同泰怡信息技术
www.ttyinfo.com

同泰怡服务器产品技术手册

——TU628V2　版本 V1.1

使用本产品前请先阅读技术手册

版权申明

本手册版权归深圳市同泰怡信息技术有限公司所有，未经本公司书面许可和授权，任何单位或个人不得以任何方式复制、抄录本文档内容的部分或全部，并不得以任何形式传播。

商标声明

本手册中出现的商标均已注册。关于第三方的注册商标归第三方所有。

注意

由于产品版本升级或其他原因，本手册内容会不定期进行更新。

本手册陈述之规格及信息，将依规格之更新而改变。

因此，制造商不承担因规格更新而造成手册内容错误或遗漏之职责。

本手册中的信息可能包含技术或印刷错误。

本手册中的图片可能与实物有差异，仅作说明之用。

同泰怡保留在不另行通知的情况下对产品进行改进/改动的权利。

目录

第一章 安全声明 3

1.1 一般安全事项 3

1.2 产品有毒有害物质或元素的名称及含量标识表 4

1.3 警示通告 5

1.4 气候环境要求 5

1.5 其他重要描述 6

第二章 产品介绍 1

2.1 系统简介 1

2.2 系统配置 1

2.2.1 系统参数： 1

2.2.2 系统架构主板框图如下： 3

2.3 系统组件介绍 3

2.3.1 前面板组件 3

2.3.2 后面板组件 7

2.3.3 主板组件 10

2.3.4 DIMM 插槽位置 13

2.3.5 内存安装要求 13

2.3.6 内存安装原则 13

2.3.7 硬盘标号 14

2.3.8 硬盘指示灯 16

2.3.9 PCIe 插槽分布后视图 17

2.3.10 系统风扇 17

第三章安装系统组件 18

3.1 CPU 的安装 18

3.2 散热器的安装 20

3.3 内存的安装 22

3.4 硬盘的安装 23

3.5 M.2 SSD 的安装 26

3.6 IO1 和 IO2 模组安装 27

3.7 IO3 模组安装 29

3.8 网络模块的安装 30
3.9 内置硬盘模块的安装 30
3.10 电源模块的安装 33
3.11 PCIe 扩展卡的安装 34
3.12 风扇模块安装 36
3.13 导风罩安装 37
3.14 光驱安装 37
3.15 LSI 9361 电池包安装 38
3.16 LCD 模块安装 38
3.17 机箱上盖安装 39
3.18 导轨组件安装 42
第四章 BIOS 参数设置说明 46
4.1 概述 47
4.2 进入 BIOS 设置界面 47
4.3 BIOS 参数设置 48
4.3.1 Main 菜单 48
4.3.2 Advanced 菜单 50
4.3.3 Platform 菜单 69
4.3.4 Socket 菜单 84
4.3.5 Server Mgmt 菜单 115
4.3.6 Security 菜单 119
4.3.7 Boot 菜单 120
4.3.8 Save & Exit 菜单 122
第五章 BMC 操作说明 124
第六章 操作系统安装指南 124
第七章 Raid 卡操作指南 124
7.1 9361 Raid 卡操作指南 124
7.2 3008 SAS 卡操作指南 124
第八章 获得帮助 124
8.1 联系同泰怡 124
第九章 附录 125
9.1 术语&缩略语 125

第一章 安全声明

1.1 一般安全事项

为防止出现重大人身及财产损失的风险，请务必遵循以下建议。

请不要自行打开系统盖板，应由经过专业培训的维修技术人员进行操作。带有闪电符号的三角形标记部分可能会有高压或电击，请勿触碰。

切记：在进行维修前，断开所有的电缆。（ 电缆可能不止一条）

严格禁止在盖板未闭合前进行开机等带电操作。

当需要进行开盖处理是，请等待内部设备冷却后再执行，否则容易对您造成烫伤。

请勿在潮湿环境中使用本设备。

如果延长线缆需要被使用，请使用三线电缆并确保其正确接地。

确保计算机接地良好。可以通过不同的接地方式，但要求必须实际连接至地面。如果您不确定是否已经安全的接地保护，请联系相应的机构或电工予以确认。如果需要绞台电缆布线，请联系同泰怡公司提供建议。

请使用带接地保护的三芯电源线与插座，不正确的接地可能会导致漏电、烧毁 爆炸甚至人身伤害。

请确保电源插座和电源接口能够紧密接触，松动的接触可能有导致起火的危险。

请在 220V 交流电压下使用设备，在不合适的电压下工作将导致设备触电、起火、甚至损坏。

要求设备通风良好并且远离热源、火源、不要阻塞散热风扇，否则设备可能会由于过热导致冒烟、起火或其他损害的危险。

如果闻到或看到设备冒烟，拔掉电源线，请立即关闭设备。

要求能方便地从电源和电源插座上插拔电源线。请保持电源线和插头的清洁卫生和完好无损、否则可能有导致触电或起火的危险。

注意：如果电池更换不当会有爆炸危险，只许使用制造商推荐的同类或等效类型的替代件，废旧电池会对环境造成污染，更换下的旧电池请按照有关说明进行设置。

使计算机远离电磁场。

远离由空调、风扇、电机、电台、电视台、发射塔等高频设备引起的电子噪声和干扰。

请不要在设备正在运行时插拔内部连接部件或移动设备，否则将可能造成设备宕机或设备损坏。

请尽量避免频繁重启或开关机，以延长设备的使用寿命。

请保持环境清洁，避免灰尘，设备工作环境温度 5℃~35℃，湿度 35%~80%。

请用户及时备份重要数据，同泰怡股份信息技术有限公司不为任何情况所导致的数据丢失负责。

本产品使用如配置光驱，光驱为 1 类激光设备。

1.2 产品有毒有害物质或元素的名称及含量标识表

在 10 年环保使用期限内，产品中含有的有毒有害物质或元素在正常使用的条件下不会发生外泄或突变，用户使用该设备不会对环境造成严重污染或对其人身，财产造成严重损害。

部件名称	有害物质					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
	(Pb)	(Hg)	(Cd)	(Cr VI)	(PBB)	(PBDE)
机箱 /挡板	X	0	0	0	0	0
机械组件（风扇、散热器、马达等。）	X	0	0	0	0	0
印刷电路部件 – PCA*	X	0	0	0	0	0

部件名称	有害物质					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
	(Pb)	(Hg)	(Cd)	(Cr VI)	(PBB)	(PBDE)
电缆 /电线 /连接器	X	0	0	0	0	0
硬盘驱动器	X	0	0	0	0	0

介质读取 /存储设备（光盘等）	X	0	0	0	0	0
电源设备 /电源适配器	X	0	0	0	0	0
电源	X	0	0	0	0	0
定点设备（鼠标等）	X	0	0	0	0	0
键盘	X	0	0	0	0	0
完整机架 /导轨产品	X	X	0	0	0	0

○ 表示该有毒有害物质在该部件所有均质材料中的含量均在 GB/T26572-2011《电子电气产品中限用物质的限量要求》规定的限量要求以下。

× 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 GB/T26572-2011《电子电气产品中限用物质的限量要求》规定的限量要求。但符合欧盟 RoHS 指令(包括其豁免条款)。

注释：此表为该设备中所有可能采用的部件所含有毒有害物质的状况，客户可依据本表查阅所购产品各部件含有毒有害物质的情况。

1.3 警示通告

本产品符合 EMC Class A 标准。

1.4 气候环境要求

- 设备最佳工作温度为 5℃—35℃；
- 系统电池

  3V CR2032 锂电池

注释：某些配置已在 40℃ 的温度和 90%（29℃ 最大露点）的湿度下进行性能验证。

温度	
工作温度	5℃ 至 35℃，最大温度梯度为每小时 10℃。
连续操作温度范围（在低于海拔 950 米或 3117 英尺时）	在设备无直接光照的情况下，5℃ 至 35℃。
存储温度范围	-40℃ 至 65℃。
湿度	

存储	最大露点为 33℃ 时，相对湿度为 5% 至 95%。空气必须始终不冷凝。
连续操作湿度百分比范围	最大露点为 26℃时，相对湿度为 10% 至 80%。

- 如果设备的使用环境避雷设施不良或没有，请在雷雨天气情况下关机、并拔掉与设备相连接的电源线、网线、电话线等。
- 请使用正版操作系统及软件，并进行正确配置。同泰怡信息技术有限公司对由于操作系统和软件引起的服务器故障不负有维护责任。
- 请不要自行拆开机箱及增减服务器硬件配置，同泰怡信息技术有限公司不为因此而造成的硬件及数据损坏负责。
- 当设备出现故障时，请首先查看本手册的内容，以确定及排除常见故障。如果您不能确定故障的原因，请及时与技术支持部门联系以获得帮助。
- 为计算机选择一个合适的环境，有助于计算机的为稳定运行，并可以延长计算机的使用寿命。

1.5 其他重要描述

“如果该设备标示有标识，表示加贴该标识的设备仅按海拔 2000m 进行安全设计与评估，因此，仅适用于在 2000m 以下安全使用，在海拔 2000m 以上使用时，可能有安全隐患”。

“如果该设备标示有此标识，表示加贴该标识的设备仅按非热带气候条件进行安全设计与评估，因此，仅适用于非热带气候条件安全使用，在热带气候条件使用时，可能有安全隐患”。

第二章 产品介绍

2.1 系统简介

TU628 V2是一款2U双路通用机架服务器，采用最新一代Intel Xeon 可扩展处理器（Ice Lake-SP），实现了计算、存储、网络等性能的全面突破。基于创新的服务器硬件模块化设计理念和技术，充分利用存储及网络资源，可根据业务需求进行弹性配置，实现了优异的性价比和能耗比，可广泛应用于互联网、云计算、数据库和大数据等应用。

2.2 系统配置

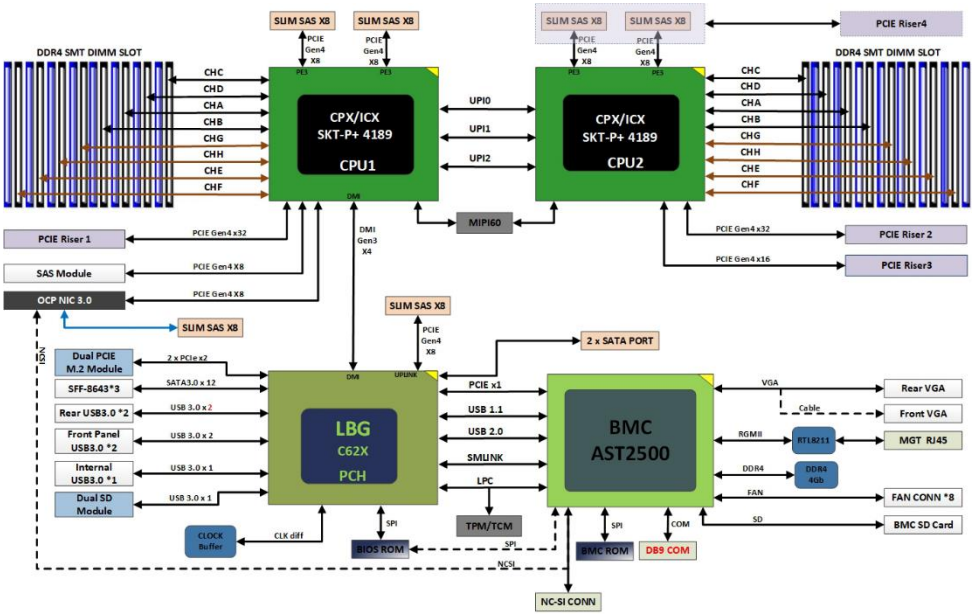
TU625 V2 服务器采用模块化设计，前置硬盘模块和后置 IO 模块均可按需配置，包括 2U8（3.5＂硬盘）盘位、2U12（3.5＂硬盘）盘位、2U8（2.5＂硬盘）、2U16（2.5＂硬盘）、2U24（2.5＂硬盘）、2U25（2.5＂硬盘）盘位等机型。

2.2.1 系统参数：

功能	技术规格
形态	2U 机架服务器
处理器	1/2 个第三代英特尔® 至强® 可扩展处理器 （Ice Lake ）（8300/6300/5300/4300 系列）， 最高 270W
芯片组	Intel C621A
内存	32 个 DDR4 内存插槽，共 16 个通道，最高 3200MHz； 最多支持 16 条英特尔® 傲腾™ 持久内存 200 系列，最高 3200MT/s
内存类型	RDIMM/LRDIMM/Intel Optane DC Persistent Memory
内存容量	单条容量 8GB，16GB，32GB，64GB，128GB，256GB，512GB，最大支持 12TB
存储控制器	集成 6Gb/s SATA 控制器；可选支持 12Gb/s SAS HBA 及 12Gb/s SAS RAID 控制器
本地存储	前置 ： 最大支持 12 个 3.5 寸或 25 个 2.5 寸硬盘 后置 ： 最大支持 4 个 3.5 寸+4 个 2.5 寸硬盘或 10 个 2.5 寸硬盘 内置 ： 支持 4 个 3.5 寸硬盘（兼容 2.5 寸） 支持 2 个 M.2(2280，PCIe 3.0 x2)、可选支持 1 个 SD 模组（支持 RAID1 双 Micro SD）

PCIe 扩展	最大支持 10 个 PCIe 4.0 扩展插槽
GPU	最大支持 4 个全高全长双宽 GPU
网络	1 个 1Gb RJ45 专用管理网口，可选 4×1GbE / 2×10Gb SFP+ / 4×10Gb SFP+/ 2×25Gb SFP28 OCP 网卡
端口	前置：1 个 VGA、2 个 USB3.0、1 个 LCD Mini USB 后置：1 个 VGA、2 个 USB3.0、1 个 RJ45 管理网口、1 个 COM 、1 个标准 OCP NIC 3.0 插槽
管理功能	集成 BMC 管理芯片，支持 IPMI2.0、Redfish、SOL、KVM、虚拟媒介等功能， 提供 1 个 1Gbps RJ45 专用管理口，可选 LCD 管理模块
安全性	可选 TPM/TCM 安全模块，机箱开盖入侵检测，加锁机箱上盖板
电源	可配置 2 个电源模块，支持 1+1 冗余，支持热插拔 可选 220v 交流/240v 直流/336v 直流/-48v 直流输入 可选 550W/800W/1300W/1600W/2000W 高效白金电源
风扇	4 个热插拔风扇模组，支持 3+1 冗余，支持智能调速和异常报警
机箱尺寸	机架式 2U，宽 447mm × 高 87mm × 深 763mm（含挂耳 783mm）
工作温度	5°C - 35°C （详情请咨询同泰怡销售人员）
工作相对湿度	0% - 90%
支持操作系统	Microsoft Windows Server、Microsoft Hyper-V Server、Red Hat Enterprise Linux、SUSE Linux Enterprise Server、CentOS、Ubuntu、Fedora、Solaris、Oracle Linux、FreeBSD、VMware ESXi、Citrix XenServer 具体版本请向销售人员咨询

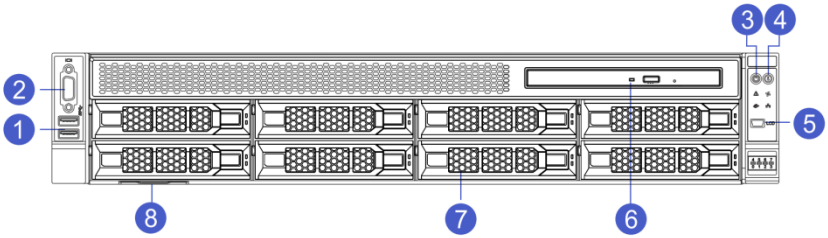
2.2.2　　系统架构主板框图如下：



2.3 系统组件介绍

2.3.1 前面板组件

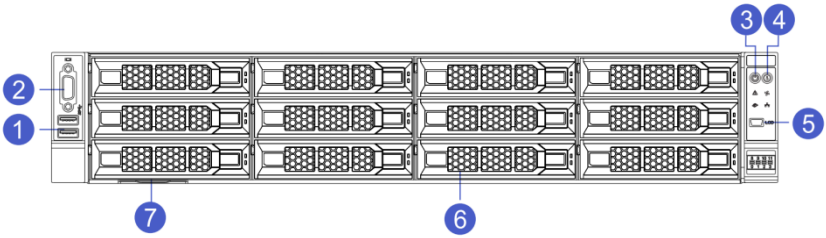
- 2U8 盘位 3.5 寸盘机型



1	USB 3.0 接口	2	VGA 接口
3	电源键	4	UID
5	MiniUSB LCD 接口	6	光驱

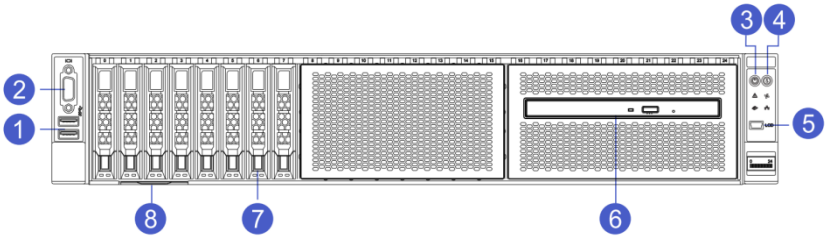
7	硬盘	8	资产标签

- 2U12 盘位 3.5 寸盘机型



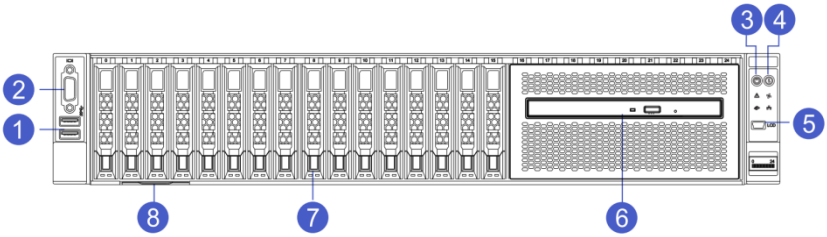
1	USB 3.0 接口	2	VGA 接口
3	电源键	4	UID
5	MiniUSB LCD 接口	6	硬盘
7	资产标签		

- 2U8 盘位 2.5 寸盘机型



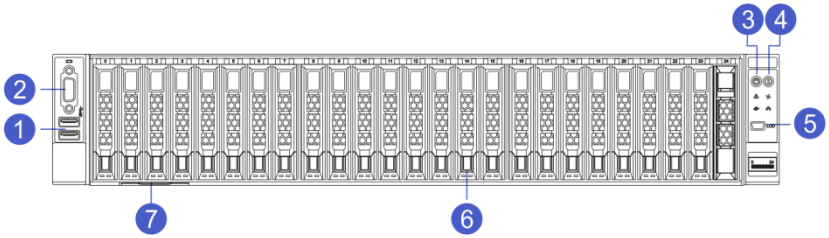
1	USB 3.0 接口	2	VGA 接口
3	电源键	4	UID
5	MiniUSB LCD 接口	6	光驱
7	硬盘	8	资产标签

- 2U16 盘位 2.5 寸盘机型



1	USB 3.0 接口	2	VGA 接口
3	电源键	4	UID
5	MiniUSB LCD 接口	6	光驱
7	硬盘	8	资产标签

- **2U25 盘位 2.5 寸盘机型**



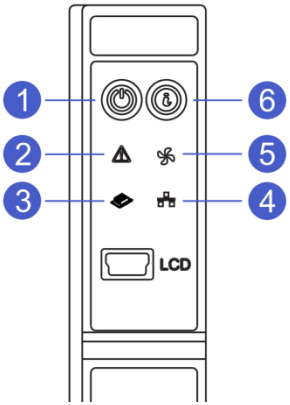
1	USB 3.0 接口	2	VGA 接口
3	电源键	4	UID
5	MiniUSB LCD 接口	6	硬盘
7	资产标签		

- **前面板接口说明：**

名称	类型	说明
VGA 接口	DB15	用于连接显示终端，例如显示器 或 KVM。
USB 接口	USB 3.0	提供外出USB接口，通过该接口可以接入USB设备。 **注意** 使用外接USB设备时请确认USB设备状态良好，否则可能导致服务器工作异常。

LCD 专用接口	Mini USB	用于连接外部LCD模块，主要用于反映服务器各部件的在位和运行状态，以及可以用于设置服务器iBMC管理网口的IP地址和查询设备状态信息及告警。 LCD与服务器上的iBMC管理模块共同构成LCD子系统。LCD直接从iBMC管理模块获取设备信息。LCD子系统不存储设备数据。

- **前面板指示灯和按钮说明**

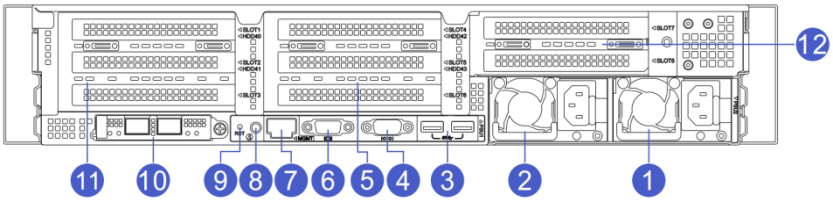


1	电源开关按钮/指示灯	4	OCP 网卡状态指示灯
2	系统故障指示灯	5	风扇故障指示灯
3	内存故障指示灯	6	UID按钮/指示灯

标识	指示灯/按钮	状态说明
	电源开关按钮/指示灯	电源指示灯说明： ✓ 绿色（常亮）：表示设备已正常上电。 ✓ 绿色（闪烁）：表示设备处于待机状态。 ✓ 绿色熄灭：表示设备未上电。 电源按钮说明： ✓ 开机状态下短按该按钮，OS正常关机。 ✓ 开机状态下长按该按钮6秒钟可以将服务器强制下电。 ✓ 待上电状态下短按该按钮，可以进行开机。
	UID 按钮/指示灯	UID按钮/指示灯用于方便地定位待操作的服务器，可通过手动按UID按钮或者iBMC命令远程控制使灯灭或灯亮。

		UID指示灯说明： ✓ 蓝色（常亮/闪烁）：表示服务器被定位。 ✓ 熄灭：表示服务器未被定位。 UID按钮说明： ✓ 短按该按钮，可以打开/关闭定位灯。 ✓ 长按UID按钮6秒，可以复位服务器BMC管理系统
	系统故障指示灯	✓ 熄灭：表示设备运转正常。 ✓ 红色闪烁：表示设备出现故障。 ✓ 红色常亮：表示设备出现异常报警。
	风扇故障指示灯	✓ 熄灭：表示风扇正常。 ✓ 红色常亮：表示风扇出现故障
	内存故障指示灯	✓ 熄灭：表示系统内存正常。 ✓ 红色常亮：表示系统内存出现故障。
	OCP 网口连接状态指示灯	OCP网卡状态指示灯。 ✓ 绿色常亮：表示OCP网卡连接正常且无数据通信。 ✓ 绿色闪烁：表示OCP网卡连接正常且有数据通信。 ✓ 熄灭：表示OCP网卡未连接网络

2.3.2 后面板组件



1	PSU2	7	IPMI 管理网口
2	PSU1	8	UID按键和指示灯
3	USB3.0 接口	9	RST按键
4	COM 接口	10	OCP 3.0网卡

5	IO 模块 2	11	IO模块1
6	VGA 接口	12	IO模块3

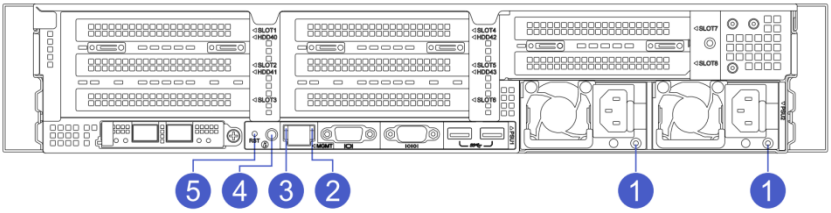
✧ **说明：**

IO模块1和IO模块2可配置3.5”或2.5”硬盘模组，IO模块3只能配置2.5”硬盘模组。PCIe扩展位都可选配后置硬盘模组或者Riser模组。本图仅供参考，具体以实际配置为准。

- **后面板接口说明：**

名称	类型	数量	说明
VGA 接口	DB15	1	用于连接显示终端，例如显示器或KVM。
管理网口	GE BASE-T	1	提供外出1000Mbit/s以太网口。通过该接口可以对本服务器进行管理。
USB 接口	USB 3.0	2	提供外出USB接口，通过该接口可以接入USB设备。 **注意：** 使用外接USB设备时请确认USB设备状态良好，否则可能导致服务器工作异常。
电源模块 AC 接口	/	1或2	您可根据自己实际需求选配电源数量，但是务必确保电源的额定功率大于整机额定功率。

- **后面板指示灯和按钮说明：（待更新）**



1	电源模块指示灯	4	UID 指示灯
2	连接状态指示灯	5	系统复位键
3	数据传输状态指示灯		

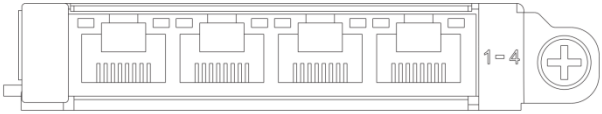
指示灯/按钮	状态说明
电源模块指示灯	✓ 绿色（常亮）：表示输入和输出正常。

	✓ 熄灭：表示无交流电源输入。 ✓ 绿色（1Hz/闪烁）：表示服务器处于standy状态。 ✓ 绿色（4Hz/闪烁）：表示电源模块处于冷备状态。 ✓ 红色（常亮）： ● 表示电源无输出，可能原因有电源过温保护、电源输出过流/短路、输出过压、器件失效（不包括所有的器件失效）等。 ● 表示电源线未接或者电源线脱落。 ✓ 红色（闪烁）：表示电源出现告警信号，电源模块可能出现高温、高负载、大电流或风扇转速过低等异常
UID指示灯	✓ UID指示灯用于方便地定位待操作的服务器，可通过手动按UID按钮或者iBMC命令远程控制使灯灭或灯亮。 ✓ 蓝色（常亮/闪烁）：表示服务器被定位。 ✓ 熄灭：表示服务器未被定位。
连接状态指示灯	✓ 绿色长亮：表示千兆Link。 ✓ 橙色长亮：表示百兆Link。 ✓ 熄灭：十兆Link。
数据传输状态指示灯	✓ 黄色（闪烁）：表示有数据正在传输。 ✓ 熄灭：表示无数据传输。
系统复位键	✓ 可用来对系统复位或NMI功能 ✓ 短按：复位系统 ✓ 长按（6秒以上）：执行NMI功能，触发服务器产生一个不可屏蔽中断 **注意** ✓ **NMI按键主要在无法使用操作系统的情况下使用。在服务器正常运行期间，不应使用该功能。** ✓ **NMI按键仅用于内部调测，使用时需要操作系统中有对应的NMI中断处理程序，否则可能引起系统崩溃。请谨慎使用。**

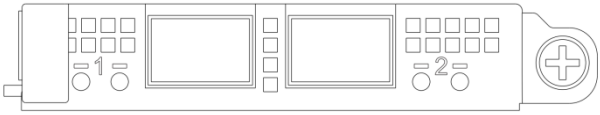
2.3.1 扩展网卡插卡：

服务器支持以下型号的灵活网卡插卡：

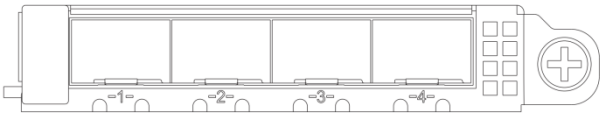
- 四千兆电口网卡：T350LO-E4



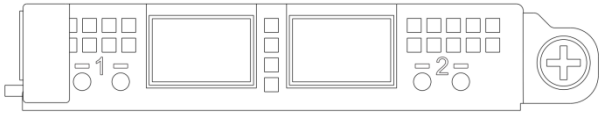
◆ 双万兆光口网卡：T710LO-F2



◆ 四万兆光口网卡：T710LO-F4

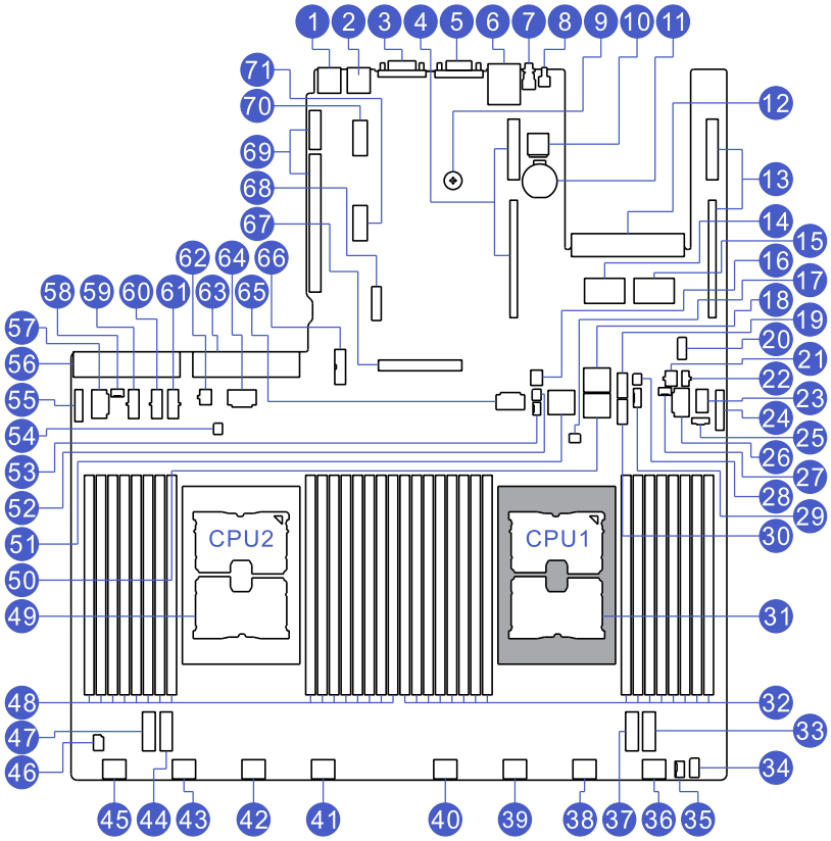


◆ 双 25G 光口网卡：TCX4LO-S2



2.3.3 主板组件

- **TU628 V2 所有机型共用主板组件，接口说明如下所示：**

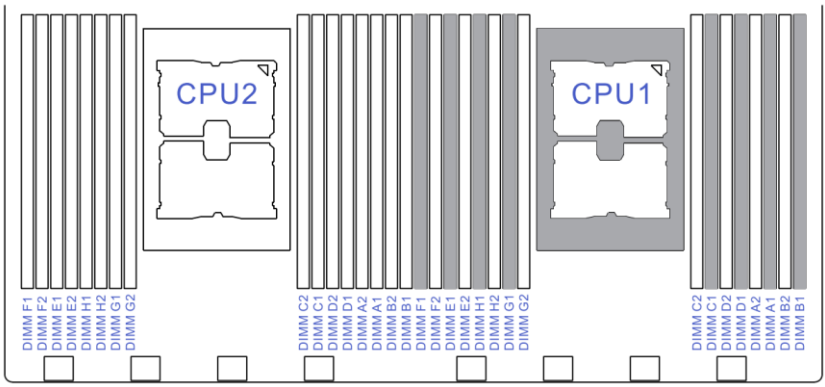


1	USB3.0 接口 2	2	USB3.0 接口 1
3	COM 接口	4	Riser 卡插槽 2（对应 CPU2）
5	VGA 接口	6	IPMI 管理网口
7	UID 按键和指示灯	8	RST 按键
9	主板固定螺丝	10	BMC SD 插槽
11	电池连接器	12	OCP 3.0 网卡连接器
13	Riser 卡插槽 1（对应 CPU1）	14	QAT SlimSAS 连接器
15	OCP SlimSAS 连接器	16	后置硬盘电源连接器 2（HDD PWR2）
17	JTAG TO BP 连接器	18	Mini SAS HD 连接器（SATA Port1）

19	SATA 信号连接器 2（HDD2）	20	NCSI 连接器
21	后置硬盘电源连接器（HDD PWR1）	22	光驱电源连接器（CDPWR）
23	内置 USB3.0 连接器	24	TPM/TCM 接口（LPC）
25	NVMe RAID KEY 连接器（Intel VROC RAID KEY）	26	GPU 电源连接器 0（GPU PWR0）
27	后置硬盘背板 I2C 连接器 0（BP I2C0）	28	后置硬盘背板信号连接器 1（LED CONN1）
29	RAID 信号连接器 1（SGPIO）	30	SATA 信号连接器 1（HDD1）
31	CPU1	32	内存插槽（对应 CPU1）
33	CPU1 Slim SAS 连接器（CPU1 SLIM0）	34	前置灯板信号连接器（FP CONN）
35	水冷散热器信号接口（Water Cooling CONN）	36	风扇连接器（FAN14/15）
37	CPU1 Slim SAS 连接器（CPU1 SLIM1）	38	风扇连接器（FAN12/13）
39	风扇连接器（FAN10/11）	40	风扇连接器（FAN8/9）
41	风扇连接器（FAN6/7）	42	风扇连接器（FAN4/5）
43	风扇连接器（FAN2/3）	44	CPU2 Slim SAS 连接器（CPU2 SLIM0）
45	风扇连接器（FAN0/1）	46	入侵开关接口（Intruder CONN）
47	CPU2 Slim SAS 连接器（CPU2 SLIM1）	48	内存插槽（对应 CPU2）
49	CPU2	50	Mini SAS HD 连接器（SATA Port0）
51	Mini SAS HD 连接器（SSATA Port0）	52	后置硬盘背板信号连接器 2（LED CONN2）
53	后置硬盘背板 I2C 连接器 1（BP I2C1）	54	后置硬盘背板信号连接器 0（LED CONN0）
55	前置 VGA 接口（FP VGA）	56	PSU2 接口
57	GPU 电源连接器（GPU PWR3）	58	后置硬盘背板 I2C 连接器 2（BP I2C2）
59	前置背板电源接口（BP PWR1）	60	前置背板电源接口（BP PWR2）
61	前置背板电源接口（BP PWR3）	62	后置硬盘电源连接器（HDD PWR3）
63	PSU1 接口	64	GPU 电源连接器（GPU PWR2）
65	GPU 电源连接器（GPU PWR1）	66	前置 USB3.0 接口（FP USB3.0 CONN）
67	SAS 扣卡接口（SAS MEZZ）	68	MICRO SD 扣卡接口（SD MODULE）
69	Riser 卡插槽 3（对应 CPU2）	70	M.2 插槽（M.2 SLOT0）
71	M.2 插槽（M.2 SLOT1）		

