Lenovo

搭载 Intel Xeon 6 处理器的 ThinkSystem 服务器 UEFI 手册

服务器型号：SR630 V4、SR650 V4、SR650a V4

第一版 (**2025 年 4 月**)

目录

第 1 章　UEFI 简介

Unified Extensible Firmware Interface（UEFI）定义了用于引导系统硬件以及与操作系统交互的平台固件的架构。UEFI 界面包含多种功能，包括但不限于：

- **系统信息和设置**
- **引导和运行时服务**
- **BMC 设置**
- **系统事件日志**
- **用户安全性**

本指南适用于以下服务器型号：

- **SR630 V4**
- **SR650 V4**
- **SR650a V4**

第 2 章　开始使用

本章介绍如何开始使用 **UEFI Setup Utility**。

首次启动

执行以下步骤以首次启动 **UEFI Setup Utility**。

1. （可选）使用线缆将本地键盘、视频和鼠标（**KVM**）连接到服务器，或在 **Lenovo XClarity Controller Web** 用户界面（**XCC Web UI**）上打开**远程控制台**页面。
2. 打开系统电源，然后按 **F1**。
3. 如果设置了开机密码，请输入正确的密码。

   等待大约 **90** 秒。随后即会显示 **Setup Utility** 窗口。

在图形模式/文本模式之间切换

Setup Utility 可以在图形模式（默认）或文本模式下启动。您可以参考以下部分在两种模式之间切换。

- **图形模式到文本模式**

执行以下步骤可从图形模式切换到文本模式：

1. 在主界面上，选择 **UEFI 设置 > 系统设置 > <F1> 启动控制**。
2. 对于 **<F1> 启动控制**，选择**文本设置程序**。
3. 保存设置。
4. 重新启动服务器，然后按 **F1**。

   等待大约 **90** 秒。随后会以文本模式显示 **Setup Utility** 窗口。

- **文本模式到图形模式**

执行以下步骤可从文本模式切换到图形模式：

1. 在主界面上，选择**系统设置 > <F1> 启动控制**。
2. 对于 **<F1> 启动控制**，选择**工具套件**或**自动**。
3. 保存设置。
4. 重新启动服务器，然后按 **F1**。

   等待大约 **90** 秒。随后会以图形模式显示 **Setup Utility**。

键盘导航提示：

以下是在文本模式下使用键盘导航浏览“**UEFI** 设置”项时的可能用到的按键：

- **Enter**：选择一个项。
- **+**：增加值。
- **–**：减小值。
- **Esc**：返回上一个界面。
- **F1**：显示帮助信息。

第 3 章　UEFI Setup Utility 概述

本主题介绍 **UEFI Setup Utility** 的一般信息。

注：

- **服务器平台差异：UEFI** 系统配置选项因服务器平台而异。本文档中描述的部分菜单或选项可能与您的特定服务器平台上的菜单或选项略有不同。
- **默认设置：**默认设置现已经过优化。对于任何您不熟悉的项，请使用默认值。请勿更改不熟悉项的值，以免出现意外问题。如果您考虑更改服务器配置，请务必谨慎操作。配置设置不正确可能会导致意外结果。
- **引导系统以使设置生效：**对于需要重新引导系统才能生效的设置，请使用以下方法之一：
  - 更改设置后，在主菜单上单击**保存设置 → 退出 Setup Utility**。
  - 更改设置后，按 **Esc** 并在主菜单上选择 **<Y> 保存并退出 Setup Utility**。

    如果是嵌套的子菜单，请反复按 **Esc** 以返回到主菜单。

下表详细介绍了 **UEFI Setup Utility** 的主菜单：

表 1. 系统配置和引导管理

项	描述
第 7 页第 4 章 “系统配置和引导管理”	主菜单
选择语言	选择显示语言。
启动图形 System Setup	启动系统设置的图形化用户界面。可以在 **UEFI 设置**页面上查看或更改 **UEFI** 设置。 **注：**在图形 **System Setup** 中导航时，系统不会通过基于文本的控制端口重定向输出屏幕。请使用 **VGA** 显示器或 **XCC** 远程控制台 **Web** 查看器来查看图形 **System Setup** 屏幕输出。
第 7 页 “系统信息”	查看系统的基本详细信息。
第 8 页 “系统设置”	查看或修改系统设置。 更改可能不会立即生效。对于需要重新引导系统才能生效的设置，请保存更改并重新引导系统。
第 53 页 “日期和时间”	设置系统的本地日期和时间。
第 54 页 “启动选项”	从“引导管理器”菜单中的首选引导顺序选择所需的引导选项。
第 54 页 “引导管理器”	更改引导顺序、引导参数和从文件引导。
第 58 页 “BMC 设置”	配置基板管理控制器（BMC）。
第 61 页 “系统事件日志”	清除或查看系统事件日志。
第 61 页 “用户安全性”	设置或更改开机密码和管理员密码。

表 1. 系统配置和引导管理 （续）

项	描述
第 63 页 “默认选项”	配置出厂默认值和自定义默认值的选项。 • [出厂默认设置]：原始制造商的设置。 • [自定义默认设置]：用户保存的设置。
第 63 页 “查看未保存的设置”	查看所有已更改但未保存的设置。
保存设置	保存更改的设置并将其提交到 BMC。
放弃设置	放弃更改。
加载默认设置	加载系统设置的默认值。
退出 Setup Utility	退出 UEFI Setup Utility。

第 4 章　系统配置和引导管理

本章详细介绍了系统 **UEFI Setup Utility**。

系统信息

本节介绍系统的配置、固件和产品数据。

表 2. 系统信息

项	描述
第 7 页 “系统摘要”	系统详细信息摘要
第 8 页 “产品数据”	系统固件信息
第 8 页 “开源许可证”	开源许可证

系统摘要

本主题提供系统信息的摘要。

表 3. 系统摘要

项	格式	描述
系统标识数据		
机器类型/型号	**10** 或 **8** 个字符的 **ASCII** 字符串	系统机器类型和型号
序列号	**10** 或 **8** 个字符的 **ASCII** 字符串	序列号
UUID 编号	**16** 字节十六进制字符串（**32** 个字符）	通用唯一标识符（**UUID**）
资产标记号	**32** 个字符的 **ASCII** 字符串	客户分配的系统资产标记号
处理器		
已安装的 CPU 封装数	**1** 个字符的 **ASCII** 字符串	已安装的 **CPU** 封装数
处理器速度	**y.yyy GHz**	处理器速度
UPI 链路速度	**yy.y GT/s**	**UPI** 链路速度 **注：**仅当装有两个或更多处理器时，**UPI** 功能才有效。
内存		
内存模式	**ASCII** 字符串	内存模式
DIMM 运行频率	**yyyy MT/s**	系统中正在运行的 **DIMM** 的当前频率。
检测到的内存总量	**yyyy GB**	所有已安装 **DIMM** 的总容量
DIMM	**yyyy GB**	系统上安装的 **DIMM** 总容量。

表 3. 系统摘要 （续）

项	格式	描述
CXL 内存	**yyyy GB**	系统上安装的 **CXL** 内存设备总容量。 **注：**如果没有 **CXL** 设备，则此项将被隐藏。
可用内存容量总量	**yyyy GB**	扣除镜像模式、预留或坏块等因素导致的开销后的可用内存量

产品数据

本主题提供有关主机系统和基板管理控制器（**BMC**）固件的基本信息。

表 4. 产品数据

项	格式	描述
主机固件		
Build ID	**7** 个字符的 **ASCII** 字符串	主机固件的 **Build ID**
版本	字符串格式：**X.YY**（其中 ***X*** 为主要修订版，***YY*** 为次要修订版）	主机固件版本
Build 日期	字符串格式：**YYYY/MM/DD**	主机固件的 **Build** 日期
BMC 固件		
Build ID	**ASCII** 字符串	基板管理控制器（**BMC**）固件的 **Build ID**
版本	**ASCII** 字符串	**BMC** 固件版本
Build 日期	字符串格式：**YYYY/MM/DD**	**BMC** 固件的 **Build** 日期

开源许可证

项	选项	功能说明
开源许可证	不适用	***开源许可证*** 的菜单标题
本页列出了开源软件的致谢信息和所需的版权声明，具体内容取决于平台。		

系统设置

本节概述了 **Unified Extensible Firmware Interface**（**UEFI**）中的可配置选项。

表 5. 系统设置

项	选项	描述
<F1> 启动控制	• **自动**（默认） • 工具套件 • 文本设置程序	使用 **F1** 键或等效的 **IPMI** 命令选择要启动的工具。 • [工具套件]：启动支持以下功能的图形化工具套件：系统信息摘要、**UEFI** 设置、平台更新、**RAID** 设置、操作系统安装和诊断。 • [文本设置程序]：在文本模式下启动 **UEFI Setup Utility**。 • [自动]：如果已启用 **Serial Over LAN**（**SOL**）或控制端口重定向，或者 **SOL** 配置为 [自动] 并检测到活动会话，则在文本模式下启动 **UEFI Setup Utility**。否则，[自动] 将启动图形化工具套件。
工作负载概要文件	• **通用计算 - 能效**（默认） • 通用计算 - 峰值频率 • 通用计算 - 最大性能 • 虚拟化 - 能效 • 虚拟化 - 最大性能 • 数据库 - 事务处理 • 低延迟 • 高性能计算 • 自定义	根据您的偏好选择概要文件。 所选工作负载概要文件将自动更改低级设置，并且不允许单独更改这些设置。要单独设置低级别设置，请选择 [自定义] 选项。 “能效”概要文件包含与 **Intel** 优化电源模式（**OPM**）相当的设置。
第 9 页 “设备和 I/O 端口”	不适用	查看和配置板载设备和 **I/O** 端口选项。
第 17 页 “驱动程序运行状况”	不适用	查看驱动程序的运行状况状态。
外部设备	不适用	查看外部设备（如果已安装）。
第 18 页 “内存”	不适用	查看和配置内存设置。
第 24 页 “网络”	不适用	查看和配置网络设备和网络相关设置。
第 34 页 “电源”	不适用	配置电源计划选项。
第 35 页 “处理器”	不适用	查看和配置处理器设置。
第 46 页 “恢复和 RAS”	不适用	配置恢复策略和高级可靠性、可用性和可维护性（**RAS**）设置。
第 47 页 “安全性”	不适用	配置系统安全性设置。
第 52 页 “存储”	不适用	管理存储适配器选项。部分系统可能使用平面设备，并可以通过**设备和 I/O 端口**菜单进行配置。

设备和 I/O 端口

根据安装的具体硬件（例如使用的转接卡类型），可用的设置可能有所不同。此菜单上的项因服务器平台而异。

表 6. 设备和 I/O 端口

项	选项	描述
基本 MM 配置	• **自动**（默认）	[自动]：系统自动分配值。 较高的值会增加 **4 GB** 以下操作系统的可用内存，但会减少可用于 **PCI** 适配器的内存映射 **I/O**（**MMIO**）资源。较低的值会增加 **MMIO** 资源，但会减少 **4 GB** 以下操作系统的可用内存。 如果更改设置后出现任何问题，您可以恢复到之前的选择。
MMIOH 基址	• **40 T** • **24 T** • **16 T** • **4 T** • **2 T** • **自动**（默认）	设置 **MMIOH** 高基址。此设置可以配置为高于已安装的总内存（包括任何 **CXL** 内存）的值。
MMIOH 大小	• **64 G** • **256 G** • **1024 G**（默认）	选择用于分配 **MMIO** 高资源的可用粒度大小。每个堆栈的 **MMIO** 高资源分配是粒度的倍数，每个堆栈默认分配 **1** 个单位。
SRIOV	• **已启用**（默认） • 已禁用	启用或禁用系统引导期间对单根 **I/O** 虚拟化（**SR-IOV**）虚拟功能的资源分配支持。 **注：**选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
可调整大小的 BAR	• **已启用**（默认） • 已禁用	可调整大小的基址寄存器（**BAR**）是一项 **PCIe** 功能。它本质上允许兼容的 **PCIe** 设备从系统协商更多的 **BAR** 资源，从而提高性能。
PCIe 访问控制服务（ACS）	• **启用**（默认） • 禁用	允许在 **UEFI** 初始化期间禁用 **PCIe** 交换机和端点的访问控制服务（**ACS**）。当 **ACS** 禁用时，**VT-d** 功能可能会受到限制。如果 **VT-d** 和/或 **SRIOV** 已启用，操作系统可能会重新启用 **PCIe ACS**。
DMA 控制选择加入标志	• **已启用**（默认） • 已禁用	启用或禁用 **DMA** 重映射（**DMAR**）**ACPI** 表中的 **DMA** 控制选择加入标志（**DMA_CTRL_PLAT-FORM_OPT_IN_FLAG**）。 此项与直接设备分配（**DDA**）不兼容。
预引导 DMA 保护	• **已启用**（默认） • 已禁用	在预引导环境中启用或禁用直接内存访问（**DMA**）保护。
第 11 页 “启用/禁用板载设备”	不适用	启用或禁用板载设备或插槽。
第 12 页 “启用/禁用适配器 ROM 选项支持”	不适用	启用或禁用符合 **UEFI** 标准的适配器支持。禁用 **UEFI** 支持可能会对预引导/引导功能产生不利影响。

表 6. 设备和 I/O 端口 （续）

项	选项	描述
第 12 页 “PCIe 代系速度选择”	不适用	选择可用 PCIe 插槽的运行速度。
第 13 页 “覆盖插槽分叉”	不适用	此设置用于覆盖物理 x16 插槽的分叉设置，以支持带有多个设备的适配器。
第 14 页 “PCIe 链路降级报告选择”	不适用	选择是否禁止显示可用 PCIe 插槽的 PCIe 链路降级错误。
第 15 页 “控制端口重定向设置”	不适用	配置控制端口重定向和 COM 端口设置
第 17 页 “Intel® VMD 技术”	不适用	启用或禁用 Intel® 卷管理设备（VMD）技术。

