



# UNISINSIGHT 服务器

## Purley 平台 BIOS 配置指导

重庆紫光华山智安科技有限公司  
[www.unisinsight.com](http://www.unisinsight.com)

资料版本：5W101-20200113  
产品版本：BIOS-2.00.32P07 及以上版本

Copyright © 2019~2020 重庆紫光华山智安科技有限公司及其许可者 版权所有，保留一切权利。

## 知识产权声明

本手册为紫光华智公司制作，手册中所有的文字、图片、表格、版面设计等均受到著作权法的保护。没有经过本公司许可，任何组织和个人不得以任何形式复制、摘抄本手册的部分或全部内容，不得以任何形式传播。

本手册中作为商标使用的商业标识、产品标识或产品名称等均为紫光华智公司注册或取得合法授权的商标。本手册基于叙述和说明等原因可能涉及到其他公司的商标，其权利由各自权利人所拥有。任何未经授权使用本手册的相关商业行为都将违反《中华人民共和国著作权法》和其他法律法规以及国际公约的规定，紫光华智保留追究法律责任的权利。

## 免责声明

由于产品版本升级或其他原因，本手册内容有可能变更。紫光华智保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光华智尽全力在本手册中提供准确的信息，但是紫光华智并不保证手册内容完全没有错误或误差，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

# 前言

本手册主要介绍 BIOS 的常用功能、BIOS 界面参数说明和缩略语等内容。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)

## 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责服务器配置和维护的管理员

## 本书约定

### 1. 命令行格式约定

格式	意义
<b>粗体</b>	命令行关键字（命令中保持不变、必须照输的部分）采用 <b>加粗</b> 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[ ]	表示用 “[ ]” 括起来的部分在命令配置时是可选的。
{ x   y   ... }	表示从多个选项中仅选取一个。
[ x   y   ... ]	表示从多个选项中选取一个或者不选。
{ x   y   ... } *	表示从多个选项中至少选取一个。
[ x   y   ... ] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

### 2. 图形界面格式约定

格式	意义
<>	带尖括号“<>”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

### 3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

### 4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

## 5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

# 目 录

1 简介 .....	1-1
1.1 适用产品 .....	1-1
1.2 文档使用说明 .....	1-1
1.3 BIOS 简介 .....	1-1
2 常用功能.....	2-1
2.1 进入 BIOS 界面.....	2-1
2.2 设置 BIOS 界面模式.....	2-4
2.3 查询 CPU 信息.....	2-4
2.4 查询内存信息 .....	2-5
2.5 查询板载硬盘信息.....	2-6
2.6 查询 HDM 网络信息 .....	2-7
2.7 设置 HDM 网络信息 .....	2-8
2.8 设置 BIOS 密码.....	2-10
2.8.1 BIOS 密码简介.....	2-10
2.8.2 密码设置注意事项.....	2-12
2.8.3 设置管理员密码 .....	2-12
2.8.4 设置用户密码.....	2-14
2.8.5 清除 BIOS 密码.....	2-17
2.9 设置系统日期和时间 .....	2-19
2.10 设置 BIOS 启动模式.....	2-20
2.11 设置服务器启动顺序 .....	2-21
2.12 配置 RAID.....	2-23
2.13 恢复 BIOS 缺省设置.....	2-23
3 界面参数说明 .....	3-1
3.1 Main 界面.....	3-1
3.2 Advanced 界面.....	3-2
3.2.1 Trusted Computing 界面 .....	3-4
3.2.2 ACPI Settings 界面 .....	3-8
3.2.3 Serial Port Console Redirection 界面.....	3-9
3.2.4 PCI Subsystem Settings 界面.....	3-13
3.2.5 USB Configuration 界面.....	3-15
3.2.6 CSM Configuration 界面 .....	3-16
3.2.7 NVMe Configuration 界面.....	3-18
3.2.8 iMS Configuration 界面.....	3-20

3.2.9 Network PXE Control 界面 .....	3-22
3.2.10 Network Stack Configuration 界面.....	3-25
3.2.11 Intel(R) VROC sSATA Controller 界面 .....	3-26
3.2.12 Intel(R) virtual RAID on CPU 界面.....	3-34
3.2.13 Slot x:Port x 界面 .....	3-44
3.2.14 Intel(R) Optane(TM) DC Persistent Memory Configuration.....	3-46
3.2.15 Driver Health 界面.....	3-76
3.3 Platform Configuration 界面.....	3-77
3.3.1 PCH Configuration 界面 .....	3-78
3.3.2 Miscellaneous Configuration 界面 .....	3-86
3.3.3 Server ME Configuration 界面 .....	3-87
3.3.4 Runtime Error Logging 界面 .....	3-89
3.4 Socket Configuration 界面 .....	3-106
3.4.1 Processor Configuration 界面.....	3-107
3.4.2 Common RefCode Configuration 界面 .....	3-112
3.4.3 UPI Configuration 界面 .....	3-114
3.4.4 Memory Configuration 界面.....	3-117
3.4.5 IIO Configuration 界面 .....	3-123
3.4.6 Advanced Power Management Configuration 界面 .....	3-133
3.5 Server Mgmt 界面.....	3-146
3.6 Security 界面.....	3-158
3.7 Boot 界面 .....	3-163
3.8 Save & Exit 界面 .....	3-168
4 缩略语 .....	4-1

# 1 简介

## 1.1 适用产品

本手册适用于以下产品：

- UNISINSIGHT AIX R4208-G3
- UNISINSIGHT US3040
- UNISINSIGHT AIX R5208L-G3
- UNISINSIGHT AIX R6220L-G3

## 1.2 文档使用说明

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，建议联系技术支持获取最新BIOS固件版本。

本文为产品通用资料。对于定制化产品，请用户以产品实际情况为准。

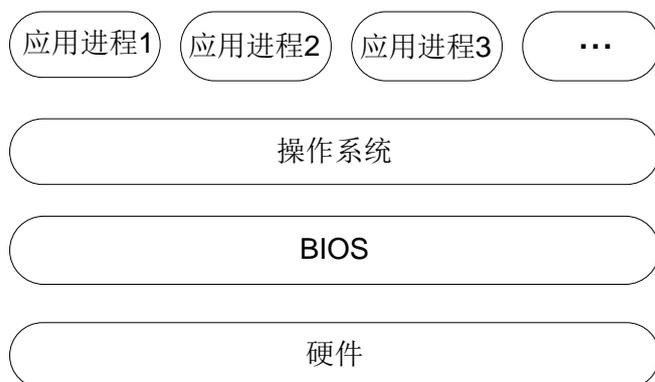
## 1.3 BIOS简介

基本输入输出系统BIOS（Basic Input Output System）固化在系统ROM中，是加载在服务器硬件系统上最基本的运行程序。BIOS在系统中的位置如 [图 1-1](#)所示，位于服务器硬件和操作系统之间，用来初始化硬件，为操作系统运行做准备。

BIOS的主要功能包括：

- POST自检。
- 检测输入输出设备和可启动设备，包括内存初始化、硬件扫描和寻找启动设备、启动系统。
- 提供高级电源管理 ACPI。
- 配置 RAID。

图1-1 BIOS在系统中的位置



## 2 常用功能

常用功能包括：

- [进入BIOS界面](#)
- [设置BIOS界面模式](#)
- [查询CPU信息](#)
- [查询内存信息](#)
- [查询板载硬盘信息](#)
- [查询HDM网络信息](#)
- [设置BIOS密码](#)
- [设置系统日期和时间](#)
- [设置BIOS启动模式](#)
- [设置服务器启动顺序](#)
- [配置RAID](#)
- [恢复BIOS缺省设置](#)

### 2.1 进入BIOS界面

(1) 在服务器上连接键盘、鼠标和显示器或启动HDM Web界面的远程控制台。

---



说明

关于启动远程控制台的具体方法，请参见HDM联机帮助。

---

(2) 启动或重启服务器。

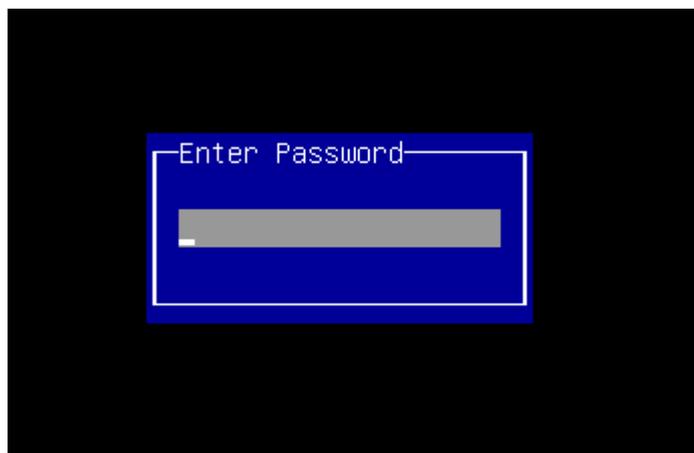
(3) 如 [图 2-1](#)所示，进入BIOS启动界面后，按 **Del**或 **Esc**。

图2-1 BIOS 启动界面



- (4) (可选) 如图 2-2 所示，如果出现输入密码对话框，请在对话框中输入密码。
- BIOS 缺省没有设置任何密码，设置密码的具体方法请参见 [2.8 设置 BIOS 密码](#)。
  - 仅设置了管理员密码的情况下，可输入管理员密码以管理员权限进入 BIOS Setup 界面，或直接按 **Enter** 键以用户权限进入。
  - 如果连续三次输入错误的密码，服务器会自动重启，稍后请重新输入密码。
  - 如果您忘记了 BIOS 密码，请将服务器下电，通过系统维护开关清除 BIOS 密码。服务器重新上电时，系统将清除 BIOS 的密码。系统维护开关的具体位置，请参见产品用户指南。

图2-2 输入密码



- (5) 如图 2-3 所示，进入 BIOS Setup 界面，可参照界面右下角的操作说明进行相关设置。操作说明的详细信息如表 2-1 所示。

图2-3 BIOS Setup 界面

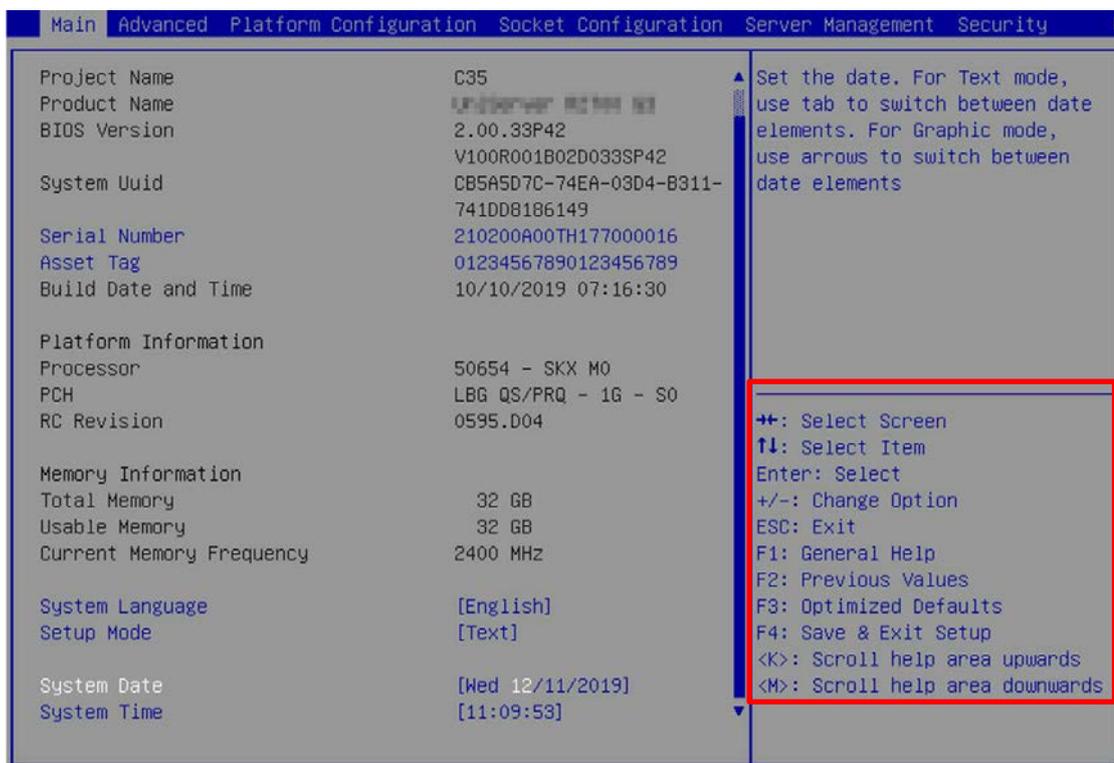


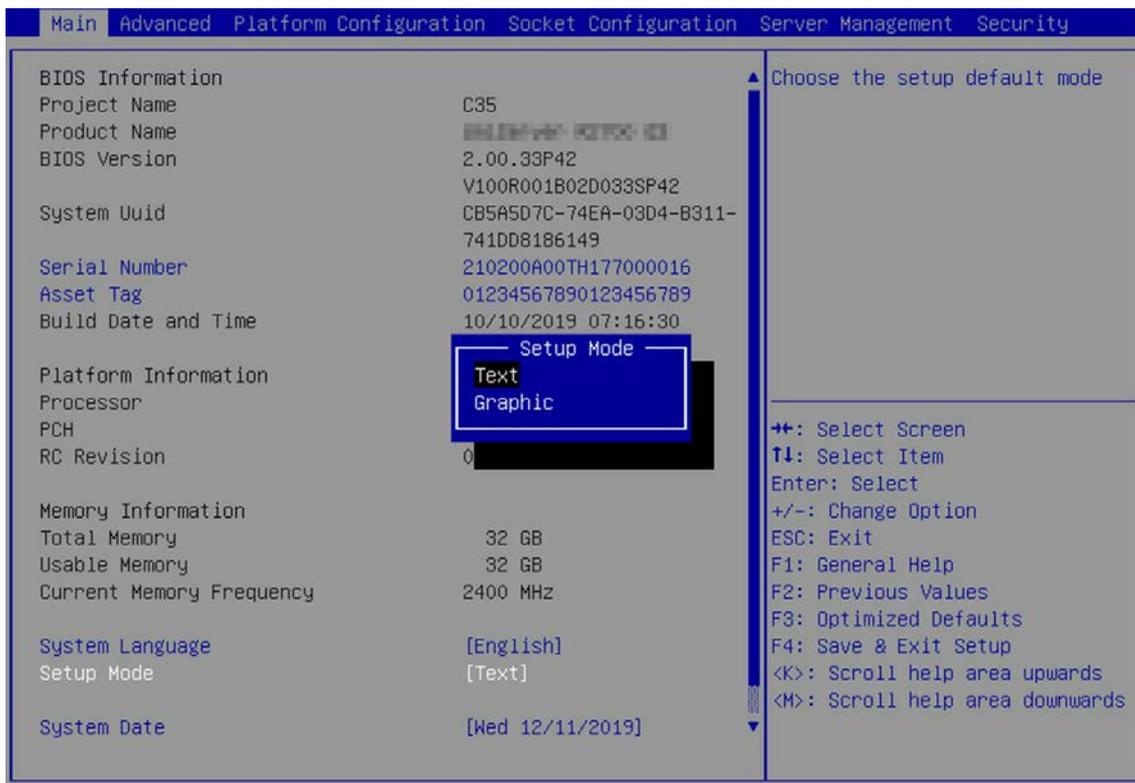
表2-1 操作说明

操作项	功能说明
↔	选择界面
↑ ↓	向上或向下选择菜单或选项
Enter	执行选项或选择菜单
+/-	选择当前选项的前一个或后一个选项或数值
ESC	退出BIOS Setup界面或返回上一层菜单
F1	获取操作项的帮助信息
F2	加载之前的设定值
F3	加载缺省值
F4	保存设置并退出BIOS Setup界面
<K>	向上滚动界面右上角的帮助信息
<M>	向下滚动界面右上角的帮助信息

## 2.2 设置BIOS界面模式

- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 如[图 2-4](#)所示，选择**Main**页签，进入Main界面。
- (3) 选择 **Setup Mode** 选项，按 **Enter**。选项包括：
  - **Text**: 文本模式。
  - **Graphic**: 图形化模式。

图2-4 Setup 模式

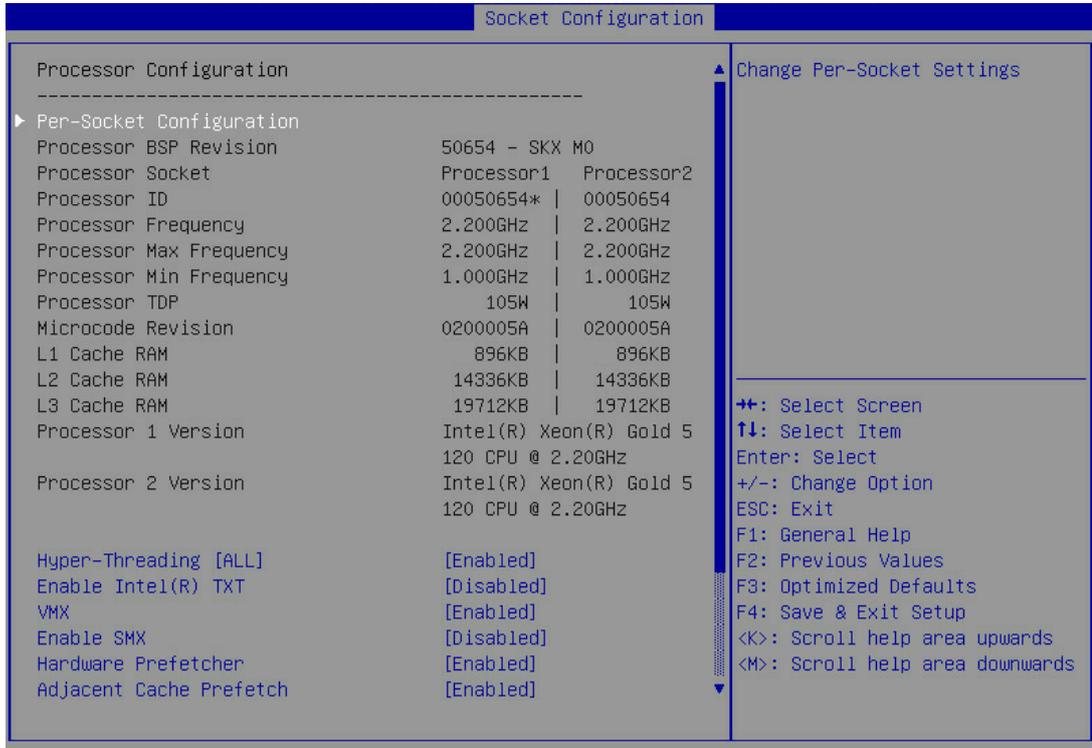


- (4) 设置完成后，按 **F4** 保存设置。设置在服务器会重启后生效。

## 2.3 查询CPU信息

- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 在BIOS Setup界面中，进入**Socket Configuration**页签，选择 **Processor Configuration**，然后按**Enter**。如[图 2-5](#)所示，进入Processor Configuration界面，显示所有CPU的详细信息。CPU的Processor Configuration界面的详细信息请参见[3.4.1 Processor Configuration界面](#)。

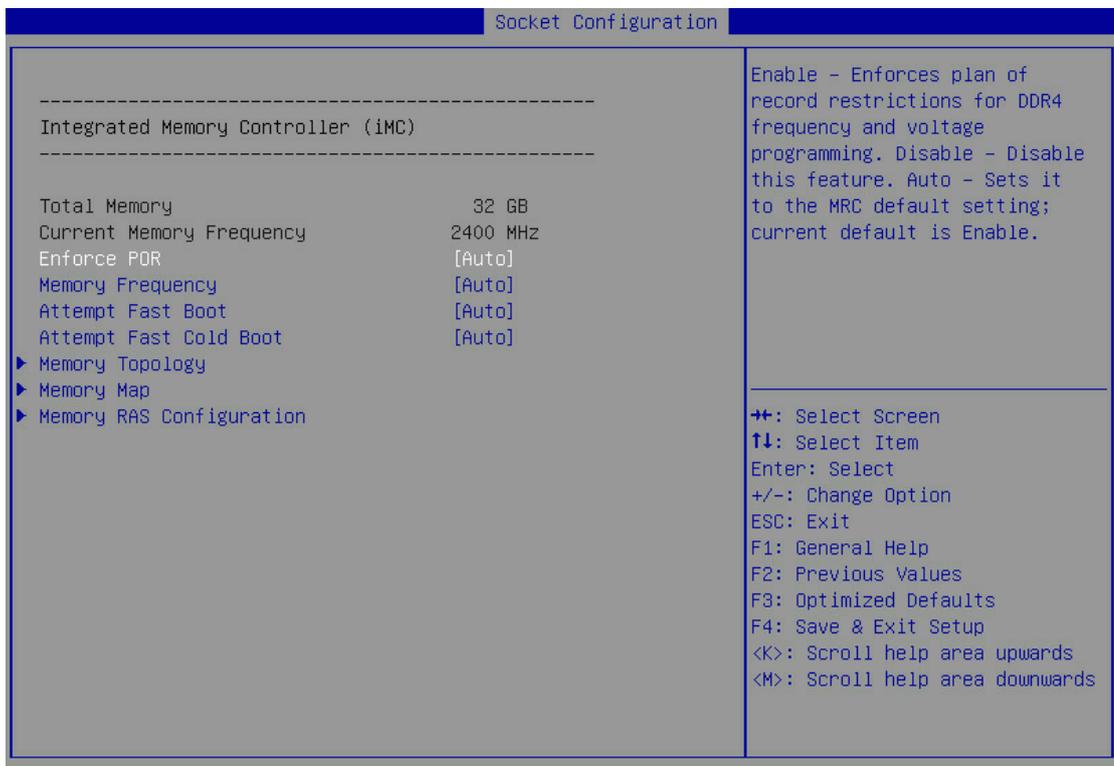
图2-5 Processor Configuration 界面



## 2.4 查询内存信息

- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 在BIOS Setup界面中，进入**Socket Configuration**页签，选择**Memory Configuration**，然后按**Enter**。如[图 2-6](#)所示，进入Memory Configuration界面，显示内存的容量和频率信息，如需查看单个DIMM的详细信息，进入Memory Topology菜单。内存的Memory Configuration界面的详细信息请参见[3.4.4 Memory Configuration界面](#)。

图2-6 Memory Configuration 界面

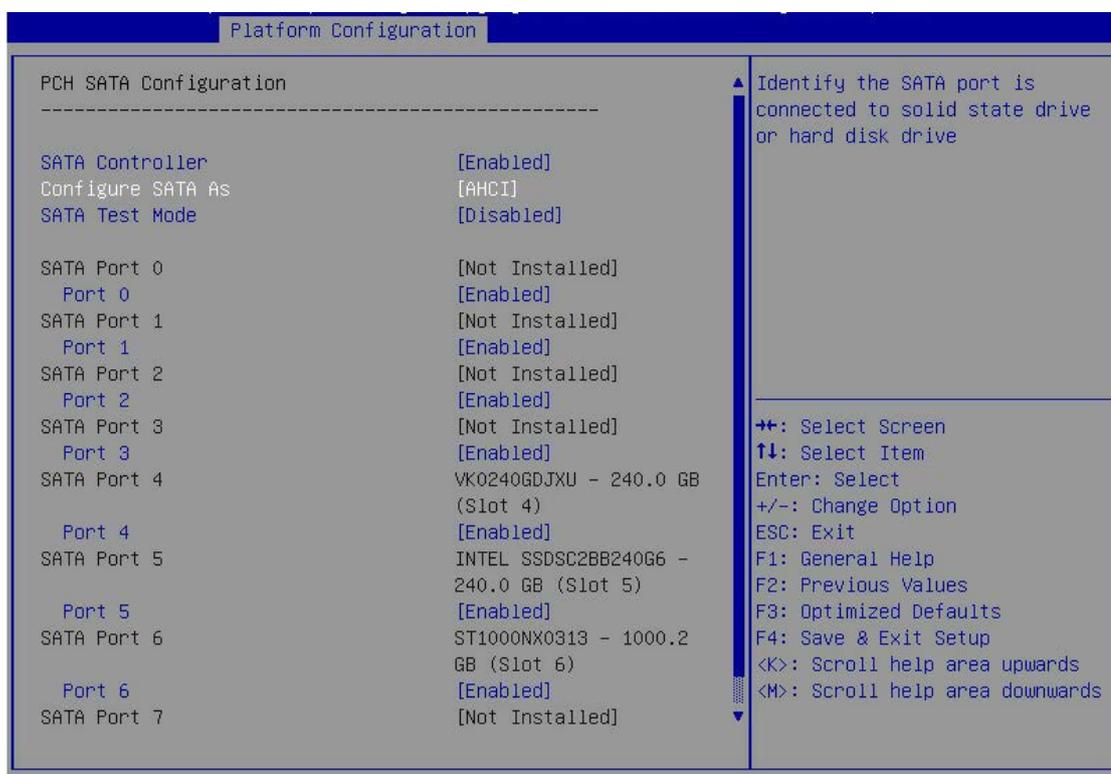


## 2.5 查询板载硬盘信息

本文以进入PCH SATA Configuration界面为例，PCH SATA Configuration和PCH sSATA Configuration的详细信息请参见[3.3.1 PCH Configuration界面](#)。

- (1) 进入服务器的 BIOS Setup 界面，具体步骤请参见 2.1 进入 BIOS 界面。
- (2) 在 BIOS Setup 界面中，进入 **Platform Configuration** 页签，选择 **PCH Configuration > PCH SATA Configuration**，然后按 **Enter**。如 [图 2-7](#) 所示，进入 PCH SATA Configuration 界面，显示硬盘信息。

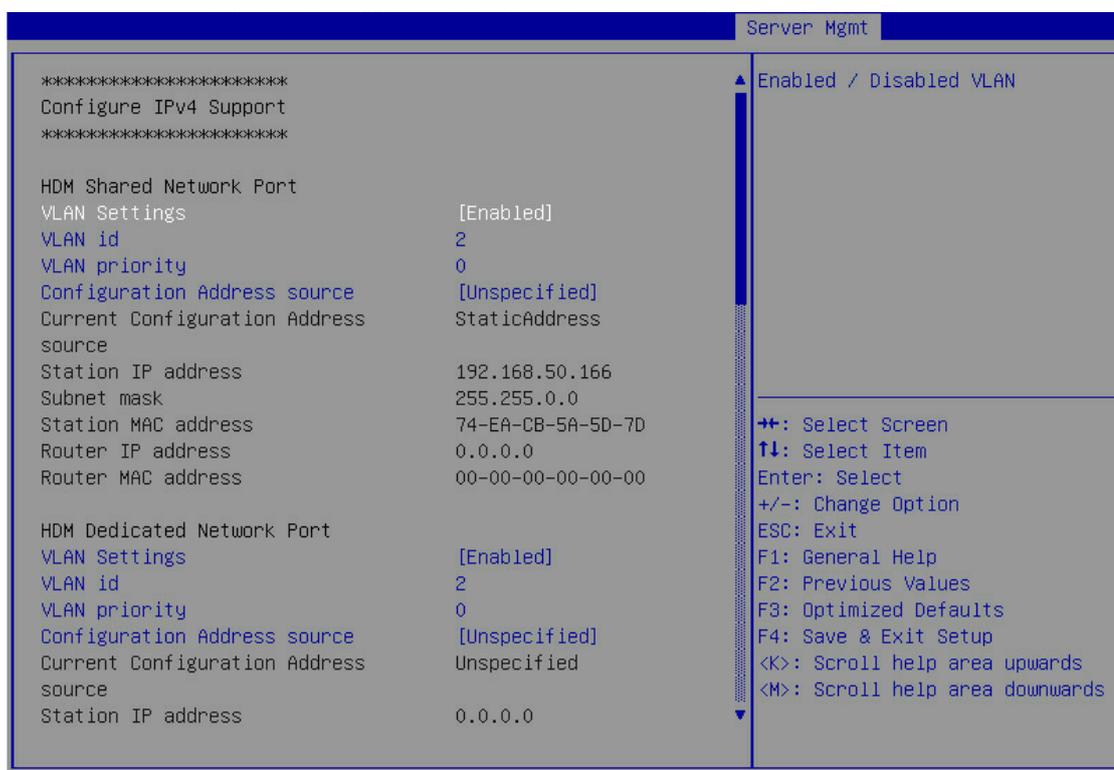
图2-7 PCH SATA Configuration 界面



## 2.6 查询HDM网络信息

- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 在BIOS Setup界面中，进入**Server Mgmt**页签，选择**HDM Network Configuration**，然后按**Enter**。如[图 2-8](#)所示，进入HDM Network Configuration界面，显示HDM网络信息。

图2-8 HDM Network Configuration 界面



## 2.7 设置HDM网络信息

### 1. 任务简介

该任务用于指导工程师通过 BIOS 设置服务器 HDM 的网络信息，包括 HDM 专用/共享网口的 IP 地址、子网掩码、网关 IP 地址及网络信息的获取方式。

### 2. 准备工作

数据准备：HDM IP 地址、子网掩码和网关 IP 地址。

### 3. 操作步骤

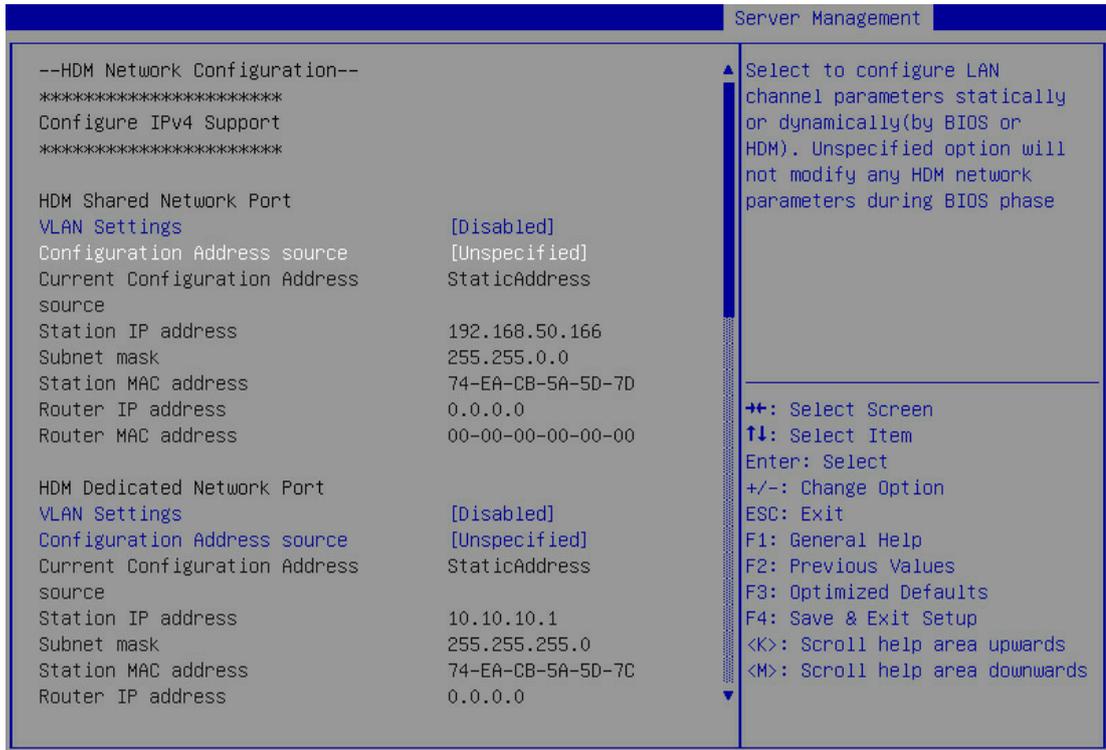
- (1) 进入服务器的 BIOS Setup 界面，具体步骤请参见 [2.1 进入 BIOS 界面](#)。
- (2) 在 BIOS Setup 界面中，进入 **Server Mgmt** 页签，选择 **HDM Network Configuration**，然后按 **Enter**。如图 2-9 所示，进入 HDM Network Configuration 界面，显示 HDM 网络信息。有 HDM 共享网口（HDM Shared Network Port）和 HDM 专用网口（HDM Dedicated Network Port）可供选择，本文以配置 HDM Dedicated Network Port 的网络信息为例。
- (3) 选择 HDM Dedicated Network Port 下的 **Configuration Address Source**，按 **Enter**。



注意

需要注意的是，为了避免引起网络风暴，HDM 共享网口和 HDM 专用网口的 IP 地址不可配置为同一网段。

图2-9 HDM Network Configuration 界面



- (4) 在弹出的对话框中选择 HDM 网络信息的获取方式。HDM 专用/共享网口获取网络信息有以下几种方式：
  - Unspecified: 保留当前的网络信息获取方式和信息。
  - Static: 手动配置网络信息。
  - DynamicHdmDhcp: 通过 DHCP 分配获取网络信息。
- (5) 如 [图 2-10](#) 所示：
  - 选择 Unspecified 或者 DynamicHdmDhcp 后，请按 **Enter**。
  - 选择 Static 后，请分别选择 [表 2-2](#) 中的参数，在弹出的对话框中输入相关信息，然后按 **Enter**。

图2-10 HDM Network Configuration 界面

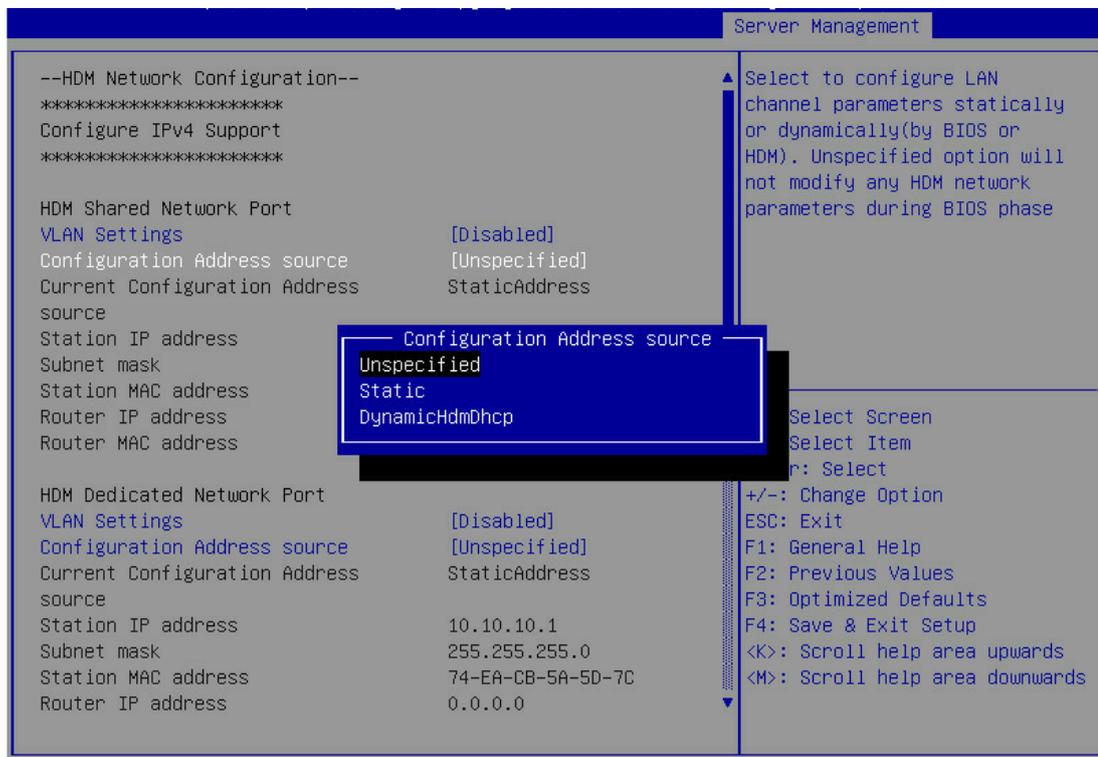


表2-2 手动配置 HDM 网络信息

界面参数	含义	备注
Station IP address	静态IP地址	必配
Subnet mask	静态IP地址对应的子网掩码	必配
Router IP address	网关IP地址	可选

(6) 设置完成后，按 **F4** 保存设置，服务器会自动重启。

## 2.8 设置BIOS密码

### 2.8.1 BIOS 密码简介

BIOS 密码包括管理员密码和用户密码。缺省情况下没有设置任何密码。

设置管理员密码和用户密码后，通过快捷键进入 BIOS Setup、Boot Menu 和 PXE Boot 时，均必须输入管理员密码或用户密码。

- 当输入的密码为管理员密码时，获取的 BIOS 权限为管理员权限。
- 当输入的密码为用户密码时，获取的 BIOS 权限为用户权限。

如果仅仅设置了管理员密码，那么该密码限制对 BIOS Setup、Boot Menu 和 PXE Boot 的访问，而且在进入 BIOS Setup、Boot Menu 和 PXE Boot 时需要提供改密码，或者直接按 Enter 键以用户权限进入。

如果仅仅设置了用户密码，那么该密码会作为开机密码，在开机时必须输入该密码。在 BIOS Setup 下，用户拥有管理员权限。

当同时设置了管理员密码和用户密码，且密码不相同，用户拥有登录密码相应的权限。如果设置的管理员密码和用户密码相同，用户拥有管理员权限。

如表 2-3 所示，当以用户权限进入 BIOS Setup 后，以下二级菜单或二级菜单对应的子选项会灰显。

表2-3 灰显菜单

一级菜单	二级菜单	子选项	状态
Advanced	ACPI Settings	Enable ACPI Auto Configuration	灰显
		Enable Hibernation	灰显
		Lock Legacy Resources	灰显
	PCI Subsystem Settings	Above 4G Decoding	灰显
		SR-IOV Support	
		BME DMA Mitigation	
	USB Configuration	Legacy USB Support	灰显
		XHCI Hand-off	
		USB Mass Storage Device Support	
	Server Mgmt	FRB-2 Timer	-
FRB-2 Timer Timeout		-	
FRB-2 Timer Policy		-	
OS Watchdog Timer		-	
OS Wtd Timer Timeout		-	
OS Wtd Timer Policy		-	
View FRU information		-	
HDM Network Configuration		-	
Security	Administrator Password	-	灰显
	Secure Boot Menu	System Mode	灰显
		Secure Boot	
		Secure Boot Mode	
		Restore Factory Keys	
		Reset To Setup Mode	
		Key Management	

## 2.8.2 密码设置注意事项

为防止未经授权人员设置和修改服务器的 BIOS 系统配置，请您同时设置管理员密码和用户密码，且两者密码不能相同。

修改密码时，禁止使用三次内的历史密码。

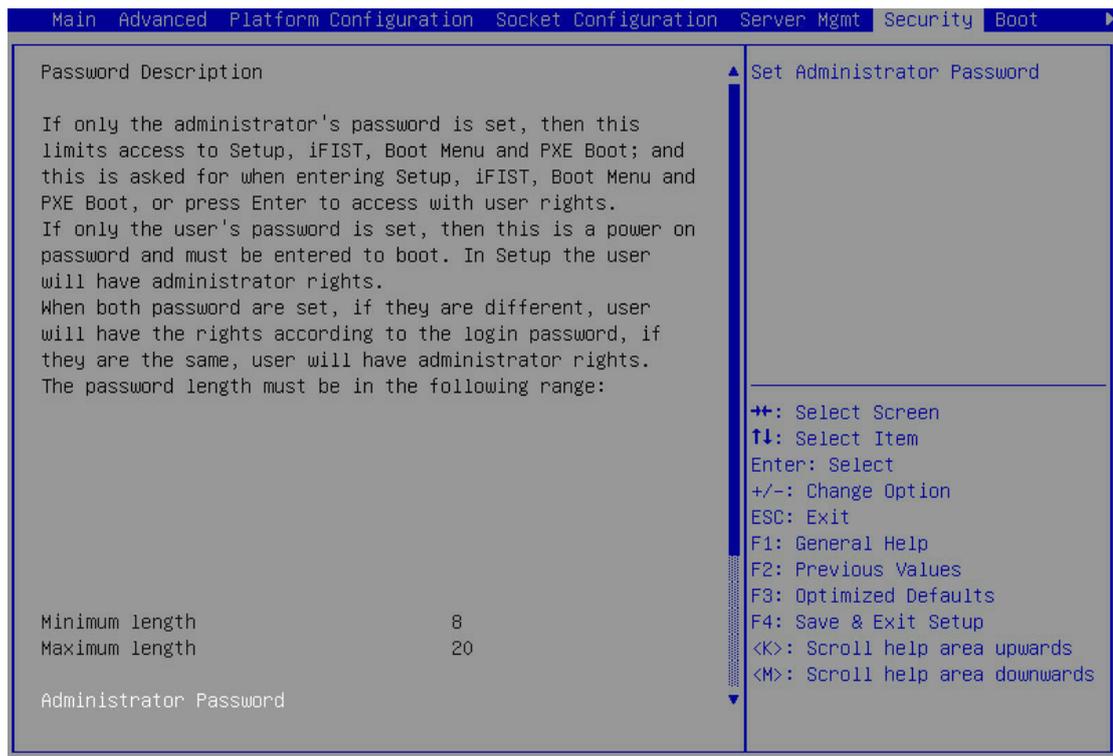
密码设置需符合以下要求：

- 密码长度为 8~20 个字符，仅支持字母、数字、空格和特殊字符 `~!@#\$%^&\*()\_+=[\{}|;:'",./<>?`，区分大小写；
- 至少包含大写字母、小写字母和数字中的两种字符；
- 至少包含一个空格或特殊字符。

## 2.8.3 设置管理员密码

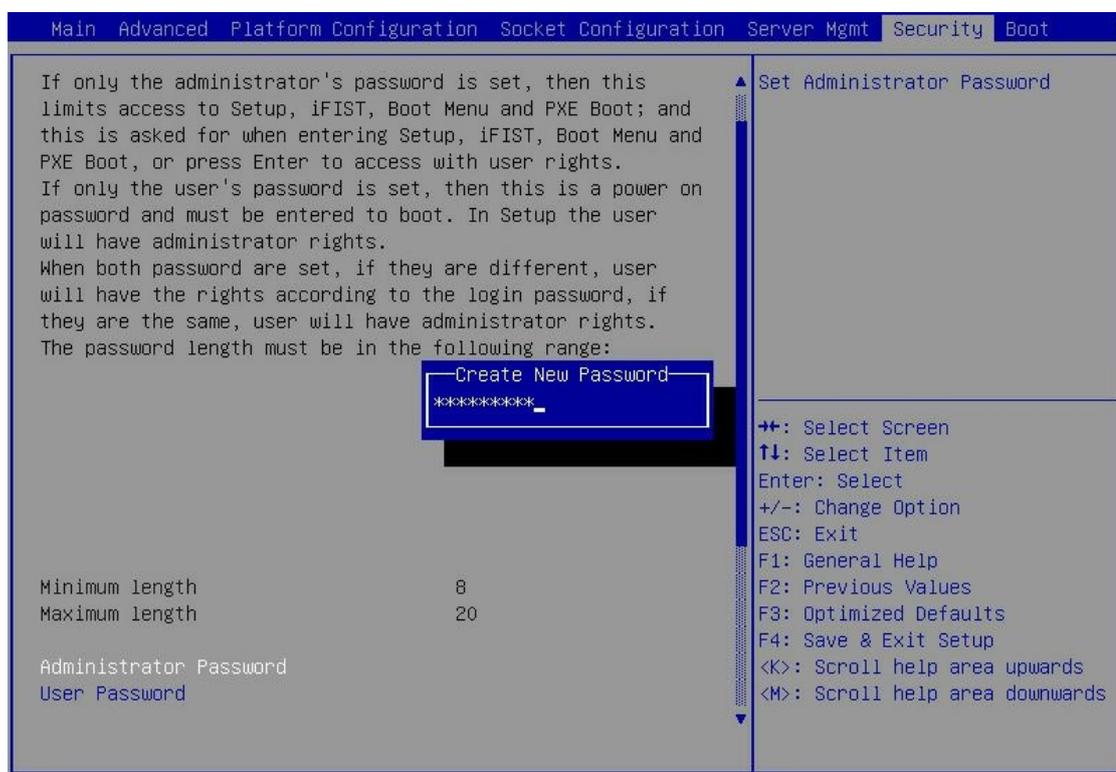
- (1) 进入服务器的 BIOS Setup 界面，具体步骤请参见 [2.1 进入 BIOS 界面](#)。
- (2) 如 [图 2-11](#) 所示，进入 **Security** 页签，选择 **Administrator Password**，按 **Enter**。

图2-11 设置管理员密码



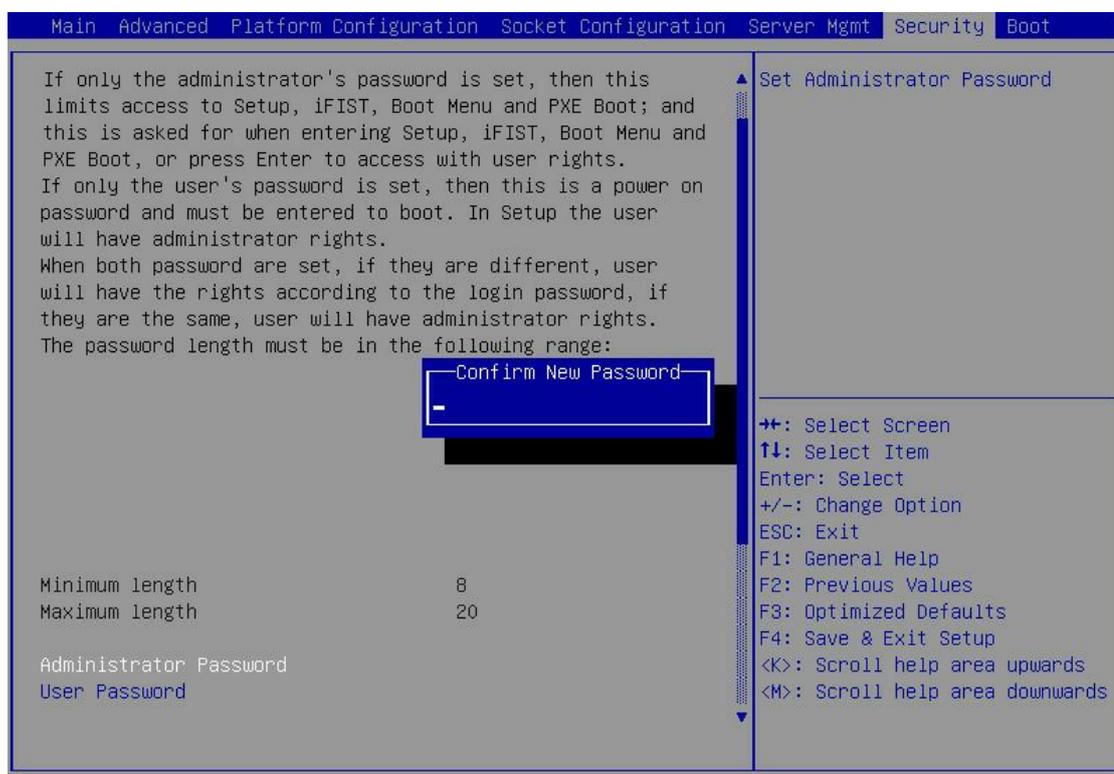
- (3) 进入 [图 2-12](#) 所示界面，在弹出的对话框中输入管理员密码，密码设置需符合 [2.8.2 密码设置注意事项](#) 的要求。输入完成后，按 **Enter**。

图2-12 输入管理员密码



(4) 进入图 2-13所示界面，再次输入密码，按Enter。

图2-13 确认管理员密码

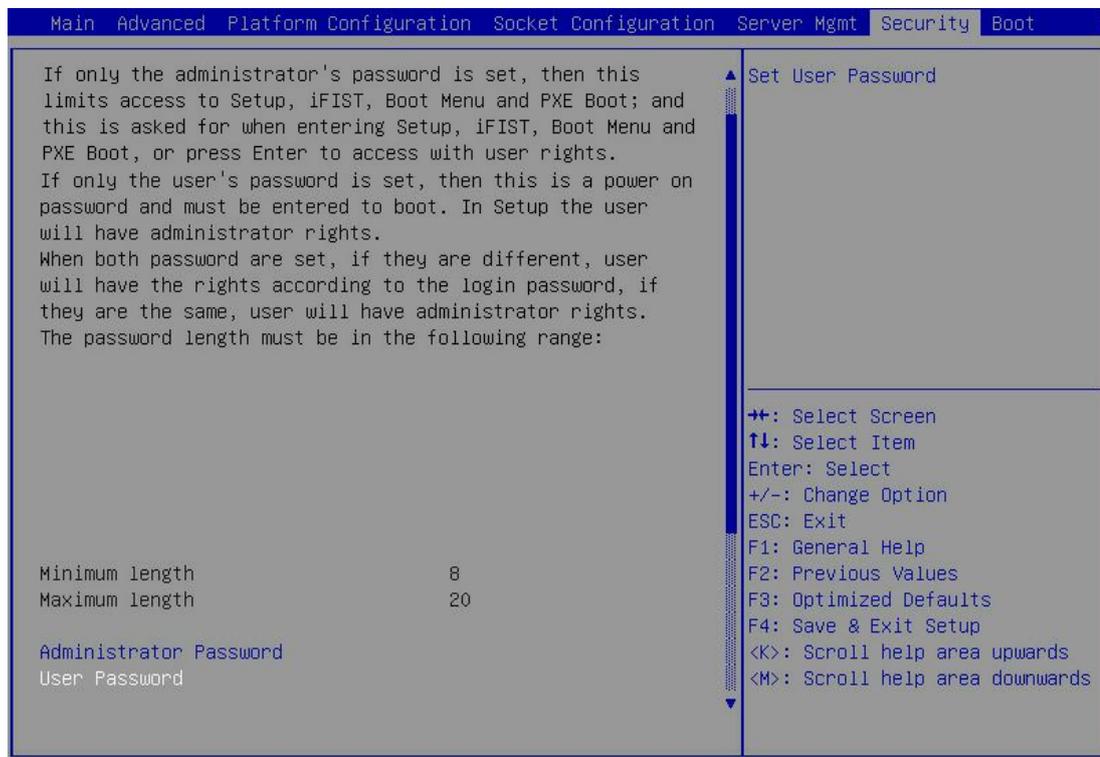


- (5) 设置完成后，按 **F4** 保存设置，设置的密码将在服务器重启后生效。

#### 2.8.4 设置用户密码

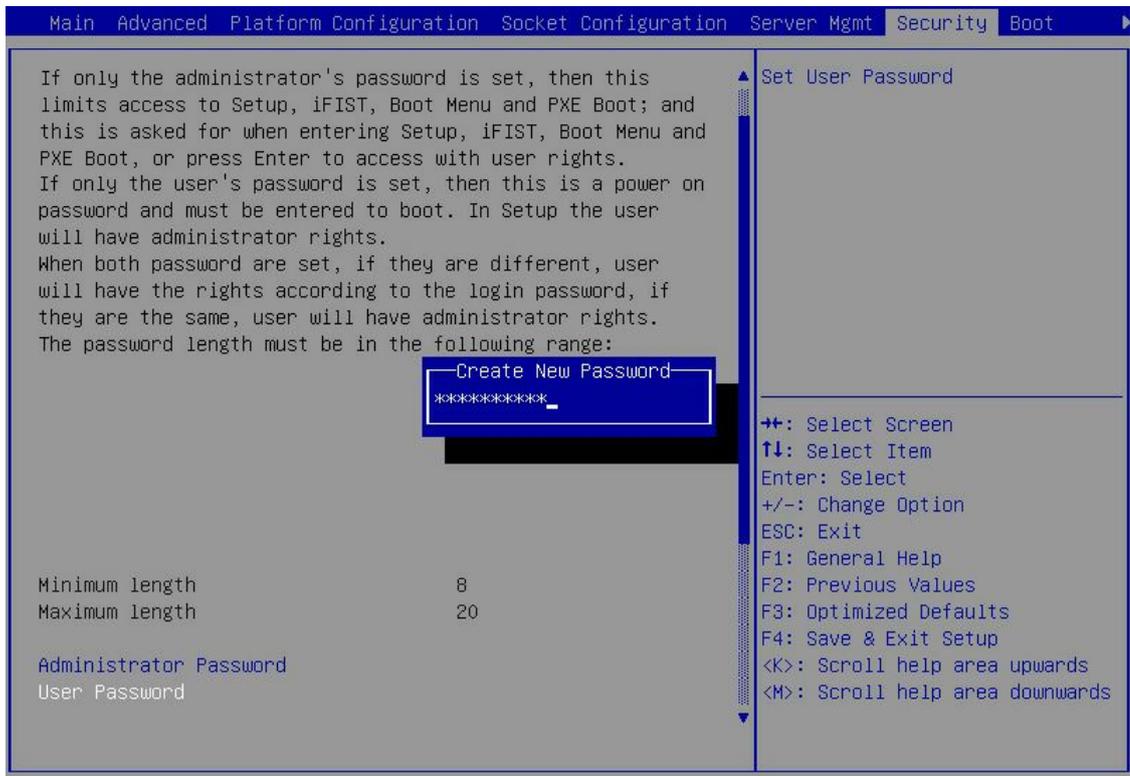
- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 如[图 2-14](#)所示，进入**Security**页签，选择**User Password**，按**Enter**。

图2-14 设置用户密码



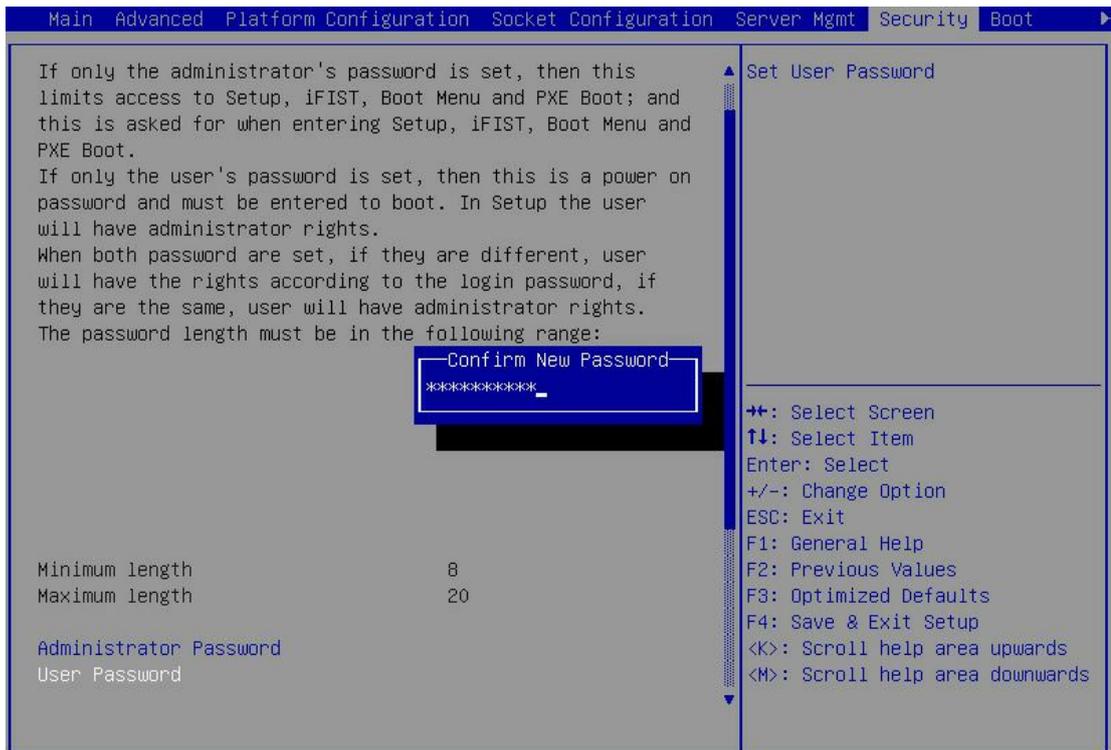
- (3) 进入图 2-15所示界面，在弹出的对话框中输入要设置的用户密码，密码需符合[2.8.2 密码设置注意事项](#)，按**Enter**。

图2-15 输入用户密码



- (4) 进入图 2-16所示界面，再次输入密码，按Enter。

图2-16 确认用户密码



(5) 设置完成后，按 **F4** 保存设置，设置的密码将在服务器重启后生效。

## 2.8.5 清除 BIOS 密码

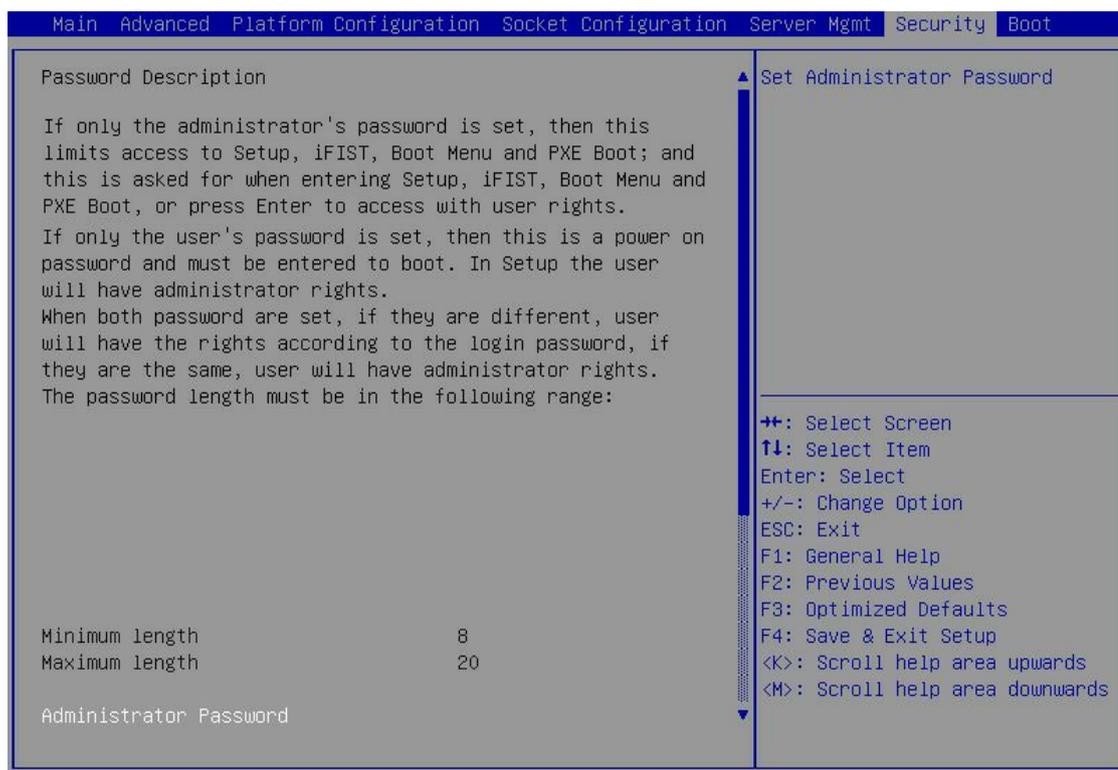


说明

清除管理员密码和清除用户密码的方法相同，本文以清除管理员密码为例。

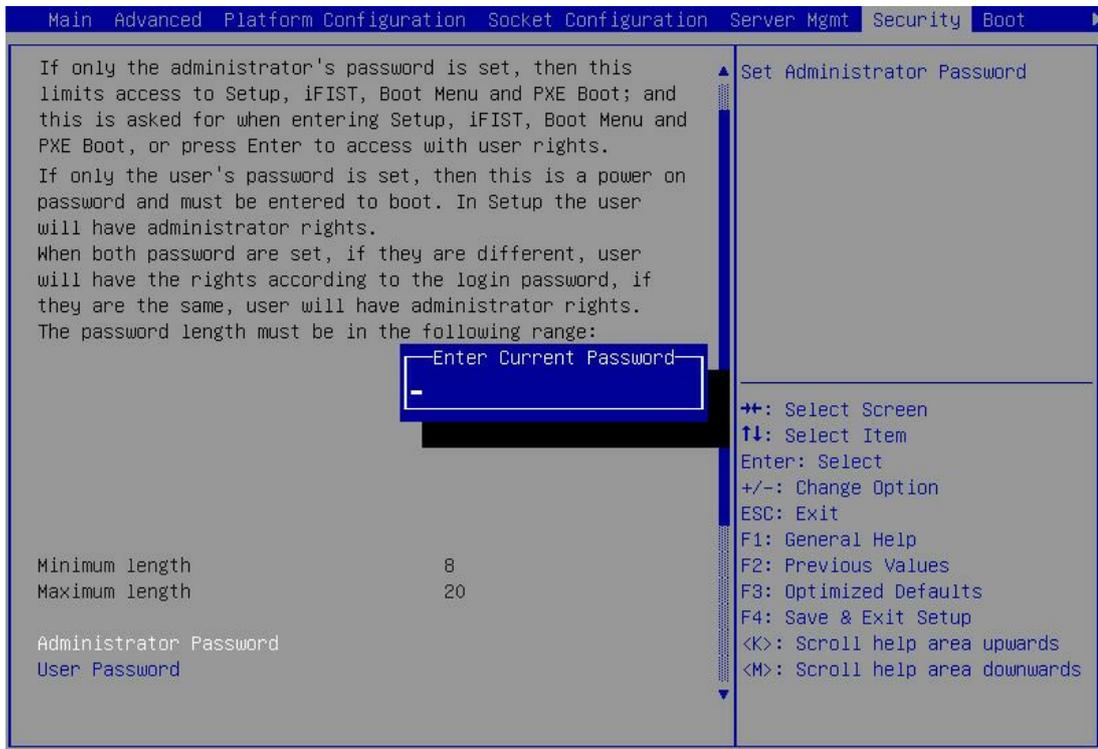
- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 如[图 2-17](#)所示，进入**Security**页签，选择**Administrator Password**，按**Enter**。

图2-17 选择管理员密码



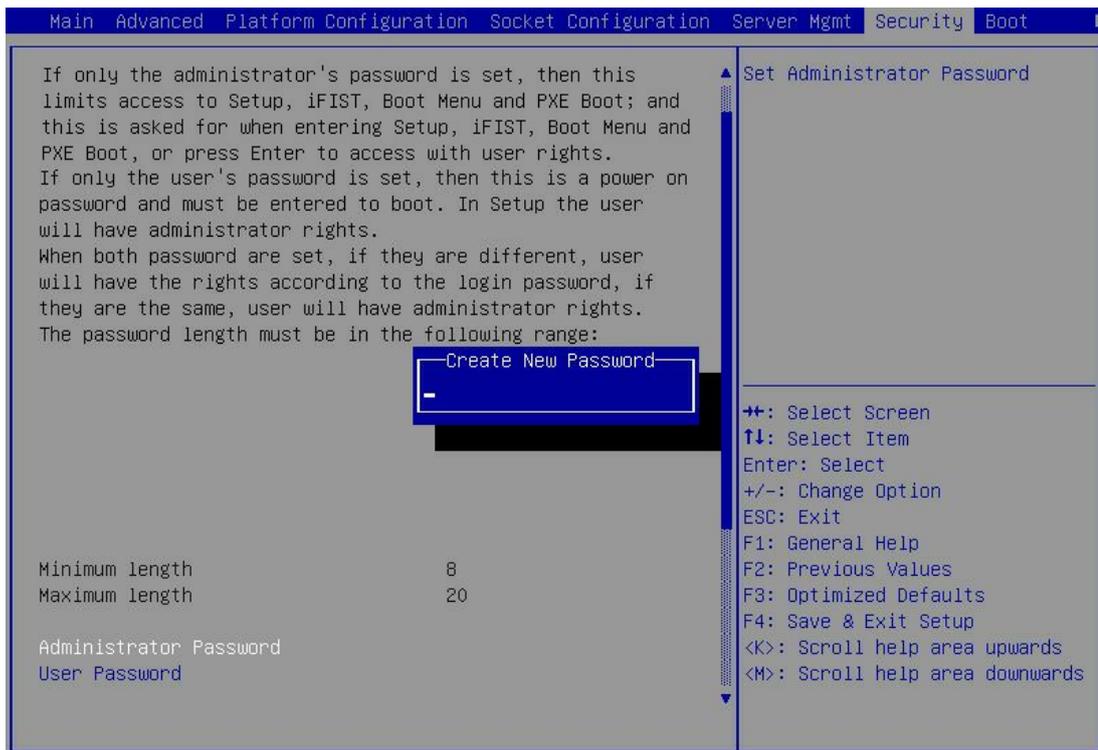
- (3) 进入[图 2-18](#)所示界面，在弹出的对话框中输入待清除的管理员密码，按**Enter**。

图2-18 输入待清除的管理员密码



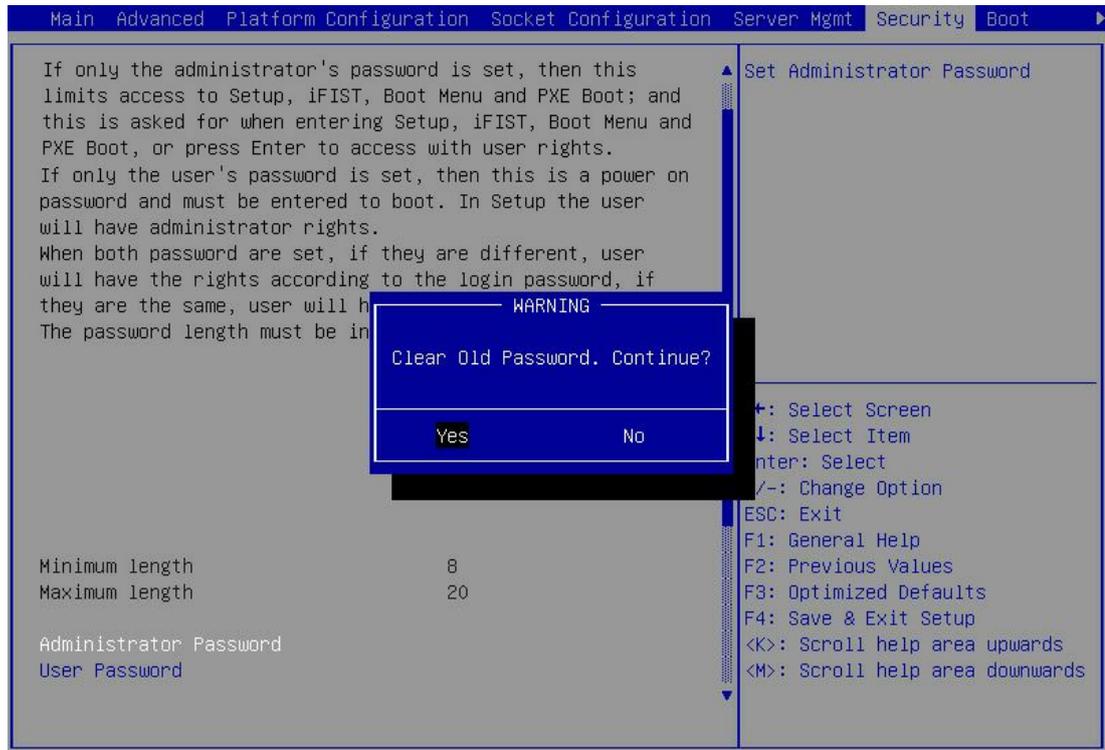
- (4) 进入图 2-19所示界面，不输入任何字符，直接按**Enter**。

图2-19 清除管理员密码



- (5) 进入图 2-20所示界面，选择Yes，按Enter。

图2-20 确认清除管理员密码

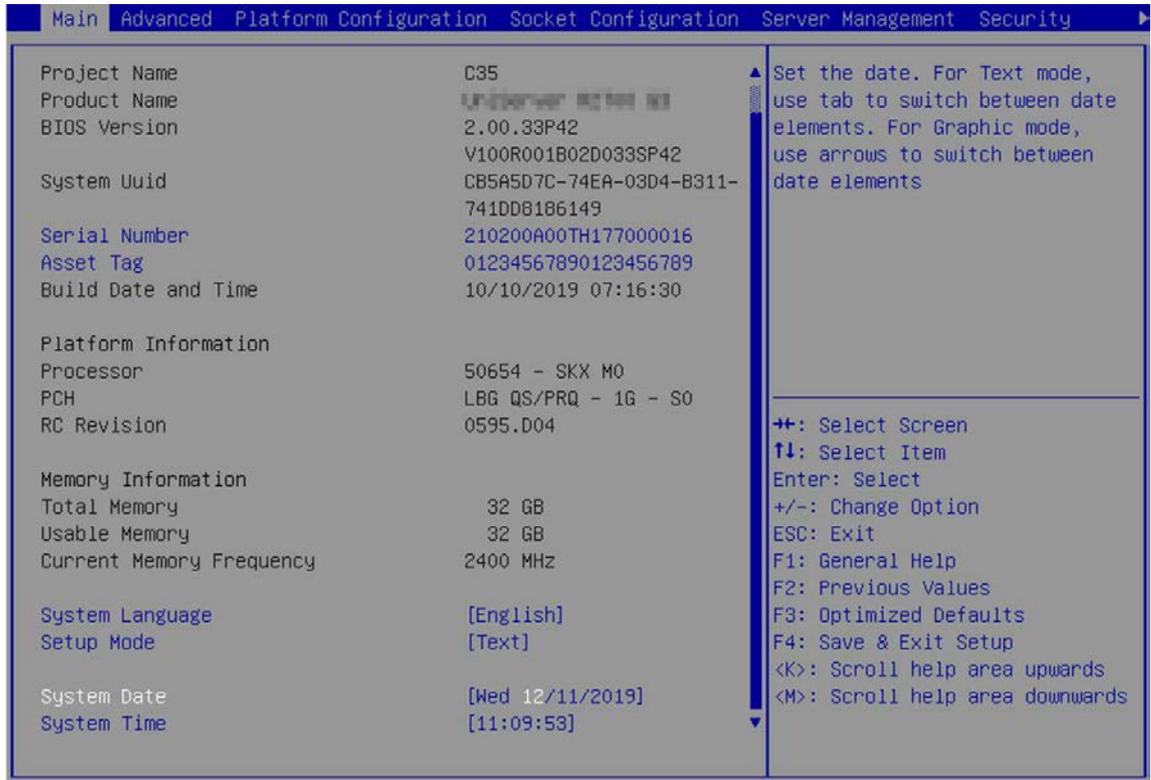


- (6) 设置完成后，按 **F4** 保存设置，服务器会继续运行。

## 2.9 设置系统日期和时间

- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 如[图 2-21](#)所示，选择**Main**页签，进入Main界面。

图2-21 Main 界面



- (3) 在图 2-21 中，选择**System Date**，系统日期的格式为“月/日/年”。按**Enter**或**Tab**键，在月、日、年之间切换，可通过以下方式来修改数值：
  - 按“+”：数值加 1。
  - 按“-”：数值减 1。
  - 按数字键：直接修改数值。
- (4) 在图 2-21 中，选择**System Time**，系统时间为 24 小时制，格式为“时:分:秒”。按**Enter**或**Tab**键，在时、分、秒之间切换，可通过以下方式来修改数值：
  - 按“+”：数值加 1。
  - 按“-”：数值减 1。
  - 按数字键：直接修改数值。

## 2.10 设置 BIOS 启动模式

### 1. 任务简介

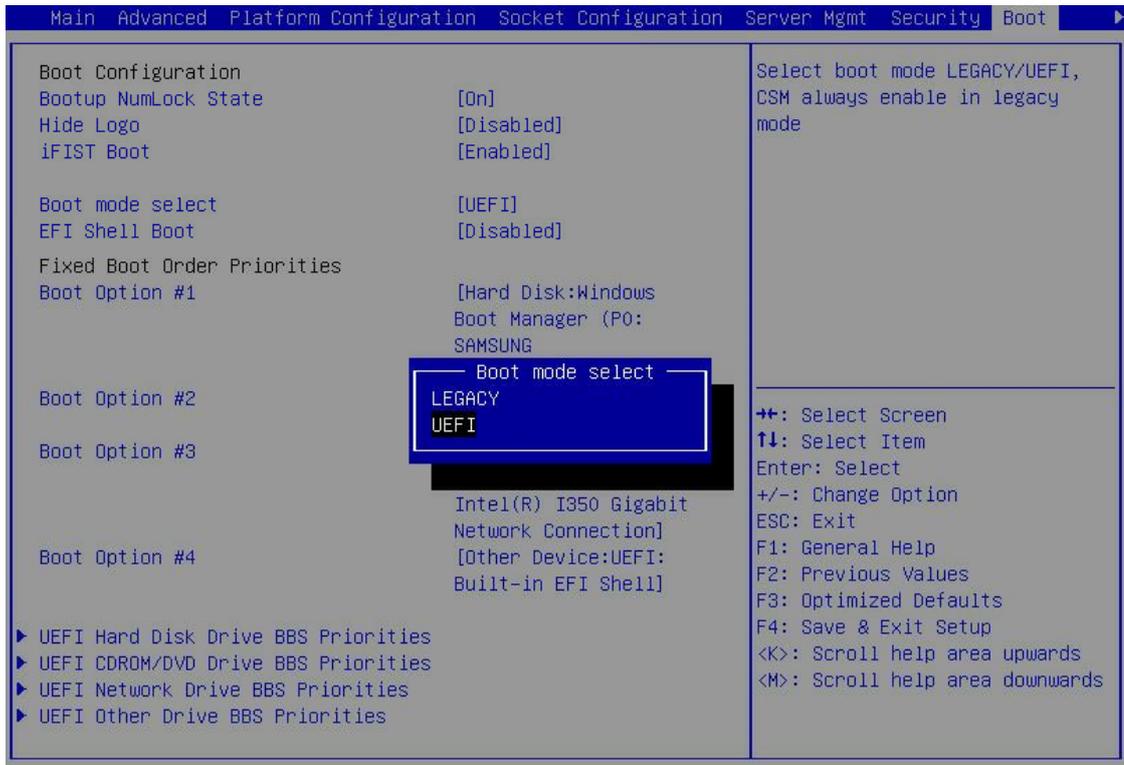
BIOS 启动模式包括 Legacy 启动模式和 UEFI 启动模式，缺省为 UEFI 启动模式。某些操作系统仅支持在 Legacy 启动模式下启动，此时，可以使用该功能修改 BIOS 的启动模式。

### 2. 操作步骤

- (1) 进入服务器的 BIOS Setup 界面，具体步骤请参见 2.1 进入 BIOS 界面。
- (2) 如图 2-22 所示，进入 Boot 页签，选择 **Boot Mode Select**，按 **Enter**，在弹出的对话框中选择启动模式。

- LEGACY: Legacy 启动模式。
- UEFI: UEFI 启动模式 (缺省)。

图2-22 设置 BIOS 启动模式



(3) 设置完成后，按 **F4** 保存设置，服务器会自动重启。

## 2.11 设置服务器启动顺序

### 1. 任务简介

服务器缺省的启动顺序如[图 2-23](#)所示，各参数含义见[表 2-4](#)，Fixed Boot Order Priorities 界面下各选项的排列顺序即服务器的启动顺序。

### 2. 操作步骤

- (1) 进入服务器的 BIOS Setup 界面，具体步骤请参见[2.1 进入 BIOS 界面](#)。
- (2) 如[图 2-23](#)所示，选择 **Boot** 页签，进入 **Boot** 页面。

图2-23 Boot 界面

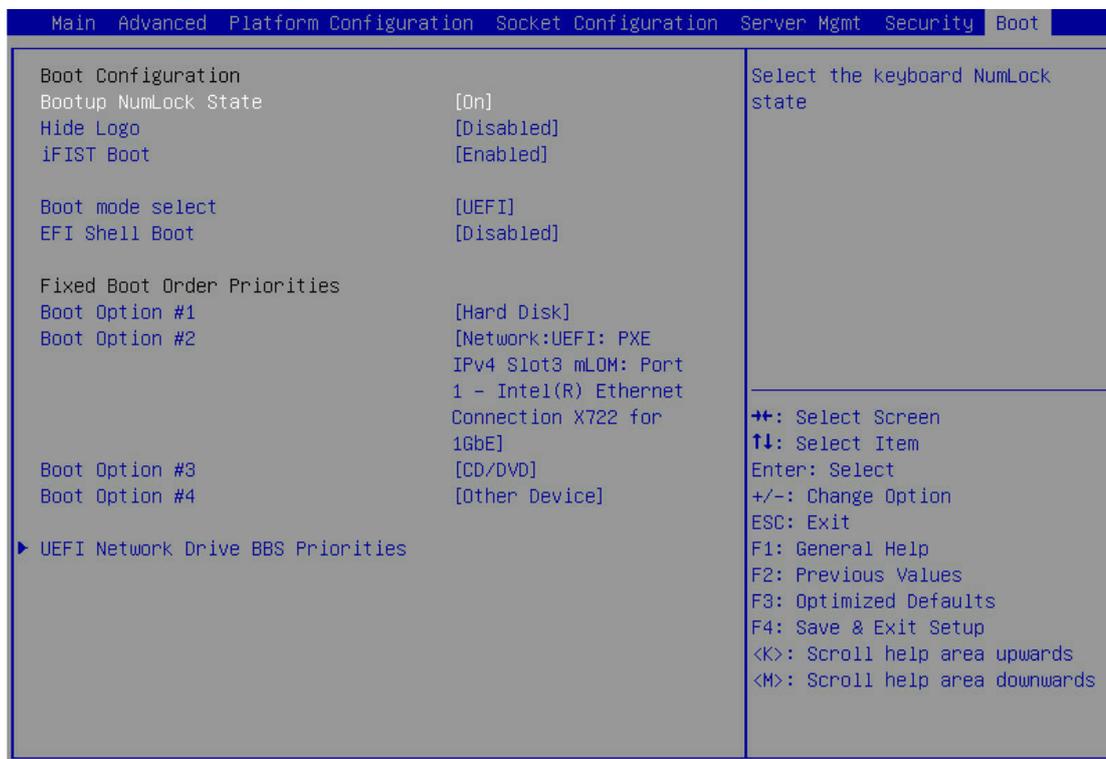
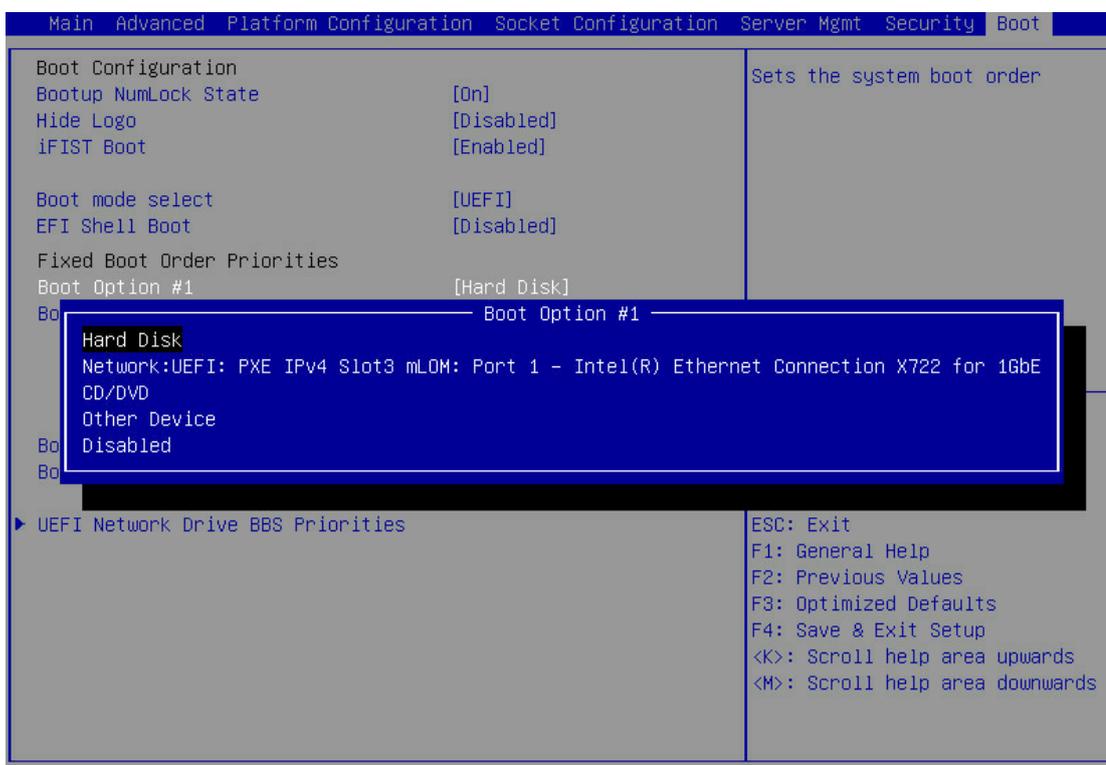


表2-4 服务器启动项

启动项	含义
Hard Disk	硬盘、USB
Network	网络启动选项
CD/DVD	光驱（包括虚拟光驱）
Other Device	内置的UEFI Shell，仅UEFI启动模式下有该启动项。当EFI Shell Boot选项设置为“Enabled”时，显示该启动项。
Disabled	禁用启动项