2.3.4 DIMM 插槽位置

服务器提供 32 个 DIMM 插槽，每个 CPU 支持 8 通道 DDR4 内存，对应插槽顺序如下图所示：



2.3.5 内存安装要求

- 同一台服务器必须使用相同型号的 DDR4 内存；
- LRDIMM 和 RDIMM 不能混用
- 安装内存时，需要先安装每个通道主内存通道的内存；
- 安装内存时必须遵循内存安装原则

2.3.6 内存安装原则

不配置 Intel 傲腾持久内存时，参考如下安装原则

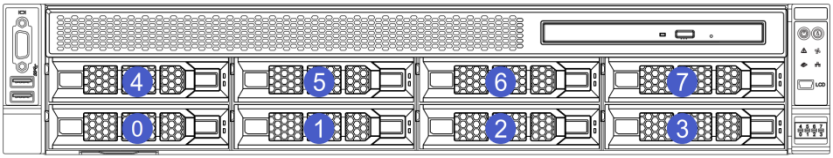
	ICX iMC#	iMC2				iMC3					iMC1				iMC0				SNC2	SNC4	Hemi	Mirror	SGX	POR/Validated
	Channel	Channel 1(F)		Channel 0 (E)		Channel 1(H)		Channel 0 (G)			Channel 0(C)		Channel 1 (D)		Channel 0(A)		Channel 1 (B)							
DDR4 + BPS	Mode	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1		Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0						
1+0	1LM									CPU		DDR4												POR&Validated
														DDR4										POR&Validated
																DDR4								POR&Validated
								DDR4										DDR4						POR&Validated
						DDR4																		POR&Validated
			DDR4																					POR&Validated
	DDR4																							POR&Validated
2+0			DDR4												DDR4				Y		Y			POR&Validated
								DDR4				DDR4							Y		Y			POR&Validated
			DDR4									DDR4				DDR4			Y		Y			POR&Validated
			DDR4					DDR4						DDR4		DDR4			Y		Y			POR&Validated
	DDR4												DDR4		DDR4			DDR4	Y		Y			POR
					DDR4								DDR4					DDR4	Y		Y			POR
	DDR4				DDR4													DDR4	Y		Y			POR
4+0			DDR4					DDR4				DDR4			DDR4				Y	Y	Y			POR&Validated
			DDR4		DDR4								DDR4		DDR4				Y	Y	Y			POR&Validated
	DDR4				DDR4								DDR4			DDR4		DDR4	Y	Y	Y			POR
	DDR4						DDR4					DDR4						DDR4	Y	Y	Y			POR
	DDR4		DDR4				DDR4					DDR4			DDR4			DDR4	Y					POR&Validated
6+0			DDR4		DDR4		DDR4					DDR4		DDR4		DDR4			Y					POR&Validated
	DDR4		DDR4		DDR4								DDR4		DDR4			DDR4	Y					POR
	DDR4				DDR4		DDR4					DDR4		DDR4				DDR4	Y					POR
8+0	DDR4		DDR4		DDR4		DDR4					DDR4		DDR4		DDR4		DDR4	Y	Y	Y	Y	Y	POR&Validated
12+0	DDR4	DDR4	DDR4	DDR4			DDR4	DDR4		DDR4	DDR4			DDR4	DDR4	DDR4	DDR4	DDR4	Y					POR&Validated
			DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4			Y					POR&Validated
	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4						DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	Y					POR
	DDR4	DDR4			DDR4	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	DDR4				DDR4	DDR4	Y					POR
	DDR4		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		DDR4	DDR4			DDR4	DDR4	DDR4	DDR4	DDR4	Y	Y	Y		Y	POR&Validated
	DDR4		DDR4	DDR4	DDR4	DDR4	DDR4				DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		DDR4	Y	Y	Y		Y	POR
	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4					DDR4	DDR4		DDR4	DDR4	DDR4	DDR4	Y	Y	Y		Y	POR
	DDR4	DDR4	DDR4		DDR4		DDR4	DDR4		DDR4	DDR4		DDR4		DDR4	DDR4	DDR4	DDR4	Y	Y	Y		Y	POR
16+0	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	Y	Y	Y	Y	Y	POR&Validated

配置 Intel 傲腾持久内存时，参考如下安装原则

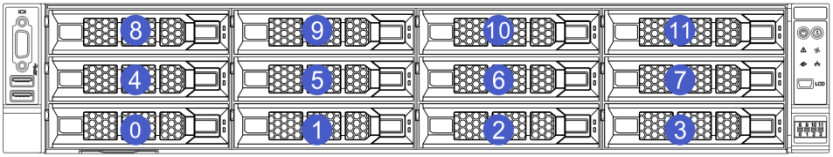
	ICX iMC#	iMC2				iMC3					iMC1				iMC0				SNC2	SNC4	Hemi	Mirror	SGX	BPS AD Interleave	POR/Validated
	Channel	Channel 1(F)		Channel 0 (E)		Channel 1(H)		Channel 0 (G)			Channel 0(C)		Channel 1 (D)		Channel 0(A)		Channel 1 (B)								
DDR4 + BPS	Mode	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1		Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0							
4+4	1LM+AD MM 1/2 Perf	BPS		DDR4		BPS		DDR4		CPU		DDR4		BPS		DDR4		BPS	Y	Y	Y			One x4	POR&Validated
		DDR4		BPS		DDR4		BPS				BPS		DDR4		BPS		DDR4	Y	Y	Y			One x4	POR&Validated
6+1	1LM+AD	DDR4		DDR4				DDR4				DDR4		BPS		DDR4		DDR4	Y						POR&Validated
				DDR4		DDR4		DDR4				DDR4		DDR4		DDR4		BPS	Y						POR&Validated
		DDR4		DDR4		BPS		DDR4				DDR4		DDR4		DDR4		DDR4	Y						POR&Validated
		BPS		DDR4		DDR4		DDR4				DDR4				DDR4			Y					One x1	POR&Validated
		DDR4		DDR4		DDR4						BPS		DDR4		DDR4		DDR4	Y					One x1	POR
		DDR4				DDR4		DDR4				DDR4		DDR4		BPS		DDR4	Y					One x1	POR
		DDR4		DDR4		DDR4		BPS				DDR4		DDR4		DDR4		DDR4	Y					One x1	POR
		DDR4		BPS		DDR4		DDR4				DDR4		DDR4		DDR4		DDR4	Y					One x1	POR
8+1	1LM+AD	DDR4		DDR4		DDR4		DDR4				DDR4		DDR4	BPS	DDR4		DDR4	Y						POR&Validated
		DDR4		DDR4		DDR4		DDR4			BPS	DDR4		DDR4		DDR4		DDR4	Y						POR&Validated
		DDR4		DDR4	BPS	DDR4		DDR4				DDR4		DDR4		DDR4		DDR4	Y						POR&Validated
		DDR4		DDR4		DDR4		DDR4	BPS			DDR4		DDR4		DDR4		DDR4	Y					One x1	POR&Validated
		DDR4		DDR4		DDR4		DDR4				DDR4	BPS	DDR4		DDR4		DDR4	Y					One x1	POR
		DDR4		DDR4		DDR4		DDR4				DDR4		DDR4		DDR4	BPS	DDR4	Y					One x1	POR
		DDR4	BPS	DDR4		DDR4		DDR4				DDR4		DDR4		DDR4		DDR4	Y					One x1	POR
		DDR4		DDR4		DDR4	BPS	DDR4				DDR4		DDR4		DDR4		DDR4	Y					One x1	POR
8+4	1LM+AD MM	DDR4		DDR4	BPS	DDR4		DDR4	BPS		BPS	DDR4		DDR4	BPS	DDR4		DDR4	Y					One x4	POR&Validated
		DDR4		DDR4	BPS	DDR4	BPS	DDR4				DDR4	BPS	DDR4	BPS	DDR4		DDR4	Y					Two x2	POR
		DDR4	BPS	DDR4		DDR4		DDR4	BPS		BPS	DDR4		DDR4		DDR4	BPS	DDR4	Y					Two x2	POR
		DDR4	BPS	DDR4		DDR4	BPS	DDR4				DDR4	BPS	DDR4		DDR4	BPS	DDR4	Y					One x4	POR
8+8		DDR4	BPS	DDR4	BPS	DDR4	BPS	DDR4	BPS		BPS	DDR4	BPS	DDR4	BPS	DDR4	BPS	DDR4	Y					One x8	POR&Validated
12+2	1LM+AD	BPS		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		BPS	Y					One x2	POR&Validated
		DDR4	DDR4	DDR4	DDR4	BPS		DDR4	DDR4		DDR4	DDR4		BPS	DDR4	DDR4	DDR4	DDR4	Y						POR&Validated
		DDR4	DDR4	BPS		DDR4	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	DDR4		BPS	DDR4	DDR4	Y						POR
		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	BPS				BPS	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	Y	Y	Y	Y	Y		POR

2.3.7 硬盘标号

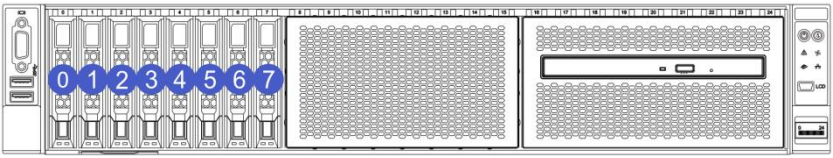
- 2U8 盘位 3.5 寸盘机型



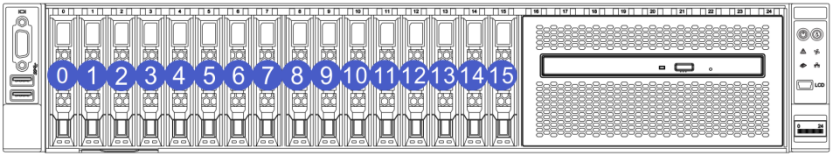
- 2U12 盘位 3.5 寸盘机型



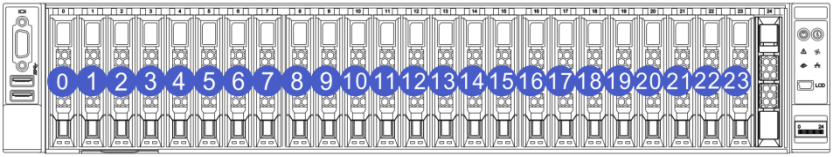
- 2U8 盘位 2.5 寸盘机型



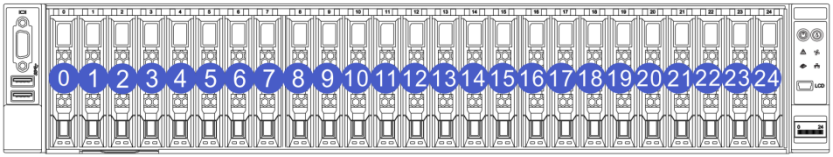
- 2U16 盘位 2.5 寸盘机型



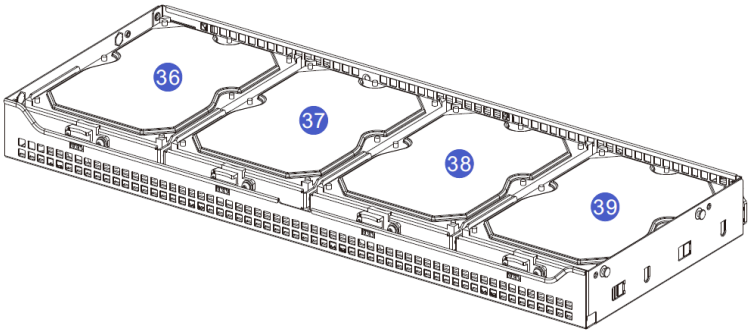
- 2U24 盘位 2.5 寸盘机型



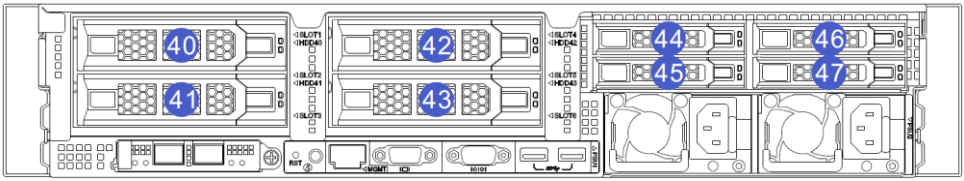
- 2U25 盘位 2.5 寸盘机型



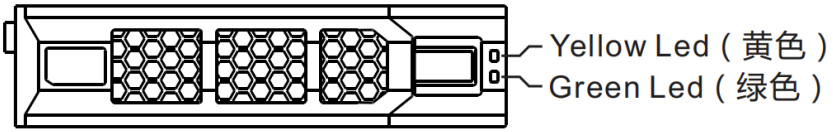
- 内置 4*3.5 硬盘标号



- 后置硬盘标号

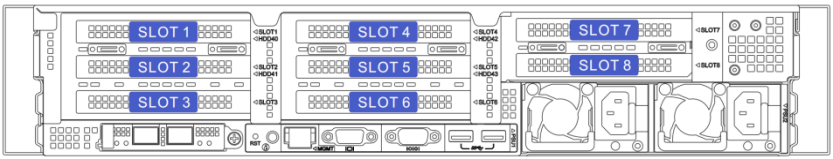


2.3.8 硬盘指示灯



硬盘状态	硬盘 Active 指示灯（绿色）	硬盘 Fault 指示灯（黄色）
硬盘不在位	熄灭	熄灭
硬盘在位，但没有数据活动	常亮	熄灭
硬盘在位，且正常活动	闪烁	熄灭
硬盘故障	常亮	常亮
硬盘被定位	常亮	闪烁（4Hz）
硬盘处于 Rebuild 状态	常亮	闪烁（1Hz）

2.3.9 PCIe 插槽分布后视图



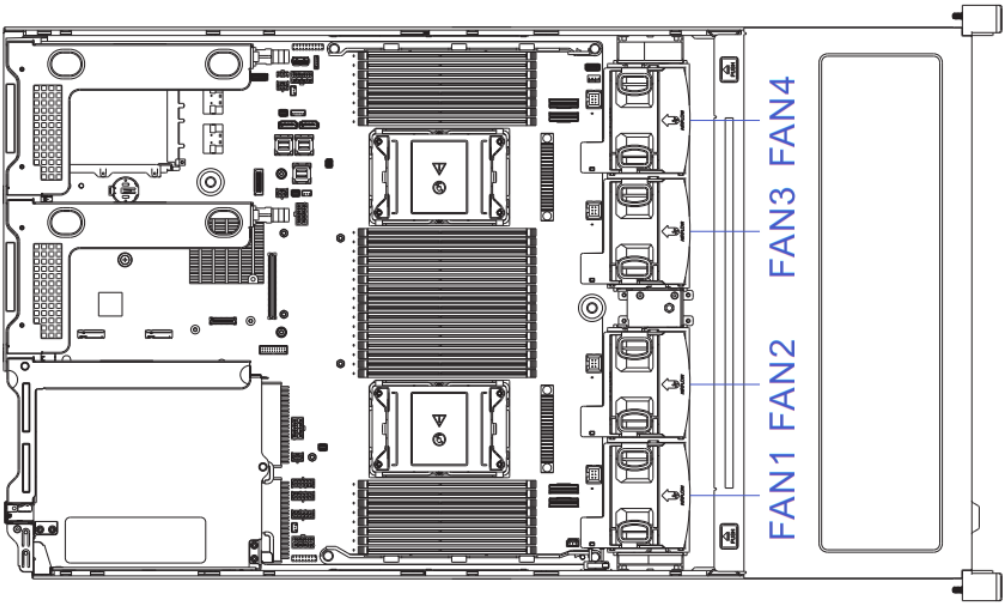
IO模组1提供的槽位为Slot 1 ～ Slot 3；
IO模组2提供的槽位为Slot 4 ～ Slot 6；
IO模组3提供的槽位为Slot 7 ～ Slot 8。

IO模组1与IO模组2可配置的规格相同，可以配置成硬盘模组或者PCIe扩展模组，当配置成3.5”硬盘模组时，Slot 1～Slot 3（Slot 4～Slot 6）不能接任何其他PCIe扩展卡；当配置成2.5”硬盘模组时，Slot 1～Slot 2（Slot 4～Slot 5）被占用，只能在Slot 3或Slot 6扩展1* PCIe X16；当配置成PCIe扩展模组时，可选2*PCIe X16或1*PCIe X16+2*PCIe X8。

IO模组3可以配置成硬盘模组或者PCIe扩展模组，当配置成2.5”硬盘模组时，Slot 7 ～ Slot 8不能接任何其他PCIe扩展卡；当配置成PCIe扩展模组时可选2*PCIe X16或2* PCIe X8；

2.3.10 系统风扇

服务器支持可变的风扇速度。一般情况风扇以最低速度转动，如果服务器温度升高，风扇会提高速度来降温。



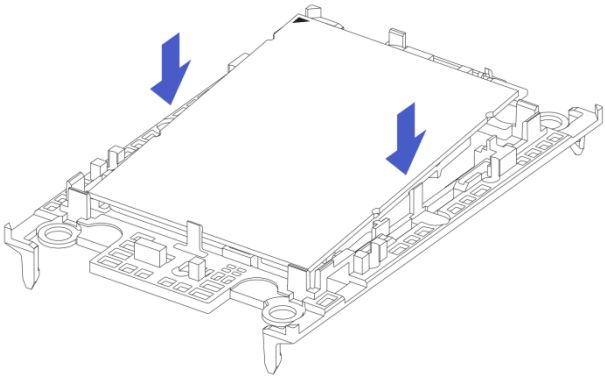
第三章安装系统组件

3.1 CPU 的安装

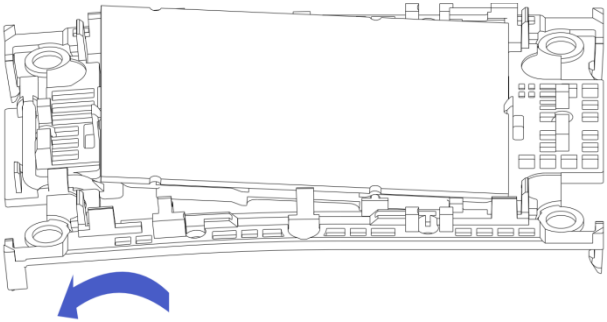
安装处理器：

步骤 1：CPU 安装

1-1.按图示倾斜CPU角度，卡在夹持片一端上，CPU的A1角（三角标志）要与夹持片上有三角形孔的一角对齐，确保处理器上的凹槽对准夹持片卡扣上的突起。



1-2.沿箭头方向，弯曲压夹持片另一端，将CPU固定到夹持片上。

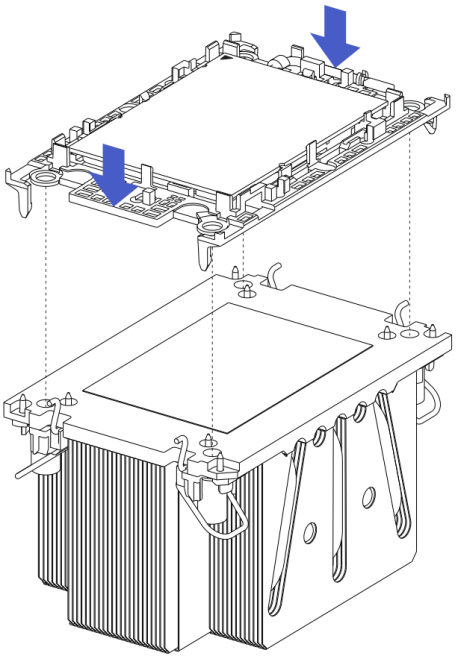


1-3.松开夹持片，使夹持片另一端卡扣勾住CPU凹槽；

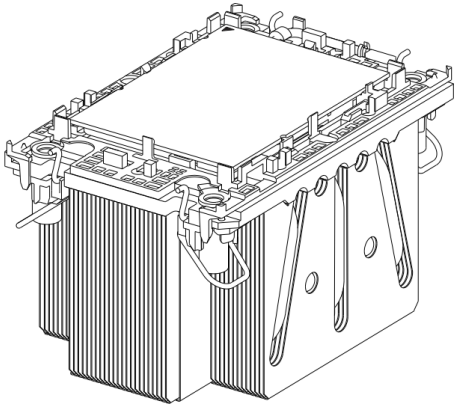
步骤 2：将 CPU 安装到散热器上，保证 CPU 和散热器表面干净无油无异物。

2-1.CPU 上涂抹大概 0.4ml 体积的导热硅脂，均匀抹平。

2-2.对齐 A1 角（三角标志），将 CPU 扣在散热器上。



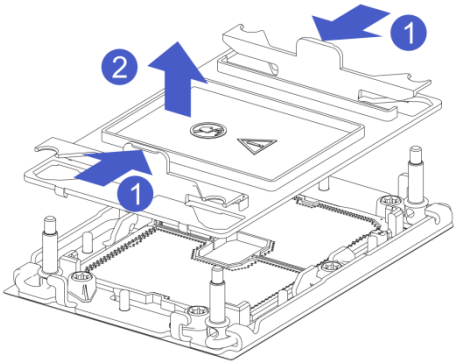
2-3.仔细检查夹持片与散热器的安装情况，保证夹持片完全卡紧和平整。



3.2 散热器的安装

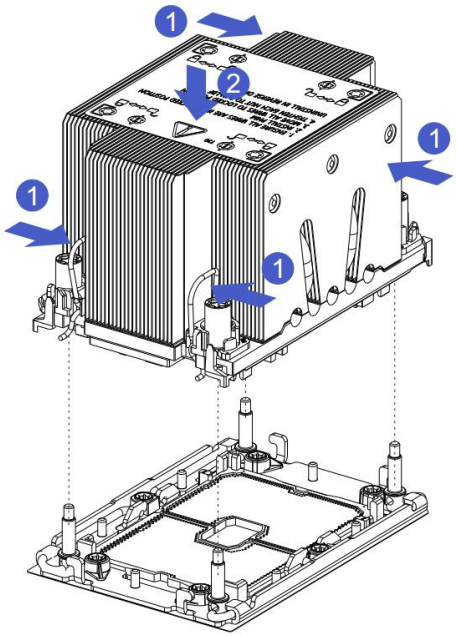
- 安装步骤：

1.沿箭头方向按住保护盖，向上拆卸保护盖。

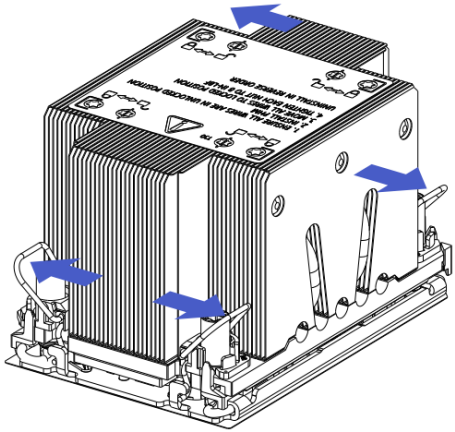


2.按箭头方向拨动散热器上的紧固锁扣，紧固锁扣处于竖直状态，将散热器与 CPU 底座上的散热器固定螺柱对齐，垂直向下放置在底座上。

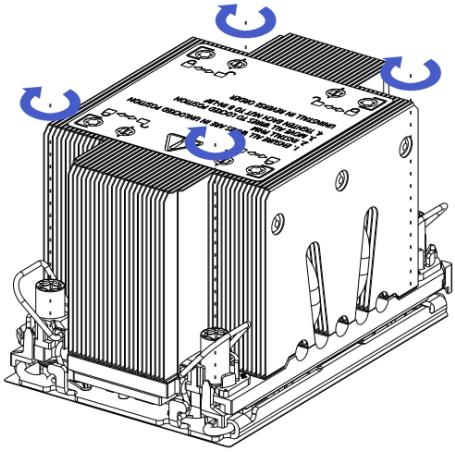
注意：主板上的插针极为脆弱，容易损坏。为避免损坏主板，请勿触摸处理器或处理器插槽触点。



