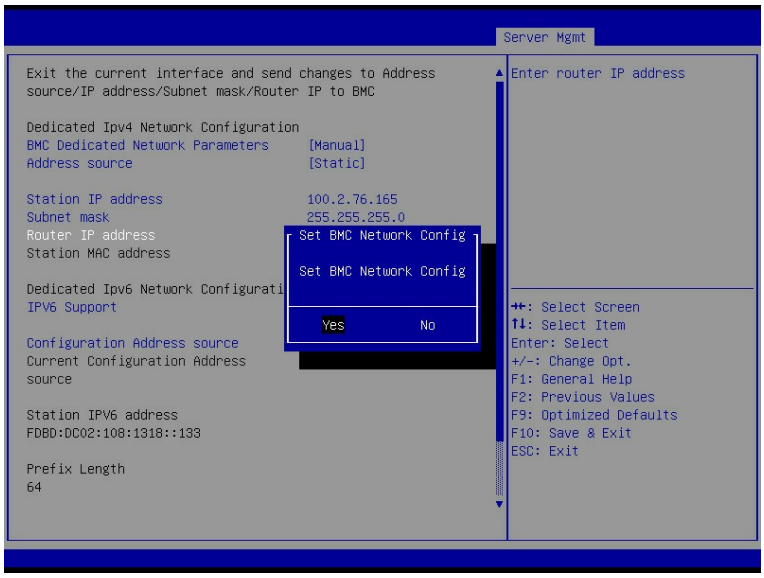
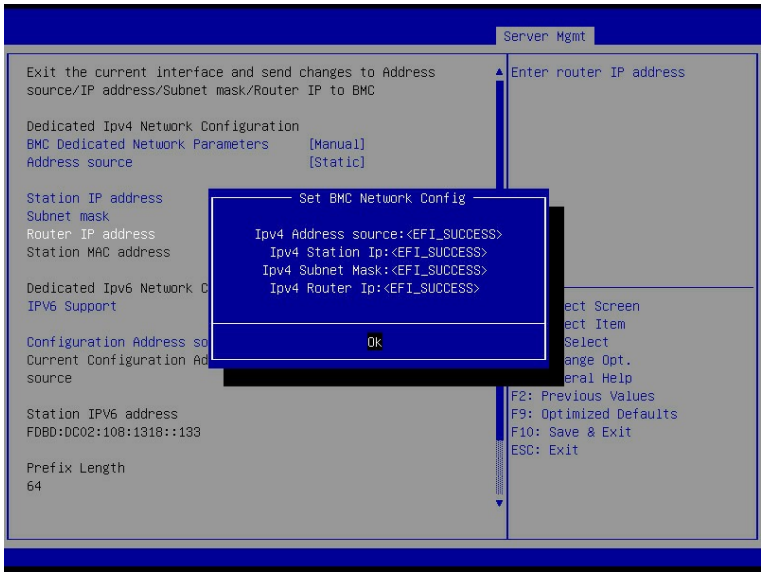


图 2-43 BMC Dedicated Network Configuration 界面



Subnet mask 和 Router IP address 设置与 Station IP address 操作类似，不再赘述，设置完成后 BMC 网络参数已生效，可登陆 BMC Web 界面进行操作。

注意

输入的 IP 无效会提示“Invalid Station IP Entered!!!”，并将 IP address 赋值为 0.0.0.0。该界面的设置不会立即生效，需要退出当前界面才会通知 BMC 修改 IP 设置。

设置 BMC 动态网络参数

将 Address source 选项设置由【Static】设为【DynamiBmcDhcp】，设置完后，按【ESC】退出当前界面，向 BMC 发送改动生效后显示如图 2-44、图 2-45 所示。

图 2-44 BMC Dedicated Network Configuration 界面

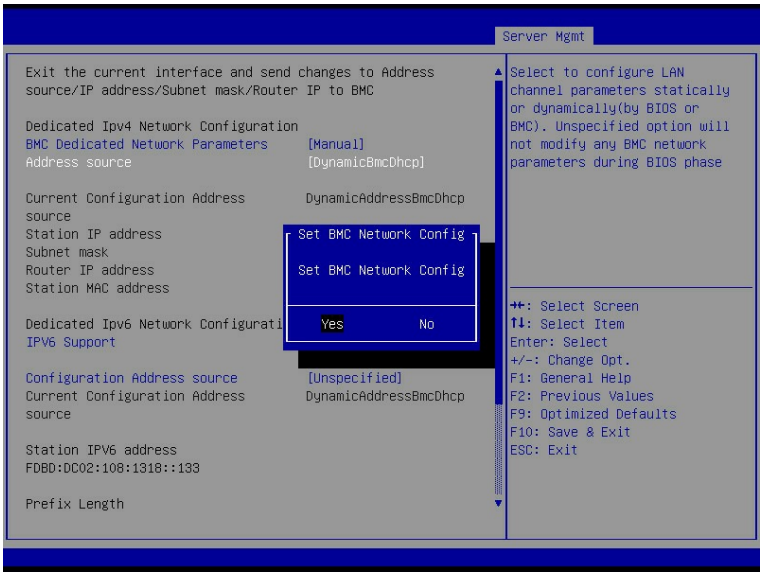
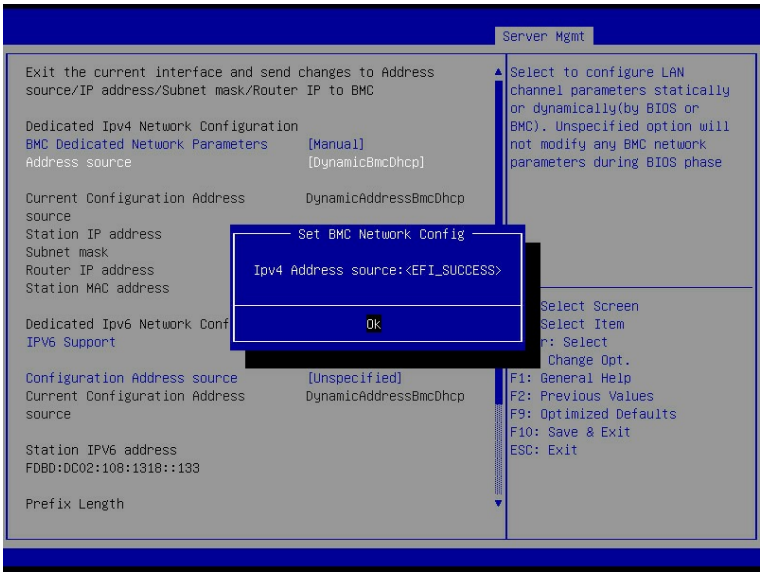


图 2-45 BMC Dedicated Network Configuration 界面



BMC IPv6 网络参数设置类似，不再赘述。

注意

配置 BMC Dedicated 网络时，请保证网线插在服务器 Mgmt 网口。

3 BIOS 参数说明

3.1 Main

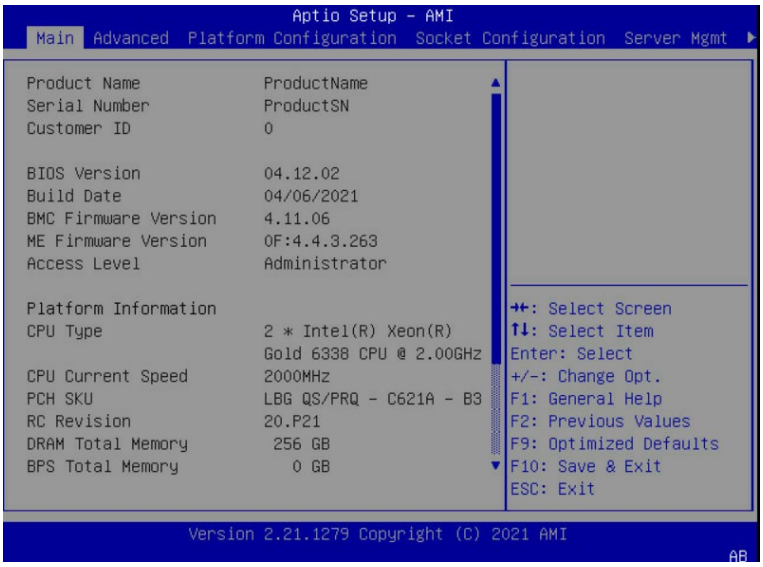
功能描述

Main 界面包含 BIOS 系统的基本信息，BIOS、BMC 和 ME 的版本信息，CPU 型号信息，内存总容量信息及系统时间等。

界面展示

Main 界面如图 3-1 所示。

图 3-1 Main 界面



参数说明

具体参数说明如表 3-1 所示。

表 3-1 Main 界面说明表

界面参数	功能说明
Product Name	产品名称
Serial Number	系列号
Customer ID	客户ID

界面参数	功能说明
BIOS Version	BIOS版本
Build Date	生成日期
BMC Firmware Version	BMC FW版本
ME Firmware Version	ME FW版本
Access Level	当前访问级别。
CPU Type	显示当前CPU的型号
CPU Current Speed	显示当前CPU的工作频率
PCH SKU	显示当前PCH版本型号
RC Revision	显示当前RC版本信息
DRAM Total Memory	显示当前DRAM内存总容量
BPS Total Memory	显示当前BPS内存总容量
System Memory Speed	显示当前内存频率
System Language	显示和设置系统语言
System Date (Day mm/dd/yyyy)	显示和设置系统日期 用<Tab>或<Enter>键在系统日期和时间的各项切换，直接键入数值修改或者是使用+/-键修改 ● 按“+”键，数值增加1 ● 按“-”键，数值减小1
System Time (hh/mm/ss)	显示和设置系统时间 用<Tab>或<Enter>键在系统日期和时间的各项切换，直接键入数值修改或者是使用+/-键修改 ● 按“+”键，数值增加1 ● 按“-”键，数值减小1

3.2 Advanced

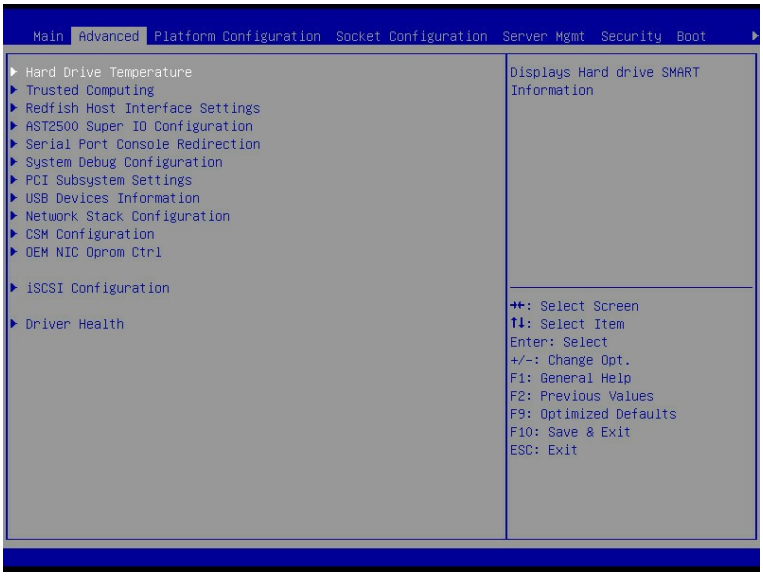
功能描述

Advanced 界面包含 BIOS 系统的参数及相关功能控制。如 ACPI、串口、PCI 子系统、CSM、USB、板载网卡等。

界面展示

Advanced 界面如图 3-2 所示。

图 3-2 Advanced 界面



参数说明

具体参数说明如表 3.2 所示。

表 3-2 Advanced 界面说明表

界面参数	功能说明
Hard Drive Temperature	硬盘温度
Trusted Computing	可信计算配置
Redfish Host Interface Settings	Redfish主机接口设置
AST2500 Super IO Configuration	AST2500 I/O芯片参数配置
Serial Port Console Redirection	串口重定向设置
System Debug Configuration	系统调试配置
PCI Subsystem Settings	PCI子系统设置
USB Devices Information	USB设备信息
Network Stack Configuration	网络堆栈配置
CSM Configuration	CSM配置
Oem NIC Oprom Ctrl	Oem NIC操作控制程序
iSCSI Configuration	iSCSI配置
Intel(R) Ethernet Converged Network Adapter XL710 -XX:XX:XX:XX:XX:XX	Intel 网卡UEFI OPROM配置（此选项会根据插的网卡动态显示）
Driver Health	驱动健康状态

3.2.1 Hard Drive Temperature

功能描述

Hard Drive Temperature 界面是显示硬盘温度的界面，会根据实际的硬盘状态进行显示。

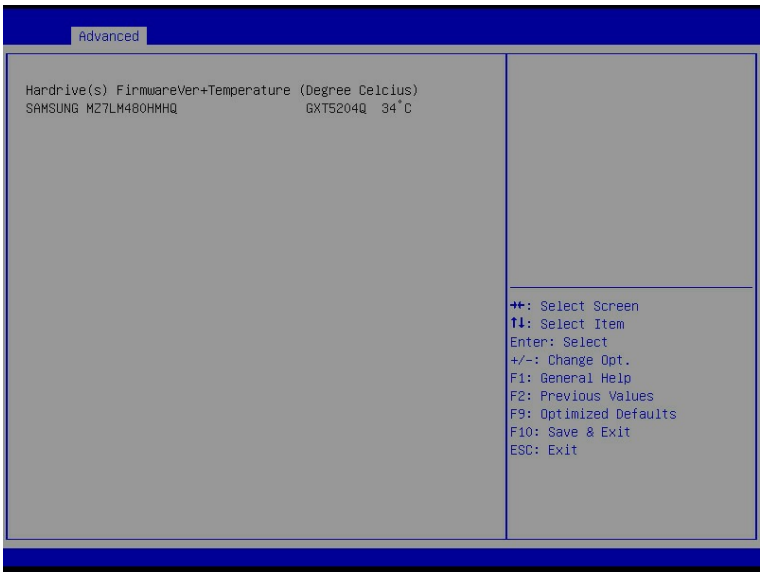
说明

此界面仅支持显示南桥芯片直连的 SATA 硬盘温度。

界面展示

Hard Drive Temperature 界面如图 3-3 所示。

图 3-3 Hard Drive Temperature 界面



3.2.2 Trusted Computing

功能描述

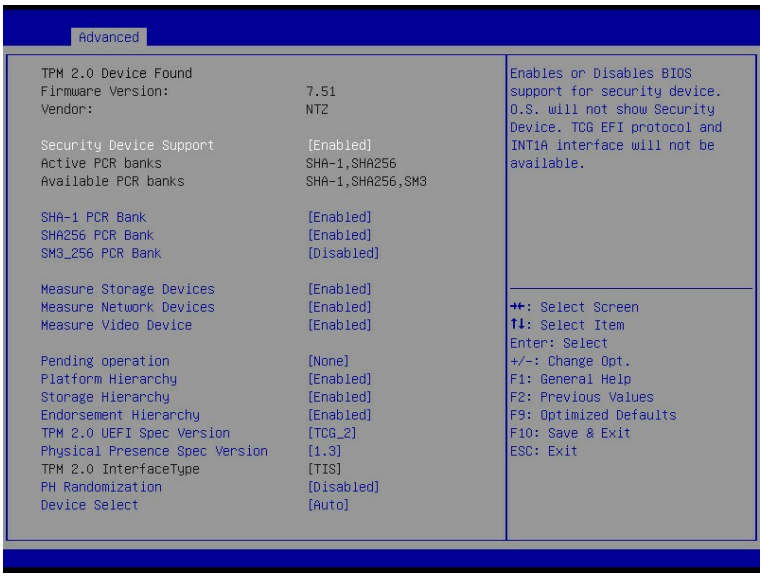
Trusted Computing 是安全设备可信计算的配置界面。可支持 TPM 和 TCM 芯片，以我们在机器上安上了 TPM2.0 芯片为例。

界面展示

Trusted Computing 界面如图 3-4 所示。实际所使用的 TPM/TCM 芯片不同，显示的选项可

能会不同，请以实际为准。

图 3-4 Trusted Computing 界面



参数说明

具体参数说明如表 3-3 所示。

表 3-3 Trusted Computing 界面说明表

界面参数	功能说明	默认值
Security Device Support	安全设备支持开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用 BIOS 支持TPM TCG Version 1.2/2.0。BIOS通过TPM软件绑定来支持TPM模块，当软件绑定验证失败时，BIOS记录错误到SEL中。	Enabled
No Security Device Found	当没有TPM芯片时显示该选项，显示当前安全设备的状态信息，目前没有信息显示，如果需要支持该功能，需要安装TPM芯片	----
SHA-1 PCR Bank	启用或者禁用SHA-1 PCR库，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
SHA256 PCR Bank	启用或者禁用SHA256 PCR库，选项参数同上。	Enabled
SM3_256 PCR Bank	启用或者禁用SM3_256 PCR库，选项参数同上。	Disabled

界面参数	功能说明	默认值
Measure Storage Devices	启用或者禁用度量存储设备的OPROM，注意如果你修改了这一项，请重新配置PCONF文件，选项参数同上。	Enabled
Measure Network Devices	启用或者禁用度量网络设备的OPROM，注意如果你修改了这一项，请重新配置PCONF文件，选项参数同上。	Enabled
Measure Video Devices	启用或者禁用度量视频设备的OPROM，注意如果你修改了这一项，请重新配置PCONF文件，选项参数同上。	Enabled
Pending operation	计划在安全设备上执行的操作，选项参数有： ● None：无 ● TPM Clear：清除TPM **注：** 当安全设备的状态改变后，服务器在开启过程中会进行重启，以使新的设定生效。	None
Platform Hierarchy	启用或者关闭平台层级。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Storage Hierarchy	启用或者关闭存储层级。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Endorsement Hierarchy	启用或者关闭签注层级。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
TPM 2.0 UEFI Spec Version	TPM 2.0 UEFI规范版本，选择TCG2支持的规范版本，选项参数有： ● TCG_1_2：适用于Win8/Win10兼容模式。 ● TCG_2：适用于Win10 后继版本，支持新的TCG2协议和事件格式。	TCG_2
Physical Presence Spec Version	选择告知OS支持的PPI规范版本是1.2还是1.3，需要注意的是一些HCK测试可能不支持1.3版本。选项参数有： ● 1.2 ● 1.3	1.3
TPM 2.0 InterfaceType	为文本信息，显示了TPM 2.0的接口类型	TIS
PH Randomization	启用或者禁用平台层级结构随机化，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：**	Disabled

界面参数	功能说明	默认值
	开发人员测试平台TXT功能时使用，请不要在生产平台中启用	
Device Select	TPM 1.2 仅支持TPM 1.2设备，TPM 2.0 仅支持TPM 2.0设备,自动选项两个设备都支持（自动设置默认支持TPM 2.0设备，如果没有TPM2.0,则主动寻找TPM1.2），选项参数有： ● TPM 1.2 ● TPM 2.0 ● Auto	Auto

3.2.3 Redfish Host Interface Settings

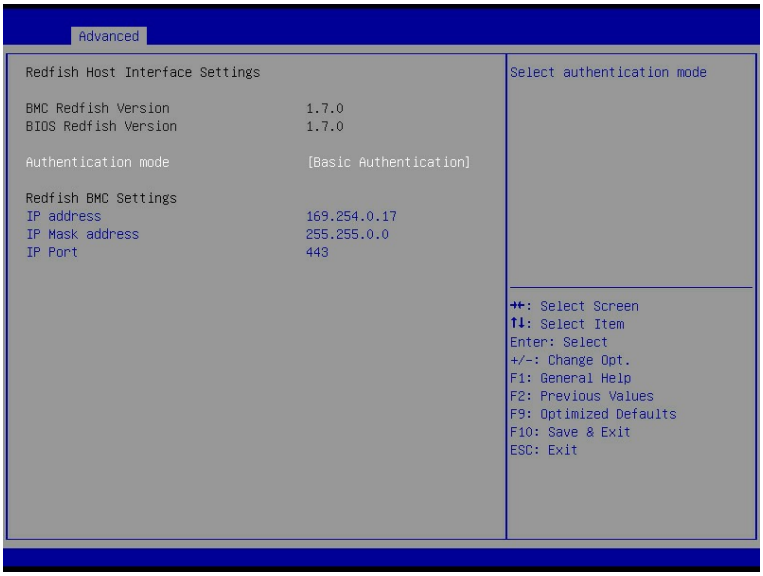
功能描述

Redfish Host Interface Settings 界面是带内 Redfish 通讯的接口设置，即 Host OS 或 BIOS 和 BMC 之间的通信接口。

界面展示

Redfish Host Interface Settings 界面如图 3-5 所示。

图 3-5 Redfish Host Interface Settings 界面



参数说明

具体参数说明如表 3-4 所示。

表 3-4 Redfish Host Interface Settings 界面说明表

界面参数	功能说明	默认值
Authentication mode	授权模式设置，选项参数有： ● Basic Authentication：基本认证 ● Session Authentication：会话认证	Basic Authentication
IP address	Redfish BMC的IP地址设置	----
IP Mask address	Redfish BMC的IP掩码地址设置	----
IP Port	Redfish BMC的IP端口设置	----

注意

Redfish Host Interface Settings 中的 IP 地址是带内 Redfish 通讯所用的 IP，如果客户端(例如管理员)需要远程访问 Redfish Service，需要通过 BMC Network Configuration 页面下的 BMC IP 地址进行访问。

3.2.4 AST2500 Super IO Configuration

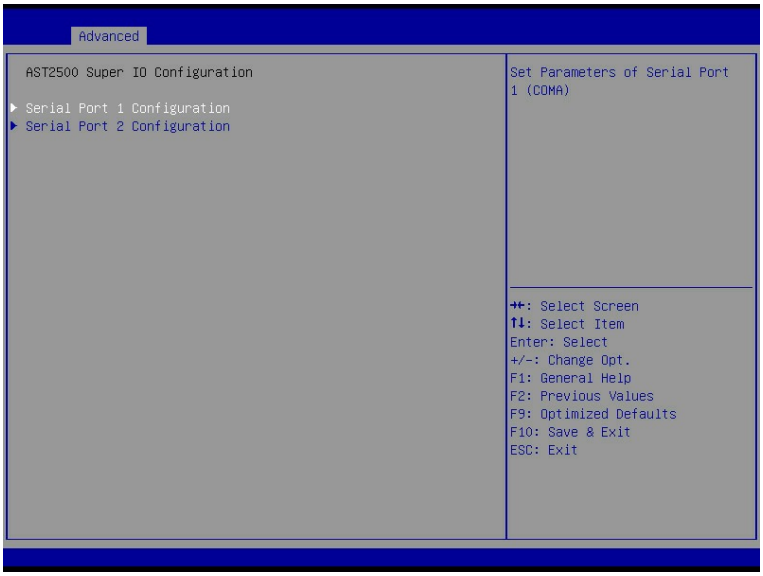
功能描述

AST2500 Super IO Configuration 界面是关于 I/O 芯片相关选项设置。

界面展示

AST2500 Super IO Configuration 界面如图 3-6 所示。

图 3-6 AST2500 Super IO Configuration 界面



参数说明

具体参数说明如表 3-5 所示。

表 3-5 AST2500 Super IO Configuration 界面说明表

界面参数	功能说明
Serial Port 1 Configuration	串口1配置设置，配置页面中提供了该串口的开关控制和资源调整控制功能，资源调整主要是可以手动调整COM PORT使用的IO PORT以及IRQ号。
Serial Port 2 Configuration	串口2配置（虚拟串口）