- (3) 如图 2-24 所示，在 Fixed Boot Order Priorities 栏选中要修改的选项，按 **Enter**，选中新启动项，按 **Enter**。

图2-24 设置启动项



(4) 设置完成后，按 **F4** 保存设置，服务器会继续运行。

#### 说明

Fixed Boot Order Priorities 界面仅可调整各启动类型的第一启动项的顺序。下面以 Hard Disk 启动类型举例说明，服务器连接多个同一类型的启动设备时的操作。

如需调整Hard Disk启动顺序，请进入UEFI Hard Disk Drive BBS Priorities界面，将要设置的启动项调整为该分类的第一启动项，具体方法与设置服务器启动顺序的方法类似。UEFI Hard Disk Drive BBS Priorities界面如[图 3-131](#)所示。

## 2.12 配置RAID

通过 BIOS 进入 RAID 配置界面配置 RAID 的具体方法请参见《UNISINSIGHT 服务器 存储控制卡 用户指南》。

## 2.13 恢复BIOS缺省设置

### 1. 任务简介

当对 BIOS 进行的未知修改导致系统出现问题时，可以使用该功能将 BIOS 恢复为缺省设置。

## 2. 操作步骤

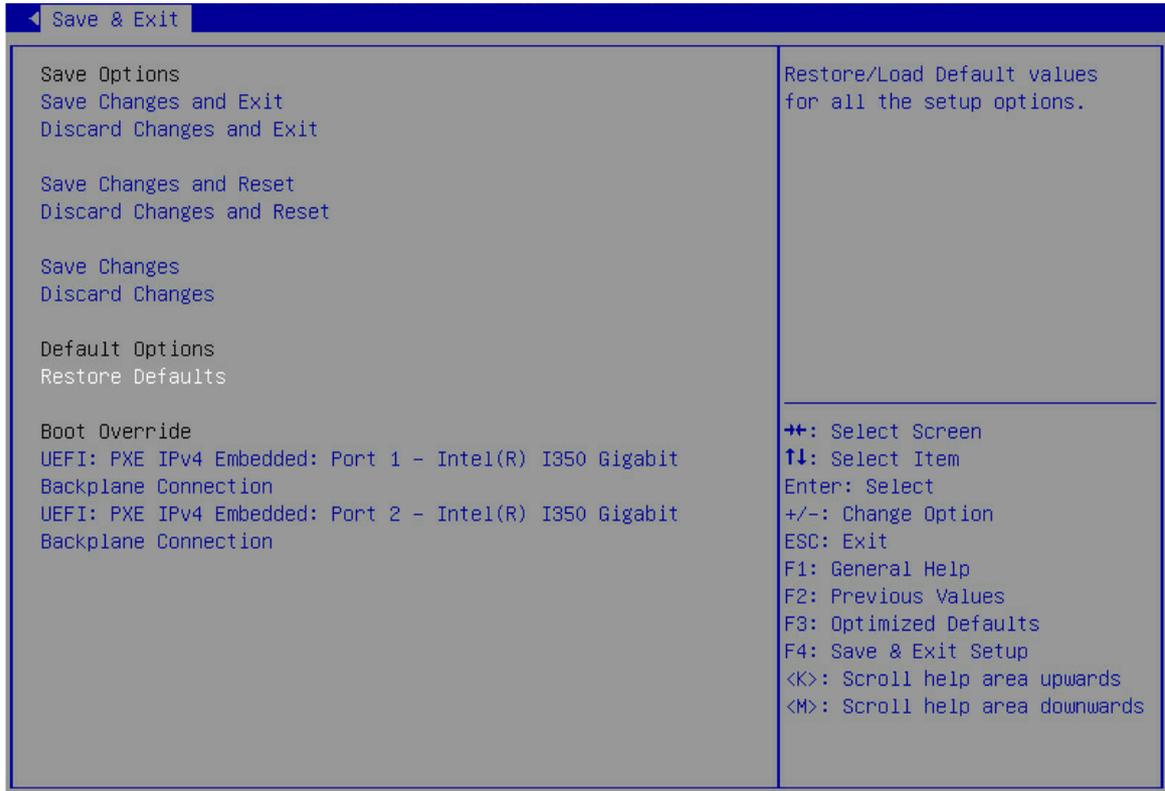
- (1) 进入服务器的BIOS Setup界面，具体步骤请参见[2.1 进入BIOS界面](#)。
- (2) 如[图 2-25](#)所示，进入**Save & Exit**页签，选择 **Restore Defaults**，按**Enter**。



说明

您也可以在 BIOS Setup 任意界面，按 **F3** 将 BIOS 恢复为缺省设置。

图2-25 恢复缺省设置



# 3 界面参数说明

## 3.1 Main界面

Main界面如图3-1所示，主要包含BIOS信息、内存信息、系统语言、系统日期和系统时间。具体参数说明如表3-1所示。

图3-1 Main界面

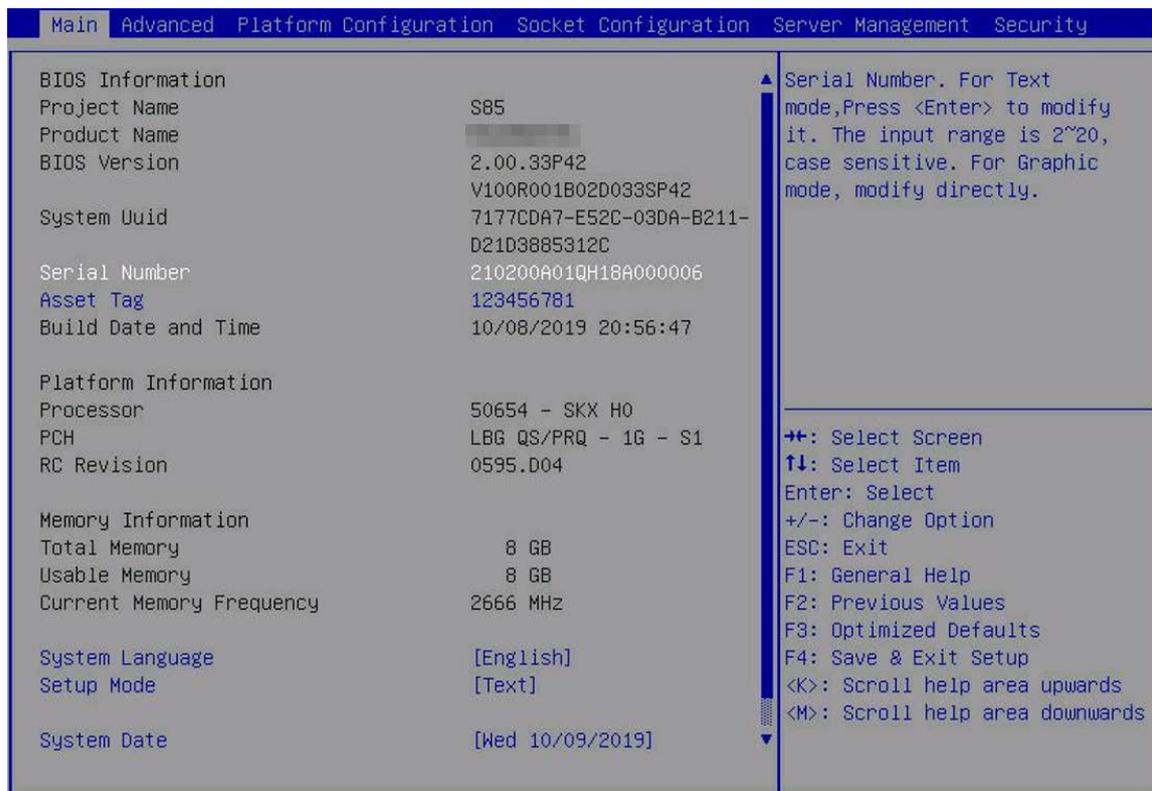


表3-1 Main界面参数

界面参数	功能说明
<b>BIOS Information</b>	
Project Name	显示项目名称。
Product Name	显示服务器型号。
BIOS Version	显示BIOS版本号。
System Uuid	系统通用唯一ID。
Asset Tag	设置服务器的资产标签，长度为2~32位，区分大小写。
Build Date and Time	显示BIOS编译日期和时间。

界面参数	功能说明
<b>Platform Information</b>	
Processor	显示CPU ID和步进。
PCH	显示PCH型号。
RC Revision	显示RC版本。
<b>Memory Information</b>	
Total Memory	显示内存总容量，单位为GiB。
Usable Memory	显示可用内存容量，单位为GiB。
Current Memory Frequency	显示当前内存频率，内存频率的设置方法请参见 <a href="#">3.4.4 Memory Configuration界面</a> 。
System Language	显示和设置当前系统语言。按Enter，选择如下两种系统语言： <ul style="list-style-type: none"> <li>• English（缺省）</li> <li>• 中文（简体）</li> </ul>
Setup Mode	设置Setup模式。菜单选项为： <ul style="list-style-type: none"> <li>• Text（缺省）：Setup显示为文本模式。</li> <li>• Graphic：Setup显示为图形化模式。</li> </ul>
System Date	显示和设置当前系统日期。 系统日期的格式为“月/日/年”。按Enter，在月、日、年之间切换，可以通过以下方式修改数值： <ul style="list-style-type: none"> <li>• 按“+”：数值加1。</li> <li>• 按“-”：数值减1。</li> <li>• 按数字键：直接修改数值。</li> </ul>
System Time	显示和设置当前系统时间。 系统时间为24小时制，格式是“时:分:秒”。按Enter，在时、分、秒之间切换，可以通过以下方式修改数值： <ul style="list-style-type: none"> <li>• 按“+”：数值加1。</li> <li>• 按“-”：数值减1。</li> <li>• 按数字键：直接修改数值。</li> </ul>

## 3.2 Advanced界面

Advanced界面如[图 3-2](#)所示，包含BIOS系统的高级配置选项，如可信计算、驱动/控制器健康、高级配置和电源接口、串口重定向、PCI子系统、网络堆栈、兼容性CSM和USB配置等。具体参数说明如[表 3-2](#)所示。

图3-2 Advanced 界面

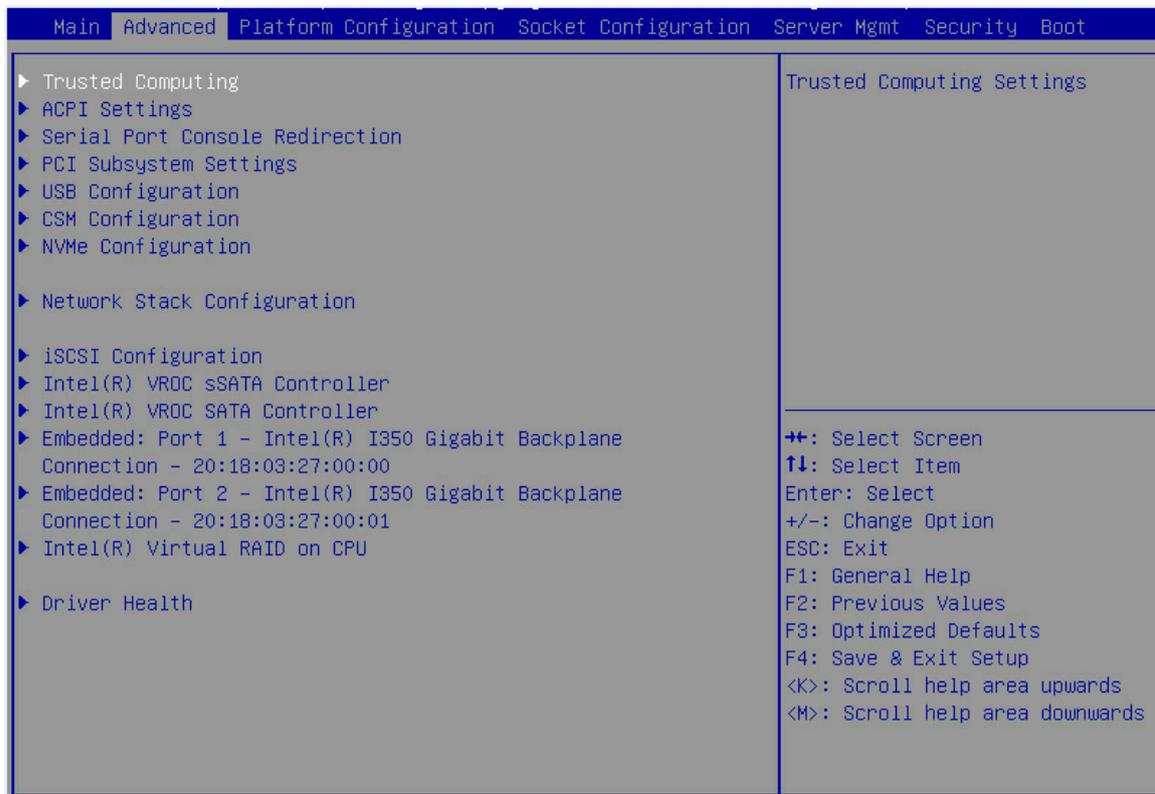


表3-2 Advanced 界面参数

界面参数	功能说明
Trusted Computing	可信计算配置菜单。
ACPI Settings	高级配置和电源接口配置菜单。
Serial Port Console Redirection	串口控制台重定向配置菜单。
PCI Subsystem Settings	PCI子系统配置菜单。
USB Configuration	USB配置菜单。
CSM Configuration	CSM配置菜单。
NVMe Configuration	NVMe配置菜单。
Network PXE Control	网卡PXE功能控制菜单。
Network Stack Configuration	网络堆栈配置菜单。
Intel(R) VROC sSATA Controller	sSATA虚拟RAID配置菜单，当PCH sSATA Configuration下将sSATA模式配置为RAID时显示该选项。
Intel(R) VROC SATA Controller	SATA虚拟RAID配置菜单，当PCH SATA Configuration下将SATA模式配置为RAID时显示该选项。
Slot3 mLom:Port x – Intel(R) I350 Gigabit Backplane Connection – 20:18:03:27:00:00	网卡端口的配置菜单。

界面参数	功能说明
Intel(R) Virtual RAID on CPU	NVMe虚拟RAID配置菜单，该选项在VMD功能未开启时不显示。
Intel(R) Optane(TM) DC Persistent Memory Configuration	Intel DCPMM内存配置菜单。该选项仅在接入Intel DCPMM内存时显示。
Driver Health	驱动/控制器的健康状态，仅UEFI启动模式下支持该功能。

### 3.2.1 Trusted Computing 界面

如图 3-3 所示，通过Trusted Computing 界面可以配置安全设备。具体参数说明如表 3-3 所示。

图3-3 Trusted Computing 界面

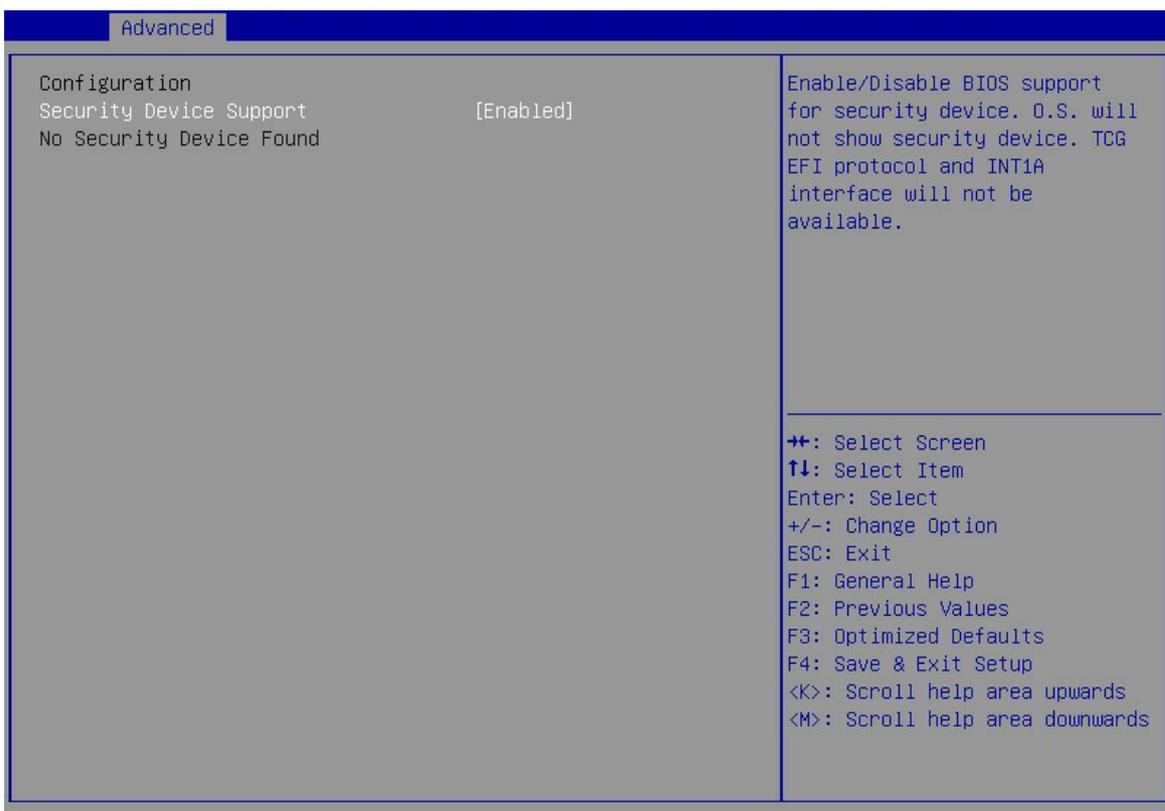


表3-3 Trusted Computing 界面参数

界面参数	功能说明
Security Device Support	对安全设备的支持使能开关，菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：使能对安全设备的支持。</li> <li>Disabled：禁止对安全设备的支持。</li> </ul>

#### 1. TPM 安全设备界面

安装TPM2.0 安全设备，TPM2.0 界面如图 3-4 所示，具体参数说明如表 3-4 所示。

图3-4 TPM2.0 界面

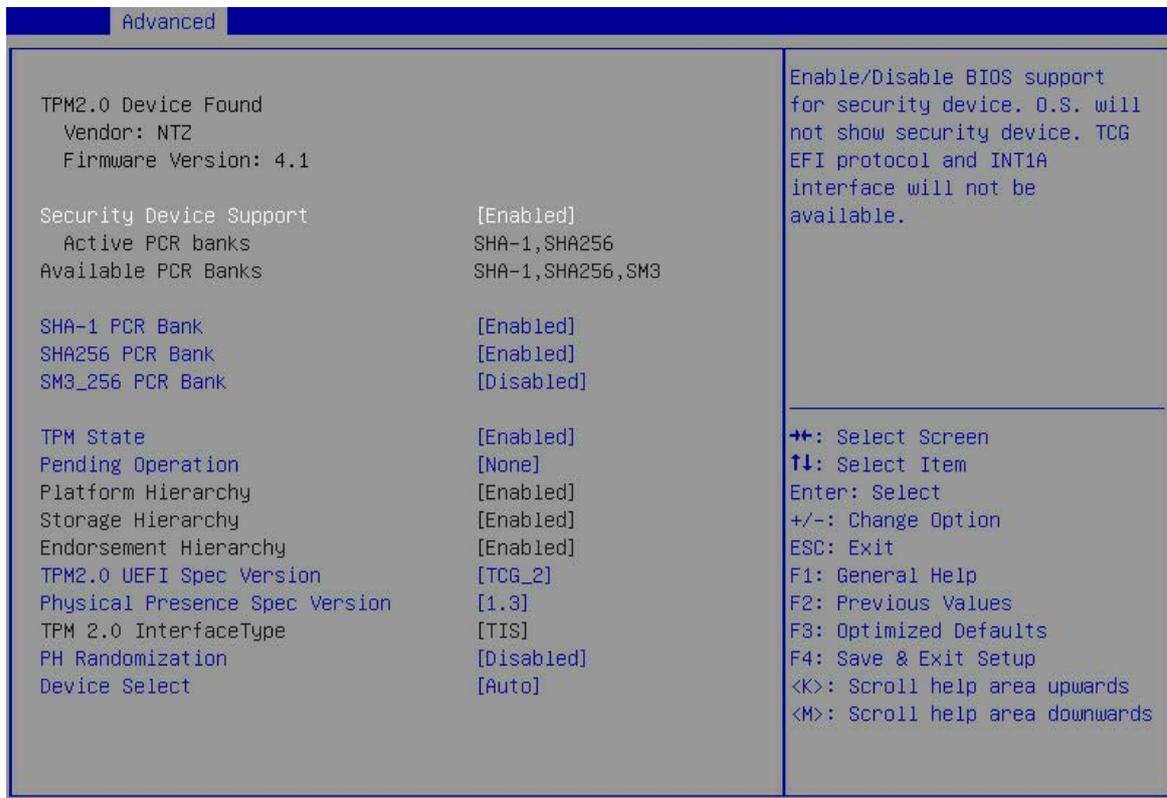


表3-4 TPM2.0 界面参数

界面参数	功能说明
Security Device Support	对安全设备的支持使能开关，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：使能对安全设备的支持。</li> <li>Disabled：禁止对安全设备的支持。</li> </ul>
Active PCR Banks	显示正在使用的PCR Banks。
Available PCR Banks	显示可用的PCR Banks。
SHA-1 PCR Bank	SHA-1 PCR Bank启用配置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 SHA-1 PCR Bank。</li> <li>Disabled：禁用 SHA-1 PCR Bank。</li> </ul>
SHA256 PCR Bank	SHA256 PCR Bank启用配置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 SHA256 PCR Bank。</li> <li>Disabled：禁用 SHA256 PCR Bank。</li> </ul>
SM3_256 PCR Bank	SM3_256 PCR Bank启用配置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 SM3_256 PCR Bank。</li> <li>Disabled：禁用 SM3_256 PCR Bank。</li> </ul>

界面参数	功能说明
TPM State	TPM状态开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用 TPM。</li> <li>• Disabled：禁用 TPM。</li> </ul>
Pending Operation	控制设备的安全操作，菜单选项为： <ul style="list-style-type: none"> <li>• None（缺省）：无操作。</li> <li>• TPM Clear：清除 TPM 的度量值。</li> </ul>
Platform Hierarchy	平台等级开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启平台等级功能。</li> <li>• Disabled：关闭平台等级功能。</li> </ul>
Storage Hierarchy	存储等级开关，存储等级由平台固件控制，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启存储等级功能。</li> <li>• Disabled：关闭存储等级功能。</li> </ul>
Endorsement Hierarchy	认可等级开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启认可等级功能。</li> <li>• Disabled：关闭认可等级功能。</li> </ul>
TPM 2.0 UEFI Spec Version	选择支持的TCG规范版本，菜单选项为： <ul style="list-style-type: none"> <li>• TCG_1_2：兼容 win8/win10 的模式。</li> <li>• TCG_2（缺省）：支持 TCG2 协议和事件格式，提供 win10 及以上的支持。</li> </ul>
Physical Presence Spec Version	选择上报给OS的支持PPI规范的版本号。菜单选项为： <ul style="list-style-type: none"> <li>• 1.2：支持的 PPI 规范为 1.2 版本。</li> <li>• 1.3（缺省）：支持的 PPI 规范为 1.3 版本。一些 HCK 测试可能不支持 1.3。</li> </ul>
TPM 2.0 InterfaceType	显示TPM 2.0接口类型
PH Randomization	平台等级随机性使能开关，仅用作开发阶段测试使用，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启平台等级随机性功能。</li> <li>• Disabled（缺省）：关闭平台等级随机性功能。</li> </ul>
Device Select	选择支持的TPM版本，菜单选项为： <ul style="list-style-type: none"> <li>• TCM 1.0：仅支持 TCM 1.0。</li> <li>• TPM 2.0：仅支持 TPM 2.0。</li> <li>• Auto（缺省）：同时支持 TPM 2.0 和 TCM 1.0，若系统检测不到 TPM 2.0，则将枚举 TCM 1.0。</li> </ul>

## 2. TCM 安全设备界面

安装TCM 1.0 安全设备，TCM界面如[图 3-5](#)所示，具体参数说明如[表 3-5](#)所示。

图3-5 TCM 界面



表3-5 TCM 界面参数

界面参数	功能说明
<b>Configuration</b>	
Security Device Support	对安全设备的支持使能开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：使能对安全设备的支持。</li> <li>• Disabled: 禁止对安全设备的支持。</li> </ul>
TCM State	TCM状态开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用 TCM。</li> <li>• Disabled: 禁用 TCM。</li> </ul>
Pending Operation	控制设备的安全操作，菜单选项为： <ul style="list-style-type: none"> <li>• None（缺省）：无操作。</li> <li>• TCM Clear: 清除 TCM 的度量值。</li> </ul>
Device Select	选择支持的TPM版本，菜单选项为： <ul style="list-style-type: none"> <li>• TCM 1.0: 仅支持 TCM 1.0。</li> <li>• TPM 2.0: 仅支持 TPM 2.0。</li> <li>• Auto（缺省）：同时支持 TPM 2.0 和 TCM 1.0，缺省为 TPM 2.0，若系统检测不到 TPM 2.0，则将枚举 TCM 1.0。</li> </ul>

界面参数	功能说明
<b>Current Status Information</b>	
TCM Enabled Status	显示TCM的使能状态， Enabled表示已启用TCM， Disabled表示已禁用TCM。
TCM Active Status	显示TCM的激活状态， Activated表示TCM已激活， Deactivated表示TCM未激活。
TCM Ower Status	显示TCM的归属状态， Owned表示TCM存在归属， Unowned表示TCM无归属。

### 3.2.2 ACPI Settings 界面

如图 3-6 所示，通过ACPI Settings界面，可以对高级电源管理相关功能进行配置。具体参数说明如表 3-6 所示。

图3-6 ACPI Settings 界面

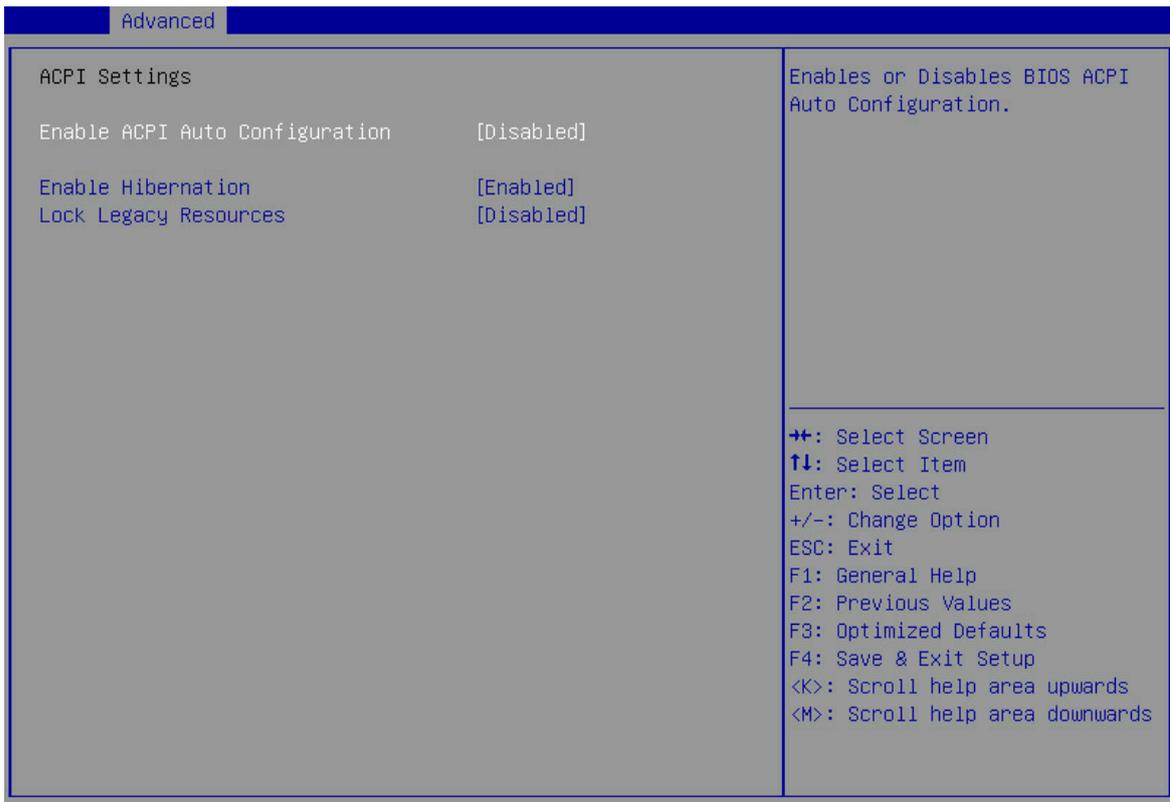


表3-6 ACPI Settings 界面参数

界面参数	功能说明
Enable ACPI Auto Configuration	ACPI自动配置开关，开启该功能后，操作系统可以合理控制和分配服务器硬件设备的电源使用情况，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启 ACPI 自动配置功能。</li> <li>Disabled (缺省): 关闭 ACPI 自动配置功能。</li> </ul>

界面参数	功能说明
Enable Hibernation	系统休眠功能开关，该选项对一些OS可能不起作用。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启系统休眠功能。</li> <li>• Disabled：关闭系统休眠功能。</li> </ul>
Lock Legacy Resources	锁定传统资源设置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启锁定传统资源功能。</li> <li>• Disabled（缺省）：关闭锁定传统资源功能。</li> </ul>

### 3.2.3 Serial Port Console Redirection 界面

如图 3-7 所示，通过 Serial Port Console Redirection 界面，可以配置串口重定向功能。具体参数说明如表 3-7 所示。

图3-7 Serial Port Console Redirection 界面

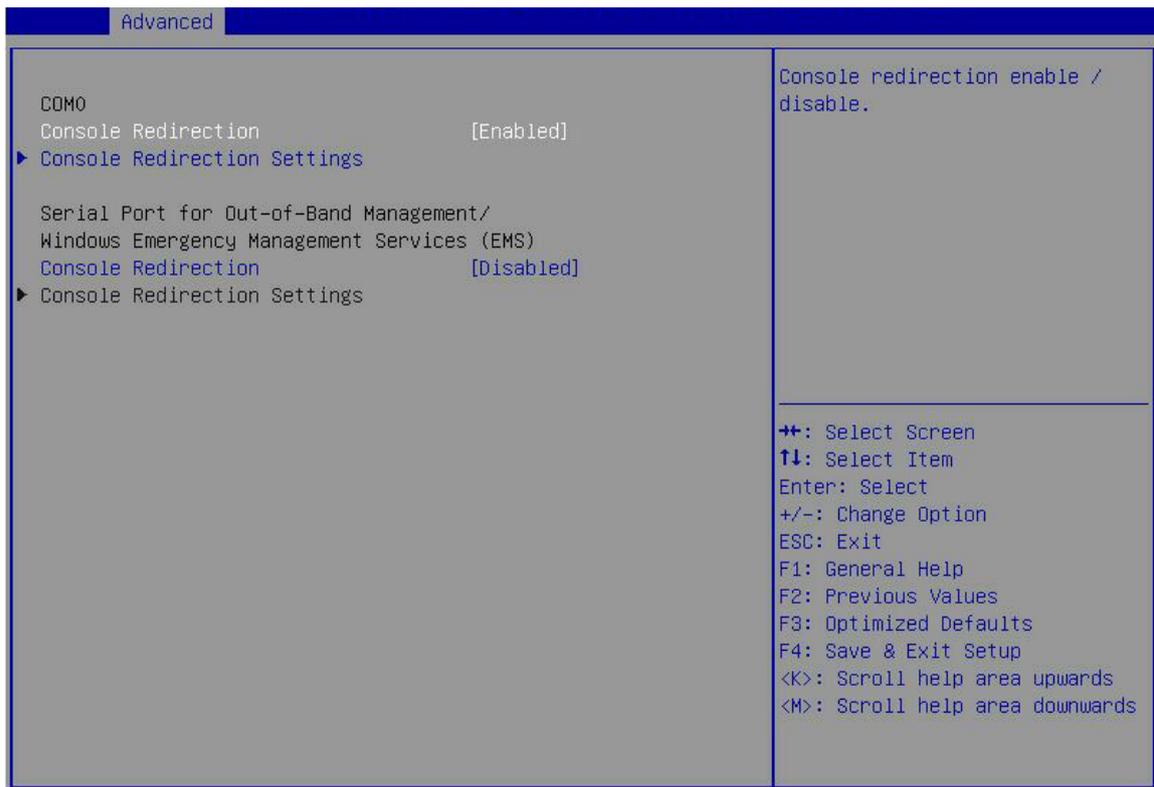


表3-7 Serial Port Console Redirection 界面参数

界面参数	功能说明
COM0	COM0端口

界面参数	功能说明
Console Redirection	串口重定向配置开关，将指定的物理串口或虚拟串口的数据映射到指定的系统串口，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启串口重定向功能。开启后可对 <b>Console Redirection Settings</b> 菜单进行配置。</li> <li>• Disabled：关闭串口重定向功能。</li> </ul>
Console Redirection Settings	串口重定向配置菜单，COM0端口的Console Redirection设置为Enabled时，该选项可用，界面如 <a href="#">图3-8</a> 所示，具体参数说明如 <a href="#">表3-8</a> 所示。
Serial Port for Out-of-Band Management/Windows Emergency Management Services（EMS）	用于带外管理/Windows紧急管理服务的串口
Console Redirection	串口重定向开关，用于Windows紧急管理服务的串口重定向，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启串口重定向功能。</li> <li>• Disabled（缺省）：关闭串口重定向功能。</li> </ul>
Console Redirection Settings	串口重定向配置菜单，用于Windows界面的串口重定向参数配置，Console Redirection设置为Enabled时，该选项可用，界面如 <a href="#">图3-9</a> 所示。具体参数说明如 <a href="#">表3-9</a> 所示。

### 1. Console Redirection Settings（COM0 端口）界面

COM0 端口的Console Redirection Settings界面如[图 3-8](#)所示。具体参数说明如[表 3-8](#)所示。

图3-8 COM0 端口的 Console Redirection Settings 界面

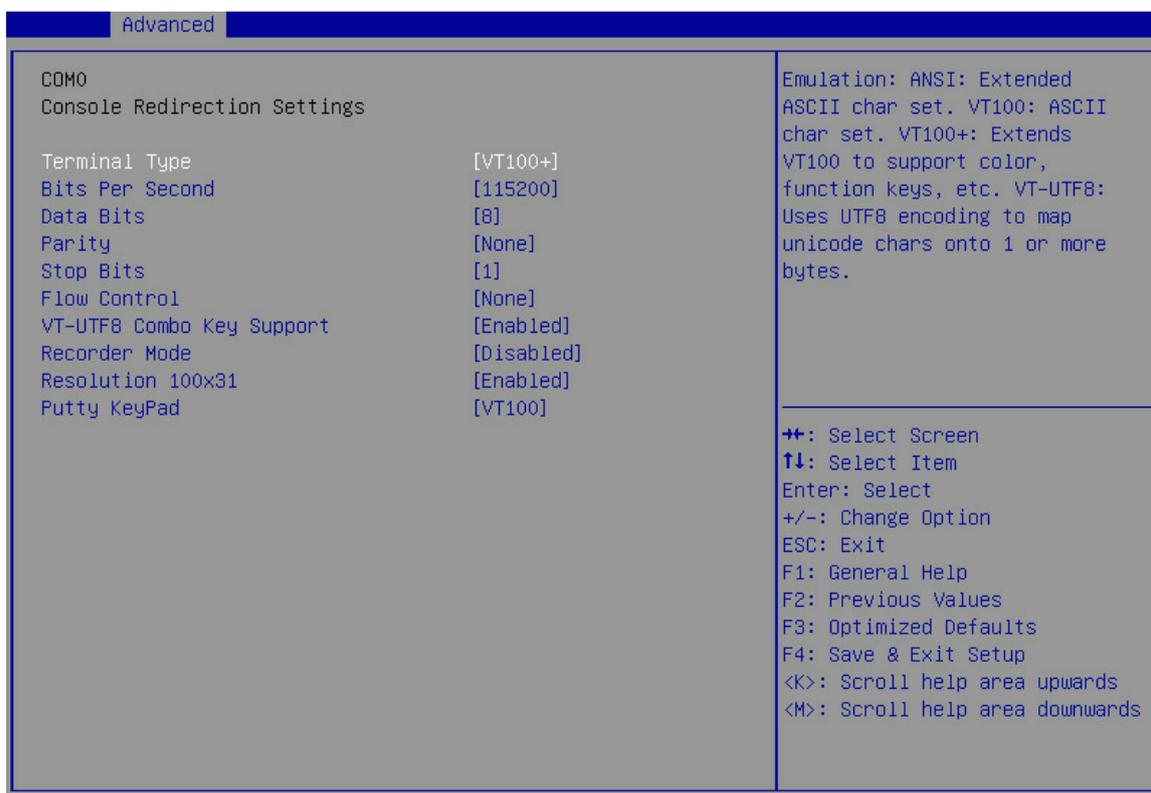


表3-8 COM0 端口的 Console Redirection Settings 界面参数

界面参数	功能说明
Terminal Type	终端类型配置，菜单选项为： <ul style="list-style-type: none"> <li>• VT100: ASCII 字符集。</li> <li>• VT100+ (缺省): 扩展的 VT100, 用于支持颜色显示、功能键等。</li> <li>• VT-UTF8: 使用 UTF8 编码映射 unicode 字符到 1 个或多个字节。</li> <li>• ANSI: 扩展 ASCII 字符集。</li> </ul>
Bits Per Second	每秒传输比特数配置，传输速度必须和对端串口匹配，超长或嘈杂的线路可能需要较低的速度，菜单选项为： <ul style="list-style-type: none"> <li>• 9600</li> <li>• 19200</li> <li>• 38400</li> <li>• 57600</li> <li>• 115200 (缺省)</li> </ul>
Data Bits	每字节中实际数据所占的比特数配置，菜单选项为： <ul style="list-style-type: none"> <li>• 7</li> <li>• 8 (缺省)</li> </ul>
Parity	奇偶校验功能，奇偶位与数据位一起发送用于检测传输错误，可能的选项有： <ul style="list-style-type: none"> <li>• None: 关闭校验功能。</li> <li>• Even: 偶校验。</li> <li>• Odd: 奇校验。</li> <li>• Mark: 标记奇偶校验。奇偶校验位始终用值 1 “标记”。如果标记奇偶校验位的值为 0, 否则发生错误。</li> <li>• Space: 空间奇偶校验。奇偶校验位始终为 0, 否则发生错误。</li> </ul>
Stop Bits	停止位（单个数据包的最后位），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，菜单选项为： <ul style="list-style-type: none"> <li>• 1 (缺省)</li> <li>• 2</li> </ul>
Flow Control	流控制配置，用于防止数据从缓冲区溢出导致数据丢失，菜单选项为： <ul style="list-style-type: none"> <li>• None (缺省): 不进行流控制。</li> <li>• Hardware RTS/CTS: 通过硬件请求发送协议/清除发送协议进行流控制。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。</li> </ul>
VT-UTF8 Combo Key Support	VT-UTF8 组合键支持，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 开启 VT-UTF8 组合键支持 ANSI/VT100 终端。</li> <li>• Disabled: 关闭 VT-UTF8 组合键支持 ANSI/VT100 终端。</li> </ul>
Recorder Mode	记录器模式，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 开启记录器模式，用于捕获终端文本数据。</li> <li>• Disabled (缺省): 关闭记录器模式，</li> </ul>

界面参数	功能说明
Resolution 100×31	设置扩展终端分辨率为100x31。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用扩展终端分辨率。</li> <li>• Disabled：禁用扩展终端分辨率。</li> </ul>
Putty KeyPad	Putty小键盘，菜单选项为： <ul style="list-style-type: none"> <li>• VT100（缺省）</li> <li>• LINUX</li> <li>• XTERMR6</li> <li>• SCO</li> <li>• ESCN</li> <li>• VT400</li> </ul>

## 2. Console Redirection Settings（EMS 端口）界面

EMS的Console Redirection Settings界面如[图 3-9](#)所示。具体参数说明如[表 3-9](#)所示。

图3-9 Console Redirection Settings 界面

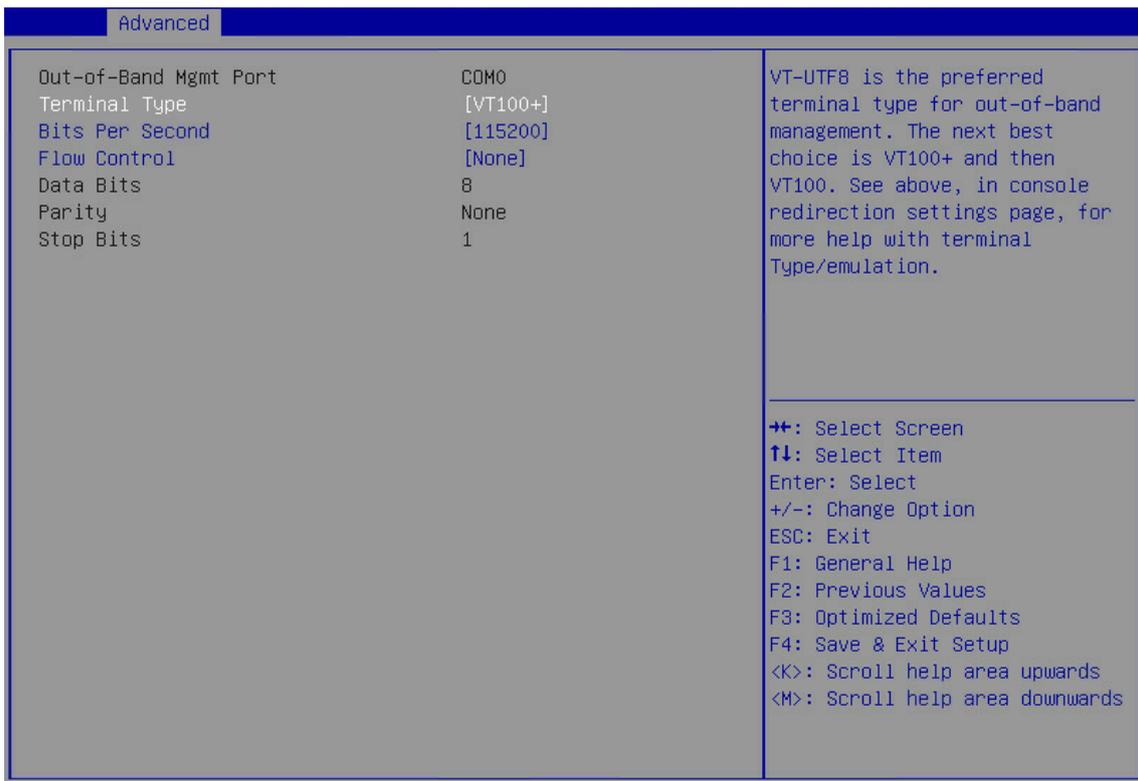


表3-9 EMS 的 Console Redirection Settings 界面参数

界面参数	功能说明
Out-of-Band Mgmt Port	带外管理串口，通过该串口可以访问Windows操作系统、收集操作系统的故障信息。

界面参数	功能说明
Terminal Type	终端类型配置，菜单选项为： <ul style="list-style-type: none"> <li>• VT100: ASCII 字符集。</li> <li>• VT100+ (缺省): 扩展的 VT100, 用于支持颜色显示、功能键等。</li> <li>• VT-UTF8: 使用 UTF8 编码映射 unicode 字符到 1 个或多个字节。</li> <li>• ANSI: 扩展 ASCII 字符集。</li> </ul>
Bits Per Second	每秒传输比特数配置，菜单选项为： <ul style="list-style-type: none"> <li>• 9600</li> <li>• 19200</li> <li>• 57600</li> <li>• 115200 (缺省)</li> </ul>
Flow Control	流控制配置，用于防止数据从缓存中溢出，菜单选项为： <ul style="list-style-type: none"> <li>• None (缺省): 不进行流控制。</li> <li>• Hardware RTS/CTS: 通过硬件请求发送协议/清除发送协议进行流控制。</li> <li>• Software Xon/Xoff: 通过 Xon/Xoff 进行流控制。Xon/Xoff 是一种通信速率匹配协议，当数据传输速率大于等于 1200b/s 时，通过控制发送方的发送速率以匹配双方的速率。</li> </ul>
Data Bits	显示串口数据位宽，表示通信中实际的数据位。
Parity	显示奇偶校验功能，奇偶位与数据位一起发送用于检测传输错误，可能的选项有： <ul style="list-style-type: none"> <li>• None: 关闭校验功能。</li> <li>• Even: 偶校验。</li> <li>• Odd: 奇校验。</li> <li>• Mark: 标记奇偶校验。奇偶校验位始终用值 1 “标记”。如果标记奇偶校验位的值为 0, 否则发生错误。</li> <li>• Space: 空间奇偶校验。奇偶校验位始终为 0, 否则发生错误。</li> </ul>
Stop Bits	显示停止位 (单个数据包的最后一位)。

### 3.2.4 PCI Subsystem Settings 界面

如[图 3-10](#)所示，通过 PCI Subsystem Settings 界面，可以对 PCI 子系统进行配置。具体参数说明如[表 3-10](#)所示。

图3-10 PCI Subsystem Settings 界面

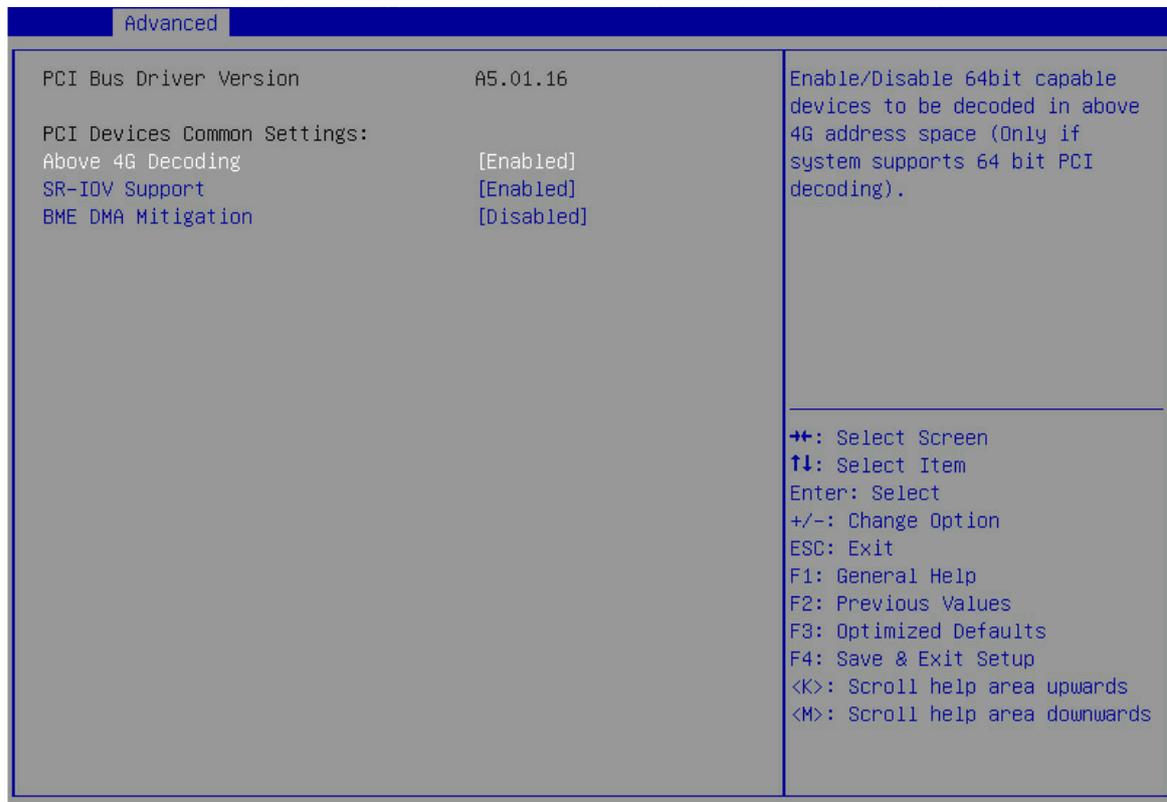


表3-10 PCI Subsystem Settings 界面参数

界面参数	功能说明
PCI Bus Driver Version	PCI总线驱动版本。
<b>PCI Devices Common Settings</b>	
Above 4G Decoding	<p>4G以上内存访问控制设置，当系统支持64位PCIe解码时，在4G以上地址空间对64位设备进行解码，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled (缺省)：开启 4G 以上译码。</li> <li>Disabled：关闭 4G 以上译码。</li> </ul> <p>Above 4GB decoding设为“Disabled”时会导致显存超过4GB的PCIe设备无法解码，如M60、K80等显卡在Above 4GB Decoding设置为“Disabled”的情况下会停在EarlyPOST 100%的地方，导致无法进入BIOS Setup或者OS。</p>
SR-IOV Support	<p>SR-IOV (Single Root I/O Virtualization) 支持设置。SR-IOV技术的主要作用是将一个物理PCIe设备模拟成多个虚拟设备，其中每一个虚拟设备可以与一个虚拟机绑定，便于不同的虚拟机访问同一个物理PCIe设备。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 SR-IOV 机制。如系统中有支持 SR-IOV 的 PCIe 设备，由 BIOS 分配虚拟化 IO 资源。</li> <li>Disabled：禁用 BIOS 对 SR-IOV 机制的支持。如果 PCIe 卡支持 SR-IOV，则由 OS 分配虚拟化 IO 资源。</li> </ul>

界面参数	功能说明
BME DMA Mitigation	<p>BME DMA 缓解，用于防止 DMA 侧信道攻击，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启该功能后可防止 DMA 侧信道攻击。</li> <li>Disabled(缺省): 关闭该功能后, 在 PCI 枚举到 PCI to PCI bridge 时, 不会阻止 DMA 的访问, 如 <code>nvidia-smi</code> 命令可正常使用。</li> </ul>

### 3.2.5 USB Configuration 界面

如图 3-11 所示，通过 USB Configuration 界面，可以查看 USB 设备信息及进行配置。具体参数说明如表 3-11 所示。

图3-11 USB Configuration 界面

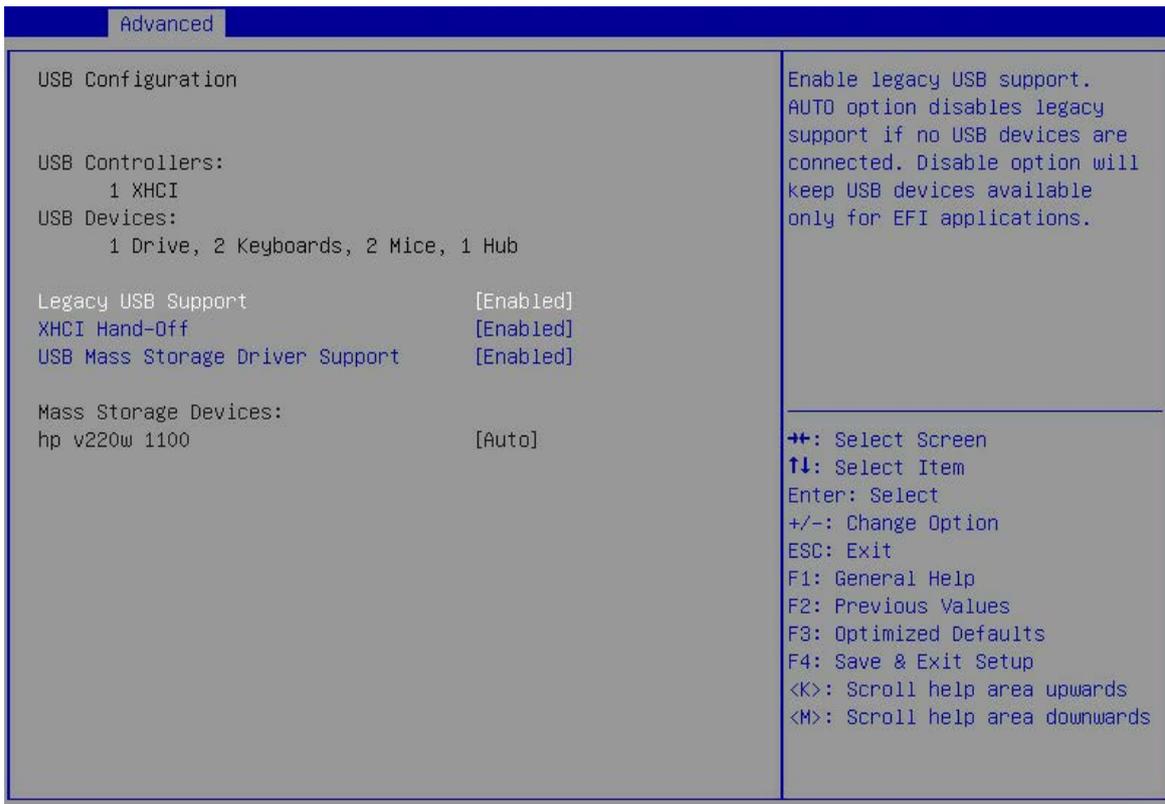


表3-11 USB Configuration 界面参数

界面参数	功能说明
USB Controllers	<p>显示USB控制器信息。</p> <ul style="list-style-type: none"> <li>XHCI: XHCI 控制器，支持 USB3.0。</li> </ul>

界面参数	功能说明
USB Devices	<p>显示USB设备信息。</p> <ul style="list-style-type: none"> <li>• Drives: 当前连接 Drives 的数量, Drive 包含物理设备和虚拟设备。</li> <li>• Keyboard: 当前连接的键盘数。</li> <li>• Mouse: 当前连接的鼠标数。</li> <li>• Hub: 当前连接的 USB Hub 数, 服务器内置了 1 个 USB Hub。</li> </ul>
Legacy USB Support	<p>支持传统USB设备功能, 菜单选项为:</p> <ul style="list-style-type: none"> <li>• Enabled (缺省): 支持传统 USB 设备。</li> <li>• Disabled: 不支持传统 USB 设备, 服务器仅在 EFI 应用程序下确保 USB 设备可用。</li> <li>• Auto: 自动选择, 如果有 USB 设备连接时, 将开启该功能; 如果没有 USB 设备连接时, 将关闭该功能。</li> </ul>
XHCI Hand-off	<p>可扩展主机控制器接口配置, 适用于USB3.0, 用于对USB 3.0 XHCI控制权的管理, 菜单选项为:</p> <ul style="list-style-type: none"> <li>• Enabled (缺省): 开启可扩展主机控制器接口功能。</li> <li>• Disabled: 关闭可扩展主机控制器接口功能。</li> </ul>
USB Mass Storage Driver Support	<p>支持大容量USB存储设备, 菜单选项为:</p> <ul style="list-style-type: none"> <li>• Enabled (缺省): 支持大容量 USB 存储设备。</li> <li>• Disabled: 不支持大容量 USB 存储设备。</li> </ul>
<b>Mass Storage Devices</b>	
Dual SD Card RAID LUN	<p>当安装Dual SD卡扩展模块及SD卡时显示该选项, 需要注意的是:</p> <ul style="list-style-type: none"> <li>• Dual SD 卡扩展模块不支持热插拔, SD 卡支持热插拔。</li> <li>• 为实现 1+1 冗余, 避免 SD 卡上的存储空间浪费, 请在 Dual SD 卡扩展模块上安装 2 张容量相同的 SD 卡。</li> <li>• 当任意一张 SD 卡出现故障需要更换时, 若在服务器上电状态下进行更换, 更换完成后, 需将服务器重启。重启完成后, 系统会在新插入的 SD 卡上重建故障 SD 卡的数据。</li> </ul>
SanDisk	U盘存储设备 (闪迪)。
ASUS SDR-08B1-U A A301	USB光驱 (华硕)。
Hp v220w 1100	U盘存储设备 (惠普)。
KingstonDataTraveler 3.0PMAP	U盘存储设备 (金士顿)。
AMI Virtual CDROM 1.00	虚拟光驱。

### 3.2.6 CSM Configuration 界面

如图 3-12 所示, 通过 CSM Configuration 界面, 可以对兼容性支持模块进行配置。具体参数说明如表 3-12 所示。

图3-12 CSM Configuration 界面

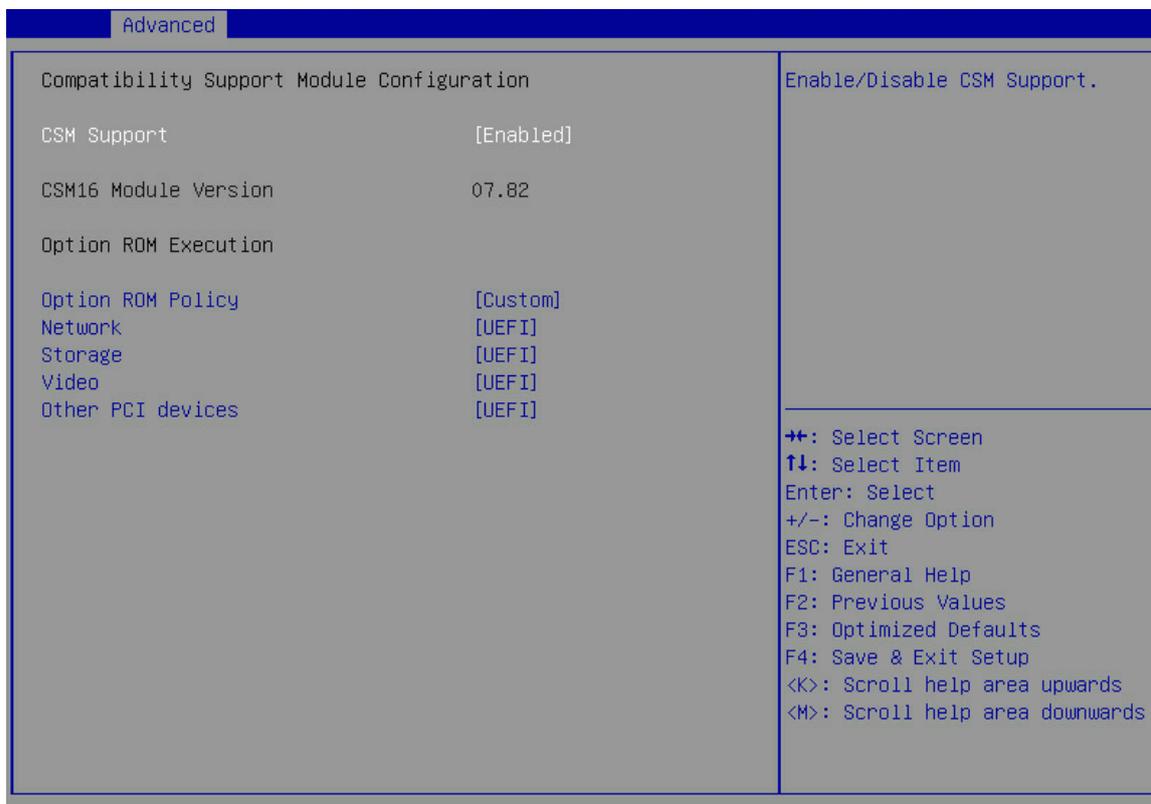


表3-12 CSM Configuration 界面参数

界面参数	功能说明
CSM Support	<p>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，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 CSM 功能。</li> <li>Disabled：关闭 CSM 功能。</li> </ul> <p>需要注意的是，Legacy启动模式下，该功能会一直处于开启状态。</p>
CSM16 Module Version	CSM16模块的版本号
Option ROM Execution	OptionRom执行配置
Option ROM Policy	<p>OptionRom 执行策略，菜单选项为：</p> <ul style="list-style-type: none"> <li>Auto(缺省): 使UEFI OptionROM运行在 UEFI 启动模式下, Legacy OptionRom 运行在 Legacy 启动模式下。</li> <li>Custom: 用户需根据 BIOS 启动模式设置相匹配的策略。错误的设置会导致某些 OptionROM无法执行，建议保持该设置为默认的 Auto 模式。</li> </ul>
Network	<p>设置网卡Option ROM的加载方式，Option ROM Policy设置为Custom时，该选项可用，菜单选项为：</p> <ul style="list-style-type: none"> <li>UEFI（缺省）：加载网卡在 UEFI 启动模式下的 Option ROM。</li> <li>Legacy：加载网卡在 Legacy 启动模式下的 Option ROM。Legacy 启动模式下，缺省加载 Legacy 模式的 Option Rom。</li> </ul>

界面参数	功能说明
Storage	设置存储设备Option ROM的加载方式，Option ROM Policy设置为Custom时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• UEFI（缺省）：加载存储设备在UEFI启动模式下的Option ROM。</li> <li>• Legacy：加载存储设备在Legacy启动模式下的Option ROM。Legacy启动模式下，缺省加载Legacy模式的Option Rom。</li> </ul>
Video	设置显示设备Option ROM的加载方式，Option ROM Policy设置为Custom时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• UEFI（缺省）：加载显示设备在UEFI启动模式下的Option ROM。</li> <li>• Legacy：加载显示设备在Legacy启动模式下的Option ROM。Legacy启动模式下，缺省加载Legacy模式的Option Rom。</li> </ul>
Other PCI Devices	设置其他PCI设备Option ROM的加载方式，比如Input设备，Option ROM Policy设置为Custom时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• UEFI（缺省）：加载其他PCI设备在UEFI启动模式下的Option ROM。</li> <li>• Legacy：加载其他PCI设备在Legacy启动模式下的Option ROM。Legacy启动模式下，缺省加载Legacy模式的Option Rom。</li> </ul>

### 3.2.7 NVMe Configuration 界面

如[图 3-13](#)所示，NVMe Configuration界面显示不带OptionRom的NVMe设备信息。具体参数说明如[表 3-13](#)所示。

图3-13 NVMe Configuration 界面

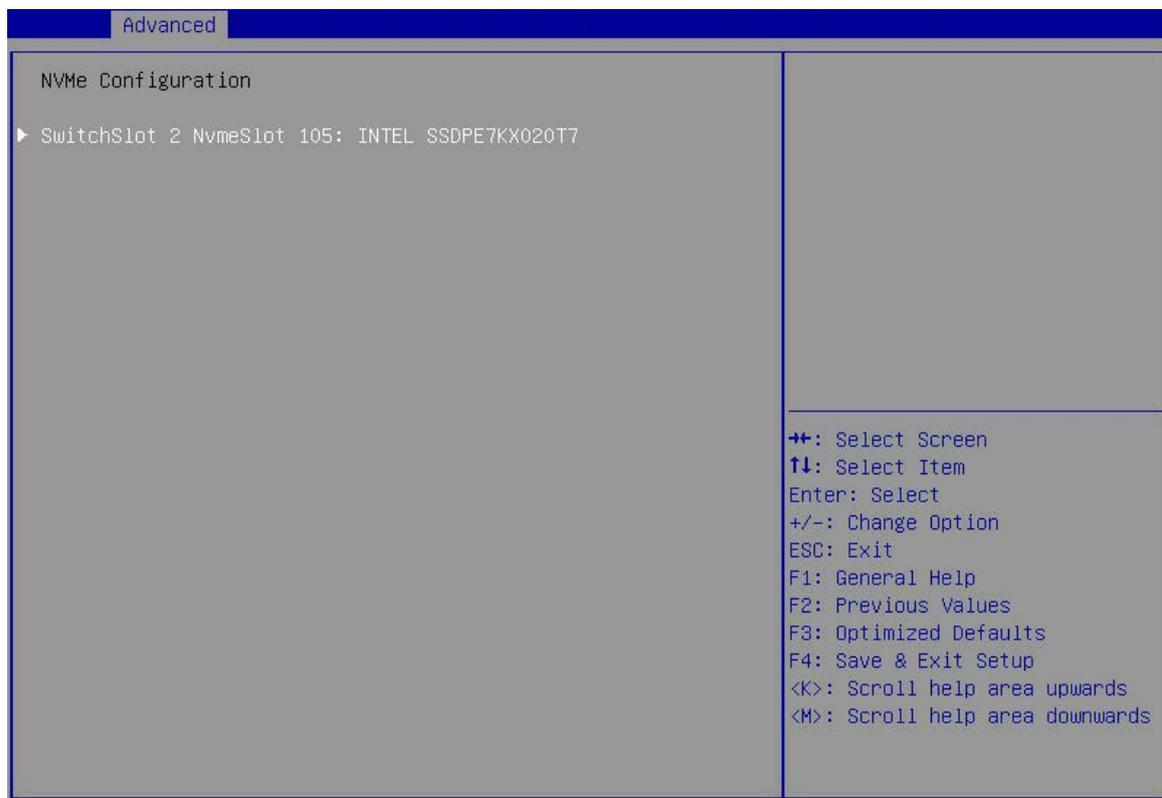


表3-13 NVMe Configuration 界面参数

界面参数	功能说明
SwitchSlot 2 NvmeSlot 105: INTEL SSDPE7KX020T7	可用的NVMe设备配置菜单 不同服务器的NVMe逻辑槽位号显示规则不同，可参见表3-14。

表3-14 NVMe 逻辑槽位号说明

产品名称	NVMe 逻辑槽位号说明
UNISINSIGHT AIX R6220L-G3	<p>显示示例：Slot 203。</p> <ul style="list-style-type: none"> <li>12LFF 硬盘机型，NVMe Slot 号显示为 Slot 200 ~Slot 203。</li> <li>24LFF 硬盘机型中，分两种情况。 <ul style="list-style-type: none"> <li>支持 8 个 NVMe 硬盘的机型，Slot 号显示为 Slot 200 ~Slot 207。</li> <li>支持 4 个 NVMe 硬盘的机型，Slot 号显示为 Slot 204 ~Slot 207。</li> </ul> </li> </ul>

如图 3-14所示，通过SwitchSlot 2 NvmeSlot 105: INTEL SSDPE7KX020T7（该NVMe设备信息）界面，可以查看该NVMe设备相关信息。具体参数说明如表 3-15所示。

图3-14 SwitchSlot 2 NvmeSlot 105: INTEL SSDPE7KX020T7 界面

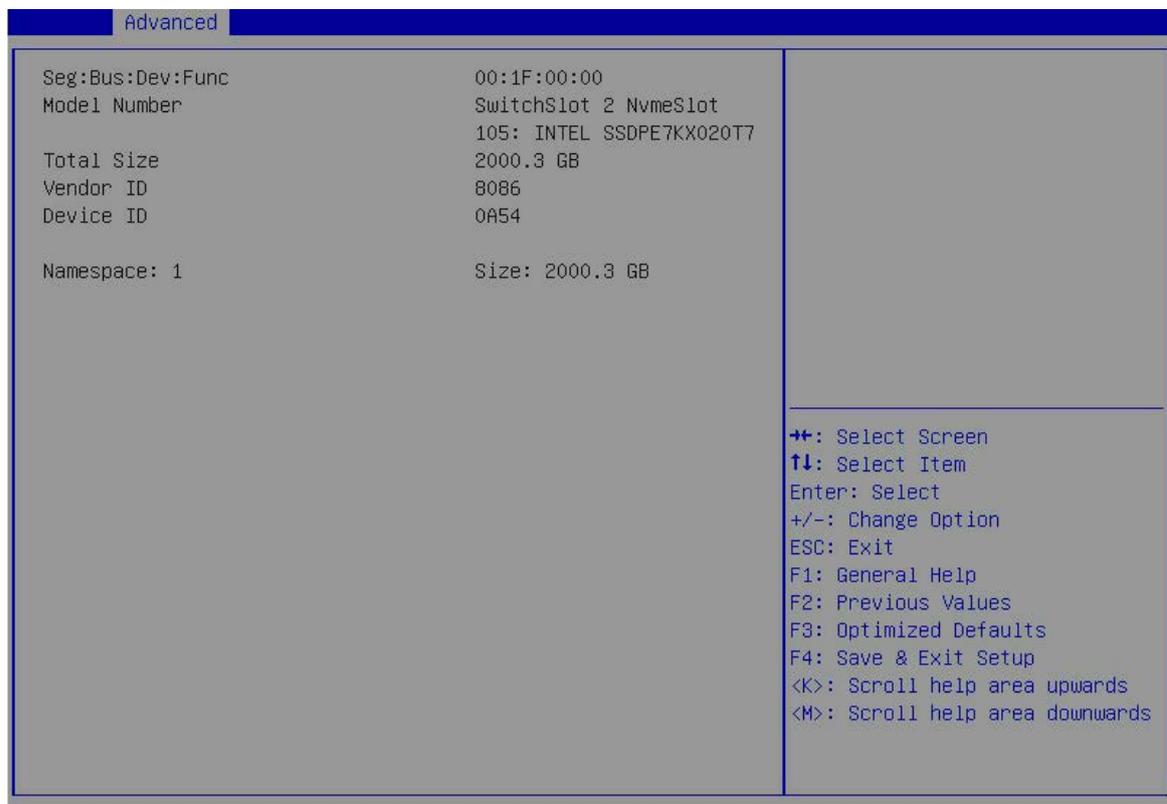


表3-15 SwitchSlot 2 NvmeSlot 105: INTEL SSDPE7KX020T7 (该 NVMe 设备信息) 界面参数

界面参数	功能说明
Seg:Bus:Dev:Func	该NVMe设备Seg:Bus:Dev:Func信息。
Model Number	该NVMe设备的类型号码。
Total Size	该NVMe设备的大小。
Vendor ID	该NVMe设备的供应商ID。
Device ID	该NVMe设备的设备ID。
Namespace	该NVMe设备的命名空间。

### 3.2.8 iMS Configuration 界面

如图 3-15 所示，通过 iMS Configuration 界面，可以通过 iMS 工具对内存进行检测。具体参数说明如表 3-16 所示。

IMS (Intelligent Memory Surveillance, 智能内存检测)，是一套完整的内存错误和故障校验、诊断和处理方法，具备内存检测、失效隔离和预警等完整的内存管理功能，解决了内存故障无法修复导致停机、故障难于定位、个别错误导致大规模内存浪费等内存错误和故障处理难题。

图3-15 iMS Configuration 界面

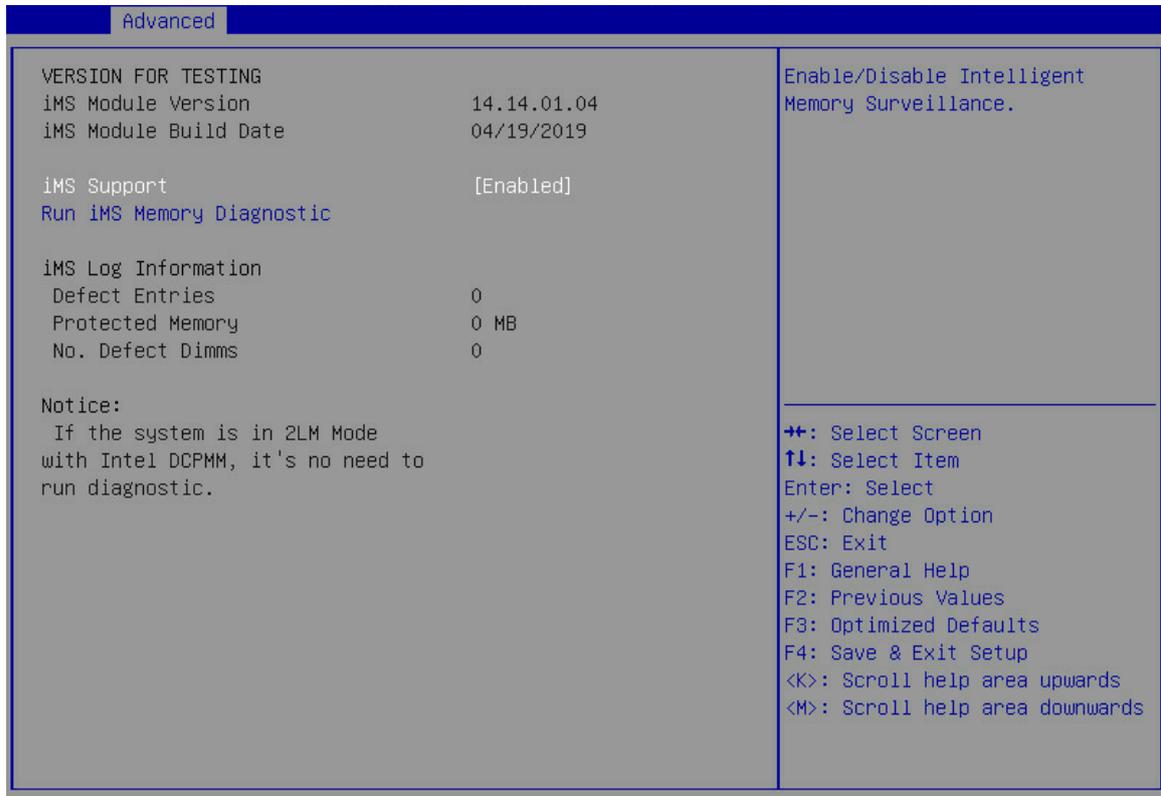


表3-16 iMS Configuration 界面参数

界面参数	功能说明
iMS Module Version	显示iMS模块版本。
iMS Module Build Date	显示iMS模块编译日期。
iMS Support	iMS支持。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 iMS 工具。启用后进入操作系统，iMS 会实时进行内存的监测、保护和处理。</li> <li>Disabled：禁用 iMS 工具。</li> </ul>
Run iMS Memory Diagnostic	运行iMS内存测试。如果系统Intel DCPMM处于2LM Mode，无需运行该测试。
iMS Log Information	iMS日志信息。
Defect Entries	检测到的缺陷内存条目，最小单位为页。
Protected Memory	受保护的内存容量，单位为MB。
No. Defect Dimms	显示缺陷内存条。

Run iMS Memory Diagnostic界面参数如[图 3-16](#)所示，具体参数说明如[表 3-17](#)所示。

图3-16 Run iMS Memory Diagnostic 界面

```
iMS Memory Diagnostic
Version 2.2.3 (22/05/2019)
Copyright KingTiger Technology

Intel(R) Xeon(R) Gold 6150 CPU @ 2.70GHz

Please select test mode: 1:Quick, 2:Standard(Default), 3:Extensive, ESC:Exit
```

表3-17 Run iMS Memory Diagnostic 参数

参数	功能说明
Test mode	可选择三种不同强度的内存测试模式，包括： <ul style="list-style-type: none"><li>• Quick: 输入 1，进入快速内存测试。</li><li>• Standard: 输入 2，进入标准内存测试。</li><li>• Extensive: 输入 3，进入强化内存测试。</li><li>• Exit: 按 ESC 退出 iMS 内存测试。测试完成后按任意键重启服务器。</li></ul>

### 3.2.9 Network PXE Control 界面

如[图 3-17](#)所示，通过Network PXE Control界面，可以对网口的PXE功能进行设置。具体参数说明如[表 3-18](#)所示。

图3-17 Network PXE Control 界面



表3-18 Network PXE Control 界面参数

界面参数	功能说明
PCIE Slot 3 (mLOM)	用PCIE Slot号来标识网卡，mLOM指网卡类型。

网卡PXE功能控制界面参数如[图 3-18](#)所示，具体参数说明如[表 3-19](#)所示。

图3-18 网卡 PXE 功能控制界面



表3-19 网卡 PXE 功能控制界面参数

界面参数	功能说明
Network Function	网卡功能控制。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用网卡。</li> <li>• Disabled: 禁用网卡。禁用时，网卡的 PXE 功能不可用，不再生成网卡的 PXE 启动项，且操作系统下将无法使用该网卡。</li> </ul>
Port X	网卡端口号，从0开始。当Network Function选项为Enabled时显示。
IPv4 PXE	网卡的IPv4 PXE功能控制，当Network Function选项为Enabled时显示。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启网口的 IPv4 PXE 功能。</li> <li>• Disabled: 关闭网口的 IPv4 PXE 功能。</li> </ul>
IPv6 PXE	网卡的IPv6 PXE功能控制。当Network Function选项为Enabled时显示。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启网口 IPv6 PXE 功能。</li> <li>• Disabled: 关闭网口 IPv6 PXE 功能。</li> </ul>

### 3.2.10 Network Stack Configuration 界面

如图 3-19 所示，通过 Network Stack Configuration 界面，对 PXE 启动功能进行配置。具体参数说明如表 3-20 所示。

图3-19 Network Stack Configuration 界面

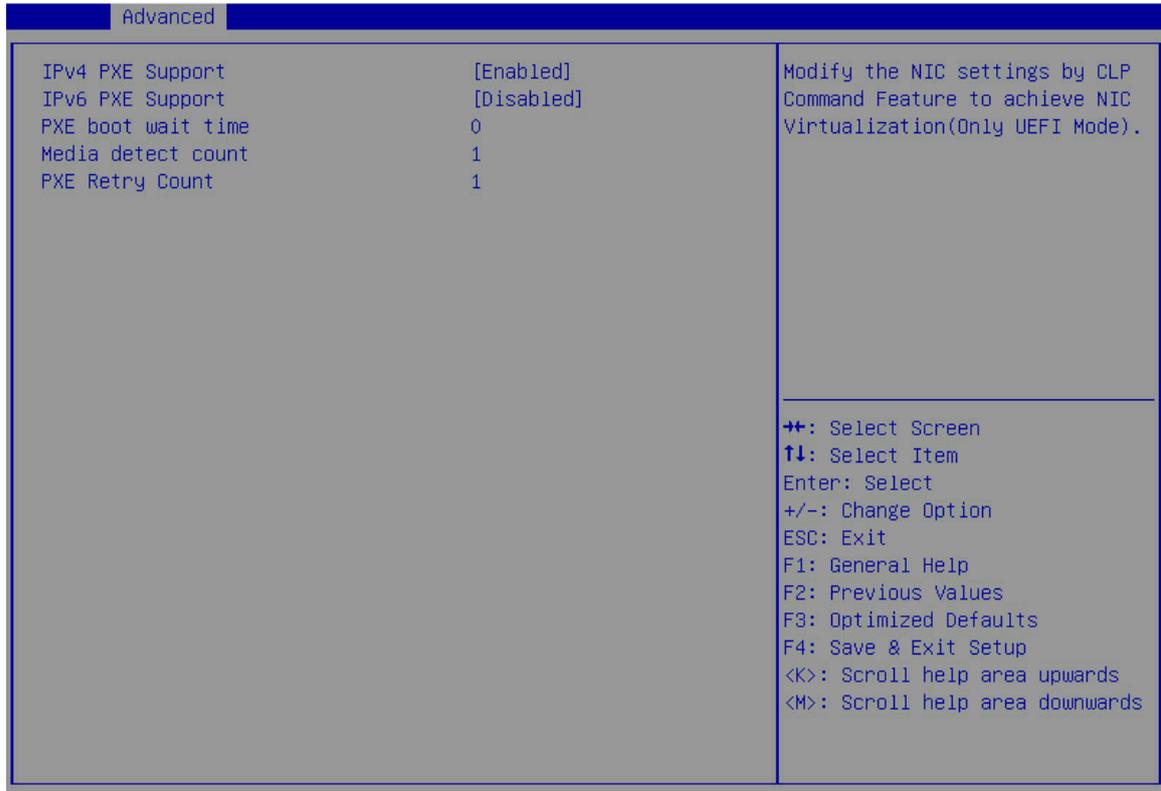


表3-20 Network Stack Configuration 界面参数

界面参数	功能说明
IPv4 PXE Support	IPv4 PXE支持，支持从IPv4网络启动操作系统，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 IPv4 PXE 功能。</li> <li>Disabled: 关闭 IPv4 PXE 功能，不会创建 IPv4 PXE 启动选项。</li> </ul>
IPv6 PXE Support	IPv6 PXE支持，支持从IPv6网络启动操作系统，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启 IPv6 PXE 功能。</li> <li>Disabled（缺省）：关闭 IPv6 PXE 功能，不会创建 IPv6 PXE 启动选项。</li> </ul>
PXE boot wait time	PXE启动等待时间。使用ESC键去终止PXE启动的等待时间，使用+/-或数字键设置该选项的值，取值范围为0~5，缺省值为0，单位为秒。
Media Detect Count	媒介设备检测计数，用于检测媒介在位次数，取值范围1~50，缺省值为1，单位为次。
PXE Retry Count	PXE轮询次数，取值范围0~50，缺省值为1，单位为次，0表示始终进行PXE轮询。

### 3.2.11 Intel(R) VROC sSATA Controller 界面

如图 3-20 所示，Intel(R) VROC sSATA Controller 界面可以配置 sSATA 总线下挂载设备的软 RAID 功能。具体参数说明如表 3-21 所示。

当 3.3.1 PCH Configuration 界面的 PCH sSATA Configuration 下将 sSATA 模式配置为 RAID 时，显示该界面。



Intel(R) VROC SATA Controller 界面信息与 Intel(R) VROC sSATA Controller 界面信息相同，不再赘述。Intel(R) VROC SATA Controller 界面用于配置挂载在 SATA 总线下设备的软 RAID 功能。

