Dell EMC PowerEdge R750xa

BIOS and UEFI Reference Guide

Part Number: E71S
Regulatory Type: E71S001
July 2021
Rev. A02

注意、小心和警告

注： “注意”表示帮助您更好地使用该产品的重要信息。

小心： **“小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。**

警告： **“警告”表示可能会导致财产损失、人身伤害甚至死亡。**

Contents

1

预装操作系统管理应用程序

通过使用系统固件，可以在不引导至操作系统的情况下管理系统的基本设置和功能。

用于管理预操作系统应用程序的选项

您可以使用以下任意一个选项来管理预装操作系统应用程序：

- 系统设置程序
- 戴尔生命周期控制器
- 引导管理器
- 预引导执行环境 (PXE)

主题：

系统设置程序

使用**系统设置**选项，您可以配置 BIOS 设置、iDRAC 设置以及系统的设备设置。

您可以使用以下界面之一访问系统设置：

- 图形用户界面 — 要访问 iDRAC 控制面板，请单击**配置** > **BIOS 设置**。
- 文本浏览器 — 要启用文本浏览器，请使用控制台重定向。

要查看**系统设置**，请启动系统，按 F2 键，然后单击 **系统设置主菜单**。

注： 如果按 F2 键之前已开始载入操作系统，等待系统完成引导过程，然后重新启动系统并重试。

注： 英特尔第 3 代至强可扩展高核心计数 (HCC) 处理器需要最低 BIOS 版本 1.2.x。

系统设置主菜单屏幕上的选项如下表中所述：

表. 1: 系统设置程序主菜单

选项	说明
系统 BIOS	允许您配置 BIOS 设置。
iDRAC 设置	允许您配置 iDRAC 设置。iDRAC 设置设置程序是一种接口，用于使用 UEFI（统一扩展固件接口）设置和配置 iDRAC 参数。可使用 iDRAC 设置实用程序启用或禁用各种 iDRAC 参数。有关使用 iDRAC 的更多信息，请参阅《*Integrated Dell Remote Access Controller User's Guide*》（Integrated Dell Remote Access Controller 用户指南），网址：www.dell.com/poweredgemanuals。
设备设置	允许您为存储控制器或网卡等设备配置设备设置。

系统 BIOS

要查看**系统 BIOS** 屏幕，启动系统、按 F2，然后单击 **系统设置主菜单** > **系统 BIOS**。

表. 2: 系统 BIOS 详细信息

选项	说明
系统信息	提供有关系统的信息，如系统型号名称、BIOS 版本、服务编号等。
内存设置	显示与所安装内存有关的信息和选项。
处理器设置	显示与处理器有关的信息和选项，如速度、高速缓存大小等。
SATA 设置	显示用于启用或禁用集成 SATA 控制器和端口的选项。
NVMe 设置	显示用于更改网络设置的选项。如果系统中包含您想要在 RAID 阵列中配置的 NVMe 驱动器，您必须将此字段和 **SATA 设置**菜单上的**嵌入式 SATA** 字段设置为 **RAID** 模式。您可能还需要将**引导模式**设置更改为 **UEFI**。否则，您应将此字段设置为**非 RAID** 模式。
引导设置	显示各选项以指定引导模式（BIOS 或 UEFI）。支持您修改 UEFI 和 BIOS 引导设置。
网络设置	指定用于管理 UEFI 网络设置和引导协议的选项。 传统网络设置从**设备设置**菜单进行管理。 **注:** BIOS 引导模式下不支持“网络设置”。
集成设备	显示用于管理集成设备控制器和端口的选项，以及指定相关的功能和选项。
串行通信	显示用于管理串行端口的选项，以及指定相关的功能和选项。
系统配置文件设置	显示用于更改处理器电源管理设置、内存频率等等的选项。
系统安全	显示用于配置系统安全设置的选项，如系统密码、设置密码、可信平台模块 (TPM) 安全和 UEFI 安全引导。它还可以管理系统上的电源按钮。
冗余操作系统控制	设置冗余操作系统控制的冗余操作系统信息。
其他设置	指定更改系统日期和时间的选项。

系统信息

要查看**系统信息**屏幕，启动系统、按 F2，然后单击 **系统设置主菜单** > **系统 BIOS** > **系统信息**。

表. 3: 系统信息详细信息

选项	说明
系统型号名称	指定系统的型号名称。
系统 BIOS 版本	指定系统上安装的 BIOS 版本。
系统 Management Engine 版本	显示 Management Engine 固件的当前版本。
系统服务编号	指定系统服务编号。
系统制造商	指定系统制造商的名称。
系统制造商联系人信息	指定系统制造商的联系信息。
系统 CPLD 版本	指定系统复杂可编程逻辑设备 (CPLD) 固件的当前版本。
UEFI 合规性版本	指定系统固件的 UEFI 合规性等级。

内存设置

要查看 **Memory Settings** 屏幕，启动系统、按 F2，然后单击 **System Setup Main Menu** > **System BIOS** > **Memory Settings**。

表. 4: Memory Settings 详细信息

选项	说明
System Memory Size	指定系统内存的大小。
System Memory Type	指定系统中安装的内存类型。
System Memory Speed	指定系统内存的速度。
System Memory Voltage	指定系统内存的电压。
Video Memory	指定视频内存的大小。
System Memory Testing	指定系统内存测试是否在系统引导期间运行。可能的选项包括 **Enabled** 和 **Disabled**。该选项默认设置为 **Disabled**。
Memory Operating Mode	指定内存运行模式。该选项可用，并且默认设置为 **Optimizer Mode**。
Current State of Memory Operating Mode	指定内存运行模式的当前状态。
Node Interleaving	启用或禁用节点交叉存取选项。指定是否支持非一体化内存体系结构 (NUMA)。如果此字段为 **Enabled**，则在安装对称内存配置的情况下支持内存交叉存取。如果为 **Disabled**，则系统支持 NUMA（非对称）内存配置。该选项默认设置为 **Disabled**。
ADDDC Settings	启用或禁用 ADDDC 设置功能。已启用自适应双 DRAM 设备纠正 (ADDDC) 时，将动态映射故障 DRAM。当设置为 **Enabled** 时，在特定工作负载下可能对系统性能造成一些影响。此功能仅适用于 x4 DIMM。该选项默认设置为 **Disabled**。
Memory training	当选项设置为 **Fast** 且未更改内存配置时，系统将使用以前保存的内存培训参数来对内存子系统和系统引导时间进行定型。如果更改了内存配置，系统将 **Retrain at Next boot** 自动启用重新培训，强制执行一次性的完整内存培训步骤，然后返回到 **Fast**。 当选项设置为 **Retrain at Next boot** 时，系统将执行 在下次开机时强制执行一次性完整内存培训步骤，并在下次引导时使引导时间变慢。 当选项设置为 **Enabled** 时，系统 在每次开机时强制执行完整内存培训步骤，并在下次引导时使引导时间变慢。
Correctable Error Logging	启用或禁用可纠正的错误日志记录。该选项默认设置为 **Enabled**。
Dark Memory: Total Memory Available	启用或禁用黑色内存功能。黑色内存功能允许软件更改内存大小。此选项默认设置为 **Disabled**，需要由个性模块启用。

