

# H3C 机架式及高密度服务器

## Purley 平台 BIOS 用户指南

新华三技术有限公司

<http://www.h3c.com>

资料版本：6W103-20190308

Copyright © 2017-2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 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，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，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。

## 环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

# 前言

H3C 机架式及高密度服务器 Purley 平台 BIOS 用户指南各章节内容如下：

- **第 1 章 BIOS 简介。**介绍 BIOS 及本手册适用的产品。
- **第 2 章 常用功能。**介绍 BIOS 的常用功能及设置方法，包括设置 HDM 网络信息、设置 BIOS 启动模式、设置服务器启动顺序、恢复 BIOS 缺省设置等。
- **第 3 章 界面参数说明。**介绍 BIOS 界面包含的参数及相关功能。
- **第 4 章 SATA sSATA 端口与背板槽位的对应关系。**介绍 SATA sSATA 端口与背板槽位的对应关系。
- **第 5 章 缩略语。**介绍手册中的缩略语。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

## 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择一个或者不选。
{ 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择一个、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参考，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。

## 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

**E-mail:** [info@h3c.com](mailto:info@h3c.com)

感谢您的反馈，让我们做得更好！

# 目 录

1 BIOS简介.....	1-1
2 常用功能.....	2-1
2.1 进入BIOS界面 .....	2-1
2.2 查询CPU信息 .....	2-5
2.3 查询内存信息.....	2-5
2.4 查询板载硬盘信息.....	2-6
2.5 查询HDM网络信息.....	2-7
2.6 设置HDM网络信息.....	2-8
2.7 设置BIOS密码 .....	2-10
2.8 设置系统日期和时间.....	2-17
2.9 设置BIOS启动模式 .....	2-18
2.10 设置服务器启动顺序.....	2-19
2.11 配置RAID.....	2-21
2.12 恢复BIOS缺省设置.....	2-22
3 界面参数说明.....	3-1
3.1 Main界面 .....	3-1
3.2 Advanced界面 .....	3-3
3.2.1 Intel(R) virtual RAID on CPU界面 .....	3-5
3.2.2 Driver Health界面 .....	3-16
3.2.3 Trusted Computing界面 .....	3-17
3.2.4 ACPI Settings界面 .....	3-22
3.2.5 Serial Port Console Redirection界面 .....	3-23
3.2.6 Slot x:Port x界面.....	3-27
3.2.7 PCI Subsystem Settings界面.....	3-30
3.2.8 Network Stack Configuration界面 .....	3-32
3.2.9 CSM Configuration界面.....	3-33
3.2.10 NVMe Configuration界面 .....	3-34
3.2.11 USB Configuration界面 .....	3-36
3.3 Platform Configuration界面.....	3-38
3.3.1 PCH Configuration界面 .....	3-39
3.3.2 Miscellaneous Configuration界面 .....	3-48
3.3.3 Server ME Configuration界面 .....	3-49

3.3.4 Runtime Error Logging界面.....	3-50
3.4 Socket Configuration界面.....	3-59
3.4.1 Processor Configuration界面.....	3-60
3.4.2 Common RefCode Configuration界面.....	3-63
3.4.3 UPI Configuration界面.....	3-65
3.4.4 Memory Configuration界面.....	3-67
3.4.5 IIO Configuration界面.....	3-75
3.4.6 Advanced Power Management Configuration界面.....	3-89
3.5 Server Management界面.....	3-97
3.6 Security界面.....	3-110
3.7 Boot界面.....	3-116
3.8 Save & Exit界面.....	3-126
<b>4 SATA sSATA端口与背板槽位的对应关系.....</b>	<b>4-1</b>
4.1 H3C UniServer R4900 G3 PCH SATA sSATA相关硬盘背板配置端口.....	4-1
4.2 H3C UniServer R4700 G3 PCH SATA sSATA相关硬盘背板配置端口.....	4-2
4.3 H3C UniServer R2900 G3 PCH SATA sSATA相关硬盘背板配置端口.....	4-3
4.4 H3C UniServer R2700 G3 PCH SATA sSATA相关硬盘背板配置端口.....	4-5
<b>5 缩略语.....</b>	<b>5-1</b>

# 1 BIOS简介



说明

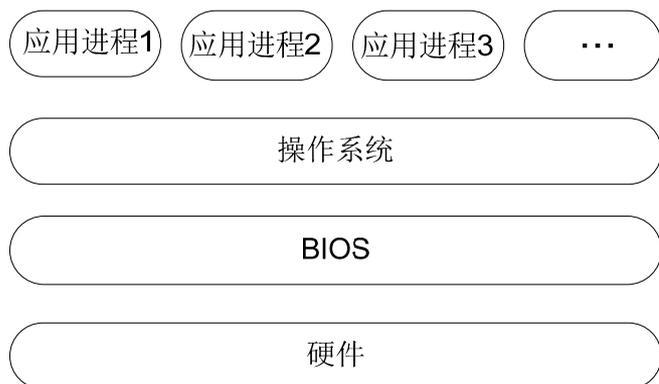
- 由于产品版本升级或其他原因，本文档内容会不定期进行更新。如需查看最新的 BIOS 界面，建议从 H3C 网站获取最新 BIOS 固件版本。
- 本文为产品通用资料。对于定制化产品，请用户以产品实际情况为准。

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，用来设置硬件，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



本手册适用于以下产品：

- H3C UniServer R4900 G3
- H3C UniServer R4700 G3
- H3C UniServer R2900 G3
- H3C UniServer R2700 G3

## 2 常用功能

常用功能如 [表 2-1](#) 所示。

表2-1 BIOS 常用功能

编号	常用功能
1	<a href="#">进入BIOS界面</a>
2	<a href="#">查询CPU信息</a>
3	<a href="#">查询内存信息</a>
4	<a href="#">查询板载硬盘信息</a>
5	<a href="#">查询HDM网络信息</a>
6	<a href="#">设置HDM网络信息</a>
7	<a href="#">设置BIOS密码</a>
8	<a href="#">设置系统日期和时间</a>
9	<a href="#">设置BIOS启动模式</a>
10	<a href="#">设置服务器启动顺序</a>
11	<a href="#">配置RAID</a>
12	<a href="#">恢复BIOS缺省设置</a>

### 2.1 进入BIOS界面

介绍如何进入 BIOS Setup 界面。

#### 1. 操作场景

该功能用于指导工程师在需要系统启动设置或系统信息查询的情况下，进入 BIOS Setup 界面。

#### 2. 操作步骤

(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。



关于启动远程控制台的具体方法，请参见 HDM 联机帮助中的“启动远程控制台”章节。

(2) 启动或重启服务器。

(3) （可选）如 [图 2-1](#) 所示，如果在启动过程中出现输入密码对话框，请在对话框中输入密码。

---

 说明

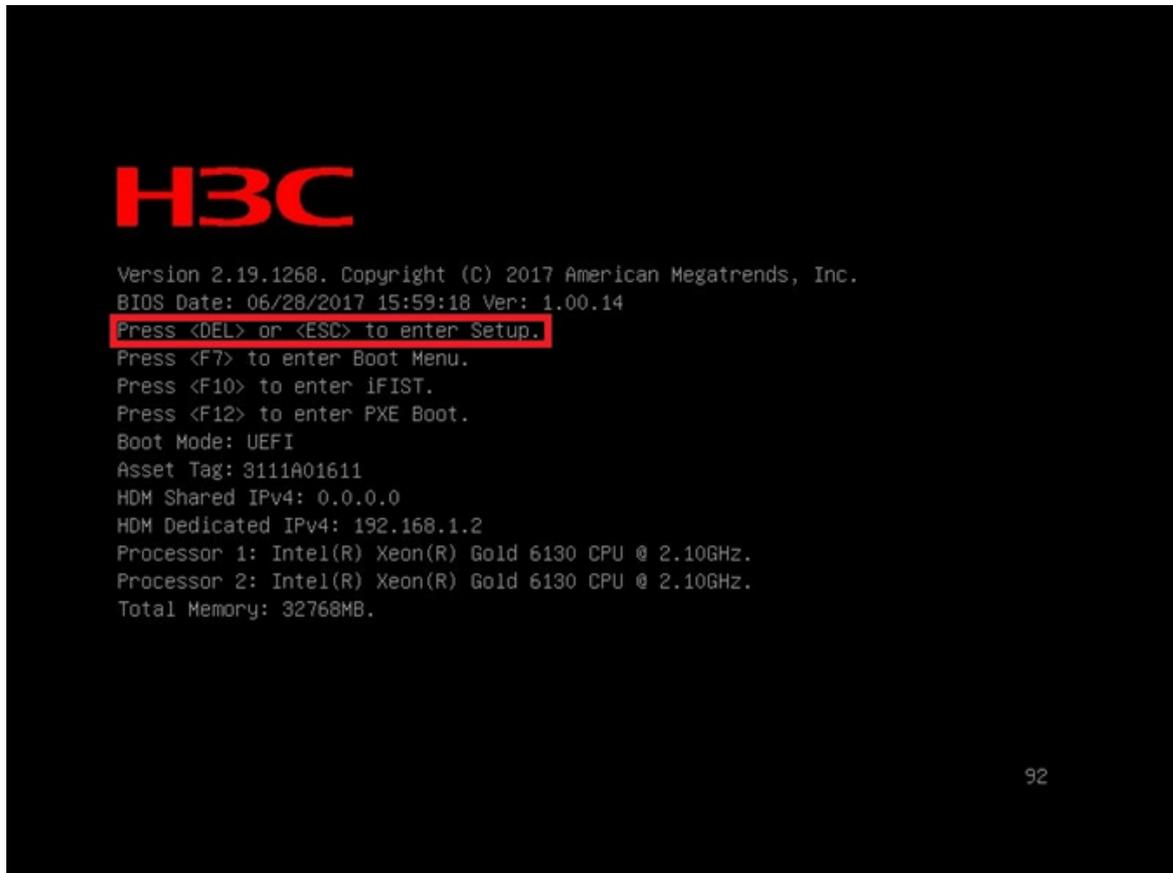
- BIOS缺省没有设置任何密码，设置密码的具体方法请参见 [2.7 设置BIOS密码](#)。
  - 如果连续三次输入错误的密码，服务器会自动重启，稍后请重新输入密码。
  - 如果您忘记了 BIOS 密码，请将服务器下电，然后将机台上的 J111 跳帽连接到 2-3 上，即可清除 BIOS Password。服务器重新上电时，系统将清除 BIOS 的密码。系统维护开关的具体位置，请参见用户指南中的“系统维护开关”章节。
- 

图2-1 输入密码



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

图2-2 BIOS 启动界面



- (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 2-2](#) 所示。

图2-3 BIOS Setup 界面

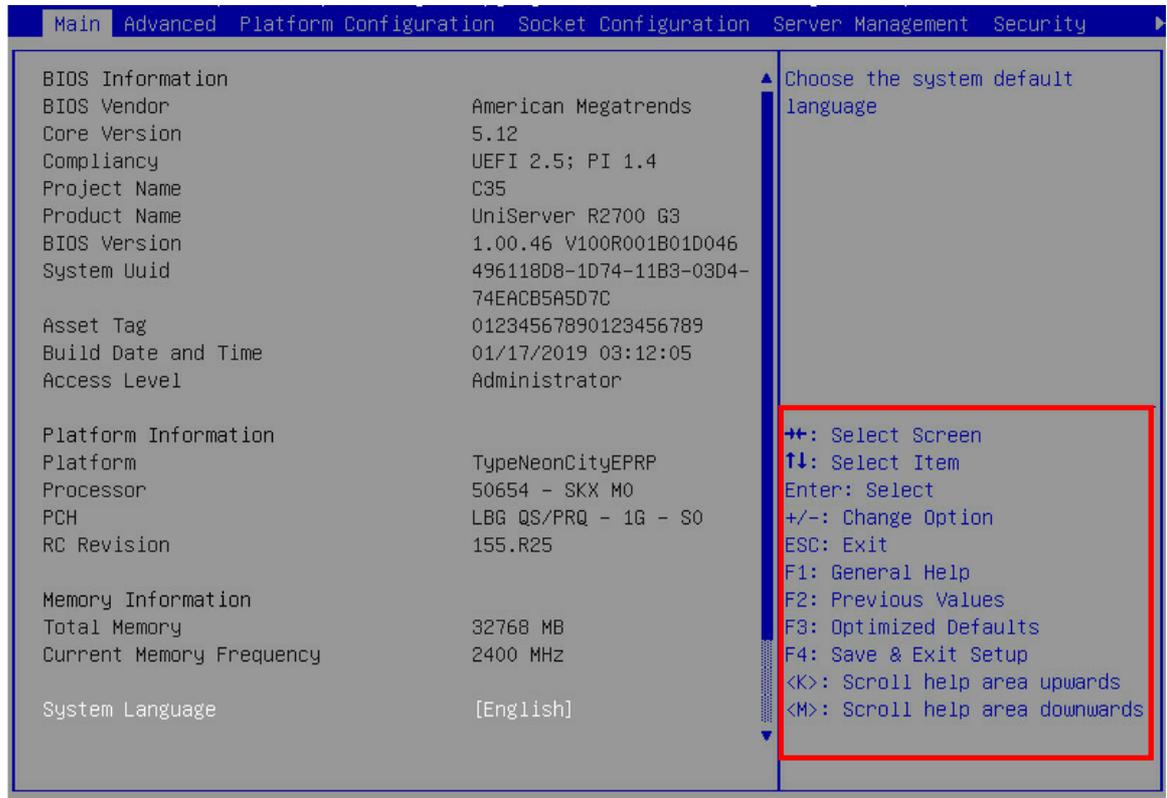


表2-2 操作说明

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界面或从子菜单返回主菜单
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 查询CPU信息

介绍如何查询服务器 CPU 的参数信息。

### 1. 操作场景

该功能用于指导工程师通过BIOS查询服务器CPU的参数信息。CPU的Processor Configuration界面的详细信息请参见 [3.4.1 Processor Configuration界面](#)。

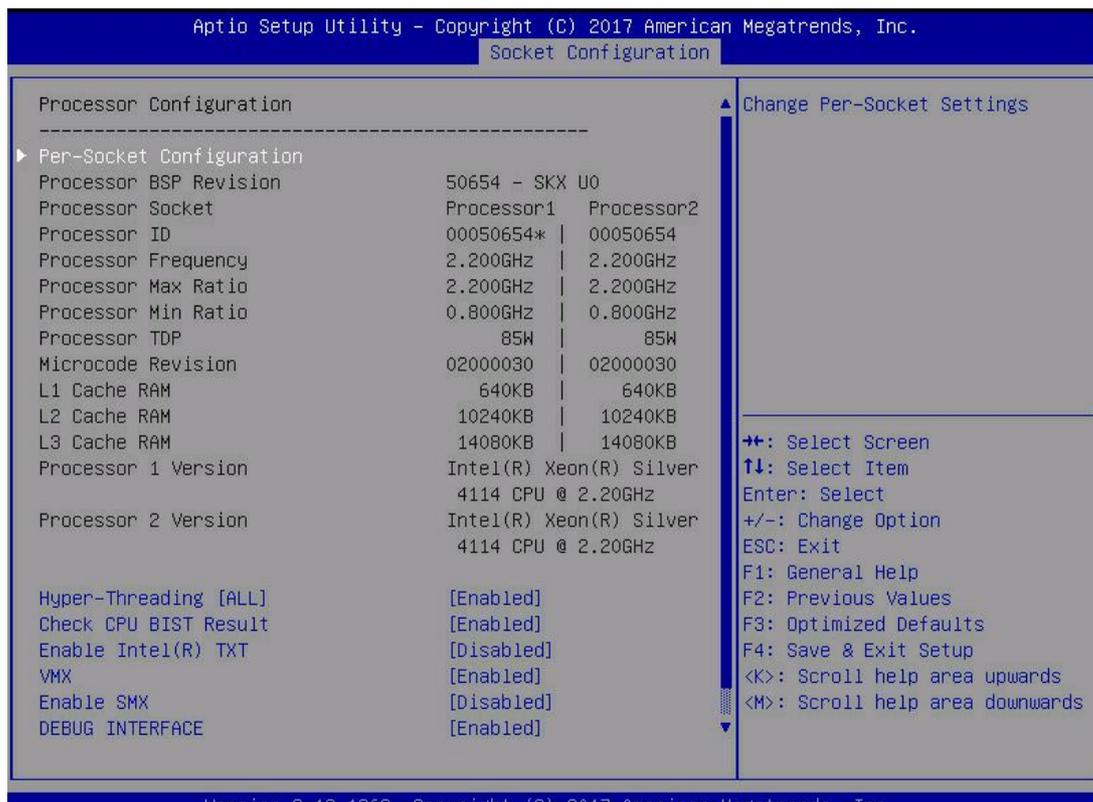
### 2. 准备工作

进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

### 3. 操作步骤

- (1) 在 BIOS Setup 界面中，选择 **Socket Configuration** 页签 > **Processor Configuration**，然后按 **Enter**。
- (2) 如 [图 2-4](#) 所示，进入Processor Configuration界面，显示所有CPU的详细信息。

图2-4 Processor Configuration 界面



## 2.3 查询内存信息

介绍如何查询服务器内存的参数信息。

## 1. 操作场景

该功能用于指导工程师通过BIOS查询服务器内存的参数信息。内存的Memory Configuration界面的详细信息请参见 [3.4.4 Memory Configuration界面](#)。

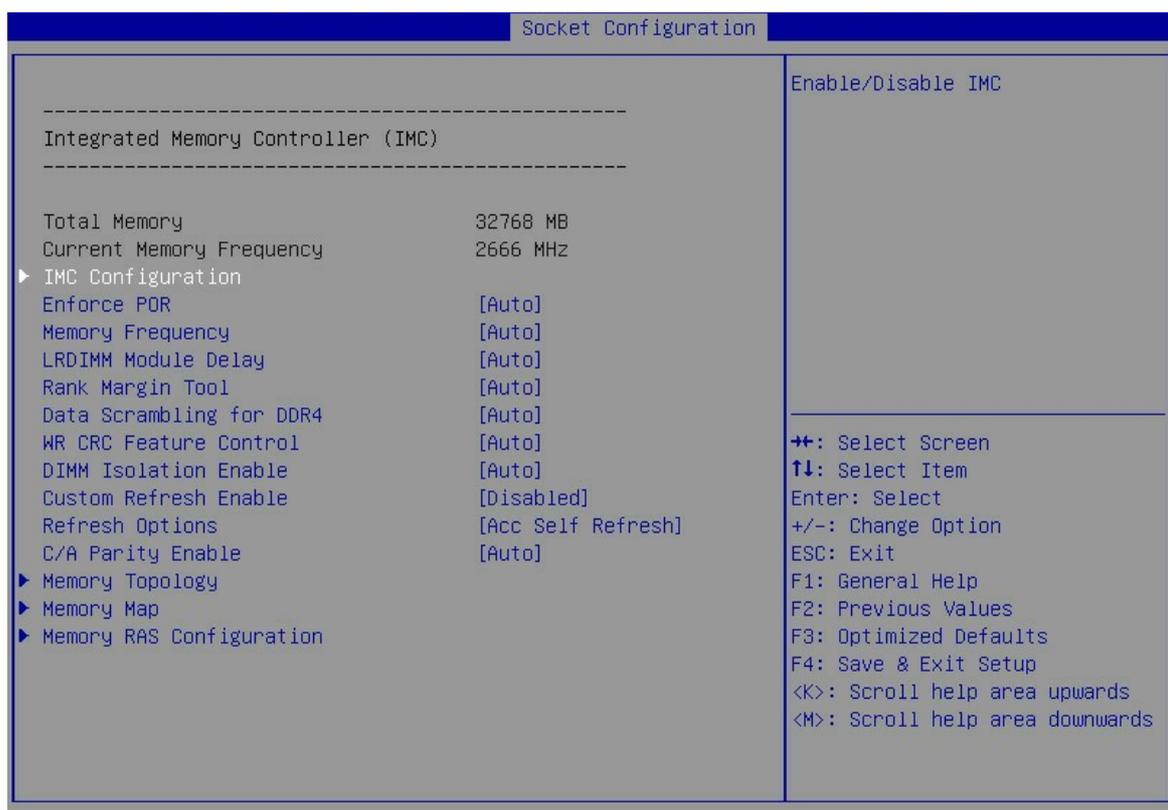
## 2. 准备工作

进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

## 3. 操作步骤

- (1) 在 BIOS Setup 界面中，选择 **Socket Configuration** 页签 > **Memory Configuration**，然后按 **Enter**。
- (2) 如 [图 2-5](#) 所示，进入Memory Configuration界面，显示内存的容量和频率信息，详细的单个DIMM信息可以通过进入Memory Topology菜单进行查看。

图2-5 Memory Configuration 界面



## 2.4 查询板载硬盘信息

介绍如何查询服务器的板载硬盘信息。

### 1. 操作场景

该功能用于指导工程师通过 BIOS 查询服务器的板载硬盘信息。

### 2. 准备工作

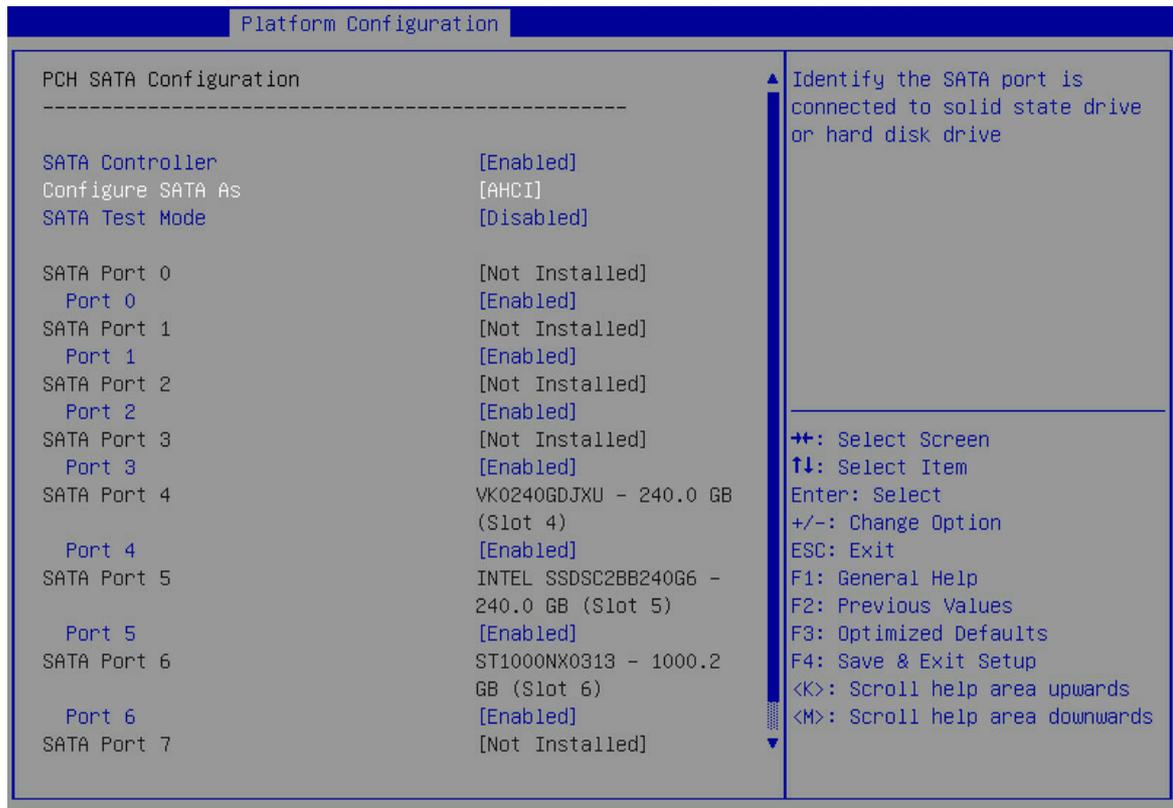
进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

### 3. 操作步骤

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 [图 3-33](#)。

- (1) 在 BIOS Setup 界面中，选择 **Platform Configuration** 页签 > **PCH Configuration** > **PCH SATA Configuration**，然后按 **Enter**。
- (2) 如 [图 2-6](#) 所示，进入 PCH SATA Configuration 界面，显示硬盘信息。

图2-6 PCH SATA Configuration 界面



## 2.5 查询HDM网络信息

介绍如何查询 HDM 的网络信息。

### 1. 操作场景

该功能用于指导工程师通过 BIOS 查询服务器 HDM 的网络信息。

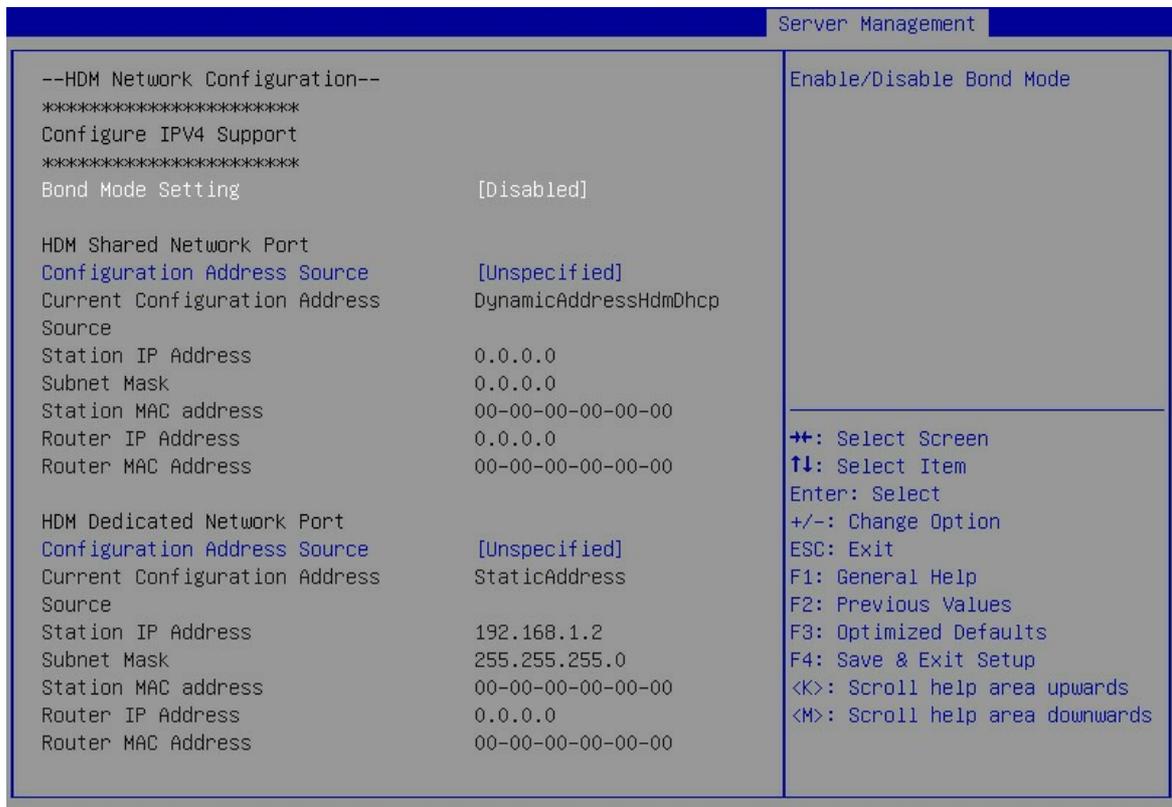
### 2. 准备工作

进入服务器的 BIOS Setup 界面，具体步骤请参见 [2.1 进入 BIOS 界面](#)。

### 3. 操作步骤

- (1) 在 BIOS Setup 界面中，选择 **Server Management** 页签 > **HDM Network Configuration**，然后按 **Enter**。
- (2) 如 [图 2-7](#) 所示，进入 HDM Network Configuration 界面，显示 HDM 网络信息。

图2-7 HDM Network Configuration 界面



## 2.6 设置HDM网络信息



说明

Bond Mode Setting 设置为 Enabled 时，HDM Network Configuration 界面仅显示 HDM Bonding Network Port（HDM Bonding 网络接口）的网络信息，HDM Bonding 网络接口和 HDM 专用/共享网络接口的界面参数相同，本文以配置 HDM 专用/共享网络接口的网络信息进行举例。

### 1. 操作场景

该功能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/共享网络接口的 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

- 操作准备

进入服务器的 BIOS Setup 界面，具体步骤请参见 [2.1 进入 BIOS 界面](#)。

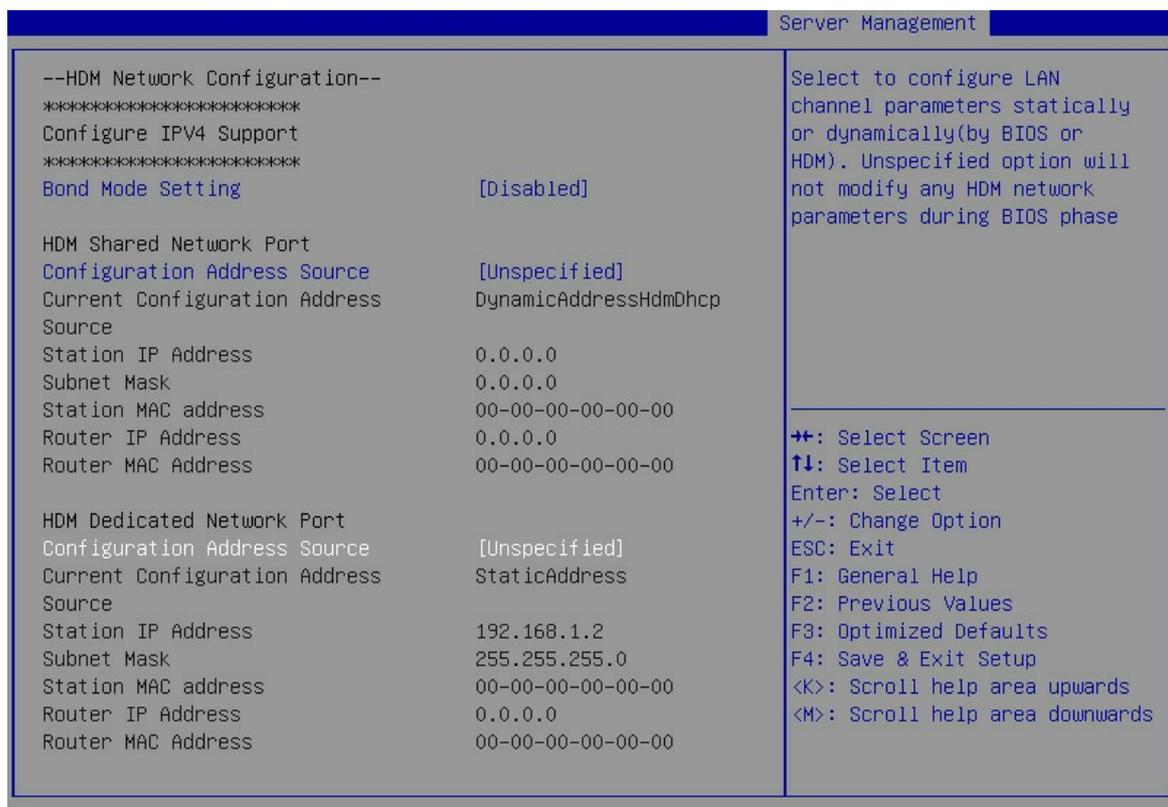
- 数据准备

HDM IP 地址、子网掩码和网关 IP 地址。

### 3. 操作步骤

- (1) 在 BIOS Setup 界面中，选择 **Server Management** 页签 > **HDM Network Configuration**，然后按 **Enter**。
- (2) 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

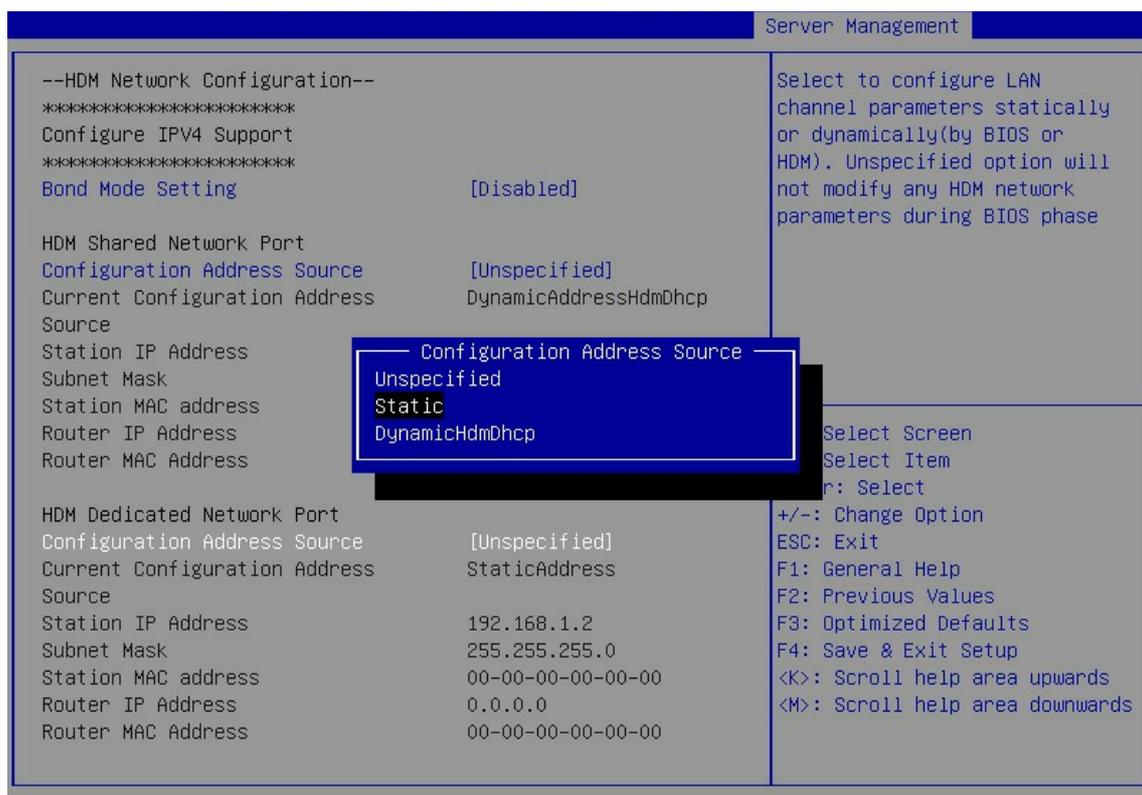


- (3) 有 HDM Shared Network Port (HDM 共享网络接口) 和 HDM Dedicated Network Port (HDM 专用网络接口) 可供选择, 需要注意的是, 为了避免引起网络风暴, HDM 共享网络接口和 HDM 专用网络接口的 IP 地址不可配置为同一网段。本文以配置 HDM Dedicated Network Port 的网络信息为例, 选择 HDM Dedicated Network Port 下的 **Configuration Address Source**, 按 **Enter**。
- (4) 在弹出的对话框中选择 HDM 网络信息的获取方式。HDM 专用/共享网络接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 2-9](#) 所示:
  - 选择 **Unspecified** 或者 **DynamicHdmDhcp** 后, 请按 **Enter**。
  - 选择 **Static** 后, 请分别选择 [表 2-3](#) 中的参数, 在弹出的对话框中输入相关信息, 然后按 **Enter**。

表2-3 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
Router MAC Address	网关MAC地址	可选

图2-9 HDM Network Configuration 界面



(6) 设置完成后，按 **F4** 保存设置，服务器会自动重启。

## 2.7 设置BIOS密码

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。

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。

设置管理员密码和用户密码后，进入系统时，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。

## 1. 操作场景

该功能用于指导工程师，通过 BIOS 设置管理员密码和用户密码。

## 2. 准备工作

进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

## 3. 操作步骤

- 设置管理员密码

(1) 如 [图 2-10](#) 所示，选择**Security**页签 > **Administrator Password**，按**Enter**。

图2-10 设置管理员密码



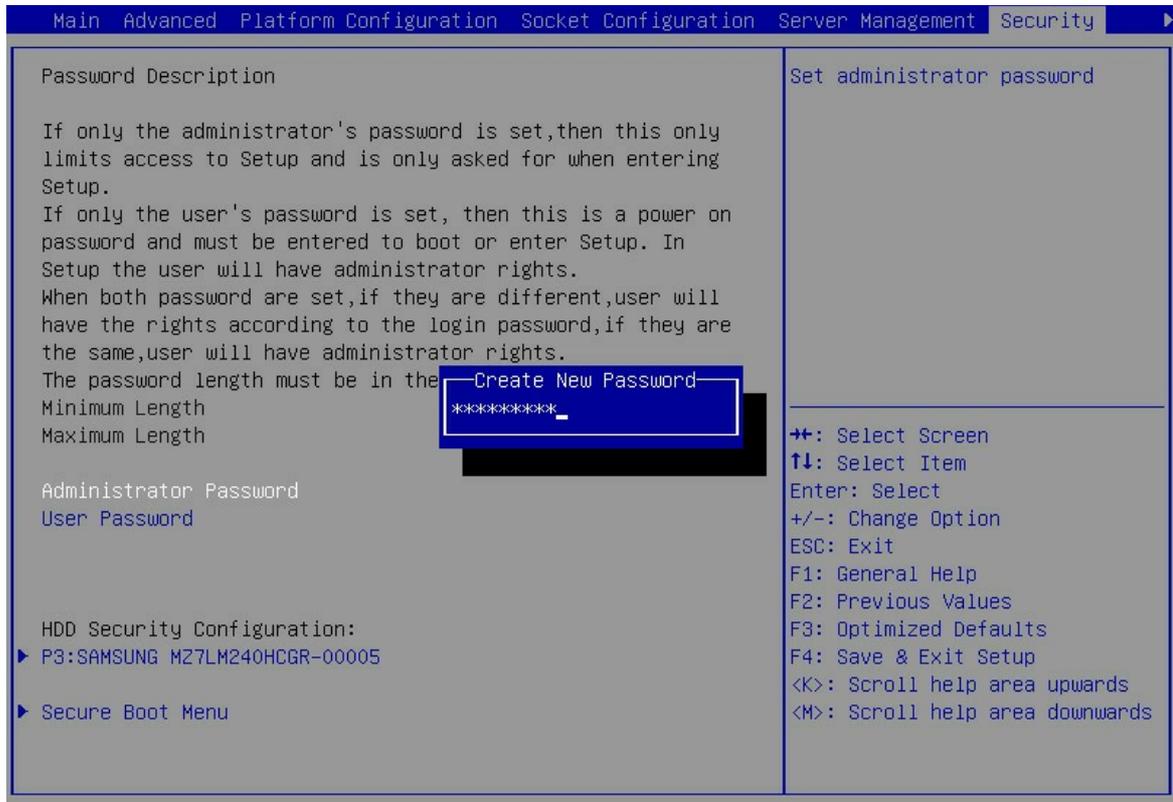
(2) 进入 [图 2-11](#) 所示界面，在弹出的对话框中输入管理员密码，按**Enter**。

### 说明

密码设置需符合以下要求：

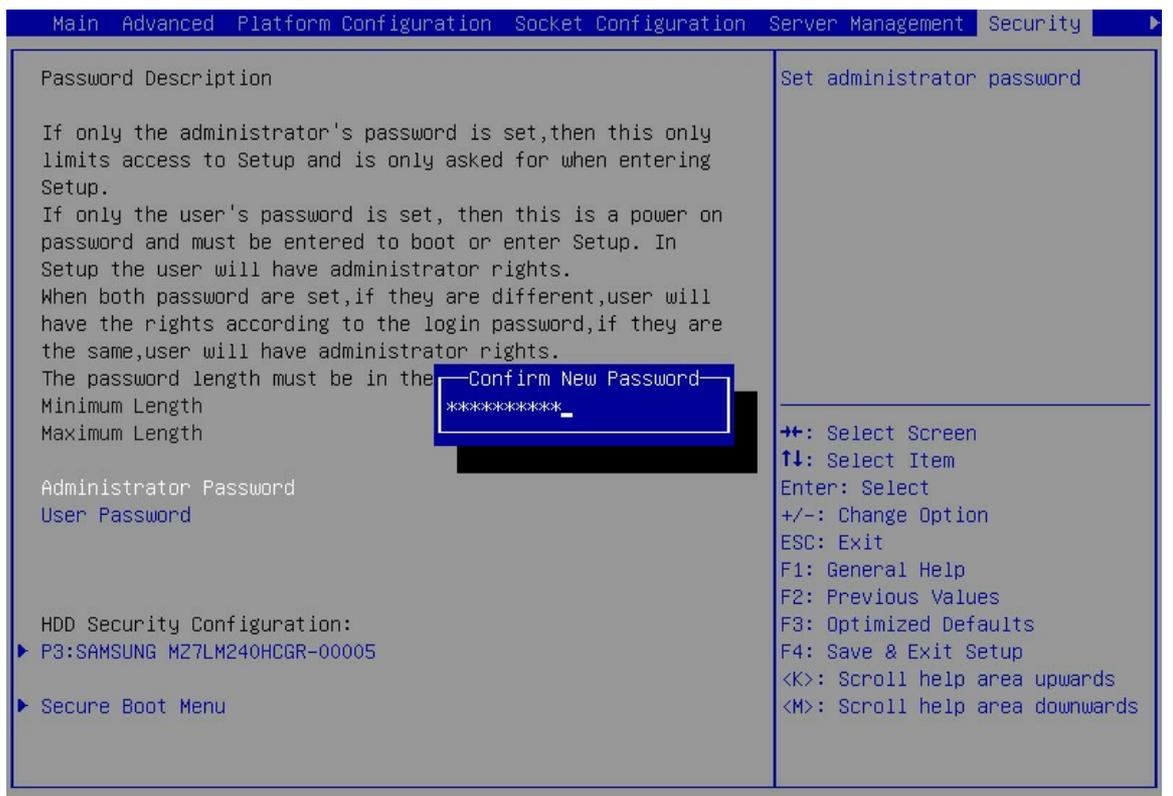
- 密码长度为 8 ~ 20 个字符，仅支持字母、数字、空格和特殊字符  
`~!@#%&\*( )\_+=[\{}|;: ",./<>?`，区分大小写；
- 至少包含大写字母、小写字母和数字中的两种字符；
- 至少包含一个空格或特殊字符。

图2-11 输入管理员密码



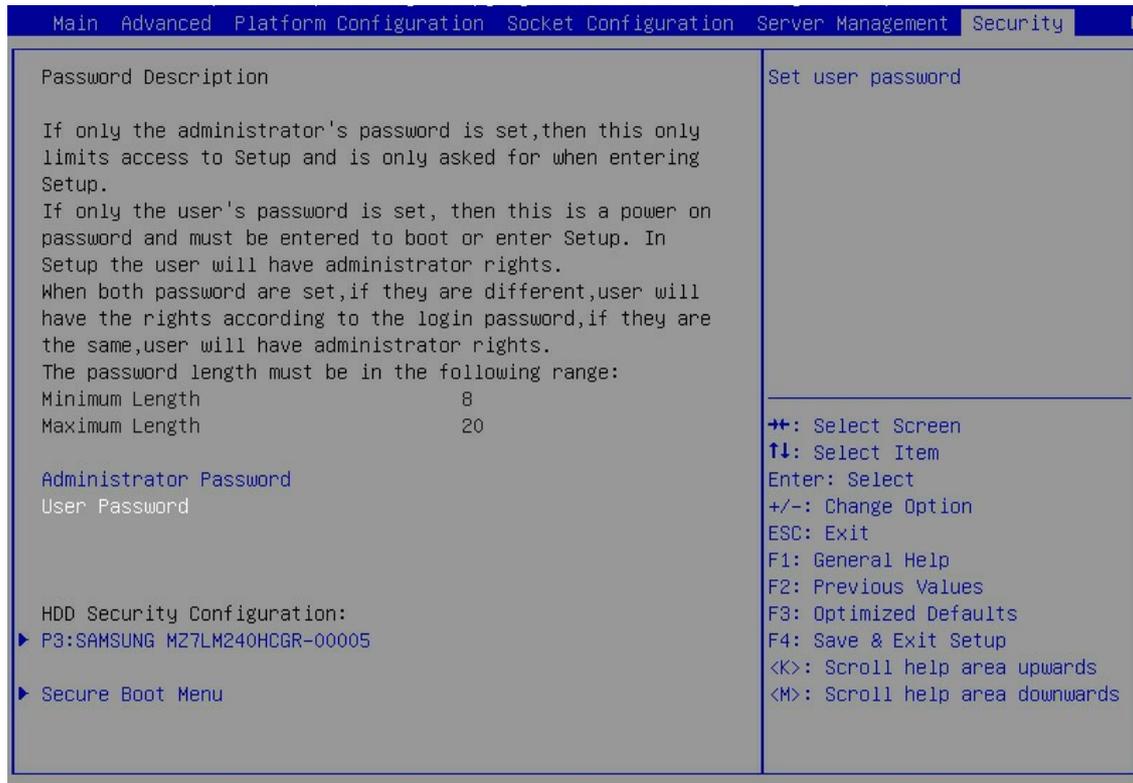
(3) 进入图2-12所示界面，再次输入密码，按Enter。

图2-12 确认管理员密码



- (4) 设置完成后，按 **F4** 保存设置，服务器会自动重启。
- 设置用户密码
- (5) 如 [图 2-13](#) 所示，选择 **Security** 页签 > **User Password**，按 **Enter**。

图2-13 设置用户密码



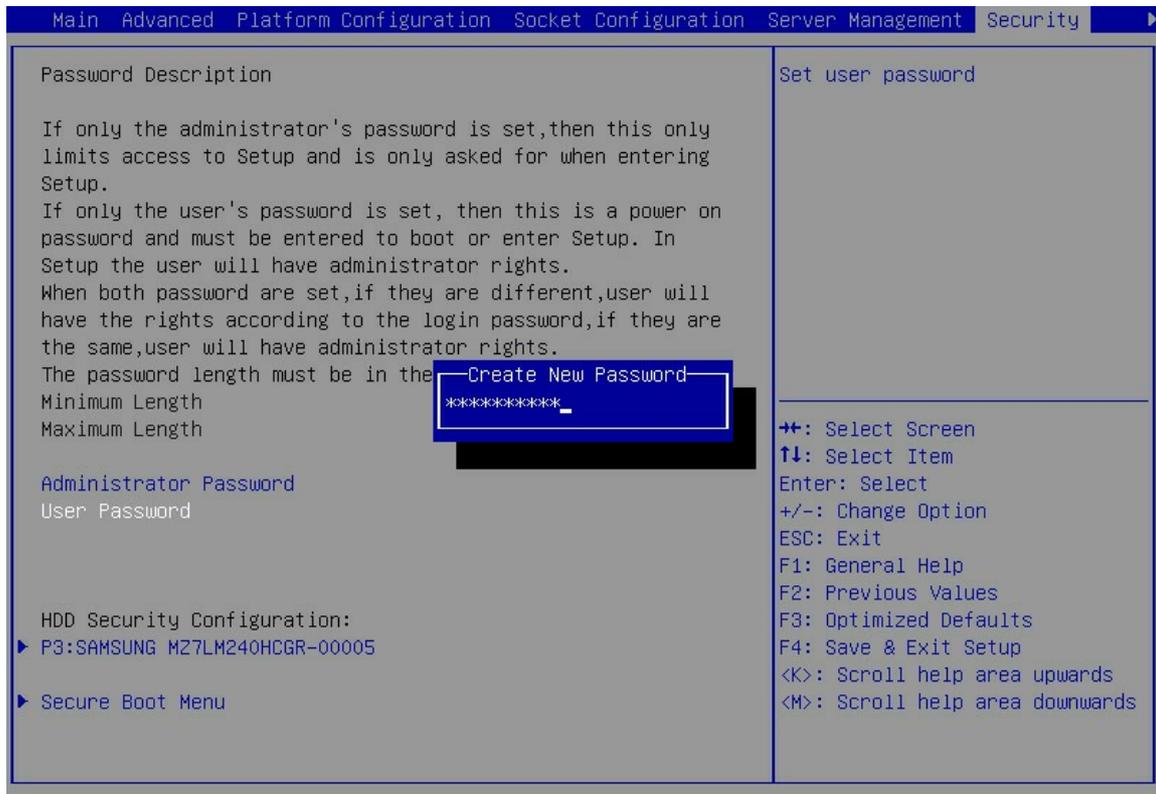
- (6) 进入 [图 2-14](#) 所示界面，在弹出的对话框中输入用户密码，按 **Enter**。

 说明

密码设置需符合以下要求：

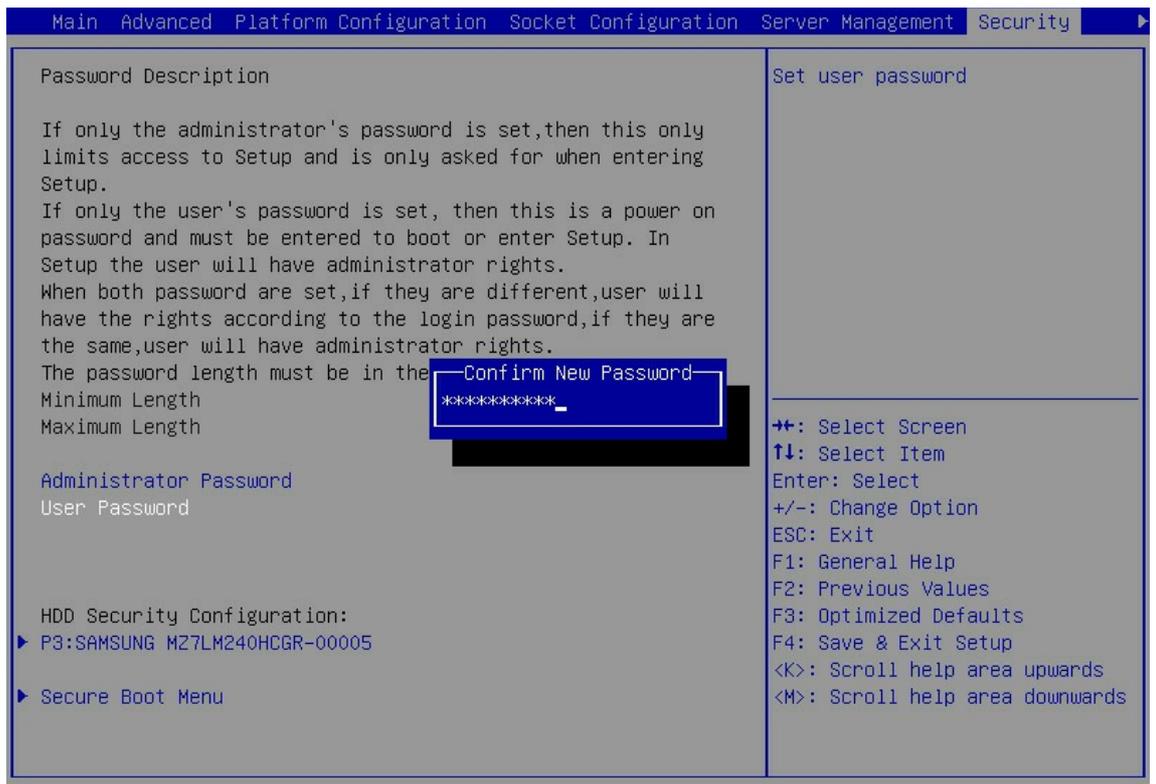
- 密码长度为 8 ~ 20 个字符，仅支持字母、数字、空格和特殊字符  
`~!@#\$%^&\*()\_+=[\{}|;':",./<>?`，区分大小写；
- 至少包含大写字母、小写字母和数字中的两种字符；
- 至少包含一个空格或特殊字符。

图2-14 输入用户密码



(7) 进入图2-15所示界面，再次输入密码，按Enter。

图2-15 确认用户密码



(8) 设置完成后，按 **F4** 保存设置，服务器会自动重启。

- 清除 BIOS 密码

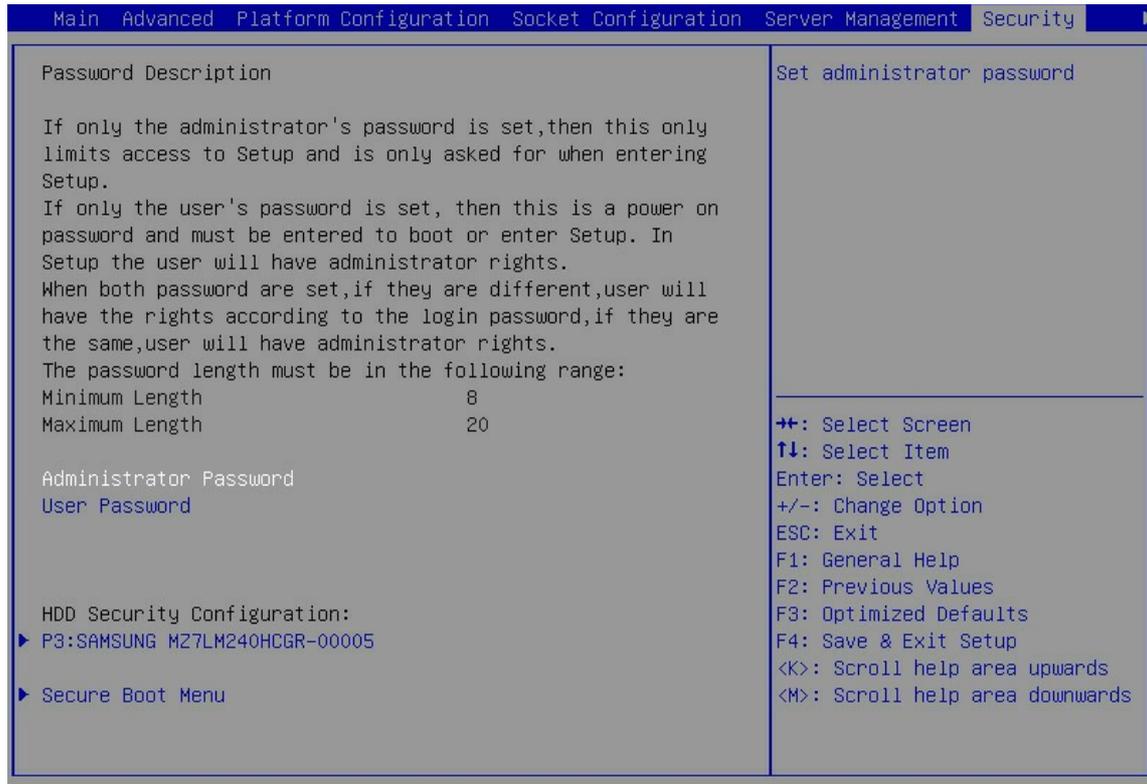


说明

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。

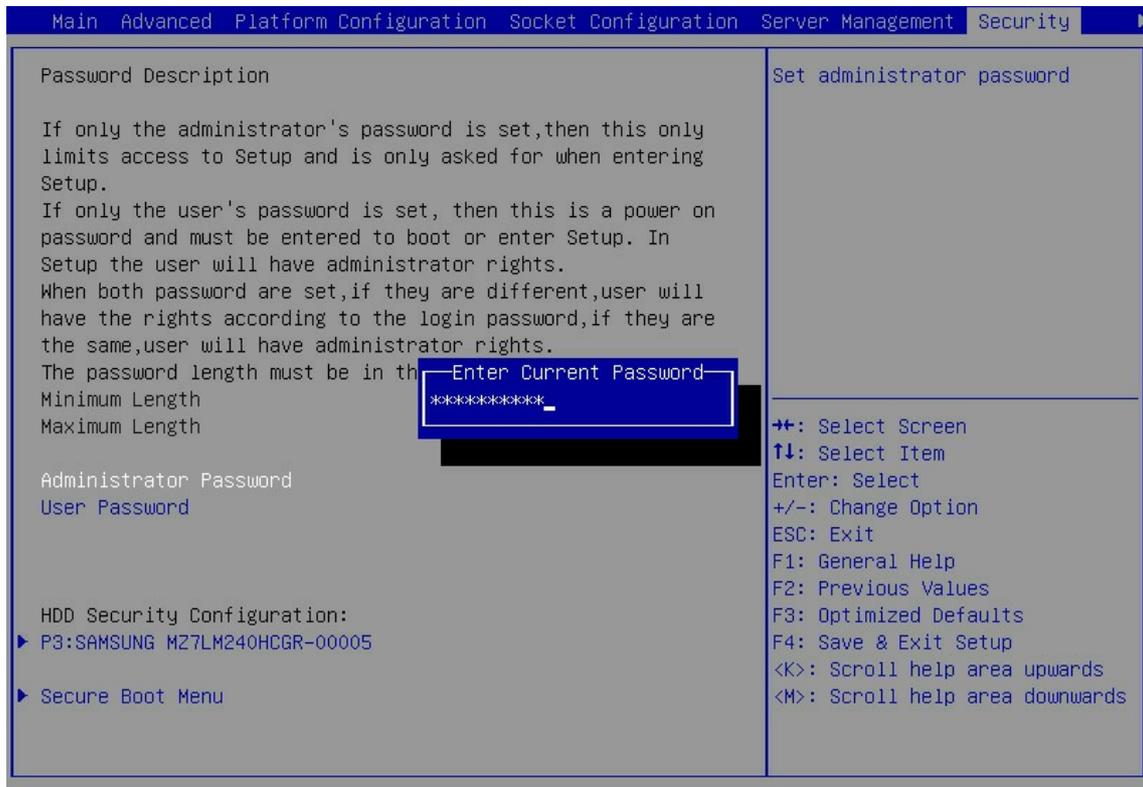
(9) 如 [图 2-16](#) 所示，选择 **Security** 页签 > **Administrator Password**，按 **Enter**。