1. Serial Port 1 Configuration

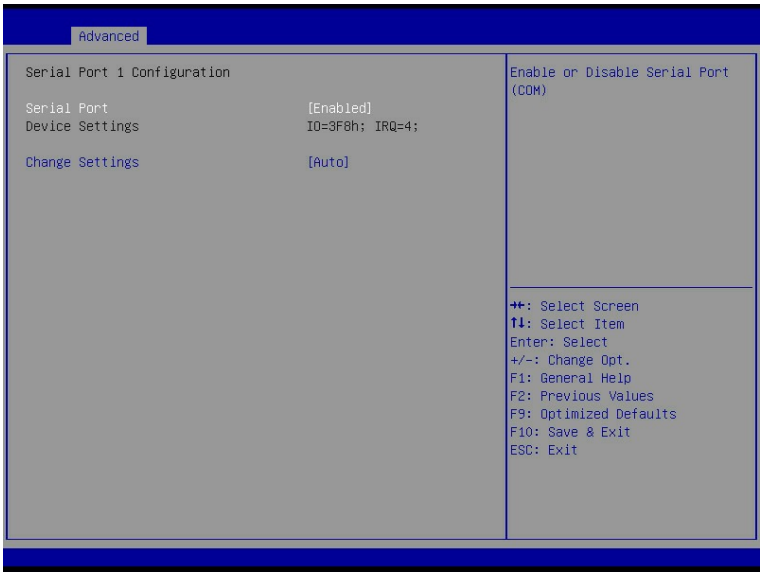
功能描述

Serial Port 1 Configuration 界面是串口 1 相关选项设置。

界面展示

Serial Port 1 Configuration 界面如图 3-7 所示。

图 3-7 Serial Port 1 Configuration 界面



参数说明

具体参数说明如表 3-6 所示。

表 3-6 Serial Port 1 Configuration 界面说明表

界面参数	功能说明	默认值
Serial Port	串口1开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Change Settings	根据需求给串口选择最优设置，选项参数有： ● Auto ● IO=3F8h; IRQ=4; ● IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; ● IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; ● IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; ● IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	Auto

2. Serial Port 2 Configuration

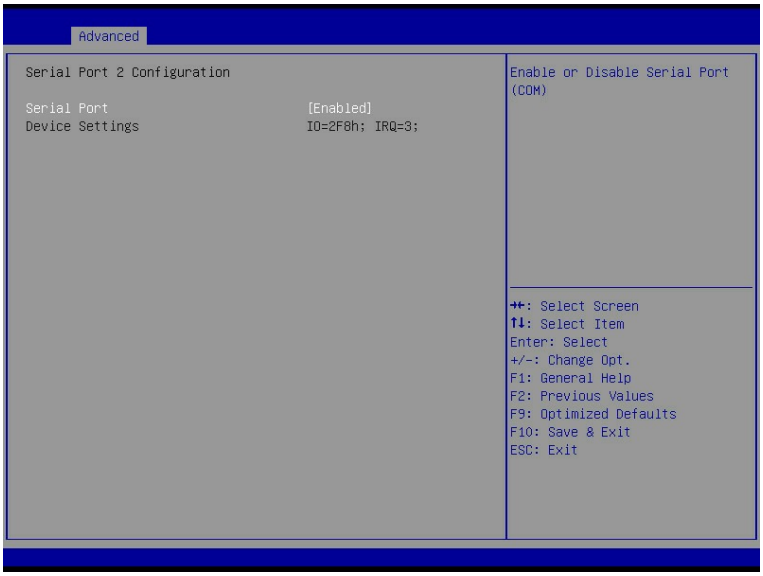
功能描述

Serial Port 2 Configuration 界面是串口 2 相关选项设置。

界面展示

Serial Port 2 Configuration 界面如图 3-8 所示。

图 3-8 Serial Port 1 Configuration 界面



参数说明

具体参数说明如表 3-7 所示。

表 3-7 Serial Port 2 Configuration 界面说明表

界面参数	功能说明	默认值
Serial Port	串口2开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled

3.2.5 Serial Port Console Redirection

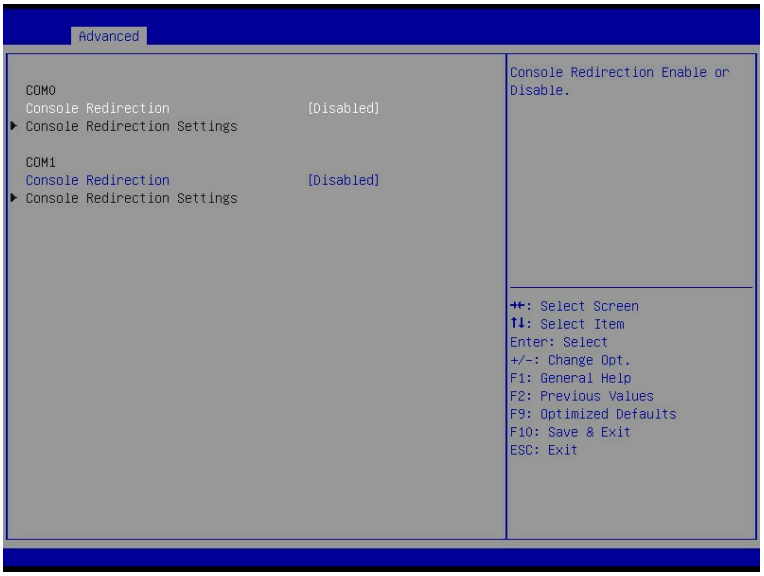
功能描述

Serial Port Console Redirection 界面是串口重定向相关选项设置。

界面展示

Serial Port Console Redirection 界面如图 3-9 所示。

图 3-9 Serial Port Console Redirection 界面



参数说明

具体参数说明如表 3-8 所示。

表 3-8 Serial Port Console Redirection 界面说明表

界面参数	功能说明	默认值
Console Redirection Com0	串口0控制台重定向开关设置，将控制台信息重定向到指定的串口中，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Console Redirection Settings	串口控制台重定向参数设置	----
Console Redirection Com1	串口1控制台重定向开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled

1. Console Redirection Settings

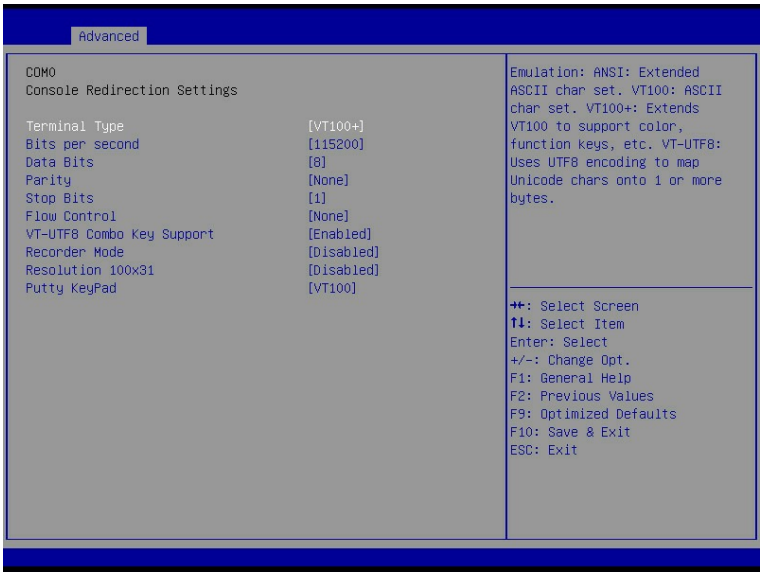
功能描述

当 Console Redirection Com0/Com1 选项设为【Enabled】，Console Redirection Settings 菜单被开启。

界面展示

Serial Port Console Redirection 界面如图 3-10 所示。

图 3-10 Console Redirection Settings 界面



参数说明

具体参数说明如表 3-9 所示。

表 3-9 Console Redirection Settings 界面说明

界面参数	功能说明	默认值
Terminal Type	终端类型设置，通过此选项可选择仿真类型，BIOS仿真类型必须与终端程序中选择的模式相匹配。选项参数有： ● VT100：ASCII字符集 ● VT100+：扩展的VT100，用于支持颜色显示、功能键等。 ● VT-UTF8：使用UTF8编码映射unicode字符到1个或多个字节。 ● ANSI：扩展ASCII字符集。	VT100+
Bits per second	波特率设置，每秒传输比特数配置，传输速率必须和对端口串口匹配，超长或嘈杂的线路可能需要较低的速度。选项参数有： ● 9600 ● 19200 ● 38400 ● 57600	115200

界面参数	功能说明	默认值
	● 115200	
Data Bits	串口数据位宽设置，每字节中实际数据所占的比特数配置。 选项参数有： ● 7 ● 8	8
Parity	奇偶校验设置。选项参数有： ● None：无校验 ● Even：偶校验 ● Odd：奇校验 ● Mark：奇偶校验 ● Space：存储器奇偶校验	None
Stop Bits	停止位设置，停止位（单个数据包的最后一位），标准设置是1位停止位，当与慢速设备通信时可能需要1个以上停止位。 选项参数有： ● 1 ● 2	1
Flow Control	流控制设置，用于防止数据从缓冲区溢出导致数据丢失。选项参数有： ● None：不进行流量控制 ● Hardware RTS/CTS：通过硬件请求发送协议/清除发送协议进行流量控制。开启该功能后，如果使用了不支持硬件流控的串口设备（如USB转串口线缆）或者未连接串口线缆，可能会导致无法加载板载和外接PCIE设备OptionROM、屏幕黑屏光标闪烁等问题。	None
VT-UTF8 Combo Key Support	VT-UTF8组合键支持开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Recorder Mode	记录器模式开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Redirection 100×31	扩展终端分辨率100×31开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Putty KeyPad	Putty的功能键和键盘设置，选项参数有： ● VT100 ● LINUX ● XTERMR6 ● SCO	VT100

界面参数	功能说明	默认值
	● ESCN ● VT400	

3.2.6 System Debug Configuration

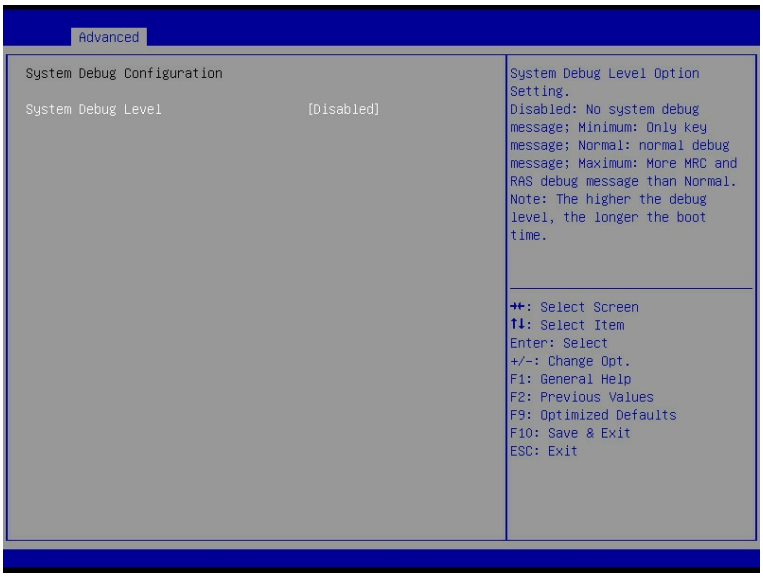
功能描述

System Debug Configuration 界面是系统调试设置。

界面展示

System Debug Configuration 界面如图 3-11 所示。

图 3-11 System Debug Configuration 界面



参数说明

具体参数说明如表 3-10 所示。

表 3-10 System Debug Configuration 界面说明

界面参数	功能说明	默认值
System Debug Level	系统调试设置，服务器系统串口输出BIOS串口日志，选项参数有： ● Disabled：仅输出异常处理接口。 ● Minimum：输出异常处理接口和少量信息，包括CPU	Disabled

界面参数	功能说明	默认值
	Info/Options/IioPCIe/DIMMInfo/Boot/RC和OptionRom Operation Info信息。 ● Normal：输出函数出入口及异常处理接口信息。 ● Maximum：在Normal的基础上，针对RAS/MRC等重点模块，细化到函数每个输出变量的逻辑判断。	

3.2.7 PCI Subsystem Settings

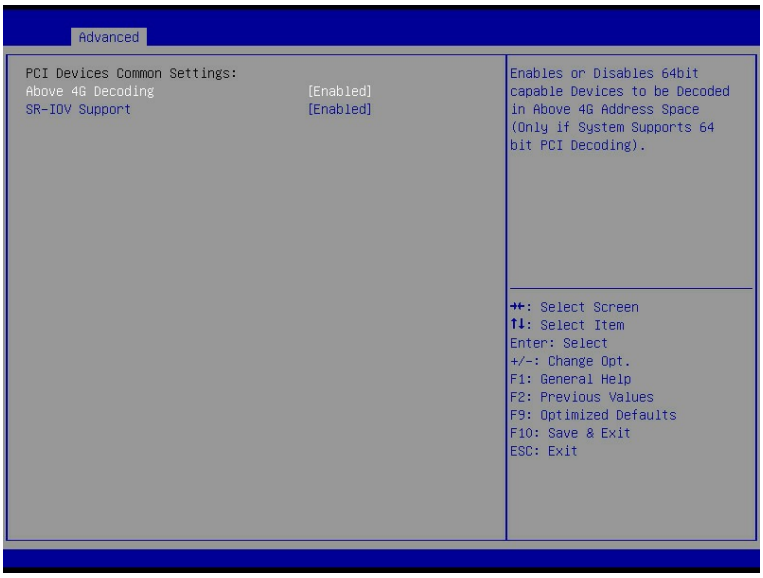
功能描述

PCI Subsystem Settings 界面是 PCI 子系统的相关选项设置。

界面展示

PCI Subsystem Settings 界面如图 3.12 所示。

图 3-12 PCI Subsystem Settings 界面



参数说明

具体参数说明如表 3-11 所示。

表 3-11 PCI Subsystem Settings 界面说明表

界面参数	功能说明	默认值
Above 4G	4G以上内存访问控制开关设置，当系统支持64位PCI解	Enabled

界面参数	功能说明	默认值
Decoding	码时，在4G以上地址空间对64位设备进行解码。选项参数有： ● Enabled：启用 ● Disabled：禁用，Above 4G Decoding设置为Disabled时，网卡的Legacy PXE功能才能用。	
SR-IOV Support	SR-IOV支持开关设置，如果启用，支持SR-IOV的PCIe设备可以虚拟出多个虚拟设备（VF, Virtual function），并且每个VF都具有独立运行所需要的资源，如同一个传统的PCIe设备，具有PCI总线中唯一的BDF (Bus device function)号，均可以被绑定到指定的客户机（虚拟机）。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled

3.2.8 USB Devices Information

功能描述

USB Devices Information 界面显示了 USB 设备相关信息。

界面展示

USB Devices Information 界面如图 3-13 所示。

图 3-13 USB Devices Information 界面

3.2.9 Network Stack Configuration

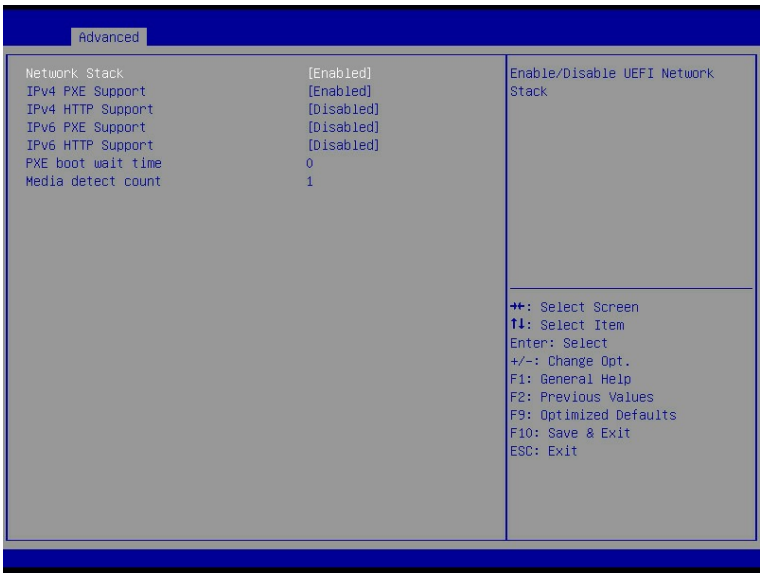
功能描述

Network Stack Configuration 界面是 Network UEFI PXE 相关选项设置。

界面展示

Network Stack Configuration 界面如图 3-14 所示。

图 3-14 Network Stack Configuration 界面



参数说明

具体参数说明如表 3-12 所示。

表 3-12 Network Stack Configuration 界面说明表

界面参数	功能说明	默认值
Network Stack	网络堆栈开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用 如果禁用该选项所有Network Stack Drvier都会被跳过，不执行。 以下选项受该选项控制，只有该选项启用，以下选项才能显示，功能才可设置。	Enabled

界面参数	功能说明	默认值
Ipv4 PXE Support	UEFI Ipv4 PXE支持的开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Ipv4 HTTP Support	Ipv4 HTTP启动支持的开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Ipv6 PXE Support	UEFI Ipv6 PXE支持的开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Ipv6 HTTP Support	Ipv6 HTTP启动支持的开关设置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
PXE boot wait time	等待按ESC键取消PXE boot的时间设置，设置范围0~5。	0
Media detect Count	设备检测次数设置，设置范围1~50。	1

3.2.10 CSM Configuration

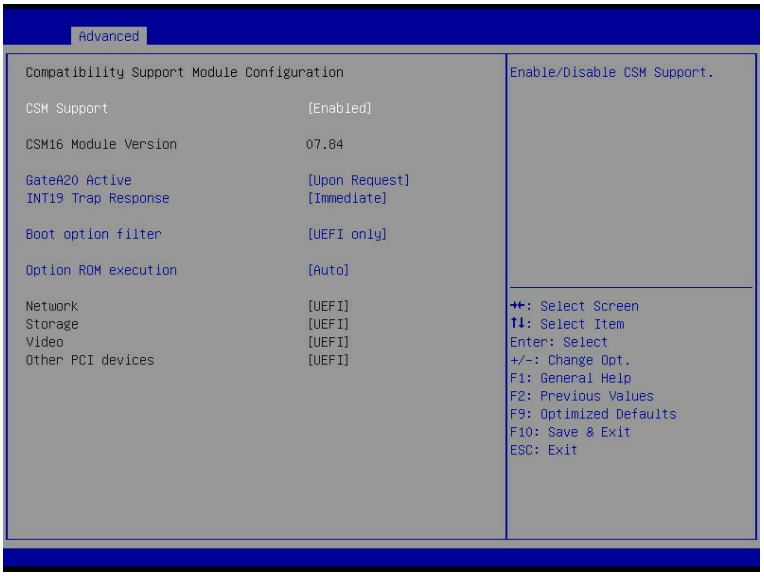
功能描述

CSM Configuration 界面是兼容模块相关选项设置。

界面展示

CSM Configuration 界面如图图 3-15 所示。

图 3-15 CSM Configuration 界面



参数说明

具体参数说明如表 3-13 所示。

表 3-13 CSM Configuration 界面说明表

界面参数	功能说明	默认值
CSM Support	兼容模式支持开关设置，UEFI兼容性支持模块，对不支持UEFI的操作系统提供兼容性支持。选项参数有： ● Enabled：启用 ● Disabled：禁用 注意Legacy启动模式下，该功能会一直处于开启状态。	Enabled
GateA20 Active	A20 地址线的控制模式设置 选项参数有： ● Upon Request：基于需要 ● Always：总是 **注：** A20是一根地址线，这根地址线控制系统对于1MB 以上的那部分内存空间如何进行访问。	Upon Request
INT19 Trap Response	中断、捕捉信号响应设置。选项参数有： ● Immediate：立即响应 ● Postponed：推迟响应	Immediate
Boot option filter	启动模式设置，控制设备Legacy或UEFI模式启动策略。选项参数有：	UEFI Only

界面参数	功能说明	默认值
	• UEFI Only：UEFI模式 • Legacy Only：传统模式	
Option ROM execution	Option ROM 执行策略，该选项控制系统Legacy Option ROM或UEFI Option ROM 的优先级。选项参数有： • Manual：手动 • Auto：自动 **注：** 设置该选项为Auto时，UEFI Option ROM会运行在UEFI启动模式下，Legacy Option ROM会运行在Legacy启动模式下；设置该选项为手动时，用户可以根据情况选择运行UEFI Option ROM或者Legacy Option ROM，若设置错误会使得某些Option ROM无法运行。建议该选项设置为Auto模式。	Auto
Network	网卡Option Rom执行方式设置，选项参数有： • Do not launch：不执行 • Legacy：Legacy模式，加载网卡的Legacy Option ROM。 • UEFI：UEFI模式，加载网卡的UEFI Option ROM。 注： 该选项在Option ROM execution为Manual时才可编辑。	UEFI
Storage	存储设备Option Rom执行方式设置，选项参数同上	UEFI
Video	Video设备Option Rom执行方式设置，选项参数同上	UEFI
Other PCI devices	其他PCI设备Option Rom执行方式设置，选项参数同上	UEFI

3.2.11 OEM NIC Oprom Ctrl

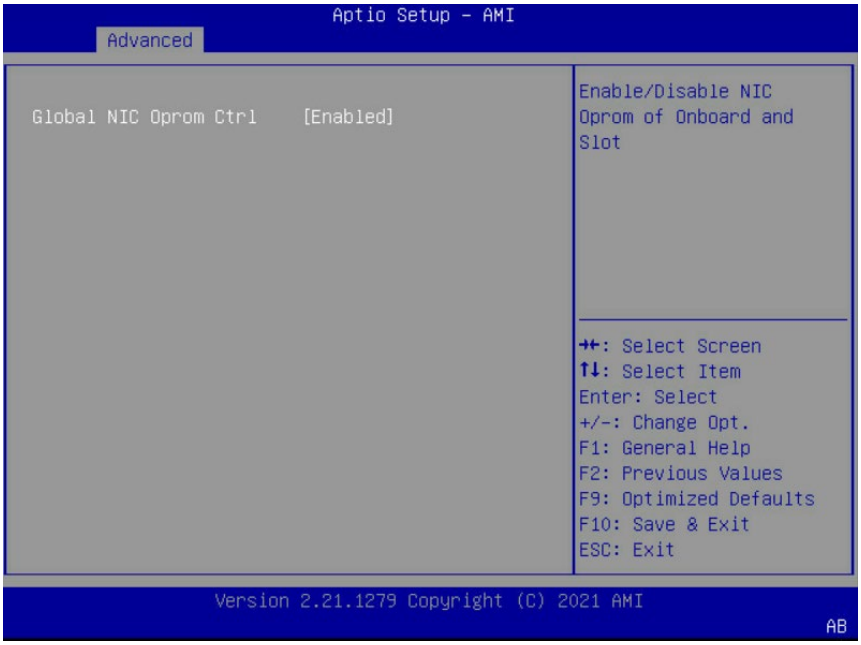
功能描述

OEM NIC Oprom Ctrl 界面是 OEM NIC 操作程序控制。

界面展示

OEM NIC Oprom Ctrl 界面如图 3-16 所示。

图 3-16 OEM NIC Oprom Ctrl 界面



参数说明

具体参数说明如表 3-14 所示。

表 3-14 OEM NIC Oprom Ctrl 界面说明表

界面参数	功能说明	默认值
Global NIC oprom Ctrl Control	全局NIC操作程序控制，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
显示有关PXE OptionRom控制选项，与主板所插设备有关	------	------

