Integrated Dell Remote Access Controller 9 User's Guide

December 2020
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

iDRAC 概览

Integrated Dell Remote Access Controller (iDRAC) 设计用于提高系统管理员的工作效率和 Dell EMC 服务器的整体可用性。iDRAC 会就系统问题警告管理员，帮助管理员执行远程系统管理，减少物理访问系统的需要。

iDRAC 技术是大型数据中心解决方案的一部分，它有助于提高业务关键型应用程序和工作负载始终的可用性。技术允许您从任何位置部署、监测、管理、配置、更新和故障排除 Dell EMC 系统，而不使用任何代理程序或操作系统。

多个产品可与 iDRAC 协作，以简化 IT 操作。以下是一些工具：

- OpenManage Enterprise
- OpenManage Power Center 插件程序
- OpenManage Integration for VMware vCenter
- Dell Repository Manager

iDRAC 有以下型号：

- iDRAC Basic — 默认在 100-500 系列服务器上提供
- iDRAC Express — 默认在所有 600 和更高系列的机架式或塔式服务器以及所有刀片服务器上提供
- iDRAC Enterprise — 在所有服务器型号上都提供
- iDRAC Datacenter — 在所有服务器型号上都提供

主□：

使用 iDRAC 的优势

优点包括：

- 增强可用性 - 尽早通知可能的或实际的故障可帮助阻止服务器发生故障或在故障发生后缩短恢复时间。
- 提高工作效率和降低总体拥有成本 (TCO) - 将管理员的范围扩展到更多数量的远程服务器可提高 IT 人员工作效率的同时降低运营成本（例如出差）。
- 安全环境 - 通过提供远程服务器的安全访问，管理员可在执行重要管理功能的同时保持服务器和网络的安全。
- 借助 Lifecycle Controller 的增强嵌入式管理 - Lifecycle Controller 通过 Lifecycle Controller GUI 为本地部署提供部署功能和更简化的适用性，并且提供 Remote Services (WSMan) 界面进行远程部署，并与 Dell OpenManage Enterprise 及合作伙伴控制台集成。

有关 Lifecycle Controller GUI 的更多信息，请参阅 *生命周期控制器用户指南*，有关远程服务，请参阅 *生命周期控制器远程服务快速入门指南*，网址为 https://www.dell.com/idracmanuals。

主要功能

iDRAC 的主要功能包括：

注: 部分功能□在具有 iDRAC Enterprise 或 Datacenter □可□的情况下可用。有关□可□可用功能的信息，□参□ iDRAC 许可证 □面上的 23。

资源清册和监测

- 遥测数据流。
- 查看受管服务器的运行状况
- 资源清册和监测网络适配器与存储子系统（PERC 和直接连接存储），不含任何操作系统代理。
- 查看和导出系统资源清册。
- 查看传感器信息，例如温度、电压和侵入。
- 监测 CPU 状态、处理器自动调节和预测性故障。
- 查看内存信息。
- 监测和控制电源使用情况。
- 支持 SNMPv3 GET 和警报。
- 对于刀片服务器，启动管理模块 Web 界面、查看 OpenManage Enterprise (OME) Modular 信息以及 WWN/MAC 地址。
  注: CMC 通过 M1000E 机箱 LCD 面板和本地控制台连接提供对 iDRAC 的访问。有关更多信息，请参阅 机箱管理控制器用户指南，*网址：*https://www.dell.com/cmcmanuals。
- 查看主机操作系统上可用的网络接口。
- iDRAC9 通过 Quick Sync 2 提供了改进的监测和管理。您需要在 Android 或 iOS 移动设备中配置您的 OpenManage Mobile 应用程序。

部署

- 管理 vFlash SD 卡分区。
- 配置前面板显示设置。
- 管理 iDRAC 网络设置。
- 配置和使用虚拟控制台及虚拟介质。
- 使用远程文件共享和虚拟介质部署操作系统。
- 启用自动查找。
- 通过 RACADM、WSMan 和 Redfish 导出或导入 XML 或 JSON 配置文件执行服务器配置。有关更多信息，请参阅 *生命周期控制器远程服务快速入门指南，网址：*https://www.dell.com/idracmanuals。
- 配置持久性策略以用于虚拟地址、启动器和存储目标。
- 在运行时远程配置连接到系统的存储设备。
- 针对存储设备执行以下操作：
  - 物理磁盘：分配或取消分配物理磁盘作为全局热备份。
  - 虚拟磁盘：
    - 创建虚拟磁盘。
    - 编辑虚拟磁盘高速缓存策略。
    - 检查虚拟磁盘一致性。
    - 初始化虚拟磁盘。
    - 加密虚拟磁盘。
    - 分配和取消分配专用热备份。
    - 删除虚拟磁盘。
  - 控制器：
    - 配置控制器属性。
    - 导入或自动导入外部配置。
    - 清除外部配置。
    - 重设控制器配置。
    - 创建或更改安全密钥。
  - PCIe SSD 设备：
    - 对服务器中 PCIe SSD 设备的运行状况进行资源清册和远程监测
    - 准备移除 PCIe SSD。
    - 安全擦除数据。
  - 设置背板模式（统一模式或拆分模式）。
  - 闪烁或取消闪烁组件 LED。
  - 立即、下次重新引导系统期间、在计划的时间应用设备设置或作为在单个作业一部分中以批处理形式应用的挂起操作。

更新

- 管理 iDRAC 许可证。
- 为 Lifecycle Controller 支持的设备更新 BIOS 和设备固件。

- 使用单个固件映像更新或回滚 iDRAC 固件和 Lifecycle Controller 固件。
- 管理分阶段更新。
- 通过 USB 直接连接访问 iDRAC 界面。
- 使用 USB 设备上的服务器配置配置文件配置 iDRAC。

维护和故障排除

- 执行与电源相关的操作和监测功耗。
- 通过修改散热设置优化系统性能和功耗。
- 生成警报不依赖于 OpenManage Server Administrator。
- 记录事件数据：Lifecycle 和 RAC 日志。
- 设置事件的电子邮件警报、IPMI 警报、远程系统日志、WS 事件日志、Redfish 事件和 SNMP 陷阱（v1、v2c 和 v3）以及改进的电子邮件警报通知。
- 捕获上次系统崩溃映像。
- 查看引导和崩溃捕获视频。
- 带外监测和提醒 CPU、内存和 I/O 模块的性能指标。
- 配置入口温度和功耗的警告阈值。
- 使用 iDRAC Service Module 执行以下操作：
  - 查看操作系统信息。
  - 将 Lifecycle Controller 日志复制到操作系统日志。
  - 系统自动恢复选项。
  - 启用或禁用 PSU 以外的所有系统组件的完全电源重启的状态。
  - 远程硬重重置 iDRAC
  - 启用带内 iDRAC SNMP 警报
  - 使用主机操作系统访问 iDRAC（实验性功能）
  - 填充 Windows Management Instrumentation (WMI) 信息。
  - 与 SupportAssist Collection 集成。这仅适用于安装有 iDRAC Service Module 2.0 版或更高版本的情况。
- 通过以下方式生成 SupportAssist 收集：
  - 自动 — 使用自动调用 OS Collector 工具的 iDRAC 服务模块。

有关 iDRAC 的 Dell 最佳做法

- Dell iDRAC 旨在用于一个单独的管理网络；它们并未专门设计也不能置于互联网中或直接连接到互联网。这样做会使连接的系统面临安全风险和其他风险，Dell 对此概不负责。
- Dell EMC 建议使用机架式和塔式服务器上可用的专用千兆位以太网端口。此接口并未与主机操作系统共享，并将管理流量分发到单独的物理网络，使其能够从应用程序流量中分离出来。此选项意味着 iDRAC 的专用网络端口单独路由其流量，与服务器的 LOM 或 NIC 端口分离。与分配给主机 LOM 或 NIC 的 IP 地址相比，专用选项允许为 iDRAC 分配来自同一子网或不同子网的 IP 地址。
- 除了将 iDRAC 置于单独的管理子网上，用户应当使用技术（例如防火墙）隔离管理子网/vLAN，并将对于子网/vLAN 的访问权限限制为授权的服务器管理员。

保护连接性

保护对关键网络资源的访问权限至关重要。iDRAC 采用了一系列的安全功能，包括：

- 安全套接字层 (SSL) 证书的自定义签名证书。
- 签名固件更新。
- 通过 Microsoft Active Directory、通用轻型目录访问协议 (LDAP) 目录服务或本地管理的用户 ID 和密码进行用户验证。
- 使用智能卡登录功能进行双重验证。双重验证基于物理智能卡和智能卡 PIN。
- 单一登录和公共密钥身份验证。
- 基于角色的授权，为每个用户配置特定的权限。
- 针对在 iDRAC 中本地存储的用户帐户的 SNMPv3 验证。建议使用此控制器，但其在默认情况下已禁用。
- 用户 ID 和密码配置。
- 默认登录密码修改。
- 使用单向散列格式设置用户密码和 BIOS 密码，以提高安全性。
- FIPS 140-2 级别 1 功能。
- 会话超时配置（以秒为单位）
- 可配置的 IP 端口（针对 HTTP、HTTPS、SSH、虚拟控制台和虚拟介质）。
- 使用加密传输层的 Secure Shell (SSH) 实现更高的安全保护。
- 每个 IP 地址的登录失败限制，在超过此限制时阻止来自该 IP 地址的登录。
- 连接到 iDRAC 的客户端的有限 IP 地址范围。
- 专用的千兆位以太网适配器可在机架式和塔式服务器上使用（可能需要额外的硬件）。

新增功能

本部分提供了在以下版本中添加的新功能的列表：

Firmware version 4.40.00.00

This release includes all the features from the previous releases. Following are the new features that are added in this release:

NOTE: For information about supported systems, refer to the respective version of Release Notes available at https://www.dell.com/support/article/sln308699 .

- Added support for enhanced HTML5 (eHTML5) virtual KVM feature in virtual console
- Added support for eHTML5 virtual media
- Enhancement in Storage GUI page
- Added support for direct updates SEP backplane
- Added support for new update for PSU update
- Added support for uploading custom defaults and reset iDRAC to default settings using custom defaults
- Enhanced system lockdown mode support for supported devices

Following are the list of other features added in this release:

- **Automation**
  - Support for Redfish Updates
- **Monitoring/Alerting/Troubleshooting**
  - FPGA Monitoring
  - SMART data logs enhancements including historical recording
  - Discrete voltage sensor reporting
  - Report actual start and completion info for job queue entries which require a server reboot to apply (Example: BIOS update).
  - Providing CPU serial numbers in SupportAssist Collection
- **Telemetry** (requires iDRAC Datacenter license)
  - Multi-client support
  - Granular metric report options
  - Provision to POST a new custom MRD (Metric Report Definition) using any of the available 193 Metric Definitions and set desired Report Interval (referred as Recurrence Interval in MRD)
  - A single MRD can have a maximum of 68 Metric Definitions (Metric IDs)
  - Provision to create up to 24 new custom MRDs which in turn will have 24 new Metric Reports. An iDRAC can support a maximum of 48 Metric Reports (24 Pre-canned and 24 Custom
- **Security**
  - Automatic Certificate Enrollment Enhancements (requires iDRAC Datacenter License)
  - Integrate RSA SecurID Client into iDRAC for 2FA (requires iDRAC Datacenter License)
  - Compliance with STIG requirement – “network device must authenticate NTP”
  - Removal of Telnet and TLS 1.0 from web server
- **Platform feature support**
  - BOSS 1.5 updates
  - Infiniband support

In 4.40.00.00 release, following features are added in Storage page on iDRAC GUI:

- From the Dashboard, you can see suggested actions to solve any health alters.
- The Storage page has been modified to included tabs for storage monitoring information, a Storage Hardware and Software Inventory, a list of Pending and Current storage jobs, and SEKM.
  - From the Storage Inventory, users can find all storage related hardware and software.
  - The Pending and Current Jobs tab allows users to queue and monitor jobs from a centralized location.
  - You can also configure SEKM via the Storage page.
- When monitoring storage devices, you can customize the columns that are displayed for each device table. Column customization will be saved and persist between user sessions.
- New basic and advanced filters provided on each device page allow you to easily and efficiently customize the list of objects displayed.

- The Storage Configuration wizard has two options to create a Virtual disk - Basic and Advanced.
  - In the basic Virtual Disk wizard, you can quickly create a VD from a list of available RAID configurations. iDRAC will automatically set the default values of the VD to streamline the process.
  - For the Advanced Virtual Disk wizard, you can select all the details of the VD. You can create a new volume for the VD or select and existing volume.
- Each devices pages has new global actions that allow you to show related devices or preform group operations.
  - For example, you can choose physical disks and perform group operation such as Blink, Unblink, and Create Virtual Disk.
  - Also, you can view the Physical disk inventory and create a Virtual Disk by choosing the drives without having to navigate away from the screen.
- Instead of the numerical value, the size of the physical disk is shown as a data visualization with values on the scale.
  - This gives you an idea of used and available space on the drive.
- You can filter disks based on the various physical disk properties.
  - The filtering properties are displayed so that the user knows what filtering is currently being applied.

固件版本 4.30.30.30

此版本包含之前版本的所有功能。以下是此版本中增加的新功能：

注: 有关受支持系统的信息，请参阅 https://www.dell.com/support/article/sln308699 上提供的相应版本的发行说明。

- 新增对 AMD 系统的 PERC 11 的支持
- 新增对 PERC 11 之后的 NVMe 驱动器的支持
- 新增对 AMD 系统的 HBA11 的支持
- 新增对 AMD 系统的 CUPS 的支持
- 新增对启动优化存储解决方案 1.5 (BOSS1.5/BOSS-S2) 的支持
- 新增对 BOSS 1.5 安全固件更新的支持
- 新增对新的 Matrox 视频驱动程序的支持
- 新增对 NVMe Opal SED 的支持
- 新增对硬件信任链安全启动的支持
- 新增对 Mellanox CX6 的 InifiniBand 适配器的支持
- 新增对 PowerEdge C6525 的 24x NVMe 背板的支持
- 新增对新的 Matrox 视频驱动程序的支持
- 新增对 Starlord (ConnectX-6 Dx 100GbE) 到 iDRAC 的支持
- 为 BOSS-S2/PERC 11/HBA 11 新增与 FQDD 相关的更改
- 新增对不带背板的存储设备（例如但不限于 M.2 和 U.2）的支持
- 新增对 NVMe 驱动器的安全企业密钥管理 (SEKM) 的支持
- 将 iDRAC 内存从 512 MB 扩展至 1024 MB
- RESTUI 已针对因禁用验证后导致的电子邮件发送失败进行了更改

固件版本 4.20.20.20

此版本中添加了以下功能：

电源设备 (PSU)

- 支持 1100W ~48W DC PSU。
- 已移除 4S PSU 限制。

NIC

- 支持 (4x 10/25 SFP28) OCP 3.0 Dell 部件号 JTK7F - Broadcom。
- 支持 (4x10/25) MX 夹层卡，Dell 部件号 DCWFP - Broadcom 和 MX 25G 四端口（在 MX 平台上）。
- 支持将 Broadcom 10GbE NIC 卡添加到 R340。

加速器和 CPU

- 支持将两个新 GPU 卡添加至 Precision 7920 机架式服务器（Navi10DT/W5700、Navi14DT/W5500）。
- 支持适用于 PowerEdge 的 Nvidia V100S。
- 支持新的 Intel 处理器：6250 和 6256。

NVMe

- 支持 Samsung PM 1735 和 PM 1733 NVMe PCIe 存储。

自动化/脚本/遥测

- 支持 Redfish 2018R3、2019R1 和 2019R2 功能。
- 支持 CLI 方法来检索开机自检代码。
- 支持在 Power Manager 插件中将遥测 CUPS 上的报告时间间隔限制从 1 分钟增加到 1 小时。
- 支持遥测（指标报告启用/禁用）。
- 支持使用 SSH 进行增强型用户日志记录。
- 支持向 PCI Add IPMI 命令添加层规范标记。

其他

- 当具有一个或多个底座的 C6420 机箱通电时，支持热传感器板电缆检测。
- 支持在 6420 的底座 GUI 中显示插槽编号。
- 在交流电源中断或全局重置时，支持为 ADR 流提供始终运行的 AEP 和 BPS 内存。
- 支持 10x2.5 英寸 BP/机箱部件号更改。
- 支持对 SEL 日志启用“不支持的配置”。

固件版本 4.10.10.10

此版本中添加了以下功能：

默认许可证支持的功能

- BIOS 恢复和信任根 (RoT)

企业版许可证支持的功能

- 安全企业密钥管理 (SEKM) — 增加了对 Vormetric Data Security Manager 的支持。

Datacenter 许可证支持的功能

- BIOS 实时扫描 — 仅适用于 AMD 系统。

固件版本 4.00.00.00

此版本包含之前版本的所有功能。以下是此版本中增加的新功能：

注: 有关受支持系统的信息，请参阅 https://www.dell.com/support/article/sln308699 上提供的相应版本的发行说明。

Datacenter 许可证支持的功能

- 遥测数据流 — 流入分析工具的指标报告
- GPU 资源清册和监测
- 散热管理 — 高级电源和冷却功能
- 自动证书注册和续订 — 对于 SSL 证书
- 虚拟剪贴板 — 支持将文本字符串剪切并粘贴到远程虚拟控制台桌面
- SFP 收发器 — 输入/输出监测
- SMART 日志 — 存储驱动器
- 系统串行数据缓冲区捕获
- 空闲服务器检测

Enterprise 或 Datacenter 许可证支持的功能

- 通过电子邮件进行多因素身份验证
- 免代理崩溃视频捕获（仅限 Windows）
- 用于 LLDP 传输的连接视图
- 系统锁定模式 — 任何页面标题栏中的新图标
- Group Manager — 支持 250 个节点
- 增强了对安全企业密钥管理 (SEKM) 的支持

默认许可证（iDRAC Basic 或 iDRAC Express）支持的功能

- **GUI 增强功能**
  - 仪表板中的“任务摘要”部分
  - 标题栏中的搜索框
  - SupportAssist 收集查看器 — 在 iDRAC GUI 中显示输出
- **API、CLI 和 SCP**
  - 按服务器配置文件 (SCP) 部署操作系统
  - 启用和禁用对 SCP 和 RACADM 的启动顺序控制
  - Redfish API 的新架构
  - 用于更改 SCP 中的启动源状态的选项
  - 用于 RACADM 中的命令/属性自动完成的自动化功能
- **警报和监控**
  - SMTP 配置中用于电子邮件警报的自定义发件人电子邮件地址
  - SMTP 中基于云的电子邮件服务器
  - 针对硬盘和 PCIe SSD 设备的 SupportAssist 日志收集中的 SMARTlogs
  - 在警报消息中包含故障组件的部件号
- **安全性**
  - 仅使用 RACADM 命令的多个 IP 筛选范围
  - iDRAC 用户密码最长长度扩展为 40 个字符
  - 通过 SCP 的 SSH 公钥
  - 用于 SSH 登录的可自定义安全横幅
  - 针对登录的强制更改密码 (FCP)
- **存储和存储控制器**
  - 启用 PERC 以切换至 SEKM 加密模式

如何使用本指南

本用户指南中的内容指导您使用以下工具执行各种任务：

- iDRAC Web 界面 — 此处仅提供与任务相关的信息。有关字段和选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）（该联机帮助可通过 Web 界面访问）。
- RACADM — 此处提供您必须使用的 RACADM 命令或对象。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

- iDRAC 设置公用程序 — 此处仅提供与任务相关的信息。有关字段和选项的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助），访问方式为：单击 iDRAC 设置 GUI 中的**帮助**（在引导期间按 <F2>，然后单击**系统设置主菜单**页面上的 **iDRAC 设置**）。
- Redfish — 此处仅提供与任务相关的信息。有关字段和选项的信息，请参阅 *iDRAC Redfish API 指南*，网址：www.api-marketplace.com。

支持的 Web 浏览器

以下浏览器支持 iDRAC：
- Internet Explorer/Edge
- Mozilla Firefox
- Google Chrome
- Safari

有关支持版本的列表，请参阅 *iDRAC 发行说明，网址：*https://www.dell.com/idracmanuals。

支持的操作系统和虚拟机监控程序

在以下 OS、虚拟机监控程序上支持 iDRAC：
- Microsoft Windows Server 和 Windows PE
- VMware ESXI
- RedHat Enterprise Linux
- SuSe Linux Enterprise Server

注: 有关支持版本的列表，请参阅 *iDRAC 发行说明，网址：*https://www.dell.com/idracmanuals。

iDRAC 许可证

基于许可证类型 iDRAC 功能可用。根据系统型号，默认情况下会安装 iDRAC Basic 或 iDRAC Express 许可证。iDRAC Enterprise 许可证、iDRAC Datacenter 许可证和 iDRAC 安全企业密钥管理器 (SEKM) 许可证可在升级时提供，并且随时可以购买。界面上只会提供已许可的功能，您可以使用这些功能来配置或使用 iDRAC。有关更多信息，请参阅在 iDRAC9 中的已许可功能。

许可证类型

iDRAC Basic 或 iDRAC Express 是您系统上可用的标准许可证。iDRAC Enterprise 和 Datacenter 许可证包括所有已授权功能，可随时购买。提供的追加销售类型如下：
- 30 天试用 — 试用许可证基于持续时间，当系统接通电源时，计时器便会运行。此许可证无法延长。
- 永久 — 许可证绑定到服务标签，而且是永久性的。

下表列出了以下系统中提供的默认许可证：

iDRAC Basic 许可证	iDRAC Express 许可证	iDRAC Enterprise 许可证	iDRAC Datacenter 许可证
PowerEdge 机架/塔式服务器系列 100-500	• PowerEdge C41XX • PowerEdge FC6XX • PowerEdge R6XX • PowerEdge R64XX • PowerEdge R7XX • PowerEdge R74XXd • PowerEdge R74XX • PowerEdge R8XX • PowerEdge R9XX • PowerEdge R9XX • PowerEdge T6XX • Dell Precision Rack R7920	所有平台，有升级选项	所有平台，有升级选项

表. 1: 默认许可证

iDRAC Express 许可证	iDRAC Enterprise 许可证	iDRAC Datacenter 许可证
• PowerEdge C41XX • PowerEdge FC6XX • PowerEdge R6XX • PowerEdge R64XX • PowerEdge R7XX • PowerEdge R74XXd • PowerEdge R74XX • PowerEdge R8XX • PowerEdge R9XX • PowerEdge R9XX • PowerEdge T6XX • Dell Precision Rack R7920	所有平台，有升级选项	所有平台，有升级选项

注: PowerEdge C64XX 系□可用的默□□可□是 BMC。BMC □可□是 C64XX 系□自定□的。

注: PowerEdge M6XX 和 MXXXX 系□可用的默□□可□是 Express for Blades。

获取许可证的方法

使用以下任何方法都可获取许可证：

- Dell Digital Locker - Dell Digital Locker 允许您在一个位置查看和管理您的产品、软件和许可信息。DRAC Web 界面提供了 Dell Digital Locker 链接，请转到**配置** > **许可证**。

注: 要了解有关 Dell Digital Locker 的更多信息，□参□网站上的常见问题解答。

- 电子邮件 - 从技术支持中心请求后，许可证会附加到发送的电子邮件中。
- 销售点 - 订购系统时即可获得许可证。

注: 要管理□可□或□□新的□可□，□□至 Dell Digital Locker。

从 Dell Digital Locker 获取许可证密钥

要从您的帐户获取许可证密钥，必须首先使用在订单确认电子邮件中发送的注册代码注册您的产品。在登录到 Dell Digital Locker 之后，必须在**产品注册**选项卡中输入此代码。

从左侧窗格中，单击 **产品**或**订单历史记录**选项卡以查看您的产品列表。基于订阅的产品列在**开单帐户**选项卡下。

要下载您的 Dell Digital Locker 帐户的许可证密钥，请执行以下操作：

1. 登录到您的 Dell Digital Locker 帐户。
2. 在左侧窗格中，单击**产品**。
3. 单击您要查看的产品。
4. 单击产品名称。
5. 在**产品管理**页面中，单 **获取密钥**。
6. 按照屏幕上的指示获取许可证密钥。

注: 如果您没有 Dell Digital Locker 帐户，请使用您在购买过程中提供的电子邮件地址创建一个帐户。

注: 要生成多个许可证密钥用于新购买，请按照**工具** > **许可证激活** > **取消激活的许可证**下的说明进行操作。

许可证操作

执行许可证管理任务之前，请确保您已获取许可证。有关详情，请参阅获取许可证的方法。

注: 如果您□□的系□已□先安装所有□可□，□无需□行□可□管理。

对于一对一许可证管理，您可以使用 iDRAC、RACADM、WSMan、Redfish 和 Lifecycle Controller 远程服务，对于一对多许可证管理，您可以使用 Dell License Manager，来执行下列许可证操作：

- 查看 - 查看当前许可证信息。
- 导入 - 获取许可证后，将许可证存储到本地存储位置，并使用受支持的界面之一将其导入 iDRAC。如果许可证通过验证检查，则会将其导入。

  注: 尽管您可以导出出厂时安装的许可证，但无法导入。要导入许可证，请从 Digital Locker 下载等效许可证或从购买许可证时收到的电子邮件中检索许可证。

  注: 导入许可证后，您需要重新登录到 iDRAC。这仅适用于 iDRAC Web 界面。
- 导出 - 导出安装的许可证。有关更多信息，请参阅 *iDRAC 联机帮助*。
- 删除 - 删除许可证。有关更多信息，请参阅 *iDRAC 联机帮助*。
- 了解详情 - 了解已安装许可证或可供服务器上已安装组件使用的许可证的详细信息。

  注: 如需使用显示正确页面的了解详情选项，请确保已在安全设置的受信任的站点列表中添加 ***.dell.com**。有关更多信息，请参阅 Internet Explorer 说明文件。

对于一对多许可证部署，您可以使用 Dell License Manager。有关更多信息，请参阅 *Dell License Manager 用户指南*，网址：https://www.dell.com/esmmanuals。

以下是不同许可证操作的用户权限要求：

- 查看和导出许可证：登录权限。
- 导入和删除许可证：登录 + 配置 iDRAC + 服务器控制权限。

使用 iDRAC Web 界面管理许可证

要使用 iDRAC Web 界面管理许可证，请转至 **Configuration（配置）** > **Licenses（许可证）**。

Licensing（许可）页面显示与设备关联的许可证，或者已安装但系统中不存在的设备的许可证。有关导入、导出或删除许可证的更多信息，请参阅 *iDRAC Online Help（iDRAC 联机帮助）*。

使用 RACADM 管理许可证

要使用 RACADM 管理许可证，请使用**许可证**子命令。有关详情，请参阅

iDRAC RACADM CLI 指南，网址：https://www.dell.com/idracmanuals。

Licensed features in iDRAC9

The following table lists iDRAC9 features that are enabled based on the license purchased:

Table 2. Licensed features in iDRAC9

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
Interfaces / Standards					
iDRAC RESTful API and Redfish	Yes	Yes	Yes	Yes	Yes
IPMI 2.0	Yes	Yes	Yes	Yes	Yes
DCMI 1.5	Yes	Yes	Yes	Yes	Yes
Web-based GUI	Yes	Yes	Yes	Yes	Yes
RACADM command line (local/remote)	Yes	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes	Yes
Serial Redirection	Yes	Yes	Yes	Yes	Yes

Table 2. Licensed features in iDRAC9 (continued)

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
WSMan	Yes	Yes	Yes	Yes	Yes
Network Time Protocol	No	Yes	Yes	Yes	Yes
Connectivity					
Shared NIC (LOM)	Yes	Yes	N/A	Yes	Yes
Dedicated NIC	Yes	Yes	Yes	Yes	Yes
VLAN tagging	Yes	Yes	Yes	Yes	Yes
IPv4	Yes	Yes	Yes	Yes	Yes
IPv6	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes
DHCP with zero touch	No	No	No	Yes	Yes
Dynamic DNS	Yes	Yes	Yes	Yes	Yes
OS pass-through	Yes	Yes	Yes	Yes	Yes
iDRAC Direct -Front panel USB	Yes	Yes	Yes	Yes	Yes
Connection View	Yes	Yes	No	Yes	Yes
Security					
Role-based authority	Yes	Yes	Yes	Yes	Yes
Local users	Yes	Yes	Yes	Yes	Yes
SSL encryption	Yes	Yes	Yes	Yes	Yes
Secure Enterprise Key Manager	No	No	No	Yes (with SEKM license)	Yes (with SEKM license)
IP blocking	No	Yes	Yes	Yes	Yes
Directory services (AD, LDAP)	No	No	No	Yes	Yes
Two-factor authentication (smart card)	No	No	No	Yes	Yes
Single sign-On	No	No	No	Yes	Yes
PK authentication (for SSH)	No	Yes	Yes	Yes	Yes
OAuth integration with Web based Authentication services	No	No	No	No	Yes
OpenID Connect for Dell EMC Consoles	No	No	No	No	Yes
FIPS 140-2	Yes	Yes	Yes	Yes	Yes
Secure UEFI boot - certificate management	Yes	Yes	Yes	Yes	Yes
Lock down mode	No	No	No	Yes	Yes
Unique iDRAC default password	Yes	Yes	Yes	Yes	Yes

Table 2. Licensed features in iDRAC9 (continued)

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
Customizable Security Policy Banner - login page	Yes	Yes	Yes	Yes	Yes
Easy Multi Factor Authentication	No	No	No	No	Yes
Auto Certificate Enrollment (SSL Certs)	No	No	No	No	Yes
iDRAC Quick Sync 2 - optional auth for read operations	Yes	Yes	Yes	Yes	Yes
iDRAC Quick Sync 2 - add mobile device number to LCL	Yes	Yes	Yes	Yes	Yes
System Erase of internal storage devices	Yes	Yes	Yes	Yes	Yes
Remote Presence					
Power control	Yes	Yes	Yes	Yes	Yes
Boot control	Yes	Yes	Yes	Yes	Yes
Serial-over-LAN	Yes	Yes	Yes	Yes	Yes
Virtual Media	No	No	Yes	Yes	Yes
Virtual Folders	No	No	No	Yes	Yes
Remote File Share	No	No	No	Yes	Yes
HTML5 access to Virtual Console	No	No	Yes	Yes	Yes
Virtual Console	No	No	Yes	Yes	Yes
VNC connection to OS	No	No	No	Yes	Yes
Quality/bandwidth control	No	No	No	Yes	Yes
Virtual Console collaboration (up to six simultaneous users)	No	No	No (One user only)	Yes	Yes
Virtual Console chat	No	No	No	Yes	Yes
Virtual Flash partitions	No	No	No	Yes	Yes
NOTE: vFlash is not available in iDRAC9 for PowerEdge Rx5xx/Cx5xx.					
Group Manager	No	No	No	Yes	Yes
HTTP / HTTPS support along with NFS/CIFS	Yes	Yes	Yes	Yes	Yes
Power and Thermal					
Real-time power meter	Yes	Yes	Yes	Yes	Yes
Power thresholds and alerts	No	Yes	Yes	Yes	Yes
Real-time power graphing	No	Yes	Yes	Yes	Yes

Table 2. Licensed features in iDRAC9 (continued)

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
Historical power counters	No	Yes	Yes	Yes	Yes
Power capping	No	No	No	Yes	Yes
Power Center integration	No	No	No	Yes	Yes
Temperature monitoring	Yes	Yes	Yes	Yes	Yes
Temperature graphing	No	Yes	Yes	Yes	Yes
PCIe airflow customization (LFM)	No	No	No	No	Yes
Custom Exhaust Control	No	No	No	No	Yes
Custom Delta-T control	No	No	No	No	Yes
System Airflow Consumption	No	No	No	No	Yes
Custom PCIe inlet temperature	No	No	No	No	Yes
Health Monitoring					
Full agent-free monitoring	Yes	Yes	Yes	Yes	Yes
Predictive failure monitoring	Yes	Yes	Yes	Yes	Yes
SNMPv1, v2, and v3 (traps and gets)	Yes	Yes	Yes	Yes	Yes
Email Alerting	No	Yes	Yes	Yes	Yes
Configurable thresholds	Yes	Yes	Yes	Yes	Yes
Fan monitoring	Yes	Yes	Yes	Yes	Yes
Power Supply monitoring	Yes	Yes	Yes	Yes	Yes
Memory monitoring	Yes	Yes	Yes	Yes	Yes
CPU monitoring	Yes	Yes	Yes	Yes	Yes
RAID monitoring	Yes	Yes	Yes	Yes	Yes
NIC monitoring	Yes	Yes	Yes	Yes	Yes
Optic Inventory	Yes	Yes	Yes	Yes	Yes
Optic Statistics	No	No	No	No	Yes
HD monitoring (enclosure)	Yes	Yes	Yes	Yes	Yes
Out of Band Performance Monitoring	No	No	No	Yes	Yes

Table 2. Licensed features in iDRAC9 (continued)

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
Alerts for excessive SSD wear	Yes	Yes	Yes	Yes	Yes
Customizable settings for Exhaust Temperature	Yes	Yes	Yes	Yes	Yes
Serial Console Logs	No	No	No	No	Yes
SMART logs for Storage Drives	No	No	No	No	Yes
Idle Server detection	No	No	No	No	Yes
Telemetry Streaming	No	No	No	No	Yes
NOTE: The OpenManage Enterprise Advanced license and the PowerManage Plugin support telemetry data pulls from the iDRAC.					
Update					
Remote agent-free update	Yes	Yes	Yes	Yes	Yes
Embedded update tools	Yes	Yes	Yes	Yes	Yes
Update from repository (Auto-Update)	No	No	No	Yes	Yes
Schedule update from repository	No	No	No	Yes	Yes
Improved PSU firmware updates	Yes	Yes	Yes	Yes	Yes
Deployment and Configuration					
Local configuration via F10	Yes	Yes	Yes	Yes	Yes
Embedded OS deployment tools	Yes	Yes	Yes	Yes	Yes
Embedded configuration tools	Yes	Yes	Yes	Yes	Yes
Auto-Discovery	No	Yes	Yes	Yes	Yes
Remote OS deployment	No	Yes	Yes	Yes	Yes
Embedded driver pack	Yes	Yes	Yes	Yes	Yes
Full configuration inventory	Yes	Yes	Yes	Yes	Yes
Inventory export	Yes	Yes	Yes	Yes	Yes
Remote configuration	Yes	Yes	Yes	Yes	Yes
Zero-touch configuration	No	No	No	Yes	Yes

Table 2. Licensed features in iDRAC9 (continued)

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
System Retire/Repurpose	Yes	Yes	Yes	Yes	Yes
Server Configuration Profile in GUI	Yes	Yes	Yes	Yes	Yes
Add BIOS configuration to iDRAC GUI	Yes	Yes	Yes	Yes	Yes
GPU properties	No	No	No	Yes	Yes
Diagnostics, Service, and Logging					
Embedded diagnostic tools	Yes	Yes	Yes	Yes	Yes
Part Replacement	No	Yes	Yes	Yes	Yes
NOTE: After performing part replacement on RAID hardware, and the process is complete for replacing firmware and configuration, Lifecycle Logs reports double part replacement entries which is expected behavior.					
Easy Restore (system configuration)	Yes	Yes	Yes	Yes	Yes
Easy Restore Auto Timeout	Yes	Yes	Yes	Yes	Yes
NOTE: Server Backup and Restore features are not available in iDRAC9 for PowerEdge Rx5xx/Cx5xx.					
LED Health status indicators	Yes	Yes	N/A	Yes	Yes
LCD screen (iDRAC9 requires optional)	Yes	Yes	N/A	Yes	Yes
iDRAC Quick Sync 2 (BLE/Wi-Fi hardware)	Yes	Yes	Yes	Yes	Yes
iDRAC Direct (front USB management port)	Yes	Yes	Yes	Yes	Yes
iDRAC Service Module (iSM) embedded	Yes	Yes	Yes	Yes	Yes
iSM to in-band alert forwarding to consoles	Yes	Yes	Yes	Yes	Yes
SupportAssist Collection (embedded)	Yes	Yes	Yes	Yes	Yes
Crash screen capture	No	Yes	Yes	Yes	Yes
Crash video capture[1]	No	No	No	Yes	Yes
Agent Free Crash Video Capture (Windows only)	No	No	No	No	Yes
Boot capture	No	No	No	Yes	Yes
Manual reset for iDRAC (LCD ID button)	Yes	Yes	Yes	Yes	Yes

Table 2. Licensed features in iDRAC9 (continued)

Feature	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express for Blades	iDRAC9 Enterprise	iDRAC9 Datacenter
Remote reset for iDRAC (requires iSM)	Yes	Yes	Yes	Yes	Yes
Virtual NMI	Yes	Yes	Yes	Yes	Yes
OS watchdog	Yes	Yes	Yes	Yes	Yes
System Event Log	Yes	Yes	Yes	Yes	Yes
Lifecycle Log	Yes	Yes	Yes	Yes	Yes
Enhanced Logging in Lifecycle Controller Log	Yes	Yes	Yes	Yes	Yes
Work notes	Yes	Yes	Yes	Yes	Yes
Remote Syslog	No	No	No	Yes	Yes
License management	Yes	Yes	Yes	Yes	Yes
Improved Customer Experience					
iDRAC -Faster processor, more memory	N/A	Yes	N/A	Yes	Yes
GUI rendered in HTML5	N/A	Yes	N/A	Yes	Yes
Add BIOS configuration to iDRAC GUI	N/A	Yes	N/A	Yes	Yes

[1] Requires iSM or OMSA agent on target server.

访问 iDRAC 的界面和协议

下表列出了访问 iDRAC 的界面。

注: 同时使用一个以上的界面可能会产生意外的结果。

表. 3: 访问 iDRAC 的界面和协议

界面或协议	说明
iDRAC 设置公用程序 (F2)	使用 iDRAC 设置公用程序执行操作系统预操作。它具有一个功能子集，可通过 iDRAC Web 界面与其他功能一起提供。 要访问 iDRAC 设置公用程序，请在引导过程中按 <F2> 键，然后在**系统设置主菜单**页面上单击 **iDRAC 设置**。
Lifecycle Controller (F10)	使用 Lifecycle Controller 执行 iDRAC 配置。要访问 Lifecycle Controller，请在引导过程中按 <F10> 然后转至**系统设置** > **高级硬件配置** > **iDRAC 设置**。有关信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller 用户指南*。
iDRAC Web 界面	使用 iDRAC Web 界面管理 iDRAC 并监测受管系统。浏览器通过 HTTPS 端口连接到 Web 服务器。数据流将使用 128 位 SSL 进行加密以确保隐私性和完整性。到 HTTP 端口的任何连接都将重定向到 HTTPS。管理员可以通过 SSL CSR 生成过程上传自己的 SSL 证书以保护 Web 服务器。可以更改默认 HTTP 和 HTTPS 端口。用户的访问权限基于用户权限。
OpenManage Enterprise (OME) Modular Web 界面	**注:** 此界面仅适用于 MX 平台。 除监测和管理机箱外，使用 OME-Modular Web 界面还可以：

表. 3: 访问 iDRAC 的界面和协议 （续）

界面或协议	说明
	• 查看受管系统的状态 • 更新 iDRAC 固件 • 配置 iDRAC 网络设置 • 登录到 iDRAC Web 界面 • 启动、停止或重设受管系统 • 更新 BIOS、PERC 和支持的网络适配器 有关更多信息，请参阅 适用于 PowerEdge MX7000 机箱的 *OME - Modular* 用户指南，网址：https://www.dell.com/openmanagemanuals。
CMC Web 界面	**注:** 此界面在 MX 平台上不可用。 除监测和管理机箱外，使用 CMC Web 界面还可以： • 查看受管系统的状态 • 更新 iDRAC 固件 • 配置 iDRAC 网络设置 • 登录到 iDRAC Web 界面 • 启动、停止或重设受管系统 • 更新 BIOS、PERC 和支持的网络适配器
服务器 LCD 面板/机箱 LCD 面板	使用服务器前面板上的 LCD 可以： • 查看警报、iDRAC IP 或 MAC 地址、用户可编程字符串。 • 设置 DHCP • 配置 iDRAC 静态 IP 设置。 对于刀片式服务器，LCD 位于机箱前面板上，并且供所有刀片共用。 要重设 iDRAC 而不重新引导服务器，请按住系统标识按钮 16 秒。 **注:** 只有支持前挡板的机架或塔式系统才提供 LCD 面板。对于刀片式服务器，LCD 位于机箱前面板上，并且供所有刀片共用。
RACADM	使用此命令行公用程序可以执行 iDRAC 和服务器管理。您可以在本地和远程使用 RACADM。 • 本地 RACADM 命令行界面在安装有服务器管理器的受管系统上运行。本地 RACADM 通过其带内 IPMI 主机接口与 iDRAC 通信。由于它安装在本地受管系统上，因此用户需要登录到操作系统，才能运行此公用程序。用户必须具有完整的管理员权限或者是根用户，才能使用此公用程序。 • 远程 RACADM 是在管理站上运行的客户端公用程序。它使用带外网络接口在受管系统上运行 RACADM 命令，并且使用 HTTPs 通道。**–r** 选项在网络上运行 RACADM 命令。 • 固件 RACADM 可以通过使用 SSH 登录 iDRAC 进行访问。您可以运行固件 RACADM 命令，无需指定 iDRAC IP、用户名或密码。 • 您无需指定 iDRAC IP、用户名或密码，即可运行固件 RACADM 命令。进入 RACADM 提示符后，您可以直接运行命令，无需 racadm 前缀。
iDRAC RESTful API 和 Redfish	Redfish 可扩展平台管理 API 是由分布式管理综合小组 (DMTF) 定义的标准。Redfish 是下一代系统管理接口标准，支持可扩展、安全且开放的服务器管理。它是一种新的界面，可使用 RESTful 界面语义访问以型号格式定义的数据，从而执行带外系统管理。它适合各种服务器，包括独立服务器、机架式或刀片式服务器环境以及大型云环境。 Redfish 可通过现有服务器管理方法提供以下好处： • 更高的简易性和可用性 • 高数据安全性 • 可轻松脚本化的可编程接口 • 遵循广泛使用的标准 有关 iDRAC Redfish API 指南的信息，请访问 www.api-marketplace.com
WSMan	LC 远程服务基于一对多系统管理任务的 WSMan 协议。您必须使用 WSMan 客户端（如 WinRM 客户端 (Windows) 或 OpenWSMan 客户端 (Linux)）来使用 LC 远程服务功能。您也可以使用 Power Shell 或 Python 来编写 WSMan 界面脚本。

表. 3: 访问 iDRAC 的界面和协议 （续）

界面或协议	说明
	Web Services for Management (WSMan) 是基于简单对象访问协议 (SOAP) 的协议，用于系统管理。iDRAC 使用 WSMan 传送基于分布式管理综合小组 (DMTF) 公用信息模型 (CIM) 的管理信息。CIM 信息可定义能够在受管系统中修改的语义和信息类型。通过 WSMan 获得的数据由映射到 DMTF 配置文件和扩展名配置文件的 iDRAC 工具界面提供。 有关更多信息，请参阅以下内容： • *生命周期控制器远程服务快速入门指南，网址：*https://www.dell.com/idracmanuals。 • MOF 和配置文件 - http://downloads.dell.com/wsman。 • DMTF 网站 - dmtf.org/standards/profiles/
SSH	使用 SSH 运行 RACADM 命令。默认情况下，在 iDRAC 上启用了 SSH 服务。可以在 iDRAC 中禁用 SSH 服务。iDRAC 只支持带有 RSA 主机密钥算法的 SSH 版本 2。首次启动 iDRAC 时将生成一个唯一的 1024 位 RSA。
IPMITool	使用 IPMITool 通过 iDRAC 访问远程系统的基本管理功能。该界面包括本地 IPMI、LAN 上 IPMI、IPMI 串行和 LAN 上串行。有关 IPMITool 的更多信息，请参阅 dell.com/idracmanuals 上的 *Dell OpenManage Baseboard Management Controller 公用程序用户指南*。 **注:** IPMI 版本 1.5 不受支持。
NTLM	iDRAC 允许 NTLM 为用户提供身份验证、完整性和机密性。NT LAN Manager (**NTLM**) 是一套 Microsoft 网络安全性协议，在 Windows 网络中运行。
SMB	iDRAC9 支持服务器消息块 (SMB) 协议。这是网络文件共享协议，默认支持的最小 SMB 版本是 2.0，SMBv1 不再受支持。
NFS	iDRAC9 支持 **网络文件**系统 (**NFS**)。这是分布式文件系统协议，使用户能够在服务器上**装载**远程目录。

iDRAC 端口信息

下表列出了通过防火墙远程访问 iDRAC 时需要的端口。这些是用于侦听连接的默认 iDRAC 端口。（可选）您可以修改大多数端口。要修改端口，请参阅 配置服务 页面上的 91。

表. 4: iDRAC 用于监听连接的端口

端口号	类型	功能	可配置端口	最高加密级别
22	TCP	SSH	是	256 位 SSL
80	TCP	HTTP	是	无
161	UDP	SNMP 代理	是	无
443	TCP	• 使用 HTTPS 的 Web GUI 访问 • 具有 eHTML5 选项的虚拟控制台和虚拟介质 • 启用 Web 服务器重定向时具有 HTML5 选项的虚拟控制台和虚拟介质	是	256 位 SSL
623	UDP	RMCP/RMCP+	否	128 位 SSL
5000	TCP	iDRAC 至 iSM	否	256 位 SSL
注: 如果同时安装了 iSM 3.4 或更高版本和 iDRAC 固件 3.30.30.30 或更高版本，则最大加密级别是 256 位 SSL。				
5900	TCP	具有 HTML5、Java 和 ActiveX 选项的虚拟控制台和虚拟介质	是	128 位 SSL
5901	TCP	VNC	是	128 位 SSL
注: 当 VNC 功能启用时，端口 5901 开放。				

下表列出了 iDRAC 用作客户端的端口：

表. 5: iDRAC 用作客户端的端口

端口号	类型	功能	可配置端口	最高加密级别
25	TCP	SMTP	是	无
53	UDP	DNS	否	无
68	UDP	DHCP 分配的 IP 地址	否	无
69	TFTP	TFTP	否	无
123	UDP	网络时间协议 (NTP)	否	无
162	UDP	SNMP 陷阱	是	无
445	TCP	通用 Internet 文件系统 (CIFS)	否	无
636	TCP	SSL 上 LDAP (LDAPS)	否	256 位 SSL
2049	TCP	网络文件系统 (NFS)	否	无
3269	TCP	全局编录 (GC) LDAPS	否	256 位 SSL
5353	UDP	mDNS	否	无
注: 启用节点启动查找或 Group Manager 时，iDRAC 通过端口 5353 使用 mDNS 进行通信。但是，当两项均被禁用时，端口 5353 被 iDRAC 的内部防火墙阻止并在端口扫描中显示为打开|筛选端口。				
514	UDP	远程系统日志	是	无

您可能需要的其他说明文件

某些 iDRAC 界面具有通过单击帮助 (?) 图标可以访问的集成*联机帮助*说明文件。*联机帮助*提供有关 web 界面上可用字段及其说明的详细信息。此外，Dell 支持网站 **dell.com/support** 上的以下说明文件提供了关于在系统中设置和操作 iDRAC 的附加信息。

- https://developer.dell.com 上提供的 iDRAC Redfish API 指南提供了有关 Redfish API 的信息。
- *iDRAC RACADM CLI 指南* 提供了有关 RACADM 子命令、支持的界面、iDRAC 属性数据库组和对象定义的信息。
- *系统管理概览指南* 提供了关于可用于执行系统管理任务的各种软件的简要信息。
- *Dell Remote Access Configuration Tool 用户指南*提供了关于如何使用工具来查找您网络中的 iDRAC IP 地址的信息，以及如何为所发现的 IP 地址执行一对多固件更新和 Active Directory 配置的信息。
- *Dell 系统软件支持值表*提供有关各种 Dell 系统、这些系统支持的操作系统以及可以安装在这些系统上的 Dell OpenManage 组件的信息。
- *iDRAC 服务模块用户指南*提供了有关如何安装 iDRAC 服务模块的信息。
- *Dell OpenManage Server Administrator 安装指南*包含帮助安装 Dell OpenManage Server Administrator 的说明。
- *Dell OpenManage Management Station 软件安装指南*包含帮助安装 Dell OpenManage Management Station 软件的说明，该软件包括 Baseboard Management Utility、DRAC 工具和 Active Directory 管理单元。
- *Dell OpenManage Baseboard Management Controller Management Utilities 用户指南*包含关于 IPMI 界面的信息。
- *发行说明*提供系统或说明文件的最新更新，或为有经验的用户或技术员提供高级技术参考资料。

可利用以下系统说明文件获取更多信息：

- 系统随附的安全说明提供了重要的安全和法规信息。其他法规信息请参阅法规合规性主页，网址是 **dell.com/regulatory_compliance**。保修信息可能包含于此说明文件中，也可能为单独的说明文件。
- 机架解决方案附带的*机架安装说明*介绍如何将系统安装到机架中。
- *入门指南* 提供了系统功能、设置系统和技术规范的概述。
- *安装和服务手册*提供了有关系统功能的信息，并说明了如何排除系统故障以及安装或更换系统组件。

联系 Dell

注: 如果您不能连接至 Internet，您可以在您的购买发票、装箱单、账单或 Dell 产品目录中找到联系信息。

Dell 提供多种联机和基于电话的支持和服务选项。具体的服务随您所在国家/地区以及产品的不同而不同，某些服务在您所在的地区可能不提供。如要联系 Dell 有关销售、技术支持或客户服务事宜，请访问 https://www.dell.com/contactdell

从 Dell 支持站点访问说明文件

您可以通过以下方式之一访问所需的说明文件：

- 使用以下链接：
  - 有关所有企业系统管理和 OpenManage Connections 说明文件 — https://www.dell.com/esmmanuals
  - 有关 OpenManage 文档 — https://www.dell.com/openmanagemanuals
  - 有关 iDRAC 和 Lifecycle Controller 文档 — https://www.dell.com/idracmanuals
  - 有关可维护性工具文档 — https://www.dell.com/serviceabilitytools
  - 有关客户端命令套件系统管理文档 — https://www.dell.com/omconnectionsclient

使用产品搜索访问说明文件

1. 访问 https://www.dell.com/support。
2. 在**“输入服务编号、序列号...”**搜索框中，键入产品名称。例如，**PowerEdge** 或 **iDRAC**。

   随即显示匹配产品的列表。
3. 选择您的产品，然后单击搜索图标或按 Enter 键。
4. 单击**文档**。
5. 单击**手册和说明文件**。

使用产品选择器访问说明文件

此外，您还可通过选择产品访问说明文件。

1. 访问 https://www.dell.com/support。
2. 单击**“浏览所有产品”**。
3. 单击所需的产品类别，例如服务器、软件、存储设备等。
4. 单击所需的产品，然后单击所需版本（如果适用）。

   注: 对于某些产品，您可能需要浏览子类别。
5. 单击**文档**。
6. 单击**手册和说明文件**。

获取 Redfish API 指南

Redfish API 指南现在可从戴尔 API 商店进行获取。要获取 Redfish API 指南，请执行以下操作：

1. 访问 www.api-marketplace.com。
2. 单击 **浏览 API**，然后单击 **API**。
3. 在 iDRAC9 Redfish API 下，单击**查看更多**。

2

登录 iDRAC

您可以以 iDRAC 用户、Microsoft Active Directory 用户或轻量级目录访问协议 (LDAP) 用户的身份登录到 iDRAC。也可以使用 OpenID Connect 和单一登录或智能卡登录。

为了提高安全性，每个系统都附带 iDRAC 的唯一密码，该密码位于系统信息标签上。此唯一密码可提高 iDRAC 和服务器的安全性。默认用户名为 *root*。

订购系统时，您可以选择保留传统密码 calvin 作为默认密码。如果选择保留传统密码，则密码在系统信息标签上不可用。

在此版本中，DHCP 默认已启用并且 iDRAC IP 地址动态分配。

注：

- 您必须具有登录到 iDRAC 的权限才能登录 iDRAC。
- iDRAC GUI 不支持浏览器按钮，例如**后退**、**前进**或**刷新**。

注： 有关□用□名和密□建□的字符的信息，□参□ 建议使用的用户名和密码字符 □面上的 135。

要更改默认密码，请参阅 更改默认登录密码 页面上的 44。

可自定义的安全横幅

您可以自定义登录页面显示的安全通知。您可以使用 SSH、RACADM、Redfish 或 WSMan 来自定义声明。声明可以是 1024 或 512 UTF-8 字符长度，具体取决于您使用的语言。

OpenID Connect

注： 此功能仅适用于 MX 平台。

您可以使用其他 Web 控制台的凭据登录到 iDRAC，例如 Dell EMC OpenManage Enterprise (OME) - Modular。启用此功能后，控制台将开始管理 iDRAC 上的用户权限。iDRAC 为用户会话提供控制台指定的所有权限。

注： 已启用锁定模式时，不会在 iDRAC 登录页面中显示 OpenID Connect 登录选项。

您现在无需登录 iDRAC 即可访问详细的帮助。使用 iDRAC 登录页面上的链接来访问帮助和版本信息、驱动程序和下载、手册和技术中心。

主□：

- 强制更改密□ (FCP)
- 使用 OpenID Connect 登□ iDRAC
- 以本地用□、Active Directory 用□或 LDAP 用□身份登□ iDRAC
- 使用智能卡作□本地用□登□ iDRAC
- 使用□一登□登□ iDRAC
- 使用□程 RACADM □□ iDRAC
- 使用本地 RACADM □□ iDRAC
- 使用固件 RACADM □□ iDRAC
- □□的双重身份□□（□□ 2FA）
- RSA SecurID 2FA
- □看系□运行状况
- 使用公共密□□□登□ iDRAC
- 多个 iDRAC 会□
- 安全默□密□
- 更改默□登□密□

- 启用或禁用默□密□警告消息
- 密□强度策略
- IP 阻止
- 使用 Web 界面启用或禁用 OS 到 iDRAC 直通
- 使用 RACADM 启用或禁用警□

强制更改密码 (FCP)

“强制更改密码”功能会提示您更改设备的出厂默认密码。该功能可在出厂配置过程中启用。

用户身份验证成功后，将显示 FCP 屏幕且不能跳过。只有在用户输入密码后，才允许正常访问和操作。此属性的状态将不受“将配置重设为默认值”操作的影响。

注: 要□置或重置 FCP 属性，您必□具有登□权限和用□配置权限。

注: 如果启用了 FCP，在更改默□用□密□后，将禁用“默□密□警告”□置。

注: 当根用□通□公共密□□□ (PKA) 登□□，将□□ FCP。

启用 FCP 时，不允许执行以下操作：

- 通过默认用户凭据使用 CLI 的任何用户界面（IPMI Over LAN 界面除外）登录到 iDRAC。
- 通过 Quick Sync-2 通过 OMM 应用程序登录 iDRAC
- 在 Group Manager 中添加成员 iDRAC。

使用 OpenID Connect 登录 iDRAC

注: 此功能仅在 MX 平台中提供。

要使用 OpenID Connect 登录 iDRAC：

1. 在支持的 Web 浏览器中，键入 `https://[iDRAC-IP-address]`，然后按 Enter 键。
   将显示登录页。
2. 从**登录方式：**菜单中选择 **OME Modular**。
   随即显示控制台登录页面。
3. 输入控制台**用户名**和**密码**。
4. 单击**登录**。
   您已使用控制台用户权限登录到 iDRAC。
   注: 已启用锁定模式时，不会在 iDRAC 登录页面中显示 OpenID Connect 登录选项。

以本地用户、Active Directory 用户或 LDAP 用户身份登录 iDRAC

在使用 Web 界面登录 iDRAC 之前，请确保已配置受支持的 Web 浏览器，并且已创建具有所需权限的用户帐户。

注: Active Directory 用户的用户名不区分大小写。所有用户的密码均区分大小写。

注: 除支持 Active Directory 外，基于 openLDAP、openDS、Novell eDir 和 Fedora 的目录服务也受支持。

注: 支持使用 OpenDS 进行 LDAP 身份验证。DH 密钥必须大于 768 位。

注: 可以为 LDAP 用户配置和启用 RSA 功能，但如果在 Microsoft Active Directory 上配置 LDAP，则不支持 RSA。因此 LDAP 用户登录将失败。仅 OpenLDAP 支持 RSA。

要以本地用户、Active Directory 用户或 LDAP 用户身份登录 iDRAC：

1. 打开支持的 Web 浏览器。

2. 在**地址**字段中，键入 `https://[iDRAC-IP-address]` 并按 Enter。

   注: 如果已更改默认 HTTPS 端口号（端口 443），请输入 `https://[iDRAC-IP-address]:[port-number]`，其中，`[iDRAC-IP-address]` 是 iDRAC IPv4 或 IPv6 地址，`[port-number]` 是 HTTPS 端口号。

   将显示**登录**页。
3. 对于本地用户：
   - 在**用户名**和**密码**字段中，输入您的 iDRAC 用户名和密码。
   - 从**域**下拉菜单中，选择**此 iDRAC**。
4. 对于 Active Directory 用户，请在**用户名**和**密码**字段中输入 Active Directory 用户名和密码。如果您已指定将域名作为用户名的一部分，请从下拉菜单中选择**此 iDRAC**。用户名的格式可为：<domain>\<username>、<domain>/<username> 或 <user>@<domain>。

   例如，dell.com\john_doe 或 JOHN_DOE@DELL.COM。

   如果未在用户名中指定域，请从**域**下拉菜单中选择 Active Directory 域。
5. 对于 LDAP 用户，请在**用户名**和**密码**字段中输入 LDAP 用户名和密码。LDAP 登录不需要域名。在默认情况下，下拉菜单中已选定**此 iDRAC**。
6. 单击**提交**。您已使用所需的用户权限登录到 iDRAC。

   如果您以配置用户权限和默认帐户凭据登录，并且如果已启用默认密码警告功能，则会显示**默认密码警告**页面，允许您轻松更改密码。

使用智能卡作为本地用户登录 iDRAC

使用智能卡作为本地用户登录之前，请确保：
- 将用户智能卡证书和受信任的认证机构 (CA) 证书上载到 iDRAC
- 启用智能卡登录。

iDRAC Web 界面会向配置为使用智能卡的用户显示智能卡登录页。

注: 根据浏览器设置的不同，第一次使用此功能时，将提示您下载并安装智能卡读卡器 ActiveX 插件。

要使用智能卡作为本地用户登录 iDRAC：

1. 使用链接 `https://[IP address]` 访问 iDRAC Web 界面。

   这将显示 **iDRAC 登录**页面，提示您插入智能卡。

   注: 如果默认 HTTPS 端口号（端口 443）已更改，请键入：`https://[IP address]:[port number]` ，其中，`[IP address]` 是 iDRAC 的 IP 地址而 `[port number]` 是 HTTPS 端口号。
2. 将智能卡插入读卡器中并单击**登录**。
   将显示输入智能卡 PIN 码的提示。无需密码。
3. 输入本地智能卡用户的智能卡 PIN 码。

   您已登录 iDRAC。

   注: 如果您是已启用**启用智能卡登录的 CRL 检查功能**的本地用户，则 iDRAC 会尝试下载证书吊销列表 (CRL) 并检查 CRL 有无用户证书。如果证书在 CRL 中列出为已吊销或 CRL 出于某些原因无法下载，则登录失败。

   注: 当 RSA 处于启用状态时，如果您使用智能卡登录 iDRAC，系统将绕过 RSA 令牌，您可以直接登录。

使用智能卡作为 Active Directory 用户登录 iDRAC

当您使用智能卡作为 Active Directory 用户登录之前，请确保您：
- 将受信任的认证机构 (CA) 证书（认证机构签署的 Active Directory 证书）上载到 iDRAC。
- 配置 DNS 服务器。
- 启用 Active Directory 登录。
- 启用智能卡登录。

要使用智能卡作为 Active Directory 用户登录 iDRAC：

1. 使用链接 `https://[IP address]` 登录 iDRAC。
   这将显示 **iDRAC 登录**页面，提示您插入智能卡。
   注: 如果默认的 HTTPS 端口号（端口 443）已更改，请键入：`https://[IP address]:[port number]`，其中，`[IP address]` 是 iDRAC IP 地址，而 `[port number]` 是 HTTPS 端口号。
2. 插入智能卡并单击**登录**。
   将显示输入智能卡 **PIN** 码的提示，
3. 输入 PIN，并单击**提交**。
   您已使用您的 Active Directory 凭据登录到了 iDRAC。
   注:

   如果 Active Directory 中存在该智能卡用户，则不需要输入 Active Directory 密码。

使用单一登录登录 iDRAC

启用单一登录 (SSO) 后，您可以直接登录 iDRAC 而无需输入您的域用户验证凭据（例如用户名和密码）。
注: 当 RSA 为启用状态并且 AD 用户配置 SSO 时，系统将绕过 RSA 令牌，用户直接登录。

使用 iDRAC Web 界面登录 iDRAC SSO

使用单一登录功能登录 iDRAC 之前，请确保：
- 您已使用有效的 Active Directory 用户帐户登录到系统。
- 单点登录选项在 Active Directory 配置过程中已启用。

要使用 Web 界面登录 iDRAC：

1. 使用有效 Active Directory 帐户登录管理站。
2. 在 Web 浏览器中，键入 `https://[FQDN address]`。
   注: 如果默认 HTTPS 端口号（端口 443）已更改，请键入：`https://[FQDN address]:[port number]`，其中 `[FQDN address]` 是 iDRAC FQDN (iDRACdnsname.domain.name)，`[port number]` 是 HTTPS 端口号。
   注: 如果使用 IP 地址而不是 FQDN，SSO 将失败。

   iDRAC 使您以相应的 Microsoft Active Directory 权限登录，使用您通过有效 Active Directory 帐户登录时在操作系统中缓存的凭据。

使用 CMC Web 界面登录 iDRAC SSO

注: 此功能在 MX 平台上不可用。

使用 SSO 功能，可以从 CMC Web 界面启动 iDRAC Web 界面。CMC 用户从 CMC 启动 iDRAC 时具有 CMC 用户权限。如果用户帐户存在于 CMC 中而不存在于 iDRAC 中，该用户仍可从 CMC 启动 iDRAC。

如果禁用 iDRAC 网络 LAN（LAN 已启用 = 否），则 SSO 不可用。

如果服务器已从机箱中卸下、iDRAC IP 地址发生了变化、或 iDRAC 网络连接中存在问题，则 CMC Web 界面中的启动 iDRAC 选项 会变灰。

有关更多信息，请参阅 机箱管理控制器用户指南，*网址：*https://www.dell.com/cmcmanuals。

使用远程 RACADM 访问 iDRAC

您可以通过 RACADM 公用程序使用远程 RACADM 访问 iDRAC。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

如果管理站没有将 iDRAC 的 SSL 证书存储到其默认的证书存储中，当您运行 RACADM 命令时将显示警告信息。但是，该命令成功执行。

注: iDRAC 证书是 iDRAC 发送给 RACADM 客户端以建立安全会话的证书。此证书由 CA 颁发或为自签名证书。在任一情况下，如果管理站无法识别 CA 或签名机构，都将显示警告。

验证 CA 证书以在 Linux 上使用远程 RACADM

在运行远程 RACADM 命令之前，验证用于安全通信的 CA 证书。

要验证使用远程 RACADM 的证书：

1. 将 DER 格式的证书转换为 PEM 格式（使用 openssl 命令行工具）：

```
openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem -out
[outcertfileinpemformat.pem] -text
```

2. 在管理站上查找默认 CA 证书包的位置。例如，对于 RHEL5 64 位，该路径是 **/etc/pki/tls/cert.pem**。
3. 将 PEM 格式的 CA 证书附加到 Management Station CA 证书。
   例如，使用 `cat command: cat testcacert.pem >> cert.pem`
4. 生成服务器证书并将其上传到 iDRAC。

使用本地 RACADM 访问 iDRAC

有关使用本地 RACADM 访问 iDRAC 的信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用固件 RACADM 访问 iDRAC

您可以使用 SSH 界面访问 iDRAC 并运行固件 RACADM 命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

简单的双重身份验证（简单 2FA）

iDRAC 提供简单的双重身份验证选项，可增强本地用户登录的安全性。当您从不同于上次登录的源 IP 地址登录时，系统会提示您输入双重身份验证详细信息。

简单的双重身份验证有两个身份验证步骤：

- iDRAC 用户名和密码
- 简单的 6 位代码，可通过电子邮件发送给用户。用户需要在出现登录提示时输入此 6 位代码。

注:

- 要收到 6 位代码，必须配置“自定义发件人地址”并具有有效的 SMTP 配置。
- 2FA 代码会在 10 分钟后过期，或者如果在过期之前已使用，该代码将失效。
- 如果用户尝试使用不同的 IP 地址从另一位置登录，而原始 IP 地址的挂起 2FA 质询仍未完成，则将从新 IP 地址发送相同的令牌，以尝试登录。
- 在获得 iDRAC Enterprise 或 Datacenter 许可证后，此功能可用。

启用 2FA 时，不允许执行以下操作：

- 通过默认用户凭据使用 CLI 的任何用户界面登录到 iDRAC。
- 通过 Quick Sync-2 通过 OMM 应用程序登录 iDRAC
- 在 Group Manager 中添加成员 iDRAC。

注: Racadm、Redfish、WSMan、IPMI LAN、串行、来自源 IP 的 CLI □在从 iDRAC GUI、SSH 等支持的界面成功登□后才能工作。

RSA SecurID 2FA

您可将 iDRAC 配置为一次使用一个 RSA AM 服务器进行验证。RSA AM 服务器上的全局设置适用于所有 iDRAC 本地用户、AD 和 LDAP 用户。

注: □当具有 Datacenter □可□□ RSA SecurID 2FA 功能才可用。

在配置 iDRAC 以启用 RSA SecurID 之前，必须满足以下前提条件：

- 配置 Microsoft Active Directory 服务器。
- 如果您尝试在所有 AD 用户上启用 RSA SecurID，请将 AD 服务器作为身份源添加到 RSA AM 服务器。
- 确保您有通用 LDAP 服务器。
- 对于所有 LDAP 用户，必须在 RSA AM 服务器中添加到 LDAP 服务器的身份源。

要在 iDRAC 上启用 RSA SecurID，需要 RSA AM 服务器的以下属性：

1. **RSA 验证 API URL** — URL 语法为：`https://<rsa-am-server-hostname>:<port>/mfa/v1_1`，默认端口为 5555。
2. **RSA 客户端 ID** — 默认情况下，RSA 客户端 ID 与 RSA AM 服务器主机名相同。在 RSA AM 服务器的验证代理配置页面找到 RSA 客户端 ID。
3. **RSA 访问密码** — 导航至**设置** > **系统设置** > **RSA SecurID** > **验证 API** 部分，可以在 RSA AM 上检索到访问密码，通常显示为 `198cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302`。要通过 iDRAC GUI 配置设置，请执行以下操作：
   - 转至 **iDRAC 设置** > **用户**。
   - 在**本地用户**部分中，选择现有本地用户，然后单击**编辑**。
   - 向下滚动到“配置”页面底部。
   - 在 **RSA SecurID** 部分中，单击 **RSA SecurID 配置**的链接，以查看或编辑这些设置。

   您还可以按如下所示配置设置：
   - 转至 **iDRAC 设置** > **用户**。
   - 从**目录服务**部分，选择 **Microsoft Active 服务**或**通用 LDAP 目录服务**，然后单击**编辑**。
   - 在 **RSA SecurID** 部分中，单击 **RSA SecurID 配置**的链接，以查看或编辑这些设置。
4. **RSA AM 服务器证书（链）**

您可以通过 iDRAC GUI 和 SSH 使用 RSA SecurID 令牌登录 iDRAC。

RSA SecurID 令牌应用程序

您需要在系统或智能手机上安装 RSA SecurID 令牌应用程序。当您尝试登录 iDRAC 时，系统将要求您输入应用程序中显示的验证码。

如果输入了错误的验证码，RSA AM 服务器会要求用户提供“下一个令牌”。即使用户输入了正确的验证码，也可能会发生这种情况。此条目可证明用户拥有生成正确验证码的正确令牌。

您可以通过单击**选项**从 RSA SecurID 令牌应用程序获取**下一个令牌**。选中**下一个令牌**就可获得下一个验证码。在此步骤中，时间很关键。否则，iDRAC 对下一个令牌的验证可能会失败。如果 iDRAC 用户登录会话超时，则需要再次尝试登录

如果输入了错误的验证码，RSA AM 服务器会要求用户提供“下一个令牌”。即使用户输入了正确的验证码，也可能会发生这种情况。此条目可证明用户拥有生成正确验证码的正确令牌。

要从 RSA SecurID 令牌应用程序获取下一个令牌，请单击**选项**，然后选中**下一个令牌**。将生成新标记。在此步骤中，时间很关键。否则，iDRAC 对下一个令牌的验证可能会失败。如果 iDRAC 用户登录会话超时，则需要再次尝试登录。

查看系统运行状况

在执行任务或触发事件之前，您可以使用 RACADM 以检查系统是否处于适当的状态。要从 RACADM 查看远程服务状态，请使用 `getremoteservicesstatus` 命令。

表. 6: 系统状态的可能值

主机系统	Lifecycle Controller (LC)	实时状态	整体状态
• 关机	• 就绪	• 就绪	• 就绪

表. 6: 系统状态的可能值 （续）

主机系统	Lifecycle Controller (LC)	实时状态	整体状态
• 在开机自检过程中 • 在开机自检完成后 • 收集系统资源清册 • 自动化任务执行 • Lifecycle Controller Unified Server Configurator • 服务器在 F1/F2 错误提示时暂停，因为 POST 错误 • 服务器在 F1/F2/F11 提示时暂停，因为无可用的引导设备 • 服务器已进入 F2 设置菜单 • 服务器已进入 F11 引导管理器菜单	• 未初始化 • 正在重新加载数据 • 已禁用 • 正在恢复 • 正在使用	• 未就绪	• 未就绪
1. 读/写：只读 2. 用户权限：登录用户 3. 所需的许可证：iDRAC Express 或 iDRAC Enterprise 4. 相关性：无			

使用公共密钥验证登录 iDRAC

您可以通过 SSH 登录 iDRAC，而不必输入密码。您也可以将单个 RACADM 命令作为命令行参数发送到 SSH 应用程序。命令行选项的效果就像远程 RACADM 一样，因为会话在命令完成之后结束。

例如：

登录：

```
ssh username@<domain>
```

或

```
ssh username@<IP_address>
```

其中，`IP_address` 是 iDRAC 的 IP 地址。

发送 RACADM 命令：

```
ssh username@<domain> racadm getversion
```

```
ssh username@<domain> racadm getsel
```

多个 iDRAC 会话

下表提供了可能使用各种界面的 iDRAC 会话数目。

表. 7: 多个 iDRAC 会话

界面	会话数
iDRAC Web 界面	8
远程 RACADM	4

表. 7: 多个 iDRAC 会话 （续）

界面	会话数
固件 RACADM	SSH - 4 串行 - 1

iDRAC 允许同一用户有多个会话。用户创建允许的最大会话数后，其他用户将无法登录到 iDRAC。这可能会导致合法管理员用户遇到*拒绝服务*。

如果出现会话耗尽，请执行以下补救措施：

- 如果基于 Web 服务器的会话耗尽，您仍可通过 SSH 或本地 RACADM 登录。
- 管理员随后可使用 racadm 命令（`racadm getssninfo`、`racadm closessn -i <index>`）终止现有会话。

安全默认密码

所有受支持的系统随附 iDRAC 的唯一默认密码，除非您在订购系统时选择将 *calvin* 设置为密码。唯一密码有助于提高 iDRAC 和服务器的安全性。要进一步提高安全性，建议您更改默认密码。

您系统的唯一密码在系统信息标签上可用。要找到标签，请参阅您服务器的说明文件，网址：https://www.dell.com/support。

注: 对于 PowerEdge C6420、M640 和 FC640，默认密码为 *calvin*。

注: 将 iDRAC 重设为出厂默认设置会将默认密码恢复为服务器随附的密码。

如果您忘记密码，并且不能访问系统信息标签，有几种方法在本地或远程重设密码。

在本地重设默认的 iDRAC 密码

如果您具有系统的物理访问权限，您可以使用以下内容重设密码：

- iDRAC 设置公用程序（系统设置程序）
- 本地 RACADM
- OpenManage Mobile
- 服务器管理 USB 端口
- USB - NIC

使用 iDRAC 设置公用程序重设默认密码

您可以使用您服务器的系统设置访问 iDRAC 设置公用程序。使用将 iDRAC 重设为默认所有功能，您可以将 iDRAC 登录凭据重设为默认值。

警告: 将 iDRAC 重设为默认全部，这将 iDRAC 重设为出厂默认值。

使用 iDRAC 设置公用程序重设 iDRAC：

1. 重新引导服务器并按下 <F2>。
2. 在**系统设置**页面，单击 **iDRAC 设置**。
3. 单击**将 iDRAC 配置重设为默认全部**。
4. 单击**是**以确认，然后单击**返回**。
5. 单击**完成**。

当所有 iDRAC 设置重设为默认设置后，重启服务器。

使用本地 RACADM 重设默认密码

1. 登录到该主机系统上安装的操作系统。
2. 访问本地 RACADM 接口。
3. 按照 使用 RACADM 更改系统将显示默认登录密码 页面上的 45 中的说明操作。

使用 OpenManage Mobile 重设默认密码

您可以使用 OpenManage Mobile (OMM) 登录并更改默认密码。要使用 OMM 登录 iDRAC，请扫描系统信息标签上的 QR 代码。有关使用 OMM 的更多信息，请参阅 适用于 PowerEdge MX7000 机箱的 *OME - Modular* 用户指南，网址：https://www.dell.com/openmanagemanuals 上的 OMM 说明文档。

注: 仅当默认凭据为默认值时，将 QR 代码日志扫描至 iDRAC。如果您已经将其从默认值进行更改，请输入更新凭据。

使用服务器管理 USB 端口重设默认密码

注: 这些步骤要求启用和配置 USB 管理端口。

使用服务器配置文件的文件

创建服务器配置文件 (SCP) 文件（具有默认帐户的新 密码），将其放置在内存密钥上，并且使用服务器上的服务器管理 USB 端口上传 SCP 文件。有关创建文件的更多信息，请参阅 使用 USB 端口进行服务器管理 页面上的 273。

使用膝上型计算机访问 iDRAC

将膝上型计算机连接至服务器管理 USB 端口并访问 iDRAC 以更改密码。有关更多信息，请参阅 通过直接 USB 连接访问 iDRAC 界面 页面上的 273。

使用 USB-NIC 更改默认密码

如果您拥有对键盘、鼠标和显示屏设备的访问权限，请使用 USB-NIC 连接到服务器以访问 iDRAC 界面并更改默认密码。

1. 将设备连接至系统。
2. 使用支持的浏览器以使用 iDRAC IP 访问 iDRAC 界面。
3. 按照 使用 Web 界面更改默认登录密码 页面上的 45 中的说明操作。

远程重设默认 iDRAC 密码

如果您没有对系统的物理访问权限，那么您可以远程重设默认密码。

远程 — 配置的系统

如果您已在系统上安装操作系统，请使用远程桌面客户端以登录到该服务器。您登录到服务器后，可使用任何本地界面（例如，RACADM 或 Web 界面）以更改密码。

远程 - 未配置的系统

如果服务器上没有安装操作系统，并且 PXE 设置可用，请使用 PXE，然后使用 RACADM 以重设密码。

更改默认登录密码

在以下情况下，显示允许您更改默认密码的警告消息：

- 您以"配置用户"权限登录到 iDRAC。
- 默认密码警告功能已启用。
- 默认 iDRAC 用户名和密码与系统信息标签一起提供。

在您使用 SSH、远程 RACADM 或 Web 界面登录到 iDRAC 时，还会显示警告消息。对于 Web 界面、SSH，系统会为每个会话显示一条警告消息。而对于远程 RACADM，系统则会为每个命令显示该警告消息。

注: 有关□□用□名和密□的建□字符的信息，□参□ 建议使用的用户名和密码字符 □面上的 135。

使用 Web 界面更改默认登录密码

当您登录 iDRAC Web 界面时，如果显示 **Default Password Warning（默认密码警告）**页面，您可以更改密码。要执行此操作：

1. 选择 **Change Default Password**（更改默认密码）选项。
2. 在 **New Password**（新密码）字段中，输入新密码。

   注: 有关用户名和密码的建议字符信息，请参阅 建议使用的用户名和密码字符 页面上的 135。

3. 在 **Confirm Password**（确认密码）字段中，再次输入密码。
4. 单击 **继续**。

   新密码即得以配置，并同时使您登录 DRAC。

   注: 只有在 **New Password**（新密码）和 **Confirm Password**（确认密码）字段匹配的情况下，**Continue**（继续）才处于启用状态。

   有关其他字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 更改系统将显示默认登录密码

要更改密码，请运行以下 RACADM 命令：

```
racadm set iDRAC.Users.<index>.Password <Password>
```

其中，`<index>` 是从 1 至 16 的值（代表用户帐户），`<password>` 是新的用户定义的密码。

注: 默认帐户的索引是 2。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

注: 有关针对用户名和密码的建议字符的信息，请参阅 建议使用的用户名和密码字符 页面上的 135。

使用 iDRAC 设置公用程序更改默认登录密码

要使用 iDRAC 设置公用程序更改默认登录密码，请执行以下操作：

1. 在 iDRAC 设置公用程序中，转至 **User Configuration**（用户配置）。
   随即会打开 **iDRAC Settings User Configuration（iDRAC 设置用户配置）**页面。
2. 在 **Change Password**（更改密码）字段中，输入新密码。

   注: 有关用户名和密码的建议字符信息，请参阅 建议使用的用户名和密码字符 页面上的 135。

3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   该详细信息即会保存。

启用或禁用默认密码警告消息

您可以启用或禁用默认密码警告消息的显示。要执行此操作，您必须拥有 Configure Users（配置用户）权限。

密码强度策略

您可以使用 iDRAC 界面来检查密码强度策略，并在不满足策略要求的情况下检查所有错误。密码策略无法应用于先前保存的密码、从其他服务器复制的服务器配置文件 (SCP) 以及配置文件中嵌入的密码。

如需访问“密码”设置，请转至 **iDRAC 设置** > **用户** > **密码设置**。

本部分中提供以下字段：

- **最低分数** — 指定最低密码强度策略分数。此字段中的值为：

- 0 — 无保护
- 1 — 弱保护
- 2 — 中保护
- 3 — 强保护

- **简单策略** — 指定安全密码中的所需字符。它包含以下选项：
  - 大写字母
  - 数字
  - 符号
  - 最小长度
- **正则表达式** — 使用正则表达式和最低分数强制实施密码策略。其值为 1-4。

IP 阻止

您可以使用 IP 阻止动态确定何时某个 IP 地址出现过多登录失败情况，并阻止或防止该 IP 地址在预先选定时间段登录 iDRAC9。IP 阻止包括：

- 允许登录失败的次数。
- 这些故障一定会发生的时间范围（以秒为单位）。
- 超出允许的总故障数后，阻止 IP 地址建立会话的时间（以秒为单位）。

随着特定 IP 地址连续登录失败次数的累积，累计次数将在内部计数器中跟踪。当用户成功登录后，失败历史记录将被清除，并且内部计数器将重置。

注: 如果来自客户端 IP 地址的连续登录尝试被拒绝，部分 SSH 客户端可能会显示以下信息：

```
ssh exchange identification: Connection closed by remote host
```

.

注: IP 阻止功能支持多达 5 个 IP 范围。您只能通过 RACADM 查看/设置这些项。

表. 8: 登录重试限制属性

属性	定义
`iDRAC.IPBlocking.BlockEnable`	启用 IP 阻止功能。当特定时间内遇到 `iDRAC.IPBlocking.FailCount` 单个 IP 地址出现连续故障时，`iDRAC.IPBlocking.FailWindow` 所有在某一时间段从该地址建立会话的后续尝试将被拒绝 `iDRAC.IPBlocking.PenaltyTime`
`iDRAC.IPBlocking.FailCount`	设置拒绝某个 IP 地址在登录尝试前允许登录失败的次数。
`iDRAC.IPBlocking.FailWindow`	计算失败尝试的时间（以秒为单位）。当失败在此时间段后出现时，将重置计数器。
`iDRAC.IPBlocking.PenaltyTime`	定义时间范围（以秒为单位），在该时间范围内拒绝失败次数过多的某个 IP 地址的登录尝试。

使用 Web 界面启用或禁用 OS 到 iDRAC 直通

要使用 Web 界面启用 OS 到 iDRAC 直通，请执行以下操作：

1. 转至 **iDRAC 设置** > **连接** > **网络** > **OS 到 iDRAC 直通**。
   此时将显示 **OS 到 iDRAC 直通**页面。
2. 将状态更改为**已启用**。
3. 为直通模式选择以下任何选项：
   - **LOM** — iDRAC 与主机操作系统之间的操作系统至 iDRAC 直通链接已通过 LOM 或 NDC 建立。
   - **USB NIC** — iDRAC 与主机操作系统之间的操作系统至 iDRAC 直通链接已通过内部 USB 总线建立。

   注: 如果您将直通模式设置为 LOM，请确保执行以下操作：
   - 操作系统和 iDRAC 位于同一子网内
   - 将网络设置中的 NIC 选择设置为 LOM
4. 如果在共享的 LOM 模式下连接了服务器，则**操作系统 IP 地址**字段将禁用。

   注: 如果已在 iDRAC 上启用 VLAN，则 LOM 直通将只在主机上配置了 VLAN 标记并且在共享 LOM 模式下有效。

   注:
   - 当将直通模式设置为 LOM 时，在冷启动后无法从主机操作系统启动 iDRAC。
   - 我们特意删除了使用专用模式功能的 LOM 直通。
5. 如果选择 **USB NIC** 作为直通配置，则输入 USB NIC 的 IP 地址。
   默认值是 169.254.1.1。建议使用默认 IP 地址。但是，如果此 IP 地址与主机系统或本地网络的其他接口的 IP 地址冲突，则必须更改此 IP 地址。

   请勿输入 169.254.0.3 和 169.254.0.4 这两个 IP 地址。这些 IP 地址是在使用 A/A 电缆时，为位于前面板上的 USB NIC 端口保留的。

   注: 如果首选 IPv6，则默认地址为 fde1:53ba:e9a0:de11::1。如果需要，可在 idrac.OS-BMC.UsbNicULA 设置中修改此地址。如果 USB NIC 上不需要 IPv6，则可以通过将地址更改为“::”来禁用它
6. 单击**应用**。
7. 单击**测试网络配置**以检查 IP 是否可访问，以及是否已在 iDRAC 和主机操作系统之间建立链接。

使用 RACADM 启用或禁用警报

使用以下命令：

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 — 已禁用

n=1 — 已启用

3

设置受管系统

如果您需要运行本地 RACADM 或启用上次崩溃屏幕捕获，请从 *Dell Systems Management Tools and Documentation* DVD 安装以下组件：

- 本地 RACADM
- 服务器管理员

有关 Server Administrator 的更多信息，请参阅 *OpenManage Server Administrator 用户指南，网址：*https://www.dell.com/openmanagemanuals。

主□：

设置 iDRAC IP 地址

您必须 根据 您的网络基础架构配置初始网络设置,以启用与 iDRAC 的通信。您可以使用下面的一种接口来设置 iDRAC IP 地址：

- iDRAC 设置公用程序
- Lifecycle Controller（请参阅 *生命周期控制器用户指南*）
- 机箱或服务器 LCD 面板（请参阅系统的 *安装和服务手册*）

  注: 在刀片服务器上，您可以通过使用机箱 LCD 面板配置网络设置仅在 CMC 初始配置期间。部署机箱后，您不能使用机箱 LCD 面板重新配置 iDRAC。
- CMC Web 界面（不适用于 MX 平台）（请参阅 *机箱管理控制器用户指南*）

对于机架式和塔式服务器，您可以设置 IP 地址，或使用默认的 iDRAC IP 地址 192.168.0.120 来配置初始网络设置，包括为 iDRAC 设置 DHCP 或静态 IP。

对于刀片服务器，默认情况下会禁用 iDRAC 网络界面。

当您配置了 iDRAC IP 地址之后：

- 请确保您更改默认用户名和密码。
- 通过以下任意界面访问 iDRAC：
  - 使用受支持的浏览器（Internet Explorer、Firefox、Chrome 或 Safari）的 iDRAC Web 界面
  - Secure Shell (SSH) - 需要如 Windows 上的 PuTTY 这样的客户端。默认情况下，SSH 可用于大多数 Linux 系统，因此无需客户端。
  - IPMITool（使用 IPMI 命令）或 Shell 提示符（在 Windows 或 Linux 中需要 Dell 定制安装程序，可以从 *Systems Management Documentation and Tools* DVD 或 https://www.dell.com/support 获得）

使用 iDRAC 设置公用程序设置 iDRAC IP

要设置 iDRAC IP 地址：

1. 打开受管系统。
2. 开机自测 (POST) 期间按 <F2>。
3. 在 **System Setup Main Menu（系统设置主菜单）**页面，单击 **iDRAC Settings（iDRAC 设置）**。
   随即会显示 **iDRAC Settings（iDRAC 设置）**页面。
4. 单击 **Network（网络）**。
   随即会显示**网络**页面。
5. 指定以下设置：
   - 网络设置
   - 常见设置
   - IPv4 设置
   - IPv6 设置
   - IPMI 设置
   - VLAN 设置
6. 依次单击**后退**、**完成**和**是**。
   网络信息即会保存并且系统会重新引导。

配置网络设置

要配置网络设置：

注: 有关各选项的信息，请参阅 *iDRAC 设置公用程序联机帮助*。

1. 在**启用 NIC** 下，选择**已启用**。
2. 根据网络需要，从 **NIC 选择**下拉菜单中，选择以下端口之一：

   注: 此选项在 MX 平台上不可用。

   - **专用**— 使远程访问设备能够利用远程访问控制器 (RAC) 上的专用网络接口。此接口并未与主机操作系统共享，并将管理流量分发到单独的物理网络，使其能够从应用程序流量中分离出来。

     此选项意味着 iDRAC 的专用网络端口单独路由其流量，与服务器的 LOM 或 NIC 端口分离。与分配给主机 LOM 或 NIC 以管理网络流量的 IP 地址相比，专用选项允许为 iDRAC 分配来自同一子网或不同子网的 IP 地址。

     注: 对于刀片服务器，“专用”选项将显示为**机箱（专用）**。
   - **LOM1**
   - **LOM2**
   - **LOM3**
   - **LOM4**

   注: 对于机架式和塔式服务器，根据服务器型号，可使用两个 LOM 选项（LOM1 和 LOM2）或者全部四个 LOM 选项。在具有两个 NDC 端口的刀片式服务器中，可使用两个 LOM 选项（LOM1 和 LOM2），在具有四个 NDC 端口的服务器上，全部四个 LOM 选项可用。

   注: 如果在有两个 NDC 的全高服务器中使用 LOM，则 *Intel 2P X520–k bNDC 10 G* 不支持共享 LOM，因为它们不支持硬件仲裁。

3. 在 **NIC 选择**下拉菜单中，选择要从中远程访问系统的端口，以下是选项内容：

   注: 此功能在 MX 平台上不可用。

   注: 您可以选择专用网络接口卡，也可以从四端口或双端口夹层卡中可用的 LOM 列表进行选择。

   - **机箱（专用）**：使远程访问设备能够使用远程访问控制器 (RAC) 上提供的专用网络接口。此接口并未与主机操作系统共享，并将管理流量分发到单独的物理网络，使其能够从应用程序流量中分离出来。

     此选项意味着 iDRAC 的专用网络端口单独路由其流量，与服务器的 LOM 或 NIC 端口分离。与分配给主机 LOM 或 NIC 以管理网络流量的 IP 地址相比，专用选项允许为 iDRAC 分配来自同一子网或不同子网的 IP 地址。
   - **适用于四端口卡 - LOM1-LOM16**
   - **适用于双端口卡 - LOM1、LOM2、LOM5、LOM6、LOM9、LOM10、LOM13、LOM14。**
4. 从**故障网络**下拉菜单中，选择剩余的 LOM 之一。如果网络发生故障，则流量通过故障转移网络进行路由。

例如，要在 LOM1 发生故障时通过 LOM2 来路由 iDRAC 网络流量，请对 **NIC 选择**选择 **LOM1**，对**故障转移网络**选择 **LOM2**。

注: 如果 **NIC 选择**设置为**专用**，则此选项被禁用。

注: 当使用**故障切换网络**设置时，建议将所有 LOM 端口连接到同一网络。

有关更多详细信息，请参阅部分 使用 Web 界面修改网络设置 页面上的 87

5. 如果 iDRAC 必须自动设置双工模式和网络速度，则在**自动协商**下，选择**打开**。
   此选项仅适用于专用模式。如果已启用，则 iDRAC 会基于网络速度将网络速度设置为 10、100 或 1000 Mbps。
6. 在**网络速度**下，选择 10 Mbps 或 100 Mbps。

   注: 您无法手动将网络速度设置为 1000 Mbps。此选项仅在**自动协商**选项已启用的情况下可用。

7. 在**双工模式**下，选择**半双工**或**全双工**选项。

   注: 如果**自动协商**设置为**启用**，则此选项被禁用。

   注: 如果使用与 NIC 选择相同的网络适配器为主机操作系统配置网络分组，则还应该配置故障转移网络。NIC 选择和故障转移网络应使用配置为网络组部分的端口。如果超过两个端口用作网络组的一部分，则故障切换网络选择应为“全部”。

8. 在 **NIC MTU** 下，输入 NIC 上的最大传输单元 (MTU) 大小。

   注: NIC 上的 MTU 的默认和最大限制为 1500，最小值为 576。如果启用了 IPv6，则要求 MTU 的值是 1280 或更高。

常见设置

如果网络基础架构有 DNS 服务器，请在 DNS 上注册 iDRAC。这些是高级功能的初始设置要求，例如目录服务（Active Directory 或 LDAP）、单一登录和智能卡等高级功能。

要注册 iDRAC：

1. 启用**向 DNS 注册 DRAC。**
2. 输入 **DNS DRAC 名称。**
3. 选择**自动配置域名**自动从 DHCP 获取域名。否则，提供 **DNS 域名。**
   对于 **DNS iDRAC 名称**字段，默认名称格式是 *idrac-Service_Tag*，其中 Service_Tag 是服务器的服务标签。最大长度为 63 个字符，并且支持以下字符：
   - A-Z
   - a-z
   - 0-9
   - 连字符 (-)

配置 IPv4 设置

配置 IPv4 设置：

1. 在 **Enable IPv4（启用 IPv4）**下选择 **Enabled（启用）**选项。

   注: 在第 14 代 PowerEdge 服务器中，DHCP 默认已启用。

2. 在 **Enable DHCP（启用 DHCP）** 下选择 **Enabled（启用）**选项，以便 DHCP 能够将 IP 地址、网关和子网掩码自动分配给 iDRAC。否则，请选择 **Disabled（禁用）**并输入以下各项的值：
   - 静态 IP 地址
   - 静态网关
   - 静态子网掩码
3. （可选），启用 **Use DHCP to obtain DNS server address（使用 DHCP 获取 DNS 服务器地址）**，以便 DHCP 服务器可以分配 **Static Preferred DNS Server（静态首选 DNS 服务器）**和 **Static Alternate DNS Server（静态备用 DNS 服务**

器）。否则，输入 **Static Preferred DNS Server（静态首选 DNS 服务器）** 和 **Static Alternate DNS Server（静态备用 DNS 服务器）**的 IP 地址。

配置 IPv6 设置

基于基础架构设置，您可以使用 IPv6 地址协议。

配置 IPv6 设置：

注: 如果 IPv6 设置为“静态”，请确保手动配置 IPv6 网关（在动态 IPv6 情况下不需要）。对于静态 IPV6，如果无法手动配置，将导致通信中断。

1. 在**启用 IPv6** 下选择**启用**选项。
2. 为了让 DHCPv6 服务器自动向 iDRAC 分配 IP 地址、网关和子网掩码，可选择**启用自动配置**下的**启用**选项。

   注: 您可同时配置静态 IP 和 DHCP IP。

3. 在**静态 IP 地址 1** 框中，输入静态 IPv6 地址。
4. 在**前缀长度**框中，输入 0 和 128 之间的值。
5. 在**网关**框中，输入网关地址。

   注: 如果您配置静态 IP，则当前 IP 地址 1 显示为静态 IP，且 IP 地址 2 显示为动态 IP。如果您清除静态 IP 设置，则当前 IP 地址 1 会显示动态 IP。

6. 如果使用 DHCP，启用**使用 DHCPv6 获取 DNS 服务器地址**从 DHCPv6 服务器获取主要 DNS 服务器和次要 DNS 服务器地址。如果需要，可进行以下配置：
   - 在**静态首选 DNS 服务器**框中，输入静态 DNS 服务器 IPv6 地址。
   - 在**静态备用 DNS 服务器**框中，输入静态备用 DNS 服务器。

配置 IPMI 设置

启用 IPMI 设置：

1. 在 **Enable IPMI Over LAN（启用 LAN 上 IPMI）**下，选择 **Enabled（启用）**。
2. 在 **Channel Privilege Limit（信道权限限制）**下，选择 **Administrator（管理员）**、**Operator（操作员）**或 **User（用户）**。
3. 在 **Encryption Key（加密密钥）**框中，输入格式为 0 到 40 个十六进制字符（不带任何空白字符）的加密密钥。默认值为全零。

VLAN 设置

可以将 iDRAC 配置入 VLAN 基础结构。要配置 VLAN 设置，请执行以下步骤：

注: 在设置为**机箱（专用）**的刀片服务器上，VLAN 设置是只读的，只能使用 CMC 进行更改。如果是在共享模式下设置服务器，则可以在 iDRAC 中的共享模式下配置 VLAN 设置。

1. 在**启用 VLAN ID** 下，选择**启用**。
2. 在 **VLAN ID** 框中，输入一个有效的数字（从 1 到 4094）。
3. 在**优先级**框中，输入一个间于 0 到 7 之间的数字以设置 VLAN ID 的优先级。

   注: 启用 VLAN 之后，iDRAC IP 在一段时间内不可访问。

使用 CMC Web 界面设置 iDRAC IP

要使用 Chassis Management Controller (CMC) Web 界面设置 iDRAC IP 地址：

注: 必须具有机箱配置管理员权限才能从 CMC 设置 iDRAC 网络设置。CMC 选项仅适用于刀片服务器。

1. 登录 CMC Web 界面。
2. 转至 **iDRAC 设置设置 CMC**。

随即会显示**部署 iDRAC** 页面。

3. 在 **iDRAC 网络设置**中，根据要求选择**启用 LAN** 以及其他网络参数。有关更多信息，请参阅 *CMC online help*（CMC 联机帮助）。
4. 有关特定于各刀片服务器的附加网络设置，请转至**服务器概述<server name>**。
   随即会显示**服务器状态**页面。
5. 单击**启动 iDRAC** 并转至 **iDRAC 设置连接性网络**。
6. 在**网络**页面中，指定下列设置：
   - 网络设置
   - 常见设置
   - IPv4 设置
   - IPv6 设置
   - IPMI 设置
   - VLAN 设置
   - 高级网络设置

   注: 有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
7. 要保存网络信息，请单击**应用**。
   有关更多信息，请参阅 机箱管理控制器用户指南，*网址：*https://www.dell.com/cmcmanuals。

自动查找

通过使用自动查找功能，新安装的服务器便可自动查找托管该配置服务器所在的远程管理控制台。配置服务器为 iDRAC 提供了自定义的管理用户凭据，以便查找未配置的服务器，并从管理控制台管理该服务器。有关调配服务器的更多信息，请参阅 *生命周期控制器远程服务快速入门指南，网址：*https://www.dell.com/idracmanuals。

配置服务器可结合静态 IP 地址使用。iDRAC 上的自动查找功能用于使用 DHCP/单播 DNS/mDNS 查找调配服务器。

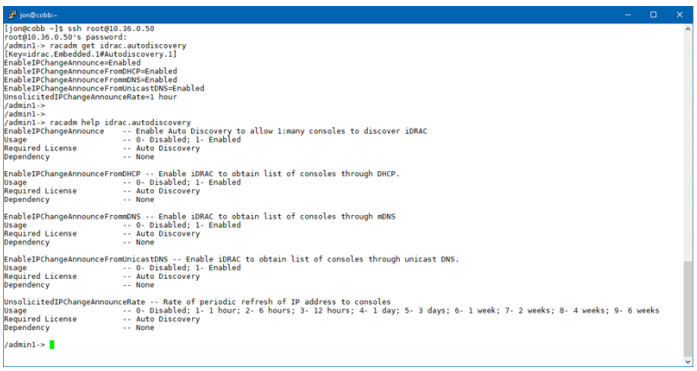
- 当 iDRAC 具有控制台地址时，它会发送自己的服务标签、IP 地址、Redfish 端口号、Web 证书等。
- 此信息会定期发布到控制台。

DHCP、DNS 服务器或默认的 DNS 主机名可查找配置服务器。如果指定了 DNS，将从 DNS 检索配置服务器 IP，无需进行 DHCP 设置。如果指定了配置服务器，则将跳过查找，因此 DHCP 和 DNS 均无需设置。

可以通过以下方式启用自动查找：

1. 使用 iDRAC GUI：**iDRAC 设置** > **连接性** > **iDRAC 自动查找**

2. 使用 RACADM：


jon@cobb:~
[jon@cobb ~]$ ssh root@10.36.0.50
root@10.36.0.50's password:
/admin1-> racadm get idrac.autodiscovery
[Key=idrac.Embedded.1#Autodiscovery.1]
EnableIPChangeAnnounce=Enabled
EnableIPChangeAnnounceFromDHCP=Enabled
EnableIPChangeAnnounceFrommDNS=Enabled
EnableIPChangeAnnounceFromUnicastDNS=Enabled
UnsolicitedIPChangeAnnounceRate=1 hour
/admin1->
/admin1->
/admin1-> racadm help idrac.autodiscovery
EnableIPChangeAnnounce -- Enable Auto Discovery to allow 1:many consoles to discover iDRAC
Usage -- 0- Disabled; 1- Enabled
Required License -- Auto Discovery
Dependency -- None
EnableIPChangeAnnounceFromDHCP -- Enable iDRAC to obtain list of consoles through DHCP.
Usage -- 0- Disabled; 1- Enabled
Required License -- Auto Discovery
Dependency -- None
EnableIPChangeAnnounceFrommDNS -- Enable iDRAC to obtain list of consoles through mDNS
Usage -- 0- Disabled; 1- Enabled
Required License -- Auto Discovery
Dependency -- None
EnableIPChangeAnnounceFromUnicastDNS -- Enable iDRAC to obtain list of consoles through unicast DNS.
Usage -- 0- Disabled; 1- Enabled
Required License -- Auto Discovery
Dependency -- None
UnsolicitedIPChangeAnnounceRate -- Rate of periodic refresh of IP address to consoles
Usage -- 0- Disabled; 1- 1 hour; 2- 6 hours; 3- 12 hours; 4- 1 day; 5- 3 days; 6- 1 week; 7- 2 weeks; 8- 4 weeks; 9- 6 weeks
Required License -- Auto Discovery
Dependency -- None
/admin1->
/admin1->

要使用 iDRAC 设置公用程序启用配置服务器，请执行以下操作：

1. 打开受管系统。
2. 在开机自检过程中，按 F2，然后转至 **iDRAC 设置** > **远程启用**。
   将显示 **iDRAC 设置远程启用**页面。
3. 启用自动查找，输入配置服务器 IP 地址，然后单击**上一步**。

   注: 指定配置服务器 IP 是可选的。如果没有设置，将使用 DHCP 或 DNS 设置进行查找（步骤 7）。

4. 单击**网络**。
   将显示 **iDRAC 设置网络**页面。
5. 启用 NIC。
6. 启用 IPv4。

   注: 自动查找不支持 IPv6。

7. 启用 DHCP 并从 DHCP 获取域名、DNS 服务器地址和 DNS 域名。

   注: 如果配置服务器 IP 地址（步骤 3）已提供，则步骤 7 是可选的。

使用自动配置功能配置服务器和服务器组件

自动配置功能可以在单次操作中配置一台服务器中的所有组件。这些组件包括 BIOS、iDRAC 和 PERC。自动配置功能通过自动导入包含所有可配置参数的服务器配置文件 (SCP) XML 或 JSON 文件。负责分配 IP 地址的 DHCP 服务器也提供了访问该 SCP 文件的详细信息。

通过配置一台“黄金配置”服务器创建 SCP 文件。将该配置导出至共享 NFS、CIFS、HTTP 或 HTTPS 网络位置，此位置可通过 DHCP 服务器以及所配置服务器的 iDRAC 访问。SCP 文件名可基于目标服务器的服务标签或型号，也可以为其指定通用名称。DHCP 服务器使用 DHCP 服务器选项指定该 SCP 文件名称（可选）、SCP 文件位置以及访问该文件位置的用户凭据。

当 iDRAC 从已进行自动配置的 DHCP 服务器获取 IP 地址时， iDRAC 将使用 SCP 来配置服务器的设备。只有在 iDRAC 从 DHCP 服务器获取其 IP 地址后，才会调用自动配置。如果未收到来自 DHCP 服务器的响应或 IP 地址，则不会调用自动配置。

HTTP 和 HTTPS 文件共享选项受 iDRAC 固件 3.00.00.00 或更高版本支持。需要提供 HTTP 或 HTTPS 地址的详细信息。如果在服务器上已启用代理，则用户需要提供进一步的代理设置以允许 HTTP 或 HTTPS 传输 信息。`-s` 选项标志更新为：

表. 9: 不同的共享类型和 pass in 值

-s (ShareType)	pass in
NFS	0 或 nfs
CIFS	2 或 cifs
HTTP	5 或 http
HTTPS	6 或 https

注: 自□配置不支持 HTTPS □□。自□配置忽略□□警告。

以下列表介绍了用于传递字符串值的必需和可选参数：

`-f (Filename)`：已导出的服务器配置配置文件的名称。对于 2.20.20.20 之前的 iDRAC 固件版本，这是必填字段。

`-n (Sharename)`：网络共享的名称。这是 NFS 或 CIFS 所需。

`-s (ShareType)`：对于 NFS 传递 0，对于 CIFS 传递 2，对于 HTTP 传递 5，对于 HTTPS 传递 6。这是 iDRAC 固件版本 3.00.00.00 的必填字段。

`-i (IPAddress)`：网络共享的 IP 地址。这是必填字段。

`-u (Username)`：用户名可以访问网络共享。这是 CIFS 的必填字段。

`-p (Password)`:用户密码可以访问网络共享。这是 CIFS 的必填字段。

`-d (ShutdownType)`：0 表示正常关机，1 表示强制关机（默认设置：0）。这是可选字段。

`-t (Timetowait)`：等待主机关闭的时间（默认设置：300）。这是可选字段。

`-e (EndHostPowerState)`：0 表示关闭，1 表示打开（默认设置：1）。这是可选字段。

在 iDRAC 固件 3.00.00.00 或更高版本中支持附加选项标志，以启用 HTTP 代理参数的配置并设置访问配置文件的重试超时：

`-pd (ProxyDefault)`：使用默认的代理设置。这是可选字段。

`-pt (ProxyType)`：用户可以传递 `http` 或 `socks`（默认设置 http）。这是可选字段。

`-ph (ProxyHost)`：代理主机的 IP 地址。这是可选字段。

`-pu (ProxyUserName)`：有权访问代理服务器的用户名。对于代理支持，这是必填字段。

`-pp (ProxyPassword)`：有权访问代理服务器的用户密码。对于代理支持，这是必填字段。

`-po (ProxyPort)`：代理服务器的端口（默认设置是 80）。这是可选字段。

`-to (Timeout)`：指定用于获取配置文件的重试超时（以分钟为单位）（默认值为 60 分钟）。

对于 iDRAC 固件 3.00.00.00 或更高版本，支持 JSON 格式配置文件。如果"文件名"参数不存在，则会使用以下文件名：

- <服务标签>-config.xml，示例：CDVH7R1-config.xml
- <型号>-config.xml，示例：R640-config.xml
- config.xml
- <服务标签>-config.json，示例：CDVH7R1-config.json
- <型号>-config.json，示例：R630-config.json
- config.json

注： 有关 HTTP 的更多信息可以在 *14G Support for HTTP and HTTPS across IDRAC9 with Lifecycle Controller Interfaces*（HTTP 和 HTTPS 的跨 IDRAC9 with Lifecycle Controller Interface 的第 14 代支持）白皮□中找到，网址□ https://www.dell.com/support。

注：

- 仅当已启用 **DHCPv4** 和 **Enable IPV4** 选项时，才能启用"自动配置"。
- 自动配置功能和自动查找功能相互排斥。要正常运行自动配置功能，必须禁用自动查找。
- 服务器执行"自动配置"操作后，将会禁用"自动配置"功能。

如果 DHCP 服务器池中的所有 Dell PowerEdge 服务器具有相同的型号类型和编号，则需要使用一个 SCP 文件 (`config.xml`)。`config.xml` 文件名用作默认 SCP 文件名。除了 `.xml` 文件之外，`. json` 文件也可以与第 14 代系统搭配使用。文件可以是 `config.json`。

用户可以使用服务器的服务标签或服务器型号，来配置需要映射不同配置文件的单独服务器。对于具有不同服务器且这些服务器具有特定要求的环境，可以使用不同的 SCP 文件名来区分各服务器或服务器类型。举个例子，如果要配置这两个型号的服务器 - PowerEdge R740s 和 PowerEdge R540s，可以使用 `R740-config.xml` 和 `R540-config.xml` 这两个 SCP 文件。

注： iDRAC 服□器配置代理会使用服□器的服□□□、型号或者默□文件名 `config.xml`，来自□生成配置文件名。

注： 如果网□共享上没有其中的任何文件，服□器配置文件□入作□将被□□□故障，原因是找不到文件。

自动配置顺序

1. 创建或修改用于配置 Dell 服务器属性的 SCP 文件。
2. 将此 SCP 文件放置在一个共享位置，该共享位置可由 DHCP 服务器以及所有已通过 DHCP 服务器分配 IP 地址的 Dell 服务器访问。
3. 在 DHCP 服务器的供应商选项 43 字段中指定此 SCP 文件位置。
4. 获取 IP 地址时，iDRAC 将公布供应商类标识符。（选项 60）
5. DHCP 服务器将供应商类与 `dhcpd.conf` 文件中的供应商选项进行匹配，并向 iDRAC 发送 SCP 文件位置和 SCP 文件名称（如有指定）。
6. iDRAC 将处理 SCP 文件并配置该文件中列出的所有属性。

DHCP 选项

DHCPv4 允许将许多全局定义的参数传递到 DHCP 客户端。每个参数作为一个 DHCP 选项。每个选项通过一个选项标签（即 1 字节值）标识。选项标签 0 和 255 将保留，分别用于填充和结束选项。所有其他值都可用于定义选项。

DHCP 选项 43 用于从 DHCP 服务器将信息发送给 DHCP 客户端。此选项已定义为一个文本字符串。此文本字符串设置为包含 SCP 文件名、共享位置和用于访问位置的凭据的值。例如：

