

浪潮英信服务器 BIOS 用户手册

文档版本 V2.3

发布日期 2023-03-10

版权所有 © 2021-2023 浪潮电子信息产业股份有限公司。保留一切权利。

未经本公司事先书面许可,任何单位和个人不得以任何形式复制、传播本手册的部分或 全部内容。

环境保护

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

商标说明

Inspur 浪潮、Inspur、浪潮、英信是浪潮集团有限公司的注册商标。 本手册中提及的其他所有商标或注册商标,由各自的所有人拥有。

内容声明

您购买的产品、服务或特性等应受浪潮集团商业合同和条款的约束。本文档中描述的全 部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定,浪 潮集团对本文档的所有内容不做任何明示或默示的声明或保证。文档中的示意图与产品 实物可能有差别,请以实物为准。本文档仅作为使用指导,不对使用我们产品之前、期 间或之后发生的任何损害负责,包括但不限于利益损失、信息丢失、业务中断、人身伤 害,或其他任何间接损失。本文档默认读者对服务器产品有足够的认识,获得了足够的 培训,在操作、维护过程中不会造成个人伤害或产品损坏。文档所含内容如有升级或更 新,恕不另行通知。

技术支持

客户服务电话: 4008600011

地 址:中国济南市浪潮路 1036 号

浪潮电子信息产业股份有限公司

- 邮 箱: <u>lckf@inspur.com</u>
- 邮 编: 250101



摘要

本手册介绍服务器 BIOS 设置的相关内容。

目标受众

本手册主要适用于以下人员:

- 技术支持工程师
- 产品维护工程师

建议由具备服务器知识的专业工程师参考本手册进行服务器运维操作。

符号约定

在本文中可能出现下列标志,它们所代表的含义如下。

图标	说明
人 危险	如不当操作,可能会导致死亡或严重的人身伤害。
▲ 警告	如不当操作,可能会导致中度或轻微的人身伤害。
1 注意	如不当操作,可能会导致设备损坏或数据丢失。
1 提示	为确保设备成功安装或配置,而需要特别关注的操作或信息。
目说明	对手册内容的描述进行必要的补充和说明。

变更记录

版本	时间	变更内容		
V1.0	2021-04-19	首版发布		
V1.1	2021-05-25	优化文档描述		
V2.0	2022-02-14	 调整文档章节顺序 补充BIOS配置操作的必要细节 		
V2.1	2022-07-25	优化文档描述		
V2.2	2022-10-12	"2.10 设置串口重定向功能"、"3.2.4 AST2500 Super IO Configuration""3.2.5 Serial Port Console Redirection"章节添加功能差异说明		
V2.3	2023-03-10	更新 "3.4.4.1 Memory Map"		

1	概述	<u>.</u> 1
	1.1	BIOS 简介1
	1.2	适用产品1
	1.3	注意事项2
2	常用	操作4
	2.1	进入 BIOS Setup 界面4
	2.2	查看系统配置信息6
	2.3	查看 CPU 详细信息7
	2.4	查看内存信息
	2.5	查看硬盘信息及 RAID 配置10
		2.5.1 查看硬盘信息10
		2.5.2 硬盘 RAID 模式配置12
	2.6	BMC 网络参数查看与设置17
		2.6.1 查看 BMC 网络参数17
		2.6.2 BMC 网络设置20
	2.7	设置 BIOS 系统语言27
	2.8	设置 BIOS 系统日期和时间27
	2.9	设置 PCle 端口
	2.10	设置串口重定向功能
	2.11	设置服务器启动模式
	2.12	设置服务器启动顺序
	2.13	恢复 BIOS 选项默认值37
3	BIO	S 参数说明

目 录

3.1	Main.		.40
3.2	Advar	nced	.41
	3.2.1	Hard Drive Temperature	.43
	3.2.2	Trusted Computing	.43
	3.2.3	Redfish Host Interface Settings	.46
	3.2.4	AST2500 Super IO Configuration	.47
	3.2.5	Serial Port Console Redirection	.50
	3.2.6	System Debug Configuration	.54
	3.2.7	PCI Subsystem Settings	.55
	3.2.8	USB Devices Information	.57
	3.2.9	Network Stack Configuration	.57
	3.2.10	CSM Configuration	. 59
	3.2.11	OEM NIC Oprom Ctrl	.61
	3.2.12	iSCSI Configuration	.62
	3.2.13	Driver Health	.63
3.3	Platfo	rm Configuration	.64
	3.3.1	PCH SATA Configuration/PCH sSATA Configuration	.65
	3.3.2	USB Configuration	.67
	3.3.3	Miscellaneous Configuration	.68
	3.3.4	Server ME Configuration	.69
	3.3.5	Runtime Error Logging	.71
3.4	Socke	t Configuration	.72
	3.4.1	Processor Configuration	.73
	3.4.2	Common RefCode Configuration	.79
	3.4.3	Uncore Configuration	.81
	3.4.4	Memory Configuration	.86
	3.4.5	IIO Configuration	.95

	3.4.6	Advanced Power Management Configuration1	02
3.5	Serve	r Mgmt1	15
	3.5.1	BMC Network Configuration1	17
	3.5.2	BMC User Settings 1	22
	3.5.3	VLAN Configuration1	27
	3.5.4	View FRU information1	29
3.6	Secur	ity 1	30
	3.6.1	Secure Boot1	32
3.7	Boot	1	34
	3.7.1	Add New Boot Option1	35
	3.7.2	Delete Boot Option1	36
3.8	Save	& Exit	37
固件	=更新		39

1 概述

1.1 BIOS 简介

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

图 1-1 BIOS 在系统中的位置



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

1.2 适用产品

本手册适用于以下产品:

产品型号	两路服务器	四路服务器	AI服务器	多节点服务器
浪潮英信服务器				
NF8260M6		•		
浪潮英信服务器				
NF8480M6		•		
浪潮英信服务器				
SN5160FM6	-			

产品型号	两路服务器	四路服务器	AI服务器	多节点服务器
浪潮英信服务器				
SN5264FM6	•			
浪潮英信服务器				
NF5280M6	•			
浪潮英信服务器				
NF5180M6	•			
浪潮英信服务器				
NF5270M6	•			
浪潮英信服务器				
NF5260M6	•			
浪潮英信服务器				
NF5260FM6	•			
浪潮英信服务器				
NF5466M6	•			
浪潮英信服务器				
NF5266M6	•			
浪潮英信服务器				
NF5468M6	•		•	
浪潮英信服务器				
NF5488M6	•		•	
浪潮英信服务器				
NF5688M6	•		•	
浪潮英信服务器i24M6	•			•
浪潮英信服务器i24LM6	•			•
浪潮英信服务器i48M6	•			•

1.3 注意事项

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

- 在改变服务器 BIOS 设置前,请记录下相应的初始设置,以便在因修改选项而出现系统
 工作异常时,可以根据记录的初始设置重新恢复。
- 通常系统出厂默认设置都是最优化设置。在未理解各参数表示的意义前,请勿试图进行 更改。
- 本文档主要对常用设置作详细说明。使用过程中较少涉及的选项仅作简单说明或未作说 明。



2.1 进入 BIOS Setup 界面

功能描述

该操作指导用户进入 BIOS Setup 界面。

操作说明

- 连接好电源并外接键盘、鼠标、显示器,或者进入 BMC Web 的远程控制台操作机器。
 进入 BMC Web 的远程控制台的具体操作步骤,请参考《浪潮英信服务器 BMC 用户手册》。
- 2. 将服务器上电开机。
- 3. 系统开始启动,屏幕出现 Logo 且下方提示 "Press to SETUP or <F11> to Boot Menu or <F12> to PXE Boot."时,按下"DEL",稍后会进入 BIOS Setup 界 面。

图 2-1 BIOS 启动界面





- 按 "F11" , 可进入启动管理界面。
- 按 "F12" , 进入网络 PXE 预引导环境。
- 因版本不同,启动界面显示的 Logo 可能存在差异,请以实际情况为准。
- 如果服务器的 System TF Card 插槽安装了 TF 卡,还会显示 "Press <F7> to TF Card Boot."。
- 如果当前 BIOS 版本没有放开 Logo 显示,当出现 "Press to Setup or <F11> to Boot Menu or <F12> to PXE Boot."时,按下 "Del"。按下 "Del"的时间不同, 屏幕的显示信息会有略微差异。

图 2-2 BIOS 启动界面(无 LOGO)



BIOS 菜单控制键说明,请参见下表。

表 2-1 BIOS Setup	界面控制键说明表
------------------	----------

按键	功能
<esc></esc>	退出或是从子菜单返回主菜单
<← >或<→ >	选择菜单
<1>或<↓>	移动光标到上或下
<home>或<end></end></home>	移动光标到屏幕顶部或是底部
<+>或<->	当前项的前一个或后一个数值
<f1></f1>	快捷键的帮助信息

按键	功能
<f2></f2>	恢复上次设置值
<f9></f9>	恢复默认设置
<f10></f10>	保存并退出
<enter></enter>	执行命令或选择子菜单
<k>或<m></m></k>	向上/下滚动帮助信息区域



- 置灰的选项表示在当前状态下不可被选中。
- 带有 "▶" 符号的项目,表示该选项包含子菜单。

2.2 查看系统配置信息

功能描述

该操作指导用户通过 BIOS 查看服务器的各项配置信息。

操作说明

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

图 2-3 Main 界面

Main Advanced Platform Cont	figuration Socket Configuration	n Server Mgmt Security Boot 🔹
Product Name Serial Number Customer ID	NF8480M6 O Barebone	Choose the system default language
BIOS Version Build Date BMC Firmware Version ME Firmware Version Access Level	4.08.02 10/26/2020 4.03.0E 0F:4.4.4.21 Administrator	
Platform Information CPU Type	4 * Intel(R) Genuine	
CPU Current Speed PCH SKU	2800MHz LBG SuperSKU - C621A - B3	↔: Select Screen ↓: Select Item Enter: Select
RC Revision DRAM Total Memory RRS Total Memory	17.P23 64 GB	+/-: Change Opt. F1: General Help
System Memory Speed	2933 MHz	F9: Optimized Defaults F10: Save & Exit
		ESC: Exit
System Date System Time	[Mon 10/26/2020] [08:21:41]	

2.3 查看 CPU 详细信息

功能描述

该操作指导用户通过 BIOS 查看服务器配置的 CPU 详细信息。

操作说明

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1 进入 BIOS Setup 界面"。
- 2. 选择 Socket Configuration 界面,如下图所示。

图 2-4 Socket Configuration 界面



3. 选择"Processor Configuration",按"Enter",查看 CPU 详细信息。

图 2-5 Processor Configuration 界面

	Socket	Configuratio	1
Processor Configuration			Active Cores Per CPU
Processor BSP Revision Processor Socket Processor Trequency Processor Max Ratio Processor Max Ratio Processor Min Ratio Microcode Revision L1 Cache RAM L2 Cache RAM L3 Cache RAM Processor Core Number Processor Socket Processor Voltage Processor Socket Processor Socket Processor Frequency Processor Frequency Processor Min Ratio Microcode Revision L1 Cache RAM L3 Cache RAM	5065B - CP) Socket 0 0005065B* 2.6006Hz 1AH 0AH 0700001E 644KB 36606KB 266 A1 1.6V Socket 2 0005065B 2.6006Hz 1AH 0AH 0700001E 64KB 1024KB 36608KB	<pre>4 A1 Socket 1 Socket 1 0005065B 2.6006Hz AAH 0AH 0700001E 64KB 1024KB 36606KB 266 A11 1.6V Socket 3 0005065B 2.6006Hz 1AH 0AH 0700001E 0AH 0AH 0700001E 1024KB 36608KB</pre>	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt, F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

2.4 查看内存信息

功能描述

该操作指导用户通过 BIOS 查看服务器配置的内存详细信息。

操作说明

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

图 2-6 Socket Configuration 界面

				Aptio Setup	- AMI			
	Main	Advanced	Platform	Configuration	Socket	Configuration	Server Mgmt	
* * * * * *	Proces Common Uncore Memory IIO Co Advanc	sor Config RefCode C Configura Configura nfiguratio ed Power M	uration onfigurati tion n anagement	on Configuration		Displays an option to c Processor S ++: Select 11: Select Enter: Sele +/-: Change F1: General F2: Previou F9: Optimiz F10: Save & ESC: Exit	d provides hange the ettings Screen Item ct Opt. Help s Values ed Defaults a Exit	
			Version 2	2.21.1278 Copyr	ight (C) 2021 AMI	A	нB
								_

3. 选择"Memory Configuration",按"Enter"进入。

图 2-7 Memory Configuration 界面

	Aptio Setup – A So	MI ocket Configuration	
SMB Clock Frequency SPD-SMBUS Access SPD Print Length DDR Cycling Mem Flows Mem FlowsExt Mem FlowsExt2 Mem FlowsExt3 BLOCK GNT2CMD1CYC Disable DDRT DIMM OPPRD Cmd Setup % Offset Periodic Rcomp Periodic Rcomp Interval Memory Topology Page Policy	So [700 Kh2] [Lock] [Disabled] [Auto] [Disabled] ffffffff ffffffff ffffffff [POR] [POR] [POR] [POR] 50 [Auto] [671.08864 ms]	 Sets DDR4 SMBus Clock Frequencies For SPD Access. Current defaul is 700Khz. Note: If Intel Optane Persister Memory (PMem) is present, SMBus Clock Frequency is restricter ++: Select Screen ++: Select Screen ++: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit 	lt nt ed ▼
Ver	Version 2.21.1278 Copyright (C) 2021 AMI		

4. 在界面下方找到"Memory Topology",按"Enter"进入,查看所插内存的厂商、 速率、容量等详细信息。

图 2-8 Memory Topology 界面

Socket Configuration	
CPU0_C0D0 : 2933MHz Hynix SRx4 16GB RDIMM CPU1_C0D0 : 2933MHz Hynix SRx4 16GB RDIMM CPU2_C0D0 : 2933MHz Hynix SRx4 16GB RDIMM CPU3_C0D0 : 2933MHz Hynix SRx4 16GB RDIMM	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>



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

2.5 查看硬盘信息及 RAID 配置

2.5.1 查看硬盘信息

功能描述

该操作指导用户通过 BIOS 查看服务器 PCH 直连硬盘的详细信息。

操作说明

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

图 2-9 Platform Configuration 界面

Aptio Setup – AMI		
Main Advanced Platform Configuration Socket	Configuration Server Mgmt ▶	
 PCH Configuration PCH SATA Configuration PCH sSATA Configuration USB Configuration Miscellaneous Configuration Server ME Configuration Server ME Debug Configuration Runtime Error Logging Reserve Memory 	Displays and provides option to change the PCH Settings ++: Select Screen fl: Select Item Enter: Select	
Setting items on this Screen to incorrect values may cause system to malfunction!	+/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.21.1279 Copyright (C) 2021 AMI AB		

选择 "PCH SATA Configuration" 或 "PCH sSATA Configuration",按 "Enter"进入,查看当前板载 SATA 端口或 sSATA 端口的硬盘详细信息。

图 2-10 PCH SATA Configuration 界面

Platform Co	nfiguration	
PCH SATA Configuration		Enable or Disable SATA Controller
SATA Controller Configure SATA as Sata 0 Port 0 Sata 1 Port 1 Sata 2 Port 2 Sata 3 Port 3	[Enabled] [AHCI] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled]	<pre>+*: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

图 2-11 PCH sSATA Configuration 界面

Platform Cor	nfiguration	
PCH sSATA Configuration		Enable or Disable sSATA Controller
sSATA Controller Configure sSATA as	[Enabled] [AHCI]	
Port 2 SSata 1 Port 4	(Enabled) [Not Installed] [Enabled]	
		++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

2.5.2 硬盘 RAID 模式配置

功能描述

该操作指导用户进行硬盘 RAID 模式配置。

操作说明

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

图 2-12 Platform Configuration 界面



3. 选择"PCH SATA Configuration"或"PCH sSATA Configuration",按"Enter"进入。

Platform Configu	ration	
Platform Configu PCH SATA Configuration SATA Controller Configure SATA as Sata 0 Port 0 Sata 1 Port 1 Sata 2 Port 2 Sata 3 Port 3	ration [Enabled] [AHCI] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled] [Not Installed] [Enabled]	Enable or Disable SATA Controller ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