图2-16 选择管理员密码



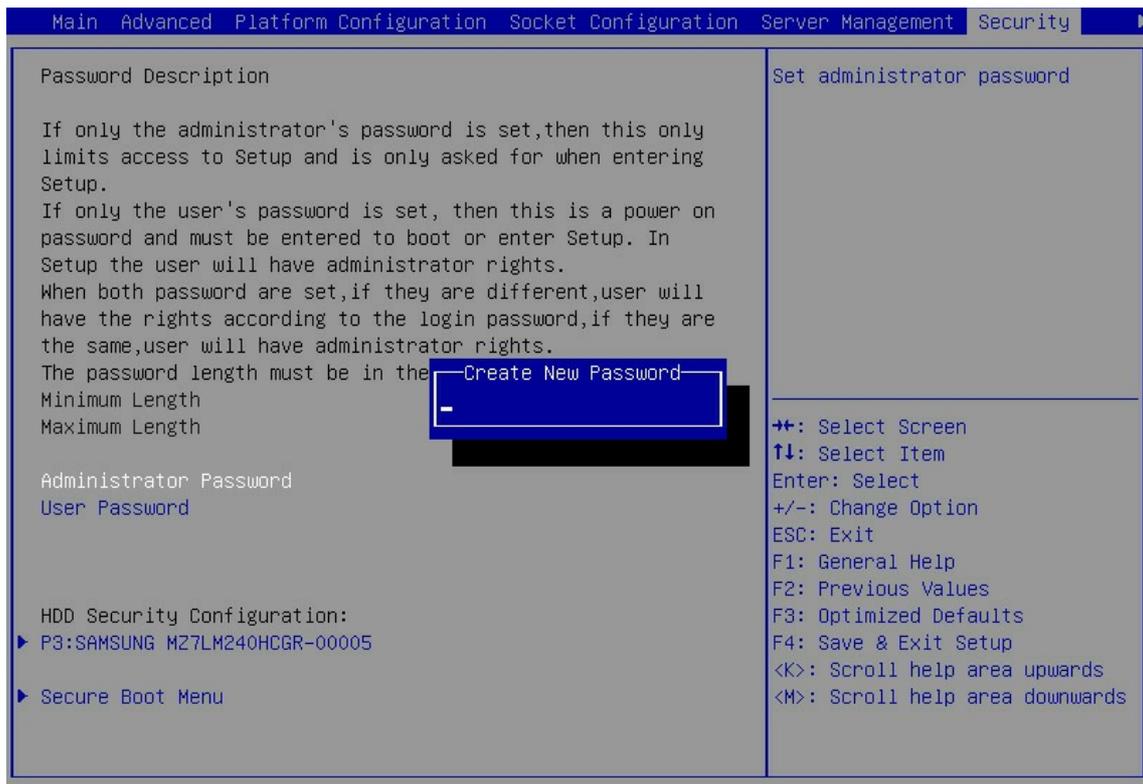
(10) 进入 [图 2-17](#) 所示界面，在弹出的对话框中输入待清除的管理员密码，按 **Enter**。

图2-17 输入待清除的管理员密码



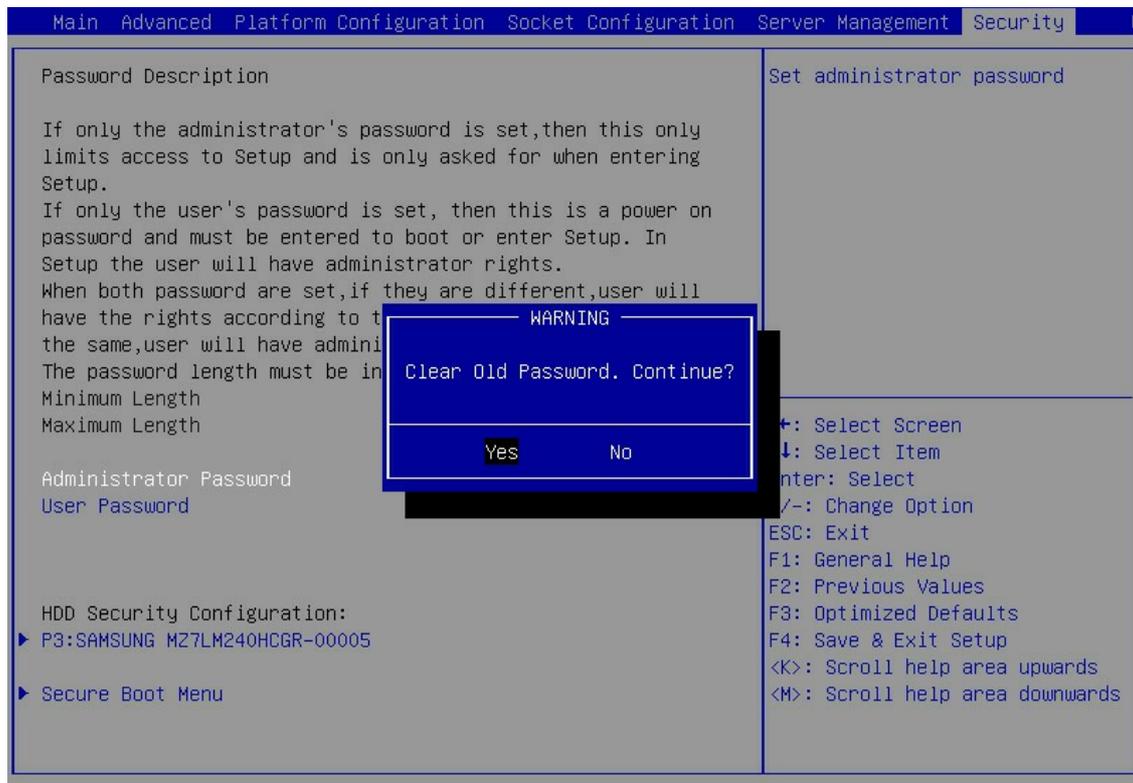
(11) 进入 图 2-18 所示界面，直接按Enter。

图2-18 清除管理员密码



(12) 进入 图 2-19 所示界面，选择Yes，按Enter。

图2-19 确认清除管理员密码



(13) 设置完成后，按 **F4** 保存设置，服务器会自动重启。

## 2.8 设置系统日期和时间

### 1. 操作场景

该功能用于指导工程师通过 BIOS 设置系统的日期和时间。

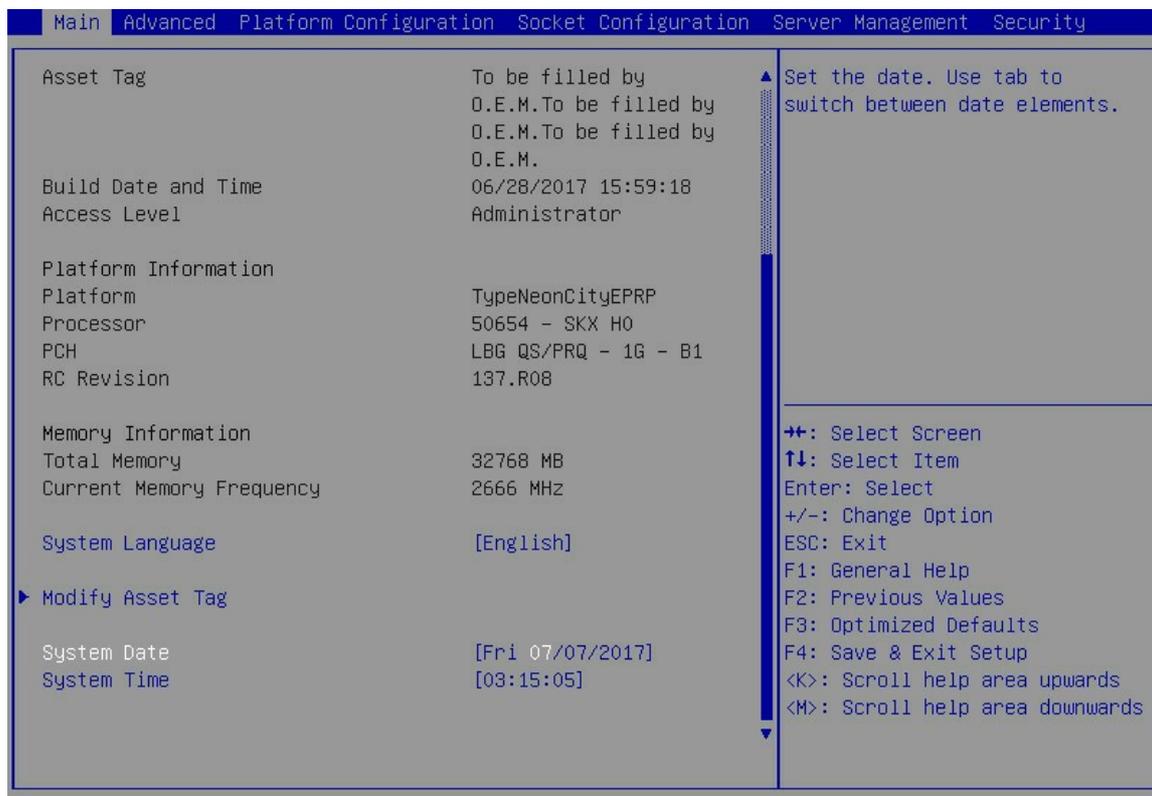
### 2. 准备工作

进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

### 3. 操作步骤

(1) 如 [图 2-20](#) 所示，选择**Main**页签，进入Main界面。

图2-20 Main 界面



- (2) 在 [图 2-20](#) 中，选择**System Date**，系统日期的格式为“月/日/年”。按**Enter**，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。
- (3) 在 [图 2-20](#) 中，选择**System Time**，系统时间为 24 小时制，格式为“时:分:秒”。按**Enter**，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。
- (4) 设置完成后，按 **F4** 保存设置，服务器会继续运行。

## 2.9 设置BIOS启动模式

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。

### 1. 操作场景

该功能用于指导工程师设置 BIOS 的启动模式。

## 2. 准备工作

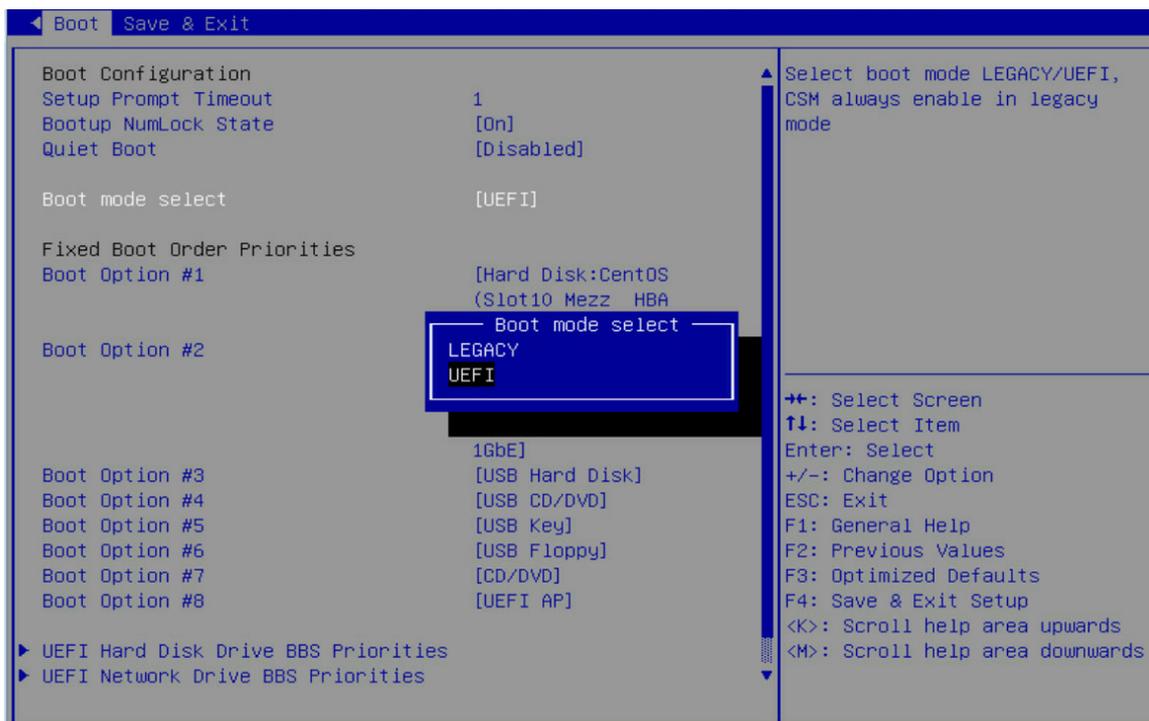
进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

## 3. 操作步骤

(1) 如 [图 2-21](#) 所示，选择 **Boot** 页签 > **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2-21 设置 BIOS 启动模式



(2) 设置完成后，按 **F4** 保存设置，服务器会自动重启。

## 2.10 设置服务器启动顺序



**Fixed Boot Order Priorities** 目录下各选项的排列顺序即服务器的启动顺序。

服务器缺省的启动顺序如 [图 2-22](#) 所示，各参数含义见 [表 2-4](#)。

### 1. 操作场景

该功能用于指导工程师通过 BIOS 设置服务器的启动顺序。

### 2. 准备工作

进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

### 3. 操作步骤

(1) 如 图 2-22 所示，选择**Boot**页签，进入**Boot**页面。

图2-22 Boot 界面

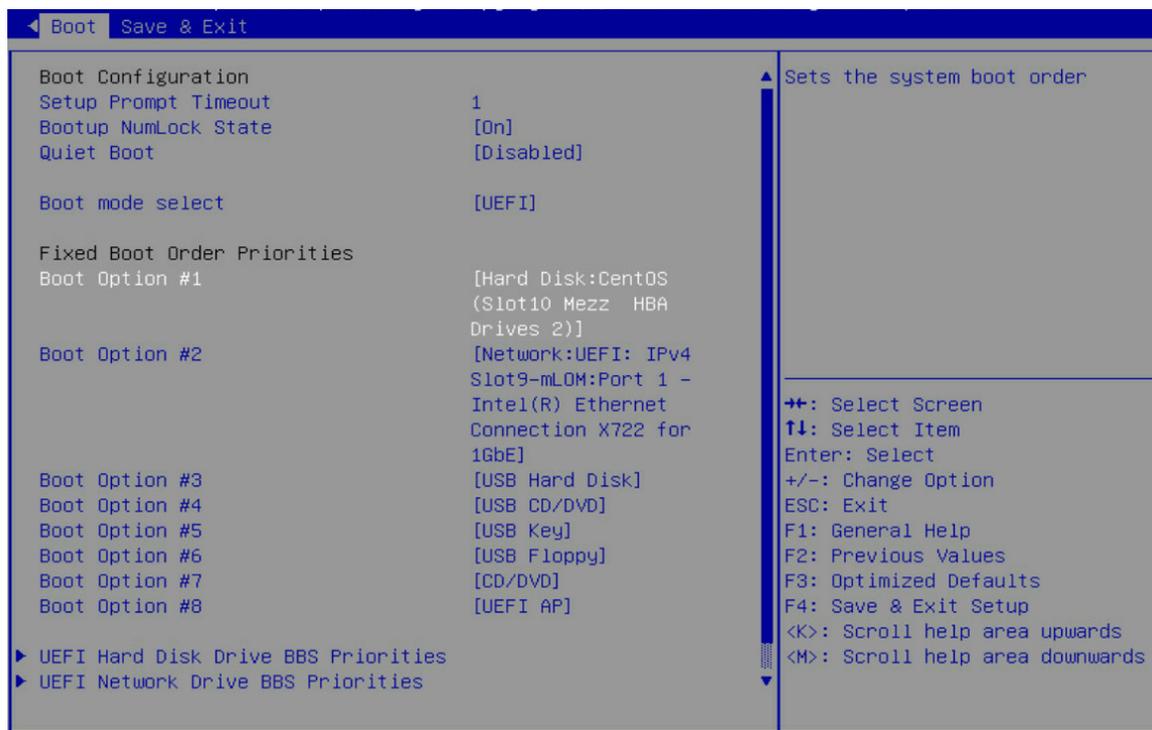
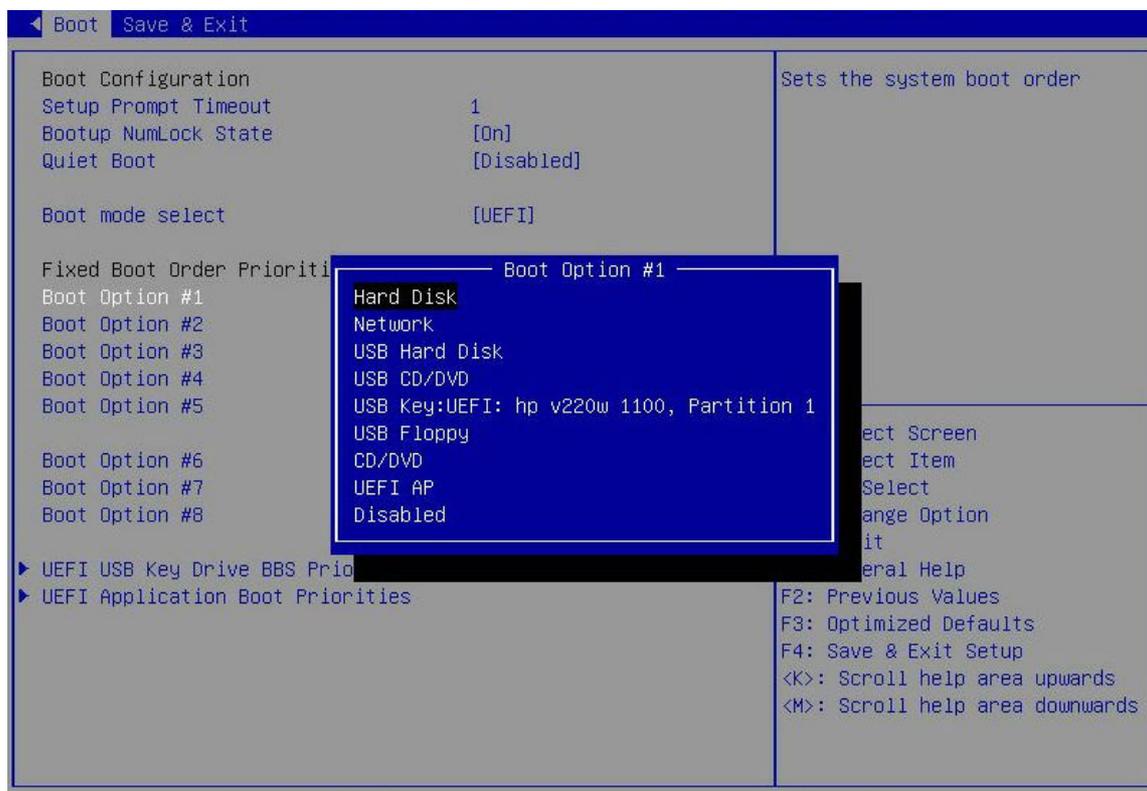


表2-4 服务器启动项

启动项	含义
Hard Disk	硬盘
CD/DVD	SATA接口光驱
USB Hard Disk	USB接口接入的硬盘
USB CD/DVD	USB接口接入的光驱
USB Key	U盘
USB Floppy	USB接口接入的软盘
USB Lan	USB网卡
Network	网络
UEFI AP	内置的UEFI Shell，仅UEFI启动模式下显示该启动项

(2) 如 图 2-23 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2-23 设置启动项



(3) 设置完成后，按 **F4** 保存设置，服务器会继续运行。

### 说明

当服务器连接多个同一类的启动项时，本文以连接两个USB CD/DVD举例。Fixed Boot Order Priorities栏仅显示UEFI USB CDROM/DVD Drive BBS Priorities界面的第一启动项。如果您需要服务器从第二个启动项启动，此时请将该启动项设置为第一启动项，具体方法与设置服务器启动顺序的方法类似。UEFI USB CDROM/DVD Drive BBS Priorities界面如 [图 3-105](#) 所示。

## 2.11 配置RAID

### 1. 操作场景

该功能指导工程师，通过 BIOS 配置 RAID。

### 2. 准备工作

已经进入BIOS界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

### 3. 操作步骤

通过 BIOS 配置 RAID 的具体方法请参见《H3C 服务器 存储控制卡用户指南》。

## 2.12 恢复BIOS缺省设置

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。

### 1. 操作场景

该功能用于指导工程师通过 BIOS 恢复 BIOS 的缺省设置。

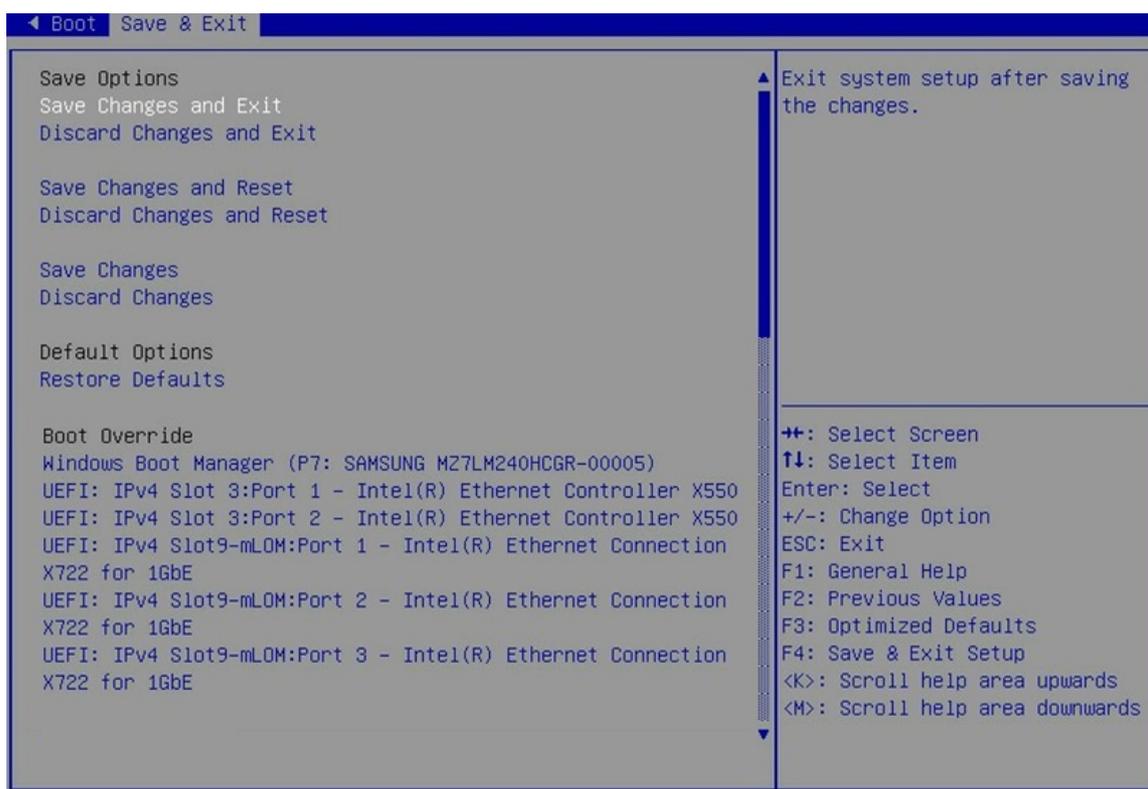
### 2. 准备工作

进入服务器的BIOS Setup界面，具体步骤请参见 [2.1 进入BIOS界面](#)。

### 3. 操作步骤

(1) 如 [图 2-24](#) 所示，选择**Save & Exit**页签 > **Restore Defaults**，按**Enter**。

图2-24 恢复缺省设置



说明

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

# 3 界面参数说明

## 3.1 Main界面

介绍 Main 界面包含的 BIOS 基本信息。

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

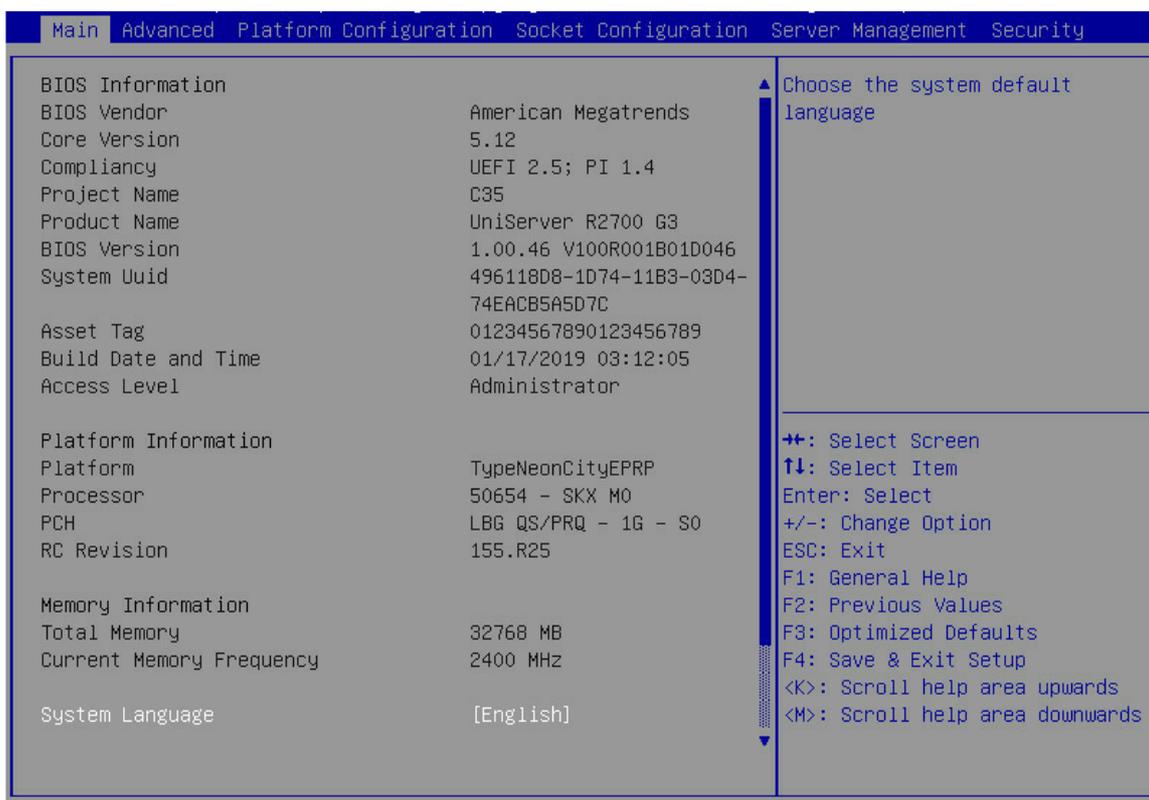


表3-1 Main 界面参数

界面参数	功能说明
<b>BIOS Information</b>	
BIOS Vendor	显示BIOS供应商
Core Version	显示BIOS内核版本号
Compliance	显示BIOS遵循的规范
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

界面参数	功能说明
System Uuid	系统通用唯一ID
Asset Tag	显示服务器的资产标签
Build Date and Time	显示BIOS编译日期和时间
Access Level	显示访问BIOS的级别，包括Administrator（管理员级别）和User（用户级别），BIOS级别的含义和设置方法请参见 <a href="#">3.6 Security界面</a>
<b>Platform Information</b>	
Platform	显示平台信息
Processor	显示CPU型号
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
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>
Modify Asset Tag	服务器资产标签配置菜单
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，可以通过以下方式来修改数值： <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，可以通过以下方式来修改数值： <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>

Modify Asset Tag界面如 [图 3-2](#) 所示，具体参数说明如 [表 3-2](#) 所示。

图3-2 Modify Asset Tag 界面

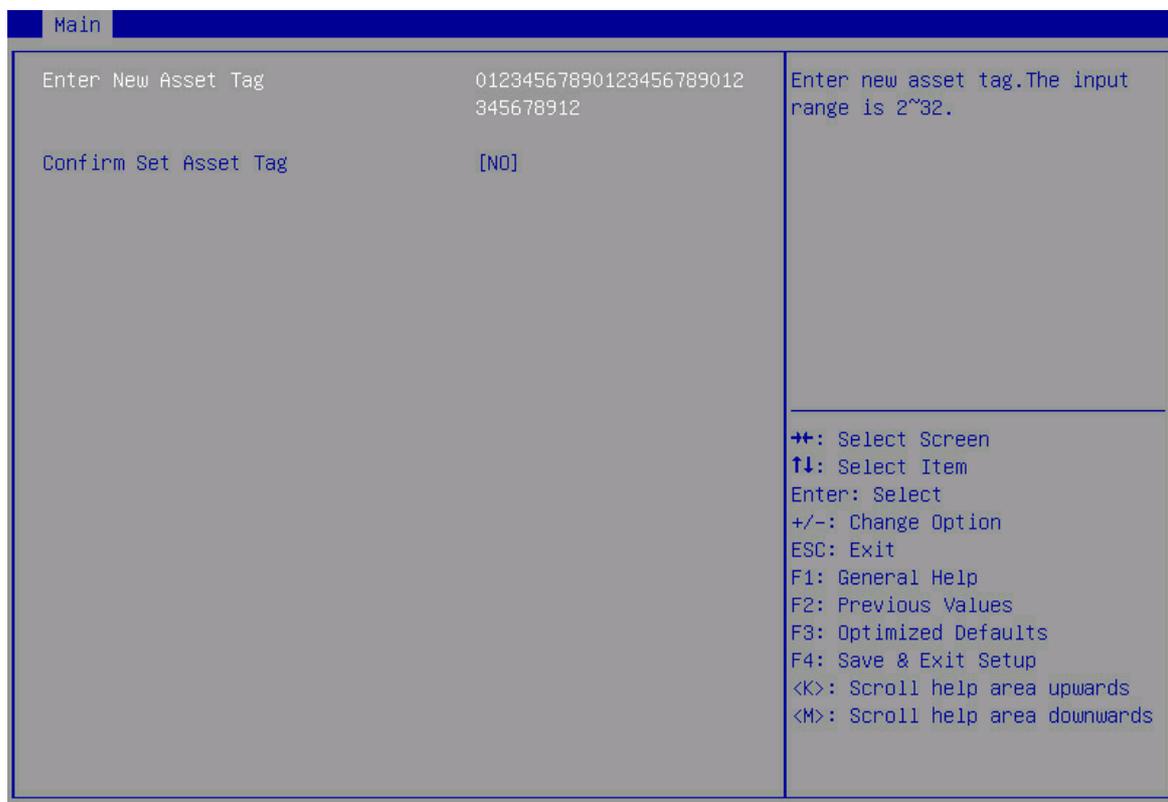


表3-2 Modify Asset Tag 界面参数

界面参数	功能说明
Enter new Asset Tag	修改服务器的资产标签。需要注意的是，修改服务器的资产标签后，还需将Confirm set Asset Tag选项设置为YES保存修改。
Confirm set Asset Tag	确认修改服务器的资产标签，菜单选项为： <ul style="list-style-type: none"> <li>NO（缺省）：放弃修改服务器的资产标签。</li> <li>YES：保存修改服务器的资产标签。</li> </ul>

## 3.2 Advanced界面

介绍 Advanced 界面包含的参数及相关功能。

Advanced界面如 [图 3-3](#) 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、PCI子系统、网络堆栈、CSM和USB配置等。具体参数说明如 [表 3-3](#) 所示。

图3-3 Advanced 界面

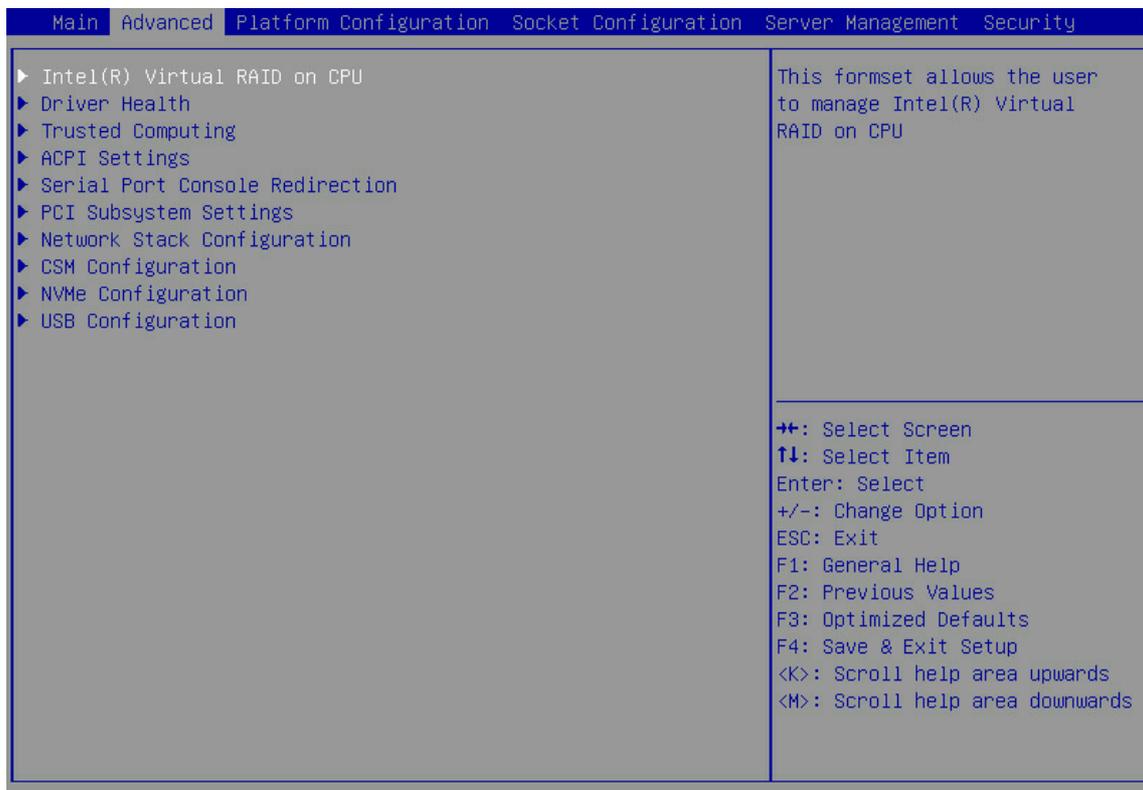


表3-3 Advanced 界面参数

界面参数	功能说明
Intel(R) Virtual RAID on CPU	NVMe虚拟RAID配置菜单
Driver Health	驱动/控制器的健康状态，仅UEFI启动模式下支持该功能。
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	串口重定向配置菜单
PCI Subsystem Settings	PCI子系统配置菜单
Network Stack Configuration	网络堆栈配置菜单，仅UEFI启动模式下支持该功能。
CSM Configuration	CSM配置菜单
NVMe Configuration	NVMe配置菜单
USB Configuration	USB配置菜单

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

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) 设置使能相应的 VMD, 选择 **Socket Configuration** 页签 > **I/O Configuration** > **Intel® VMD technology**, 然后按 **Enter**。
- (3) 根据设备所安装的处理器选择 Processor 1 或者 Processor 2。以安装的位置为 CPU1 为例, 选择 **Intel® VMD for Volume Management Device on Processor 1** > **Intel® VMD for Volume Management Device for PStack0** > **Enabled**, 如 [图 3-4](#) 所示。

图3-4 Intel® VMD for Volume Management Device on Processor 1 界面

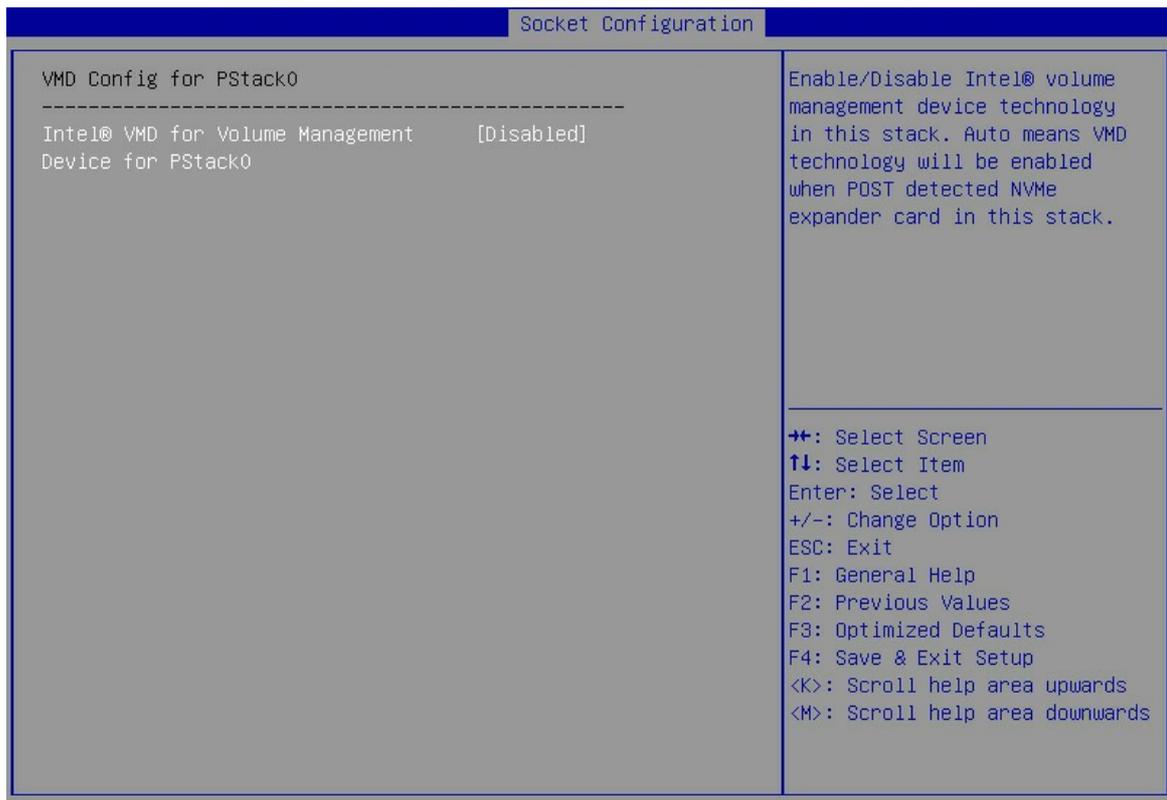


表3-4 Intel® VMD for Volume Management Device on Processor 1 界面参数

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，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled: 禁用此 PStack0 栈中英特尔®卷管理设备技术。</li> <li>• Auto (缺省): 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> <p>VMD默认设置是关闭的。VMD功能必须配合NVMe SSD使用，只有在G3服务器上安装了NVMe 4Port扩展卡(Retimer卡)或NVMe 8Port扩展卡(Switch卡)时，才能使能对应槽位的VMD功能，否则会导致该槽位上的PCIe设备无法正常使用。</p>

设置 Intel virtual RAID on CPU 信息：

- (4) 设置成功VMD后，进入**Advanced**页签 > **Intel(R) virtual RAID on CPU**菜单，然后按**Enter**。  
如 [图 3-5](#) 所示

图3-5 Intel(R) virtual RAID on CPU 界面

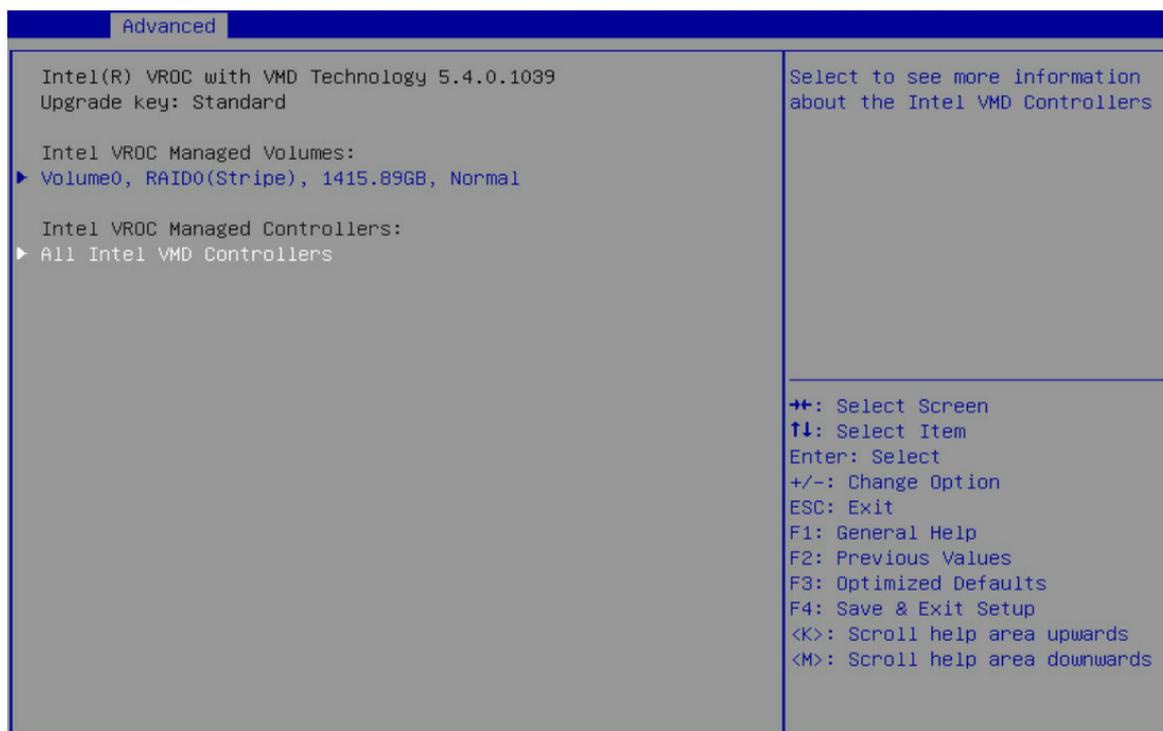


表3-5 Intel(R) virtual RAID on CPU 界面参数

界面参数	功能说明
Volume0, RAID0 (Stripe), 1415.89GB, Normal	<p>已创建的RAID 信息:</p> <p>Volume0: 该RAID名字, RAID0: 该RAID级别 1415.89GB (Size) : 该RAID大小, Normal: 该RAID状态</p>
All Intel VMD Controllers	所有的Intel VMD控制器菜单

Volume0, RAID0 (Stripe), 1415.89GB, Normal 菜单界面参数如 [图 3-6](#) 所示, 具体参数说明如 [表 3-6](#) 所示。



Volume x, RAID x(Stripe), Size, Status 菜单表示已经组成 RAID 的卷的信息。本文以已知的 RAID 卷: Volume0, RAID0 (Stripe), 1415.89GB, Normal 为例进行介绍。

图3-6 Volume0, RAID0 (Stripe), 1415.89GB, Normal 界面

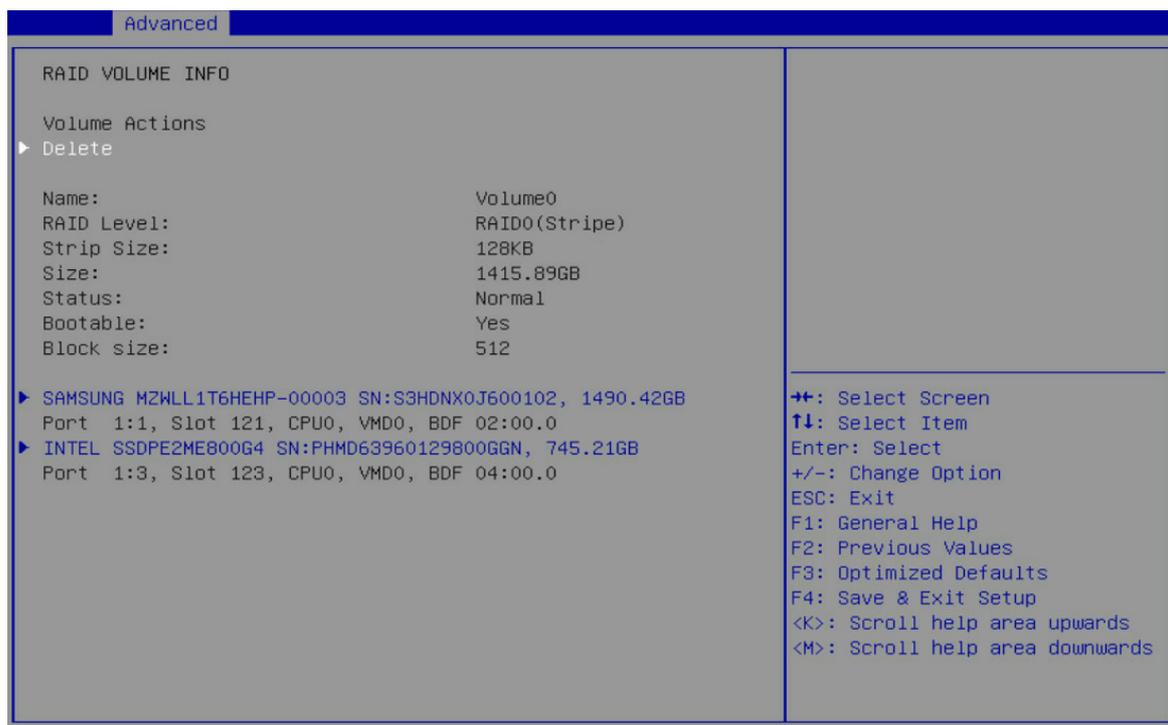


表3-6 Volume0, RAID0 (Stripe), 1415.89GB, Normal 界面参数

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

界面参数	功能说明
Block Size	块大小
RAID Member Disks: 该RAID中的成员硬盘	
SAMSUNG MZWLL1T6HEHP-00003 SN:S3HDNX0J600102,1490.42GB Port 1:1,Slot 121,CPU0,VMD0,BDF 02:00.0	组成该RAID的硬盘(port1:1)信息菜单
INTEL SSDPE2ME800G4 SN:PHMD63960129800GGN,745.21GB Port 1:3,Slot 123,CPU0,VMD0,BDF 04:00.0	组成该RAID的硬盘(port1:3)信息菜单

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。

- 若安装的是 4 端口的 NVME SSD 扩展卡且该卡安装在 PCIe Riser 卡插槽 1, 则硬盘端口按当前的显示为准。
- 若安装的是 8 端口的 NVME SSD 扩展卡, 则端口统一显示为 Port x:0; 若安装在 PCIe Riser 卡插槽 1, 则 x 显示为 1, 若安装在 PCIe Riser 卡插槽 2, 则 x 显示为 2。

Delete菜单界面参数如 [图 3-7](#) 所示，具体参数说明如 [表 3-7](#) 所示。

图3-7 Delete 界面

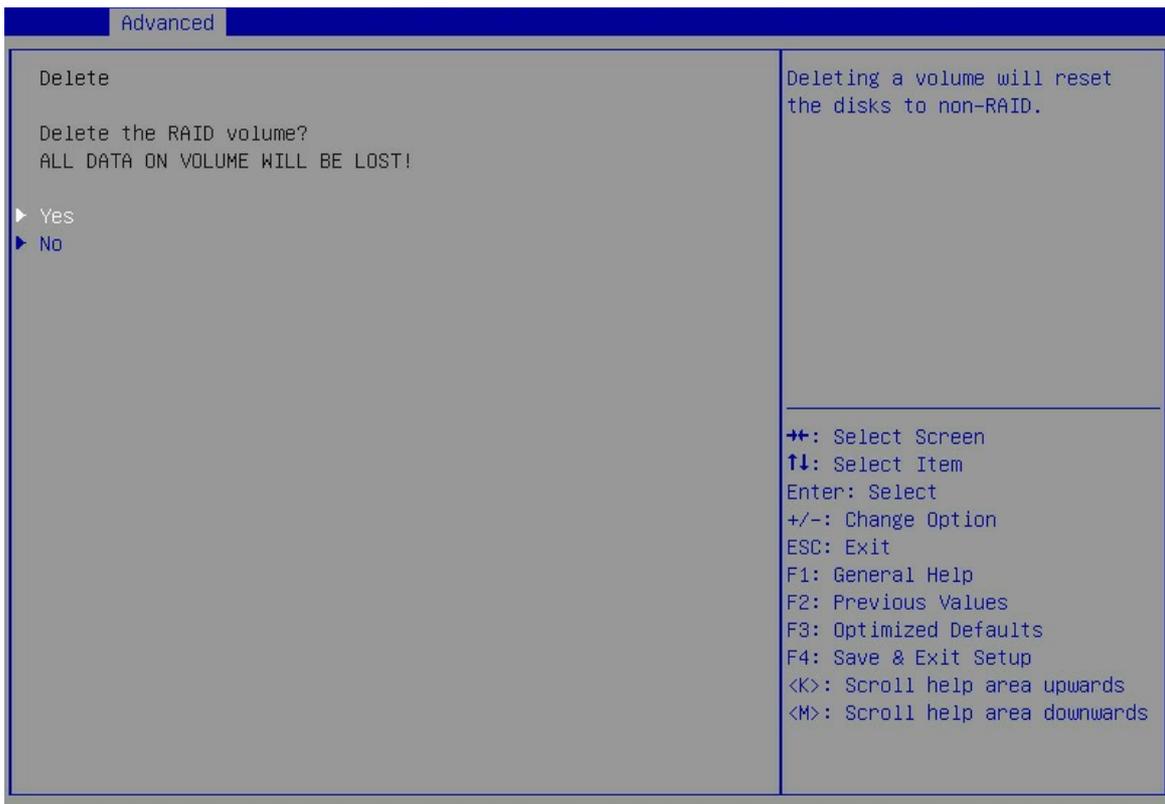


表3-7 Delete 界面参数

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 3-8](#) 所示，具体参数说明如 [表 3-8](#) 所示。



说明

SAMSUNG MZWLL1T6HEHP-00003 SN:S3HDNX0J600102,1490.42GB

Port 1:1,Slot 121,CPU0,VMD0,BDF 02:00.0 和 INTEL SSDPE2ME800G4

SN:PHMD63960129800GGN,745.21GB Port 1:3,Slot 123,CPU0,VMD0,BDF 04:00.0 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 SSDPE2ME800G4

SN:PHMD63960129800GGN,745.21GB 为例进行介绍。

图3-8 INTEL SSDPE2ME800G4 SN:PHMD63960129800GGN,745.21GB 界面

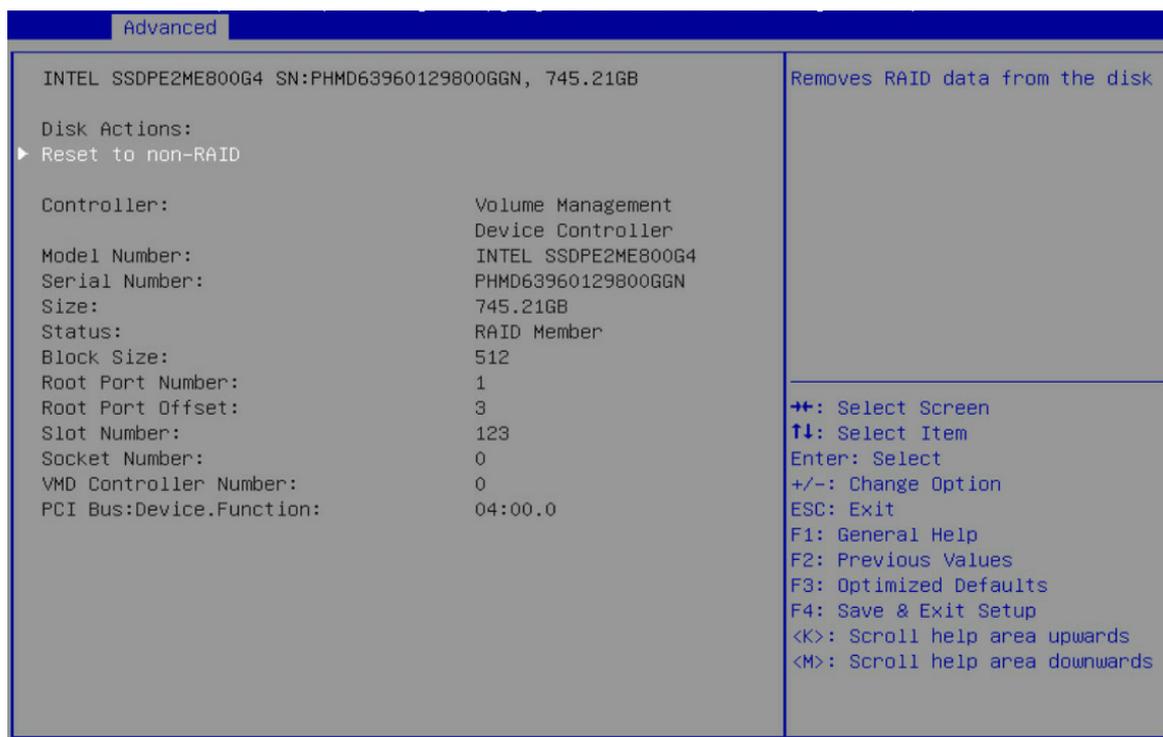


表3-8 INTEL SSDPE2ME800G4 SN:PHMD63960129800GGN,745.21GB 界面参数

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。
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
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

Reset to non-RAID菜单界面参数如 [图 3-9](#) 所示，具体参数说明如 [表 3-9](#) 所示。

图3-9 Reset to non-RAID 界面

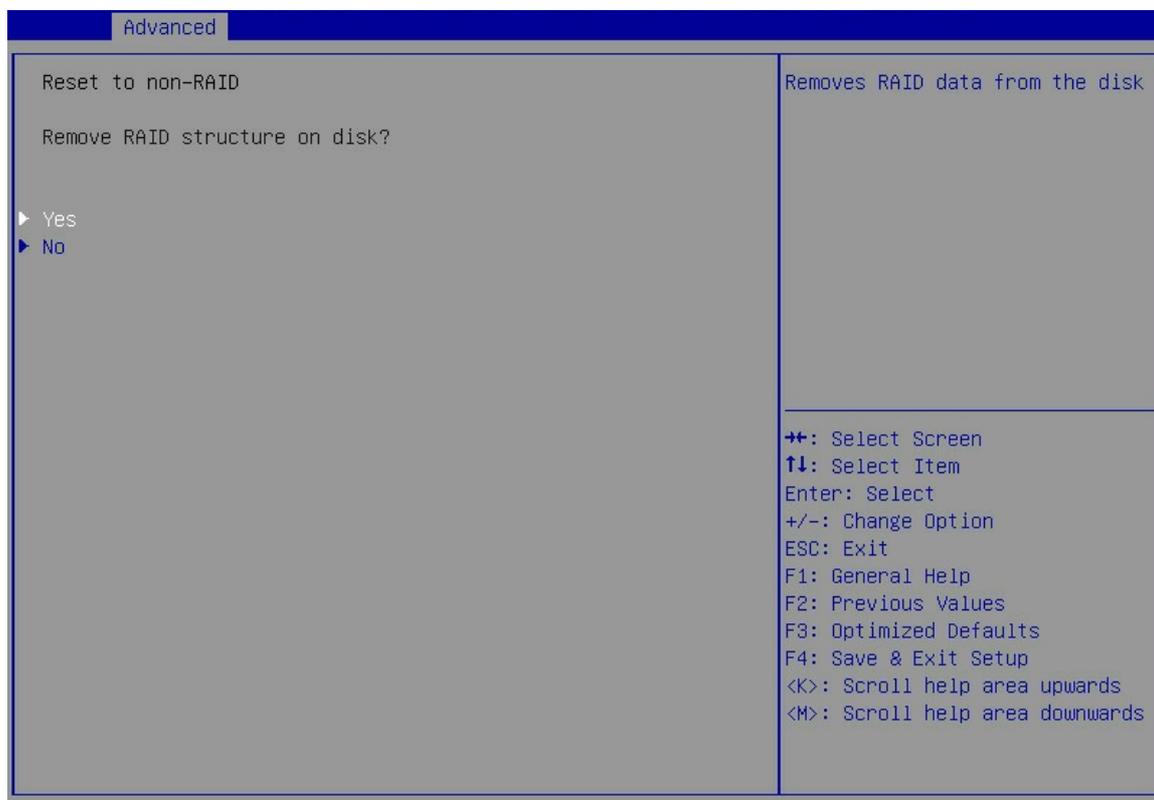


表3-9 Reset to non-RAID 界面参数

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

All Intel VMD Controllers界面如 [图 3-10](#)所示，具体参数说明如 [表 3-10](#)所示。

图3-10 All Intel VMD Controllers 界面

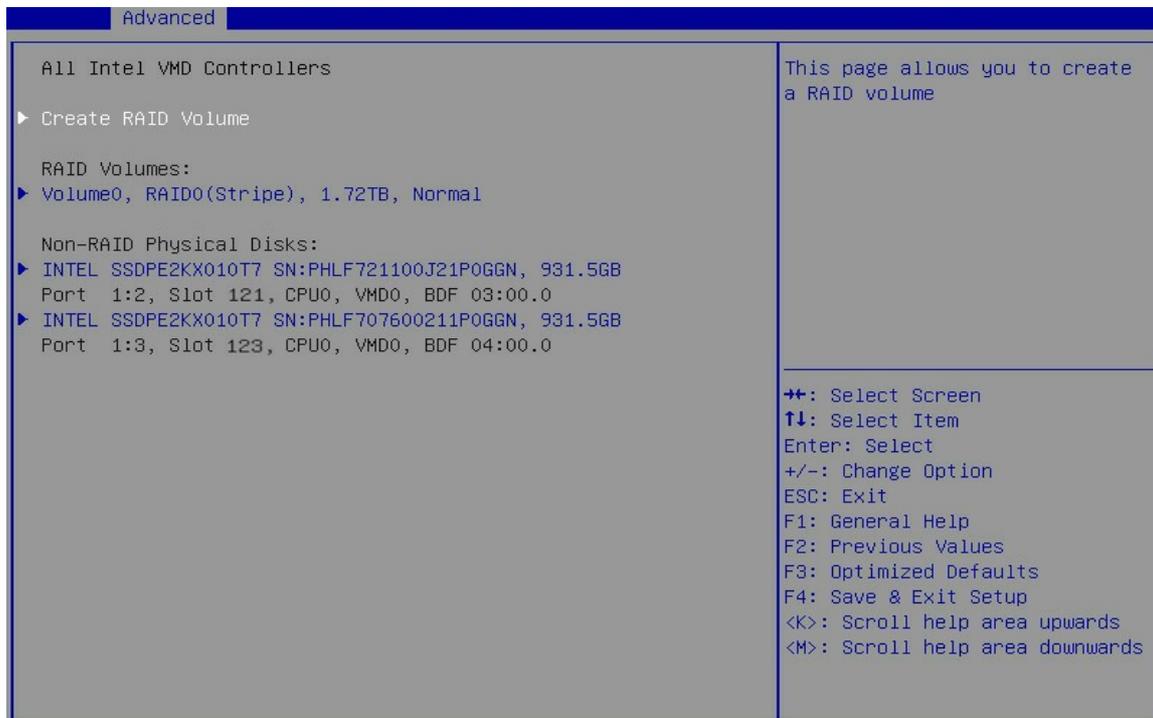


表3-10 All Intel VMD Controllers 界面参数

界面参数	功能说明
Create RAID Volume	创建RAID卷的菜单
RAID Volume: 已创建的RAID 信息	
Volume0, RAID0 (Stripe) ,1.72TB,Normal	Volume0: 该RAID名字 RAID0: 该RAID级别 1.72TB,Normal: 该RAID大小, 该RAID状态
Non-RAID Physical Disks: 未被创建RAID 物理硬盘	
INTEL SSDPE2KX010T7 SN:PHLF721100J21P0GGN,931.5GB Port 1:2,Slot 121,CPU0,VMD0,,BDF 03:00.0	未被创建RAID物理硬盘信息,以Port1:2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。 <ul style="list-style-type: none"> <li>若安装的是 4 端口的 NVME SSD 扩展卡且该卡安装在 PCIe Riser 卡插槽 1, 则硬盘端口按当前的显示为准。</li> <li>若安装的是 8 端口的 NVME SSD 扩展卡, 则端口统一显示为 Port x:0; 若安装在 PCIe Riser 卡插槽 1, 则 x 显示为 1, 若安装在 PCIe Riser 卡插槽 2, 则 x 显示为 2。</li> </ul>