永久性内存详细信息

永久性内存屏幕详情可在《*PMem 用户指南*》中查看，网址：https://www.dell.com/poweredgemanuals。

处理器设置

要查看 **Processor Settings** 屏幕，请启动系统、按 F2，然后单击 **System Setup Main Menu** > **System BIOS** > **Processor Settings**。

表. 5: Processor Settings 详细信息

选项	说明
Logical Processor	每个处理器内核最多支持两个逻辑处理器。如果此选项设置为 **Enabled**，BIOS 会显示所有逻辑处理器。如果此选项设置为 **Disabled**，BIOS 只会显示每个核心的一个逻辑处理器。该选项默认设置为 **Enabled**。
CPU Interconnect Speed	使您能够监管系统中的处理器之间的通信链接频率。

表. 5: Processor Settings 详细信息 （续）

选项	说明
	注: 标准和基本 bin 处理器支持较低的链路频率。 可用的选项是 **Maximum data rate**、**11.2 GT / s**、**10.4 GT/s** 和 **9.6 GT/s**。此选项默认设置为 **Maximum data rate**。 最大数据速率表示 BIOS 以处理器支持的最大频率运行通信链路。您也可以选择特定的频率的处理器支持,该驱动器可以有所不同。 为获得最佳性能,您应选择 **Maximum data rate**。通信链路频率的任何降低都会影响非本地内存访问的性能和高速缓存一致性流量。它会降低从特定处理器对非本地 I/O 设备的访问速度。 但是，如果节能的注意事项优于性能，则降低处理器通信链路的频率。降低频率之前，您必须本地化连接到最近的 NUMA 节点的内存和 I/O 访问，以最小化到系统性能的影响。
Virtualization Technology	启用或禁用的处理器虚拟化技术。该选项默认设置为 **Enabled**。
Directory Mode	启用或禁用目录模式。该选项默认设置为 **Enabled**。
Adjacent Cache Line Prefetch	针对需要大量使用顺序内存访问的应用程序优化系统。该选项默认设置为 **Enabled**。您可以禁用需要大量使用随机内存访问的应用程序的此选项。
Hardware Prefetcher	启用或禁用硬件预取器。该选项默认设置为 **Enabled**。
DCU Streamer Prefetcher	启用或禁用数据高速缓存设备 (DCU) 流转化器预取器。该选项默认设置为 **Enabled**。
DCU IP Prefetcher	启用或禁用数据高速缓存设备 (DCU) IP 预取器。该选项默认设置为 **Enabled**。
Sub NUMA Cluster	启用或禁用子 NUMA 群集。该选项默认设置为 **Disabled**。
MADT Core Enumeration	指定 MADT Core 枚举。此选项在 **Round Robin** 中设置为默认值。
UPI Prefetch	支持您尽早获取 DDR 总线上的内存读数。超路径互连 (UPI) Rx 路径会直接将推测内存读数蔓延到集成内存控制器 (iMC)。该选项默认设置为 **Enabled**。
XPT Prefetch	该选项默认设置为 **Enabled**。
LLC Prefetch	启用或禁用所有线程上的 LLC 预取。该选项默认设置为 **Enabled**。
Dead Line LLC Alloc	启用或禁用截止日期 LLC 分配。该选项默认设置为 **Enabled**。您可以启用此选项以在 LLC 中输入失效行，或者禁用在 LLC 中输入失效行的选项。
Directory AtoS	启用或禁用“Directory AtoS”。AToS 优化可以减少重复读取访问的远程读取延迟，而不影响写入。该选项默认设置为 **Disabled**。
Logical Processor Idling	可让您以提高系统的能源效率。它使用操作系统核心休眠算法，并将系统中的一些逻辑处理器置于休眠状态，这反过来又允许相应的处理器核心数转换为低功耗空闲状态。仅当操作系统支持它可以启用此选项。该选项默认设置为 **Disabled**。 **注:** 如果 CPU 电源管理设置为 **Maximum Performance**，此功能不受支持。

表. 5: Processor Settings 详细信息 （续）

选项	说明
AVX P1	使您能够基于系统的电力和热传递能力在 POST 期间重新配置处理器热设计功耗 (TDP) 级别。TDP 验证冷却系统需要消散的最大热量。此选项默认设置为 **Normal**。 **注:** 此选项仅在处理器的某些库存单位 (SKU) 上可用。
Dynamic SST-Performance Profile	允许您使用动态或静态速度选择技术来重新配置处理器。该选项默认设置为 **Disabled**。
SST-Performance Profile	允许您使用速度选择技术重新配置处理器。
Intel SST-BF	启用“Intel SST-BF”。如果已选择性能功耗比（操作系统）或自定义（当 OSPM 已启用时）系统配置文件，将显示此选项。该选项默认设置为 **Disabled**。
Intel SST-CP	启用“Intel SST-CP”。如果已选择性能功耗比（操作系统）或自定义（当 OSPM 已启用时）系统配置文件，将显示此选项。对于每个系统配置文件模式，此选项都会显示并可选择。此选项默认设置为 **Disabled**。
x2APIC Mode	启用或禁用“x2APIC Mode”。该选项默认设置为 **Enabled**。 **注:** 对于两个处理器 64 核心配置，如果启用了 256 线程（BIOS 设置：已启用所有 CCD、核心和逻辑处理器），则 x2APIC 模式不可切换。
AVX ICCP Pre-Grant License	启用或禁用 AVX ICCP 预授予许可证。该选项默认设置为 **Disabled**。
AVX ICC Pre-Grant Level	使您可以在英特尔提供的不同 AVX ICC 转移级别之间进行选择。此选项默认设置为 **128 heavy**。
Dell Controlled Turbo	
Dell Controlled Turbo Settings	控制涡轮增压。只有当系统配置文件设置为 **Performance** 或 **Custom** 且 CPU 电源管理设置为 **Performance** 时启用可为每个系统配置文件模式选择此项。该选项默认设置为 **Disabled**。 **注:** 根据安装的处理器数量，可能会有多达两个处理器列表。
Dell AVX Scaling Technology	允许您配置戴尔 AVX 扩展技术。该选项默认设置为 **0**。输入 0 至 12 bin 的值。当已启用戴尔控制的睿频功能时，输入的值降低了戴尔 AVX 扩展技术频率。
Optimizer Mode	启用或禁用 CPU 性能。当此选项设置为 **Auto** 时，将 CPU 电源管理设置为“Max Performance”。当设置为 **Enabled** 时，启用 CPU 电源管理设置。当设置为 **Disabled** 时，CPU 电源管理选项将被禁用。此选项默认设置为 **Auto**。
Number of Cores per Processor	控制每个处理器中的已启用核心数。此选项默认设置为 **All**。
Processor Core Speed	显示处理器的最大内核频率。
Processor Bus Speed	指定处理器的总线速度。 **注:** 处理器总线速度选项仅在同时安装两个处理器时才显示。
Local Machine Check Exception	启用或禁用本地计算机检查异常。这是 MCA 恢复机制的扩展，它提供了将未纠正的可恢复 (UCR) 软件可恢复操作 (SRAR) 错误发送至一个或多个特定逻辑处理器线程（接收之前污染或损坏的数据）的功能。启用时，UCR SRAR 机器将检查异常仅传送到受影响的线程，而不是广播至系统中的所有线程。当检测到接近临近的多个可恢复故障时，此功能支持操作系统恢复，否则会导致严重的机器检查事件。此功能仅适用于高级 RAS 处理器。该选项默认设置为 **Disabled**。