图 2-13 PCH SATA Configuration 界面

图 2-14 PCH sSATA Configuration 界面

Platform Configuration			
PCH sSATA Configuration		Enable or Disable sSATA Controller	
sSATA Controller Configure sSATA as	[Enabled] [AHCI]		
sSata 0 Port 2 sSata 1 Port 4	LITEON EGT-240 – 240 GB [Enabled] [Not Installed] [Enabled]		
		+: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	

- 4. 选择 "Configure SATA as" 或 "Configure sSATA as" 选项,按 "Enter",在弹出的选项对话框中选择 "RAID",按 "F10",单击 "Yes",保存重启生效。
- 5. 服务器重启进入 BIOS Setup 界面,当选项"Boot option filter"为"UEFI Only"模式,在 Advanced 界面,会出现"Intel(R) VROC SATA Controller"或"Intel(R) VROC sSATA Controller"选项。

图 2-15 Advanced 界面

 Hand Drive Temperature Trusted Computing Redfish Host Interface Settings Redfish Host Interface Settings Redfish Host Interface Settings Serial Port Console Redirection System Debug Configuration POI Subsystem Settings USB Devices Information OEM NIC Oprom Ctrl SiGSI Configuration OEM NIC Oprom Ctrl SiGSI Configuration Intel(R) VROC SATA Controller Driver Health Driver Health 	Main Advanced Platform Configuration	Socket Configuration	Server Mgmt Security Boot 🕨
	 Hand Drive Temperature Trusted Computing Reddish Host Interface Settings AST2500 Super 10 Configuration Serial Port Console Redirection System Debug Configuration PCI Subsystem Settings USB Devices Information Network Stack Configuration CSM Configuration GSM Configuration DEH NIC Oprom Ctrl ISCSI Configuration Intel(R) VROC SATA Controller Intel(R) VROC SATA Controller Oriver Health 		Displays Hand drive SMART Information ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit



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

- 选择 "Intel(R) VROC SATA Controller" 或 "Intel(R) VROC sSATA Controller",按 "Enter"进入,显示可执行操作及当前的硬盘信息。
 - 图 2-16 Intel(R) VROC SATA Controller 界面



1. 创建 RAID 模式

选择"Create RAID Volume"选项,按"Enter"进入,具体选项操作说明请参考

"Create RAID 选项操作说明表"。

图 2-17 Create RAID Volume 界面 2-1

Advanced		
Create RAID Volume		Enter a unique volume name that does not
		contain space at the
RAID Level:	[RAIDO(Stripe)]	beginning or backslash and is 16 characters or
Select Disks:		less.
Port 0, HGST	[]	
HUS726T4TALA6L4		
SN:V6G2S9ZN, 3726.02GB	1992).	and a second
Port 1, HGST	[]	
HUS 726141ALA6L4		++: Select Screen
SN:VEG2RGWN, 3726.02GB	r 1	I+: Select Item
PUPIC 2, HUST	LJ	Enter: Select
SN+V60250NN 3726 0208		F1: Ceneral Hain
Port 3 HGST	[]	E2: Previous Values
HUS726T4TALA6L4		F9: Ontimized Defaults
SN:V66253EN, 3726.026B		▼ F10: Save & Exit
		ESC: Exit

图 2-18 Create RAID Volume 界面 2-2

Advanced		
Port 5, HGST HUS726T4TALA6L4 SN:V662RXUN 3726 026B	[]	Create a volume with the settings specified above
Port 6, HGST HUS726T4TALA6L4 SN:V6G2RMZN, 3726.02GB	[X]	
Port 7, HGST HUS726T4TALA6L4 SN:V6G2RJHN, 3726.02GB	[X]	
Strip Size:	[128KB]	↔: Select Screen
Capacity (GB):	7079.43	†↓: Select Item
		Enter: Select
▶ Preste Volume		+/-: Change Opt.
• Greate Volume		F2: Previous Values
		F9: Optimized Defaults
	•	F10: Save & Exit
		ESU: EXIT

表 2-2 Create RAID 选项操作说明表

界面参数	功能说明
Name	请输入少于16个不包含特殊字符的名称。
	请选择RAID模式级别,如果目前还没有创建任何RAID,在此
RAID Level	有RAID0(Stripe)、RAID1(Mirror),RAID5(Parity)和

界面参数	功能说明
	RAID10(RAID0+1)四个级别可供选择,请根据实际需求选择
	级别。
	RAID0: RAID0
	• RAID1: RAID1
	• RAID5: RAID5, 至少需要3块以上硬盘
	• RAID10: RAID0+1, 需要4块硬盘
	选择要组建RAID模式的硬盘,按"Enter"键,选择"X",
Select Disks	然后按"Enter"键回到RAID模式创建界面,表示选中该硬
	盘。
Chrin Cine	请选择RAID的带大小,只有RAID0和RAID5模式才能选择该
Strip Size	项。
	输入需要设置的RAID容量大小,在右侧Help信息中可以看到
Capacity(GB)	最大容量信息。
Create Volume	设置完以上参数信息后,点击该选项创建RAID。

2. 删除 RAID 模式

选择已创建的 RAID Volume 选项,按"Enter"进入。选择"Delete",会进入 Delete 提示菜单,提示是否要删除 RAID 模式。如果删除,选择"Yes",按"Enter",如果不删除,选择"No",按"Enter"。

图 2-19 RAID Volume 界面

Advanced	
Intel(R) VROC 7.5.0.1030 SATA Driver	Select to see more information about the
▶ Create RAID Volume	RAID Volume
RAID Volumes:	
▶ VolumeO, RAIDO(Stripe), 7079.43GB, Normal	
▶ Volume1, RAIDO(Stripe), 7079.43GB, Normal	
▶ Volume2, RAIDO(Stripe), 7079.43GB, Normal	
▶ Volume3, RAIDO(Stripe), 7079.43GB, Normal	

图 2-20 RAID Volume Info 界面

Γ	RAID VOLUME INFO		
Þ	Volume Actions Delete		
	Name: RAID Level: Strip Size: Size: Status: Bootable: Block size:	Volume3 RAIDO(Stripe) 128KB 7079.436B Normal Yes 512	++: Select Screen †↓: Select Item
•	RAID Member Disks: Port 6, HGST HUS726T4TAL 3726.02GB Port 7, HGST HUS726T4TAL 3726.02GB	A6L4 SN∶V6G2RMZN, A6L4 SN∶V6G2RJHN,	<pre>Finter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

图 2-21 RAID Volume Delete 界面





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

2.6 BMC 网络参数查看与设置

2.6.1 查看 BMC 网络参数

功能描述

该操作指导用户通过 BIOS 查看服务器 BMC 管理网口的 IP 信息。

操作说明

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

图 2-22 Server Mgmt 界面

Main Advanced Platfor	Aptio Setup – m Configuration	AMI Socket Configuration Server Mgm	t 🕨
BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version IPMI BMC Interface	PASSED 32 1 4.11.0B 2.0 KCS	▲ Configure BMC network parameters	
BMC Support IPMI Interface Type Wait For BMC FRB-2 Timer FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer OS Wtd Timer Timeout OS Wtd Timer Policy Serial Mux BMC network configuration	[Enabled] [Kcs Interface] [Enabled] [Enabled] 6 [Do Nothing] [Disabled] 10 [Reset] [Disabled] m	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults ▼ F10: Save & Exit ESC: Exit</pre>	
Version 2.21.1279 Copyright (C) 2021 AMI AB			

3. 选择"BMC Network Configuration",按"Enter"进入。

图 2-23 BMC Network Configuration 界面

Aptio Setup - AMI	Server Mgmt
Sharelink Support [Auto]	Sharelink Support Help
Above option, if any changes, please click "Save Network Configuration" to send to BMC Save Network Configuration	
▶ BMC Dedicated Network Configuration	
	↔: Select Screen t↓: Select Item
	Enter: Select
	F1: General Help
	F2: Previous Values F9: Optimized Defaults
	F10: Save & Exit
	ESC: Exit
Version 2.21.1279 Copyright (C) 2	021 AMI AB

 选择 "BMC Dedicated Network Configuration "或" BMC Sharelink Network Configuration",按 "Enter"进入,可查看当前 BMC Dedicated 和 BMC Sharelink 网络参数的配置情况,如下图所示。



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

图 2-24 BMC Dedicated Network Configuration 界面

		Server Mgmt
Exit the current interface and send source/IP address/Subnet mask/Router	changes to Address IP to BMC	BMC Dedicated Network Parameters Help
Dedicated Ipv4 Network Configuration BMC Dedicated Network Parameters	I [Auto]	
Current Configuration Address	DynamicAddressBmcDhcp	
Station IP address	100.2.76.194	
Subnet mask	255.255.255.0	
Router IP address	100.2.76.1	
Station MAC address	B4-05-50-0F-AC-E0	
Dedicated Ipv6 Network Configuration IPV6 Support Configuration Address source Current Configuration Address source Station IPV6 address FDBD:DC02:108:1318::192	[Enabled] [Unspecified] DynamicAddressBmcDhcp	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Prefix Length 64		

图 2-25 BMC Sharelink Network Configuration 界面



2.6.2 BMC 网络设置

功能描述

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

操作说明

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

图 2-26 Server Mgmt 界面

Main Advanced Platfor	Aptio Setup – m Configuration	AMI Socket Configuration Server Mgr	nt 🕨
BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version IPMI BMC Interface	PASSED 32 1 4.11.08 2.0 KCS	▲ Configure BMC network parameters	
BMC Support IPMI Interface Type Wait For BMC FRB-2 Timer timeout FRB-2 Timer timeout OS Watchdog Timer OS Wtd Timer Timeout OS Wtd Timer Policy Serial Mux • BMC network configuration	[Enabled] [Kcs Interface] [Enabled] [Enabled] 6 [Do Nothing] [Disabled] 10 [Reset] [Disabled] m	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	5
Version 2.21.1279 Copyright (C) 2021 AMI AB			

3. 选择"BMC Network Configuration",按"Enter"进入。

图 2-27 BMC Network Configuration 界面

Aptio Setup – AMI		
	Server Mgilit	
Sharelink Support [Auto]	Sharelink Support Help	
Above option, if any changes, please click "Save Network Configuration" to send to BMC Save Network Configuration		
▶ BMC Dedicated Network Configuration		
	++: Select Screen	
	↑↓: Select Item	
	⊢nter: Select +/−: Change Opt.	
	F1: General Help	
	F2: Previous values F9: Optimized Defaults	
	F10: Save & Exit ESC: Exit	
Version 2.21.1279 Copuright (C) 2	021 AMI	
	AB	

🗏 说明

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

 选择 "BMC Dedicated Network Configuration",按 "Enter"进入。以 BMC Dedicated 网络配置为例,介绍 BMC 网络参数的设置,具体参数设置如 "BMC Network Configuration 界面说明表"。

	Aptio Setup – AMI	Server Mgmt
Exit the current interfa Address source/IP addres IP to BMC	ice and send changes to s/Subnet mask/Router	BMC Dedicated Network Parameters Help
Dedicated Ipv4 Network C BMC Dedicated Network Parameters	onfiguration [Auto]	
Current Configuration	DynamicAddressBmcDhcp	
Station IP address	100 3 8 5	++: Select Screen
Subnet mask	255,255,255,0	↑↓: Select Item
Router IP address	100.3.8.254	Enter: Select
Station MAC address	B4-05-5D-4A-12-33	+/-: Change Opt.
Dedicated True Natwork (configuration	F1: General Help
TRV6 Support	[Epobled]	E9: Optimized Defaulte
	[LINDICU]	F10: Save & Exit
		ESC: Exit
Version	2.21.1279 Convright (C) :	2021 AMT
1010101	ereriters copyright (of t	AB

图 2-28 BMC Dedicated Network Configuration 界面

表 2-3 BMC Network Configuration 界面说明表

界面参数	功能说明	默认值
	获取BMC专口网络参数的方式设置,该选项可	Auto
BMC Dedicated	选值有:	
Parameters	Auto:自动获取当前BMC网络设置参数	
T drameters	Manual: 手动设置BMC网络设置参数	
	配置BMC网络状态,该选项可选值有:	Unspecified
	Unspecified:不修改BMC网络参数	
Address source	Static: 设置静态参数	
	DynamicBmcDhcp:动态获取BMC网络参数	
Current		
Configuration	当前BMC配置地址状态	
Address source		
Station IP address	端口的IP地址	
Subnet mask	子网掩码	
Router IP address	路由IP地址	
CMC0 IP address		
(多节点服务器才会	从BMC获取的CMC IP0地址	
有此项)		
CMC1 IP address	从BMC获取的CMC IP1地址	

界面参数	功能说明	默认值
(多节点服务器才会		
有此项)		
Station MAC address	端口的MAC地址	
	是否支持IPV6,选项参数有:	Enabled
IPV6 Support	Enabled: 启用	
	Disabled: 禁用	
	配置BMC网络状态,选项参数有:	Unspecified
	Unspecified:将不修改BMC网络参数	
Configuration	Static: 静态	
Address Source	DynamicBmcDhcp:动态获取BMC网络参数	
	参数设置成功后立即生效。	
Station IPv6	端口的12%6地址	
address		
Prefix Length	前缀长度	
IPV6 Router1 IP	 PV6路由IP1地址	
Address		
IPV6 address	 PV6地址状态	
status		
IPV6 DHCP	IPV6 DHCP算法	
Algorithm		



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

1. 设置 BMC 静态网络参数

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

图 2-29 BMC Dedicated Network Configuration 界面



在 Station IP address、Subnet mask、Router IP address 设置完后,按"ESC"
 键,会提示"Set BMC Network Config",点击"Yes"向 BMC 发送设置,点击"OK"
 键退出当前界面,设置成功如下图所示。设置完成后 BMC 网络参数已生效,可登录
 BMC Web 界面进行操作。

图 2-30 BMC Dedicated Network Configuration 界面 2-1

		Server Mgmt
Exit the current interface and sen source/IP address/Subnet mask/Rout Dedicated Ipv4 Network Configurati BMC Dedicated Network Parameters Address source Station IP address Subnet mask Router IP address Station MAC address	d changes to Address er IP to BMC on [Manual] [Static] 100.2.76.165 225.225.255.0 Set BMC Network Config Set BMC Network Config	Server Mgmt
Dedicated Ipv6 Network Configurati IPV6 Support Configuration Address source Current Configuration Address source Station IPV6 address FDBD:DC02:108:1318::133 Prefix Length 64	Yes No	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit *</pre>

图 2-31 BMC Dedicated Network Configuration 界面 2-2



目说明

Subnet mask 和 Router IP address 设置与 Station IP address 操作类似,请参考配置。



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

2. 设置 BMC 动态网络参数

将 Address source 选项设置由 [Static] 设为 [DynamiBmcDhcp]。设置完成后, 按[ESC] 退出当前界面, 点击"Yes", 向 BMC 发送改动信息, 配置生效。

图 2-32 BMC Dedicated Network Configuration 界面



图 2-33 BMC Dedicated Network Configuration 界面



目说明

BMC IPv6 网络参数设置类似,请参考配置。



配置 BMC Dedicated 网络时,请保证网线正确连接服务器的 BMC 管理网口。

2.7 设置 BIOS 系统语言

功能描述

该操作指导用户在 BIOS 下进行系统语言的设置。

操作说明

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1 进入 BIOS Setup 界面"。
- 2. 选择 Main 界面,如下图所示。
- 图 2-34 Main 界面

Aptio Setup - AMI									
			ľ						
BMC Firmware Version	4.11.06	Choose the system							
ME Firmware Version	0F:4.4.3.236	default language							
Access Level	Administrator								
Platform Information	2 . Totol(R) Copuipo								
CPU Type	2 * Intel(K) Genuine								
CPU Current Sneed	Sustem Language								
PCH SKU	English								
RC Revision	中文 (简体)		-						
DRAM Total Memory		+: Select Screen							
BPS Total Memory		↓: Select Item							
System Memory Speed	2666 MHz	Enter: Select							
		+/-: Change Opt.							
System Language	[English]	F1: General Help							
Sustem Date	[Sup_11/12/2056]	F9: Ontimized Defaults							
System Time	[09:35:00]	▼ F10: Save & Exit							
		ESC: Exit							
Version 2.21.1278 Copyright (C) 2020 AMI									