Create RAID Volume界面如 [图 3-11](#) 所示, 具体参数说明如 [表 3-11](#) 所示。

图3-11 Create RAID Volume 界面

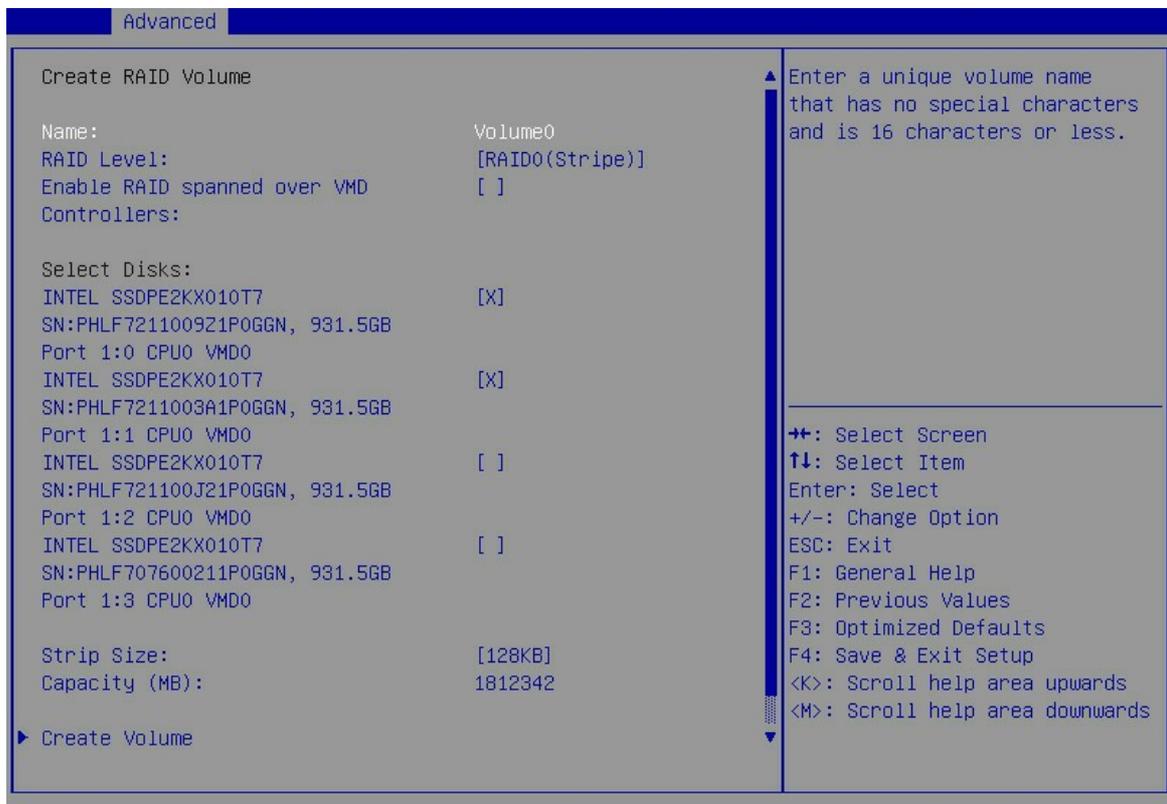


表3-11 Create RAID Volume 界面参数

界面参数	功能说明
Create RAID Volume: 创建RAID卷的菜单	
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
INTEL SSDPE2ME800G4 SN:PHMD63960129800GGN,745.21GB Port 1:3,CPU0,VMD0	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

界面参数	功能说明
Capacity(MB)	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

Non-RAID Physical Disk(以INTEL SSDPE2KX010T7 SN:PHLF721100J21P0GGN,931.5GB为例，其他各个未组RAID的硬盘信息界面与之相同)界面如 [图 3-12](#) 所示，具体参数说明如 [表 3-12](#) 所示。

图3-12 INTEL SSDPE2KX010T7 SN:PHLF721100J21P0GGN,931.5GB 界面

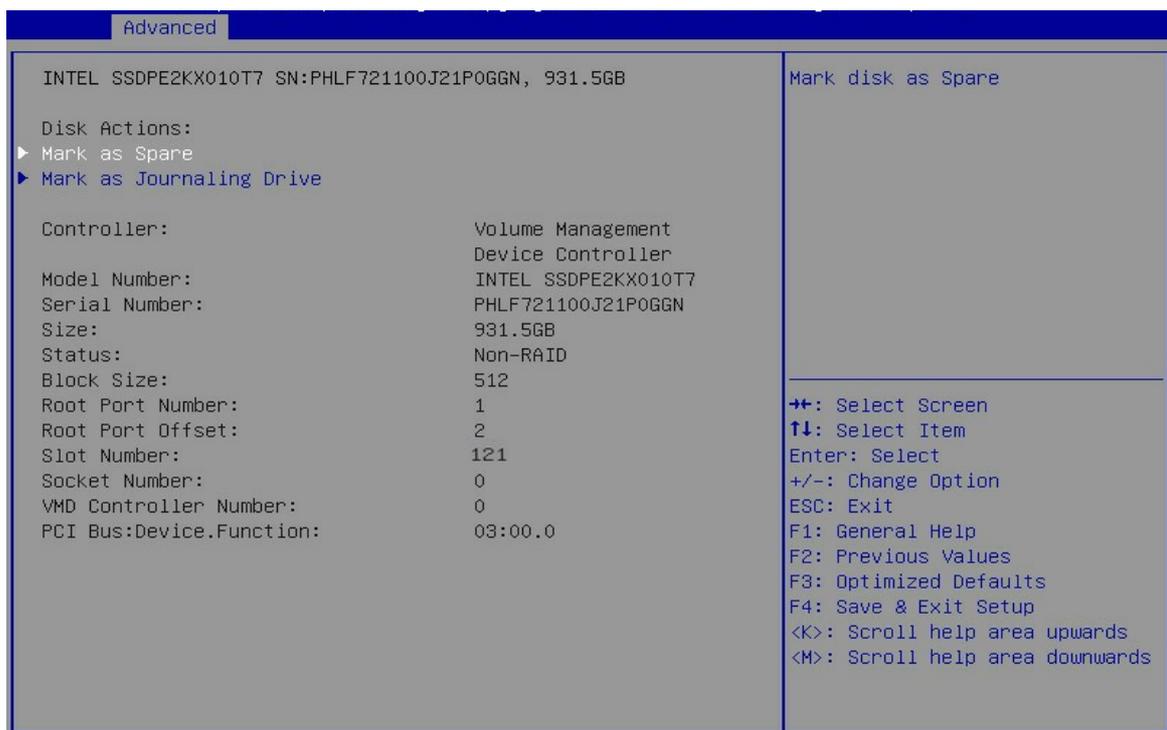


表3-12 INTEL SSDPE2KX010T7 SN:PHLF721100J21P0GGN,931.5G 界面参数

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

界面参数	功能说明
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

Mark as Spare界面如 [图 3-13](#)所示，具体参数说明如 [表 3-13](#)所示。

图3-13 Mark as Spare 界面

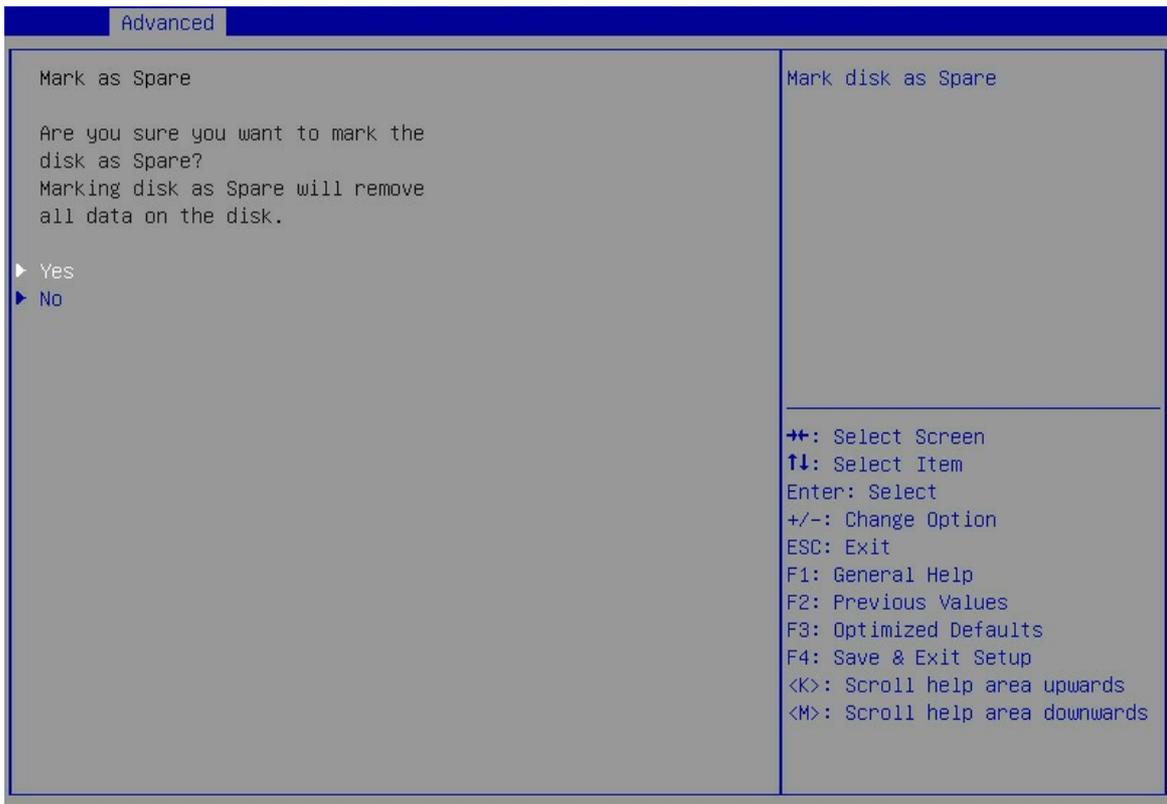


表3-13 Mark as Spare 界面参数

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

Mark as Journaling Drive界面如 [图 3-14](#)所示，具体参数说明如 [表 3-14](#)所示。

图3-14 Mark as Journaling Drive 界面

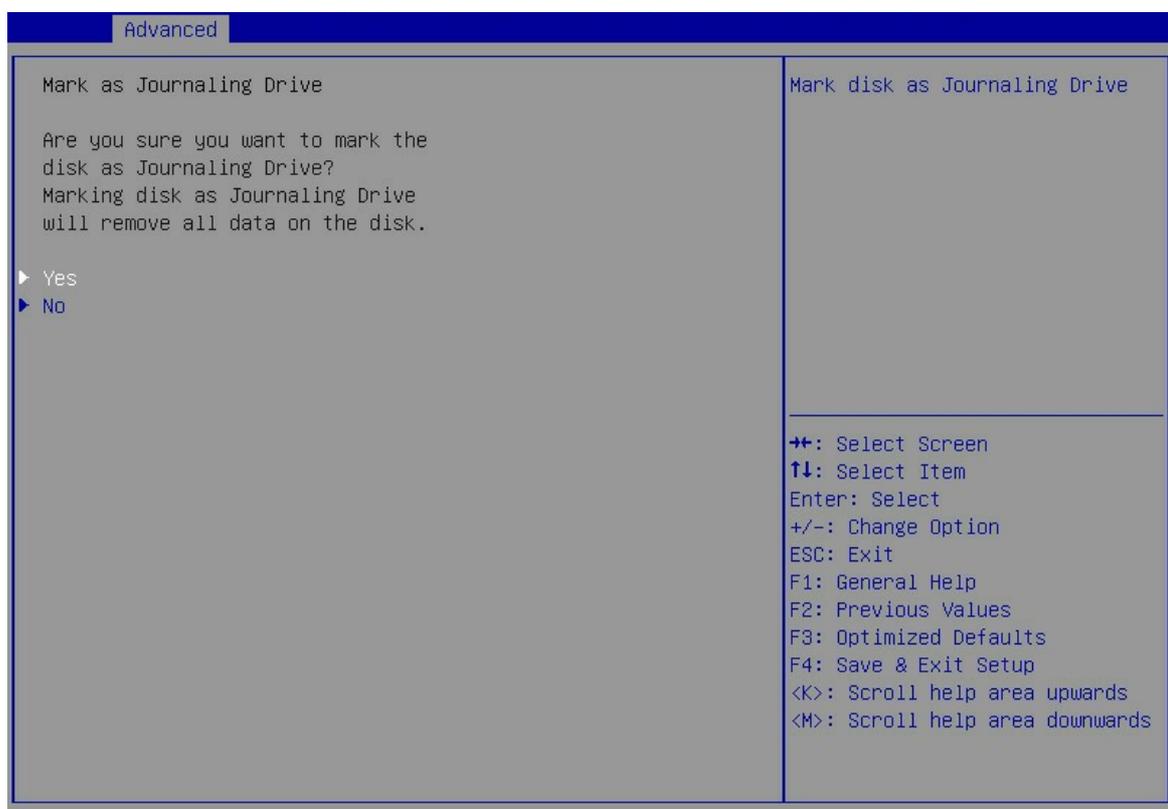


表3-14 Mark as Journaling Drive 界面参数

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

### 3.2.2 Driver Health界面

如 [图 3-15](#) 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 3-15](#) 所示。

图3-15 Driver Health 界面

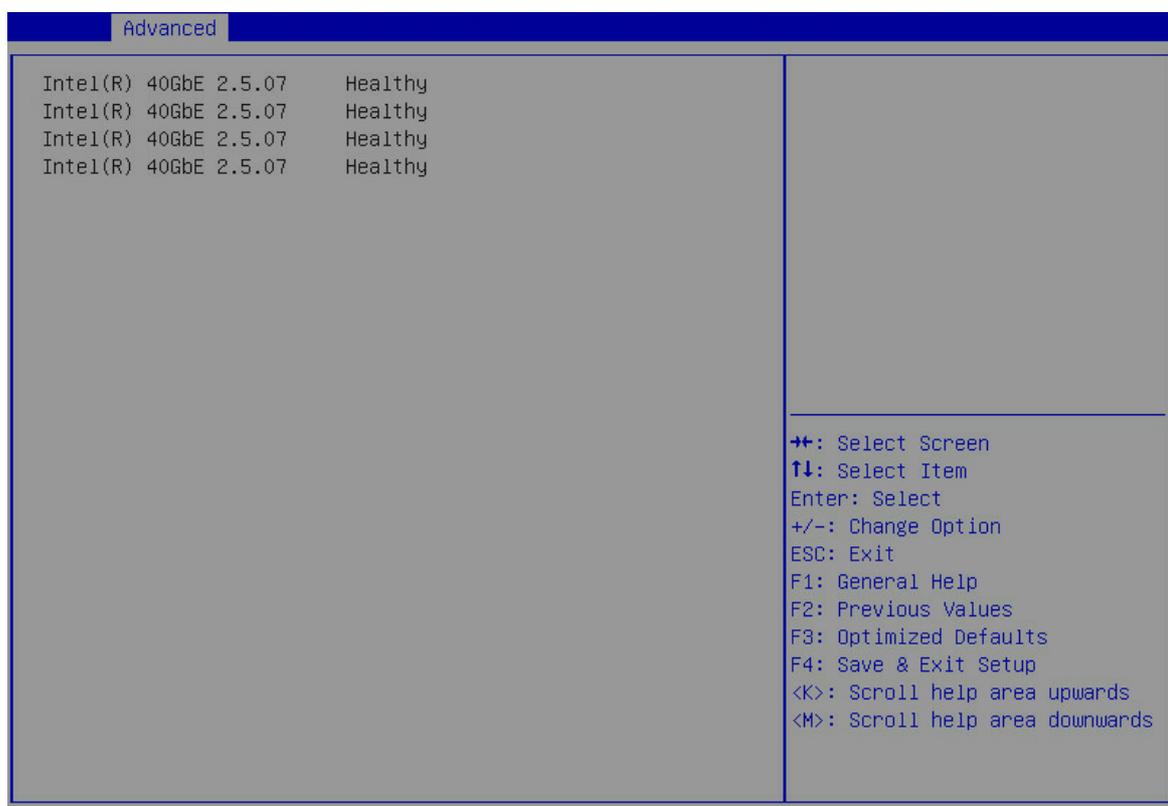


表3-15 Driver Health 界面参数

界面参数	功能说明
Intel(R) 40GbE 2.5.07 (该界面体现服务器实际安装的驱动/控制器的状态, 当前安装的是一张4端口的mLOM网卡, 以其中一个控制器为例说明)	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。

### 3.2.3 Trusted Computing界面

介绍配置安全设备的方法。

如 [图 3-16](#) 所示, 通过Trusted Computing界面可以配置安全设备(如H3C UIS系列可信密码模块)。具体参数说明如 [表 3-16](#) 所示。

图3-16 Trusted Computing 界面



表3-16 Trusted Computing 界面参数

界面参数	功能说明
Security Device Support	始终启用对安全设备的支持

安装TPM2.0 安全设备，TPM2.0 界面如 [图 3-17](#) 所示，具体参数说明如 [表 3-17](#) 所示。

图3-17 TPM2.0 界面

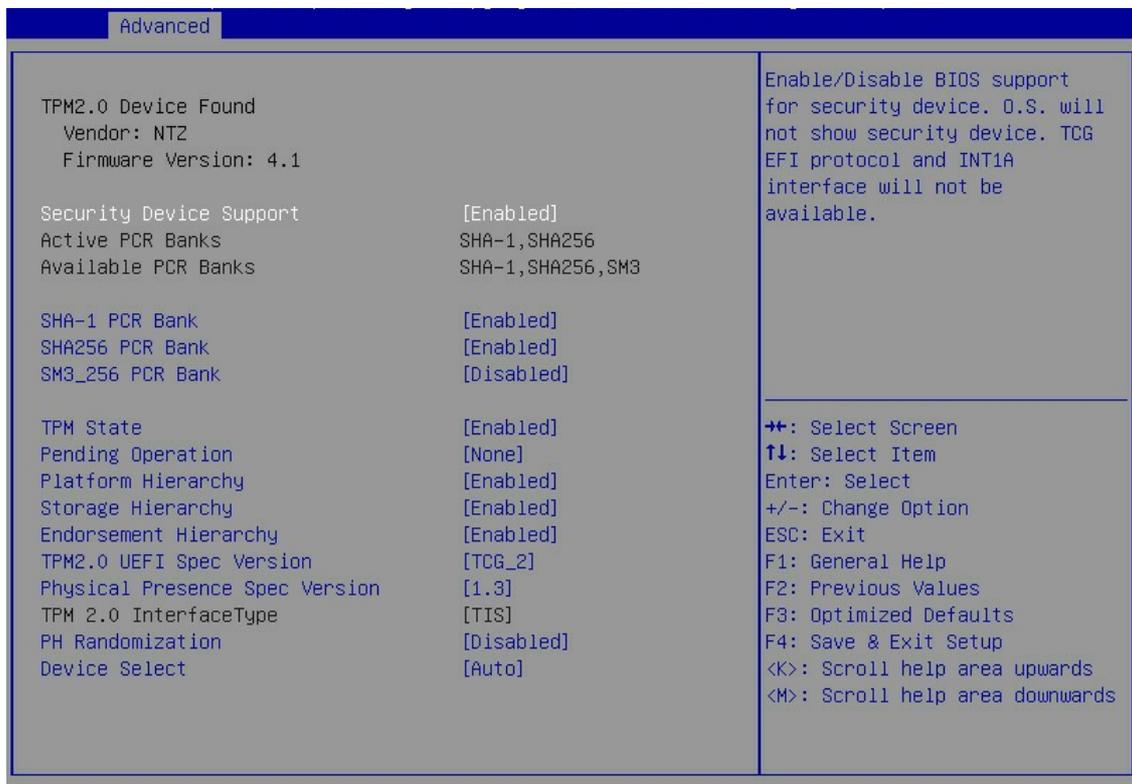


表3-17 TPM2.0 界面参数

界面参数	功能说明
Security Device Support	始终启用对安全设备的支持
Active PCR Banks	活动的PCR Banks
Available PCR Banks	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_256PCR Bank	SM3_256PCR Bank启用配置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled（缺省）：启用 SM3_256PCR Bank。</li> <li>Disabled：禁用 SM3_256PCR Bank。</li> </ul>
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>

界面参数	功能说明
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，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>

安装TCM安全设备，TCM界面如 [图 3-18](#) 所示，具体参数说明如 [表 3-18](#) 所示。

图3-18 TCM 界面

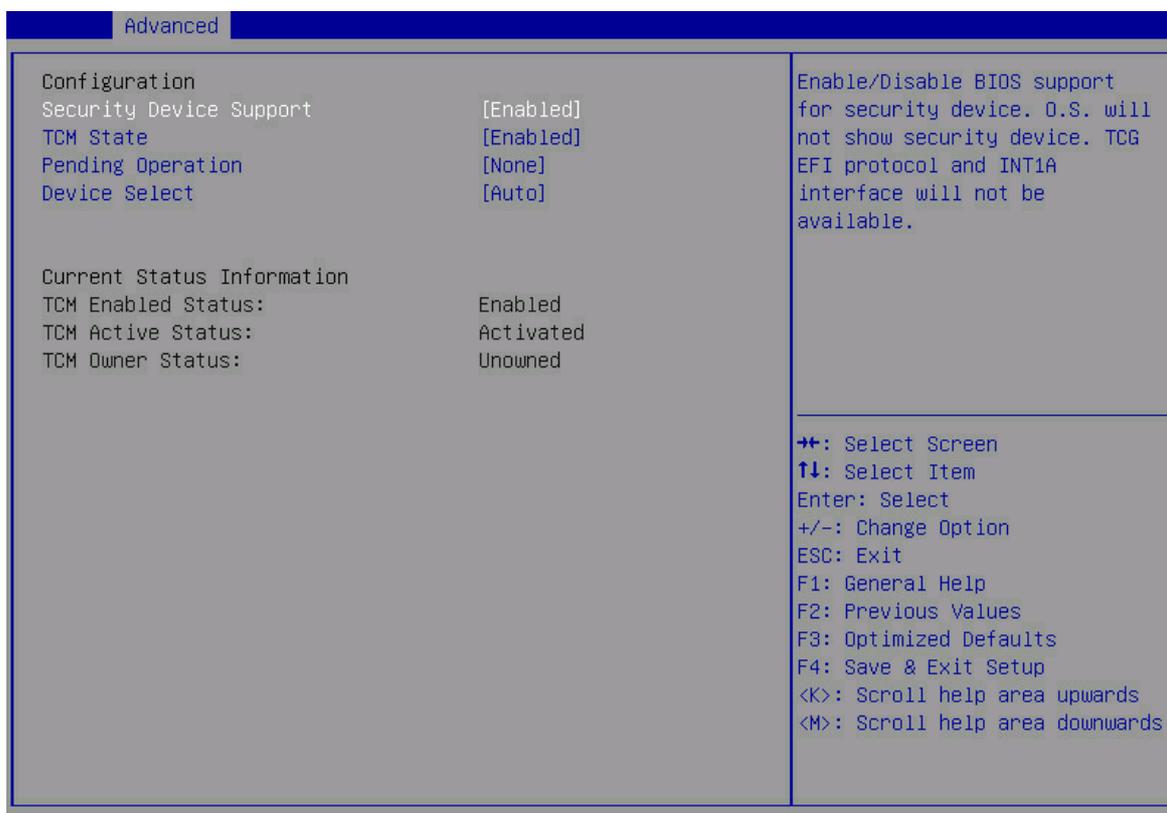


表3-18 TCM 界面参数

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。

### 3.2.4 ACPI Settings界面

如 [图 3-19](#) 所示，通过ACPI Settings界面，可以对ACPI进行配置。具体参数说明如 [表 3-19](#) 所示。

图3-19 ACPI Settings 界面

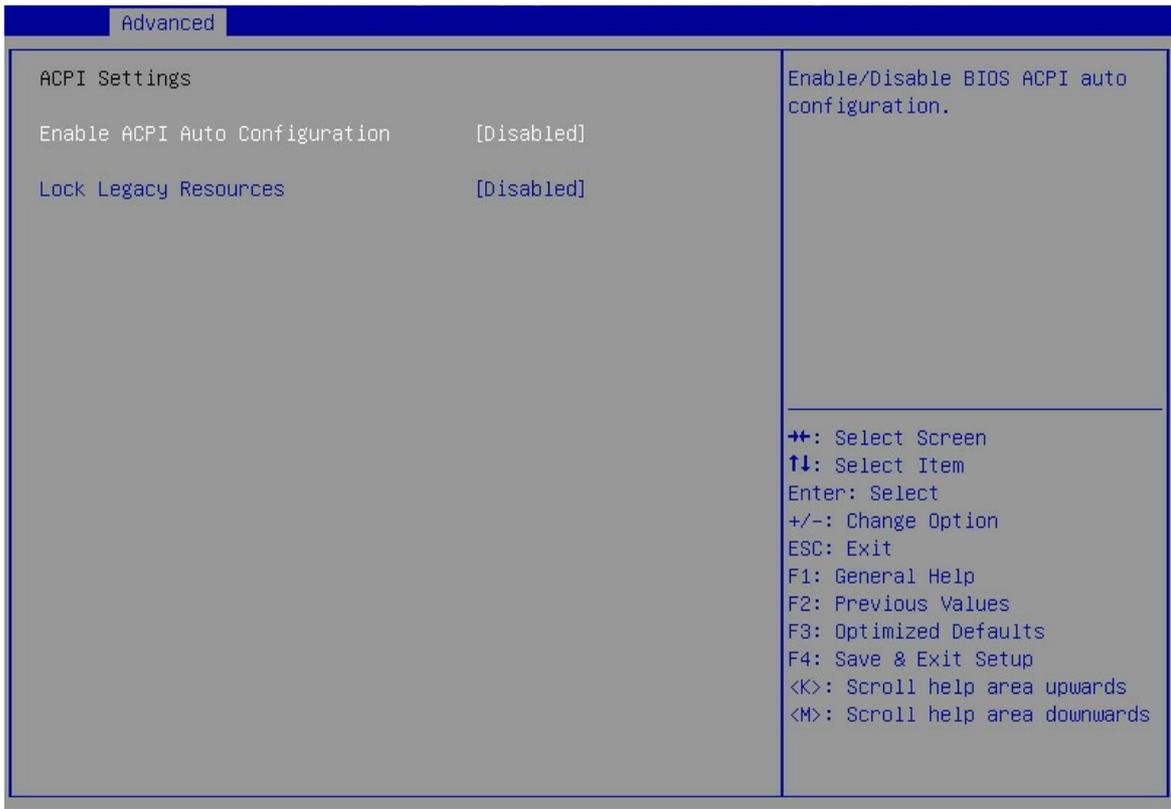


表3-19 ACPI Settings 界面参数

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
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>

### 3.2.5 Serial Port Console Redirection界面

如 [图 3-20](#) 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 3-20](#) 所示。

图3-20 Serial Port Console Redirection 界面

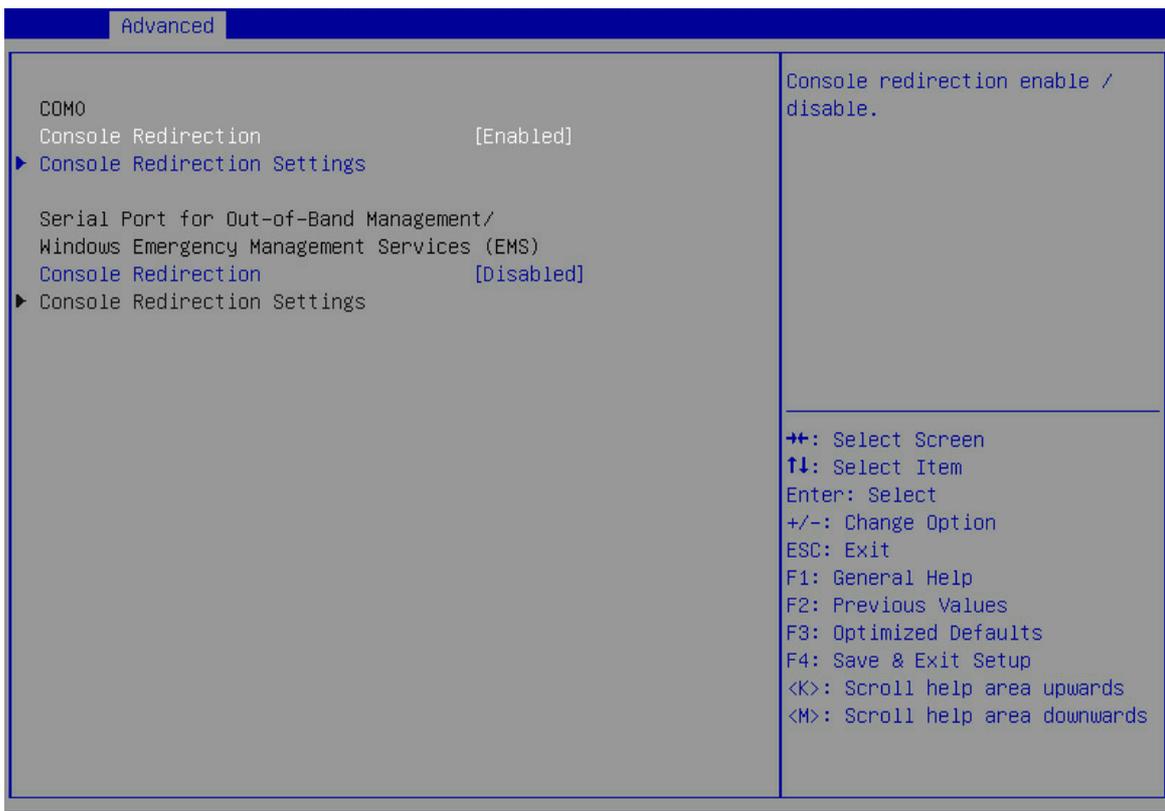


表3-20 Serial Port Console Redirection 界面参数

界面参数	功能说明
COM0	COM0端口
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 Console Redirection Settings 菜单进行配置。</li> <li>• Disabled: 关闭串口重定向功能。</li> </ul>

界面参数	功能说明
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3-21</a> 所示，具体参数说明如 <a href="#">表3-21</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3-22</a> 所示。具体参数说明如 <a href="#">表3-22</a> 所示。

COM0 端口的Console Redirection Settings界面如 [图 3-21](#) 所示。具体参数说明如 [表 3-21](#) 所示。

图3-21 COM0 端口的 Console Redirection Settings 界面

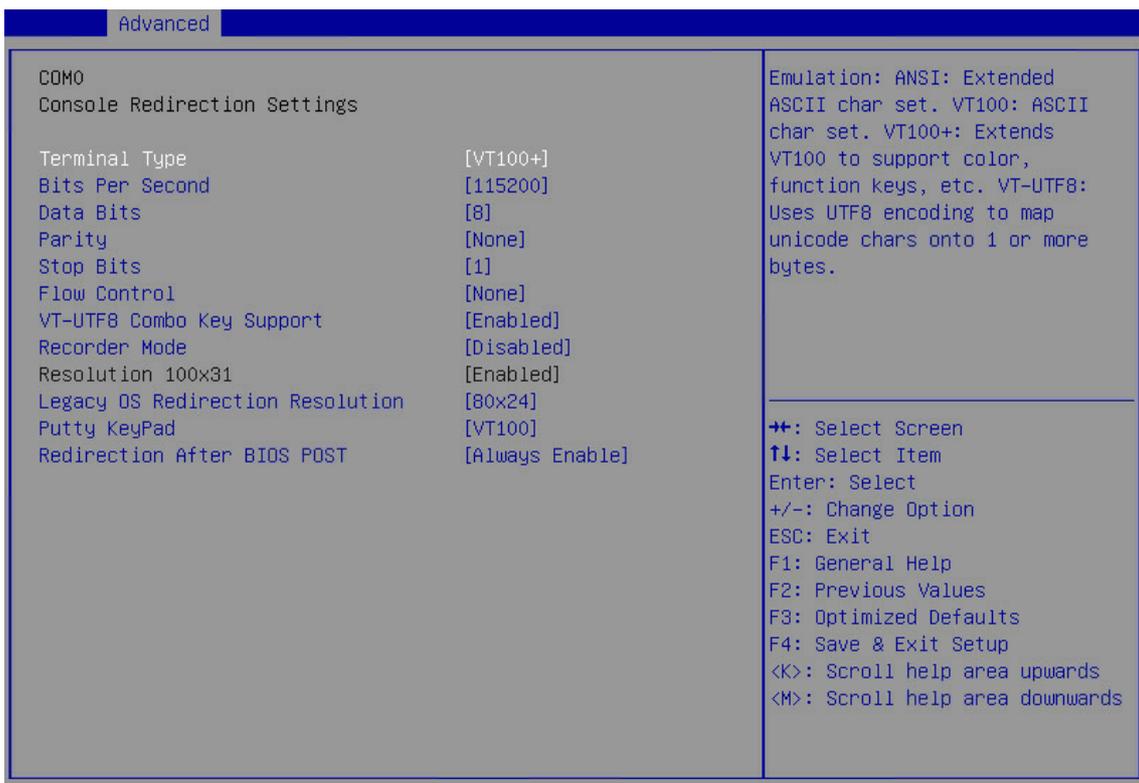


表3-21 COM0 端口的 Console Redirection Settings 界面参数

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，菜单选项为： <ul style="list-style-type: none"> <li>• None (缺省): 无校验，不进行数据的校验。</li> <li>• Even: 偶校验。</li> <li>• Odd: 奇校验。</li> <li>• Mark: 奇偶校验位始终为 1。</li> <li>• Space: 奇偶校验位始终为 0。</li> </ul> Mark和Space奇偶校验不支持错误检测。
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	显示扩展终端分辨率为100x31
Legacy OS Redirection Resolution	Legacy OS重定向分辨率，设置支持重定向的行数和列数，菜单选项为： <ul style="list-style-type: none"> <li>• 80×24（缺省）</li> <li>• 80×25</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>
Redirection After BIOS POST	BIOS上电自检后重定向设置，菜单选项为： <ul style="list-style-type: none"> <li>• Always Enable（缺省）：始终启用 Legacy 控制台重定向。</li> <li>• BootLoader：选择启动加载程序，在启动到 Legacy 启动模式下安装的操作系统之后禁用 Legacy 控制台重定向。</li> </ul>

EMS的Console Redirection Settings界面如 [图 3-22](#) 所示。具体参数说明如 [表 3-22](#) 所示。

图3-22 Console Redirection Settings 界面

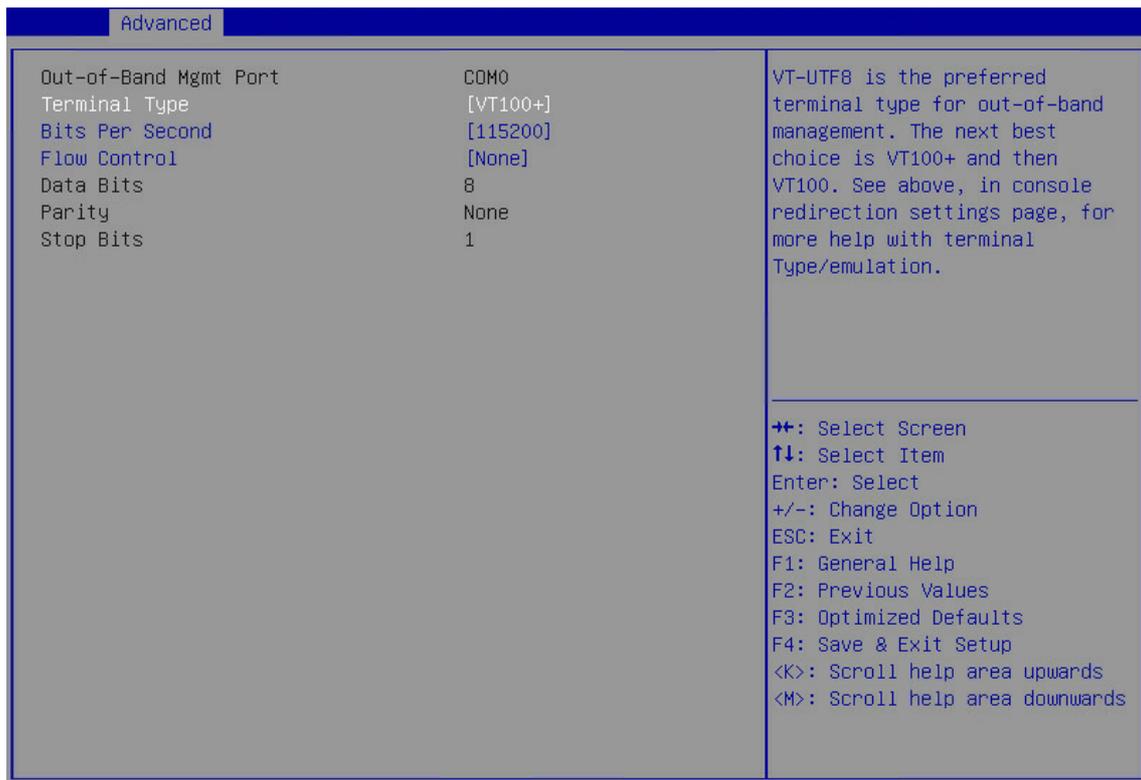


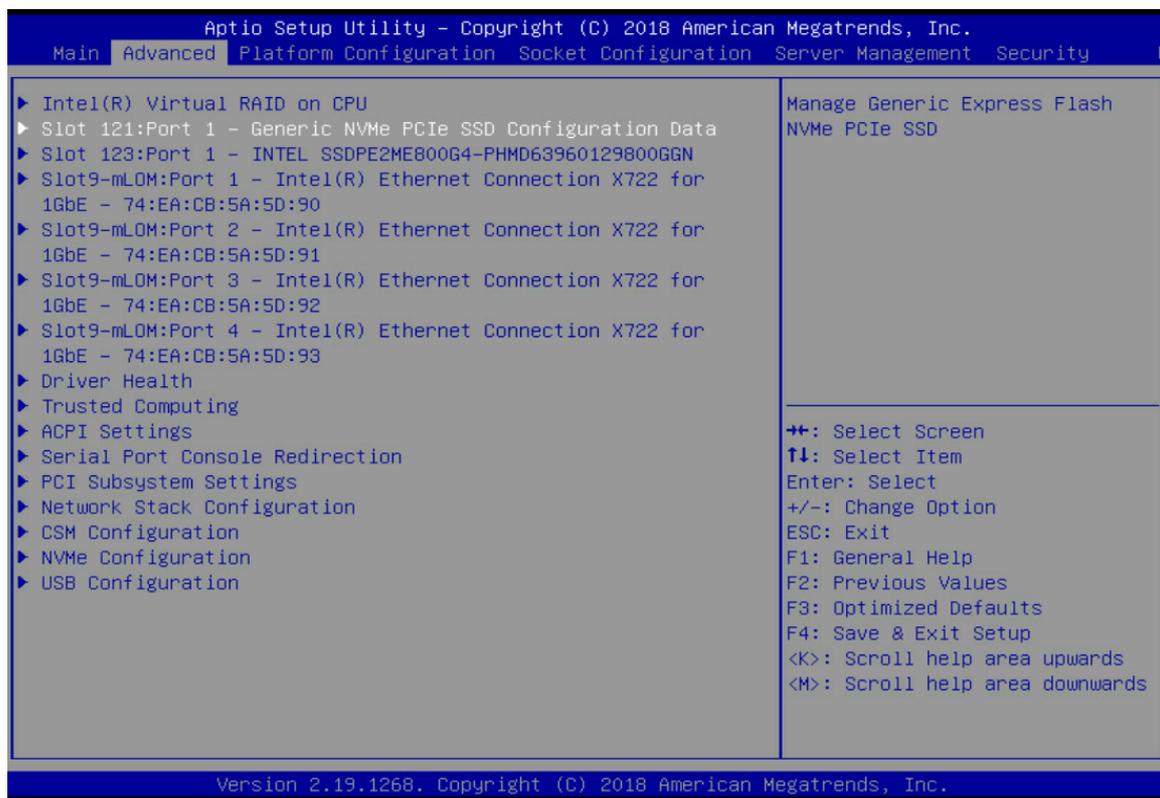
表3-22 EMS 的 Console Redirection Settings 界面参数

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。
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，None表示不进行校验。
Stop Bits	显示停止位（单个数据包的最后一位）。

### 3.2.6 Slot x:Port x界面

如 [图 3-23](#) 所示，通过Slot x:Port x界面，可以对以太网、RAID卡、带有OptionRom的Nvme盘进行配置接口进行配置。具体参数说明如 [表 3-23](#) 所示。

图3-23 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。下面 [图 3-24](#)，以板载的mLOM以太网卡Slot 9-mLOM:Port 1 为例说明界面参数。

图3-24 Slot 9-mLOM:Port 1 界面

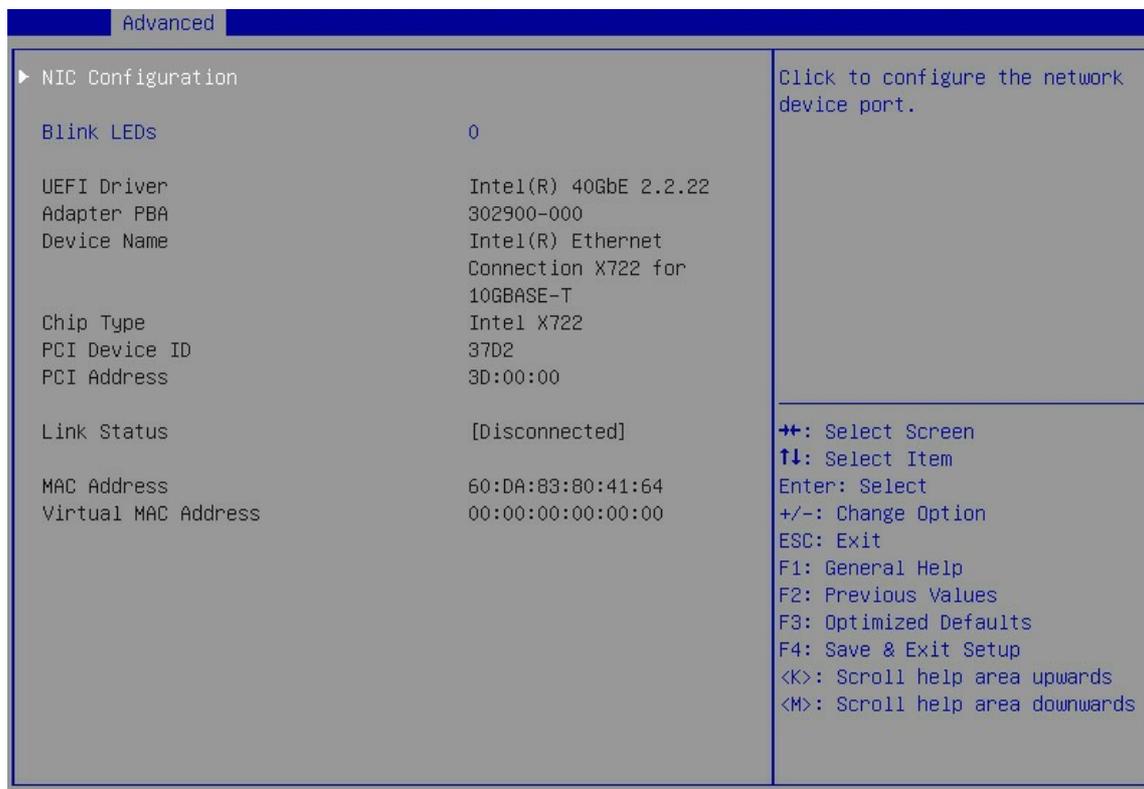


表3-23 Slot 9-mLOM:Port 1 界面参数

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 3-25](#) 所示。具体参数说明如 [表 3-24](#) 所示。

图3-25 NIC Configuration 界面

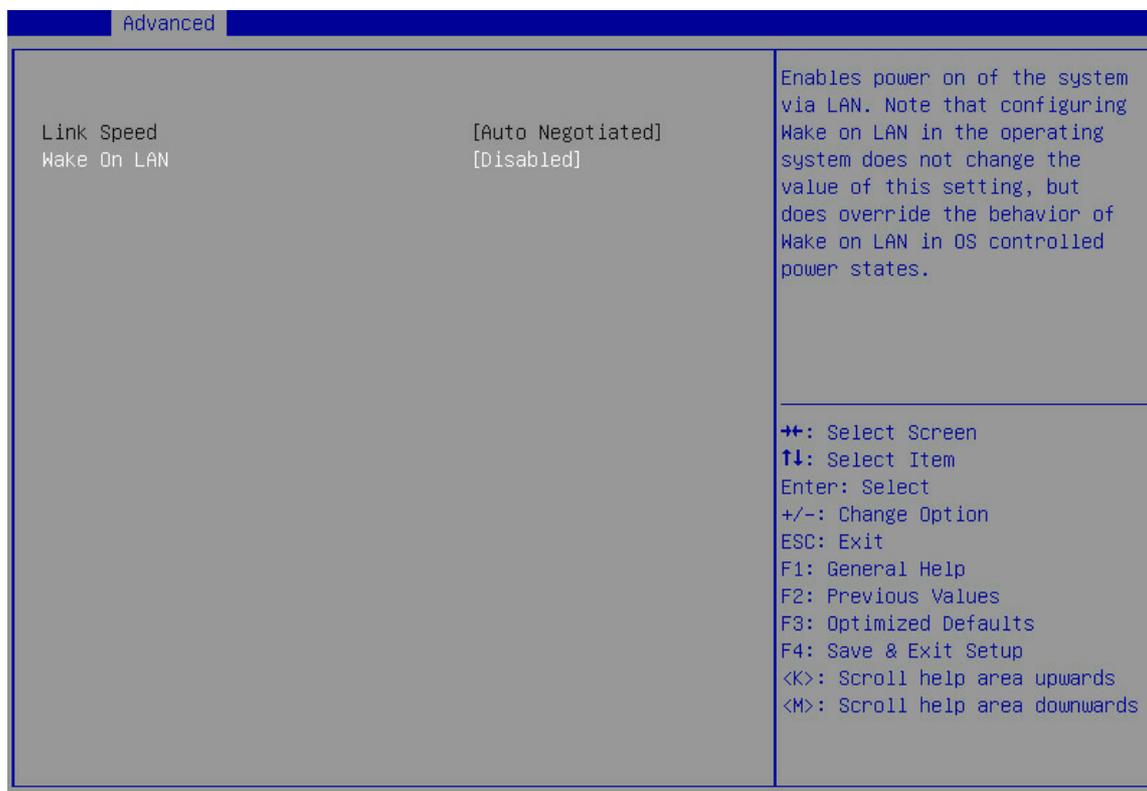


表3-24 NIC Configuration 界面参数

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：开启局域网唤醒功能。</li> <li>• Disabled（缺省）：关闭局域网唤醒功能。</li> </ul>

### 3.2.7 PCI Subsystem Settings界面

如 [图 3-26](#) 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 3-25](#) 所示。

图3-26 PCI Subsystem Settings 界面

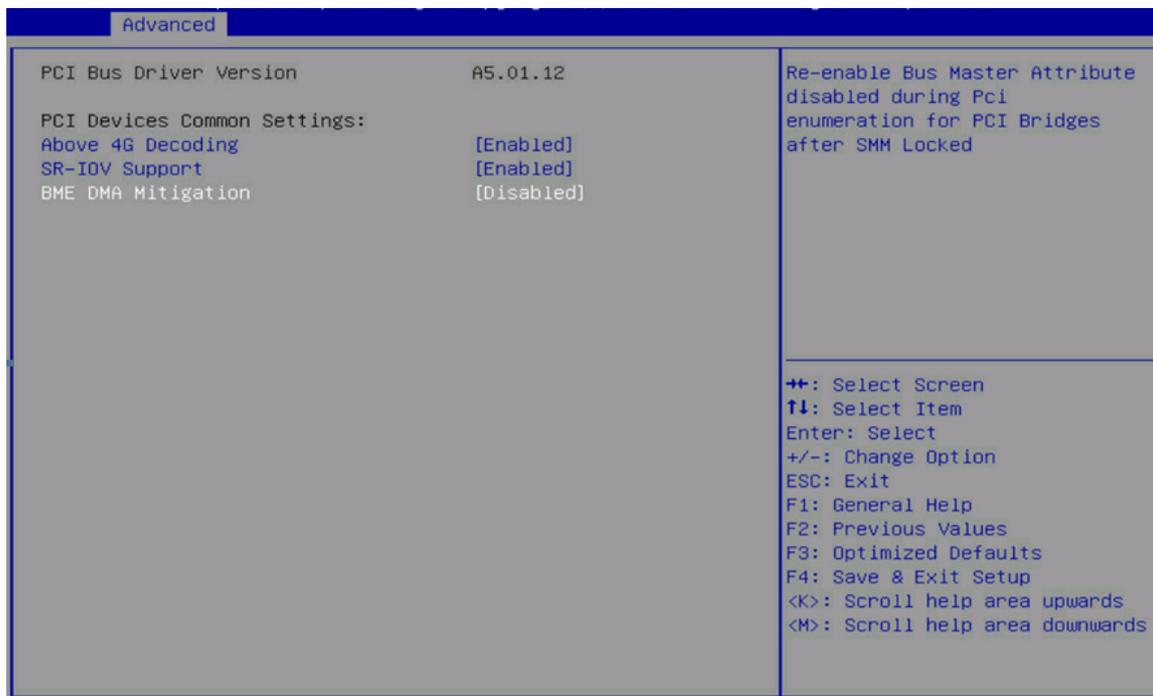


表3-25 PCI Subsystem Settings 界面参数

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PCI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>4GB Above 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4GB Above 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>虚拟化IO支持设置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：支持系统虚拟化IO。</li> <li>Disabled：如果PCIe卡支持SR-IOV，则由OS分配IO资源，如果PCIe卡不支持SR-IOV，则自动关闭虚拟化IO。</li> </ul>
BME DMA Mitigation	<p>BME DMA 减缓，用于阻止DMA侧信道攻击，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled：开启该功能后可阻止DMA侧信道攻击，会造成PCIe设备性能下降。</li> <li>Disabled（缺省）：设置为该选项后，DMA功能可用，PCIe设备性能正常。</li> </ul>

### 3.2.8 Network Stack Configuration界面

如 [图 3-27](#) 所示，通过Network Stack Configuration界面，可以对网络堆栈进行配置。具体参数说明如 [表 3-26](#) 所示。

图3-27 Network Stack Configuration 界面

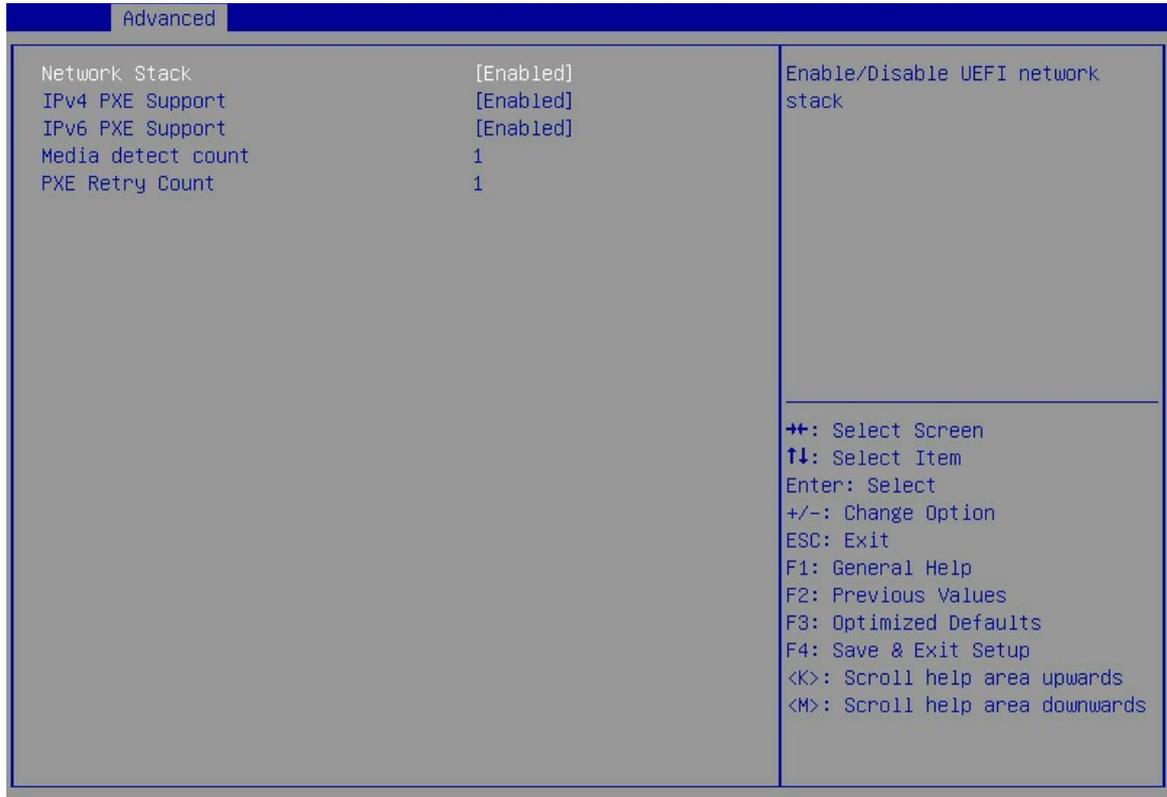


表3-26 Network Stack Configuration 界面参数

界面参数	功能说明
Network Stack	<p>网络堆栈配置，仅用于在UEFI启动模式下预先启动内建网络，开启该功能后，服务器可以从PXE服务器中获取镜像文件、从网络中启动操作系统，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启网络堆栈功能。</li> <li>• Disabled：关闭网络堆栈功能。</li> </ul>
IPv4 PXE Support	<p>IPv4 PXE支持，支持从IPv4网络启动操作系统，菜单选项为：</p> <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	<p>IPv6 PXE支持，支持从IPv6网络启动操作系统，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 IPv6 PXE 功能。</li> <li>• Disabled：关闭 IPv6 PXE 功能，不会创建 IPv6 PXE 启动选项。</li> </ul>