3.按箭头方向按下散热器上的紧固锁扣，使之与处理器底座的卡钩卡住。



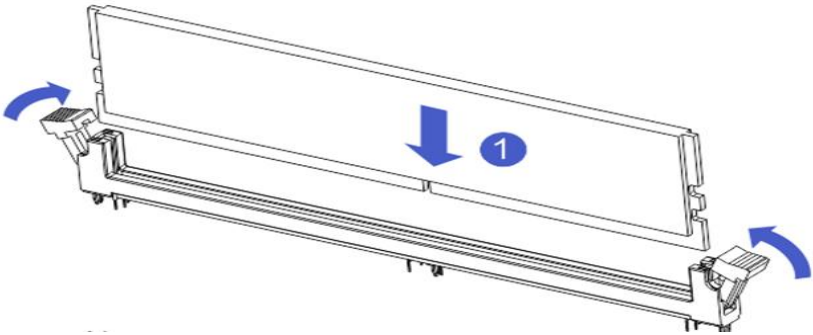
4.使用 T30 梅花螺丝刀拧紧固定散热器的螺钉。

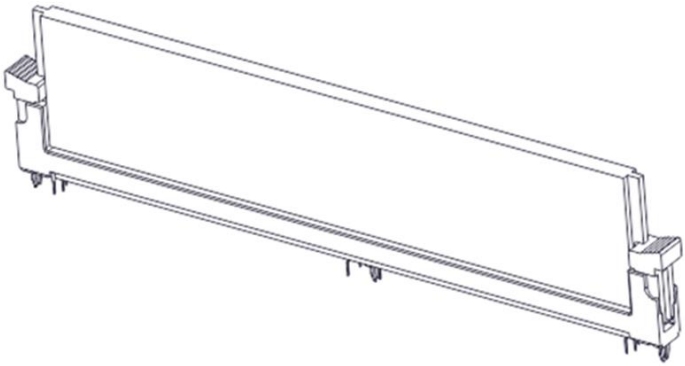


3.3 内存的安装

步骤1 打开内存插槽两侧的扳手，将内存对准内存插槽，需要注意内存条上的缺口与内存插槽的对应；

步骤2 用力将内存垂直卡入内存插槽中，直至听到内存扳手锁定的声音。



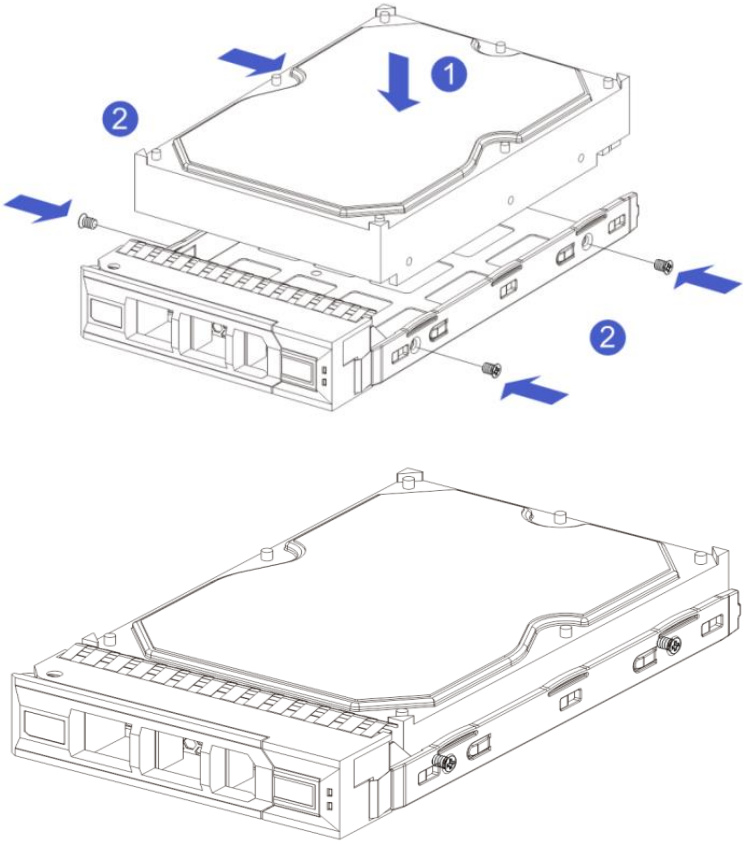


3.4 硬盘的安装

安装 3.5 寸硬盘

1-1. 将硬盘放置托盘中

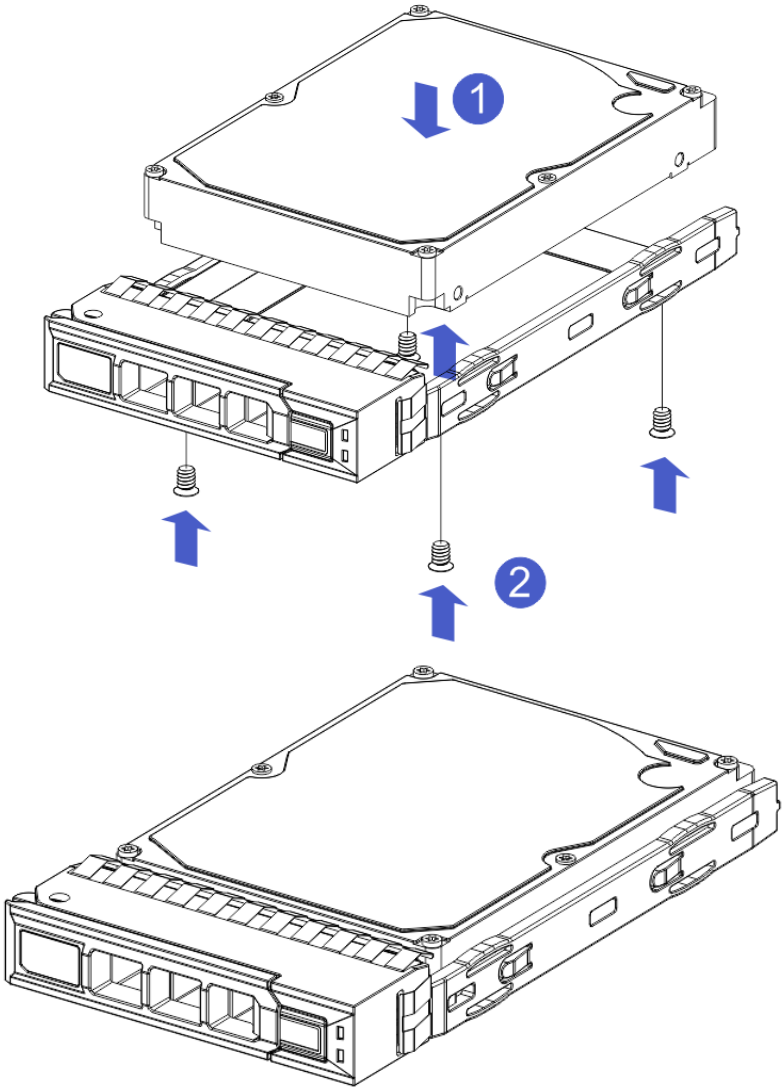
1-2. 左右两侧共 4 颗沉头螺钉锁紧硬盘（螺钉头不得凸出托盘两侧滑道表面）



安装 2.5 寸硬盘

1-1. 将硬盘放置托盘中

2-2. 底部 4 颗沉头螺钉锁紧硬盘（螺钉头凸出托盘底面）

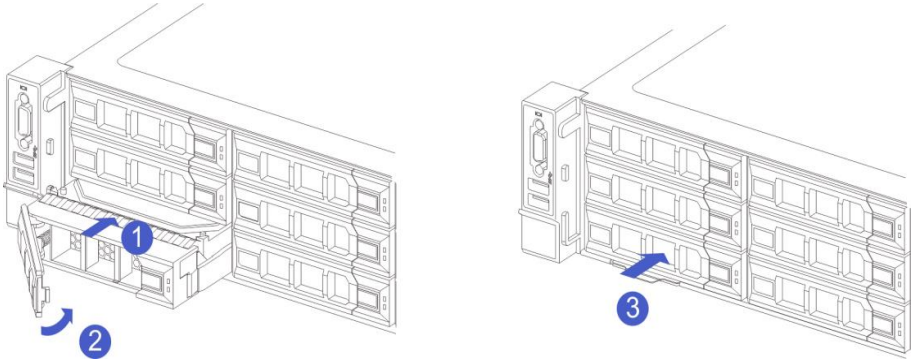


硬盘托盘组件安装到机箱中

1. 硬盘扳手打开的状态下，推入机箱

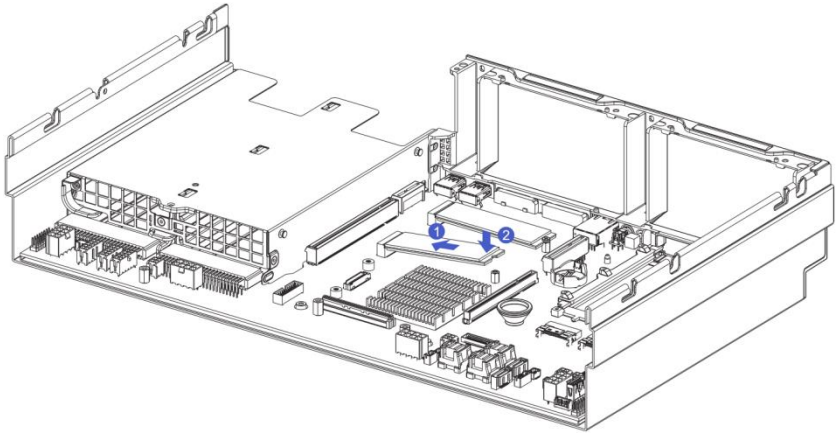
2. 当硬盘金手指触碰到背板器件的时候，按箭头方向转动扳手

3. 硬盘安装到位示意图

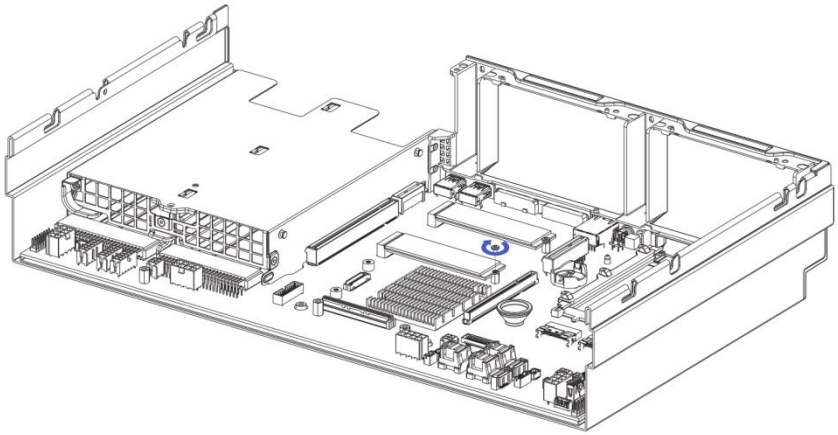


3.5 M.2 SSD 的安装

1-1.按图示，将 M.2 卡连接器端倾斜插入主板连接器中，按压 M.2 卡的另外一端至定位螺柱平面。



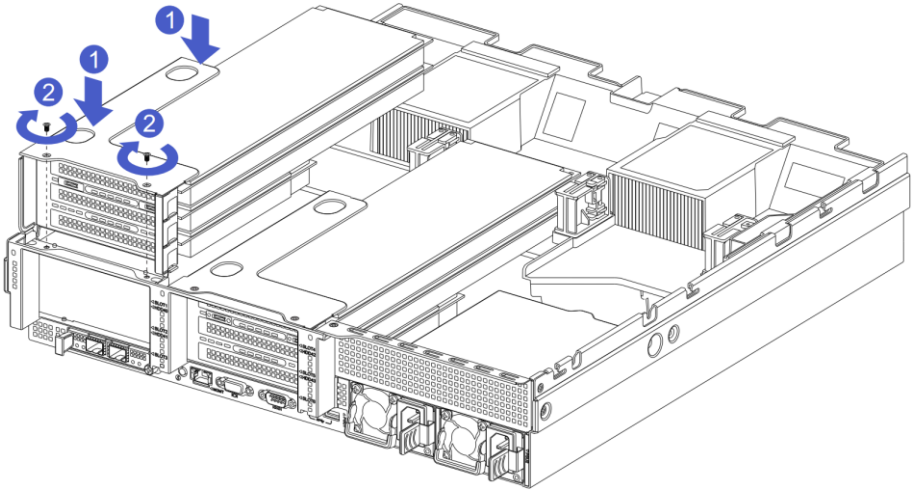
1-2.安装 M.2 卡的固定螺丝。



3.6 IO1 和 IO2 模组安装

- IO1 及 IO2 模组 1（3xPCIe&2PCIe 模块）的安装方法：

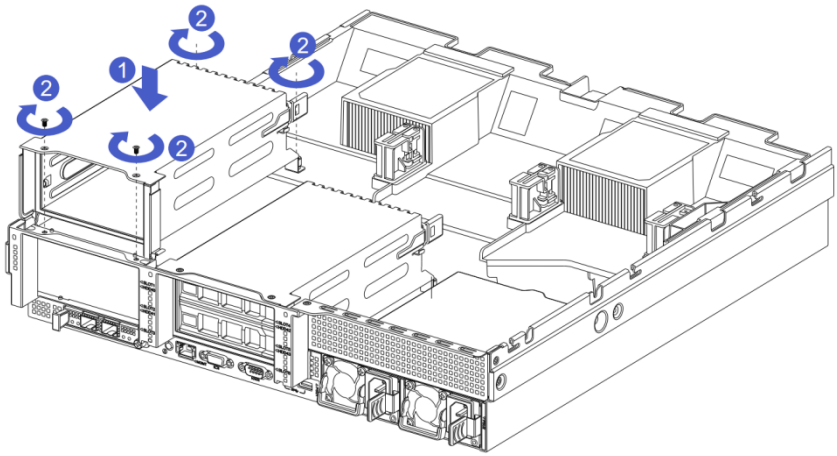
步骤 1. 后窗 PCIe 组件，垂直向下放置对准 PCIe 插槽，对准定位孔，放置与后窗平齐。
步骤 2. 使用十字螺丝刀拧紧固定模块的螺钉。



- IO1 及 IO2 模组 2（2x3.5 硬盘模块）的安装方法：

步骤 1.硬盘盒垂直向下放置与后窗平齐。

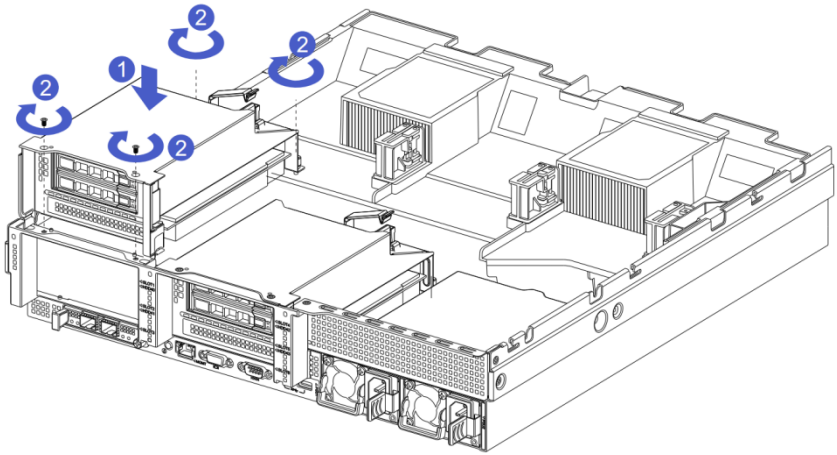
步骤 2.使用十字螺丝刀拧紧固定模块的螺钉。



- IO1 及 IO2 模组 3（2x2.5 硬盘+PCIe 模块）的安装方法：

步骤 1.硬盘盒垂直向下放置与后窗平齐。

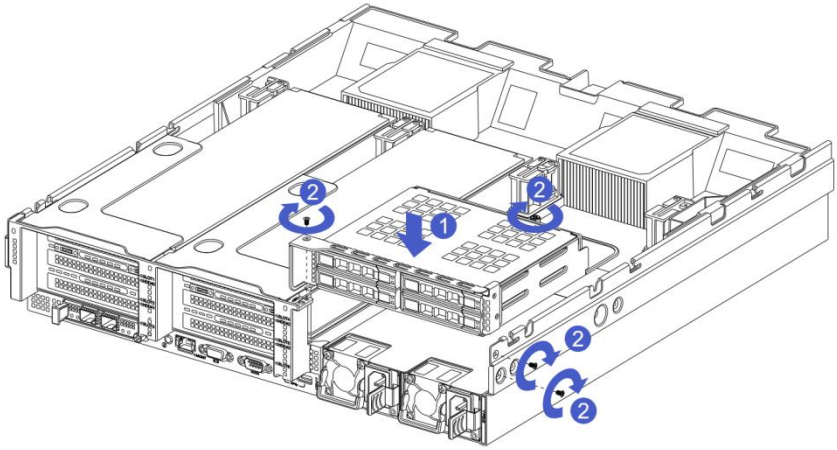
步骤 2.使用十字螺丝刀拧紧固定模块的螺钉。



3.7 IO3 模组安装

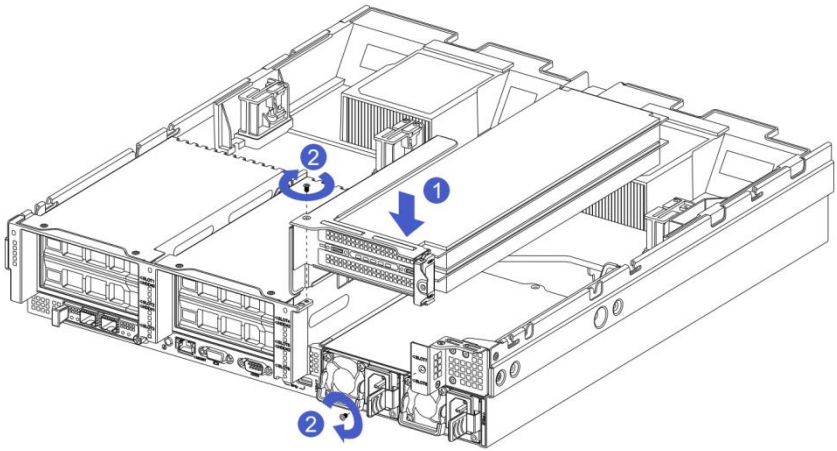
- IO3 模组 1（4x2.5 寸硬盘盒）的安装方法：

1-1.垂直向下放置，对准下端的导向钉。
1-2.放置平整后，使用十字螺丝刀拧紧固定模块的螺钉。



- IO3 模组 2（2xPCIe 全高模块）的安装方法：

1-1.垂直向下放置，对准下端的导向钉。
1-2.放置平整后，使用十字螺丝刀拧紧固定模块的螺钉。

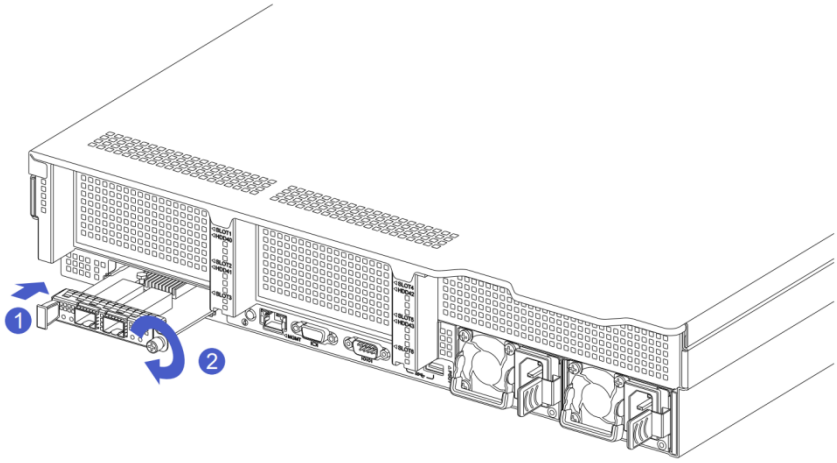


3. 8 网络模块的安装

步骤：安装 OCP 扩展网卡

1-1. 将 OCP 扩展网卡对准机箱后窗滑道推入，直至不能推动，检查松不脱螺钉安装面是否与后窗面贴紧。

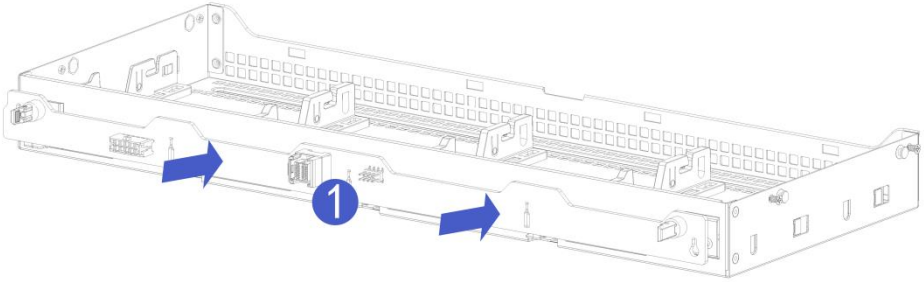
1-2.用十字螺丝刀拧紧灵活 IO 卡的固定螺钉。



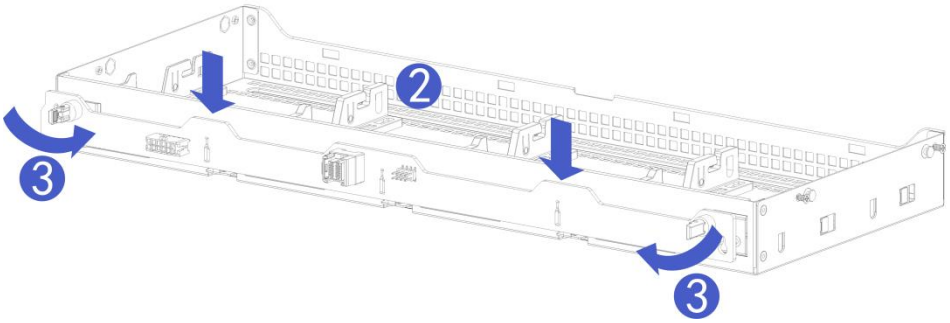
3. 9 内置硬盘模块的安装

- 内置硬盘背板安装

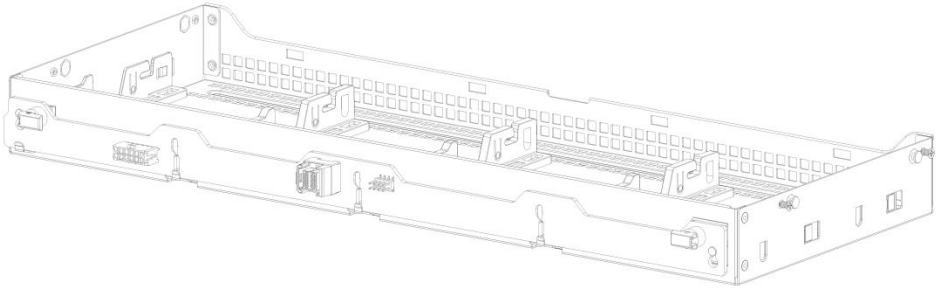
1-1.硬盘背板左右两侧的葫芦孔和挂孔对齐硬盘框架的挂钉，按箭头方向推进



1-2. 在硬盘背板推到底到位后，向下按压背板，直到两侧的葫芦钉和挂孔全部到位

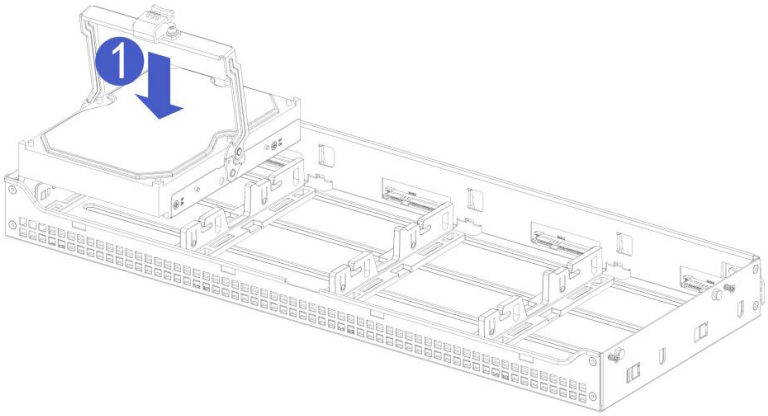


1-3.翻转硬盘背板上左右两侧的固定件使固定件中的销钉落入孔中，完成安装。

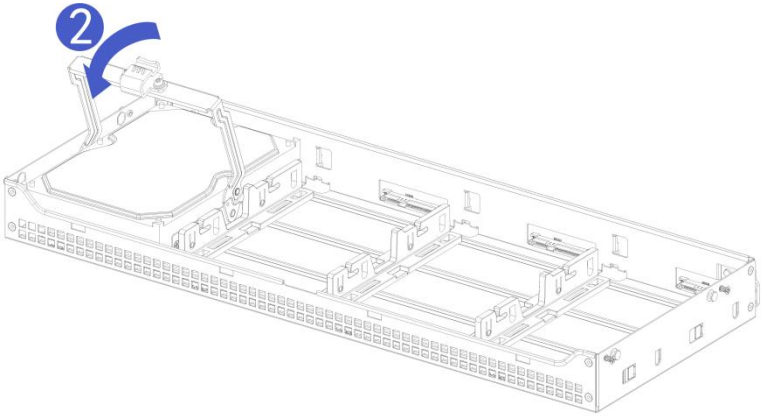


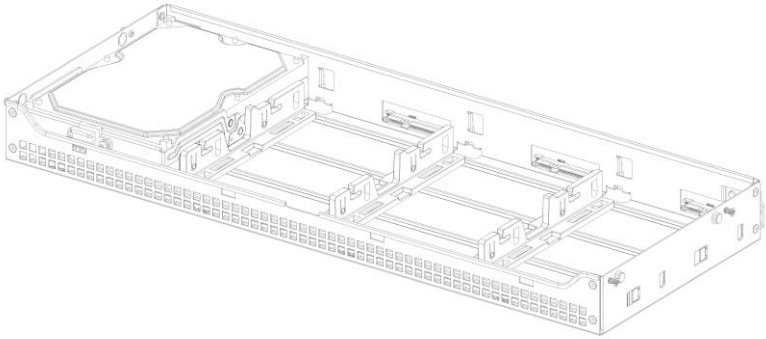
- 内置硬盘托盘安装

1-1. 将内置硬盘托盘放置内置硬盘支架中



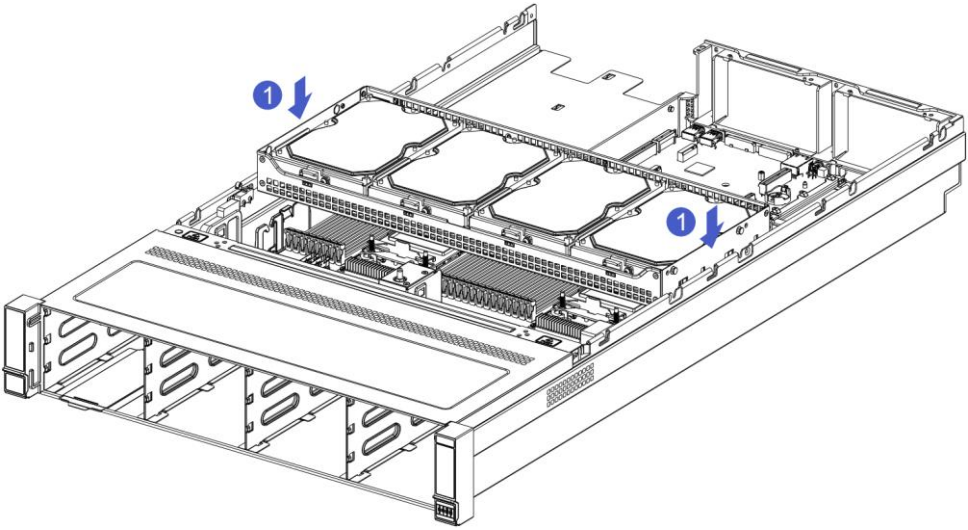
1-2. 按箭头方向转动扳手直至卡勾卡入内置硬盘支架中



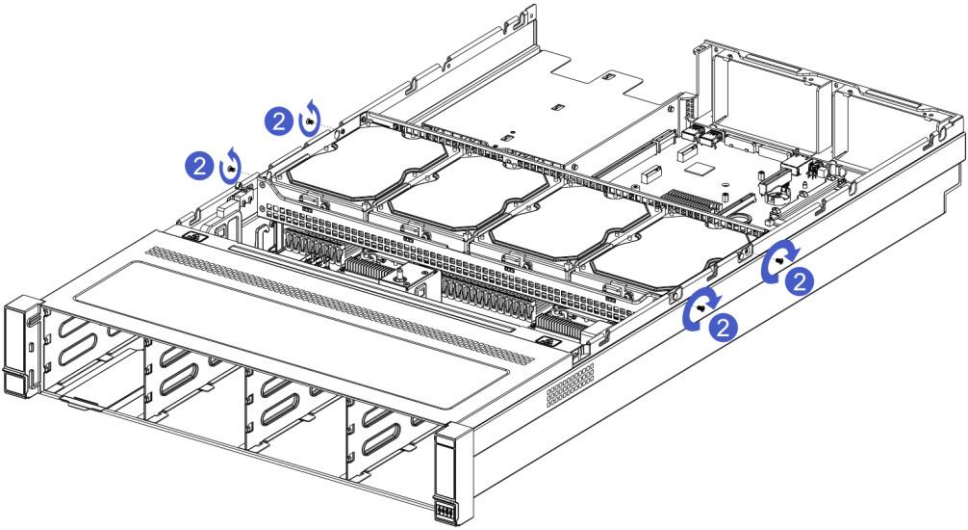


- 内置硬盘模块安装

1-1. 内置硬盘模块对准左右两侧的挂点，垂直向下放置。

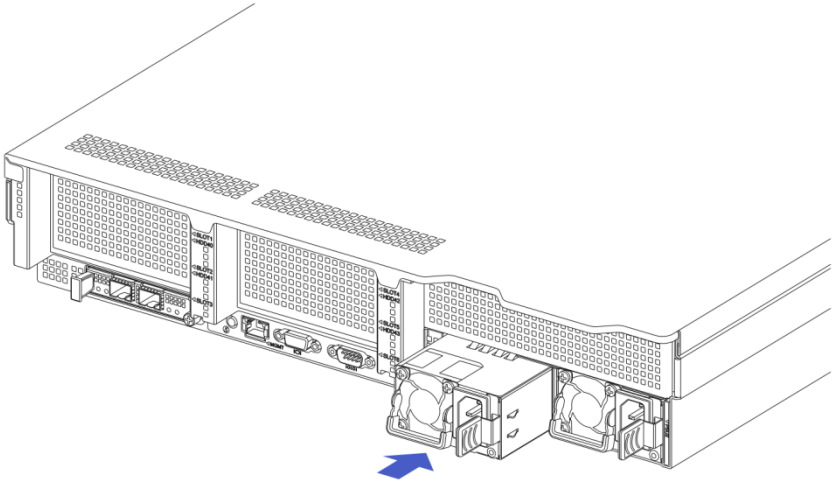


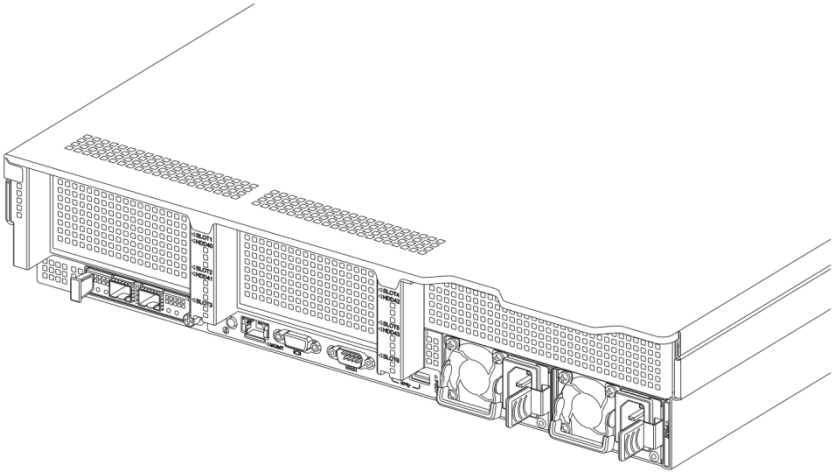
1-2. 锁紧两侧螺钉，完成组装。



3.10 电源模块的安装

步骤：电源按箭头方向推入到底，右侧的弹片扳手发出咔擦一声响后，表示安装到位；





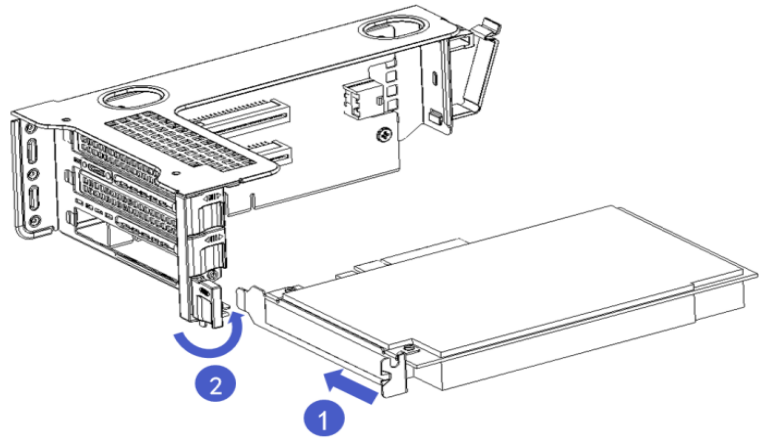
3.11 PCIe 扩展卡的安装

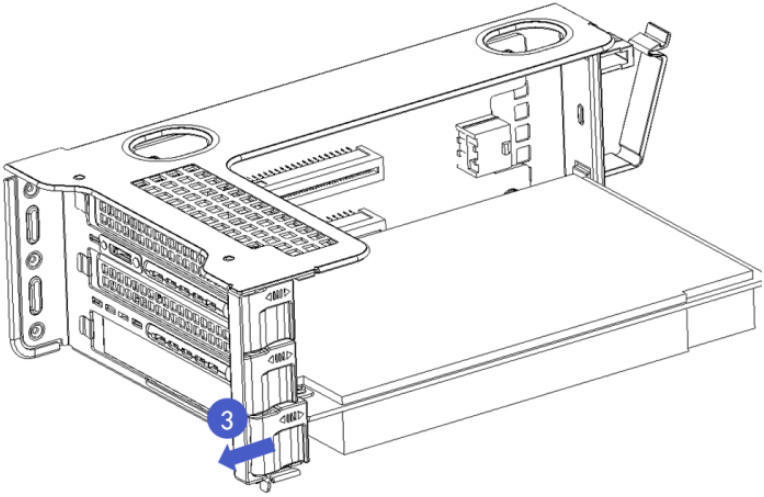
步骤：安装 PCIe 卡

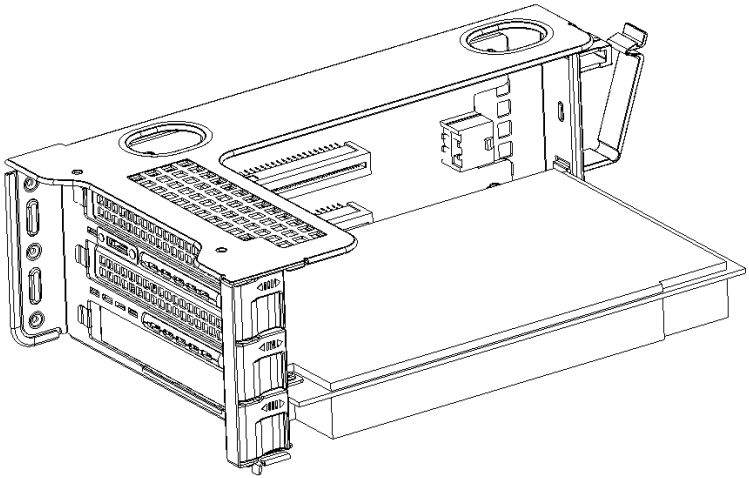
1-1. 按图示意方向装入 PCIe 卡

1-2. 旋转 PCIe 卡锁扣

1-3. 按箭头方案，将 PCIe 卡锁扣锁止

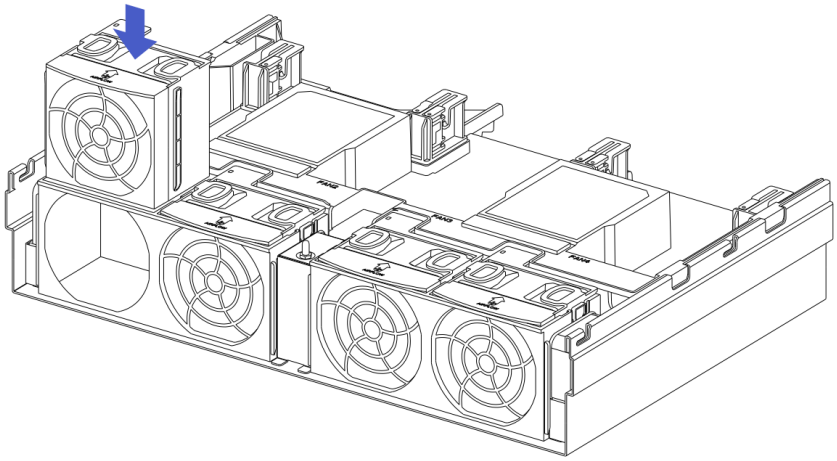

2
1

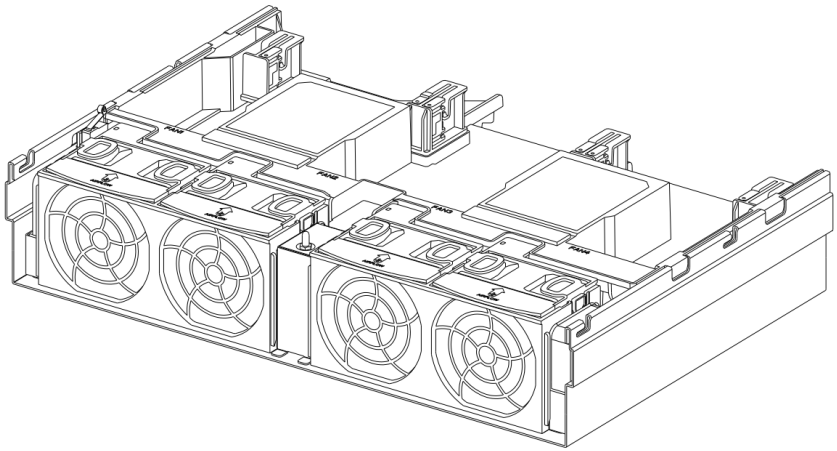

3



3.12 风扇模块安装

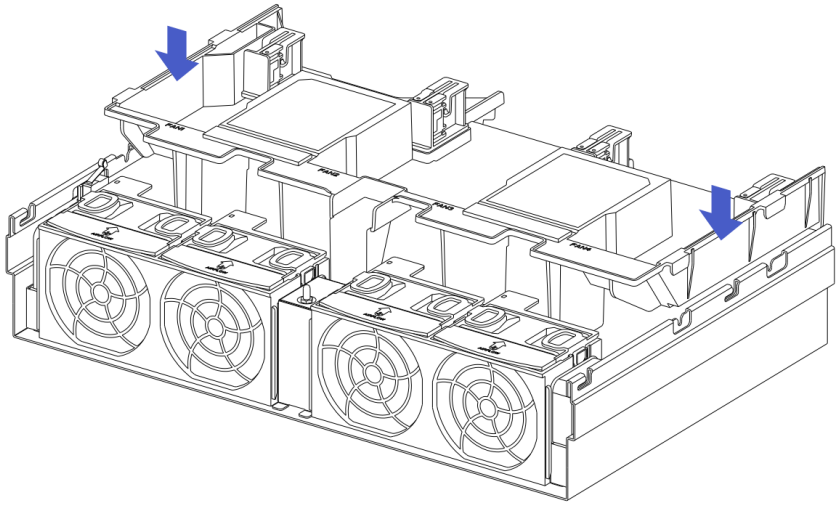
步骤：风扇模块按箭头（注意风扇模块朝向）方向垂直向下放置到位即可





3.13 导风罩安装

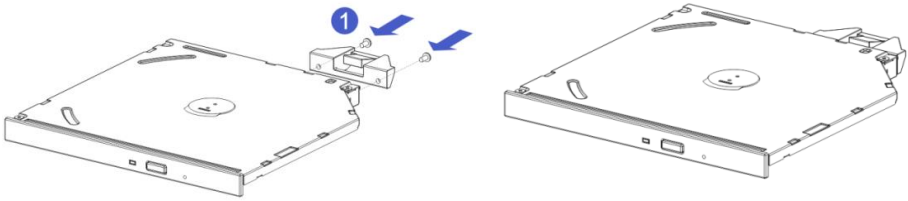
步骤：导风罩模块对准左右两侧的挂点，垂直向下放置-高度低于箱体高度



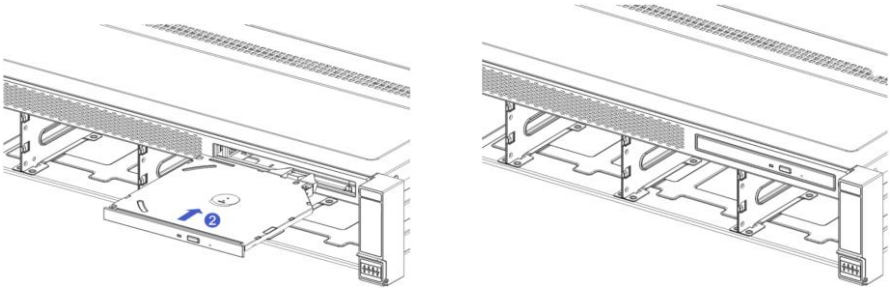
3.14 光驱安装

步骤：安装光驱

1-1. 按箭头方向安装光驱的固定件，锁紧盘头螺钉

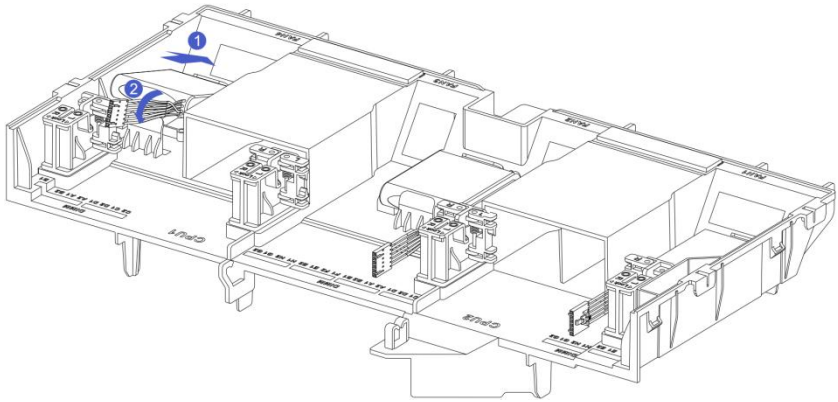


1-2. 对齐机箱上光驱位置开口，按箭头方向推入光驱至固定件自动锁住即可。



3.15 LSI 9361 电池包安装

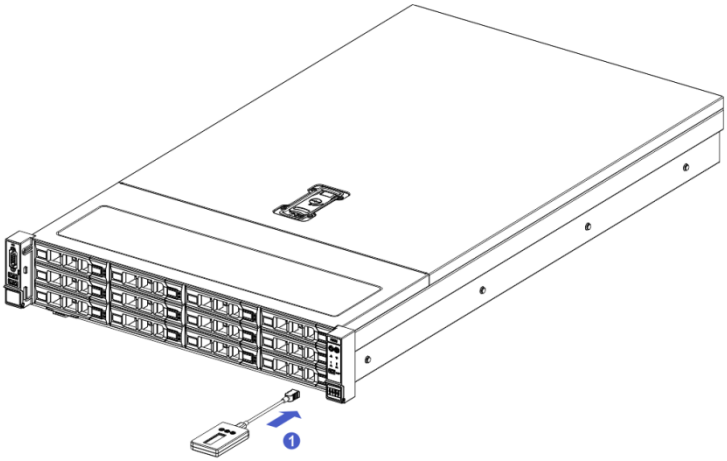
步骤：导风罩上面有三处电池包放置处，按箭头方向对准导风罩上电池包安装槽位放置 LSI 9361 电池包。

