Dell EMC PowerEdge R240

BIOS 和 UEFI 参考指南

部件号: E57S Series
管制类型： E57S001
Dec 2020
Rev. A00

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

章 1: 预装操作系统管理应用程序.....4
用于管理预操作系统应用程序的选项.....4
系统设置.....4
查看系统设置程序.....4
系统设置程序详细信息.....4
System BIOS（系统 BIOS）.....5
iDRAC 设置公用程序.....20
设备设置.....20
戴尔生命周期控制器.....20
嵌入式系统管理.....20
引导管理器.....21
查看引导管理器.....21
引导管理器主菜单.....21
一次性 UEFI 引导菜单.....21
系统公用程序.....21
PXE 引导.....21

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。

主题：

- 用于管理预操作系统应用程序的选项
- 系统设置
- 戴尔生命周期控制器
- 引导管理器
- PXE 引导

用于管理预操作系统应用程序的选项

系统提供了以下用于管理预操作系统应用程序的选项：

- 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)

系统设置

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

注: 默认情况下，所选字段的帮助文本显示在图形浏览器中。要在文本浏览器中查看帮助文本，请按 F1。

您可以通过以下方法之一访问系统设置程序：

- 标准图形浏览器 — 默认设置下启用的浏览器。
- 文本浏览器 — 这种浏览器通过控制台重定向启用。

查看系统设置程序

要查看**系统设置程序**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

系统设置程序详细信息

系统设置主菜单屏幕详细信息如下：

选项	说明
System BIOS（系统 BIOS）	允许您配置 BIOS 设置。
iDRAC Settings	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 设置公用程序启用或禁用各种 iDRAC 参数。有关此实用程序的更多信息，请参阅 *Integrated Dell Remote Access Controller User's Guide（集成戴尔远程访问控制器用户指南）*，网址：。
Device Settings（设备设置）	允许您配置设备设置。

System BIOS（系统 BIOS）

您可以使用 **System BIOS** 屏幕编辑特定功能，如引导顺序、系统密码、设置密码、设置 SATA 模式，以及启用或禁用 USB 端口。

查看系统 BIOS

要查看**系统 BIOS**，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。

系统 BIOS 设置详细信息

关于此任务

System Profile Settings（系统配置文件设置）屏幕详细信息说明如下：

选项	说明
System Information（系统信息）	显示有关系统的信息，如系统型号名称、BIOS 版本、服务标签等。
Memory Settings	显示与所安装内存有关的信息和选项。
Processor Settings（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 Settings（SATA 设置）	显示用于启用或禁用集成 SATA 控制器和端口的选项。
Boot Settings（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 **Device Settings（设备设置）**菜单将受管。
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。

选项	说明
Serial Communication	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。
System Profile Settings（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。
System Security	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。
Miscellaneous Settings	指定更改系统日期和时间的选项。

系统信息

您可以使用**系统信息**屏幕来查看系统属性，如服务标签、系统型号名称和 BIOS 版本。

查看系统信息

要查看 **System Information**（系统信息），请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**系统信息**。

System Information（系统信息）的详细信息

关于此任务

System Information（系统信息）屏幕详细信息如下：

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。
系统服务标签	指定系统服务标签。
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

您可以使用**内存设置**屏幕来查看所有内存设置以及启用或禁用特定内存功能，如系统内存测试和节点交叉。

查看内存设置

要查看**内存设置**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**内存设置**。

内存设置详细信息

关于此任务

内存设置屏幕详细信息如下：

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	指定系统内存测试是否在系统引导期间运行。选项包括**已启用**和**已禁用**。该选项默认设置为**已禁用**。
内存运行模式	指定内存运行模式。该选项默认设置为**优化器模式**。 **注:** 根据系统内存配置，**内存运行模式**可能有不同的默认设置和可用选项。
内存运行模式的当前状态	指定内存运行模式的当前状态。

Processor Settings（处理器设置）

您可以使用 **Processor Settings（处理器设置）**屏幕查看处理器设置和执行特定功能，如启用虚拟化技术、硬件预取器和逻辑处理器空闲。

查看处理器设置

要查看**处理器设置**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。

2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**处理器设置**。

处理器设置详细信息

关于此任务

处理器设置屏幕详细信息如下：

选项	说明
逻辑处理器	启用或禁用逻辑处理器并显示逻辑处理器的数量。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 只会显示每个核心的一个逻辑处理器。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**。
相邻缓存行预取	针对需要大量使用顺序内存访问的应用程序优化系统。此选项默认设置为**已启用**。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。
硬件预取器	启用或禁用硬件预取器。此选项默认设置为**已启用**。
逻辑处理器空闲	可让您以提高系统。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**已禁用**。
x2APIC 模式	启用或禁用 x2APIC 模式。该选项默认设置为**已禁用**。
每个处理器的核心数	控制每个处理器中的已启用核心数。该选项默认设置为**所有**。
处理器核心速率	显示处理器的最大核心频率。
处理器 1	以下设置仅对系统中安装的每个处理器显示：