界面参数	功能说明
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。

### 3.2.9 CSM Configuration界面

如 [图 3-28](#) 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 3-27](#) 所示。

图3-28 CSM Configuration 界面

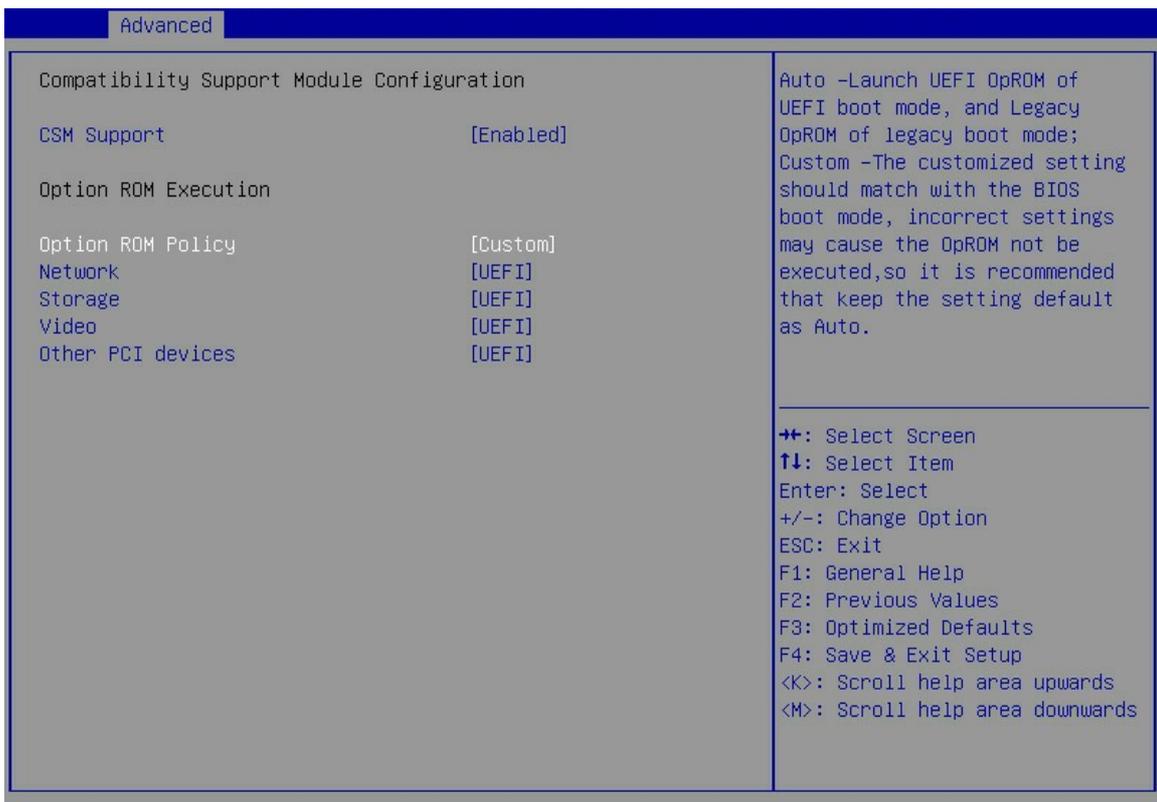


表3-27 CSM Configuration 界面参数

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>

界面参数	功能说明
<b>Option ROM Execution</b>	
Option ROM Policy	<p>配置Option ROM的加载策略，Option ROM可以理解为驱动程序，当CSM Support选项设置为Enabled时，该选项才显示菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto（缺省）：自动模式。</li> <li>• Custom：自定义模式 UEFI 启动模式下，4 个菜单（Network、Storage、Video、Other PCI Devices）选项均为 UEFI；Legacy 启动模式下，4 个菜单选项均为 Legacy，用户可以根据需求对四个选项进行分别自定义设置。</li> </ul>
Network	<p>设置网卡Option ROM的加载方式，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。</li> </ul>
Storage	<p>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：</p> <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。</li> </ul>
Video	<p>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：</p> <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。</li> </ul>
Other PCI Devices	<p>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：</p> <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。</li> </ul>

### 3.2.10 NVMe Configuration界面



说明

在 BIOS 下，VMD 功能不支持对 NVMe 硬盘进行点灯操作。

如 [图 3-29](#) 所示，通过 NVMe Configuration 界面，可以对 NVMe 进行配置。具体参数说明如 [表 3-28](#) 所示。

图3-29 NVMe Configuration 界面

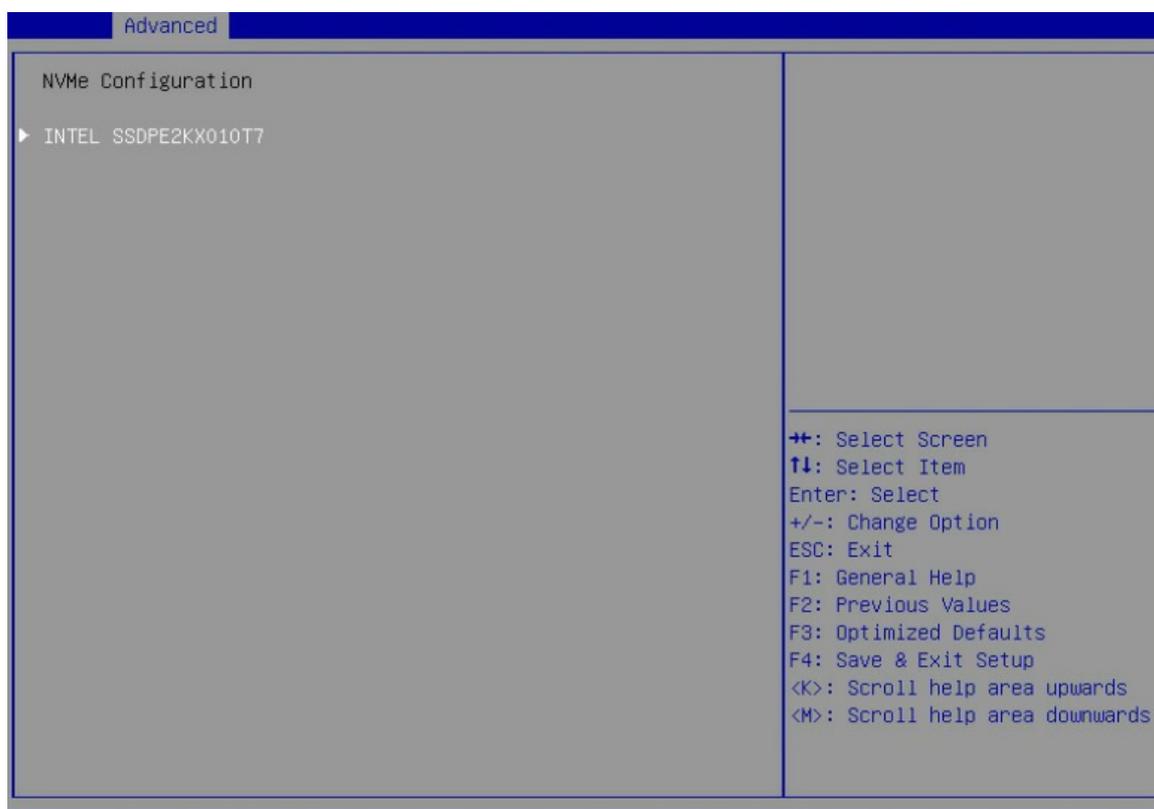


表3-28 NVMe Configuration 界面参数

界面参数	功能说明
INTEL SSDPE2KX010T7	可用的NVMe设备配置菜单（当连接NVMe设备时显示该设备）

如 [图 3-30](#) 所示，通过INTEL SSDPE2KX010T7（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 3-29](#) 所示。

图3-30 INTEL SSDPE2KX010T7（该 NVMe 设备信息）界面

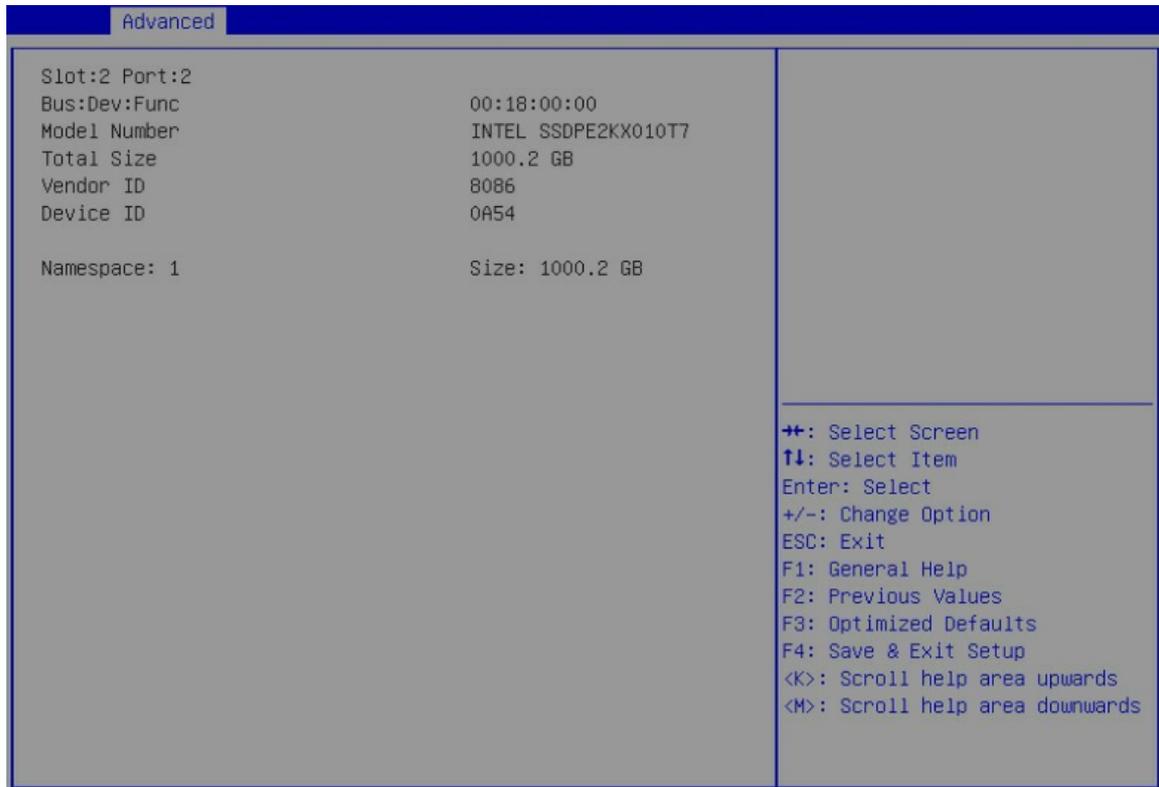


表3-29 INTEL SSDPE2KX010T7（该 NVMe 设备信息）界面参数

界面参数	功能说明
Slot: Port:	该NVMe设备的槽位号、端口号信息
Bus:Dev:Func	该NVMe设备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

### 3.2.11 USB Configuration界面

如 [图 3-31](#) 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 3-30](#) 所示。

图3-31 USB Configuration 界面

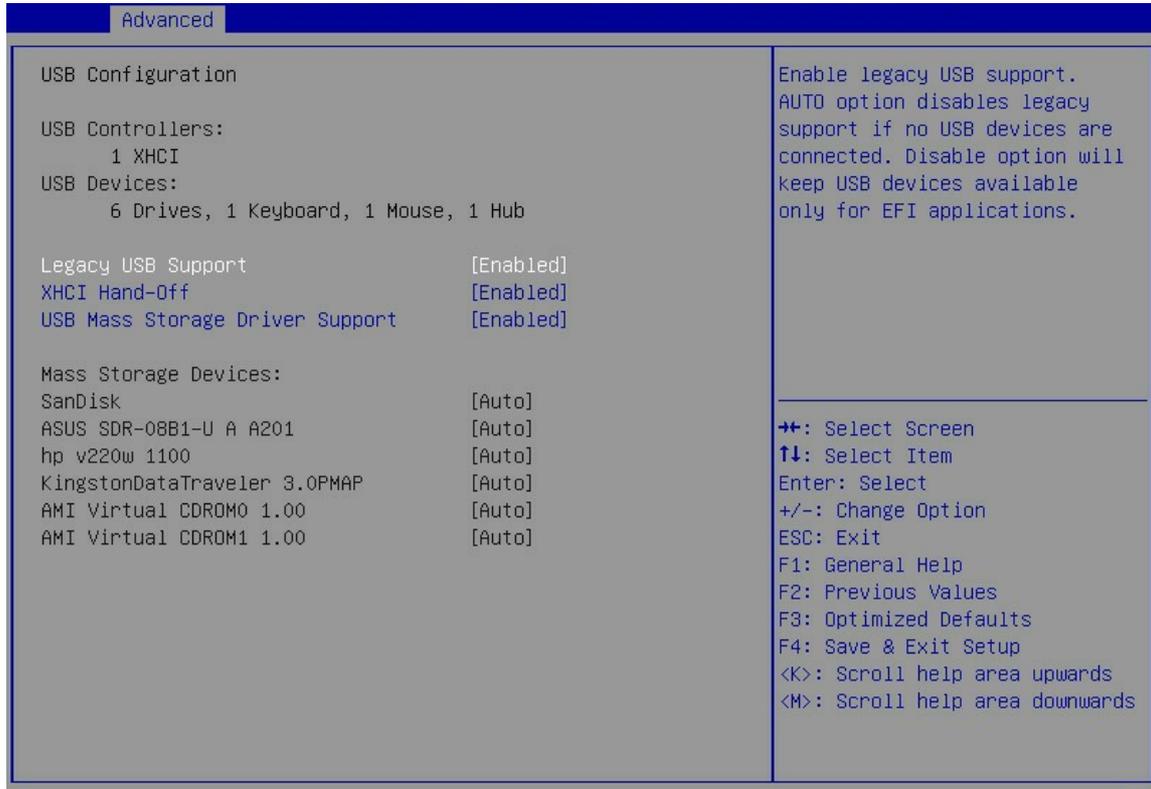


表3-30 USB Configuration 界面参数

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>
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>

界面参数	功能说明
USB Mass Storage Driver Support	支持大容量USB存储设备，菜单选项为： <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	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： <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 CDROM0 1.00	虚拟光驱
H3C Virtual CDROM0 1.00	启动远程控制台后，默认会挂载虚拟CDROM0，虚拟CDROM可实现与物理CDROM相同的功能。
H3C Virtual Floppy0 1.00	启动远程控制台后，默认会挂载Floppy0，虚拟Floppy可实现与物理Floppy相同的功能。
H3C Virtual HDisk0 1.00	启动远程控制台后，默认会挂载虚拟HDisk0，虚拟HDisk可实现与物理HDisk相同的功能。
H3C Virtual CDROM1 1.00	启动远程控制台后，默认会挂载虚拟CDROM1，虚拟CDROM可实现与物理CDROM相同的功能。
H3C Virtual Floppy1 1.00	启动远程控制台后，默认会挂载虚拟Floppy1，虚拟Floppy可实现与物理Floppy相同的功能。
H3C Virtual HDisk1 1.00	启动远程控制台后，默认会挂载虚拟HDisk1，虚拟HDisk可实现与物理HDisk相同的功能。

### 3.3 Platform Configuration界面

介绍 Platform Configuration 界面包含的参数及相关功能。

Platform Configuration界面如 [图 3-32](#) 所示，主要包含PCH配置、混合配置菜单、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 3-31](#) 所示。

图3-32 Platform Configuration 界面

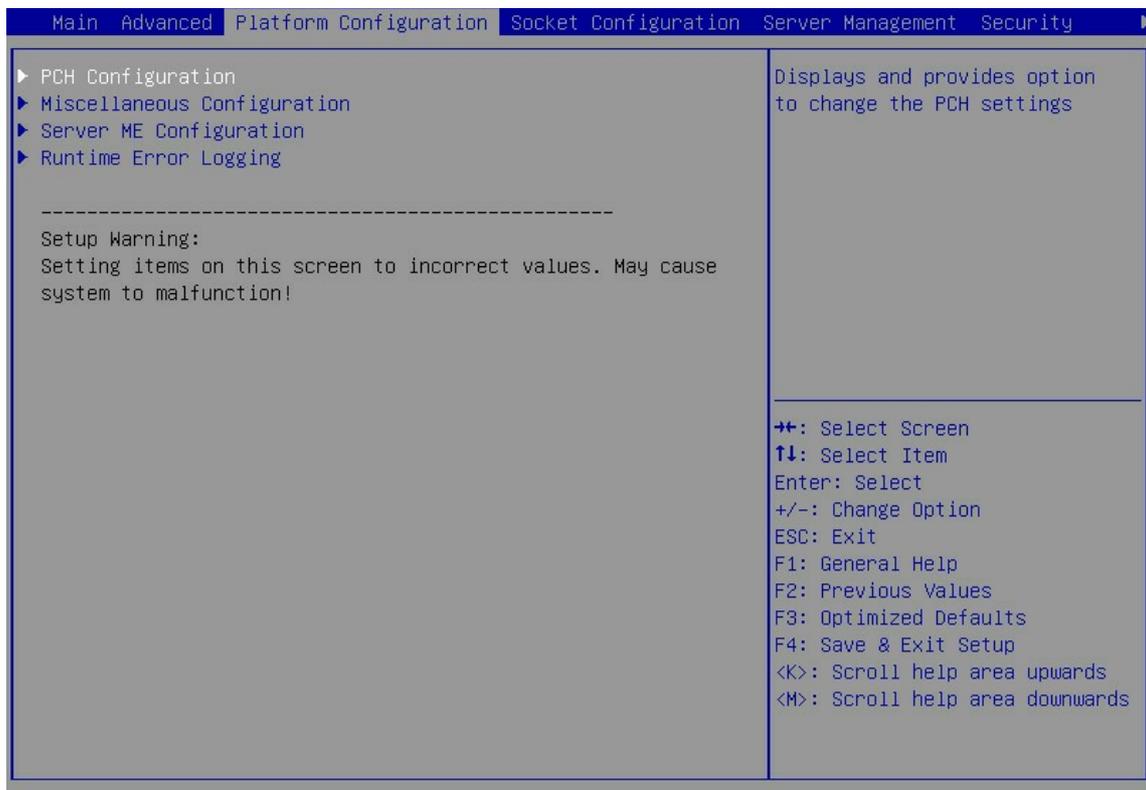


表3-31 Platform Configuration 界面参数

界面参数	功能说明
PCH Configuration	PCH配置菜单
Miscellaneous Configuration	混合配置菜单
Server ME Configuration	服务器ME配置菜单
Runtime Error Logging	运行错误记录菜单

### 3.3.1 PCH Configuration 界面

如 [图 3-33](#) 所示，通过PCH Configuration界面，可以对PCH进行配置，包括PCH设备、硬盘接口、USB等。具体参数说明如 [表 3-32](#) 所示。

图3-33 PCH Configuration 界面

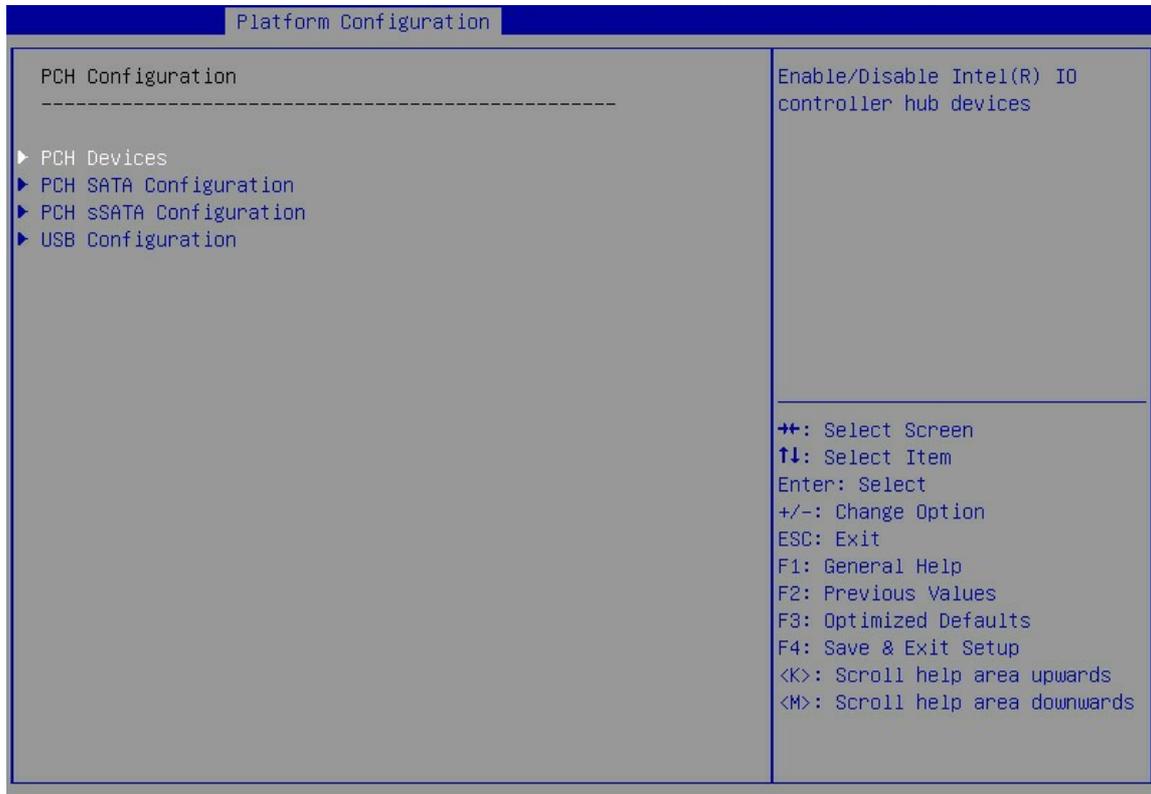


表3-32 PCH Configuration 界面参数

界面参数	功能说明
PCH Devices	PCH设备配置菜单
PCH SATA Configuration	PCH SATA配置菜单
PCH sSATA Configuration	PCH sSATA配置菜单
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 3-34](#) 和 [表 3-35](#)。

PCH Devices界面如 [图 3-34](#) 所示。具体参数说明如 [表 3-33](#) 所示。

图3-34 PCH Devices 界面

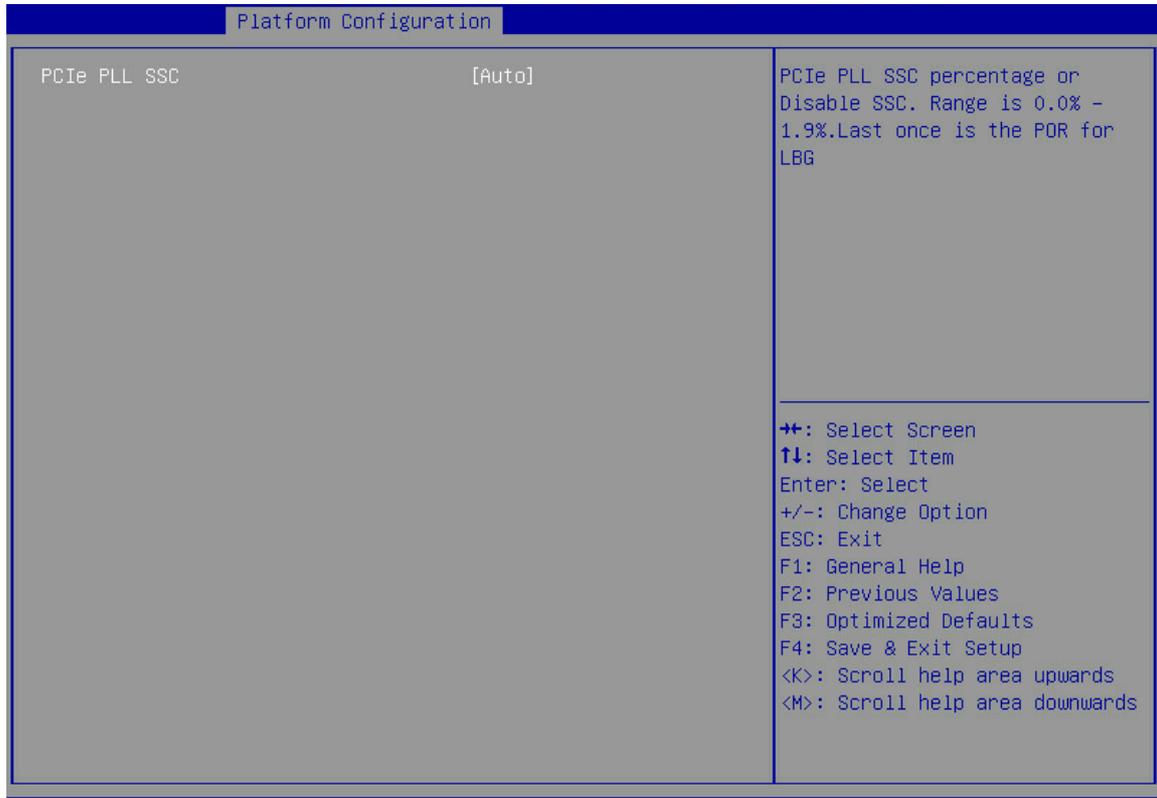


表3-33 PCH Devices 界面参数

界面参数	功能说明
PCIe PLL SSC	PCIe PLL SSC配置，设置PCIe锁相环扩频时钟，菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 禁用扩频时钟。</li> <li>• Auto (缺省): 根据设备自动配置扩频时钟频率。</li> <li>• 0.5%: 设置扩频时钟为总线时钟的百分比。</li> </ul>

PCH SATA Configuration界面如 [图 3-35](#) 所示。具体参数说明如 [表 3-34](#) 所示。

图3-35 PCH SATA Configuration 界面

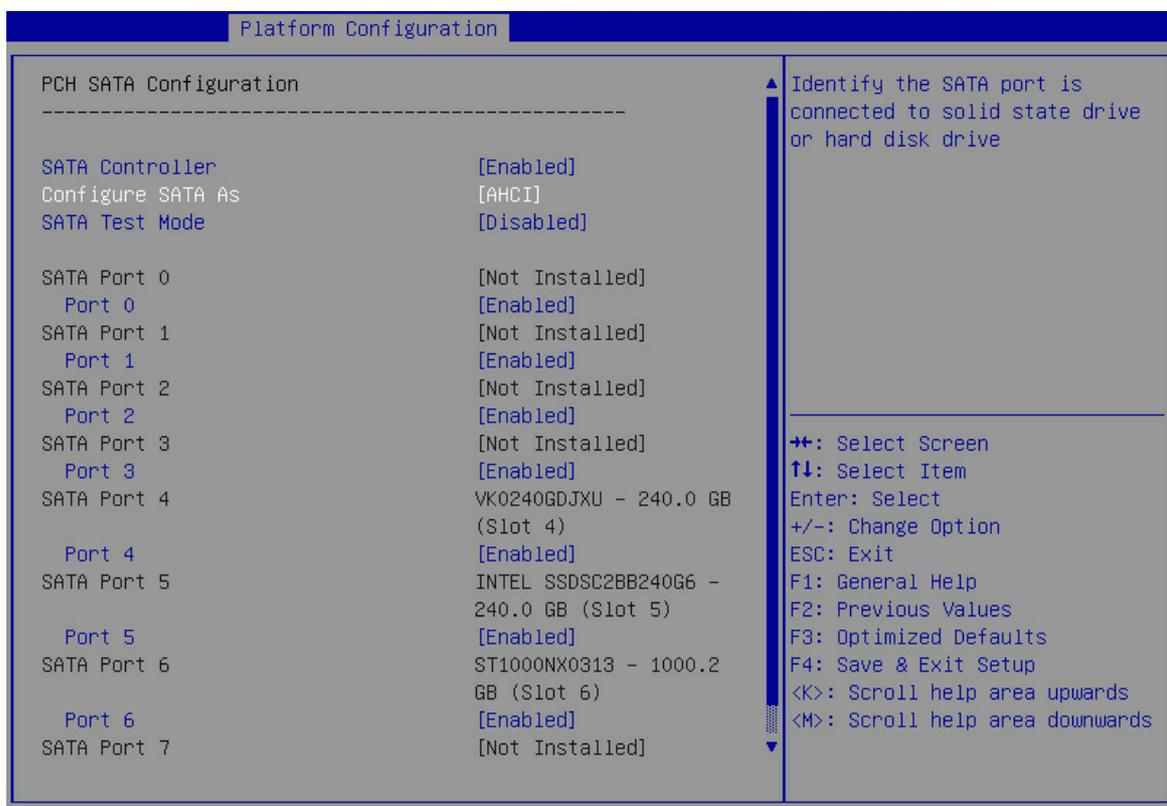


表3-34 PCH SATA Configuration 界面参数

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 控制器功能。</li> <li>Disabled: 关闭 SATA 控制器功能。</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。</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 0	<p>SATA端口0的设备名称以及槽位号, 设备不在位时显示Not Installed。 SATA端口与背板槽位的对应关系请参见<a href="#">4 SATA sSATA端口与背板槽位的对应关系</a>。</p>

界面参数	功能说明
Port 0	端口0设备开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 SATA 端口 0 设备。</li> <li>• Disabled：关闭 SATA 端口 0 设备。</li> </ul> SATA Port 1、SATA Port 2、SATA Port 3、SATA Port 4、SATA Port 5 与SATA Port 0的界面参数相同，本文以SATA Port 0为例。

 说明

PCH sSATA Configuration 的界面相关选项配置内容会根据机型的不同而产生不同的差异。R4900、R4700 属于 24DIMM 机台,其 sSATA 控制器仅输出一个 port。R2900、R2700 属于 16DIMM 机台,其 sSATA 控制器输出 6 个 port。具体如下图所示:

PCH sSATA Configuration界面如 [图 3-36](#) 和 [图 3-37](#) 所示。具体参数说明如 [表 3-35](#) 所示。

图3-36 PCH sSATA Configuration 界面(H3C UniServer R4900 G3 和 H3C UniServer R4700 G3)

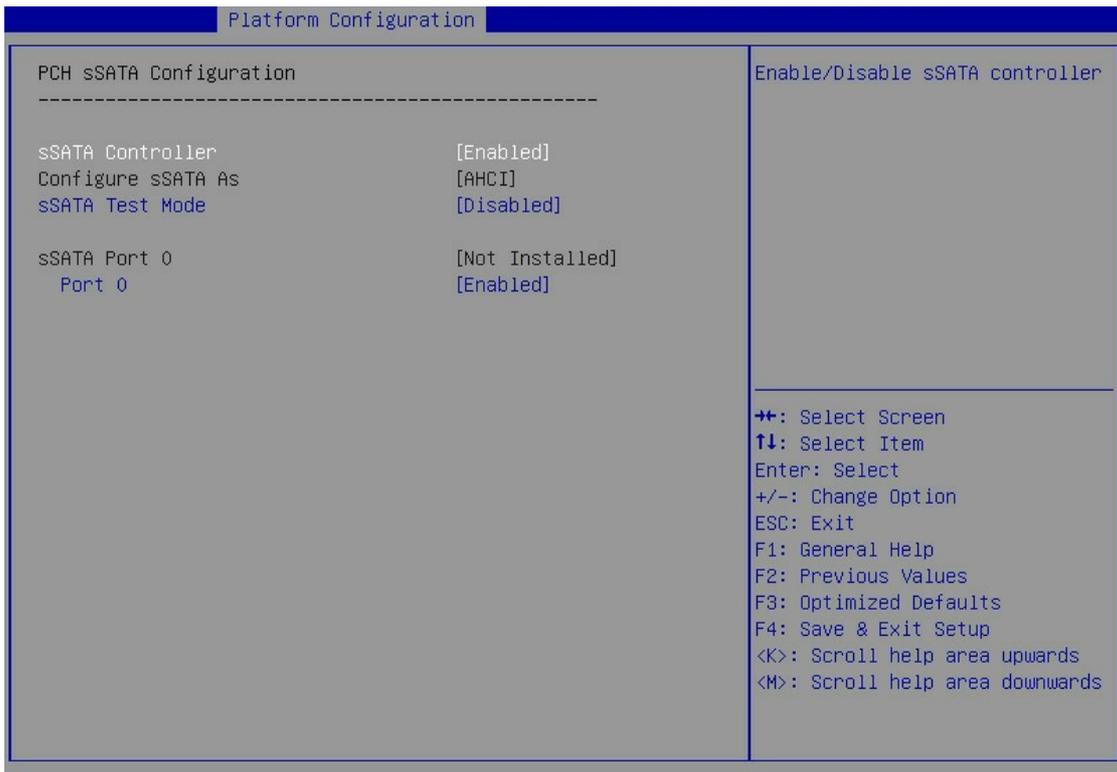


图3-37 PCH sSATA Configuration 界面(H3C UniServer R2900 G3 和 H3C UniServer R2700 G3)

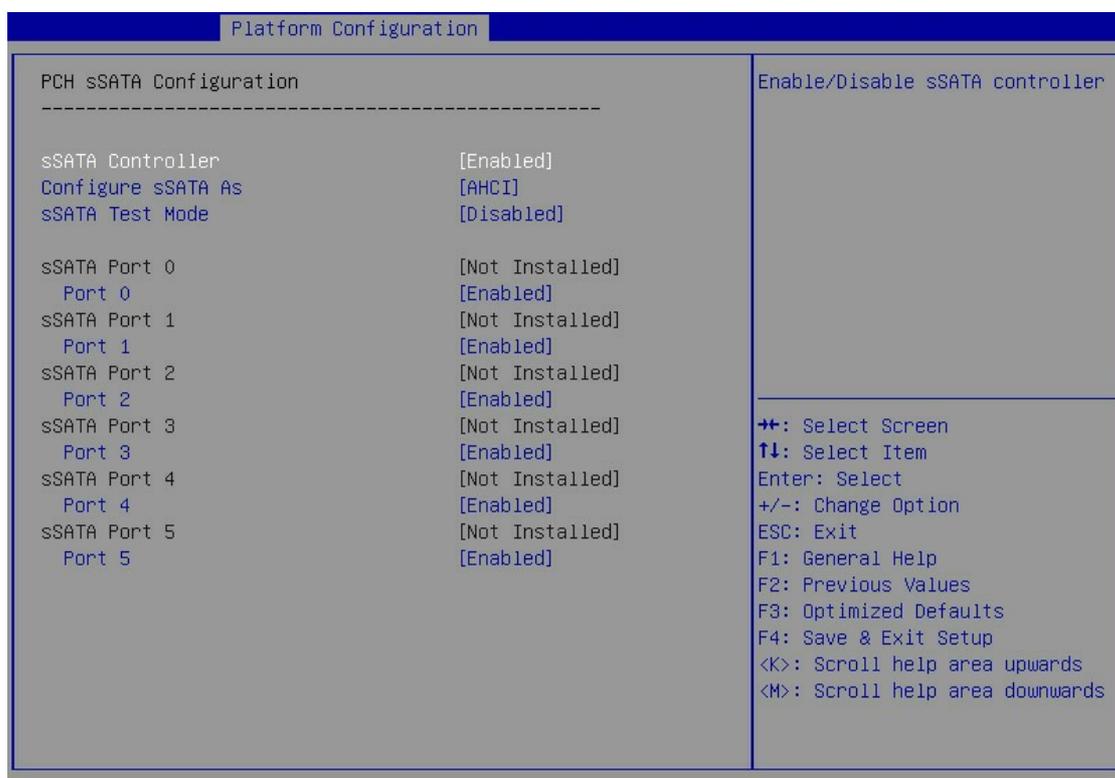


表3-35 PCH sSATA Configuration 界面参数

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 SATA Test 模式进行配置。</li> <li>Disabled：关闭 sSATA 控制器功能。</li> </ul>
Configure sSATA as	配置sSATA模式，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	SATA Test模式开关，菜单选项为： <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>
sSATA Port X	sSATA端口0的设备名称以及槽位号，设备不在位时显示Not Installed。sSATA端口与背板槽位的对应关系请参见 <a href="#">4 SATA sSATA端口与背板槽位的对应关系</a> 。

界面参数	功能说明
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> sSATA Port 1（slot1）、sSATA Port 2（slot2）、sSATA Port 3（slot3）与sSATA Port 0（slot0）的界面参数相同，本文以sSATA Port 0（slot0）为例。

 说明

USB Configuration的界面USB端口配置情况会根据机型的不同而产生不同的差异。R4900 和 2900 属于 2U机型，USB端口的配置多出一个前部右挂耳USB3.0 端口；而R4700 和 2700 属于 1U机型，USB端口的配置无前部右挂耳USB端口。具体如 [图 3-38](#) 和 [图 3-39](#) 所示：

USB Configuration界面如 [图 3-38](#) 和 [图 3-39](#) 所示。具体参数说明如 [表 3-36](#) 所示。

图3-38 USB Configuration 界面（H3C UniServer R4900 G3 和 H3C UniServer R2900 G3）

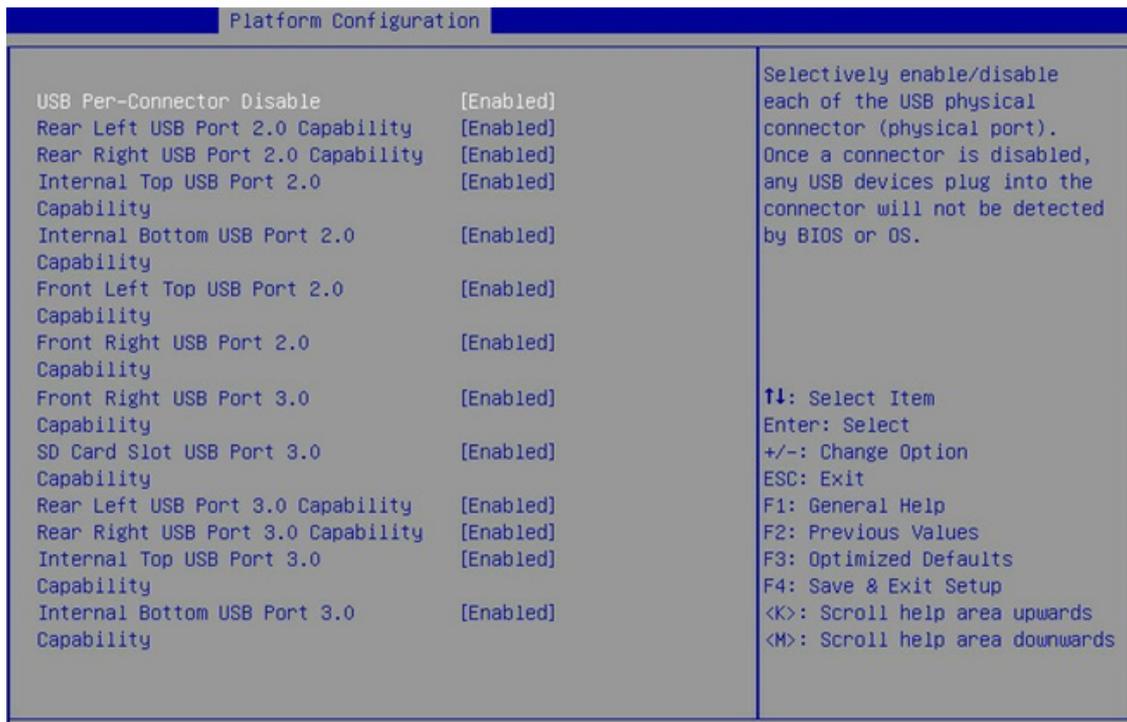


图3-39 USB Configuration 界面（H3C UniServer R4700 G3 和 H3C UniServer R2700 G3）

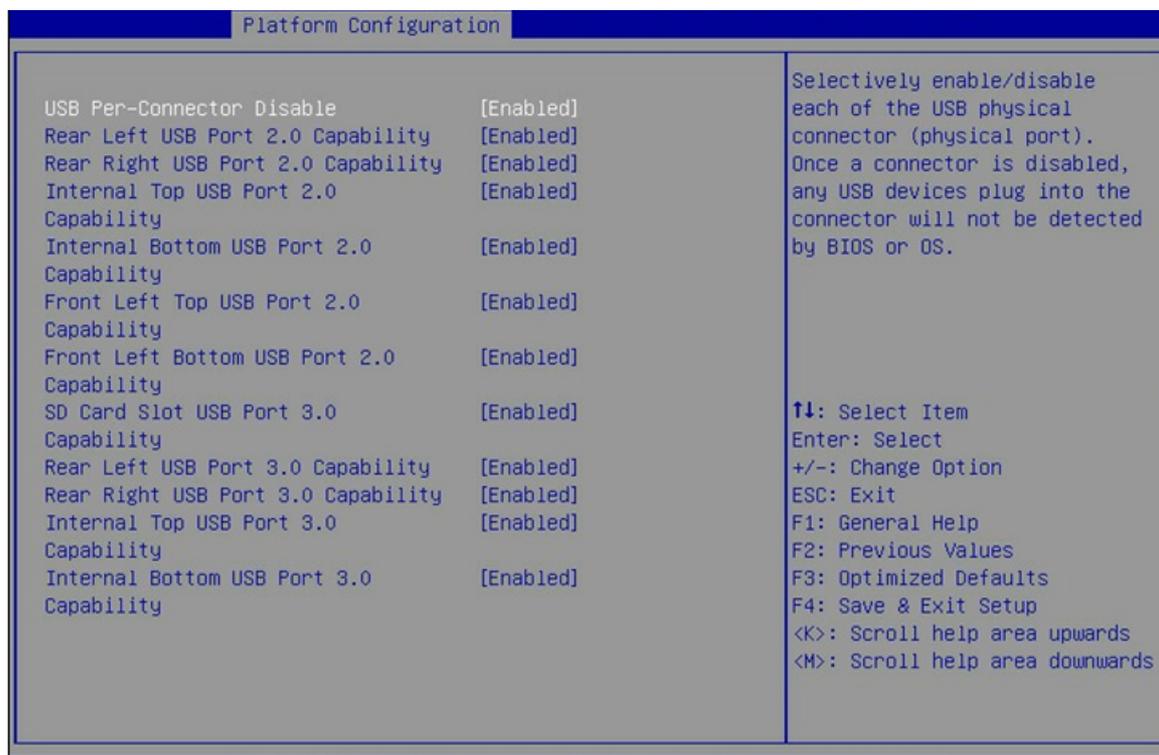


表3-36 USB Configuration 界面参数

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>
Rear Left USB Port 2.0 Capability	<p>后部左端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled（缺省）：开启后部左端 USB 2.0 功能。</li> <li>Disabled: 关闭后部左端 USB 2.0 功能。</li> </ul>
Rear Right USB Port 2.0 Capability	<p>后部右端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）：开启后部右端 USB 2.0 功能。</li> <li>Disabled: 关闭后部右端 USB 2.0 功能。</li> </ul>
Internal Top USB Port 2.0 Capability	<p>内部顶端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）：开启内部顶端 USB 2.0 功能。</li> <li>Disabled: 关闭内部顶端 USB 2.0 功能。</li> </ul>

界面参数	功能说明
Internal Bottom USB Port 2.0 Capability	内部底端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启内部底端 USB 2.0 功能。</li> <li>• Disabled：关闭内部底端 USB 2.0 功能。</li> </ul>
Front Left Top 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 Left Bottom USB Port 2.0 Capability	前部左挂耳底端USB 2.0功能配置，当USB Per-Connector Disable设置为Enabled时显示，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启前部左挂耳底端 USB 2.0 功能。</li> <li>• Disabled：关闭前部左挂耳底端 USB 2.0 功能。</li> </ul>
Front Right USB Port 3.0 Capability	前部右挂耳USB 3.0功能配置，R4900/2900（2U）机型的服务器才配置该USB端口，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 3.0 功能。</li> <li>• Disabled：关闭前部右挂耳 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 Left USB Port 3.0 Capability	后部左端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）：开启后部左端 USB 3.0 功能。</li> <li>• Disabled：关闭后部左端 USB 3.0 功能。</li> </ul>
Rear Right USB Port 3.0 Capability	后部右端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）：开启后部右端 USB 3.0 功能。</li> <li>• Disabled：关闭后部右端 USB 3.0 功能。</li> </ul>
Internal Top USB Port 3.0 Capability	内部顶端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）：开启内部顶端 USB 3.0 功能。</li> <li>• Disabled：关闭内部顶端 USB 3.0 功能。</li> </ul>
Internal Bottom USB Port 3.0 Capability	内部底端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）：开启内部底端 USB 3.0 功能。</li> <li>• Disabled：关闭内部底端 USB 3.0 功能。</li> </ul>

### 3.3.2 Miscellaneous Configuration界面

如 图 3-40 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、SOL模式开关等。具体参数说明如 表 3-37 所示。

图3-40 Miscellaneous Configuration 界面

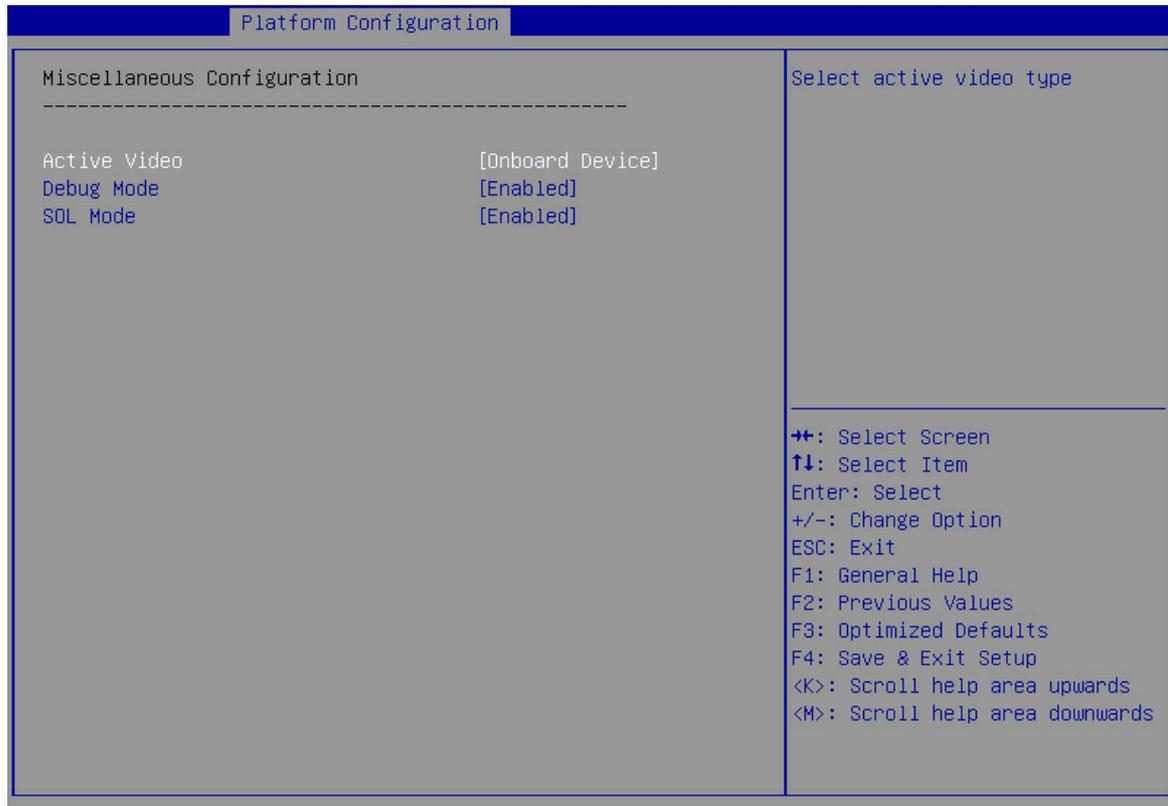


表3-37 Miscellaneous Configuration 界面参数

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。 开启该功能后，如果安装了 GPU 卡，在 Leagcy 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。</li> <li>• <b>PCIe Device:</b> 服务器通过 PCIe 设备 GPU 卡进行界面显示。 安装 GPU 卡并开启该功能后，在 Leagcy 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。</li> </ul>

界面参数	功能说明
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 (缺省):</b> 关闭 BIOS 串口日志输出功能。</li> </ul>
SOL Mode	<p>SOL功能开关，仅当Debug Mode选项设置为Enabled时，才会出现该选项。开启该功能后，您可以在Linux操作系统下，通过“<code>curl http://HDM IP地址/cgi/download_cpsol.cgi   tr -d '\000' &gt; sol.txt</code>”命令从服务器下载BIOS串口日志。</p> <ul style="list-style-type: none"> <li>• <b>HDM IP 地址:</b> 服务器 HDM 共享网络接口或 HDM 专用网络接口的 IP 地址。</li> <li>• <b>sol.txt:</b> 下载后的 BIOS 串口日志文件的名称，您可根据需求对文件进行重命名。</li> </ul> <p>菜单项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled (缺省):</b> 开启 SOL 功能。</li> <li>• <b>Disabled:</b> 关闭 SOL 功能。</li> </ul>

### 3.3.3 Server ME Configuration界面

如 [图 3-41](#) 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 3-38](#) 所示。

图3-41 Server ME Configuration 界面

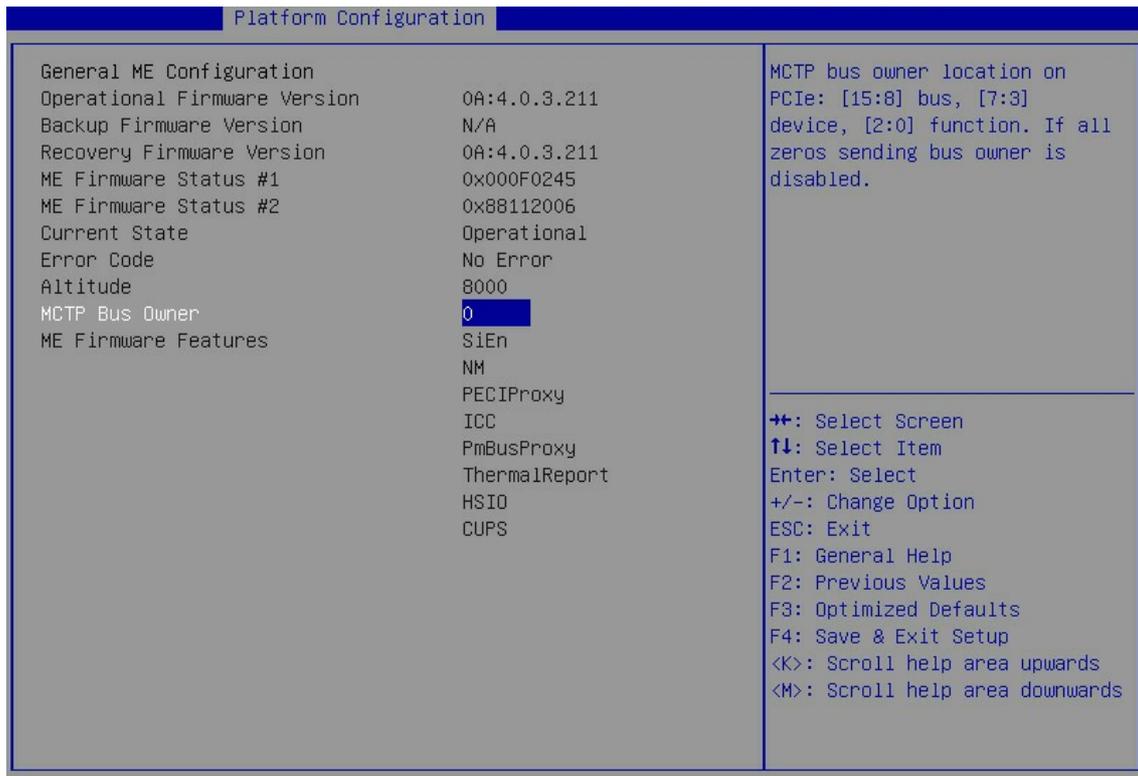


表3-38 Server ME Configuration 界面参数

界面参数	功能说明
Operational 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。
Altitude	显示平台位置的高度，缺省值为8000，单位为米。
MCTP Bus Owner	MCTP可以用来监测CPU，改变或者交换总线用户。
ME Firmware Features	显示ME固件的特征信息。

### 3.3.4 Runtime Error Logging界面

如 [图 3-42](#) 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 3-39](#) 所示。

图3-42 Runtime Error Logging 界面

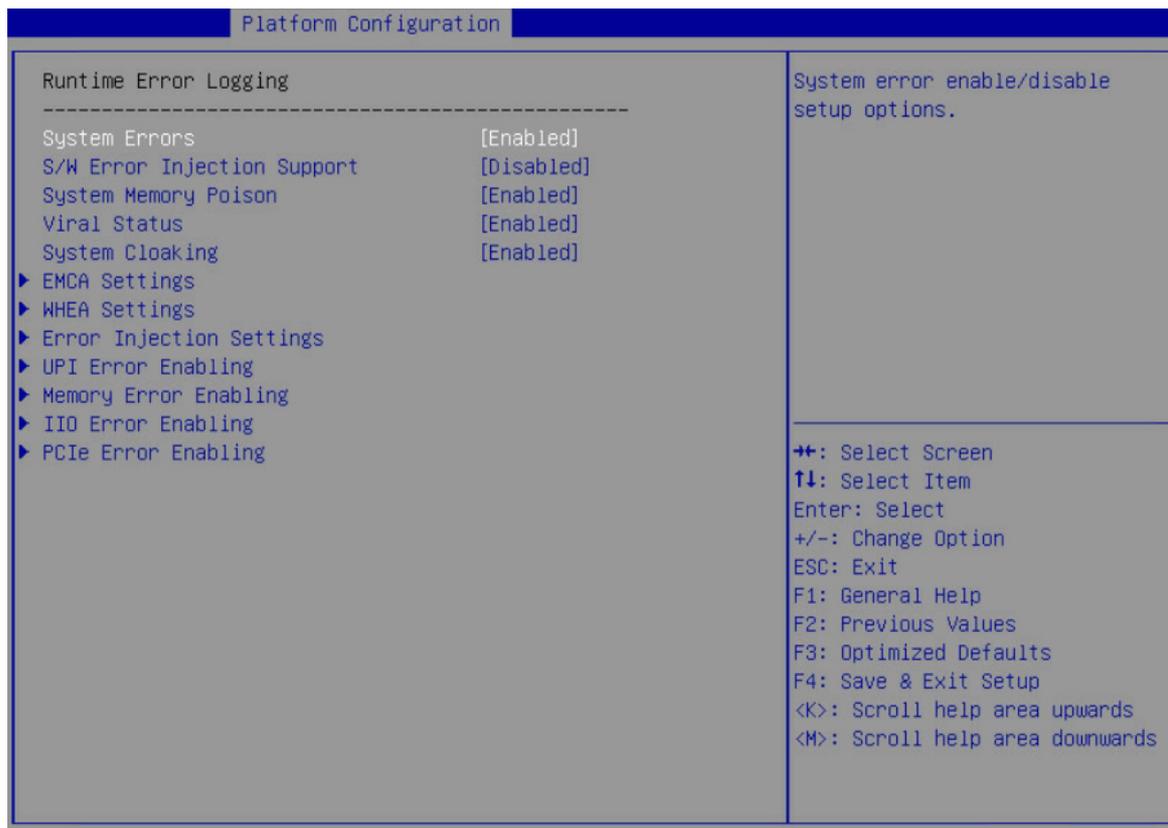


表3-39 Runtime Error Logging 界面参数

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>• <b>Enabled</b>（缺省）：开启系统错误记录功能。</li> <li>• <b>Disabled</b>：关闭系统错误记录功能。</li> </ul>
S/W 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>• <b>Enabled</b>：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>• <b>Disabled</b>（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，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>• <b>Enabled</b>（缺省）：开启系统内存 Poison 功能。</li> <li>• <b>Disabled</b>：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>
Viral Status	<p>病毒状态配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>（缺省）：启用内存病毒。</li> <li>• <b>Disabled</b>：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>
System Cloaking	<p>系统Cloaking功能配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>（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>• <b>Disabled</b>：禁用系统 Cloaking 功能。</li> </ul>
EMCA Settings	EMCA设置菜单
WHEA Settings	WHEA设置菜单
Error Injection Settings	错误注入设置菜单
UPI Error Enabling	UPI错误启用菜单
Memory Error Enabling	内存错误启用菜单
IIO Error Enabling	IIO错误启用菜单
PCIe Error Enabling	PCIE错误启用菜单

EMCA Settings界面如 [图 3-43](#) 所示。具体参数说明如 [表 3-40](#) 所示。

图3-43 EMCA Settings 界面

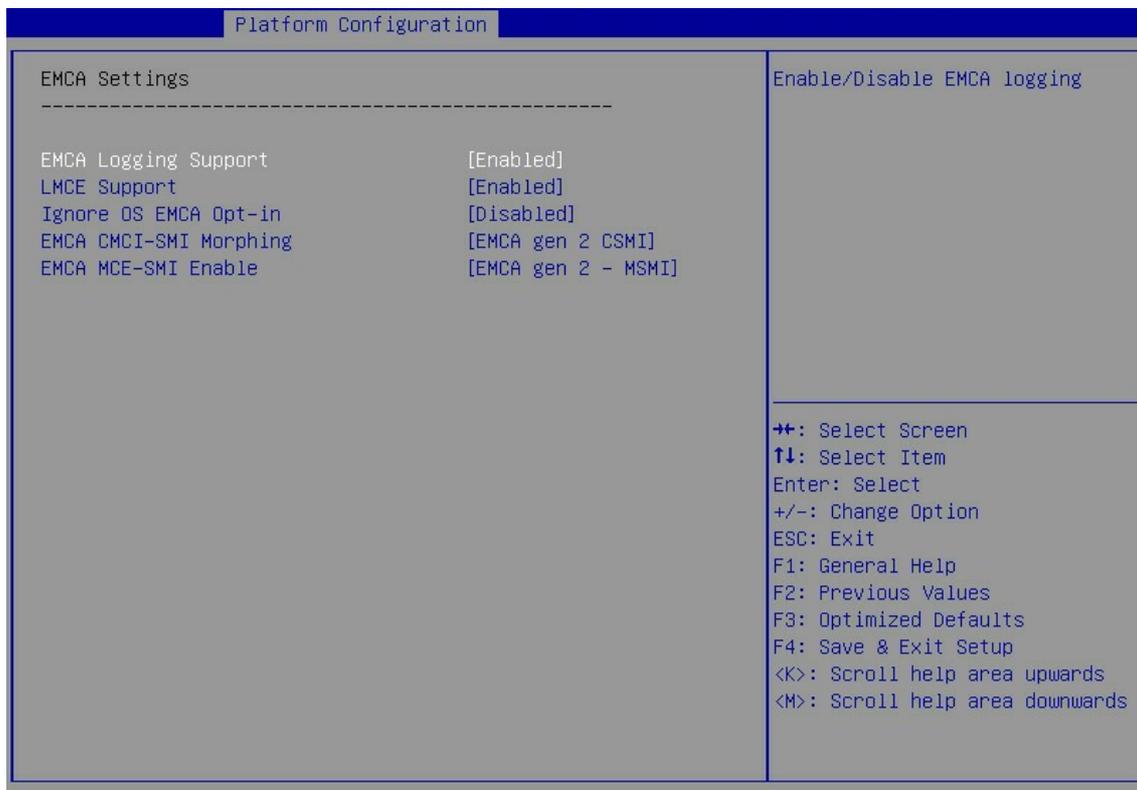


表3-40 EMCA Settings 界面参数

界面参数	功能说明
EMCA Logging Support	EMCA记录支持设置，该功能可以为服务器提供MCA错误报告，菜单选项为： <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	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： <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	忽略OS EMCA选入功能，当System Errors设置为Enabled时显示，菜单选项为： <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System Errors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，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>