图3-20 Intel(R) VROC sSATA Controller 界面

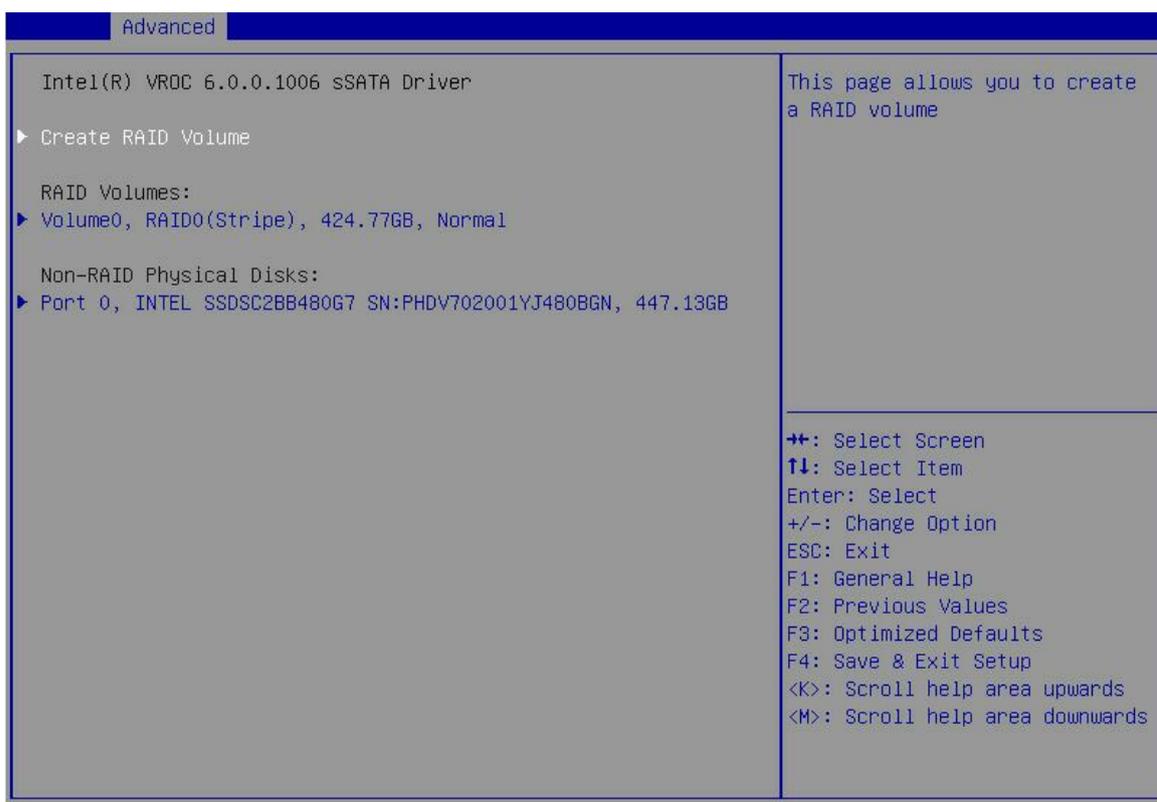


表3-21 Intel(R) VROC sSATA Controller 界面参数

界面参数	功能说明
Create RAID Volume	创建 RAID 卷的菜单。仅当 SATA 或 sSATA 控制器对应的接口存在两个及以上的硬盘时，显示该选项。
RAID Volumes	已创建的 RAID 列表。
Volume0, RAID0(Stripe), 424.77GB, Normal	已创建的 RAID 信息，Volume0: 该 RAID 名字，RAID0: 该 RAID 级别，424.77GB (Size): 该 RAID 大小，Normal: 该 RAID 状态。
Non-RAID Physical Disks	未被创建 RAID 的物理硬盘列表。

界面参数	功能说明
Port 0,INTEL SSDSC2BB480G7 SN:PHDV702001YJ480BGN,447.14GB	未被创建RAID物理硬盘信息，以Port 0为例，其他未被创建RAID的硬盘的该菜单信息是一致的。

## 1. Create RAID Volume 界面

Create RAID Volume界面如图 3-21所示，具体参数说明如表 3-22所示。

图3-21 Create RAID Volume 界面

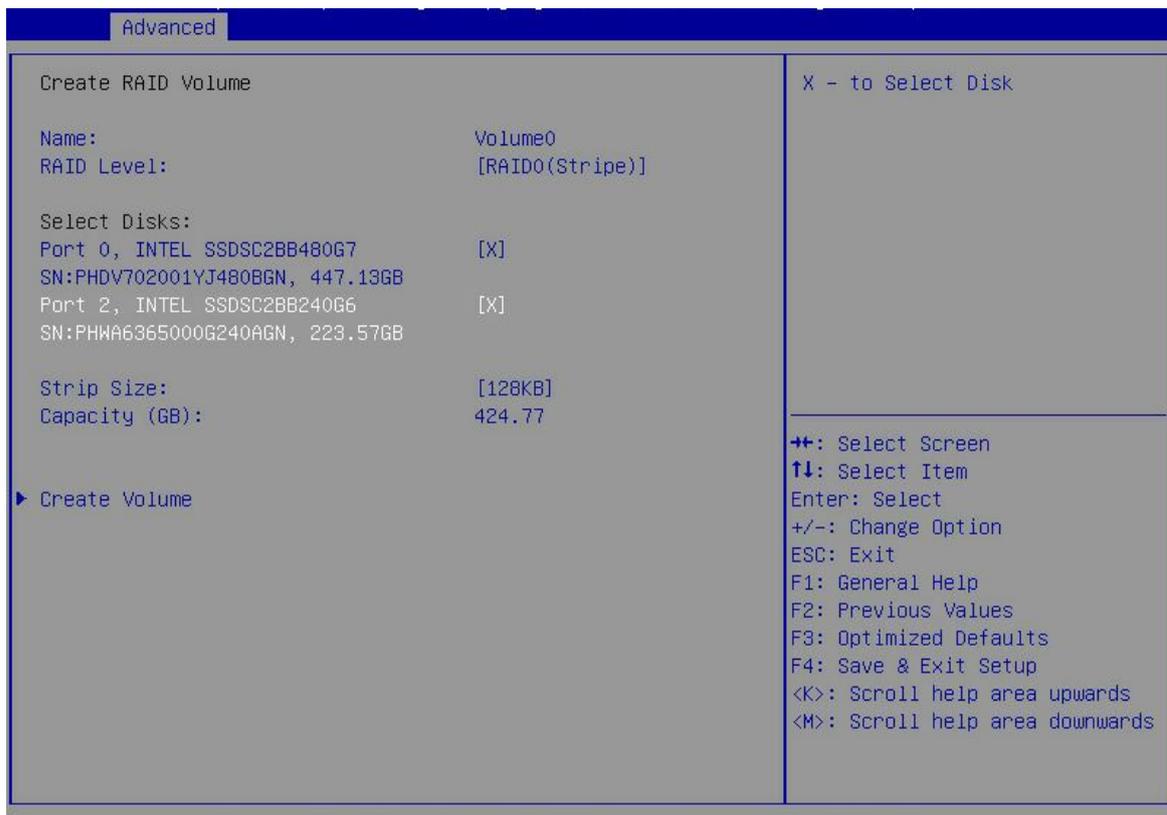


表3-22 Create RAID Volume 界面参数

界面参数	功能说明
<b>Create RAID Volume</b>	
Name	Volume0：设置待创建的RAID的名称。 需要注意的是：创建RAID时，请确保RAID的名称不包含特殊字符。
RAID Level	RAID等级选择，菜单选项为： <ul style="list-style-type: none"> <li>RAID0(Stripe)（缺省）：RAID0</li> <li>RAID1(Mirror)：RAID1</li> </ul>
Select Disks	显示可用于组建RAID的硬盘。

界面参数	功能说明
Port 0,INTEL SSDSC2BB480G7 SN:PHDV702001YJ480BGN,447.14GB	选择组建RAID的硬盘，菜单选项为： <ul style="list-style-type: none"> <li>（缺省）：未选中该硬盘。</li> <li>X：选中该硬盘。</li> </ul>
Stripe Size	RAID条带大小。菜单选项为： <ul style="list-style-type: none"> <li>4KB</li> <li>8KB</li> <li>16KB</li> <li>32KB</li> <li>64KB</li> <li>128KB（缺省）</li> </ul>
Capacity(GB)	RAID空间容量。
Create Volume	创建RAID卷操作，按下enter后即创建成功，并在All Intel VMD Controllers界面下可以查看已创建的RAID卷RAID Volume。

## 2. RAID VOLUME INFO 界面

RAID VOLUME INFO界面如[图 3-22](#)所示，具体参数说明如[表 3-23](#)所示。

图3-22 RAID VOLUME INFO 界面

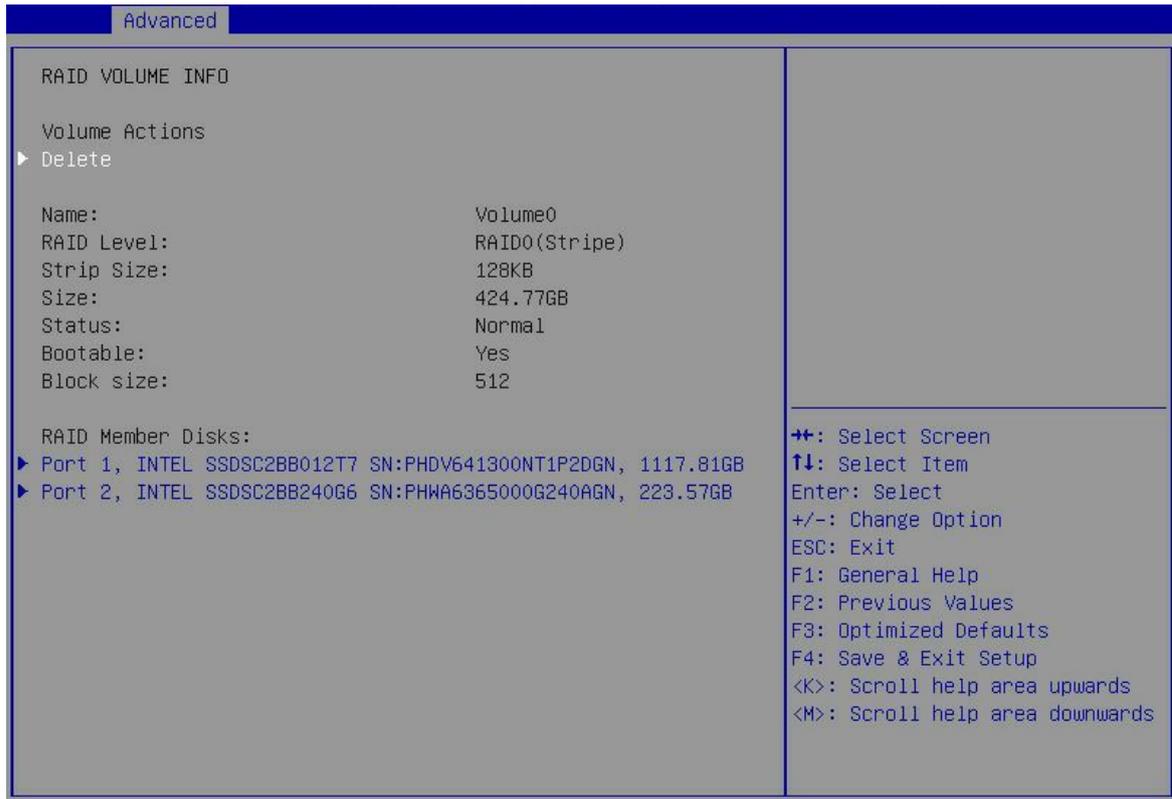


表3-23 RAID VOLUME INFO 界面参数

界面参数	功能说明
Volume Action: RAID 卷操作	
Delete	删除该已组好的RAID卷，直接按enter键即可。
Name	RAID名字。
RAID Level	RAID等级。
Strip Size	RAID的条带大小。
Size	RAID大小。
Status	RAID状态。
Bootable	可启动性（是否可启动），Yes表示可启动，No表示不可启动。
Block Size	块大小。
RAID Member Disks: 该RAID中的成员硬盘。	
Port 1,INTEL SSDSC2BB012T7 SN:PHDV641300NT1P2DGN,1117.81GB	组成该RAID的硬盘(Port 1)信息菜单。

### 3. Delete 界面

Delete菜单界面参数如[图 3-23](#)所示，具体参数说明如[表 3-24](#)所示。

图3-23 Delete 界面

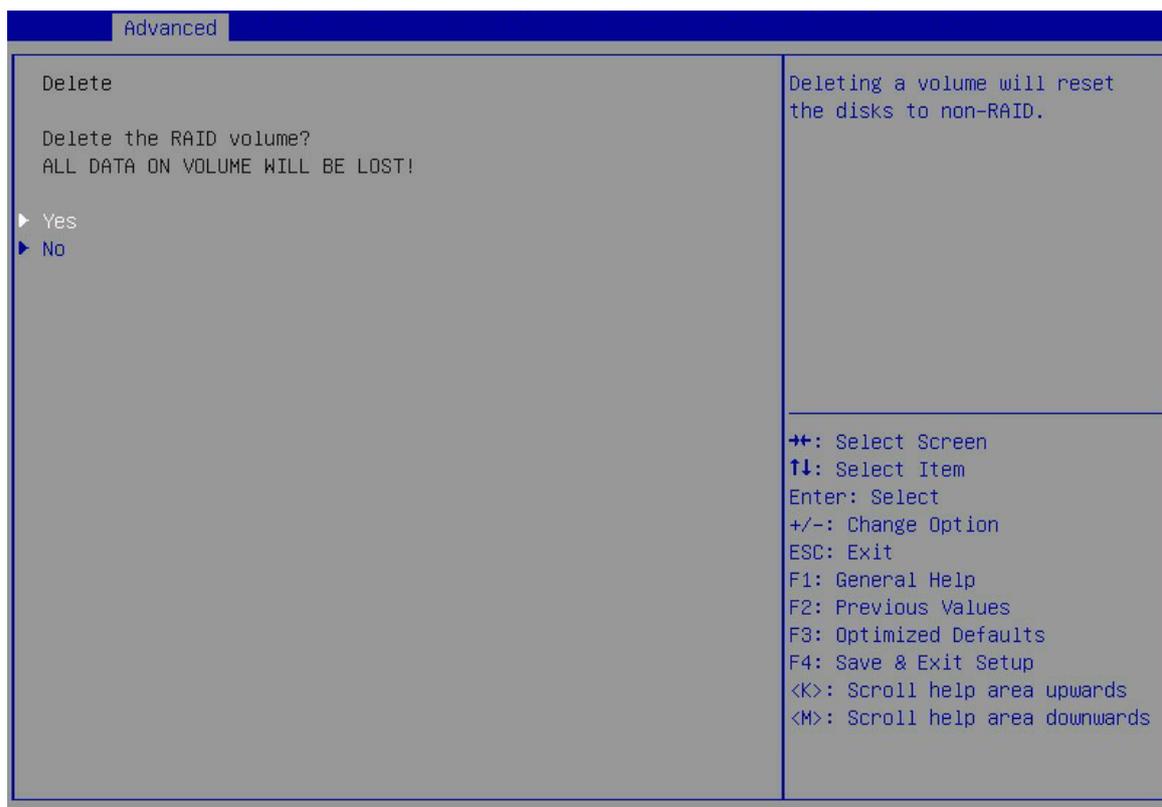


表3-24 Delete 界面参数

界面参数	功能说明
RAID卷Delete操作，所有该卷上的内容将会被丢失。	
Yes	确定要删除该RAID，按enter后即可删除。
No	取消删除该RAID的动作，按enter后即可取消。

#### 4. PHYSICAL DISK INFO 界面

PHYSICAL DISK INFO模块菜单界面参数如图 3-24所示，具体参数说明如表 3-25所示。

图3-24 PHYSICAL DISK INFO 界面

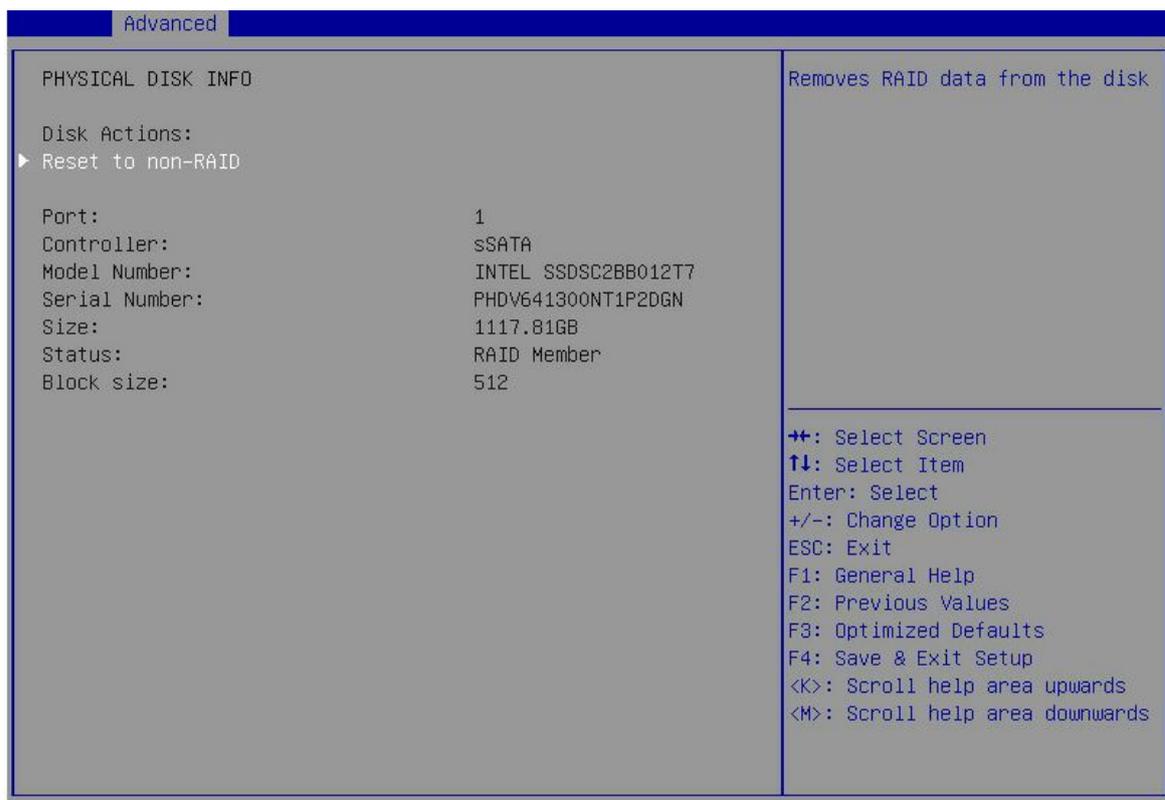


表3-25 PHYSICAL DISK INFO 界面参数

界面参数	功能说明
Disk Actions	
Reset to non-RAID	该RAID的硬盘信息重置菜单，即删除该硬盘上的RAID信息。
Port	端口号。
Controller	硬盘控制器信息，该例中是sSATA。
Model Number	设备型号。
Serial Number	设备序列号。

界面参数	功能说明
Size	硬盘容量。
Status	硬盘状态。
Block Size	块大小。

## 5. Reset to non-RAID 界面

Reset to non-RAID菜单界面参数如[图 3-25](#)所示，具体参数说明如[表 3-26](#)所示。

图3-25 Reset to non-RAID 界面



表3-26 Reset to non-RAID 界面参数

界面参数	功能说明
RAID	卷上该硬盘信息的重置操作，即删除该硬盘上的RAID信息。
Yes	确定要重置该硬盘，按enter后即可删除。
No	取消删除该硬盘的动作，按enter后即可取消。

## 6. Non-RAID Physical Disk 界面

Non-RAID Physical Disk界面下会列出未创建RAID的硬盘，以其中一个Port 0,INTEL SSDSC2BB480G7 SN:PHDV702001YJ480BGN,447.14GB的设备界面为例，如[图 3-26](#)所示，具体参数说明如[表 3-27](#)所示。

图3-26 Non-RAID Physical Disk 界面



表3-27 Non-RAID Physical Disk 界面参数

界面参数	功能说明
<b>Disk Actions</b>	
Mark as Spare	标记该硬盘为备用硬盘，不能组RAID使用。
Mark as Journaling Drive	标记该硬盘为Journaling Drive，不能组RAID使用。
Port	硬盘接入的端口号。
Controller	硬盘控制器信息，该例中是sSATA。
Model Number	厂商模型序号。
Serial Number	设备系列号。
Size	硬盘容量。
Status	硬盘状态。
Block Size	块大小。

## 7. Mark as Spare 界面

Mark as Spare界面如[图 3-27](#)所示，具体参数说明如[表 3-28](#)所示。

图3-27 Mark as Spare 界面

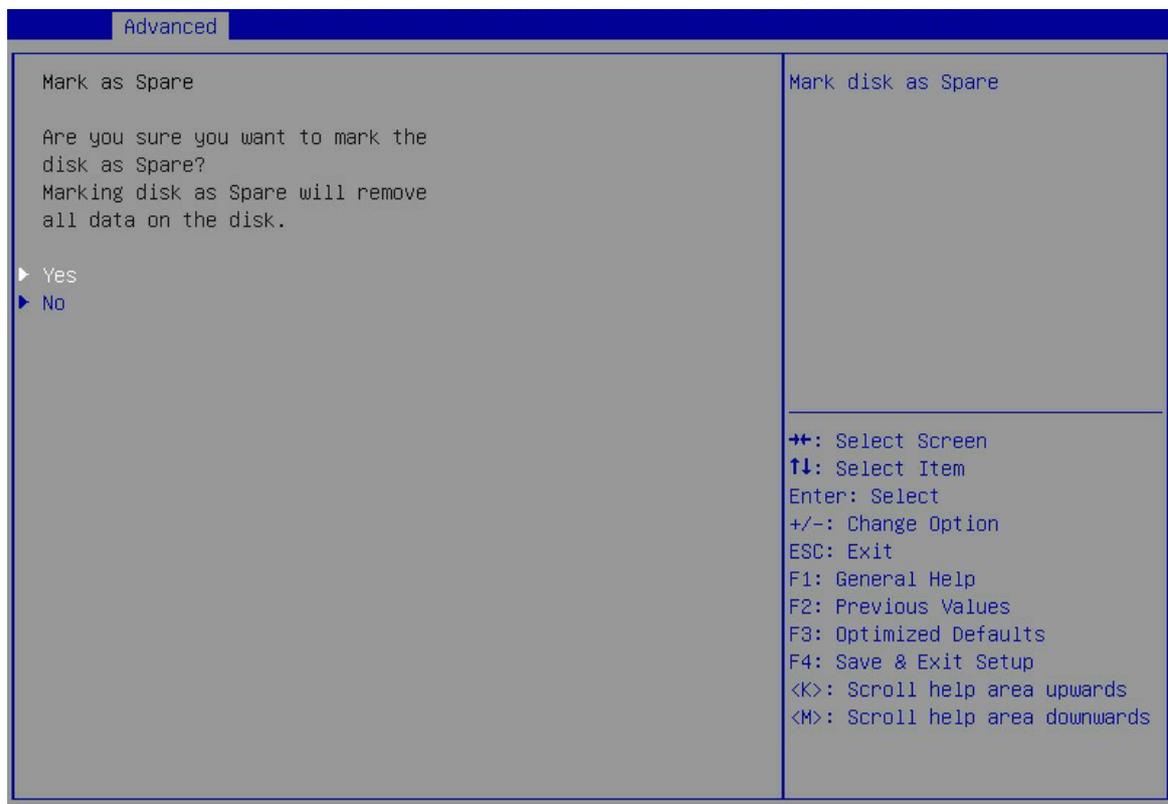


表3-28 Mark as Spare 界面参数

界面参数	功能说明
	标记该硬盘为备用盘，一旦执行该操作，此盘内的数据将会被全部删除。
Yes	确定要标记该硬盘为备用盘，按enter后即可执行该操作。
No	取消标记该硬盘为备用盘，按enter后即可取消。

## 8. Mark as Journaling Drive 界面

Mark as Journaling Drive界面如[图 3-28](#)所示，具体参数说明如[表 3-29](#)所示。

图3-28 Mark as Journaling Drive 界面

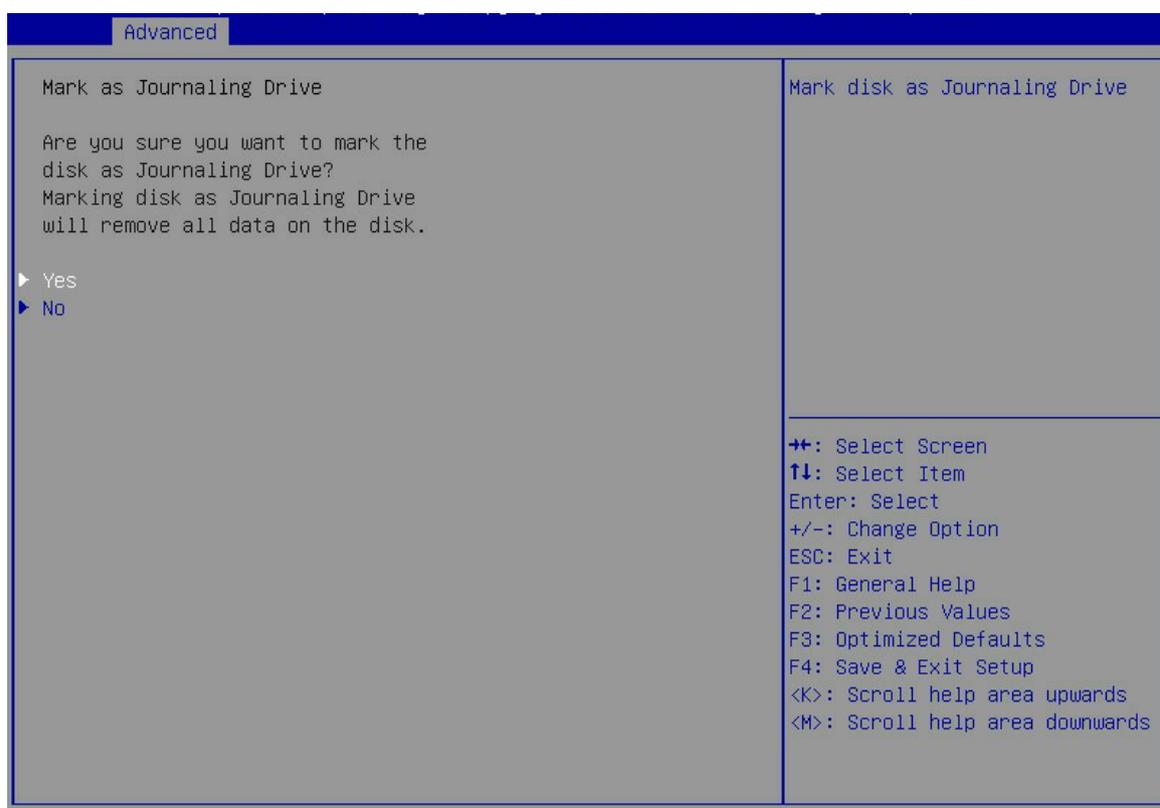


表3-29 Mark as Journaling Drive 界面参数

界面参数	功能说明
	标记该硬盘为Journaling Drive，一旦执行该操作，此盘内的数据将会被全部删除。
Yes	确定要标记该硬盘为Journaling Drive，按Enter后即可执行该操作。
No	取消标记该硬盘为Journaling Drive，按Enter后即可取消。

### 3.2.12 Intel(R) virtual RAID on CPU 界面

Intel(R) virtual RAID on CPU 界面可以配置 NVMe 盘的虚拟 RAID 功能。该选项在 Intel VMD 功能未使能的情况下不显示。

前期 VMD 准备工作：

(1) 安装 Intel NVMe VROC 密钥模块。

- 如果安装密钥模块标准版，则支持创建 RAID 0、RAID 1 和 RAID 10。
- 如果安装密钥模块高级版，则支持创建 RAID 0、RAID 1、RAID 5 和 RAID 10。
- 如果安装密钥模块 Intel 版，则仅支持对 Intel 的 NVMe SSD 硬盘创建 RAID 0、RAID 1、RAID 5 和 RAID 10。

- (2) 如图 3-105所示，选择**Socket Configuration**页签 > **I/O Configuration** > **Intel® VMD technology**，根据表 3-95，找到NVMe设备对应的VMD功能设置选项，使能VMD选项。
- (3) 设置成功VMD后，进入**Advanced**页签 > **Intel(R) virtual RAID on CPU**菜单，然后按**Enter**。进入如图 3-29所示界面。

图3-29 Intel(R) virtual RAID on CPU 界面

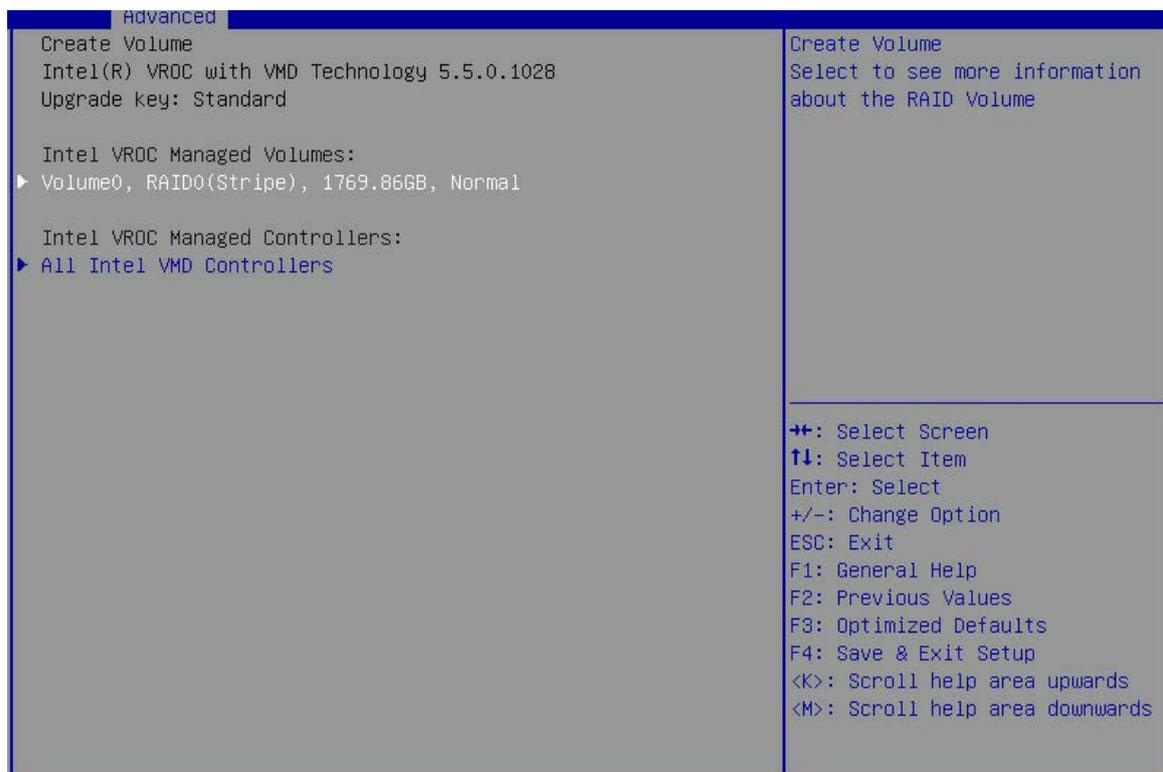


表3-30 Intel(R) virtual RAID on CPU 界面参数

界面参数	功能说明
Intel VROC Managed Volumes	列出已创建的RAID卷。
Volume0, RAID0 (Stripe), 1769.86GB, Normal	已创建的RAID 信息。 Volume0: 该RAID名字, RAID0: 该RAID级别, 1769.86GB (Size): 该RAID大小, Normal: 该RAID状态。
Intel VROC Managed Controllers	列出Intel VROC下管理的控制器。
All Intel VMD Controllers	所有的Intel VMD控制器菜单。

### 1. Volume0, RAID0 (Stripe), 1769.86GB, Normal 界面

Volume0, RAID0(Stripe), 1769.86GB, Normal菜单界面参数如图 3-30所示，具体参数说明如表 3-31所示。



说明

Volume x,RAID x,Size ,Status 菜单表示已经组成 RAID 的卷的信息。本文以已添加的 RAID 卷: Volume0,RAID0 (Stripe) , 1769.86GB,Normal 为例进行介绍。

图3-30 Volume0, RAID0 (Stripe) , 1769.86GB,Normal 界面

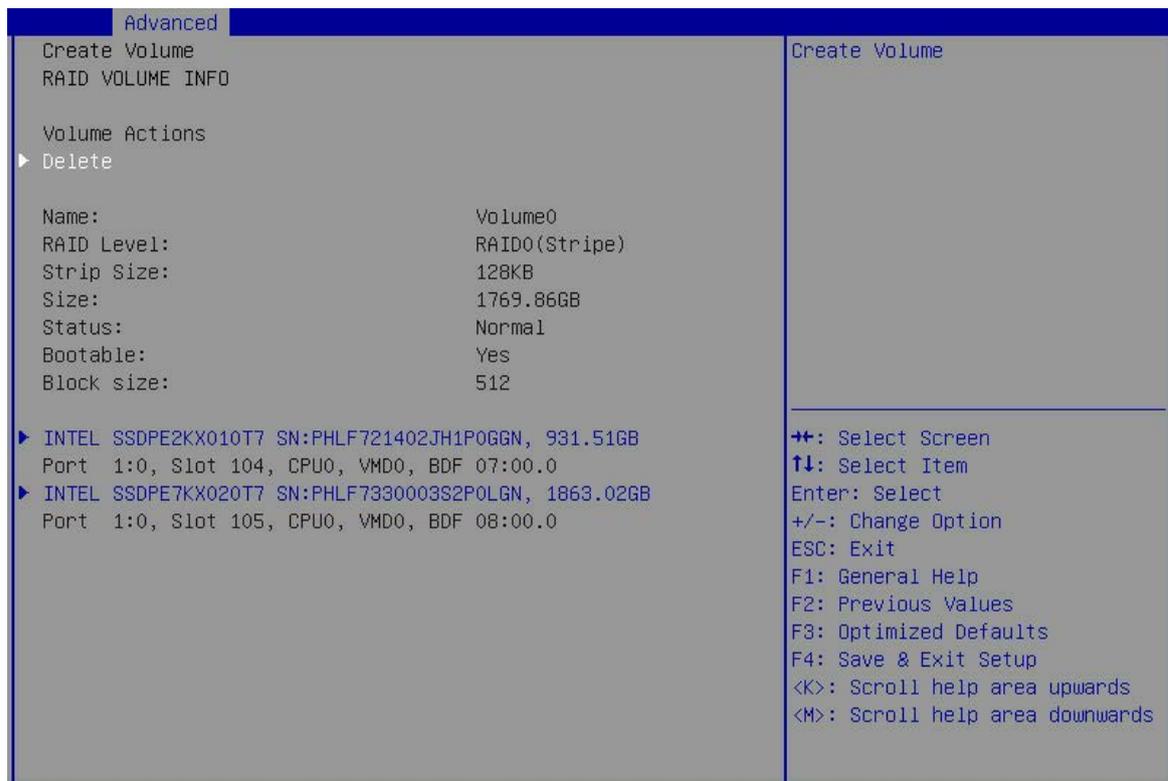


表3-31 Volume0, RAID0 (Stripe) , 1415.89GB,Normal 界面参数

界面参数	功能说明
Volume Action: RAID 卷操作。	
Delete	删除该已组好的RAID卷，直接按enter键即可。
Name	RAID卷名称。
RAID Level	RAID等级。
Strip Size	RAID的条带大小。
Size	RAID大小。
Status	RAID状态。
Bootable	可启动性（是否可启动），Yes表示可启动，No表示不可启动。
Block Size	块大小。

界面参数	功能说明
RAID Member Disks: 该RAID中的成员硬盘。	
INTEL SSDPE2KX010T7 SN:PHLF721402JH1P0LGN 931.51GB Port 1:0,Slot 104,CPU0,VMD0,BDF 07:00.0	组成该RAID的硬盘(Port1:0, Slot 104)信息菜单。
INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB Port 1:0,Slot 105,CPU0,VMD0,BDF 08:00.0	组成该RAID的硬盘(Port1:0, Slot 105)信息菜单。
<p>需要注意的是: VMD功能使能之后, NVMe信息显示在Intel(R) virtual RAID on CPU界面。</p> <p>如VMD功能未启动, NVMe设备信息将显示在Slot x: Port x界面或NVMe Configuration界面(取决于NVMe设备内是否包含OptionRom), NVMe设备逻辑槽位号显示规则可查看<a href="#">表3-14</a>。</p>	

## 2. Delete 界面

Delete菜单界面参数如[图 3-31](#)所示, 具体参数说明如[表 3-32](#)所示。

图3-31 Delete 界面

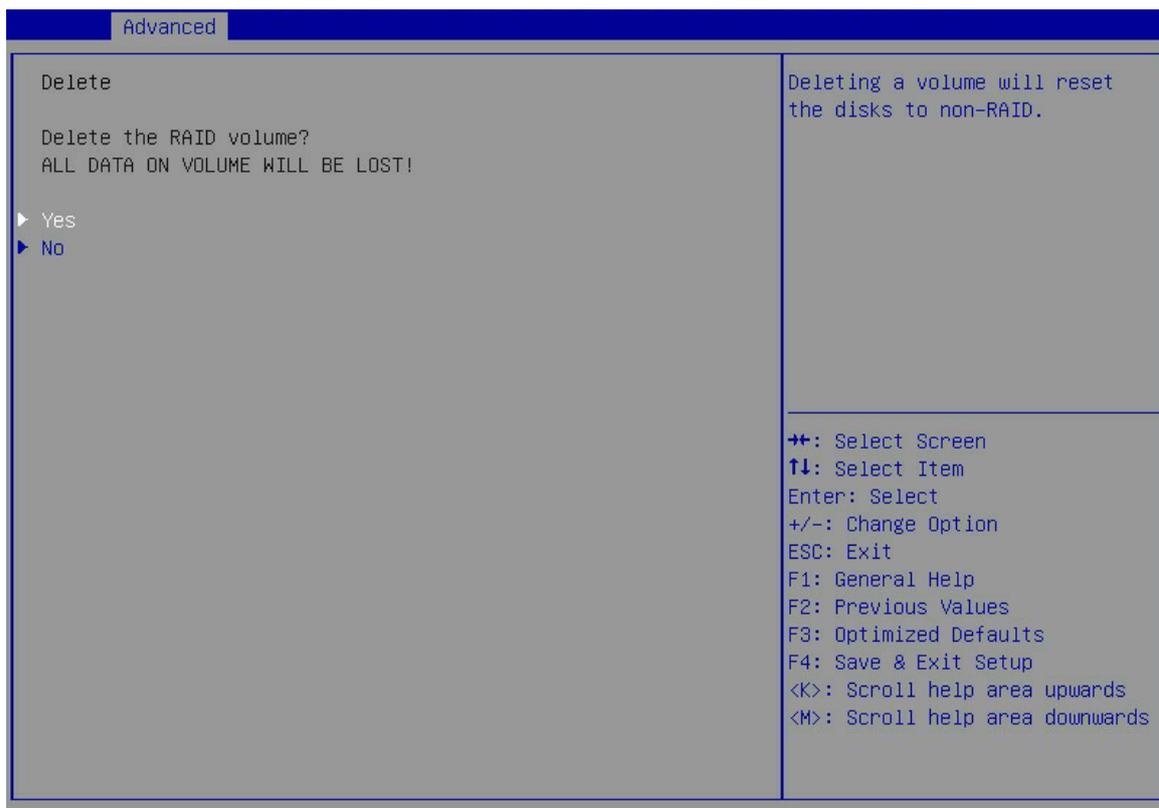


表3-32 Delete 界面参数

界面参数	功能说明
RAID卷Delete操作, 所有该卷上的内容将会被丢失。	
Yes	确定要删除该RAID, 按enter后即可删除。
No	取消删除该RAID的动作, 按enter后即可取消。

RAID Member Disks模块中Port0 菜单界面参数如图 3-32所示，具体参数说明如表 3-33所示。



INTEL SSDPE2KX010T7 SN:PHLF721402JH1P0LGN 931.51GB Port 1:0,Slot 104,CPU0,VMD0,BDF 07:00.0 和 INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB Port 1:0,Slot 105,CPU0,VMD0,BDF 08:00.0 菜单选项中的内容相同，都表示组成该 RAID 卷的硬盘的信息，其他组成 RAID 的硬盘的信息选项也是该格式内容。本文以其中一个硬盘为例：INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB 为例进行介绍。

图3-32 INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB 界面

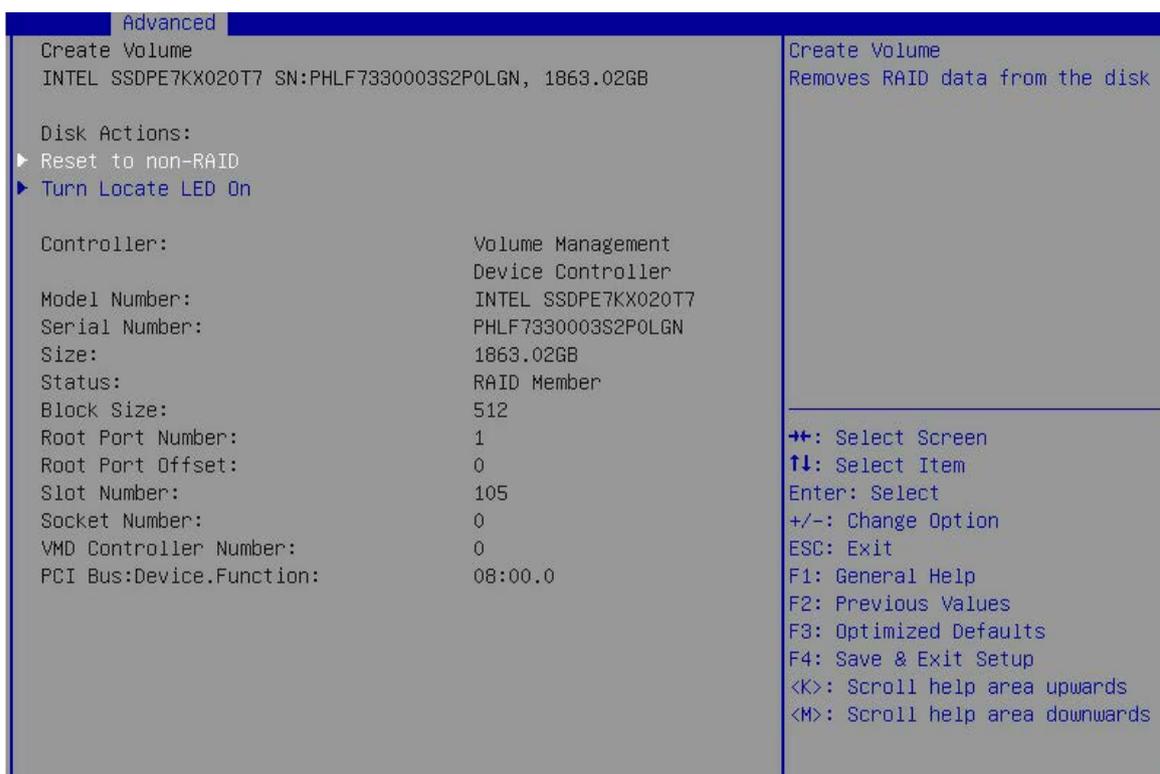


表3-33 INTEL SSDPE2ME800G4 SN:PHMD63960129800GGN,745.21GB 界面参数

界面参数	功能说明
Disk Actions	
Reset to non-RAID	该RAID的硬盘信息重置菜单，即删除该硬盘上的RAID信息。
Turn Locate LED On	定位LED灯开关。
Controller	控制器信息，该例中是VMD Controller。
Model Number	设备型号。
Serial Number	设备序列号。

界面参数	功能说明
Size	硬盘容量。
Status	硬盘状态。
Block Size	块大小。
Root Port Number	该硬盘的根端口号。
Root Port Offset	该硬盘的根端口偏移量。
Slot Number	该硬盘的槽位号。
Socket Number	该硬盘所连接的CPU的插槽号。
VMD Controller Number	VMD控制器编号。
PCI Bus: Device.Function	该硬盘Bus:Dev:Func信息。

### 3. Reset to non-RAID 界面

Reset to non-RAID菜单界面参数如[图 3-33](#)所示，具体参数说明如[表 3-34](#)所示。

图3-33 Reset to non-RAID 界面

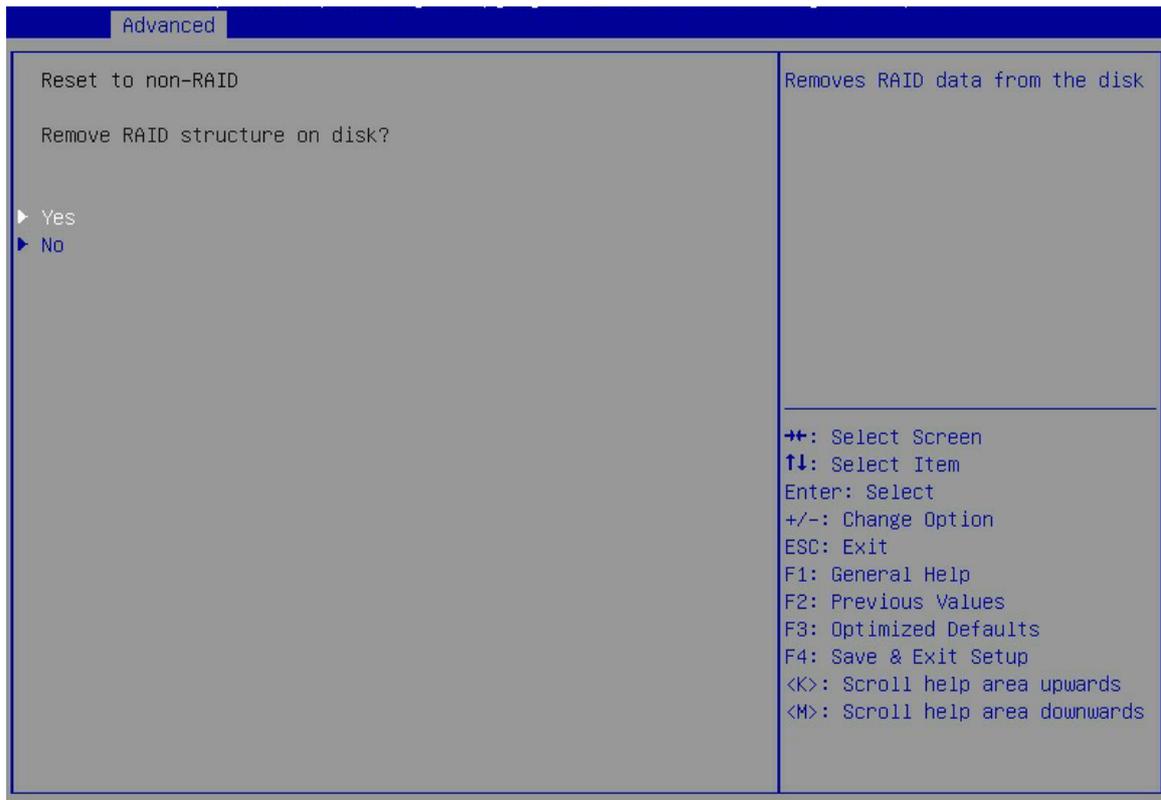


表3-34 Reset to non-RAID 界面参数

界面参数	功能说明
RAID 卷上该硬盘信息的重置操作，即删除该硬盘上的RAID信息。	
Yes	确定要重置该硬盘，按enter后即可删除。
No	取消删除该硬盘的动作，按enter后即可取消。

#### 4. All Intel VMD Controllers 界面

All Intel VMD Controllers界面如图3-34所示，具体参数说明如表3-35所示。

图3-34 All Intel VMD Controllers 界面



表3-35 All Intel VMD Controllers 界面参数

界面参数	功能说明
Create RAID Volume	创建RAID卷的菜单。
Non-RAID Physical Disks: 未被创建RAID 物理硬盘	
INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB Port 1:0,Slot 105,CPU0,VMD0,BDF 08:00.0	未被创建RAID物理硬盘信息,以Port1:0 Slot 105为例，其他未被创建RAID的硬盘的该菜单信息是一致的。 需要注意的是：硬盘端口信息的显示跟服务器中安装的 NVMe SSD扩展卡类型以及安装的位置有关。

## 5. Create RAID Volume 界面

Create RAID Volume界面如图3-35所示，具体参数说明如表3-36所示。

图3-35 Create RAID Volume 界面

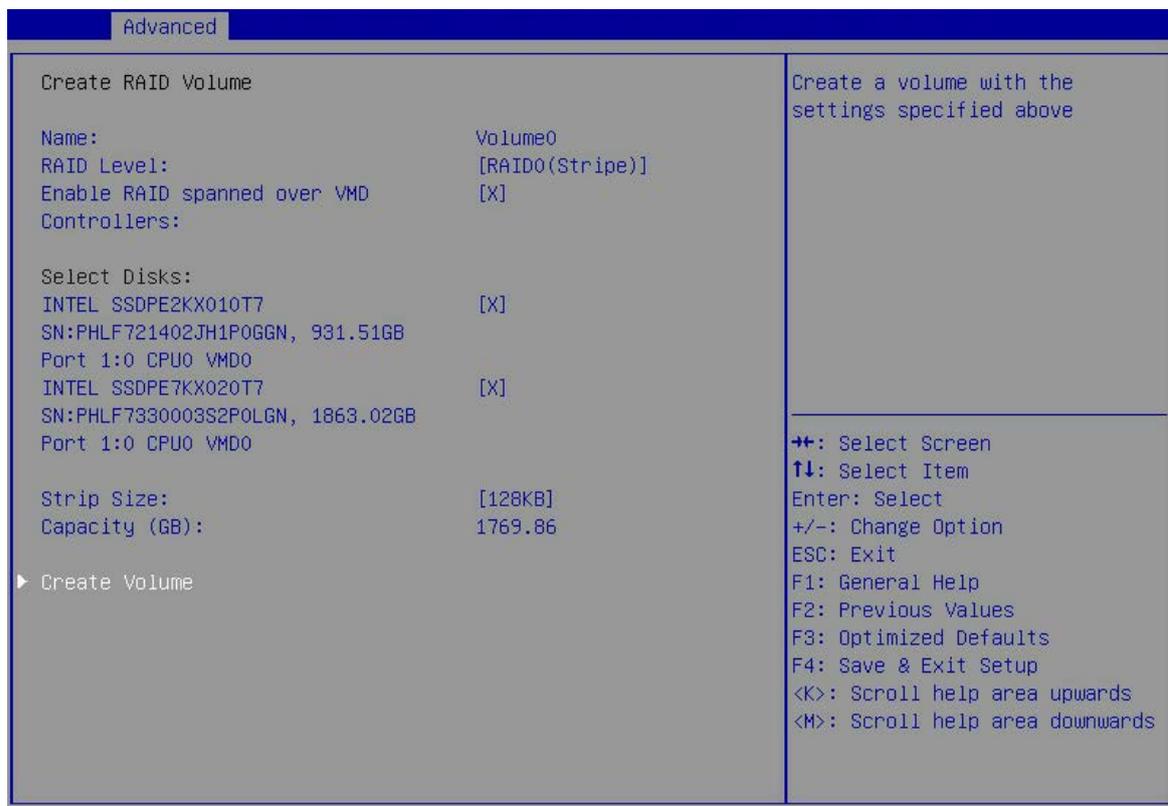


表3-36 Create RAID Volume 界面参数

界面参数	功能说明
<b>Create RAID Volume</b>	
Name	Volume0：设置待创建的RAID的名称。 需要注意的是：创建RAID时，请确保RAID的名称不包含特殊字符。
RAID Level	RAID等级选择，菜单选项为： <ul style="list-style-type: none"> <li>RAID0(Stripe)（缺省）：RAID0</li> <li>RAID1(Mirror)：RAID1</li> <li>RAID5(Parity)：RAID5</li> <li>RAID10(RAID0+1)：RAID10</li> </ul>
Enable RAID spanned over VMD Controllers	RAID跨越VMD控制器使能选项，当选择了该项之后，可以同时选择VMD0和VMD1控制器下的硬盘进行组建RAID。
Select Disks	显示可用于组建RAID的硬盘。

界面参数	功能说明
INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB Port 1:0,Slot 105,CPU0,VMD0,BDF 08:00.0	选择组建RAID的硬盘，菜单选项为： <ul style="list-style-type: none"> <li>（缺省）：未选中该硬盘。</li> <li>X：选中该硬盘。</li> </ul>
Stripe Size	RAID条带大小。
Capacity(GB)	RAID空间容量。
Create Volume	创建RAID卷操作，按下enter后即创建成功，并在All Intel VMD Controllers界面下可以查看已创建的RAID卷RAID Volume。

## 6. Non-RAID Physical Disk 界面

Non-RAID Physical Disk（以INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB为例，其他各个未组RAID的硬盘信息界面与之相同）界面如[图 3-36](#)所示，具体参数说明如[表 3-37](#)所示。

图3-36 INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB 界面

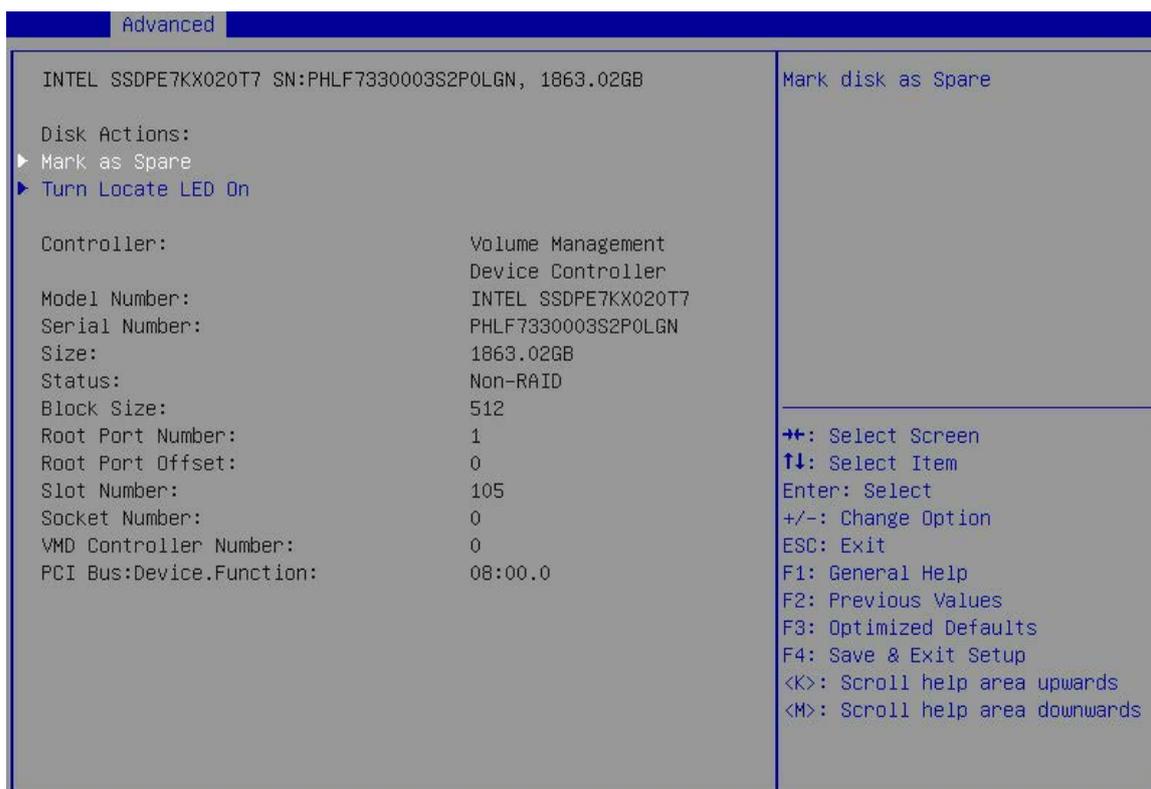


表3-37 INTEL SSDPE7KX020T7 SN:PHLF7330003S2P0LGN 1863.02GB 界面参数

界面参数	功能说明
<b>Disk Actions</b>	
Mark as Spare	标记该硬盘为备用硬盘，不能组RAID使用。

界面参数	功能说明
Turn Locate LED On	定位LED灯开关。
Controller	控制器信息，该例中是VMD Controller。
Model Number	厂商模型序号。
Serial Number	设备系列号。
Size	硬盘容量。
Status	硬盘状态。
Block Size	块大小。
Root Port Number	该硬盘的根端口号。
Root Port Offset	该硬盘的根端口偏移量。
Slot Number	该硬盘的的槽位号。
Socket Number	该硬盘所连接的CPU的插槽号。
VMD Controller Number	控制器信息。
PCI Bus: Device.Function	该硬盘Bus:Dev:Func信息。

## 7. Mark as Spare 界面

Mark as Spare界面如图 3-37所示，具体参数说明如表 3-38所示。

图3-37 Mark as Spare 界面

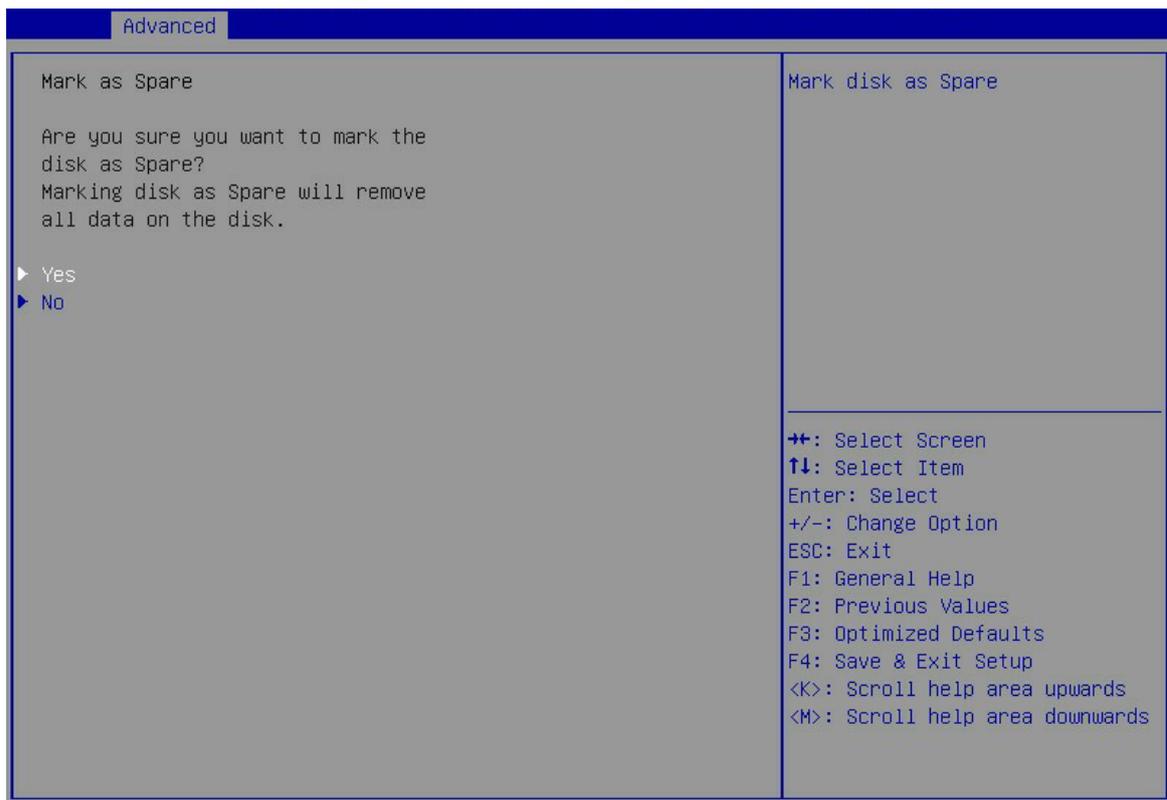


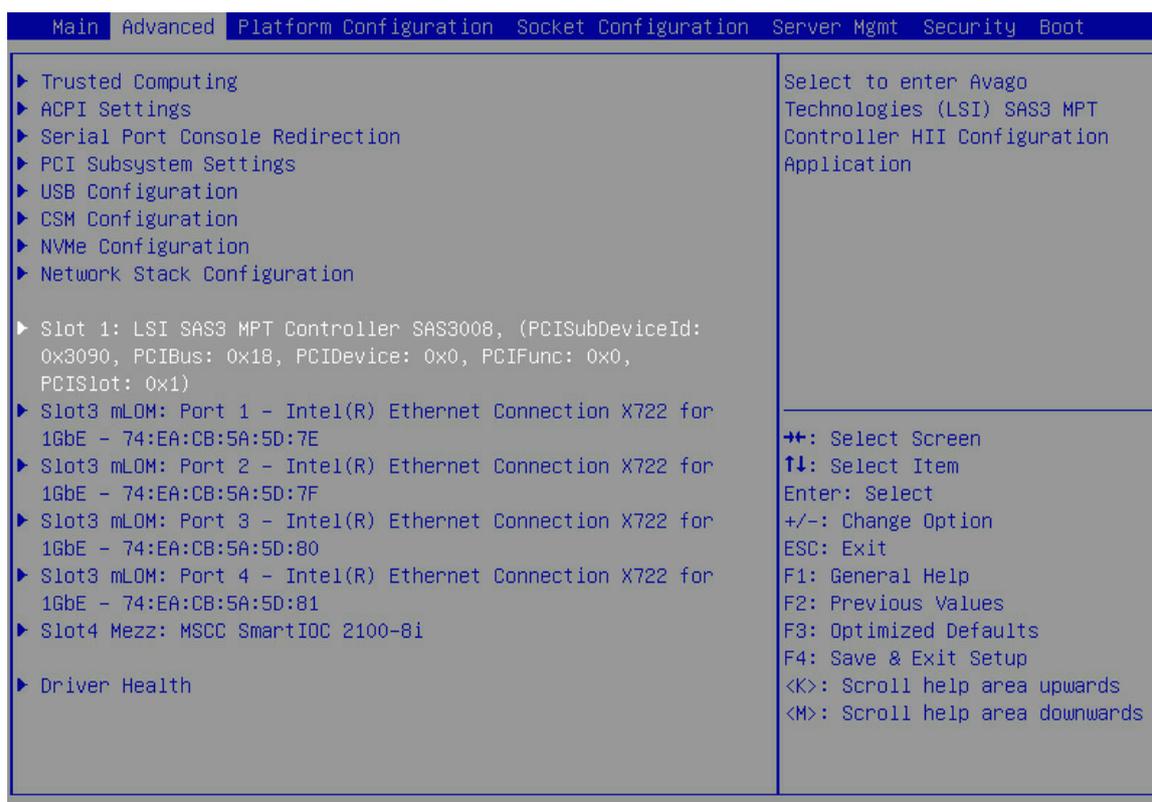
表3-38 Mark as Spare 界面参数

界面参数	功能说明
标记该硬盘为备用盘，一旦执行该操作，此盘内的数据将会被全部删除	
Yes	确定要标记该硬盘为备用盘，按enter后即可执行该操作。
No	取消标记该硬盘为备用盘，按enter后即可取消。

### 3.2.13 Slot x:Port x 界面

如图 3-38 所示，通过 Slot x:Port x 界面，可以对以太网接口、RAID 卡、带有 OptionRom 的 NVMe 盘进行配置。具体参数说明如表 3-39 所示。

图3-38 Slot x:Port x 界面



#### 说明

Slot x:Port x 界面由 PCIe 设备内 OptionRom 生成，界面内选项参数由设备厂商定义。需要注意的是，不同厂商、不同类型的 PCIe 设备界面均不相同，以实际显示为准。如图 3-39，以板载的 mLOM 以太网卡 Slot 3-mLOM:Port 1 为例说明界面参数。

图3-39 Slot 3-mLom : Port 1 界面

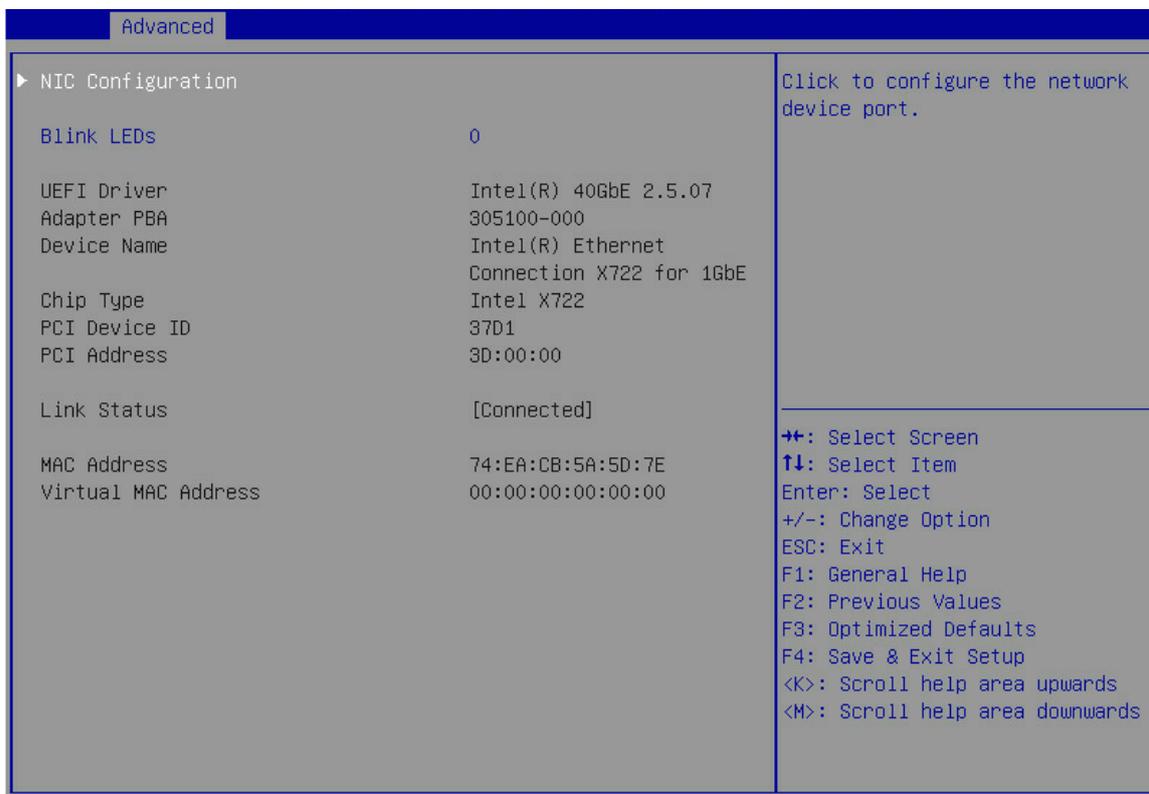


表3-39 Slot 3-mLom : Port 1 界面参数

界面参数	功能说明
NIC Configuration	配置网络设备端口参数。
Blink LEDs	以太网接口连接状态指示灯闪烁时间，取值范围0~15，缺省值为0，单位为秒。
UEFI Driver	显示板载网卡驱动程序的名称。
Adapter PBA	显示适配器PBA。
Device Name	显示板载网卡的名称。
Chip Type	显示板载网卡的芯片类型。
PCI Device ID	显示PCI设备ID。
PCI Address	显示PCI地址。
Link Status	显示链路状态，包括Disconnected（未连接）和Connected（已连接）。
MAC Address	显示板载网卡的MAC地址。
Virtual MAC Address	显示板载网卡的虚拟MAC地址。

NIC Configuration界面如[图 3-40](#)所示。具体参数说明如[表 3-40](#)所示。

图3-40 NIC Configuration 界面

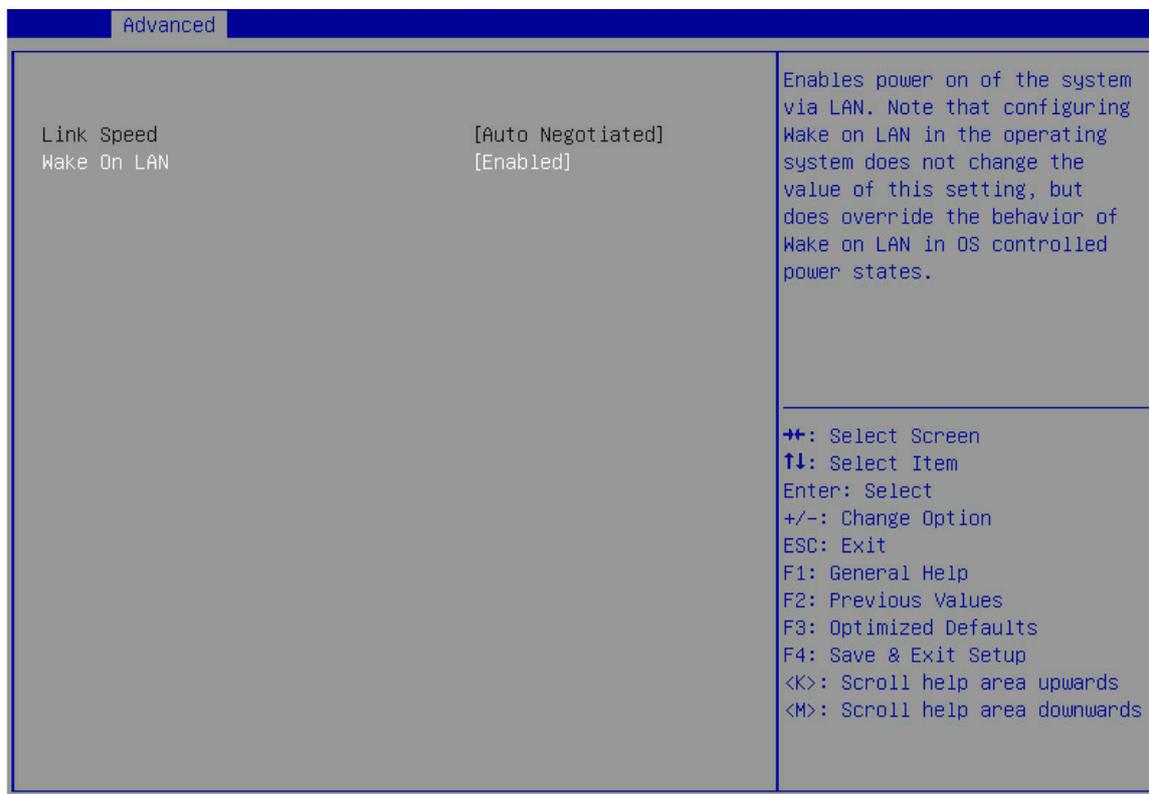


表3-40 NIC Configuration 界面参数

界面参数	功能说明
Link Speed	<p>网络设备端口链路速度配置，该选项已置灰，不可对其进行修改，默认是自动协商模式，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto Negotiated（缺省）：自协商。</li> <li>• 10 Mbps Half：10 Mbps 半双工。</li> <li>• 10 Mbps Full：10 Mbps 全双工。</li> <li>• 100 Mbps Half：100 Mbps 半双工。</li> <li>• 100 Mbps Full：100 Mbps 全双工。</li> </ul>
Wake On LAN	<p>允许服务器通过一个带外的Magic Packet开机，即局域网唤醒（唤醒操作系统），菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启局域网唤醒功能。</li> <li>• Disabled：关闭局域网唤醒功能。</li> </ul>

### 3.2.14 Intel(R) Optane(TM) DC Persistent Memory Configuration

如图 3-41 所示，通过 Intel(R) Optane(TM) DC Persistent Memory Configuration 界面可以查看及设置 Intel DCPMM 内存信息。本界面仅当系统内安装了 Intel DCPMM 内存时显示。

图3-41 Intel(R) Optane(TM) DC Persistent Memory Configuration 界面

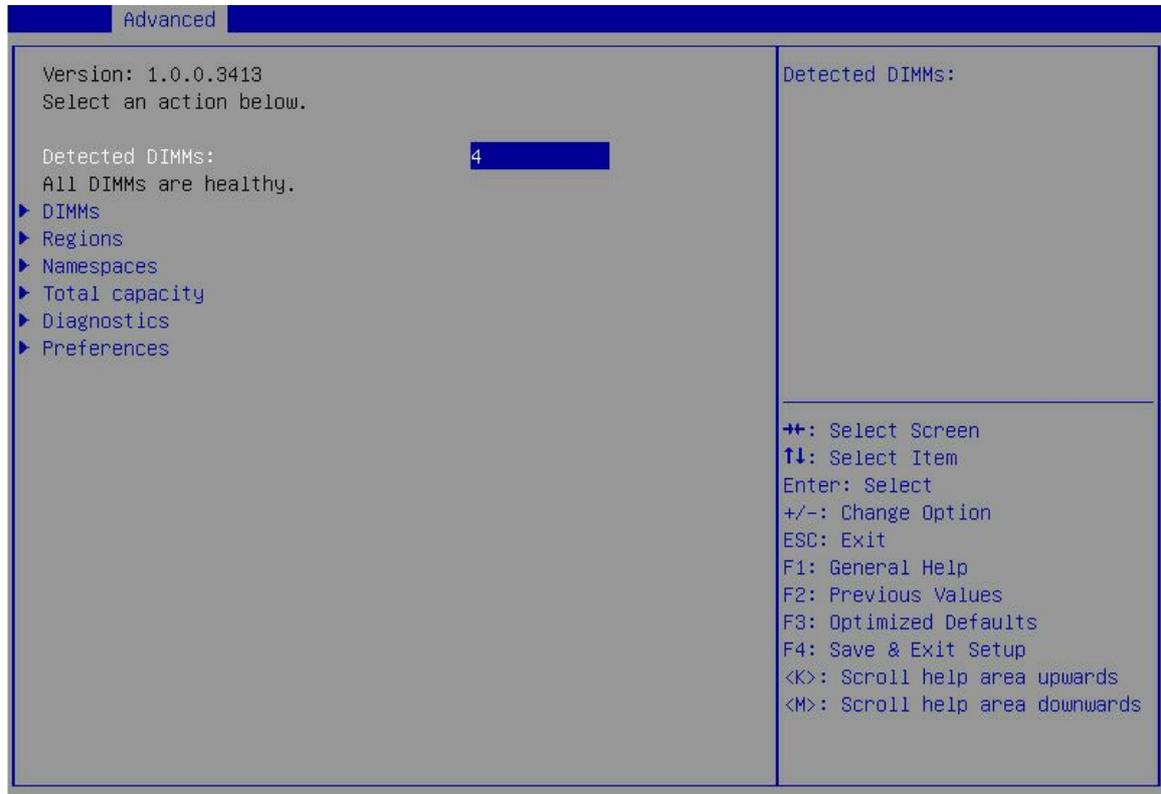


表3-41 Intel(R) Optane(TM) DC Persistent Memory Configuration 界面参数

界面参数	功能说明
Detected DIMMs	显示当前检测到的Intel DCPMM内存条数。
DIMMs	内存信息菜单。
Regions	区域配置菜单。
Namespaces	命名空间配置菜单。
Total capacity	总容量显示菜单。
Diagnostics	诊断菜单。
Preferences	性能配置菜单。

### 1. DIMMs 界面

如图 3-42 所示，通过 DIMMs 界面，可以查看并配置已安装的 Intel DCPMM 内存。具体参数说明如表 3-42 所示。

图3-42 DIMMs 界面

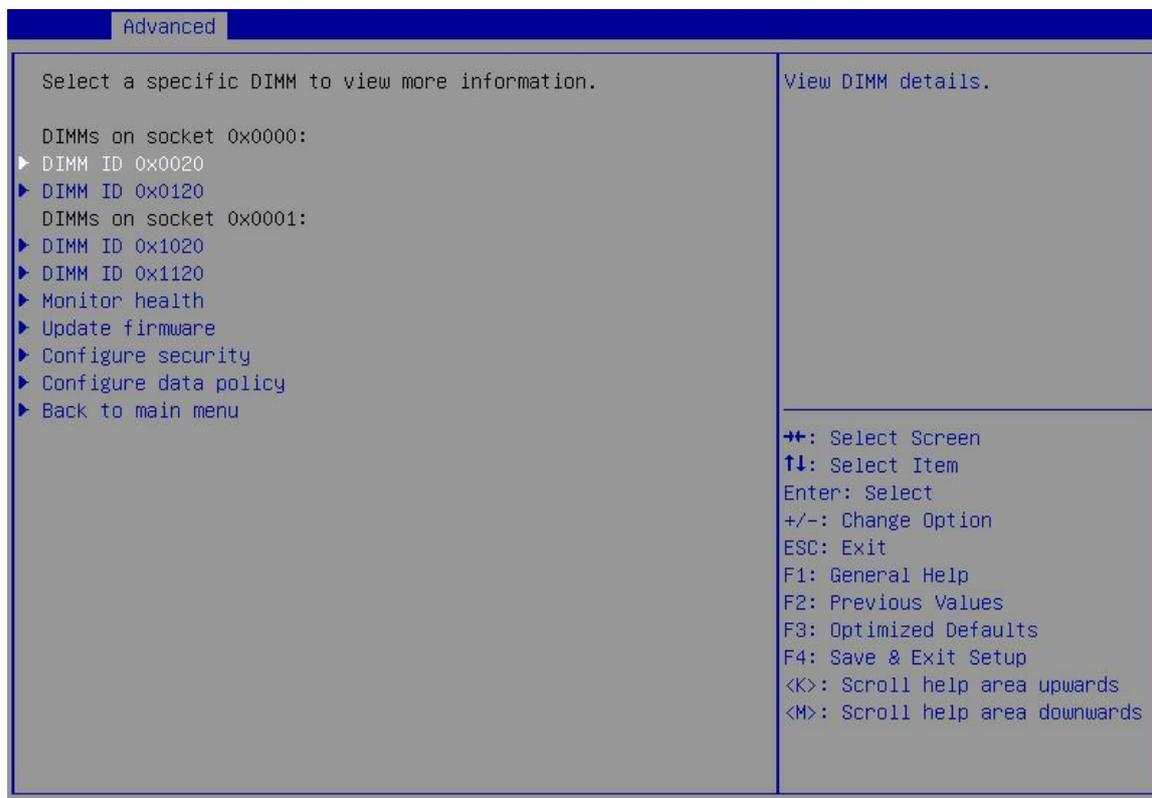


表3-42 DIMMs 界面参数

界面参数	功能说明
DIMM ID	对应ID的Intel DCPMM内存详细信息菜单。
Monitor health	传感器配置菜单。
Update firmware	Intel DCPMM内存固件升级菜单。
Configure security	安全配置菜单。
Configure data policy	数据策略配置菜单。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-43 所示，通过 DIMM ID 界面，可以查看并配置已安装的 Intel DCPMM 内存。图 3-44、图 3-45、图 3-46 和图 3-47 显示 Intel DCPMM 内存的详细信息，这些选项仅当 Show more details+ 设置为 Enabled 时显示。具体参数说明如表 3-43 所示。