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.255.0 {
# default gateway
        option routers 192.168.0.1;
    option subnet-mask 255.255.255.0;
    option nis-domain  "domain.org";
    option domain-name "domain.org";
    option domain-name-servers 192.168.1.1;
    option time-offset -18000; #Eastern Standard Time
    option vendor-class-identifier "iDRAC";
    set vendor-string = option vendor-class-identifier;
    option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s
2 -d 0 -t 500";
```

其中，-i 为远程文件共享的位置，-f 为字符串格式的文件名和远程文件共享的凭据。

DHCP 选项 60 可识别和关联特定供应商的 DHCP 客户端。配置为基于客户端的供应商 ID 采取操作的任何 DHCP 服务器均应配置选项 60 和选项 43。使用 Dell PowerEdge 服务器时，iDRAC 可通过以下供应商 ID 进行识别：*iDRAC*。因此，您必须添加一个新的“供应商类别”并在其下针对“代码 60”创建一个“范围选项”，然后为 DHCP 服务器启用新的范围选项。

在 Windows 上配置选项 43

要在 Windows 上配置选项 43，请执行以下操作：

1. 在 DHCP 服务器上，转至 **Start（开始）** > **Administration Tools（管理工具）** > **DHCP**，以打开 DHCP 服务器管理工具。
2. 找到服务器并展开其下的所有项目。
3. 右键单击 **Scope Options**（范围选项）并选择 **Configure Options**（配置选项）。
   此时将显示 **Scope Options**（范围选项）对话框。
4. 向下滚动并选择 **043 Vendor Specific Info**（043 供应商特定信息）。
5. 在 **Data Entry（数据输入）**字段中，单击 **ASCII** 下方区域内的任意位置，然后输入具有共享位置（其中包含 SCP 文件）的服务器的 IP 地址。
   当您在 **ASCII** 下键入值时，将显示所键入的值，不过该值也会以二进制形式显示在左侧。
6. 单击 **OK**（确定）保存配置。

在 Windows 上配置选项 60

要在 Windows 上配置选项 60，请执行以下操作：

1. 在 DHCP 服务器上，转至**开始** > **管理工具** > **DHCP** 以打开 DHCP 服务器管理工具。
2. 查找服务器并展开其下的项目。
3. 右键单击 **IPv4** 并选择 **Define Vendor Classes（定义供应商类）**。
4. 单击**添加**。
   随即将显示包含以下字段的对话框：
   - **显示名称：**
   - **说明：**
   - **ID: 二进制: ASCII:**
5. 在**显示名称：**字段中，键入 `iDRAC`。
6. 在**说明：**字段中，键入供应商类。
7. 单击 **ASCII:** 部分并键入 `iDRAC`。
8. 单击**确定**，然后单击**关闭**。
9. 在 DHCP 窗口中，右键单击 **IPv4** 并选择 **Set Predefined Options（设置预定义选项）**。
10. 在**选项类**下拉式菜单中，选择 **iDRAC**（已在步骤 4 中创建），然后单击 **添加**。
11. 在**选项类型**对话框中，输入以下信息：
    - **名称** - `iDRAC`
    - **数据类型** - 字符串
    - **代码** - 060
    - **说明** - Dell 供应商类标识符

12. 单击**确定**两次，以返回 **DHCP** 窗口。
13. 展开服务器名称下的所有项目，右键单击**范围选项**，然后选择**配置选项**。
14. 单击**高级**选项卡。
15. 通过 **Vendor class（供应商类）**下拉菜单，选择 **iDRAC**。`060 iDRAC` 将显示在 **Available Options（可用选项）**列中。
16. 选择 **060 iDRAC** 选项。
17. 输入必须发送到 iDRAC 的字符串值（以及标准 DHCP 提供的 IP 地址）。该字符串值可帮助导入正确的 SCP 文件。
    有关该选项的 **DATA 条目、字符串值**设置，请使用具有以下字母选项和值的文本参数：
    - `Filename (-f)` — 表示导出的服务器配置文件 (SCP) 的名称。
    - `Sharename (-n)` — 指示网络共享的名称。
    - `ShareType (-s)` —

      除了支持基于 NFS 和 CIFS 的文件共享，iDRAC 固件 3.00.00.00 或更高版本还支持通过使用 HTTP 或 HTTPS 访问配置文件。`-s option` 标志更新为：

      `-s (ShareType)`：类型 nfs 或 0 适用于 NFS；cifs 或 2 适用于 CIFS；http 或 5 适用于 HTTP；https 或 6 适用于 HTTPS（强制）。
    - `IPAddress (-i)` — 指示文件共享的 IP 地址。

      注: `Sharename (-n)`、`ShareType (-s)` 和 `IPAddress (-i)` 是必须传递的必要属性。-n 不是 HTTP 或 HTTPs 所必需的。
    - `Username (-u)` — 指示访问网络共享所需的用户名。仅 CIFS 需要此信息。
    - `Password (-p)` — 指示访问网络共享所需的密码。仅 CIFS 需要此信息。
    - `ShutdownType (-d)` — 指示关机的模式。0 表示正常关机，1 表示强制关机。

      注: 默认设置为 0。
    - `Timetowait (-t)` — 指示主机系统关闭之前等待的时间。默认设置为 300。
    - `EndHostPowerState (-e)` — 指示主机的电源状态。0 表示关闭，1 表示打开。默认设置为 1。

      注: `ShutdownType (-d)`、`Timetowait (-t)` 和 `EndHostPowerState (-e)` 是可选的属性。

    NFS: -f system_config.xml -i 192.168.1.101 -n /nfs_share -s 0 -d 1
    CIFS: -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u *<USERNAME>* -p *<PASSWORD>* -d 1 -t 400
    HTTP: -f system_config.json -i 192.168.1.101 -s 5
    HTTP: -f http_share/system_config.xml -i 192.168.1.101 -s http
    HTTP: -f system_config.xml -i 192.168.1.101 -s http -n http_share
    HTTPS: -f system_config.json -i 192.168.1.101 -s https

在 Linux 上配置选项 43 和选项 60

更新 `/etc/dhcpd.conf` 文件。这些选项的配置步骤与 Windows 步骤相似：

1. 留出可由此 DHCP 服务器分配的地址块或地址池。
2. 设置选项 43，并为选项 60 使用名称供应商类标识符。

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.0.0  {
#default gateway
    option routers            192.168.0.1;
    option subnet-mask        255.255.255.0;
    option nis-domain        "domain.org";
    option domain-name        "domain.org";
    option domain-name-servers    192.168.1.1;
    option time-offset        -18000;    # Eastern Standard Time
    option vendor-class-identifier "iDRAC";
  set vendor-string = option vendor-class-identifier;
  option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d 0 -t 500";
    range dynamic-bootp 192.168.0.128 192.168.0.254;
    default-lease-time 21600;
    max-lease-time 43200;
        }
}
```

以下是供应商类标识符字符串中必须传递的必要参数和可选参数：

- 文件名 (-f) — 表示导出的服务器配置文件的名称。

注: 有关文件命名规则的更多信息，请参阅 使用自动配置功能配置服务器和服务器组件 页面上的 54。

- Sharename (-n) - 指示网络共享名称。
- ShareType (-s) — 指示共享类型。0 表示 NFS，2 表示 CIFS，5 表示 HTTP，6 表示 HTTPS。

  注: Linux NFS、CIFS、HTTP、HTTPS 共享示例：
  - **NFS**: `-f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500`

    确保为 NFS 网络共享使用 NFS2 或 NFS3。
  - **CIFS**: `-f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400`
  - **HTTP**: `-f system_config.xml -i 192.168.1.101 -s http -n http_share`
  - **HTTPS**: `-f system_config.json -i 192.168.1.101 -s https`
- IPAddress (-i) - 指示文件共享的 IP 地址。

  注: Sharename (-n)、ShareType (-s) 和 IPAddress (-i) 为必须传递的属性。-n 对于 HTTP 或 HTTPS 非必需。
- Username (-u) — 指示访问网络共享时所需的用户名。仅 CIFS 需要此信息。
- Password (-p) — 访问网络共享时所需的密码。仅 CIFS 需要此信息。
- ShutdownType (-d) — 指示关机的模式。0 表示正常关机，1 表示强制关机。

  注: 默认设置为 0。
- Timetowait (-t) - 指示主机系统关闭之前等待的时间。默认设置为 300。
- EndHostPowerState (-e) — 指示主机的电源状态。0 表示关闭，1 表示打开。默认设置为 1。

  注: ShutdownType (-d)、Timetowait (-t) 和 EndHostPowerState (-e) 为可选属性。

以下是从 dhcpd.conf 文件保留静态 DHCP 的示例：

```
host my_host {
host my_host {
hardware ethernet b8:2a:72:fb:e6:56;
fixed-address 192.168.0.211;
option host-name "my_host";
option myname " -f r630_raid.xml -i 192.168.0.1 -n /nfs -s 0 -d 0 -t 300";
}
```

注: 编辑 `dhcpd.conf` 文件后，确保重新启动 dhcpd 服务以应用更改。

启用自动配置的前提条件

在启用自动配置功能前，请确保已进行如下设置：

- 支持的网络共享（NFS、CIFS、HTTP 和 HTTPS）在与 iDRAC 和 DHCP 服务器相同的子网上提供。测试网络共享以确保它可通过防火墙并且用户权限设置正确。
- 服务器配置文件将导出到网络共享。此外还要确保 SCP 文件已进行必要的更改，以便在启动自动配置过程时可以应用正确的设置。
- 根据 iDRAC 的要求设置了 DHCP 服务器和更新了 DHCP 配置，以便调用服务器和启动自动配置功能。

使用 iDRAC Web 界面启用自动配置功能

确保已启用 DHCPv4 和 Enable IPv4（启用 IPv4）选项，并且已禁用自动查找功能。

要启用自动配置功能，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **Network（网络）** > **Auto Config（自动配置）**。
   随即会显示**网络**页面。
2. 在**自动配置**部分，从**启用 DHCP 配置**下拉菜单中选择下面的一个选项：
   - **Enable Once（启用一次）** — 仅使用 DHCP 服务器所引用的 SCP 文件来配置组件一次。此次配置后，将禁用自动配置。

- **Enable once after reset（在重设后启用一次）** — 在 iDRAC 重设后，仅使用 DHCP 服务器所引用的 SCP 文件来配置组件一次。此次配置后，将禁用自动配置。
- **禁用** — 禁用自动配置功能。

3. 单击**应用**可应用设置。
网络页面随之自动刷新。

使用 RACADM 启用自动配置功能

要使用 RACADM 启用自动配置功能，请使用 `iDRAC.NIC.AutoConfig` 对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

有关自动配置功能的更多信息，请参阅 https://www.dell.com/support 上提供的 *Zero-Touch, bare-metal server provisioning using the Dell EMC iDRAC with Lifecycle Controller Auto Config feature*（使用 Dell EMC iDRAC with Lifecycle Controller 的自动配置功能零接触配置裸机服务器配置）白皮书。

使用散列密码提供更高的安全性

在带 iDRAC 版本 3.00.00.00 的 PowerEdge 服务器上，您可以使用单向散列格式来设置用户密码和 BIOS 密码。用户的身份验证机制不会受到影响（SNMPv3 和 IPMI 除外），您可以提供纯文本格式的密码。

通过新的密码散列功能：

- 您可以生成您自己的 SHA256 散列值以设置 iDRAC 用户密码和 BIOS 密码。这允许您在服务器配置文件、RACADM 和 WSMan 中提供 SHA256 值。提供 SHA256 密码值时，您将无法通过 SNMPv3 和 IPMI 进行验证。
  注: 远程 RACADM 或 WSMan 或 Redfish 无法用于 iDRAC 的散列密码配置/更换。您可以使用 SCP 在远程 RACADM 或 WSMan 或 Redfish 上进行散列密码配置/更换。
- 您可以设置一个模板服务器，其中包括使用当前纯文本机制的所有 iDRAC 用户帐户和 BIOS 密码。服务器设置后，您可以导出具有密码哈希值的服务器配置文件。导出包括 SNMPv3 和 IPMI 认证所需的散列值。导入此配置文件后，必须使用最新的 Dell IPMI 工具，如果使用较旧版本的工具，则对于设置了散列密码值的用户，IPMI 身份验证将失败。
- 其他界面（例如 iDRAC GUI）将显示用户帐户已启用。

您可以使用 SHA256 生成包含和不包含 Salt 的散列密码。

您必须具有“服务器控制”权限才能包括和导出散列密码。

如果失去了对所有帐户的访问权限，请使用 iDRAC 设置公用程序或本地 RACADM 将 iDRAC 重设为默认任务。

如果仅使用 SHA256 密码散列设置 iDRAC 用户帐户的密码，而未使用其他散列（SHA1v3Key 或 MD5v3Key 或 IPMIKey），那么将无法通过 SNMP v3 和 IPMI 进行验证。

使用 RACADM 的散列密码

要设置散列密码，请将以下对象配合 `set` 命令使用：

- iDRAC.Users.SHA256Password
- iDRAC.Users.SHA256PasswordSalt

注: `SHA256Password` 和 `SHA256PasswordSalt` 字段为 XML 导入而保留，且不使用命令行工具进行设置。设置其中一个字段可能会导致当前用户无法登录 iDRAC。使用 `SHA256Password` 导入密码时，iDRAC 不会强制执行密码长度检查。

使用以下命令将散列密码包括在导出的服务器配置文件中：

```
racadm get -f <file name> -l <NFS / CIFS / HTTP / HTTPS share> -u <username> -p
<password>  -t <filetype> --includePH
```

设置关联的散列时，必须设置 Salt 属性。

注: 这些属性不适用于 INI 配置文件。

服务器配置文件中的散列密码

可以选择在服务器配置文件中导出新的散列密码。

当导入服务器配置文件时，您可以取消注释现有密码属性或新密码散列值属性。如果两个都已取消注释，则会生成的错误并且密码未设置。导入期间不得应用注释的属性。

不使用 SNMPv3 和 IPMI 验证生成散列密码

不使用 SNMPv3 和 IPMI 验证（加或不加盐）即可生成散列密码。两者都需要 SHA256。

要加盐生成散列密码：

1. 对于 iDRAC 用户帐户，必须使用 SHA256 对密码执行加盐操作。

   当您为密码加盐时，将会附加 16 字节二进制字符串。Salt 必须是 16 个字节的长度（如果提供）。一旦附加，它将成为 32 个字符的字符串。格式“密码”+“加盐”，例如：

   密码 = SOMEPASSWORD

   盐 = ALITTLEBITOFSALT—附加的 16 个字符

2. 打开 Linux 命令提示符并运行以下命令：

   ```
   Generate Hash-> echo-n SOMEPASSWORDALITTLEBITOFSALT|sha256sum  -><HASH>
   ```

   ```
   Generate Hex Representation of Salt -> echo -n ALITTLEBITOFSALT | xxd -p   -> <HEX-SALT>
   ```

   ```
   set iDRAC.Users.4.SHA256Password <HASH>
   ```

   ```
   set iDRAC.Users.4.SHA256PasswordSalt <HEX-SALT>
   ```

3. 在导入的服务器配置文件、RACADM 命令、Redfish 或 WAMAN 中提供散列值和加盐。

   注: 如果您希望清除一个先前加盐的密码，请确保密码加盐明确设置为空字符串，即，

   ```
   set iDRAC.Users.4.SHA256Password
   ca74e5fe75654735d3b8d04a7bdf5dcdd06f1c6c2a215171a24e5a9dcb28e7a2
   ```

   ```
   set iDRAC.Users.4.SHA256PasswordSalt
   ```

4. 设置密码之后，普通的纯文本密码验证仍然可以使用，但 SNMP v3 和 IPMI 验证不适用于具有使用散列算法进行更新的密码的 iDRAC 用户帐户。

修改本地管理员帐户设置

设置 iDRAC IP 地址后，您可以使用 iDRAC 设置公用程序修改本地管理员帐户设置（即用户 2）。要执行此操作：

1. 在 iDRAC 设置公用程序中，转至 **User Configuration**（用户配置）。
   随即会打开 **iDRAC Settings User Configuration（iDRAC 设置用户配置）**页面。
2. 指定**用户名**、**LAN 用户权限**、**串行端口用户权限**和**更改密码**的详细信息。
   有关各选项的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   本地管理员帐户设置即配置完成。

设置受管系统位置

您可以使用 iDRAC Web 界面或 iDRAC 设置公用程序指定数据中心中受管系统的位置详细信息。

使用 Web 界面设置受管系统位置

要指定系统位置详细信息：

1. 在 iDRAC Web 界面中，转至 **System（系统）** > **Details（详情）** > **System Details（系统详情）**。

随即显示 **System Details（系统详细信息）**页面。

2. 在 **System Location（系统位置）**下，输入数据中心中受管系统的位置详细信息。
   有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。系统位置详细信息将会保存到 iDRAC 中。

使用 RACADM 设置受管系统位置

要指定系统位置详细信息，请使用 `System.Location` 组对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序设置受管系统位置

要指定系统位置详细信息：

1. 在 iDRAC 设置公用程序中，转至 **System Location（系统位置）**。
   随即会显示 **iDRAC Settings System Location（iDRAC 设置系统位置）**。
2. 输入数据中心中受管系统的位置详细信息。有关各选项的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   该详细信息即会保存。

优化系统性能和功耗

冷却服务器所需的电力将显著占据整个系统电源。散热控制是系统冷却通过风扇速度和系统电源管理进行的有效管理，确保系统可靠运行，同时最大限度地降低系统功耗、通风和系统声音输出。您可以调整散热控制设置并根据系统性能和每瓦特性能要求进行优化。

使用 iDRAC Web 界面、RACADM 或 iDRAC 设置公用程序，您可以更改以下散热设置：

- 优化性能
- 优化最小功率
- 设置最大空气排放温度
- 如果需要，通过风扇偏移增加气流
- 通过提高最低风扇速度来增加气流

以下是散热管理中的功能列表：

- **系统气流消耗**：显示实时系统气流消耗（CFM 中），以便在机架和数据中心级别达到气流平衡。
- **自定义 Delta-T**：限制进气到排气的空气温度上升，调整基础架构级冷却性能。
- **排气温度控制**：指定空气排出服务器的温度限制，以便满足数据中心需要。
- **自定义 PCIe 入口温度**：选择正确的输入入口温度，以满足第三方设备要求。
- **PCIe 气流设置**：提供服务器的全面 PCIe 设备冷却视图，并允许对第三方卡进行冷却自定义。

使用 iDRAC Web 界面修改散热设置

要修改散热设置：

1. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **硬件设置** > **散热配置**。
2. 指定以下各项：
   - **散热配置文件优化** - 选择散热配置文件：
     - **默认的热量配置文件设置（最小功率）** - 意味着热量算法将使用**系统 BIOS** > **系统 BIOS 设置系统配置文件设置**页面下定义的相同“系统配置文件”设置。

     默认情况下，此选项设置为**默认的热量配置文件设置**。您也可选择独立于 BIOS 配置文件的自定义算法。可用选项有：
     - **最大性能（性能已优化）**：
       - 内存或 CPU 节流的可能性降低。
       - Turbo 模式激活的可能性提高。
       - 一般情况下，空闲和压力载荷下风扇速率较高。
     - **最小功率（每瓦性能已优化）**：

    - 根据最佳的风扇电源状态进行了优化以获得最低系统功耗。
    - 一般情况下，空闲和压力载荷下风扇速率较低。
  - **声音限制** — 声音限制可减少服务器的声音输出，但要以牺牲性能为代价。启用“声音限制”可能包括对占用的空间中的服务器临时进行部署或评估，但不要在基准测试或性能敏感性应用中使用。

  注: 选择**最大性能**或**最小功率**，将覆盖**系统 BIOS** > **系统 BIOS 设置.系统配置文件设置**页面“系统配置文件”设置的相关热量设置。
- **最大排气温度限制** — 从下拉菜单中，选择最大排气温度。这些值将根据系统显示。

  默认值为**默认值，70°C (158°F)**。

  此选项允许系统风扇速率变化，使得排气温度不超过所选的排气温度限制。由于取决于系统负载和系统的冷却能力，因此这并不能在所有的系统操作情况下始终得到保证。
- **风扇速率偏移** - 此选项为服务器提供额外的冷却能力。如果添加了硬件设备（例如，新的 PCIe 卡），则可能需要额外的冷却能力。风扇速率偏移会导致风扇速率比通过热量控制算法计算的基准风扇速率提高（偏移的百分比值）。可能的值包括：
  - **低风扇速率** — 将风扇速率提高到适度风扇速率。
  - **中等风扇速率** — 将风扇速率提高到接近中等。
  - **高风扇速率** — 将风扇速率提高到接近全速。
  - **最大风扇速率** — 将风扇速率提高到全速。
  - **关闭** - 风扇速率被设为关闭。这是默认值。如果设置为关闭，则不显示百分比。将使用没有任何偏移的默认风扇速率。相反，最大设置将使所有风扇以最大速率运行。

  风扇速率偏移是动态的，并且基于系统。每个偏移的风扇速率提高值会显示在每个选项旁边。

  风扇速率偏移会将所有风扇速率提高相同的百分比。根据单个组件冷却要求，风扇速率可能会提高到超过偏移速率。整体系统功耗预计会增加。

  风扇速率偏移允许您通过四个步进增量值提高系统风扇速率。这些步进值在服务器系统风扇的典型基准速率与最大速率之间平均划分。某些硬件配置会导致较高的基准风扇速率，进而导致获得最大速率的偏移不是最大偏移。

  最常见的使用案例是非标准 PCIe 适配器冷却。不过，该功能可用于提高针对其他目的的散热能力。

  注: 即使系统没有任何风扇，iDRAC 中也提供风扇配置设置。这是因为，iDRAC 会将指定的配置发送到机箱管理器，机箱管理器可以处理来自 iDRAC 的数据，并根据配置将所需的冷却发送到系统。
- **阈值**
  - **最大 PCIe 入口温度限制** - 默认值为 55°C。从需要较低入口温度的第三方 PCIe 卡中选择 45°C 的较低温度。
  - **排气温度限制** - 您可以通过修改以下值来设置排气温度限制：
    - **设置最大排气温度限制**
    - **设置空气温度上升限制**
  - **PWM 中的最低风扇速率（最大值的百分比）** - 选择此选项对风扇速率进行微调。通过此选项，您可以设置更高的基准系统风扇速率，或者如果其他自定义风扇速率选项无法达到所需的更高风扇速率，可以使用此选项来提高系统风扇速率。
    - **默认** - 根据系统散热算法将最小风扇速率设置为默认值。
    - **自定义** - 输入您要更改的风扇转速的百分比。范围是 9-100。

    最低风扇速率 PWM 所允许的范围根据系统配置的不同而有所变化。第一个值为空闲速度和第二个值是配置最大值（其可能是也可能不是完全基于系统配置）。

    系统风扇可以根据系统的散热要求，以高于此速率的速率运行，但不低于所定义的最低速率。例如，将“最小风扇速率”设置为 35% 将会限制风扇速率永远不会低于 35% PWM。

    注: 0% PWM 不表示风扇关闭。这是风扇可以达到的最低风扇速率。

这些设置是持久性的，意味着一旦进行设置并应用，它们将不会在系统重新引导、关机后再开机、iDRAC 或 BIOS 更新期间自动更改为默认设置。自定义散热选项可能并不在所有服务器上受支持。如果选项不受支持，将不会显示或者您无法提供自定义值。

3. 单击**应用**应用设置。

   系统将显示以下消息：

   ```
   It is recommended to reboot the system when a thermal profile change has been made. This is to ensure all power and thermal settings are activated.
   ```
4. 单击**稍后重新引导**或**立即重新引导**。

注: 必须重新引导系统以使设置生效。

使用 RACADM 修改散热设置

要修改散热设置，请将 **system.thermalsettings** 组中的对象与下表中提供的 **set** 子命令结合使用。

表. 10: 散热设置

对象	说明	使用情况	示例

AirExhaustTemp	用于设置最大排气温度限制。	设置为以下任何值（基于系统）：
		• 0 - 表示 40° C
		• 1 - 表示 45° C
		• 2 - 表示 50° C
		• 3 - 表示 55° C
		• 4 - 表示 60° C
		• 255 - 表示 70°C（默认）
			要检查系统中的现有设置：
			`racadm get system.thermalsettings.AirExhaustTemp`
			输出为：
			`AirExhaustTemp=70`
			该输出意味着系统已设置为将空气排放温度限制为 70°C。
			要设置排气温度以将其限制为 60°C：
			`racadm set system.thermalsettings.AirExhaustTemp 4`
			输出为：
			`Object value modified successfully.`
			如果系统不支持特定的空气排放温度限制，那么应该运行以下命令：
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			屏幕上将显示以下错误信息：
			`ERROR: RAC947: Invalid object value specified.`
			确保根据对象类型指定值。
			有关更多信息，请参阅 RACADM 帮助。
			要将限制设置为默认值：
			`racadm set system.thermalsettings.AirExhaustTemp 255`

FanSpeedHighOffsetVal	• 使用此变量将会以 %PWM 读取“高风扇速率偏移”设置的风扇速率偏移值。 • 此值取决于系统。	值为 0 - 100	`racadm get system.thermalsettings`

表. 10: 散热设置 （续）

对象	说明	使用情况	示例
	• 请使用 FanSpeedOffset 对象和索引值 1 来设置此值。		FanSpeedHighOffsetVal 此命令返回一个值，如“66”。这意味着在使用以下命令时，将会应用超过基准风扇速率的风扇速率偏移“高值” (66% PWM)。 racadm set system.thermalsettings FanSpeedOffset 1
FanSpeedLowOffsetVal	• 使用此变量将会以 %PWM 读取“低风扇速率偏移”设置的风扇速率偏移值。 • 此值取决于系统。 • 请使用 FanSpeedOffset 对象和索引值 0 来设置此值。	值为 0 - 100	racadm get system.thermalsettings FanSpeedLowOffsetVal 此命令返回一个值，如“23”。这意味着在使用以下命令时，将会应用超过基准风扇速率的风扇速率偏移“低值” (23% PWM)。 racadm set system.thermalsettings FanSpeedOffset 0
FanSpeedMaxOffsetVal	• 使用此变量将会以 %PWM 读取“最大风扇速率偏移”设置的风扇速率偏移值。 • 此值取决于系统。 • 请使用 FanSpeedOffset 对象和索引值 3 来设置此值。	值为 0 - 100	racadm get system.thermalsettings FanSpeedMaxOffsetVal 此命令返回一个值，如“100”。这意味着在使用以下命令时，将会应用最大风扇速率偏移（即全速，100% PWM）。通常，此偏移会导致风扇速率提高到全速。 racadm set system.thermalsettings FanSpeedOffset 3
FanSpeedMediumOffsetVal	• 使用此变量将会以 %PWM 读取“中等风扇速率偏移”设置的风扇速率偏移值。 • 此值取决于系统。 • 请使用 FanSpeedOffset 对象和索引值 2 来设置此值	值为 0 - 100	racadm get system.thermalsettings FanSpeedMediumOffsetVal 此命令返回一个值，如“47”。这意味着在使用以下命令时，将会应用超过基准风扇速率的

表. 10: 散热设置 （续）

对象	说明	使用情况	示例
			风扇速率偏移“中值”（47% PWM）。 `racadm set system.thermalsettings FanSpeedOffset 2`

`FanSpeedOffset`	• 使用此对象和 get 命令将会显示目前的风扇速率偏移值。
	• 将此对象与 set 命令配合使用，可以设置所需的风扇速率偏移值。
	• 索引值决定了所应用的偏移，`FanSpeedLowOffsetVal`、`FanSpeedMaxOffsetVal`、`FanSpeedHighOffsetVal` 和 `FanSpeedMediumOffsetVal` 对象（此前已定义）是所应用的偏移的值。
		值为：
		• 0 - 低风扇速率
		• 1 - 高风扇速率
		• 2 - 中等风扇速率
		• 3 - 最大风扇速率
		• 255 - 无
			要查看现有设置：
			`racadm get system.thermalsettings.FanSpeedOffset`
			要将风扇速率偏移设置为“高值”（如 `FanSpeedHighOffsetVal` 中所定义）
			`racadm set system.thermalsettings.FanSpeedOffset 1`

`MFSMaximumLimit`	读取 MFS 的最大值限制	值为 1 - 100	要显示可以使用 `MinimumFanSpeed` 选项设置的最大值： `racadm get system.thermalsettings.MFSMaximumLimit`
`MFSMinimumLimit`	读取 MFS 的最小值限制	值从 0 到 `MFSMaximumLimit` 默认值为 255（表示无）	要显示可以使用 `MinimumFanSpeed` 选项设置的最小值。 `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• 允许配置系统运行所需的最低风扇速率。 • 它定义风扇速率的基准（标准）值，并且系统允许风扇低于此定义的风扇速率值。 • 此值是风扇速率的 %PWM 值。	从 `MFSMinimumLimit` 到值 `MFSMaximumLimit` 如果 get 命令报告 255，则表明未应用用户配置的偏移。	要确保系统最低速度不会减少低于 45% PWM（45 必须是介于 `MFSMinimumLimit` 到 `MFSMaximumLimit` 之间的值）： `racadm set system.thermalsettings.MinimumFanSpeed 45`
`ThermalProfile`	• 允许指定“热量基本算法”。 • 允许您根据需要为配置文件关联的散热行为设置系统配置文件。	值： • 0 - 自动 • 1 - 最高性能 • 2 - 最低功耗	要查看现有的散热配置文件设置： `racadm get system.thermalsettings.ThermalProfile`

表. 10: 散热设置 （续）

对象	说明	使用情况	示例
			要将散热配置文件设置为“最高性能”： `racadm set system.thermalsettings.ThermalProfile 1`
`ThirdPartyPCIFanResponse`	• 第三方 PCI 卡的散热覆盖。 • 允许您启用或禁用检测到的第三方 PCI 卡的默认系统风扇响应。 • 您可以查看 Lifecycle Controller 日志中的消息 ID PCI3018，来确认是否存在第三方 PCI 卡。	值： • 1 - 启用 • 0 - 禁用 **注:** 默认值为 1。	要禁用任何默认的风扇速率响应设置，以支持检测到的第三方 PCI 卡： `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

使用 iDRAC 设置公用程序修改散热设置

要修改散热设置：

1. 在 iDRAC 设置公用程序中，转至 **Thermal（耐热）**。
   随即会显示 **iDRAC Settings Thermal（iDRAC 设置耐热）**页面。
2. 指定以下各项：
   - 热量配置文件
   - 最大排气温度限制
   - Fan Speed Offset（风扇速率偏移）
   - 最低风扇速率

   设置将永久存在，这表示一旦设置和应用它们，它们不会在系统重新引导、重新启动、iDRAC 或 BIOS 更新期间自动更改为默认设置。一些 Dell 服务器可能支持也可能不支持部分或所有的自定义用户冷却选项。如果不支持这些选项，它们将不会显示并且您也无法提供自定义值。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   耐热设置即配置完成。

使用 iDRAC Web 界面修改 PCIe 气流设置

自定义高功率 PCIe 卡需要提高热容限时，使用 PCIe 气流设置。

注: PCIe 气流设置在 MX 平台上不可用。

要修改 PCIe 气流设置：

1. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **硬件设置** > **散热配置**。
   PCIe 气流设置页面将显示在风扇设置部分下方。
2. 指定以下各项：
   - **LFM 模式** — 选择**自定义**模式以启用自定义 LFM 选项。
   - **自定义 LFM** — 输入 LFM 值。
3. 单击**应用**应用设置。

   系统将显示以下消息：

   ```
   It is recommended to reboot the system when a thermal profile change has been made. This is to ensure all power and thermal settings are activated.
   ```

   单击**稍后重新引导**或**立即重新引导**。

   注: 必须重新引导系统以使设置生效。

设置管理站

管理站是用于访问 iDRAC 界面的计算机，用于远程监测和管理 PowerEdge 服务器。

要设置管理站：

1. 安装受支持的操作系统。有关更多信息，请参阅发行说明。
2. 安装并配置一个支持的 Web 浏览器。有关更多信息，请参阅发行说明。
3. 安装最新的 Java Runtime Environment (JRE)（如果使用 Java 插件类型用来访问使用 Web 浏览器的 iDRAC，则需要）。

   注: 您需要 Java 8 或更高版本以使用此功能通过 IPv6 网络启动 iDRAC 虚拟控制台。

4. 从 *Dell Systems Management Tools and Documentation* DVD 中，从 SYSMGMT 文件夹安装远程 RACADM VMCLI。否则，运行 DVD 上的**设置**来通过默认和其他 OpenManage 软件安装远程 RACADM。有关 RACADM 的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。
5. 根据要求安装下列组件：
   - SSH 客户端
   - TFTP
   - Dell OpenManage Essentials

远程访问 iDRAC

要从管理站远程访问 iDRAC Web 界面，请确保管理站与 iDRAC 位于同一网络中。例如：

- 刀片服务器 - 管理站必须与 CMC 和 OME Modular 位于同一网络中。有关将 CMC 网络与受管系统的网络隔离的更多信息，请参阅 机箱管理控制器用户指南，*网址：* https://www.dell.com/cmcmanuals。
- 机架和塔式服务器 - 将 iDRAC NIC 设置为“专用”或 LOM1 并确保管理站与 iDRAC 位于同一网络中。

要从管理站访问受管系统的控制台，请通过 iDRAC Web 界面使用虚拟控制台。

配置支持的 Web 浏览器

注: 有关支持的浏览器及其版本的更多信息，请参阅 https://www.dell.com/idracmanuals 上提供的*发行说明*。

可以使用具有默认设置的浏览器访问 iDRAC Web 界面的大多数功能。要使用某些功能，您必须更改一些设置。这些设置包括禁用弹出窗口阻止程序、启用 Java、ActiveX 或 HTML5 插件支持等。

如果从通过代理服务器连接到 Internet 的 Management Station 连接到 iDRAC Web 界面，则需要配置 Web 浏览器以从该服务器访问 Internet。

注: 如果您使用 Internet Explorer 或 Firefox 以访问 iDRAC Web 界面，您可能需要根据本章节的描述配置特定设置。您可以使用其他受支持的浏览器及其默认设置。

注: 空代理设置被视为相当于无代理。

配置 Internet Explorer

本章节提供了有关配置 Internet Explorer (IE) 的详细信息，以确保您可以访问和使用 iDRAC Web 界面的所有功能。这些设置包括：

- 重新设置安全设置
- 将 iDRAC IP 添加至受信任的站点
- 配置 IE 以启用 Active Directory SSO
- 禁用 IE 增强的安全配置

重新设置 Internet Explorer 安全设置

确保 Internet Explorer (IE) 设置已设置为 Microsoft 推荐的默认设置且按照本章节介绍的内容自定义设置。

1. 以管理员身份打开 IE，或使用管理员帐户。
2. 单击**工具 Internet 选项 安全本地网络**或**本地局域网**。
3. 单击 **Custom Level（自定义级别）**，选择 **Medium-Low（中低级）**，单击 **Reset（重设）**。单击 **OK**（确定）以确认。

将 iDRAC IP 添加到受信任站点列表

访问 iDRAC Web 界面时，如果受信任域列表中缺少 iDRAC IP 地址，则系统会提示您将该 IP 地址添加到列表中。完成后，单击 **Refresh（刷新）**或重新启动 Web 浏览器以建立到 iDRAC Web 界面的连接。如果未提示您添加 IP，建议您手动将 IP 添加到受信任站点列表中。

注: 当连接至带有浏览器不信任证书的 iDRAC Web 界面时，在确认首次警告后，可能会再次显示浏览器证书错误警告。

要将 iDRAC IP 地址添加到受信任站点列表：

1. 单击 **Tools（工具）** > **Internet Options（Internet 选项）** > **Security（安全）** > **Trusted sites（受信任站点）** > **Sites（站点）**。
2. 在**将该网站添加到区域**中输入 iDRAC IP 地址。
3. 单击 **Add（添加）**，单击 **OK（确定）**，然后单击 **Close（关闭）**。
4. 单击 **OK（确定）**，然后刷新浏览器。

配置 Internet Explorer 以启用 Active Directory SSO

配置 Internet Explorer 的浏览器设置：

1. 在 Internet Explorer 中，导航至 **Local Intranet（本地 Intranet）**并单击 **Sites（站点）**。
2. 仅选择以下选项：
   - Include all local (intranet) sites not listed on other zones（包括没有列在其他区域的所有本地 [Intranet] 站点）。
   - Include all sites that bypass the proxy server（包括所有不使用代理服务器的站点）。
3. 单击 **Advanced（高级）**。
4. 添加所有将被用作 SSO 配置一部分的 iDRAC 实例的相关域名（例如，**myhost.example.com**）。
5. 单击 **Close（关闭）**并单击 **OK（确定）**两次。

禁用 Internet Explorer 增强的安全配置

为确保您可以使用 Web 界面下载日志文件和其他本地元素，建议从 Windows 禁用 Internet Explorer 增强的安全配置功能。有关禁用 Windows 版本上此功能的信息，请参阅 Microsoft 说明文件。

配置 Mozilla Firefox

本部分介绍有关配置 Firefox 的详细信息，以确保您可以访问和使用 iDRAC Web 界面上的所有功能。这些设置包括：

- 禁用白名单功能
- 配置 Firefox 以启用 Active Directory SSO

注: □于 iDRAC □机帮助□面，Mozilla Firefox □□器可能没有滚□条。

禁用 Firefox 中的白名单功能

Firefox 具有“白名单”安全功能，需要用户权限来为托管插件的每个独特站点安装插件。如果已启用，白名单功能会要求您为每个访问的 iDRAC 安装虚拟控制台查看器，即使查看器版本都相同。

要禁用白名单功能和避免安装不必要的插件，请执行下列步骤：

1. 打开 Firefox Web 浏览器窗口。
2. 在地址字段中，输入 `about:config` 并按 <Enter> 键。
3. 在 **Preference Name（首选项名称）**列中，找到并双击 **xpinstall.whitelist.required**。

   Preference Name（首选项名称）、**Status（状态）**、**Type（类型）**和 **Value （值）**的值会更改为粗体文本。**Status（状态）**的值将变成用户设置并且 **Value（值）**会变成 False。

4. 在 **Preferences Name（首选项名称）**列中，找到 **xpinstall.enabled**。
   确保 **Value（值）** 为 **True**。如果不是，双击 **xpinstall.enabled** 以将 **Value（值）**设置为 **True**。

配置 Firefox 以启用 Active Directory SSO

配置 Firefox 的浏览器设置：

1. 在 Firefox 地址栏中，输入 `about:config`。
2. 在 **Filter（过滤器）**中，输入 `network.negotiate`。
3. 将域名添加至 network.negotiate-auth.trusted-uris（使用逗号分隔的列表）。
4. 将域名添加至 network.negotiate-auth.delegation-uris（使用逗号分隔的列表）。

配置 Web 浏览器以使用虚拟控制台

要在管理站上使用虚拟控制台：

1. 确保已安装浏览器（Internet Explorer (Windows) 或 Mozilla Firefox（Windows 或 Linux）、Google Chrome、Safari）的支持版本。

   有关支持的浏览器版本的更多信息，请参阅 https://www.dell.com/idracmanuals 上提供的 *Release Notes*（发行说明）。

2. 要使用 Internet Explorer，请将 IE 设置为**以管理员身份运行。**
3. 配置 Web 浏览器以使用 ActiveX、Java 或 HTML5 插件。

   ActiveX Viewer 只受 Internet Explorer 支持。HTML5 或 Java 查看器在任何浏览器上都受支持。

   注: 您需要 Java 8 或更高版本以使用此功能通过 IPv6 网络启动 iDRAC 虚拟控制台。

4. 在受管系统上导入根证书，以免出现提示您验证证书的弹出式窗口。
5. 安装与 **compat-libstdc++-33-3.2.3-61** 相关的软件包。

   注: 在 Windows 上，与 `compat-libstdc++-33-3.2.3-61` 相关的软件包可能包含在 .NET 框架软件包或操作系统软件包中。

6. 如果您使用 MAC 操作系统，请选择 **Universal Access**（通用访问）窗口下的 **Enable access for assistive devices**（启用对辅助设备的访问）选项。
   有关更多信息，请参阅 MAC 操作系统说明文件。

配置 Internet Explorer 以使用基于 HTML 5 的插件

HTML5 虚拟控制台和虚拟介质 API 可通过使用 HTML5 技术来创建。HTML5 技术的优势如下：

- 不需要在客户端工作站上安装。
- 兼容性是基于浏览器而非操作系统或已安装的组件。
- 兼容大多数台式机和移动平台。
- 快速部署和客户端作为 Web 页面的一部分下载。

您必须先配置 Internet Explorer (IE) 设置，然后启动并运行基于 HTML5 的虚拟控制台和虚拟介质应用程序。要配置浏览器设置：

1. 禁用弹出窗口拦截程序。为此，可单击 **Tools（工具）** > **Internet Options（Internet 选项）** > **Privacy（隐私）**并清除 **Turn on Pop-up Blocker（打开弹出窗口拦截程序）**复选框。
2. 使用以下任何方法之一启动 HTML5 虚拟控制台：
   - 在 IE 中，单击 **Tools（工具）** > **Compatibility View Settings（兼容性视图设置）**并清除 **Display intranet sites in Compatibility View（在兼容性视图中显示内部网站点）**复选框。
   - 在 IE 中使用 IPv6 地址，按如下所示修改 IPv6 地址：

     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/ to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/
     ```

- 在 IE 中使用 IPv6 地址引导 HTML5 虚拟控制台，按如下所示修改 IPv6 地址：

```
https://[fe80::d267:e5ff:fef4:2fe9]/console to https://fe80--d267-e5ff-
fef4-2fe9.ipv6-literal.net/console
```

3. 要在 IE 浏览器中显示标题栏信息，可转到 **Control Panel（控制面板）** > **Appearance and Personalization（外观和个性化）** > **Personalization（个性化）** > **Windows Classic（Windows 经典）**

配置 Microsoft Edge 以使用基于 HTML5 的插件

您必须先配置 Edge 设置，然后才能启动和运行基于 HTML5 的虚拟控制台和虚拟介质应用程序。要配置浏览器设置：

1. 单击**设置** > **查看高级设置**并禁用**阻止弹出窗口**选项。
2. 按以下方式修改 IPv6 地址：

```
https://2607:f2b1:f083:147::1eb.ipv6:literal.net/restgui to https://2607-f2b1-
f083-147--1eb.ipv6-literal.net/restgui
```

配置 Web 浏览器以使用 Java 插件

如果您使用 Firefox 或 IE 并且想要使用 Java 查看器，请安装 Java Runtime Environment (JRE)。

注: 在 64 位操作系□上可安装 32 位或 64 位 JRE 版本，或在 32 位操作系□上可安装 32 位 JRE 版本。

要配置 IE 以使用 Java 插件：

- 在 Internet Explorer 中禁用文件下载的自动提示。
- 在 Internet Explorer 中禁用 *Enhanced Security Mode（增强的安全模式）*。

配置 IE 以使用 ActiveX 插件

您必须先配置 IE 浏览器设置，然后才能启动和运行基于 ActiveX 的虚拟控制台和虚拟介质应用程序。ActiveX 应用程序是作为签名的 CAB 文件从 iDRAC 服务器提供。如果在虚拟控制台中将插件类型设置为 Native-ActiveX 类型，则当您尝试启动虚拟控制台时，CAB 文件将下载到客户端系统并且基于 ActiveX 的虚拟控制台将启动。Internet Explorer 需要经过某些配置，才能下载、安装并运行基于这些 ActiveX 的应用程序。

在 64 位操作系统上，您可以安装 32 位或 64 位版本的 Internet Explorer。您可以使用 32 位或 64 位，但是您必须安装相应的插件。例如，如果您在 64 位浏览器上安装插件，然后在 32 位浏览器中打开查看器，那么您必须再次安装插件。

注: 您只可以将 ActiveX 插件与 Internet Explorer 一起使用。

注: 要在使用 Explorer 9 的系统上使用 ActiveX 插件，在配置 Internet Explorer 前，应确保在 Windows Server 操作系统中的 Internet Explorer 或服务器管理器中禁用增强的安全模式。

对于 Windows 7、Windows 2008 和 Windows 10 配置中的 ActiveX 应用程序，需配置下列 Internet Explorer 设置以使用 ActiveX 插件：

1. 清除浏览器的高速缓存。
2. 将 iDRAC IP 或主机名添加到 **Local Internet site（本地 Internet 站点）**列表。
3. 将自定义设置重置为 **Medium-low（中-低）**或更改设置以允许安装签名的 ActiveX 插件。
4. 支持浏览器下载加密的内容并启用第三方浏览器扩展。要进行此操作，请转至 **Tools（工具）** > **Internet Options（Internet 选项）** > **Advanced（高级）**，清除 **Do not save encrypted pages to disk（请勿将加密的页面保存到磁盘）**选项，然后选择 **Enable third-party browser extensions（启用第三方浏览器扩展名）**选项。

   注: 重新启动 Internet Explorer 以使 Enable third-party browser extensions（启用第三方浏览器扩展）设置生效。

5. 转至 **Tools（工具）** > **Internet Options（Internet 选项）** > **Security（安全）**并选择您要运行该应用程序的区域。
6. 单击 **Custom Level（自定义级别）**。在 **Security Settings（安全设置）**窗口中，执行下列操作：
   - 对 **Automatic prompting for ActiveX controls（ActiveX 控件自动提示）**选择 **Enable（启用）**。
   - 对 **Download signed ActiveX controls（下载已签名的 ActiveX 控件）**选择 **Prompt（提示）**。
   - 对**运行 ActiveX 控件和插件**选择**启用**或**提示**。
   - 对**对标记为可安全执行脚本的 ActiveX 控件执行脚本**选择**启用**或**提示**。

7. 单击 **OK（确定）**关闭 **Security Settings（安全设置）**窗口。
8. 单击 **OK（确定）**关闭 **Internet Options（Internet 选项）**窗口。

注: 在使用 Internet Explorer 11 的系统上，确保通过单击 **Tools（工具）** > **Compatibility View settings（兼容性视图设置）**添加 iDRAC IP。

注:

- 各个不同版本的 Internet Explorer 具有相同的 **Internet Options（Internet 选项）**。因此，在针对一种浏览器将服务器添加到受信站点列表后，其他浏览器将使用相同的设置。
- 安装 ActiveX 控件前，Internet Explorer 可能会显示一条安全警告。要完成 ActiveX 控件安装过程，必须在 Internet Explorer 显示安全警告提示时接受 ActiveX 控件。
- 如果您在启动虚拟控制台时收到错误 **Unknown Publisher（未知发布程序）**，则可能是由于更改为代码签名证书路径导致的。要解决此错误，您必须下载补充密钥。使用搜索引擎来搜索 **Symantec 16958**，并且从搜索结果中按照 Symantec 网站上的说明进行操作。

Windows Vista 或更新的 Microsoft 操作系统的附加设置

Windows Vista 或更新的操作系统中的 Internet Explorer 浏览器有一项称为 *Protected Mode （保护模式）*的附加安全功能。

使用*保护模式*在 Internet Explorer 浏览器中启动并运行 ActiveX 应用程序：

1. 作为管理员运行 IE。
2. 转至 **Tools（工具）** > **Internet Options（Internet 选项）** > **Security（安全）** > **Trusted Sites（可信站点）**。
3. 请确保没有为可信站点区域选择 **Enable Protected Mode（启用受保护模式）**选项。或者，可以将 iDRAC 地址添加到 Intranet 区域中的站点。默认情况下，受保护模式将针对 Intranet 区域和可信站点区域中的站点关闭。
4. 单击**站点**。
5. 在**将该网站添加到区域**字段中，添加 iDRAC 的地址，然后单击**添加**。
6. 单击**关闭**，然后单击**确定**。
7. 关闭并重新启动浏览器使设置生效。

清除浏览器高速缓存

如果运行虚拟控制台时出现问题（超出范围错误，同步问题等），则应清除浏览器的高速缓存，移除或删除系统上可能存储的任何旧版本查看器并重试。

注: 您必须拥有管理员权限才能清除浏览器的高速缓存。

清除 Java 早期版本

要清除 Windows 或 Linux 中旧版本的 Java 查看器，请执行以下操作：

1. 在命令提示符下，运行 `javaws-viewer` 或 `javaws-uninstall`。
   此时会显示 **Java Cache（Java 高速缓存）**查看器。
2. 删除标题为 *iDRAC 虚拟控制台客户端*的项目。

将 CA 证书导入管理站

当启动虚拟控制台或虚拟媒体时，系统将显示验证证书的提示。如有自定义 Web 服务器证书，则可以通过将 CA 证书导入到 Java 或 ActiveX 受信任的证书存储区来避免这些提示。

有关自动证书注册 (ACE) 的详细信息，请参阅部分 证书自动注册 页面上的 102

将 CA 证书导入到 Java 受信证书库

要将 CA 证书导入到 Java 信任证书存储区：

1. 启动 **Java Control Panel（Java 控制面板）**。
2. 单击**安全**选项卡，然后单击**证书**。

将显示 **Certificates（证书）**对话框。

3. 从 Certificate type（证书类型）下拉式菜单中，选择 **Trusted Certificates（信任的证书）**。
4. 单击 **Import（导入）**，浏览并选择 CA 证书（以 Base64 编码格式），然后单击 **Open（打开）**。
   选定的证书将导入到 Web 启动的信任证书存储区。
5. 单击**关闭**，然后单击**确定**。**Java Control Panel（Java 控制面板）**窗口将关闭。

将 CA 证书导入 ActiveX 受信证书库

您必须使用 OpenSSL 命令行工具来使用安全哈希算法 (SHA) 创建证书散列值。建议使用 OpenSSL 工具 1.0.x 和更高版本，因为它默认使用 SHA。CA 证书必须采用 Base64 编码的 PEM 格式。这是导入每个 CA 证书的一次性过程。

要将 CA 证书导入 ActiveX 可信证书库：

1. 打开 OpenSSL 命令提示窗口。
2. 使用以下命令运行管理站上当前正在使用的 CA 证书的 8 字节散列算法：`openssl x509 -in (name of CA cert) -noout -hash`
   系统会生成一个输出文件。例如，如果 CA 证书文件名为 **cacert.pem**，该命令为：

   ```
   openssl x509 -in cacert.pem -noout -hash
   ```

   系统会生成类似于“431db322”的输出文件。
3. 将 CA 文件重命名为输出文件名，并在扩展名中添加一个“.0”。例如，431db322.0。
4. 将重命名的 CA 认证复制到您的主目录。例如，**C:\Documents and Settings\<user> directory**。

查看 Web 界面的本地化版本

iDRAC Web 界面支持以下语言：

- 英语 (en-us)
- 法语 (fr)
- 德语 (de)
- 西班牙语 (es)
- 日语 (ja)
- 简体中文 (zh-cn)

包含在圆括号中的 ISO 标识符表示受支持的语言变量。对于某些受支持的语言，将浏览器窗口重新调整为 1024 像素宽才能查看所有功能。

iDRAC Web 界面旨在与本地化键盘配合使用以支持语言变量。iDRAC Web 界面的某些功能（如虚拟控制台）可能需要额外的步骤才能访问特定的功能或字母。其他键盘不受支持且可能导致意外问题。

注： □参□□□器文档了解如何配置或□置不同的□言并□看本地化版本的 iDRAC Web 界面。

更新设备固件

使用 iDRAC 可以更新 iDRAC、BIOS 和所有借助 Lifecycle Controller 更新支持的设备固件，例如：

- 光纤信道 (FC) 卡
- 诊断程序
- 操作系统驱动程序包
- 网络接口卡 (NIC)
- RAID 控制器
- 电源设备 (PSU)
- NVMe PCIe 设备
- SAS/SATA 硬盘驱动器
- 内部和外部机柜的背板更新
- OS 收集器

小心：PSU 固件更新可能需要几分□□□，具体取决于系□配置和 PSU 型号。□了避免□坏 PSU，在 PSU 固件更新期□□不要系□上的中断更新□程或□源。

注: 在更新 PowerEdge C 系列服□器的 PSU 固件□，□确保同一机箱中的所有服□器首先关□□源。如果机箱中的任何其他服□器已打开□源，□更新□程将失□。

您必须将所需的固件上载到 iDRAC。在上载完成后，会显示安装在设备上的固件的当前版本和正在应用的版本。如果正在上载的固件无效，则会显示一条错误消息。不需要重新引导的更新会立即应用。需要系统重新引导的更新会分阶段进行和提交，以便在下次系统重新引导时运行。只需一次系统重新引导便可执行所有更新。

注:

- 如果控制器上启用了 SEKM 模式，则在从 SEKM 版本转变为非 SEKM iDRAC 版本后 iDRAC 固件降级/升级尝试将会失败。在 SEKM 版本中进行 iDRAC 固件升级/降级应会通过。
- 在启用 SEKM 的情况下，PERC 固件降级将会失败。

在固件更新后，**系统资源清册**页面显示更新的固件版本并记录日志。

支持的固件映像文件类型包括：

- `.exe` — 基于 Windows 的 Dell Update Package (DUP)。您必须具有控制和配置权限才能使用此映像文件类型。
- `.d9` — 包含 iDRAC 和 Lifecycle Controller 二者的固件

对于扩展名为 `.exe` 的文件，您必须具有系统控制权限。必须启用经许可的远程固件更新功能和 Lifecycle Controller。

对于扩展名为 `.d9` 的文件，您必须具有"配置"权限。

注: 在更新 PSU 固件之前，□确保系□中的所有□点均已关□□源。

注: 在升□ iDRAC 固件之后，您可能会注意到生命周期控制器日志中□示的□□戳存在差异。LC 日志中□示的□□与 iDRC 重置期□少数日志的 NTP/Bios □□不同。

您可以使用以下方法执行固件更新：

- 从本地系统或网络共享加载受支持的映像类型，每次加载一种类型。
- 连接至 FTP、TFTP、HTTP 或 HTTPS 站点或网络存储库（其中包含 Windows DUP 和相应的目录文件）。

  可使用 Dell Repository Manager 创建自定义存储库。有关更多信息，请参阅 *Dell Repository Manager 数据中心用户指南*。iDRAC 可以提供系统上安装的 BIOS 和固件之间的差异报告以及存储库中的可用更新。存储库中包含的所有适用更新均会应用于系统。在获得 iDRAC Enterprise 或 iDRAC Datacenter 许可证后，此功能可用。

  注: HTTP/HTTPS 仅支持摘要验证或无验证。
- 通过使用目录文件和自定义存储库计划循环自动固件更新。

有多种可用于更新 iDRAC 固件的工具和接口。下表仅适用于 iDRAC 固件。表格列出了支持的接口、映像文件类型以及 Lifecycle Controller 是否必须处于已启用状态时才会更新固件。

表. 11: 映像文件类型和相关性

	.D9 映像		iDRAC DUP	
界面	**支持**	**需要 LC 已启用**	**支持**	**需要 LC 已启用**
BMCFW64.exe 公用程序	是	否	否	不适用
Racadm FWUpdate（旧版）	是	否	否	不适用
Racadm Update（新版）	是	是	是	是
iDRAC UI	是	是	是	是
WSMan	是	是	是	是
带内操作系统 DUP	否	不适用	是	否
Redfish	是	不适用	是	不适用

下表提供了关于在更新特定组件的固件时是否需要重新启动系统的信息。

注: 当通□□外方式□用多个固件更新□，将以尽可能高效的□序排列□些更新，以减少不必要的系□重新启□。

表. 12: 固件更新 — 支持的组件

组件名称	支持固件回滚？（“是”或“否”）	带外 — 系统需要重新启动？	带内 — 系统需要重新启动？	Lifecycle Controller GUI — 需要重新启动？
诊断程序	否	否	否	否
操作系统驱动程序包	否	否	否	否
iDRAC	是	否	否*	是
BIOS	是	是	是	是
RAID 控制器	是	是	是	是
BOSS	是	是	是	是
NVDIMM	否	是	是	是
背板	是	是	是	是
注： • 对于扩展器（主动）背板，需要重新启动系统。 • 对于 SEP（被动）背板，无需重新启动的更新仅从版本 4.00.00.00 开始受支持。				
机柜	是	是	否	是
NIC	是	是	是	是
电源设备	是	是	是	是
CPLD	否	是	是	是
注： CPLD 固件升级完成后，iDRAC 将自动重新启动。				
FC 卡	是	是	是	是
NVMe PCIe SSD 驱动器	是	是	是	是
注： 从版本 5.00.00.00 开始，某些设备支持无需重新启动的更新。				
SAS/SATA 硬盘驱动器	否	是	是	否
OS 收集器	否	否	否	否
CMC（位于 PowerEdge FX2 服务器上）	否	是	是	是
TPM	否	是	是	是
注： 从版本 5.00.00.00 开始支持 TPM，操作将被暂存。仅支持固件更新。不支持降级和重新安装同一固件。				

注： 有关 MX 平台的受支持组件的信息，请参阅表 13。

表. 13: 固件更新 — MX 平台的受支持组件

组件名称	支持固件回滚？（“是”或“否”）	带外 — 系统需要重新启动？	带内 — 系统需要重新启动？	Lifecycle Controller GUI — 需要重新启动？
诊断程序	否	否	否	否
操作系统驱动程序包	否	否	否	否
iDRAC	是	否	否*	是
BIOS	是	是	是	是
RAID 控制器	是	是	是	是
BOSS	是	是	是	是

表. 13: 固件更新 — MX 平台的受支持组件 （续）

组件名称	支持固件回滚？ （“是”或“否”）	带外 — 系统需要重新启动?	带内 — 系统需要重新启动?	Lifecycle Controller GUI — 需要重新启动?
NVDIMM	否	是	是	是
背板	是	是	是	是
机柜	是	是	否	是
NIC	是	是	是	是
电源设备	否	否	否	否
CPLD	否	是	是	是
FC 卡	是	是	是	是
NVMe PCIe SSD 驱动器	是	否	否	否
SAS/SATA 硬盘驱动器	否	是	是	否
OS 收集器	否	否	否	否

* 表示虽然不需要重新启动系统，但必须重新启动 iDRAC 才能应用更新。可能暂时中断 iDRAC 通信和监测功能。

当您检查更新时，标记为**可用**的版本并不总表示它是可用的最新版本。当您安装更新前，请确保您选择安装的版本比当前安装的版本更新。如果要控制 iDRAC 检测到的版本，请使用 Dell Repository Manager (DRM) 创建定制存储库并配置 iDRAC 以使用该存储库检查更新。

使用 iDRAC Web 界面更新固件

您可以使用在本地系统中可用的固件映像从网络共享（CIFS、NFS、HTTP 或 HTTP）存储库或 FTP 更新设备固件。

更新单个设备固件

在使用单个设备更新方法更新固件之前，请确保已将固件映像下载到本地系统上的某个位置。

注: 确保用于□个□件 DUP 的文件名不包含任何空格。

要使用 iDRAC Web 界面更新单个设备固件：

1. 转至**维护** > **S 系统更新。**

   此时将显示**固件更新**页面。

2. 在**更新**选项卡中，选择**本地**作为**位置类型。**

   注: 如果您选择本地，请确保将固件映像下载到本地系统上的某个位置。选择要暂存到 iDRAC 以用于更新的一个文件。可以选择要上载到 iDRAC 的附加文件，一次一个文件。这些文件将上载到 iDRAC 上的一个暂存空间，其总大小限制为约 300MB。

3. 单击**浏览**，为所需组件选择固件映像文件，然后单击**上载。**
4. 上载完成后，将在**更新详细信息**部分显示每个已上载到 iDRAC 的固件文件及其状态。

   如果固件映像文件有效并已成功上载，**内容**列将显示一个加号图标 图标，位于该固件映象文件名的旁边。展开该名称可查看**设备名**、**当前**和**可用的固件版本**信息。

5. 选择所需固件文件并执行以下操作之一：
   - 对于不需要主机系统重新启动的固件映像，请单击**安装**（唯一的选项）。例如，iDRAC 固件文件。
   - 对于需要主机系统重新引导的固件映像，请单击**安装并重新引导**或**下次重新引导时安装。**
   - 要取消固件更新，请单击**取消。**

   在您单击**安装**、**安装并重新引导**或**下次重新引导时安装**时，将显示消息 `Updating Job Queue`。

6. 要显示**作业队列**页面，请单击**作业队列。**使用此页面查看并管理分阶段固件更新或单击**确定**刷新当前页面并查看固件更新状态。

   注: 如果未保存更新就离开此页面，则会显示一条错误消息并且所有已上载的内容都会丢失。

注: 如果会□在尚在固件文件后□期，您将无法□□。只能通□ RACADM `reset` 来解决此□□。

注: 固件更新完成后，会□示一条□□消息：`RAC0508: An unexpected error occurred. Wait for few minutes and retry the operation. If the problem persists, contact service provider.`。□是□期的行□。您可以等待一段□□，然后刷新□□器。然后，您将被重定向到登□□面。

计划自动固件更新

您可以为 iDRAC 创建定期更新计划以检查新的固件更新。在计划的日期和时间，iDRAC 会连接到指定的目标，检查新的更新，并应用或部署所有适用的更新。将会在远程服务器上创建一个日志文件，其中包含有关服务器访问权限和已部署固件更新的信息。

建议您使用 Dell Repository Manager (DRM) 创建存储库和配置 iDRAC 以使用此存储库来检查和执行固件更新。使用内部存储库可让您控制 iDRAC 可用的固件和版本，并帮助避免任何意外的固件更改。

注: 有关 DRM 的更多信息，□参□ www.dell.com/openmanagemanuals > Repository Manager。

计划自动更新需要 iDRAC Enterprise 或 Datacenter 许可证。

您可以使用 iDRAC Web 界面或 RACADM 计划自动固件更新。

注: 不支持使用 IPv6 地址□划自□固件更新。

使用 Web 界面计划自动固件更新

要使用 Web 界面计划自动固件更新，请执行以下操作：

注: 如果作业已经计划，则不要创建自动更新作业的下一次计划复现。它会覆盖当前计划的作业。

1. 在 iDRAC Web 界面中，转至 **Maintenance（维护）** > **System Update（系统更新）** > **Automatic Update（自动更新）**。此时将显示 **Firmware Update**（固件更新）页面。
2. 单击 **Automatic Update**（自动更新）选项卡。
3. 选择 **Enable Automatic Update**（启用自动更新）选项。
4. 选择以下任何选项可指定在暂存更新后是否需要重新引导系统：
   - **计划更新** — 暂存固件更新，但不重新引导服务器。
   - **计划更新并重新引导服务器** — 在暂存固件更新后启用服务器重新引导。
5. 选择以下任一项以指定固件映像的位置：
   - **Network（网络）** — 使用来自网络共享（CIFS、NFS、HTTP 或 HTTPS、TFTP）的目录文件。输入网络共享位置的详细信息。
     注: 在指定网络共享设置时，建议不要对用户名和密码使用特殊字符，也不要用百分号来编码特殊字符。
   - **FTP** — 使用来自 FTP 站点的目录文件。输入 FTP 站点的详细信息。
   - **HTTP** 或 **HTTPS** — 允许目录文件流传输和通过 HTTP 和 HTTPS 文件传输。
6. 根据在步骤 5 中执行的选择，输入网络设置或 FTP 设置。
   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
7. 在 **Update Window Schedule**（更新窗口计划）部分中，指定固件更新操作的开始时间和更新频率（每天、每周或每月一次）。
   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
8. 单击**计划更新**。
   将在作业队列中创建下一个计划的作业。在复现作业的第一个实例开始五分钟后，将创建下一个时间周期的作业。

使用 RACADM 计划自动固件更新

要计划自动固件更新，请使用以下命令：

- 要启用自动固件更新：

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
```

- 要查看自动固件更新的状态：

```
racadm get lifecycleController.lcattributes.AutoUpdate
```

- 要计划固件更新操作的开始时间和频率：

```
racadm AutoUpdateScheduler create -u username -p password -l <location>  [-f
catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt <proxytype>]
-time < hh:mm> [-dom < 1 - 28,L,'*'> -wom <1-4,L,'*'> -dow <sun-sat,'*'>] -rp <1-366>
-a <applyserverReboot (1-enabled | 0-disabled)>
```

  例如，
  - 要使用 CIFS 共享自动更新固件：

```
racadm AutoUpdateScheduler create -u admin -p pwd -l //1.2.3.4/CIFS-share -f
cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

  - 要使用 FTP 自动更新固件：

```
racadm AutoUpdateScheduler create -u admin -p pwd -l ftp.mytest.com -pu puser -pp
puser -po 8080 -pt http -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- 要查看当前固件更新计划：

```
racadm AutoUpdateScheduler view
```

- 要禁用自动固件更新：

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
```

- 要清除计划详细信息：

```
racadm AutoUpdateScheduler clear
```

使用 RACADM 更新设备固件

要使用 RACADM 更新设备固件，请使用 `update` 子命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*中的 *https://www.dell.com/idracmanuals*。

示例：

- 从远程 HTTP 共享上载更新文件：

```
racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share
```

- 从远程 HTTPS 共享上载更新文件：

```
racadm update -f <updatefile> -u admin -p mypass -l https://1.2.3.4/share
```

- 要使用更新存储库生成比较报告，请使用以下命令：

```
racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verifycatalog
```

- 要在使用 `myfile.xml` 作为目录文件的情况下从更新存储库执行所有适用的更新，并执行正常重新引导，请使用以下命令：

```
racadm update -f "myfile.xml" -b "graceful" -l //192.168.1.1 -u test -p passwd
```

- 要在使用 `Catalog.xml` 作为目录文件的情况下从 FTP 更新存储库执行所有适用的更新，请使用以下命令：

```
racadm update -f "Catalog.xml" -t FTP -e 192.168.1.20/Repository/Catalog
```

使用 CMC Web 界面更新固件

您可以使用 CMC Web 界面更新用于刀片服务器的 iDRAC 固件。

要使用 CMC Web 界面更新 iDRAC 固件：

1. 登录到 CMC Web 界面。
2. 转至 **iDRAC Settings（iDRAC 设置）** > **Settings（设置）** > **CMC**。
   随即会显示 **Deploy iDRAC**（部署 iDRAC）页面。
3. 单击 **Launch iDRAC**（启动 iDRAC）Web 界面并执行 **iDRAC Firmware Update**（iDRAC 固件更新）。

使用 DUP 更新固件

使用 Dell 更新软件包 (DUP) 更新固件之前，请确保：

- 安装并启用 IPMI 和受管系统驱动程序。
- 如果您的系统运行 Windows 操作系统，启用并启动 Windows Management Instrumentation (WMI) 服务。

  注: 在 Linux 中使用 DUP 实用程序更新 iDRAC 固件时，如果看到控制台中显示 `usb 5-2: device descriptor read/64, error -71` 之类的错误消息，请忽略。
- 如果系统安装了 ESX 管理程序，则对于要运行的 DUP 文件，请确保使用以下命令停止“usbarbitrator”服务：`service usbarbitrator stop`

某些版本的 DUP 会相互冲突。随着时间推移，当创建新版本的软件时，会发生这种情况。较新版本的软件可能会放弃对传统设备的支持。可能添加了对新设备的支持。例如，考虑两个 DUP：Network_Firmware_NDT09_WN64_21.60.5.EXE 和 Network_Firmware_8J1P7_WN64_21.60.27.50.EXE。这些 DUP 支持的设备分为三组。

- 组 A 是传统设备，仅受 NDT09 支持。
- 组 B 是 NDT09 和 8J1P7 均支持的设备。
- 组 C 是仅 8J1P7 支持的新设备。

请考虑具有一个或多个设备（来自组 A、B 和 C 中的每一个）的服务器。如果每次使用一个 DUP，则应该会取得成功。使用 NDT09 本身会更新组 A 和组 B 中的设备。使用 8J1P7 本身会更新组 B 和组 C 中的设备。但是，如果您尝试同时使用这两个 DUP，则可能会尝试同时为组 B 设备创建两个更新。这可能会失败，并显示有效的错误：“此设备的作业已存在”。更新软件无法解决以下冲突：两个有效的 DUP 同时尝试在相同设备上执行两个有效更新。同时，需要两个 DUP 来支持组 A 和组 C 设备。冲突也会扩展到对设备执行回滚。最佳做法是，建议单独使用每个 DUP。

要使用 DUP 更新 iDRAC：

1. 基于安装的操作系统下载 DUP 并在受管系统上运行它。
2. 运行 DUP。
   固件将更新。固件更新完成后无需重新启动系统。

使用远程 RACADM 更新固件

1. 将固件映像下载到 TFTP 或 FTP 服务器，例如，`C:\downloads\firmimg.d9`
2. 运行以下 RACADM 命令：

   TFTP 服务器：

   - 使用 `fwupdate` 命令：

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -g -u -a <path>
     ```

     path

     是 TFTP 服务器上存储 `firmimg.d9` 的位置。
   - 使用 `update` 命令：

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

   FTP 服务器：

   - 使用 `fwupdate` 命令：

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate –f <ftpserver IP>
     <ftpserver username> <ftpserver password> –d <path>
     ```

     path

     是 FTP 服务器上存储 `firmimg.d9` 的位置。

- 使用 `update` 命令：

```
racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 Lifecycle Controller 远程服务更新固件

有关使用 Lifecycle Controller – 远程服务更新固件的信息，请参阅 *生命周期控制器远程服务快速入门指南，网址：*https://www.dell.com/idracmanuals。

从 iDRAC 更新 CMC 固件

在 PowerEdge FX2/FX2s 机箱中，可以从 iDRAC 为 Chassis Management Controller 以及任何可由 CMC 更新和服务器共享的组件更新固件。

应用更新之前，请确保：

- 不允许 CMC 开启服务器电源。
- 带 LCD 的机箱必须显示一条指示“正在更新”的消息。
- 不带 LCD 的机箱必须使用 LED 闪烁模式表示更新的进展。
- 在更新过程中，机箱操作电源命令被禁用。

对于某些需要所有服务器处于空闲状态的的组件（如 IOM 的 Programmable System-on-Chip (PSoC)）的更新，将在机箱下次通电开机时才应用。

设置 CMC 以从 iDRAC 更新 CMC 固件

在 PowerEdge FX2/FX2s 机箱中，在从 iDRAC 更新 CMC 及其共享组件的固件前，请先执行以下操作：

1. 启动 CMC Web 界面
2. 转至 **iDRAC Settings（iDRAC 设置）** > **Settings（设置）** > **CMC。**
   随即会显示 **Deploy iDRAC**（部署 iDRAC）页面。
3. 从 **Chassis Management at Server Mode（服务器模式下的机箱管理）**下拉菜单中，选择 **Manage and Monitor（管理和监测）**，然后单击 **Apply（应用）**。

设置 iDRAC 以更新 CMC 固件

在 PowerEdge FX2/FX2s 机箱中，请先在 iDRAC 中进行以下设置，然后再从 iDRAC 更新 CMC 及其共享组件的固件：

1. 转至 **iDRAC Settings（iDRAC 设置）** > **Settings（设置）** > **CMC。**
2. 单击 **Chassis Management Controller Firmware Update（机箱管理控制器固件更新）**
   此时将显示 **Chassis Management Controller Firmware Update Settings**（Chassis Management Controller 固件更新设置）页面。
3. 对于 **Allow CMC Updates Through OS and Lifecycle Controller**（允许通过操作系统和 Lifecycle Controller 更新 CMC），请选择 **Enabled**（启用）以启用从 iDRAC 更新 CMC 固件。
4. 在 **Current CMC Setting（当前 CMC 设置）**下，确保 **Chassis Management at Server Mode（服务器模式下的机箱管理）**选项显示 **Manage and Monitor（管理和监测）**。您可以在 CMC 中设置此选项。

查看和管理分阶段更新

您可以查看和删除计划的作业，包括配置和更新作业。这是一项授权的功能。在队列中将在下一次重新引导期间运行的所有作业都可以被删除。

使用 iDRAC Web 界面查看和管理分阶段更新

要使用 iDRAC Web 界面查看已计划的作业列表，请转至 **Maintenance（维护）** > **Job Queue（作业队列）**。**Job Queue（作业队列）**页面会显示 Lifecycle Controller 作业队列中作业的状态。有关所显示的字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

要删除作业，可选中该作业，然后单击 **Delete（删除）**。而后页面将刷新，选中的作业将从 Lifecycle Controller 作业队列中移除。您可以在下一次重新引导期间删除所有作业队列。您不能删除处于活动状态的作业，即具有*正在运行*或 *下载*状态的作业。

必须具有服务器控制权限才能删除作业。

使用 RACADM 查看和管理分阶段更新

要使用 RACADM 查看分阶段更新，请使用 `jobqueue` 子命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

回滚设备固件

您可以回滚 iDRAC 或 Lifecycle Controller 所支持的 iDRAC 或任何设备的固件，即使以前使用另一个界面执行了升级。例如，如果固件已使用 Lifecycle Controller GUI 升级，您可以使用 iDRAC Web 界面回滚固件。您可通过一次系统重新引导执行多个设备的固件回滚。

在具有单个 iDRAC 和 Lifecycle Controller 固件的 Dell 第 14 代 PowerEdge 服务器上，回滚 iDRAC 固件还将回滚 Lifecycle Controller 固件。

建议让固件保持最新，以确保您具有最新功能和安全更新。如果在更新后遇到任何问题，则可能需要回滚更新或安装较早的版本。要安装较早的版本，请使用 Lifecycle Controller 来检查更新并选择您要安装的版本。

有关固件回滚支持和不支持的组件的详细信息，请参阅表 固件更新 — 支持的组件 页面上的 74

您可以为以下组件执行固件回滚：

- 带 Lifecycle Controller 的 iDRAC
- BIOS
- 网络接口卡 (NIC)
- 电源设备 (PSU)
- RAID 控制器
- 背板

注： 不能□□断程序、□□程序包和 CPLD □行固件回滚。

回滚固件之前，请确保：

- 您有回滚 iDRAC 固件的“配置”权限。
- 您有“服务器控制”权限并已启用 Lifecycle Controller 来回滚除 iDRAC 以外的任何其他设备的固件。
- 如果 NIC 模式设置为**共享 LOM**，将该模式更改为**专用**。

您可以使用以下任何方法将固件回滚到之前安装的版本：

- iDRAC Web 界面
- CMC Web 界面（在 MX 平台上不受支持）
- OME-Modular Web 界面（在 MX 平台上不受支持）
- CMC RACADM CLI（在 MX 平台上不受支持）
- iDRAC RACADM CLI
- Lifecycle Controller GUI
- Lifecycle Controller 远程服务

使用 iDRAC Web 界面回滚固件

要回滚设备固件，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Maintenance（维护）** > **System Update（系统更新）** > **Rollback（回滚）**。
   Rollback（回滚）页面将显示可以为其回滚固件的设备。您可以查看设备名称、关联的设备、当前安装的固件版本和可用固件回滚版本。

2. 选择一个或多个要为其回滚固件的设备。
3. 基于所选设备，单击 **Install and Reboot（安装并重新引导）**或 **Install Next Reboot（下次重新引导时安装）**。如果仅选择 iDRAC，那么单击 **Install（安装）**。
   当单击**安装并重新引导**或**下次重新引导时安装**时，将显示“正在更新作业队列”消息。
4. 单击 **Job Queue**（作业队列）。
   此时将显示**作业队列**页面，您可以在此处查看和管理已暂存的固件更新。

   注：
   - 在回滚模式下时，即使您离开此页面，回滚进程也会在后台继续执行。

   在以下情况下将显示错误消息：
   - 您没有回滚 iDRAC 以外任何固件的服务器控制权限，或没有回滚 iDRAC 固件的配置权限。
   - 固件回滚已在另一个会话中执行。
   - 已暂存要运行的更新或更新已处于运行状态。

   如果 Lifecycle Controller 已禁用或处于恢复状态，并且您尝试为 iDRAC 以外的任何设备执行固件回滚，则在启用 Lifecycle Controller 时将显示相应的警告消息。

使用 CMC Web 界面回滚固件

要使用 CMC Web 界面回滚：

1. 登录到 CMC Web 界面。
2. 转至 **iDRAC Settings（iDRAC 设置）** > **Settings（设置）** > **CMC**。
   随即会显示 **Deploy iDRAC**（部署 iDRAC）页面。
3. 单击 **Launch iDRAC（启动 iDRAC）**并执行 使用 iDRAC Web 界面回滚固件 页面上的 80 中所述的设备固件回滚。

使用 RACADM 回滚固件

1. 使用 `swinventory` 命令检查回滚状态和 FQDD：

   ```
   racadm swinventory
   ```

   对于要为其回滚固件的设备，`Rollback Version`（回滚版本）必须为 `Available`（可用）。另外，请记录 FQDD。

2. 使用以下命令回滚设备固件：

   ```
   racadm rollback <FQDD>
   ```

   有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 Lifecycle Controller 回滚固件

有关信息，请参阅 *生命周期控制器用户指南，网址：*https://www.dell.com/idracmanuals。

使用 Lifecycle Controller 远程服务回滚固件

有关信息，请参阅 *生命周期控制器远程服务快速入门指南，网址：*https://www.dell.com/idracmanuals。

恢复 iDRAC

iDRAC 支持两个操作系统映像，以确保可引导的 iDRAC。在出现无法预见的灾难性错误并且您丢失两个引导路径时，请执行以下操作：

- iDRAC 引导程序会检测到没有可引导的映像。
- 系统健康状态和识别 LED 指示灯以大约 1/2 秒的速率闪烁。（LED 指示灯位于机架式和塔式服务器的背面，位于刀片式服务器的正面。）

- 引导程序现在正在轮询 SD 卡插槽。
- 使用 Windows 操作系统将 SD 卡格式化为 FAT 格式，或者使用 Linux 操作系统将其格式化为 EXT3 格式。
- 将 **firmimg.d9** 复制到 SD 卡。
- 将 SD 卡插入服务器。
- 引导程序会检测 SD 卡，让闪烁的 LED 指示灯变成稳定的琥珀色，读取 firmimg.d9，重新编程 iDRAC，然后重新引导 iDRAC。

使用其他系统管理工具监测 iDRAC

您可以使用 Dell Management Console 或 Dell OpenManage Essentials 查找和监测 iDRAC。您也可以使用 Dell Remote Access Configuration Tool (DRACT) 来查找 iDRAC、更新固件和设置 Active Directory。有关更多信息，请参阅相应的用户指南。

支持服务器配置配置文件 — 导入和导出

服务器配置配置文件 (SCP) 允许您导入和导出服务器配置文件。

注: 您需要管理员权限来执行导出和导入 SCP 任务。

您可以从本地管理站和网络共享（CIFS、NFS、HTTP 或 HTTPS）导入和导出。使用 SCP，您可以选择并导入或导出 BIOS、NIC 和 RAID 的组件级别配置。您可以将 SCP 导入和导出至本地管理站或者 CIFS、NFS、HTTP 或 HTTPS 网络共享。您可以导入和导出 iDRAC、BIOS、NIC 和 RAID 的单个配置文件或将它们作为单一的文件全部导出。

您可以指定作业正在运行的 SCP 的预览导入或导出，会生成配置结果，但不会应用配置。

通过 GUI 启动导入或导出后即创建作业。可在作业队列页面中查看作业状态。

注: 目标地址仅接受主机名或 IP 地址。

注: 您可以浏览到特定位置以导入服务器配置文件。您需要选择要导入的正确服务器配置文件。例如，导入 .xml。

注: 根据导出的文件格式（您所选的），扩展名将会自动添加。例如，`export_system_config.xml`。

注: SCP 以最少的重新启动次数将完整配置应用于单个作业。但在一些系统配置中，某些属性会改变设备的操作模式，或者可能创建具有新属性的子设备。出现此情况时，SCP 可能无法在单个作业中应用所有设置。查看作业的 ConfigResult 条目，以解决任何待处理的配置设置。

SCP 允许使用跨多个系统的单个 xml/json 文件执行操作系统部署 (OSD)。此外，您还可以一次性执行现有操作，如配置和存储库更新。

SCP 还允许导出和导入所有 iDRAC 用户的 SSH 公共密钥。为所有用户提供 4 个 SSH 公共密钥。

以下是使用 SCP 进行操作系统部署的步骤：

1. 导出 SCP 文件
2. SCP 文件包含执行 OSD 所需的所有抑制属性。
3. 编辑/更新 OSD 属性，然后执行导入操作。
4. 然后，这些 OSD 属性将由 SCP 构造器进行验证。
5. SCP 构造器执行 SCP 文件中指定的配置和存储库更新。
6. 完成配置和更新后，主机操作系统关闭。

   注: CIFS 和 NFS 共享仅受主机操作系统介质支持。
7. SCP Orchestrator 通过连接所选操作系统的驱动程序启动 OSD，然后对 NFS/Share 中存在的操作系统介质启动一次性启动。
8. LCL 显示作业进度。
9. BIOS 引导至操作系统介质后，SCP 作业显示为完成。
10. 在 65535 秒或 `OSD.1#ExposeDuration` 属性指定的持续时间后，系统会自动分离连接的介质和操作系统介质。

使用 iDRAC Web 界面导入服务器配置配置文件

要导入服务器配置配置文件：

1. 转至**配置** > **服务器配置配置文件**
   随即显示**服务器配置配置文件**页面。
2. 选择以下任一项指定文件类型：
   - **本地**导入保存在本地驱动器中的配置文件。
   - **网络共享**从 CIFS 或 NFS 共享中导入配置文件。
   - **HTTP 或 HTTPS** 使用 HTTP/HTTPS 文件传输，从本地文件中导入配置文件。

   注: 根据位置类型，您必须输入网络设置或 HTTP/HTTPS 设置。如果针对 HTTP/HTTPS 配置代理，还需要代理设置。
3. 选择**导入组件**选项中列出的组件。
4. 选择**关机**类型。
5. 选择**最长等待时间**以指定导入完成后至系统关闭前的等待时间。
6. 单击**导入**。

使用 iDRAC Web 界面导出服务器配置配置文件

要导出服务器配置配置文件：

1. 转至**配置** > **服务器配置配置文件**
   随即显示**服务器配置配置文件**页面。
2. 请单击**导出**。
3. 选择以下任一项指定文件类型：
   - **本地** 配置文件保存在本地驱动器上。
   - **网络共享**以在 CIFS 或 NFS 共享上保存配置文件。
   - **HTTP 或 HTTPS** 使用 HTTP/HTTPS 文件传输，将配置文件保存到本地文件。

   注: 根据位置类型，您必须输入网络设置或 HTTP/HTTPS 设置。如果针对 HTTP/HTTPS 配置代理，还需要代理设置。
4. 选择您需要备份配置的组件。
5. 选择**导出类型**，以下为可用的选项：
   - **基本**
   - **更换导出**
   - **克隆导出**
6. 选择**导出文件格式**。
7. 选择**其他导出项目**。
8. 请单击**导出**。

BIOS 设置或 F2 中的安全引导配置

UEFI Secure Boot 是一项技术，可消除在 UEFI 固件和 UEFI 操作系统 (OS) 交接期间可能出现的重大安全失效。在 UEFI Secure Boot 中，链中的每个组件需先针对特定证书进行验证和授权，然后才允许加载或运行。Secure Boot 可消除威胁，并在引导的每个步骤中提供软件身份检查 - 平台固件、选件卡和操作系统引导加载程序。

统一可扩展固件接口 (UEFI) 论坛 - 一家开发预引导软件标准的行业机构，他们在 UEFI 规范中定义了 Secure Boot。计算机系统供应商、扩展卡供应商和操作系统提供商就此规范进行协作以促进互操作性。作为 UEFI 规范的一部分，Secure Boot 代表了预引导环境中的安全行业标准。

启用时，UEFI Secure Boot 会阻止加载未签名的 UEFI 设备驱动程序，显示错误消息并且不允许设备运行。您必须禁用 Secure Boot 才能加载未签名的设备驱动程序。

在 Dell 第 14 代和更高版本的 PowerEdge 服务器上，您可以使用不同的界面（RACADM、WSMAN、REDFISH, 和 LC-UI）来启用或禁用 Secure Boot 功能。

可接受的文件格式

Secure Boot 策略在 PK 中仅包含一个密钥，但可能有多个密钥位于 KEK 中。在理想情况下，平台制造商或平台拥有者维护与公用 PK 对应的私钥。第三方（例如操作系统提供商和设备提供商）维护与 KEK 中的公共密钥对应的私钥。这样一来，平台所有者或第三方可在特定系统的 db 或 dbx 中添加或移除条目。

Secure Boot 策略使用 db 和 dbx 授权预引导映像文件执行。为了使某个映像文件可以执行，它必须与 db 中的密钥或散列值关联，而不是与 dbx 中的密钥或散列值关联。更新 db 或 dbx 的内容的任何尝试都必须通过专用 PK 或 KEK 签名。更新 PK 或 KEK 内容的任何尝试都必须通过专用 PK 签名。

表. 14: 可接受的文件格式

策略组件	可接受的文件格式	可接受的文件扩展名	允许的最大记录
PK	X.509 证书（仅限二进制 DER 格式）	1. .cer 2. .der 3. .crt	一声
KEK	X.509 证书（仅限二进制 DER 格式） 公共密钥库	1. .cer 2. .der 3. .crt 4. .pbk	多个
DB 和 DBX	X.509 证书（仅限二进制 DER 格式） EFI 映像（系统 BIOS 将计算并导入映像摘要）	1. .cer 2. .der 3. .crt 4. .efi	多个

通过单击系统 BIOS 设置下的系统安全可以访问安全引导设备设置功能。要转至系统 BIOS 设置，请在开机自检过程中显示公司徽标时按 F2。

- 默认情况下，禁用安全引导，并且将安全引导策略设置为标准。要配置安全引导策略，您必须启用安全引导。
- 当安全引导模式设置为标准，它表示系统具有出厂时加载的默认证书和映像摘要或散列值。此项迎合标准固件、驱动程序、选件 ROM 和引导加载程序的安全性。
- 要在服务器上支持新的驱动程序或固件，必须在 Secure Boot 证书存储区的 DB 中注册各自的证书。因此，必须将“Secure Boot 策略”配置为“自定义”。

将“Secure Boot 策略”配置为“自定义”时，它会继承默认情况下系统中加载的标准证书和映像（您可以修改这些标准证书和映像）。将“Secure Boot 策略”配置为“自定义”允许您执行诸如以下的操作：查看、导出、导入、删除、全部删除、重置和全部重置。使用这些操作，您可以配置“Secure Boot 策略”。

将“Secure Boot 策略”配置为“自定义”会启用一些选项，以允许在 PK、KEK、DB 和 DBX 上通过使用诸如以下的各种操作管理证书存储区：导出、导入、删除、全部删除、重置和全部重置。您可以通过单击相应的链接选择要更改并执行适当操作的策略 (PK / KEK / DB / DBX)。每个部分都将具有用于执行导入、导出、删除和重置操作的链接。链接基于适用项目启用，而适用项目取决于当时的配置。“全部删除”和“全部重置”是具有对所有策略都有影响的操作。“全部删除”会删除“自定义”策略中的所有证书和映像摘要，“全部重置”会还原“标准”或“默认”证书存储区中的所有证书和映像摘要。

BIOS 恢复

BIOS 恢复功能允许您从存储映像中手动恢复 BIOS。开启系统时选中 BIOS，如果检测到损坏或被破坏的 BIOS，则会显示错误消息。您随后使用 RACADM 启动 BIOS 恢复过程。要执行手动 BIOS 恢复，请参阅 https://www.dell.com/idracmanuals 上提供的 iDRAC RACADM Command Line Interface Reference Guide（iDRAC RACADM 命令行界面参考指南）。

4

配置 iDRAC

通过 iDRAC 可配置 iDRAC 属性、设置用户以及设置警报，以执行远程管理任务。

在配置 iDRAC 之前，请确保已配置 iDRAC 网络设置和受支持的浏览器，并且已更新需要的许可证。有关 iDRAC 中可获许可的功能的更多信息，请参阅 iDRAC 许可证 页面上的 23。

您可以使用以下方法配置 iDRAC：

- iDRAC Web 界面
- RACADM
- 远程服务（请参阅 *Lifecycle Controller Remote Services 用户指南*）
- IPMITool（请参阅 *Baseboard Management Controller 管理公用程序用户指南*）

要配置 iDRAC：

1. 登录到 iDRAC。
2. 如有必要，修改网络设置。

   注: 如果您已配置 iDRAC 网络设置，请在 iDRAC IP 地址设置过程中使用 iDRAC 设置公用程序，然后忽略此步骤。

3. 配置访问 iDRAC 的界面。
4. 配置前面板显示。
5. 如有必要，配置系统位置。
6. 如有必要，配置时区和网络时间协议 (NTP)。
7. 建立到 iDRAC 的以下任何备选通信方法：
   - IPMI 或 RAC 串行
   - IPMI LAN 上串行
   - LAN 上 IPMI
   - SSH
8. 获取所需证书。
9. 添加和配置具有权限的 iDRAC 用户。
10. 配置和启用电子邮件警报、SNMP 陷阱或 IPMI 警报。
11. 如有必要，设置功率上限策略。
12. 启用上次崩溃屏幕。
13. 如有必要，配置虚拟控制台和虚拟媒体。
14. 如有必要，配置 vFlash SD 卡。
15. 如有必要，设置第一引导设备。
16. 如有必要，将 OS 设置为 iDRAC 直通。

主□：

- □看 iDRAC 信息
- 修改网□□置
- 密□□□□
- FIPS 模式
- 配置服□
- 使用 VNC 客□端管理□程服□器
- 配置前面板□示屏
- 配置□区和 NTP
- □置第一引□□□
- 启用或禁用 OS 到 iDRAC 直通
- □取□□
- 使用 RACADM 配置多个 iDRAC
- 禁用□□以修改主机系□上的 iDRAC 配置□置

查看 iDRAC 信息

您可以查看 iDRAC 的基本属性。

使用 Web 界面查看 iDRAC 信息

在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Overview（概览）**，以查看与 iDRAC 相关的以下信息。有关属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

iDRAC 详细信息

- 设备类型
- 硬件版本
- 固件版本
- 固件更新
- RAC 时间
- IPMI 版本
- 可能的会话数
- 当前会话数
- IPMI 版本

iDRAC 服务模块

- 状态

连接视图

- 状态
- 交换机连接 ID
- 交换机端口连接 ID

当前网络设置

- iDRAC MAC 地址
- 活动的 NIC 接口
- DNS 域名

当前 IPv4 设置

- IPv4 已启用
- DHCP
- 当前 IP 地址
- 当前子网掩码
- 当前网关
- 使用 DHCP 获取 DNS 服务器地址
- 当前首选 DNS 服务器
- 当前备用 DNS 服务器

当前 IPv6 设置

- 启用 IPv6
- 自动配置
- 当前 IP 地址
- 当前 IP 网关
- 链路本地地址
- 使用 DHCPv6 获取 DNS
- 当前首选 DNS 服务器
- 当前备用 DNS 服务器

使用 RACADM 查看 iDRAC 信息

要使用 RACADM 查看 iDRAC 信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals 中提供的 `getsysinfo` 或 `get` 子命令详细信息。

修改网络设置

使用 iDRAC 设置实用程序配置 iDRAC 网络设置后，您还可以通过 iDRAC Web 界面、RACADM、生命周期控制器和 Server Administrator （启动至操作系统后）修改设置。有关工具和权限设置的详细信息，请参阅相应的用户指南。

要使用 iDRAC Web 界面或 RACADM 修改网络设置，您必须具有**配置**权限。

注: 更改网□□置可能会使指向 iDRAC 的当前网□□接中断。

使用 Web 界面修改网络设置

要修改 iDRAC 网络设置：

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置** > **连接性** > **网络** > **网络设置**。
   随即会显示**网络**页面。
2. 根据您的要求指定网络设置、常用设置、IPv4、IPv6、IPMI 和/或 VLAN 设置并单击**应用**。
   如果您选择**网络设置**下的**自动专用 NIC**，则当 iDRAC 将其 NIC 选择作为共享 LOM（1、2、3 或 4）并且在 iDRAC 专用 NIC 上检测到链接时，iDRAC 会更改其 NIC 选择来使用专用 NIC。如果在专用 NIC 上检测不到链接，则 iDRAC 使用共享 LOM。从共享 NIC 切换到专用 NIC 的超时为五秒，而从专用 NIC 切换到共享 NIC 的超时为 30 秒。您可以使用 RACADM 或 WSMan 配置此超时值。

   有关各字段的信息，请参阅 *iDRAC 联机帮助*。

   注: 如果 iDRAC 正在使用 DHCP 并且已租用其 IP 地址，则在禁用 NIC 或 IPv4 或 DHCP 后，该 DHCP 租约将被释放回 DHCP 服务器地址池中。

使用本地 RACADM 修改网络设置

要生成可用网络属性列表，使用该命令

```
racadm get iDRAC.Nic
```

要使用 DHCP 获得 IP 地址，请使用下面的命令写入对象 `DHCPEnable` 并启用此功能。

```
racadm set iDRAC.IPv4.DHCPEnable 1
```

以下示例介绍如何使用命令配置所需的 LAN 网络属性：

```
racadm set iDRAC.Nic.Enable 1
racadm set iDRAC.IPv4.Address 192.168.0.120
racadm set iDRAC.IPv4.Netmask 255.255.255.0
racadm set iDRAC.IPv4.Gateway 192.168.0.120
racadm set iDRAC.IPv4.DHCPEnable 0
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNS1 192.168.0.5
racadm set iDRAC.IPv4.DNS2 192.168.0.6
racadm set iDRAC.Nic.DNSRegister 1
racadm set iDRAC.Nic.DNSRacName RAC-EK00002
racadm set iDRAC.Nic.DNSDomainFromDHCP 0
racadm set iDRAC.Nic.DNSDomainName MYDOMAIN
```

注: 如果将 `iDRAC.Nic.Enable` 或 **iDRAC.Nic.Enable** 设置为 0，则即使启用 DHCP，iDRAC LAN 也会处于禁用状态。

配置 IP 筛选

除了用户验证之外，访问 iDRAC 时使用以下选项可提供更高的安全性：

- IP 筛选限制访问 iDRAC 的客户端的 IP 地址范围。它将传入登录的 IP 地址与指定的范围进行比较，并只允许来自管理站（其 IP 地址位于该范围内）的 iDRAC 访问。所有其他登录请求都将被拒绝。
- 当特定 IP 地址发生重复登录失败时，则会阻止该地址在预选的时间长度内登录 iDRAC。如果您登录失败多达两次，则仅允许您在 30 秒后再次登录。如果您登录失败多达两次，则仅允许您在 60 秒后再次登录。

注: 此功能最多支持 5 个 IP 范□。您可以使用 RACADM 和 Redfish □看/□置此功能。

随着特定 IP 地址登录失败次数的累积，累计次数将在内部计数器中记录。当用户成功登录后，失败历史记录将被清除，并且内部计数器将重置。

注: 如果来自客□端 IP 地址的登□□□被阻止，少数 SSH 客□端会□示以下信息：`ssh exchange identification: Connection closed by remote host`。

使用 iDRAC Web 界面配置 IP 筛选

您必须具有"配置"权限才能执行这些步骤。

要配置 IP 筛选：

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置连接性网络网络设置高级网络设置**。
   随即会显示**网络**页面。
2. 单击**高级网络设置**。
   随即会显示**网络安全性**页面。
3. 使用 **IP 地址范围**和 **IP 范围子网掩码**指定 IP 筛选设置。
   有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击**应用**保存设置。
   联邦信息处理标准 — FIPS 是美国政府机关和承包商所使用的一套标准。FIPS 模式旨在满足 FIPS 140-2 1 级的要求。有关 FIPS 的更多信息，请参阅用于 iDRAC 的 FIPS 用户指南和用于非 MX 平台的 CMC。
   注: 启用 **FIPS 模式**，将 iDRAC 重设为默认设置。

使用 RACADM 配置 IP 筛选

您必须具有"配置"权限才能执行这些步骤。

配置 IP 筛选，使用 `iDRAC.IPBlocking` 组中的以下 RACADM 对象：

- RangeEnable
- RangeAddr
- RangeMask

`RangeMask` 属性对接入 IP 地址和 `RangeAddr` 属性均适用。如果结果相同，则允许接入登录请求访问 iDRAC。从此范围外的 IP 地址登录会导致错误。

注: 配置 IP 筛选支持多达 5 个 IP 范围。

如果以下表达式等于零，登录将会继续：

```
RangeMask & (<incoming-IP-address> ^ RangeAddr)
```

&
按位和数量

^
按位独占 - 或

IP 筛选的示例

以下 RACADM 命令会阻塞 192.168.0.57 以外的所有 IP 地址：

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
```

要将登录限制到一组四个相邻 IP 地址（例如，192.168.0.212 到 192.168.0.215），则选择掩码中除最低两个位以外的所有位：

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.252
```

范围掩码的最后字节设置为 252，十进制数字为 11111100b。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

密码组选择

“密码组选择”可用于在 iDRAC 或客户端通信中限制密码，并确定如何使用安全连接。它提供了筛选生效的使用中 TLS 密码组的另一个级别。这些设置可通过 iDRAC Web 界面、RACADM 和 WSMAN 命令行界面配置。

使用 iDRAC Web 界面配置密码组选择

小心: 使用 OpenSSL 密码命令来解析语法无效的字符串可能会导致出现意外错误。

注: 这是一个高级安全选项。在配置此选项之前，请确保您拥有以下方面的全面知识：

- OpenSSL 密码字符串语法及其使用方法。
- “工具和步骤”以验证产生的密码组配置，以确保结果符合预期和要求。

注: 在您配置 TLS 密码组的高级设置之前，请确保您使用的是受支持的 Web 浏览器。

要添加自定义密码字符串：

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置** > **服务** > **Web 服务器**。
2. 单击**自定义密码字符串**选项下的**设置密码字符串**。
   此时将显示**设置自定义密码字符串**页面。
3. 在**自定义密码字符串**字段中，输入有效的字符串，然后单击**设置密码字符串**。

   注: 有关密码字符串的更多信息，请参阅：www.openssl.org/docs/man1.0.2/man1/ciphers.html。

4. 单击**应用**。
   设置自定义密码字符串会终止当前 iDRAC 会话。等待几分钟，然后再打开新的 iDRAC 会话。

iDRAC 在端口 5000 上支持以下密码：

ssl-enum-ciphers：

TSLv1.1 密码：

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048)

TLSv1.2 密码：

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048)

使用 RACADM 配置密码组选择

要使用 RACADM 配置密码组选择，请使用以下命令之一：

- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-GCM-SHA384`
- `racadm set idraC.webServer.customCipherString ALL:-DHE-RSA-CAMELLIA256-SHA`
- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-SHA256:+AES256-GCM-SHA384:-DHE-RSA-CAMELLIA256-SHA`

有关这些对象的更多信息，请参阅 dell.com/idracmanuals 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC RACADM 命令行界面参考指南）。

FIPS 模式

FIPS 是美国政府代理和合约方必须使用计算机的安全标准。从版本 iDRAC 2.40.40.40 开始，iDRAC 支持启用 FIPS 模式。

将来 iDRAC 将获得正式认证以支持 FIPS 模式。

支持的 FIPS 模式和获得 FIPS 验证的不同

已通过完成加密模块验证程序进行验证的软件称为 FIPS 认证。由于完成 FIPS 所需的时间，并非所有版本的 iDRAC 都会验证。有关 iDRAC 的 FIPS 验证的最新状态相关信息，请参阅 NIST Web 站点上的“Cryptographic Module Validation Program”（加密模块验证程序）页面。

启用 FIPS 模式

小心: 启用 FIPS 模式可将 iDRAC 重□□出厂默□□置。如果您要恢复□置，先□份服□器配置文件 (SCP)，然后启用 FIPS 模式，并在重启 iDRAC 后恢复 SCP。

注: 如果您要重新安装或升□ iDRAC 固件，FIPS 模式会禁用。

使用 Web 界面启用 FIPS 模式

1. 在 iDRAC Web 界面中，导航至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **Network（网络）** > **Network Settings（网络设置）** > **Advanced Network Settings（高级网络设置）**。
2. 在 **FIPS 模式**中，选择**启用**并单击**应用**。

   注: 启用 FIPS 模式会将 iDRAC 重设为默认设置。

3. 系统会显示消息，提示您确认更改。单击 **OK（确定）**。
   iDRAC 在 FIPS 模式中重新启动。等待至少 60 秒，然后重新连接至 iDRAC。
4. 安装 iDRAC 的受信任证书。

注: 默认的 SSL 证书在 FIPS 模式中不允许。

注: 某些 iDRAC 界面，如 IPMI 和 SNMP 的标准兼容实施，不支持兼容 FIPS。

使用 RACADM 启用 FIPS 模式

使用 RACADM CLI 以执行以下命令：

```
racadm set iDRAC.Security.FIPSMode <Enable>
```

禁用 FIPS 模式

要禁用 FIPS 模式，您必须将 iDRAC 重设为出厂默认设置。

配置服务

您可以在 iDRAC 上配置和启用以下服务：

本地配置	使用本地 RACADM 和 iDRAC 设置公用程序禁止（从主机系统）访问 iDRAC 配置。
网络服务器	允许访问 iDRAC Web 界面。如果您禁用该 Web 界面，则远程 RACADM 也将被禁用。使用本地 RACADM 重新启用 Web 服务器和远程 RACADM。
SEKM 配置	使用客户端服务器体系结构在 iDRAC 上启用安全企业密钥管理功能。
SSH	通过固件 RACADM 访问 iDRAC。
远程 RACADM	远程访问 iDRAC。
SNMP 代理	在 iDRAC 中启用对 SNMP 查询（GET、GETNEXT 和 GETBULK 操作）的支持。
自动系统恢复代理程序	启用上次系统崩溃屏幕。
Redfish	启用 Redfish RESTful API 的支持。
VNC 服务器	启用带有或不带 SSL 加密 的 VNC 服务器。

使用 Web 界面配置服务

要使用 iDRAC Web 界面配置服务：

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置** > **服务**。
   将显示**服务**页面。
2. 指定所需信息，然后单击**应用**。
   有关各设置的信息，请参阅 *iDRAC 联机帮助*。

   注: 不要选中**阻止此页面创建附加的对话框**复选框。选择此选项会阻止您配置服务。

   您可以从“iDRAC 设置”页面配置 **SEKM**。单击 **iDRAC 设置** > **服务** > **SEKM 配置**。

   注: 有关配置 SEKM 的详细逐步操作过程，请参阅 *iDRAC 联机帮助*。

   注: 当**安全性（加密）**模式从**无**更改为 **SEKM** 时，实时作业不可用。但它将被添加至分级作业列表。然而，当该模式从 **SEKM** 更改为**无**时，实时作业成功。

   在更改 KeySecure 服务器上“客户端证书”部分中**用户名**字段的值时，例如：将值从**通用名称 (CN)** 更改为**用户 ID (UID)** 时，验证以下方面
   a. 使用现有帐户时：
      - 在 iDRAC SSL 证书中，验证**用户名**字段（而非**通用名称**字段）是否与 KMS 上的现有用户名相匹配。如果它们不匹配，则您必须设置“用户名”字段，并再次重新生成 SSL 证书，使其在 KMS 上签名并重新上传到 iDRAC。

b. 使用新的用户帐户时：
   - 确保**用户名**字符串与 iDRAC SSL 证书中的“用户名”字段相匹配。
   - 如果它们不匹配，则您需要重新配置 iDRAC KMS 属性（即，“用户名”和“密码”）。
   - 一旦验证确定证书包含用户名，需要进行的唯一更改是将密钥所有权从旧用户更改为新用户，以匹配新创建的 KMS 用户名。

在使用 Vormetric Data Security Manager 作为 KMS 时，请确保 iDRAC SSL 证书中的通用名称 (CN) 字段与添加到 Vormetric Data Security Manager 的主机名相匹配。否则，可能无法成功导入证书。

注：
- 当 `racadm sekm getstatus` 报告为**失败**时，**重新加密**选项将禁用。
- 对于客户端证书下面的**用户名**字段，SEKM 仅支持**通用名称**、**用户 ID** 或**组织单元**。
- 如果您使用第三方 CA 为 iDRAC CSR 进行签名，则确保第三方 CA 支持客户端证书中**用户名**字段的值 **UID**。如果它不受支持，请使用**通用名称**作为**用户名**字段的值。
- 如果您使用的是“用户名”和“密码”字段，请确保 KMS 服务器支持这些属性。

注： 对于 KeySecure 密钥管理服务器，
- 创建 SSL 证书请求时，必须在**主题备用名称**字段中包含密钥管理服务器的 IP 地址
- IP 地址必须采用以下格式：IP:xxx.xxx.xxx.xxx。

使用 RACADM 配置服务

要使用 RACADM 启用和禁用服务，请使用 `set` 命令和以下对象组中的对象：
- iDRAC.LocalSecurity
- iDRAC.LocalSecurity
- iDRAC.SSH
- iDRAC.Webserver
- iDRAC.Racadm
- iDRAC.SNMP

有关这些对象的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

启用或禁用 HTTPS 重定向

如果由于与默认 iDRAC 证书相关的警告问题而不想从 HTTP 自动重定向至 HTTPS 或作为临时设置用于调试目的，您可以按照以下方式配置 iDRAC：禁用从 http 端口（默认为 80）重定向到 https 端口（默认为 443）。默认情况下，它处于启用状态。您必须注销并登录到 iDRAC 以使此设置生效。如果禁用此功能，会显示一条警告消息。

您必须具有“配置 iDRAC”权限才能启用或禁用 HTTPS 重定向。

在启用或禁用该功能时，将在 Lifecycle Controller 日志文件中记录一个事件。

要禁用 HTTP 到 HTTPS 的重定向：

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

要启用 HTTP 到 HTTPS 的重定向：

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

要查看 HTTP 到 HTTPS 的重定向的状态：