WHEA Settings界面如 [图 3-44](#) 所示。具体参数说明如 [表 3-41](#) 所示。

图3-44 WHEA Settings 界面



表3-41 WHEA Settings 界面参数

界面参数	功能说明
WHEA Support	<p>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：</p> <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>

Error Injection Settings界面如 [图 3-45](#) 所示。具体参数说明如 [表 3-42](#) 所示。

图3-45 Error Injection Settings 界面

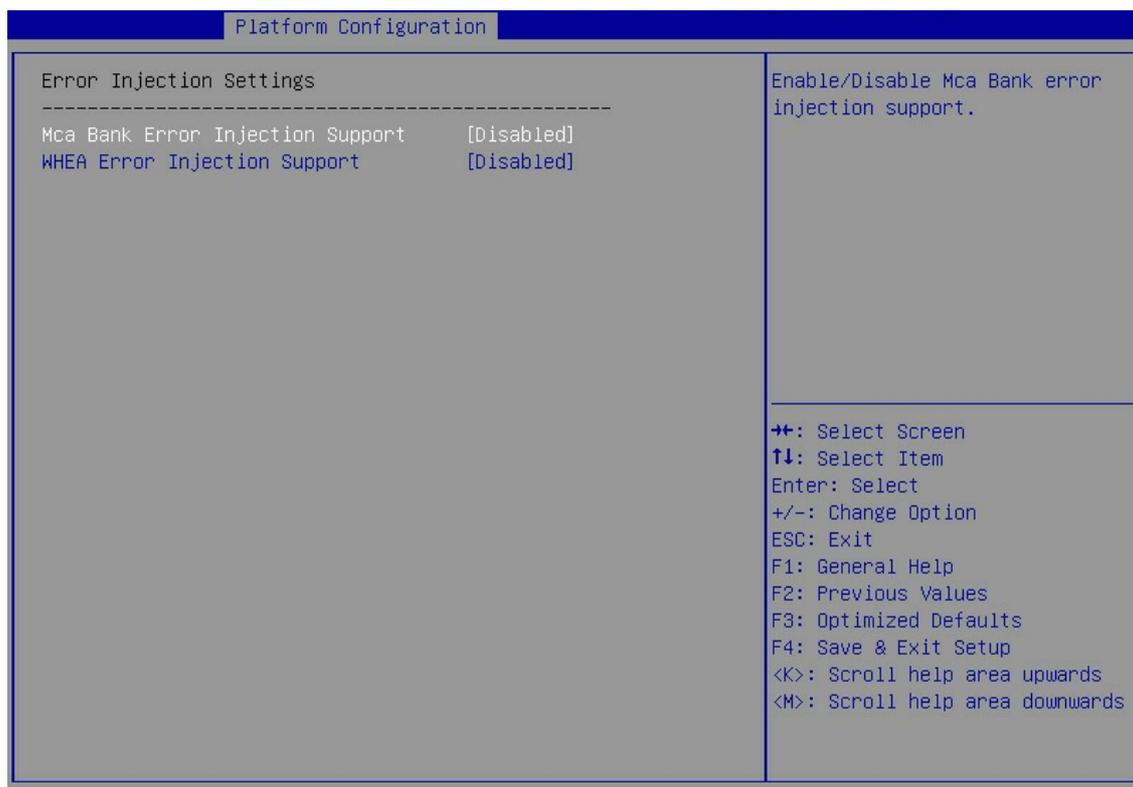


表3-42 Error Injection Settings 界面参数

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 Error Injection 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>

UPI Error Enabling界面如 [图 3-46](#) 所示。具体参数说明如 [表 3-43](#) 所示。

图3-46 UPI Error Enabling 界面

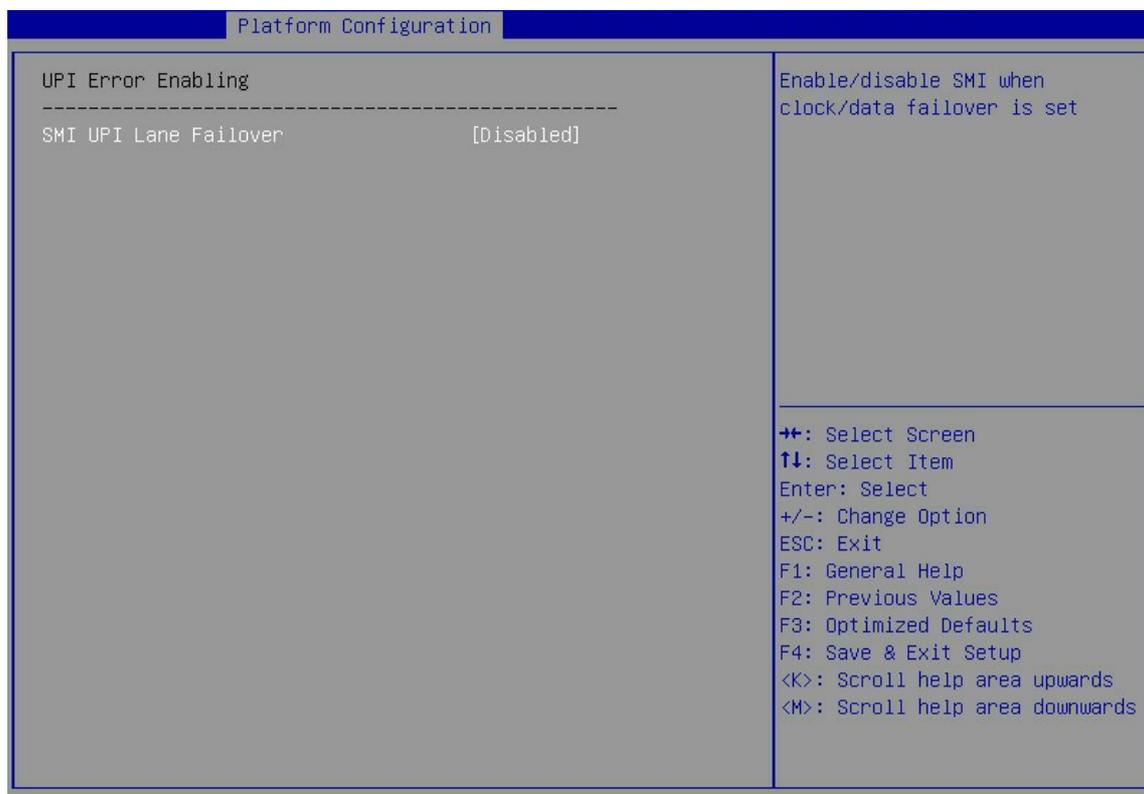


表3-43 UPI Error Enabling 界面参数

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>

Memory Error Enabling 界面如 [图 3-47](#) 所示。具体参数说明如 [表 3-44](#) 所示。

图3-47 Memory Error Enabling 界面

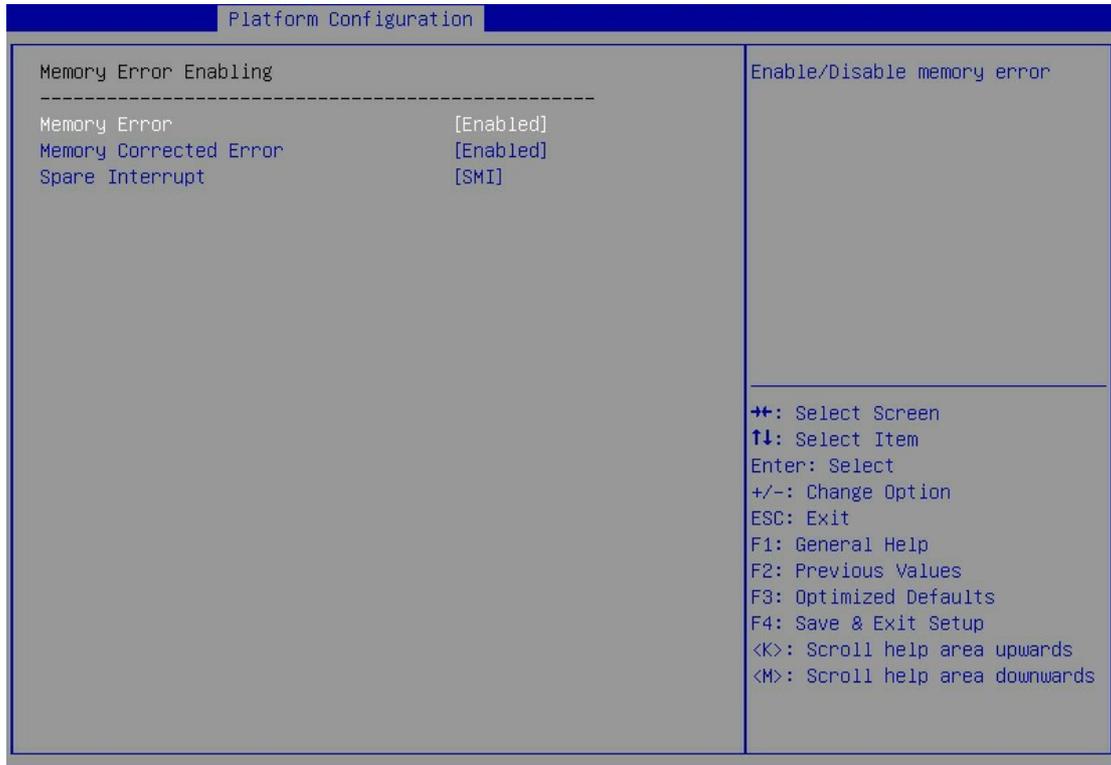


表3-44 Memory Error Enabling 界面参数

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，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>
Spare Interrupt	Spare Interrupt类型设置，Memory Corrected Error设置为Enabled时，该选项可用，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> </ul>

I/O Error Enabling界面如 [图 3-48](#) 所示。具体参数说明如 [表 3-45](#) 所示。

图3-48 IIO Error Enabling 界面

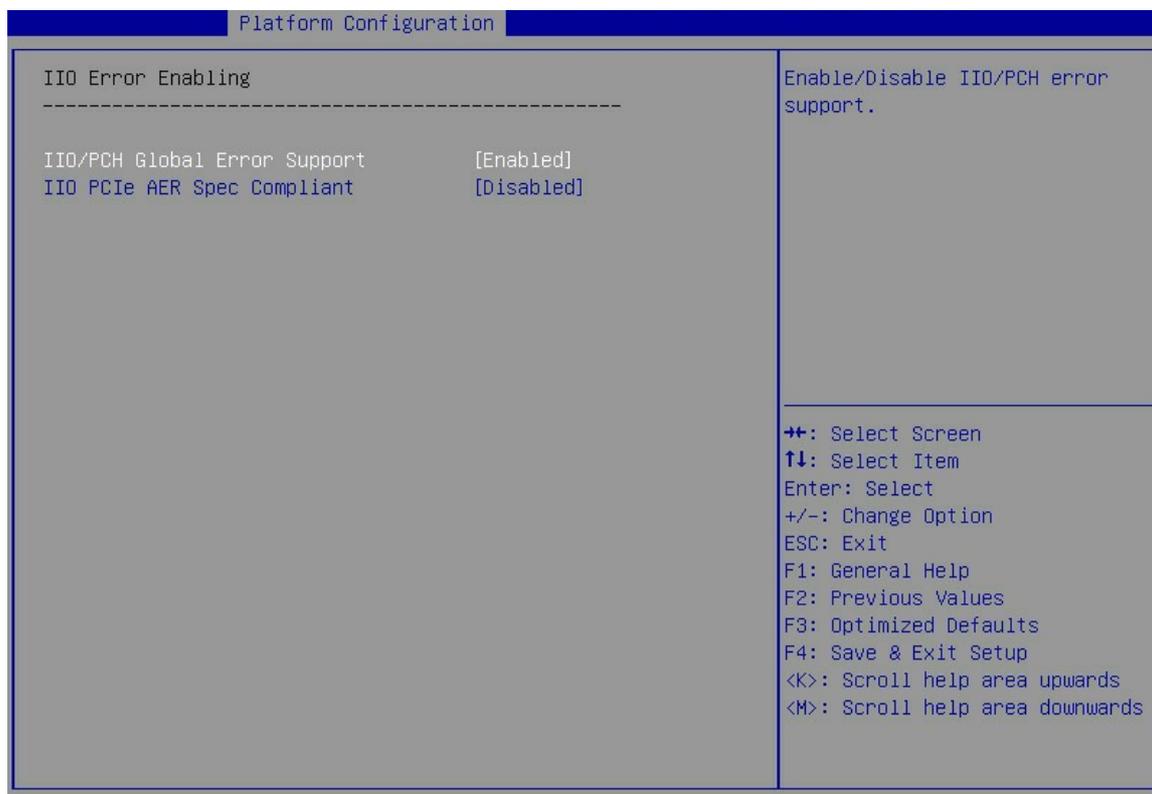


表3-45 IIO Error Enable 界面参数

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。</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。</li> <li>Disabled（缺省）：关闭 IIO PCIe AER Spec 合规功能。</li> </ul>

PCI Error Enabling界面如 [图 3-49](#) 所示。具体参数说明如 [表 3-46](#) 所示。

图3-49 PCI Error Enabling 界面

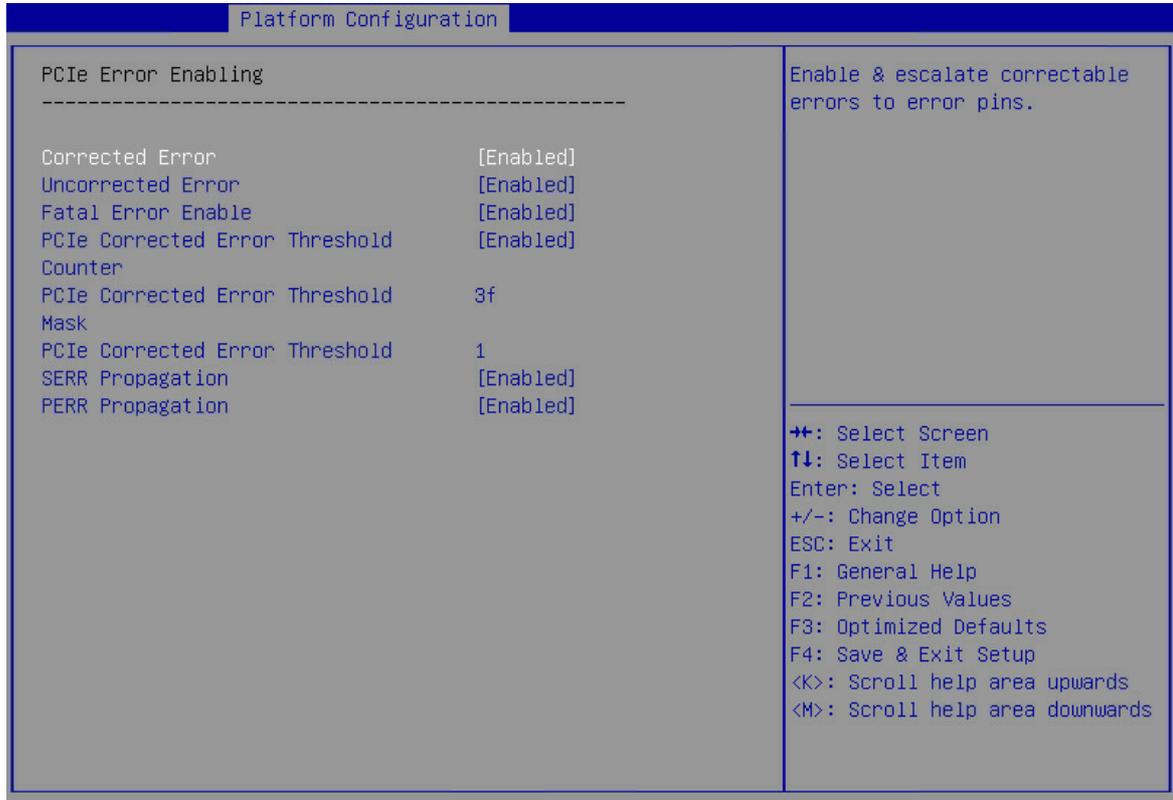


表3-46 PCI Error Enabling 界面参数

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 可修正错误功能。</li> <li>Disabled：关闭 PCIe 可修正错误功能。</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 不可修正错误功能。</li> <li>Disabled：关闭 PCIe 不可修正错误功能。</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。</li> <li>Disabled：关闭 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。</p> <ul style="list-style-type: none"> <li>Enabled：开启 PCIe 可修正错误阈值计数器功能。</li> <li>Disabled（缺省）：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。当PCIe Corrected Error Threshold Counter 选项设置为Enabled时显示。</p>
PCIe Corrected Error Threshold	<p>PCIe可修正错误阈值设置。当PCIe Corrected Error Threshold Counter 选项设置为Enabled时显示。</p>

界面参数	功能说明
SERR Propagation	SERR Propagation设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省): 开启 SERR Propagation 功能。</li> <li>Disabled: 关闭 SERR Propagation 功能。</li> </ul>
PERR Propagation	PERR Propagation设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled (缺省): 开启 PERR Propagation 功能。</li> <li>Disabled: 关闭 PERR Propagation 功能。</li> </ul>

### 3.4 Socket Configuration界面

介绍 Socket Configuration 界面包含的参数及相关功能。

Socket Configuration界面如 [图 3-50](#) 所示，主要包含CPU配置、通用RefCode配置、UPI配置、内存配置、高级电源管理配置等。具体参数说明如 [表 3-47](#) 所示

图3-50 Socket Configuration 界面



表3-47 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

界面参数	功能说明
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 3-51 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 3-48 所示。

图3-51 Processor Configuration 界面

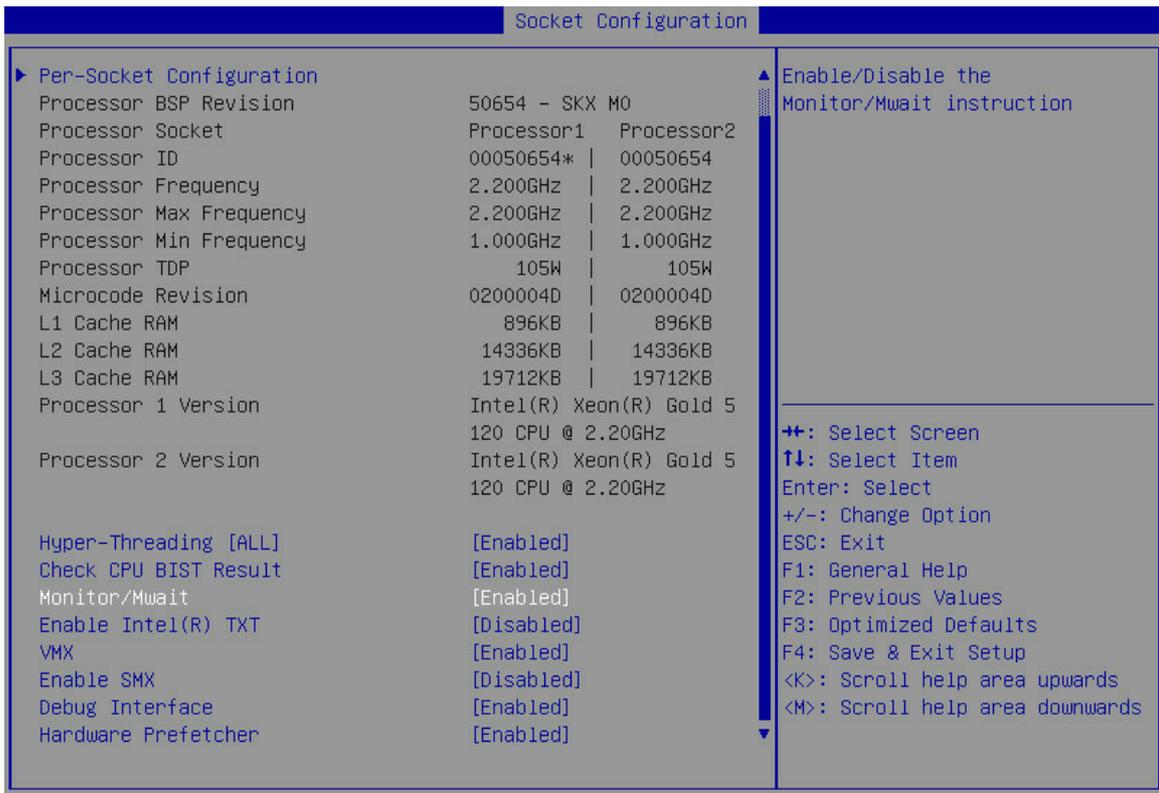


表3-48 Processor Configuration 界面参数

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

界面参数	功能说明
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 1 Version	显示CPU1版本信息
Processor 2 Version	显示CPU2版本信息
Hyper-Threading [ALL]	<p>超线程开关，超线程技术可以使CPU中的1颗内核如同2颗内核那样在操作系统中发挥作用，提高系统的整体性能。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>
Check CPU BIST Result	<p>检查CPU BIST结果配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：开启检查CPU BIST结果，关闭失败的BIST Core。</li> <li>• Disabled（缺省）：关闭检查CPU BIST结果，忽略BIST结果。</li> </ul>
Monitor/Mwait	<p>Monitor/Mwait指令开关，对于某些OS要同时关闭Monitor/Mwait和C state，才能完全关闭C State。</p> <ul style="list-style-type: none"> <li>• Enabled：开启Monitor/Mwait指令。</li> <li>• Disabled：关闭Monitor/Mwait指令。</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 Interface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
Debug Interface	<p>调试接口开关，Debug Interface设置为Enabled时，系统进入可调式状态。菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启调试接口功能。</li> <li>• Disabled：关闭调试接口功能。</li> </ul>
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>

Per-Socket Configuration界面如 [图 3-52](#) 所示。具体参数说明如 [表 3-49](#) 所示。

图3-52 Per-Socket Configuration 界面

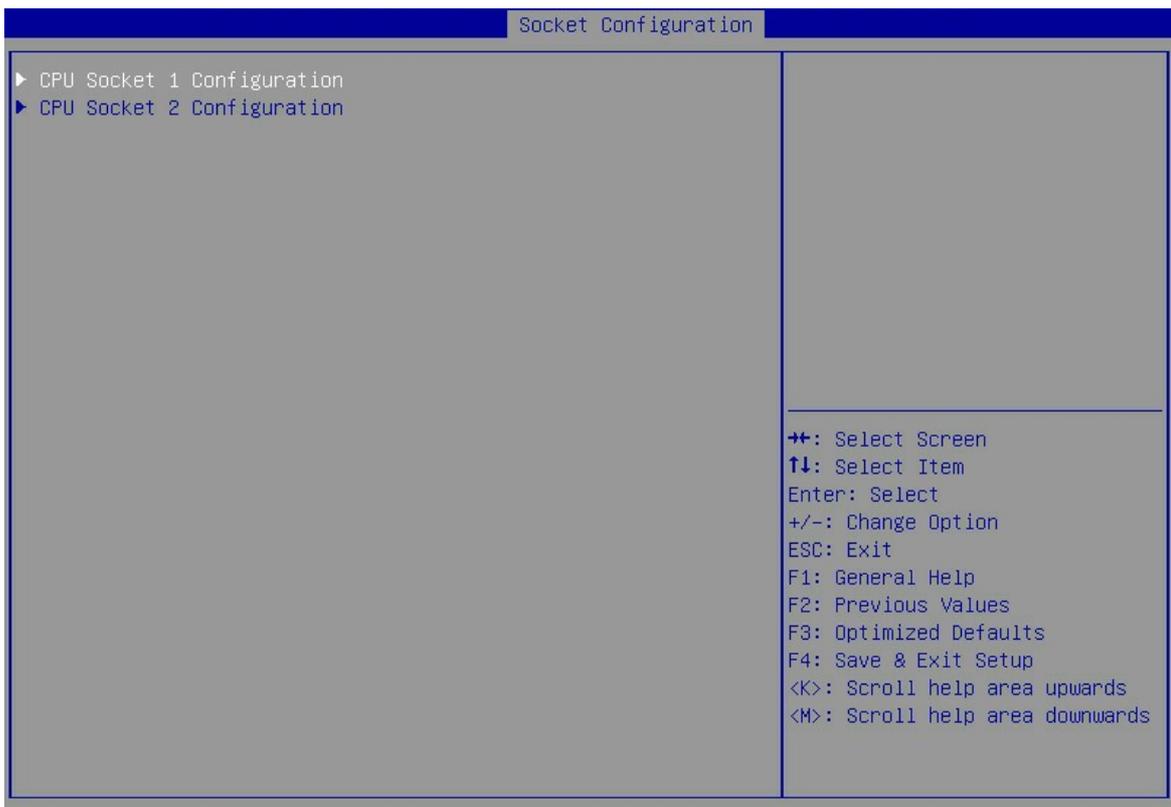


表3-49 Per-Socket Configuration 界面参数

界面参数	功能说明
CPU Socket 1 Configuration	CPU 1配置菜单
CPU Socket 2 Configuration	CPU 2配置菜单，CPU 2在位时显示该菜单，否则不显示。

CPU Socket 1 Configuration与CPU Socket 2 Configuration的界面参数相同，本文以CPU Socket 1 Configuration为例。CPU Socket 1 Configuration界面如 [图 3-53](#) 所示。具体参数说明如 [表 3-50](#) 所示。

图3-53 CPU Socket 1 Configuration 界面

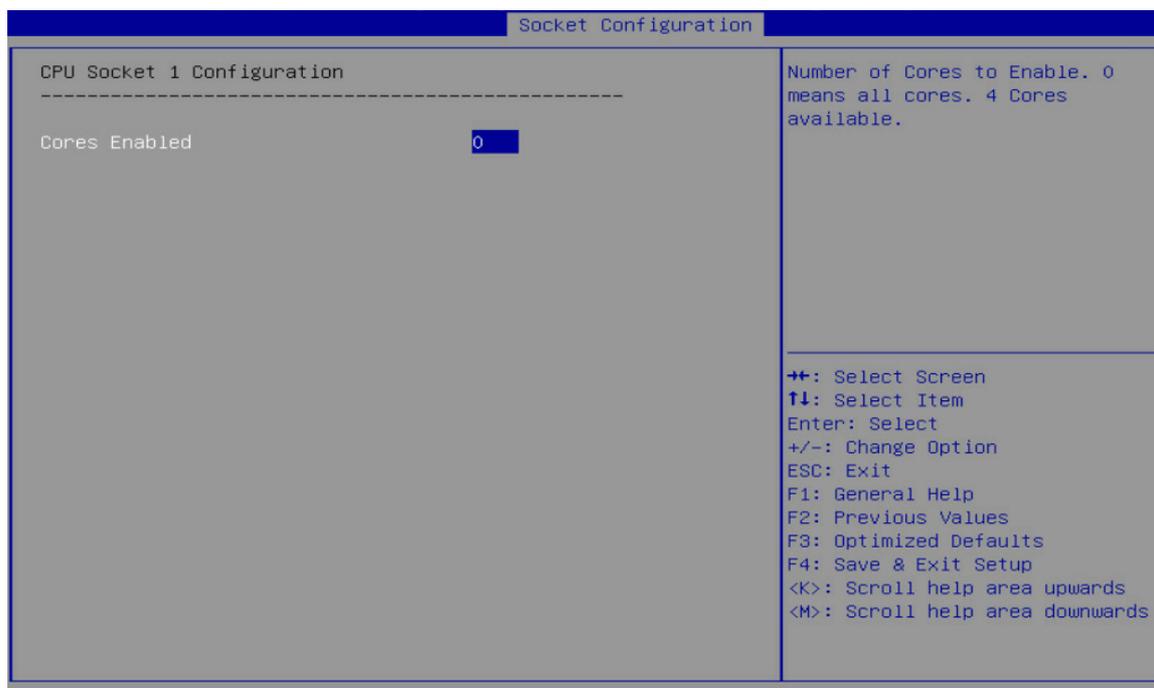


表3-50 CPU Socket 1 Configuration 界面参数

界面参数	功能说明
Cores Enabled	启用CPU的内核数配置，0表示启用所有内核。

### 3.4.2 Common RefCode Configuration界面

如 [图 3-54](#) 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 3-51](#) 所示。

图3-54 Common RefCode Configuration 界面

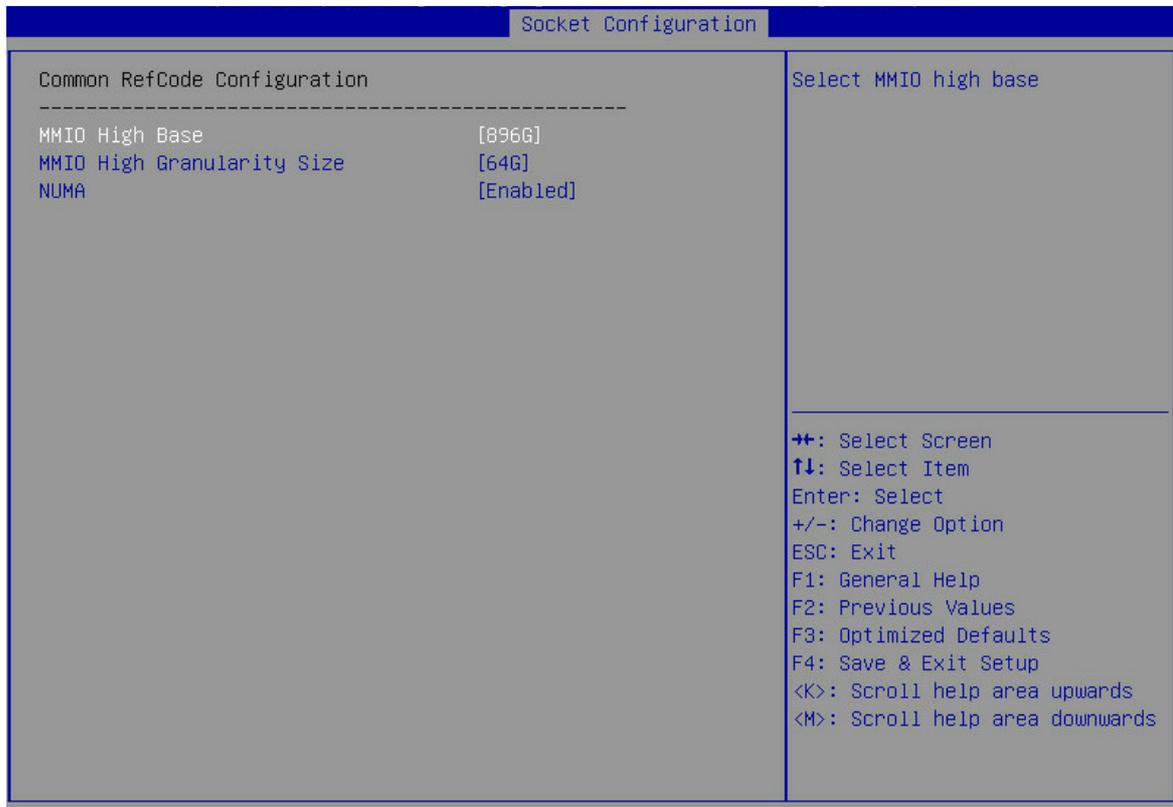


表3-51 Common RefCode Configuration 界面参数

界面参数	功能说明
MMIO High Base	4G以上MMIO基址配置，MMIO指内存映射I/O，菜单选项为： <ul style="list-style-type: none"> <li>• 56T</li> <li>• 40T</li> <li>• 24T</li> <li>• 16T</li> <li>• 4T</li> <li>• 1T</li> <li>• 896G（缺省）</li> </ul>
MMIO High Granularity Size	4G以上MMIO高位地址大小配置，MMIO指内存映射I/O，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>• 512G</li> <li>• 1024G</li> </ul>

界面参数	功能说明
NUMA	<p>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：</p> <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 3-55](#) 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 3-52](#) 所示。

图3-55 UPI Configuration 界面

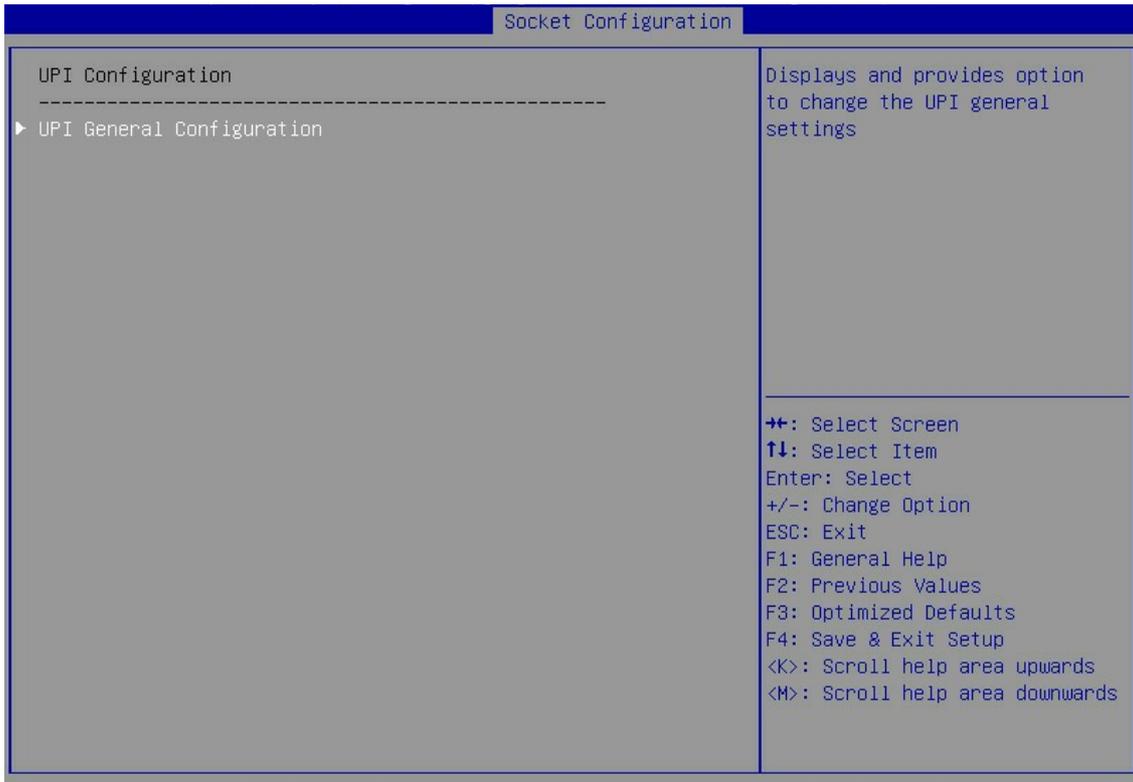


表3-52 UPI Configuration 界面参数

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

UPI General Configuration界面如 [图 3-56](#) 所示。具体参数说明如 [表 3-53](#) 所示。

图3-56 UPI General Configuration 界面

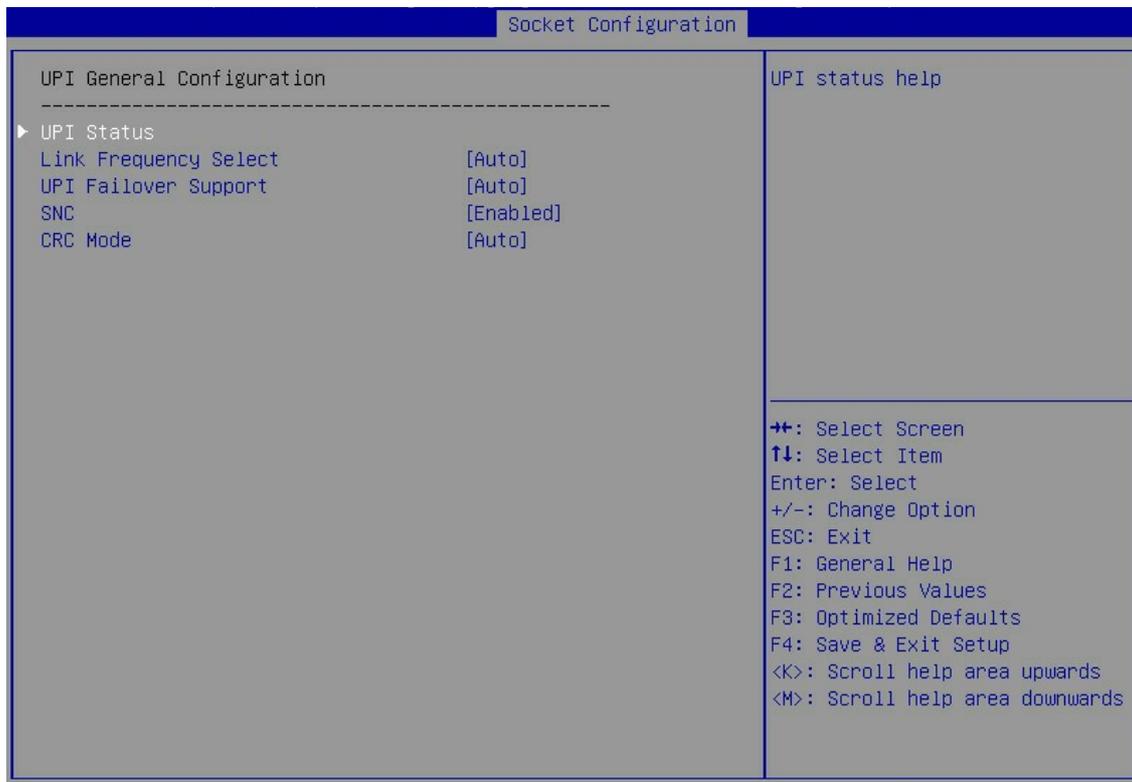


表3-53 UPI General Configuration 界面参数

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>
UPI Failover Support	UPI故障切换支持配置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启 UPI 故障切换支持。</li> <li>• Disabled：关闭 UPI 故障切换支持。</li> <li>• Auto（缺省）：自动选择 UPI 故障切换是否支持。</li> </ul>
SNC	SNC功能配置，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>
CRC Mode	UPI CRC 校验模式配置，菜单选项为： <ul style="list-style-type: none"> <li>• 16 Bit CRC：使用 16 位 CRC。</li> <li>• 32 Bit Rolling CRC：使用 32 位滚动 CRC。</li> <li>• Auto（缺省）：自动选择 CRC 校验模式。</li> </ul>

UPI Status界面如 [图 3-57](#) 所示。具体参数说明如 [表 3-54](#) 所示。

图3-57 UPI Status 界面

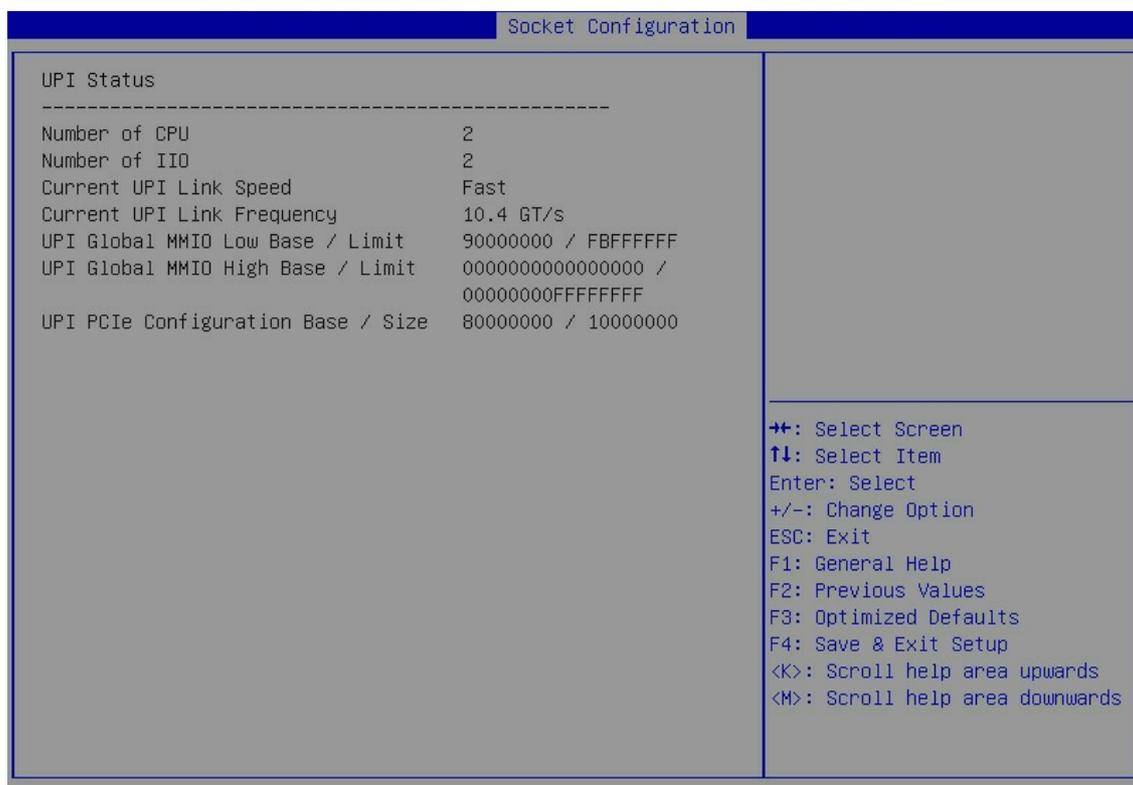


表3-54 UPI Status 界面参数

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
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 3-58](#) 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 3-55](#) 所示。

图3-58 Memory Configuration 界面

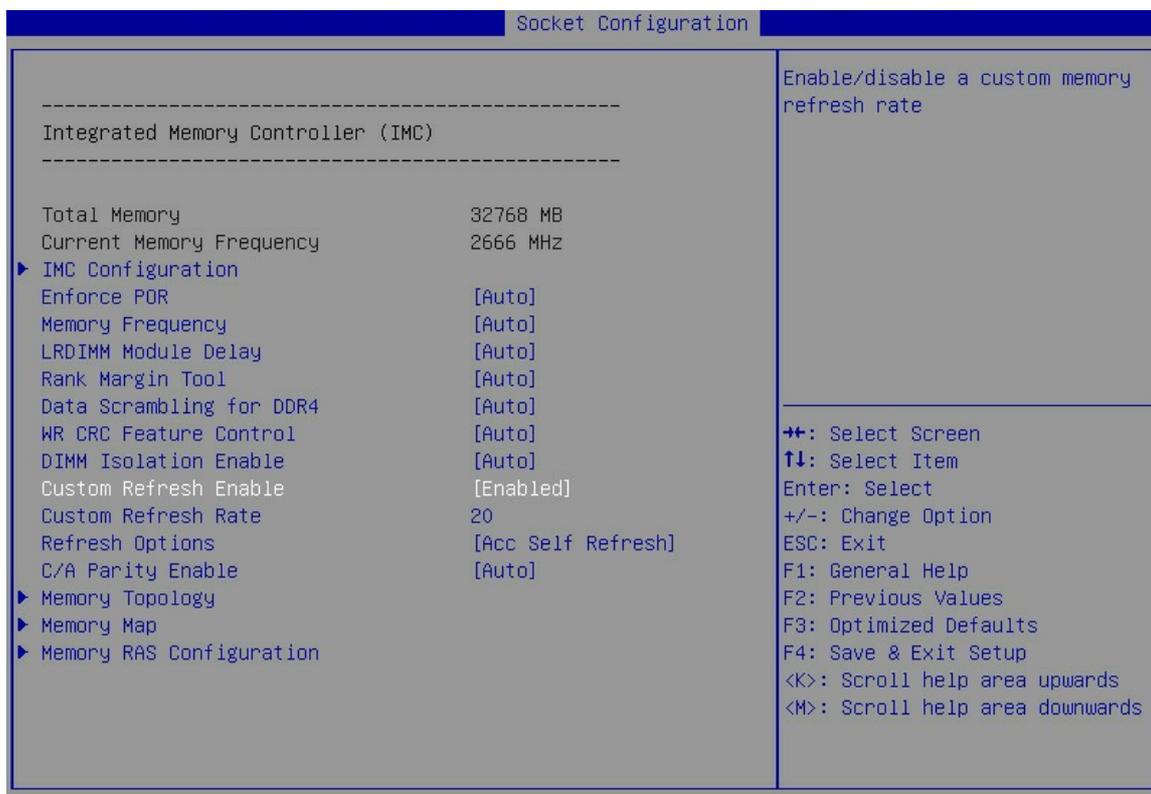


表3-55 Memory Configuration 界面参数

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
IMC Configuration	IMC配置菜单
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>• Enforce POR：开启 POR，可以提升内存的稳定性。</li> <li>• Disabled：关闭 POR。</li> </ul>
Memory Frequency	<p>内存频率设置，菜单选项为：</p> <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> </ul>

界面参数	功能说明
LRDIMM Module Delay	LRDIMM模块延迟设置，菜单选项为： <ul style="list-style-type: none"> <li>• Disabled: 关闭 LRDIMM 模块延迟功能，MRC 不使用 SPD 的 90 到 95 字节作为 LRDIMM 模块的延迟。</li> <li>• Auto (缺省): 自动选择，如果 SPD 是 0 或者超出范围，MRC 将使用 LRDIMM 的默认值。</li> </ul>
Rank Margin Tool	Rank Margin工具，菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 自动选择为 MRC 默认设置。</li> <li>• Disabled: 启用 Rank Margin 工具，将会在 DDR4 内存 training 之后使用。</li> <li>• Enabled: 禁用 Rank Margin 工具。</li> </ul>
Data Scrambling	数据扰频设置，开启该功能后，可提高对DDR地址线错误的侦测能力，菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 自动选择。</li> <li>• Disabled: 关闭数据扰频功能。</li> <li>• Enabled: 开启数据扰频功能。</li> </ul>
WR CRC Feature Control	写CRC功能控制，菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 设置为 MRC 默认设置，如果用户选择启用，选项会显示为自动。</li> <li>• Disabled: 禁用写 CRC。</li> <li>• Enabled: 启用写 CRC。</li> </ul>
DIMM Isolation Enable	DIMM隔离控制，菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 设置为 MRC 默认设置，如果用户选择启用，选项会显示为自动。</li> <li>• Disabled: 为命令/地址校验和写 CRC 禁用 DIMM 隔离。</li> <li>• Enabled: 为命令/地址校验和写 CRC 启用 DIMM 隔离。</li> </ul>
Custom Refresh Enable	自定义内存刷新使能控制，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled: 启用自定义的内存刷新速率。</li> <li>• Disabled: 禁用自定义的内存刷新速率。</li> </ul>
Custom Refresh Rate	自定义内存刷新速率，可以手动输入数字；该选项在Custom Refresh Enable设置为Enabled的时候才显示
Refresh Options	刷新选项，菜单选项为： <ul style="list-style-type: none"> <li>• Acc Self Refresh: 加速自刷新。</li> <li>• 2x Refresh: 2x 刷新。</li> </ul>
C/A Parity Enable	C/A校验启用选项，菜单选项为： <ul style="list-style-type: none"> <li>• Auto (缺省): 保持 MRC 默认设置，如果用户选择启用，选项会显示为自动。</li> <li>• Disabled: 禁用 DDR4 命令地址校验。</li> <li>• Enabled: 启用 DDR4 命令地址校验功能。</li> </ul>
Memory Topology	内存拓扑信息菜单

界面参数	功能说明
Memory Map	内存映射配置菜单
Memory RAS Configuration	内存RAS配置菜单

IMC Configuration界面如 [图 3-59](#) 所示。具体参数说明如 [表 3-56](#) 所示。

图3-59 IMC Configuration 界面

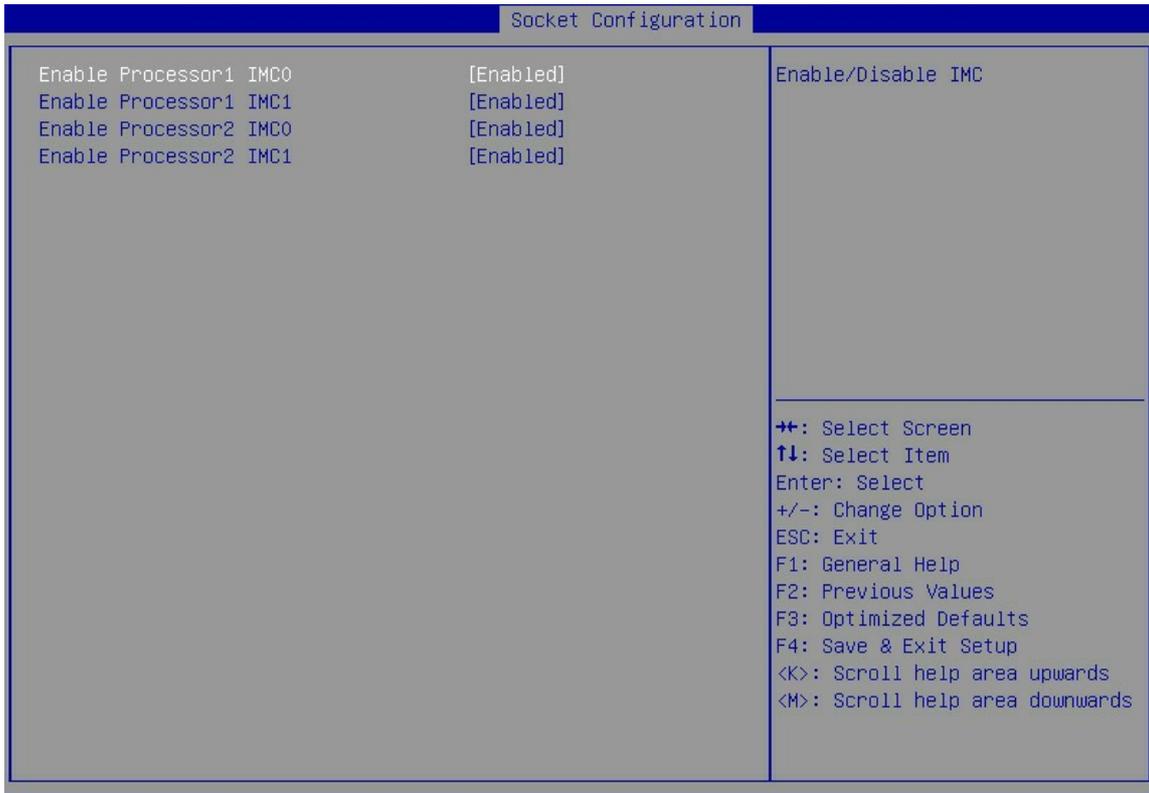


表3-56 IMC Configuration 界面参数

界面参数	功能说明
Enable Processor <i>Number</i> IMC	<p>处理器内存控制器配置菜单，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled: 禁用相对应的 CPU 内存控制器对应的内存控制器。</li> <li>• Enabled (缺省)：启用相对应的 CPU 内存控制器对应的内存控制器。</li> </ul>

Memory Topology界面如 [图 3-60](#) 所示。具体参数说明如 [表 3-57](#) 所示。

图3-60 Memory Topology 界面

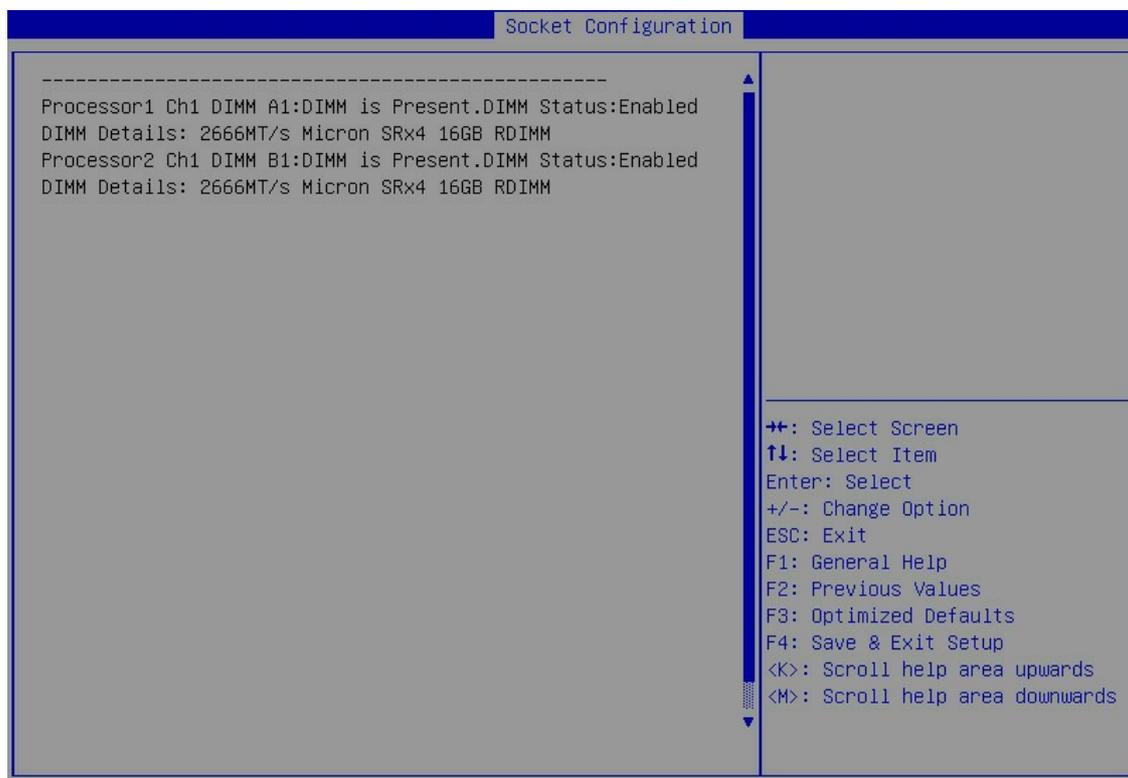


表3-57 Memory Topology 界面参数

界面参数	功能说明
Processor 1 Ch1 DIMM A1: DIMM is Present. DIMM Status: Enabled. DIMM Details: 2666MT/s Micron SRx4 16GB RDIMM	表示Processor 1通道1 DIMM A1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，16GB表示内存容量，SRx4中SR是RANK数量，x4是内存颗粒的位宽，RDIMM表示内存类型。

Memory Map界面如 [图 3-61](#) 所示。具体参数说明如 [表 3-58](#) 所示。

图3-61 Memory Map 界面

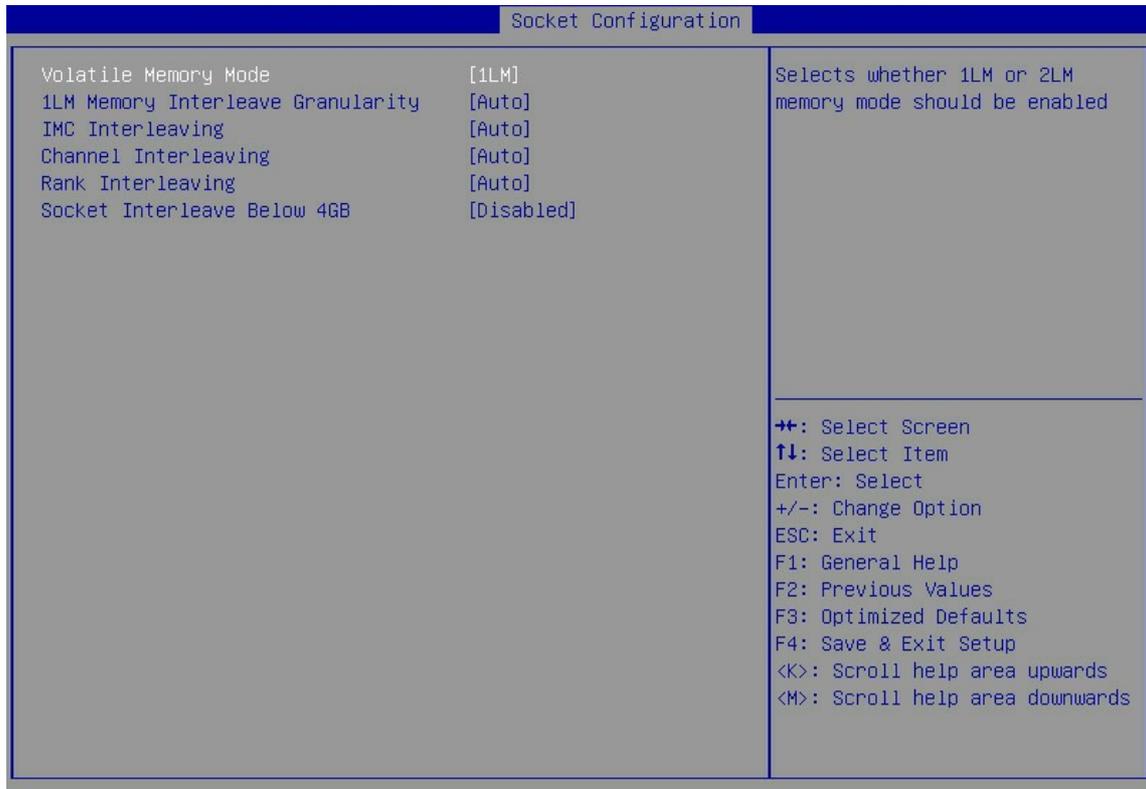


表3-58 Memory Map 界面参数

界面参数	功能说明
Volatile Memory Mode	易失性内存模式配置选项，菜单选项为： <ul style="list-style-type: none"> <li>• 1LM（缺省）：启用 1LM 模式。</li> <li>• 2LM：启用 2LM 模式。</li> <li>• Auto：自动设置易失性内存配置模式。</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。</li> </ul>
IMC Interleaving	IMC交织设置，用于提升内存的读写性能，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>
Channel Interleaving	Channel交织设置，用于提升内存的读写性能，菜单选项为： <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>

