Dell EMC

BIOS 和 UEFI 参考指南

DELL EMC

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。**

目录

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
- 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

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**，然后单击 **BIOS 设置**。
- 文本浏览器 — 这种浏览器通过控制台重定向启用。

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。

系统设置主菜单屏幕详细信息如下所示：

表. 1: 系统设置主菜单

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*》，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。如果系统中包含的 NVMe 驱动器您想要配置在 RAID 阵列中,您必须在此字段和**嵌入式 SATA** 字段中设置 **SATA 设置** 菜单上为 **RAID 模式**。您可能还需要将**引导模式**设置更改为 **UEFI**。如果不是,则应将此字段设置为 **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**菜单将受管。 **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。
AGESA 版本	指定 AGESA 参考代码版本。
SMU 版本	指定 SMU 固件版本。
DXIO 版本	指定 DXIO 固件版本。

内存设置

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

表. 4: 内存设置详细信息

选项	说明
系统内存大小	指定系统的内存大小。
系统内存类型	指定系统中安装的内存类型。
系统内存速度	指定系统内存速度。
系统内存电压	指定系统内存电压。
视频内存	指定视频内存容量。
系统内存测试是	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**已启用**和**已禁用**。此选项默认设置为**已禁用。**
DRAM 刷新延迟	通过启用 **CPU 内存控制器**来推迟运行**刷新**命令，您可以提高一些工作负载的性能。通过最小化延迟时间，可确保内存控制器定期运行**刷新**命令。对于基于英特尔的服务器，此设置仅影响配置 DIMM（使用 8 Gb 密度 DRAM）的系统。该选项默认设置为**最小值。**
内存运行模式	指定内存运行模式。该选项可用，并且默认设置为**优化器模式。**
内存运行模式的当前状态	指定在内存运行模式下选择的模式。
内存交叉存取	启用或禁用内存交叉存取选项。可用的两个选项为**自动**和**已禁用**。此选项默认设置为**自动。**
伺机自刷新	启用或禁用伺机自刷新功能。此选项默认设置为**已禁用。**
可纠正的错误日志记录	启用或禁用可纠正的错误日志记录。此选项默认设置为**已启用。**

处理器设置

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

表. 5: 处理器设置详细信息

选项	说明
逻辑处理器	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**已启用**，BIOS 会显示所有逻辑处理器。如果此选项设置为**已禁用**，BIOS 只会显示每个内核的一个逻辑处理器。此选项默认设置为**已启用。**
虚拟化技术	启用或禁用的处理器虚拟化技术。此选项默认设置为**已启用。**
IOMMU 支持	启用或禁用 IOMMU 支持。需要创建 IVRS ACPI 表。此选项默认设置为**已启用。**
L1 流硬件预取器	启用或禁用 L1 流硬件预取器。此选项默认设置为**已启用。**
L2 流硬件预取器	启用或禁用 L2 流硬件预取器。此选项默认设置为**已启用。**
MADT Core 枚举	指定 MADT Core 枚举。此选项默认设置为**线性。**
每插槽 NUMA 节点数	指定每个插槽的 NUMA 节点数。此选项默认设置为 **1。**
L3 高速缓存作为 NUMA 域	启用或禁用“L3 高速缓存作为 NUMA 域”。此选项默认设置为**已禁用。**
最小 SEV 非 ES ASID	确定安全加密的虚拟化 ES 和非 ES 可用地址空间 ID 的数量。此选项默认设置为 **1。**
x2APIC 模式	启用或禁用 x2APIC 模式。此选项默认设置为**已启用。** **注:** 对于两个 CPU 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。
每处理器 CCD 数	控制每个处理器中的已启用 CCD 数。此选项默认设置为**全部。**

表. 5: 处理器设置详细信息（续）

选项	说明
每 CCD 核心数	指定每个 CCD 的核心数。此选项默认设置为**全部**。
处理器内核速度	显示处理器的最大内核频率。
处理器总线速度	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。
处理器 n	**注:** 根据 CPU 数量，最多可能会列出 n 个处理器。 以下设置仅对系统中安装的每个处理器显示：

