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

2. 图形界面格式约定

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

3. 各类标志

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

▲ 警告	该标志后的注释需给予格外关注,不当的操作可能会对人身造成伤害。	
1 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。	
쭏 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。
ROUTER	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。
A CONTRACT	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。
T •)	该图标及其相关描述文字代表无线终结单元。
(T)	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。
BroBlack	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插 卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

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

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

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

感谢您的反馈,让我们做得更好!

1 B I	OS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	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	2-19
	2.11 配置RAID2	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 Advanced界面 ······ 3.2.1 Intel(R) virtual RAID on CPU界面 ······	3-3 3-5
	3.2 Advanced界面 ······ 3.2.1 Intel(R) virtual RAID on CPU界面 ······· 3.2.2 Driver Health界面 ····································	3-3 3-5 -16
	 3.2 Advanced界面	3-3 3-5 3-16 3-17
	 3.2 Advanced界面 ····································	3-3 3-5 -16 -17
	 3.2 Advanced界面 ····································	3-3 3-5 -16 -17 -22
	 3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3.2.3 Trusted Computing界面 3.2.4 ACPI Settings界面 3.2.5 Serial Port Console Redirection界面 3.2.6 Slot x:Port x界面 	3-3 3-5 -16 -17 -22 -23 -23
	 3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3.2.3 Trusted Computing界面 3.2.4 ACPI Settings界面 3.2.5 Serial Port Console Redirection界面 3.2.6 Slot x:Port x界面 3.2.7 PCI Subsystem Settings界面 	3-3 3-5 -16 -17 -22 -23 -23 -27
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3.2.3 Trusted Computing界面 3.2.4 ACPI Settings界面 3.2.5 Serial Port Console Redirection界面 3.2.6 Slot x:Port x界面 3.2.7 PCI Subsystem Settings界面 3.2.8 Network Stack Configuration界面	3-3 3-5 -16 -17 -22 -23 -27 -30 -32
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.1 Intel(R) virtual RAID on CPU界面 3 3.2.2 Driver Health界面 3 3.2.3 Trusted Computing界面 3 3.2.4 ACPI Settings界面 3 3.2.5 Serial Port Console Redirection界面 3 3.2.6 Slot x:Port x界面 3 3.2.7 PCI Subsystem Settings界面 3 3.2.8 Network Stack Configuration界面 3 3.2.9 CSM Configuration界面 3	3-3 3-5 -16 -17 -22 -23 -27 -30 -32 -33
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3.2.3 Trusted Computing界面 3.2.3 Trusted Computing界面 3.2.4 ACPI Settings界面 3.2.5 Serial Port Console Redirection界面 3.2.6 Slot x:Port x界面 3.2.7 PCI Subsystem Settings界面 3.2.8 Network Stack Configuration界面 3.2.9 CSM Configuration界面 3.2.10 NVMe Configuration界面	3-3 3-5 -16 -17 -22 -23 -23 -30 -32 -32 -33 -34
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3.2.3 Trusted Computing界面 3.2.3 Trusted Computing界面 3.2.4 ACPI Settings界面 3.2.5 Serial Port Console Redirection界面 3.2.6 Slot x:Port x界面 3.2.7 PCI Subsystem Settings界面 3.2.8 Network Stack Configuration界面 3.2.9 CSM Configuration界面 3.2.10 NVMe Configuration界面 3.2.11 USB Configuration界面	3-3 3-5 3-16 3-17 3-22 3-23 3-24 3-33 3-34 3-34
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3 3.2.3 Trusted Computing界面 3 3.2.4 ACPI Settings界面 3 3.2.5 Serial Port Console Redirection界面 3 3.2.6 Slot x:Port x界面 3 3.2.7 PCI Subsystem Settings界面 3 3.2.8 Network Stack Configuration界面 3 3.2.10 NVMe Configuration界面 3 3.2.11 USB Configuration界面 3 3.3 Platform Configuration界面 3	3-3 3-5 -16 -17 -22 -23 -23 -27 -30 -32 -33 -34 -34 -36 -38
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3.2.3 Trusted Computing界面 3.2.3 Trusted Computing界面 3.2.4 ACPI Settings界面 3.2.5 Serial Port Console Redirection界面 3.2.6 Slot x:Port x界面 3.2.7 PCI Subsystem Settings界面 3.2.8 Network Stack Configuration界面 3.2.10 NVMe Configuration界面 3.2.11 USB Configuration界面 3.3.3 Platform Configuration界面 3.3.1 PCH Configuration界面	3-3 3-5 -16 -17 -22 -23 -23 -27 -30 -32 -32 -33 -34 -36 -38 -38
	3.2 Advanced界面 3.2.1 Intel(R) virtual RAID on CPU界面 3.2.2 Driver Health界面 3 3.2.3 Trusted Computing界面 3 3.2.4 ACPI Settings界面 3 3.2.5 Serial Port Console Redirection界面 3 3.2.6 Slot x:Port x界面 3 3.2.7 PCI Subsystem Settings界面 3 3.2.8 Network Stack Configuration界面 3 3.2.9 CSM Configuration界面 3 3.2.10 NVMe Configuration界面 3 3.2.11 USB Configuration界面 3 3.3.2 Platform Configuration界面 3 3.3.1 PCH Configuration界面 3 3.3.2 Miscellaneous Configuration界面 3	3-3 3-5 -16 -17 -22 -23 -23 -27 -30 -32 -33 -34 -36 -38 -38 -38 -39 -34

3.3.4 Runtime Error Logging界面
3.4 Socket Configuration界面
3.4.1 Processor Configuration界面
3.4.2 Common RefCode Configuration界面
3.4.3 UPI Configuration界面
3.4.4 Memory Configuration界面
3.4.5 IIO Configuration界面
3.4.6 Advanced Power Management Configuration界面
3.5 Server Management界面
3.6 Security界面3-110
3.7 Boot界面
3.8 Save & Exit界面
4 SATA sSATA端口与背板槽位的对应关系4-1
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
5 缩略语

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

(应用进程1) (应用进程2) (应用进程3) ()
操作系统	
BIOS	
硬件	

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



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

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。

🕑 说明

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。



- 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

—Enter Password———	

(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

Main Advanced Platform Confi	guration Socket Configuration	Server Management Security
BIOS Information		▲ Choose the system default
BIOS Vendor	American Megatrends	1anguage
Core Version	5.12	
Compliancy	UEFI 2.5; PI 1.4	
Project Name	C35	
Product Name	UniServer R2700 G3	
BIOS Version	1.00.46 V100R001B01D046	
System Uuid	496118D8-1D74-11B3-03D4-	
	74EACB5A5D7C	
Asset Tag	01234567890123456789	
Build Date and Time	01/17/2019 03:12:05	
Access Level	Administrator	
Platform Information		++: Select Screen
Platform	TypeNeonCityEPRP	†↓: Select Item
Processor	50654 – SKX MO	Enter: Select
PCH	LBG QS/PRQ - 1G - SO	+/-: Change Option
RC Revision	155.R25	ESC: Exit
		F1: General Help
Memory Information		F2: Previous Values
Total Memory	32768 MB	F3: Optimized Defaults
Current Memory Frequency	2400 MHz	F4: Save & Exit Setup
		<pre><k>: Scroll help area upwards</k></pre>
System Language	[English]	<pre><m>: Scroll help area downwards</m></pre>
		×

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></k>	向上滚动界面右上角的帮助信息
<m></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 <u>3.4.1_Processor Configuration界面</u>。

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

Aptio Setup Utilit	y – Copyright (C) 2017 America Socket Configuration	n Megatrends, Inc.
Processor Configuration		Change Per-Socket Settings
 Per-Socket Configuration Processor BSP Revision 	50654 - SKX U0	
Processor ID Processor Frequency Processor Max Ratio	00050654* 00050654 2.200GHz 2.200GHz 2.200GHz 2.200GHz	
Processor Min Ratio Processor TDP Microcode Revision	0.800GHz 0.800GHz 85W 85W 02000030 02000030	
L1 Cache RAM L2 Cache RAM L3 Cache RAM	640KB 640KB 10240KB 10240KB 14080KB 14080KB	++: Select Screen
Processor 1 Version Processor 2 Version	Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz Intel(R) Xeon(R) Silver	T∔: Select Item Enter: Select +/-: Change Option
Hyper-Threading [ALL] Check CPU BIST Result Enable Intel(R) TXT VMX Enable SMX DEBUG INTERFACE	(Enabled) [Enabled] [Disabled] [Enabled] [Disabled] [Disabled] [Enabled]	F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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 <u>3.4.4 Memory Configuration界面</u>。

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

EnaIntegrated Memory Controller (IMC)Total Memory32768 MBCurrent Memory Frequency2666 MHzIMC ConfigurationEnforce POR[Auto]Memory FrequencyIAuto]Rank Margin Tool[Auto]Data Scrambling for DDR4[Auto]WR CRC Feature Control[Auto]USTOM Refresh Enable[Disabled]C/A Parity Enable[Auto]Memory TopologyF1:Memory RAS ConfigurationF3:	ble/Disable IMC Select Screen Select Item er: Select : Change Option : Exit General Help Previous Values Optimized Defaults Save & Exit Setup

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

Platform Configuration		
PCH SATA Configuration		 Identify the SATA port is connected to solid state drive or hard disk drive
SATA Controller	[Enabled]	
Configure SATA As	[AHCI]	
SATA Test Mode	[Disabled]	
SATA Port O	[Not Installed]	
Port O	[Enabled]	
SATA Port 1	[Not Installed]	
Port 1	[Enabled]	
SATA Port 2	[Not Installed]	
Port 2	[Enabled]	
SATA Port 3	[Not Installed]	++: Select Screen
Port 3	[Enabled]	↑↓: Select Item
SATA Port 4	VK0240GDJXU – 240.0 GB	Enter: Select
	(Slot 4)	+/-: Change Option
Port 4	[Enabled]	ESC: Exit
SATA Port 5	INTEL SSDSC2BB240G6 -	F1: General Help
N.Z. 877. 97	240.0 GB (Slot 5)	F2: Previous Values
Port 5	[Enabled]	F3: Optimized Defaults
SATA Port 6	ST1000NX0313 - 1000.2	F4: Save & Exit Setup
	GB (Slot 6)	K>: Scroll help area upwards
Port 6	[Enabled]	<m>: Scroll help area downwards</m>
SATA Port 7	[Not Installed]	•

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

		Server Management
HDM Network Configuration жжжжжжжжжжжжжжжжжж Configure IPV4 Support жжжжжжжжжжжжжжжжжжж		Enable/Disable Bond Mode
Bond Mode Setting	[Disabled]	
HDM Shared Network Port		
Configuration Address Source	[Unspecified]	
Current Configuration Address Source	DynamicAddressHdmDhcp	
Station IP Address	0.0.0	
Subnet Mask	0.0.0	
Station MAC address	00-00-00-00-00	
Router IP Address	0.0.0.0	↔+: Select Screen
Router MAC Address	00-00-00-00-00	↑↓: Select Item
		Enter: Select
HDM Dedicated Network Port		+/-: Change Option
Configuration Address Source	[Unspecified]	ESC: Exit
Current Configuration Address	StaticAddress	F1: General Help
Source		F2: Previous Values
Station IP Address	192.168.1.2	F3: Optimized Defaults
Subnet Mask	255.255.255.0	F4: Save & Exit Setup
Station MAC address	00-00-00-00-00	<k>: Scroll help area upwards</k>
Router IP Address	0.0.0	<m>: Scroll help area downwards</m>
Router MAC Address	00-00-00-00-00	

2.6 设置HDM网络信息



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

- 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

		Server Management
HDM Network Configuration жжжжжжжжжжжжжжжж Configure IPV4 Support жжжжжжжжжжжжжжжж		Select to configure LAN channel parameters statically or dynamically(by BIOS or HDM). Unspecified option will
Bond Mode Setting	[Disabled]	not modify any HDM network parameters during BIOS phase
HUM Shared Network Port		
Configuration Address Source	[Unspec1fied]	
Source	рупатіснааressнатрпср	
Station IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Station MAC address	00-00-00-00-00	
Router IP Address	0.0.0.0	++: Select Screen
Router MAC Address	00-00-00-00-00	↑↓: Select Item
		Enter: Select
HDM Dedicated Network Port		+/-: Change Option
Configuration Address Source	[Unspecified]	ESC: Exit
Current Configuration Address	StaticAddress	F1: General Help
Source		F2: Previous Values
Station IP Address	192.168.1.2	F3: Optimized Defaults
Subnet Mask	255.255.255.0	F4: Save & Exit Setup
Station MAC address	00-00-00-00-00	<k>: Scroll help area upwards</k>
Router IP Address	0.0.0	<pre><m>: Scroll help area downwards</m></pre>
Router MAC Address	00-00-00-00-00	

- (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 M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

		Server Management
HDM Network Configuration жжжжжжжжжжжжжжжжж Configure IPV4 Support жжжжжжжжжжжжжжжж Bond Mode Setting	[Disabled]	Select to configure LAN channel parameters statically or dynamically(by BIOS or HDM). Unspecified option will not modify any HDM network parameters during BIOS phase
HDM Shared Network Port Configuration Address Source Current Configuration Address Source	[Unspecified] DynamicAddressHdmDhcp	
Station IP Address Subnet Mask Station MAC address Sta	 Configuration Address Source pecified tic 	
Router IP Address Dyn Router MAC Address	amicHdmDhcp	Select Screen Select Item r: Select
HDM Dedicated Network Port		+/-: Change Option
Configuration Address Source	[Unspecified]	ESC: Exit
Current Configuration Address Source	StaticAddress	F1: General Help F2: Previous Values
Station IP Address	192.168.1.2	F3: Optimized Defaults
Subnet Mask	255.255.255.0	F4: Save & Exit Setup
Station MAC address	00-00-00-00-00	<k>: Scroll help area upwards</k>
Router IP Address	0.0.0.0	<m>: Scroll help area downwards</m>
Router MAC Address	00-00-00-00-00-00	

(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

Main Advanced Platform (Configuration Socket Configuration)Server Management Security 🗾 🕨
Password Description		Set administrator password
If only the administrator's limits access to Setup and Setup. If only the user's password password and must be entered Setup the user will have ad When both password are set have the rights according to the same, user will have adh The password length must be Minimum Length	s password is set,then this only is only asked for when entering d is set, then this is a power on ed to boot or enter Setup. In Mministrator rights. if they are different,user will to the login password,if they are ministrator rights. e in the following range:	
Maximum Length	20	↔: Select Screen
20 10 10 10 10 10 10 10 10 10 10 10 10 10		†↓: Select Item
Administrator Password		Enter: Select
User Password		+/-: Change Option ESC: Exit F1: General Help F2: Previous Values
HDD Security Configuration		F3: Optimized Defaults
P3:SAMSUNG MZ7LM240HCGR-000	005	F4: Save & Exit Setup <k>: Scroll help area upwards</k>
▶ Secure Boot Menu		<m>: Scroll help area downwards</m>

(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。



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

Main Advanced Platform Configuration	Socket Configuration	Server Management S	ecurity 📃 🕨
Password Description		Set administrator p	assword
If only the administrator's password is	set,then this only		
limits access to Setup and is only asked	d for when entering		
Setup. If aply the year's receiverd is set, the	this is a nowar or		
nassword and must be entered to boot or	enter Setun. In		
Setup the user will have administrator (rights.		
When both password are set, if they are (different,user will		
have the rights according to the login ;	bassword,if they are		
the same, user will have administrator r.	ights.		
Minimum Length	kate New Passworu		
Maximum Length		++: Select Screen	
		1↓: Select Item	
Administrator Password		Enter: Select	
User Password		+/-: Change Option	
		ESU: EXIT	
		F2: Previous Values	
HDD Security Configuration:		F3: Optimized Defau	lts
P3:SAMSUNG MZ7LM240HCGR-00005		F4: Save & Exit Set	up
		<k>: Scroll help an</k>	ea upwards
Secure Boot Menu		<pre><m>: Scroll help ar</m></pre>	ea downwards