界面参数	功能说明
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，如果打开了NUMA开关（具体请参见<a href="#">3.4.2 Common RefCode Configuration界面</a>），则该功能会处于关闭状态，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>

Memory RAS Configuration界面如 [图 3-62](#) 所示。具体参数说明如 [表 3-59](#) 所示。

图3-62 Memory RAS Configuration 界面

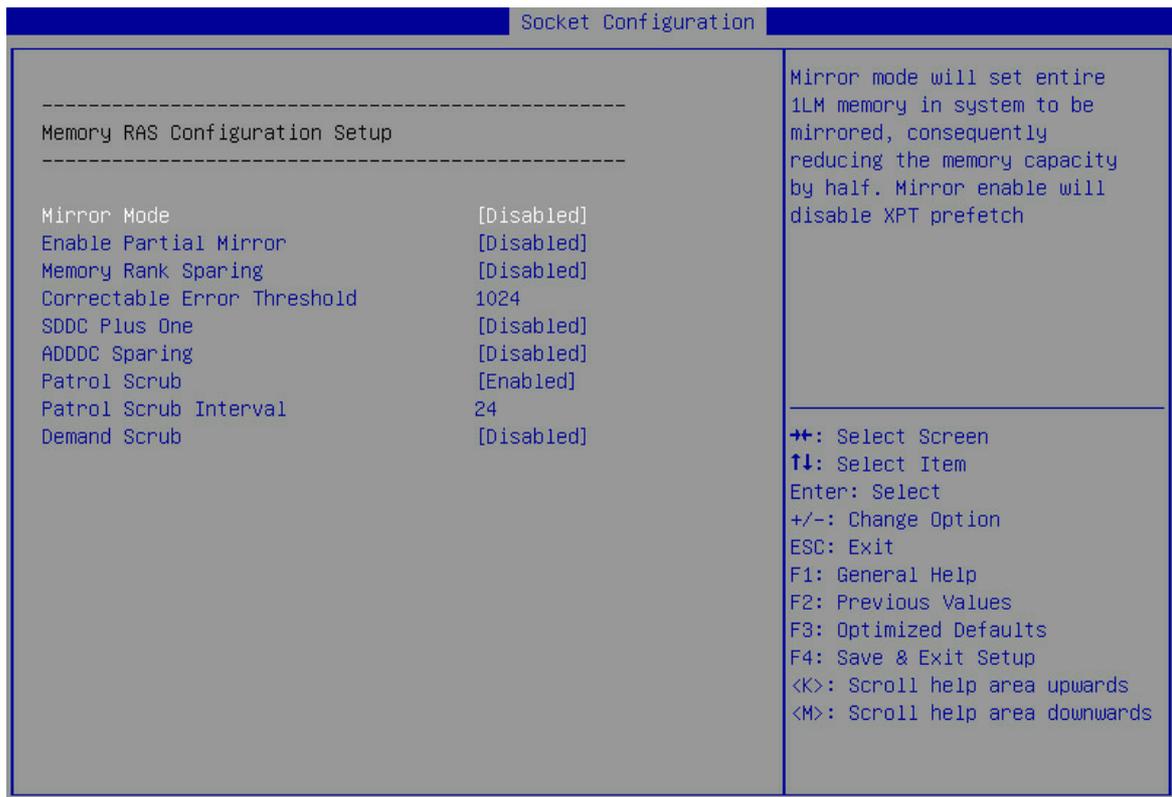


表3-59 Memory RAS Configuration 界面参数

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>• Mirror Mode 1LM：使用 1LMirror Mode。</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>
Enable Partial Mirror	<p>启用Partial Mirror设置，Partial Mirror将启用需要的内存大小被镜像,若Memory Rank Sparing被启用，Partial Mirror将不起作用，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Disabled（缺省）：禁用部分镜像模式。</li> <li>• Mirror Mode 1LM：使用部分镜像模式 1LM。</li> </ul>
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：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1~32767，缺省值为4096，0表示没有阈值。</p>
SDDC Plus One	<p>单设备数据校正加一设置（Single-Device Data Correction Plus One），该功能可以纠正单颗粒的数据错误后再纠正1bit数据错误，菜单选项为</p> <ul style="list-style-type: none"> <li>• Enabled：启用 SDDC 加一功能。</li> <li>• Disabled（缺省）：禁用 SDDC 加一功能。</li> </ul>
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>

界面参数	功能说明
Patrol Scrub	Patrol Scrub设置, CPU主动对内存的数据进行检测并纠正可纠正的内存错误, 菜单选项为: <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	显示Patrol Scrub间隔, 缺省值为24。当Patrol Scrub选项设置为Enabled后该选项才会显示, 用户可以修改该间隔。
Demand Scrub	Demand Scrub设置, 当CPU对内存进行读操作时, 才对内存的数据进行检测, 菜单选项为: <ul style="list-style-type: none"> <li>Enabled: 开启 Demand Scrub 功能。</li> <li>Disabled (缺省): 关闭 Demand Scrub 功能。</li> </ul>

### 3.4.5 IIO Configuration界面

如 [图 3-63](#) 所示, 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。具体参数说明如 [表 3-60](#) 所示。

图3-63 IIO Configuration 界面

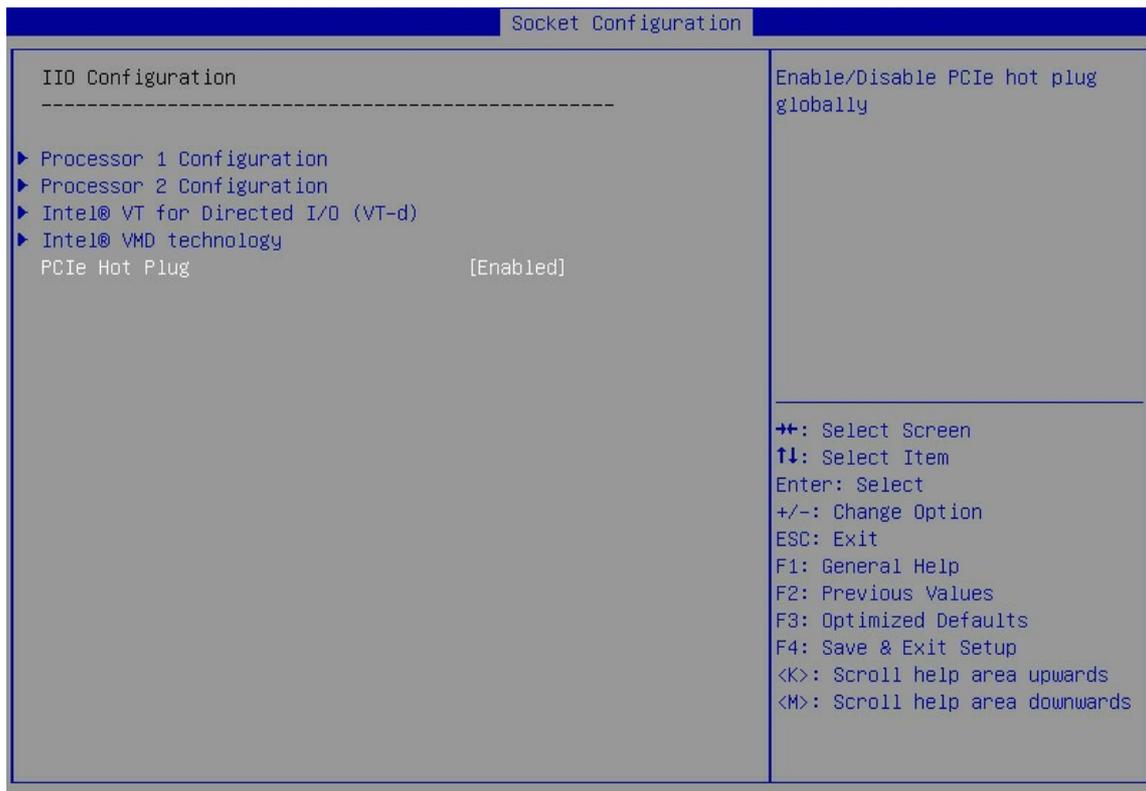


表3-60 IIO Configuration 界面参数

界面参数	功能说明
Processor 1 Configuration	处理器1的IIO配置菜单，该配置界面内的相关配置选项会根据R4900\4700\2900\2700机型变化而变化，详情后续会进行说明
Processor 2 Configuration	处理器2的IIO配置菜单，该配置界面内的相关配置选项会根据R4900\4700\2900\2700机型变化而变化，详情后续会进行说明
Intel VMD technology	英特尔®VMD卷管理设备配置菜单
PCIe Hot Plug	PCIe热插拔配置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：开启 PCIe 热插拔功能。</li> <li>• Disabled：关闭 PCIe 热插拔功能。</li> </ul>

 说明

Processor 1 Configuration 和 Processor 2 Configuration 的界面相关选项配置内容会根据机型的不同而产生不同的差异，另外也会根据 riser 插槽上安装的设备类型有所变化，鉴于 PCIE 插槽的设备较多，不对其做一一的遍历说明，本文仅对机型的不同产生的该界面的不同配置内容作出说明，即对 R4900、R4700、R2900、R2700 的 Processor 1 Configuration 和 Processor 2 Configuration 的界面进行分别说明。

Processor 1 Configuration 界面如 [图 3-64](#)、[图 3-65](#)、[图 3-66](#) 和 [图 3-67](#) 所示。具体参数说明如 [表 3-61](#) 所示。

图3-64 Processor 1 Configuration 界面（H3C UniServer R4900 G3）

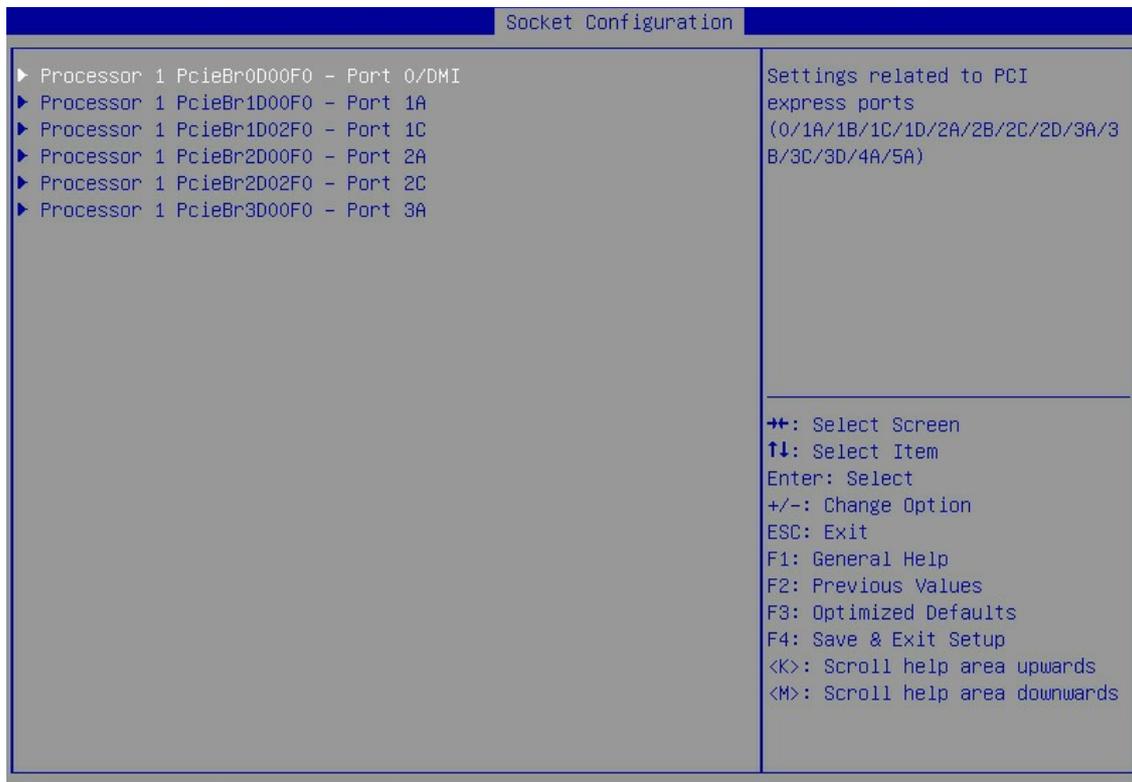


图3-65 Processor 1 Configuration 界面（H3C UniServer R4700 G3）

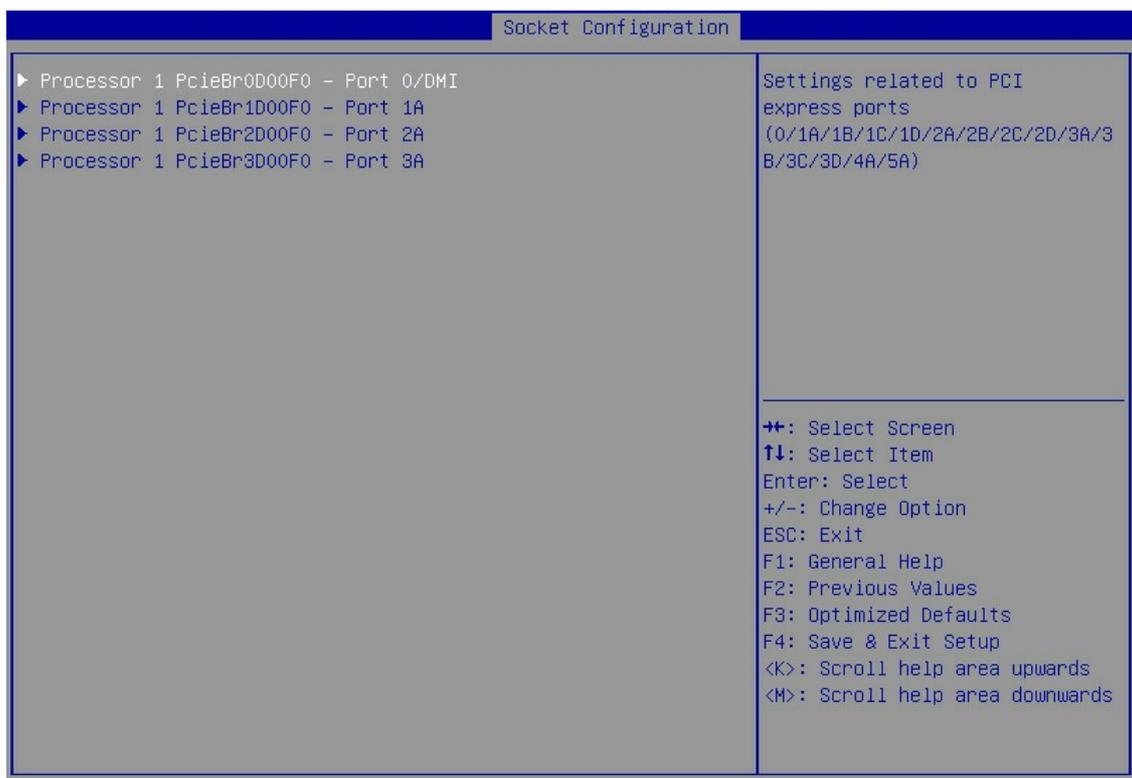


图3-66 Processor 1 Configuration 界面（H3C UniServer R2900 G3）

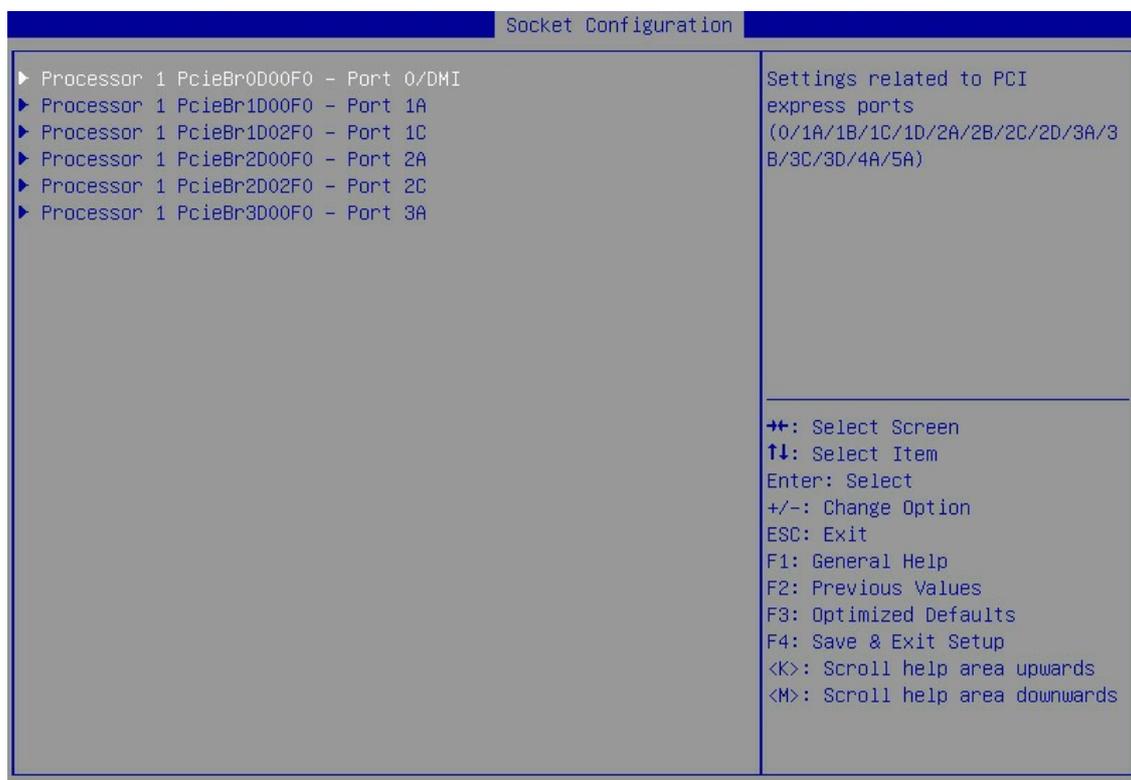


图3-67 Processor 1 Configuration 界面（H3C UniServer R2700 G3）

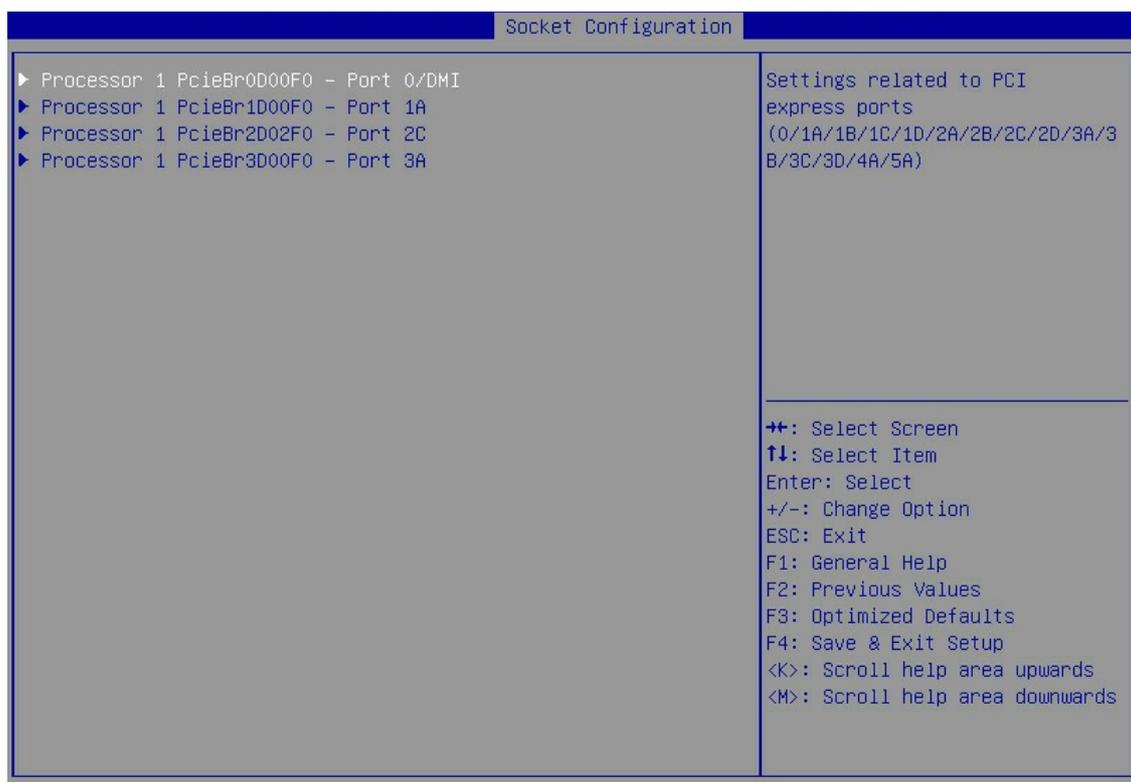


表3-61 Processor 1 Configuration 界面参数(本参数以 R4900 G3 为例)

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 PcieBr1D02F0 - Port 1C	Processor 1 PcieBr1D02F0 - Port 1C配置菜单
Processor 1 PcieBr2D00F0 - Port 2A	Processor 1 PcieBr2D00F0 - Port 2A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

Processor 1 PcieBr0D00F0 - Port 0/DMI界面如 [图 3-68](#) 所示。具体参数说明如 [表 3-62](#) 所示。

图3-68 Processor 1 PcieBr0D00F0 - Port 0/DMI 界面

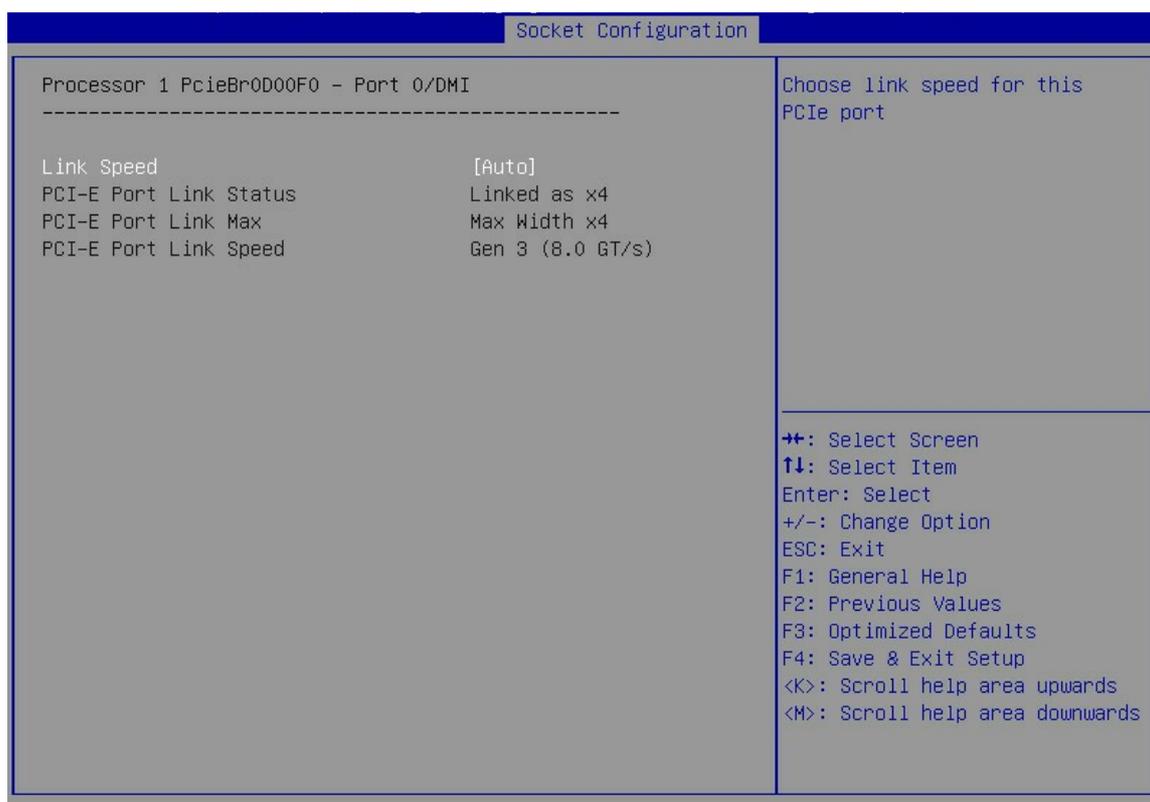


表3-62 Processor 1 PcieBr0D00F0 - Port 0/DMI 界面参数

界面参数	功能说明
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（5.0 GT/s）</li> <li>• Gen 3（8.0 GT/s）</li> </ul>

界面参数	功能说明
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。

 说明

Processor 1 PcieBr1D02F0 - Port 1C、 Processor 1 PcieBr2D00F0 – Port12A、 Processor 1 PcieBr2D02F0 - Port 2C、 Processor 1 PcieBr3D00F0 - Port 3A 与 Processor 1 PcieBr1D00F0 - Port 1A 的界面参数相同，本文以 Processor 1 PcieBr1D00F0 - Port 1A 为例。

Processor 1 PcieBr1D00F0 - Port 1A界面如 [图 3-69](#)所示。具体参数说明如 [表 3-63](#)所示。

图3-69 Processor 1 PcieBr1D00F0 - Port 1A 界面

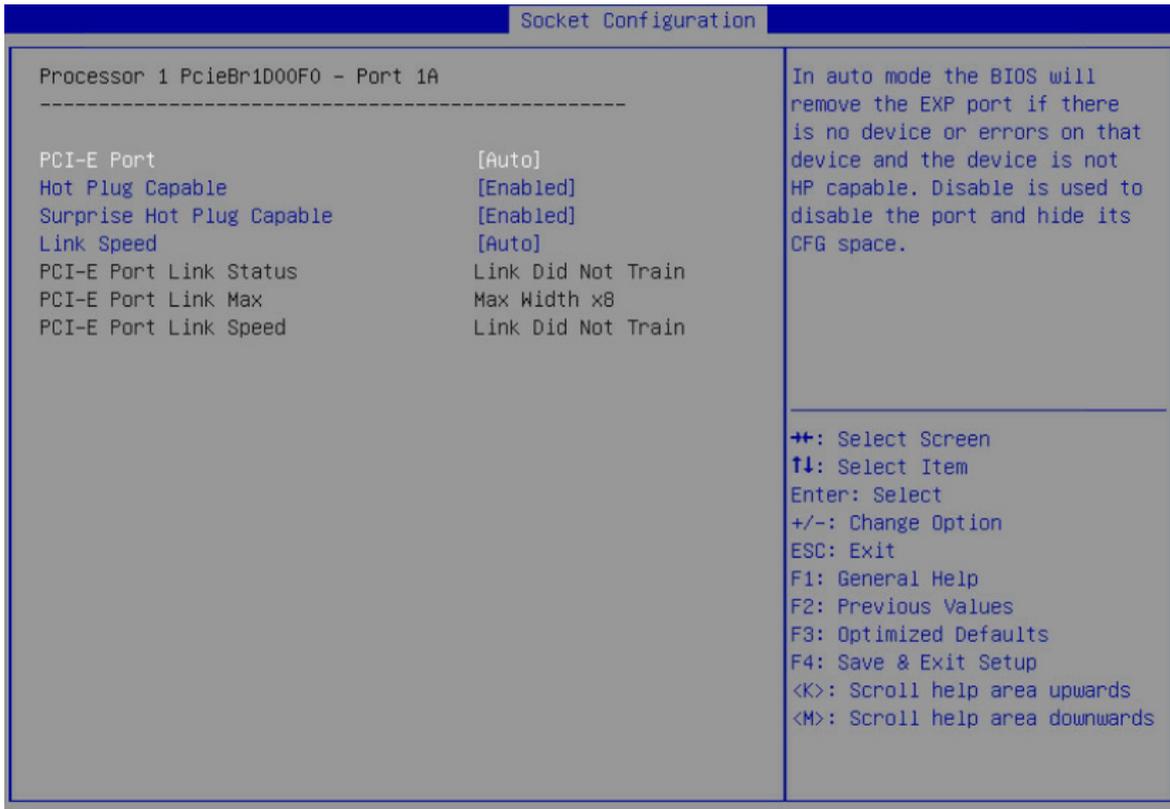


表3-63 Processor 1 PcieBr1D00F0 - Port 1A 界面参数

界面参数	功能说明
PCI-E Port	PCI-E端口开关，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>
Hot Plug Capable	热插拔能力配置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启该 PCIe 端口的热插拔能力。</li> <li>• Disabled：关闭该 PCIe 端口的热插拔能力。</li> </ul>
Surprise Hot Plug Capable	意外热插拔能力配置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启该 PCIe 端口的意外热插拔能力。</li> <li>• Disabled：关闭该 PCIe 端口的意外热插拔能力。</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。

Processor 2 Configuration界面如 [图 3-70](#)、[图 3-71](#)、[图 3-72](#) 和 [图 3-73](#) 所示。具体参数说明如 [表 3-64](#) 所示。

图3-70 Processor 2 Configuration 界面 (H3C UniServer R4900 G3)

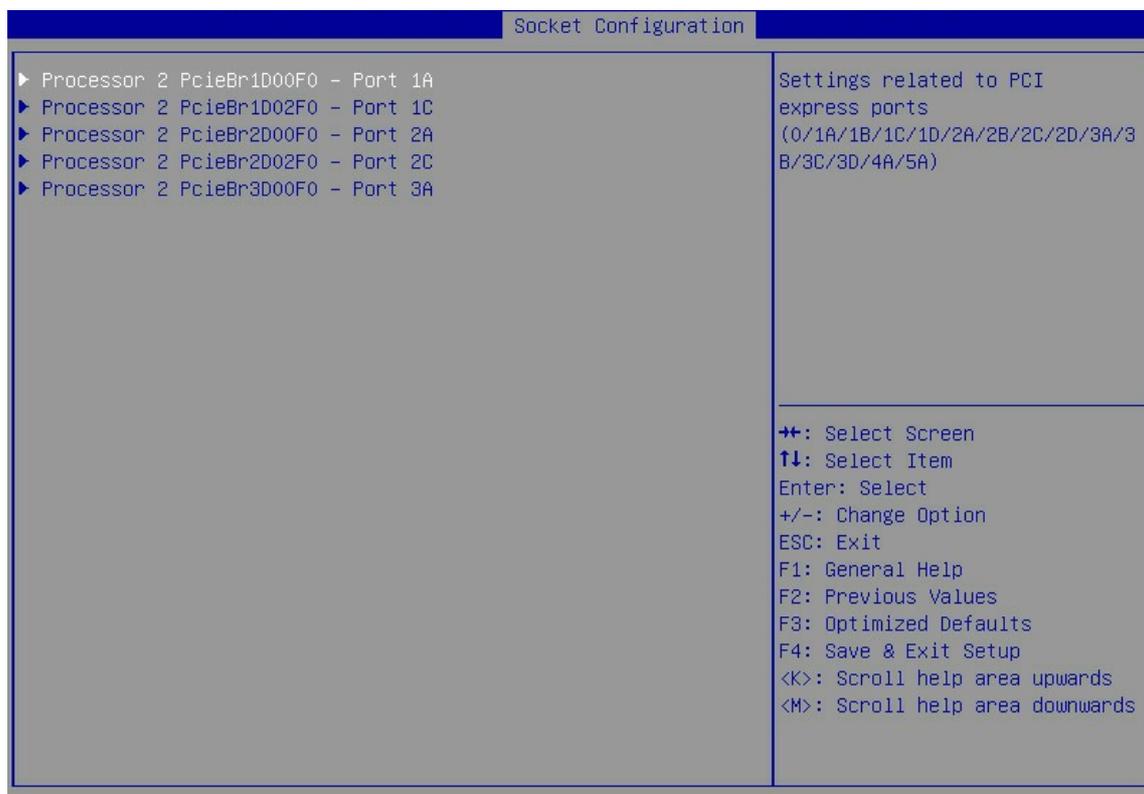


图3-71 Processor 2 Configuration 界面 (H3C UniServer R4700 G3)

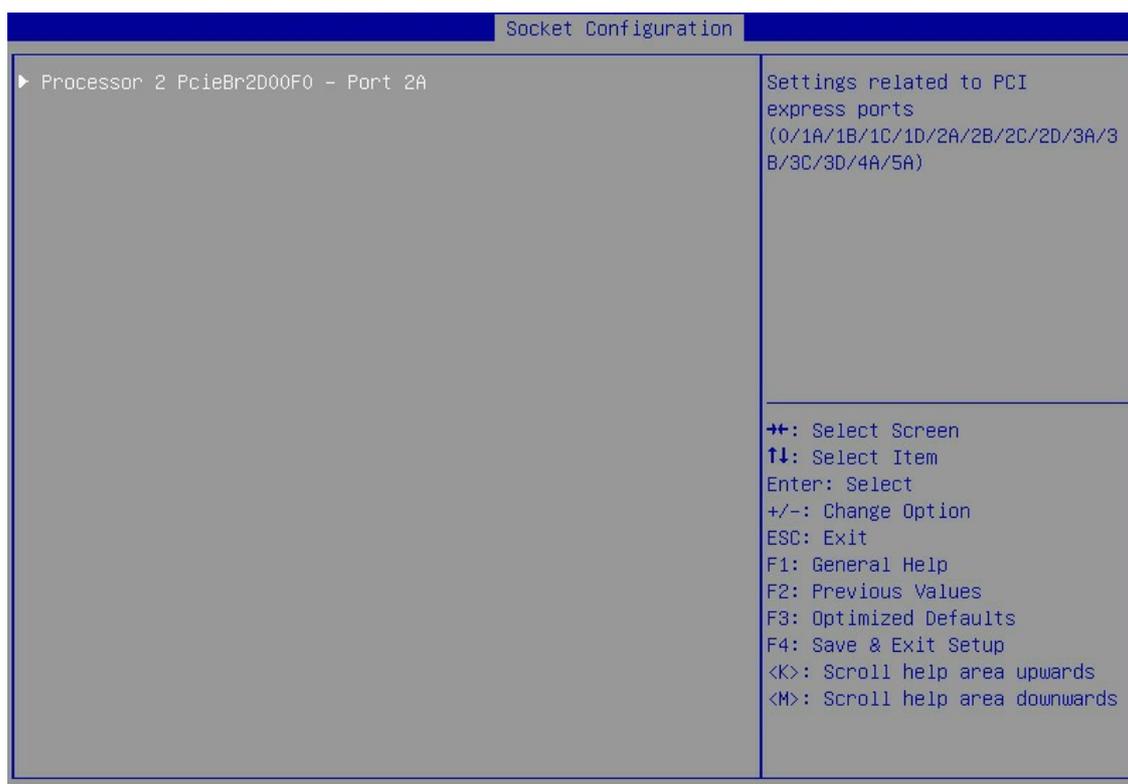


图3-72 Processor 2 Configuration 界面（H3C UniServer R2900 G3）

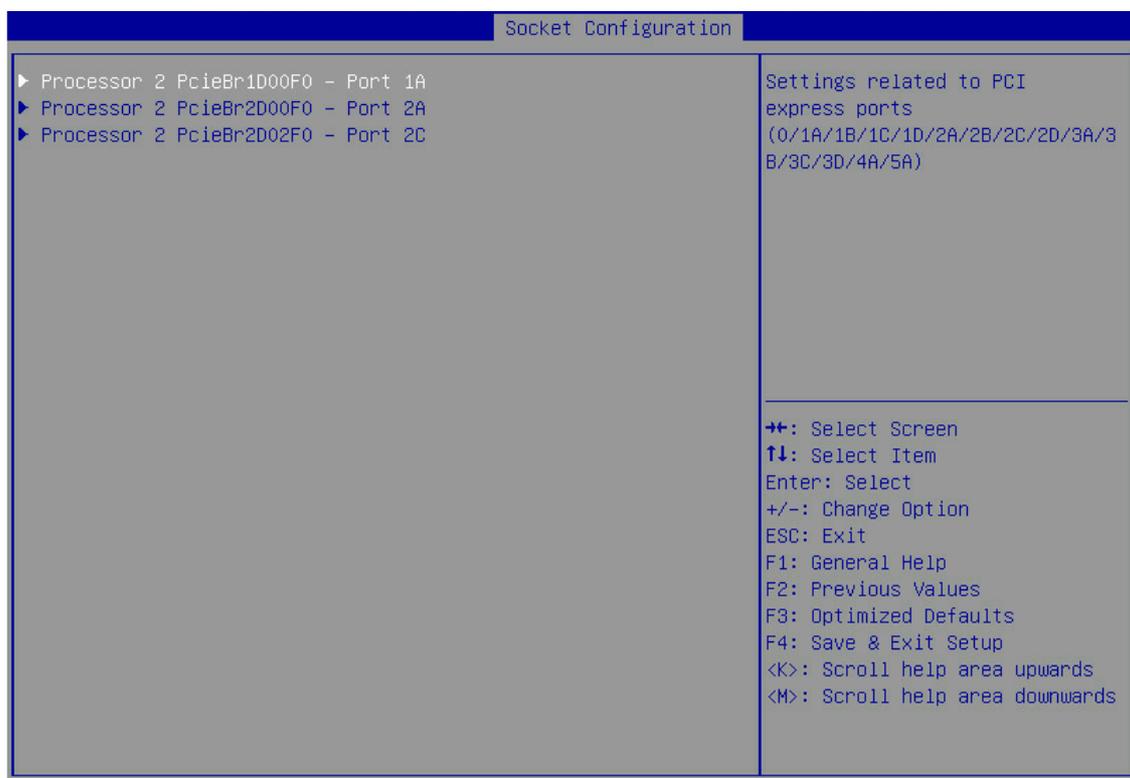


图3-73 Processor 2 Configuration 界面（H3C UniServer R2700 G3）

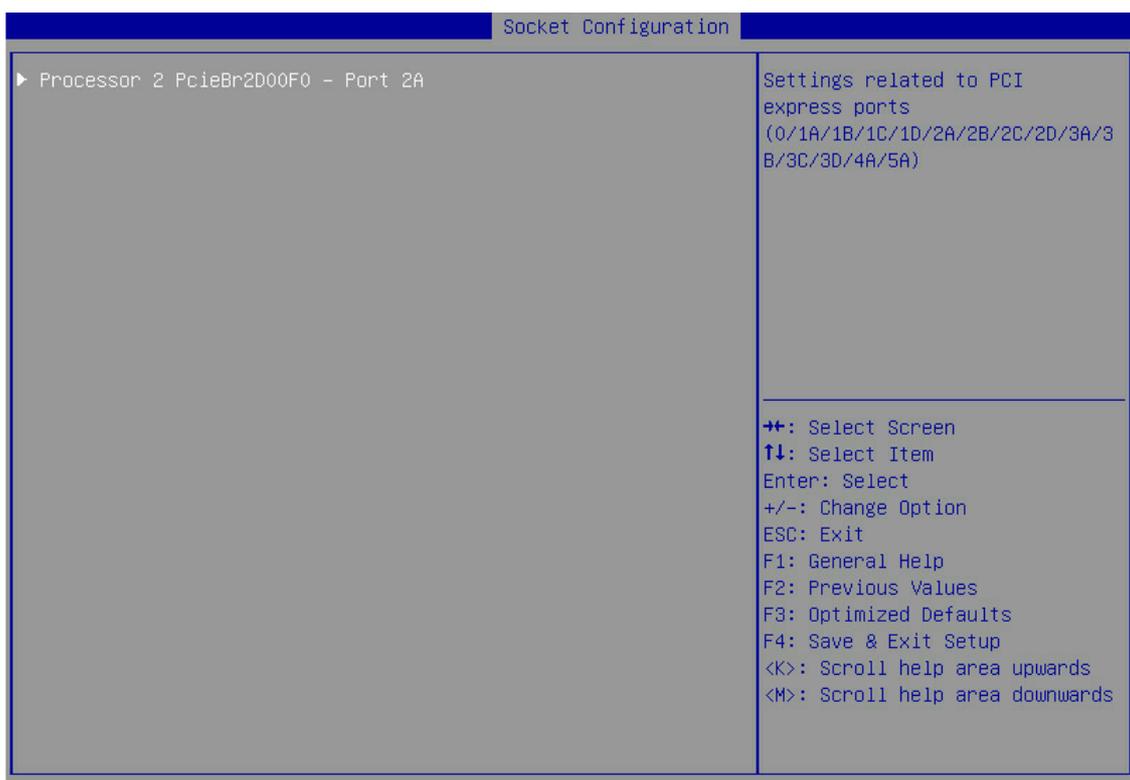


表3-64 Processor 2 Configuration 界面参数(本参数以 R4900 G3 为例，其他机型与其相同)

界面参数	功能说明
Processor 2 PcieBr1D00F0 - Port 1A	Processor 2 PcieBr1D00F0 - Port 1A配置菜单。
Processor 2 PcieBr1D02F0 - Port 1C	Processor 2 PcieBr1D02F0 - Port 1C配置菜单。
Processor 2 PcieBr2D00F0 - Port 2A	Processor 2 PcieBr2D00F0 - Port 2A配置菜单。
Processor 2 PcieBr2D02F0 - Port 2C	Processor 2 PcieBr2D02F0 - Port 2C配置菜单。
Processor 2 PcieBr3D00F0 - Port 3A	Processor 2 PcieBr3D00F0 - Port 3A配置菜单。



说明

Processor 2 PcieBr1D02F0 - Port 1C、Processor 2 PcieBr2D00F0 - Port 2A、Processor 2 PcieBr2D02F0 - Port 2C、Processor 2 PcieBr3D00F0 - Port 3A 与 Processor 2 PcieBr1D00F0 - Port 1A 的界面参数相同，本文以 Processor 2 PcieBr1D00F0 - Port 1A 为例。

Processor 2 PcieBr1D00F0 - Port 1A界面如 [图 3-74](#) 所示。具体参数说明如 [表 3-65](#) 所示。

图3-74 Processor 2 PcieBr1D00F0 - Port 1A 界面

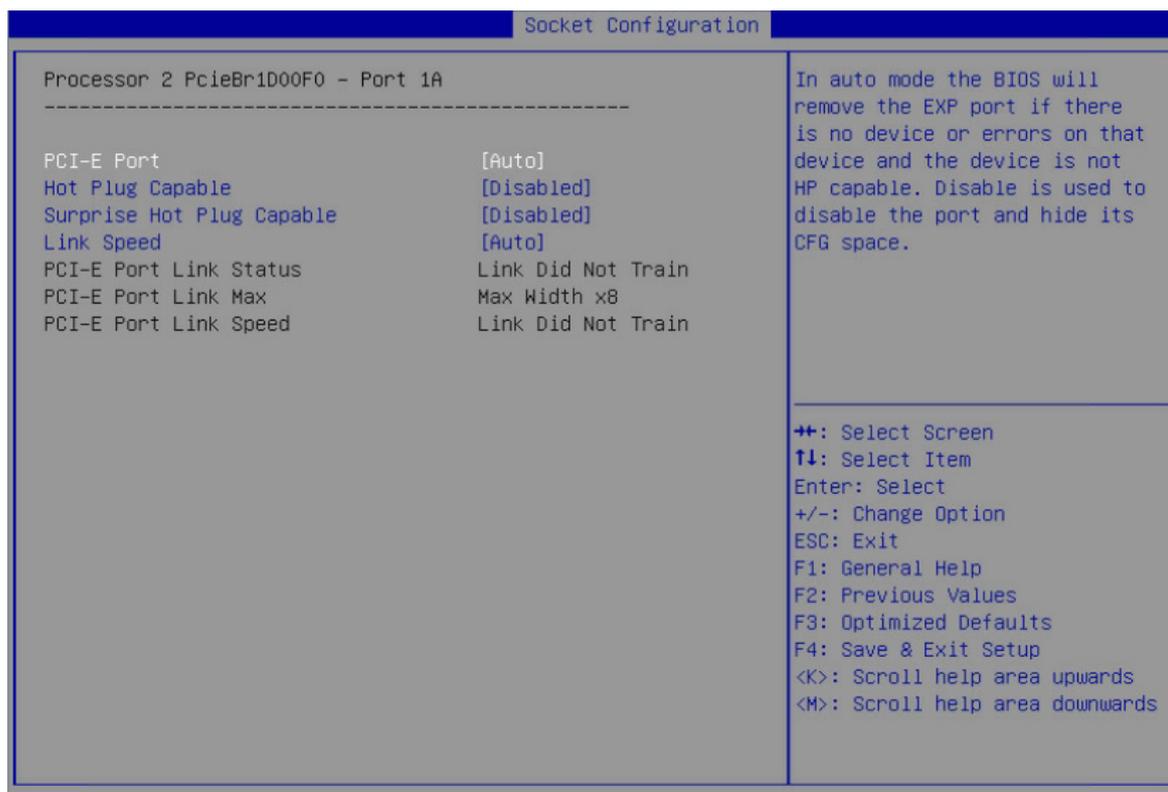


表3-65 Processor 2 PcieBr1D00F0 - Port 1A 界面参数

界面参数	功能说明
PCI-E Port	<p>PCI-E端口开关，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 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>
Hot Plug Capable	<p>热插拔能力配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：开启该 PCIe 端口的热插拔能力。</li> <li>• Disabled：关闭该 PCIe 端口的热插拔能力。</li> </ul>
Surprise Hot Plug Capable	<p>意外热插拔能力配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Enabled：开启该 PCIe 端口的意外热插拔能力。</li> <li>• Disabled：关闭该 PCIe 端口的意外热插拔能力。</li> </ul>
Link Speed	<p>链路速度配置，菜单选项为：</p> <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。

Intel VT for Directed I/O（VT-d）界面如 [图 3-75](#) 所示。具体参数说明如 [表 3-66](#) 所示。

图3-75 Intel VT for Directed I/O (VT-d) 界面

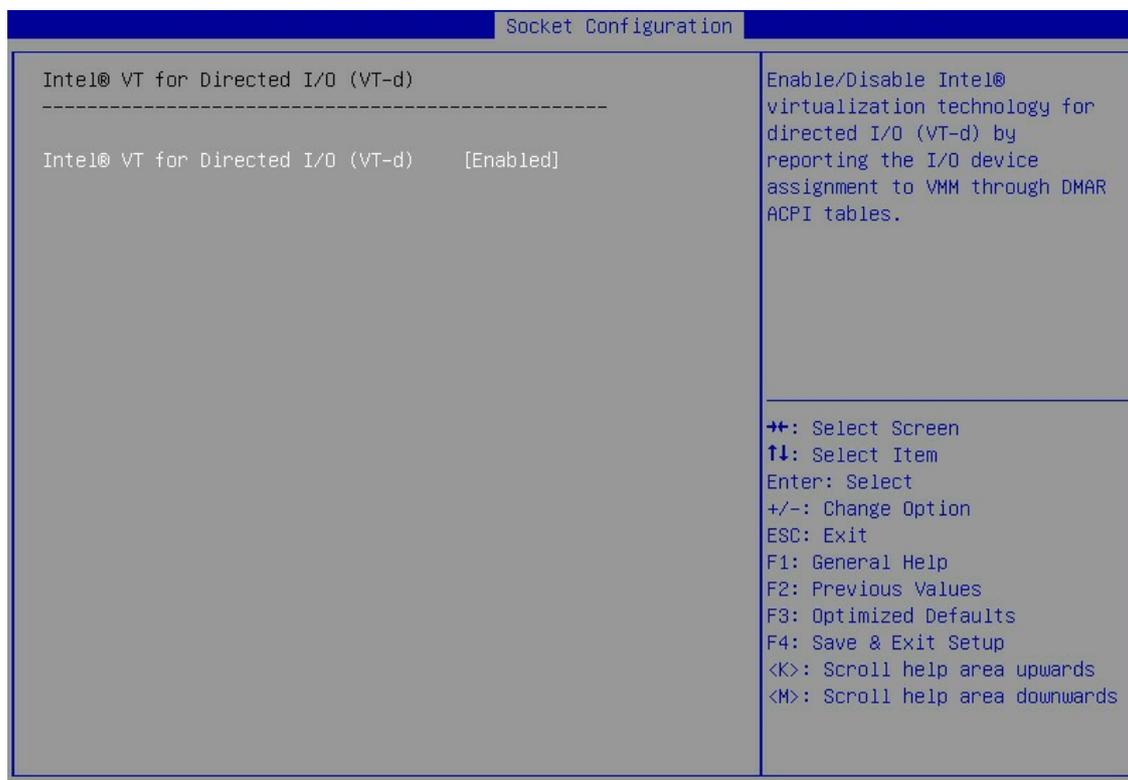


表3-66 Intel VT for Directed I/O (VT-d) 界面参数

界面参数	功能说明
Intel VT for Directed I/O (VT-d)	<p>Intel VT-d开关，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，菜单选项为：</p> <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>

Intel® VMD technology界面如 [图 3-76](#) 所示。具体参数说明如 [表 3-67](#) 所示。

图3-76 Intel® VMD technology 界面

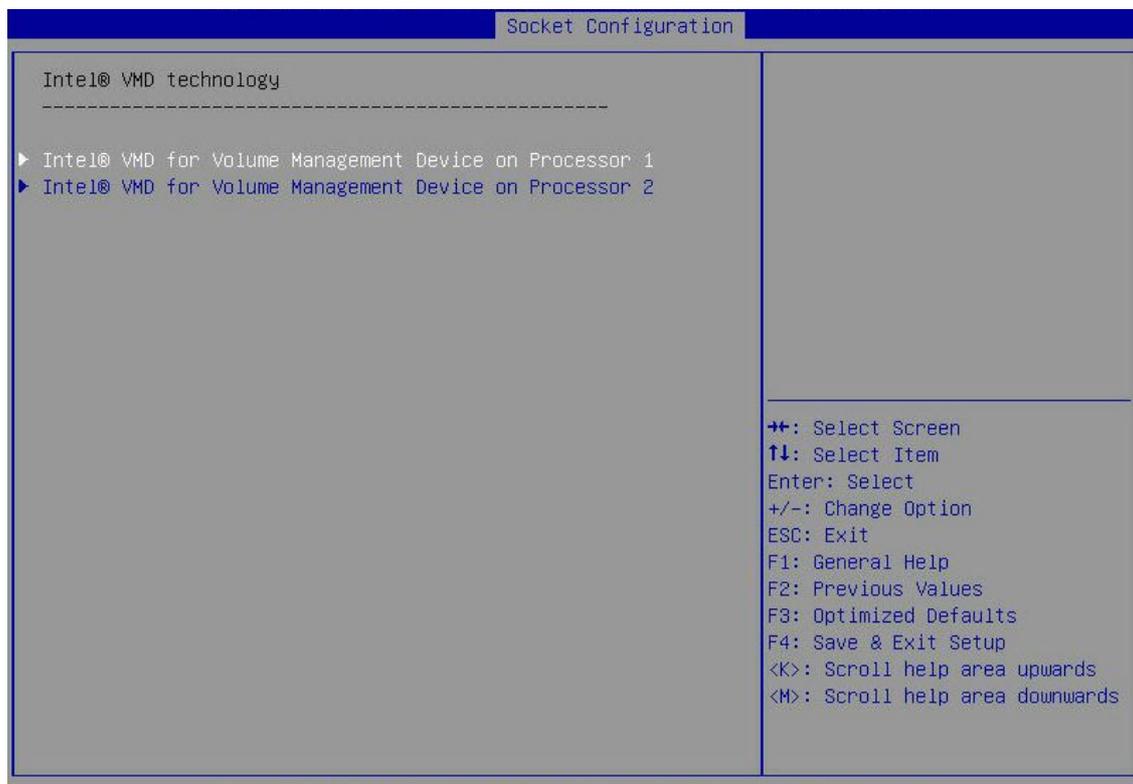


表3-67 Intel® VMD technology 界面参数

界面参数	功能说明
Intel® VMD for Volume Management Device on Processor 1	处理器1中的英特尔®VMD卷管理设备配置菜单。
Intel® VMD for Volume Management Device on Processor 2	处理器2中的英特尔®VMD卷管理设备配置菜单。

Intel® VMD for Volume Management Device on Processor 1 界面如 [图 3-77](#) 所示。具体参数说明如 [表 3-68](#) 所示。

图3-77 Intel® VMD for Volume Management Device on Processor 1 界面

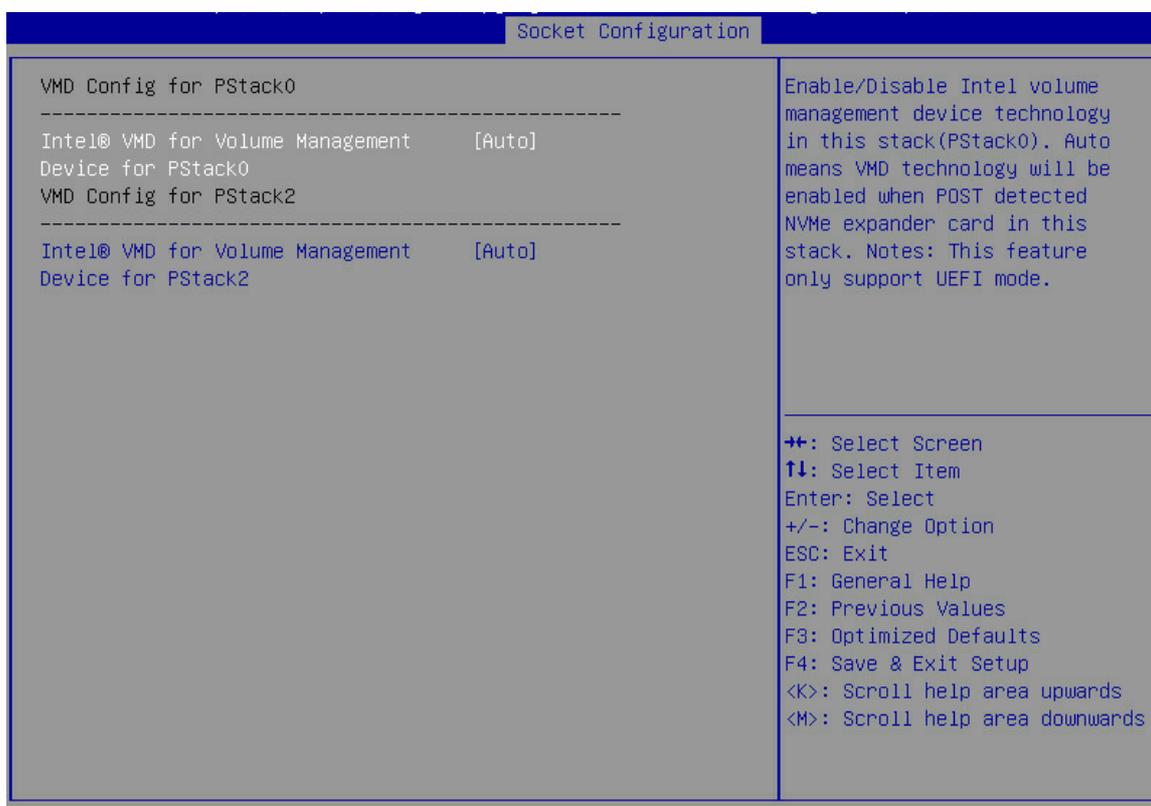


表3-68 Intel® VMD for Volume Management Device on Processor 1 界面参数

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: 启用此 PStack0 栈中英特尔®卷管理设备技术。</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: 启用此 PStack2 栈中英特尔®卷管理设备技术。</li> </ul> <p>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。</p>

Intel® VMD for Volume Management Device on Processor 2 界面如 [图 3-78](#) 所示。具体参数说明如 [表 3-69](#) 所示。

图3-78 Intel® VMD for Volume Management Device on Processor 2 界面

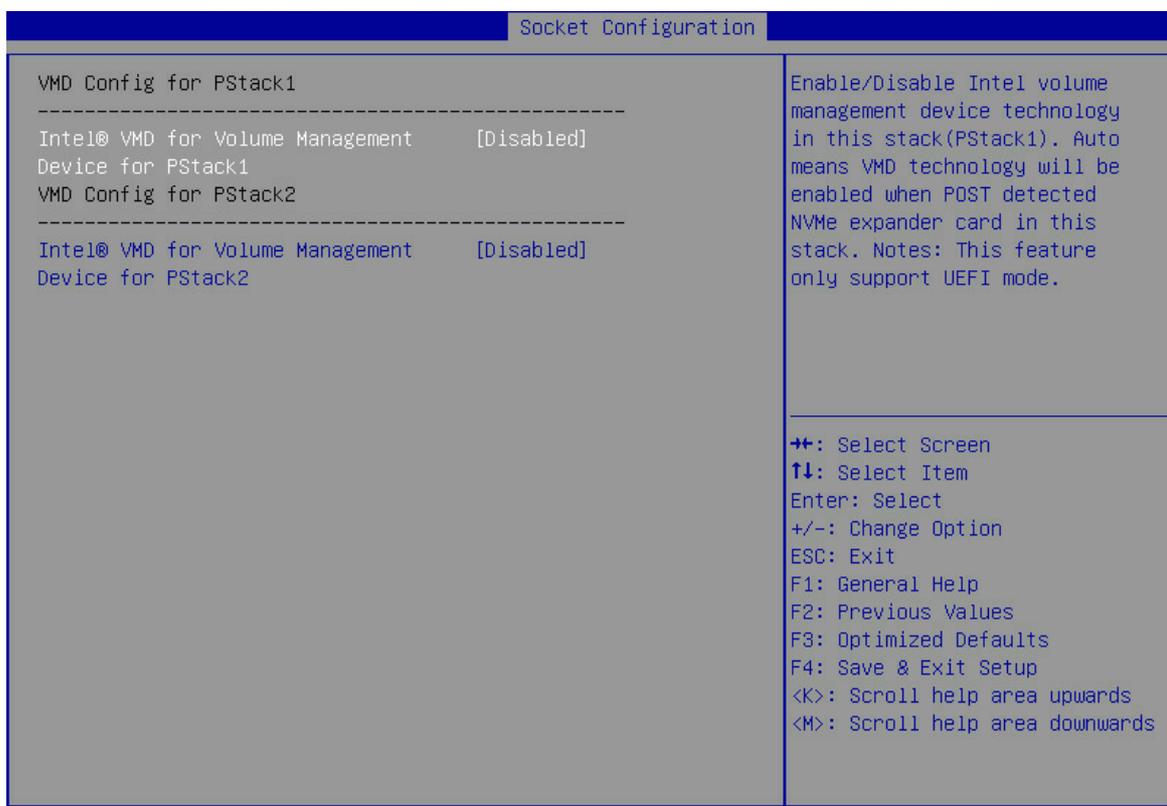


表3-69 Intel® VMD for Volume Management Device on Processor 2 界面参数

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 栈中英特尔®卷管理设备技术。</li> <li>• Enabled: 启用此 PStack1 栈中英特尔®卷管理设备技术。</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 栈中英特尔®卷管理设备技术。</li> <li>• Enabled: 启用此 PStack2 栈中英特尔®卷管理设备技术。</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>