表. 6: 处理器 n 详细信息

选项	说明
系列、型号和步进	指定 AMD 定义的处理器系列、型号和步进。
品牌	显示品牌名称。
2 级高速缓存	显示 L2 高速缓存总和。
3 级高速缓存	显示 L3 高速缓存总和。
核心数量	显示每个处理器的内核数。
微码	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**。此选项默认设置为 **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。此选项默认设置为**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。此选项默认设置为**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。该选项默认设置为**非 RAID** 模式。

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。以下参数仅在**系统配置文件**设置为**自定义**时才可用。
  - 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. 9: 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。如果启用此字段后系统引导失败，系统将在 30 秒后重新尝试引导顺序。此选项默认设置为**已启用**。
硬盘故障切换	启用或禁用硬盘故障切换。此选项默认设置为**已禁用**。
通用 USB 引导	启用或禁用通用 USB 引导占位符。此选项默认设置为**已禁用**。
硬盘占位符	启用或禁用硬盘占位符。此选项默认设置为**已禁用**。
清理所有 Sysprep 顺序和变量	当设置为**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。此选项默认设置为**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. 10: 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）是增强版 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。

步骤

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: 有关 Linux 网络性能设置的信息，请参阅 *Linux Network Tuning Guide for AMD EPYC Processor Based Servers*，网址：AMD.com。

注: BIOS 引导模式下不支持“网络设置”。

表. 11: 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 to 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 to 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 to 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 to 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. 12: 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**。此选项默认设置为**禁用**。
Vlan ID	显示 PXE 设备的 Vlan ID

表. 12: PXE 设备 n 设置详细信息（续）

选项	说明
Vlan 优先级	显示 PXE 设备的 Vlan 优先级。

表. 13: HTTP 设备 n 设置详细信息

选项	说明
界面	指定用于 HTTP 设备的 NIC 接口。
协议	指定用于 HTTP 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 HTTP 设备启用 Vlan。此选项设置为**启用**或**禁用**。此选项默认设置为**禁用**。
Vlan ID	显示 HTTP 设备的 Vlan ID
Vlan 优先级	显示 HTTP 设备的 Vlan 优先级。
DHCP	为此 HTTP 设备启用或禁用 DHCP。此选项默认设置为**启用**。
IP 地址	指定 HTTP 设备的 IP 地址。
子网掩码	指定 HTTP 设备的子网掩码。
网关	指定 HTTP 设备的网关。
通过 DHCP 启用或禁用 DNS 信息	从 DHCP 启用或禁用 DNS 信息。此选项默认设置为**启用**。
主要 DNS	指定 HTTP 设备的主 DNS 服务器 IP 地址。
次要 DNS	指定 HTTP 设备的辅助 DNS 服务器 IP 地址。
URI	如果未指定，则从 DHCP 服务器获取 URI。
TLS 身份验证配置	指定 TLS 身份验证配置的选项。

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。此选项默认设置为**已禁用**。
iSCSI 设备 1 设置	允许您控制 iSCSI 设备的配置。

表. 15: ISCSI 设备设置屏幕详细信息

选项	说明
连接 1	启用或禁用 iSCSI 连接。此选项默认设置为**禁用**。
连接 2	启用或禁用 iSCSI 连接。此选项默认设置为**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: Integrated Devices 详细信息

