UNIS 服务器

Hygon 海光处理器 BIOS 用户指南

紫光恒越技术有限公司
http://www.unisyue.com

资料版本：6W101-2021930
产品版本：H65-BIOS-5.13 及以上版本

前 言

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

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定

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

2. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

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

5. 示例约定

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

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目　录

1 简介

1.1 适用产品

本手册适用于以下产品：

- UNIS Server R3830 G5
- UNIS Server R3630 G5

1.2 文档使用说明

由于产品版本升级或其他原因，本文档内容会不定期进行更新。如需查看最新的 BIOS 界面，建议联系技术支持获取。

本文为产品通用资料。对于定制化产品，请用户以产品实际情况为准。

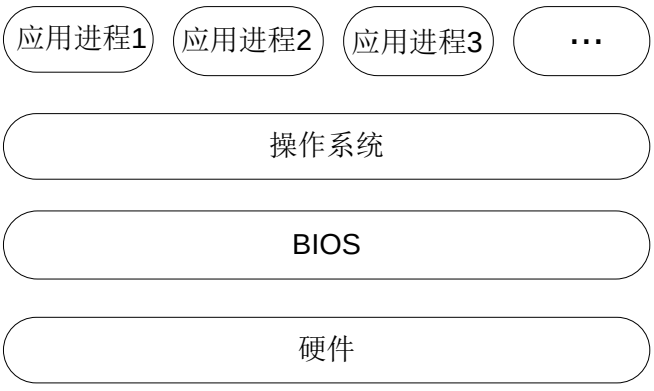
1.3 BIOS简介

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

BIOS 的主要功能包括：

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

图1-1 BIOS 在系统中的位置



2 常用功能

常用功能包括：

2.1 进入BIOS界面

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

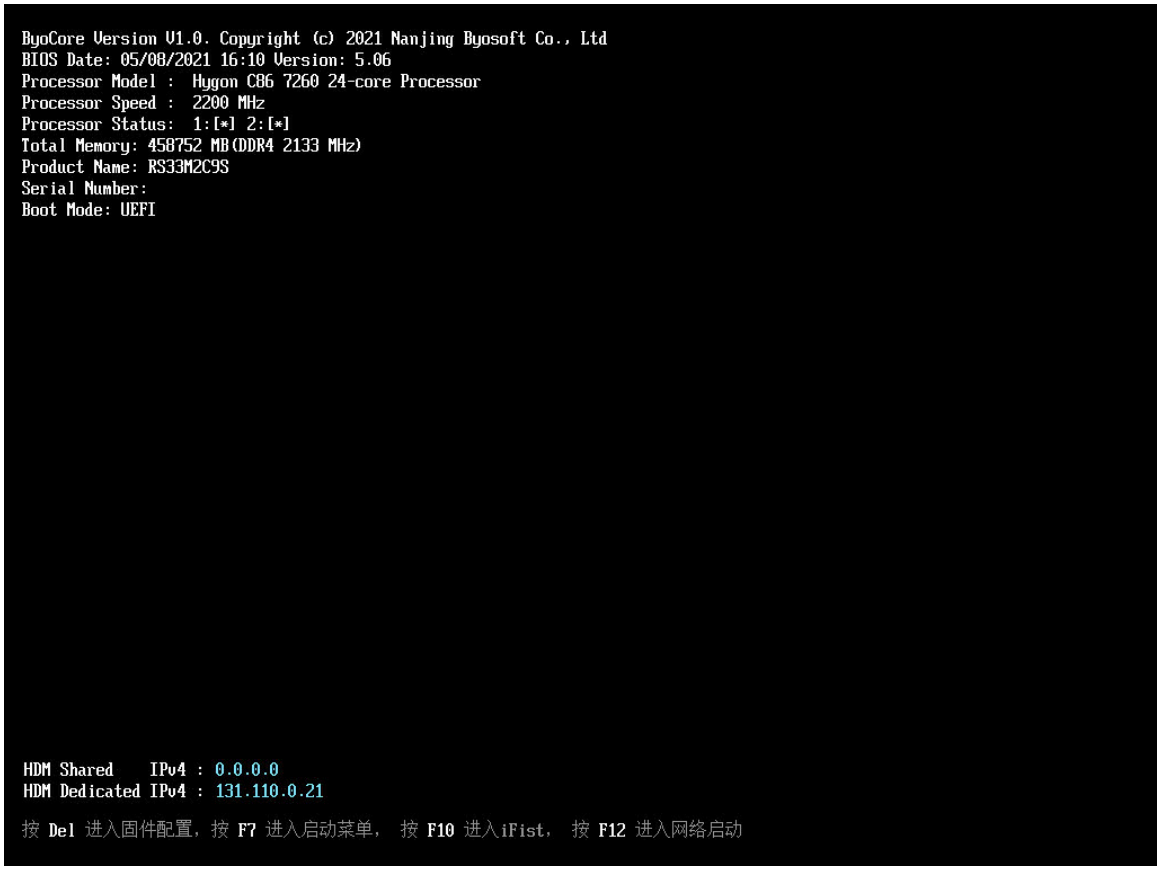
说明

关于启动远程控制台的具体方法，请参见 HDM 联机帮助。

(2) 启动或重启服务器。

(3) 如图 2-1 所示，进入 BIOS 启动界面后，按 **Del** 进入 BIOS 配置页面。

图2-1 BIOS 启动界面



(4) （可选）如图 2-2 所示，如设置了 BIOS 管理员和用户密码，进入 BIOS Setup 时，需要先选择登录角色，再输入对应角色的密码，如_所示，以管理员密码为例。

- BIOS 缺省没有设置任何密码，设置密码的具体方法请参见 2.7 设置 BIOS 密码。
- 如果连续三次输入错误的密码，服务器会自动重启，稍后请重新输入密码。
- 如果您忘记了 BIOS 密码，请将服务器下电，通过系统维护开关清除 BIOS 密码。服务器重新上电时，系统将清除 BIOS 的密码。系统维护开关的具体位置，请参见产品用户指南。

图2-2 选择登录角色

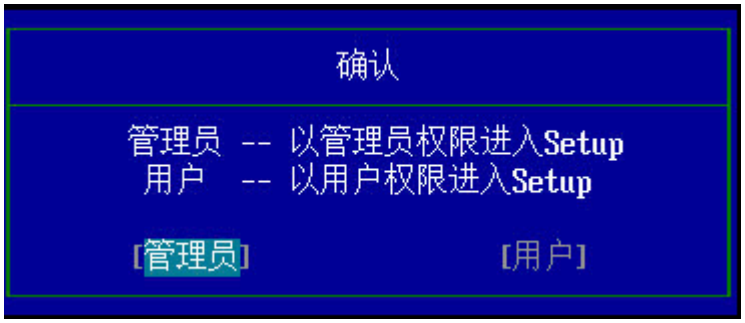
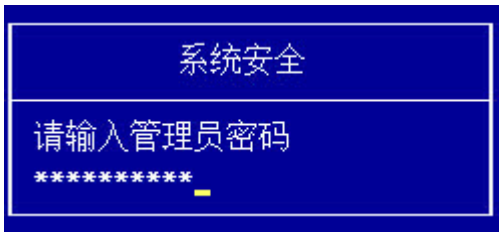


图2-3 输入 BIOS 密码



(5) 如图 2-4 所示，进入 BIOS 配置界面，可参照界面下方的操作说明进行相关设置。操作说明的详细信息如表 2-1 所示。

图2-4 BIOS 配置界面

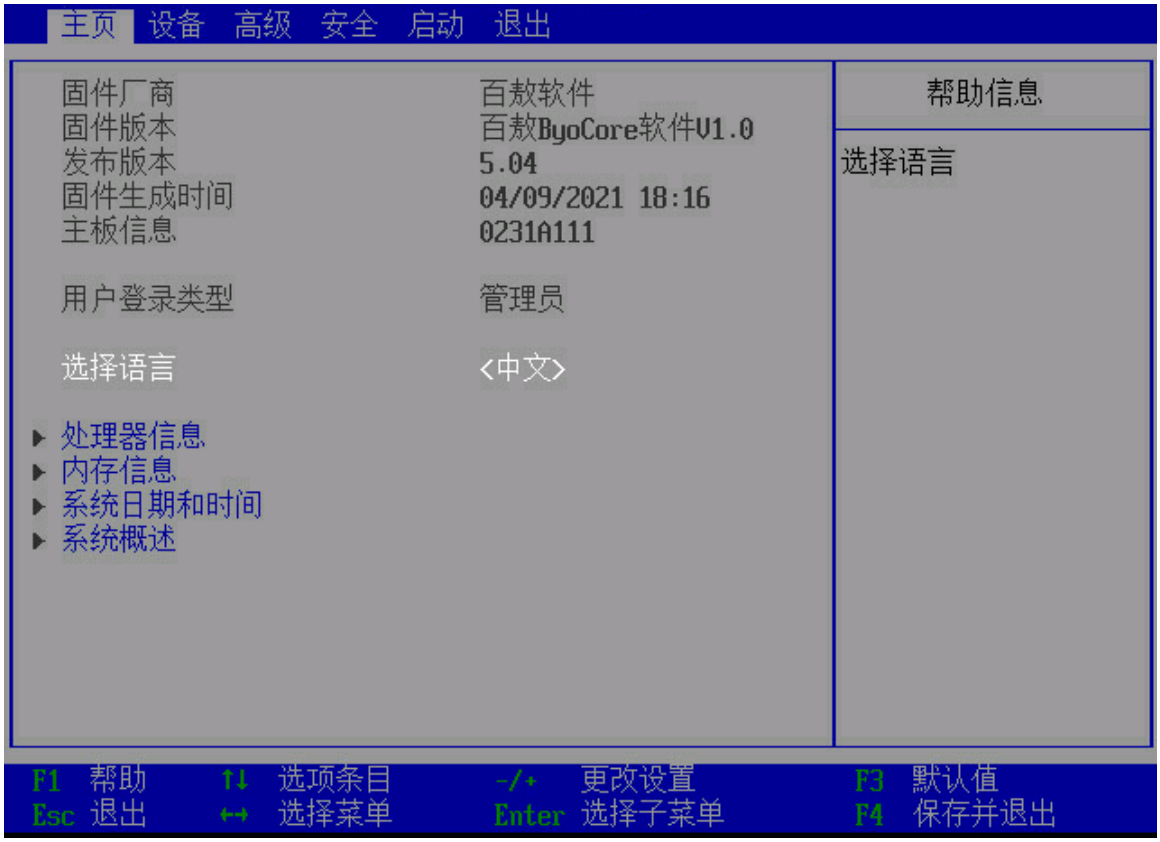


表2-1 操作说明

操作项	功能说明
F1	获取操作项的帮助信息
F3	加载缺省值
F4	保存设置并退出BIOS配置界面
Esc	退出BIOS配置界面或返回上一层菜单

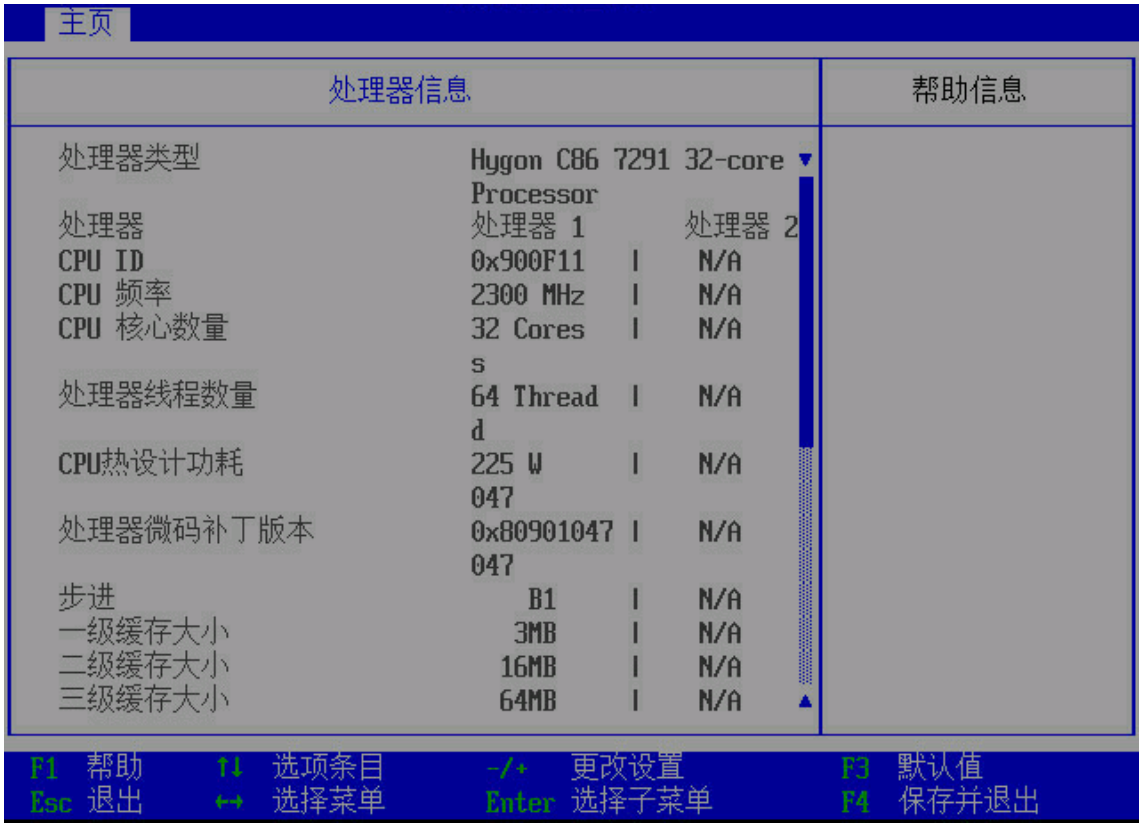
↑ ↓	向上或向下选择选项
←→	向左或向右选择菜单
+/-	选择当前选项的前一个或后一个选项或数值
回车键	执行选项或选择子菜单

2.2 查询处理器信息

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 在 BIOS 配置界面中，进入**主页**页签，选择**处理器信息**，然后按**回车**键。如图 2-5 所示，进入**处理器信息**界面。

图2-5 处理器信息界面

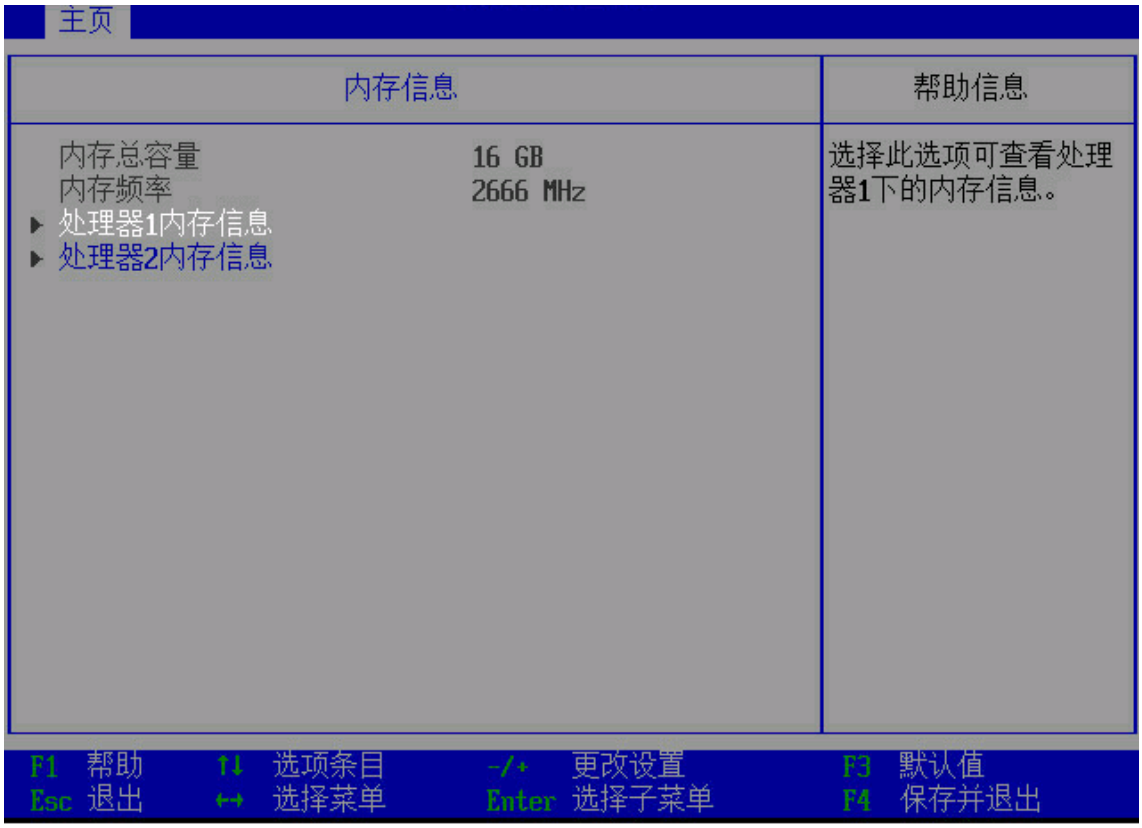


2.3 查询内存信息

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 在 BIOS 配置界面中，进入**主页**页签，选择**内存信息**，进入如图 2-6 所示界面。

图2-6 内存信息界面



(3) 以查询处理器 1 下的内存详细信息为例进行介绍。选择**处理器 1 内存信息**菜单项，然后按**回车**键，进入如图 2-7 所示界面，可以查看到对应槽位安装的内存的详细信息。

图2-7 处理器 1 内存信息

2.4 查询板载硬盘信息

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 在 BIOS 配置界面中，进入**设备**页签，选择 **SATA 配置**，然后按**回车**键。如图 2-8 所示，进入 SATA（Serial Advanced Technology Attachment，串行 ATA）配置界面，显示硬盘信息。

图2-8 SATA 配置界面

(3) 选择 **SATA 控制器 1 配置**，然后按**回车**键。如图 2-9 所示，进入 SATA 控制器 1 配置界面，显示硬盘信息。

图2-9 SATA 控制器 1 配置界面

2.5 查询HDM网络信息

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 在 BIOS 配置界面中，进入[高级/服务管理/HDM 网络配置]界面，如图 2-10 所示，显示 HDM 网络信息。

图2-10 HDM 网络配置界面

2.6 设置HDM网络信息

1. 功能简介

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

2. 准备工作

数据准备：HDM 专用/共享网口的 IP 地址、子网掩码和网关。

3. 操作步骤

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 在 BIOS 配置界面中，进入[高级/服务管理/HDM 网络配置]界面，如图 2-10 所示，显示 HDM 网络信息。有 HDM 共享网口（共享局域网配置）和 HDM 专用网口（专用局域网配置）可供选择，本文以配置 HDM 专用网口的 IPv4 网络信息为例进行介绍。

(3) 选择“专用局域网配置”下的 **IPv4 地址模式**，按**回车**键。

注意

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

(4) 在弹出的对话框中选择 HDM 网络信息的获取方式。HDM 专用/共享网口获取网络信息有以下几种方式：

- 静态：手动配置网络信息。
- 动态：通过 DHCP 自动分配获取网络信息。

(5) 如图 2-11 所示：

- 选择**静态**或者**动态**后，请按**回车**键。
- 选择**静态**时，请分别选择表 2-2 中的参数，在弹出的对话框中输入相关信息，然后按**回车**键。

图2-11 HDM 网络配置界面

表2-2 手动配置 HDM IPv4 网络信息

界面参数	含义	备注
IPv4地址	静态IP地址	必配

界面参数	含义	备注
IPv4子网掩码	静态IP地址对应的子网掩码	必配
IPv4默认网关	网关IP地址	可选

(6) 设置完成后，按 **F4** 保存并退出。

2.7 设置BIOS密码

2.7.1 BIOS 密码简介

BIOS 密码包括开机密码和 BIOS Setup 的管理员密码、用户密码。缺省情况下没有设置任何密码。

- 开机密码需要在服务器开机过程中输入，设置后每次启动均需要输入。
- 管理员密码和用户密码需要在进入 BIOS Setup 时输入。
  - 当使用管理员角色登录时，获取的 BIOS 权限为管理员权限。通过热键进入 BIOS Setup、iFIST、Boot Menu 和 PXE Boot 时均需要提供管理员密码。
  - 当使用用户角色登录时，获取的 BIOS 权限为用户权限。当以用户权限进入 BIOS Setup 后，仅支持对用户密码进行设置，其余选项仅支持查看。