表. 5: Processor Settings 详细信息 （续）

选项	说明
Processor n	**注:** 根据处理器数量，最多可能会列出 n 个处理器。 对于每个处理器，将显示下列设置：

表. 6: 处理器 n 详细信息

选项	说明
Family-Model-Stepping	显示英特尔定义的处理器系列、型号和步进。
Brand	显示品牌名称。
Level 2 Cache	显示 L2 高速缓存总和。
Level 3 Cache	显示 L3 高速缓存总和。
Number of Cores	显示每个处理器的内核数。
Maximum Memory Capacity	指定每个处理器的最大内存容量。
Microcode	指定处理器微码版本。

SATA 设置

要查看 **SATA 设置**屏幕，启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **SATA 设置**。

表. 7: SATA 设置详细信息

选项	说明
嵌入式 SATA	支持将嵌入式 SATA 选项设置为**关闭**、**AHCI 模式**或 **RAID 模式**。该选项默认设置为 **AHCI 模式**。 **注:** 1. 您可能还需要将引导模式设置更改为 UEFI。否则，应将此字段设置为非 RAID 模式。 2. 在 RAID 模式下不支持 ESXi 和 Ubuntu 操作系统。
安全冻结锁定	在开机自测过程中将安全冻结锁定命令发送给嵌入式 SATA 驱动器。此选项仅适用于 AHCI 模式。该选项默认设置为**已启用**。
写入高速缓存	在 POST 过程中启用或禁用嵌入式 SATA 驱动器的命令。该选项默认设置为**已禁用**。
端口 n	设置所选设备的驱动器类型。 对于 **AHCI 模式** 或 **RAID 模式**，总是启用 BIOS 支持。

表. 8: 端口 n

选项	说明
型号	指定所选设备的驱动器型号。
驱动器类型	指定连接至 SATA 端口的驱动器类型。
容量	指定驱动器的总容量。对于可移动介质设备，如光驱，此字段未定义。

NVMe 设置

此选项可设置 NVMe 驱动器模式。如果系统中包含您想要在 RAID 阵列中配置的 NVMe 驱动器，您必须将 SATA 设置菜单上的此字段和“嵌入式 SATA”字段设置为 RAID 模式。您可能还需要的“引导模式”设置更改为 UEFI。

要查看 **NVMe 设置**屏幕，请启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **NVMe 设置**。

表. 9: NVMe 设置详细信息

选项	说明
NVMe 模式	启用或禁用引导模式。该选项默认设置为**非 RAID** 模式。
BIOS NVMe 驱动程序	设置用于引导 NVMe 驱动程序的驱动器类型。可用的选项有**戴尔合格的驱动器**和**所有驱动器**。该选项默认设置为**戴尔合格的驱动器**。

引导设置

您可以使用**引导设置**屏幕将引导模式设置为 **BIOS** 或 **UEFI**。它还允许您指定引导顺序。

- **UEFI**:统一可扩展固件接口(UEFI)都是一个新接口之间的操作系统和平台固件。该接口中包含数据表和平台相关信息，以及操作系统及其加载程序可用的引导和运行时服务呼叫。以下优势仅在**引导模式**设置为 **UEFI** 时才能体现。
  - 支持大于 2 TB 的驱动器分区。
  - 增强的安全性(例如, UEFI 安全引导)。
  - 更快的引导时间。

  注: 您必须使用 UEFI 引导模式，以便从 NVMe 驱动器进行引导。
- **BIOS**：**BIOS 引导模式**是传统引导模式。此位置支持向后兼容性。

要查看**引导设置**屏幕，启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **引导设置**。

表. 10: 引导设置详细信息

选项	说明
引导模式	允许您设置系统的引导模式。如果操作系统支持 UEFI，则可将此选项设置为 UEFI。将此字段设置为 BIOS 后，可与非 UEFI 操作系统兼容。该选项默认设置为 **UEFI**。 **小心: 如果操作系统不是在同一种引导模式下安装，则切换引导模式可能会阻止系统引导。** **注:** 将此字段设置为 UEFI 将禁用 **BIOS 引导设置**菜单。
引导顺序重试	启用或禁用引导顺序重试功能或重置系统。如果此选项设置为**已启用**并且系统引导失败，系统将在 30 秒后重新尝试引导顺序。当此选项设置为**重置**并且系统无法引导时，系统会立即重新引导。该选项默认设置为**已启用**。
硬盘故障切换	启用或禁用硬盘故障切换。该选项默认设置为**已禁用**。
通用 USB 引导	启用或禁用通用 USB 引导占位符。该选项默认设置为**已禁用**。
硬盘占位符	启用或禁用硬盘占位符。该选项默认设置为**已禁用**。
清理所有 Sysprep 顺序和变量	当此选项设置为**无**时，BIOS 将不执行任何操作。当设置为**是**时，BIOS 将删除 SysPrep #### 和 SysPrepOrder 的变量。此选项是一次性选项，删除变量时将重设为“无”。此设置仅在 **UEFI 引导模式**下可用。该选项默认设置为**无**。
UEFI 引导设置	指定 UEFI 引导顺序。启用或禁用 UEFI 引导选项。 **注:** 此选项控制 UEFI 引导顺序。将首先尝试列表中的第一个选项。