选项	说明
User Accessible USB Ports	禁用前端用户可访问 USB 端口。选择**关闭所有端口**会禁用所有正面和背面 USB 端口。此选项默认设置为**打开所有端口**。 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。
内部 SD 卡 端口	启用或禁用**内部 SD 卡 端口**。此选项设置为**开**或**关**。此选项默认设置为**开**。
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 **Off（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**。
Embedded NIC1	启用或禁用 **Embedded NIC1** 选项。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 **Embedded NIC1** 选项。
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，即使已安装附加式图形卡。当设置为**已禁用**时，附加式图形卡将用作主显示器。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。此选项默认设置为**已启用**。 **注:** 当系统中已安装附加式图形卡时，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。
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（即没有安装附加图形卡），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。
PCIe 首选 IO 总线	当设置为**已启用**时，您可以提供总线地址（十进制），以选择适用于首选 IO 总线的终端设备。此选项默认设置为**已禁用**。
增强的首选 IO	当设置为**已启用**时，已启用首选 IO 的根联合体的 LCLK 速度将自动设置为 600 MHz（有效值为 593 MHz）。
SR-IOV Global Enable	启用或禁用单根 I/O 虚拟化 (SR-IOV) 设备的 BIOS 配置。此选项默认设置为**已禁用**。
OS Watchdog Timer	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。
内存映射 I/O 限制	控制 MMIO 映射到的位置。**1 TB** 选项适合不支持超过 1 TB MMIO 的特定操作系统。此选项默认设置为 **8 TB**。默认选项是系统支持的最大地址，并且大多数情况下推荐此选项。
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。只有当安装的外围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，Option ROM（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。 **Slot n**：启用或禁用或仅针对 PCIe 插槽 n 禁用引导驱动程序。此选项默认设置为**已启用**。
插槽分支	**插槽发现分支设置**允许设置为**平台默认分支**和**手动分支控制**。 默认设置为**平台默认分支**。当设置为**手动分支控制**时，插槽分支字段可访问，当设置为**平台默认分支**时，插槽分支字段呈灰显。

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**。

表. 17: 串行通信详细信息

选项	说明
串行端口地址	允许您设置串行设备的端口地址。。此字段可将串行端口地址设置为 COM1 或 COM2（COM1=0x3F8、COM2=0x2F8）。 **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。此选项默认设置为**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**每瓦特性能 (OS)**。其他选项包括**性能**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 **OS DBPM**。其他选项包括**最大性能**。
内存频率	设置系统内存的速度。您可以选择**最大性能**或特定速度。此选项默认设置为**最大性能**。
Turbo Boost	允许您启用或禁用处理器在 turbo boost 模式下运行。此选项默认设置为**已启用**。
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。此选项默认设置为**已启用**。
写入数据 CRC	当设置为**已启用**时，在“写入”操作过程中将检测并纠正 DDR4 数据总线问题。影响性能的 CRC 位代需要两个额外的周期。除非将“系统配置文件”设置为**自定义**，否则为只读。此选项默认设置为**已禁用**。
内存轮巡	设置内存轮巡模式。此选项默认设置为**关**。
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**。
PCI ASPM L1 链接电源管理	启用或禁用 PCI Slot ASPM L 1 链接电源管理。此选项默认设置为**已启用**。
确定性滑块	通过**供电决策**或**性能决策**设置系统决策。此选项默认设置为**性能决策**。
效率优化模式	效率优化模式可通过适时降低频率/功率来更大限度地提高性能功耗比。启用或禁用效率优化模式。
算法性能提升禁用 (ApbDis)	启用或禁用“算法性能提升禁用 (ApbDis)”。此选项默认设置为**已禁用**。
动态链路宽度管理 (DLWM)	当链路上未检测到流量时，将插槽间的 xGMI 链路宽度从 x16 降至 x8（默认值）。该选项默认设置为**非强制**。

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。此选项默认设置为**已启用**。
系统密码	允许您设置系统密码。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。
设置系统密码	允许您设置系统密码。如果系统上未安装密码跳线，此选项为只读。
密码状态	允许您设置系统密码。此选项默认设置为**所有**。

表. 20: TPM 1.2 安全信息

选项	说明
TPM Security	**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，进行预引导测量**，则仅可修改 TPM 状态和 TPM 激活。 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，不进行预引导测量**。 安装了 TPM 2.0 时, **TPM 安全**选项设置为**开**或**关**。此选项默认设置为**关**。
TPM 信息	允许您更改 TPM 的操作状态。此选项默认设置为**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，命令将不会发送到 TPM。当设置为**激活**时，将启用并激活 TPM。当设置为**停用**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。此选项默认设置为**无**。