```
racadm get iDRAC.Webserver.HttpsRedirection
```

SEKM 功能

以下是 iDRAC 中提供的 SEKM 功能：

1. **SEKM 密钥清除策略** — iDRAC 提供了一个策略设置，允许您将 iDRAC 配置为在执行重新加密操作时清除密钥管理服务器 (KMS) 中旧的未使用密钥。您可以将 iDRAC 可读写属性 KMSKeyPurgePolicy 设置为以下值之一：
   - Keep All Keys — 这是默认设置以及现有行为，即 iDRAC 在执行重新加密操作时保持 KMS 上的所有密钥不变。
   - Keep N and N-1 keys — 在执行重新加密操作时，iDRAC 删除 KMS 中除当前 (N) 和上一个密钥 (N-1) 以外的所有密钥。
2. **禁用 SEKM 上的 KMS 密钥清除** — 作为 Secure Enterprise Key Manager (SEKM) 解决方案的一部分，iDRAC 允许您禁用 iDRAC 上的 SEKM。禁用 SEKM 后，iDRAC 在 KMS 中生成的密钥将不会被使用，并保留在 KMS 中。此功能用于允许 iDRAC 在 SEKM 被禁用时删除这些密钥。iDRAC 为现有的传统命令“racadm sekm disable”提供新的选项“-purgeKMSKeys”，这将允许您在 iDRAC 上的 SEKM 被禁用时清除 KMS 中的密钥。

   注: 如果 SEKM 已被禁用，并且您想要清除旧密钥，您必须重新启用 SEKM，然后禁用传入选项 -purgeKMSKeys。
3. **密钥创建策略** — 在此版本中，iDRAC 预配置了密钥创建策略。属性 KeyCreationPolicy 为只读，并且设置为“Key per iDRAC”值。
   - iDRAC 只读属性 iDRAC.SEKM.KeyIdentifierN 报告由 KMS 创建的密钥标识符。

     ```
     racadm get iDRAC.SEKM.KeyIdentifierN
     ```
   - iDRAC 只读属性 iDRAC.SEKM.KeyIdentifierNMinusOne 在执行重新加密操作后报告之前的密钥标识符。

     ```
     racadm get iDRAC.SEKM.KeyIdentifierNMinusOne
     ```
4. **SEKM 重新加密** — iDRAC 提供了两个选项来重新加密 SEKM 解决方案，即重新加密 iDRAC 或 PERC。建议重新加密 iDRAC，因为这会重新加密所有支持/启用 SEKM 安全的设备。
   - *SEKM iDRAC 重新加密 [iDRAC.Embedded.1 FQDD 上的重新加密]* — 在执行 `racadm sekm rekey iDRAC.Embedded.1` 时，所有支持/启用 SEKM 安全的设备都通过来自 KMS 的新密钥重新加密，这是所有启用了 SEKM 的设备的通用密钥。还可以从 iDRAC GUI **iDRAC 设置** > **服务** > **SEKM 配置** > **重新加密**执行 iDRAC 重新加密操作。执行此操作后，可以通过读取 KeyIdentifierN 和 KeyIdentifierNMinusOne 属性来验证密钥更改。
   - *SEKM PERC 重新加密（控制器 [示例 RAID.Slot.1-1] FQDD 上的重新加密）* — 在执行 `racadm sekm rekey <controller FQDD>` 时，相应的启用 SEKM 的控制器将通过从 KMS 创建的当前活动 iDRAC 通用密钥进行重新加密。还可以从 iDRAC GUI **存储** > **控制器** > **<控制器 FQDD>** > **操作** > **编辑** > **安全** > **安全（加密）** > **重新加密**执行存储控制器重新加密操作。

使用 VNC 客户端管理远程服务器

您可以使用标准开放式 VNC 客户端来管理同时使用桌面和移动设备（如 DELL Wyse PocketCloud）的远程服务器。当数据中心内的服务器停止运行时，iDRAC 或操作系统会向管理站上的控制台发送警报。控制台将向移动设备发送包含所需信息的电子邮件或 SMS，然后在管理站中启动 VNC 查看器应用程序。VNC 查看器可以连接到服务器上的操作系统/管理程序，并提供对主机服务器的键盘、视频和鼠标的访问权限以执行必要的补救措施。在启动 VNC 客户端之前，您必须启用 VNC 服务器并配置 iDRAC 中的 VNC 服务器设置，如密码、VNC 端口号、SSL 加密和超时值。您可以使用 iDRAC Web 界面或 RACADM 来配置这些设置。

注: VNC 功能已□得□可，在 iDRAC Enterprise 或 Datacenter □可□中提供。

您可以从许多 VNC 应用程序或桌面客户端（如 RealVNC 或 Dell Wyse PocketCloud 中的相应项）中进行选择。

可同时激活 2 个 VNC 客户端会话。第二个会话处于只读模式。

如果 VNC 会话活动，则只能使用启动虚拟控制台而不是虚拟控制台查看器来启动虚拟介质。

如果已禁用视频加密，则 VNC 客户端将直接启动 RFB 握手过程，并且无需进行 SSL 握手。在 VNC 客户端握手（RFB 或 SSL）过程中，如果另一个 VNC 会话处于活动状态，或者虚拟控制台会话处于打开状态，则新 VNC 客户端会话将被拒绝。在完成初始握手过程后，VNC 服务器将禁用虚拟控制台并只允许使用虚拟介质。在 VNC 会话终止之后，VNC 服务器将恢复虚拟控制台的原始状态（启用或禁用）。

注:

- 启动 VNC 会话时，如果您遇到 RFB 协议错误，请将 VNC 客户端设置更改为“高质量”，然后重新启动会话。
- 当 iDRAC NIC 处于共享模式并关闭再启动主机系统时，网络连接会中断几秒钟。在这段时间内，如果您在活动的 VNC 客户端中执行任何操作，VNC 会话可能会关闭。您必须等待超时（针对 iDRAC Web 界面**服务**页面中 VNC 服务器设置所配置的值），然后重新建立 VNC 连接。
- 如果 VNC 客户端窗口最小化超过 60 秒，客户端窗口将会关闭。您必须打开新的 VNC 会话。您必须打开新的 VNC 会话。如果您在 60 秒内最大化 VNC 客户端窗口，那么可以继续使用。

使用 iDRAC Web 界面配置 VNC 服务器

要配置 VNC 服务器设置，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **Virtual Console（虚拟控制台）**。
   将显示 **Virtual Console（虚拟控制台）**页面。
2. 在 **VNC Serve**（VNC 服务器）部分中，启用 VNC 服务器，指定密码、端口号，并启用或禁用 SSL 加密。
   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。
   VNC 服务器即已配置。

使用 RACADM 配置 VNC 服务器

要配置 VNC 服务器，请使用 `set` 命令和 `VNCserver` 中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

设置带 SSL 加密的 VNC 查看器

在配置 iDRAC 中的 VNC 服务器设置时，如果 **SSL 加密** 选项已启用，则必须使用 SSL 隧道应用程序以及 VNC 查看器以建立与 iDRAC VNC 服务器的 SSL 加密的连接。

注: 大多数 VNC 客户端没有内置的 SSL 加密支持。

要配置 SSL 隧道应用程序：

1. 配置 SSL 隧道以接受 `<localhost>:<localport number>` 上的连接。例如，127.0.0.1:5930。
2. 配置 SSL 隧道以连接到 `<iDRAC IP address>:<VNC server port Number>`。例如，192.168.0.120:5901。
3. 启动隧道应用程序。
   要通过 SSL 加密的信道与 iDRAC VNC 服务器建立连接，则将 VNC 查看器连接至本地主机（链路本地 IP 地址）和本地端口号（127.0.0.1: < 本地端口号 >）。

设置不带 SSL 加密的 VNC 查看器

一般情况下，所有兼容远程帧缓冲 (RFB) 的 VNC 查看器都可使用为 VNC 服务器配置的 iDRAC IP 地址和端口号连接到 VNC 服务器。如果配置 iDRAC 中的 VNC 服务器设置时禁 SSL 加密选项，则执行以下操作以连接到 VNC 查看器：

在 **VNC 查看器** 对话框中，在 **VNC 服务器** 字段中输入 iDRAC IP 地址和端口号。

格式为 `<iDRAC IP address:VNC port number>`

例如，如果 iDRAC IP 地址是 192.168.0.120，而 VNC 端口号是 5901，则输入 `192.168.0.120:5901`。

配置前面板显示屏

您可以配置受管系统的前面板 LCD 和 LED 显示屏。

对于机架和塔式服务器，有两种类型的前面板可用：

- LCD 前面板和系统 ID LED
- LED 前面板和系统 ID LED

对于刀片式服务器，服务器前面板上只有系统 ID LED 可用，因为刀片式机箱已有 LCD。

配置 LCD 设置

您可以在受管系统的 LCD 前面板上设置和显示默认字符串（例如 iDRAC 名称、IP 等）或用户定义的字符串。

使用 Web 界面配置 LCD 设置

要配置服务器 LCD 前面板显示：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **Front Panel configuration（前面板配置）**。
2. 在 **LCD Settings**（LCD 设置）部分，从 **Set Home Message**（设置主屏幕消息）下拉菜单中，选择下列选项之一：
   - 服务标签（默认）
   - 资产标签
   - DRAC MAC 地址
   - DRAC IPv4 地址
   - DRAC IPv6 地址
   - 系统功率
   - 环境温度
   - 系统型号
   - 主机名
   - 用户定义
   - 无

   如果您选择 **User Defined**（用户定义），请在文本框中输入所需消息。

   如果您选择 **None**（无），则不会在服务器 LCD 前面板上显示主屏幕消息。
3. 启用虚拟控制台指示（可选）。如果启用，则服务器上的 Live Front Panel Feed（前面板实时信息）部分和 LCD 面板会在存在活动虚拟控制台会话时显示 `Virtual console session active`（虚拟控制台会话活动）消息。
4. 单击**应用**。
   服务器 LCD 前面板显示配置的主屏幕消息。

使用 RACADM 配置 LCD 设置

要配置服务器 LCD 前面板显示，使用 `System.LCD` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置 LCD 设置

要配置服务器 LCD 前面板显示：

1. 在 iDRAC 设置公用程序中，转至 **Front Panel Security**（前面板安全性）。
   此时将显示 **iDRAC Settings.Front Panel Security**（iDRAC 设置前面板安全性）。
2. 启用或禁用电源按钮。
3. 指定以下各项：
   - 对前面板的访问
   - LCD 消息字符串
   - 系统电源装置、环境温度装置和错误显示
4. 启用或禁用虚拟控制台指示。
   有关各选项的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
5. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。

配置系统 ID LED 设置

要识别服务器，请在受管系统上启用或禁用 ID LED 闪烁。

使用 Web 界面配置系统 ID LED 设置

配置系统 ID LED 显示屏：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **Front Panel configuration（前面板配置）**。显示 **System ID LED Settings（系统 ID LED 设置）**页面。
2. 在 **System ID LED Settings（系统 ID LED 设置）**区域中，选择以下任意选项以启用或禁用 LED 闪烁：
   - 闪烁关
   - 闪烁开
   - 闪烁开 1 天超时
   - 闪烁开 1 周超时
   - 闪烁开 1 月超时
3. 单击**应用**。
   前面板上的 LED 闪烁即配置完成。

使用 RACADM 配置系统 ID LED 设置

要配置系统 ID LED，使用 `setled` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

配置时区和 NTP

您可以使用网络时间协议 (NTP) 而非 BIOS 或主机系统时间在 iDRAC 上配置时区并同步 iDRAC 时间。

必须具有配置权限才能配置时区或 NTP 设置。

使用 iDRAC Web 界面配置时区和 NTP

要使用 iDRAC Web 界面配置时区和 NTP，请执行以下操作：

1. 转到 **iDRAC Settings（iDRAC 设置）** > **Settings（设置）** > **Time zone and NTP Settings（时区和 NTP 设置）**。
   随即显示 **Time zone and NTP**（时区和 NTP）页面。
2. 要配置时区，请从 **Time Zone**（时区）下拉菜单中选择所需的时区，然后单击 **Apply**（应用）。
3. 要配置 NTP，请启用 NTP，输入 NTP 服务器地址，然后单击 **Apply**（应用）。
   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 配置时区和 NTP

要配置时区和 NTP，请使用 `set` 命令和 `iDRAC.Time` 和 `iDRAC.NTPConfigGroup` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

注: iDRAC 与主机同步时间（本地时间）。因此，建议将 iDRAC 和主机配置为相同时区，以使时间同步正确。如果想要更改时区，则需要在主机和 iDRAC 上更改它，然后需要重新启动主机。

设置第一引导设备

您可以仅对下一次引导或之后的所有重新引导设置第一引导设备。如果您设置在之后的所有重新引导使用该设备，其将作为 BIOS 中的第一引导设备，直到再次从 iDRAC Web 界面或从 BIOS 引导顺序更改。

您可以将第一引导设备设置为以下一种：

- 正常引导
- PXE
- BIOS 设置
- 本地软盘/主要可移动介质
- 本地 CD/DVD
- 硬盘驱动器
- 虚拟软盘
- 虚拟 CD/DVD/ISO

- 本地 SD 卡
- Lifecycle Controller
- BIOS 引导管理器
- UEFI 设备路径
- UEFI HTTP

注：
- BIOS 设置 (F2)、Lifecycle Controller (F10) 和 BIOS Boot Manager (F11) 不能设置作为永久引导设备。
- iDRAC Web 界面中的第一引导设备设置会覆盖系统 BIOS 引导设置。

使用 Web 界面设置第一引导设备

要使用 iDRAC Web 界面设置第一引导设备：

1. 转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **First Boot Device（第一引导设备）**。
   将显示 **First Boot Device（第一引导设备）**页面。
2. 从下拉式列表中选择所需的第一引导设备，然后单击 **Apply（应用）**。
   系统将从被选择为要进行后续重新引导的设备引导。
3. 要在下一次引导时从所选设备引导一次，请选择 **Boot Once（引导一次）**。此后，系统将从 BIOS 引导顺序中的第一引导设备引导。
   有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 设置第一引导设备

- 要设置第一引导设备，使用 `iDRAC.ServerBoot.FirstBootDevice` 对象。
- 要为设备启用一次引导，使用 `iDRAC.ServerBoot.BootOnce` 对象。

有关这些对象的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用虚拟控制台设置第一引导设备

服务器通过其引导顺序进行引导之前，您可以在虚拟控制台查看器中查看服务器时选择从哪个设备进行引导。引导一次受 设置第一引导设备 页面上的 96 中所列的所有设备支持。

要使用虚拟控制台设置第一引导设备，请执行以下操作：

1. 启动虚拟控制台。
2. 在虚拟控制台查看器中，从 **Next Boot**（下次引导）菜单中设置所需的设备作为第一引导设备。

启用上次崩溃屏幕

要对受管系统崩溃的原因进行故障排除，您可以使用 iDRAC 来捕获系统崩溃图像。

注： 有关 Server Administrator 的更多信息，请参阅 OpenManage *安装指南*，网址：https://www.dell.com/openmanagemanuals。

主机系统应具有 Windows 操作系统方可使用此功能。

注：
- 此功能在 Linux 系统上不适用。
- 此功能独立于任何代理或属性。

启用或禁用 OS 到 iDRAC 直通

在具有网络子卡 (NDC) 或嵌入式主板上的 LAN (LOM) 设备的服务器中，您可以启用 OS 到 iDRAC 直通功能。此功能可通过共享 LOM、专用 NIC 或 USB NIC 在 iDRAC 和主机操作系统之间提供高速双向带内通信。在获得 iDRAC Enterprise 或 iDRAC Datacenter 许可证后，此功能可用。

注: iDRAC Service Module (iSM) 提供了更多的功能，可用于通□操作系□管理 iDRAC。有关更多信息，□参□ www.dell.com/idracservicemodule 上提供的 iDRAC Service Module User's Guide（iDRAC Service Module 用□指南）。

通过专用 NIC 启用时，您可以在主机操作系统中启动浏览器，然后访问 iDRAC Web 界面。适用于刀片服务器的专用 NIC 通过 Chassis Management Controller 控制。

在专用 NIC 或共享 LOM 之间切换不要求重新启动或重设主机操作系统或 iDRAC。

您可以通过以下方式启用此信道：

- iDRAC Web 界面
- RACADM 或 WSMan（后操作系统环境）
- iDRAC 设置公用程序（预操作系统环境）

如果通过 iDRAC Web 界面更改了网络配置，则必须至少等待 10 秒才能启用 OS 到 iDRAC 直通。

如果您通过 RACADM、WSMan 或 Redfish 使用服务器配置文件来配置服务器，并且如果此文件中的网络设置发生变化，则您必须等待 15 秒启用 OS 到 iDRAC 直通功能或设置 OS 主机 IP 地址。

在启用 OS 到 iDRAC 直通之前，请确保：

- iDRAC 配置为使用专用 NIC 或共享模式（即 NIC 选择分配到某个 LOM）。
- 主机操作系统和 iDRAC 位于同一子网和同一 VLAN 中。
- 已配置主机操作系统 IP 地址。
- 已安装支持操作系统至 iDRAC 直通功能的卡。
- 您具有配置权限。

在启用此功能时：

- 在共享模式下，将使用主机操作系统的 IP 地址。
- 在专用模式中，您必须提供主机操作系统的有效 IP 地址。如果多个 LOM 处于活动状态，则输入第一个 LOM 的 IP 地址。

如果在启用操作系统到 iDRAC 的直通功能后该功能不工作，请务必检查以下项目：

- iDRAC 专用的 NIC 电缆已正确连接。
- 至少一个 LOM 处于活动状态。

注: 使用默□的 IP 地址。确保 USB NIC 接口的 IP 地址与 iDRAC 或主机操作系□的 IP 地址不在相同网□子网内。如果此 IP 地址与主机系□或本地网□的其他接口的 IP 地址冲突，□必□更改此 IP 地址。

注: 如果在 USB 网卡□于禁用状□的情况下启□ iDRAC 服□模□，□ iDRAC 服□模□会将 USB 网卡 IP 地址更改□ 169.254.0.1。

注: □勿使用 169.254.0.3 和 169.254.0.4 IP 地址。□些 IP 地址是当使用 A/A □□□，□位于前面板上的 USB NIC 端口保留的。

注: 启用 NIC □□□，可能无法通□ LOM 直通从主机服□器□□ iDRAC。然后，可以使用 iDRAC USB NIC 从主机服□器操作系□或通□ iDRAC □用 NIC □外部网□□□ iDRAC。

支持 OS 到 iDRAC 直通功能的卡

下表提供了支持通过使用 LOM 实现 OS 到 iDRAC 直通功能的卡的列表。

表. 15: 通过使用 LOM 实现 OS 到 iDRAC 直通 — 支持的卡

类别	制造商	类型
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T
	Intel	• x520/i350 QP rNDC 1G BASE-T

内置的 LOM 卡也支持 OS 到 iDRAC 直通功能。

支持 USB NIC 的操作系统

支持 USB NIC 的操作系统包括：

- Server 2012 R2 Foundation Edition
- Server 2012 R2 Essentials Edition
- Server 2012 R2 Standard Edition

- Server 2012 R2 Datacenter Edition
- Server 2012 for Embedded Systems（Base 和带 SP1 的 R2）
- Server 2016 Essentials Edition
- Server 2016 Standard Edition
- Server 2016 Datacenter Edition
- RHEL 7.3
- RHEL 6.9
- SLES 12 SP2
- ESXi 6.0 U3
- vSphere 2016
- XenServer 7.1

对于 Linux 操作系统，请首先在主机操作系统上将 USB NIC 配置为 DHCP，然后再启用 USB NIC。

对于 vSphere，必须安装 VIB 文件，然后再启用 USB NIC。

注: 要在 Linux 操作系统或 XenServer 中将 USB NIC 配置为 DHCP，请参阅操作系统或管理程序文档。

安装 VIB 文件

对于 vSphere 操作系统，在启用 USB NIC 之前，必须安装 VIB 文件。

要安装 VIB 文件，请执行以下操作：

1. 使用 Win-SCP 将 VIB 文件复制到 ESX-i 主机操作系统的 `/tmp/` 文件夹。
2. 转到 ESXi 提示符处并运行以下命令：

   ```
   esxcli software vib install -v /tmp/ iDRAC_USB_NIC-1.0.0-799733X03.vib --no-sig-check
   ```

   输出为：

   ```
   Message: The update completed successfully, but the system needs to be rebooted for
   the changes to be effective.
   Reboot Required: true
   VIBs Installed: Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03
   VIBs Removed:
   VIBs Skipped:
   ```

3. 重新引导服务器。
4. 在 ESXi 提示符处运行以下命令：`esxcfg-vmknic -l`。
   输出将显示 usb0 条目。

使用 Web 界面启用或禁用 OS 到 iDRAC 直通

要使用 Web 界面启用 OS 到 iDRAC 直通，请执行以下操作：

1. 转至 **iDRAC 设置** > **连接** > **网络** > **OS 到 iDRAC 直通**。
   此时将显示 **OS 到 iDRAC 直通**页面。
2. 将状态更改为**已启用**。
3. 为直通模式选择以下任何选项：
   - **LOM** — iDRAC 与主机操作系统之间的操作系统至 iDRAC 直通链接已通过 LOM 或 NDC 建立。
   - **USB NIC** — iDRAC 与主机操作系统之间的操作系统至 iDRAC 直通链接已通过内部 USB 总线建立。

   注: 如果您将直通模式设置为 LOM，请确保执行以下操作：
   - 操作系统和 iDRAC 位于同一子网内
   - 将网络设置中的 NIC 选择设置为 LOM
4. 如果在共享的 LOM 模式下连接了服务器，则**操作系统 IP 地址**字段将禁用。

   注: 如果已在 iDRAC 上启用 VLAN，则 LOM 直通将只在主机上配置了 VLAN 标记并且在共享 LOM 模式下有效。

   注:

- 当将直通模式设置为 LOM 时，在冷启动后无法从主机操作系统启动 iDRAC。
- 我们特意删除了使用专用模式功能的 LOM 直通。

5. 如果选择 **USB NIC** 作为直通配置，则输入 USB NIC 的 IP 地址。
   默认值是 169.254.1.1。建议使用默认 IP 地址。但是，如果此 IP 地址与主机系统或本地网络的其他接口的 IP 地址冲突，则必须更改此 IP 地址。

   请勿输入 169.254.0.3 和 169.254.0.4 这两个 IP 地址。这些 IP 地址是在使用 A/A 电缆时，为位于前面板上的 USB NIC 端口保留的。

   注: 如果首选 IPv6，则默认地址为 fde1:53ba:e9a0:de11::1。如果需要，可在 idrac.OS-BMC.UsbNicULA 设置中修改此地址。如果 USB NIC 上不需要 IPv6，则可以通过将地址更改为"::"来禁用它

6. 单击**应用**。
7. 单击**测试网络配置**以检查 IP 是否可访问，以及是否已在 iDRAC 和主机操作系统之间建立链接。

使用 RACADM 启用或禁用 OS 到 iDRAC 直通

要使用 RACADM 启用或禁用 OS 到 iDRAC 直通，使用 `iDRAC.OS-BMC` 组中的对象。

有关更多信息，请参阅 *iDRAC 属性注册表*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序启用或禁用 OS 到 iDRAC 直通

要使用 iDRAC 设置公用程序启用或禁用 OS 到 iDRAC 直通，请执行以下操作：

1. 在 iDRAC 设置公用程序中，转至**通信权限**。
   这将显示 **iDRAC 设置通信权限**页面。
2. 选择以下任一选项以启用 OS 到 iDRAC 直通：
   - **LOM** — iDRAC 与主机操作系统之间的操作系统至 iDRAC 直通链接已通过 LOM 或 NDC 建立。
   - **USB NIC** — iDRAC 与主机操作系统之间的操作系统至 iDRAC 直通链接已通过内部 USB 总线建立。

   注: 如果您将直通模式设置为 LOM，请确保执行以下操作：
   - 操作系统和 iDRAC 位于同一子网内
   - 将网络设置中的 NIC 选择设置为 LOM

   要禁用此功能，请选择**已禁用**。

   注: 只有在卡支持"操作系统至 iDRAC 直通"功能时，才能选择 LOM 选项。否则，该选项将显示为灰色。

3. 如果选择 **LOM** 作为直通配置，并且使用专用模式连接服务器，则输入操作系统的 IPv4 地址。

   注: 如果在共享的 LOM 模式下连接了服务器，则**操作系统 IP 地址**字段将禁用。

4. 如果选择 **USB NIC** 作为直通配置，则输入 USB NIC 的 IP 地址。
   默认值是 169.254.1.1。但是，如果此 IP 地址与主机系统或本地网络的其他接口的 IP 地址冲突，则必须更改此 IP 地址。请勿输入 169.254.0.3 和 169.254.0.4 这两个 IP 地址。这些 IP 地址是在使用 A/A 电缆时，为位于前面板上的 USB NIC 端口保留的。

   注: 如果首选 IPv6，则默认地址为 fde1:53ba:e9a0:de11::1。如果需要，可在 idrac.OS-BMC.UsbNicULA 设置中修改此地址。如果 USB NIC 上不需要 IPv6，则可以通过将地址更改为"::"来禁用它

5. 依次单击**后退**、**完成**和**是**。
   该详细信息即会保存。

获取证书

下表列出了基于登录类型的证书类型。

表. 16: 基于登录类型的证书类型

登录类型	证书类型	获取方法
使用 Active Directory 的单点登录	可信 CA 证书	生成 CSR 并从证书颁发机构获取签名 SHA-2 证书也受支持。
本地或 Active Directory 用户的智能卡登录	• 用户证书 • 可信 CA 证书	• 用户证书 - 使用智能卡供应商提供的卡管理软件将智能卡用户证书导出为基于 64 位编码的文件。 • 可信 CA 证书 - 此证书由 CA 颁发。 SHA-2 证书也受支持。
Active Directory 用户登录	可信 CA 证书	此证书由 CA 颁发。 SHA-2 证书也受支持。
本地用户登录	SSL 证书	生成 CSR 并从可信 CA 获取签名 **注:** iDRAC 附带默认的自签名 SSL 服务器证书。iDRAC Web 服务器、虚拟介质和虚拟控制台使用此证书。 SHA-2 证书也受支持。

SSL 服务器证书

iDRAC 包含一个 Web 服务器，该服务器配置为使用行业标准 SSL 安全协议，以通过网络传输加密数据。提供了 SSL 加密选项以禁用较弱密码。SSL 基于非对称加密技术构建，广泛用于在客户端和服务器之间提供经过验证和加密的通信，以防止在网络上窃听。

启用 SSL 的系统可以执行下列任务：

- 向启用 SSL 的客户端验证自身
- 允许两个系统建立加密的连接

注: 如果 SSL 加密□置□ 256 位或更改以及 168 位或更改，□您的虚□机□境（JVM、IcedTea）的密□系□□境可能需要安装 Unlimited Strength Java Cryptography Extension Policy Files 以允□将 iDRAC 插件（例如 vConsole）用于此□别加密。有关安装策略文件的信息，□参□ Java 的□明文件。

默认情况下，iDRAC Web 服务器具有 Dell 自签名的唯一 SSL 数字证书。您可以将默认 SSL 证书更换为公认的认证机构 (CA) 签名的证书。认证机构是信息技术行业认可的企业实体，可满足高标准的可靠性审查、识别和其他重要安全标准。例如，Thwate 和 VeriSign 均为 CA。要启动获取 CA 签名证书的流程，请使用您的公司信息通过 iDRAC Web 界面或 RACADM 界面生成证书签名请求 (CSR)，然后将生成的 CSR 提供给 CA（如 VeriSign 或 Thawte）。CA 可以是根 CA 或中间 CA。收到 CA 签名的 SSL 证书后，将其上传到 iDRAC。

对于管理站信任的每个 iDRAC，该 iDRAC 的 SSL 证书必须放在管理站的证书存储区。一旦管理站上安装 SSL 证书后，支持的浏览器可以访问 iDRAC 而不会显示证书警告。

您也可以上传自定义签名证书以签署 SSL 证书，而不是依赖于默认的签名证书执行此功能。通过将一个自定义签名证书导入所有管理站，使用自定义签名证书的所有 iDRAC 都将受信任。如果在已使用自定义 SSL 证书的情况下上传自定义签名证书，则自定义 SSL 证书会被禁用并使用一次性自动生成且带有自定义签名证书的 SSL 证书。您可以下载自定义签名证书（无需私钥）。您也可以删除现有的自定义签名证书。删除自定义签名证书后，iDRAC 将会重设并自动生成新的自签名 SSL 证书。如果重新生成一个自签名证书，则必须在该 iDRAC 和管理工作站之间重新建立信任。自动生成的 SSL 证书自带签名并且有效期为七年零一天，开始日期为过去的某一天（针对管理站和 iDRAC 上不同的时区设置）。

当生成证书自签名请求 (CSR) 时，iDRAC Web 服务器 SSL 证书支持星号字符 (*) 作为常用名称最左侧组件的部分。例如 *.qa.com 或 *.company.qa.com。这称为通配符证书。如果在 iDRAC 以外生成通配符 CSR，您可以获得签名的单个通配符 SSL 证书并为多个 iDRAC 上传该证书，并且所有 iDRAC 都受到受支持的浏览器的信任。使用支持通配符证书的受支持浏览器连接到 iDRAC Web 界面时，iDRAC 将受到浏览器的信任。在启动查看器时，iDRAC 将受到查看器客户端的信任。

生成新的证书签名请求

CSR 是向认证机构 (CA) 提交的 SSL 服务器证书的数字请求。SSL 服务器证书使服务器客户端能够信任服务器的身份并与服务器协商加密会话。

CA 在收到 CSR 后会审核和验证 CSR 中包含的信息。如果申请人符合 CA 的安全标准，CA 会发出数字签名的 SSL 服务器证书，当申请人的服务器与 Management Station 上运行的浏览器建立 SSL 连接时，该证书可唯一地标识申请人的服务器。

CA 批准 CSR 并颁发 SSL 服务器证书后，该证书可上载到 iDRAC。用于生成 CSR（存储在 iDRAC 固件上）的信息必须与 SSL 服务器证书中包含的信息匹配，即该证书必须通过 iDRAC 创建的 CSR 生成。

使用 Web 界面生成 CSR

生成新 CSR：

注： 每个新 CSR 都会覆盖固件中存储的任何以前的 CSR 数据。CSR 中的信息必须匹配 SSL 服务器证书中的信息。否则，iDRAC 不会接受该证书。

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置** > **服务** > **Web 服务器** > **SSL 证书**，选择**生成证书签名请求 (CSR)**，然后单击**下一步**。
   将显示**生成一个新证书签名请求**页面。
2. 输入每个 CSR 属性的值。
   有关更多信息，请参阅 *iDRAC 联机帮助* i。
3. 单击**生成**。
   此时将生成新的 CSR。将其保存到管理站。

使用 RACADM 生成 CSR

要使用 RACADM 生成 CSR，请使用 `set` 命令以及 `iDRAC.Security` 组中的对象，然后使用 `sslcsrgen` 命令生成 CSR。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

证书自动注册

在 iDRAC 中，证书自动注册功能让您可以自动安装和续订 Web 服务器使用的证书。启用此功能时，现有 Web 服务器证书将被替换为新证书。

注：

- 证书自动注册是一项许可功能，需要 Datacenter 许可证。
- 发布服务器证书需要设置有效的 NDES（网络设备注册服务）。

以下是证书自动注册配置参数：

- 启用/禁用
- SCEP 服务器 URL
- 质询密码

注： 有关□些参数的更多信息，□参□ *iDRAC 联机帮助*。

以下是证书自动注册的可用状态：

- 已注册 — 证书自动注册已启用。证书会受监视并可到期时发布新证书。
- 注册 — 证书自动注册启用后的中间状态。
- 错误 — NDES 服务器出现问题。
- 无 — 默认值。

注： 启用□□自□注册后，Web 服□器将重新启□，并且会注□所有□有 Web 会□。

上载服务器证书

生成 CSR 后，您可以将签名的 SSL 服务器证书上传到 iDRAC 固件。iDRAC 必须重设以应用证书。iDRAC 只接受 X509、Base 64 编码的 Web 服务器证书。SHA-2 证书也受支持。

小心：重□期□，iDRAC 在几分□内不可用。

使用 Web 界面上载服务器证书

上载 SSL 服务器证书：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **SSL** > **SSL certificate（SSL 证书）**，选择 **Upload Server Certificate（上传服务器证书）**并单击 **Next（下一步）**。
   将显示 **Certificate Upload（证书上载）**页面。
2. 在 **File Path（文件路径）**下，单击 **Browse（浏览）**并选择 Management Station 上的证书。
3. 单击**应用**。
   SSL 服务器证书将会上载到 iDRAC。
4. 将会显示一条弹出消息，要求您立即或稍后重设 iDRAC。根据需要，单击 **Reset iDRAC（重设 iDRAC）**或 **Reset iDRAC Later（稍后重设 iDRAC）**。
   iDRAC 将重设并且会应用新证书。iDRAC 重设期间会在几分钟内不可用。

   注： 必须重设 iDRAC 才能应用新证书。iDRAC 重设之前，现有证书处于活动状态。

使用 RACADM 上载服务器证书

要上载 SSL 服务器证书，请使用 `sslcertview` 命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

如果在具有可用私钥的 iDRAC 外部生成了 CSR，则将证书上载到 iDRAC：

1. 将 CSR 发送至公认的根 CA。CA 将签署 CSR。CSR 将变为有效证书。
2. 使用远程 racadm `sslkeyupload` 命令上载私钥。
3. 使用远程 racadm `sslcertupload` 命令将签署的证书上载到 iDRAC。
   新的证书将会被上载到 iDRAC。将会显示一条消息，要求您重设 iDRAC。
4. 运行 racadm `racreset` 命令重设 iDRAC。
   iDRAC 将会重设并应用新证书。重设期间，iDRAC 在几分钟内不可用。

   注： 您必须重设 iDRAC 才能应用新证书。在 iDRAC 重设之前，现有证书将保持活动状态。

查看服务器证书

您可以查看当前在 iDRAC 中使用的 SSL 服务器证书。

使用 Web 界面查看服务器证书

在 iDRAC Web 界面中，转至 **iDRAC 设置** > **服务** > **Web 服务器** > **SSL 证书**。**SSL** 页面在页面顶部显示当前使用的 SSL 服务器证书。

使用 RACADM 查看服务器证书

要查看 SSL 服务器证书，请使用 `sslcertview` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

上载自定义签名证书

您可以上载自定义签名证书来签署 SSL 证书。SHA-2 证书也受支持。

使用 Web 界面上载自定义签名证书

要使用 iDRAC Web 界面上载自定义签名证书：

1. 转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **SSL**。
   此时将显示 **SSL** 页面。
2. 在 **Custom SSL Certificate Signing Certificate（自定义 SSL 证书签名证书）**，请单击 **Upload Signing Certificate（上传签名证书）**。
   此时将显示 **Upload Custom SSL Certificate Signing Certificate**（上载自定义 SSL 证书签名证书）页面。
3. 单击 **Choose File（选择文件）**并选择自定义 SSL 证书签名证书文件。
   只支持符合公钥加密标准 #12 (PKCS #12) 的证书。
4. 如果证书受密码保护，请在 **PKCS#12 Password**（PKCS#12 密码）字段中输入密码。
5. 单击**应用**。
   证书将会被上载到 iDRAC。
6. 将会显示一条弹出消息，要求您立即或稍后重设 iDRAC。根据需要，单击 **Reset iDRAC（重设 iDRAC）**或 **Reset iDRAC Later（稍后重设 iDRAC）**。
   重设 iDRAC 后才能应用新的证书。iDRAC 重设期间会在几分钟内不可用。
   注: 必须重设 iDRAC 才能应用新证书。iDRAC 重设之前，现有证书处于活动状态。

使用 RACADM 上载自定义 SSL 证书签名证书

要使用 RACADM 上载自定义 SSL 证书签名证书，请使用 `sslcertupload` 命令，然后使用 `racreset` 命令以重设 iDRAC。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

下载自定义 SSL 证书签名证书

您可以使用 iDRAC Web 界面或 RACADM 下载自定义签名证书。

下载自定义签名证书

要使用 iDRAC Web 界面下载自定义签名证书：

1. 转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **SSL**。
   此时将显示 **SSL** 页面。
2. 在 **Custom SSL Certificate Signing Certificate**（自定义 SSL 证书签名证书）下，选择 **Download Custom SSL Certificate Signing Certificate**（下载自定义 SSL 证书签名证书）并单击 **Next**（下一步）。
   此时会显示一条弹出消息，指示可以将自定义签名证书保存到所选位置。

使用 RACADM 下载自定义 SSL 证书签名证书

要下载自定义 SSL 证书签名证书，请使用 `sslcertdownload` 子命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

删除自定义 SSL 证书签名证书

您还可以使用 iDRAC Web 界面或 RACADM 删除现有的自定义签名证书。

使用 iDRAC Web 界面删除自定义签名证书

要使用 iDRAC Web 界面删除自定义签名证书：

1. 转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **SSL**。
   此时将显示 **SSL** 页面。
2. 在 **Custom SSL Certificate Signing Certificate**（自定义 SSL 证书签名证书）下，选择 **Delete Custom SSL Certificate Signing Certificate**（删除自定义 SSL 证书签名证书）并单击 **Next**（下一步）。

3. 将会显示一条弹出消息，要求您立即或稍后重设 iDRAC。根据需要，单击 **Reset iDRAC（重设 iDRAC）**或 **Reset iDRAC Later（稍后重设 iDRAC）**。
   重设 iDRAC 之后，将会生成新的自签名证书。

使用 RACADM 删除自定义 SSL 证书签名证书

要使用 RACADM 删除自定义 SSL 证书签名证书，请使用 `sslcertdelete` 子命令。然后使用 `racreset` 命令重设 iDRAC。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 RACADM 配置多个 iDRAC

您使用 RACADM 可以配置一个或多个具有相同属性的 iDRAC。当您使用其组 ID 和对象 ID 查询特定 iDRAC 时，RACADM 会根据检索到的信息创建 .cfg 配置文件。将文件导入其他 iDRAC，以采用相同的方式来进行配置。

注:

- 配置文件包含适用于特定服务器的信息。这些信息在不同的对象组下进行组织。
- 少数配置文件包含唯一的 iDRAC 信息，例如静态 IP 地址，您必须修改此信息然后才能将文件导入到其他 iDRAC。

您还可以借助 RACADM 使用系统配置配置文件 (SCP) 配置多个 iDRAC。SCP 文件包含组件配置信息。您可以使用此文件通过文件导入目标系统来应用 BIOS、iDRAC、RAID 和 NIC 的配置。有关更多信息，请参阅 *XML 配置工作流程*白皮书，网址：https://www.dell.com/manuals。

要使用配置文件配置多个 iDRAC：

1. 使用以下命令查询包含所需配置的的目标 iDRAC：

   ```
   racadm get -f <file_name>.xml -t xml -c iDRAC.Embedded.1
   ```

   该命令要求 iDRAC 配置并生成配置文件。

   注: 使用 `get -f` 将 iDRAC 配置重定向至文件仅在本地和远程 RACADM 界面中受支持。

   注: 生成的配置文件不包含用户密码。

   `get` 命令显示组（通过组名称和索引指定）中的所有配置属性并显示用户的所有配置属性。

2. 使用文本编辑器修改配置文件（如果需要）。

   注: 建议使用简单文本编辑器编辑此文件。RACADM 公用程序使用 ASCII 文本分析器。任何格式化操作都会干扰分析器并可能损坏 RACADM 数据库。

3. 在目标 iDRAC 上使用以下命令修改设置：

   ```
   racadm set -f <file_name>.xml -t xml
   ```

   这会将信息加载到其他 iDRAC。您可以使用 `set` 子命令将用户和密码数据库与 Server Administrator 同步。
4. 使用以下命令重设目标 iDRAC：`racadm racreset`

禁用访问以修改主机系统上的 iDRAC 配置设置

您可以禁用访问以通过本地 RACADM 或 iDRAC 设置公用程序修改 iDRAC 配置设置。但是，您可以查看这些配置设置。要执行此操作：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Services（服务）** > **Local Configurations（本地配置）**。
2. 选择以下两项之一或两者：
   - **Disable the iDRAC Local Configuration using iDRAC Settings（使用 iDRAC 设置禁用 iDRAC 本地配置）** — 在 iDRAC 设置公用程序中禁用访问以修改配置设置。
   - **Disable the iDRAC Local Configuration using RACADM（使用 RACADM 禁用 iDRAC 本地配置）** — 在本地 RACADM 中禁用访问以修改配置设置。

3. 单击**应用**。

注: 如果访问已禁用，您将无法使用 Server Administrator 或 IPMITool 执行 iDRAC 配置。但是，您可以使用 LAN 上 IPMI。

5

使用 OAuth 2.0 的委派授权

通过委派授权功能，用户或控制台可以使用首先从授权服务器获取的 OAuth 2.0 JSON Web 令牌 (JWT) 访问 iDRAC API。一旦 OAuth JWT 被检索，用户或控制台就可以使用它调用 iDRAC API。这样无需指定用户名和密码就可访问 API。

注: 此功能□适用于数据中心□可□。您需要具有配置 iDRAC 或配置用□权限才能使用此功能。

iDRAC 支持配置最多 2 个授权服务器。配置要求用户指定以下授权服务器详细信息：

- **名称** — 标识 iDRAC 上的授权服务器的字符串。
- **元数据 URL** — 服务器通告的 OpenID Connect 兼容 URL。
- **HTTPS 证书** — iDRAC 应用于与服务器通信的服务器公钥。
- **离线密钥** — 授权服务器的 JWK 设置文档。
- **离线颁发者** — 授权服务器所颁发的令牌中使用的颁发者字符串。

对于联机配置：

- 在配置授权服务器时，iDRAC 管理员需要确保 iDRAC 具有对授权服务器的在线网络访问权限。
- 如果 iDRAC 无法访问授权服务器，配置将失败，并且即使显示有效的令牌，随后尝试访问 iDRAC API 也会失败。

对于离线配置：

- iDRAC 不需要与授权服务器进行通信，而是使用其已离线下载的元数据详细信息进行配置。当进行离线配置时，iDRAC 拥有签名密钥的公共部分，并且可以在没有到授权服务器的网络连接的情况下验证令牌。

6

查看 iDRAC 和受管系统信息

您可以查看 iDRAC 和受管系统的运行状况和属性、硬件和固件资源清册、传感器运行状况、存储设备、网络设备以及查看和终止用户会话。对于刀片服务器，您还可以查看 Flex 地址或远程分配地址（仅适用于 MX 平台）。

主□：

- □看受管系□运行状况和属性
- 配置□□跟踪
- □看系□□源清册
- □看□感器信息
- □□ CPU、内存和□入□出模□的性能指□
- 空□服□器□□
- GPU (Accelerators) Management
- □□系□的新□空气符合性
- □看□史温度数据
- □看主机操作系□上可用的网□接口
- 使用 RACADM □看主机操作系□上可用的网□接口
- □看 FlexAddress 夹□卡光□□接
- □看或□止 iDRAC 会□

查看受管系统运行状况和属性

在登录 iDRAC Web 界面时，通过**系统摘要**页面可以查看受管系统的运行状况和 iDRAC 的基本信息，预览虚拟控制台，添加和查看工作注释，以及快速启动任务（如打开或关闭、重启、查看日志、更新和回滚固件、打开或关闭前面板 LED 以及重设 iDRAC 等）。

要访问**系统摘要**页面，请转至**系统** > **概览** > **摘要**。随即会显示 **System Summary**（系统摘要）页面。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

您还可以使用 iDRAC 设置公用程序查看基本系统摘要信息。要实现这一点，请在 iDRAC 设置公用程序中转至**系统摘要**。随即会显示 **iDRAC Settings System Summary**（iDRAC 设置系统摘要）页面。有关更多信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。

配置资产跟踪

iDRAC 中的“资产跟踪”功能使您能够配置与服务器相关的各种属性。这包括诸如采购、保修、服务之类的信息。

注: iDRAC 中的“资产跟踪”类似于 OpenManage Server Administrator 中的“资产标签”功能。但是，必须在这两个工具中单独输入属性信息，以让它们报告相关的资产数据。

要配置“资产跟踪”，请执行以下操作：

1. 在 iDRAC 界面中，转至**配置** > **资产跟踪**。
2. 单击**添加自定义资产**，以添加默认情况下未在此页面上指定的任何附加属性。
3. 输入服务器资产的所有相关信息，然后单击**应用**。
4. 要查看“资产跟踪报告”，请转至**系统详细信息** > > **资产跟踪**。

查看系统资源清册

您可以查看有关管理系统上安装的硬件和固件组件的信息。要执行此操作，在 iDRAC Web 界面中，请转至**系统** > **资源清册**。有关所显示的属性的信息，请参阅 *iDRAC 联机帮助*。

硬件资源清册部分显示管理系统中以下可用组件的信息：

- iDRAC
- RAID 控制器
- 电池
- CPU
- DIMM
- HDD
- 背板
- 网络接口卡（集成式和嵌入式）
- 视频卡
- SD 卡
- 电源设备 (PSU)
- 风扇
- 光纤信道 HBA
- USB
- NVMe PCIe SSD 设备

固件资源清册部分显示以下组件的固件版本：

- BIOS
- Lifecycle Controller
- iDRAC
- 操作系统驱动程序包
- 32 位诊断程序
- 系统 CPLD
- PERC 控制器
- 电池
- 物理磁盘
- 电源
- NIC
- 光纤通道
- 背板
- 机柜
- PCIe SSD

注：

- 软件资源清册仅显示固件版本的最后 4 个字节和版本日期信息。例如，如果固件版本是 FLVDL06，则固件资源清册会显示 DL06。
- 使用 Redfish 界面收集软件资源清册时，仅针对支持回滚的组件显示版本日期信息。

注： 在 Dell PowerEdge FX2/FX2s 服务器上，iDRAC GUI 中显示的 CMC 版本的命名约定与 CMC GUI 中显示的版本不同。不过，仍然是同一版本。

当您更换任何硬件组件或更新固件版本时，请确保启用并运行**重新引导时收集系统资源清册** (CSIOR) 选项以在重新引导时收集系统资源清册。几分钟后，登录 iDRAC，然后导航至**系统资源清册**页面查看详细信息。信息可能需要长达 5 分钟才能可用，具体视服务器上安装的硬件而定。

注： CSIOR 选项在默认情况下已启用。

注： 执行服务器重启之前，在操作系统内所做的配置更改和固件更新可能不会正确地反映在资源清册中。

单击**导出**可将硬件资源清册以 XML 格式导出并保存到选定位置。

查看传感器信息

下列传感器可用于监测受管系统的运行状况：

- **电池** - 提供关于系统板 CMOS 和主板存储 RAID (ROMB) 上电池的信息。
  注： 只有当系统具有包含电池的 ROMB 时，存储 ROMB 电池设置才可用。
- **风扇**（仅适用于机架式和塔式服务器）- 提供关于系统风扇的信息，包括风扇冗余和显示风扇速度和阈值的风扇列表。
- **CPU** - 指示受管系统中 CPU 的运行状况和状态。它还报告处理器自动调节和预测性故障。

- **内存** - 指示受管系统中存在的双列直插式内存模块 (DIMM) 的运行状况和状态。
- **侵入** - 提供有关机箱的信息。
- **电源设备**（仅适用于机架式和塔式服务器）- 提供关于电源设备和电源设备冗余状态的信息。

  注: 如果系统中只有一个电源设备，则会将电源设备冗余设置为**已禁用**。
- **可移动闪存介质** - 提供关于内部 SD 模块（vFlash 和内部双 SD 模块 (IDSDM)）的信息。
  - 如果启用 IDSDM 冗余，则会显示以下 IDSDM 传感器状态 — IDSDM 冗余状态、IDSDM SD1、IDSDM SD2。禁用冗余时，仅显示 IDSDM SD1。
  - 如果当系统开机或 iDRAC 重设后，IDSDM 冗余最初处于禁用状态，IDSDM SD1 传感器状态仅在插入卡后才会显示。
  - 如果启用 IDSDM 冗余且 IDSDM 中存在两个 SD 卡，并且其中一个 SD 卡的状态是联机，而另一个卡的状态是脱机。您需要重新引导系统才能恢复 IDSDM 中两个 SD 卡之间的冗余性。恢复冗余性后，IDSDM 中两个 SD 卡的状态都会变成联机。
  - 在重建操作以恢复 IDSDM 中两个 SD 卡之间的冗余性时，由于 IDSDM 传感器已关闭，因此不会显示 IDSDM 状态。

    注: 如果主机系统在 IDSDM 重建操作期间重新引导，iDRAC 将不会显示 IDSDM 信息。要解决此问题，请再次重建 IDSDM 或者重设 iDRAC。
  - 在 IDSDM 模块中，具有写保护或损坏的 SD 卡的系统事件日志 (SEL) 不会重复，除非使用可写或良好的 SD 卡分别进行更换而将日志清除。

  注: 当 iDRAC 固件从 3.30.30.30 之前的版本更新时，iDRAC 需要重置为默认值，以便 IDSDM 设置显示在 Server Administrator 的平台事件过滤器中。
- **温度** - 提供关于系统板入口温度和排气温度（仅适用于机架式服务器）的信息。温度探测器会指示探测器的状态是否位于预设的警告和严重阈值范围内。
- **电压** - 指示多个系统组件上电压传感器的状态和读数。

下表提供有关利用 iDRAC Web 界面和 RACADM 查看传感器信息的信息。有关在 Web 界面上显示的属性的信息，请参阅 *iDRAC 联机帮助*。

注: 硬件概□□面□□示系□上呈□的□感器的数据。

表. 17: 使用 Web 界面和 RACADM 的传感器信息

查看传感器信息	使用 Web 界面	使用 RACADM
电池	**仪表板** > **系统运行状况** > **电池**	使用 `getsensorinfo` 命令。 对于电源设备，您还可以使用 `System.Power.Supply` 命令和 `get` 子命令。 有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。
Fan	**仪表板** > > **系统运行状况** > **风扇**	
CPU	**仪表板** > **系统运行状况** > **CPU**	
内存	**仪表板** > **系统运行状况** > **内存**	
侵入	**仪表板** > **系统运行状况** > **侵入**	
电源设备	> **硬件** > **电源设备**	
可移除闪存介质	**仪表板** > **系统运行状况** > **可移动闪存介质**	
温度	**仪表板** > **系统运行状况** > **电源/散热** > **温度**	
电压	**仪表板** > **系统运行状况** > **电源/散热** > **电压**	

监测 CPU、内存和输入输出模块的性能指标

在第 14 代 Dell PowerEdge 服务器中，Intel ME 支持每秒计算单位 (CUPS) 的功能。CUPS 功能可实时监测系统的 CPU、内存和 I/O 使用情况以及系统级利用率指标。Intel ME 允许带外 (OOB) 性能监视，并且不会占用 CPU 资源。Intel ME 具有系统 CUPS

传感器，能够以“CUPS 指标”的形式提供计算、内存和 I/O 资源利用率的值。iDRAC 监测整体系统利用率的 CUPS 指数，还监测 CPU、内存和 I/O 的瞬时利用率指数。

注： CUPS 功能在以下服□器上不受支持：

- PowerEdge R240
- PowerEdge R240xd
- PowerEdge R340
- PowerEdge R6415
- PowerEdge R7415
- PowerEdge R7425
- PowerEdge T140

CPU 和芯片组具有专用的资源监视计数器 (RMC)。查询这些 RMC 中的数据以获得系统资源的利用率信息。这些 RMC 数据由节点管理器汇总，以度量其中每个系统资源的累积利用率（使用现有内部通信机制从 iDRAC 读取，从而通过带外管理接口提供这些重要数据）。

Intel 传感器提供的性能参数和索引值对应的是完整物理系统。因此界面上的性能数据表示对应于整个物理系统，即使系统已虚拟化系统并托管多个虚拟主机也是如此。

要显示性能参数，服务器上必须存在受支持的传感器。

四个系统利用率参数包括：

- **CPU 利用率** — 针对每个 CPU 核心的 RMC 的数据进行聚合，以提供系统中所有核心的累积利用率。此利用率基于处于活动状态的时间和处于非活动状态的时间。每六秒钟收集一个 RMC 样本。
- **内存利用率** - RMC 衡量每个内存通道或内存控制器实例上发生的内存流量。这些 RMC 聚合起来的数据衡量系统上所有内存通道的累计内存流量。其衡量的是内存带宽占用量，而非内存利用量。iDRAC 每隔一分钟聚合一次计数器，因此，它与其他操作系统工具（如 Linux 中的 **top**）所显示的内存利用率可能一致，也可能不一致。iDRAC 显示的内存带宽利用率将指示工作负载是否为内存密集型工作负载。
- **I/o 利用率** —PCI Express Root Complex 中的每个根端口有一个 RMC，以测量从根端口和更低段传出或传入的 PCI Express 流量。将聚合这些 RMC 中的数据以测量从软件包传出的所有 PCI Express 段的 PCI Express 流量。这是系统的 I/O 带宽利用率度量。
- **系统级 CUPS 指标** - CUPS 指标是根据每个系统资源的预先定义的负载系数，通过聚合 CPU、内存和 I/O 指标而计算得出。负载系数取决于系统上工作负载的性质。CUPS 指标表示服务器上可用的计算资源的余量。因此，如果系统具有很高的 CUPS 指标值，则该系统上可用于额外工作负载的余量可能有限。随着资源消耗量减少，系统 CUPS 指标将降低。低 CUPS 指标值表明服务器上存在大量计算资源余量，因此该服务器可作为接收新工作负载或者迁移工作负载操作的主要目标，并置于较低功耗状态以降低功耗。然后，可在整个数据中心中应用此类工作负载监测，以提供数据中心工作负载的完整高级视图，从而提供动态数据中心解决方案。

注： CPU、内存和 I/O 利用率指□将一分□□行一次聚合。因此，如果在□些指□中存在任何瞬□峰□，□些峰□可能会□藏。它□用于表示工作□□模式而非□源利用量。

如果达到利用率指标阈值并且已启用传感器事件，将生成 IPMI、SEL 和 SNMP 陷阱。默认情况下，传感器事件标志已禁用。可使用标准 IPMI 接口启用该标志。

所需的权限包括：

- 监测性能数据时所需的登录权限。
- 设置警告阈值和重设历史峰值时所需的配置权限。
- 登录权限和企业版许可证需要读取历史静态数据。.

使用 Web 界面监测 CPU、内存和输入输出模块的性能指标

要在 iDRAC Web 界面中监测 CPU、内存和 I/O 模块的性能指标，请转至 **System（系统）** > **Performance（性能）**。

- **系统性能**部分 - 在图形视图中显示 CPU、内存和 I/O 利用率指标和系统级 CUPS 指标的当前读数及警告读数。
- **系统性能历史数据**部分：
  - 提供 CPU、内存、IO 利用率以及系统级 CUPS 指数的统计数据。如果主机系统已关闭，则图表将显示低于 0% 的关机线。
  - 您可以重设特定传感器的峰值利用率。单击 **Reset Historical Peak（重设历史峰值）**。您必须具有“配置”权限才能重设峰值。
- **性能指标**部分：
  - 显示状态和当前读数
  - 显示或指定警告性利用率阈值限制。您必须具有服务器配置权限才能设置此阈值。

有关所显示的属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 监测 CPU、内存和输入输出模块的性能指标

使用 **SystemPerfStatistics** 子命令监测 CPU、内存和 I/O 模块的性能指标。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

空闲服务器检测

iDRAC 提供服务器组件（如 CPU、内存和 I/O）的带外性能监测索引。

服务器级别 CUPS 索引的历史记录数据用于监测服务器是否在长时间使用或处于空闲状态。如果服务器在定义的时间间隔（以小时为单位）内未充分利用且利用率低于特定阈值，则将其报告为空闲服务器。

此功能仅在具有 CUPS 功能的 Intel 平台上受支持。无 CUPS 功能的 AMD 和 Intel 平台不支持此功能。

注：
- 此功能需要 Datacenter 许可证。
- 要读取空闲服务器配置参数的配置，您需要登录权限并修改您需要 iDRAC 配置权限的参数。

要查看或修改参数，请导航至**配置** > **系统设置**。

根据以下参数报告空闲服务器检测：
- 空闲服务器阈值 (%) — 默认设置为 20%，并且可配置为 0% 到 50%。重置操作会将阈值设置为 20%。
- 空闲服务器扫描间隔（以小时为单位）— 这是收集每小时采样的时间段，用于确定空闲服务器。默认设置为 240 小时，并且可配置为 1 到 9000 小时。重置操作会将时间间隔设置为 240 小时。
- 服务器利用率百分比 (%) — 利用率百分比值可设置为 80% 至 100%。默认值是 80%。如果 80% 的每小时样本都低于利用率阈值，则将其视为空闲服务器。

使用 RACADM 修改空闲服务器检测参数

```
racadm get system.idleServerDetection
```

使用 Redfish 修改闲置服务器检测参数

```
https://<iDRAC IP>/redfish/v1/Managers/System.Embedded.1/Attributes
```

使用 WSMAN 修改闲置服务器检测参数

```
winrm e http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_SystemAttribute
-u:root -p:calvin -r:https://<iDRAC IP>/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8
-a:basic
```

注： iDRAC GUI 不支持查看或修改属性。

GPU (Accelerators) Management

Dell PowerEdge servers are shipped with Graphics Processing Unit (GPU). GPU management enables you to view the various GPUs connected to the system and also monitor power, temperature, and thermal information for the GPUs.

NOTE: This is a licensed feature and is available only with iDRAC Datacenter and Enterprise licenses. Below properties require Datacenter/Enterprise license, other properties are listed even without these license:
- **Thermal Metrics:**

- GPU Target Temperature
- Minimum GPU HW Slowdown Temperature
- GPU Shutdown Temperature
- Maximum Memory Operating temperature
- Maximum GPU Operating Temperature
- Thermal Alert State
- Power Brake State

- **Power Metrics:**
  - Power Supply Status
  - Board Power Supply Status
- **Telemetry** — All GPU telemetry reports data

NOTE: GPU properties will not be listed for Embedded GPU cards and the Status is marked as **Unknown**.

GPU has to be in ready state before the command fetches the data. GPUStatus field in Inventory shows the availability of the GPU and whether GPU device is responding or not. If the GPU status is ready, GPUStatus shows OK, otherwise the status shows Unavailable.

The GPU offers multiple health parameters which can be pulled through the SMBPB interface of the NVIDIA controllers. This feature is limited only to NVIDIA cards. Following are the health parameters retrieved from the GPU device:

- Power
- Temperature
- Thermal

NOTE: This feature is only limited to NVIDIA cards. This information is not available for any other GPU that the server may support. The interval for polling the GPU cards over the PBI is 5 seconds.

The host system must have the NVIDIA driver installed and running for the Power consumption, GPU target temperature, Min GPU slowdown temperature, GPU shutdown temperature, Max memory operating temperature, and Max GPU operating temperature features to be available. These values are shown as **N/A** if the GPU driver is not installed.

In Linux, when the card is unused, the driver down-trains the card and unloads in order to save power. In such cases, the Power consumption, GPU target temperature, Min GPU slowdown temperature, GPU shutdown temperature, Max memory operating temperature, Max memory operating temperature, and Max GPU operating temperature features are not available. Persistent mode should be enabled for the device to avoid unload. You can use nvidia-smi tool to enable this using the command `nvidia-smi -pm 1`.

You can generate GPU reports using Telemetry. For more information on telemetry feature, see 遥□流式□□ on page 193

NOTE: In Racadm, You may see dummy GPU entries with empty values. This may happen if device is not ready to respond when iDRAC queries the GPU device for the information. Perform iDRAC `racrest` operation to resolve this issue.

FPGA Monitoring

Field-programmable Gate Array (FPGA) devices needs real-time temperature sensor monitoring as it generates significant heat when in use. Perform the following steps to get FPGA inventory information:

- Power off the server.
- Install FPGA device on the riser card.
- Power on the server.
- Wait until POST is complete.
- Login to iDRAC GUI.
- Navigate to **System** > **Overview** > **Accelerators**. You can see both GPU and FPGA sections.
- Expand the specific FPGA component to see the following sensor information:
  - Power consumption
  - Temperature details

NOTE: You must have iDRAC Login privilege to access FPGA information.

NOTE: Power consumption sensors are available only for the supported FPGA cards and is available only with Datacenter license.

检查系统的新鲜空气符合性

新鲜空气冷却直接使用外部空气冷却数据中心中的系统。符合新鲜空气标准的系统可以在高于其正常环境工作范围的条件下运行（温度高达 113°F [45° C]）。

注: 某些服务器或服务器配置可能不符合新鲜空气标准。请参阅具体的服务器手册，了解与新鲜空气符合性相关的详细信息，或者联系 Dell 以获得更多详细信息。

要检查系统的新鲜空气符合性：

1. 在 iDRAC Web 界面中，转至 **System（系统）** > **Overview（概览）** > **Cooling （散热）** > **Temperature overview（温度概览）**。
   此时会显示 **Temperature overview（温度概览）**页面。
2. 查看**新鲜空气**部分，该部分指示服务器是否具有新鲜空气符合性。

查看历史温度数据

您可以监测系统在超过正常支持的新鲜空气温度阈值的环境温度下运行的时间百分比。过一段时间即获取系统板温度传感器读数，以监测温度。系统出厂后，首次打开电源时便开始收集数据。只要系统通电，就一直收集并显示数据。您可以跟踪和存储过去七年监测的温度。

注: 您甚至可以跟踪不具有新□空气符合性的系□的入口温度□史。但是，与□□限制和新□空气相关的警告将基于新□空气支持的限制生成。限制□ 42ºC □行警告，47ºC □□重□。□些□与 40ºC 和 45ºC 新□空气限制□□，偏差 2ºC 以确保准确性。

将跟踪两个与新鲜空气限制关联的固定温度范围：

- 警告带 — 包含系统在超过温度传感器警告阈值 (42ºC) 的情况下运行的持续时间。系统可以在 12 个月时间的 10% 的警告带内操作。
- 严重带 — 包含系统在超过温度传感器严重阈值 (47ºC) 的情况下运行的持续时间。系统可以在 12 个月时间的 1% 的严重带内操作，也可以在警告带内增长。

收集的数据以图形化形式跟踪以表示 10% 和 1% 级别。只能在从工厂发货之前清除所记录的温度数据。

如果系统继续在支持的正常温度阈值上运行指定的可运行时间，将生成事件。如果超过指定的运行时间的平均温度大于或等于警告级别 (>= 8%) 或严重级别 (>= 0.8%)，则会在生命周期日志中记录事件，并生成相应的 SNMP 陷阱。事件：

- 当在过去 12 个月内，温度大于警告阈值的持续时间大于或等于 8% 时，将生成警告事件。
- 当在过去 12 个月内，温度大于警告阈值的持续时间大于或等于 10% 时，将生成严重事件。
- 当在过去 12 个月内，温度大于严重阈值的持续时间大于或等于 0.8% 时，将生成警告事件。
- 当在过去 12 个月内，温度大于严重阈值的持续时间大于或等于 1% 时，将生成严重事件。

您还可以配置 iDRAC 以生成附加事件。有关更多信息，请参阅 设置警报复现事件 页面上的 163 部分。

使用 iDRAC Web 界面查看历史温度数据

查看历史温度数据：

1. 在 iDRAC Web 界面中，转至**系统** > **概览** > **冷却** > **温度概览**。
   此时会显示**温度概览**页面。
2. 请参阅**系统板温度历史数据**部分，其中提供了过去一天、过去 30 天和过去一年中存储的温度（平均值和峰值）的图形显示。
   有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

   注: 在执行 iDRAC 固件更新或 iDRAC 重设之后，某些温度数据可能不会显示在图表中。

   注: WX3200 AMD GPU 卡当前不支持温度传感器的 I2C 接口。因此，此卡的温度读数无法从 iDRAC 界面获得。

使用 RACADM 查看历史温度数据

要使用 RACADM 查看历史数据，请使用 `inlettemphistory` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

配置入口温度的警告阈值

您可以修改系统板入口温度传感器的最小和最大警告阈值。如果重设为默认操作，则温度阈值将设置为默认值。您必须具有"配置"用户权限，才能设置入口温度传感器的警告阈值。

使用 Web 界面配置入口温度警告阈值

要配置入口温度警告阈值，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**系统** > **概览** > **冷却** > **温度概览**。
   此时会显示**温度概览**页面。
2. 在**温度探测器**部分，在**系统板进气孔温度**中以摄氏度或华氏度输入**警告阈值**的最小和最大值。如果您输入摄氏度值，系统将自动计算的并显示华氏度值。与此类似，如果您输入华氏度值，系统也会显示摄氏度值。
3. 单击**应用**。
   值已配置。

   注: 默认阈值的更改不会反映在历史数据图表中，因为图表限制仅针对新鲜空气限制值。超出自定义阈值的警告不同于有关超出新鲜空气阈值的警告。

查看主机操作系统上可用的网络接口

您可以查看有关主机操作系统上可用的所有网络接口的信息，例如已分配给服务器的 IP 地址。iDRAC Service Module 向 iDRAC 提供此信息。操作系统 IP 地址信息包括 IPv4 和 IPv6 地址、MAC 地址、子网掩码或前缀长度、网络设备的 FQDD、网络接口名称、网络接口描述、网络接口状态、网络接口类型（以太网、隧道、回路等）、网关地址、DNS 服务器地址和 DHCP 服务器地址。

注: 此功能随 iDRAC Express 和 iDRAC Enterprise/Datacenter □可□提供。

要查看操作系统信息，请确保满足以下要求：

- 您具有"登录"权限。
- iDRAC Service Module 已在主机操作系统上安装并正在运行。
- 已在 **iDRAC 设置** > **概览** > **iDRAC Service Module** 页面中启用"操作系统信息"选项。

iDRAC 可显示主机操作系统上已配置的所有接口的 IPv4 和 IPv6 地址。

相应的 IPv4 或 IPv6 DHCP 服务器地址不一定会显示，这取决于主机操作系统如何检测 DHCP 服务器。

使用 Web 界面查看主机操作系统上可用的网络接口

要使用 Web 界面查看主机操作系统上可用的网络接口，请执行以下操作：

1. 转至 **System（系统）** > **Host OS（主机操作系统）** > **Network Interfaces（网络接口）**。
   网络接口页面将显示主机操作系统上所有可用的网络接口。
2. 要查看与网络设备关联的网络接口的列表，请从**网络设备 FQDD** 下拉菜单中选择网络设备并单击**应用**。
   将在**主机操作系统的网络接口**部分中显示操作系统的 IP 详细信息。
3. 从**设备 FQDD** 列中，单击网络设备的链接。
   相应的设备页面将会显示从 **Hardware（硬件）** > **Network Devices（网络设备）**部分显示，您可以在其中查看设备的详细信息。有关属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击 + 显示更多详细信息。
   同样，可以从 **Hardware（硬件）** > **Network Devices（网络设备）**页面中查看与网络设备关联的主机操作系统的网络接口信息。单击 **View Host OS Network Interfaces（查看主机操作系统网络接口）**。

   注: 对于 iDRAC Service Module v2.3.0 或更高版本中的 ESXi 主机操作系统，**Additional Details（附加详细信息）**列表中的 **Description（描述）**列采用以下格式显示：

   ```
   <List-of-Uplinks-Configured-on-the-vSwitch>/<Port-Group>/<Interface-name>
   ```

使用 RACADM 查看主机操作系统上可用的网络接口

可以使用 RACADM 通过 `gethostnetworkinterfaces` 命令查看主机操作系统上可用的网络接口。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

查看 FlexAddress 夹层卡光纤连接

在刀片式服务器中，FlexAddress 允许为每个受管服务器端口连接使用永久、机箱分配的全球名称和 MAC 地址 (WWN/MAC)。

您可以查看每个安装的嵌入式以太网和可选夹层卡端口的以下信息：

- 卡连接到的光纤。
- 光纤类型。
- 服务器分配的、机箱分配的或远程分配的 MAC 地址。

要查看 iDRAC 中的 Flex Address 信息，请在 Chassis Management Controller (CMC) 上配置和启用 Flex Address 功能。有关更多信息，请参阅 机箱管理控制器用户指南，*网址：*https://www.dell.com/cmcmanuals。如果启用或禁用 FlexAddress 设置，则任何现有虚拟控制台或虚拟介质会话会终止。

注： 要避免可能□致无法开启受管系□的□□，每个端口和光□□接都*必须*安装正确类型的夹□卡。

FlexAddress 功能会使用机箱分配的 MAC 地址更换服务器分配的 MAC 地址，并且与刀片式 LOM、夹层卡和 I/O 模块一起为 iDRAC 实施。iDRAC FlexAddress 功能支持为机箱中的 iDRAC 保留插槽特定的 MAC 地址。机箱分配的 MAC 地址存储在 CMC 非易失性存储器中，并且在 iDRAC 引导过程中或当已启用 CMC FlexAddress 时，将该 MAC 地址发送到 iDRAC。

如果 CMC 启用机箱分配的 MAC 地址，iDRAC 会显示下列任何页面上的 **MAC 地址**：

- **系统详细信息 iDRAC 详细信息。**
- **系统服务器 WWN/MAC。**
- **iDRAC 设置** > **概览** > **当前网络设置。**

小心：启用 FlexAddress 后，如果从服□器分配的 MAC 地址切□到机箱分配的 MAC 地址或者相反，iDRAC IP 地址也会□化。

查看或终止 iDRAC 会话

您可以查看当前登录到 iDRAC 的用户数以及终止用户会话。

使用 Web 界面终止 iDRAC 会话

没有管理权限的用户必须先具备“配置 iDRAC”权限才能使用 iDRAC Web 界面终止 iDRAC 会话。

要查看和终止 iDRAC 会话：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **users（用户）** > **Sessions（会话）**。
   Sessions（会话）页面会显示会话 ID、用户名、IP 地址和会话类型。有关这些属性的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
2. 要终止会话，在 **Terminate（终止）**列下，单击会话的回收站图标。

使用 RACADM 终止 iDRAC 会话

您必须具有管理员权限才能使用 RACADM 终止 iDRAC 会话。

要查看当前用户会话，请使用 `getssninfo` 命令。

要终止用户会话，请使用 `closessn` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

7

设置 iDRAC 通信

可以使用下列模式之一与 iDRAC 通信：

- iDRAC Web 界面
- 使用 DB9 电缆（RAC 串行或 IPMI 串行）进行串行连接 - 仅适用于机架式服务器和塔式服务器。
- IPMI LAN 上串行
- LAN 上 IPMI
- 远程 RACADM
- 本地 RACADM
- 远程服务

注： 要确保本地 RACADM □入或□出命令可正常工作，□确保 USB 大容量存□主机在操作系□中已启用。有关启用 USB 存□主机的信息，□参□操作系□的□明文件。

T 下表概述了支持的协议、支持的命令和先决条件：

表. 18: 通信模式 - 摘要

通信模式	支持的协议	支持的命令	先决条件
iDRAC Web 界面	Internet 协议 (https)	不适用	网络服务器
使用串行通信 DB9 电缆的串行接□	串行协议	RACADM IPMI	iDRAC 固件的组成部分 RAC 串行或 IPMI 串行已启用
IPMI LAN 上串行	智能平台管理总线协议 SSH	IPMI	IPMITool 已安装且 IPMI LAN 上串行已启用
LAN 上 IPMI	智能平台管理总线协议	IPMI	IPMITool 已安装且 IPMI 设置已启用
远程 RACADM	https	远程 RACADM	远程 RACADM 已安装并启用
固件 RACADM	SSH	固件 RACADM	固件 RACADM 已安装并启用。
本地 RACADM	IPMI	本地 RACADM	本地 RACADM 已安装
远程服务 [1]	WSMan	WinRM (Windows) OpenWSMan (Linux)	WinRM 已安装 (Windows) 或 OpenWSMan 已安装 (Linux)
	Redfish	各种浏览器插件、CURL（Windows 和 Linux）、Python 请求和 JSON 模块	已安装插件、CURL、Python 模块。
[1] 有关更多信息，请参阅 *生命周期控制器用户指南，网址：* https://www.dell.com/idracmanuals。			

主□：

- 使用 DB9 □□通□串行□接与 iDRAC □行通信
- 使用 DB9 □□□在 RAC 串行和串行控制台之□切□
- 使用 IPMI SOL 与 iDRAC □行通信
- 使用 LAN 上 IPMI 与 iDRAC 通信
- 启用或禁用□程 RACADM
- 禁用本地 RACADM
- 启用受管系□上的 IPMI
- □ RHEL 6 引□期□的串行控制台配置 Linux
- 在 RHEL 7 中配置串行□端

- 支持的 SSH 加密方案

使用 DB9 电缆通过串行连接与 iDRAC 进行通信

您可以使用以下任何通信方法通过到机架和塔式服务器的串行连接执行系统管理任务：

- RAC 串行
- IPMI 串行 - 直接连接基本模式和直接连接终端模式

注： 对于刀片式服务器，通过机箱建立串行连接。有关更多信息，请参阅机箱管理控制器用户指南，*网址：* https://www.dell.com/cmcmanuals（不适用于 MX 平台）适用于 PowerEdge MX7000 机箱的 *OME - Modular* 用户指南，网址：https://www.dell.com/openmanagemanuals（适用于 MX 平台）。

要建立串行连接，请执行以下操作：

1. 配置 BIOS 以启用串行连接。
2. 将串行通信 DB9 电缆从管理站的串行端口连接到受管系统的外部串行连接器。

   注： 从 vConsole 或 GUI 中将服务器关闭电源后重启，以让任何波特率更改生效。

   注： 如果禁用了 iDRAC 串行连接身份验证，则对于波特率中的任何更改，都需要 iDRAC racreset。

3. 确保管理站的终端仿真软件配置用于使用以下任何一项的串行连接：
   - Xterm 中的 Linux Minicom
   - Hilgraeve 的 HyperTerminal Private Edition（版本 6.3）

   根据受管系统处于其引导过程中的位置，您可以看到开机自检屏幕或操作系统屏幕。这基于以下配置：SAC（适用于 Windows）和 Linux 文本模式屏幕（适用于 Linux）。
4. 在 iDRAC 中启用 RAC 串行连接或 IPMI 串行连接。

针对串行连接配置 BIOS

针对串行连接配置 BIOS：

注： 这仅适用于机架和塔式服务器中的 iDRAC。

1. 开启或重新启动系统。
2. 按 F2。
3. 转到 **System BIOS Settings（系统 BIOS 设置）** > **Serial Communication（串行通信）**。
4. 选择到 **Remote Access device（远程访问设备）**的 **External Serial Connector（外部串行连接器）**。
5. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
6. 按 Esc 键退出 **System Setup（系统设置）**。

启用 RAC 串行连接

在 BIOS 中配置串行连接后，在 iDRAC 中启用 RAC 串行。

注： □□适用于机架和塔式服□器中的 iDRAC。

使用 Web 界面启用 RAC 串行连接

启用 RAC 串行连接：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Network（网络）** > **Serial（串行）**。
   随即会显示**串行**页面。
2. 在 **RAC Serial（RAC 串行）**下，选择 **Enabled（已启用）**并指定属性的值。
3. 单击**应用**。
   RAC 串行设置已配置。

使用 RACADM 启用 RAC 串行连接

要使用 RACADM 启用 RAC 串行连接，请使用 `set` 命令和 `iDRAC.Serial` 组中的对象。

启用 IPMI 串行连接基本和终端模式

要启用 BIOS 到 iDRAC 的 IPMI 串行路由，请在以下任意模式的 iDRAC 中配置 IPMI 串行：

注: □□适用于机架和塔式服□器中的 iDRAC。

- IPMI 基本模式 — 支持程序访问的二进制接口，例如随 Baseboard Management Utility (BMU) 附带的 IPMI shell (ipmish)。例如，要通过 IPMI 基本模式使用 ipmish 打印系统事件日志，请运行以下命令：

  ```
  ipmish -com 1 -baud 57600 -flow cts -u <username> -p <password> sel get
  ```

  注: 默认 iDRAC 用户名和密码与系统徽章一起提供。
- IPMI 终端模式 — 支持从串行终端发送的 ASCII 命令。此模式支持作为十六进制 ASCII 字符键入的有限数量的命令（包括电源控制）和原始 IPMI 命令。它允许您在通过 SSH 或 Telnet 登录 iDRAC 时查看操作系统引导顺序上至 BIOS。您需要使用 `[sys pwd -x]` 从 IPMI 终端注销，以下是 IPMI 终端模式命令的示例。
  - `[sys tmode]`
  - `[sys pwd -u root calvin]`
  - `[sys health query -v]`
  - `[18 00 01]`
  - `[sys pwd -x]`

使用 Web 界面启用串行连接

确保禁用 RAC 串行接口以启用 IPMI 串行接口。

配置 IPMI 串行设置：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **Serial（串行）**。
2. 在 **IPMI Serial（RAC 串行）**下，指定属性的值。有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。

使用 RACADM 启用串行连接 IPMI 模式

要配置 IPMI 模式，请禁用 RAC 串行接口，然后启用 IPMI 模式.。

```
racadm set iDRAC.Serial.Enable 0
racadm set iDRAC.IPMISerial.ConnectionMode <n>
```

n=0 — 终端模式

n=1 — 基础模式

使用 RACADM 启用串行连接 IPMI 串行设置

1. 使用以下命令将 IPMI 串行连接模式更改为相应的设置。

   ```
   racadm set iDRAC.Serial.Enable 0
   ```

2. 使用命令设置 IPMI 串行波特率。

   ```
   racadm set iDRAC.IPMISerial.BaudRate <baud_rate>
   ```

参数	允许的值（单位：bps）
<baud_rate>	9600、19200、57600 和 115200。

3. 使用命令启用 IPMI 串行硬件流控制。

```
racadm set iDRAC.IPMISerial.FlowContro 1
```

4. 使用命令设置 IPMI 串行通道最小权限级别。

```
racadm set iDRAC.IPMISerial.ChanPrivLimit <level>
```

参数	权限级别
<level> = 2	用户
<level> = 3	操作员
<level> = 4	管理员

5. 确保串行 MUX（外部串行连接器）在 BIOS 设置程序中正确设置为远程访问设备以针对串行连接配置 BIOS。

有关这些属性的详细信息，请参阅 IPMI 2.0 规范。

IPMI 串行终端模式的附加设置

本节提供 IPMI 串行终端模式的其他配置设置。

使用 Web 界面配置 IPMI 串行终端模式的附加设置

要设置终端模式设置：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **Serial（串行）**。
   随即会显示 **Serial（串行）**页面。
2. 启用 IPMI 串行。
3. 单击 **Terminal Mode Settings（终端模式设置）**。
   随即会显示 **Terminal Mode Settings（终端模式设置）**页面。
4. 指定以下值：
   - Line Editing（行编辑）
   - Delete control（删除控制）
   - 回声控制
   - Handshaking Control（握手控制）
   - New Line Sequence（新行序列）
   - Input new line sequences（输入新行序列）

   有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
5. 单击**应用**。
   终端模式设置即配置完成。
6. 确保串行 MUX（外部串行连接器）在 BIOS 设置程序中正确设置为远程访问设备以针对串行连接配置 BIOS。

使用 RACADM 配置 IPMI 串行终端模式的附加设置

要配置终端模式设置，请使用 `set` 命令和 `idrac.ipmiserial` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 DB9 电缆时在 RAC 串行和串行控制台之间切换

iDRAC 支持 Esc 键序列，该序列操作允许在机架式和塔式服务器上的 RAC 串行接口通信与串行控制器之间切换。

从串行控制台切换到 RAC 串行

要在串行控制器模式中切换至 RAC 串行界面通信模式，请按 Esc+Shift, 9。

以上键序列会定向到 `iDRAC Login` 提示符（如果 iDRAC 设置为 RAC Serial [RAC 串行] 模式）或 Serial Connection（串行连接）模式，在该模式可以发送终端命令（如果 iDRAC 设置为 IPMI Serial Direct Connect Terminal Mode [IPMI 串行直接连接终端模式]）。

从 RAC 串行切换到串行控制台

要在 RAC 串行接口通信模式切换到串行控制台模式，请按 Esc+Shift, Q。

在终端模式下，要将连接切换为串行控制台模式，请按 Esc+Shift, Q。

在串行控制台模式下时，要返回终端模式用途，请按 Esc+Shift, 9。

使用 IPMI SOL 与 iDRAC 进行通信

IPMI LAN 上串行 (SOL) 允许通过 iDRAC 的专用或共享带外以太网管理网络来重定向受管系统中基于文本的控制台串行数据。使用 SOL，您可以执行以下操作：

- 远程访问操作系统而不会超时。
- 在 Windows 的紧急管理服务 (EMS) 或 Special Administrator Console (SAC) 上或 Linux Shell 中诊断主机系统。
- 开机自检过程中查看服务器的进度并重新配置 BIOS 设置程序。

设置 SOL 通信模式：

1. 配置串行连接的 BIOS。
2. 配置 iDRAC 以使用 SOL。
3. 启用支持的协议（SSH、IPMItool）。

针对串行连接配置 BIOS

注: 这仅适用于机架和塔式服务器中的 iDRAC。

1. 开启或重新启动系统。
2. 按 F2。
3. 转到 **System BIOS Settings（系统 BIOS 设置）** > **Serial Communication（串行通信）**。
4. 指定以下值：
   - Serial Communication（串行通信） — On With Console Redirection
   - Serial Port Address（串行端口地址） — COM2。
     注: 如果**串行端口地址**字段中的**串行设备 2** 也设置为 com1，那么可以将**串行通信**字段设置为**开启，通过 com1 进行串行重定向。**
   - External serial connector（外部串行连接器） -- Serial device 2（串行设备 2）
   - Failsafe Baud Rate（故障保护波特率） — 115200
   - Remote Terminal Type（远程终端类型） — VT100/VT220
   - Redirection After Boot（引导后重定向） – Enabled（启用）
5. 单击 **Back（下一步）**，然后单击 **Finish（完成）**。
6. 单击 **Yes（是）**以保存更改。
7. 按 <Esc> 键退出 **System Setup（系统设置）**。

   注: BIOS 屏幕以 25 x 80 的格式发送串行数据。用于调用 `console com2` 命令的 SSH 窗口必须设置为 25 x 80。然后，重定向的屏幕将可以正确显示。

   注: 如果引导加载程序或操作系统提供串行重定向（例如 GRUB 或 Linux），则 BIOS **Redirection After Boot（引导后重定向）**设置必须禁用。这可以避免多个组件访问串行端口时潜在的争用情况。

配置 iDRAC 以使用 SOL

您可以使用 Web 界面、RACADM 或 iDRAC 设置公用程序来指定 iDRAC 中的 SOL 设置。

使用 iDRAC Web 界面配置 iDRAC 以使用 SOL

配置 IPMI LAN 上串行 (SOL)：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）** > **Serial Over LAN（LAN 上串行）**。
   随即会显示 **Serial Over LAN（LAN 上串行）**页面。
2. 启用 SOL，指定各值，然后单击 **Apply（应用）**。
   IPMI SOL 设置即配置完成。
3. 要设置字符积累间隔时间和字符发送阈值，请选择 **Advanced Settings（高级设置）**。
   随即会显示 **Serial Over LAN Advanced Settings（LAN 上串行高级设置）**页面。
4. 指定各属性的值并单击 **Apply（应用）**。

   IPMI SOL 高级设置即配置完成。这些值有助于提升性能。

   有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 配置 iDRAC 以使用 SOL

配置 IPMI LAN 上串行 (SOL)：

1. 使用命令启用 IPMI LAN 上串行。

```
racadm set iDRAC.IPMISol.Enable 1
```

2. 使用命令更新 IPMI SOL 最低权限级别。

```
racadm set iDRAC.IPMISol.MinPrivilege <level>
```

参数	权限级别
<level> = 2	用户
<level> = 3	操作员
<level> = 4	管理员

注: 要激活 IPMI SOL，您必须具有 IMPI SOL 中定义的最低权限。有关更多信息，请参阅 IPMI 2.0 规范。

3. 使用命令更新 IPMI SOL 波特率。

```
racadm set iDRAC.IPMISol.BaudRate <baud_rate>
```

注: 要重定向 LAN 上串行控制台，请确保 SOL 波特率与受管系统的波特率完全相同。

参数	允许的值（单位：bps）
<baud_rate>	9600、19200、57600 和 115200。

4. 使用命令为每个用户启用 SOL。

```
racadm set iDRAC.Users.<id>.SolEnable 2
```

参数	说明
<id>	唯一的用户 ID

注: 要重定向 LAN 上串行控制台，请确保 SOL 波特率与受管系统的波特率完全相同。

启用支持的协议

支持的协议有 IPMI 和 SSH。

使用 Web 界面启用支持的协议

要启用 SSH，请转至 **iDRAC 设置** > **服务**，然后为 SSH 选择**已启用**。

要启用 IPMI，请转至 **iDRAC 设置** > **连接**，然后选择 **IPMI 设置**。请确保**加密密钥**值全为零，或者按退格键清除并将值更改为空字符。

使用 RACADM 启用支持的协议

要启用 SSH，请使用以下命令。

SSH

```
racadm set iDRAC.SSH.Enable 1
```

要更改 SSH 端口：

```
racadm set iDRAC.SSH.Port <port number>
```

您可以使用如下的工具：

- IPMItool（适用于使用 IPMI 协议）
- Putty/OpenSSH（适用于使用 SSH 协议）

使用 IPMI 协议的 SOL

基于 IPMI 的 SOL 公用程序和使用 RMCP+ 的 IPMItool 通过 UDP 数据报传输到端口 623。使用 IPMI 2.0 时，RMCP+ 提供改进的身份验证、数据完整性检查、加密以及承载多种有效载荷类型的功能。有关更多信息，请参阅 **http://ipmitool.sourceforge.net/manpage.html**。

RMCP+ 使用 40 个字符的十六进制字符串（字符 0-9、a-f 和 A-F）加密密钥进行身份验证。默认值为 40 个零组成的字符串。

必须使用加密密钥（密钥生成器密钥）对 RMCP+ 与 iDRAC 的连接进行加密。您可以使用 iDRAC Web 界面或 iDRAC 设置公用程序配置加密密钥。

要从 Management Station 使用 IPMItool 启动 SOL 会话：

注: 如有必要，您可以通过 **iDRAC 设置** > **服务**更改 SOL 超时。

1. 从 *Dell Systems Management Tools and Documentation* DVD 安装 IPMITool。
   有关安装说明，请参阅*《软件快速安装指南》*。
2. 在命令提示符窗口中（Windows 或 Linux），运行以下命令以从 iDRAC 开始 SOL：

   ```
   ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate
   ```

   该命令会将 Management Station 连接到受管系统的串行端口。
3. 要从 IPMItool 退出 SOL 会话，按下 ~，然后按下 .（句号）。

   注: 如果 SOL 会话未终止，请重设 iDRAC 并等待两分钟以便完成引导。

注: 从运行的 Windows 操作系统的客户端将大型输入文本复制到运行 Linux 操作系统的主机时，IPMI SOL 会话可能会终止。要避免会话突然终止，请将任何大型文本转换为基于 UNIX 的行末端。

注: 如果存在使用 RACADM 工具创建的 SOL 会话，则使用 IPMI 工具启动另一个 SOL 会话时将不会显示有关现有会话的任何通知或错误。

注: 由于 Windows 操作系统的设置，在启动后，通过 SSH 和 IPMI 工具连接的 SOL 会话可能会进入空白屏幕。请断开并重新连接 SOL 会话以返回 SAC 提示符。

使用 SSH 的 SOL

Secure Shell (SSH) 是用于执行到 iDRAC 的命令行通信的网络协议。您可以通过此接口解析远程 RACADM 命令。

SSH 改进了安全性。iDRAC 仅支持带有密码验证的 SSH 版本 2，并且默认已启用。iDRAC 同时最多支持两个到四个 SSH 会话。

注: 从 iDRAC 版本 4.40.00.00 开始，telnet 功能将被删除，因此任何相关属性注册表属性都将过时。虽然其中的一些属性在 iDRAC 中仍可用，以便与现有的控制台应用程序和脚本保持向后兼容性，但 iDRAC 固件会忽略相应的设置。

注: 建立 SSH 连接时，将显示一条安全消息“需要进一步进行身份验证”。即使 2FA 被禁用。

注: 对于 MX 平台来说，一个 SSH 会话将用于 iDRAC 通信。如果所有会话都在使用中，则 iDRAC 不会启动，直至出现空闲会话。

使用在 Management Station 上支持 SSH 的开源程序（例如 PuTTY 或 OpenSSH）连接到 iDRAC。

注: 从 Windows 上的 VT100 或 ANSI 终端仿真程序中运行 `OpenSSH`。在 Windows 命令提示符下运行 `OpenSSH` 会导致功能无法完全正常运行（即，某些键不响应并且不显示图形）。

使用 SSH 与 iDRAC 通信之前，请确保：

1. 配置 BIOS 以启用串行控制台。
2. 在 iDRAC 中配置 SOL。
3. 使用 iDRAC Web 界面或 RACADM 启用 SSH。

   SSH（端口 22）客户端 <--> WAN 连接 <--> iDRAC

   通过使用 SSH 协议且基于 IPMI 的 SOL，无需再使用额外的公用程序，因为串行到网络转换在 iDRAC 内进行。您使用的 SSH 控制台必须能够解释和响应来自受管系统的串行端口的数据。串行端口通常连接到仿真 ANSI 或 VT100/VT220 终端的 Shell 上。串行控制台会自动重定向至 SSH。

从 Windows 上的 Putty 使用 SOL

注: 如有必要，您可以通过 **iDRAC 设置** > **服务**更改 SSH 超时。

从 Windows Management Station 上的 Putty 启动 IPMI SOL：

1. 运行以下命令以连接到 iDRAC

   ```
   putty.exe [-ssh] <login name>@<iDRAC-ip-address> <port number>
   ```

   注: 端口号是可选的。仅当重新分配端口号时才需要该项。

2. 运行命令 `console com2` 或 `connect` 以启动 SOL 并引导受管系统。

   将打开从管理站到受管系统的、使用 SSH 协议的 SOL 会话。要访问 iDRAC 命令行控制台，请执行 Esc 键序列操作。Putty 和 SOL 连接行为：

   - 在开机自检过程中通过 putty 访问受管系统时，如果 putty 上的功能键和键盘选项设置为：
     - VT100+ — F2 通过，但 F12 无法通过。
     - ESC[n~ — F12 通过，但 F2 无法通过。
   - 在 Windows 中，如果紧急管理系统 (EMS) 控制台在主机重新引导后立即打开，则 Special Admin Console (SAC) 终端可能会损坏。退出 SOL 会话，关闭终端，打开另一个终端，然后使用相同的命令启动 SOL 会话。

注: 由于 Windows 操作系统的设置，在启动后，通过 SSH 和 IPMI 工具连接的 SOL 会话可能会进入空白屏幕。请断开并重新连接 SOL 会话以返回 SAC 提示符。

从 Linux 上的 OpenSSH 使用 SOL

从 Linux 管理站上的 OpenSSH 启动 SOL：

注: 如有必要，您可以通过 **iDRAC 设置** > **服务**更改默认 SSH 会话超时。

1. 启动 shell。
2. 使用以下命令连接到 iDRAC：ssh *<iDRAC-ip-address>* -l *<login name>*
3. 在命令提示符下输入以下命令之一启动 SOL：
   - `connect`
   - `console com2`

   这会将 iDRAC 连接到受管系统的 SOL 端口。一旦建立 SOL 会话后，iDRAC 命令行控制台将不可用。按照转义序列正确操作以打开 iDRAC 命令行控制台。一旦 SOL 会话连接后，转义序列也会在屏幕上打印。受管系统关闭时，建立 SOL 会话需要一些时间。

   注: 您可以使用控制台 com1 或控制台 com2 启动 SOL。重新引导服务器以建立连接。

   `console -h com2` 命令显示等待键盘输入或来自串行端口的新字符前串行历史记录缓冲区的内容。

   历史记录缓冲区的默认（和最大）大小为 8192 字符。您可以使用以下命令将此数值设置为较小的值：

   ```
   racadm set iDRAC.Serial.HistorySize <number>
   ```

4. 退出 SOL 会话以关闭活动的 SOL 会话。

在 iDRAC 命令行控制台中断开 SOL 会话连接

断开 SOL 会话连接的命令基于公用程序。仅当 SOL 会话完全终止时才能退出公用程序。

要断开 SOL 会话连接，请从 iDRAC 命令行控制台终止 SOL 会话：

- 要退出 SOL 重定向，按 Enter 键、Esc 键、T。
  SOL 会话将关闭。

如果公用程序中的 SOL 会话没有完全终止，则其他 SOL 会话可能不可用。要解决此问题，请在 Web 界面中的 **iDRAC 设置** > **连接性** > **LAN 上串行**下终止命令行控制台。

使用 LAN 上 IPMI 与 iDRAC 通信

您必须配置 iDRAC 的 LAN 上 IPMI 以启用或禁用对任何外部系统的 LAN 信道上的 IPMI 命令。如果未配置 LAN 上 IPMI，则外部系统无法使用 IPMI 命令与 iDRAC 服务器通信。

注: IPMI □□基于 Linux 的操作系□提供 IPv6 地址□□支持。

使用 Web 界面配置 LAN 上 IPMI

配置 LAN 上 IPMI：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Connectivity（连接）**。
   随即会显示**网络**页面。
2. 在 **IPMI Settings（IPMI 设置）**下，指定属性值，然后单击 **Apply（应用）**。

   有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

   LAN 上 IPMI 设置已配置。

使用 iDRAC 设置公用程序配置 LAN 上 IPMI

配置 LAN 上 IPMI：

1. 在 **iDRAC Settings Utility（iDRAC 设置公用程序）**中，转至 **Network（网络）**。
   将显示 **iDRAC Settings Network（iDRAC 设置网络）**页面。
2. 对于 **IPMI Settings（IPMI 设置）**，指定值。

   有关各选项的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   LAN 上 IPMI 设置已配置。

使用 RACADM 配置 LAN 上 IPMI

1. 启用 LAN 上 IPMI

   ```
   racadm set iDRAC.IPMILan.Enable 1
   ```

   注： 此设置可确定使用 LAN 上 IPMI 接口执行的 IPMI 命令。有关更多信息，请参阅 **intel.com** 上的 IPMI 2.0 规格。
2. 更新 IPMI 信道权限。

   ```
   racadm set iDRAC.IPMILan.PrivLimit <level>
   ```

参数	权限级别
<level> = 2	用户
<level> = 3	操作员
<level> = 4	管理员

3. 如果需要，设置 IPMI LAN 信道密钥。

   ```
   racadm set iDRAC.IPMILan.EncryptionKey <key>
   ```

参数	说明
<key>	20 个字符秘钥采用有效的十六进制格式。

注： iDRAC IPMI 支持 RMCP+ 协议。有关更多信息，请参阅 **intel.com** 上的 IPMI 2.0 规格。

启用或禁用远程 RACADM

您可以使用 iDRAC Web 界面或 RACADM 启用或禁用远程 RACADM：您可以并行运行最多五个远程 RACADM 会话。

注： 默□情况下，已启用□程 RACADM。

使用 Web 界面启用或禁用远程 RACADM

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Services（服务）**。
2. 在**远程 RACADM** 下，选择所需选项，然后单击**应用**。
   远程 RACADM 将根据选择启用或禁用。

使用 RACADM 启用或禁用远程 RACADM

注: 建议使用本地 RACADM 或固件 RACADM 运行这些命令。

- 要禁用远程 RACADM：

```
racadm set iDRAC.Racadm.Enable 0
```

- 要启用远程 RACADM：

```
racadm set iDRAC.Racadm.Enable 1
```

禁用本地 RACADM

默认情况下，本地 RACADM 已启用。要禁用，请参阅 禁用访问以修改主机系统上的 iDRAC 配置设置 页面上的 105。

启用受管系统上的 IPMI

在受管系统上，使用 Dell Open Manage Server Administrator 可启用或禁用 IPMI。有关更多信息，请参阅 *OpenManage Server Administrator 用户指南，网址：* https://www.dell.com/openmanagemanuals。

注: 自 iDRAC v2.30.30.30 或更高版本起，IPMI □于基于 Linux 的操作系□支持 IPv6 地址□□。

为 RHEL 6 引导期间的串行控制台配置 Linux

以下步骤特定于 Linux GRand Unified Bootloader (GRUB)。如果使用不同的引导加载程序，则需要类似的更改。

注: 在配置客户端 VT100 仿真窗口时，将显示重定向虚拟控制台的窗口或应用程序设置为 25 行 x 80 列以确保文本正确显示。否则，有些文本屏幕可能会出现乱码。否则，有些文本屏幕可能会出现乱码。

按照以下说明编辑 **/etc/grub.conf** 文件：

1. 找到文件的常规设置部分并添加以下内容：

```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```

2. 在内核行上追加两个选项：

```
kernel ............. console=ttyS1,115200n8r console=tty1
```

3. 禁用 GRUB 的图形界面并使用基于文本的界面。否则，GRUB 屏幕不会显示在 RAC 虚拟控制台中。要禁用图形界面，请注释以 `splashimage` 开始的行。

   以下示例提供了示例 **/etc/grub.conf** 文件，显示在此过程中说明的更改。

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sdal
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

```
title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. 要启用多个 GRUB 选项来通过 RAC 串行连接启动虚拟控制台会话，将以下行添加到所有选项：

```
console=ttyS1,115200n8r console=tty1
```

本例显示 `console=ttyS1,57600` 添加到了第一个选项。

注: 如果引导加载程序或操作系统提供串行重定向（例如 GRUB 或 Linux），则 BIOS **引导后重定向**设置必须禁用。这可以避免多个组件访问串行端口时潜在的争用情况。

允许在引导后登录到虚拟控制台

在文件 **/etc/inittab** 中，新增一行以在 COM2 串行端口上配置 `agetty`：

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

以下示例显示带有新增行的示例文件。

```
#inittab This file describes how the INIT process should set up
#the system in a certain run-level.
#Author:Miquel van Smoorenburg
#Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this)
#1 - Single user mode
#2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode
#4 - unused
#5 - X11
#6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
#System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
#Things to run in every runlevel.
ud::once:/sbin/update
ud::once:/sbin/update
#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few
#minutes of power left. Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have power installed and your
#UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
#Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
```

```
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

#Run xdm in runlevel 5
#xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

在文件 **/etc/securetty** 中，使用 COM2 的串行 tty 名称新增一行：

```
ttyS1
```

以下示例显示带有新增行的示例文件。

注： 使用中断键序列 (~B) 在串行控制台上使用 IPMI 工具执行 Linux **Magic SysRq** 键命令。

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

在 RHEL 7 中配置串行终端

在 RHEL 7 中配置串行终端，请执行以下操作：

1. 添加或更新以下行至 `/etc/default/grub`：

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8"
   ```

   ```
   GRUB_TERMINAL="console serial"
   ```

   ```
   GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1"
   ```

   `GRUB_CMDLINE_LINUX_DEFAULT` 仅将此配置应用于默认菜单条目，使用 `GRUB_CMDLINE_LINUX` 将其应用到所有菜单条目。

   每个行只应在 `/etc/default/grub` 中出现一次。如果该行已经存在，则对其进行修改以避免再次复制。因此，只允许 `GRUB_CMDLINE_LINUX_DEFAULT` 一行。

2. 重建 `/boot/grub2/grub.cfg` 配置文件，方法为按照以下方式运行 `grub2-mkconfig -o` 命令：
   - 在基于 BIOS 的系统上：

     ```
     ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
     ```

- 在基于 UEFI 的系统上：

```
~]# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

有关更多信息，请访问 redhat.com 参阅 RHEL 7 系统管理员指南。

从串行控制台控制 GRUB

您可以配置 GRUB 以使用串行控制台而不是 VGA 控制台。这允许您中断引导进程并选择其他内核或添加内核参数，例如引导至单用户模式。

要配置 GRUB 以使用串行控制台，需为初始图像添加注释，并将 `serial` 和 `terminal` 选项添加至 `grub.conf`：

```
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
serial --unit=0 --speed=1152001
```

注: 重新启动系统以使设置生效。

支持的 SSH 加密方案

要使用 SSH 协议与 iDRAC 通信，它支持下表中列出的多种密码方案。

表. 19: SSH 密码方案

方案类型	算法
非对称加密	
公钥	ssh-rsa

表. 19: SSH 密码方案 （续）

方案类型	算法
	ecdsa-sha2-nistp256
对称加密	
密钥交换	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1
Encryption（加密）	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com
MAC	hmac-sha1 hmac-ripemd160 umac-64@openssh.com
压缩	无

注: 如果启用 OpenSSH 7.0 或更高版本，DSA 公共密钥支持将禁用。为了确保 iDRAC 的更好的安全性，Dell 建议不启用 DSA 公共密钥支持。

对 SSH 使用公共密钥验证

iDRAC 支持通过 SSH 的公共密钥验证 (PKA)。这是一项授权的功能。正确设置和使用了基于 SSH 的 PKA 时，您必须输入登录 iDRAC 时的用户名。这对于设置自动脚本以执行各种功能非常有用。上传的密钥必须采用 RFC 4716 或 OpenSSH 格式。否则，您必须转换为该格式的密钥。

在任何情况下，必须在 Management Station 上生成一对私有和公共密钥。将公共密钥上传到 iDRAC 本地用户和 SSH 客户端会使用私有密钥建立管理站与 iDRAC 之间的信任关系。

您可以通过以下方法生成公共或私有密钥对：

- 对于运行 Windows 的客户端，使用 *PuTTY Key Generator* 应用程序
- 对于运行 Linux 的客户端，使用 *ssh-keygen* CLI。

小心: 通常□ iDRAC 上属于管理□用□□成□的用□保留□权限。但也可将此权限分配属于“自定□”用□□中的用□。具有此权限的用□可以修改任何用□的配置。□包括□建和□除任何用□、用□的 SSH 密□管理等。因此，□□慎分配此权限。

小心: 上□、□看和/或□除 SSH 密□的功能取决于配置用□的用□权限。此权限允□用□配置其他用□的 SSH 密□。您□□慎授予此权限。

生成在 Windows 中使用的公共密钥

要使用 *PuTTY Key Generator* 应用程序创建基本密钥：

1. 启动应用程序并选择 RSA 作为密钥类型。
2. 输入密钥的位数。必须是介于 2048 和 4096 位之间的位数。
3. 单击**生成**，按指示在窗口中移动鼠标。

密钥即会生成。

4. 您可以修改密钥备注字段。
5. 输入密码短语以保护密钥。
6. 保存公共和私有密钥。

生成在 Linux 中使用的公共密钥

要使用 *ssh-keygen* 应用程序创建基本密钥，请打开终端窗口并在 shell 提示符下，输入 `ssh-keygen -t rsa -b 2048 -C testing`

其中：

- `-t` 是 *rsa*。
- `-b` 选项指定介于 2048 和 4096 之间的加密位数。
- `-C` 允许修改公共密钥注释，该选项是可选的。

注： 选项区分大小写。

按照说明操作。命令执行后，请上传公共文件。

小心：使用 ssh-keygen 从 Linux 管理站生成的密钥不是 4716 格式。使用 `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` 将密钥转换为 4716 格式。不要更改密钥文件的权限。必须使用默认权限进行转换。

注： iDRAC 不支持密钥的 ssh-agent 转发。

上载 SSH 密钥

您可以为*每个用户*上传最多四个公共密钥以在 SSH 接口上使用。在添加公共密钥之前，请确保查看密钥是否已设置，以免意外覆盖密钥。

添加新公共密钥时，请确保现有的密钥未在添加了新密钥的索引中。iDRAC 不执行检查以确保在添加新密钥删除之前的密钥。在添加新密钥时，如果启用 SSH 接口将非常有用。

使用 Web 界面上载 SSH 密钥

上载 SSH 密钥：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Local Users（本地用户）**。
   此时会显示 **Local Users（本地用户）**页面。
2. 在 **User ID**（用户 ID）列中，单击用户 ID 编号。
   将显示 **Users Main Menu（用户主菜单）**页面。
3. 在 **SSH Key Configurations（SSH 密钥配置）**下，选择 **Upload SSH Key(s)（上载 SSH 密钥）**，然后单击 **Next（下一步）**。
   将显示 **Upload SSH Key(s)（上载 SSH 密钥）**页面。
4. 通过以下方式之一上载 SSH 密钥：
   - 上载密钥文件。
   - 将密钥文件的内容复制到文本框。

   有关更多信息，请参阅 iDRAC Online Help（iDRAC 联机帮助）。
5. 单击**应用**。

使用 RACADM 上载 SSH 密钥

要上载 SSH 密钥，请运行以下命令：

注： 上载和复制密钥不能同时进行。

- 对于本地 RACADM：`racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- 对于远程 RACADM，使用 SSH：`racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

例如，要使用文件将有效密钥上载到第一个密钥空间中的 iDRAC 用户 ID 2，请运行以下命令：

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

注： `-f` 选项在 ssh/串行 RACADM 上不受支持。

查看 SSH 密钥

您可以查看已上载到 iDRAC 的密钥。

使用 Web 界面查看 SSH 密钥

查看 SSH 密钥：

1. 在 Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）**。
   此时会显示 **Local Users（本地用户）**页面。
2. 在 **User ID**（用户 ID）列中，单击用户 ID 编号。
   将显示 **Users Main Menu（用户主菜单）**页面。
3. 在 **SSH 密钥配置**下，选择**查看/删除 SSH 密钥**，然后单击**下一步**。
   将显示 **View/Remove SSH Key(s)（查看/删除 SSH 密钥）**页面及密钥详细信息。

删除 SSH 密钥

在删除公共密钥之前，请确保查看密钥是否是设置的，以免误删密钥。

使用 Web 界面删除 SSH 密钥

要删除 SSH 密钥：

1. 在 Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）**。
   此时会显示 **Local Users（本地用户）**页面。
2. 在 **ID** 列中，选择用户 ID 编号，然后单击 **Edit（编辑）**。
   将显示 **Edit User（编辑用户）**页面。
3. 在 **SSH Key Configurations（SSH 密钥配置）**中，选择 SSH 密钥，然后单击 **Edit（编辑）**。
   SSH Key（SSH 密钥）页面将显示 **Edit From（编辑自）**详情。
4. 针对要删除的密钥选择 **Remove（移除）**，然后单击 **Apply（应用）**。
   所选密钥即被删除。

使用 RACADM 删除 SSH 密钥

要删除 SSH 密钥，请运行以下命令：

- 特定密钥 — `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- 所有密钥 — `racadm sshpkauth -i <2 to 16> -d -k all`

8

配置用户帐户和权限

您可以设置具有特定权限（*基于角色的授权*）的用户帐户，以使用 iDRAC 管理系统和保持系统安全。默认情况下，iDRAC 使用本地管理员帐户进行配置。默认 iDRAC 用户名和密码与系统徽章一起提供。作为管理员，您可以设置用户帐户，以允许其他用户访问 iDRAC。有关更多信息，请参阅服务器文档。

您可以设置本地用户或使用目录服务（如 Microsoft Active Directory 或 LDAP）来设置用户帐户。使用目录服务可提供一个集中位置来管理授权的用户帐户。

iDRAC 支持基于角色访问具有一组相关权限的用户。角色可为管理员、操作员、只读用户或无角色。角色定义可用的最大权限。

主□：

iDRAC 用户角色和权限

iDRAC 角色和权限名称已从前一代服务器更改。角色名为：

表. 20: iDRAC 角色

目前这一代	前一代	权限
管理员	管理员	登录、配置、配置用户、日志、系统控制、访问虚拟控制台、访问虚拟介质、系统操作、调试
操作员	高级用户	登录、配置、系统控制、访问虚拟控制台、访问虚拟介质、系统操作、调试
只读	来宾用户	登录
无	无	无

下表说明了用户权限：

表. 21: iDRAC 用户权限

目前这一代	前一代	说明
登录	登录 iDRAC	允许用户登录到 iDRAC。
配置	配置 iDRAC	允许用户配置 iDRAC。通过该权限，用户可以配置电源管理、虚拟控制台、虚拟介质、许可证、系统设置、存储设备、BIOS 设置、SCP 等。
注: 管理员角色将覆盖其他组件的所有权限，例如 BIOS 设置密码。		
配置用户	配置用户	使用户可以允许特定用户访问系统。
日志	清除日志	使用户可以只清除系统事件日志 (SEL)。
系统控制	控制和配置系统	可对主机系统关机后再开机。