### 3.4.6 Advanced Power Management Configuration界面

如 [图 3-79](#) 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 3-70](#) 所示。

图3-79 Advanced Power Management Configuration 界面

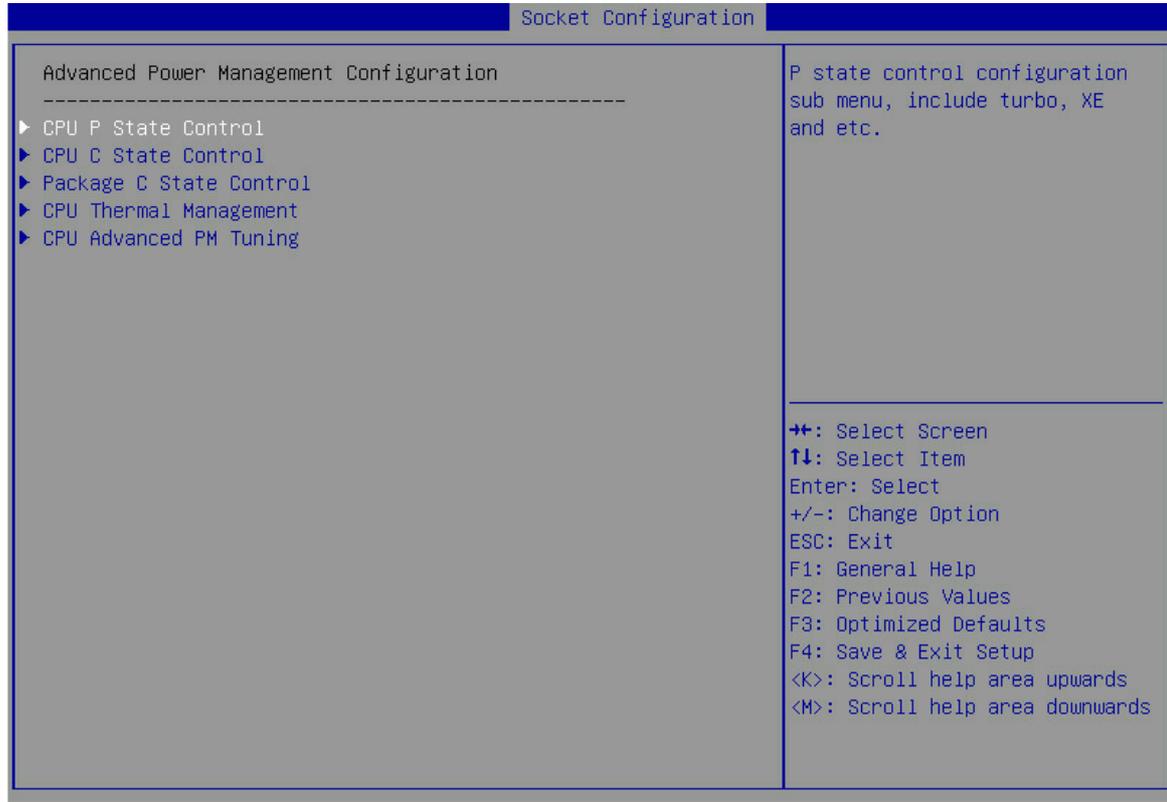


表3-70 Advanced Power Management Configuration 界面参数

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。
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。

CPU P State Control界面如 [图 3-80](#) 所示。具体参数说明如 [表 3-71](#) 所示。

图3-80 CPU P State Control 界面



表3-71 CPU P State Control 界面参数

界面参数	功能说明
EIST (P-State)	<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>
Turbo Mode	<p>Turbo模式开关，菜单选项为：</p> <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 C State Control界面如 [图 3-81](#) 所示。具体参数说明如 [表 3-72](#) 所示。

图3-81 CPU C State Control 界面



表3-72 CPU C State Control 界面参数

界面参数	功能说明
Autonomous Core C-State	自主的CPU核的C状态，菜单选项为： <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>
CPU C6 Report	向操作系统报告C6状态开关，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled：开启向操作系统报告 C6 状态功能。</li> <li>• Disabled（缺省）：关闭向操作系统报告 C6 状态功能。</li> <li>• Auto</li> </ul>
Enhanced Halt State (C1E)	C1E开关，开启本功能后，操作系统可自动调节C状态。 <ul style="list-style-type: none"> <li>• Enabled：开启 Enhanced Halt State 功能。</li> <li>• Disabled（缺省）：关闭 Enhanced Halt State 功能。</li> </ul>

Package C State Control界面如 [图 3-82](#) 所示。具体参数说明如 [表 3-73](#) 所示。

图3-82 Package C State Control 界面

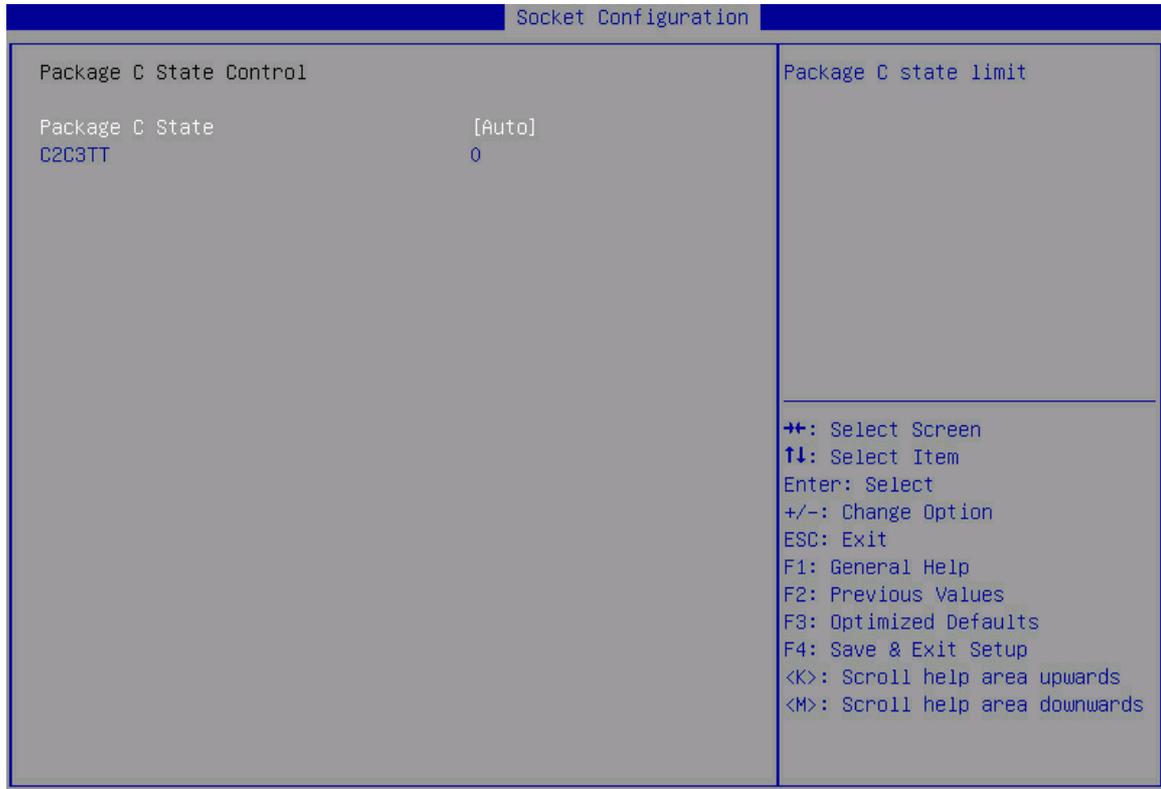


表3-73 Package C State Control 界面参数

界面参数	功能说明
Package C State	<p>Package C State限制选项，菜单选项为：</p> <ul style="list-style-type: none"> <li>• Auto（缺省）：默认 C 状态，由 CPU 决定。</li> <li>• (C0/C1 state)：设置成 C0/C1 状态。</li> <li>• C2 state：设置成 C2 状态。</li> <li>• C6(non Retention) state：设置成 C6（非残留）状态。</li> <li>• C6(Retention) state：设置成 C6（残留）状态。</li> <li>• No Limit：设置成无限制模式。</li> </ul>
C2C3TT	C2状态至C3状态转换计时器

CPU Thermal Management界面如 [图 3-83](#) 所示。具体参数说明如 [表 3-74](#) 所示。

图3-83 CPU Thermal Management 界面

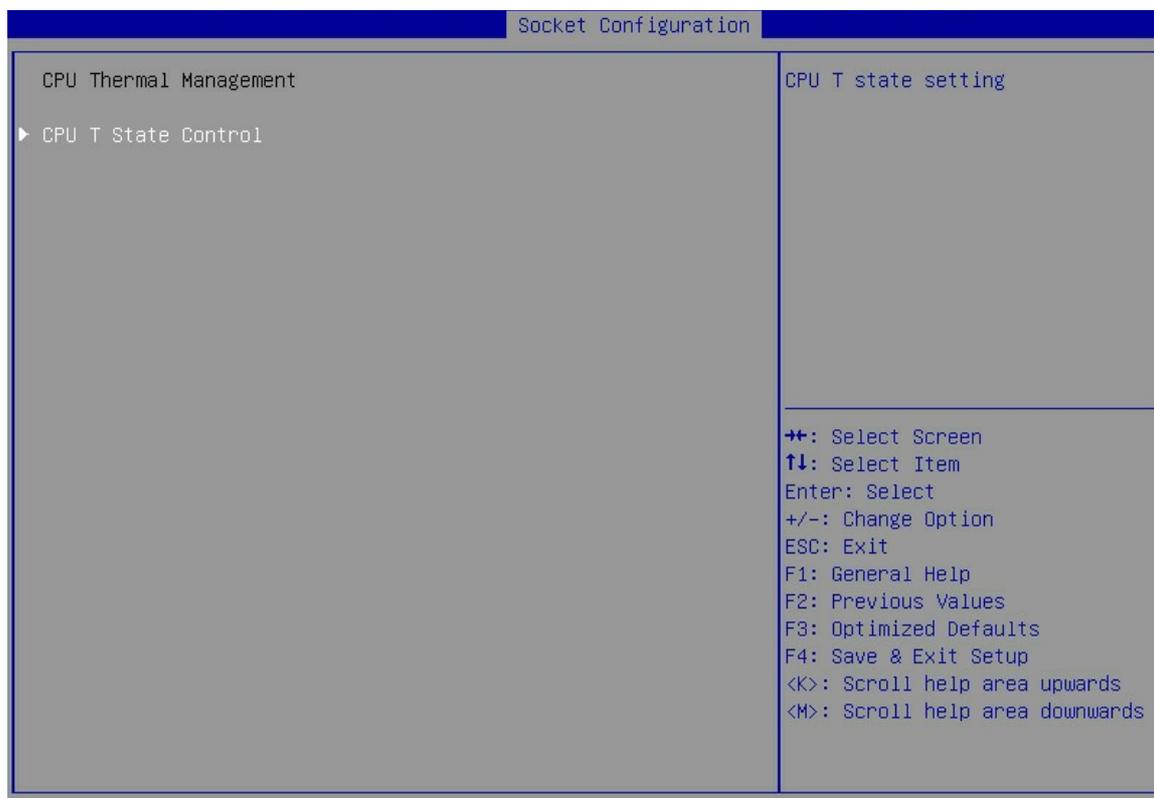


表3-74 CPU Thermal Management 界面参数

界面参数	功能说明
CPU T State Control	CPU T状态控制菜单

CPU T State Control界面如 [图 3-84](#) 所示。具体参数说明如 [表 3-75](#) 所示。

图3-84 CPU T State Control 界面

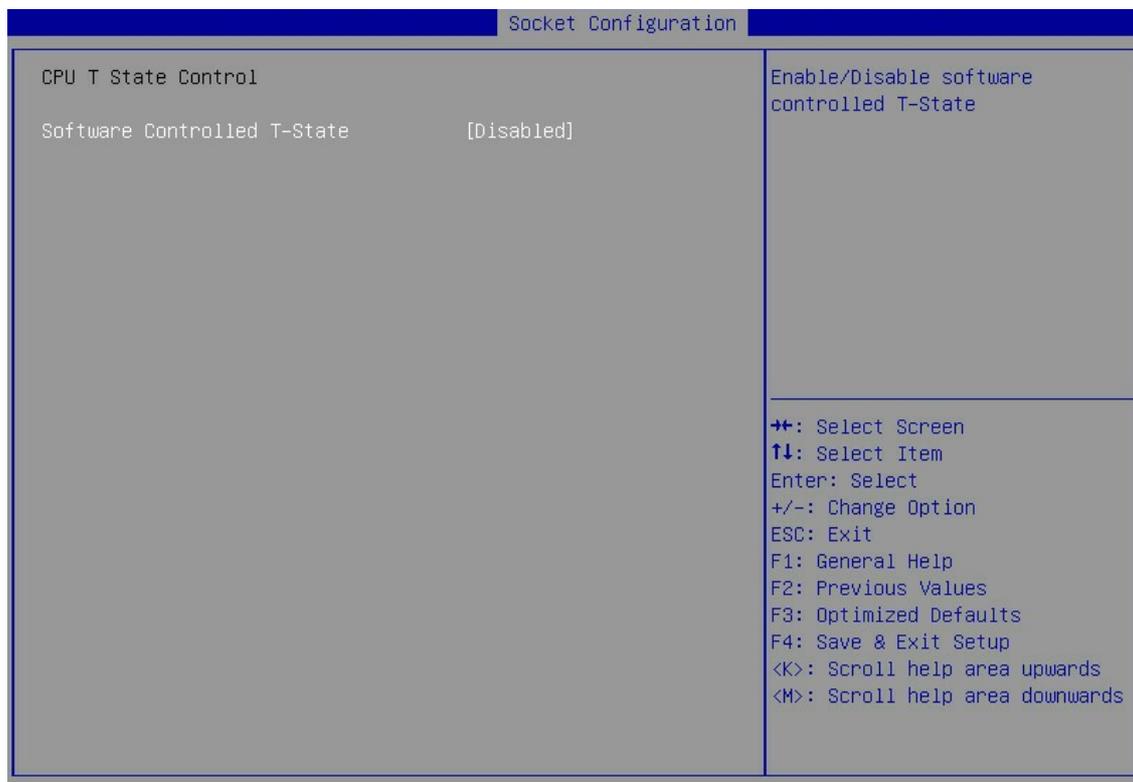


表3-75 CPU T State Control 界面参数

界面参数	功能说明
Software Controlled T-States	启用/禁用软件控制T状态： <ul style="list-style-type: none"> <li>• <b>Enabled:</b> 开启软件控制 T 状态功能。</li> <li>• <b>Disabled (缺省):</b> 关闭软件控制 T 状态功能。</li> </ul>

CPU Advanced PM Tuning界面如 [图 3-85](#) 所示。具体参数说明如 [表 3-76](#) 所示。

图3-85 CPU Advanced PM Tuning 界面

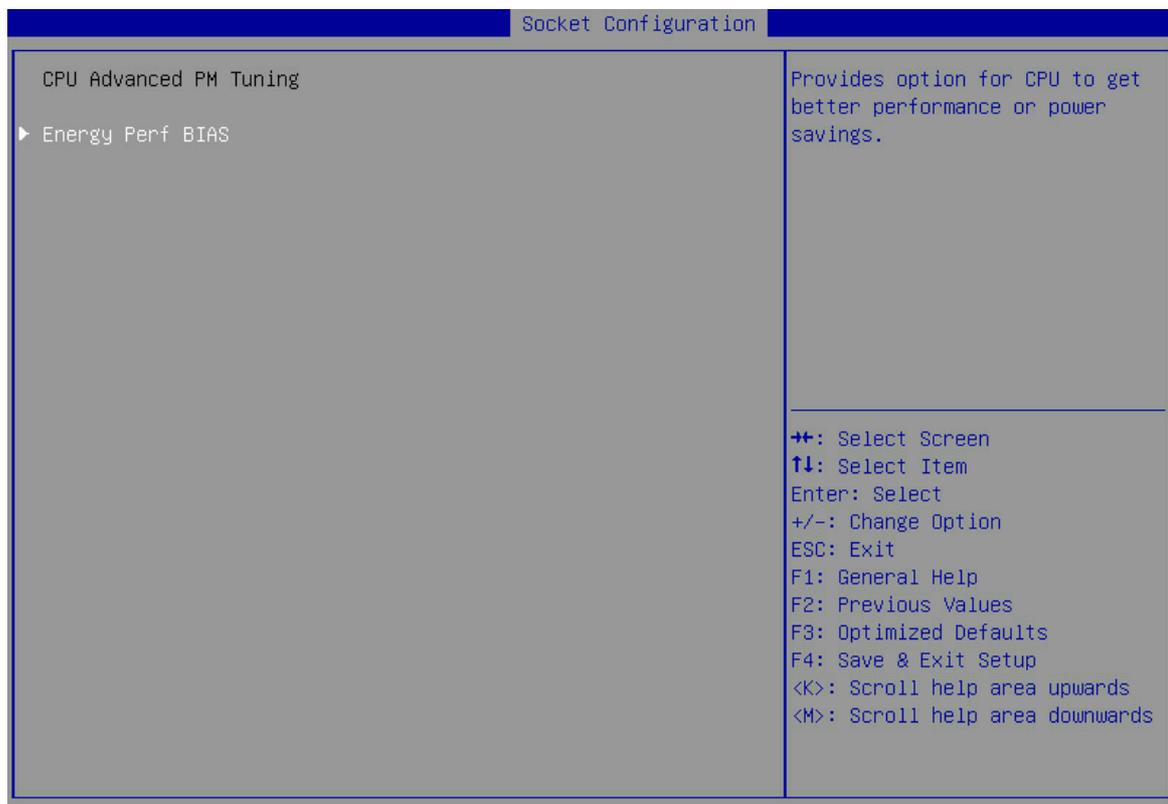


表3-76 CPU Advanced PM Tuning 界面参数

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。

Energy Perf BIAS界面如 [图 3-86](#) 所示。具体参数说明如 [表 3-77](#) 所示。

图3-86 Energy Perf BIAS 界面

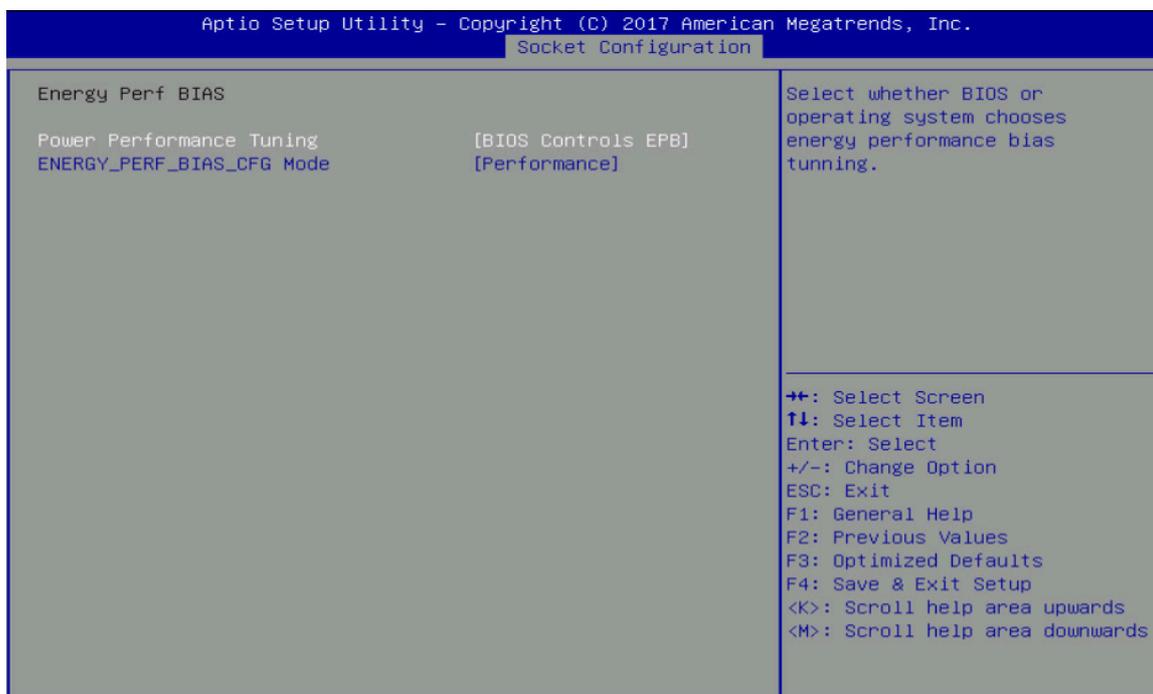


表3-77 Energy Perf BIAS 界面参数

界面参数	功能说明
Energy Performance Tuning	<p>选择BIOS或者OS进行CPU的节能性能调整，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>
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能量性能调整的配置，Energy 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>

### 3.5 Server Management界面

介绍 Server Management 界面包含的参数及相关功能。

Server Management界面如 [图 3-87](#) 所示，主要包含FRB-2 计时器配置、看门狗配置、系统事件日志配置、HDM网络配置、固件信息、等。具体参数说明如 [表 3-78](#) 所示。

图3-87 Server Management 界面

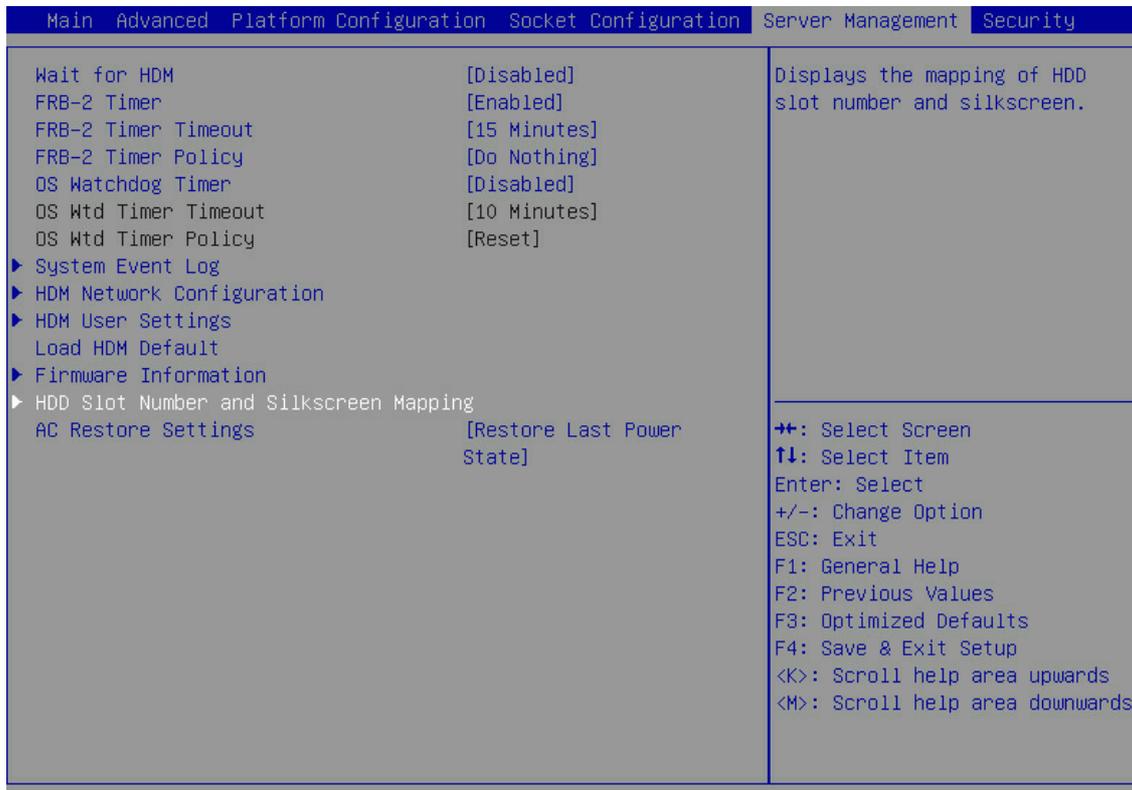


表3-78 Server Management 界面参数

界面参数	功能说明
Wait for HDM	等待HDM设置，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 开启等待 HDM 功能。</li> <li>Disabled (缺省): 关闭等待 HDM 功能。</li> </ul>
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>

界面参数	功能说明
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（缺省）：无动作。</li> <li>Reset：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>
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>
System Event Log	系统事件日志配置菜单
HDM Network Configuration	HDM网络配置菜单
HDM User Settings	HDM用户配置菜单
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30s，服务器重启之前请勿设置与HDM相关的选项。
Firmware Information	显示固件信息菜单
HDD Slot Number and Silkscreen Mapping	BIOS Setup界面下硬盘的槽位号与硬盘丝印槽位号的对应关系
AC Restore Settings	AC恢复配置状态设置，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> <p>需要注意的是：AC Restore Settings的缺省项与HDM的设置有关。</p>

System Event Log界面如 [图 3-88](#) 所示。具体参数说明如 [表 3-79](#) 所示。

图3-88 System Event Log 界面

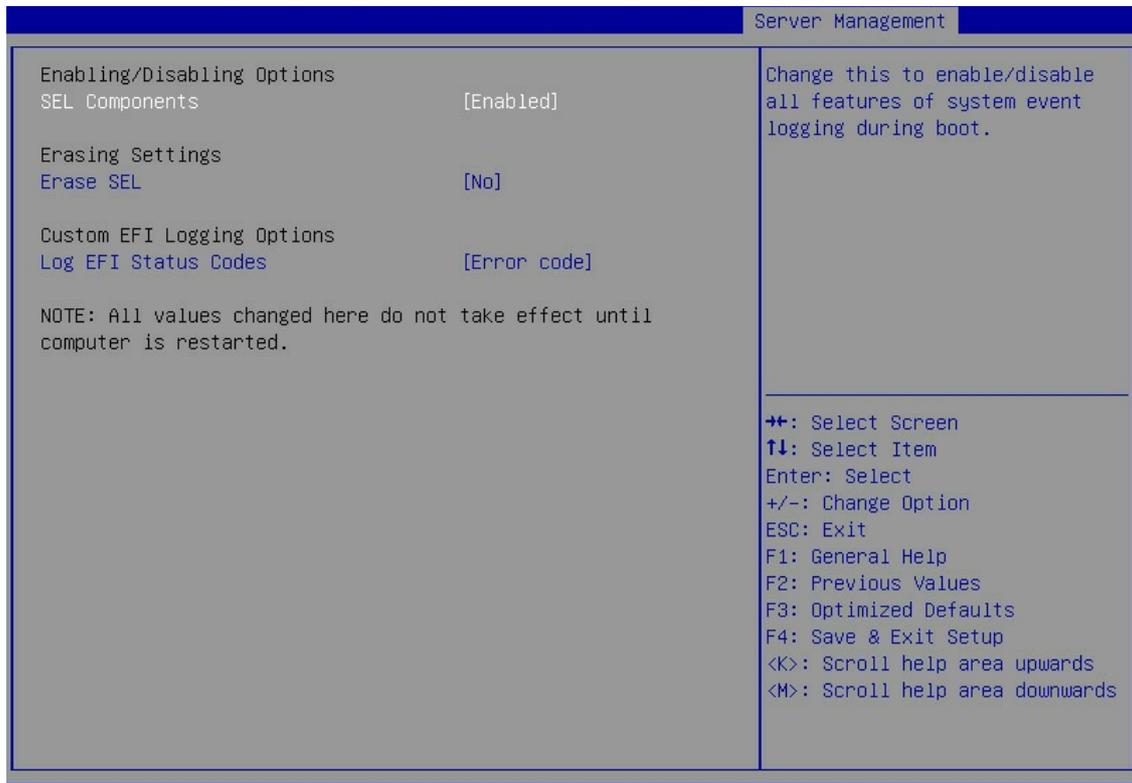


表3-79 System Event Log 界面参数

界面参数	功能说明
<b>Enabling/Disabling Options</b>	
SEL Components	SEL组件开关设置，菜单选项为： <ul style="list-style-type: none"> <li>• Enabled（缺省）：启用 SEL 组件。</li> <li>• Disabled：禁用 SEL 组件。</li> </ul>
<b>Erasing Settings</b>	
Erase SEL	系统事件日志的擦除设置，当SEL Components设置为Enabled时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• No（缺省）：不擦除系统事件日志。</li> <li>• Yes, On next reset：下次重启擦除系统事件日志。</li> <li>• Yes, On every reset：每次重启擦除系统事件日志。</li> </ul>
<b>Custom EFI Logging Options</b>	
Log EFI Status Codes	记录EFI状态代码设置，当SEL Components设置为Enabled时，该选项可用，菜单选项为： <ul style="list-style-type: none"> <li>• Disabled：禁用记录 EFI 状态代码。</li> <li>• Both：同时记录 EFI 错误码和进程码。</li> <li>• Error Code（缺省）：只记录 EFI 错误码。</li> <li>• Progress Code：只记录 EFI 进程码。</li> </ul>

HDM Network Configuration界面如 [图 3-89](#) 所示。具体参数说明如 [表 3-80](#) 所示。



说明

HDM Shared Network Port（HDM 共享网络接口）、HDM Dedicated Network Port（HDM 专用网络接口）和 HDM Bonding Network Port（HDM Bonding 网络接口）的配置参数相同，本文以 HDM Shared Network Port 为例。

图3-89 HDM Network Configuration 界面

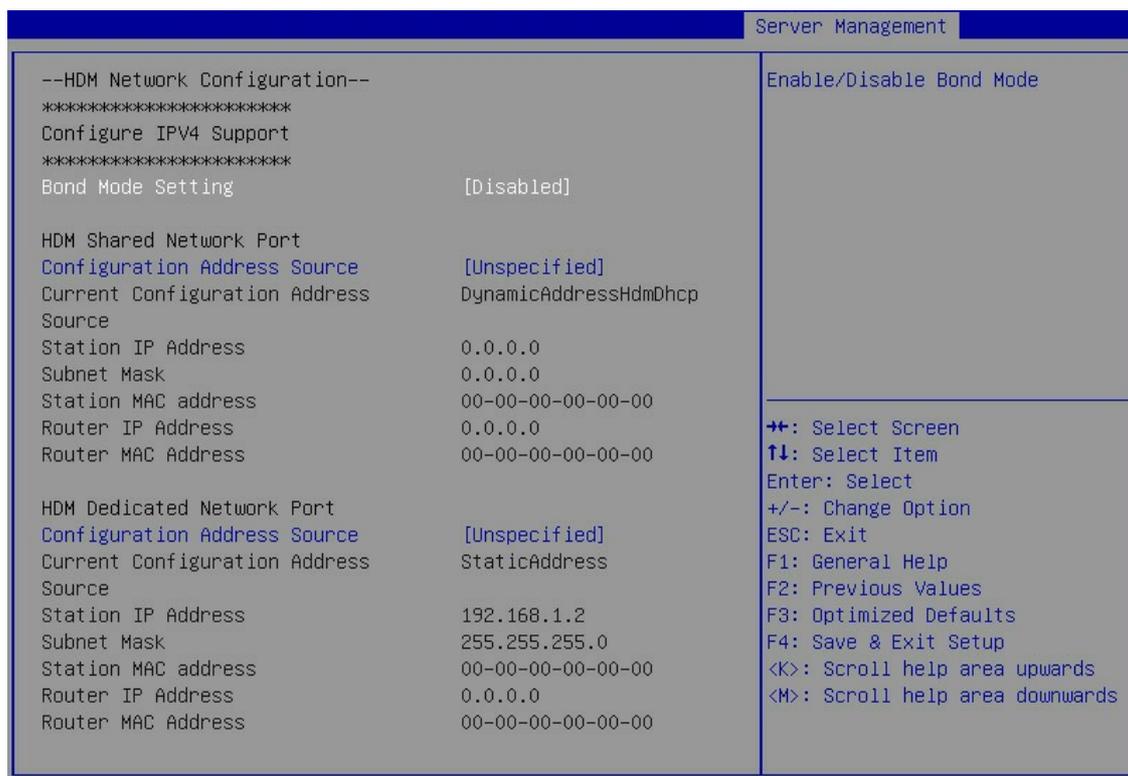


表3-80 HDM Network Configuration 界面参数

界面参数	功能说明
Bond Mode Setting	<p>Bond模式配置，菜单选项为：</p> <ul style="list-style-type: none"> <li>Enabled: 开启 Bond 模式。开启该模式后，将 HDM Dedicated Network Port(HDM 专用网络接口)的 IP 地址作为 HDM Bonding Network Port（HDM Bonding 网络接口）的 IP 地址。</li> <li>Disabled（缺省）：关闭 Bond 模式。</li> </ul> <p>需要注意的是，开启该模式后：</p> <ul style="list-style-type: none"> <li>HDM Network Configuration 界面仅显示 HDM Bonding Network Port（HDM Bonding 网络接口）的网络信息。连接 HDM 共享网络接口和 HDM 专用网络接口中的任意一个，都能通过 HDM Bonding 网络接口的 IP 地址访问 HDM。</li> <li>BIOS 启动界面仅显示 HDM Bonding 网络接口的 IP 地址。</li> </ul>

界面参数	功能说明
Configuration Address Source	配置HDM网络状态参数：可设置静态IP，动态获取IP，Unspecified将不修改HDM网络参数 <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	配置当前地址源
Station IP Address	端口的IP地址
Subnet Mask	子网掩码
Station MAC Address	端口的MAC地址
Router IP Address	网关IP地址
Router MAC Address	网关MAC地址

HDM User Settings界面如 [图 3-90](#) 所示。具体参数说明如 [表 3-81](#) 所示。

图3-90 HDM User Settings 界面

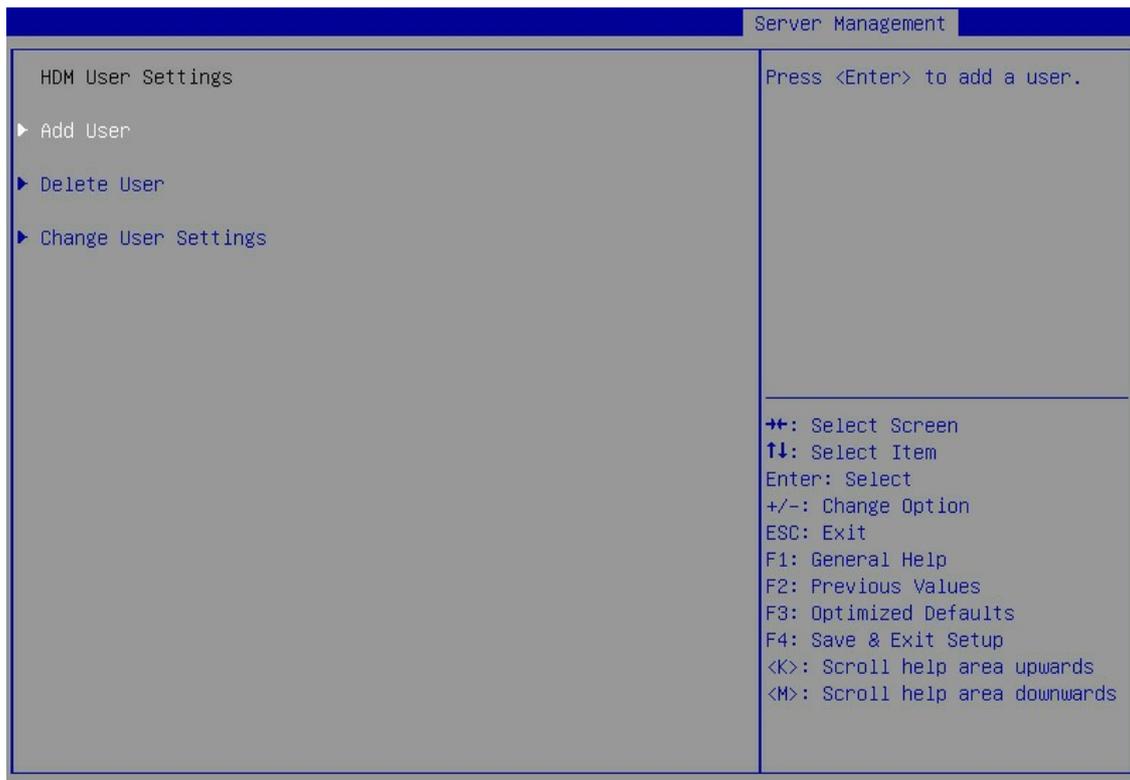


表3-81 HDM User Settings 界面参数

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 3-91](#)所示。具体参数说明如 [表 3-82](#)所示。

图3-91 Add User 界面

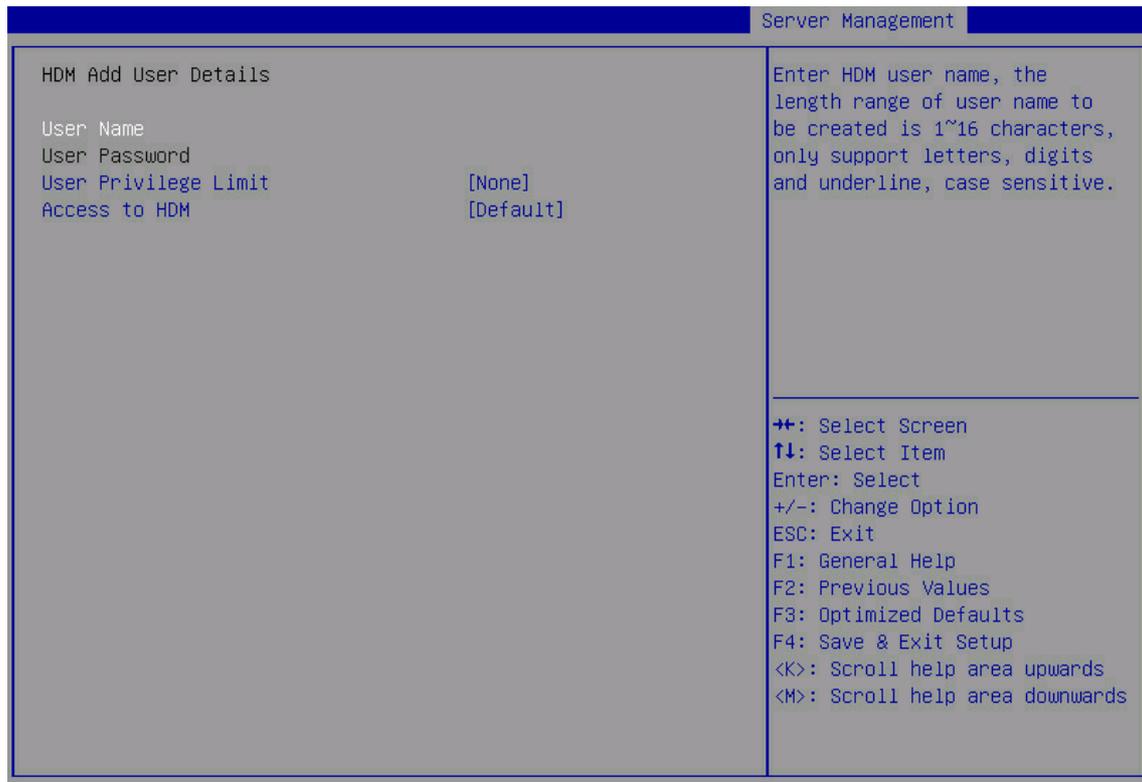


表3-82 Add User 界面参数

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8~16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2~16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>
User Privilege Limit	<p>HDM用户权限，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>None</b>（缺省）：保留当前的HDM用户权限。</li> <li>• <b>User</b>：用户权限。</li> <li>• <b>Operator</b>：操作员权限。</li> <li>• <b>Administrator</b>：管理员权限。</li> </ul>
Access to HDM	<p>用户访问开关，菜单选项为：</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>：开启用户访问功能。</li> <li>• <b>Disabled</b>：关闭用户访问功能。</li> <li>• <b>Default</b>（缺省）：保留上次保存的用户访问权限。</li> </ul>

Delete User界面如 [图 3-92](#) 所示。具体参数说明如 [表 3-83](#) 所示。

图3-92 Delete User 界面

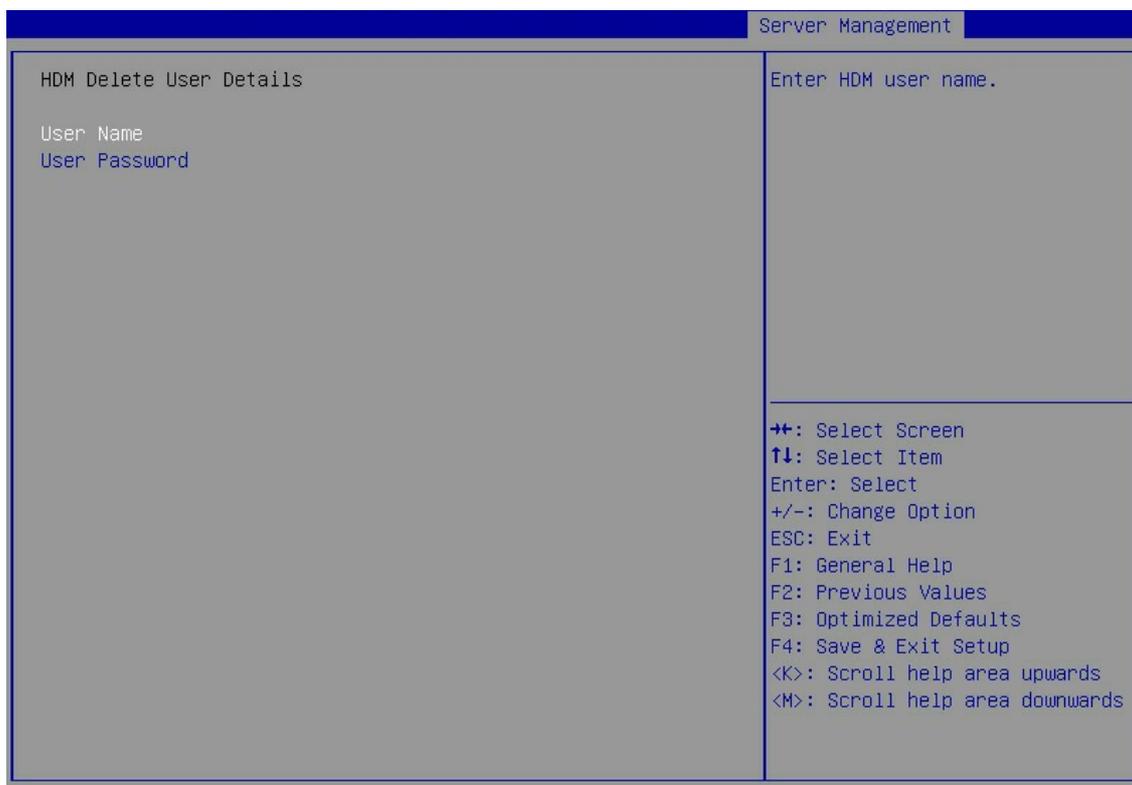


表3-83 Delete User 界面参数

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 3-93](#) 所示。具体参数说明如 [表 3-84](#) 所示。

图3-93 Change User Settings 界面

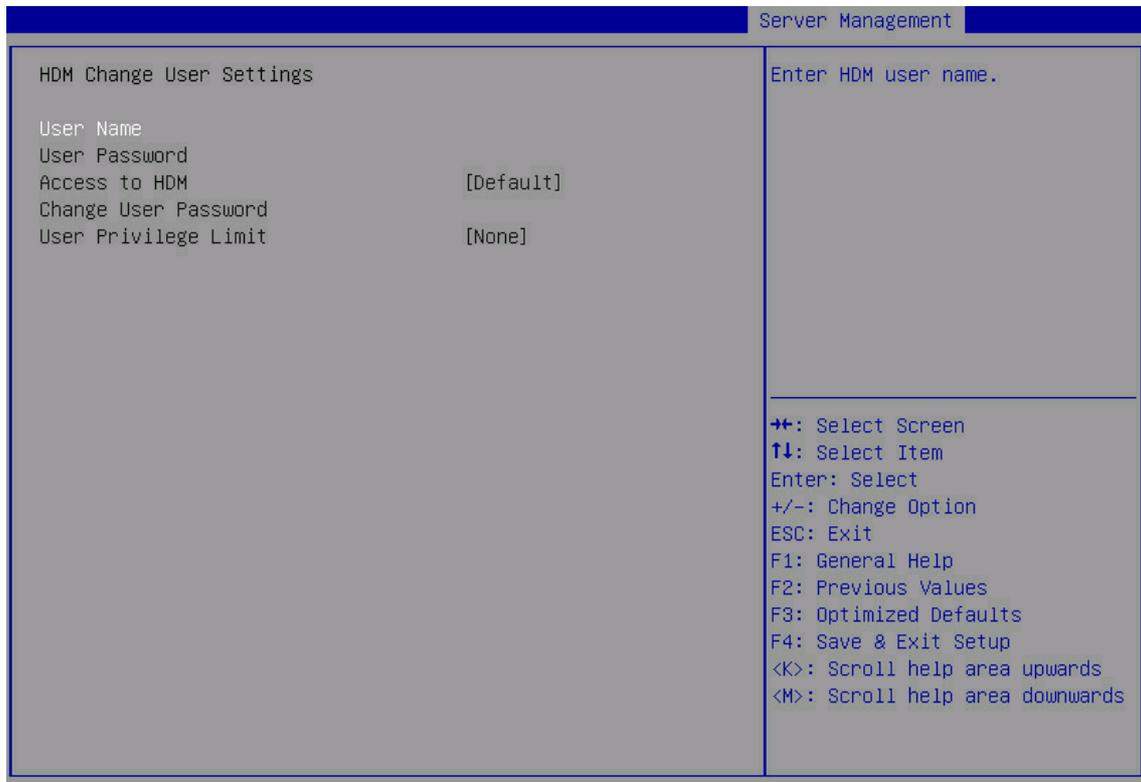


表3-84 Change User Settings 界面参数

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
Access to HDM	<p>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：</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> 开启用户访问功能。</li> <li>• <b>Disabled:</b> 关闭用户访问功能。</li> <li>• <b>Default (缺省):</b> 保留上次保存的用户访问权限。</li> </ul>



表3-85 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

HDD Slot Number and Silkscreen Mapping界面如 图 3-95 所示。具体参数说明如 表 3-86 所示。

图3-95 HDD Slot Number and Silkscreen Mapping 界面

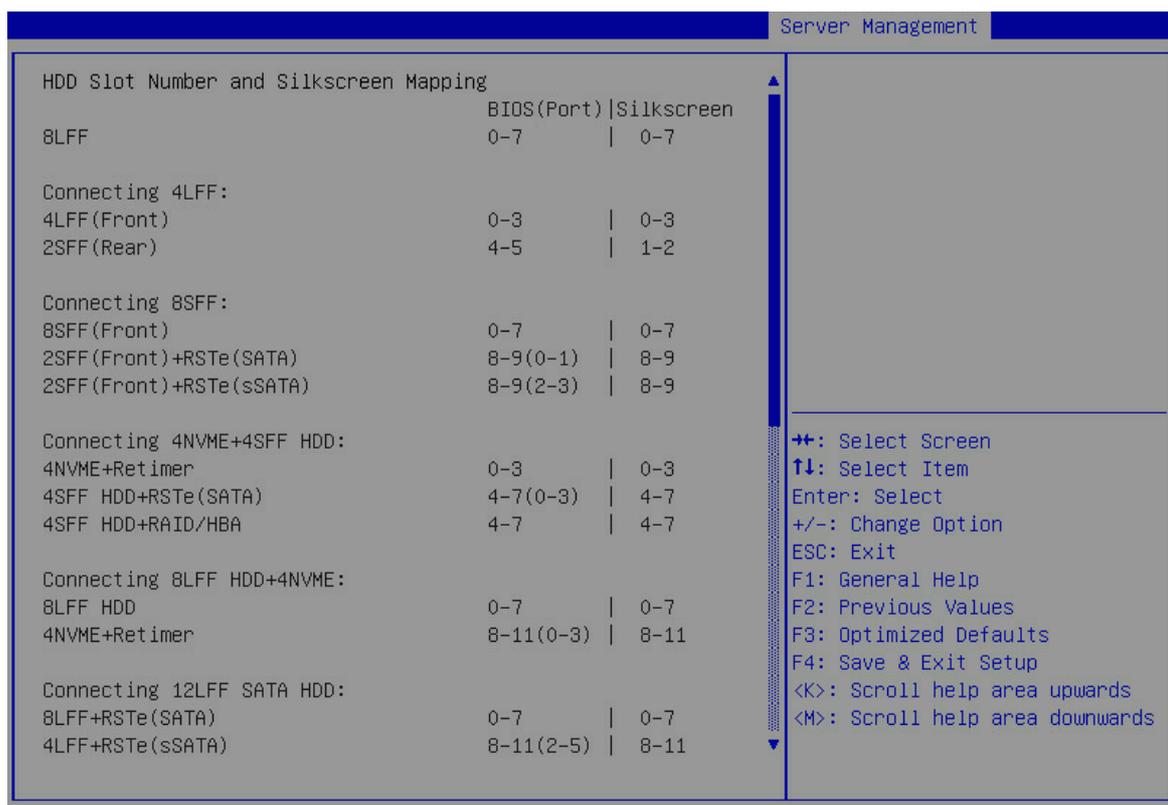


表3-86 HDD Slot Number and Silkscreen Mapping 界面参数

界面参数	功能说明
8LF	BIOS Setup界面下，8LFF硬盘的槽位号0~7对应硬盘丝印槽位0~7
<b>Connecting 4LFF</b>	
4LFF(Front)	BIOS Setup界面下，前面板4LFF硬盘的槽位号0~3对应前面板硬盘丝印槽位号0~3。
2SFF(Rear)	BIOS Setup界面下，后面板2SFF硬盘的槽位号4~5对应前面板硬盘丝印槽位号1~2。
<b>Connecting 8SFF</b>	
8SFF(Front)	BIOS Setup界面下，前面板8SFF硬盘的槽位号0~7对应前面板硬盘丝印槽位号0~7。
2SFF(Front) + RSTe(SATA)	使用RSTe板载软RAID时，BIOS Setup界面PCH SATA Configuration选项下，前面板2SFF硬盘的槽位号8~9(实际是PCH SATA port 0~1)对应前面板硬盘丝印槽位号8~9。
2SFF(Front) + RSTe(sSATA)	使用RSTe板载软RAID时，BIOS Setup界面PCH sSATA Configuration选项下，前面板2SFF硬盘的槽位号8~9(实际是PCH sSATA port 2~3)对应前面板硬盘丝印槽位号8~9。
<b>Connecting 4NVME+4SFF HDD</b>	
4NVME+Retimer	使用Retimer卡接四个NVME时，BIOS Setup界面下，前面板4NVME硬盘的槽位号0~3对应前面板硬盘丝印槽位号0~3。
4SFF HDD + RSTe(SATA)	使用RSTe板载软RAID时，BIOS Setup界面PCH SATA Configuration选项下，前面板4SFF硬盘的槽位号4~7（实际是PCH SATA port 0~1）对应前面板硬盘丝印槽位号4~7。
4SFF HDD +RAID/HBA	使用RAID卡或HBA卡时，BIOS Setup界面下，前面板4SFF硬盘的槽位号4~7对应前面板硬盘丝印槽位号4~7。
<b>Connecting 8LFF HDD+4NVME</b>	
8LFF HDD	BIOS Setup界面下，前面板8LFF硬盘的槽位号0~7对应前面板硬盘丝印槽位号0~7。
4NVME+Retimer	使用Retimer卡接四个NVME时，BIOS Setup界面下，前面板4NVME硬盘的槽位号8~11（对应Retimer卡0~3接口）对应前面板硬盘丝印槽位号8~11。
<b>Connecting 12LFF SATA HDD</b>	
8LFF+ RSTe(SATA)	使用RSTe板载软RAID时，BIOS Setup界面PCH SATA Configuration选项下，前面板8LFF硬盘的槽位号0~7对应前面板硬盘丝印槽位号0~7。
4LFF+ RSTe(sSATA)	使用RSTe板载软RAID时，BIOS Setup界面PCH sSATA Configuration选项下，前面板4LFF硬盘的槽位号8~11（实际是PCH sSATA port 2~5）对应前面板硬盘丝印槽位号8~11。
<b>Connecting 8NVME</b>	
8NVME+ Retimer（slot 1/2）	使用一个Retimer卡1（1U机型接slot1,2U机型接slot2）时，BIOS Setup界面下，前面板8NVME硬盘的槽位号0~3对应前面板硬盘丝印槽位号0~3。

界面参数	功能说明
8NVME+ Retimer (slot 2/5)	使用Retimer卡2 (1U机型接slot2,2U机型接slot5) 时, BIOS Setup界面下, 前面板8NVME硬盘的槽位号4~7 (对应Retimer卡0~3接口), 对应前面板硬盘丝印槽位号4~7。
8NVME+ Switch	使用Switch卡连接NVME硬盘时。BIOS Setup界面下, 后面板8NVME硬盘的槽位号0~7对应后面板硬盘丝印槽位号0~7。
<b>Connecting 10SFF</b>	
10SFF(Front)	BIOS Setup界面下, 前面板10LFF硬盘的槽位号0~9对应前面板硬盘丝印槽位号0~9。
2SFF(Rear)	BIOS Setup界面下, 后面板2SFF硬盘的槽位号10~11对应后面板硬盘丝印槽位号1~2。
<b>Connecting 12LFF</b>	
12LFF(Front)	BIOS Setup界面下, 前面板12LFF硬盘的槽位号0~11对应前面板硬盘丝印槽位号0~11。
4LFF(Rear)	BIOS Setup界面下, 后面板4LFF硬盘的槽位号20,21,23,24对应后面板硬盘丝印槽位号1,2,4,5。
2LFF(Rear)	BIOS Setup界面下, 后面板2LFF硬盘的槽位号23~24对应后面板硬盘丝印槽位号4~5。
4SFF(Rear)	BIOS Setup界面下, 后面板4SFF硬盘的槽位号26~29对应后面板硬盘丝印槽位号7~10。
2SFF(Rear)	BIOS Setup界面下, 后面板2SFF硬盘的槽位号28~29对应后面板硬盘丝印槽位号9~10。
<b>Connecting 25SFF</b>	
25SFF(Front)	BIOS Setup界面下, 前面板25SFF硬盘的槽位号0~24对应前面板硬盘丝印槽位号0~24。
2LFF(Rear)	BIOS Setup界面下, 后面板2LFF硬盘的槽位号33~34对应后面板硬盘丝印槽位号4~5。
4SFF(Rear)	BIOS Setup界面下, 后面板4SFF硬盘的槽位号36~39对应后面板硬盘丝印槽位号7~10。
2SFF(Rear)	BIOS Setup界面下, 后面板2SFF硬盘的槽位号38~39对应后面板硬盘丝印槽位号9~10。

G3 四款机型SATA sSATA端口与背板槽位的对应关系请参见“[4 SATA sSATA端口与背板槽位的对应关系](#)”。

## 3.6 Security界面

介绍通过 Security 界面, 可以对安全功能进行控制包括设置 BIOS 密码等。

Security界面如 [图 3-96](#) 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 3-87](#) 所示。

图3-96 Security 界面

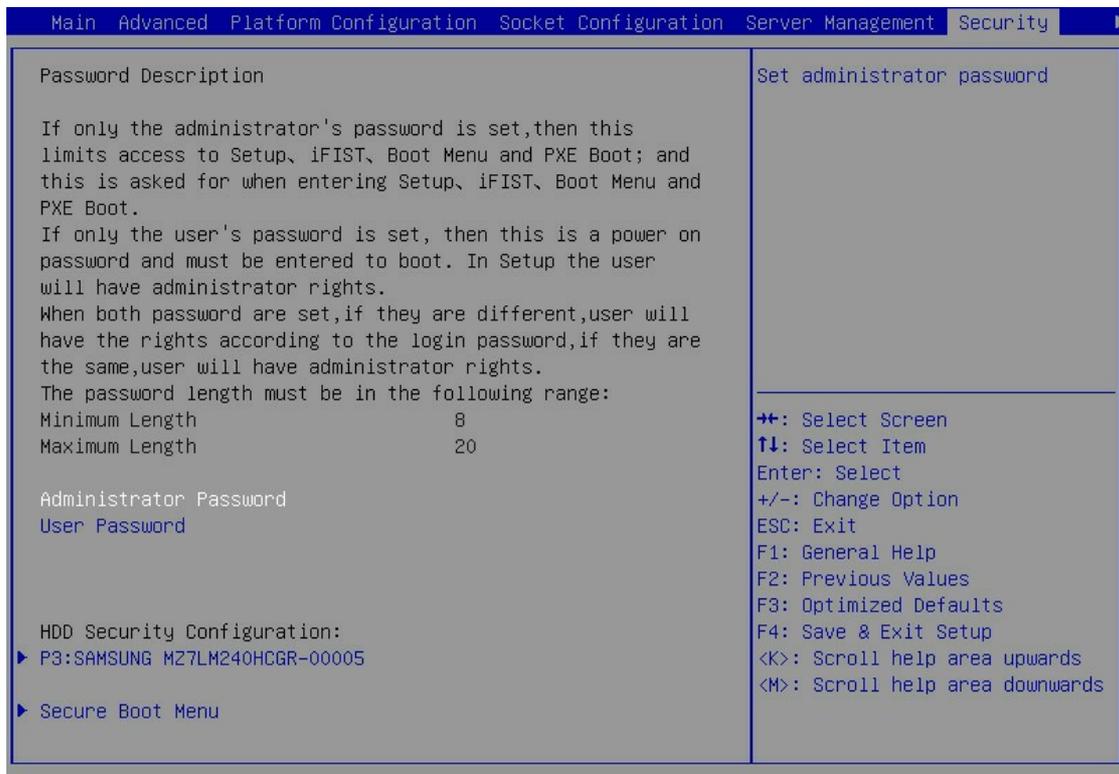


表3-87 Security 界面参数

界面参数	功能说明
Password Description	密码描述
Administrator Password	创建管理员密码
User Password	创建用户密码
HDD Security Configuration	硬盘安全配置菜单，当安装的硬盘支持安全配置时显示该菜单。如果安装了多块支持安全配置的硬盘，会依次显示。
Secure Boot Menu	安全启动菜单，仅UEFI启动模式下显示该菜单。