启用/禁用板载设备

根据安装的具体硬件（例如使用的转接卡类型），可用的设置可能有所不同。此菜单上的项因服务器平台而异。

表 7. 启用/禁用板载设备

项	选项	描述
板载视频	• **已启用**（默认） • 已禁用	启用或禁用板载视频设备。 如果选择 [已禁用]，则在后续引导过程中将不会枚举关联的设备。 [自动] 将在未安装设备或在该设备上检测到错误时禁用此端口。
插槽 1	• 已禁用 • **已启用**（默认） 或 • 已禁用 • 已启用 • **自动**（默认）	启用或禁用关联的设备。 如果选择 [已禁用]，则在后续引导过程中将不会枚举关联的设备。 [自动] 将在未安装设备或在该设备上检测到错误时禁用此端口。
插槽 2	• 已禁用 • **已启用**（默认） 或 • 已禁用 • 已启用 • **自动**（默认）	启用或禁用关联的设备。 如果选择 [已禁用]，则在后续引导过程中将不会枚举关联的设备。 [自动] 将在未安装设备或在该设备上检测到错误时禁用此端口。

表 7. 启用/禁用板载设备 （续）

项	选项	描述
插槽（n...）	• 已禁用 • **已启用**（默认） 或 • 已禁用 • 已启用 • **自动**（默认）	启用或禁用关联的设备。 如果选择 [已禁用]，则在后续引导过程中将不会枚举关联的设备。 [自动] 将在未安装设备或在该设备上检测到错误时禁用此端口。
M.2 NVMe 插槽（n...）	• 自动 • **已启用**（默认） • 已禁用	启用或禁用关联的设备。 如果选择 [已禁用]，则在后续引导过程中将不会枚举关联的设备。 [自动] 将在未安装设备或在该设备上检测到错误时禁用此端口。

启用/禁用适配器 ROM 选项支持

根据安装的具体硬件（例如使用的转接卡类型），可用的设置可能有所不同。此菜单上的项因服务器平台而异。

此菜单上项的实际顺序可能与下表不同，因为其中一些项是动态扫描的。

表 8. 启用/禁用适配器 ROM 选项支持

项	选项	描述
板载视频	• **已启用**（默认） • 已禁用	启用或禁用板载视频设备的 **ROM** 选项。 **注**：禁用某些 **UEFI ROM** 选项可能会对 **iSCSI** 和 **BoFM** 操作产生不利影响。
插槽 1	• **已启用**（默认） • 已禁用	启用或禁用 **PCIe** 设备的 **ROM** 选项。 **注**：禁用某些 **UEFI ROM** 选项可能会对 **iSCSI** 和 **BoFM** 操作产生不利影响。
插槽 2	• **已启用**（默认） • 已禁用	启用或禁用 **PCIe** 设备的 **ROM** 选项。 **注**：禁用某些 **UEFI ROM** 选项可能会对 **iSCSI** 和 **BoFM** 操作产生不利影响。
插槽（n...）	• **已启用**（默认） • 已禁用	启用或禁用 **PCIe** 设备的 **ROM** 选项。 **注**：禁用某些 **UEFI ROM** 选项可能会对 **iSCSI** 和 **BoFM** 操作产生不利影响。
M.2 NVMe 插槽（n...）	• **已启用**（默认） • 已禁用	启用或禁用 **M.2 NVMe** 设备的 **ROM** 选项。 **注**：禁用某些 **UEFI ROM** 选项可能会对 **iSCSI** 和 **BoFM** 操作产生不利影响。

PCIe 代系速度选择

根据安装的具体硬件（例如使用的转接卡类型），可用的设置可能有所不同。此菜单上的项因服务器平台而异。

表 9. PCIe 代系速度选择

项	选项	描述
插槽 1	• **自动**（默认） • **Gen1** • **Gen2** • **Gen3** • **Gen4** • **Gen5** **注**：显示的选项取决于设备支持的速度。	设置 **PCIe** 插槽支持的最大速度。
插槽 2	• **自动**（默认） • **Gen1** • **Gen2** • **Gen3** • **Gen4** • **Gen5** **注**：显示的选项取决于设备支持的速度。	设置 **PCIe** 插槽支持的最大速度。
插槽（n...）	• **自动**（默认） • **Gen1** • **Gen2** • **Gen3** • **Gen4** • **Gen5** **注**：显示的选项取决于设备支持的速度。	设置 **PCIe** 插槽支持的最大速度。
M.2 NVMe 插槽（n...）	• **自动**（默认） • **Gen1** • **Gen2** • **Gen3** • **Gen4** • **Gen5** **注**：显示的选项取决于设备支持的速度。	设置 **PCIe** 设备支持的最大速度。

覆盖插槽分叉

根据安装的具体硬件（例如使用的转接卡类型），可用的设置可能有所不同。此菜单上的项因服务器平台而异。

表 10. 覆盖插槽分叉

项	选项	描述
插槽 1	• **x16**（默认） • **x8x8** • **x8x4x4** • **x4x4x8** • **x4x4x4x4**	配置物理 **x16** 插槽的分叉设置，以支持带有多个设备的适配器。 • **[x16]**：使用系统设置对插槽进行分叉。 • **[x8x8]**：将物理 **x16** 插槽分叉，以最多支持两个 **x8** 设备。 • **[x8x4x4]** 或 **[x4x4x8]**：将物理 **x16** 插槽分叉，以最多支持一个 **x8** 设备和两个 **x4** 设备。 • **[x4x4x4x4]**：将物理 **x16** 插槽分叉，以最多支持四个 **x4** 设备。
插槽 2	• **x16**（默认） • **x8x8** • **x8x4x4** • **x4x4x8** • **x4x4x4x4**	配置物理 **x16** 插槽的分叉设置，以支持带有多个设备的适配器。 • **[x16]**：使用系统设置对插槽进行分叉。 • **[x8x8]**：将物理 **x16** 插槽分叉，以最多支持两个 **x8** 设备。 • **[x8x4x4]** 或 **[x4x4x8]**：将物理 **x16** 插槽分叉，以最多支持一个 **x8** 设备和两个 **x4** 设备。 • **[x4x4x4x4]**：将物理 **x16** 插槽分叉，以最多支持四个 **x4** 设备。
插槽（n...）	• **x16**（默认） • **x8x8** • **x8x4x4** • **x4x4x8** • **x4x4x4x4**	配置物理 **x16** 插槽的分叉设置，以支持带有多个设备的适配器。 • **[x16]**：使用系统设置对插槽进行分叉。 • **[x8x8]**：将物理 **x16** 插槽分叉，以最多支持两个 **x8** 设备。 • **[x8x4x4]** 或 **[x4x4x8]**：将物理 **x16** 插槽分叉，以最多支持一个 **x8** 设备和两个 **x4** 设备。 • **[x4x4x4x4]**：将物理 **x16** 插槽分叉，以最多支持四个 **x4** 设备。

PCIe 链路降级报告选择

根据安装的具体硬件（例如使用的转接卡类型），可用的设置可能有所不同。此菜单上的项因服务器平台而异。

表 11. PCIe 链路降级报告选择

项	选项	描述
插槽 1	• **已启用**（默认） • 已禁用	选择是否禁止显示 **PCIe** 插槽的 **PCIe** 链路降级错误。
插槽 2	• **已启用**（默认） • 已禁用	选择是否禁止显示 **PCIe** 插槽的 **PCIe** 链路降级错误。

表 11. PCIe 链路降级报告选择 （续）

项	选项	描述
插槽（n...）	• **已启用**（默认） • 已禁用	选择是否禁止显示 **PCIe** 插槽的 **PCIe** 链路降级错误。
M.2 NVMe 插槽（n...）	• **已启用**（默认） • 已禁用	选择是否禁止显示 **PCIe** 插槽的 **PCIe** 链路降级错误。

控制端口重定向设置

在此菜单上，您可以配置控制台输出的管理方式，尤其是针对远程管理和故障诊断等目的。

表 12. 控制端口重定向设置

项	选项	描述
COM 端口 1	• **已启用**（默认） • 已禁用	启用或禁用 **COM 1** 设备。 选择 **[**已禁用**]** 时，关联的 **COM 1** 终端设置将被隐藏。
虚拟 COM 端口 2	• **已启用**（默认） • 已禁用	启用或禁用虚拟 **COM** 端口 **2** 设备。 选择 **[**已禁用**]** 时，将禁用用于控制端口重定向的 **SSH**。
控制端口重定向	• 已启用 • **已禁用**（默认） 或 • 已启用 • 已禁用 • **自动**（默认） **注**：选项取决于 **UEFI** 版本。	启用或禁用控制端口重定向。 选择 **[**自动**]** 时，如果 **IPMI Serial over LAN** 状态为活动，则会自动启用控制端口重定向。
串口共享	• 已启用 • **已禁用**（默认）	启用 **BMC** 以允许访问系统串口。 选择 **[**已启用**]** 时，允许 **BMC** 根据远程控制命令的请求控制串行通信端口。 选择 **[**已禁用**]** 时，除非**串口访问模式**设置为 **[**已禁用**]**，否则会将串口分配给 **BMC**。
串口访问模式	• 共享 • 专用 • **已禁用**（默认）	此选项可用于控制系统 **BMC** 对系统串口的访问。 • **[**共享**]**：串口可用于 **POST** 和操作系统；但是，**BMC** 将/可以监控串行数据以接管控制权。 • **[**专用**]**：**BMC** 可以完全控制串口。**POST** 和/或操作系统将无法使用串口。 • **[**已禁用**]**：**BMC** 无法访问串口。

表 12. 控制端口重定向设置 （续）

项	选项	描述
SP 重定向	• 已启用 • **已禁用**（默认）	**Serial over LAN**（**SOL**）或 **Serial over SSH** 重定向使系统管理员能够将 **BMC** 用作串行终端服务器。此项可用于选择重定向的模式，即 **SOL** 或 **SSH**。 • 选择 **[**已禁用**]** 时，将配置为 **SOL** 重定向。 • 选择 **[**已启用**]** 时，可以通过 **SSH** 连接（虚拟 **COM 2**）访问服务器串口。 **注**：仅当“控制端口重定向”设置为 **[**已启用**]** 时，才会显示此项。
	• 已启用 • 已禁用 • **自动**（默认）	**[**已启用**]**：控制台将重定向到**虚拟 COM2**。**Serial Over LAN**（**SOL**）或 **SHH** 重定向使系统管理员能够将 **BMC** 用作串行终端服务器。 **[**自动**]**：当选择 **[**自动**]** 时，如果 **IPMI Serial over LAN**（**SOL**）或 **SSH** 处于活动状态，控制台将重定向到**虚拟 COM2**。将 **SP** 重定向设置为 **[**已启用**]** 时，即可通过 **SSH** 连接（虚拟 **COM2**）来访问服务器串口。
COM1 设置		
COM1 波特率	• **115200** （默认） • **57600** • **38400** • **19200** • **9600**	设置主机和远程系统之间的连接速度。
COM1 数据位数	• **8** （默认） • **7**	设置每个字符中的数据位数。
COM1 奇偶校验	• **无**（默认） • 奇数 • 偶数	将每个字符中的奇偶校验位设置为 **[**无**]**、**[**奇数**]** 或 **[**偶数**]**。 **[**无**]** 表示不传输奇偶校验位。
COM1 停止位	• **2** • **1** （默认）	设置停止位。停止位在每个字符的末尾发送，允许信号接收器检测字符的末尾并与字符流重新同步。
COM1 终端模拟	• **VT100** • **VT100Plus** • **VT-UTF8** • **ANSI**（默认）	仅当远程模拟器不支持 **ANSI** 文本图形时，才选择 **[VT100]**。 **注**：如果需要，请更改远程模拟器中的字符编码设置，以确保字符正确显示。
COM1 流量控制	• **已禁用**（默认） • 硬件	仅当远程模拟器支持并正在使用硬件流量控制时，才选择 **[**硬件**]**。

Intel® VMD 技术

Intel® 卷管理设备（VMD）技术旨在增强对 NVMe 固态硬盘的管理，尤其是在使用 Intel Xeon 处理器的企业环境中。

表 13. Intel® VMD 技术

项	选项	描述
Intel® VMD 技术	不适用	按 **Enter** 进入 **Intel® VMD** 技术的配置菜单。
启用/禁用 Intel® VMD	• 已启用 • **已禁用**（默认）	启用或禁用 **Intel® VMD** 技术。

驱动程序运行状况

此菜单显示系统中控制器的运行状况状态，这些状态由其相应的驱动程序报告。

表 14. 驱动程序运行状况

项	选项	描述
该平台：	• **状况良好** • 需要维修 • 需要配置 • 操作失败 • 需要重新连接 • 需要重新引导 • 需要关机 • 无需操作	显示系统的运行状况状态。
驱动程序/控制器状态		
驱动程序/控制器名称 - 状态	• **状况良好** • 需要维修 • 需要配置 • 操作失败 • 需要重新连接 • 需要重新引导 • 需要关机 • 无需操作	显示驱动程序/控制器的运行状况状态。
POST 尝试驱动程序	• **状况良好** • 需要维修 • 需要配置 • 操作失败 • 需要重新连接 • 需要重新引导 • 需要关机 • 无需操作	显示 **POST** 尝试驱动程序的运行状况状态。

外部设备

注：此菜单的内容可能因您的系统配置（例如，安装的设备）而异。

表 15. 外部设备

项	描述
外部设备 列出外部设备（如果已安装）	此菜单会显示已安装的所有外部设备。

内存

此菜单会显示并提供更改内存设置的选项。

表 16. 内存

项	选项	描述
第 20 页 “系统内存详细信息”	不适用	查看系统内存的状态。
内存纠正错误	• 已禁用 • **已启用**	启用/禁用运行时内存纠正错误报告。[已禁用] 导致 ADDDC 备用、运行时 PPR 和镜像故障转移不生效。 选择预设的工作负载 **profile** 时，低级设置不可更改。如果用户想要更改低级设置，请在“系统设置”子菜单下的“工作负载 **Profile**”中选择 [自定义]，然后根据需要更改各个设置。
ADDDC 备用	• **已禁用**（默认） • 已启用	自适应双设备数据校正（ADDDC）备用是一种 RAS 功能，可在虚拟锁步模式下提供更可靠的内存纠错。 **注：** • 如果系统具有 **x8 DIMM**，ADDDC 备用将不会生效。 • 启用完全镜像或部分镜像时，此设置为 [已禁用] 并灰显。您可以通过**内存 → 镜像配置 → 完全镜像**或**内存 → 镜像配置 → 部分镜像**来访问镜像设置。
页面策略	• **已关闭**（默认） • 自适应	“页面策略”设置决定内存控制器是否保持上次访问的页面处于打开状态。 • **[自适应]**：提高具有高度局部化内存访问模式的应用程序的性能。 • **[已关闭]**：有利于更随机地访问内存的应用程序。
DDR MBIST	• **已禁用**（默认） • 已启用	启用或禁用 **DDR** 内存内置自检（**MBIST**）。
DRAM 封装后修复	• **已启用**（默认） • 已禁用	启用或禁用 **DRAM** 封装后修复（**PRR**）。
内存测试	• 已禁用 • **已启用**（默认）	在正常引导期间启用或禁用内存测试。