选项	说明
系列-型号-步进	显示英特尔定义的处理器系列、型号和步进。
品牌	显示品牌名称。
二级高速缓存	显示 L2 高速缓存总和。
三级高速缓存	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	指定微码。

SATA 设置

您可以使用 **SATA 设置**屏幕来查看 SATA 设备的 SATA 设置并在系统上启用 SATA。

查看 SATA 设置

要查看 **SATA Settings**（SATA 设置）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。

2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击 **SATA 设置**。

SATA Settings（SATA 设置）详细信息

关于此任务

SATA 设置屏幕详细信息如下所述：

选项	说明
Embedded SATA	支持将嵌入式 SATA 选项设置为 **Off**、**AHCI** 或 **RAID** 模式。该选项默认设置为 **AHCI 模式**。
Security Freeze Lock	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 Mode（AHCI 模式）。此选项的默认设置为**启用**。
Write Cache	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**。
Port n	设置所选设备的驱动器类型。 对于 **AHCI 模式**或 **RAID 模式**，BIOS 支持始终启用。

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，如光盘驱动器，此字段未定义。

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。
- **BIOS**: **BIOS 引导模式** 是 传统 引导模式。此位置支持向后兼容性。

查看引导设置

要查看**引导设置**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。

4. 在**系统 BIOS** 屏幕中，单击**引导设置**。

引导设置详细信息

关于此任务

Boot Settings（引导设置）屏幕详细信息如下所述：

选项	说明
Boot Mode	允许您设置系统的引导模式。 **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。** 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**。 **注:** 将此字段设置为 UEFI 将禁用 BIOS Boot Settings（UEFI 引导设置）菜单。
Boot Sequence Retry	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 **Enabled（已启用）**。
Hard-Disk Failover	指定在驱动器发生故障的情况下进行引导的驱动器。所选中的设备 **引导选项设置上 Hard - Disk Drive Sequence (硬盘驱动器顺序**)菜单。此选项设置为 **Disabled（已禁用）**时，将仅尝试引导列表中的第一个驱动器。此选项设置为 **Enabled（已启用）**时，将尝试按顺序引导 **Hard-Disk Drive Sequence（硬盘驱动器顺序）**中已选的所有驱动器。未为 **UEFI 引导模式已启用此选项**。该选项默认设置为 **Disabled（已禁用）**。
Generic USB boot	启用或禁用通用 USB 引导。该选项默认设置为 **Disabled（已禁用）**。
Hard-disk Drive Placeholder	启用或禁用硬盘占位符。
UEFI 引导设置	启用或禁用 UEFI 引导选项。 引导选项包括 **IPv 4 PXE** 和 **Ipv 6 PXE**。该选项默认设置为 **Off**（关）。 **注:** 此选项仅在引导模式为 UEFI 时启用。
UEFI Boot Sequence	允许您更改引导设备的顺序。
Boot Options Enable/Disable	允许您选择已启用或已禁用的引导设备。

网络设置

您可以使用**网络设置**屏幕修改 UEFI PXE、iSCSI 和 HTTP 引导设置。 “网络设置”选项仅在 UEFI 模式下可用。

注: BIOS 不会在 BIOS 引导模式下控制网络设置。对于 BIOS 引导模式，网络控制器的可选的引导 ROM 可以处理网络设置。

查看网络设置

要查看**网络设置**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。

4. 在**系统 BIOS** 屏幕中，单击**网络设置**。

网络设置屏幕详细信息

网络设置屏幕详细信息如下所述：

关于此任务

选项	说明
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 = 1-4)	允许您控制 PXE 设备的配置。
HTTP 设备 n (n = 1-4)	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. 1: 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。启用时，则为 iSCSI 设备自动创建 UEFI 引导选项。默认设置为**已启用**。
iSCSI 设备 1 设置	允许您控制 iSCSI 设备的配置。

集成设备

您可以使用 **Integrated Devices（集成设备）**屏幕来查看和配置所有集成设备的设置，包括视频控制器、集成 RAID 控制器和 USB 端口。

查看集成设备

要查看 **Integrated Devices**（集成设备）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**集成设备**。