- 3. 选择"System Language",按"Enter"。
- 根据需要,在弹出的选项对话框中选择 "English" 或 "中文(简体)",按 "Enter"。
- 5. 设置完成后,按 "F10",然后单击 "Yes",保存重启生效。

2.8 设置 BIOS 系统日期和时间

功能描述

该操作指导用户在 BIOS 下进行系统日期和时间的设置。

操作说明

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1进入 BIOS Setup 界面"。
- 2. 选择 Main 界面,如下图所示。

图 2-35 Main 界面



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



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

4. 设置完成后,按"F10",然后单击"Yes",保存重启生效。

2.9 设置 PCIe 端口

功能描述

该操作指导用户在 BIOS 下进行 PCIe 端口的设置。

操作说明

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1 进入 BIOS Setup 界面"。
- 2. 选择 Socket Configuration 界面,如下图所示。

图 2-36 Socket Configuration 界面

Main	Advanced	Platform	Aptio Setup Configuration	– AMI Socket	Configuration	Server Mgmt	►
 Proces Common Uncore Memory IIO Co Advanc 	sor Config RefCode C Configura Configuratio ed Power M	uration onfigurati tion n anagement	on Configuration		Displays an option to c Processor S ++: Select 14: Select 14: Select t-: Change F1: General F2: Previou F9: Optimiz F10: Save & ESC: Exit	d provides hange the ettings Screen Item ct : Opt. Help s Values ed Defaults : Exit	
		Version 2	2.21.1278 Copyr	ight (C)) 2021 AMI	f	ìВ

3. 选择"IIO Configuration",按"Enter"进入,如下图所示。

图 2-37 IIO Configuration 界面


Socket 的个数与 CPU 的个数一致,请以实际机型为准。

 选择对应的 CPU 配置界面,如 "Socket0 Configuration" 代表 CPU0 的配置界面,按 "Enter"进入,如下图所示。

图 2-38 Socket0 Configuration 界面



说明

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

5. 选择对应的端口,如 "CPU0_PE2 ",按 "Enter" 进入,如下图所示。

图 2-39 CPU0_PE2 界面

Aptio Setup — AMI			
	Socket Co	nfiguration	
CPU0_PE2 PCI-E Port Link Speed PCI-E Port Link Status PCI-E Port Link Max PCI-E Port Link Speed PCI-E Port Clock Gating Data Link Feature Exchange PCI-E Port Max Payload Size PCI-E ASPM Support SERRE	[Auto] [Auto] L PCI-E Port M Auto Disabled [Enabled [En [Auto] [Disabled] [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. Enable/Disable is used **: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.21.1278 Copyright (C) 2021 AMI			

- 6. 选择"PCI-E Port",按"Enter"。
- 在弹出的选项对话框中选择"Auto"、"Disabled"或"Enabled",按"Enter"。
 其中, "Auto"/"Enabled"都表示开启 PCIe 端口。
- 8. 设置完成后,按 "F10",然后单击 "Yes",保存重启生效。

2.10 设置串口重定向功能

功能描述

该操作指导用户在 BIOS 下进行串口重定向的设置。

操作说明

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1 进入 BIOS Setup 界面"。
- 2. 选择 Advanced 界面,如下图所示。

图 2-40 Advanced 界面



3. 选择 "Serial Port Console Redirection", 按 "Enter" 进入, 如下图所示。

图 2-41 Serial Port Console Redirection 界面

Advanced		
COMO Console Redirection ▶ Console Redirection Settings	[Disabled]	Console Redirection Enable or Disable.
COM1 Console Redirection ▶ Console Redirection Settings	(Disabled)	
		++: Select Screen 14: Select Tiem Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

 4. 串口重定向功能是通过"COM0"或"COM1"来实现,默认是通过"COM0"。选择 "Console Redirection",按"Enter"。



因硬件设计差异,部分机型串口重定向不支持 "COM1",具体信息请咨询客服。

- 5. 根据需要在弹出的选项对话框中选择"Disabled"或"Enabled",按"Enter"。其中, "Disabled"表示关闭相应 COM 口的串口重定向功能, "Enabled"表示开启相应 COM 口的串口重定向功能。
- 当 "Console Redirection"设置为 "Enabled"时,选择 "Console Redirection Settings",按 "Enter",可以设置串口重定向具体参数,如下图所示。

Advanced Emulation: ANSI: Extended COMO ABCII char set. VT100+: Extended ABCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more Console Redirection Settings Terminal Type Bits per second Data Bits [VT100+] [115200] [8] [8] [None] [1] [None] [Enabled] [Disabled] [Disabled] Parity Stop Bits bytes. Flow Control VT-UTF8 Combo Key Support Recorder Mode Resolution 100x31 Putty KeyPad [VT100] ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Evit F10: Save & Exit ESC: Exit

图 2-42 Console Redirection Settings 界面



- 当 "Console Redirection" 设置为 "Disabled" 时, "Console Redirection Settings"
 选项是置灰的,无法选中。
- 串口重定向具体参数设置请参见"3.2.5 Serial Port Console Redirection"。
- 7. 设置完成后,按"F10",然后单击"Yes",保存重启生效。

2.11 设置服务器启动模式

功能描述

该操作指导用户在 BIOS 下进行 UEFI/Legacy 启动模式切换。

操作说明

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

2. 选择 Advanced 界面,如下图所示。

图 2-43 Advanced 界面

Aptio Setup – AMI		
Main Advanced Platform Configuration Socket	Configuration Server Mgmt 🕨	
 Hand Drive Temperature Trusted Computing Redfish Host Interface Settings AST2500 Super ID Configuration Serial Port Console Redirection System Debug Configuration PCI Subsystem Settings USB Devices Information Network Stack Configuration CON Devices Information 	Displays Hard drive SMART Information	
OEM NIC Oprom Ctrl	↔: Select Screen	
 ▶ iSCSI Configuration ▶ Generic NVMe PCIe SSD Configuration Data 	↑↓: Select Item Enter: Select +/-: Change Opt. E1: General Helm	
▶ Driver Health	F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.21.1278 Copyright (C) 2021 AMI	
	AB	

3. 选择"CSM Configuration",按"Enter"进入,如下图所示。

图 2-44 CSM Configuration 界面

Compatibility Support Module Configuration Enable/Disable CSM Support. CSM Support [Enabled] GateA20 Active [Upon Request] INT19 Trap Response [Immediate] Boot option filter [UEFI only] Option ROM execution [Auto] Network [UEF1] Storage [UEF1] Other PCI devices [UEF1] H: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F2: Optimized Defaults F10: Save & Exit ESC: Exit Esc: Exit	Advanced		
CSH Support IEnabled] GateA20 Active [Upon Request] INT19 Trap Response [Immediate] Boot option filter [UEFI only] Option ROM execution [Auto] Network [UEF1] Storage [UEF1] Video [UEF1] Other PCI devices [UEF1] Other PCI devices [UEF1] H: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit	Compatibility Support Module Config	uration	Enable/Disable CSM Support.
	Compatibility Support Module Config CSM Support GateA20 Active INT19 Trap Response Boot option filter Option ROM execution Network Storage Video Other PCI devices	uration [Enabled] [Upon Request] [Immediate] [UEFI only] [Auto] [UEFI] [UEFI] [UEFI] [UEFI]	Enable/Disable CSM Support. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

- 4. 选择"Boot option filter",按"Enter"。
- 5. 根据需要在弹出的选项对话框中选择"Legacy only"或"UEFI only",按 "Enter"。
- 6. 按 "F10", 然后单击 "Yes", 保存重启生效。



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



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

2.12 设置服务器启动顺序

功能描述

该操作指导用户在 BIOS 下进行服务器启动顺序的设置。

操作说明

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1 进入 BIOS Setup 界面"。
- 2. 选择 Boot 界面,如下图所示。

图 2-45 Boot 界面



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

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

2.13 恢复 BIOS 选项默认值

功能描述

该操作指导用户恢复 BIOS Setup 选项默认值。

操作说明

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

1. Setup 选项

- 1. 进入 BIOS Setup 界面,具体操作步骤请参见"2.1 进入 BIOS Setup 界面"。
- 2. 选择 Save&Exit 界面,显示 "Default Options"相关选项,如下图所示。

图 2-46 Save&Exit 界面

≺ Save & Exit		
Save & Exit Save Options Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Changes Discard Changes Discard Changes Default Options Restore Defaults Save as User Defaults	Load Optimized Defaults Load Optimized Defaults?	Restore/Load Default values for all the setup options.
Restore User Defaults Boot Override	Yes No	<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

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



如果您之前使用" Save as User Defaults"选项保存过用户默认值, 可通过 "Restore User Defaults" 选项恢复用户默认值。

2. Setup 快捷键

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

3. Clear CMOS

Clear CMOS 可以通过两种方式实现:

- 方法一:将服务器断电,取下 CMOS 电池以清空 CMOS,重新安装 CMOS 电池。服务 器上电开机,即可恢复选项的默认值。
- 方法二:将服务器断电,将主板上的 RTC Jumper 跳线接 2、3 引脚或将
 BIOS_LOAD_DEFAULT 对应的拨码开关打开,完成 CMOS 放电,即可恢复大部分选项的默认值。操作完成后,将跳线帽或拨码开关恢复原始状态。

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

4. IPMI 命令行

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



上述命令中的
bmcip>为服务器 BMC IP, <username>和<password>分别为 BMC 的用 户名和密码,设置 BMC IP 具体操作步骤请参见"2.6 BMC 网络参数查看与设置"。



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

3 BIOS 参数说明

3.1 Main

功能描述

Main 界面包含当前系统信息概要,显示 BIOS、BMC 和 ME 的版本信息,以及 CPU、PCH、 RC 版本、内存等概要信息。

界面展示

Main 界面如下图所示。

图 3-1 Main 界面



参数说明

具体参数说明如下表所示。

表 3-1 Main 界面说明表

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

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

3.2 Advanced

功能描述

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

界面展示

Advanced 界面如下图所示。

图 3-2 Advanced 界面



参数说明

具体参数说明如下表所示。

表 3-2 Advanced 界面说明表

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

3.2.1 Hard Drive Temperature

功能描述

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



此界面仅支持显示南桥芯片直连的 SATA 硬盘温度。

界面展示

Hard Drive Temperature 界面如下图所示。

图 3-3 Hard Drive Temperature 界面



3.2.2 Trusted Computing

功能描述

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

界面展示

Trusted Computing 界面如下图所示。实际所使用的 TPM/TCM 芯片不同,显示的选项可能

会不同,请以实际为准。

图 3-4 Trusted Computing 界面

Advanced		
TPM 2.0 Device Found Firmware Version: Vendor:	7.51 NTZ	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and
Security Device Support Active PCR banks Available PCR banks	[Enabled] SHA-1,SHA256 SHA-1,SHA256,SM3	INT1A interface will not be available.
SHA-1 PCR Bank SHA256 PCR Bank SM3_256 PCR Bank	[Enabled] [Enabled] [Disabled]	
Measure Storage Devices Measure Network Devices Measure Video Device	[Enabled] [Enabled] [Enabled]	++: Select Screen fl: Select Item
Pending operation Platform Hierarchy Storage Hierarchy	[None] [Enabled] [Enabled]	Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values
Endorsement Hierarchy TPM 2.0 UEFI Spec Version Physical Presence Spec Version TPM 2.0 InterfaceType	[Enabled] [TCG_2] [1.3] [TIS]	F9: Optimized Defaults F10: Save & Exit ESC: Exit
PH Kandomization Device Select	[DISaoled] [Auto]	

参数说明

具体参数说明如下表所示。

表 3-3 Trusted Computing 界面说明表

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

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

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

3.2.3 Redfish Host Interface Settings

功能描述

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

界面展示

Redfish Host Interface Settings 界面如下图所示。

图 3-5 Redfish Host Interface Settings 界面

Advanced		
Redfish Host Interface Settings		Select authentication mode
BMC Redfish Version BIOS Redfish Version	1.7.0 1.7.0	
Authentication mode		
Redfish BMC Settings IP address IP Mask address IP Port	169.254.0.17 255.255.0.0 443	++: Select Screen †J: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

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

界面参数	功能说明	默认值
Authentication	授权模式设置,选项参数有:	
mode	● Basic Authentication:基本认证	Basic Authentication
	● Session Authentication:会话认证	
IP address	Redfish BMC的IP地址设置	
IP Mask	Podfich BMC的ID 捺码地址设置	
address	Keulish bhealf 地口地址以且	
IP Port	Redfish BMC的IP端口设置	



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

3.2.4 AST2500 Super IO Configuration



因硬件设计差异,部分机型不支持 AST2500 Super IO Configuration 选项,具体信息请 咨询客服。

功能描述

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

界面展示

AST2500 Super IO Configuration 界面如下图所示。

图 3-6 AST2500 Super IO Configuration 界面



参数说明

具体参数说明如下表所示。

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

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

1. Serial Port 1 Configuration

功能描述

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

界面展示

Serial Port 1 Configuration 界面如下图所示。

图 3-7 Serial Port 1 Configuration 界面

Advanced		
Serial Port 1 Configuration		Enable or Disable Serial Port
Serial Port Device Settings	[Enabled] IO=3F8h; IRQ=4;	(CON)
Change Settings	[Auto]	
		++: Select Screen ↑↓: Select Item
		Enter: Select +/-: Change Opt.
		F1: General Help F2: Previous Values F9: Optimized Defaults
		F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

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

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

2. Serial Port 2 Configuration

功能描述

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

界面展示

Serial Port 2 Configuration 界面如下图所示。

图 3-8 Serial Port 1 Configuration 界面



参数说明

具体参数说明如下表所示。

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

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

3.2.5 Serial Port Console Redirection



因硬件设计差异,部分机型串口重定向不支持 "COM1",具体信息请咨询客服。

功能描述

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

界面展示

Serial Port Console Redirection 界面如下图所示。

图 3-9 Serial Port Console Redirection 界面



参数说明

具体参数说明如下表所示。

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

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

1. Console Redirection Settings

功能描述

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

界面展示

Serial Port Console Redirection 界面如下图所示。

 Advanced

 COMO

 Console Redirection Settings

 Terminal Type
 (VT1004)

 Bits per second
 [115200]

 Data Bits
 [B]

 Parity
 [None]

 Stop Bits
 [1]

 Flow Control
 [None]

 VT-UTF8 Combo Key Support
 [Enabled]

 Recorder Mode
 [Disabled]

 Putty KeyPad
 [VT100]

 ++: Select Screen

 11: Select Item

 Enter Help

 F: General Help

 F: Optimized Defaults

 F: Optimized Defaults

 F: Select Screen

 11: Select Item

 Enter Help

 F: Optimized Defaults

 F: Optimized Defaults

 F: Select Screen

 11: Select Item

 Enter: Select

 */-: Change Opt.

 F: General Help

 F: Optimized Defaults

 F: Select Screen

 I: Select Item

 Enter: Select

 */-: Change Opt.