表 16. 内存 （续）

项	选项	描述
运行时 PPR/行备用	• **已禁用** （默认） • 已启用	启用或禁用运行时 PRR/行备用。 **注**：此项不适用于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”）。
快速冷引导	• 已禁用 • **已启用** （默认）	启用或禁用“快速冷引导”。
快速 AC 引导	• 已禁用 • **已启用** （默认）	启用或禁用“快速 **AC** 引导”，仅适用于 **AC** 引导。 **注**：仅当启用**快速冷引导**时，此项才可用且有效。
全局数据加扰	• 已禁用 • **已启用** （默认）	数据总线上的内存流量并非随机，可能会导致 **DIMM** 上出现电流“热点”。“内存数据加扰”利用内存控制器中的数据加扰功能，在数据总线上创建伪随机模式，以降低因过度电流波动影响而发生数据位错误的可能性。
轮巡检查	• 已禁用 • **已启用** （默认）	启用/禁用“轮巡检查”（此功能主动搜索系统内存以修复可纠正的错误）。选择 **[**已启用**]** 后，轮巡检查将在 **POST** 结束时生效。 选择预设的工作负载 **profile** 时，低级设置不可更改。如果用户想要更改低级设置，请在“系统设置”子菜单下的“工作负载 **Profile**”中选择 **[**自定义**]**，然后根据需要更改各个设置。
插槽交错	• **NUMA**（默认） • 非 **NUMA**	“插槽交错”决定了内存映射在系统中的布局方式。内存的布局方式有两种：一种是使每个 **CPU** 都具有本地附加内存的映射（**NUMA**），另一种是采用没有 **NUMA** 节点的扁平内存模型（非 **NUMA**）。 • **[NUMA]**：内存不会在处理器之间交错。 • **[**非 **NUMA]**：内存会在处理器之间交错。 **注**： • 此项不适用于以下处理器： – **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”） – **Intel Xeon 6** 处理器（原代号为“**Granite Rapids**”）：**LCC** 或 **UCC SKU** – **Intel Xeon 6** 处理器（原代号为“**ClearWaterForest**”） • 此项在以下情况下为只读： – 已启用 **SGX**。 – 仅启用一个 **CPU** 插槽，或者不支持 **NUMA**。
动态 ECC 模式选择	• 已禁用 • **已启用** （默认）	启用或禁用动态 **ECC** 模式选择。

表 16. 内存 （续）

项	选项	描述
内存速度	• **最大性能**（默认） • 均衡 • 最小功耗	选择所需的内存速度。 • [最大性能] 模式会将性能最大化。 • [均衡] 模式在性能和功耗之间实现平衡。 • [最小功耗] 模式会将节能最大化。 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
DDR5 ECS	• 已禁用 • **已启用**（默认） • 启用带结果收集的 **ECS**	错误检查和清理（**ECS**）功能可以提前检测到可能的 **DRAM** 故障，从而避免或减少停机时间。 • [已禁用]：禁用 **ECS** 功能。 • [已启用]：启用不带结果收集的 **ECS**。 • [启用带结果收集的 **ECS**]：启用带结果收集的 **ECS**。
第 20 页 “镜像配置”	不适用	查看和配置内存镜像状态。 **注**：仅当“**ADDDC** 备用”已禁用且内存插入情况符合要求时，才能配置此项。
第 22 页 “CXL 内存条”	不适用	**CXL** 内存条（**CMM**）信息、状态和配置。

系统内存详细信息

本节介绍系统中安装的 **DIMM** 的基本信息。

系统内存详细信息

表 17. 系统内存详细信息

项	描述
处理器 X 的 DIMM 详细信息	查看与特定处理器关联的已安装 **DIMM** 的状态。

DIMM 详细信息

如果 **DIMM** 上发生双位错误（**DBE**），[已启用] 和 [已禁用] 选项将可用。对于当前一代，默认设置为 [已启用]。

镜像配置

在此菜单上，您可以管理和配置内存镜像设置。

表 18. 镜像配置

项	选项	描述
镜像故障转移	• 已禁用 • **已启用**（默认）	启用/禁用镜像故障转移。启用此项时，一个持久性内存不可纠正错误将触发镜像故障转移。此功能处于禁用状态时，即使发生永久性不可纠正错误，也可以跳过镜像故障转移。此功能仅在启用“完全镜像”或“部分镜像”时生效。 **注：** • 如果是 **HBM SKU**，则不支持此项。
由操作系统设定的配置	不适用	显示由操作系统实用程序定义的内存镜像配置。 找到定义后，可以使用**删除由操作系统设定的配置**来清除它。
4 GB 以下的镜像	无	显示 **4 GB** 以下内存的镜像配置。 **注：**操作系统配置内存镜像后，此选项可以是 **[TRUE]** 或 **[FALSE]**。
部分镜像比率（以基点计）	无	显示 **4 GB** 以上内存的镜像比率（以基点计）。 镜像选项为 **5%**、**10%**、**15%**、**20%**、**25%**、**30%**、**35%** 和 **40%**，分别代表 **500**、**1000**、**1500**、**2000**、**2500**、**3000**、**3500** 和 **4000**。输入的任何其他数字将四舍五入到最接近的较大数字。例如，如果数字大于 **2000** 但小于或等于 **2500**（即，**2000** < 数字 <= **2500**），将四舍五入为 **2500**。大于 **4000** 的数字（> **4000**）将四舍五入为 **4000**。 **注：** • 操作系统配置内存镜像后，此选项可能是 **1–5000** 范围内的值。 • 此项不适用于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”）。
由 UEFI 设定的配置	不适用	显示由 **UEFI Setup Utility** 定义的内存镜像配置。 如果 **UEFI Setup Utility** 定义的值与操作系统定义的值冲突，则优先采用操作系统定义的值。
完全镜像	• **已禁用**（默认） • 已启用	完全镜像可将可用系统内存减少到已安装总内存的 **50%**。 当 **ADDDC 备用**或**部分镜像**为 **[已启用]** 时，此设置为 **[已禁用]** 并灰显。 **注：** • 当 **CXL** 内存条中的“内存模式”为“异构交错”时，此设置将灰显。要启用此设置，需要确保将 **CXL** 内存条中的“内存模式”设置为“**1LM + Vol**”。

表 18. 镜像配置 （续）

项	选项	描述
部分镜像	• **已禁用**（默认） • 已启用	部分镜像可将每个处理器的可用系统内存最多减少 **40%**。该比例由**部分镜像比率（以基点计）**设置。 当 **ADDDC 备用**或**完全镜像**为 [已启用] 时，此设置为 [已禁用] 并灰显。 **注：** • 此项不适用于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”）。 • 当 **CXL** 内存条中的“内存模式”为“异构交错”时，此设置将灰显。要启用此设置，需要确保将 **CXL** 内存条中的“内存模式”设置为“**1LM + Vol**”。
4 GB 以下的镜像	• **已禁用**（默认） • 已启用	启用此选项后，将镜像低于 **4 GB** 地址限制的所有可用系统内存（通常为 **1 GB** 到 **3 GB**）。 **注：**此项不适用于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”）。
部分镜像比率（以基点计）	• 值范围：**1 - 4000** • **200** （默认）	为 **4 GB** 以上的内存配置镜像比率（以基点计）。 镜像选项为 **5%**、**10%**、**15%**、**20%**、**25%**、**30%**、**35%** 和 **40%**，分别代表 **500**、**1000**、**1500**、**2000**、**2500**、**3000**、**3500** 和 **4000**。输入的任何其他数字将四舍五入到最接近的较大数字。例如，如果数字大于 **2000** 但小于或等于 **2500**（即，**2000** < 数字 <= **2500**），将四舍五入为 **2500**。大于 **4000** 的数字（> **4000**）将四舍五入为 **4000**。 **注：**此项不适用于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”）。

CXL 内存条

项	选项	功能说明
内存模式	**1LM + Vol** 异构交错	**[1LM + Vol]：DRAM** 和 **CMM** 在软件中显示为两个独立的 **NUMA** 节点。 **[异构交错]：DRAM** 和 **CMM** 在软件中显示为一个 **NUMA** 节点，并且相互交错。 注： 启用内存模式取决于硬件配置和固件配置。如果检测到任何依赖关系未满足，**UEFI** 将回退到 **1LM + Vol** 模式。详细配置方法请参阅产品手册。

		注：要启用 [异构交错] 模式，必须满足以下要求，否则 **UEFI** 会自动将系统配置为 **1LM + Vol** 模式（设置不变）： 1. 系统设置 -> 处理器 -> **SNC** = <已禁用> 2. 系统设置 -> 处理器 -> **UPI** 亲和性 = <已禁用> 3. 系统设置 -> 内存 -> 插槽交错 =<**NUMA**> 4. 系统设置 -> 内存 -> 镜像配置 -> 完全镜像 = <已禁用> 和系统设置 -> 内存 -> 镜像配置 -> 部分镜像 = <已禁用> 5. 确保 **DIMM** 和 **CXL** 内存设备的配置符合用户指南要求。
MEFN 支持	• 已禁用 • **固件优先** • 操作系统优先	内存错误固件通知（**MEFN**）机制用于报告 **CMM** 内存错误。 • **[已禁用]**：禁用 **CMM** 错误事件通知。 • **[固件优先]**：启用固件来处理 **CMM** 错误。 • **[操作系统优先]**：启用操作系统来处理 **CMM** 错误。
插槽 XX：CMM YY-ZZ-MM		**CMM** 信息和状态。
...		
插槽 XX：CMM YY-ZZ-MM		**CMM** 信息和状态。

注：XX、YY、ZZ 和 MM 是与指定平台相关的设备插槽 ID、总线、设备和功能编号。

CMM 详细信息

项	**描述**
制造商	**CMM** 制造商。
固件版本	**CMM** 固件版本。
序列号	**CMM** 控制器序列号。

容量	CMM 内存大小。
运行状况	设备总体运行状况状态摘要。 • [正常]：CMM 状态正常。 • [需要维护]：需要进行 PPR 或内置测试。 • [性能下降]：因初始化期间检测到不可恢复的错误导致性能下降。 • [内存容量下降]：因初始化期间检测到不可恢复的错误导致容量下降。 • [需要更换硬件]：需要更换 CMM。

网络

此菜单显示网络设备和网络相关设置。

表 19. 网络

项	描述
第 24 页 “网络引导设置”	配置网络引导参数。
第 27 页 “iSCSI 设置”	配置 iSCSI 参数。
第 32 页 “网络栈设置”	配置网络栈设置。
第 32 页 “HTTP 引导配置”	配置 HTTP 引导参数。 **注**：仅当已启用**网络 -> 网络栈设置 -> IPv4 HTTP 支持**或 **IPv6 HTTP 支持**时，此项才可用。
第 33 页 “Tls 认证配置”	您可以按 Enter 选择 Tls 认证配置。 **注**：仅当已启用**网络 -> 网络栈设置 -> IPv4 HTTP 支持**或 **IPv6 HTTP 支持**时，此项才可用。
网络设备列表	查看网络设备。此处将显示板载卡或附加卡的信息，例如卡的标题、MAC 地址或 PFA。

网络引导设置

表 20. 网络引导设置

项	描述
MAC:XX:XX:XX:XX:XX:XX **SlotXXX PCI X:XX:X:X**	在 **MAC XX:XX:XX:XX:XX:XX** 上设置引导配置参数 **PCI 功能地址：Bus XX:Dev XX:Func XX**
VLAN 配置列表： **插槽 X：VLAN 配置** **注**：对于板载设备，没有“插槽 X：”字符串。	配置 VLAN 参数。 （**MAC:XXXXXXXXXXXX**）

表 20. 网络引导设置 （续）

项	描述
IPv4 配置列表： **插槽 X：IPv4 网络配置** **注**：对于板载设备，没有“插槽 **X**：”字符串。	配置 **IPv4** 网络参数。 （**MAC:XXXXXXXXXXXX**）
IPv6 配置列表： **插槽 X：IPv6 网络配置** **注**：对于板载设备，没有“插槽 **X**：”字符串。	配置 **IPv6** 网络参数。 （**MAC:XXXXXXXXXXXX**）

MAC：板载 PCI

表 21. MAC：板载 PFA 1:0:0

项	选项	描述
UEFI PXE 模式	• **已启用**（默认） • 已禁用	启用或禁用 **NIC**，以在通用 **PXE** 网络引导期间包含或跳过引导尝试。

VLAN 配置

在**进入配置菜单**上，按 **Enter** 进入 **VLAN** 配置菜单。

表 22. VLAN 配置

项	选项	描述
新建 VLAN		
VLAN ID	**0–4094**	设置新 **VLAN** 或现有 **VLAN** 的 **VLAN ID**。有效值为 **0–4094**。
优先级	**0–7**	设置 **802.1Q** 优先级。有效值为 **0–7**。
添加 VLAN	不适用	新建 **VLAN** 或更新现有 **VLAN**。
已配置 VLAN 列表		
已配置的 **VLAN** 的列表。仅在配置了 **VLAN** 时显示。 示例：**VLAN ID: X, 优先级: X**	复选框： • **空** • **X**	从列表中选择一个 **VLAN** 以将其删除。
删除 VLAN	不适用	删除选定的 **VLAN**。

IPv4 网络配置

表 23. 插槽 X：IPv4 网络配置

项	选项	描述
已配置	复选框： • **空** • **X**	指示网络地址是否已配置成功。
保存更改并退出	不适用	保存更改并退出。

IPv6 网络配置

在**进入配置菜单**上，按 **Enter** 进入 **IPv6** 网络配置菜单。

表 24. 插槽 X：IPv6 当前设置

项	选项	描述
接口名称	不适用	网络接口的名称
接口类型	不适用	网络接口的类型，在 **RFC1700** 中定义
MAC 地址	**XX-XX-XX-XX-XX-XX**	网络接口的硬件地址
主机地址	**XXXX::XXXX:XXXX:XXXX:X-XXX/XX**	主机地址列表，其中包含本地 **IPv6** 地址和相应的前缀长度信息
路由表	**XXXX::/64>>::**	此接口上运行的 **IPv6** 网络栈路由表
网关地址	不适用	当前网关 **IPv6** 地址列表
DNS 地址	不适用	当前网关 **DNS** 地址列表
接口 ID	不适用	设备的 **64** 位备用接口 **ID**。该字符串以冒号分隔。例如 **ff:dd:88:66:cc:1:2:3**
DAD 传输计数	不适用	在对暂定地址执行重复地址检测（**DAD**）时发送的连续邻居请求消息的数量。值“**0**”（零）表示不执行重复地址检测。
策略	• **自动** • 手动	配置网络配置策略。
高级配置	不适用	手动配置接口的网络设置，包括 **IP** 地址、网关地址和 **DNS** 服务器地址。
保存更改并退出	不适用	保存更改并退出。