(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

Main Advanced Platform	Configuration Socket Configuration	Server Management Security
Password Description		Set administrator password
If only the administrator limits access to Setup ar Setup. If only the user's passwo password and must be ente Setup the user will have When both password are se have the rights according the same,user will have a	's password is set,then this only ad is only asked for when entering ard is set, then this is a power on ered to boot or enter Setup. In administrator rights. et,if they are different,user will s to the login password,if they are administrator rights.	
Minimum Length	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
Maximum Length		++: Select Screen
Administrator Password		Enter: Select
User Password		+/-: Change Option
		ESC: Exit
		F1: General nerp F2: Previous Values
HDD Security Configuratio	in:	F3: Optimized Defaults
▶ P3:SAMSUNG MZ7LM240HCGR-C	0005	F4: Save & Exit Setup
		<k>: Scroll help area upwards</k>
Secure Boot Menu		<m>: Scroll help area downwards</m>

- (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

Main Advanced Platform Configuration	ocket Configuration Server Management Security
Password Description	Set user password
If only the administrator's password is so limits access to Setup and is only asked Setup. If only the user's password is set, then a password and must be entered to boot or en Setup the user will have administrator rig When both password are set, if they are di- have the rights according to the login pa- the same, user will have administrator rig The password length must be in the follow Minimum Length	t,then this only or when entering his is a power on ter Setup. In hts. ferent,user will sword,if they are ts. ng range:
Maximum Length 20	↔+: Select Screen
	↑↓: Select Item
Administrator Password	Enter: Select
User Password	+/−: Change Option ESC: Exit F1: General Help F2: Previous Values
HDD Security Configuration:	F3: Optimized Defaults
▶ P3:SAMSUNG MZ7LM240HCGR-00005	F4: Save & Exit Setup <k>: Scroll help area upwards</k>
▶ Secure Boot Menu	<m>: Scroll help area downwards</m>

(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。



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

Main Advanced Platform Configuration Socket Configuration	Server Management Security 🗾 🕨
Password Description	Set user password
If only the administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. If only the user's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the user will have administrator rights. When both password are set, if they are different, user will have the rights according to the login password, if they are the same, user will have administrator rights. The password length must be in the <u>Create New Password</u>	
Minimum Length אאאאאאאאאאאאאאאאאאאאאאאאאאאאאאאאאאאא	→+: Select Screen ↑↓: Select Item
Administrator Password User Password	Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values
HDD Security Configuration: ▶ P3:SAMSUNG MZ7LM240HCGR-00005	F3: Optimized Defaults F4: Save & Exit Setup
▶ Secure Boot Menu	<k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

(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

Main Advanced Platform Configuration Socket Configuration	Server Management Security 🗾 🕨
Password Description	Set user password
If only the administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. If only the user's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the user will have administrator rights. When both password are set, if they are different, user will have the rights according to the login password, if they are the same, user will have administrator rights. The password length must be in the Confirm New Password	
Maximum Length	↔: Select Screen
Advision Decouvered	↑↓: Select Item
User Password	+/-: Change Option
	ESC: Exit
	F1: General Help
HDD Security Configuration:	F3: Optimized Defaults
P3:SAMSUNG MZ7LM240HCGR-00005	F4: Save & Exit Setup
	<k>: Scroll help area upwards</k>
▶ Secure Boot Menu	<m>: Scroll neip area downwards</m>

(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



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

	Main Advanced Platform Configura	tion Socket Configuration	Server Management	Security
	Password Description		Set administrator	password
	If only the administrator's passwor limits access to Setup and is only Setup. If only the user's password is set, password and must be entered to boo Setup the user will have administra When both password are set, if they have the rights according to the lo the same, user will have administrat The password length must be in the Minimum Length	d is set,then this only asked for when entering then this is a power on t or enter Setup. In tor rights. are different,user will gin password,if they are or rights. following range:		
	Maximum Length	20	++: Select Screen	
			↑↓: Select Item	
	Administrator Password		Enter: Select	
	User Password		+/-: Change Option	n
			ESC: Exit	
			F1: General Help	
	HDD Security Configuration:		F2: Previous value F3: Ontimized Def:	es aulte
	P3:SAMSUNG_M27LM240HCGR-00005		E4: Save & Exit S	etun
			<pre><k>: Scroll help ;</k></pre>	area upwards
Þ	Secure Boot Menu		<m>: Scroll help :</m>	area downwards
_				

(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

	Main Advanced Platform Configuration Socket Co	nfiguration Server Management Security
	Password Description	Set administrator password
	If only the administrator's password is set, then t	his only
	Setup.	CITCI THE
	If only the user's password is set, then this is a	a power on
	password and must be entered to boot or enter Setu	ıp. In
	When both password are set, if they are different.	ıser will
	have the rights according to the login password, if	they are
	the same,user will have administrator rights.	
	Ine password length must be in the Enter Current	
	Maximum Length	++: Select Screen
		↑↓: Select Item
	Administrator Password	Enter: Select
	user rassworu	ESC: Exit
		F1: General Help
		F2: Previous Values
	HDD Security Configuration:	F3: Optimized Defaults
┣	P3:SAMSUNG MZ7LM240HCGR-00005	F4: Save & Exit Setup
	Secure Boot Menu	<m>: Scroll help area downwards</m>

(11) 进入 图 2-18 所示界面,直接按Enter。

图2-18 清除管理员密码

Main Advanced Platform Configuration Socket Configuration	Server Management Security 🗾 🕨
Password Description	Set administrator password
If only the administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. If only the user's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the user will have administrator rights. When both password are set, if they are different, user will have the rights according to the login password, if they are the same, user will have administrator rights. The password length must be in the <u>Create New Password</u>	
Maximum Length	↔: Select Screen
Administrator Password	î∔: Select Item Enter: Select
User Password	+/-: Change Option ESC: Exit F1: General Help F2: Previous Values
HDD Security Configuration:	F3: Optimized Defaults
► P3:SAMSUNG MZ7LM240HCGR-00005	F4: Save & Exit Setup <k>: Scroll help area upwards</k>
▶ Secure Boot Menu	<m>: Scroll help area downwards</m>

(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

	Main Advanced Platform Configuration Sock	et Configuration	Server Management Security
Γ	Password Description		Set administrator password
	If only the administrator's password is set,t limits access to Setup and is only asked for	hen this only when entering	
	Setup.		
	If only the user's password is set, then this	is a power on	
	password and must be entered to boot or enter Setup the user will have administrator rights	Setup. In	
	When both password are set, if they are differ	ent,user will	
	have the rights according to t	RNING	
	the same,user will have admini	sword Continue?	
	Minimum Length	Sword, Sontinae,	
	Maximum Length		←: Select Screen
	Administrator Password	NO	↓: Select Item nter: Select
	User Password		/-: Change Option
			ESC: Exit
			F1: General Help F2: Previous Values
	HDD Security Configuration:		F3: Optimized Defaults
Þ	P3:SAMSUNG MZ7LM240HCGR-00005		F4: Save & Exit Setup
	Secure Boot Menu		<pre><k>: Scroll help area upwards </k></pre>
ľ			Chr. Scient help allea downwallus
-			

(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

	Main Advanced Platform Configurat	ion Socket Configuration	Server Management Security 🔹 🕨
	Asset Tag Build Date and Time	To be filled by O.E.M.To be filled by O.E.M.To be filled by O.E.M. 06/28/2017 15:59:18	Set the date. Use tab to switch between date elements.
	Access Level	Administrator	
	Platform Information		
	Platform	TypeNeonCityEPRP	
	Processor	50654 - SKX HO	
	PCH	LBG QS/PRQ - 1G - B1	
	RC Revision	137.R08	
	Memory Information		→+: Select Screen
	Total Memory	32768 MB	↑↓: Select Item
	Current Memory Frequency	2666 MHz	Enter: Select
			+/−: Change Option
	System Language	[English]	ESC: Exit
			F1: General Help
Þ	Modify Asset Tag		F2: Previous Values
			F3: Optimized Defaults
	System Date	[Fr1 07/07/2017]	F4: Save & Exit Setup
	System lime	[03:15:05]	<pre><k>: Scroll nelp area upwards </k></pre>
			Chr. Scroff help area downwards

- (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 <u>图 2-21</u>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

◄ Boot Save & Exit		
Boot Configuration Setup Prompt Timeout Bootup NumLock State Quiet Boot	1 [On] [Disabled]	▲ Select boot mode LEGACY/UEFI, CSM always enable in legacy mode
Boot mode select		
Fixed Boot Order Priorities		
Boot Option #1	[Hard Disk:CentOS	
Boot Option #2	Boot mode select -	
		++: Select Screen
	1GbE]	Enter: Select
Boot Option #3	[USB Hard Disk]	+/-: Change Option
Boot Option #4	[USB CD/DVD]	ESC: Exit
Boot Option #5	[USB Key]	F1: General Help
Boot Option #6	[USB Floppy]	F2: Previous Values
Boot Option #7	[CD/DVD]	F3: Optimized Defaults
Boot Option #8	[UEFI AP]	F4: Save & Exit Setup
		K>: Scroll help area upwards
▶ UEFI Hard Disk Drive BBS Priori	ties	<pre><m>: Scroll help area downwards</m></pre>
UEFI Network Drive BBS Prioriti	es	*

(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

🕑 说明

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 <u>2-22</u>所示,选择**Boot**页签,进入Boot页面。

图2-22 Boot 界面

◄ Boot Save & Exit		
Boot Configuration Setup Prompt Timeout Bootup NumLock State Quiet Boot	1 [On] [Disabled]	Sets the system boot order
Boot mode select	[UEFI]	
Fixed Boot Order Priorities		
Boot Option #1	[Hard Disk:CentOS (Slot10 Mezz HBA Drives 2)]	
Boot Option #2	[Network:UEFI: IPv4 Slot9-mLOM:Port 1 - Intel(R) Ethernet Connection X722 for 1GbE]	↔: Select Screen ↓: Select Item Enter: Select
Boot Option #3	[USB Hard Disk]	+/-: Change Option
Boot Option #4	[USB_CD/DVD]	ESC: Exit
Boot Uption #5	[USB Key]	F1: General Help
Boot Option #5		F2: Previous values
Boot Option #8	[UEET AP]	F4: Save & Exit Setun
	court in j	<k>: Scroll help area upwards</k>
• UEFI Hard Disk Drive BBS Priorities		<m>: Scroll help area downwards</m>
UEFI Network Drive BBS Priorities	••••	

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 <u>图 2-23</u>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

≺ Boot Save & Exit		
Boot Configuration Setup Prompt Timeout Bootup NumLock State Quiet Boot Boot mode select	1 [On] [Disabled] [UEFI]	Sets the system boot order
Fixed Boot Order Prioriti	Boot Option #1	
Boot Option #1	Hard Disk	
Boot Option #2	Network	
Boot Option #3	USB Hard Disk	
Boot Option #4	USB CD/DVD	
Boot Option #5	USB Key:UEFI: hp v220w 1100, Partition 1	
	USB Floppy	ect Screen
Boot Option #6	CD/DVD	ect Item
Boot Option #7	UEFI AP	Select
Boot Option #8	Disabled	ange Option
a constant and the second states of the		it
UEFI USB Key Drive BBS Pr.		eral Help
UEFI Application Boot Price	orities	F2: Previous Values
		F3: Uptimized Defaults
		F4: Save & Exit Setup
		<pre></pre>
		THY. SET UTT HETP al ca dominal us

(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

DUUL SAVE & EXIL	
Save Options Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Changes Discard Changes Default Options Restore Defaults	Exit system setup after saving the changes.
Restore Defaults Boot Override Windows Boot Manager (P7: SAMSUNG MZ7LM240HCGR-00005) UEFI: IPv4 Slot 3:Port 1 - Intel(R) Ethernet Controller X550 UEFI: IPv4 Slot9-mLOM:Port 1 - Intel(R) Ethernet Connection X722 for 1GbE UEFI: IPv4 Slot9-mLOM:Port 2 - Intel(R) Ethernet Connection X722 for 1GbE UEFI: IPv4 Slot9-mLOM:Port 3 - Intel(R) Ethernet Connection X722 for 1GbE	<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>



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

Main Advanced Platform Config	uration Socket Configuration	Server Management Security
BIOS Information		▲ Choose the system default
BIOS Vendor	American Megatrends	language
Core Version	5.12	
Compliancy	UEFI 2.5; PI 1.4	
Project Name	C35	
Product Name	UniServer R2700 G3	
BIOS Version	1.00.46 V100R001B01D046	
System Uuid	496118D8-1D74-11B3-03D4-	
	74EACB5A5D7C	
Asset Tag	01234567890123456789	
Build Date and Time	01/17/2019 03:12:05	
Access Level	Administrator	
Platform Information		++: Select Screen
Platform	TypeNeonCityEPRP	I↓: Select Item
Processor	50654 - SKX MO	Enter: Select
PCH	LBG QS/PRQ - 1G - SO	+/-: Change Uption
RU Revision	155.825	ESC: EXIT
Manager Talanathan		F1: General Help
Memory Information	007C0 ND	F2: Previous values
Tutal Memory Cuppert Memory Energy	32768 MB	F3: Uptimized Defaults
current Memory Frequency	2400 MHZ	KX: Sepall balp apag upwande
Sustem Landuade	[English]	ZMX: Scroll help area downwards
		The set of the the area downwards

表3-1 Main 界面参数

界面参数	功能说明
BIOS Information	
BIOS Vendor	显示BIOS供应商
Core Version	显示BIOS内核版本号
Compliancy	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 <u>3.6 Security界面</u>	
Platform Information		
Platform	显示平台信息	
Processor	显示CPU型号	
РСН	显示PCH型号	
RC Revision	显示RC版本	
Memory Information		
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 <u>3.4.4 Memory</u> Configuration界面	
	显示和设置当前系统语言。按Enter,选择如下两种系统语言:	
System Language	● English (缺省)	
	 中文(简体) 	
Modify Asset Tag	服务器资产标签配置菜单	
	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:	
System Date	● 按"+":数值加1。	
	 ● 按"-":数值减1。 	
	• 按数字键:直接修改数值。	
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:	
	 ● 按 "+":数值加 1。 	
	 ● 按"-":数值减 1。 	
	• 按数字键:直接修改数值。	

Modify Asset Tag界面如 图 <u>3-2</u>所示,具体参数说明如 <u>表 3-2</u>所示。

图3-2 Modify Asset Tag 界面

Main		
Enter New Asset Tag	01234567890123456789012 345678912	Enter new asset tag.The input range is 2~32.
Confirm Set Asset Tag	[NO]	
		<pre>++: Select Screen f4: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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。
	确认修改服务器的资产标签,菜单选项为:
Confirm set Asset Tag	• NO (缺省): 放弃修改服务器的资产标签。
	• YES:保存修改服务器的资产标签。

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

Main Advanced Platform Configuration	Socket Configuration	Server Management Security
 Intel(R) Virtual RAID on CPU Driver Health Trusted Computing ACPI Settings Serial Port Console Redirection PCI Subsystem Settings Network Stack Configuration CSM Configuration NVMe Configuration USB Configuration 		This formset allows the user to manage Intel(R) Virtual RAID on CPU
		<pre> ++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 > IIO 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

	Socket Configuration	
VMD Config for PStack0 Intel® VMD for Volume Management [Dis Device for PStack0	Socket Configuration	Enable/Disable Intel® volume management device technology in this stack. Auto means VMD technology will be enabled when POST detected NVMe expander card in this stack.
		F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

界面参数	功能说明
Intel® VMD for Volume Management Device for PStack0	PStack0中的英特尔®VMD卷管理设备配置菜单,菜单选项为:
	• Disabled: 禁用此 PStack0 栈中英特尔®卷管理设备技术。
	• 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。
	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PCle设备无法正常使用。

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

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

Advanced	
Intel(R) VROC with VMD Technology 5.4.0.1039 Upgrade key: Standard	Select to see more information about the Intel VMD Controllers
Intel VROC Managed Volumes: ▶ VolumeO, RAIDO(Stripe), 1415.89GB, Normal	
Intel VROC Managed Controllers: ▶ All Intel VMD Controllers	
	++: Select Screen 14: Select Item
	Enter: Select +/-: Change Option
	F1: General Help F2: Previous Values
	F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards</k>
	<m>: Scroll help area downwards</m>

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	已创建的RAID 信息:
	Volume0:该RAID名字,RAID0:该RAID级别
	1415.89GB(Size): 该RAID大小, Normal: 该RAID状态
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 <u>3-6</u>所示, 具体参数说明如 <u>表</u> <u>3-6</u>所示。