 F: General Help

 F: Select Serie

 F: Select Serie

 F: Select Serit

图 3-10 Console Redirection Settings 界面

参数说明

具体参数说明如下表所示。

表 3-9 Console Redirection Settings 界面说明

界面参数	功能说明	默认值
Terminal Type	终端类型设置,通过此选项可选择仿真类型,BIOS仿真类型 必须与终端程序中选择的模式相匹配。选项参数有:	
	 VT100: ASCII字符集 VT100+: 扩展的VT100,用于支持颜色显示、功能键 	VT100+
	等。	

界面参数	功能说明	默认值
	● 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。	
	波特率设置,每秒传输比特数配置,传输速率必须和串口匹	
	配,超长或嘈杂的线路可能需要较低的速度。选项参数有:	
Bits per	• 9600	
second	• 19200	115200
	• 38400	
	• 57600	
	中口数掂位苋 以直,母子 卫中头际数掂 所 百的 几 特数 匙直。 	
Data Bits		8
	_● 奇偶校验设置。洗项参数有:	
	● None: 无校验	
	● Even: 偶校验	
Parity	● Odd: 奇校验	None
	● Mark: 奇偶校验	
	● Space: 存储器奇偶校验	
	停止位设置,停止位(单个数据包的最后一位),标准设置	
	 是1位停止位,当与慢速设备通信时可能需要1个以上停止	
Stop Bits	位。选项参数有:	1
	• 1	
	• 2	
	流控制设置,用于防止数据从缓冲区溢出导致数据丢失。选	
	项参数有:	
	● None:不进行流量控制	
Flow	● Hardware RTS/CTS:通过硬件请求发送协议/清除发	News
Control	送协议进行流量控制。开启该功能后,如果使用了不支	None
	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	VT-UTF8组合键支持开关设置。选项参数有:	
Combo Key	● Enabled: 启用	Enabled
Support	● Disabled: 禁用	
Recorder	记录器模式开关设置。选项参数有:	Dia a la la al
Mode	● Enabled: 启用	Disabled

界面参数	功能说明	默认值
	● Disabled: 禁用	
Resolution	扩展终端分辨率100×31开关设置。选项参数有:	
100×31	● Enabled: 启用	Disabled
100/51	● Disabled: 禁用	
Putty KeyPad	Putty的功能键和键盘设置,选项参数有:	
	• VT100	
	• LINUX	VT100
	• XTERMR6	VIIOO
	• SCO	
	• ESCN	
	• VT400	

3.2.6 System Debug Configuration

功能描述

System Debug Configuration 界面是系统调试设置。

界面展示

System Debug Configuration 界面如下图所示。

图 3-11 System Debug Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-10 System Debug Configuration 界面说明

界面参数	功能说明	默认值
	系统调试设置,服务器系统串口输出BIOS串口日志,选项	
	参数有:	
	● Disabled: 仅输出异常处理接口。	
System	● Minimum:输出异常处理接口和少量信息,包括CPU	
Debug	Info/Options/lioPCle/DIMMInfo/Boot/RC和	Disabled
Level	OptionRom Operation Info信息。	
	● Normal:输出函数出入口及异常处理接口信息。	
	● Maximum:在Normal的基础上,针对RAS/MRC等	
	重点模块,细化到函数每个输出变量的逻辑判断。	

3.2.7 PCI Subsystem Settings

功能描述

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

界面展示

PCI Subsystem Settings 界面如下图所示。

图 3-12 PCI Subsystem Settings 界面



参数说明

具体参数说明如下表所示。

表 3-11 PCI Subsystem Settings 界面说明表

界面参数	功能说明	默认值
	4G以上内存访问控制开关设置,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。选项	
Above 4G	参数有:	Enabled
Decoding	● Enabled: 启用	Enabled
	● Disabled:禁用, Above 4G Decoding设置为	
	Disabled时,网卡的Legacy PXE功能才能用。	
	SR-IOV支持开关设置,如果启用,支持SR-IOV的PCIe	
	设备可以虚拟出多个虚拟设备(VF, Virtual	
	function),并且每个VF都具有独立运行所需要的资	
SR-IOV	源,如同一个传统的PCle设备,具有PCl总线中唯一的	Fashlad
Support	BDF (Bus device function)号,均可以被绑定到指定的	Enabled
	客户机(虚拟机)。选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	

3.2.8 USB Devices Information

功能描述

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

界面展示

USB Devices Information 界面如下图所示。

图 3-13 USB Devices Information 界面



3.2.9 Network Stack Configuration

功能描述

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

界面展示

Network Stack Configuration 界面如下图所示。

图 3-14 Network Stack Configuration 界面

Advanced		
Network Stack IPv4 PXE Support IPv6 FXE Support IPv6 FTF Support PXE boot wait time Hedia detect count	[Enabled] [Enabled] [Disabled] [Disabled] [Disabled] 0 1	Enable/Disable UEFI Network Stack →t: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-12 Network Stack Configuration 界面说明表

界面参数	功能说明	默认值
	网络堆栈开关设置。选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	Enabled
Network Stack	如果禁用该选项所有Network Stack Drvier都会	
	被跳过,不执行。	
	以下选项受该选项控制,只有该选项启用,以下	
	选项才能显示,功能才可设置。	
	UEFI IPv4 PXE支持的开关设置。选项参数有:	
IPv4 PXE Support	● Enabled: 启用	Enabled
	● Disabled: 禁用	
	IPv4 HTTP启动支持的开关设置。选项参数有:	
IPv4 HTTP Support	● Enabled: 启用	Disabled
	● Disabled: 禁用	
	UEFI IPv6 PXE支持的开关设置。选项参数有:	
IPv6 PXE Support	● Enabled: 启用	Disabled
	● Disabled: 禁用	
IDv6 HTTP Support	IPv6 HTTP启动支持的开关设置。选项参数有:	Disabled
	● Enabled: 启用	מטנוע

界面参数	功能说明	默认值
	● Disabled: 禁用	
PXE boot wait time	等待按ESC键取消PXE boot的时间设置,设置范	0
	围0~5。	U
Media detect	设备检测次数设置 设置范围1~50	1
Count		

3.2.10 CSM Configuration

功能描述

CSM Configuration 界面是兼容模块相关选项设置。

界面展示

CSM Configuration 界面如下图所示。

图 3-15 CSM Configuration 界面

Advanced		
Compatibility Support Module Conf	iguration	Enable/Disable CSM Support.
CSM Support		
CSM16 Module Version	07.84	
GateA20 Active INT19 Trap Response	[Upon Request] [Immediate]	
Boot option filter	(UEFI only)	
Option ROM execution	[Auto]	
Network Storage Video Other PCI devices	(UEFI) [UEFI] [UEFI] [UEFI]	<pre>+*: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

参数说明

具体参数说明如下表所示。

表 3-13 CSM Configuration 界面说明表

界面参数	功能说明	默认值
	兼容模式支持开关设置,UEFI兼容性支持模块,对不支持	
CSM Support	UEFI的操作系统提供兼容性支持。选项参数有:	
	● Enabled: 启用	Enabled
	● Disabled: 禁用	
	注意Legacy启动模式下,该功能会一直处于开启状态。	
	A20地址线的控制模式设置	
	选项参数有:	
Cate A 20	● Upon Request:基于需要	Upon
Active	● Always: 总是	Request
/ cuve	注:	Request
	A20是一根地址线,这根地址线控制系统对于1MB 以上的	
	那部分内存空间如何进行访问。	
	中断、捕捉信号响应设置。选项参数有:	
Response	● Immediate: 立即响应	Immediate
Response	● Postponed: 推迟响应	
	启动模式设置,控制设备Legacy或UEFI模式启动策略。选	
Boot	项参数有:	
filter	● UEFI Only: UEFI模式	UEFI UNIY
muer	● Legacy Only:传统模式	
	Option ROM执行策略,该选项控制系统Legacy Option	
	ROM或UEFI Option ROM的优先级。选项参数有:	
	● Manual: 手动	
	● Auto: 自动	
Option	注:	
ROM	设置该选项为Auto时,UEFI Option ROM会在UEFI模式下	Auto
execution	运行,Legacy Option ROM会在Legacy模式下运行;设	
	置该选项为手动时,用户可以根据情况选择运行UEFI	
	Option ROM或者Legacy Option ROM,若设置错误会使	
	得某些Option ROM无法运行。建议该选项设置为Auto模	
	式。	
	网卡Option Rom执行方式设置,选项参数有:	
	• Do not launch: 不执行	
Network		UEFI
	• Legacy: Legacy模式,加载网卡的Legacy Option	
	ROM。	

界面参数	功能说明	默认值
	• UEFI:UEFI模式,加载网卡的UEFI Option ROM。	
	注:	
	该选项在Option ROM execution为Manual时才可编辑。	
Storage	存储设备Option Rom执行方式设置,选项参数同上 UE	
Video	Video设备Option Rom执行方式设置,选项参数同上 UEFI	
Other PCI	│ │ 其他PCI设备Ontion Rom执行方式设置,选顶会数同上	
devices		

3.2.11 OEM NIC Oprom Ctrl

功能描述

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

界面展示

OEM NIC Oprom Ctrl 界面如下图所示。

图 3-16 OEM NIC Oprom Ctrl 界面

Advanced	Hptio Setup - HMI	
Global NIC Oprom Ctrl Intel(R) I350 Gigabit Network Connection(80-61-5F-05 -50-66)	[Enabled] [Enabled]	Enable/Disable NIC Oprom of Onboard and Slot
Intel(R) I350 Gigabit Network Connection(80-61-5F-05 -50-E7)	(Enabled)	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.22.1282 Copyright (C) 2022 AMI 84		

参数说明

具体参数说明如下表所示。

表 3-14 OEM NIC Oprom Ctrl 界面说明表

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

3.2.12 iSCSI Configuration

功能描述

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

界面展示

iSCSI Configuration 界面如下图所示。

图 3-17 iSCSI Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-15 iSCSI Configuration 界面说明表

界面参数	功能说明	默认值
	尝试优先级设置。选项参数有:	
	● Host Attempt:主机优先	
	● Redfish Attempt: Redfish优先	
	注:	Host Attempt
Attempt Priority	此选项的作用是调整两个可选项的优先	Redfish Attempt
	级,通过上下方向键选择要调整的可选	
	项,通过+/-来上下移动此可选项,从而	
	调整优先级。	
Host iSCSI Configration	主机iSCSI配置	
	iSCSI启动器名称,用来设置iSCSI启动器	
	名称,需要按照iSCSI限定名称	
	IQN(iSCSI Qualified Name)格式输	
iSCSI Initiator Name	入,"iqn." + "年-月" "." + "颠倒的	
	域名"+":"+"具体的设备名称",	
	如:iqn.	
	2020-11.com.example:test01234	
Add an Attempt	增加一个连接结点	
Delete Attempts	删除连接结点	
Change Attempt Order	修改尝试连接结点顺序	

3.2.13 Driver Health

功能描述

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

界面展示

Driver Health 界面如下图所示。

图 3-18 Driver Health 界面



3.3 Platform Configuration

功能描述

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

界面展示

Platform Configuration 界面如下图所示。

图 3-19 Platform Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-16 Platform Configuration 界面说明表

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

3.3.1 PCH SATA Configuration/PCH sSATA Configuration

功能描述

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

界面展示

界面如下图所示, 以 PCH SATA Configuration 菜单为例, 介绍板载 SATA 口硬盘配置, PCH sSATA Configuration 界面类似。
图 3-20 PCH SATA Configuration 界面

Platform Config	ration	
Platform Configu PCH SATA Configuration SATA Controller Configure SATA as Sata 0 Port 0 Sata 1 Port 1 Sata 2 Port 2 Sata 3 Port 3	(Enabled) (AHCI) (Not Installed) (Enabled) (Not Installed) (Enabled) (Not Installed) (Enabled) (Not Installed) (Enabled) (Not Installed) (Enabled)	Enable or Disable SATA Controller ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults
		F10: Save & Exit ESC: Exit

图 3-21 PCH sSATA Configuration 界面

Platform Config	ration	
PCH sSATA Configuration		Enable or Disable sSATA Controller
sSATA Controller Configure sSATA as sSata 0 Port 2 sSata 1 Port 4	[Enabled] [AHCI] LITEON EGT-240 - 240 GB [Enabled] [Not Installed] [Enabled]	+: Select Screen fl: Select Item Enter: Select r/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit



SATA/sSATA端口数量显示以实际机型为准。

参数说明

具体参数说明如下表所示。

表 3-17 PCH SATA Configuration 界面说明表

界面参数	功能说明	默认值
	SATA控制器开关设置,选项参数有:	
SAIA	● Enabled: 启用	Enabled
Controller	● Disabled: 禁用	
	设置SATA模式,选项参数有:	
	● AHCI:串行ATA高级主控接口,把硬盘模拟为SATA硬	
SATA as	盘,需要安装SATA硬盘驱动,支持热插拔。	AHCI
	● 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 N	SATA端口N所接硬盘信息	
	SATA端口开关设置,选项参数有:	
Port-N	● Enabled: 启用	Enabled
	● Disabled: 禁用	

3.3.2 USB Configuration

功能描述

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

界面展示

USB Configuration 界面如下图所示。

图 3-22 USB Configuration 界面

Platform Config	uration	
Rear USB0(down) 2.0 Rear USB1(up) 2.0 Drobard USB(J115) 2.0 Front USB0(Up) 2.0 Front USB1(down) 2.0 DCP3.0 USB 2.0 Reserver Connect to TF Card USB 2.0 Connect to TF Card USB 2.0 Rear USB1(up) 3.0 Rear USB1(up) 3.0 Drobard USB(J115) 3.0 Front USB0(up) 3.0	[Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled]	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB2.0 devices plug into the connector will not be detected by OS. **: Select Screen 11: Select Item Enter: Select */-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit



USB 端口显示以实际机型为准。

参数说明

具体参数说明如下表所示。

表 3-18 USB Configuration 界面说明表

界面参数	功能说明	默认值
	USB端口开关设置,包括前置、后置与板载的USB设备(具体	
	显示由丝印信息控制,如Onboard USB0(J115) 3.0),选项参	
	数有:	
	● Enabled: 启用	
USB N	● Disabled: 禁用	Enabled
	注:	
	不同服务器的USB Configuration界面,USB端口配置情况不	
	同,请以实际服务器硬件设计为准;出于服务器安全考虑,建	
	议将不使用的USB端口设置为Disabled	

3.3.3 Miscellaneous Configuration

功能描述

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

界面展示

Miscellaneous Configuration 界面如下图所示。

图 3-23 Miscellaneous Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-19 Miscellaneous Configuration 界面说明表

界面参数	功能说明	默认值
	AC上电开机电源状态设置,选项参数有:	
Restore AC	● Power On:开机状态	Power
Power Loss	● Power Off:关机状态	Off
	● Last State:恢复上次的状态	
	决定何时通过KCS接口发送IPMI命令,选项参数有:	
KCS Access	● Allow All: 始终	
Control Policy	● Restricted:直到发出BIOS DONE信号为止	Allow All
	● Deny All:从不	
	提示性选项,选项值开机自动更新,根据平台是否支持	
PFK Supported	PFR显示为"yes"或"no"	

3.3.4 Server ME Configuration

功能描述

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



Server ME Configuration 界面如下图所示。

图 3-24 Server ME Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-20 Server ME Configuration 界面说明表

界面参数	功能说明	默认值	
General ME Configuration			
Oper. Firmware Version	ME有效固件版本		
Recovery Firmware Version	ME备份固件版本		
ME Firmware Status #1	ME FW状态值#1		
ME Firmware Status #2	ME FW状态值#2		
Current State	当前状态		
Error code	错误码代码		
Recovery Cause	恢复原因	N/A	
	平台位置在海平面以上的高度,十六进制	0000	
Allitude	数,以米为单位。	8000	
	MCTP 总线主控者位于PCle: [15:8] bus,		
MCTP Bus Owner	[7:3] device, [2:0] function设置为0,表	0	
	示为禁用		

界面参数	功能说明	默认值
Server ME Firmware	服冬哭ME用供功能列主	
Features list	版分码IPE回针列能列表	

3.3.5 Runtime Error Logging

功能描述

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

界面展示

Runtime Error Logging 界面如下图所示。

图 3-25 Runtime Error Logging 界面

Platform Configuration		
Platform Confi Runtime Error Logging System Errors Fault Diagnosis Support System RAS Mode Select	[Enabled] [Enabled] [Enabled] [Enterprise]	System Error Enable/Disable setup options.