集成设备详细信息

关于此任务

集成设备屏幕详细信息如下所述：

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**仅打开背面端口**会禁用正面 USB 端口，选择**关闭所有端口**会禁用所有正面和背面 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。 **注:** 选择**仅打开背面端口**和**关闭所有端口**将禁用 USB 管理端口并限制对 iDRAC 功能的访问。
内部 USB 端口	启用或禁用内部 USB 端口。此选项设置为**打开**或**关闭**。该选项默认设置为**打开**。
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**打开**或**关闭**。当设置为**关闭**时，iDRAC 无法检测到此管理端口中安装的任何 USB 设备。该选项默认设置为**打开**。
嵌入式 NIC1 和 NIC2	**注:** 嵌入式 NIC1 和 NIC2 选项仅在未安装**集成网卡 1** 的系统上可用。 启用或禁用嵌入式 NIC1 和 NIC2 选项。当设置为**已禁用**时，NIC 仍可用于嵌入式管理控制器的共享网络访问。嵌入式 NIC1 和 NIC2 选项仅可用于没有网络子卡 (NDC) 的系统。嵌入式 NIC1 和 NIC2 选项与集成网卡 1 选项互相排斥。通过使用设备的 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。
嵌入式视频控制器	启用或禁用将嵌入式视频控制器作为主要显示屏使用。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。此选项默认设置为**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。
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），那么即使设置为**已禁用**，嵌入式视频控制器也会自动用作主显示屏。
OS 监护程序计时器	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。此选项时设置为**已禁用**（默认值），计时器不会对系统造成任何影响。
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。此选项默认设置为**已启用**。
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，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。

表. 2: 插槽禁用

选项	说明
插槽 1	启用或禁用或仅引导驱动程序已针对 PCIe 插槽 1 禁用。此选项默认设置为**已启用**。
插槽 2	启用或禁用或仅引导驱动程序已针对 PCIe 插槽 2 禁用。此选项默认设置为**已启用**。

串行通信

您可以使用**串行通信**屏幕来查看串行通信端口的属性。

查看串行通信

要查看 **Serial Communication**（串行通信）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**串行通信**。

Serial Communication（串行通信）详细信息

关于此任务

串行通信屏幕详细信息如下所述：

选项	说明
Serial Communication	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。该选项默认设置为 **关**。
串行端口地址	允许您设置串行设备的端口地址。此字段可将端口地址设置为 COM1 或 COM2（COM1=0x3F8、COM2=0x2F8）。此选项默认设置为 **串行设备 1 = COM2 或串行设备 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设置转换为设置为 串行设备 1 的默认设置。
External Serial Connector（外部串行连接器）	您可以使用此选项将外部串行连接器与**串行设备 1**、**串行设备 2** 或**远程访问设备**关联起来。该选项的默认设置为 **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。该选项默认设置为 **115200**。
远程终端类型	允许您设置远程控制台终端类型。该选项默认设置为 **ANSIVT100/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 **Enabled（已启用）**。

系统配置文件设置

您可以使用**系统配置文件设置**屏幕启用特定系统的性能设置，如电源管理。

查看系统配置文件设置

要查看**系统配置文件设置**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**系统配置文件设置**。

System Profile Settings（系统配置文件设置）详细信息

关于此任务

System Profile Settings（系统配置文件设置）屏幕详细信息如下所述：

选项	说明
System Profile	允许您设置系统密码。如果将 **System Profile**（系统配置文件）选项设置为除 Custom（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 **Custom**（自定义）时，才可更改其余选项。此选项默认设置为 **Performance Per Watt (OS)（性能功耗比 [OS]）**。 **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 Power Management	设置的 CPU Power Management（CPU 电源管理）。该选项默认设置为 **OS DBPM**。
Memory Frequency	设置系统内存的速度。您可以选择 **最佳性能**、**最大可靠性**，或特定速度。该选项默认设置为 **All**（所有）。
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 **Enabled（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。此选项默认设置为 **Enabled（已启用）**。
C States	允许您启用或禁用处理器在所有可用电源状态下运行。此选项默认设置为 **Enabled（已启用）**。
Memory Refresh Rate	将“内存刷新率”设置为 1x 或 2x。该选项默认设置为 **Immediate**（立即）。
Uncore Frequency	可用于选择 **Processor Uncore Frequency**（处理器非内核频率）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。优化非 核心 频率以节省电源或 Optimize performance (优化性能)受 Energy Efficiency Policy **(能效策略)设置的** 选项。
Number of Turbo Boot Enabled Cores for Processor 1（处理器 1 的 Turbo 引导已启用核心的数量）	**注:** 如果系统中安装了两个处理器，将显示 **Number of Turbo Boost Enabled Cores for Processor 2**（处理器 2 的 Turbo 引导已启用核心的数量）。 配置处理器启用了睿频加速技术的核心数的最大内 核 数是已启用)(默认为 Enabled [已启用])。
Monitor/Mwait	启用处理器中的 Monitor / Mwait 指令。此选项设置为 Enabled **(已启用)** ,将所有 系统 配置文件(除外 **)自定义(** 已禁用)(默认设置)。