3.2.12 iSCSI Configuration

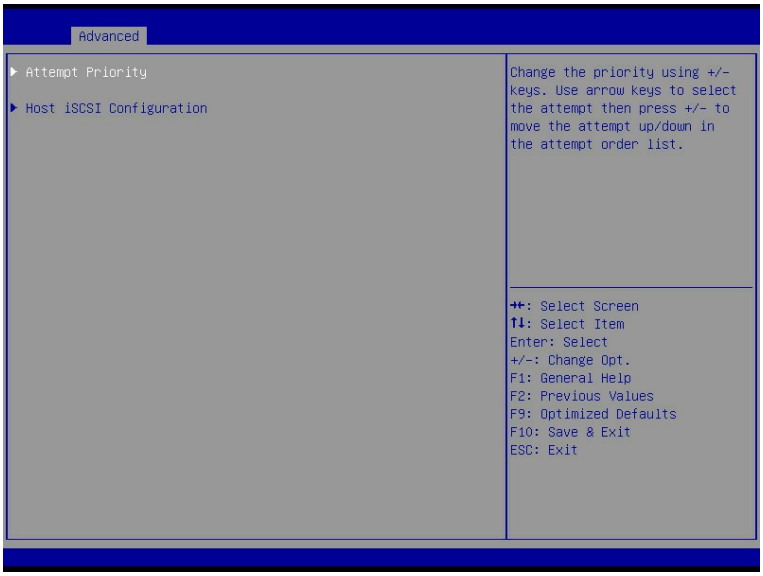
功能描述

iSCSI Configuration 界面是 iSCSI 参数配置，它是在 IP 协议的上层运行的 SCSI 指令集，提供块级的数据访问。

界面展示

iSCSI Configuration 界面如图 3-17 所示。

图 3-17 iSCSI Configuration 界面



参数说明

具体参数说明如表 3-15 所示。

表 3-15 iSCSI Configuration 界面说明表

界面参数	功能说明	默认值
Attempt Priority	尝试优先级设置。选项参数有： ● Host Attempt：主机优先 ● Redfish Attempt：Redfish优先 ● RSD Attempt：RSD优先 **注：** 此选项的作用是调整三个可选项的优先级，通过上下方向键选择要调整的可选项，通过+/-来上下移动此可选项，从而调整优先级。	Host Attempt Redfish Attempt RSD Attempt
Host iSCSI Configration	主机iSCSI 配置	------
iSCSI Initiator Name	iSCSI启动器名称，用来设置iSCSI启动器名称，需要按照iSCSI 限定名称IQN(iSCSI Qualified Name)格式输入，“iqn.”+“年-月”“.”+“颠倒的域名”+“:”+“具体的设备名称”，如：iqn.2020-11.com.example:test01234	------
Add an Attempt	增加一个连接结点	------

界面参数	功能说明	默认值
Delete Attempts	删除连接结点	------
Change Attempt Order	修改尝试连接结点顺序	------

3.2.13 Driver Health

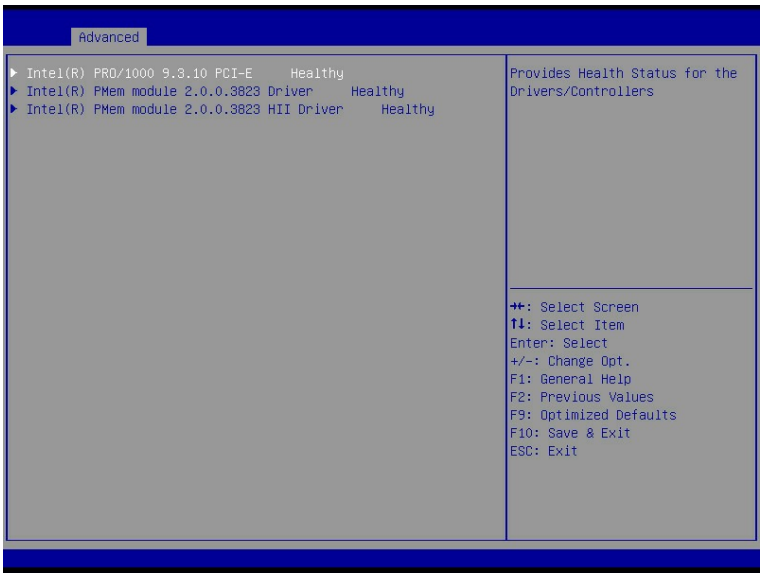
功能描述

Driver Health 界面是设备驱动菜单，表征了设备驱动的健康状态，根据实际设备状态显示。

界面展示

Driver Health 界面如下图 3-18 所示。

图 3-18 Driver Health 界面



3.3 Platform Configuration

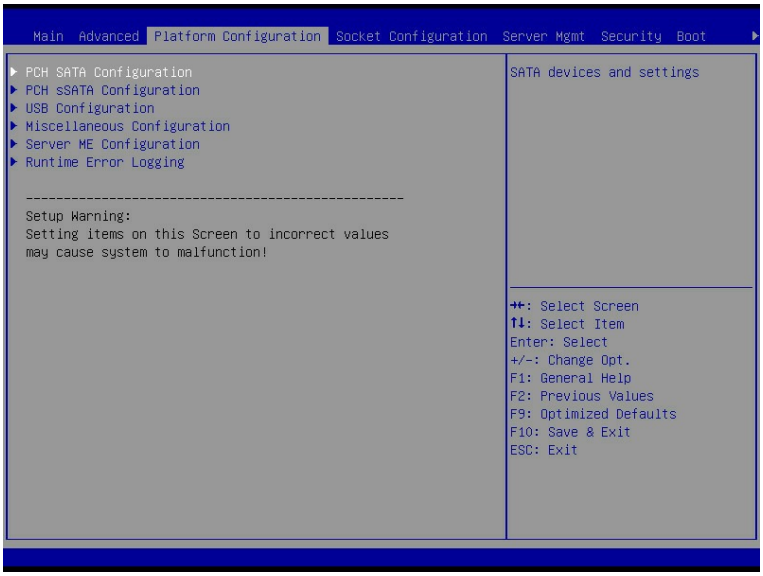
功能描述

Platform Configuration 界面包含 PCH SATA/sSATA 配置菜单、USB 配置菜单、服务器 ME 配置菜单，以及运行时错误日志的配置菜单。

界面展示

Platform Configuration 界面如图 3-19 所示。

图 3-19 Platform Configuration 界面



参数说明

具体参数说明如表 3-16 所示。

表 3-16 Platform Configuration 界面说明表

界面参数	功能说明
PCH SATA Configuration	PCH SATA配置
PCH sSATA Configuration	PCH sSATA配置
USB Configuration	USB配置
Miscellaneous Configuration	一些杂项的配置
Server ME Configuration	服务器ME配置
Runtime Error Logging	运行时错误日志配置

3.3.1 PCH SATA Configuration/PCH sSATA Configuration

功能描述

PCH sSATA Configuration 及 PCH SATA Configuration 界面是对板载的 sSATA 及 SATA 端口进行配置。

界面展示

界面如图 3-20、图 3-21 所示，以 PCH SATA Configuration 菜单为例，介绍板载 SATA 口硬盘配置，PCH sSATA Configuration 界面类似，不再重复。

图 3-20 PCH SATA Configuration 界面

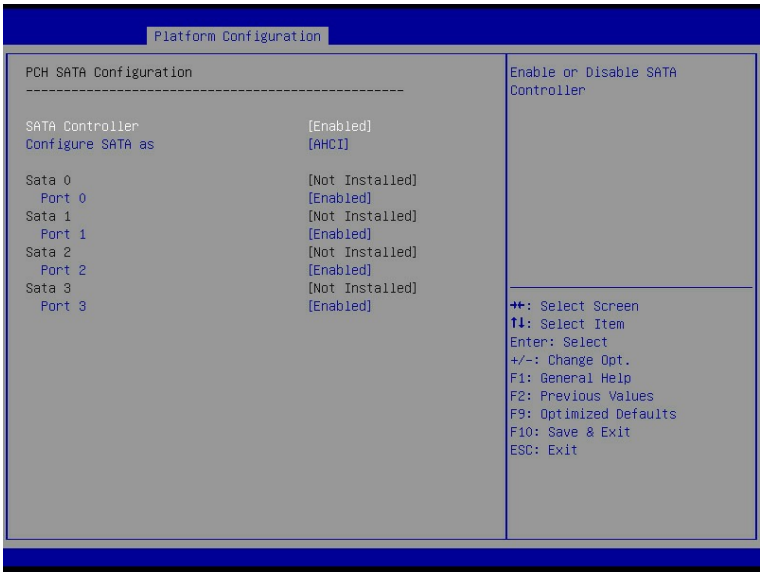
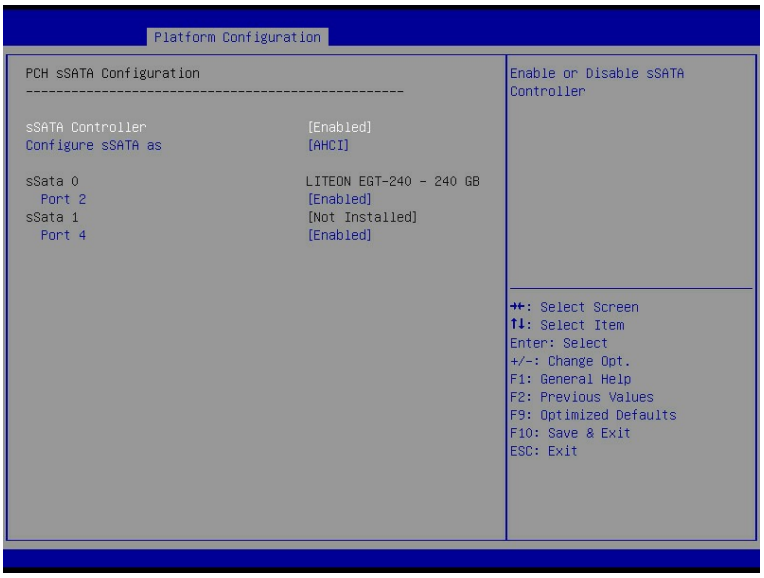


图 3-21 PCH sSATA Configuration 界面



注意

SATA/sSATA端口数量显示以实际机型为准。

参数说明

具体参数说明如表 3-17 所示。

表 3-17 PCH SATA Configuration 界面说明表

界面参数	功能说明	默认值
SATA Controller	SATA控制器开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Configure SATA as	设置SATA模式，选项参数有： ● AHCI：串行ATA高级主控接口，把硬盘模拟为SATA硬盘，需要安装SATA硬盘驱动，支持热插拔。 ● RAID：独立冗余磁盘阵列，把多块独立的物理硬盘按不同的方式组成一个逻辑硬盘。	AHCI
SATA N	SATA端口N所接硬盘信息	----
Port-N	SATA端口开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled

3.3.2 USB Configuration

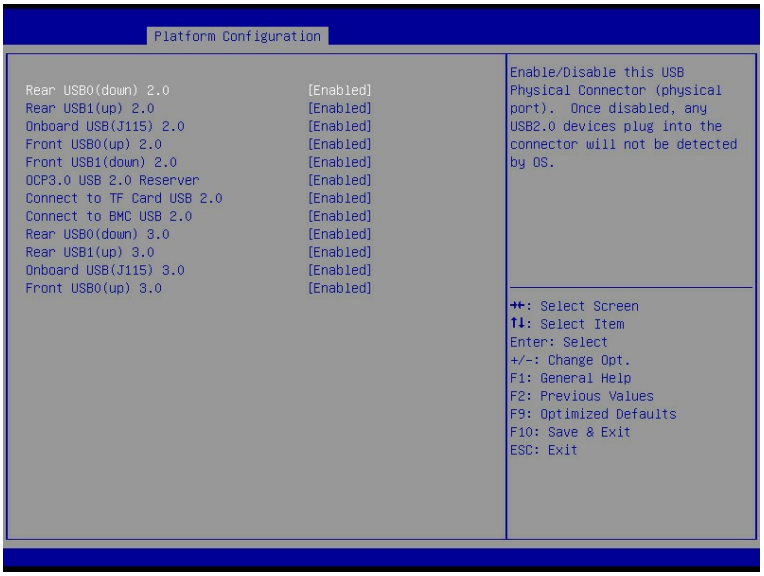
功能描述

USB Configuration 界面是对板载的 USB 端口进行开关设置。

界面展示

USB Configuration 界面如图 3-22 所示。

图 3-22 USB Configuration 界面



注意

USB 端口显示以实际机型为准。

参数说明

具体参数说明如表 3-18 所示。

表 3-18 USB Configuration 界面说明表

界面参数	功能说明	默认值
USB N	USB端口开关设置，包括前置、后置与板载的USB设备（具体显示由丝印信息控制，如Onboard USB0(J116)2.0），选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** 不同服务器的USB Configuration 界面USB 端口配置情况不同，请以实际服务器硬件设计为准；出于服务器安全考虑，建议将不使用的USB端口设置为Disabled	Enabled

3.3.3 Miscellaneous Configuration

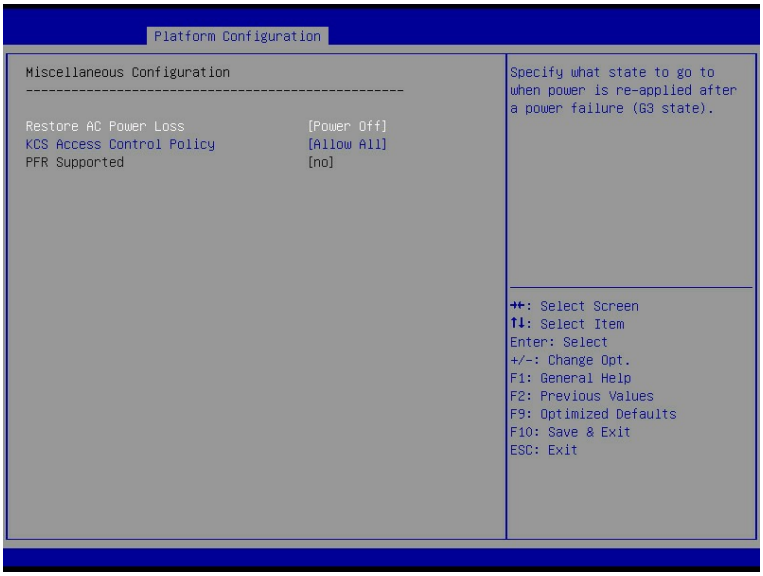
功能描述

Miscellaneous Configuration 界面是混杂常用设置项配置。

界面展示

Miscellaneous Configuration 界面如图 3-23 所示。

图 3-23 Miscellaneous Configuration 界面



参数说明

具体参数说明如表 3-19 所示。

表 3-19 Miscellaneous Configuration 界面说明表

界面参数	功能说明	默认值
Restore AC Power Loss	AC上电开机电源状态设置，选项参数有： ● Power On：开机状态 ● Power Off：关机状态 ● Last State：恢复上次的状态	Power Off
KCS Access Control Policy	决定何时通过KCS接口发送IPMI命令，选项参数有： ● Allow All：始终 ● Restricted：直到发出BIOS DONE信号为止 ● Deny All：从不	Allow All

界面参数	功能说明	默认值
PFR Supported	提示性选项，选项值开机自动更新，根据平台是否支持PFR显示为“yes”或“no”	----

3.3.4 Server ME Configuration

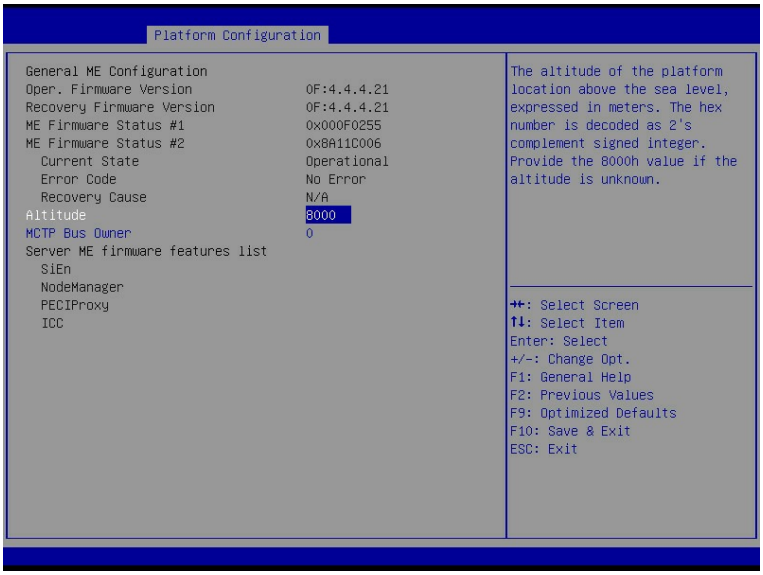
功能描述

Server ME Configuration 界面是服务器 ME 信息显示及相关配置设置。

界面展示

Server ME Configuration 界面如图 3-24 所示。

图 3-24 Server ME Configuration 界面



参数说明

具体参数说明如表 3-20 所示。

表 3-20 Server ME Configuration 界面说明表

界面参数	功能说明	默认值
General ME Configuration	----	----
Oper. Firmware Version	ME有效固件版本	----
Recovery Firmware Version	ME备份固件版本	----
ME Firmware Status #1	ME FW状态值#1	----

界面参数	功能说明	默认值
ME Firmware Status #2	ME FW状态值#2	----
Current State	当前状态	----
Error code	错误码代码	----
Recovery Cause	恢复原因	N/A
Altitude	平台位置在海平面以上的高度，十六进制数，以米为单位。	8000
MCTP Bus Owner	MCTP 总线主控者位于PCIe: [15:8] bus, [7:3] device, [2:0] function设置为0，表示为禁用	0
Server ME Firmware Features list	服务器ME固件功能列表	----

3.3.5 Runtime Error Logging

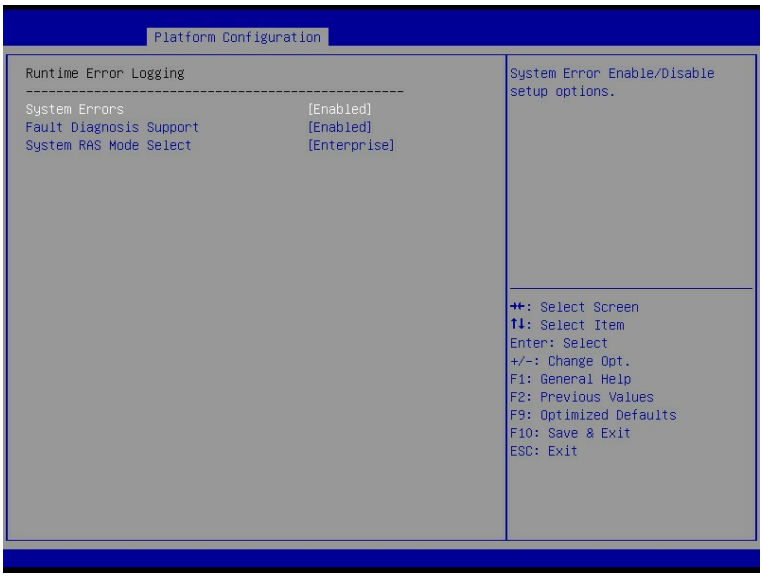
功能描述

通过 Runtime Error Logging 界面，可以对故障诊断、日志收集和 RAS 模式等特性进行配置。

界面展示

Runtime Error Logging 界面如图 3-25 所示。

图 3-25 Runtime Error Logging 界面



参数说明

具体参数说明如表 3-21 所示。

表 3-21 Runtime Error Logging 界面说明表

界面参数	功能说明	默认值
System Errors	系统错误日志记录设置，启用该功能后，会收集关键部件的错误并记录日志。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Fault Diagnosis Support	故障诊断支持：错误信息收集。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
System RAS Mode Select	选择系统RAS模式，选项参数有： ● Enterprise：企业模式 ● Cloud：云模式 ● Custom：自定义模式 **注：** 选择企业模式时，BIOS优先处理可纠正错误；选择云模式时，操作系统优先，完全由操作系统处理可纠正错误。	Enterprise

3.4 Socket Configuration

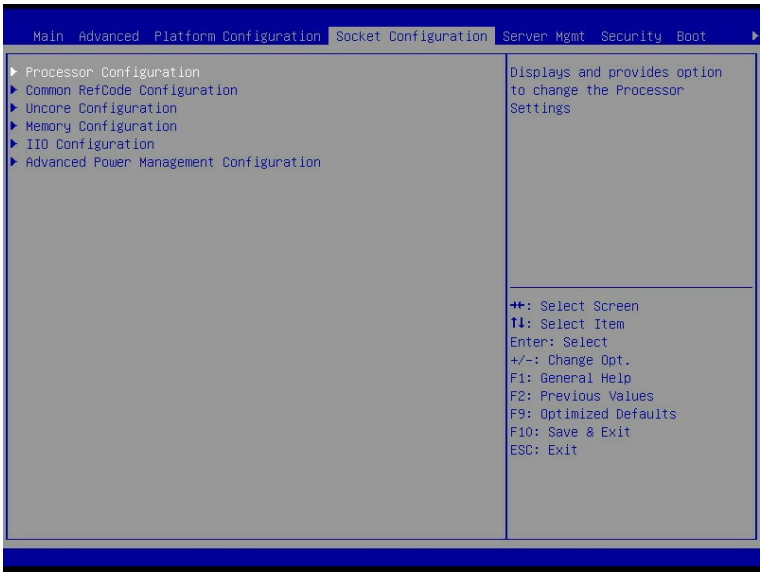
功能描述

Socket Configuration 界面是处理器，内存等相关选项设置。

界面展示

Socket Configuration 界面如图 3-26 所示。

图 3-26 Socket Configuration 界面



参数说明

具体参数说明如表 3-22 所示。

表 3-22 Socket Configuration 界面说明表

界面参数	功能说明
Processor Configuration	处理器配置
Common RefCode Configuration	常用Reference Code配置
Uncore Configuration	Uncore配置
Memory Configuration	内存配置
IIO Configuration	IIO配置
Advanced Power Management Configuration	高级电源管理配置