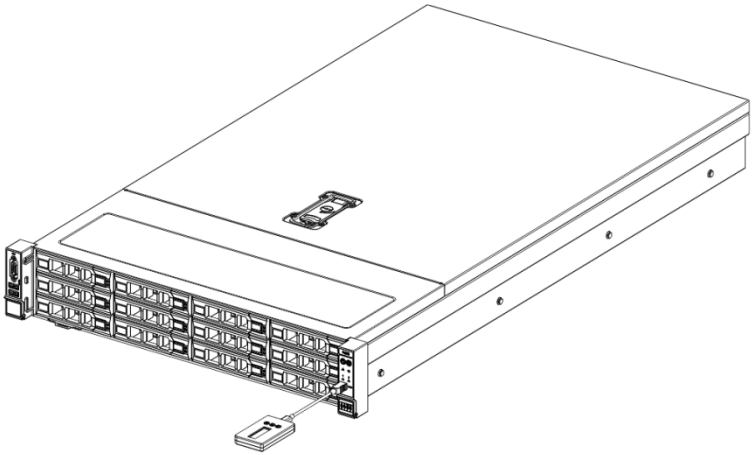


3.16 LCD 模块安装

步骤：LCD 模块安装

1-1.将接好线缆的 LCD 模块连接到机箱挂耳的 LCD 接口

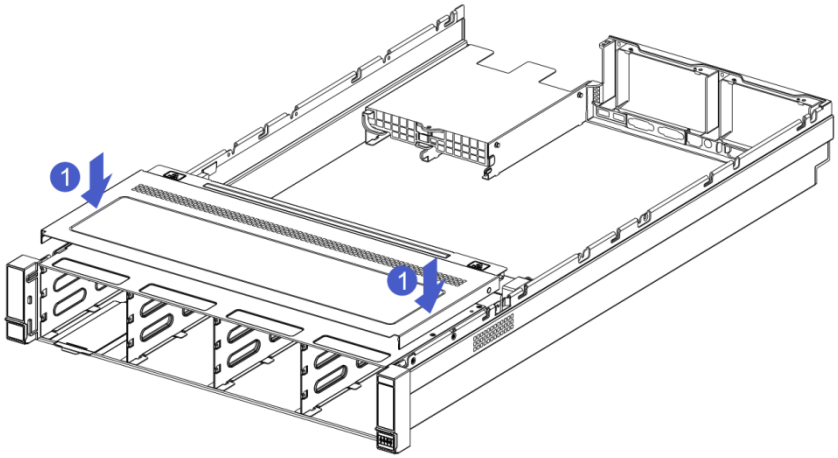




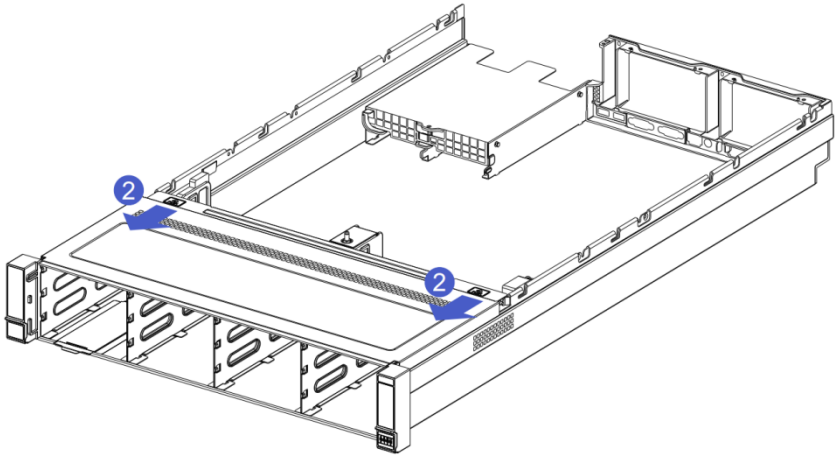
3.17 机箱上盖安装

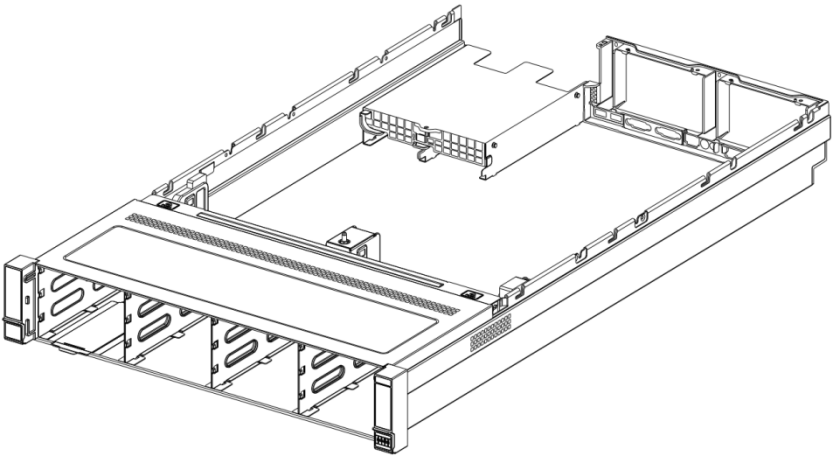
步骤 1：安装机箱前上盖

1-1. 上盖挂钉对齐箱体的开口位置，向下放置。



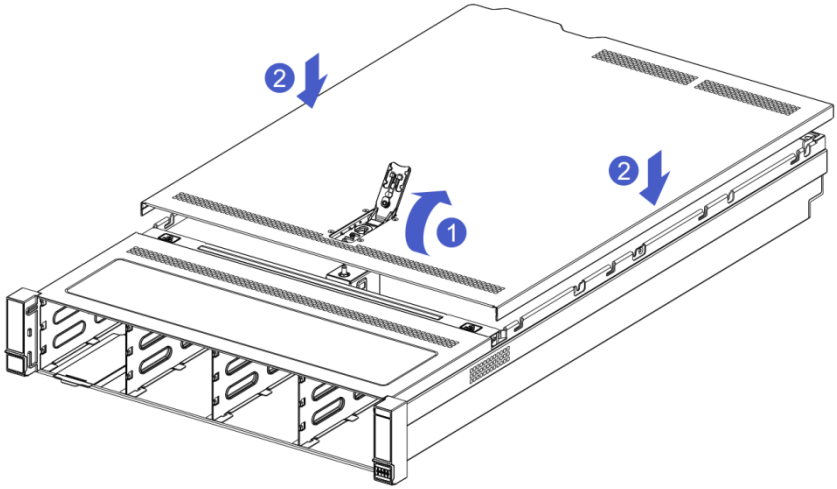
1-2.按箭头方向推进到前上盖与机箱前端面平齐及两侧锁扣咔的一声锁止到位。



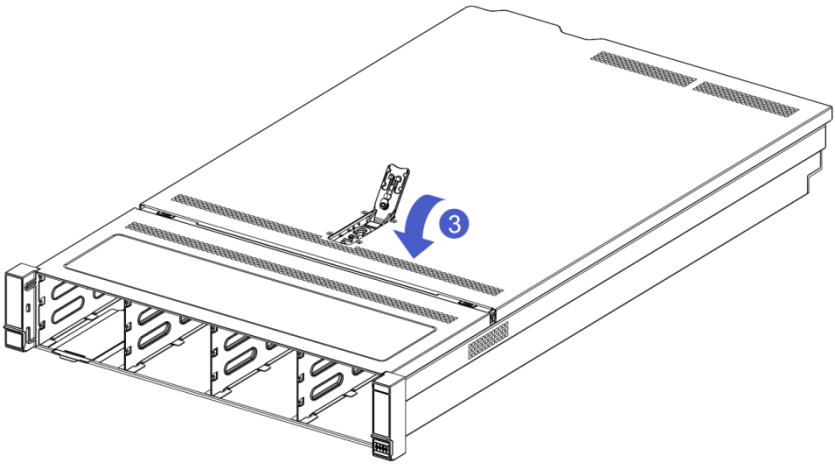


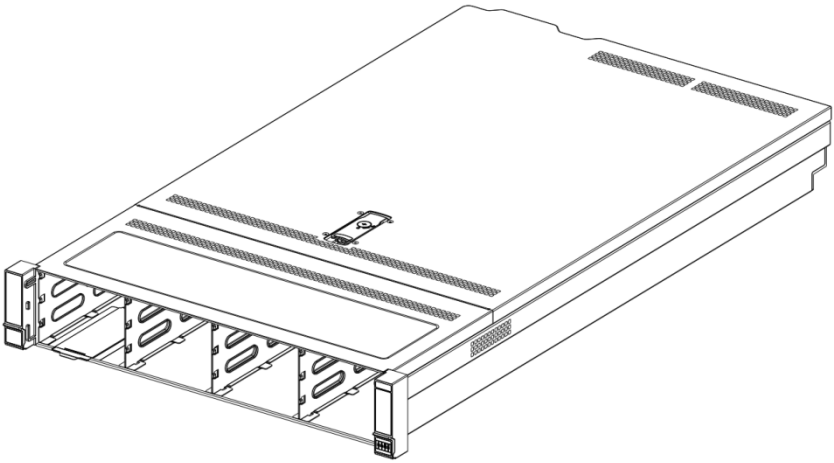
步骤 2：安装机箱后上盖

2-1.按箭头方向打开机箱锁扣，将上盖挂钉对齐箱体的开口位置，向下放置。



2-2.按箭头方向旋转上盖锁扣，锁止到位。





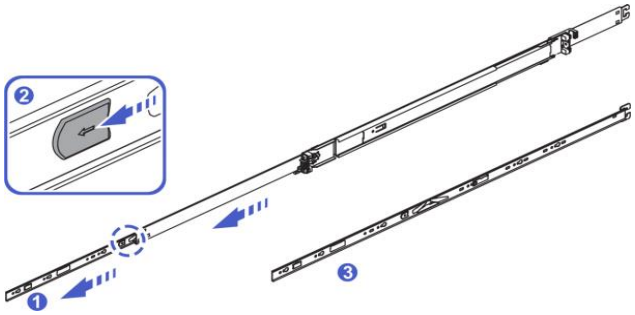
3.18 导轨组件安装

步骤 1.从导轨中取出内轨后，将中轨推入导轨中

1-1.将内轨从导轨中向外抽出，能够听见咔嚓一声响后止位

1-2.按照箭头方向推动白色按键同时向外完全抽出内轨

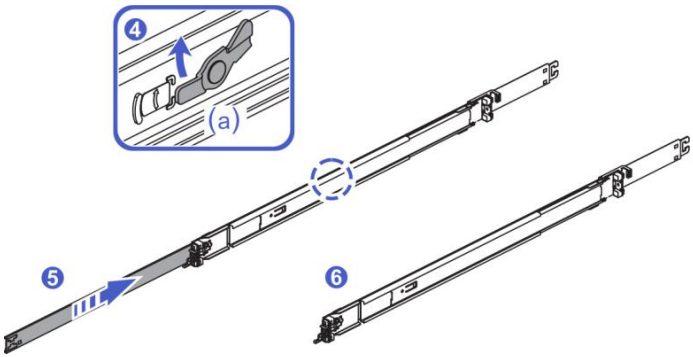
1-3.完成取出内轨



1-4. 按照箭头方向推动导轨中的 a 卡扣

1-5. 同时将中轨推入滑轨中

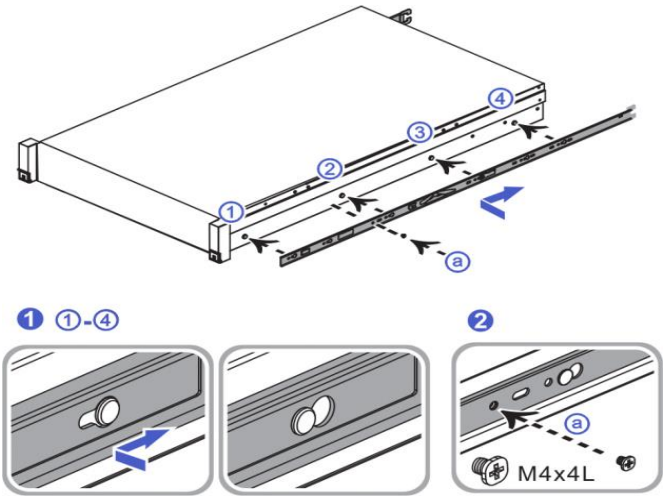
1-6. 完成步骤 1



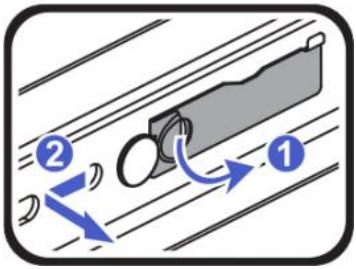
步骤 2. 安装内轨到机箱上(左右内轨一样，请重复安装）

2-1. 将内轨的 ①-④ 定位孔对准机箱一侧的 4 个挂钉，按照图示安装内轨到机箱上，安装完成能够听见咔嚓一声响，需保证安装到位.

2-2. 在机箱 a 处，将附件中的 M4x4 螺钉锁入机箱 a 处。完成步骤 2



注：将内轨从机箱中取出时，需解锁内轨中的卡扣如图所示



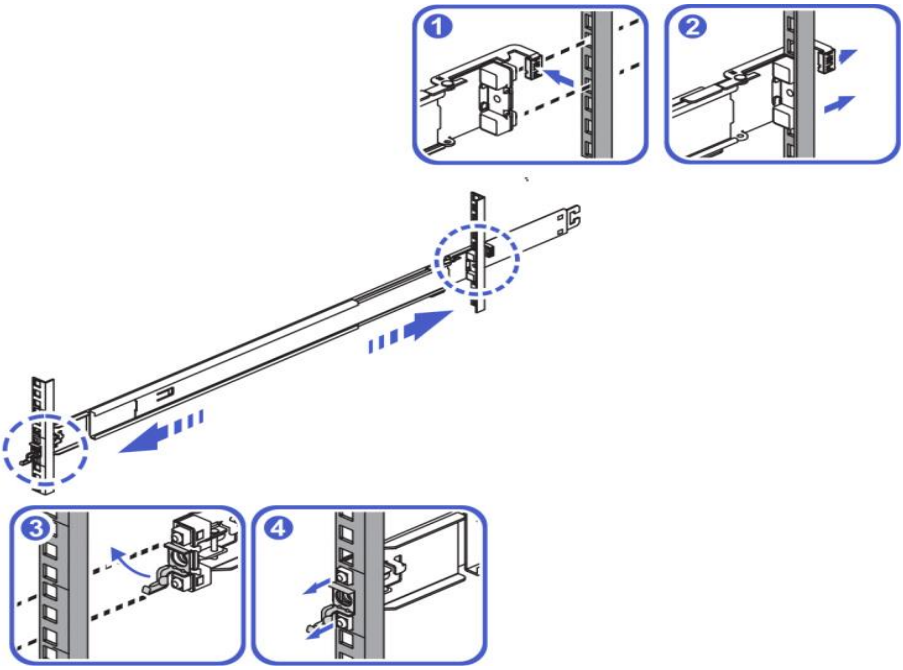
步骤 3. 安装导轨到机架内（左右导轨对称，请重复安装）

3-1. 按照箭头指示推动导轨后端卡勾，对准机架孔位将导轨装入机架。

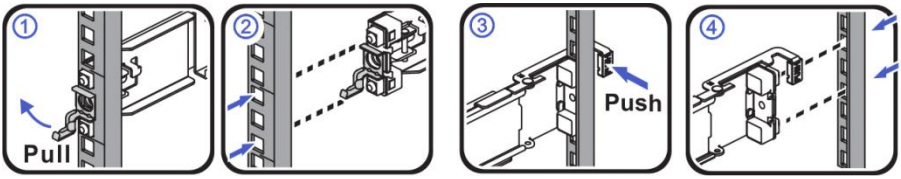
3-2. 将导轨装入机架后端听见咔嚓响声后完成导轨后端安装.

3-3. 按照箭头指示推动导轨前端卡勾，对准机架孔位将导轨装入机架。

3-4. 将导轨装入机架前端听见咔嚓响声后，完成步骤 3。



注：将导轨从机架中取出时，需解锁导轨中的卡扣如图所示



步骤 4. 安装服务器到机架中.

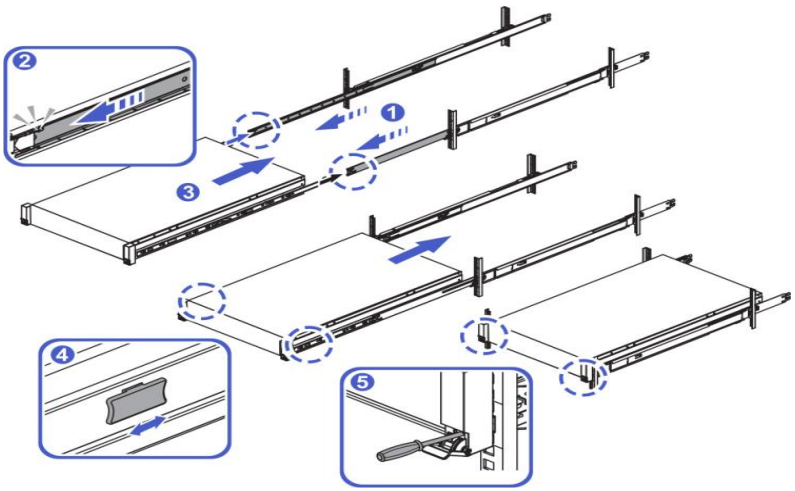
4-1. 将安装在机架中的两侧中轨抽出，能够听见咔嚓一声响后止位。

4-2. 抬起服务器将导轨内轨对准中轨，按照箭头方向将服务器推入机架,确保内轨顺畅装入中轨。

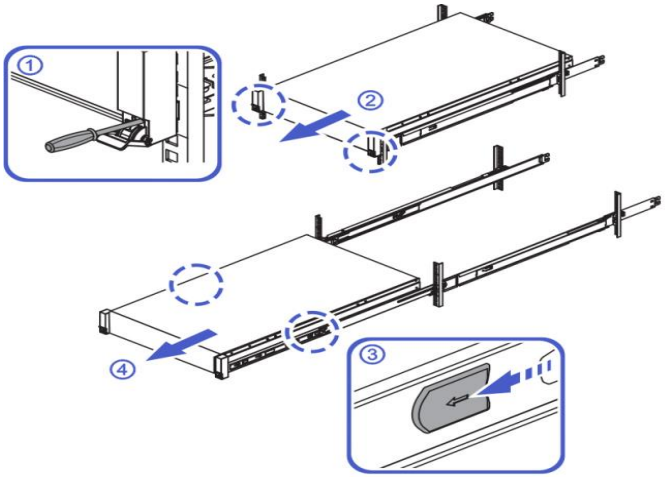
4-3. 将服务器推入到中轨后,能够听见咔嚓一声响后止位.

4-4. 按照箭头方向拨动蓝色按钮,按住按钮同时将服务器推入机架中.

4-5. 掰开两侧前挂耳，使用螺丝刀锁紧螺丝,完成步骤 4.



注：将服务器从机架中取出，需解锁两侧螺丝与白色按键，如图所示



第四章 BIOS 参数设置说明

4.1 概述

BIOS UEFI 固件是遵循 UEFI 2.8 版本的规范要求的标准固件产品。其适用于 TU628 V2 和 TU618 V2 等产品,用于初始化平台的硬件和加载并引导操作系统。本文档适用于本产品 UEFI BIOS 固件，描述了 BIOS 配置界面中选项的功能及相应的设置方法。

基本功能

a) 符合 UEFI 2.8/PI 1.7 规范
b) 支持串口重定向
c) 支持 USB 键盘、鼠标
d) 支持通过 USB 设备安装、启动操作系统
e) 支持 PXE 启动
f) 具备 UEFI BIOS 的其他基本功能

4.2 进入 BIOS 设置界面

6.2.1 概述

设置界面是 UEFI BIOS 提供的用于显示、设置、修改 BIOS 选项的环境，该界面支持 USB/PS2 键盘以及串口重定向操作。

本章描述了设置界面的使用方法。

6.2.2 如何进入 UEFI BIOS 的设置界面

操作步骤：

1. 将服务器主板上电开机，接上键盘；
2. 在 POST 过程，注意观察 Logo 画面左下方进入 BIOS Setup 界面的提示，“Press <DEL> or <ESC> to enter setup, <F7> to enter Boot Menu.”；
3. 按键盘<DEL> 或者 <ESC>键，准备进入 BIOS Setup 界面；

4.3 BIOS 参数设置

本节中对 BIOS 设置界面的参数功能和设置方法进行了介绍，您可以通过该程序对 BIOS 的基本配置进行设置，BIOS 设置不当可能会引起硬件资源的冲突或者降低系统的运行性能，一般建议您使用系统出厂时的默认值。
在改变服务器 BIOS 设置时记录初始设置，以便可以根据记录恢复到初始设置。

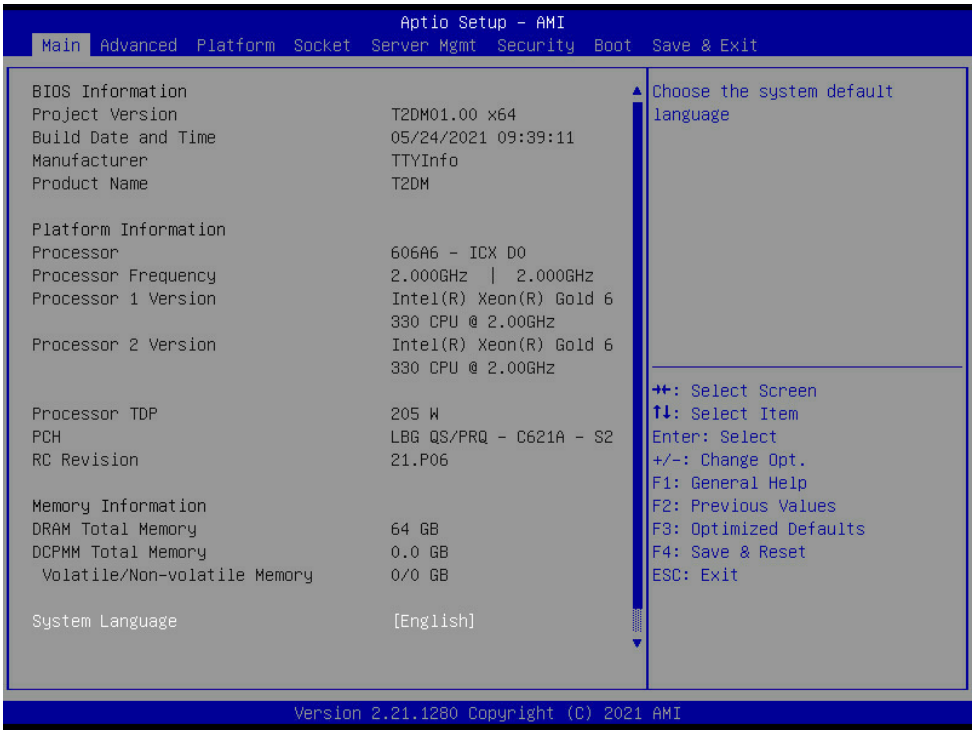
注: 本手册中所涉及的 BIOS 设置方法基于拟制本手册时所使用的 BIOS 版本，客户实际看到的设置界面可能会与本手册图示有差异。

4.3.1 导航键说明

→←:	菜单切换（Select Screen）
↑ ↓:	项目切换（Select Item）
Enter:	确定（Select）
+/-:	改变选项（Change Opt.）
F1:	通用帮助信息（General Help）
F2:	上一次保存值（Previous Values）
F3:	默认优化值（Optimized Defaults）
F4:	保存修改并重启系统（Save & Reset）
ESC:	退出（Exit）

4.3.1 Main 菜单

Main 界面包含 BIOS 系统的基本信息，如 BIOS 版本号、CPU 型号、内存容量，可以设置系统时间和系统语言。



Server Board Information

Project Version:

显示 BIOS 的版本信息。

Build Date and Time:

显示 BIOS 的发布日期和时间。

Manufacturer:

显示主板制造商。

Product Name:

显示主板型号。

Platform Information

Processor:

CPU ID 和步进信息。

Processor Frequency:

CPU 频率信息。

Processor 1 Version

CPU1 具体型号信息。

Processor 2 Version

CPU2 具体型号信息。

Processor TDP:

CPU TDP。

PCH:

PCH 型号和版本信息

RC Revision:

显示 RC 代码版本信息。

Memory Information:

DRAM Total Memory:

显示 DDR 内存总容量。

DCPMM Total Memory:

显示 Intel 傲腾可持久内存总容量。

Volatile/Non-volatile Memory:

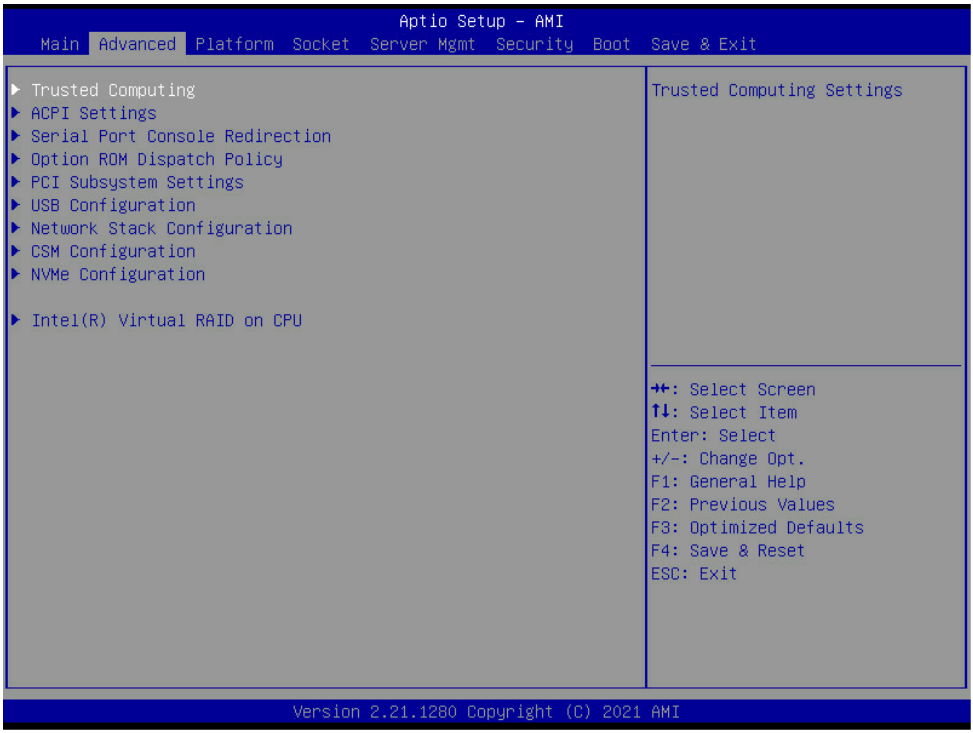
显示 Intel 傲腾可持久内存配置信息

System Language:

用于设置菜单界面语言。

4.3.2 Advanced 菜单

Advanced 菜单允许用户更改 CPU 和其他系统的设置。



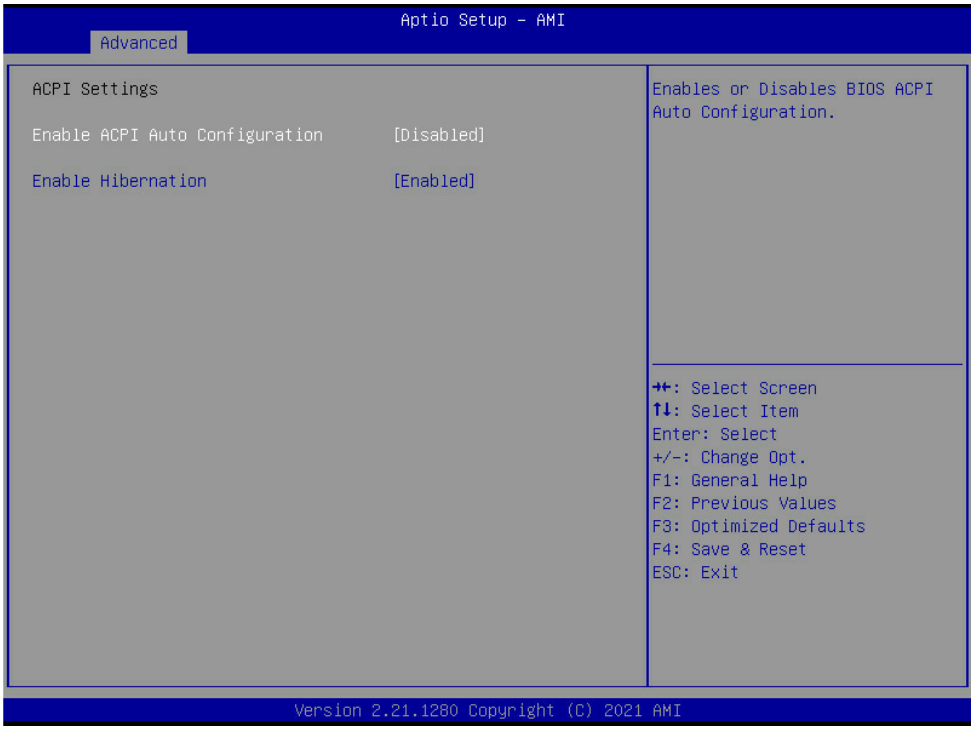
4.3.2.1 Trusted Computing

显示和设置 TCM/TPM 模块信息，不同模块选项设置有差异，用户可根据 Setup 帮助说明进行设置。

未设置管理员密码，不可编辑此菜单。

Aptio Setup – AMI
Advanced
Configuration
Security Device Support [Enable]
NO Security Device Found
Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit
Version 2.21.1280 Copyright (C) 2021 AMI