💕 说明

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

Advanced		
RAID VOLUME INFO		
Volume Actions ▶ Delete		
Name: RAID Level: Strip Size: Size: Status: Bootable: Block size:	Volume0 RAIDO(Stripe) 128KB 1415.89GB Normal Yes 512	
 SAMSUNG MZWLL1T6HEHP-00003 SN:S3HDNX0J600102, 1490.42GB Port 1:1, Slot 121, CPU0, VMD0, BDF 02:00.0 INTEL SSDPE2MEB00G4 SN:PHMD63960129800GGN, 745.21GB Port 1:3, Slot 123, CPU0, VMD0, BDF 04:00.0 		<pre>++: Select Screen tl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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	

- 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

Advanced Advanced	
Delete Delete the RAID volume? ALL DATA ON VOLUME WILL BE LOST! > Yes > No	Deleting a volume will reset the disks to non-RAID.
	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

Advanced		
INTEL SSDPE2ME800G4 SN:PHMD63960129800GGN, 745.21GB		Removes RAID data from the disk
Disk Actions: Reset to non-RAID Controller: Model Number: Serial Number: Size: Status: Block Size: Root Port Number: Root Port Offset: Slot Number: Socket Number: VMD Controller Number:	Volume Management Device Controller INTEL SSDPE2ME800G4 PHMD63960129800GGN 745.21GB RAID Member 512 1 3 123 0	++: Select Screen f4: Select Item Enter: Select +/-: Change Option
PCI Bus:Device.Function:	04:00.0	ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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	

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

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

Advanced	
Reset to non-RAID	Removes RAID data from the disk
Remove RAID structure on disk?	
▶ Yes ▶ Na	
	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

Advanced	
All Intel VMD Controllers	This page allows you to create a RAID volume
▶ Create RAID Volume	
RAID Volumes: ▶ Volume0, RAIDO(Stripe), 1.72TB, Normal	
Non-RAID Physical Disks: ▶ INTEL SSDPE2KX010T7 SN:PHLF721100J21P0GGN, 931.5GB	
Port 1:2, Slot 121, CPUO, VMDO, BDF 03:00.0 ▶ INTEL SSDPE2KX010T7 SN:PHLF707600211P0GGN, 931.5GB Port 1:3, Slot 123, CPUO, VMDO, BDF 04:00.0	
	↔: Select Screen
	Enter: Select
	+/-: Change Option
	ESC: Exit E1: General Heln
	F2: Previous Values
	F3: Optimized Defaults
	<pre>K>: Save & Exit Setup K>: Scroll help area upwards</pre>
	<m>: Scroll help area downwards</m>

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。	
	 若安装的是4端口的 NVME SSD 扩展卡且该卡安装在 PCle 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 PCle Riser 卡插槽 1,则 x 显示为 1,若安装在 PCle Riser 卡插槽 2,则 x 显示为 2。 	

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

Advanced		
Create RAID Volume		Enter a unique volume name that has no special characters
Name:	Volume0	and is 16 characters or less.
RAID Level:	[RAIDO(Stripe)]	
Enable RAID spanned over VMD	[]	
Controllers:		
Select Disks:		
INTEL SSDPE2KX010T7	[X]	
SN:PHLF7211009Z1P0GGN, 931.5GB		
Port 1:0 CPU0 VMD0		
INTEL SSDPE2KX010T7	[X]	
SN:PHLF7211003A1POGGN, 931.5GB		
Port 1:1 CPU0 VMD0		↔: Select Screen
INTEL SSDPE2KX010T7	[]	↑↓: Select Item
SN:PHLF721100J21P0GGN, 931.5GB		Enter: Select
Port 1:2 CPU0 VMD0		+/-: Change Option
INTEL SSDPE2KX010T7	[]	ESC: Exit
SN:PHLF707600211P0GGN, 931.5GB		F1: General Help
Port 1:3 CPU0 VMD0		F2: Previous Values
		F3: Optimized Defaults
Strip Size:	[128KB]	F4: Save & Exit Setup
Capacity (MB):	1812342	<pre><k>: Scroll help area upwards</k></pre>
		M>: Scroll help area downwards
▶ Create Volume		

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: RAID0(Stripe)(缺省): RAID0 RAID1(Mirror): RAID1 RAID5(Parity): RAID5 RAID10(RAID0+1): RAID10 	
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键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: (缺省):未选中该硬盘。 X:选中该硬盘。 	
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

	Advanced		
Γ	INTEL SSDPE2KX010T7 SN:PHLF721100J2	1P0GGN, 931.5GB	Mark disk as Spare
	INTEL SSDPE2KX010T7 SN:PHLF721100J2 Disk Actions: Mark as Spare Mark as Journaling Drive Controller: Model Number: Serial Number: Size: Status: Block Size: Root Port Number: Root Port Number: Slot Number: Slot Number: Socket Number: VMD Controller Number: PCI Bus:Device.Function:	1POGGN, 931.5GB Volume Management Device Controller INTEL SSDPE2KX010T7 PHLF721100J21POGGN 931.5GB Non-RAID 512 1 2 121 0 0 0 03:00.0	Mark disk as Spare ++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults
			F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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 <u>3-13</u>所示,具体参数说明如 <u>表 3-13</u>所示。

图3-13 Mark as Spare 界面

	Advanced Advanced	
Γ	Mark as Spare	Mark disk as Spare
	Are you sure you want to mark the disk as Spare? Marking disk as Spare will remove all data on the disk.	
Þ	Yes	
	No	
L		
		→+: Select Screen ↑1· Select Item
		Enter: Select
		+/−: Change Option
		ESC: Exit
		F1: General Help F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit Setup
		<k>: Scroll help area upwards</k>
		<m>: Scroll help area downwards</m>
L		

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

Advanced Advanced	
Mark as Journaling Drive	Mark disk as Journaling Drive
Are you sure you want to mark the disk as Journaling Drive? Marking disk as Journaling Drive will remove all data on the disk.	
▶ Yes	
▶ No	
	↔: Select Screen
	↑↓: Select Item
	⊢nter: Select +/−: Change Option
	ESC: Exit
	F1: General Help
	F3: Optimized Defaults
	F4: Save & Exit Setup
	<pre><k>: Scroll help area upwards </k></pre>
	CH2. SCHOIT HEID AFEA COMPMARUS

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		
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 <u>表 3-15</u> 所示。

图3-15 Driver Health 界面

Advanced		
Intel(R) 40GbE 2.5.07 Intel(R) 40GbE 2.5.07 Intel(R) 40GbE 2.5.07 Intel(R) 40GbE 2.5.07	Healthy Healthy Healthy Healthy	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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:	
	● Healthy: 正常。	
	• Failed:异常,需要修复。按 Enter,并按照界面提示可修复驱动/控制器。	
	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 <u>表 3-16</u>所示。

图3-16 Trusted Computing 界面

Advanced		
Configuration Security Device Support No Security Device Found	[Enabled]	Enable/Disable BIOS support for security device. O.S. will not show security device. TCG EFI protocol and INT1A interface will not be available.
		<pre> ++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

Advanced		
TPM2.0 Device Found Vendor: NTZ Firmware Version: 4.1		Enable/Disable BIOS support for security device. O.S. will not show security device. TCG EFI protocol and INT1A interface will not be
Security Device Support	[Enabled]	available.
Active PCR Banks	SHA-1,SHA256	
Available PCR Banks	SHA-1,SHA256,SM3	
SHA-1 PCR Bank SHA256 PCR Bank SM3_256 PCR Bank	[Enabled] [Enabled] [Disabled]	
TPM State	[Enabled]	++: Select Screen
Pending Operation	[None]	↑↓: Select Item
Platform Hierarchy	[Enabled]	Enter: Select
Storage Hierarchy	[Enabled]	+/-: Change Ontion
Endorsement Hierarchy	[Enabled]	ESC: Exit
TPM2.0 UEFI Spec Version	[TCG_2]	F1: General Help
Physical Presence Spec Version	[1.3]	F2: Previous Values
TPM 2.0 InterfaceType	[TIS]	F3: Optimized Defaults
PH Randomization	[Disabled]	F4: Save & Exit Setup
Device Select	[Auto]	<k>: Scroll help area upwards</k>
		<m>: Scroll help area downwards</m>

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启用配置,菜单选项为:
SHA-1 PCR Bank	• Enabled(缺省): 启用 SHA-1 PCR Bank。
	• Disabled: 禁用 SHA-1 PCR Bank。
	SHA256 PCR Bank启用配置,菜单选项为:
SHA256 PCR Bank	• Enabled(缺省): 启用 SHA256 PCR Bank。
	• Disabled: 禁用 SHA256 PCR Bank。
	SM3_256PCR Bank启用配置, 菜单选项为:
SM3_256PCR Bank	• Enabled(缺省): 启用 SM3_256PCR Bank。
	• Disabled: 禁用 SM3_256PCR Bank。
	TPM状态开关,菜单选项为:
TPM State	● Enabled(缺省): 启用 TPM。
	• Disabled: 禁用 TPM。

界面参数	功能说明		
	控制设备的安全操作,菜单选项为:		
Pending Operation	• None (缺省): 无操作。		
	• TPM Clear: 清除 TPM 的度量值。		
	平台等级开关,菜单选项为:		
Platform Hierarchy	• Enabled (缺省): 开启平台等级功能。		
	• Disabled: 关闭平台等级功能。		
	存储等级开关,存储等级由平台固件控制,菜单选项为:		
Storage Hierarchy	• Enabled (缺省): 开启存储等级功能。		
	• Disabled: 关闭存储等级功能。		
	认可等级开关,菜单选项为:		
Endorsement Hierarchy	• Enabled (缺省): 开启认可等级功能。		
	• Disabled: 关闭认可等级功能。		
	选择支持的TCG规范版本,菜单选项为:		
TPM 2.0 LIFEL Spec Version	• TCG_1_2: 兼容 win8/win10 的模式。		
	• TCG_2 (缺省): 支持 TCG2 协议和事件格式,提供 win10 及以上的 支持。		
	选择上报给OS的支持PPI规范的版本号。菜单选项为:		
Physical Presence Spec Version	• 1.2: 支持的 PPI 规范为 1.2 版本。		
	• 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。		
TPM 2.0 InterfaceType	显示TPM 2.0接口类型		
	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:		
PH Randomization	• Enabled: 开启平台等级随机性功能。		
	• Disabled (缺省): 关闭平台等级随机性功能。		
	选择支持的TPM版本,菜单选项为:		
	• TCM 1.0: 仅支持 TCM 1.0。		
Device Select	• TPM 2.0: 仅支持 TPM 2.0。		
	• 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。		

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

Advanced		
Configuration Security Device Support TCM State Pending Operation Device Select	[Enabled] [Enabled] [None] [Auto]	Enable/Disable BIOS support for security device. O.S. will not show security device. TCG EFI protocol and INT1A interface will not be available.
Current Status Information TCM Enabled Status: TCM Active Status: TCM Owner Status:	Enabled Activated Unowned	
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards </m></k></pre>

表3-18 TCM 界面参数

界面参数	功能说明			
Configuration				
	对安全设备的支持使能开关,菜单选项为:			
Security Device Support	• Enabled (缺省): 使能对安全设备的支持。			
	• Disabled: 禁止对安全设备的支持。			
	TCM状态开关,菜单选项为:			
TCM State	● Enabled(缺省): 启用 TCM。			
	• Disabled: 禁用 TCM。			
	控制设备的安全操作,菜单选项为:			
Pending Operation	• None (缺省): 无操作。			
	• TCM Clear: 清除 TCM 的度量值。			
	选择支持的TPM版本,菜单选项为:			
	• TCM 1.0: 仅支持 TCM 1.0。			
Device Select	• TPM 2.0: 仅支持 TPM 2.0。			
	 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。 			

界面参数	功能说明			
Current Status Information				
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 <u>图 3-19</u>所示,通过ACPI Settings界面,可以对ACPI进行配置。具体参数说明如 <u>表 3-19</u>所示。 图3-19 ACPI Settings 界面

Advanced		
ACPI Settings		Enable/Disable BIOS ACPI auto
Enable ACPI Auto Configuration	[Disabled]	configuration.
Lock Legacy Resources	[Disabled]	
		↔: Select Screen †↓: Select Item
		Enter: Select +/-: Change Option
		ESC: Exit F1: General Help
		F2: Previous Values F3: Optimized Defaults
		F4: Save & Exit Setup <k>: Scroll belo area upwards</k>
		<m>: Scroll help area downwards</m>

表3-19 ACPI Settings 界面参数

界面参数	功能说明		
	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:		
Enable ACPI Auto Configuration	• Enabled: 开启 ACPI 自动配置功能。		
	• Disabled (缺省):关闭 ACPI 自动配置功能。		

界面参数	功能说明		
	锁定传统资源设置,菜单选项为:		
Lock Legacy Resources	• Enabled: 开启锁定传统资源功能。		
	• Disabled (缺省):关闭锁定传统资源功能。		

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 <u>表 3-20</u> 所示。

图3-20 Serial Port Console Redirection 界面

Advanced		
COMO Console Redirection Console Redirection Settings Serial Port for Out-of-Band Managemen Windows Emergency Management Services Console Redirection Console Redirection Settings	[Enabled] t/ (EMS) [Disabled]	Console redirection enable ∕ disable.
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-20	Serial	Port	Console	Redirection	界面参数
-------	--------	------	---------	-------------	------

界面参数	功能说明
COM0	COM0端口
	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:
Console Redirection	 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。
	• Disabled: 关闭串口重定向功能。

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,界面如图3-21所示,具体参数说明如表3-21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:
	• Enabled: 开启串口重定向功能。
	• Disabled (缺省):关闭串口重定向功能。
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 <u>图3-22</u> 所 示。具体参数说明如 <u>表3-22</u> 所示。

COM0 端口的Console Redirection Settings界面如 图 3-21 所示。具体参数说明如 <u>表 3-21</u>所示。 图3-21 COM0 端口的 Console Redirection Settings 界面

界面参数	功能说明
Terminal Type	终端类型配置,菜单选项为:
	• VT100: ASCII 字符集。
	• VT100+ (缺省): 扩展的 VT100, 用于支持颜色显示、功能键等。
	• VT-UTF8: 使用 UTF8 编码映射 unicode 字符到 1 个或多个字节。
	• ANSI: 扩展 ASCII 字符集。
	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:
	• 9600
Bits Per Second	• 19200
	• 38400
	• 57600
	 115200(缺省)
	每字节中实际数据所占的比特数配置,菜单选项为:
Data Bits	• 7
	 8(缺省)
	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:
	• None (缺省): 无校验,不进行数据的校验。
Devity	● Even: 偶校验。
Fanty	• Odd: 奇校验。
	• Mark: 奇偶校验位始终为 1。
	• Space: 奇偶校验位始终为0。
	Mark和Space奇偶校验不支持错误检测。
	停止位(单个数据包的最后一位),标准设置是1位停止位,当与慢速设 备通信时可能需要1个以上停止位,菜单选项为:
Stop Bits	● 1 (缺省)
	• 2
	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:
	• None (缺省):不进行流控制。
Flow Control	• 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 PCle 设备 OptionROM、屏幕黑屏光标闪烁等问题。
	VT-UTF8组合键支持,菜单选项为:
VT-UTF8 Combo Key Support	• Enabled (缺省):开启 VT-UTF8 组合键支持 ANSI/VT100 终端。
	• Disabled:关闭 VT-UTF8 组合键支持 ANSI/VT100 终端。
	记录器模式,菜单选项为:
Recorder Mode	• Enabled: 开启记录器模式,用于捕获终端文本数据。
	• Disabled (缺省): 关闭记录器模式,

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

界面参数	功能说明
Resolution 100×31	显示扩展终端分辨率为100x31
	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:
Legacy OS Redirection Resolution	• 80×24 (缺省)
	• 80×25
	Putty小键盘,菜单选项为:
	• VT100(缺省)
	• LINUX
Putty KeyPad	• XTERMR6
	• SCO
	• ESCN
	• VT400
	BIOS上电自检后重定向设置,菜单选项为:
Redirection After BIOS POST	 Always Enable (缺省): 始终启用 Legacy 控制台重定向。
	 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。

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

Advanced		
Out-of-Band Mgmt Port Terminal Type Bits Per Second Flow Control Data Bits Parity Stop Bits	CDM0 [VT100+] [115200] [None] 8 None 1	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in console redirection settings page, for more help with terminal Type/emulation.
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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: VT100: ASCII 字符集。 VT100+(缺省): 扩展的 VT100,用于支持颜色显示、功能键等。 VT-UTF8:使用 UTF8 编码映射 unicode 字符到 1 个或多个字节。 ANSI:扩展 ASCII 字符集。 	
Bits Per Second	每秒传输比特数配置,菜单选项为: 9600 19200 57600 115200(缺省)	
Flow Control	 流控制配置,用于防止数据从缓存中溢出,菜单选项为: None(缺省):不进行流控制。 Hardware RTS/CTS:通过硬件请求发送协议/清除发送协议进行流控制。 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速率以匹配双方的速率。 	
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)。	

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

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 <u>表 3-23</u> 所示。

图3-23 Slot x:Port x 界面

Aptio Setup Utility – Copyright (C) 2018 American Main Advanced Platform Configuration Socket Configuration S	Megatrends, Inc. Server Management Security →
 Intel(R) Virtual RAID on CPU Slot 121:Port 1 - Generic NVME PCIE SSD Configuration Data Slot 123:Port 1 - INTEL SSDPE2ME800G4-PHMD63960129800GGN Slot9-mLOM:Port 1 - Intel(R) Ethernet Connection X722 for 1GbE - 74:EA:CB:SA:5D:90 Slot9-mLOM:Port 2 - Intel(R) Ethernet Connection X722 for 1GbE - 74:EA:CB:SA:5D:91 Slot9-mLOM:Port 3 - Intel(R) Ethernet Connection X722 for 1GbE - 74:EA:CB:SA:5D:92 Slot9-mLOM:Port 4 - Intel(R) Ethernet Connection X722 for 1GbE - 74:EA:CB:SA:5D:93 Driver Health Two remembers 	Manage Generic Express Flash NVMe PCIe SSD
 ACPI Settings Serial Port Console Redirection PCI Subsystem Settings Network Stack Configuration CSM Configuration NVMe Configuration USB Configuration 	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>
Version 2.19.1268. Copyright (C) 2018 American Me	egatrends, Inc.