选项	说明
	注: 仅当 **C States**（C 状态）选项在 **Custom**（自定义）模式下设置为 **disabled**（已禁用）时，才能禁用此选项。 **注:** 当 **C States** 在（C 状态） **Custom**（自定义）模式下设置为 **Enabled**（已启用）时，更改 Monitor/Mwait 设置不会影响系统电源或性能。
PCI ASPM L1 Link Power Management	启用或禁用 PCI Slot ASPM L 1 链接" Power Management "(电源管理)。此选项默认设置为 **Enabled（已启用）**。

系统安全

您可以使用**系统安全**屏幕来执行特定的功能，如设置系统密码、设置密码和禁用电源按钮。

查看系统安全

要查看 **System Security**（系统安全）屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**系统安全**。

系统安全设置详细信息

关于此任务

系统安全设置屏幕详细信息如下所述：

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	锁定系统密码。该选项默认设置为**所有**。
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**关闭**。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。
TPM 信息	允许您更改 TPM 的操作状态。该选项默认设置为**无更改**。
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**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。该选项默认设置为**无**。

选项	说明
	小心：清除 TPM 会导致 TPM 中的所有密钥丢失。丢失 TPM 密钥可能对引导至操作系统产生影响。 当 **TPM 安全保护**设置为**关闭**时，此字段为只读。该操作需要额外重新引导才能生效。
英特尔® TXT	启用或禁用英特尔可信执行技术 (TXT)。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**关闭**。 安装了 TPM 2.0 时，**TPM 2 算法**选项可用。它可让您选择 TPM 支持的哈希算法（SHA1、SHA256）。**TPM 2 算法**选项必须设置为 **SHA 256**，以启用 TXT。
英特尔® TXT	启用或禁用英特尔软件保护扩展 (SGX) 选项。此选项默认设置为**软件**。 **注：** SGX 菜单仅在已安装 SGX 支持的处理器时可用。
SGX 启动控制策略	允许控制软件保护扩展 (SGX) 技术的启动控制策略 (LCP)。该选项默认设置为**所有**。
电源按钮	允许您启用或禁用系统正面的电源按钮。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**。
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**。
用户定义的延迟（60 秒到 240 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，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。
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。此选项默认设置为**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。
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**。
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**。

选项	说明
用户模式	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。
审核模式	在**审核模式**下，PK 不存在。BIOS 不会对策略对象的编程更新进行身份验证，也不会在模式之间转换。 **审核模式**对于通过编程方法决定策略对象的工作集非常有用。 BIOS 在预引导映像上执行签名验证并在映像执行信息表上记录结果，但无论它们通过还是验证失败都会执行映像。
部署模式	**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。

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 **System Setup Main Menu**（系统设置主菜单）屏幕中,单击 **System BIOS**（**系统 BIOS**） > **System Security**（系统安全）。
3. 在 **System Security**（系统安全保护）屏幕中，验证 **Password Status**（密码状态）是否设置为 **Unlocked**（已解锁）。
4. 在 **System Password**（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。
   - 密码可包含数字 0 至 9。
   - 只允许使用以下特殊字符：空格、(")、(+)、(,)、(-)、(.)、(/)、(;)、([)、(\)、(])、(`)。

   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 **OK**（确定）。
6. 在 **Setup Password**（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 **OK**（确定）。
8. 按 Esc 键返回 System BIOS（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。

使用系统密码保护系统

关于此任务

如果已分配设置密码，系统会将设置密码视为备选系统密码。

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 **P 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**系统设置程序主菜单**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。

   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。如果删除系统密码或设置密码，将出现一则消息，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 **Setup Password（设置密码）**设置为 **Enabled（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 **System Password（系统密码）**设置为 **Enabled（已启用）**，并且未通过 **Password Status（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 Password Status（密码状态）选项与 Setup Password（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