表 25. 高级配置

项	选项	描述
新 IPv6 地址	不适用	仅当**策略**设置为**手动**时，才能配置此项。 用空格分隔 IP 地址以配置多个地址。例如 **2002::1/64 2002::2/64**
新网关地址	不适用	仅当**策略**设置为**手动**时，才能配置此项。 用空格分隔 IP 地址以配置多个地址。
新 DNS 地址	不适用	仅当**策略**设置为**手动**时，才能配置此项。 用空格分隔 IP 地址以配置多个地址。
提交更改并退出	不适用	提交更改并退出。
放弃更改并退出	不适用	放弃更改并退出。

iSCSI 设置

在此菜单上，您可以配置 **iSCSI** 发起程序，它允许系统通过网络连接到 **iSCSI** 目标。

表 26. iSCSI 设置

项	选项	描述
iSCSI 发起方名称	**Iqn.1986-03.com.example**	**iSCSI** 发起方的全球唯一名称 仅接受 **iSCSI** 限定名称（**IQN**）格式。
第 28 页 “添加尝试”	不适用	配置并添加尝试。
尝试列表 例如 • 尝试 **1** • 尝试 **2** 选择列表中的任何项都将显示**第 28 页 “尝试设置”**	不适用	添加尝试后，此处将列出该尝试。 每次尝试的值将显示如下：**MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX，“iSCSI 模式”：[%s1]，“Internet 协议”：[%s1]**。 **注：** • 具体值会有所不同，具体取决于尝试设置。 • **%s1** 是 **iSCSI** 模式的选项名称。 • **%s2** 是 **Internet** 协议的设置名称。
第 30 页 “删除尝试”	不适用	删除一个或多个尝试。
第 31 页 “更改尝试顺序”	不适用	您可以使用 +/- 键更改尝试顺序。使用方向键选择尝试，然后按 +/- 在尝试顺序列表中向上/向下移动尝试。

添加尝试

表 27. MAC 选择

项	描述
系统中的 NIC 列表： 示例：**MAC XX:XX:XX:XX:XX:XX**	您可以选择要添加的项。尝试的格式如下：**PFA: Bus XX | Dev XX | Func XX**。

尝试设置

表 28. 尝试设置

项	选项	描述
iSCSI 尝试名称	不适用	**iSCSI** 尝试的人类可读名称。此项为只读。
iSCSI 模式	• **已禁用**（默认） • 已启用 • 为 **MPIO** 启用	启用或禁用 **iSCSI** 模式，或为多路径 **I/O**（**MPIO**）启用 **iSCSI** 模式。 **注**：在启用此功能之前，请确保正确设置了所有必要项（例如发起方 **IP**、目标 **IP** 和认证设置）。否则，重新引导后此尝试可能会丢失。
Internet 协议	• **IPv4**（默认） • **IPv6** • 自动配置	• **[IPv4]**：默认设置 • **[IPv6]**：由系统分配发起方 **IP** 地址。 • **[自动配置]**：**iSCSI** 驱动程序会尝试通过 **IPv4** 堆栈连接 **iSCSI** 目标。如果失败，它将尝试通过 **IPv6** 堆栈进行连接。
连接重试次数	**0**	最小值为 **0**，最大值为 **16**。 值“**0**”表示您不想重试。
连接建立超时	**1000**	超时值以毫秒为单位 最小值为 **100** 毫秒，最大值为 **20** 秒。
ISID	例如，**C68EF8**	**OUI** 格式的 **ISID**（**6** 个字节），**iSCSI** 会话标识符（**ISID**）指定登录期间的 **iSCSI** 发起方。 默认值派生自 **MAC** 地址。只有最后 **3** 个字节是可配置的。 示例：通过输入 **F07901** 将 **0ABBCCDDEEFF** 更新为 **0ABBCCF07901**。

表 28. 尝试设置 （续）

项	选项	描述
启用 DHCP	复选框： • **空**（默认） • **X**	启用或禁用 **DHCP**。
发起方 IP 地址	**0.0.0.0**	以点分十进制表示法设置发起方 **IP** 地址。 **注**：仅当**启用 DHCP** 未启用时，此项才可用。
发起方子网掩码	**0.0.0.0**	以点分十进制表示法设置发起方子网掩码 **IP** 地址。 **注**：仅当**启用 DHCP** 未启用时，此项才可用。
网关	**0.0.0.0**	以点分十进制表示法设置发起方网关 **IP** 地址。 **注**：仅当**启用 DHCP** 未启用时，此项才可用。
通过 DHCP 获取目标信息	复选框： • **空**（默认） • **X**	通过 **DHCP** 获取目标信息。 **注**：仅当**启用 DHCP** 已启用时，此项才可用。
目标名称	不适用	目标的全球唯一名称。仅接受 **IQN** 格式。 **注**：已启用**通过 DHCP 获取目标信息**时，此项不可用。 **I**
目标地址	不适用	输入 **IPv4** 或 **IPv6** 地址或 **URL** 字符串。 如果输入 **URL** 字符串，则需要预先配置 **DNS** 服务器地址。 **注**：已启用**通过 DHCP 获取目标信息**时，此项不可用。
目标端口	**3260**	设置目标端口号。 **注**：已启用**通过 DHCP 获取目标信息**时，此项不可用。

表 28. 尝试设置 （续）

项	选项	描述
引导 LUN	**0**	设置引导逻辑单元（LUN）编号的十六进制表示形式。 示例：**4751-3A4F-6b7e-2F99**、**6734-9-156f-127**、**4186-9** **注**：已启用**通过 DHCP 获取目标信息**时，此项不可用。
认证类型	• **CHAP** • **无**（默认）	选择认证方法。
CHAP 类型	• 单向 • **双向**（默认）	设置质询握手认证协议（CHAP）类型。 **注**：仅当**认证类型**设置为 **[CHAP]** 时，此项才可用。
CHAP 名称	不适用	设置 **CHAP** 名称。 **注**：仅当**认证类型**设置为 **[CHAP]** 时，此项才可用。
CHAP 密钥	不适用	设置 **CHAP** 密钥密码。密钥长度范围为 **12** 到 **16** 个字节。 **注**：仅当**认证类型**设置为 **[CHAP]** 时，此项才可用。
反向 CHAP 名称	不适用	反向 **CHAP** 名称。 **注**：仅当 **CHAP 类型**设置为 **[双向]** 时，此项才可用。
反向 CHAP 密钥	不适用	反向 **CHAP** 密钥密码。密钥长度范围为 **12** 到 **16** 个字节。 **注**：仅当 **CHAP 类型**设置为 **[双向]** 时，此项才可用。
保存更改	不适用	需要手动重新引导系统才能使更改生效。
返回到上一页	不适用	返回上一页。

删除尝试

表 29. 删除尝试

项	选项	描述
尝试列表 例如，尝试 **1**	复选框： • **空**（默认） • **X**	您可以选择要删除的尝试。 每次尝试的值将显示如下：**MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func**

表 29. 删除尝试 （续）

项	选项	描述
		XX，“iSCSI 模式”：[%s1]，“Internet 协议”：[%s2] **注：** • 具体值会有所不同，具体取决于尝试设置。 • **%s1** 是 **iSCSI** 模式的选项名称。 • **%s2** 是 **Internet** 协议的设置名称。
提交更改并退出	不适用	保存更改并退出。
放弃更改并退出	不适用	放弃更改并退出。

表 30. 删除尝试

项	选项	描述
尝试列表 例如，尝试 **1**	复选框： • **空**（默认） • **X**	您可以选择要删除的尝试。 每次尝试的值将显示如下：**MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX，“iSCSI 模式”：[%s1]，“Internet 协议”：[%s2]** **注：** • 具体值会有所不同，具体取决于尝试设置。 • **%s1** 是 **iSCSI** 模式的选项名称。 • **%s2** 是 **Internet** 协议的设置名称。
提交更改并退出	不适用	保存更改并退出。
放弃更改并退出	不适用	放弃更改并退出。

更改尝试顺序

表 31. 更改尝试顺序

项	选项	描述
更改尝试顺序	• 例如 • 尝试 **1**	此处列出了现有的尝试。 您可以使用 +/- 键更改尝试顺序。使用方向键选择尝试，然后按 +/-

表 31. 更改尝试顺序 （续）

项	选项	描述
	• 尝试 **2**	在尝试顺序列表中向上/向下移动尝试。
提交更改并退出	不适用	保存更改并退出。
放弃更改并退出	不适用	放弃更改并退出。

网络栈设置

在此菜单上，您可以配置系统在引导过程中与网络资源的交互方式，特别是对于基于网络的引导方法，如预引导执行环境（**PXE**）和 **HTTP** 引导。

表 32. 网络栈设置

项	选项	描述
网络栈	• **已启用**（默认） • 已禁用	启用或禁用 **UEFI** 网络栈。
IPv4 PXE 支持	• **已启用**（默认） • 已禁用	启用或禁用 **IPv4 PXE** 引导支持。 如果禁用了此项，则不会创建 **IPv4 PXE** 引导选项。
IPv4 HTTP 支持	• 已启用 • **已禁用**（默认）	启用或禁用 **IPv4 HTTP** 引导支持。 如果禁用了此项，则不会创建 **IPv4 HTTP** 引导选项。
IPv6 PXE 支持	• **已启用**（默认） • 已禁用	启用或禁用 **IPv6 PXE** 引导支持。 如果禁用了此项，则不会创建 **IPv6 PXE** 引导选项。
IPv6 HTTP 支持	• 已启用 • **已禁用**（默认）	启用或禁用 **IPv6 HTTP** 引导支持。 如果禁用了此项，则不会创建 **IPv6 HTTP** 引导选项。
PXE 引导等待时间	**0**	按 **Esc** 键中止 **PXE** 引导的等待时间（以秒为单位）。使用 **+/-** 或数字键设置该值。
介质检测计数	**1**	检查介质存在的次数。使用 **+/-** 或数字键设置该值。

HTTP 引导配置

在此菜单上，您可以设置使用 **HTTP** 协议进行网络引导。

注：

- 仅当启用了 **IPv4 HTTP 支持**或 **IPv6 HTTP 支持**时，才会显示 **HTTP 引导配置**菜单。要启用 **IPv4 HTTP** 支持或 **IPv6 HTTP** 支持，请转到**网络 → 网络栈设置**。
- 只有当系统中装有网络适配器时，才会显示子菜单。否则，**HTTP 引导配置**窗体中将不会显示任何内容。

表 33. HTTP 引导配置

项	选项	描述
系统中的 NIC 列表 例如，**MAC:XX:XX:XX:XX:XX:XX HTTP 引导配置**	不适用	配置 **HTTP** 引导参数。 （**MAC: XXXXXXXXXXXX**）

表 34. MAC:xxxxxxxxxxxx-HTTP 引导配置

项	选项	描述
输入描述	不适用	输入引导描述。
Internet 协议	• **IPv4** • **IPv6**	选择 **Internet** 协议版本。
引导 URI	不适用	将根据引导 **URI** 创建一个新引导选项。

Tls 认证配置

注：仅当启用了 **IPv4 HTTP 支持**或 **IPv6 HTTP 支持**时，才会显示 **Tls 认证配置**菜单。要启用 **IPv4 HTTP** 支持或 **IPv6 HTTP** 支持，请转到**网络 → 网络栈设置**。

表 35. Tls 认证配置

项	描述
第 33 页 “服务器 CA 配置”	您可以按 **Enter** 配置服务器证书颁发机构（**CA**）。
客户端证书配置	目前不支持客户端证书配置。

服务器 CA 配置

表 36. 服务器 CA 配置

项	描述
第 33 页 “注册证书”	您可以按 **Enter** 注册证书。
第 34 页 “删除证书”	您可以按 **Enter** 删除证书。

注册证书

表 37. 注册证书

项	描述
使用文件注册证书	使用证书文件注册证书。
证书 GUID	按以下格式输入证书 **GUID：11111111-2222-3333-4444-1234567890ab**。
提交更改并退出	保存更改并退出。
放弃更改并退出	放弃更改并退出。

删除证书

表 38. 删除证书

项	选项	描述
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	复选框： • **空** • **X**	证书 **GUID** 列表。您可以选中该复选框以删除证书。 **注**：如果没有安全证书文件，则不会显示证书 **GUID**。

电源

在此菜单上，您可以配置电源方案选项。

表 39. 电源

项	选项	描述
功耗/性能偏好	• **平台控制**（默认） • 操作系统控制 • **PECI** 控制	功耗/性能偏好决定了处理器进行电源管理和进入睿频模式的积极程度。并非所有操作系统都支持此功能。 • **[平台控制]**：由系统控制该设置。 • **[操作系统控制]**：由操作系统控制该设置。 • **[PECI 控制]**：此选项允许 **BMC** 控制能耗/性能偏好。 **注**：当**处理器 → CPU P-state 控制**设置为**自治**时，**[操作系统控制]** 选项不可用。
平台控制类型	• 高性能 • **均衡性能**（默认） • 均衡功耗 • 电源	控制处理器的电源控制单元（**PCU**）进行电源管理的积极程度，以及 **CPU** 核心如何进入睿频模式。 • **[高性能]**：允许以最积极的方式使用睿频模式。禁用电源管理功能，因而会增加功耗。 • **[功耗]**：禁用睿频模式并最大限度地利用电源管理功能。 • **[均衡性能]** 和 **[均衡功耗]** 是 **[高性能]** 和 **[功耗]** 之间的两个中间选项，前者更倾向于提高性能，后者更倾向于降低功耗。 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。