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

Advanced		
▶ NIC Configuration		Click to configure the network
Blink LEDs	0	
UEFI Driver Adapter PBA Device Name	Intel(R) 40GbE 2.2.22 302900–000 Intel(R) Ethernet Connection X722 for 10GBASE–T	
Chip Type PCI Device ID PCI Address	Intel X722 37D2 3D:00:00	
Link Status	[Disconnected]	↔: Select Screen 1↓: Select Item
MAC Address Virtual MAC Address	60:DA:83:80:41:64 00:00:00:00:00:00	Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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

Advanced		
Link Speed Wake On LAN	[Auto Negotiated] [Disabled]	Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-24 NIC Configuration 界面参数

界面参数	功能说明	
Link Speed	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:	
	• Auto Negotiated (缺省): 自协商。	
	• 10 Mbps Half: 10 Mbps 半双工。	
	• 10 Mbps Full: 10 Mbps 全双工。	
	• 100 Mbps Half: 100 Mbps 半双工。	
	• 100 Mbps Full: 100 Mbps 全双工。	
Wake On LAN	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:	
	• Enabled: 开启局域网唤醒功能。	
	• Disabled (缺省):关闭局域网唤醒功能。	

3.2.7 PCI Subsystem Settings界面

如 <u>图 3-26</u>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 <u>表 3-25</u>所示。

图3-26 PCI Subsystem Settings 界面

Advanced	ng ang ang ang ang ang ang ang ang ang a	
PCI Bus Driver Version	A5.01.12	Re-enable Bus Master Attribute
PCI Devices Common Settings:		enumeration for PCI Bridges
Above 46 Decoding	[Enabled]	after SMM Locked
SR-IOV Support	[Enabled]	
BME DMA Mitigation	[Disabled]	
		++: Select Screen
		T+: Select Item
		Enter: Select
		ESC. Evit
		E1: General Heln
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit Setup
		<pre><k>: Scroll help area upwards</k></pre>
		<m>: Scroll help area downwards</m>

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	
PCI Devices Common Settings		
Above 4G Decoding	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:	
	• Enabled (缺省): 开启 4G 以上译码。	
	• Disabled: 关闭 4G 以上译码。	
	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。	
	虚拟化IO支持设置,菜单选项为:	
SB-IOV Support	• Enabled (缺省): 支持系统虚拟化 IO。	
	 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。 	
BME DMA Mitigation	BME DMA 减缓,用于阻止 DMA 侧信道攻击,菜单选项为:	
	• 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。	
	• Disabled (缺省): 设置为该选项后, DMA 功能可用, PCle 设备 性能正常。	

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。



Advanced		
Network Stack IPv4 PXE Support IPv6 PXE Support Media detect count PXE Retry Count	[Enabled] [Enabled] [Enabled] 1 1	Enable/Disable UEFI network stack ++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

表3-26 Network Stack Configuration 界面参数

界面参数	功能说明
Network Stack	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:
	• Enabled (缺省): 开启网络堆栈功能。
	• Disabled: 关闭网络堆栈功能。
IPv4 PXE Support	IPv4 PXE支持,支持从IPv4网络启动操作系统,菜单选项为:
	• Enabled (缺省): 开启 IPv4 PXE 功能。
	• Disabled: 关闭 IPv4 PXE 功能,不会创建 IPv4 PXE 启动选项。
IPv6 PXE Support	IPv6 PXE支持,支持从IPv6网络启动操作系统,菜单选项为:
	• Enabled (缺省):开启 IPv6 PXE 功能。
	• Disabled: 关闭 IPv6 PXE 功能,不会创建 IPv6 PXE 启动选项。

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 <u>表 3-27</u> 所示。

图3-28 CSM Configuration 界面

Advanced		
Compatibility Support Module Configu	uration	Auto -Launch UEFI OpROM of
CSM Support	[Enabled]	OpROM of legacy boot mode; Custom —The customized setting
Option ROM Execution		should match with the BIOS boot mode, incorrect settings
Option ROM Policy Network Storage Video Other PCI devices	[Custom] [UEFI] [UEFI] [UEFI] [UEFI]	may cause the OpROM not be executed,so it is recommended that keep the setting default as Auto.
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-27 CSM Configuration 界面参数

界面参数	功能说明
CSM Support	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:
	• Enabled (缺省): 开启 CSM 功能。
	• Disabled:关闭 CSM 功能。
	需要注意的是,Legacy启动模式下,该功能会一直处于开启状态。

界面参数	功能说明
Option ROM Execution	
	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:
	● Auto (缺省): 自动模式。
Option ROM Policy	• 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; Leagcy 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。
Network	设置网卡Option ROM的加载方式,菜单选项为:
	• UEFI (缺省): 加载网卡在 UEFI 启动模式下的 Option ROM。
	• Legacy: 加载网卡在 Legacy 启动模式下的 Option ROM。
	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:
Storage	• UEFI (缺省):加载存储设备在 UEFI 启动模式下的 Option ROM。
	• Legacy:加载存储设备在 Legacy 启动模式下的 Option ROM。
	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:
Video	• UEFI (缺省): 加载显示设备在 UEFI 启动模式下的 Option ROM。
	• Legacy:加载显示设备在 Legacy 启动模式下的 Option ROM。
Other PCI Devices	设置其他PCI设备Option ROM的加载方式,比如Input设备,Option ROM Policy设置为Custom时,该选项可用,菜单选项为:
	• UEFI (缺省): 加载其他 PCI 设备在 UEFI 启动模式下的 Option ROM。
	• Legacy: 加载其他 PCI 设备在 Legacy 启动模式下的 Option ROM。

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 <u>图 3-29</u>所示,通过NVMe Configuration界面,可以对NVMe进行配置。具体参数说明如 <u>表 3-28</u> 所示。

图3-29 NVMe Configuration 界面

Advanced	
NVMe Configuration	
• INTEL SSDPE2KX010T7	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 <u>表 3-29</u>所示。

Advanced		
Slot:2 Port:2 Bus:Dev:Func Model Number Total Size Vendor ID Device ID Namespace: 1	00:18:00:00 INTEL SSDPE2KX010T7 1000.2 GB 8086 0A54 Size: 1000.2 GB	++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>
		F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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

Advanced		
USB Configuration USB Controllers: 1 XHCI USB Devices: 6 Drives, 1 Keyboard, 1 Mouse,	1 Hub	Enable legacy USB support. AUTO option disables legacy support if no USB devices are connected. Disable option will keep USB devices available only for EFI applications.
Legacy USB Support XHCI Hand-Off USB Mass Storage Driver Support Mass Storage Devices: SanDisk	[Enabled] [Enabled] [Enabled] [Auto]	
ASUS SDR-08B1-U A A201 hp v220w 1100 KingstonDataTraveler 3.0PMAP AMI Virtual CDROMO 1.00 AMI Virtual CDROM1 1.00	[Auto] [Auto] [Auto] [Auto] [Auto]	<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards</k></pre>
		<m>: Scroll help area downwards</m>

表3-30 USB Configuration 界面参数

界面参数	功能说明
LICD Controllero	显示USB控制器信息。
USB Controllers	• XHCI: XHCI 控制器,支持 USB3.0。
	显示USB设备信息。
	• Drives: 当前连接 Drives 的数量, Drive 包含物理设备和虚拟设备。
USB Devices	• Keyboard: 当前连接的键盘数。
	● Mouse: 当前连接的鼠标数。
	• Hub: 当前连接的 USB Hub 数,服务器内置了 1 个 USB Hub。
	支持传统USB设备功能,菜单选项为:
	• Enabled (缺省): 支持传统 USB 设备。
Legacy USB Support	• 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。
	 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。
XHCI Hand-off	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:
	• Enabled (缺省): 开启可扩展主机控制器接口功能。
	• Disabled:关闭可扩展主机控制器接口功能。

界面参数	功能说明
	支持大容量USB存储设备,菜单选项为:
USB Mass Storage Driver Support	• Enabled (缺省): 支持大容量 USB 存储设备。
	• Disabled:不支持大容量 USB 存储设备。
Mass Storage Devices	
	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:
	• Dual SD 卡扩展模块不支持热插拔, SD 卡支持热插拔。
Dual SD Card RAID LUN	• 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。
	 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。
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 <u>表 3-31</u> 所示。

图3-32 Platform Configuration 界面

Main Advanced Platform Configuration Socket Configuration S	Server Management Security 🔹 🕨
 PCH Configuration Miscellaneous Configuration Server ME Configuration Runtime Error Logging 	Displays and provides option to change the PCH settings
	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 <u>表 3-32</u>所示。

图3-33 PCH Configuration 界面

Platform Configuration	
PCH Configuration	Enable/Disable Intel(R) IO controller hub devices
 PCH Devices PCH SATA Configuration PCH sSATA Configuration USB Configuration 	
	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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



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<u>表 3-34</u>和<u>表 3-35</u>。

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

Pl	atform Configuration	
PCIe PLL SSC	[Auto]	PCIE PLL SSC percentage or Disable SSC. Range is 0.0% – 1.9%.Last once is the POR for LBG
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-33 PCH Devices 界面参数

界面参数	功能说明	
PCIe PLL SSC	PCle PLL SSC配置,设置PCle锁相环扩频时钟,菜单选项为:	
	• Disabled: 禁用扩频时钟。	
	• Auto (缺省): 根据设备自动配置扩频时钟频率。	
	• 0.5%: 设置扩频时钟为总线时钟的百分比。	

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

Platform Configuration		
PCH SATA Configuration		▲ Identify the SATA port is connected to solid state drive
		or hard disk drive
SATA Controller	[Enabled]	
Configure SATA As	[AHCI]	
SATA Test Mode	[Disabled]	
SATA Port 0	[Not Installed]	
Port 0	[Not installed]	
SATA Port 1	[Not Installed]	
Port 1	[Not installed]	
SATA Port 2	[Not Installed]	
Port 2	[Fnabled]	
SATA Port 3	[Not Installed]	++: Select Screen
Port 3	[Enabled]	14: Select Item
SATA Port 4	VK0240GDJXII - 240.0 GB	Enter: Select
	(Slot 4)	+/-: Change Option
Port 4	[Enabled]	ESC: Exit
SATA Port 5	INTEL SSDSC2BB240G6 -	F1: General Help
	240.0 GB (Slot 5)	F2: Previous Values
Port 5	[Enabled]	F3: Optimized Defaults
SATA Port 6	ST1000NX0313 - 1000.2	F4: Save & Exit Setup
	GB (Slot 6)	<pre><k>: Scroll help area upwards</k></pre>
Port 6	[Enabled]	KM>: Scroll help area downwards
SATA Port 7	[Not Installed]	

表3-34 PCH SATA Configuration 界面参数

界面参数	功能说明
	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:
SATA Controller	• Enabled (缺省): 开启 SATA 控制器功能。
	• Disabled: 关闭 SATA 控制器功能。
Configure SATA as	配置SATA模式,菜单选项为: 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。 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。
	SATA Test模式开关,菜单选项为:
SATA Test Mode	• Enabled: 开启 SATA Test 模式。
	• Disabled (缺省):关闭 SATA Test 模式。
SATA Port 0	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 <u>4 SATA sSATA端口与背板槽</u> 位的对应关系。

_
界面参数	功能说明
Port 0	端口0设备开关,菜单选项为:
	● Enabled (缺省): 开启 SATA 端口 0 设备。
	• Disabled:关闭 SATA 端口 0 设备。
	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)

Platform Conf	iguration	
PCH sSATA Configuration		Enable/Disable sSATA controller
sSATA Controller Configure sSATA As sSATA Test Mode sSATA Port O Port O	[Enabled] [AHCI] [Disabled] [Not Installed] [Enabled]	
		<pre> ++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

Platform Con	figuration	
PCH sSATA Configuration		Enable/Disable sSATA controller
sSATA Controller Configure sSATA As sSATA Test Mode SSATA Port 0 Port 0 sSATA Port 1 Port 1 sSATA Port 2 Port 2 sSATA Port 2 Port 3 sSATA Port 3 Port 3 sSATA Port 4 Port 4 sSATA Port 5 Port 5	[Enabled] [AHCI] [Disabled] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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: 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。 Disabled:关闭 sSATA 控制器功能。
Configure sSATA as	配置sSATA模式,菜单选项为: 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。 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。
sSATA Test Mode	 SATA Test模式开关,菜单选项为: Enabled:开启 SATA Test 模式。 Disabled(缺省):关闭 SATA Test 模式。
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 <u>4 SATA sSATA端口与背板槽</u> 位的对应关系。

界面参数	功能说明
	sSATA端口开关,菜单选项为:
Port X	● Enabled(缺省):开启 sSATA 端口。
	• Disabled: 关闭 sSATA 端口。
	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)

Platform Configuration		
		Selectively enable/disable
USB Per-Connector Disable	[Enabled]	each of the USB physical
Rear Left USB Port 2.0 Capability	[Enabled]	connector (physical port).
Rear Right USB Port 2.0 Capability	[Enabled]	Once a connector is disabled,
Internal Top USB Port 2.0 Capability	[Enabled]	any USB devices plug into the connector will not be detected
Internal Bottom USB Port 2.0 Capability	[Enabled]	by BIOS or OS.
Front Left Top USB Port 2.0	[Enabled]	
Capability		
Front Right USB Port 2.0 Capability	[Enabled]	
Front Right USB Port 3.0	[Enabled]	†↓: Select Item
Capability		Enter: Select
SD Card Slot USB Port 3.0	[Enabled]	+/-: Change Option
Capability		ESC: Exit
Rear Left USB Port 3.0 Capability	[Enabled]	F1: General Help
Rear Right USB Port 3.0 Capability	[Enabled]	F2: Previous Values
Internal Top USB Port 3.0	[Enabled]	F3: Optimized Defaults
Capability		F4: Save & Exit Setup
Internal Bottom USB Port 3.0	[Enabled]	<k>: Scroll help area upwards</k>
Capability		<m>: Scroll help area downwards</m>

Platform Configurat	tion	
		Selectively enable/disable
USB Per–Connector Disable	[Enabled]	each of the USB physical
Rear Left USB Port 2.0 Capability	[Enabled]	connector (physical port).
Rear Right USB Port 2.0 Capability	[Enabled]	Once a connector is disabled,
Internal Top USB Port 2.0 Capability	[Enabled]	any USB devices plug into the connector will not be detected
Internal Bottom USB Port 2.0 Capability	[Enabled]	by BIOS or OS.
Front Left Top USB Port 2.0 Capability	[Enabled]	
Front Left Bottom USB Port 2.0	[Enabled]	
SD Card Slot USB Port 3.0	[Enabled]	↑↓: Select Item
Capability		Enter: Select
Rear Left USB Port 3.0 Capability	[Enabled]	+/-: Change Option
Rear Right USB Port 3.0 Canability	[Enabled]	ESC: Exit
Internal Ton USB Port 3.0	[Enabled]	E1: General Heln
Canability		E2: Previous Values
Internal Bottom USB Port 3.0	[Enabled]	E3: Ontimized Defaults
Canability	[21100200]	F4: Save & Exit Setun
oupdotting		(K): Scroll bein area unwards
		(M): Scroll help area downwards