3.4.1 Processor Configuration

功能描述

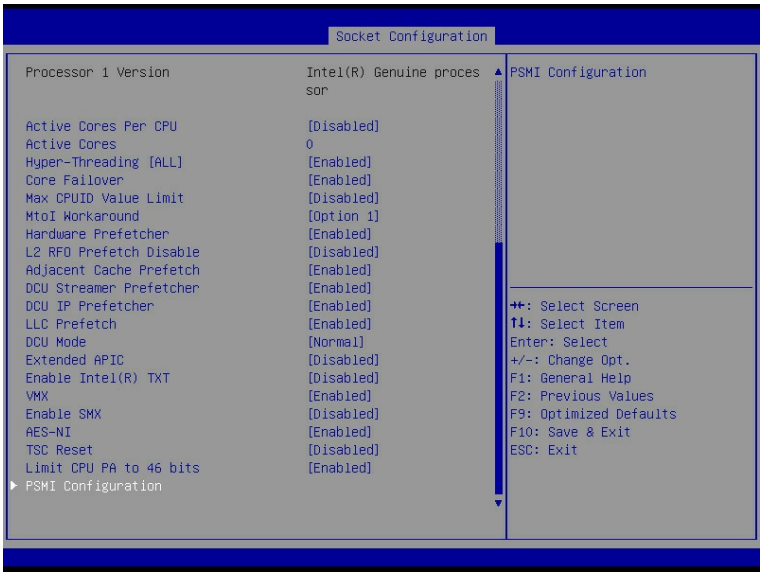
Processor Configuration 界面是处理器的相关选项设置。

界面展示

Processor Configuration 界面如图 3-27 和图 3-28 所示。

图 3-27 Processor Configuration 界面

图 3-28 Processor Configuration 界面



参数说明

具体参数说明如表 3-23 所示。

表 3-23 Processor Configuration 界面说明表

界面参数	功能说明	默认值
Processor BSP Revision等	处理器信息子菜单，处理器的详细信息	----

界面参数	功能说明	默认值
Active Cores Per CPU	控制是否启用每个CPU的所有核心，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** 当启用该选项时，启用CPU的核心数由选项Core Disabled Bitmap (Hex)显示，0表示开启所有的核心数，且每个CPU至少开启一个核心。	Disabled
Active Cores(Active Cores Per CPU为Disabled时显示，且该选项的值会影响Available Bitmap的值)	启用CPU核心数设置，当选项Active Cores Per CPU设置为Disabled时此选项显示。输入所要开启的CPU核数，Help信息中会根据当前CPU的情况，显示该选项可以设置的有效值和CPU的最大物理核数。 默认值0表示开启所有核心数。	0
Hyper-Threading [ALL]	超线程技术开关设置，启用该功能，会使得一个实体CPU具有两个逻辑线程进行数据处理，有利于提高系统的整体性能。选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Core Failover(两路产品)	启用备用核心来代替BIST自检失败的核心，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Max CPUID Value Limit	最大CPUID值限制开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 当传统操作系统启动不支持CPU扩展CPUID功能时，请启用该选项。	Disabled
Hardware Prefetcher	硬件预取开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** 硬件预取是指CPU处理指令或数据之前，将这些指令或数据从内存预取到L2缓存	Enabled

界面参数	功能说明	默认值
	中，以减少内存读取的时间，帮助消除潜在的瓶颈，以此提高系统效能	
L2 RFO Prefetch Disable	L2 RFO Prefetch禁用功能开关，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Adjacent Cache Prefetch	相邻缓存预取开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** 开启相邻缓存预取功能后，计算机在读取数据时，会智能的认为要读取数据的旁边或邻近的数据也是需要的，于是在处理的时候就会将这些邻近的数据预先读取出来，这样可以加快读取速度。	Enabled
DCU Streamer Prefetcher	DCU流预取开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** DCU(Data Cache Unit)流预取器是L1 Data Cache的预取器，如果DCU流预取器检测到在一段时间内从同一缓存行进行多次加载，即认为下一缓存行将被使用，从而把下一缓存行从L2缓存或内存中预取到L1 Data Cache中。	Enabled
DCU IP Prefetcher	DCU IP预取开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** DCU IP预取器是L1 Cache的预取器，DCU IP预取器根据历史加载记录决定是否从内存或L2缓存中预取下一条数据放入到L1 Cache中。	Enabled
LLC Prefetcher	所有线程LLC预取开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disable(四路产品) Enabled(两路产品)
DCU Mode	DCU Mode设置，选项参数有：	Normal

界面参数	功能说明	默认值
	● Normal：正常模式 ● Mirror-Mode：镜像模式(两路产品)	
Extended APIC	扩展APIC(Advanced Programmable Interrupt Controlle)开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** 扩展APIC功能需要VT-d的支持。当扩展APIC设置为Enabled，而VT-d为Disabled时，某些操作系统会无法正确的处理Interrupt，需要VT-d Interrupt Remmaping的功能支持。所以，当扩展APIC设置为Enabled时，建议VT-d也设置为Enabled状态。 当所配置的处理器总核数（线程数）超过256个时，建议开启扩展APIC功能以使操作系统更高效的支持CPU多核特性功能。	Disabled
Enable Intel(R) TXT	Intel可信执行技术支持开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
VMX(选项Enable Intel(R) TXT为Enabled时，选项不可选)	Intel硬件辅助虚拟化技术开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** VMX(Virtual Machine Extensions)是Intel 64或IA-32架构虚拟化技术提供的虚拟化扩展，启用该选项后，Intel 64或IA-32平台可以作为多个虚拟系统（或虚拟机）使用。每个虚拟机可以在单独的隔离区中运行操作系统和应用程序。	Enabled
Enable SMX(选项Enable Intel(R) TXT为Enabled时，选项不可选)	安全模式扩展开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：**	Disabled

界面参数	功能说明	默认值
	SMX(Safer Mode Extensions)为系统软件提供了一个编程接口，用于在平台内建立一个可测量的环境，以支持终端用户的可信决策，可测量环境所使用的测量和保护机制需要Intel(R) TXT支持。	
AES-NI	AES指令开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 **注：** 该菜单主要控制CPU是否支持AES指令，这些指令主要用于虚拟化系统，打开该指令之后，系统性能能得到提升。	Enabled
TSC Reset(两路产品)	在热重启期间启用或禁用TSC重置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Limit CPU PA to 46 bits(两路产品)	将CPU物理地址限制为46位以支持旧的Hyper-V，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled(四路产品) Enabled(两路产品)

Intel TXT (Intel Trusted Execution Technology，可信执行技术)，是安全功能的集合，主要通过使用特定的 Intel CPU、专用硬件以及相关固件，建立一个从开机就可信的环境，进而为系统软件提供多种方法，实现数据的保护，建立安全的系统。

1. PSMI configuration

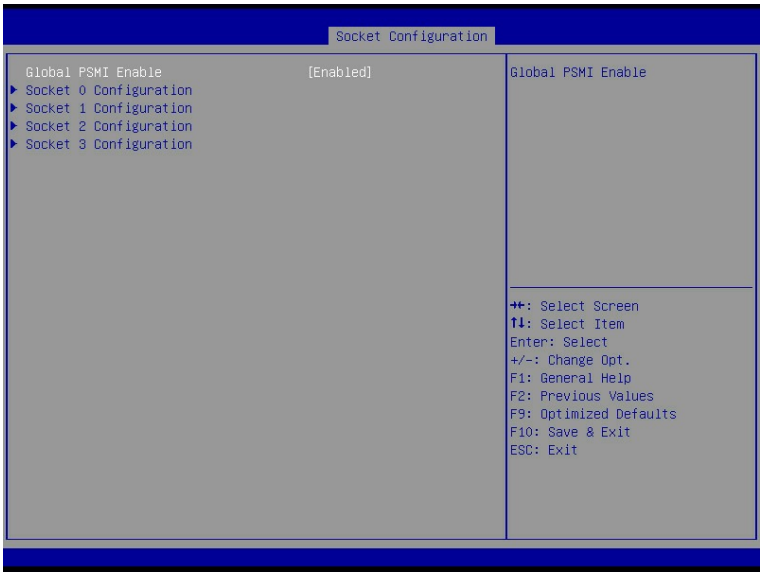
功能描述

PSMI configuration 界面是电源配置管理接口选项设置。

界面展示

PSMI configuration 界面如图 3-29 所示。

图 3-29 PSMI configuration 界面



参数说明

具体参数说明如表 3-24 所示。

表 3-24 PSMI configuration 界面说明表

界面参数	功能说明	默认值
Global PSMI Enable	全局PSMI开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Socket (0-n) Configuration	每个Socket的PSMI配置界面，只有在Global PSMI Enable设置为Enabled时可见	----

3.4.2 Common RefCode Configuration

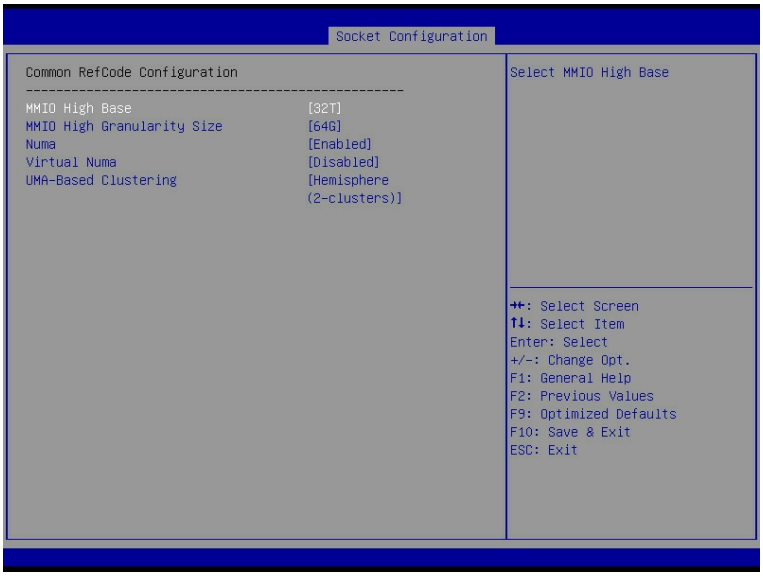
功能描述

Common RefCode Configuration 界面是通用选项设置。

界面展示

Common RefCode Configuration 界面如图 3-30 所示。

图 3-30 Common RefCode Configuration 界面



参数说明

具体参数说明如表 3-25 所示。

表 3-25 Common RefCode Configuratio 界面说明表

界面参数	功能说明	默认值
MMIO High Base	MMIO内存映射IO高位基地址设置，选项参数有： ● 56T ● 40T ● 32T ● 24T ● 16T ● 4T ● 2T ● 1T ● 512G 注： 一般情况下，该选项的值要大于当前服务器物理内存的总容量，否则可能会导致内存初始化失败。若选项的值小于服务器物理内存的总容量，因为MMIO Hight Base的限制，在OS下看到的内存容量会比实	32T (NF5488M6/NF5468M5/NF5688M5默认4T)

界面参数	功能说明	默认值
	际内存容量小。某些情况下，为了兼容某些板卡，特别是Legacy下，可适当选择较小的选项参数。	
MMIO High Granularity Size	MMIO内存映射IO高位粒度大小设置，默认等同于每个栈分配的MMIO资源大小。选项参数有： ● 1G ● 4G ● 16G ● 64G ● 256G ● 1024G 注： 当MMIO High Base为56T该选项不能设置为1024G。	64G (NF5488M6/NF5468M5/NF5688M5默认1024G)
Numa	Numa开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 注： 非统一内存访问（Non-uniform memory access，Numa）是一种内存共享架构，启用后，每个CPU可以使用自己本地内存，又可以访问其他CPU的内存。访问本地内存具有低时延-高带宽的性能，访问其他CPU的内存具有高延时-低带宽的性能。	Enabled
Virtual Numa(两路产品)	在ACPI表中将物理NUMA节点划分为均匀大小的虚拟NUMA节点，提高Windows在搭配超过64个逻辑处理器的CPU时的性能。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabed
UMA-Based Clustering (两路产品)	UMA集群设置， ● Disable (All2All)：禁用 ● Hemisphere (2-clusters)：半球（2-clusters）	Hemisphere (2-clusters)

界面参数	功能说明	默认值
	注： 这些选项仅在禁用SNC时有效。如果启用了SNC，则BIOS将自动禁用基于UMA的群集。	

3.4.3 Uncore Configuration

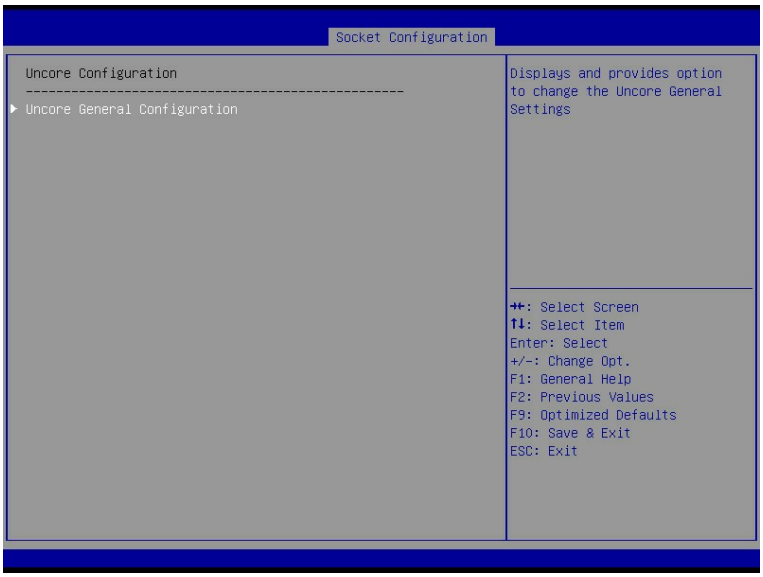
功能描述

Uncore Configuration 界面是 Uncore 相关选项设置。

界面展示

Uncore Configuration 界面如图 3-31 所示。

图 3-31 Uncore Configuration 界面



参数说明

具体参数说明如表 3-26 所示。

表 3-26 Uncore Configuration 界面说明表

界面参数	功能说明	默认值
Uncore General Configuration	Uncore通用功能控制菜单	----

1. Uncore General Configuration

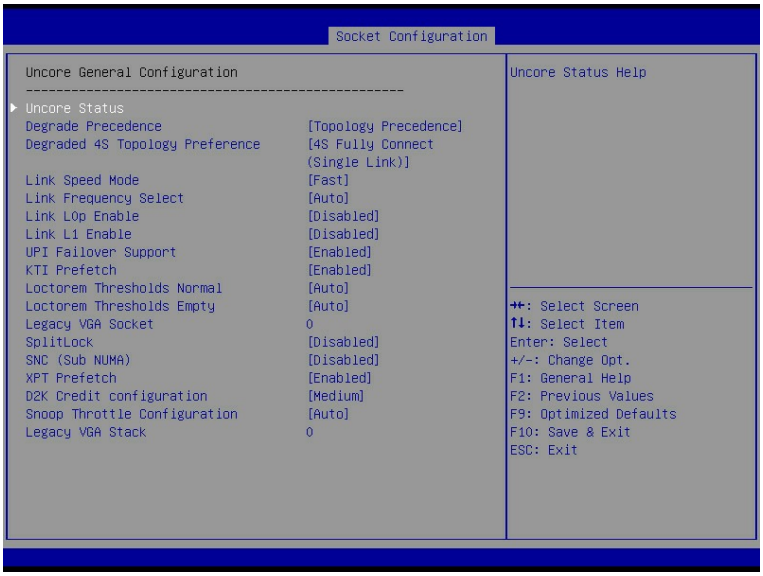
功能描述

Uncore General Configuration 界面是 Uncore 通用功能选项设置。

界面展示

Uncore General Configuration 界面如图 3-32 所示。

图 3-32 Uncore General Configuration 界面



参数说明

具体参数说明如表 3-27 所示。

表 3-27 Uncore General Configuration 界面说明表

界面参数	功能说明	默认值
Uncore Status	Uncore链接状态子菜单，显示当前UPI链接状态	----
Degrade Precedence	降低优先级设置，选项参数有： ● Topology Precedence：拓扑优先 ● Feature Precedence：特征优先 注： 当系统设置冲突时通过设置Topology Precedence来降低Feature，或通过设置Feature Precedence来降低	Topology Precedence

界面参数	功能说明	默认值
	Topology。	
Degraded 4S Topology Preference	当系统可以降级为4S1Lfully Connect或4S2LRing拓扑时，选择降级的拓扑： ● 4S Fully Connect (Single Link) ● 4S Ring (Dual Link)	4S Fully Connect (Single Link)
Link Speed Mode	链接速度模式设置，选项参数有： ● Slow ● Fast	Fast
Link Frequency Select	链接频率选择设置，选项参数有： ● Auto ● 9.6 GT/s ● 10.4GT/s ● 11.2GT/s(两路产品) 注： Auto将获取当前配置可支持的最大链接频率。若将链路频率设置为较低速度，以较低频率运行可降低功耗，但同时会影响系统性能。	Auto
Link L0p Enable	L0p节能选项开关设置，选项参数有： ● Disabled：禁用 ● Enabled：启用 ● Auto：自动 注： Auto默认为Enabled。	Disabled
Link L1 Enable	L1节能选项开关设置，选项参数有： ● Disabled：禁用 ● Enabled：启用 ● Auto：自动 注： Auto默认为Enabled。	Disabled
UPI Failover Support	UPI失效转移支持开关设置，选项参数有： ● Disabled：禁用 ● Enabled：启用 ● Auto：自动 注： Auto默认为Enabled。	Enabled
XPT Remote Prefetch (两路产品)	XPT远程预取的开关设置，选项参数有： ● Disabled：禁用 ● Enabled：启用	Auto

界面参数	功能说明	默认值
	● Auto：自动 注：Auto根据CPU型号来判断是否Enabled。	
KTI Prefetch	KTI预取的开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 ● Auto：自动 注： Auto默认为Enabled。	Enabled
Loctorem Thresholds Normal	TOR阈值-Loctorem Normal阈值设置，选项参数有： ● Disabled：禁用 ● Auto：自动 ● Low：低 ● Medium：中 ● High：高	Auto
Loctorem Thresholds Empty	TOR阈值- Loctorem Empty阈值设置，选项参数有： ● Disabled：禁用 ● Auto：自动 ● Low：低 ● Medium：中 ● High：高	Auto
Legacy VGA Socket	传统VGA个数设置，有效值范围0~3。	0
SplitLock	SplitLock开关设置，选项参数有： ● Disabled：禁用 ● Enabled：启用 ● Auto：自动 注： Auto默认为Enabled。	Disabled
SNC (Sub NUMA)（四路产品)	四路产品 CPU的Sub NUMA集群设置，选项参数有： ● Disabled：不支持SNC功能 ● Enabled：支持所有的SNC集群（2-clusters）和1-way的IMC交错 ● Auto：根据IMC交错支持1-cluster 或者2-clusters	Disabled
SNC (Sub NUMA)（两路产品)	两路产品CPU的Sub NUMA集群设置，选项参数有： ● Disabled：支持1-clusters（XPT/KTI预取启用）的SNC集群4-way的IMC交错	Disabled

界面参数	功能说明	默认值
	• Enable SNC2 (2-clusters)：支持2-clusters的SNC集群和2-way的IMC交错	
XPT Prefetch	XPT预取的开关设置，选项参数有： • Disabled：禁用 • Enabled：启用 • Auto：自动 注： Auto默认为Enabled。	Enabled
D2K Credit configuration (四路产品)	选择可用的D2K VNA BL积分级别重新进行分配： • Low：低级 • Medium：中级 • High：高级	Medium
Snoop Throttle Configuration	选择CHA的侦听门限级别： • Disabled：禁用 • Low：低级 • Medium：中级 • High：高级 • Auto：自动	Auto
Legacy VGA Stack	传统VGA堆栈个数设置，有效值范围0~6	0
PCIe Remote P2P Relaxed Ordering(两路产品)	Pcie远程P2P放宽排序开关设置，选项参数有： • Disabled：禁用，硬件将强制执行P2P写入顺序 • Enabled：启用，由软件决定放宽P2P写入顺序	Disabled

3.4.4 Memory Configuration

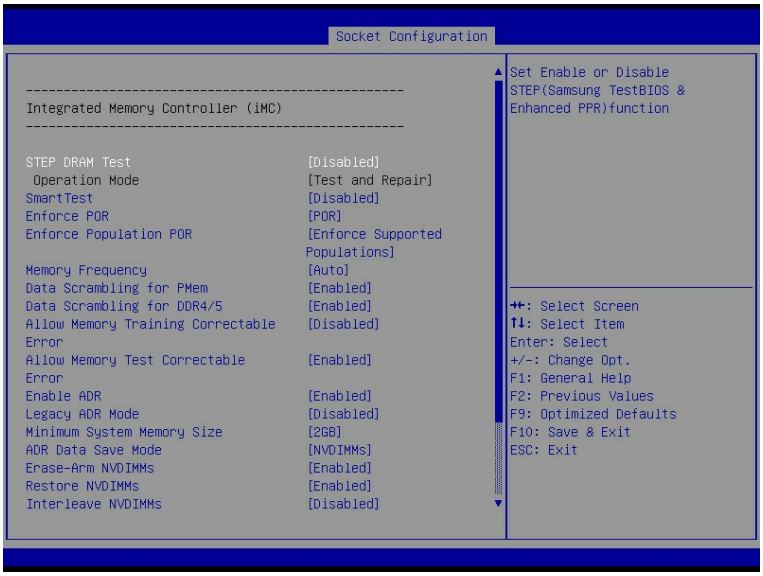
功能描述

Memory Configuration 界面是内存相关选项设置。

界面展示

Memory Configuration 界面如图 3-33 所示。

图 3-33 Memory Configuration 界面



参数说明

具体参数说明如表 3-28 所示。

表 3-28 Memory Configuration 界面说明表

界面参数	功能说明	默认值
Enforce POR	强制执行POR设置，选项参数有： ● POR ● Disabled：禁用 注： POR(Plan of Record)是指Intel提供限制DDR4执行频率规定，若设置该选项的值为POR，则系统会强制按照POR原则对DDR4内存频率进行设置。	POR
STEP DRAM Test(四路产品)	打开或关闭STEP(Samsung TestBIOS & Enhanced PPR)功能，选项参数有： ● Disabled：禁用 ● Enabled：启用	Disabled
Operation Mode(四路产品)	设置操作模式，选项参数有： ● Test and Repair：检测并修复 ● Test Only：仅检测	Test and Repair
SmartTest(四路产品)	● Disabled：禁用 ● Enabled：启用	Disabled
SmartTest	● Disabled：禁用	Enabled

界面参数	功能说明	默认值
PPR(四路产品，选项SmartTest为Enabled时显示)	● Enabled：启用	
Enforce Population POR(Enforce POR选项为POR时显示)	强制执行内存集合POR，选项参数有： ● Disable Enforcement：关闭 ● Enforce Supported Populations：启用支持的集合 ● Enforce Validated Populations：启用已验证的集合	Enforce Supported Populations
Memory Frequency	内存频率设置，选项参数有： ● Auto ● 1866 ● 2133 ● 2400 ● 2666 ● 2933 ● 3200 注： Auto设置的内存频率为内存的默认频率和CPU支持的最大内存频率这两者中的较小值。	Auto
Data Scrambling for PMem	PMem数据扰频开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Data Scrambling for DDR4/5	DDR4/5数据扰频开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Allow Memory Training Correctable Error	允许内存训练可修复的错误，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Allow Memory Test Correctable Error	允许内存测试可修复的错误，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Enable ADR	ADR (Asynchronous Dram Refresh) 异步内存刷新使能开关设置，启用该选项后，可在电源异常情况下，保护内存数据不丢失。选项参数有： ● Enabled：启用	Enabled

界面参数	功能说明	默认值
	● Disabled：禁用	
Legacy ADR Mode	传统ADR模式开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Minimum System Memory Size	仅在有JEDEC NVDIMM时为系统分配的最小内存，选项参数有： ● 2GB ● 4GB ● 6GB ● 8GB	2GB
NVDIMM Energy Policy(两路产品)	设置NVDIMM的能耗策略，选项参数有： ● Device-Managed：设备控制 ● Host-Managed：主机控制	Device-Managed
ADR Data Save Mode	ADR数据保存模式设置，选项参数有： ● Disabled：禁用 ● Batterybacked DIMMs：电源保存 ● NVDIMMs：不易失内存	NVDIMMs
Erase-Arm NVDIMMs	Erase-Arm NVDIMMs开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Restore NVDIMMs	修复NVDIMMs开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Interleave NVDIMMs	交错NVDIMMs开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
SPD-SMBUS Access(Only for两路产品)	控制CPU的SPD SMBUS访问权限，选项参数有： ● Lock：锁定 ● UnLock：解锁	Lock
SPD Print	控制SPD打印开关，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
SPD Print Length(SPD Print选项Enabled时可选)	控制SPD打印长度，选项参数有： Auto：自动 ● 256 Byte：256字节 ● 512 Bytes：512字节 **注：**	Auto