表. 11: UEFI 引导设置

选项	说明
UEFI 引导顺序	允许您更改引导设备的顺序。
引导选项启用/禁用	允许您选择已启用或已禁用的引导设备。

选择系统引导模式

系统设置程序也能让您指定其中一个用于安装操作系统的引导模式：

- UEFI 引导模式（默认）是增强的 64 位引导接口。

如果您已将系统配置为引导至 UEFI 模式，则会更换系统 BIOS。

1. 单击**系统设置程序主菜单**中的**引导设置**，然后选择**引导模式**。
2. 选择您希望系统引导至的 UEFI 引导模式。

   小心：如果操作系统不是在同一种引导模式下安装，则切换引导模式可能会阻止系统引导。
3. 在系统以指定引导模式引导后，从该模式安装操作系统。

注： 操作系统必须与 UEFI 兼容才能从 UEFI 引导模式安装。DOS 和 32 位操作系统不支持 UEFI，只能通过 BIOS 引导模式进行安装。

注： 有关支持的操作系统的最新信息，请转至 www.dell.com/ossupport。

更改引导顺序

关于此任务

如果您想从 USB 闪存盘或光驱引导，您可能需要更改引导顺序。如果您已选择了 **BIOS Boot Mode**（引导模式），则此处给出的说明可能会有所不同。

注： 只有在 BIOS 引导模式下才支持更改驱动器引导顺序。

步□

1. 在**系统设置主菜单**屏幕上，单击**系统 BIOS** > **引导设置** > **UEFI 引导设置** > **UEFI 引导顺序**。
2. 使用箭头键选择引导设备，然后使用加号 (+) 和减号 (-) 将设备按顺序向下或向上移动。
3. 单击**退出**，然后单击**是**以在退出后保存设置。

   注： 您还可以根据需要启用或禁用引导顺序设备。

网络设置

要查看**网络设置**屏幕，请启动系统，按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **网络设置**。

注： BIOS 引导模式下不支持“网络设置”。

表. 12: 网络设置详细信息

选项	说明
UEFI PXE 设置	允许您控制 UEFI PXE 设备的配置。
PXE 设备 n (n = 1-4)	启用或禁用此设备。启用时，则为设备创建 UEFI PXE 引导选项。
PXE 设备 n 设置 (n = 1 至 4)	允许您控制 PXE 设备的配置。
UEFI HTTP 设置	允许您控制 UEFI HTTP 设备的配置
HTTP 设备 n (n = 1 至 4)	启用或禁用此设备。启用时，则为设备创建 UEFI HTTP 引导选项。
HTTP 设备 n 设置 (n = 1-4)	允许您控制 HTTP 设备的配置。
UEFI iSCSI 设置	允许您控制 iSCSI 设备的配置。

表. 13: PXE 设备 n 设置详细信息

选项	说明
界面	确定用于 PXE 设备的 NIC 接口。
协议	指定用于 PXE 设备的协议。此选项设置为 **IPv4** 或 **IPv6**。此选项默认设置为 **IPv4**。
Vlan	为 PXE 设备启用 Vlan。此选项设置为**启用**或**禁用**。该选项默认设置为**禁用**。
Vlan ID	显示 PXE 设备的 Vlan ID
Vlan 优先级	显示 PXE 设备的 Vlan 优先级。

表. 14: UEFI iSCSI 设置屏幕详细信息

选项	说明
iSCSI 启动器名称	指定 iSCSI 启动器的名称（IQN 格式）。
iSCSI 设备 1	启用或禁用 iSCSI 设备。禁用后，将为 iSCSI 设备自动创建 UEFI 引导选项。该选项默认设置为**已禁用**。
iSCSI 设备 1 设置	允许您控制 iSCSI 设备的配置。

表. 15: ISCSI 设备 1 设置屏幕详细信息

选项	说明
连接 1	启用或禁用 iSCSI 连接。该选项默认设置为**禁用**。
连接 2	启用或禁用 iSCSI 连接。该选项默认设置为**禁用**。
连接 1 设置	允许您控制 iSCSI 连接的配置。
连接 2 设置	允许您控制 iSCSI 连接的配置。
连接顺序	允许您控制尝试进行 iSCSI 连接的顺序。

集成设备

要查看**集成设备**屏幕，请启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **集成设备**。

表. 16: 集成设备详细信息

选项	说明
用户可访问 USB 端口	禁用前端用户可访问 USB 端口。选择**仅背面端口打开**可禁用正面 USB 端口；选择**所有端口关闭**可禁用所有短裤和背面 USB 端口；选择**所有端口关闭（动态）**可在 POST 期间禁用所有正面和背面 USB 端口。默认情况下，此选项设置为**打开所有端口**。 当用户可访问 USB 端口设置为**关闭所有端口（动态）**时，**仅启用正面端口**选项已启用。 • **仅启用正面端口**：在操作系统运行时启用或禁用正面 USB 端口。 在引导过程中 USB 键盘和鼠标在某些 USB 端口中仍可正常工作，具体取决于选择。引导过程完成后，USB 端口将根据设置启用或禁用。
iDRAC Direct USB 端口	iDRAC Direct USB 端口由 iDRAC 专门管理，主机不可见。此选项设置为**开**或**关**。当设置为**关**时，iDRAC 无法检测到此管理端口中安装的任何 USB 设备。此选项默认设置为**开**。
内部 SD 卡端口	内部双 SD 模块(IDSDM)启用或禁用内部 SD 卡端口。此选项默认设置为**开**。
内部 SD 卡冗余	配置内部双 SD 模块 (IDSDM) 的冗余模式。如果设置为**镜像**模式，数据将同时写入两张 SD 卡。数据写入两个 SD 卡中。一旦其中一个卡发生故障或对故障的卡进行了更换，在系统引导期间活动卡上的数据就被复制到脱机卡中。 内部 SD 卡冗余设置为**已禁用**时，则仅主要 SD 卡在操作系统中可见。该选项默认设置为**已禁用**。
内部 SD 主卡	默认情况下，已选择主要 SD 卡作为 SD 卡 1。如果 SD 卡 1 不存在，则该控制器将选择 SD 卡 2 作为主要 SD 卡。
嵌入式 NIC1 和 NIC2	启用或禁用嵌入式 NIC1 和 NIC2。当设置为**已禁用 (OS)** 时，NIC 仍可用于嵌入式管理控制器的共享网络访问。通过使用系统的 NIC 管理实用程序配置**嵌入式 NIC1 和 NIC2** 选项。
I/OAT DMA 引擎	启用或禁用 I/O 加速技术 (I/OAT) 选项。I/OAT 是一系列 DMA 功能，旨在加速网络通信并降低 CPU 利用率。仅在硬件和软件均支持此功能时启用。该选项默认设置为**已禁用**。