表 39. 电源 （续）

项	选项	描述
工作负载配置	• **均衡**（默认） • **I/O 敏感**	工作负载配置偏好用于调节系统的 I/O 带宽特性。此设置调节系统分配处理器核心和非核心频率以处理 I/O 请求的积极程度。 • **[均衡]**：均衡 CPU 核心和非核心频率，以便在 I/O 任务和应用程序工作负载线程之间提供均等的性能权重。 • **[I/O 敏感]**：对 CPU 核心与非核心频率进行权重分配，以在 CPU 核心利用率较低时，分配足够的资源以提供高 I/O 带宽。 **[I/O 敏感]** 推荐用于在处理器核心空闲时需要高带宽 I/O 的扩展卡，以便提供足够的频率来处理工作负载。
ASPM	• 自动 • **已禁用**（默认）	PCIe 主动状态电源管理（ASPM）是一项 PCIe 省电功能。当 PCIe 链路空闲时，它会将链路置于低功耗模式。 • **[自动]**：在支持 ASPM 的 PCIe 端点适配器上启用 ASPM。 • **[已禁用]**：禁用所有 PCIe 端点的 ASPM。
ACPI 固定电源按钮	• **已启用**（默认） • 已禁用	禁用该设置后，手动按下位于系统前面的电源按钮将不会执行操作系统的电源按钮策略，例如关机或关闭显示器。此外，“BMC 服务器（Web）电源操作”功能下的以下选项也会被禁用： • 正常关闭服务器电源 • 正常重新启动服务器

处理器

此菜单提供用于更改处理器设置的选项。

表 40. 处理器

项	选项	描述
第 45 页 “处理器详细信息”	不适用	已安装处理器的摘要
超线程	• **已启用**（默认） • 已禁用	启用超线程将允许在每个核心上运行多个逻辑处理器线程。 **注：** • 更改此设置需要执行“电源正常”重置才能生效。 • 此项不适用于 Intel Xeon 6 处理器（原代号为“Sierra Forest”）。

表 40. 处理器 （续）

项	选项	描述
睿频模式	• **已启用**（默认） • 已禁用	启用睿频模式可以在尚未完全利用所有 CPU 核心时提升整体 CPU 性能。当 CPU 核心处于睿频模式时，其可以在短时间内以高于其额定频率的速度运行。 **注：** • 如果处理器不支持此功能，则此项不可用。 • 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
节能睿频	• **已启用**（默认） • 已禁用	启用节能睿频后，将根据 CPU 利用率动态调整 CPU 的最佳睿频。**功耗/性能偏好**设置也会影响节能睿频。 **注：**选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
CPU P-state 控制	• 无 • **Legacy** • **自治**（默认） • 无 **Legacy** 协作 • 有 **Legacy** 协作	处理器活动电源管理状态（**P-state** 控制）会影响根据工作负载选择 CPU 运行频率的方式。 • **[自治]**：此模式是 **Intel** 硬件电源管理（**HWPM**）功能的一部分，为默认模式。在此模式下，所有 **CPU P-state** 管理都在后台自动处理，无需任何操作系统干预。自治模式用于正常的节能，适用于大多数典型的业务应用程序。 • **[Legacy]**：处理器 **P-state** 将呈现给操作系统，操作系统电源管理（**OSPM**）将直接控制选择哪个 **P-state**。**Legacy** 控制机制目前在搭载 **Intel Xeon** 可扩展处理器（代号 **Skylake**）之前的处理器的系统中实现。使用标准 **ACPI** 接口。通过操作系统级别频率控制受益的应用程序可使用此模式。 • **[无 Legacy 协作]**：**UEFI** 不提供 **Legacy P-state**。操作系统会向处理器的电源控制单元（**PCU**）提供所需的 **P-state** 的最小/最大级别的提示。**PCU** 在自治模式下运行，直到操作系统设置所需的频率。操作系统提供的提示会影响 **PCU** 选择的最终 **P-state**。 • **[有 Legacy 协作]**：**UEFI** 将保留最初启用的 **Legacy P-state** 接口，除非稍后有能识别 **Intel** 硬件 **P-state**（**HWP**）原生模式的操作系统来设置该位。在操作系统设置 **HWP** 原生模式之前，将使用 **Legacy P-state**。之后，**P-state** 将切换到与“无 **Legacy** 协作”相同的行为。 • **[无]**：不为 **P-state** 创建 **ACPI** 表条目。**P-state** 已被禁用。使用此设置可最大程度地减少 **P-state** 转换导致的延迟。建议用于对延迟敏感的工作负载。**CPU** 以额定频率运行，如果已启用睿频，则以睿频模式运行。

表 40. 处理器 （续）

项	选项	描述
		对于对时钟频率敏感的应用程序，建议使用协作模式或 **Legacy** 模式进行测试。 **注：**选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
C-state	• **Legacy**（默认） • 已禁用	**C-state** 可降低空闲期间的功耗。 选择 **[Legacy]** 后，操作系统将启动 **C-state** 转换。部分操作系统软件可能会破坏 **ACPI** 映射（例如 **intel_idle** 驱动程序）。 **注：**选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
封装 C-state	• **C0/C1** • **C2** • **C6NR**（默认） • 无限制	低功率 **C-state** 的退出延迟较高，高功率 **C-state** 的退出延迟较低。 **注：** • 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。 • 此项不适用于搭载 **Intel Xeon 6** 处理器（原代号为“**Granite Rapids**”）的 **8** 插槽平台。
C1 增强模式	• **已启用**（默认） • 已禁用	启用 **C1E**（**C1** 增强）状态可通过暂停处于空闲状态的 **CPU** 核心来节省电源。必须安装支持 **C1E** 状态的操作系统才能支持此功能。 **注：**选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。更改将在系统重新引导后生效。
非核心频率调节	• **已启用**（默认） • 已禁用	启用时，处理器会根据工作负载动态更改频率。**CPU** 封装内的所有杂项逻辑都被视为非核心。 **注：**选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
延迟优化模式	• **已禁用** • 已启用	启用/禁用延迟优化模式（性能）。 选择预设的工作负载 **profile** 时，低级设置不可更改。如果用户想要更改低级设置，请在“系统设置”子菜单下的“工作负载 **Profile**”中选择 **[**自定义**]**，然后根据需要更改单个设置。

表 40. 处理器 （续）

项	选项	描述
可信执行技术	• 已启用 • **已禁用**（默认）	启用或禁用 **Intel** 可信执行技术（**Intel TXT**）。 **Intel TXT** 是一组针对 **Intel** 处理器和芯片组的硬件扩展，提供启动测量和执行保护等安全功能，可增强数字办公平台的安全性。
Intel 虚拟化技术	• 已禁用 • **已启用**（默认）	启用或禁用 **Intel** 虚拟化技术。 **Intel** 虚拟化技术可使硬件抽象化，从而支持多个工作负载共用一组公共资源。 **注**：选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
硬件预取器	• **已启用**（默认） • 已禁用	启用后，硬件预取器会将数据从主系统内存预取到二级高速缓存，从而加速数据事务，提升内存性能。 对于轻线程应用程序和部分基准测试，启用硬件预取器会带来一定的优势。
相邻缓存预取	• **已启用**（默认） • 已禁用	相邻缓存行预取器会自动将相邻缓存行提取到程序正在访问的缓存行。在处理器需要时，下一缓存行立即可用，从而减少缓存延迟。 对于轻线程应用程序和部分基准测试，启用相邻缓存行预取器会带来一定的优势。
DCU 流预取器	• **已启用**（默认） • 已禁用	数据缓存单元（**DCU**）流预取器会在特定时间段内检测对单个缓存行的多次读取，并选择将后续缓存行加载到 **L1** 数据缓存中。 对于轻线程应用程序和部分基准测试，启用 **DCU** 流预取器会带来一定的优势。
DCU IP 预取器	• **已启用**（默认） • 已禁用	**DCU IP** 预取器通过查找顺序加载历史记录来确定是否将后续数据预取到 **L1** 缓存。 对于大多数环境，都建议启用 **DCU IP** 预取器。但是，对于 **Java** 等环境，禁用该预取器会带来一定的优势。
L1 下一页预取器	• **已启用**（默认） • 已禁用	下一页预取器是一种 **L1** 数据缓存页预取器（**MSR 1A4h [4]**），它会检测可能跨越页边界的访问并提前启动访问。 **注**：此项仅适用于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”）。

表 40. 处理器 （续）

项	选项	描述
AMP 预取	• **已启用**（默认） • 已禁用	此选项可启用其中一个中级缓存（MLC）AMP 硬件预取器。 对于部分基准测试，启用 MLC 预取会带来一定的优势。 **注**：此项仅适用于： • Intel Xeon 6 处理器（原代号为“Granite Rapids”） • Intel Xeon D 处理器（原代号为“Granite Rapids-D”）
LLC 预取	• **已禁用**（默认） • 已启用	末级缓存（LLC）预取器是在现有的预取机制之上的一种额外预取机制，这些现有预取器会将数据预取到核心 DCU 和 MLC 中。 启用 LLC 预取可使核心预取器能够将数据直接预取到 LLC 中，而不必先填充到 MLC 中 **注**：此项仅适用于： • Intel Xeon 6 处理器（原代号为“Granite Rapids”） • Intel Xeon D 处理器（原代号为“Granite Rapids-D”）
无主预取	• 已启用 • 已禁用 • **自动**（默认）	当 L1 缓存资源不足时，允许对 MLC 进行预先提取。根据 CPU 类型自动映射到硬件默认设置。 **注**：此项仅适用于： • Intel Xeon 6 处理器（原代号为“Granite Rapids”） • Intel Xeon D 处理器（原代号为“Granite Rapids-D”）
UPI 链路禁用	• **已启用所有链路**（默认） • 已启用的最小链路数	将 QPI/UPI 连接限制为最小数量可以节省电力。如果需要最大性能，则应将所有 QPI 链路保持为启用状态。 **注**：此项仅在安装 1 个以上 CPU 时可见。
SNC	• 已启用 • **已禁用**（默认）	子 NUMA 集群（SNC）将核心和末级缓存（LLC）划分为多个集群，每个集群绑定到系统中的一组内存控制器，从而将每个 CPU 封装划分为多个 NUMA 节点。这可以改善末级缓存的平均延迟。 **注**：此项适用于以下处理器： • Intel Xeon 6 处理器（原代号为“Sierra Forest”）：ZCC SKU • Intel Xeon 6 处理器（原代号为“Granite Rapids”）

表 40. 处理器 （续）

项	选项	描述
UPI 亲和性	• 已启用 • **已禁用**（默认）	**UPI** 亲和性可以优化 **CPU** 核心和 **UPI** 链路之间的亲和性，帮助最大限度地减少跨 **CPU** 内存访问延迟。 **注**：仅当安装了多个 **CPU** 时，此项才可见且可正常使用，同时 **CPU** 类型应为 **GraniteRapids XCC** 或 **GraniteRapids UCC**。
虚拟 Numa	• 已启用 • **已禁用**（默认）	在 **ACPI** 表中将物理 **NUMA** 节点分成大小均匀的虚拟 **NUMA** 节点。这可能会提高具有 **64** 个以上逻辑处理器的 **CPU** 上的 **Windows** 性能。
虚拟 Numa 节点数	**0**	按物理 **NUMA** 节点的虚拟 **NUMA** 节点数。**0** 表示根据系统配置自动设置虚拟 **NUMA** 节点的数量。**1** 等于禁用虚拟 **NUMA**。 **注**：如果已禁用虚拟 **Numa**，则此项将隐藏。
目录模式启用	• 已启用 • 已禁用 • **自动**（默认）	启用后，系统将使用机会侦听广播（**OSB**）、**HitME** 缓存和 **I/O** 目录缓存（**IODC**）等附加功能来减少目录读取的开销。禁用后，所有内存访问都将需要侦听。对于大多数工作负载，都不建议侦听所有内存访问。 **注**：选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
XPT 预取器	• **已启用**（默认） • 已禁用	扩展预测表（**XPT**）预取器是一种从核心进行内存预取的机制，它允许发送到末级缓存的读取请求推测性地向内存控制器预取发出该读取的副本。该机制旨在减少本地内存访问的延迟。
UPI 预取器	• **已启用**（默认） • 已禁用	超级通道互联（**UPI**）预取功能能够在内存总线上提前进行内存读取。**UPI** 接收路径会向内存控制器预取器发起内存读取。 **注**：此项仅在安装 **1** 个以上 **CPU** 时可见。
D2U	• 已启用 • 已禁用 • **自动**（默认）	远程读取事务的延迟节省功能。禁用 **D2U** 时，高度依赖远程空闲延迟的工作负载可能会受到影响。 **注**：仅当装有两个或更多处理器时，此项才可用。
IODC	• 已禁用 • **自动**（默认） • 为远程 **InvItoM** 混合推送启用 • 为远程 **InvItoM AllocFlow** 启用 • 为远程 **InvItoM** 混合 **AllocNonAlloc** 启用	启用 **I/O** 目录缓存（**IODC**）后，基于目录的写入开销会减少。禁用时，不会抑制不可缓存的写入事务的目录读取/更新。 **注**：仅当装有两个或更多处理器时，此项才可用。

表 40. 处理器 （续）

项	选项	描述
	• 为远程 **InvItoM** 和远程 **WCiLF** 启用	
Loctorem 阈值正常	• 已禁用 • **自动**（默认） • 低 • 中 • 高	**BIOS** 选项提供了一组阈值，可以控制各类请求在请求表（**TOR**）中所占的比例，从而帮助避免本地请求与远程请求之间的不均衡。此 **BIOS** 选项控制当管道中没有远程请求（**EMPTY**）以及管道中存在远程请求（**NORMAL**）时，允许在管道中进行的本地到远程（**Loctorem**）请求的数量。 **自动**为默认值，由 **Si** 兼容性控制。
Loctorem 阈值为空	• 已禁用 • **自动**（默认） • 低 • 中 • 高	**BIOS** 选项提供了一组阈值，可以控制各类请求在请求表（**TOR**）中所占的比例，从而帮助避免本地请求与远程请求之间的不均衡。此 **BIOS** 选项控制当管道中没有远程请求（**EMPTY**）以及管道中存在远程请求（**NORMAL**）时，允许在管道中进行的本地到远程（**Loctorem**）请求的数量。 **自动**为默认值，由 **Si** 兼容性控制。
总内存加密	• **已禁用**（默认） • 已启用	**Intel** 总内存加密（**TME**）使用单个加密密钥对系统的整个物理内存进行加密。
多密钥总内存加密	• **已禁用**（默认） • 已启用	**Intel** 多密钥总内存加密（**MK-TME**）技术构建在 **Intel TME** 基础之上。它支持使用多个加密密钥，允许使用处理器页表为每个内存页选择一个加密密钥。 **注：**仅当**总内存加密**设置为 **[**已启用**]** 时，此项才可用。
内存完整性	• **已禁用**（默认） • 已启用	启用或禁用内存完整性。内存完整性是核心隔离的一项功能。 **注：**仅当**总内存加密**设置为 **[**已启用**]** 时，此项才可用。
最大 MKTME 密钥数量	动态值	**TME-MT** 可以使用的密钥总数。 **注：**仅当**总内存加密**设置为 **[**已启用**]** 时，此项才可用。
信任域扩展（TDX）	• **已禁用**（默认） • 已启用	启用或禁用信任域扩展（**TDX**）。
TDX 安全仲裁模式加载器（SEAM 加载器）	• **已禁用**（默认） • 已启用	启用或禁用 **TDX** 安全仲裁模式加载器（**SEAM** 加载器）。 **注：**如果已禁用 **TDX**，此项将灰显。
TME-MT/TDX 密钥拆分	• **0x1**（默认） 该值的范围为 **1** 到 **N**，其中 **N** 取决于系统配置。	指定用于 **TDX** 的位数。其余部分将由 **TME-MT** 使用。 **注：**如果已禁用 **TDX**，此项将不可用。