界面参数	功能说明	默认值
	Auto默认为最大长度512字节。	
Cmd Setup % Offset	Cmd设置/保持百分比偏移量，用于后期cmd训练结果。可选范围0~100	50
Periodic Rcomp(两路产品)	内存周期补偿寄存器开关设置，选项参数有： ● Auto：自动 ● Enabled：启用 ● Disabled：禁用 **注：** Auto默认使用CSR MemComp comp_disable寄存器的值。	Auto
Periodic Rcomp Interval(Only for两路产品，选项Periodic Rcomp为Disabled时隐藏)	内存周期补偿寄存器的值，选项参数有： ● 10.24us ● 20.48us ● 40.96us ● 163.84us ● 327.68us ● 655.36us ● 1310.72us ● 2621.44us ● 5242.88us ● 10.48576ms ● 20.67152ms ● 41.94304ms ● 83.88608ms ● 167.77216ms ● 335.54432ms ● 671.08864 ms	671.08864 ms
Memory Topology	内存拓扑子菜单，显示在位内存详细信息	----
Memory Map	内存Map子菜单	----
Memory RAS Configuration	内存RAS配置子菜单	----

1. Memory Map

功能描述

Memory Map 界面是内存模式设置。

界面展示

Memory Map 界面如图 3-34 所示。

图 3-34 Memory Map 界面

参数说明

具体参数如表 3-29 所示。

表 3-29 Memory Map 界面说明表

界面参数	功能说明	默认值
Volatile Memory Mode (四路产品隐藏，两路产品中Numa 选项为Disabled时不可选)	易失内存模式设置，选择启用1LM内存模式或启用2LM内存模式，选项参数有： ● 1LM ● 2LM	2LM
AppDirect cache(Volatile Memory Mode选项为1LM时隐藏)	为内存区域启用缓存的开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
eADR Support	支持eADR功能的开关设置，选项参数有： ● Auto：自动 ● Enabled：启用 ● Disabled：禁用 注： Auto默认为Disabled。	Disabled
CPU Cache Flush	eADR开启时，eADR程序刷新CPU缓存的执行	Serial

界面参数	功能说明	默认值
Mode(选项eADR Support为Enabled时显示)	模式，选项参数有： ● Serial：串行 ● Parallel：并行	
1LM Memory Interleave Granularity(四路产品且Volatile Memory Mode为1LM才显示)	1LM内存交叉间隔设置，选项参数有： ● 256B Target, 256B Channel ● 64B Target, 64B Channel	256B Target, 256B Channel

2. Memory RAS Configuration

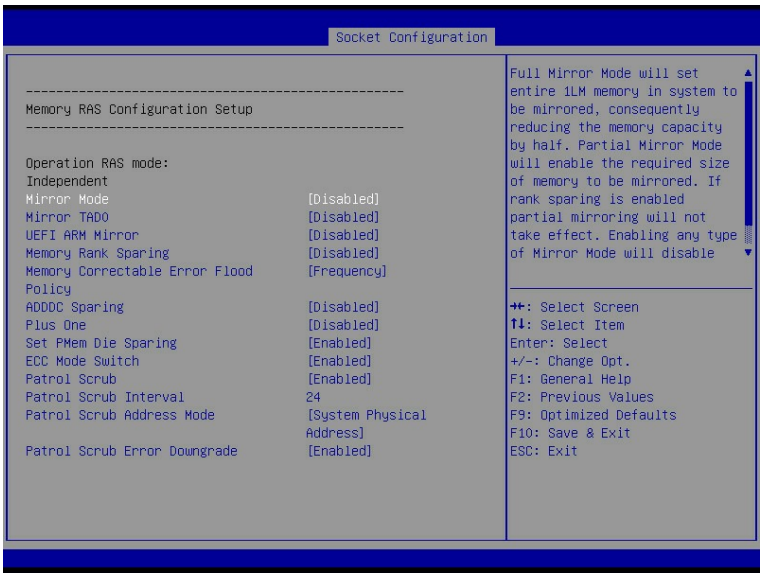
功能描述

Memory RAS Configuration 界面是内存 RAS 特性相关选项设置。

界面展示

Memory RAS Configuration 界面如图 3-35 所示。

图 3-35 Memory RAS Configuration 界面



参数说明

具体参数说明如表 3-30 所示。

表 3-30 Memory RAS Configuration 界面说明表

界面参数	功能说明	默认值
NEW SDDC Mode (两路产品)	使能48B SDDC ECC ● Enabled：启用 ● Disabled：禁用	Enabled
Enable Pcode WA for SAI PG (两路产品)	启用SAI策略组的Pcode解决方法： ● Enabled：启用 ● Disabled：禁用	Disabled
Mirror Mode(ADDDC Sparing为Enabled时不可选)	镜像模式设置，选项参数有： ● Disabled：禁用 ● Full Mirror Mode：全局镜像模式 ● Patial Mirror Mode：局部镜像模式 注： 全局镜像模式会将系统中的整个1LM内存设置为镜像，从而内存容量将会减少一半；启用局部镜像模式是将部分内存设置镜像，若启用了Rank Sparing，则局部镜像模式将不会生效；且无论启用任何镜像模式都会禁用XPT Prefetch。	Disabled
Partial Mirror 1 Size (GB) (Mirror Mode选项为Partial Mirror Mode时显示)	选择创建的SAD 容量大小，单位1GB。 注意镜像大小必须小于总内存大小的一半。 0-X (X为系统总内存容量的1/2)	0
Mirror TAD0(Mirror Mode为非Full Mirror Mode时可选，ADDDC Sparing为Enabled时不可选)	镜像TAD0模式开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
UEFI ARM Mirror(Mirror Mode为Disabled时可选，ADDDC Sparing为Enabled时不可选)	UEFI ARM镜像模式开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
ARM Mirror percentage(UEFI ARM Mirror为Enabled时显示)	输入UEFI ARM镜像的百分比，5000代表50%，可选范围： 0-5000	0
Memory Rank	内存Rank热备开关设置，选项参数有：	Disabled

界面参数	功能说明	默认值
Sparing(四路产品，Mirror Mode为Disabled且UEFI ARM Mirror为Disabled，且没有AEP/BPS三个条件同时存在时此选项可选)	● Enabled：启用 ● Disabled：禁用 注： 当启用该选项后，一个Rank可作为同一通道的其它Rank的备用，若有Rank出现缺陷，可以用同一内存通道中其它闲置的Rank来代替，将有缺陷Rank的数据复制到代替Rank中。	
Multi Rank Sparing(四路产品，Memory Rank Sparing为Enabled时可选)	选择内存Rank热备的数量，选项参数有： ● One Rank：要求通道中的Rank数量大于2 ● Two Rank：要求通道中的Rank数量大于4	Two Rank
Memory Correctable Error Flood Policy	内存可修复错误的放行策略： ● Disabled：不放行 ● Once：一次 ● Frequency：多次	Frequency
ADDDC Sparing(没有AEP/BPS且Memory Rank Sparing为Disabled时可选)	ADDDC(Adaptive Double Device Data Correction Sparing) 自适应双设备数据校正备用设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 注： 启用该选项后，针对运行阶段检测到的内存可修复错误，BIOS最多支持在一个内存通道内做两次失效区域替换和一次备份处理。若考虑性能优先，建议禁用该选项，若考虑可靠性优先，建议开启该功能。	Disabled
Plus One(Memory Rank Sparing为Disabled时可选)	启用SDDC+1，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Enable ADDDC Error Inject(ADDDC Sparing为Enable时显示)	允许ADDDC注错，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Set NGN Die Sparing	设置NGN Die热备开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
ECC mode switch(四	允许内存控制器由模式A切换到模式B，选项参	Enabled

界面参数	功能说明	默认值
路产品)	数有： ● Enabled：启用 ● Disabled：禁用	
Patrol Scrub	内存巡检开关设置，选项参数： ● Enabled：启用 ● Disabled：禁用 ● Enable at End of POST：在POST结束启用 注： 启用该选项后，系统会提供内存巡检功能，及时处理内存的可纠正错误,防止可纠正错误积累成不可纠正错误。	Enable at End of POST
Patrol Scrub Interval	内存巡检间隔时间设置，单位是小时，范围是0~24 设置为0，表示为自动	24
Patrol Scrub Address Mode (四路产品)	内存巡检地址模式设置，选项参数有： ● System Physical Address:系统物理地址 ● Reverse Address：相反地址	System Physical Address
Patrol Scrub Error Downgrade (四路产品)	将无法纠正的Patrol Scrub错误降级成为可纠正的错误，参数选项有： ● Enabled：启用 ● Disabled：禁用	Enabled

3.4.5 IIO Configuration

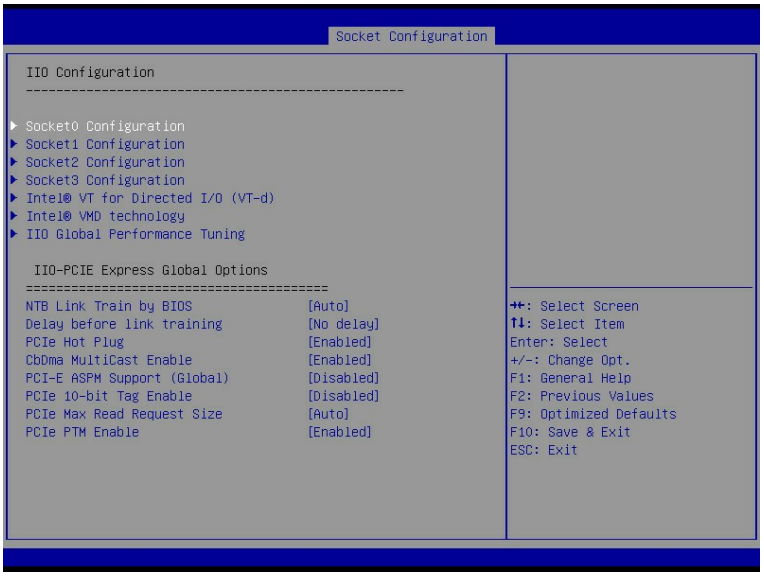
功能描述

IIO Configuration 界面是对 PCIe 插槽进行配置。

界面展示

IIO Configuration 界面如图 3-36 所示。

图 3-36 IIO Configuration 界面



参数说明

具体参数说明如表 3-31 所示。

表 3-31 IIO Configuration 界面说明表

界面参数	功能说明	默认值
Socket N Configuration	Socket N配置子菜单，用来设置CPU0的PCIE上设备的Link speed及Max Payload Size，ASPM等设置，并显示当前PCIE端口的链接状态，最大链接，当前链接速率等。	----
Intel VT for Directed I/O (VT-d)	Intel VT-d技术相关设置子菜单，Intel VT-d技术开关设置，用于提高系统的安全性和可靠性，提高I/O设备在虚拟环境中的性能。	----
Intel VMD Technology(UEFI模式显示)	Intel VMD技术相关设置子菜单，每个CPU的每个PStack上VMD的开关设置。	----
IIO Global Performance Tuning	IIO性能控制菜单	----
Retimer workaround(两路产品)	是否启用Retimer的解决方案，选项参数有： ● No：不启用 ● Yes：启用	No
NTB Link Train by BIOS	是否启用NTB链路训练，选项参数有： ● Disabled：禁用	Auto

界面参数	功能说明	默认值
	● Enabled：启用 ● Auto：自动 注： Auto根据CPU型号调整选项值。	
Delay before link training	选择训练开始前的延时，选项参数有： ● No Delay：不延时 ● 100ms ● 300ms ● 500ms ● 1s ● 2s	No delay
PCIe Hot Plug	全局PCIe热拔插开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 ● Auto(四路产品)：自动 ● Manual(四路产品)：手动 注： Auto不会打开所有的HotPlug寄存器，相当于Disabled。	Enabled
CbDma MultiCast Enable	是否开启用于验证的CbDma MultiCast，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
PCI-E ASPM Support (Global)	PCIE ASPM总开关设置，选项参数有： ● Disabled：禁用 ● Per-Port：每个port单独控制 ● L1 Only：仅L1 注： 需要PCIe设备本身也支持ASPM功能。	Disabled
PCIe 10-bit Tag Enable	启用或禁用PCIe 10位标签支持，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
PCIe Max Read Request Size	PCIe最大读取请求大小设置，选项参数有： ● Auto ● 128B ● 256B ● 512B ● 1024B	Auto

界面参数	功能说明	默认值
	● 2048B ● 4096B 注： Auto默认为最大值4096B。	
PCIe PTM Enable	PCIe PTM启用设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled(两路产品) Enabled(四路产品)

1. Intel VT for Directed I/O (VT-d)

功能描述

Intel VT for Directed I/O (VT-d)界面对 Intel VT-d 特性进行设置。

界面展示

Intel VT for Directed I/O (VT-d)界面如图 3-37 所示。

图 3-37 Intel VT for Directed I/O (VT-d)界面

参数说明

具体参数说明如表 3-32 所示。

表 3-32 Intel VT for Directed I/O (VT-d)界面说明表

界面参数	功能说明	默认值
Intel® VT for Directed I/O (VT-d)	VT-d功能开关，可以使得多个虚拟机访问同一个物理I/O，提高了虚拟机的性能，选项参数有： ● Enabled：启用 ● Disabled：禁用 注： 当Intel® VT for Directed I/O (VT-d) 选项为Enabled时显示下面选项。	Enabled(两路产品) Disabled(四路产品)
Interrupt Remapping	VT-d中断重映射开关，可为定向I/O提供中断重映射功能，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Posted Interrupt(四路产品)	VT-d中断重映射扩展功能，暂存可映射的中断请求到物理内存中，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
ATS(四路产品)	ATS功能开关，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Coherency Support(Non-Isoch)(四路产品)	非同步一致性功能开关，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled

2. Intel VMD Technology

功能描述

Intel VMD Technology 界面是对 PCIe 接口的 VMD 特性进行设置，此功能在 LEGACY 模式下不支持，仅在 UEFI 模式下显示。

界面展示

Intel VMD Technology 界面如图 3-38 所示。

图 3-38 Intel VMD Technology 界面

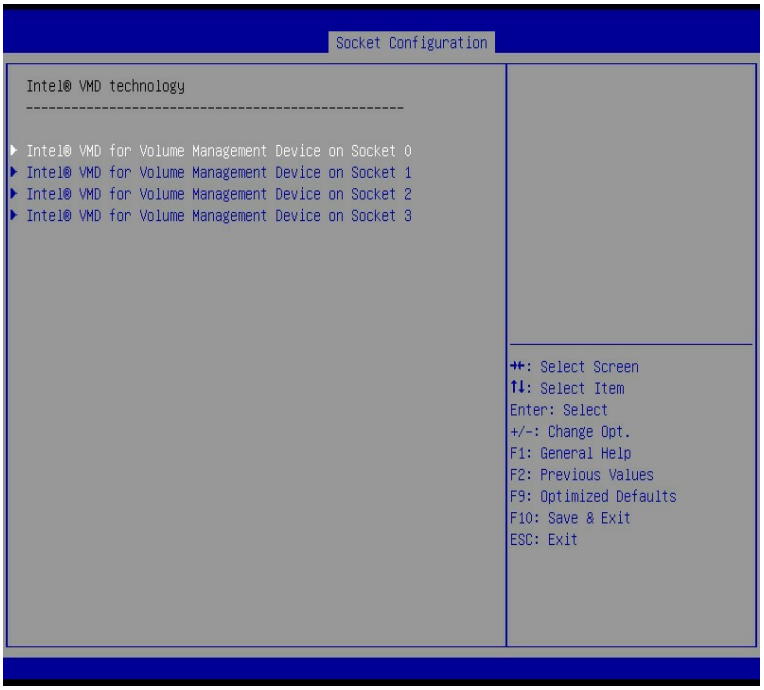
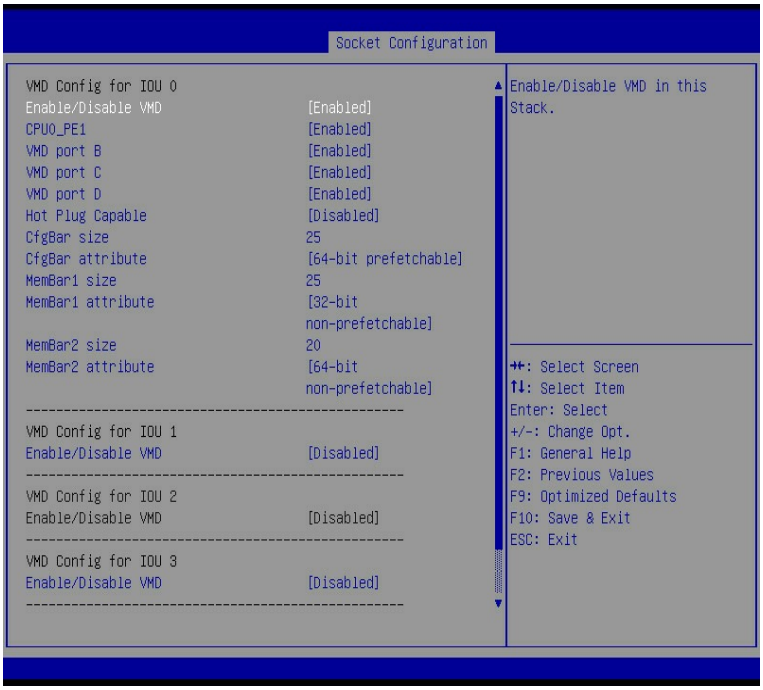


表 3-33 Intel VMD Technology 界面说明表

界面参数	功能说明	默认值
Intel® VMD for Volume Management Device on Socket n (n为CPU个数)	英特尔卷管理设备配置菜单	----

图 3-39 Intel® VMD for Volume Management Device on Socket n 界面



参数说明

具体参数说明如表 3-34 所示。

表 3-34 Intel® VMD for Volume Management Device on Socket n 界面说明表

界面参数	功能说明	默认值
Enable/Disable VMD	VMD功能开关，选项参数有： ● Enabled：启用 ● Disabled：禁用 注： 选项Enable/Disable VMD启用后，以下选项显示	Disabled
VMD port x(x=A~D,是否可选由硬件设计决定)	VMD端口x是否启用VMD特性，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Hot Plug Capable	VMD热插拔功能开关，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
CfgBar Size	VMD Bar大小，设置范围20~27	25
CfgBar attribute	VMD Bar属性，选项参数有： ● 32-bit non-prefetchable：32位不可预	64-bit prefetchable

界面参数	功能说明	默认值
	取 ● 64-bit non-prefetchable：64位不可预取 ● 64-bit prefetchable：64位可预取	
MemBar1 size	内存Bar1大小，设置范围20~39	25
MemBar1 attribute	内存Bar2属性，选项参数有： ● 32-bit non-prefetchable：32位不可预取 ● 64-bit non-prefetchable：64位不可预取 ● 64-bit prefetchable：64位可预取	32-bit non-prefetchable
MemBar2 size	内存Bar1大小，设置范围20~39	20
MemBar2 attribute	内存Bar2属性，选项参数有： ● 32-bit non-prefetchable：32位不可预取 ● 64-bit non-prefetchable：64位不可预取 ● 64-bit prefetchable：64位可预取	64-bit non-prefetchable

注意

请设置连接 NVMe 硬盘的 VMD 端口,其余 PCIe 端口的 VMD 功能不建议设置为 Enabled，可能会导致对应 PCIe 槽位上接入的设备无法识别。

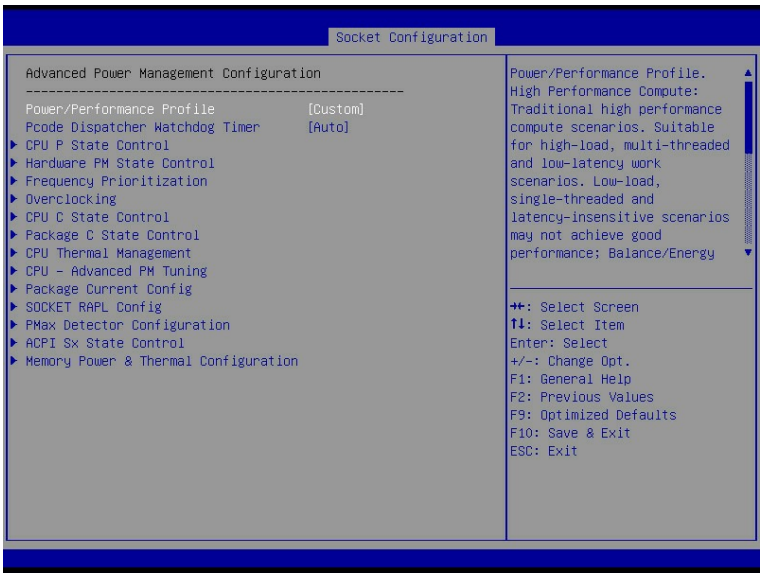
3.4.6 Advanced Power Management Configuration

功能描述

Advanced Power Management Configuration 界面是 CPU 电源管理相关选项设置，具体参数说明如表 3-35 所示，Advanced Power Management Configuration 界面如图 3-40 所示。

界面展示

图 3-40 Advanced Power Management Configuration 界面



参数说明

表 3-35 Advanced Power Management Configuration 界面说明表

界面参数	功能说明	默认值
Power/Performance Profile	节能/性能配置，选项参数有： ● High Performance Compute：最大性能 ● Balance/Energy Efficiency：平衡/能源效率 ● Power Saving：节能 ● Low Latency：低延时 ● OLTP：联机事务处理 ● Virtualization：虚拟化 ● Custom：自定义	Custom
CPU P State Control	CPU P状态控制设置子菜单	----
Hardware PM State Control	硬件电源管理状态控制子菜单	----
CPU C State Control	CPU C状态控制设置子菜单	----
Package C State Control	Package C状态控制子菜单	----
CPU-Advanced PM Tuning	CPU性能和节能调整子菜单	----
SOCKET RAPL Config	Socket RAPL配置子菜单	----

1. Power/Performance Profile

功能描述

Power/Performance Profile(能效场景功能)提供 7 种典型的能效场景，通过设置能效场景可一键完成相关 BIOS 参数设置。能效场景对应的 BIOS 设置根据基准测试结果，功能测试工具（如虚拟化场景）和客户实际应用中的一些典型案例制定。这些参数对优化典型工作场景有很好的效果，对具体真实工作场景的优化也有不错的借鉴意义。能效场景设置侧重实际应用，兼顾功能，性能，节能，稳定性，以更好满足各应用场景下的实际需求。

需要注意的是主流的基准测试，无论是 Linpack 等综合基准测试，Spec 基准测试，还是尽量模拟真实运行环境的 TPC 基准测试，都与真实具体的工作场景不同。在真实工作场景下，负载、应用不同，对性能、节能、可靠性的侧重也有不同，如果要达到最优效果，需要根据实际情况适当微调。

- High Performance Compute：传统高性能计算场景，典型应用为大规模科学计算和工程计算。特点是高负载，多线程，低延时，CPU 和内存利用率极高，IO 利用率低。该设定对低负载，单线程，延迟不敏感的场景未必能取得最好的效果。此场景下会关闭节能，以获取更高 CPU 频率和内存吞吐量。低负载场景更多需要开启节能，使 Idle 的核心进入 C6，而使工作的单核心获得更多的功耗和散热裕量，从而可以使工作核心持续保持在高频工作状态以获取更好的性能和爆发力。

