Integrated Dell Remote Access Controller 8 (iDRAC8) 和 iDRAC7 v2.20.20.20 用户指南

注、小心和警告

注: “注”表示可以帮助您更好地使用计算机的重要信息。

小心: “小心”表示可能会损坏硬件或导致数据丢失，并说明如何避免此类问题。

警告: “警告”表示可能会造成财产损失、人身伤害甚至死亡。

2015 - 09

Rev. A00

目录

1 概览

Integrated Dell Remote Access Controller (iDRAC) 设计用于使服务器管理员提高工作效率和改善 Dell 服务器的整体可用性。iDRAC 提醒管理员服务器存在的问题，可以帮助他们执行远程服务器管理，并减少了实际访问服务器的需要。

使用 Lifecycle Controller 技术的 iDRAC 是大型数据中心解决方案的组成部分，有助于保持业务关键型应用程序和工作负荷始终可用。该技术允许管理员从任何位置部署、监测、管理、配置、更新、故障排除和修复 Dell 服务器，而无需使用代理。无论操作系统或管理程序是否存在或状态为何，它都能实现这些功能。

多个产品可与 iDRAC 和 Lifecycle Controller 协作，以简化 IT 操作，例如：

- Dell Management plug-in for VMware vCenter
- Dell Repository Manager
- Dell Management Packs for Microsoft System Center Operations Manager (SCOM) 和 Microsoft System Center Configuration Manager (SCCM)
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

iDRAC 有以下型号：

- 带 IPMI 的 Basic Management（默认在 200-500 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）

有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *iDRAC Overview and Feature Guide*（iDRAC 概览和功能指南）。

iDRAC 配合 Lifecycle Controller 一起使用的优点

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（WS 管理）界面进行远程部署，并与 Dell OpenManage Essentials 及合作伙伴控制台集成。

有关 Lifecycle Controller GUI 的更多信息，请参阅 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）；有关远程服务的信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller Remote Services 用户指南）。

主要功能特色

iDRAC 中的主要功能包括：

注: 某些功能仅限 iDRAC Enterprise 许可证提供。有关许可证可用功能的信息，请参阅管理许可证。

资源清册和监测

- 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 Chassis Management Controller (CMC) Web 界面，查看 CMC 信息和 WWN/MAC 地址。

  注: CMC 通过 M1000E 机箱 LCD 面板和本地控制台连接提供访问 iDRAC 的权限。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Chassis Management Controller User's Guide*（Chassis Management Controller 用户指南）。
- 查看主机操作系统上可用的网络接口。
- 使用 iDRAC 快速同步功能和移动设备查看资源清册和监测信息并配置基本 iDRAC 设置。

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、虚拟介质和 VMCLI 部署操作系统。
- 启用自动查找。
- 通过 RACADM 和 WS-MAN 使用导出或导入 XML 配置文件功能执行服务器配置。有关更多信息，请参阅 *Lifecycle Controller Remote Services Quick Start Guide*（Lifecycle Controller Remote Services 快速入门指南）。
- 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。
- 备份和还原服务器配置文件。
- 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、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。
– 填充 Windows Management Instrumentation (WMI) 信息。
– 与技术支持报告集成。仅在已安装 iDRAC Service Module 2.0 或更高版本时才适用。有关更多信息，请参阅生成技术支持报告。
– 准备移除 NVMe PCIe SSD。有关更多信息，请参阅准备移除 PCIe SSD。

- 通过以下方式生成技术支持报告：
  – 自动 — 使用自动调用 OS Collector 工具的 iDRAC 服务模块。
  – 手动 - 使用 OS Collector 工具。

保护连接性

保护对关键网络资源的访问权限非常重要。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的双重身份验证。双重身份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。
- 对在 iDRAC 中本地存储的用户帐户执行 SNMPv3 验证。建议使用此功能，但默认情况下此功能处于禁用状态。
- 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。
- SMCLP 和 Web 界面支持 128 位和 40 位加密（针对某些不支持 128 位加密的国家/地区），并使用 SSL 3.0 标准。
- 会话超时配置（以秒为单位）
- 可配置的 IP 端口（针对 HTTP、HTTPS、SSH、Telnet、虚拟控制台和虚拟介质）。

  注: Telnet 不支持 SSL 加密，并且在默认情况下处于禁用状态。

- 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）。

此发行版中的新功能

- 支持对 Half-Height Half-Length (HHHL) PCIe SSD 卡进行监测和资源清册。
- 支持更新 SAS 硬盘驱动器和固态驱动器 (SSD) 上的固件。
- 在应用服务器配置文件时支持 **NoReboot** 选项。
- 增加了对 `System.ThermalSettings.ThirdPartyPCIFanResponse` 属性的支持，当系统中插入了第三方 PCI 卡时，通过该属性可启用或禁用自动风扇速度功能。

如何使用本用户指南

本用户指南中的内容指导您使用以下工具执行任务：

- 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，请参阅位于 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。
- 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**）。

支持的 Web 浏览器

以下浏览器支持 iDRAC：

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

有关版本的列表，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 Release Notes*（iDRAC8 发行说明）。

管理许可证

iDRAC 的功能根据购买的许可证（Basic Management、iDRAC Express 或 iDRAC Enterprise）提供。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。例如，iDRAC Web 界面、RACADM、WS-MAN、OpenManage Server Administrator 等。某些功能（如专用 NIC 或 vFlash）需要 iDRAC 端口卡。在 200-500 系列服务器上该卡是可选的。

iDRAC 许可证管理和固件更新功能可通过 iDRAC Web 界面和 RACADM 提供。

许可证类型

提供的许可证类型包括：

- 30 天评估和扩展 - 许可证在 30 天后到期并且可延长 30 天。评估许可证基于持续时间，计时器在为系统通电时开始计时。
- 永久 - 许可证绑定到服务标签，而且是永久性的。

获取许可证的方法

使用以下任何方法都可获取许可证：

- 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。
- 自助服务门户 - 指向自助服务门户的链接可从 iDRAC 获得。单击此链接可在 Internet 上打开许可自助服务门户。当前，您可以使用许可证自助服务门户检索随服务器购买的许可证。您必须联系销售代表或技术支持来购买新许可证或升级许可证。有关更多信息，请参阅自助服务门户页面的联机帮助。

- 销售点 - 订购系统时即可获得许可证。

许可证操作

在执行许可证管理任务之前，请确保获得许可证。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Overview and Feature Guide*（概述和功能指南）。

注: 如果您购买的系统已预先安装所有许可证，请无需进行许可证管理。

对于一对一许可证管理，您可以使用 iDRAC、RACADM、WS-MAN 和 Lifecycle Controller 远程服务执行下列许可证操作，对于一对多许可证管理，您可以使用 Dell License Manager 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: 对于新功能，需要重新启动系统才能启用功能。
- 导出 - 将安装的许可证导出至外部存储设备进行备份，或者在更换部件或主板后重新安装许可证。导出许可证的文件名和格式为 **<EntitlementID>.xml**。
- 删除 - 如果组件丢失，则会删除分配给该组件的许可证。删除许可证之后，它不会存储在 iDRAC 中，并且基本产品功能将会启用。
- 更换 - 将许可证更换为扩展评估许可证，更改许可证类型（如使用购买的许可证更改评估许可证），或者扩展过期的许可证。
  - 您可以使用升级的评估许可证或购买的许可证更换评估许可证。
  - 您可以使用更新的许可证或升级的许可证更换购买的许可证。
- 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: 为了让 Learn More（了解详情）选项显示正确的页面，请确保在 Security Settings“安全设置”中已将 ***.dell.com** 添加到 Trusted Sites（受信任的站点）列表中。有关更多信息，请参阅“Internet Explorer 帮助”文档。