参数说明

具体参数说明如下表所示。

表 3-21 Runtime Error Logging 界面说明表

界面参数	功能说明	默认值
System Errors	系统错误日志记录设置,启用该功能后,会收集关键部件的错误并记录日志。选项参数有:	Enabled
	● Enabled: 启用	

界面参数	功能说明	默认值
	● Disabled: 禁用	
Fault	故障诊断支持:错误信息收集。选项参数有:	
Diagnosis	● Enabled: 启用	Disabled
Support	● Disabled: 禁用	
System	选择系统RAS模式,选项参数有:	
	● Enterprise:企业模式	
	● Cloud:云模式	
RAS	● Custom: 自定义模式	Enterprise
Select	注:	
Select	选择企业模式时,BIOS优先处理可纠正错误;选择云模式	
	时,操作系统优先,完全由操作系统处理可纠正错误。	

3.4 Socket Configuration

功能描述

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

界面展示

Socket Configuration 界面如下图所示。

图 3-26 Socket Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-22 Socket Configuration 界面说明表

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

3.4.1 Processor Configuration

功能描述

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

界面展示

Processor Configuration 界面如下图所示。

图 3-27 Processor Configuration 界面

	Socket Conf.	iguration	
Processor Configuration		4	Active Cores Per CPU
Processon BSP Revision Processon Socket Processon ID Processon Max Ratio Processon Max Ratio Processon Min Ratio Microcode Revision Li Cache RAM L3 Cache RAM	606A4 - ICX L0 Sacket 0 Sac 000606A4* 000 2.600GH2 2.1 1AH 0B000280 0BH 80KB 1 1280KB 1 36864KB 30	sket 1 0606A4 500GHZ 1AH 08H 000280 80KB 1280KB 5864KB	
Processor Core Number Processor Stepping Processor Voltage	24 L0 1.6V	24 L0 1.6V	++: Select Screen 14: Select Item Enter: Select
Processor O Version Processor 1 Version	Intel(R) Genuina sor Intel(R) Genuina sor	proces	+/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Evit
Active Cores Per CPU Active Cores Hyper-Threading [ALL] Core Failover	(Disabled) O (Enabled) (Enabled)		ESC: Exit

图 3-28 Processor Configuration 界面

	Socket Configuration	
Processor 1 Version	Intel(R) Genuine proces 4 sor	PSMI Configuration
Active Cores Per CPU Active Cores Hyper-Threading [ALL] Core Failover Max CPUID Value Limit Mtol Workaround Hardware Prefetcher L2 RFD Prefetch Disable Adjacent Cache Prefetch DCU IP Prefetcher LLC Prefetch DCU IP Prefetcher LLC Prefetch DCU Node Extended APIC Enable Intel(R) TXT VMX Enable SMX AES-NI TSC Reset Limit CPU PA to 46 bits > PSMI Configuration	[Disabled] 0 [Enabled] [Enabled] [Option 1] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Disabled] [Enabled] [Disabled] [Enabled] [Disabled] [Enabled] [Disabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled]	 +: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

界面参数	功能说明	默认值
Processor BSP	小理器信息之荧色,处理器的详细信息	
Revision等		
	控制是否启用每个CPU的所有核心,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	
Active Cores Per	注:	Disabled
CPU	当启用该选项时,启用CPU的核心数由选项Core	
	Disabled Bitmap (Hex)显示,0表示开启所有的核	
	心数,且每个CPU至少开启一个核心。	
Active	自用CDU核心粒设置。当选顶Active Cores Per	
Cores(Active		
Cores Per CPU为		
Disabled时显示 <i>,</i>	的CPU核数,Help信息中会根据当前CPU的情况,	0
且该选项的值会影	显示该选项可以设置的有效值和CPU的最大物理核 	
响Available	数。	
Bitmap的值)	默认值0表示开启所有核心数。 	

界面参数	功能说明	默认值
	超线程技术开关设置,启用该功能,会使得一个实	
	体CPU具有两个逻辑线程进行数据处理,有利于提	
Hyper-Inreading	高系统的整体性能。选项参数有:	Enabled
	● Enabled: 启用	
	● Disabled: 禁用	
	启用备用核心来代替BIST自检失败的核心,选项参	
Core Failover(两	数有:	Enabled
路产品)	● Enabled: 启用	Enabled
	● Disabled: 禁用	
	最大CPUID值限制开关设置,选项参数有:	
	● Enabled: 启用	
Max CPUID Value	● Disabled: 禁用	Disabled
	当传统操作系统启动不支持CPU扩展CPUID功能	
	时,请启用该选项。	
	硬件预取开关设置,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	
Hardware	注:	Enabled
Prefetcher	硬件预取是指CPU处理指令或数据之前,将这些指	
	令或数据从内存预取到L2缓存中,以减少内存读取	
	的时间,帮助消除潜在的瓶颈,以此提高系统效能	
	L2 RFO Prefetch禁用功能开关,选项参数有:	
L2 RFO Prefetch	● Enabled: 启用	Disabled
Disable	● Disabled: 禁用	
	相邻缓存预取开关设置,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	
Adjacent Cache	注:	Enabled
Prefetch	开启相邻缓存预取功能后,计算机在读取数据时,	Enableu
	会智能的认为要读取数据的旁边或邻近的数据也是	
	需要的,于是在处理的时候就会将这些邻近的数据	
	预先读取出来,这样可以加快读取速度。	
	DCU流预取开关设置,选项参数有:	
DCU Streamer	● Enabled: 启用	Enabled
Prefetcher	● Disabled: 禁用	
	注:	

界面参数	功能说明	默认值
	DCU(Data Cache Unit)流预取器是L1 Data Cache	
	的预取器,如果DCU流预取器检测到在一段时间内	
	从同一缓存行进行多次加载,即认为下一缓存行将	
	被使用,从而把下一缓存行从L2缓存或内存中预取	
	到L1 Data Cache中。	
	DCU IP预取开关设置,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	
DCU IP	注:	Enabled
Prefetcher	DCU IP预取器是L1 Cache的预取器,DCU IP预取器	
	根据历史加载记录决定是否从内存或L2缓存中预取	
	下一条数据放入到L1 Cache中。	
	5. 左梁田山 6. 弦动开关沉空,坐在会坐去。	Disabled(四
	所有线柱LLL	路产品)
LLC Prefetcher	Enabled: 后用	Enabled(两
	Disabled: 禁用	路产品)
	DCU Mode设置,选项参数有:	
DCU Mode	Normal:正常模式	Normal
	Mirror-Mode: 镜像模式(两路产品)	
	扩展APIC(Advanced Programmable Interrupt	
	Controlle)开关设置,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	
	注:	
	扩展APIC功能需要VT-d的支持。当扩展APIC设置为	
Extended APIC	Enabled,而VT-d为Disabled时,某些操作系统会	Disabled
	无法正确的处理Interrupt,需要VT-d Interrupt	
	Remapping的功能支持。所以,当扩展APIC设置	
	为Enabled时,建议VT-d也设置为Enabled状态。	
	当所配置的处理器总核数(线程数)超过256个	
	时,建议开启扩展APIC功能以使操作系统更高效的	
	支持CPU多核特性功能。	
	Intel可信执行技术支持开关设置,选项参数有:	
Enable Intel(R)	● Enabled: 启用	Disabled
	● Disabled: 禁用	
VMX(选项Enable	Intel硬件辅助虚拟化技术开关设置,选项参数有:	Frankla /
Intel(R) TXT为	● Enabled: 启用	FUSDIED

界面参数	功能说明	默认值
Enabled时 <i>,</i> 选项	● Disabled: 禁用	
不可选)	注:	
	VMX(Virtual Machine Extensions)是Intel 64或	
	IA-32架构虚拟化技术提供的虚拟化扩展,启用该选	
	项后,Intel 64或IA-32平台可以作为多个虚拟系统	
	(或虚拟机)使用。每个虚拟机可以在单独的隔离	
	区中运行操作系统和应用程序。	
	安全模式扩展开关设置,选项参数有:	
	● Enabled: 启用	
Enable SMX(选项	● Disabled: 禁用	
Enable Intel(R)	注:	Disabled
TXT为Enabled	SMX(Safer Mode Extensions)为系统软件提供了	DISabled
时,选项不可选)	一个编程接口,用于在平台内建立一个可测量的环	
	境,以支持终端用户的可信决策,可测量环境所使	
	用的测量和保护机制需要Intel(R) TXT支持。	
	AES指令开关设置,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	
AES-NI	注:	Enabled
	该菜单主要控制CPU是否支持AES指令,这些指令	
	主要用于虚拟化系统,打开该指令之后,系统性能	
	能得到提升。	
TSC Pacat/西欧产	在热重启期间启用或禁用TSC重置,选项参数有:	
150 (19501())301	Enabled: 启用	Disabled
	Disabled: 禁用	
	将CPU物理地址限制为46位以支持旧的Hyper-V,	Disabled(四
Limit CPU PA to	选项参数有:	路产品)
46 bits(两路产品)	Enabled: 启用	Enabled(两
	Disabled: 禁用	路产品)



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

1. PSMI configuration

功能描述

PSMI configuration 界面是电源配置管理接口选项设置。

界面展示

PSMI configuration 界面如下图所示。

图 3-29 PSMI configuration 界面

	Socket Configuration	
Global PSMI Enable (Er Socket 0 Configuration Socket 1 Configuration Socket 2 Configuration Socket 3 Configuration	nabled]	Global PSMI Enable ++: Select Screen ++: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F3: Optimized Sefaults F3: Set & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-24 PSMI configuration 界面说明表

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

3.4.2 Common RefCode Configuration

功能描述

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

界面展示

Common RefCode Configuration 界面如下图所示。

图 3-30 Common RefCode Configuration 界面

	Socket Configuration	
Common RefCode Configuration		Select MMIO High Base
MMIO High Base MMIO High Granularity Size Numa Virtual Numa UMA-Based Clustering	[327] [646] [Enabled] [Disabled] [Hemisphere (2-clusters)]	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-25 Common RefCode Configuration 界面说明表

界面参数	功能说明	默认值
MMIO High Base	 MMIO内存映射IO高位基地址设 置,选项参数有: 56T 40T 32T 24T 16T 4T 2T 	32T (NF5488M6/NF5468M5/NF5688M5 默认4T)

界面参数	功能说明	默认值
	 1T 512G 注: 一般情况下,该选项的值要大于当前服务器物理内存的总容量,否则可能会导致内存初始化失败。若选项的值小于服务器物理内存的总容量,因为MMIO Hight Base的限制,在OS下看到的内存容量会比实际内存容量小。某些情况下,为了兼容某些板卡,特别是Legacy下,可适当选择较小的选项参数。 	
MMIO High Granularity Size	 MMIO内存映射IO高位粒度大小设置,默认等同于每个栈分配的 MMIO资源大小。选项参数有: 1G 4G 16G 64G 256G 1024G 注: 当MMIO High Base为56T该选项 不能设置为1024G。 	64G (NF5488M6/NF5468M5/NF5688M5 默认1024G)
Numa	Numa开关设置,选项参数有: ● Enabled: 启用 ● Disabled: 禁用 注: 非统一内存访问 (Non-uniform memory access, Numa) 是一 种内存共享架构, 启用后,每个 CPU可以使用自己本地内存,又可 以访问其他CPU的内存。访问本地 内存具有低时延-高带宽的性能, 访问其他CPU的内存具有高延时- 低带宽的性能。	Enabled

界面参数	功能说明	默认值	
	在ACPI表中将物理NUMA节点划		
	分为均匀大小的虚拟NUMA节点,		
Virtual	提高Windows在搭配超过64个逻		
Numa(两路	辑处理器的CPU时的性能。选项参	Disabed	
产品)	数有:		
	● Enabled: 启用		
	● Disabled: 禁用		
	UMA集群设置,选项参数有:		
	● Disable (All2All): 禁用		
UMA-	• Hemisphere (2-clusters):		
Based	半球(2-clusters)	Hemisphere (2 slusters)	
Clustering	注:	Hemisphere (2-clusters)	
(两路产品)	这些选项仅在禁用SNC时有效。如		
	果启用了SNC,则BIOS将自动禁		
	用基于UMA的群集。		

3.4.3 Uncore Configuration

功能描述

Uncore Configuration 界面是 Uncore 相关选项设置。

界面展示

Uncore Configuration 界面如下图所示。

图 3-31 Uncore Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-26 Uncore Configuration 界面说明表

界面参数	功能说明	默认值
Uncore General	Uncore通田功能控制荧角	
Configuration	のにのと通用功能注刷未手	

1. Uncore General Configuration

功能描述

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

界面展示

Uncore General Configuration 界面如下图所示。

图 3-32 Uncore General Configuration 界面

Socket Configuration	on
Uncore General Configuration	Uncore Status Help
 Uncore Status Degrade Precedence Degraded 4S Topology Preference (4S Fully Connect (Single Link)] Link Speed Mode [Fast] Link Frequency Select [Auto] Link L0 Enable [Disabled] Link L1 Enable [Disabled] Link L1 Enable [Disabled] Lortorem Thresholds Normal [Auto] Leqacy V&A Socket 0 Splitlock Socket [Disabled] NPT Prefetch [Enabled] Loctorem Thresholds Empty [Auto] Legacy V&A Socket 0 Splitlock [Enabled] Disabled] DYP Frefetch [Enabled] NPT Prefetch [Enabled] Socket 0 Splitlock [Disabled] DSabled] DYP Prefetch [Enabled] Legacy V&A Stack 0 Shoop Throttle Configuration [Auto] Legacy V&A Stack 0 	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

参数说明

具体参数说明如下表所示。

表 3-27 Uncore General Configuration 界面说明表

界面参数	功能说明	默认值
Uncore Status	Uncore链接状态子菜单,显示当前UPI链接状态	
Degrade Precedence	 降低优先级设置,选项参数有: Topology Precedence:拓扑优先 Feature Precedence:特征优先 注: 当系统设置冲突时通过设置Topology Precedence来降低 KFeature,或通过设置Feature Precedence来降低 Topology。 	Topology Precedence
Degraded 4S Topology Preference Link Speed Mode	当系统可以降级为4S1Lfully Connect或4S2LRing拓扑 时,选择降级的拓扑: 4S Fully Connect (Single Link) 4S Ring (Dual Link) 链接速度模式设置,选项参数有: Slow	4S Fully Connect (Single Link) Fast

界面参数	功能说明	默认值
Link Frequency Select	 链接频率选择设置,选项参数有: Auto 9.6 GT/s 10.4GT/s 11.2GT/s(两路产品) 注: Auto将获取当前配置可支持的最大链接频率。若将链路频率设置为较低速度,以较低频率运行可降低功耗,但 同时会影响系统性能。 	Auto
Link L0p Enable	LOp节能选项开关设置,选项参数有: Disabled:禁用 Enabled: 启用 Auto:自动 注: Auto默认为Enabled。 	Disabled
Link L1 Enable	L1节能选项开关设置,选项参数有: Disabled: 禁用 Enabled: 启用 Auto: 自动 注: Auto默认为Enabled。 	Disabled
UPI Failover Support	 UPI失效转移支持开关设置,选项参数有: Disabled:禁用 Enabled: 启用 Auto:自动 注: Auto默认为Enabled。 	Enabled
XPT Remote Prefetch (两路 产品)	 XPT远程预取的开关设置,选项参数有: Disabled:禁用 Enabled: 启用 Auto:自动 注:Auto根据CPU型号来判断是否Enabled。 	Auto
KTI Prefetch	 KTI预取的开关设置,选项参数有: Enabled: 启用 Disabled: 禁用 Auto: 自动 	Enabled

界面参数	功能说明	默认值
	注:	
	Auto默认为Enabled。	
Loctorem Thresholds Normal Loctorem Thresholds Empty	 TOR阈值-Loctorem Normal阈值设置,选项参数有: Disabled:禁用 Auto:自动 Low:低 Medium:中 High:高 TOR阈值-Loctorem Empty阈值设置,选项参数有: Disabled:禁用 Auto:自动 Low:低 Medium:中 	Auto
	● High: 高	
Legacy VGA Socket	传统VGA个数设置,有效值范围0~3。	0
SplitLock	SplitLock开关设置,选项参数有: Disabled: 禁用 Enabled: 启用 Auto: 自动 注: Auto默认为Enabled。 	Disabled
SNC (Sub NUMA)(四路 产品)	 四路产品CPU的Sub NUMA集群设置,选项参数有: Disabled:不支持SNC功能 Enabled:支持所有的SNC集群(2-clusters)和1- way的IMC交错 Auto:根据IMC交错支持1-cluster或者2-clusters 	Disabled
SNC (Sub NUMA)(两路 产品)	 两路产品CPU的Sub NUMA集群设置,选项参数有: Disabled:支持1-cluster(XPT/KTI预取启用)的 SNC集群和4-way的IMC交错 Enable SNC2 (2-clusters):支持2-clusters的 SNC集群和2-way的IMC交错 	Disabled