图3-43 DIMM ID 界面 1

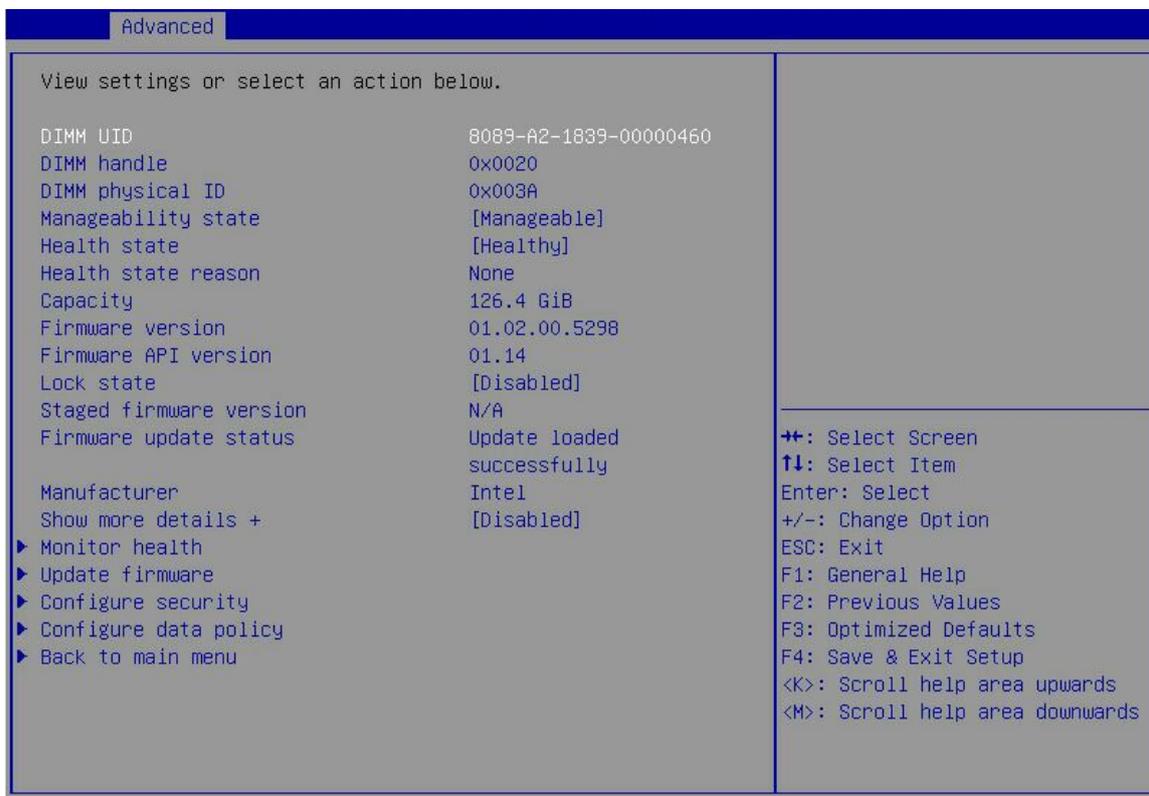


图3-44 DIMM ID 界面 2

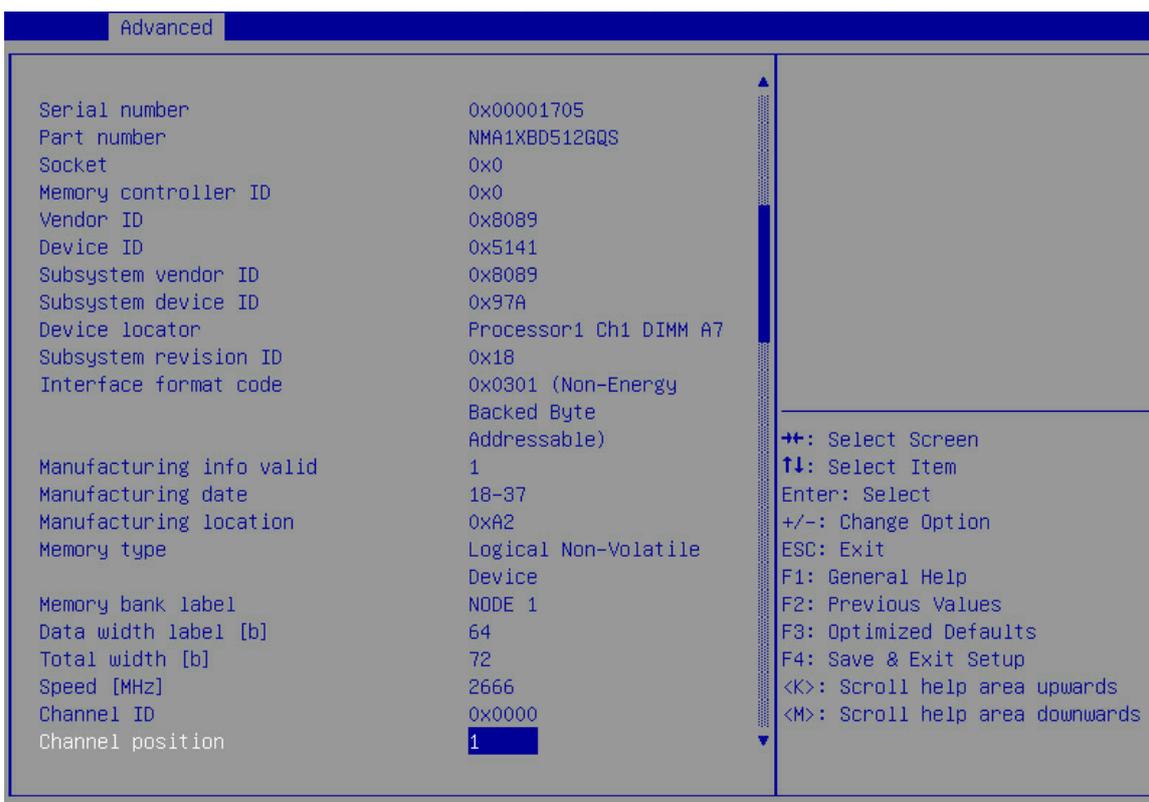


图3-45 DIMM ID 界面 3

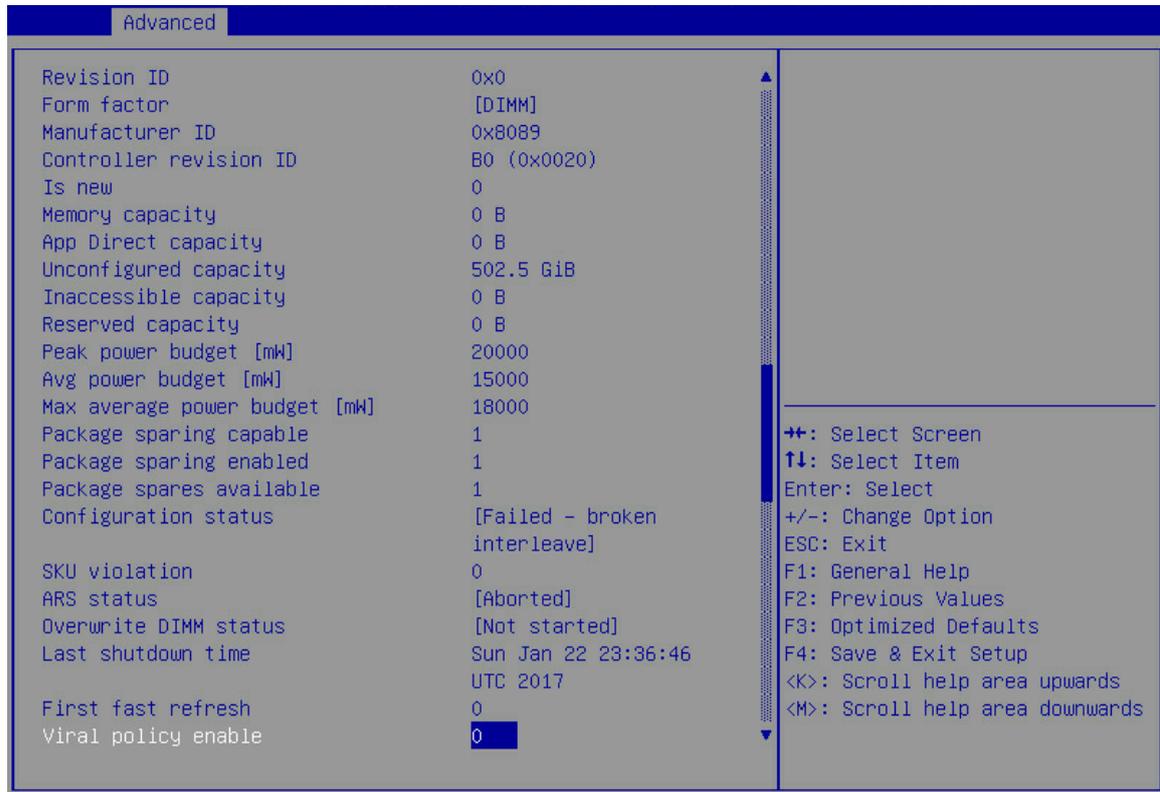


图3-46 DIMM ID 界面 4

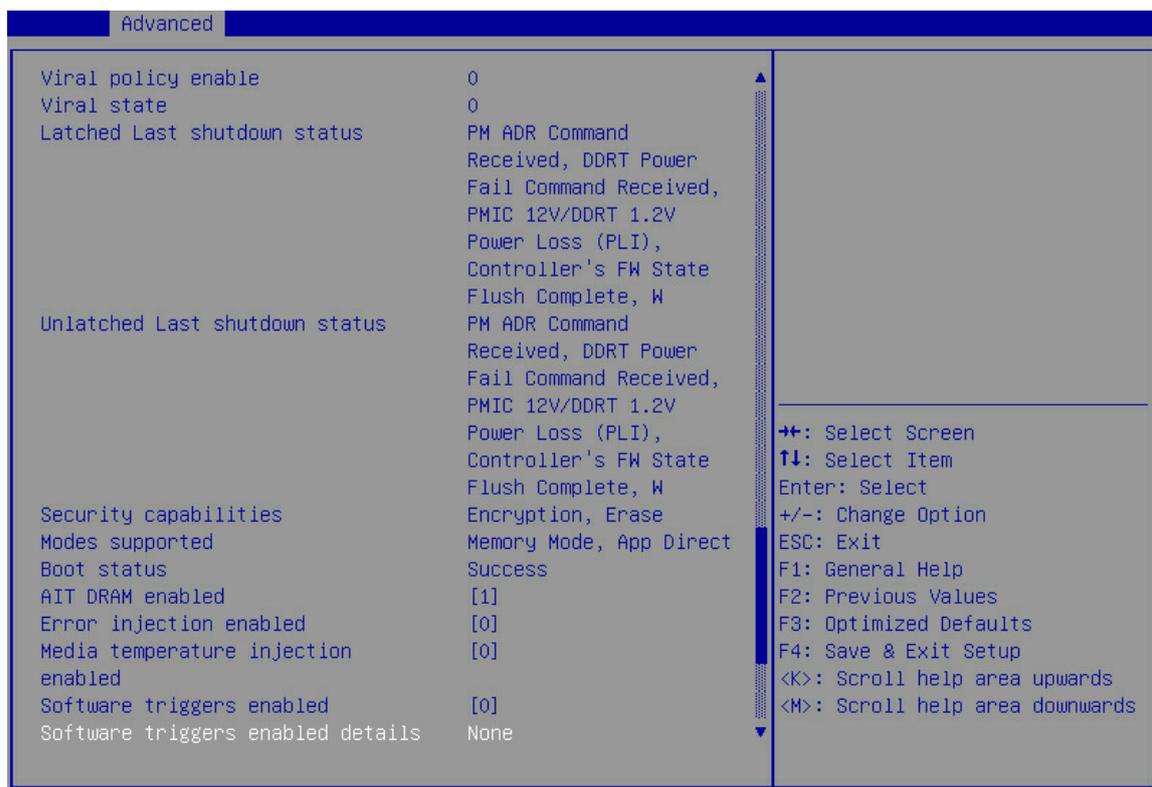


图3-47 DIMM ID 界面 5

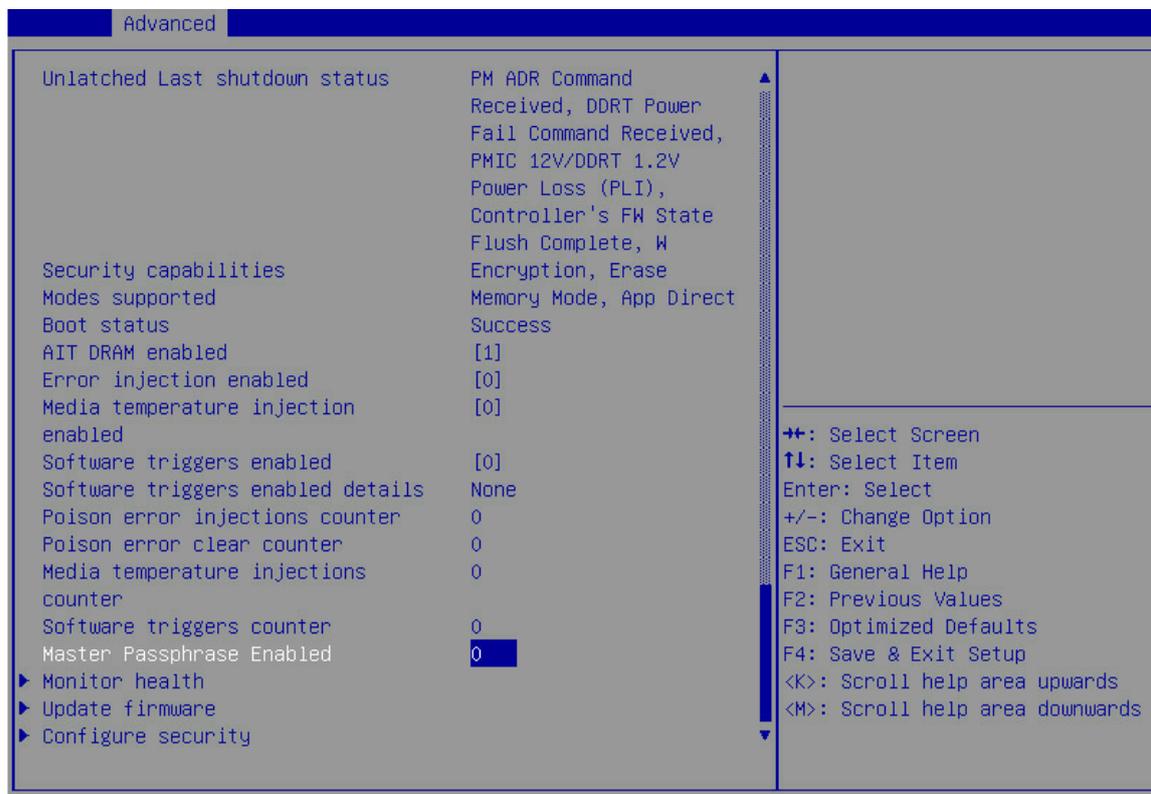


表3-43 DIMM ID 界面参数

界面参数	功能说明
DIMM UID	内存条的唯一标识ID，格式为VVVV-ML-MDMD-SNSNSNSN或者VVVV-SNSNSNSN(当生产信息无效的情况下使用)。 <ul style="list-style-type: none"> <li>• VVVV: 生产厂商ID。</li> <li>• ML: 制造地点。</li> <li>• MDMD: 生产日期。</li> <li>• SNSNSNSN: 序列号。</li> </ul>
DIMM handle	内存句柄。由ACPI决定。
DIMM physical ID	内存物理ID，用十六进制表示。
Manageability state	显示管理状态。可能的状态有： <ul style="list-style-type: none"> <li>• Manageable: 表示DIMM可以由BIOS管理。</li> <li>• Unmanageable: 表示DIMM无法由当前版本的BIOS管理。</li> </ul>
Health state	显示内存整体健康状态。可能的健康状态包括Healthy、Minor failure、Critical failure、Non-recoverable error、Unknown、Unmanageable。
Health state reason	当检测到Intel DCPMM健康状态异常时，显示异常原因。健康状态正常时显示为None。
Capacity	内存条容量。

界面参数	功能说明
Firmware version	固件版本号，格式为PN.RN.SV.bbbb。 <ul style="list-style-type: none"> <li>• PN: 2位数的产品编号。</li> <li>• RN: 2位数的修订号。</li> <li>• SV: 2位数的安全修订号。</li> <li>• bbbb: 4位数的编译版本。</li> </ul>
Firmware API version	固件API版本号。
Lock state	锁状态，表示内存当前安装状态。可能的状态有： <ul style="list-style-type: none"> <li>• Unknown: 无法获取到安全状态（例如，当Intel DCPMM内存无法被当前BIOS管理的情况）。</li> <li>• Disabled: 安全性未被启用。</li> <li>• Unlocked: 安全性已启用并已解锁。</li> <li>• Locked: 安全性已启用并已锁定。</li> <li>• Frozen: 可以启用和解锁安全性，也可以禁用安全性。但是，需要重启才能更改安全状态。</li> <li>• Exceeded: 已达到密码短语限制。需要电源循环来更改安全状态。</li> <li>• Not supported: 不支持安全性。</li> </ul>
Staged firmware version	分阶段固件版本。
Firmware update status	固件更新状态。
Manufacturer	生产厂商。
Show more details+	显示更多信息。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 显示更多Intel DCPMM内存信息。</li> <li>• Disabled: 隐藏Intel DCPMM内存信息。</li> </ul>
Monitor health	传感器信息菜单。 当Manageability state为Unmanageable时，该选项置灰。
Update firmware	固件升级菜单。 当Manageability state为Unmanageable时，该选项置灰。
Configure security	安全配置菜单。 当Manageability state为Unmanageable时，该选项置灰。
Configure data policy	数据策略配置菜单。 当Manageability state为Unmanageable时，该选项置灰。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。
<b>Intel DCPMM内存详细信息（Show more details+为Enabled时显示）</b>	
Serial number	序列号，十六进制显示。
Part number	供应商分配的部件号。
Socket	表示Intel DCPMM内存安装的处理器Socket号，十六进制数。
Memory controller ID	相关的内存控制器标识符。十六进制数。

界面参数	功能说明
Vendor ID	厂商号。十六进制数。
Device ID	设备号。十六进制数。
Subsystem vendor ID	非易失性存储器子系统控制器的供应商标识符。十六进制数。
Subsystem device ID	非易失性存储器子系统控制器的设备标识符。十六进制数。
Device locator	描述设备位置，处理器号-Channel号-内存槽位号。
Subsystem revision ID	非易失性存储器子系统控制器的修订标识符。十六进制数。
Interface format code	内存的类型。
Manufacturing info valid	标识生产信息是否有效。0表示无效，1表示有效。
Manufacturing date	生产日期。如果Manufacturing info valid为0，则为“N/A”。十六进制数。
Manufacturing location	制造地点。如果Manufacturing info valid为0，则为“N/A”。十六进制数。
Memory type	内存类型，Logical Non-Volatile Device表示逻辑非易失性设备。
Memory bank label	标识内存设备所在的物理Bank。
Data width label	用于存储用户数据的位宽度，单位为Bit。
Total width	数据和纠错和/或数据冗余的位宽。单位为Bit。
Speed	内存最大频率。
Channel ID	通道ID。
Channel position	通道位置。
Revision ID	修订标识符。
Form factor	组成因素。包含DIMM、SODIMM或者Unknown。
Manufacturer ID	生产厂商ID。
Controller revision ID	控制器版本ID。
Is new	Intel DCPMM是否与系统中的其余Intel DCPMM内存合并。 <ul style="list-style-type: none"> <li>0: 已配置。</li> <li>1: 需要配置。</li> </ul>
Memory capacity	配置为内存模式时的内存大小。
App Direct capacity	配置为App Direct模式时的内存大小。
Unconfigured capacity	无法访问的内存大小，这部分内存未映射到系统物理地址空间。
Inaccessible capacity	由于许可问题而无法访问的内存大小。
Reserved capacity	预留用于内存模式下正确对齐的内存大小。
Peak power budget [mW]	峰值功率预算。如果启用了电源管理策略，则以mW（10000-20000）显示用于瞬时功率的功率预算。默认值为10000 mW。

界面参数	功能说明
Avg power budget [mW]	平均功率预算。如果启用了电源管理策略，则以平均功耗的mW（10000-18000 mW）显示功率预算。默认值为10000 mW。
Max average power budget [mW]	以mW（10000-18000 mW）显示最大平均功率预算。
Package sparing capable	标识是否支持Package sparing策略。0表示不支持。1表示支持。
Package sparing enabled	标识是否启用了Package sparing策略。0表示未启用。1表示启用。
Package spares available	可用于Package sparing的设备数量。
Configuration status	内存的配置状态。包括： <ul style="list-style-type: none"> <li>Valid: 配置有效。</li> <li>Not configured: Intel DCPMM 未被配置。</li> <li>Failed - bad configuration: 配置错误，配置已损坏。</li> <li>Failed- broken interleave: 此内存是未完成的内存交织的一部分。</li> <li>Failed – reverted: 配置失败并恢复为上次已知的正确配置。</li> <li>Failed – unsupported: 该配置与安装的 BIOS 不兼容。</li> </ul>
SKU violation	表示是否由于许可证问题，不支持配置Intel DCPMM。 <ul style="list-style-type: none"> <li>0 表示不支持配置 Intel DCPMM。</li> <li>1 表示支持配置 Intel DCPMM。</li> </ul>
ARS status	ARS操作状态，ARS全称Address range scrub，地址范围清理。可能的状态包括： <ul style="list-style-type: none"> <li>Unknown: 无法确定 ARS 操作状态。</li> <li>Not started: 最后一次启动时未运行 ARS 操作。</li> <li>In progress: ARS 操作目前正在进行中。</li> <li>Completed: 自上次启动以来完成的 ARS 操作。</li> <li>Aborted: ARS 操作在上次启动时启动但由于中止而未完成。</li> </ul>
Overwrite DIMM status	内存重写状态。状态包括： <ul style="list-style-type: none"> <li>Unknown: 无法确定重写操作状态。</li> <li>Not started: 最后一次启动时没有运行重写操作。</li> <li>In progress: 目前正在进行重写操作。</li> <li>Completed: 完成重写操作并需要重新启动才能使用内存。</li> </ul>
Last shutdown time	系统上次关闭的时间。
First fast refresh	是否为Intel DIMM启用了第一个刷新周期的加速。 <ul style="list-style-type: none"> <li>0: 表示禁用。</li> <li>1: 启用。在开始基准测试之前，客户必须等待预定的时间（5-6分钟）。</li> </ul>
Viral policy enable	设置病毒模式策略。菜单选项为： <ul style="list-style-type: none"> <li>0: 不启用。</li> <li>1: 启用。如果主机操作系统软件检测到无法纠正的错误情况并指示病毒状态以防止损坏扩散，则 Intel 内存上的持久性内存将进入只读模式。</li> </ul>

界面参数	功能说明
Viral state	表示当前是否处于病毒状态。0表示不处于，1表示处于。
Latched Last shutdown status	<p>锁定Intel内存上次关闭的状态。可能的状态包括：</p> <ul style="list-style-type: none"> <li>• Unknown: 无法确定上次关机状态。</li> <li>• FW Flush Complete: 固件刷新完成。</li> <li>• PM ADR Command: 收到电源管理 ADR 命令。</li> <li>• PM S3: 收到电源管理 S3 命令。</li> <li>• PM S5: 收到电源管理 S5 命令。</li> <li>• DDRT Power Fail Command: 收到 DDR 电源故障命令。</li> <li>• PMIC 12V/DDRT 1.2V Power Loss (PLI): PMIC 功率损耗。</li> <li>• PM Warm Reset: 接收电源管理热复位。</li> <li>• Thermal Shutdown: 触发过温重启。</li> <li>• Controller's FW Statue Flush Complete: 刷新完成。</li> <li>• Viral Interrupt: 收到病毒中断。</li> <li>• Surprise Clock Stop: 出现意外的时钟暂停。</li> <li>• Write Data Flush Complete: 写数据刷新完成。</li> <li>• PM S4: 收到电源管理 S4 命令。</li> <li>• PM Idle: 收到电源管理空闲状态。</li> <li>• DDRT Surprise Reset: 意外重启。</li> </ul>
Unlatched last shutdown status	<p>解锁Intel内存上次关闭的状态。可能的状态包括：</p> <ul style="list-style-type: none"> <li>• Unknown: 无法确定上次关机状态。</li> <li>• FW Flush Complete: 固件刷新完成。</li> <li>• PM ADR Command: 收到电源管理 ADR 命令。</li> <li>• PM S3: 收到电源管理 S3 命令。</li> <li>• PM S5: 收到电源管理 S5 命令。</li> <li>• DDRT Power Fail Command: 收到 DDRT 电源故障命令。</li> <li>• PMIC 12V/DDRT 1.2V Power Loss (PLI): PMIC 功率损耗。</li> <li>• PM Warm Reset: 接收电源管理热复位。</li> <li>• Thermal Shutdown: 触发过温重启。</li> <li>• Controller's FW Statue Flush Complete: 刷新完成。</li> <li>• Viral Interrupt: 收到病毒中断。</li> <li>• Surprise Clock Stop: 出现意外的时钟暂停。</li> <li>• Write Data Flush Complete: 写数据刷新完成。</li> <li>• PM S4: 收到电源管理 S4 命令。</li> <li>• PM Idle: 收到电源管理空闲状态。</li> <li>• DDRT Surprise Reset: 意外重启。</li> </ul>

界面参数	功能说明
Security capabilities	显示支持的安全功能，包括： <ul style="list-style-type: none"> <li>• <b>None:</b> 不支持任何安装功能。</li> <li>• <b>Encryption:</b> 支持通过设置密码来支持持久性内存加密。</li> <li>• <b>Erase:</b> 可擦除。</li> </ul>
Modes supported	Intel DCPMM内存支持的模式列表。包括： <ul style="list-style-type: none"> <li>• <b>Memory Mode:</b> Intel DCPMM 内存存在操作系统的控制下充当系统内存。在内存模式下，平台中的任何DDR都将充当与Intel DCPMM配合使用的缓存。</li> <li>• <b>App Direct:</b> 英特尔 DIMM 和 DDR 在应用程序的直接加载/存储控制下充当独立的内存资源。</li> </ul>
Boot status	由引导状态寄存器中的固件报告的Intel DIMM的初始化状态。包括： <ul style="list-style-type: none"> <li>• <b>Unknown:</b> 无法读取引导状态寄存器。</li> <li>• <b>Success:</b> 初始化期间未报告任何错误。</li> </ul> 以下状态表明内存未生效，因此访问需要使用内存的用户数据和操作将失败。 <ul style="list-style-type: none"> <li>• <b>Media not ready:</b> 固件无法完成内存 Tranning。访问需要使用媒体的用户数据和操作将失败。</li> <li>• <b>Media error:</b> 固件在内存 Tranning 期间检测到错误。</li> <li>• <b>Media disabled:</b> 由于严重问题，固件禁用了内存。</li> </ul> 以下状态表明与固件的通信不起作用。 <ul style="list-style-type: none"> <li>• <b>DDRT not ready:</b> DDRT 接口未正确初始化。</li> <li>• <b>FW Assert:</b> 固件在初始化期间报告了断言。</li> <li>• <b>Mailbox not ready:</b> 固件无法初始化通信接口。</li> </ul>
AIT DRAM enabled	是否启用了Intel DIMM AIT DRAM。 <ul style="list-style-type: none"> <li>• <b>0:</b> 禁用，如果 AIT DRAM 被禁用，将引起内存性能下降。</li> <li>• <b>1:</b> 启用。</li> </ul>
Error injection enabled	是否启用故障注入。 <ul style="list-style-type: none"> <li>• <b>0 (缺省):</b> 表示禁用。</li> <li>• <b>1:</b> 表示启用。</li> </ul>
Media temperature injection enabled	是否启用故障注入。 <ul style="list-style-type: none"> <li>• <b>0 (缺省):</b> 表示禁用。</li> <li>• <b>1:</b> 表示启用。</li> </ul>
Software trigger enabled	是否启用软件触发。 <ul style="list-style-type: none"> <li>• <b>0 (缺省):</b> 表示禁用。</li> <li>• <b>1:</b> 表示启用。</li> </ul>
Poison error injections counter	Poison错误注入计数。每次成功执行set poison error命令时，此计数器都会递增。
Poison error clear counter	Poison错误清空计数。每次成功执行clear poison error命令时，此计数器都会递增。

界面参数	功能说明
Media temperature injections counter	每次注入Media温度时，此计数器都会递增。
Software triggers counter	每次启用软件触发时，此计数器都会递增。
Master Passphrase Enabled	表示已启用主密码。

如[图 3-48](#)、[图 3-49](#)和[图 3-50](#)所示，通过Monitor health界面可查看并配置Intel DCPMM内存传感器的参数。具体参数说明如[表 3-44](#)所示。

图3-48 Monitor health 界面 1

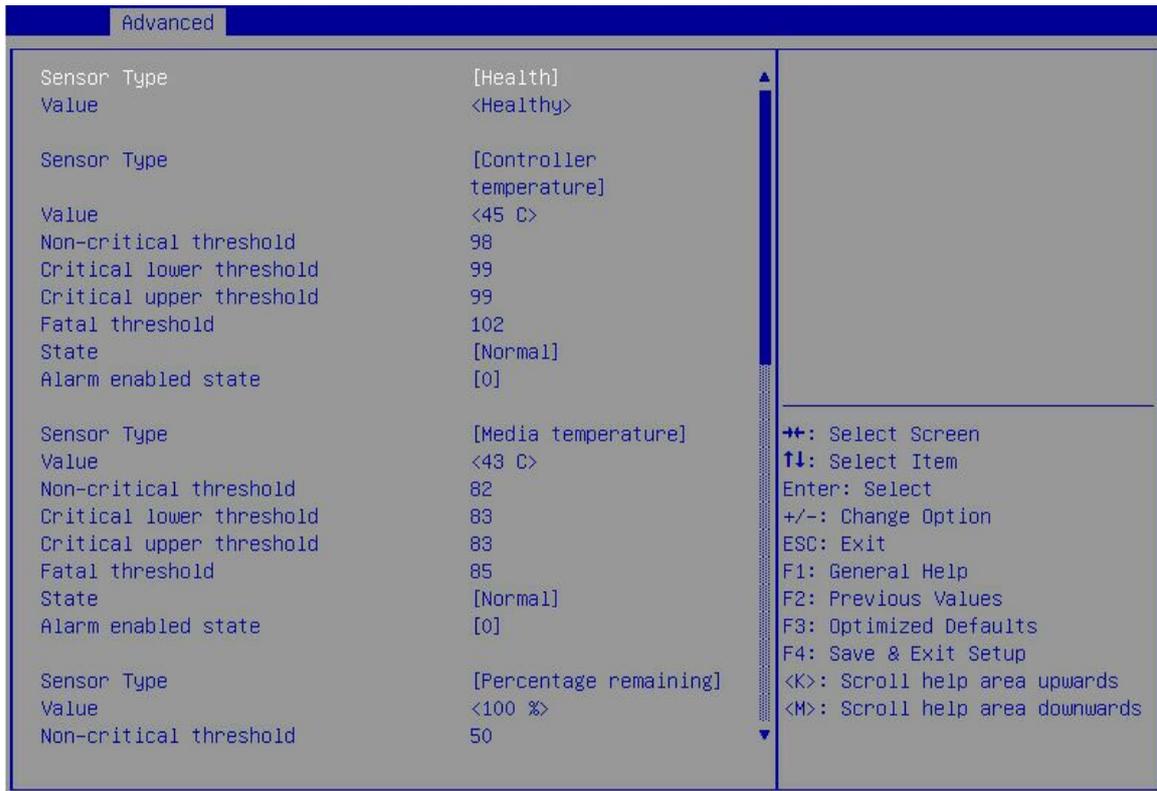


图3-49 Monitor health 界面 2

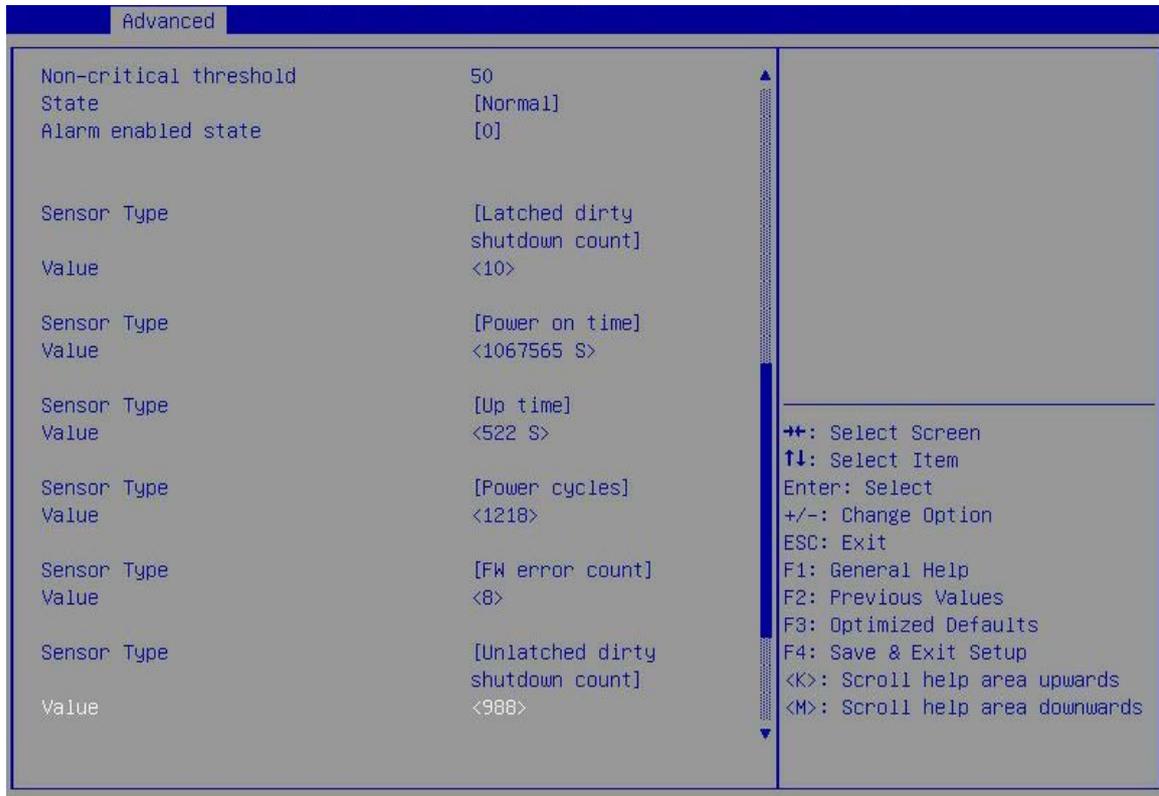


图3-50 Monitor health 界面 3

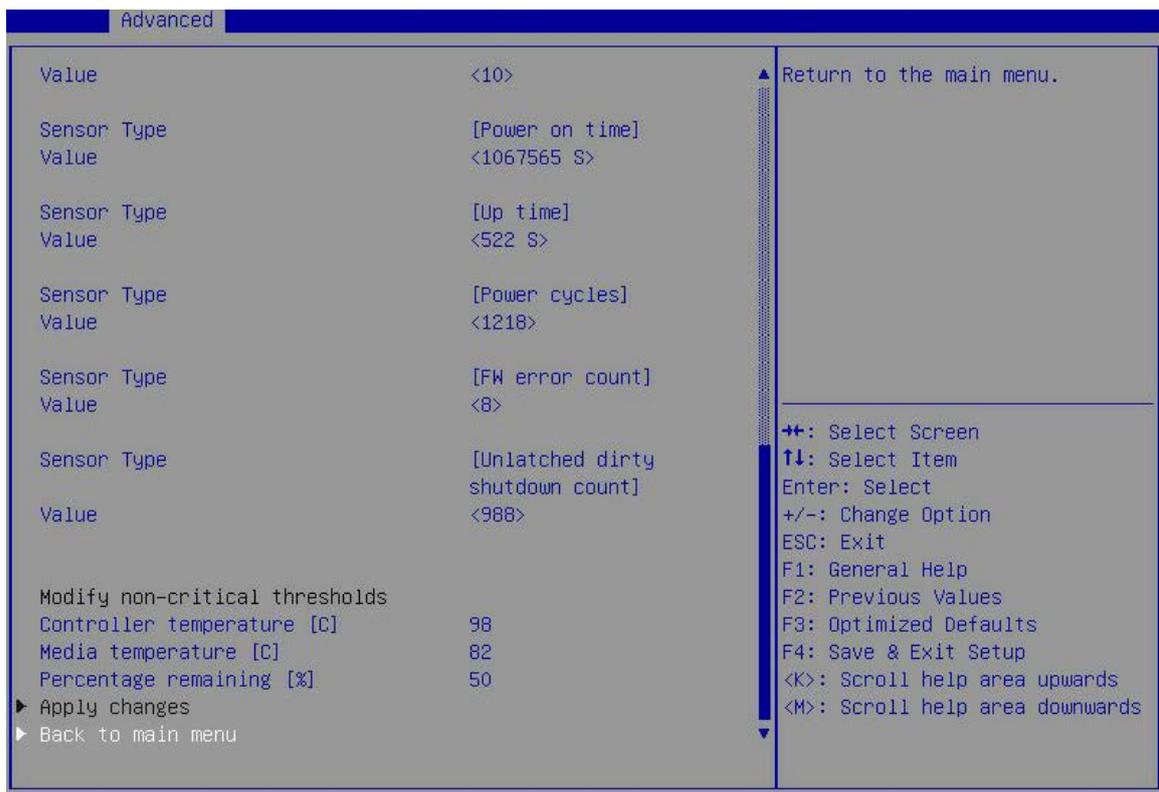


表3-44 Monitor health 界面参数

界面参数	功能说明
Sensor Type	<p>显示当前传感器的类型。Intel DCPMM内存上的传感器包括以下几种类型：</p> <ul style="list-style-type: none"> <li>• Health: 表示 Intel DCPMM 内存总健康状态传感器。</li> <li>• Controller temperature: 控制器温度传感器。</li> <li>• Media temperature: 介质温度传感器。</li> <li>• Percentage remaining: 剩余容量百分比。</li> <li>• Latched dirty shutdown count: 锁定异常掉电次数。</li> <li>• Power on time: 上电时长。</li> <li>• Up time: 运行时间。</li> <li>• Power cycles: 重新启动。</li> <li>• FW error count: 固件错误计数。</li> <li>• Unlatched dirty shutdown count: 解锁异常掉电次数</li> </ul>
Value	显示当前传感器的值。
Non-critical threshod	温度传感器上报非严重错误的阈值。
Critical lower threshod	温度传感器上报严重错误的阈值下限。
Critical upper threshod	温度传感器上报严重错误的阈值上限。
Fatal threshod	温度传感器上报致命错误阈值。
State	<p>当前传感器状态。可能的状态包括：</p> <ul style="list-style-type: none"> <li>• Unknown: 状态无法确定。</li> <li>• Normal: 表示 当前读数在正常范围内。</li> <li>• Noncritical: 表示 当前读数在非临界范围内。</li> <li>• Critical: 表示 当前读数在临界范围内。</li> <li>• Fatal: 目前的读数在致命范围内。</li> </ul> <p>仅Controller temperature, Media temperature和Percentage remaining 传感器显示该选项。</p>
Alarm enabled state	<p>警报启用状态。</p> <ul style="list-style-type: none"> <li>• 0: 表示未启用。</li> <li>• 1: 表示启用。启用后, 当温度传感器检测到超过非严重错误阈值时发出警报。</li> </ul>
<b>Modity non-critical thresholds</b>	
Controller temperature	设置控制器温度阈值, 单位为摄氏度。最低20℃, 最高105℃。
Media temperature	设置介质温度阈值, 单位为摄氏度。最低20℃, 最高85℃
Percentage remaining	最低1%, 最高99%。
Apply changes	应用修改, 当修改了传感器非严重阈值后, 需要点本选项保存修改, 修改即时生效。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-51 所示，通过 Update firmware 界面可查看并升级 Intel DCPMM 内存固件版本。具体参数说明如表 3-45 所示。

图3-51 Update firmware 界面

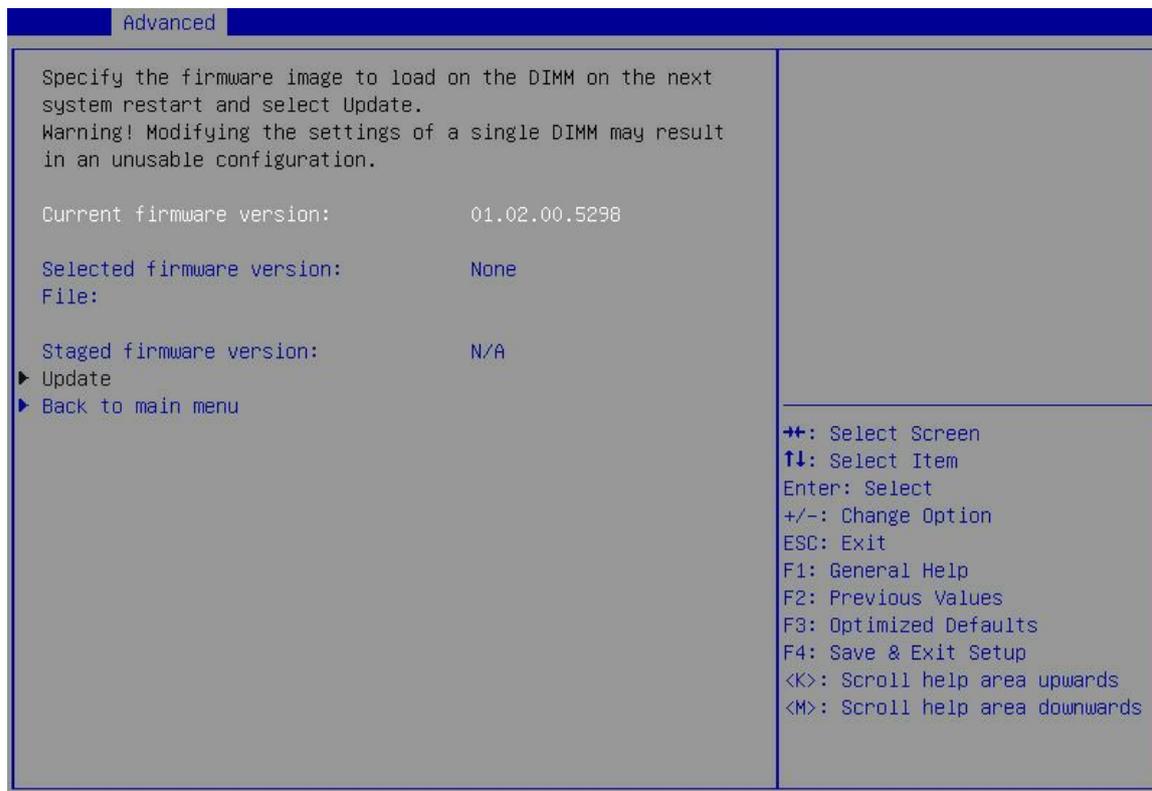


表3-45 Update firmware 界面参数

界面参数	功能说明
Current firmware version	显示当前固件版本号。
Selected firmware version	显示当前选择的固件版本。 <ul style="list-style-type: none"> <li>None: 用户尚未在File选项中输入文件路径。</li> <li>Incorrect FW: 用户输入了无效的文件路径。</li> <li>(version): 指定的FW文件的固件版本。</li> </ul>
File	输入保存固件文件的路径，需要输入与根路径的相对地址。比如： \\firmware\\newFirmware.bin
Staged firmware version	显示当前的暂存的固件版本。Mixed表示多个Intel DCPMM内存中包含了不同版本的固件，N/A表示没有固件暂存在Intel DCPMM内存中。
Update	开始固件升级。重启后生效。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-52 所示，通过 Configure security 界面可配置 Intel DCPMM 内存安全功能。具体参数说明如表 3-46 所示。

图3-52 Configure security 界面

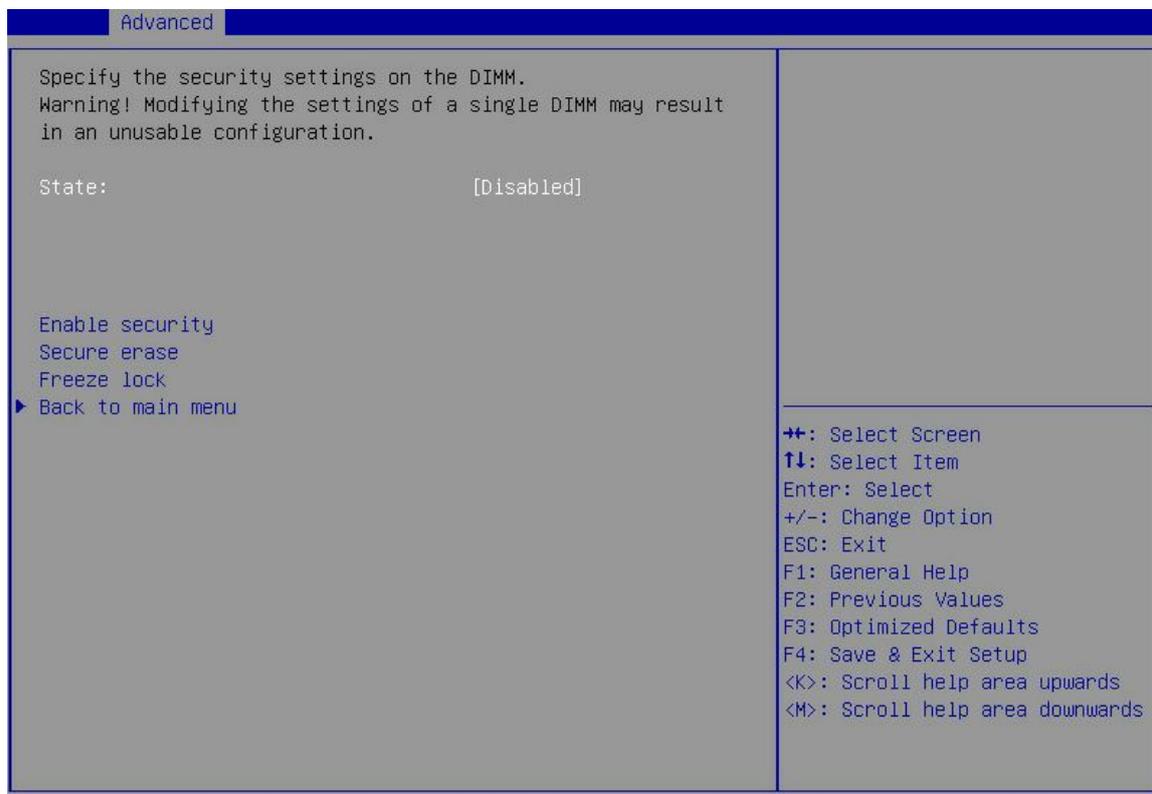


表3-46 Configure security 界面参数

界面参数	功能说明
State	当前安全状态。可能的状态包含： <ul style="list-style-type: none"> <li>• Disabled: 安全性未启用。</li> <li>• Unlocked: 安全性已启用并已解锁。</li> <li>• Locked: 安全性已启用并已锁定。</li> <li>• Frozen: 安全性已启用并已解锁。但是，需要重新启动才能更改安全状态。</li> <li>• Exceeded: 已达到密码限制。需要重启来更改安全状态。</li> <li>• Not supported: 不支持安全性。</li> </ul>
Enable security	选择该选项，启用Intel DCPMM内存安全设置。设置后需要重启生效。
Secure erase	用户擦除Intel DIMM上的持久性内存。如果Intel DIMM处于解锁状态，则需要输入当前密码。如果禁用安全性，则会显示确认弹出窗口。仅在解锁或禁用Intel DIMM的安全状态时可见。
Freeze lock	用户可以防止对Intel DIMM进一步锁定状态更改，直到下次重新启动。无需密码即可将安全状态更改为冻结状态。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-53 所示，通过Configure data policy界面可配置Intel DCPMM内存数据策略。具体参数说明如表 3-47 所示。

图3-53 Configure data policy 界面

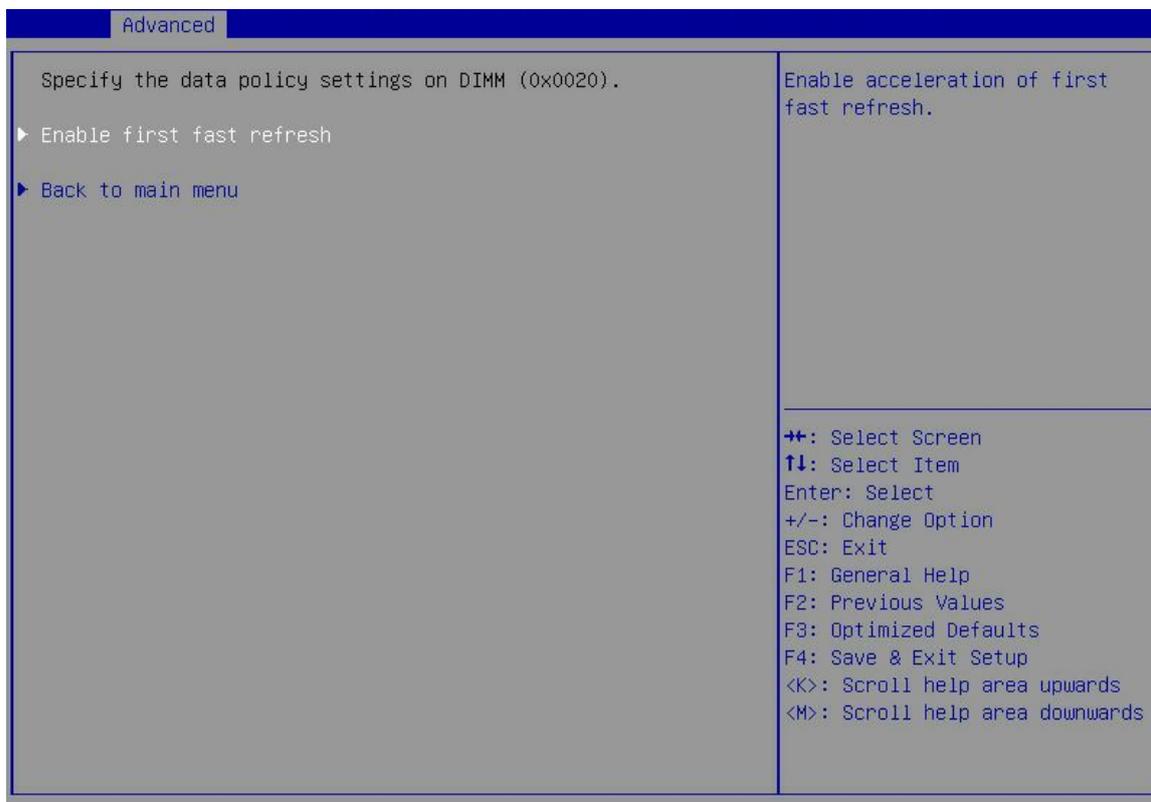


表3-47 Configure data policy 界面参数

界面参数	功能说明
First fast refresh state	<p>第一快速自刷新状态。仅当从表3-42的“Configure data policy选项”进入此页面时显示，表示所有内存的第一快速自刷新状态。可能显示的状态包括：</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> 启用第一次快速刷新。</li> <li>• <b>Disabled:</b> 禁用第一次快速刷新。</li> <li>• <b>Mixed:</b> 多根 Intel DIMM 的第一次快速刷新策略不同。</li> </ul>
Enable first fast refresh	启用第一个快速刷新周期的加速。仅当禁用了第一次快速刷新时显示。
Disable first fast refresh	禁用第一个快速刷新周期的加速。仅当启用了第一次快速刷新时显示。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

## 2. Regions 界面

由于修改内存配置需要重新启动才能生效，因此可以将任何目标配置视为待定目标配置。可以同时具有当前配置和待定目标配置。

重新启动系统后，将应用待定的目标配置，它将应用为当前配置，也可以在重启之前删除待定目标配置。

如图 3-54所示，Regions界面以区域的形式显示系统中持久性内存的当前配置，使用户能够查看系统中指定的任何待定目标配置。具体参数说明如表 3-48所示。

图3-54 Regions 界面

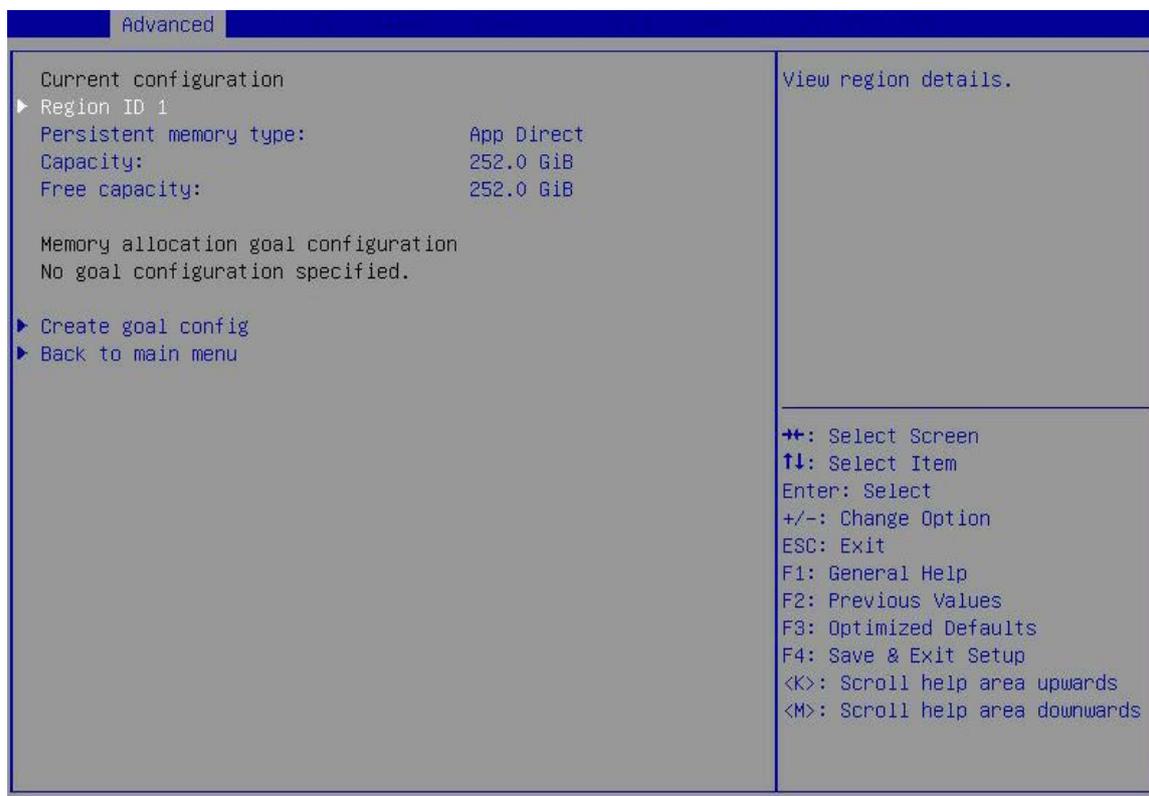


表3-48 Regions 界面参数

界面参数	功能说明
<b>Current configuration</b>	
Region ID	对应区域的详细信息菜单
Persistent memory type	当前内存类型，包括App Direct和App Direct Not Interleaved。
Capacity	区域总容量（GB）
Free capacity	空闲容量大小（GB）
<b>Memory allocation goal configuration（仅当在create goal config页面创建目标配置后，未重启生效前显示）</b>	
DIMM ID	目标内存配置详细信息菜单。
MemorySize	内存大小。对于每个待定内存配置目标，在相应的Dimm ID操作下针对每个Intel DIMM重复显示。 仅在存在一个或多个待定内存配置目标时显示。
AppDirect1Size	第一个App Direct交织的容量
AppDirect2Size	第二个App Direct交织的容量
Create goal config	创建DIMM区域的目标配置。

界面参数	功能说明
Delete goal config	丢弃区域目标配置，仅当在Create goal config页面创建目标配置后，未重启生效前显示。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图3-55所示，通过Region ID界面显示了持久内存区域的详细信息。具体参数说明如表3-49所示。

图3-55 Region ID 界面

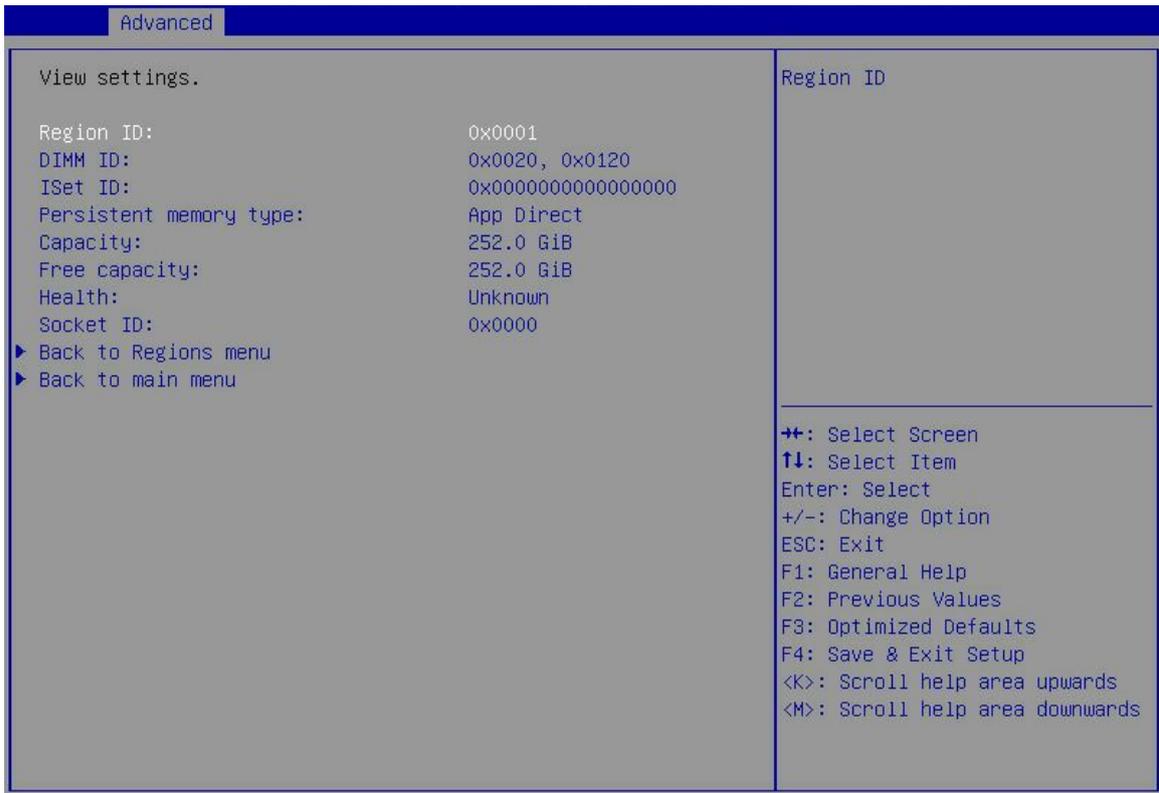


表3-49 Region ID 界面参数

界面参数	功能说明
Region ID	显示区域ID。十六进制数。
DIMM ID	显示区域包含的DIMM ID。
ISet ID	ISet编号。
Persistent memory type	该区域中持久性内存容量的基础类型列表。 <ul style="list-style-type: none"> <li>App Direct: 跨两个或更多Intel DIMM交织App Direct容量。默认为该选项。</li> <li>App Direct Not Interleaved: App Direct容量完全包含在单个Intel DIMM中。</li> </ul>
Capacity	总可用容量，已分配和未分配的总和。
Free capacity	剩余的可用容量。

界面参数	功能说明
Health	Intel DIMM容量的健康状况。可能的状态包含： <ul style="list-style-type: none"> <li>• Health: 所有基础英特尔DIMM持久性内存均可用。</li> <li>• Pending: 已创建新的内存分配目标但未应用。</li> <li>• Error: 交织设置错误。</li> <li>• Locked: 一个或多个底层Intel DIMM已锁定。</li> <li>• Unknown: 区域健康状态无法确定。</li> </ul>
Socket ID	区域所属的Socket ID。
Back to Regions menu	返回Regions菜单
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-56所示，通过DIMM ID界面 显示待定目标配置的详细信息。具体参数说明如表 3-49所示。

图3-56 DIMM ID 界面

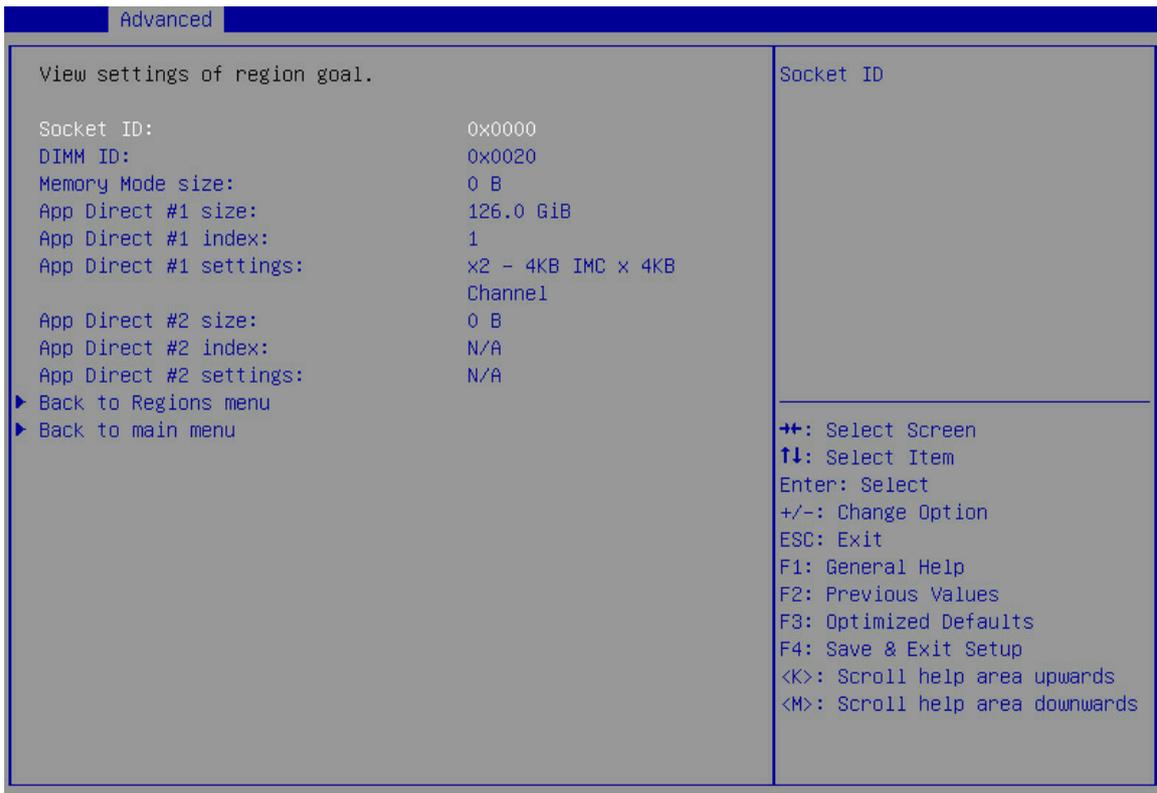


表3-50 DIMM ID 界面参数

界面参数	功能说明
Socket ID	显示该内存条所属的Socket编号。
DIMM ID	显示内存条的编号。
Memory Mode size	将在内存模式下配置的Intel DIMM容量。

界面参数	功能说明
App Direct #1 size	将配置为第一个App Direct交织的容量。
App Direct #1 index	第一个App Direct交织集的唯一标识。当App Direct #1 size为0时，显示为N/A。
App Direct #1 setting	第一个App Direct交织集的格式设置为： x(DIMM编号) – (IMC大小) IMC x (Channel size) Channel 当App Direct #1 size为0时，显示为N/A。
App Direct #2 size	将配置为第二个App Direct交织的容量。
App Direct #2 index	第二个App Direct交织集的唯一标识。当App Direct #2 size为0时，显示为N/A。
App Direct #2 setting	第二个App Direct交织集的格式设置为： x(DIMM编号) – (IMC大小) IMC x (Channel size) Channel 当App Direct #2 size为0时，显示为N/A。
Back to Regions menu	返回Regions菜单。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-57 所示，通过Create goal config界面 创建一个新的内存分配目标。具体参数说明如表 3-51 所示。

图3-57 Create goal config 界面

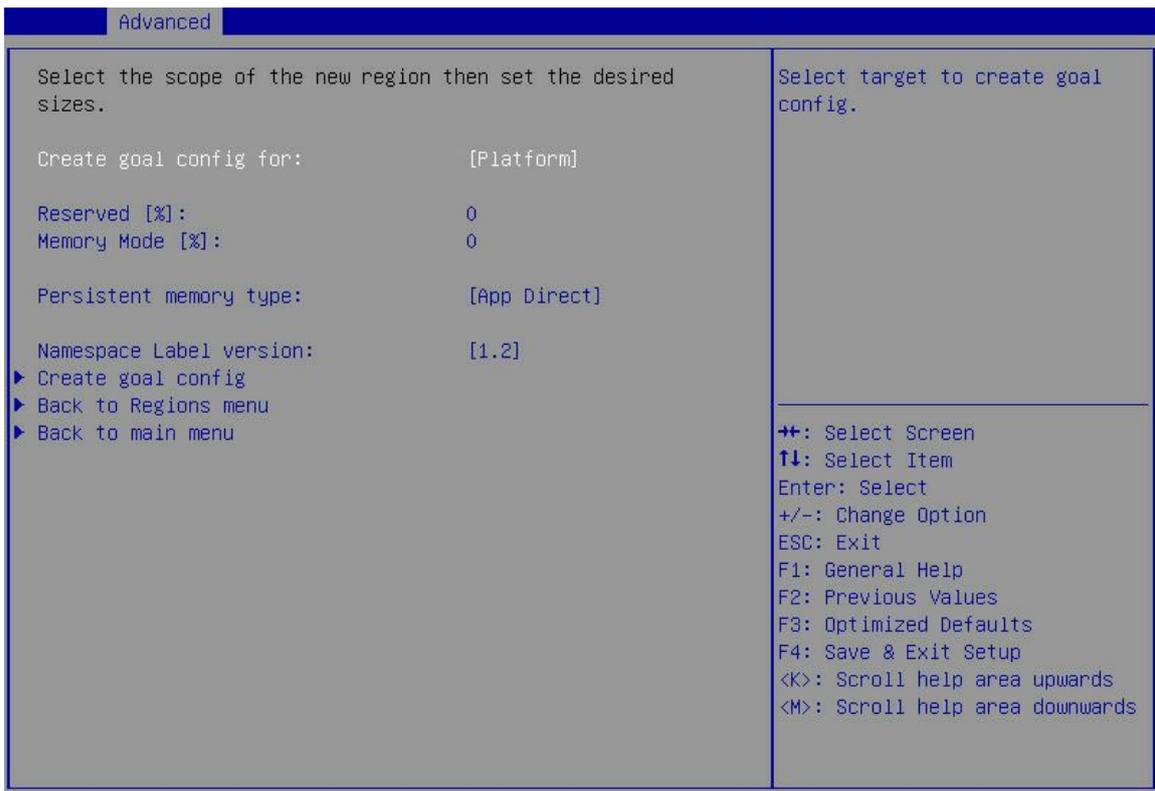


表3-51 Create goal config 界面参数

界面参数	功能说明
Create goal config for	<p>选择目标以创建目标配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Platform:</b> 在平台中的所有 <b>Socket</b>上创建内存分配目标。这是默认值。</li> <li>• <b>Socket:</b> 在用户指定的 <b>Socket</b>上的Intel DIMM上创建内存分配目标。</li> <li>• <b>Partially-configured sockets:</b> 在用户选择的 <b>Socket</b>上创建内存分配目标，这些 <b>Socket</b>由于添加了新的Intel DIMM而部分配置。如果已配置至少一个DIMM，并且至少有一个DIMM未配置，则部分配置这个 <b>Socket</b>。该选项在没有部分配置的 <b>Socket</b>时不显示。</li> </ul>
Reserved	预留空间的百分比（0%~100%）。保留一段空间不映射到系统物理地址空间。
Memory Mode	设置使用在内存模式的比例（0%~100%），由于平台内存对齐要求，设置的值将自动对齐。
Persistent memory type	<p>选择要创建的持久性内存容量的类型。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>App Direct:</b> 跨 DIMM 交织。</li> <li>• <b>App Direct Not Interleaved:</b> 不使用硬件交织。</li> </ul> <p>该选项在 <b>Memory Mode</b> 设置为 100%时置灰。</p>
Namespace Label version	<p>命名空间标签版本。菜单选项为：</p> <ul style="list-style-type: none"> <li>• 1.2</li> <li>• 1.1</li> </ul>
Create goal config	创建目标配置。
Back to Regions menu	返回Regions菜单。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如[图 3-58](#)所示，通过Delete goal config界面删除已经存在的内存目标配置。具体参数说明如[表 3-52](#)所示。

图3-58 Delete goal config 界面

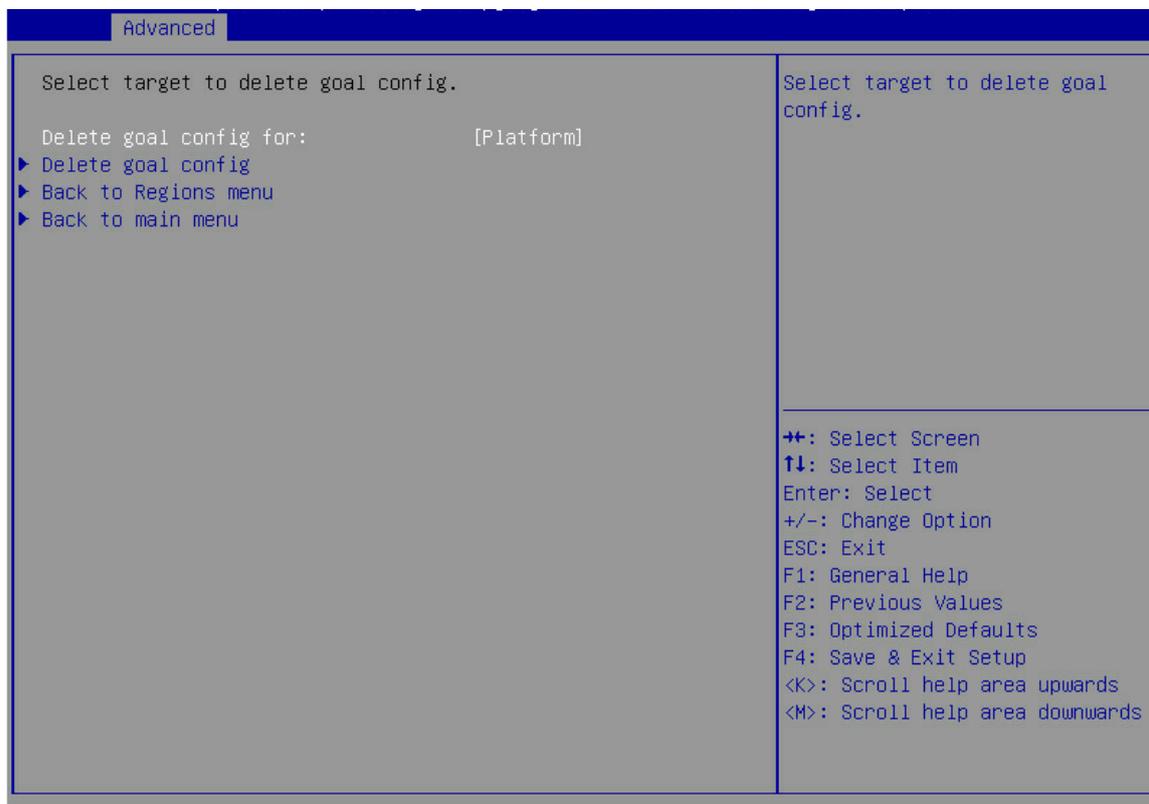


表3-52 Delete goal config 界面参数

界面参数	功能说明
Delete goal config for	选择删除目标配置的目标。菜单选项为： <ul style="list-style-type: none"> <li>Platform</li> <li>Socket</li> </ul>
Delete goal config	删除选定的目标配置。
Back to Regions menu	返回Regions菜单
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

### 3. Namespaces 界面

如图 3-59所示，通过Namespace界面可查看和配置命名空间。Namespace需要在已存在Region的情况下配置。具体参数说明如表 3-53所示。

图3-59 Namespace 界面

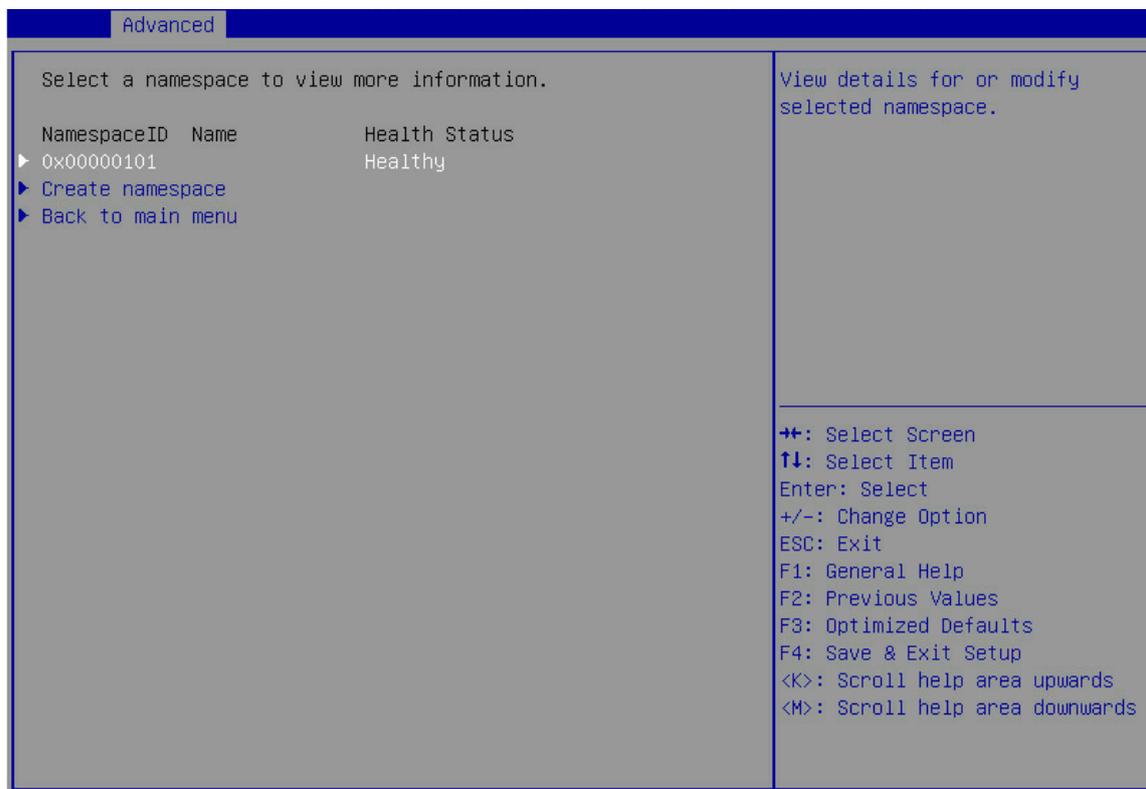


表3-53 Namespace 界面参数

界面参数	功能说明
Namespace ID / Name / Health Status	命名空间配置菜单。仅当系统中存在命名空间时显示。 <ul style="list-style-type: none"> <li>• <b>Namespace ID:</b> 命名空间的 ID，以十六进制数。</li> <li>• <b>Name:</b> 创建命名空间时输入的命名空间名称。</li> <li>• <b>Health Status:</b> 健康状态。可能的状态包括：<b>Healthy / Warning / Critical / Locked / Unknown</b>。</li> </ul>
Create namespace	创建命名空间菜单。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如[图 3-60](#)所示，通过Create namespace界面可创建命名空间。具体参数说明如[表 3-54](#)所示。

图3-60 Create namespace 界面

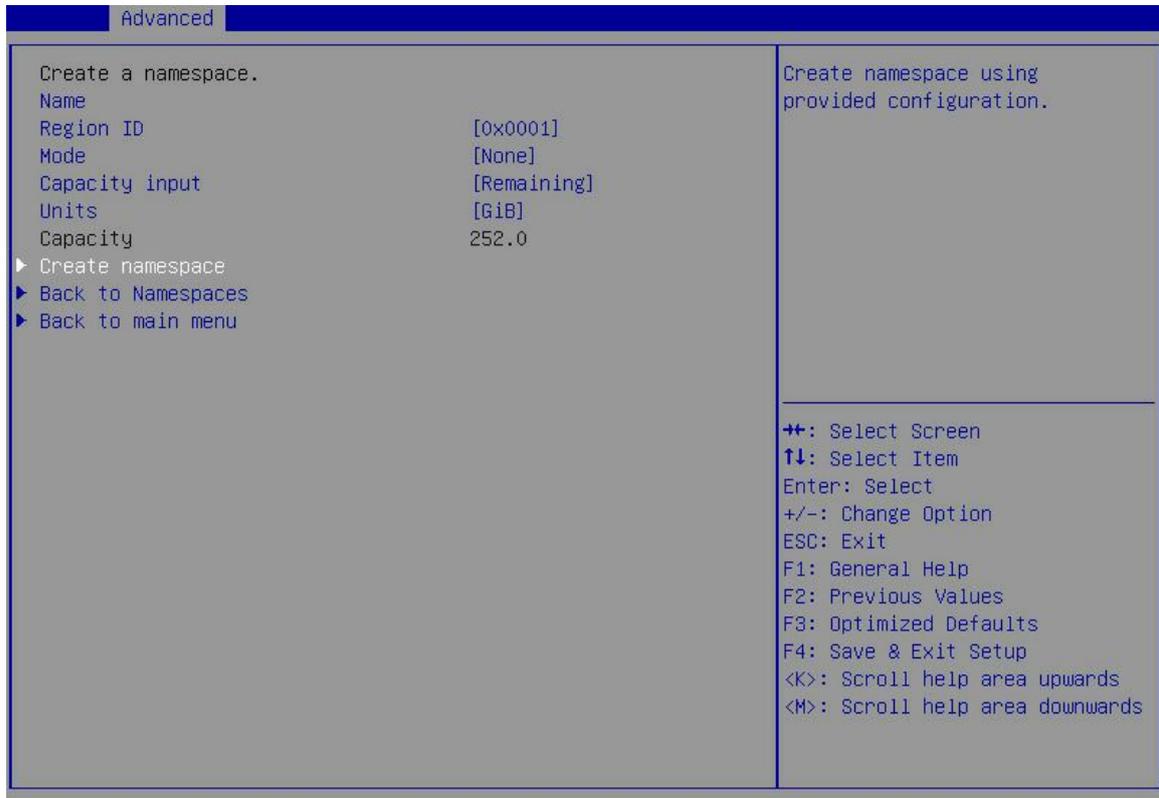


表3-54 Create namespace 界面参数

界面参数	功能说明
Name	输入命名空间名称。最多 63 个字符。
Region ID	创建命名空间的区域ID。
Mode	命名空间的模式。菜单选项为： <ul style="list-style-type: none"> <li>• None（缺省）：仅限原始访问。</li> <li>• Sector：通过块转换表（BTT）保证powerfail写入的原子性。</li> </ul>
Capacity input	使用最大可用容量或手动输入容量。菜单选项为： <ul style="list-style-type: none"> <li>• Remaining（缺省）：使用指定区域上指定持久性内存类型的最大可用容量作为新命名空间。</li> <li>• Manual：手动输入新命名空间的容量。</li> </ul>
Units	显示容量的单位。菜单选项为： <ul style="list-style-type: none"> <li>• GiB（缺省）</li> <li>• GB</li> <li>• B</li> <li>• MB</li> <li>• MiB</li> <li>• TB</li> <li>• TiB</li> </ul>

界面参数	功能说明
Capacity	命名空间的容量。当Capacity input选项设置为Remaining时，该选项置灰。
Create namespace	创建命名空间。
Back to Namespaces	返回命名空间配置菜单
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

如图 3-61 所示，通过命名空间配置界面可修改和删除现有的命名空间，必须点击“保存”才能使对该命名空间的修改生效。具体参数说明如表 3-55 所示。

图3-61 命名空间配置界面

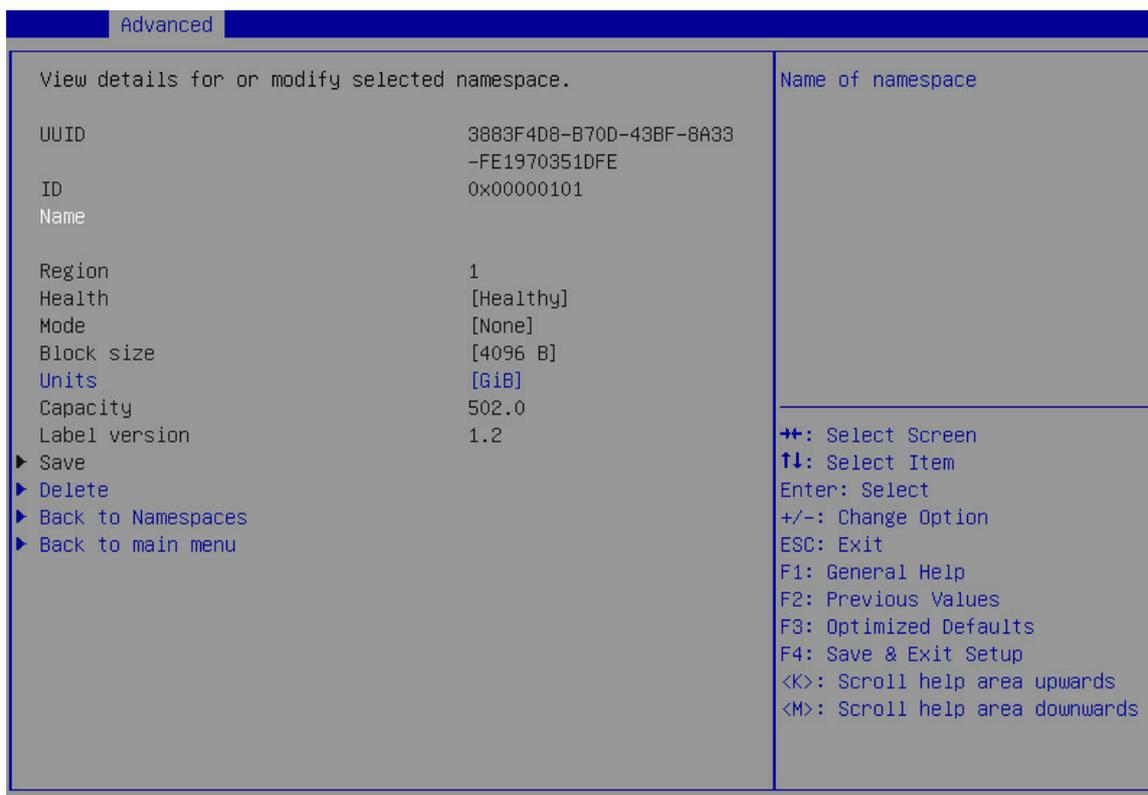


表3-55 命名空间配置界面参数

界面参数	功能说明
UUID	命名空间的唯一标识符。
ID	命名空间ID，十六进制。
Name	命名空间名称，最长 63 个字符。
Region	创建命名空间的区域的标识符。以十进制显示。