2.7.2 密码设置注意事项

修改密码时，禁止使用三次内的历史密码。

密码设置需符合以下要求：

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

2.7.3 设置 BIOS 密码操作

说明

- 设置管理员密码和设置用户密码或开机密码的方法相同，本文以设置管理员密码为例进行介绍。
- 设置用户密码时，建议同时设置管理员密码。

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 进入**安全**页签，选择**设置管理员密码**，按**回车**键。

(3) 进入图 2-12所示界面，在弹出的对话框中输入密码，密码设置需符合 2.7.2 密码设置注意事项的要求。输入完成后，按**回车**键。

图2-12 输入密码

(4) 进入图 2-13 所示界面，再次输入密码，按**回车**键。

图2-13 确认密码

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

2.7.4 清除 BIOS 密码操作

说明

清除管理员密码和清除用户密码或开机密码的方法相同，本文以清除管理员密码为例。

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 进入**安全**页签，选择**设置管理员密码**，按**回车**键。

(3) 弹出如图 2-14 所示对话框，输入已设定的管理员密码。

图2-14 输入原密码

(4) 弹出如图 2-15 所示的对话框，不输入任何字符，按**回车**键。

图2-15 输入新密码

(5) 弹出如图 2-16 所示的对话框，选择“是”，按**回车**键。

图2-16 确认删除密码

(6) 密码删除成功。

2.8 设置系统日期和时间

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 在 BIOS 配置界面中，进入**主页**页签，选择**系统日期与时间**，进入如图 2-17 所示界面。

图2-17 Main 界面

(3) 选择**系统日期**，系统日期的格式为“月/日/年”。按 **Tab** 在月、日、年之间切换，可通过以下方式来修改数值：

- 按“**+**”：数值加 1。
- 按“**-**”：数值减 1。
- 按数字键：直接修改数值。

(4) 选择**系统时间**，系统时间为 24 小时制，格式为“时:分:秒”。按 **Tab** 在时、分、秒之间切换，可通过以下方式来修改数值：

- 按“**+**”：数值加 1。
- 按“**-**”：数值减 1。
- 按数字键：直接修改数值。

2.9 设置BIOS启动模式

1. 功能简介

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

2. 操作步骤

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 如图 2-18 所示，进入**启动**页签，选择**启动模式**，按**回车**键，在弹出的对话框中选择启动模式。

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

图2-18 设置 BIOS 启动模式

(3) 设置完成后，按 **F4** 保存并退出。

2.10 设置服务器启动顺序

1. 功能简介

服务器缺省的启动顺序如图 2-19 所示，各参数含义见表 2-3，各选项的排列顺序即服务器的启动顺序。

2. 操作步骤

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 如图 2-19 所示，选择**启动**页签，进入启动页面。

图2-19 启动界面

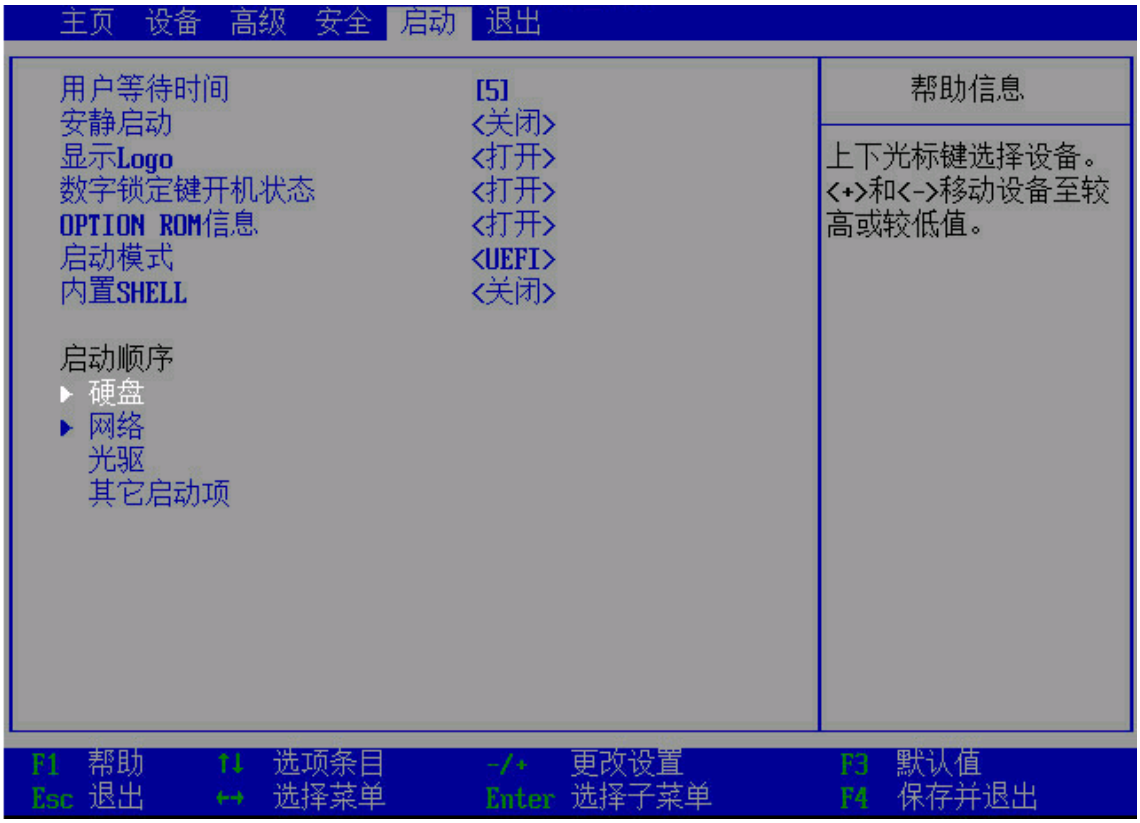
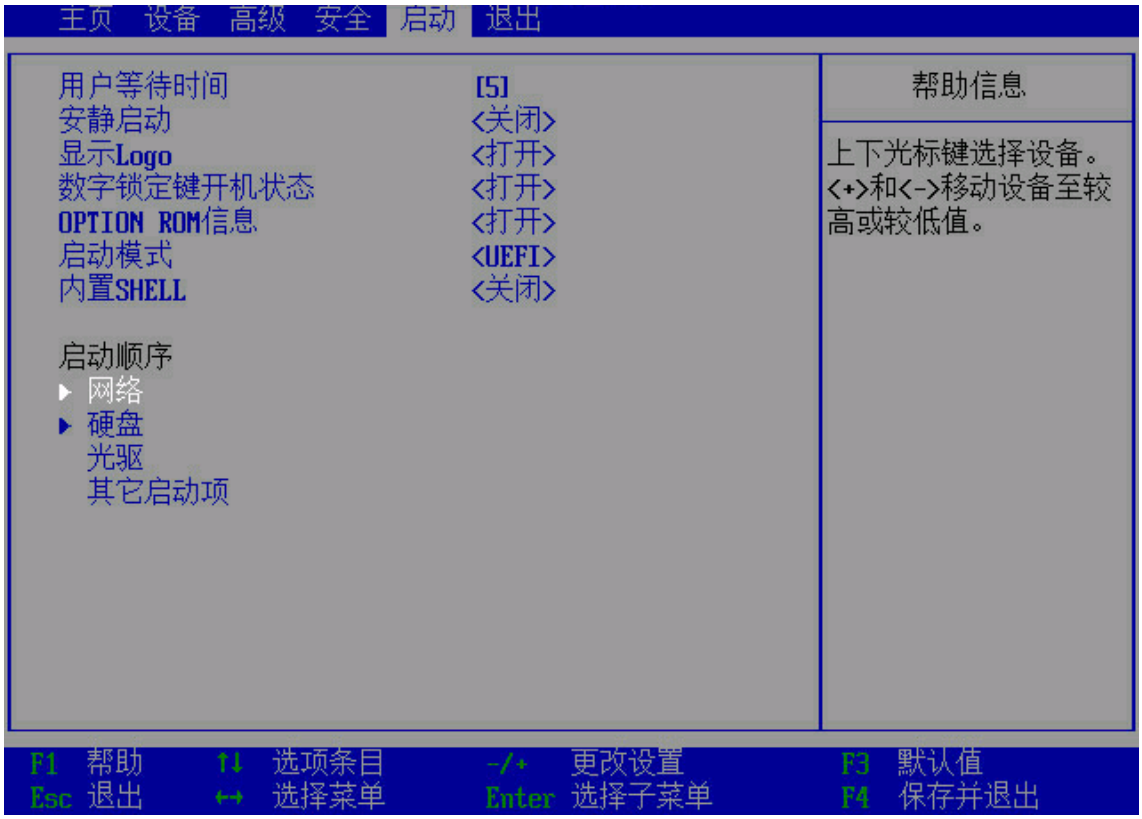


表2-3 服务器启动项

启动项	含义
硬盘	硬盘和USB的启动项
网络	网络启动选项，如PXE的启动项
光驱	光驱（包括虚拟光驱）
其它启动项	其他启动设备，包括进入内置的UEFI Shell的启动项，当“内置SHELL”选项设置为“打开”时才显示

(3) 如图 2-20 所示，选择要调整顺序的启动项类别，通过“+”键向上调整，“-”键向下调整。

图2-20 设置启动项



(4) 如需设置某一类启动项内的子项顺序，选择该启动项类别后，按**回车**键，如图 2-21 所示，通过“+”键向上调整，“-”键向下调整。

图2-21 设置启动项

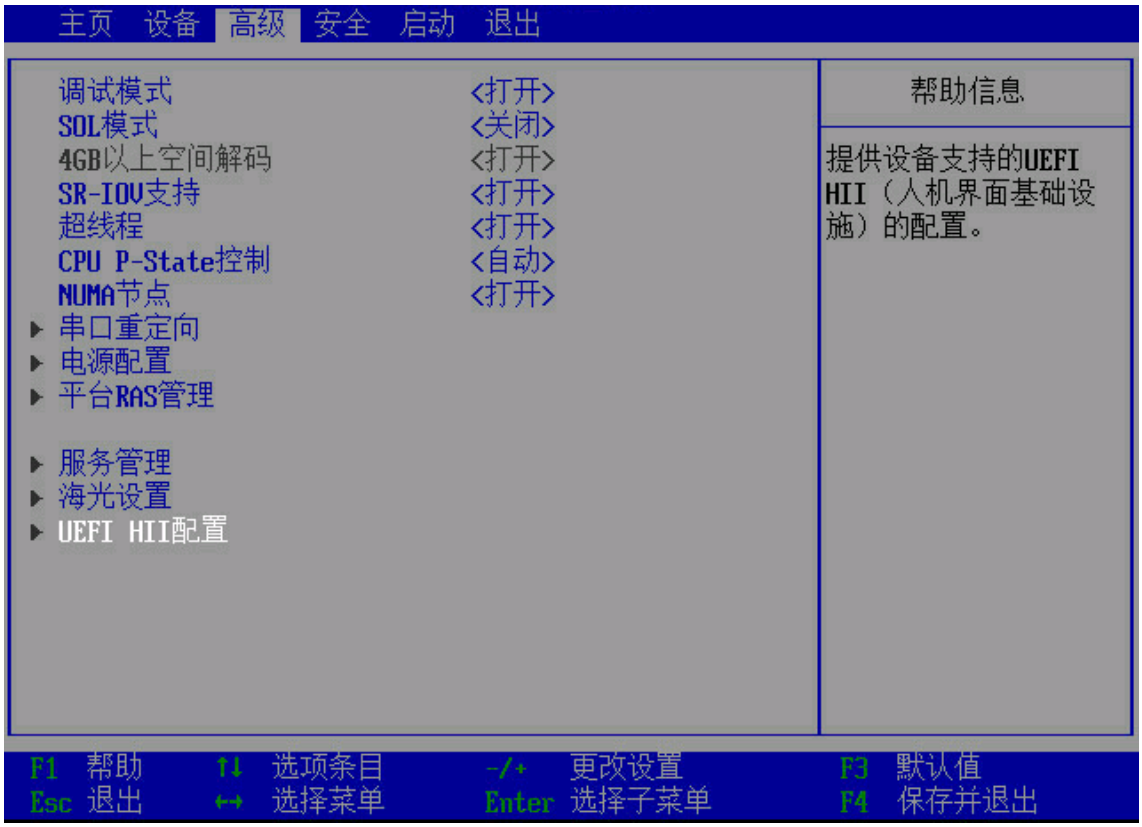
(5) 设置完成后，按 **F4** 保存并退出。

2.11 配置RAID

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

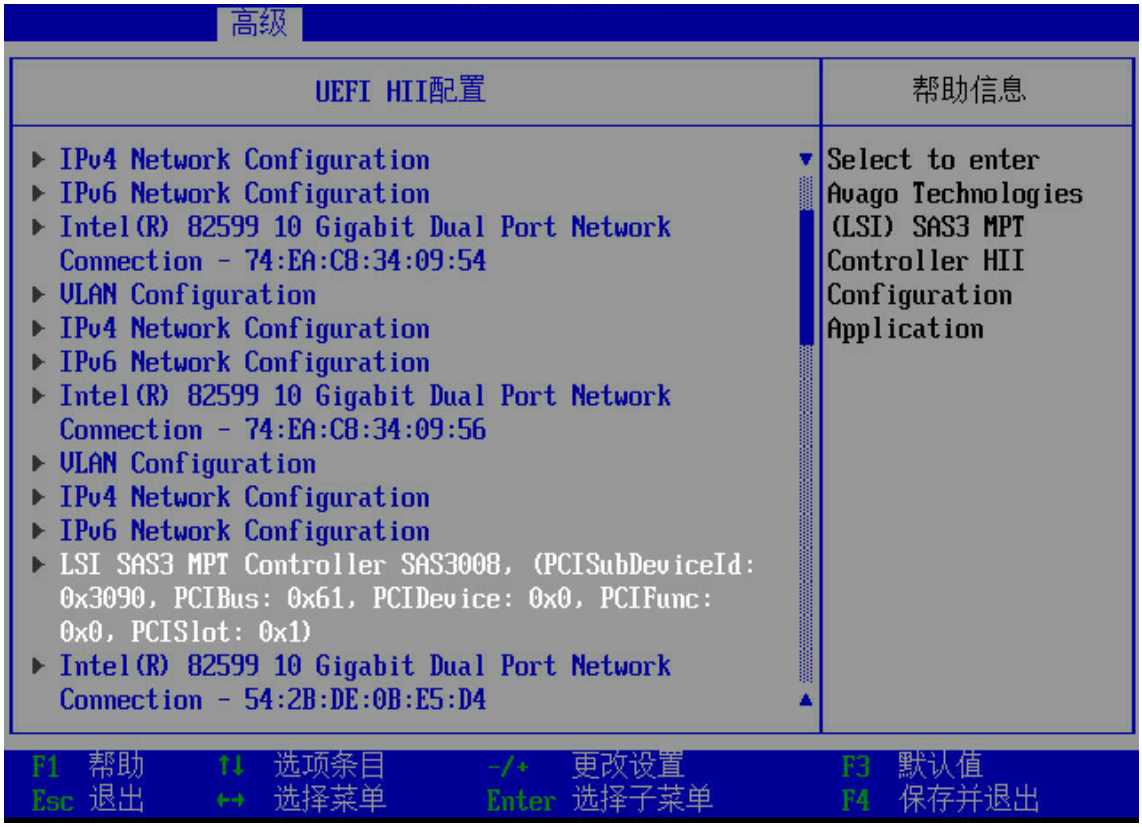
(2) 如图 2-22 所示，选择**高级**页签，选择 **UEFI HII 配置**选项，按**回车**键。

图2-22 选择 UEFI HII 配置



(3) 如图 2-23 所示，进入 UEFI HII 配置界面，选择对应存储控制卡的配置选项，进入存储控制卡配置页面。通过 BIOS 配置 RAID 的具体方法请参见《UNIS 服务器 存储控制卡用户指南》。

图2-23 UEFI HII 配置页面



2.12 恢复BIOS缺省设置

1. 功能简介

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

2. 操作步骤

(1) 进入服务器的 BIOS 配置界面，具体步骤请参见 2.1 进入 BIOS 界面。

(2) 如图 2-24 所示，进入**退出**页签，选择**恢复初始值**，按**回车**键。

提示

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

图2-24 恢复缺省设置


主页 设备 高级 安全 启动 退出
保存更改
保存退出
放弃修改
不保存并且退出
恢复初始值
BIOS固件更新
关机
重启
Boot Override
UEFI Slot 16: Port 1 - Intel(R) I350 Gigabit Network Connection PXE IPv4
UEFI Slot 16: Port 2 - Intel(R) I350 Gigabit Network Connection PXE IPv4
UEFI Slot 16: Port 3 - Intel(R) I350 Gigabit
帮助信息
为每个选项恢复/加载默认值。
F1 帮助
Esc 退出
↑↓ 选项条目
↔ 选择菜单
-/+ 更改设置
Enter 选择子菜单
F3 默认值
F4 保存并退出

3 界面参数说明

3.1 主页界面

主页界面如图 3-1 所示，主要包含 BIOS 固件信息、处理器信息、内存信息、系统日期和时间、系统概述。具体参数说明如表 3-1 所示。

图3-1 主页界面

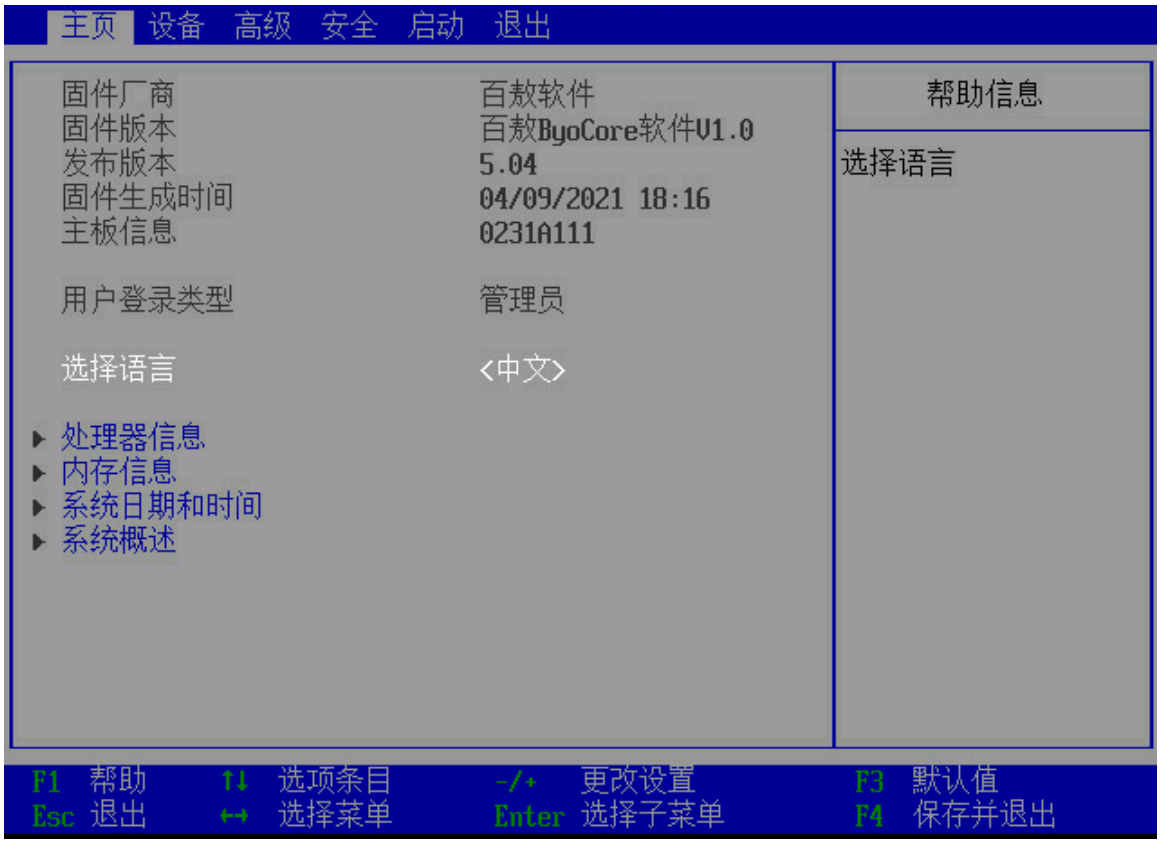


表3-1 主页界面参数

界面参数	功能说明
固件厂商	显示固件厂商
固件版本	显示BIOS固件版本
发布版本	显示BIOS固件版本的对外版本号
固件生成时间	显示BIOS编译日期和时间
主板信息	显示主板编号
用户登录类型	显示用户的登录类型，分为管理员和用户两种