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.com/support/manuals** 上提供的 *Dell License Manager User's Guide*（Dell License Manager 用户指南）。

在更换主板后导入许可证

如果您最近更换了主板，需要在本地重新安装 iDRAC Enterprise 许可证（没有网络连接）并激活专用 NIC，可以使用本地 iDRAC Enterprise 许可证安装工具。此公用程序安装 30 天试用版 iDRAC Enterprise 许可证并允许您将 iDRAC 重设为从共享 NIC 更改为专用 NIC。

有关此公用程序和下载此工具的更多信息，请单击此处。

许可证组件的状态或条件以及可用操作

下表提供了基于许可证状态或条件的可用许可证操作列表。

表. 1: 基于状态或条件的许可证操作

许可证/组件状态或条件	导入	导出	删除	替换	了解更多
非管理员登录	否	否	否	否	是
活动许可证	是	是	是	是	是
过期许可证	否	是	是	是	是
许可证已安装但组件丢失	否	是	是	否	是

注: 在 iDRAC Web 界面中的**许可证**页面上，展开设备即可查看下拉菜单中的**替换**选项。

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**概览** → **服务器** → **许可证**。

许可证页面将会显示与设备相关联的许可证，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、删除或替换许可证的更多信息，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 **license** 子命令。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）。

在 iDRAC7 和 iDRAC8 中的已许可功能

下表列出了基于购买的许可证启用的 iDRAC7 和 iDRAC8 功能：

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
接口/标准								
IPMI 2.0	是	是	是	是	是	是	是	是
DCMI 1.5	否	是	否	是	否	是	否	是
基于 Web 的 GUI	否	是	是	是	是	是	是	是
Racadm 命令行（本地/远程）	否	是	是	是	是	是	是	是
SMASH-CLP（仅限 SSH）	否	是	是	是	是	是	是	是

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
Telnet	否	是	是	是	是	是	是	是
SSH	否	是	是	是	是	是	是	是
WS-MAN	是	是	是	是	是	是	是	是
网络时间协议	否	否	是	是	是	是	是	是
Connectivity（连接性）								
共享 NIC (LOM)	是	是	是	是	不适用	不适用	是	是
专用 NIC[2]	否	是	否	是	是	是	是	是 [1]
VLAN 标记	是	是	是	是	是	是	是	是
IPv4	是	是	是	是	是	是	是	是
IPv6	否	是	是	是	是	是	是	是
DHCP	否	是	否	是	否	是	否	是
动态 DNS	否	是	是	是	是	是	是	是
操作系统直通	否	是	否	是	否	是	否	是
前面板 USB	否	是	否	是	否	是	否	是
安全性								
基于角色的权限	是	是	是	是	是	是	是	是
本地用户	是	是	是	是	是	是	是	是
SSL 加密	是	是	是	是	是	是	是	是
IP 阻止	否	否	否	是	否	是	否	是
目录服务（AD、LDAP）	否	否	否	否	否	否	是	是
双重身份验证（智能卡）	否	否	否	否	否	否	是	是

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
单一登录 (Kerberos)	否	否	否	是	否	是	是	是
PK 身份验证（适用于 SSH）	否	否	否	是	否	是	否	是
远程存在								
电源控制	是 [4]	是	是	是	是	是	是	是
引导控制	否	是	否	是	否	是	否	是
LAN 上串行	是	是	是	是	是	是	是	是
虚拟介质	否	否	否	否	是	是	是	是
虚拟文件夹	否	否	否	否	否	否	是	是
远程文件共享	否	否	否	否	否	否	是	是
虚拟控制台	否	否	否	否	单个用户	单个用户	是	6 个用户
与操作系统的 VNC 连接	否	否	否	否	否	否	是	是
质量/带宽控制	否	否	否	否	否	是	否	是
虚拟控制台协作（最多六个并发用户）	否	否	否	否	否	否	否	是
虚拟控制台聊天	否	否	否	否	否	否	是	是
虚拟闪存分区	否	否	否	否	否	否	是	是 [1、2]
电源和散热								
断电后自动开机	否	是	否	是	否	是	否	是
实时功率计量器	是	是	是	是	是	是	是	是
功率阈值和警报（包括净空容量）	否	否	否	是	否	是	否	是

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
实时功率图表	否	否	是	是	是	是	是	是
历史功率计数器	是	否	是	是	是	是	是	是
功率限额	否	否	否	否	否	否	是	是
Power Center 集成	否	否	否	否	否	否	否	是
温度监测	否	是	否	是	否	是	否	是
温度图表	否	否	否	是	否	是	否	是
运行状况监测								
完整的免代理监测	否	是	否	是	否	是	否	是
预测性故障监测	否	是	否	是	否	是	否	是
SNMPv1、SNMP v2 和 v3（陷阱并获取）	否	是	是	是	是	是	是	是
电子邮件警报	否	否	是	是	是	是	是	是
可配置的阈值	否	是	否	是	否	是	否	是
风扇监测	否	是	否	是	否	是	否	是
电源设备监测	否	是	是	是	是	是	是	是
内存监测	否	是	否	是	否	是	否	是
CPU 监测	否	是	否	是	否	是	否	是
RAID 监测	否	是	否	是	否	是	否	是
NIC 监测	否	是	否	是	否	是	否	是
高清监测（机柜）	否	是	否	是	否	是	否	是
带外性能监测	否	否	否	否	否	否	否	是
更新								

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
远程免代理更新	是 [3]	是	是	是	是	是	是	是
嵌入式更新工具	否	是	否	是	否	是	否	是
与存储库同步（计划的更新）	否	否	否	否	否	否	是	是
自动更新	否	否	否	否	否	否	否	是
部署和配置								
嵌入式操作系统部署工具	否	是	否	是	否	是	否	是
嵌入式配置工具（iDRAC 设置公用程序）	否	是	否	是	否	是	否	是
嵌入式配置向导（Lifecycle Controller 向导）	否	是	否	是	否	是	否	是
自动查找	否	是	是	是	是	是	是	是
远程操作系统部署	否	否	否	是	否	是	否	是
嵌入式驱动程序包	否	是	否	是	否	是	否	是
完全配置的资源清册	否	是	否	是	否	是	否	是
资源清册导出	否	是	否	是	否	是	否	是
远程配置	否	是	是	是	是	是	是	是
全自动配置	否	否	否	否	否	否	否	是
系统淘汰/重新调整用途	否	是	否	是	否	是	否	是
诊断程序、服务和日志记录								
嵌入式诊断工具	是	是	是	是	是	是	是	是
部件更换	否	是	是	是	是	是	是	是