表. 21: iDRAC 用户权限 （续）

目前这一代	前一代	说明
访问虚拟控制台	访问虚拟控制台重定向（适用于刀片式服务器） 访问虚拟控制台（适用于机架式和塔式服务器）	使用户可以运行虚拟控制台。
访问虚拟介质	访问虚拟介质	使用户可以运行和使用虚拟介质。
系统操作	测试警报	允许以异步通知的方式发送用户发起和生成的事件以及信息并进行记录。
调试	执行诊断命令	使用户可以运行诊断命令。

建议使用的用户名和密码字符

本节提供有关在创建和使用用户名和密码时建议使用的字符的详细信息。

注: 密码必须包含一个大写字母和一个小写字母、一个数字和一个特殊字符。

创建用户名和密码时，使用以下字符：

表. 22: 建议使用的用户名字符

字符	长度
0-9 A-Z a-z - ! # $ % & ( ) * ; ? [\ ] ^ _ ` { | } ~ + < = >	1–16

表. 23: 建议使用的密码字符

字符	长度
0-9 A-Z a-z ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1-40

注: 您可以创建包含其他字符的用户名和密码。但是，为了确保与所有接口兼容，Dell 建议仅使用此处列出的字符。

注: 网络共享的用户名和密码中允许的字符由网络共享类型决定。iDRAC 支持通过共享类型定义的网络共享凭据的有效字符，但 <、> 和 ，（逗号分隔）除外。

注: 为了提高安全性，建议使用八个或更多字符的复杂密码，并包括小写字母、大写字母、数字和特殊字符。如果可能的话，另建议定期更改密码。

配置本地用户

您可以通过特定访问权限在 iDRAC 中配置多达 16 个本地用户。在创建一个 iDRAC 用户前，请验证是否存在任何当前用户。您可以使用这些用户的权限设置用户名、密码和角色。您可以使用任何 iDRAC 保护界面（即 Web 界面、RACADM 或 WSMan）更改用户名和密码。您还可以启用或禁用每个用户的 SNMPv3 验证。

使用 iDRAC Web 界面配置本地用户

要添加和配置本地 iDRAC 用户：

注： 您必须具有配置用户权限才能创建 iDRAC 用户。

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **User（用户）**。
   此时会显示 **Local Users（本地用户）**页面。
2. 在用户 **ID** 列中，选择用户 ID 编号，然后单击 **Edit（编辑）**。

   注： 用户 1 用于 IPMI 匿名用户，您无法更改此配置。

   显示 **User Configuration（用户配置）**页面。
3. 添加 **User Account Settings（用户帐户设置）**和 **Advanced Settings（高级设置）** 详细信息以配置用户帐户。

   注： 启用用户 ID 并指定用户的用户名、密码和用户角色（访问权限）。您也可以启用用户的 LAN 权限级别、串行端口权限级别、LAN 上串行状态、SNMPv 3 验证、验证类型和隐私类型。有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击 **Save（保存）**。即会创建具有所需权限的用户。

使用 RACADM 配置本地用户

注： 必须以用户 **root** 登录才能在远程 Linux 系统上执行 RACADM 命令。

您可以使用 RACADM 配置一个或多个 iDRAC 用户。

要使用相同配置设置按照以下步骤配置多个 iDRAC 用户：

- 参考本节中的 RACADM 示例，创建 RACADM 命令的批处理文件，然后在各个受管系统上执行该批处理文件。
- 在使用同一配置文件的各管理系统上创建 iDRAC 配置文件并执行 `racadm set` 子命令。

如果您正在配置新的 iDRAC 或者您已经使用 `racadm racresetcfg` 命令，那么检查系统铭牌上的默认 iDRAC 用户名和密码。`racadm racresetcfg` 令将 iDRAC 重设为默认值。

注： 如果服务器上已启用 SEKM，则在使用此命令之前，请使用 `racadm sekm disable` 命令禁用 SEKM。如果通过执行此命令从 iDRAC 中擦除了 SEKM 设置，则这可以避免被 iDRAC 保护的所有存储设备被锁定。

注： 此后可以启用或禁用用户。因此，在每个 iDRAC 上，用户可能具有不同的索引编号。

要验证用户是否存在，每个索引进入一次以下命令 (1–16)：

```
racadm get iDRAC.Users.<index>.UserName
```

多个参数和对象 ID 会与其当前值一起列出。密钥字段是 `iDRAC.Users.UserName=`。如果“=”后显示了用户名称，该索引号即会被此用户名使用。

注： 您可以利用

```
racadm get -f <myfile.cfg>
```

并查看或编辑

```
myfile.cfg
```

文件，其中包括所有 iDRAC 配置参数。

为用户启用 SNMP v3 身份验证，请使用 **SNMPv3AuthenticationType**、**SNMPv3Enable**、**SNMPv3PrivacyType** 对象。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

如果您使用服务器配置配置文件来配置用户，请使用 **AuthenticationProtocol**、**ProtocolEnable** 和 **PrivacyProtocol** 属性来启用 SNMPv3 验证。

使用 RACADM 添加 iDRAC 用户

1. 设置索引和用户名。

```
racadm set idrac.users.<index>.username <user_name>
```

参数	说明
<index>	唯一的用户索引
<user_name>	用户名

2. 设置密码。

```
racadm set idrac.users.<index>.password <password>
```

3. 设置用户权限。

   有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

4. 启用用户。

```
racadm set.idrac.users.<index>.enable 1
```

要验证，请使用以下命令：

```
racadm get idrac.users.<index>
```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

启用具有权限的 iDRAC 用户

启用具有特定管理权限的用户（基于角色的授权）：

1. 找到可用用户索引。

```
racadm get iDRAC.Users <index>
```

2. 使用新用户名和密码键入以下命令。

```
racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
```

注: 默认权限值为 0，表示用户没有启用任何权限。有关特定用户权限的有效位掩码值的列表，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

配置 Active Directory 用户

如果您的公司使用 Microsoft Active Directory 软件，那么可以配置该软件以提供对 iDRAC 的访问权限，从而允许您向目录服务中的现有用户添加 iDRAC 用户权限并进行控制。这是一项授权的功能。

您可以通过 Active Directory 配置用户身份验证以登录到 iDRAC。您还可以提供基于角色的授权，使管理员能为每位用户配置特定权限。

注: 对于通过 MX 模板进行的任何部署，并且在模板中启用了 CA 验证，用户必须在首次登录时上传 CA 证书，或在将身份验证服务从 LDAP 更改为 Active Directory（反之亦然）之前上传 CA 证书。

对 iDRAC 使用 Active Directory 验证的前提条件

要使用 iDRAC 的 Active Directory 身份验证功能，请确保已执行下列操作：

- 部署有 Active Directory 基础架构。有关更多信息，请参阅 Microsoft 网站。
- 将 PKI 集成到 Active Directory 基础架构。iDRAC 使用标准公钥基础架构 (PKI) 机制来安全验证 Active Directory。有关更多信息，请参阅 Microsoft 网站。
- 在 iDRAC 连接到的所有域控制器上启用安全套接字层 (SSL)，以验证所有域控制器的安全性。

在域控制器上启用 SSL

当 iDRAC 通过 Active Directory 域控制器验证用户时，它将使用域控制器启动一个 SSL 会话。在这段时间内，域控制器必须发布由认证机构 (CA) 签署的证书 — 其根证书也上传到 iDRAC。如需 iDRAC 验证*任何*域控制器 — 无论是根还是子域控制器 — 该域控制器必须具有由域 CA 签署且启用了 SSL 的证书。

如果您使用 Microsoft Enterprise Root CA *自动*将您的所有域控制器分配到 SSL 证书，则必须：

1. 在每个域控制器上安装 SSL 证书。
2. 将域控制器根 CA 证书导出到 iDRAC。
3. 导入 iDRAC 固件 SSL 证书。

安装每个域控制器的 SSL 证书

安装每个域控制器的 SSL 证书：

1. 单击 **Start（开始）** > **Administrative Tools（管理工具）** > **Domain Security Policy（域安全策略）**。
2. 展开 **Public Key Policies（公共密钥策略）**文件夹，右键单击 **Automatic Certificate Request Settings（自动证书申请设置）**并单击 **Automatic Certificate Request（自动证书申请）**。
   将显示 **Automatic Certificate Request Setup Wizard（自动证书申请设置向导）**。
3. 单击 **Next（下一步）**并选择 **Domain Controller（域控制器）**。
4. 单击 **Next（下一步）**，然后单击 **Finish（完成）**。SSL 证书已安装。

将域控制器根 CA 证书导出至 iDRAC

要将域控制器根 CA 证书导出至 iDRAC：

1. 找到运行 Microsoft Enterprise CA 服务的域控制器。
2. 单击**开始** > **运行**。
3. 输入 `mmc`，然后单击**确定**。
4. 在**控制台 1** (MMC) 窗口中，单击**文件**（或**控制台**）并选择**添加/删除管理单元**。
5. 在**添加/删除管理单元**窗口中，单击**添加**。
6. 在**独立管理单元**窗口中，选择**证书**并单击**添加**。
7. 选择**计算机**并单击**下一步**。
8. 选择**本地计算机**，单击**完成**，然后单击**确定**。
9. 在**控制台 1** 窗口中，转到**证书个人证书**文件夹。
10. 找到并右键单击根 CA 证书，选择**所有任务**，然后单击**导出...**。
11. 在**证书导出向导**中，单击**下一步**并选择**不，不导出私有密钥**。
12. 单击**下一步**并选择**基于 64 位编码的 X.509 (.cer)**作为格式。
13. 单击**下一步**并将证书保存至系统上的目录。
14. 将在步骤 13 中保存的证书上载到 iDRAC。

导入 iDRAC 固件 SSL 证书

iDRAC SSL 证书是用于 iDRAC Web 服务器的相同证书。所有 iDRAC 控制器都配有默认自签名证书。

如果 Active Directory 服务器设置为在 SSL 会话初始化阶段验证客户端，您需要将 iDRAC 服务器证书上传到 Active Directory 域控制器。如果 Active Directory 在 SSL 会话初始化期间不执行客户端验证，则不需要这一额外步骤。

注: 如果 iDRAC 固件 SSL 证书是 CA 签名的并且该 CA 的证书已经位于域控制器的“受信任的根认证机构”列表中，请勿执行本节中的步骤。

将 iDRAC 固件 SSL 证书导入到所有域控制器信任的证书列表：

1. 使用以下 RACADM 命令下载 iDRAC SSL 证书：

   ```
   racadm sslcertdownload -t 1 -f <RAC SSL certificate>
   ```

2. 在域控制器上，打开 **MMC 控制台**窗口并选择**证书** > **受信任的根认证机构**。
3. 右键单击**证书**，选择**所有任务**并单击**导入**。
4. 单击**下一步**并浏览到 SSL 证书文件。
5. 在每个域控制器的**受信任的根认证机构**中安装 iDRAC SSL 证书。

   如果已安装自己的证书，请确保为证书签名的 CA 位于**可信的根证书机构**列表中。如果该机构不在列表中，则必须在所有的域控制器上安装它。

6. 单击**下一步**并选择是否要 Windows 根据证书类型自动选择证书存储区，或浏览到所选存储区。
7. 单击**完成**并单击**确定**。将 iDRAC 固件 SSL 证书导入到所有域控制器信任的证书列表。

支持的 Active Directory 验证机制

您可以通过两种方法使用 Active Directory 定义 iDRAC 用户访问权限：

- *标准架构*解决方案，仅使用 Microsoft 的默认 Active Directory 组对象。
- *扩展架构*解决方案具有自定义的 Active Directory 对象。所有访问控制对象都在 Active Directory 中维护。它提供了最大的灵活性，以在具有各种权限级别不同 iDRAC 上配置用户访问权限。

标准架构 Active Directory 概览

如下图所示，为 Active Directory 集成使用标准架构需要在 Active Directory 和 iDRAC 上都进行配置。

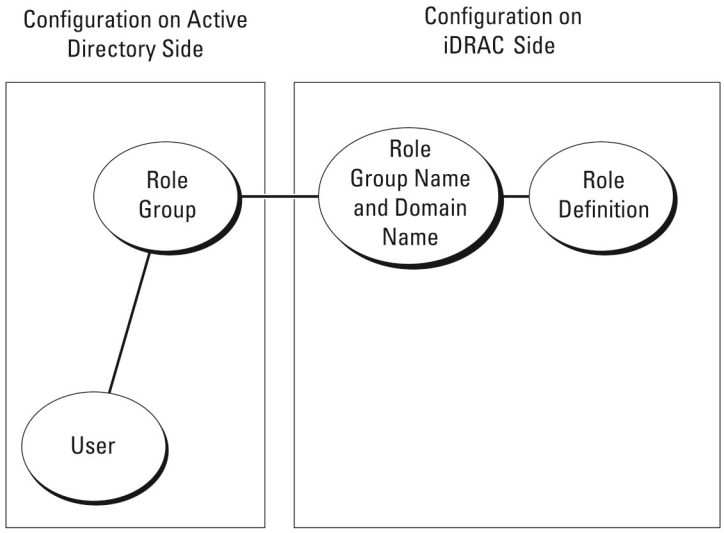


图 1: 使用 Active Directory 标准架构配置 iDRAC

在 Active Directory 中，使用标准组对象作为角色组。具有 iDRAC 访问权限的用户是角色组的成员。要为此用户提供特定 iDRAC 的访问权限，需要在特定 iDRAC 上配置角色组名称及其域名。在每个 iDRAC（而非 Active Directory）中定义角色和权限级别。您可以在每个 iDRAC 中配置多达十五个角色组。表参考编号显示默认角色组的权限。

表. 24: 默认角色组权限

角色组	默认权限级别	授予的权限	位掩码
角色组 1	无	登录到 iDRAC、配置 iDRAC、配置用户、清除日志、执行服务器控制命令、访问虚拟控制台、访问虚拟介质、测试警报、执行诊断命令	0x000001ff

表. 24: 默认角色组权限 （续）

角色组	默认权限级别	授予的权限	位掩码
角色组 2	无	登录到 iDRAC、配置 iDRAC、执行服务器控制命令、访问虚拟控制台、访问虚拟介质、测试警报、执行诊断命令	0x000000f9
角色组 3	无	登录到 iDRAC。	0x00000001
角色组 4	无	没有分配权限	0x00000000
角色组 5	无	没有分配权限	0x00000000

注: “位掩□”□只有在用 RACADM □置□准架构□才使用。

单域和多域情况

如果所有登录用户和角色组（包括嵌套组）在相同域中，则仅需要在 iDRAC 上配置域控制器地址。在这种单域情况中，支持所有组类型。

如果所有登录用户和角色组（包括嵌套组）来自多个域中，则必须在 iDRAC 上配置全局目录服务器地址。在这种多域情况中，所有角色组和嵌套组（如果有）必须为通用组类型。

配置标准架构 Active Directory

在配置标准架构 Active Directory 之前，请确保：

- 您拥有 iDRAC Enterprise 或 Datacenter 许可证。
- 该配置在用作域控制器的服务器上执行。
- 服务器上的 dat、时间和时区正确无误。
- iDRAC 网络设置已配置，或者在 iDRAC Web 界面中转到 **iDRAC 设置 > 连接性 > 网络 > 通用设置**以配置网络设置。

要配置 iDRAC 以进行 Active Directory 登录访问：

1. 在 Active Directory 服务器（域控制器）上，打开 Active Directory 用户和计算机管理单元。
2. 创建 iDRAC 组和用户。
3. 在 iDRAC 上使用 iDRAC Web 界面或 RACADM 配置组名、域名和角色权限。

使用 iDRAC Web 界面配置具有标准架构的 Active Directory

注: 有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Directory Services（目录服务）**。
   随即显示**目录服务**页面。
2. 选择 **Microsoft Active Directory** 选项，然后单击 **Edit（应用）**。
   随即显示 **Active Directory 配置与管理**页面。
3. 单击 **Configure Active Directory（配置 Active Directory）**。
   将显示 **Active Directory Configuration and Management Step 1 of 4（Active Directory 配置和管理第 1 步，共 4 步）**页面。
4. 当与 Active Directory (AD) 服务器通信时，可选择启用证书验证并上载 SSL 连接初始化期间所用的认证机构签署的数字证书。对于此，必须指定域控制器和全局目录 FQDN 。这将在下一个步骤完成。因此，应在网络设置中正确配置 DNS 。
5. 单击 **Next**（下一步）。

   将显示 **Active Directory Configuration and Management Step 2 of 4（Active Directory 配置和管理第 2 步，共 4 步）**页面。
6. 启用 Active Directory 并指定关于 Active Directory 服务器和用户帐户的位置信息。此外，指定在 iDRAC 登录过程中 iDRAC 必须等待来自 Active Directory 的响应的时间。

注: 如果证书验证已启用，请指定域控制器服务器地址和全局编录 FQDN。确保 **iDRAC Settings（iDRAC 设置）** > **Network（网络）**。

7. 单击 **Next**（下一步）。将显示 **Active Directory Configuration and Management Step 3 of 4（Active Directory 配置和管理第 3 步，共 4 步）**页面。
8. 选择 **Standard Schema（标准架构）**并单击 Next（下一步）。
   将显示 **Active Directory Configuration and Management Step 4a of 4（Active Directory 配置和管理第 4a 步，共 4 步）**页面。
9. 输入 Active Directory 全局编录服务器的位置并指定用于授权用户的权限组。
10. 单击 **Role Group（角色组）**配置标准架构模式下用户的控制授权策略。
    将显示 **Active Directory Configuration and Management Step 4b of 4（Active Directory 配置和管理第 4b 步，共 4 步）**页面。
11. 指定权限并单击 **Apply（应用）**。

    将应用设置并显示 **Active Directory Configuration and Management Step 4a of 4（Active Directory 配置和管理第 4a 步，共 4 步）**页面。

12. 单击**完成**。标准架构的 Active Directory 设置即配置完成。

使用 RACADM 配置具有标准架构的 Active Directory

1. 使用以下命令：

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ADGroup.Name <common name of the role group>
racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
racadm set iDRAC.ADGroup.Privilege <Bit-mask value for specific RoleGroup permissions>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP
address of the domain controller>
```

- 输入域控制器的全称域名 (FQDN)，而不是域的 FQDN。例如，输入 `servername.dell.com` 而不是 `dell.com`。
- 有关特定角色组权限的位掩码值，请参阅默认角色组权限。
- 您必须至少提供三个域控制器地址中的一个。iDRAC 尝试依次连接到每个配置的地址，直到实现成功连接为止。使用标准架构时，这些是用户帐户和角色组所在的域控制器的地址。
- 只在用户帐户和角色组处于不同域时，标准架构才需要全局编录服务器。在多个域的情况下，仅可以使用通用组。
- 如果证书验证已启用，您在此字段中指定的 FQDN 或 IP 地址必须与域控制器证书的主题或主题备用名称字段匹配。
- 要在 SSL 握手的过程中禁用证书验证，使用以下命令：

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  在此情况下，无需上载认证机构 (CA) 证书。
- 要在 SSL 握手过程中强制执行证书验证（可选），使用以下命令：

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  在此情况下，必须使用以下命令上载 CA 证书：

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

  注: 如果证书验证已启用，请指定域控制器服务器地址和全局编录 FQDN。确保 DNS 已在**概览** > **iDRAC 设置** > **网络**下正确配置。

以下 RACADM 命令可选用。

```
racadm sslcertdownload -t 1 -f <RAC SSL certificate>
```

2. 如果 iDRAC 上已启用 DHCP 并且您希望使用 DHCP 服务器提供的 DNS，则输入以下命令：

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3. 如果 iDRAC 上已禁用 DHCP 或者您想手动输入 DNS IP 地址，请输入以下 RACADM 命令：

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4. 如果要配置用户域列表以便在登录到 Web 界面时只需输入用户名，则输入以下命令：

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address
of the domain controller>
```

您最多可配置 40 个用户域，索引编号介于 1 到 40 之间。

扩展架构 Active Directory 概览

使用扩展架构解决方案需要 Active Directory 架构扩展。

扩展架构的最佳做法

扩展架构使用 Dell 关联对象加入 iDRAC 和权限。这将使您能够基于授予的整体权限使用 iDRAC。Dell 关联对象的默认访问控制列表 (ACL) 允许自管理员和域管理员管理 iDRAC 对象的权限和范围。

默认情况下，Dell 关联对象不继承父 Active Directory 对象的所有权限。如果您启用 Dell 关联对象继承，则该关联对象的继承权限将授予所选用户和组。这可能会导致为 iDRAC 提供意外权限。

要安全地使用扩展架构，Dell 建议不要在扩展架构实施中启用 Dell 关联对象的继承。

Active Directory 架构扩展

Active Directory 数据是*属性*和*类的分布式数据库*。Active Directory 架构包含规则以确定可添加或包含在数据库中的数据类型。用户类是数据库中存储的*类*的一个示例。用户类属性的一些示例包括用户的名字、姓氏、电话号码等。您可以通过添加自己独特的*属性*和*类来扩展 Active Directory 数据库*，以满足特定要求。Dell 扩展了架构，以包括必要的更改，支持使用 Active Directory 进行远程管理身份验证和授权。

添加到现有活动目录架构中每个*属性*或*类*都必须通过唯一 ID 进行定义。为了保持 ID 在整个行业的唯一性，Microsoft 维护了一个 Active Directory 对象识别符 (OID) 数据库，以便公司在将扩展添加到架构师可以保证唯一性并且不会与其他公司发生冲突。要扩展 Microsoft Active Directory 中的架构，Dell 收到了添加到目录服务的属性和类的唯一 OID、唯一扩展名以及唯一关联属性 ID。

- 扩展名是：`dell`
- Base OID 是：`1.2.840.113556.1.8000.1280`
- RAC LinkID 范围是：`12070 to 12079`

iDRAC 架构扩展概览

Dell 扩展了架构以包括*关联*、*设备*和*权限*属性。*关联*属性可用于将具有一组特定权限的用户或组链接到一个或多个 iDRAC 设备。此型号为管理员提供了极大的灵活性，在网络上支持多种不同用户、iDRAC 权限和 iDRAC 设备组合，十分简便。

对于您想要与 Active Directory 集成以进行验证和授权的网络上的每个物理 iDRAC 设备，请创建至少一个关联对象和一个 iDRAC 设备对象。您可以创建多个关联对象，每个关联对象都可以按需链接到任意多个用户、用户组或 iDRAC 设备对象。用户和 iDRAC 用户组可以是企业中任何域的成员。

不过，每个关联对象都只能链接（或者，可以链接用户、用户组或 iDRAC 设备对象）到一个权限对象。此示例允许管理员控制特定 iDRAC 设备上的每个用户权限。

iDRAC 设备对象是到 iDRAC 固件的链接，用于查询 Active Directory 以进行验证和授权。将 iDRAC 添加到网络后，管理员必须使用 Active Directory 名称配置 iDRAC 及其设备对象，以便用户可以通过 Active Directory 执行验证和授权。此外，管理员还必须将 iDRAC 添加到至少一个关联对象以便用户能够进行验证。

下图显示为提供验证和授权所需连接的关联对象。

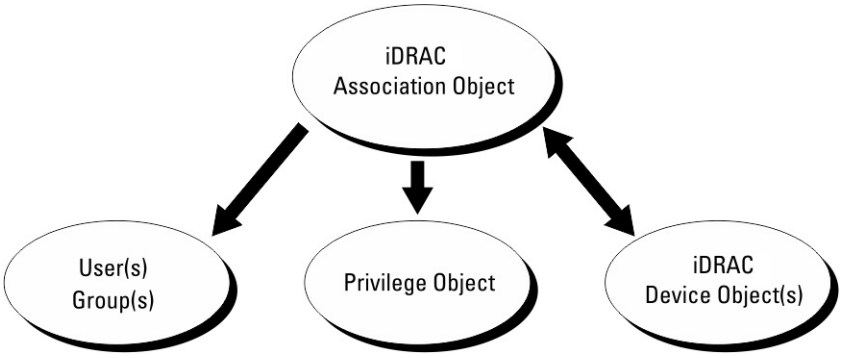


图 2: Active Directory 对象的典型设置

您可以根据需要创建任意数量的关联对象。但是，您必须创建至少一个关联对象，并且网络上要与 Active Directory 集成以通过 iDRAC 验证和授权的每个 iDRAC 设备必须有一个 iDRAC 设备对象。

关联对象允许有任意数量的用户和/或组以及 iDRAC 设备对象。然而，每个关联对象只包括一个权限对象。关联对象可连接在 iDRAC 设备上拥有权限的用户。

针对 ADUC MMC 管理单元的 Dell 扩展只允许将来自相同域的权限对象和 iDRAC 对象与关联对象进行关联。Dell 扩展不允许将来自其他域的组或 iDRAC 对象添加为关联对象的产品成员。

添加来自不同域的通用组时，请创建一个具有通用范围的关联对象。Dell Schema Extender 公用程序创建的默认关联对象是域本地组，不能与来自其他域的通用组一起使用。

来自任何域的用户、用户组或嵌套的用户组都可以添加到关联对象中。扩展架构解决方案支持嵌套在 Microsoft Active Directory 允许的多个域之间的任何用户组类型和任何用户组。

累积使用扩展架构的权限

扩展架构验证机制支持通过不同关联对象与同一用户相关的不同权限对象进行权限累积。换言之，扩展架构验证可以累积权限，以允许用户拥有与同一用户关联的不同权限对象对应的所有已分配权限的超级集合。

下图提供了一个使用扩展架构累积权限的示例。

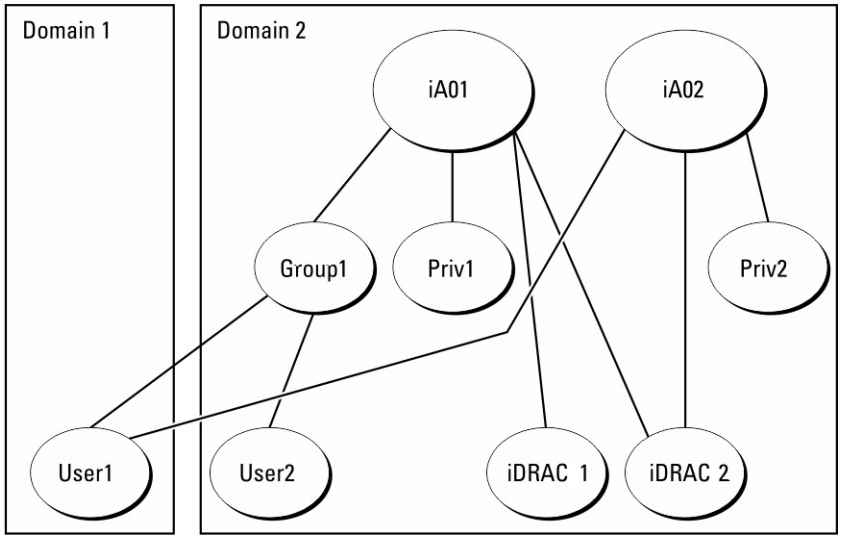


图 3: 用户权限累积

该图显示两个关联对象 — A01 和 A02。User1 通过两个关联对象与 iDRAC2 关联。

扩展架构验证利用相同用户关联的不同权限对象的已分配权限，将权限加以累积，从而使用户拥有最大的权限集合。

在本示例中，User1 拥有 iDRAC2 上的 Priv1 和 Priv2 权限。User1 仅拥有 iDRAC1 上的 Priv1 权限。User2 拥有 iDRAC1 和 iDRAC2 上的 Priv1 权限。另外，此图显示 User1 可在其他域中，而且可以是组成员。

配置扩展架构 Active Directory

要配置 Active Directory 以访问 iDRAC：

1. 扩展 Active Directory 架构。
2. 扩展 Active Directory 用户和计算机管理单元。
3. 将 iDRAC 用户及其特权添加到 Active Directory。
4. 使用 iDRAC Web 界面或 RACADM 配置 iDRAC Active Directory 属性。

扩展 Active Directory 架构

扩展 Active Directory 架构将会在 Active Directory 架构中添加 Dell 组织单元、架构类和属性以及示例权限和关联对象。扩展架构之前，确保在域林的架构主文件 FSMO 角色拥有者上拥有架构管理员权限。

注: 此□品的架构□展与前几代有所不同。□早的架构不能用于此□品。

注: □展新架构不会影响之前版本的□品。

可使用以下任一方法扩展架构：

- Dell Schema Extender 公用程序
- LDIF 脚本文件

如果使用 LDIF 脚本文件，则不会将 Dell 组织单元添加到架构中。

LDIF 文件和 Dell Schema Extender 分别位于 *Dell Systems Management Tools and Documentation* DVD 的以下目录中：

- DVDdrive :`\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files`
- <DVDdrive>: `\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender`

要使用 LDIF 文件，请参阅 **LDIF_Files** 目录中自述文件中的说明。

可以从任意位置复制并运行 Schema Extender 或 LDIF 文件。

使用 Dell Schema Extender

小心: Dell Schema Extender 使用 SchemaExtenderOem.ini 文件。要确保 Dell Schema Extender 公用程序正常工作，请勿修改此文件的名称。

1. 在 **Welcome（欢迎）**屏幕上，单击 **Next（下一步）**。
2. 阅读并了解警告，然后单击**下一步**。
3. 选择 **Use Current Log In Credentials（使用当前登录凭据）**或输入具有架构管理员权限的用户名和密码。
4. 单击**下一步**运行 Dell Schema Extender。
5. 单击**完成**。

   架构可扩展。要验证架构扩展，请使用 MMC 和 Active Directory 架构管理单元来验证 类和属性 页面上的 144 是否存在。有关使用 MMC 和 Active Directory 架构管理单元的详细信息，请参阅 Microsoft 说明文件。

类和属性

表. 25: 添加到 Active Directory 架构中类的类定义

类名称	分配的对象标识号 (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2

表. 25: 添加到 Active Directory 架构中类的类定义 （续）

类名称	分配的对象标识号 (OID)
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表. 26: DelliDRACdevice 类

OID	1.2.840.113556.1.8000.1280.1.7.1.1
说明	代表 Dell iDRAC 设备。iDRAC 必须在 Active Directory 中配置为 delliDRACDevice。此配置使 iDRAC 可将轻量级目录访问协议 (LDAP) 查询发送到 Active Directory。
类的类型	结构类
超类	dellProduct
属性	dellSchemaVersion dellRacType

表. 27: delliDRACAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.7.1.2
说明	代表 Dell 关联对象。关联对象用于提供用户与设备之间的连接。
类的类型	结构类
超类	组
属性	dellProductMembers dellPrivilegeMember

表. 28: dellRAC4Privileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.3
说明	为 iDRAC 定义权限（授权权限）
类的类型	辅助类
超类	无
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser

表. 28: dellRAC4Privileges 类 （续）

OID	1.2.840.113556.1.8000.1280.1.1.1.3
	dellIsDebugCommandAdmin

表. 29: dellPrivileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.4
说明	用作 Dell 权限（授权权限）的容器类。
类的类型	结构类
超类	用户
属性	dellRAC4Privileges

表. 30: dellProduct 类

OID	1.2.840.113556.1.8000.1280.1.1.1.5
说明	所有 Dell 产品派生所依据的主类。
类的类型	结构类
超类	计算机
属性	dellAssociationMembers

表. 31: 添加到 Active Directory 架构的属性的列表

属性名称/说明	分配的 OID/语法对象标识符	单值
dellPrivilegeMember 属于此属性的 dellPrivilege 对象的列表。	1.2.840.113556.1.8000.1280.1.1.2.1 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers 属于此角色的 dellRacDevice 和 DelliDRACDevice 对象的列表。此属性是指向 dellAssociationMembers 后退链接的正向链接。 链接 ID：12070	1.2.840.113556.1.8000.1280.1.1.2.2 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser 如果用户具有设备的登录权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin 如果用户具有设备的卡配置权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin 如果用户具有设备的用户配置权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE

表. 31: 添加到 Active Directory 架构的属性的列表 （续）

属性名称/说明	分配的 OID/语法对象标识符	单值
如果用户具有设备的日志清除权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser 如果用户具有设备的服务器重设权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser 如果用户具有设备的虚拟控制台权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser 如果用户具有设备的虚拟介质权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser 如果用户具有设备的测试警报用户权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin 如果用户具有设备的调试命令管理员权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion 当前架构版本用于更新架构。	1.2.840.113556.1.8000.1280.1.1.2.12 忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType 此属性是 delliDRACDevice 对象的当前 RAC 类型以及到 dellAssociationObjectMembers 前进链接的后退链接。	1.2.840.113556.1.8000.1280.1.1.2.13 忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers 属于此产品的 dellAssociationObjectMembers 的列表。此属性是到 dellProductMembers 链接属性的反向链接。 链接 ID：12071	1.2.840.113556.1.8000.1280.1.1.2.14 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

安装用于 Active Directory 用户和计算机管理单元的 Dell 扩展

扩展 Active Directory 中的架构时，还必须扩展 Active Directory 用户和计算机管理单元，以使管理员能够管理 iDRAC 设备、用户和用户组、iDRAC 关联和 iDRAC 权限。

使用 *Dell Systems Management Tools and Documentation* DVD 安装系统管理软件时，可以在安装过程中选择 **Active Directory Users and Computers Snap-in（Active Directory 用户和计算机管理单元）**选项来扩展管理单元。请参阅“Dell OpenManage Software Quick Installation Guide”（《Dell OpenManage 软件快速安装指南》），进一步了解如何安装系统管理软件。对于 64 位 Windows 操作系统来说，管理单元安装程序位于：

<DVD 驱动器>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

有关 Active Directory 用户和计算机管理单元的更多信息，请参阅 Microsoft 说明文件。

将 iDRAC 用户和权限添加到 Active Directory

使用 Dell 扩展的 Active Directory 用户和计算机管理单元，您可以通过创建设备、关联和权限对象添加 iDRAC 用户和权限。要添加每个对象，请执行以下操作：

- 创建 iDRAC 设备对象
- 创建权限对象
- 创建关联对象
- 将对象添加到关联对象

创建 iDRAC 设备对象

要创建 iDRAC 设备对象，请执行以下操作：

1. 在 MMC 的 **Console Root（控制台根目录）**窗口中，右键单击一个容器。
2. 选择 **New（新建）** > **Dell Remote Management Object Advanced（Dell 高级远程管理对象）**。
   将显示 **New Object （新建对象）**窗口。
3. 为新对象输入名称。该名称必须与您在使用 iDRAC Web 界面配置 Active Directory 属性时输入的 iDRAC 名称完全相同。
4. 选择 iDRAC **Device Object（设备对象）**，然后单击 OK（确定）。

创建权限对象

要创建权限对象：

注: 您必须在相关关联对象的同一个域中创建权限对象。

1. 在**控制台根节点** (MMC) 窗口中，右键单击一个容器。
2. 选择 **New（新建）** > **Dell Remote Management Object Advanced（Dell 高级远程管理对象）**。
   将显示 **New Object （新建对象）**窗口。
3. 为新对象输入名称。
4. 选择 **Privilege Object（权限对象）**，然后单击 OK（确定）。
5. 右键单击已创建的权限对象并选择**属性**。
6. 单击 **Remote Management Privileges（远程管理权限）**选项卡并为用户或组分配权限。

创建关联对象

要创建关联对象，请执行以下操作：

注: iDRAC 关联对象从组派生而来，其范围设置为“本地域”。

1. 在**控制台根节点** (MMC) 窗口中，右键单击一个容器。
2. 选择 **New（新建）** > **Dell Remote Management Object Advanced（Dell 高级远程管理对象）**。
   系统会显示**新建对象**窗口。
3. 输入新对象的名称并选择**关联对象**。
4. 选择 **Association Object（关联对象）**的范围，然后单击 OK（确定）。
5. 向验证用户提供访问创建的关联对象的访问权限。

为关联对象提供用户访问权限

要向验证用户提供访问创建的关联对象的访问权限：

1. 转到 **Administrative Tools（管理工具）** > **ADSI Edit（ADSI 编辑）**。将显示 **ADSI Edit（ADSI 编辑）**窗口。
2. 在右侧窗格中，导航至创建的关联对象，右键单击并选择 **Properties（属性）**。
3. 在**安全**选项卡中，单击**添加**。
4. 键入 `Authenticated Users`，单击 **Check Names（检查名称）**，然后单击 **OK（确定）**。验证的用户将添加到 **Groups and user names（组和用户名称）**列表。
5. 单击 **OK（确定）**。

将对象添加到关联对象

使用**关联对象属性**窗口，可以关联用户或用户组、权限对象和 iDRAC 设备或 iDRAC 设备组。

您可以添加用户组和 iDRAC 设备组。

添加用户或用户组

要添加用户或用户组，请执行以下操作：

1. 右键单击**关联对象**并选择**属性**。
2. 选择**用户**选项卡并单击**添加**。
3. 输入用户或用户组名称并单击 **OK（确定）**。

添加权限

要添加权限，请执行以下操作：

单击 **Privilege Object（权限对象）**选项卡，将权限对象添加到验证 iDRAC 设备时定义用户或用户组权限的关联中。只能将一个权限对象添加到关联对象。

1. 选择 **Privileges Object（权限对象）**选项卡，并单击 **Add（添加）**。
2. 输入权限对象名称并单击**确定**。
3. 单击 **Privilege Object（权限对象）**选项卡，将权限对象添加到验证 iDRAC 设备时定义用户或用户组权限的关联中。只能将一个权限对象添加到关联对象。

添加 iDRAC 设备或 iDRAC 设备组

要添加 iDRAC 设备或 iDRAC 设备组：

1. 选择**产品**选项卡并单击**添加**。
2. 输入 iDRAC 设备或 iDRAC 设备组名称并单击**确定**。
3. 在**属性**窗口中，依次单击**应用**、**确定**。
4. 单击 **Products（产品）**选项卡以添加一个已连接到可用于所定义的用户或用户组的网络的 iDRAC 设备。您可以将多个 iDRAC 设备添加到一个关联对象。

使用 iDRAC Web 界面配置具有扩展架构的 Active Directory

要使用 Web 界面以扩展架构配置 Active Directory：

注: 有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Directory Services（目录服务）** > **Microsoft Active Directory**。单击 **Edit（编辑）**
   将显示 **Active Directory Configuration and Management Step 1 of 4（Active Directory 配置和管理第 1 步，共 4 步）**页面。
2. 当与 Active Directory (AD) 服务器通信时，可选择启用证书验证并上载 SSL 连接初始化期间所用的认证机构签署的数字证书。
3. 单击 **Next**（下一步）。
   将显示 **Active Directory Configuration and Management Step 2 of 4（Active Directory 配置和管理第 2 步，共 4 步）**页面。
4. 指定关于 Active Directory (AD) 服务器和用户帐户的位置信息。此外，指定登录期间 iDRAC 必须等待 AD 响应的时间。

   注:
   - 如果证书验证已启用，请指定域控制器服务器地址和 FQDN。确保在 **iDRAC Settings（iDRAC 设置）** > **Network（网络）**下正确配置 DNS
   - 如果用户和 iDRAC 对象位于不同的域中，则不要选择 **User Domain from Login（来自登录的用户域）**选项。而应选择 **Specify a Domain（指定域）**选项并输入提供 iDRAC 对象的域名。

5. 单击 **Next**（下一步）。将显示 **Active Directory Configuration and Management Step 3 of 4（Active Directory 配置和管理第 3 步，共 4 步）**页面。

6. 选择**扩展架构**并单击 **Next（下一步）**。
   将显示 **Active Directory Configuration and Management Step 4 of 4”（Active Directory 配置和管理第 4 步，共 4 步）**页面。
7. 输入 Active Directory (AD) 中的 iDRAC 设备对象的名称和位置，并单击 **Finish（完成）**。
   扩展架构模式的 Active Directory 设置配置完成。

使用 RACADM 配置具有扩展架构的 Active Directory

使用 RACADM 配置具有扩展架构的 Active Directory：

1. 使用以下命令：

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ActiveDirectory.RacName <RAC common name>
racadm set iDRAC.ActiveDirectory.RacDomain <fully qualified rac domain name>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
```

   - 输入域控制器的全称域名 (FQDN)，而不是域的 FQDN。例如，输入 `servername.dell.com` 而不是 `dell.com`。
   - 您必须至少提供以下三个地址中的一个。iDRAC 尝试依次连接到每个配置的地址，直到实现成功连接为止。使用扩展架构时，这些是此 iDRAC 设备所在的域控制器的 FQDN 或 IP 地址。
   - 要在 SSL 握手的过程中禁用证书验证，使用以下命令：

     ```
     racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
     ```

     在此情况下，您无需上载 CA 证书。
   - 在 SSL 握手过程中强制执行证书验证（可选）：

     ```
     racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
     ```

     在此情况下，您需要使用以下 RACADM 命令上载 CA 证书：

     ```
     racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
     ```

     注: 如果证书验证已启用，请指定域控制器服务器地址和 FQDN。确保 **iDRAC 设置** > **网络**下的 DNS 已正确配置。

     以下 RACADM 命令可选：

     ```
     racadm sslcertdownload -t 1 -f <RAC SSL certificate>
     ```

2. 如果 iDRAC 上已启用 DHCP 并且您希望使用 DHCP 服务器提供的 DNS，则输入以下命令：

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3. 如果 iDRAC 上已禁用 DHCP 或您希望手动输入 DNS IP 地址，请输入以下命令：

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4. 如果您希望配置用户域列表以便在登录到 iDRAC Web 界面时只需输入用户名，请使用以下命令：

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address
of the domain controller>
```

   您最多可配置 40 个用户域，索引编号介于 1 到 40 之间。

测试 Active Directory 设置

您可以测试 Active Directory 设置以验证您的配置是否正确，或诊断 Active Directory 登录失败的问题。

使用 iDRAC Web 界面测试 Active Directory 设置

测试 Active Directory 设置：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Directory Services（目录服务）** > **Microsoft Active Directory**，单击 **Test（测试）**。
   随即显示 **Test Active Directory Settings（测试 Active Directory 设置）**页面。
2. 单击**测试**。
3. 输入测试用户的名称（例如 **username@domain.com**）和密码，然后单击 **Start Test（开始测试）**。随即会显示详细测试结果和测试日志。

   如果任何步骤失败，请查看测试日志中的详细信息以确定问题和可能的解决方案。

   注: 如果在已勾选“Enable Certificate Validation”（启用证书验证）的情况下测试 Active Directory 设置，则 iDRAC 要求 Active Directory 服务器被 FQDN（而不是 IP 地址）标识。如果 Active Directory 服务器通过 IP 地址标识，则证书验证会因为 iDRAC 无法与 Active Directory 服务器通信而失败。

使用 RACADM 测试 Active Directory 设置

要测试 Active Directory 设置，请使用 `testfeature` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

配置通用 LDAP 用户

iDRAC 提供通用解决方案来支持基于轻量级目录访问协议 (LDAP) 的验证。此功能不需要在目录服务上进行任何架构扩展。

为了使 iDRAC LDAP 实施通用，将利用不同目录服务之间的通用性对用户进行分组并映射用户-组关系。目录服务的特定操作是架构。例如，用户、组以及用户和组之间的链接有不同的属性名称。这些操作可在 iDRAC 中进行配置。

注: 通用 LDAP 目□服□不支持基于智能卡的双重□□ (TFA) 和□一登□ (SSO)。

使用 iDRAC 基于 Web 的界面配置通用 LDAP 目录服务

要使用 Web 界面配置通用 LDAP 目录服务，请执行以下操作：

注: 有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Directory Services（目录服务）** > **Generic LDAP Directory Service（通用 LDAP 目录服务）**，单击 **Edit（编辑）**。
   Generic LDAP Configuration and Management Step 1 of 3（通用 LDAP 配置和管理第 1 步，共 3 步）页面中显示当前的通用 LDAP 设置。
2. 或者，在与通用 LDAP 服务器通信时的 SSL 连接初始化过程中启用证书验证并上载使用的数字证书。

   注: 在此版本中，不支持基于非 SSL 端口的 LDAP 绑定。仅支持 SSL 上的 LDAP。

3. 单击 **Next**（下一步）。
   将显示 **Generic LDAP Configuration and Management Step 2 of 3（通用 LDAP 配置和管理第 2 步，共 3 步）**页面。
4. 启用通用 LDAP 验证并指定关于通用 LDAP 服务器和用户帐户的位置信息。

   注: 如果证书验证已启用，请指定 LDAP 服务器的 FQDN 并确保 DNS 在 **iDRAC Settings（iDRAC 设置）** > **Network（网络）**下正确配置。

   注: 在此版本中，不支持嵌套组。固件将搜索与用户 DN 相匹配的组的直接成员。另外，仅支持单域。不支持交叉域。

5. 单击 **Next**（下一步）。
   将显示 **Generic LDAP Configuration and Management Step 3a of 3（通用 LDAP 配置和管理第 3a 步，共 3 步）**页面。
6. 单击 **Role Group（角色组）**。
   将显示 **Generic LDAP Configuration and Management Step 3b of 3（通用 LDAP 配置和管理第 3b 步，共 3 步）**页面。
7. 指定可按组分辨的名称，与该组关联的权限，然后单击 **Apply（应用）**。

   注: 如果您使用 Novell eDirectory 并对组 DN 名称使用了以下字符：#（井号）、"（双引号）、；（分号）、>（大于号）、，（逗号）或 <（小于号），则必须转义。

   角色组设置将保存。**Generic LDAP Configuration and Management Step 3a of 3（通用 LDAP 配置和管理第 3a 步，共 3 步）**页面将显示角色组设置。
8. 如果要配置其他角色组，请重复第 7 步和第 8 步。
9. 单击**完成**。通用 LDAP 目录服务配置完成。

使用 RACADM 配置通用 LDAP 目录服务

要配置 LDAP 目录服务，使用 `iDRAC.LDAP` 和 `iDRAC.LDAPRole` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

测试 LDAP 目录服务设置

您可以测试 LDAP 目录服务设置以验证您的配置是否正确，或诊断 LDAP 登录失败的问题。

使用 iDRAC Web 界面测试 LDAP 目录服务设置

要测试 LDAP 目录服务设置：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Directory Services（目录服务）** > **Generic LDAP Directory Service（通用 LDAP 目录服务）**。
   Generic LDAP Configuration and Management（通用 LDAP 配置和管理）页面中显示当前的通用 LDAP 设置。
2. 单击**测试**。
3. 输入选为测试 LDAP 设置的目录用户的用户名和密码。格式取决于使用的*用户登录属性*并且输入的用户名必须与所选的属性匹配。

   注: 在已勾选 **Enable Certificate Validation（启用证书验证）**的情况下测试 LDAP 设置时，iDRAC 要求 LDAP 服务器被 FQDN 而不是 IP 地址识别。如果 LDAP 服务器由 IP 地址来识别，则证书验证失败，因为 iDRAC 无法与 LDAP 服务器通信。

   注: 如果启用通用 LDAP，iDRAC 首先会尝试以目录用户的身份登录用户。如果失败，则会启用本地用户查找。

   随即会显示测试结果和测试日志。

使用 RACADM 测试 LDAP 目录服务设置

要测试 LDAP 目录服务设置，请使用 `testfeature` 命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

9

系统配置锁定模式

系统配置锁定模式有助于在系统配置完成后防止意外更改。锁定模式适用于配置和固件更新。当系统被锁定时，任何改变系统配置的尝试都会被阻止。如果尝试更改关键系统设置，则会显示错误消息。启用系统锁定模式将阻止使用供应商工具进行第三方 I/O 卡的固件更新。

系统锁定模式仅适用于企业许可的客户。

在 4.40.00.00 版本中，系统锁定功能也扩展至 NIC。

注: NIC 的增强□定只包括防止固件更新的固件□定。不支持配置 (x-UEFI) □定。

注: 启用系□□定模式后，您无法更改任何配置□置。系□□置字段□禁用状□。

通过以下界面可以启用或禁用锁定模式：

- iDRAC Web 界面
- RACADM
- WSMan
- SCP（系统配置配置文件）
- Redfish
- 在开机自检期间使用 F2 并选择 iDRAC 设置
- 工厂系统擦除

注: 要启用□定模式，您必□具有 iDRAC Enterprise 或 Datacenter □可□和控制与配置系□权限。

注: 您可以在系□□于□定模式□□□ vMedia，但不允□配置□程文件共享。

注: OMSA、SysCfg 和 USC 等接口只能□□□置，但不能修改配置。

下表列出了受锁定模式影响的运行和未运行的功能、界面和公用程序：

注: 锁定模式启用时，不支持使用 iDRAC 更改引导顺序。但是，vConsole 菜单中提供了引导控制选项，当 iDRAC 处于锁定模式时，该选项无效。

表. 32: 受锁定模式影响的项目

已禁用	保持正常工作

• 删除许可证
• DUP 更新
• SCP 导入
• 重设为默认值
• OMSA/OMSS
• IPMI
• DRAC/LC
• DTK-Syscfg
• Redfish
• OpenManage Essentials
• BIOS（F2 设置变为只读）
• Group Manager
• 选择网卡
	• 电源操作 - 开机/关机、重设
	• 功率上限设置
	• 电源优先级
	• 识别设备（机箱或 PERC）
	• 部件更换、轻松还原以及系统板更换
	• 运行诊断程序
	• 模块化操作（FlexAddress 或远程分配地址）
	• Group Manager 密码
	• 可直接访问设备的所有供应商工具（排除所选 NIC）
	• 许可证导出
	• PERC
	  ○ PERC CLI
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• 可直接访问设备的所有供应商工具
	• NVMe
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R

表. 32: 受锁定模式影响的项目

已禁用	保持正常工作

	• BOSS-S1
	  ○ Marvell CLI
	  ○ F2/Ctrl+R
	• ISM/OMSA 设置（OS BMC 启用、监督程序 ping、OS 名称、OS 版本）

注: 已启用锁定模式时，不会在 iDRAC 登录页面中显示 OpenID Connect 登录选项。

10

配置 iDRAC 以进行单一登录或智能卡登录

本节提供配置 iDRAC 以进行智能卡登录（适用于本地用户和 Active Directory 用户）和单一 (SSO) 登录（适用于 Active Directory 用户）的信息。SSO 和智能卡登录是已许可的功能。

iDRAC 支持基于 Kerberos 的 Active Directory 验证来支持智能卡和 SSO 登录。有关 Kerberos 的信息，请参阅 Microsoft 网站。

主□：

Active Directory 单一登录或智能卡登录的前提条件

基于 Active Directory 的 SSO 或智能卡登录的前提条件包括：

- iDRAC 时间与 Active Directory 域控制器时间同步。否则，iDRAC 上的 kerberos 验证失败。您可以使用时区和 NTP 功能同步时间。要执行此操作，请参阅 配置时区和 NTP 页面上的 96。
- 将 iDRAC 注册为 Active Directory 根域中的计算机。
- 使用 ktpass 工具生成 keytab 文件。
- 要为扩展架构启用单一登录，请确保在 **Delegation（委派）**选项卡上为 keytab 用户选中了 **Trust this user for delegation to any service (Kerberos only)（对任何服务的委派均信任此用户（仅限 Kerberos））**选项。该选项卡仅在使用 ktpass 公用程序创建 keytab 文件后才可用。
- 配置浏览器以启用 SSO 登录。
- 创建 Active Directory 对象并提供所需权限。
- 对于 SSO，请为 iDRAC 所在子网的 DNS 服务器配置反向查询区域。

  注: 如果主机名与反向 DNS 查询不匹配，Kerberos 身份验证会失败。
- 配置浏览器以支持 SSO 登录。有关更多信息，请参阅 单一登录 页面上的 322。

  注: Google Chrome 和 Safari 不支持使用 Active Directory 进行 SSO 登录。

在域名系统上注册 iDRAC

在 Active Directory 根域中注册 iDRAC：

1. 单击 **iDRAC 设置** > **连接性** > **网络**。
   随即会显示**网络**页面。
2. 您可以根据 IP 设置选择 **IPv4 设置**或 **IPv6 设置**。
3. 提供有效的**首选/备用 DNS 服务器** IP 地址。该值是作为根域组成部分的有效 DNS 服务器 IP 地址。
4. 选择**向 DNS 注册 iDRAC**。
5. 提供有效 **DNS 域名**。
6. 验证网络 DNS 配置与 Active Directory DNS 信息匹配。
   有关各选项的更多信息，请参阅 *iDRAC 联机帮助*。

创建 Active Directory 对象并提供权限

登录到基于 Active Directory 标准方案的 SSO

对基于 Active Directory 标准方案的 SSO 登录执行以下步骤：

1. 创建用户组。
2. 为标准方案创建一个用户。

注： 使用现有的 AD 用户组和 AD 用户。

登录到基于 Active Directory 扩展方案的 SSO

对基于 Active Directory 扩展架构的 SSO 登录执行以下步骤：

1. 在 Active Directory 服务器中创建设备对象、权限对象和关联对象。
2. 设置所创建权限对象的访问权限。

   注： 建议不要提供管理员权限，因为这可能会绕过一些安全检查。
3. 使用关联对象关联设备对象和权限对象。
4. 将之前的 SSO 用户（登录用户）添加至设备对象。
5. 为*验证用户*提供访问权限，以访问创建的关联对象。

登录到 Active Directory SSO

对 Active Directory SSO 登录执行以下步骤：

1. 创建一个 Kerberos keytab 用户，其用于创建 keytab 文件。

注： 为每个 iDRAC IP 创建新的 KERBROS 密钥。

为 Active Directory 用户配置 iDRAC SSO 登录

在为 Active Directory SSO 登录配置 iDRAC 之前，请确保已完成所有前提条件。

当您基于 Active Directory 设置用户帐户时，可以为 Active Directory SSO 配置 iDRAC。

在 Active Directory 中创建用户以进行 SSO 登录

在 Active Directory 中创建用户以进行 SSO 登录，请执行以下操作：

1. 在组织单位中创建新用户。
2. 转至 **Kerberos 用户 > 属性 > 帐户 > 为此帐户使用 Kerberos AES 加密类型**
3. 使用以下命令在 Active Directory 服务器中生成 Kerberos Keytab：

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -mapuser
DOMAINNAME\username -mapop set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
[password] -out c:\krbkeytab
```

扩展方案注意事项

- 更改 Kerberos 用户的“委派”设置。
- 转至 **Kerberos 用户 > 属性 > 委派 > 对任何服务的委派均信任此用户（仅限 Kerberos）**

注： 更改以上设置后，让管理站 Active Directory 用户注销然后重新登录。

生成 Kerberos Keytab 文件

为支持 SSO 和智能卡登录身份验证，iDRAC 支持相应的配置，以在 Windows Kerberos 网络上启用自身作为 Kerberos 服务。iDRAC 上的 Kerberos 配置涉及的步骤与将非 Windows Server Kerberos 服务配置为 Windows Server Active Directory 中的安全主体相同。

ktpass 工具（由 Microsoft 作为服务器安装 CD/DVD 的一部分提供）用于创建到用户帐户的服务主体名称 (SPN) 绑定，并将信任信息导出到 MIT 式 Kerberos *密钥表*文件中，这可实现外部用户或系统与密钥分发中心 (KDC) 之间的信任关系。密钥表文件包含加密密钥，用于对服务器和 KDC 之间的信息进行加密。Ktpass 工具允许基于 UNIX 的服务（支持 Kerberos 身份验证）使用由 Windows Server Kerberos KDC 服务提供的互操作功能。有关 **ktpass** 实用程序的详细信息，请参阅 Microsoft 网站：**technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

在生成密钥表文件之前，您必须创建一个 Active Directory 用户帐户，以便与 `ktpass` 命令的 **-mapuser** 选项一起使用。此外，您必须具有与您将生成的密钥表文件上传到的 iDRAC DNS 相同的名称。

使用 ktpass 工具生成 keytab 文件：

1. 在希望将 iDRAC 映射到 Active Directory 中用户帐户的域控制器（Active Directory 服务器）上运行 *ktpass* 公用程序。
2. 使用以下 ktpass 命令创建 Kerberos keytab 文件：

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -mapuser
DOMAINNAME\username -mapop set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
[password] -out c:\krbkeytab
```

加密类型为 AES256-SHA1。主体类型为 KRB5_NT_PRINCIPAL。服务主体名称将映射到的目标用户帐户的属性必须启用**为此帐户使用 AES 256 加密类型**属性。

注: 对于 **iDRACname** 和**服务主体名称**，请使用小写字母。请对域名使用大写字母，如示例中所示。

将生成一个 keytab 文件。

注: 如果发现为其创建密钥表文件的 iDRAC 用户存在任何问题，请创建一个新用户和一个新的密钥表文件。如果再次执行最初创建的同一密钥表文件，则无法正确配置。

使用 Web 界面为 Active Directory 用户配置 iDRAC SSO 登录

要配置 iDRAC 以进行 Active Directory SSO 登录：

注: 有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

1. 验证 iDRAC DNS 名称与 iDRAC 完全限定的域名是否匹配。要执行此操作，请在 iDRAC Web 界面中，转至 **iDRAC 设置** > **网络** > **常见设置**，然后参阅 **DNS iDRAC 名称**属性。
2. 配置 Active Directory 以基于标准架构或扩展架构设置用户帐户时，请执行以下两个附加步骤来配置 SSO：
   - 在 **Active Directory Configuration and Management Step 1 of 4（Active Directory 配置和管理第 1 步，共 4 步）**页面中上载 keytab 文件。
   - 在 **Active Directory Configuration and Management Step 2 of 4（Active Directory 配置和管理第 2 步，共 4 步）**页面中选择**启用单一登录**选项。

使用 RACADM 为 Active Directory 用户配置 iDRAC SSO 登录

要启用 SSO，完成步骤以配置 Active Directory，并运行以下命令：

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

管理站设置

为 Active Directory 用户配置 SSO 登录后，请执行以下步骤：

1. 在“网络”属性中设置 DNS 服务器 IP 并提供首选 DNS 服务器 IP。
2. 转至“我的电脑”并添加 ***domain.tld** 域。
3. 将 Active Directory 用户添加至管理员（方法是导航到**我的电脑** > **管理** > **本地用户和组** > **组** > **管理员**），并添加 Active Directory 用户。

4. 注销系统并使用 Active Directory 用户凭据登录。
5. 在 Internet Explorer 设置中，添加 *domain.tld 域，如下所示：
   a. 转至**工具** > **Internet 选项** > **安全** > **本地 Internet** > **站点**，取消选中**自动检测 Intranet 网络设置**。选择其余的三个选项，然后单击**高级**以添加 *domain.tld。
   b. 在 IE 中打开新窗口，并使用 iDRAC 主机名启动 iDRAC GUI。
6. 在 Mozilla Firefox 设置中，添加 *domain.tld 域：
   - 启动 Firefox 浏览器并在 URL 中键入 about:config。
   - 在过滤器文本框中使用协商。双击包含 *auth.trusted.uris* 的结果。键入该域，保存设置并关闭浏览器。
   - 在 Firefox 中打开新窗口，并使用 iDRAC 主机名启动 iDRAC GUI。

启用或禁用智能卡登录

在启用或禁用 iDRAC 的智能卡登录之前，请确保：
- 您具有“配置 iDRAC”权限。
- 具有相应证书的 iDRAC 本地用户配置或 Active Directory 用户配置已完成。

注： 如果智能卡登□已启用，□ SSH、Telnet、LAN 上 IPMI、LAN 上串行和□程 RACADM 均已禁用。此外，如果您禁用智能卡登□，□接口不会自□启用。

使用 Web 界面启用或禁用智能卡登录

要启用或禁用智能卡登录功能：
1. 在 iDRAC Web 界面中，转到 **iDRAC Settings（iDRAC 设置）** > **Users（用户）** > **Smart Card（智能卡）**。
   随即会显示 **Smart Card（智能卡）**页面。
2. 从 **Configure Smart Card Logon（配置智能卡登录）**下拉菜单中，请选择 **Enabled（启用）**以启用智能卡登录，或者选择 **Enabled With Remote RACADM（使用远程 RACADM 启用）**。否则，选择 **Disabled（已禁用）**。
   有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**应用设置。
   使用 iDRAC Web 界面进行任何后续登录尝试时，系统会提示您进行智能卡登录。

使用 RACADM 启用或禁用智能卡登录

要启用智能卡登录，请使用 `set` 命令以及 `iDRAC.SmartCard` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序启用或禁用智能卡登录

要启用或禁用智能卡登录功能：
1. 在 iDRAC 设置公用程序中，转至 **Smart Card（智能卡）**。
   将显示 **iDRAC Settings Smart Card（iDRAC 设置智能卡）**页面。
2. 选择 **Enabled（已启用）**以启用智能卡登录。否则，选择 **Disabled（已禁用）**。有关选项的更多信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   智能卡登录功能将根据选择启用或禁用。

配置智能卡登录

注： 对于 Active Directory 智能卡配置，必须使用标准方案或扩展方案 SSO 登录配置 iDRAC。

为 Active Directory 用户配置 iDRAC 智能卡登录

为 Active Directory 用户配置 iDRAC 智能卡登录之前，请确保您已完成所需的前提条件。

要配置 iDRAC 以进行智能卡登录：

1. 在 iDRAC Web 界面中，配置 Active Directory 以设置基于标准架构或扩展架构的用户帐户时，在 **Active Directory 配置和管理步骤 1 / 4** 页面中：
   - 启用证书验证。
   - 上载信任的 CA 签名证书。
   - 上载 Keytab 文件。
2. 启用智能卡登录。有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

为本地用户配置 iDRAC 智能卡登录

要配置 iDRAC 本地用户以进行智能卡登录：

1. 将智能卡用户证书和受信 CA 证书上载到 iDRAC。
2. 启用智能卡登录。

上载智能卡用户证书

上载用户证书之前，请确保来自智能卡供应商的用户证书以 Base64 格式导出。SHA-2 证书也受支持。

使用 Web 界面上载智能卡用户证书

上载智能卡用户证书：

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置** > **用户** > **智能卡**。

   注: 智能卡登录功能需要本地配置和/或 Active Directory 用户证书。

2. 在**配置智能卡登录**下，选择**与远程 RACADM 一起启用**以启用配置。
3. 设置选项为**启用智能卡登录的 CRL 检查**。
4. 单击**应用**。

使用 RACADM 上载智能卡用户证书

要上载智能卡用户证书，请使用 **usercertupload** 对象。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

请求用于进行智能卡注册的证书

执行以下步骤以申请用于进行智能卡注册的证书：

1. 将智能卡连接至客户端系统并安装所需的驱动程序和软件。
2. 在设备管理器中验证驱动程序状态。
3. 在浏览器中启动智能卡注册代理程序。
4. 输入**用户名**和**密码**，然后单击**确定**。
5. 单击**请求证书**。
6. 单击**高级证书请求**。
7. 通过使用智能卡证书注册站，代表另一个用户单击智能卡的**请求证书**。
8. 通过单击**选择用户**按钮选择要注册的用户。
9. 单击**注册**并输入智能卡凭据。
10. 输入智能卡 PIN，并单击**提交**。

上载智能卡的信任 CA 证书

上载 CA 证书之前，请确保拥有 CA 签名的证书。

使用 Web 界面上载智能卡的受信 CA 证书

上载用于智能卡登录的受信 CA 证书：

1. 在 iDRAC Web 界面中，转至 **iDRAC Settings（iDRAC 设置）** > **Network（网络）** > **User Authentication（用户验证）** > **Local Users（本地用户）**。
   此时将显示**用户**页面。
2. 在 **User ID**（用户 ID）列中，单击用户 ID 编号。
   将显示 **Users Main Menu（用户主菜单）**页面。
3. 在 **Smart Card Configurations（智能卡配置）**下，选择 **Upload Trusted CA Certificate（上载受信 CA 证书）**，然后单击 **Next（下一步）**。
   将显示 **Trusted CA Certificate Upload（受信 CA 证书上载）**页面。
4. 浏览并选择受信 CA 证书，然后单击**应用**。

使用 RACADM 为智能卡上载受信 CA 证书

要上载用于智能卡登录的受信 CA 证书，请使用 **usercertupload** 对象。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用智能卡登录

注: 只有 Internet Explorer 上支持智能卡登录。

要使用智能卡登录：

1. 启用智能卡后，从 iDRAC GUI 注销。
2. 使用 `http://IP/` 启动或使用 FQDN `http://FQDN/` 启动
3. 下载智能卡插件后，单击**安装**。
4. 输入智能卡 PIN，并单击**提交**。
5. iDRAC 将使用智能卡成功登录。

11

配置 iDRAC 以发送警报

您可以在受管系统设置的特定事件的警报和操作。当系统组件的状况大于预定义条件时，就会发生事件。如果事件与事件筛选器匹配并且您已配置该筛选器以生成警报（电子邮件、SNMP 陷阱、IPMI 警报、远程系统日志、Redfish 事件或 WS 事件），然后警报将发送到一个或多个配置目标。如果同一事件筛选器还被配置为执行操作（例如重新引导、关机后重启或关闭系统电源），则将执行该操作。您只能为每个事件设置一个操作。

要配置 iDRAC 以发送警报，请执行以下操作：

1. 启用警报。
2. 您还可以根据类别或严重程度筛选警报。
3. 配置电子邮件警报、IPMI 警报、SNMP 陷阱、远程系统日志、Redfish 事件、操作系统日志和/或 WS 事件设置。
4. 启用事件警报和操作，如：
   - 将电子邮件警报、IPMI 警报、SNMP 陷阱、远程系统日志、Redfish 事件、操作系统日志或 WS 事件发送到已配置的目标。
   - 对受管系统执行重新引导、关机或关机后再开机操作。

主□：

启用或禁用警报

如需将警报发送到配置的目标或者执行事件操作，您必须启用全局警报选项。此属性会覆盖设置的单个警报或事件操作。

使用 Web 界面启用或禁用警报

要启用或禁用生成警报，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **警报配置**。
   随即会显示**警报**页面。
2. 在**警报**部分：
   - 选择**启用**以启用警报生成或执行事件操作。
   - 选择**禁用**以禁用警报生成或禁用事件操作。
3. 单击**应用**保存设置。

快速警报配置

要批量配置警报，请执行以下操作：

1. 转至**警报配置**页面下的**快速警报配置**。
2. 在**快速警报配置**部分下，执行以下操作：
   - 选择警报类别。

- 选择问题严重性通知。
- 选择您想要接收这些通知的位置。

3. 单击**应用**保存设置。

注: 必须选择至少 1 个类别、1 个严重性和 1 个目标类型以应用配置。

所有已配置警报的总数显示在**警报配置摘要**下。

使用 RACADM 启用或禁用警报

使用以下命令：

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 — 已禁用

n=1 — 已启用

使用 iDRAC 设置公用程序启用或禁用警报

启用或禁用警报或事件生成操作：

1. 在 iDRAC 设置公用程序中，转至 **Alerts（警报）**。
   将显示 **iDRAC Settings Alerts（iDRAC 设置警报）**页面。
2. 在 **Platform Events（平台事件）**下，选择 **Enabled（已启用）**，以启用警报生成或事件操作。否则，选择 **Disabled（已禁用）**。有关选项的更多信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   警报设置配置完成。

筛选警报

您可以根据类别和严重性筛选警报。

使用 iDRAC Web 界面筛选警报

要根据类别和严重性过滤警报：

注: 即使您是具有只读权限的用户，也可以过滤警报。

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Alerts and Remote System Log Configuration（警报和远程系统日志配置）**。
2. 在 **Alerts and Remote System Log Configuration（警报和远程系统日志配置）**部分，选择 **Filter（筛选器）**：
   - 系统运行状况 — 表示系统机箱内与硬件相关的所有警报的系统运行状况类别。示例包括温度故障、电压故障、设备错误。
   - 存储运行状况 — 存储运行状况类别代表与存储子系统相关的警报。示例包括控制器错误、物理磁盘错误、虚拟磁盘错误。
   - 配置 — 表示与硬件、固件和软件配置更改相关的警报配置类别。示例包括添加/移除的 PCI-E 卡、更改的 RAID 配置、更改的 iDRAC 许可证。
   - 审核 — 表示审核日志的审核类别。示例包括用户登录/注销信息、密码验证故障、会话信息、电源状态。
   - 更新 — 更新类别表示由于固件/驱动程序升级/降级生成的警报。
     注: 这不表示固件资源清册。
   - 工作注释
3. 选择下列一个或多个严重性等级：
   - 通知
   - 警告
   - 严重

4. 单击**应用**。
   Alert Results（警报结果）部分将根据所选的类别和严重性显示结果。

使用 RACADM 筛选警报

要筛选警报，请使用 **eventfilters** 命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

设置事件警报

您可以设置要发送给配置目标的事件警报，例如电子邮件警报、IPMI 警报、SNMP 陷阱、远程系统日志、操作系统日志和 WS 事件。

使用 Web 界面设置事件警报

要使用 Web 界面设置事件警报：

1. 确保您已经配置了电子邮件警报、IPMI 警报、SNMP 陷阱设置和/或远程系统日志设置。
2. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **警报和远程系统日志配置**。
3. 在**类别**下，选择以下所需事件的一个或所有警报：
   - 电子邮件
   - SNMP 陷阱
   - IPMI 警报
   - 远程系统日志
   - WS 事件
   - 操作系统日志
   - Redfish 事件
4. 选择**操作**。
   设置即会保存。
5. （可选）您可以发送测试事件。在**消息 ID 到测试事件**字段中，输入要测试的消息 ID（如果已生成警报），并单击**测试**。有关系统固件和代理（用于监测系统组件）生成的事件和错误消息的更多信息，请参阅 iDRACmanuals 上的*事件和错误消息参考指南*。

使用 RACADM 设置事件警报

要使用 **eventfilters** 命令设置事件警报。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

设置警报复现事件

如果系统继续在大于进气孔温度阈值限制的温度下运行，您可以配置 iDRAC 以生成具有特定间隔的附加事件。默认间隔为 30 天。有效范围是 0 到 366 天。值为“0”表示禁用事件复现。

注： 您必□具有“配置 iDRAC”权限，才能□置警□复□□。

使用 RACADM 设置警报复现事件

要使用 RACADM 设置警报复现事件，请使用 **eventfilters** 命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC Web 界面设置警报复现事件

设置警报复现值：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Alert Recurrence（警报复现）**。
2. 在**复现**列中，为所需的类别、警报和严重性类型输入警报频率值。
   有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。
   将保存警报复现设置。

设置事件操作

您可以设置事件操作，例如在系统上执行重新引导、关机后再开机、关机或不执行操作。

使用 Web 界面设置事件操作

设置事件操作：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Alert and Remote System Log Configuration（警报和远程系统日志配置）**。
2. 在 **Actions（操作）**下拉式菜单中，为每个事件选择一个操作：
   - 重新引导
   - 关闭电源后重启
   - Power Off（关闭电源）
   - 无操作
3. 单击**应用**。
   设置即会保存。

使用 RACADM 设置事件操作

要配置事件操作，请使用 `eventfilters` 命令。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

配置电子邮件警报、SNMP 陷阱或 IPMI 陷阱设置

管理站使用简单网络管理协议 (SNMP) 和智能平台管理接口 (IPMI) 陷阱从 iDRAC 接收数据。对于带有大量节点的系统，管理站针对每种可能发生的情况轮询每个 iDRAC 的效率较低。例如，事件陷阱可以帮助管理站在节点之间实现负载平衡或通过在身份验证发生故障时发出警报。SNMP v1、v2 和 v3 格式均受支持。

您可以配置 IPv4 和 IPv6 警报目标、电子邮件设置和 SMTP 服务器设置，并测试这些设置。您还可以指定要向其发送 SNMP 陷阱的 SNMP v3 用户。

在配置电子邮件、SNMP 或 IPMI 陷阱设置之前，请确保：

- 您具有 Configure RAC（配置 RAC）的权限。
- 已经配置事件筛选器。

配置 IP 警报目标

您可以配置 IPv6 或 IPv4 地址以接收 IPMI 警报或 SNMP 陷阱。

有关使用 SNMP 监测服务器时所需的 iDRAC MIB 的更多信息，请参阅 *Dell EMC OpenManage SNMP 参考指南，网址：*https://www.dell.com/openmanagemanuals。

使用 Web 界面设置 IP 警报目标

要使用 Web 界面配置警报目标设置，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **SNMP and E-mail Settings（SNMP 和电子邮件设置）**。
2. 选择 **State**（状态）选项启用警报目标（IPv4 地址、IPv6 地址或完全限定域名 (FQDN)）来接收陷阱。
   您最多可以指定八个目标地址。有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 选择要向其发送 SNMP 陷阱的 SNMP v3 用户。
4. 输入 iDRAC SNMP 团体字符串（只适用于 SNMPv1 和 SNMP v2）和 SNMP 警报端口号。
   有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
   注: 团体字符串值表示要在从 iDRAC 发送的简单网络管理协议 (SNMP) 警报陷阱中使用的团体字符串。请确保目标团体字符串与 iDRAC 团体字符串相同。默认值是“Public”（公共）。
5. 要测试 IP 地址是否正在接收 IPMI 或 SNMP 陷阱，请单击 **Send**（发送）（分别位于 **Test IPMI Trap**（测试 IPMI 陷阱）和 **Test SNMP Trap**（测试 SNMP 陷阱）下）。
6. 单击**应用**。
   警报目标即完成配置。
7. 在 **SNMP 陷阱格式**部分中，选择要用于发送陷阱目标上陷阱的协议版本 - **SNMP v1**、**SNMP v2** 或 **SNMP v3**，然后单击**应用**。
   注: **SNMP Trap Format（SNMP 陷阱格式）**选项仅适用于 SNMP 陷阱，不适用于 IPMI 陷阱。IPMI 陷阱始终以 SNMP v1 格式发送，不会基于配置的 **SNMP Trap Format（SNMP 陷阱格式）**选项。

   SNMP 陷阱格式即完成配置。

使用 RACADM 配置 IP 警报目标

配置陷阱警报设置：

1. 启用陷阱：

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

参数	说明
<index>	目标索引。允许的值为 1 到 8。
<n>=0 **<n>**=1	禁用陷阱 启用陷阱

2. 配置陷阱目标地址：

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

参数	说明
<index>	目标索引。允许的值为 1 到 8。
<Address>	有效 IPv4、IPv6 或 FQDN 地址

3. 配置 SNMP 公共名称字符串：

```
racadm set idrac.ipmilan.communityname <community_name>
```

参数	说明
<community_name>	SNMP 团体名称。

4. 要配置 SNMP 目标：

- 设置 SNMPv3 的 SNMP 陷阱目标：

  ```
  racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
  ```

- 为陷阱目标设置 SNMPv3 用户：

  ```
  racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
  ```

- 为用户启用 SNMPv3：

  ```
  racadm set idrac.users.<index>.SNMPv3Enable Enabled
  ```

5. 如有必要，请测试陷阱：

   ```
   racadm testtrap -i <index>
   ```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置 IP 警报目标

您可以使用 iDRAC 设置公用程序配置警报目标（IPv4、IPv6 或 FQDN）。要执行此操作：

1. 在 **iDRAC Settings utility**（iDRAC 设置公用程序中）中，转至 **Alerts**（警报）。
   将显示 **iDRAC Settings Alerts**（iDRAC 设置警报）页面。
2. 在 **Trap Settings（陷阱设置）**下，启用接收陷阱的 IP 地址，并输入 IPv4、IPv6 或 FQDN 目标地址。您最多可以指定 8 个地址。
3. 输入团体字符串名称。
   有关各选项的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
4. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   警报目标即完成配置。

配置电子邮件警报设置

您可以配置发件人电子邮件地址和收件人（目标）电子邮件地址以接收电子邮件警报。此外，配置 SMTP 服务器地址设置。

注: □子□件警□支持 IPv4 和 IPv6 地址。使用 IPv6 □，必□指定 iDRAC DNS 域名。

注: 如果正在使用外部 SMTP 服□器，□确保 iDRAC 可与□服□器通信。如果□服□器无法□□，□在□□□送□□□件□会□示□□ RAC0225。

使用 Web 界面配置电子邮件警报设置

要使用 Web 界面配置电子邮件警报设置，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **SMTP（电子邮件）配置。**
2. 键入有效的电子邮件地址。
3. 单击**测试电子邮件**下的**发送**测试配置的电子邮件警报设置。
4. 单击**应用。**
5. 请为 SMTP（电子邮件）服务器设置提供以下详细信息：
   - SMTP（电子邮件）服务器 IP 地址或 FQDN/DNS 名称
   - 自定义发件人地址 - 此字段包含以下选项：
     - **默认** - 不可编辑"地址"字段
     - **自定义** - 您可以输入可从中接收电子邮件警报的电子邮件 ID
   - 自定义邮件主题前缀 - 此字段包含以下选项：
     - **默认** - 不可编辑默认邮件
     - **自定义** - 您可以选择要在电子邮件的**主题**行中显示的消息
   - SMTP 端口号 - 可以加密连接，并且可以通过安全端口发送电子邮件：
     - **无加密** - 端口 25（默认值）

- **SSL** — 端口 465
- 连接加密 - 当您的公司没有电子邮件服务器时，您可以使用基于云的电子邮件服务器或 SMTP 中继。要配置云电子邮件服务器，您可以从下拉列表中将此功能设置为以下任意值：
  - **无** - 与 SMTP 服务器的连接没有加密。这是默认值。
  - **SSL** — 通过 SSL 运行 SMTP 协议

  注：
  - 此功能无法通过组管理器配置。
  - 这是一项需要许可的功能，在 iDRAC Basic 许可证中不可用。
  - 您必须具备“配置 iDRAC”权限才能使用此功能。
- 验证
- 用户名

对于服务器设置，端口使用情况取决于 `connectionencryptiontype`，并且只能使用 RACADM 进行配置。

6. 单击**应用**。有关各选项的更多信息，请参阅 *iDRAC 联机帮助*。

使用 RACADM 配置电子邮件警报设置

1. 要启用电子邮件警报，请执行以下操作：

```
racadm set iDRAC.EmailAlert.Enable.[index] [n]
```

参数	说明
index	电子邮件目标索引。允许的值为 1 到 4。
n=0 **n=1**	禁用电子邮件警报。 启用电子邮件警报。

2. 要配置电子邮件设置，请执行以下操作：

```
racadm set iDRAC.EmailAlert.Address.[index] [email-address]
```

参数	说明
index	电子邮件目标索引。允许的值为 1 到 4。
email-address	接收平台事件警报的目的地电子邮件地址。

3. 要配置发件人电子邮件设置，请执行以下操作：

```
racadm set iDRAC.RemoteHosts.[index] [email-address]
```

参数	说明
index	发件人电子邮件地址索引。
email-address	发送平台事件警报的发件人电子邮件地址。

4. 配置自定义信息：

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

参数	说明
index	电子邮件目标索引。允许的值为 1 到 4。
custom-message	自定义消息

5. 要测试配置的电子邮件警报（如有必要），请执行以下操作：

```
racadm testemail -i [index]
```

参数	说明
index	要测试的电子邮件目标索引。允许的值为 1 到 4。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

配置 SMTP 电子邮件服务器地址设置

您必须配置 SMTP 服务器地址以将电子邮件警报发送到指定目标。

使用 iDRAC Web 界面配置 SMTP 电子邮件服务器地址设置

配置 SMTP 服务器地址：

1. 在 iDRAC Web 界面中，转至 **Configuaration（配置）** > **System Settings（系统设置）** > **Alert Configuration（警报配置）** > **SNMP (E-mail Configuration)（SNMP [电子邮件配置]）**。
2. 输入要在配置中使用的 SMTP 服务器的有效 IP 地址或完全限定域名 (FQDN)。
3. 选择 **Enable Authentication**（启用验证）选项，然后提供用户名和密码（有权访问 SMTP 服务器的用户的用户名和密码）。
4. 输入 SMTP 端口号。
   有关各字段的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
5. 单击**应用**。
   SMTP 设置已配置。

使用 RACADM 配置 SMTP 电子邮件服务器地址设置

要配置 SMTP 电子邮件服务器，请执行以下操作：

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

配置 WS 事件

WS 事件协议用于客户端服务（用户）向服务器（事件源）注册感兴趣（订阅）的内容，从而接收包含服务器事件的消息（通知或事件消息）。有兴趣接收 WS 事件消息的客户可以订阅 iDRAC 并接收与 Lifecycle Controller 作业相关的事件。

配置 WS 事件功能以接收与 Lifecycle Controller 作业相关的变更的 WS 事件消息所需的步骤在针对 iDRAC 1.30.30 的 Web 服务事件支持规范文档中提供了说明。除了本规范，请参阅 DSP0226（DMTF WS 管理规范）、部分 10 通知（事件）文档，以了解完整的 WS 事件协议的信息。在 DCIM 作业控制配置文件文档中介绍了 Lifecycle Controller 相关作业。

配置 Redfish 事件

Redfish 事件协议用于客户端服务（订阅者）以为服务器（事件源）注册利益（订阅），接收包含 Redfish 事件的消息（通知或事件消息）。对接收 Redfish 事件消息感兴趣的客户可以订阅 iDRAC 并接收与事件相关的 Lifecycle Controller 作业。

监测机箱事件

在 PowerEdge FX2/FX2s 机箱中，您可以在 iDRAC 中启用**机箱管理和监视**设置，以执行机箱管理和监视任务，例如监视机箱组件、配置警报、使用 iDRAC RACADM 传递 CMC RACADM 命令和更新机箱管理固件。此设置允许您管理机箱中的服务器，即使 CMC 不在网络上也是如此。您可以将值设置为**已禁用**以转发机箱事件。默认情况下，此设置设为**已启用**。

注: □□此□置生效，必□确保在 CMC 中，将**服务器模式下的机箱管理**□置□□**监测**或**管理和监测**。

当**机箱管理和监视**选项设置为**已启用**时，iDRAC 会生成并记录机箱事件。生成的事件会集成到 iDRAC 事件子系统中，并且会生成与其余事件相似的警报。

CMC 还会将生成的事件转发到 iDRAC。如果服务器上的 iDRAC 无法正常工作，CMC 将对前 16 个事件进行排队并将其余事件记录在 CMC 日志中。一旦**机箱监视**设置为已启用，这 16 个事件将发送至 iDRAC。

在 iDRAC 检测到缺少必需 CMC 功能的场合，将显示警告消息，通知您如果不升级 CMC 固件，某些功能可能无法运行。

注: iDRAC 不支持以下机箱属性：

- `ChassisBoardPartNumber`
- `ChassisBoardSerialNumber`

使用 iDRAC Web 界面监测机箱事件

要使用 iDRAC Web 界面监测机箱事件，请执行以下步骤：

注: 本部分仅适用于 PowerEdge FX2/FX2s 机箱，并且仅当在 CMC 中将**服务器模式下的机箱管理**设置为**监测**或**管理和监测**时才出现。

1. 在 CMC 界面中，单击 **Chassis Overview（机箱概览）** > **Setup（设置）** > **General（常规）**。
2. 从**服务器模式下的机箱管理**下拉菜单中，选择**管理和监测**，然后单击**应用**。
3. 启动 iDRAC Web 界面，单击 **Overview（概览）** > **iDRAC Settings（iDRAC 设置）** > **CMC**。
4. 在**服务器模式下的机箱管理**部分下，确保将 **iDRAC 中的功能**下拉列表框设置为**已启用**。

使用 RACADM 监测机箱事件

此设置仅适用于 PowerEdge FX2/FX2s 服务器，并且仅当在 CMC 中将**服务器模式下的机箱管理**设置为**监测**或**管理和监测**时才适用。

要使用 iDRAC RACADM 检测机箱事件：

```
racadm get system.chassiscontrol.chassismanagementmonitoring
```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

警报消息 ID

下表提供了显示警报的信息 ID 的列表。

表. 33: 警报信息 ID

信息 ID	说明	说明（用于 MX 平台）
AMP	安培	安培
ASR	自动重置系统	自动重置系统
BAT	电池事件	电池事件
BIOS	BIOS 管理	BIOS 管理
引导	引导控制	引导控制
CBL	电缆	电缆
CPU	处理器	处理器
CPUA	处理器不存在	处理器不存在

表. 33: 警报信息 ID （续）

信息 ID	说明	说明（用于 MX 平台）
CTL	存储控制	存储控制
DH	证书管理	证书管理
DIS	自动查找	自动查找
ENC	存储机柜	存储机柜
FAN	风扇事件	风扇事件
FSD	调试	调试
HWC	硬件配置	硬件配置
IPA	DRAC IP 更改	DRAC IP 更改
ITR	侵入	侵入
JCP	作业控制	作业控制
LC	Lifecycle Controller	Lifecycle Controller
LIC	许可	许可
LNK	链路状态	链路状态
LOG	日志事件	日志事件
MEM	内存	内存
NDR	NIC 操作系统驱动程序	NIC 操作系统驱动程序
NIC	NIC 配置	NIC 配置
OSD	操作系统部署	操作系统部署
OSE	操作系统事件	操作系统事件
PCI	PCI 设备	PCI 设备
PDR	物理磁盘	物理磁盘
PR	部件交换	部件交换
PST	BIOS 开机自检	BIOS 开机自检
PSU	电源	电源
PSUA	PSU 不存在	PSU 不存在
PWR	电源使用	电源使用
RAC	RAC 事件	RAC 事件
RDU	冗余	冗余
RED	固件下载	固件下载

表. 33: 警报信息 ID （续）

信息 ID	说明	说明（用于 MX 平台）
RFL	IDSDM 介质	IDSDM 介质
RFLA	IDSDM 不存在	IDSDM 不存在
RFM	FlexAddress SD	不适用
RRDU	IDSDM 冗余	IDSDM 冗余
RSI	远程服务	远程服务
SEC	安全事件	安全事件
系统事件日志	系统事件日志	系统事件日志
SRD	软件 RAID	软件 RAID
SSD	PCIe SSD	PCIe SSD
STOR	存储	存储
SUP	固件更新作业	固件更新作业
SWC	软件配置	软件配置
SWU	软件更改	软件更改
SYS	系统信息	系统信息
TMP	温度	温度
TST	测试警报	测试警报
UEFI	UEFI 事件	UEFI 事件
USR	用户跟踪	用户跟踪
VDR	虚拟磁盘	虚拟磁盘
VF	vFlash SD 卡	vFlash SD 卡
VFL	vFlash 事件	vFlash 事件
VFLA	vFlash 不存在	vFlash 不存在
VLT	电压	电压
VME	虚拟介质	虚拟介质
VRM	虚拟控制台	虚拟控制台
WRK	工作注释	工作注释

12

iDRAC 9 Group Manager

Group Manager 使用□可以□有多个控制台体□，并且提供□化的基本 iDRAC 管理。

Dell 第 14 代服务器可以利用 iDRAC 组管理器功能来简化管理使用 iDRAC GUI 的位于本地网络上的 iDRAC 和关联服务器。组管理器提供一对多控制台体验，而不涉及单独的应用程序。它允许用户通过执行更强大的功能查看一组服务器的详细信息，而不是直观地检查服务器故障和使用其他手动方法。

组管理器是一项受许可的功能，也是企业版许可证的一部分。只有 iDRAC 管理员用户可以访问 Group Manager 功能。

注: □了提供更好的用□体□，Group Manager 支持多达 250 个服□器□点。

主□：

Group Manager

要使用 **Group Manager** 功能，您需要从 iDRAC 索引页面或 Group Manager 欢迎屏幕上启用 **Group Manager**。Group Manager 欢迎屏幕提供下表所列的选项。

表. 34: Group Manager 中的选项

选项	说明
加入现有组	允许您加入现有的组，您需要了解**组名称**和**密码**以加入特定的组。 **注:** 密码与 iDRAC 用户凭据关联。然而，一个密码与一个组相关联，以便在同一组中的不同 iDRAC 之间建立经过身份验证的设备通信。
创建新组	允许您创建新组。具有已创建组的特定 iDRAC 将是主组（主控制器）。
禁用该系统的组管理器	如果不想加入特定系统的任何组，请选择此选项。但是，您可以随时通过选择 iDRAC 索引页面中的"打开组管理器"来访问组管理器。一旦禁用了组管理器，用户需要等待 60 秒，才能执行进一步组管理器操作。

一旦 Group Manager 功能已启用，则 iDRAC 可让您选择创建或加入一个 iDRAC 本地组。本地网络中可以设置多个 iDRAC 组，但单个 iDRAC 每次只能是一个组的成员。要更改组（加入新组），iDRAC 必须首先离开其当前组，然后再加入新组。默认情况下，创建了组的 iDRAC 将选定为组的主控制器。用户无需定义专用 Group Manager 主控制器以控制该组。主控制器将托管 Group Manager Web 界面，并提供基于 GUI 的工作流程。如果当前的主控制器离线较长时间，则 iDRAC 成员会为该组自选一个新的主控制器，但这不会影响最终用户。通过从 iDRAC 索引页面单击 Group Manager，您可以从所有 iDRAC 成员正常访问 Group Manager。

摘要视图

您需要具有管理员权限才能访问组管理器页面。如果非管理员用户登录到 iDRAC，则组管理器部分不会显示各自的凭据。组管理器主页（摘要视图）大致分为三个部分。第一个部分显示汇总摘要以及汇总摘要详细信息。

- 本地组中服务器总数。
- 显示每个服务器型号的服务器数量的图表。
- Doughnut 图表按运行状况状态显示服务器（单击图表部分可筛选服务器列表，以便仅显示具有所选运行状况的服务器）。
- 如果在本地网络中检测到重复的组，则显示警告框。重复的组通产具有相同的名称，但密码不同。如果没有重复的组，则不显示此警告框。
- 显示控制组的 iDRAC（主要和次要控制器）。

第二个部分提供了在整个组上执行操作的按钮，第三个部分显示了组中所有 iDRAC 的列表。

它将显示组中的所有系统及其当前的运行状况状态，并且允许用户按需采取更正措施。服务器属性特定于下表中所述的服务器。

表. 35: 服务器属性

服务器属性	说明
运行状况	表示特定服务器的运行状况。
主机名	显示服务器名称。
iDRAC IP 地址	显示确切的 IPV4 和 IPV6 地址。
服务标签	显示服务标签信息。
型号	显示 Dell 服务器的型号。
iDRAC	显示 iDRAC 版本。
上次状态更新	显示服务器状态上次更新的时间戳。

“System Information”（系统信息）面板提供关于服务器的详细信息，例如，iDRAC 网络连接状态、服务器主机电源状态、快速服务代码、操作系统、资产标签、节点 ID、IDRAC DNS 名称、服务器 BIOS 版本、服务器 CPU 信息、系统内存以及位置信息。您可以在行上双击，或单击启动 iDRAC 按钮，以执行单一签名登录重定向至所选 iDRAC 索引页面。在所选服务器上，可以从“More Actions”（更多操作）下拉列表访问虚拟控制台或执行服务器电源操作。

管理 iDRAC 用户登录、警报配置和组资源清册导出为支持的组操作。

网络配置要求

Group Manager 使用 IPv6 链路本地网络在 iDRAC 之间进行通信（不包括 Web 浏览器 GUI）。链路本地通信被定义为非路由数据包，这意味着不能在本地组中加入由路由器分隔的任何 iDRAC。如果分配给 vLAN 的是 iDRAC 专用端口或共享 LOM，则 vLAN 会限制可以加入组的 iDRAC 数量（iDRAC 必须在同一 vLAN 上且流量不得通过路由器传递）。

启用 Group Manager 后，无论 iDRAC 的当前用户定义网络配置如何，iDRAC 都会启用 IPv6 链路本地地址。当 iDRAC 被配置为 IPv4 或 IPv6 IP 地址时，可以使用 Group Manager。

Group Manager 使用 mDNS 查找网络上的其他 iDRAC，并使用链路本地 IP 地址发送加密的数据包。使用 IPv6 链路本地网络意味着 Group Manager 端口和数据包绝不会离开本地网络，也不能访问外部网络。

端口（特定于 Group Manager 的独特功能不包括所有 iDRAC 端口）为：

- 5353 (mDNS)
- 443（Web 服务器） - 可配置
- 5670（多播组通信）
- C000 -> F000 动态识别用于每个成员在组中进行通信的一个空闲端口

最佳网络实践

- 组应当保持小型，并且处于相同的物理链路本地网络上。
- 建议使用专用 iDRAC 网络端口，以提高安全性。此外，支持共享 LOM。

附加网络信息

由网络拓扑中的路由器分隔的两个 iDRAC 被视为单独的本地网络，并且不能加入同一个 iDRAC 本地组中。这意味着，如果 iDRAC 配置为专用 NIC 设置，则连接到服务器背面 iDRAC 专用端口的网络电缆必须位于所有相关服务器的本地网络下。

如果 iDRAC 配置为共享 LOM 网络设置配置，则需要在本地网络下连接服务器主机和 IDRAC 所使用的共享网络连接，以供 Group Manager 检测并将这些服务器集成到一个通用组中。如果 IDRAC 配置有专用和共享 LOM 模式，则如果所有网络连接都不通过路由器传递，则 NIC 设置也可以集成到通用组。

VLAN 环境中的 MLD 侦听对组管理器发现的影响

由于组管理器对节点启动的发现使用 IPv6 多播寻址，名为 MLD 侦听的功能可防止支持组管理器的设备在未正确配置的情况下发现彼此。MLD 侦听是一项通用的以太网交换机功能，旨在减少网络上不必要的 IPv6 多播流量。

如果 MLD 侦听在任何网络中处于活动状态，请确保启用 MLD 查询器，以使以太网交换机与网络上的活动组管理器设备保持同步。或者，如果不需要 MLD 侦听功能，可以将其禁用。请注意，某些网络交换机默认启用 MLD 侦听。对于 MX7000 机箱中的模块切换也是如此。

注:

例如

- 在 MX5108n IOM 上禁用 VLAN 中的 MLD 侦听：

  MX5108N-B1# configure terminal

  MX5108N-B1(config)# interface vlan 194

  MX5108N-B1(conf-if-vl-194)#no ipv6 mld snooping

- 在 MX5108n IOM 上启用 VLAN 中的 MLD 查询器：

  MX5108N-B1# configure terminal

  MX5108N-B1(config)# interface vlan 194

  MX5108N-B1(conf-if-vl-194)#ipv6 mld snooping querier

管理登录

使用此部分可在组中 **Add New User（添加新用户）**、**Change User Password（更改用户密码）**和 **Delete User（删除用户）**。

组作业（包括管理登录）是服务器的一次性配置。Group Manager 使用 SCP 和作业进行任何更改。对于每个 Group Manager 作业，组中的每个 iDRAC 在其作业队列中各有一个作业。Group Manager 无法检测到成员 iDRAC 上的更改或锁定成员配置。

注: □作□无法配置或覆盖任何特定 iDRAC 的□定模式。

保留一个组不会更改本地用户或更改成员 iDRAC 上的设置。

添加新用户

使用此部分可在该组中的所有服务器上创建和添加新用户配置文件。需要创建组作业以将用户添加到该组中的所有服务器。可以在 **GroupManager** > **Jobs（作业）**页面找到组作业的状态。

注: 默□情况下，通□本地管理□□□配置 iDRAC。您可以通□本地管理□□□□□每个参数的更多信息。

有关详情，请参阅配置用户帐户和权限。

表. 36: 新用户选项

选项	说明
新用户信息	允许您提供新用户的信息详情。

表. 36: 新用户选项 （续）

选项	说明
iDRAC 权限	允许您定义用户角色以供将来使用。
高级用户设置	允许您设置 (IPMI) 用户权限，并帮助您启用 SNMP。

注: 属于同一□且已启用系□□定的任何成□ iDRAC 将返回一个用□密□未更新的□□。

更改用户密码

使用此部分可更改用户的密码信息。您可以查看 **Users（用户）**详细信息，其中包括各个用户的 **User Name（用户名）**、**Role（角色）**和 **Domain（域）**信息。需要创建组作业以更改该组中所有服务器的用户密码。可以在 **GroupManager** > **Jobs（作业）**页面找到组作业的状态。

如果用户已存在，则可更新密码。属于该组且已启用系统锁定的任何成员 iDRAC 将返回一个用户密码未更新的错误。如果用户不存在，然后返回错误到 Group Manager，指出用户在系统中不存在。Group Manager GUI 中所示的用户列表基于充当主控制器的 iDRAC 上的当前用户列表。它不显示所有 iDRAC 的所有用户。

删除用户

使用此部分可从所有组服务器中删除用户。需要创建组作业以从所有组服务器中删除用户。可以在 **GroupManager** > **Jobs（作业）**页面找到组作业的状态。

如果成员 iDRAC 上已存在用户，则用户可以被删除。属于该组且已启用系统锁定的任何成员 iDRAC 将返回一个用户未删除的错误。如果用户不存在，则会针对该 iDRAC 显示已成功删除。Group Manager GUI 中所示的用户列表基于充当主控制器的 iDRAC 上的当前用户列表。它不显示所有 iDRAC 的所有用户。

配置警报

使用此部分可配置电子邮件警报。默认情况下，警报已禁用。但是，您可以随时启用警报。组作业将创建，以将电子邮件警报配置应用到所有组服务器。组作业的状态可在 **GroupManager** > **Jobs（作业）**页面进行监测。Group Manager 电子邮件警报可配置所有成员上的电子邮件警报。它会设置同一组中所有成员的 SMTP 服务器设置。每个 iDRAC 单独配置。电子邮件配置不会全局保存。当前值基于充当主控制器的 iDRAC。保留一个组不会重新配置电子邮件警报。

有关配置警报的更多信息，请参阅配置 iDRAC 以发送警报。

表. 37: 配置警报选项

选项	说明
SMTP（电子邮件）服务器地址设置	允许您配置服务器 IP 地址、SMTP 端口号并启用身份验证。在您启用身份验证的情况下，您需要提供用户名和密码。
电子邮件地址	允许您配置多个电子邮件 ID 以接收关于系统状态更改的电子邮件通知。您可以从系统向所配置的帐户发送一封测试电子邮件。
警报类别	允许您选择多个警报类别以接收电子邮件通知。

注: 属于同一组且已启用系统锁定的任何成员 iDRAC 将返回一个用户密码未更新的错误。

导出

使用此部分可将组摘要导出到本地系统。可以导出 CSV 文件格式的信息。它包含与组中的每个单独的系统相关的数据。导出包括以下以 CSV 格式的信息。服务器详细信息：

- 运行状况
- 主机名
- iDRAC IPV4 地址

- iDRAC IPV6 地址
- 资产标签
- 型号
- iDRAC 固件版本
- 上次状态更新
- 快速服务代码
- iDRAC 连接性
- 电源状态
- 操作系统
- 服务标签
- 节点 ID
- iDRAC DNS 名称
- BIOS 版本
- CPU 详细信息
- 系统内存 (MB)
- 位置详细信息

注: 如果您使用的是 Internet Explore，请禁用增强的安全性设置以成功下载 CSV 文件。

查找到的服务器视图

创建本地组后，iDRAC 组管理器会通知本地网络上的所有其他 iDRAC，指出已创建一个新组。对于在查找到的服务器下显示的 iDRAC，应在每个 iDRAC 中启用组管理器功能。查找到的服务器视图显示在同一网络上检测到的 iDRAC 列表，它们可以是任何组的一部分。如果 iDRAC 没有出现在查找到的系统列表中，则用户必须登录到特定的 iDRAC 并加入组。创建组的 iDRAC 将显示为基础视图中的唯一成员，直到更多的 iDRAC 加入组。

注: 组管理器控制台上查找到的服务器视图允许您将视图中列出的一个或多个服务器加入到该组。可以从 **GroupManager** > **Jobs（作业）**跟踪活动的进度。或者您可以登录到 iDRAC 并从下拉列表中选择您想要将其加入该组的组。从 iDRAC 索引页面中，您可以访问 GroupManager 欢迎屏幕。

表. 38: 组板载选项

选项	说明
加入和更改登录	选择一个特定行，然后选择“Onboard and Change Login”（加入并更改登录）选项，将新查找到的系统加入到组中。您必须为新的系统提供管理员登录凭据以加入组。如果系统具有默认密码，您需要在将其加入到组时进行更改。 组加入允许您将相同的组警报设置应用到新系统。
忽略	如果您不想将系统添加到任何组中，您可从查找到的服务器列表中忽略它。
取消忽略	允许您选择您想要在查找到的服务器列表中恢复的系统。
重新扫描	允许您扫描并随时生成查找到的服务器列表。

作业视图

作业视图使用户可以跟踪组作业的进度，有助于使用简单恢复步骤来更正连接导致的故障。它还显示作为审核日志执行的最近一次组操作的历史记录。用户可以使用作业视图来跟踪整个组的操作进度或取消计划在未来执行的操作。作业视图让用户可以查看已运行的最近 50 个作业的状态以及发生的任何成功或失败。

表. 39: 作业视图

选项	说明
状态	显示作业的状态和正在进行中的作业的状态。
作业	显示作业的名称。

表. 39: 作业视图 （续）

选项	说明
ID	显示作业的 ID。
开始时间	显示开始时间。
结束时间	显示结束时间。
操作	• 取消 — 在移到运行状态之前，可以取消计划的作业。可以通过使用停止按钮停止正在运行的作业。 • 重新运行 — 在作业失败的情况下，允许用户重新运行作业。 • 移除 — 允许用户移除已完成的旧作业。
导出	您可以将组作业信息导出到本地系统以备将来参考。作业列表可以导出为 CSV 文件格式。其中包含与单独的作业相关的数据。

注: 对于每个作业条目，系统列表中可提供最多 100 个系统的详细信息。每个系统条目包含主机名、服务标签、成员作业状态和消息（如果作业失败）。

在所有组成员上执行创建作业的所有组操作并且立即生效。可以执行以下任务：

- 添加/编辑/删除用户
- 配置电子邮件警报
- 更改组密码和名称

注: 只要所有成员均处于联机状态且可访问，组作业就会快速完成。从作业开始到完成可能需要 10 分钟。对于不可访问的系统，作业将等待并重试长达 10 个小时。

注: 机载作业正在运行时，无法计划其他作业。作业包括：

- 添加新用户
- 更改用户密码
- 删除用户
- 配置警报
- 机载附加系统
- 更改组密码
- 更改组名称

如果在机载任务处于活动状态时调用其他作业，则会显示 GMGR0039 错误代码。一旦机载任务第一次尝试加入所有新系统，将可以在任意时间点创建作业。

作业导出

您可以将日志导出到本地系统作为进一步的参考。作业列表可以导出为 CSV 文件格式。其中包含与每个作业相关的所有数据。

注: 导出的 csv 文件仅可提供英文版。

Group Information（组信息）面板

组管理器摘要视图右上角中的“Group Information”（组信息）面板显示了一个整合的组摘要。通过单击“Group Settings”（组设置）按钮可以访问“Group Settings”（组设置）页面，并从该页面中编辑当前的组配置。它会显示组中有多少个系统。它还提供了组的主要和次要控制器的相关信息。

组设置

“Group settings”（组设置）页面提供所选组的属性列表。

表. 40: 组设置属性

组属性	说明
组名称	显示该组的名称。
系统数量	显示该组中的系统总数。
创建时间	显示时间戳的详细信息。
创建者	显示组管理员的详细信息。
控制系统	显示用作控制系统的系统服务标签并协调组管理任务。
备份系统	显示用作备份系统的系统服务标签。如果控制系统不可用，则取代控制系统的角色。

允许用户执行组下表中列出的操作。系统将为这些操作创建组配置作业（更改组名称、更改组密码、删除成员以及删除组）。可以从 **GroupManager** > **Jobs（作业）**页面查看或修改组作业的状态。

表. 41: 组设置操作

操作	说明
更改名称	允许您将 **Current Group Name（当前组名称）**更改为 **New Group Name（新组名称）**。
更改密码	允许您通过输入 **New Group Passcode（新组密码）**更改现有组密码，并通过 **Reenter New Group Passcode**（重新输入新组密码）验证该密码。
移除系统	允许您一次从组中移除多个系统。
删除组	允许您删除组。要使用组管理器的任何功能，用户应具有管理员权限。删除组后，任何待处理作业都将被停止。

在所选服务器上的操作

在“Summary”（摘要）页面上，您可以双击某行以通过单一登录重定向启动该服务器的 iDRAC。请确保在浏览器设置中关闭弹出窗口阻止程序。您可以从 **More Actions（更多操作）**下拉列表中单击适当的项目，以在选定的服务器上执行以下操作。

表. 42: 选定服务器上的操作

选项	说明
正常关机	关闭操作系统并断开系统电源。
冷引导	关闭电源，然后重新引导系统。
虚拟控制台	通过在新的浏览器窗口上的单一登录启动虚拟控制台。 **注:** 从浏览器禁用弹出窗口阻止程序以使用此功能。

Group Manager 单一登录

该组中的所有 iDRAC 基于共享的密码和共享组名称相互信任。因此，通过 Group Manager Web 界面单一登录访问时，组成员 IDRAC 中的管理员用户在任何组成员 IDRAC 中将获得管理员级别权限。iDRACs 将 <user>-<SVCTAG> 记录为登录到对等成员的用户。<SVCTAG> 是用户第一次登录的 iDRAC 的服务标签。

Group Manager 的概念 — 控制系统

- 自动选中 — 默认情况下，第一个 iDRAC 配置为 Group Manager。
- 提供了 Group Manager GUI 工作流程。
- 保持跟踪所有成员。
- 协调任务。

- 如果用户登录到任何成员并单击“Open Group Manager”（打开 Group Manager），则浏览器将重定向至主控制器。

Group Manager 的概念 — 备份系统

- 主控制器自动选择次要控制器，以便在主控制器在较长一段时间内（超过 10 分钟）处于离线状态时接管。
- 如果主要和次要控制器都在较长一段时间内（超过 14 分钟）处于离线状态，则会选出新的主要和次要控制器。
- 将保留所有组成员和任务的 Group Manager 高速缓存的副本。
- 控制系统和备份系统由 Group Manager 自动确定。
- 无需用户配置或干预。

iDRAC 组固件更新

对于 iDRAC 组固件更新，请从本地目录中的 DUP 文件执行以下步骤：

1. 访问组管理器控制台基本视图，然后单击摘要视图下的**更新 iDRAC 固件**。
2. 在显示的固件更新对话框中，浏览并选择要安装的本地 iDRAC DUP 文件。单击**上载**。
3. 文件将上传到 iDRAC 并验证完整性。
4. 确认固件更新。组 iDRAC 固件更新作业计划为立即执行。如果组管理器有其他组作业正在运行，则会在上一个作业完成后执行。
5. 您可以从组作业视图跟踪 iDRAC 更新作业执行。

注: □ iDRAC 3.50.50.50 及更高版本支持此功能。

13

管理日志

iDRAC 提供生命周期日志，其中包含与系统、存储设备、网络设备、固件更新、配置更改、许可证消息等相关的事件。不过，系统事件还可通过称为系统事件日志 (SEL) 的单独日志提供。您可以通过 iDRAC Web 界面、RACADM 和 WSMAN 界面访问生命周期日志。

生命周期日志的大小达到 800 KB 时，日志将压缩和存档。您只能查看未存档的日志条目，然后应用筛选器并备注未存档的日志。要查看存档的日志，您必须将整个生命周期日志导出到系统上的一个位置。

主□：

查看系统事件日志

当受管系统上发生系统事件时，此事件将记录在系统事件日志 (SEL) 中。LC 日志中也提供了相同的 SEL 条目。

注： 当 iDRAC 正在重新启□□，SEL 和 LC 日志在□□戳中可能不匹配。

使用 Web 界面查看系统事件日志

要在 iDRAC Web 界面中查看 SEL，请转至 **Maintenance（维护）** > **System Event Log（系统事件日志）**。

System Event Log（系统事件日志）页面显示系统运行状况指示灯、时间戳和每个记录事件的说明。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