界面参数	功能说明
选择语言	显示和设置当前系统语言。按回车键，选择如下两种系统语言： • English • 中文（缺省）
处理器信息	查询处理器的信息的菜单
内存信息	查询内存信息的菜单
系统日期和时间	设置系统日期和时间的菜单
系统概述	系统概述菜单

3.1.1 处理器信息

处理器信息界面如图 3-2 和图 3-3 所示，主要显示 CPU 和 PSP（Platform Security Processor，平台安全处理器）固件版本的基本信息。具体参数说明如表 3-2 所示。

图3-2 处理器信息界面 1

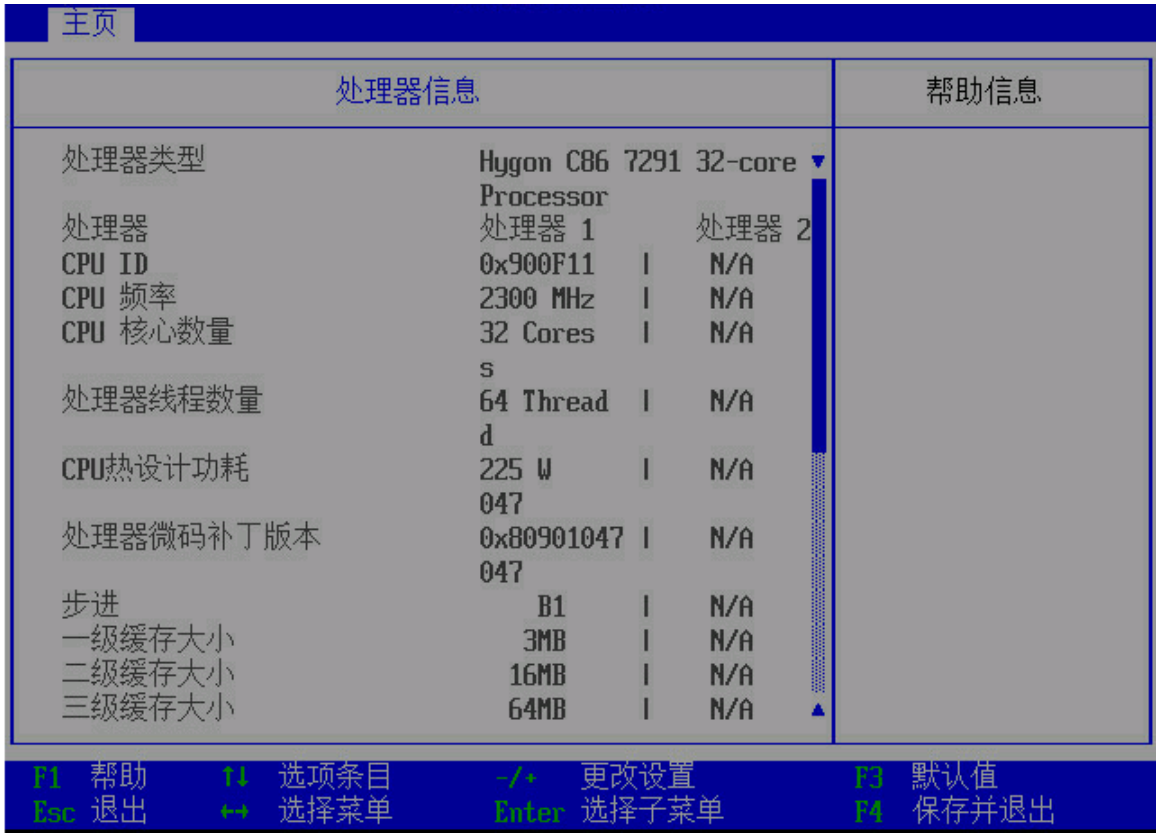


图3-3 处理器信息界面 2

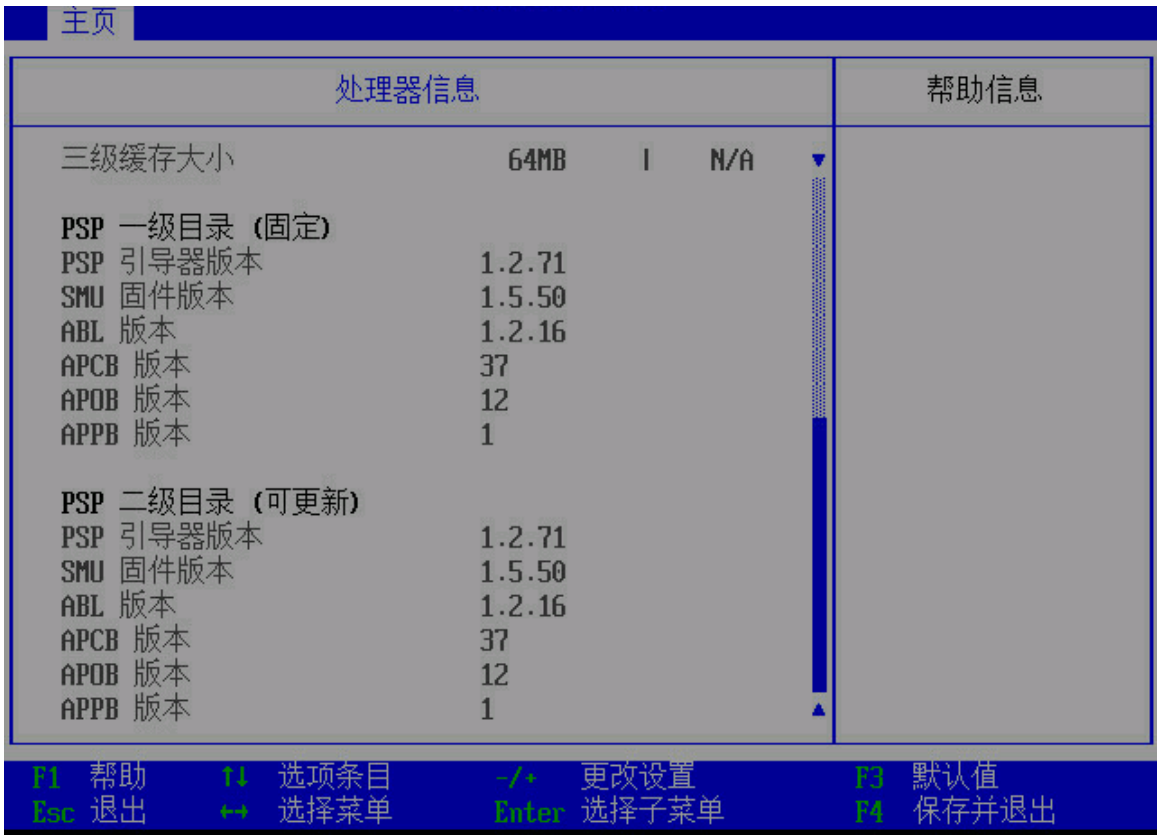


表3-2 处理器信息界面参数

界面参数	功能说明
CPU类型	显示CPU型号
CPU ID	显示CPU ID
CPU频率	显示CPU主频
CPU核心数量	显示CPU核心数量
一级缓存大小	显示CPU L1缓存容量
二级缓存大小	显示CPU L2缓存容量
三级缓存大小	显示CPU L3缓存容量
PSP固件版本	显示PSP固件版本信息
PSP一级目录（固定）	显示PSP一级目录信息，该版本为固定的PSP版本
PSP引导器版本	显示PSP可恢复的BootLoader版本
SMU固件版本	显示SMU（System Management Unit，系统管理单元）固件版号

界面参数	功能说明
ABL版本	显示ABL（AGESA boot loader）版本号
APCB版本	显示APCB（AMD PSP Control Block）版本号
APOB版本	显示APOB（AGESA PSP Output Block）版本号
APPB版本	显示APPB（AGESA PSP PMU Block）版本号
PSP二级目录（可更新）	下方选项显示PSP二级目录信息，该版本为可更新版本
PSP引导器版本	显示PSP BootLoader版本
SMU固件版本	显示SMU固件版本
ABL版本	显示ABL版本号
APCB版本	显示APCB版本号
APOB版本	显示APOB版本号
APPB版本	显示APPB版本号

3.1.2 内存信息

内存信息界面如图 3-4 所示，主要显示内存容量、内存频率和已接入的内存基本信息。具体参数说明如表 3-3 所示。

图3-4 内存信息界面

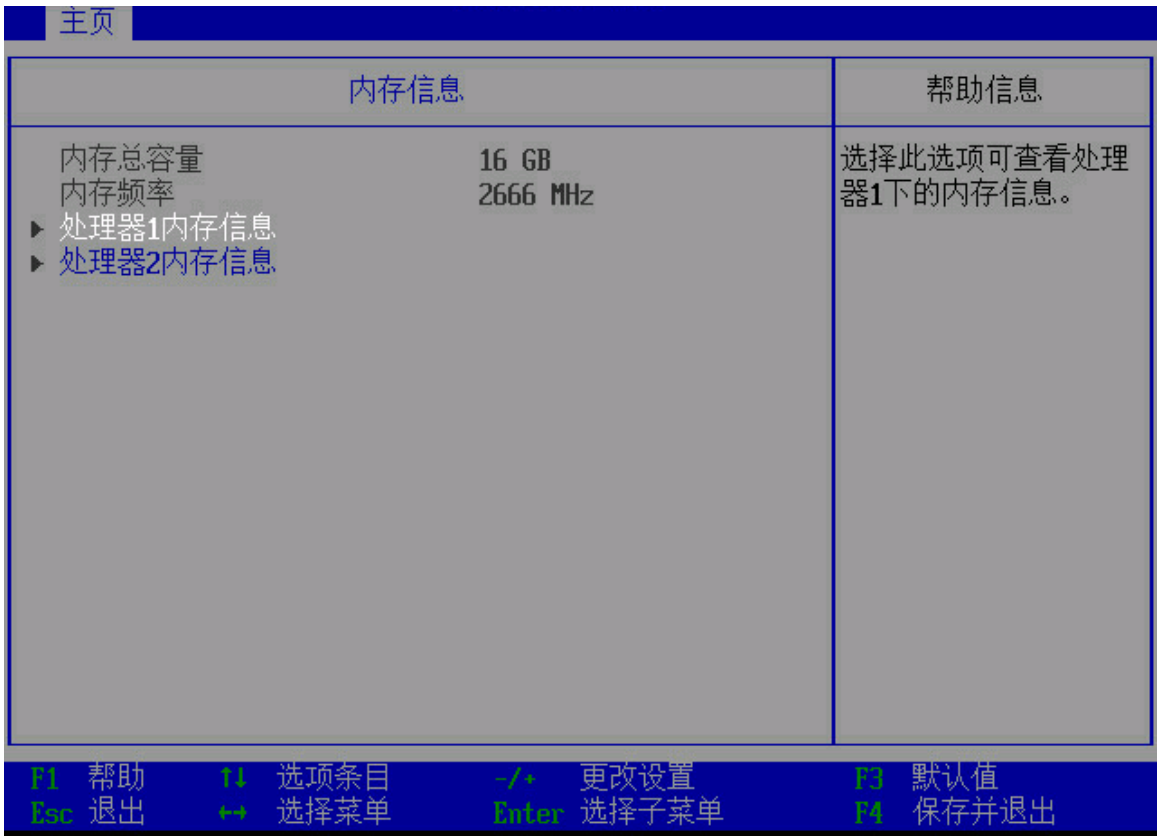


表3-3 内存信息界面参数

界面参数	功能说明
内存总容量	显示接入的内存总容量，单位为GB
内存频率	显示最大内存频率，单位MHz
处理器*n*内存信息	对应处理器下的内存信息菜单

处理器内存信息界面如图 3-5 所示，具体参数说明如表 3-4 所示。

图3-5 处理器内存信息界面

表3-4 处理器内存信息界面参数

界面参数	功能说明
Processor1 Ch3 DIMM C0（示例）	显示内存信息及在位情况，不在位时显示“未安装” 内存信息中，包含生产商、PN码、容量及位宽、内存类型、是否支持ECC、SN码

3.1.3 系统日志和时间

系统日期和时间界面如图 3-6 所示，对系统的日期和时间进行设置。具体参数说明如表 3-5 所示。

图3-6 系统日期和时间界面

表3-5 系统日期和时间界面参数

界面参数	功能说明
系统日期（月/日/年）	设置系统日期，按照月/日/年的格式显示，使用Tab键可以在日期区域切换
系统时间（时：分：秒）	设置系统时间，按照时：分：秒的格式设置，使用Tab键可以在时间区域切换

3.1.4 系统概述

系统概述界面如图 3-7 所示，显示系统信息及设置主机编号和资产管理名称。具体参数说明如表 3-6 所示。

图3-7 系统概述界面

表3-6 系统概述界面参数

界面参数	功能说明
主机商标标识	显示主机的厂商
产品型号	显示产品型号
主机编号	设置服务器的产品序列号，长度为2~20位，仅支持字母和数字
资产管理名称	设置资产编号，长度为1～48个字符，仅支持字母、数字、空格和特殊字符`~!@#$%^&*()_+-=[]{}|;':\",./<>?
系统UUID	显示系统的UUID
UEFI版本号	显示UEFI的版本号和PI版本号

3.2 设备界面

设备界面如图 3-8 所示，用于配置各种硬件设备的功能。具体参数说明如表 3-7 所示。

图3-8 设备界面

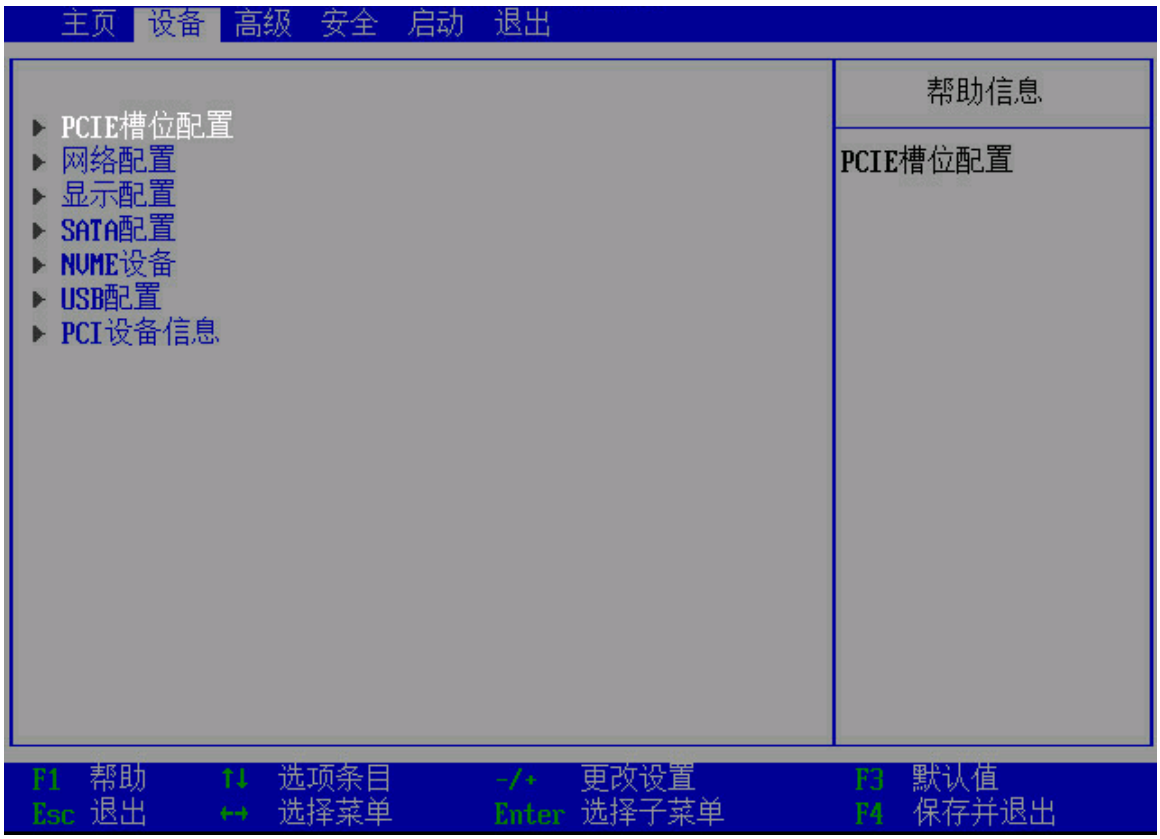


表3-7 设备界面参数

界面参数	功能说明
PCIE槽位配置	PCIe槽位配置菜单
网络配置	网络配置菜单，包括PXE网络引导设置等
显示配置	显示配置菜单，用于设置优先使用的显卡
SATA配置	SATA配置菜单
NVME设备	NVMe（Non-Volatile Memory Express，非易失性内存标准）设备配置菜单
USB配置	USB（Universal Serial Bus，通用串行总线）配置菜单
PCI设备信息	PCI（Peripheral Component Interface，外围组件接口）设备显示菜单

3.2.1 PCIe 槽位配置

PCIe 槽位配置界面如图 3-9 所示。本页面选项根据接入的 PCIe 设备动态显示。具体参数说明如表 3-8 所示。

图3-9 PCIe 槽位配置界面

表3-8 PCIe 槽位配置界面参数

界面参数	功能说明
OCP3.0	OCP3.0网卡功能的开关。菜单选项为： • 打开（缺省） • 关闭
RISER1	
Slot *n*	RISER下各个槽位的功能控制开关。菜单选项为： • 打开（缺省） • 关闭

3.2.2 网络配置

网络配置界面如图 3-10 所示。具体参数说明如表 3-9 所示。

图3-10 网络配置界面

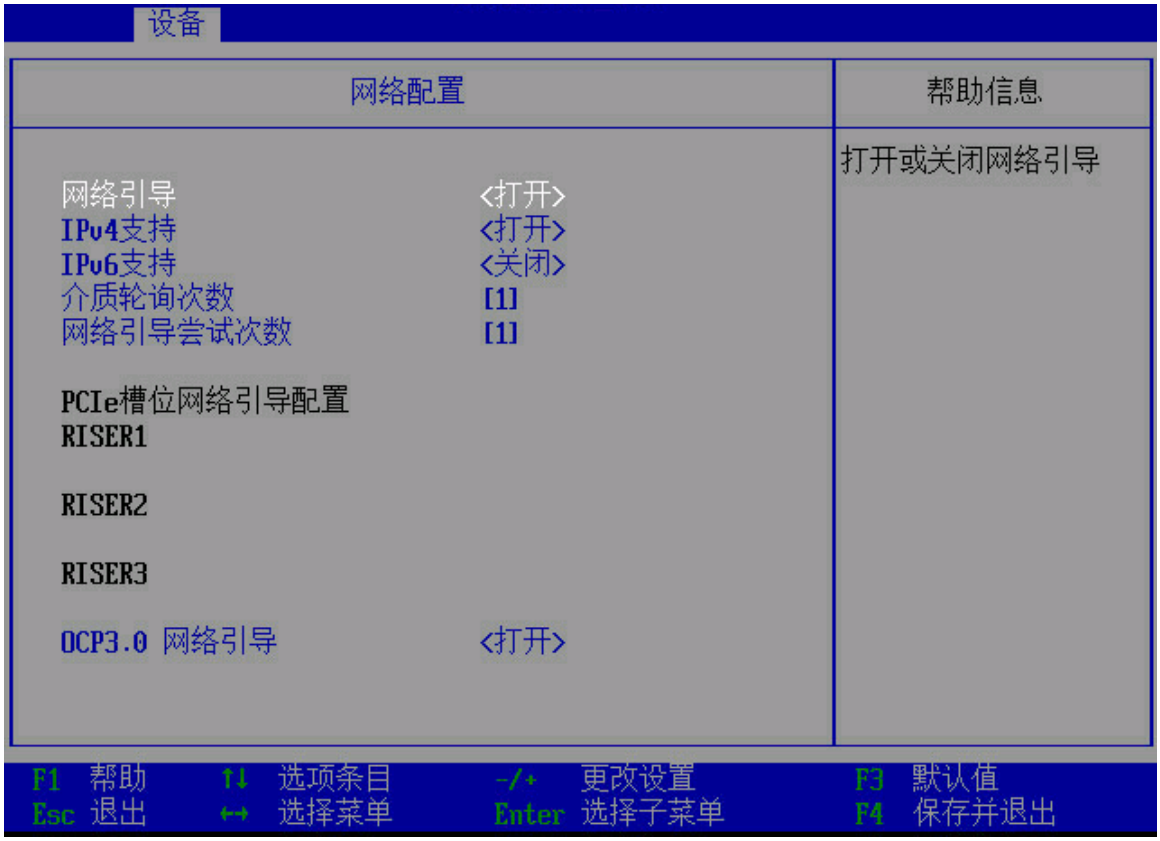


表3-9 网络配置界面参数

界面参数	功能说明
网络引导	设置是否启用PXE网络引导。菜单选项为： • 打开（缺省） • 关闭
IPv4支持	支持IPv4网络引导功能开关，菜单选项为： • 打开（缺省） • 关闭
IPv6支持	支持IPv6网络引导功能开关，菜单选项为： • 打开 • 关闭（缺省）
介质轮询次数	媒介设备检测计数，用于检测媒介在位次数，取值范围1～50，缺省值为1，单位为次
网络引导尝试次数	PXE轮询次数，取值范围0～50，缺省值为1，单位为次，0表示始终进行PXE轮询