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
服务器配置备份	否	否	否	否	否	否	是	是
服务器配置还原	否	否	否	否	否	否	是	是
轻松还原（系统配置）	否	是	否	是	否	是	否	是
运行状况 LED / LCD	否	是	否	是	否	是	否	是
快速同步（需要 NFC 挡板）	否	是	否	是	否	不适用	否	是
iDRAC Direct（前置 USB 管理端口）	否	是	否	是	否	是	否	是
iDRAC Service Module (iSM)	否	是	是	是	是	是	是	是
嵌入式技术支持报告	否	是	是	是	是	是	是	是
崩溃屏幕捕获 [5]	否	否	是	是	是	是	是	是
崩溃视频捕获 [5]	否	否	否	否	否	否	是	是
引导捕获	否	否	否	否	否	否	是	是
手动重设 iDRAC	否	是	否	是	否	是	否	是
虚拟 NMI	否	是	否	是	否	是	否	是
操作系统监视程序	否	是	否	是	否	是	否	是
嵌入式运行状况报告	否	是	否	是	否	是	否	是
系统事件日志	否	是	是	是	是	是	是	是
Lifecycle 日志	否	是	否	是	否	是	否	是
工作注释	否	是	否	是	否	是	否	是
远程系统日志	否	否	否	否	否	否	是	是

功能	Basic Management (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	iDRAC8 Express for Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
许可证管理	否	是	否	是	否	是	否	是

[1] 500 系列和更低的机架式服务器和塔式服务器需要硬件卡才能启用此功能；此硬件将会产生额外的成本。

[2] 需要 vFlash SD 卡介质。

[3] 远程免代理更新功能仅使用 IPMI 提供。

[4] 仅使用 IPMI 提供。

[5] 目标服务器上需要 OMSA 代理。

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. 2: 访问 iDRAC 的界面和协议

界面或协议	说明
iDRAC 设置公用程序	使用 iDRAC 设置公用程序可以执行操作系统预操作。该公用程序中包含一个功能子集，可通过 iDRAC Web 界面与其他功能一起使用。 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**。
iDRAC Web 界面	使用 iDRAC Web 界面可管理 iDRAC 和监测受管系统。浏览器通过 HTTPS 端口连接到 Web 服务器。数据流使用 128 位 SSL 加密来提供保密性和完整性。指向 HTTP 端口的任何连接都会重定向至 HTTPS。管理员可以通过 SSL CSR 生成流程上载其 SSL 证书以保护 Web 服务器。默认的 HTTP 和 HTTPS 端口可以进行更改。用户访问权限基于用户权限。
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 命令行界面在安装了 Server Administrator 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。并且，用户必须具有完整的管理员权限或者属于 root 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。 • 可以通过使用 SSH 或 telnet 登录到 iDRAC 来访问固件 RACADM。您可以在不指定 iDRAC IP、用户名和密码的情况下运行固件 RACADM 命令。 • 您无须指定 iDRAC IP、用户名或密码，即可运行固件 RACADM 命令。进入 RACADM 提示界面后，您可以直接运行命令（无需 racadm 前缀）。

界面或协议	说明
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 System Identification（系统标识）按钮 16 秒钟。
CMC Web 界面	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
Lifecycle Controller	使用 Lifecycle Controller 可以执行 iDRAC 配置。要访问 Lifecycle Controller，请在引导过程中按 <F10> 并转到**系统设置 → 高级硬件配置 → iDRAC 设置**。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。
Telnet	使用 Telnet 可以访问 iDRAC，在其中您可以运行 RACADM 和 SMCLP 命令。有关 RACADM 的详细信息，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）。有关 SMCLP 的详细信息，请参阅使用 SMCLP。 **注**: Telnet 不是安全协议，并且在默认情况下处于禁用状态。Telnet 可传输所有数据，包括纯文本形式的密码。当传输敏感信息时，请使用 SSH 界面。
SSH	使用 SSH 可以运行 RACADM 和 SMCLP 命令。它提供与使用加密传输层来实现更高安全保护的 Telnet 控制台相同的功能。在 iDRAC 上，SSH 服务在默认情况下已启用。iDRAC 中的 SSH 服务可以禁用。iDRAC 仅支持具有 DSA 和 RSA 主机密钥算法的 SSH 版本 2。首次启动 iDRAC 时，将会生成唯一的 1024 位 DSA 和 1024 位 RSA 主机密钥。
IPMITool	通过 iDRAC 可使用 IPMITool 访问远程系统的基本管理功能。该界面包括本地 IPMI、LAN 上 IPMI、串行上 IPMI 以及 LAN 上串行。有关 IPMITool 的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *Dell OpenManage Baseboard Management Controller Utilities User's Guide*（Dell OpenManage Baseboard Management Controller 公用程序用户指南）。 **注**: IPMI 版本 1.5 不受支持。
VMCLI	使用虚拟介质命令行界面 (VMCLI) 可通过管理站访问远程介质，并在多个受管系统上部署操作系统。
SMCLP	使用服务器管理工作组服务器管理命令行协议 (SMCLP) 可执行系统管理任务。这通过 SSH 或 Telnet 提供。有关 SMCLP 的更多信息，请参阅使用 SMCLP。

界面或协议	说明
WS-MAN	LC 远程服务基于 WS-Management 协议来执行一对多系统管理任务。您必须使用 WS-MAN 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 和 Python 来编写 WS-MAN 界面脚本。 Web Services for Management (WS-Management) 是基于简单对象访问协议 (SOAP) 的系统管理协议。iDRAC 使用 WS–Management 来传送基于分布式管理任务组 (DMTF) 通用信息模型 (CIM) 的管理信息。CIM 信息定义语义和信息类型，这些语义和信息类型可在受管系统中修改。WS-Management 提供的数据通过映射到 DMTF 配置文件和扩展配置文件的 iDRAC 设备接口提供。 有关更多信息，请参阅以下内容： • **dell.com/idracmanuals** 上提供的 Lifecycle Controller-Remote Services User's Guide（Lifecycle Controller Remote Services 用户指南）。 • **dell.com/support/manuals** 上提供的 Lifecycle Controller Integration Best Practices Guide（Lifecycle Controller 集成最佳实践指南）。 • Dell TechCenter 上的 Lifecycle Controller 页面 — **delltechcenter.com/page/Lifecycle+Controller** • Lifecycle Controller WS-Management 脚本中心 — **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller** • MOF 和配置文件 - **delltechcenter.com/page/DCIM.Library** • DTMF 网站 — **dmtf.org/standards/profiles/**

iDRAC 端口信息

穿过防火墙对 iDRAC 进行远程访问时需要以下端口。下面是 iDRAC 用于监听连接的默认端口。（可选）您可以修改大多数端口。要实现这一点，请参阅配置服务。

表. 3: iDRAC 用于监听连接的端口

Port Number（端口号）	功能
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
161*	SNMP
5900*	虚拟控制台键盘和鼠标重定向、虚拟介质、虚拟文件夹和远程文件共享
5901	VNC 启用 VNC 功能后，端口 5901 将打开。

Port Number（端口号）	功能
* 可配置端口	

下表列出了 iDRAC 用作客户端的端口。

表. 4: iDRAC 用作客户端的端口

Port Number（端口号）	功能
25*	SMTP
53	DNS
68	DHCP 分配的 IP 地址
69	TFTP
162*	SNMP 陷阱
445	通用 Internet 文件系统 (CIFS)
636	SSL 上 LDAP (LDAPS)
2049	网络文件系统 (NFS)
123	网络时间协议 (NTP)
3269	全局编录 (GC) LDAPS
* 可配置端口	

您可能需要的其他说明文件

除本指南以外，Dell 支持网站 **dell.com/support/manuals** 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。