在**冗余操作系统控制**屏幕上，您可以设置冗余操作系统信息。它允许您在系统上设置物理恢复磁盘。

查看冗余操作系统控制

要查看 **Redundant OS Control** 屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

   ```
   F2 = System Setup
   ```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS**。
4. 在**系统 BIOS** 屏幕中，单击**冗余操作系统控制**。

冗余操作系统控制屏幕详细信息

冗余操作系统控制屏幕详尽的解释如下：

关于此任务

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** • **IDSDM** • **AHCI 模式中的 SATA 端口** • **BOSS PCIe 卡（内部 M.2 驱动器）** • **内置 USB** **注:** 不包括 RAID 配置和 NVMe 卡，因为 BIOS 不能区分将这些配置中的各个驱动器。
冗余操作系统状态	**注:** 如果**冗余操作系统位置**设置为**无**，此选项将禁用。 当设置为**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。该选项默认设置为 **可见。** **注:** BIOS 将在硬件中禁用设备，因此操作系统无法访问。
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。该选项默认设置为**已禁用。**

其他设置

您可以使用**其他设置**屏幕来执行特定功能，如更新资产标签以及更改系统日期和时间。

查看其他设置

要查看**其他设置**屏幕，请执行以下步骤：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时立即按 F2：

```
F2 = System Setup
```

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

3. 在**系统设置程序主菜单**屏幕中，单击**系统 BIOS。**
4. 在**系统 BIOS** 屏幕中，单击**其他设置。**

Miscellaneous Settings（其他设置）的详细信息

关于此任务

Miscellaneous Settings（其他设置）屏幕详细信息如下所述：

选项	说明
System Time	允许您设置系统时间。

选项	说明
System Date	允许您设置系统日期。
Asset Tag	指定资产标签，并且允许您出于安全保护和跟踪目的修改资产标签。
Keyboard NumLock	允许您设置系统引导是否启用或禁用 NumLock（数码锁定）。该选项默认设置为 **Immediate（立即）**。 **注:** 此选项不适用于 84 键键盘。
F1/F2 Prompt on Error	启用或禁用 F1/F2 Prompt on Error（发生错误时 F1/F2 提示）。此选项默认设置为 **Enabled（已启用）**。F1/F2 提示还包括键盘错误。
Load Legacy Video Option ROM	使您能够确定系统 BIOS 是否从视频控制器加载旧式视频 (INT 10H) 选项 ROM。在操作系统中选择 **Enabled**（已启用）不支持 UEFI 视频输出标准。此字段仅适用于 UEFI 引导模式。如果已启用 **UEFI Secure Boot**（UEFI 安全引导）模式，您无法将此选项设置为 **Enabled**（已启用）。该选项默认设置为 **Disabled（已禁用）**。
Dell Wyse P25/P45 BIOS Access	启用或禁用 Dell Wyse P25/P45 BIOS 的访问权限。此选项默认设置为 **Enabled（已启用）**。
Power Cycle Request	启用或禁用电源关闭后重启请求。该选项默认设置为 **None（无）**。

iDRAC 设置公用程序

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

注: 访问 iDRAC 设置公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（戴尔集成远程访问控制器用户指南）*，网址：。

设备设置

设备设置可用于配置以下设备参数：

- 控制器配置实用程序
- 嵌入式 NIC Port1-X 配置
- slotX 中的 NIC，Port1-X 配置
- BOSS 卡配置

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

Dell Lifecycle Controller 在系统的整个生命周期提供高级嵌入式系统管理。Dell Lifecycle Controller 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 Dell Lifecycle Controller 提供的整套功能。

有关设置 Dell Lifecycle Controller、配置硬件和固件以及部署操作系统的更多信息，请参阅 Dell Lifecycle Controller 说明文件，网址：。

引导管理器

Boot Manager（引导管理器）屏幕允许您选择引导选项和诊断公用程序。

查看引导管理器

关于此任务

要进入引导管理器，请执行以下操作：

步骤

1. 开启或重新启动系统。
2. 显示以下消息时按 F11 键：

   ```
   F11 = Boot Manager
   ```

   如果按 F11 键之前已开始加载操作系统，请让系统完成引导，然后重新启动系统并重试。

引导管理器主菜单

菜单项	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	通过该菜单项可以启动系统公用程序菜单，例如系统诊断和 UEFI shell。

一次性 UEFI 引导菜单

一次性 UEFI 引导菜单允许您选择引导设备。

系统公用程序

系统公用程序包含以下可以启动的公用程序：

- 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。