单击 **Save As**（另存为）将 **SEL** 保存到您所选的位置。

注： 如果您使用的是 Internet Explorer，并且如果在保存时出现问题，请下载 Internet Explorer 的累积安全更新。您可以从以下 Microsoft 支持网址下载：**support.microsoft.com**。

要清除日志，单击 **Clear Log**（清除日志）。

注： 只有在具备**清除日志**权限时，“清除日志”才会显示。

清除 SEL 条目后，在 Lifecycle Controller 日志中将记录一个条目。日志条目包括已清除 SEL 的用户名和 IP 地址。

使用 RACADM 查看系统事件日志

查看 SEL：

```
racadm getsel <options>
```

如果没有指定参数，将显示整个日志。

要显示 SEL 条目数：`racadm getsel -i`

要清除 SEL 条目：`racadm clrsel`

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序查看系统事件日志

您可以使用 iDRAC 设置公用程序查看系统事件日志 (SEL) 中记录的总数并清除日志。要执行此操作：

1. 在 iDRAC 设置公用程序中，转至**系统事件日志。**
   iDRAC Settings.System Event Log（iDRAC 设置系统事件日志）显示 **Total Number of Records**（记录的总数）。
2. 要清除记录，请选择 **Yes**（是）。否则，请选择 **No（否）**。
3. 要查看系统事件，请单击 **Display System Event Log**（显示系统事件日志）。
4. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。

查看 Lifecycle 日志

Lifecycle Controller 日志提供有关受管系统上所安装组件的更改历史记录。您还可以在每个日志条目中添加工作注释。

以下事件和活动均已记录：

- 全部
- 系统运行状况 — 表示系统机箱内与硬件相关的所有警报的系统运行状况类别。
- 存储 — 存储运行状况类别代表与存储子系统相关的警报。
- 更新 — 更新类别表示由于固件/驱动程序升级/降级生成的警报。
- 审核 — 表示审核日志的审核类别。
- 配置 — 表示与硬件、固件和软件配置更改相关的警报配置类别。
- 工作注释

当您使用以下任一界面登录或注销 iDRAC 时，将在 Lifecycle 日志中记录登录、注销或登录失败事件：

- SSH
- Web 界面
- RACADM
- Redfish
- LAN 上 IPMI
- 串行
- 虚拟控制台
- 虚拟介质

您可以根据类别和严重性级别查看和筛选日志。您还可以在日志条目中添加和导出工作注释。

注: 特性模式的 Lifecycle 日志更改□在主机的□引□期□生成。

如果您使用 RACADM CLI 或 iDRAC Web 界面启动配置作业，Lifecycle 日志将包含有关用户、使用的界面以及启动作业的系统的 IP 地址的信息。

注: 在 MX 平台上，Lifecycle Controller 会□□使用 OME - Modular □建的配置或安装作□□□多个作□ ID。有关已□行作□的更多信息，□参□ OME - Modular 日志。

使用 Web 界面查看 Lifecycle 日志

要查看生命周期日志，单击 **Maintenance（维护）** > **Lifecycle Log（生命周期日志）**。此时将显示 **Lifecycle Log（生命周期日志）**页面。有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

筛选 Lifecycle 日志

您可以根据类别、严重性、关键字或日期范围筛选日志。

筛选 Lifecycle 日志：

1. 在 **Lifecycle Log**（Lifecycle 日志）页面的 **Log Filter**（日志筛选）区域中，执行以下任意或所有操作：
   - 从下拉式列表中选择 **Log Type**（日志类型）。
   - 从 **Severity**（严重性）下拉列表中选择严重性级别。
   - 输入一个关键字。

- 指定日期范围。

2. 单击**应用**。
   筛选的日志条目显示在**日志结果**中。

将备注添加到 Lifecycle 日志

将要备注添加到 Lifecycle 日志：

1. 在 **Lifecycle Log（Lifecycle 日志）**页面中，单击所需日志条目的 + 图标。
   随即会显示消息 ID 详细信息。
2. 在 **Comment（备注）**框中输入该日志条目的备注。
   备注会显示在 **Comment（备注）**框中。

使用 RACADM 查看 Lifecycle 日志

要查看 Lifecycle 日志，请使用 `lclog` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

导出 Lifecycle Controller 日志

您可以通过单个压缩的 XML 文件将整个 Lifecycle Controller 日志（活动和存档条目）导出到网络共享或本地系统。压缩的 XML 文件扩展名是 `.xml.gz`。文件条目根据顺序编号按顺序排列，从最低的顺序到最高的顺序排列。

使用 Web 界面导出 Lifecycle Controller 日志

要使用 Web 界面导出 Lifecycle Controller 日志，请执行以下操作：

1. 在 **Lifecycle Log**（Lifecycle 日志）页面中，单击 **Export**（导出）。
2. 选择以下选项之一：
   - **Network（网络）** — 将 Lifecycle Controller 日志导出到网络上的共享位置。
   - **Local（本地）** — 将 Lifecycle Controller 日志导出到本地系统上的位置。

   注: 在指定网络共享设置时，建议不要对用户名和密码使用特殊字符，也不要用百分号来编码特殊字符。

   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击 **Export**（导出）将日志导出到指定位置。

使用 RACADM 导出 Lifecycle Controller 日志

要导出 Lifecycle Controller 日志，使用 `lclog export` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

添加工作注释

登录到 iDRAC 的每个用户都可以添加工作注释，并且工作注释会作为事件存储在生命周期日志中。您必须拥有 iDRAC 日志权限才能添加工作注释。每个新工作注释最多支持 255 个字符。

注: 您不能删除工作注释。

要添加工作注释：

1. 在 iDRAC Web 界面中，转至 **Dashboard（仪表板）** > **Notes（注释）** > **add note（添加注释）**。
   此时将显示 **Work Notes（工作注释）**页面。
2. 在 **Work Notes（工作注释）**下，在空白文本框中输入文本。

注: 建议不要使用太多的特殊字符。

3. 单击 **Save（保存）**。
   工作注释便添加到日志中。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

配置远程系统日志记录

您可以将生命周期日志发送到远程系统。在开始之前，请确保：

- iDRAC 和远程系统之间有网络连接。
- 远程系统和 iDRAC 位于同一网络。

使用 Web 界面配置远程系统日志记录

要配置远程系统日志服务器设置：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Remote Syslog Settings（远程系统日志设置）**。
   随即会显示 **Remote Syslog Settings（远程系统日志设置）**屏幕。
2. 启用远程系统日志、指定的服务器地址和端口号。有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。
   将保存设置。写入生命周期日志的所有日志还会同时写入配置的远程服务器。

使用 RACADM 配置远程系统日志记录

要配置远程系统日志记录设置，使用 `set` 命令和 `iDRAC.SysLog` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

14

在 iDRAC 中监测和管理电源

您可以使用 iDRAC 监测和管理受管系统的电源需求。通过适当分布和调整系统的能耗，可以防止系统发生断电。

主要功能有：

- **电源监控** — 查看受管系统的电源状态、电源计量历史记录和当前平均值、峰值等。
- **功率封顶** — 查看和设置受管系统的功率限值，包括显示最小和最大潜在能耗。此功能需要许可证。这是一项授权的功能。
- **电源控制** — 让您可以远程执行受管系统上的电源控制操作（例如开机、关机、系统重置、关机后再开机和正常关机）。
- **电源选项** — 配置电源选项，例如冗余策略、热备用和功率系数修正。

主□：

监测功率

iDRAC 会持续监测系统中的功耗并显示下列功率值：

- 功耗警告和临界阈值。
- 累计功率、峰值功率以及峰值电流。
- 前一个小时、前一天或上一周内的功率消耗。
- 平均、最小和最大功耗。
- 历史峰值和峰值时间戳。
- 峰值余量和瞬时余量值（针对机架式和塔式服务器）。

注： 系□功耗□□（每小□、每天、每周）的直方□□在 iDRAC 运行□被予以保留。如果 iDRAC 重启，□□有的功耗数据将会□失而直方□也将重新开始。

注： iDRAC 固件更新或重置之后，功耗□形将被擦除/重置。

使用 Web 界面监测 CPU、内存和输入输出模块的性能指标

要在 iDRAC Web 界面中监测 CPU、内存和 I/O 模块的性能指标，请转至 **System（系统）** > **Performance（性能）**。

- **系统性能**部分 - 在图形视图中显示 CPU、内存和 I/O 利用率指标和系统级 CUPS 指标的当前读数及警告读数。
- **系统性能历史数据**部分：
  - 提供 CPU、内存、IO 利用率以及系统级 CUPS 指数的统计数据。如果主机系统已关闭，则图表将显示低于 0% 的关机线。
  - 您可以重设特定传感器的峰值利用率。单击 **Reset Historical Peak（重设历史峰值）**。您必须具有"配置"权限才能重设峰值。
- **性能指标**部分：
  - 显示状态和当前读数
  - 显示或指定警告性利用率阈值限制。您必须具有服务器配置权限才能设置此阈值。

有关所显示的属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 监测 CPU、内存和输入输出模块的性能指标

使用 **SystemPerfStatistics** 子命令监测 CPU、内存和 I/O 模块的性能指标。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

设置功耗的警告阈值

您可为机架式和塔式系统中的功耗传感器设置警告阈值。机架式和塔式系统的警告/严重功率阈值可能会随系统电源重启而变化，这取决于 PSU 容量和冗余策略。但是，即使冗余策略的电源设备容量发生更改，警告阈值也不能超出严重阈值。

刀片系统的功率警告阈值设置为 CMC（对于非 MX 平台）或 OME 模块化（对于 MX 平台）的功率分配。

如果重设为默认设置，则功率阈值将设置为默认值。

您必须具有"配置用户"权限才能设置功耗传感器的警告阈值。

注: □行 racreset 或 iDRAC 更新后，警告□□的□重□□默□□。

使用 Web 界面设置功耗警告阈值

1. 在 iDRAC Web 界面中，转至 **System（系统）** > **Overview（概览）** > **Present Power Reading and Thresholds（当前的功率读数和阈值）**。
2. 在 **Present Power Reading and Thresholds（当前的功率读数和阈值）**部分，单击 **Edit Warning Threshold（编辑警告阈值）**。
   此时会显示 **Edit Warning Threshold（编辑警告阈值）**页面。
3. 在 **Warning Threshold（警告阈值）** 列中，以**瓦特**或 **BTU/小时**为单位输入值。
   该值必须低于**故障阈值**。这些值舍入到最接近能被 14 整除的值。如果您输入**瓦特**，系统将自动计算并显示 **BTU/小时**的值。与此类似，如果您输入的是 BTU/小时，则显示**瓦特**的值。
4. 单击 **Save（保存）**。值已配置。

执行电源控制操作

使用 Web 界面或 RACADM，您可以对 iDRAC 远程执行开机、关机、重设、正常关机、非屏蔽中断 (NMI) 或关机后再开机。

您也可以使用 Lifecycle Controller Remote Services 或 WSMan 执行这些操作。有关更多信息，请参阅 https://www.dell.com/support.上提供的 *生命周期控制器远程服务快速入门指南，网址：* https://www.dell.com/idracmanuals 和 *Dell Power State Management Profile*（Dell 电源状态管理配置文件）说明文件。

从 iDRAC 启动的服务器电源控制操作独立于在 BIOS 中配置的电源按钮行为。您可以使用按钮功能来正常关闭或打开系统，即使 BIOS 配置为按下实际电源按钮时不采取任何措施也不例外。

使用 Web 界面执行电源控制操作

要执行功率控制操作：

1. 在 iDRAC Web 界面中，转至**配置** > **电源管理** > **电源控制**。此时将显示**电源控制**选项。
2. 选择所需电源操作：
   - 打开系统电源
   - 关闭系统电源
   - NMI（非屏蔽中断）
   - 正常关机
   - 重设系统（热引导）
   - 关闭系统电源后重启（冷引导）
3. 单击**应用**。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 执行电源控制操作

要执行电源操作，请使用 **serveraction** 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

功率限额

您可以查看功率阈值限制，这包括当数据中心存在高负载系统时的交流和直流功率消耗。这是一项授权的功能。

刀片服务器中的功率上限

在打开刀片式服务器之前，根据有限的硬件资源清册，iDRAC 会将刀片服务器的电源要求提供给机箱管理器。如果功耗随着时间增加，并且服务器消耗的功率接近分配的最大功率，iDRAC 可能会请求 CMC（用于非 MX 平台）或 OME（用于 MX 平台）增加最大可能功耗，从而增大功率范围。这仅增加电源传输请求。如果功耗减少，它不会请求电源传输。

系统启动并初始化后，iDRAC 会根据实际的硬件配置计算新的电源要求。即使 CMC（不用于 MX 平台）或 OME Modular（不用于 MX 平台）无法分配新的电源请求，系统也会保持开机状态。

CMC 或 OME Modular 从低优先级服务器回收任何未用功率，并将其分配给较高优先级的基础架构模块或服务器。

查看和配置功率上限策略

当启用功率上限策略时，将对系统强制执行用户定义的功率限制。如果未启用功率上限，则使用默认的硬件电源保护策略。此电源保护策略独立于用户定义策略。系统性能将动态调整以便将功耗维持在指定阈值。

实际功耗取决于工作负载。在性能调整完成之前，实际功耗可能会暂时超过阈值。例如，设想一个最小和最大潜在功耗值分别为 500 W 和 700 W 的系统。您可以指定功率预算阈值以降低功耗至 525 W。配置此功耗预算后，系统性能会动态调整以保持 525 W 或更低的功耗。

如果您设置的功率上限非常低或者环境温度非常高，则在启用或重置系统时，功耗可能暂时超过功率上限。

如果设置的功率上限值低于推荐的最小阈值，iDRAC 可能无法保持请求的功率上限值。

您可以用瓦特、BTU/hr 或以推荐功率上限的百分比来指定该值。

以 BTU/hr 为单位设置功率上限阈值时，转换的以瓦特为单位的值会四舍五入为最接近的整数。从系统读取功率上限阈值时，从瓦特转换为 BTU/hr 值也将被舍入。由于舍入方法，实际值可能略有不同。

使用 Web 界面配置功率上限策略

要查看和配置电源策略，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **电源管理** > **功率上限策略**。
   当前电源策略限制会显示在**功率上限限制**部分。
2. 选择**功率上限**下的**启用**。
3. 在**功率上限**部分，以瓦特和 BTU/hr 或以推荐系统限制的上限百分比输入功率上限。
4. 单击**应用**以应用该值。

使用 RACADM 配置功率限额策略

要查看和配置当前功率上限值，将以下对象配合 `set` 命令使用。

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置功率上限策略

要查看和配置电源策略，请执行以下操作：

1. 在 iDRAC 设置公用程序中，转至 **Power Configuration**（电源配置）。

   注: 仅当服务器电源设备支持电源监测时，**Power Configuration**（电源配置）链接才可用。

   此时将显示 **iDRAC Settings Power Configuration**（iDRAC 设置电源配置）页面。
2. 选择**启用**以启用**功率上限策略**。否则，选择**禁用**。
3. 使用所建议的设置，或在**用户定义的功率上限策略**下输入所需的限制。
   有关选项的更多信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
4. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   电源限额值已配置。

配置电源设备选项

您可以配置电源设备选项，如冗余策略、热备用和功率因数校正。

热备盘是电源设备功能，可配置冗余电源装置 (PSU) 根据服务器负荷关闭。这样，其余 PSU 就可以承担更高负荷并且更有效率。这要求支持此功能并在需要时能够迅速开机的 PSU。

在两个 PSU 系统中，PSU1 或 PSU2 都可以配置为主 PSU。

启用热备用后，PSU 可根据负荷情况变为活动状态或进入睡眠状态。如果启用了热备用，将在两个 PSU 之间启用非对称电流共享。一个 PSU 处于*唤醒*状态，并提供大部分电流；另一个 PSU 处于睡眠模式，并提供少量电流。这通常称为带有两个 PSU 的 1+0 模式，并已启用热备用。如果所有 PSU-1 位于电路 A 上，所有 PSU-2 位于电路 B 上，则在已启用热备用功能的情况下（默认的出厂热备用配置），电路 B 上的负荷将少很多，并会触发警告。如果禁用了热备用，则两个 PSU 之间将分别提供 50% 的电流共享，并且电路 A 和电路 B 通常具有相同的负荷。

功率因数是实际消耗功率与可视功率的比率。当启用功率因数校正时，服务器会在主机关闭时消耗少量的功率。默认情况下，功率因数更正会在服务器出厂时得到启用。

使用 Web 界面配置电源设备选项

要配置电源设备选项，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **Power Management（电源管理）** > **Power Configuration（电源配置）**。
2. 在 **Power Redundancy Policy（电源冗余策略）**下，选择所需的选项。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。电源设备选项已配置。

使用 RACADM 配置电源设备选项

要配置电源设备选项，请将以下对象配合 `get/set` 命令使用：

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置电源设备选项

要配置电源设备选项，请执行以下操作：

1. 在 iDRAC 设置公用程序中，转至 **Power Configuration**（电源配置）。

   注: 仅当服务器电源设备支持电源监测时，**Power Configuration**（电源配置）链接才可用。

将显示 **iDRAC Settings Power Configuration**（iDRAC 设置电源配置）页面。

2. 在**电源设备选项**下：
   - 启用或禁用 power supply redundancy（电源设备冗余）。
   - 启用或禁用 hot spare（热备用）。
   - 设置 primary power supply unit（主要电源设备）。
   - 启用或禁用功率因数校正。有关选项的更多信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   电源设备选项已配置。

启用或禁用电源按钮

要启用或禁用受管系统上的电源按钮：

1. 在 iDRAC 设置公用程序中，转至 **Front Panel Security**（前面板安全性）。
   此时将显示 **iDRAC Settings Front Panel Security**（iDRAC 设置前面板安全性）页面。
2. 选择 **Enabled**（已启用）以启用电源按钮或 **Disabled**（已禁用）以禁用该按钮。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   将保存设置。

多向量冷却

多向量冷却 可在 Dell EMC 服务器平台中采用多管齐下的热控制方法。您可以通过 iDRAC Web 界面配置多向量冷却选项，方法是导航到**配置** > **系统设置** > **硬件设置，** > **风扇配置**。它包括（但不限于）：

- 大量的传感器（散热、电源、资源清册），可以准确解释服务器内各个位置的实时系统散热状况。它仅根据配置显示一小部分与客户需求相关的传感器。
- 智能和自适应闭环控制算法可优化风扇响应以保持组件温度。它还可以降低风扇功耗、气流消耗和噪音。
- 通过使用风扇区域映射，将在组件需要时针对组件启动冷却。因此，这可产生最大性能而不会影响电源利用率的效率。
- 根据 LFM 指标（线性英尺/分钟 - 普遍接受的行业标准，它指定 PCIe 卡的空气流量要求），精确地表示逐个插槽的 PCIe 气流。在各种 iDRAC 界面中显示此指标使用户能够：
  1. 了解服务器内每个插槽的最大 LFM 能力。
  2. 了解每个插槽的 PCIe 冷却采用何种方法（气流控制、温度控制）。
  3. 如果卡是第三方卡（用户定义的自定义卡），了解要传送到插槽的最低 LFM。
  4. 设置第三方卡的自定义最小 LFM 值，以便更准确地定义与用户所知的自定义卡规格相符的卡冷却需求。
- 在各种 iDRAC 界面中向用户显示实时系统气流指标（CFM，立方英尺/分钟），从而允许基于单位服务器 CFM 消耗的聚合实现数据中心气流平衡。
- 允许自定义散热设置，如散热配置文件（最大性能与最大性能/瓦特，声音上限），自定义风扇速度选项（最小风扇速度，风扇速度偏移）以及自定义排气温度设置。
  1. 大多数这些设置都允许为散热算法生成的基准冷却提供额外的冷却，但不允许风扇速度低于系统冷却要求。
     注: 不过上面的陈述存在一个例外，那就是为第三方 PCIe 卡添加的风扇速度。散热算法为第三方卡提供气流可能比实际的卡冷却需求更多或更少，而且客户可通过输入与第三方卡对应的 LFM 微调对卡的响应。
  2. “自定义排气温度”选项可以将排气温度限制在客户所需的设置。
     注: 务必要注意，在某些配置和工作负载中，将排气减少到理想设定点以下可能实际并不可行（例如，若将自定义排气设置设定为 45℃，但却具有高进气温度 [例如 30℃] 以及加载配置[高系统功耗，低气流]，这种情况下就不可行）
  3. “声音上限”选项是第 14 代 PowerEdge 服务器的新增内容。它可限制 CPU 功耗并控制风扇速度和噪音上限。这是噪音部署特有的，并可能会降低系统性能。
- 系统布局和设计允许提高气流容量（通过允许高功率）和密集系统配置。还可提供更少的系统限制并提高功能密度。
  1. 简化的气流实现高效的气流与风扇功耗比率。
- 自定义风扇旨在获得更高的效率、更佳的性能、更长的寿命和更少的振动。它还可提供更好的噪音结果。
  1. 即使风扇始终保持全速运转，也能有很长的使用寿命（一般而言，它可以运转超过 5 年）。
- 自定义散热器旨在以最低（必需）但可支持高性能 CPU 的气流优化组件冷却效果。

15

iDRAC 直接更新

iDRAC 提供带外功能来更新 PowerEdge 服务器的各种组件的固件。iDRAC 直接更新有助于在更新期间消除暂存作业。

过去，iDRAC 使用暂存更新来启动组件的固件更新。从此版本开始，直接更新已应用于 PSU 和背板。使用直接更新和背板可以获得更快的更新。对于 PSU，可以避免一次重新启动（用于初始化更新），并且单次重新启动后就可以进行更新。

通过 iDRAC 中的直接更新功能，可以避免启动更新的第一次重新启动。第二次重新启动将由设备本身控制，如果需要通过作业状态进行单独的重设，iDRAC 将通知用户。

16

对网络设备执行资源清册、监测和配置操作

可对下列网络设备执行资源清册、监测和配置操作：

- 网络接口卡 (NIC)
- 聚合网络适配器 (CNA)
- 板载网卡 (LAN On Motherboards, LOM)
- 网络子卡 (NDC)
- 夹层卡（Mezzanine cards，仅适用于刀片式服务器）

禁用 NPAR 或 CNA 设备上的单独分区之前，确保清除所有 I/O 标识属性（例如：IP 地址、虚拟地址、启动器和存储目标）和分区级属性（例如：带宽和分配）。您可以将 VirtualizationMode 属性设置为 NPAR 或者禁用分区上的所有个性化设置，以禁用分区。

根据已安装的 CNA 设备类型，可能无法从上次处于活动状态的分区保留分区属性的设置。启用分区时，设置所有 I/O 标识属性和分区相关的属性。您可以将 VirtualizationMode 属性设置为 NPAR 或者启用分区上的所有个性化设置（例如：NicMode），以启用分区。

主□：

- □源清册和□□网□□□
- □源清册和□□ FC HBA □□
- □源清册和□□ SFP 收□器□□
- 遥□流式□□
- 串行数据捕□
- □□配置虚□地址、启□器和存□目□□置

资源清册和监测网络设备

您可以远程监测受管系统中的网络设备的运行状况并查看其资源清册。

对于每个设备，您可以查看端口和启用的分区的以下信息：

- 链路状态
- 属性
- 设置和功能
- Receive and Transmit Statistics（接收和传送统计数据）
- iSCSI、FCoE 启动器和目标信息

使用 Web 界面监测网络设备

要使用 Web 界面查看网络设备信息，请转至 **System（系统）** > **Overview（概览）** > **Network Devices（网络设备）**。将显示**网络设备**页面。有关显示的属性的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 监测网络设备

要查看有关网络设备的信息，请使用 `hwinventory` 和 `nicstatistics` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

除了 iDRAC Web 界面中显示的属性以外，使用 RACADM 或 WSMan 时还可能显示其他属性。

连接视图

对服务器的网络连接进行手动检查和故障排除在数据中心环境中不可管理。iDRAC9 将通过 iDRAC 连接视图简化此项作业。此功能可让您从用于部署、更新、监测和维护服务器的同一个集中式 GUI 中对网络连接进行远程检查和故障排除。iDRAC9 中的“连接视图”提供了交换机端口到服务器的网络端口的物理映射和 iDRAC (integrated Dell Remote Access Controller) 专用端口连接的详细信息。所有受支持的网络卡无论是什么品牌，在“连接视图”中都可见。

不是对服务器的网络连接进行手动检查和故障排除，而是可以远程查看和管理网络电缆连接。

连接视图提供连接到服务器端口和 iDRAC 专用端口的交换机端口信息。服务器网络端口包括那些在 PowerEdge LOM、NDC、夹层卡和 PCIe 附加卡的端口。

要查看网络设备连接视图，请导航至**系统** > **概览** > **网络设备** > **连接视图**以查看“连接视图”。

您也可以单击 **iDRAC 设置** > **连接** > **网络** > **常见设置** > **连接视图**以启用或禁用连接视图。

“连接视图”可通过 racadm `SwitchConnection View` 命令浏览，也可以通过命令查看。

字段或选项	说明
已启用	选择**已启用**可启用连接视图。默认情况下，选择**已启用**选项。
状态	如果您从 iDRAC 设置下的**连接视图**中启用连接视图选项，则将显示**已启用**。
交换机连接 ID	显示可供设备端口进行连接的交换机的 LLDP 机箱 ID。
交换机端口连接 ID	显示设备端口连接到的交换机端口的 LLDP 端口 ID。

注: 一旦连接视图启用并且链路已连接，则交换机连接 ID 和交换机端口连接 ID 可用。关联的网络卡需要与连接视图兼容。仅具有 iDRAC 配置权限的用户可以修改连接视图设置。

在 iDRAC9 4.00.00.00 和更高版本上，iDRAC 支持将标准 LLDP 数据包发送到外部交换机。这将提供用于在网络上查找 iDRAC 的选项。iDRAC 会将两种类型的 LLDP 数据包发送到出站网络：

- **拓扑 LLDP** - 在此功能中，LLDP 数据包将通过所有受支持的服务器 NIC 端口，以便外部交换机可以找到发起服务器、NDC 端口 [NIC FQDD]、IOM 在机箱中的位置、刀片式机箱服务标签等。在 iDRAC9 4.00.00.00 和更高版本中，拓扑 LLDP 可作为所有 PowerEdge 服务器的选项提供。LLDP 数据包包含服务器网络设备连接信息，并由 I/O 模块和外部交换机用于更新其配置。

  注:
  - 必须启用拓扑 LLDP，以使 MX 机箱配置正常工作。
  - 1GbE 控制器上不支持拓扑 LLDP，选择 10GbE 控制器（Intel X520、QLogic 578xx）。
- **查找 LLDP** - 在此功能中，LLDP 数据包仅通过使用中的活动 iDRAC NIC 端口（专用 NIC 或共享 LOM），因此，相邻的交换机可以在该交换机中找到 iDRAC 连接端口。查找 LLDP 仅特定于活动 iDRAC 网络端口，不会在服务器中的所有网络端口上可见。查找 LLDP 将具有 iDRAC 的一些详细信息（比如 IP 地址、MAC 地址、服务标签等），以便交换机可以自动发现与其相连的 iDRAC 设备以及 iDRAC 的某些数据。

  注: 如果在端口/分区上清除了虚拟 MAC 地址，则虚拟 MAC 地址将与 MAC 地址相同。

要启用或禁用拓扑 LLDP，请导航至 **iDRAC 设置** > **连接性** > **网络** > **通用设置** > **拓扑 LLDP** 以启用或禁用拓扑 LLDP。默认情况下，为 MX 服务器启用此设置，并为所有其他服务器禁用此设置。

要启用或禁用 iDRAC 查找 LLDP，请导航至 **iDRAC 设置** > **连接性** > **网络** > **通用设置** > **iDRAC 查找 LLDP**。默认情况下，选择 Enabled（已启用）选项。

从 iDRAC 发起的 LLDP 数据包可使用以下命令从交换机进行查看：`show lldp neighbors`。

刷新连接视图

使用**刷新连接视图**获取交换机连接 ID 和交换机端口连接 ID 的最新信息。

注: 如果 iDRAC 具有服务器网络端口或 iDRAC 网络端口的交换机连接和交换机端口连接信息，并且由于某种原因，交换机连接和交换机端口连接信息已有 5 分钟未刷新，则交换机连接和交换机端口连接信息对于所有用户界面都显示为过时的数据（最后知道的正常数据）。在用户界面中，您看到黄色感叹号，它是自然形式显示，不表示任何警告。

连接视图可能的值

可能的连接视图数据	说明
功能被禁用	连接视图功能已被禁用，以查看连接视图数据启用功能。
无链接	表示与网络控制器端口关联的链接已关闭。
不可用	在交换机上未启用 LLDP。检查是否在交换机端口上启用了 LLDP。
不支持	网络控制器不支持连接视图功能。
过时的数据	最后知道的正常数据，为网络控制器端口链接已关闭或系统已关机。使用刷新选项刷新连接视图详细信息以获取最新的数据。
有效的数据	显示有效的交换机连接 ID 和交换机端口连接 ID 信息。

连接视图支持的网络控制器

以下卡或控制器支持连接视图功能。

制造商	类型
Broadcom	• 57414 rNDC 25GE • 57416/5720 rNDC 10GbE • 57412/5720 rNDC 10GbE • 57414 PCIe FH/LP 25GE • 57412 PCIe FH/LP 10GbE • 57416 PCIe FH/LP 10GbE
Intel	• X710 bNDC 10Gb • X710 DP PCIe 10Gb • X710 QP PCIe 10Gb • X710 + I350 rNDC 10Gb+1Gb • X710 rNDC 10Gb • X710 bNDC 10Gb • XL710 PCIe 40Gb • XL710 OCP 夹层卡 10Gb • X710 PCIe 10Gb
Mellanox	• MT27710 rNDC 40Gb • MT27710 PCIe 40Gb • MT27700 PCIe 100Gb
QLogic	• QL41162 PCIe 10GE 2P • QL41112 PCIe 10GE 2P • QL41262 PCIe 25GE 2P

资源清册和监测 FC HBA 设备

您可以远程监测受管系统中光纤通道总线适配器 (FC HBA) 设备的运行状况并查看其资源清册。支持 Emulex 和 QLogic FC HBA。对于每个 FC HBA 设备，您可以查看端口的以下信息：

- 链接状态和信息
- 端口属性
- Receive and Transmit Statistics（接收和传送统计数据）

注： Emulex FC8 HBA 不受支持。

使用 Web 界面监测 FC HBA 设备

要使用 Web 界面查看 FC HBA 设备信息,请转至 **System（系统）** > **Overview（概览）** > **Network Devices（网络设备）** > **Fibre Channel（光纤信道）**。有关显示的属性的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

此页面还显示插槽编号（FC HBA 可用时）和 FC HBA 设备的类型。

使用 RACADM 监测 FC HBA 设备

要使用 RACADM 查看 FC HBA 设备信息，请使用 `hwinventory` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

资源清册和监测 SFP 收发器设备

您可以远程监测连接到系统的 SFP 收发器设备的运行状况并查看其资源清册。以下是受支持的收发器：

- SFP
- SFP+
- SFP28
- SFP-DD
- QSFP
- QSFP+
- QSFP28
- QSFP-DD
- Base-T 模块
- AOC 和 DAC 电缆
- 使用以太网连接的 RJ-45 Base-T
- 光纤信道
- IB 适配器端口

最有用的收发器信息为收发器 EPROM 中的序列号和部件号。这将允许在对连接问题进行故障排除时验证远程安装的收发器。对于每个 SFP 收发器设备，您可以查看端口的以下信息：

- 供应商名称
- 部件号
- 修订版
- 序列号
- 设备标识符/类型信息
- 缆线长度（以米为单位）

使用 Web 界面监测 SFP 收发器设备

要使用 Web 界面查看 SFP 收发器设备信息，请转至**系统** > **概览** > **网络设备**，然后单击特定设备。有关所示属性的更多信息，请参阅 *iDRAC 联机帮助*。

页面名称还在端口统计信息下显示收发器设备可用的插槽编号。

使用 RACADM 监测 SFP 收发器设备

要使用 RACADM 查看 SFP 收发器设备信息，请使用 `hwinventory` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

遥测流式传输

通过遥测，用户可以从 PowerEdge 服务器收集实时设备指标、事件和数据日志并将其流式传输到外部的订阅客户端或服务器应用程序。使用遥测，您可以设置需要生成的报告类型和频率。

注: 此功能在所有平台上均受支持，且需要 iDRAC Datacenter □可□。

遥测是“一对多”解决方案，用于从一个或多个 PowerEdge 服务器 (iDRAC) 收集实时系统数据并将其流式传输到集中式“远程服务器监测、分析和警报服务”。此功能还支持按需收集数据。

遥测数据包括指标/库存和日志/事件。数据可以从 iDRAC 流式传输（拉出）或收集至远程消费者（如 Redfish 客户端和远程系统日志服务器）或由其从 iDRAC 流式传输或收集。还可以按需向 iDRAC SupportAssist Data Collector 提供遥测数据。数据收集和报告以预定义的 Redfish 遥测指标、触发器和报告定义为基础。可以通过 RACADM、Redfish 和服务器配置配置文件 (SCP) 配置遥测流式传输设置。

要配置遥测，请启用或选择定义数据流式传输行为和频率所需的设备报告或日志。请转至**配置** > **系统设置**页面以配置遥测。在禁用遥测之前，会自动进行数据流式传输。

下表描述了可以使用遥测生成的指标报告：

类型	指标组	资源清册	传感器	统计数据	配置	指标
I/O 设备	NIC	否	是	是	否	否
	FC HBA	否	是	是	否	否
服务器设备	CPU	否	是	否	否	是
	内存	否	是	否	否	是
	风扇	否	是	否	否	否
	PSU	否	否	否	否	是
	传感器	否	是	否	否	否
环境参数	散热	否	是	否	否	是
	功率	否	否	是	否	是
	性能	否	否	是	否	否
加速器	GPU	否	否	是	否	是

要了解有关遥测部分的字段说明，请参阅 *iDRAC 联机帮助*。

注:

- StorageDiskSMARTDATA 仅在具有 SAS/SATA 总线协议和 BOSS 控制器后的 SSD 驱动器上受支持。
- 仅针对处于就绪/联机/非 RAID 模式下且不在 BOSS 控制器后的驱动器报告 StorageSensor 数据。
- NVMeSMARTData 仅受具有 PCIe 总线协议（不是在 SWRAID 后面）的 SSD (PCIeSSD / NVMe Express) 驱动器支持。
- GPGPUStatistics 数据仅在支持 ECC 内存功能的特定 GPGPU 型号中可用。
- PSUMetrics 在模块化平台上不可用。
- 某些平台的风扇功率和 PCIe 电源指标可能显示为 0。
- 在 4.40.00.00 版本中，CUPS 报告重命名为 SystemUsage，并且在 INTEL 和 AMD 平台上均受支持。

遥测工作流：

1. 安装 Datacenter 许可证（如果尚未安装）。
2. 配置全局遥测设置，包括使用 RACADM、Redfish、SCP 或 iDRAC GUI 启用遥测和 Rsyslog 服务器网络地址和端口。
3. 使用 RACADM 或 Redfish 界面在所需设备报告或日志上配置以下遥测报告流参数：
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

   注: 针对需要遥测报告的特定硬件启用 iDRAC 警报和 Redfish 事件。
4. Redfish 客户端会在 iDRAC 上发出 Redfish EventService 订阅请求。
5. 当满足预定义的触发条件时，iDRAC 会生成指标报告或日志/事件数据并将其推送到订阅的客户端。

功能限制：

1. 出于安全原因，iDRAC 仅支持与客户端进行基于 HTTPS 的通信。
2. 出于稳定性原因，iDRAC 最多支持八个订阅。
3. 仅通过 Redfish 界面删除受支持的订阅，甚至可以由管理员手动删除。

遥测功能的行为：

- 当满足预定义的触发条件时，iDRAC 会生成指标报告或日志/事件数据并将其推送 (HTTP POST) 到订阅中规定的目标订阅客户端。客户端仅在成功创建订阅时才会接收新数据。
- 从来源收集数据时，指标数据包含 ISO 格式的时间戳。
- 客户端可以通过 Redfish 界面将 HTTP DELETE 消息发送至订阅资源的 URI 来终止订阅。
- 如果 iDRAC 或客户端删除了订阅，则 iDRAC 不会发送 (HTTP POST) 报告。如果发送错误数超过了预定义的阈值，则 iDRAC 可能会删除订阅。
- 如果用户具有管理员权限，则只能通过 Redfish 界面删除订阅。
- iDRAC 可通过发送“订阅终止”事件作为最后一条消息来通知客户端有关订阅终止的信息。
- 订阅是永久的，即使在 iDRAC 重新启动后仍可保留。但是，可以通过执行 `racresetcfg` 或 LCwipe 操作将其删除。
- RACADM、Redfish、SCP 和 iDRAC 等用户界面显示客户端订阅的当前状态。

串行数据捕获

iDRAC 允许使用串行数据捕获功能捕获控制台重定向串行，以便稍后检索。此功能需要 iDRAC Datacenter 许可证。

串行数据捕获功能的目的是捕获系统序列数据并将其存储起来，以便客户稍后出于调试目的检索。

您可以使用 RACADM、Redfish、iDRAC 界面启用或禁用串行数据捕获。此属性启用时，iDRAC 将捕获在主机串行设备 2 上接收的串行流量，而不考虑串行 Mux 模式设置。

要使用 iDRAC GUI 启用/禁用串行数据捕获，请转至**维护** > **诊断** > **串行数据日志**页面，并选中复选框以启用或禁用。

注：

- 此属性在 iDRAC 重新引导后保持不变。
- 固件重设为默认值将禁用此功能。
- 启用串行数据捕获时，缓冲区将继续附加最近数据。如果用户禁用串行捕捉并再次启用，则 iDRAC 会从上次更新开始附加。

当用户从任何界面启用串行数据捕获标记时，系统串行数据捕获即开始。如果在系统启动后启用串行数据捕获，则必须重新启动系统，以便 BIOS 可以查看新设置（iDRAC 请求的控制台重定向已启用）以获取串行数据。iDRAC 将连续启动数据捕获，并存储到有 512 KB 字节限制的共享内存中。此缓冲区将循环。

注：

- 要使此功能正常工作，用户必须具有登录权限和系统控制权限。
- 此功能需要 iDARC Datacenter 许可证。

动态配置虚拟地址、启动器和存储目标设置

您可以动态地查看和配置虚拟地址、启动器和存储目标设置，并应用持久性策略。它允许应用程序基于电源状态更改应用设置（即，操作系统重新启动、热重设、冷重设或交流点重启），同时还可以基于该电源状态的持久性策略设置。这提供了更灵活的部署，满足将系统的工作负载快速重新配置到另一个系统的需求。

虚拟地址是：

- 虚拟 MAC 地址
- 虚拟 iSCSI MAC 地址
- 虚拟 FIP MAC 地址
- 虚拟 WWN
- 虚拟 WWPN

注： 在清除持久性策略后，所有虚□地址将重□□出厂□置的默□永久地址。

注： 在具有虚□ FIP、虚□ WWN 和虚□ WWPN MAC 属性的某些卡上，虚□ WWN 和虚□ WWPN MAC 属性会在您配置虚□ FIP □自□配置。

通过使用 IO 标识功能，您可以执行以下操作：

- 查看和配置网络和光纤信道设备（例如，NIC、CNA、FC HBA）的虚拟地址。
- 配置启动器（对应于 iSCSI 和 FCoE）和存储目标设置（对应于 iSCSI、FCoE 和 FC）。
- 指定在系统 AC 断电、系统冷/热重设时保留或清除已配置的值。

为虚拟地址、启动器和存储目标配置的值可能会随系统重设期间对主电源的处理方式发生更改，或者根据 NIC、CNA 或 FC HBA 设备是否具有辅助电源而发生更改。可根据通过 iDRAC 生成的策略设置来实现 I/O 标识设置的持久性。

仅当启用 I/O 标识功能时，持久性策略才会生效。每次系统重设或开机，这些值都根据策略设置保留或清除。

注: 将□清除后，在运行配置作□之前，您将无法重新□用□。

支持 I/O 标识优化功能的卡

下表提供了可支持 I/O 标识优化功能的卡。

表. 43: 支持 I/O 标识优化功能的卡

制造商	类型
Broadcom	• 5719 夹层卡 1GB • 5720 PCIe 1 GB • 5720 bNDC 1 GB • 5720 rNDC 1 GB • 57414 PCIe 25GbE
Intel	• i350 DP FH PCIe 1GB • i350 QP PCIe 1GB • i350 QP rNDC 1GB • i350 夹层卡 1GB • i350 bNDC 1GB • x520 PCIe 10GB • x520 bNDC 10GB • x520 夹层卡 10GB • x520 + i350 rNDC 10GB+1GB • X710 bNDC 10GB • X710 QP bNDC 10GB • X710 PCIe 10 GB • X710 + I350 rNDC 10GB+1GB • X710 rNDC 10GB • XL710 QSFP DP LP PCIe 40GE • XL710 QSFP DP FH PCIe 40GE • X550 DP BT PCIe 2 x 10 Gb • X550 DP BT LP PCIe 2 x 10 Gb • XXV710 Fab A/B 夹层卡 25 Gb（*用于 MX 平台*）
Mellanox	• ConnectX-3 Pro 10G 夹层卡 10GB • ConnectX-4 LX 25GE SFP DP rNDC 25GB • ConnectX-4 LX 25GE DP FH PCIe 25GB • ConnectX-4 LX 25GE DP LP PCIe 25GB • ConnectX-4 LX Fab A/B 夹层卡 25GB（*用于 MX 平台*）
Qlogic	• 57810 PCIe 10GB • 57810 bNDC 10GB • 57810 夹层卡 10GB • 57800 rNDC 10GB+1GB • 57840 rNDC 10GB • 57840 bNDC 10GB • QME2662 夹层卡 FC16 • QLE 2692 SP FC16 Gen 6 HBA FH PCIe FC16 • SP FC16 Gen 6 HBA LP PCIe FC16 • QLE 2690 DP FC16 Gen 6 HBA FH PCIe FC16 • DP FC16 Gen 6 HBA LP PCIe FC16 • QLE 2742 DP FC32 Gen 6 HBA FH PCIe FC32

表. 43: 支持 I/O 标识优化功能的卡 （续）

制造商	类型
	• DP FC32 Gen 6 HBA LP PCIe FC32 • QLE2740 PCIe FC32 • QME2692-DEL Fab C 夹层卡 FC16（*对于 MX 平台*） • QME2742-DEL Fab C 夹层卡 FC32（*对于 MX 平台*） • QL41262HMKR-DE Fab A/B 夹层卡 25 Gb（*对于 MX 平台*） • QL41232HMKR-DE Fab A/B 夹层卡 25 Gb（*对于 MX 平台*） • QLogic 1x32Gb QLE2770 FC HBA • QLogic 2x32Gb QLE2772 FC HBA
Emulex	• LPe15002B-M8 (FH) PCIe FC8 • LPe15002B-M8 (LP) PCIe FC8 • LPe15000B-M8 (FH) PCIe FC8 • LPe15000B-M8 (LP) PCIe FC8 • LPe31000-M6-SP PCIe FC16 • LPe31002-M6-D DP PCIe FC16 • LPe32000-M2-D SP PCIe FC32 • LPe32002-M2-D DP PCIe FC32 • LPe31002 -D Fab C 夹层卡 FC16（*对于 MX 平台*） • LPe32002 -D Fab C 夹层卡 FC32（*对于 MX 平台*） • LPe35002-M2 FC32 2 端口 • LPe35000-M2 FC32 1 端口

支持 I/O 标识优化功能的 NIC 固件版本

在第 14 代 Dell PowerEdge 服务器中，默认情况下已提供必需的 NIC 固件。

下表提供了支持 I/O 标识优化功能的 NIC 固件版本。

iDRAC 设置为远程分配地址模式或控制台模式时的虚拟地址/远程分配地址和持久性策略行为

下表描述虚拟地址管理 (VAM) 配置和持久性策略行为以及相关性。

表. 44: 虚拟/远程分配地址和持久政策行为

OME Modular 中的远程分配地址功能状态	iDRAC 中设置的模式	IO 标识在 iDRAC 中的功能状态	SCP	持久性策略	清除持久性策略 - 虚拟地址
已启用远程分配地址	远程分配地址模式	已启用	虚拟地址管理 (VAM) 已配置	配置的 VAM 仍然存在	设置为远程分配地址
已启用远程分配地址	远程分配地址模式	已启用	未配置 VAM	设置为远程分配地址	无持久性 - 设置为远程分配地址
已启用远程分配地址	远程分配地址模式	已禁用	使用 Lifecycle Controller 中提供的路径配置	设置为该周期的远程分配地址	无持久性 - 设置为远程分配地址
已启用远程分配地址	远程分配地址模式	已禁用	未配置 VAM	设置为远程分配地址	设置为远程分配地址
已禁用远程分配地址	远程分配地址模式	已启用	VAM 已配置	配置的 VAM 仍然存在	仅限持久性 - 不能清除
已禁用远程分配地址	远程分配地址模式	已启用	未配置 VAM	设置为硬件 MAC 地址	不支持持久性。取决于卡行为

表. 44: 虚拟/远程分配地址和持久政策行为 （续）

OME Modular 中的远程分配地址功能状态	iDRAC 中设置的模式	IO 标识在 iDRAC 中的功能状态	SCP	持久性策略	清除持久性策略 - 虚拟地址
已禁用远程分配地址	远程分配地址模式	已禁用	使用 Lifecycle Controller 中提供的路径配置	该周期的 Lifecycle Controller 配置仍然存在	不支持持久性。取决于卡行为
已禁用远程分配地址	远程分配地址模式	已禁用	未配置 VAM	设置为硬件 MAC 地址	设置为硬件 MAC 地址
已启用远程分配地址	游戏机模式	已启用	VAM 已配置	配置的 VAM 仍然存在	必须同时使用持久性和清除
已启用远程分配地址	游戏机模式	已启用	未配置 VAM	设置为硬件 MAC 地址	设置为硬件 MAC 地址
已启用远程分配地址	游戏机模式	已禁用	使用 Lifecycle Controller 中提供的路径配置	该周期的 Lifecycle Controller 配置仍然存在	不支持持久性。取决于卡行为
已禁用远程分配地址	游戏机模式	已启用	VAM 已配置	配置的 VAM 仍然存在	必须同时使用持久性和清除
已禁用远程分配地址	游戏机模式	已启用	未配置 VAM	设置为硬件 MAC 地址	设置为硬件 MAC 地址
已禁用远程分配地址	游戏机模式	已禁用	使用 Lifecycle Controller 中提供的路径配置	该周期的 Lifecycle Controller 配置仍然存在	不支持持久性。取决于卡行为
已启用远程分配地址	游戏机模式	已禁用	未配置 VAM	设置为硬件 MAC 地址	设置为硬件 MAC 地址

FlexAddress 和 IO 标识的系统行为

表. 45: FlexAddress 和 I/O 标识的系统行为

类型	FlexAddress 在 CMC 中的功能状态	IO 标识在 iDRAC 中的功能状态	重新引导周期远程代理 VA 的可用性	VA 编程源代码	重新引导周期 VA 持久性行为
具备 FA 同等持久性的服务器	已启用	已禁用		从 CMC FlexAddress	根据 FlexAddress 规格
	不适用，已启用或已禁用	已启用	是 - 新增或持久	远程代理虚拟地址	根据 FlexAddress 规格
			否	虚拟地址已清除	
	已禁用	已禁用			
具备 VAM 持久性策略功能的服务器	已启用	已禁用		从 CMC FlexAddress	根据 FlexAddress 规格
	已启用	已启用	是 - 新增或持久	远程代理虚拟地址	根据远程代理策略设置
			否	从 CMC FlexAddress	根据 FlexAddress 规格
	已禁用	已启用	是 - 新增或持久	远程代理虚拟地址	根据远程代理策略设置
			否	虚拟地址已清除	
	已禁用	已禁用			

启用或禁用 I/O 标识优化功能

通常，设备在系统引导后被配置，然后在系统重新引导后被初始化。您可以启用“I/O 标识优化”功能以实现引导优化。如果启用此功能，它会在设备重设之后及初始化之前设置虚拟地址、启动器和存储目标属性，因而无需第二次 BIOS 重启。设备配置和引导操作通过一次系统启动而完成，并针对引导时间性能进行优化。

启用 I/O 标识优化功能之前，请确保：

- 您拥有登录、配置和系统控制权限。
- BIOS、iDRAC 和网卡已更新为最新固件。

启用 I/O 标识优化功能后，从 iDRAC 导出服务器配置配置文件，在 SCP 文件中修改所需的 I/O 标识属性，然后将此文件重新导入 iDRAC。

有关 SCP 文件中可修改的 I/O 标识优化功能属性的列表，请参阅 https://www.dell.com/support 上提供的 *NIC Profile*（NIC 配置文件）说明文件。

注: 不要修改非 I/O □□□化功能属性。

使用 Web 界面启用或禁用 I/O 标识优化功能

要启用或禁用 I/O 标识优化功能，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **I/O Identity Optimization（I/O 标识优化）**。
   随即会显示 **I/O Identity Optimization（I/O 身份优化）**页面。
2. 单击 **I/O Identity Optimization（I/O 身份优化）**选项卡，选择 **Enable（启用）**选项以启用此功能。要禁用，则清除此选项。
3. 单击**应用**可应用设置。

使用 RACADM 启用或禁用 I/O 标识优化功能

要启用 I/O 标识优化功能，请使用以下命令：

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

启用此功能后，您必须重新启动系统才能使设置生效。

要禁用 I/O 标识优化功能，请使用以下命令：

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

要查看 I/O 标识优化功能设置，请使用以下命令：

```
racadm get iDRAC.IOIDOpt
```

SSD 磨损阈值

iDRAC 使您能够配置所有 SSD 的剩余额定写入寿命的阈值，以及 NVMe PCIe SSD 可用备盘。

当“SSD 剩余额定写入寿命”和“NVMe PCIe SSD 可用备盘”值低于阈值时，iDRAC 会将此事件记录在 LC 日志中，根据警报类型选择，iDRAC 还会执行电子邮件警报、SNMP 陷阱、IPMI 警报、远程系统日志中的日志记录、WS 事件和操作系统日志。

当“SSD 剩余额定写入寿命”低于设置的阈值时，iDRAC 会提醒用户，以便系统管理员可以执行 SSD 备份或更换。

仅对于 NVMe PCIe SSD，iDRAC 显示**可用备盘**，并提供警告阈值。对于 PERC 和 HBA 背后连接的 SSD，**可用备盘**不可用。

使用 Web 界面配置 SSD 磨损阈值警报功能

要使用 Web 界面配置剩余额定写入寿命和可用备盘警报阈值，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **硬件设置** > **SSD 磨损阈值**。
   将显示 **SSD 磨损阈值**页面。

2. **剩余额定写入寿命** - 您可以将值设置为 1-99%。默认值是 10%。
   此功能的警报类型为 **SSD 磨损写入寿命**，并且由于阈值事件，导致安全警报为**警告。**
3. **可用备盘警报阈值** - 您可以将值设置为 1-99%。默认值是 10%。
   此功能的警报类型为 **SSD 磨损可用备盘**，并且由于阈值事件，导致安全警报为**警告。**

使用 RACADM 配置 SSD 磨损阈值警报功能

要配置剩余额定写入寿命，请使用以下命令：

```
racadm set System.Storage.RemainingRatedWriteEnduranceAlertThreshold n
```

，其中 n= 1 至 99%。

要配置可用备盘警报阈值，请使用以下命令：

```
racadm System.Storage.AvailableSpareAlertThreshold n
```

，其中 n= 1 至 99%。

配置持久性策略设置

通过使用 IO 标识功能，您可以配置策略以用于确定系统重设和电源重启行为，从而确定虚拟地址、启动器和存储目标设置的保留和清除。每个单独的持久性策略属性将应用于系统中所有适用设备的所有端口和分区。辅助供电设备与非辅助供电设备之间的设备行为不同。

注: 如果将**持久性策略**功能□置□默□□，□□功能在下列情况下可能无法正常工作：如果在 iDRAC 上将 **VirtualAddressManagement** 属性□置□ **FlexAddress**（非 MX 平台）或 **RemoteAssignedAddress**（MX 平台）模式，并且如果在 CMC（非 MX 平台）或 OME Modular（MX 平台）中禁用 FlexAddress 或 Remote-Assigned Address 功能；□确保在 iDRAC 中将 **VirtualAddressManagement** 属性□置□**控制台**模式，或者在 CMC 或 OME Modular 中启用 FlexAddress 或 Remote-Assigned Address 功能。

可以配置以下持久性策略：
- 虚拟地址：辅助供电设备
- 虚拟地址：非辅助供电设备
- 启动器
- 存储目标

在应用持久性策略之前，请确保：
- 对网络硬件至少进行一次资源清册，即，启用“重启时收集系统资源清册”操作。
- 启用 I/O 标识优化功能。

在以下情况下，事件将记录到 Lifecycle Controller 日志：
- 启用或禁用 I/O 标识优化功能。
- 持久性策略发生更改。
- 虚拟地址、启动器和目标值均根据持久性策略设置。系统将为配置的设备及应用此策略时这些设备设定的值记录单一一条日志条目。

针对 SNMP、电子邮件或 WS-eventing 通知启用事件操作。日志也包括在远程系统日志中。

持久性策略的默认值

表. 46: 持久性策略的默认值

持久性策略	AC 断电	冷引导	热引导
虚拟地址：辅助供电设备	未选中	已选择	已选择
虚拟地址：非辅助供电设备	未选中	未选中	已选择
启动器	已选择	已选择	已选择
存储目标	已选择	已选择	已选择

注: 禁用持久性续策略并执行会丢失虚拟地址的操作时，重新启用持久性续策略不会检索虚拟地址。您必须在启用持久性策略后再次设置虚拟地址。

注: 如果有持久性策略正在生效并且在 CNA 设备分区上设置了虚拟地址、启动器或存储目标，则在更改 VirtualizationMode 属性或分区的个人设置之前，不要重置或清除为虚拟地址、启动器和存储目标配置的值。禁用持久性策略时，将自动执行该操作。您还可以使用配置作业来将虚拟地址属性显式设置为 0s，并根据中的定义设置启动器和存储目标的值 iSCSI 启动器和存储目标默认值 页面上的 201。

使用 iDRAC Web 界面配置持久性策略设置

要配置持久性策略，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **系统设置** > **硬件设置** > **I/O 标识优化**。
2. 单击 **I/O 标识优化**选项卡。
3. 在**持久性策略**部分中，为每个持久性策略选择下列其中一项或多项：
   - **热重设** - 在发生热重设时保留虚拟地址或目标设置。
   - **冷重设** - 在发生冷重设时保留虚拟地址或目标设置。
   - **AC 断电** - 在发生 AC 断电情况时保留虚拟地址或目标设置。
4. 单击**应用**。
   将配置持久性策略。

使用 RACADM 配置持久性策略设置

要设置持久性策略，请将以下 racadm 对象与 **set** 子命令结合使用：

- 对于虚拟地址，请使用 **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** 和 **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd** 对象
- 对于启动器，请使用 **iDRAC.IOIDOPT.InitiatorPersistencePolicy** 对象
- 对于存储目标，请使用 **iDRAC.IOIDOpt.StorageTargetPersistencePolicy** 对象

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

iSCSI 启动器和存储目标默认值

下表提供了清除持久性策略之后的 iSCSI 启动器和存储目标的默认值的列表。

表. 47: iSCSI 启动器 - 默认值

iSCSI Initiator（iSCSI 启动器）	IPv4 模式下的默认值	IPv6 模式下的默认值
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0

表. 47: iSCSI 启动器 - 默认值 （续）

iSCSI Initiator（iSCSI 启动器）	IPv4 模式下的默认值	IPv6 模式下的默认值
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
IscsiInitiatorName	已清除值	已清除值
IscsiInitiatorChapId	已清除值	已清除值
IscsiInitiatorChapPwd	已清除值	已清除值
IPVer	Ipv4	Ipv6

表. 48: iSCSI 存储目标属性 - 默认值

iSCSI 存储目标属性	IPv4 模式下的默认值	IPv6 模式下的默认值
ConnectFirstTgt	已禁用	已禁用
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	已清除值	已清除值
FirstTgtChapId	已清除值	已清除值
FirstTgtChapPwd	已清除值	已清除值
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	已禁用	已禁用
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	已清除值	已清除值
SecondTgtChapId	已清除值	已清除值
SecondTgtChapPwd	已清除值	已清除值
SecondTgtIpVer	Ipv4	

17

管理存储设备

从 iDRAC 3.15.15.15 版本开始，iDRAC 在第 14 代 PowerEdge 服务器中支持引导优化存储解决方案 (BOSS) 控制器。BOSS 控制器旨在专门用于引导服务器的操作系统。这些控制器支持有限的 RAID 功能和暂存配置。

从 iDRAC 4.30.30.30 版本开始，iDRAC 支持适用于 AMD 系统的 PERC 11、HBA 11 和 BOSS 1.5。

注: BOSS 控制器□支持 RAID □别 1。

注: □于 BOSS 控制器，当两个 PD 拔出并重新插入后，完整的虚□磁□信息可能不可用。

注: PERC 11 和更高版本的控制器支持硬件信任根 (RoT)。

iDRAC 扩展了免代理管理，以包括直接配置 PERC 控制器。它允许您在运行时远程配置连接到系统的存储组件。这些组件包括 RAID 和非 RAID 控制器以及连接到它们的通道、端口、机柜和磁盘。PowerEdge Rx4xx/Cx4xx 服务器支持 PERC 9 和 PERC 10 控制器。PowerEdge Rx5xx/Cx5xx AMD 平台服务器支持 PERC 11。

完整的存储子系统的查找、拓扑、运行状况监测和配置将在综合嵌入式管理 (CEM) 框架中完成，方法是基于 I2C 接口通过 MCTP 协议与内部和外部 PERC 控制器进行通信。对于实时配置，CEM 支持 PERC9 控制器和更高版本。PERC9 控制器上的固件版本必须是 9.1 或更高版本。

注: □件 RAID (SWRAID) 不受 CEM 支持，因此在 iDRAC GUI 中不受支持。可以使用 RACADM、WSMan 或 Redfish 来管理 SWRAID。

通过使用 iDRAC，您可以执行 OpenManage Storage Management 中提供的大多数功能，包括实时（无需重新引导）配置命令（例如，创建虚拟磁盘）。您可以在安装操作系统之前先完整地配置 RAID。

您无需访问 BIOS 即可配置和管理控制器功能。这些功能包括配置虚拟磁盘并应用 RAID 级别和热备用以实现数据保护。您可以启动许多其他控制器功能，例如重建和故障排除。您可以通过配置数据冗余或分配热备用来保护数据。

存储设备包括：

- 控制器 — 大多数操作系统无法直接从磁盘读写数据，而是将读取和写入说明发送到控制器。控制器是系统中与磁盘直接交互的硬件以写入和检索数据。控制器具有连接至一个或多个物理磁盘或包含物理磁盘的机柜的连接器（信道或端口）。RAID 控制器可以跨越磁盘边界，使用多个磁盘的容量创建一个经过扩展的存储空间或虚拟磁盘。控制器还能执行其他任务，比如启动重建和初始化磁盘等。要完成任务，控制器需要称为固件和驱动程序的特殊软件。为了正常工作，控制器必须装有所需的最低固件和驱动程序版本。不同的控制器在读取和写入数据以及执行任务方面具有不同的特征。理解这些功能有助于更有效地管理存储。
- 物理磁盘或物理设备 — 位于机柜内或连接到控制器。在 RAID 控制器上，物理磁盘或物理设备用于创建虚拟磁盘。
- 虚拟磁盘 — RAID 控制器从一个或多个物理磁盘创建的存储。虽然虚拟磁盘可能由多个物理磁盘创建，但是操作系统将其视为单个磁盘。根据使用的 RAID 级别，如果存在磁盘故障或具有特定的性能属性，虚拟磁盘可能会保留冗余数据。虚拟磁盘只能在 RAID 控制器上创建。
- 机柜 - 其连接到系统的外部，而背板及其物理磁盘则位于内部。
- 背板 — 它与机柜类似。在背板中，控制器连接器和物理磁盘连接到机柜，但它不具备与外部机柜关联的管理功能（温度探测器、警报等）。物理磁盘可以包含在机柜中，也可以连接到系统背板。

注: 在任何包含存□底座和□算底座的 MX 机箱中，与□机箱中的任何□算底座有关的 iDRAC 将□告所有存□底座（已分配和未分配）。如果任何一个已分配或未分配的刀片式服□器□于“警告”或“□重”运行状□，□刀片控制器也会□告相同的状□。

除了管理机柜中包含的物理磁盘，您还可以监测机柜中的风扇、电源设备和温度探测器的状态。您可以热插拔机柜。热插拔就是在操作系统仍然运行的时候将组件添加到系统中。

连接到控制器的物理设备必须具有最新的固件。如需最新的受支持固件，请联系您的服务提供商。

存储事件从 PERC 映射到 SNMP 陷阱和 WSMan 事件（如果适用）。对存储配置所做的任何更改都将记录在 Lifecycle 日志中。

表. 49: PERC 功能

PERC 功能	支持 CEM 配置的控制器（PERC 9.1 或更高版本）	不支持 CEM 配置的控制器（PERC 9.0 版和更低版本）
实时	**注:** PowerEdge Rx5xx/Cx5xx 服务器支持 PERC 9、PERC 10 和 PERC 11 控制器。 如果控制器没有现有挂起作业或已计划的作业，则应用配置。 如果该控制器具有待处理作业或已计划的作业，则必须清除这些作业，或者您必须等待这些作业完成，然后再在运行时应用配置。运行时或实时意味着，不需要重新启动。	将应用配置。此时会显示一条错误消息。创建任务未成功，并且您无法使用 Web 界面创建实时作业。
分阶段	如果已设置的所有操作均分阶段进行，则配置会采用分阶段方式，并在重新引导后应用或者实时地应用。	将在重新引导后应用配置

主□：

- 理解 RAID 概念
- 支持的控制器
- 支持的机柜
- 支持的存□□□功能的摘要
- □源清册和□□存□□□
- □看存□□□拓扑
- 管理物理磁□
- 管理虚□磁□
- RAID 配置功能
- 管理控制器
- 管理 PCIe SSD
- 管理机柜或背板
- □□要□用□置的操作模式
- □看和□用挂起操作
- 存□□□ - □用操作方案
- □□或取消□□□件 LED
- □重新启□

理解 RAID 概念

Storage Management 使用独立磁盘冗余阵列 (RAID) 技术提供存储管理功能。了解 Storage Management，就需要理解 RAID 的概念并且熟悉 RAID 控制器和操作系统如何查看您的系统上的磁盘空间。

什么是 RAID

RAID 是一个用于管理驻留或连接到系统的物理磁盘上的数据存储技术。RAID 的一个重要方面是跨接物理磁盘，以便可以将多个物理磁盘的组合存储容量视为单个扩展的磁盘空间。RAID 是另一个重要方面是能够维护冗余数据，可用于在发生磁盘故障时恢复数据。RAID 使用不同的技术，例如分拆、镜像和奇偶校验，以存储和重新构建数据。不同的 RAID 级别使用不同的方法，以备将来存放和重新构建数据。RAID 级别在读/写性能、数据保护和存储容量方面具有不同的特性。并非所有 RAID 级别都维护冗余数据，这意味着，某些 RAID 级别丢失的数据无法恢复。您选择的 RAID 级别取决于您的优先级是性能、保护还是存储容量。

注: RAID Advisory Board (RAB) 定□了用于□施 RAID 的□格。虽然 RAB 定□了 RAID □别，但不同的供□商□ RAID □别的商□□□与□□ RAID □格可能会有所不同。由特定供□商□施的方案可能会影响□取和写入性能和数据冗余的程度。

硬件和软件 RAID

RAID 可以通过硬件或软件实施。使用硬件 RAID 的系统具有实施了 RAID 级别的 RAID 控制器，并且可处理到物理磁盘的数据读取和写入。使用操作系统提供的软件 RAID 时，操作系统将实现 RAID 级别。因此，使用软件 RAID 本身会降低系统性能。不过，您可以使用软件 RAID 及硬件 RAID 卷，以实现更好的性能和多种 RAID 卷配置。例如，您可以跨两个 RAID 控制器镜像一对硬件 RAID 5 卷，以提供 RAID 控制器冗余。

RAID 概念

RAID 使用特定的技术将数据写入磁盘。这些技术使 RAID 能够提供数据冗余或更好的性能。这些技术包括：

- 镜像 — 数据从一个物理磁盘复制到另一个物理磁盘。镜像通过维护不同物理磁盘上相同数据的两个副本提供数据冗余。如果镜像中的一个磁盘出现故障，则系统可以继续使用未受影响的磁盘执行操作。镜像的两端始终包含相同数据。镜像的任何一端都可以作为运行端。镜像的 RAID 磁盘组与 RAID 5 磁盘组相比，读取操作中的性能类似，但写入操作中的性能更快。
- 分条 — 磁盘分条会在虚拟磁盘钟的所有物理磁盘上写入数据。每个分条均包含连续的虚拟磁盘数据地址，可使用连续模式以固定大小的单位映射至虚拟磁盘中的每个物理磁盘。例如，如果虚拟磁盘包括 5 个物理磁盘，则分条会将数据写入物理磁盘 1 至 5，而不会对任何物理磁盘执行重复操作。每个分条在每个物理磁盘占用的空间量都相同。位于物理磁盘上的分条部分即分条元素。分条本身不提供数据冗余。分条与奇偶校验结合可提供数据冗余。
- 条带大小 — 由条带（不包括奇偶校验磁盘）使用的总磁盘空间。例如，假设条带包含 64 KB 磁盘空间，并且在条带中的每个磁盘上有 16 KB 的数据。在此情况下，条带大小是 64 KB，而磁条元素大小为 16 KB。
- 元素带 — 元素带是位于单个物理磁盘上的条带部分。
- 条带元素大小 — 条带元素使用的磁盘空间量。例如，假设条带包含 64 KB 磁盘空间，并且在条带中的每个磁盘上有 16 KB 的数据。在此情况下，条带元素大小是 16 KB，而条带大小是 64 KB。
- 奇偶校验 — 奇偶校验是指使用算法与条带结合的方式维护冗余数据。当一个分条磁盘发生故障时，可以使用该算法从奇偶校验信息重新构建数据。
- 跨接 — 跨接是一种 RAID 技术，用于将物理磁盘组的存储空间组合为 RAID 10、50 或 60 虚拟磁盘。

RAID 级别

每种 RAID 级别都使用某种镜像、分条和奇偶校验组合，以提供数据冗余或提高读取和写入性能。有关各个 RAID 级别的特定信息，请参阅选择 RAID 级别。

为了可用性和性能组织数据存储

RAID 提供不同的方法或 RAID 级别来排列磁盘存储。某些 RAID 级别保存冗余数据，以便在磁盘出现故障后您可以恢复数据。不同的 RAID 级别也会导致系统的 I/O（读取和写入）性能提高或降低。

保存冗余数据需要使用额外的物理磁盘。随着磁盘数量增加，会导致磁盘发生故障的可能性提高。由于 I/O 性能和冗余性不同，某个 RAID 级别可能比另一个更适合，这取决于操作环境中的应用程序和所存储数据的性质。

选择某个 RAID 级别后，需要注意以下性能和成本问题：

- 可用性或容错 — 可用性或容错是指当其中一个组件发生故障时，系统维持操作并提供数据访问的能力。在 RAID 卷中，可用性或容错通过维护冗余数据实现。冗余数据包括镜像（重复数据）和奇偶校验信息（使用一种算法重建数据）。
- 性能 — 读取和写入性能可以提高或降低，具体取决于您选择的 RAID 级别。某些 RAID 级别可能更适合于特定应用程序。
- 成本效率 — 维护与 RAID 卷关联的冗余数据或奇偶校验信息需要额外的磁盘空间。如果数据是临时的、可轻松重新生成或者非必要，数据冗余性成本增加可能是不合理的。
- 平均故障间隔时间 (MTBF) — 如果使用额外的磁盘维护数据冗余性，在任何给定的时刻，也增加了磁盘故障的几率。尽管在需要冗余数据的情况下此选项无法避免，但这确实会影响组织中系统支持人员的工作负担。
- 卷 — 卷是指单个磁盘的非 RAID 虚拟磁盘。您可以使用 O-ROM <Ctrl> <r> 等外部公用程序创建卷。Storage Management 不支持创建卷。不过，您可以查看这些卷并使用这些卷中的驱动器创建新的虚拟磁盘的卷或对现有的虚拟磁盘进行联机容量扩展 (OCE)（前提是有可用空间）。

选择 RAID 级别

您可以使用 RAID 以在多个磁盘上控制数据存储。每种 RAID 级别或串联都具有不同的性能和数据保护特点。

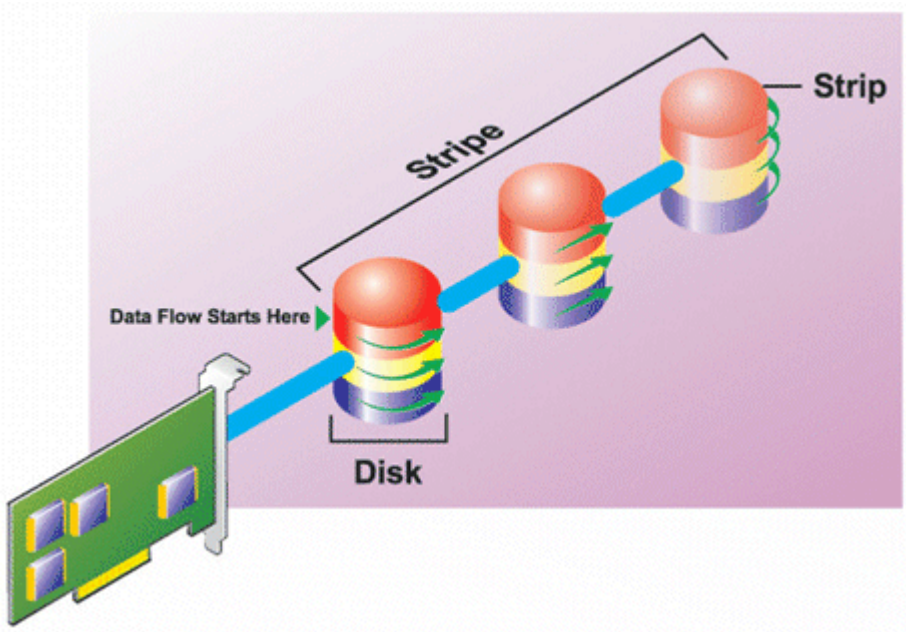
注: H3xx PERC 控制器不支持 RAID □别 6 至 60。

以下主题具体提供了各种 RAID 级别存储数据的方式，以及各自的性能和保护特点：

- RAID 级别 0（分条）
- RAID 级别 1（镜像）
- RAID 级别 5（带有分布式奇偶校验的分条）
- RAID 级别 6（带有额外分布式奇偶校验的分条）
- RAID 级别 50（在 RAID 5 组上分条）
- RAID 级别 60（在 RAID 6 组上分条）
- RAID 级别 10（在镜像组上分条）

RAID 级别 0 - 分条

RAID 0 使用数据分条，将数据写入跨物理磁盘的相等大小分段。RAID 0 不提供数据冗余。

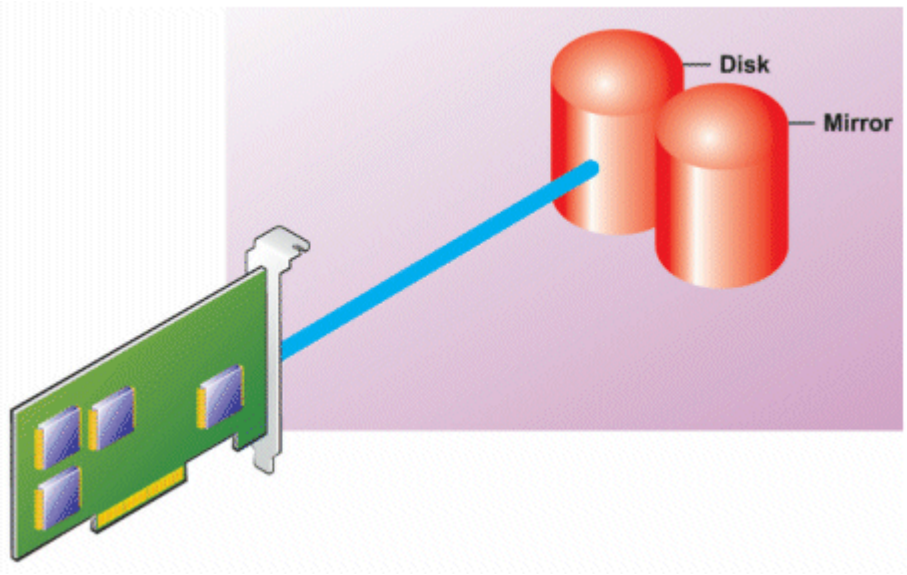


RAID 0 特点：

- 将 *n* 个磁盘组合成一个大虚拟磁盘，其容量为（最小磁盘大小）**n* 个磁盘。
- 数据交替存储到磁盘上。
- 不存储冗余数据。如果一个磁盘发生故障，大虚拟磁盘也会发生故障，并且无法重建数据。
- 更好的读写性能。

RAID 级别 1 - 镜像

RAID 1 是维护冗余数据的最简单形式。在 RAID 1 中，数据会镜像或复制一个或多个物理磁盘上。如果物理磁盘发生故障，则可使用镜像另一端的数据重新构建数据。

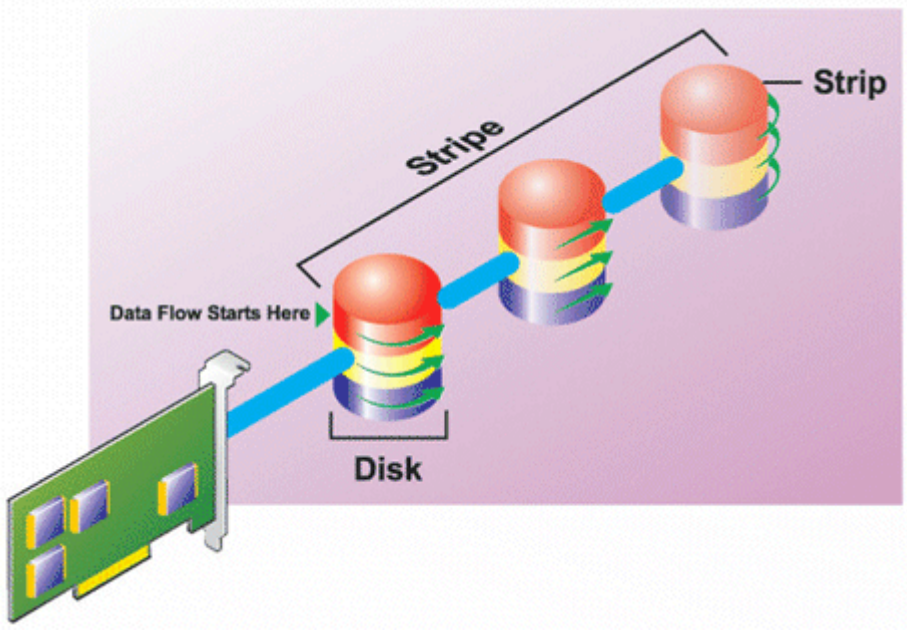


RAID 1 特点：

- 将 *n* + *n* 个磁盘分组为一个具有 *n* 个磁盘容量的虚拟磁盘。当前由 Storage Management 支持的控制器允许在创建 RAID 1 时选择两个磁盘。由于这些磁盘已镜像，总存储容量相当于一个磁盘。
- 数据同时复制到这两个磁盘。
- 当磁盘发生故障时，虚拟磁盘仍将工作。数据将从故障磁盘的镜像中读取。
- 读性能更好，但写性能较差。
- 用于保护数据的冗余。
- RAID 1 在磁盘空间方面成本较高，因为用来存储数据的磁盘数目是不使用冗余时的两倍。

RAID 级别 5 或 带有分布式奇偶校验的分条

RAID 5 通过结合使用数据分条和奇偶校验信息提供数据冗余。奇偶校验信息跨磁盘组中的所有物理磁盘进行分条，而不是将某个物理磁盘专用于奇偶校验。



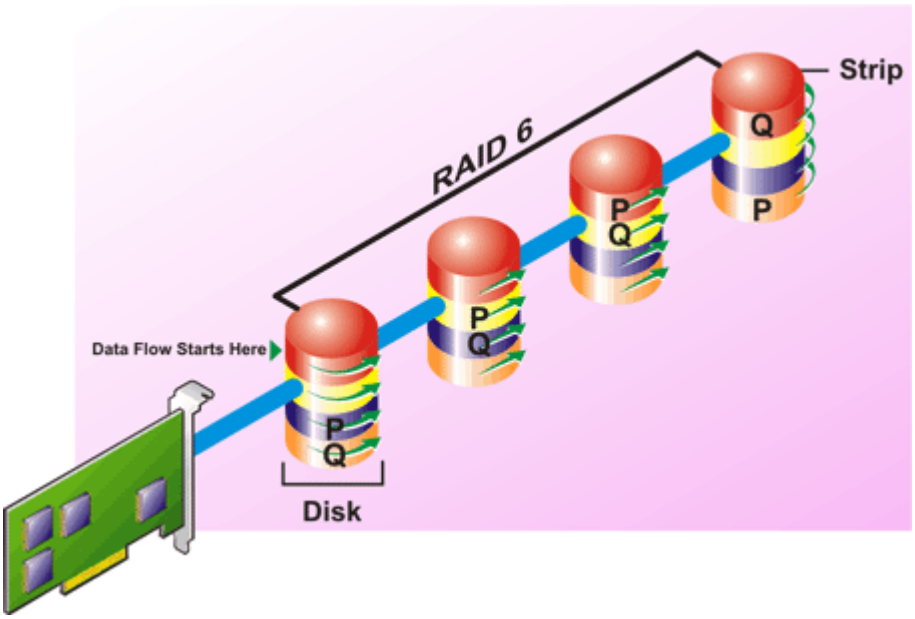
RAID 5 特点：

- 将 *n* 个磁盘组合为一个具有 (*n*-1) 个磁盘容量的大虚拟磁盘。
- 冗余信息（奇偶校验）交替存储在所有磁盘上。
- 如果一个磁盘发生故障，虚拟磁盘仍将工作，但是会在降级状态下运行。将从仍正常运行的磁盘重新构建数据。

- 读性能更好，但写性能较慢。
- 用于保护数据的冗余。

RAID 级别 6（带有额外分布式奇偶校验的分条）

RAID 6 通过结合使用数据分拆和奇偶校验信息提供数据冗余。与 RAID 5 相似，奇偶校验分布于每个磁条中。但是 RAID 6 使用附加的物理磁盘维持奇偶校验，从而使得磁盘组中的每个磁条能够使用奇偶校验信息维护两个磁盘块。附加的奇偶校验可在两个磁盘发生故障时提供数据保护。在下图中，将两组奇偶校验信息标识为 **P** 和 **Q**。



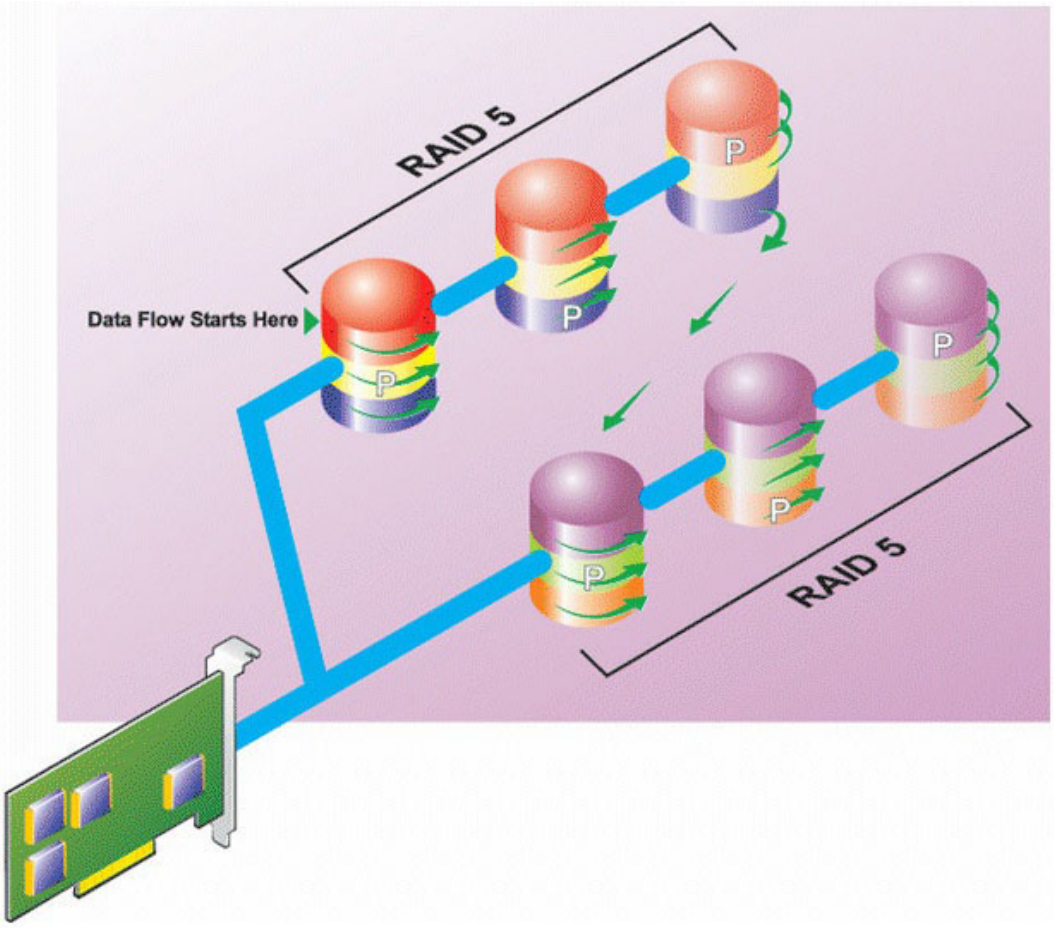
RAID 6 特点：

- 将 *n* 个磁盘组合为一个具有 (*n*-2) 个磁盘容量的大虚拟磁盘。
- 冗余信息（奇偶校验）交替存储在所有磁盘上。
- 最多两个磁盘发生故障时，虚拟磁盘仍将正常工作。将从仍正常运行的磁盘重新构建数据。
- 读性能更好，但写性能较慢。
- 用于保护数据的提高的冗余。
- 每个跨接需要有两个磁盘用于奇偶校验。RAID 6 在磁盘空间方面成本较高。

RAID 级别 50（在 RAID 5 组上分条）

RAID 50 跨多个物理磁盘实现分条。例如，一个实施了三个物理磁盘的 RAID 5 磁盘组，接着配置具有另外三个物理磁盘的磁盘组就是 RAID 50。

即使硬件不直接支持它，也有可能实现 RAID 50。在这种情况下，您可以实施多个 RAID 5 虚拟磁盘，然后将这些 RAID 5 磁盘转换为动态磁盘。然后，您可以创建一个跨接所有 RAID 5 虚拟磁盘的动态卷。

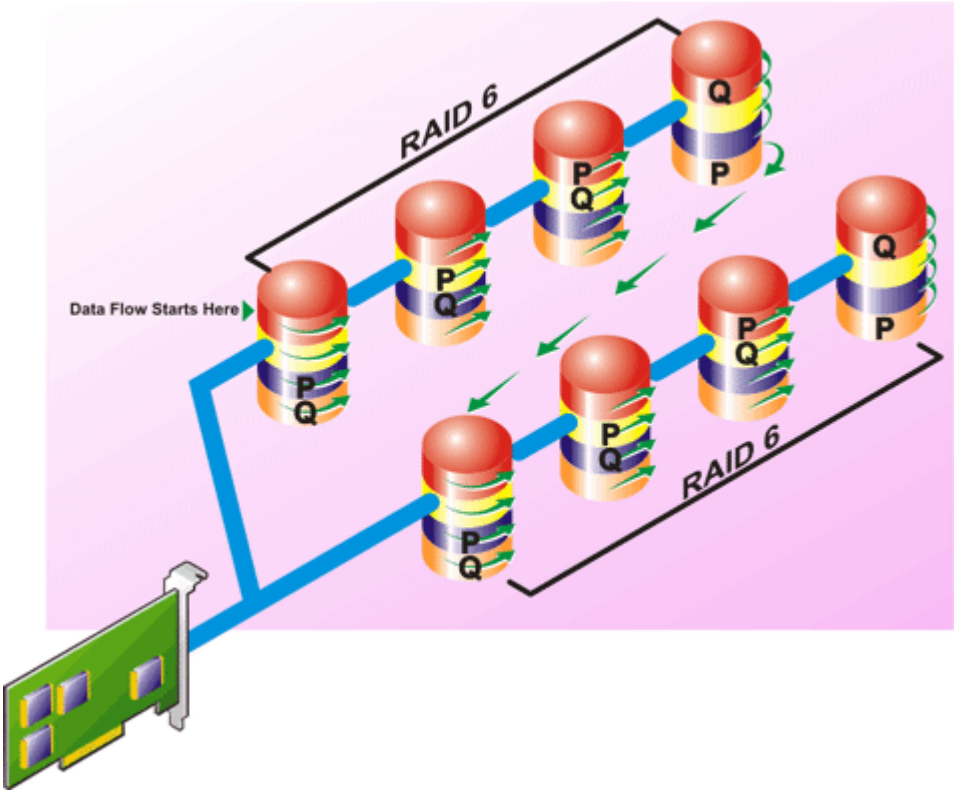


RAID 50 特点：

- 将 *n***s* 个磁盘组合为一个大虚拟磁盘，容量为 *s**(*n*-1) 个磁盘，其中 *s* 是跨接数，*n* 是每个跨接中的磁盘数。
- 冗余信息（奇偶校验）交替存储在每个 RAID 5 跨接的所有磁盘上。
- 读性能更好，但写性能较慢。
- 需要与标准 RAID 5 一样多的奇偶校验信息。
- 数据将在所有跨接上分条。RAID 50 在磁盘空间方面成本更高。

RAID 级别 60（在 RAID 6 组上分条）

RAID 60 在配置为 RAID 6 的多个物理磁盘跨接上实现分条。例如，一个实施了四个物理磁盘的 RAID 6 磁盘组接着配置一个具有另外四个物理磁盘的磁盘组就是 RAID 60。

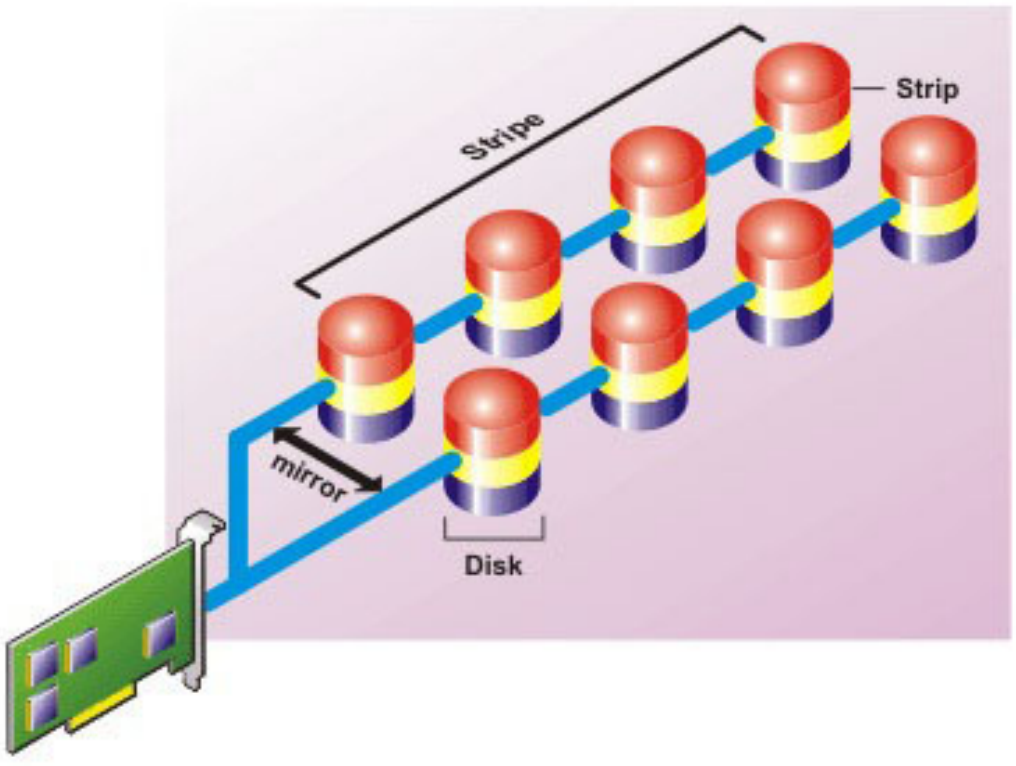


RAID 60 特点：

- 将 *n***s* 个磁盘组合为一个大虚拟磁盘，容量为 *s**(*n*-2) 个磁盘，其中 *s* 是跨接数，*n* 是每个跨接中的磁盘数。
- 冗余信息（奇偶校验）交替存储在每个 RAID 6 跨接的所有磁盘上。
- 读性能更好，但写性能较慢。
- 增加的冗余提供了比 RAID 50 更高的数据保护。
- 按照比例，需要与 RAID 6 一样多的奇偶校验信息。
- 每个跨接需要有两个磁盘用于奇偶校验。RAID 60 在磁盘空间方面成本较高。

RAID 级别 10 - 带有镜像的分条

RAB 将 RAID 级别 10 视为 RAID 级别 1 的实施。RAID 10 将镜像物理磁盘 (RAID 1) 与数据分条 (RAID 0) 相结合。使用 RAID 10，数据将跨多个物理磁盘分条。然后，分条的磁盘组将镜像到另一组物理磁盘上。RAID 10 可视为*分条的镜像*。



RAID 10 特点：

- 将 *n* 个磁盘组合为一个大虚拟磁盘，容量为 (*n*/2) 个磁盘，其中 *n* 是一个偶数整数。
- 数据的镜像映像将跨一组物理磁盘分条。此级别通过镜像提供冗余。
- 当磁盘发生故障时，虚拟磁盘仍将工作。数据将从未出现故障的镜像磁盘中读取。
- 读写性能均有所提高。
- 用于保护数据的冗余。

比较 RAID 级别的性能

下表比较了一些常用 RAID 级别的相关性能特点。此表提供了选择 RAID 级别的一般原则。选择 RAID 级别之前，评估具体的环境要求。

表. 50: RAID 级别性能比较

RAID 级别	数据冗余	读性能	写性能	重建性能	所需的最小磁盘	建议的用途
RAID 0	无	很好	很好	不适用	否	不重要数据。
RAID 1	极好	很好	良好	良好	2N (N = 1)	小型数据库、数据库日志和重要信息。
RAID 5	良好	按顺序读：好。 按事务读：很好	一般，除非使用回写高速缓存	一般	N + 1（N = 至少为两个磁盘）	数据库和其他读密集型事务性使用。
RAID 10	极好	很好	一般	良好	2N x X	数据密集型环境（大记录）。
RAID 50	良好	很好	一般	一般	N + 2（N = 至少为 4）	中等程度的事务性或数据密集型使用。
RAID 6	极好	按顺序读：好。 按事务读：很好	一般，除非使用回写高速缓存	差	N + 2（N = 至少为两个磁盘）	重要信息。数据库和其他读密集型事务性使用。

表. 50: RAID 级别性能比较 （续）

RAID 级别	数据冗余	读性能	写性能	重建性能	所需的最小磁盘	建议的用途
RAID 60	极好	很好	一般	差	X x (N + 2) （N = 至少为 2）	重要信息。中等程度的事务性或数据密集型使用。
N = 物理磁盘数 X = RAID 组数						

支持的控制器

支持的 RAID 控制器

iDRAC 界面支持以下 BOSS 控制器：
- BOSS-S1 适配器
- BOSS-S1 Modular（用于刀片服务器）
- BOSS-S2 适配器

iDRAC 接口支持以下 PERC11 控制器：
- PERC H755 适配器
- PERC H755 前端
- PERC H755N 前端

iDRAC 界面支持以下 PERC10 控制器：
- PERC H740P Mini
- PERC H740P 适配器
- PERC H840 适配器
- PERC H745P MX

iDRAC 接口支持以下 PERC9 控制器：
- PERC H330 Mini
- PERC H330 适配器
- PERC H730P Mini
- PERC H730P 适配器
- PERC H730P MX

支持的非 RAID 控制器

iDRAC 界面支持 12 Gbps SAS HBA 外部控制器和 HBA330 Mini 或适配器控制器。

iDRAC 支持 HBA330 MMZ、HBA330 MX 适配器。

支持的机柜

iDRAC 支持 MD1400 和 MD1420 机柜。

注: 不支持连接到 HBA 控制器的廉价磁盘冗余阵列 (RBODS)。

注: PERC H480（版本为 10.1 或更高版本）固件支持每个端口最多 4 个机柜。

支持的存储设备功能的摘要

下表提供了存储设备通过 iDRAC 支持的功能。

表. 51: 支持的存储控制器功能

功能部件	PERC 11			PERC 10			PERC 9				
	H755 前端	H755N 前端	H755 适配器	H740P Mini	H740P 适配器	H840 适配器	H330 Mini	H330 适配器	H730P Mini	H730P 适配器	FD33xS
分配或取消分配物理磁盘作为全局热备用	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
转换为 RAID	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用
转换为 RAID/非 RAID，	实时（将驱动器转换为非 RAID ePD-PT 卷）	实时（将驱动器转换为非 RAID ePD-PT 卷）	实时（将驱动器转换为非 RAID ePD-PT 卷）	实时（仅在 eHBA 控制器模式下受支持，将驱动器转换为非 RAID ePD-PT 卷）	实时（仅在 eHBA 控制器模式下受支持，将驱动器转换为非 RAID ePD-PT 卷）	实时（仅在 eHBA 控制器模式下受支持，将驱动器转换为非 RAID ePD-PT 卷）	实时	实时	实时	实时	实时
重建	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
取消重建	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
创建虚拟磁盘	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
重命名虚拟磁盘	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
编辑虚拟磁盘高速缓存策略	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
检查虚拟磁盘一致性	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
取消检查一致性	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
初始化虚拟磁盘	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
取消初始化	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
加密虚拟磁盘	实时	实时	实时	实时	实时	实时	不适用	不适用	实时	实时	实时
分配和取消分配专用热备用	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时

表. 51: 支持的存储控制器功能 （续）

功能部件	PERC 11			PERC 10			PERC 9				
	H755 前端	H755N 前端	H755 适配器	H740P Mini	H740P 适配器	H840 适配器	H330 Mini	H330 适配器	H730P Mini	H730P 适配器	FD33xS
删除虚拟磁盘	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
取消后台初始化	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
联机容量扩展	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
RAID 级别迁移	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
丢弃保留的高速缓存	实时	实时	实时	实时	实时	实时	不适用	不适用	实时	实时	实时
设置巡检读取模式	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
手动巡检读取模式	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
巡检读取未配置区域	实时	实时	实时	实时	实时	实时	实时（仅限 Web 界面中）	实时（仅限 Web 界面中）	实时（仅限 Web 界面中）	实时（仅限 Web 界面中）	实时（仅限 Web 界面中）
检查一致性模式	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
回写模式	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
负载平衡模式	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
检查一致性率	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
重建率	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
后台初始化 (BGI) 率	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
重构率	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
导入外部配置	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
自动导入外部配置	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
清除外部配置	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
重设控制器配置	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时

表. 51: 支持的存储控制器功能 （续）

功能部件	PERC 11			PERC 10			PERC 9				
	H755 前端	H755N 前端	H755 适配器	H740P Mini	H740P 适配器	H840 适配器	H330 Mini	H330 适配器	H730P Mini	H730P 适配器	FD33xS
创建或更改安全密钥	实时	实时	实时	实时	实时	实时	不适用	不适用	实时	实时	实时
安全企业密钥管理器	分阶段	分阶段	分阶段	分阶段	分阶段	分阶段	不适用	不适用	不适用	不适用	不适用
对 PCIe SSD 设备运行状况进行资源清册和远程监测	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用
准备 PCIe SSD 以待移除	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用
安全擦除 PCIe SSD 的数据	不适用	实时	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用
配置背板模式（拆分/统一）	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
闪烁或取消闪烁组件 LED	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时	实时
切换控制器模式	不适用	不适用	不适用	分阶段	分阶段	分阶段	分阶段	分阶段	分阶段	分阶段	分阶段
虚拟磁盘的 T10PI 支持	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用

注: 增加了对以下各项的支持

- PERC 10.2 或更高版本固件的 eHBA 模式，支持转换为非 RAID 磁盘
- 将控制器转换为 HBA 模式
- RAID 10 不对等跨接

表. 52: 用于 MX 平台的存储控制器支持的功能

功能	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
初始化虚拟磁盘	实时	实时	实时
取消初始化	实时	实时	实时
加密虚拟磁盘	实时	实时	实时

表. 52: 用于 MX 平台的存储控制器支持的功能 （续）

功能	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
分配和取消分配专用热备用	实时	实时	实时
删除虚拟磁盘	实时	实时	实时
取消后台初始化	实时	实时	实时
联机容量扩展	实时	实时	实时
RAID 级别迁移	实时	实时	实时
丢弃保留的高速缓存	实时	实时	实时
设置巡检读取模式	实时	实时	实时
手动巡检读取模式	实时	实时	实时
巡检读取未配置区域	实时	实时	实时（仅限 Web 界面中）
检查一致性模式	实时	实时	实时
回写模式	实时	实时	实时
负载平衡模式	实时	实时	实时
检查一致性率	实时	实时	实时
重建率	实时	实时	实时
后台初始化 (BGI) 率	实时	实时	实时
重构率	实时	实时	实时
导入外部配置	实时	实时	实时
自动导入外部配置	实时	实时	实时
清除外部配置	实时	实时	实时
重设控制器配置	实时	实时	实时
创建或更改安全密钥	实时	实时	实时
对 PCIe SSD 设备运行状况进行资源清册和远程监测	实时	不适用	不适用
准备 PCIe SSD 以待移除	不适用	不适用	不适用
安全擦除 PCIe SSD 的数据	实时	不适用	不适用
配置背板模式（拆分/统一）	实时	不适用	不适用
闪烁或取消闪烁组件 LED	实时	实时	实时
切换控制器模式	不适用	不适用	分阶段
虚拟磁盘的 T10PI 支持	不适用	不适用	不适用

注: 对于 PERC 10.2 及更高版本，H745P MX 支持 eHBA 模式。

表. 53: 支持的存储设备功能

功能部件	PCIe SSD	BOSS S1	BOSS S2
创建虚拟磁盘	不适用	分阶段	分阶段
重设控制器配置	不适用	分阶段	分阶段
快速初始化	不适用	分阶段	分阶段
删除虚拟磁盘	不适用	分阶段	分阶段

表. 53: 支持的存储设备功能 （续）

功能部件	PCIe SSD	BOSS S1	BOSS S2
完全初始化	不适用	不适用	不适用
对 PCIe SSD 设备运行状况进行资源清册和远程监测	实时	不适用	不适用
准备 PCIe SSD 以待移除	实时	不适用	不适用
安全擦除 PCIe SSD 的数据	分阶段	不适用	不适用
闪烁或取消闪烁组件 LED	实时	不适用	实时
热插拔驱动器	实时	不适用	实时

资源清册和监测存储设备

您可以使用 iDRAC Web 界面远程监测受管系统中以下启用综合嵌入式管理 (CEM) 功能的存储设备的运行状况并查看其资源清册：

- RAID 控制器、非 RAID 控制器、BOSS 控制器和 PCIe 扩展器
- 机柜，包括机柜管理模块 (EMM)、电源设备、风扇探测器和温度探测器
- 物理磁盘
- 虚拟磁盘
- 电池

还将显示存储设备最近的存储事件和拓扑。

生成存储事件的警报和 SNMP 陷阱。事件记录在 Lifecycle 日志中。

注：

- 如果您在系统上枚举机柜视图的 WSMAN 命令，并移除一个 PSU 电缆，机柜视图的主要状态将报告为**健康**，而不是**警告**。
- 对于 BOSS 控制器的准确资源清册，请确保完成重新引导时收集系统资源清册操作 (CSIOR)。默认启用 CSIOR。
- 存储运行状况汇总遵照 Dell EMC OpenManage 产品一样的惯例。有关更多信息，请参阅 *OpenManage Server Administrator 用户指南，网址：*https://www.dell.com/openmanagemanuals。
- 具有多个块背板的系统中的物理磁盘可能会被列在不同背板下。使用闪烁功能来识别磁盘。
- 在软件资源清册和硬件资源清册中，某些背板的 FQDD 可能不相同。
- 在处理过去的 PERC 控制器事件时，PERC 控制器的生命周期日志不可用，这不会影响此功能。过去事件的处理可能因配置而异

使用 Web 界面监测存储设备

使用 Web 界面查看存储设备信息：

- 转至**存储** > **概览** > **摘要**查看存储组件和最近记录事件的摘要。此页面每隔 30 秒自动刷新。
- 转至**存储** > **概览** > **控制器**查看 RAID 控制器信息。此时会显示**控制器**页面。
- 转至**存储** > **概览** > **物理磁盘**查看物理磁盘信息。将显示**物理磁盘**页面。
- 转至**存储** > **概览** > **虚拟磁盘**查看虚拟磁盘信息。将显示**虚拟磁盘**页面。
- 转至**存储** > **概览** > **机柜**查看机柜信息。此时将显示**机柜**页面。

您还可以使用筛选器查看特定的设备信息。

注：

- 如果系统中没有支持 CEM 的存储设备，则不会显示存储硬件列表。
- 非戴尔认证或第三方 NVMe 设备的行为在 iDRAC 中可能不一致。
- 如果背板插槽中的 NVMe SSD 支持 NVMe-MI 命令，并且 I2C 与背板插槽连接正常，则 iDRAC 会发现这些 NVMe SSD 并在界面中报告它们，这与各自背板插槽的 PCI 连接无关。

注：

类型	Web GUI 支持	其他界面支持
SATA	不可用	资源清册和 RAID 配置
NVMe	仅限物理磁盘资源清册	资源清册和 RAID 配置

有关所示属性以及使用筛选器选项的更多信息，请参阅 iDRAC 联机帮助。

使用 RACADM 监测存储设备

要查看存储设备信息，请使用的 `storage` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序监测背板

在 iDRAC 设置公用程序中，转至 **System Summary（系统摘要）**。随即会显示 **iDRAC Settings.System Summary**（iDRAC 设置.系统摘要）页面。**Backplane Inventory（背板资源清册）**部分中显示背板的信息。有关各字段的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。

查看存储设备拓扑

可查看关键存储组件的分层物理容器的视图，即，控制器及其所连机柜的列表以及一个指向每个机柜中的物理磁盘的链接。会显示物理磁盘直接连接到控制器。

要查看存储设备拓扑，转至 **Storage（存储）** > **Overview（概览）**。Overview（**概览**）页面显示系统中存储组件的层次化表示。可用的选项有：

- 控制器
- 物理磁盘
- 虚拟磁盘
- 机柜

单击此链接可查看相应组件的详细信息。

管理物理磁盘

可以对物理磁盘执行以下操作：

- 查看物理磁盘属性。
- 分配或取消分配物理磁盘作为全局热备用。
- 转换为 RAID 型磁盘。
- 转换为非 RAID 磁盘。
- 闪烁或取消闪烁 LED。
- 重建物理磁盘
- 取消重建物理磁盘
- 加密擦除

分配或取消分配物理磁盘作为全局热备用

全局热备份是磁盘组中一个未使用的备份磁盘。热备用保持在待机模式中。如果虚拟磁盘中的某个物理磁盘发生故障，会激活分配的热备用来更换出现故障的物理磁盘，而不用中断系统或要求用户干预。如果激活热备用，就会为原来使用那个出现故障的物理磁盘的所有冗余虚拟磁盘重建数据。

注： 自 iDRAC v3.00.00.00 或更高版本起，如果未□建虚□磁□，□可添加全局□□用。

用户可以通过取消磁盘分配并选择另一个所需磁盘来更改热备用的分配。用户也可以将一个以上的物理磁盘分配为全局热备用。

全局热备用的分配和取消分配必须手动执行。全局热备用并不分配给具体的虚拟磁盘。如果您想要将热备用分配给虚拟磁盘（它会替换虚拟磁盘中发生故障的任何物理磁盘），请参阅分配和取消分配专用热备用。

在删除虚拟磁盘时，如果删除了与控制器关联的最后一个虚拟磁盘，则可能会自动取消分配所有已分配的全局热备用。

如果重设配置，将删除虚拟磁盘，并取消分配所有热备用。

必须熟悉与热备用相关的大小要求和其他注意事项。

将物理磁盘分配为全局热备用之前的准备工作：

- 确保已启用 Lifecycle Controller。
- 如果不存在处于就绪状态的磁盘驱动器，请插入额外的磁盘驱动器，并确保这些驱动器处于就绪状态。
- 如果物理磁盘处于非 RAID 模式，则使用 iDRAC 界面（例如 iDRAC Web 界面、RACADM、Redfish 或 WSMan 或 <CTRL+R>）将它们转换为 RAID 模式。

  注: 在开机自检过程中，按 F2 键进入系统设置或设备设置。对于 PERC 10，不再支持 CTRL+R 选项。仅当“引导模式”设置为 BIOS 时，Ctrl+R 才可用于 PERC 9。

如果您已在“添加到挂起操作”模式中取消将物理磁盘分配为全局热备用，将创建挂起操作，但不会创建任务。因此，如果您尝试将此磁盘分配为全局热备用，将会清除此取消分配全局热备用挂起操作。因此，如果您尝试取消将此相同磁盘分配为全局热备用，将会清除此分配全局热备用挂起操作。

如果您已在“添加到挂起操作”模式中取消将物理磁盘分配为全局热备用，将创建挂起操作，但不会创建任务。因此，如果您尝试将此磁盘分配为全局热备用，将会清除此取消分配全局热备用挂起操作。

如果删除最后一个虚拟磁盘，全局热备份也会恢复为就绪状态。

如果物理磁盘已经是全局热备盘，用户仍可再次将它指定为全局热备盘。

使用 Web 界面分配或取消分配全局热备用

要为物理磁盘驱动器分配或取消分配全局热备用，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **存储配置**。
   此时会显示**存储配置**页面。
2. 从**控制器**下拉菜单中，选择控制器以查看关联的物理磁盘。
3. 单击**物理磁盘配置**。
   此时将会显示所有与该控制器关联的物理磁盘。
4. 要分配为全局热备用，请从**操作**列中的下拉菜单中，对一个或多个物理磁盘选择**分配全局热备用**。
5. 要取消分配热备用，请从**操作**列中的下拉菜单中，对一个或多个物理磁盘选择**取消分配热备用**。
6. 单击**立即应用**。
   根据您的需要，您还可以选择应用**在下次重新引导时**或**在计划的时间**。将根据选定的操作模式应用这些设置。