- Balance/Energy Efficiency：均衡性能和节能，以取得较高的能效比。主要是在对性能影响最小的前提下开启节能以获取较高的效率。可用于大部分普通应用，有利于在保持良好性能的前提下获取好的节能效果。

- Power Saving：主要用于对能耗要求高的场合。此场景会开启绝大部分节能选项并开启最大节能状态，使得系统在 Idle 状态下功耗更低。当有负载开始运行时，从节能状态退出会有一定的时延。负载运行期间，某些部件会因为长时间没有被访问而进入节能状态，当需要访问这些部件时，部件从节能状态退出也会有一定的时延。高负载运行时，因为各部件不满足进入节能状态的条件，效果与节能关闭差异不大。

- Low Latency：用于对时延要求严苛的场景，例如实时操作系统。对于计算量大，多线程，持续时间较长的负载需要更多考虑平均计算速度，高平均计算速度的获取有时需要开启节能以使核心间协作更加协调，而不是争抢功耗和散热空间的裕量。对于突发短促的负载，需要侧重反应速度。此场景会关闭可能引入时延的节能选项和其他管理功能，并使 CPU 在 idle 状态下保持最高频率以获取更快的反应。

- OLTP：应用于在线传输业务，即联机事务处理(Online Transaction Processing)，主要以小的事务以及小的查询为主，并发量高，典型的 OLTP 系统有电子商务系统，银行，

证券等。请求-相应时间是一个重要指标，这需要快速的数据库访问速度和计算处理速度，需要平衡 CPU 的峰值速度和 Memory/IO 吞吐量。

- Virtualization：主要应用于虚拟化场景。此场景下会开启所有虚拟化功能，并设定好和虚拟化有关联的相关选项，以更好支持虚拟化。
- Custom：主要用来供用户根据具体应用场景自行定制以达到最好的效果。

用户根据不同的使用场景将 Power/Performance Profile 选项分别设置为七种不同能效场景时，相关选项参数的默认值也会有所不同。

参数说明

不同能效场景下各相应选项对应的默认值如表 3-36 和表 3-37 所示。

表 3-36 不同能效场景下相关选项参数默认值说明表

相关参数	High Performance Compute	Balance/Energy Efficiency	Power Saving
Hardware Prefetcher	Enabled	Disabled	Disabled
Adjacent Cache Prefetch	Enabled	Disabled	Disabled
DCU Streamer Prefetcher	Enabled	Disabled	Disabled
DCU IP Prefetcher	Enabled	Disabled	Disabled
Hyper-Threading [ALL]	Enabled	Enabled	Disabled
Turbo Mode	Enabled	Enabled	Disabled
SNC (Sub NUMA)(两路产品)	Enable SNC2 (2-clusters)	Enable SNC2 (2-clusters)	Disabled
SNC (Sub NUMA)(四路产品)	Enabled	Enabled	Disabled
KTI Prefetch	Enabled	Auto	Disabled
Numa	Enabled	Enabled	Enabled
Energy Efficient Turbo	Disabled	Enabled	Disabled
Page Policy	Adaptive	Adaptive	Closed
Hardware P-States	Disabled	Native Mode	Native Mode
Static Turbo Mode	Disabled	Disabled	Disabled
Patrol Scrub	Disabled	Enabled	Enabled
Enhanced Halt State (C1E)	Disabled	Enabled	Enabled
VMX	Disabled	Enabled	Enabled
Intel® VT for Directed I/O (VT-d)	Disabled	Disabled	Disabled

相关参数	High Performance Compute	Balance/Energy Efficiency	Power Saving
SpeedStep (Pstates)	Disabled	Enabled	Enabled
Enable Monitor MWAIT	Enabled	Enabled	Enabled
CPU C6 report	Disabled	Enabled	Enabled
Package C State	C0/C1 state	C6(non Retention) state	C6(Retention) state(四路产品) C6(non Retention) state(两路产品)
ENERGY_PERF_BIAS_CFG mode	Performance	Balance Performance	Power
Workload Configuration	Balanced	Balanced	Balanced
Link L0p Enable	Disabled	Enabled	Enabled
Uncore Freq Scaling (UFS)	MAX Frequency	Enabled	Min Frequecy
Power Performance Tuning	BIOS Controls EPB	BIOS Controls EPB	BIOS Controls EPB
PCI-E ASPM Support (Global)(在Socket Configuration菜单内)	Disabled	Disabled	Disabled
SR-IOV Support	-	-	-

设置 Power/Performance Profile 为 Low Latency、OLTP、Virtualization、Custom 四种场景情况下相关选项的默认值如下表所示。

表 3-37 不同能效场景下相关选项参数默认值说明表

相关参数	Low Latency	OLTP	Virtualization
Hardware Prefetcher	Enabled	Enabled	Enabled
Adjacent Cache Prefetch	Enabled	Enabled	Enabled
DCU Streamer Prefetcher	Enabled	Enabled	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled
Hyper-Threading [ALL]	Disabled	Enabled	Enabled
Turbo Mode	Enabled	Enabled	Enabled
SNC (Sub NUMA)(两路产品)	Enable SNC2 (2-clusters)	Disabled	Disabled
SNC (Sub NUMA)(四路产品)	Enabled	Disabled	Disabled

相关参数	Low Latency	OLTP	Virtualization
KTI Prefetch	Enabled	Enabled	Enabled
Numa	Enabled	Enabled	Enabled
Energy Efficient Turbo	Disabled	Disabled	Disabled
Page Policy	Adaptive	Adaptive	Adaptive
Hardware P-States	Disabled	Disabled	Disabled
Static Turbo Mode	Disabled	Disabled	Disabled
Patrol Scrub	Disabled	Enabled	Enabled
Enhanced Halt State (C1E)	Disabled	Disabled	Disabled
VMX	Disabled	Enabled	Enabled
Intel® VT for Directed I/O (VT-d)	Disabled	Disabled	Enabled
SpeedStep (Pstates)	Disabled	Enabled	Enabled
Enable Monitor MWAIT	Enabled	Enabled	Enabled
CPU C6 report	Disabled	Disabled	Disabled
Package C State	C0/C1 state	C0/C1 state	C0/C1 state
ENERGY_PERF_BIAS_CFG mode	Performance	Performance	Performance
Workload Configuration	Balanced	I/O sensitive	Balanced
Link L0p Enable	Disabled	Disabled	Disabled
Uncore Freq Scaling (UFS)	MAX Frequency	MAX Frequency	MAX Frequency
Power Performance Tuning	BIOS Controls EPB	BIOS Controls EPB	BIOS Controls EPB
PCI-E ASPM Support (Global)(在Socket Configuration菜单内)	Disabled	Disabled	Disabled
SR-IOV Support	-	-	Enabled

2. CPU P State Control

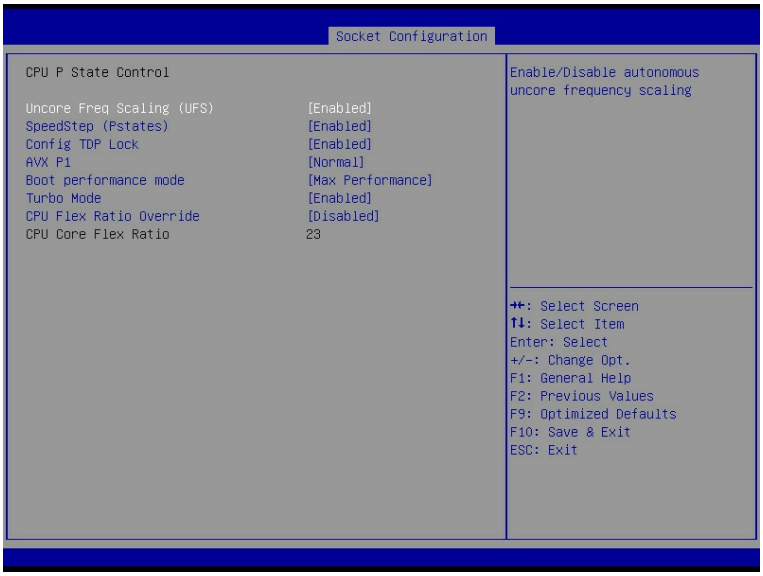
功能描述

CPU P State Control 界面是 CPU P 状态相关选项设置。

界面展示

CPU P State Control 界面如图 3-41 所示。

图 3-41 CPU P State Control 界面



参数说明

具体参数说明如表 3-38 所示。

表 3-38 CPU P State Control 界面说明表

界面参数	功能说明	默认值
Uncore Freq Scaling (UFS)	Uncore Frequency Scaling功能开关。启用UFS时，处理器可以通过内部的电压调节器，改变内部核心和非核心的电压/频率，实现功率在核心和非核心之间的最佳分配，选项参数有： ● Enabled：启用 ● Min Frequency：最小频率 ● MAX Frequency：最大频率 ● Custom：自定义 注： 该选项设置为非Enabled时，自动调节功能关闭，Uncore的频率固定。	Enabled
Uncore Frequency (Uncore Freq Scaling (UFS)选项为Custom时显示)	选择具体的Uncore扩展频率，可选范围由BIOS从CPU读取，并显示在Help信息中	16
SpeedStep (Pstates)	CPU PStates开关设置，开启后CPU进入性能模式，选项参数有：	Enabled

界面参数	功能说明	默认值
	● Enabled：启用 ● Disabled：禁用	
Config TDP Lock (四路产品，SpeedStep(Pstates)为Enabled时显示)	TDP锁的设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
AVX P1 (SpeedStep (Pstates)选项为Enabled时显示)	选择AVX P1等级，选项参数有： ● Normal：正常 ● Level 1：级别1 ● Level 2：级别2	Normal
Boot performance mode (SpeedStep (Pstates)选项为Enabled时可选)	进入OS之前BIOS的性能状态设置，选项参数有： ● Max Performance：最大性能 ● Max Efficient：最大效率 ● Set by Intel Node Manager：由英特尔节点管理器设置	Max Performance
Turbo Mode (SpeedStep (Pstates)为Enabled时显示)	动态Turbo开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
CPU Flex Ratio Override	启用CPU核心频率重写，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
CPU Core Flex Ratio (选项CPU Flex Ratio Override为Enabled时可选)	当CPU Flex Ratio Override选项Enabled时，选择要重写的CPU核心频率，步长为1，可选范围从CPU读取，动态显示在帮助信息中。	23 (CPU频率不同默认值会有所不同)
GPSS timer (两路产品)	P-State变化时的迟滞时间窗口，选项参数有： ● 0us ● 50us ● 500us	500 us

3. Hardware PM State Control

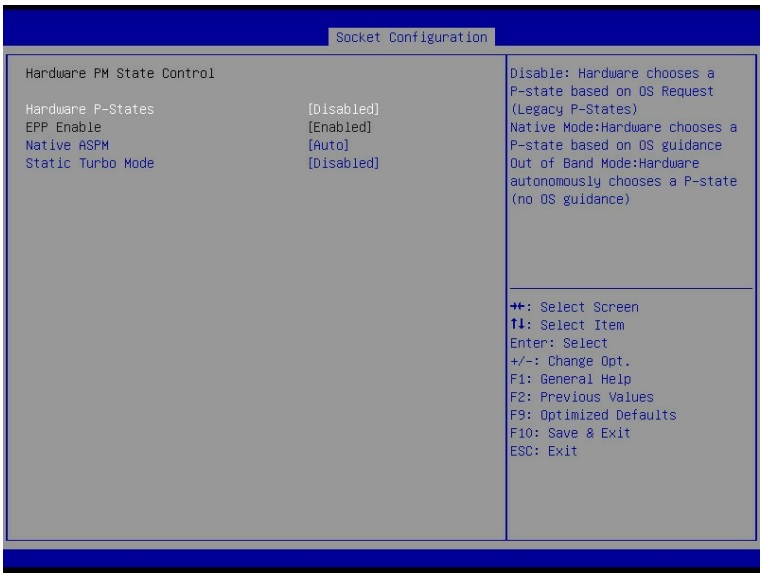
功能描述

Hardware PM State Control 界面是硬件 PM 状态相关选项设置。

界面展示

Hardware PM State Control 界面如图 3-42 所示。

图 3-42 Hardware PM State Control 界面



参数说明

具体参数说明如表 3-39 所示。

表 3-39 Hardware PM State Control 界面说明表

界面参数	功能说明	默认值
Hardware P-States	HWP功能选择开关，选项参数有： ● Disabled：关闭HWP功能 ● Native Mode： 通过OS直接访问HWPM寄存器，对CPU进行配置，该模式既支持传统ACPI表，也支持新的ACPI规范 ● Out of Band Mode： OS无法访问HWPM寄存器，只能通过BMC以带外的方式进行CPU配置 ● Native Mode with No Legacy Support： 与“Native Mode”相同，但仅支持新的ACPI规范	Disabled
EPP Enable (Hardware P-States为非Disabled时可选)	EPP使能设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled

界面参数	功能说明	默认值
Native ASPM	ASPM控制模式选择，选项参数有： ● Auto：BIOS控制ASPM ● Disabled：ASPM关闭 ● Enabled：OS控制ASPM	Auto
Static Turbo Mode	静态Turbo模式，启用后，会关闭P-State以使CPU保持在Turbo频率，选项参数有： ● Disabled：禁用 ● Enabled：启用 注： 静态Turbo模式会将CPU的频率维持在CPU当前配置中可达到的最高频率，但是会增加系统功耗。	Disabled

4. CPU C State Control

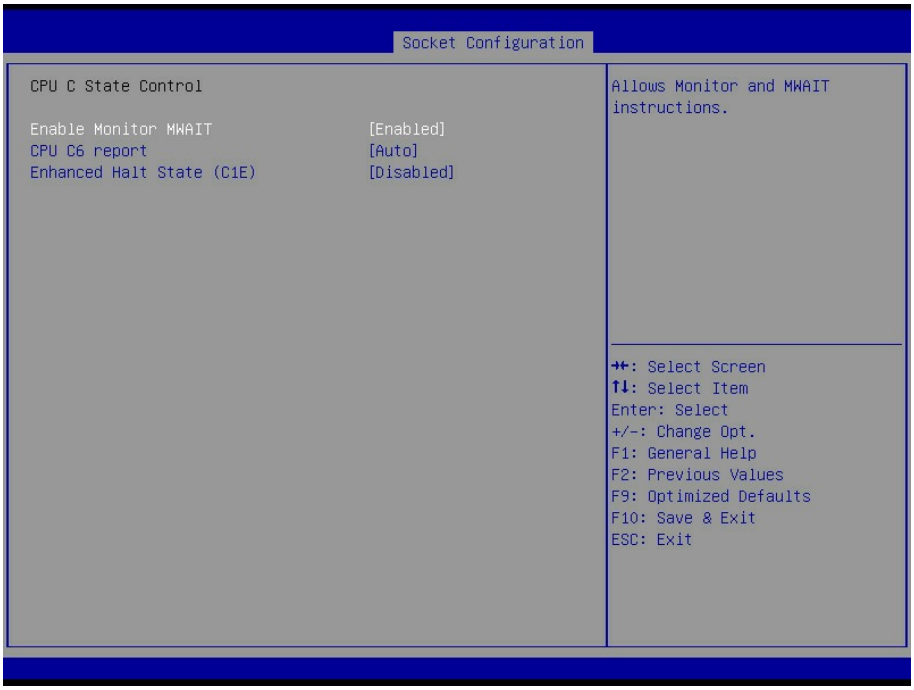
功能描述

CPU C State Control 界面是 CPU C 状态相关选项设置，用来控制 CPU 在空闲状态下的电源消耗。

界面展示

CPU C State Control 界面如图 3-43 所示。

图 3-43 CPU C State Control 界面



参数说明

具体参数说明如表 3-40 所示。

表 3-40 CPU C State Control 界面说明表

界面参数	功能说明	默认值
Enable Monitor MWAIT	Monitor Mwait支持开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
CPU C6 report	向OS报告C6状态开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 ● Auto：自动 注： Auto相当于Enabled。	Disabled
Enhanced Halt State (C1E)	C1E开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled

注意

- MWAIT/MONITOR 是 CPU 的一组指令。启用该选项后，MWAIT 指令和 MONITOR 指令配合，调度 CPU Core 进入和退出 C1、C6 等节能状态。
- 其原理是 MWAIT 指令接收一个状态值，使 CPU 进入指定的睡眠状态；在此之前，调用 MONITOR 指令，该指令接收一个内存地址，当这个内存地址的数据发生变化时，就可以将此 CPU 唤醒至 C0 状态。以此达到 idle 状态更低的能耗，工作 core 更高的工作频率。
- 根据 ACPI 规范定义，BIOS 会将 BIOS Setup 菜单中支持的 CPU C STATE 种类通过 ACPI table 的形式汇报给 OS，让 OS 可以知晓它可以调度的 C STATE 种类，但是目前看来 Windows 与 Linux 有不同的处理策略：
- Windows 系统严格遵守 ACPI 规范，客户通过调整 BIOS Setup 中 C STATE 相关选项即可控制开启和关闭各种 C STATE；
- Linux 在某些版本中可能绕过 ACPI table 中的内容，通过 idle driver 直接调度 MWAIT 指令切换 C STATE，因此针对这些版本的 Linux 系统若想开启或关闭 C STATE，需要您了解此版 Linux 系统调度 CPU C STATE 的方式后，修改相关的 BIOS Setup 选项，否则直接修改 BIOS 选项，可能达不到预期效果。
- 理论上操作系统下应用 MWAIT 指令的线程，应该会获得更好的能效比，但 C-State 越深，退出 C-State 所需的时间越长，因此某些低延迟高并发的业务场景中 CPU 可能无法进入节能状态，达不到启用 Monitor/MWAIT 的预期效果。
- 建议您根据实际的应用场景调整此选项，如在低响应延迟高并发的系统中关闭 Monitor/MWAIT；在低并发且对响应延迟要求不高的系统中开启 Monitor/MWAIT。

5. Package C State Control

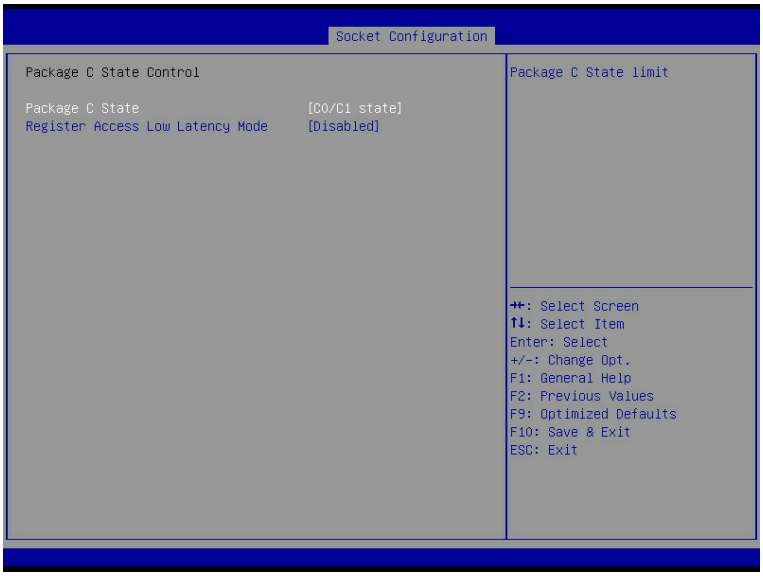
功能描述

Package C State Control 界面是 Package C 状态相关选项设置。

界面展示

Package C State Control 界面如图 3-44 所示。

图 3-44 Package C State Control 界面



参数说明

具体参数说明如表 3-41 所示。

表 3-41 Package C State Control 界面说明表

界面参数	功能说明	默认值
Package C State	Package C状态设置，选项参数有： ● C0/C1 state：C0/C1状态 ● C2 state：C2状态 ● C6(non Retention) state：C6(不保留)状态 ● C6(Retention) state(四路产品)：C6(保留)状态 ● No Limit(四路产品)：无限制 ● Auto：自动 注： Auto默认为C0/C1 state，但也会根据具体的CPU型号进行调整。	C0/C1 state
Register Access Low Latency Mode (两路产品)	使能注册访问低延时模式，选项参数有： ● Enabled：启用 ● Disabled：禁用 注： 使能这个模式之后将会组织PkgC6作为注册访问结构进入静止状态。	Disabled

6. CPU-Advanced PM Tuning

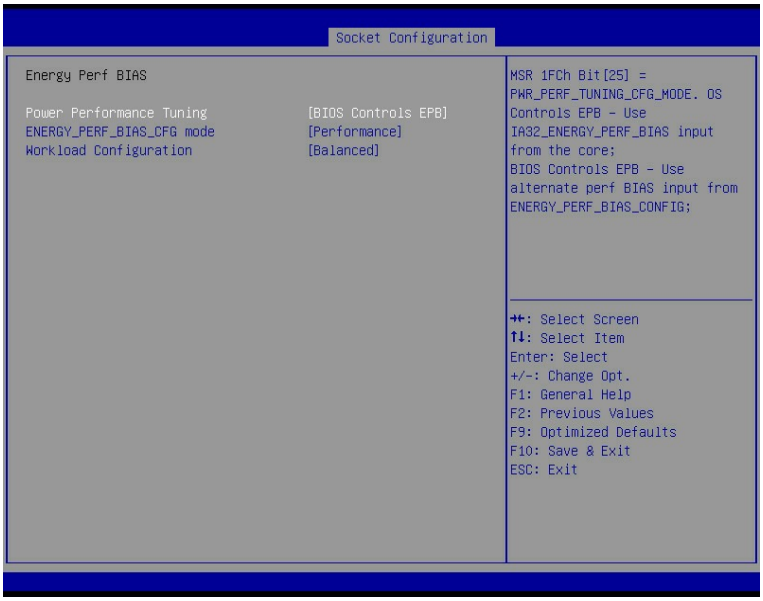
功能描述

CPU-Advanced PM Tuning 界面是 CPU 高级电源管理相关选项设置，下设 Energy Perf BIAS 菜单。

界面展示

Energy Perf BIAS 界面如图 3-45 所示。

图 3-45 Energy Perf BIAS 界面



参数说明

具体参数说明如表 3-42 所示。

表 3-42 Energy Perf BIAS 界面说明表

界面参数	功能说明	默认值
Power Performance Tuning	电源性能调整设置，选项参数有： ● OS Controls EPB：OS控制电源性能 ● BIOS Controls EPB：BIOS控制电源性能 ● PECI Controls EPB (两路产品)：PECI控制电源性能	BIOS Controls EPB

界面参数	功能说明	默认值
ENERGY_PERF_BIAS_CFG mode (Power Performance Tuning选项为BIOS Controls EPB时可选)	电源性能调优配置。CPU根据该设置来调节处理器的内部运行，满足高性能或是节能的需求。这个设置只有能效调整设置为BIOS控制能效策略时才可用，选择任何一个都会覆盖OS下对CPU性能调整的配置。选项参数有： ● Performance：性能 ● Balanced Performance：均衡性能 ● Balanced Power：均衡节能 ● Power：节能	Performance
Workload Configuration	对工作负载特性优化设置，选项参数有： ● Balanced：平衡 ● I/O Sensitive：I/O敏感	Balanced