表 40. 处理器 （续）

项	选项	描述
TME-MT 密钥数量	动态值，具体取决于 **TME-MT/TDX 密钥拆分**的值	指定用于 **TME-MT** 的密钥数量 **注**：如果已禁用 **TDX**，此项将不可用。
TDX 密钥数量	值 = 最大 **MKTME** 密钥数量 - **TME-MT** 密钥数量	指定用于 **TDX** 的密钥数量 **注**：如果已禁用 **TDX**，此项将不可用。
SW Guard Extensions	• **已禁用**（默认） • 已启用	启用或禁用 **Software Guard Extensions（SGX）**。 **注**：仅当系统支持总内存加密（**TME**）并已启用 **TME** 时，此项才可用。此外，在启用 **SGX** 之前，请禁用“轮巡检查”和“镜像模式”。否则，**SGX** 功能可能会无法正常使用。
SGX 恢复出厂设置	• **已禁用**（默认） • 已启用	启用或禁用“**SGX** 恢复出厂设置”。 选择 [已启用] 后，它会在后续引导时擦除所有注册数据，并在启用了 **SGX** 时额外强制执行初始平台建立流程。 **注**：仅当系统支持总内存加密（**TME**）并已启用 **TME** 时，此项才可用。此外，在启用 **SGX** 之前，请禁用“轮巡检查”和“镜像模式”。否则，**SGX** 功能可能会无法正常使用。
SGX 封装信息带内访问	• **已禁用**（默认） • 已启用	启用或禁用“**Software Guard Extensions（SGX）** 封装信息带内访问”。 **注**：仅当系统支持总内存加密（**TME**）并已启用 **TME** 时，此项才可用。此外，在启用 **SGX** 之前，请禁用“轮巡检查”和“镜像模式”。否则，**SGX** 功能可能会无法正常使用。
SGX PRM 大小	• **1 G**（默认） • **2 G** • **4 G** • **8 G** **注**：默认值和选项会根据系统配置动态变化。	“**SGX PRM** 大小”只是其中一部分，可能不等于总 **PRM** 大小。 **注**：如果禁用了“**SW Guard Extensions**”，此项将灰显。

表 40. 处理器 （续）

项	选项	描述
Intel Speed Select	• 基础 • **自动** • **Config1** • **Config2** • **Config3** • **Config4** • **SST-PP V2** **注**：根据 CPU 配置，[基础]、[Config1]、[Config2]、[Config3] 、 [Config4] 和 [SST-PP V2] 可能不会显示或隐藏。	**Intel Speed Select Technology**（SST）可以在 **UEFI** 中启用的 **CPU** 核心数量减少的情况下提高 **CPU** 额定频率。一般而言，借助 **SST** 可以实现有保障的 **CPU** 睿频。 如果安装的处理器不支持 **SST**，则无论选择何种设置，都将使用 [基础] 选项。 • **[基础]**：实际禁用 **SST**。 • **[自动]**：根据 **UEFI** 中已启用的 **CPU** 核数自动控制 **SST** 启用级别。 • **[Config1]/[Config2]/[Config3]/[Config4]**：根据所选择的配置选项强制启用 **SST** 核心限制。注：**[Config1]/[Config2]/[Config3]/[Config4]** 可能会覆盖 **UEFI** 中启用 **CPU** 核心数的选项。 • **[SST-PP V2]** 启用动态 **SST-PP** 模式。选择 **SST-PP V2** 后，该模式可以在 **Linux** 操作系统中实现运行时动态更改。 **注**：如果 **CPU** 不支持动态 **SST-PP**，或者“**CPU P** 状态控制”不是“无 **Legacy** 协作”或“有 **Legacy** 协作”，则“**SST-PP V2**”不可用。
SST-BF	• 已启用 • **已禁用**（默认）	此选项允许启用 **SST-BF**，并允许 **BIOS** 配置 **SST-BF** 高优先级核心，无需再通过软件进行配置。 **注**：如果 **CPU** 不支持 **SST-BF**，或 **CPU P-state 控制**未设置为 **[无 Legacy 协作]**，此项将不可用。
PECI 受信任	• 已禁用 • **已启用**（默认）	启用或禁用对系统的平台环境控制接口（**PECI**）的信任。 如果需要更高级别的安全性，可以选择 **[已禁用]**，但某些功能（如内存和 **I/O** 利用率报告）可能无法正常使用。
CPU 封装中的核心数量	• **所有**（默认） 基于 **CPU** 架构的所有可用核心数量列表	选择在每个 **CPU** 封装中启用的核心数量。 **注**：可用核心数量取决于 **CPU** 架构。 • 对于 **Intel Xeon 6** 处理器（原代号为“**Sierra Forest**”），可用选项是 **2** 或 **4** 的整数倍，具体取决于 **CPU** 内部封装。 • 对于 **Intel Xeon 6** 处理器（原代号为“**Granite Rapids**”），最小核心数量取决于 **CPU** 计算芯片的数量。
CPU PCIe 宽松排序	• 已启用 • **已禁用**（默认）	启用 **CPU PCIe** 松散排序将始终允许下游完成传递已发布的写入。
启用 OSB	• 已启用 • 已禁用 • **自动**（默认）	机会侦听广播（**OSB**）功能会尝试通过侦听本地（主）代理和远程套接字对端来避免内存读取延迟。 **自动**为默认值，由 **Si** 兼容性控制。

表 40. 处理器 （续）

项	选项	描述
A 到 S 状态转换	• 已启用 • 已禁用 • **自动**（默认）	**A 到 S 状态转换**控制缓存行在侦听未命中时是否应从 **A**（**snoopAll**）状态转换为 **S**（共享）状态。
LLC 失效行分配	• **已启用** （默认） • 已禁用 • 自动	• [已启用]：**LLC** 会利用可用空间适时将失效行填充到 **LLC** 中。 • [已禁用]：失效行将始终被丢弃，不会填充到 **LLC** 中。
UPI 链路频率	• 最低功耗 • 均衡 • **最高性能**（默认）	选择所需的 **UPI** 链路频率。 • [最高性能]：最大限度地提高性能。 • [均衡]：在性能和功耗之间实现平衡。 • [最低功耗]：最大限度地节省电源。 **注**：此项仅在安装 **1** 个以上 **CPU** 时可见。
第 46 页 “CPU 频率限制”	• **全速睿频提升**（默认） • 限制最大频率	最大频率（睿频、**AVX** 和非睿频）可以限制为所安装 **CPU** 的最大睿频和 **1.2 GHz** 之间的频率。这对于同步 **CPU** 任务非常有用。 注意，**N+1** 核的最大频率不能高于 **N** 核。如果输入了不支持的频率，则该频率将自动限制为支持的值。如果通过应用程序软件控制 **CPU** 频率限制，请将此菜单项保留为默认设置（[全速睿频提升]）。 **注**： • 此选项仅在启用 “睿频模式” 时可用。 • 在以下情况下，此项将隐藏：**CPU** 为 **SRF** 或 **CWF**。
火箭模式	• 已启用 • **已禁用**（默认）	选择 [已启用] 后，“火箭模式” 允许核心立即跳至最大睿频，而不是按照平滑曲线提升。 启用 “火箭模式” 后，仅当 **P-state** 设置为 [自治] 时才会生效。
C0 休止时间	**0**	控制在 **C0** 子状态下允许休止的最长时间，并控制是否支持 **C0.2**。
第 45 页 “UPI 电源管理”	不适用	为 **CPU UPI** 接口选择所需的电源管理级别。与 **[L0p]** 或 [已禁用] 相比，**[L1]** 节省的电力最多，但延迟更长。 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。

处理器详细信息

表 41. 处理器详细信息

项	格式	描述
处理器插槽	• 插槽 **1** • 插槽 **n**	处理器插槽表
处理器 ID	**ASCII** 字符串	处理器 **ID** 标记
处理器频率	**ASCII** 字符串	处理器频率值
处理器修订版	**ASCII** 字符串	微码修订版本的值
L1 高速缓存 RAM	**ASCII** 字符串	**L1** 高速缓存 **RAM** 的大小
L2 高速缓存 RAM	**ASCII** 字符串	**L2** 高速缓存 **RAM** 的大小
L3 高速缓存 RAM	**ASCII** 字符串	**L3** 高速缓存 **RAM** 的大小
每个插槽的核心数（支持/已启用）	**ASCII** 字符串	每个处理器插槽支持和已启用的处理器核心数
每个插槽的线程数（支持/已启用）	**ASCII** 字符串	每个处理器插槽支持和已启用的处理器线程数
处理器 1 版本	**ASCII** 字符串	处理器 **1** 的版本
处理器 n 版本	**ASCII** 字符串	处理器 **n** 的版本

UPI 电源管理

表 42. UPI 电源管理

项	选项	描述
L1	• **已启用**（默认） • 已禁用	为 **CPU UPI** 接口选择所需的电源管理级别。与 **[L0p]** 或 **[已禁用]** 相比，**[L1]** 节省的电力最多，但延迟更长。 **注：** • 仅当装有两个或更多处理器时，**UPI** 功能才有效。 • 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设置 → 工作负载概要文件 → 自定义**。然后，您便可更改此设置。
L0p	• **已启用**（默认） • 已禁用	为 **CPU UPI** 接口选择所需的电源管理级别。与 **[L0p]** 或 **[已禁用]** 相比，**[L1]** 节省的电力最多，但延迟更长。 **注：** • 仅当装有两个或更多处理器时，**UPI** 功能才有效。 • 选择预设工作负载 **profile** 时，低级别设置不可更改并将灰显。要更改此设置，请先选择**系统设**

表 42. UPI 电源管理 （续）

项	选项	描述
		置 → 工作负载概要文件 → 自定义。然后，您便可更改此设置。

CPU 频率限制

表 43. CPU 频率限制

项	选项	描述
CPU 频率限制		
处理器 X 到 X 核心处于活动状态 **注**：此项为动态文本，具体取决于当前处理器状态。 将“**CPU 频率限制**”设置为“限制最大频率”时，此子菜单将显示。 如果 **CPU** 为 **SRF** 或 **CWF**，则此项将隐藏。	• **最大睿频档位** • 最大睿频减 **1** 档 • 最大睿频减 **2** 档 • **...** • 基础频率加 **1** 档	最大频率（睿频、**AVX** 和非睿频）可以限制为所安装 **CPU** 的最大睿频和 **1.2 GHz** 之间的频率。这对于同步 **CPU** 任务非常有用。 **N+1** 核的最大频率不能高于 **N** 核的最大频率。如果输入了不支持的频率，则该频率将自动限制为支持的值。如果通过应用程序软件控制 **CPU** 频率限制，请将此菜单项保留为默认设置（[全速睿频提升]）。

恢复和 RAS

在此菜单上，您可以配置恢复策略以及高级可靠性、可用性和可维护性设置。

表 44. 恢复和 RAS

项	描述
第 46 页 “POST 尝试”	配置在调用恢复机制之前尝试 **POST** 的次数。
第 47 页 “高级 RAS”	选择是否启用各种高级 **RAS** 选项。
第 47 页 “磁盘 GPT 恢复”	配置磁盘 **GUID** 分区表（**GPT**）恢复选项。
第 47 页 “系统恢复”	配置系统恢复设置。

POST 尝试

表 45. POST 尝试

项	选项	描述
POST 尝试限制	• 已禁用 • **9** • **6** • **3** （默认）	配置在调用恢复机制之前尝试 **POST** 的次数。 当连续失败 **POST** 尝试次数达到此限制时，系统将以出厂默认设置重新引导。

高级 RAS

表 46. 高级 RAS

项	选项	描述
机器检测恢复	• **已启用**（默认） • 已禁用	启用后，将使软件层（操作系统、VMM、DBMS、应用程序）能够帮助系统从硬件不可纠正的错误中恢复
PCI 错误恢复	• **已启用**（默认） • 已禁用	启用此项后，允许系统从不可纠正的 PCIe 故障中恢复。发生故障的 PCIe 设备将被禁用以便遏制错误，并会通知操作系统重新扫描 PCIe 总线。 禁用此项后，不可纠正的 PCIe 故障将导致 NMI。
出现致命错误时重置 PCIe 端点	• **已禁用**（默认） • 已启用	启用时，系统会在发生致命错误时重置 PCIe 端点。

磁盘 GPT 恢复

表 47. 磁盘 GPT 恢复

项	选项	描述
磁盘 GPT 恢复	• 自动 • 手动 • **无**（默认）	• [自动]：系统 UEFI 将自动修复损坏的 GUID 分区表（GPT）。 • [手动]：系统 UEFI 只会根据用户输入修复损坏的 GPT。 • [无]：系统 UEFI 不会修复损坏的 GPT。可以从系统事件日志中检索恢复结果。

系统恢复

表 48. 系统恢复

项	选项	描述
POST 看守程序计时器	• 已启用 • **已禁用**（默认）	启用或禁用 POST 看守程序计时器。
POST 看守程序计时器值	[5]	在指定范围（5-20 分钟）内输入 POST 看守程序计时器值。
在 NMI 期间重新引导系统	• **已启用**（默认） • 已禁用	指定是否在不可屏蔽中断（NMI）期间重新引导系统。