- *iDRAC Online Help*（iDRAC 联机帮助）提供关于 iDRAC Web 界面上可用字段的详细信息及其描述。安装 iDRAC 后，您可以访问联机帮助。
- *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）提供关于 RACADM 子命令、支持的界面以及 iDRAC 属性数据库组和对象定义的信息。
- *iDRAC RACADM Support Matrix*（iDRAC RACADM 支持值表）提供适用于特定 iDRAC 版本的子命令和对象的列表。
- *Systems Management Overview Guide*（系统管理概述指南）提供关于可用于执行系统管理任务的各种软件的简要信息。
- *Dell Lifecycle Controller Graphical User Interface For 12th and 13th Generation Dell PowerEdge Servers User's Guide*（适用于第 12 代和第 13 代 Dell PowerEdge 服务器的 Dell Lifecycle Controller 图形用户界面用户指南）提供了有关使用 Lifecycle Controller 图形用户界面 (GUI) 的信息。
- *Dell Lifecycle Controller Remote Services For 12th and 13th Generation Dell PowerEdge Servers Quick Start Guide*（适用于第 12 代和第 13 代 Dell PowerEdge 服务器的 Dell Lifecycle Controller 远程服务快

速入门指南）提供远程服务功能的概览、有关远程服务、Lifecycle Controller API 的入门信息，以及提供对 Dell TechCenter 中各种资源的参考。

- *Dell Remote Access Configuration Tool User's Guide*（Dell Remote Access Configuration Tool 用户指南）提供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 Systems Software Support Matrix*（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 Service Module Installation Guide*（iDRAC 服务模块安装指南）提供了有关如何安装 iDRAC 服务模块的信息。
- *Dell OpenManage Server Administrator Installation Guide*（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 Software Installation Guide*（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 User's Guide*（Dell OpenManage Baseboard Management Controller Management Utilities 用户指南）包含关于 IPMI 界面的信息。
- *Release Notes*（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。
- *词汇表*介绍本说明文件中使用的术语。

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 Regulatory Compliance（法规合规性）主页，网址是 **dell.com/regulatory_compliance**。保修信息可能包含于此处，也可能为单独的说明文件。
- 机架解决方案附带的 *Rack Installation Instructions*（机架安装说明）介绍如何将系统安装到机架中。
- *Getting Started Guide*（入门指南）概略介绍系统功能、系统设置以及技术规范。
- *Owner's Manual*（用户手册）提供有关系统功能的信息，并说明如何排除系统故障以及如何安装或更换系统组件。

相关任务

联系 Dell
从 Dell 支持站点访问说明文件

社交媒体参考

要了解更多有关产品、最佳实践以及 Dell 解决方案和服务方面的信息，可以访问诸如 Dell TechCenter 等社交媒体平台。您可以通过位于 **www.delltechcenter.com/idrac** 的 iDRAC 维基页面来访问这些博客、论坛、白皮书、演示视频等等。

有关 iDRAC 和其他相关固件说明文件，请参阅 **dell.com/esmmanuals**。

联系 Dell

注: 如果没有活动的 Internet 连接，您可以在购货发票、装箱单、帐单或 Dell 产品目录上查找联系信息。

Dell 提供了若干联机及电话支持和服务选项。服务会因所在国家和地区以及产品的不同而有所差异，您所在的地区可能不提供某些服务。如要联系 Dell 解决有关销售、技术支持或客户服务问题：

1. 请转至 **dell.com/support**。
2. 选择您的支持类别。
3. 在页面底部的**选择国家/地区**下拉列表中，确认您所在的国家或地区。
4. 根据您的需要，选择相应的服务或支持链接。

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：
  - 所有企业系统管理说明文件 - Dell.com/SoftwareSecurityManuals
  - OpenManage 说明文件 - Dell.com/OpenManageManuals
  - 远程企业系统管理说明文件 - Dell.com/esmmanuals
  - OpenManage Connections 企业系统管理说明文件 - Dell.com/OMConnectionsEnterpriseSystemsManagement
  - 适用性工具说明文件 - Dell.com/ServiceabilityTools
  - OpenManage Connections 客户端系统管理说明文件 - Dell.com/DellClientCommandSuiteManuals
- 从 Dell 支持网站：
  a. 转至 Dell.com/Support/Home。
  b. 在**选择产品**部分下，单击**软件和安全**。
  c. 在**软件和安全**组框中，通过以下项单击所需的链接：
     - **企业系统管理**
     - **远程企业系统管理**
     - **Serviceability Tools**
     - **Dell 客户端命令套件**
     - **Connections 客户端系统管理**
  d. 要查看说明文件，请单击所需的产品版本。
- 使用搜索引擎：
  - 在搜索框中键入说明文件的名称和版本。

2

登录 iDRAC

您可以使用 iDRAC 用户、Microsoft Active Directory 用户或轻型目录访问协议 (LDAP) 用户的身份登录 iDRAC。默认用户名和密码分别是 root 和 calvin。您还可以使用单一登录或智能卡进行登录。

注: 您必须具有登录到 iDRAC 的权限才能登录 iDRAC。

相关任务

以本地用户、Active Directory 用户或 LDAP 用户身份登录 iDRAC
使用智能卡登录 iDRAC
使用单一登录登录 iDRAC
更改默认登录密码

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。

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，输入 `https://[iDRAC-IP-address]`，然后按 <Enter> 键。

   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。

   随即会显示 **Login**（登录）页面。
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 **Domain**（域）下拉菜单中，选择 **This iDRAC**（此 iDRAC）。
4. 对于 Active Directory 用户，请在 **Username**（用户名）和 **Password**（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 **This iDRAC**（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 **Domain**（域）下拉菜单中选择 Active Directory 域。

5. 对于 LDAP 用户，请在 **Username**（用户名）和 **Password**（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 **This iDRAC**（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 Configure Users（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 **Default Password Warning**（默认密码警告）页面，允许您轻松更改密码。

相关概念

配置用户帐户和权限
更改默认登录密码

相关任务

配置支持的 Web 浏览器

使用智能卡登录 iDRAC

您可以使用智能卡登录 iDRAC。智能卡提供二元验证 (TFA)，该认证提供双层安全性：

- 物理智能卡设备。
- 加密代码（例如密码或 PIN）。

用户必须使用智能卡和 PIN 验证其凭据。

相关任务

使用智能卡作为本地用户登录 iDRAC
使用智能卡作为 Active Directory 用户登录 iDRAC

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 **Login（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 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。

相关概念

启用或禁用智能卡登录

相关任务

为本地用户配置 iDRAC 智能卡登录

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：

- 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]` iDRAC 的 IP 地址而 `[port number]` 是 HTTPS 端口号。
2. 插入智能卡并单击 **Login（登录）**。
   将显示 **PIN** 弹出窗口。
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。

相关概念

启用或禁用智能卡登录

相关任务

为 Active Directory 用户配置 iDRAC 智能卡登录

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）。

相关概念

为 Active Directory 用户配置 iDRAC SSO 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) 而 `[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

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 **dell.com/support/manuals** 上提供的 *Chassis Management Controller User's Guide*（Chassis Management Controller 用户指南）。

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 **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）。

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。

相关任务

验证 CA 证书以在 Linux 上使用远程 RACADM

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 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

使用固件 RACADM 访问 iDRAC

您可以使用 SSH 或 Telnet 界面访问 iDRAC 并运行固件 RACADM 命令。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）。