表. 16: 集成设备详细信息 （续）

选项	说明
嵌入式视频控制器	启用或禁用“嵌入式视频控制器”作为主要显示屏的使用。当设置为**已启用**时，嵌入式视频控制器将用作主显示器，即使已安装附加式显卡。当设置为**已禁用**时，附加式显卡将用作主显示器。BIOS 在开机自检过程中和预引导环境中将输出显示为两个主要附加式视频和嵌入式视频。在操作系统引导之前，嵌入式视频将立即被禁用。该选项默认设置为**已启用**。 **注:** 当系统中已安装附加式显卡时，在 PCI 枚举过程中查找到的第一个卡已选中作为主视频。您可能需要重新排列插槽中的插卡，以便控制哪些插卡是主视频。
I/O 监听推迟响应	选择 PCI I/O 可以拒绝的 CPU 监测请求的周期数，以留出时间完成其自己的 LLC 写入。此设置可帮助改进性能上的吞吐量和延迟严重的工作负载。
嵌入式视频控制器的当前状态	显示嵌入式视频控制器的当前状态。**嵌入式视频控制器的当前状态**选项为只读字段。如果嵌入式视频控制器是系统中唯一的显示功能（即没有安装附加显卡），那么即使**嵌入式视频控制器**设置为 **已禁用**，“嵌入式视频控制器”设置也会自动用作主显示屏。
SR-IOV 全局启用	启用或禁用单根 I/O 虚拟化 (SR-IOV) 设备的 BIOS 配置。该选项默认设置为**已禁用**。
OS 监督计时器	如果系统停止响应，则此监督计时器可帮助恢复操作系统。此选项设置为**已启用**时，操作系统会初始化计时器。此选项设置为**已禁用**（默认值）时，计时器不会对系统造成任何影响。
空插槽取消隐藏	启用或禁用 BIOS 和操作系统可访问的所有空插槽的根端口。该选项默认设置为**已禁用**。
高于 4 GB 的内存映射 I/O	启用或禁用需要大量内存的 PCIe 设备的支持。启用此选项仅适用于 64 位操作系统。该选项默认设置为**已启用**。
内存映射 I/O 基础	当设置为 **12 TB** 时，系统将 MMIO 基础映射至 12 TB。对于需要 44 位 PCIe 寻址的操作系统启用此选项。当设置为 **512 GB** 时，系统将 MMIO 基础映射为 512 GB，并将支持的最大内存降低到小于 512 GB。启用此选项仅适用于 4 GPU dgma 问题。此选项默认设置为 **56 TB**。
插槽禁用	启用或禁用系统上可用的 PCIe 插槽。“插槽禁用”功能控制指定插槽中安装的 PCIe 卡的配置。只有当安装的外设卡无法引导至操作系统或导致系统启动延迟时才必须使用插槽禁用功能。如果禁用插槽，选项 ROM 和 UEFI 驱动程序都会被禁用。只能是可用于控制系统上存在的插槽。
	插槽 n：启用或禁用或仅针对 PCIe 插槽 n 禁用引导驱动程序。该选项默认设置为**已启用**。
插槽分支	**自动发现分支设置**允许**平台默认分支**、和**手动分支控制**。
	此选项默认设置为**平台默认分支**。当设置为**手动分支控制**时，插槽分支字段将可访问；当设置为**平台默认分支**时，插槽分支字段将呈灰显。 **注:** 该插槽分支仅支持 PCIe 插槽，不支持从 Paddle 卡到提升板和超薄连接器到提升板的插槽类型。

串行通信

要查看**串行通信**屏幕，请启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **串行通信**。

注: 串行端口对于 PowerEdgeR750xa 系统是可选的。只有在系统中安装了串行 COM 端口时，“串行通信”选项才适用。

表. 17: 串行通信详细信息

选项	描述
串行通信	启用串行通信选项。选择 BIOS 中的串行通信设备。（串行设备 1 和串行设备 2）。也可以启用 BIOS 控制台重定向,并可指定端口地址。

表. 17: 串行通信详细信息 （续）

选项	描述
	没有串行 COM 端口 (DB9) 的系统可用选项为：**在没有控制台重定向情况下打开**、**在有控制台重定向的情况下打开**、**关闭**。该选项默认设置为**关闭**。 带串行 COM 端口 (DB9) 的系统可用的选项为**在没有控制台重定向的情况下打开**、**在有控制台重定向的情况下打开（通过 Com1）**、**在有控制台重定向的情况下打开（通过 Com2）**、**关闭**、**打开**。此选项默认设置为**自动**。
串行端口地址	允许您设置串行设备的端口地址。此选项默认设置为**串行设备 1 = COM2**、**串行设备 2 = COM1**。 **注:** 只能将串行设备 2 用于 LAN 上串行 (SOL) 功能。要通过 SOL 使用控制台重定向，请为控制台重定向和串行设备配置相同的端口地址。 **注:** 每次系统启动时，BIOS 中同步 iDRAC 中保存的串行 MUX 设置。串行 MUX 设置可单独在 iDRAC 中进行更改。因此，从 BIOS 设置实用程序加载 BIOS 默认设置并不总会将此串行 MUX 设置转换为设置为“串行设备 1”的默认设置。
外部串行连接器	通过使用此选项允许您将外部串行连接器关联到**串行设备 1**、**串行设备 2** 或**远程访问设备**。此选项默认设置为**串行设备 1**。 **注:** 只能将串行设备 2 用于 LAN 上串行 (SOL)。要通过 SOL 使用控制台重定向，请为控制台重定向和串行设备配置相同的端口地址。 **注:** 每次系统启动时，BIOS 中同步 iDRAC 中保存的串行 MUX 设置。串行 MUX 设置可单独在 iDRAC 中进行更改。因此，从 BIOS 设置实用程序加载 BIOS 默认设置并不总会将此设置转换为设置为 串行设备 1 的默认设置。
故障保护波特率	显示用于控制台重定向的故障保护波特率。BIOS 尝试自动确定波特率。仅当尝试失败时才使用故障保护波特率且不得更改此值。此选项默认设置为 **115200**。
远程终端类型	允许您设置远程控制台终端类型。此选项默认设置为 **VT100/VT220**。
引导后重定向	允许您在载入操作系统后启用或禁用 BIOS 控制台重定向。该选项默认设置为**已启用**。

系统配置文件设置

要查看**系统配置文件设置** 屏幕，请启动系统、按 F2，然后单击 **系统设置主菜单** > **系统 BIOS** > **系统配置文件设置**。

表. 18: 系统配置文件设置详细信息

选项	说明
系统配置文件	允许您设置系统密码。如果将**系统配置文件**选项设置为除自定义外的其它模式，BIOS 将自动设置其余选项。仅在模式设置为**自定义**时，才可更改其余选项。此选项默认设置为 **Performance Per Watt (DAPC)**。其他选项包括**性能**、**性能功耗比 (OS)**、**工作站**和**自定义**。 **注:** 只有在**系统配置文件**选项设置为**自定义**时，系统配置文件设置屏幕上的所有参数方可用。
CPU 电源管理	设置 CPU 电源管理。此选项默认设置为**系统 DBPM (DAPC)**。其他选项包括**最大性能**、**OS DBPM**。
内存频率	设置系统内存的速度。您可以选择**最大性能**、**最大可读性**，或特定速度。此选项默认设置为**最大性能**。
睿频加速	启用或禁用处理器在睿频加速模式下运行。该选项默认设置为**已启用**。
C1E	允许您在处理器处于闲置状态时启用或禁用处理器切换至最低性能状态。该选项默认设置为**已启用**。