界面参数	功能说明	默认值
XPT Prefetch	 XPT预取的开关设置,选项参数有: Disabled:禁用 Enabled: 启用 Auto:自动 注: Auto默认为Enabled。 	Enabled
D2K Credit configuration (四路产品)	选择可用的D2K VNA BL积分级别重新进行分配: Low:低级 Medium:中级 High:高级 	Medium
Snoop Throttle Configuration	选择CHA的侦听门限级别: Disabled: 禁用 Low: 低级 Medium: 中级 High: 高级 Auto: 自动 	Auto
Legacy VGA Stack	传统VGA堆栈个数设置,有效值范围0~6	0
PCIe Remote P2P Relaxed Ordering(两 路产品)	Pcie远程P2P放宽排序开关设置,选项参数有: Disabled:禁用,硬件将强制执行P2P写入顺序 Enabled:启用,由软件决定放宽P2P写入顺序 	Disabled

3.4.4 Memory Configuration

功能描述

Memory Configuration 界面是内存相关选项设置。

界面展示

Memory Configuration 界面如下图所示。

图 3-33 Memory Configuration 界面

	Socket Configuration	
Integrated Memory Controller (IMC) STEP DRAM Test Operation Mode SmartTest Enforce POR Enforce POR Memory Frequency Data Scrambling for PMem Data Scrambling for DDR4/5 Allow Memory Training Correctable Error Allow Memory Test Correctable Error Enable ADR Legacy ADR Mode Minimum System Memory Size ADR Data Save Mode Errore MUNDIMME	Socket Configuration	 Set Enable or Disable STEP(Samsung TestBIDS & Enhanced PPR)function **: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F10: Save & Exit ESC: Exit
Ersse-AFM NVDIAMS Restore NVDIAMS Interleave NVDIAMS	(Enabled) [Enabled] [Disabled]	

参数说明

具体参数说明如下表所示。

表 3-28 Memory Configuration 界面说明表

界面参数	功能说明	默认值
	强制执行POR设置,选项参数有:	
	• POR	
	● Disabled: 禁用	
Enforce POR	注:	POR
	POR(Plan of Record)是指Intel提供限制DDR4执行频	
	率规定,若设置该选项的值为POR,则系统会强制按	
	照POR原则对DDR4内存频率进行设置。	
	打开或关闭STEP(Samsung TestBIOS & Enhanced	
SIEP DRAM	PPR)功能,选项参数有:	5. 11 1
	● Disabled: 禁用	Disabled
	● Enabled: 启用	
Operation	设置操作模式,选项参数有:	
Mode(四路产	● Test and Repair: 检测并修复	Test and
品)	● Test Only:仅检测	Repair
SmartTest (四	● Disabled: 禁用	Disablad
路产品)	● Enabled: 启用	Disabled

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

界面参数	功能说明	默认值
	● Enabled: 启用	
	● Disabled: 禁用	
	传统ADR模式开关设置,选项参数有:	
Legacy ADR	● Enabled: 启用	Disabled
моае	● Disabled: 禁用	
	仅在有JEDEC NVDIMM时为系统分配的最小内存,选	
Miningung	项参数有:	
System	• 2GB	2 G B
Memory Size	• 4GB	200
	• 6GB	
	• 8GB	
NVDIMM	设置NVDIMM的能耗策略,选项参数有:	Dovico
Energy Policy	● Device-Managed:设备控制	Managed
(两路产品)	● Host-Managed: 主机控制	Manageu
	ADR数据保存模式设置,选项参数有:	
ADR Data Save	● Disabled: 禁用	
Mode	● Batterybacked DIMMs:电源保存	NVDIMMS
	● NVDIMMs:不易失内存	
	Erase-Arm NVDIMMs开关设置,选项参数有:	
Erase-Arm	● Enabled: 启用	Enabled
NVDIMMS	● Disabled: 禁用	
	修复NVDIMMs开关设置,选项参数有:	
Restore	● Enabled: 启用	Enabled
NVDIMMS	● Disabled: 禁用	
	交错NVDIMMs开关设置,选项参数有:	
Interleave	● Enabled: 启用	Enabled
NVDIMMS	● Disabled: 禁用	
SPD-SMBUS	控制CPU的SPD SMBUS访问权限,选项参数有:	
Access (Only	● Lock: 锁定	Lock
for两路产品)	● UnLock: 解锁	
	控制SPD打印开关,选项参数有:	
SPD Print	● Enabled: 启用	Disabled
	● Disabled: 禁用	
SPD Print		
Length (SPD	控制SPD引印长度, 选项参数有:	
Print选项	● Auto: 目动	Auto
Enabled时可	● 256 Bytes: 256字节	
选)	● 512 Bytes:512字节	

界面参数	功能说明	默认值
	注:	
	Auto默认为最大长度512字节。	
Cmd Setup %	Cmd设置/保持百分比偏移量,用于后期cmd训练结	50
Offset	果。可选范围0~100	50
	内存周期补偿寄存器开关设置,选项参数有:	
	● Auto: 自动	
Periodic	● Enabled: 启用	
Rcomp(两路产	● Disabled: 禁用	Auto
品)	注:	
	Auto默认使用CSR MemComp comp_disable寄存器	
	的值。	
	内存周期补偿寄存器的值,选项参数有:	
	• 10.24us	
	• 20.48us	
	• 40.96us	
Periodic	• 163.84us	
Rcomp Interval	• 327.68us	
(Only for两路	• 655.36us	
产品,选项	• 1310.72us	671 08864
Periodic	• 2621.44us	07 1.00004
Pcomn为	• 5242.88us	1115
	• 10.48576ms	
DISADLEC的隐	• 20.67152ms	
藏)	• 41.94304ms	
	• 83.88608ms	
	• 167.77216ms	
	• 335.54432ms	
	• 671.08864 ms	
Memory		
Topology	內仔拍扩于米平,亚示仕12内仔许细信息 	
Memory Map	内存Map子菜单	
Memory RAS		
Configuration		

1. Memory Map

功能描述

Memory Map 界面是内存模式设置。

界面展示

Memory Map 界面如下图所示。

图 3-34 Memory Map 界面

Volatile Memory Mode AppDirect cache	[2LM] [Disabled]	Selects 1LM or 2LM mod for volatile memory. For 2LM memory mode, BIOS will try to
		configure 2LM but if BIOS is unable to configure 2LM, volatil memory mode will fall
		++: Select Screen fl: Select Item Enter: Select +/-: Change Opt
		F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit FSC: Fvit

参数说明

具体参数如下表所示。

表 3-29 Memory Map 界面说明表

界面参数	功能说明	默认值
Volatile Memory Mode (四路产品隐藏,两路产 品中Numa 选项为 Disabled时不可选)	 易失内存模式设置,选择启用1LM内存模式或 启用2LM内存模式,选项参数有: ● 1LM ● 2LM 	2LM
AppDirect cache (Volatile Memory Mode选项为1LM时隐 藏)	为内存区域启用缓存的开关设置,选项参数 有: • Enabled:启用 • Disabled:禁用	Disabled
1LM Memory Interleave Granularity(四路产品 且Volatile Memory Mode为1LM才显示)	1LM内存交叉间隔设置,选项参数有: ● 256B Target, 256B Channel ● 64B Target, 64B Channel	256B Target, 256B Channel

2. Memory RAS Configuration

功能描述

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

界面展示

Memory RAS Configuration 界面如下图所示。

图 3-35 Memory RAS Configuration 界面

Full Mirror Mode will set Memory RAS Configuration Setup be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode Operation RAS mode: Independent		Socket Configuration	
Hirror Mode [Disabled] Fank sparing is enabled Mirror TADO [Disabled] partial mirroring will not UEFI ARM Mirror [Disabled] partial mirroring will not UEFI ARM Mirror [Disabled] take effect. Enabling any type Memory Rank Sparing [Disabled] of Mirror Mode will disable Memory Correctable Error Flood [Frequency] Policy	Memory RAS Configuration Setup Operation RAS mode: Independent Mirror Hode Mirror TADO UEFI ARM Mirror Memory Rank Sparing Memory Correctable Error Flood Policy ADDDC Sparing Plus One Set FNem Die Sparing ECC Mode Switch Patrol Scrub Interval Patrol Scrub Interval Patrol Scrub Address Mode Patrol Scrub Error Downgrade	[Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Frequency] [Disabled] [Enabled] [Enabled] [Enabled] [Enabled] 24 [System Physical Address] [Enabled]	Full Mirror Mode will set entire 11M memory in system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Enabling any type of Mirror Mode will disable +*: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-30 Memory RAS Configuration 界面说明表

界面参数	功能说明	默认值
	使能48B SDDC ECC	
NEW SDDC Mode (西欧产品)	● Enabled: 启用	Enabled
	● Disabled: 禁用	
Enable Pcode WA	启用SAI策略组的Pcode解决方法:	
for SAI PG(两路产	● Enabled: 启用	Disabled
品)	● Disabled: 禁用	
Mirror Mode	镜像模式设置,选项参数有:	
(ADDDC Sparing为	● Disabled: 禁用	Disabled
Enabled时不可选)	● Full Mirror Mode:全局镜像模式	

界面参数	功能说明	默认值
	 Partial Mirror Mode:局部镜像模式 注: 全局镜像模式会将系统中的整个1LM内存设置 为镜像,从而内存容量将会减少一半;启用局 部镜像模式是将部分内存设置镜像,若启用了 Rank Sparing,则局部镜像模式将不会生效; 且无论启用任何镜像模式都会禁用XPT Prefetch。 	
Partial Mirror 1 Size (GB) (Mirror Mode 选项为Partial Mirror Mode时显示)	选择创建的SAD容量大小,单位1GB。 注意镜像大小必须小于总内存大小的一半。 0-X (X为系统总内存容量的1/2)	0
Mirror TAD0(Mirror Mode为非Full Mirror Mode时可选, ADDDC Sparing为 Enabled时不可选)	镜像TAD0模式开关设置,选项参数有: • Enabled: 启用 • Disabled: 禁用	Disabled
UEFI ARM Mirror (Mirror Mode为 Disabled时可选 <i>,</i> ADDDC Sparing为 Enabled时不可选)	UEFI ARM镜像模式开关设置,选项参数有: • Enabled: 启用 • Disabled: 禁用	Disabled
ARM Mirror percentage(UEFI ARM Mirror为 Enabled时显示)	输入UEFI ARM镜像的百分比,5000代表 50%,可选范围: 0-5000	0
Memory Rank Sparing (四路产品, Mirror Mode为 Disabled且UEFI ARM Mirror为Disabled, 且没有AEP/BPS三个 条件同时存在时此选 项可选)	内存Rank热备开关设置,选项参数有: Enabled: 启用 Disabled: 禁用 注: 当启用该选项后,一个Rank可作为同一通道的 其它Rank的备用,若有Rank出现缺陷,可以 用同一内存通道中其它闲置的Rank来代替,将 有缺陷Rank的数据复制到代替Rank中。 	Disabled
Multi Rank Sparing (四路产品, Memory Rank Sparing为 Enabled时可选)	选择内存Rank热备的数量,选项参数有: ● One Rank:要求通道中的Rank数量大于 2	Two Rank

界面参数	功能说明	默认值
	• Two Rank:要求通道中的Rank数量大于	
	4	
	内存可修复错误的放行策略:	
Memory Correctable	● Disabled:不放行	Frequency
Error Flood Policy	• Once: 一次	Frequency
	● Frequency: 多次	
	ADDDC(Adaptive Double Device Data	
	Correction Sparing)自适应双设备数据校正备	
	用设置,选项参数有:	
ADDDC Sparing(没	● Enabled: 启用	
有AEP/BPS且	● Disabled: 禁用	
Memory Rank	注:	Disabled
Sparing为Disabled		
· · · · · · · · · · · · · · · · · · ·	 修复错误,BIOS最多支持在一个内存通道内做	
	两次失效区域替换和一次备份处理。若考虑性	
	能优先 建议 举田该洗顶 若老虎可靠性优	
	此"亿",建议采用改造项,石与心马非正化 生 建议工户该功能	
Dius One (Memory)		
Plus One (Memory	后用SDDC+1, 远坝参数有:	
	● Enabled: 后用	Disabled
Disabled时可选)	● Disabled: 禁用	
Enable ADDDC Error	允许ADDDC注错,选项参数有:	
	● Enabled: 启用	Enabled
Sparing为Enable时	● Disabled:禁用	
显示)		
	设置NGN Die热备开关设置,选项参数有:	
Set NGN Die Sparing	● Enabled: 启用	Enabled
	• Disabled: 禁用	
	允许内存控制器由模式A切换到模式B,选项参	
ECC mode switch	数有:	Enabled
(四路产品)	● Enabled: 启用	LIIdbled
	● Disabled: 禁用	
	内存巡检开关设置,选项参数:	
	● Enabled: 启用	
	● Disabled: 禁用	Enable at End
Patrol Scrub	● Enable at End of POST:在POST结束启	of POST
	用	
	注:	

界面参数	功能说明	默认值
	启用该选项后,系统会提供内存巡检功能,及 时处理内存的可纠正错误,防止可纠正错误积 累成不可纠正错误。	
Patrol Scrub Interval	内存巡检间隔时间设置,单位是小时,范围是 0~24 设置为0,表示为自动	24
Patrol Scrub Address Mode(四 路产品)	 内存巡检地址模式设置,选项参数有: System Physical Address:系统物理地址 Reverse Address:相反地址 	System Physical Address
Patrol Scrub Error Downgrade(四路产 品)	 将无法纠正的Patrol Scrub错误降级成为可纠 正的错误,参数选项有: Enabled: 启用 Disabled: 禁用 	Enabled

3.4.5 IIO Configuration

功能描述

IIO Configuration 界面是对 PCIe 插槽进行配置。

界面展示

IIO Configuration 界面如下图所示。

图 3-36 IIO Configuration 界面

	Socket Configuration	
IIO Configuration		
 Socket0 Configuration Socket1 Configuration Socket2 Configuration Socket3 Configuration Socket3 Configuration Intel0 VT for Directed I/O (VT-d) Intel0 VMD technology IIO Global Performance Tuning IIO-PCIE Express Global Options 		
NTB Link Train by BIOS Delay before link training PCIE Hot Plug CDDma MultiCast Enable PCI-E ASPM Support (Global) PCIE 10-bit Tag Enable PCIE Max Read Request Size PCIE PTM Enable	(Auto) (No delay) (Enabled) (Disabled) (Disabled) (Disabled) (Auto) (Enabled)	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-31 IIO Configuration 界面说明表

界面参数	功能说明	默认值
	Socket N配置子菜单,用来设置CPU0的PCIe上	
Socket N	设备的Link speed及Max Payload Size,ASPM	
Configuration	等设置,并显示当前PCIe端口的链接状态,最大	
	链接,当前链接速率等。	
Intel VT for	Intel VT-d技术相关设置子菜单,Intel VT-d技术	
Directed I/O (VT-	开关设置,用于提高系统的安全性和可靠性,提	
d)	高I/O设备在虚拟环境中的性能。	
Intel VMD	 Intel VMD技术相关设置子菜单,每个CPU的每	
Technology	个PStack上VMD的开关设置。	
(UEFI模式显示)		
IIO Global	山〇件能控制英色	
Tuning	110 住能控制来半	
Retimer	└────────────────────────────────────	
workaround(两	● No: 不启用	No
路产品)	● Yes: 启用	
NTB Link Train	是否启用NTB链路训练,选项参数有:	
by BIOS	● Disabled: 禁用	Auto

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

界面参数	功能说明	默认值
	• 2048B	
	• 4096B	
	注:	
	Auto默认为最大值4096B。	
		Disabled(两路
	PCIE PTM后用设直, 远坝参敛有:	产品)
PCIE PTM Enable	● Enabled:后用	Enabled(四路产
	● Disabled: 禁用	品)