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	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:	
	• 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。	
	• Disabled (缺省):关闭 USB 端口中单端口禁用控制功能。	
	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:	
Rear Left USB Port 2.0 Capability	• Enabled (缺省):开启后部左端 USB 2.0 功能。	
	• Disabled:关闭后部左端 USB 2.0 功能。	
	后部右端USB 2.0功能能配置,当USB Per-Connector Disable设置为Enabled时显示,菜单选项为:	
Rear Right USB Port 2.0 Capability	• Enabled (缺省):开启后部右端 USB 2.0 功能。	
	• Disabled:关闭后部右端 USB 2.0 功能。	
Internal Top USB Port 2.0 Capability	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:	
	• Enabled (缺省):开启内部顶端 USB 2.0 功能。	
	• Disabled:关闭内部顶端 USB 2.0 功能。	

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:
	 Enabled (缺省):开启内部底端 USB 2.0 功能。 Disabled, 关闭内部底端 USB 2.0 功能。
	● Disabled: 天闲內印成缅 USB 2.0 功能。
Front Loff Ton LICD Dort 2.0 Conschiller	设置为Enabled时显示,菜单选项为:
Front Left Top USB Port 2.0 Capability	• Enabled (缺省): 开启前部左挂耳顶端 USB 2.0 功能。
	Disabled: 关闭前部左挂耳顶端 USB 2.0 功能。
Front Left Bottom LISB Port 2.0	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:
Capability	• Enabled (缺省):开启前部左挂耳底端 USB 2.0 功能。
	• Disabled: 关闭前部左挂耳底端 USB 2.0 功能。
	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:
From Hight OOD For 0.0 Oupdointy	• Enabled (缺省):开启前部右挂耳 USB 3.0 功能。
	• Disabled: 关闭前部右挂耳 USB 3.0 功能。
SD Cord Slot LISD Dart 2.0 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:
SD Card Slot USB Port 3.0 Capability	• Enabled (缺省):开启 SD 卡槽 USB 3.0 功能。
	● Disabled:关闭 SD 卡槽 USB 3.0 功能。
Roar Left LISB Port 3.0 Canability	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:
Real Left USB Fort 5.0 Capability	• Enabled (缺省):开启后部左端 USB 3.0 功能。
	● Disabled:关闭后部左端 USB 3.0 功能。
	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:
Rear Right USB Port 3.0 Capability	• Enabled (缺省): 开启后部右端 USB 3.0 功能。
	• Disabled:关闭后部右端 USB 3.0 功能。
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:
	• Enabled (缺省): 开启内部顶端 USB 3.0 功能。
	• Disabled:关闭内部顶端 USB 3.0 功能。
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:
	• Enabled (缺省):开启内部底端 USB 3.0 功能。
	● Disabled:关闭内部底端 USB 3.0 功能。

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 <u>表 3-37</u>所示。

图3-40 Miscellaneous Configuration 界面

Platform Configuration		
Miscellaneous Configuration		Select active video type
Active Video Debug Mode SOL Mode	[Onboard Device] [Enabled] [Enabled]	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-37	Miscellaneous	Configuration	界面参数
			/ //

界面参数	功能说明
	显示设备选择,菜单选项为:
	• Auto: 根据设备自动设置界面显示方式。
	• Onboard Device (缺省): 服务器通过板载 VGA 接口进行界面显示。
Active Video	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。
	• PCle Device: 服务器通过 PCle 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。

界面参数	功能说明
Debug Mode	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:
	 Enabled: 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。
	• Disabled (缺省):关闭 BIOS 串口日志输出功能。
SOL Mode	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"curl http://HDM IP 地址/cgi/download_cpsol.cgi tr -d \000' > sol.txt"命令从服务器下载 BIOS串口日志。
	• HDM IP 地址: 服务器 HDM 共享网络接口或 HDM 专用网络接口的 IP 地址。
	• sol.txt: 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。
	菜单项为:
	• Enabled (缺省): 开启 SOL 功能。
	• Disabled: 关闭 SOL 功能。

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

Platform Configu	ration	
General ME Configuration Operational Firmware Version Backup Firmware Version Recovery Firmware Version ME Firmware Status #1 ME Firmware Status #2 Current State Error Code Altitude MCTP Bus Owner ME Firmware Features	0A:4.0.3.211 N/A 0A:4.0.3.211 0x000F0245 0x88112006 Operational No Error 8000 0 SiEn NM PECIProxy ICC PmBusProxy	MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.
	ThermalReport HSIO CUPS	Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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

Platform Configuration		
Platform Configu Runtime Error Logging System Errors S/W Error Injection Support System Memory Poison Viral Status System Cloaking EMCA Settings WHEA Settings Error Injection Settings UPI Error Enabling Memory Error Enabling IID Error Enabling PCIe Error Enabling	(Enabled) (Disabled) (Enabled) (Enabled) (Enabled) (Enabled)	System error enable/disable setup options. ++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults E4: Save & Evit Setup
 IIO Error Enabling PCIe Error Enabling 		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-39	Runtime	Error	Logging	界面参数
-------	---------	-------	---------	------

界面参数	功能说明	
System Errors	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:	
	• Enabled (缺省):开启系统错误记录功能。	
	• Disabled: 关闭系统错误记录功能。	
	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:	
S/W Error Injection Support	• Enabled: 开启软件错误注入支持功能,通过软件注入错误来检验 系统的性能。	
	• Disabled (缺省): 关闭软件错误注入支持功能。	
	系统内存Poison开关,System Errors设置为Enabled时,该选项可用, 菜单选项为:	
System Memory Poison	• Enabled (缺省): 开启系统内存 Poison 功能。	
System Memory Poison	• Disabled: 关闭系统内存 Poison 功能。	
	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。	
	病毒状态配置,菜单选项为:	
	• Enabled (缺省): 启用内存病毒。	
Viral Status	• Disabled: 禁用内存病毒。	
	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。	
	系统Cloaking功能配置,菜单选项为:	
System Cloaking	• Enabled (缺省): 启用系统 Cloaking 功能,当启用时,修正的和 UCNA 错误将被 OS/SW 屏蔽。	
	• Disabled: 禁用系统 Cloaking 功能。	
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

Platform Cont	figuration	
EMCA Settings		Enable/Disable EMCA logging
EMCA Logging Support LMCE Support Ignore OS EMCA Opt-in EMCA CMCI-SMI Morphing EMCA MCE-SMI Enable	[Enabled] [Disabled] [EMCA gen 2 CSMI] [EMCA gen 2 - MSMI]	<pre>**: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-40 EMCA Settings 界面参数

界面参数	功能说明
	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:
EMCA Logging Support	• Enabled (缺省): 开启 EMCA 功能。
	• Disabled:关闭 EMCA 功能。
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:
	• Enabled (缺省): 启用本地 MCE 固件支持。
	• Disabled: 禁用本地 MCE 固件支持。
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:
	• Enabled: 开启忽略 OS EMCA 选入功能。
	• Disabled (缺省): 关闭忽略 OS EMCA 选入功能。

界面参数	功能说明
EMCA CMCI-SMI Morphing	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:
	• EMCA gen 1 Lite: 配置 EMCA CMCI-SMI Morphing 为 EMCA gen 1 Lite 模式。
	 EMCA gen 2 CSMI(缺省): 配置 EMCA CMCI-SMI Morphing 为 EMCA gen 2 CSMI 模式。
	• Disabled:关闭 EMCA CMCI-SMI Morphing。
	EMCA MCE-SMI启用设置,菜单选项为:
EMCA MCE-SMI Enable	 EMCA gen 1 Dual Mode: 启用 EMCA gen 1 双模式的 EMCA MCE-SMI 功能
	 EMCA gen 2 – MSMI(缺省): 启用 EMCA gen 2 MSMI 模式的 EMCA MCE-SMI 功能
	• Disabled: 禁用 EMCA MCE-SMI 功能。

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

	Platform Configuration	
WHEA Settings		Enable/Disable WHEA support
WHEA Support	[Enabled]	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <<>>: Scroll help area upwards <</pre>

表3-41 WHEA Settings 界面参数

界面参数	功能说明
	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:
WHEA Support	• Enabled (缺省): 开启 WHEA 功能。
	• Disabled:关闭 WHEA 功能。

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

Platform Configura	ation	
Error Injection Settings		Enable/Disable Mca Bank error
Mca Bank Error Injection Support WHEA Error Injection Support	[Disabled] [Disabled]	<pre> Hubic/ofsault heb bank circl injection support. ++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards </m></k></pre>
		<k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

表3-42 Error Injection Settings 界面参数

界面参数	功能说明	
	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:	
Mca Bank Error Injection Support	• Enabled: 开启 Mca Bank 错误注入功能。	
	• Disabled (缺省):关闭 McBank Error Injection 功能。	
	WHEA错误注入功能开关,菜单选项为:	
WHEA Error Injection Support	• Enabled: 开启 WHEA 错误注入功能。	
	• Disabled (缺省):关闭 WHEA 错误注入功能。	

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

Platform Configuration		
UPI Error Enabling		Enable/disable SMI when
SMI UPI Lane Failover	[Disabled]	<pre>clock/data failover is set **: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-43 UPI Error Enabling 界面参数

界面参数	功能说明	
	UPI Lane发生错误时触发SMI中断设置,菜单选项为:	
SMI UPI Lane Failover	• Enabled: 开启 UPI Lane 发生错误时触发 SMI 中断。	
	• Disabled (缺省): 关闭 UPI Lane 发生错误时触发 SMI 中断。	

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

Platform Conf	iguration	
Memory Error Enabling		Enable/Disable memory error
Memory Error Memory Corrected Error Spare Interrupt	[Enabled] [Enabled] [SMI]	<pre>**: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-44 Memory Error Enabling 界面参数

界面参数	功能说明
	内存错误使能设置,菜单选项为:
Memory Error	• Enabled (缺省): 开启内存误功能。
	• Disabled: 关闭内存错误功能。
	内存可纠正错误使能设置,菜单选项为:
Memory Corrected Error	• Enabled (缺省): 开启内存可纠正错误功能。
	• Disabled: 关闭内存可纠正错误功能。
	Spare Interrupt类型设置, Memory Corrected Error设置为Enabled时, 该选项可用, 菜单选项为:
Spare Interrupt	• Disabled: 禁止使用内存备用中断。
	● SMI (缺省): SMI 中断。

IIO 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

Platform Configuration	
IIO Error Enabling	Enable/Disable IIO/PCH error support.
IIO/PCH Global Error Support [Enabled] IIO PCIe AER Spec Compliant [Disabled]	<pre>**: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-45 IIO Error Enable 界面参数

界面参数	功能说明	
	IIO/PCH全局错误支持功能配置,菜单选项为:	
IIO/PCH Global Error Support	• Enabled (缺省): 开启 IIO/PCH 全局错误支持功能。	
	• Disabled: 关闭 IIO/PCH 全局错误支持功能。	
	IIO PCIe AER Spec合规配置,菜单选项为:	
IIO PCIe AER Spec Compliant	• Enabled: 开启 IIO PCIe AER Spec 合规功能。	
	• Disabled (缺省):关闭 IIO PCIe AER Spec 合规功能。	

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

Platform Configur	ration	
PCIe Error Enabling		Enable & escalate correctable errors to error pins.
Corrected Error Uncorrected Error Fatal Error Enable PCIE Corrected Error Threshold Counter PCIE Corrected Error Threshold Mask PCIE Corrected Error Threshold SERR Propagation PERR Propagation	[Enabled] [Enabled] [Enabled] 3f 1 [Enabled] [Enabled]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-46 PCI Error Enabling 界面参数

界面参数	功能说明	
	PCle可修正错误使能设置,菜单选项为:	
Corrected Error	• Enabled (缺省): 开启 PCle 可修正错误功能。	
	• Disabled:关闭 PCle 可修正错误功能。	
	PCle不可修正错误设置,菜单选项为:	
Uncorrected Error	• Enabled (缺省): 开启 PCle 不可修正错误功能。	
	• Disabled: 关闭 PCIe 不可修正错误功能。	
	PCle致命错误使能设置,菜单选项为:	
Fatal Error Enable	• Enabled (缺省): 开启 PCle 致命错误功能。	
	• Disabled: 关闭 PCIe 致命错误功能。	
	PCle可修正错误阈值计数器使能设置。	
PCIe Corrected Error Threshold Counter	• Enabled: 开启 PCIe 可修正错误阈值计数器功能。	
	• Disabled (缺省):关闭 PCle 可修正错误阈值计数器功能。	
PCIe Corrected Error Threshold Mask	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。	
PCIe Corrected Error Threshold	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。	

界面参数	功能说明	
	SERR Propagation设置,菜单选项为:	
SERR Propagation	• Enabled (缺省): 开启 SERR Propagation 功能。	
	• Disabled: 关闭 SERR Propagation 功能。	
	PERR Propagation设置,菜单选项为:	
PERR Propagation	• Enabled (缺省): 开启 PERR Propagation 功能。	
	• Disabled:关闭 PERR Propagation 功能。	

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 <u>表 3-47</u> 所示

图3-50 Socket Configuration 界面

Main Advanced Platform Configuration	Socket Configuration	Server Management Security 💦 🕨
 Processor Configuration Common RefCode Configuration UPI Configuration Memory Configuration IIO Configuration Advanced Power Management Configuration 		Displays and provides option to change the processor settings
		<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 <u>表 3-48</u> 所示。

图3-51 Processor Configuration 界面

	Socket Configuration	
 Per-Socket Configuration Processor BSP Revision Processor Socket Processor ID Processor Frequency Processor Max Frequency Processor Min Frequency Processor TDP Microcode Revision L1 Cache RAM L2 Cache RAM L3 Cache RAM Processor 1 Version	50654 - SKX M0 Processor1 Processor2 00050654* 00050654 2.200GHz 2.200GHz 2.200GHz 2.200GHz 1.000GHz 1.000GHz 105W 105W 0200004D 0200004D 896KB 896KB 14336KB 14336KB 19712KB 19712KB Intel(R) Xeon(R) Sold 5	Enable/Disable the Monitor/Mwait instruction
Processor 2 Version Hyper-Threading [ALL] Check CPU BIST Result Monitor/Mwait Enable Intel(R) TXT VMX Enable SMX Debug Interface Hardware Prefetcher	Intel(R) Xeon(R) dold 5 120 CPU @ 2.20GHz Intel(R) Xeon(R) Gold 5 120 CPU @ 2.20GHz [Enabled] [Enabled] [Enabled] [Disabled] [Enabled] [Enabled] [Enabled]	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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]	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: Enabled(缺省):开启超线程功能。 Disabled:关闭超线程功能。 	
Check CPU BIST Result	 检查CPU BIST结果配置,菜单选项为: Enabled:开启检查 CPU BIST 结果,关闭失败的 BIST Core。 Disabled(缺省):关闭检查 CPU BIST 结果,忽略 BIST 结果。 	
Monitor/Mwait	 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。 Enabled:开启 Monitor/Mwait 指令。 Disabled:关闭 Monitor/Mwait 指令。 	
Enable Intel(R) TXT	 Intel可信执行技术开关,菜单选项为: 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。 Disabled(缺省):关闭 Intel 可信执行技术支持。 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。 	
VMX	 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Eabled时该选项置灰,菜单选项为: 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。 Disabled:关闭 Intel 硬件辅助虚拟化技术。 	
Enable SMX	 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Eabled时该选项置灰,菜单选 项为: Enabled: 开启安全模式扩展功能。 Disabled(缺省):关闭安全模式扩展功能。 	

界面参数	功能说明
Debug Interface	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:
	• Enabled (缺省): 开启调试接口功能。
	• Disabled: 关闭调试接口功能。
Hardware Prefetcher	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:
	• Enabled (缺省): 开启硬件预取功能。
	• Disabled: 关闭硬件预取功能。

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

	Socket Configuration	
 CPU Socket 1 Configuration CPU Socket 2 Configuration 		<pre> ++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 <u>表 3-50</u>所示。