表. 18: 系统配置文件设置详细信息 （续）

选项	说明
C 状态	允许您启用或禁用处理器在所有可用电源状态下运行。C 状态允许处理器在空闲时进入低功率状态。当设置为**已启用**（操作系统控制）或设置为**自治**（如果支持硬件控制器）时，处理器能够在所有可用的电源状态下运行以节省电量，但可能会增加内存延迟和频率抖动。该选项默认设置为**已启用**。
内存轮巡	设置内存轮巡模式。此选项默认设置为**标准**。
内存刷新率	将“内存刷新率”设置为 1x 或 2x。此选项默认设置为 **1x**。
非核心频率	允许您选择**非内核频率**选项。 **动态模式**使处理器能够在运行时跨核心和非核心优化电源资源。将非核心频率优化设置为节省电源，否则优化性能将受**能效策略**选项的设置影响。
能效策略	允许您选择**能效策略**选项。CPU 会使用该设置来操作处理器的内部行为并确定是定位更高的性能还是更好的节能效果。此选项默认设置为**平衡性能**。
Monitor/Mwait	启用处理器中的 Monitor/Mwait 指令。对于所有系统配置文件，此选项默认设置为**已启用**，**自定义**除外。 **注:** 仅当 C 状态选项在自定义模式下设置为已禁用时，才能禁用此选项。 **注:** 当 C States 在 Custom 模式下设置为 Enabled 时，更改 Monitor/Mwait 设置不会影响系统电源或性能。
CPU 互连总线链路电源管理	启用或禁用 CPU 互连总线链路电源管理。该选项默认设置为**已启用**。
PCI ASPM L1 链路电源管理	启用或禁用 PCI **ASPM L1 链路电源管理**。该选项默认设置为**已启用**。
处理器 EIST	启用或禁用 PCI **处理器 EIST**。该选项默认设置为**已启用**。
英特尔永久性内存 CR QoS	允许选择调整 QoS 旋钮的的**方法 1** 并且建议有效目录中的 2-2-2 内存配置，QoS 旋钮的的**方法 2** 并且建议有效目录中的其他内存配置，或者 QoS 旋钮的的**方法 3** 并且建议为每个通道配置 1 个 DIMM。该选项默认设置为**模式 0**。
英特尔永久性内存性能设置	允许根据工作负载行为选择 NVMe 性能设置。如果此选项设置为 **BW 优化**，则针对 DDR 和 DDRT 带宽优化性能。如果此选项设置为**延迟优化**，则性能是更好的 DDR 延迟。此选项默认设置为 **BW 优化**。

系统安全

要查看**系统安全**屏幕，启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **系统安全**。

表. 19: 系统安全详细信息

选项	说明
CPU AES-NI	通过使用高级加密标准指令集 (AES-NI) 执行加密和解密来提高应用程序速度。默认设置为已启用。该选项默认设置为**已启用**。
系统密码	设置系统密码。此选项默认设置为**已启用**，并且如果系统上未安装密码跳线，此选项为只读。
设置密码	设置系统密码。如果系统上未安装密码跳线，此选项为只读。
密码状态	锁定系统密码。该选项默认设置为**已解锁**。
TPM 信息	指示可信平台模块的类型（如果有）。

表. 20: TPM 1.2 安全信息

选项	说明
TPM 信息	
TPM 安全	**注:** TPM 菜单仅在安装 TPM 模块时可用。 使您能够控制可信平台模块 (TPM) 的报告模式。默认情况下，**TPM 安全**选项设置为**关**。如果 **TPM 状态**字段设置为**开，进行预引导测量**或**开，不进行预引导测量**，则仅可修改 TPM 状态和 TPM 激活。

表. 20: TPM 1.2 安全信息 （续）

选项	说明
	已安装 TPM 1.2 时，**TPM 安全**选项设置为**关**、**开，进行预引导测量** 或 **开，不进行与引导测量。**
TPM 信息	更改 TPM 的操作状态。该选项默认设置为**无更改。**
TPM 固件	指示 TPM 的固件版本。
TPM 状态	指定 TPM 状态。
TPM 命令	安装可信平台模块 (TPM)。当设置为**无**时，不会将命令发送到 TPM。当设置为**激活**时，将启用并激活 TPM。当设置为**取消激活**时，将禁用并取消激活 TPM。当设置为**清除**时，将清除 TPM 的所有内容。该选项默认设置为**无。**

表. 21: TPM 2.0 安全信息

选项	说明
TPM 信息	
TPM 安全	**注:** TPM 菜单仅在安装 TPM 模块时可用。 使您能够控制可信平台模块 (TPM) 的报告模式。默认情况下，**TPM 安全**选项设置为**关。**如果 **TPM 状态**字段设置为**开，进行预引导测量**或**开，不进行预引导测量**，则仅可修改 TPM 状态和 TPM 激活。 安装了 TPM 2.0 时，**TPM 安全**选项设置为**开**或**关。**该选项默认设置为**关。**
TPM 信息	更改 TPM 的操作状态。该选项默认设置为**无更改。**
TPM 固件	指示 TPM 的固件版本。
TPM 层级结构	启用、禁用或清除存储和认可层级结构。当设置为**已启用**时，存储和认可层级结构可以使用。 当设置为**已禁用**时，存储和认可层级结构无法使用。 当设置为**清除**时，存储和认可层级结构中的任何值都被清除，然后重设为**已启用。**
TPM 高级设置	指定 TPM 高级设置详情。

表. 22: 系统安全详细信息

选项	说明
英特尔(R) TXT	支持设置英特尔可信执行技术 (TXT) 选项。要启用此**英特尔 TXT** 选项，必须启用虚拟化技术以及进行预引导测量的 TPM 安全保护。该选项默认设置为**关。**
内存加密	启用或禁用英特尔总内存加密 (TME)。当选项设置为**已禁用**时，BIOS 将同时禁用 TME 和 MK-TME 技术。当选项设置为**已启用**时，BIOS 将启用 TME 技术。该选项默认设置为**已禁用。**
英特尔(R) SGX	允许您设置英特尔软件保护扩展 (SGX) 选项。要启用**英特尔 SGX** 选项，处理器必须支持 SGX，内存填充必须兼容（每个 CPU 插槽最少 8 个完全相同的 DIMM1 到 DIMM8），必须在优化程序模式下设置内存操作模式，必须启用内存加密，并且必须禁用节点交叉存取。该选项默认设置为**关。**当此选项设置为**关**时，BIOS 将禁用 SGX 技术。当此选项设置为**开**时，BIOS 将启用 SGX 技术。
SGX 软件包信息带内访问	允许您访问英特尔软件保护扩展 (SGX) 软件包信息带内选项。该选项默认设置为**关。**
PPMRR 大小	设置 PPMRR 大小。
SGX QoS	启用或禁用 SGX 服务质量。
选择所有者 EPOCH 输入类型	使您能够选择**更改为新的随机所有者 EPOCH** 或**手动用户定义的所有者 EPOCH。**每个 EPOCH 为 64 位。在生成新的 EPOCH 后，通过选择**更改为新的随机所有者 EPOCH**，选择将恢复回**手动用户定义的所有者 EPOCH。**
	Software Guard Extensions Epoch n：设置软件防护扩展 Epoch 值。
启用从操作系统/软件写入到 SGXLEPUBKEYHASH[3:0]	启用或禁用“启用从操作系统/软件写入到 SGXLEPUBKEYHASH [3:0]”。