使用 SMCLP 访问 iDRAC

当您使用 Telnet 或 SSH 登录 iDRAC 时，SMCLP 是默认的命令行提示符。有关更多信息，请参阅使用 SMCLP。

使用公共密钥验证登录 iDRAC

您可以通过 SSH 登录 iDRAC（无需输入密码）。您还可以将单一的 RACADM 命令作为命令行参数发送到 SSH 应用程序。由于该会话在命令完成时结束，因此该命令行选项的行为与远程 RACADM 类似。

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
```

相关概念

对 SSH 使用公共密钥验证

多个 iDRAC 会话

下表提供了可能使用各种界面的多个 iDRAC 会话的列表。

表. 5: 多个 iDRAC 会话

界面	会话数
iDRAC Web 界面	6
远程 RACADM	4
固件 RACADM / SMCLP	SSH - 2 Telnet - 2 串行 - 1

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。
- 任何当前已启用的帐户的凭据是 root/calvin。

使用 SSH、Telnet、远程 RACADM 或 Web 界面登录 iDRAC 时，还会显示一条警告消息。对于 Web 界面、SSH 和 Telnet，会为每个会话显示一条警告消息。对于远程 RACADM，会为每个命令显示该警告消息。

相关任务

启用或禁用默认密码警告消息

使用 Web 界面更改默认登录密码

在您登录 iDRAC Web 界面时，如果显示**默认密码警告**页面，则可以更改密码。要实现这一点，请执行以下操作：

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。

   密码的最大字符数为 20。字符进行屏蔽处理。支持使用以下字符：

   - 0-9
   - A-Z
   - a-z
   - 特殊字符：+、&、?、>、-、}、|、.、!、(、'、,、_、[、"、@、#、)、*、;、$、]、/、`、%、=、<、:、{、I、\
3. 在 **Confirm Password**（确认密码）字段中，再次输入密码。
4. 单击 **Continue**（继续）。新密码即配置好并且您登录到 iDRAC。

   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 到 16 的值（代表用户帐户），`<password>` 是新的用户定义的密码。

有关更多信息，请参阅 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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）。
   随即会显示 **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。
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。要实现这一点，您必须拥有 Configure Users（配置用户）权限。

使用 Web 界面启用或禁用默认密码警告消息

要在登录 iDRAC 后启用或禁用默认密码警告消息的显示，请执行以下操作：

1. 转至**概览** → **iDRAC 设置** → **用户验证** → **本地用户**。
   此时将显示**用户**页面。
2. 在**默认密码警告**部分，选择**启用**，然后单击**应用**以启用在登录 iDRAC 时显示**默认密码警告**页面。否则，请选择**禁用**。
   或者，如果此功能已启用并且您不希望为后续登录显示警告消息，请在 **Default Password Warning**（默认密码警告）页面上，选择 **Do not show this warning again**（不再显示此警告）选项，然后单击 **Apply**（应用）。

使用 RACADM 启用或禁用警告消息以更改默认登录密码

要使用 RACADM 来启用警告消息的显示以便更改默认登录密码，请使用 `idrac.tuning.DefaultCredentialWarning` 对象。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

无效密码凭据

为确保安全，防止未经授权的用户和拒绝服务 (DoS) 攻击，iDRAC 在阻止 IP 和 SNMP 陷阱（如果已启用）之前提供了以下措施：

- 一系列登录错误和警报
- 增加每次连续的错误登录尝试的时间间隔
- 日志条目

注: 登录错误和警报、增加每次错误登录的时间间隔以及日志条目，在使用任何 iDRAC 界面（例如 Web 界面、Telnet、SSH、远程 RACADM、WS-MAN 和 VMCLI）时均有提供。

表. 6: iDRAC Web 界面错误登录尝试行为

登录尝试次数	阻止（秒）	记录的错误 (USR00034)	GUI 显示消息	SNMP 警报（如果已启用）
第一次错误登录	0	否	无	否
第二次错误登录	30	是	• `RAC0212：登录失败。请验证用户名和密码是否正确。登录延迟 30 秒。` • 禁用**重试**按钮 30 秒。	是
第三次错误登录	60	是	• `RAC0212：登录失败。请验证用户名和密码是否正确。登录延迟 60 秒。` • 禁用**重试**按钮 60 秒。	是
每次额外错误登录	60	是	• `RAC0212：登录失败。请验证用户名和密码是否正确。登录延迟 60 秒。` • 禁用**重试**按钮 60 秒。	是

注: 24 小时后，这些计数器重置并应用上述限制。

3

设置受管系统和管理站

要使用 iDRAC 执行带外系统管理，您必须配置 iDRAC 的远程访问功能，设置管理站和受管系统，并且配置受支持的 Web 浏览器。

注: 对于刀片式服务器，请在机箱中安装 CMC 和 I/O 模块，并在执行配置前将系统实际安装到机箱中。

iDRAC Express 和 iDRAC Enterprise 出厂时均配置有默认的静态 IP 地址。此外 Dell 还提供了以下两个选项：

- **配置服务器** - 如果您在数据中心环境安装了一台配置服务器，可使用此选项。配置服务器可管理并自动执行操作系统及 Dell PowerEdge 服务器应用程序的部署或升级。 通过启用配置服务器选项，服务器在首次引导时会搜索配置服务器，以便控制并开始自动执行部署或升级过程。
- **DHCP** - 如果数据中心环境安装了动态主机配置协议 (DHCP) 服务器，或者如果是使用 iDRAC 的自动配置功能或 OpenManage Essentials Configuration Manager 来自动执行服务器配置，可使用此选项。DHCP 服务器将自动为 iDRAC 分配 IP 地址、网关和子网掩码。

您可以在订购服务器时启用配置服务器或 DHCP。启用任一功能皆为免费。但无法同时启用两种设置。

相关概念

[设置 iDRAC IP 地址]
[设置受管系统]
[更新设备固件]
[回滚设备固件]

相关任务

[设置管理站]
[配置支持的 Web 浏览器]

设置 iDRAC IP 地址

您必须根据您的网络基础架构来配置初始网络设置，以启用与 iDRAC 之间的通信。您可以使用以下界面之一来设置 IP 地址：

- iDRAC 设置公用程序
- Lifecycle Controller（请参阅 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南））
- Dell Deployment Toolkit（请参阅 *Dell Deployment Toolkit User's Guide*（Dell Deployment Toolkit 用户指南））
- 机箱或服务器 LCD 面板（请参阅系统的 *Hardware Owner's Manual*（硬件用户手册））

  注: 对于刀片服务器，只有在 CMC 初始配置期间，您才能使用机箱的 LCD 面板配置网络设置。当完成机箱部署后，您不能使用机箱 LCD 面板重新配置 iDRAC。
- CMC Web 界面（请参阅 *Dell Chassis Management Controller Firmware User's Guide*（Dell Chassis Management Controller 固件用户指南））

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：

- 确保*在设置 iDRAC IP 地址之后变更默认用户名和密码*。
- 通过以下任意界面访问它：
  - 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。
  - Telnet（由于默认情况下它被禁用，因此必须先启用它）
  - 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 **support.dell.com** 获得）

相关任务

使用 iDRAC 设置公用程序设置 iDRAC IP
使用 CMC Web 界面设置 iDRAC IP
启用配置服务器
使用自动配置功能配置服务器和服务器组件

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 **Network**（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。

相关任务

网络设置
常见设置
IPv4 设置
IPv6 设置
IPMI 设置

[VLAN 设置](#)

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 **Enable NIC**（**启用 NIC**）下，选择 **Enabled**（**启用**）选项。
2. 根据网络需要，从 **NIC Selection**（**NIC 选择**）下拉菜单中，选择以下端口之一：
   - **专用** — 启用远程访问设备，以使用 Remote Access Controller (RAC) 上可用的专用网络界面。该界面不与主机操作系统共享，并将管理流量路由至一个单独的物理网络，使得可以将其从应用程序流量中分离出来。

     该选项意味着 iDRAC 的专用网络端口会将其流量从服务器的 LOM 或 NIC 端口分离出来单独进行路由。从管理网络流量方面来说，"专用"选项允许为 iDRAC 分配的 IP 地址可以与分配给主机 LOM 或 NIC 的 IP 地址位于相同或不同的子网。

     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，有两个 LOM 选项（LOM1 和 LOM2）可用或四个 LOM 选项都可用，具体取决于服务器型号。对于有两个 NDC 端口的刀片服务器，有两个 LOM 选项（LOM1 和 LOM2）可用，而在有四个 NDC 端口的服务器上，四个 LOM 选项都可用。

   注: 如果在有两个 NDC 的全高服务器中使用 LOM，则以下 bNDC 不支持共享 LOM，因为它们不支持硬件仲裁：

   - Intel 2P X520–k bNDC 10 G
   - Emulex OCM14102–N6–D bNDC 10 Gb
   - Emulex OCm14102-U4-D bNDC 10 Gb
   - Emulex OCm14102-U2-D bNDC 10 Gb
   - QLogic QMD8262–k DP bNDC 10 G
3. 从 **Failover Network**（**故障转移网络**）下拉菜单中，选择其余 LOM 中的一个。如果网络发生故障，流量将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: 如果您在 **NIC 选择**下拉菜单中选择了**专用**，则该选项将变灰。

注: 在共享 LOM 上，以下 Emulex rNDC 和 bNDC 不支持故障转移：

- Emulex OCM14104-UX-D rNDC 10 Gbx
- Emulex OCM14104-U1-D rNDC 10 Gb
- Emulex OCM14104-N1-D rNDC 10 Gb
- Emulex OCM14104B-N1-D rNDC 10 Gb
- Emulex OCM14102-U2-D bNDC 10 Gb