图3-53 CPU Socket 1 Configuration 界面

Socket Configuration	
CPU Socket 1 Configuration Cores Enabled 0	Number of Cores to Enable. O means all cores. 4 Cores available.
	<pre>\$\$\$ \$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$</pre>
	F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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 <u>表 3-51</u> 所示。

图3-54 Common RefCode Configuration 界面

	Socket Configura	ation
Common RefCode Configuration		Select MMIO high base
Common RefCode Configuration MMIO High Base MMIO High Granularity Size NUMA	[896G] [64G] [Enabled]	Select MMIO high base ++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup
		<m>: Scroll help area downwards</m>

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: 56T 40T 24T 16T 4T 1T 896G(缺省)
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: 1G 4G 16G 64G(缺省) 512G 1024G

界面参数	功能说明
NUMA	NUMA开关,内存访问时间取决于待访问的内存是否为当前CPU对应的 内存,开启NUMA功能后,CPU访问本地存储器的速度比非本地存储器 的速度快,菜单选项为:
	● Enabled (缺省): 开启 NUMA。
	• Disabled: 关闭 NUMA。

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 <u>表</u> 3-52 所示。

图3-55 UPI Configuration 界面

	Socket Configuration	
UPI Configuration ► UPI General Configuration		Displays and provides option to change the UPI general settings
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

	Socket Configuration	
UPI General Configuration		UPI status help
 UPI Status Link Frequency Select UPI Failover Support SNC CRC Mode 	[Auto] [Auto] [Enabled] [Auto]	<pre>**: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k></pre>

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: 9.6GT/s 10.4GT/s Auto(缺省):自动选择 UPI 的链路频率。 	
UPI Failover Support	 UPI故障切换支持配置,菜单选项为: Enabled: 开启 UPI 故障切换支持。 Disabled: 关闭 UPI 故障切换支持。 Auto (缺省): 自动选择 UPI 故障切换是否支持。 	
SNC	 SNC功能配置,菜单选项为: Enabled:开启 SNC 功能。 Disabled(缺省):关闭 SNC 功能。 Auto:自动选择 SNC 功能是否开启。 	
CRC Mode	 UPI CRC 校验模式配置,菜单选项为: 16 Bit CRC:使用 16 位 CRC。 32 Bit Rolling CRC:使用 32 位滚动 CRC。 Auto(缺省):自动选择 CRC 校验模式。 	

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

	Socket Configuration	
UPI Status		
Number of CPU Number of IIO Current UPI Link Speed Current UPI Link Frequency UPI Global MMIO Low Base / Limit UPI Global MMIO High Base / Limit UPI PCIe Configuration Base / Size	2 Fast 10.4 GT/S 90000000 / FBFFFFF 000000000000000 / 00000000FFFFFF 80000000 / 10000000	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 <u>表 3-55</u> 所示。

图3-58 Memory Configuration 界面

	Socket Configuration	
 Integrated Memory Controller (IMC) Total Memory Curpent Memory	32768 MB	Enable/disable a custom memory refresh rate
 IMC Configuration Enforce POR Memory Frequency LRDIMM Module Delay Rank Margin Tool Data Scrambling for DDR4 WR CRC Feature Control DIMM Isolation Enable Custom Refresh Enable Custom Refresh Rate Refresh Options C/A Parity Enable Memory Topology Memory Map Memory RAS Configuration 	[Auto] [Auto] [Auto] [Auto] [Auto] [Auto] [Enabled] 20 [Acc Self Refresh] [Auto]	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k></pre>

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	
	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:	
Enforce POR	• Auto (缺省): 自动选择。	
	• Enforce POR:开启 POR,可以提升内存的稳定性。	
	• Disabled: 关闭 POR。	
	内存频率设置,菜单选项为:	
	• Auto (缺省)	
Memory Frequency	• 1600	
	• 1866	
	• 2133	
	• 2400	
	• 2666	

界面参数	功能说明	
	LRDIMM模块延迟设置,菜单选项为:	
LRDIMM Module Delay	 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。 	
	 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。 	
	Rank Margin工具,菜单选项为:	
	• Auto(缺省): 自动选择为 MRC 默认设置。	
Rank Margin Tool	• Disabled: 启用 Rank Margin 工具,将会在 DDR4 内存 training 之 后使用。	
	• Enabled: 禁用 Rank Margin 工具。	
	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:	
Data Scrambling	● Auto (缺省): 自动选择。	
	• Disabled: 关闭数据扰频功能。	
	• Enabled: 开启数据扰频功能。	
WR CRC Feature Control	写CRC功能控制,,菜单选项为:	
	• 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。	
	• Disabled: 禁用写 CRC。	
	• Enabled: 启用写 CRC。	
	DIMM隔离控制,菜单选项为:	
DIMM Isolation Enable	• 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。	
	• Disabled:为命令/地址校验和写 CRC 禁用 DIMM 隔离。	
	• Enabled:为命令/地址校验和写 CRC 启用 DIMM 隔离。	
	自定义内存刷新使能控制,菜单选项为:	
Custom Refresh Enable	• Enabled: 启用自定义的内存刷新速率。	
	• Disabled: 禁用自定义的内存刷新速率。	
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	
	刷新选项,菜单选项为:	
Refresh Options	• Acc Self Refresh: 加速自刷新。	
	• 2x Refresh: 2x 刷新。	
	C/A校验启用选项,菜单选项为:	
C/A Parity Enable	 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。 	
	• Disabled: 禁用 DDR4 命令地址校验。	
	• Enabled: 启用 DDR4 命令地址校验功能。	
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

	Socket Configuration	
Enable Processor1 IMC0 [Enable Processor1 IMC1 [Enable Processor2 IMC0 [Enable Processor2 IMC1 [[Enabled] [Enabled] [Enabled] [Enabled]	Enable/Disable IMC ++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

表3-56 IMC Configuration 界面参数

界面参数	功能说明		
Enable Processor Number IMC	处理器内存控制器配置菜单,菜单选项为: Disabled: 禁用相对应的 CPU 内存控制器对应的内存控制器。 Enabled(缺省): 启用相对应的 CPU 内存控制器对应的内存控制 		
	器。		

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

Socket Configuration	
Processor1 Ch1 DIMM A1:DIMM is Present.DIMM Status:Enabled DIMM Details: 2666MT/s Micron SRx4 16GB RDIMM Processor2 Ch1 DIMM B1:DIMM is Present.DIMM Status:Enabled DIMM Details: 2666MT/s Micron SRx4 16GB RDIMM	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

	Socket Configuration	
Volatile Memory Mode 1LM Memory Interleave Granularity IMC Interleaving Channel Interleaving Rank Interleaving Socket Interleave Below 46B	[1LM] [Auto] [Auto] [Auto] [Auto] [Disabled]	Selects whether 1LM or 2LM memory mode should be enabled
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-58 Memory Map 界面参数

界面参数	功能说明		
	易失性内存模式配置选项,菜单选项为:		
Volatile Memory Mode	• 1LM (缺省): 启用 1LM 模式。		
	• 2LM: 启用 2LM 模式。		
	• Auto: 自动设置易失性内存配置模式。		
	1LM内存交织颗粒配置选项,菜单选项为:		
11 M Momony Interlociyo Granularity	• Auto (缺省): 自动设置 1LM 内存交织颗粒配置大小的交织颗粒。		
TLM Memory Interleave Granularity	• 256B Target,256B Channel:设置 256B 大小的交织颗粒。		
	• 64B Target,64B Channel: 设置 64B。		
	IMC交织设置,用于提升内存的读写性能,菜单选项为:		
IMC Interleaving	• Auto (缺省): 自动选择。		
	 1-way Interleave: 1 路交织设置。 		
	• 2-way Interleave: 2 路交织设置。		
	Channel交织设置,用于提升内存的读写性能,菜单选项为:		
Channel Interleaving	• Auto (缺省): 自动设置 Channel Interleaving。		
	 1-way Interleave: 1 路交织设置。 		
	• 2-way Interleave: 2 路交织设置。		
	• 3-way Interleave: 3 路交织设置。		

界面参数	功能说明	
	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:	
	• Auto (缺省): 自动选择。	
Rank Interleaving	• 1-way Interleave: 1 路交织设置。	
	• 2-way Interleave: 2 路交织设置。	
	 4-way Interleave: 4 路交织设置。 	
	• 8-way Interleave: 8 路交织设置。	
Socket Interleave Below 4GB	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 <u>3.4.2 Common RefCode Configuration界面</u>),则该 功能会处于关闭状态,菜单选项为:	
	• Enabled: 开启 4GB 以下内存交织功能。	
	• Disabled (缺省):关闭 4GB 以下内存交织功能。	

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
	wichnory	10.00	Configuration	лещ

	Socket Configuration	
Memory RAS Configuration Setup Mirror Mode Enable Partial Mirror Memory Rank Sparing Correctable Error Threshold SDDC Plus One ADDDC Sparing Patrol Scrub Patrol Scrub Interval	[Disabled] [Disabled] [Disabled] [Disabled] 1024 [Disabled] [Disabled] [Enabled] 24	Mirror mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Mirror enable will disable XPT prefetch
Demand Scrub	[Disabled]	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

	表3-59	Memory	RAS	Configuration	界面参数
--	-------	--------	-----	---------------	------

界面参数	功能说明	
	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:	
	• Disabled (缺省): 禁用内存 Mirror Mode。	
	• Mirror Mode 1LM: 使用 1LMMirror Mode。	
Mirror Mode	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。	
	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。	
	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:	
Enable Partial Mirror	• Disabled (缺省): 禁用部分镜像模式。	
	• Mirror Mode 1LM: 使用部分镜像模式 1LM。	
	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:	
	• Enabled: 开启内存 Rank 备用功能。	
	• Disabled (缺省):关闭内存 Rank 备用功能。	
Memory Rank Sparing	需要注意的是:	
	 系统不支持将内存模式同时设置为 Mirror Mode 和 Memory Rank Sparing。 	
	 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。 	
	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:	
Multi Rank Sparing	• One Rank: 选择 1Rank 作为备用,要求通道中 Rank 数量大于等于 2。	
	• Two Rank: 选择 2Rank 作为备用,要求通道中 Rank 数量大于等于 4。	
Correctable Error Threshold	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。	
SDDC Plus One	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	
	• Enabled: 启用 SDDC 加一功能。	
	• Disabled (缺省): 禁用 SDDC 加一功能。	
	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	
ADDDC Sparing	• Enabled: 启用 ADDC 备用功能。	
	• Disabled (缺省): 禁用 ADDC 备用功能。	

界面参数	功能说明	
	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:	
Patrol Scrub	• Enabled (缺省): 开启 Patrol Scrub 功能。	
	• Disabled:关闭 Patrol Scrub 功能。	
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:	
	• Enabled: 开启 Demand Scrub 功能。	
	• Disabled (缺省):关闭 Demand Scrub 功能。	

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 <u>表 3-60</u>所示。

图3-63 IIO Configuration 界面

	Socket Configuration	
IIO Configuration		Enable/Disable PCIe hot plug globally
 Processor 1 Configuration Processor 2 Configuration Intel® VT for Directed I/O (VT-d) Intel® VMD technology PCIe Hot Plug 	[Enabled]	
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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	
	PCle热插拔配置,菜单选项为:	
PCIe Hot Plug	• Enabled (缺省): 开启 PCle 热插拔功能。	
	• Disabled: 关闭 PCle 热插拔功能。	



Processor 1 Configuration 和 Processor 2Configuration 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 2Configuration 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。

	Socket Configuration	
 Processor 1 PcieBr0D00F0 - Port 0/DMI Processor 1 PcieBr1D00F0 - Port 1A Processor 1 PcieBr1D02F0 - Port 1C Processor 1 PcieBr2D00F0 - Port 2A Processor 1 PcieBr2D02F0 - Port 2C Processor 1 PcieBr3D00F0 - Port 3A 		Settings related to PCI express ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3 B/3C/3D/4A/5A)
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

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

	Socket Configuration	
 Processor 1 PcieBr0D00F0 - Port 0/DMI Processor 1 PcieBr1D00F0 - Port 1A Processor 1 PcieBr2D00F0 - Port 2A Processor 1 PcieBr3D00F0 - Port 3A 		Settings related to PCI express ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3 B/3C/3D/4A/5A)
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

	Socket Configuration	
 Processor 1 PcieBr0D00F0 - Port 0/DMI Processor 1 PcieBr1D00F0 - Port 1A Processor 1 PcieBr1D02F0 - Port 1C Processor 1 PcieBr2D00F0 - Port 2A Processor 1 PcieBr2D02F0 - Port 2C Processor 1 PcieBr3D00F0 - Port 3A 		Settings related to PCI express ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3 B/3C/3D/4A/5A)
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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



	Socket Configuration					
 Processor 1 PcieBr0D00F0 - Port 0/DMI Processor 1 PcieBr1D00F0 - Port 1A Processor 1 PcieBr2D02F0 - Port 2C Processor 1 PcieBr3D00F0 - Port 3A 	Socket Configuration	Settings related to PCI express ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3 B/3C/3D/4A/5A) ++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup				
		<pre><k: &="" <k="" exit="" save="" setup="">: Scroll help area upwards <m>: Scroll help area downwards</m></k:></pre>				
表3-61	Processor 1	Configuration	界面参数	(本参数以	R4900 0	33 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

	Socket Configuration	
Processor 1 PcieBr0D00F0 – Port 0/DMI		Choose link speed for this PCIe port
Link Speed PCI-E Port Link Status PCI-E Port Link Max PCI-E Port Link Speed	[Auto] Linked as x4 Max Width x4 Gen 3 (8.0 GT/s)	<pre> ++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

界面参数	功能说明
	链路速度配置,菜单选项为:
	● Auto (缺省)
Link Speed	• Gen 1 (2.5 GT/s)
	• Gen 2 (5.0 GT/s)
	• Gen 3 (8.0 GT/s)

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。



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 <u>图 3-69</u>所示。具体参数说明如 <u>表 3-63</u>所示。 图3-69 Processor 1 PcieBr1D00F0 - Port 1A 界面

	Socket Configuration	
Processor 1 PcieBr1D00F0 - Port 1A PCI-E Port Hot Plug Capable Surprise Hot Plug Capable Link Speed PCI-E Port Link Status PCI-E Port Link Max PCI-E Port Link Speed	[Auto] [Enabled] [Enabled] [Auto] Link Did Not Train Max Width x8 Link Did Not Train	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
		<pre>++: Select Screen t4: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

界面参数	功能说明		
	PCI-E端口开关,菜单选项为:		
	• Auto (缺省): 自动选择。		
	● Enabled: 开启 PCI-E 端口。		
	• Disabled:关闭 PCI-E 端口,用于关闭端口和隐藏配置空间。		
	热插拔能力配置,菜单选项为:		
Hot Plug Capable	• Enabled: 开启该 PCIe 端口的热插拔能力。		
	• Disabled:关闭该 PCIe 端口的热插拔能力。		
	意外热插拔能力配置,菜单选项为:		
Surprise Hot Plug Capable	• Enabled: 开启该 PCIe 端口的意外热插拔能力。		
	• Disabled:关闭该 PCIe 端口的意外热插拔能力。		
	链路速度配置,菜单选项为:		
	● Auto (缺省)		
Link Speed	• Gen 1 (2.5 GT/s)		
	• Gen 2 (5 GT/s)		
	• Gen 3 (8 GT/s)		
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。		

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

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 <u>表</u> 3-64 所示。





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





Socket Configurat:	ion
▶ Processor 2 PcieBr1D00F0 – Port 1A ▶ Processor 2 PcieBr2D00F0 – Port 2A ▶ Processor 2 PcieBr2D02F0 – Port 2C	Settings related to PCI express ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3 B/3C/3D/4A/5A)
	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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。



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

	Socket Configuration	n <mark>en en e</mark>
Processor 2 PcieBr1D00F0 – Port 14 PCI-E Port Hot Plug Capable	(Auto) [Disabled]	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to
Surprise Hot Plug Capable Link Speed PCI-E Port Link Status PCI-E Port Link Max PCI-E Port Link Speed	[Disabled] [Auto] Link Did Not Train Max Width x8 Link Did Not Train	disable the port and hide its CFG space.
		++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults
		F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