使用 RACADM 分配或取消分配全局热备用

使用 `storage` 命令并将类型指定为全局热备件。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

将物理磁盘转换为 RAID 或非 RAID 模式

将物理磁盘转换为 RAID 模式可使磁盘执行所有 RAID 操作。当磁盘处于非 RAID 模式时，不像未配置的良好磁盘一样对操作系统显示，并且可在直通模式下使用。

不支持 PERC 10 将驱动器转换为非 RAID。但在 PERC 10.2 和更高版本中受支持。

要将物理磁盘驱动器转换为 RAID 或非 RAID 模式，请执行以下操作：

- 使用 iDRAC 界面，例如 iDRAC Web 界面、RACADM、Redfish 或 WSMan。
- 在重新启动服务器时，按 <Ctrl+R> 组合键并选择所需控制器。

注: 如果□接到 PERC 控制器的物理□□器□于非 RAID 模式，□ iDRAC 界面（例如 iDRAC GUI、RACADM、Redfish 和 WSMan）中□示的磁□大小可能略小于磁□的□□大小。但是，您可以使用整个磁□容量来部署操作系□。

注:

- PERC H330 中的热插拔磁盘始终为非 RAID 模式。在其他 RAID 控制器中，它们始终为 RAID 模式。

- PERC 11 中的热插拔磁盘处于就绪状态或“EPD-PT”状态，具体取决于当前的自动配置行为设置。

使用 iDRAC Web 界面将物理磁盘转换为 RAID 模式或非 RAID 模式

要将物理磁盘转换为 RAID 模式或非 RAID 模式，请执行以下步骤：

1. 在 iDRAC Web 界面中，单击**存储** > **概览** > **物理磁盘**。
2. 请参阅**筛选选项**。将显示两个选项 - **清除所有筛选器**和**高级筛选器**。单击**高级筛选器**选项。
   将显示一个详细的列表，允许您配置不同参数。
3. 从**分组方式**下拉菜单中，选择一个机柜或虚拟磁盘。
   此时将显示与机柜或虚拟磁盘关联的参数。
4. 选择所有所需参数后，单击**应用**。有关各字段的更多信息，请参阅 *iDRAC 联机帮助*。
   将根据操作模式中的所选选项应用设置。

使用 RACADM 将物理磁盘转换为 RAID 模式或非 RAID 模式

根据要转换为 RAID 模式或非 RAID 模式，使用以下 RACADM 命令

- 要转换为 RAID 模式，请使用 `racadm storage converttoraid` 命令。
- 要转换为非 RAID 模式，请使用 `racadm storage converttononraid` 命令。

注: 在 S140 控制器上，您只能使用 RACADM 界面将驱动器从非 RAID 转换为 RAID 模式。支持的软件 RAID 模式是 Windows 或 Linux 模式。

有关命令的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

擦除物理磁盘

系统擦除功能让您可以擦除物理驱动器的内容。使用 RACADM 或 LC GUI 可访问此功能。服务器上的物理驱动器可分成两个类别。

- 安全擦除驱动器 — 包括能提供加密擦除的驱动器，例如 ISE、SED SAS、SATA 驱动器和 PCIe SSD。
- 覆盖擦除驱动器 — 包括不支持加密擦除的所有驱动器。

注: 在擦除 vFlash 之前，您必须先使用 iDRAC 接口分离所有分区，然后再执行此操作。

注: 系统擦除仅适用于服务器中的驱动器。iDRAC 无法擦除外部存储模块中的驱动器，例如 JBOD。

RACADM SystemErase 子命令包括以下类别的选项：

- **SecureErasePD** 选项加密擦除所有安全擦除驱动器。
- **OverwritePD** 选项覆盖所有驱动器上的数据。

注: 可以通过 `SystemErase` 方法完成对 BOSS 物理磁盘的加密擦除，LC UI、Wsman 和 Racadm 均支持此擦除方法

执行 SystemErase 之前，使用以下命令检查服务器的所有物理磁盘擦除功能：

```
# racadm storage get pdisks -o -p SystemEraseCapability
```

注: 如果服务器上已启用 SEKM，则在使用此命令之前，请使用 `racadm sekm disable` 命令禁用 SEKM。如果通过执行此命令从 iDRAC 中擦除了 SEKM 设置，则这可以避免被 iDRAC 保护的所有存储设备被锁定。

要擦除 ISE 和 SED 驱动器，请使用此命令：

```
# racadm systemerase -secureerasepd
```

要擦除覆盖擦除驱动器，请使用以下命令：

```
# racadm systemerase -overwritepd
```

注: RACADM SystemErase 从通过上述命令擦除的物理磁盘中移除所有虚拟磁盘。

注: RACADM SystemErase 将会使服务器重新启动来执行擦除操作。

注: 使用 iDRAC GUI 或 RACADM 可以擦除单个 PCIe SSD 或 SED 设备。有关更多信息，请参阅*擦除 PCIe SSD 设备数据*和*擦除 SED 设备数据*部分。

有关 Lifecycle Controller GUI 内的系统擦除功能，请参阅 *生命周期控制器用户指南，网址：*https://www.dell.com/idracmanuals。

擦除 SED/ISE 设备数据

注: 当支持的□□是“虚□磁□”的一部分□，不支持此操作。在□行□□擦除之前，必□从虚□磁□中移除目□支持□□。

“加密擦除”将永久擦除磁盘上现有的所有数据。在 SED/ISE 上执行加密擦除时，将覆盖所有数据块并导致受支持设备上的所有数据永久性丢失。在加密擦除过程中，主机无法访问此受支持的设备。SED/ISE 设备擦除可以实时执行，也可以在系统重新启动后进行应用。

如果系统在加密擦除期间重新引导或遇到断电，则该操作将被取消。您必须重新引导系统并重启此过程。

在擦除 SED/ISE 设备数据之前，请确保：

- 已启用 Lifecycle Controller。
- 您具有服务器控制权限和登录权限。
- 所选的受支持驱动器不是虚拟磁盘的一部分。

注:

- SED/ISE 擦除可以实时执行，也可以分阶段操作。
- 驱动器擦除后，可能会因数据高速缓存的原因，仍然在操作系统中显示为活动。如果发生这种情况，请重新启动操作系统，随后已擦除的驱动器将不再显示或报告任何数据。
- 热插拔 NVMe 磁盘不支持加密擦除操作。在开始操作之前重新启动服务器。如果操作仍然失败，请确保启用了 CSIOR，并且 NVMe 磁盘符合 Dell Technologies 的要求。

使用 Web 界面擦除 SED/ISE 设备数据

要擦除支持的设备上的数据，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**存储** > **概览** > **物理磁盘**。
   将显示**物理磁盘**页面。
2. 从**控制器**下拉菜单中，选择控制器以查看关联的设备。
3. 从下拉菜单中，对一个或多个 SED/ISE 选择**加密擦除**。
   如果您已选择**加密擦除**，并且要查看下拉菜单中的其他选项，请选择**操作**，然后单击下拉菜单以查看其他选项。
4. 从**应用操作模式**下拉菜单中，选择以下选项之一：
   - **立即应用** — 选择此选项可立即应用操作，而无需重新启动系统。
   - **在下次重新引导时** — 在下次系统引导期间选择此选项应用该操作。
   - **在计划的时间** — 选择此选项可在计划的日期和时间应用操作：
     - **开始时间**和**结束时间** — 单击日历图标并选择日期。从下拉菜单中，选择时间。操作将在开始时间和结束时间之间应用。
     - 从下拉菜单中，选择重新引导类型：
       - 不重新引导（手动重新引导系统）
       - 正常关机
       - 强制关机
       - 关闭系统电源后重启（冷引导）
5. 单击**应用**。
   如果未创建作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
   如果作业创建成功，将显示一条消息，指示为所选控制器创建了作业 ID。单击**作业队列**，可在作业队列页面中查看该作业的进度。
   如果未创建挂起操作，将显示一条错误消息。如果挂起操作成功，而作业创建未成功，则会显示一条错误消息。

使用 RACADM 擦除 SED 设备数据

要安全地擦除 SED 设备：

```
racadm storage cryptographicerase:<SED FQDD>
```

要在执行 `cryptographicerase` 命令后创建目标作业：

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -realtime
```

要在执行 cryptographicerase 命令后创建目标分阶段作业：

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -e <start_time>
```

要查询返回的作业 ID：

```
racadm jobqueue view -i <job ID>
```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

重建物理磁盘

重建物理磁盘功能可重新构建发生故障的磁盘中的内容。仅当自动重建选项设置为 false 这才可用。如果有冗余虚拟磁盘，重建操作可以重新构建为出现故障的物理磁盘的内容。可以在正常操作过程中进行重建，但会降低性能。

取消重建可用于取消正在进行的重建。如果取消重建，则虚拟磁盘保持在降级状态。另一个物理磁盘出现故障时可能会导致虚拟磁盘发生故障，并可能导致数据丢失。建议尽早在故障物理磁盘上执行重建。

如果您取消对已分配为热备用的物理磁盘的重建，按顺序在同一物理磁盘上执行重建以还原数据。取消物理磁盘重建，然后将另一个物理磁盘分配为热备用都不会导致新分配的热备用重建数据。

管理虚拟磁盘

可对虚拟磁盘执行以下操作：

- 创建
- 删除
- 编辑策略
- 初始化
- 检查一致性
- 取消检查一致性
- 加密虚拟磁盘
- 分配或取消分配专用热备用
- 闪烁和取消闪烁虚拟磁盘
- 取消后台初始化
- 联机容量扩展
- RAID 级别迁移

注： 您可以使用 iDRAC 界面管理和□□ 240 个虚□磁□。要□建虚□磁□，□使用□□□置 (F2)、PERCCLI 命令行工具或 Dell OpenManage Server Administrator (OMSA)。

注： PERC 10 □数低，因□它不支持菊花□排布。

创建虚拟磁盘

以实施 RAID 功能，您必须创建一个虚拟磁盘。虚拟磁盘是指 RAID 控制器使用一个或多个物理磁盘创建的存储。尽管虚拟磁盘可从多个物理磁盘创建，但其对操作系统显示为单个磁盘。

在创建虚拟磁盘前，您应该熟悉创建虚拟磁盘前的注意事项中的信息。

您可以使用连接到 PERC 控制器的物理磁盘创建虚拟磁盘。要创建虚拟磁盘，您必须具有服务器控制用户权限。您可以在同一个驱动器组中创建 64 个虚拟驱动器和 16 个虚拟驱动器。

如果出现以下情况，则您无法创建虚拟磁盘：

- 物理磁盘驱动器不可用于创建虚拟磁盘。安装附加的物理磁盘驱动器。
- 已达到可在控制器上创建的最大虚拟磁盘数。您必须删除至少一个虚拟磁盘，然后才能创建新的虚拟磁盘。
- 已达到驱动器组支持的最大虚拟磁盘数。您必须从选定的组中删除一个虚拟磁盘，然后才能创建新的虚拟磁盘。
- 一个作业当前正在运行或计划在所选控制器上运行。您必须等待此作业完成，或者您可以删除该作业，然后再尝试新操作。您可以查看和管理作业队列页面中计划的作业的状态。
- 物理磁盘处于非 RAID 模式。必须使用 iDRAC 界面（例如 iDRAC Web 界面、RACADM、WSMan）或 <CTRL+R> 将其转换为 RAID 模式。

注： 如果在“添加到挂起操作”模式下□建虚□磁□且未□建作□，如果之后□除□虚□磁□，□□□□虚□磁□的“□建挂起操作”将被清除。

注： PERC H330 不支持 RAID 6 和 60。

注： BOSS 控制器□允□您□建与全尺寸 M.2 物理存□介□相等的虚□磁□。使用服□器配置配置文件□建 BOSS 虚□磁□□，确保将虚□磁□大小□置□零。□于其他界面（如 RACADM、WSMan 和 Redfish），不□指定虚□磁□大小。

创建虚拟磁盘前的注意事项

创建虚拟磁盘之前，请考虑以下事项：

- 虚拟磁盘名称没有储存在控制器上 — 所创建虚拟磁盘的名称没有存储在控制器上。这意味着如果您使用另一种操作系统重新引导，新操作系统将会使用自己的命名惯例来重命名虚拟磁盘。
- 磁盘分组是连接到创建了一个或多个虚拟磁盘的 RAID 控制器的磁盘逻辑分组，磁盘组中的所有虚拟磁盘都使用磁盘组中的所有物理磁盘。当前的实施支持在创建逻辑设备期间屏蔽混合磁盘组。
- 物理磁盘绑定于磁盘组中。因此，在同一磁盘组中没有混合的 RAID 级别。
- 虚拟磁盘中可以包括的物理磁盘有数目限制。这些限制根据控制器而有所不同。创建虚拟磁盘时，控制器支持一定数目的条带和跨越（合并物理磁盘上存储空间的方法）。由于条带和跨越的总数目有限制，所以可以使用的物理磁盘的数目也有限制。对条带和跨越的限制将影响 RAID 级别，如下所示：
  - 跨接最大数影响 RAID 10、RAID 50 和 RAID 60。
  - 条带最大数影响 RAID 0、RAID 5、RAID 50、RAID 6 和 RAID 60。
  - 镜像中的物理磁盘数目总是 2。这会影响 RAID 1 和 RAID 10。

  注：
  - BOSS 控制器仅支持 RAID 1。
  - SWRAID 控制器仅支持 RAID 0、1、5 和 10。
- 无法在 PCIe SSD 上创建虚拟磁盘。但 PERC 11 和更高版本的控制器支持使用 PCIe SSD 创建虚拟磁盘。

使用 Web 界面创建虚拟磁盘

要创建虚拟磁盘，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**存储** > **概览** > **虚拟磁盘高级过滤器**。
2. 在**虚拟磁盘**部分中，执行以下操作：
   a. 从**控制器**下拉菜单中，选择您要为其创建虚拟磁盘的控制器。
   b. 从**布局**下拉菜单中，选择虚拟磁盘的 RAID 级别。
   只有受控制器支持的那些 RAID 级别才会显示在下拉菜单中，并且 RAID 级别的可用性将基于可用物理磁盘总数。
   c. 选择**介质类型**、**条带大小**、**读取策略**、**写入策略**和**磁盘高速缓存策略**、。
   只有受控制器支持的那些值才会显示在这些属性的下拉菜单中。
   d. 在**容量**字段中，键入虚拟磁盘的大小。
   在选中磁盘时，将显示并更新磁盘最大大小。
   e. 此时将根据所选的物理磁盘（步骤 3）显示**跨越计数**字段。您无法设置此值。在为多 RAID 级别选择磁盘后，系统会自动计算此值。**跨区数**字段仅适用于 RAID 10、RAID 50 和 RAID 60。如果您已选择 RAID 10 并且控制器支持非均匀 RAID 10，则不会显示跨越计数值。控制器将自动设置适当的值。对于 RAID 50 和 RAID 60，当使用最少数量的磁盘以创建 RAID 时，不会显示此字段。如果使用更多磁盘，则此信息可能会更改。
3. 在**选择物理磁盘**部分中，选择物理磁盘的数量。

有关各字段的更多信息，请参阅 *iDRAC 联机帮助*

4. 在**应用操作模式**下拉菜单中，选择要应用设置的时间。
5. 单击**创建虚拟磁盘**。

将根据选定的**应用操作模式**应用设置。

注: 可以在磁盘名称中使用字母数字字符、空格、连字符和下划线。

在创建虚拟磁盘时，您输入的任何其他特殊字符都将被移除并替换为空格。

使用 RACADM 创建虚拟磁盘

使用 `racadm storage createvd` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

注: 在 S140 控制器管理的驱动器上使用 RACADM，不支持磁盘分片或配置部分虚拟磁盘。

编辑虚拟磁盘高速缓存策略

您可以更改虚拟磁盘的读取、写入或磁盘高速缓存策略。

注: 某些控制器并不支持所有□取或写入策略。因此，在□用策略□将会□示一条□□消息。

读取策略将表示控制器在搜索数据时是否必须读取虚拟磁盘连续扇区：

- **自适应预读** - 仅当两个最新读取请求访问磁盘的顺序扇区时控制器才启动预读策略。如果后续的读取请求访问的是磁盘的随机扇区，则控制器将恢复为使用不预读策略。控制器将继续评估读取请求是否访问磁盘的连续扇区时，并启动预读（如有必要）。
- **预读** - 控制器在搜寻数据时读取虚拟磁盘的顺序扇区。如果将数据写入虚拟磁盘的顺序扇区，预读策略可以提高系统性能。
- **不预读** - 选择不预读策略表示控制器不应使用预读策略。

写策略指定控制器是否在数据一进入高速缓存或写入该磁盘后就发送写请求完成信号。

- **直写** - 只有在数据写入磁盘后控制器才发出写入请求完成信号。直写式高速缓存提供比回写式高速缓存更好的数据安全性，因为系统假设仅在安全写入磁盘后数据才可用。
- **回写** — 只要数据在控制器缓存中但尚未写入磁盘时，控制器即发送写入请求完成信号。回写式高速缓存可能会提供改善的性能，因为后续的读取请求可以从高速缓存然后从磁盘中快速检索数据。但是，在发生系统故障时可能会发生数据丢失，导致数据无法写入磁盘。当操作假设数据在磁盘上可用时，其他应用程序也可能会遇到问题。
- **强制回写** — 启用了写入高速缓存（不管控制器是否具有电池）。如果控制器无电池且已使用强制回写高速缓存，出现电源故障时，可能发生数据丢失。

磁盘高速缓存策略适用于特定虚拟磁盘上的读取。这些设置不影响预读策略。

注:

- 控制器的非易失性高速缓存和控制器高速缓存的备用电池将影响控制器可支持的读取策略或写入策略。所有 PERC 系统都不具有电池和高速缓存。
- 预读和回写需要高速缓存。因此，如果控制器没有高速缓存，则不允许您设置策略值。

  同样，如果 PERC 具有高速缓存但没有电池，并且策略设置为需要访问高速缓存，则如果基础系统关闭，将可能发生数据丢失。因此大多数 PERC 可能允许使用该策略。

  因此，将根据 PERC 设置策略值。

删除虚拟磁盘

删除虚拟磁盘会破坏虚拟磁盘上包括文件系统和卷在内的所有信息，并从控制器配置移除虚拟磁盘。在删除虚拟磁盘时，如果删除了与控制器关联的最后一个虚拟磁盘，则可能会自动取消分配所有已分配的全局热备用。删除磁盘组的最后一个虚拟磁盘时，所有已分配的专用热备用都自动变为全局热备用。

如果您删除全局热备用的所有虚拟磁盘，则全局热备用将被自动删除。

您必须具有登录权限和服务器控制权限才能删除虚拟磁盘。

允许此操作时，您可以删除引导虚拟驱动器。这通过边带完成并且独立于操作系统。因此，在删除虚拟驱动器之前会显示一个警告消息。

如果您删除一个虚拟磁盘并立即创建一个新的虚拟磁盘，并且所有特性与已删除的特性一样，那么控制器可识别数据，即使第一个虚拟磁盘数据从未删除。在这种情况下，如果您不想在重新创建新虚拟磁盘后使用旧数据，则重新初始化虚拟磁盘。

检查虚拟磁盘一致性

此操作验证冗余（奇偶校验）信息的准确性。此任务仅适用于冗余虚拟磁盘。如果需要，检查一致性任务可重建冗余数据。如果虚拟驱动器有已降级状态，运行检查一致性可能会使虚拟驱动器返回至就绪状态。您可以使用 Web 界面或 RACADM 执行一致性检查。

您还可以取消检查一致性操作。取消一致性检查的操作是实时操作。

您必须具有登录权限和服务器控制权限，才能检查虚拟磁盘的一致性。

注： 在 RAID0 模式中□置□□器□，不支持一致性□□。

注： 如果在没有□行一致性□□操作□□行取消一致性操作，□ GUI 中的挂起操作将□示□“取消 BGI”，而不是“取消一致性□□”。

初始化虚拟磁盘

初始化虚拟磁盘将擦除磁盘上的所有数据，但不会更改虚拟磁盘配置。您必须初始化配置的虚拟磁盘才能使用它。

注： 当□□重新□建□有配置□，□勿初始化虚□磁□。

可以执行快速初始化、完全初始化或取消初始化操作。

注： 取消初始化是□□操作。您可以使用 iDRAC Web 界面（而非 RACADM）取消初始化。

快速初始化

快速初始化操作会初始化虚拟磁盘中包括的所有物理磁盘。它可以更新物理磁盘上的元数据，以使所有磁盘空间可用于以后的写操作。初始化任务可快速完成，因为物理磁盘上现有的信息未被擦除，尽管以后的写操作会覆盖物理磁盘上保留的任何信息。

快速初始化仅删除引导扇区和条带信息。只有您受时间限制或者硬盘驱动器是新的或未使用的情况下，才可以执行快速初始化。快速初始化会需要较少的时间才能完成（通常是 30 - 60 秒）。

小心：执行快速初始化会导致现有数据无法访问。

快速初始化任务不会在物理磁盘的磁盘块上写入零。这是因为快速初始化任务不执行写操作，所以导致磁盘降级程度不高。

虚拟磁盘的快速初始化将覆盖虚拟磁盘上的第一个和最后一个 8 MB 区段，清除所有引导记录或分区信息。该操作仅需 2 至 3 秒即可完成，因此建议在重新创建虚拟磁盘时选择该操作。

后台初始化会在快速初始化完成后五分钟内启动。

完全或慢速初始化

完全初始化（又称慢速初始化）操作会初始化虚拟磁盘中包括的所有物理磁盘。它会更新物理磁盘上的元数据，并擦除所有现有数据和文件系统。您可以在创建虚拟磁盘后执行完全初始化。与快速初始化操作比较，如果发现物理磁盘有问题或怀疑有磁盘坏块，您可能需要使用完全初始化。完全初始化操作会重新映射坏块并将零写入所有磁盘块。

如果执行一个虚拟磁盘的完全初始化，则不需要后台初始化。完全初始化过程中，主机无法访问虚拟磁盘。如果系统在完全初始化过程中重新引导，则操作会终止，同时在虚拟磁盘上执行后台初始化流程。

它建议始终在先前包含数据的驱动器上执行完全初始化。完全初始化过程中最多可能需要 1 - 2 分钟/GB 初始化的速度取决于控制器硬盘驱动器型号、速度和固件版本。

完全初始化任务一次将初始化一个物理磁盘。

注： 完全初始化仅实时支持。只有少数控制器支持完全初始化。

加密虚拟磁盘

在控制器上已禁用加密时（即删除安全保护密钥），可以使用 SED 驱动器为创建的虚拟磁盘手动启用加密。如果在控制器上启用加密后创建虚拟磁盘，则虚拟磁盘会自动加密。它会自动配置为加密虚拟磁盘，除非在虚拟磁盘创建过程中已禁用所启用的加密选项。

您必须具有登录权限和服务器控制权限才能管理加密密钥。

注： 尽管在控制器中已启用加密，□用□需要手□启用 VD 上的加密（如果 VD 是从 iDRAC □建）。只有在从 OMSA □建 VD □，它会自□加密。

分配或取消分配专用热备用

专用热备用是一个已分配给一个虚拟磁盘的未使用备份磁盘。如果虚拟磁盘中的某个物理磁盘发生故障，热备用就会激活以更换故障物理磁盘，而不用中断系统或需要用户干预。

您必须具有登录权限和服务器控制权限才能运行此操作。

只能向 4K 虚拟磁盘分配 4K 驱动器以作为热备用。

如果您在添加到待处理模式中分配了物理磁盘作为专用热备用，则会创建待处理操作，但不会创建作业。然后，如果您尝试取消分配专用热备用，则分配专用热备用待处理操作将被清除。

如果您在添加到待处理模式中取消分配了物理磁盘作为专用热备用，则会创建待处理操作，但不会创建作业。然后，如果您尝试分配专用热备用，则取消分配专用热备用待处理操作将被清除。

注： 日志□出操作正在□行□，您将无法在 **Manage Virtual Disks（管理虚拟磁盘）**□面上□看有关□用□□用的信息。日志□出操作完成后，重新加□或刷新 **Manage Virtual Disks（管理虚拟磁盘）**□面以□看信息。

重命名 VD

要更改虚拟磁盘的名称，用户必须具有系统控制权限。虚拟磁盘名称只能包含字母数字字符、空格、连字符和下划线。名称的最大长度取决于单独的控制器。在大多数情况下，最大长度为 15 个字符。此名称不能以空格开始或结尾或保持空白。每次重命名虚拟磁盘时，都将创建 LC 日志。

编辑磁盘容量

通过联机容量扩展 (OCE)，您可以在系统仍处于联机状态时增加所选 RAID 级别的存储容量。控制器重新分布阵列上的数据（称为重新配置），从而将新的可用空间放置在每个 RAID 阵列的末端。

联机容量扩展 (OCE) 可通过两种方法实现：

- 如果启动虚拟磁盘的 LBA 后虚拟磁盘组上最小的物理驱动器中有可用空间，那么可以在该可用空间内扩展虚拟磁盘的容量。此选项允许您输入新增加的虚拟磁盘的大小。如果虚拟磁盘中的磁盘组只有在开始 LBA 之前才有可用空间，那么即便物理驱动器上有可用空间，也不允许在同一磁盘组中“编辑磁盘容量”。
- 也可通过在现有的虚拟磁盘组中添加额外的兼容物理磁盘，扩展虚拟磁盘的容量。此选项不允许您输入新增加的虚拟磁盘的大小。根据特定虚拟磁盘上现有物理磁盘组的已用磁盘空间、虚拟磁盘的现有 RAID 级别和添加到虚拟磁盘的新驱动器数量，计算新增加的虚拟磁盘大小并将其显示给用户。

容量扩展允许用户指定最终的 VD 大小。内部最终的 VD 大小以百分比的方式传递给 PERC（此百分比是用户打算从阵列中剩余的空白空间用于本地磁盘扩展的百分比）。由于这个百分比逻辑，在重新配置完成后，最终的 VD 大小可能不同于用户在方案中提供的大小，在方案中用户没有提供最大的 VD 大小作为最终的 VD 大小（百分比小于 100%）。如果用户输入了可能的最大 VD 大小，那么在重新配置后，用户不会看到输入的 VD 大小与最终 VD 大小之间有差异。

Raid 级别迁移

RAID 级别迁移 (RLM) 是指更改虚拟磁盘的 RAID 级别。iDRAC9 提供了使用 RLM 增加虚拟磁盘大小的选项。在某种程度上，RLM 允许迁移虚拟磁盘的 RAID 级别，这反过来又可能增加虚拟磁盘的大小。

RAID 级别迁移是将虚拟磁盘的某一个 RAID 级别转换为另一个级别的过程。当您将虚拟磁盘迁移到不同的 Raid 级别时，其上的用户数据将重新分配为新配置的格式。

分阶段和实时均支持此配置。

下表介绍了在添加磁盘和未添加磁盘的情况下重新配置 (RLM) 虚拟磁盘时可能的可重新配置的虚拟磁盘布局。

表. 54: 可能的虚拟磁盘布局

源虚拟磁盘布局	在添加磁盘的情况下可能的目标虚拟磁盘布局	在未添加磁盘的情况下可能的目标虚拟磁盘布局
R0（单个磁盘）	R1	不适用
R0	R5/R6	不适用
R1	R0/R5/R6	R0
R5	R0/R6	R0
R6	R0/R5	R0/R5

当 OCE 或 RLM 正在进行时允许的操作

当 OCE/RLM 正在进行时，允许执行以下操作：

表. 55: 允许的操作

从虚拟磁盘在后台进行 OCE/RLM 的控制器端	从虚拟磁盘端（正在进行 OCE/RLM）	从同一控制器上的任何其他就绪状态物理磁盘	从同一控制器上的任何其他虚拟磁盘端（未进行 OCE/RLM）
重设配置	删除	闪烁	删除
导出日志	闪烁	取消闪烁	闪烁
设置巡检读取模式	取消闪烁	分配全局热备用	取消闪烁
启动巡检读取		转换为非 RAID 磁盘	重命名
更改控制器属性			更改策略
管理物理磁盘电源			慢速初始化
转换为 RAID 型磁盘			快速初始化
转换为非 RAID 磁盘			更换成员磁盘
更改控制器模式			

OCE 和 RLM 限制

以下是通用的 OCE 和 RLM 限制：

- OCE/RLM 限制为磁盘组中仅包含一个 VD 的情况。
- RAID50 和 RAID60 不支持 OCE。RAID10、RAID50 和 RAID60 不支持 RLM。
- 如果控制器包含的虚拟磁盘数量已达最大值，则无法对任何虚拟磁盘进行 RAID 级别迁移或容量扩展。
- 控制器将所有正在进行 RLM/OCE 的虚拟磁盘的写入高速缓存策略更改为直写，直到 RLM/OCE 完成。
- 重新配置虚拟磁盘通常会影响磁盘性能，直至重新配置操作完成。
- 磁盘组中物理磁盘的总数不能超过 32 个。
- 如果任何后台操作（如 BGI/重建/回写/巡检读取）已在相应的 VD/PD 上运行，则不允许在这时重新配置 (OCE/RLM)。
- 在与 VD 关联的驱动器上正在执行重新配置 (OCE/RLM) 时执行任何类型的磁盘迁移 (OCE/RLM) 都会导致重新配置失败。
- 重建完成后，任何为 OCE/RLM 新添加的驱动器都将成为虚拟磁盘的一部分。但这些新驱动器的状态会在重建开始后更改为“Online”（联机）。

取消初始化

此功能能够取消虚拟磁盘上的后台初始化。在 PERC 控制器上，冗余虚拟磁盘的后台初始化操作在虚拟磁盘创建后自动启动。冗余虚拟磁盘的后台初始化会准备虚拟磁盘，以保存奇偶校验信息并提高写入性能。但是，后台初始化正在进行时，创建虚拟磁盘等某些过程无法运行。取消初始化能够手动取消后台初始化。一旦取消，后台初始化会在 0 到 5 分钟内自动重新启动。

注: 后台初始化不适用于 RAID 0 虚拟磁盘。

使用 Web 界面管理虚拟磁盘

1. 在 iDRAC Web 界面中，转至**配置** > **存储配置** > **虚拟磁盘配置**。
2. 从**虚拟磁盘**中，选择您想要为其管理虚拟磁盘的控制器。
3. 从**操作**下拉菜单中，选择一个操作。

   当您选择某个操作时，将显示一个附加的**操作**窗口。选择/输入所需的值。
   - **重命名**
   - **删除**
   - **编辑高速缓存策略** - 您可以更改以下选项的高速缓存策略：
     - **读取策略** - 以下值可供选择：
       - **自适应预读** - 表示对于给定的卷，如果在连续的扇区中出现两个最新的磁盘访问，则控件可使用预先读取高速缓存策略。如果读取请求为随机，则该控制器返回至无预先读取模式。
       - **不预读** — 表示对于给定的卷，不采用不预读策略。
       - **预读** - 表示对于给定的卷，控制器按顺序读取请求的数据之前的数据并将附加的数据存储在高速缓存内存中，预计数据要求。这样可加快读取连续的数据，但访问随机数据时，速度提高不明显。
     - **写入策略** — 将写高速缓存策略更改为以下选项之一：
       - **直写** - 表示对于给定的卷，磁盘子系统收到交易中的所有数据后，控制器将数据传输完成的信号发送至主机系统。
       - **回写** - 表示对于给定的卷，控制器高速缓存收到交易中的所有数据后，控制器将数据传输完成的信号发送至主机系统。然后控制器将高速缓存的数据写入至后台的存储设备。
       - **强制回写** - 使用强制回写高速缓存时，启用了写入高速缓存（不管控制器是否具有电池）。如果控制器无电池且已使用强制回写高速缓存，出现电源故障时，可能发生数据丢失。
     - **磁盘高速缓存策略** — 将磁盘高速缓存策略更改为以下选项之一：
       - **默认值** - 表示磁盘正在使用其默认写入高速缓存模式。对于 SATA 磁盘，此模式已启用；对于 SAS 磁盘，此模式已禁用。
       - **已启用** - 表示磁盘的写入高速缓存已启用。如果断电，则会增加数据丢失的性能和概率。
       - **已禁用** - 表示磁盘的写入高速缓存已禁用。会降低数据丢失的性能和概率。
   - **编辑磁盘容量** - 您可以在此窗口中将物理磁盘添加至所选虚拟磁盘。此窗口还显示虚拟磁盘在添加物理磁盘后的当前容量和新容量。
   - **RAID 级别迁移** - 显示磁盘名称、当前 RAID 级别和虚拟磁盘大小。允许您选择一个新的 RAID 级别。用户必须向现有虚拟磁盘添加更多驱动器才能迁移到新的 RAID 级别。此功能不适用于 RAID 10、50 和 60。
   - **初始化：快速** - 更新物理磁盘上的元数据，以使所有磁盘空间可用于以后的写操作。初始化可以快速完成，因为虽然以后的写操作会覆盖物理磁盘上保留的任何信息，但是物理磁盘上的现有信息并不会擦除。
   - **初始化：完全** - 擦除现有的全部数据和文件系统。

     注: **初始化：完全**选项不适用于 PERC H330 控制器。
   - **检查一致性** - 要检查虚拟磁盘的一致性，从相应的下拉菜单中选择**检查一致性**。

     注: 驱动器设置为 RAID0 模式时不支持一致性检查。

   有关这些选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击**立即应用**可以立即应用更改，单击**在下次重新启动时**可以在下次重新启动时应用更改，单击**在计划的时间**可以在特定时间应用更改，并且单击**放弃所有待定更改**可以放弃更改。

   将根据选定的操作模式应用这些设置。

使用 RACADM 管理虚拟磁盘

可使用以下命令管理虚拟磁盘：

- 要删除虚拟磁盘：

```
racadm storage deletevd:<VD FQDD>
```

- 要初始化虚拟磁盘：

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

- 要检查虚拟磁盘的一致性（RAID0 上不支持）：

```
racadm storage ccheck:<vdisk fqdd>
```

要取消一致性检查：

```
racadm storage cancelcheck: <vdisks fqdd>
```

- 要加密虚拟磁盘：

```
racadm storage encryptvd:<VD FQDD>
```

- 要分配或取消分配专用热备件：

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD
of VD>
```

<option>=yes
分配热备件

<Option>=no
取消分配热备件

RAID 配置功能

下表列出了可在 RACADM 和 WSMan 中使用的一些 RAID 配置功能：

小心：强制让物理磁盘进入联机或脱机状态可能导致数据丢失。

表. 56: RAID 配置功能

功能部件	RACADM 命令	说明
强制联机	`racadm storage forceonline:<PD FQDD>`	电源故障、损坏的数据或某些其他原因可能会导致物理磁盘进入脱机状态。用尽了所有其他选项时，您可以使用此功能来强制物理磁盘回到联机状态。一旦运行了该命令，控制器就会将驱动器重置回联机状态，并还原其在虚拟磁盘中的成员资格。仅当控制器可以从驱动器中读取并可写入其元数据时，才会出现这种情况。
注： 仅当磁盘的损坏部分有限时，才能进行数据恢复。强制联机功能无法修复已发生故障的磁盘。		
强制脱机	`racadm storage forceoffline:<PD FQDD>`	此功能会从虚拟磁盘配置中删除驱动器，使它进入脱机状态，从而导致降级的虚拟磁盘配置。如果某个驱动器近期很可能会发生故障或者报告 SMART 故障但它仍然处于联机状态，则此功能非常有用。如果您要利用属于现有 RAID 配置的一部分的驱动器，也可以使用此功能。
更换物理磁盘	`racadm storage replacephysicaldisk:<Source PD FQDD > -dstpd <Destination PD FQDD>`	可让您将数据从属于虚拟磁盘成员的物理磁盘复制到另一个物理磁盘。源磁盘应处于“联机”状态，而目标磁盘应该处于“就绪”状态并且大小和类型类似，以替换源磁盘。

表. 56: RAID 配置功能 （续）

功能部件	RACADM 命令	说明
虚拟磁盘作为启动设备	`racadm storage setbootvd:<controller FQDD> -vd <VirtualDisk FQDD>`	可以使用此功能将虚拟磁盘配置为启动设备。当选择具有冗余的虚拟磁盘作为引导设备并且其上安装了操作系统时，这可实现容错功能。
解锁外部配置	`racadm storage unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>`	此功能将用于验证源控制器与目标控制器的加密方式不同的锁定驱动器的身份。解除锁定后，可成功地将驱动器从一个控制器迁移到另一个驱动器。

管理控制器

可以为控制器执行以下操作：

- 配置控制器属性
- 导入或自动导入外部配置
- 清除外部配置
- 重设控制器配置
- 创建、更改或删除安全密钥
- 丢弃保留的高速缓存

配置控制器属性

对于控制器，可配置以下属性：

- 巡检读取模式（自动或手动）
- 启动或停止巡检读取（如果巡检读取模式为手动模式）
- 巡检读取未配置区域
- 检查一致性模式
- 回写模式
- 负载平衡模式
- 检查一致性率
- 重建率
- 后台初始化 (BGI) 率
- 重构率
- 增强的自动导入外部配置
- 创建或更改安全密钥
- 加密模式（本地密钥管理和安全企业密钥管理器）

您必须有登录权限和服务器控制权限才能配置控制器属性。

巡检读取模式注意事项

巡检读取会识别磁盘错误以避免磁盘故障、数据丢失或损坏。它每周会在 SAS 和 SATA HDD 上自动运行一次。

巡检读取不会在处于以下情况的物理磁盘上运行：

- 物理磁盘为 SSD。
- 物理磁盘没有包括在虚拟磁盘中或分配为热备份。

- 物理磁盘包括在正在执行以下一项操作的虚拟磁盘中：
  - 重建
  - 重新配置或重新构建
  - 后台初始化
  - 检查一致性

此外，巡检读取操作会在频繁输入/输出活动期间暂挂，并在输入/输出操作完成后恢复。

注： 有关在“自动”模式下巡检读取操作的运行频率的更多信息，请参阅相应的控制器说明文件。

注： 如果控制器中的虚拟磁盘不可用，则不支持**启动**和**停止**等巡检读取模式操作。即使您可以使用 iDRAC 界面成功调用操作，在启动关联的作业时操作也会失败。

负载平衡

负载平衡属性能够自动使用连接到同一机柜的两个控制器端口或连接器发送 I/O 请求。此属性仅在 SAS 控制器上可用。

后台初始化 (BGI) 率

注： H330 和 H345 都需要加载驱动程序才能运行后台初始化操作。

在 PERC 控制器上，冗余虚拟磁盘的后台初始化将在虚拟磁盘创建后 0 到 5 分钟内自动开始。冗余虚拟磁盘的后台初始化会使虚拟磁盘做好准备，以维持冗余数据并提高写入性能。例如，RAID 5 虚拟磁盘的后台初始化操作完成后，奇偶校验信息已初始化。RAID 1 虚拟磁盘的后台初始化操作完成后，物理磁盘将被镜像。

后台初始化过程可帮助控制器识别和纠正冗余数据今后可能发生的问题。在这方面，后台初始化过程与检查一致性过程类似。应允许后台初始化运行才能完成该过程。如果取消，后台初始化会在 0 到 5 分钟内自动重新启动。当后台初始化正在运行时，可能发生某些过程（例如读取和写入操作）。其他过程（例如创建虚拟磁盘）将无法与后台初始化同时运行。这些过程会导致后台初始化取消。

后台初始化率可配置为 0% 到 100%，代表专用于运行后台初始化任务的系统资源的百分比。显示为 0% 时，对于控制器，后台初始化具有最低优先级，需要较长的时间才能完成，并且是对系统性能影响最小的设置。后台初始化率为 0% 不表示后台初始化已停止或暂停。显示为 100% 时，对于控制器，后台初始化具有最高优先级。后台初始化时间较短，并且是对系统性能影响最大的设置。

检查一致性

检查一致性任务可验证冗余（奇偶校验）信息的准确性。此任务仅适用于冗余虚拟磁盘。如果需要，检查一致性任务可重建冗余数据。当虚拟磁盘处于“失败的冗余”状态时，运行检查一致性可能让虚拟磁盘返回到就绪状态。

检查一致性率可配置为 0% 到 100%，代表专用于运行检查一致性任务的系统资源的百分比。显示为 0% 时，对于控制器，检查一致性具有最低优先级，需要较长的时间才能完成，并且是对系统性能影响最小的设置。检查一致性率为 0% 不表示检查一致性已停止或暂停。显示为 100% 时，对于控制器，检查一致性具有最高优先级。检查一致性时间较短，并且是对系统性能影响最大的设置。

创建或更改安全密钥

配置控制器属性时，您可以创建或更改安全密钥。控制器使用加密密钥来锁定或解锁对 SED 的访问。您只可以为每个具有加密功能的控制器创建一个加密密钥。使用以下功能来管理安全密钥：

1. **本地密钥管理 (LKM) 系统** - LKM 可用于生成保护虚拟磁盘所需的密钥 ID 和密码或密钥。如果使用 LKM，则必须通过提供加密密钥标识符和密码短语来创建加密密钥。
2. **安全企业密钥管理器 (SEKM)** - 此功能可用于使用密钥管理服务器 (KMS) 生成密钥。如果您使用的是 SEKM，则必须用 KMS 信息以及与 SSL 相关的配置对 iDRAC 进行配置。

注：

- 在 eHBA 模式下运行的 PERC 硬件控制器上不支持此任务。
- 如果您在“添加到挂起操作”模式下创建安全密钥且未创建任务，并且之后如果删除该安全密钥，则会清除创建安全密钥挂起操作。

注：

- 要启用 SEKM，请确保安装了受支持的 PERC 固件。
- 如果您启用 SEKM，则无法将 PERC 固件降级到先前的版本。相同系统中未处于 SEKM 模式的其他 PERC 控制器固件的降级也可能失败。要将未处于 SEKM 模式的 PERC 控制器的固件降级，您可以使用 OS DUP 更新方法，或在控制器上禁用 SEKM，然后重新尝试从 iDRAC 降级。

注: 将热插拔锁定卷从一台服务器导入另一台服务器时，您将在 LC 日志中看到正在应用的控制器属性的 CTL 条目。

使用 Web 界面配置控制器属性

1. 在 iDRAC Web 界面中，转至 **Storage（存储）** > **Overview（概览）** > **Controllers（控制器）**。
   此时会显示**设置控制器**页面。
2. 在 **Controller（控制器）**部分中，选择您想要配置的控制器。
3. 为各个属性指定所需的信息。
   Current Value（当前值）列将显示每个属性现有的值。您可以通过从每个属性的 **Action（操作）**下拉菜单中选择选项修改该值。
   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 在 **Apply Operation Mode（应用操作模式）**下拉菜单中，选择要应用设置的时间。
5. 单击**应用**。
   将根据选定的操作模式应用这些设置。

使用 RACADM 配置控制器属性

- 要设置巡检读取模式：

```
racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
```

- 如果巡检读取模式已设置为手动，请使用以下命令来启动和停止巡检读取模式：

```
racadm storage patrolread:<Controller FQDD> -state {start|stop}
```

  注: 如果控制器中的虚拟磁盘不可用，则不支持“启动”和“停止”等巡检读取模式操作。即使您可以使用 iDRAC 界面成功调用操作，当关联的作业已启动时操作也将失败。
- 要指定一致性检查模式，请使用 **Storage.Controller.CheckConsistencyMode** 对象。
- 要启用或禁用回写模式，请使用 **Storage.Controller.CopybackMode** 对象。
- 要启用或禁用负载平衡模式，请使用 **Storage.Controller.PossibleloadBalancedMode** 对象。
- 要指定专用于对虚拟冗余磁盘执行一致性检查的系统资源百分比，请使用 **Storage.Controller.CheckConsistencyRate** 对象。
- 要指定专用于重建故障磁盘的控制器资源百分比，请使用 **Storage.Controller.RebuildRate** 对象
- 要指定专用于在创建虚拟磁盘后对其执行后台初始化 (BGI) 的控制器资源百分比，请使用 **Storage.Controller.BackgroundInitializationRate** 对象
- 要指定专用于在添加物理磁盘或更改磁盘组上虚拟磁盘的 RAID 级别后重构磁盘组的控制器资源百分比，请使用 **Storage.Controller.ReconstructRate** 对象。
- 要为控制器启用或禁用增强的外部配置自动导入功能，请使用 **Storage.Controller.EnhancedAutoImportForeignConfig** 对象
- 要创建、修改或删除安全密钥以加密虚拟驱动器，请使用以下命令：

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd <passphrase>
racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd <old
passphrase> -newpasswd <new passphrase>
racadm storage deletesecuritykey:<Controller FQDD>
```

导入或自动导入外部配置

外部配置是驻留在从一个控制器移到另一个控制器的物理磁盘上的数据。已移动的驻留在物理磁盘上的虚拟磁盘被视为外部配置。

您可以导入外部配置，以便在物理磁盘移动后不会丢失虚拟磁盘。仅当外部配置中包含处于“就绪”或“降级”状态的虚拟磁盘，或包含专用于可导入或已存在的虚拟磁盘的热备用时，才能导入该外部配置。

所有虚拟磁盘数据必须存在，但如果虚拟磁盘正在使用冗余 RAID 级别，则不需要额外的冗余数据。

例如，如果外部配置中只包含 RAID 1 虚拟磁盘中的镜像的一端，那么虚拟磁盘处于降级状态并且可以导入。如果外部配置仅包含一个最初使用三个物理磁盘配置为 RAID 5 的物理磁盘，那么该 RAID 5 虚拟磁盘处于故障状态且不能导入。

除虚拟磁盘外，外部配置还可能包含在一个控制器上分配为热备用然后移至另一个控制器的物理磁盘。导入外部配置任务可将新物理磁盘作为热备用导入。如果该物理磁盘在以前的控制器上设置为专用热备用，但热备用所分配到的虚拟磁盘在外部配置中不再存在，则会将该物理磁盘作为全局热备用导入。

如果检测到使用本地密钥管理器 (LKM) 锁定的任何外部配置，则在此版本的 iDRAC 中，导入外部配置操作不可用。您必须通过 CTRL-R 解锁驱动器，然后继续从 iDRAC 导入外部配置。

仅当控制器检测到的外部配置时，才会显示导入外部配置任务。您也可以通过检查物理磁盘状态识别物理磁盘中是否包含外部配置（虚拟磁盘或热备用）。如果物理磁盘状态为外部，则物理磁盘包含所有或部分虚拟磁盘或分配了热备用。

注: □入外部配置任□会□入添加到控制器的物理磁□上□留的所有虚□磁□。如果存在多个外部虚□磁□，□□入所有配置。

PERC9 控制器支持自动导入外部配置，无需用户交互。自动导入可以启用或禁用。如果已启用，PERC 控制器可自动导入检测到的任何外部配置，而无需手动干预。如果已禁用，则 PERC 不会自动导入任何外部配置。

您必须具有登录权限和服务器控制权限才能导入外部配置。

在 HBA 模式下运行的 PERC 硬件控制器上不支持该任务。

注: 系□上的操作系□正在运行□，不建□移除外部机柜□□。在重新建立□接□移除□□可能会□生外部配置。

可管理以下情况中的外部配置：

- 配置中的所有物理磁盘都已卸下并重新插入。
- 配置中的部分物理磁盘已卸下并重新插入。
- 虚拟磁盘中的所有物理磁盘在不同的时间卸下，然后重新插入。
- 非冗余虚拟磁盘中的物理磁盘已卸下。

以下限制适用于待导入的物理磁盘：

- 从扫描外部配置到实际导入期间，物理磁盘的驱动器状态可能发生改变。只有在处于“Unconfigured Good”（未配置，良好）状态时，驱动器上才能进行外部导入。
- 无法导入出现故障或处于脱机状态的驱动器。
- 固件不允许导入超过八个的外部配置。

使用 Web 界面导入外部配置

注: 如果系统中存在不完整的外部磁盘配置，则一个或多个现有联机虚拟磁盘的状态也会显示为外来状态。

注: 不支持导入 BOSS 控制器的外部配置。

要导入外部配置，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **存储配置**。
2. 从**控制器**下拉菜单中，选择您要为其导入外部配置的控制器。
3. 单击**外部配置**下的**导入**，然后单击**应用**。

使用 RACADM 导入外部配置

要导入外部配置，请执行以下操作：

```
racadm storage importconfig:<Controller FQDD>
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

清除外部配置

将物理磁盘从一个控制器移动到另一个后，您可能会发现包含所有或部分虚拟磁盘的物理磁盘（外部配置）。您可以通过检查物理磁盘的状态识别以前使用的物理磁盘是否包含外部配置（虚拟磁盘）。如果物理磁盘状态为外部，则物理磁盘包含所有或部分虚拟磁盘。您可以从新连接的物理磁盘中清除或擦除虚拟磁盘信息。

清除外部配置操作将永久擦除驻留在添加到控制器的的物理磁盘上的所有数据。如果存在多个外部虚拟磁盘，则所有配置均将被擦除。您可能更希望导入虚拟磁盘而非破坏数据。卸下外部数据时必须执行初始化。如果遇到无法导入的不完整外部配置，可以使用清除外部配置选项来擦除物理磁盘上的外部数据。

使用 Web 界面中清除外部配置

要清除外部配置，其执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **存储配置** > **控制器配置**。
   此时会显示**控制器配置**页面。
2. 从**控制器**下拉菜单中，选择您要为其清除外部配置的控制器。

   注: 要清除 BOSS 控制器上外部配置，请单击“重设配置”。

3. 单击**清除配置**。
4. 单击**应用**。
   将根据选定的操作模式擦除物理磁盘上的虚拟磁盘。

使用 RACADM 清除外部配置

要清除外部配置：

```
racadm storage clearconfig:<Controller FQDD>
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

重设控制器配置

您可以重设控制器配置。此操作将删除虚拟磁盘驱动器，并取消所有控制器上热备用。它不会从配置中擦除移除磁盘之外的任何数据。重设配置不会删除任何外部配置。对此功能的实时支持仅适用于 PERC 9.1 固件。重设配置不会擦除任何数据。可以重新创建完全相同的配置而不执行初始化操作，初始化操作可能会导致数据被恢复。您必须具有服务器控制权限。

注: 重□控制器配置不会□除外部配置。要□除外部配置，□□行清除配置操作。

使用 Web 界面重设控制器配置

要重设控制器配置：

1. 在 iDRAC Web 界面中，转至 **Storage（存储）** > **Overview（概览）** > **Controllers（控制器）**。
2. 从 **Actions（操作）** 下拉菜单中，为一个或多个控制器选择 **Reset Configuration（重设配置）**。
3. 对于每个控制器，在**应用操作模式**下拉菜单中，选择要应用设置的时间。
4. 单击**应用**。

将根据选定的操作模式应用这些设置。

使用 RACADM 重设控制器配置

要重设控制器配置：

```
racadm storage resetconfig:<Controller FQDD>
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

切换控制器模式

在 PERC 9.1 和更高版本的控制器上，可通过将模式从 RAID 切换到 HBA 来更改控制器的特征。此控制器的操作与 HBA 控制器相似，即驱动程序通过操作系统传递。控制器模式更改是一个分阶段的选项，不能实时更改。

PERC 10 及更高版本的控制器支持增强型 HBA 模式，取代了当前控制器模式选项中的 HBA。但是，PERC 9 仍然继续支持 HBA 模式。

注：
- 增强型 HBA 支持非 RAID PD 和所有 RAID 级别 VD。
- 它只能支持创建 RAID0、RAID1 和 RAID10 VD。
- 增强型 HBA 在 PERC 11 上不受支持。

增强的 HBA 模式提供以下功能：
- 使用 RAID 级别 0、1 或 10 创建虚拟磁盘。
- 向主机显示非 RAID 磁盘。
- 将虚拟磁盘的默认高速缓存策略配置为带预读的回写。
- 将虚拟磁盘和非 RAID 磁盘配置为有效的引导设备。
- 自动将所有未配置的磁盘转换为非 RAID：
  - 在系统启动时
  - 在控制器重设时
  - 当热插入未配置的磁盘时

注： 不支持□建或□入 RAID 5、6、50 或 60 虚□磁□。另外，在增强型 HBA 模式下，先以升序排序枚□非 RAID 磁□，再以降序□序枚□ RAID 卷。

在将控制器的模式从 RAID 更改为 HBA 之前，请确保：
- RAID 控制器支持控制器模式更改。在 RAID 特征需要许可证的控制器上，没有更改控制器模式的选项。
- 必须删除或移除所有虚拟磁盘。
- 必须删除或移除热备用。
- 必须删除或清除外部配置。
- 必须移除所有处于故障状态的物理磁盘，或者需要清除固定高速缓存。
- 必须删除任何与 SED 关联的本地安全密钥。
- 控制器不能有保留的高速缓存。
- 您拥有切换控制器模式的服务器控制权限。

注： □确保在切□模式之前先□份外部配置、安全密□、虚□磁□和□□用，因□□些数据将被□除。

注： □确保在更改控制器模式之前，□ PERC FD33xS 和 FD33xD 存□底座提供 CMC □可□（不适用于 MX 平台）。有关存□底座 CMC □可□的更多信息，□参□ dell.com/cmcmanuals 上提供的*适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller 版本 1.2 用户指南*。

切换控制器模式时的例外

以下列表提供使用 iDRAC 界面（例如 Web 界面、RACADM 和 WSMan）设置控制器模式时的例外：
- 如果 PERC 控制器处于 RAID 模式，则必须先清除所有虚拟磁盘、热备用、外部配置、控制器密钥或保留的高速缓存，然后再将该模式更改为 HBA 模式。

- 设置控制器模式时，不能配置其他 RAID 操作。例如，如果 PERC 处于 RAID 模式，且将 PERC 的待定值设置为 HBA 模式，而您尝试设置 BGI 属性，则此待定值不会启动。
- 将 PERC 控制器从 HBA 切换到 RAID 模式时，驱动器仍处于非 RAID 状态，而且不会自动设置为“就绪”状态。此外，**RAIDEnhancedAutoImportForeignConfig** 属性会自动设置为 **Enabled（已启用）**。

以下列表提供使用服务器配置文件功能通过 WSMan 或 RACADM 界面设置控制器模式时的例外：

- 服务器配置文件功能允许您在设置控制器模式时配置多个 RAID 操作。例如，，如果 PERC 控制器处于 HBA 模式，您可以编辑导出服务器配置文件 (SCP) 以将控制器模式更改为 RAID，将设备转换为就绪并创建虚拟磁盘。
- 从模式从 RAID 更改为 HBA 时，**RAIDaction pseudo** 属性将设置为更新 9 默认行为）。发生故障时属性将运行并创建一个虚拟磁盘。控制器模式将更改，但是，作业已完成时会提示有错误。要避免此问题，您必须在 SCP 文件中注释 RAIDaction 属性。
- 当 PERC 控制器处于 HBA 模式时，如果对编辑为将控制器模式更改为 RAID 的导出 SCP 运行导入预览，并尝试创建 VD，则创建虚拟磁盘会失败。导入预览不支持验证更改控制器模式的堆栈 RAID 操作。

使用 iDRAC Web 界面切换控制器模式

要切换控制器模式，请执行以下步骤：

1. 在 iDRAC Web 界面中，单击**存储** > **概览** > **控制器**。
2. 在**控制器**页面上，单击**操作** > **编辑**。
   当前值列将显示控制器的当前设置。
3. 从下拉菜单中选择要切换到的控制器模式，然后单击**下次重新引导时**。
   重新引导系统以使更改生效。

使用 RACADM 切换控制器模式

要使用 RACADM 切换控制器模式，运行下列命令。

- 要查看控制器当前模式：

```
$ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
```

  系统将显示以下输出：

```
RequestedControllerMode = NONE
```

- 要将控制器模式设置为 HBA：

```
$ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
```

- 要创建一个作业并应用更改：

```
$ racadm jobqueue create <Controller Instance ID> -s TIME_NOW -r pwrcycle
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC RACADM 命令行界面参考指南）。

12Gbps SAS HBA 适配器操作

Dell PowerEdge 服务器必须安装操作系统并加载正确的设备驱动程序，以便 Dell HBA 运行。POST 完成后，HBA 端口将被禁用。HBA 设备驱动程序负责重置 HBA 并允许其端口连接到存储设备。如果没有操作系统，将不会加载驱动程序，并且无法保证 iDRAC 能够显示连接到 Dell HBA 的存储设备。

非 RAID 控制器是具有较少 RAID 功能的 HBA。它们不支持虚拟磁盘。

14G iDRAC 界面支持 12 Gbps SAS HBA 控制器、HBA330（集成和适配器）控制器、HBA330 MMZ 和 HBA330 MX 适配器。

AMD 平台支持 HBA355i 前端和 HBA355i 适配器控制器。

可为非 RAID 控制器执行下列操作：

- 查看适用于非 RAID 控制器的控制器、物理磁盘和机柜属性。此外，查看与机柜关联的 EMM、风扇、电源设备和温度探测器属性。将根据控制器类型显示属性。
- 查看硬件和软件的资源清册信息。
- 为 12 Gbps SAS HBA 控制器后的机柜更新固件（分阶段方式）

- 在检测到更改时，监测物理磁盘 SMART 触发状态的轮询操作或轮询频率
- 监测物理磁盘的热插拔或热卸除状态
- 闪烁或取消闪烁 LED

注：
- 磁带机连接到 12gbps SAS 或 HBA355e 后，其可获得有限的支持。
- 即使 LED 指示灯不适用于磁带机，闪烁/取消闪烁选项也能成功。

注：
- 在对非 RAID 控制器执行资源清册和监测操作之前，必须执行重新引导时收集系统资源清册 (CSIOR) 操作。
- 仅会为 12 Gbps SAS HBA 控制器和 HBA330 内部控制器执行针对已启用 SMART 的驱动器和 SES 机柜传感器的实时监测。

注： 不支持□□ SAS HBA 控制器后面的故障□□器。

监测驱动器上的预测性故障分析

存储管理支持在已启用 SMART 的物理磁盘上执行自我监测分析和报告技术 (SMART)。

SMART 可在每个磁盘上执行预测性故障分析并在预测到磁盘故障时发送警报。控制器将检查物理磁盘的故障预测，如果找到，则将此信息传递给 iDRAC。iDRAC 立即记录一个警报。

非 RAID 模式或 HBA 模式下的控制器操作

如果控制器处于非 RAID 模式（HBA 模式），则：
- 虚拟磁盘或热备用不可用。
- 控制器的安全状态被禁用。
- 所有物理磁盘处于非 RAID 模式。

如果控制器处于非 RAID 模式，您可以执行以下操作：
- 闪烁/取消闪烁物理磁盘。
- 配置的所有属性，包括以下选项：
  - 负载平衡模式
  - 检查一致性模式
  - 巡检读取模式
  - 回写模式
  - 控制器引导模式
  - 增强的自动导入外部配置
  - 重建率
  - 检查一致性率
  - 重构率
  - 后台初始化 (BGI) 率
  - 机柜或背板模式
  - 巡检读取未配置区域
- 查看适用于 RAID 控制器的所有属性（虚拟磁盘除外）。
- 清除外部配置

注： 如果某操作在非 RAID 模式中不受支持，会□示一条□□消息。

当控制器处于非 RAID 模式时，无法监测机柜温度探测器、风扇和电源设备。

在多个存储控制器上运行 RAID 配置作业

当从任何受支持的 iDRAC 界面对两个以上的存储控制器执行操作时，请确保：
- 单独对每个控制器运行作业。等待每个作业完成，然后再开始在下一个控制器上进行配置和创建作业。
- 使用计划选项将多个作业计划为在以后某个时间运行。

管理保留的高速缓存

受管保留的高速缓存功能是控制器选项，可让用户选择放弃控制器高速缓存数据。在回写式策略中，数据写入到高速缓存中，然后写入物理磁盘。如果虚拟磁盘由于任何原因变为脱机或被删除，则高速缓存中的数据将被删除。

在电源故障或电缆断开时，PREC 控制器将保留写入在保留的或故障的高速缓存中的数据，直到用户恢复虚拟磁盘或清除高速缓存。

控制器的状态受保留的高速缓存影响。如果控制器已保留高速缓存，则控制器状态显示为已降级。仅当满足以下所有条件时，才可放弃保留的高速缓存：

- 控制器没有任何外部配置。
- 控制器没有任何脱机或缺失的虚拟磁盘。
- 连接到任何虚拟磁盘的电缆没有断开连接。

管理 PCIe SSD

外围组件互联高速 (PCIe) 固态设备 (SSD) 是一种高性能存储设备，适用于要求低延迟、较高的每秒输入输出操作数 (IOPS) 和企业级存储可靠性和维护保养方便性的解决方案。PCIe SSD 是基于单层单元 (SLC) 和多层单元 (MLC) NAND 闪存技术而设计的，具有高速 PCIe 2.0、PCIe 3.0 或 PCIe 4.0 兼容接口。在第 14 代 PowerEdge 服务器中，共有三种不同的方法来连接 SSD。您可以使用扩展器通过背板连接 SSD，使用超薄线缆直接将 SSD 从背板连接到主板（无需使用扩展器），以及使用位于主板上的 HHHL（附加）卡。

注：

- 第 14 代 PowerEdge 服务器支持基于行业标准 NVMe-MI 规格的 NVMe SSD
- PERC 11 支持 PERC 资源清册监视和配置下的 PCIe SSD/NVMe 设备。

通过使用 iDRAC 界面，可以查看和配置 NVMe PCIe SSD。

PCIe SSD 的重要功能有：

- 热插拔功能
- 高性能设备

极少数第 14 代 PowerEdge 服务器最多可支持 32 个 NVMe SSD。

可为 PCIe SSD 执行以下操作：

- 对服务器中 PCIe SSD 的运行状况进行资源清册以及远程监测
- 进行 PCIe SSD 卸下准备
- 安全地擦除数据
- 设备 LED 闪烁或取消闪烁（标识设备）

可为 HHHL SSD 执行以下操作：

- 对服务器中的 HHHL SSD 进行资源清册和实时监测
- 在 iDRAC 和 OMSS 中报告和记录出故障的插卡
- 安全擦除数据并卸下插卡
- TTY 日志报告

您可为 SSD 执行以下操作：

- 报告驱动器状态，例如联机、故障和脱机

注： □插拔功能、卸下准□以及□□ LED 指示灯□□或取消□□不适用于 HHHL PCIe SSD □□。

注： 当 NVMe □□控制在 S140 之后□，不支持“准□□除”和“加密擦除”操作，支持□□和取消□□。

对 PCIe SSD 进行资源清册和监测

以下资源清册和监测信息适用于 PCIe SSD：

- 硬件信息：
  - PCIe SSD 扩展卡
  - PCIe SSD 背板

    如果系统具有专用 PCIe 背板，将显示两个 FQDD。一个 FQDD 用于常规驱动器，而另一个用于 SSD。如果背板共享（通用），仅显示一个 FQDD。如果直接连接 SSD，控制器 FQDD 将报告为 CPU.1，这表示 SSD 直接连接至 CPU。

- 软件资源清册仅包括用于 PCIe SSD 的固件版本。

使用 Web 界面对 PCIe SSD 进行资源清册和监测

要对 PCIe SSD 设备进行资源清册和监测，请转至 **Storage（存储）** > **Overview（概述）** > **Physical Disks（物理磁盘）**。此时将显示**属性**页。对于 PCIe SSD，**Name（名称）**列中将显示 **PCIe SSD**。展开可查看属性。

使用 RACADM 对 PCIe SSD 进行资源清册和监测

使用 `racadm storage get controllers:<PcieSSD controller FQDD>` 命令资源清册和监测 PCIe SSD。

要查看所有 PCIe SSD 驱动器，请使用以下命令：

```
racadm storage get pdisks
```

要查看 PCIe 扩展卡，请使用以下命令：

```
racadm storage get controllers
```

要查看 PCIe SSD 背板的信息，请使用以下命令：

```
racadm storage get enclosures
```

注： 使用所有上述命令时，都会显示 PERC 设备。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

准备移除 PCIe SSD

注： 在出□以下情况□不支持此操作：

- 已使用 S140 控制器配置 PCIe SSD。
- NVMe 设备在 PERC 11 的后面。

PCIe SSD 支持有序热交换操作，允许您添加或移除设备，而不必停止或重新启动安装这些设备的系统。为防止数据丢失，必须先使用“准备移除”操作，然后再实际移除设备。

仅当 PCIe SSD 安装于运行受支持操作系统的受支持 Dell 系统上时支持有序热交换。要确保您的 PCIe SSD 具有正确的硬件配置，请参阅系统特定的用户手册。

VMware vSphere (ESXi) 系统中的 PCIe SSD 以及 HHHL PCIe SSD 设备不支持准备移除操作。

注： 使用 ESXi 6.0 和 iDRAC Service Module 2.1 版本或更高版本的系□支持准□移除操作。

准备移除操作可以使用 iDRAC Service Module 实时执行。

“准备移除”操作会停止所有后台活动和所有正在进行的 I/O 活动，以便可以安全地移除设备。此操作将导致设备上的状态 LED 闪烁。在启动“准备移除”操作后，可以从下列条件下的系统中安全移除设备：

- PCIe SSD 以安全移除 LED 模式闪烁（呈琥珀色闪烁）。
- 系统不再能够访问 PCIe SSD。

在准备 PCIe SSD 以待移除 之前，请确保：

- 已安装 iDRAC Service Module。
- 已启用 Lifecycle Controller。
- 您具有服务器控制权限和登录权限。

使用 Web 界面准备移除 PCIe SSD

要准备 PCIe SSD 以待移除，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Storage（存储）** > **Overview（概览）** > **Physical Disks（物理磁盘）**。
   此时将显示**设置物理磁盘**页面。

2. 从**控制器**下拉菜单中，选择扩展器以查看关联的 PCIe SSD。
3. 从下拉菜单中，为一个或多个 PCIe SSD 选择**准备移除**。
   如果已选择**准备移除**，并且要查看下拉菜单中的其他选项，请选择**操作**，然后单击下拉菜单以查看其他选项。
   注： 确保已安装并运行 iSM 以执行 `preparetoremove` 操作。
4. 在**应用操作模式**下拉菜单中，选择**立即应用**以立即应用这些操作。
   如果存在要完成的任务，此选项将灰显。
   注： 对于 PCIe SSD 设备，只有 **Apply Now（立即应用）**选项可用。此操作在暂存模式中不受支持。
5. 单击**应用**。
   如果未创建作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
   如果作业创建成功，将显示一条消息，指出为所选控制器创建的作业 ID。单击**作业队列**，可在**作业队列**页面中查看该作业的进度。
   如果未创建待处理操作，将显示一则错误消息。如果待处理操作成功并且作业创建未成功，则将显示一条错误消息。

使用 RACADM 准备移除 PCIe SSD

要准备 PCIeSSD 驱动器以待移除，请执行以下操作：

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

在执行 `preparetoremove` 命令后，创建目标作业：

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

要查询返回的作业 ID：

```
racadm jobqueue view -i <job ID>
```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

擦除 PCIe SSD 设备数据

注： 当使用 SWRAID 控制器配置 PCIe SSD □，不支持此操作。

“加密擦除”将永久擦除磁盘上现有的所有数据。在 PCIe SSD 上执行加密擦除时，将覆盖所有数据块并导致该 PCIe SSD 上的所有数据永久性丢失。在加密擦除过程中，主机无法访问该 PCIe SSD。更改将在系统重新引导后应用。

如果系统在加密擦除期间重新引导或遇到断电，则该操作将被取消。您必须重新引导系统并重启此过程。

在擦除 PCIe SSD 设备数据之前，请确保：

- 已启用 Lifecycle Controller。
- 您具有服务器控制权限和登录权限。

注：

- 擦除 PCIe SSD 只能作为阶段性操作执行。
- 在擦除驱动器后，驱动器将在操作系统中显示为联机，但未初始化。您必须重新初始化并重新格式化驱动器，然后才能使用它。
- 在热插拔 PCIe SSD 后，可能需要等待几秒种，该 PCIe SSD 才会显示在 Web 界面中。

使用 Web 界面擦除 PCIe SSD 设备数据

要擦除 PCIe SSD 设备上的数据，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Storage（存储）** > **Overview（概览）** > **Physical Disks（物理磁盘）**。
   此时将显示 **Physical Disk（物理磁盘）**页面。
2. 从**控制器**下拉菜单中，选择控制器以查看关联的 PCIe SSD。

3. 从下拉菜单中，对一个或多个 SSD 选择 **Cryptographic Erase（安全擦除）**选项。
   如果您已选择 **Cryptographic Erase（安全擦除）**，并且要查看下拉菜单中的其他选项，请选择 **Action（操作）**，然后单击下拉菜单以查看其他选项。
4. 从**应用操作模式**下拉菜单中，选择以下选项之一：
   - **At Next Reboot（下次重新引导时）** - 选择此选项可在下一次系统重新引导期间应用操作。
   - **在计划的时间** - 选择此选项可在计划的日期和时间应用操作：
     - **开始时间**和**结束时间** - 单击日历图标并选择日期。从下拉菜单中，选择时间。操作将在开始时间和结束时间之间应用。
     - 从下拉菜单中，选择重新引导类型：
       - 不重新引导（手动重新引导系统）
       - 正常关机
       - 强制关机
       - 关闭系统电源后重启（冷引导）
5. 单击**应用**。
   如果未创建作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
   如果作业创建成功，将显示一条消息，指出为所选控制器创建的作业 ID。单击**作业队列**，可在作业队列页面中查看该作业的进度。
   如果未创建待处理操作，将显示一则错误消息。如果待处理操作成功并且作业创建未成功，则将显示一条错误消息。

使用 RACADM 擦除 PCIe SSD 设备数据

要安全地擦除 PCIe SSD 设备：

```
racadm storage secureerase:<PCIeSSD FQDD>
```

要在执行 `secureerase` 命令后创建目标作业：

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

要查询返回的作业 ID：

```
racadm jobqueue view -i <job ID>
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

管理机柜或背板

可以对机柜或背板执行以下操作：
- 查看属性
- 配置统一模式或拆分模式
- 查看插槽信息（通用或共享）
- 设置 SGPIO 模式
- 设置资产标签
- 资产名称

配置背板模式

第 14 代 Dell PowerEdge 服务器支持新的内部存储拓扑，其中两个存储控制器 (PERC) 可通过单个扩展器连接到一组内部驱动器。此配置用于没有故障转移或高可用性 (HA) 功能的高性能模式。扩展器将在两个存储控制器之间拆分内部驱动器阵列。在这种模式下，虚拟磁盘创建只会显示已连接到某个特定控制器的驱动器。此功能无需任何许可要求。此功能仅在部分操作系统上受支持。

背板支持以下模式：

- 统一模式 — 此模式为默认模式。主要 PERC 控制器有权访问所有连接至背板的驱动器，即使已安装了第二个 PERC 控制器也是如此。
- 拆分模式 - 一个控制器可访问前 12 个驱动器，另一个控制器可访问后 12 个驱动器。连接至第一个控制器的驱动器编号为 0-11，连接至第二个控制器的驱动器编号为 12-23。
- 拆分模式 4:20 - 一个控制器可访问前 4 个驱动器，另一个控制器可访问后 20 个驱动器。连接至第一个控制器的驱动器编号为 0-3，连接至第二个控制器的驱动器编号为 4-23。
- 拆分模式 8:16 - 一个控制器可访问前 8 个驱动器，另一个控制器可访问后 16 个驱动器。连接至第一个控制器的驱动器编号为 0-7，连接至第二个控制器的驱动器编号为 8-23。
- 拆分模式 16:8 - 一个控制器可访问前 16 个驱动器，另一个控制器可访问后 8 个驱动器。连接至第一个控制器的驱动器编号为 0-15，连接至第二个控制器的驱动器编号为 16-23。
- 拆分模式 20:4 - 一个控制器可访问前 20 个驱动器，另一个控制器可访问后 4 个驱动器。连接至第一个控制器的驱动器编号为 0-19，连接至第二个控制器的驱动器编号为 20-23。
- 拆分模式 6:6:6:6 — 一个机箱安装 4 个刀片，每个刀片分配 6 个驱动器。此模式仅在 PowerEdge C 系列刀片服务器上受支持。
- 信息不可用 - 控制器信息不可用。

如果扩展器具有支持此配置的功能，则 iDRAC 允许拆分模式设置。确保在安装第二个控制器之前启用此模式。iDRAC 会在允许配置此模式之前先检查扩展器功能，并且不会检查是否存在第二个 PERC 控制器。

注： 如果您将背板□置□拆分模式且只□接了一个 PERC，或者将背板□置□□一模式，并□接了两个 PERC，□可能会出□□□□□（或其他□□）。

要修改这些设置，您必须具有服务器控制权限。

如果任何其他 RAID 操作处于挂起状态，或者已计划了任何 RAID 作业，则不能更改背板模式。同样地，如果此设置处于挂起状态，则不能计划其他 RAID 作业。

注：

- 在更改设置时会显示警告消息，因为可能会发生数据丢失。
- LC 擦除或 iDRAC 重设操作不会更改此模式的扩展器设置。
- 此操作仅在实时模式受支持，在分阶段模式中不受支持。
- 您可以多次更改背板配置。
- 如果驱动器关联从一个控制器更改为另一个控制器，背板拆分操作可能会导致数据丢失或配置不适宜。
- 背板拆分操作过程中，RAID 配置可能会受到影响，具体取决于驱动器关联。

只有在系统电源重启后，对此设置的任何更改才会生效。如果从拆分模式更改为统一模式，在下次引导时会显示一条错误消息，因为第二个控制器看不到任何驱动器。此外，第一个控制器将看到外部配置。如果忽略此错误，则现有虚拟磁盘将会丢失。

使用 Web 界面配置背板模式

要使用 iDRAC Web 界面配置背板模式，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **存储配置** > **机柜配置**。
2. 从**控制器**菜单中，选择要配置其关联机柜的控制器。
3. 从**操作**下拉菜单中，选择**编辑机柜模式**。
   此时将显示**编辑机柜模式**页面。
4. 在**当前值**列中，为背板或机柜选择所需机柜模式：提供的选项包括：
   - 统一模式
   - 拆分模式
   - 拆分模式 4:20
   - 拆分模式 8:16
   - 拆分模式 16:8
   - 拆分模式 20:4

   注： 对于 C6420，可用模式为：拆分模式和拆分模式-6:6:6:6。某些平台上可能仅支持少量数值。

   对于 R740xd 和 R940，需要服务器的打开电源后再关闭电源以应用新背板分区，对于 C6420、刀片机箱的 A/C 关机后再开机以应用新背板分区。
5. 单击**添加至待处理操作**。
   将创建作业 ID。

6. 单击**立即应用**。
7. 转到**作业队列**页面，并验证其中是否将作业状态显示为“已完成”。
8. 关闭系统电源后重启，以使设置生效。

使用 RACADM 配置机柜

要配置机柜或背板，请使用 `set` 命令和 **BackplaneMode** 中的对象。

例如，要将 BackplaneMode 属性设置为拆分模式，请执行以下操作：

1. 运行以下命令来查看当前背板模式：

   ```
   racadm get storage.enclosure.1.backplanecurrentmode
   ```

   输出为：

   ```
   BackplaneCurrentMode=UnifiedMode
   ```

2. 运行以下命令来查看所需模式：

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   输出为：

   ```
   BackplaneRequestedMode=None
   ```

3. 运行以下命令将所需背板设置模式为拆分模式：

   ```
   racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
   ```

   显示该消息，提示命令成功。

4. 运行以下命令来验证是否已将 **backplanerequestedmode** 属性设置为拆分模式：

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   输出为：

   ```
   BackplaneRequestedMode=None (Pending=SplitMode)
   ```

5. 运行 `storage get controllers` 命令并记录控制器实例 ID。
6. 运行以下命令来创建作业：

   ```
   racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
   ```

   将返回作业 ID。

7. 运行以下命令来查询作业的状态：

   ```
   racadm jobqueue view -i JID_xxxxxxxx
   ```

   其中，`JID_xxxxxxxx` 是在步骤 6 中获得的作业 ID。

   状态显示为“挂起”。

   继续查询作业 ID，直到显示“已完成”状态（此过程最多可能需要 3 分钟时间）。

8. 运行以下命令来查看 `backplanerequestedmode` 属性值。

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   输出为：

   ```
   BackplaneRequestedMode=SplitMode
   ```

9. 运行以下命令来冷重新引导服务器：

```
racadm serveraction powercycle
```

10. 当系统完成 POST 和 CSIOR 后，键入以下命令来验证 `backplanerequestedmode`：

```
racadm get storage.enclosure.1.backplanerequestedmode
```

输出为：

```
BackplaneRequestedMode=None
```

11. 运行以下命令来验证背板模式是否设置为拆分模式：

```
racadm get storage.enclosure.1.backplanecurrentmode
```

输出为：

```
BackplaneCurrentMode=SplitMode
```

12. 运行以下命令并验证是否只显示驱动器 0-11：

```
racadm storage get pdisks
```

有关 RACADM 命令的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC RACADM 命令行界面参考指南）。

查看通用插槽

某些第 14 代 PowerEdge 服务器背板可在同一个插槽中支持 SAS/SATA 和 PCIe SSD 驱动器。这些插槽称为通用插槽并连接至主要存储控制器 (PERC)。CPU 背板管理的 PCIe 扩展卡或直接连接管理器支持相同插槽中的 SAS/SATA 或 PCIe SSD 驱动器。背板固件将提供有关支持该功能的插槽的信息。背板支持 SAS/SATA 磁盘或 PCIe SSD。通常情况下，四个编号较高的插槽是通用插槽。例如，在支持 24 个插槽的通用背板中，插槽 0-19 仅支持 SAS/SATA 磁盘，插槽 20-23 则可支持 SAS/SATA 或 PCIe SSD。

机柜的汇总运行状况提供了机柜中所有驱动器的合并运行状况。**拓扑**页面上的机柜链接可显示全部机柜信息，而无论其是与哪个控制器关联。虽然两个存储控制器（PERC 和 PCIe 扩展器）可连接至同一个背板，但在**系统资源清册**页面上仅会显示与 PERC 控制器关联的背板。

在**存储** > **机柜** > **属性**页面中，**物理磁盘概览**部分将显示以下选项：

- **插槽为空** — 如果插槽为空。
- **支持 PCIe** — 如果没有支持 PCIe 的插槽，该栏不会显示。
- **总线协议** — 如果是通用型背板，且在其中一个插槽中安装了 PCIe SSD ，该栏会显示 **PCIe**。
- **热备件** — 该栏不适用于 PCIe SSD。

注: 通用插槽支持□交□功能。如果要移除 PCIe SSD □□器并将其更□□ SAS/SATA □□器，□确保先□ PCIe SSD □□器完成“准□移除”任□。如果不□行□任□，主机操作系□可能会遇到□□，如□屏、内核□□等。

设置 SGPIO 模式

存储控制器可连接至 I2C 模式（Dell 背板的默认设置）或串行通用输入/输出 (SGPIO) 模式下的背板。要闪烁驱动器上的 LED，需建立此连接。Dell PERC 控制器和背板可同时支持这两种模式。要支持某些信道适配器，必须将背板模式更改为 SGPIO 模式。

仅无源背板可支持 SGPIO 模式。处于下游模式中的基于扩展器的背板或无源背板不支持此模式。背板固件将提供有关功能、当前状态和所需状态的信息。

在执行 LC 擦除操作或将 iDRAC 重设为默认值后，SGPIO 模式将重设为禁用状态。它会比较 iDRAC 设置与背板设置。如果背板已设置为 SGPIO 模式，iDRAC 会将其设置更改为与背板设置匹配。

要使任何设置更改生效，必须关闭服务器电源后重启。

您必须具有服务器控制权限才能修改此设置。

注: 不能使用 iDRAC Web 界面□置 SGPIO 模式。

使用 RACADM 设置 SGPIO 模式

要配置 SGPIO 模式，使用 `set` 命令以及 `SGPIOMode` 组中的对象。

如果将其设置为已禁用，则为 I2C 模式。如果已启用，则设置为 SGPIO 模式。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC RACADM 命令行界面参考指南）。

设置机柜资产标签

设置机柜资产标签允许您配置存储机柜的资产标签。

用户可以更改机柜的资产标签属性以识别机柜。这些字段均已选中无效的值，并且如果输入了无效的值，则会显示错误。这些字段是机柜固件的一部分；数据最初显示固件中保存的值。

注: 资产标签有一个字符限制为 10，其中包括 NULL 字符。

注: 这些操作在机柜内部不受支持。

设置机柜资产名称

设置机柜资产名称使用户能够配置存储机柜资产名称。

用户可以更改机柜资产名称属性以轻松识别机柜。这些字段均已选中无效的值，并且如果输入了无效的值，则会显示错误。这些字段是机柜固件的一部分；数据最初显示固件中保存的值。

注: 资产名称有一个字符限制为 32，其中包括 NULL 字符。

注: 这些操作在机柜内部不受支持。

选择要应用设置的操作模式

在创建和管理虚拟磁盘及设置物理磁盘、控制器、机柜或重设控制器时，您必须在应用各种设置之前选择操作模式。即，指定这些设置的应用时间：

- 立即
- 下次系统重新引导期间
- 在计划的时间
- 作为在单个作业一部分中以批处理形式应用的挂起操作。

使用 Web 界面选择操作模式

要选择操作模式以应用设置，请执行以下操作：

1. 当位于以下任何页面上时，可选择操作模式：
   - **Storage（存储）** > **Physical Disks（物理磁盘）**。
   - **Storage（存储）** > **Virtual Disks（虚拟磁盘）**
   - **Storage（存储）** > **Controllers（控制器）**
   - **Storage（存储）** > **Enclosures（盘柜）**
2. 从**应用操作模式**下拉菜单中选择下列任一项：
   - **Apply Now（立即应用）** — 选择此选项可立即应用设置。此选项仅适用于 PERC 9 控制器。如果存在要完成的任务，此选项将灰显。此作业需要至少等待 2 分钟才能完成。
   - **At Next Reboot（下次重新引导时）** - 选择此选项可在下一次系统重新引导期间应用设置。
   - **在计划的时间** - 选择此选项可在计划的日期和时间应用设置：

- **开始时间**和**结束时间** - 单击日历图标并选择日期。从下拉菜单中，选择时间。将在开始时间和结束时间之间应用设置。
- 从下拉菜单中，选择重新引导类型：
  - 不重新引导（手动重新引导系统）
  - 正常关机
  - 强制关机
  - 关闭系统电源后重启（冷引导）

- **Add to Pending Operations（添加到待处理操作）** - 选择此选项可创建待处理操作以应用设置。您可以在 **Storage（存储）** > **Overview（概览）** > **Pending Operations（待处理操作）**页面查看控制器的所有待处理操作。

注：

- **Add to Pending Operations（添加到待处理操作）**选项不适用于 **Pending Operations（待处理操作）**页面，以及 **Physical Disks（物理磁盘）** > **Setup（设置）**页面中的 PCIe SSD。
- 在**机柜设置**页面中，只有**立即应用**选项可用。

3. 单击**应用**。
   将会根据所选的操作模式应用设置。

使用 RACADM 选择操作模式

要选择操作模式，请使用 `jobqueue` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

查看和应用挂起操作

您可以查看并提交存储控制器的所有待处理操作。所有设置在下次重新引导期间或根据选定的选项在计划的时间将立即应用。您可以删除控制器的所有待处理操作。您不能删除单个待处理操作。

将在选定组件（如控制器、机柜、物理磁盘和虚拟磁盘）上创建挂起操作。

仅会在控制器上创建配置作业。对于 PCIe SSD，将在 PCIe SSD 磁盘而非 PCIe 扩展器上创建作业。

使用 Web 界面查看、应用或删除挂起操作

1. 在 iDRAC Web 界面中，转至 **Storage（存储）** > **Overview（概览）** > **Pending Operations（待处理操作）**。
   将显示**挂起操作**页面。
2. 在**组件**下拉菜单中，选择要查看、提交或删除其挂起操作的控制器。
   将显示选定控制器的挂起操作的列表。

注：

- 为导入外部配置、清除外部配置、安全密钥操作和加密虚拟磁盘创建了挂起操作。但是，在**挂起操作**页面和“挂起操作”弹出消息中未显示这些操作。
- 无法从**挂起操作**页面中创建 PCIe SSD 的作业

3. 要删除选定控制器的挂起操作，请单击**删除全部挂起操作**。
4. 从下拉菜单中，选择以下选项之一，然后单击**应用**提交挂起操作：
   - **Apply Now（立即应用）** — 选择此选项可立即提交所有操作。此选项仅适用于具有最新固件版本的 PERC 9 控制器。
   - **At Next Reboot（在下次重新引导时）** — 选择此选项可在下一次系统重新引导期间提交所有操作。
   - **At Scheduled Time（在计划的时间）** — 选择此选项可在计划的日期和时间应用操作。
     - **开始时间**和**结束时间** - 单击日历图标并选择日期。从下拉菜单中，选择时间。操作将在开始时间和结束时间之间应用。
     - 从下拉菜单中，选择重新引导类型：
       - 不重新引导（手动重新引导系统）
       - 正常关机
       - 强制关机

- 关闭系统电源后重启（冷引导）

5. 如果未创建提交作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
6. 如果提交作业创建成功，将显示一条消息，指出为所选控制器创建的作业 ID。单击 **Job Queue（作业队列）**，可在 **Job Queue（作业队列）**页面中查看该作业的进度。

   如果清除外部配置、导入外部配置、安全密钥操作或加密虚拟磁盘操作处于待处理状态，并且如果这些是仅有的待处理操作，那么您不能从 **Pending Operations（待处理操作）**页面中创建作业。您必须执行任何其他存储配置操作，或使用 RACADM 或 WSMan 在所需的控制器上创建所需的配置作业。

   您无法在 **Pending Operations（待处理器操作）**页面中查看或清除 PCIe SSD 的待处理操作。使用 racadm 命令可清除 PCIe SSD 的待处理操作。

使用 RACADM 查看和应用挂起操作

要应用挂起操作，请使用 **jobqueue** 命令。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

存储设备 - 应用操作方案

案例 1：已选择一项应用操作（“立即应用”、“在下次重新引导时”或“在计划的时间”），并且没有现有的挂起操作

如果您选择了**立即应用**、**在下次重新引导时**或**在计划的时间**，然后单击**应用**，首先将为所选的存储配置操作创建挂起操作。

- 如果挂起操作成功，并且没有先前存在的挂起操作，则将创建作业。如果作业创建成功，将显示一条消息，指出为所选设备创建的作业 ID。单击**作业队列**，可在**作业队列**页面中查看该作业的进度。如果未创建作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
- 如果未成功创建挂起操作，并且没有先前存在的挂起操作，将显示一条错误消息，其中包含 ID 和建议的响应操作。

案例 2：已选择一项应用操作（“立即应用”、“在下次重新引导时”或“在计划的时间”），并且存在现有的挂起操作

如果您选择了**立即应用**、**在下次重新引导时**或**在计划的时间**，然后单击**应用**，首先将为所选的存储配置操作创建挂起操作。

- 如果挂起操作已成功创建，并且如果存在现有的挂起操作，则将显示一条消息。
  - 单击**查看挂起操作**链接可查看设备的挂起操作。
  - 单击 **Create Job（创建作业）**以为所选设备创建作业。如果作业创建成功，将显示一条消息，指出为所选设备创建的作业 ID。单击**作业队列**，可在**作业队列**页面中查看该作业的进度。如果未创建作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
  - 单击**取消**不会创建作业，并停留在该页面上，以执行更多存储配置操作。
- 如果未成功创建挂起操作，并且如果存在现有的挂起操作，则将显示一条错误消息。
  - 单击**挂起操作**，可查看设备的挂起操作。
  - 单击**为成功操作创建作业**可为现有的挂起操作创建作业。如果作业创建成功，将显示一条消息，指出为所选设备创建的作业 ID。单击**作业队列**，可在**作业队列**页面中查看该作业的进度。如果未创建作业，将显示一条消息，指出该作业创建失败。另外，还将显示消息 ID 和建议的响应操作。
  - 单击**取消**不会创建作业，并停留在该页面上，以执行更多存储配置操作。

案例 3：已选择“添加到挂起操作”，并且没有现有的挂起操作

如果您已选择**添加到挂起操作**，然后单击**应用**，首先将为所选的存储配置操作创建挂起操作。

- 如果已成功创建挂起操作，并且如果没有现有的挂起操作，则将显示一条信息消息：
  - 单击**确定**可停留在该页面上，以执行更多存储配置操作。
  - 单击**挂起操作**，可查看设备的挂起操作。直到在所选控制器上创建了作业，才会应用这些挂起操作。
- 如果未成功创建挂起操作，并且如果没有现有的挂起操作，则将显示一条错误消息。

案例 4：已选择“添加到挂起操作”，并且有先前存在的挂起操作

如果您已选择**添加到挂起操作**，然后单击**应用**，首先将为所选的存储配置操作创建挂起操作。

- 如果已成功创建挂起操作，并且如果存在现有的挂起操作，则将显示一条信息消息：
  - 单击**确定**可停留在该页面上，以执行更多存储配置操作。
  - 单击**挂起操作**，可查看设备的挂起操作。
- 如果未成功创建挂起操作，并且如果存在现有的挂起操作，则将显示一条错误消息。
  - 单击**确定**可停留在该页面上，以执行更多存储配置操作。
  - 单击**挂起操作**，可查看设备的挂起操作。

注:

- 在任何时候，如果您未看到用于在存储配置页面上创建作业的选项，请转至**存储概览** > **挂起操作**页面，以查看现有的挂起操作，并在所需的控制器上创建作业。
- 仅案例 1 和 2 适用于 PCIe SSD。您将无法查看 PCIe SSD 的待处理操作，因此 **Add to Pending Operations（添加到待处理操作）**选项不可用。使用 racadm 命令可清除 PCIe SSD 的待处理操作。

闪烁或取消闪烁组件 LED

可以通过闪烁磁盘上的发光二极管 (LED) 之一找到机柜内的物理磁盘、虚拟磁盘驱动器和 PCIe SSD。

您必须具有登录权限才能闪烁或取消闪烁 LED。

控制器必须支持实时配置。对此功能的实时支持仅在 PERC 9.1 和更高版本固件中可用。

注: □于不□背板的服□器，不支持□行□□或取消□□操作。

使用 Web 界面闪烁或取消闪烁组件 LED

要闪烁或取消闪烁组件 LED，请执行以下操作：

1. 在 iDRAC Web 界面中，根据要求转至下列任一页面：
   - **Storage（存储）** > **Overview（概览）** > **Physical Disks（物理磁盘）** > **Status（状态）** – 显示识别的物理磁盘页面，您可以在该页面中闪烁或取消闪烁物理磁盘和 PCIe SSD。
   - **Storage（存储）** > **Overview（概览）** > **Physical Disks（虚拟磁盘）** > **Status（状态）** - 显示识别的虚拟磁盘页面，您可以在该页面中闪烁或取消闪烁虚拟磁盘。
2. 如果您选择物理磁盘：
   - 选择或取消选择所有组件的 LED - 选择 **Select/Deselect All（全选/取消全选）**选项，然后单击 **Blink（闪烁）**可开始闪烁组件的 LED。同样，单击**取消闪烁**可停止闪烁组件的 LED。
   - 选择或取消选择单个组件的 LED - 选择一个或多个组件，然后单击**闪烁**可开始闪烁所选组件的 LED。同样，单击**取消闪烁**可停止闪烁组件的 LED。
3. 如果您选择虚拟磁盘：
   - 选择或取消选择所有物理磁盘驱动器或 PCIe SSD - 选择 **Select/Deselect All（全选/取消全选）**选项，然后单击 **Blink（闪烁）**可开始闪烁所有物理磁盘驱动器和 PCIe SSD。同样，单击**取消闪烁**可停止闪烁 LED。
   - 选择或取消选择单个物理磁盘驱动器或 PCIe SSD - 选择一个或多个物理磁盘驱动器，然后单击**闪烁**可开始闪烁物理磁盘驱动器或 PCIe SSD 的 LED。同样，单击**取消闪烁**可停止闪烁 LED。
4. 如果位于**识别虚拟磁盘**页面上：
   - 选择或取消选择所有虚拟磁盘 - 选择 **Select/Deselect All（全选/取消全选）**选项，然后单击 **Blink（闪烁）**以开始闪烁所有虚拟磁盘的 LED。同样，单击**取消闪烁**可停止闪烁 LED。
   - 选择或取消选择单个虚拟磁盘 - 选择一个或多个虚拟磁盘，然后单击**闪烁**以开始闪烁虚拟磁盘的 LED。同样，单击**取消闪烁**可停止闪烁 LED。

   如果闪烁或取消闪烁操作未成功，则会显示错误消息。

使用 RACADM 闪烁或取消闪烁组件 LED

要闪烁或取消闪烁组件 LED，请使用以下命令：

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

热重新启动

在执行热重新启动时，将观察到以下行为：

- 在热重新启动后，iDRAC UI 中的 PERC 控制器将立即灰显。在热重新启动后，一旦完成重新资源清册，PERC 控制器将可用。这仅适用于 PERC 控制器，而不适用于 NVME/HBA/BOSS。
- 当 GUI 中 PERC 控制器灰显时，SupportAssist 中的存储文件将为空。
- 在 `perc reinventory` 期间，为 PERC 执行过去事件和严重事件的 LC 日志记录。PERC 组件的其余所有 LCL 都将被禁止。在完成 PERC 重新资源清册后，LCL 才会恢复。
- 在 PERC 重新资源清册完成之前，无法启动任何实时作业。
- 在 PERC 重新资源清册完成之前，不会收集遥测数据。
- PERC 资源清册完成后，行为恢复正常。

18

BIOS 设置

您可以在 BIOS 设置下查看用于特定服务器的多个属性。您可以从此 BIOS 配置设置修改每个属性的不同参数。一旦您选择一个属性，它显示与该特定属性相关的不同参数。您可以修改一个属性的多个参数，并且在修改不同属性之前应用更改。当用户展开配置组时，属性会按字母顺序显示。

注:

- 属性级别帮助内容会动态生成。
- 即使禁用了所有 USB 端口，仍可使用 iDRAC Direct USB 端口，且无需重新启动主机。

应用

应用按钮呈灰色显示，直至修改任意一种属性。一旦您所更改一种属性，然后单击**应用**,它将允许您对属性所需更改进行修改。如果请求无法设置 BIOS 属性，将抛出映射 SMIL API 错误或作业创建错误的相应 HTTP 响应状态代码的错误。此时，将生成并显示一条消息。有关更多信息，请参阅 第 14 代 Dell EMC PowerEdge 服务器的事件和错误消息参考指南，网址：https://www.dell.com/idracmanuals。

放弃更改

放弃更改按钮将呈灰色显示，直至修改任意一种属性。如果您单击**放弃更改**按钮，将放弃所有最近更改，并还原为先前或初始值。

应用和重新引导

当用户修改属性值或引导顺序时，用户都将有两个选择来应用配置；**应用和重新引导**或**在下次重新引导时应用**。在任一应用选项中，用户将被重定向到作业队列页面以监测该特定作业的进度。

用户可以查看与 LC 日志中 BIOS 配置相关的审计信息。

如果您单击**应用和重新引导**，它将会立即重新启动服务器以配置所有所需更改。如果请求无法设置 BIOS 属性，将抛出映射 SMIL API 错误或作业创建错误的相应 HTTP 响应状态代码的错误。此时，将生成并显示一条 EEMI 消息。

在下次重新引导时应用

当用户修改属性值或引导顺序时，用户都将有两个选择来应用配置；**应用和重新引导**或**在下次重新引导时应用**。在任一应用选项中，用户将被重定向到作业队列页面以监测该特定作业的进度。

用户可以查看与 LC 日志中 BIOS 配置相关的审计信息。

如果您单击**在下次重新引导时应用**，它将在下次重新启动服务器时配置所有所需更改。根据最新配置更改，您将不会遇到任何立即修改，直至成功进行下一次重新引导。如果请求无法设置 BIOS 属性，将抛出映射 SMIL API 错误或作业创建错误的相应 HTTP 响应状态代码的错误。此时，将生成并显示一条 EEMI 消息。

删除所有待定值

仅基于最新配置更改存在待定值时，启用**删除所有待定值**按钮。如果用户决定不应用配置更改，用户可以单击**删除所有待定值**按钮来终止所有修改。如果请求无法删除 BIOS 属性，将抛出映射 SMIL API 错误或作业创建错误的相应 HTTP 响应状态代码的错误。此时，将生成并显示一条 EEMI 消息。

待处理值

通过 iDRAC 的 BIOS 属性的配置将不会立即更新至 BIOS。它要求重新引导服务器执行更改。当您修改 BIOS 属性时，那么将更新**待定值**。如果属性已具有待定值（已被配置），它将显示在 GUI 上。

修改 BIOS 配置

修改 BIOS 配置将导致会输入到 LC 日志中的审核日志条目。

BIOS 实时扫描

当主机接通电源但尚未进行开机自检时，BIOS 实时扫描会验证 BIOS 主 ROM 中 BIOS 映像的完整性和真实性。

注：
- 此功能需要 iDRAC Datacenter 许可证。
- 您需要具有调试权限才能运行此功能。

在以下情况下，iDRAC 会自动对 BIOS 映像的不可变部分执行验证：
- 交流电源关闭后重启/冷启动
- 按照用户确定的计划执行
- 按需（由用户发起）

成功完成实时扫描的结果将记录到 LC 日志中。故障结果将记录到 LCL 和 SEL。

主□：

- BIOS □□□描
- BIOS 恢复和硬件信任根 (RoT)

BIOS 实时扫描

当主机接通电源但尚未进行开机自检时，BIOS 实时扫描会验证 BIOS 主 ROM 中 BIOS 映像的完整性和真实性。

注：
- 此功能需要 iDRAC Datacenter 许可证。
- 您需要具有调试权限才能运行此功能。

在以下情况下，iDRAC 会自动对 BIOS 映像的不可变部分执行验证：
- 交流电源关闭后重启/冷启动
- 按照用户确定的计划执行
- 按需（由用户发起）

成功完成实时扫描的结果将记录到 LC 日志中。故障结果将记录到 LCL 和 SEL。

BIOS 恢复和硬件信任根 (RoT)

在恶意攻击或电涌或任何其他不可预见事件导致 BIOS 映像损坏或受损后，PowerEdge 服务器必须恢复 BIOS。恢复 BIOS 需要备用的 BIOS 映像，以使 PowerEdge 服务器从无法启动模式恢复到正常运行模式。此备用/恢复 BIOS 存储在次要 SPI 中（与主 BIOS SPI 通过 MUX 连接）。

可以通过以下方法之一启动恢复序列，将 iDRAC 用作 BIOS 恢复任务的主构造器：

1. **BIOS 主映像/恢复映像自动恢复** — 在 BIOS 自己检测到 BIOS 损坏后，系统会在主机启动过程中自动恢复 BIOS 映像。
2. **BIOS 主/恢复映像强制恢复** — 用户发起更新 BIOS 的 OOB 请求。通常是由于用户有新的更新 BIOS，或者 BIOS 只是因无法启动而崩溃。
3. **主 BIOS ROM 更新** — 单个主 ROM 拆分为数据 ROM 和代码 ROM。iDRAC 对代码 ROM 具有完全访问/控制权。必要时，它会切换 MUX 以访问代码 ROM。

4. **BIOS 硬件信任根 (RoT)** — 此功能在型号为 RX5X、CX5XX 和 TX5X 的服务器中可用。在每个主机启动过程中（仅限冷启动或交流电源关闭后重启，不包括热重启），iDRAC 会确保 RoT 的执行。RoT 会自动运行，用户无法使用任何界面启动它。此 iDRAC 首先启动政策将在每次交流电源关闭后重启和主机直流电源关闭后重启验证主机 BIOS ROM 的内容。此过程可确保 BIOS 的安全启动并进一步保护主机启动过程。

注: 有关硬件 RoT 的详细信息，请参阅以下链接： https://downloads.dell.com/Manuals/Common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf

19

配置并使用虚拟控制台

iDRAC 在 vConsole 中添加了增强的 HTML5 选项，在标准 VNC 客户端上支持 vKVM （虚拟键盘、视频和鼠标）。您可以使用虚拟控制台来通过管理站上的键盘、视频和鼠标管理远程系统，以便控制受管服务器上相应的设备。这是适用于机架式和塔式服务器的许可功能。该功能在刀片式服务器中默认可用。您需要 iDRAC 配置权限才能访问虚拟控制台上的所有配置。

以下是虚拟控制台中可配置的属性列表：

- vConsole 启用 — 已启用/已禁用
- 最大会话数 — 1-6
- 活动会话数 — 0-6
- 远程存在端口（不适用于 eHTML5 插件程序）
- 视频加密 — 已启用/已禁用（不适用于 eHTML5 插件程序）
- 本地服务器视频 — 已启用/已禁用
- 插件类型 — eHTML5（默认）、ActiveX、Java、HTML5
- 共享请求超时后的动态操作 — 完全访问权限、只读访问权限和拒绝访问权限
- 自动系统锁定 — 已启用/已禁用
- 键盘/鼠标连接状态 — 自动连接、连接和分离

主要功能有：

- 可同时支持最多六个虚拟控制台会话。所有会话同时查看同一个受管服务器控制台。
- 您可通过使用 Java、ActiveX、HTML5 或 eHTML5 插件在支持的 Web 浏览器中启动虚拟控制台。

  注: 默认情况下，虚拟控制台类型设置为 eHTML5。

  注: Web 服务器配置的任何更改都将导致现有虚拟控制台会话终止。
- 打开虚拟控制台会话时，受管服务器不会显示控制台已经重定向。
- 您可以同时打开从一个 Management Station 到一个或多个受管系统的多个虚拟控制台会话。
- 您不能使用相同的 HTML5 插件程序打开从管理站到受管服务器的两个虚拟控制台会话。
- 如果第二位用户请求虚拟控制台会话，第一位用户会收到通知并可以选择拒绝访问选项、允许只读访问权限或允许完全共享访问。第 2 位用户也将被告知另一用户享有控制权。第一位用户必须在 32 秒内响应，否则访问权限将基于默认设置授予第二位用户。如果既不是第一个也不是第二个用户具有管理员权限吗，则终止第一个用户的会话会自动终止第二位用户的会话。
- 启动日志和崩溃日志将捕获为视频日志，并采用 MPEG1 格式。
- 崩溃屏幕捕获为 JPEG 文件。
- 在所有插件都支持键盘宏。
- 在所有插件都支持键盘宏。下面是 ActiveX 和 Java 插件支持的宏列表：

表. 57: ActiveX 和 Java 插件支持的键盘宏

Mac 客户端	Win 客户端	Linux 客户端
Ctrl-Al-Del	Ctrl-Alt-Del	Ctrl-Alt-Del
Alt-SysRq-B	Alt-SysRq-B	Alt-SysRq-B
-	Win-P	-
-	-	Ctrl-Alt-F<1-12>
Alt-SysRq	-	-
SysRq	-	-
PrtScrn	-	-
Alt-PrtScrn	-	-
暂停	-	-

注: 有关在 HTML 插件中支持的键盘宏，请参阅基于 HTML5 的虚拟控制台一节。

注: Web 界面中□示的活□虚□控制台会□的数量□□□活□的 Web 界面会□。□数□不包括来自 SSH 和 RACADM 等其他接□的会□数。

注: 有关配置□□器以□□虚□控制台的信息，□参□ 配置 Web 浏览器以使用虚拟控制台 □面上的 69。

注: 要禁用 KVM □□，□使用 OME Modular Web 界面中的机箱□置下的**禁用**□□。

主□：

- 支持的屏幕分辨率和刷新率
- 配置虚□控制台
- □□虚□控制台
- 启□虚□控制台
- 使用虚□控制台□看器

支持的屏幕分辨率和刷新率

下表列出了对于受管服务器上运行的虚拟控制台会话所支持的屏幕分辨率和相应的刷新率。

表. 58: 支持的屏幕分辨率和刷新率

屏幕分辨率	刷新率 (Hz)
720x400	70
640x480	60、72、75、85
800x600	60、70、72、75、85
1024x768	60、70、72、75、85
1280x1024	60
1920x1200	60

建议将显示器的显示分辨率配置为 1920x1200 像素。

在刷新率为 60 Hz 时，虚拟控制台支持的最大视频分辨率为 1920x1200。要达到此分辨率，需满足下列条件：

- KVM/显示器连接到支持 1920x1200 分辨率的 VGA
- 最新 Matrox 视频驱动程序（适用于 Windows）

当最大分辨率低于 1920x1200 的本地 KVM/显示器连接到任一 VGA 连接器时，它将降低虚拟控制台中支持的最大分辨率。

iDRAC 虚拟控制台利用板载 Matrox G200 图形控制器来确定出现物理显示器时连接的显示器的最大分辨率。当显示器支持 1920x1200 或更高分辨率时，虚拟控制台支持 1920x1200 分辨率。如果连接的显示器支持更低的最大分辨率（如许多 KVM），则虚拟控制台最大分辨率会受到限制。

基于显示器显示比率的最大虚拟控制台分辨率：

- 16:10 显示器：1920x1200 将为最大分辨率
- 16:9 显示器：1920x1080 将为最大分辨率

当物理显示器未连接到服务器上的任意 VGA 端口时，安装的操作系统将指示虚拟控制台的可用解决方案。

基于主机操作系统（无物理监视器）的最大虚拟控制台分辨率：

- Windows：1600x1200（1600x1200、1280x1024、1152x864、1024x768、800x600）
- Linux：1024x768（1024x768、800x600、848x480、640x480）

注: 如果在物理 KVM 或显示器不存在时需要通过虚拟控制台实现更高的分辨率，则可以使用 VGA 显示屏仿真程序连接器模拟分辨率高达 1920x1080 的外部显示器连接。

注: 如果有处于活动状态的虚拟控制台会话，并且较低分辨率显示器已连接至虚拟控制台，则服务器控制台分辨率可能会重置（如果在本地控制台上选择了服务器）。如果系统正在运行 Linux 操作系统，则在本地显示器上可能无法查看 X11 控制台。在 iDRAC 虚拟控制台上按 <Ctrl><Alt><F1> 以将 Linux 切换为文本控制台。

配置虚拟控制台

配置虚拟控制台之前，请确保已配置 Management Station。

您可以使用 iDRAC Web 界面或 RACADM 命令行界面配置虚拟控制台。

使用 Web 界面配置虚拟控制台

要使用 iDRAC Web 界面配置虚拟控制台：

1. 转至**配置** > **虚拟控制台**。单击**启动虚拟控制台**链接，然后会显示虚拟控制台页面。
2. 启用虚拟控制台并指定所需的值。有关各选项的信息，请参阅 *iDRAC 联机帮助*。

   注: 如果您正在使用 Nano 操作系统，禁用**虚拟控制台**页面的**自动系统锁定**功能。

3. 单击**应用**。虚拟控制台已配置。

使用 RACADM 配置虚拟控制台

要配置虚拟控制台，请使用 `set` 命令以及 **iDRAC.VirtualConsole** 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

预览虚拟控制台

启动虚拟控制台之前，您可以在 **System（系统）** > **Properties（属性）** > **System Summary（系统摘要）**页面上预览虚拟控制台的状态。**Virtual Console Preview（虚拟控制台预览）**部分显示一个图像，表明虚拟控制台的状态。此图像每 30 秒刷新一次。这是一项授权的功能。

注: 该虚拟控制台图像仅在您启用虚拟控制台时可用。

启动虚拟控制台

您可以使用 iDRAC Web 界面或 URL 启动虚拟控制台。

注: 不要从受管系□上的 Web □□器启□虚□控制台会□。

启动虚拟控制台之前，请确保：

- 您具有管理员权限。
- Web 浏览器配置为使用 HTML5、eHTML5、Java 或 ActiveX 插件。
- 可用的最小网络带宽为 1 MB/秒。

注: 如果嵌入式□□控制器在 BIOS 中已禁用，同□启□虚□控制台，□虚□控制台□看器□空白。

使用 32 位或 64 位 IE 浏览器启动虚拟控制台时，使用 HTML5/eHTML5 或者使用相应浏览器中可用的所需插件（Java 或 ActiveX）。“Internet 选项”设置对所有浏览器通用。

使用 Java 插件启动虚拟控制台时，您可能偶尔会看到 Java 编译错误。要解决此问题，请转至 **Java 控制面板** > **常规** > **网络设置**，并选择**直接连接**。

如果虚拟控制台配置为使用 ActiveX 插件，初次可能无法启动。这是因为网络连接缓慢并且临时证书（虚拟控制台用于连接）超时为两分钟。ActiveX 客户端插件下载时间可能超过此时间。成功下载插件后，您可以正常启动虚拟控制台。

要使用 HTML5/eHTML5 插件启动虚拟控制台，必须禁用弹出窗口拦截程序。

虚拟控制台具有以下控制台控件：

1. **常规** — 您可以设置键盘宏、宽高比和触摸模式。
2. **KVM** — 显示帧速率、带宽、压缩和数据包速率的值。
3. **性能** — 您可以使用此选项更改视频质量和视频速度。
4. **用户列表** — 您可以查看连接到控制台的用户的列表。

您可以通过单击虚拟控制台中的**连接到虚拟介质**选项来访问虚拟介质。

使用 Web 界面启动虚拟控制台

您可以通过下列方式启动虚拟控制台：

- 转至**配置** > **虚拟控制台**。单击**启动虚拟控制台**链接。将显示虚拟控制台页面。

虚拟控制台查看器显示远程系统的桌面。使用此查看器，您可以从管理站控制远程系统的鼠标和键盘功能。

在您启动此应用程序后可能会出现多个消息框。为了防止未授权访问该应用程序，请在三分钟内浏览这些消息框。否则，您将需要重新启动应用程序。

如果在启动查看器时显示一个或多个安全警报窗口，请单击是以继续。

查看器窗口可能会显示两个鼠标指针：一个是管理服务器的鼠标指针，另一个是管理站的鼠标指针。

使用 URL 启动虚拟控制台

要使用 URL 启动虚拟控制台：

1. 打开受支持的 Web 浏览器并在地址栏中输入以下 URL（小写）：**https://iDRAC_ip/console**
2. 根据登录配置，会显示相应的 **Login（登录）**页面：
   - 如果禁用单一登录而启用本地、Active Directory、LDAP 或智能卡登录，则会显示相应的 **Login（登录）**页面。
   - 如果启用单一登录，则会启动 **Virtual Console Viewer（虚拟控制台查看器）**，并在后台显示 **Virtual Console（虚拟控制台）**页面。

   注: Internet Explorer 支持本地、Active Directory、LDAP、智能卡 (SC) 和单一登录 (SSO) 登录。在基于 Windows 的操作系统上 Firefox 支持本地、AD 和 SSO 登录，在基于 Linux 的操作系统上 Firefox 支持本地、Active Directory 和 LDAP 登录。

   注: 如果您没有访问虚拟控制台的权限，但是具有访问虚拟介质的权限，则可使用此 URL 启动虚拟介质，但不能启动虚拟控制台。

使用 Java 或 ActiveX 插件禁用虚拟控制台或虚拟介质启动过程中的警告消息

可以使用 Java 插件禁用在启动虚拟控制台或虚拟介质时显示的警告消息。

注: 您需要 Java 8 或更高版本以使用此功能，并通过 IPv6 网络启动 iDRAC 虚拟控制台。

1. 当您最初通过 Java 插件启动虚拟控制台或虚拟介质时，将显示用于验证发行商的提示窗口。单击**是**。
   会显示一条证书警告消息，指出未找到受信任的证书。

   注: 如果未在操作系统的证书存储区中找到证书，或在以前指定的用户位置中找到了证书，将不会显示此警告消息。

2. 单击 **继续**。
   将启动虚拟控制台查看器或虚拟介质查看器。

   注: 如果虚拟控制台已禁用，将启动虚拟介质查看器。

3. 从 **Tools**（工具）菜单中，选择 **Session Options**（会话选项），然后选择 **Certificate**（证书）选项卡。
4. 单击 **Browse Path**（浏览路径），指定用于存储用户证书的位置，依次单击 **Apply**（应用）和 **OK**（确定），然后退出查看器。
5. 重新启动虚拟控制台。
6. 在证书警告消息中，选择 **Always trust this certificate**（始终信任此证书）选项，然后单击 **Continue**（继续）。
7. 退出查看器。
8. 当您重新启动虚拟控制台时，将不会显示此警告消息。

使用虚拟控制台查看器

虚拟控制台查看器提供各种控制，例如鼠标同步、虚拟控制台扩展、聊天选项、键盘宏、电源操作、下一次引导设备和对虚拟介质的访问。有关使用这些功能的信息，请参阅 *iDRAC Online Help（iDRAC 联机帮助）*。

注: 如果□程服□器关□，□会□示消息“No Signal”（无信号）。

虚拟控制台查看器标题栏显示从管理站连接的 iDRAC 的 DNS 名称或 IP 地址。如果 iDRAC 没有 DNS 名称，则显示 IP 地址。格式为：

- 对于机架式和塔式服务器：