界面参数	功能说明
PCIe槽位网络引导配置	PCIe槽位网络引导功能设置，对应Riser下接入了PCIe设备时，显示设置选项
OCP3.0网络引导	OCP 3.0网络引导功能开关，菜单选项为： • 打开（缺省） • 关闭

3.2.3 显示配置

显示配置界面如图 3-11 所示。具体参数说明如表 3-10 所示。

图3-11 显示配置界面

表3-10 显示配置界面参数

界面参数	功能说明
优先显示控制器	设置优先选择的输出显卡，菜单选项为： • 外插显卡 • 板载显卡（缺省）

界面参数	功能说明
板载显卡	显示板载显卡的型号
外插显卡	显示外插显卡的型号

3.2.4 SATA 配置

SATA 配置界面如图 3-12 所示。具体参数说明如表 3-11 所示。

图3-12 SATA 配置界面

表3-11 SATA 配置界面参数

界面参数	功能说明
SATA控制器 *n* 配置	该 SATA 控制器下 SATA 设备的配置菜单

SATA 控制器配置界面如图 3-13 所示。具体参数说明如表 3-12 所示。

图3-13 SATA 控制器配置界面

表3-12 SATA 控制器配置界面参数

界面参数	功能说明
SATAPort*n*	SATA端口控制，菜单选项为： • 打开（缺省）：启用该 SATA 端口 • 关闭：禁用该 SATA 端口
SATA Portn Speed	SATA端口速率控制，菜单选项为： • 最大支持（缺省）：使用支持的最大速率 • Gen1 • Gen2
驱动器名	当对应SATA端口的设备在位时，显示设备信息。设备不在位时，显示未安装

3.2.5 NVMe 设备

NVMe 设备界面如图 3-14 所示。具体参数说明如表 3-13 所示。

图3-14 NVMe 设备界面

表3-13 NVMe 设备界面参数

界面参数	功能说明
Slot 29：INTEL SSDPE2KX010T8 SN:PHLJ9120022R1P0FGN Size:1000.2GB	显示NVMe设备的信息，包括槽位号、厂商、名称、SN号和容量信息

3.2.6 USB 配置

USB 配置界面如图 3-15 所示。具体参数说明如表 3-14 所示。

图3-15 USB 配置界面

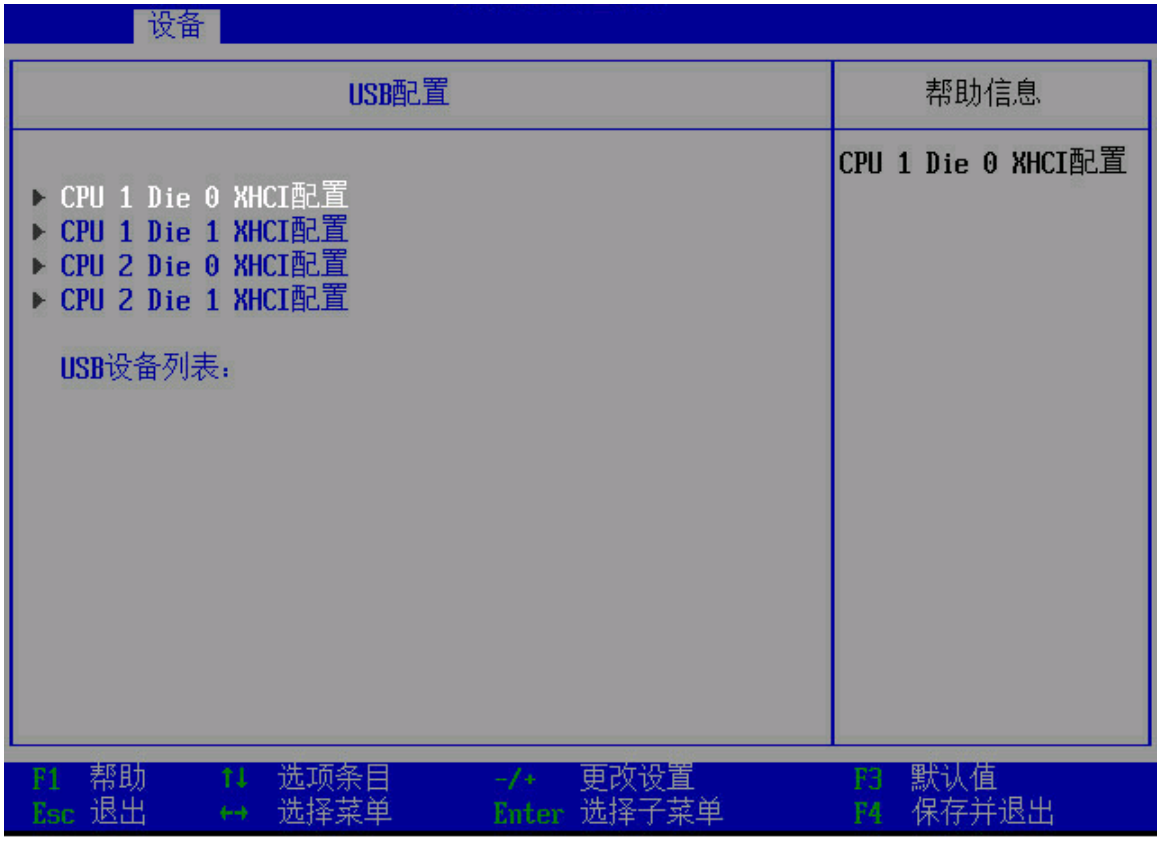


表3-14 USB 配置界面参数

界面参数	功能说明
CPU1 Die 0 XHCI配置	CPU1 Die 0 XHCI 配置菜单
CPU1 Die 1 XHCI配置	CPU1 Die 1 XHCI配置菜单
CPU2 Die 0 XHCI配置	CPU2 Die 0 XHCI 配置菜单
CPU2 Die 1 XHCI配置	CPU2 Die 1 XHCI配置菜单
USB设备列表	查看当前接入的USB设备列表

USB 配置界面如图 3-16 所示。具体参数说明如表 3-15 所示。

图3-16 USB 配置界面

表3-15 USB 配置界面参数

界面参数	功能说明
USB2.0 Port *n*	USB2.0 端口功能控制开关。菜单选项为： • 打开（缺省） • 关闭
USB3.0 Port *n*	USB3.0 端口功能控制开关。菜单选项为： • 打开（缺省） • 关闭

3.2.7 PCI 设备信息

PCI 配置界面如图 3-17 所示，显示系统下所有 PCI 设备信息。具体参数说明如表 3-16 所示。

图3-17 PCI 设备信息界面

表3-16 PCI 设备信息界面参数

界面参数	功能说明
BUS	列出 PCI 设备的总线号
DEV	列出 PCI 设备的设备号
FUN	列出 PCI 设备的功能号
Vendor ID	列出PCI设备的厂商ID
Device ID	列出PCI设备的设备ID
Device Class	列出PCI设备的设备类型

3.3 高级界面

高级界面如图 3-18 所示。具体参数说明如表 3-17 所示。

图3-18 高级界面

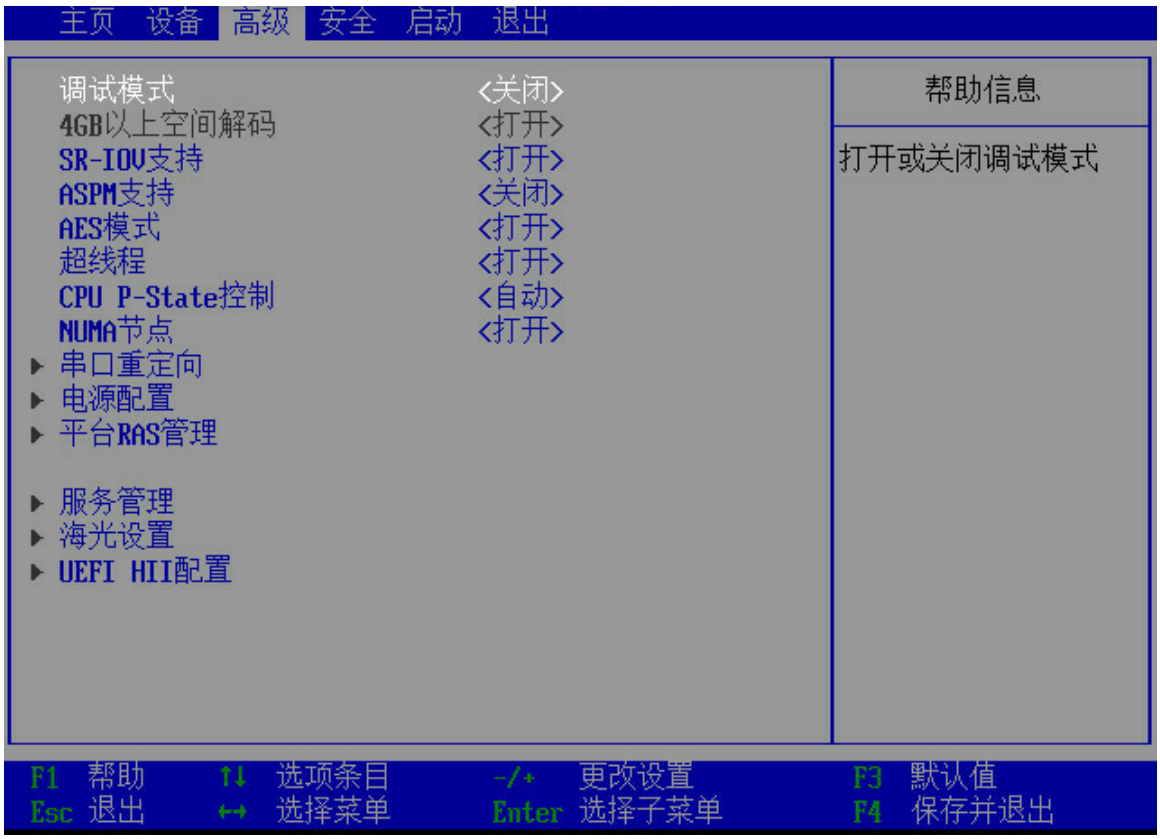


表3-17 高级界面参数

界面参数	功能说明
调试模式	BIOS调试模式开关，开启该功能后，服务器能输出BIOS串口日志，菜单选项为： • 打开（缺省）：开启 BIOS 串口日志输出功能。选择该选项后，您可以通过连接串口，获取 BIOS 串口日志 • 关闭：关闭 BIOS 串口日志输出功能
4GB以上空间解码	4GB以上内存访问控制设置，当系统支持64位PCIe解码时，在4GB以上地址空间对64位设备进行解码，菜单选项为： • 打开（缺省）：开启 4G 以上译码 • 关闭：关闭 4G 以上译码 “4GB以上空间解码”设为“关闭”时会导致显存超过4GB的PCIe设备无法解码

界面参数	功能说明
SR-IOV支持	SR-IOV（Single Root I/O Virtualization，单根I/O虚拟化）支持设置。SR-IOV技术的主要作用是将一个物理PCIe设备模拟成多个虚拟设备，其中每一个虚拟设备可以与一个虚拟机绑定，便于不同的虚拟机访问同一个物理PCIe设备。菜单选项为： • 打开（缺省）：启用 SR-IOV 机制。如系统中有支持 SR-IOV 的 PCIe 设备，由 BIOS 分配虚拟化 IO 资源 • 关闭：禁用 BIOS 对 SR-IOV 机制的支持。如果 PCIe 卡支持 SR-IOV，则由 OS 分配虚拟化 IO 资源
ASPM支持	配置ASPM（Active State Power Management，活动状态电源管理）链路电源管理控制功能。菜单选项为： • 打开：启动 ASPM 支持 • 关闭（缺省）：禁用 ASPM 支持
AES模式	配置AES（Advanced Encryption Standard，高级加密标准）模式功能。菜单选项为： • 打开（缺省）：启用 AES 模式 • 关闭：禁用 AES 模式
超线程	超线程开关，超线程技术可以把1个物理内核模拟成2个逻辑内核，让单个处理器都能使用线程级并行计算，进而兼容多线程操作系统和软件，减少CPU闲置时间，提高CPU的运行效率，不支持超线程功能的CPU不显示该选项，菜单选项为： • 打开（缺省）：开启超线程功能 • 关闭：关闭超线程功能
CPU P-State控制	CPU的P状态控制选项。菜单选项为： • 打开：启用 CPU P-State 控制，启用后，处理器可以依据运算量负载轻重，调整运行频率的高低 • 关闭：禁用 CPU P-State 控制 • 自动（缺省）：自动启用 CPU P-State 控制
NUMA节点	选择是否打开NUMA（Non-uniform memory access，非统一内存访问架构）。在NUMA架构下，处理器更多的访问本地内存，相较访问非本地内存（内存位于另一个处理器，或者是处理器之间共享的内存）快一些，降低CPU对内存的访问时间。菜单选项为： • 打开（缺省）：启用 NUMA 节点 • 关闭：禁用 NUMA 节点
串口重定向	串口重定向设置菜单

界面参数	功能说明
电源配置	电源配置菜单
平台RAS管理	RAS配置菜单
服务管理	服务管理菜单
海光设置	海光设置菜单
UEFI HII配置	UEFI HII配置菜单

3.3.1 串口重定向

串口重定向界面如图 3-19 所示。具体参数说明如表 3-18 所示。

图3-19 串口重定向界面

表3-18 串口重定向界面参数

界面参数	功能说明
串口重定向	串口重定向配置开关,将指定的物理串口或虚拟串口的数据映射到指定的系统串口，菜单选项为： • 打开：开启串口重定向功能 • 关闭（缺省）：关闭串口重定向功能
串口波特率	每秒传输比特数配置，传输速度必须和对端串口匹配，超长或嘈杂的线路可能需要较低的速度。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • 9600 • 19200 • 38400 • 57600 • 115200（缺省）
数据位	串口传输中有效数据位数。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • 7 • 8（缺省）
奇偶校验	串口传输中奇偶校验设置。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • 无：关闭校验功能 • 偶校验 • 奇校验 • 标记：标记奇偶校验。奇偶校验位始终用值 1“标记”。如果标记奇偶校验位的值为 0，否则发生错误 • 空白：空白奇偶校验。奇偶校验位始终为 0，否则发生错误
停止位	串口传输中停止位设置。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • 1（缺省） • 2
流控制	串口传输中流控制设置。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • 无（缺省） • 硬件 RTS/CTS

界面参数	功能说明
终端模式	设置串口模式。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • 100 X 31 • 80 X 25（缺省）
终端类型	设置终端类型。当“串口重定向”选项设置为“打开”时显示该选项，菜单选项为： • ANSI • VT100 • VT100+ • VT-UTF8（缺省）

3.3.2 电源管理

电源管理界面如图 3-20 所示。具体参数说明如表 3-19 所示。

图3-20 电源管理界面

表3-19 电源管理界面参数

界面参数	功能说明
PCIe/PCI唤醒	PCIe/PCI唤醒功能开关。菜单选项为： • 打开：启用 PCIe/PCI 唤醒功能，启用后可以通过 PCIe 设备唤醒处于深度睡眠状态下的系统 • 关闭（缺省）：禁用 PCIe/PCI PME 唤醒功能

3.3.3 平台 RAS 管理

平台 RAS 管理如图 3-21 所示。具体参数说明如表 3-20 所示。

图3-21 平台 RAS 管理界面

表3-20 平台 RAS 管理界面参数

界面参数	功能说明
平台优先错误处理	设置平台优先错误处理，菜单选项为： • 打开（缺省）：启用平台优先错误处理 • 关闭：禁用平台优先错误处理

界面参数	功能说明
MCA错误数量控制	设置MCA（Machine Check Architecture，硬件检测架构）错误数量控制，菜单选项为： • 0：表示关闭 • 1 • 5 • 10 • 100 • 1000 • 2000（缺省）
内存CE风暴阈值	设置每分钟可纠正内存ECC（Error Checking and Correcting，错误检查和纠正）风暴阈值，菜单选项为： • 关闭（缺省） • 60 • 120 • 240 • 1200
内存CE累积阈值	设置内存CE（Corrected Error，可纠正错误）累积阈值，菜单选项为： • 关闭 • 1 • 500 • 1000 • 1200 • 2000（缺省） • 5000 • 10000

3.3.4 服务管理

服务管理界面如图 3-22 所示。具体参数说明如表 3-21 所示。

图3-22 服务管理界面

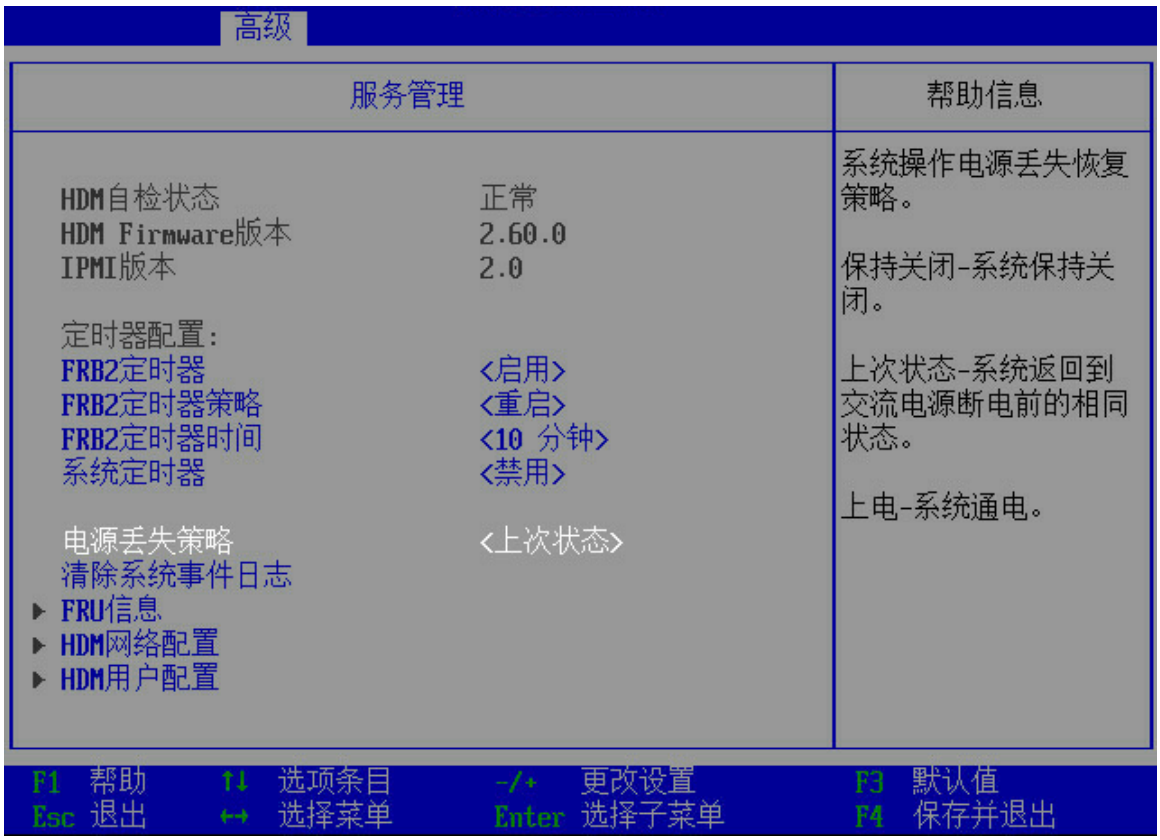


表3-21 服务管理界面参数

界面参数	功能说明
HDM自检状态	显示 HDM 自检状态
HDM Firmware版本	显示 HDM 固件版本号
IPMI版本	显示 IPMI 规范的版本号
定时器配置	
FRB2定时器	FRB-2定时器设置，菜单选项为： • 启用（缺省）：启用 FRB-2 定时器 • 禁用：禁用 FRB-2 定时器
FRB2定时器策略	FRB-2定时器到期后的策略设置，菜单选项为： • 重启（缺省） • 关闭电源 • 重新上电