界面参数	功能说明
Health	基础 Intel DIMM 的健康状态。可能的状态包括： <ul style="list-style-type: none"> <li>• Healthy</li> <li>• Warning</li> <li>• Critical</li> <li>• Locked</li> <li>• Unknown</li> <li>• Unsupported: 不支持命名空间的类型。</li> </ul>
Mode	命名空间模式。 <ul style="list-style-type: none"> <li>• Sector: 通过块转换表 (BTT) 保证powerfail写入原子性。</li> <li>• Fsdax: 支持filesystem-dax。</li> <li>• None: 仅限原始访问。</li> </ul>
Block size	逻辑块大小。
Units	可设置容量的单位。菜单选项为： <ul style="list-style-type: none"> <li>• GiB</li> <li>• GB</li> <li>• B</li> <li>• MB</li> <li>• MiB</li> <li>• TB</li> <li>• TiB</li> </ul>
Capacity	命名空间的容量。
Label Version	LSA版本。对于所有命名空间应该是相同的。有1.1版本和1.2版本。
Save	保存修改。必须点击“保存”才能使对该命名空间的修改生效
Delete	删除命名空间。
Back to Namespaces	返回命名空间配置菜单
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

#### 4. Total capacity 界面

如[图 3-62](#)所示，通过Total capacity界面可查看系统中 整个Intel DCPMM内存资源分配情况。具体参数说明如[表 3-56](#)所示。

图3-62 Total capacity 界面

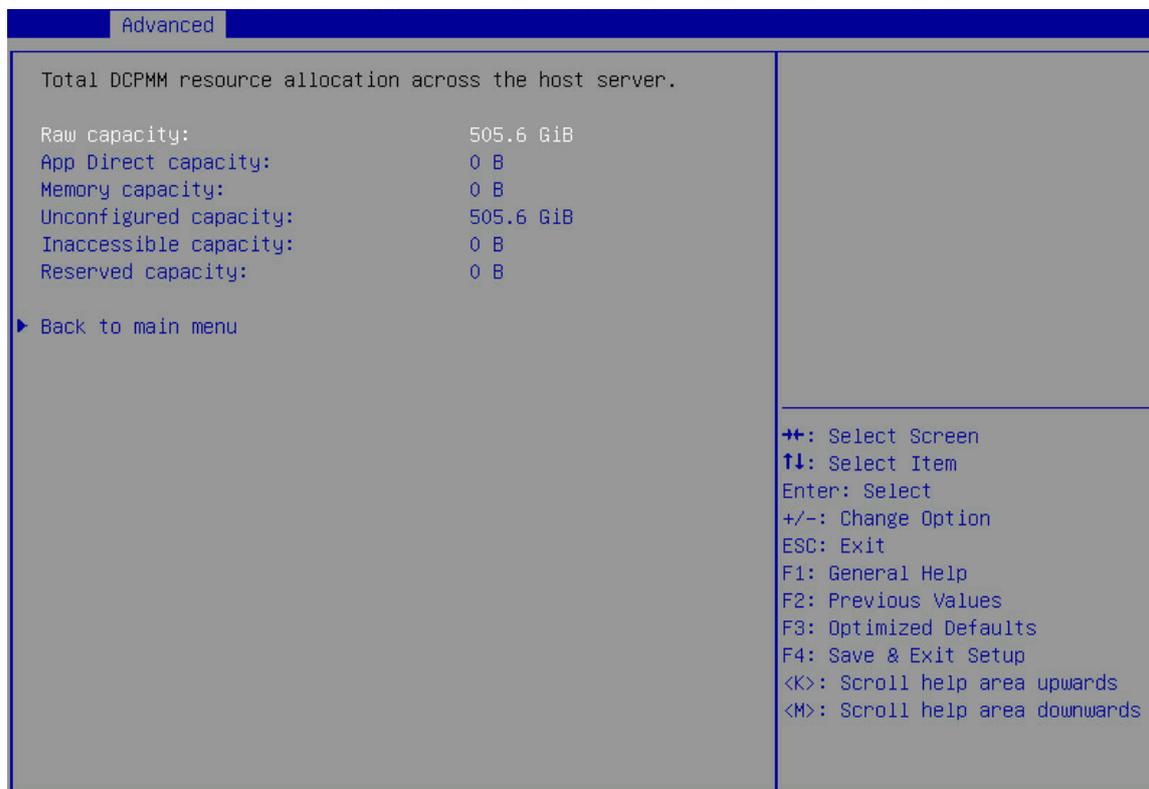


表3-56 Total capacity 界面参数

界面参数	功能说明
Raw capacity	Intel 内存总容量。
App Direct capacity	用于App Direct模式的总容量。
Memory capacity	用于内存模式的总容量。
Unconfigured capacity	不可配置的容量大小，这部分内存未映射到系统物理地址空间中。
Inaccessible capacity	由于许可问题而无法访问的Intel DIMM总容量。
Reserved capacity	预留的内存容量大小。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

## 5. Diagnostics 界面

如图 3-63所示，通过Diagnostics界面可 使用户能够在Intel DCPMM上运行不同诊断测试的组合。具体参数说明如表 3-57所示。

图3-63 Diagnostics 界面

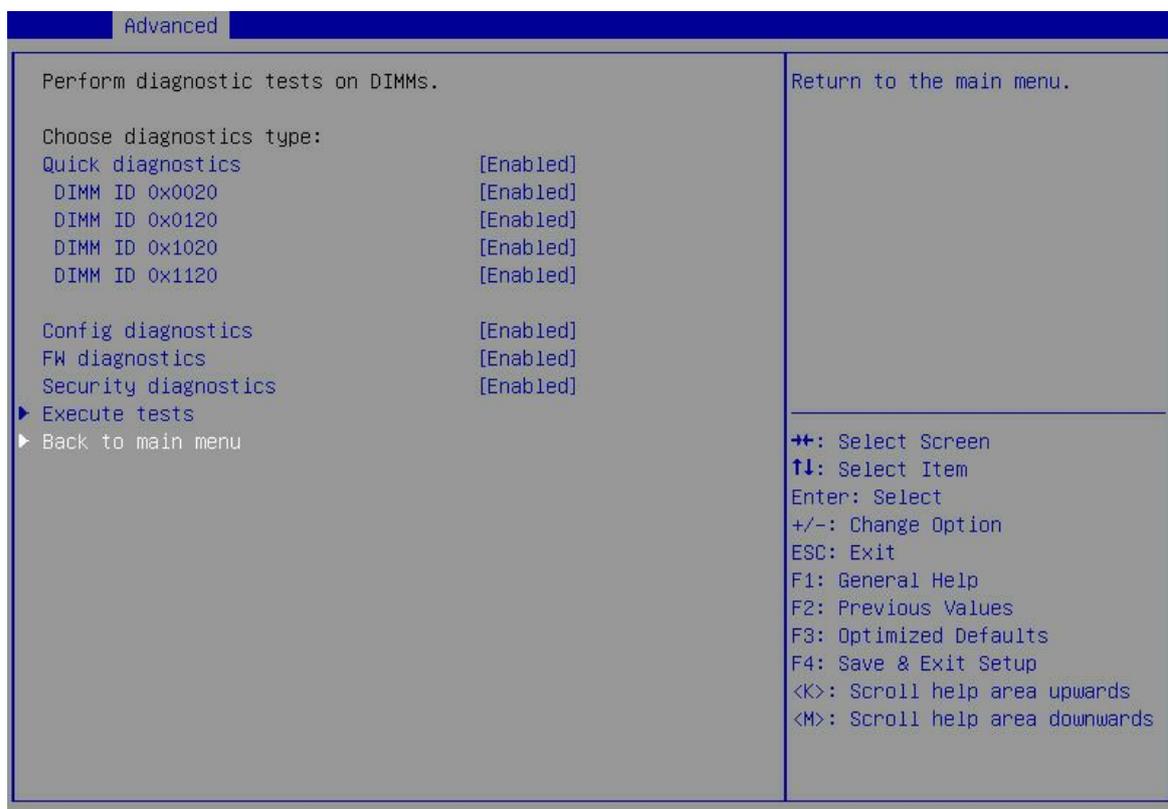


表3-57 Diagnostics 界面参数

界面参数	功能说明
Quick diagnostics	执行快速诊断测试。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 启用。</li> <li>• Disabled: 禁用。</li> </ul>
DIMM ID	选择要诊断的 Intel DCPMM 内存。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 启用对该内存条的诊断。</li> <li>• Disabled: 禁用对该内存条的诊断。</li> </ul>
Config diagnostics	执行平台配置诊断测试。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 启用。</li> <li>• Disabled: 禁用。</li> </ul>
FW diagnostics	执行固件诊断测试。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 启用。</li> <li>• Disabled: 禁用。</li> </ul>
Security diagnostics	执行安全性诊断测试。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 启用。</li> <li>• Disabled: 禁用。</li> </ul>

界面参数	功能说明
Execute tests	执行诊断。如果未选择诊断任何一根内存或快速诊断开启时，该选项置灰。未选择进行任何一项测试时，该选项也置灰。
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

## 6. Preferences 界面

如[图 3-64](#)所示，通过Preferences界面可 查看并改用户首选项。。具体参数说明如[表 3-58](#)所示。

图3-64 Preferences 界面

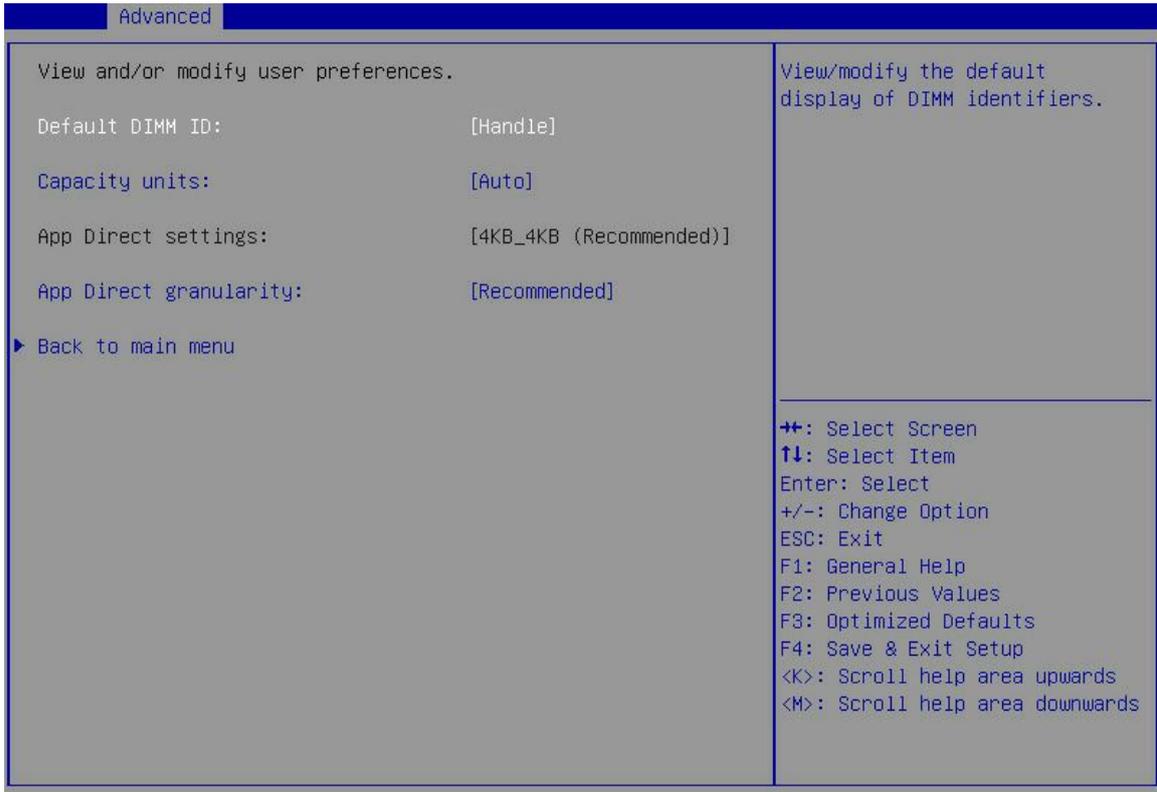


表3-58 Preferences 界面参数

界面参数	功能说明
Default DIMM ID	设置DIMM标识符的默认显示。菜单选项为： <ul style="list-style-type: none"> <li>• Handle（缺省）：根据 SMBIOS Type17 设置。</li> <li>• UID：使用<a href="#">表 3-43</a>中DIMM UID的值作为DIMM标识符。</li> </ul>

界面参数	功能说明
Capacity units	内存容量的单位。菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省)</li> <li>• Auto_10</li> <li>• B</li> <li>• MB</li> <li>• MiB</li> <li>• GB</li> <li>• GiB</li> <li>• TB</li> <li>• TiB</li> </ul>
App Direct settings	创建App Direct容量时要使用的交织设置选项，默认设置是使用BIOS推荐的交织设置。 选项值的格式如下： <ul style="list-style-type: none"> <li>• (IMC大小) _ (通道大小) [ (推荐) ]</li> </ul> 如果系统上已存在App Direct容量，则显示为灰色。
App Direct granularity	设置每个DIMM的最小App Direct粒度。菜单选项为： <ul style="list-style-type: none"> <li>• Recommended (缺省)：使用推荐的App Direct粒度为 32 GiB。</li> <li>• 1：允许 1 GiB App Direct粒度。</li> </ul>
Back to main menu	返回Intel DCPMM内存配置主界面菜单。

### 3.2.15 Driver Health 界面

如[图 3-65](#)所示，通过Driver Health界面可以查看驱动/控制器的健康状态。当驱动/控制器的状态为Failed状态时，可根据界面提示进行修复。具体参数说明如[表 3-59](#)所示。

图3-65 Driver Health 界面

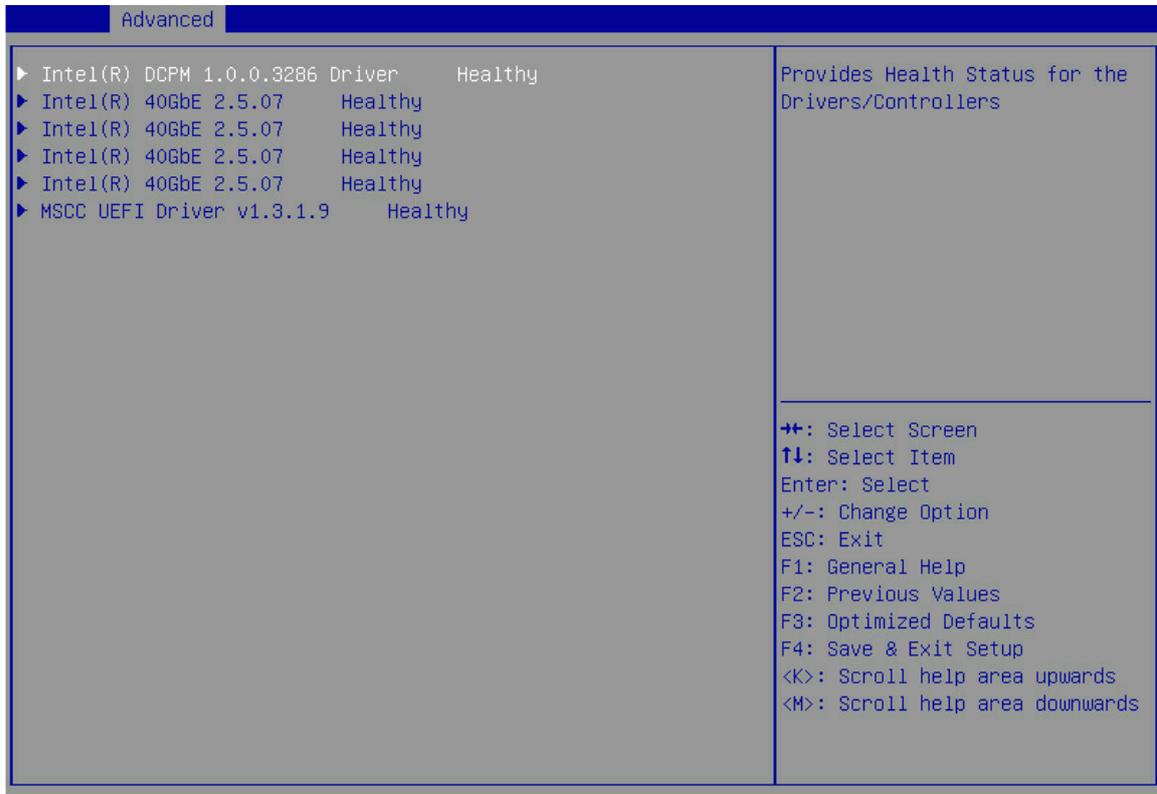


表3-59 Driver Health 界面参数

界面参数	功能说明
Intel® DCPM 1.0.0.3286 Driver (该界面体现服务器实际安装的驱动/控制器的状态)	该驱动/控制器的健康状态。菜单选项为： <ul style="list-style-type: none"> <li>• <b>Healthy:</b> 正常。</li> <li>• <b>Failed:</b> 异常，需要修复。按 <b>Enter</b>，并按照界面提示可修复驱动/控制器。</li> </ul> 不同的驱动/控制器的修复方法有差异，请根据界面提示修复Failed状态的驱动/控制器。

### 3.3 Platform Configuration界面

Platform Configuration界面如图 3-66所示，主要包含PCH配置、其他配置菜单、服务器ME配置菜单、运行错误记录菜单等。具体参数说明如表 3-60所示。

图3-66 Platform Configuration 界面

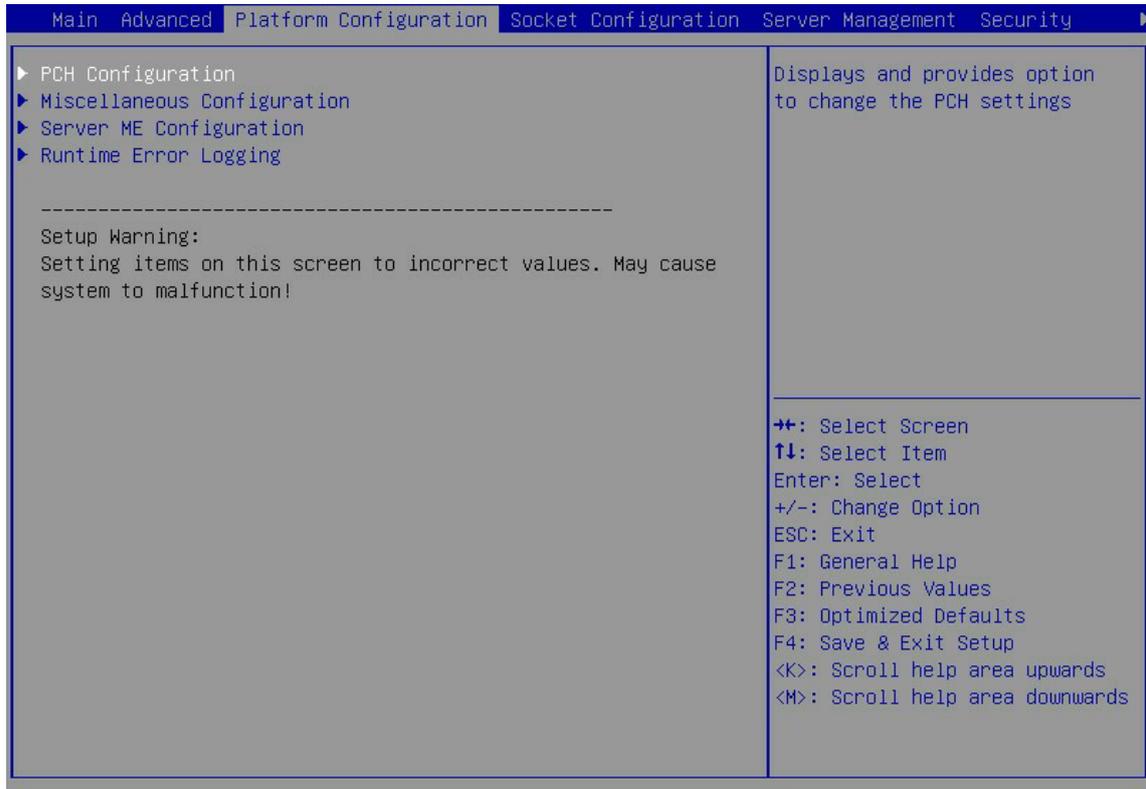


表3-60 Platform Configuration 界面参数

界面参数	功能说明
PCH Configuration	PCH配置菜单。
Miscellaneous Configuration	其他配置菜单。
Server ME Configuration	服务器ME配置菜单。
Runtime Error Logging	运行时错误记录菜单。

### 3.3.1 PCH Configuration 界面

如图3-67所示，通过PCH Configuration界面，可以对PCH进行配置，包括硬盘接口、USB等。具体参数说明如表3-61所示。

图3-67 PCH Configuration 界面



表3-61 PCH Configuration 界面参数

界面参数	功能说明
PCH SATA Configuration	PCH SATA配置菜单。如要配置软RAID，需要在此界面选择将SATA模式配置为RAID模式。 说明：
PCH sSATA Configuration	PCH sSATA配置菜单。如要配置软RAID，需要在此界面选择将sSATA模式配置为RAID模式。 说明：
USB Configuration	USB配置菜单。

 说明

如果同时使用了SATA接口和sSATA接口，需要分别对SATA控制器和sSATA控制器进行配置。配置参数的详细信息请参见[表 3-62](#)和[表 3-63](#)。

### 1. PCH SATA Configuration 界面

PCH SATA Configuration界面如[图 3-68](#)所示。具体参数说明如[表 3-62](#)所示。

UNISINSIGHT AIX R6220L-G3 服务器PCH SATA Configuration界面如[图 3-69](#)所示，显示SATA端口对应的硬盘槽位号。当硬盘背板的型号不同，显示有差异，以实际界面显示为准。

图3-68 PCH SATA Configuration 界面

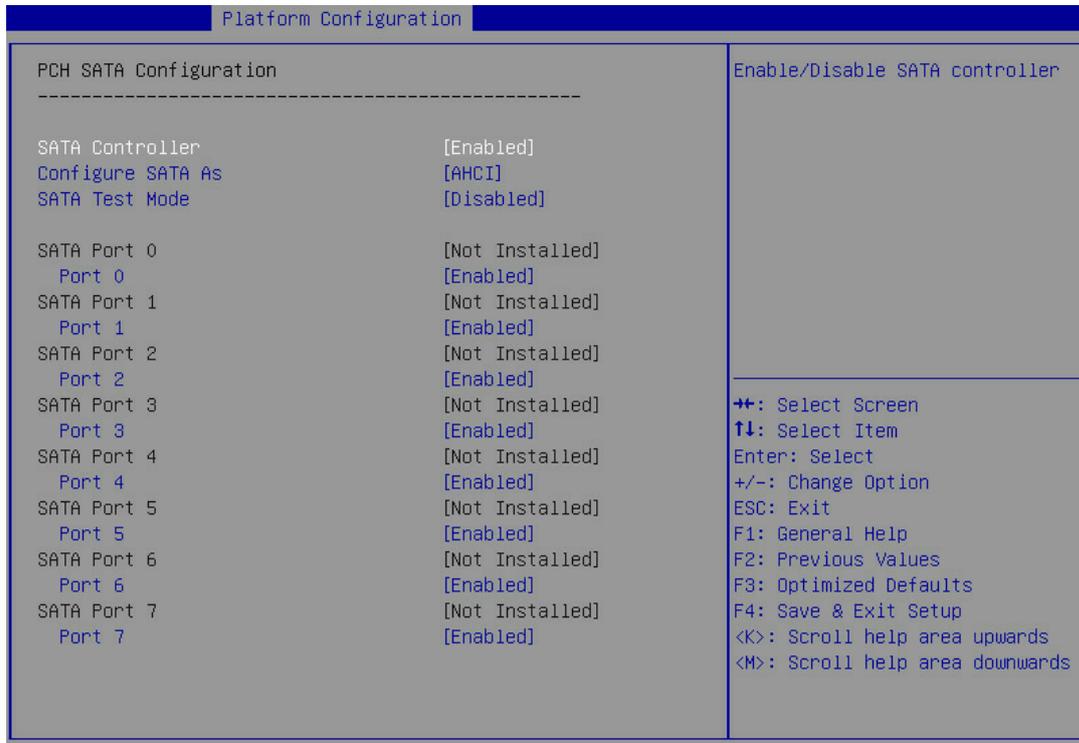


图3-69 PCH SATA Configuration 界面 (UNISINSIGHT AIX R6220L-G3 服务器)

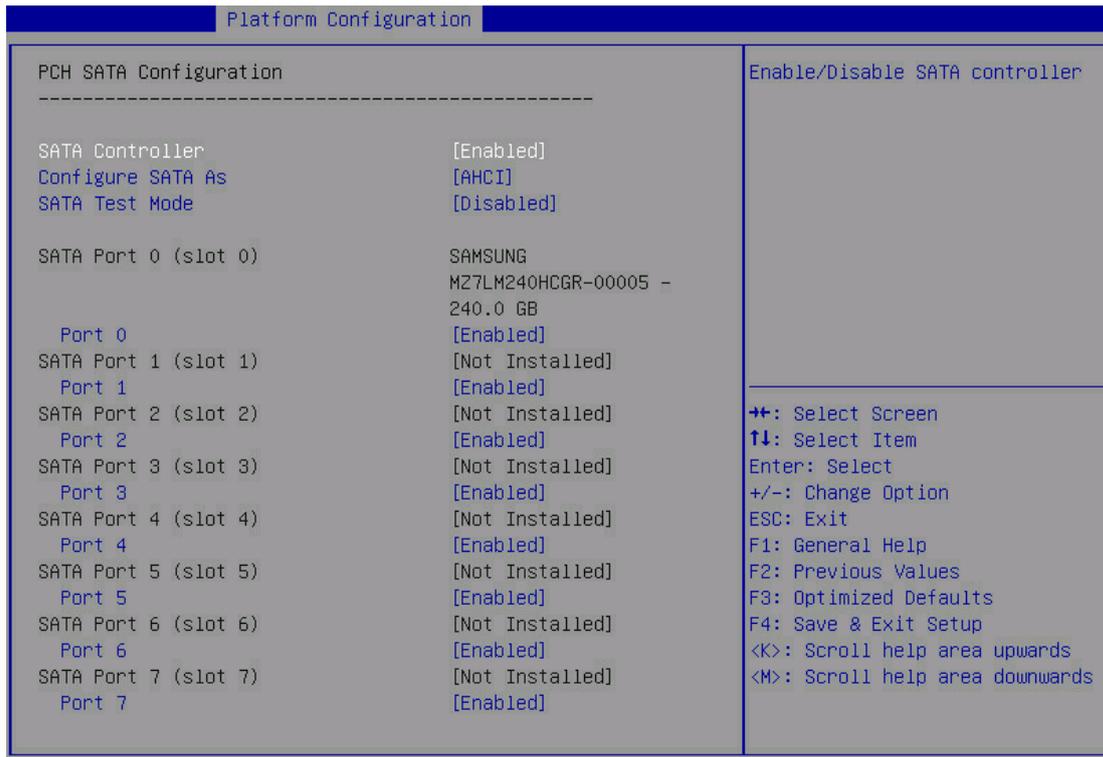


表3-62 PCH SATA Configuration 界面参数

界面参数	功能说明
SATA Controller	<p>SATA控制器开关。开启后可以对SATA模式和SATA Test模式进行配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 SATA 控制器。开启后可以对 SATA 模式和 SATA Test 模式进行配置。</li> <li>Disabled: 关闭 SATA 控制器。</li> </ul>
Configure SATA as	<p>配置SATA模式，菜单选项为：</p> <ul style="list-style-type: none"> <li>AHCI（缺省）：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。</li> <li>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。需要配置软 RAID 时需配置为该选项。</li> </ul>
SATA Test Mode	<p>SATA Test模式开关，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启 SATA Test 模式。</li> <li>Disabled（缺省）：关闭 SATA Test 模式。</li> </ul>
SATA Port x	<p>显示接入SATA端口的设备名称，根据硬盘在位情况动态获取。设备不在位时显示Not Installed。</p> <p>UNISINSIGHT AIX R6220L-G3服务器该选项括号内的slot编号表示该SATA端口对应的硬盘槽位号。</p>
Port x	<p>SATA端口开关，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 SATA 端口。</li> <li>Disabled: 关闭 SATA 端口。</li> </ul>

## 2. PCH sSATA Configuration 界面

PCH sSATA Configuration界面如[图 3-70](#)所示。具体参数说明如[表 3-63](#)所示。

UNISINSIGHT AIX R6220L-G3 服务器PCH sSATA Configuration界面如[图 3-71](#)所示，显示sSATA端口对应的硬盘槽位号。当硬盘背板的型号不同，显示有差异，以实际界面显示为准。

图3-70 PCH sSATA Configuration 界面

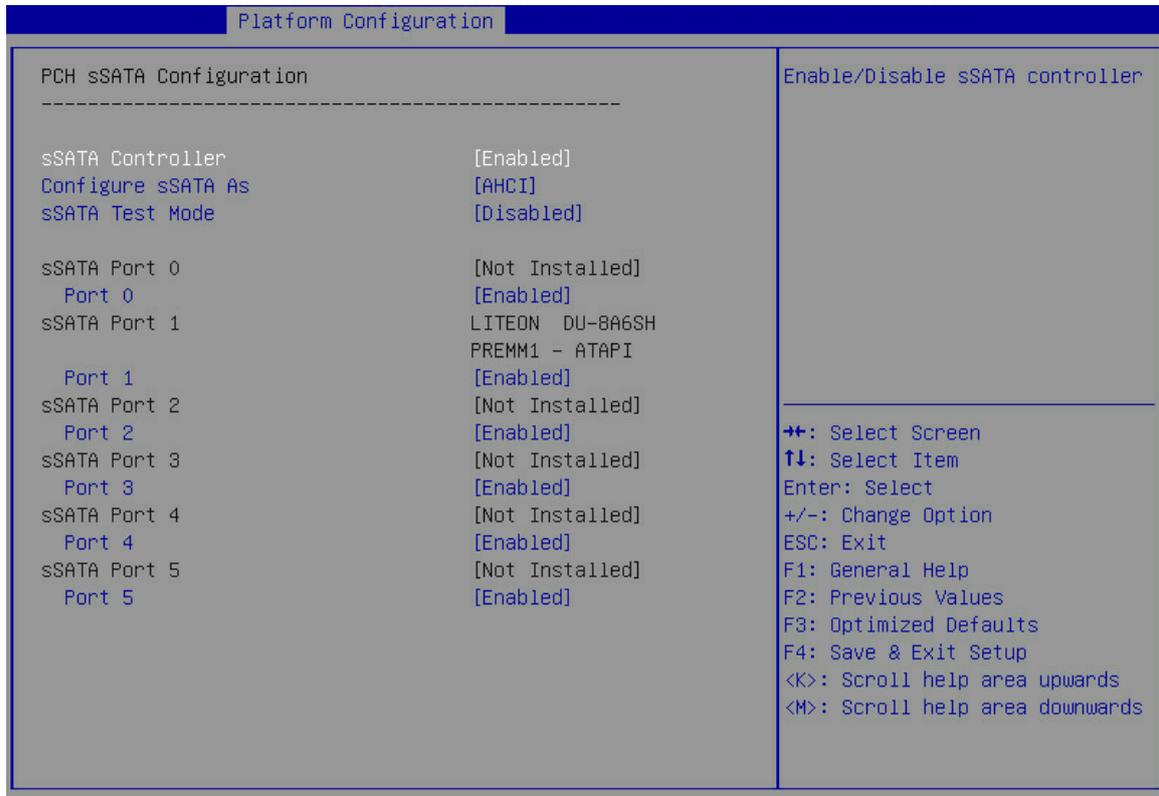


图3-71 PCH sSATA Configuration 界面 (UNISINSIGHT AIX R6220L-G3 服务器)

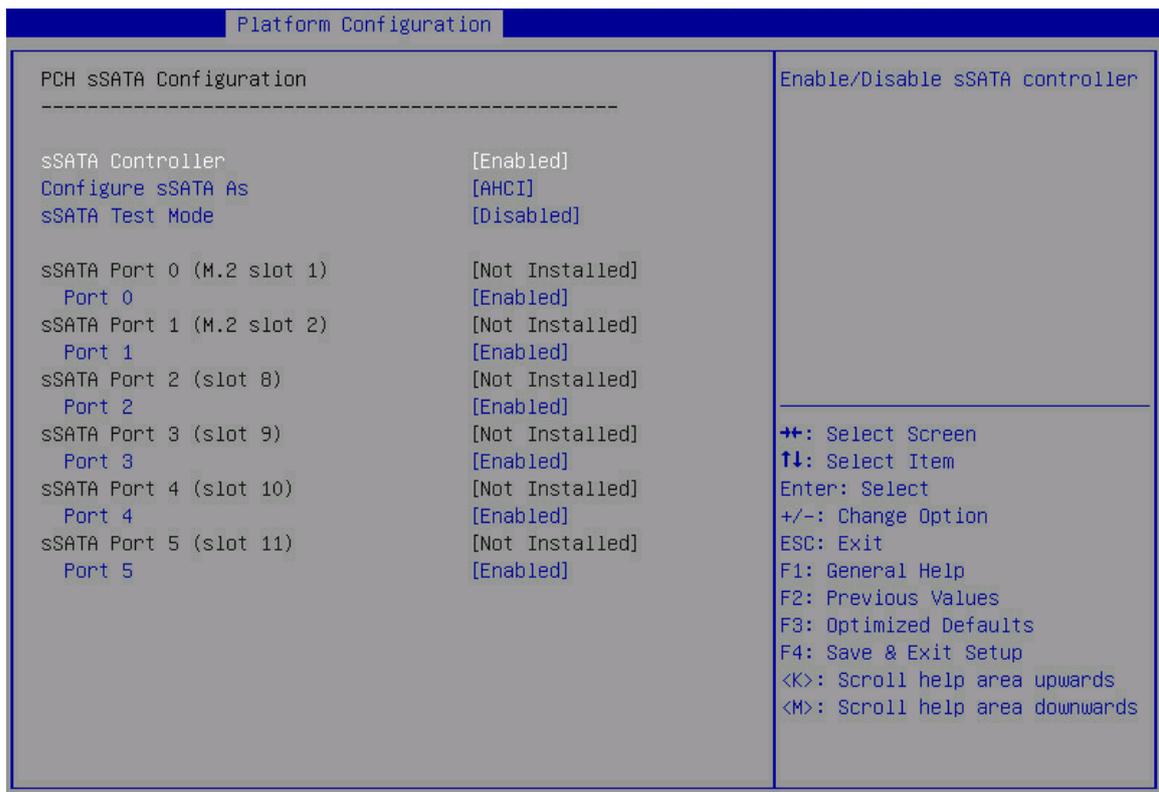


表3-63 PCH sSATA Configuration 界面参数

界面参数	功能说明
sSATA Controller	sSATA控制器开关，菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：开启 sSATA 控制器功能，开启后可以对 sSATA 模式和 sSATA Test 模式进行配置。</li> <li>Disabled: 关闭 sSATA 控制器功能。</li> </ul>
Configure sSATA as	硬盘控制器工作模式配置。菜单选项为： <ul style="list-style-type: none"> <li>AHCI (缺省)：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。</li> <li>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。</li> </ul>
sSATA Test Mode	sSATA Test模式开关，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启 sSATA Test 模式。</li> <li>Disabled (缺省)：关闭 sSATA Test 模式。</li> </ul>
sSATA Port x	显示接入sSATA端口的设备名称，根据硬盘在位情况动态获取。设备不在位时显示Not Installed。 UNISINSIGHT AIX R6220L-G3服务器该选项括号内的slot编号表示该sSATA端口对应的硬盘槽位号。
Port x	sSATA端口开关，菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：开启 sSATA 端口。</li> <li>Disabled: 关闭 sSATA 端口。</li> </ul>

 说明

不同服务器PCH sSATA Configuration界面端口配置选项和USB Configuration界面USB端口配置选项有差异，具体如下[表 3-64](#)所示：

表3-64 服务器对应 sSATA 输出端口、USB 端口选项

产品名称	sSATA 端口	USB 端口
UNISINSIGHT AIX R6220L-G3	port 0~5	USB 2.0: 后部底端、后部顶端、内部顶端、内部底端、前部右挂耳、前部左挂耳底端、前部左挂耳顶端。 USB3.0: 前部右挂耳、后部顶部、后部底部、内部顶端、内部底端。

### 3. USB Configuration 界面

USB Configuration界面如[图 3-72](#)所示，具体参数如[表 3-65](#)所示。

图3-72 USB Configuration 界面

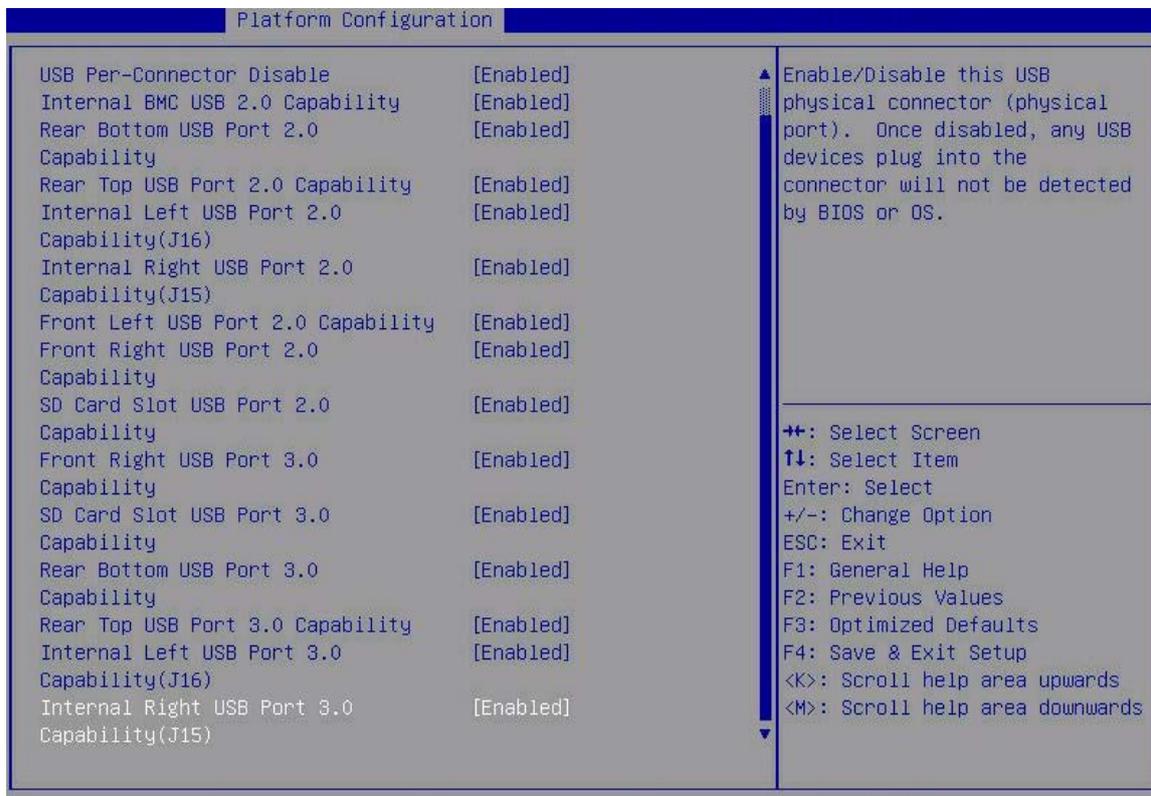


表3-65 USB Configuration 界面参数

界面参数	功能说明
USB Per-Connector Disable	<p>USB端口中单端口禁用控制配置，当其中的USB物理连接器被禁用，任何USB设备插入此连接器将不会被BIOS或操作系统检测到，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启 USB 端口中单端口禁用控制功能，可以对主板上的每个 USB 端口进行单独控制。</li> <li>Disabled (缺省)：关闭 USB 端口中单端口禁用控制功能。</li> </ul>
Internal BMC USB Port 2.0 Capability	<p>内部BMC USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled (缺省)：开启内部 BMC USB 2.0 功能。</li> <li>Disabled: 关闭内部 BMC USB 2.0 功能。</li> </ul>
Rear Bottom USB Port 2.0 Capability	<p>后部底端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled (缺省)：开启后部底端 USB 2.0 功能。</li> <li>Disabled: 关闭后部底端 USB 2.0 功能。</li> </ul>
Rear Top USB Port 2.0 Capability	<p>后部顶端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled (缺省)：开启后部顶端 USB 2.0 功能。</li> <li>Disabled: 关闭后部顶端 USB 2.0 功能。</li> </ul>

界面参数	功能说明
Internal Left USB Port 2.0 Capability(J16)	内部左端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启内部左端 USB 2.0 功能。</li> <li>• Disabled: 关闭内部左端 USB 2.0 功能。</li> </ul>
Internal Right USB Port 2.0 Capability(J15)	内部右挂耳USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启内部右端 USB 2.0 功能。</li> <li>• Disabled: 关闭内部右端 USB 2.0 功能。</li> </ul>
Front Left USB Port 2.0 Capability	前部左挂耳顶端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启前部左挂耳顶端 USB 2.0 功能。</li> <li>• Disabled: 关闭前部左挂耳顶端 USB 2.0 功能。</li> </ul>
Front Right USB Port 2.0 Capability	前部右挂耳USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启前部右挂耳 USB 2.0 功能。</li> <li>• Disabled: 关闭前部右挂耳 USB 2.0 功能。</li> </ul>
SD Card Slot USB Port 2.0 Capability	SD卡槽USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 SD 卡槽 USB 2.0 功能。</li> <li>• Disabled: 关闭 SD 卡槽 USB 2.0 功能。</li> </ul>
Front Right USB Port 3.0 Capability	前部右端USB 3.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启前部右端 USB 3.0 功能。</li> <li>• Disabled: 关闭前部右端 USB 3.0 功能。</li> </ul>
SD Card Slot USB Port 3.0 Capability	SD卡槽USB 3.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 SD 卡槽 USB 3.0 功能。</li> <li>• Disabled: 关闭 SD 卡槽 USB 3.0 功能。</li> </ul>
Rear Bottom USB Port 3.0 Capability	后部底端USB 3.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启后部底端 USB 3.0 功能。</li> <li>• Disabled: 关闭后部底端 USB 3.0 功能。</li> </ul>
Rear Top USB Port 3.0 Capability	后部顶端USB 3.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启后部顶端 USB 3.0 功能。</li> <li>• Disabled: 关闭后部顶端 USB 3.0 功能。</li> </ul>
Internal Left USB Port 3.0 Capability (J16)	内部左端USB 3.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启内部左端 USB 3.0 功能。</li> <li>• Disabled: 关闭内部左端 USB 3.0 功能。</li> </ul>

界面参数	功能说明
Internal Right USB Port 3.0 Capability (J15)	内部右端USB 3.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启内部右端 USB 3.0 功能。</li> <li>• Disabled: 关闭内部右端 USB 3.0 功能。</li> </ul>

### 3.3.2 Miscellaneous Configuration 界面

如[图 3-73](#)所示，通过Miscellaneous Configuration界面，可以对一些混杂的配置项进行配置，包括显示设备选择、Debug模式开关等。具体参数说明如[表 3-66](#)所示。

图3-73 Miscellaneous Configuration 界面

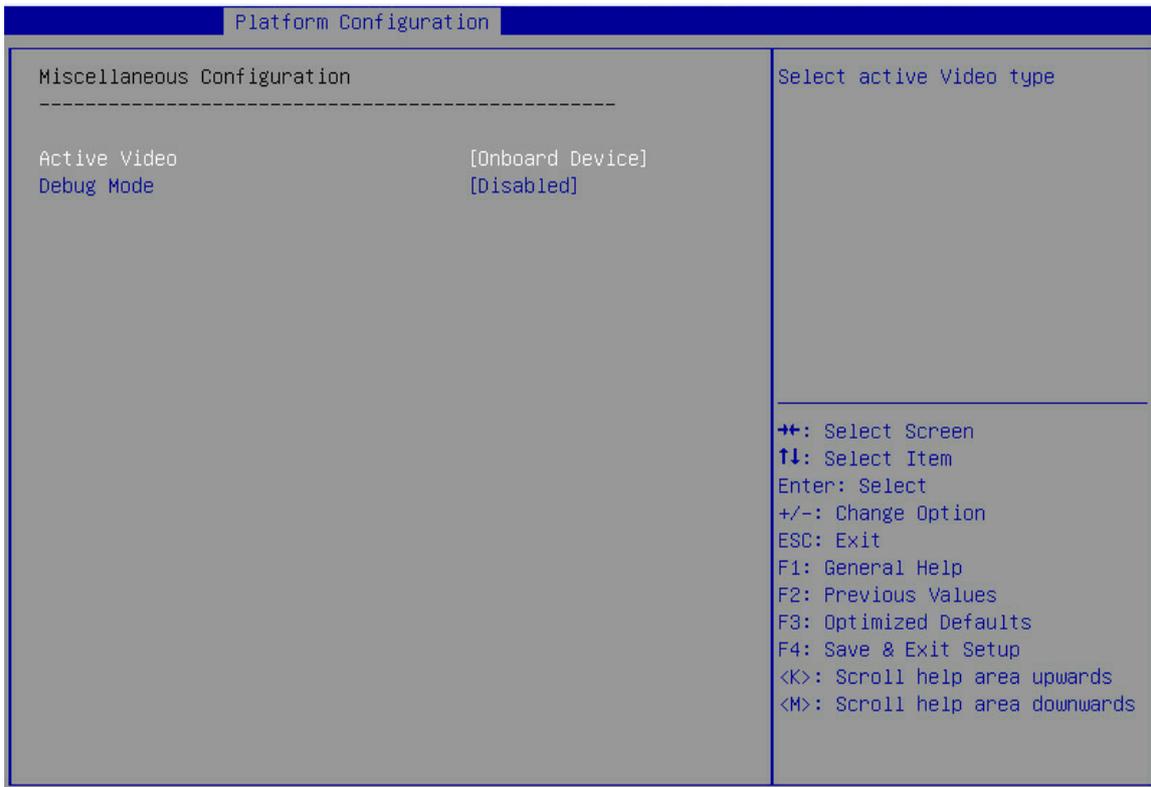


表3-66 Miscellaneous Configuration 界面参数

界面参数	功能说明
Active Video	<p>显示设备选择，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Auto</b>：根据设备自动设置界面显示方式。</li> <li>• <b>Onboard Device</b>（缺省）：服务器通过板载 VGA 接口进行界面显示。</li> </ul> <p>开启该功能后，如果安装了 GPU 卡，在 Legacy 启动模式下，GPU 卡连接的显示设备仅支持显示操作系统界面，无法显示 BIOS 界面。其余情况下，板载 VGA 接口和 GPU 卡连接的显示设备，均能正常显示 BIOS 和操作系统界面。</p> <ul style="list-style-type: none"> <li>• <b>PCIe Device</b>：服务器通过 PCIe 设备 GPU 卡进行界面显示。</li> </ul> <p>安装 GPU 卡并开启该功能后，在 Legacy 启动模式下，板载 VGA 接口连接的显示设备仅支持显示操作系统界面，无法显示 BIOS 界面。其余情况下，板载 VGA 接口和 GPU 卡连接的显示设备，均能正常显示 BIOS 和操作系统界面。</p>
Debug Mode	<p>BIOS 串口日志输出开关，开启该功能后，服务器能输出 BIOS 串口日志，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>：开启 BIOS 串口日志输出功能。选择该选项后，您可以通过连接串口，获取 BIOS 串口日志。</li> <li>• <b>Disabled</b>（缺省）：关闭 BIOS 串口日志输出功能。</li> </ul>

### 3.3.3 Server ME Configuration 界面

如[图 3-74](#)和[图 3-75](#)所示，通过 Server ME Configuration 界面，可以查看固件信息。具体参数说明如[表 3-67](#)所示。

图3-74 Server ME Configuration 界面 1

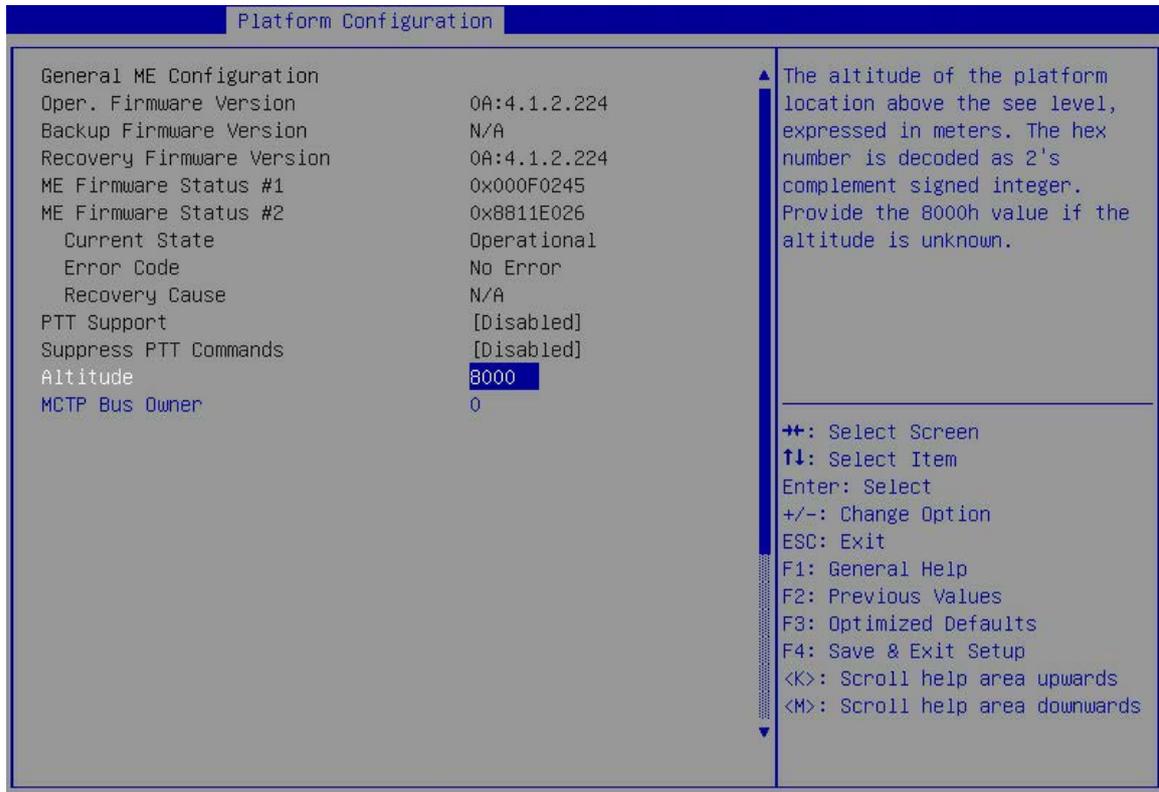


图3-75 Server ME Configuration 界面 2

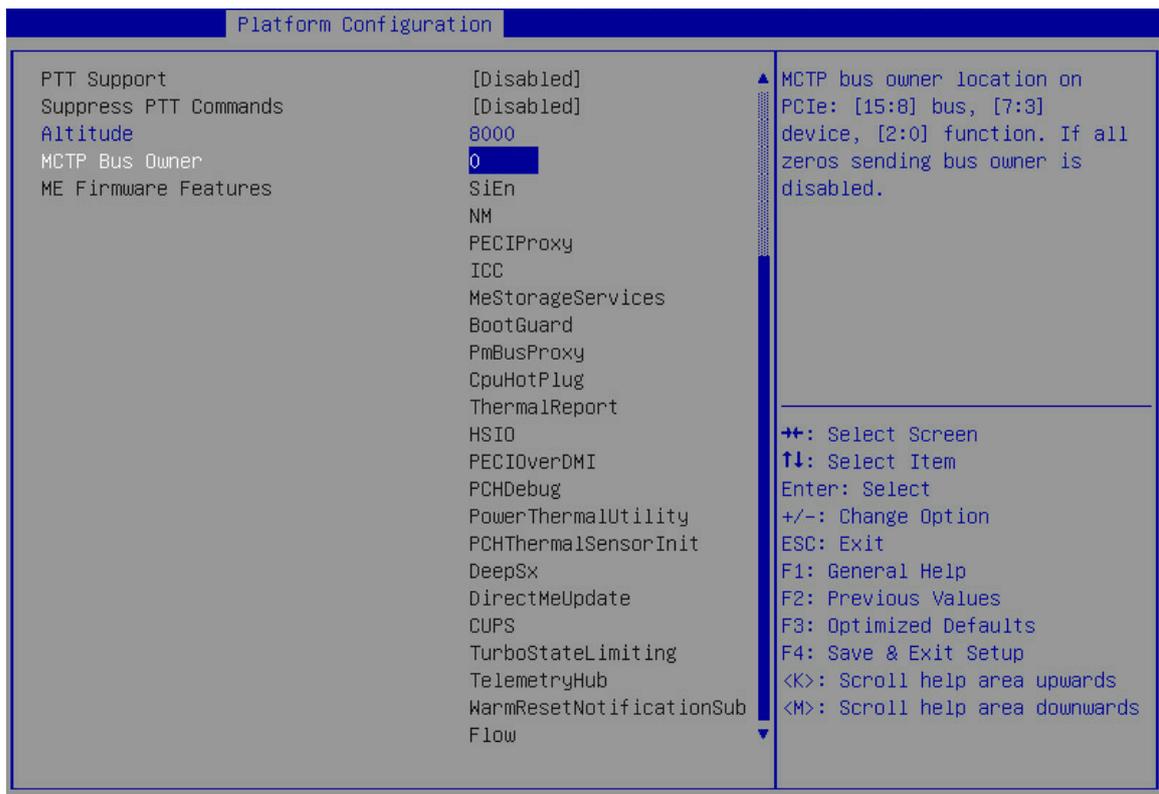


表3-67 Server ME Configuration 界面参数

界面参数	功能说明
<b>General ME Configuration</b>	
Oper. Firmware Version	显示有效固件版本。
Backup Firmware Version	显示备份固件版本。
Recovery Firmware Version	显示恢复固件版本。
ME Firmware Status #1	显示ME固件状态值#1。
ME Firmware Status #2	显示ME固件状态值#2。
Current State	显示ME当前状态。
Error Code	显示ME固件错误码信息。
Recovery Cause	显示恢复原因。
PTT Support	显示平台可新技术（PTT）支持。
Suppress PTT Commands	显示隐藏PTT命令。
Altitude	平台位置的高度，缺省值为8000，单位为米，是一个十六进制数。
MCTP Bus Owner	MCTP可以用来监测CPU，改变或者交换总线用户。 该选项用于设置MCTP总线所有者位于PCIe总线的位置，[15:8]bit表示Bus号，[7:3]bit表示Device号，[2:0]bit表示Function号。缺省值为0，表示MCTP总线所有者将被禁用。
ME Firmware Features	显示ME固件的特征信息。

### 3.3.4 Runtime Error Logging 界面

如[图 3-76](#)所示，通过Runtime Error Logging界面，可以查看运行错误日志。具体参数说明如[表 3-68](#)所示。

图3-76 Runtime Error Logging 界面

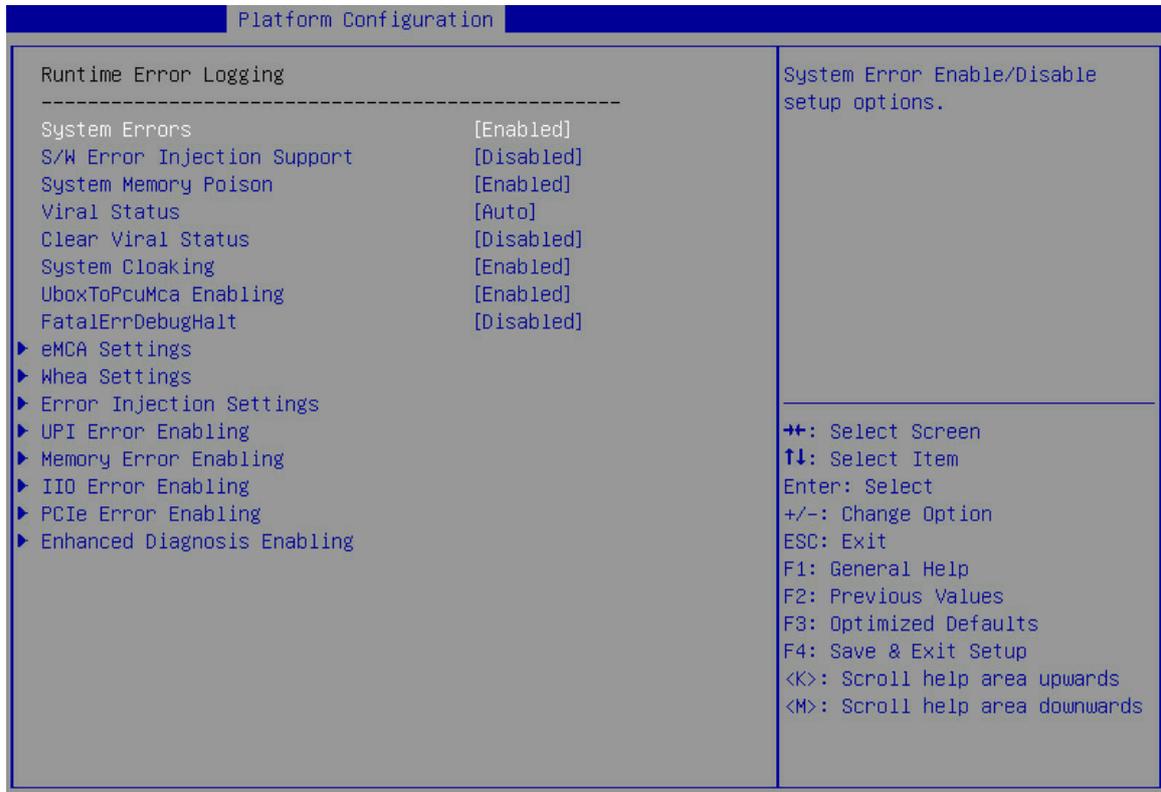


表3-68 Runtime Error Logging 界面参数

界面参数	功能说明
System Errors	<p>系统错误记录开关，开启该功能后，会进行错误纠正，不可纠正错误会上报给HDM和OS，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启系统错误记录功能。</li> <li>Disabled：关闭系统错误记录功能。</li> </ul>
SW Error Injection Support	<p>软件错误注入支持开关，当System Errors设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled：开启软件错误注入支持功能，通过软件注入错误来检验系统的性能。</li> <li>Disabled（缺省）：关闭软件错误注入支持功能。</li> </ul>
System Memory Poison	<p>系统内存Poison开关，当System Errors设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启系统内存 Poison 功能。</li> <li>Disabled：关闭系统内存 Poison 功能。</li> </ul> <p>当注入不可纠正的内存错误时，需要将System Memory Poison和Viral Status同时设置为Disabled，事件日志才能上报HDM。</p>

界面参数	功能说明
Viral Status	<p>病毒状态配置，当System Errors设置为Enabled时，该选项可用。当服务器的CPU不支持Advanced RAS功能时，该选项置灰。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto（缺省）：根据当前CPU和内存情况，自动决定是否启用内存病毒。</li> <li>• Enabled：启用内存病毒。</li> <li>• Disabled：禁用内存病毒。</li> </ul> <p>当注入不可纠正的内存错误时，需要将System Memory Poison和Viral Status同时设置为Disabled，事件日志才能上报HDM。</p>
Clear Viral Status	<p>清除病毒状态配置，当Viral Status设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：启用清除病毒状态。</li> <li>• Disabled（缺省）：禁用清除病毒状态。</li> </ul>
System Cloaking	<p>系统Cloaking功能配置，当System Errors设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用系统Cloaking功能，当启用时，修正的和UCNA错误将被OS/SW屏蔽。</li> <li>• Disabled：禁用系统Cloaking功能。</li> </ul>
UboxToPcuMca Enabling	<p>Ubox本地错误传递给MCA使能开关，当System Errors设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启将Ubox本地错误传递给MCA。</li> <li>• Disabled：关闭将Ubox本地错误传递给MCA。</li> </ul>
FatalErrDebugHalt	<p>致命错误暂停调试，当System Errors设置为Enabled时显示。仅为McBank致命错误情况的调试。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：启用致命错误暂停调试。只有在连接了ITP作为线程将暂停在致命错误流时，启选择此选项。</li> <li>• Disabled（缺省）：关闭致命错误暂停调试。</li> </ul>
eMCA Settings	eMCA设置菜单，当System Errors设置为Enabled时，该选项可用。
Whea Settings	Whea设置菜单，当System Errors设置为Enabled时，该选项可用。
Error Injection Settings	错误注入设置菜单，当System Errors设置为Enabled时，该选项可用。
UPI Error Enabling	UPI错误启用菜单，当System Errors设置为Enabled时，该选项可用。
Memory Error Enabling	内存错误启用菜单，当System Errors设置为Enabled时，该选项可用。
IIO Error Enabling	IIO错误启用菜单，当System Errors设置为Enabled时，该选项可用。
PCle Error Enabling	PCIE错误启用菜单，当System Errors设置为Enabled时，该选项可用。
Enhanced Diagnosis Enabling	增强诊断功能启用菜单，当System Errors设置为Enabled时，该选项可用。

## 1. eMCA Settings 界面

eMCA Settings界面如[图 3-77](#)所示。具体参数说明如[表 3-69](#)所示。

图3-77 eMCA Settings 界面

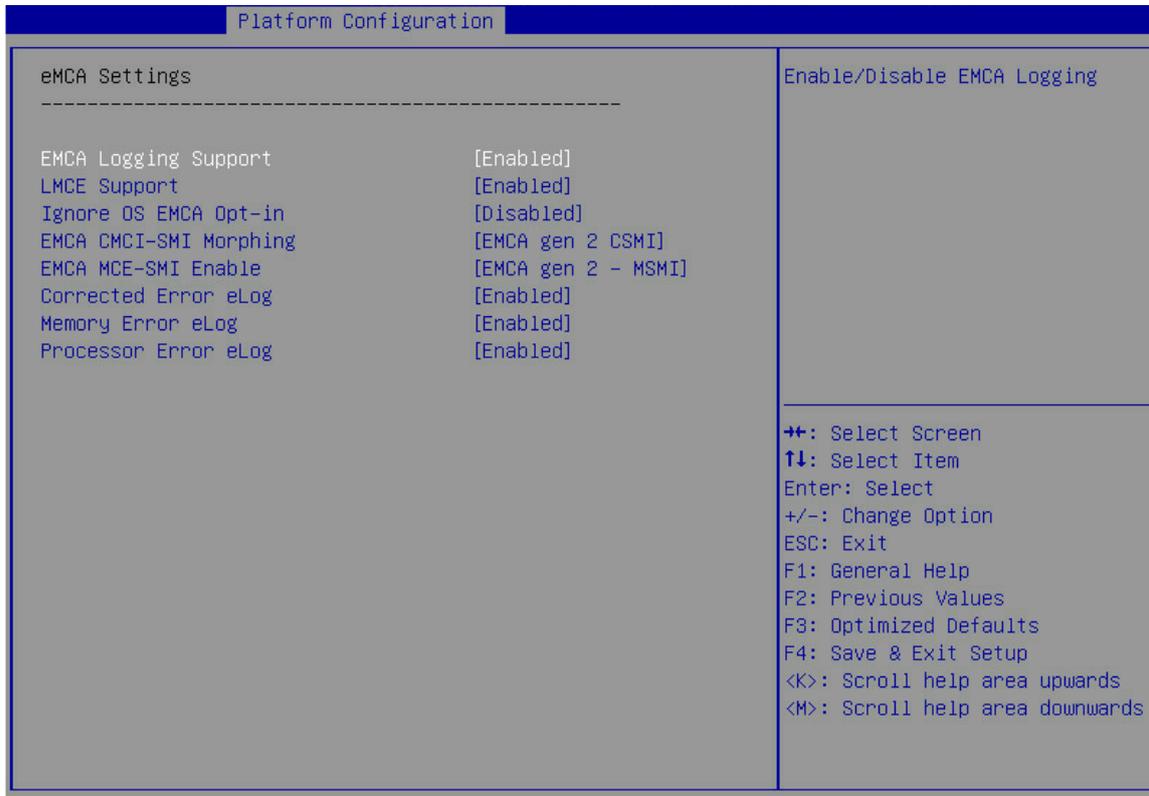


表3-69 eMCA Settings 界面参数

界面参数	功能说明
EMCA Logging Support	<p>eMCA (Enhanced Machine Check Architecture) 记录日志开关, 该功能可以为服务器提供MCA错误报告, 菜单选项为:</p> <ul style="list-style-type: none"> <li>Enabled (缺省): 开启 EMCA 功能。</li> <li>Disabled: 关闭 EMCA 功能。</li> </ul>
LMCE Support	<p>本地的MCE支持设置, 该功能可以为服务器提供硬件错误检测机制中的固件支持能力, 可以相应的错误信息记录到固件中特殊的寄存器, 菜单选项为:</p> <ul style="list-style-type: none"> <li>Enabled (缺省): 启用本地 MCE 固件支持。</li> <li>Disabled: 禁用本地 MCE 固件支持。</li> </ul>
Ignore OS EMCA Opt-in	<p>忽略OS EMCA选入功能, 当EMCA Logging Support设置为Enabled时显示, 菜单选项为:</p> <ul style="list-style-type: none"> <li>Enabled: 开启忽略 OS EMCA 选入功能。</li> <li>Disabled (缺省): 关闭忽略 OS EMCA 选入功能。</li> </ul>

界面参数	功能说明
EMCA CMCI-SMI Morphing	<p>EMCA CMCI-SMI Morphing选项，当EMCA Logging Support设置为Enabled时显示。开启EMCA CMCI-SMI Morphing后，可纠正错误每发生一次，均可触发SMI。McBank上可纠正错误超过阈值，也会触发SMI，不触发CMCI。菜单选项为：</p> <ul style="list-style-type: none"> <li>• EMCA gen 1 Lite: 配置 EMCA CMCI-SMI Morphing 为 EMCA gen 1 Lite 模式。</li> <li>• EMCA gen 2 CSMI(缺省): 配置 EMCA CMCI-SMI Morphing 为 EMCA gen 2 CSMI 模式。</li> <li>• Disabled: 关闭 EMCA CMCI-SMI Morphing。</li> </ul>
EMCA MCE-SMI Enable	<p>EMCA MCE-SMI启用设置，当EMCA Logging Support设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• EMCA gen 1 Dual Mode: 启用 EMCA gen 1 双模式的 EMCA MCE-SMI 功能</li> <li>• EMCA gen 2 – MSMI(缺省): 启用 EMCA gen 2 MSMI 模式的 EMCA MCE-SMI 功能</li> <li>• Disabled: 禁用 EMCA MCE-SMI 功能。</li> </ul>
Corrected Error eLog	<p>可纠正错误日志功能，当EMCA Logging Support设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）: 开启 eMCA 可纠正错误日志记录。</li> <li>• Disabled: 关闭 eMCA 可纠正错误日志记录。</li> </ul>
Memory Error eLog	<p>内存错误日志功能，当EMCA Logging Support设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）: 开启 eMCA 内存错误日志记录功能。</li> <li>• Disabled: 关闭 eMCA 内存错误日志记录功能。</li> </ul>
Processor Error eLog	<p>处理故障日志功能，当EMCA Logging Support设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）: 开启 eMCA 处理器错误记录功能。</li> <li>• Disabled: 关闭 eMCA 处理器错误记录功能。</li> </ul>

## 2. Whea Settings 界面

Whea Settings界面如[图 3-78](#)所示。具体参数说明如[表 3-70](#)所示。

图3-78 Whea Settings 界面

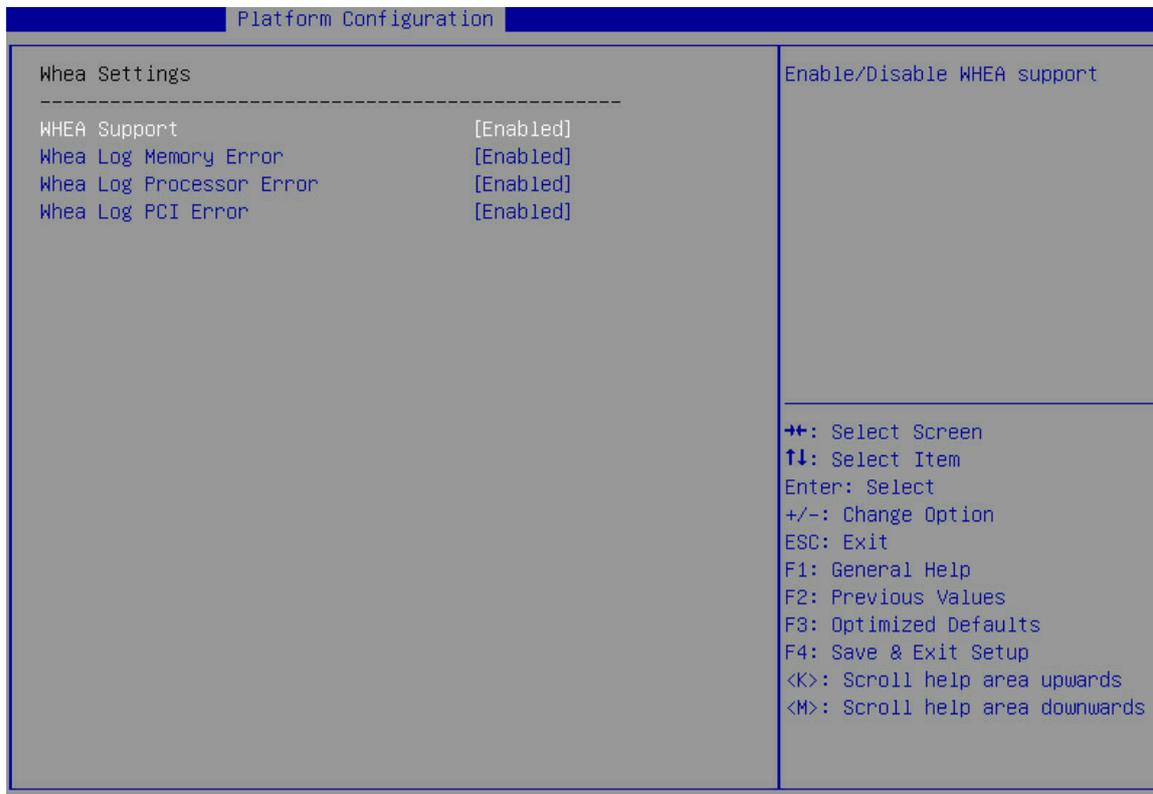


表3-70 Whea Settings 界面参数

界面参数	功能说明
WHEA Support	WHEA支持设置，该功能可以为服务器提供硬件错误报告，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 WHEA 功能。</li> <li>Disabled：关闭 WHEA 功能。</li> </ul>
Whea Log Memory Error	Whea记录内存错误功能，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 Whea 内存错误记录功能。</li> <li>Disabled：关闭 Whea 内存错误记录功能。</li> </ul>
Whea Log Processor Error	Whea记录处理器错误功能，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 Whea 处理器错误记录功能。</li> <li>Disabled：关闭 Whea 处理器错误记录功能。</li> </ul>
Whea Log PCI Error	Whea记录PCI错误功能，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 Whea 记录 PCI 错误功能。</li> <li>Disabled：关闭 Whea 记录 PCI 错误功能。</li> </ul>

### 3. Error Injection Settings 界面

Error Injection Settings界面如[图 3-79](#)所示。具体参数说明如[表 3-71](#)所示。

图3-79 Error Injection Settings 界面

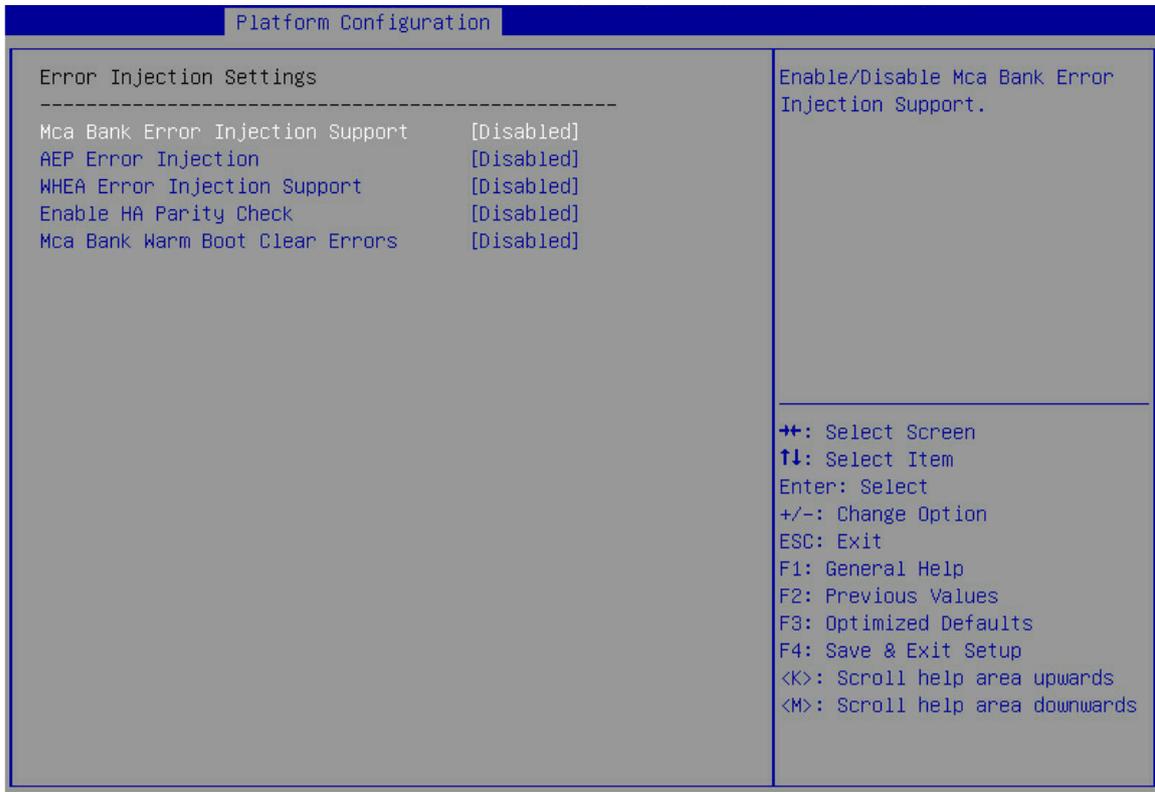


表3-71 Error Injection Settings 界面参数

界面参数	功能说明
Mca Bank Error Injection Support	<p>Mca Bank错误注入功能开关，开启该功能后，故障注入的寄存器写功能会开启，System Errors设置为Enabled时，该选项可用，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启 Mca Bank 错误注入功能。</li> <li>Disabled (缺省)：关闭 McBank 错误注入功能。</li> </ul>
AEP Error Injection	<p>AEP错误注入功能，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启 AEP 错误注入功能。</li> <li>Disabled (缺省)：关闭 AEP 错误注入功能。</li> </ul>
WHEA Error Injection Support	<p>WHEA错误注入功能开关，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启 WHEA 错误注入功能。</li> <li>Disabled (缺省)：关闭 WHEA 错误注入功能。</li> </ul>
WHEA Error Injection 5.0 Support Extension	<p>WHEA错误注入5.0扩展支持功能开关。Whea EINJ ACPI 5.0支持通过地址和供应商设置错误类型。当WHEA Error Injection Support选项设置为Enabled时，显示该选项。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled (缺省)：开启 WHEA 错误注入 5.0 扩展支持功能。</li> <li>Disabled: 关闭 WHEA 错误注入 5.0 扩展支持功能。</li> </ul>

界面参数	功能说明
Whea PCIe Error Injection Support	Whea PCIe错误注入支持功能开关。当WHEA Error Injection Support选项设置为Enabled时，显示该选项。菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启 WHEA PCIe 错误注入功能。</li> <li>Disabled (缺省): 关闭 WHEA PCIe 错误注入功能。</li> </ul>
Whea PCIe Error Injection Action Table	Whea PCIe错误注入行为表开关，当WHEA Error Injection Support选项设置为Enabled时，显示该选项。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省): 开启 WHEA PCIe 错误注入行为表功能。</li> <li>Disabled: 关闭 WHEA PCIe 错误注入行为表功能。</li> </ul>
Enable HA Parity Check	HA 奇偶校验设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启 HA 奇偶校验。</li> <li>Disabled (缺省): 关闭 HA 奇偶校验。</li> </ul>
Mca Bank Warm Boot Clear Errors	热复位时，清空MCA Bank记录的故障功能，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启热复位清空 MCA Bank 故障。</li> <li>Disabled (缺省): 热复位不清空 MCA Bank 记录的故障信息。</li> </ul>

#### 4. UPI Error Enabling 界面

UPI Error Enabling界面如[图 3-80](#)所示。具体参数说明如[表 3-72](#)所示。

图3-80 UPI Error Enabling 界面

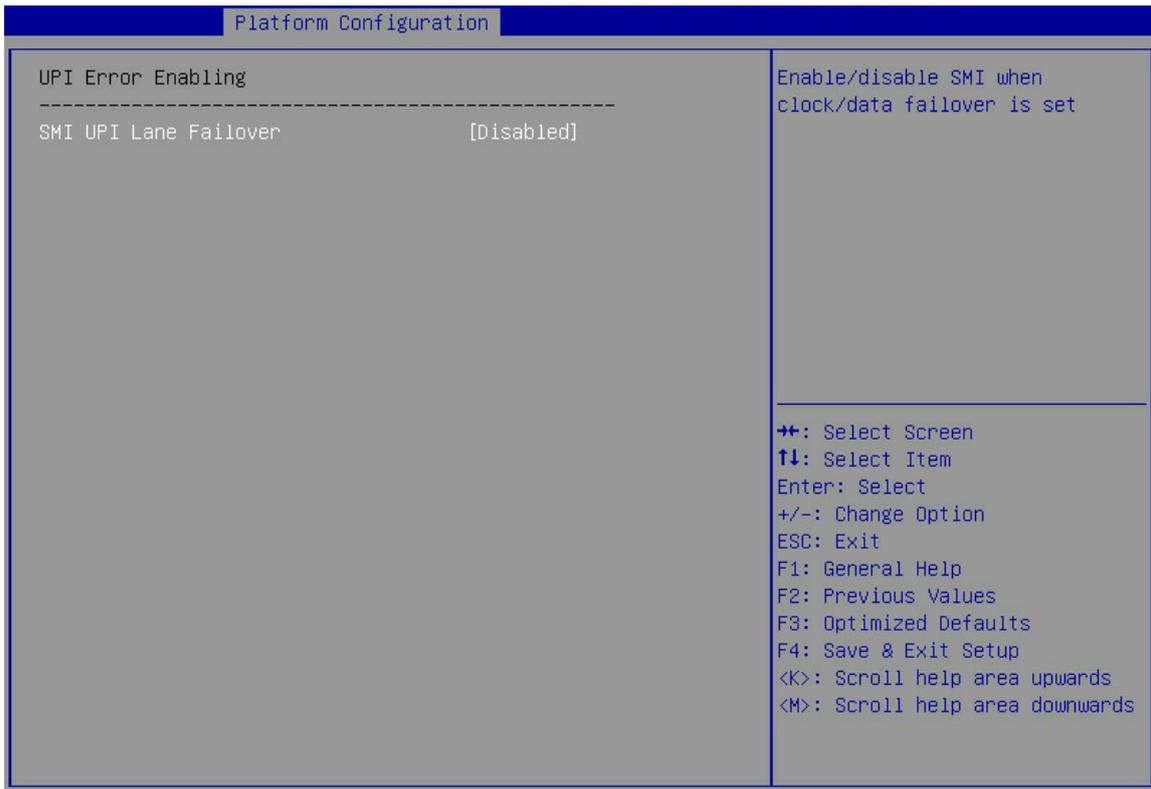


表3-72 UPI Error Enabling 界面参数

界面参数	功能说明
SMI UPI Lane Failover	UPI Lane发生错误时触发SMI中断设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启 UPI Lane 发生错误时触发 SMI 中断。</li> <li>Disabled (缺省): 关闭 UPI Lane 发生错误时触发 SMI 中断。</li> </ul>