- Emulex OCM14102-U4-D bNDC 10 Gb
- Emulex OCM14102-N6-D bNDC 10 Gb

注: 在 PowerEdge FM120x4 服务器上，机箱底座配置不支持**故障转移网络**。有关机箱底座配置的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 Chassis Management Controller (CMC) User's Guide（Chassis Management Controller (CMC) 用户指南）。

注: 在 PowerEdge FM120x4 服务器上配置增强的网络适配器隔离时，请确保在主机系统中禁用 LOM2，并且没有为 iDRAC NIC 选择 LOM2。有关机箱底座配置的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 Chassis Management Controller (CMC) User's Guide（Chassis Management Controller (CMC) 用户指南）。

4. 如果 iDRAC 必须自动设置双工模式和网络速度，请在**自动协商**下，选择**打开**。该选项仅用于专用模式。如果启用，iDRAC 会根据网络速度将网络速度设置为 10、100 或 1000 Mbps。
5. 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。只有在启用 **Auto Negotiation（自动协商）**选项的情况下，该选项才可用。

6. 在 **Duplex Mode（双工模式）**下，选择 **Half Duplex（半双工）**或 **Full Duplex（全双工）**选项。

   注: 如果您启用 **Auto Negotiation（自动协商）**，该选项变灰。

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 **Register DRAC on DNS（向 DNS 注册 DRAC）**。
2. 输入 **DNS DRAC Name（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**。

IPv4 设置

配置 IPv4 设置：

1. 在 **Enable IPv4**（启用 IPv4）下选择 **Enabled**（启用）选项。
2. 在**启用 DHCP** 下选择**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**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. 或者，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。

IPv6 设置

或者，基于基础架构设置，您可以使用 IPv6 地址协议。

配置 IPv6 设置：

1. 在 **Enable IPv6**（启用 IPv6）下选择 **Enabled**（启用）选项。
2. 对于 DHCPv6 服务器，要将 IP 地址、网关和子网掩码自动分配给 iDRAC，请在**启用自动配置**下选择**启用**选项。如果已启用，将禁用静态值。否则，继续下一步以使用静态 IP 地址进行配置。
3. 在 **Static IP Address 1**（静态 IP 地址 1）框中，输入静态 IPv6 地址。
4. 在 **Prefix Length**（前缀长度）框中，输入 0 和 128 之间的值。
5. 在 **Gateway**（网关）框中，输入网关地址。
6. 如果使用 DHCP，启用 **DHCPv6 to obtain DNS Server addresses**（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。否则，请选择 **Disabled**（禁用）并执行以下操作：
   - 在 **Static Preferred DNS Server**（静态首选 DNS 服务器）框中，输入静态 DNS 服务器 IPv6 地址。
   - 在 **Static Alternate DNS Server**（静态备用 DNS 服务器）框中，输入静态备用 DNS 服务器。

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 **Priority（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 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。

1. 登录到 CMC Web 界面。
2. 转至 **Server Overview（服务器概述）** → **Setup（设置）** → **iDRAC**。

   随即会显示 **Deploy iDRAC**（部署 iDRAC）页面。

3. 在 **iDRAC Network Settings**（iDRAC 网络设置）中，根据要求选择 **Enable LAN**（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 **Server Overview（服务器概述） → <server name>**。

   随即会显示 **Server Status**（服务器状态）页面。
5. 单击 **Launch iDRAC**（启动 iDRAC）并转至 **Overview（概述） → iDRAC Settings（iDRAC 设置） → Network（网络）**。
6. 在 **Network**（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

   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 **Apply**（应用）。

   有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Chassis Management Controller User's Guide*（Chassis Management Controller 用户指南）。

启用配置服务器

借助配置服务器功能，新安装的服务器可以自动查找托管配置服务器的远程管理控制台。*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。有关配置服务器的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller Remote Services 用户指南）。

配置服务器可结合静态 IP 地址使用。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。

您可以使用 iDRAC 设置公用程序或使用 Lifecycle Controller 启用配置服务器功能。有关使用 Lifecycle Controller 的信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。

如果出厂的系统未启用配置服务器功能，则将启用默认的管理员帐户（用户名为 root，密码为 calvin）。在启用配置服务器之前，确保禁用该管理员帐户。如果 Lifecycle Controller 中启用了配置服务器功能，所有 iDRAC 用户帐户均被禁用，直至*查找到*该配置服务器。

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 Settings（iDRAC 设置） → Remote Enablement（远程启用）**。

   将显示 **iDRAC Settings Remote Enablement**（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 **Back**（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 **Network**（网络）。

将显示 **iDRAC Settings Network**（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

自动配置功能通过自动导入包含所有可配置参数的 Server Configuration Profile (SCP) XML 文件，可以在单次操作中配置一台服务器中的所有组件（例如 BIOS、iDRAC 和 PERC）。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。

SCP 文件的创建方法是：配置一台“黄金配置”服务器，并将该服务器的配置导出至共享位置（CIFS 或 NFS），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 服务器选项来指定 SCP 文件名（可选）、SCP 文件位置以及用于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。

注:

- 只有在已启用 **DHCPv4** 和 **Enable IPv4**（启用 IPv4）选项之后，才能启用自动配置功能。
- 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，自动配置功能将被禁用。有关启用自动配置的更多信息，请参阅使用 RACADM 启用自动配置功能。

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 为默认的 SCP 文件名。

您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 R730s 和 PowerEdge R530s，可以使用 R730-config.xml 和 R530-config.xml 这两个 SCP 文件。

注: 在装有 iDRAC 2.20.20.20 及更高版本的系统上，如果 DHCP 选项 60 中没有文件名参数，iDRAC 服务器配置代理会使用服务器的服务标签、型号或者默认文件名 config.xml，来自动生成配置文件名。

iDRAC 服务器配置代理将采用以下顺序的规则，来确定要对每台 iDRAC 或 PowerEdge 服务器应用文件共享中的哪些 XML 文件：

1. 在 DHCP 选项 60 中指定的文件名。
2. <ServiceTag>-config.xml - 如果未在 DHCP 选项 60 中指定文件名，将使用系统服务标签来唯一标识系统的 SCP 文件。例如，CDVH7R1-config.xml
3. <Model number>-config.xml - 如果未指定选项 60 文件名，并且找不到 <Service Tag>-config.xml 文件，则使用系统型号作为要使用的 XML 配置文件名的基础。例如，R520-config.xml。
4. config.xml - 如果选项 60 文件名、基于服务标签和基于型号的文件不可用，则使用默认的 config.xml 文件。

注: 如果网络共享上没有其中的任何文件，服务器配置文件导入作业将被标记为故障，原因是找不到文件。

相关概念

[自动配置顺序](#)
[DHCP 选项](#)

相关任务

[使用 iDRAC Web 界面启用自动配置功能](#)
[使用 RACADM 启用自动配置功能](#)

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. iDRAC 获取 IP 地址过程中将公布供应商类别标识符 iDRAC。（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给 DHCP 客户端。每个参数即一个 DHCP 选项。每个选项使用一个选项标签进行标识，选项标签为一个单字节的值。选项标签 0 和 255 分别预留用于填充和结束选项。所有其他的值可用于定义选项。

DHCP 选项 43 用于从 DHCP 服务器发送信息给 DHCP 客户端。这些选项被定义为文本字符串形式。此文本字符串被设置为包含 XML 文件名、共享位置和用于访问该位置的凭据的值。例如，