表. 22: 系统安全详细信息 （续）

选项	说明
	SGX LE Public Key Hash0：为 SGX 启动 SGX Launch Enclave Public Key Hash 设置 0-7 的字节。
	SGX LE Public Key Hash1：为 SGX 启动 SGX Launch Enclave Public Key Hash 设置 8-15 的字节。
	SGX LE Public Key Hash2：为 SGX Launch Enclave Public Key Hash 设置 16-23 的字节。
	SGX LE Public Key Hash3：为 SGX Launch Enclave Public Key Hash 设置 24-31 的字节。
启用/禁用 SGX 自动 MP 注册代理	启用将禁用 SGX 自动 MP 注册。MP 注册代理负责注册平台。
SGX 出厂重置	允许您将 SGX 选项重置为出厂设置。该选项默认设置为**关**。
电源按钮	允许您启用或禁用系统前面的电源按钮。该选项默认设置为**已启用**。
交流电源恢复	设置系统恢复交流电源后系统如何反应。该选项默认设置为**持续**。 **注:** 主机系统将不会通电，直至 iDRAC 信任根 (RoT) 完成，主机开机将在应用交流电后的最短 90 秒内延迟。
交流电源恢复延迟	设置系统恢复交流电源后系统的开机延迟时间。该选项默认设置为**立即**。当此选项设置为**立即**时，将不会延迟开机。当此选项设置为**随机**时，系统会为开机创建随机延迟。当此选项设置为**用户定义**时，系统延迟时间为手动开机。
用户定义延迟（60 秒到 600 秒）	在为**交流电源恢复延迟**选择**用户定义**选项时，设置**用户定义延迟**选项。
UEFI 变量访问	提供保护 UEFI 变量的各种度。当设置为**标准**（默认值）时，可以按照 UEFI 规范在操作系统中访问 UEFI 变量。当设置为**受控**时，所选 UEFI 变量在环境中受保护，并且新的 UEFI 引导条目强制为当前引导顺序的末端。
带内可管理性界面	设置为**已禁用**时，此设置将对操作系统隐藏管理引擎 (ME)、HECI 设备和系统的 IPMI 设备。这会导致操作系统无法更改 ME 电源上限设置，并阻止访问所有带内管理工具。所有管理应通过带外进行管理。该选项默认设置为**已启用**。 **注:** BIOS 更新需要 HECI 设备正常运行，并且 DUP 更新需要 IPMI 界面正常工作。此设置需要设置为已启用，以避免更新错误。
SMM 安全迁移	启用或禁用 UEFI SMM 安全迁移保护。
安全引导	启用安全引导，BIOS 使用安全引导策略中的证书来验证每个预引导映像。安全引导在默认设置下已禁用。安全引导默认设置为**已禁用**。
安全引导策略	当安全引导策略设置为**标准**时，BIOS 将使用系统制造商密钥和证书来验证预引导映像。当安全引导策略设置为**自定义**时，BIOS 将使用用户定义的密钥和证书。安全引导策略默认设置为**标准**。
安全引导模式	配置 BIOS 如何使用安全引导策略对象（PK、KEK、db、dbx）。 如果当前模式设置为**部署模式**时，则可用的选项为**用户模式**和**部署模式**。如果当前模式设置为**用户模式**时，则可用的选项为**用户模式**、**审核模式**和**部署模式**。 **表. 23: 安全引导模式** 选项 / 说明： **用户模式** — 在**用户模式**下，PK 必须安装并且 BIOS 在编程尝试更新策略对象时执行签名验证。BIOS 允许不需要身份验证的编程模式之间转换。 **审核模式** — 在**审核模式**下，PK 不存在。BIOS 不验证对策略对象的编程更新和在模式之间转换。BIOS 在预引导映像上执行签名验证并在映像执行信息表中记录结果，但无论验证成功还是失败都会执行映像。**审核模式**用于所使用策略对象集的编程决策。

表. 22: 系统安全详细信息 （续）

选项	说明
	表. 23: 安全引导模式 （续） 选项：**部署模式** 说明：**部署模式**是最安全的模式。在**部署模式**中，PK 必须安装并且 BIOS 在编程尝试更新策略对象时执行签名验证。 **部署模式**限制编程模式转换。
安全引导策略摘要	显示安全引导用于验证映像的证书和哈希值列表。
安全引导自定义策略设置	配置安全引导自定义策略。要启用此选项，将安全引导策略设置为**自定义**选项。

创建系统密码和设置密码

前提条件

请确保 密码 跳线已启用。密码跳线用于启用或禁用系统密码和设置密码功能。有关更多信息，请参阅“系统板跳线设置”部分。

注: 如果密码跳线设置已禁用，将删除现有系统密码和设置密码，无需提供系统密码即可引导系统。

步

1. 要进入系统设置，请在开机或重新启动后立即按 F2。
2. 在**系统设置主菜单**屏幕中，单击**系统 BIOS** > **系统安全**。
3. 在**系统安全保护**屏幕中，验证**密码状态**是否设置为**已解锁**。
4. 在**系统密码**字段中，输入系统密码，然后按 Enter 或 Tab。
   采用以下原则设定系统密码：
   - 一个密码最多可包含 32 个字符。

   将显示一条消息，提示您重新输入系统密码。
5. 重新输入系统密码，然后单击**确定**。
6. 在**设置密码**字段中，输入系统密码，然后按 Enter 或 Tab。
   将显示一条消息，提示您重新输入设置密码。
7. 重新输入设置密码，然后单击**确定**。
8. 按 Esc 键返回系统 BIOS 屏幕。再按一次 Esc 键。
   将出现一条消息，提示您保存更改。
   注: 重新引导系统之后，密码保护才能生效。

使用您的系统密码保护您的系统

关于此任务

如果已设定设置密码，系统会将设置密码视为另一个系统密码。

步

1. 打开或重新引导系统。
2. 键入系统密码，然后按 Enter 键。

后续步骤

如果**“密码状态”**设置为**“已锁定”**，则必须在重新引导时根据提示键入系统密码并按 Enter 键。

注: 如果键入错误的系统密码，则系统会显示一条消息并提示您重新输入密码。您有三次机会键入正确的密码。第三次尝试失败后，系统将显示一条错误消息，表示系统已停止工作，必须关机。即使您关闭并重新启动系统，系统仍然会显示该错误信息，直到输入正确的密码。