界面参数	功能说明		
	PCI-E端口开关,菜单选项为:		
	● Auto (缺省): 自动选择。		
	● Enabled: 开启 PCI-E 端口。		
	• Disabled:关闭 PCI-E 端口,用于关闭端口和隐藏配置空间。		
	热插拔能力配置,菜单选项为:		
Hot Plug Capable	• Enabled: 开启该 PCIe 端口的热插拔能力。		
	• Disabled:关闭该 PCIe 端口的热插拔能力。		
	意外热插拔能力配置,菜单选项为:		
Surprise Hot Plug Capable	• Enabled: 开启该 PCIe 端口的意外热插拔能力。		
	• Disabled: 关闭该 PCIe 端口的意外热插拔能力。		
	链路速度配置,菜单选项为:		
	● Auto (缺省)		
Link Speed	• Gen 1 (2.5 GT/s)		
	• Gen 2 (5 GT/s)		
	• Gen 3 (8 GT/s)		
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。		

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

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
	Inter v i		" U	(1 0/	- アド曲

Socket Configuration	
Intel® VT for Directed I/O (VT-d)	Enable/Disable Intel® virtualization technology for directed I/O (VT-d) by
Intel® VT for Directed I/O (VT-d) [Enabled]	<pre>reporting the I/O device assignment to VMM through DMAR ACPI tables. ++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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-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: Enabled(缺省):开启Intel VT-d功能。 	
Intel VI for Directed I/O (VI-d)		
	• Disabled:关闭 Intel VT-d 功能。	

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 <u>3-77</u>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

	Socket Configuration	
VMD Config for PStack0		Enable/Disable Intel volume management device technology
Intel® VMD for Volume Management Device for PStack0 VMD Config for PStack2	[AUTO]	n this stack(PStackO). Auto means VMD technology will be enabled when POST detected
Intel® VMD for Volume Management Device for PStack2	[Auto]	stack. Notes: This feature only support UEFI mode.
		<pre> ++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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	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:	
	• Disabled: 禁用此 PStack0 中英特尔®卷管理设备技术。	
	• Enabled: 启用此 PStack0 栈中英特尔®卷管理设备技术。	
	• 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。	
	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:	
Intel® VMD for Volume Management Device for PStack2	• Disabled: 禁用此 PStack2 中英特尔®卷管理设备技术。	
	• Enabled: 启用此 PStack2 栈中英特尔®卷管理设备技术。	
	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。	

Intel® VMD for Volume Management Device on Processor 2 界面如 图 <u>3-78</u>所示。具体参数说明 如 <u>表 3-69</u>所示。

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

	Socket Configura	tion
VMD Config for PStack1		Enable/Disable Intel volume management device technology
Device for PStack1 VMD Config for PStack2	[VISADIED]	means VMD technology will be enabled when POST detected
Intel® VMD for Volume Management Device for PStack2	[Disabled]	stack. Notes: This feature only support UEFI mode.
		↔: Select Screen ↑↓: Select Item Enter: Select
		+/-: Change Option ESC: Exit F1: General Help
		F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup
		<k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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	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:	
	• Disabled: 禁用此 PStack1 栈中英特尔®卷管理设备技术。	
	• Enabled: 启用此 PStack1 栈中英特尔®卷管理设备技术。	
	• 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。	
Intel® VMD for Volume Management Device for PStack2	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:	
	• Disabled: 禁用此 PStack2 栈中英特尔®卷管理设备技术。	
	• Enabled: 启用此 PStack2 栈中英特尔®卷管理设备技术。	
	• 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。	

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。

	Socket Configuration	
Advanced Power Management Configuration CPU P State Control CPU C State Control Package C State Control CPU Thermal Management CPU Advanced PM Tuning		P state control configuration sub menu, include turbo, XE and etc.
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

	Socket Configuration	
CPU P State Control		Enable/Disable EIST (P-States)
EIST (P-States) Turbo Mode	[Enabled] [Enabled]	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k></pre>

表3-71 CPU P State Control 界面参数

界面参数	功能说明	
	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:	
EIST (P-State)	• Enabled (缺省): 开启 EIST 功能。	
	• Disabled:关闭 EIST 功能。	
	Turbo模式开关,菜单选项为:	
Turbo Mode	● Enabled(缺省): 开启 Turbo 模式。	
	• Disabled:关闭 Turbo 模式。	

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

	Socket Configuration	
CPU C State Control		Core C1E auto promotion control. Takes effect after
Autonomous Core C-State CPU C6 Report Enhanced Halt State (C1E)	[Disabled] [Disabled] [Disabled]	reboot.
		++: Select Screen
		T4: Select Item Enter: Select
		+/−: Change Option ESC: Exit
		F1: General Help F2: Previous Values
		F3: Optimized Defaults F4: Save & Exit Setup
		<k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

表3-72 CPU C State Control 界面参数

界面参数	功能说明
	自主的CPU核的C状态,菜单选项为:
Autonomous Core C-State	• Enabled: 开启自主的 CPU 核的 C 状态。
	• Disabled (缺省):关闭自主的 CPU 核的 C 状态。
CPU C6 Report	向操作系统报告C6状态开关,菜单选项为:
	• Enabled: 开启向操作系统报告 C6 状态功能。
	• Disabled (缺省):关闭向操作系统报告 C6 状态功能。
	Auto
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。
	• Enabled: 开启 Enhanced Halt State 功能。
	• Disabled (缺省): 关闭 Enhanced Halt State 功能。

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

	Socket Configuration	
Package C State Control		Package C state limit
Package C State C2C3TT	[Auto] O	
		<pre> ++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards </m></k></pre>

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限制选项,菜单选项为:	
Package C State	• Auto (缺省):默认 C 状态,由 CPU 决定。	
	• (C0/C1 state):设置成 C0/C1 状态。	
	• C2 state: 设置成 C2 状态。	
	• C6(non Retention) state: 设置成 C6(非残留)状态。	
	• C6(Retention) state:设置成 C6(残留)状态。	
	• No Limit: 设置成无限制模式。	
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

Socket	Configuration
CPU Thermal Management	CPU T state setting
▶ CPU T State Control	++: Select Screen 11: Select Item Enter: Select +/-: Change Ontion
	ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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

	Socket Configuration	
CPU T State Control		Enable/Disable software
Software Controlled T-State [[isabled]	<pre>controlled T-State ++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-75 CPU T State Control 界面参数

界面参数	功能说明	
	启用/禁用软件控制 T 状态:	
Software Controlled T-States	• Enabled: 开启软件控制 T 状态功能。	
	• Disabled (缺省): 关闭软件控制 T 状态功能。	

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

Socket Configure	ation
CPU Advanced PM Tuning	Provides option for CPU to get
▶ Energy Perf BIAS	savings.
	<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

Aptio Setup Utility -	Copyright (C) 2017 American Socket Configuration	Megatrends, Inc.
Energy Perf BIAS Power Performance Tuning ENERGY_PERF_BIAS_CFG Mode	[BIOS Controls EPB] [Performance]	Select whether BIOS or operating system chooses energy performance bias tunning.
		<pre>→+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-77 Energy Perf BIAS 界面参数

界面参数	功能说明	
Energy Performance Tuning	选择BIOS或者OS进行CPU的节能性能调整,菜单选项为:	
	• OS Controls EPB:选择 OS 进行 CPU 的节能性能调整。	
	• BIOS Controls EPB (缺省):选择 BIOS 进行 CPU 的节能性能调整。	
	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:	
ENERGY_PERF_BIAS_CFG Mode	• Performance (缺省):性能优先。	
	• Balanced Performance: 平衡性能。	
	• Balanced Power: 平衡功耗。	
	• Power: 节能优先。	

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

Main Advanced Platform	Configuration Socket Configuration	on Server Management Security
Wait for HDM 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 Load HDM Default Firmware Information	[Disabled] [Enabled] [15 Minutes] [Do Nothing] [Disabled] [10 Minutes] [Reset]	Displays the mapping of HDD slot number and silkscreen.
AC Restore Settings	[Restore Last Power State]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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:
	• Enabled: 开启等待 HDM 功能。
	• Disabled (缺省): 关闭等待 HDM 功能。
FRB-2 Timer	FRB-2时钟设置,菜单选项为:
	• Enabled (缺省): 启用 FRB-2 时钟。
	• Disabled: 禁用 FRB-2 时钟。
	FRB-2时钟到期时间设置,菜单选项为:
	• 3 Minutes
	• 4 Minutes
	• 5 Minutes
	6 Minutes
	• 10 Minutes
	● 15 Minutes(缺省)
	20 Minutes

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:	
	• Do Nothing (缺省):无动作。	
	• Reset: 立即重启。	
	• Power Down:正常关机。	
	• Power Cycle : 关机并重新开机。	
	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,	
OS Watchdog Timer		
	● Enabled: 开启 OS 看门狗定时器。	
	● Disabled(缺省): 天闭 OS 有门狗定时器。	
	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:	
	• 5 Minutes	
OS wid filmer filmeout	● 10 Minutes(缺省)	
	• 15 Minutes	
	20 Minutes	
	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:	
	• Do Nothing: 无动作。	
OS Wtd Timer Policy	• Reset (缺省): 立即重启。	
	• Power Down:正常关机。	
	• Power Cycle: 关机并重新开机。	
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	
	恢复HDM的出厂配置	
Load HDM Default	注意:按Enter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恢复配置状态设置,菜单选项为:	
	• Always Power On:系统处于工作状态。	
AC Restore Settings	• Always Remain Off: 系统处于关机状态。	
	• Restore Last Power State (缺省):保持上次断电时的状态。	
	需要注意的是:AC Restore Settings的缺省项与HDM的设置有关。	

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

		Server Management
Enabling/Disabling Options SEL Components	[Enabled]	Change this to enable/disable all features of system event
Erasing Settings Erase SEL	[No]	logging during boot.
Custom EFI Logging Options Log EFI Status Codes	[Error code]	
NOTE: All values changed here do not computer is restarted.	take effect until	
		<pre> ++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <h>: Scroll help area downwards</h></k></pre>

表3-79 System Event Log 界面参数

界面参数	功能说明
Enabling/Disabling Options	
	SEL组件开关设置,菜单选项为:
SEL Components	• Enabled (缺省): 启用 SEL 组件。
	• Disabled: 禁用 SEL 组件。
Erasing Settings	
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:
	• No (缺省):不擦除系统事件日志。
	• Yes, On next reset: 下次重启擦除系统事件日志。
	• Yes, On every reset: 每次重启擦除系统事件日志。
Custom EFI Logging Options	
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:
	• Disabled: 禁用记录 EFI 状态代码。
	• Both: 同时记录 EFI 错误码和进程码。
	• Error Code (缺省): 只记录 EFI 错误码。
	• Progress Code: 只记录 EFI 进程码。

💕 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

		Server Management
——HDM Network Configuration—— жножжжжжжжжжжжж Configure IPV4 Support жножжжжжжжжж		Enable/Disable Bond Mode
Bond Mode Setting	[Disabled]	
HDM Shared Network Port Configuration Address Source Current Configuration Address Source Station IP Address Subnet Mask Station MAC address Router IP Address Router IP Address Router MAC Address HDM Dedicated Network Port Configuration Address	[Unspecified] DynamicAddressHdmDhcp 0.0.0.0 0.0.00 00-00-00-00-00-00 0.0.0.0 00-00-00-00-00-00 [Unspecified] StaticAddress	++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help
Source		F2: Previous Values
Station IP Address	192.168.1.2	F3: Optimized Defaults
Subnet Mask	255.255.255.0	F4: Save & Exit Setup
Station MAC address	00-00-00-00-00	<k>: Scroll help area upwards</k>
Router IP Address	0.0.0.0	<m>: Scroll help area downwards</m>
Router MAC Address	00-00-00-00-00	

表3-80	HDM	Network	Configuration	界面参数
-------	-----	---------	---------------	------

界面参数	功能说明
	Bond模式配置,菜单选项为:
	 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。
	• Disabled(缺省):关闭 Bond 模式。
Bond Mode Setting	需要注意的是,开启该模式后:
	 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。
	• BIOS 启动界面仅显示 HDM Bonding 网络接口的 IP 地址。

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	
	• Unspecified (缺省): 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。	
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 <u>3-90</u>所示。具体参数说明如 <u>表 3-81</u>所示。

图3-90 HDM User Settings 界面

	Server Management
HDM User Settings	Press <enter> to add a user.</enter>
▶ Add User	
▶ Delete User	
▶ Change User Settings	<pre>**: Select Screen f1: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

		Server Management
HDM Add User Details User Name User Password User Privilege Limit Access to HDM	[None] [Default]	Enter HDM user name, the length range of user name to be created is 1~16 characters, only support letters, digits and underline, case sensitive.
		<pre> ++: Select Screen f↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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。	
	HDM用户的密码。	
	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。	
	 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。 	
	 密码长度为8~16个字符,仅支持字母、数字、空格和特殊字符`~!@#\$%^&*()_+-=[]\{};:",./<>?,区分大小写; 	
Liser Password	。 至少包含大写字母、小写字母和数字中的两种字符;	
User Fassword	o 至少包含一个空格或特殊字符;	
	o 不能与用户名或用户名的倒序相同。	
	 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。 	
	 密码长度为 2~16 个字符, 仅支持字母、数字、空格和特殊字符`~!@#\$%^&*()_+-=[]\{};':",./<>?, 区分大小写。 	
	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。	
	HDM用户权限,菜单选项为:	
	• None (缺省):保留当前的 HDM 用户权限。	
User Privilege Limit	● User: 用户权限。	
	● Operator:操作员权限。	
	• Administrator: 管理员权限。	
	用户访问开关,菜单选项为:	
	● Enabled:开启用户访问功能。	
Access to HDM	● Disabled:关闭用户访问功能。	
	• Default (缺省): 保留上次保存的用户访问权限。	

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

	Server Management
HDM Delete User Details	Enter HDM user name.
User Name User Password	
	<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-83 Delete User 界面参数

界面参数	功能说明
User Name	己创建的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

		Server Management
HDM Change User Settings		Enter HDM user name.
User Password Access to HDM Change User Password	[Default]	
User Privilege Limit	[None]	
		↔: Select Screen tl: Select Item
		Enter: Select +/-: Change Option
		ESC: Exit F1: General Help
		F2: Previous Values F3: Optimized Defaults
		F4: Save & Exit Setup <k>: Scroll help area upwards</k>
		<m>: Scroll help area downwards</m>

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	
	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:	
Access to HDM	• Enabled: 开启用户访问功能。	
	• Disabled: 关闭用户访问功能。	
	• Default (缺省): 保留上次保存的用户访问权限。	

界面参数	功能说明	
Change User Password	 修改HDM用户的密码,输入正确的HDM用户名和密码后,该选项可用。 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。 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。 密码长度为8~16个字符,仅支持字母、数字、空格和特殊字符`~!@#\$%^&*()_++=[]\{} ;'.",/<>?,区分大小写; 至少包含一个空格或特殊字符; 不能与用户名或用户名的倒序相同。 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。 密码长度为2~16个字符,仅支持字母、数字、空格和特殊字符`~!@#\$%^&*()_++=[]\{} ;'.",/<>?,区分大小写。 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。 	
User Privilege Limit	修改HDM用户权限,输入正确的HDM用户名和密码后,该选项可用,菜 单选项为: None(缺省):保留当前的 HDM 用户权限。 User:用户权限。 Operator:操作员权限。 Administrator:管理员权限。	

Firmware Information界面如 图 3-94 所示。具体参数说明如 表 3-85 所示。

图3-94 Firmware Information 界面

		Server Management
BIOS Information BIOS Vendor Compliancy Project Name BIOS Version Build Date and Time	American Megatrends UEFI 2.5; PI 1.4 C35 1.00.18 08/15/2017 13:26:09	
HDM Information HDM Self Test Status HDM Device ID HDM Device Revision HDM Firmware Revision IPMI Version	PASSED 32 1 1.10.17 2.0	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-85	Firmware	Information	界面参数
-------	----------	-------------	------

界面参数	功能说明	
BIOS Information		
BIOS Vendor	显示BIOS供应商	
Compliancy	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	
HDM Information		
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