```
option myname code 43 = text; subnet 192. 168.0.0 netmask 255.255.255.0 { # 默认
网关选项路由器 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; #东部标准时间 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 用于标识 DHCP 客户端并将其与特定供应商关联起来。应该对任何配置为根据客户端的供应商 ID 执行操作的 DHCP 服务器配置选项 43 和选项 60。在 Dell PowerEdge 服务器中，iDRAC 将使用供应商 ID：*iDRAC* 标识其自身。因此，您必须添加一个新“供应商类”，并在其下为“代码 60”创建“范围选项”，然后为 DHCP 服务器启用此新范围选项。

相关任务

[在 Windows 上配置选项 43](#)
[在 Windows 上配置选项 60](#)
[在 Linux 上配置选项 43 和选项 60](#)

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** 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 XML 配置文件）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 **Start**（开始） → **Administration Tools**（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**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 **Advanced**（**高级**）选项卡。
15. 从**供应商类**下拉菜单中选择 **iDRAC**。**可用选项**列中将显示 `060 iDRAC`。
16. 选择 **060 iDRAC** 选项。
17. 输入必须要发送至 iDRAC 的字符串值（以及标准 DHCP 所提供的 IP 地址）。此字符串值有助于导入正确的 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) - 指示导出的服务器配置文件的 XML 文件名。在 iDRAC 2.20.20.20 版或更高版本中，可选填此文件名。

  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。

- 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。
- 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。

- Username (-u) - 指示访问网络共享所需的用户名。仅 CIFS 要求提供此信息。
- Password (-p) - 指示访问网络共享所需的密码。仅 CIFS 要求提供此信息。
- ShutdownType (-d) - 指示关机模式。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 表示开启。 默认设置为 1。

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

注: 在运行 Windows 操作系统的 DHCP 服务器上，如果使用的是 iDRAC 2.20.20.20 版之前的版本，请务必在 (–f) 前面添加一个空格。

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 <*2USERNAME*> -p <*PASSWORD*> -d 1 -t 400

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：

- Filename (–f) - 指示导出的服务器配置文件的 XML 文件名。在 iDRAC 2.20.20.20 版或更高版本中，可选填文件名。

  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。

- 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。
- 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。

- Username (-u) - 指示访问网络共享所需的用户名。仅 CIFS 要求提供此信息。
- Password (-p) - 指示访问网络共享所需的密码。仅 CIFS 要求提供此信息。

  注: Linux NFS 和 CIFS 共享示例：

  – **NFS:** -f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500

  – **CIFS:** -f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400

  确保为 NFS 网络共享使用 NFS2 或 NFS3

- ShutdownType (-d) - 指示关机模式。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 表示开启。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 {

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：

- 在与 iDRAC 及 DHCP 服务器相同的子网上，存在受支持的可用网络共享（NFS 或 CIFS）。测试网络共享，确保其可以访问且防火墙和用户权限设置无误。
- 服务器配置文件已导出至网络共享。此外还要确保 XML 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**概览** → **iDRAC 设置** → **网络**。

   随即会显示 **Network**（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 XML 文件来配置组件一次。此次配置后，将禁用自动配置。

- **在重设后启用一次 —** 重设 iDRAC 后，仅使用 DHCP 服务器所引用的 XML 文件配置组件一次。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**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 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

注: 有关自动配置功能的更多信息，请参阅 **delltechcenter.com/idrac** 上提供的 *Zero-Touch Bare Metal Server Provisioning using Dell iDRAC with Lifecycle Controller Auto Config*（使用 Dell iDRAC with Lifecycle Controller 的自动配置功能零接触配置裸机服务器）白皮书。

使用散列密码提供更高的安全性

在版本为 2.*xx.xx.xx* 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），并且可以纯文本格式提供密码。

通过新的密码散列功能：

- 您可以生成自己的 SHA256 散列，用于设置 iDRAC 用户密码和 BIOS 密码。这可允许您在服务器配置文件、RACADM 和 WSMAN 中获得 SHA256 值。提供 SHA256 密码值时，您不能通过 SNMPv3 和 IPMI 进行验证。
- 您可以设置一个模板服务器，其中包括所有使用当前纯文本机制的 iDRAC 用户帐户和 BIOS 密码。在设置服务器之后，您可以使用包含散列值的密码导出服务器配置文件。导出中包含 SNMPv3 和 IPMI 验证所需的散列值。

注: 在将 Dell 第 12 代 PowerEdge 服务器从版本 2.xx.xx.xx 降级到 1.xx.xx 时，如果服务器是使用散列身份验证设置的，则除非将密码设置为默认值，否则无法登录任何界面。

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 密码散列算法设置 iDRAC 用户帐户的密码，而未使用其他散列（SHA1v3Key 或 MD5v3Key），那么无法通过 SNMP v3 和 IPMI 进行验证。

使用 RACADM 的散列密码

使用以下对象和 **set** racadm 子命令来设置散列密码：

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

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 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。