## 5. Memory Error Enabling 界面

Memory Error Enabling界面如图3-81所示。具体参数说明如表3-73所示。

图3-81 Memory Error Enabling 界面

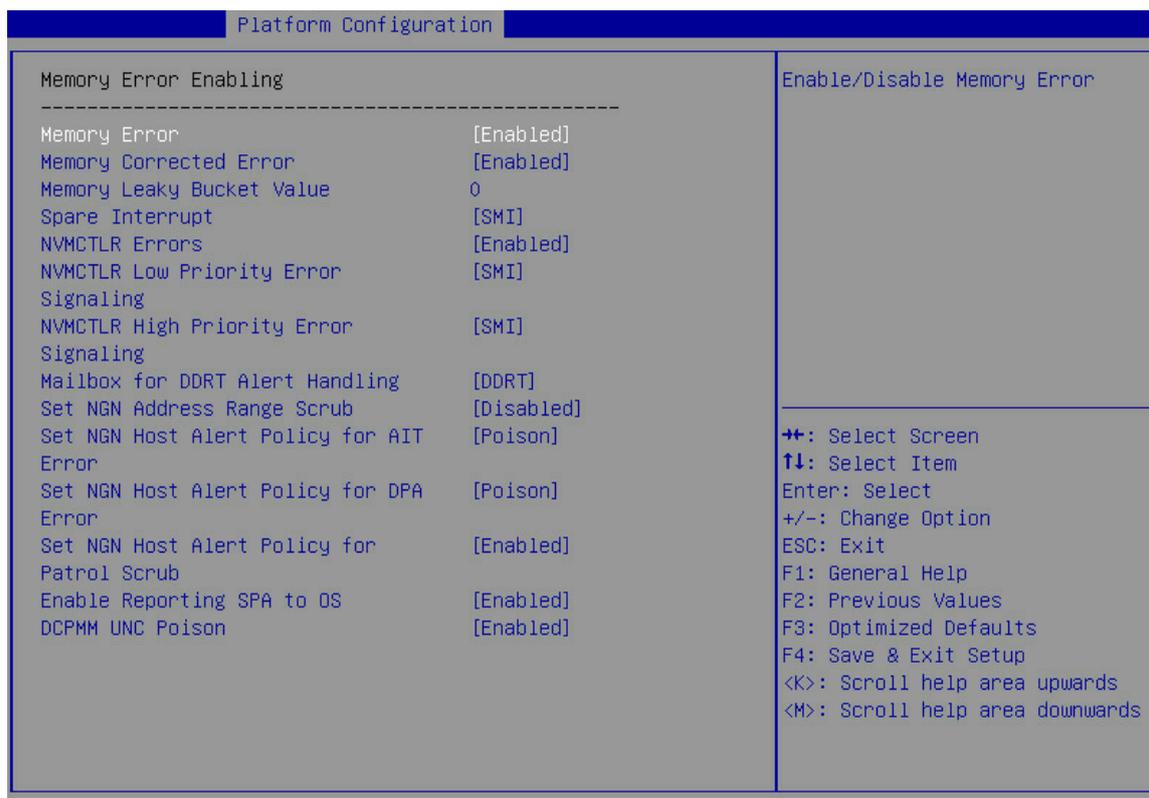


表3-73 Memory Error Enabling 界面参数

界面参数	功能说明
Memory Error	内存错误使能设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省): 开启内存错误功能。</li> <li>Disabled: 关闭内存错误功能。</li> </ul>
Memory Corrected Error	内存可纠正错误使能设置，当Memory Corrected Error设置为Enabled时，显示该选项。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省): 开启内存可纠正错误功能。</li> <li>Disabled: 关闭内存可纠正错误功能。</li> </ul>

界面参数	功能说明
Memory Leaky Bucket Value	内存漏桶值,默认为0,可设定为0x0000-0xffff之间。当Memory Corrected Error设置为Enabled时,显示该选项。
Spare Interrupt	Spare Interrupt类型设置,当Memory Corrected Error设置为Enabled时,显示该选项。菜单选项为: <ul style="list-style-type: none"> <li>• Disabled: 禁止使用内存备用中断。</li> <li>• SMI (缺省): SMI 中断。</li> <li>• Error Pin: Error Pin 中断。</li> <li>• CMCI: CMCI 中断。</li> </ul>
NVMCTLR Errors	NVMCTLR 错误记录及上报功能。当Memory Corrected Error设置为Enabled时,显示该选项。菜单选项为: <ul style="list-style-type: none"> <li>• Enabled (缺省): 开启 NVMCTLR 错误记录及上报功能。</li> <li>• Disabled: 关闭 NVMCTLR 错误记录及上报功能。</li> </ul>
NVMCTLR Low Priority Error Signaling	NVMCTLR 低优先级错误信号设置,当Memory Corrected Error设置为Enabled时,显示该选项。菜单选项为: <ul style="list-style-type: none"> <li>• Disabled: 不上报 NVMCTLR 低优先级错误。</li> <li>• SMI (缺省): 使用 SMI 中断发出 NVMCTLR 低优先级错误信号。</li> <li>• ERRO# Pin: 使用 ERRO# Pin 发出 NVMCTLR 低优先级错误信号。</li> </ul>
NVMCTLR High Priority Error Signaling	NVMCTLR 高优先级错误信号设置,当Memory Corrected Error设置为Enabled时,显示该选项。菜单选项为: <ul style="list-style-type: none"> <li>• Disabled: 不上报 NVMCTLR 高优先级错误</li> <li>• SMI (缺省): 使用 SMI 中断发出 NVMCTLR 高优先级错误信号。</li> <li>• ERRO# Pin: 使用 ERRO# Pin 发出 NVMCTLR 高优先级错误信号。</li> </ul>
Mailbox for DDRT Alert Handling	Mailbox收到DDRT告警时的处理方式。当Memory Corrected Error设置为Enabled时,显示该选项。菜单选项为: <ul style="list-style-type: none"> <li>• DDRT (缺省): 通过 DDRT 处理告警。</li> <li>• SMBUS: 通过 SMBUS 处理告警。该选项仅用于验证。</li> </ul>
Set NGN Address Range Scrub	设置NGN DIMM物理地址范围擦除。当Memory Corrected Error设置为Enabled时,显示该选项。菜单选项为: <ul style="list-style-type: none"> <li>• Enabled: 启用 NGN DIMM 物理地址范围擦除。</li> <li>• Disabled (缺省): 禁用 NGN DIMM 物理地址范围擦除。</li> </ul>
Set NGN Host Alert Policy for AIT Error	设置NGN主机的AIT错误告警策略。当Memory Corrected Error设置为Enabled时,显示该选项。根据接收地址间接表,配置信号为Poison或病毒。菜单选项为: <ul style="list-style-type: none"> <li>• Poison (缺省): 配置信号为 Poison。</li> <li>• Viral: 配置信号为病毒。</li> </ul>

界面参数	功能说明
Set NGN Host Alert Policy for DPA Error	<p>设置NGN主机的DPA错误告警策略，当服务器的CPU不支持Advanced RAS功能时，该选项置灰。根据接收DIMM物理地址错误，配置信号为Poison或病毒。当Memory Corrected Error设置为Enabled时，显示该选项。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Poison（缺省）：配置信号为Poison。</li> <li>• Viral：配置信号为病毒。</li> </ul>
Set NGN Host Alert Policy for Patrol Scrub	<p>启用/禁用NGN主机的Patrol Scrub错误告警策略，当服务器的CPU不支持Advanced RAS功能时，该选项置灰。根据接收NGN Patrol Scrub检测到的不可纠正错误来触发DDRT中断。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enable（缺省）：开启NGN主机的Patrol Scrub错误告警策略。</li> <li>• Disable：关闭NGN主机的Patrol Scrub错误告警策略。</li> </ul>
Enable Reporting SPA to OS	<p>设置是否上报SPA(system physical address)给操作系统。当Memory Corrected Error设置为Enabled时，显示该选项。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：使能SPA上报操作系统，仅禁用MCE恢复阈值。</li> <li>• Disabled：禁用SPA上报操作系统。</li> </ul>
DCPMM UNC Poison	<p>设置是否启用Intel DCPMM内存的Poison模式。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用。当检测到Intel DCPMM内存的不可纠正错误时，为异常数据打上Poison标记并继续传输。</li> <li>• Disabled：禁用。当检测到Intel DCPMM内存出现不可纠正错误时，直接上报不可纠正错误。</li> </ul>

## 6. IIO Error Enabling 界面

IIO Error Enabling界面如[图 3-82](#)和[图 3-83](#)所示。具体参数说明如[表 3-74](#)所示。

图3-82 IIO Error Enabling 界面 1

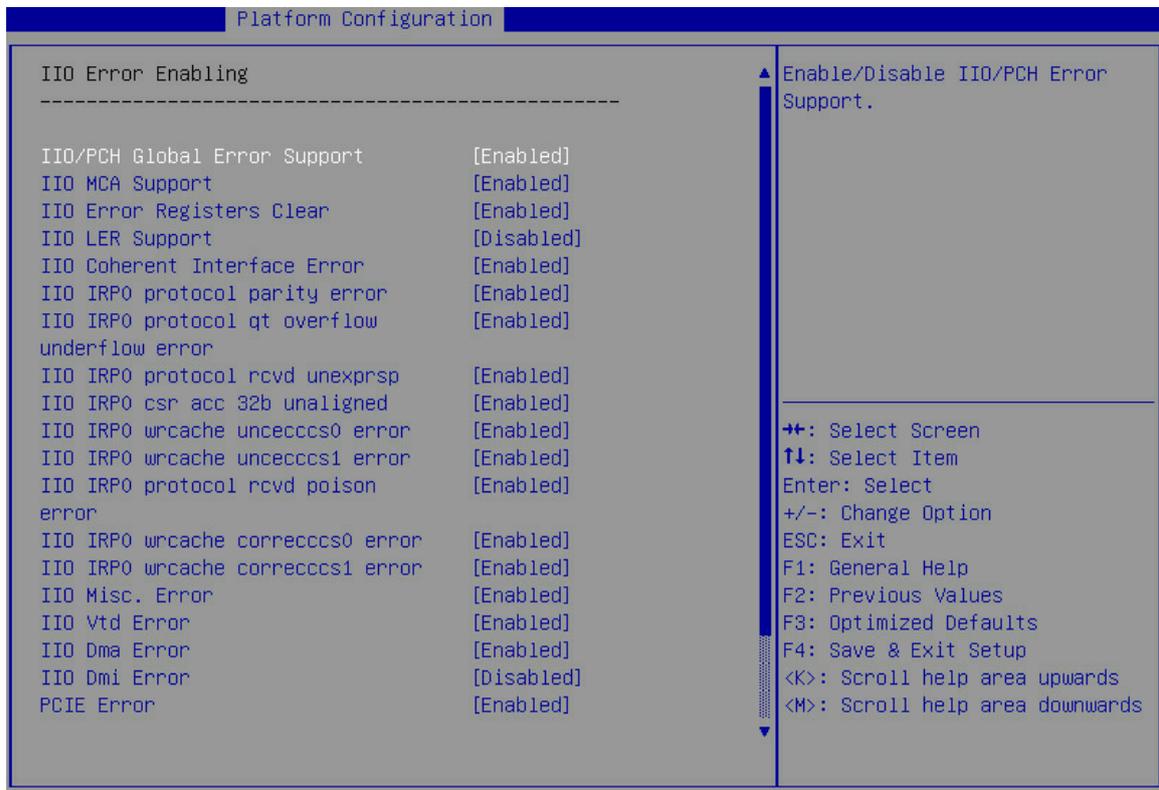


图3-83 IIO Error Enabling 界面 2

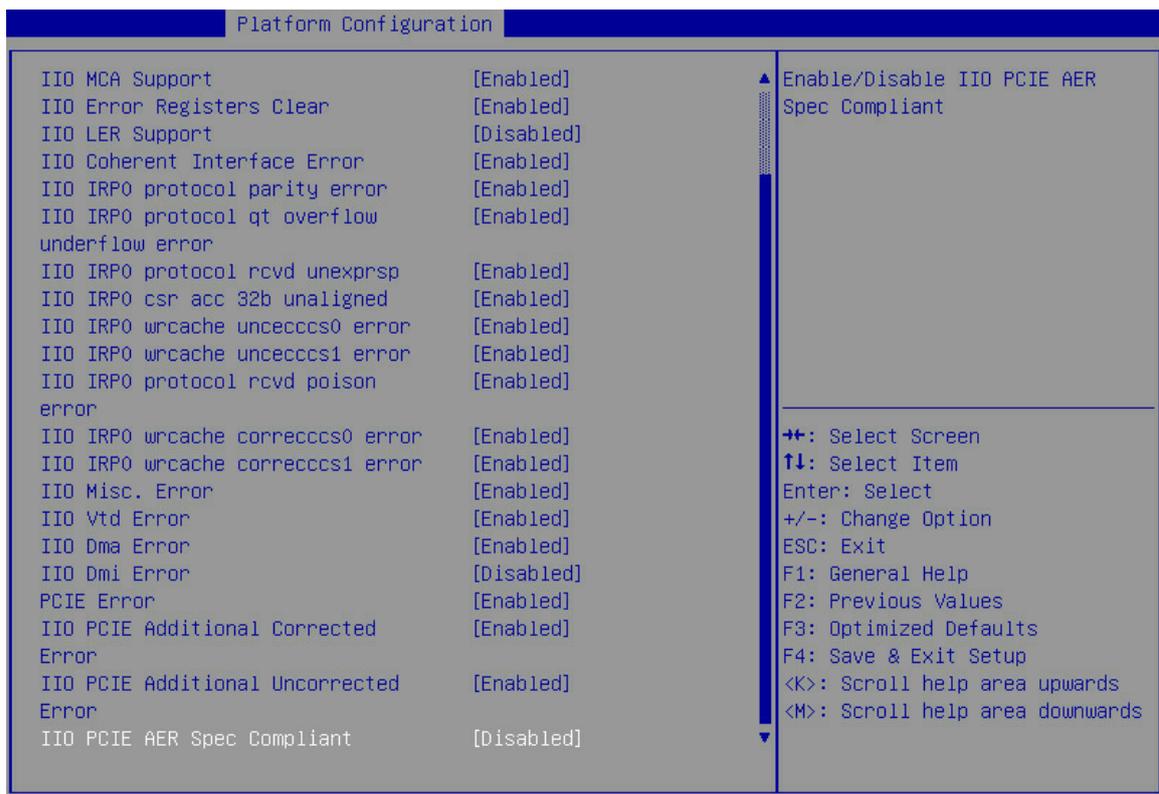


表3-74 IIO Error Enable 界面参数

界面参数	功能说明
IIO/PCH Global Error Support	IIO/PCH全局错误支持功能配置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 IIO/PCH 全局错误支持功能。</li> <li>• Disabled: 关闭 IIO/PCH 全局错误支持功能。当设置为该选项时，下面 IIO 错误的选项均不显示。</li> </ul>
IIO MCA Support	启用/禁用 IIO MCA 支持。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用 IIO MCA 支持。</li> <li>• Disabled: 禁用 IIO MCA 支持。</li> </ul>
IIO Error Pin Programming	启用/禁用 IIO 错误 Pin 可编程功能。当 IIO MCA Support 设置为 Disabled 时，显示该选项。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 启用消除 IIO 错误寄存器。</li> <li>• Disabled（缺省）：禁用消除 IIO 错误寄存器。</li> </ul>
IIO Error Registers Clear	启用/禁用 IIO 错误寄存器清除。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用消除 IIO 错误寄存器。</li> <li>• Disabled: 禁用消除 IIO 错误寄存器。</li> </ul>
IIO LER Support	IIO LER（Live Error Recovery，实时错误恢复）功能支持配置，当服务器的CPU不支持Advanced RAS功能时，该选项置灰。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 启用 IIO LER 支持。</li> <li>• Disabled（缺省）：禁用 IIO LER 支持。</li> </ul>
LER MA Error Logging	该选项用于当开启LER功能时，关闭PCIe MCA错误记录。当IIO LER Support选项设置为Enabled时，显示该选项。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用关闭 PCIe MCA 错误记录。</li> <li>• Disabled: 禁用关闭 PCIe MCA 错误记录。</li> </ul>
IIO Coherent Interface Error	IIO一致接口错误检测。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用 IIO 一致接口错误检测。</li> <li>• Disabled: 屏蔽 IIO 一致接口错误。</li> </ul>
IIO IRPO protocol parity error	IIO IRPO协议奇偶校验错误配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用一致接口协议 IIO 奇偶校验错误检测。</li> <li>• Disabled: 屏蔽一致接口协议 IIO 奇偶校验错误。</li> </ul>
IIO IRPO protocol qt overflow underflow error	IIO IRPO 队列表溢出错误上报配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用 IIO 一致接口协议层队列表溢出或下溢错误上报。</li> <li>• Disabled: 禁用 IIO 一致接口协议层队列表溢出或下溢错误上报。</li> </ul>

界面参数	功能说明
IIO IRPO protocol rcvd unexprsp	<p>IIO IRPO协议rcvd unexprsp配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> (缺省)：启用 IIO 一致接口协议层接收到不期望的响应或者完成错误报告。</li> <li>• <b>Disable</b>：禁用 IIO 一致接口协议层接收到不期望的响应或者完成错误报告。</li> </ul>
IIO IRPO csr acc 32b unaligned	<p>IIO IRPO csr acc 32b未对齐配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> (缺省)：启用 IIO 一致接口 CSR 接入穿过 32-bit 边界错误报告。</li> <li>• <b>Disabled</b>：禁用 IIO 一致接口 CSR 接入穿过 32-bit 边界错误报告。</li> </ul>
IIO IRPO wrcache uncecccs0 error	<p>IIO IRPO wrcache uncecccs0错误配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> (缺省)：启用 IIO 一致接口写缓存不可修正 ECC 错误报告。</li> <li>• <b>Disabled</b>：禁用 IIO 一致接口写缓存不可修正 ECC 错误报告。</li> </ul>
IIO IRPO wrcache uncecccs1 error	<p>IIO IRPO wrcache uncecccs1错误配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> (缺省)：启用 IIO 一致接口写缓存不可修正 ECC 错误报告。</li> <li>• <b>Disabled</b>：禁用 IIO 一致接口写缓存不可修正 ECC 错误报告。</li> </ul>
IIO IRPO protocol rcvd poison error	<p>IIO IRPO协议rcvd poison错误配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> (缺省)：启用 IIO 一致接口协议层接收到 Poison 包错误报告。</li> <li>• <b>Disabled</b>：禁用 IIO 一致接口协议层接收到 Poison 包错误报告。</li> </ul>
IIO IRPO wrcache correcccs0 error	<p>IIO IRPO wrcache correcccs0错误配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> (缺省)：启用 IIO 一致接口写缓存可修复 ECC 错误报告。</li> <li>• <b>Disabled</b>：禁用 IIO 一致接口写缓存可修复 ECC 错误报告。</li> </ul>
IIO IRPO wrcache correcccs1 error	<p>IIO IRPO wrcache correcccs1错误配置。当IIO Coherent Interface Error选项设置为Disabled时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> (缺省)：启用 IIO 一致接口写缓存可修复 ECC 错误报告。</li> <li>• <b>Disabled</b>：禁用 IIO 一致接口写缓存可修复 ECC 错误报告。</li> </ul>

界面参数	功能说明
IIO Misc. Error	IIO其他错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 IIO 其他错误检测。</li> <li>Disabled：屏蔽 IIO 其他错误。</li> </ul>
IIO Vtd Error	IIO Vtd错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 IIO Vtd 错误检测。</li> <li>Disabled：屏蔽 IIO Vtd 错误。</li> </ul>
IIO Dma Error	IIO DMA错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 IIO DMA 错误检测。</li> <li>Disabled：屏蔽 IIO DMA 错误。</li> </ul>
IIO Dmi Error	IIO DMI错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled：启用 IIO DMI 错误检测。</li> <li>Disabled (缺省)：屏蔽 IIO DMI 错误。</li> </ul>
PCIE Error	PCIE错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 PCIE 错误检测。</li> <li>Disabled：屏蔽 PCIE 错误。</li> </ul>
IIO PCIE Additional Corrected error	IIO PCIE附加可纠正错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 IIO PCIE 附加可纠正错误检测。</li> <li>Disabled：屏蔽 IIO PCIE 附加可纠正错误。</li> </ul>
IIO PCIE Additional Uncorrected error	IIO PCIE附加不可纠正错误配置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省)：启用 IIO PCIE 附加不可纠正错误检测。</li> <li>Disabled：屏蔽 IIO PCIE 附加不可纠正错误。</li> </ul>
IIO PCIE AER Spec Compliant	IIO PCIE AER Spec合规配置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled：开启 IIO PCIE AER Spec 合规功能。此时，带有 Poison 标记的错误，仍被记录为致命错误。</li> <li>Disabled (缺省)：关闭 IIO PCIE AER Spec 合规功能。Poison 错误会被记录为非致命错误。</li> </ul>

## 7. PCI Error Enabling 界面

PCI Error Enabling界面如[图 3-84](#)所示。具体参数说明如[表 3-75](#)所示。

图3-84 PCI Error Enabling 界面

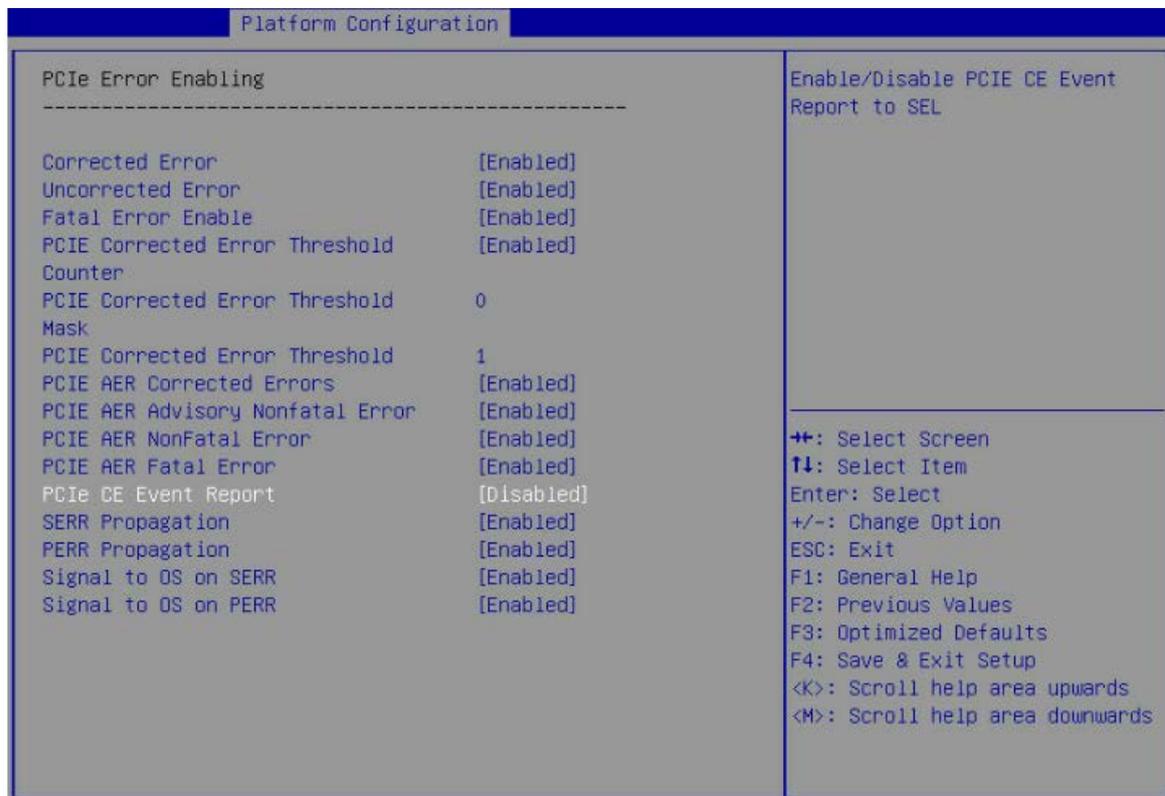


表3-75 PCI Error Enabling 界面参数

界面参数	功能说明
Corrected Error	<p>PCIe可修正错误使能设置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PCIe 可修正错误检测。</li> <li>Disabled：屏蔽 PCIe 可修正错误。</li> </ul>
Uncorrected Error	<p>PCIe不可修正错误设置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PCIe 不可修正错误检测。</li> <li>Disabled：屏蔽 PCIe 不可修正错误。</li> </ul>
Fatal Error Enable	<p>PCIe致命错误使能设置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PCIe 致命错误功能检测。</li> <li>Disabled：屏蔽 PCIe 致命错误功能。</li> </ul>
PCIE Corrected Error Threshold Counter	<p>PCIe可修正错误阈值计数器使能设置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PCIe 可修正错误阈值计数器功能。</li> <li>Disabled：关闭 PCIe 可修正错误阈值计数器功能。</li> </ul>
PCIE Corrected Error Threshold Mask	<p>PCIe可修正错误阈值掩码，缺省为0。当PCIE Corrected Error Threshold Counter选项设置为Enabled时可配置。</p>
PCIE Correctable Error Threshold	<p>PCIe可修正错误阈值设置，缺省为1。当PCIE Corrected Error Threshold Counter选项设置为Enabled时可配置。</p>

界面参数	功能说明
PCIE AER Corrected Errors	PCIE AER可修正错误设置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PCIE AER 可修正错误检测。</li> <li>Disabled：屏蔽 PCIE AER 可修正错误。</li> </ul>
PCIE AER Advisory Nonfatal Error	PCIE AER建议非致命错误设置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 PCIE AER 建议非致命错误检测。</li> <li>Disabled：屏蔽 PCIE AER 建议非致命错误。</li> </ul>
PCIE AER NonFatal Error	PCIE AER非致命错误设置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 PCIE AER 非致命错误检测。</li> <li>Disabled：屏蔽 PCIE AER 非致命错误。</li> </ul>
PCIE AER Fatal Error	PCIE AER致命错误设置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 PCIE AER 致命错误检测。</li> <li>Disabled：屏蔽 PCIE AER 致命错误。</li> </ul>
PCIE CE Event Report	PCIE AER可纠正错误上报至SEL（System Event Log，系统事件日志）。菜单选项为： <ul style="list-style-type: none"> <li>Enabled：启用 PCIE AER 可纠正错误上报。</li> <li>Disabled（缺省）：禁用 PCIE AER 可纠正错误上报。</li> </ul>
SERR Propagation	SERR传播设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 SERR 传播功能。</li> <li>Disabled：关闭 SERR 传播功能。</li> </ul>
PERR Propagation	PERR传播设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PERR 传播功能。</li> <li>Disabled：关闭 PERR 传播功能。</li> </ul>
Signal to OS on SERR	SERR上报OS信号。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 SERR 上至 OS 信号。</li> <li>Disabled：禁用 SERR 上至 OS 信号。</li> </ul>
Signal to OS on PERR	PERR上报OS信号。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 PERR 上至 OS 信号。</li> <li>Disabled：禁用 PERR 上至 OS 信号。</li> </ul>

## 8. Enhanced Diagnosis Enabling 界面

Enhanced Diagnosis Enabling界面如[图 3-84](#)所示。具体参数说明如[表 3-75](#)所示。

图3-85 Enhanced Diagnosis Enabling 界面

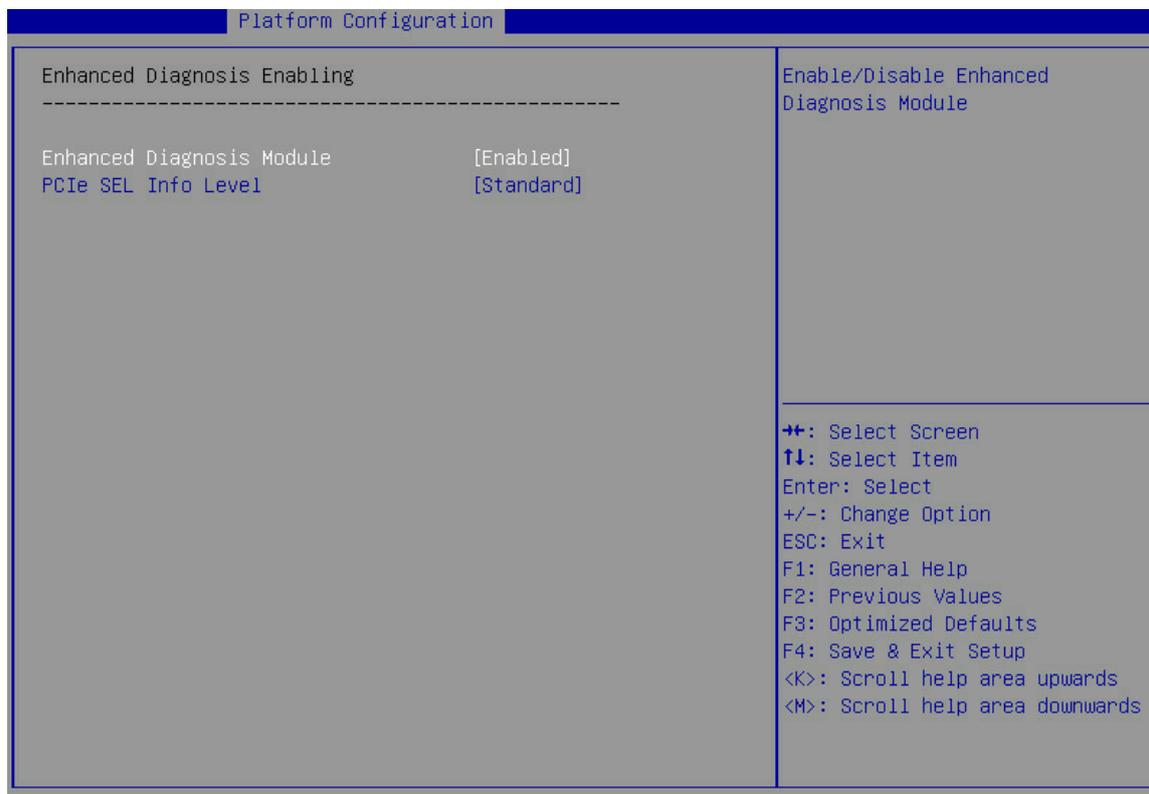


表3-76 Enhanced Diagnosis Enabling 界面参数

界面参数	功能说明
Enhanced Diagnosis Module	<p>增强诊断模块，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用增强诊断模块。</li> <li>• Disabled：禁用增强诊断模块。</li> </ul>
PCIe SEL Info Level	<p>设置PCIe模块的SEL日志上报等级。Enhanced Diagnosis Module选项设置为Enabled时可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Standard（缺省）：上报标准格式的PCIe SEL日志。</li> <li>• Detailed：上报详细的PCIe SEL日志。相比标准上报格式，增加了PCIe错误类型。</li> </ul>

### 3.4 Socket Configuration 界面

Socket Configuration界面如[图 3-86](#)所示，主要包含CPU配置、通用RefCode配置、UPI配置、内存配置、IIO配置、高级电源管理配置等。具体参数说明如[表 3-77](#)所示。

图3-86 Socket Configuration 界面

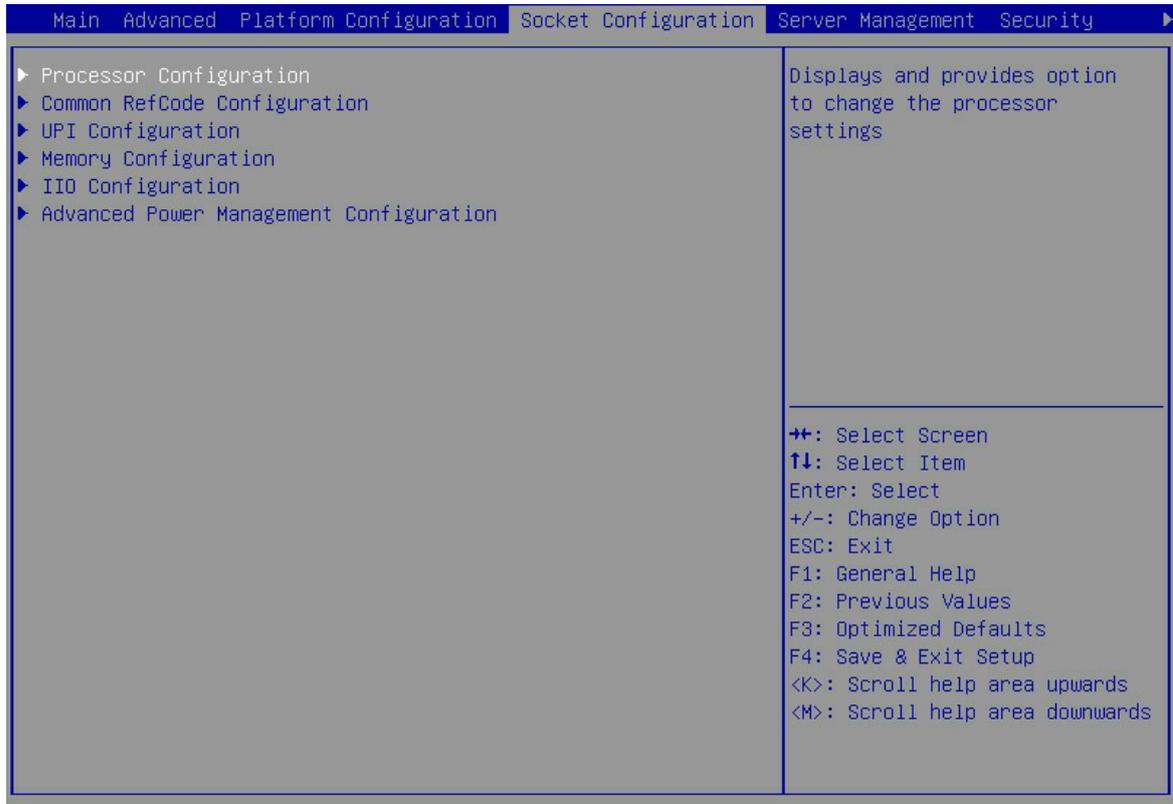


表3-77 Socket Configuration 界面参数

界面参数	功能说明
Processor Configuration	CPU配置菜单。
Common RefCode Configuration	通用RefCode配置菜单。
UPI Configuration	UPI配置菜单。
Memory Configuration	内存配置菜单。
IIO Configuration	IIO配置菜单。
Advanced Power Management Configuration	高级电源管理配置菜单。

### 3.4.1 Processor Configuration 界面

如图 3-87和图 3-88所示，通过Processor Configuration界面，可以对CPU进行配置，包括超线程、Intel硬件辅助虚拟化、硬件预取等。具体参数说明如表 3-78所示。

图3-87 Processor Configuration 界面 1

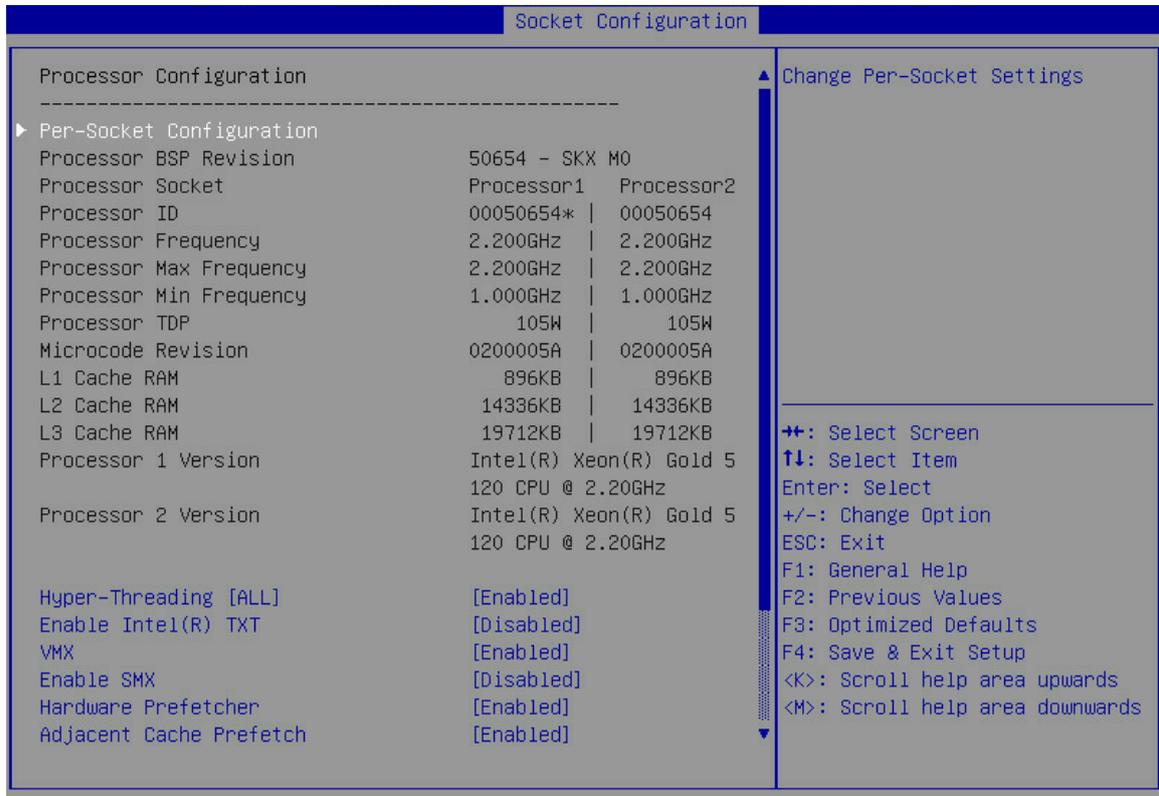


图3-88 Processor Configuration 界面 2

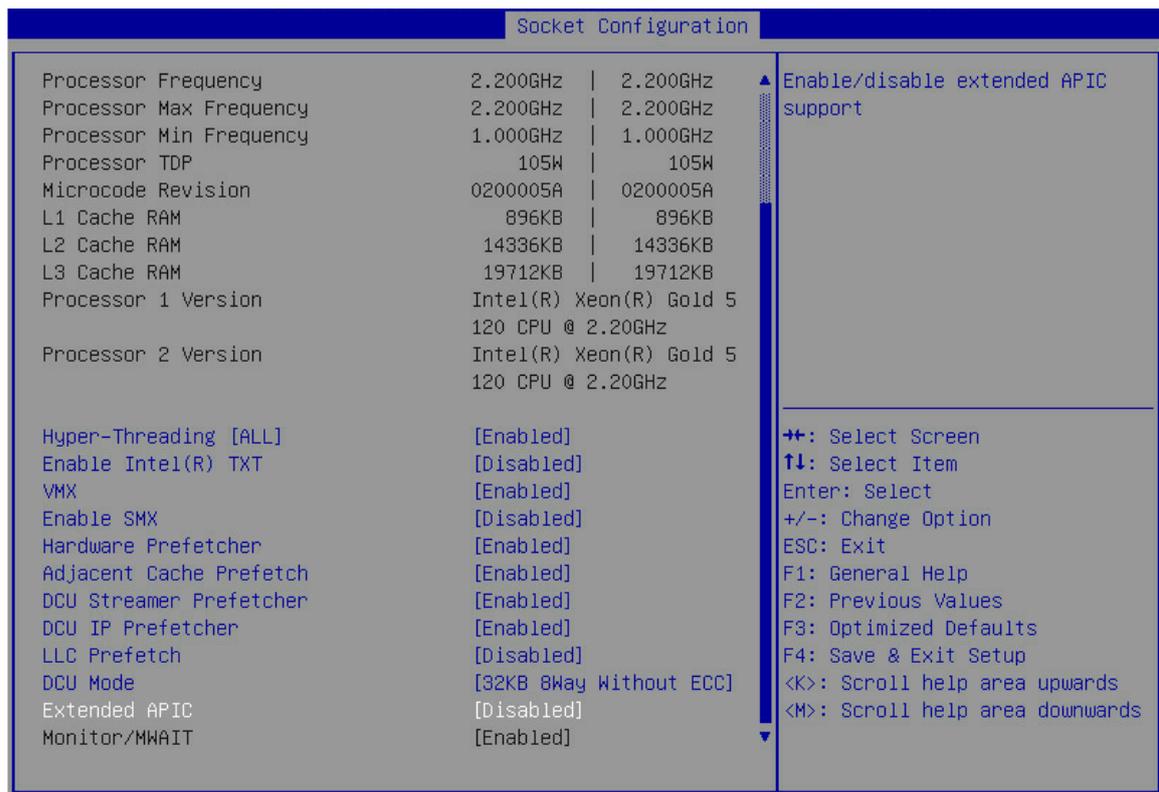


表3-78 Processor Configuration 界面参数

界面参数	功能说明
Per-Socket Configuration	每个插槽上的CPU配置。
Processor BSP Revision	处理器BSP修订版本。
Processor Socket	显示CPU插槽序号。
Processor ID	显示CPU ID。
Processor Frequency	显示CPU主频。
Processor Max Frequency	显示CPU最大频率。
Processor Min Frequency	显示CPU最小频率。
Processor TDP	显示CPU的热设计功耗。
Microcode Revision	显示CPU的微码版本信息。
L1 Cache RAM	显示1级缓存容量。
L2 Cache RAM	显示2级缓存容量。
L3 Cache RAM	显示3级缓存容量。
Processor X Version	显示CPU X 版本信息。CPU在位时显示该选项，否则不显示。
Hyper-Threading [ALL]	<p>超线程开关，超线程技术可以把1个物理内核模拟成2个逻辑内核，让单个处理器都能使用线程级并行计算，进而兼容多线程操作系统和软件，减少CPU闲置时间，提高CPU的运行效率。不支持超线程功能的CPU不显示该选项。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启超线程功能。</li> <li>• Disabled：关闭超线程功能。</li> </ul>
Enable Intel(R) TXT	<p>Intel可信执行技术开关，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：开启 Intel 可信执行技术支持，可以全面保护虚拟计算环境中数据的安全。</li> <li>• Disabled（缺省）：关闭 Intel 可信执行技术支持。</li> </ul> <p>需注意的是：在开启Intel可信执行技术开关时，请将Debug Mode选项设置为Disabled，以避免安全隐患。</p>
VMX	<p>Intel硬件辅助虚拟化技术开关，Enable Intel(R) TXT设置为Disabled时可修改该选项，Enable Intel(R) TXT设置为Enabled时该选项置灰，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 Intel 硬件辅助虚拟化技术，可以提高服务器硬件资源的利用率。</li> <li>• Disabled：关闭 Intel 硬件辅助虚拟化技术。</li> </ul>
Enable SMX	<p>开启安全模式扩展功能，Enable Intel(R) TXT设置为Disabled时可修改该选项，Enable Intel(R) TXT设置为Enabled时该选项置灰，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：开启安全模式扩展功能。</li> <li>• Disabled（缺省）：关闭安全模式扩展功能。</li> </ul>

界面参数	功能说明
Hardware Prefetcher	<p>硬件预取配置，CPU处理指令或数据之前，将这些指令或数据从内存中预取到L2缓存中，减少内存读取的时间，帮助消除潜在的瓶颈，以此提高系统性能，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启硬件预取功能。</li> <li>Disabled：关闭硬件预取功能。</li> </ul>
Adjacent Cache Prefetcher	<p>邻近高速缓冲预取，即MLC空间预取。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启邻近高速缓冲预取。</li> <li>Disabled：关闭邻近高速缓冲预取。</li> </ul>
DCU Streamer Prefetcher	<p>数据高速缓存单元预取流设置。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 DCU 流预取，会预取流并发送到它的一级缓存，以改善数据处理和系统性能。</li> <li>Disabled：关闭 DCU 流预取。</li> </ul>
DCU IP Prefetcher	<p>数据高速缓存单元预取IP设置。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 DCU IP 预取，会预取 IP 地址以改善网络连接和系统性能。</li> <li>Disabled：关闭 DCU IP 预取。</li> </ul>
LLC Prefetch	<p>三级缓存预取特性开关。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled：开启三级缓存预取。</li> <li>Disabled（缺省）：关闭三级缓存预取。</li> </ul>
DCU Mode	<p>选择数据缓存单元DCU模式。菜单选项为：</p> <ul style="list-style-type: none"> <li>32KB 8way without ECC（缺省）：选择配置为 32KB 8 路无 ECC。</li> <li>16KB 4way with ECC：选择配置为 16KB 4 路有 ECC。</li> </ul>
Extended APIC	<p>扩展APIC模式设置，当所配置的处理器总核数超过256个时，建议开启该选项以使操作系统能更高效支持CPU多核特性功能。菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled：开启扩展 APIC 模式。</li> <li>Disabled（缺省）：关闭扩展 APIC 模式。</li> </ul>
Monitor/Mwait	<p>Monitor/Mwait指令开关，开启该指令后可以优化CPU的指令运行。如需关闭CPU C State节能状态，部分操作系统下需要同时关闭本选项。该选项当前不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>Auto：自动设置，当前为启用 Monitor/Mwait 指令。</li> <li>Enabled（缺省）：开启 Monitor/Mwait 指令。</li> <li>Disabled：关闭 Monitor/Mwait 指令。</li> </ul>

## 1. Per-Socket Configuration 界面

下面介绍服务器的Per-Socket Configuration界面，如[图 3-89](#)。具体参数说明如[表 3-79](#)所示。

图3-89 Per-Socket Configuration 界面

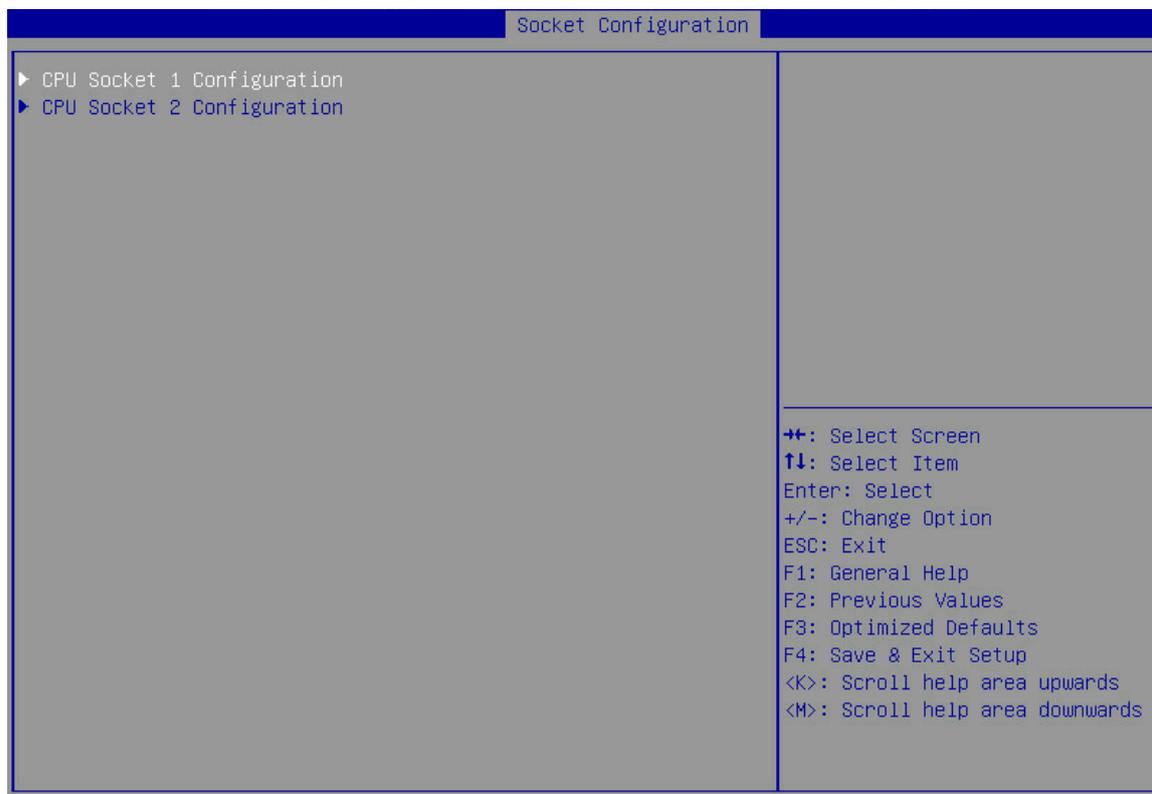


表3-79 Per-Socket Configuration 界面参数

界面参数	功能说明
CPU Socket X Configuration	CPU X 配置菜单。CPU在位时显示该菜单，否则不显示。

## 2. CPU Socket Configuration 界面

每个CPU Socket配置界面参数相同，本文以CPU Socket 1 Configuration为例。CPU Socket 1 Configuration界面如[图 3-90](#)所示。具体参数说明如[表 3-80](#)所示。

图3-90 CPU Socket 1 Configuration 界面

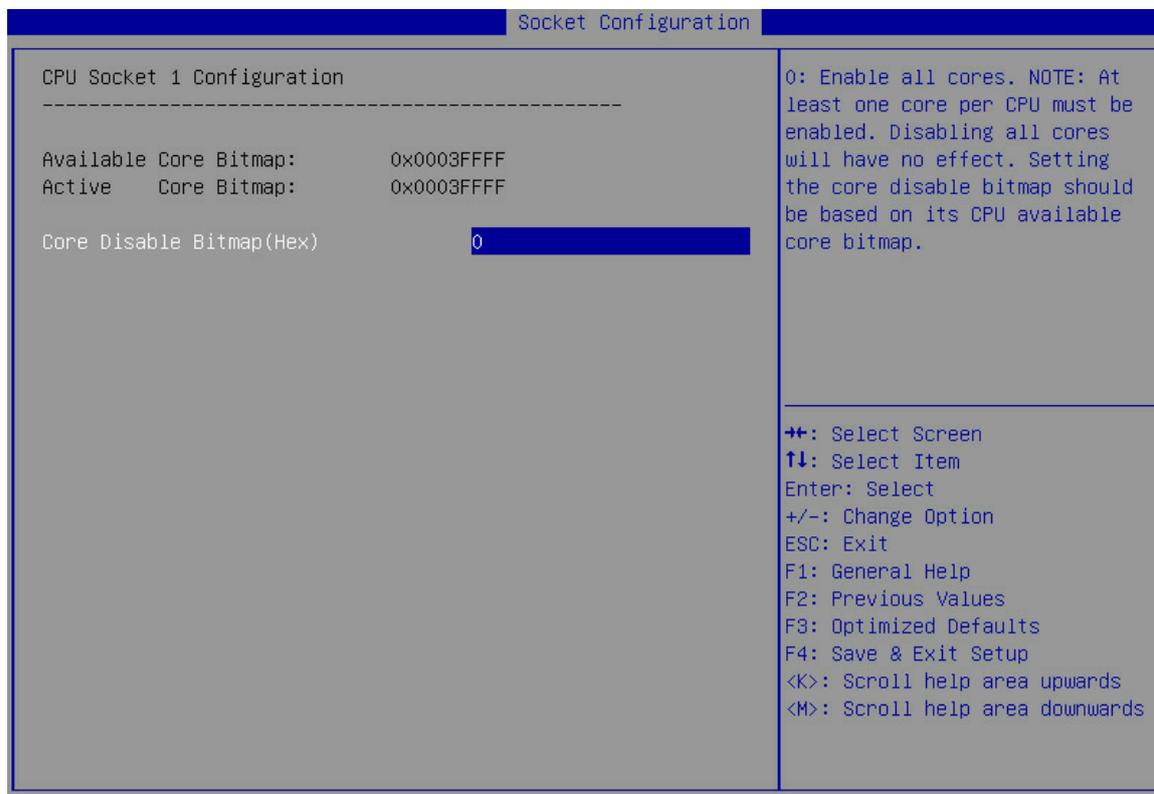


表3-80 CPU Socket 1 Configuration 界面参数

界面参数	功能说明
Available Core Bitmap	显示可用核位映射。
Active Core Bitmap	显示活动核位映射。
Core Disable Bitmap(Hex)	核禁用位映射，为十六进制数。缺省为0，表示使能所有核。 设置要禁用的核时，请参照当前CPU Socket的可用核位映射（Available Core Bitmap）。需要注意的是，每个处理器至少要使能1个核，禁用所有核的配置将不会生效。

### 3.4.2 Common RefCode Configuration 界面

如图 3-91 所示，通过 Common RefCode Configuration 界面，可以对通用 RefCode 进行配置，包括 4G 以上 MMIO 基址、NUMA 等。具体参数说明如表 3-81 所示。

图3-91 Common RefCode Configuration 界面

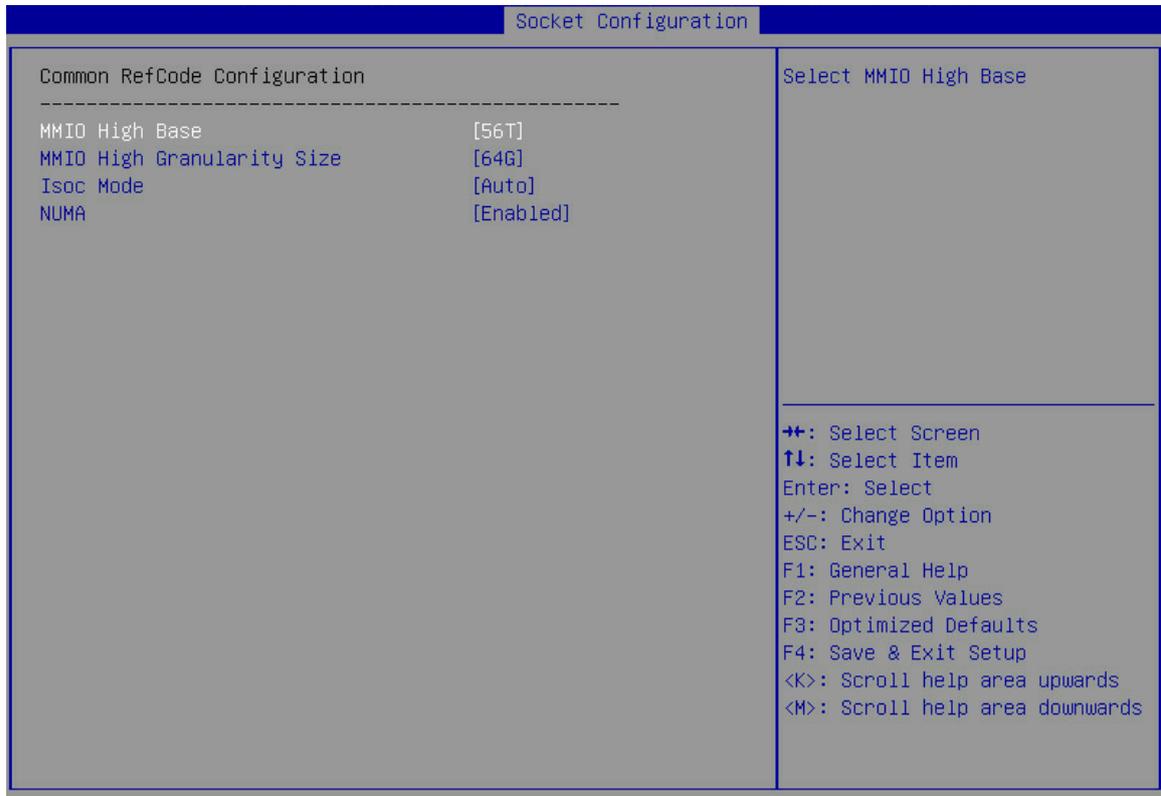


表3-81 Common RefCode Configuration 界面参数

界面参数	功能说明
MMIO High Base	内存映射I/O高位基地址，MMIO指内存映射I/O，菜单选项为： <ul style="list-style-type: none"> <li>• 56T（缺省）</li> <li>• 40T</li> <li>• 24T</li> <li>• 16T</li> <li>• 4T</li> <li>• 1T</li> </ul> UNISINSIGHT AIX R6220L-G3 服务器该选项的缺省值为 4T。
MMIO High Granularity Size	内存映射I/O高位粒度大小，默认分配给每个栈的MMIO资源大小等于内存映射I/O高位粒度大小。菜单选项为： <ul style="list-style-type: none"> <li>• 1G</li> <li>• 4G</li> <li>• 16G</li> <li>• 64G（缺省）</li> <li>• 256G</li> <li>• 1024G</li> </ul> UNISINSIGHT AIX R6220L-G3 服务器该选项的缺省值为 1024G。

界面参数	功能说明
Isoc Mode	Isoc模式。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 关闭 Isoc 模式。</li> <li>• Enabled: 开启 Isoc 模式。</li> <li>• Auto (缺省): 系统自动选择。</li> </ul>
NUMA	NUMA开关，内存访问时间取决于待访问的内存是否为当前CPU对应的内存，开启NUMA功能后，CPU访问本地存储器的速度比非本地存储器的速度快，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 开启 NUMA。</li> <li>• Disabled: 关闭 NUMA。</li> </ul>

### 3.4.3 UPI Configuration 界面

如图 3-92 所示，通过UPI Configuration界面，可以对CPU之间的UPI进行配置。具体参数说明如表 3-82 所示。

图3-92 UPI Configuration 界面

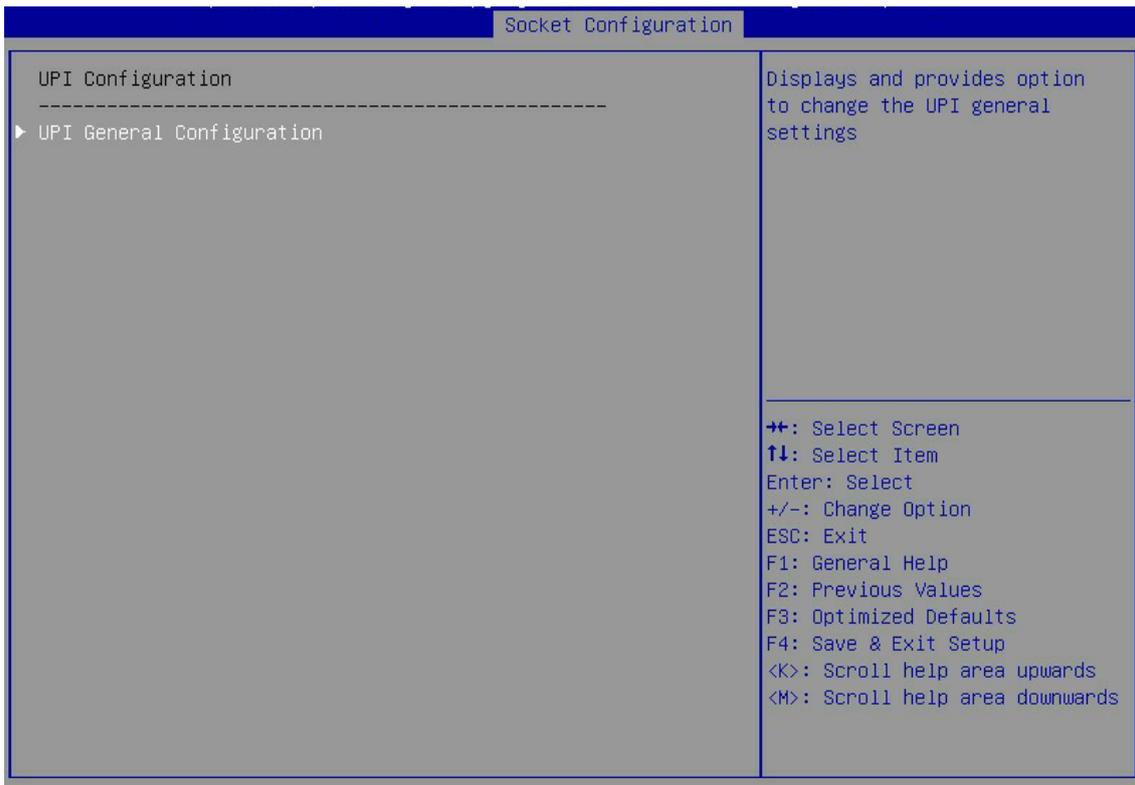


表3-82 UPI Configuration 界面参数

界面参数	功能说明
UPI General Configuration	UPI通用配置菜单。

## 1. UPI General Configuration 界面

UPI General Configuration界面如图 3-93所示。具体参数说明如表 3-83所示。

图3-93 UPI General Configuration 界面

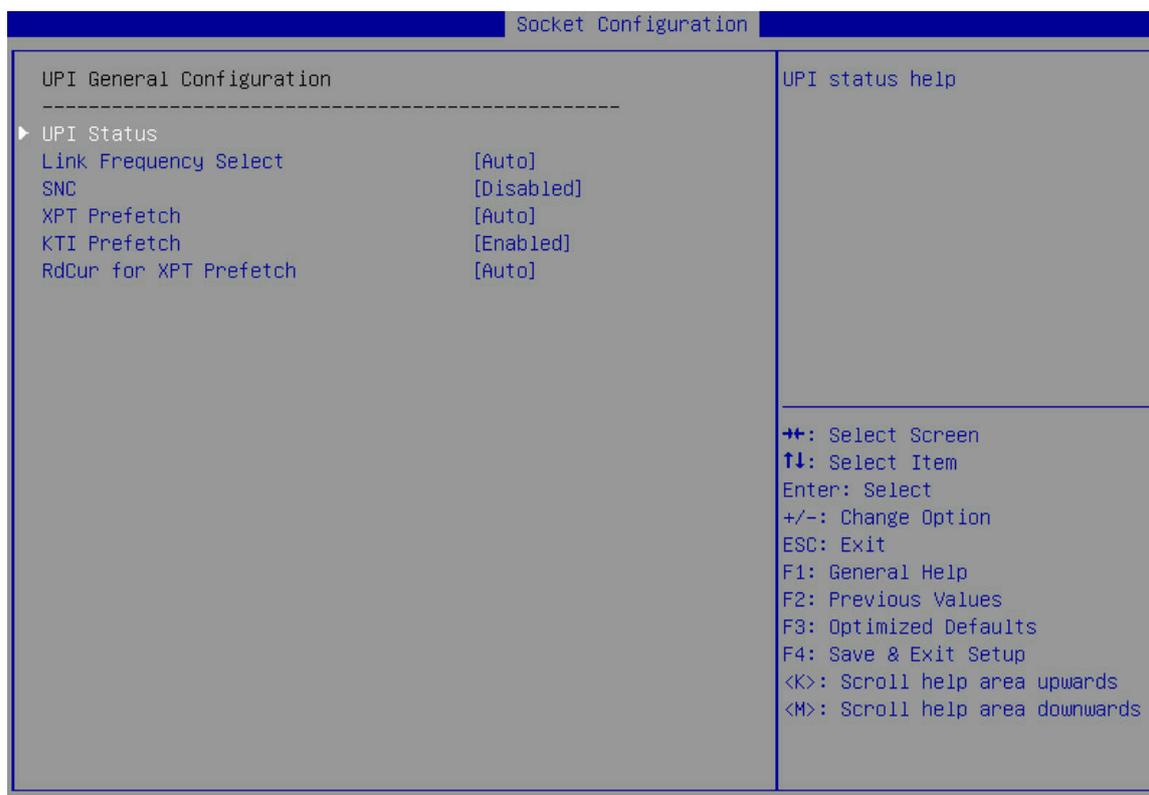


表3-83 UPI General Configuration 界面参数

界面参数	功能说明
UPI Status	显示UPI的状态信息。
Link Frequency Select	链路频率选择配置，菜单选项为： <ul style="list-style-type: none"> <li>• 9.6GT/s</li> <li>• 10.4GT/s</li> <li>• Auto（缺省）：自动选择UPI的链路频率。</li> </ul>
SNC	SNC功能配置，SNC（Sub NUMA Clustering）可改善LLC到内存的延迟。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启SNC功能。</li> <li>• Disabled（缺省）：关闭SNC功能。</li> <li>• Auto：自动选择SNC功能是否开启。</li> </ul>
XPT Prefetch	XPT预取。菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）：自动选择XPT预取功能是否开启。</li> <li>• Enabled：开启XPT预取。</li> <li>• Disabled：关闭XPT预取。</li> </ul>

界面参数	功能说明
KTI Prefetch	KTI预取。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 KTI 预取。</li> <li>Disabled: 关闭 KTI 预取。</li> </ul>
RdCur for XPT Prefetch	XPT 预取的 RdCur。菜单选项为： <ul style="list-style-type: none"> <li>Auto（缺省）：基于 Si 兼容性自动设定。</li> <li>Enabled: 设置 suppress_mem_rd_prefetch_rdcur。</li> <li>Disabled: 重设。</li> </ul>

## 2. UPI Status 界面

UPI Status界面如图 3-94所示。具体参数说明如表 3-84所示。

图3-94 UPI Status 界面

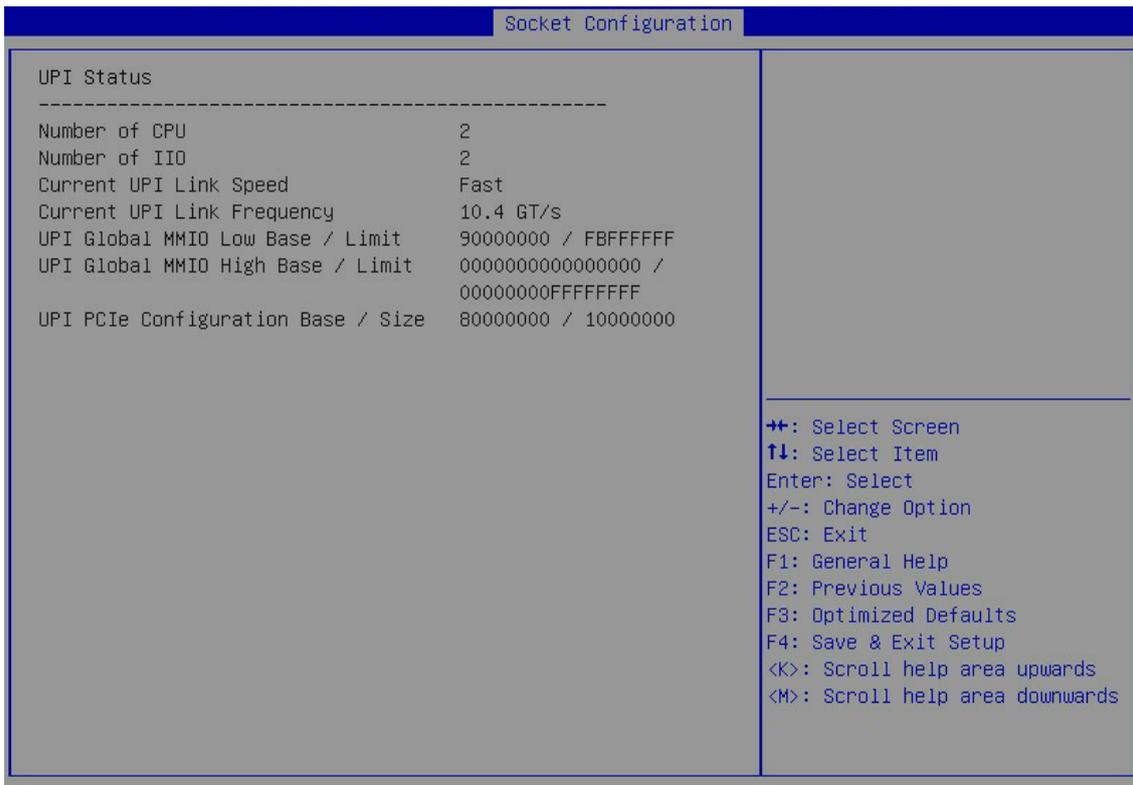


表3-84 UPI Status 界面参数

界面参数	功能说明
Number of CPU	显示CPU个数。
Number of IIO	显示IIO的数量。
Current UPI Link Speed	显示当前UPI链路速度。
Current UPI Link Frequency	显示当前UPI链路频率。

界面参数	功能说明
UPI Global MMIO Low Base/Limit	显示UPI全局MMIO低位基址/限制。
UPI Global MMIO High Base/Limit	显示UPI全局MMIO高位基址/限制。
UPI PCIe Configuration Base/Size	显示UPI Pci-e配置基址/大小。

### 3.4.4 Memory Configuration 界面

如图 3-95 所示，通过 Memory Configuration 界面，可以对内存进行配置，包括内存速率、内存的RAS特性等。具体参数说明如表 3-85 所示。

图3-95 Memory Configuration 界面

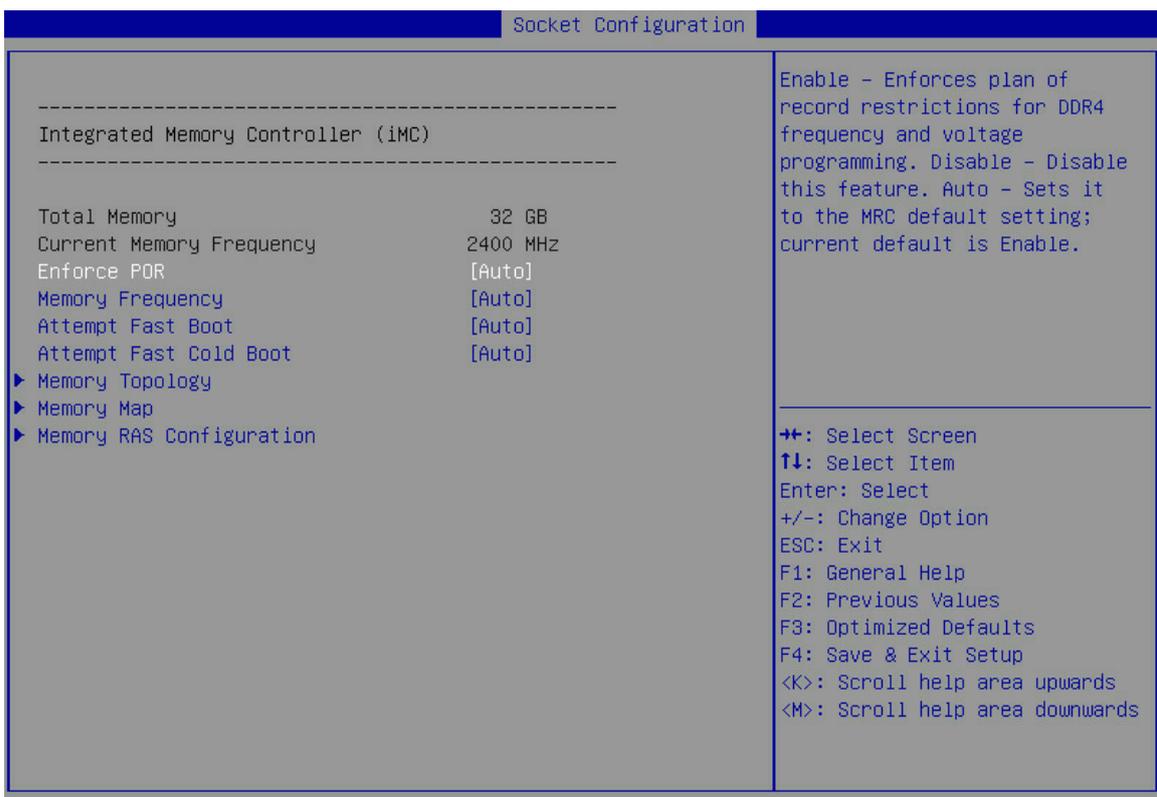


表3-85 Memory Configuration 界面参数

界面参数	功能说明
Total Memory	显示内存总容量。
Current Memory Frequency	显示内存当前运行频率。
Enforce POR	<p>POR设置，系统自动按照POR的规则对DDR4的频率进行设置，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto（缺省）：自动选择。</li> <li>• Enabled：开启POR，可以提升内存的稳定性。</li> <li>• Disabled：关闭POR。</li> </ul>

界面参数	功能说明
Memory Frequency	内存频率设置，单位为MHz。菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）</li> <li>• 1600</li> <li>• 1866</li> <li>• 2133</li> <li>• 2400</li> <li>• 2666</li> <li>• 2933（当使用 CascadeLake CPU 时，支持该内存频率选择）</li> </ul> 说明：使用 Intel DCPMM 内存时，支持的内存频率设置范围是 1866MHz 到 2666MHz。
Attempt Fast Boot	尝试快速启动。菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）：默认启用。</li> <li>• Enabled：当跳过内存引用代码的部分代码有可能加快热启动速度时，其将被跳过。</li> <li>• Disabled：禁用快速启动。</li> </ul>
Attempt Fast Cold Boot	尝试快速冷启动。菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）：默认启用。</li> <li>• Enabled：启用后，当跳过内存引用代码的部分代码有可能加快冷启动速度时，其将被跳过。</li> <li>• Disabled：禁用快速冷启动。</li> </ul>
Memory Topology	内存拓扑信息菜单。
Memory Map	内存映射配置菜单。
Memory RAS Configuration	内存RAS配置菜单。

### 1. Memory Topology 界面

Memory Topology界面如[图 3-96](#)所示。具体参数说明如[表 3-86](#)所示。

图3-96 Memory Topology 界面

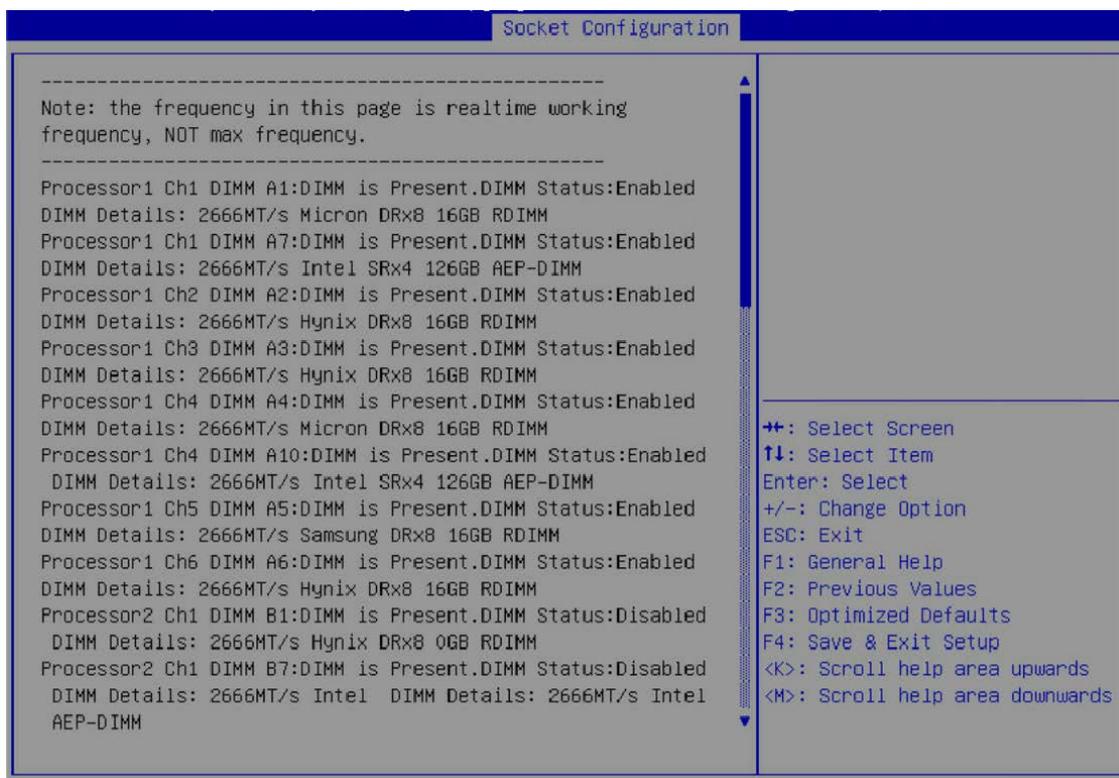


表3-86 Memory Topology 界面参数

界面参数	功能说明
Processor 1 Ch1 DIMM A1: DIMM is Present.DIMM Status:Enabled.DIMM Details:2666MT/s Micron DRx8 16GB RDIMM	表示Processor 1通道3 DIMM A3的内存信息: 在位情况和使能情况, 2666MT/s表示内存频率, Micron表示生产商, DRx8 中DR是RANK数量, x8是内存颗粒的位宽, 16GB表示内存容量, RDIMM表示内存类型。

## 2. Memory Map 界面

Memory Map界面如[图 3-97](#)所示。具体参数说明如[表 3-87](#)所示。

图3-97 Memory Map 界面

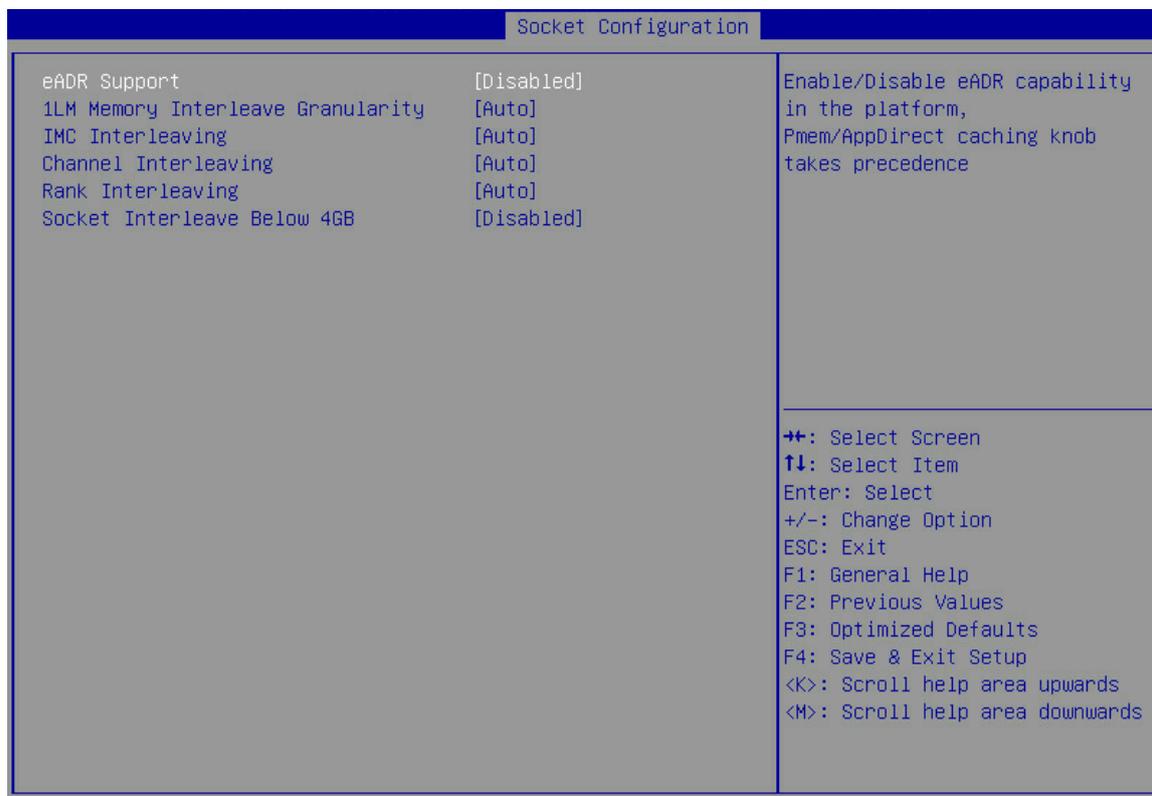


表3-87 Memory Map 界面参数

界面参数	功能说明
eADR Support	eADR功能支持。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 开启 eADR 支持。</li> <li>• Disabled (缺省): 关闭 eADR 支持。</li> </ul>
1LM Memory Interleave Granularity	1LM内存交织颗粒配置选项，菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 自动设置 1LM 内存交织颗粒配置大小的交织颗粒。</li> <li>• 256B Target,256B Channel: 设置 256B 大小的交织颗粒。</li> <li>• 64B Target,64B Channel: 设置 64B 大小的交织颗粒。</li> </ul>
IMC Interleaving	IMC交织设置，用于提升内存的读写性能。当NUMA选项（具体请参见 <a href="#">3.4.2 Common RefCode Configuration界面</a> ）关闭时，IMC Interleaving选项会被隐藏。菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 自动选择。</li> <li>• 1-way Interleave: 1 路交织设置。</li> <li>• 2-way Interleave: 2 路交织设置。</li> </ul>

界面参数	功能说明
Channel Interleaving	<p>Channel交织设置，通过此选项来修改内存通道所配置的交织级别。通常情况下，较高的内存交织级别可产生最高性能，但是降低交错级别可节省功耗。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto（缺省）：自动设置 Channel Interleaving。</li> <li>• 1-way Interleave：1 路交织设置。</li> <li>• 2-way Interleave：2 路交织设置。</li> <li>• 3-way Interleave：3 路交织设置。</li> </ul>
Rank Interleaving	<p>Rank交织设置，可以在指定通道的多Rank之间划分缓存线，用于提升内存的读写性能，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto（缺省）：自动选择。</li> <li>• 1-way Interleave：1 路交织设置。</li> <li>• 2-way Interleave：2 路交织设置。</li> <li>• 4-way Interleave：4 路交织设置。</li> <li>• 8-way Interleave：8 路交织设置。</li> </ul>
Socket Interleave Below 4GB	<p>4GB以下内存交织设置，用于提升内存的读写性能。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：开启 4GB 以下内存交织功能。</li> <li>• Disabled（缺省）：关闭 4GB 以下内存交织功能。</li> </ul>