安全性

在此菜单上，您可以配置系统安全设置。

表 49. 安全性

项	描述
第 48 页 “安全引导配置”	配置安全引导选项。
第 51 页 “可信平台模块”	配置 TPM 设置选项。

安全引导配置

注：如果有新的密钥更新，您必须在更新 **UEFI** 固件后手动加载“出厂策略”。（例如，**UEFI** 更新只会将新的证书添加到 **dbDefault** 而非 **db**，因此用户必须将所有密钥重置为默认的“出厂策略”才能将 **dbDefault** 复制到 **db**。）

表 50. 安全引导配置

项	选项	描述
安全引导状态	• 已禁用 • 已启用	显示当前安全引导状态。
安全引导模式	• 用户模式 • 设置模式	当此项设置为 [用户模式] 且启用了安全引导时，系统将执行安全引导认证。
安全引导设置	• 已启用 • **已禁用**（默认）	启用或禁用安全引导。模式更改需要重新引导系统。 仅当启用了安全引导、注册了平台密钥（**PK**）且系统处于 [用户模式]（**安全引导模式**）时，安全引导功能才可用。
安全引导策略	• **出厂策略**（默认） • 自定义策略 • 删除所有密钥 • 删除 **PK**	安全引导策略选项： • [出厂策略]：重新引导后将使用出厂默认密钥。选择此选项后，将删除自定义密钥。 • [自定义策略]：重启后将使用自定义密钥。选择此选项后，您可以进入**安全引导自定义策略**页面进行密钥自定义，例如添加/删除特定密钥或注册 **UEFI** 映像。 • [删除所有密钥]：重启后将删除平台密钥（**PK**）、密钥交换密钥（**KEK**）、授权签名数据库（**DB**）和禁用签名数据库（**DBX**）。删除所有密钥后，**安全引导模式**将为 [设置模式]，**安全引导策略**将为 [自定义策略]。 • [删除 **PK**]：重启后将删除 **PK**。删除 **PK** 后，**安全引导模式**将为 [设置模式]，**安全引导策略**将为 [自定义策略]。 • [将所有密钥重置为默认值]：重新引导后，所有密钥都将设置为出厂默认密钥，“安全引导策略”将设置为 [出厂策略]。 **注：**这些选项无法在 **UEFI Setup Utility** 中加载为默认值。
第 49 页 “查看安全引导密钥”	不适用	查看 **PK**、**KEK**、**DB** 和 **DBX** 的详细信息。
第 49 页 “安全引导自定义策略”	不适用	自定义 **PK**、**KEK**、**DB** 和 **DBX**。 **注：**仅当**安全引导策略**设置为 [自定义策略] 时，才能配置此菜单。

查看安全引导密钥

表 51. 查看安全引导密钥

项	描述
安全引导变量	表头，列出了平台密钥（PK）、密钥交换密钥（KEK）、授权签名数据库（DB）和禁用签名数据库（DBX）。
大小	表头，显示密钥字节数。
密钥	表头，显示证书数量。
密钥来源	表头，显示证书来源。来源可以是**出厂默认密钥**、**无密钥**或**自定义密钥**。
PK	查看 **PK** 中的证书。 **注：**系统中只有一个 **PK**。
KEK	查看 **KEK** 中的所有证书。
DB	查看 **DB** 中的所有证书。
DBX	查看 **DBX** 中的所有证书。

安全引导自定义策略

表 52. 安全引导自定义策略

项	描述
第 49 页 “PK 选项”	注册自定义 **PK** 或删除现有 **PK**。 **注：**系统中只有一个 **PK**。如果需要插入自定义 **PK**，请先删除原始 **PK**。删除 **PK** 后，将禁用安全引导。
第 50 页 “KEK 选项”	注册 **KEK** 条目或从 **KEK** 列表中删除现有条目。
第 50 页 “DB 选项”	注册 **DB** 条目或从 **DB** 列表中删除现有条目。
第 50 页 “DBX 选项”	注册 **DBX** 条目或从 **DBX** 列表中删除现有条目。

PK 选项

表 53. PK 选项

项	描述
注册 PK	注册自定义 **PK**。 **注：**系统中只有一个 **PK**。如果需要插入自定义 **PK**，请先删除原始 **PK**。删除 **PK** 后，将禁用安全引导。
删除 PK	删除现有的 **PK**。 **注：**系统中只有一个 **PK**。如果需要插入自定义 **PK**，请先删除原始 **PK**。删除 **PK** 后，将禁用安全引导。
使用文件注册 PK	使用外部 **USB** 或存储设备从文件注册自定义 **PK**。
提交更改并退出	提交更改并退出。
放弃更改并退出	放弃更改并退出。

KEK 选项

表 54. KEK 选项

项	描述
注册 KEK	注册 **KEK**。
删除 KEK	从 **KEK** 列表中删除现有的 **KEK**。
使用文件注册 KEK	使用外部 **USB** 或存储设备从文件注册 **KEK**。
提交更改并退出	提交更改并退出。
放弃更改并退出	放弃更改并退出。

DB 选项

表 55. DB 选项

项	描述
注册签名	注册签名条目。
删除签名	从 **KEK** 列表中删除签名条目。
使用文件注册签名	使用外部 **USB** 或存储设备从文件注册签名。
提交更改并退出	提交更改并退出。
放弃更改并退出	放弃更改并退出。

DBX 选项

表 56. DBX 选项

项	选项	描述
注册签名	不适用	注册签名条目。
删除签名	不适用	从 **KEK** 列表中删除签名条目。
使用文件注册签名	不适用	使用外部 **USB** 或存储设备从文件注册签名。
签名 GUID		
签名格式	• **X509 CERT SHA256** • **X509 CERT SHA384** • **X509 CERT SHA512** • **X509 CERT**	注册了不同的 **X509 DER-Cert**。选择一个选项以将其注册到 **DBX** 列表中。
始终吊销	复选框	指示是否始终吊销证书。
提交更改并退出	不适用	提交更改并退出。
放弃更改并退出	不适用	放弃更改并退出。

删除签名数据表

项	描述
删除所有签名数据	删除所有签名数据，无论勾选了多少签名数据。 **注：** *选择此子菜单时，将弹出以下消息。* ***按“Y”删除签名列表。*** ***按其他键取消并退出。***
签名日期，条目 x [] ***示例:*** ***签名数据，条目 1*** ***签名数据，条目 2*** ***签名数据，条目 3***	所有者 **GUID:** **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** **SHA256（32 位）:** **yyyyyyyyyyyyyyyyyyyyyy** **注：** ***x – 显示 GUID*** ***y – 显示签名的内容。***

删除签名列表表格

项	描述
删除所有签名列表	删除所有签名列表 **注：** *选择此子菜单时，将弹出以下消息。* ***按“Y”删除签名列表。*** ***按其他键取消并退出。***
签名列表，条目 1	列表类型: **xxxxx** 条目编号: **yyy** 注: **xxxxxx**–显示列表类型 例如， **SHA256**、**SHA384** 或 **SHA512** 等。 **yyy**–显示签名数据计数

可信平台模块

可信平台模块（**TPM**）是一种基于硬件的安全组件，用于为加密密钥、数字证书和其他用于验证系统身份的敏感数据提供安全存储。

表 57. 可信平台模块

项	选项	描述
第 52 页 “TPM 2.0”	不适用	配置 **TPM 2.0** 设置选项。

可信平台模块（TPM 2.0）

表 58. 可信平台模块（TPM 2.0）

项	选项	描述
TPM 状态		
TPM 供应商	不适用	**TPM** 设备的供应商信息
TPM 固件版本	不适用	**TPM** 设备的当前固件版本
TPM 设置		
TPM2 操作	• **无操作**（默认） • 清除	可以选择 [清除] 以清除 **TPM** 数据。 **注意**：这将擦除 **TPM** 的内容。需要重新引导系统。
TPM 设备	• **已启用**（默认） • 已禁用	如果禁用 **TPM** 设备，则 **TPM** 设备对象将不会出现在操作系统中。

存储

该设备列表基于您的系统配置和系统设置。此页面的内容由存储供应商的 **HII** 实用程序动态生成。

表 59. 存储

项	描述
第 52 页 “NVMe”	列出 **NVMe** 设备。

NVMe

表 60. NVMe

项	描述
插槽 X：NVMe Bus-Dev-Fun 例如 **NVMe 64-0-0**	此字符串由平台定义。各个平台显示的字符串可能会不同。 “**X**”是插槽编号。“**Bus-Dev-Fun**”是 **PCI** 地址值。

NVMe 详细信息

表 61. NVMe 详细信息

项	格式	描述
型号名称	**ASCII** 字符串	**NVMe** 设备的型号名称
序列号	**ASCII** 字符串	**NVMe** 设备的序列号
固件修订版	**ASCII** 字符串	**NVMe** 设备的固件修订版

表 61. NVMe 详细信息 （续）

项	格式	描述
供应商 ID	**0xXXXX** （**XXX** 为十六进制数）	**NVMe** 设备的供应商 **ID**
Device ID	**0xXXXX** （**XXX** 为十六进制数）	**NVMe** 设备的设备 **ID**
子系统供应商 ID	**0xXXXX** （**XXX** 为十六进制数）	**NVMe** 设备的子系统供应商 **ID**
子系统 ID	**0xXXXX** （**XXX** 为十六进制数）	**NVMe** 设备的子系统 **ID**
最大链路速度	**Gen N** （**N** 为数字）	最大链路速度
最大链路宽度	**xN** （**N** 为数字）	最大链路宽度
协商链路速度	**Gen N** （**N** 为数字）	协商链路速度
协商链路宽度	**xN** （**N** 为数字）	协商链路宽度
命名空间数量	**N** （**N** 为数字）	命名空间数量
总大小	**X.XX TB** （单位可以是 **GB** 或 **MB**，具体取决于大小）	总大小
设备驱动程序数据链路		
设备 HII 标题	不适用	设备 **HII** 的描述 标题和描述由已安装的存储供应商 **HII** 实用程序生成。如果设备未提供 **HII** 数据，则将显示“不适用”。

日期和时间

在此菜单上，您可以设置系统的本地日期和时间。

表 62. 日期和时间

项	格式	描述
系统日期	**YYYY/MM/DD**	您可以使用 +/- 键或数字键以月、日和年（**2000-2099**）的格式设置日期。 日期在设置后即可保存。
系统时间	**HH:MM:SS**	您可以使用 +/- 键或数字键以时、分、秒的格式设置时间。 使用 **24** 小时格式输入小时，例如，**15:00** 表示下午 **3** 点。

启动选项

以下是默认引导顺序设置的摘要。如果系统的引导顺序不同，内容将会有所不同。

表 63. 启动选项

项	描述
DVD ROM	设备路径：**VenHw(61A3F2B1-3611-43BD-BF73-74472A2DEFFB,01000000)**
硬盘	设备路径：**VenHw(61A3F2B1-3611-43BD-BF73-74472A2DEFFB,02000000)**
网络	设备路径：**VenHw(61A3F2B1-3611-43BD-BF73-74472A2DEFFB,03000000)**
USB 存储	设备路径：**VenHw(61A3F2B1-3611-43BD-BF73-74472A2DEFFB,04000000)**

引导管理器

在此菜单上，您可以管理各种引导设置，包括引导顺序、选项、模式和系统重新引导功能。

表 64. 引导管理器

项	选项	描述
引导顺序		
第 55 页 “添加 UEFI 完整路径引导选项”	不适用	添加一个 **UEFI** 应用程序或一个可移动文件系统作为引导选项。
第 55 页 “引导选项维护”	不适用	更改引导顺序、选择引导选项或删除引导选项。
第 56 页 “设置引导优先顺序”	不适用	设置设备组中设备的引导优先级。
其他引导功能		
第 56 页 “从文件引导”	**Xxxx {xxxx-xxx-xxx…}**	从特定文件或设备引导系统。
第 56 页 “选择下一次引导的一次性引导选项”	不适用	为下一次引导选择一次性引导选项。

表 64. 引导管理器 （续）

项	选项	描述
系统		
第 56 页 “引导模式”	不适用	更改引导设置。
第 58 页 “重新引导系统”	不适用	重新引导系统。 如果按 <Y>，则所有设置更改都会丢失，并且系统将重新引导。

添加 UEFI 完整路径引导选项

表 65. 添加 UEFI 完整路径引导选项

项	选项	描述
引导选项文件路径	不适用	指定新创建的引导选项的文件路径
输入描述	不适用	指定新建引导选项的名称
选择设备路径选项	**Xxxx {xxxx-xxx-xxx…}**	从可用的文件系统中选择一个进行引导。
提交更改并退出	不适用	保存更改并退出。

引导选项维护

表 66. 引导选项维护

项	选项	描述
引导顺序	不适用	您可以使用数字键盘上的 +/- 键来更改引导顺序。
选择引导选项		
引导选项列表 例如 • **DVD ROM** • 硬盘 • 网络 • **USB** 存储 引导选项列表因平台而异。	复选框： • 空 • **X**（默认）	您可以通过选中复选框来选择引导选项。 选择引导选项后，此选项将被添加到引导顺序中。如果清除复选框，相应引导选项将从引导顺序中删除。
删除引导选项		
• **Shell** 引导选项列表因平台而异。	复选框： • **空**（默认） • **X**	您可以通过选中复选框来删除引导选项。

设置引导优先顺序

表 67. 设置引导优先顺序

项	描述
DVD ROM 优先顺序	如果系统中存在多个 **DVD ROM** 设备，请设置 **DVD ROM** 设备组的引导优先顺序。
硬盘优先顺序	如果系统中存在多个硬盘，请设置硬盘组的引导优先顺序。
网络优先顺序	如果系统中存在多个网络设备，请设置网络设备组的引导优先顺序。
USB 优先顺序	如果系统中存在多个 **USB** 设备，请设置 **USB** 设备组的引导优先顺序。

从文件引导

使用此菜单可从特定文件或设备引导系统。系统将显示消息框以指导您完成整个过程。

选择下一次引导的一次性引导选项

使用此菜单为下一次引导选择一次性引导选项。

表 68. 选择下一次引导的一次性引导选项

项	选项	描述
选择下一次引导的一次性引导选项	• 系统设置 • **DVD ROM** • 硬盘 • 网络 • **USB** 存储 • **无**（默认） **注：** 此选项列表包含当前引导顺序列表、[系统设置] 和 [无] 中的引导选项。如果系统具有不同的引导顺序，则选项会有所不同。	为下一次引导选择一次性引导选项。