表. 21: TPM 2.0 安全信息

选项	说明
TPM 信息	允许您更改 TPM 的操作状态。此选项默认设置为**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
电源按钮	允许您启用或禁用系统前面的电源按钮。此选项默认设置为**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**。
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，根据 UEFI 规范可在操作系统中访问 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。
安全引导	启用安全引导，以便 BIOS 使用安全引导策略中的证书来验证每个预引导映像。安全引导默认设置为**已禁用**。

表. 22: 系统安全详细信息（续）

<table>
<tr><th>选项</th><th>说明</th></tr>
<tr><td>安全引导策略</td><td>当安全引导策略设置为标准时，BIOS 将使用系统制造商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。</td></tr>
<tr><td>安全引导模式</td><td>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,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，则可用的选项为用户模式、审计模式、和部署模式。
表. 23: 安全引导模式<table><tr><th>选项</th><th>说明</th></tr><tr><td>用户模式</td><td>在用户模式下，PK 必须已安装并且 BIOS 在编程尝试时执行签名验证以更新策略对象。
BIOS 允许不需要身份验证的编程模式之间转换。</td></tr><tr><td>部署模式</td><td>部署模式是最安全的模式。在部署模式下，PK 必须安装并且 BIOS 在编程尝试时执行签名验证以更新策略对象。
部署模式将限制编程模式转换。</td></tr><tr><td>审计模式</td><td>在审计模式下，PK 不存在。BIOS 不验证策略对象的编程更新,并模式之间转换。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。
审计模式用于所使用策略对象集的编程决策。</td></tr></table></td></tr>
<tr><td>授权设备固件</td><td>指定设备固件的状态。</td></tr>
<tr><td>安全引导策略摘要</td><td>显示安全引导用于验证映像的证书和哈希值列表。
表. 24: 安全引导自定义策略设置屏幕<table><tr><th>选项</th><th>说明</th></tr><tr><td>平台密钥</td><td>导入、导出、删除或恢复平台密钥 (PK)。</td></tr><tr><td>密钥交换密钥数据库</td><td>允许导入、导出、删除或恢复密钥交换密钥 (KEK) 数据库中的条目。</td></tr><tr><td>授权签名数据库</td><td>导入、导出、删除或恢复授权签名数据库 (db) 中的条目。</td></tr><tr><td>禁用的签名数据库</td><td>导入、导出、删除或恢复禁用的签名数据库 (dbx) 中的条目。</td></tr></table></td></tr>
</table>

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。

步骤

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。

步骤

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。

步骤

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.
```

```
Password Invalid. Number of unsuccessful password attempts: <x> Maximum number of password
attempts exceeded.System halted.
```

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. 25: 冗余操作系统控制详细信息

选项	说明
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** • **AHCI Mode (AHCI 模式中的 SATA 端口** • **boss PCIe 卡(内部的 M .2 驱动器)** • 内部 SD 卡
冗余操作系统状态	**注:** 如果 **NIC 选择**设置为**专用**，则此选项被禁用。 时设置为**可见**,备份磁盘到引导列表中可见和操作系统。当设置为**隐藏**、备份磁盘已禁用且到的引导列表和操作系统中不可见。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**冗余操作系统的位置**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**冗余操作系统的位置**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**禁用**，BIOS 会保留当前引导列表设置。此选项默认设置为**已启用。**

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. 26: 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。
键盘数码锁定	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。此选项默认设置为**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。此选项默认设置为**已禁用。**

表. 26: 其他设置详细信息（续）

选项	说明
Dell Wyse P25/P45 BIOS 访问	启用或禁用 Dell Wyse P25/P45 BIOS 的访问权限。此选项默认设置为**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。此选项默认设置为**无。**

iDRAC 设置实用程序

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. 27: 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。
系统实用程序	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。