4.3.2.2 ACPI Settings



Enable ACPI Auto Configuration

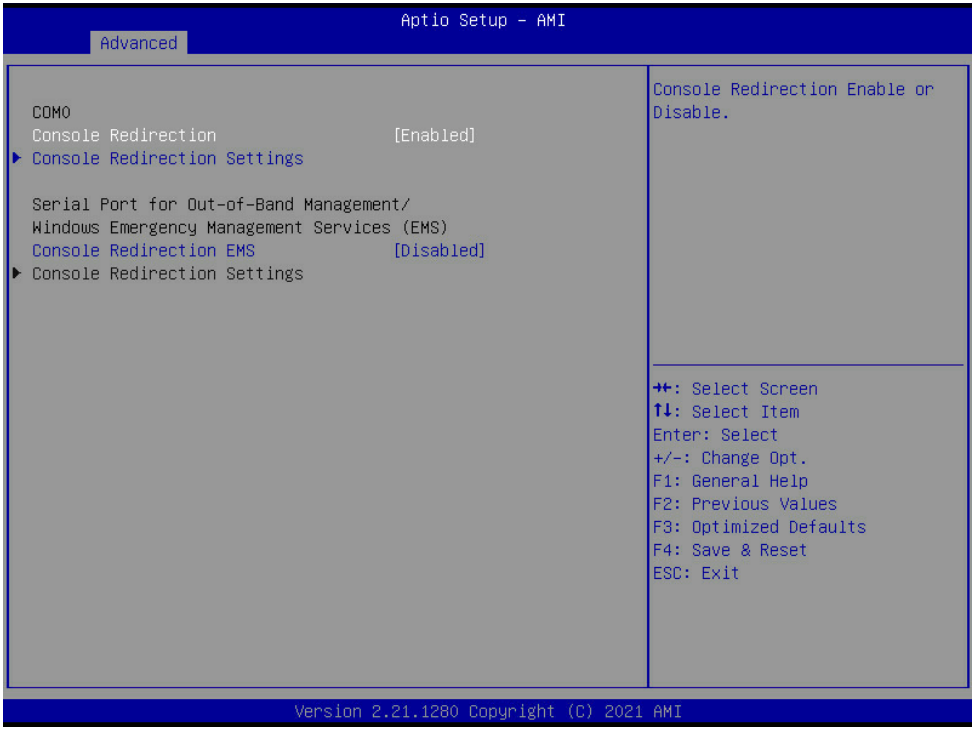
此选项用于启用或禁用 BIOS ACPI 自动配置

Enable Hibernation

此项用于启用或禁用系统休眠功能（OS/S4 睡眠状态）。 该选项在某些操作系统上可能无效。

4.3.2.3 Serial Port Console Redirection

串口重定向配置



Console Redirection

操控台重定向功能开关，将操控台（如显卡）输出到显示器的信息重定向到串口。

●Disabled：关闭重定向功能。

●Enabled：开启重定向功能。

默认值：Enabled

Console Redirection Settings

Terminal Type:

通过此选项可选择仿真类型，BIOS 仿真类型必须与终端程序中选择的模式相匹配。菜单选项为：

●VT100

●VT100+

●VT-UTF8

●ANSI

默认值：VT100

Bits per second

串口重定向速率，取值范围为 9600～115200

默认值：115200

Data Bits

串口重定向数据位长，菜单选项为：

●8

●7

默认值：8

Parity

串口重定向校验开关，菜单选项为：

●None：无校验

●Even：偶校验

●Odd：奇校验

●Mark：校验位始终为 1

●Space：校验位始终为 0

默认值：None

⚠ Mark 和 Space 校验不允许用于侦测错误。

Stop Bits

串口数据包结束标志位，菜单选项为：

●1

●2

默认值：1

Flow Control

串口重定向控制流选择开关，菜单选项为：

●None：关闭串口重定向控制流

●Hardware RTS/CTS：请求发送/清除发送

默认值：None

Recorder Mode

记录模式开关，开启此功能，仅仅文本信息将被发送，菜单选项为：

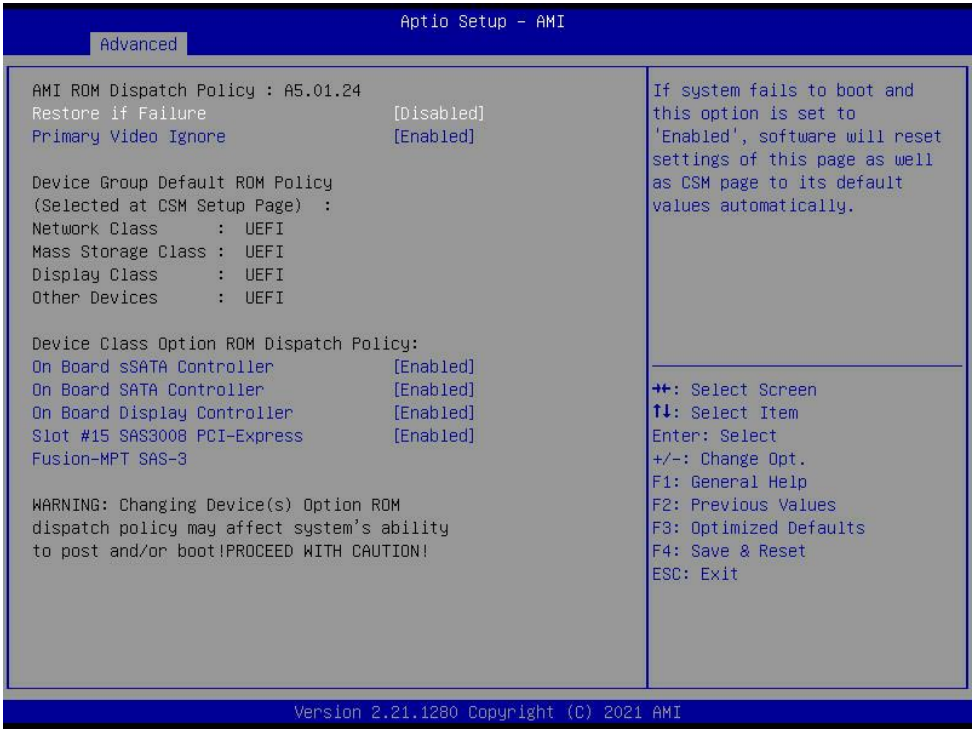
●Enabled：开启

●Disabled：关闭

默认值：Disabled

4.3.2.4 Option ROM Dispatch Policy

显示网络类、存储类、显示类及其他类设备当前 Option ROM 运行策略，UEFI 模式和 Legacy 模式两种。



Restore if Failure

启动失败恢复功能。当在 Option ROM Dispatch Policy 和 CSM 页面，设置选项导致启动失败时，将恢复默认值，菜单选项为：

●Enabled：开启

●Disabled：关闭

默认值：Disabled

Primary Video Ignore

最优先显示设备忽略设置功能。用户将最优先显示设备 OptionROM 关闭时，系

统将忽略此设置，将恢复 Enabled，菜单选项为：

●Enabled：开启

●Disabled：关闭

默认值：Enabled

On board sSATA Controller

板载 sSATA 控制器 OptionROM 运行控制开关。在帮助信息中，提示此设备对 Legacy 和 UEFI 的支持，ROM Policy 为 Legacy 时，关闭开关将停止运行 Legacy OptionROM，ROM Policy 为 UEFI 时，关闭开关将停止运行 UEFI Driver，菜单选项为：

●Enabled：开启

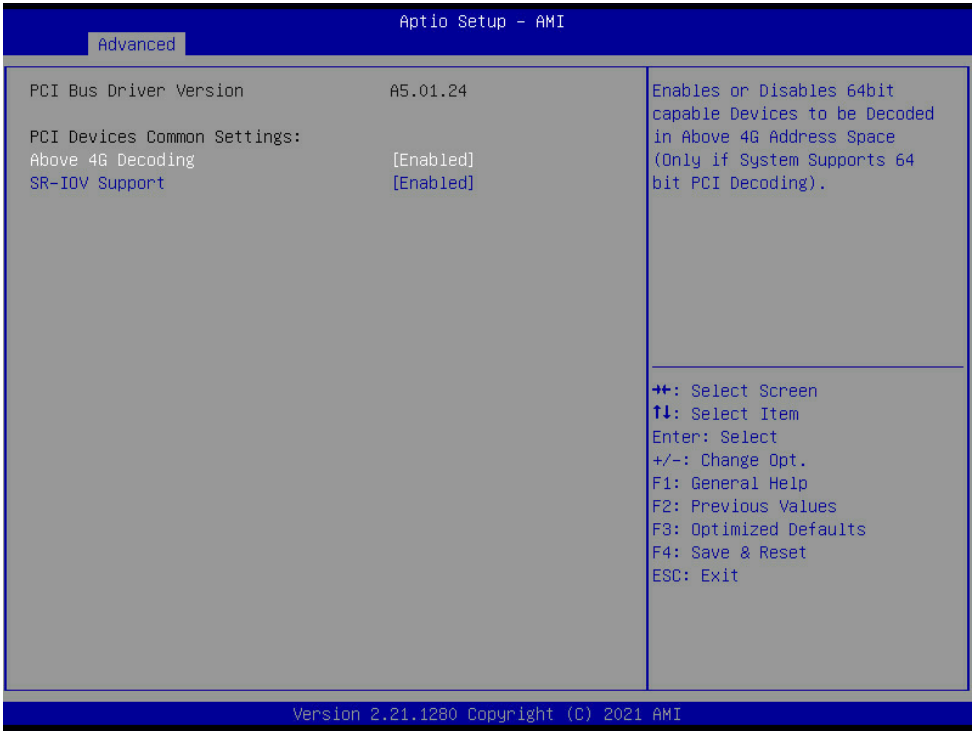
●Disabled：关闭

默认值：Enabled

此界面为动态界面，与实际板载设备和外接设备数量一致。

4.3.2.5 PCI Subsystem Settings

用于 PCI 子系统配置，在此模块可以打开或关闭 4G 以上内存地址访问空间；打开或关闭网卡 SR-IOV 虚拟化功能



Above 4G Decoding

4G 以上内存空间资源解码控制开关，菜单选项为：

●Enabled：开启

●Disabled：关闭

默认值：Enabled

SR-IOV Support

SR-IOV 技术使能开关，菜单选项为：

●Enabled：开启

●Disabled：关闭

默认值：Enabled

4.3.2.6 USB Configuration

显示 USB 控制器和 USB 设备信息。

Legacy USB Support

Legacy 环境 USB 支持控制开关，菜单选项为：

●Enabled：开启

●Disabled：关闭

默认值：Enabled

XHCI Hand-off

改变 XHCI 控制权开关，此功能对不支持改变 XHCI 控制权的操作系统有效。一般由 XHCI 驱动来改变 XHCI 的控制权。

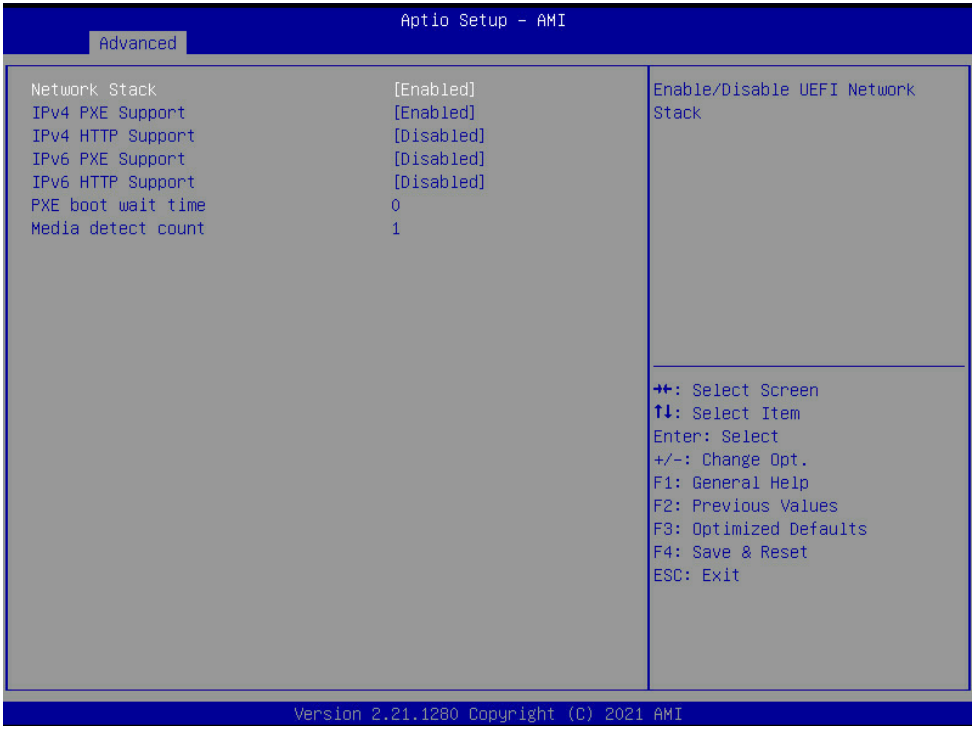
●Enabled：开启

●Disabled：关闭
默认值：Enabled

USB Mass Storage Driver Support
USB 存储设备驱动控制开关，菜单选项为：
●Enabled：开启
●Disabled：关闭
默认值：Enabled

4.3.2.7 Network Stack Configuration

网络协议栈设置：是否支持 IPV4/6 的 PXE 功能



Network Stack

网络堆栈控制开关，菜单选项为：
●Enabled：开启
●Disabled：关闭
默认值：Enabled

Ipv4 PXE Support
Ipv4 UEFI PXE 功能控制开关，菜单选项为：
●Enabled：开启
●Disabled：关闭
默认值：Enabled

Ipv4 HTTP Support
Ipv4 HTTP 功能控制开关，菜单选项为：
●Enabled：开启
●Disabled：关闭
默认值：Disabled

Ipv6 PXE Support
Ipv6 UEFI PXE 功能控制开关，菜单选项为：
●Enabled：开启
●Disabled：关闭
默认值：Disabled

Ipv6 HTTP Support
Ipv6 HTTP 功能控制开关，菜单选项为：
●Enabled：开启
●Disabled：关闭
默认值：Disabled

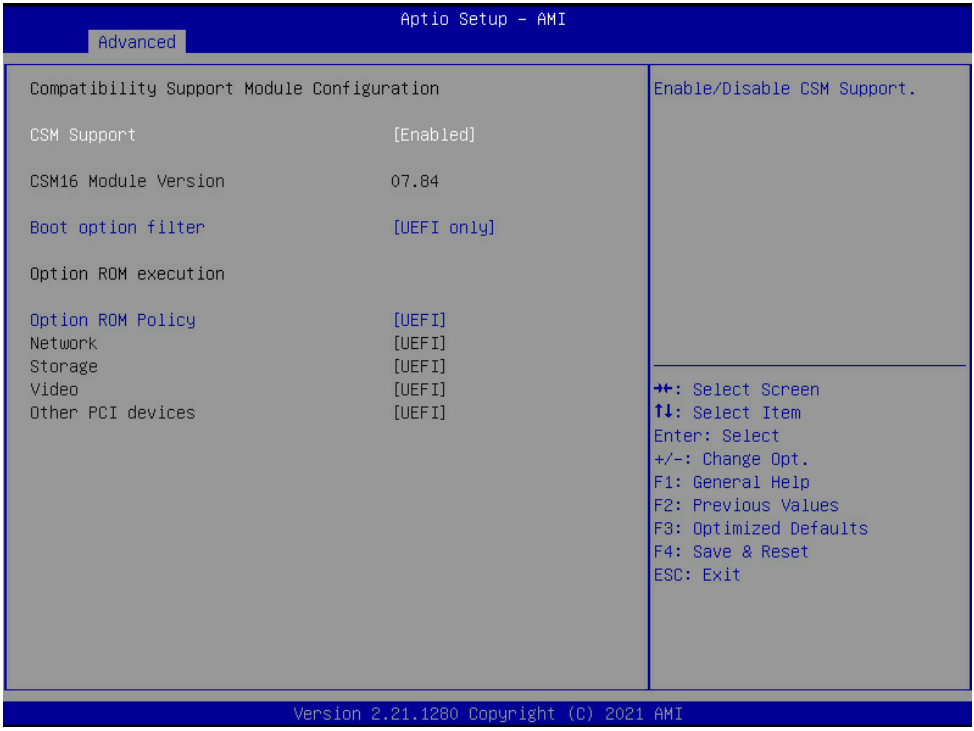
PXE boot wait time
PXE 启动等待时间，用户可输入 PXE 启动等待时间，等待过程可以按“ESC”放弃 PXE 启动，默认为 0。

Media detect count

设备在位侦测次数，用户可输入设备网卡设备侦测次数，默认为 1.

4.3.2.8 CSM Configuration

兼容性模块配置



CSM Support

CSM 模块支持控制开关，菜单选项为：

●Enabled：开启

●Disabled：关闭

默认值：Enabled

Boot option filter

启动选项类控制开关，菜单选项为：

●UEFI and Legacy：UEFI 和 Legacy 启动项

●UEFI only：UEFI 启动项

●Legacy only：Legacy 启动项

默认值：UEFI Only

Option ROM Policy

设备 Option ROM 运行策略控制开关，菜单选项为：

●UEFI：UEFI 模式

●Legacy：Legacy 模式

默认值：UEFI

此选项选择后，网络类、存储类、显示类、及其他类设备将遵循此选择。

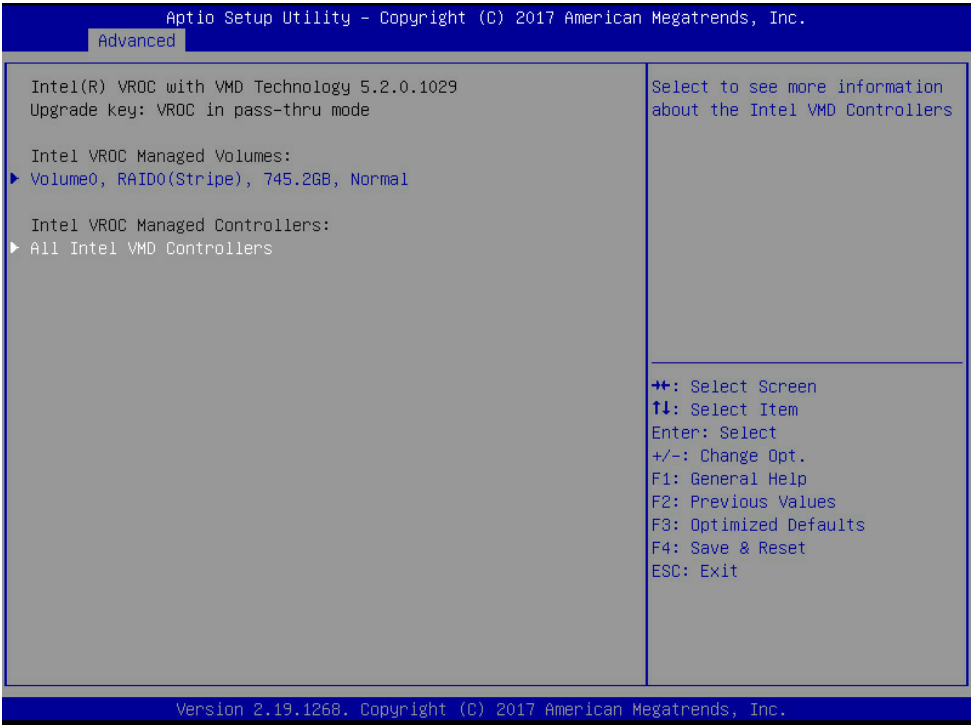
4.3.2.9 NVMe Configuration

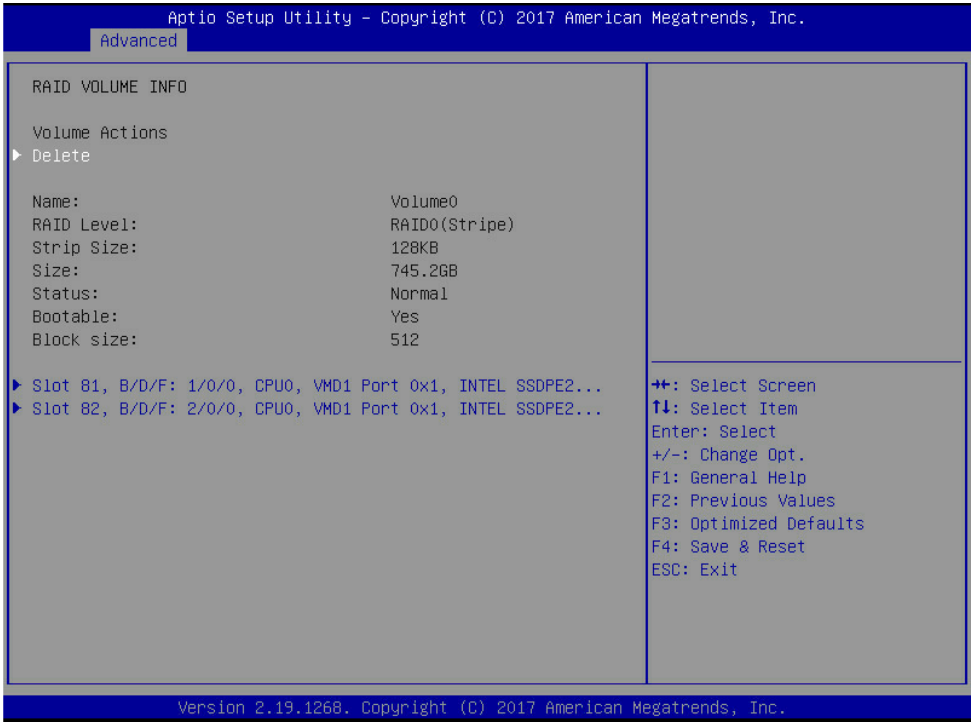
在此页面，可以进行 NVMe 组、更改或配置等设置

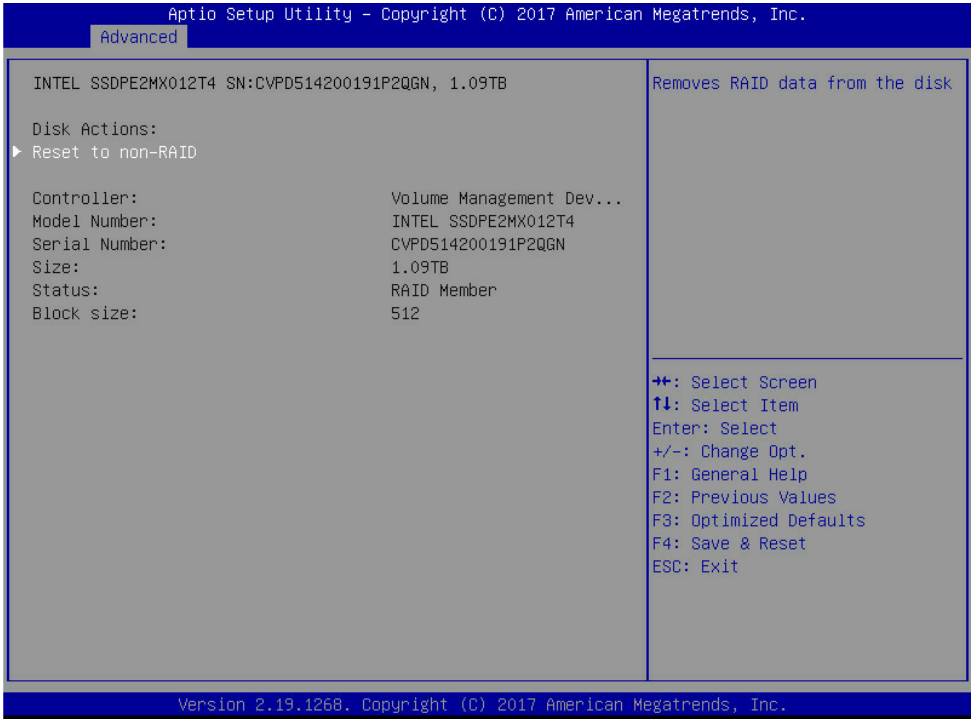
4.3.2.10 Intel® Virtual RAID on CPU

显示和设置 NVMe 接口的硬盘信息以及 RAID 配置。

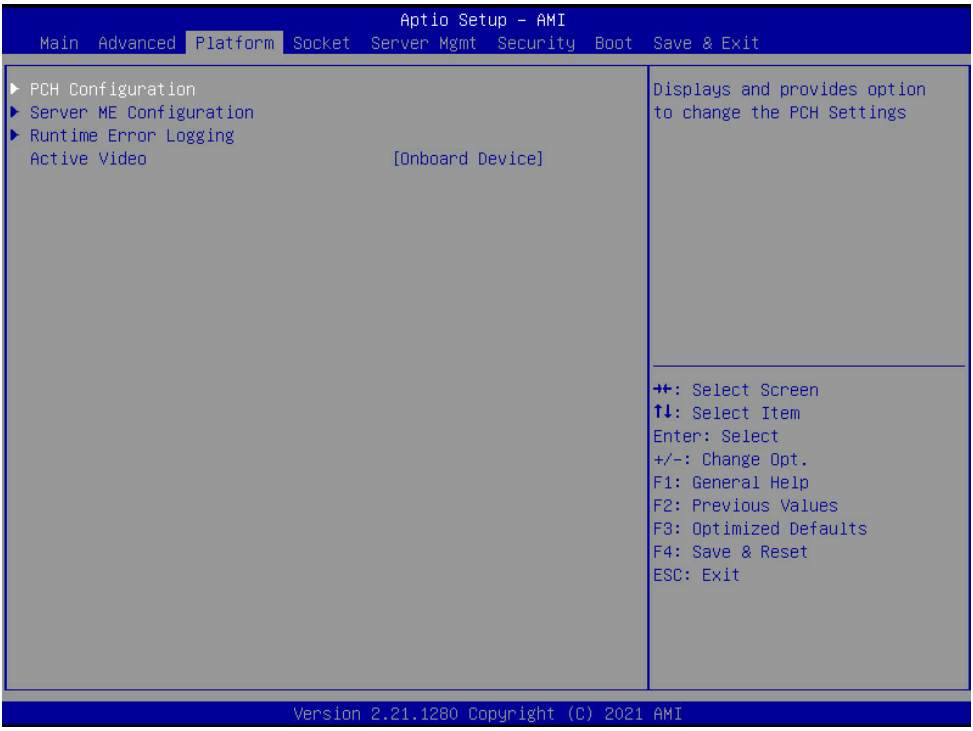
⚠ 对于配置不同品牌的 NVMe 硬盘 RAID，需要在主板上插入 Key.


Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Advanced
Intel(R) VROC with VMD Technology 5.2.0.1029
Upgrade key: VROC in pass-thru mode
Intel VROC Managed Volumes:
Volume0, RAID0(Stripe), 745.2GB, Normal
Intel VROC Managed Controllers:
All Intel VMD Controllers
Select to see more information about the Intel VMD Controllers
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit
Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.


Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Advanced
RAID VOLUME INFO
Volume Actions
Delete
Name: Volume0
RAID Level: RAID0(Stripe)
Strip Size: 128KB
Size: 745.2GB
Status: Normal
Bootable: Yes
Block size: 512
Slot 81, B/D/F: 1/0/0, CPU0, VMD1 Port 0x1, INTEL SSDPE2...
Slot 82, B/D/F: 2/0/0, CPU0, VMD1 Port 0x1, INTEL SSDPE2...
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit
Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.


Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Advanced
INTEL SSDPE2MX012T4 SN:CVPD514200191P2QGN, 1.09TB
Disk Actions:
Reset to non-RAID
Controller: Volume Management Dev...
Model Number: INTEL SSDPE2MX012T4
Serial Number: CVPD514200191P2QGN
Size: 1.09TB
Status: RAID Member
Block size: 512
Removes RAID data from the disk
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit
Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.