界面参数	功能说明
FRB2定时器时间	FRB-2定时器到期时间设置，菜单选项为： • 5 分钟 • 6 分钟 • 7 分钟 • 8 分钟 • 9 分钟 • 10 分钟（缺省） • 15 分钟 • 30 分钟
系统定时器	OS看门狗定时器开关，开启该功能后，系统进入OS时，开启定时器，菜单选项为： • 启用：开启 OS 看门狗定时器 • 禁用（缺省）：关闭 OS 看门狗定时器
系统定时器策略	OS看门狗定时器策略设置，设置系统进入OS时，定时器超时后的动作。“系统定时器”设置为启用时，该选项可用，菜单选项为： • 重启 • 关闭电源（缺省） • 重新上电
系统定时器时间	OS看门狗定时器超时设置，设置系统进入OS时，定时器超时时间。“系统定时器”设置为启用时，该选项可用，菜单选项为： • 5 分钟 • 6 分钟 • 7 分钟 • 8 分钟 • 9 分钟 • 10 分钟（缺省） • 15 分钟 • 30 分钟

界面参数	功能说明
电源丢失策略	配置电源恢复时的策略，默认值为HDM默认值。BIOS LoadDefault时此菜单值不受影响。菜单选项为： • 保持关闭：电源恢复后，系统保持关闭 • 上次状态（缺省）：电源恢复后，系统返回到 AC 断电前的相同状态 • 上电：电源恢复后，系统上电
清除系统事件日志	清除系统事件日志选项，选择后将清除系统事件日志，SEL中所有当前目录都将丢失。此选项立即生效，无需重新启动
FRU信息	FRU信息菜单
HDM网络配置	HDM网络配置菜单
HDM用户配置	HDM用户配置菜单

1. FRU 信息

FRU 信息界面如图 3-23 所示。具体参数说明如表 3-22 所示。

图3-23 FRU 信息界面

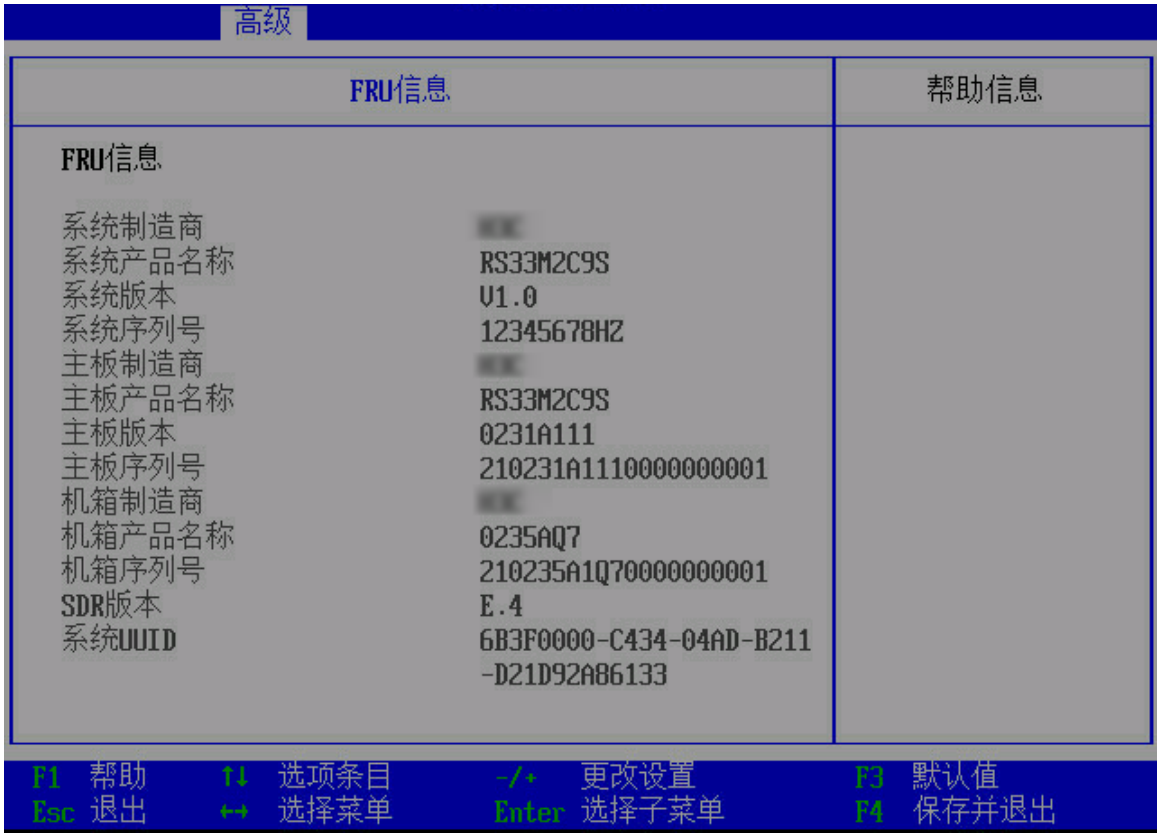


表3-22 FRU 信息界面参数

界面参数	功能说明
系统制造商	显示系统制造商
系统产品名称	显示系统产品名称
系统版本	显示系统版本
系统序列号	显示系统序列号
主板制造商	显示主板制造商
主板产品名称	显示主板产品名称
主板版本	显示主板版本
主板序列号	显示主板序列号
机箱制造商	显示机箱制造商
机箱产品名称	显示机箱产品名称
机箱序列号	显示机箱序列号
SDR版本	显示SDR版本
系统UUID	显示系统通用唯一识别码

2. HDM 网络配置

HDM 网络配置界面如图 3-24 所示。具体参数说明如表 3-23 所示。

图3-24 HDM 网络配置界面

说明

共享局域网配置和专用局域网配置的参数相同，配置时请注意不要将 HDM 共享局域网与专用局域网的 IP 地址配置在同一网段。

表3-23 HDM 网络配置界面参数

界面参数	功能说明
网口模式	显示HDM网络模式。根据从HDM获取的信息动态显示，可能的网络模式有： • 正常模式：该模式下可通过 HDM 共享网口或 HDM 专用网口访问 HDM • 网口自适应模式：该模式下 HDM 管理流量优先选择专用网口作为通信端口 • Bonding 模式：该模式将 HDM 共享网口和 HDM 专用接口作为一个逻辑上的网口使用
共享/专用局域网配置	

界面参数	功能说明
IPv4地址模式	配置网口的IPv4地址获取方式。菜单选项为： • 静态：手动配置网络信息 • 动态：通过 DHCP 分配获取网络信息
IPv4地址	网口的 IPv4 地址，当 IPv4 地址获取方式为静态时可设置。
IPv4子网掩码	网口的IPv4子网掩码，当IPv4地址获取方式为静态时可设置。
IPv4默认网关	网口的IPv4网关地址，当IPv4地址获取方式为静态时可设置。
IPv6	配置网口的IPv6地址是否启用。菜单选项为： • 启用 • 禁用
IPv6地址模式	配置网口的IPv6地址获取方式。菜单选项为： • 静态：手动配置网络信息 • 动态：通过 DHCP 分配获取网络信息
IPv6地址	网口的IPv6地址，当IPv6地址获取方式为静态时可设置。
IPv6前缀长度	网口的IPv6前缀长度，当IPv6地址获取方式为静态时可设置。

3. HDM 用户配置

HDM 用户配置界面如图 3-25 所示。具体参数说明如表 3-24 所示。

图3-25 HDM 用户配置界面

表3-24 HDM 用户配置界面参数

界面参数	功能说明
增加用户	添加用户配置菜单
删除用户	删除用户配置菜单
修改用户	修改用户配置菜单

增加用户

增加用户界面如图 3-26 所示。具体参数说明如表 3-25 所示。

图3-26 增加用户界面

表3-25 增加用户界面参数

界面参数	功能说明
用户名称	待创建的用户名称，长度为1～16个字符，仅支持字母、数字、句点（.）、连接符（-）和下划线（_），区分大小写

界面参数	功能说明
用户密码	HDM用户的密码。 密码的设置规则与是否在HDM Web界面上开启了密码复杂度检查有关，缺省情况下密码复杂度检查功能处于开启状态 • 开启密码复杂度检查功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查 ○ 密码长度为 8～20 个字符，仅支持字母、数字、空格和特殊字符`~!@#$%^&*()_+-=[]\{}\|;':",./<>?，区分大小写   ○ 至少包含大写字母、小写字母和数字中的两种字符   ○ 至少包含一个空格或特殊字符   ○ 不能与用户名或用户名的倒序相同 • 关闭密码复杂度检查功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查   ○ 密码长度为 2～20 个字符，仅支持字母、数字、空格和特殊字符`~!@#$%^&*()_+-=[]\{}|;':",./<>?，区分大小写 开启或关闭密码复杂度检查的详细方法请参见HDM联机帮助
用户权限	HDM用户权限，菜单选项为： • 无（缺省）：保留当前的 HDM 用户权限 • 用户：用户权限 • 操作人：操作员权限 • 管理员：管理员权限
用户状态	HDM用户启用。菜单选项为： • 启用：启用 HDM 用户 • 禁用（缺省）：禁用 HDM 用户

删除用户

删除用户界面如图 3-27 所示。具体参数说明如表 3-26 所示。

图3-27 删除用户界面

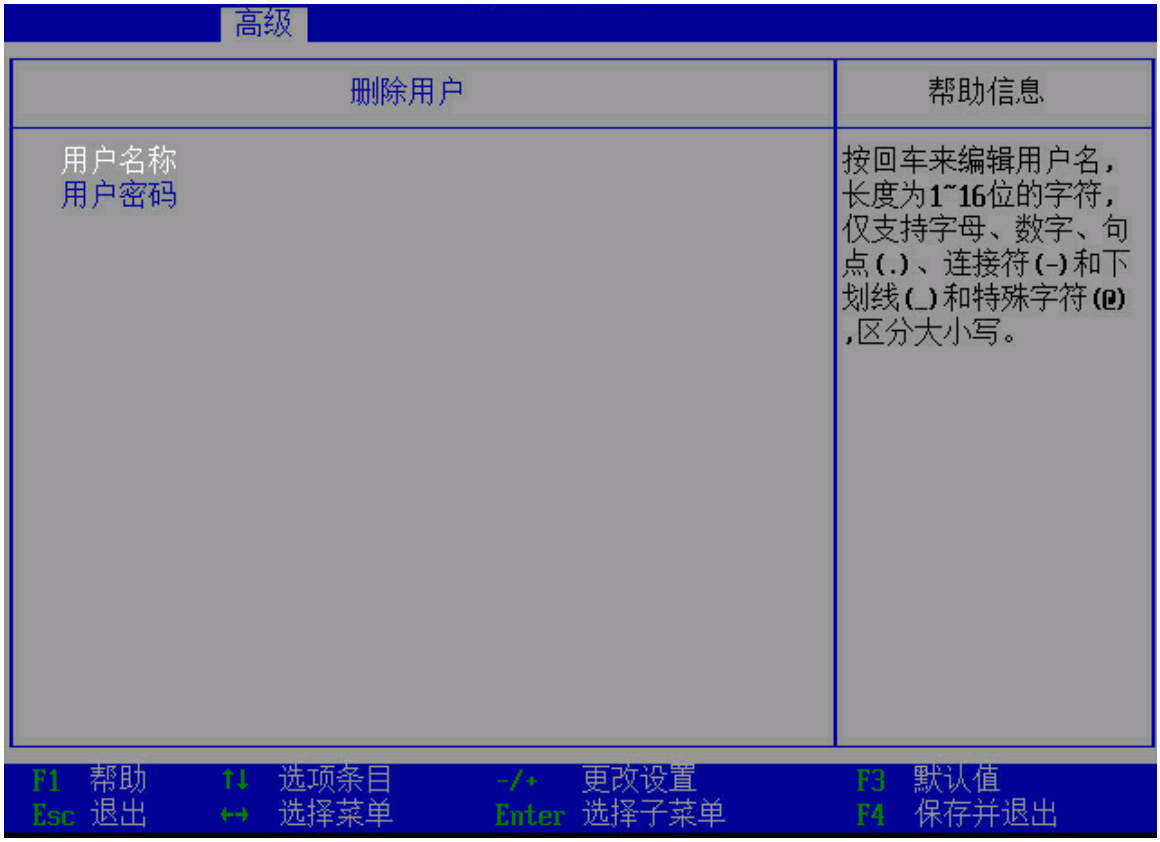


表3-26 删除用户界面参数

界面参数	功能说明
用户名称	已创建的HDM用户名
用户密码	HDM用户名对应的密码

修改用户

修改用户界面如图 3-28 所示。具体参数说明如表 3-27 所示。

图3-28 修改用户界面

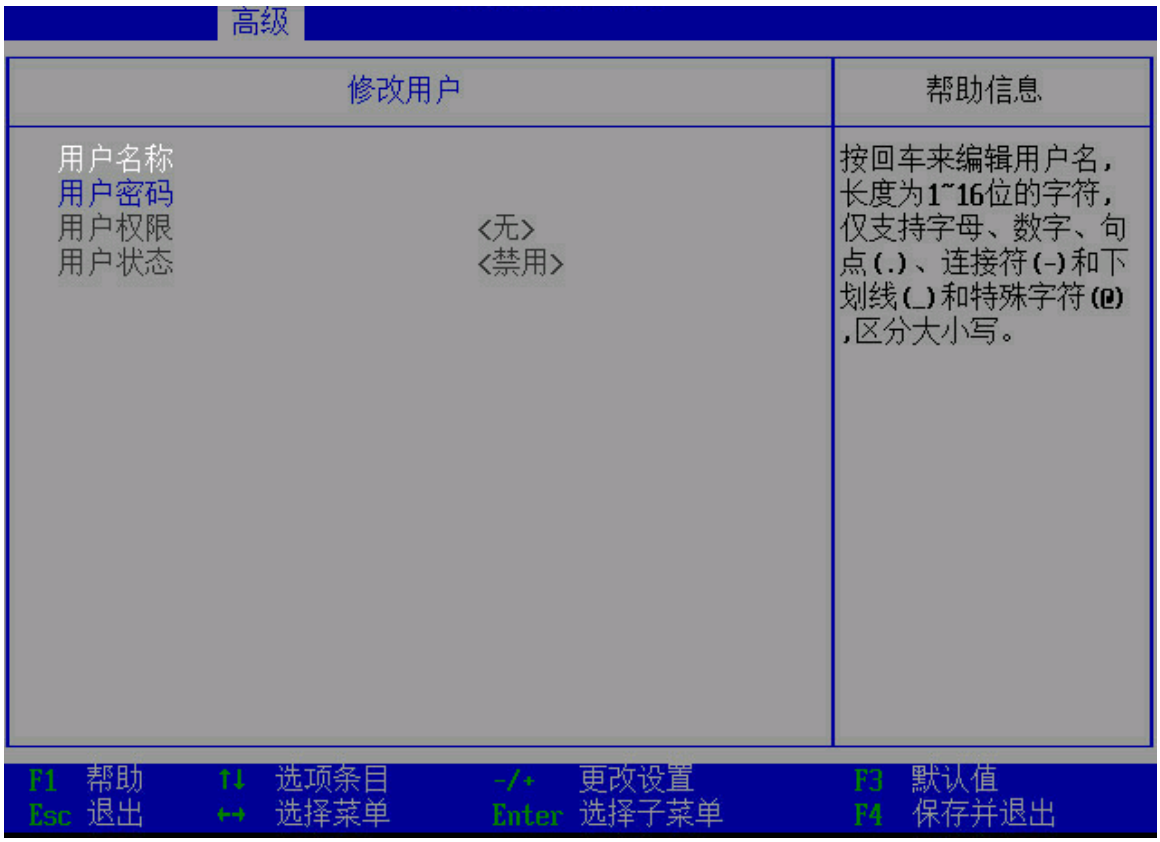


表3-27 修改用户界面参数

界面参数	功能说明
用户名称	已创建的HDM用户名
用户密码	HDM用户名对应的密码 用户登录失败的次数达到HDM设定的次数后，HDM会锁定该用户的登录。HDM默认的登录失败次数为五次，默认登录失败锁定时长为五分钟
用户权限	修改HDM用户权限，输入正确的HDM用户名和密码后，该选项可用，菜单选项为： • 无（缺省）：保留当前的 HDM 用户权限 • 用户：用户权限 • 操作人：操作员权限 • 管理员：管理员权限
用户状态	用户访问开关，输入正确的HDM用户名和密码后，该选项可用，菜单选项为： • 启用：开启用户访问功能 • 禁用（缺省）：关闭用户访问功能

3.3.5 海光设置

海光设置界面如图 3-29 所示。具体参数说明如表 3-28 所示。

图3-29 海光设置界面

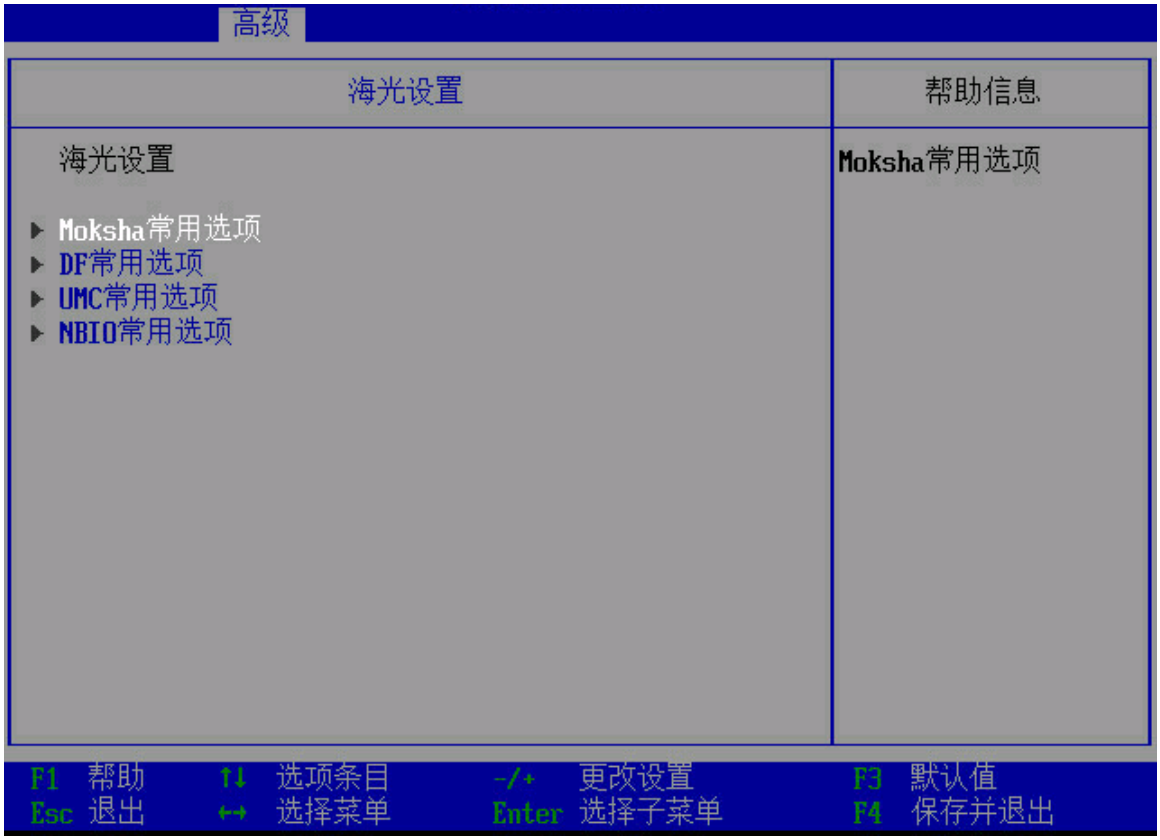


表3-28 海光设置界面参数

界面参数	功能说明
Moksha常用选项	Moksha 常用选项菜单
DF常用选项	DF（Data Fabric）常用选项菜单
UMC常用选项	UMC（Unified Memory Controllers，统一内存控制器）常用选项菜单
NBIO常用选项	NBIO（NorthBridge IO，北桥IO）常用选项菜单