7. SOCKET RAPL Config

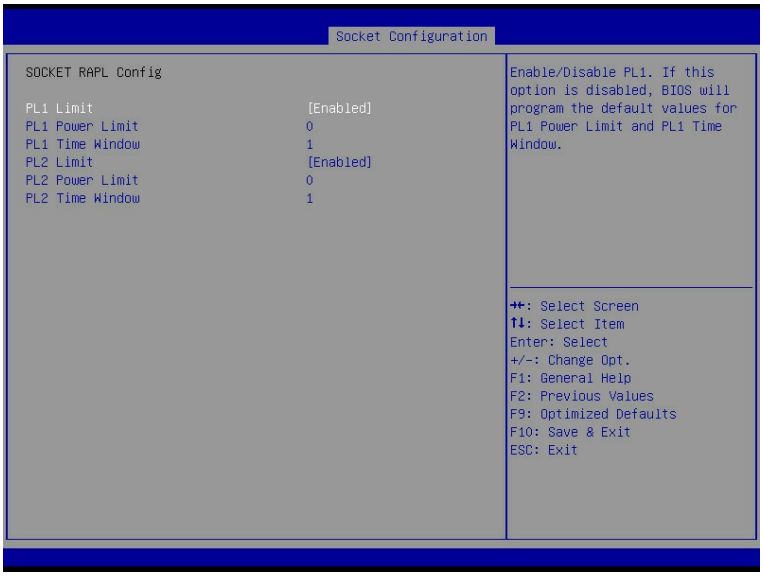
功能描述

SOCKET RAPL Config 界面是处理器 RAPL 配置相关选项设置。

界面展示

Energy Perf BIAS 界面如图 3-46 所示。

图 3-46 SOCKET RAPL Config 界面



参数说明

具体参数说明如表 3-43 所示。

表 3-43 SOCKET RAPL Config 界面说明表

界面参数	功能说明	默认值
PL1 Limit	PL1限制的开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
PL1 Power Limit (PL1 Limit为Disabled时隐藏)	PL1功率限制设置，单位为瓦特，取值范围为0到Fused Value，如果该值为0，则会取Fused Value作为此时的功率，若该值大于Fused Value，同样会取Fused Value作为此时的功率，Fused Value为固化在芯片中的最高功率。	0
PL1 Time Window (PL1 Limit为Disabled时隐藏)	PL1时窗设置，单位为秒，设置范围0~56	1
PL2 Limit (PL1 Limit为Disabled时隐藏)	PL2限制的开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
PL2 Power Limit	PL2功率限制设置，单位为瓦特，该值可从0到Fused Value，如果该值为0，则会取125%*Fused Value作为此时的功率。	0
PL2 Time Window	PL2时窗设置，单位为秒，设置范围0~56	1

3.5 Sever Mgmt

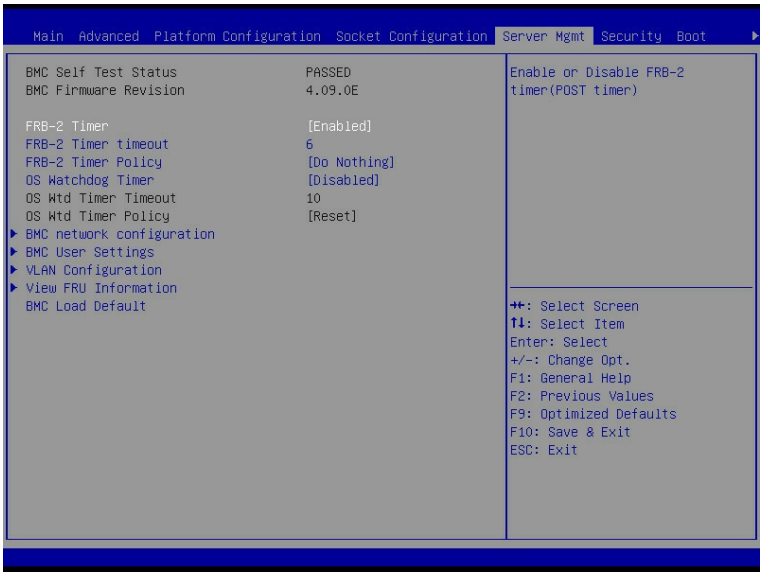
功能描述

Server Mgmt 界面是服务器管理相关选项设置，包含看门狗、BMC 网络设置、BMC 用户设置等。

界面展示

Server Mgmt 界面如图 3-47 所示。

图 3-47 Server Mgmt 界面



参数说明

具体参数说明如表 3-44 所示。

表 3-44 Server Mgmt 界面说明表

界面参数	功能说明	默认值
BMC Self Test Status	BMC自检状态	----
BMC Firmware Revision	当前主板BMC固件版本号	----
FRB-2 Timer	FRB-2时钟开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
FRB-2 Timer Timeout	FRB-2时钟超时时间设置，选项参数有： 3-30min	20(两路机型); 30(四路机型)
FRB-2 Timer policy	FRB-2时钟超时后的策略设置，选项参数有： ● Do Nothing：无动作 ● Reset：重启 ● Power Down：关机 ● Power Cycle：关机并重新开机	Do Nothing
OS Watchdog Timer	OS看门狗时钟开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled

界面参数	功能说明	默认值
OS Wtd Timer Timeout	OS 看门狗时钟超时时间设置，选项参数有： 3-30min	10
OS Wtd Timer policy	OS看门狗时钟超时后的策略设置，选项参数有： ● Do Nothing：无动作 ● Reset：重启 ● Power Down：关机 ● Power Cycle：关机并重新开机	Reset
BMC network Configuration	BMC网络配置子菜单	----
BMC User Settings	BMC用户设置子菜单	----
VLAN Configuration	VLAN配置子菜单	----
View FRU information	查看FRU信息子菜单	----
BMC Load Default	BMC恢复默认值	----

3.5.1 BMC network configuration

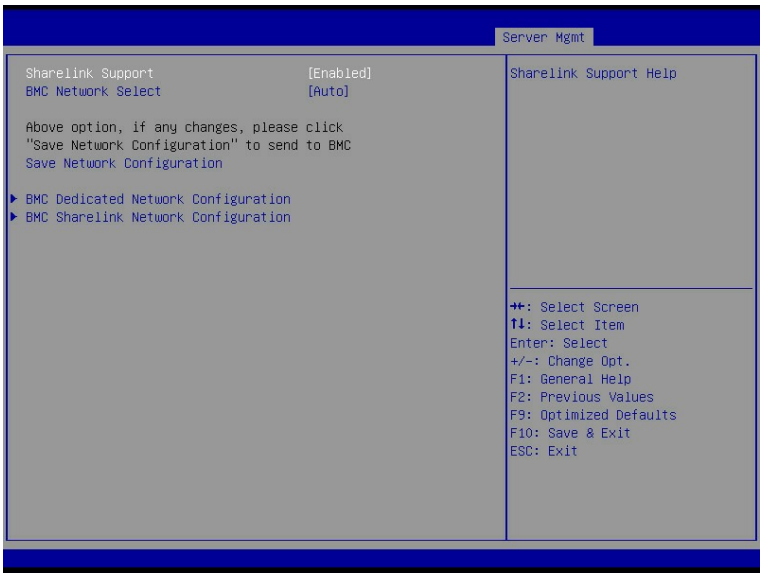
功能描述

BMC network configuration 界面是通过 BIOS 对 BMC 管理网络进行配置。

界面展示

BMC network configuration 界面如图 3-48 所示。

图 3-48 BMC network configuration 界面



参数说明

具体参数说明如表 3-45 所示。

表 3-45 BMC network configuration 界面说明表

界面参数	功能说明	默认值
Sharelink Support	BMC Sharelink网络开关设置，每次开机从BMC读取，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
BMC Network Select	配置BMC网络，选项参数有： ● Auto：自动 ● Manual：手动	Auto
Auto Failover Nic Count(BMC Network Select选项 Manual时显示)	1 仅专用或NCIS支持远程管理 2 专用和一个NCIS支持远程管理	1
BMC Network Type(BMC Network Select选项 Manual时显示)	BMC网络类型，选项参数有： ● MGMT：MGMT管理网口 ● OCP：OCP网口 ● PCIE：PCIE网口	MGMT
BMC Dedicated Network Configuration	BMC专用网络参数设置	----
BMC Sharelink Network Configuration	BMC复用网络参数设置	----

1. BMC Dedicated Network Configuration

功能描述

BMC Dedicated Network Configuration 界面是通过 BIOS 对 BMC 专用网络进行配置。

界面展示

BMC Dedicated Network Configuration 界面如图 3-49 和图 3-50 所示。

图 3-49 BMC Dedicated Network Configuration 界面

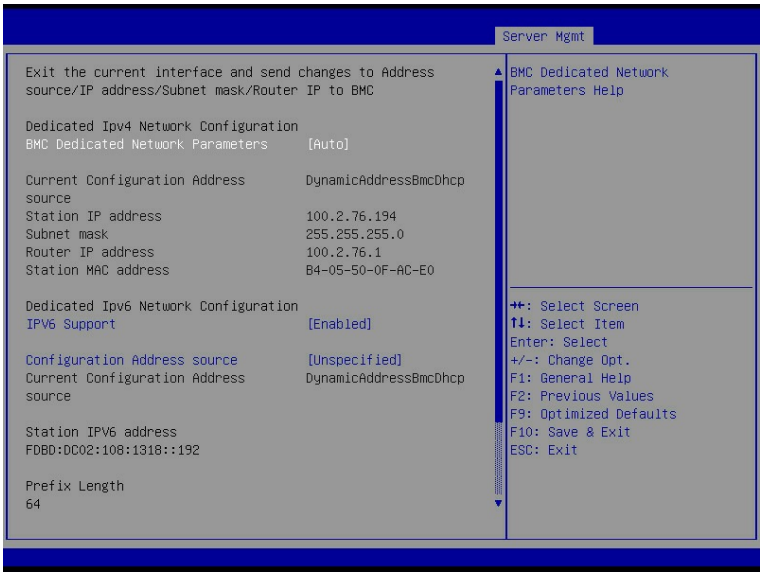
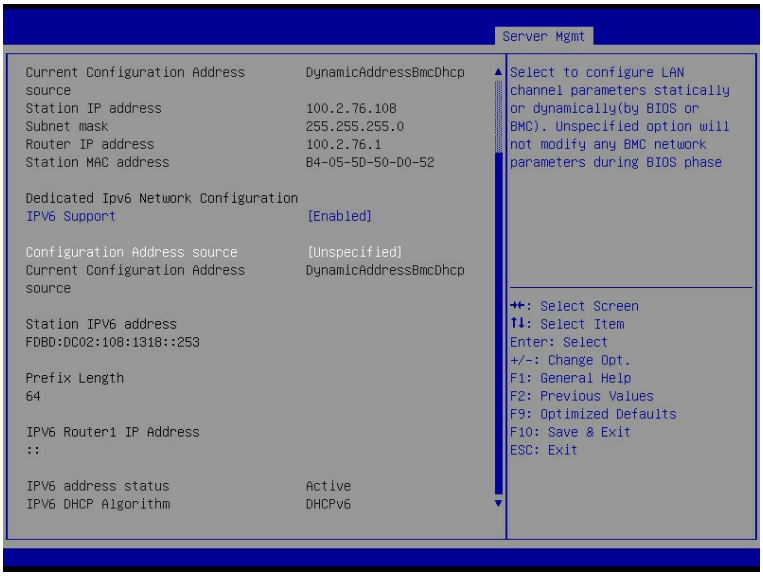


图 3-50 BMC Dedicated Network Configuration 界面



参数说明

具体参数说明如表 3-46 所示。

表 3-46 BMC Dedicated Network Configuration 界面说明表

界面参数	功能说明	默认值
BMC Dedicated Network Parameters	获取BMC专口管理网口参数的方式置，选项参数有：	Auto

界面参数	功能说明	默认值
	● Auto：自动获取当前BMC网络设置 ● Manual：手动设置BMC网络	
Address source(BMC Dedicated Network Parameters为Manual时显示)	配置BMC网络状态，选项参数有： ● Unspecified：将不修改BMC网络参数 ● Static：设定静态BMC网络参数 ● DynamicBmcDhcp:动态获取BMC网络参数	Unspecified
Current Configuration Address source	当前BMC配置地址状态	----
Station IP address	端口的IP地址	----
Subnet mask	子网掩码	----
Router IP address	路由IP地址	----
CMC0 IP address (多节点服务器有此IP，如I48M6)	从BMC获取的CMC IP0地址	----
CMC1 IP address (多节点服务器有此IP，如I48M6)	从BMC获取的CMC IP1地址	----
Station MAC address	端口的MAC地址	----
IPV6 Support	是否支持IPV6，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Configuration Address Source	配置BMC网络状态，选项参数有： ● Unspecified：将不修改BMC网络参数 ● Static：设定静态BMC网络参数 ● DynamicBmcDhcp:动态获取BMC网络参数 注： 参数设置成功后立即生效。	Unspecified
Current Configuration Address source	当前BMC配置地址状态	----
Station IPv6 address	端口的IPv6地址	----
Prefix Length	前缀长度	----
IPV6 Router1 IP Address	IPV6路由IP1地址	----
IPV6 address status	IPV6地址状态	----
IPV6 DHCP Algorithm	IPV6 DHCP算法	

2. BMC Sharelink Network Configuration

功能描述

BMC Sharelink Network Configuration 界面是通过 BIOS 对 BMC 管理网络进行配置。

界面展示

BMC Sharelink Network Configuration 界面如图 3-51 和图 3-52 所示。

图 3-51 BMC Sharelink Network Configuration 界面

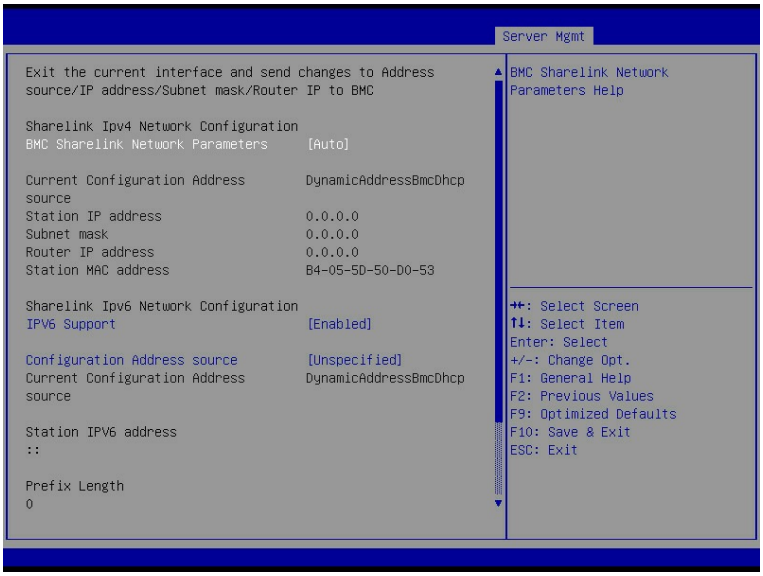
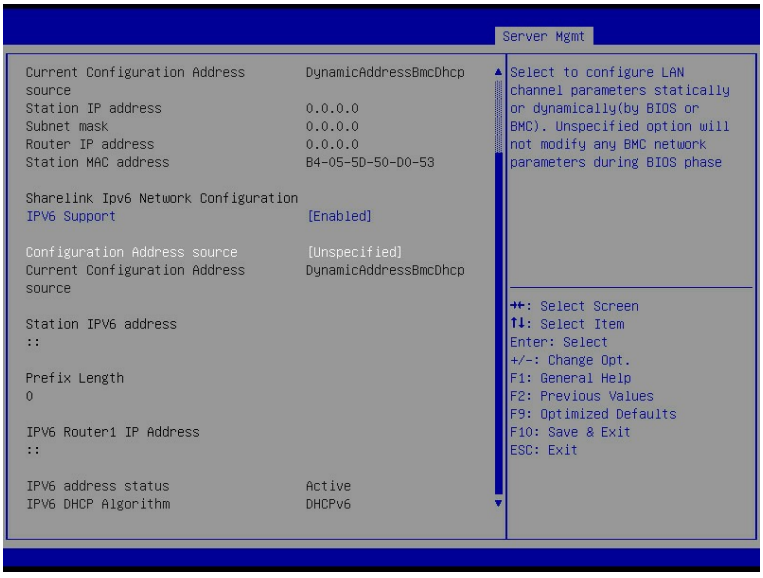


图 3-52 BMC Sharelink Network Configuration 界面



参数说明

具体参数说明如表 3-47 所示。

表 3-47 BMC Sharelink Network Configuration 界面说明表

界面参数	功能说明	默认值
BMC Sharelink Network Parameters	获取BMC共享口管理网口参数的方式设置，选项参数有： ● Auto：自动获取当前BMC网络设置 ● Manual：手动设置BMC网络	Auto
Address Source(BMC Sharelink Network Parameters为Manual时显示)	配置BMC网络状态，选项参数有： ● Unspecified：将不修改BMC网络参数 ● Static：设定静态BMC网络参数 ● DynamicBmcDhcp：动态获取BMC网络参数	Unspecified
Current Configuration Address source	当前BMC配置地址状态	----
Station IP address	端口的IP地址	----
Subnet mask	子网掩码	----
Router IP address	路由IP地址	
Station MAC address	端口的MAC地址	
IPV6 Support	是否支持IPV6，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Configuration Address source	配置BMC网络状态，选项参数有： ● Unspecified：将不修改BMC网络参数 ● Static：设定静态BMC网络参数 ● DynamicBmcDhcp：动态获取BMC网络参数	Unspecified
Current Configuration Address source	当前BMC配置地址状态	
Station IPv6 address	端口的IPv6地址	
Prefix Length	前缀长度	
IPV6 Router1 IP Address	IPV6路由IP1地址	
IPV6 address status	IPV6地址状态	
IPV6 DHCP Algorithm	IPV6 DHCP算法	

3.5.2 BMC User Settings

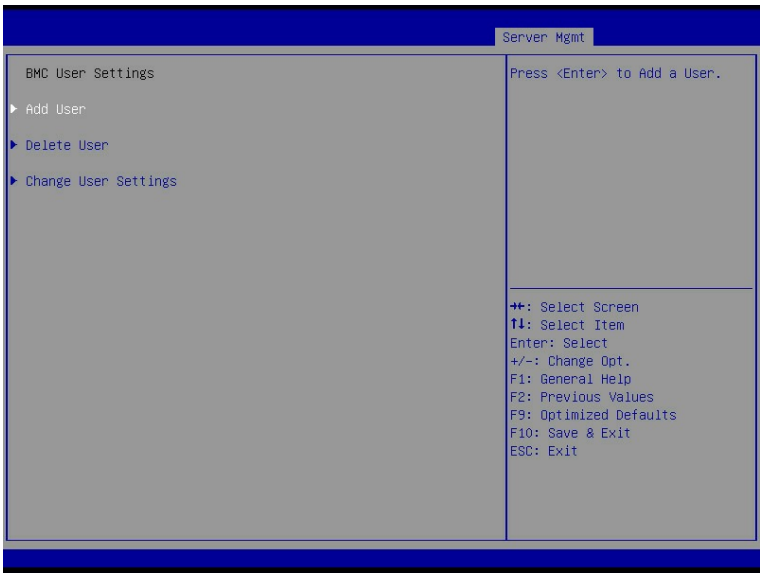
功能描述

BMC User Settings 界面是通过 BIOS 对 BMC 用户进行配置。

界面展示

BMC User Settings 界面如图 3-53 所示。

图 3-53 BMC User Settings 界面



参数说明

具体参数说明如表 3-48 所示。

表 3-48 BMC User Settings 界面说明表

界面参数	功能说明
Add User	增加BMC用户子菜单
Delete User	删除BMC用户子菜单
Change User Settings	修改BMC用户设置子菜单

1. Add User

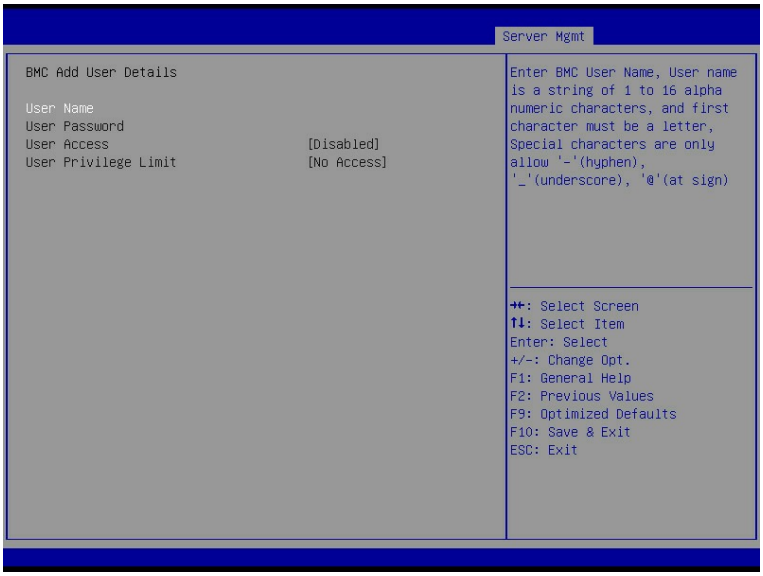
功能描述

Add User 界面是通过 BIOS 增加 BMC 用户，添加完成，将会立即生效，用户会被添加到 BMC 用户列表中。

界面展示

Add User 界面如图 3-54 所示。

图 3-54 Add User 界面



参数说明

具体参数说明如表 3-49 所示。

表 3-49 Add User 界面说明表

界面参数	功能说明	默认值
User Name	用户名称设置，用户名为字母数字字符，且首字符必须是字母，特殊字符只允许’_’、’-’、’@’，最大支持16字符	----
User Password	用户密码设置，密码必须包含大小写字母，特殊字符及数字，启用BMC密码复杂度后，密码复杂度由BMC指定。设置成功后提示“Added User successfully”	----
User Access	用户权限开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled

界面参数	功能说明	默认值
User Privilege Limit	用户权限设置，选项参数有： ● No Access：没有权限 ● User：用户 ● Operator：操作 ● Administrator：管理员 设置成功后，会提示“Set User Access Command Passed”，BMC User立即生效	No Access

2. Delete User

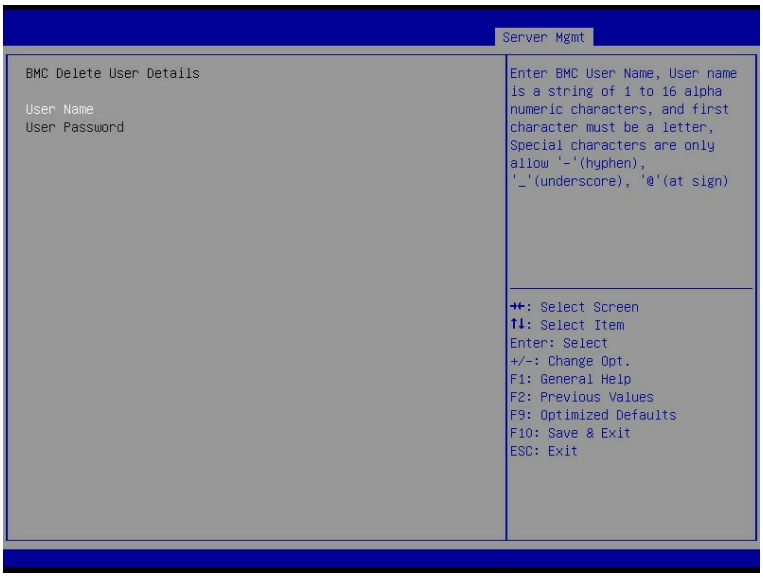
功能描述

Delete User 界面是通过 BIOS 删除 BMC 用户，删除成功后会立即生效，该用户将无法登陆 BMC Web 界面。

界面展示

Delete User 界面如图 3-55 所示。

图 3-55 Delete User 界面



参数说明

具体参数说明如表 3-50 所示。

表 3-50 Delete User 界面说明表

界面参数	功能说明
User Name	输入要删除用户名称
User Password	输入要删除用户密码，输入密码正确后，会弹出提示“User Deleted!!!”，删除成功的用户将立即在BMC中生效，该用户将无法再登录BMC Web界面