4.3.3 Platform 菜单



➔PCH Configuration

PCH 设备相关配置。

➔Server ME Configuration

服务器 ME 配置。

➔Runtime Error Logging

Active Video

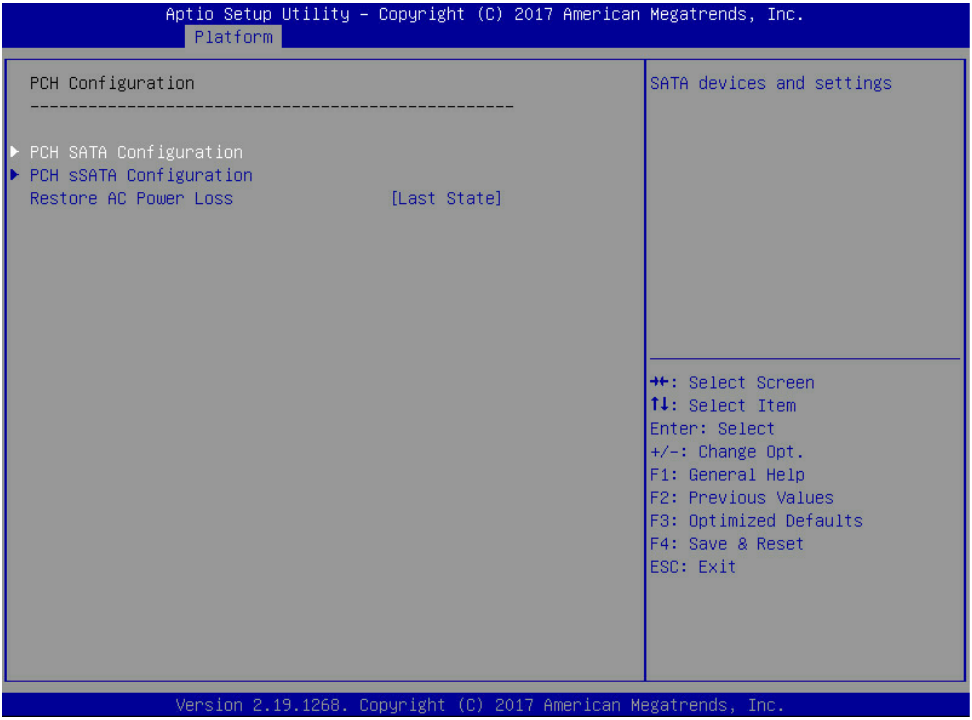
显示设备控制开关，菜单选项为：

Onboard Device：板载显示设备

Offboard Device：外接显示设备

默认值：Onboard Device

4.3.4.1 PCH Configuration



●PCH SATA Configuration

PCH SATA 设备配置。

●PCH sSATA Configuration

PCH sSATA 设备配置。

Restore AC Power Loss

AC 断电后再上电系统状态控制开关，菜单选项为：

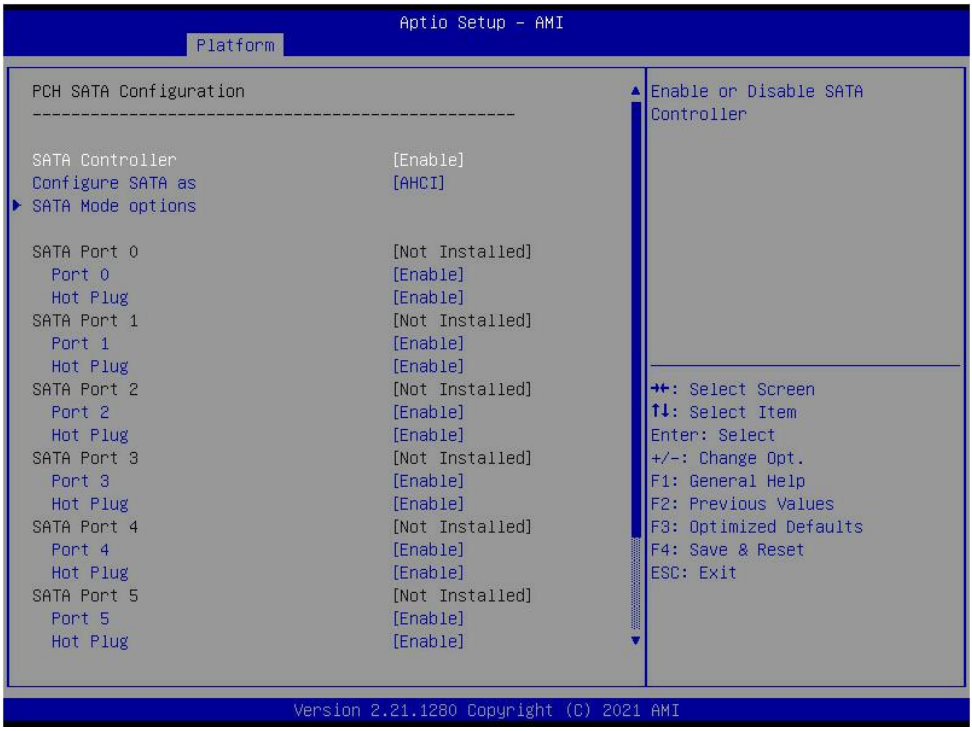
●PowerOn：开机

●PowerOff：关机

●Last State：保持掉电前状态

默认值：Last State

PCH SATA Configuration



SATA Controller

SATA 控制器开启关闭控制开关，菜单选项为：

Enable：开启

Disable：关闭

默认值：Enable

Configure SATA as

SATA 控制器工作模式选择开关，菜单选项为：

AHCI：AHCI 模式

RAID：RAID 模式

默认值：AHCI

SATA Port X

显示 SATA 端口 0~7 设备信息，根据硬盘在位情况动态获取，设备不在位时显示 Not Installed。

Port X

SATA 端口开关，菜单选项为：

Enable：开启

Disable：关闭

默认值：Enable

Hot Plug

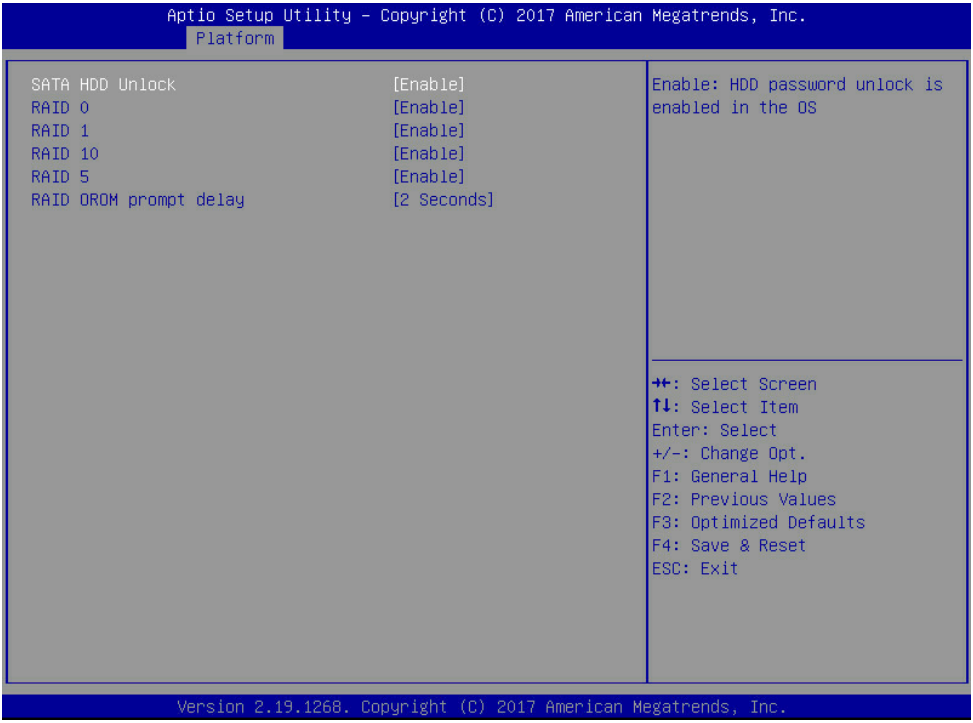
热插拔，菜单选项为：

Enable：开启

Disable：关闭

默认值：Enable

➔SATA Mode options



SATA HDD Unlock

操作系统下 SATA 硬盘密码解锁控制开关，菜单选项为：

Enable：开启

Disable：关闭

默认值：Enable

RAID X

RAID 模式控制开关，菜单选项为：

Enable：开启

Disable：关闭

默认值：Enable

⚠ RAID 模式可见。

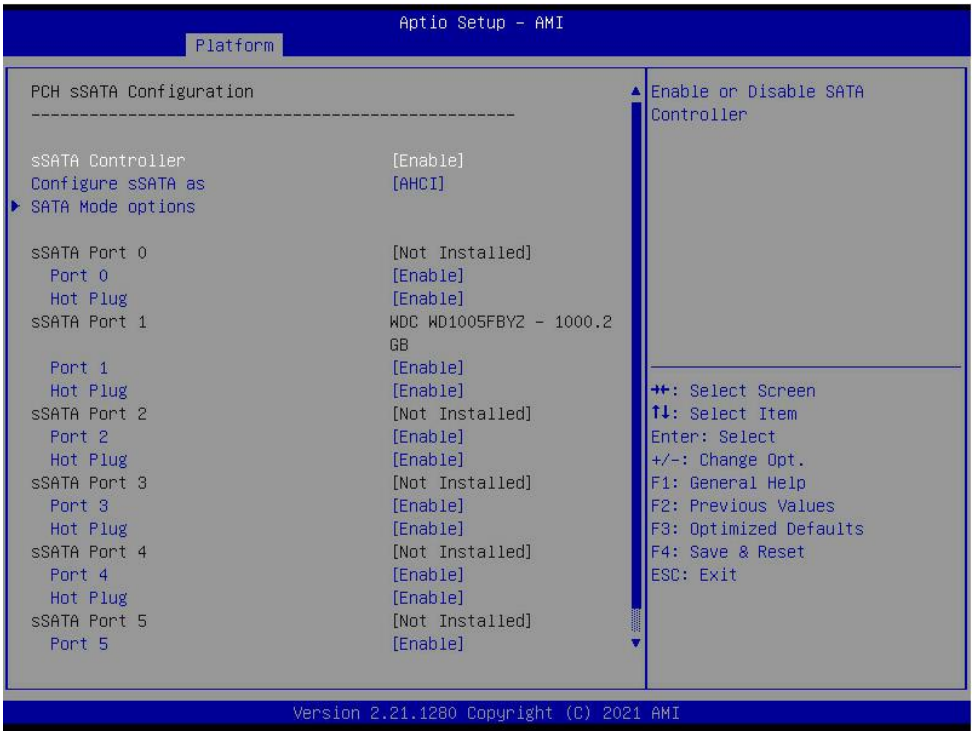
RAID OROM prompt delay

RAID OROM 运行提示时间，用户可输入，默认 2 秒。

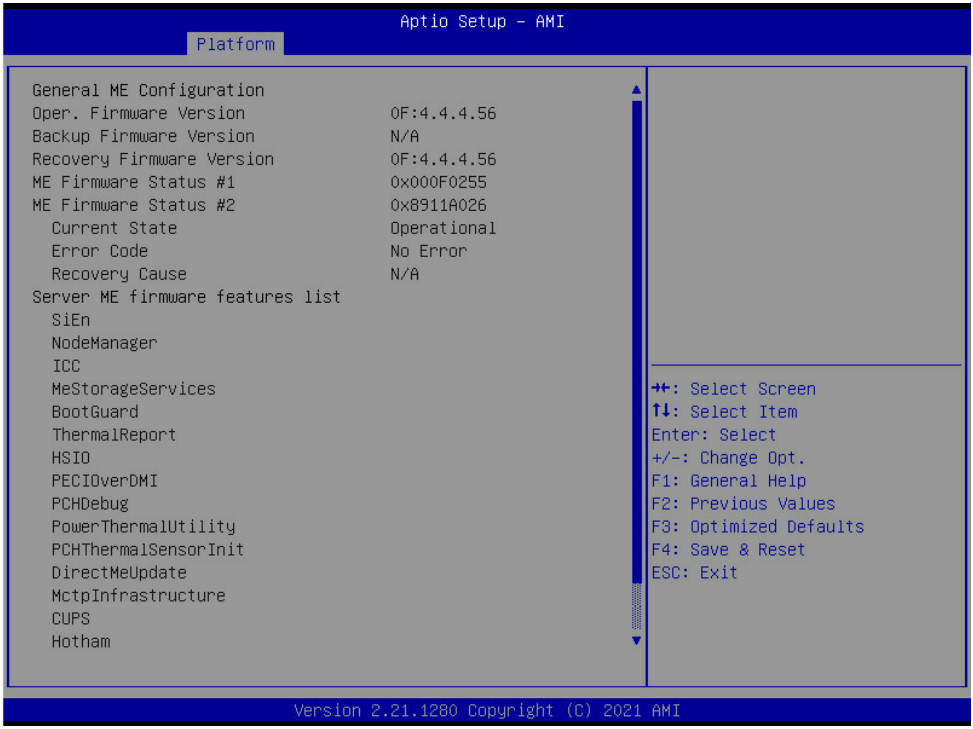
RAID 模式可见。

PCH sSATA Configuration

PCH sSATA 配置菜单，操作方式与 SATA configuration 一样



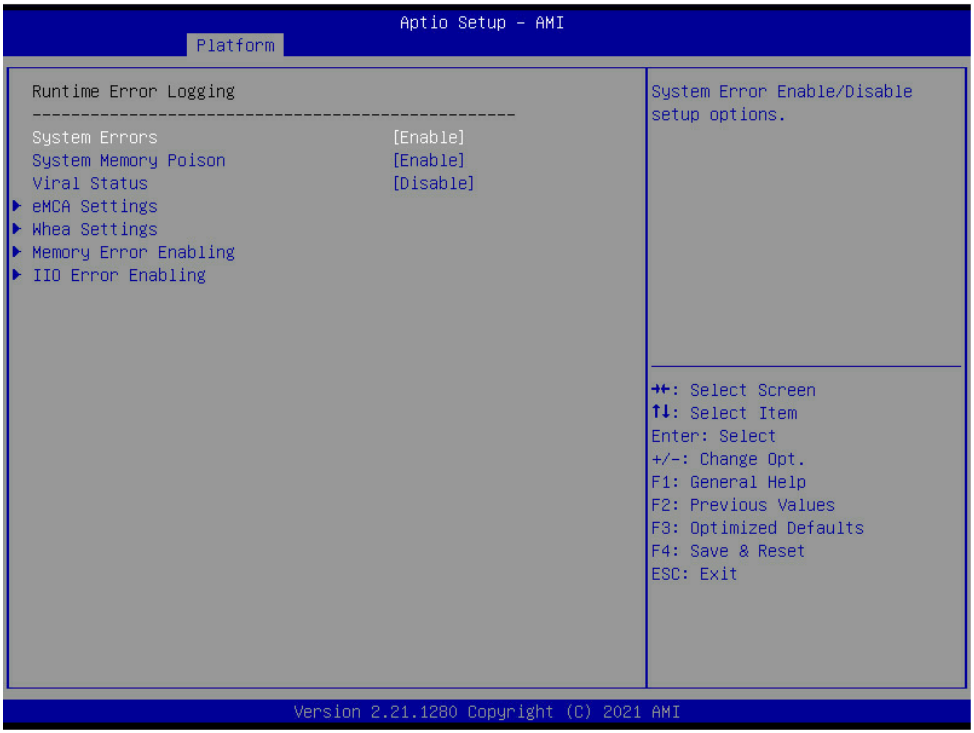
4.3.4.2 Server ME Configuration



显示服务器 ME 的版本、状态、功能等信息。

4.3.4.3 Runtime Error Logging

对系统错误记录功能进行设置，包括系统错误记录、System Poison 等等



System Errors

系统错误记录开关，打开本开关，就可以进行错误纠正。不可纠正错误上报，分别上报给 BMC 和 OS，菜单选项为：

Enable：开启系统错误记录功能

Disable：关闭系统错误记录功能

默认值：Enable

System Memory Poison

系统内存 Poison 模式开关，开启后，如果发现错误，会对错误信息打上 poison 标签，而不会马上触发，直到使用这个错误数据时才会触发中断，菜单选项为：

Enable：开启系统内存 Poison 模式

Disable：关闭系统内存 Poison 模式

默认值：Enable

注：当“System Errors”设置为 Disable 时，“System Memory Poisoning”不可见。

Viral Status

病毒状态配置

Enable：启用内存病毒

Disable：禁用内存病毒

默认值：Disable

注：当“System Errors”设置为 Disable 时，“Viral Status”不可见，当“System Memory Poisoning”设置为 Disable 时，“Viral Status”显示为灰色。

Clear Viral Status

清除病毒状态配置

Enable：启用内存病毒

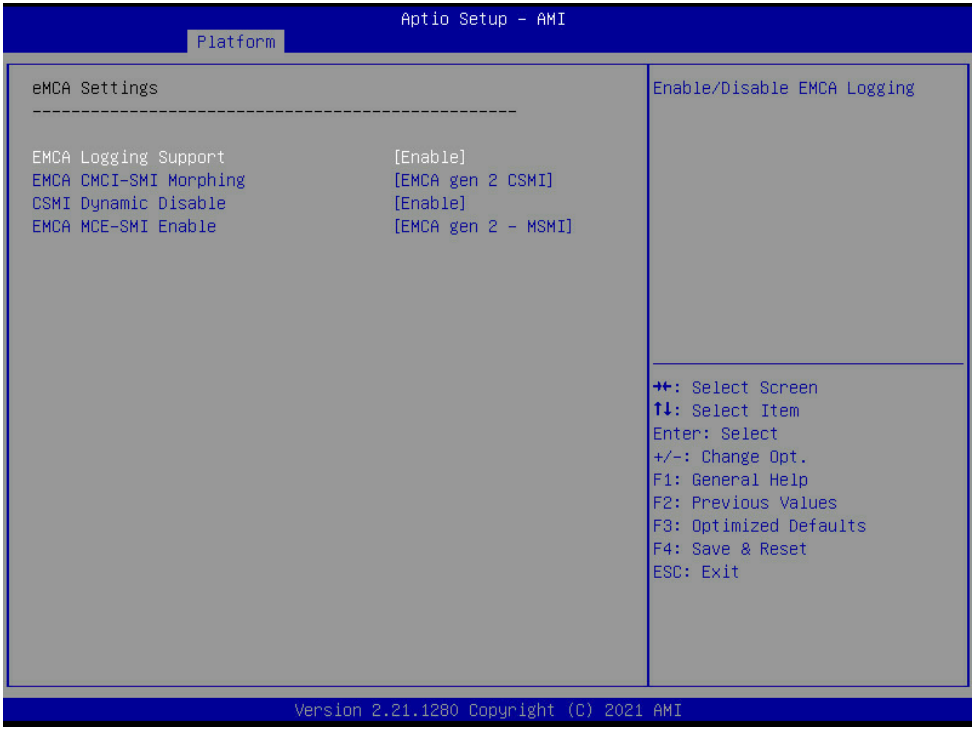
Disable：禁用内存病毒

默认值：Disable

注：当“Viral Status”设置为 Disable 时，“Clear Viral Status”不可见。

eMCA Settings

eMCA（ Enhanced Machine Check Architecture）设置选项，当 System Errors 设置为 Enabled 时，该选项可用。



EMCA Logging Support

eMCA 记录日志开关，菜单选项为：

Enable：开启 eMCA 记录日志功能

Disable：关闭 eMCA 记录日志功能

默认值：Disable

EMCA CMCI-SMI Morphing:

eMCA CMCI-SMI Morphing 功能选项，开启后，可纠正错误每发生一次，均可触发 SMI；菜单选项为：

EMCA gen 1 Lite：配置为 EMCA gen1 Lite 模式

EMCA gen 2 CSMI：配置为 EMCA gen 2 CSMI 模式

Disable：关闭 eMCA CMCI-SMI Morphing 功能

默认值：EMCA gen 2 CSMI

注：当“EMCA Logging Support”设置为 Disable 时，“eMCA CMCI-SMI Morphing”不可见。

CSMI Dynamic Disable:

CSMI 开关选项，菜单选项为：

Enable：当达到错误阈值时，BIOS 禁用 CSMI

Disable：CSMI 始终开启

默认值：Disable

注：当“EMCA Logging Support”设置为 Disable 时，“CSMI Dynamic Disable”不可见。

EMCA MCE-SMI Enable:

EMCA MCE-SMI 启用设置菜单选项为：

EMCA gen 1 Dual Mode：启用 EMCA gen 1 双模式的 EMCA

EMCA gen 2 – MSMI：启用 EMCA gen 2 MSMI 模式的 EMCA MCE-SMI 功能

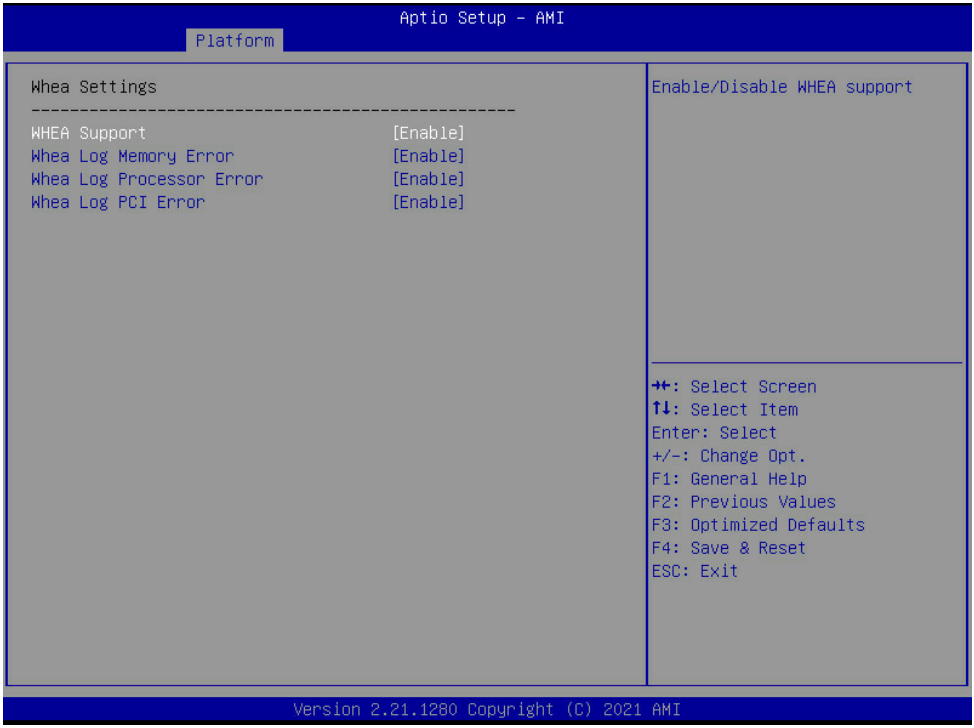
Disabled：禁用 EMCA MCE-SMI 功能。

默认值：EMCA gen 2 – MSMI

注：当“EMCA Logging Support”设置为 Disable 时，“EMCA MCE-SMI”不可见。

Whea Settings

Whea 设置菜单，当 System Errors 设置为 Enabled 时，该选项可用



WHEA Support:

WHEA 支持设置，该功能可以为服务器提供硬件错误报告，菜单选项为：

Enabled：开启 WHEA 功能。

Disabled：关闭 WHEA 功能。

默认值：Enabled

Whea Log Memory Error:

Whea 记录内存错误功能，菜单选项为：

Enabled：开启 Whea 内存错误记录功能。

Disabled：关闭 Whea 内存错误记录功能。

默认值：Enabled

注：当“WHEA Support”设置为 Disable 时，该选项不可见。

Whea Log Processor Error:

Whea 记录处理器错误功能，菜单选项为：

Enabled：开启 Whea 处理器错误记录功能。

Disabled：关闭 Whea 处理器错误记录功能。

默认值：Enabled

注：当“WHEA Support”设置为 Disable 时，该选项不可见。

Whea Log PCI Error:

Whea 记录 PCI 错误功能，菜单选项为：

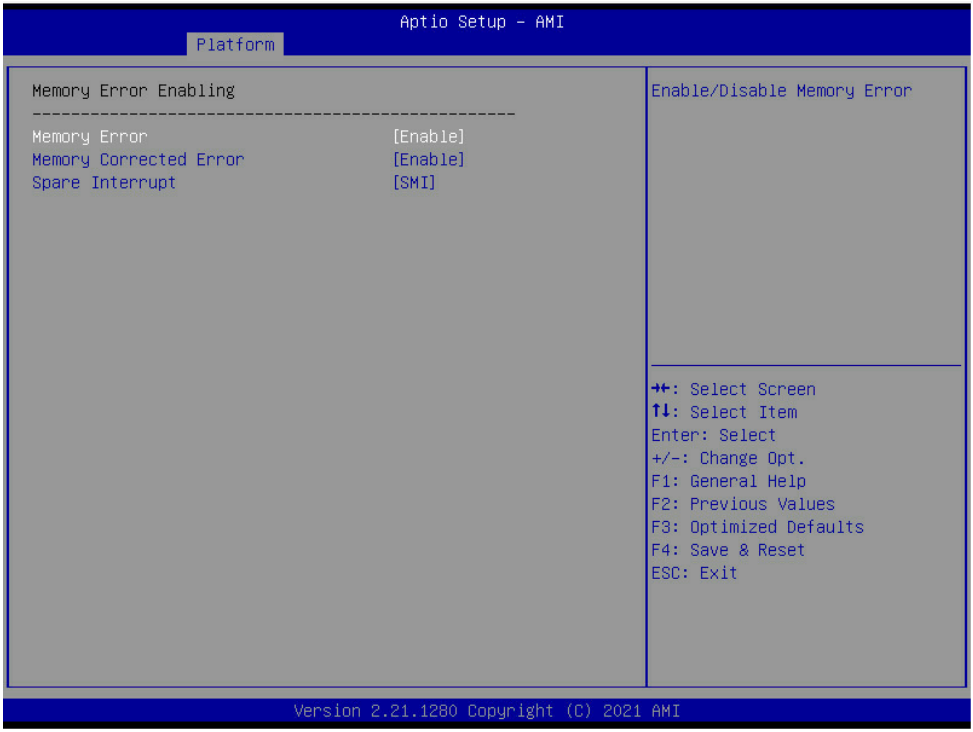
Enabled：开启 Whea 记录 PCI 错误功能。

Disabled：关闭 Whea 记录 PCI 错误功能。

默认值：Enabled

注：当“WHEA Support”设置为 Disable 时，该选项不可见。

Memory Error Enabling 界面



Memory Error:

内存错误使能设置，菜单选项为：

Enabled：开启内存错误功能。

Disabled：关闭内存错误功能。

默认值：Enabled

Memory Corrected Error:

内存可纠正错误使能设置，菜单选项为：

Enabled：开启内存可纠正错误功能。

Disabled：关闭内存可纠正错误功能。

默认值：Enabled

注：当“Memory Error”设置为 Disable 时，该选项不可见。

Spare Interrupt:

Spare Interrupt 类型设置，菜单选项为：

Disabled：禁止使用内存备用中断。

SMI：SMI 中断。

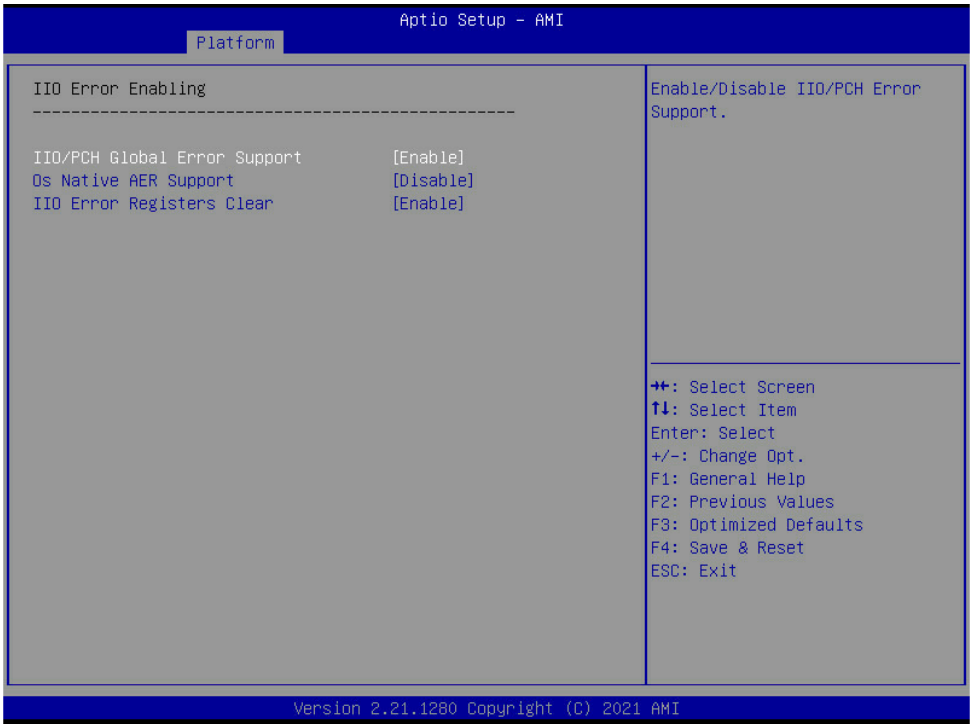
Error Pin：Error Pin 中断。

CMCI：CMCI 中断。Spare Interrupt Selection

默认值：SMI

注：当“Memory Corrected Error”设置为 Disable 时，该选项不可见。

IIO Error Enabling 界面



IIO/PCH Global Error Support:

设置是否处理 IIO/PCH 全局错误开关，菜单选项为：

Enabled：开启处理 IIO/PCH 全局错误功能。

Disabled：关闭处理 IIO/PCH 全局错误功能。

默认值：Enable

Os Native AER Support:

OS 控制 AER 错误处理功能，默认是 FW 优先控制 AER 错误处理，如果需要由 OS 控制 AER 错误，需要将此参数设置为“Enable”。菜单选项为：

Enable：OS 控制 AER 错误处理功能。

Disable：FW 控制 AER 错误处理功能。

默认值：Disable

注：当“IIO/PCH Global Error Support”设置为 Disable 时，该选项不可见。

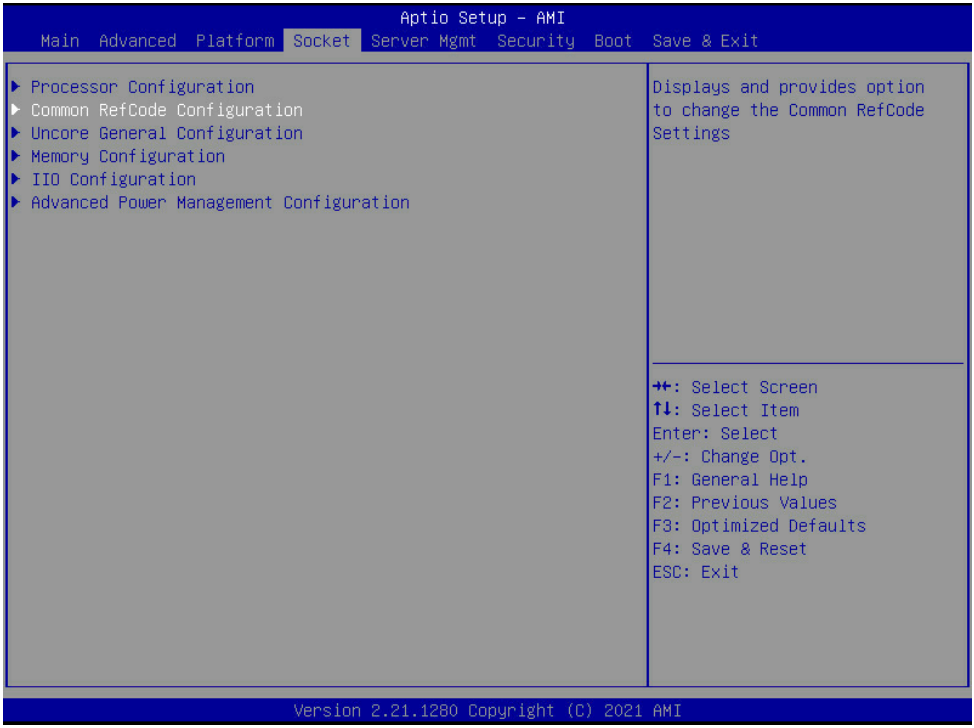
IIO Error Registers Clear:

设置是否清除 IIO 错误处理后寄存器信息，菜单选项为：

Enabled：不清除 IIO 错误处理后寄存器信息。
Disabled：清除 IIO 错误处理后寄存器信息。
默认值：Enable
注：当“IIO/PCH Global Error Support”设置为 Disable 时，该选项不可见。

4.3.4 Socket 菜单

在该界面，可以查看 CPU、内存的相关信息，并对 CPU 的工作状态进行设置



●Processor Configuration
处理器配置
●Common RefCode Configuration
常见参考代码配置，如启用/禁用非一致性内存访问技术（numa）
●Uncore General Configuration
Uncore 部分配置

●Memory Configuration

内存配置

●IIO Configuration

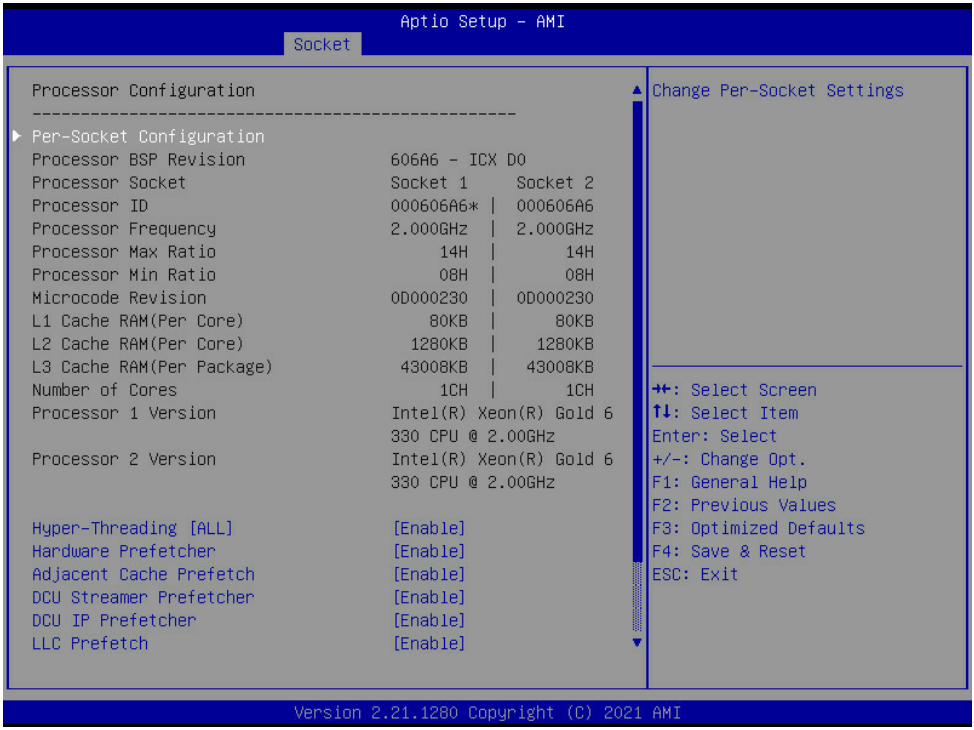
集成输入/输出相关配置，如启用/禁用 Intel VT-d 功能

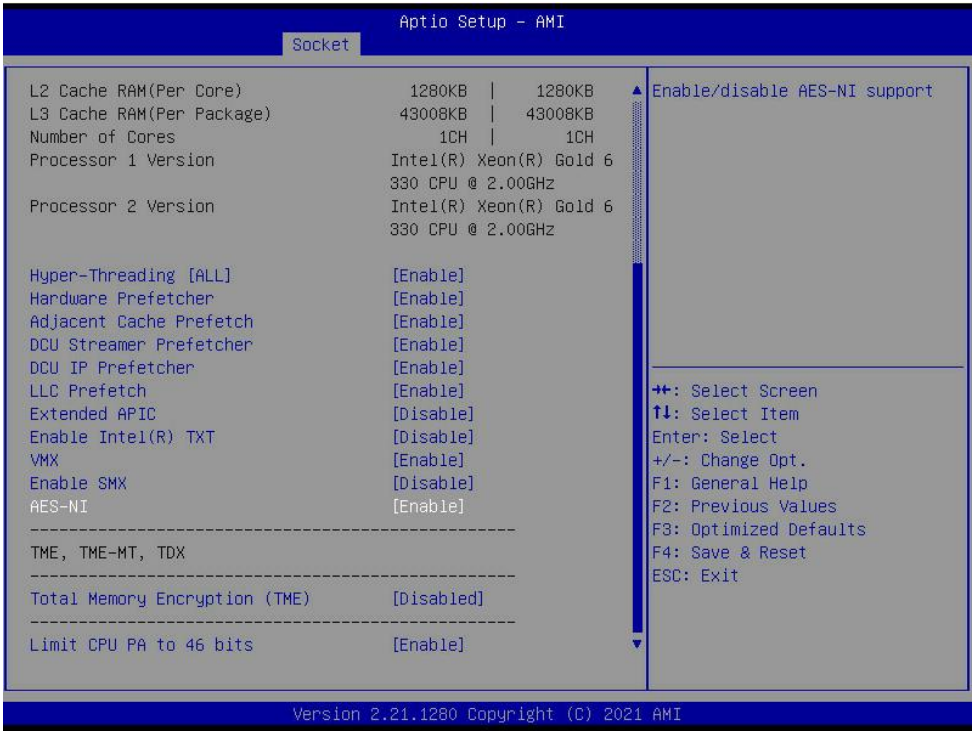
●Advanced Power Management Configuration

高级电源管理配置

4.3.4.1 Processor Configuration

显示处理器的型号、ID 号、频率、Microcode 版本、L1/L2/L3 缓存容量、处理器具体型号等信息。





Hyper-Threading [ALL]

超线程控制开关，此选项可以启用或停用英特尔处理器超线程功能。启用该功能，每个物理处理器核心相当于两个逻辑处理器核心；停用该功能，每个物理处理器核心只相当于一个逻辑处理器核心。启用该功能会带来更高的处理器核心计数，提高应用的整体性能。菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Enable

Hardware Prefetcher

硬件预取是指 CPU 处理指令或数据之前，它将这些指令或数据从内存预取到 L2 缓存中，借此减少内存读取的时间，帮助消除潜在的瓶颈，以此提高系统效能。菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Enable

Adjacent Cache Prefetch

开启相邻缓存预取功能后，计算机在读取数据时，会智能的认为要读取的数据旁边或邻近的数据也是需要的，于是在处理的时候就会将这些邻近的数据预先读取出来，这样可以加快读取速度。当应用场景是顺序访问内存时，启用该功能会提升性能。当应用场景是随机访问内存时，建议停用该选项。菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Enable

DCU Streamer Prefetcher

DCU 流预取特性开关，该选项启用（默认）或停用数据缓存单元（DCU）流预取，该设置根据运行在服务器上的应用，对性能产生影响。菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Enable

DCU IP Prefetcher

DCU IP 预取特性开关，该选项启用（默认）或停用数据缓存单元（DCU）IP 预取器，该设置根据运行在服务器上的应用，对性能产生影响。菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Enable