  ```
  <DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>
  ```

- 对于刀片式服务器：

  ```
  <DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>
  ```

有时，虚拟控制台查看器可能会显示低质量视频。这是由于启动虚拟控制台会话时网络连接缓慢导致丢失一个或两个视频帧。要传输所有视频帧和改进后续视频质量，执行以下任一操作：

- 在 **System Summary**（系统摘要）页面中的 **Virtual Console Preview**（虚拟控制台预览）部分，单击 **Refresh**（刷新）。
- 在 **Virtual Console Viewer**（虚拟控制台查看器）中的 **Performance**（性能）选项卡中，将滑块设置为 **Maximum Video Quality**（最高视频质量）。

基于 eHTML5 的虚拟控制台

注: 使用 eHTML5 □□虚□控制台□，必□在客□端以及目□□□布局、操作系□和□□器之□使用一致的□言。例如，必□都是英□（美国）或任何支持的□言。

要启动 eHTML5 虚拟控制台，您必须从 iDRAC 虚拟控制台页面启用虚拟控制台功能，并将**插件类型**选项设置为 eHTML5。

注: 默□情况下，虚□控制台类型□置□ eHTML5。

您可借助以下方法之一将虚拟控制台作为弹出窗口启动：

- 在 iDRAC 主页中，单击控制台预览会话中可用的**启动虚拟控制台**链接
- 从 iDRAC 虚拟控制台页面，单击**启动虚拟控制台**链接。
- 从 iDRAC 登录页面中，键入 **https//<iDRAC IP>/console**。此方法称为直接启动。

在 eHTML5 虚拟控制台中提供以下菜单选项：

- 功率
- 引导
- 聊天
- 键盘
- 屏幕捕捉
- 刷新
- 全屏
- 断开查看器的连接
- 控制台控件
- 虚拟介质

将所有击键操作传递到服务器选项在 eHTML5 虚拟控制台上不受支持。所有功能键使用键盘和键盘宏。

- **常规 —**
  - **控制台控**件 - 此项具有以下配置选项：
    - 键盘宏 — 这在 eHTML5 虚拟控制台中受支持，并且列为以下下拉列表选项。单击**应用**以在服务器上应用所选键组合。
      - Ctrl+Alt+Del
      - Ctrl+Alt+F1
      - Ctrl+Alt+F2
      - Ctrl+Alt+F3
      - Ctrl+Alt+F4
      - Ctrl+Alt+F5
      - Ctrl+Alt+F6

- Ctrl+Alt+F7
- Ctrl+Alt+F8
- Ctrl+Alt+F9
- Ctrl+Alt+F10
- Ctrl+Alt+F11
- Ctrl+Alt+F12
- Alt+Tab
- Alt+ESC
- Ctrl+ESC
- Alt+空格键
- Alt+Enter
- Alt+连字号键
- Alt+F1
- Alt+F2
- Alt+F3
- Alt+F4
- Alt+F5
- Alt+F6
- Alt+F7
- Alt+F8
- Alt+F9
- Alt+F10
- Alt+F11
- Alt+F12
- PrntScrn
- Alt+PrntScrn
- F1
- 暂停
- 选项卡
- Ctrl+Enter
- SysRq
- Alt+SysRq
- Win-P

▪ 纵横比 — eHTML5 虚拟控制台视频图像会自动调整大小，以使图像可见。以下配置选项显示为下拉列表：
- 维护
- 不保持

单击**应用**以在服务器上应用所选设置。

▪ 触摸模式 — eHTML5 虚拟控制台支持触控模式功能。以下配置选项显示为下拉列表：
- 直接
- 相对

单击**应用**以在服务器上应用所选设置。

- **虚拟剪贴板** - 虚拟剪贴板使您能够从虚拟控制台剪切文本缓存内容并将其复制/粘贴到 iDRAC 主机服务器。主机服务器可以是 BIOS、UEFI 或位于操作系统提示中。这是仅限从客户端计算机到 iDRAC 主机服务器的单向操作。请按照以下步骤使用虚拟剪贴板：
  - 将鼠标光标或键盘焦点放置在主机服务器桌面上的所需窗口中。
  - 从 vConsole 中选择**控制台控件**菜单。
  - 使用键盘热键、鼠标或触摸板控件（取决于客户端操作系统）复制操作系统剪贴板缓存内容。或者，您可以在文本框中手动键入文本。
  - 单击**将剪贴板发送到主机**。
  - 然后，文本将显示在主机服务器的活动窗口中。

  注:
  - 此功能只能在拥有数据中心许可证的情况下可用。
  - 此功能仅支持 ASCII 文本。
  - 不支持控制字符。

    - 支持**新行**和**标签**等字符。
    - 文本缓冲内容大小不得超过 4000 个字符。
    - 如果粘贴的缓冲内容超过最大值，则 iDRAC GUI 中的编辑框会将其截断为最大缓冲内容大小。
- **KVM** - 此菜单包含以下只读组件的列表：
    - 帧频
    - 带宽
    - 压缩
    - 数据包速率
- **性能** - 您可以使用滑块按钮来调整**最大视频质量**和**最大视频速度**。
- **用户列表** - 您可以看到登录到虚拟控制台的用户的列表。
- **键盘** - 物理和虚拟键盘的区别是，虚拟键盘根据浏览器语言更改其布局。
- **虚拟介质** - 单击**连接虚拟介质**选项可启动虚拟介质会话。
    - **连接虚拟介质** - 此菜单包含用于映射 CD/DVD、映射可移动磁盘、映射外部设备和重设 USB 的选项。
    - **虚拟介质统计信息** - 此菜单显示传输速率（只读）。此外，它还显示 CD/DVD 和可移动磁盘的详细信息，例如映射详细信息、状态（只读或非只读）、持续时间和读/写字节。
    - **创建映像** - 此菜单允许您选择本地文件夹，并使用本地文件夹内容生成 FolderName.img 文件。

注: 出于安全的原因，在 eHTML5 中□□虚□控制台□□/写□□已禁用。使用 Java 或 ActiveX 插件□，您可以在□插件授予□/写权限之前接受安全消息。

支持的浏览器

在以下浏览器上支持 eHTML5 虚拟控制台：
- Internet Explorer 11
- Chrome 78/79
- Firefox 70/71
- Safari 13.1

注: 建□在系□中安装 Mac OS 版本 10.10.2（或更高版本）。

有关支持的浏览器和版本的更多详细信息，请参阅 *iDRAC 发行说明，网址：*https://www.dell.com/idracmanuals。

基于 HTML5 的虚拟控制台

注: 使用 HTML5 □□虚□控制台□，必□在客□端以及目□□□布局、操作系□和□□器之□使用一致的□言。例如，必□都是英□（美国）或任何支持的□言。

要启动 HTML5 虚拟控制台，您必须从 iDRAC 虚拟控制台页面启用虚拟控制台功能，并将**插件类型**选项设置为 HTML5。

您可借助以下方法之一将虚拟控制台作为弹出窗口启动：
- 在 iDRAC 主页中，单击控制台预览会话中可用的**启动虚拟控制台**链接
- 从 iDRAC 虚拟控制台页面，单击**启动虚拟控制台**链接。
- 从 iDRAC 登录页面中，键入 **https//<iDRAC IP>/console**。此方法称为直接启动。

在 HTML5 虚拟控制台中提供以下菜单选项：
- 功率
- 引导
- 聊天
- 键盘
- 屏幕捕捉
- 刷新
- 全屏
- 断开查看器的连接
- 控制台控件
- 虚拟介质

将所有击键操作传递到服务器选项在 HTML5 虚拟控制台上不受支持。所有功能键使用键盘和键盘宏。
- **控制台控**件 - 此项具有以下配置选项：

- 键盘宏 — 这在 HTML5 虚拟控制台中受支持，并且列为以下下拉列表选项。单击**应用**以在服务器上应用所选键组合。
  - Ctrl+Alt+Del
  - Ctrl+Alt+F1
  - Ctrl+Alt+F2
  - Ctrl+Alt+F3
  - Ctrl+Alt+F4
  - Ctrl+Alt+F5
  - Ctrl+Alt+F6
  - Ctrl+Alt+F7
  - Ctrl+Alt+F8
  - Ctrl+Alt+F9
  - Ctrl+Alt+F10
  - Ctrl+Alt+F11
  - Ctrl+Alt+F12
  - Alt+Tab
  - Alt+ESC
  - Ctrl+ESC
  - Alt+空格键
  - Alt+Enter
  - Alt+连字号键
  - Alt+F1
  - Alt+F2
  - Alt+F3
  - Alt+F4
  - Alt+F5
  - Alt+F6
  - Alt+F7
  - Alt+F8
  - Alt+F9
  - Alt+F10
  - Alt+F11
  - Alt+F12
  - PrntScrn
  - Alt+PrntScrn
  - F1
  - 暂停
  - 选项卡
  - Ctrl+Enter
  - SysRq
  - Alt+SysRq
  - Win-P
- 纵横比 — HTML5 虚拟控制台视频图像会自动调整大小，以使图像可见。以下配置选项显示为下拉列表：
  - 维护
  - 不保持

  单击**应用**以在服务器上应用所选设置。
- 触摸模式 — HTML5 虚拟控制台支持触控模式功能。以下配置选项显示为下拉列表：
  - 直接
  - 相对

  单击**应用**以在服务器上应用所选设置。

- **虚拟剪贴板** - 虚拟剪贴板使您能够从虚拟控制台剪切文本缓存内容并将其复制/粘贴到 iDRAC 主机服务器。主机服务器可以是 BIOS、UEFI 或位于操作系统提示中。这是仅限从客户端计算机到 iDRAC 主机服务器的单向操作。请按照以下步骤使用虚拟剪贴板：
  - 将鼠标光标或键盘焦点放置在主机服务器桌面上的所需窗口中。
  - 从 vConsole 中选择**控制台控件**菜单。

- 使用键盘热键、鼠标或触摸板控件（取决于客户端操作系统）复制操作系统剪贴板缓存内容。或者，您可以在文本框中手动键入文本。
- 单击**将剪贴板发送到主机**。
- 然后，文本将显示在主机服务器的活动窗口中。

注:
- 此功能只能在拥有数据中心许可证的情况下可用。
- 此功能仅支持 ASCII 文本。
- 不支持控制字符。
- 支持**新行**和**标签**等字符。
- 文本缓冲内容大小不得超过 4000 个字符。
- 如果粘贴的缓冲内容超过最大值，则 iDRAC GUI 中的编辑框会将其截断为最大缓冲内容大小。

- **键盘** - 物理和虚拟键盘的区别是，虚拟键盘根据浏览器语言更改其布局。
- 触摸模式 - HTML5 虚拟控制台支持触控模式功能。以下配置选项显示为下拉列表：
  - 直接
  - 相对

  单击**应用**以在服务器上应用所选设置。
- 鼠标加速 - 根据操作系统选择鼠标加速。以下配置选项显示为下拉列表：
  - 绝对（Windows、最新版本的 Linux、Mac OS-X）
  - 相对，无加速
  - 相对（RHEL、Linux 较早版本）
  - Linux RHEL 6.x 和 SUSE Linux Enterprise Server 11 或更高版本

  单击**应用**以在服务器上应用所选设置。
- **虚拟介质** - 单击**连接虚拟介质**选项可启动虚拟介质会话。连接虚拟介质后，您可以查看映射 CD/DVD、映射可移动磁盘和重设 USB 等选项。

注: 出于安全的原因，在 HTML5 中□□虚□控制台□□/写□□已禁用。使用 Java 或 ActiveX 插件□，您可以在□插件授予□/写权限之前接受安全消息。

支持的浏览器

在以下浏览器上支持 HTML5 虚拟控制台：
- Internet Explorer 11
- Chrome 78/79
- Firefox 70/71
- Safari 13.1

注: 建□在系□中安装 Mac OS 版本 10.10.2（或更高版本）。

有关支持的浏览器和版本的更多详细信息，请参阅 *iDRAC 发行说明，网址：*https://www.dell.com/idracmanuals。

同步鼠标指针

注: 此功能不适用于 eHTML5 插件程序类型。

当您通过虚拟控制台连接到受管系统时，受管系统上的鼠标加速可能与管理站上的鼠标指针不同步，因此会在查看器窗口中显示两个鼠标指针。

当使用 Red Hat Enterprise Linux 或 Novell SUSE Linux 时，请在启动虚拟控制台查看器之前先配置 Linux 的鼠标模式。操作系统的默认鼠标设置用于控制虚拟控制台查看器中的鼠标箭头。

当客户端虚拟控制台查看器上显示两个鼠标指针时，表示服务器的操作系统支持相对定位。这种情况对 Linux 操作系统或 Lifecycle Controller 很常见，如果服务器的鼠标加速设置与虚拟控制台客户端上的鼠标加速设置不同，则会产生两个鼠标指针。要解决此问题，请切换到单个指针或使受管系统和管理站上的鼠标加速相匹配：
- 要切换到单个指针，请从**工具**菜单中选择**单个指针**。
- 要设置鼠标加速，请转至**工具** > **会话选项** > **鼠标**。在**鼠标加速**选项卡下，请基于操作系统选择 **Windows** 或 **Linux**。

要退出单个鼠标指针模式，请按 <F9> 或配置的终止键。

注: □□运行 Windows 操作系□的受管系□不适用，因□□操作系□支持□□定位。

如果使用虚拟控制台连接到安装了最新 Linux 分发操作系统的受管系统时，您可能会遇到鼠标同步问题。这可能是由 GNOME 桌面的可预测指针加速功能所导致的。要在 iDRAC 虚拟控制台上正确同步鼠标，必须禁用此功能。要禁用可预测指针加速，请在 **/etc/X11/xorg.conf** 文件中的鼠标部分添加：

`Option "AccelerationScheme" "lightweight"`。

如果仍然出现同步问题，请在 **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** 文件中进行以下附加更改：

将 `motion_threshold` 和 `motion_acceleration` 的值更改为 `-1`。

如果在 GNOME 桌面上关闭鼠标加速，请在虚拟控制台查看器中，转至**工具** > **会话选项** > **鼠标**。在**鼠标加速**选项卡中，选择**无**。

为了独占访问托管的服务器控制台，必须禁用本地控制台并在**虚拟控制台**页面上将**最大会话数**重新配置为 `1`。

通过 Java 或 ActiveX 插件的虚拟控制台传递所有键击

您可以启用 **Pass all keystrokes to server（将所有键击传递到服务器）**选项并通过虚拟控制台查看器将所有键击和键组合从管理站发送到受管系统。如果它已禁用，它会直接将所有按键组合定向到正在运行虚拟控制台会话的管理站。要将所有键击传递到服务器，请在虚拟控制台查看器中，转至 **Tools（工具）** > **Session Options（会话选项）** > **General（通用）**选项卡，然后选择 **Pass all keystrokes to server（将所有键击传递到服务器）**选项，以将管理站的键击传递到受管系统。

Pass all keystrokes to server（将所有键击传递到服务器）功能的行为取决于：

- 虚拟控制台会话基于哪种插件类型（Java 或 ActiveX）启动。

  对于 Java 客户端，必须加载原生库，以便将所有键击传递给服务器并确保单光标模式正常工作。如果未加载原生库，则取消选择 **Pass all keystrokes to server（将所有键击传递到服务器）**和 **Single Cursor（单光标）**选项。如果您尝试选择这些选项之一，则会显示一条错误消息，指示所选的选项不受支持。

  对于 ActiveX 客户端，必须加载原生库，才能将所有键击传递给服务器功能，以正常工作。如果未加载原生库，则取消选择 **Pass all keystrokes to server（将所有键击传递到服务器）**选项。如果您尝试选择此选项，则会显示一条错误消息，指示该功能不受支持。

  对于 MAC 操作系统，启用 **Universal Access**（通用访问）下的 **Enable access of assistive device**（启用对辅助设备的访问）选项，Pass all keystrokes to server（将所有键击传递到服务器）功能才会起作用。

- 操作系统在管理站和受管系统上运行。对于管理站上的操作系统有意义的键组合不会传递给受管系统。
- 虚拟控制台查看器模式—Windowed（窗口）或 Full Screen（全屏）。

  在 Full Screen（全屏）模式下，**Pass all keystrokes to server**（将所有键击传递到服务器）功能在默认情况下已启用。

  在 Windowed（窗口）模式下，仅当虚拟控制台查看器可见并且活动时才会传递按键。

  从 Full Screen（全屏）模式更改为 Windowed（窗口）模式时，以前的传递所有按键的状态将恢复。

在 Windows 操作系统上运行的基于 Java 的虚拟控制台会话

- 系统不会将 Ctrl+Alt+Del 键发送到受管系统，但是始终会通过 Management Station 进行解释。
- 如果已启用 Pass All Keystrokes to Server（将所有键击传递给服务器），以下按键不会发送到受管系统：
  - 浏览器返回按键
  - 浏览器前进按键
  - 浏览器刷新按键
  - 浏览器停止按键
  - 浏览器搜索按键
  - 浏览器收藏夹按键
  - 浏览器开始和主页按键
  - 静音按键
  - 减小音量按键
  - 增大音量按键
  - 下一曲目按键
  - 上一曲目按键
  - 停止介质按键

- 播放/暂停介质按键
- 启动邮件按键
- 选择介质按键
- 启动应用程序 1 按键
- 启动应用程序 2 按键

- 所有单独的按键（不是不同按键组合，而是单次击键）将始终发送到受管系统。这包括所有功能键、Shift、Alt、Ctrl 键和菜单键。其中一些按键会同时影响管理站和受管系统。

  例如，如果管理站和受管系统运行的是 Windows 操作系统并且“Pass All Keys”（传递所有按键）已禁用，则当您按 Windows 键以打开**开始**菜单时，**开始**菜单在管理站和受管系统中都会打开。但是，如果“Pass All Keys”（传递所有按键）已启用，则**开始**菜单将仅在受管系统而非管理站上打开。

- 如果禁用 Pass All Keys（传递所有按键），则取决于按下的组合键和特殊组合由 Management Station 上的操作系统进行解释。

在 Linux 操作系统上运行的基于 Java 的虚拟控制台会话

除下面几点外，所述 Windows 操作系统的行为也适用于 Linux 操作系统：

- 如果启用 Pass all keystrokes to server（将所有键击传递给服务器），系统会将 <Ctrl+Alt+Del> 传递给受管系统上的操作系统。
- Magic SysRq 键是 Linux 内核解释的组合键。如果管理站或受管系统上的操作系统停止响应并且您需要恢复系统，它非常有用。您可以使用以下方法之一在 Linux 操作系统上启用 Magic SysRq 键：
  - 将一个条目添加到 **/etc/sysctl.conf**
  - echo "1" > /proc/sys/kernel/sysrq
- 如果启用“Pass all keystrokes to server”（将所有键击传递给服务器），系统会将 Magic SysRq 键传递给受管系统上的操作系统。重设操作系统的键顺序行为（在未卸载或同步的情况下重新引导）取决于在管理站上是已启用还是禁用 Magic SysRq 键：
  - 如果 Management Station 上已启用 SysRq，则 <Ctrl+Alt+SysRq+b> 或 <Alt+SysRq+b> 会重置 Management Station，而不管系统状态为何。
  - 如果 Management Station 上已禁用 SysRq，则 <Ctrl+Alt+SysRq+b> 或 <Alt+SysRq+b> 按键会重置受管系统上的操作系统。
  - 系统会将其他 SysRq 按键组合（例如，<Alt+SysRq+k>、<Ctrl+Alt+SysRq+m> 等）传递给受管系统，而不管 Management Station 上是否启用 SysRq 按键。

通过远程控制台使用 SysRq 魔术键

您可以使用以下任意一种方式通过远程控制台启用 SysRq 魔术键：

- Opensoure IPMI 工具
- 使用 SSH 或外部串行连接器

使用 Opensource IPMI 工具

确保 BIOS/iDRAC 设置支持使用 SOL 重定向控制台。

1. 在命令提示符下，运行 SOL 激活命令：

   ```
   Ipmitool -I lanplus -H <ipaddr> -U <username> -P <passwd> sol activate
   ```

   SOL 会话将被激活。
2. 服务器引导至操作系统后，将显示 `localhost.localdomain` 登录提示符。使用操作系统用户名和密码登录。
3. 如果 SysRq 未启用，则使用 `echo 1 >/proc/sys/kernel/sysrq` 启用它。
4. 运行中断顺序 `~B`。
5. 使用 SysRq 魔术键启用 SysRq 功能。例如，以下命令将在控制台显示内存信息：

   ```
   echo m > /proc/sysrq-trigger displays
   ```

使用 SSH 或外部串行连接器（通过串行电缆直接连接）

1. 对于 telnet/SSH 会话，使用 iDRAC 用户名和密码登录后，在 `/admin>` 提示符处运行命令 `console com2`。localhost.localdomain 提示。随机将显示 `localhost.localdomain` 提示。
2. 对于控制台重定向，通过串行电缆使用外部串行连接器直接连接到系统，在服务器引导至操作系统后，将显示登录提示 `localhost.localdomain`。
3. 使用操作系统用户名和密码登录。
4. 如果未启用 SysRq，请使用 `echo 1 >/proc/sys/kernel/sysrq` 启用。
5. 使用魔术键启用 SysRq 功能。例如，使用以下命令将重新引导服务器：

```
echo b > /proc/sysrq-trigger
```

注: 您不必运行中断顺序即可使用 SysRq 魔术键。

在 Windows 操作系统上运行的基于 ActiveX 的虚拟控制台会话

对于在 Windows 操作系统上运行的基于 ActiveX 的虚拟控制台会话，将所有按键发送到其中的服务器功能的行为与在 Windows Management Station 上运行的基于 Java 的虚拟控制台会话的所述行为类似，但下面几点除外：

- 如果禁用 Pass All Keys（传递所有按键），则按 F1 会同时启动 Management Station 和受管系统上的应用程序帮助，并显示以下消息：

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- 系统可能不会明确阻止媒体按键。
- 系统不会将 <Alt + Space>、<Ctrl + Alt + +> 和 <Ctrl + Alt + -> 发送到受管系统，这些按键组合由 Management Station 上的操作系统进行解释。

20

使用 iDRAC 服务模块

iDRAC Service Module 是一个软件应用程序，建议将其安装在服务器上（默认情况下不会安装）。此应用程序为 iDRAC 完善操作系统的监测信息。它可通过提供额外数据以用于 iDRAC 界面（例如，Web 界面、RACADM 和 WSMan）来完善 iDRAC。您可以配置受 iDRAC Service Module 监测的功能以控制服务器操作系统的 CPU 和内存占用。已引入主机操作系统命令行界面，以启用或禁用 PSU 以外的所有系统组件的完全电源重启的状态。

注: iDRAC9 使用 iSM 版本 3.01 及更高版本。

注: □在安装 iDRAC Express 或 iDRAC Enterprise/Datacenter □可□之后，才能使用 iDRAC Service Module。

使用 iDRAC 服务模块前，请确保：

- 您在 iDRAC 中拥有登录、配置和服务器控制权限，以启用或禁用 iDRAC Service Module 功能。
- 您不能禁用**使用局部 RACADM 的 iDRAC 配置**选项。
- 操作系统到 iDRAC 的直通信道可在 iDRAC 中通过内部 USB 总线启用。

注: 如果□行 LC 擦除， `idrac.Servicemodule` □可能会仍然□示旧□。

注:

- 当 iDRAC 服务模块首次运行时，默认情况下将在 iDRAC 中启用 OS 到 iDRAC 直通通道。如果在安装 iDRAC 服务模块后禁用此功能，则必须在 iDRAC 中手动启用该功能。
- 如果已通过 iDRAC 中的 LOM 启用 OS 到 iDRAC 直通通道，则无法使用 iDRAC Service Module。

主□：

安装 iDRAC 服务模块

您可以从 **dell.com/support** 下载并安装 iDRAC 服务模块。您必须拥有管理员权限，才能在服务器的操作系统上安装 iDRAC 服务模块。有关更多安装信息，请参阅 www.dell.com/idracservicemodule 上提供的 iDRAC Service Module User's Guide（iDRAC Service Module 用户指南）。

注: 此功能不适用于 Dell Precision PR7910 系统。

从 iDRAC Express 和 Basic 安装 iDRAC Service Module

在 iDRAC Service Module Setup（iDRAC Service Module 设置）页面中，单击 Install Service Module（安装 Service Module）。

1. Service Module 安装程序可用于在 iDRAC 中创建的主机操作系统和作业。
   对于 Microsoft Windows 操作系统或 Linux 操作系统，请远程或本地登录到该服务器。
2. 查找设备列表中标记为“**SMINST**”的卷，然后运行相应的脚本：
   - 在 Windows 上，打开命令提示符并运行 **ISM-Win.bat** 批处理文件。
   - 在 Linux 上，打开 shell 提示符下并运行 **ISM-Lx.sh** 脚本文件。
3. 安装完成后，iDRAC 会将服务模块显示为 **Installed（已安装）**以及安装日期。

   注: 安装程序将在 30 分钟内对主机操作系统可用。如果在 30 分钟内不启动安装，您必须重新启动 Service Module 安装。

从 iDRAC Enterprise 安装 iDRAC Service Module

1. 在 **SupportAssist Registration（SupportAssist 注册）**向导中，单击 **Next（下一步）**。
2. 在 **iDRAC Service Module Setup（iDRAC Service Module 设置）**页面中，单击 **Install Service Module（安装 Service Module）**。
3. 单击 **Launch Virtual Console（启动虚拟控制台）**，然后单击 **Continue（继续）**安全警告对话框。
4. 要查找 iSM 安装程序文件，远程或本地登录到该服务器。

   注: 安装程序将在 30 分钟内对主机操作系统可用。如果在 30 分钟内不启动安装，您必须重新启动安装。

5. 查找设备列表中标记为“**SMINST**”的卷，然后运行相应的脚本：
   - 在 Windows 上，打开命令提示符并运行 **ISM-Win.bat** 批处理文件。
   - 在 Linux 上，打开 shell 提示符下并运行 **ISM-Lx.sh** 脚本文件。
6. 按照屏幕上的说明完成安装过程。
   在 **iDRAC Service Module Setup（iDRAC Service Module 设置）**页面，**Install Service Module（安装 Service Module）**按钮将在安装完成后禁用，并且 Service Module 状态将显示为 **Running（正在运行）**。

iDRAC Service Module 支持的操作系统

有关 iDRAC Service Module 支持的操作系统的列表，请参阅 www.dell.com/idracservicemodule 上提供的 iDRAC Service Module User's Guide（iDRAC Service Module 用户指南）。

iDRAC Service Module 监测功能

iDRAC 服务模块 (iSM) 提供以下监测功能：

- Redfish 配置文件对于网络属性的支持
- iDRAC 硬重置
- 经由主机操作系统的 iDRAC 访问（实验性功能）
- 带内 iDRAC SNMP 警报
- 查看操作系统 (OS) 信息
- 将 Lifecycle Controller 日志复制到操作系统日志
- 执行自动系统恢复选项
- 安装 Windows Management Instrumentation (WMI) 管理提供程序
- 与 SupportAssist Collection 集成。这仅适用于安装有 iDRAC Service Module 2.0 版或更高版本的情况。
- 准备卸下 NVMe PCIe SSD。如需了解详情，请查看 https://www.dell.com/support/article/sln310557。
- 远程服务器重启

Redfish 配置文件对于网络属性的支持

iDRAC Service Module v2.3 或更高版本为 iDRAC 提供额外的网络属性，这些网络属性可通过来自 iDRAC 的 REST 客户端获取。有关更多详细信息，请参阅 iDRAC Redfish 配置文件支持。

操作系统信息

OpenManage Server Administrator 当前与 iDRAC 共享操作系统信息和主机名。iDRAC Service Module 提供与 iDRAC 类似的信息，例如操作系统名称、操作系统版本和完全限定域名 (FQDN)。默认情况下，已启用此监测功能。如果已在主机操作系统上安装 OpenManage Server Administrator，则不会禁用此选项。

在 iSM 版本 2.0 或更高版本中，已修正操作系统信息功能，增加了操作系统网络接口监测内容。将 iDRAC 2.00.00.00 与 iDRAC Service Module 2.0 或更高版本配合使用时，将开始监测操作系统网络接口。您可以使用 iDRAC Web 界面、RACADM 或 WSMan 查看此信息。

将 Lifecycle 日志复制到操作系统日志

在 iDRAC 中启用该功能时，您可以将 Lifecycle Controller 日志复制到操作系统日志。这类似于由 OpenManage Server Administrator 执行的系统事件日志 (SEL) 复制。已选择**操作系统日志**选项作为目标（在**警报**页面中，或者在 RACADM 或 WSMan 界面的类似页面中）的所有事件都使用 iDRAC Service Module 复制到操作系统日志中。包含在操作系统日志中的默认日志集与为 SNMP 警报或陷阱配置的日志相同。

操作系统无法正常工作时，iDRAC Service Module 还将记录发生的事件。由 iDRAC Service Module 执行的操作系统日志记录将遵循基于 Linux 的操作系统所使用的 IETF syslog 标准。

注: 从 iDRAC Service Module 2.1 版开始，Windows OS 中的 Lifecycle Controller 日志复制位置可以使用 iDRAC Service Module 安装程序进行配置。在安装 iDRAC Service Module 或修改 iDRAC Service Module 安装程序时，您可以配置该位置。

如果已安装 OpenManage Server Administrator，则已禁用此监测功能，以避免操作系统日志中出现重复的 SEL 条目。

注: 在 Microsoft Windows 中，如果 iSM 事件在系统日志下记录，而不是应用改程序日志，重新启动 Windows 事件日志服务或重新启动主机 OS。

系统自动恢复选项

自动系统恢复功能是一种基于硬件的计时器。如果出现硬件故障，则可能没有通知，但服务器将重设，就好像电源开关被激活了一样。ASR 使用计时器实现，它会持续计数。运行状况监测器频繁重新加载计数器，以防止其重置为零。如果 ASR 重置为零，则假定操作系统已锁定并且系统会自动尝试重新引导。

您可以执行系统自动恢复操作，例如在指定的时间间隔后重新引导、重启或关闭服务器。只有操作系统监督计时器已禁用，才会启用此功能。如果已安装 OpenManage Server Administrator，则已禁用此监测功能，以避免出现重复的监督计时器。

Windows Management Instrumentation 提供程序

WMI 是一组对 Windows 驱动程序模型的扩展，可提供操作系统界面，以便仪表化组件在其中提供信息和通知。WMI 是 Microsoft 实施的来自分布式管理综合小组 (DMTF) 的基于 Web 的企业管理 (WBEM) 和公用信息模型 (CIM) 标准，以管理服务器硬件、操作系统和应用程序。WMI 提供程序有助于与系统管理控制台（例如 Microsoft System Center）集成，并允许通过脚本管理 Microsoft Windows 服务器。

您可以启用或禁用 iDRAC 中的 WMI 选项。iDRAC 通过 iDRAC Service Module 显示 WMI 类，提供服务器的运行状况信息。默认情况下，WMI 信息功能已启用。iDRAC Service Module 在 iDRAC 中通过 WMI 显示 WSMan 受监测的类。类显示在 `root/cimv2/dcim` 命名空间中。

可以使用任何标准的 WMI 客户端接口对类进行访问。有关更多信息，请参阅配置文件文档。

本内容使用 **DCIM_iDRACCardString** 和 **DCIM_iDRACCardInteger** 类来说明 WMI 信息功能在 iDRAC Service Module 中提供的功能。有关受支持的类和配置文件的详情，请参阅 WSMan 配置文件说明文件，网址为 https://www.dell.com/support。

列出的属性用于配置**用户帐户**及所需的权限：

AttributeName	WSMAN-Class	权限	许可证	说明	支持的操作
用户名	DCIM_iDRACCardString	**写入权限：** ConfigUsers、登录 **读取权限：** 登录	基本	16 个用户： Users.1#UserName 到 Users.16#UserName	Enum、Get、Invoke
密码	DCIM_iDRACCardString	**写入权限：** ConfigUsers、登录 **读取权限：** 登录	基本	Users.1#Password 到 Users.16#Password	Enum、Get、Invoke
权限	DCIM_iDRACCardInteger	**写入权限：** ConfigUsers、登录 **读取权限：** 登录	基本	Users.1#Password 到 Users.16#Password	Enum、Get、Invoke

- `Enumerate` 对所提及的类的 `Get` 操作将提供属性相关数据。

- 可以通过从 **DCIM_iDRACCardService** 类调用 `ApplyAttribute` 或 `SetAttribute` 命令来设置属性。

注: 从 WSMAN 中删除了 **DCIM_Account** 类，并通过属性模型提供此功能。**DCIM_iDRACCardString** 和 **DCIM_iDRACCardInteger** 类提供类似的支持来配置 iDRAC 用户帐户。

远程 iDRAC 硬重置

通过使用 iDRAC，您可以监测支持的服务器，以了解严重的系统硬件、固件或软件问题。有时，iDRAC 可能会因各种原因变得无响应。在这种情况下，您必须关闭服务器并重设 iDRAC。要重设 iDRAC CPU，您必须关闭或打开服务器，或者执行交流电重启。

通过使用远程 iDRAC 硬重设功能，无论何时 iDRAC 变得无响应，您都可以执行远程 iDRAC 重设操作，无需交流电重启。要远程重设 iDRAC，请确保您在主机操作系统上拥有管理权限。默认情况下，远程 iDRAC 硬重设功能已启用。您可以使用 iDRAC Web 界面、RACADM 和 WSMan 执行远程 iDRAC 硬重设。

命令用法

本节提供 Windows、Linux 和 ESXi 操作系统执行 iDRAC 硬重置的命令使用方法。

- **Windows**
  - 使用本地 Windows Management Instrumentation (WMI)：
  - `winrm i iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID=" iSMExportedFunctions"`
  - 使用远程 WMI 界面：

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice?
    InstanceID="iSMExportedFunctions" -u:<admin-username> -p:<admin-password> -r:http://
    <remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck -skipCNCheck
    ```

  - 强制或非强制使用 Windows PowerShell 脚本：

    ```
    Invoke-iDRACHardReset -force

    Invoke-iDRACHardReset
    ```

  - 使用**程序菜单**快捷方式：

    为提高便利性，iSM 在 Windows 操作系统的**程序菜单**中提供快捷方式。当您选择**远程 iDRAC 硬重设**选项时，系统会提示您确认以重设 iDRAC。您确认后，iDRAC 将重设并且会显示操作的结果。

    注: 在**应用程序日志**类别下的**事件查看器**中会显示以下警告消息。此警告不需要任何进一步的措施。

    注: `A provider, ismserviceprovider, has been registered in the Windows Management Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.`

- **Linux**

  iSM 可在所有 iSM 支持的 Linux 操作系统上提供可执行命令。您可以通过使用 SSH 或同类工具登录操作系统以运行此命令。

  ```
  Invoke-iDRACHardReset

  Invoke-iDRACHardReset -f
  ```

- **ESXi**

  在所有 iSM 支持的 ESXi 操作系统上，iSM 2.3 版支持通用管理编程界面 (CMPI) 方法提供程序，以使用 WinRM 远程命令远程执行 iDRAC 重置。

  ```
  winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/
  DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID= iSMExportedFunctions -u:<root-
  username> -p:<passwd> -r:https://<Host-IP>:443/WSMan -a:basic -encoding:utf-8
  -skipCNCheck -skipCACheck -skipRevocationcheck
  ```

  注: 在重置 iDRAC 之前，VMware ESXi 操作系统不会发出确认提示。

  注: 由于 VMware ESXi 操作系统的限制，iDRAC 重设后不会完全还原连接。确保您手动重设 iDRAC。

表. 59: 错误处理

结果	说明
0	成功
1	不支持 iDRAC 重置的 BIOS 版本
2	不支持的平台
3	访问被拒
4	iDRAC 重设失败

对 iDRAC SNMP 警报的带内支持

通过使用 iDRAC Service Module 2.3 版，可以接收来自主机操作系统的 SNMP 警报（类似于 iDRAC 生成的警报）。

您也可以在不配置 iDRAC 的情况下监测 iDRAC SNMP 警报，并通过在主机操作系统上配置 SNMP 陷阱和目标远程管理服务器。在 iDRAC Service Module v2.3 或更高版本中，此功能会将操作系统日志中复制的所有生命周期日志转换为 SNMP 陷阱。

注: 该功能仅在 Lifecycle 日志重复功能启用时激活。

注: 在 Linux 操作系统上，该功能需要通过 SNMP 多路复用 (SMUX) 协议启用主要或操作系统 SNMP。

默认情况下，此功能处于禁用状态。尽管带内 SNMP 报警机制可与 iDRAC SNMP 报警机制共存，但已记录日志可能具有来自这两个源的冗余 SNMP 警报。建议使用带内或带外选项，而不是同时使用两者。

命令用法

本节提供 Windows、Linux 和 ESXi 操作系统的命令使用方法。

- **Windows 操作系统**
  - 使用本地 Windows Management Instrumentation (WMI):

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    ```

  - 使用远程 WMI 界面:

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"} -u:<admin-username> -p:<admin-
    passwd> -r:http://<remote-hostname OR IP>/WSMan -a:Basic -encoding:utf-8 -skipCACheck
    -skipCNCheck
    ```

- **Linux 操作系统**

  在所有 iSM 支持的 Linux 操作系统上，iSM 提供了可执行命令。您可以通过使用 SSH 或同类工具登录操作系统以运行此命令。

  以 iSM 2.4.0 开始时，您可以使用以下命令将 Agent-x 配置为默认协议，支持带内 iDRAC SNMP 报警:

  ```
  ./Enable-iDRACSNMPTrap.sh 1/agentx -force
  ```

  如果未指定 `-force`，确保已配置 Net-SNMP 并重新启动 snmpd 服务。

  - 要启用此功能，请执行以下操作:

    ```
    Enable-iDRACSNMPTrap.sh 1
    ```

    ```
    Enable-iDRACSNMPTrap.sh enable
    ```

- 要禁用此功能，请执行以下操作：

```
Enable-iDRACSNMPTrap.sh 0
```

```
Enable-iDRACSNMPTrap.sh disable
```

注： **--force** 选项可配置 Net-SNMP 以转发陷阱。但是，您必须配置陷阱目标。

- **VMware ESXi 操作系统**

  在所有 iSM 支持的 ESXi 操作系统上，iSM 2.3 版支持通用管理编程界面 (CMPI) 方法提供程序，以使用 WinRM 远程命令远程启用该功能。

```
winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService? __cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<user-name> -p:<passwd> -r:https://<remote-host-name
```

```
ip-address>:443/WSMan -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck @{state="[0/1]"}
```

注： 您必须为陷阱检查并配置 VMware ESXi 系统级 SNMP 设置。

注： 有关更多详细信息，请参阅位于 https://www.dell.com/support 的 **In-BandSNMPAlerts** 技术的白皮书。

通过主机操作系统访问 iDRAC

通过使用此功能，您可以使用主机 IP 地址通过 iDRAC Web 界面、WSMan 和 RedFish 界面配置和监测硬件参数，无需配置 iDRAC IP 地址。如果 iDRAC 服务器尚未配置或继续使用同一 iDRAC 凭据或者 iDRAC 服务器之前已配置，您可以使用默认的 iDRAC 凭据。

经由 Windows 操作系统的 iDRAC 访问

您可以使用以下方法之一执行此任务：

- 借助 webpack 安装 iDRAC 访问功能。
- 使用 iSM PowerShell 脚本进行配置

通过使用 MSI 安装

您可以通过使用 Web 包安装此功能。此功能在典型 iSM 安装中已禁用。如果已启用，则默认的侦听端口号是 1266。您可以在 1024 到 65535 的范围内修改此端口号。iSM 会将连接重定向至 iDRAC。然后，iSM 将创建一个入站防火墙规则 OS2iDRAC。侦听端口号添加主机操作系统中的 OS2iDRAC 防火墙规则后，将允许传入连接。此功能已启用时，防火墙规则将自动启用。

以 iSM 2.4.0 开始时，通过使用以下 Powershell cmdlet，您可以检索当前状态和监听端口配置：

```
Enable-iDRACAccessHostRoute -status get
```

此命令的输出表示是否已启用或已禁用此功能。如果已启用该功能，它会显示侦听端口号。

注： 要让此功能正常工作，请确保 Microsoft IP Helper 服务正在您的系统上运行。

要访问 iDRAC Web 界面，可在浏览器中使用格式 `https://<host-name>` 或 `OS-IP>:443/login.html`，其中：

- `<host-name>` — 安装了 iSM 并配置为通过 OS 访问 iDRAC 功能的服务器上的完整主机名。如果主机名不存在，您可以使用操作系统 IP 地址。
- `443` — 默认 iDRAC 端口号。这称为连接端口号，侦听端口号上的所有传入连接都将重定向到该端口号。您可以通过 iDRAC Web 界面、WSMAN 和 RACADM 界面修改端口号。

通过使用 iSM PowerShell cmdlet 来配置

如果安装 iSM 时禁用此功能，您可以使用 iSM 提供的以下 Windows PowerShell 命令启用该功能：

```
Enable-iDRACAccessHostRoute
```

如果已经配置了功能，您可以通过使用 PowerShell 命令以及相应的选项禁用或修改它。可用的选项如下：

- **状态** - 此参数为必填项。值不区分大小写且值可以是 **True**、**False** 或 **get**。

- **端口** - 这是侦听端口号。如果您未提供端口号，则使用默认端口号 (1266)。如果**状态**参数值为“FALSE”，那么您可忽略参数的其余部分。您必须输入一个未为此功能配置的新端口编号。新端口号设置可覆盖现有的 OS2iDRAC 带内防火墙规则，并且您可以使用新的端口号连接到 iDRAC。值的范围是 1024 到 65535。
- **IPRange** - 此参数是可选的，它提供允许通过主机操作系统连接到 iDRAC 的 IP 地址范围。IP 地址范围的格式是无类别域间路由 (CIDR) 格式，是 IP 地址和子网掩码的组合。例如，10.94.111.21/24。对 iDRAC 的访问仅限于不在范围内的 IP 地址。

注: 此功能只支持 IPv4 地址。

经由 Linux 操作系统的 iDRAC 访问

您可以通过使用 Web 包中可用的 `setup.sh` 文件安装此功能。此功能在默认或典型 iSM 安装上已禁用。要获得此功能的状态，请使用以下命令：

```
Enable-iDRACAccessHostRoute get-status
```

要安装、启用并配置此功能，请使用以下命令：

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0

禁用

<source-port> 和 <source-IP-range/source-ip-range-mask> 不是必须的。

<Enable-Flag>=1

启用

<source-port> 是必须的，<source-ip-range-mask> 是可选的。

<source-IP-range>

IP 范围采用 *<IP 地址/子网掩码>* 格式。示例：10.95.146.98/24

OpenManage Server Administrator 和 iDRAC Service Module 的共存

在系统中，OpenManage Server Administrator 和 iDRAC 服务模块可以共存，并可继续正确地独立运行。

如果您已在 iDRAC Service Module 安装期间启用监测功能，则在完成安装后，如果 iDRAC Service Module 检测到存在 OpenManage Server Administrator，则会禁用重叠的监测功能集。如果 OpenManage Server Administrator 正在运行，则 iDRAC Service Module 将在登录到操作系统和 iDRAC 后禁用重叠的监测功能。

当您以后通过 iDRAC 界面重新启用这些监测功能时，将执行相同的检查，并根据 OpenManage Server Administrator 是否正在运行来启用功能。

从 iDRAC Web 界面使用 iDRAC Service Module

要从 iDRAC Web 界面使用 iDRAC Service Module，请执行以下操作：

1. 转至 **iDRAC 设置** > **概览** > **iDRAC Service Module** > **配置服务模块**。
   将显示 **iDRAC 服务模块设置**页面。
2. 您可以查看以下项：
   - 已在主机操作系统上安装的 iDRAC 服务模块版本
   - iDRAC 中的 iDRAC 服务模块的连接状态。

   注: 当一台服务器上有多个操作系统且所有操作系统均安装了 iDRAC Service Module 时，iDRAC 仅连接所有操作系统中的最新 iSM 实例。对于其他操作系统上的较早 iSM 实例，将显示错误。要在已安装 iSM 的任何其他操作系统上将 iSM 与 iDRAC 连接，请在该特定操作系统上卸载并重新安装 iSM。
3. 要执行带外监测功能，请选择以下一个或多个选项：
   - **操作系统信息** — 查看操作系统的信息。
   - **在操作系统日志中复制生命周期日志** — 将 Lifecycle Controller 日志包括到操作系统日志中。如果已在系统上安装 OpenManage Server Administrator，将禁用此选项。
   - **WMI 信息** — 包括 WMI 信息。
   - **自动系统恢复操作** — 在指定时间（以秒为单位）后在系统上执行自动恢复操作：

- **重新引导**
- **关闭系统电源**
- **系统电源关闭后重启**

如果已在系统上安装 OpenManage Server Administrator，将禁用此选项。

从 RACADM 中使用 iDRAC Service Module

要从 RACADM 使用 iDRAC Service Module，请使用 `ServiceModule` 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

21

使用 USB 端口进行服务器管理

在第 14 代服务器上，可使用专用 Micro USB 端口来配置 iDRAC。使用 Micro USB 端口可执行以下功能：

- 使用 USB 网络接口连接到系统以访问系统管理工具，例如 iDRAC Web 界面和 RACADM。
- 通过使用存储在 USB 驱动器上的 SCP 文件配置服务器。

注： 要管理 USB 端口，或者通□在 USB □□器上□入服□器配置文件 (SCP) 文件来配置服□器，您必□具有系□控制权限。

注： 插入 USB □□□，将生成警□/□告。此功能□在基于 Intel 的服□器上可用。

要配置管理 USB 设置，请转至 **iDRAC 设置** > **设置** > **管理 USB 设置**。以下选项可用：

- **USB 管理端口** - 选择**已启用**以启用端口在连接 USB 驱动器时导入 SCP 文件，或使用 Micro USB 端口访问 iDRAC。

  注： 请确保 USB 驱动器包含有效的 SCP 文件。

  注： 使用 OTG 适配器从 Type-A 转换为 Micro-B USB。不支持从 USB 集线器进行连接。
- **iDRAC 管理：USB SCP** - 选择以下任一种选项，以通过导入存储在 USB 驱动器上的 SCP 文件来配置系统。
  - **已禁用**- 禁用 SCP 导入
  - **仅当服务器具有默认凭据设置时启用** - 如果选中此选项，则对于下列选项，仅当未更改默认密码时才能导入 SCP：
    - BIOS
    - iDRAC Web 界面
  - **仅针对压缩的配置文件启用** - 选择此选项以仅在文件处于压缩格式时才允许 SCP 文件导入。

    注： 选择此选项允许您密码保护压缩的文件。您可以使用 **Zip 文件的密码**选项输入密码来保护该文件。
  - **已启用** - 选择此选项将允许在运行时期间导入 SCP 文件而不运行检查。

主□：

- 通□直接 USB □接□□ iDRAC 界面
- 使用 USB □□上的服□器配置文件配置 iDRAC

通过直接 USB 连接访问 iDRAC 界面

iDRAC Direct 功能允许您直接将膝上型计算机直接连接到 iDRAC 的 USB 端口。此功能允许您直接与 iDRAC 界面（如 Web 界面、RACADM 和 WSMan）交互以执行高级服务器管理和维护操作。

有关支持的浏览器及操作系统的列表，请参阅 *iDRAC 发行说明，网址：*https://www.dell.com/idracmanuals。

注： 如果您使用的是 Windows 操作系统,您可能需要安装一个 RNDIS 驱动程序以使用此功能。

要通过 USB 端口访问 iDRAC 界面，请执行以下操作：

1. 关闭所有无线网络，并断开与其它任何硬连线的网络的连接。
2. 请确保已启用 USB 端口。有关更多信息，请参阅 配置 USB 管理端口设置 页面上的 274。
3. 等待膝上型计算机以获取 IP 地址 169.254.0.4。可能需要数秒钟以获取 IP 地址。iDRAC 服务器获取 IP 地址 169.254.0.3。
4. 开始使用 iDRAC 网络界面，例如 Web 界面、RACADM、Redfish 或 WSMan。
   例如，要访问 iDRAC Web 界面，请打开一个支持的浏览器，键入地址 *169.254.0.3*，然后按 Enter 键。
5. 当 iDRAC 使用 USB 端口时，LED 将闪烁以表示处于活动状态。闪烁频率是每秒四次。
6. 完成所需操作后，从系统处断开 USB 电缆。
   然后 LED 将关闭。

使用 USB 设备上的服务器配置文件配置 iDRAC

通过 iDRAC USB 管理端口，您可以对 iDRAC 进行服务器配置。在 iDRAC 中配置 USB 管理端口设置，并插入含有服务器配置文件的 USB 设备，然后将 USB 设备中的服务器配置文件导入到 iDRAC。

注: 只有在没有任何 USB □□□接服□器□，才能使用 iDRAC 接口□定 USB 管理端口□置。

配置 USB 管理端口设置

您可以使用系统 BIOS 启用或禁用 iDRAC Direct USB 端口。导航至**系统 BIOS** > **集成设备**。选择**打开**可启用，选择**关闭**可禁用 iDRAC Direct USB 端口。

在 iDRAC 中，您必须具有服务器控制权限才能配置 USB 管理端口。在连接 USB 设备后，**系统清单清册**页面将在"硬件资源清册"部分下显示 USB 设备信息。

在下列情况下，将在 Lifecycle Controller 日志中记录一个事件：
- 设备处于"自动"或 iDRAC 模式，并且 USB 设备已插入或移除。
- USB 管理端口模式已修改。
- 设备自动从 iDRAC 切换到操作系统。
- 设备从 iDRAC 或操作系统弹出

当设备超出 USB 规格所允许的电源要求时，此设备将断开连接，并且会通过以下属性生成过电流事件：
- 类别：系统运行状况
- 类型：USB 设备
- 严重级别：警告
- 允许的通知：电子邮件、SNMP 陷阱、远程系统日志和 WS 事件
- 操作：无

在下列情况下，将显示错误消息并将其记录到 Lifecycle Controller 日志：
- 您在无"服务器控制"用户权限的情况下尝试配置 USB 管理端口。
- USB 设备正由 iDRAC 使用，并且您尝试修改 USB 管理端口模式。
- USB 设备正由 iDRAC 使用，并且您移除设备。

使用 Web 界面配置 USB 管理端口

要配置 USB 端口，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **iDRAC 设置** > > **管理 USB 设置**。
2. **USB 管理端口**设置为已启用。
3. 从 **iDRAC 管理：USB SCP** 配置下拉菜单中选择选项以配置服务器（通过导入存储在 USB 驱动器上的服务器配置文件实现）：
   - **已禁用**
   - **仅当服务器具有默认凭据设置时启用**
   - **仅启用压缩的配置文件**
   - **已启用**

   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

   注: 在您选择"仅针对压缩的配置文件启用"以在导入前压缩文件之后，iDRAC9 允许您使用密码保护压缩的文件。您可以使用"Zip 文件的密码"选项输入密码来保护该文件。
4. 单击**应用**应用设置。

使用 RACADM 配置 USB 管理端口

要配置 USB 管理端口，请使用以下 RACADM 子命令和对象：
- 要查看 USB 端口状态：

```
racadm get iDRAC.USB.PortStatus
```

- 要查看 USB 端口配置：

```
racadm get iDRAC.USB.ManagementPortMode
```

- 要查看 USB 设备的资源清册：

```
racadm hwinventory
```

- 要在当前警报配置上进行设置：

```
racadm eventfilters
```

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置 USB 管理端口

要配置 USB 端口，请执行以下操作：

1. 在 iDRAC 设置公用程序中，转至**介质和 USB 端口设置**。
   将显示 **iDRAC 设置介质和 USB 端口设置**页面。
2. 从 **iDRAC Direct：USB 配置 XML** 下拉菜单中选择选项以配置服务器（通过导入存储在 USB 驱动器中的服务器配置文件实现）：
   - **已禁用**
   - **仅当服务器具有默认凭据设置时启用**
   - **仅启用压缩的配置文件**
   - **已启用**

   有关各字段的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 单击**上一步**、**完成**，然后单击**是**以应用设置。

从 USB 设备导入服务器配置文件

确保在 USB 设备的根目录中创建一个名称为 `System_Configuration_XML` 的目录，该目录包含 config 和 control 文件：

- 服务器配置文件 (SCP) 位于 USB 设备根目录下的 `System_Configuration_XML` 子目录中。此文件中包含服务器的所有属性值对。其中包括 iDRAC、PERC、RAID 和 BIOS 的属性。您可以编辑此文件以配置服务器上的任何属性。文件名可以是 `<servicetag>-config.xml`、`<servicetag>-config.json`、`<modelnumber>-config.xml`、`<modelnumber>-config.json`、`config.xml` 或 `config.json`。
- 控制文件 - 包括一些参数以控制导入操作，不包括 iDRAC 或系统中任何其它组件的属性。此控制文件中包含三个参数：
  - ShutdownType - 正常、强制、不重新引导。
  - TimeToWait（秒）- 最小值为 300，最大值为 3600。
  - EndHostPowerState - 开/关。

`control.xml` 文件示例：

```
<InstructionTable>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>ShutdownType</Instruction>
     <Value>NoReboot</Value>
     <ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>TimeToWait</Instruction>
     <Value>300</Value>
     <ValuePossibilities>Minimum value is 300 -Maximum value is
      3600 seconds.</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>EndHostPowerState</Instruction>
```

```
      <Value>On</Value>
      <ValuePossibilities>On,Off</ValuePossibilities>
   </InstructionRow>
</InstructionTable>
```

您必须具有服务器控制权限才能执行此操作。

注: 在导入 SCP 时，如更改 SCP 文件中的 USB 管理设置，会导致作业失败或作业虽完成但发生了错误。您可以对 SCP 中的属性添加注释，以避免错误的发生。

要将服务器配置文件从 USB 设备导入 iDRAC：

1. 配置 USB 管理模块：
   - 将 **USB 管理端口模式**设置为**自动**或 **iDRAC**。
   - 将 **iDRAC 管理：USB XML 配置**设置为**使用默认凭据启用**或**启用**。
2. 将包含 `configuration.xml` 和 `control.xml` 文件的 USB 闪存盘插入 iDRAC USB 端口。

   注: XML 文件的文件名称和文件类型是区分大小写的。确保二者都是小写。
3. 将在 USB 设备根目录下的 `System_Configuration_XML` 子目录中发现服务器配置文件。按照以下顺序发现该文件：
   - `<servicetag>-config.xml` / `<servicetag>-config.json`
   - `<modelnum>-config.xml` / `<modelnum>-config.json`
   - `config.xml` / `config.json`
4. 服务器配置文件导入作业将开始。

   如果未找到此配置文件，操作会停止。

   如果 **iDRAC 管理：USB XML 配置**已设置为**使用默认凭据启用**并且 BIOS 设置密码不为空，或者如果其中一个 iDRAC 用户帐户已被修改，则会显示一条错误消息并停止操作。
5. LCD 面板和 LED（如果有）会显示状态 - 已启动导入作业。
6. 如果存在需分阶段的配置，并且控制文件中的**关闭类型**已指定为**不重新引导**，则必须重新引导服务器以配置设置。否则，服务器将重新引导，并应用配置。仅当服务器已关闭时，会应用已分阶段的配置，即使已指定**不重新引导**选项。
7. 在导入作业完成后，LCD/LED 将指示该作业已完成。如果需要重新引导，LCD 将该任务的状态显示为“暂停，等待重新引导”。
8. 如果 USB 设备仍插入在服务器中，则导入操作的结果会记录在 USB 设备中的 `results.xml` 文件中。

LCD 消息

如果 LCD 面板可用，它将按顺序显示以下消息：

1. 导入 - 正在从 USB 设备复制服务器配置文件时。
2. 应用 - 作业正在执行时。
3. 已完成 - 作业已成功完成时。
4. 已完成但发生错误 - 作业已完成但发生错误时。
5. 已失败 - 作业已失败。

有关更多详细信息，请参阅 USB 设备上的结果文件。

LED 闪烁行为

USB LED 指示正在使用 USB 端口执行的服务器配置文件操作的状态。此 LED 可能不适用于所有系统。

- 呈绿色稳定亮起 - 正在从 USB 设备复制服务器配置文件。
- 呈绿色闪烁 - 正在执行作业。
- 呈琥珀色闪烁 - 作业失败，或已完成但有错误。
- 呈绿色稳定亮起 - 作业已成功完成。

注: 在 PowerEdge R840 和 R940xa 中，如果存在 LCD，当使用 USB 端口进行导入操作时，USB LED 不会闪烁。使用 LCD 检查操作状态。

日志文件和结果文件

将为导入操作记录以下信息：

- 将在 Lifecycle Controller 日志文件中记录从 USB 执行自动导入的操作。
- 如果 USB 设备保持为插入状态，会在 USB 闪存盘上的结果文件中记录作业结果。

将在子目录中更新或创建一个名为 `Results.xml` 的结果文件，其中包含以下信息：

- 服务标签 - 在导入操作返回作业 ID 或返回错误之后记录数据。
- 作业 ID - 在导入操作返回作业 ID 之后记录数据。
- 作业的开始日期和时间 - 在导入操作返回作业 ID 之后记录数据。
- 状态 - 在导入操作返回作业 ID 或在任务结果可用时记录数据。

22

使用 Quick Sync 2

利用在 Android 或 iOS 移动设备上运行的 Dell OpenManage Mobile，您可以轻松地直接访问或通过 OpenManage Essentials 或 OpenManage Enterprise (OME) 控制台访问服务器。它允许您查看服务器详情和清单、查看 LC 和系统事件日志、从 OME 控制台获得有关移动设备的自动通知、分配 IP 地址和修改 iDRAC 密码、配置主要 BIOS 属性，以及按需采取修复措施。您也可以重启服务器、访问系统控制台或访问 iDRAC GUI。

OMM 可以从 Apple App Store 或 Google Play Store 免费下载。

您必须在移动设备上安装 OpenManage Mobile 应用程序（支持 Android 5.0+ 和 iOS 9.0+ 移动设备）以使用 iDRAC Quick Sync 2 界面管理服务器。

注： 本部分□□示于在机架耳上具有 Quick Sync 2 模□的服□器中。

注： 此功能目前在采用 Android 操作系□和 Apple iOS 的移□□□上受支持。

在当前版本中，此功能在所有第 14 代 PowerEdge 服务器上都可用。它需要 Quick Sync 2 左侧控制面板（嵌入在**左侧机架吊耳**中）和已启用低功耗蓝牙（以及 Wi-Fi）的移动设备。因此，它是硬件上行销售，并且功能不依赖 iDRAC 软件许可。

注： 有关在 MX 平台系□中配置 Quick Sync2 的□□信息，□参□《*OpenManage Enterprise 模块化用户指南*》和《*OpenManage Mobile 用户指南*》，网址：**dell.com/support/manuals**。

iDRAC Quick Sync 2 配置过程：

注： 不适用于 MX 平台。

配置 Quick Sync 后，将激活左侧控制面板上的 Quick Sync 2 按钮。确保 Quick Sync 2 指示灯亮起。通过移动设备访问 Quick Sync 2 信息（Android 5.0+ 或 IOS 9.0+、OMM 2.0 或更高版本）。

通过 OpenManage Mobile，可以执行以下操作：

- 查看清单信息
- 查看监视信息
- 配置基本 iDRAC 网络设置

有关 OpenManage Mobile 的详细信息，请参阅 *Dell EMC OpenManage Mobile 用户指南，网址：*https://www.dell.com/openmanagemanuals。

主□：

配置 iDRAC Quick Sync 2

通过使用 iDRAC Web 界面、RACADM、WSMan 和 iDRAC HII，您可以配置 iDRAC Quick Sync 2 功能以访问移动设备：

- **访问** - 配置为读写、只读和已禁用。读写是默认选项。
- **超时** - 配置为已启用或已禁用。默认选项是已启用。
- **超时限制** - 表示禁用 Quick Sync 2 模式之后的时间。默认选择为秒。默认值是 120 秒。范围为 120 到 3600 秒。
  1. 如果已启用，您可以指定在关闭 Quick Sync 2 模式之后的时间。要打开，请再次按重新激活按钮。
  2. 如果已禁用，计时器将不允许您输入超时的时长。
- **读取验证** - 配置为“已启用”，这是默认选项。
- **WiFi** - 配置为“已启用”，这是默认选项。

您必须具有“服务器控制”权限才能配置这些设置。无需重新引导系统以使设置生效。配置之后，您可以在左侧控制面板上激活 Quick Sync 2 按钮。确保 Quick Sync 指示灯亮起。然后，通过移动设备访问 Quick Sync 信息。

在配置发生修改时，会在 Lifecycle Controller 日志中记录一个条目。

使用 Web 界面配置 iDRAC Quick Sync 2 设置

要配置 iDRAC Quick Sync 2：

1. 在 iDRAC Web 界面中,转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **iDRAC Quick Sync。**
2. 在 **iDRAC Quick Sync** 部分中，从 **Access（访问）**下拉菜单中选择下列选项之一以访问 Android 或 iOS 移动设备：
   - Read-write（读写）
   - Read-only（只读）
   - 已禁用
3. 启用计时器。
4. 指定超时限制。
   有关各字段的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
5. 单击**应用**应用设置。

使用 RACADM 配置 iDRAC 快速同步 2 设置

要配置 iDRAC 快速同步 2 功能，请使用 **System.QuickSync** 组中的 racadm 对象。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置 iDRAC Quick Sync 2 设置

要配置 iDRAC Quick Sync 2：

1. 在 iDRAC GUI 中,转至 **Configuration（配置）** > **Systems Settings（系统设置）** > **Hardware Settings（硬件设置）** > **iDRAC Quick Sync。**
2. 在 **iDRAC 快速同步**部分中：
   - 指定访问级别。
   - 启用超时。
   - 指定用户定义的超时限制（范围是 120 到 3600 秒）。

   有关各字段的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   将应用设置。

使用移动设备查看 iDRAC 信息

要从移动设备查看 iDRAC 信息，请参阅步骤中的 *Dell EMC OpenManage Mobile 用户指南，网址：*https://www.dell.com/openmanagemanuals。

23

管理虚拟介质

iDRAC 使用具有本地 ISO 和 IMG 文件、远程 ISO 和 IMG 文件支持的基于 HTML5 的客户端提供虚拟介质。虚拟介质允许受管服务器访问 Management Station 上的介质设备或者网络共享的 ISO CD/DVD 映像，就好像是受管服务器上的设备一样。您需要具有 iDRAC 配置权限才能修改配置。

以下是可配置的属性：

- 已连接介质启用 — 已启用/已禁用
- 连接模式 — 自动连接、连接和断开
- 最大会话数 — 1
- 活动会话数 — 1
- 虚拟介质加密 — 已启用（默认）
- 软盘仿真 — 已禁用（默认）
- 启动一次 — 已启用/已禁用
- 连接状态 — 已连接/已断开

使用虚拟介质功能，您可以：

- 通过网络远程访问连接到远程系统的介质
- 安装应用程序
- 更新驱动程序
- 在受管系统上安装操作系统

这是适用于机架式和塔式服务器的许可功能。对于刀片式服务器，该功能默认可用。

主要功能有：

- 虚拟介质支持虚拟光驱 (CD/DVD) 和 USB 闪存盘。
- 您只能在受管系统的 Management Station 上附加一个 USB 闪存盘、映像、密钥或一个光盘驱动器。支持的光盘驱动器包括最多一个可用的光盘驱动器或 ISO 映像文件。

  下图显示了典型的虚拟介质设置。

- 在受管系统上，任何连接的虚拟介质都会模拟物理设备。
- 在基于 Windows 的受管系统上，如果虚拟介质驱动器已附加并配置驱动器号，则会自动加载。
- 在具有某些配置的基于 Linux 的受管系统上，虚拟介质驱动器不会自动加载。要手动加载驱动器，请使用加载命令。
- 从受管系统发出的所有虚拟驱动器访问请求都会通过网络转发至 Management Station。
- 在驱动器中没有安装介质的受管系统上，虚拟设备会显示为两个驱动器。
- 您可以在两个受管系统间共享 Management Station CD/DVD 驱动器（只读），但不能共享 USB 介质。
- 虚拟介质至少需要 128 Kbps 的可用网络带宽。
- 如果 LOM 或 NIC 失败，虚拟介质会话可能会断开。

通过虚拟控制台连接虚拟介质映像后，驱动器可能无法显示在 Windows 主机操作系统中。在 Windows 设备管理器中检查所有未知大容量存储设备。右键单击未知设备并更新驱动程序，或选择卸载驱动程序。在断开并重新连接 vMedia 后，该设备将被 Windows 识别。

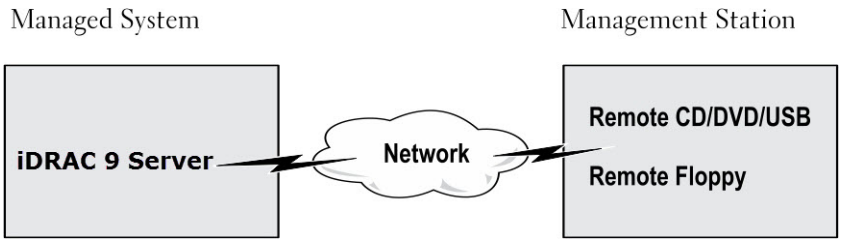


图 4: 虚拟介质设置

主□：

- 支持的□□器和□□

- 配置虚□介□
- □□虚□介□
- 通□ BIOS □置引□□序
- 启用一次性虚□介□引□

支持的驱动器和设备

下表列出了通过虚拟介质支持的驱动器。

表. 60: 支持的驱动器和设备

驱动器	支持的存储介质
虚拟光驱	• CD-ROM • DVD • CD-RW • 带有 CD-ROM 介质的复合驱动器
USB 闪存盘	• 带有 CD-ROM 介质的 USB CD-ROM 驱动器 • ISO9660 格式的 USB 闪存盘映像文件

配置虚拟介质

配置虚拟介质设置前，确保已配置 Web 浏览器以使用 Java 或 ActiveX 插件。

使用 iDRAC Web 界面配置虚拟介质

要配置虚拟介质设置：

小心: 运行虚拟介质会话时请勿重设 iDRAC。否则会产生不良后果，包括数据丢失。

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **Virtual Media（虚拟界面）** > **Attached Media（连接的介质）**。
2. 指定所需的设置。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击 **Apply**（应用）保存设置。

使用 RACADM 配置虚拟介质

要配置虚拟介质，使用 `set` 命令以及 **iDRAC.VirtualMedia** 组中的对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序配置虚拟介质

可使用 iDRAC 设置公用程序附加、分离或自动附加虚拟介质。要执行此操作：

1. 在 iDRAC 设置公用程序中，转至**介质和 USB 端口设置**。
   将显示 **iDRAC 设置介质和 USB 端口设置**页面。
2. 在 **Virtual Media（虚拟介质）**部分，根据要求选择 **Detach（拆离）**、**Attach（附加）**或 **Auto Attach（自动附加）**。有关选项的更多信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   虚拟介质设置即完成配置。

连接的介质状态和系统响应

下表说明了基于附加介质设置的系统响应。

表. 61: 连接的介质状态和系统响应

附加的介质状态	系统响应
分离	无法将映像映射到系统。
附加	关闭 **Client View（客户端视图）**时甚至也可以映射介质。
自动分离	**Client View（客户端视图）**打开时映射介质，**客户端视图**关闭时不映射。

用于查看虚拟介质中虚拟设备的服务器设置

您必须配置的管理站中的以下设置以允许空驱动器可见。要执行此操作，请在 Windows 资源管理器中的 **Organize（组织）**菜单中，单击 **Folder and search options（文件夹和搜索选项）**。在 **View（视图）**选项卡中，取消选中 **Hide empty drives in the Computer folder（隐藏计算机文件夹中的空驱动器）**选项并单击 **OK（确定）**。

访问虚拟介质

您可以使用或不使用虚拟控制台访问虚拟介质。访问虚拟介质之前，务必要配置您的 Web 浏览器。

虚拟介质与 RFS 是互斥的。如果 RFS 连接处于活动状态，那么当您尝试启动虚拟介质客户端时，屏幕上将显示以下错误信息：*Virtual Media is currently unavailable（虚拟介质当前不可用）。A Virtual Media or Remote File Share session is in use.（虚拟介质或远程文件共享会话正在使用中。）*

如果 RFS 连接处于非活动状态，那么当您尝试启动虚拟介质客户端时，可以成功启动客户端。然后您可以使用虚拟介质客户端将设备和文件映射到虚拟介质虚拟驱动器。

使用虚拟控制台启动虚拟介质

通过虚拟控制台启动虚拟介质前，请确保：

- 已启用虚拟控制台。
- 系统配置为不隐藏空驱动器 — 在 Windows 资源管理器中，导航到 **Folder Options（文件夹选项）**，并清除 **Hide empty drives in the Computer folder（隐藏计算机文件夹中的空驱动器）**选项，然后单击 **OK（确定）**。

要使用虚拟控制台访问虚拟介质：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **Virtual Console（虚拟控制台）**。
   将显示 **Virtual Console（虚拟控制台）**页面。
2. 单击 **Launch Virtual Console**（启动虚拟控制台）。
   Virtual Console Viewer（虚拟控制台查看器）即会启动。
   注: 在 Linux 上，JAVA 是用于访问虚拟控制台的默认插件类型。在 Windows 上，打开 `.jnlp` 文件以使用 Java 启动虚拟控制台。
3. 单击 **Virtual Media（虚拟介质）** > **Connect Virtual Media（连接虚拟介质）**。
   将建立虚拟介质会话，并且 **Virtual Media（虚拟介质）**菜单将显示可映射的设备的列表。
   注: 访问虚拟介质时，**Virtual Console Viewer（虚拟控制台查看器）**窗口必须保持活动。

不使用虚拟控制台启动虚拟介质

当禁用**虚拟控制台**时，在启动虚拟介质之前，请确保已将系统配置为显示空驱动器。要执行此操作，请在 Windows 资源管理器中转至**文件夹选项**，清除**隐藏计算机文件夹中的空驱动器**选项，然后单击**确定**。

当禁用虚拟控制台时，要访问虚拟介质：

1. 在 iDRAC Web 界面中，转至**配置** > **虚拟介质**。
2. 单击**连接虚拟介质**。

或者，您也可以通过这些步骤启动虚拟介质：

1. 转至**配置** > **虚拟控制台**。

2. 单击**启动虚拟控制台**。系统将显示以下消息：

```
Virtual Console has been disabled. Do you want to continue using Virtual Media
redirection?
```

3. 单击**确定**。此时将显示**虚拟介质**窗口。
4. 在**虚拟介质**菜单中，单击**映射 CD/DVD** 或**映射可移动磁盘**。有关更多信息，请参阅映射虚拟驱动器。
5. **虚拟介质统计信息**显示目标驱动器的列表、其映射、状态（只读或非只读）、连接持续时间、读/写字节和传输速率。

注: 受管系统上的虚拟设备驱动器号与 Management Station 上的物理驱动器号不一致。

注: 在运行 Windows 操作系统的系统上，如果启用 Internet Explorer Enhanced Security（Internet Explorer 增强的安全配置），虚拟介质可能无法正常工作。要解决此问题，请参阅 Microsoft 操作系统文档或联系系统管理员。

添加虚拟介质映像

您可以创建远程文件夹的介质映像，并将其作为 USB 设备连接至服务器的操作系统。要添加虚拟介质映像，请执行以下操作：

1. 单击 **Virtual Media（虚拟介质）** > **Create Image...（创建映像...）**。
2. 在 **Source Folder（源文件夹）**字段中，单击 **Browse（浏览）**，然后指定要用作映像文件源的文件或目录。管理站上的映像文件或受管系统上的 C: 驱动器。
3. 在**映像文件名称**字段中，会显示用于存储所创建映像文件的默认路径（通常是桌面目录）。要更改该位置，请单击 **Browse（浏览）**并浏览到位置。
4. 单击**创建映像**。

   映像创建过程将启动。如果映像文件位于源文件夹中，系统会显示警告消息，指示映像文件位于源文件夹内导致无限循环，因此映像创建无法继续。如果映像文件不在源文件夹内，则映像创建会继续。

   创建映像之后，系统会显示成功消息。
5. 单击**完成**。

   ISO 映像即已创建。

   作为映像添加文件夹时，系统会在管理站的桌面上创建 **.img** 文件以使用此功能。如果移动或删除此 .img 文件，那么在 **Virtual Media（虚拟介质）**菜单下此文件夹中相应的条目不起作用。因此，建议正在使用映像时不要移动或删除 **.img** 文件。但是，**.img** 文件可以在第一次取消选中相关条目后被移除，然后使用 **Remove Image（移除映像）**以移除条目。

查看虚拟设备详细信息

要查看虚拟设备详细信息，请在虚拟控制台查看器中，单击 **Tools（工具）** > **Stats（统计信息）**。在 **Stats（统计信息）**窗口中，**Virtual Media（虚拟介质）**部分将显示映射的虚拟设备以及每台设备的读/写活动。如果虚拟介质已连接，将显示此信息。如果没有连接虚拟介质，将显示"未连接虚拟介质"消息。

如果在未使用虚拟控制台的情况下启动虚拟介质，则 **Virtual Media（虚拟介质）**部分将显示为一个对话框，会提供关于已映射设备的信息。

访问驱动程序

Dell EMC PowerEdge 服务器已将所有受支持的操作系统驱动程序嵌入在系统闪存中。使用 iDRAC，您可以轻松地装载或卸载驱动程序，以在您的服务器上部署操作系统。

要装载驱动程序，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**配置** > **虚拟介质**。
2. 单击**装载驱动程序**。
3. 从弹出窗口中选择操作系统，然后单击**装载驱动程序**。

   注: 默认情况下，"公开"持续时间是 18 小时。

要在装载完成后卸载驱动程序，请执行以下操作：

1. 转至**配置** > **虚拟介质**。
2. 单击**卸载驱动程序**。
3. 在弹出窗口中单击**确定**。

注: 如果□□程序包在系□上不可用，□可能不会□示**装载驱动程序**□□。确保从 https://www.dell.com/support 中下□并安装最新的□□程序包。

重设 USB

要重置 USB 设置：

1. 在虚拟控制台查看器中，单击 **Tools（工具）** > **Stats（统计信息）**。
   将显示 **Stats（统计信息）**窗口。
2. 在 **Virtual Media（虚拟介质）**下，单击 **USB Reset（USB 重设）**。
   系统会显示一条消息来警告用户，如果重置 USB 连接，则会影响目标设备的所有输入，包括虚拟介质、键盘和鼠标。
3. 单击**是**。
   USB 随即会重置。

   注: 即使您注销 iDRAC Web 界面会话，iDRAC 虚拟介质也不会终止。

映射虚拟驱动器

要映射虚拟驱动器：

注: 在使用基于 ActiveX 或基于 Java 的虚拟介质时，您必须拥有管理权限才能映射操作系统 DVD 或 USB 闪存驱动器（即连接到管理站）。要映射驱动器，以管理员身份启动 IE 或将 iDRAC IP 地址添加到信任站点列表中。

1. 要建立虚拟介质会话，请从**虚拟介质**菜单中单击**连接虚拟介质**。
   对于每个允许从主机服务器映射的设备，都会在**虚拟介质**菜单下方显示一个菜单项。该菜单项是根据设备类型命名的，例如：
   - 映射 CD/DVD
   - 映射可移动磁盘

   映射 DVD/CD 选项可以用于 ISO 文件，**映射可移动磁盘**选项可用于映像。

   注:
   - 您无法通过使用基于 HTML5 的虚拟控制台映射物理介质，例如基于 USB 的驱动器、CD 或 DVD。
   - 您无法通过 RDP 会话使用虚拟控制台/虚拟介质将 USB 闪存盘映射为虚拟磁盘。
   - 您不能在 ehtml 可移动介质中映射 NTFS 格式的物理介质，请使用 FAT 或 exFAT 设备
2. 单击您要映射的设备类型。

   注: 如果虚拟介质会话当前为活动状态（既可以来自当前 Web 接口会话，也可以来自任何另一个 Web 接口会话，则会显示活动会话。
3. 在**驱动器/映像文件**字段中，从下拉列表中选择设备。
   列表中包含所有可映射的可用（未映射）设备（CD/DVD、可移动磁盘）以及可映射的映像文件类型（ISO 或 IMG）。映像文件位于默认映像文件目录（通常为用户桌面）中。如果设备不在下拉列表中，请单击**浏览**指定设备。

   对于 CD/DVD，正确的文件类型是 ISO；对于可移动磁盘，则为 IMG。

   如果在默认路径（桌面）中创建映像，当您选择**映射可移动磁盘**时，可在下拉菜单中选择已创建的映像。

   如果在不同的位置创建映像，则在选择**映射可移动磁盘**时，无法在下拉菜单中选择已创建的映像。单击**浏览**以指定映像。

   注:
   - 在基于 ehtml5 的 JAVA 可移动介质中，**只读**选项将显示为灰色。
   - ehtml5 插件不支持软盘仿真。
4. 选择**只读**可以将可写设备映射为只读设备。
   对于 CD/DVD 设备，默认情况下启用该选项并且无法禁用。

   注: 如果您使用 HTML5 虚拟控制台映射 ISO 和 IMG 文件，则会将它们作为只读文件映射。
5. 单击**映射设备**以将设备映射到主机服务器。

映射设备/文件后，其**虚拟介质**菜单项的名称会发生变化，以指示设备名称。例如，如果已将 CD/DVD 设备映射到名为 `foo.iso` 的映像文件，则“虚拟介质”菜单中的 CD/DVD 菜单项命名为 **foo.iso 映射到 CD/DVD**。该菜单项会有一个复选标记指示其已被映射。

显示正确的虚拟驱动器用于映射

在基于 Linux 的管理站上，虚拟介质**客户端**窗口可显示可移动磁盘，它们不属于管理站。要确保有正确的虚拟驱动器可以映射，必须启用已连接 SATA 硬盘驱动器的端口设置。要执行此操作：

1. 重新引导管理站上的操作系统。在开机自检过程中，按 <F2> 键进入**系统设置**。
2. 转至 **SATA 设置**。随即会显示端口详细信息。
3. 启用实际存在并已连接到硬盘驱动器的端口。
4. 访问虚拟介质**客户端**窗口。该窗口显示可映射的正确驱动器。

取消映射虚拟驱动器

要取消映射虚拟驱动器：

1. 在 **Virtual Media**（虚拟介质）菜单中，执行以下任一操作：
   - 单击要取消映射的设备。
   - 单击 **Disconnect Virtual Media**（断开虚拟介质）。

   系统会显示请求确认消息。
2. 单击**是**。
   该菜单项的复选标记会消失，以指示未映射到主机服务器。

   注: 从运行 Macintosh 操作系统的客户端系统取消映射连接到 vKVM 的 USB 设备后，取消映射的设备在客户端上可能不可用。重新启动系统或在客户端系统上手动装在设备以查看设备。

注: 要取消映射 Linux 操作系统上的虚拟 DVD 驱动器，请卸载驱动器并将其弹出。

通过 BIOS 设置引导顺序

使用系统 BIOS 设置公用程序，您可以将受管系统 设置为从虚拟光盘驱动器或虚拟软盘驱动器引导。

注: 在连接期间更改虚拟介质会停止系统引导顺序。

要使受管系统开始引导：

1. 引导受管系统。
2. 按 <F2> 进入 **System Setup（系统设置）**页面。
3. 转至 **System BIOS Settings（系统 BIOS 设置）** > **Boot Settings（引导设置）** > **BIOS Boot Settings（BIOS 引导设置）** > **Boot Sequence（引导顺序）**。
   在弹出窗口中，虚拟光盘驱动器和虚拟软盘驱动器与标准引导设备列在一起。
4. 确保虚拟驱动器已启用并列为可引导介质的第一个设备。如果需要，请遵循屏幕上的说明修改引导顺序。
5. 单击**确定**，返回**系统 BIOS 设置**页面，然后单击**完成**。
6. 单击 **Yes（是）**保存更改并退出。

   受管系统重新引导。

   受管尝试 根据引导顺序从可引导设备引导。如果虚拟设备已连接并且有可引导介质，系统会引导至该虚拟设备。否则，系统会忽略此设备 — 类似于没有可引导介质的物理设备。

启用一次性虚拟介质引导

在连接远程虚拟介质设备之后，您只能更改一次引导顺序。

在启用一次性引导选项之前，请确保：

- 您具有 *Configure User*（配置用户）权限。
- 使用 Virtual Media（虚拟介质）选项，将本地或虚拟驱动器（CD/DVD、软盘或 USB 闪存设备）映射到可引导介质或映像。

- 虚拟介质处于 *Attached*（已附加）状态，以便虚拟驱动器在引导顺序中显示。

要启用一次性引导选项并从虚拟介质引导受管系统：

1. 在 iDRAC Web 界面中，转至**概览** > **服务器** > **已附加介质**。
2. 在 **Virtual Media**（虚拟介质）下，选择 **Enable Boot Once**（启用一次性引导）然后单击 **Apply**（应用）。
3. 在引导期间打开受管系统并按 **<F2>**。
4. 将引导顺序更改为从远程虚拟介质设备引导。
5. 重新引导服务器。
   受管系统将从虚拟介质一次性引导。

24

管理 vFlash SD 卡

注: AMD 平台服□器支持 vFlash。

vFlash SD 卡是可从工厂订购和安装的安全数字 (SD) 卡。您可以使用最大 16 GB 容量的卡。插入该卡后，必须启用 vFlash 功能以创建和管理分区。vFlash 是一项授权的功能。

注: SD 卡的大小不受限制，您可以打开并用更高容量的 SD 卡替□出厂安装的 SD 卡。由于 vFlash 使用 FAT32 文件系□，因此文件大小限制□ 4GB。

如果该卡在系统的 vFlash SD 卡插槽中不可用，将在 iDRAC Web 界面的**概览** > **服务器** > **vFlash** 下显示以下错误消息：

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

注: 确保□在 iDRAC vFlash 卡插槽中插入兼容 vFlash 的 SD 卡。如果您插入不兼容的 SD 卡，□初始化□卡□将□示以下□□消息：*初始化 SD 卡时发生错误。*

主要功能有：

- 提供存储空间并模拟 USB 设备。
- 创建最多 16 个分区。这些分区在附加时对系统显示为软盘驱动器、硬盘驱动器或 CD/DVD 驱动器，具体视选定的模拟模式而定。
- 从支持的文件系统类型创建分区。支持 .**img** 格式用于软盘、**.iso** 格式用于 CD/DVD 以及 **.iso 和 .img** 格式用于硬盘模拟类型。
- 创建可引导的 USB 设备。
- 一次性引导到模拟的 USB 设备。

  注: vFlash 操作期间 vFlash 许可证可能会过期。如果出现此情况，则正在进行的 vFlash 操作会正常完成。

注: 如果 FIPS 模式已启用，您无法□行任何 vFlash 操作。

主□：

- 配置 vFlash SD 卡
- 管理 vFlash 分区

配置 vFlash SD 卡

在配置 vFlash 之前,请确保将 vFlash SD 卡已安装在系统上。关于如何从系统安装和移除卡的信息，请参阅 安装和服务手册，网址：https://www.dell.com/poweredgemanuals。

注: 必□具有"□□虚□介□"权限才能启用或禁用 vFlash 功能，以及□卡□行初始化操作。

查看 vFlash SD 卡属性

启用 vFlash 功能后，您可以使用 iDRAC Web 界面或 RACADM 查看 SD 卡属性。

使用 Web 界面查看 vFlash SD 卡属性

要查看 vFlash SD 卡属性，请在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash**。随即会显示 Card Properties（卡属性）页面。有关所显示的属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 查看 vFlash SD 卡属性

要使用 RACADM 查看 vFlash SD 卡属性，请使用 `get` 命令其以下对象：

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

有关这些对象的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序查看 vFlash SD 卡属性

要查看 vFlash SD 卡属性，在 **iDRAC Settings Utility（iDRAC 设置公用程序）**中，转至 **Media and USB Port Settings（介质和 USB 端口设置）**。**Media and USB Port Settings（介质和 USB 端口设置）**页面中显示属性。有关显示的属性的信息，请参阅 *iDRAC Settings Utility Online Help*（iDRAC 设置公用程序联机帮助）。

启用或禁用 vFlash 功能

必须启用 vFlash 功能才能执行分区管理。

使用 Web 界面启用或禁用 vFlash 功能

要启用或禁用 vFlash 功能：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash**。
   随即会显示 **SD Card Properties（SD 卡属性）**页面。
2. 选中或清除 **vFlash Enabled（已启用 vFlash）**选项以启用或禁用 vFlash 功能。如果连接有任何 vFlash 分区，将不能禁用 vFlash 并且会显示错误消息。

   注: 如果禁用 vFlash 功能，则不会显示 SD 卡属性。

3. 单击**应用**。vFlash 功能即根据选择启用或禁用。

使用 RACADM 启用或禁用 vFlash 功能

要使用 RACADM 启用或禁用 vFlash 功能：

```
racadm set iDRAC.vflashsd.Enable [n]
```

n=0
已禁用

n=1
已启用

注: 只有存在 vFlash SD 卡时，RACADM 命令才起作用。如果不存在卡，则会显示以下消息：*ERROR: SD Card not present（错误：SD 卡不存在）*。

使用 iDRAC 设置公用程序启用或禁用 vFlash 功能

要启用或禁用 vFlash 功能：

1. 在 iDRAC 设置公用程序中，转至**介质和 USB 端口设置**。
   iDRAC Settings（iDRAC 设置）。将显示 **Media and USB Port Settings（介质和 USB 端口设置）**页面。
2. 在 **vFlash 介质**部分中，选择**启用**来启用 vFlash 功能或选择**禁用**来禁用 vFlash 功能。
3. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。
   vFlash 功能即根据选择启用或禁用。

初始化 vFlash SD 卡

初始化操作会重新格式化 SD 卡并配置该卡上的初始 vFlash 系统信息。

注: 如果 SD 卡□于写保□状□，将会禁用“初始化”□□。

使用 Web 界面初始化 vFlash SD 卡

要初始化 vFlash SD 卡：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash。**
   随即会显示 **SD Card Properties（SD 卡属性）**页面。
2. 启用 **vFLASH** 并单击 **Initialize（初始化）**。

   所有现有内容都将被删除，卡将使用新的 vFlash 系统信息重新格式化。

   如果连接有任何 vFlash 分区，初始化操作将会失败并且会显示错误消息。

使用 RACADM 初始化 vFlash SD 卡

要使用 RACADM 初始化 vFlash SD 卡：

```
racadm set iDRAC.vflashsd.Initialized 1
```

系统随即会删除所有现有分区并重新格式化该卡。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

使用 iDRAC 设置公用程序初始化 vFlash SD 卡

要使用 iDRAC 设置公用程序初始化 vFlash SD 卡：

1. 在 iDRAC 设置公用程序中，转至**介质和 USB 端口设置。**
   iDRAC Settings（iDRAC 设置）。将显示 **Media and USB Port Settings（介质和 USB 端口设置）**页面。
2. 单击 **Initialize vFlash（初始化 vFlash）。**
3. 单击**是。**初始化操作将启动。
4. 单击 **Back（返回）**并导航至同一 **iDRAC Settings（iDRAC 设置）。Media and USB Port Settings（介质和 USB 端口设置）**页面可查看成功消息。
   所有现有内容都将被删除，卡将使用新的 vFlash 系统信息重新格式化。

使用 RACADM 获取上次状态

要获取上次发送给 vFlash SD 卡的初始化命令的状态：

1. 打开系统的 SSH 或串行控制台并登录。
2. 输入以下命令：`racadm vFlashsd status`
   随即会显示发送给 SD 卡的命令的状态。
3. 要获取所有 vflash 分区的上次状态，请使用命令：`racadm vflashpartition status -a`
4. 要获取特定分区的上次状态，请使用命令：`racadm vflashpartition status -i (index)`

   注: 如果重设 iDRAC，上次分区操作的状态会丢失。

管理 vFlash 分区

您可以使用 iDRAC Web 界面或 RACADM 执行以下操作：

注: 管理□可以在 vFlash 分区上□行所有操作。否□，您必□□有 **Access Virtual Media（访问虚拟介质）**权限才能□建、□除、格式化、附加、分离或复制分区的内容。

- 创建空白分区
- 使用映像文件创建分区
- 格式化分区
- 查看可用分区
- 修改分区
- 连接或断开分区
- 删除现有分区
- 下载分区内容
- 引导至分区

注: 如果在□用程序（例如 WSMan、iDRAC □置公用程序或 RACADM）使用 vFlash □□□ vFlash □面上的任何□□，或□航到 GUI 中的其他一些□面，iDRAC 可能会□示以下信息：`vFlash is currently in use by another process. Try again after some time`（vFlash 当前正被其他□程使用。□一段□□后再次□□。）。

没有其他正在进行的 vFlash 操作（例如，格式化、附加分区等）时，vFlash 能够执行快速分区创建。因此，建议您在执行其他单独的分区操作之前首先创建所有分区。

创建空白分区

当空白分区连接到系统时类似于空白 USB 闪存驱动器。您可以在 vFlash SD 卡上创建空白分区。您可以创建*软盘*或*硬盘类型的分区*。使用映像创建分区时仅支持分区类型 CD。

创建空白分区前，请确保：

- 具有 **Access Virtual Media（访问虚拟介质）**权限。
- 卡已初始化。
- 卡没有受写保护。
- 尚未对卡执行初始化操作。

使用 Web 界面创建空白分区

要创建空白 vFlash 分区：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **Systems Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Create Empty Partition（创建空分区）**。
   将会显示 **Create Empty Partition（创建空白分区）**页面。
2. 指定所需信息，然后单击 **Apply（应用）**。有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
   默认情况下，将创建一个具有只读权限的新的未格式化空白分区。将显示页面指示进度百分比。下列情况下会显示错误消息：
   - 卡处于写保护状态。
   - 卷标名称与现有分区的卷标一样。
   - 为分区大小输入了非整数值，该值超过卡上的可用空间，或分区大小大于 4 GB。
   - 正在对卡执行初始化操作。

使用 RACADM 创建空白分区

要创建空白分区：

1. 使用 SSH 或串行控制台登录系统。
2. 输入以下命令：

```
racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s [n]
```

其中 `[n]` 是分区大小。

默认情况下，创建的空白分区为具备读写属性。

如果未使用用户名/密码配置共享，则需要将参数指定为

```
-u anonymous -p anonymous
```

。

使用映像文件创建分区

您可以在 vFlash SD 卡上使用映像文件（以 **.img** 或 **.iso** 格式提供）创建新分区。这些分区为模拟类型：软盘（**.img**）、硬盘（**.img**）或 CD（**.iso**）。创建的分区大小等于映像文件大小。

从映像文件创建分区之前，请确保：

- 具有 Access Virtual Media（访问虚拟介质）权限。
- 卡已初始化。
- 卡没有受写保护。
- 尚未对卡执行初始化操作。
- 映像类型与模拟类型匹配。

  注： 上传的映像类型与仿真类型必须匹配。iDRAC 仿真设备时映像类型不正确会出现问题。例如，如果使用 ISO 映像创建分区并且仿真类型指定为硬盘，则 BIOS 无法从该映像引导。
- 映像文件大小小于或等于卡上的可用空间。
- 映像文件大小小于或等于 4 GB，支持的最大分区大小为 4 GB。但是，使用 Web 浏览器创建分区时，映像文件大小必须小于 2 GB。

注： vFlash 分区是 FAT32 文件系□上的映像文件。因此，映像文件具有 4 GB 的限制。

注： 不支持完整操作系□安装。

使用 Web 界面使用映像文件创建分区

从映像文件创建 vFlash 分区：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Create From Image（从映像创建）**。
   将显示 **Create Partition from Image File（从映像文件创建分区）**页面。
2. 输入所需的信息，然后单击 **Apply（应用）**。有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
   将创建一个新分区。对于 CD 仿真类型，将创建只读分区。对于软盘或硬盘仿真类型，将创建一个读写分区。下列情况下会显示错误消息：
   - 卡受写保护。
   - 卷标名称与现有分区的卷标一样。
   - 映像文件大小大于 4GB 或超过卡上的可用空间。
   - 映像文件不存在或映像文件扩展既不是 .img 也不是 .iso。
   - 已经在对卡执行初始化操作。

使用 RACADM 从映像文件创建分区

使用 RACADM 从映像文件创建分区：

1. 使用 SSH 或串行控制台登录系统。
2. 输入命令

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/
sharedfolder/foo.iso -u root -p mypassword
```

默认情况下，创建的分区为只读。对于映像文件扩展名，此命令区分大小写。如果文件扩展名为大写字母形式（例如 FOO.ISO，而非 FOO .iso），则命令将返回语法错误。

注： 本地 RACADM 中不支持此功能。

注： 不支持从启用 CFS 或 NFS IPv6 的网络共享上的映像文件创建 vFlash 分区。

如果未使用用户名/密码配置共享，则需要将参数指定为

```
-u anonymous -p anonymous
```

。

格式化分区

您可以根据文件系统类型格式化 vFlash SD 卡上的现有分区。支持的文件系统类型是 EXT2、EXT3、FAT16 和 FAT32。您可以仅键入硬盘或软盘磁盘格式化分区，而不是 CD。只读分区无法格式化。

在使用映像文件创建分区之前，确保：

- 具有 **Access Virtual Media（访问虚拟介质）**权限。
- 卡已初始化。
- 卡没有受写保护。
- 尚未对卡执行初始化操作。

要格式化 vFlash 分区：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Format（格式）**。
   将会显示 **Format Partition（格式化分区）**页面。
2. 输入所需的信息，然后单击 **Apply（应用）**。
   有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
   将显示警告信息，提示分区中的所有数据将被清除。
3. 单击 **OK（确定）**。
   所选分区将格式化为指定的文件系统类型。下列情况下会显示错误消息：
   - 卡处于写保护状态。
   - 已经在对卡执行初始化操作。

查看可用分区

确保 vFlash 功能已启用，以便于查看可用分区的列表。

使用 Web 界面查看可用分区

要查看可用的 vFlash 分区，请在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Manage（管理）**。此时将显示 **Manage Partitions（管理分区）**页面，其中列出可用分区和每个分区的相关信息。有关分区的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 查看可用分区

要使用 RACADM 查看用分区及其属性：

1. 打开系统的 SSH 或串行控制台并登录。
2. 输入以下命令：
   - 要列出所有现有分区及其属性：

     ```
     racadm vflashpartition list
     ```

   - 要获取操作分区 1 的状况：

     ```
     racadm vflashpartition status -i 1
     ```

   - 要获取所有现有分区的状况：

     ```
     racadm vflashpartition status -a
     ```

   注: -a 选项仅在使用状态操作时有效。

修改分区

您可以将只读分区更改为读写分区，反之亦然。修改分区内容之前，请确保：

- vFlash 功能已启用。
- 具有 **Access Virtual Media（访问虚拟介质）**的权限。

注: 默□□建只□分区。

使用 Web 界面修改分区

要修改分区：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Manage（管理）**。
   将会显示 **Manage Partitions（管理分区）**页面。
2. 在 **Read-Only（只读 ）**列中：
   - 选择分区的复选框，然后单击 **Apply（应用）**更改为 read-only（只读）。
   - 清除分区的复选框，然后单击 **Apply（应用）**更改为 read-write（读写）。

     分区根据所做的选择更改为只读或读写。

   注: 如果分区类型是 CD，则状态为只读。无法将状态更改为读写。如果分区已连接，则复选框将显示为灰色。

使用 RACADM 修改分区

要查看卡上的可用分区及其属性：

1. 使用 SSH 或串行控制台登录系统。
2. 可使用以下方法之一：
   - 使用 `set` 命令更改分区的读写状态：
     - 要将只读分区更改为读写分区：

       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 1
       ```

     - 要将读写分区更改为只读分区：

       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 0
       ```

   - 使用 `set` 命令指定仿真类型：

     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

连接或断开分区

当您附加一个或多个分区时，它们作为 USB 大容量存储设备对操作系统和 BIOS 可见。当您附加多个分区时，根据分配的索引，它们在操作系统和 BIOS 引导顺序菜单中会以升序列出。

如果分离分区，则分区不会显示在操作系统和 BIOS 引导顺序菜单中。

当您附加或分离分区时，受管系统中的 USB 总线会重设。这会影响正在使用 vFlash 的应用程序，并且会断开 iDRAC 虚拟介质会话。

附加或分离分区前，请确保：

- vFlash 功能已启用。
- 尚未对卡执行初始化操作。
- 具有 **Access Virtual Media（访问虚拟介质）**的权限。

使用 Web 界面连接或断开分区

要连接或断开分区连接：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Manage（管理）**。
   将会显示 **Manage Partitions（管理分区）**页面。
2. 在 **Attached（已附加）**列中：
   - 选中分区的复选框，然后单击 **Apply（应用）**附加分区。
   - 清除分区的复选框，然后单击 **Apply（应用）**分离分区。

   分区根据所做的选择附加或分离。

使用 RACADM 连接或断开分区

要连接或断开分区连接：

1. 使用 SSH 或串行控制台登录系统。
2. 使用以下命令：
   - 要连接分区：

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 1
     ```
   - 要断开分区连接：

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 0
     ```

操作系统对附加分区的行为

对于 Windows 和 Linux 操作系统：

- 操作系统控制和分配附加分区的盘符。
- 只读分区是操作系统中的只读驱动器。
- 操作系统必须支持已附加分区的文件系统。否则，您无法从操作系统读取或修改分区的内容。例如，在 Windows 环境中，操作系统无法读取 Linux 系统原生的 EXT2 分区类型。此外，在 Linux 环境中，操作系统无法读取 Windows 系统原生的 NTFS 分区类型。
- vFlash 分区标签与仿真 USB 设备上的文件系统的卷名称不同。您可以从操作系统更改仿真 USB 设备的卷名。但是，它不会更改 iDRAC 中存储的分区卷标签名称。

删除现有分区

删除现有分区前，请确保：

- vFlash 功能已启用。
- 卡没有受写保护。
- 分区未附加。
- 尚未对卡执行初始化操作。

使用 Web 界面删除现有分区

删除现有分区：

1. 在 iDRAC Web 界面中，转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Manage（管理）**。
   将会显示 **Manage Partitions（管理分区）**页面。
2. 在 **Delete（删除）**列中，单击您要删除的分区的删除图标。
   将显示一条信息，表明此操作会永久删除该分区。
3. 单击 **OK（确定）**。
   分区即被删除。

使用 RACADM 删除现有分区

删除分区：

1. 打开系统的 SSH 或串行控制台并登录。
2. 输入以下命令：
   - 删除分区：

     ```
     racadm vflashpartition delete -i 1
     ```
   - 要删除所有分区，请重新初始化 vFlash SD 卡。

下载分区内容

您可以将 **.img** 或 **.iso** 格式的 vFlash 分区内容下载到：

- 受管系统（iDRAC 在其中运行的系统）
- 映射到 management station 的网络位置。

下载分区内容之前，请确保：

- 具有 Access Virtual Media（访问虚拟介质）的权限。
- vFlash 功能已启用。
- 尚未对卡执行初始化操作。
- 读写分区不能附加。

要下载 vFlash 分区的内容：

1. 在 iDRAC Web 界面中,转至 **Configuration（配置）** > **System Settings（系统设置）** > **Hardware Settings（硬件设置）** > **vFlash** > **Download（下载）**。
   将会显示 **Download Partition（下载分区）**页面。
2. 从 **Label（卷标）**下拉菜单中，选择要下载的分区，然后单击 **Download（下载）**。

   注: 所有现有的分区（附加分区除外）都显示在列表中。默认情况下选择第一个分区。

3. 指定保存文件的位置。
   选定分区的内容将下载到指定位置。

   注: 只要指定了文件夹位置，就会将分区卷标作为文件名称，CD 和硬盘类型分区的扩展名为 **.iso**，软盘和硬盘类型分区的扩展名为 **.img**。

引导至分区

可以将已附加 vFlash 分区设置为下一次引导操作的引导设备。

引导分区之前，请确保：

- vFlash 分区中包含可引导的映像（**.img** 或 **.iso** 格式）以从设备引导。
- vFlash 功能已启用。
- 具有 Access Virtual Media（访问虚拟介质）的权限。

使用 Web 界面引导至分区

要将 vFlash 分区设置为第一引导设备，请参阅 使用 Web 界面引导至分区 页面上的 295。

注: 如果**第一引导设备**下拉菜单中未列出已附加的 vFlash 分区，请确保 BIOS 已更新为最新版本。

使用 RACADM 引导至分区

要将 vFlash 分区设置为第一个引导设备，使用 `iDRAC.ServerBoot` 对象。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

注: 运行此命令时，vFlash 分区标签自动设置为引导一次（`iDRAC.ServerBoot.BootOnce` 设置为 `1`）。引导一次只能将设备一次性引导到分区，并且不会将其永久保留在引导顺序中的第一位。

25

使用 SMCLP

注： SMCLP □在低于 4.00.00.00 的 iDRAC 版本中受支持。

Server Management Command Line Protocol（服务器管理命令行协议，SMCLP）规范可实现基于 CLI 的系统管理。它定义了通过面向标准字符的流传输的管理命令协议。此协议使用面向人的命令集来访问公共信息模型对象管理器 (CIMOM)。SMCLP 是分布式管理任务组 (DMTF) SMASH 计划用来简化多平台系统管理的一个子组件。SMCLP 规范以及 Managed Element Addressing Specification（受管元素寻址规范）和 SMCLP 映射规范的许多配置文件描述了各种管理任务执行的标准动词和目标。