### 3. Memory RAS Configuration 界面

Memory RAS Configuration界面如[图 3-98](#)所示。具体参数说明如[表 3-88](#)所示。

图3-98 Memory RAS Configuration 界面

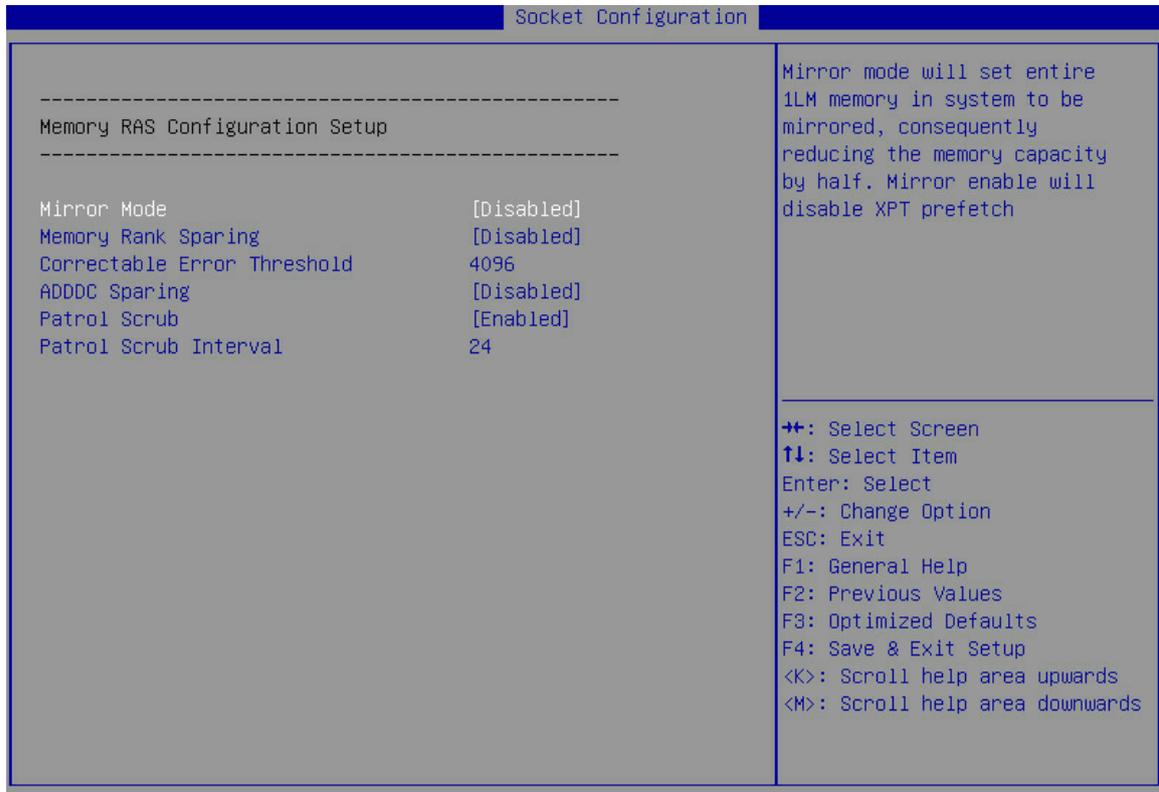


表3-88 Memory RAS Configuration 界面参数

界面参数	功能说明
Mirror Mode	<p>Mirror Mode设置，Mirror Mode将设置系统中所有1LM内存被镜像,因而减少一半内存容量，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用内存 Mirror Mode。</li> <li>• Enable Mirror Mode 1LM：使用 1LM Mirror Mode。当启用镜像模式时，Memory Rank Sparing、ADDDC Sparing 均选项不可配置。</li> </ul> <p>在通过Mirror Mode设置内存镜像的情况下，在Total Memory Size查看到的是可用的总内存容量的大小。在shell或linux等操作系统中通过命令行查看到Smbios Type 17字段，显示的是物理内存大小。</p> <p>需要注意的是：由于硬件上的限制，一段地址空间要在Socket/IMC/Channel/Rank之间平分，因此内存满配时，在镜像模式下，POST自检界面和BIOS Setup界面中，显示的内存容量大于实际安装的内存总容量的一半。</p>

界面参数	功能说明
Memory Rank Sparing	<p>Memory Rank Sparing设置，开启该功能后，使用通道中的一部分Rank作为该通道中其他Rank（非备用Rank）的备用Rank，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启内存 Rank 备用功能。</li> <li>Disabled（缺省）：关闭内存 Rank 备用功能。</li> </ul> <p>需要注意的是：</p> <ul style="list-style-type: none"> <li>系统不支持将内存模式同时设置为 Mirror Mode 和 Memory Rank Sparing。</li> <li>当您将 RAS 模式设置为 Independent Mode 后，如果启用 Memory Rank Sparing，此时 Independent Mode、Memory Rank Sparing 会同时生效。</li> </ul>
Multi Rank Sparing	<p>备用Rank的数量设置，仅当Memory Rank Sparing设置为Enabled时，才会出现该选项，菜单选项为：</p> <ul style="list-style-type: none"> <li>One Rank: 选择 1Rank 作为备用，要求通道中 Rank 数量大于等于 2。</li> <li>Two Rank(缺省): 选择 2Rank 作为备用，要求通道中 Rank 数量大于等于 4。</li> </ul>
Correctable Error Threshold	<p>显示可修正错误阈值，取值范围0~32767(十进制)，缺省值为4096，0表示没有阈值。</p>
Leaky bucket low bit	<p>漏桶低位，当Memory Rank Sparing设置为Enabled时显示，缺省值为10（十六进制），取值范围0~3F。</p>
Leaky bucket high bit	<p>漏桶高位，当Memory Rank Sparing设置为Enabled时显示，缺省值为11（十六进制），取值范围0~29。</p>
ADDDC Sparing	<p>自适应双设备数据校正备用设置（Adaptive Double Device Data Correction Sparing），可纠正两个内存颗粒上的数据错误，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 启用 ADDC 备用功能。</li> <li>Disabled（缺省）：禁用 ADDC 备用功能。</li> </ul>
Enable ADDDC Error Injection	<p>ADDDC故障注入功能，当ADDDC Sparing设置为Enabled时显示。</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：启动 ADDDC 故障注入功能。</li> <li>Disabled: 禁用 ADDDC 故障注入功能。</li> </ul>
Patrol Scrub	<p>内存巡检设置，CPU主动对内存的数据进行周期性的巡检并纠正可纠正的内存错误，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 Patrol Scrub 功能。</li> <li>Disabled: 关闭 Patrol Scrub 功能。</li> </ul>
Patrol Scrub Interval	<p>设置内存巡检的时间间隔，缺省值为24小时。当Patrol Scrub选项设置为Enable后显示该选项，用户可以修改该间隔。</p>

### 3.4.5 IIO Configuration 界面

通过 IIO Configuration 界面，可以对 PCIe 插槽进行配置，包括 PCIe 端口链路速率、PCIe 端口最大负载等。

I/O Configuration界面选项与安装的处理器个数有关，如[图 3-99](#)和[图 3-100](#)所示。具体参数说明如[表 3-89](#)所示。

图3-99 I/O Configuration 界面 1

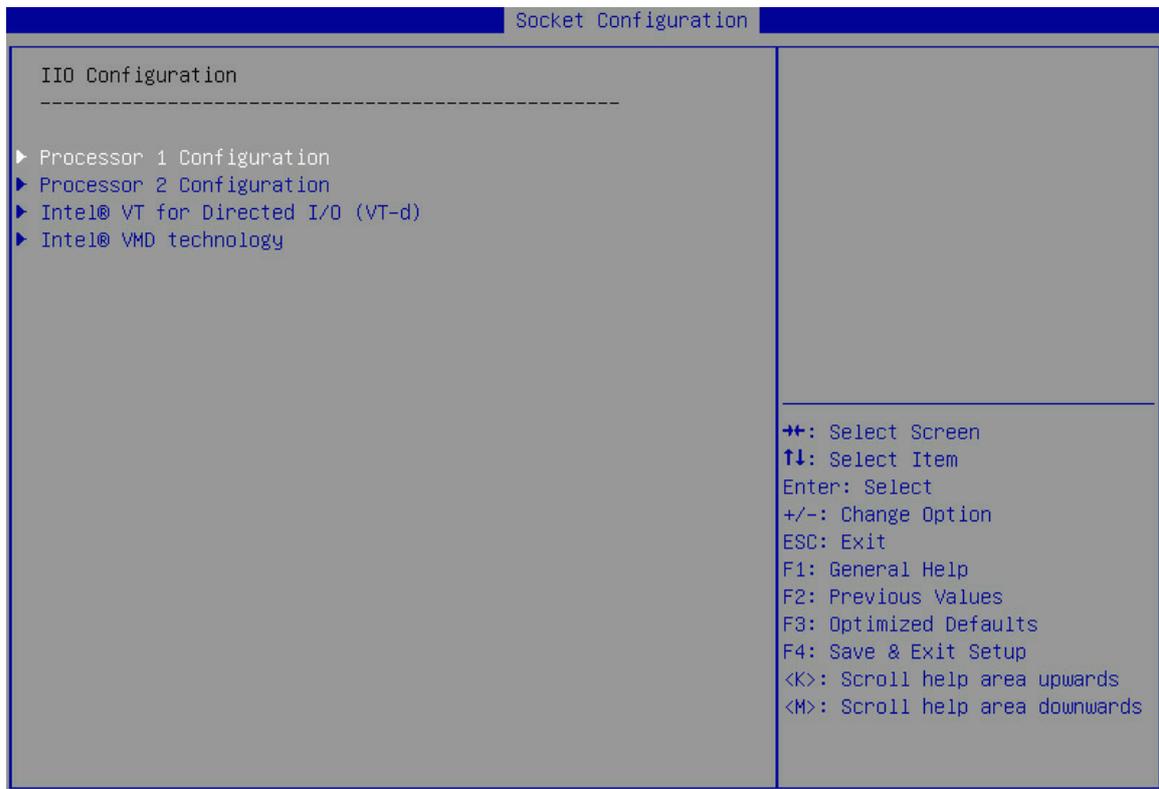


图3-100 IIO Configuration 界面 2

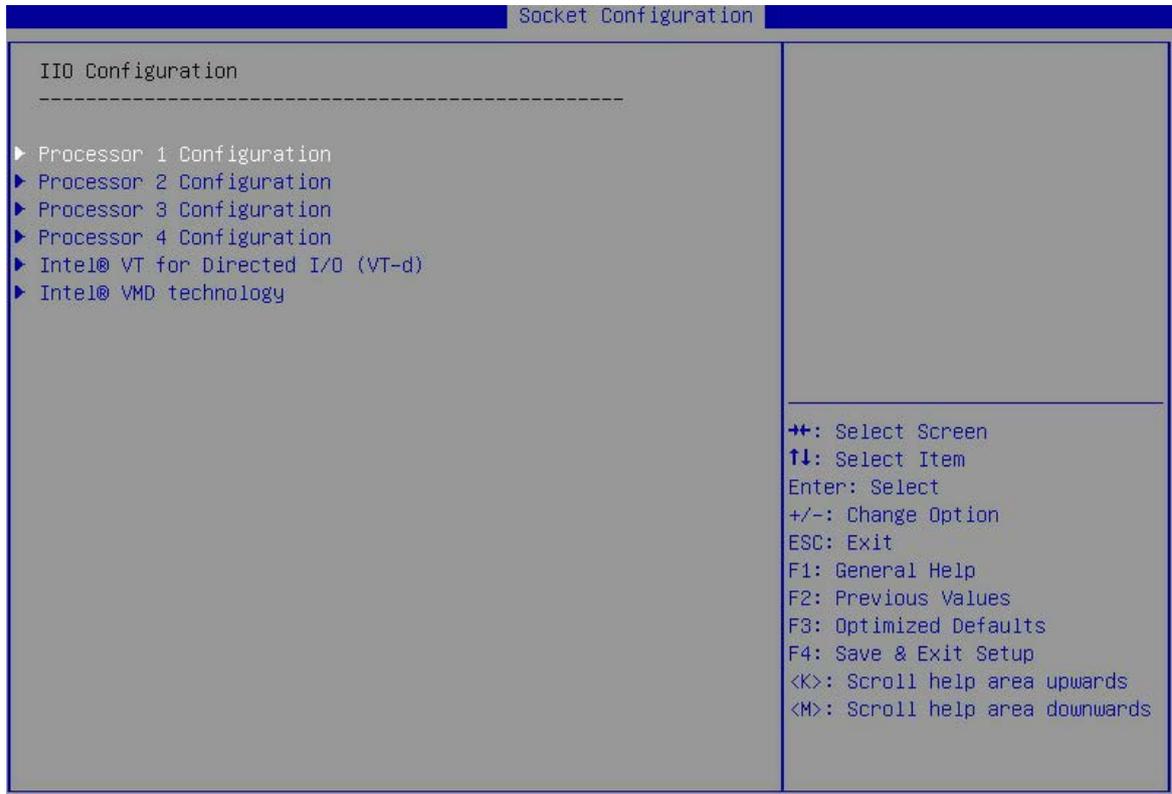


表3-89 IIO Configuration 界面参数

界面参数	功能说明
Processor X Configuration	处理器X的IIO配置菜单。当处理器在位时显示该选项。
Intel® VT for Directed I/O (VT-d)	英特尔®VT-d配置菜单。
Intel VMD technology	英特尔®VMD卷管理设备配置菜单。

### 1. Processor Configuration 界面



说明

Processor Configuration 界面内选项会根据服务器型号的不同而产生差异，另外也会根据安装的 PCIe Riser 卡不同有所变化，下面仅以一个 Processor 1 Configuration 的界面为例进行说明。

Processor 1 Configuration 界面如[图 3-101](#)所示，具体参数说明如[表 3-90](#)所示。

图3-101 Processor 1 Configuration 界面

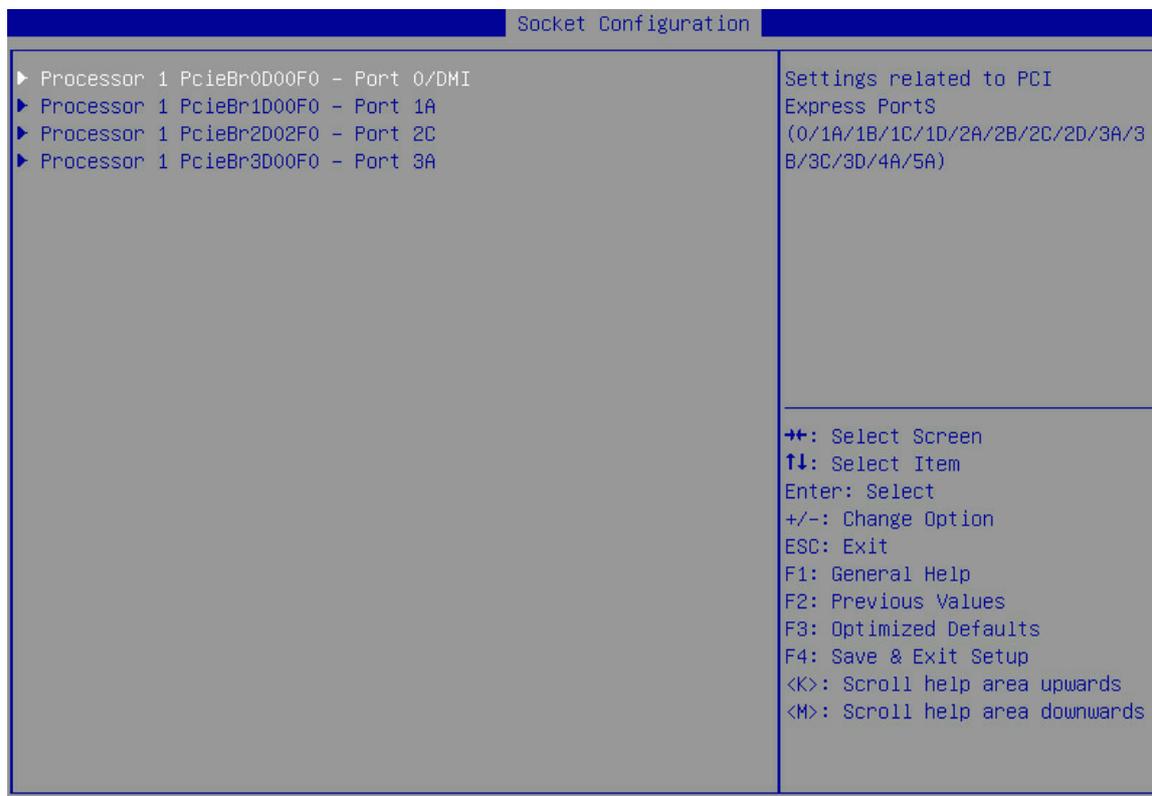


表3-90 Processor 1 Configuration 界面参数

界面参数	功能说明
Processor 1 PcieBr0D00F0 - Port 0/DMI	处理器1 PcieBr0D00F0-端口0/DMI配置菜单。
Processor 1 PcieBr1D00F0 - Port 1A	Processor 1 PcieBr1D00F0 - Port 1A配置菜单。
Processor 1 PcieBr2D02F0 - Port 2C	Processor 1 PcieBr2D02F0 - Port 2C配置菜单。
Processor 1 PcieBr3D00F0 - Port 3A	Processor 1 PcieBr3D00F0 - Port 3A配置菜单。

每个 Processor Pcie端口配置界面内部参数基本相同，下面以Processor 1 PcieBr1D00F0 - Port 1A 为例。如[图 3-102](#)，具体参数说明如[表 3-91](#)所示。

图3-102 Processor 1 PcieBr1D00F0 - Port 1A 界面

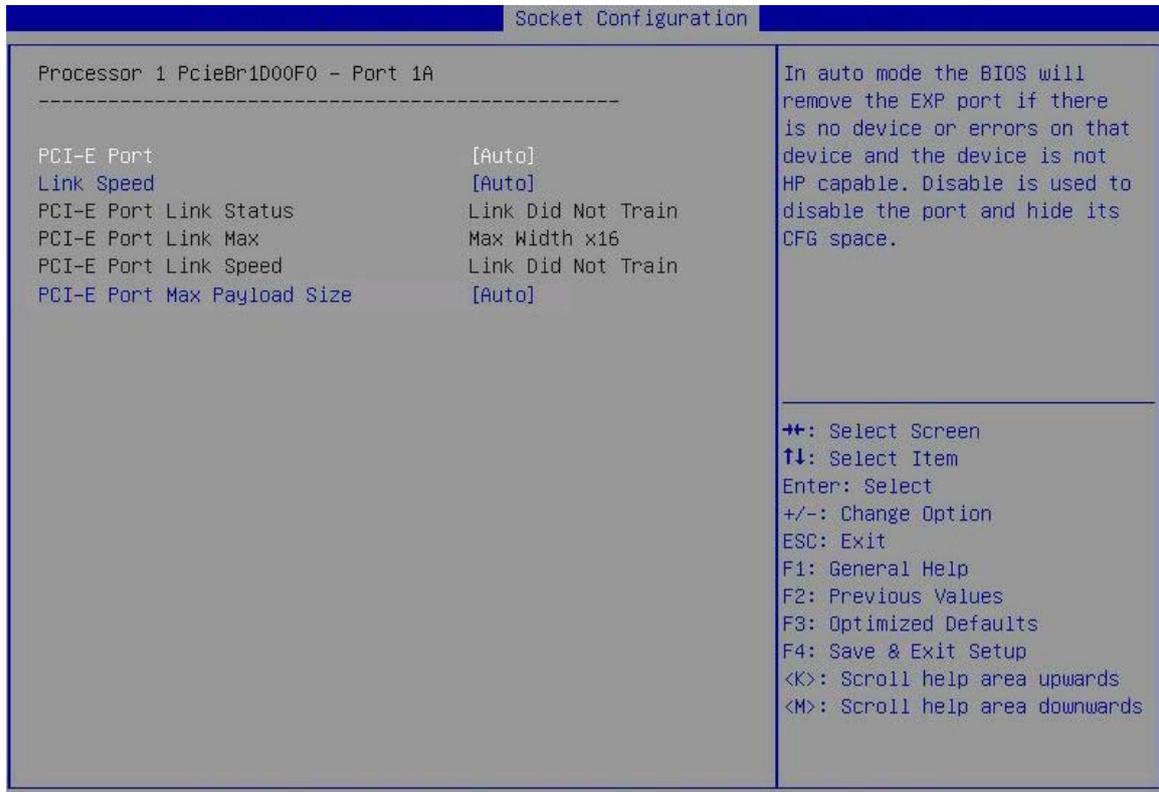


表3-91 Processor 1 PcieBr1D00F0 - Port 1A 界面参数

界面参数	功能说明
PCI-E Port	PCI-E端口开关（DMI端口没有该选项）。菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）：自动选择。</li> <li>• Enabled：开启 PCI-E 端口。</li> <li>• Disabled：关闭 PCI-E 端口，用于关闭端口和隐藏配置空间。</li> </ul>
Link Speed	链路速度配置，菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）</li> <li>• Gen 1（2.5 GT/s）</li> <li>• Gen 2（5 GT/s）</li> <li>• Gen 3（8 GT/s）</li> </ul>
PCI-E Port Link Status	显示PCI-E端口链路状况信息。
PCI-E Port Link Max	显示PCI-E端口链路最大带宽信息。
PCI-E Port Link Speed	显示PCI-E端口链路速度信息。

界面参数	功能说明
PCI-E Port Max Payload Size	设置PCIe端口的最大有效负载。菜单选项为： <ul style="list-style-type: none"> <li>• Auto（缺省）：默认为 256B。</li> <li>• 128B：设置 PCIe 端口的最大有效负载为 128B，可能会影响 NVMe 硬盘的性能。在低版本操作系统下，进行 NVMe 热插拔出现重启现象时，可尝试切换到此选项。</li> <li>• 256B：设置 PCIe 端口的最大有效负载为 256B。</li> </ul>

## 2. Intel VT for Directed I/O（VT-d）界面

Intel VT for Directed I/O（VT-d）界面如[图 3-103](#)所示。具体参数说明如[表 3-92](#)所示。

图3-103 Intel VT for Directed I/O（VT-d）界面

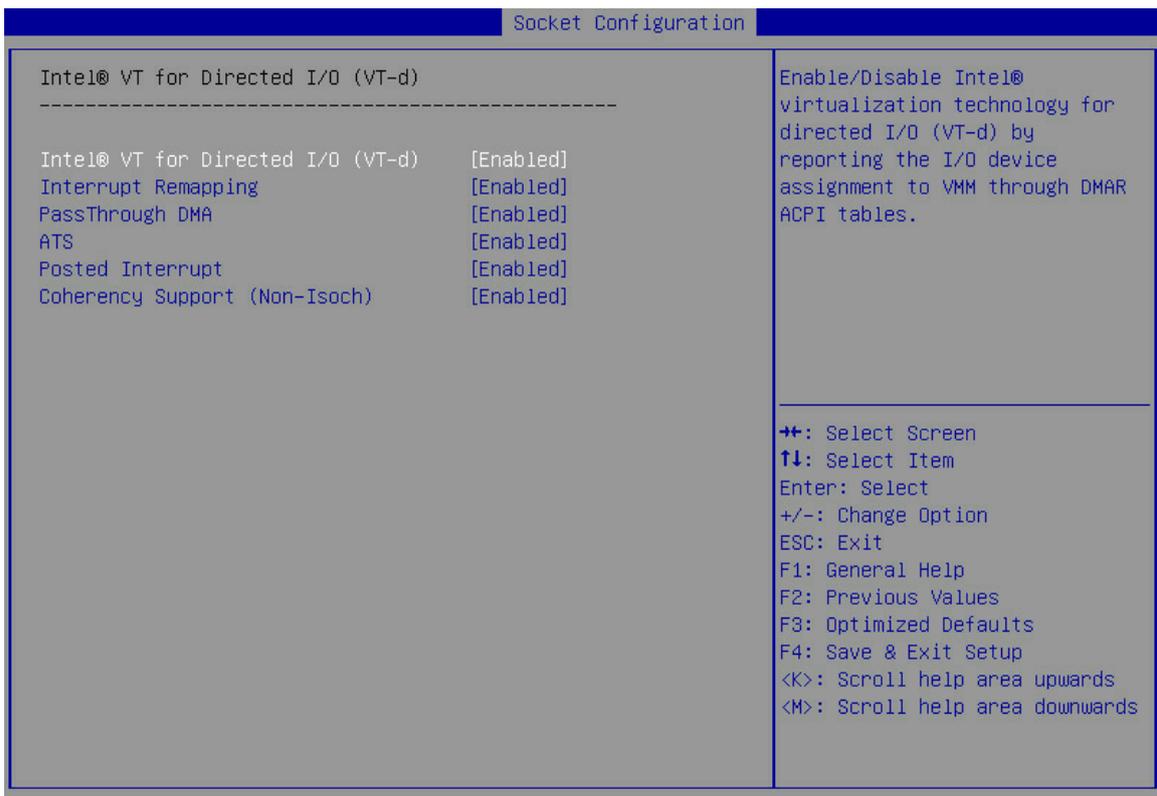


表3-92 Intel VT for Directed I/O（VT-d）界面参数

界面参数	功能说明
Intel VT for Directed I/O（VT-d）	Intel VT-d开关，启用后，支持此选项的管理程序和操作系统能够为定向I/O使用Intel虚拟化技术提供的硬件功能。用于提高系统的安全性和可靠性，并改善I/O设备在虚拟化环境中的性能，即使不使用应用此选项的管理程序和操作系统，也可以保持启用此选项。
Interrupt Remapping	VT-d中断重映射支持设置。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 Intel VT-d 中断映射功能。</li> <li>• Disabled：关闭 Intel VT-d 中断映射功能。</li> </ul>

界面参数	功能说明
PassThrough DMA	PassThrough DMA支持设置。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 PassThrough DMA 功能。</li> <li>Disabled: 关闭 PassThrough DMA 功能。</li> </ul>
ATS	非Isoch VT-d引擎ATS支持。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 Intel VT-d 功能。</li> <li>Disabled: 关闭 Intel VT-d 功能。</li> </ul>
Posted Interrupt	设置VT-d Posted中断。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启 VT-d Posted 中断功能。</li> <li>Disabled: 关闭 VT-d Posted 中断功能。</li> </ul>
Coherency Support(Non-Isoch)	非Isoch的一致性支持。菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：开启非 Isoch 的一致性功能。</li> <li>Disabled: 关闭非 Isoch 的一致性功能。</li> </ul>

### 3. Intel® VMD technology 界面

Intel® VMD technology界面如图 3-104所示，该界面配置VMD功能的菜单选项数量与处理器数量对应。具体参数说明如表 3-93所示。

图3-104 Intel® VMD technology 界面

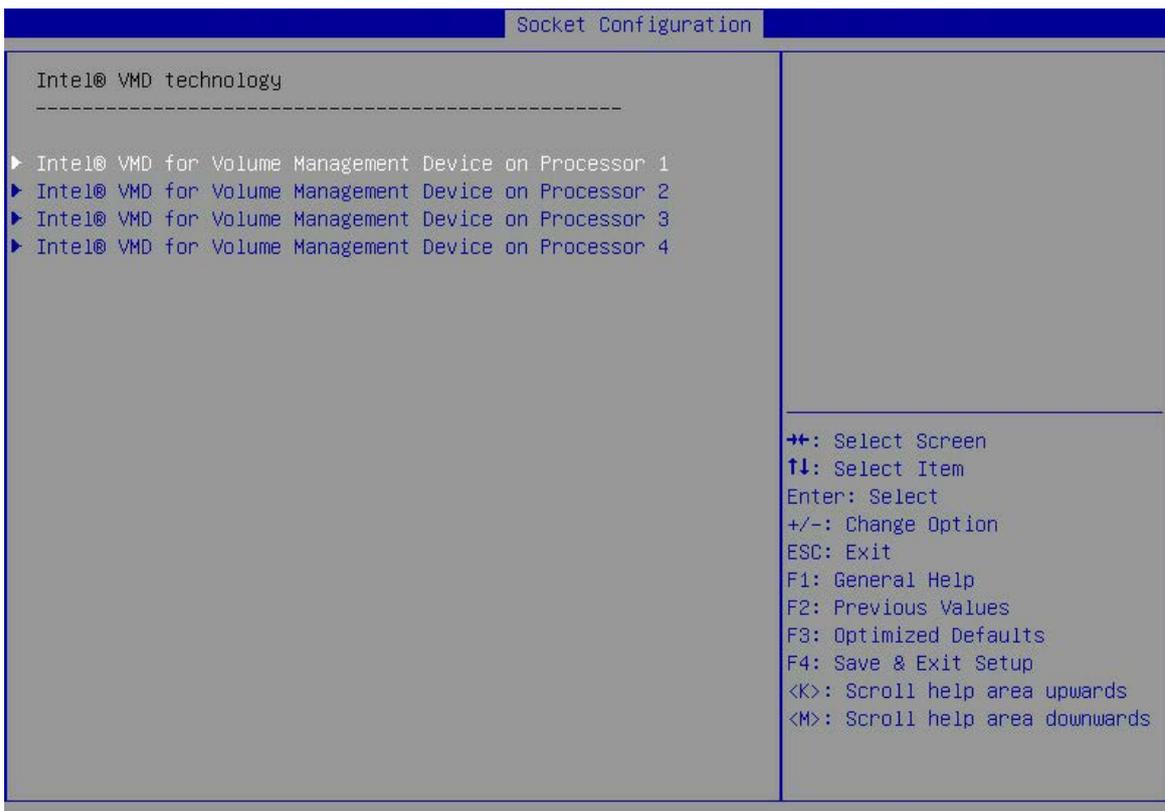


表3-93 Intel® VMD technology 界面参数

界面参数	功能说明
Intel® VMD for Volume Management Device on Processor X	处理器X的英特尔®VMD卷管理设备配置菜单。当处理器在位时显示该选项。

每个处理器的Intel® VMD for Volume Management Device on Processor界面内参数均相同，下面以Processor 1 界面为例，如图 3-105所示。具体参数说明如表 3-94所示。

图3-105 Intel® VMD for Volume Management Device on Processor 1 界面

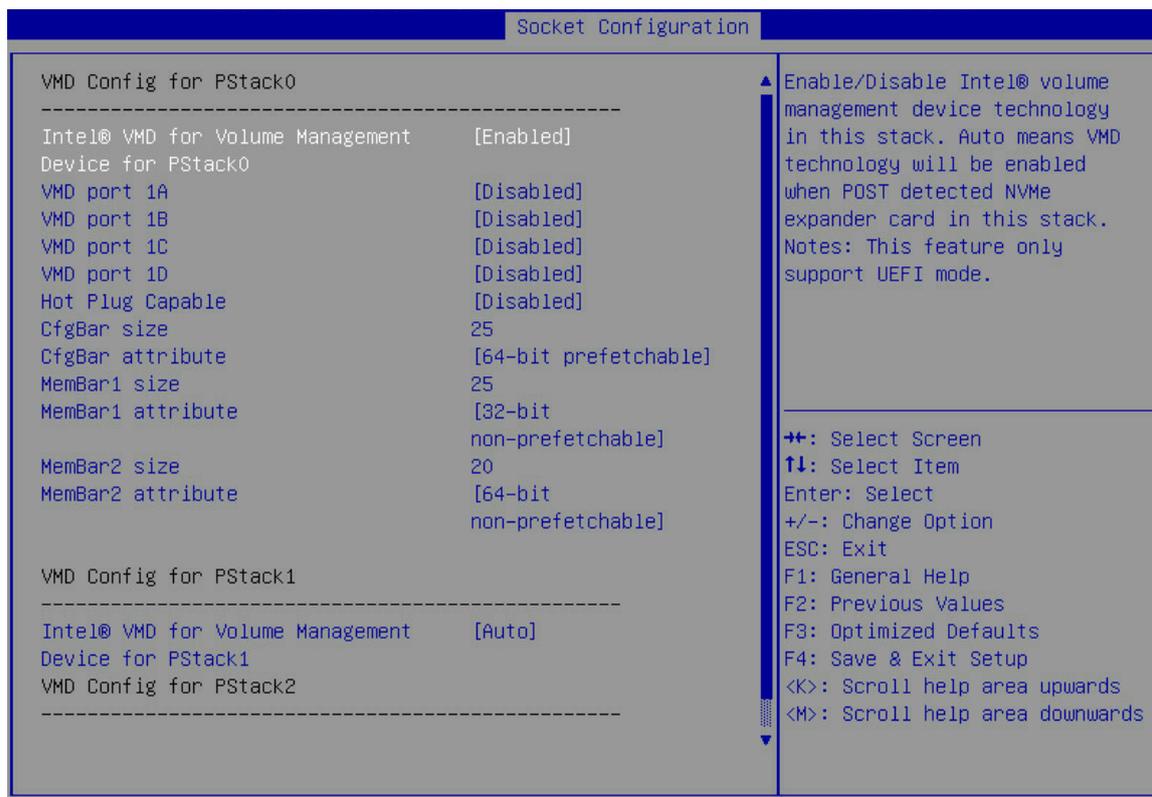


表3-94 Intel® VMD for Volume Management Device on Processor 1 界面参数

界面参数	功能说明
Intel® VMD for Volume Management Device for PStack0	<p>PStack0中的英特尔®VMD卷管理设备配置菜单，此功能在LEGACY模式下不支持，仅支持UEFI模式，菜单选项为：</p> <ul style="list-style-type: none"> <li>Disabled: 禁用此 PStack0 中英特尔®卷管理设备技术。</li> <li>Enabled: 启用 PStack0 上的 VMD 技术。当选择此项时，显示更加细致的配置选项。</li> <li>Auto (缺省): 自动表示当 POST 阶段检测到此栈上有 NVMe 扩展卡接入时,将自动启用 VMD 技术。</li> </ul>
VMD port 1A	<p>VMD端口1A配置选项。当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>Disabled (缺省): 禁用 VMD 端口 1A。</li> <li>Enabled: 启用 VMD 端口 1A。</li> </ul>

界面参数	功能说明
VMD port 1B	<p>VMD端口1B配置选项。当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用 VMD 端口 1B。</li> <li>• Enabled：启用 VMD 端口 1B。</li> </ul>
VMD port 1C	<p>VMD端口1C配置选项。当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用 VMD 端口 1C。</li> <li>• Enabled：启用 VMD 端口 1C。</li> </ul>
VMD port 1D	<p>VMD端口1D配置选项。当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用 VMD 端口 1D。</li> <li>• Enabled：启用 VMD 端口 1D。</li> </ul>
Hot Plug Capable	<p>热插拔功能配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用对应的 PCIe Root Port 热插拔功能。</li> <li>• Enabled：启用对应的 PCIe Root Port 热插拔功能。</li> </ul> <p>当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>
CfgBar Size	<p>设置VMD配置BAR大小(以bits表示,最小=20,最大=27)，默认为25。 当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>
CfgBar attribute	<p>设置VMD配置BAR属性。默认为64-bit prefetchable。 当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>
MemBar1 size	<p>内存Bar1大小。默认为25。 当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>
MemBar1 attribute	<p>设置VMD内存BAR1属性。菜单选项为：</p> <ul style="list-style-type: none"> <li>• 32-bit non-prefetchable（缺省）</li> <li>• 64-bit non-prefetchable</li> <li>• 64-bit prefetchable</li> </ul> <p>当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>
MemBar2 size	<p>内存Bar2大小。默认为20 当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>
MemBar2 attribute	<p>设置VMD内存BAR2属性。菜单选项为</p> <ul style="list-style-type: none"> <li>• 64-bit non-prefetchable（缺省）</li> <li>• 64-bit prefetchable</li> </ul> <p>当对应的Intel® VMD for Volume Management Device for PStack设置为Enabled时显示。</p>

界面参数	功能说明
Intel® VMD for Volume Management Device for PStack1	<p>PStack1中的英特尔®VMD卷管理设备配置菜单,此功能在LEGACY模式下不支持,仅支持UEFI模式,菜单选项为:</p> <ul style="list-style-type: none"> <li>Disabled: 禁用此 PStack1 中英特尔®卷管理设备技术。</li> <li>Enabled: 启用 PStack1 上的 VMD 技术。当选择此项时,显示更加细致的配置选项。</li> <li>Auto (缺省): 自动表示当 POST 检测到此栈上有 NVMe 扩展卡接入时,将自动启用 VMD 技术。</li> </ul>
Intel® VMD for Volume Management Device for PStack2	<p>PStack2中的英特尔®VMD卷管理设备配置菜单,此功能在LEGACY模式下不支持,仅支持UEFI模式,菜单选项为:</p> <ul style="list-style-type: none"> <li>Disabled: 禁用此 PStack2 中英特尔®卷管理设备技术。</li> <li>Enabled: 启用 PStack2 上的 VMD 技术。当选择此项时,显示更加细致的配置选项。</li> <li>Auto (缺省): 自动表示当 POST 检测到此栈上有 NVMe 扩展卡接入时,将自动启用 VMD 技术。</li> </ul>

#### 4. VMD 选项与 NVMe 设备的对应关系

服务器可以根据NVMe设备逻辑槽位号判断对应控制的VMD选项,可查看[表 3-95](#)。



注意

除下表中对应 NVMe 的 VMD 选项,其余 VMD Port 是支持 PCIe 标准设备的。不建议修改不对应 NVMe 的 VMD 选项,会导致 PCIe 槽位上接入的设备无法识别。

表3-95 NVMe 逻辑槽位号与 VMD 开关对应关系

NVMe 逻辑槽位号	VMD 选项		
<b>UNISINSIGHT AIX R6220L-G3 (12LFF硬盘机型)</b>			
Slot 200	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3A
Slot 201	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3B
Slot 202	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3C
Slot 203	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3D
<b>UNISINSIGHT AIX R6220L-G3 (24LFF硬盘机型)</b>			
Slot 200	Intel® VMD for Volume Management Device on Processor 1	Intel® VMD for Volume Management Device for PStack2	VMD port 3A

NVMe 逻辑槽位号	VMD 选项		
Slot 201	Intel® VMD for Volume Management Device on Processor 1	Intel® VMD for Volume Management Device for PStack2	VMD port 3B
Slot 202	Intel® VMD for Volume Management Device on Processor 1	Intel® VMD for Volume Management Device for PStack2	VMD port 3C
Slot 203	Intel® VMD for Volume Management Device on Processor 1	Intel® VMD for Volume Management Device for PStack2	VMD port 3D
Slot 204	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3A
Slot 205	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3B
Slot 206	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3C
Slot 207	Intel® VMD for Volume Management Device on Processor 2	Intel® VMD for Volume Management Device for PStack2	VMD port 3D

### 3.4.6 Advanced Power Management Configuration 界面

如[图 3-106](#)所示，通过Advanced Power Management Configuration界面，可以对CPU的电源管理进行高级配置，包括电源策略、CPU P状态、CPU C状态等。具体参数说明如[表 3-96](#)所示。

图3-106 Advanced Power Management Configuration 界面

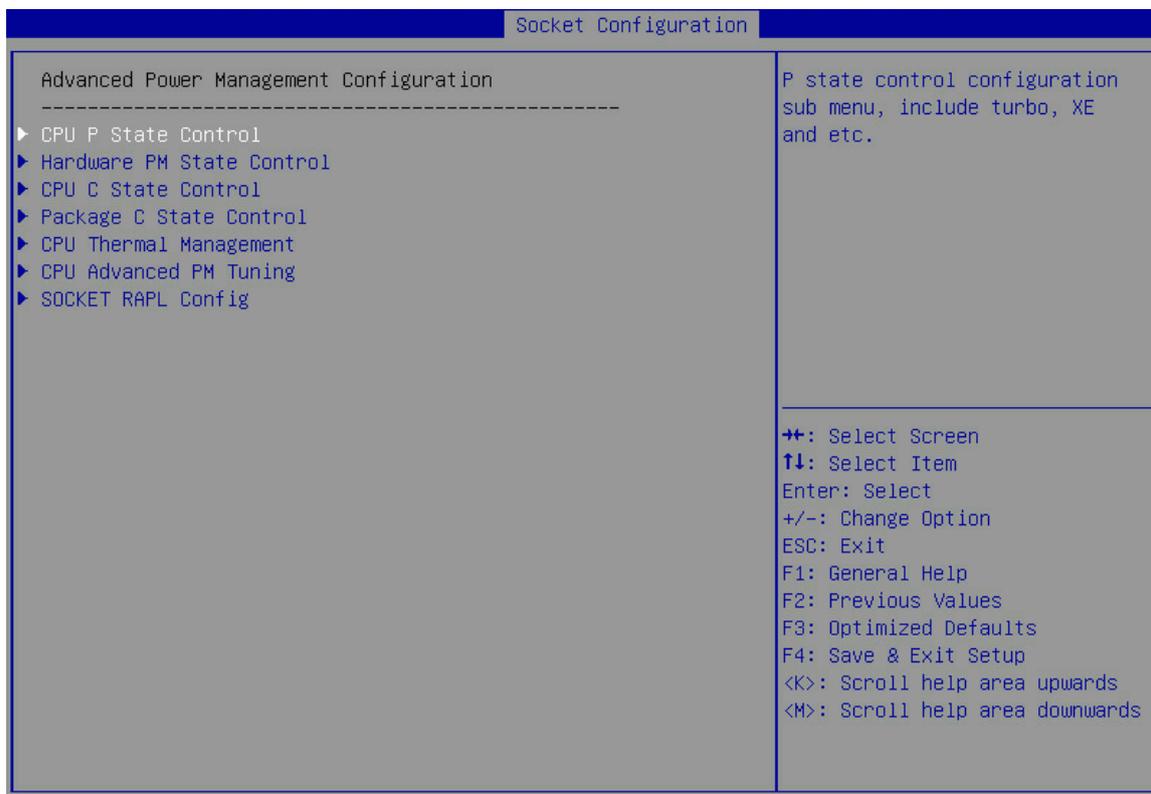


表3-96 Advanced Power Management Configuration 界面参数

界面参数	功能说明
CPU P State Control	CPU P状态控制配置菜单，用来控制CPU的频率。
Hardware PM State Control	硬件PM状态控制菜单。
CPU C State Control	CPU C状态控制配置菜单，用来控制CPU在空闲状态下的电源消耗，该配置菜单可用。
Package C State Control	Package C状态控制配置菜单,包括C2状态至C3状态转换计时器设置。
CPU Thermal Management	CPU热管理配置菜单，其中可以用以控制CPU T状态配置。
CPU Advanced PM Tuning	CPU Advanced PM调整菜单。
SOCKET RAPL Config	CPU RAPL配置菜单。

### 1. CPU P State Control 界面

CPU P State Control界面如[图 3-107](#)所示。具体参数说明如[表 3-97](#)所示。

图3-107 CPU P State Control 界面

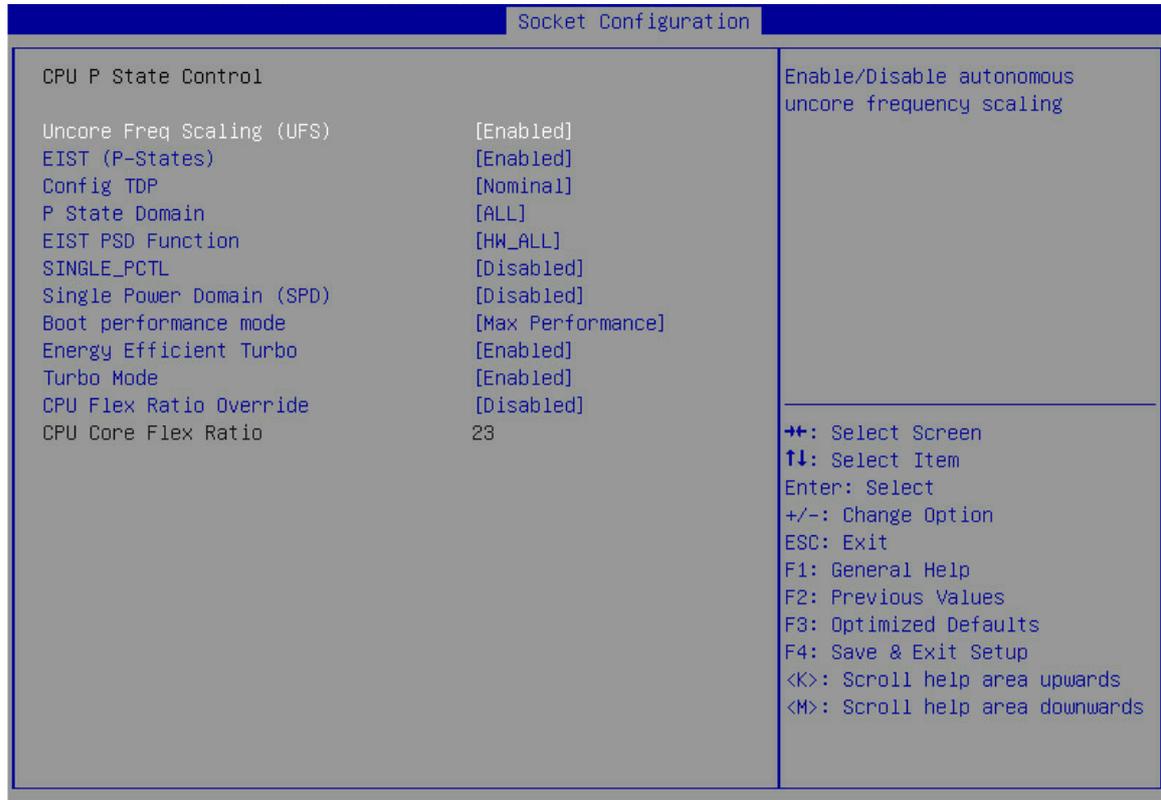


表3-97 CPU P State Control 界面参数

界面参数	功能说明
Uncore Freq Scaling (UFS)	<p>Uncore 频率缩放 (UFS)。菜单选项为:</p> <ul style="list-style-type: none"> <li>Enabled (缺省): 开启 Uncore 频率缩放功能。</li> <li>Disabled: 关闭 Uncore 频率缩放功能。</li> </ul>
EIST (P-States)	<p>EIST开关, 开启该功能后, 当系统处于空闲状态时, 自动降低CPU的频率, 菜单选项为:</p> <ul style="list-style-type: none"> <li>Enabled (缺省): 开启 EIST 功能。</li> <li>Disabled: 关闭 EIST 功能。</li> </ul>
Config TDP	<p>配置TDP等级。TDP (Thermal Design Power) 指的是冷却系统需要消耗的最大功率量。当EIST (P-States) 选项设置为Enabled时, 显示该选项。菜单选项为:</p> <ul style="list-style-type: none"> <li>Nominal (缺省): 标准模式, 默认的 TDP 等级。</li> <li>Level1: 支持配置的 TDP 等级一。</li> <li>Level2: 支持配置的 TDP 等级二。</li> </ul>
P State Domain	<p>P状态域设置, 菜单选项为:</p> <ul style="list-style-type: none"> <li>ALL (缺省): P 状态域设置成 ALL 模式。</li> <li>ONE: P 状态域设置成 ONE 模式。</li> </ul>

界面参数	功能说明
EIST PSD Function	选择EIST功能调节CPU频率和电压的途径，自动降低CPU的频率，菜单选项为： <ul style="list-style-type: none"> <li>• HW_ALL（缺省）：通过所有硬件协调。</li> <li>• SW_ALL：所有软件协调。</li> <li>• SW_ANY：任意软件协调。</li> </ul>
SINGLE_PCTL	SINGLE_PCTL模式开关。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled（缺省）：开启 SINGLE_PCTL 模式。</li> <li>• Enabled：关闭 SINGLE_PCTL 模式。</li> </ul>
Single Power Domain（SPD）	SPD设置项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled（缺省）：开启 SPD 设置。</li> <li>• Enabled：关闭 SPD 设置。</li> </ul>
Boot performance mode	启动性能模式，选择BIOS进入OS前将设置的性能状态。 <ul style="list-style-type: none"> <li>• Max Performance（缺省）：最大性能模式。</li> <li>• Max Efficient：最大效率模式。</li> <li>• Set by Intel Node Manager：由英特尔节点管理器设置。</li> </ul>
Energy Efficient Turbo	节能Turbo。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启节能 Turbo 模式。</li> <li>• Disabled：关闭节能 Turbo 模式。</li> </ul>
Turbo Mode	Turbo模式开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 Turbo 模式。</li> <li>• Disabled：关闭 Turbo 模式。</li> </ul>
CPU Flex Ratio Override	CPU动态倍频。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：允许重写 CPU 频率。选择该选项时，CPU 核频率可以被修改。</li> <li>• Disabled（缺省）：关闭重写 CPU 频率。</li> </ul>
CPU Core Flex Ratio	CPU核心动态倍频。当CPU Flex Ratio Override配置为enable时，该选项可以修改，默认为23。

## 2. Hardware PM State Control 界面

Hardware PM State Control界面如[图 3-108](#)所示。具体参数说明如[表 3-98](#)所示。

图3-108 Hardware PM State Control 界面

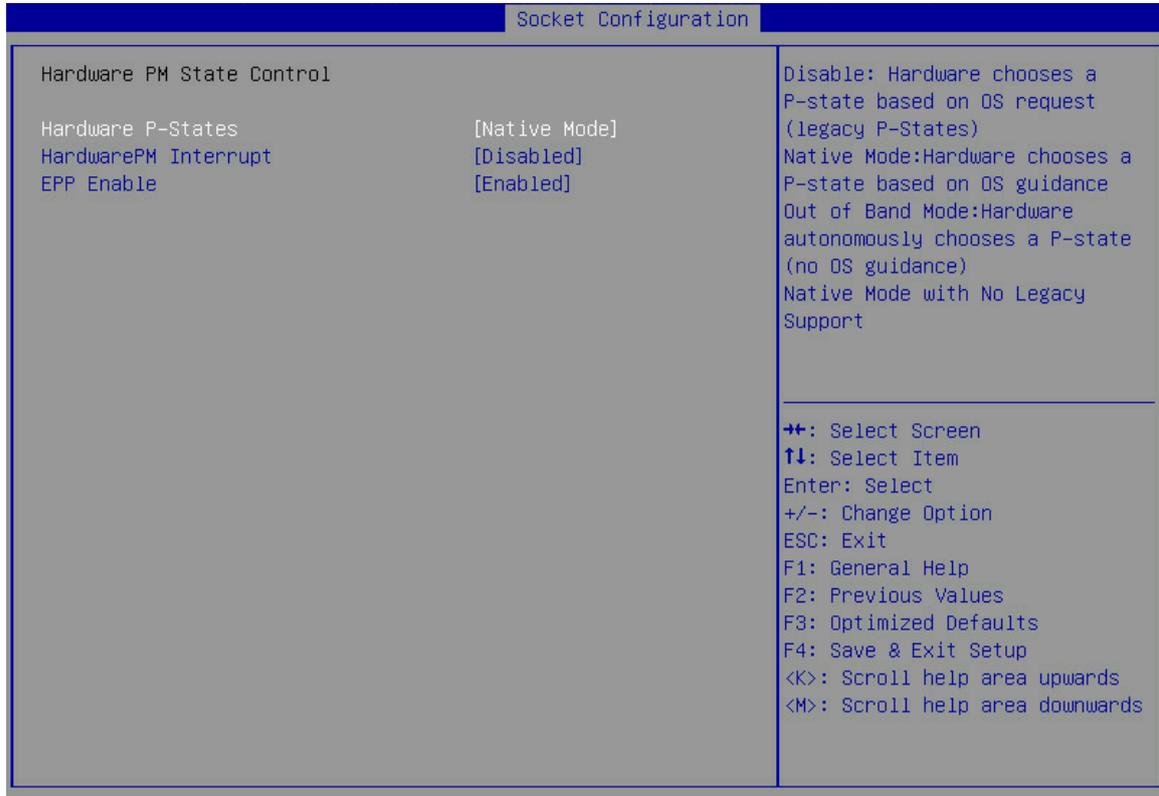


表3-98 Hardware PM State Control 界面参数

界面参数	功能说明
Hardware P-States	<p>硬件P状态。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled: 基于 OS 请求的硬件选择 P 状态。</li> <li>• Native Mode (缺省)：硬件基于 OS 的引导选择 P 状态。</li> <li>• Out of Band Mode: 硬件自动选择 (不需 OS 引导)。</li> <li>• Native Mode with No Legacy Support: 不支持 Legacy 的本地模式。</li> </ul>
HardwarePM Interrupt	<ul style="list-style-type: none"> <li>• 硬件 PM 中断。当 Hardware P-States 选项为 Native Mode 时，该选项可配置。菜单选项为：</li> <li>• Disabled (缺省)：禁用 PM 中断。</li> <li>• Enabled: 启动 PM 中断。</li> </ul>
EPP Enable	<ul style="list-style-type: none"> <li>• EPP (ENERGY_PERFORMANCE_PREFERENCE) 启用。当 Hardware P-States 设置为 Disabled 时，该选项不可配置。菜单选项为：</li> <li>• Disabled: 禁用后，使用 EPB(ENERGY_PERF_BIAS)作为 EPP。</li> <li>• Enabled (缺省)：启动 EPP。</li> </ul>

界面参数	功能说明
EPP profile	<p>EPP 模式设置，当 Hardware P-States 设置为 Out of Band Mode 时显示。EPP Enable 选项为 Disabled 时，该选项不可配置。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Performance: 性能优先模式。</li> <li>• Balanced Performance (缺省): 性能均衡模式。</li> <li>• Balanced Power: 节能均衡模式。</li> <li>• Power: 节能优先模式。</li> </ul>

### 3. CPU C State Control 界面

CPU C State Control 界面如 [图 3-109](#) 所示。具体参数说明如 [表 3-99](#) 所示。

图3-109 CPU C State Control 界面

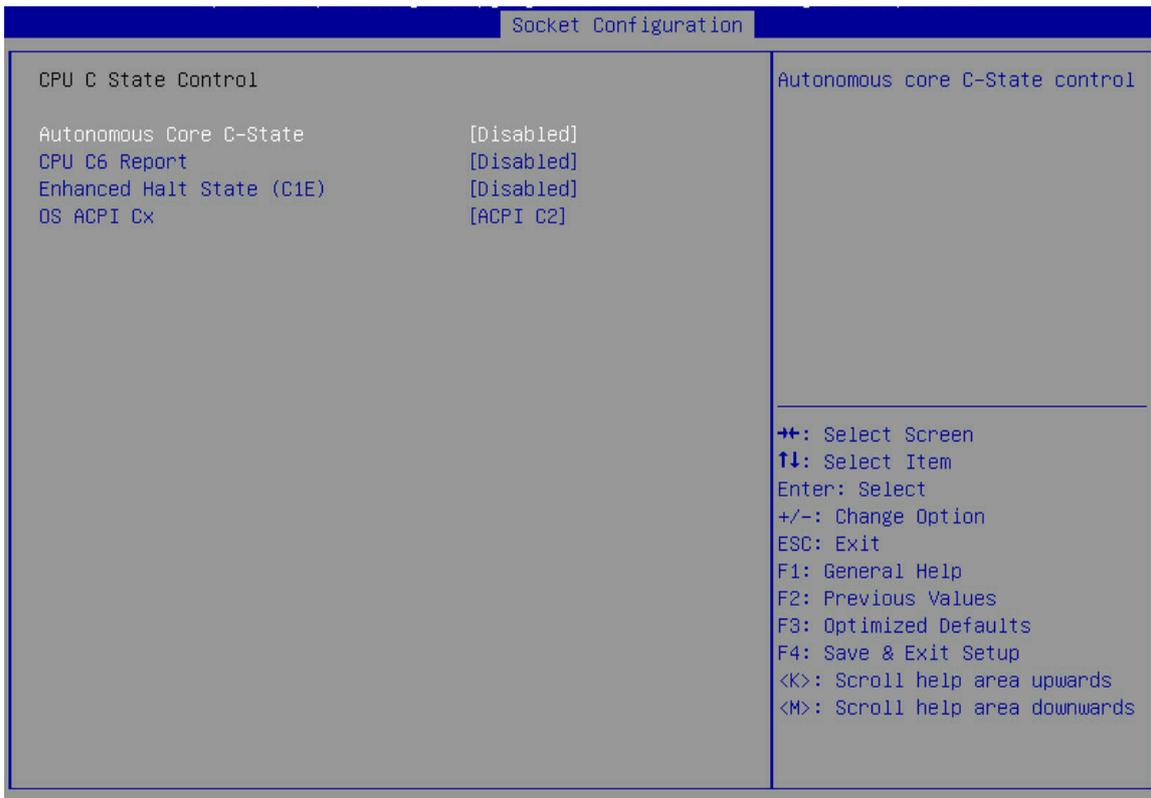


表3-99 CPU C State Control 界面参数

界面参数	功能说明
Autonomous Core C-State	<p>自主的CPU核的C状态，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled: 开启自主的 CPU 核的 C 状态。</li> <li>• Disabled (缺省): 关闭自主的 CPU 核的 C 状态。</li> </ul>

界面参数	功能说明
CPU C6 Report	<p>向操作系统报告C6状态开关，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> 开启向操作系统报告 C6 状态功能。</li> <li>• <b>Disabled (缺省):</b> 关闭向操作系统报告 C6 状态功能。</li> <li>• <b>Auto:</b> 默认开启向操作系统报告 C6 状态功能</li> </ul>
Enhanced Halt State (C1E)	<p>C1E开关，开启本功能后，操作系统可自动调节C状态。配置该选项后，需要重启后生效。</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> 开启 Enhanced Halt State 功能。</li> <li>• <b>Disabled (缺省):</b> 关闭 Enhanced Halt State 功能。</li> </ul>
OS ACPI Cx	<p>选择报告C3/C6状态到操作系统的ACPI。菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>ACPI C2 (缺省):</b> 选择报告到操作系统的 ACPI C2。</li> <li>• <b>ACPI C3:</b> 选择报告到操作系统的 ACPI C3。</li> </ul>

#### 4. Package C State Control 界面

Package C State Control界面如图 3-110所示。具体参数说明如表 3-100所示。

图3-110 Package C State Control 界面

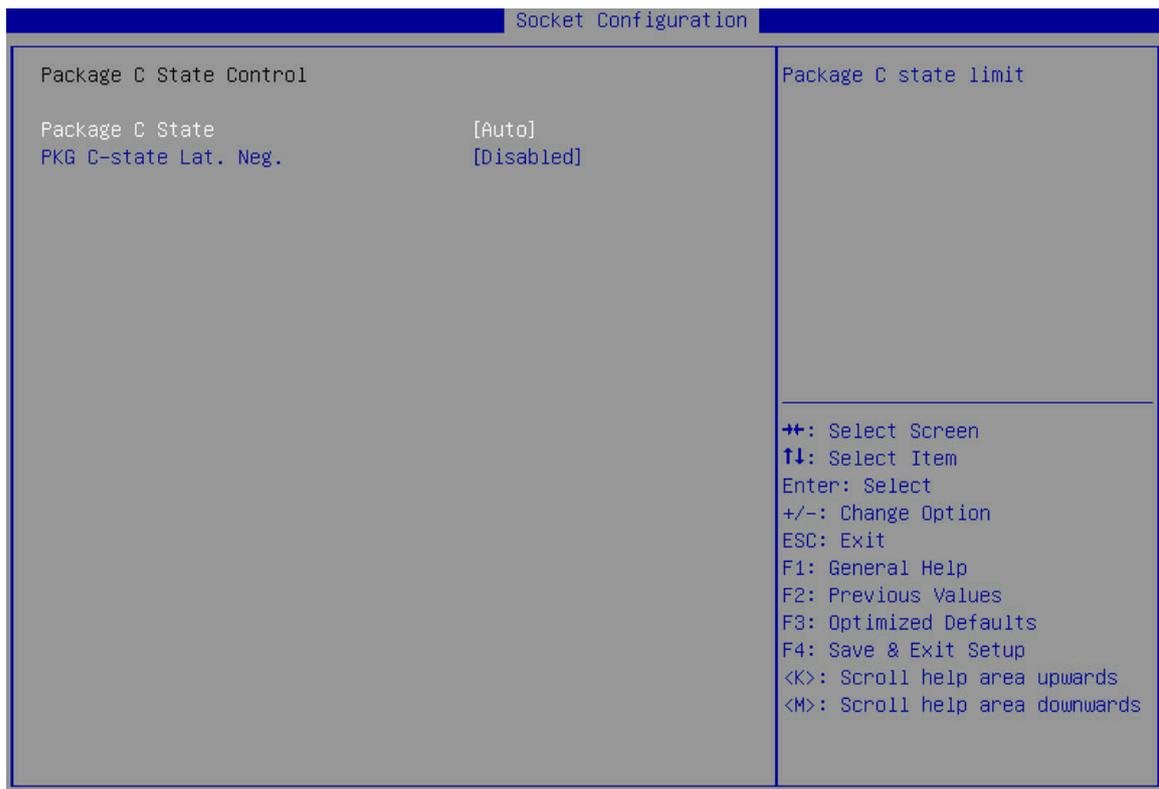


表3-100 Package C State Control 界面参数

界面参数	功能说明
Package C State	封装C状态限制。菜单选项为： <ul style="list-style-type: none"> <li>• C0/C1 state: C0/C1 状态</li> <li>• C2 state: C2 状态</li> <li>• C6 (non Retention)state: C6 (非保留) 状态</li> <li>• C6 (Retention) state: C6 (保留) 状态</li> <li>• No Limit: 无限制</li> <li>• Auto (缺省): 自动</li> </ul>
PKG C-state Lat. Neg.	PKG C状态Lat.Neg。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 开启 PKG C-state Lat. Neg.功能。</li> <li>• Disabled (缺省): 关闭 PKG C-state Lat. Neg.功能。</li> </ul>

## 5. CPU Thermal Management 界面

CPU Thermal Management界面如[图 3-111](#)所示。具体参数说明如[表 3-101](#)所示。

图3-111 CPU Thermal Management 界面



表3-101 CPU Thermal Management 界面参数

界面参数	功能说明
CPU T State Control	CPU T状态控制菜单。
PROCHOT Modes	CPU过热告警信号模式。菜单选项为： <ul style="list-style-type: none"> <li>• Output-only: 配置为仅输出模式。</li> <li>• Disabled: 禁用 PROCHOT 信号。</li> <li>• Both Input and Output (缺省): 双向传输。</li> <li>• Input-only: 配置为仅输入模式。</li> </ul>
Thermal Monitor	热监控。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省): 开启热监控。</li> <li>• Disabled: 关闭热监控。</li> </ul>
PROCHOT RATIO	热敏电阻比率，默认为0。
TCC Activation Offset	TCC激活偏移，默认为0。

## 6. CPU T State Control 界面

CPU T State Control界面如[图 3-112](#)所示。具体参数说明如[表 3-102](#)所示。

图3-112 CPU T State Control 界面

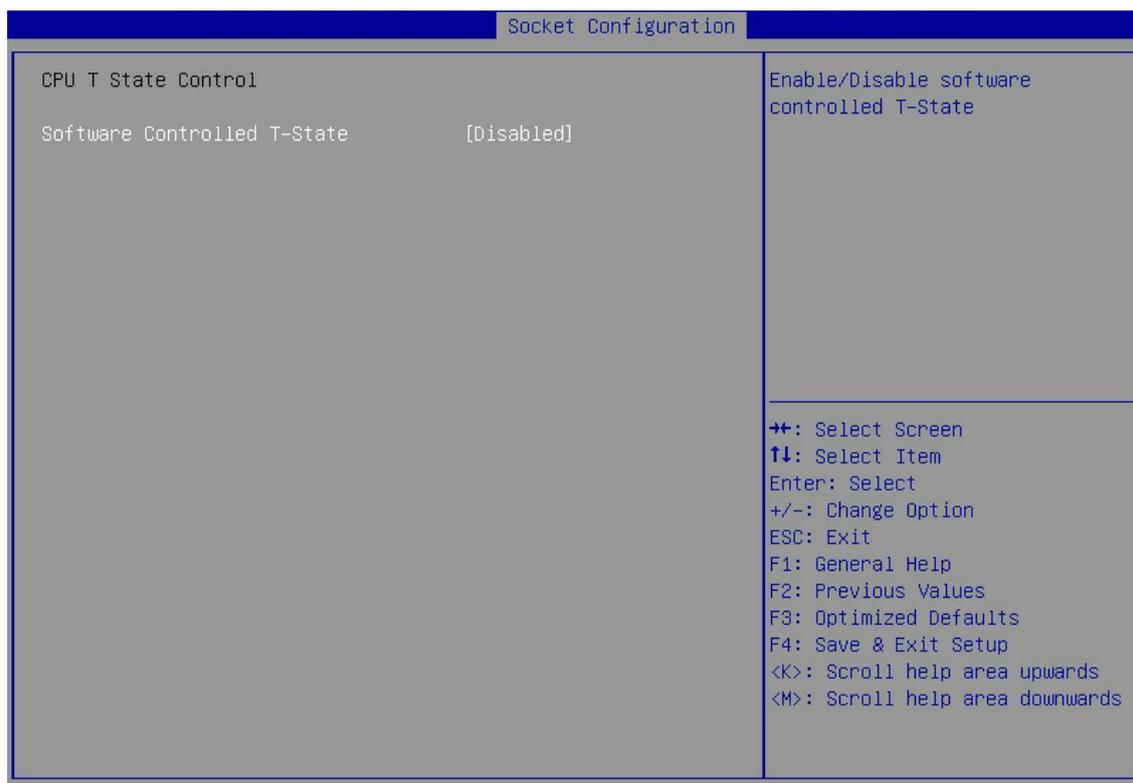


表3-102 CPU T State Control 界面参数

界面参数	功能说明
Software Controlled T-States	启用/禁用软件控制T状态。菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 开启软件控制 T 状态功能。</li> <li>• Disabled (缺省): 关闭软件控制 T 状态功能。</li> </ul>
T-State Throttle Level	T状态节流等级设置。当Software Controlled T-States选项设置为Enabled时，BIOS显示该选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled (缺省): 关闭 T 状态节流功能。</li> <li>• 18.75%</li> <li>• 25.0%</li> <li>• 31.25%</li> <li>• 37.5%</li> <li>• 43.75%</li> <li>• 50.0%</li> <li>• 56.25%</li> <li>• 62.5%</li> <li>• 68.75%</li> <li>• 75.0%</li> <li>• 81.25%</li> <li>• 87.5%</li> <li>• 93.75%</li> </ul>

## 7. CPU Advanced PM Tuning 界面

CPU Advanced PM Tuning界面如[图 3-113](#)所示。具体参数说明如[表 3-103](#)所示。

图3-113 CPU Advanced PM Tuning 界面

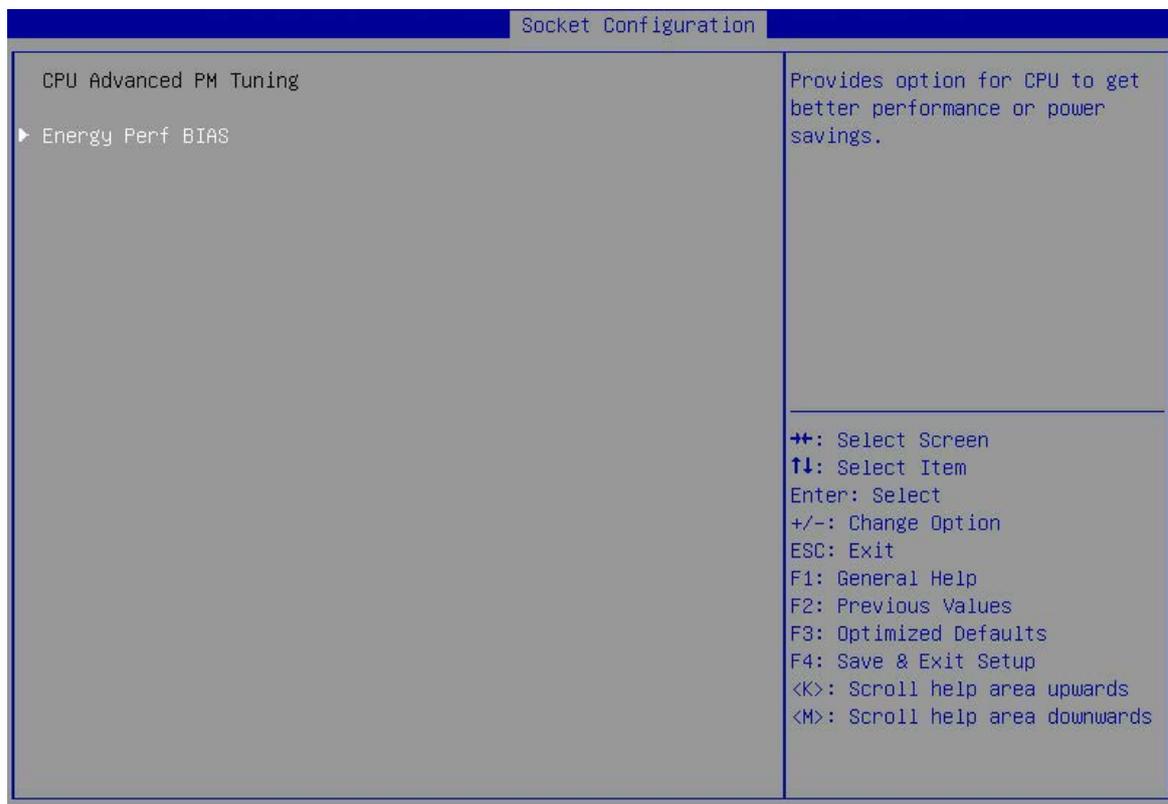


表3-103 CPU Advanced PM Tuning 界面参数

界面参数	功能说明
Energy Perf BIAS	节能性能管理配置菜单，用于优化CPU的性能和功耗。

### 8. Energy Perf BIAS 界面

Energy Perf BIAS界面如[图 3-114](#)所示。具体参数说明如[表 3-104](#)所示。

图3-114 Energy Perf BIAS 界面

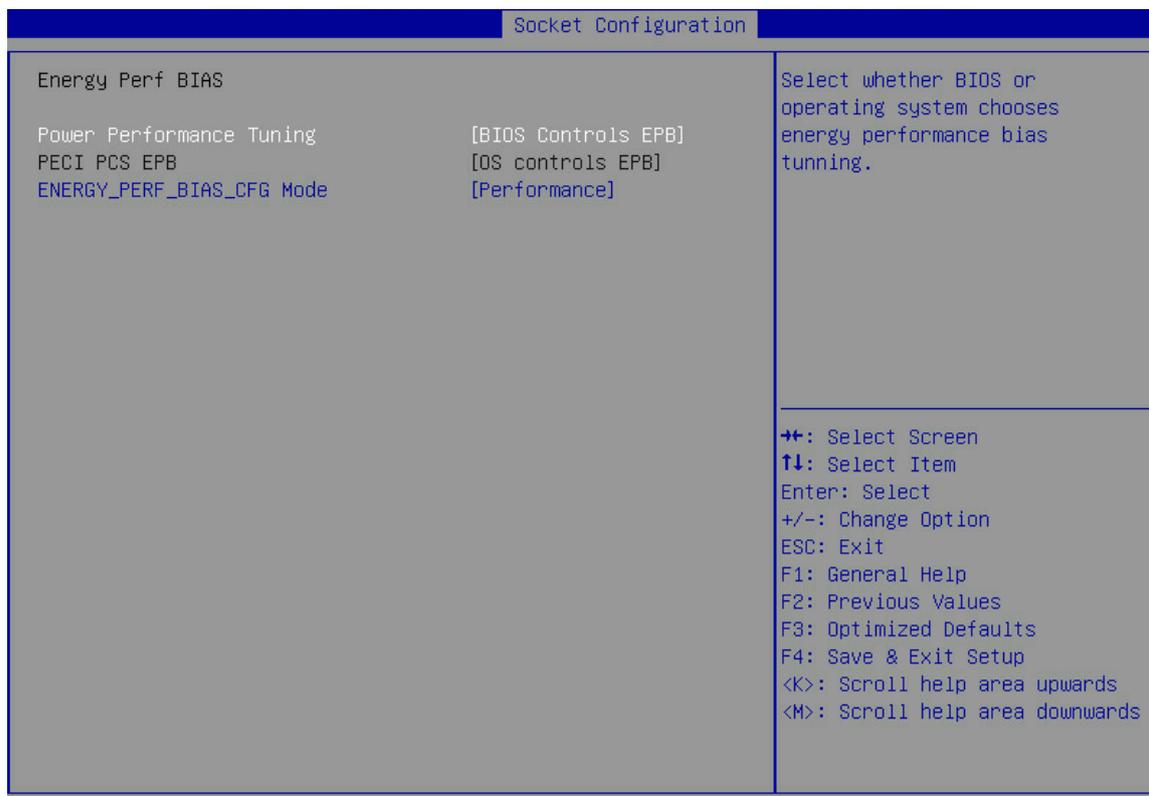


表3-104 Energy Perf BIAS 界面参数

界面参数	功能说明
Power Performance Tuning	<p>选择通过BIOS或者OS进行CPU的节能性能调整，当Hardware P-States选项设置为Out of Band Mode时，该选项置灰。菜单选项为：</p> <ul style="list-style-type: none"> <li>OS Controls EPB：选择 OS 进行 CPU 的节能性能调整。</li> <li>BIOS Controls EPB（缺省）：选择 BIOS 进行 CPU 的节能性能调整。</li> </ul>
PECI PCS EPB	<p>设置PECI是否具有EPB（Energy/Performance Bias）的控制权。当Hardware P-States选项设置为Out of Band Mode或者Power Performance Tuning设置为BIOS Controls EPB时，该选项不可配置。菜单选项有：</p> <ul style="list-style-type: none"> <li>OS controls EPB（缺省）：设置为由系统控制 EPB。</li> <li>PECI controls EPB using PCS：设置为 Peci 使用 PCS 控制 EPB。</li> </ul>
ENERGY_PERF_BIAS_CFG Mode	<p>节能性能管理配置，选择任何一个都会覆盖OS下对CPU节能性能调整的配置，Power Performance Tuning设置为BIOS Controls EPB时，才能对该选项进行配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Performance（缺省）：性能优先。</li> <li>Balanced Performance：平衡性能。</li> <li>Balanced Power：平衡功耗。</li> <li>Power：节能优先。</li> </ul>

## 9. SOCKET RAPL Config 界面

SOCKET RAPL Config界面如图 3-115所示。具体参数说明如表 3-105所示。

图3-115 SOCKET RAPL Config 界面

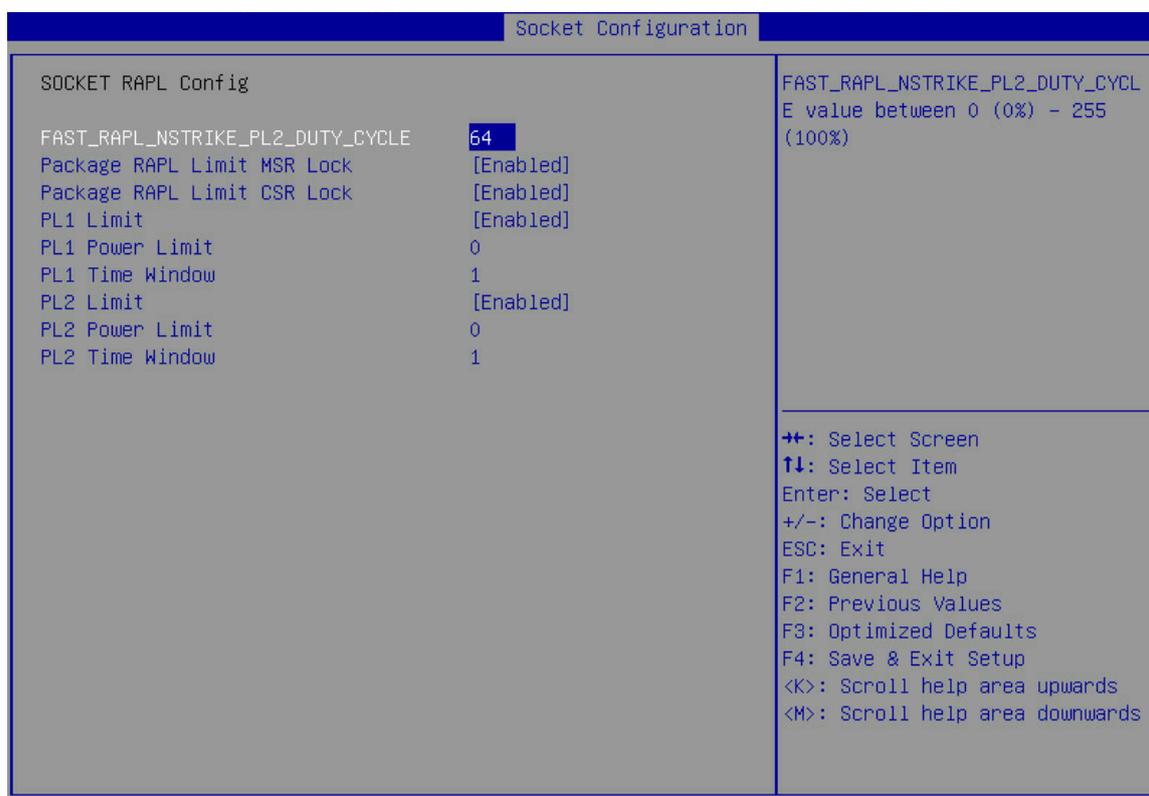


表3-105 SOCKET RAPL Config 界面参数

界面参数	功能说明
FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE	FAST功能，默认为64，取值范围在0~255之间。
Package RAPL Limit MSR Lock	PACKAGE_RAPL_LIMIT MSR寄存器设置锁，菜单选项为： <ul style="list-style-type: none"> <li>Enabled(缺省)：锁定 PACKAGE_RAPL_LIMIT MSR 寄存器。</li> <li>Disabled：解锁 PACKAGE_RAPL_LIMIT MSR 寄存器。</li> </ul>
Package RAPL Limit CSR Lock	PACKAGE_RAPL_LIMIT CSR寄存器设置锁，菜单选项为： <ul style="list-style-type: none"> <li>Enabled(缺省)：锁定 PACKAGE_RAPL_LIMIT CSR 寄存器。</li> <li>Disabled：解锁 PACKAGE_RAPL_LIMIT CSR 寄存器。</li> </ul>
PL1 Limit	PL1限制功能，设置CPU LIMIT1平均功率的阈值和持续时间的开关。菜单选项为： <ul style="list-style-type: none"> <li>Enabled(缺省)：开启 CPU LIMIT1 平均功率的阈值和持续时间的开关。</li> <li>Disabled：禁用 PL1 限制时，BIOS 将为 PL1 功率限制和 PL1 时间窗编程设定为默认值。</li> </ul>

界面参数	功能说明
PL1 Power Limit	PL1 功率限制。单位为瓦特，默认为0。该值可从0到熔断值，如果该值为0，通过BIOS编程设定。
PL1 Time Window	PL1时间窗口，单位为秒，默认为1，取值范围从0到56。表示时间窗口上TDP应该维护的值。如果该值设置为0，该熔断值将被编程设定。
PL2 Limit	PL2限制功能。菜单选项为： <ul style="list-style-type: none"> <li>Enabled(缺省): 启动 PL2 限制功能。</li> <li>Disabled: 禁用 PL2时，BIOS 将为 PL2 功率限制和 PL2 时间窗设定默认值。</li> </ul>
PL2 Power Limit	PL2功率限制，单位为瓦特，默认为0。该值可从0到熔断值，如果该值为0，BIOS设定为125%*TDP。
PL2 Time Window	PL2时间窗口，单位为秒，默认为1，取值范围从0到56。表示时间窗口上TDP应该维护的值。如果该值设置为0，该熔断值将被编程设定。

### 3.5 Server Mgmt界面

Server Mgmt界面如[图 3-116](#)所示，主要包含FRB-2 计时器配置、看门狗配置、HDM网络配置、HDM用户配置、固件信息等。具体参数说明如[表 3-106](#)所示。