删除或更改系统密码和设置密码

前提条件

注: 如果**密码状态**设置为**锁定**，则无法删除或更改现有系统密码或设置密码。

步

1. 要进入系统设置程序，请在开启或重新启动系统后立即按 F2 键。
2. 在**系统设置主菜单**屏幕中，单击**系统 BIOS** > **系统安全**。
3. 在**系统安全**屏幕中，确保**密码状态**设置为**已解锁**。
4. 在**系统密码**字段中，更改或删除现有系统密码，然后按 Enter 或 Tab 键。
5. 在**设置密码**字段中，更改或删除现有设置密码，然后按 Enter 或 Tab 键。
   如果更改系统密码和/或设置密码，将出现一则信息，提示您重新输入新密码。如果删除系统密码和/或设置密码，将出现一则信息，提示您确认删除操作。
6. 按 Esc 键返回**系统 BIOS** 屏幕。再按一次 Esc 键，将出现提示您保存更改的消息。
7. 选择**设置密码**，更改或删除现有设置密码并按 Enter 或 Tab 键。
   注: 如果更改系统密码或设置密码，将出现一则信息，提示您重新输入新密码。如果删除系统密码和/或设置密码，将出现一则信息，提示您确认删除操作。

在已启用设置密码的情况下进行操作

如果将**设置密码**设置为**已启用**，则必须输入正确的设置密码才能修改系统设置选项。

如果您尝试输入三次密码，但均不正确，系统会显示以下信息：

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must
power down.
```

即使您关闭并重新启动系统，系统仍然会显示该错误信息，直到键入正确的密码。支持以下选项：

- 如果未将**系统密码**设置为**已启用**，并且未通过**密码状态**选项加以锁定，则您可以设定系统密码。有关更多信息，请参阅系统的“安全设置屏幕”部分。
- 您不能禁用或更改现有的系统密码。

注: 您可以将密码状态选项与设置密码选项配合使用，以防止他人擅自更改系统密码。

冗余操作系统控制

要查看**冗余操作系统控制**屏幕，启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **冗余操作系统控制**。

表. 24: 冗余操作系统控制详细信息

选项	描述
冗余操作系统位置	可让您选择从以下设备的备份磁盘,请执行以下操作: • **无** • **IDSDM** • **SATA 端口（AHCI 模式中）** • **boss PCIe 卡(内部的 M .2 驱动器)** • **内置 USB** **注:** 不包含 RAID 配置和 NVMe 卡，因为 BIOS 中不具备区分这些配置中的各个驱动器的功能。 • **内部 SD 卡**

表. 24: 冗余操作系统控制详细信息 （续）

选项	描述
冗余操作系统状态	**注:** 如果**冗余操作系统位置**设置为**无**，此选项会被禁用。 如果设置为**可见**，则备份磁盘对引导列表和操作系统可见。如果设置为**隐藏**，则备份磁盘已禁用且对引导列表和操作系统不可见。此选项默认设置为**可见。** **注:** BIOS 将在硬件中禁用设备，因此它无法被操作系统访问。
冗余操作系统引导	**注:** 如果**冗余操作系统位置**设置为**无**，或者**冗余操作系统状态**设置为**隐藏**，此选项将被禁用。 如果**冗余操作系统位置**设置为**启用**，BIOS 将使用指定的位置引导设备。如果此选项设置为**已禁用**，BIOS 会保留当前引导列表设置。该选项默认设置为**已禁用。**

其他设置

技术规格**其他设置**屏幕，启动系统、按 F2，然后单击**系统设置主菜单** > **系统 BIOS** > **其他设置。**

表. 25: 其他设置详细信息

选项	说明
系统时间	允许您设置系统时间。
系统日期	允许您设置系统日期。
资产编号	指定资产编号，并且允许您出于安全保护和跟踪目的修改资产编号。
键盘 Numlock	允许您设置系统引导是否启用或禁用数码锁定。此选项默认设置为**开。** **注:** 此选项不适用于 84 键键盘。
发生错误时 F1/F2 提示	启用或禁用发生错误时提示按 F1/F2。该选项默认设置为**已启用。** F1/F2 提示还包括键盘错误。
加载旧版视频选项 ROM	启用或禁用加载传统视频 ROM 选项。该选项默认设置为**已禁用。**
Dell Wyse P25/P45 BIOS 访问	启用或禁用 Dell Wyse P25/P45 BIOS 的访问权限。该选项默认设置为**已启用。**
电源关闭后重启请求	启用或禁用电源关闭后重启请求。该选项默认设置为**无。**

iDRAC 设置公用程序

iDRAC 设置实用程序是使用 UEFI 设置和配置 iDRAC 参数的接口。可使用 iDRAC 设置实用程序启用或禁用各种 iDRAC 参数。

注: 访问 iDRAC 设置实用程序中的某些功能需要升级 iDRAC Enterprise 许可证。

有关使用 iDRAC 的更多信息，请参阅《*Dell Integrated Dell Remote Access Controller User's Guide*》，网址：https://www.dell.com/idracmanuals。

设备设置

设备设置允许您配置设备参数，例如存储控制器或网卡。

戴尔生命周期控制器

戴尔生命周期控制器 (LC) 可提供高级嵌入式系统管理功能，包括系统部署、配置、更新、维护和诊断。LC 是 iDRAC 带外解决方案和戴尔系统嵌入式统一可扩展固件接口 (UEFI) 应用程序的一部分。

嵌入式系统管理

戴尔生命周期控制器在系统的整个生命周期提供高级嵌入式系统管理。戴尔生命周期控制器可在引导顺序期间启动，并可独立于操作系统工作。

注: 某些平台配置可能不支持戴尔生命周期控制器提供的整套功能。

有关设置戴尔生命周期控制器、配置硬件和固件以及部署操作系统的更多信息，请参阅《戴尔生命周期控制器说明文件》，网址：https://www.dell.com/idracmanuals。

引导管理器

引导管理器选项允许您选择引导选项和诊断实用程序。

要进入**引导管理器**，请启动系统并按 F11。

表. 26: 引导管理器详细信息

选项	说明
持续正常引导	系统尝试从引导顺序中的第一项开始引导至设备。如果引导尝试失败，系统将继续从引导顺序中的下一项进行引导，直到引导成功或者找不到引导选项为止。
一次性引导菜单	通过该菜单项可访问引导菜单，然后可以选择要从中引导的一次性引导设备。
启动系统设置	允许您访问系统设置程序。
启动生命周期控制器	退出引导管理器，并启动戴尔生命周期控制器程序。
系统公用程序	使您能够启动系统实用程序菜单，例如启动诊断程序、BIOS 更新文件资源管理器、重新引导系统。

PXE 引导

您可使用预引导执行环境 (PXE) 选项来远程引导和配置联网的系统。

要访问 **PXE 引导**选项，请引导系统并在 POST 期间按 F12，而不是从 BIOS 设置程序使用标准引导顺序。它不拉动任何菜单或允许管理网络设备。