引导模式

表 69. 引导模式

项	选项	描述
系统引导模式	• **UEFI 模式**（默认）	引导管理器尝试引导驱动程序、**ROM** 选项和操作系统加载程序。

表 69. 引导模式 （续）

项	选项	描述
		[UEFI 模式] 运行 **UEFI** 驱动程序并引导 **UEFI** 操作系统加载程序。仅支持 **UEFI** 模式。
无限引导重试	• 已启用 • **已禁用**（默认）	系统不断尝试引导顺序。 确保在“引导顺序”中指定了可引导设备。
防止操作系统更改引导顺序	• 已启用 • **已禁用**（默认）	选择 **[已启用]** 时，**UEFI** 会从引导顺序列表中删除由操作系统或操作系统安装程序创建的引导选项。
加速引导	• **已禁用**（默认） • 已启用	如果没有错误或异常，加速引导会极大地加快 **UEFI** 引导过程。 选择进行硬件更改和固件更新时，请禁用此项。否则，可能会出现限制。 **注：** 如果未安装 **BMC** 许可证，此项将不可用。

重新引导系统

表 70. 重新引导系统

项	描述
重新引导系统	提示重新引导系统。如果按 <Y>，则所有设置更改都会丢失，并且系统将重新引导。

BMC 设置

在此菜单上，您可以配置基板管理控制器（BMC）设置。

注：BMC 页面下的所有设置都无法使用**加载默认设置**重置为默认值。请使用此页面上的**重置出厂默认设置**将这些设置重置为默认值。

表 71. BMC 设置

项	选项	描述
电源恢复策略	• 始终关闭 • 恢复 • 始终开启	确定系统在电源恢复后如何反应。更改需要几分钟时间才能生效。 • [始终关闭]：系统在电源恢复后仍保持关闭状态。 • [恢复]：系统恢复到断电前的状态。 • [始终开启]：系统在电源恢复后自动开启。
电源恢复随机延迟	• 已启用 • 已禁用	为开机提供 **1** 到 **15** 秒的随机延迟。如果在电源故障发生前服务器为“开启”状态，则在电源恢复后，开机将延迟。 **注：**当**电源恢复策略**设置为 [始终关闭] 时，此项不可用。
Ethernet over USB 接口	• 已启用 • 已禁用	控制用于与 BMC 进行带内通信的 **Ethernet over USB** 接口。 • [已启用]：启用 BMC 与服务器上运行的 **xClarity Essentials** 带内更新实用程序之间的带内通信。 • [已禁用]：阻止 **xClarity Essentials** 和服务器上运行的其他应用程序请求 BMC 执行任务。 **注：**更改设置后，设置可能会暂时保持原有状态，不会立即生效。
第 58 页 “网络设置”	不适用	配置 BMC 的网络设置。
重置出厂默认设置	不适用	将所有 BMC 设置恢复为出厂默认设置，包括网络配置和凭证。BMC 将会自动重新启动。
重新启动 BMC	不适用	重新启动 BMC。

网络设置

注意：需要单击此页面底部的**保存网络设置**才能保存此页面及其子页面上的更改。

表 72. 网络设置

项	选项	描述
网络接口	• 专用 • 共享 • 上行链路 MAC	选择系统管理网络端口。 **注**：选项因平台而异。
故障转移目标 NIC 端口	• 无 • 故障转移到共享（选配卡 **ML2**） • 故障转移到共享（选配卡 **PHY**） • 故障转移到共享（板载端口）	选择主 **NIC** 失去连接时的故障转移目标 **NIC** 端口。 **注**： • 仅当**网络接口**设置为 **[**专用**]** 时，此项才可用。 • 选项因平台而异。
共享 NIC 端口	**OCP** 卡	选择共享 **NIC** 端口。 **注**：仅当**网络接口**设置为 **[**共享**]** 时，此项才可用。
网络设置	• 同步 • 独立	当**故障转移目标 NIC 端口**启用为板载端口或可选卡时，此项将为可选状态。请在 **NIC** 故障转移模式下将“同步”更改为“独立”后设置共享模式网络设置。
固化 MAC 地址	不适用	网络接口控制器的固化 **MAC** 地址
主机名	不适用	**BMC** 控制器的主机名 **BMC** 主机名由字符串“**XCC-**”后跟服务器机器类型和服务器序列号组成（例如：“**XCC-7DG8-1234567890**”） 您可以通过在此字段中输入最多 **63** 个字符来更改主机名。
DHCP 控制	• 静态 **IP** • 启用 **DHCP** • **DHCP**（带回退）	配置 **DHCP** 控制或手动配置静态 **IP** 地址。 • **[**静态 **IP]**：手动输入 **IP** 地址。 • **[**启用 **DHCP]**：**IP** 地址将由 **DHCP** 服务器自动分配。 • **[DHCP**（带回退）**]**：如果 **DHCP** 失败，将使用静态 **IP** 地址。
IP 地址	**x.x.x.x**	输入以点分十进制表示的 **IP** 地址。
子网掩码	**x.x.x.x**	输入以点分十进制表示的子网掩码地址。
默认网关	**x.x.x.x**	输入以点分十进制表示的默认网关地址。
IPv6	• 已启用 • 已禁用	在管理端口上启用或禁用 **IPv6** 支持。 **注**：此项无法通过主菜单上的**加载默认设置**重置为默认值。
本地链路地址	不适用	本地链路地址

表 72. 网络设置 （续）

项	选项	描述
VLAN 支持	• 已启用 • 已禁用	启用或禁用虚拟 LAN（VLAN）支持。 启用 **VLAN** 时，您可以为管理网络端口指定 **802.1q VLAN ID**。 **注**：此项无法通过主菜单上的**加载默认设置**重置为默认值。
VLAN ID	**1**	指定 **VLAN ID**。该值范围为 **1** 到 **4094**。 **注**：仅当已启用“**VLAN** 支持”时，此项才可用。
自动协商	• 是 • 否	指定是否启用网络连接之间的自动协商。 • **[**否**]**：您可以手动选择数据速率和双工模式。 • **[**是**]**：自动设置数据速率和双工模式。 **注**：此项无法通过主菜单上的**加载默认设置**重置为默认值。
数据速率	• **100 Mb**（以太网） • **10 Mb**（以太网）	设置每秒要通过 **LAN** 连接传输的数据量。 **注**： • 仅当**自动协商**设置为 **[**否**]** 时，此项才可用。如果已启用自动协商，则会自动选择数据速率。 • 此项无法通过主菜单上的**加载默认设置**重置为默认值。
双工	• 半双工 • 全双工	设置网络中使用的通信通道类型。 • **[**全双工**]** 允许同时在两个方向上传输数据。 • **[**半双工**]** 允许一次向一个方向传输数据。 **注**： • 仅当**自动协商**设置为 **[**否**]** 时，此项才可用。如果已启用自动协商，则会自动选择双工模式。 • 此项无法通过主菜单上的**加载默认设置**重置为默认值。
最大传输单元	**1500**	指定网络接口的数据包的最大大小（以字节为单位）。 对于 **IPv4** 网络，**MTU** 范围为 **68-1500** 字节 对于 **IPv6** 网络，**MTU** 范围为 **1280-1500** 字节。
保存网络设置	不适用	保存对 **BMC** 的网络设置更改。更改需要几分钟时间才能生效。

系统事件日志

系统事件日志（SEL）提供与硬件及系统操作相关的重大事件的记录。此菜单提供用于管理这些日志的选项。

表 73. 系统事件日志

项	描述
系统事件日志	查看系统事件日志。
清除系统事件日志	清除系统事件日志。

用户安全性

“用户密码”页面和子菜单下的所有设置都无法加载为默认设置。清除 CMOS 只会将“规则”和“策略”下的项重置为默认设置，但不会重置开机密码和管理员密码。

表 74. 用户安全性

项	描述
第 62 页 “密码规则和策略”	设置密码规则和策略。
设置开机密码	设置开机密码。 密码只能包含以下字符（不包括空格字符）：**A-Z**、**a-z**、**0-9**、~‘!@#$%^&*()-+={}[]|:;"’<>,?/._ 必须至少包含一个字母。 必须至少包含一个数字。 必须至少包含以下两种字符的组合： • 至少一个大写字母 • 至少一个小写字母 • 至少一个特殊字符 同一字符的连续出现次数不超过两次 如果未设置**最短密码长度**，则必须至少包含 **8** 个字符。
清除开机密码	清除开机密码。

表 74. 用户安全性 （续）

项	描述
设置管理员密码	设置管理员密码。 密码只能包含以下字符（不包括空格字符）：**A-Z**、**a-z**、**0-9**、~‘!@#$%^&*()-+={}[]|:;"'<>,?/._ 必须至少包含一个字母。 必须至少包含一个数字。 必须至少包含以下两种字符的组合： • 至少一个大写字母 • 至少一个小写字母 • 至少一个特殊字符 同一字符的连续出现次数不超过两次 如果未设置**最短密码长度**，则必须至少包含 **8** 个字符。
清除管理员密码	清除管理员密码。

密码规则和策略

表 75. 密码规则和策略

项	选项	功能
最短密码长度	**8-20**	最小字符数，这是指定有效密码的规则的一部分 您可以设置介于 **8** 到 **20** 之间的值。
密码有效期	**0-365**	密码在必须更改之前还可使用的天数 您可以设置介于 **0** 和 **365** 之间的值。如果将该值设置为“**0**”，则密码将永不过期。
密码到期警告周期	**0-365**	密码过期前收到警告的天数 您可以设置介于 **0** 和 **365** 之间的值。如果将该值设置为“**0**”，则永不收到警告。
最短密码更改时间间隔	**0-240**	更改密码前必须经过的小时数 您可以设置介于 **0** 到 **240** 之间的值。该值不能超过为**密码有效期**指定的值。如果将该值设置为“**0**”，则可以立即更改密码。
最短密码重用周期	**0-10**	旧密码可以重用之前必须设置的唯一新密码数 您可以设置介于 **0** 到 **10** 之间的值。如果将该值设置为 **0**，则可以立即重复使用旧密码。

表 75. 密码规则和策略 （续）

项	选项	功能
登录失败次数上限	**0-100**	用户帐户被锁定前可以使用错误密码尝试登录的次数。锁定期在**达到登录失败次数上限后的锁定期**中指定。 您可以设置介于 **0** 到 **10** 之间的值。如果将该值设置为“**0**”，则永不锁定帐户。
达到登录失败次数上限后的锁定期	**0-2880**	锁定用户在再次尝试登录前必须等待的时间段（以分钟为单位）。在锁定期间，输入有效密码也无法解锁帐户。 您可以设置介于 **0** 到 **2880** 之间的值。如果将该值设置为“**0**”，则即使超过登录失败次数上限，帐户也不会被锁定。

默认选项

在此菜单上，您可以管理和配置系统的默认设置，允许出厂默认配置和自定义默认配置。

表 76. 默认选项

项	选项	描述
保存自定义默认设置	不适用	保存所有当前设置作为自定义默认设置。
删除自定义默认设置	不适用	删除现有的自定义默认设置。 **注**：如果不存在自定义默认设置，此项将灰显。
选择默认设置	• 自定义默认值 • **出厂默认值**	指定加载默认设置时是加载出厂默认设置还是自定义默认设置。 **注**：如果不存在自定义默认设置，此项将灰显。

查看未保存的设置

此菜单清晰有序地显示已更改但未保存的任何设置。

表 77. 查看未保存的设置

项	选项	描述
已更改的设置（X）	新值	显示所有已更改但未保存的设置。 **注**：***X*** 是未保存设置的数量。如果 ***X*** 为 **0**，则不会显示额外的信息。
未保存的设置列表	不适用	• **路径**：**.../X**。 指示已修改的特定设置的导航路径 • **旧值**：**X** 指示在进行任何更改之前当前保存在系统中的值。 • **帮助**：**X**：

表 77. 查看未保存的设置 （续）

项	选项	描述
		这将提供与所选设置相关的有用信息或注释，帮助用户了解其更改的含义

附录 A　声明

本文档中讨论的 **Lenovo** 产品、服务或功能可能未在部分国家或地区提供。有关您当前所在区域的产品和服务的信息，请向您当地的 **Lenovo** 代表咨询。

任何对 **Lenovo** 产品、程序或服务的引用并非意在明示或暗示只能使用该 **Lenovo** 产品、程序或服务。只要不侵犯 **Lenovo** 的知识产权，任何同等功能的产品、程序或服务，都可以代替 **Lenovo** 产品、程序或服务。但是，用户需自行负责评估和验证任何其他产品、程序或服务的运行情况。

Lenovo 公司可能已拥有或正在申请与本文档中所描述内容有关的各项专利。提供本文档并非要约，因此本文档不提供任何专利或专利申请下的许可证。您可以用书面方式将查询寄往以下地址：

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

Lenovo“按现状”提供本文档，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销性和特定用途适用性的保证。部分管辖区域在特定交易中不允许免除明示或暗含的保证，因此本声明可能不适用于您。

本文档可能包含技术性偏差或印刷错误。文档中的信息将定期更改并在新版本中呈现。**Lenovo** 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本文档中描述的产品不应用于移植或其他生命支持应用场景，否则可能因故障而导致人身伤害或死亡。本文档中包含的信息不影响或更改 **Lenovo** 产品规格或保修。根据 **Lenovo** 或第三方的知识产权，本文档中的任何内容都不能充当明示或暗含的许可或保障。本文档中所含的全部信息均在特定环境中获得，并且作为演示提供。在其他操作环境中获得的结果可能不同。

Lenovo 可以按其认为适当的任何方式使用或分发您所提供的任何信息，而无须对您承担任何责任。

本文档对非 **Lenovo** 网站的任何引用均仅为方便起见，并不以任何方式充当对此类网站的担保。此类网站中的资料并非本 **Lenovo** 产品资料的一部分，因此使用此类网站带来的风险将由您自行承担。

本文档中的所有性能数据均在受控环境下测得。因此，在其他操作环境中获得的数据可能会有明显的不同。部分测量可能在开发级系统上进行，因此不保证与一般可用系统上进行的测量结果相同。此外，部分测量可能是通过推算得出。实际结果可能会有差异。本文档的用户应验证其特定环境的适用数据。

商标

LENOVO 和 **LENOVO** 徽标是 **Lenovo** 的商标。

所有其他商标均是其各自所有者的财产。© **2024 Lenovo**