		Server Management
HDD Slot Number and Silkscreen Mappin	ng	*
····	BIOS(Port) Silkscree	en 📕
8LFF	0-7 0-7	
Connecting 4LEE:		
4LFF(Front)	0-3 0-3	
2SFF(Rear)	4-5 1-2	
Connecting 8SFF:		
8SFF(Front)		
23FF(Front)+R3TE(3HTH) 29FF(Front)+R9Te(c9ATA)	0-0(V-1) 0-0 8-9(2-3) 8-9	
Zarr (rront) =Nate(sarin)	0-9(2-8) 0-9	
Connecting 4NVME+4SFF HDD:		++: Select Screen
4NVME+Retimer	0-3 0-3	↑↓: Select Item
4SFF HDD+RSTe(SATA)	4-7(0-3) 4-7	Enter: Select
4SFF HDD+RAID/HBA	4-7 4-7	+/-: Change Option
		ESC: Exit
Connecting 8LFF HDD+4NVME:		F1: General Help
8LFF HDD	0-7 0-7	F2: Previous Values
4NVME+Retimer	8-11(0-3) 8-11	F3: Optimized Defaults
Connecting 12LEE SATA HDD:		KX: Scroll beln area unwards
8I FE+RSTe(SATA)	0-7 0-7	<pre>(<) def dif help area downwards (</pre>
4LFF+RSTe(sSATA)	8-11(2-5) 8-11	

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	
Connecting 4LFF		
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。	
Connecting 8SFF		
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。	
Connecting 4NVME+4SFF HDD		
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。	
Connecting 8LFF HDD+4NVME		
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。	
Connecting 12LFF SATA HDD		
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。	
Connecting 8NVME		
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。	
Connecting 10SFF		
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。	
Connecting 12LFF		
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。	
Connecting 25SFF		
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"<u>4_SATA sSATA端口与背板槽位的对</u>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

Main Advanced Platform Con	figuration Socket Configuration	Server Management Security
Password Description		Set administrator password
If only the administrator's pa limits access to Setup, iFIST this is asked for when enterin PXE Boot. If only the user's password is password and must be entered will have administrator rights When both password are set, if have the rights according to the same, user will have admin The nassword length must be in	assword is set,then this , Boot Menu and PXE Boot; and ng Setup, iFIST, Boot Menu and s set, then this is a power on to boot. In Setup the user s. they are different,user will the login password,if they are istrator rights. the following range:	
Minimum Length	8	++: Select Screen
Maximum Length	20	↑↓: Select Item
Administrator Password User Password		Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults
HDD Security Configuration:		F4: Save & Exit Setup
P3:SAMSUNG MZ7LM240HCGR-00005		<k>: Scroll help area upwards</k>
▶ Secure Boot Menu		<m>: Scroll help area downwards</m>

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 Sottings	Enable ACPI Auto Configuration	灰显	
	ACFI Settings	Lock Legacy Resources	灰显	
	PCI Subsystem	Above 4G Decoding	灰显	
	Settings	SR-IOV Support		
	USB Configuration	Legacy USB Support		
		XHCI Hand-off		
		USB Mass Storage Device Support		
	Wait for HDM			
	FRB-2 Timer			
	FRB-2 Timer Timeout		灰显	
	FRB-2 Timer Policy			
	OS Watchdog Timer			
Server Mgmt	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

			Security
HDD Password Description : Allows access to set, modify and clear hard disk user passwords.'Set user password' need to installed for enabling security. If the 'Set User Password' option is grayed out,do power cycle to enable the option again. NOTE: all disks have same password.Use below option to configure all HDDs. HDD Password Configuration:		Set HDD User Password. *** Advisable to power cycle system after setting hard disk passwords ***. Discard or save changes option in setup does not have any impact on HDD when password is set or removed. If the 'Set User Password' option is grayed out, do power cycle to enable the option again	
Security Supported Security Enabled Security Locked Security Frozen HDD User Pwd Status Set User Password	: : : : : : : : : : : : : : : : : : : :	Yes No No NOT INSTALLED	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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,Yes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。No表示硬盘未 设置用户密码。
Security Locked	显示硬盘安全锁的状态,Yes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。No表示硬盘未被锁定。
Security Frozen	显示硬盘的冻结状态,Yes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。No表示硬盘未被冻结。
HDD User Pwd Status	显示硬盘用户密码的状态,Not Installed表示未设置硬盘用户密码。 Installed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

		Security
System Mode Secure Boot Vendor Keys Attempt Secure Boot Secure Boot Mode ▶ Key Management	Setup Not Active Not Modified [Disabled] [Customized]	Secure Boot can be enabled if 1.System running in user mode with enrolled platform key(PK) 2.CSM function is disabled.
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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	显示供应商秘钥
Attempt Secure Boot	 安全启动配置,菜单选项为: Enabled:开启安全启动。同时满足以下两种情况时开启安全启动。 。系统运行在注册平台秘钥的用户模式。 。CSM(兼容性支持模块)功能未开启。 Disabled(缺省):关闭安全启动。
Secure Boot Mode	安全启动模式配置,菜单选项为: Standard:标准模式。 Customized(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秘钥。
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

		Security
Provision Factory Default Keys [D ▶ Install Factory Default Keys ▶ Save All Secure Boot Variables)isabled]	Allow to provision factory default secure boot keys when system is in setup mode
Secure Boot Variable Size Keys# Ke Platform Key(PK) 0 0 No Key Exchange Keys 0 0 No Authorized Signatures 0 0 No Forbidden Signatures 0 0 No Authorized TimeStamps 0 0 No OSRecovery Signatures 0 0 No	ey Source 5 Key 5 Key 5 Key 6 Key 6 Key 6 Key	
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-91 Key Management 界面参数

界面参数	功能说明		
	提供出厂默认秘钥,菜单选项为:		
Provision Factory Default Keys	• Enabled:提供出厂默认秘钥。		
	• Disabled (缺省): 不提供出厂默认秘钥。		
Install Factory Default Keys	注册所有的出厂默认秘钥,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)	平台秘钥配置,菜单选项为:		
	• Set New Var: 设置新的秘钥。		
	交换秘钥设置,菜单选项为:		
Key Exchange Keys	• Set New Var: 设置新的秘钥。		
	● Append Key: 添加秘钥。		
	经授权的签名,菜单选项为:		
Authorized Signatures	• Set New Var: 设置新的秘钥。		
	• Append Key: 添加秘钥。		

界面参数	功能说明	
	被禁止的签名,菜单选项为:	
Forbidden Signatures	• Set New Var: 设置新的秘钥。	
	● Append Key: 添加秘钥。	
	经授权的时间戳,菜单选项为:	
Authorized TimeStamps	• Set New Var: 设置新的秘钥。	
	● Append Key: 添加秘钥。	
	系统恢复的签名,菜单选项为:	
OsRecovery Signatures	• Set New Var: 设置新的秘钥。	
	● Append Key: 添加秘钥。	

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。

◀ Boot Save & Exit		
Boot Configuration Setup Prompt Timeout Bootup NumLock State	1 [0n]	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite
Quiet Boot Boot mode select	[Disabled] [UEFI]	waiting,it ranges from 1 to 65535
Fixed Boot Order Priorities		
Boot Option #1	[Hard Disk:CentOS (Slot10 Mezz HBA Drives 2)]	
Boot Option #2	[Network:UEFI: IPv4 Slot9-mLOM:Port 1 - Intel(R) Ethernet Connection X722 for 1GbE]	→+: Select Screen ↑↓: Select Item Enter: Select
Boot Option #3	[USB Hard Disk]	+/-: Change Option
Boot Option #4	[USB_CD/DVD]	ESC: Exit
Boot Option #5	[USB Key]	F1: General Help
Boot Option #6	[USB Floppy]	F2: Previous Values
Boot Option #7	[CD/DVD]	F3: Optimized Defaults
Boot Option #8	[UEFI AP]	F4: Save & Exit Setup
NUTET Used Disk Dailys DDD Dailys itigs		<k>: Scroll help area upwards</k>
UEFI Hard Disk Drive BBS Priorities		<m>: Scroll help area downwards</m>
DEFI NETWORK UPIVE BBS Priorities		

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: On(缺省):打开启动后键盘上数字锁定键状态。 Off:关闭启动后键盘上数字锁定键状态。
Quiet Boot	以安静模式启动系统,菜单选项为: Enabled:开启安静启动设置。 Disabled(缺省):关闭安静启动设置。
Boot Mode Select	 启动模式选择设置,菜单选项为: Legacy: Legacy 启动模式。 UEFI(缺省): UEFI 启动模式。
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

◀ Boot Save & Exit		
Boot Configuration Setup Prompt Timeout Bootup NumLock State Quiet Boot	1 [On] [Disabled]	Sets the system boot order
Boot mode select	[UEFI]	
Fixed Boot Order Priorities		
Boot Option #1	[Hard Disk:CentOS (Slot10 Mezz HBA Drives 2)]	
Boot Option #2	[Network:UEFI: IPv4 Slot9-mLOM:Port 1 - Intel(R) Ethernet Connection X722 for 1GbE]	↔: Select Screen †↓: Select Item Enter: Select
Boot Option #3	[USB Hard Disk]	+/-: Change Option
Boot Option #4	[USB CD/DVD]	ESC: Exit
Boot Option #5	[USB Key]	F1: General Help
Boot Option #6	[USB Floppy]	F2: Previous Values
Boot Option #7		F3: Optimized Defaults
Boot uption #8	[UEFI AP]	<pre>K>: Save & Exit Setup K>: Scroll help area upwards</pre>
UEFI Hard Disk Drive BBS Priorities		<m>: Scroll help area downwards</m>
▶ UEFI Network Drive BBS Priorities	•••	

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。

Boot Boot		
Boot Option #1 [F (F M2	edHat Boot Manager 3: SAMSUNG 7LM240HCGR-00005)]	Sets the system boot order ++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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。

		Boot	
Boot Option #1	[UEFI: hp DU8D5SH]	DVD D	Sets the system boot order.
			<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Option F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup ESC: Exit <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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。

	Boot	
Boot Option #1	[UEFI: hp x705w 1.00, Partition 1]	Sets the system boot order.
		++: Select Screen 11: Select Item Enter: Select +/-: Change Option F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup ESC: Exit <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k>

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。

	Boot	
Boot Option #1	[UEFI: H3C Virtual CDROMO 1 OO]	Sets the system boot order.
Boot Option #2	[UEFI: H3C Virtual CDROM1 1.00]	
		<pre> ++: Select Screen 14: Select Item Enter: Select +/-: Change Option F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup ESC: Exit <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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。

	Boot Boot	
Boot Option #1	[UEFI: hp x705w 1100, Partition 1]	Sets the system boot order.
		<pre> ++: Select Screen 14: Select Item Enter: Select +/-: Change Option F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup ESC: Exit <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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。

	Boot	
Boot Option #1	[UEFI: NEC USB UF000x 1.50]	Sets the system boot order.
		<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Option F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup ESC: Exit <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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

	Boot Boot	
Boot Option #1	[UEFI: IPv4 ▲ Sets the system boot order Embedded:Port 1 - Intel(R) I350 Gigabit	`•
Boot Option #2	[UEFI: IPv4 Embedded:Port 2 – Intel(R) I350 Gigabit Network Connection]	
Boot Option #3	[UEFI: IPv4 Embedded:Port 3 – Intel(R) I350 Gigabit Network Connection]	
Boot Option #4	[UEFI: IPv4 Embedded:Port 4 - Intel(R) I350 Gigabit 11: Select Item Network Connection]	
Boot Option #5	[UEFI: IPv6+/-: Change OptionEmbedded:Port 1 -F1: General HelpIntel(R) I350 GigabitF2: Previous ValuesNetwork Connection]F3: Optimized Defaults	
Boot Option #6	[UEFI: IPv6 Embedded:Port 2 – Intel(R) I350 Gigabit Network Connection]	ards wards

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。

	Boot	
Boot Option #1	[UEFI: Built-in EFI Shell]	Sets the system boot order.
		<pre>++: Select Screen f4: Select Item Enter: Select +/-: Change Option F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup ESC: Exit <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

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 <u>表</u> 3-102 所示。

图3-110 Save & Exit 界面

BUUL SAVE & EXIL	
Save Options Save Changes and Exit Discard Changes and Exit	Exit system setup after saving the changes.
Save Changes and Reset Discard Changes and Reset	
Save Changes Discard Changes	
Default Options Restore Defaults	
Boot Override Windows Boot Manager (P7: SAMSUNG MZ7LM240HCGR-00005) UEFI: IPv4 Slot 3:Port 1 - Intel(R) Ethernet Controller X550 UEFI: IPv4 Slot9-mLOM:Port 1 - Intel(R) Ethernet Connection X722 for 1GbE UEFI: IPv4 Slot9-mLOM:Port 2 - Intel(R) Ethernet Connection X722 for 1GbE UEFI: IPv4 Slot9-mLOM:Port 3 - Intel(R) Ethernet Connection X722 for 1GbE	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Option ESC: Exit F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit Setup <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>

表3-102 Save & Exit 界面参数

界面参数	功能说明
Save Options	
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
Default Options	
Restore Defaults	恢复缺省设置
	选择从以下启动项启动。您也可以通过在BIOS启动界面(图2-2)按F7进入Boot Menu界面,选择对应的启动项。
	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 & Reset对话框,在对话框中,可执行以下操作:
Boot Override	 Yes: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。
	 No: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 图 3-110 中的Discard Changes或按F2 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。

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。



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	PCle槽位2(存储适配卡)	未使用PCH SATA sSATA端口,不显示
配置四	PCle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+PCle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)+PCle 槽位2(NVMe4 端口适配卡)	未使用PCH SATA sSATA端口,不显示
配置三	PCle槽位6(存储适配卡)+PCle 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	PCle槽位2(存储适配卡)	未使用PCH SATA sSATA端口,不显示
配置四	PCle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+PCle 槽位5(NVMe 4 端口适配卡)+PCle 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)+PCle 槽位5(NVMe 4端口适配卡)+PCle 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)+PCle 槽位2(NVMe 8端口适配卡)	未使用PCH SATA sSATA端口,不显示
配置五	PCle槽位6(存储适配卡)+PCle 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+PCle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)+PCle槽位1(NVMe 4端口适配卡)	未使用PCH SATA sSATA端口,不显示
配置三	PCle槽位1(存储适配卡)+PCle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) + PCle槽位1 (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	PCle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4-8 H3C UniServer R4700 G3 8SFF HDD 机型

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	PCle 槽位2(存储适配卡)	未使用PCH SATA sSATA端口,不显示
配置四	PCle 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)+PCle 槽位2(NVMe 4端口适配卡)	未使用PCH SATA sSATA端口,不显示
配置三	PCle 槽位6(存储适配卡)+ PCle 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	PCle 槽位2(存储适配卡)	未使用PCH SATA sSATA端口,不显示
配置四	PCle 槽位6(存储适配卡)	未使用PCH SATA sSATA端口,不显示

配置	硬盘数据线缆	说明
配置一	底板PCH Mini SAS J11+PCle 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+PCle 槽位5 (NVMe 4 端口适配卡)+PCle 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)+PCle 槽位5(NVMe 4端口适配卡)+PCle 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)+PCle 槽位2(NVMe 8端口适配卡)	未使用PCH SATA sSATA端口,不显示
配置五	PCle 槽位6(存储适配卡)+PCle 槽位5(NVMe 8端口适配卡)	未使用PCH SATA sSATA端口,不显示

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

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)+PCle 槽位1(NVMe 4端口适配卡)	未使用PCH SATA sSATA端口,不显示
配置三	PCle 槽位1(存储适配卡)+ PCle 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) + PCle 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	PCle 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



表5-1 缩略语

缩略语	英文解释	中文解释
Α	1	1
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
В		
BIOS	Basic Input Output System	基本输入输出系统
С		
COD	Cluster On Die	芯片集群
CFG	Config	配置
CSM	Compatibility Support Module	兼容性支持模块
D		
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
E		
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
G		<u>.</u>
GPU	Graphics Processing Unit	图形处理器
Н		
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
I	1	
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
М		
MAC	Media Access Control	介质访问控制
МСТР	Management Component Transport Protocol	管理元件传输协议
ME	Management Engine	管理引擎
ΜΜΙΟ	Memory mapping I/O	内存映射I/O
MRC	Memory Reference Code	内存参考代码
Ν		
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
0		
OS	Operating System	操作系统
Р	1	
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
РК	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
R		
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
S		
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
т		
TCG	Trusted Computing Group	可信计算组织
TDP	Thermal Design Power	热设计功耗
ТРМ	Trusted Platform Module	可信平台模块
ТХТ	Trusted Execution Technologies	可信执行技术
U		
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
V		
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
X		
XHCI	eXtensible Host Controller Interface	可扩展的主机控制器接口