注： 假定您熟悉 Systems Management Architecture for Server Hardware（服□器硬件的系□管理架构，SMASH）□准以及 Server Management Working Group (SMWG) SMCLP □范。

SM-CLP 是分布式管理任务组 (DMTF) SMASH 倡导用来简化多平台服务器管理的一个子组件。SM-CLP 规范以及受管元素寻址规范和 SM-CLP 映射规范的许多配置文件描述了各种管理任务执行的标准动词和目标。

从 iDRAC 控制器固件开始托管 SMCLP 并支持 SSH 和基于串行的界面。iDRAC SMCLP 界面基于 DMTF 组织提供的 SMCLP 规范版本 1.0。

注： 在 https://www.dell.com/support 上提供了关于配置文件、□展和 MOF 的信息，在 **dmtf.org/standards/profiles/** 上提供了所有 DMTF 信息。

SM-CLP 命令采用了本地 RACADM 命令的一个子集。这些命令对脚本编写非常有用，因为您可以从 Management Station 命令行执行这些命令。您可以在格式良好的文件中检索这些命令的输出（包括 XML），从而简化脚本编写并与现有报告和管理工具集成。

主□：

使用 SMCLP 的系统管理功能

iDRAC SMCLP 允许您执行以下操作：

- 管理服务器电源 — 打开、关闭或重新引导系统
- 管理系统事件日志 (SEL) — 显示或清除 SEL 记录
- 查看 iDRAC 用户帐户
- 查看系统属性

运行 SMCLP 命令

您可以使用 SSH 界面运行 SMCLP 命令。打开 SSH 界面并以管理员身份登录 iDRAC。将会显示 SMCLP 提示符 (admin ->)。

SMCLP 提示符：

- yx1x 刀片服务器使用 `-$`。
- yx1x 机架和塔式服务器使用 `admin->`。
- yx2x 刀片、机架和塔式服务器使用 `admin->`。

其中，y 是字母数字字符，例如 M（表示刀片服务器）、R（表示机架服务器）和 T（表示塔式服务器）；而 x 为数字。该数字表示 Dell PowerEdge 服务器为第几代。

注: 使用 `-$` 的脚本可将□些用于 yx1x 系□；但从 yx2x 系□开始，使用 `admin->` 的脚本可用于刀片、机架和塔式服□器。

iDRAC SMCLP 语法

iDRAC SMCLP 使用动词和目标的概念，通过 CLI 提供系统管理功能。动词表示要执行的操作，而目标确定了要运行操作的实体（或对象）。

SMCLP 命令行语法：

```
<verb> [<options>] [<target>] [<properties>]
```

下表提供了动词及其定义。

表. 62: SMCLP 动词

动词	定义
cd	使用 Shell 导航 MAP
set	将属性设定为特定值
帮助	显示指定目标的帮助
reset	重设目标
show	显示目标属性、动词和子目标
start	打开目标
stop	关闭目标
exit	从 SMCLP shell 会话退出
版本	显示目标的版本属性
load	将二进制映像从一个 URL 移至指定目标地址

下表提供了目标列表。

表. 63: SMCLP 目标

目标	定义
`admin1`	管理员域
`admin1/profiles1`	iDRAC 中已注册的配置文件
`admin1/hdwr1`	硬件
`admin1/system1`	受管系统目标
`admin1/system1/capabilities1`	受管系统 SMASH 收集功能
`admin1/system1/capabilities1/elecap1`	受管系统目标功能

表. 63: SMCLP 目标 （续）

目标	定义
admin1/system1/logs1	记录日志收集目标
admin1/system1/logs1/log1	系统事件日志 (SEL) 记录条目
admin1/system1/logs1/log1/record*	受管系统上的单独 SEL 记录实例
admin1/system1/settings1	受管系统 SMASH 收集设置
admin1/system1/capacities1	受管系统功能 SMASH 收集
admin1/system1/consoles1	受管系统控制台 SMASH 收集
admin1/system1/sp1	服务处理器
admin1/system1/sp1/timesvc1	服务处理器时间服务
admin1/system1/sp1/capabilities1	服务处理器功能 SMASH 收集
admin1/system1/sp1/capabilities1/clpcap1	CLP 服务功能
admin1/system1/sp1/capabilities1/ pwrmgtcap1	系统中电源状态管理服务功能
admin1/system1/sp1/capabilities1/ acctmgtcap*	帐户管理服务功能
admin1/system1/sp1/capabilities1/ rolemgtcap*	基于本地角色的管理功能
admin1/system1/sp1/capabilities1/elecap1	验证功能
admin1/system1/sp1/settings1	服务处理器设置收集
admin1/system1/sp1/settings1/clpsetting1	CLP 服务设置数据
admin1/system1/sp1/clpsvc1	CLP 服务协议服务
admin1/system1/sp1/clpsvc1/clpendpt*	CLP 服务协议端点
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP 服务协议 TCP 端点

表. 63: SMCLP 目标 （续）

目标	定义
admin1/system1/sp1/jobq1	CLP 服务协议作业队列
admin1/system1/sp1/jobq1/job*	CLP 服务协议作业
admin1/system1/sp1/pwrmgtsvc1	电源状态管理服务
admin1/system1/sp1/account1-16	Local user account（本地用户帐户）
admin1/sysetm1/sp1/account1-16/identity1	本地用户身份帐户
admin1/sysetm1/sp1/account1-16/identity2	IPMI 身份 (LAN) 帐户
admin1/sysetm1/sp1/account1-16/identity3	IPMI 身份（串行）帐户
admin1/sysetm1/sp1/account1-16/identity4	CLP 身份帐户
admin1/system1/sp1/acctsvc2	IPMI 帐户管理服务
admin1/system1/sp1/acctsvc3	CLP 帐户管理服务
admin1/system1/sp1/rolesvc1	本地角色基础授权 (RBA) 服务
admin1/system1/sp1/rolesvc1/Role1-16	本地角色
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	本地角色权限
admin1/system1/sp1/rolesvc2	IPMI RBA 服务
admin1/system1/sp1/rolesvc2/Role1-3	IPMI 角色
admin1/system1/sp1/rolesvc2/Role4	IPMI LAN 上串行 (SOL) 角色
admin1/system1/sp1/rolesvc3	CLP RBA 服务
admin1/system1/sp1/rolesvc3/Role1-3	CLP 角色
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP 角色权限

导航 MAP 地址空间

可以使用 SM-CLP 管理的对象通过在分层空间（称为可管理性访问点 [MAP] 地址空间）中安排的目标表示。地址路径指定从地址空间的根到地址空间中对象的路径。

根目标通过斜线 (/) 或反斜线 (\) 表示。这是登录 iDRAC 时的默认起始点。使用 cd 动词可从根向下导航。

注: 斜□ (/) 和反斜□ (\) 在 SM-CLP 地址路径中可以互□。但是，命令行□尾的反斜□表示命令在下一行□□并将在分析命令□被忽略。

例如，要导航到系统事件日志 (SEL) 中的第三个记录，输入以下命令：

```
->cd /admin1/system1/logs1/log1/record3
```

输入不带目标的 cd 动词可在地址空间中查找您的当前位置。.. 和 . 缩写词如在 Windows 和 Linux 中一样发挥作用：.. 指父级，. 指当前级别。

使用 show 动词

要了解关于目标的更多信息，请使用 show 动词。此动词显示目标的属性、子目标、关联和该位置允许的 SM-CLP 动词列表。

使用 -display 选项

show -display 选项允许限制命令输出到一个或多个属性、命令、关联和动词。例如，要只显示当前位置的属性和目标，使用以下命令：

```
show -display properties,targets
```

要仅列出某些属性，按以下命令予以限定：

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

如果只想显示一个属性，可以省略括号。

使用 -level 选项

show -level 选项在指定目标下的其他级别上执行 show。要查看地址空间中的所有目标和属性，使用 -l all 选项。

使用 -output 选项

-output 选项指定 SM-CLP 动词输出的四种格式之一：**text**、**clpcsv**、**keyword** 和 **clpxml**。

默认情况下，格式为 **text**，并且这是最可读的输出。**clpcsv** 格式是逗号分隔格式，适合加载到电子数据表程序中。**keyword** 格式输出信息是 keyword=value 对的列表，每行一个。**clpxml** 格式 XML 文档，其中包含 **response** XML 元素。DMTF 指定了 **clpcsv** 和 **clpxml** 格式，并且其规范可以在 DMTF 网站 (**dmtf.org**) 上找到。

以下示例显示了如何以 XML 输出 SEL 内容：

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

用法示例

此节提供 SMCLP 的用法示例方案：

服务器电源管理

以下示例介绍了在受管系统上如何使用 SMCLP 来执行电源管理操作。

请在 SMCLP 命令提示符下输入以下命令：

- 要关闭服务器：

  ```
  stop /system1
  ```

  屏幕上将显示以下信息：

  ```
  system1 has been stopped successfully
  ```

- 要开启服务器：

  ```
  start /system1
  ```

  屏幕上将显示以下信息：

  ```
  system1 has been started successfully
  ```

- 要重新引导服务器：

  ```
  reset /system1
  ```

  屏幕上将显示以下信息：

  ```
  system1 has been reset successfully
  ```

SEL 管理

以下示例显示了在受管系统上如何使用 SMCLP 来执行 SEL 相关操作。请在 SMCLP 命令提示符下输入以下命令：

- 查看 SEL：

  ```
  show/system1/logs1/log1
  ```

  系统将显示以下输出 ：

  ```
  /system1/logs1/log1
  Targets:
  Record1
  Record2
  Record3
  Record4
  Record5
  Properties:
  InstanceID = IPMI:BMC1 SEL Log
  MaxNumberOfRecords = 512
  CurrentNumberOfRecords = 5
  Name = IPMI SEL
  EnabledState = 2
  OperationalState = 2
  HealthState = 2
  Caption = IPMI SEL
  Description = IPMI SEL
  ElementName = IPMI SEL
  Commands:
  cd
  show
  ```

```
help
exit
version
```

- 查看 SEL 记录：

  ```
  show/system1/logs1/log1
  ```

  系统将显示以下输出 ：

  ```
  /system1/logs1/log1/record4
  Properties:
  LogCreationClassName= CIM_RecordLog
  CreationClassName= CIM_LogRecord
  LogName= IPMI SEL
  RecordID= 1
  MessageTimeStamp= 20050620100512.000000-000
  Description= FAN 7 RPM: fan sensor, detected a failure
  ElementName= IPMI SEL Record
  Commands:
  cd
  show
  help
  exit
  version
  ```

映射目标导航

以下示例显示了如何使用 cd 动词导航 MAP。在所有示例中，假定初始的默认目标为 /。

请在 SMCLP 命令提示符下输入以下命令：

- 导航到系统目标并重新引导：

  cd system1 reset 当前默认目标为 /。

- 导航到 SEL 目标并显示日志记录：

  ```
  cd system1
  cd logs1/log1
  show
  ```

- 要显示当前目标：

  类型 `cd .`

- 要向上移动一级：

  类型 `cd ..`

- 要退出：

  ```
  exit
  ```

26

部署操作系统

您可以使用以下任意公用程序将操作系统部署到受管系统：
- 远程文件共享
- 控制台

主□：

使用远程文件共享部署操作系统

使用远程文件共享 (RFS) 部署操作系统之前，请确保：
- 为用户启用 iDRAC 的**配置用户**和**访问虚拟介质**权限。
- 网络共享包含以业界标准格式（例如 **.img** 或 **.iso**）提供的驱动程序和操作系统可引导映像文件。

  注: 创建映像文件时，按照基于网络的标准安装步骤进行操作，并将部署映像标记为只读，以确保每个目标系统引导并执行相同的部署步骤。

要使用 RFS 部署操作系统：

1. 使用远程文件共享 (RFS)，通过 NFS、CIFS、HTTP 或 HTTPs 将 ISO 或 IMG 映像文件挂载到受管系统。

   注: 不支持使用 HTTP、基本或摘要验证的 RFS，需要无验证。对于 HTTPS，不支持基本验证，仅支持摘要验证或无验证。

2. 转至**配置** > **系统设置** > **硬件设置** > **第一引导设备**。
3. 在**第一引导设备**下拉列表中设置引导顺序，以选择软盘、CD、DVD 或 ISO 等虚拟介质。
4. 选择**引导一次**选项，启用受管系统以使用映像文件仅对下一个实例重新引导。
5. 单击**应用**。
6. 重新引导受管系统并按照屏幕上的说明完成部署。

管理远程文件共享

通过使用远程文件共享 (RFS) 功能，您可以设置网络共享上的 ISO 或 IMG 映像文件，并使其作为虚拟驱动器供受管服务器的操作系统使用（方法是使用 NFS、CIFS、HTTP 或 HTTPs 将其作为 CD 或 DVD 进行挂载）。RFS 是一种许可的功能。

远程文件共享仅支持 **.img** 和 **.iso** 映像文件格式。将 **.img** 文件重定向为虚拟软盘，将 **.iso** 文件重定向为虚拟 CDROM。

必须拥有虚拟介质权限才能挂载 RFS。

RFS 和虚拟介质功能是互斥的。

- 如果虚拟介质客户端不处于活动状态，则当您尝试建立 RFS 连接时，可以建立连接并且可在主机操作系统中看到远程映像。
- 如果虚拟介质客户端处于活动状态，则当您尝试建立 RFS 连接时，会显示以下错误消息：

  虚拟介质与所选虚拟驱动器断开连接或重定向。

RFS 连接状态在 iDRAC 日志中可用。一旦连接，安装 RFS 的虚拟驱动器不会断开，即使注销 iDRAC 也不例外。如果重设 iDRAC 或网络连接断开，RFS 连接会关闭。Web 界面和命令行选项还可在 CMCOME Modular 和 iDRAC 中使用，以关闭 RFS 连接。CMC 中的 RFS 连接始终会覆盖 iDRAC 中已有的 RFS。

注:
- CIFS 和 NFS 同时支持 IPv4 和 IPv6 地址。

- 如果 iDRAC 配置了 IPv4 和 IPv6，DNS 服务器可以包含将 iDRAC 主机名与两个地址相关联的记录。如果在 iDRAC 中禁用 IPv4 选项，则 iDRAC 可能无法访问外部 IPv6 共享。这是因为 DNS 服务器可能仍包含 IPv4 记录，并且 DNS 名称解析可以返回 IPv4 地址。这种情况下，禁用 iDRAC 中的 IPv4 选项时，建议从 DNS 服务器中删除 IPv4 DNS 记录。
- 如果您使用 CIFS 和 Active Directory 域的一部分，请在映像文件路径中输入域名及 IP 地址。
- 如果您想要从 NFS 共享访问文件，则配置以下共享权限。因为 iDRAC 界面在非根模式下运行，所以需要这些权限。
  - Linux：确保共享权限针对**其他**账户设置为至少**读取**。
  - Windows：转至共享属性的**安全**选项卡并将**每个人**添加到具有**读取和执行**权限的**组或用户名**字段。
- 如果 ESXi 在受管系统上运行，并且如果您使用 RFS 挂载软盘映像（**.img**），则 ESXi 操作系统不能使用连接的软盘映像。
- iDRAC vFlash 功能与 RFS 没有关联。
- 网络共享文件路径仅支持英文 ASCII 字符。
- 使用 RFS 连接虚拟介质时，不支持 OS 驱动器弹出功能。
- 通过 HTTP 或 HTTPs 功能的 RFS 在 CMC Web 界面上不可用。

使用 Web 界面配置远程文件共享

启用远程文件共享：

1. 在 iDRAC Web 界面中，转至**配置** > **虚拟介质** > **已附加介质**。
   将显示**已附加介质**页面。
2. 在**已附加介质**下，选择**附加**或**自动附加**。
3. 在**远程文件共享**下，指定映像文件路径、域名、用户名和密码。有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

   映像文件路径示例：
   - CIFS — `//<IP to connect for CIFS file system>/<file path>/<image name>`
   - NFS — `< IP to connect for NFS file system>:/<file path>/<image name>`
   - HTTP — `http://<URL>/<file path>/<image name>`
   - HTTPs — `https://<URL>/<file path>/<image name>`

   注: 为避免 I/O 错误，使用在 Windows 7 系统上托管的 CIFS 共享时，请修改以下注册表项：
   - 将 HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache 设置为 1
   - 将 HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size 设置为 3

   注: "/"或"\"字符均可用于文件路径。

   CIFS 支持 IPv4 和 IPv6 地址，但 NFS 仅支持 IPv4 地址。

   如果使用 NFS 共享，因为会区分大小写，请确保提供准确的 <文件路径> 和 <映像名称> 。

   注: 有关用户名和密码的建议字符信息，请参阅 建议使用的用户名和密码字符 页面上的 135。

   注: 网络共享的用户名和密码中允许的字符由网络共享类型决定。iDRAC 支持通过共享类型定义的网络共享凭据的有效字符，但 <、> 和 ,（逗号分隔）除外。

4. 单击**应用**，然后单击**连接**。
   在建立连接后，**连接状态**显示为**已连接**。

   注: 即使已配置远程文件共享，出于安全原因，Web 界面也不会显示用户凭据信息。

   注: 如果映像路径包含用户凭据，请使用 HTTPS 以避免凭据显示在 GUI 和 RACADM 中。如果在 URL 中输入凭据，请避免使用"@"符号，因为这是一个分隔符。

   对于 Linux 分发，在运行级别 init 3 操作时，此功能可能需要手动挂载命令。命令的语法如下：

```
mount /dev/OS_specific_device / user_defined_mount_point
```

   其中， `user_defined_mount_point` 是您选择的与任何挂载命令类似的用于挂载的任何目录。

对于 RHEL，CD 设备（**.iso** 虚拟设备）是 `/dev/scd0`，软盘设备（**.img** 虚拟设备）是 `/dev/sdc`。

对于 SLES，CD 设备是 `/dev/sr0`，软盘设备是 /dev/sdc。为了确保使用正确的设备（用于 SLES 或 RHEL），当您在 Linux 操作系统上连接虚拟设备时，您必须立即运行该命令：

```
tail /var/log/messages | grep SCSI
```

这将显示可识别设备（例如，SCSI 设备 sdc）的文本。在运行级别 init 3 中使用 Linux 发行版本时，此过程也适用于虚拟介质。默认情况下，在 init 3 中虚拟介质不会自动安装。

使用 RACADM 配置远程文件共享

要使用 RACADM 配置远程文件共享，请使用：

```
racadm remoteimage
```

```
racadm remoteimage <options>
```

选项是：

`-c`：连接映像

`-d`：断开映像连接

`-u`<用户名>：用于访问网络共享的用户名

`-p`<密码>：用于访问网络共享的密码

`-l`<映像位置>：映像在网络共享上的位置；使用双引号将位置括起来。请在“使用 Web 界面配置远程文件共享”部分查看映像文件路径的示例

`-s`：显示当前状态

注: 用户名、密码和映像_位置可使用除以下字符外的所有其他字符（包括字母数字和特殊字符）：’（单引号）、”（双引号）、,（逗号）、<（小于号）和 >（大于号）。

注: 为避免 I/O 错误，使用在 Windows 7 系统上托管的 CIFS 共享时，请修改以下注册表项：

- 将 HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache 设置为 1
- 将 HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size 设置为 3

使用虚拟介质部署操作系统

使用虚拟介质部署操作系统之前，请确保：

- 虚拟介质处于 *Attached*（已附加）状态，以便虚拟驱动器在引导顺序中显示。
- 如果虚拟介质处于 *Auto Attached（自动附加）*模式，则虚拟介质应用程序必须启动，然后才能引导系统。
- 网络共享包含以业界标准格式（例如 **.img** 或 **.iso**）提供的驱动程序和操作系统可引导映像文件。

要部署操作系统，必须使用虚拟介质：

1. 请执行以下某项操作：
   - 将操作系统安装 CD 或 DVD 插入 Management Station CD 或 DVD 驱动器中。
   - 附加操作系统映像。
2. 选择 Management Station 中具有所需映像的驱动器以映射它。
3. 使用以下方法之一引导到所需设备：
   - 使用 iDRAC Web 界面将引导顺序设置为从**虚拟软盘**或**虚拟 CD/DVD/ISO** 引导一次。
   - 通过在引导过程中按 <F2> 键，从 **System Setup（系统设置）** > **System BIOS Settings（系统 BIOS 设置）**设置引导顺序。
4. 重新引导受管系统并按照屏幕上的说明完成部署。

从多个磁盘安装操作系统

1. 取消映射现有的 CD/DVD。

2. 将下一张 CD/DVD 插入远程光盘驱动器中。
3. 重新映射 CD/DVD 驱动器。

在 SD 卡上部署嵌入式操作系统

在 SD 卡上安装嵌入式管理程序：

1. 将两个 SD 卡插入系统的内部双 SD 模块 (IDSDM) 插槽中。
2. 在 BIOS 中启用 SD 模块和冗余（如有必要）。
3. 引导过程中按 <F11> 键验证 SD 卡在其中一个驱动器上是否可用。
4. 部署嵌入式操作系统并按照操作系统安装说明进行操作。

在 BIOS 中启用 SD 模块和冗余

在 BIOS 中启用 SD 模块和冗余：

1. 引导过程中按 <F2> 键。
2. 转至 **System Setup（系统设置）** > **System BIOS Settings（系统 BIOS 设置）** > **Integrated Devices（集成式设备）**。
3. 将 **Internal USB Port（内部 USB 端口）**设置为 **ON（打开）**。如果它设置为 **Off（关闭）**，则 IDSDM 无法用作引导设备。
4. 如果不需要冗余（单 SD 卡），请将**内部 SD 卡端口**设置为**开**并将**内部 SD 卡冗余**设置为**已禁用。**
5. 如果需要冗余（双 SD 卡），请将 **Internal SD Card Port（内部 SD 卡端口）**设置为 **On（开）**并将 **Internal SD Card Redundancy（内部 SD 卡冗余）**设置为 **Mirror（镜像）**。
6. 单击 **Back（返回）**并单击 **Finish（完成）**。
7. 单击 **Yes（是）**保存设置并按 <Esc> 键退出 **System Setup（系统设置）**。

关于 IDSDM

内部双 SD 模块 (IDSDM) 只能在适用的平台上使用。IDSDM 通过使用镜像第一个 SD 卡的内容的另一个 SD 卡，在虚拟机监控程序 SD 卡上提供冗余。

两个 SD 卡中的任意一个可作为主卡。例如，如果在 IDSDM 中安装两个新的 SD 卡，则 SD1 为活动（主）卡，而 SD2 为备用卡。数据将同时写入两个卡，但从 SD1 读取数据。在任何时候，如果 SD1 发生故障或被移除，则 SD2 将自动变为活动（主）卡。

您可以使用 iDRAC Web 界面或 RACADM 查看 IDSDM 的状态、运行状况和可用性。SD 卡冗余状态和故障事件将记录到 SEL，显示在前面板上，并生成 PET 警报（如果启用了警报）。

27

使用 iDRAC 排除受管系统故障

可使用以下内容对远程受管系统进行诊断或故障排除：

- 诊断控制台
- 开机自检代码
- 启动和崩溃捕获视频
- 上次系统崩溃屏幕
- 系统事件日志
- Lifecycle 日志
- 前面板状态
- 故障指示灯
- 系统运行状况

主□：

使用诊断控制台

iDRAC 提供了标准网络诊断工具集，与基于 Microsoft Windows 或 Linux 的系统包括的工具类似。使用 iDRAC Web 界面，可以访问网络调试工具。

要访问诊断控制台：

1. 在 iDRAC Web 界面中，转至 **Maintenance（维护）** > **Diagnostics（诊断）**。
   随即会显示 **Diagnostics Console Command（诊断控制台命令）**页面。
2. 在**命令**文本框中，输入命令并单击**提交**。有关命令的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
   随即结果会显示在同一页面上。

重设 iDRAC 并将 iDRAC 重设为默认设置

1. 在 iDRAC Web 界面中，转至**维护** > **诊断**。
   您还可以选择以下选项：
   - 单击**重设 iDRAC** 以重设 iDRAC。在 iDRAC 上执行正常重新引导操作。重新引导后，刷新浏览器以重新连接并登录到 iDRAC。
   - 单击**将 iDRAC 重设为默认设置**以将 iDRAC 重设为默认设置。当您单击**将 iDRAC 重设为默认设置**后，**将 iDRAC 重设为出厂默认设置**窗口将显示。此操作将 iDRAC 重设为出厂默认设置。选择以下任一选项：
     a. 保留用户和网络设置。
     b. 放弃所有设置并将用户重设为出厂值（root/发货值）。
     c. 放弃所有设置并重置用户名和密码。

2. 随即将显示一条警告消息。单击**确定**继续。

计划远程自动诊断

您可以在服务器上远程调用自动脱机诊断程序作为一次性事件并返回结果。如果诊断程序需要重新引导，您可以立即重新引导或分阶段进行后续重新引导或维护周期（类似于更新）。诊断程序运行时，结果将收集并存储在内部 iDRAC 存储。然后您可以使用 `diagnostics export` racadm 命令将结果导出到 NFS、CIFS、HTTP 或 HTTPs 网络共享。您也可以使用相应的 WSMan 命令运行诊断程序。有关详情，请参阅 WSMan 说明文件。

您必须具有 iDRAC Express 许可证，才能使用远程自动诊断程序。

可以立即运行诊断程序，或将其计划为在特定日期和时间运行，以及指定诊断类型和重新引导类型。

要制定计划，可以指定以下设置：

- 开始时间 - 在将来的日期和时间运行诊断程序。如果您指定“TIME NOW”（当前时间），将在下一次重新引导时运行诊断程序。
- 结束时间 - 在开始时间后的日期和事件运行诊断程序。如果它未在结束事件启动，则通过通过结束时间已过期标记为失败。如果您指定“TIME NA”（时间不适用），则等待时间不适用。

诊断测试的类型包括：

- 快速测试
- 扩展测试
- 按顺序执行这两者

重新引导类型包括：

- 关闭系统电源后重启
- 正常关机（等待操作系统关闭或重新启动）
- 强制正常关机（指示操作系统关闭并等待 10 分钟。如果操作系统未关闭，则 iDRAC 关将重启系统）

一次只可以计划或运行一个诊断作业。诊断作业可以成功完成，完成但有错误或失败。诊断事件（包括结果）记录在 Lifecycle Controller 日志中。您可以使用远程 RACADM 或 WSMan 检索上次诊断执行的结果。

可以将已远程计划的上次完成的诊断作业的诊断结果导出到网络共享（例如 CIFS、NFS、HTTP 或 HTTPS）。最大文件大小为 5 MB。

当作业的状态为未计划或已计划时，您可以取消诊断作业。如果诊断程序正在运行，则重新启动系统以取消作业。

在运行远程诊断之前，请确保：

- 已启用 Lifecycle Controller。
- 您有登录和服务器控制权限。

使用 RACADM 计划远程自动诊断

- 要运行远程诊断程序并在本地系统上保存结果，请使用以下命令：

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
```

- 要导出上次运行的远程诊断结果，请使用以下命令：

```
racadm diagnostics export -f <file name> -l <NFS / CIFS / HTTP / HTTPs share> -u
<username> -p <password>
```

有关选项的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

查看开机自检代码

开机自检代码是系统 BIOS 中的进度指标，指示从上电复位开始的引导顺序的各个阶段，并且允许您诊断与系统启动相关的任何故障。**Post Codes（开机自检代码）**页面在引导操作系统前显示上次系统开机自检代码。

要查看开机自检代码，请转至 **Maintenance（维护）** > **Troubleshooting（故障排除）** > **Post Code（开机自检代码）**。

Post Codes（开机自检代码）页面显示系统运行状况指标、十六进制代码和代码说明。

查看引导和崩溃捕获视频

您可以查看下列录制视频：

- 最后三次引导循环 — 引导循环视频记录了引导循环的事件序列。引导周期视频按从最新到最旧的顺序排列。
- 最后一次崩溃视频 — 崩溃视频记录导致故障的事件序列。

这是一项授权的功能。

iDRAC 在引导时记录五十个帧。它以每秒一帧的速度播放引导屏幕。如果重设 iDRAC，引导捕获视频将不再可用，因为该视频存储在 RAM 中并且已删除。

注：

- 您必须具有访问虚拟控制台或管理员权限才能播放引导捕获视频和崩溃捕获视频。
- IDRAC GUI 视频播放器中显示的视频捕获时间可能不同于其他视频播放器中显示的视频捕获时间。IDRAC GUI 视频播放器显示 iDRAC 时区的时间，而所有其他视频播放器显示各个操作系统时区的时间。

注： DVC 引□捕□文件不是□□。它□是在服□器引□□程中□行的屏幕序列（每个特定解决方案）。DVC 播放器可□□□些屏幕，□建引□□□。将□□从 DVC（□□快照和差异）□出□ .mov（□□□□）格式□，□□会使用与最初用来□□的□□相同的分辨率或类似的分辨率。需要将□□□出□与捕□□类似的分辨率。

注： 引□捕□文件可用性中出□延□的原因是引□捕□□冲内容在主机启□后不完整。

要查看**引导捕获**屏幕，请单击**维护** > **故障排除** > **视频捕获**。

视频捕获屏幕显示录制视频。有关更多信息，请参阅 *iDRAC 联机帮助*。

注： 当嵌入式□□控制器被禁用且服□器具有附加□□控制器□，□□引□捕□会出□些□延□。因此，将在下次捕□中□□□□的 POST □束消息。

配置视频捕获设置

要配置视频捕获设置，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Maintenance（维护）** > **Troubleshooting（故障排除）** > **Video Capture（视频捕获）**。将显示**视频捕获**页面。
2. 从**视频捕获设置**下拉菜单中，选择下列任一选项：
   - **禁用** — 禁用引导捕获。
   - **捕获，直至缓冲区装满** — 捕获引导顺序，直至达到缓冲区容量。
   - **捕获，直至 POST 结束** — 捕获引导顺序，直至 POST（开机自检）结束。
3. 单击**应用**应用设置。

查看日志

您可以查看系统事件日志 (SEL) 和生命周期日志。有关更多信息，请参阅查看系统事件日志和查看生命周期日志。

查看上次系统崩溃屏幕

上次崩溃屏幕功能可捕获和保存最新的系统崩溃屏幕截图，并在 iDRAC 中显示该截图。这是一项授权的功能。

要查看上次崩溃屏幕：

1. 确保上次崩溃屏幕功能已启用。
2. 在 iDRAC Web 界面中，转至 **Overview（概览）** > **Server（服务器）** > **Troubleshooting（故障排除）** > **Last Crash Screen（上次崩溃屏幕）**。

   Last Crash Screen（上次崩溃屏幕）页面显示受管系统上最新保存的崩溃屏幕。

   单击 **Clear（清除）**可删除上次崩溃屏幕。

注: 一旦 iDRAC 已重设或发生交流电源后重事件，则会清除崩溃捕获的数据。

查看系统状态

系统状态汇总了系统中以下组件的状态：

- 摘要
- 电池
- 散热
- CPU
- 前面板
- 入侵
- 内存
- 网络设备
- 电源设备
- 电压
- 可移除闪存介质
- 机箱控制器

您可以查看受管系统的状态：

- 对于机架和塔式服务器：LCD 前面板和系统 ID LED 状态或 LED 前面板和系统 ID LED 状态。
- 对于刀片服务器：仅限系统 ID LED。

查看系统前面板 LCD 状态

要查看相应机架和塔式服务器的 LCD 前面板状态，请在 iDRAC Web 界面中转至**系统** > **概览** > **前面板**。此时将显示**前面板**页面。

前面板部分显示当前在 LCD 前面板上显示的实时消息。当系统正常工作时（通过 LCD 前面板中的蓝色长亮表示），则**隐藏错误**和**取消隐藏错误**灰显。

注: 您可以仅对机架和塔式服务器隐藏或取消隐藏错误。

根据此选择，文本框会显示当前值。如果您选择用户定义，请在文本框中输入所需消息。字符数限制在 62 以内。如果选择无，LCD 上不会显示任何主页消息。

要使用 RACADM 查看 LCD 前面板状态，请使用 `System.LCD` 组中的对象。有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

查看系统前面板 LED 状态

要查看当前系统 ID LED 状态，请在 iDRAC Web 界面中，转至 **系统** > **概览** > **前面板**。**前面板**部分显示当前前面板状态：

- 蓝色长亮 - 受管系统上没有错误。
- 蓝色闪烁 - 已启用识别模式（无论是否存在受管系统错误）。
- 琥珀色长亮 - 受管系统处于失效保护模式。
- 琥珀色闪烁 - 受管系统上存在错误。

系统正常运行时（通过 LED 前面板上的蓝色运行状况图标指示，**隐藏错误**和**取消隐藏错误**灰显。您仅可以对机架和塔式服务器隐藏或取消隐藏错误。您可以仅对机架和塔式服务器隐藏或取消隐藏错误。

要使用 RACADM 查看系统 ID LED 状态，请使用 `getled` 命令。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

硬件故障指示灯

硬件相关问题包括：

- 未能通电

- 风扇有噪音
- 网络连接丢失
- 硬盘驱动器故障
- USB 介质故障
- 物理损坏

根据具体情况使用下列方法解决问题：
- 重置模块或组件并重新启动系统
- 对于刀片式服务器，请将模块重新插入机箱中不同的插槽。
- 更换硬盘驱动器或 USB 闪存盘
- 重新连接或更换电源和网络电缆

如果问题仍然存在，请参阅 安装和服务手册，网址：https://www.dell.com/poweredgemanuals 中关于硬件设备的特定故障排除信息。

小心：您只能根据□品□明文件中的授权，或者在□机或□□服□和支持□□的指□下□行故障排除和□□□修。任何未□ Dell 授权的服□所□致的□坏均不在保修范□之列。□□□并遵循□品附□的安全□明。

查看系统运行状况

您可以查看 iDRAC、CMC 和 OME-Modular Web 界面上以下组件的状态：
- 电池
- CPU
- 散热
- 侵入
- 内存
- 电源设备
- 可移除闪存介质
- 电压
- 其他

单击**服务器运行状况**部分的任何组件名称，即可查看关于此组件的详细信息。

在服务器状态屏幕上检查错误消息

当 LED 呈琥珀色闪烁并且特定服务器出现错误时，LCD 上的主服务器状态屏幕将以橙色高亮显示受影响的服务器。使用 LCD 导航按钮可高亮度显示受影响的服务器，然后单击中间按钮。将在第 2 行显示错误和警告信息。有关 LCD 面板上显示的错误信息列表，请参阅服务器的《用户手册》。

重新启动 iDRAC

您可以执行软/硬 iDRAC 重启而无需关闭服务器：
- 硬重启动 — 在服务器中，按住 LED 按钮 15 秒。
- 软重启动 — 使用 iDRAC Web 界面或 RACADM。

重置为自定义默认设置 (RTD)

您可以使用“重置为自定义默认设置”功能将自定义配置文件和 RTD 上传为设置。新设置是在保留用户和网络设置的基础上应用的。

“重置为自定义默认设置”功能的选项如下：

- 上传自定义默认设置 —
  - 您可以上传自定义默认设置文件。可以通过导出 XML 格式（此功能不支持 JSON 格式）的服务器配置配置文件 (SCP) 来获取此文件。客户可修改该文件的内容，以添加或删除设置。
  - 您可以使用 iDRAC GUI 或 RACADM 界面上传 SCP XML 文件。
  - 已上传的配置保存在默认数据库中。

- 将当前设置另存为自定义默认设置 —
  - 此操作将当前设置另存为默认设置。
  - 只有通过 RACADM 界面才支持此功能。
- 下载自定义默认设置 —
  - 您可以下载 SCP XML 以获取所有默认设置。
  - 只有通过 RACADM 界面才支持此功能。
- 启动重置为自定义默认设置 —
  - 将应用已上传/保存的默认设置。

使用 iDRAC Web 界面重设 iDRAC

要重置 iDRAC，请在 iDRAC Web 界面中执行以下操作之一：

- 上传自定义默认设置文件：
  - 转至**配置** > **服务器配置文件** > **自定义默认设置** > **上传自定义默认设置**
  - 从本地共享路径上传自定义的 *CustomConfigured.xml* 文件
  - 单击**应用**。此时将会创建新的上传自定义默认设置作业。
- 重置为自定义默认设置：
  - 当"上传自定义默认设置"作业成功时，转至**维护** > **诊断**，单击**将 iDRAC 重置为出厂默认设置**选项。
  - 选择**放弃所有设置**并设置为**自定义默认设置配置**。
  - 单击**继续**以启动"重置为自定义默认设置"配置。

使用 RACADM 重设 iDRAC

要重新启动 iDRAC，请使用 **racreset** 命令。有关更多信息，请参阅 机箱管理控制器 RACADM CLI 指南，*网址：*https://www.dell.com/cmcmanuals。有关更多信息，请参阅 *适用于 PowerEdge MX7000 机箱的 OME - Modular RACADM CLI 指南*，网址：https://www.dell.com/openmanagemanuals

对于重置为默认设置的操作，请使用以下命令：

- 上传自定义默认设置文件 — `racadm -r <iDracIP> -u <username> -p <Password> set -f <filename> -t xml --customdefaults`
- 将当前设置另存为默认设置 — `racadm -r <iDracIP> -u <username> -p <Password> set --savecustomdefaults`
- 下载自定义默认设置 — `racadm -r <iDracIP> -u <username> -p <Password> get -f <filename> -t xml --customdefaults`
- 重置为自定义默认设置 — `Racadm -r <iDracIP> -u <username> -p <Password> racresetcfg -custom`

擦除系统和用户数据

注: 不支持从 iDRAC GUI 擦除系统和用户数据。

您可以擦除系统组件和以下组件的用户数据。

- BIOS 重设为默认值
- 嵌入式诊断程序
- 嵌入式操作系统驱动程序包
- Lifecycle Controller 数据
- iDRAC 重设为默认值
- 覆盖不支持即时安全擦除 (ISE) 的硬盘
- 重设控制器高速缓存
- 重设 vFLASH
- 擦除支持 ISE 的硬盘、SSD 和 NVMe
- 清除所有操作系统应用程序

执行系统擦除之前，请确保：

- 您拥有 iDRAC 服务器控制权限。
- 已启用 Lifecycle Controller。

Lifecycle Controller 数据选项将擦除任何内容，例如 LC 日志、配置数据库、回滚固件、出厂附带日志以及 FP SPI（或管理提升板）中的配置信息。

注: Lifecycle Controller 日志包含有关系统擦除请求的信息，以及在 iDRAC 重启时生成的任何信息。所有之前的信息都会删除。

您可以使用 **SystemErase** 命令删除单个或多个系统组件：

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

其中，

- BIOS - BIOS 重设为默认值
- DIAG - 嵌入式诊断程序
- DRVPACK - 嵌入式操作系统驱动程序包
- LCDATA - 清除 Lifecycle Controller 数据
- iDRAC - iDRAC 重设为默认值
- overwritepd —覆盖不支持即时安全擦除 (ISE) 的硬盘驱动器
- percnvcache — 重设控制器高速缓存
- vflash — 重设 vFLASH
- secureerasepd — 擦除支持 ISE 的硬盘驱动器、SSD 和 NVMes
- allapps — 清除所有操作系统应用程序

注: 擦除 vFlash 时，请确保在执行操作之前已分离 vFlash 卡上的所有分区。

注: 如果服务器上已启用 SEKM，则在使用此命令之前，请使用 `racadm sekm disable` 命令禁用 SEKM。如果通过执行此命令从 iDRAC 中擦除了 SEKM 设置，则这可以避免被 iDRAC 保护的所有存储设备被锁定。

有关更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

注: Dell 技术中心链接显示在 Dell 品牌系统上的 iDRAC GUI 中。如果您使用 WSMan 命令擦除系统数据，然后想该链接再次出现，请手动重新引导主机，并等待 CSIOR 运行。

注: 您运行系统擦除后，VD 可能仍然会显示。完成系统擦除并重新引导 iDRAC 后，运行 CSIOR。

将 iDRAC 重设为出厂默认设置

您可以使用 iDRAC 设置公用程序或 iDRAC Web 界面将 iDRAC 重设为出厂默认设置。

使用 iDRAC Web 界面将 iDRAC 重设为出厂默认设置

要使用 iDRAC Web 界面将 iDRAC 重设为出厂默认设置，请执行以下操作：

1. 转至 **Maintenance（维护）** > **Diagnostics（诊断程序）**。
   随即会显示 **Diagnostics Console**（诊断控制台）页面。
2. 单击 **Reset iDRAC to Default Settings**（将 iDRAC 重设为默认设置）。
   完成状态以百分比显示。iDRAC 将重新引导并还原至出厂默认设置。iDRAC IP 将重设且不可访问。您可以使用前面板或 BIOS 配置 IP。

使用 iDRAC 设置公共程序将 iDRAC 重设为出厂默认设置

要使用 iDRAC 设置公用程序将 iDRAC 重设为出厂默认值，请执行以下操作：

1. 转至 **Reset iDRAC configurations to defaults**（将 iDRAC 配置重设为默认值）。
   此时将显示 **iDRAC Settings Reset iDRAC configurations to defaults**（iDRAC 设置将 iDRAC 配置重设为默认值）页面。
2. 单击**是**。
   iDRAC 重设启动。
3. 单击 **Back**（上一步）导航至同一 **Reset iDRAC configurations to defaults**（将 iDRAC 配置重设为默认值）页面，查看成功消息。

28

iDRAC 中的 SupportAssist 集成

SupportAssist 允许您创建 SupportAssist 收集，并利用其他 SupportAssist 功能以监测您的系统和数据中心。iDRAC 提供了一个应用程序接口，用于收集启用支持服务的平台信息，有助于您解决平台和系统问题。iDRAC 有助于您生成服务器的 SupportAssist 收集，然后将该收集导出到管理站（本地）上的一个位置，或导出到一个共享的网络位置（如 FTP、简单文件传输协议 (TFTP)、HTTP、HTTPS、通用 Internet 文件系统 (CIFS) 或网络文件共享 (NFS)）。此收集以标准 ZIP 格式生成。可将此收集发送至技术支持部门进行故障排除或收集资源清册。

主□：

SupportAssist 注册

要利用 SupportAssist 的自动化、主动性和预测性功能，您必须使用 SupportAssist 注册您的系统。

您可以在本地或网络上生成并保存集合，也可以发送给 Dell EMC 而无需注册。

注： 某些 OEM 客户没有型号名称。后端 Support Assist 不允许向戴尔注册此类系统。

联系人和发运信息

要完成注册，您必须提供联系人和发运信息。

主要联系人信息

输入公司名称、国家地区、名字*、姓氏*、电话号码*、备用号码和电子邮件地址*。检查详细信息是否正确显示并做出更改（如果您想要编辑任何字段）。

* 表示该字段为必填项。

第二联系人信息

输入名字、姓氏、电话号码、备用电话号码和电子邮件地址，并检查详细信息是否显示正确，并在想要编辑任何字段时便进行修改。

注： 您可以随时删除第二联系人信息。

自动派送

当通过已针对 SupportAssist 注册的 iDRAC 向 Dell-EMC 报告严重事件时，可能会启动自动派送工作流程。此工作流程基于所转发的事件以及注册设备 SupportAssist 保修级别。在 SupportAssist 注册过程中，您必须输入**派送信息**才能启用自动派送工作流程。如果需要现场支持及派送部件，则选择**现场支持及派送部件**。

注: 在具有 iDRAC Service Module (iSM) v3.4.0 for Windows 的系统中启用了自动派送。将来的 iSM 的版本将针对其他操作系统支持自动派送。

派送地址

输入地址和首选联系时间。

终端用户许可协议

提供所有所需的信息后，您需要接受终端用户许可协议 (EULA) 以完成注册过程。您可以选择打印 EULA 以进行进一步的参考。您可以随时取消和终止注册过程。

安装服务模块

要注册和使用 SupportAssist，您必须在系统安装 iDRAC 服务模块 (iSM)。一旦您**启动服务模块安装**，您可以看到安装说明。**Next（下一步）**按钮将一直保持禁用，直到您成功安装 iSM。

服务器操作系统代理信息

如果出现连接问题，则将提示用户提供操作系统代理信息。输入**服务器、端口、用户名**和**密码**，以配置代理设置。

SupportAssist

SupportAssist 配置完成后，您可以检查 SupportAssist 仪表板以查看**服务请求摘要**、**保修状态**、**SupportAssist 概述**、**服务请求**和**收集日志**。查看或发送收集日志无需注册。

服务请求门户

服务请求详细显示了每个事件的**状态**（打开/关闭）、**说明**、**来源**（时间/电话）、**服务请求 ID**、**打开日期**和**关闭日期**。您可以选择和查看每个事件的进一步详情。您可以选择检查服务请求门户以查看任何单个案例的其它信息。

集合日志

收集日志显示**收集日期和时间**、**收集类型**（手动、计划、基于事件）、**收集的数据**（自定义选项、所有数据）、**收集状态**（已完成但有错误、完成）、**作业 ID**、**发送状态**和**发送日期和时间**的详细信息。您可以将 iDRAC 中的最后一个持久集合发送到 Dell。

注: 生成后，收集日志详细信息将被过滤，以根据用户选择删除个人身份信息 (PII)。

生成 SupportAssist 收集

要生成操作系统和应用程序日志：

- 必须在主机操作系统中安装和运行 iDRAC Service Module。
- OS Collector 出厂安装在 iDRAC 中，如果已移除，则必须安装在 iDRAC 中。

如果您与技术支持合作解决服务器问题，但安全策略限制直接连接 Internet，那么您可以为技术支持提供必要的数据，以便于故障排除问题，而不必安装软件或者从 Dell 下载工具，也无需从服务器操作系统或 iDRAC 访问 Internet。

您可以生成服务器的运行状况报告，然后导出收集日志：

- 到管理站（本地）上的一个位置。
- 到共享网络位置，例如通用 Internet 文件系统 (CIFS) 或网络文件共享 (NFS)。要导出到网络共享（如 CIFS 或 NFS），需要直接通过网络连接到 iDRAC 共享或专用网络端口。
- 针对 Dell EMC。

SupportAssist Collection 将以标准 ZIP 格式生成。收集可能包含以下信息：

- 所有组件的硬件资源清册（包括系统组件配置和固件详细信息、母板系统事件日志、iDRAC 状态信息和 Lifecycle Controller 日志）。
- 操作系统和应用程序信息。
- 存储控制器日志。
- iDRAC 调试日志
- 它包含收集完成后即可进行访问的 HTML5 查看器。
- 收集以用户友好的格式提供了大量的详细系统信息和日志，无需将收集上传到技术支持网站即可进行查看。

生成数据后，您可以查看其中包含多个 XML 文件和日志文件的数据。

每次执行数据收集时，将在 Lifecycle Controller 日志中记录一个事件。事件包含诸如报告发起用户、所使用的接口以及导出日期和时间等信息。

在 Windows 上，如果 WMI 已禁用，则 OS Collector 收集操作会停止，并显示一条错误消息。

检查相应的权限级别，并确保防火墙或安全设置不会阻止收集注册表或软件数据。

在生成运行状况报告前，请确保：

- 已启用 Lifecycle Controller。
- 已启用 Collect System Inventory On Reboot (CSIOR)（重新引导时收集系统资源清册 [CSIOR]）。
- 您有登录和服务器控制权限。

使用 iDRAC Web 界面手动生成 SupportAssist 收集

要手动生成 SupportAssist 收集，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**维护** > **SupportAssist**。
2. 如果未为 SupportAssist 注册服务器，则会显示 SupportAssist 注册向导。单击**取消** > **取消注册**。
3. 单击**开始收集**。
4. 选择要包含在收集中的数据集。
5. 您可以选择筛选 PII 收集。
6. 选择需要将 Collection 保存到的目标。
   a. 如果服务器已连接到互联网，并且**立即发送**选项已启用，则选择此选项将收集日志导出到 Dell EMC SupportAssist。
   b. **保存在本地**选项允许您在本地系统中保存生成的 Collection。
   c. **保存到网络**选项可将生成的 Collection 保存到用户定义的 CIFS 或 NFS 共享位置。

      注: 如果已选择*保存到网络*且没有可用的默认位置，则所提供的网络详细信息将保存到未来收集的默认位置。如果默认位置已存在，则收集将仅使用指定的详情一次。

   如果已选择**保存到网络**选项，则用户提供的网络详细信息将另存为默认值（如果未保存之前的网络共享位置），以用于今后进行的任何收集。
7. 单击**收集**以继续生成 Collection。
8. 如果出现提示，请接受**最终用户级别协议 (EULA)**以继续。

   如果存在以下状况，则 OS 和应用程序数据选项将变为灰色且不可选：
   - 主机操作系统中未安装或运行 iSM，或
   - 已从 iDRAC 中移除 OS Collector，或
   - 在 iDRAC 中已禁用 OS-BMC 直通功能，或
   - 之前收集的缓存操作系统应用程序数据在 iDRAC 中不可用

设置

此页面允许您配置收集日志设置，如果已注册，则您可以更新联系人详细信息，启用或禁用电子邮件通知，以及更改语言设置。

收集设置

您可以将集合保存到首选的网络位置。使用 **Set Archive Directory（设置存档目录）**可以设置网络位置。您可以将收集保存到首选的网络位置。使用“Set Archive Directory”（设置存档目录）以设置网络位置。测试网络连接之前，请输入您要选择的协议类型 (CIFS/NFS)、相应的 IP 地址、共享名称、域名称、用户名称和密码。“Test Network Connection”（测试网络连接）按钮将确认与目标共享的连接。

如果已注册，您可以在“Collection Settings”（收集设置）中选择当您将数据发送到 Dell 时包括标识信息。

允许您启用和计划 **Automatic Collection（自动收集）**选项以避免任何手动干预，并保持对系统的定期检查。默认情况下，在触发事件并创建支持案例时，SupportAssist 会配置为自动从生成警报并上传至 Dell 的设备收集系统日志。您可以启用或禁用基于事件的自动收集。您可以计划基于合适的要求自动收集。可用选项为每周、每月、每季度或从不。此外，您还可配置计划的定期事件的日期和时间。配置自动收集时，您可以选择启用或禁用 **ProSupport Plus Recommendation Report（ProSupport Plus 建议报告）**。

联系信息

此页面显示了在注册 SupportAssist 过程中已添加的详细联系信息，并允许您进行更新。

29

常见问题

本部分列出了下列常见问题：

- 系统事件日志
- 网络安全性
- Active Directory
- 单一登录
- 智能卡登录
- 虚拟控制台
- 虚拟介质
- vFlash SD 卡
- SNMP 验证
- 存储设备
- iDRAC 服务模块
- RACADM
- 其他

主□：

- 系□事件日志
- iDRAC 警□的自定□□件人□子□件配置
- 网□安全性
- 遥□流式□□
- Active Directory
- □一登□
- 智能卡登□
- 虚□控制台
- 虚□介□
- vFlash SD 卡
- SNMP □□
- 存□□□
- GPU（加速器）
- iDRAC 服□模□
- RACADM
- 永久□置默□密□至 calvin
- 其他

系统事件日志

通过 Internet Explorer 使用 iDRAC Web 界面时，为什么 SEL 不使用“另存为”选项进行保存?

这是由于浏览器设置。要解决此问题，请执行以下操作：

1. 在 Internet Explorer 中，转至 **Tools（工具）** > **Internet Options（Internet 选项）** > **Security（安全）**，选择要尝试下载至其中的区域。

   例如，如果 iDRAC 设备位于本地内部网中，则选择**本地 Intranet**，然后单击**自定义级别...**。

2. 在**安全设置**窗口的**下载**下，确保启用以下选项：
   - Automatic prompting for file downloads（文件下载的自动提示）（如果此选项可用）
   - File download（文件下载）

   小心: 要确保用于访问 iDRAC 的计算机的安全，请不要在其他下启用启动应用程序和不安全文件选项。

iDRAC 警报的自定义发件人电子邮件配置

警报生成的电子邮件不是来自在基于云的电子邮件服务上设置的自定义发件人电子邮件。

您需要通过此过程注册云电子邮件：Support.google.com。

网络安全性

访问 iDRAC Web 界面时，系统会显示一条安全警告以声明证书认证机构 (CA) 所颁发的 SSL 证书不可信。

iDRAC 包含一个默认的 iDRAC 服务器证书来确保在通过基于 Web 的界面和远程 RACADM 进行访问时的网络安全。该证书不是由可信 CA 颁发的。要解决此问题，请上载一个由可信 CA（例如，Microsoft Certificate Authority、Thawte 或 Verisign）颁发的 iDRAC 服务器证书。

为什么 DNS 服务器不注册 iDRAC?

某些 DNS 服务器注册包含多达 31 个字符的 iDRAC 名称。

访问 iDRAC 基于 Web 的界面时，系统会显示一条安全警告来声明 SSL 证书主机名与 iDRAC 主机名不匹配。

iDRAC 包含一个默认的 iDRAC 服务器证书来确保在通过基于 Web 的界面和远程 RACADM 进行访问时的网络安全。如果使用该证书，Web 浏览器会显示一条安全警告，因为颁发给 iDRAC 的默认证书与 iDRAC 主机名（例如，IP 地址）不匹配。

要解决此问题，请上载一个颁发给该 IP 地址或 iDRAC 主机名的 iDRAC 服务器证书。当生成 CSR（用于颁发证书）时，请确保 CSR 的常用名 (CN) 与 iDRAC IP 地址（如果证书颁发给 IP）或注册的 DNS iDRAC 名称（如果证书颁发给 iDRAC 注册的名称）匹配。

要确保 CSR 与注册的 DNS iDRAC 名称匹配：

1. 在 iDRAC Web 界面中，转至**概览** > **iDRAC 设置** > **网络**。随即会显示**网络**页面。
2. 在**常见设置**部分：
   - 选择**在 DNS 上注册 iDRAC** 选项。
   - 在 **DNS iDRAC 名称**字段中，输入 iDRAC 名称。
3. 单击**应用**。

为什么我无法从我的 Web 浏览器访问 iDRAC?

如果启用了 HTTP Strict Transport Security (HSTS)，则可能会出现此问题。HSTS 是一种 Web 安全机制，它允许 Web 浏览器只使用安全的 HTTPS 协议而不是 HTTP 进行交互。

在您的浏览器上启用 HTTPS 并登录到 iDRAC 以解决此问题。

为什么我无法完成涉及远程 CIFS 共享的操作?

如果只使用 SMBv1，则涉及 CIFS 共享的导入/导出或任何其他远程文件共享操作都会失败。请确保已在提供 SMB/CIFS 共享的服务器上启用 SMBv2 协议。有关如何启用 SMBv2 协议的信息，请参阅操作系统文档。

遥测流式传输

在流式传输 Rsyslog 服务器的遥测报告时，少量报告数据缺失。

较早版本的 rsyslog 服务器可能会在某些报告中偶尔缺失少量报告数据。您可以升级到较新版本，以避免此问题。

Active Directory

Active Directory 登录失败。如何解决此问题?

要对问题进行诊断 **Active Directory Configuration and Management（Active Directory 配置管理）**页面，单击 **Test Settings（测试设置）**。检查测试结果并修复问题。更改配置并运行测试，直到测试用户通过授权步骤。

通常，请检查下列项目：

- 登录时，请确保您使用正确的用户域名（而不是 NetBIOS 名称）。如果您有本地 iDRAC 用户帐户，请使用本地凭据登录 iDRAC。登录后，请确保：

- 在 **Active Directory 配置和管理**页面上选中**启用 Active Directory** 选项。
- **iDRAC 网络配置**页面上的 DNS 设置正确。
- 如果已启用证书验证，则将正确 Active Directory 根 CA 证书上载到 iDRAC。
- 如果您使用扩展架构，iDRAC 名称和 iDRAC 域名与 Active Directory 环境配置匹配。
- 如果您使用标准架构，组名和组域名与 Active Directory 配置匹配。
- 如果用户和 iDRAC 对象位于不同的域中，则不要选择 **User Domain from Login（登录的用户域）**选项。而应选择 **Specify a Domain（指定域）**选项并输入 iDRAC 对象所在的域名。

- 检查域控制器 SSL 证书以确保 iDRAC 时间在证书有效期内。

Active Directory 登录失败，即使已启用证书验证。测试结果显示以下错误消息。为什么会发生这种情况，如何解决?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct
Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if
the iDRAC date is within the valid period of the certificates and if the Domain
Controller Address configured in iDRAC matches the subject of the Directory Server
Certificate.
```

如果已启用证书验证，当 iDRAC 与目录服务器建立 SSL 连接时，iDRAC 将使用已上传的 CA 证书验证目录服务器证书。导致证书验证失败的最常见原因包括：

- iDRAC 日期不在服务器证书或 CA 认证的有效时间段内。检查证书的 iDRAC 时间和有效时间段。
- 在 iDRAC 中配置的域控制器地址与目录服务器证书的主题或主题备用名称不匹配。如果您使用 IP 地址，请阅读下一个问题。如果您使用 FQDN，请确保您使用的是域控制器的 FQDN，而不是域。例如，是 **servername.example.com** 而不是 **example.com**。

即使使用 IP 地址作为域控制器地址，证书验证也会失败。如何解决此问题?

检查域控制器证书的“Subject or Subject Alternative Name”（主题或主题备用名称）字段。正常情况下，Active Directory 使用主机名称而不是域控制器证书的“Subject or Subject Alternative Name”（主题或主题备用名称）字段中域控制器的 IP 地址。要解决此问题，请执行以下操作之一：

- 在 iDRAC 上将域控制器的主机名 (FQDN) 配置为*域控制器地址*，以与服务器证书的主题或主题备用名称匹配。
- 重新颁发服务器证书以在“主题”或“主题备用名称”字段中使用 IP 地址，从而与在 iDRAC 中配置的 IP 地址匹配。
- 如果选择信任此域控制器而无需在 SSL 握手过程中验证证书，请禁用证书验证。

当在多域环境中使用扩展架构时，如何配置域控制器地址?

这必须是 iDRAC 对象所在域中域控制器的主机名 (FQDN) 或 IP 地址。

何时配置 Global Catalog Address（全局编录地址）?

如果您使用标准架构且用户和角色组来自不同的域，则必须填写全局编录地址。在此情况下，您只能使用通用组。

如果使用的是标准架构且所有用户和角色组都在相同域中，则不必配置全局编录地址。

如果使用的是扩展架构，则不使用全局编录地址。

标准架构的查询方式是什么?

iDRAC 首先连接到所配置的域控制器地址。如果用户和角色组位于该域中，则保存权限。

如果配置了全局控制器地址，则 iDRAC 会继续查询全局编录。如果从全局编录检索到额外的权限，则会累加这些权限。

iDRAC 始终在 SSL 上使用 LDAP 吗?

可以。所有传输都通过安全端口 636 和/或 3269 进行传输。在测试设置过程中，iDRAC 仅执行 LDAP CONNECT 以隔离该问题，而不是在非安全连接上执行 LDAP BIND。

为什么 iDRAC 默认启用证书验证?

iDRAC 强制实行强大的安全性，以确保 iDRAC 连接到域控制器的身份。没有证书验证，黑客可以欺骗域控制器并劫持 SSL 连接。如果您选择信任安全边界内的所有域控制器而无需验证证书，那么您可通过 Web 界面或 RACADM 将其禁用。

iDRAC 是否支持 NetBIOS 名称?

此版本不支持。

为什么使用 Active Directory 单一登录或智能卡登录时需要长达四分钟才能登录到 iDRAC?

Active Directory 单一登录和智能卡登录通常只需要不到 10 秒钟就能完成，但是如果您指定了首选 DNS 服务器和备用 DNS 服务器，而首选 DNS 服务器已发生故障，则可能需要长达四分钟才能登录。DNS 服务器停机时预期会出现 DNS 超时。iDRAC 将使用备用 DNS 服务器让您登录。

Active Directory 配置为 Windows Server 2008 Active Directory 中存在的域。该域中有一个子域，用户和组位于同一子域并且用户是组的成员。尝试使用子域中的用户登录 iDRAC 时，Active Directory 单一登录将失败。

这可能由于组类型不正确。Active Directory 服务器中有两种组类型：

- Security（安全） - 安全组允许您管理用户并使用计算机访问共享资源以及筛选组策略设置。
- 分发 - 分发组仅供用于电子邮件分发列表。

始终确保该组类型是安全的。您不能使用分发组在任何对象上分配权限，但是可以使用它们来筛选组策略设置。

单一登录

在 Windows Server 2008 R2 x64 上 SSO 登录失败。解决此问题所需的设置是什么?

1. 为域控制器和域策略运行 **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** 中介绍的操作。
2. 配置计算机以使用 DES-CBC-MD5 密码组。

   这些设置可能会影响您的环境中客户端计算机或服务与应用程序的兼容性。Kerberos 策略设置允许的配置加密类型位于：**Computer Configuration（计算机配置）** > **Security Settings（安全设置）** > **Local Policies（本地策略）** > **Security Options（安全选项）**。
3. 请确保域客户端具有更新的 GPO。
4. 在命令行处，键入 `gpupdate /force` 并使用 `klist purge` 命令删除旧 Keytab。
5. 更新 GPO 后，创建新的 keytab。
6. 将 keytab 上载到 iDRAC。

现在可以使用 SSO 登录 iDRAC。

为什么在 Windows 7 和 Windows Server 2008 R2 上，Active Directory 用户进行单一登录失败?

您必须启用 Windows 7 和 Windows Server 2008 R2 的加密类型。要启用加密类型：

1. 以管理员或具有管理权限的用户身份登录。
2. 转至**开始**并运行 **gpedit.msc**。将显示 **ocal Group Policy Editor（本地组策略编辑器）**窗口。
3. 转至 **Local Computer Settings（本地计算机设置）** > **Windows Settings（Windows 设置）** > **Security Settings（安全设置）** > **Local Policies（本地策略）** > **Security Options（安全选项）**。
4. 右键单击 **Network Security: Configure encryption types allowed for kerberos（网络安全：配置 Kerberos 允许的加密类型）**并选择 **Properties（属性）**。
5. 启用所有选项。
6. 单击 **OK（确定）**。现在可以使用 SSO 登录 iDRAC。

对于 Extended Schema（扩展架构），执行以下附加设置：

1. 在 **Local Group Policy Editor（本地组策略编辑器）**窗口中，导航至 **Local Computer Settings（本地计算机设置）** > **Windows Settings（Windows 设置）** > **Security Settings（安全设置）** > **Local Policies（本地策略）** > **Security Options（安全选项）**。
2. 右键单击 **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote server（网络安全：限制 NTLM：发往远程服务器的出站 NTLM 通信量）**并选择 **Properties（属性）**。
3. 选择 **Allow all（全部允许）**，单击 **OK（确定）**，然后关闭 **Local Group Policy Editor（本地组策略编辑器）**窗口。
4. 转至**开始**并运行 cmd。此时将显示命令提示符窗口。
5. 运行命令 `gpupdate /force`。组策略将更新。关闭命令提示符窗口。
6. 转至**开始**并运行 regedit。此时将显示 **Registry Editor（注册表编辑器）**窗口。
7. 导航至 **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Control** > **LSA**。
8. 在右侧窗格中，右键单击并选择 **New（新建）** > **DWORD (32-bit) Value（DWORD [32 位] 值）**。
9. 将新注册表项命名为 **SuppressExtendedProtection**。
10. 右键单击 **SuppressExtendedProtection** 并单击 **Modify（修改）**。
11. 在 **Value data（值数据）**字段中键入 **1** 并单击 **OK（确定）**。
12. 关闭 **Registry Editor** 窗口。现在可以使用 SSO 登录 iDRAC。

如果为 iDRAC 启用了 SSO 并使用 Internet Explorer 登录 iDRAC，SSO 会失败并提示输入用户名和密码。如何解决此问题?

确保 iDRAC IP 地址列在 **Tools（工具）** > **Internet Options（选项）** > **Security（安全性）** > **Trusted sites（可信站点）**中。如果未列出，SSO 将失败并提示输入用户名和密码。单击 **Cancel（取消）**并继续。

智能卡登录

使用 Active Directory 智能卡登录功能登录 iDRAC 需要最多四分钟时间。

正常的 Active Directory 智能卡登录过程通常不超过 10 秒，但如果您在**网络**页面中指定了首选 DNS 服务器和备用 DNS 服务器，并且首选 DNS 服务器失败，则可能需要长达四分钟。DNS 服务器停机时预期会出现 DNS 超时。iDRAC 将使用备用 DNS 服务器让您登录。

ActiveX 插件无法检测到智能卡阅读器。

确保 Microsoft Windows 操作系统支持智能卡。Windows 支持有限的几种智能卡加密服务提供程序 (CSP)。

一般来说，要检查特定客户端上是否存在智能卡 CSP，在出现 Windows 登录 (Ctrl-Alt-Del) 屏幕时将智能卡插入读卡器并查看 Windows 是否检测到智能卡并显示 PIN 对话框。

智能卡 PIN 不正确。

检查智能卡是否因不正确的 PIN 尝试次数过多而锁定。在这种情况下，请联系智能卡发卡机构获取新的智能卡。

虚拟控制台

启动虚拟控制台需要什么 Java 版本？

您需要 Java 8 或更高版本以使用此功能通过 IPv6 网络启动 iDRAC 虚拟控制台。

即使您已从 iDRAC Web 界面注销，虚拟控制台会话仍然保持活动。这是预期的行为吗？

可以。关闭虚拟控制台查看器窗口可以登出相应的会话。

在服务器上的本地视频关闭时可以启动新的远程控制台视频会话吗？

可以。

为什么请求关闭本地视频后需要 15 秒才能关闭服务器上的本地视频？

使本地用户有机会在视频关闭前采取某些操作。

打开本地视频时有时间延迟吗？

没有，iDRAC 收到本地视频打开请求后，视频就立刻打开。

本地用户也可以关闭或打开视频吗？

当本地控制台禁用时，本地用户不能关闭或打开视频。

关闭本地视频是否也会关闭本地键盘和鼠标？

否。

关闭本地控制台是否会关闭远程控制台会话上的视频？

不会，打开或关闭本地视频与远程控制台会话无关。

iDRAC 用户打开或关闭本地服务器视频需要什么权限？

任何具有 iDRAC 配置权限的用户都可以打开或关闭本地控制台。

如何获得本地服务器视频的最新状况？

状况信息显示在虚拟控制台页面上。

要显示对象 `iDRAC.VirtualConsole.AttachState` 的状态，请使用以下命令：

```
racadm get idrac.virtualconsole.attachstate
```

或者从 SSH 或远程会话使用下列命令：

```
racadm -r (iDrac IP) -u (username) -p (password) get iDRAC.VirtualConsole.AttachState
```

在虚拟控制台 OSCAR 显示中也会看到状态。本地控制台启用后，会在服务器名称旁边显示绿色状态。禁用时，黄色圆点表示 iDRAC 已经锁定本地控制台。

为什么在虚拟控制台窗口中看不到系统屏幕底部？

确保 Management Station 的显示器分辨率设置为 1280x1024。

为什么 Virtual Console Viewer 窗口在 Linux 操作系统中出现乱码？

Linux 上的控制台查看器需要 UTF-8 字符集。检查区域设置并重设字符集（如果需要）。

为什么 Lifecycle Controller 中 Linux 文本控制台下的鼠标不同步？

虚拟控制台需要 USB 鼠标驱动程序，但 USB 鼠标驱动程序仅在 X-Window 操作系统下可用。在虚拟控制台查看器中，执行下列任一操作：

- 转至**工具** > **会话选项** > **鼠标**选项卡。在**鼠标加速**，选择 **Linux**。
- 在**工具**菜单下，选择**单一光标**选项。

如何在 Virtual Console Viewer 窗口中同步鼠标指针?

在启动虚拟控制台会话前，确保为操作系统选择了正确的鼠标。

确保已经选中 iDRAC 虚拟控制台客户端上的**单一光标**选项（位于 iDRAC 虚拟控制台菜单的**工具**下）。默认为双光标模式。

通过虚拟控制台远程安装 Microsoft 操作系统时，可以使用键盘或鼠标吗?

否。当您在 BIOS 中已启用虚拟控制台的系统上远程安装支持的 Microsoft 操作系统时，系统将发送 EMS 连接信息，要求您远程选择**确定**。您必须在本地系统上选择**确定**，或者重新启动远程管理的服务器，重新安装，然后在 BIOS 中关闭虚拟控制台。

此信息由 Microsoft 生成，用来提醒用户虚拟控制台已启用。要确保不显示此消息，请务必关闭 iDRAC 设置公用程序中的虚拟控制台，然后再远程安装操作系统。

为什么 Management Station 上的数字锁定指示灯不能反映远程服务器上数字锁定的状态?

当通过 iDRAC 访问时，管理站上的 Num Lock 指示灯不一定与远程服务器上的 Num Lock 保持一致。Num Lock 的状态取决于连接远程会话时远程服务器的设置，与管理站上的 Num Lock 状态无关。

为什么从本地主机建立虚拟控制台会话时显示多个 Session Viewer 窗口?

您正在从本地系统配置虚拟控制台会话。此操作不受支持。

如果虚拟控制台会话正在进行并且有本地用户访问受管服务器，第一个用户是否会收到警告信息?

否。如果本地用户访问系统，两者都有系统控制权。

运行虚拟控制台会话需要多少带宽?

建议使用 5 MBPS 连接以获得良好性能。最低性能需要 1 MBPS 连接速度。

管理站运行虚拟控制台有什么最低系统要求?

management station 要求 Intel Pentium III 500 MHz 处理器和至少 256 MB RAM。

为什么虚拟控制台查看器窗口有时会显示“无信号”的消息?

您看到此消息可能是因为 iDRAC 虚拟控制台插件未接收到远程服务器桌面视频。一般情况下，当远程服务器关闭时，可能会出现此行为。有时，可能会因为远程服务器桌面视频接收故障而显示此消息。

为什么 Virtual Console Viewer 窗口有时会显示超出范围的信息?

您看到此信息可能是因为捕获视频所需的参数超出 iDRAC 能够捕获视频的范围。显示分辨率或刷新率等参数过高会导致超出范围的情况。通常，物理限制（例如视频内存大小或带宽）可设置参数的最大范围。

从 iDRAC Web 界面启动虚拟控制台会话时，为什么会显示 ActiveX 安全弹出窗口?

iDRAC 可能未在受信任的站点列表中。要防止在每次启动虚拟控制台会话时显示安全弹出窗口，请将 iDRAC 添加到客户端浏览器的受信站点列表中：

1. 单击**工具** > **Internet 选项** > **安全** > **可信站点**。
2. 单击**站点**并输入 iDRAC 的 IP 地址或 DNS 名称
3. 单击**添加**。
4. 单击**自定义级别**。
5. 在**安全设置**窗口中，在**下载未签名的 ActiveX 控件**下选择**提示**。

为什么 Virtual Console Viewer 窗口为空白?

如果您有虚拟介质权限，但没有虚拟控制台权限，那么可以启动查看器访问虚拟介质功能，但不会显示受管服务器的控制台。

使用虚拟控制台时，为什么鼠标在 DOS 中不同步?

Dell BIOS 将鼠标驱动程序模拟为 PS/2 鼠标。根据设计，PS/2 鼠标使用鼠标指针的相对位置，这会造成同步延迟。iDRAC 带有 USB 鼠标驱动程序，允许使用绝对位置并且能够提供距离更近的鼠标指针跟踪。即使 iDRAC 将 USB 的绝对鼠标位置传递给 Dell BIOS，BIOS 仿真也会将其转换为相对位置并且行为保持不变。要修复此问题，在配置屏幕中将鼠标模式设置为“USC/Diags”。

启动虚拟控制台后，鼠标的光标在虚拟控制台中可活动，但在本地系统中不活动。为什么会发生这种情况，如何解决?

如果将**鼠标模式**设置为 **USC/Diags**，就会发生这种情况。按下 **Alt+M** 热键即可在本地系统上使用鼠标。再次按下 **Alt + M** 可使用虚拟控制台上的鼠标。

启动虚拟控制台之后立刻从 CMC 启动 iDRAC 界面时，为什么 GUI 会话会超时?

从 CMC Web 界面启动 iDRAC 的虚拟控制台时，将打开弹出窗口以启动虚拟控制台。虚拟控制台打开后不久弹出窗口将关闭。

在管理站上针对同一 iDRAC 系统启动 GUI 和虚拟控制台时，如果在弹出窗口关闭之前 GUI 已启动，则 iDRAC GUI 会话超时。如果在弹出窗口和虚拟控制台关闭后从 CMC Web 界面启动 iDRAC GUI，此问题不会出现。

注: 不适用于 MX 平台。

为什么 Linux SysRq 键在 Internet Explorer 上无法使用?

Linux SysRq 键行为与从 Internet Explorer 使用虚拟控制台时不同。要发送 SysRq 键，在按住 **Ctrl** 和 **Alt** 键的同时，按下 **Print Screen** 键后释放在使用 Internet Explorer 的同时，要通过 iDRAC 将 SysRq 键发送到远程 Linux 服务器，请执行以下操作：

1. 激活远程 Linux 服务器上的魔术键功能。您可以使用以下命令在 Linux 终端上进行激活：

```
echo 1 > /proc/sys/kernel/sysrq
```

2. 激活 Active X Viewer 的键盘直通模式。
3. 按下 **Ctrl+Alt+Print Screen**。
4. 仅释放 **Print Screen**。
5. 按下 **Print Screen+Ctrl+Alt**.

注: Internet Explorer 和 Java 当前不支持 SysRq 功能。

为什么在虚拟控制台底部显示“连接中断”的信息?

在服务器重新引导过程中使用共享网络端口时，iDRAC 将断开连接，同时 BIOS 重设网卡。如果使用的是 10 Gb 网卡，此持续时间会较长，而且如果连接的网络交换机已启用生成树协议 (STP)，则持续时间会非常长。在这种情况下，建议您为连接到服务器的交换机端口启用 PortFast。在大多数情况下，虚拟控制台将自行还原。

更新 iDRAC 固件后，借助 Java 插件启动虚拟控制台失败。

删除 Java 高速缓存，然后启动虚拟控制台。

使用 Web 服务器端口 (443) 启用控制台重定向

```
racadm>>set iDRAC.VirtualConsole.WebRedirect Enabled
```

要关闭外部虚拟控制台端口 (5900)，请设置以下 iDRAC 属性。

要关闭外部虚拟控制台端口 (5900)，必须同时启用 `iDRAC.VirtualConsole.WebRedirect` 和 `iDRAC.VirtualConsole.CloseUnusedPort`。

```
racadm>>set iDRAC.VirtualConsole.CloseUnusedPort Enabled
```

注:

- 如果禁用了虚拟介质端口，则不能访问独立的虚拟介质，您可以通过虚拟控制台使用虚拟介质。
- 启用“CloseUnusedPort”时，基于 Java 和 ActiveX 的虚拟控制台和虚拟介质将无法运行，因为它们需要专用的外部端口。使用 HTML5 插件程序的虚拟控制台和虚拟介质将在 iDRAC Web 服务器端口 (443) 上运行。

虚拟介质

为什么虚拟介质客户端连接有时会断开?

出现网络超时后，iDRAC 固件会断开连接，将断开服务器和虚拟驱动器间的连接。

如果在客户端系统中更改 CD，新的 CD 将具有自动运行功能。在这种情况下，如果客户端系统用较长时间读取 CD，固件可能超时，连接将会中断。如果连接断开，可以从 GUI 重新连接并继续之前的操作。

如果在 iDRAC Web 界面中或通过本地 RACADM 命令更改“虚拟介质”配置设置，在应用此配置更改后，任何已连接的介质会断开连接。

要重新连接虚拟驱动器，请使用虚拟介质**客户端视图**窗口。

为什么通过虚拟介质安装 Windows 操作系统要花费更长的时间?

如果使用 *Dell Systems Management Tools and Documentation DVD* 安装 Windows 操作系统，并且网络连接较慢，由于网络延迟，安装过程可能需要更长的时间才能访问 iDRAC Web 界面。安装窗口不会指示安装进度。

如何将虚拟设备配置为可引导设备?

在受管系统，访问 BIOS 设置并转至引导菜单。找到虚拟 CD、虚拟软盘或 vFlash 并根据需要更改设备引导顺序。此外，还可以在 CMOS 设置的引导顺序中按“空格”键，将虚拟设备设置为可引导。例如，要从 CD 驱动器引导，需要将 CD 驱动器配置为引导顺序中的第一个设备。

哪些介质类型可以设置为可引导设备?

iDRAC 允许您从以下可引导介质引导：

- CDROM/DVD 数据介质
- ISO 9660 映像
- 1.44 软盘或软盘映像
- 被操作系统认作可移动磁盘的 USB 闪存盘
- USB 闪存盘映像

如何将 USB 闪存盘设为可引导设备?

您可以通过 Windows 98 启动盘引导，并将系统文件从启动盘复制到 USB 闪存盘。例如，在 DOS 提示符下，输入下列命令：

```
sys a: x: /s
```

其中，x: 是需要设置为可引导设备的 USB 闪存盘。

虚拟介质已经附加并连接到远程软盘。但是无法在运行 Red Hat Enterprise Linux 或 SUSE Linux 操作系统的系统上找到虚拟软盘/虚拟 CD 设备。如何解决此问题?

某些 Linux 版本不会使用相同的方法自动加载虚拟软盘驱动器和虚拟 CD 驱动器。要加载虚拟软盘驱动器，需要找到 Linux 分配到虚拟软盘驱动器的设备节点。要加载虚拟软盘驱动器：

1. 打开 Linux 命令提示符并运行以下命令：

   ```
   grep "Virtual Floppy" /var/log/messages
   ```

2. 找到该信息的最新条目并记下时间。
3. 在 Linux 提示符处运行以下命令：

   ```
   grep "hh:mm:ss" /var/log/messages
   ```

   hh:mm:ss 是 grep 在步骤 1 返回信息的时间戳。
4. 在步骤 3 中，查看 grep 命令的结果并找到赋予虚拟软盘的设备名。
5. 确保已附加并连接到虚拟软盘驱动器。
6. 在 Linux 提示符处运行以下命令：

   ```
   mount /dev/sdx /mnt/floppy
   ```

   其中，`/dev/sdx` 是步骤 4 中发现的设备名，`/mnt/floppy` 是加载点。

要加载虚拟 CD 驱动器，需要找到 Linux 分配到虚拟 CD 驱动器的设备节点。要加载虚拟 CD 驱动器：

1. 打开 Linux 命令提示符并运行以下命令：

   ```
   grep "Virtual CD" /var/log/messages
   ```

2. 找到该信息的最新条目并记下时间。
3. 在 Linux 提示符处运行以下命令：

   ```
   grep "hh:mm:ss" /var/log/messages
   ```

   hh:mm:ss 是 grep 在步骤 1 返回信息的时间戳。
4. 在步骤 3 中，查看 grep 命令的结果并找到赋予 *Dell 虚拟* CD 的设备名。
5. 确保已经附加并连接虚拟 CD 驱动器。
6. 在 Linux 提示符处运行以下命令：

   ```
   mount /dev/sdx /mnt/CD
   ```

   其中，`/dev/sdx` 是步骤 4 中发现的设备名，`/mnt/floppy` 是加载点。

为什么在使用 iDRAC Web 界面执行远程固件更新之后，连接到服务器的虚拟驱动器会被删除?

固件更新会导致 iDRAC 重设，断开远程连接并卸载虚拟驱动器。iDRAC 完成重设后，驱动器将会重新出现。

为什么连接 USB 设备之后，所有的 USB 设备都断开连接?

虚拟介质设备和 vFlash 设备作为复合 USB 设备连接到主机 USB 总线，它们共享同一个通用 USB 端口。每当任何虚拟介质或 vFlash USB 设备连接到主机 USB 总线或断开连接，所有虚拟介质和 vFlash 设备都将从主机 USB 总线暂时断开连接，然后它们将重新连接。如果主机操作系统使用虚拟介质设备，请不要连接或分离一个或多个虚拟介质或 vFlash 设备。建议先连接所有所需的 USB 设备，然后再予以使用。

USB 重设按钮有什么作用?

它可重设连接到服务器的远程 USB 设备和本地 USB 设备。

如何实现虚拟介质的最佳性能?

要实现虚拟介质的最佳性能，请启动禁用了虚拟控制台的虚拟介质，或执行下列任一操作：

- 将性能滑块调至最大速度。
- 禁用虚拟介质和虚拟控制台的加密。

  注: 在此情况下，受管服务器和虚拟介质及虚拟控制台的 iDRAC 之间的数据传输不受保护。
- 如果使用任何 Windows 服务器操作系统，请停止 Windows 服务 Windows Event Collector。要执行此操作，请转至**开始** > **管理工具** > **服务**。右键单击 **Windows Event Collector**，然后单击**停止**。

在查看软盘驱动器或 USB 闪存盘的内容时，通过虚拟介质连接同一个驱动器，为什么会出现连接失败的消息?

不允许同时访问虚拟软盘驱动器。在尝试虚拟化驱动器之前，请关闭用于查看驱动器内容的应用程序。

虚拟软盘驱动器上支持何种文件系统类型?

虚拟软盘驱动器支持 FAT16 或 FAT32 文件系统。

为什么在通过虚拟介质连接 DVD/USB 时，即使虚拟介质当前未使用，仍然显示错误消息?

如果远程文件共享功能 (RFS) 正在使用，将会显示错误消息。每次仅允许使用 RFS 或虚拟介质二者的其中一个，不能同时使用。

即使 iDRAC 将虚拟介质*连接状态*显示为*已连接*，虚拟介质也无法访问。

当 iDRAC 中**链接模式**设置为**断开**时，如果您尝试使用 ActiveX 或 Java 插件访问虚拟介质，则连接状态可能显示为**已连接**。将**连接模式**更改为**自动连接**或**连接**以访问虚拟介质。

vFlash SD 卡

vFlash SD 卡何时锁定?

操作正在进行中时 vFlash SD 卡已锁定。例如，在初始化操作过程中。

SNMP 验证

为什么显示信息“Remote Access: SNMP Authentication Failure”（远程访问：SNMP 验证失败）?

在查找过程中，IT Assistant 会尝试验证设备的 get 和 set 团体名称。在 IT Assistant 中，get 团体名称 = public，而 set 团体名称 = private。默认情况下，用于 iDRAC 代理程序的 SNMP 代理程序团体名称是 public。当 IT Assistant 发出 set 请求时，iDRAC 代理程序会生成 SNMP 验证错误，因为它仅接受来自团体 = public 的请求。

要防止生成 SNMP 验证错误，您必须输入代理程序接受的团体名称。由于 iDRAC 只允许一个团体名称，您必须将相同的 get 和 set 团体名称用于 IT Assistant 查找设置。

存储设备

所有连接到系统的存储设备的信息未显示，并且 OpenManage Storage Management 显示的存储设备比 iDRAC 多。为什么?

iDRAC 仅显示综合嵌入式管理 (CEM) 所支持的设备的信息。

对于 HBA 后面的外部 JBOD/Insight，将使用 EEMI 消息 ID ENC42 生成 SAS 连接器/IOM 删除的 EEMI 消息，但不会生成 SAS 连接器/IOM 恢复的 EEMI 消息 ENC41。

确认在 iDRAC Web 界面中恢复 IOM，请执行以下操作：

1. 转至**存储** > **概要** > **机柜**
2. 选择机柜。
3. 在**高级属性**下，确保**冗余路径**的值设置为**存在**，然后确认 IOM 还原。

GPU（加速器）

IDRAC GUI 中 CPU/加速器下的加速器部分灰显。

当 Redfish 中的相应属性被禁用时，GUI 中的少数页面可能不会显示预期响应。

iDRAC 服务模块

某些 PowerEdge 服务器的 iDRAC GUI 页面中的 iSM 详细信息缺失/未正确更新

当用户在分组下添加子 NIC 时，配置无效。这将导致 iSM 无法正确地与 iDRAC 通信。

在安装或运行 iDRAC Service Module 前，是否应卸载 OpenManage Server Administrator?

否，您不需要卸载 Server Administrator。在安装或运行 iDRAC Service Module 之前，请确保已停止 iDRAC Service Module 提供的 Server Administrator 功能。

如何检查主机操作系统中是否已安装 iDRAC Service Module?

要确定系统中是否已安装 iDRAC Service Module，

- 在运行 Windows 的系统上：

  打开**控制面板**，验证 iDRAC Service Module 是否列于已安装程序的列表中。

- 在运行 Linux 的系统上：

  运行命令 `rpm –qi dcism`。如果已安装 iDRAC Service Module，显示的状态将是**已安装**。

- 在运行 ESXi 的系统上，在主机上运行命令 `esxcli software vib list|grep -i open`。此时将显示 iDRAC Service Module。

注: 要检查 Red Hat Enterprise Linux 7 上是否安装了 iDRAC Service Module，请使用 `systemctl status dcismeng.service` 命令，而非 `init.d` 命令。

如何检查系统中安装的 iDRAC Service Module 的版本号?

要检查系统中的 iDRAC Service Module 的版本，请执行以下任一操作：

- 依次单击**开始** > **控制面板** > **程序和功能**。已安装 iDRAC Service Module 的版本将列在**版本**选项卡中。
- 转至**我的电脑** > **卸载或更改程序**。

安装 iDRAC 服务模块所需的最低权限级别是什么?

要安装 iDRAC Service Module，您必须具有管理员级别的权限。

在 iDRAC Service Module 2.0 版及更早版本中，在安装 iDRAC Service Module 时，将显示错误消息，指出此服务器不受支持。有关受支持的服务器的更多信息，请参阅《用户指南》。如何解决此错误?

安装 iDRAC Service Module 之前，请确保服务器是第 12 代 PowerEdge 服务器或更高版本。此外，确保您使用的是 64 位系统。

在操作系统日志中将显示以下消息，即使已正确配置“基于 USBNIC 的 OS 到 iDRAC 直通”功能也是如此。为什么?

The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel

iDRAC Service Module 使用基于 USB NIC 功能的 OS 到 iDRAC 直通，建立与 iDRAC 的通信。有时，尽管 USB NIC 接口配置了正确的 IP 端点，但通信仍未建立。当主机操作系统路由表具有同一个目标掩码的多个条目以及 USB NIC 目标未列为路由顺序的第一个目标时，可能会出现这种情况。

表. 64: 布线顺序示例

目标	网关	网络掩码	标志	度量指标	参考	使用接口
默认值	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

在示例中，**enp0s20u12u3** 是 USB NIC 接口。链路-本地目标掩码是重复的，并且 USB NIC 在顺序中不是第一个。这导致 iDRAC Service Module 通过操作系统到 iDRAC 的直通与 iDRAC 的连接出现问题。要诊断连接问题，请确保可从主机操作系统访问 iDRAC USBNIC IPv4 地址（默认地址是 169.254.1.1）。

否则，请执行以下操作：

- 在唯一的目标掩码上更改 iDRAC USB NIC 地址。
- 从路由表中删除不需要的条目，以确保在主机要访问 iDRAC USB NIC IPv4 地址时，路由将选中 USB NIC。

在 iDRAC Service Module 2.0 和更早的版本上，在 VMware ESXi 服务器中卸载 iDRAC Service Module 时，虚拟交换机被命名为 vSwitchiDRACvusb，端口组在 vSphere 客户端上被命名为 iDRAC Network。如何将其删除?

在 VMware ESXi 服务器上安装 iDRAC Service Module VIB 时，iDRAC Service Module 将创建 vSwtich 和 PortGroup，以便在 USB NIC 模式下基于 OS 到 iDRAC 直通与 iDRAC 进行通信。卸载后，虚拟交换机 **vSwitchiDRACvusb** 和端口组 **iDRAC 网络** 不会被删除。要手动删除，请执行以下步骤之一：

- 转至 vSphere 客户端配置向导，然后删除条目。
- 转至 Esxcli 并键入以下命令：
  - 要删除端口组：`esxcfg-vmknic -d -p "iDRAC Network"`
  - 要删除 vSwitch：`esxcfg-vswitch -d vSwitchiDRACvusb`

  注: 您可以在 VMware ESXi 服务器上重新安装 iDRAC Service Module，因为这不会对服务器造成功能问题。

复制的 LifeCycle 日志位于操作系统中的什么位置?

要查看复制 LifeCycle 日志：

表. 65: 生命周期日志位置

操作系统	位置
Microsoft Windows	**事件查看器** > **Windows 日志** > **系统**.所有 iDRAC Service Module 生命周期日志都将复制到源名称 **iDRAC Service Module** 下。 **注:** 在 iSM 2.1 和更高版本中，生命周期日志将复制到 Lifecycle Controller 日志源名称下。在 iSM 2.0 和更低版本中，日志将复制到 iDRAC Service Module 源名称下。 **注:** 生命周期日志的位置可以使用 iDRAC Service Module 安装程序进行配置。您在安装 iDRAC Service Module 或修改安装程序时，可配置此位置。
Red Hat Enterprise Linux、SUSE Linux、CentOS 和 Citrix XenServer	`/var/log/messages`
VMware ESXi	`/var/log/syslog.log`

在完成 Linux 安装时可安装哪些 Linux 从属软件包或可执行文件?

要查看 Linux 从属软件包的列表，请参阅 *iDRAC Service Module 用户指南*，网址：https://www.dell.com/idracmanuals 中的 *Linux 相关性*一节。

如何提高某些配置的 GPU 性能?

BIOS 系统性能配置文件设置为性能

在“处理器”设置下，将 NPS 设置为 4，并将 CCX 设置为 auto

每个通道最小 1 DIMM

IOmmu = Linux OS 上的直通

RACADM

执行 iDRAC 重设（通过使用 racadm racreset 命令）后，如果发出任何命令，会显示以下消息。这表示什么意思?

```
ERROR: Unable to connect to RAC at specified IP address
```

此消息指出您必须等到 iDRAC 完成重设后，才能发出另一个命令。

使用 RACADM 命令和子命令时，某些错误不明确。

使用 RACADM 命令时，可能会遇到以下一个或多个错误：
- 本地 RACADM 错误信息 — 如语法、印刷错误和名称错误等问题。
- 远程 RACADM 错误信息 — 如 IP 地址错误、用户名错误或密码错误等问题。

对 iDRAC 进行 Ping 测试期间，如果在专用模式和共享模式之间切换网络模式，则没有 Ping 响应。

清除系统上的 ARP 表。

远程 RACADM 无法从 SUSE Linux Enterprise Server (SLES) 11 SP1 连接到 iDRAC。

请确保已安装官方的 openssl 和 libopenssl 版本。运行以下命令以安装 RPM 软件包：

```
rpm -ivh --force < filename >
```

其中，`filename` 是 openssl 或 libopenssl rpm 软件包文件。

例如：

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

为什么在属性更改后，远程 RACADM 和基于 Web 的服务会变得不可用?

重设 iDRAC Web 服务器后，可能需要等待几分钟，远程 RACADM 服务和基于 Web 的界面才会变为可用。

在以下情况下会重设 iDRAC Web 服务器：
- 使用 iDRAC Web 用户界面更改网络配置或网络安全性属性时。
- iDRAC.Webserver.HttpsPort 属性已更改，包括 `racadm set -f <config file>` 对其进行的更改。
- 使用 `racresetcfg` 命令。
- iDRAC 已重设时。
- 上载了新的 SSL 服务器证书。

使用本地 RACADM 创建它后，如果您试图删除分区，为何显示错误消息?

这是因为创建分区操作正在进行中。不过，分区在一段时间后会被删除，并且将显示分区被删除的消息。如果没有显示消息，请等待创建分区操作完成后再删除该分区。

永久设置默认密码至 calvin

如果您的系统随附唯一的 iDRAC 默认密码，但您想要将 *calvin* 设置为默认密码，您必须使用系统板上的可用跳线。

小心: 更改跳线设置将永久更改默认密码为 *calvin*。即便将 iDRAC 重设为出厂设置，您仍无法恢复到唯一密码。

有关跳线位置和步骤的信息，请参阅您的服务器说明文件，网址为：https://www.dell.com/support。

其他

升级到最新版本时升级失败。

注: 3.30.30.30 是升级到更高版本的 4.00.00.00/4.10.10.10 所需的最低 iDRAC 版本。

重设 iDRAC 后，iDRAC GUI 可能不会显示所有值。

注: 如果出于某些原因重设了 iDRAC，请确保在重设 iDRAC 之后至少等待两分钟，以访问或修改 iDRAC 中的任何设置。

已安装操作系统时，主机名可能会自动显示/更改。

有两种情况：
- 情况 1：安装操作系统时 iDRAC 未显示最新主机名。您需要与 iDRAC 一起安装 OMSA 或 iSM 以反映主机名。

- 情况 2：iDRAC 具有特定操作系统的主机名并且已安装另一个不同的操作系统，同时主机名仍然显示为旧主机名而不覆盖主机名。其原因是主机名是来自操作系统的信息，iDRAC 仅保存信息。如果已安装新的操作系统，iDRAC 将无法重设主机名的值。但是，较新版本的操作系统能够在第一次操作系统启动期间更新 iDRAC 中的主机名。

如何查找刀片式服务器的 iDRAC IP 地址?

注: Chassis Management Controller (CMC) 选项仅适用于刀片服务器。

- **使用 CMC Web 界面**：

  转至 **机箱** > **服务器** > **设置** > **部署**.在显示的表格中，查看服务器的 IP 地址。

- **使用虚拟控制台**：重新引导服务器以在开机自检过程中查看 iDRAC IP 地址。在 OSCAR 界面中选择“Dell CMC”控制台，以通过本地串行连接登录到 CMC。CMC RACADM 命令可以从该连接发送。

  有关 CMC RACADM 命令的更多信息，请参阅 机箱管理控制器 RACADM CLI 指南，*网址：*https://www.dell.com/cmcmanuals。

  有关 iDRAC RACADM 命令的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

- **使用本地 RACADM**

  使用以下命令：`racadm getsysinfo`，例如：

```
$ racadm getniccfg -m server-1
DHCP Enabled = 1
IP Address    = 192.168.0.1
Subnet Mask   = 255.255.255.0
Gateway       = 192.168.0.1
```

- **使用 LCD**：

  在主菜单上，高亮显示服务器并按检查按钮，然后选择所需的服务器并按下检查按钮。

如何查找刀片式服务器的 iDRAC IP 地址?

注: OME-Modular Web 界面选项仅适用于 MX 平台。

- **使用 OME-Modular Web 界面**：

  转至 **设备** > **计算**.选择计算机底座，iDRAC IP 将显示为**管理 IP**。

- **使用 OMM 应用程序**，请参阅 *Dell EMC OpenManage Mobile 用户指南，网址：*https://www.dell.com/openmanagemanuals
- **使用串行连接**
- **使用 LCD**：在主菜单上，高亮显示服务器并按检查按钮，然后选择所需的服务器并按下检查按钮。

如何查找与刀片式服务器相关的 CMC IP 地址?

注: 不适用于 MX 平台。

- **从 iDRAC Web 界面**：

  转至 **iDRAC 设置** > **CMC**.此时 **CMC 摘要**页面将显示 CMC IP 地址。

- **从虚拟控制台**：

  在 OSCAR 界面中选择“Dell CMC”控制台，以通过本地串行连接登录到 CMC。CMC RACADM 命令可以从该连接发出。

```
$ racadm getniccfg -m chassis
NIC Enabled         = 1
DHCP Enabled        = 1
Static IP Address   = 192.168.0.120
Static Subnet Mask  = 255.255.255.0
Static Gateway      = 192.168.0.1
Current IP Address  = 10.35.155.151
```

```
Current Subnet Mask = 255.255.255.0
Current Gateway     = 10.35.155.1
Speed               = Autonegotiate
Duplex              = Autonegotiate
```

注: 也可使用远程 RACADM 执行此操作。

有关 CMC RACADM 命令的更多信息，请参阅 机箱管理控制器 RACADM CLI 指南，*网址：*https://www.dell.com/cmcmanuals。

有关 iDRAC RACADM 命令的更多信息，请参阅 *iDRAC RACADM CLI 指南*，网址：https://www.dell.com/idracmanuals。

如何查找 OME Modular IP 地址?

注: 仅适用于 MX 平台。

- **从 iDRAC Web 界面**:

  转至 **iDRAC 设置** > **管理模块**.**管理模块**页面将显示 OME Modular IP 地址。

如何查找机架式服务器和塔式服务器的 iDRAC IP 地址?

- **从本地 RACADM**:

  使用命令 `racadm getsysinfo`。

- **从 LCD**:

  在物理服务器上，使用 LCD 面板导航按钮查看 iDRAC IP 地址。转至**设置视图** > **视图** > **iDRAC IP** > **IPv4** 或 **IPv6** > **IP**。

- **从 OpenManage 服务器管理员**:

  在 Server Administrator Web 界面中，转至 **模块化机柜** > **系统/服务器模块** > **主系统机箱/主系统** > **远程访问**.

iDRAC 网络连接不工作。

对于刀片式服务器:

- 确保 LAN 电缆已连接到 CMC。 (不适用于 MX 平台)
- 确保已为网络启用 NIC 设置、IPv4 或 IPv6 设置，以及静态或 DHCP。

对于机架式和塔式服务器:

- 在共享模式中，确保 LAN 电缆已连接到 NIC 端口，此端口中有扳手标志。
- 在专用模式中，确保 LAN 电缆已连接到 iDRAC LAN 端口。
- 确保已为网络启用 NIC 设置、IPv4 和 IPv6 设置，以及静态或 DHCP。

iDRAC 在共享 LOM 中无法访问

如果主机操作系统中存在严重错误（例如 Windows 中的蓝屏死机错误），iDRAC 可能无法访问。要访问 iDRAC，请重新启动主机以恢复连接。

启用链路聚合控制协议 (LACP) 后，共享 LOM 无法正常工作。

必须在启用 LACP 之前加载网络适配器的主机操作系统驱动程序。但是，如果正在使用被动 LACP 配置，在加载主机操作系统驱动程序之前，共享 LOB 可能正常工作。有关 LACP 配置，请参阅交换机文档。

注: 如果交换机配置了 LACP，将无法在预引导状态访问 iDRAC 的共享 LOM IP。

已将刀片式服务器插入机箱，并按下电源开关，但是这并不会通电。

- 服务器通电前，iDRAC 最多需要两分钟进行初始化。
- 检查 CMC 和 OME Modular（仅适用于 MX 平台）电源预算。机箱电源预算可能超支。

如何检索 iDRAC 管理用户名和密码？

您必须将 iDRAC 恢复为默认设置。有关更多信息，请参阅将 iDRAC 重设为出厂默认设置 页面上的 314。

如何更改机箱中系统的插槽名称？

注: 不适用于 MX 平台。

1. 登录 CMC Web 界面并转至 **机箱** > **服务器** > **设置**.
2. 在服务器的行中输入插槽的新名称并单击**应用**。

刀片服务器上的 iDRAC 在引导期间未响应。

卸下并重新插入服务器。

检查 CMC（不适用于 MX 平台）和 OME Modular（适用于 MX 平台）Web 界面以查看 iDRAC 是否显示为可升级组件。如果是，请按照使用 CMC Web 界面更新固件 页面上的 77 中的说明更新固件。

注: 更新功能不适用于 MX 平台。

如果问题依然存在，请联系技术支持。

尝试引导受管服务器时，电源指示灯为绿色，但是根本没有开机自检或视频。

出现这种现象是因为出现以下情况：

- 内存未安装或不可访问。
- CPU 内存未安装或不可访问。
- 视频转接卡丢失或未正确连接。

同时，使用 iDRAC Web 界面或从服务器 LCD 阅读 iDRAC 日志中的错误消息。

在 Linux 或 Ubuntu 上无法使用 Firefox 浏览器登录到 iDRAC Web 界面。无法输入密码。

要解决此问题，请重新安装或升级 Firefox 浏览器。

在 SLES 和 Ubuntu 中无法通过 USB 网卡访问 iDRAC

注: 在 SLES 中，将 iDRAC 接口设置为 DHCP。

在 Ubuntu 中，使用 Netplan 公用程序将 iDRAC 接口配置为 DHCP 模式。要配置 DHCP，请执行以下操作：

1. 使用 `/etc/netplan/01-netcfg.yaml`。
2. 对于 iDRAC DHCP，指定“是”。
3. 应用配置。

图 5: 在 Ubuntu 中将 iDRAC 界面配置为 DHCP 模式

未在 Redfish 中列出嵌入式网络适配器的型号、制造商和其他属性

嵌入式设备的 FRU 详细信息将不会显示。嵌入在主板上的设备将不会有任何 FRU 对象。因此，依赖属性将不会出现。

30

使用案例场景

本节帮助您导航至本指南中特定的章节来执行特定用户的案例场景。

主□：

- 排除受管系□不可□□的故障
- □取系□信息和□□系□运行状况
- □置警□和配置□子□件警□
- □看并□出系□事件日志和生命周期日志
- 用于更新 iDRAC 固件的界面
- □行正常关机
- □建新的管理□用□□□
- 启□服□器□程控制台和挂□ USB □□器
- 使用□接的虚□介□和□程文件共享安装裸机操作系□
- 管理机架密度
- 安装新的□子□可□
- 在一次主机系□重新引□中□多个网卡□用 I/O □□配置□置

排除受管系统不可访问的故障

收到来自 OpenManage Essentials 的警报后，Dell 管理控制台或本地陷阱收集器、数据服务中心中的 5 个服务器均无法访问，出现类似操作系统或服务器挂起的问题。需要使用 iDRAC 查明原因以进行故障排除并使服务器恢复。

排除不可访问的系统故障前，请确保满足以下先决条件：

- 启用上次崩溃屏幕
- 已在 iDRAC 上启用警报

要查明原因，请检查 iDRAC Web 界面中的以下内容，并重新连接到系统：

注： 如果您不能□□ iDRAC Web 界面，□□至服□器，□□ LCD 面板，并□下 IP 地址或主机名，然后使用管理站中的 iDRAC Web 界面□行以下操作：

- 服务器的 LED 状态 — 闪烁的琥珀色或稳定琥珀色。
- 前面板 LCD 状态或错误消息 — 琥珀色 LCD 或错误消息。
- 操作系统映像可在虚拟控制台查看。如果可以看到映像，请重置系统（热引导）并再次登录。如果您可以登录，则该问题已得到修复。
- 上次崩溃屏幕。
- 启动捕获视频。
- 崩溃捕获视频。
- 服务器运行状况 — 红色 *x* 图标表示系统组件有问题。
- 存储阵列状态 — 阵列可能离线或无效
- 与系统硬件和固件相关的重要事件 Lifecycle 日志及系统崩溃时记录的日志条目。
- 生成技术支持报告并查看所收集的数据。
- 使用 iDRAC 服务模块所提供的监测功能

获取系统信息和访问系统运行状况

要获取系统信息和访问系统运行状况：

- 在 iDRAC Web 界面中，转至 **Overview（概览）** > **Summary（摘要）**以查看系统性信息并访问此页面上的各个链接以访问系统运行状况。例如，您可以查看机箱风扇的运行状况。
- 您还可以配置机箱探测器 LED，根据颜色确定系统的运行状况。

- 如果已安装 iDRAC 服务模块，将显示操作系统主机信息。

设置警报和配置电子邮件警报

要设置警报和配置电子邮件警报，请执行以下操作：

1. 启用警报。
2. 配置电子邮件警报并检查端口。
3. 对受管系统执行重新引导、关机或关机后再开机操作。
4. 发送测试警报。

查看并导出系统事件日志和生命周期日志

查看并导出 Lifecycle 日志和系统事件日志 (SEL)：

1. 在 iDRAC Web 界面中，转至 **Maintenance（维护）** > **System Event Logs（系统事件日志）**以查看 SEL，转至 **Lifecycle Log（生命周期日志）**以查看生命周期日志。

   注: SEL 也会记录在生命周期日志中。使用筛选选项可查看 SEL。

2. SEL 或生命周期日志通过 XML 格式导出到外部位置（管理站、USB、网络共享等）。或者，您可以启用远程系统记录，以便写入到生命周期日志的所有日志也同时写入到已配置的远程服务器。
3. 如果您正在使用 iDRAC Service Module，则将生命周期日志导出到操作系统日志。

用于更新 iDRAC 固件的界面

使用以下界面更新 iDRAC 固件：

- iDRAC Web 界面
- Redfish API
- RACADM CLI (iDRAC_) 和 CMC（不适用于 MX 平台）
- Dell 更新软件包 (DUP)
- CMC（不适用于 MX 平台）OME Modular（仅适用于 MX 平台） Web 界面
- Lifecycle Controller – 远程服务
- Lifecycle Controller
- Dell 远程访问配置工具 (DRACT)

执行正常关机

要执行正常关机，请在 iDRAC Web 界面中转至下列任一位置：

- 在 **Dashboard（仪表板）**中，选择 **Graceful Shutdown（正常关机）**，然后单击 **Apply（应用）**。

有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

创建新的管理员用户帐户

您可以修改默认的本地管理员用户帐户或创建新的管理员用户帐户。要修改本地管理员用户帐户，请参阅修改本地管理员帐户设置。

要创建新的管理员帐户，请参阅下列部分：

- 配置本地用户
- 配置 Active Directory 用户
- 配置通用 LDAP 用户

启动服务器远程控制台和挂载 USB 驱动器

要启动远程控制台和加载 USB 驱动器：

1. 将 USB 闪存盘（具有所需映像）连接到 Management Station。
2. 要使用以下方法通过 iDRAC Web 界面启动虚拟控制台，请执行以下操作：
   - 转至 **Dashboard（仪表板）** > **Virtual Console（虚拟控制台）**，然后单击 **Launch Virtual Console（启动虚拟控制台）**。

   随即会显示 **Virtual Console Viewer（虚拟控制台查看器）**。
3. 从 **File（文件）**菜单中，单击 **Virtual Media（虚拟媒体）** > **Launch Virtual Media（启动虚拟媒体）**。
4. 单击 **Add Image（添加映像）**并选择位于 USB 闪存盘上的映像。
   该映像即会添加到可用驱动器的列表中。
5. 选择要映射该映像的驱动器。USB 闪存盘上的映像即会映射到受管系统。

使用连接的虚拟介质和远程文件共享安装裸机操作系统

请参阅"使用远程文件共享部署操作系统"部分。

管理机架密度

在机架安装附加服务器时，您必须确定机架中的剩余容量。

要估计机架容量以增加额外的服务器：

1. 查看服务器的当前能耗数据和历史能耗数据。
2. 根据这些数据、电源基础架构和散热系统的限制，决定功耗上限策略并设定功耗上限值。

   注: 推荐设置接近峰值的最大值，然后使用上限水平确定机架上剩余多少容量可以用于增加更多的服务器。

安装新的电子许可证

请参阅许可证操作了解更多信息。

在一次主机系统重新引导中为多个网卡应用 I/O 标识配置设置

如果位于存储区域网络 (SAN) 环境中的服务器中具有多个网卡，并且您要向这些卡应用不同的虚拟地址、发起程序和目标配置设置，可使用 I/O 标识优化功能缩短配置过程的时间。要执行此操作：

1. 请确保 BIOS、iDRAC 和网卡已更新为最新固件版本。
2. 启用 IO 标识优化功能。
3. 从 iDRAC 配置文件 (SCP) 文件导出服务器配置文件。
4. 在 SCP 文件中编辑 I/O 标识优化设置。
5. 将 SCP 文件导入 iDRAC。