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，进入系统时，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 [表 3-88](#) 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3-88 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	
		Lock Legacy Resources	灰显	
	PCI Subsystem Settings	Above 4G Decoding	灰显	
		SR-IOV Support		
	USB Configuration	Legacy USB Support		
		XHCI Hand-off		
		USB Mass Storage Device Support		
	Server Mgmt	Wait for HDM		灰显
		FRB-2 Timer		
FRB-2 Timer Timeout				
FRB-2 Timer Policy				
OS Watchdog Timer				
OS Wtd Timer Timeout				
OS Wtd Timer Policy				
System Event Log				
HDM Network Configuration				
HDM User Settings				
Security	Administrator Password		灰显	
	Secure Boot Menu	System Mode	灰显	
		Secure Boot		
		Vendor Keys		
		Attempt Secure Boot		
		Secure Boot Mode		
Key Management				

HDD Security Configuration界面如 [图 3-97](#) 所示，具体参数说明如 [表 3-89](#) 所示。

图3-97 HDD Security Configuration 界面

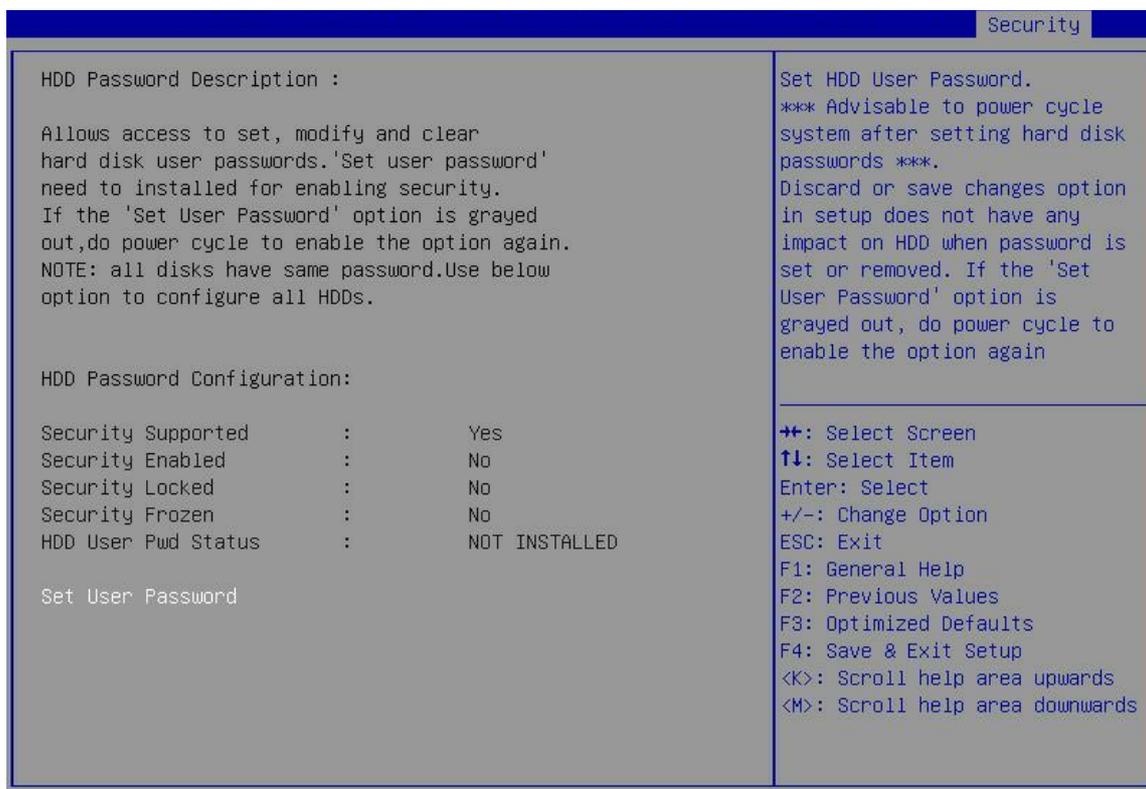


表3-89 HDD Security Configuration 界面参数

界面参数	功能说明
Security Supported	显示支持硬盘安全配置
Security Enabled	显示硬盘安全的启用状态， <b>Yes</b> 表示硬盘已设置用户密码，此时需要输入正确的密码后才能正常使用硬盘，否则硬盘会被锁定。 <b>No</b> 表示硬盘未设置用户密码。
Security Locked	显示硬盘安全锁的状态， <b>Yes</b> 表示硬盘已被锁定，此时硬盘不可用，输入正确的密码后可解除硬盘锁定。 <b>No</b> 表示硬盘未被锁定。
Security Frozen	显示硬盘的冻结状态， <b>Yes</b> 表示硬盘已被冻结，此时硬盘可以正常使用但不支持设置硬盘用户密码，将服务器下电并重新启动后可解除硬盘冻结。 <b>No</b> 表示硬盘未被冻结。
HDD User Pwd Status	显示硬盘用户密码的状态， <b>Not Installed</b> 表示未设置硬盘用户密码。 <b>Installed</b> 表示已设置硬盘用户密码。
Set User Password	设置硬盘用户密码，长度为1~32个字符，支持字母、数字、空格和特殊字符`~!@#%&*()_+=[[{}];':",./<>?`，区分大小写。设置硬盘用户密码后，请妥善保管密码。服务器在启动过程中，会提示您输入硬盘用户密码，请根据提示输入密码。如果连续三次输入错误硬盘会被锁定，此时硬盘不可用。

Secure Boot Menu界面如 [图 3-98](#) 所示，具体参数说明如 [表 3-90](#) 所示。

图3-98 Secure Boot Menu 界面

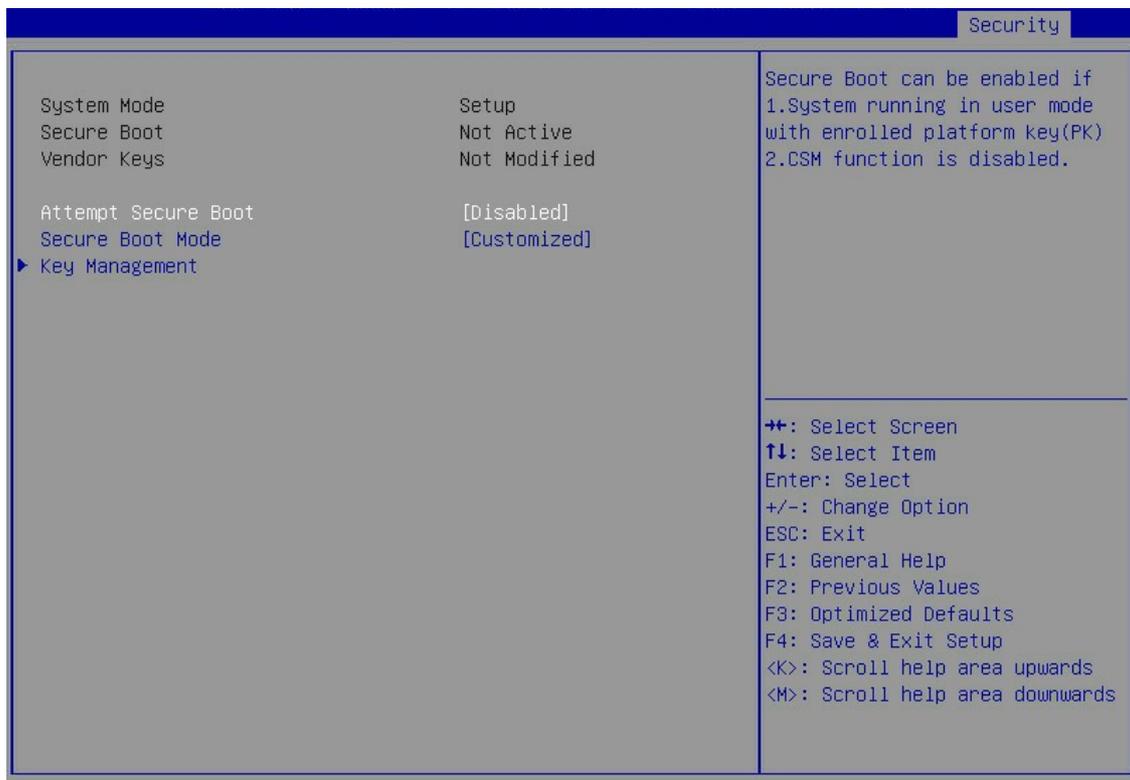


表3-90 Secure Boot Menu 界面参数

界面参数	功能说明
System Mode	显示系统模式
Secure Boot	显示安全启动
Vendor Keys	显示供应商密钥
Attempt Secure Boot	安全启动配置，菜单选项为： <ul style="list-style-type: none"> <li>• <b>Enabled</b>：开启安全启动。同时满足以下两种情况时开启安全启动。 <ul style="list-style-type: none"> <li>◦ 系统运行在注册平台密钥的用户模式。</li> <li>◦ CSM（兼容性支持模块）功能未开启。</li> </ul> </li> <li>• <b>Disabled</b>（缺省）：关闭安全启动。</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>Customized</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>
Key Management	更改安全启动变量

Key Management界面如 [图 3-99](#) 所示，具体参数说明如 [表 3-91](#) 所示。

图3-99 Key Management 界面

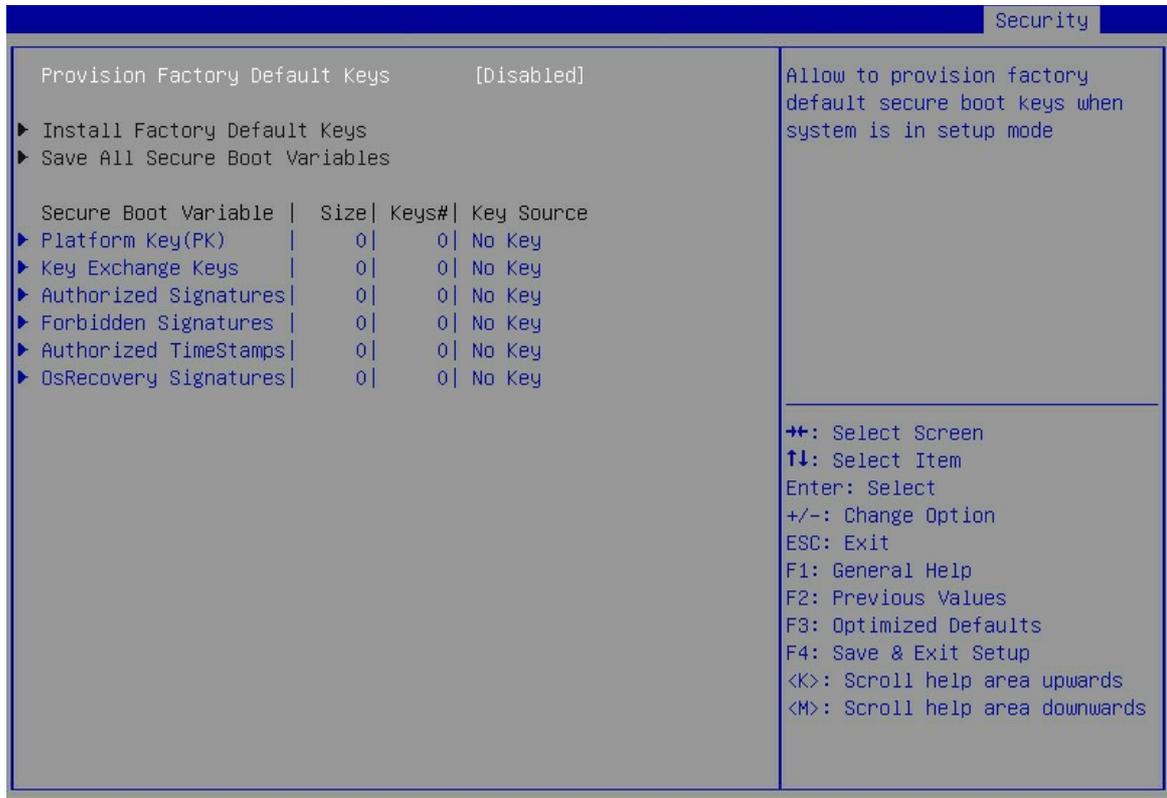


表3-91 Key Management 界面参数

界面参数	功能说明
Provision Factory Default Keys	提供出厂默认密钥，菜单选项为： <ul style="list-style-type: none"> <li>Enabled: 提供出厂默认密钥。</li> <li>Disabled (缺省): 不提供出厂默认密钥。</li> </ul>
Install Factory Default Keys	注册所有的出厂默认密钥，完成注册后，该选项会变为Reset all Secure Boot Variables。
Save all Secure Boot Variables	保存所有的安全启动变量
Platform Key(PK)	平台密钥配置，菜单选项为： <ul style="list-style-type: none"> <li>Set New Var: 设置新的密钥。</li> </ul>
Key Exchange Keys	交换密钥设置，菜单选项为： <ul style="list-style-type: none"> <li>Set New Var: 设置新的密钥。</li> <li>Append Key: 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>Set New Var: 设置新的密钥。</li> <li>Append Key: 添加密钥。</li> </ul>

界面参数	功能说明
Forbidden Signatures	被禁止的签名，菜单选项为： <ul style="list-style-type: none"> <li>• Set New Var: 设置新的密钥。</li> <li>• Append Key: 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>• Set New Var: 设置新的密钥。</li> <li>• Append Key: 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>• Set New Var: 设置新的密钥。</li> <li>• Append Key: 添加密钥。</li> </ul>

### 3.7 Boot界面

介绍通过 **Boot** 界面，可以对启动功能进行控制包括服务器的启动顺序、**BIOS** 的启动模式等。

**Boot**界面如 [图 3-100](#)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 3-92](#)所示。

图3-100 Boot 界面

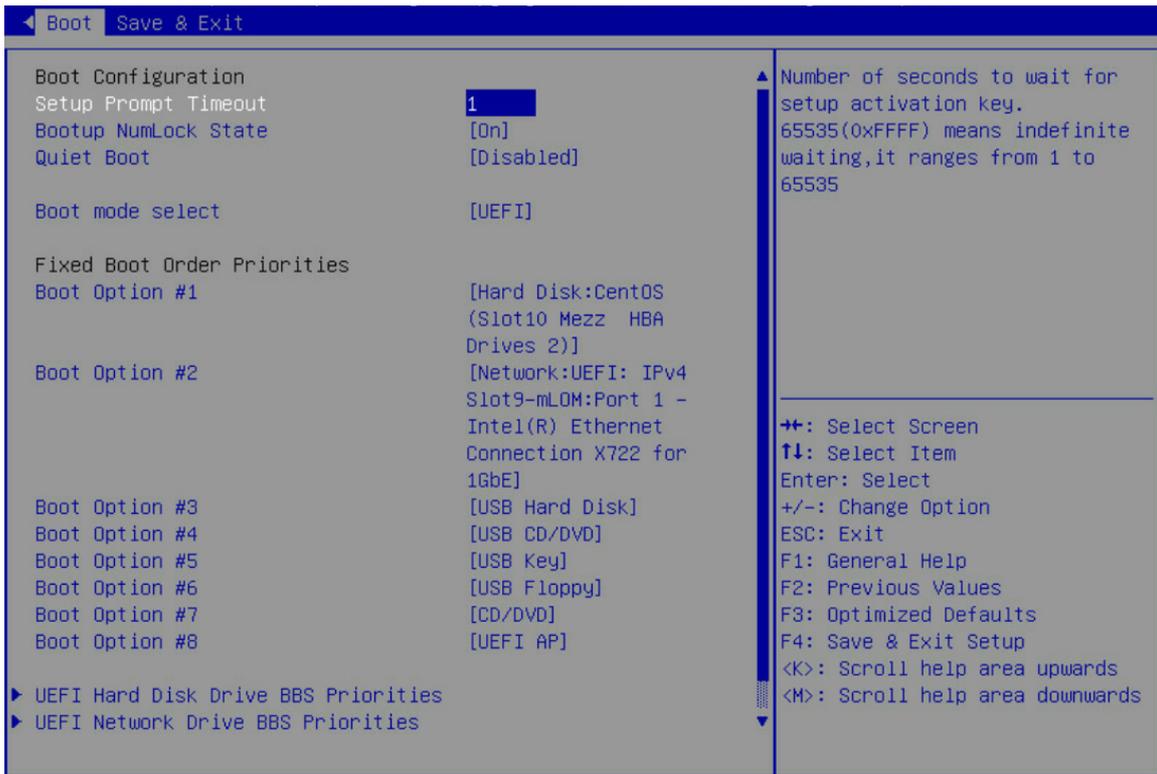


表3-92 Boot 界面参数

界面参数	功能说明
Setup Prompt Timeout	设置提示超时时间，等待Setup激活热键的时间，取值范围1~65535，缺省值为1。
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>
Quiet Boot	以安静模式启动系统，菜单选项为： <ul style="list-style-type: none"> <li>Enabled：开启安静启动设置。</li> <li>Disabled (缺省)：关闭安静启动设置。</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>
Fixed Boot Order Priorities	启动优先级配置菜单
UEFI Hard Disk Drive BBS Priorities (UEFI启动模式) / Hard Disk Drive BBS Priorities (Legacy启动模式)	硬盘启动优先级配置菜单，从可用的硬盘驱动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 USB Hard Disk Drive BBS Priorities (UEFI启动模式) / USB Hard Disk Drive BBS Priorities (Legacy启动模式)	USB接口接入的硬盘启动优先级配置菜单，从可用的USB接口接入的硬盘中指定启动的优先级顺序。当连接可启动USB接口接入的硬盘时，显示该菜单。
UEFI USB CDROM/DVD Drive BBS Priorities (UEFI启动模式) / USB CDROM/DVD Drive BBS Priorities (Legacy启动模式)	USB接口接入的光驱启动优先级配置菜单，从可用的USB接口接入的光驱中指定启动的优先级顺序。当连接可启动USB接口接入的光驱时，显示该菜单。
UEFI USB Key Drive BBS Priorities (UEFI启动模式) / USB Key Drive BBS Priorities (Legacy启动模式)	U盘启动优先级配置菜单，从可用的U盘中指定启动的优先级顺序。当连接U盘时，显示该菜单。
UEFI USB Floppy Drive BBS Priorities (UEFI启动模式) / USB Floppy Drive BBS Priorities (Legacy启动模式)	USB接口接入的软盘优先级配置菜单，从可用的USB接口接入的软盘中指定启动的优先级顺序。当连接可启动USB接口接入的软盘时，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 Application Boot Priorities	UEFI启动模式下Application启动优先级配置菜单，从可用的应用中指定启动设备的优先级顺序，仅UEFI启动模式下显示该菜单。

Fixed Boot Order Priorities界面如 [图 3-101](#) 所示。具体参数说明如 [表 3-93](#) 所示。

图3-101 Fixed Boot Order Priorities 界面

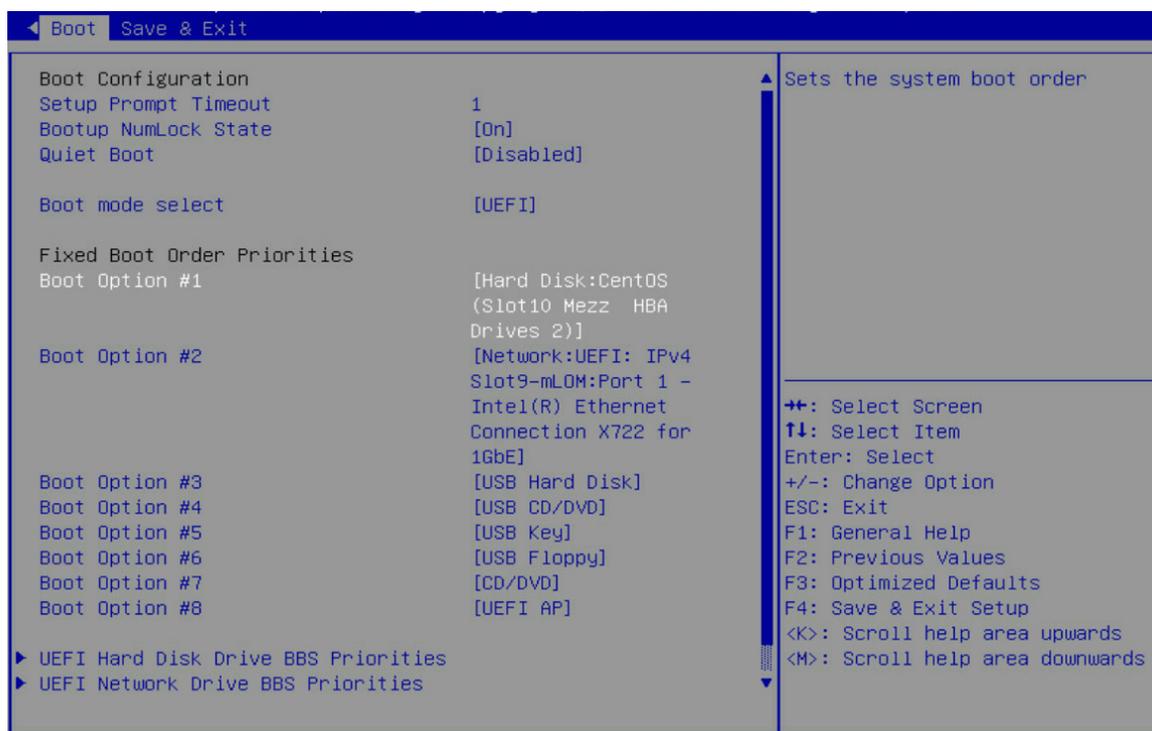


表3-93 Fixed Boot Order Priorities 界面参数

界面参数	功能说明
Boot Option #1	设置系统的第1启动选项
Boot Option #2	设置系统的第2启动选项
Boot Option #3	设置系统的第3启动选项
Boot Option #4	设置系统的第4启动选项
Boot Option #5	设置系统的第5启动选项
Boot Option #6	设置系统的第6启动选项
Boot Option #7	设置系统的第7启动选项
Boot Option #8	设置系统的第8启动选项
Boot Option #9	设置系统的第9启动选项，仅UEFI启动模式下显示该启动项。

UEFI Hard Disk Drive BBS Priorities界面如 [图 3-102](#) 所示。具体参数如 [表 3-94](#) 所示。

图3-102 UEFI Hard Disk Drive BBS Priorities 界面

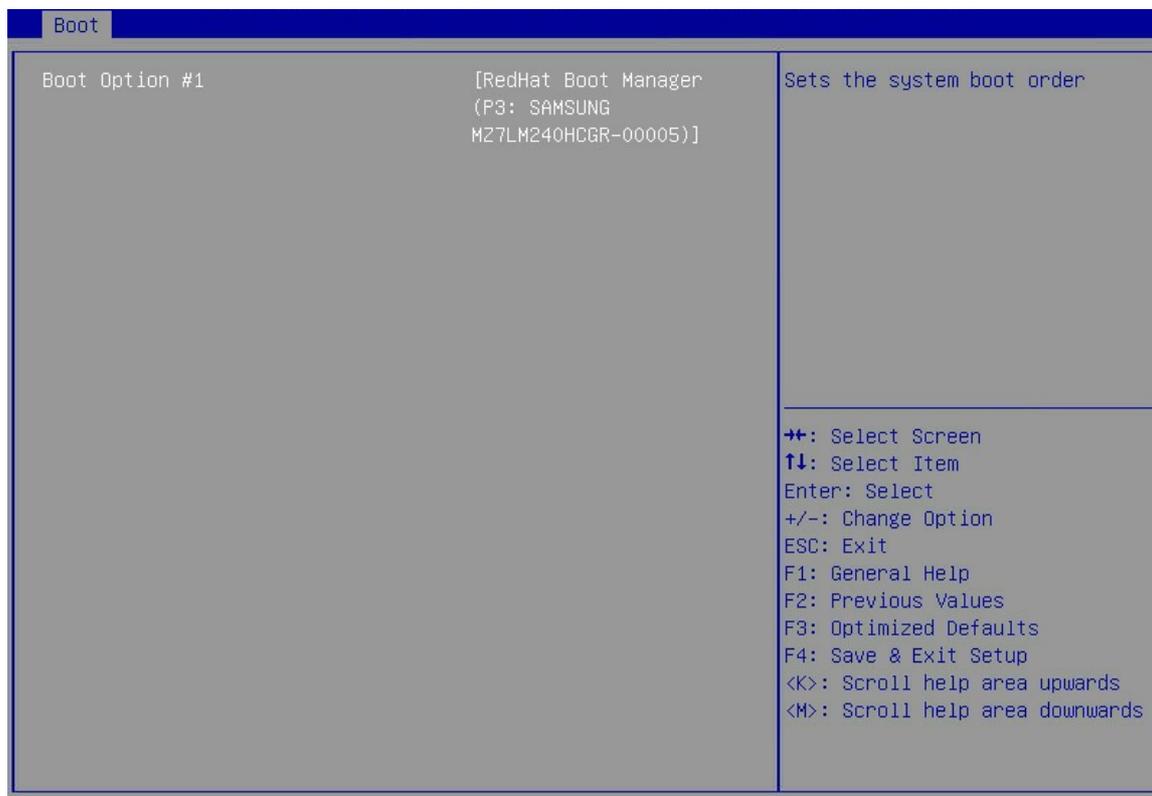


表3-94 UEFI Hard Disk Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项
Boot Option #2	第2启动选项

UEFI CDROM/DVD Drive BBS Priorities界面如 [图 3-103](#) 所示。具体参数如 [表 3-95](#) 所示。

图3-103 UEFI CDROM/DVD Drive BBS Priorities 界面



表3-95 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

UEFI USB Hard Disk Drive BBS Priorities界面如 [图 3-104](#) 所示。具体参数如 [表 3-96](#) 所示。

图3-104 UEFI USB Hard Disk Drive BBS Priorities 界面

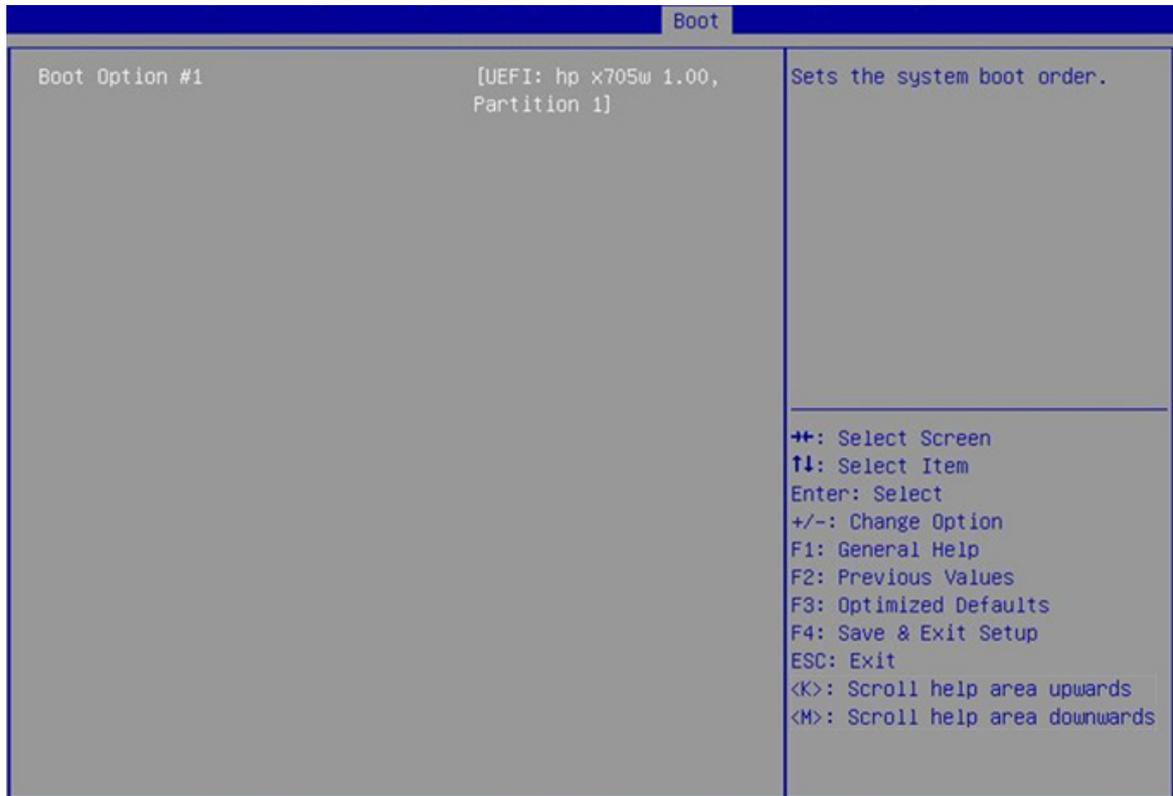


表3-96 UEFI USB Hard Disk Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项

UEFI USB CDROM/DVD Drive BBS Priorities界面如 [图 3-105](#)所示。具体参数如 [表 3-97](#)所示。

图3-105 UEFI USB CDROM/DVD Drive BBS Priorities 界面

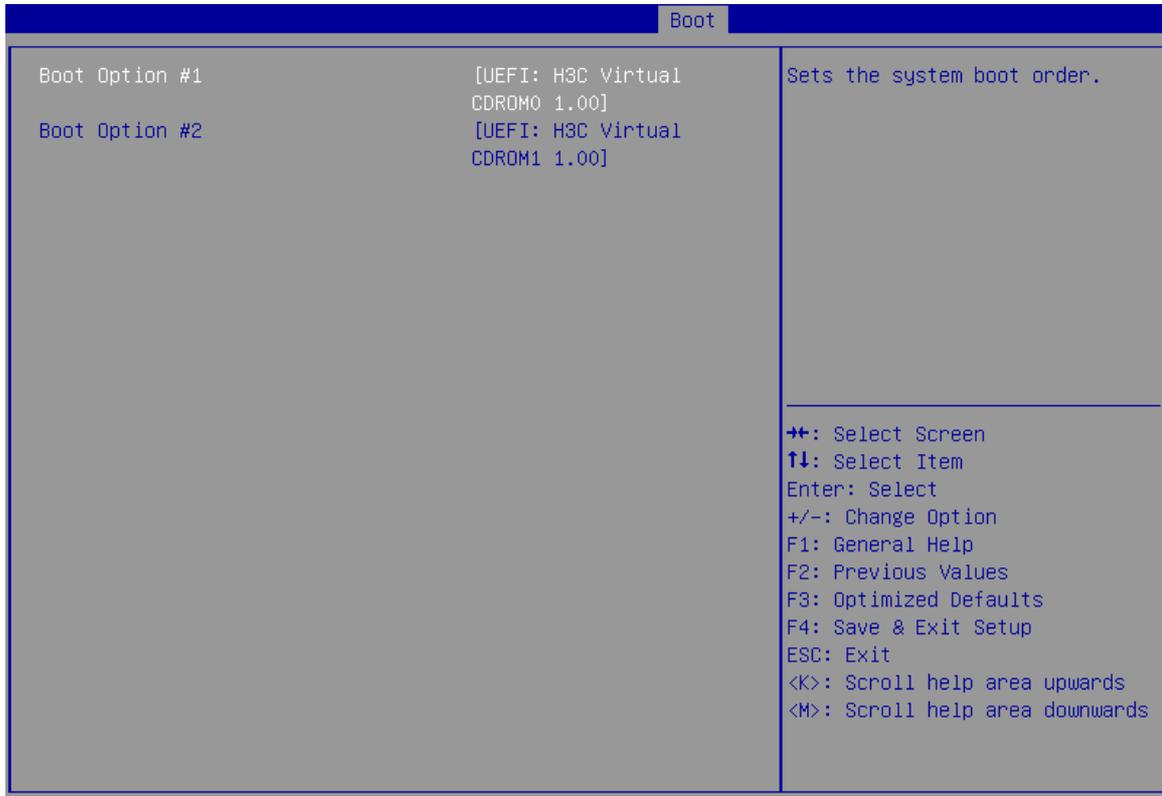


表3-97 UEFI USB CDROM/DVD Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项
Boot Option #2	第2启动选项

UEFI USB Key Drive BBS Priorities界面如 [图 3-106](#) 所示。具体参数如 [表 3-98](#) 所示。

图3-106 UEFI USB Key Drive BBS Priorities 界面



表3-98 UEFI USB Key Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项

UEFI USB Floppy Drive BBS Priorities界面如 [图 3-107](#)所示。具体参数如 [表 3-99](#)所示。

图3-107 UEFI USB Floppy Drive BBS Priorities 界面



表3-99 UEFI USB Floppy Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项

UEFI Network Drive BBS Priorities界面如 [图 3-108](#) 所示。具体参数如 [表 3-100](#) 所示。

图3-108 UEFI Network Drive BBS Priorities 界面

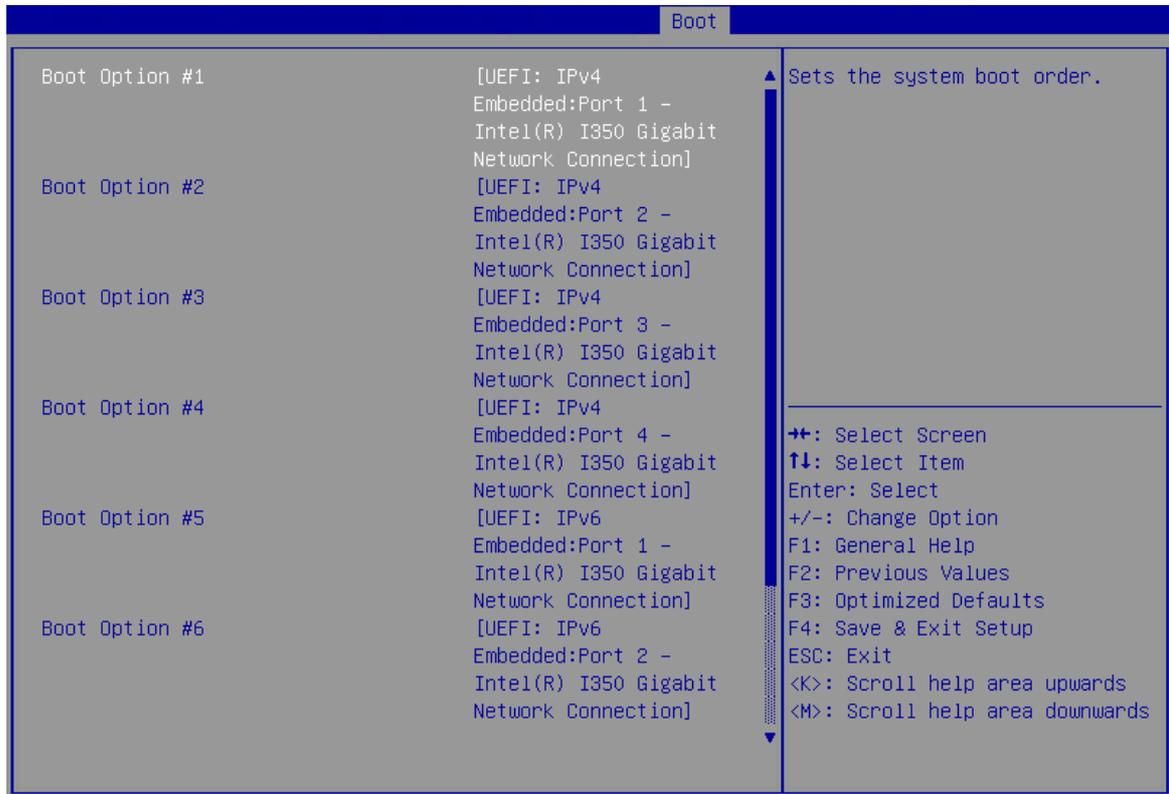


表3-100 UEFI Network Drive BBS Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项
Boot Option #2	第2启动选项
Boot Option #3	第3启动选项
Boot Option #4	第4启动选项
Boot Option #5	第5启动选项
Boot Option #6	第6启动选项
Boot Option #7	第7启动选项
Boot Option #8	第8启动选项

UEFI Application Boot Priorities界面如 [图 3-109](#) 所示。具体参数如 [表 3-101](#) 所示。

图3-109 UEFI Application Boot Priorities 界面

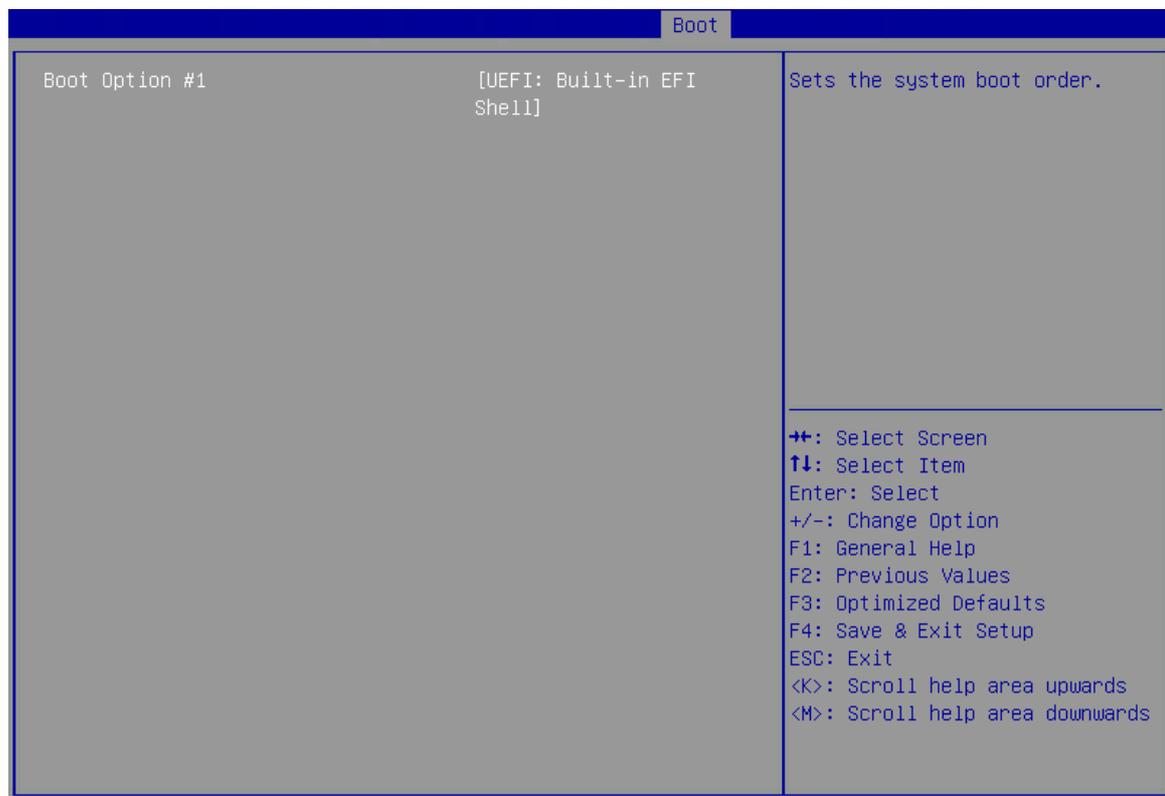


表3-101 UEFI Application Boot Priorities 界面参数

参数	功能说明
Boot Option #1	第1启动选项

## 3.8 Save & Exit界面

介绍通过 Save & Exit 界面，可以对 BIOS 参数修改及退出功能进行控制。

Save & Exit界面如 [图 3-110](#) 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 3-102](#) 所示。

图3-110 Save & Exit 界面

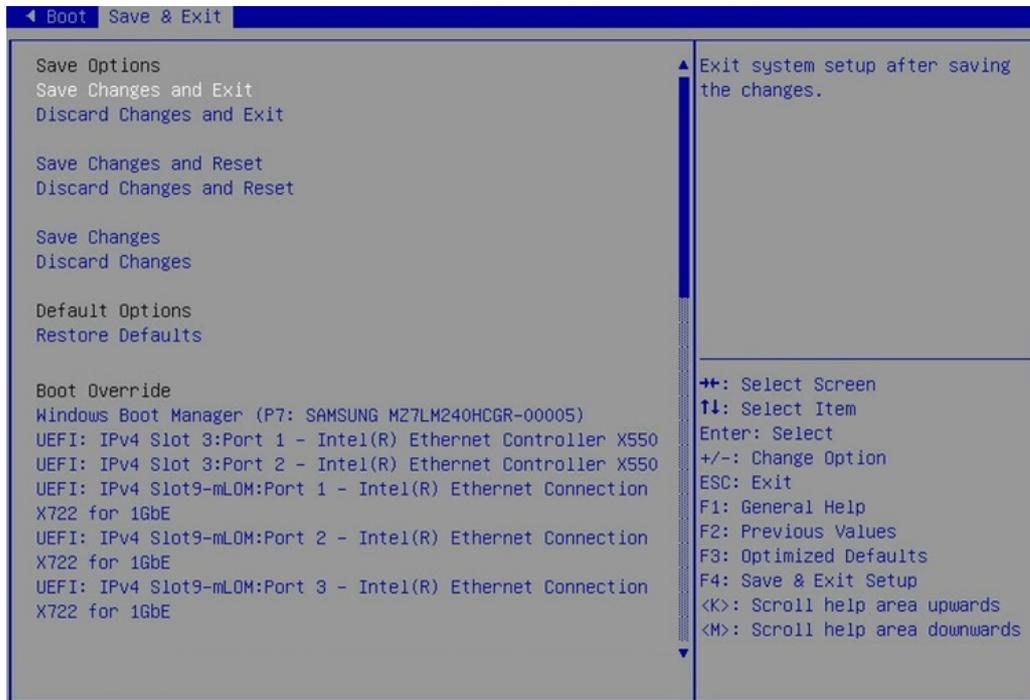


表3-102 Save & Exit 界面参数

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
<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2-2</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 3-110</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>

界面参数	功能说明
UEFI: IPv4 Slot9-mLOM: Port 1 – Intel(R) Ethernet Connection X722 for 1GbE (UEFI启动模式) / IBA 40G Slot 3D00 v1060 (Legacy启动模式)	mLOM卡的端口1与IPv4 PXE服务器相连时，您可以选择从该启动项启动。
UEFI: IPv4 Slot9-mLOM: Port 2 – Intel(R) Ethernet Connection X722 for 1GbE (UEFI启动模式) / IBA 40G Slot 3D00 v1060 (Legacy启动模式)	mLOM卡的端口2与IPv4 PXE服务器相连时，您可以选择从该启动项启动。
UEFI: IPv4 Slot9-mLOM: Port 3 – Intel(R) Ethernet Connection X722 for 1GbE (UEFI启动模式) / IBA 40G Slot 3D00 v1060 (Legacy启动模式)	mLOM卡的端口3与IPv4 PXE服务器相连时，您可以选择从该启动项启动。
UEFI: IPv4 Slot9-mLOM: Port 4 – Intel(R) Ethernet Connection X722 for 1GbE (UEFI启动模式) / IBA 40G Slot 3D00 v1060 (Legacy启动模式)	mLOM卡的端口4与IPv4 PXE服务器相连时，您可以选择从该启动项启动。
UEFI: IPv6 Slot9-mLOM: Port 1 – Intel(R) Ethernet Connection X722 for 1GbE: Port 1 – Intel(R) I350 Gigabit Network Connection	UEFI启动模式下，从mLOM卡的端口1启动。当mLOM卡的端口1与IPv6 PXE服务器相连时，您可以选择从该启动项启动。仅UEFI启动模式下显示该启动项。
UEFI: IPv6 Embedded: Port 2 – Intel(R) I350 Gigabit Network Connection	UEFI启动模式下，从mLOM卡的端口2启动。当mLOM卡的端口2与IPv6 PXE服务器相连时，您可以选择从该启动项启动。仅UEFI启动模式下显示该启动项。
UEFI: IPv6 Embedded: Port 3 – Intel(R) I350 Gigabit Network Connection	UEFI启动模式下，从mLOM卡的端口3启动。当mLOM卡的端口3与IPv6 PXE服务器相连时，您可以选择从该启动项启动。仅UEFI启动模式下显示该启动项。
UEFI: IPv6 Embedded: Port 4 – Intel(R) I350 Gigabit Network Connection	UEFI启动模式下，从mLOM卡的端口4启动。当mLOM卡的端口4与IPv6 PXE服务器相连时，您可以选择从该启动项启动。仅UEFI启动模式下显示该启动项。

### 说明

Legacy启动模式下，当服务器连接多个同一类的启动项时，本文以连接两个USB CD/DVD举例。Boot界面的Fixed Boot Order Priorities栏及Save & Exit界面的Boot Override栏仅显示USB CDROM/DVD Drive BBS Priorities界面的第一启动项。如果您需要服务器从第二个启动项启动，此时请将该启动项设置为第一启动项，具体方法与设置服务器启动顺序的方法类似。USB CDROM/DVD Drive BBS Priorities界面如 [图 3-105](#) 所示。

# 4 SATA sSATA端口与背板槽位的对应关系

## 4.1 H3C UniServer R4900 G3 PCH SATA sSATA相关硬盘背板配置端口

表4-1 H3C UniServer R4900 G3 8LFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号为SATA端口 0~7，背板槽位对应为槽位0~7
配置二	Mezz槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe槽位2（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	PCIe槽位6（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-2 H3C UniServer R4900 G3 8LFF HDD+4LFF NVMe 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+PCIe槽位2（NVMe 4端口适配卡）	PCH Mini SAS J11逻辑序号为SATA端口 0~7，背板槽位对应为槽位0~7
配置二	Mezz槽位（存储适配卡）+PCIe 槽位2（NVMe4端口适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe槽位6（存储适配卡）+PCIe 槽位5（NVMe 4端口适配卡）	未使用PCH SATA sSATA端口，不显示

表4-3 H3C UniServer R4900 G3 8SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号为SATA端口 0~7，背板槽位对应为槽位0~7
配置二	Mezz槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe槽位2（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	PCIe槽位6（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-4 H3C UniServer R4900 G3 8SFF HDD+8SFF NVMe 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+PCIe 槽位2（NVMe 8端口适配卡）	底板PCH Mini SAS J11逻辑序号为SATA端口 0~7，背板槽位对应为槽位0~7
配置二	底板PCH Mini SAS J11+PCIe 槽位5（NVMe 4端口适配卡）+PCIe 槽位2（NVMe 4端口适配卡）	底板PCH Mini SAS J11逻辑序号为SATA端口 0~7，背板槽位对应为槽位0~7

配置	硬盘数据线缆	说明
配置三	Mezz 槽位（存储适配卡）+PCIe 槽位5（NVMe 4端口适配卡）+PCIe 槽位2（NVMe 4端口适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	Mezz 槽位（存储适配卡）+PCIe 槽位2（NVMe 8端口适配卡）	未使用PCH SATA sSATA端口，不显示
配置五	PCIe槽位6（存储适配卡）+PCIe 槽位2（NVMe 8端口适配卡）	未使用PCH SATA sSATA端口，不显示

## 4.2 H3C UniServer R4700 G3 PCH SATA sSATA相关硬盘背板配置端口

表4-5 H3C UniServer R4700 G3 4LFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~3对应背板槽位号0~3
配置二	Mezz槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-6 H3C UniServer R4700 G3 4LFF HDD+ 2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~3接4LFF背板，对应背板槽位号0~3；逻辑序号SATA端口4~5接后部2SFF背板，对应背板槽位号4~5
配置二	Mezz槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-7 H3C UniServer R4700 G3 4SFF NVMe+4SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+PCIe槽位1（NVMe 4端口适配卡）	底板PCH Mini SAS J11逻辑序号SATA端口0~3接4SFF HDD部分，对应槽位号4~7
配置二	Mezz槽位（存储适配卡）+PCIe槽位1（NVMe 4端口适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe槽位1（存储适配卡）+ PCIe槽位2（NVMe 4端口适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	前部LP 槽位（存储适配卡）+ PCIe槽位1（NVMe 4端口适配卡）	未使用PCH SATA sSATA端口，不显示

表4-8 H3C UniServer R4700 G3 8SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号为SATA端口0~7，背板槽位对应为槽位0~7
配置二	Mezz槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe槽位1（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	前部LP槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-9 H3C UniServer R4700 G3 8SFF HDD+2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	Mezz 槽位（存储适配卡）+底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~1接2SFF HDD部分，背板槽位对应为槽位8~9
配置二	PCIe 槽位1（存储适配卡）+底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~1接2SFF HDD部分，背板槽位对应为槽位8~9

表4-10 H3C UniServer R4700 G3 8SFF NVME+2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	PCIe槽位1（NVMe 8端口适配卡）+底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~1接2SFF HDD部分，背板槽位对应为槽位8~9
配置二	PCIe槽位1（NVMe 4端口适配卡）+PCIe 槽位2（NVMe 4端口适配卡）+底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~1接2SFF HDD部分，背板槽位对应为槽位8~9

## 4.3 H3C UniServer R2900 G3 PCH SATA sSATA相关硬盘背板配置端口

表4-11 H3C UniServer R2900 G3 8LFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号为SATA端口0~7，背板槽位对应为槽位0~7
配置二	Mezz 槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe 槽位2（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	PCIe 槽位6（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-12 H3C UniServer R2900 G3 12LFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS HD J12+J11	底板PCH Mini SAS J11逻辑序号为SATA端口0~7，背板槽位对应为槽位0~7； 底板PCH Mini SAS J12逻辑序号为sSATA端口2~5，背板槽位对应为槽位8~11

表4-13 H3C UniServer R2900 G3 12LFF HDD+2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS HD J12+J11+7PIN SATA	底板PCH Mini SAS J11逻辑序号为SATA端口0~7，背板槽位对应为槽位0~7； 底板PCH Mini SAS J12逻辑序号为sSATA端口2~5，背板槽位对应为槽位8~11； 底板PCH 7PIN SATA逻辑序号为sSATA端口0~1，背板槽位对应为槽位28~29；

表4-14 H3C UniServer R2900 G3 8LFF HDD+4LFF NVMe 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+ PCIe 槽位2(NVMe 4端口适配卡)	8LFF HDD部分接底板PCH Mini SAS J11逻辑序号为SATA端口0~7，背板槽位对应为槽位 0~7
配置二	Mezz 槽位(存储适配卡)+ PCIe 槽位2(NVMe 4端口适配卡)	未使用PCH SATA sSATA端口，不显示
配置三	PCIe 槽位6(存储适配卡)+ PCIe 槽位5(NVMe 4端口适配卡)	未使用PCH SATA sSATA端口，不显示

表4-15 H3C UniServer R2900 G3 8SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号为SATA端口 0~7，背板槽位对应为槽位 0~7
配置二	Mezz 槽位(存储适配卡)	未使用PCH SATA sSATA端口，不显示
配置三	PCIe 槽位2(存储适配卡)	未使用PCH SATA sSATA端口，不显示
配置四	PCIe 槽位6(存储适配卡)	未使用PCH SATA sSATA端口，不显示

表4-16 H3C UniServer R2900 G3 8SFF HDD+8SFF NVMe 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+PCIe 槽位2 (NVMe 8 端口适配卡)	底板PCH Mini SAS J11逻辑序号为SATA端口0~7, 背板槽位对应为槽位 0~7
配置二	底板PCH Mini SAS J11+PCIe 槽位5 (NVMe 4 端口适配卡) +PCIe 槽位2 (NVMe 4端口适配卡)	底板PCH Mini SAS J11逻辑序号为SATA端口0~7, 背板槽位对应为槽位 0~7
配置三	Mezz 槽位 (存储适配卡)+PCIe 槽位5 (NVMe 4端口适配卡) +PCIe 槽位2 (NVMe 4端口适配卡)	未使用PCH SATA sSATA端口, 不显示
配置四	Mezz 槽位 (存储适配卡)+PCIe 槽位2 (NVMe 8端口适配卡)	未使用PCH SATA sSATA端口, 不显示
配置五	PCIe 槽位6 (存储适配卡)+PCIe 槽位5 (NVMe 8端口适配卡)	未使用PCH SATA sSATA端口, 不显示

## 4.4 H3C UniServer R2700 G3 PCH SATA sSATA相关硬盘背板配置端口

表4-17 H3C UniServer R2700 G3 4LFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS HD J11	底板PCH Mini SAS J11逻辑序号SATA端口0~3对应背板槽位号0~3
配置二	Mezz 槽位 (存储适配卡)	未使用PCH SATA sSATA端口, 不显示

表4-18 H3C UniServer R2700 G3 4LFF HDD+2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS HD J11	底板PCH Mini SAS J11逻辑序号SATA端口0~3接4LFF背板, 对应背板槽位号0~3; 逻辑序号SATA端口4~5接后部2SFF背板, 对应背板槽位号4~5
配置二	Mezz 槽位 (存储适配卡)	未使用PCH SATA sSATA端口, 不显示

表4-19 H3C UniServer R2700 G3 4SFF NVMe+4SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+ PCIe 槽位1 (NVMe 4端口适配卡)	底板PCH Mini SAS J11逻辑序号SATA端口0~3接4SFF HDD部分, 背板槽位对应为槽位4~7
配置二	Mezz 槽位 (存储适配卡)+ PCIe 槽位1 (NVMe 4端口适配卡)	未使用PCH SATA sSATA端口, 不显示
配置三	PCIe 槽位1 (存储适配卡)+ PCIe 槽位2 (NVMe 4端口适配卡)	未使用PCH SATA sSATA端口, 不显示

配置	硬盘数据线缆	说明
配置四	前部LP 槽位（存储适配卡）+ PCIe 槽位1（NVMe 4端口适配卡）	未使用PCH SATA sSATA端口，不显示

表4-20 H3C UniServer R2700 G3 8SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11	底板PCH Mini SAS J11逻辑序号SATA端口0~7，背板槽位对应为槽位 0~7
配置二	Mezz 槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置三	PCIe 槽位1（存储适配卡）	未使用PCH SATA sSATA端口，不显示
配置四	前部LP 槽位（存储适配卡）	未使用PCH SATA sSATA端口，不显示

表4-21 H3C UniServer R2700 G3 8SFF HDD+2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS HD J11+底板PCH Mini SAS HD J12	底板PCH Mini SAS J11逻辑序号SATA端口0~7接8SFF HDD部分，背板槽位对应为槽位0~7； 底板PCH Mini SAS J12逻辑序号sSATA端口2~3接2SFF HDD部分，背板槽位对应为槽位8~9
配置二	Mezz 槽位(存储适配卡)+ 底板PCH Mini SAS HD J12	底板PCH Mini SAS J12逻辑序号sSATA端口2~3接2SFF HDD部分，背板槽位对应为槽位8~9
配置三	PCIe 槽位1（存储适配卡）+ 底板PCH Mini SAS HD J12	底板PCH Mini SAS J12逻辑序号sSATA端口2~3接2SFF HDD部分，背板槽位对应为槽位8~9

表4-22 H3C UniServer R2700 G3 8SFF NVMe+2SFF HDD 机型

配置	硬盘数据线缆	说明
配置一	PCIe 槽位1（NVMe 8端口适配卡）+底板PCH Mini SAS HD J12	底板PCH Mini SAS J12逻辑序号sSATA端口2~3接2SFF HDD部分，背板槽位对应为槽位8~9
配置二	PCIe 槽位1（NVMe 4端口适配卡）+ PCIe 槽位2（NVMe 4端口适配卡）+底板PCH Mini SAS HD J12	底板PCH Mini SAS J12逻辑序号sSATA端口2~3接2SFF HDD部分，背板槽位对应为槽位8~9

# 5 缩略语

表5-1 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
AES	Advanced Encryption Standard	高级加密标准
AHCI	Advanced Host Controller Interface	高级主机控制器接口
APIC	Advanced Programmable Interrupt Controller	高级可编程中断控制器
<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
<b>E</b>		
E2E	End To End	端到端
ECC	Error Checking and Correcting	差错校验纠正
EFI	Extensible Firmware Interface	可扩展固件接口
EHCI	Enhanced Host Controller Interface	增强型主机控制器接口
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	H3C Device Management	H3C设备管理

缩略语	英文解释	中文解释
<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
IMC	Integrated Memory Controller	集成内存控制器
IRQ	Interrupt Request	中断请求
<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	网络接口控制器
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
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
RMT	Rank Margin Tool	内存裕度测试工具
ROM	Read-Only Memory	只读存储器

缩略语	英文解释	中文解释
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
SPD	Serial Presence Detect	串行存在检查
SR-IOV	Single-Root I/O Virtualization	单路I/O虚拟化
<b>T</b>		
TCG	Trusted Computing Group	可信计算组织
TDP	Thermal Design Power	热设计功耗
TPM	Trusted Platform Module	可信平台模块
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
VMD	Volume Management Device	卷管理设备
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