1. Moksha 常用选项

Moksha 常用选项界面如图 3-30 所示。具体参数说明如表 3-29 所示。

图3-30 Moksha 常用选项界面

表3-29 Moksha 常用选项界面参数

界面参数	功能说明
L2 TLB关联性	L2 TLB（Translation Lookaside Buffer，转译后备缓冲区）关联性控制选项。菜单选项为： • 自动（缺省） • 1：L2 TLB 方式仅适用于 4K • 0：L2 TLB 方式是完全关联的
核心性能提升	核心性能加速开关。菜单选项为： • 禁用：关闭核心性能加速 • 启用（缺省）：启用核心性能加速
启用IBS	控制 IBS（Instruction Based Sampling）功能。菜单选项为： • 自动（缺省） • 启用 • 禁用

界面参数	功能说明
CPU C状态控制	控制是否启用CPU C-state省电模式。菜单选项为： • 自动：自动设置 • 启用：启用 CPU C-state 省电模式 • 禁用（缺省）：禁用 CPU C-state 省电模式
Opcache 控制	Opcache缓存控制选项。菜单选项为： • 自动（缺省） • 启用 • 禁用
SEV-ES ASID空间限制	设置SEV-ES ASID（Address Space Identifiers，地址空间标识符）空间限制，使用低于SEV-ES ASID空间限制的ASID的SEV VM必须启用SEV-ES功能，十六进制数，缺省值为0x05，取值范围为0x1（1）～0x10（16）
核心/线程启用	核心/线程启用设置菜单
流式存储控制	控制流式存储功能。菜单选项为： • 启用 • 禁用 • 自动（缺省）
RDSEED和RDRAND控制	RDSEED 和 RDRAND 控制，菜单选项为： • 启用 • 禁用 • 自动（缺省）
加载微代码控制	控制是否加载微码。菜单选项为： • 启用（缺省） • 禁用
可使用PSP CCP VQ数量	设置有效的PSP CCP VQ数量，取值范围0~4
SMEE控制	是否开启内存安全加密，菜单选项为： • 启用（缺省）：开启安全加密 • 禁用：关闭安全加密

界面参数	功能说明
SVM控制	虚拟化模式控制，菜单选项为： • 启用（缺省）：启用时，VMM（Virtual Machine Monitor，虚拟机监视器）可以利用 CPU 提供的额外硬件性能 • 禁用：关闭虚拟化模式
Prefetcher	预取设置菜单

核心/线程启用

进入“核心/线程启用设置界面”前，会出现如图 3-31 所示的警告信息界面，具体参数说明如表 3-30 所示。

图3-31 核心/线程启用警告界面

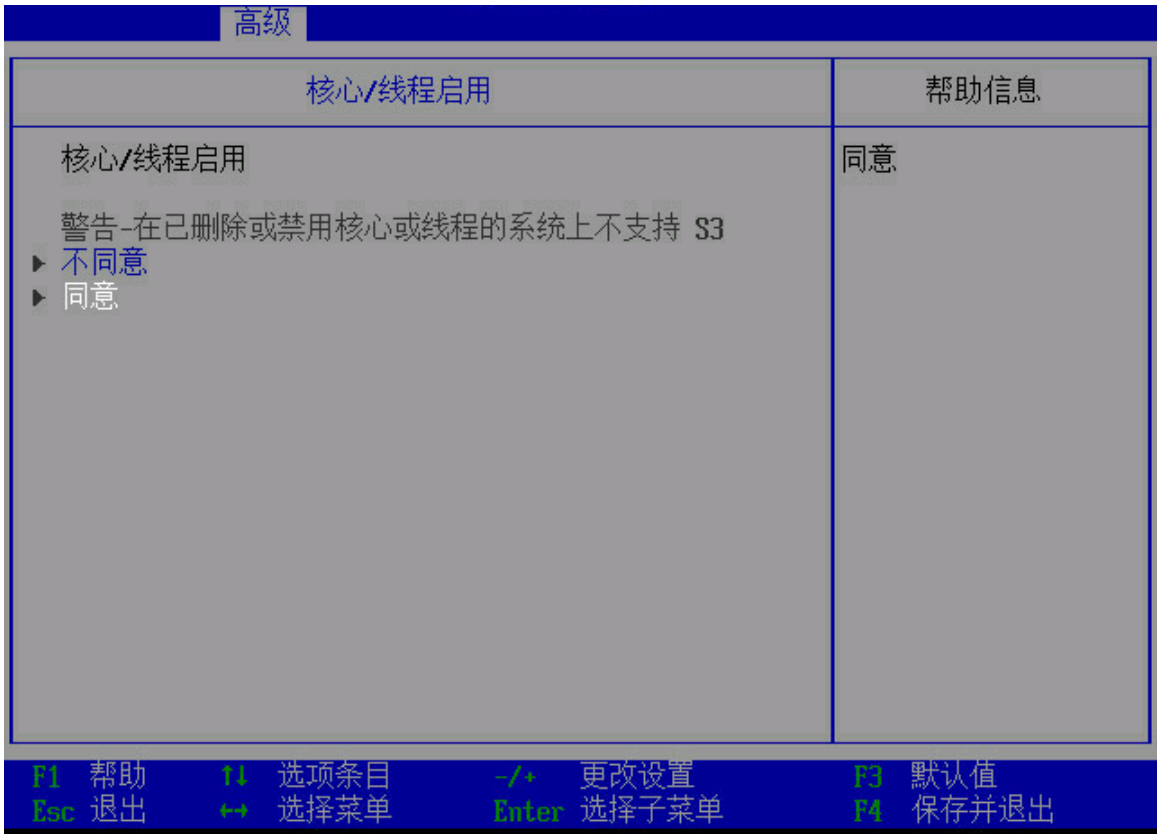


表3-30 核心/线程启用警告界面参数

界面参数	功能说明
不同意	拒绝进入核心/线程启用设置界面
同意	接受并进入核心/线程启用设置界面

接受警告信息后进入核心/线程启用设置界面，如图 3-32 所示，具体参数说明如表 3-31 所示。

图3-32 核心/线程启用设置界面

表3-31 核心/线程启用设置界面参数

界面参数	功能说明
下行控制	设置要使用的核心数，重启后生效。菜单选项为： • 2（1+1）：每个 Socket 使能一个核 • 2（2+0）：Socket 0 使能两个核 • 3（3+0）：Socket 0 使能三个核 • 4（2+2）：每个 Socket 使能两个核 • 4（4+0）：Socket 0 使能四个核 • 6（3+3）：每个 Socket 使能三个核 • 自动（缺省）

Prefetcher

Prefetcher 界面如图 3-33 所示，可开启或禁用各级缓存预取。具体参数说明如表 3-32 所示。

图3-33 Prefetcher 界面

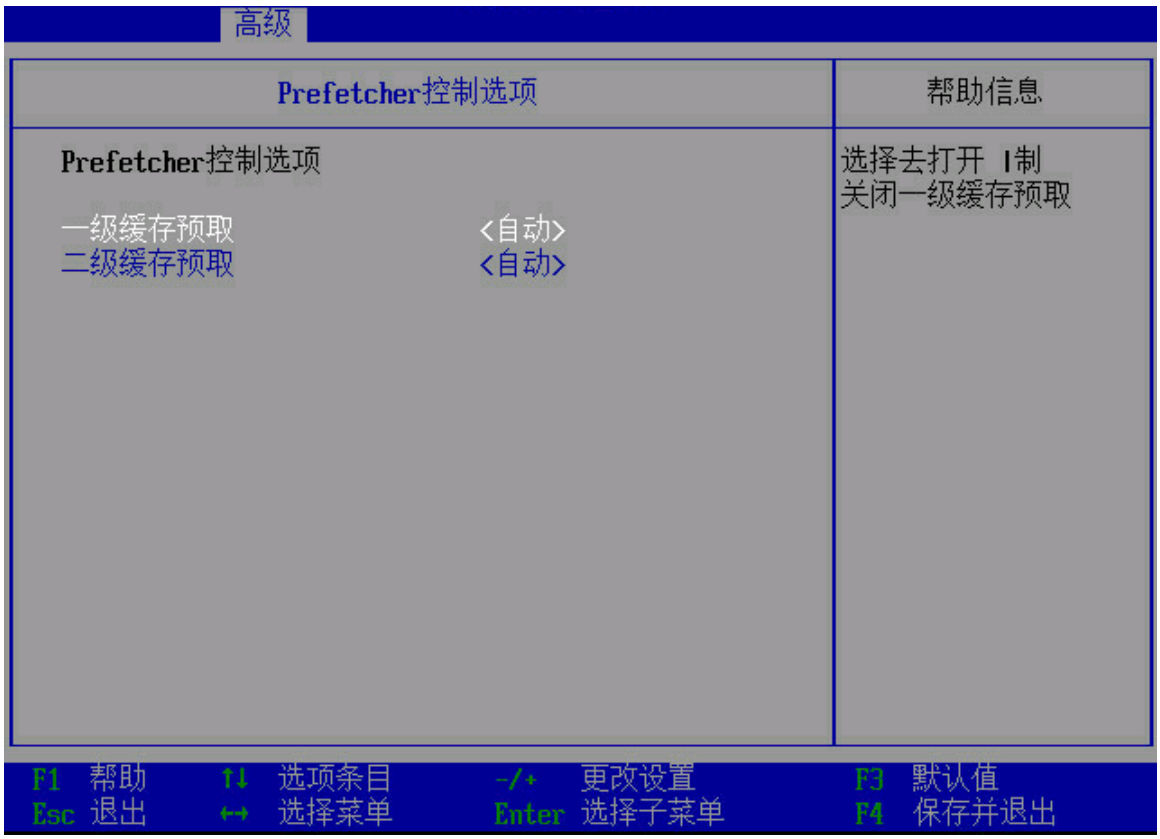


表3-32 Prefetcher Settings 界面参数

界面参数	功能说明
一级缓存预取	一级缓存硬件流预取，菜单选项为： • 自动（缺省）：自动 • 禁用：禁用一级缓存硬件流预取 • 启用：启用一级缓存硬件流预取
二级缓存预取	二级缓存硬件流预取，菜单选项为： • 自动（缺省）：自动 • 禁用：禁用二级缓存硬件流预取 • 启用：禁用二级缓存硬件流预取

2. DF 常用选项

DF 常用选项界面如图 3-34 所示。具体参数说明如表 3-33 所示。

图3-34 DF 常用选项界面

表3-33 DF 常用选项界面参数

界面参数	功能说明
DRAM擦洗时间	DRAM擦洗时间，用于设置擦洗内存的时间。菜单选项为： • 禁用 • 1 小时 • 4 小时 • 8 小时 • 16 小时 • 24 小时 • 48 小时 • 自动（缺省）

界面参数	功能说明
重定向洗涤器控件	重定向擦除控制。重定向擦除程序通过向正常操作期间访问的DRAM地址发出写回操作来清除DRAM，用于纠正cache line中的单个比特可纠正错误。菜单选项为： • 禁用：关闭重定向擦除 • 启用：：每当内存读取检测到已纠正的 ECC 错误时，便会调用重定向擦除程序 • 自动（缺省）：自动
禁用DF同步洪流传播	禁用DF同步洪流传播设置。同步洪流传播可以向所有链路传播连续的同步数据包，用于在没有其他方法时快速停止潜在的错误数据的传输。菜单选项为： • 禁用同步洪流 • 启用同步洪流 • 自动（缺省）
冻结DF模块队列出	发生错误时冻结DF模块队列设置。菜单选项为： • 禁用 • 启用 • 自动（缺省）
GMI加密控制	控制GMI（Global Memory Interconnect，全局内存互连）链接加密。菜单选项为： • 禁用 • 启用 • 自动（缺省）
xGMI加密控制	控制xGMI链接加密。菜单选项为： • 禁用 • 启用 • 自动（缺省）
CC6内存区域加密	控制CC6（Core C6状态）保存或恢复内存是否加密。菜单选项为： • 禁用 • 启用 • 自动（缺省）

界面参数	功能说明
专用内存区域的位置	控制专用内存区域（PSP、SMU、CC6）是位于内存顶部还是分散式。菜单选项为： • 分散式 • 综合 • 自动（缺省）
系统探针过滤器	控制是否启用探针过滤器，菜单选项为： • 禁用 • 启用 • 自动（缺省）
内存交错	内存交错设置。菜单选项为： • 自动（缺省）：自动 • 插槽：基于 Socket 的内存交错 • 裸片：基于 Die 的内存交错 • 通道：基于 Channel 的内存交错 • 没有：不启用内存交错 注意：选择通道、裸片和插槽对内存安装有要求，且若内存不支持所选设置则该设置将被忽略
内存交错大小	控制内存交错大小。菜单选项为： • 自动（缺省） • 256 Bytes • 512 Bytes • 1KB，仅当“信道交错哈希”选项设置为“禁用”时可设置为此参数 • 2KB，仅当“信道交错哈希”选项设置为“禁用”时可设置为此参数
信道交织哈希	控制在通道交错模式期间是否对地址位进行散列。除非将交错设置为通道且交错大小为256或512字节，否则不应启用此字段。菜单选项为： • 禁用 • 启用 • 自动（缺省）

界面参数	功能说明
清除内存	清除内存设置。菜单选项为： • 禁用：禁用此功能后，BIOS 在内存训练后不会进行内存清除（仅当使用非 ECC DIMM 时） • 启用：启用 MemClear • 自动（缺省）

3. UMC 常用选项

UMC 常用选项界面如图 3-35 所示。具体参数说明如表 3-34 所示。

图3-35 UMC 常用选项界面

表3-34 UMC 常用选项界面参数

界面参数	功能说明
DDR4通用选项	DDR4 通用选项配置菜单
DRAM内存映射	DRAM 内存映射配置菜单

DDR4 通用选项

DDR4 通用选项界面如图 3-36 所示。具体参数说明如表 3-35 所示。

图3-36 DDR4 通用选项界面

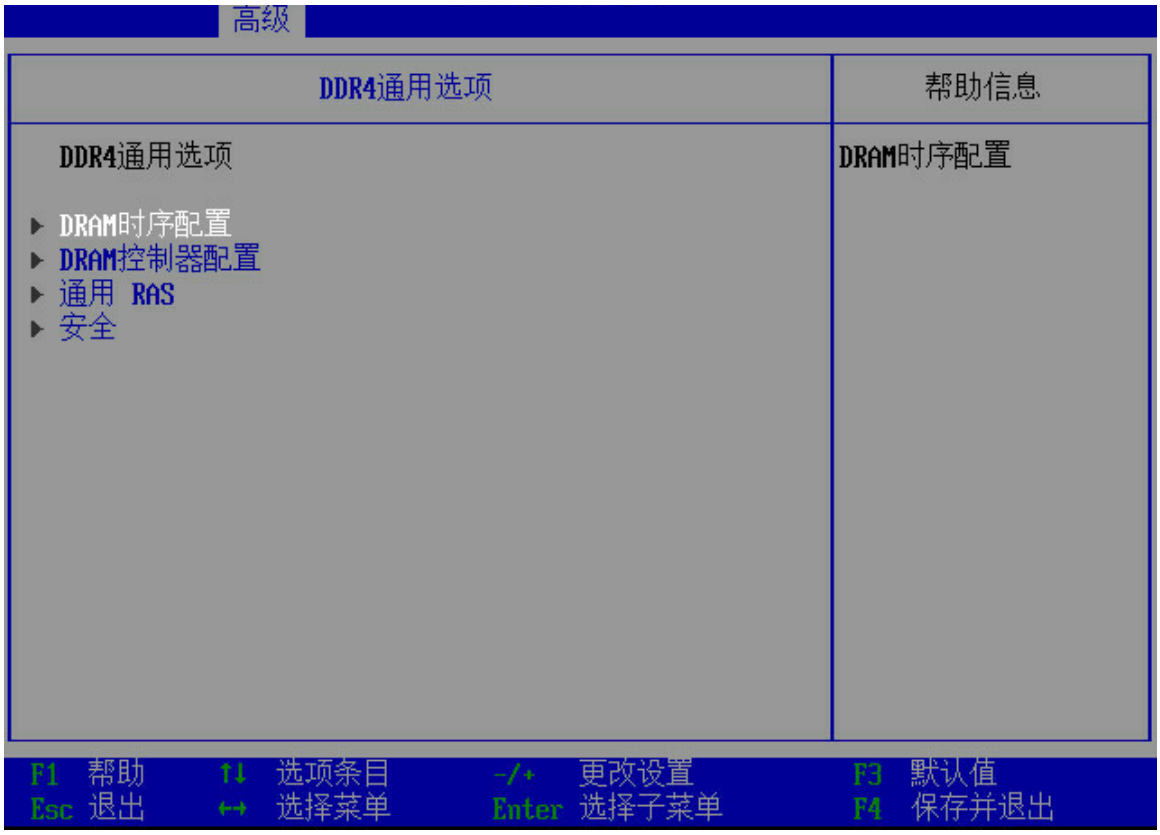


表3-35 DDR4 通用选项界面参数

界面参数	功能说明
DRAM时序配置	DRAM 时序配置菜单
DRAM控制器配置	DRAM 控制器配置菜单
通用RAS	通用RAS（Reliability、Availability、Serviceability，高可靠性、高可用性、高服务性）配置菜单
安全	安全配置菜单