3. Change User Settings

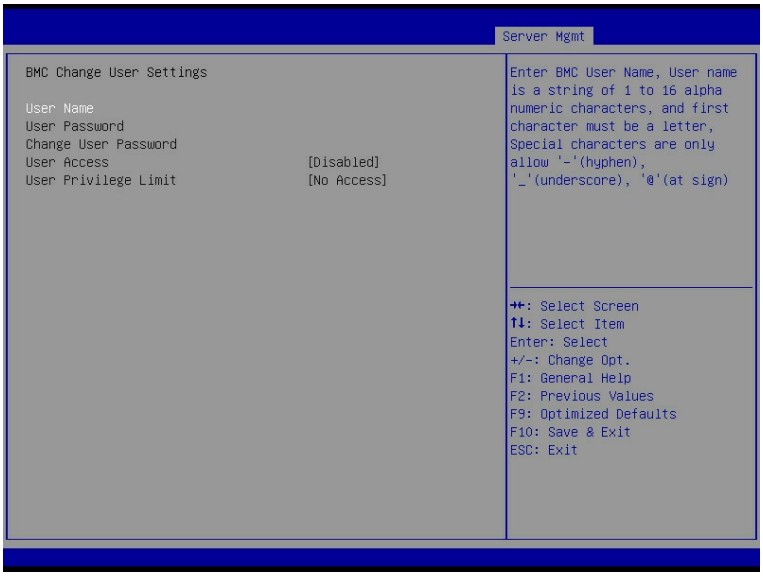
功能描述

Change User Settings 界面是通过 BIOS 修改 BMC 用户设置。

界面展示

Change User Settings 界面如图 3-56 所示。

图 3-56 Change User Settings 界面



参数说明

具体参数说明如表 3-51 所示。

表 3-51 Change User Settings 界面说明表

界面参数	功能说明	默认值

界面参数	功能说明	默认值
User Name	输入要修改用户名称	----
User Password	输入要修改用户密码，只有名称和密码输入确，下面选项才可以修改	----
Change User Password	修改用户密码，密码必须包含大小写字母，特殊字符及数字，启用BMC密码复杂度后，密码复杂度由BMC指定	----
User Access	用户权限开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
User Privilege Limit	修改用户权限设置，选项参数有： ● No Access：没有权限 ● User：用户 ● Operator：操作 ● Administrator：管理员	No Access

注意

BMC 对 BMC 默认管理员账号有保护，BIOS 无法删除和修改 BMC 默认管理员账号。

3.5.3 VLAN Configuration

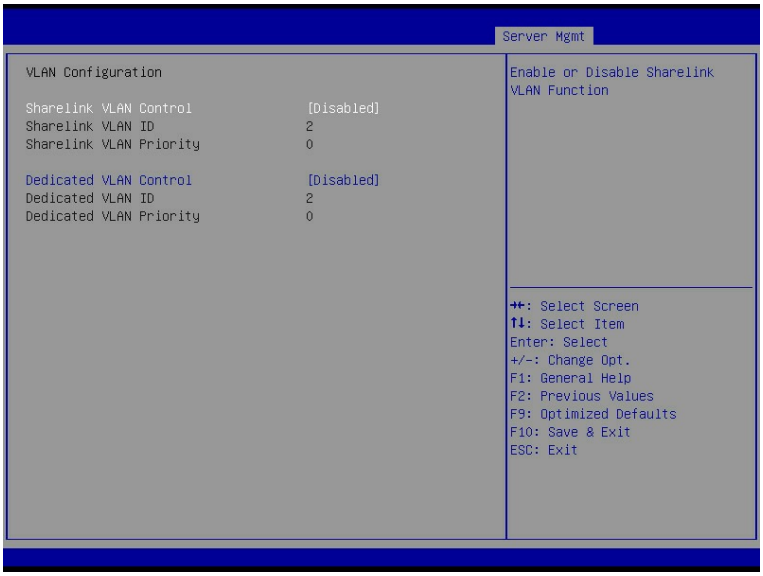
功能描述

VLAN Configuration 界面 BIOS 设置 BMC VLAN 网络参数。

界面展示

VLAN Configuration 界面如图 3-57 所示。

图 3-57 VLAN Configuration 界面



参数说明

具体参数说明如表 3-52 所示。

表 3-52 VLAN Configuration 界面说明表

界面参数	功能说明	默认值
Sharelink/Dedicated VLAN Control	BMC共享口/专口的VLAN控制开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 如果启用VLAN，需要设置VLAN ID才能设置VLAN可用	Disabled
Sharelink/Dedicated VLAN ID (Sharelink/Dedicated VLAN Control选项为Enabled时可选)	BMC共享口/专口的VLAN ID设置，范围2~4094 设置完VLAN ID后，立即生效	2
Sharelink/Dedicated VLAN Priority (Sharelink/Dedicated VLAN Control选项为Enabled时可选)	BMC共享口/专口的VLAN优先级设置，范围0~7 设置完VLAN Priority后，立即生效	0

3.5.4 View FRU information

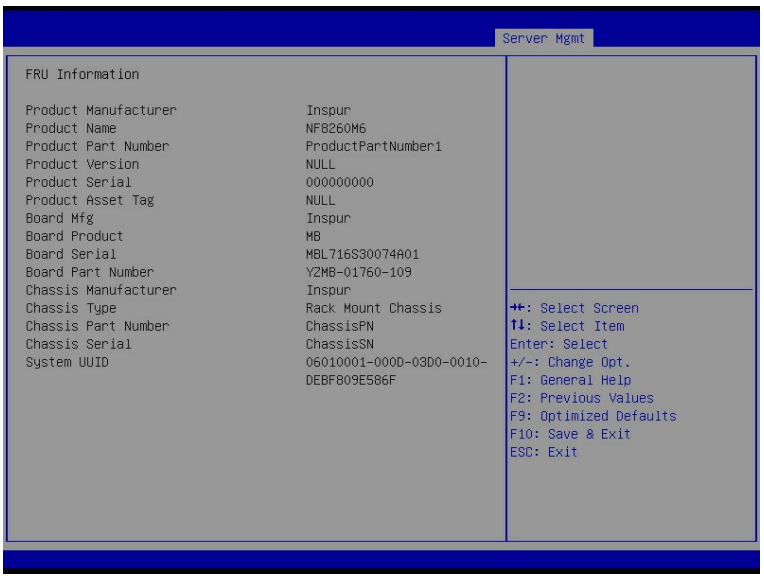
功能描述

View FRU information 显示 BIOS 读取的 BMC FRU 的信息，每次重启系统 BIOS 会和 BMC 交互，保持 FRU 信息的同步更新。

界面展示

View FRU information 显示界面如图 3-58 所示。

图 3-58 View FRU information 界面



参数说明

具体参数说明如表 3-53 所示。

表 3-53 View FRU information 界面说明表

界面参数	功能说明	默认值
Product Manufacturer	产品制造商	----
Product Name	产品名称	----
Product Part Number	产品料号	----
Product Version	产品版本	----
Product Serial	产品序列号	----
Product Asset Tag	产品资产编码	----
Board Mfg	主板制造商	----

界面参数	功能说明	默认值
Board Product	主板名称	----
Board Serial	主板序列号	----
Board Part Number	主板料号	----
Chassis Manufacturer	机箱制造商	----
Chassis Type	机箱类型	----
Chassis Part Number	机箱料号	----
System UUID	系统UUID	----

3.6 Security

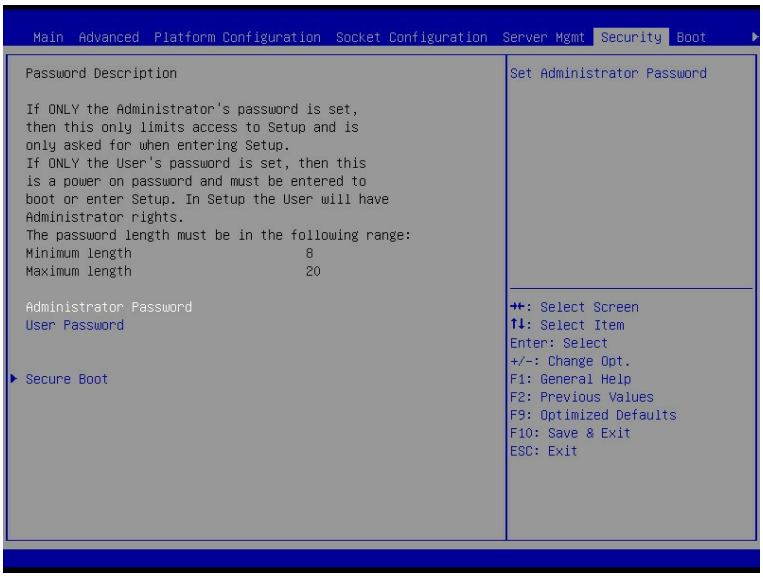
功能描述

Security 界面是管理员及用户密码设置。

界面展示

Security 界面如图 3-59 所示。

图 3-59 Security 界面



参数说明

具体参数说明如表 3-54 所示。

表 3-54 Security 界面说明表

界面参数	功能说明	默认值
Administrator Password	创建BIOS管理员密码，输入密码字符必须包含大小写字母，特殊字符及数字，最少8个字符，最大20个字符	----
User Password	创建BIOS普通用户密码，输入密码字符必须包含大小写字母，特殊字符及数字，最少8个字符，最大20个字符	----
Secure Boot	安全启动菜单	----

注意

- BIOS 密码包括管理员（Administrator）密码和用户（User）密码。建议用户首次登陆 BIOS Setup 时配置管理员密码，增加 BIOS Setup 的安全性。
- 当仅设置了管理员密码，将仅会限制进入 BIOS Setup，只有在进入 Setup 时才会要求输入管理员密码。
- 当仅设置了用户密码，这将是一个开机密码，在进入 Setup 或者 Boot 时都要输入用户密码，并且进入 Setup 之后，将使用管理员权限。
- 当设置了管理员密码和用户密码后，使用管理员密码登录 BIOS Setup，则获得管理员权限。管理员权限具有全部 BIOS 管理权限，可以设置和修改管理员密码和用户密码。
- 当设置了管理员密码和用户密码后，使用用户密码登录 BIOS Setup，则获得用户权限。用户权限只有查看各个菜单选项、设置/修改用户密码和保存退出的权限。
- 若开机或进入 Setup 时密码输入三次不正确，则无法继续输入，需要重新启动服务器。
- 若要清除密码，则登录 BIOS Setup 后，选择要清除的管理员或用户密码菜单，此时弹窗要求输入当前密码：“Enter Current Administrator/User Password”。输入完成后，弹窗要求输入新的密码：“Create New Administrator/User Password”，此时保证密码为空，直接按 Enter 键，则会弹窗提示是否要清除旧的密码：“Clear Old Administrator/User Password?”，选择 Yes，密码清除成功。
- 若忘记密码，无法登录 BIOS Setup 清除密码，则需要通过主板上的跳线清除密码。具体方法为：关机，将主板上的 Clear Password 跳线连接为 2-3 pin，然后开机进入 Setup。若不再提示需要输入密码，则密码清除成功。
- 除上述清除密码的方式外，刷新 BIOS 和清除 CMOS，密码都不会丢失。

3.6.1 Secure Boot

功能描述

Secure boot 界面用于配置安全启动功能。

界面展示

Security 界面如图 3-60 所示。

图 3-60 Secure Boot 界面

参数说明

具体参数说明如表 3-55 所示。

表 3-55 Secure Boot 界面说明表

界面参数	功能说明	默认值
Secure Boot	如果启用该功能，则安全启动功能处于活动状态。如果已注册平台密钥（Platform key，PK），并且系统处于用户模式，更改模式需要平台重置。选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Secure Boot Mode	安全启动模式选择器：标准或自定义。选项参数有： ● Custom：自定义模式 ● Standard：标准模式 注： 自定义模式：在自定义模式下多种指令可以灵活使用。在自定义模式下更新PK、KEK变量不需要原始PK签署，且更新Image signature database	Custom

界面参数	功能说明	默认值
	(db/dbx)或Authorized Timestamp Database (dbt)也不需要PK或KEK的签署 标准模式：是UEFI规范描述的默认模式	
Restore Factory Keys	强制系统进入用户模式。安装出厂默认的安全启动密钥数据库，选项参数有： ● Yes：是 ● No：否	Yes
Reset To Setup Mode	从NVRAM删除所有安全启动密钥数据库，选项参数有： ● Yes：是 ● No：否	No
Enter Audit Mode	进入审核模式工作流程。从用户到审核模式的转换将导致PK变量的删除	----
Key Management	对安全启动的密钥进行管理,包括密钥的查看，添加，删除，授权和恢复出厂设置等操作	----

注意

- 平台密钥（Platform key，PK）在平台的所有者和平台固件之间建立信任关系，平台所有者将密钥的一半注册到平台固件中。
- 安全启动共有 4 种模式，Setup Mode、User Mode、Audit Mode、Deployed Mode。
- 当未注册 PK 时，安全启动在 Setup Mode 模式下运行，在修改 PK、KEK、DB 和 DBX 变量时 BIOS 无需认证，此时通过编写 PK、KEK、DB 和 DBX 变量来配置安全引策略。BIOS 可工作在 Setup Mode 和 Audit Mode 模式，且从 Setup Mode 模式可以直接修改为 Audit Mode。
- 当注册了 PK 后，且 BIOS 在 User Mode 模式下运行时，User Mode 模式要求所有可执行文件在运行之前都要经过认证。此时 BIOS 可工作在 User Mode 和 Deployed Mode 模式下，且从 User Mode 模式可以直接修改为 Deployed Mode。
- Audit Mode 是 Setup Mode 的一种延伸，Deployed Mode 是 User Mode 的一种延伸。Audit Mode 和 User Mode 都可以直接转换到 Deployed Mode，但 Deployed Mode 转换到其他安全模式需要删除 PK 或者是特定安全转换方法。

3.7 Boot

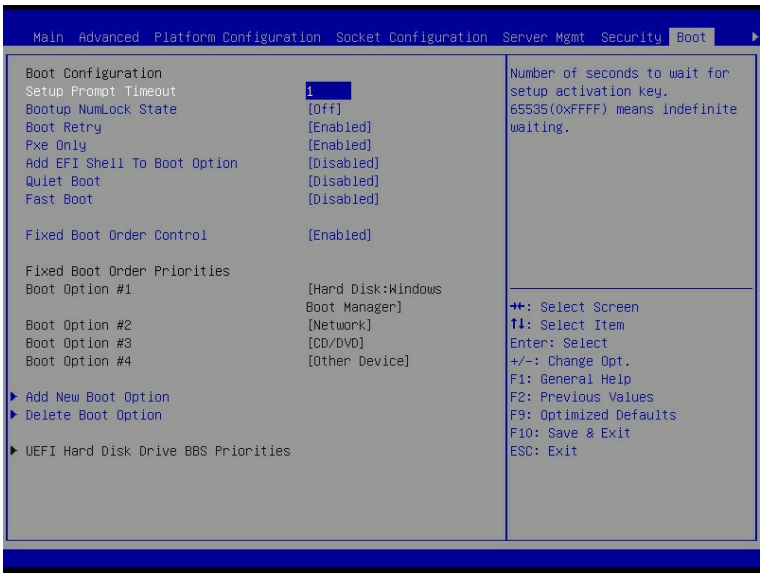
功能描述

Boot 界面是相关启动项设置，含启动方式设置、启动顺序设置及启动过程设置等。

界面展示

Boot 界面如图 3-61 所示。

图 3-61 Boot 配置界面



参数说明

具体参数说明如表 3-56 所示。

表 3-56 Boot 配置界面说明表

界面参数	功能说明	默认值
Setup Prompt Timeout	Setup提示超时设置，设置等待Setup激活键的时间，最大值为65535秒	1
Bootup NumLock State	开机启动过程中键盘Numlock指示灯状态开关设置，选项参数有： ● On：开 ● Off：关	Off
Boot Retry	设备轮询开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Pxe Only	启用或禁用仅Pxe引导重试功能，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled

界面参数	功能说明	默认值
Add EFI Shell To Boot Option	增加EFI Shell到启动选项的开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Quiet Boot	安静模式启动开关设置，选项参数有： ● Enabled：启用 ● Disabled：禁用 设置为Enabled，开机Logo显示为制造商设置的Logo，设置Disabled，开机画面为文本模式Post界面。	Disabled
Fast Boot	使用活动启动选项所需的最少设备来初始化启用或禁用引导，对于BBS引导选项无效，选项参数有： ● Enabled：启用 ● Disabled：禁用	Disabled
Fixed Boot Order Control	当该选项禁用时，用户可手动更改设备的启动顺序，选项参数有： ● Enabled：启用 ● Disabled：禁用	Enabled
Fixed Boot Order Priorities Boot Option #X	启动项优先级设置	----
Add New boot Option	添加新启动项	
Delete Boot Option	删除启动项	
XXXX BBS Priorities	XXXX设备BBS优先级设置	----

3.7.1 Add New boot Option

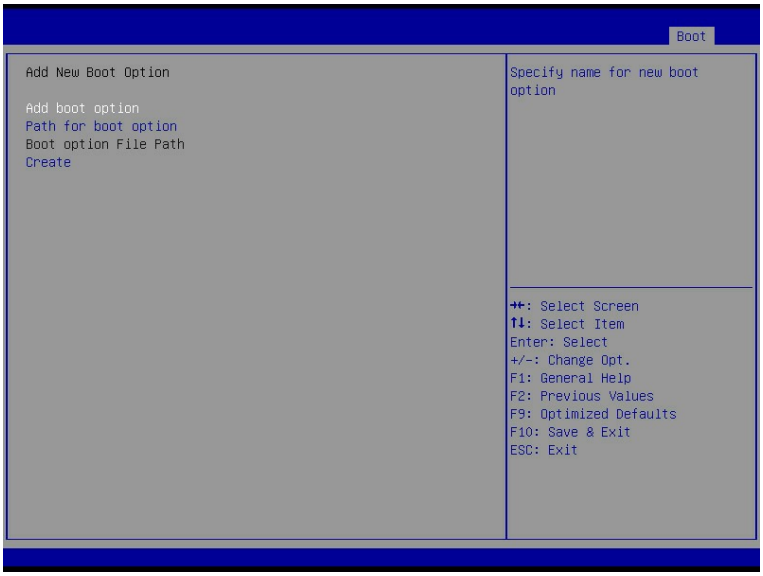
功能描述

Add New boot Option 界面是添加引导项界面。

界面展示

Boot 界面如图 3-62 所示。

图 3-62 Add New boot Option 界面



参数说明

具体参数说明如表 3-57 所示。

表 3-57 Add New boot Option 界面说明表

界面参数	功能说明	默认值
Add boot option	指定新启动选项的名称	----
Path for boot option	以格式输入引导选项的路径 fsx:\path\filename.efi	----
Boot option file Path	新创建的引导选项的文件路径	----
Create	创建新形成的引导选项	----

3.7.2 Delete Boot Option

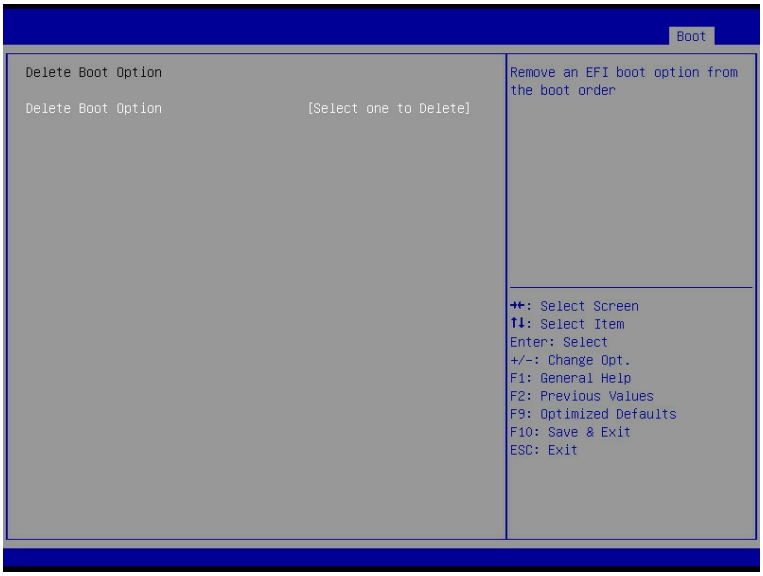
功能描述

Delete Boot Option 界面是删除引导项界面。

界面展示

Boot 界面如图 3-63 所示。

图 3-63 Delete Boot Option 界面



参数说明

具体参数说明如表 3-58 所示。

表 3-58 Delete Boot Option 界面说明表

界面参数	功能说明	默认值
Delete Boot Option	从引导顺序中删除EFI引导选项	----

3.8 Save & Exit

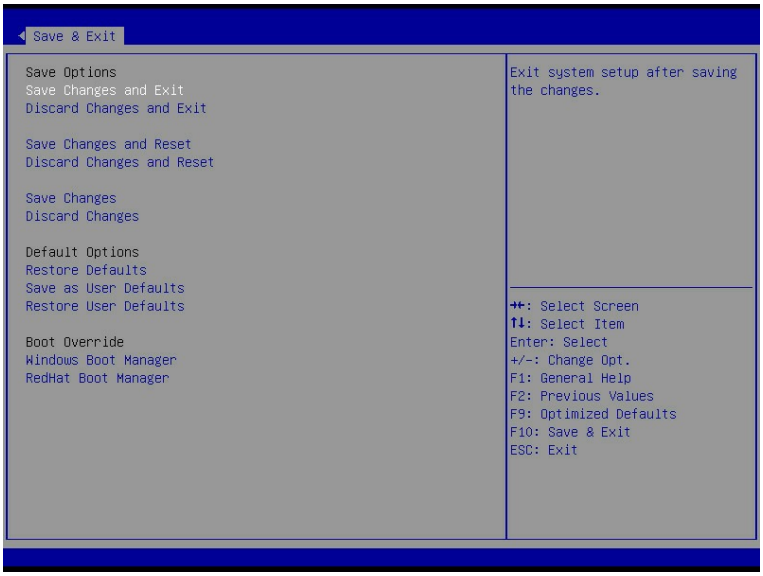
功能描述

Save&Exit 界面是 BIOS 参数修改保存和退出相关选项设置。

界面展示

Save&Exit 界面如图 3-64 所示。

图 3-64 Save & Exit 界面



参数说明

具体参数说明如表 3-59 所示.

表 3-59 Save&Exit 界面说明表

界面参数	功能说明
Save Changes and Exit	保存修改并退出
Discard Changes and Exit	放弃修改并退出
Save Changes and Reset	保存修改并且重启
Discard Changes and Reset	放弃修改并且重启
Save Changes	保存修改
Discard Changes	放弃修改
Restore Defaults	重载默认设置
Save as user Defaults	保存成用户默认设置
Restore user Defaults	重载用户默认配置
Boot Override	启动项重载，可以选择界面展示的启动项启动

4 固件更新

BIOS 固件升级方法，请参考《浪潮英信服务器 BIOS 升级手册》。