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

功能描述

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

界面展示

Intel VT for Directed I/O (VT-d)界面如下图所示。

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

	Socket Configuration	
Intel® VT for Directed I/O (VT-d) Intel® VT for Directed I/O (VT-d) Interrupt Remapping Posted Interrupt ATS Coherency Support (Non-Isoch)	(Enabled) (Enabled) (Enabled) (Enabled) (Enabled)	Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

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

界面参数	功能说明	默认值
Intel® VT for Directed I/O (VT-d)	 VT-d功能开关,可以使得多个虚拟机访问同一个物理 I/O,提高了虚拟机的性能,选项参数有: Enabled: 启用 Disabled: 禁用 注: 当Intel® VT for Directed I/O (VT-d)选项为 Enabled时显示下面选项。 	Enabled(两路 产品) Disabled(四路 产品)
Interrupt Remapping	 VT-d中断重映射开关,可为定向I/O提供中断重映射 功能,选项参数有: Enabled: 启用 Disabled: 禁用 	Enabled
Posted Interrupt(四 路产品)	 VT-d中断重映射扩展功能,暂存可映射的中断请求到物理内存中,选项参数有: Enabled: 启用 Disabled: 禁用 	Enabled
ATS(四路产 品)	ATS功能开关,选项参数有: Enabled: 启用 Disabled: 禁用 	Enabled
Coherency Support(Non- Isoch) (四路 产品)	非同步一致性功能开关,选项参数有: • Enabled:启用 • Disabled:禁用	Enabled

2. Intel VMD Technology

功能描述

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

界面展示

Intel VMD Technology 界面如下图所示。

图 3-38 Intel VMD Technology 界面

Socket Configuration	
Intel® VMD technology	
 Intel® VMD for Volume Management Device on Socket 0 Intel® VMD for Volume Management Device on Socket 1 Intel® VMD for Volume Management Device on Socket 2 Intel® VMD for Volume Management Device on Socket 3 	<pre>#: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

表 3-33 Intel VMD Technology 界面说明表

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

	Socket Configuration	1
VMD Config for IOU 0		▲ Enable/Disable VMD in this
Enable/Disable VMD		Stack.
CPU0_PE1	[Enabled]	
VMD port B	[Enabled]	
VMD port C	[Enabled]	
VMD port D	[Enabled]	
Hot Plug Capable	[Disabled]	
CfgBar size	25	
CfgBar attribute	[64-bit prefetchable]	
MemBar1 size	25	
MemBar1 attribute	[32-bit	
	non-prefetchable]	
MemBar2 size	20	
MemBar2 attribute	[64-bit	++: Select Screen
	non-prefetchable]	↑↓: Select Item
		Enter: Select
VMD Config for IOU 1		+/-: Change Opt.
Enable/Disable VMD	[Disabled]	F1: General Help
		F2: Previous Values
VMD Config for IOU 2		F9: Optimized Defaults
Enable/Disable VMD	[Disabled]	F10: Save & Exit
VMD Config for IOU 3		ESC. EXIL
Enable/Disable VMD	[Disabled]	

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

参数说明

具体参数说明如下表所示。

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

界面参数	功能说明	默认值
Enable/Disable VMD	VMD功能开关,选项参数有:	
	● Enabled: 启用	
	● Disabled: 禁用	Disabled
	注:	
	选项Enable/Disable VMD启用后,以下选项显示	
VMD port x	VMD端口x是否启用VMD特性,选项参数有:	
(x=A~D,是否可选	● Enabled: 启用	Disabled
由硬件设计决定)	● Disabled: 禁用	
Hot Plug Capable	VMD热插拔功能开关,选项参数有:	
	● Enabled: 启用	Disabled
	● Disabled: 禁用	
CfgBar Size	VMD Bar大小,设置范围20~27	25
	VMD Bar属性,选项参数有:	
CfgBar attribute	● 32-bit non-prefetchable:32位不可预取	64-bit
	● 64-bit non-prefetchable:64位不可预取	prefetchable
界面参数	功能说明	默认值
--------------	-------------------------------------	--------------
	● 64-bit prefetchable: 64位可预取	
MemBar1 size	内存Bar1大小,设置范围20~39	25
	内存Bar1属性,选项参数有:	
MemBar1	● 32-bit non-prefetchable:32位不可预取	32-bit non-
attribute	● 64-bit non-prefetchable:64位不可预取	prefetchable
	● 64-bit prefetchable:64位可预取	
MemBar2 size	内存Bar2大小,设置范围20~39	20
	内存Bar2属性,选项参数有:	
MemBar2	● 32-bit non-prefetchable:32位不可预取	64-bit non-
attribute	● 64-bit non-prefetchable:64位不可预取	prefetchable
	● 64-bit prefetchable:64位可预取	



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

3.4.6 Advanced Power Management Configuration

功能描述

Advanced Power Management Configuration 界面是 CPU 电源管理相关选项设置。



图 3-40 Advanced Power Management Configuration 界面

Socket Configuration			
Advanced Power Management Configuration Power/Performance Profile Pcode Dispatcher Matchdog Timer CPU P State Control Handware PM State Control Prequency Prioritization Overclocking CPU C State Control Package C State Control Package Current Config Package Current Config Package Current Config PMax Detector Configuration ACPI Sx State Control Memory Power & Thermal Configuration	ON [Custom] [Auto]	Power/Performance Profile. High Performance Compute: Traditional high performance compute scenarios. Suitable for high-load, multi-threaded and low-latency work scenarios. Low-load, single-threaded and latency-insensitive scenarios may not achieve good performance; Balance/Energy * *: Select Screen Th: Select Tiem Enter: Select H-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	

参数说明

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

界面参数	功能说明	默认值
	节能/性能配置,选项参数有:	
	● High Performance Compute:最大性能	
	● Balance/Energy Efficiency:平衡/能源效	
David (David and a second	率	
Power/Performance	• Power Saving: 节能	Custom
FIOIRE	● Low Latency: 低延时	
	● OLTP: 联机事务处理	
	● Virtualization: 虚拟化	
	● Custom: 自定义	
CPU P State Control	CPU P状态控制设置子菜单	
Hardware PM State	硬件由源管理状态控制子莖单	
Control		
CPU C State Control	CPU C状态控制设置子菜单	
Package C State		
Control		
CPU-Advanced PM	CPU性能和节能调整子莁单	
Tuning		

界面参数	功能说明	默认值
SOCKET RAPL Config	Socket RAPL配置子菜单	

1. Power/Performance Profile

功能描述

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

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

- High Performance Compute:传统高性能计算场景,典型应用为大规模科学计算和 工程计算。特点是高负载,多线程,低延时,CPU和内存利用率极高,IO利用率低。 该设定对低负载,单线程,延迟不敏感的场景未必能取得最好的效果。此场景下会关闭 节能,以获取更高 CPU 频率和内存吞吐量。低负载场景更多需要开启节能,使Idle的 核心进入 C6,而使工作的单核心获得更多的功耗和散热裕量,从而可以使工作核心持 续保持在高频工作状态以获取更好的性能。
- Balance/Energy Efficiency:均衡性能和节能,以取得较高的能效比。主要是在对性 能影响最小的前提下开启节能以获取较高的效率。可用于大部分普通应用,有利于在保 持良好性能的前提下获取好的节能效果。
- Power Saving: 主要用于对能耗要求高的场合。此场景会开启绝大部分节能选项并开 启最大节能状态,使得系统在 Idle 状态下功耗更低。当有负载开始运行时,从节能状 态退出会有一定的时延。负载运行期间,某些部件会因为长时间没有被访问而进入节能 状态,当需要访问这些部件时,部件从节能状态退出也会有一定的时延。高负载运行 时,因为各部件不满足进入节能状态的条件,效果与节能关闭差异不大。
- Low Latency:用于对时延要求严苛的场景,例如实时操作系统。对于计算量大,多线程,持续时间较长的负载需要更多考虑平均计算速度,高平均计算速度的获取有时需要开启节能以使核心间协作更加协调,而不是争抢功耗和散热裕量。对于突发短促的负载,需要侧重反应速度。此场景会关闭可能引入时延的节能选项和其他管理功能,并使CPU 在 idle 状态下保持最高频率以获取更快的反应。

- OLTP:应用于在线传输业务,即联机事务处理(Online Transaction Processing),主要以小的事务以及小的查询为主,并发量高,典型的OLTP系统有电子商务系统,银行,证券等。请求响应时间是一个重要指标,这需要快速的数据库访问速度和计算处理速度,需要平衡CPU的峰值速度和 Memory/IO 吞吐量。
- Virtualization: 主要应用于虚拟化场景。此场景下会开启所有虚拟化功能,并设定好 和虚拟化有关联的相关选项,以更好支持虚拟化。
- Custom: 主要用来供用户根据具体应用场景自行定制以达到最好的效果。

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

2. CPU P State Control

功能描述

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

界面展示

CPU P State Control 界面如下图所示。

图 3-41 CPU P State Control 界面

	Socket Configuration	
CPU P State Control Uncore Free Scaling (UFS) SpeedStep (Pstates) Config TDP Lock AVX P1 Boot performance mode Turbo Mode CPU Flex Ratio Override CPU Core Flex Ratio	[Enabled] [Enabled] [Enabled] [Normal] [Max Performance] [Enabled] [Disabled] 23	Enable/Disable autonomous uncore frequency scaling
		+: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-36 CPU P State Control 界面说明表

界面参数	功能说明	默认值
Uncore Freq Scaling (UFS)	Uncore Frequency Scaling功能开关。启用UFS 时,处理器可以通过内部的电压调节器,改变内 部核心和非核心的电压/频率,实现功率在核心 和非核心之间的最佳分配,选项参数有: • Enabled: 启用 • Min Frequency:最小频率 • MAX Frequency:最大频率 • Custom:自定义 注: 该选项设置为非Enabled时,自动调节功能关 闭,Uncore的频率固定。	Enabled
Uncore Frequency (Uncore Freq Scaling (UFS)选项为 Custom时显示)	选择具体的Uncore扩展频率,可选范围由BIOS 从CPU读取,并显示在Help信息中	16
SpeedStep (Pstates)	 CPU PStates开关设置,开启后CPU进入性能模式,选项参数有: Enabled: 启用 Disabled: 禁用 	Enabled
Config TDP Lock (四路产品 <i>,</i> SpeedStep(Pstates) 为Enabled时显示)	TDP锁的设置,选项参数有: • Enabled: 启用 • Disabled: 禁用	Enabled
AVX P1 (SpeedStep (Pstates)选项为 Enabled时显示)	选择AVX P1等级,选项参数有: Normal:正常 Level 1:级别1 Level 2:级别2 	Normal
Boot performance mode(SpeedStep (Pstates)选项为 Enabled时可选)	 进入OS之前BIOS的性能状态设置,选项参数 有: Max Performance:最大性能 Max Efficient:最大效率 Set by Intel Node Manager:由英特尔节 点管理器设置 	Max Performance
Turbo Mode (SpeedStep	可応TUTDO升大设直,选项参致有: ● Enabled:启用 ● Disabled:禁用	Enabled

界面参数	功能说明	默认值
(Pstates)为Enabled		
时显示)		
	启用CPU核心频率重写,选项参数有:	
CPU Flex Ratio	● Enabled: 启用	Disabled
Overnide	● Disabled: 禁用	
CPU Core Flex Ratio (选项CPU Flex Ratio Override为 Enabled时可选)	当CPU Flex Ratio Override选项Enabled时,选 择要重写的CPU核心频率,步长为1,可选范围 从CPU读取,动态显示在帮助信息中。	23 (CPU频率 不同默认值会 有所不同)
GPSS timer(两路产 品)	 P-State变化时的迟滞时间窗口,选项参数有: Ous 50us 500us 	500 us

3. Hardware PM State Control

功能描述

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

界面展示

Hardware PM State Control 界面如下图所示。

图 3-42 Hardware PM State Control 界面

	Socket Configuration	
Hardware PM State Control Hardware P-States EPP Enable Native ASPM Static Turbo Mode	[Disabled] [Enabled] [Auto] [Disabled]	Disable: Hardware chooses a P-state based on OS Request (Legacy P-States) Native Mode:Hardware chooses a P-state based on OS guidance Out of Band Mode:Hardware autonomously chooses a P-state (no OS guidance) ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-37 Hardware PM State Control 界面说明表

界面参数	功能说明	默认值
Hardware P- States	 HWP功能选择开关,选项参数有: Disabled:关闭HWP功能 Native Mode: 通过OS直接访问HWPM寄存器,对CPU进行配置,该模式既支持传统ACPI表,也支持新的ACPI规范 Out of Band Mode: OS无法访问HWPM寄存器,只能通过BMC以带外的方式进行CPU配置 Native Mode with No Legacy Support: 与 "Native Mode"相同,但仅支持新的ACPI规范 	Disabled
EPP Enable (Hardware P- States为非 Disabled时可选)	EPP使能设置,选项参数有: • Enabled: 启用 • Disabled: 禁用	Enabled
Native ASPM	ASPM控制模式选择,选项参数有: Auto: BIOS控制ASPM Disabled: ASPM关闭 Enabled: OS控制ASPM 	Auto
Static Turbo Mode	静态Turbo模式,启用后,会关闭P-State以使CPU 保持在Turbo频率,选项参数有: Disabled:禁用 Enabled:启用 注: 静态Turbo模式会将CPU的频率维持在CPU当前配 置中可达到的最高频率,但是会增加系统功耗。	Disabled

4. CPU C State Control

功能描述

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

界面展示

CPU C State Control 界面如下图所示。

图 3-43 CPU C State Control 界面

	Socket Configuration	
CPU C State Control Enable Monitor MWAIT CPU C6 report Enhanced Halt State (C1E)	[Enabled] [Auto] [Disabled]	Allows Monitor and MWAIT instructions. +: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-38 CPU C State Control 界面说明表

界面参数	功能说明	默认值
	Monitor Mwait支持开关设置,选项参数有:	
MWAIT	● Enabled: 启用	Disabled
	● Disabled: 禁用	
CPU C6 report	向OS报告C6状态开关设置,选项参数有:	Disabled
	● Enabled: 启用	DISabled

界面参数	功能说明	默认值
	● Disabled: 禁用	
	● Auto: 自动	
	注:	
	Auto相当于Enabled。	
	C1E开关设置,选项参数有:	
Enhanced Halt	● Enabled: 启用	Disabled
	● Disabled: 禁用	



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

5. Package C State Control

功能描述

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

界面展示

Package C State Control 界面如下图所示。

图 3-44 Package C State Control 界面



参数说明

具体参数说明如下表所示。

表 3-39 Package C State Control 界面说明表

界面参数	功能说明	默认值
	Package C状态设置,选项参数有:	
	• C0/C1 state: C0/C1状态	
	● C2 state:C2状态	
	● C6(non Retention) state:C6(不保留)状态	
	● C6(Retention) state(四路产品):C6(保留)状态	C0/C1
Package C State	● No Limit(四路产品):无限制	state
	● Auto: 自动	
	注:	
	Auto默认为C0/C1 state,但也会根据具体的CPU型	
	号进行调整。	
Register Access	Register Access 使能注册访问低延时模式,选项参数有:	
Low Latency ● Enabled: 启用		Dissibility
Mode(两路产	路产 ● Disabled: 禁用	
品)	注:	

界面参数	功能说明	默认值
	使能这个模式之后将会组织PkgC6作为注册访问结构	
	进入静止状态。	

6. CPU-Advanced PM Tuning

功能描述

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

界面展示

Energy Perf BIAS 界面如下图所示。

图 3-45 Energy Perf BIAS 界面

	Socket Configuration	
Energy Perf BIAS Power Performance Tuning ENERGY_PERF_BIAS_DFG mode Workload Configuration	[BIOS Controls EPB] [Performance] [Balanced]	MSR 1FCh Bit[25] = PMR_PERF_TUNING_CFG_MODE. OS Controls EPB - Use IA32_ENERGY_PERF_BIAS input from the core; BIOS Controls EPB - Use alternate perf BIAS input from ENERGY_PERF_BIAS_CONFIG; **: Select Screen 11: Select Item Enter: Select */-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-40 Energy Perf BIAS 界面说明表

界面参数	功能说明	默认值
Power Performance	中酒州能调整沿置、洗顶会粉方・	BIOS Controls
Tuning	宅际住能购主议重,选项参数有.	EPB