进入“DRAM 时序配置界面”前，会出现如图 3-37 所示的警告信息界面，具体参数说明如表 3-36 所示。

图3-37 DRAM 时序配置警告界面

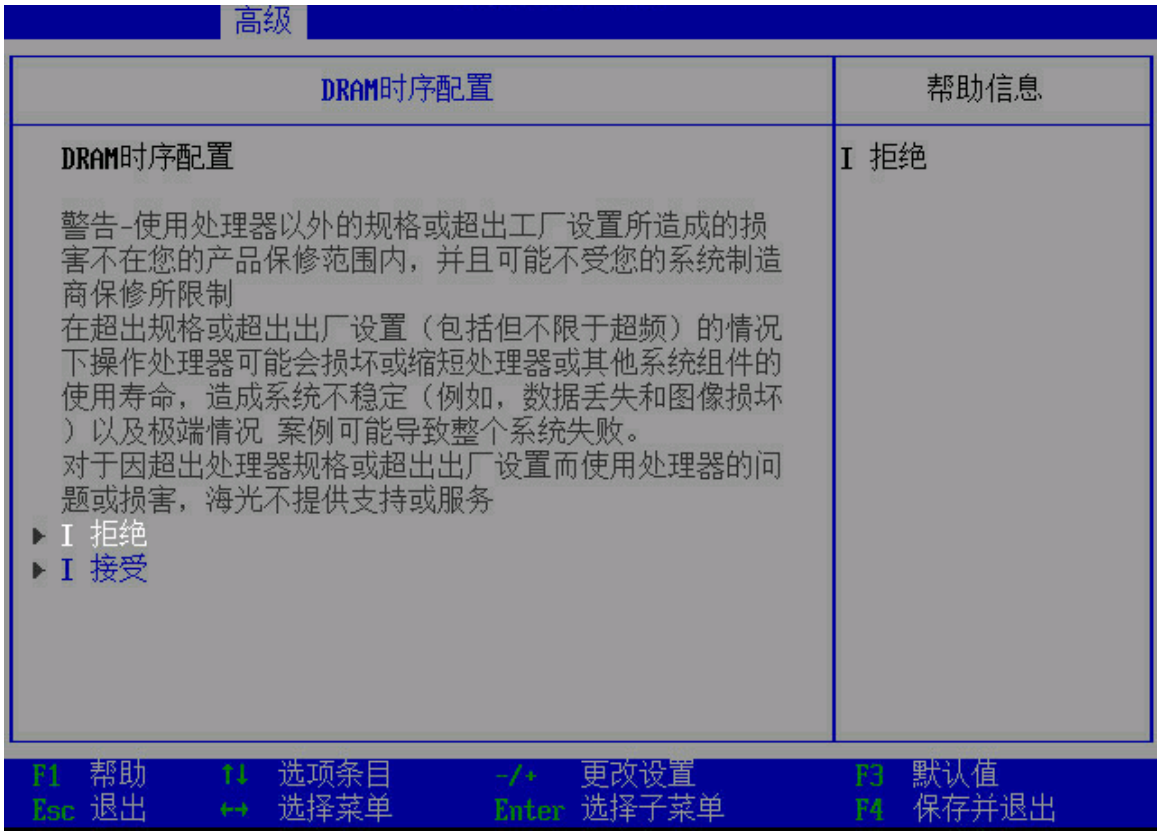


表3-36 DRAM 时序配置警告界面参数

界面参数	功能说明
拒绝	拒绝设置DRAM时序
接受	接受并进入 DRAM 时序配置界面

接受警告信息后进入 DRAM 时序配置界面，如图 3-38 所示，具体参数说明如表 3-37 所示。

图3-38 DRAM 时序配置界面

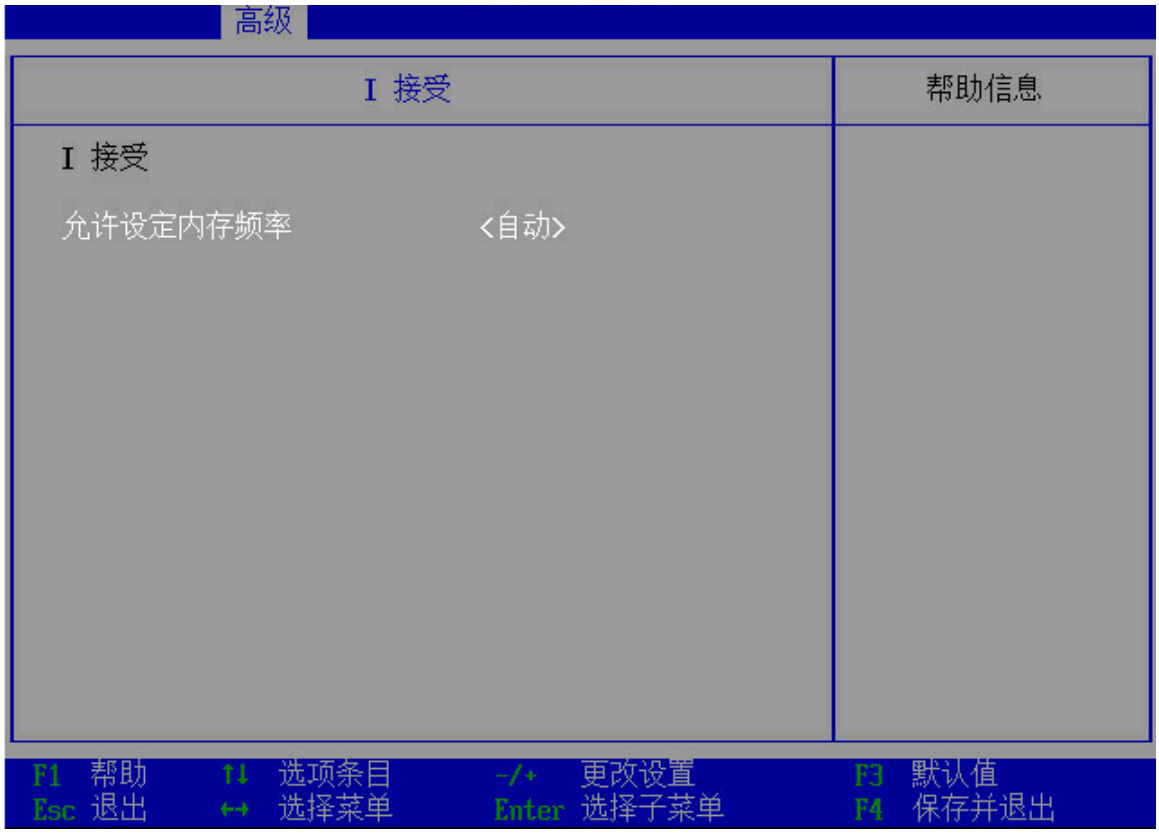


表3-37 DRAM 时序配置界面参数

界面参数	功能说明
允许设定内存频率	内存频率相关设置配置项开关。菜单选项为： • 自动（缺省） • 启用：启用后，将允许设定内存频率

DRAM 控制器配置选项界面如图 3-39 所示。具体参数说明如表 3-38 所示。

图3-39 DRAM 控制器配置界面

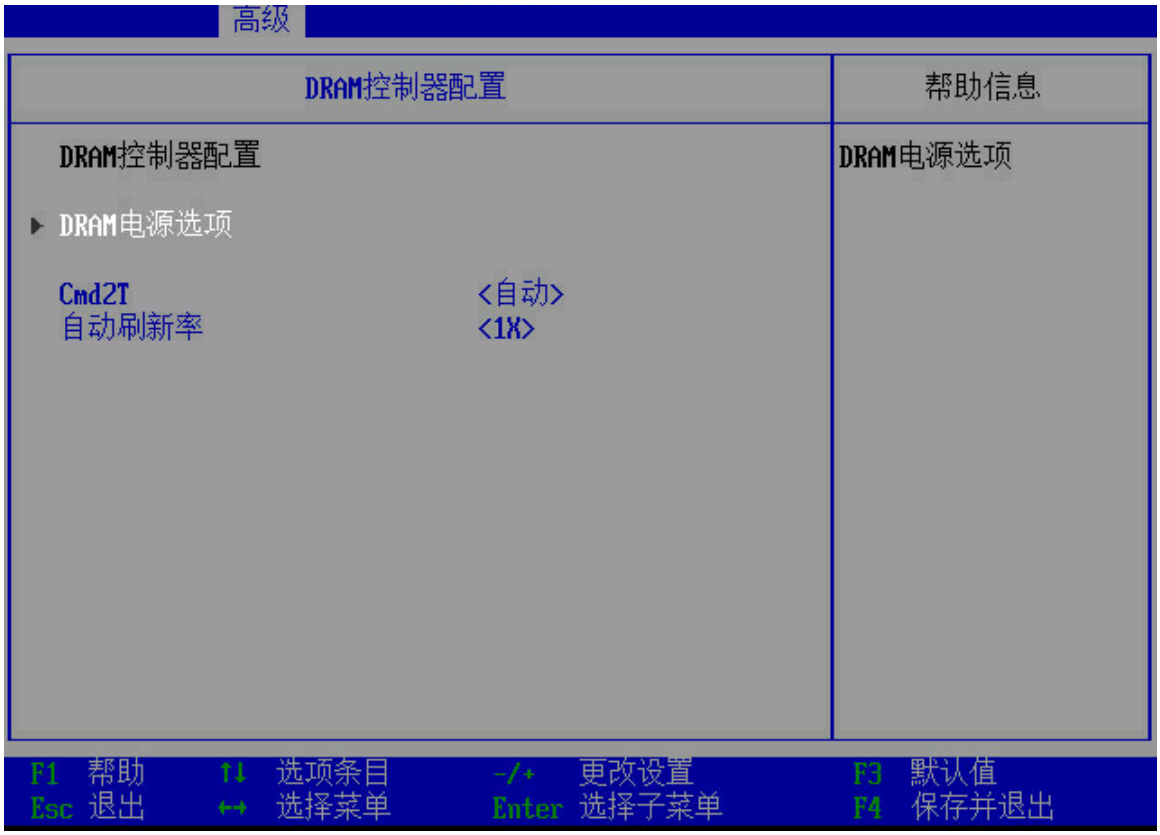


表3-38 DRAM 控制器配置界面参数

界面参数	功能说明
DRAM电源选项	DRAM 电源选项菜单
Cmd2T	针对ADDR/CMD选择1T和2T模式。菜单选项为： • 1T • 2T • 自动（缺省）
自动刷新率	内存自刷新率设置。菜单选项为： • 1X（缺省）：内存正常刷新 • 2X • 4X

DRAM 电源选项界面如图 3-40 所示。具体参数说明如表 3-39 所示。

图3-40 DRAM 电源选项界面

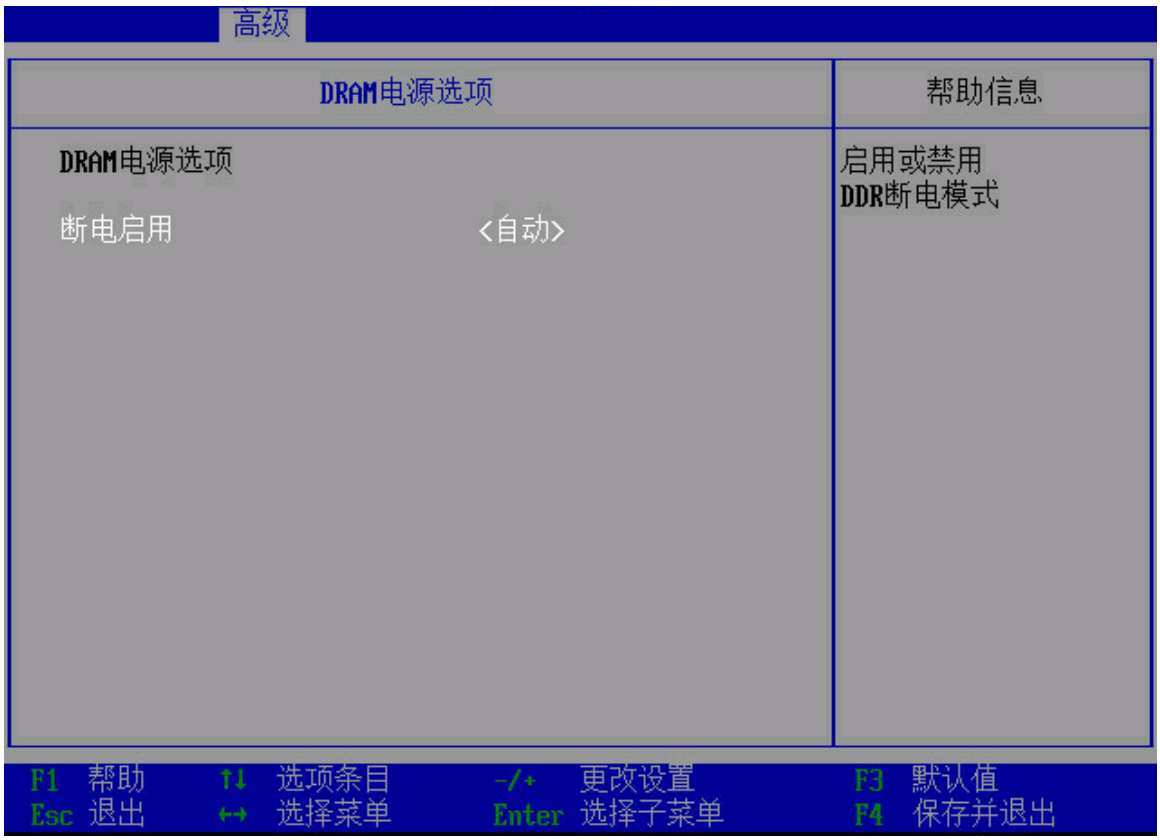


表3-39 DRAM 电源选项界面参数

界面参数	功能说明
断电启用	控制DDR下电模式。通过将一段时间不活动的DRAM置于静止状态，可以适度地节省系统功耗，但会增加DRAM延迟。菜单选项为： • 启用：启用 DDR 下电模式 • 禁用：禁用 DDR 下电模式 • 自动（缺省）

通用 RAS 配置界面如图 3-44 所示。具体参数说明如表 3-40 所示。

图3-41 通用 RAS 配置界面

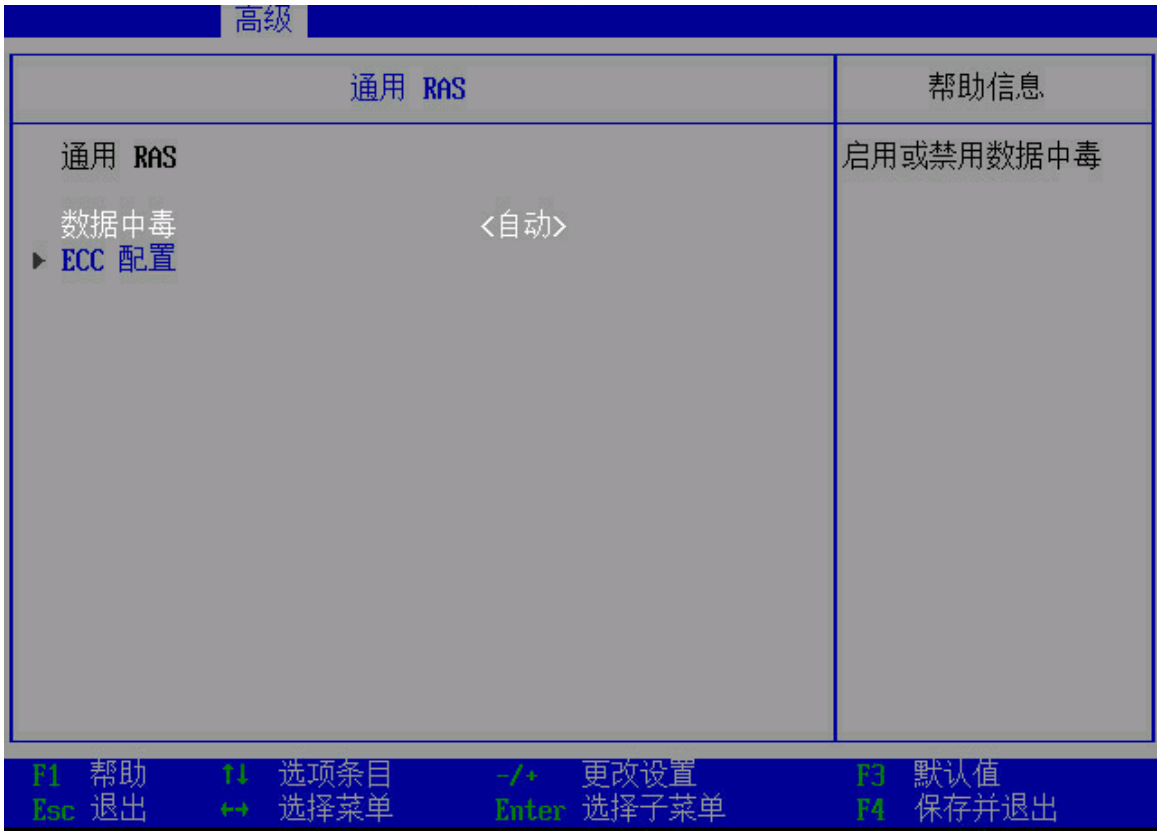


表3-40 通用 RAS 配置界面参数

界面参数	功能说明
数据中毒	数据中毒设置。菜单选项为： • 自动（缺省） • 启用 • 禁用
ECC配置	ECC配置菜单

ECC 配置界面如图 3-42 所示。具体参数说明如表 3-41 所示。

图3-42 ECC 配置界面

表3-41 ECC 配置界面参数

界面参数	功能说明
DRAM ECC符号大小	内存 ECC 大小，菜单选项为 • X4 • X8 • 自动（缺省）
DRAM ECC启用	内存 ECC 设置，菜单选项为： • 自动（缺省）：设置为自动，将开启 ECC • 启用 • 禁用

安全配置界面如图 3-43 所示。具体参数说明如表 3-42 所示。

图3-43 安全配置界面

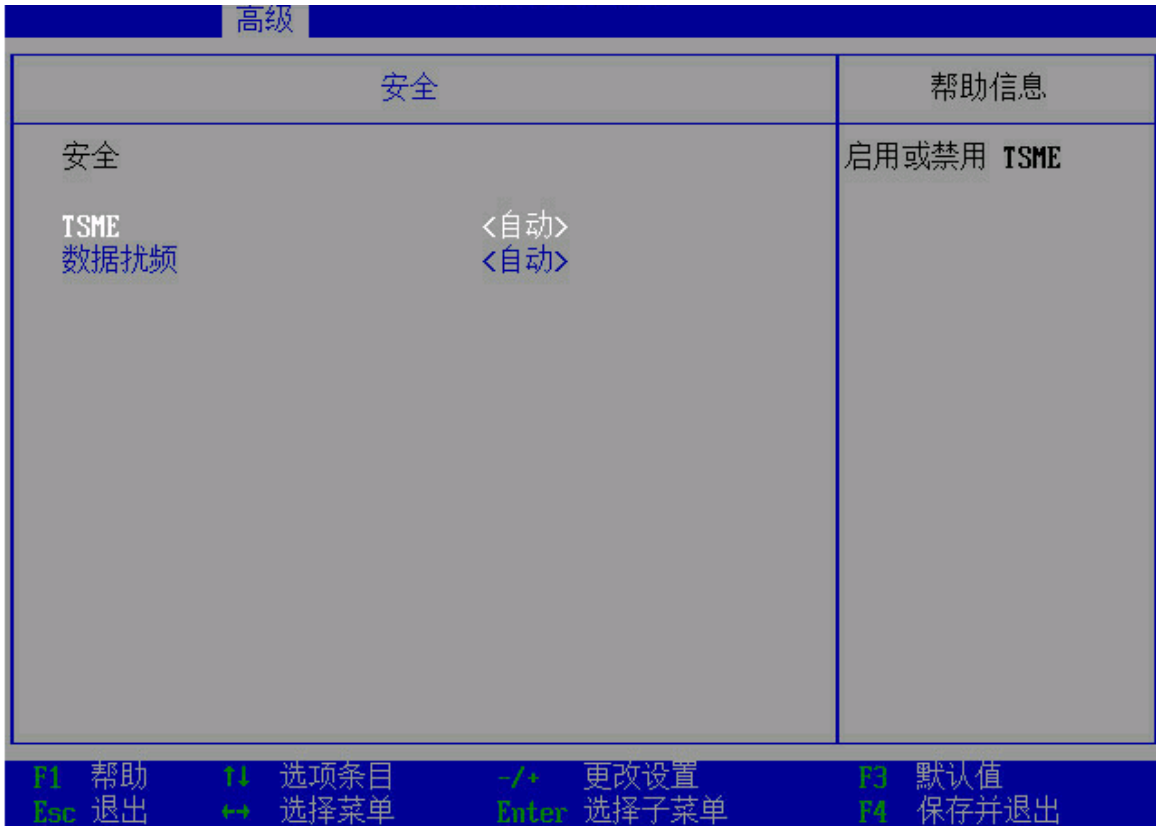


表3-42 安全配置界面参数

界面参数	功能说明
TSME	透明 SME 设置，菜单选项为： • 自动（缺省） • 启用 • 禁用
数据扰频	数据扰频设置，用于在数据传输时防止数据泄露，保证数据的安全性。菜单选项为： • 自动（缺省） • 启用 • 禁用