图3-116 Server Mgmt 界面

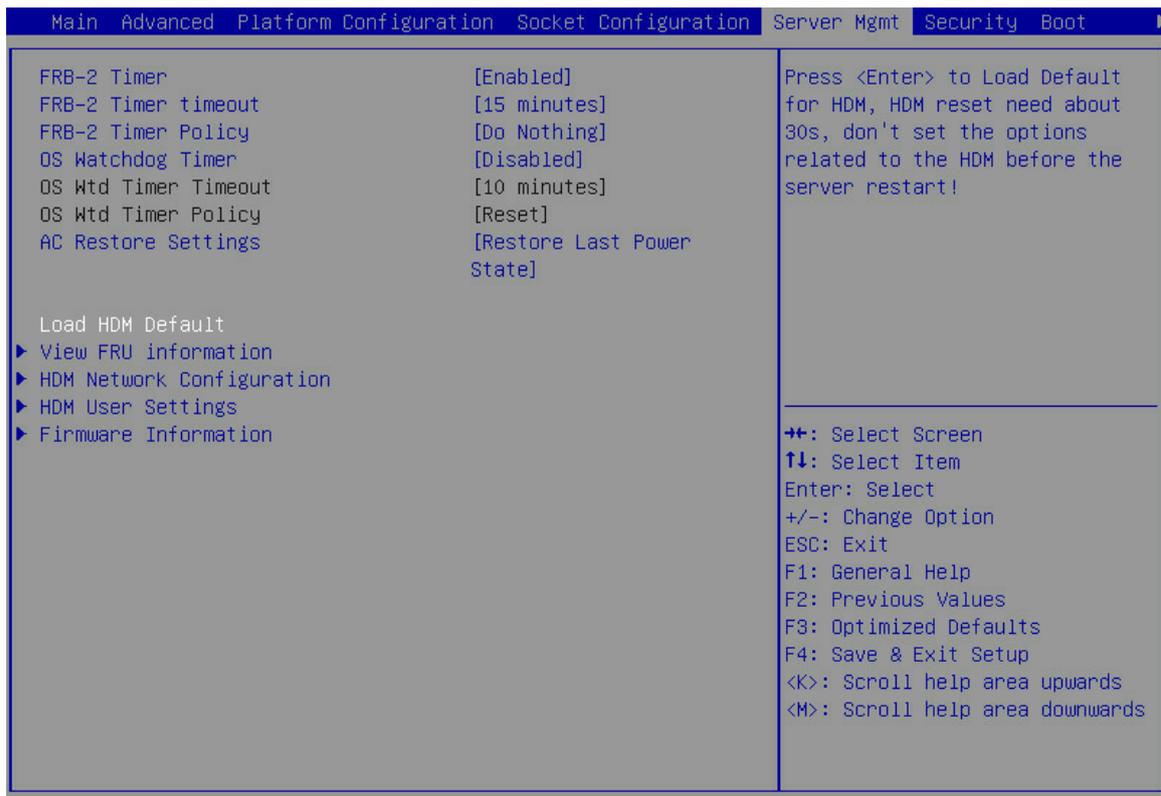


表3-106 Server Mgmt 界面参数

界面参数	功能说明
FRB-2 Timer	FRB-2时钟设置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled (缺省)：启用 FRB-2 时钟。</li> <li>• Disabled: 禁用 FRB-2 时钟。</li> </ul>
FRB-2 Timer Timeout	FRB-2时钟到期时间设置，菜单选项为： <ul style="list-style-type: none"> <li>• 3 Minutes</li> <li>• 4 Minutes</li> <li>• 5 Minutes</li> <li>• 6 Minutes</li> <li>• 10 Minutes</li> <li>• 15 Minutes (缺省)</li> <li>• 20 Minutes</li> </ul>
FRB-2 Timer Policy	FRB-2时钟到期后的策略设置，菜单选项为： <ul style="list-style-type: none"> <li>• Do Nothing: 无动作。</li> <li>• Reset: 立即重启。</li> <li>• Power Down: 正常关机。</li> <li>• Power Cycle (缺省)：关机并重新开机。</li> </ul>
OS Watchdog Timer	OS看门狗定时器开关，开启该功能后，系统进入OS时，开启定时器，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 开启 OS 看门狗定时器。</li> <li>• Disabled (缺省)：关闭 OS 看门狗定时器。</li> </ul>
OS Wtd Timer Timeout	OS看门狗定时器超时设置，设置系统进入OS时，定时器超时时间。OS Watchdog Timer设置为Enabled时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• 5 Minutes</li> <li>• 10 Minutes (缺省)</li> <li>• 15 Minutes</li> <li>• 20 Minutes</li> </ul>
OS Wtd Timer Policy	OS看门狗定时器策略设置，设置系统进入OS时，定时器超时后的动作。OS Watchdog Timer设置为Enabled时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• Do Nothing: 无动作。</li> <li>• Reset (缺省): 立即重启。</li> <li>• Power Down: 正常关机。</li> <li>• Power Cycle: 关机并重新开机。</li> </ul>
AC Restore Settings	AC恢复配置状态设置，对本选项的修改将立即生效。菜单选项为： <ul style="list-style-type: none"> <li>• Always Power On: 系统处于工作状态。</li> <li>• Always Remain Off: 系统处于关机状态。</li> <li>• Restore Last Power State (缺省)：保持上次断电时的状态。</li> </ul> 需要注意的是：AC Restore Settings的缺省项与HDM的设置有关。

界面参数	功能说明
Load HDM Default	恢复HDM的出厂配置。 注意：按 <b>Enter</b> 恢复HDM出厂配置，重置HDM大概需要一分钟，服务器重启之前请勿设置与HDM相关的选项。
View FRU information	查看FRU信息菜单。
HDM Network Configuration	HDM网络配置菜单。
HDM User Settings	HDM用户配置菜单。
Firmware Information	显示固件信息菜单。

### 1. View FRU information 界面

View FRU information界面如图3-117所示。具体参数说明如表3-107所示。

图3-117 View FRU information 界面

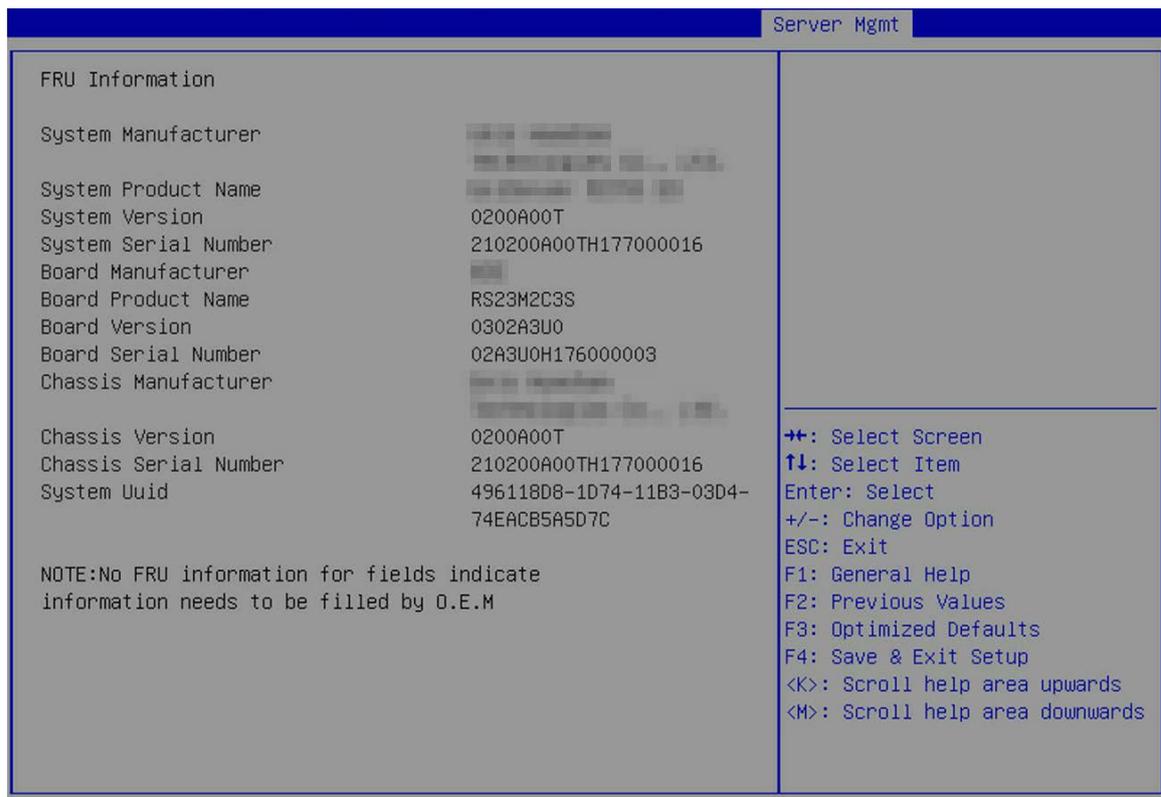


表3-107 View FRU information 界面参数

界面参数	功能说明
System Manufacturer	系统厂商信息
System Product Name	系统产品名称
System Version	系统版本
System Serial Number	系统序列号

界面参数	功能说明
Board Manufacturer	主板制造商
Board Product Name	主板产品名称
Board Version	主板版本号
Board Serial Number	主板序列号
Chassis Manufacturer	机箱制造商
Chassis Version	机箱版本
Chassis Serial Number	机箱序列号
System Uuid	系统通用唯一识别码

## 2. HDM Network Configuration 界面

HDM Network Configuration界面如[图 3-118](#)和[图 3-119](#)所示。具体参数说明如[表 3-108](#)所示。



说明

HDM Shared Network Port（HDM 共享网口）和 HDM Dedicated Network Port（HDM 专用网口）的界面参数相同，配置时请注意不要将 HDM 共享网口与专用网口的 IP 地址配置在同一网段。本文以 HDM Shared Network Port 为例。

图3-118 HDM Network Configuration 界面 1

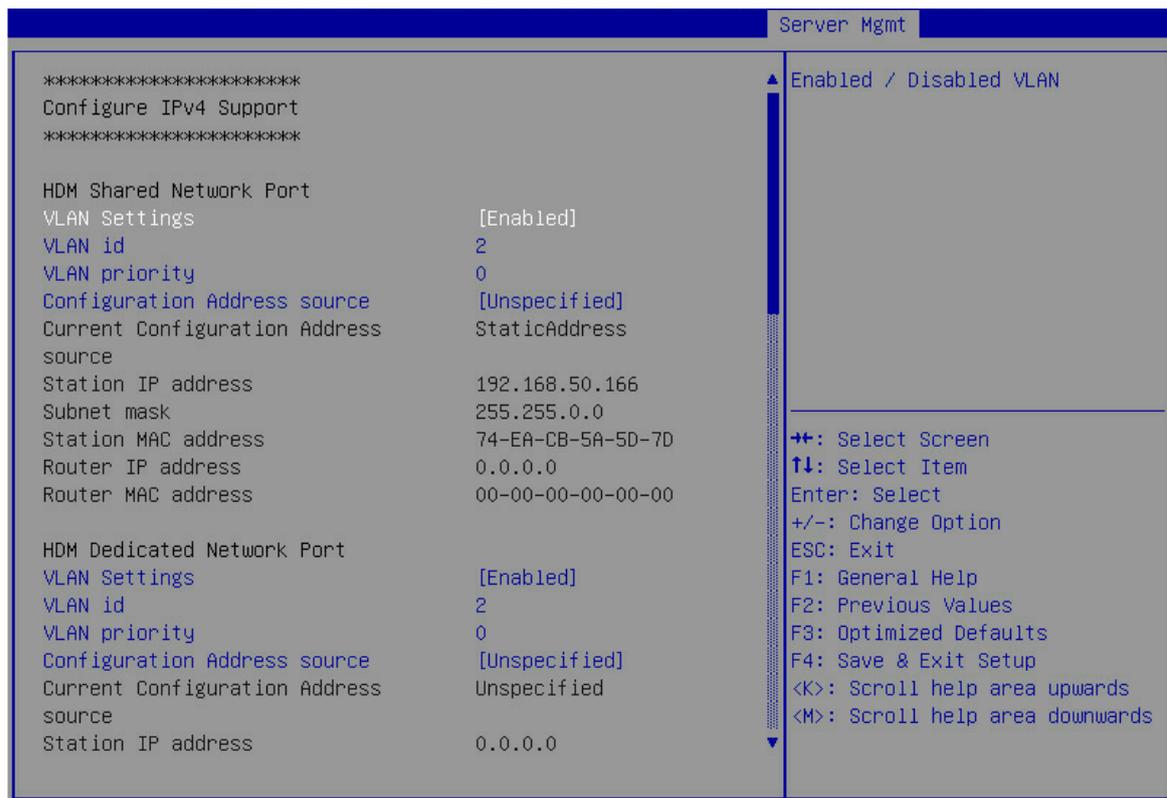


图3-119 HDM Network Configuration 界面 2

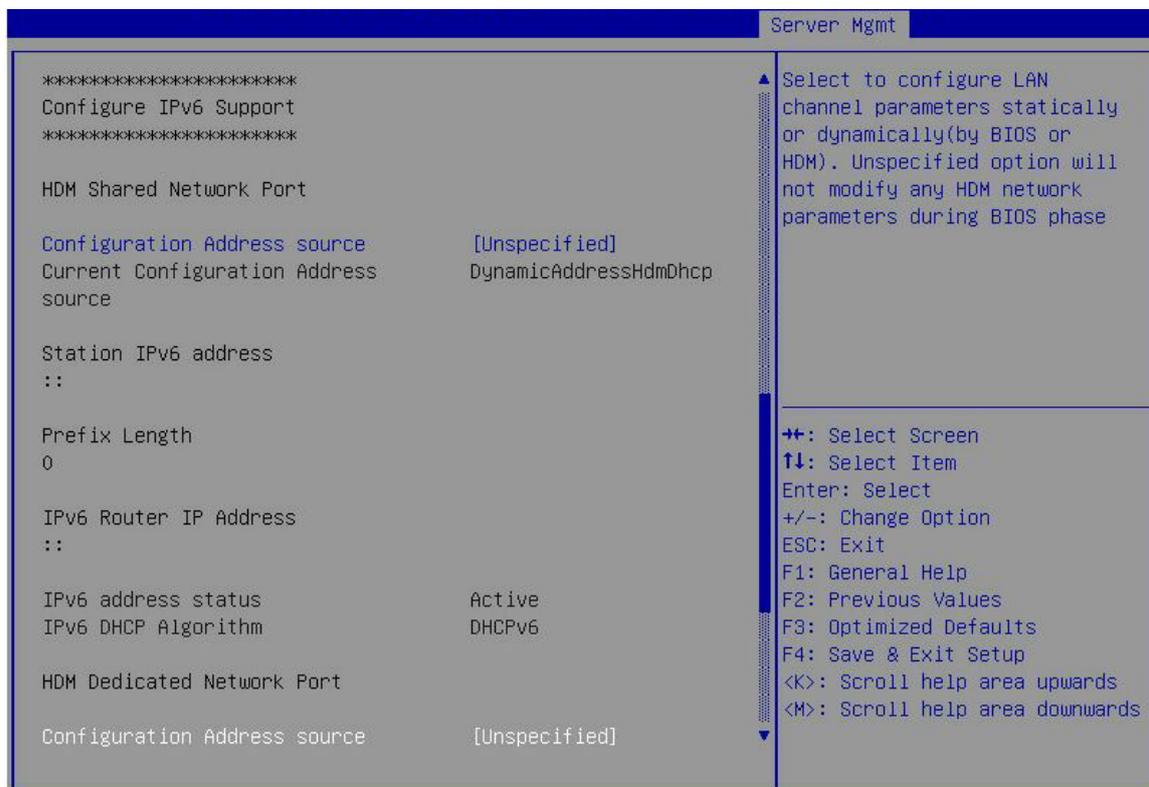


表3-108 HDM Network Configuration 界面参数

界面参数	功能说明
<b>Configure IPv4 Support</b>	
Vlan Setting	设置是否启用HDM网口Vlan功能。菜单选项为： <ul style="list-style-type: none"> <li>Disabled (缺省): 禁用 Vlan 配置。</li> <li>Enabled: 启用 Vlan 配置。</li> </ul>
Vlan id	配置Vlan ID, 缺省为2, 取值范围2~4094。当Vlan Setting设置为Enabled时, 显示该选项。
Vlan priority	指定Vlan的优先级, 缺省为0, 取值范围是0~7, 数值越大, 优先级越高。当端口发生传输拥塞时, 通过识别Vlan优先级, 优先发送优先级高的数据帧。当Vlan Setting设置为Enabled时, 显示该选项。
Configuration Address Source	配置HDM网络状态参数。菜单选项为： <ul style="list-style-type: none"> <li>Unspecified (缺省): 保留当前的网络信息获取方式和信息。</li> <li>Static: 手动配置网络信息。</li> <li>DynamicHdmDhcp: 通过 DHCP 分配获取网络信息。</li> </ul>
Current Configuration Address Source	显示当前地址源。
Station IP Address	端口的IP地址。当Configuration Address Source设置为Static时, 该选项可配置。 该选项与Subnet Mask选项均配置后, 配置的HDM静态IPv4地址才可生效。

界面参数	功能说明
Subnet Mask	子网掩码，默认值为0.0.0.0。如需设置HDM的静态IPv4地址，需要配置该选项。 当Configuration Address Source设置为Static时，该选项可配置。
Station MAC Address	端口的MAC地址。
Router IP Address	网关IP地址。当Configuration Address Source设置为Static时，该选项可配置。
Router MAC Address	网关MAC地址。
<b>Configure IPv6 Support</b>	
Configuration Address source	配置HDM网络状态参数。菜单选项为： <ul style="list-style-type: none"> <li>• Unspecified（缺省）：保留当前的网络信息获取方式和信息。</li> <li>• Static：手动配置网络信息。</li> <li>• DynamicHdmDhcp：通过DHCP分配获取网络信息。</li> </ul>
Current Configuration Address source	显示当前地址源。
Station IPv6 address	端口的IPv6地址。当Configuration Address Source设置为Static时，该选项可配置。 该选项与Prefix Length选项均配置后，配置的HDM静态IPv6地址才可生效。
Prefix Length	前缀长度，有效输入范围是1~127。0表示未设置前缀长度（默认为0）。如需设置HDM的静态IPv6地址，需要配置该选项。 当Configuration Address Source设置为Static时，该选项可配置。
IPv6 Router IP Address	IPv6网关地址。当Configuration Address Source设置为Static时，该选项可配置。IPv6网关IP需保持和端口IPv6地址在同一网段。
IPv6 address status	IPv6地址状态。
IPv6 DHCP Algorithm	IPv6 DHCP算法。

### 3. HDM User Settings 界面

HDM User Settings界面如[图 3-120](#)所示。具体参数说明如[表 3-109](#)所示。

图3-120 HDM User Settings 界面

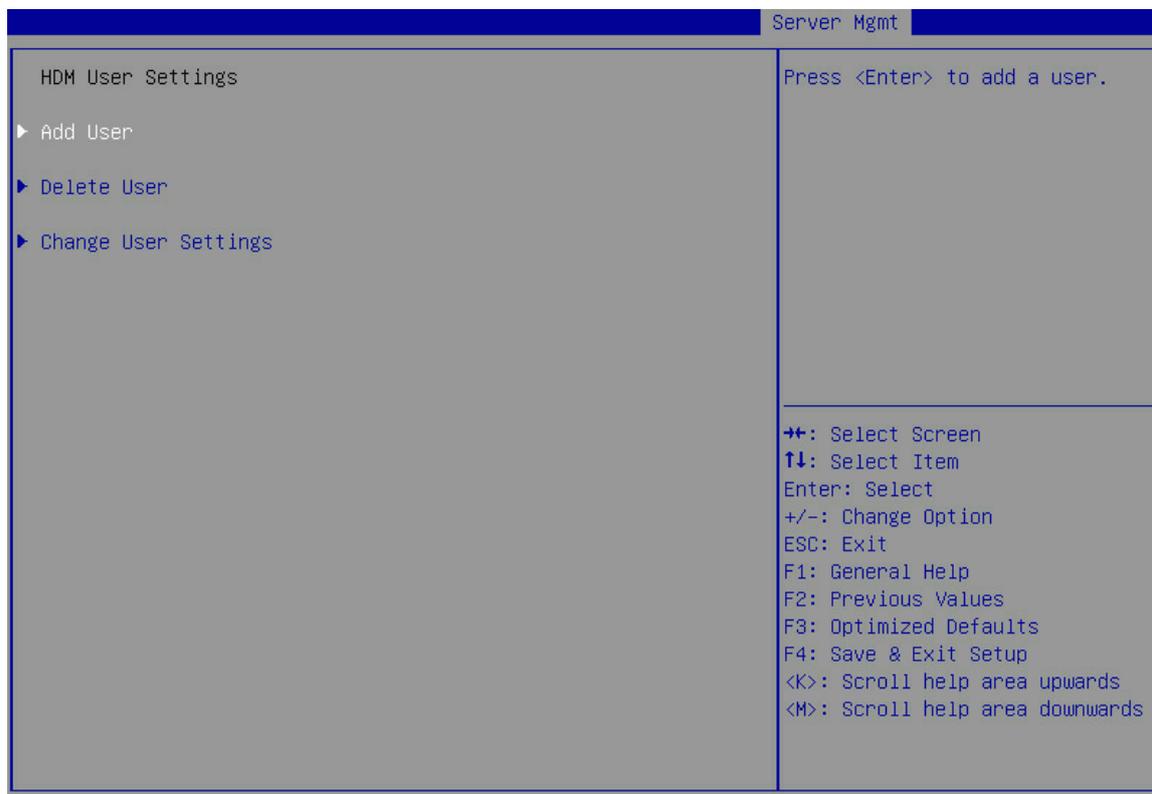


表3-109 HDM User Settings 界面参数

界面参数	功能说明
Add User	添加用户配置菜单。
Delete User	删除用户配置菜单。
Change User Settings	修改用户配置菜单。

Add User界面如[图 3-121](#)所示。具体参数说明如[表 3-110](#)所示。

图3-121 Add User 界面

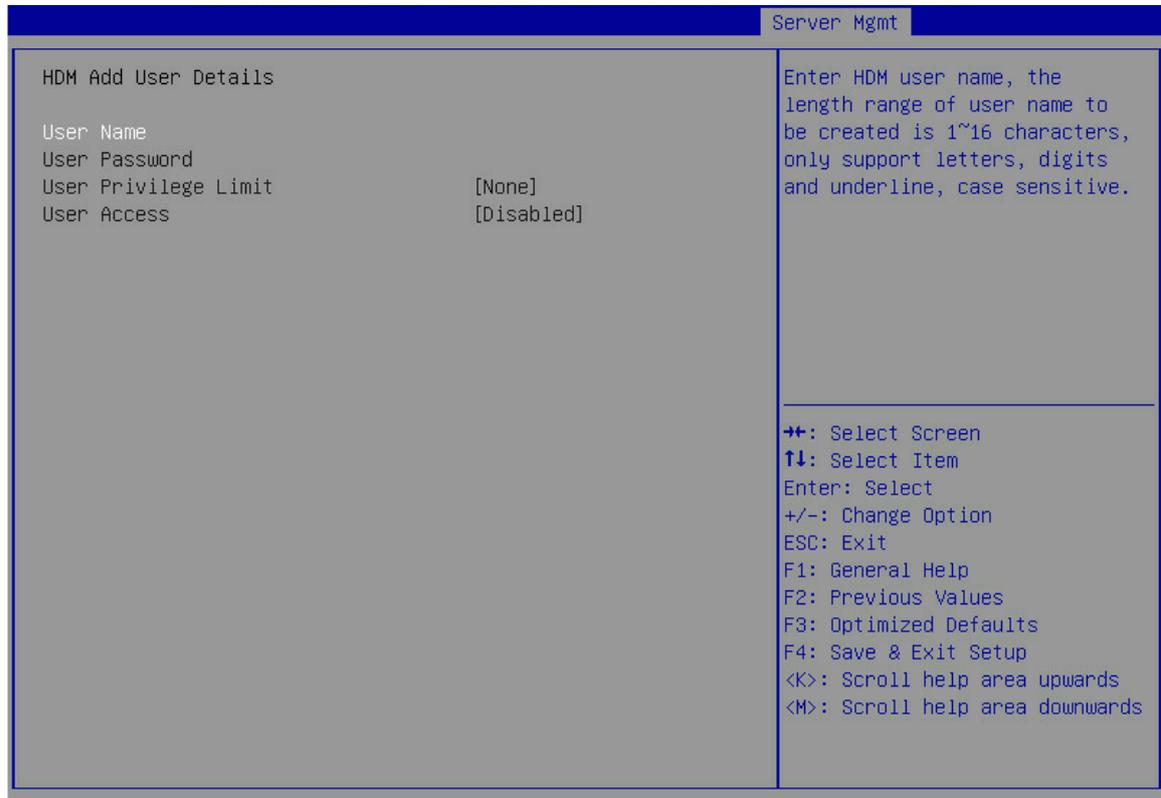


表3-110 Add User 界面参数

界面参数	功能说明
User Name	待创建的HDM用户名，长度为1~16个字符，仅支持字母、数字和下划线，区分大小写。
User Password	<p>HDM用户的密码。</p> <p>密码的设置规则与是否在HDM Web界面上开启了密码复杂度检查有关，缺省情况下密码复杂度检查功能处于开启状态。</p> <ul style="list-style-type: none"> <li>• 开启密码复杂度检查功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。 <ul style="list-style-type: none"> <li>○ 密码长度为8~20个字符，仅支持字母、数字、空格和特殊字符~!@#%&amp;^&amp;*( )_+=[\{} ;: ",./&lt;&gt;?, 区分大小写;</li> <li>○ 至少包含大写字母、小写字母和数字中的两种字符;</li> <li>○ 至少包含一个空格或特殊字符;</li> <li>○ 不能与用户名或用户名的倒序相同。</li> </ul> </li> <li>• 关闭密码复杂度检查功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。 <ul style="list-style-type: none"> <li>○ 密码长度为2~20个字符，仅支持字母、数字、空格和特殊字符~!@#%&amp;^&amp;*( )_+=[\{} ;: ",./&lt;&gt;?, 区分大小写。</li> </ul> </li> </ul> <p>开启或关闭密码复杂度检查的详细方法请参见HDM联机帮助中的“密码规则高级设置”章节。</p>

界面参数	功能说明
User Privilege Limit	HDM用户权限，菜单选项为： <ul style="list-style-type: none"> <li>• None（缺省）：保留当前的HDM用户权限。</li> <li>• User：用户权限。</li> <li>• Operator：操作员权限。</li> <li>• Administrator：管理员权限。</li> </ul>
User Access	用户访问开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启用户访问功能。</li> <li>• Disabled（缺省）：关闭用户访问功能。</li> </ul>

Delete User界面如[图 3-122](#)所示。具体参数说明如[表 3-111](#)所示。

图3-122 Delete User 界面

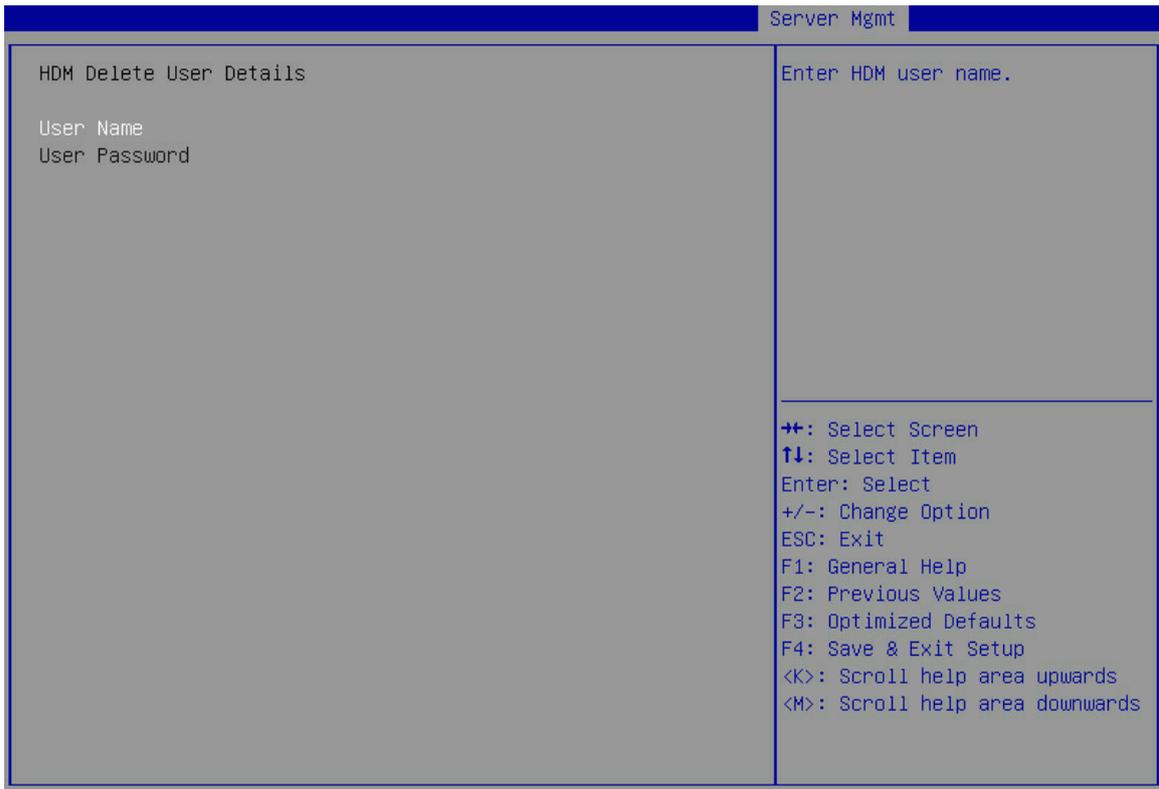


表3-111 Delete User 界面参数

界面参数	功能说明
User Name	已创建的HDM用户名。
User Password	HDM用户名对应的密码。

Change User Settings界面如[图 3-123](#)所示。具体参数说明如[表 3-112](#)所示。

图3-123 Change User Settings 界面

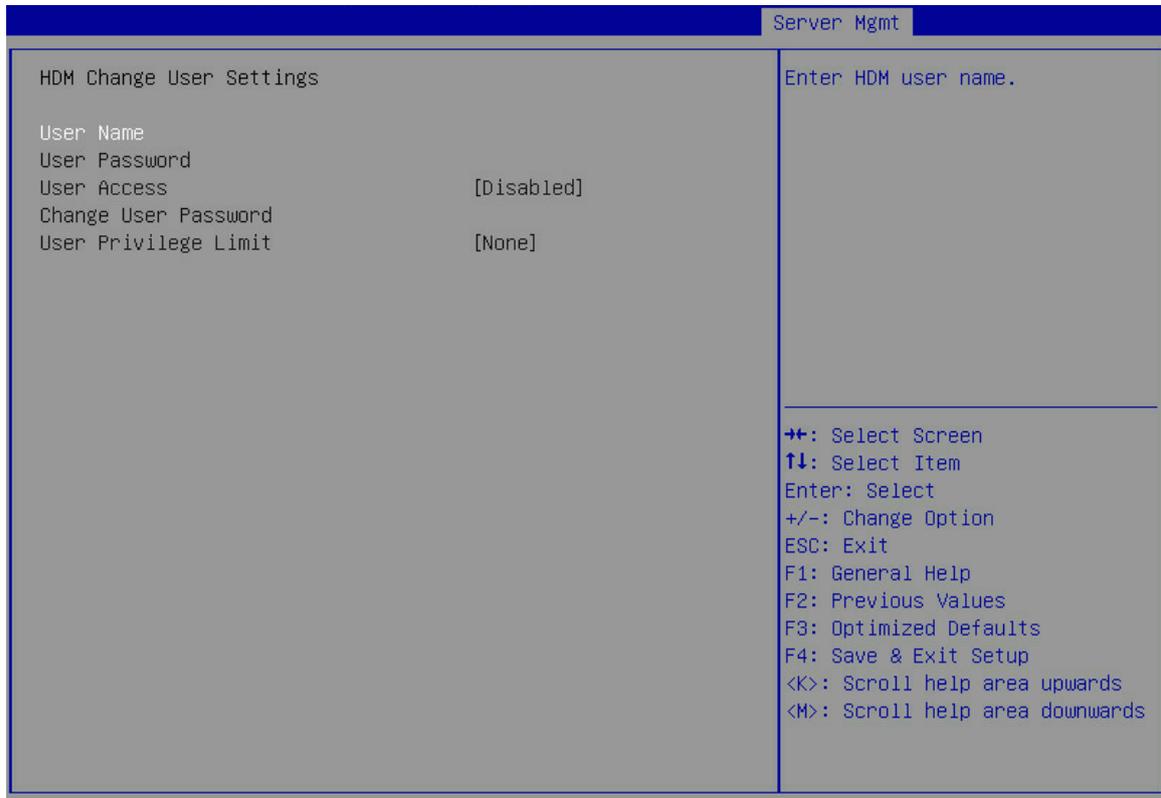


表3-112 Change User Settings 界面参数

界面参数	功能说明
User Name	已创建的HDM用户名
User Password	HDM用户名对应的密码。 用户登录失败的次数达到HDM设定的次数后，HDM会锁定该用户的登录。HDM默认的登录失败次数为五次，默认登录失败锁定时长为五分钟。
User Access	用户访问开关，输入正确的HDM用户名和密码后，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 开启用户访问功能。</li> <li>• Disabled (缺省)：关闭用户访问功能。</li> </ul>



图3-124 Firmware Information 界面

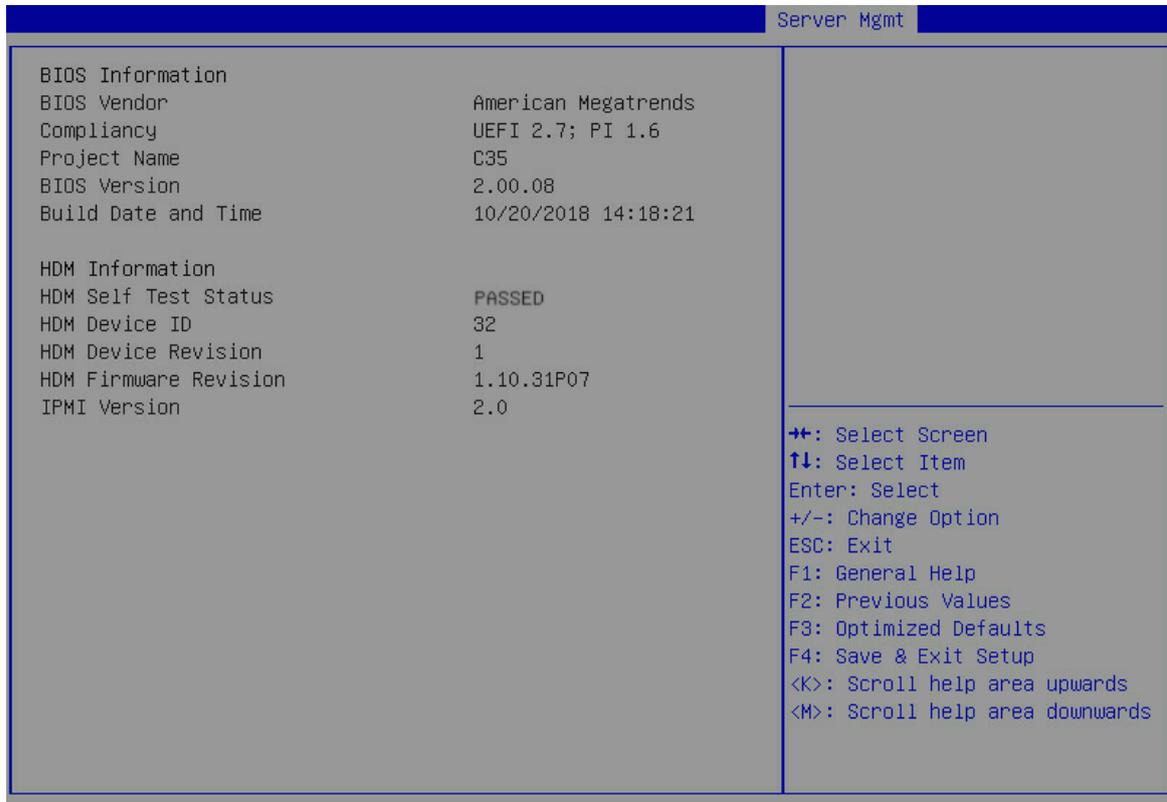


表3-113 Firmware Information 界面参数

界面参数	功能说明
<b>BIOS Information</b>	
BIOS Vendor	显示BIOS供应商。
Compliance	显示BIOS遵循的规范。
Project Name	显示项目名称。
BIOS Version	显示BIOS版本号。
Build Date and Time	显示BIOS的编译日期和时间。
<b>HDM Information</b>	
HDM Self Test Status	显示HDM自检状态。
HDM Device ID	显示HDM设备ID。
HDM Device Revision	显示HDM设备版本号。
HDM Firmware Revision	显示HDM固件版本号。
IPMI Version	显示IPMI版本号。

## 3.6 Security界面

Security界面如图 3-125和图 3-126所示，主要包含对管理员密码、用户密码进行配置。具体参数说明如表 3-114所示。

图3-125 Security 界面 1

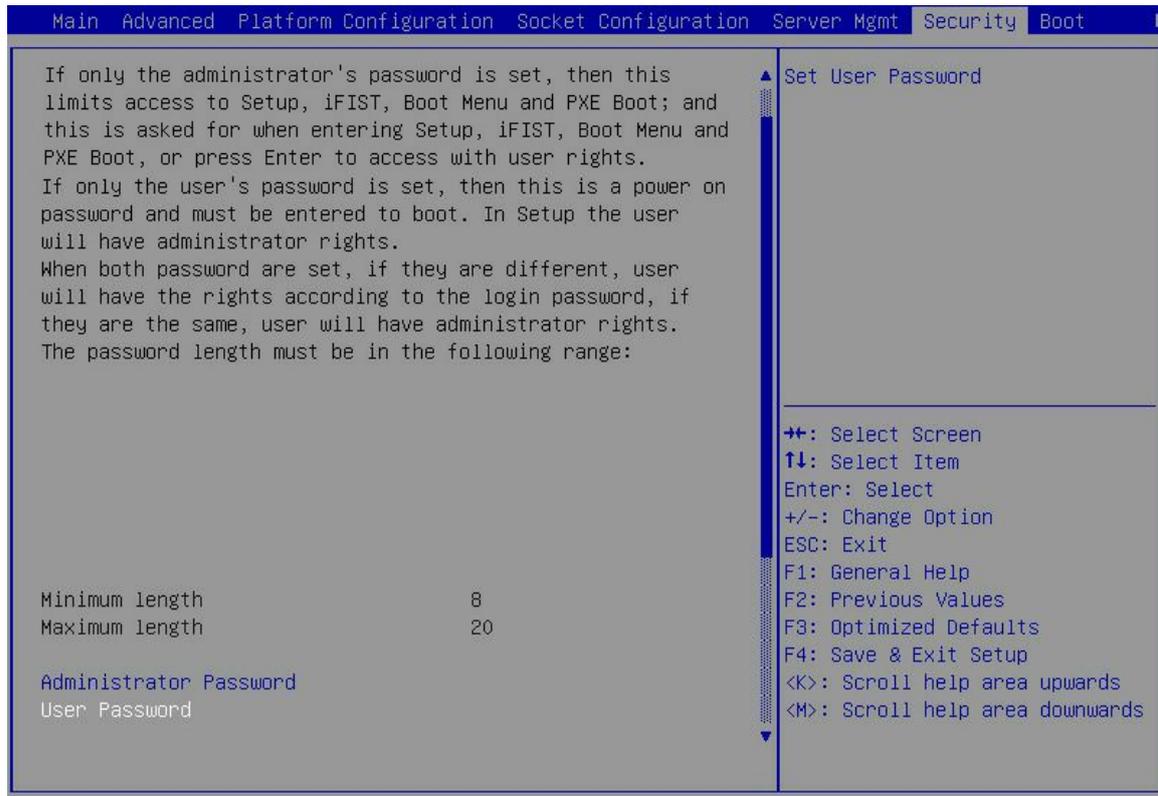


图3-126 Security 界面 2

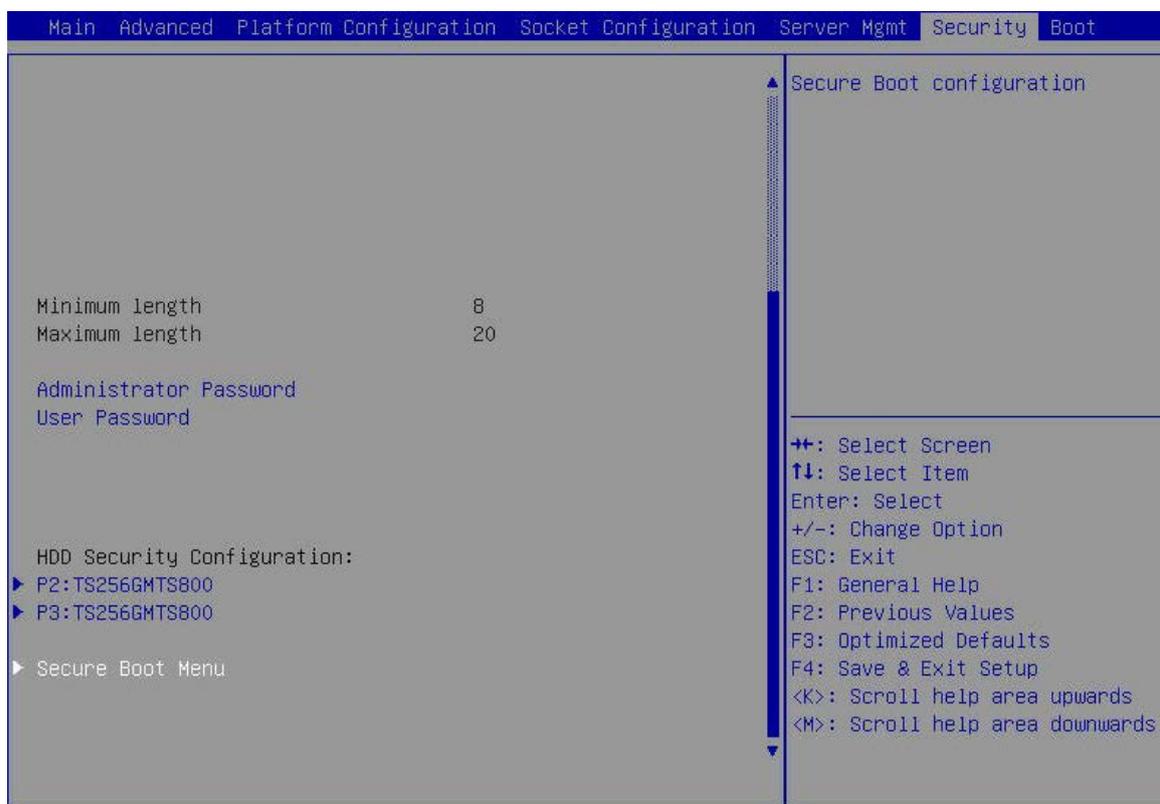


表3-114 Security 界面参数

界面参数	功能说明
Password Description	密码描述。
Administrator Password	创建管理员密码。密码设置规则请查看 <a href="#">2.8.2 密码设置注意事项</a> 。
User Password	创建用户密码。密码设置规则请查看 <a href="#">2.8.2 密码设置注意事项</a> 。
HDD Security Configuration	硬盘安全配置，仅部分支持HDD Security功能的硬盘接入板载SATA槽位时显示。
P2:TS256GMTS800	硬盘安全配置页面。
Secure Boot Menu	安全启动菜单，仅UEFI启动模式下显示该菜单。

HDD Security Configuration界面如[图 3-127](#)所示，具体参数说明如[表 3-115](#)所示。

图3-127 HDD Security Configuration 界面

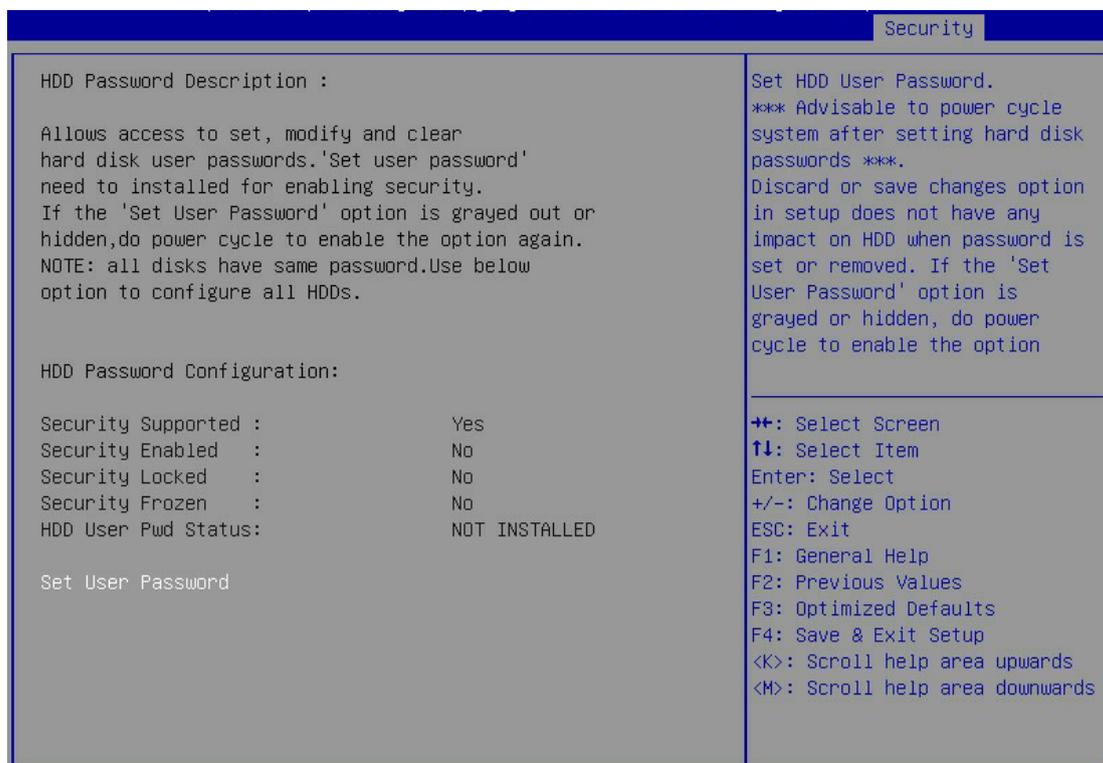


表3-115 HDD Security Configuration 界面参数

界面参数	功能说明
Security Supported	显示HDD是否支持安全设置。
Security Enabled	显示 HDD 安全功能使能状态。
Security Locked	显示 HDD 安全锁定状态。
Security Frozen	显示HDD安全冻结状态，如使能将无法进行硬盘格式化。
HDD User Pwd Status	显示HDD用户密码当前状态。
Set User Password	设置HDD用户密码。如果HDD用户密码已经设置或移除，则BIOS内的设置将无法影响到该密码。 该选项置灰或隐藏时，通过掉电重启服务器，可以再次显示该选项。

Secure Boot Menu界面如[图 3-128](#)所示，具体参数说明如[表 3-116](#)所示。

图3-128 Secure Boot Menu 界面

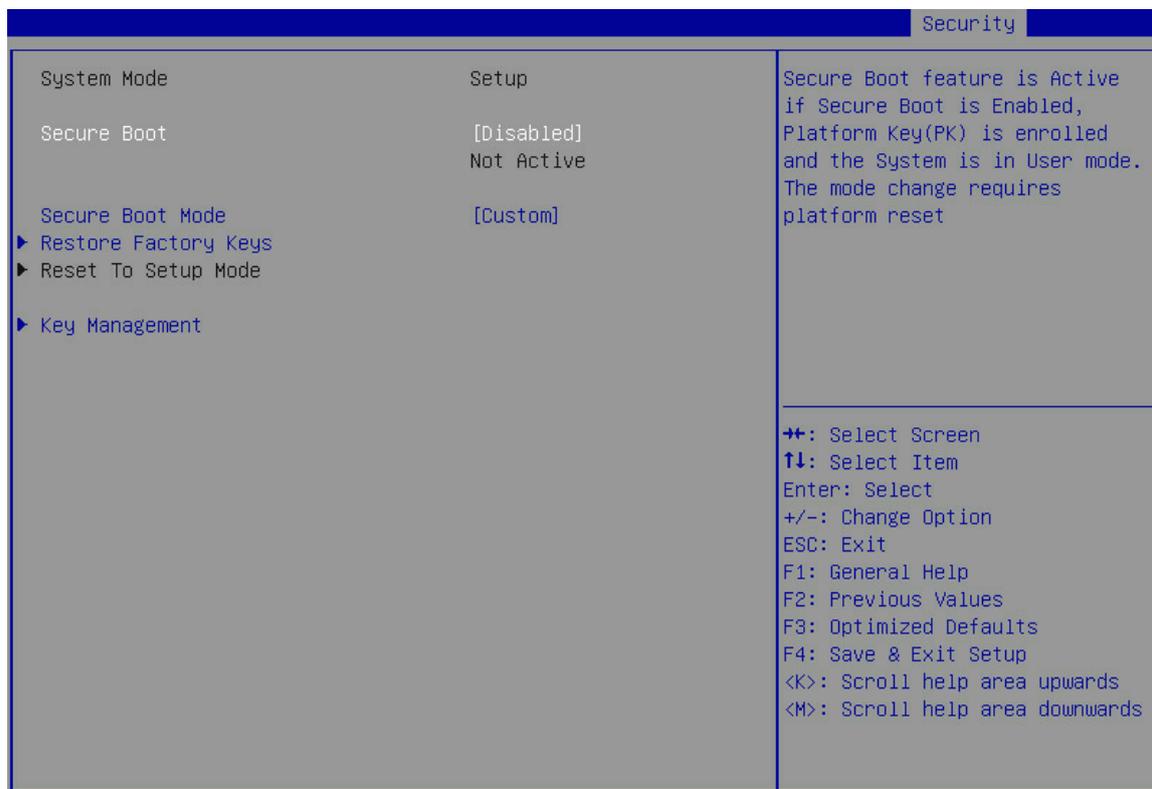


表3-116 Secure Boot Menu 界面参数

界面参数	功能说明
System Mode	显示系统模式。
Secure Boot	安全启动功能配置，菜单选项为： <ul style="list-style-type: none"> <li>• <b>Disabled</b>（缺省）：禁用安全启动功能。</li> <li>• <b>Enabled</b>：启用安全启动功能。注册平台密钥（PK）且系统将处于用户模式。</li> </ul>
Secure Boot Mode	安全启动模式配置，菜单选项为： <ul style="list-style-type: none"> <li>• <b>Standard</b>：标准模式。</li> <li>• <b>Custom</b>（缺省）：用户模式，用户模式允许用户改变 Image 执行策略以及管理安全启动密钥。</li> </ul>
Restore Factory Keys	恢复出厂密钥。
Reset To Setup Mode	重置为设置模式。
Key Management	密钥管理菜单。

Key Management 界面如 [图 3-129](#) 所示，具体参数说明如 [表 3-117](#) 所示。

图3-129 Key Management 界面

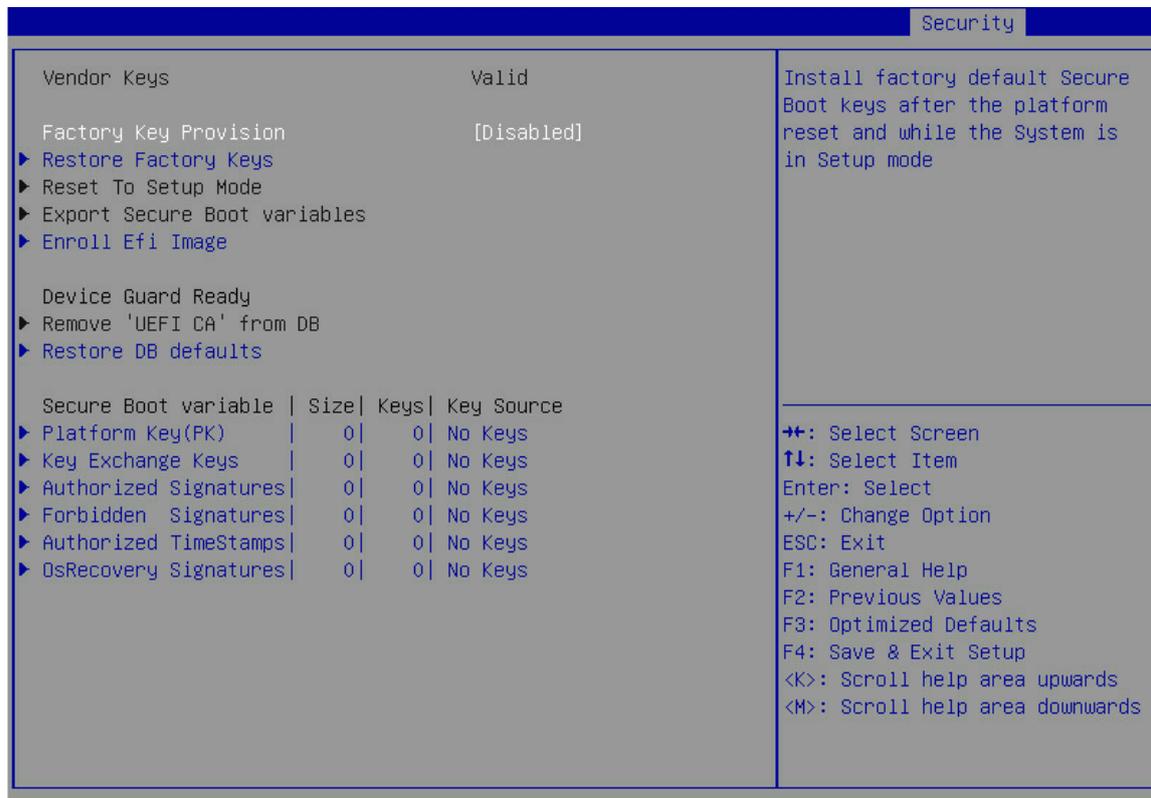


表3-117 Key Management 界面参数

界面参数	功能说明
Vendor Keys	供应商密钥。
Factory Key Provision	安装工厂密钥。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用工厂密钥安装。</li> <li>• Enabled：启用工厂密钥安装。请安装出厂默认安全启动密钥。</li> </ul>
Restore Factory Keys	恢复工厂密钥。 强制系统到用户模式，安装出厂默认安全启动密钥数据库。
Reset To Setup Mode	重设为设置模式。
Export SECURE Boot Variables	导出所有安全启动变量。
Enroll Efi Image	注册Efi镜像。允许镜像以安全模式运行，在授权签名数据库（DB）中注册一个PE镜像的SHA256认证信息。
Device Guard Ready	设备保护就绪。
Remove 'UEFI CA' from DB	从数据中移除“UEFI CA”。
Restore DB defaults	恢复数据库默认值。
Platform Key(PK)	平台密钥配置，菜单选项为： <ul style="list-style-type: none"> <li>• Update：更新密钥。</li> </ul>

界面参数	功能说明
Key Exchange Keys	交换密钥设置，菜单选项为： <ul style="list-style-type: none"> <li>• Update: 更新密钥。</li> <li>• Append: 添加密钥。</li> </ul>
Authorized Signatures	经授权的签名，菜单选项为： <ul style="list-style-type: none"> <li>• Update: 更新密钥。</li> <li>• Append: 添加密钥。</li> </ul>
Forbidden Signatures	被禁止的签名，菜单选项为： <ul style="list-style-type: none"> <li>• Update: 更新密钥。</li> <li>• Append: 添加密钥。</li> </ul>
Authorized TimeStamps	经授权的时间戳，菜单选项为： <ul style="list-style-type: none"> <li>• Update: 更新密钥。</li> <li>• Append: 添加密钥。</li> </ul>
OsRecovery Signatures	系统恢复的签名，菜单选项为： <ul style="list-style-type: none"> <li>• Update: 更新密钥。</li> <li>• Append: 添加密钥。</li> </ul>

### 3.7 Boot界面

Boot界面如[图 3-130](#)所示，主要包含设置服务器的启动顺序、BIOS的启动模式等。具体参数说明如[表 3-118](#)所示。

图3-130 Boot 界面

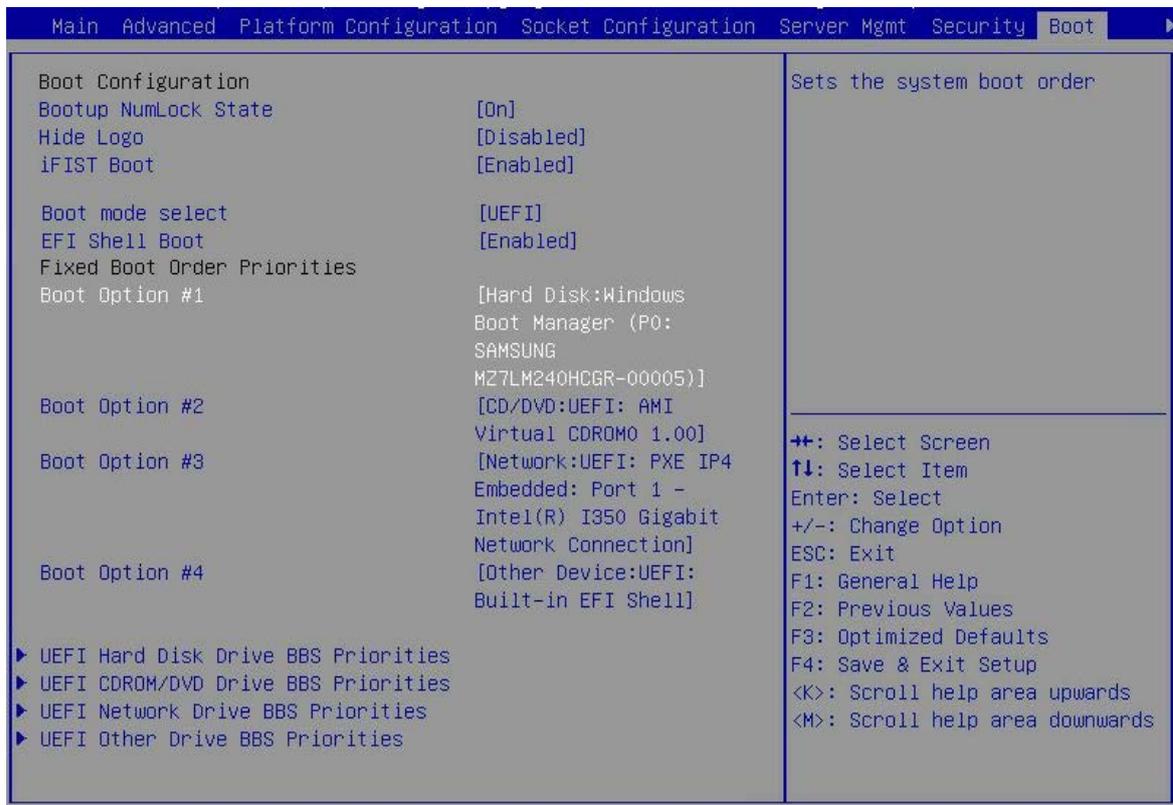


表3-118 Boot 界面参数

界面参数	功能说明
Bootup NumLock State	启动后键盘上数字锁定键状态设置，菜单选项为： <ul style="list-style-type: none"> <li>On（缺省）：打开启动后键盘上数字锁定键状态。</li> <li>Off：关闭启动后键盘上数字锁定键状态。</li> </ul>
Hide Logo	启动界面的Logo显示设置。菜单选项为： <ul style="list-style-type: none"> <li>Disabled（缺省）：显示启动界面的 Logo。</li> <li>Enabled：隐藏启动界面的 Logo。</li> </ul>
iFIST Boot	iFIST功能设置。菜单选项为： <ul style="list-style-type: none"> <li>Disabled：禁用iFIST功能。禁用后，图 2-1 BIOS启动界面中的iFIST Boot按钮将隐藏，且按F10将无法启动iFIST。</li> <li>Enabled（缺省）：启用 iFIST 功能。</li> </ul>
Boot Mode Select	启动模式选择设置，菜单选项为： <ul style="list-style-type: none"> <li>LEGACY：Legacy 启动模式。</li> <li>UEFI（缺省）：UEFI 启动模式。</li> </ul>
EFI Shell Boot	Shell启动开关。Shell是EFI 内置的命令行。菜单选项为： <ul style="list-style-type: none"> <li>Disabled（缺省）：禁用 shell。</li> <li>Enabled：设置 Enable 后，显示 Shell 启动项。</li> </ul>

界面参数	功能说明
Fixed Boot Order Priorities	启动优先级配置菜单。
Boot Option #1	设置系统的第1启动选项。可通过Disabled选项禁用启动项。
Boot Option #2	设置系统的第2启动选项。可通过Disabled选项禁用启动项。
Boot Option #3	设置系统的第3启动选项。可通过Disabled选项禁用启动项。
Boot Option #4	设置系统的第4启动选项。可通过Disabled选项禁用启动项。
UEFI Hard Disk Drive BBS Priorities (UEFI启动模式) / Hard Disk Drive BBS Priorities (Legacy启动模式)	硬盘、USB启动优先级配置菜单，从可用的硬盘驱动和USB中指定启动设备的优先级顺序。
UEFI CDROM/DVD Drive BBS Priorities (UEFI启动模式) / CDROM/DVD Drive BBS Priorities (Legacy启动模式)	光驱启动优先级配置菜单，从可用的光驱中指定启动设备的优先级顺序。当连接可启动介质的光驱时，显示该菜单。
UEFI Network Drive BBS Priorities (UEFI启动模式) / Network Drive BBS Priorities (Legacy启动模式)	网络启动优先级配置菜单，从可用的网络中指定启动的优先级顺序。
UEFI Other Drive BBS Priorities	其他设备启动优先级配置菜单，EFI Shell Boot选项设置为Enabled时，显示该菜单。

UEFI Hard Disk Drive BBS Priorities界面如[图 3-131](#)所示。具体参数如[表 3-119](#)所示。

图3-131 UEFI Hard Disk Drive BBS Priorities 界面

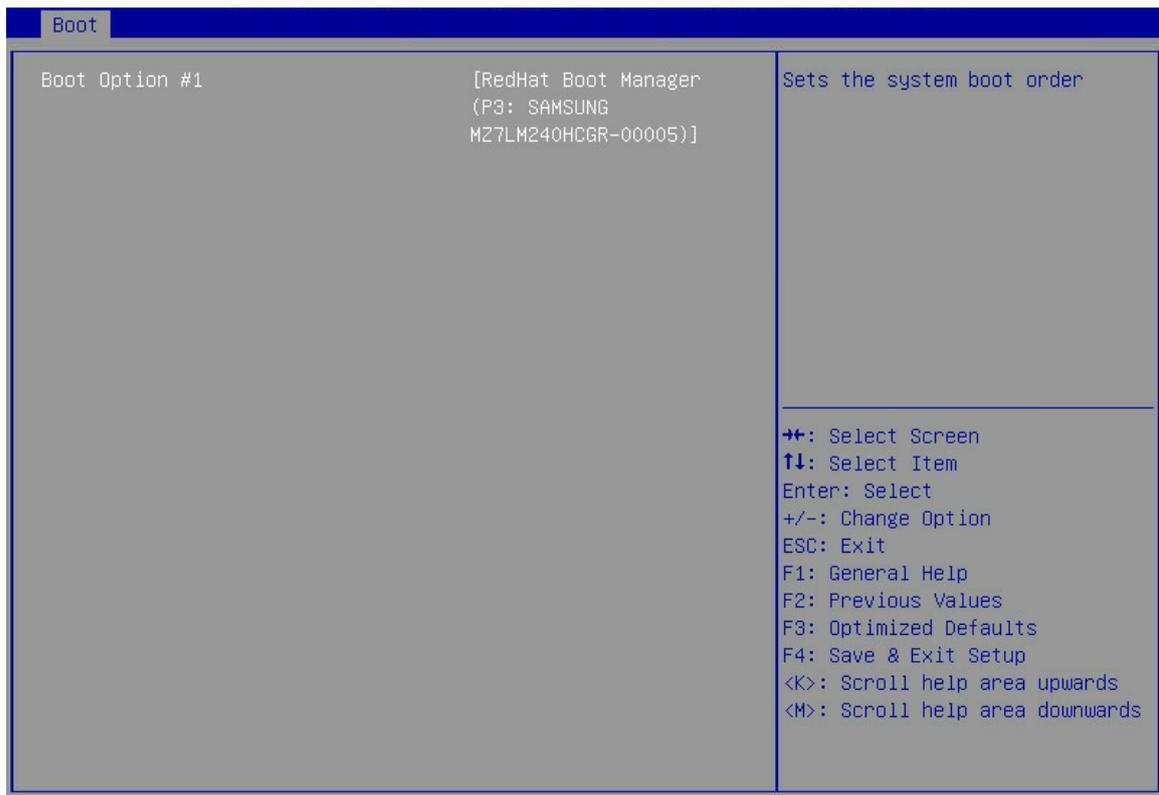


表3-119 UEFI Hard Disk Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的硬盘启动设备。</li> </ul>

UEFI CDROM/DVD Drive BBS Priorities界面如[图 3-132](#)所示。具体参数如[表 3-120](#)所示。

图3-132 UEFI CDROM/DVD Drive BBS Priorities 界面



表3-120 UEFI CDROM/DVD Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的光盘启动设备。</li> </ul>

UEFI Network Drive BBS Priorities界面如[图 3-133](#)所示。具体参数如[表 3-121](#)所示。

图3-133 UEFI Network Drive BBS Priorities 界面

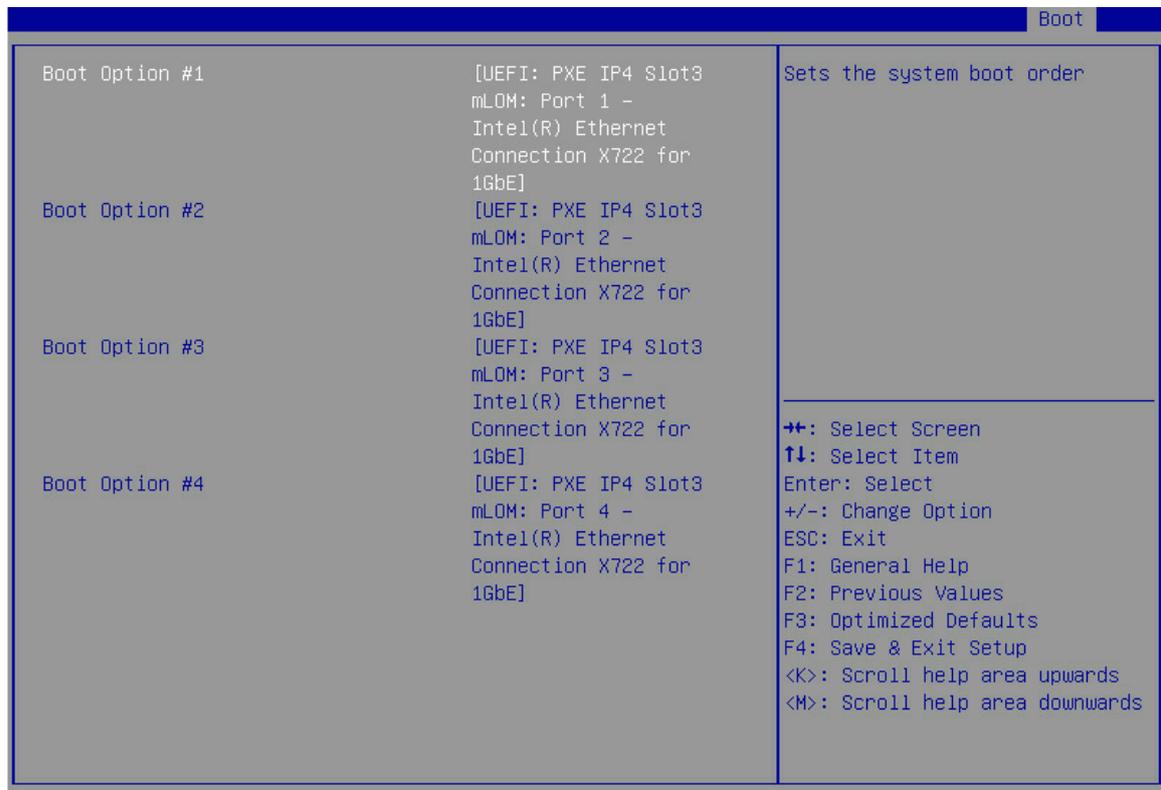


表3-121 UEFI Network Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的 PXE 启动设备。</li> </ul>
Boot Option #2	第2启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的 PXE 启动设备。</li> </ul>
Boot Option #3	第3启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的 PXE 启动设备。</li> </ul>
Boot Option #4	第4启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的 PXE 启动设备。</li> </ul>

UEFI Other Drive BBS Priorities界面如[图 3-134](#)所示。具体参数如[表 3-122](#)所示。

图3-134 UEFI Other Drive BBS Priorities 界面

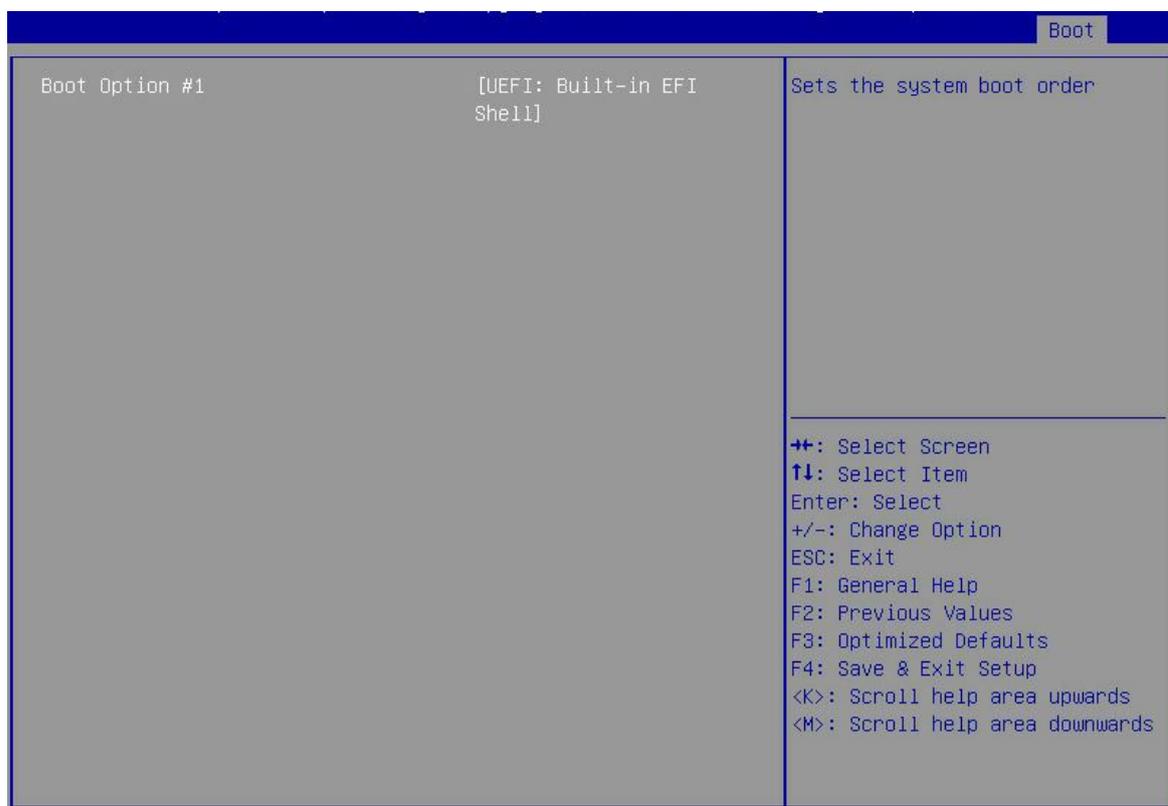


表3-122 UEFI Other Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项。菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用该启动项。</li> <li>• 可选择的其他启动设备。</li> </ul>

 说明

Legacy启动模式下，当服务器连接多个同一类的启动项时，本文以Hard Disk举例。Fixed Boot Order Priorities栏仅显示Hard Disk Drive BBS Priorities界面的第一启动项。如果您需要服务器从Hard Disk的其他启动项启动，此时请进入Hard Disk Drive BBS Priorities界面将对应的启动项设置为该分类的第一启动项，具体方法与[2.11 设置服务器启动顺序](#)的方法类似。

### 3.8 Save & Exit界面

Save & Exit界面如[图 3-135](#)所示，主要包含控制BIOS参数修改及退出功能。具体参数说明如[表 3-123](#)所示。

图3-135 Save & Exit 界面

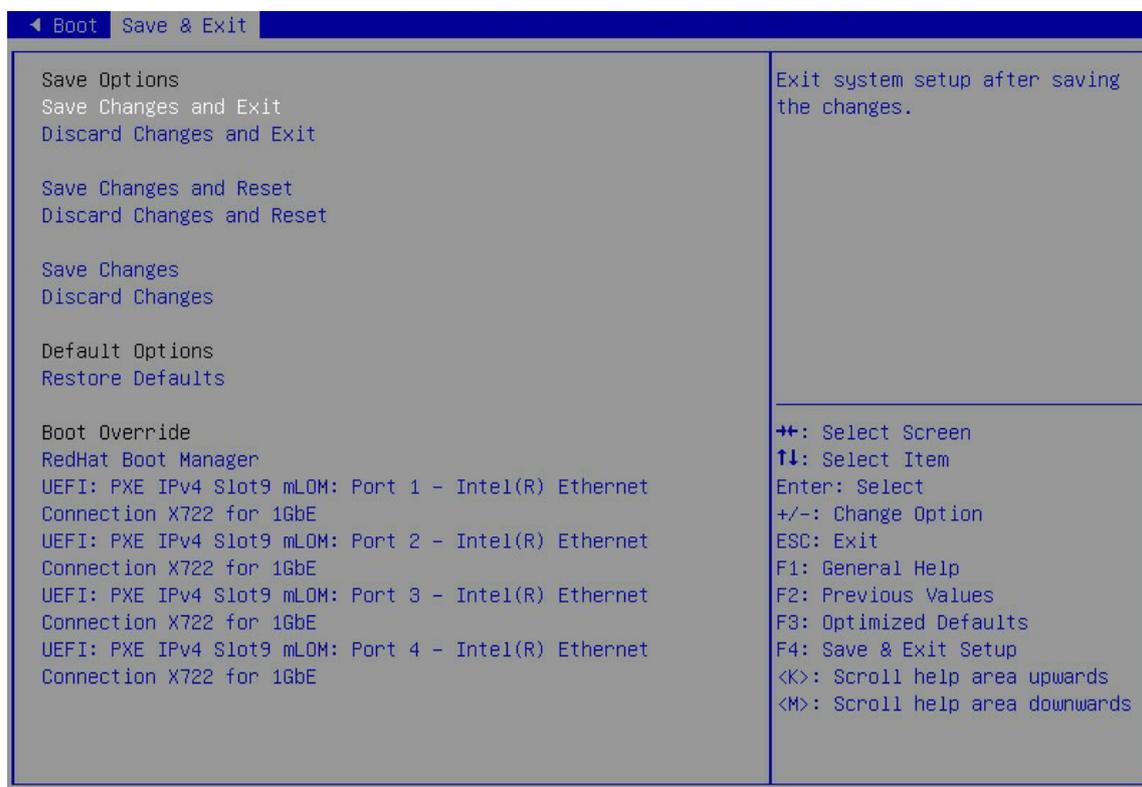


表3-123 Save & Exit 界面参数

界面参数	功能说明
<b>Save Options</b>	
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	保存修改并重启服务器。
Discard Changes and Reset	放弃修改并重启服务器。
Save Changes	保存修改。
Discard Changes	放弃修改。
<b>Default Options</b>	
Restore Defaults	恢复缺省设置。

界面参数	功能说明
<b>Boot Override</b>	<p>选择从以下启动项启动。您可以通过在BIOS启动界面（<a href="#">图2-1</a>）按<b>F7</b>进入Boot Menu界面，选择对应的启动项。</p> <p>需要注意的是，修改了BIOS Setup界面的参数但没有保存的情况下，选择Boot Override中任一启动项，会弹出Save &amp; Reset对话框，在对话框中，可执行以下操作：</p> <ul style="list-style-type: none"> <li>• <b>Yes:</b> 选择Yes，系统会保存修改并重启，并不会从您选择的启动项启动。</li> <li>• <b>No:</b> 选择No，对话框会自动关闭，此时系统不会从您选择的启动项启动。您可以放弃当前修改（方法：选择<a href="#">图 3-135</a>中的Discard Changes或按<b>F2</b>快捷键），重新选择Boot Override中的任一启动项，系统会立即从该启动项启动。</li> </ul>
UEFI: PXE IPv4 Slot9 mLOM: Port x – Intel(R) Ethernet Connection X722 for 1GbE (UEFI启动模式) / IBA 40G Slot 3D00 v1066 (Legacy启动模式)	<p>网卡的端口x与IPv4 PXE服务器相连时，您可以选择从该启动项启动。</p>

# 4 缩略语

表4-1 缩略语

缩略语	英文解释	中文解释
<b>A</b>		
ACPI	Advanced Configuration and Power Interface	高级配置和电源接口
AHCI	Advanced Host Controller Interface	高级主机控制器接口
<b>B</b>		
BIOS	Basic Input Output System	基本输入输出系统
<b>C</b>		
COD	Cluster On Die	芯片集群
CFG	Config	配置
CSM	Compatibility Support Module	兼容性支持模块
<b>D</b>		
DCU	Drive Control Unit	驱动控制单元
DMA	Direct Memory Access	直接存储器存取
DRAM	Dynamic Random Access Memory	动态随机存取存储器
DCPMM	Intel® Optane™ DC PMEM module	Intel制造的下一代非易失性存储器
<b>E</b>		
ECC	Error Checking and Correcting	差错校验纠正
EFI	Extensible Firmware Interface	可扩展固件接口
EIST	Enhanced Intel SpeedStep Technology	智能降频技术
EMS	Emergency Management Services	紧急管理服务
EMCA	Enhanced Machine Check Architecture	高级机器校验架构
<b>G</b>		
GPU	Graphics Processing Unit	图形处理器
<b>H</b>		
HBA	Host Bus Adapter	主机总线适配器
HDM	Hardware Device Management	设备管理
<b>I</b>		
IDE	Integrated Drive Electronics	电子集成驱动器
IIO	Integrated I/O Module	集成I/O模块

缩略语	英文解释	中文解释
IMC	Integrated Memory Controller	集成内存控制器
iSCSI	Internet Small Computer System Interface	互联网小型计算机系统接口
<b>L</b>		
LLC	Last Level Cache	三级缓存
LUN	Logical Unit Number	逻辑单元号
LLDP	Link Layer Discovery Protocol	链路层发现协议
<b>M</b>		
MAC	Media Access Control	介质访问控制
MCTP	Management Component Transport Protocol	管理元件传输协议
ME	Management Engine	管理引擎
MMIO	Memory mapping I/O	内存映射I/O
MRC	Memory Reference Code	内存参考代码
<b>N</b>		
NIC	Network Interface Controller	网口控制器
NMI	Non Maskable Interrupt	非屏蔽中断
NUMA	Non Uniform Memory Access	非统一内存访问
<b>O</b>		
OS	Operating System	操作系统
<b>P</b>		
PCH	Platform Controller Hub	平台控制器中心
PCI	Peripheral Component Interface	外围组件接口
PCIe	Peripheral Component Interconnect Express	外围组件快速互连
PCU	Power Controller Unit	电源控制单元
PECI	Platform Environment Control Interface	平台环境式控制接口
PK	Platform Key	平台密钥
POR	Plan Of Record	计划记录
POST	Power On Self Test	开机自检
PXE	Preboot Execute Environment	预启动执行环境
<b>R</b>		
RAID	Redundant Arrays of Independent Disks	独立磁盘冗余阵列
RAPL	Running Average Power Limit	运行平均功率限制
RAS	Reliability, Availability, Serviceability	可靠性、可用性和可服务性

缩略语	英文解释	中文解释
ROM	Read-Only Memory	只读存储器
RFO	Request For Ownership	请求所有权
RTS/CTS	Request To Send/Clear To Send	请求发送/清除发送协议
<b>S</b>		
SAS	Serial Attached SCSI	串行连接的SCSI
SATA	Serial Advanced Technology Attachment	串行ATA
SCSI	Small Computer System Interface	小型计算机系统接口
SEL	System Event Log	系统事件日志
SMI	System Management Interrupt	系统管理中断
SR-IOV	Single-Root I/O Virtualization	单路I/O虚拟化
SMBIOS	System Management BIOS	以标准格式显示产品管理信息所需遵循的统一规范
<b>T</b>		
TPM	Trusted Platform Module	可信平台模块
TCM	trusted computing platform	可信计算平台
TDP	Thermal Design Power	热设计功耗
TXT	Trusted Execution Technologies	可信执行技术
<b>U</b>		
UEFI	Unified Extensible Firmware Interface	统一的可扩展固件接口
UID	Unit Identification	设备标识
UPI	Ultra Path Interconnect	极速通道互联
<b>V</b>		
VT-d	Intel Virtualization Technology For Directed I/O	英特尔定向I/O虚拟化技术
VGA	Video Graphics Array	视频图形阵列
<b>X</b>		
XHCI	eXtensible Host Controller Interface	可扩展的主机控制器接口