界面参数	功能说明	默认值
	● OS Controls EPB: OS控制电源性	
	能	
	● BIOS Controls EPB: BIOS控制电	
	源性能	
	● PECI Controls EPB(两路产品):	
	PECI控制电源性能	
	电源性能调优配置。CPU根据该设置来	
	调节处理器的内部运行,满足高性能或	
	是节能的需求。这个设置只有能效调整	
ENERGY_PERF_BIAS_CFG	设置为BIOS控制能效策略时才可用,选	
mode (Power	择任何一个都会覆盖OS下对CPU性能调	
Performance Tuning选	整的配置。选项参数有:	Performance
项为BIOS Controls EPB时	● Performance: 性能	
可选)	● Balanced Performance:均衡性	
	能	
	● Balanced Power:均衡节能	
	● Power: 节能	
	对工作负载特性优化设置,选项参数	
Workload Configuration	有:	Palancod
	● Balanced: 平衡	balanceu
	● I/O Sensitive: I/O敏感	

7. SOCKET RAPL Config

功能描述

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

界面展示

SOCKET RAPL Config 界面如下图所示。

图 3-46 SOCKET RAPL Config 界面



参数说明

具体参数说明如下表所示。

表 3-41 SOCKET RAPL Config 界面说明表

界面参数	面参数 功能说明		
	PL1限制的开关设置,选项参数有:		
PL1 Limit	● Enabled: 启用	Enabled	
	● Disabled: 禁用		
DI 1 Dowor Limit	PL1功率限制设置,单位为瓦特,取值范围为0到		
PLT POwer Limit (PL1 Limit为	Fused Value,如果该值为0,则会取Fused Value		
Disabled时陷	作为此时的功率,若该值大于Fused Value,同样	0	
盛)	会取Fused Value作为此时的功率,Fused Value		
)H2G)	为固化在芯片中的最高功率。		
PL1 Time			
Window (PL1	DI1时窗设罢 单位为孙 设置范围056	1	
Limit为Disabled	「口时國反重,半位內位,反直尼回0~50		
时隐藏)			
PL2 Limit(PL1	PL2限制的开关设置,选项参数有:		
Limit为Disabled	● Enabled: 启用	Enabled	
时隐藏)	● Disabled: 禁用		

界面参数	功能说明	默认值
	PL2功率限制设置,单位为瓦特,该值可从0到	
PL2 Power Limit	Fused Value,如果该值为0,则会取125%*Fused	0
	Value作为此时的功率。	
PL2 Time	DI 2时窗设置 单位为孙 设置范围056	1
Window	FLZ时囱以直,丰位为秒,以直池固0~50	1

3.5 Server Mgmt

功能描述

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

界面展示

Server Mgmt 界面如下图所示。

图 3-47 Server Mgmt 界面



参数说明

具体参数说明如下表所示。

表 3-42 Server Mgmt 界面说明表

界面参数	功能说明	默认值
BMC Self Test Status	BMC自检状态	
BMC Firmware	当前主板BMC固件版本号	
Revision		
	FRB-2的钾开大攻直,远坝参数有:	En als la al
FRB-2 Timer	● Enabled: 后用	Enabled
FRB-2 Timer	FRB-2时钟超时时间设置,选项参数有:	20(两路机型);
Timeout	3-30min	30(四路机型)
	FRB-2时钟超时后的策略设置,选项参数	
	有:	
FRB-2 Timer policy	● Do Nothing:无动作	Power Cycle
	● Reset: 重启	i offer eyele
	● Power Down:关机	
	● Power Cycle:关机并重新开机	
	OS看门狗时钟开关设置,选项参数有:	
OS Watchdog Timer	● Enabled: 启用	Disabled
	● Disabled:禁用	
	OS 看门狗时钟超时时间设置,选项参数	
OS Wtd Timer	有:	10
Imeout	3-30min	
	OS看门狗时钟超时后的策略设置,选项参数	
	有:	
	● Do Nothing:无动作	
OS Wtd Timer policy	● Reset: 重启	Reset
	● Power Down:关机	
	● Power Cycle:关机并重新开机	
BMC network		
Configuration		
BMC User Settings	BMC用户设置子菜单	
VLAN Configuration	VLAN配置子菜单	
View FRU	查看FRU信息子菜单	
information		
BMC Load Default	BMC恢复默认值	

3.5.1 BMC Network Configuration

功能描述

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

界面展示

BMC Network Configuration 界面如下图所示。

图 3-48 BMC Network Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-43 BMC Network Configuration 界面说明表

界面参数	功能说明	默认值	
	BMC Sharelink网络开关设置,每次开机		
Charolink Cupport	从BMC读取,选项参数有:		
Sharelink Support	● Enabled: 启用	Enabled	
	● Disabled:禁用		
	配置BMC网络,选项参数有:		
BMC Network Select	● Auto: 自动	Auto	
	● Manual: 手动		

界面参数	功能说明	默认值
Auto Failover Nic Count (BMC Network Select选项 Manual时显示)	1 仅专用或NCIS支持远程管理 2 专用和一个NCIS支持远程管理	1
BMC Network Type(BMC Network Select选项 Manual时显示)	BMC网络类型,选项参数有: MGMT: MGMT管理网口 OCP: OCP网口 PCle: PCle网口	MGMT
BMC Dedicated Network Configuration	BMC专用网络参数设置	
BMC Sharelink Network Configuration	BMC复用网络参数设置	

1. BMC Dedicated Network Configuration

功能描述

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

界面展示

BMC Dedicated Network Configuration 界面如下图所示。

图 3-49 BMC Dedicated Network Configuration 界面



图 3-50 BMC Dedicated Network Configuration 界面

		Server Mgmt
Current Configuration Address Source Station IP address Subnet mask Router IP address Station MAC address Dedicated Ipv6 Network Configuration IPV6 Support	DynamicAddressBmcDhcp 100.2.76.108 255.255.255.0 100.2.76.1 B4-05-5D-50-00-52	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Configuration Address source Current Configuration Address source Station IPV6 address	[Unspecified] DynamicAddressBmcDhcp	++: Select Screen 11: Select Item
FDBD:DC02:108:1318::253 Prefix Length 64 TPV6 Router1 TP Address		Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Evit
IPV6 address status IPV6 DHCP Algorithm	Active DHCP∨6 ▼	ESC: Exit

参数说明

具体参数说明如下表所示。

表	3-44 BN	1 C Dedicated	Network	Configuration	界面说明表
---	---------	----------------------	---------	---------------	-------

界面参数	功能说明	默认值
BMC Dedicated Network Parameters	 获取BMC专口管理网口参数的方式置,选项参数有: Auto:自动获取当前BMC网络设置 Manual:手动设置BMC网络 	Auto
Address source(BMC Dedicated Network Parameters为Manual 时显示)	 配置BMC网络状态,选项参数有: Unspecified:将不修改BMC网络参数 Static:设定静态BMC网络参数 DynamicBmcDhcp:动态获取BMC网络参数 	Unspecified
Current Configuration Address source	当前BMC配置地址状态	
Station IP address	端口的IP地址	
Subnet mask	子网掩码	
Router IP address	路由IP地址	
CMC0 IP address (多节点服务器有此 IP,如I48M6)	从BMC获取的CMC IP0地址	

界面参数	功能说明	默认值
CMC1 IP address (多节点服务器有此 IP,如l48M6)	从BMC获取的CMC IP1地址	
Station MAC address	端口的MAC地址	
IPV6 Support	是否支持IPV6,选项参数有: ● Enabled: 启用 ● Disabled: 禁用	Enabled
Configuration Address Source	 配置BMC网络状态,选项参数有: Unspecified:将不修改BMC网络参数 Static:设定静态BMC网络参数 DynamicBmcDhcp:动态获取BMC网络参数 注: 参数设置成功后立即生效。 	Unspecified
Current Configuration Address source	当前BMC配置地址状态	
Station IPv6 address	端口的IPv6地址	
Prefix Length	前缀长度	
IPV6 Router1 IP Address	IPV6路由IP1地址	
IPV6 address status	IPV6地址状态	
IPV6 DHCP Algorithm	IPV6 DHCP算法	

2. BMC Sharelink Network Configuration

功能描述

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

界面展示

BMC Sharelink Network Configuration 界面如下图所示。

图 3-51 BMC Sharelink Network Configuration 界面



图 3-52 BMC Sharelink Network Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-45 BMC Sharelink Network Configuration 界面说明表

界面参数	功能说明	默认值
BMC Sharelink Network	获取BMC共享口管理网口参数的方式设置,选	Ato
Parameters	项参数有:	Auto

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

3.5.2 BMC User Settings

功能描述

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



BMC User Settings 界面如下图所示。

图 3-53 BMC User Settings 界面



参数说明

具体参数说明如下表所示。

表 3-46 BMC User Settings 界面说明表

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

1. Add User

功能描述

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

界面展示

Add User 界面如下图所示。

图 3-54 Add User 界面

		Server Mgmt
BMC Add User Details User Name User Password User Access User Privilege Limit	[Disabled] [No Access]	Enter BMC User Name, User name is a string of 1 to 16 alpha numeric characters, and first character must be a letter, Special characters are only allow ''(hyphen), '_'(underscore), '@'(at sign)
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

参数说明

具体参数说明如下表所示。

表 3-47 Add User 界面说明表

界面参数	功能说明	默认值
User	用户名称设置,用户名为字母数字字符,且首字符必须是字	
Name	母,特殊字符只允许'_'、'-'、'@',最大支持16字符	
	用户密码设置,密码必须包含大小写字母,特殊字符及数字,	
User	启用BMC密码复杂度后,密码复杂度由BMC指定。设置成功	
Passworu	后提示 "Added User successfully"	
	用户权限开关设置,选项参数有:	
User	● Enabled: 启用	Disabled
ACCESS	● Disabled: 禁用	
	用户权限设置,选项参数有:	
	● No Access:没有权限	
User	● User: 用户	
Privilege	● Operator: 操作	No Access
Limit	● Administrator: 管理员	
	设置成功后,会提示"Set User Access Command	
	Passed!!!" , BMC User立即生效	

2. Delete User

功能描述

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

界面展示

Delete User 界面如下图所示。

图 3-55 Delete User 界面



参数说明

具体参数说明如下表所示。

表 3-48 Delete User 界面说明表

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

3. Change User Settings

功能描述

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

界面展示

Change User Settings 界面如下图所示。

图 3-56 Change User Settings 界面



参数说明



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

具体参数说明如下表所示。

表 3-49 Change User Settings 界面说明表

界面参数	功能说明	默认值
User Name	输入需要修改密码的用户名	
User Password	输入该用户的原密码,用户名和密码验证成功	
	后,下方选项才可进行修改	

界面参数	功能说明	默认值
	输入新密码,密码必须包含大小写字母,特殊字	
Change User	符及数字,启用BMC密码复杂度后,密码复杂度	
Password	由BMC指定。设置成功后提示"Password	
	Changed Successfully"	
	用户权限开关设置,选项参数有:	
User Access	● Enabled: 启用	Disabled
	● Disabled: 禁用	
	修改用户权限设置,选项参数有:	
User Privilege Limit	● No Access:没有权限	
	● User: 用户	
	● Operator: 操作	No Access
	● Administrator: 管理员	
	设置成功后提示"Set User Access Command	
	Passed!!!", BMC User立即生效	

3.5.3 VLAN Configuration

功能描述

VLAN Configuration 界面 BIOS 设置 BMC VLAN 网络参数。

界面展示

VLAN Configuration 界面如下图所示。

图 3-57 VLAN Configuration 界面



参数说明

具体参数说明如下表所示。

表 3-50 VLAN Configuration 界面说明表

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

3.5.4 View FRU information

功能描述

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

界面展示

View FRU information 显示界面如下图所示。

图 3-58 View FRU information 界面

参数说明

具体参数说明如下表所示。

表 3-51 View FRU information 界面说明表

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

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

3.6 Security

功能描述

Security 界面是管理员及用户密码设置。

界面展示

Security 界面如下图所示。

图 3-59 Security 界面



参数说明

具体参数说明如下表所示。

表 3-52 Security 界面说明表

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



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

3.6.1 Secure Boot

功能描述

Secure boot 界面用于配置安全启动功能。

界面展示

Security 界面如下图所示。

图 3-60 Secure Boot 界面

		Security
System Mode	Setup	Secure Boot feature is Active
Secure Boot	[Disabled] Not Active	Platform Key(PK) is enrolled and the System is in User mode. The mode change requires
Secure Boot Mode ► Restore Factory Keys ► Reset To Setup Mode ► Enter Audit Mode	[Custom]	platform reset
▶ Key Management		
		<pre>+: Select Screen 14: Select Item Enter: Select +/-: Change Opt, F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

参数说明

具体参数说明如下表所示。

表 3-53 Secure Boot 界面说明表

界面参数	功能说明	默认值
	如果启用该功能,则安全启动功能处于活动状态。	
Secure Boot	如果已注册平台密钥(Platform key,PK),并且	
	系统处于用户模式,更改模式需要平台重置。选项	Dischlad
	参数有:	Disabled
	● Enabled: 启用	
	● Disabled: 禁用	
Secure Boot	安全启动模式选择器:标准或自定义。选项参数	Custom
Mode	有:	Custom

界面参数	功能说明	默认值
	● Custom: 自定义模式	
	● Standard:标准模式	
	注:	
	自定义模式:在自定义模式下多种指令可以灵活使	
	用。在自定义模式下更新PK、KEK变量不需要原始	
	PK签署,且更新Image signature database	
	(db/dbx)或Authorized Timestamp Database	
	(dbt)也不需要PK或KEK的签署	
	标准模式:是UEFI规范描述的默认模式	
	强制系统进入用户模式。安装出厂默认的安全启动	
Restore Factory	密钥数据库,选项参数有:	Vac
Keys	● Yes: 是	res
	● No: 否	
	从NVRAM删除所有安全启动密钥数据库,选项参数	
Reset To Setup	有:	No
Mode	● Yes: 是	NO
	● No: 否	
Enter Audit Mode	进入审核模式工作流程。从用户到审核模式的转换	
	将导致PK变量的删除	
Кеу	对安全启动的密钥进行管理,包括密钥的查看,添	
Management	加,删除,授权和恢复出厂设置等操作	



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

3.7 Boot

功能描述

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

界面展示

Boot 界面如下图所示。

图 3-61 Boot 配置界面



参数说明

具体参数说明如下表所示。

表 3-54 Boot 配置界面说明表

界面参数	功能说明	默认值
Setup Prompt	ompt Setup提示超时设置,设置等待Setup激活键的时	
Timeout	间,最大值为65535秒	I
	开机启动过程中键盘Numlock指示灯状态开关设	
Bootup NumLock	置,选项参数有:	0.44
State	• On: 开	UII
	• Off: 关	
De et Detro	设备轮询开关设置,选项参数有:	Franklad
BOOT RETRY	● Enabled: 启用	Enabled

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

3.7.1 Add New Boot Option

功能描述

Add New Boot Option 界面是添加引导项界面。

界面展示

Boot 界面如下图所示。

图 3-62 Add New Boot Option 界面

	Boot
Add New Boot Option Add boot option Path for boot option Boot option File Path Create	Specify name for new boot option
	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-55 Add New Boot Option 界面说明表

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

3.7.2 Delete Boot Option

功能描述

Delete Boot Option 界面是删除引导项界面。

界面展示

Boot 界面如下图所示。

图 3-63 Delete Boot Option 界面

	Boot
Delete Boot Option	Remove an EFI boot option from
Delete Boot Option	
	++: Select Screen
	Enter: Select
	F1: General Help
	F9: Optimized Defaults F10: Save & Exit
	ESC: Exit

参数说明

具体参数说明如下表所示。

表 3-56 Delete Boot Option 界面说明表

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

3.8 Save & Exit

功能描述

Save&Exit 界面是 BIOS 参数修改保存和退出相关选项设置。

界面展示

Save&Exit 界面如下图所示。
图 3-64 Save & Exit 界面



参数说明

具体参数说明如下表所示.

表 3-57 Save&Exit 界面说明表

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



BIOS 升级方法,请参考《浪潮英信服务器 BIOS 升级手册》。