LLC Prefetch

三级缓存预取特性开关，菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Disable

Extenderd APIC

启用或禁用处理器 x2APIC 支持模式，菜单选项为：

●Enable：开启
●Disable：关闭
默认值：Disable
如果启用了 x2APIC，这将自动启用 VT-d

Enable Intel(R) TXT
启用或禁用 Intel TXT 功能，菜单选项为：
●Enable：开启
●Disable：关闭
默认值：Disable

VMX
启用或禁用 VMX 功能，重启后生效，菜单选项为：
●Enable：开启
●Disable：关闭
默认值：Enable

Enable SMX
启用或禁用更安全模式扩展，菜单选项为：
●Enable：开启
●Disable：关闭
默认值：Disable

AES-NI
启用或禁用英特尔高级加密标准新指令，菜单选项为：
●Enable：开启
●Disable：关闭
默认值：Enable

Total Memory Encryption(TME)
启用或禁用英特尔 TME 功能，菜单选项为：
●Enable：开启

●Disable：关闭

默认值：Disable

Limit CPU PA to 46 bits

将 CPU 物理地址限制为 46 位以支持较老版本的 Hyper-v。如果启用，将自动禁用 TME-MT；菜单选项为：

●Enable：开启

●Disable：关闭

默认值：Enable

4.3.4.2 Common RefCode Configuration

MMIO High Base

配置 MMIOH 起始地址

MMIO High Granularity Size

配置每个 stack 的 MMIOH 分配单位大小。

Isoc Mode

数据等时传送特性，开启后可以提高传输数据的质量，但是会减少内存带宽，降低内存性能。菜单选项为：

●Auto：

●Enable：开启 ISOC Mode。

●Disable：关闭 ISOC Mode。

Numa

可通过此选项禁用或开启系统的 NUMA 架构属性。菜单选项为：

●Enable：开启

●Disable：关闭

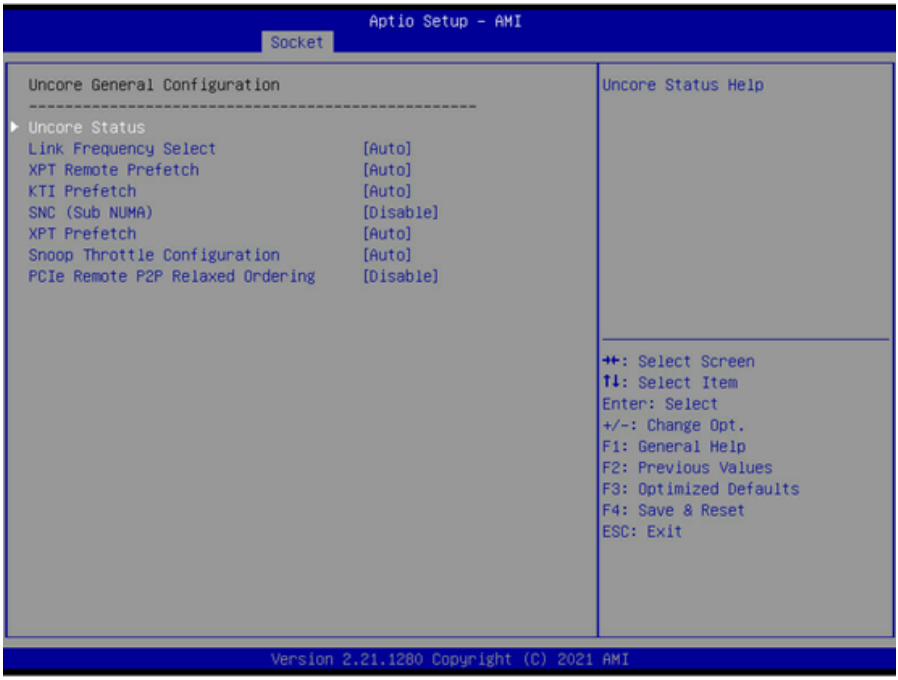
Virtual Numa

在 ACPI 表中将物理 NUMA 节点划分为大小均匀的虚拟 NUMA 节点。这可能会提高具有超过 64 个逻辑处理器的 CPU 上的 Windows 性能。菜单选项为：

●Enable：开启

●Disable：关闭

4.3.4.3 Uncore General Configuration



➔Uncore status

Uncore 模块状态信息显示

显示系统 CPU 数量、IIO 数量、当前 UPI 速度模式、当前 UPI 链接速度信息。

➔Link Frequency Select

链接频率选择配置，将 UPI 链路频率设置为较低速度，以较低频率运行可降低功耗，但同时会影响系统性能。存在两个 CPU 时，才能配置此选项。菜单选项为：

●Auto：自动设置

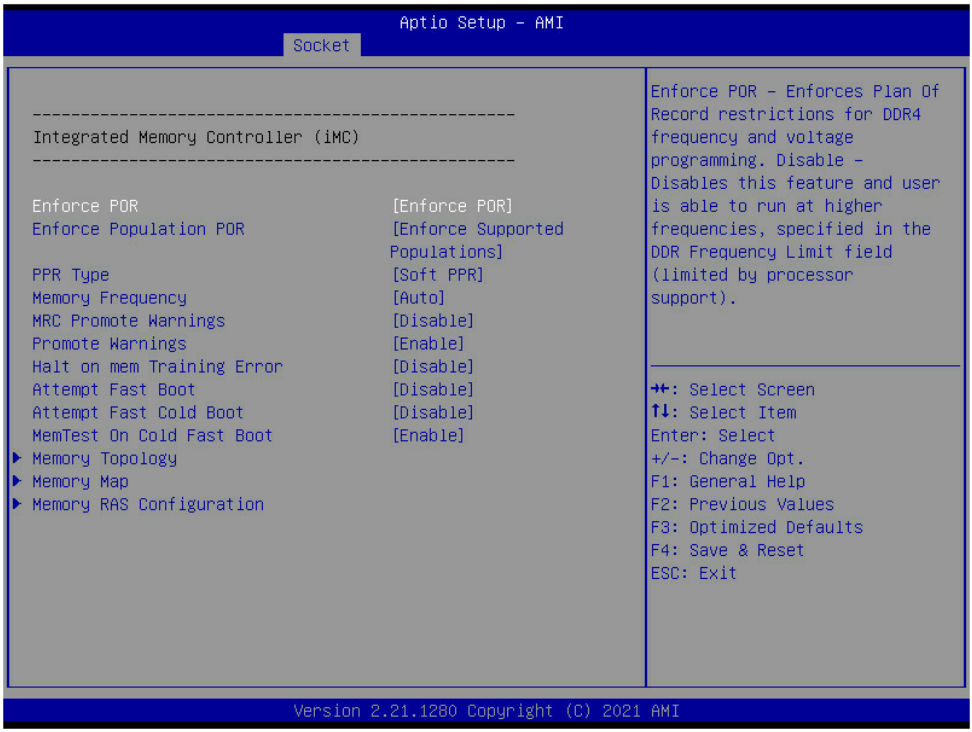
●9.6GT/s：每秒 9.6 千兆传输

●10.4GT/s：每秒 10.4 千兆传输

●Use Per Link Setting

默认值：Auto

4.3.4.4 Memory Configuration



Enforce POR

执行 POR 功能，Auto 和 POR 为开启此功能，内存频率和电压将受到平台参数设计限制。Disable 时，将忽略参数设计限制。菜单选项为：

- Auto
- POR
- Disable

默认值：Auto

Enforce Population POR

启动内存 POR 强制执行

Memory Frequency

内存速度配置

MRC Promote Warnings:
确定 MRC 警告是否提升到系统级别

Promote Warnings:
确定警告是否提升到系统级别

Halt on mem Training Error:
禁用/启用内存训练错误时系统暂停

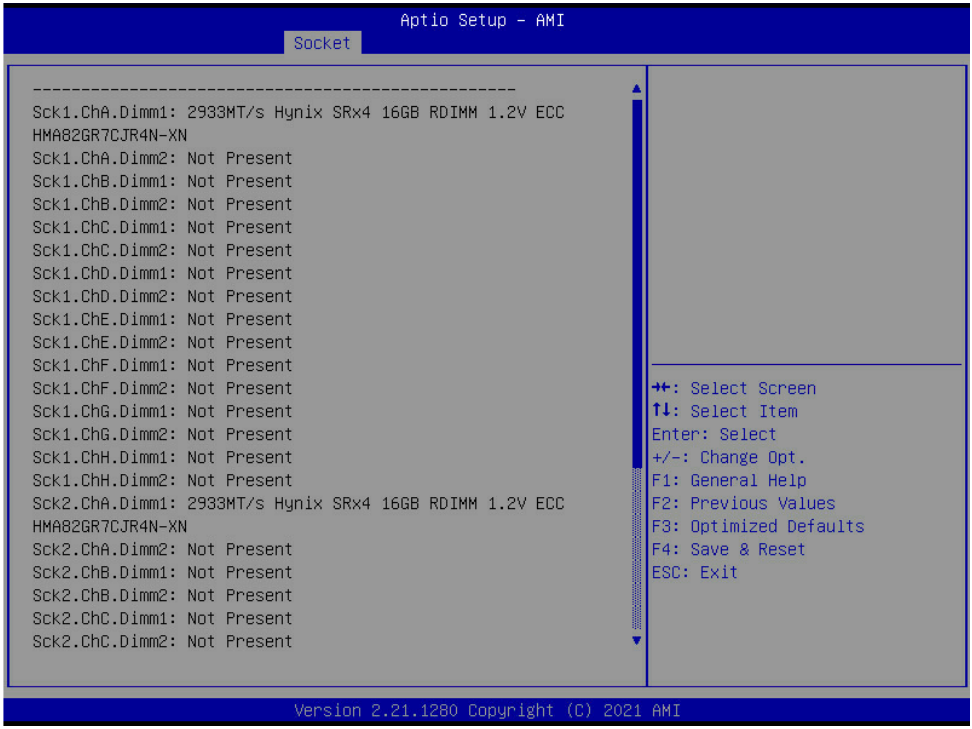
Attempt Fast Boot
设置快速热启动，菜单选项为：
●Auto：自动
●Enable：开启
●Disable：关闭
默认值：Disable

Attempt Fast Cold Boot
设置快速冷启动，菜单选项为：
●Auto：自动
●Enable：开启
●Disable：关闭
默认值：Disable

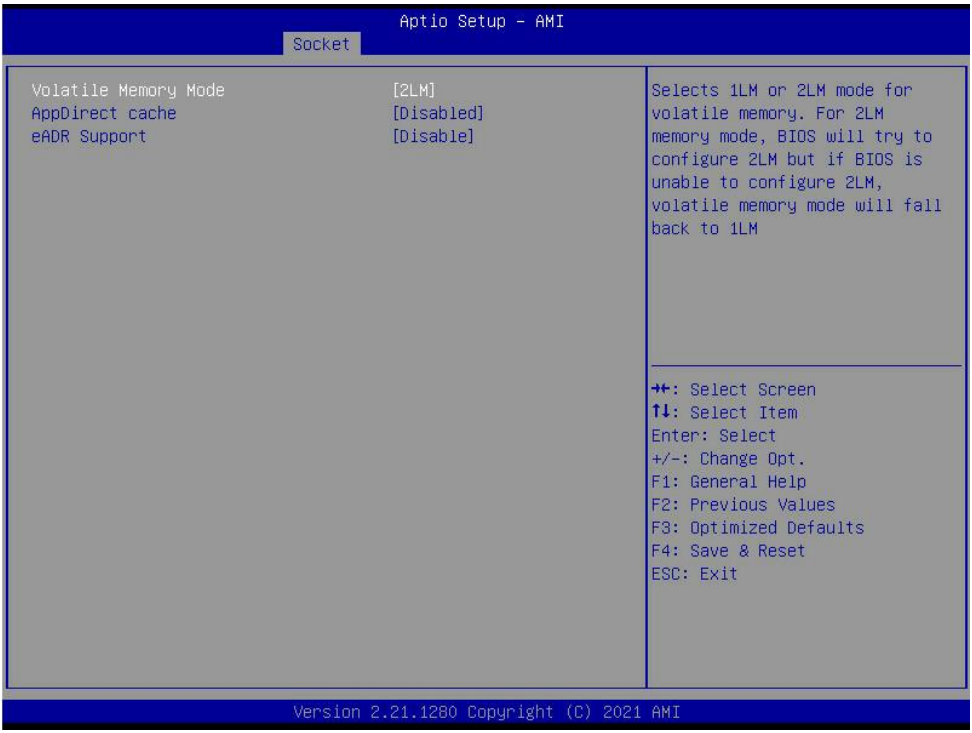
MemTest On Fast Boot
Fast Boot 过程中，设置 memory test 是否开启，菜单选项为：
●Auto：自动
●Enable：开启
●Disable：关闭
默认值：Disable

●Memory Topology 菜单

显示内存信息



●Memory Map 菜单



Volatile Memory Mode

选择是否启用 1LM 或 2LM 内存模式，菜单选项为：

●1LM

●2LM

●Auto

AppDirect cache

选择是否为内存域启用缓存，菜单选项为：

●Auto：自动

●Enable：开启

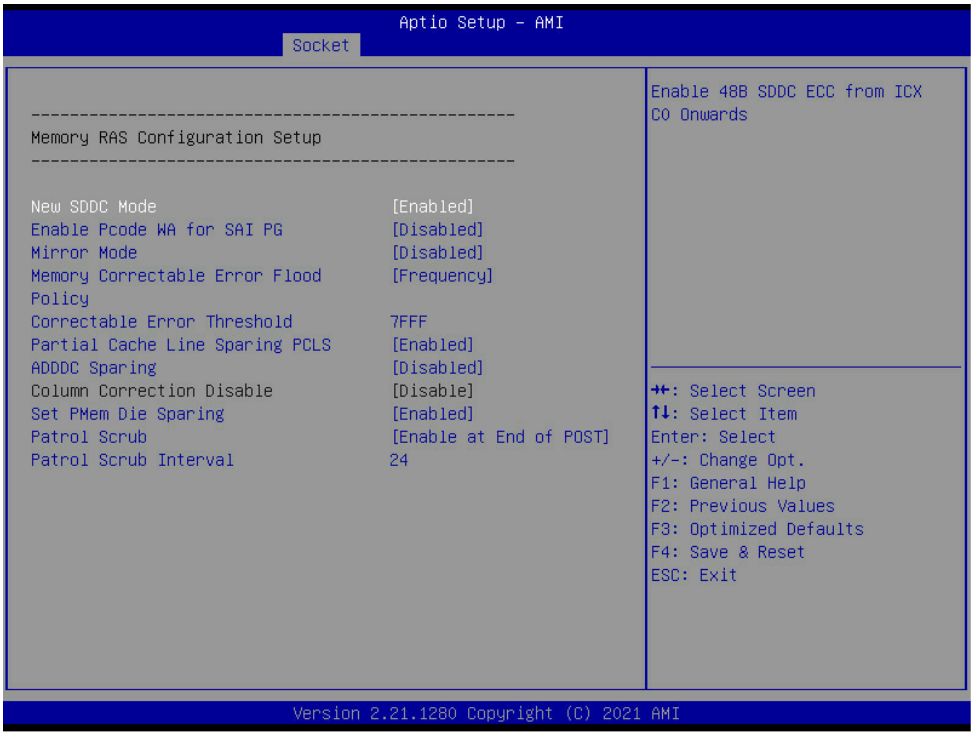
●Disable：关闭

eADR Support

eADR 功能开关，菜单选项为：

●Auto：自动
●Enable：开启
●Disable：关闭

●Memory RAS Configuration 菜单
内存 RAS 配置



New SDDC Mode
Enable Pcode WA for SAI PG
静态虚拟 Lockestep 模式，菜单选项为：
●Enable：开启
●Disable：关闭
默认值：Disable

Mirror mode

内存镜像模式，菜单选项为：

●Disable：关闭内存镜像模式

●Mirror Mode 1LM

●Mirror Mode 2LM

默认值：Disable

Mirror TAD0

低地址镜像功能，菜单选项为：

●Disable：关闭

●Enable：开启

默认值：Disable

Enable Partial Mirror

部分镜像功能，菜单选项为：

●Disable：关闭部分内存镜像模式

●Partial Mirror Mode 1LM

●Partial Mirror Mode 2LM

默认值：Disable

Patrol Scrub

内存巡查功能，在发现可纠正错误时尽早纠正，可防止错误累积成不可纠正错误。当设置为关闭时，系统将不提供内存巡查功能，菜单选项为：

●Disable：关闭

●Enable：开启

默认值：Enable

Patrol Scrub Interval

选择完成内存刷新所需的小时数，0 值表示自动选择，用户可选择输入范围是 0～24，默认值为 24.

Patrol Scrub Address Mode

内存巡查地址模式，菜单选项为：

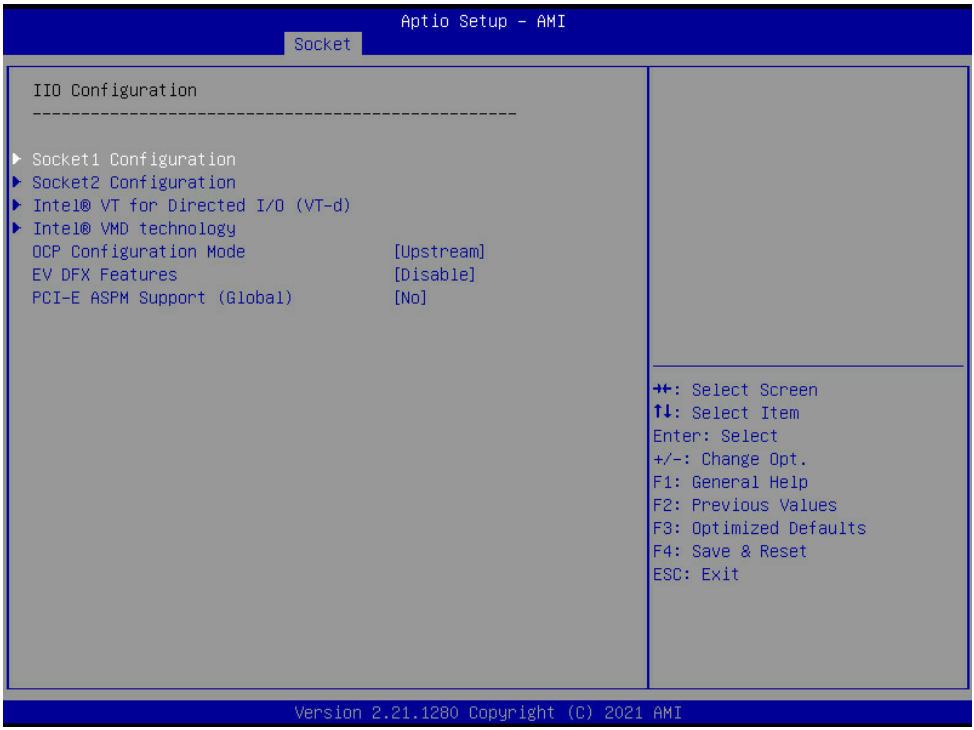
●Reverse Address：反转地址

●System Physical Address：系统物理地址

默认值：System Physical Address

4.3.4.5 IIO Configuration 菜单

在此界面，可以对 PCIe 插槽进行配置，包括 PCIe 端口链接速度、PCIe 端口最大负载等等。



●Socket1 Configuration 菜单

CPU1 配置菜单

●Socket2 Configuration 菜单

CPU2 配置菜单

●Intel® VT for Directed I/O (VT-d)菜单

英特尔虚拟化配置菜单

●Intel® VMD technology 菜单

英特尔 VMD 技术配置菜单

●OCP Configuration Mode

OCP 配置模式选项

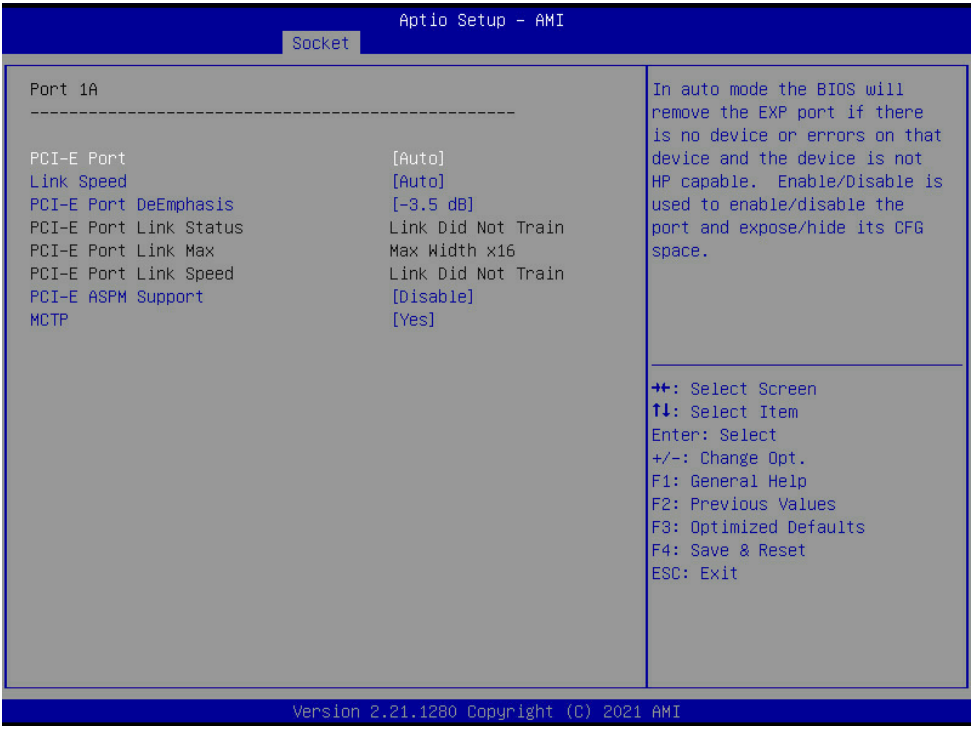
●EV DFX Features

EV DFX 特性开关

● PCI-E ASPM Support (Global)

ASPM 节能功能使能开关

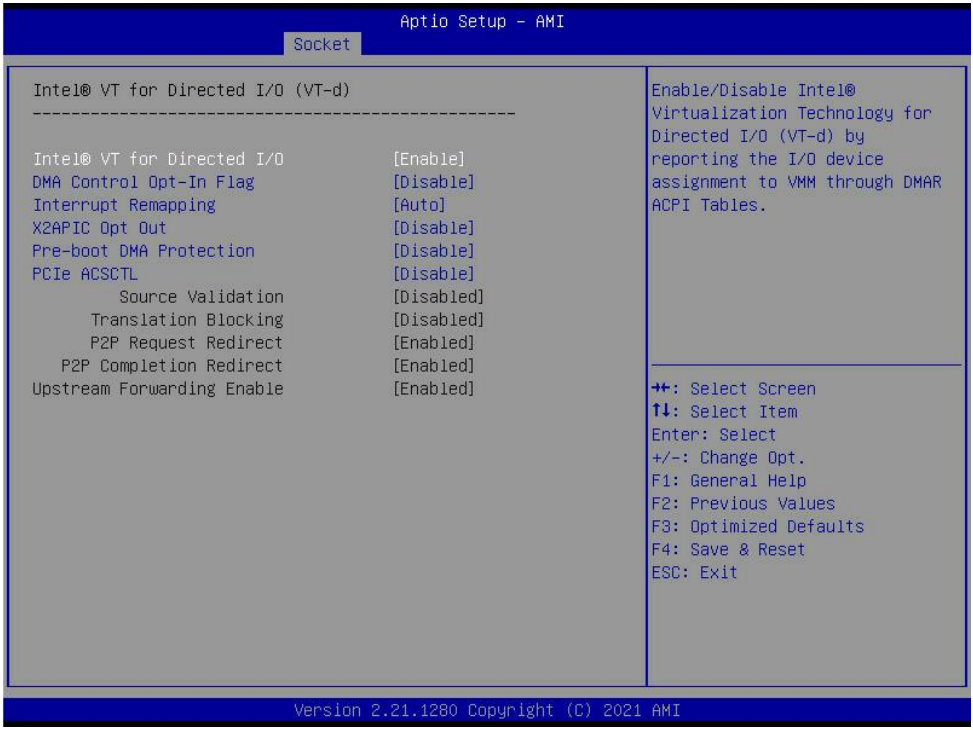
Socket Configuration 菜单



显示所有 PCIE 设备配置菜单，此为动态显示界面，会根据主板接入转接口不同，显示有差别。

Intel® VT for Directed I/O (VT-d)菜单

通过“Intel(R) VT for Directed I/O(VT-d)”界面，对 VT-d 特性进行配置。



●Intel® VT for Directed I/O (VT-d)

VT-d 功能使能开关，菜单选项为：

Disable：关闭

Enable：开启

默认值：Disable

●DMA Control Opt-In Flag

DMA 开关，本功能与虚拟化功能相关。菜单选项为：

Enabled：开启 DMA 功能

Disabled：关闭 DMA 功能

默认值：Disable

●Interrupt Remapping

VT_D 中断重映射开关，开启后，支持此选项的管理程序和操作系统能够为定向 I/O 使用英特尔虚拟化技术提供中断重映射的硬件功能。菜单选项为：

Disable：关闭

Enable：开启
默认值：Enable

Intel® VT for Directed I/O (VT-d)为 Enable 时可见。

●X2APIC Opt Out:
扩展 APIC 开关，允许操作系统在多核心数的服务器中高效地运行，并优化虚拟化环境中的中断分配。
Enabled：开启 X2APIC 功能
Disabled：关闭 X2APIC 功能
默认值：Disable

●Pre-boot DMA Protection:
在预引导环境中启用 DMA 保护
Enabled：开启 X2APIC 功能
Disabled：关闭 X2APIC 功能
默认值：Disable

●PCIe ACSCTL:
启用 PCI 根端口中 PCI 访问控制服务控制寄存器的覆盖。
Enabled：开启 X2APIC 功能
Disabled：关闭 X2APIC 功能
默认值：Disable

Intel® VMD technology 菜单

通过“Intel(R) VMD Technology”界面，对 PCIe 的 VMD 特性进行配置。

U.2 Device NVMe Mode

U.2 接口 NVMe 设备的控制模式开关。选择 VMD Mode，CPU 下面挂的 U.2 接口 NVMe 设备使用 VMD 功能管理，菜单选项为：

●VMD Mode：VMD 模式

●Non-VMD Mode：Non-VMD 模式

默认值：VMD Mode

⚠ VMD Mode 改为 Non-VMD Mode 时，不支持保存热重启操作，可选择先保存，关机，再开机。

OCP Configuration Mode:

设置 OCP 配置模式

EV DFX Features:

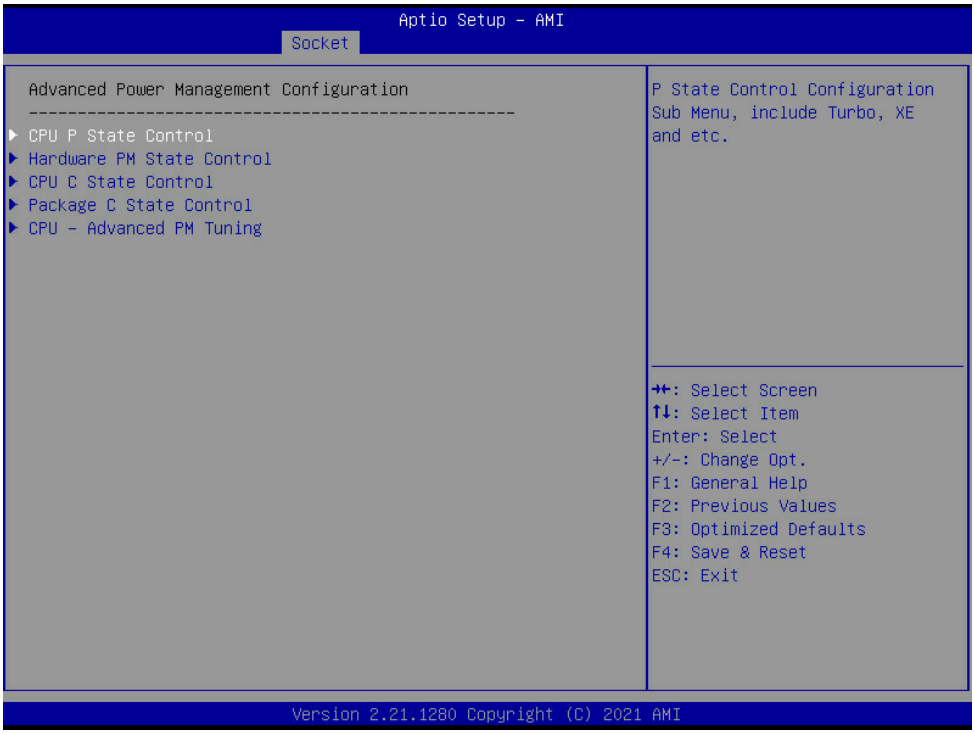
EV DFX 特性开关，开启后，允许 DFX 锁定位保持清空，菜单选项为：
●Enabled：开启 EV DFX 功能
●Disabled：关闭 EV DFX 功能
默认值：Disable

PCI-E ASPM Support (Global):

PCI-E ASPM 功能使能开关
●Auto：根据场景自动设置。
●L1 Only：设置成只进入 L1 模式。
●Disabled：关闭 ASPM 功能
默认值：Disable

4.3.4.6 Advanced Power Management Configuration 菜单

在此界面下，可以对处理器的供电进行高级配置



●CPU P State Control 菜单

CPU P 状态控制菜单

●Hardware PM State Control

硬件 PM 状态控制菜单

●CPU C State Control 菜单

CPU C 状态控制菜单

●Package C State Control 菜单

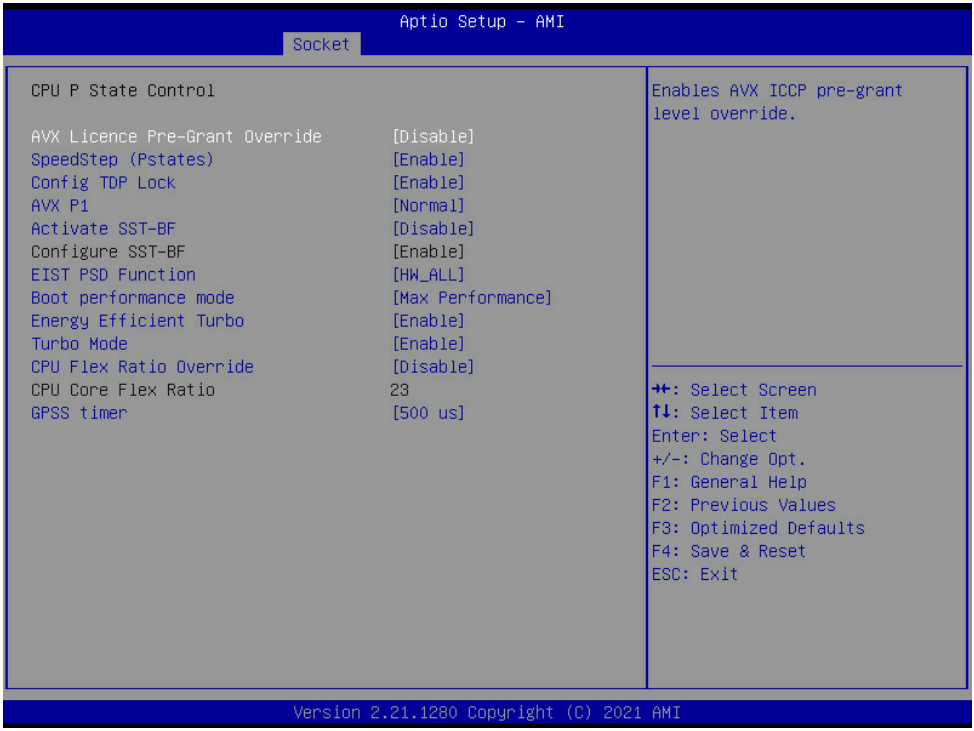
Package C 状态控制菜单

●CPU - Advanced PM Tuning 菜单

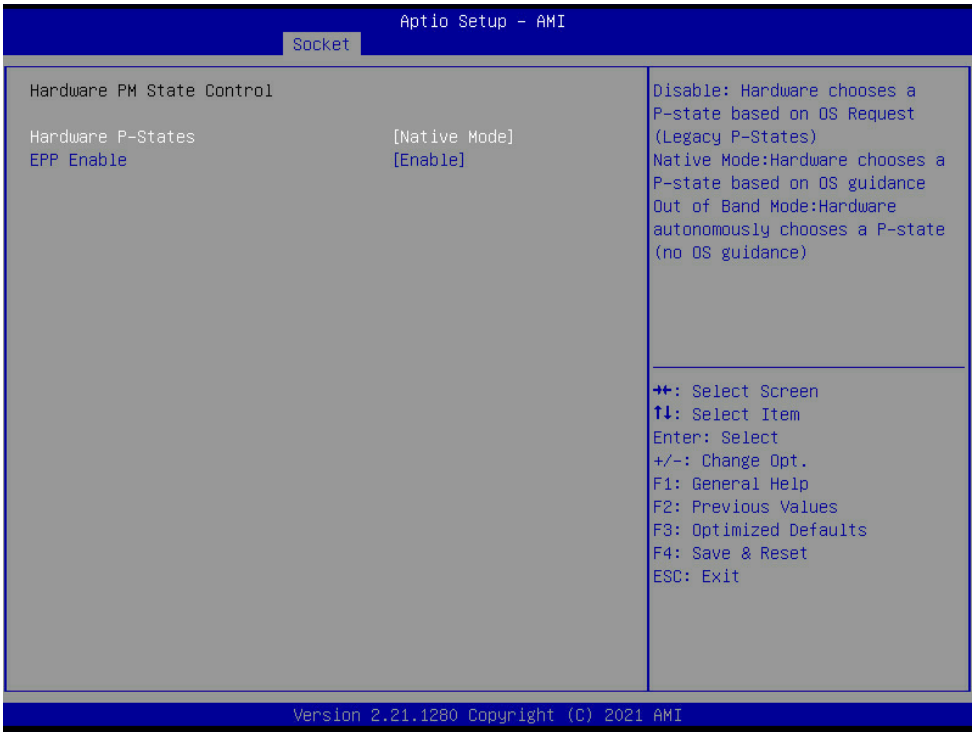
CPU 高级电源管理调谐控制菜单

CPU P State Control 菜单

在此界面，可以对 CPU 的 P 状态功能进行配置。



Hardware PM State Control



●Hardware P-States

硬件 P 状态选项，菜单选项为：

Disabled：硬件根据操作系统请求选择 P 状态。

Native Mode：硬件根据操作系统引导选择 P 状态。

Out-of-band Mode：硬件自主选择 P 状态。

●EPP Enable:

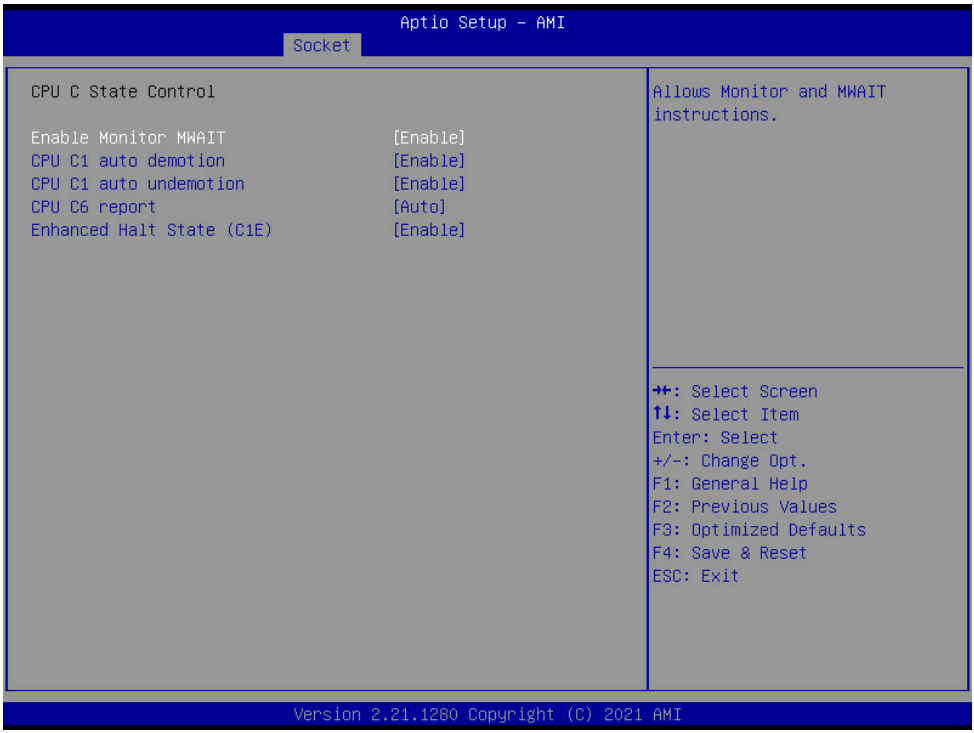
EPP（ENERGY_PERFORMANCE_PREFERENCE）功能使能，菜单选项为：

Disabled：禁用后，使用 EPB（ENEGY_PERF_BIAS）作为 EPP

Enabled：启动 EPP

⚠ 当“Hardware P-States”设置为 Disabled 时，该选项不可配置

CPU C State Control 菜单



●Enable Monitor MWAIT:

MONITOR/MWAIT 功能开关，开启后，可以监视 CPU 状态，从而优化 CPU 的指令运行。开启该选项可能会使部分 OS 获得自主调节节能选项的能力，所以如果要关闭节能选项请关闭此参数。

●CPU C1 auto demotion:

设置为 Enable 后，允许 CPU 自动降级到 C1 状态；

●CPU C1 auto undemotion：

设置为 Enable 后，允许 CPU 自动从 C1 取消降级；

●CPU C6 report

C6 状态控制开关，菜单选项为：

Auto：自动设置

Enable：开启

Disable：关闭

默认值：Auto

Autonomous Core C-state 选择 Enable 时，此项不可编辑。

Enhanced Halt State (C1E)

C1E 状态控制开关，菜单选项为：

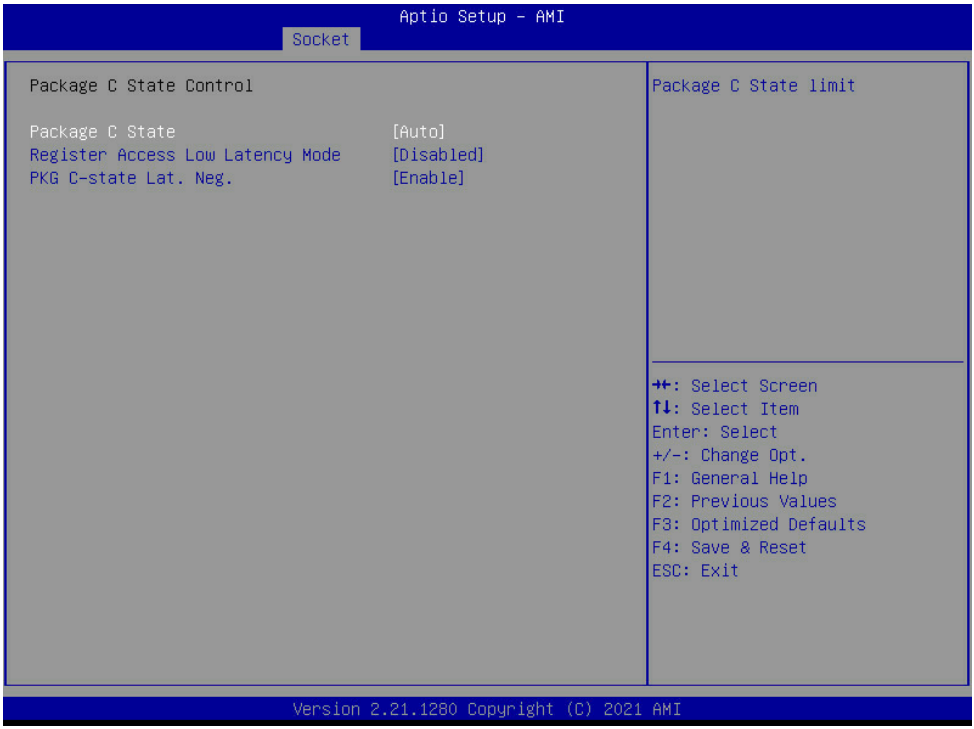
●Enable：开启

●Disable：关闭

默认值：Enable

Autonomous Core C-state 选择 Enable 时，此项不可编辑。

Package C State Control 菜单



Package C State：

Package C State 限制选项，菜单选项为：

●Auto：自动

●C0/C1 state：设置成 C0/C1 状态

●C2 state：设置成 C2 状态

●C6(non Retention) state：设置成 C6（非残留）状态

●C6(Retention) state：设置成 C6（残留）状态

●No Limit：设置成无限制模式

默认值：Auto

Register Access Low Latency Mode:

为寄存器访问启用低延迟模式。

●Enable：开启

●Disabled：关闭

默认值：Disabled

CPU - Advanced PM Tuning 菜单

Uncore Freq Scaling:

Uncore Frequency Scaling 功能开关，处理器可以通过内部的电压调节器，改变内部核心和非核心的电压/频率。启用时，会实现功率在核心和非核心之间的最佳分配，实现最大性能。菜单选项为：

●Enable：启用 UFS 运行最优频率。

●Disabled_Max：停用 UFS 运行最大频率。

●Disabled_Min：停用 UFS 运行最小频率。

默认值：Enable

Energy Perf BIAS

性能偏向菜单。

●Power Performance Tuning:

电源性能调整功能，菜单选项为：

●OS Controls EPB

●BIOS Controls EPB

●ENERGY_PERF_BIAS_CFG mode

设置 ENERGY_PERF_BIAS_CFG mode 模式，菜单选项为：

●Performance：性能优先

●Balanced Performance：性能优先，节省功耗

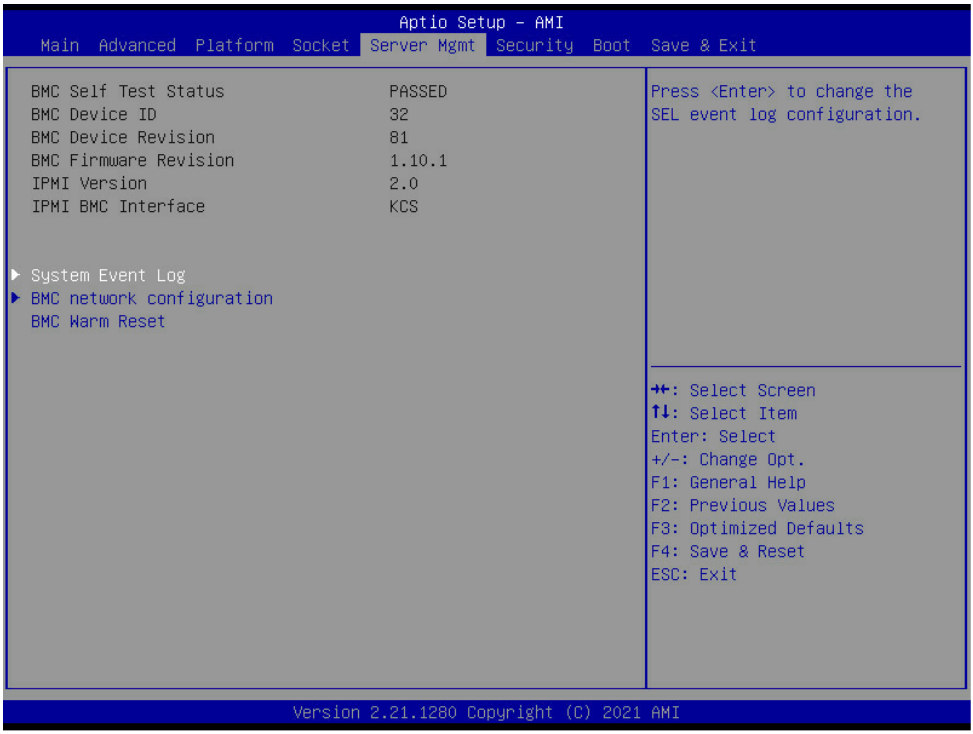
●Balanced Power：功耗优先，提高性能

●Power：功耗优先

默认值：Balanced Performance

Power Performance Tuning 设置为 OS Controls EPB，此项不可编辑。

4.3.5 Server Mgmt 菜单



显示 BMC 自检状态、设备 ID、设备版本、BMC 软件版本、支持 IPMI 规范版本。

●System Event Log 菜单

系统事件记录控制菜单

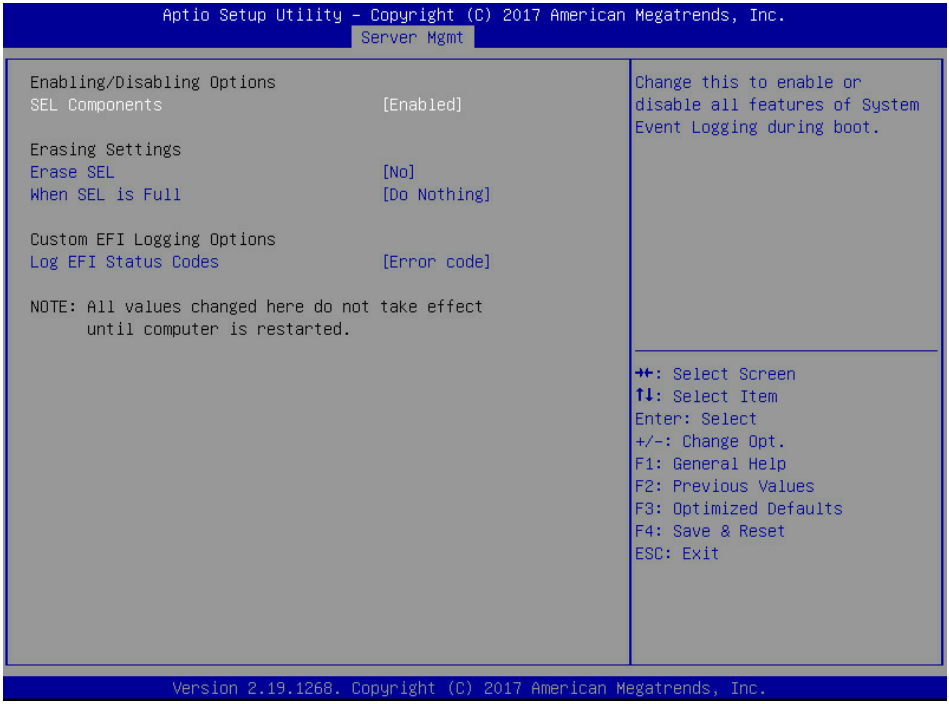
●BMC network configuration 菜单

BMC 网络配置菜单

●BMC Warm Reset

通过此选项，可重启 BMC

System Event Log 菜单



SEL Components

启动过程系统事件记录功能控制开关，菜单选项：

●Enabled：开启

●Disabled：关闭

默认值：Enabled

Erase SEL

清除系统事件记录控制开关，菜单选项：

●No：不清除

●Yes, On next reset：下次重启清除一次

●Yes, On every reset：每次重启都清除一次

默认值：No

When SEL is Full

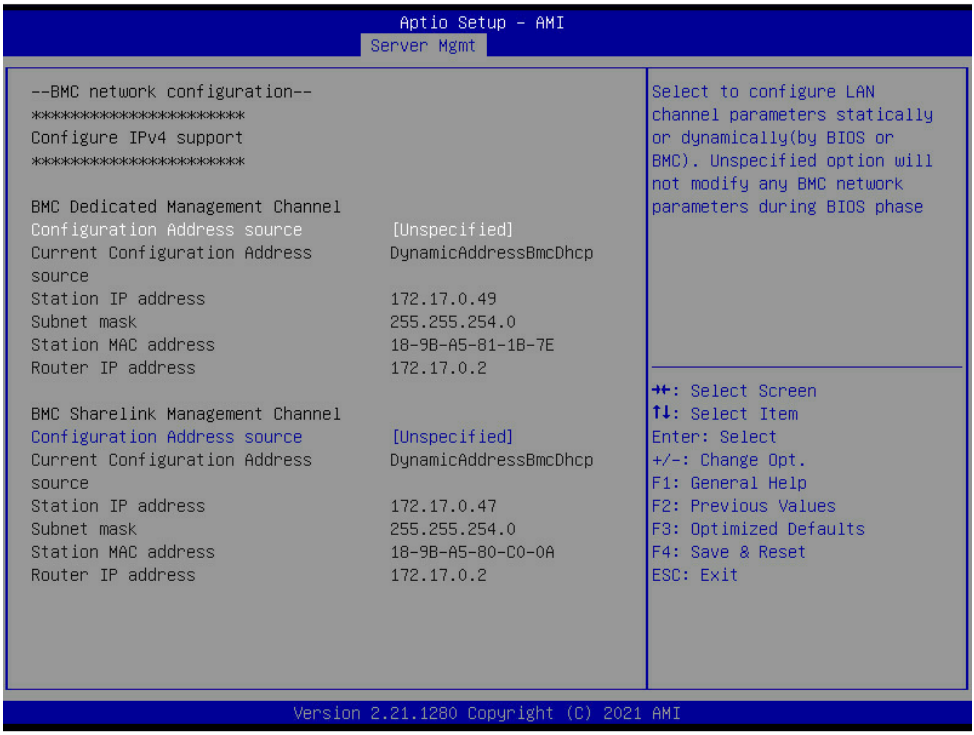
系统事件记录存储空间已满时，操作控制开关，菜单选项：

●Do Nothing：不操作

●Erase Immediately：立即清除

默认值：Do Nothing

BMC network configuration 菜单



BMC Dedicated Management Channel

显示 IPMI 专用网口的网路参数信息，当前 IP 配置方式、BMC IP、子网掩码、MAC 地址、路由 IP。

BMC Sharelink Management Channel

显示系统共享网口的网路参数信息，当前 IP 配置方式、BMC IP、子网掩码、

MAC 地址、路由 IP。

Configuration Address source

配置 BMC IP 地址分配模式，菜单选项为：

●Unspecified：不改变 BMC 参数

●Static：BIOS 静态 IP 设置

●DynamicBmcDhcp：BMC 运行 DHCP 动态分配 IP

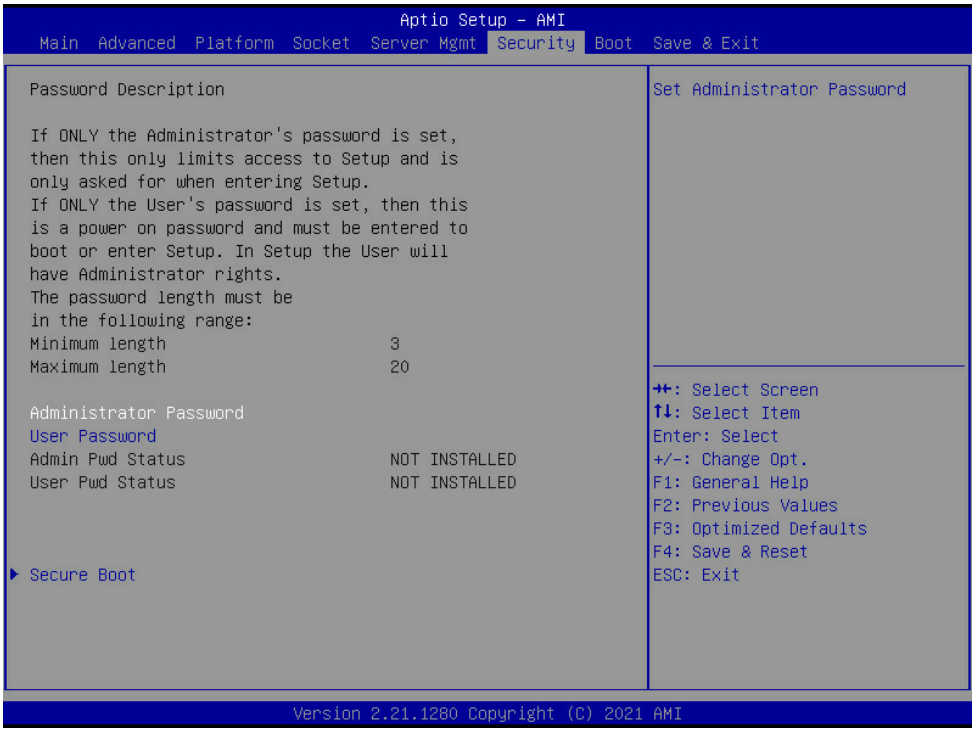
●DynamicBmcNonDhcp：BMC 运行 Non-DHCP 协议动态分配 IP

默认值：Unspecified

从 Unspecified 修改为其他参数，保存重启执行以后，选项将恢复 Unspecified 值，

无需每次启动过程都配置 BMC IP。

4.3.6 Security 菜单



Administrator Password

管理员密码设置选项，选择此选项，可编辑管理员密码。

User Password

用户密码设置选项，选择此选项，可编辑用户密码。

Admin Pwd Status

显示管理员密码状态，有密码“INSTALLED”，无密码“NOT INSTALLED”。

User Pwd Status

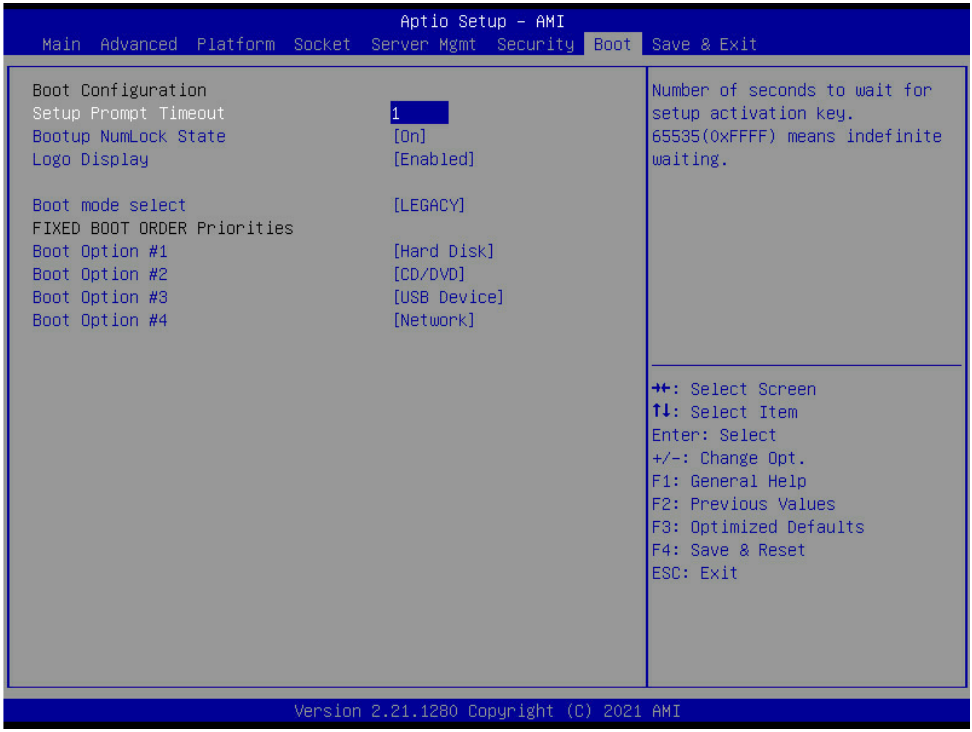
显示用户密码状态，有密码“INSTALLED”，无密码“NOT INSTALLED”。

Seacure Boot

安全启动功能选项。

4.3.7 Boot 菜单

Boot 界面（Legacy 模式）



Setup Prompt Timeout

启动选择提示时间控制。用户可输入范围 1~65535 秒，输入 65535 时，BIOS 将等待用户输入控制，再进行启动，默认为 1 秒。

Bootup NumLock State

键盘 NumLock 灯状态选择开关，菜单选项为：

●on：打开

●off：关闭

默认值：on

Logo Display

选择 Logo 模式，开启此选项时，输出 Logo 模式，关闭时输出文本模式，菜单

选项为：

●Enabled：开启

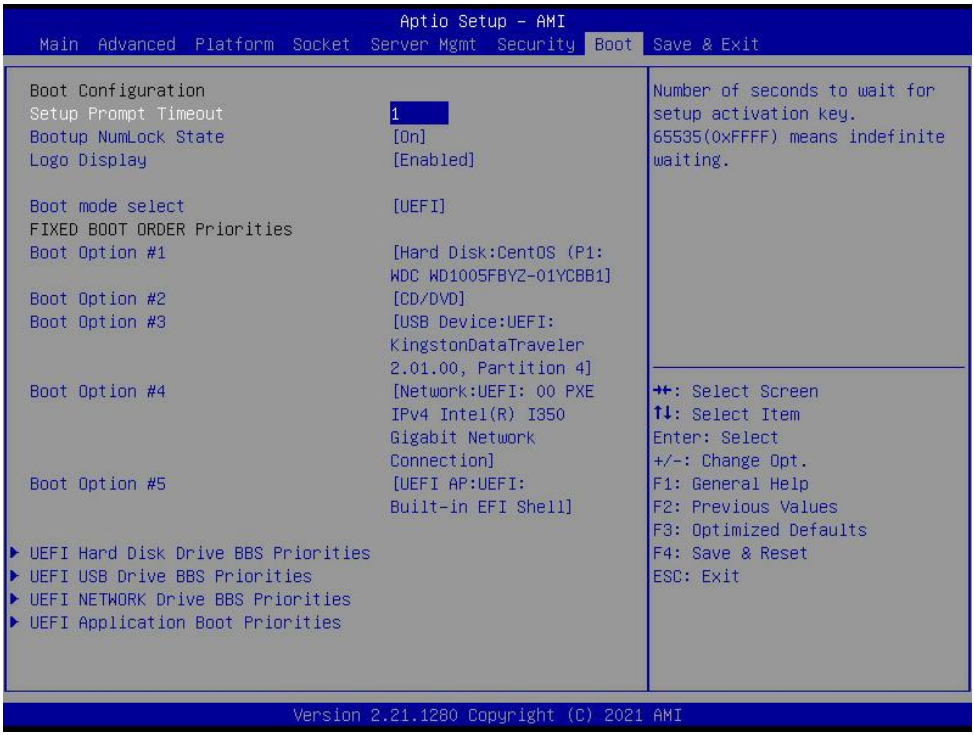
●Disabled：关闭

默认值：Enabled

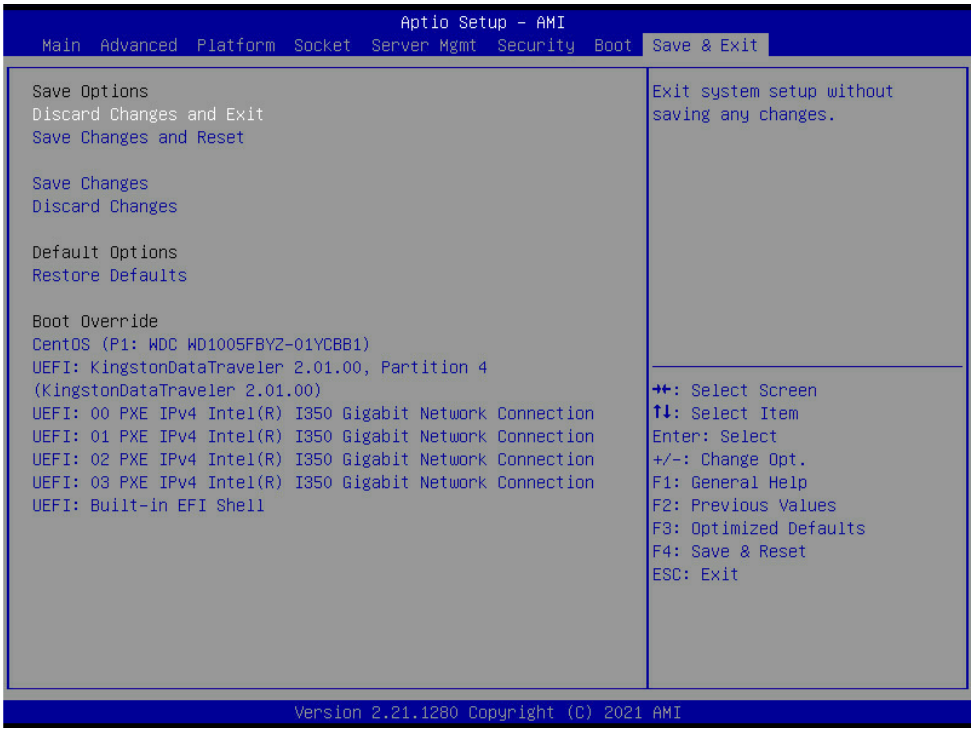
Boot Option Priorities

启动选项列表，此列表为动态显示，由系统中启动选项数量决定，无启动项时，不显示。

Boot 界面（UEFI 模式）



4.3.8 Save & Exit 菜单



Discard Changes and Exit

放弃改变并退出 Setup 界面。

Save Changes and Reset

保存改变并重启系统。

Save Changes

保存改变。

Discard Changes

放弃改变。

Restore Defaults

加载 BIOS 出厂默认值。

Boot Override

启动选项列表，可在此选择启动选项。

第五章 BMC 操作说明

详见同泰怡-Whitley 平台 T2DM BMC 功能说明

第六章 操作系统安装指南

详见 TTY TU628 V2 操作系统安装指南

第七章 Raid 卡操作指南

7.1 9361 Raid 卡操作指南

详见 LSI 9361-8i RAID 卡操作手册

7.2 3008 SAS 卡操作指南

详见 T3008HM SAS 卡操作手册

第八章 获得帮助

8.1 联系同泰怡

- 热线电话：400-168-6818
- 同泰怡官网：www.ttyinfo.com

第九章 附录

9.1 术语&缩略语

A	**AC**	Alternating Current	交流电
	ACPI	Advanced Configuration and Power Management Interface	高级配置和电源管理接口
	AES	Advanced Encryption Standard New Instruction Set	高级加密标准新指令集
	AVX	Advanced Vector Extensions	高级矢量扩展指令集
	AOC	Active Optical Cables	有源光缆
	API	Application Program Interface	应用程序接口
	ARP	Address Resolution Protocol	地址解析协议
	AEP	Apache Pass	Intel 第一代可持久内存
B	**BIOS**	Basic Input Output System	基本输入输出系统
	BMC	Baseboard Management Controller	主板管理控制单元
	BBU	Backup Battery Unit	备份电池单元
	BPS	Barlow Pass	Intel 第二代可持久内存
C	**CMOS**	Complementary Metal-Oxide-Semiconductor Transistor	互补金属氧化物半导体
	CPLD	Complex Programming Logic Device	复杂可编程逻辑器件
	CPU	Central Processing Unit	中央处理器
	CRPS	Common Redundant Power Supplies	通用冗余电源
	CSM	Compatibility Support Module	兼容性支持模块
D	**DC**	Direct Current	直流电
	DHCP	Dynamic Host Configuration Protocol	动态主机设置协议
	DEMT	Dynamic Energy Management Technology	动态能耗管理技术
	DIMM	Dual-Inline-Memory-Modules	双列直插内存模块
	DDR4	Double Date Rate 4	双倍数据速率 4
	DRAM	Dynamic Random-Access Memory	动态随机存储设备
	DNS	Domain Name System	域名服务系统

E	**ECC**	Error Checking and Correcting	内存错误检查和纠正
	EMC	ELECTRO MAGNETIC COMPATIBILITY	电磁兼容性
	EMI	ELECTRO MAGNETIC INTERFERENCE	电磁干扰
	ESD	ELECTRO STATIC DISCHARGE	静电释放
F	**FC**	Fiber Channel	光纤通道
	FRU	Field-Replaceable Unit	现场可更换部件
	FTP	File Transfer Protocol	文本传输协议
	FCoE	Fibre Channel Over Ethernet	以太网光纤通道
	FW	Firmware	固件
G	**GE**	Gigabit Ethernet	千兆以太网
	GPIO	General Purpose Input/Output	通用输入输出
	GPU	Graphics Processing Unit	图形处理单元
	GUI	Graphical User Interface	图形用户界面
H	**HBA**	Host Bus Adapter	主机总线适配器
	HCA	Host Channel Adapter	主机通道适配器
	HDD	Hard Disk Drive	机械硬盘驱动器
	HPC	High Performance Computing	高性能计算
	HTML	Hyper Text Markup Language	超文本标记语言
	HTTP	Hypertext Transfer Protocol	超文本传输协议
	HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
I	**I/O**	Input/Output	输入输出单元
	IEC	International Electrotechnical Commission	国际电工委员会
	IOPS	Input/Output Operations Per Second	每秒进行读写操作的次数
	IP	Internet Protocol	网际互连协议
	IPMB	Intelligent Platform Management Bus	智能平台管理总线
	IPMI	Intelligent Platform Management Interface	智能平台管理接口
	IRQ	INTERRUPT REQUEST	中断请求

K	**KVM**	Keyboard Video Mouse	键盘，显示器，鼠标三合一
L	**LAN**	Local Area Network	局域网
	LRDIMM	Load Reduced Dual In-Lane Memory Module	低负载双列直插式内存模块
	LOM	LAN On Motherboard	板载网卡
M	**MAC**	Media Access Control	媒体接入控制
	MBR	MASTER BOOT RECORD	主引导记录
	ME	Management Engine	英特尔管理引擎
N	**NCSI**	National Communication System Instructions	国家通信系统指南
	NIC	Network Interface Controller	网络接口控制器
	NTP	Network Time Protocol	网络时间协议
	NVDIMM	Non-Volatile Dual In-Line Memory Module	非易失性双列直插内存模块
	NVMe	Non-Volatile Memory Express	非易失性存储器标准
O	**OCP**	Open Compute Project	开放计算项目
	OS	Operating System	操作系统
P	**PCH**	Platform Controller Hub	平台路径控制器
	PCIe	Peripheral Component Interconnect express	快捷外围部件互连标准
	PDU	Power Distribution Unit	配电单元
	PHY	Physical	端口物理层
	POST	Power On Self Test	上电自检
	PSU	Power Supply Unit	电源设备
	PMBUS	Power Management Bus	电源管理总线
	PXE	Pre-boot Execution Environment	预启动运行环境
	PWM	Pulse-width Modulation	脉冲宽度调制

R	**RAS**	Reliability, Availability and Serviceability	可靠性、可用性、可服务性
	RAM	Random-Access Memory	随机存储器
	RAID	Redundant Arrays of Independent Drives	独立磁盘冗余阵列
	RDIMM	Registered Dual In-line Memory Module	暂存型双列直插内存模块
	ROM	Read-Only Memory	只读存储器
	RTC	Real Time Clock	实时时钟
S	**SAS**	Serial Attached Small Computer System Interface	串行连接的小型计算机系统接口
	SATA	Serial Advanced Technology Attachment	串行高级技术附件
	SFP	Small Form-factor Pluggable	小型可插拔收发光模块
	SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
	SNMP	Simple Network Management Protocol	简单网络管理协议
	SSD	Solid State Disk	固态磁盘
	SSH	Secure Shell	安全外壳协议
	SERDES	Serializer/Deserializer	串行器/解串器
	SEL	System Event Log	系统事件日志
	SOL	Serial Over LAN	串口重定向
T	**TCG**	Trusted Computing Group	可信计算组织
	TCM	Trusted Cryptography Module	可信密码模块
	TCO	Total Cost of Ownership	总拥有成本
	TDP	Thermal Design Power	热设计功耗
	TPCM	Trusted Platform Control Module	可信平台控制模块
	TPM	Trusted Platform Module	可信平台模块
U	**UEFI**	Unified Extensible Firmware Interface	统一可扩展固件接口
	UID	User Identification	定位指示灯
	UPI	Ultra Path Interconnect	超级通道互联
	UPS	Uninterruptible Power Supply	不间断电源
V	**VGA**	Video Graphics Array	视频图形阵列
	VLAN	Virtual Local Area Network	虚拟局域网
X	**XDP**	eXtend Debug Port	XDP 扩展调试接口