DRAM 内存映射

DRAM 内存映射界面如图 3-44 所示。具体参数说明如表 3-43 所示。

图3-44 DRAM 内存映射界面

表3-43 DRAM 内存映射界面界面参数

界面参数	功能说明
芯片选择交错	片选交错，在node0选择的DRAM芯片组之间交叉存取内存区块。菜单选项为： • 自动（缺省）：自动 • 禁用：禁用片选交错功能
集团互换	设置内存Bank群组交换。菜单选项为： • 自动（缺省）：自动设置 • 启用：启用内存 Bank 群组交换 • 禁用：禁用内存 Bank 群组交换
集团互换Alt	内存Bank群组交换更改。菜单选项为： • 自动（缺省）：自动设置 • 启用：启用内存 Bank 群组交换更改 • 禁用：禁用内存 Bank 群组交换更改

界面参数	功能说明
地址哈希Bank	Bank地址哈希校验。菜单选项为： • 自动（缺省）：自动设置 • 启用：启用 Bank 地址哈希校验 • 禁用：禁用 Bank 地址哈希校验
地址哈希CS	CS地址哈希校验。菜单选项为： • 自动（缺省）：自动设置 • 启用：启用 CS 地址哈希校验 • 禁用：禁用 CS 地址哈希校验

4. NBIO 常用选项

NBIO 常用选项界面如图 3-45 所示。具体参数说明如表 3-44 所示。

图3-45 NBIO 常用选项界面

表3-44 NBIO 常用选项界面参数

界面参数	功能说明
NB配置	NB 配置菜单

界面参数	功能说明
NBIO内部错误消耗	NBIO 内部错误消耗，菜单选项为： • 禁用 • 启用 • 自动（缺省）
NBIO RAS控制	NBIO RAS 控制。菜单选项为： • 禁用 • 启用 • 自动（缺省）
系统决策	系统决策，菜单选项为： • 自动（缺省）：使用默认的性能确定性设置 • 节能：节能优先 • 性能：性能优先
cTDP控制	当前的TDP（Thermal Design Power，热设计功率）控制，菜单选项为： • 自动（缺省）：使用熔断 TDP 的值 • 手动：用户可自定义 TDP 的值
cTDP	用于自定义TDP的值。当“cTDP控制”选项设置为手动时，显示该选项。单位为W。
效能优化模式	效能优化模式设置。菜单选项为： • 禁用 • 启用 • 自动（缺省）
PSI	PSI（Power Status Indicator，电源状态指示灯）设置。菜单选项为： • 自动（缺省） • 禁用
PCIe ACS支持	ACS（Access Control Services，存取控制服务）启用。该选项启用之前必须启用AER（Advanced Error Reporting，高级错误报告）才能实现功能。菜单选项为： • 禁用 • 启用 • 自动（缺省）

界面参数	功能说明
PCIe ARI支持	备用路径 ID 解释支持设置。菜单选项为： • 禁用 • 启用 • 自动（缺省）
CLD0 VDDP控制	CLD0_VDDP 控制。菜单选项为： • 手动：用户可以设置自定义 CLD0_VDDP 电压 • 自动（缺省）
阻断PCIe回环	阻断 PCIe 热插拔槽位回环模式。菜单选项为： • 禁用 • 启用 • 自动（缺省）
CRS 延时	热插拔操作 CRS 延时设置，缺省为 6us
CRS 限制	热插拔操作 CRS 限制设置，缺省为 6us
PCIE热插拔支持	热插拔控制支持功能控制，菜单选项为： • 禁用 • 启用 • 自动（缺省）

NB 界面如图 3-46 所示。具体参数说明如表 3-45 所示。

图3-46 NB 配置界面

表3-45 NB 配置参数

界面参数	功能说明
IOMMU	IO内存管理单元设置，菜单选项为： • 自动（缺省）：使用默认 • 启用：启用 IOMMU • 禁用：禁用 IOMMU
同步训练	同步训练设置选项，菜单选项为： • 自动（缺省）：使用默认 • 启用 • 禁用

3.3.6 UEFI HII 配置

UEFI HII 配置界面如图 3-47 所示，显示接入服务器的设备配置菜单。具体选项与接入的设备有关。

图3-47 UEFI HII 配置界面

3.4 安全界面

安全界面如图 3-48 所示。具体参数说明如表 3-46 所示。

图3-48 安全界面

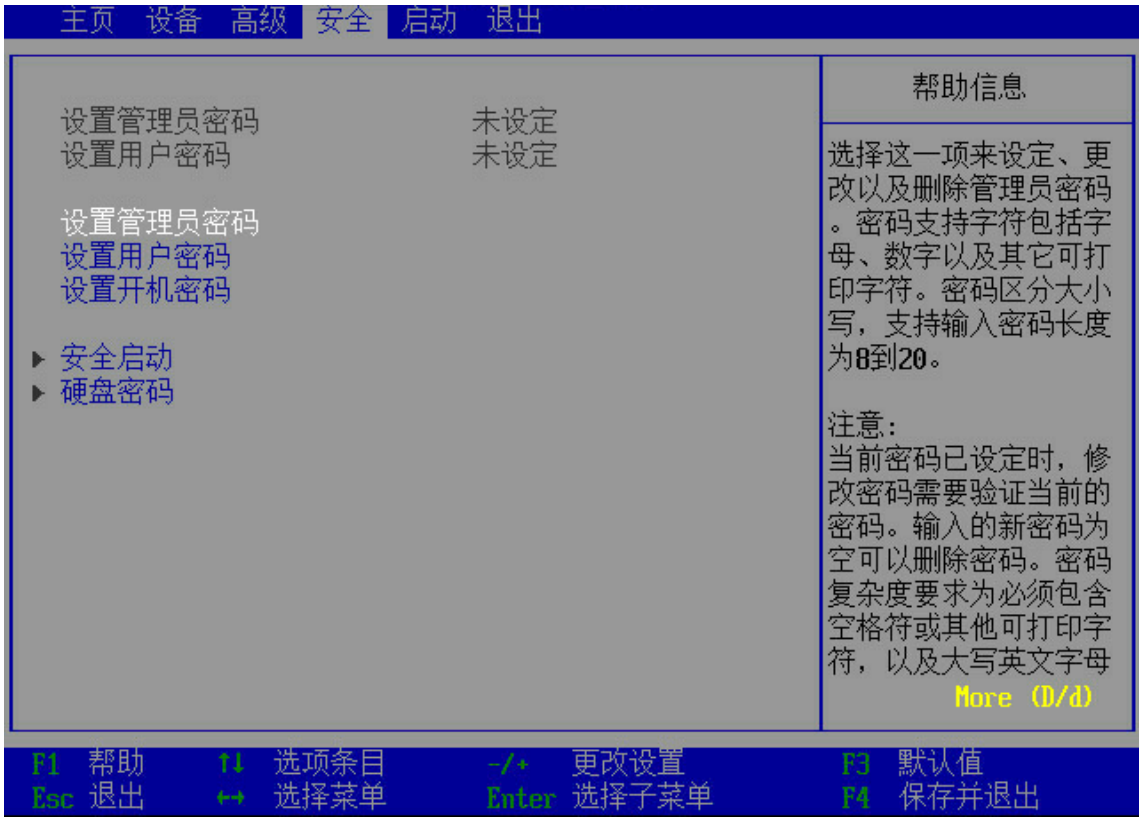


表3-46 安全界面参数

界面参数	功能说明
设置管理员密码	设置管理员密码，密码设置规则请查看2.7.2 密码设置注意事项
设置用户密码	设置用户密码，密码设置规则请查看2.7.2 密码设置注意事项
设置开机密码	设置开机密码，密码设置规则请查看2.7.2 密码设置注意事项
安全启动	安全启动配置菜单
硬盘密码	硬盘密码配置菜单

3.4.1 安全启动

安全启动界面如图 3-49 所示。具体参数说明如表 3-47 所示。

图3-49 安全启动界面

表3-47 安全启动界面参数

界面参数	功能说明
安全启动状态	显示安全启动的模式，包括工厂模式、用户模式
安全启动	显示安全启动设置的状态
恢复出厂设置	将安全启动设置恢复为出厂设置

3.4.2 硬盘密码

硬盘密码界面如图 3-50 所示，选择硬盘后进入对应硬盘的密码设置界面，如图 3-51 所示。具体参数说明如表 3-48 所示。

图3-50 硬盘密码界面


安全
硬盘密码
帮助信息
选择驱动器
SATA2-7: SAMSUNG MZ7LM960HMJP-00005
F1 帮助
↑↓ 选项条目
-/+ 更改设置
F3 默认值
Esc 退出
↔ 选择菜单
Enter 选择子菜单
F4 保存并退出

图3-51 硬盘密码配置界面

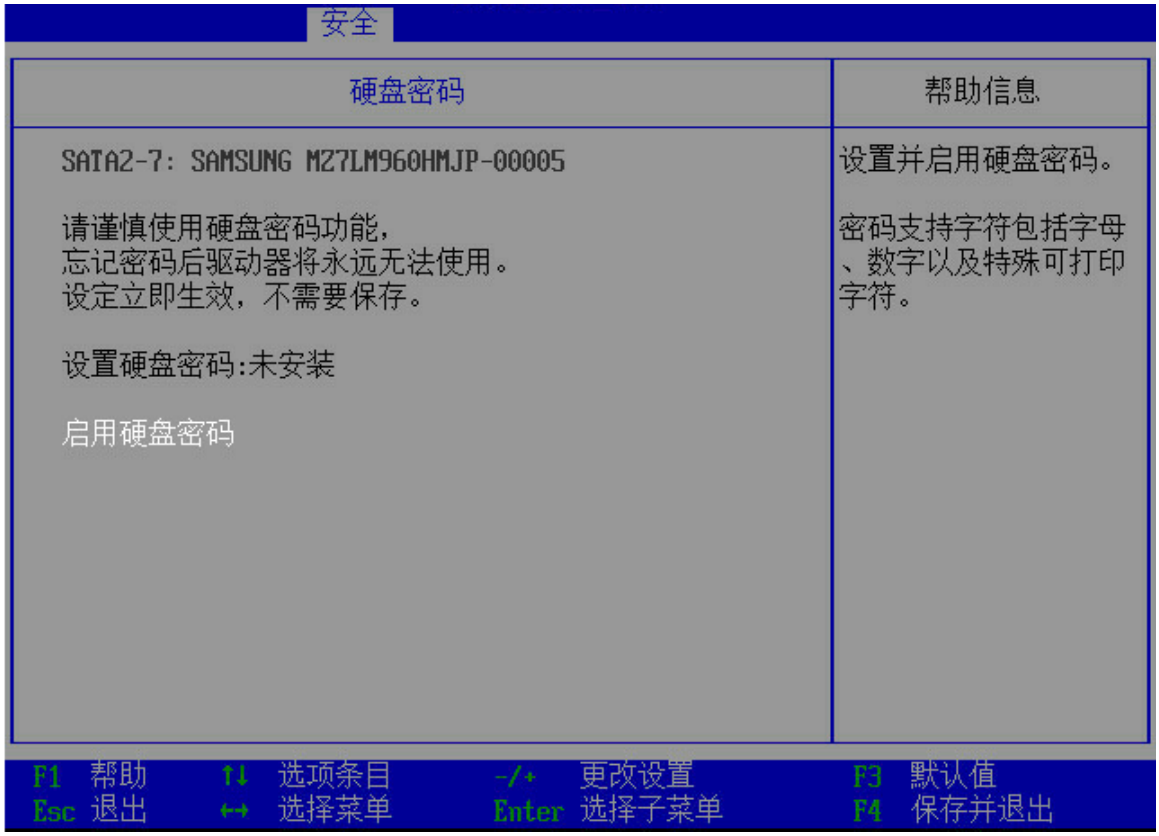


表3-48 安全启动界面参数

界面参数	功能说明
启用硬盘密码	设置并启用硬盘密码。有效密码长度为1～32，输入空密码可以删除已设置的密码。新密码在保存重启后生效

3.5 启动界面

启动界面如图 3-52 所示，主要包含设置服务器的启动顺序、BIOS 的启动模式等。具体参数说明如表 3-49 所示。

图3-52 启动界面

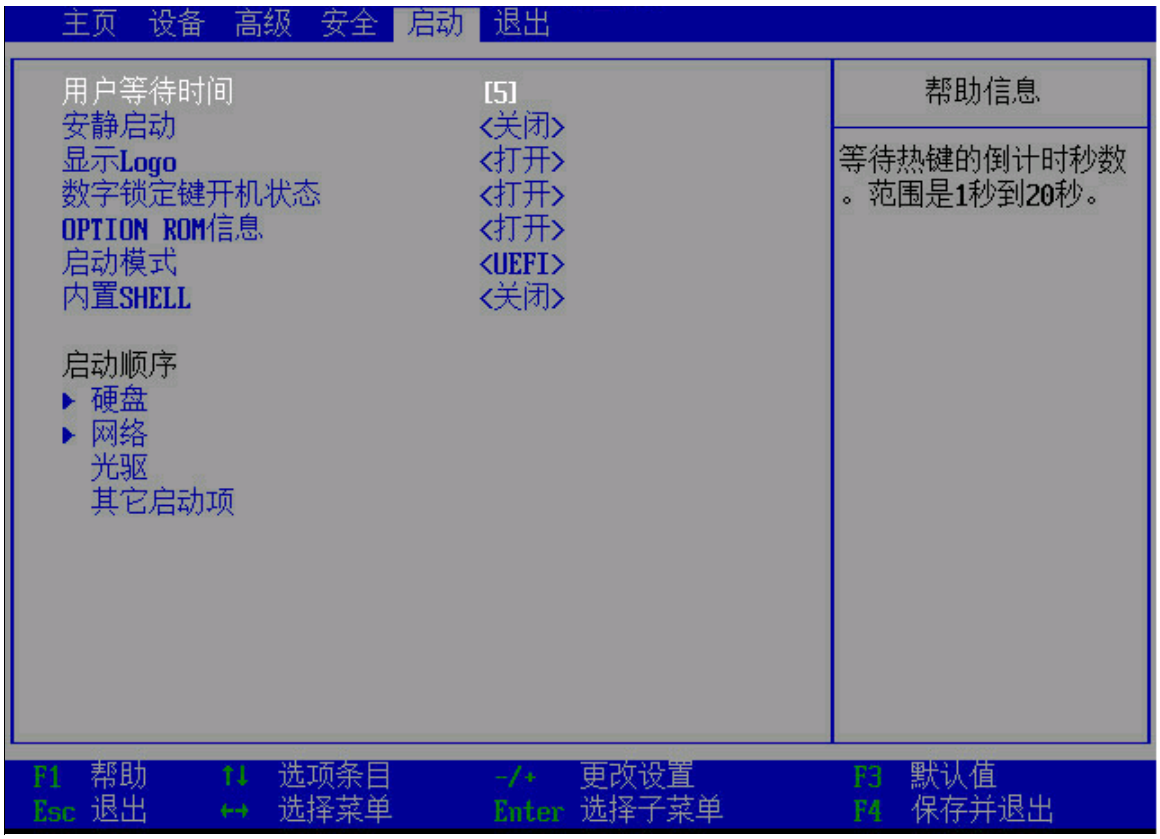


表3-49 启动界面参数

界面参数	功能说明
用户等待时间	设置启动过程中等待热键的倒计时描述。范围是 1～20 秒。缺省值为 5 秒
安静启动	设置安静启动，用于设置系统启动过程中的显示状态。菜单选项为： • 打开：显示厂商标志 • 关闭（缺省）：隐藏厂商标志
显示Logo	显示或隐藏启动 Logo，菜单选项为： • 打开（缺省）：显示启动 Logo • 关闭：隐藏启动 Logo
数字锁定键开机状态	启动后键盘上数字锁定键状态设置，菜单选项为： • 打开（缺省）：打开启动后键盘上数字锁定键状态 • 关闭：关闭启动后键盘上数字锁定键状态

界面参数	功能说明
OPTION ROM信息	Option ROM 信息显示设置。菜单选项为： • 打开（缺省） • 关闭
启动模式	启动模式选择设置，菜单选项为： • UEFI（缺省）：UEFI 启动模式 • LEGACY：Legacy 启动模式
内置SHELL	Shell启动开关，Shell是EFI内置的命令行，该选项在Boot Mode Select选项设置为“仅Legacy”时不显示。菜单选项为： • 关闭（缺省）：禁用 Shell • 打开：启用后，将显示 Shell 启动项
启动顺序	
硬盘	硬盘、USB启动优先级配置，从可用的硬盘驱动和USB中指定启动设备的优先级顺序
网络	网络PXE启动优先级配置，从可用的网络中指定启动的优先级顺序
光驱	系统内置光驱启动优先级配置菜单，从可用的系统内置光驱中指定启动设备的优先级顺序
其它启动项	其他启动项优先级配置菜单，如UEFI Shell

3.6 退出界面

退出界面如图 3-53 所示，主要包含控制 BIOS 参数修改及退出功能。具体参数说明如表 3-50 所示。

图3-53 退出界面

表3-50 退出界面参数

界面参数	功能说明
保存更改	保存修改
保存退出	保存修改并退出
放弃修改	放弃修改
不保存并且退出	不保存修改并且退出
恢复初始值	恢复缺省设置
BIOS固件更新	选择文件更新BIOS
关机	关闭服务器
重启	重启服务器
Boot Override	选择从以下启动项启动，您也可以通过在BIOS启动界面（图2-1）按**F7**进入Boot Menu界面，选择对应的启动项

4 缩略语

表4-1 缩略语

缩略语	英文解释	中文解释
A		
ACPI	Advanced Configuration and Power Interface	高级配置和电源接口
ABL	AGESA boot loader	-
ACPI	Advanced Configuration and Power Interface	高级配置和电源接口
APCB	AMD PSP Control Block	-
ARI	Alternative Routing-ID	备用路由ID
B		
BIOS	Basic Input Output System	基本输入输出系统
C		
CE	Corrected Error	可纠正错误
CPU	Central Processing Unit	中央处理器
D		
DF	Data Fabric	用于CPU，I/O和DRAM之间的通信
DRAM	Dynamic Random Access Memory	动态随机存取存储器
E		
ECC	Error Checking and Correcting	错误检查和纠正
EFI	Extensible Firmware Interface	可扩展固件接口
G		
GMI	Global Memory Interconnect	全局内存互连
I		
IBS	Instruction Based Sampling	-
IP	Internet Protocol	网络协议

缩略语	英文解释	中文解释
IPMI	Intelligent Platform Management Interface	智能平台管理接口
H		
HDM	Hardware Device Management	硬件设备管理
HII	Human Interface Infrastructure	人机界面基础架构
M		
MAC	Media Access Control	介质访问控制
MBIST	Memory built-in self-test	内存内建自检测
N		
NBIO	NorthBridge IO	北桥IO
NTB	Non-Transparent Bridging	非透明桥接
NUMA	Non Uniform Memory Access	非统一内存访问
NVMe	Non-Volatile Memory Express	非易失性内存标准
O		
OS	Operating System	操作系统
P		
PCI	Peripheral Component Interface	外围组件接口
PCIe	Peripheral Component Interconnect Express	外围组件快速互连
PN	Production Number	生产编号
POST	Power On Self Test	开机自检
PSP	Platform Security Processor	平台安全处理器
PXE	Preboot Execute Environment	预启动执行环境
R		
RAID	Redundant Arrays of Independent Disks	独立磁盘冗余阵列
RAS	Reliability，Availability，Serviceability	可靠性、可用性和可服务性
ROM	Read-Only Memory	只读存储器
S		

缩略语	英文解释	中文解释
SAS	Serial Attached SCSI	串行连接的SCSI
SATA	Serial Advanced Technology Attachment	串行ATA
SCSI	Small Computer System Interface	小型计算机系统接口
SEL	System Event Log	系统事件日志
SEV	Secure Encrypted Virtualization	安全加密虚拟化
SMU	System Management Unit	系统管理单元
SN	Serial Number	产品序列号
SOL	Serial Over Lan	串口重定向
SR-IOV	Single-Root I/O Virtualization	单路I/O虚拟化
SVM	Secure virtual machine	安全虚拟机
T		
TDP	Thermal Design Power	热设计功耗
TLB	Translation Lookaside Buffer	转译后备缓冲区
U		
UEFI	Unified Extensible Firmware Interface	统一的可扩展固件接口
UMC	Unified Memory Controllers	统一内存控制器
USB	Universal Serial Bus	通用串行总线
UUID	Universally Unique Identifier	通用唯一识别码
V		
VGA	Video Graphics Array	视频图形阵列
X		
XHCI	eXtensible Host Controller Interface	可扩展的主机控制器接口