导入服务器配置文件时，您可以对现有密码属性或新密码散列属性取消注释。如果两者都已取消注释，则会生成错误，不会设置密码。导入期间不会应用注释的属性。

不使用 SNMPv3 和 IPMI 验证生成散列密码

要在不使用 SNMPv3 和 IPMI 验证的情况下生成散列密码：

1. 对于 iDRAC 用户账户，必须使用 SHA256 对密码执行 Salt 操作。

   对密码执行 Salt 操作时，将会添加一个 16 个字节长度的二进制字符串。如果提供，Salt 必须是 16 个字节长度。
2. 在导入的服务器配置文件、RACADM 或 WAMAN 中提供散列值和 Salt。
3. 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。

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. 安装支持的操作系统。有关更多信息，请参阅发行说明。
2. 安装和配置支持的 Web 浏览器（Internet Explorer、Firefox、Chrome 或 Safari）。
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）。
4. 从 *Dell Systems Management Tools and Documentation* DVD 中的 SYSMGMT 文件夹安装远程 RACADM 和 VMCLI。否则，按照默认方式运行 DVD 上的 **Setup** 以安装远程 RACADM 和其他 OpenManage 软件。有关 RACADM 的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。
5. 根据要求安装下列组件：
   - Telnet
   - SSH 客户端
   - TFTP
   - Dell OpenManage Essentials

相关概念

安装和使用 VMCLI 公用程序

相关任务

配置支持的 Web 浏览器

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 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 **dell.com/support/manuals** 上提供的 *Chassis Management Controller User’s Guide*（Chassis Management Controller 用户指南）。

- 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。

相关概念

启动虚拟控制台

相关任务

网络设置

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 **dell.com/support/manuals** 上提供的 *Dell OpenManage Server Administrator User’s Guide*（Dell OpenManage Server Administrator 用户指南）。

相关任务

修改本地管理员帐户设置

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**概览** → **服务器** → **属性** → **详细信息**。
   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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。有关各选项的详细信息，请参阅 *《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

服务器散热所需的功率可使总体系统功率显著增加。热控制是通过风扇速度和系统功率管理来主动管理系统散热，在尽量降低系统功耗、气流和系统输出噪音的同时确保系统稳定运行。您可以调节热控制设置并针对系统性能和每瓦性能要求进行优化。

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

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**概览** → **硬件** → **风扇** → **设置**。

   这将显示**风扇设置**页面。

2. 指定以下各项：
   - **散热配置文件** - 选择散热配置文件：
     - **默认的散热配置文件设置** — 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，该选项设置为**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。

  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散热能力。如果添加了硬件设备（例如，新的 PCIe 卡），则可能需要额外的散热能力。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）。可能的值有：
  - **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** - 风扇速率偏移设置为“关闭”。这是默认值。如果设置为关闭，则不显示百分比。默认的风扇速率将不会发生任何偏移。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 适配器散热。不过，该功能可用于提高针对其他目的的散热能力。

- **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 —** 输入百分比值。

  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。部分 Dell 服务器可能支持，也可能不支持部分或所有这些自定义的用户散热选项。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。
   随即显示以下消息：

   ```
   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。

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。

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`
			这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`
			将显示以下错误消息：
			`ERROR: RAC947: Invalid object value specified.`
			确保根据对象类型来指定值。
			有关更多信息，请参阅 RACADM 帮助。

对象	说明	使用情况	示例
			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。
	• 请使用 `FanSpeedOffset` 对象和索引值 1 来设置此值。
		值为 0 - 100	`racadm get system.thermalsettings 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”。这意味着使用以下命令时，将会应用风扇速率偏移的“最大值”（即全速，100% PWM）。在大多数情况下，此偏移将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风扇速率偏移“中值”(47% PWM)。
			
			`racadm set system.thermalsettings FanSpeedOffset 2`

对象	说明	使用情况	示例
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	值为 0 至 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。	值从 MFSMinimumLimit 到 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 要将散热配置文件设置为“最高性能”： racadm set system.thermalsettings.ThermalProfile 1

对象	说明	使用情况	示例
`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： • 0 - 启用 • 1 - 禁用 **注:** 默认值为 0。	要为检测到的第三方 PCI 卡禁用任何默认的风扇速度响应设置，可以使用：`racadm set system.thermalsettings.ThirdPartyPCIFanResponse 1`

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
   - 风扇速率偏移
   - 最低风扇速率

   有关各字段的信息，请参阅使用 Web 界面修改散热设置。

   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。部分 Dell 服务器可能支持，也可能不支持部分或所有这些自定义的用户散热选项。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. 依次单击 **Back**（后退）、**Finish**（完成）和 **Yes**（是）。

   耐热设置即配置完成。

配置支持的 Web 浏览器

Internet Explorer、Mozilla Firefox、Google Chrome 和 Safari Web 浏览器支持 iDRAC。有关版本的信息，请参阅 **dell.com/idracmanuals** 上提供的 *Release Notes*（发行说明）。

如果从通过代理服务器连接到 Internet 的管理站连接到 iDRAC Web 界面，则必须配置 Web 浏览器以从该服务器访问 Internet。此部分提供配置 Internet Explorer 的信息。

配置 Internet Explorer Web 浏览器：

1. 将 IE 设置为**以管理员身份运行**。
2. 在 Web 浏览器中，转至**工具** → **Internet 选项** → **安全** → **本地网络**。
3. 单击**自定义级别**，选择**中-低**，然后单击**重设**。单击**确定**确认。单击**自定义级别**打开该对话框。
4. 向下滚动到标有 ActiveX 控件和插件的部分，并设置以下各项：

   注: “中-低”状态中的设置取决于 IE 版本。

   - ActiveX 控件自动提示：启用
   - 二进制和脚本行为：启用

- 下载已签名的 ActiveX 控件：提示
- 对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本：提示
- 运行 ActiveX 控件和插件：启用
- 对标记为可安全执行脚本的 ActiveX 控件执行脚本：启用

在**下载**下：

- 文件下载的自动提示：启用
- 文件下载：启用
- 字体下载：启用

在**其他**下：

- 允许 META REFRESH：启用
- 允许 Internet Explorer 网页浏览器控件的脚本：启用
- 允许由脚本初始化的窗口，不受大小和位置限制：启用
- 没有证书或只有一个证书时不提示进行客户端证书选择：启用
- 在 IFRAME 中加载程序和文件：启用
- 基于内容打开文件，而不是基于文件扩展名：启用
- 软件频道权限：安全级 - 低
- 提交非加密表单数据：启用
- 使用弹出窗口阻止程序：禁用

在**脚本**下：

- 活动脚本：启用
- 允许通过脚本进行粘贴操作：启用
- Java 小程序脚本：启用

5. 转至**工具** → **Internet 选项** → **高级**。
6. 在**浏览**下：
   - 总是以 UTF-8 发送 URL：选中
   - 禁用脚本调试 (Internet Explorer)：选中
   - 禁用脚本调试（其他）：选中
   - 显示每个脚本错误的通知：清除
   - 启用即需安装（其他）：选中
   - 启用页面转换：选中
   - 启用第三方浏览器扩展：选中
   - 再次使用窗口来启动快捷方式：清除

   在 **HTTP 1.1 设置**下：

   - 使用 HTTP 1.1：选中
   - 通过代理连接使用 HTTP 1.1：选中

   在 **Java (Sun)** 下：

   - 使用 JRE 1.6.x_yz：选中（可选；版本可能不同）

   在**多媒体**下：

   - 启用自动图像大小调整：选中

- 播放网页中的动画：选中
- 播放网页中的视频：选中
- 显示图片：选中

在安全下：

- 检查发行商的证书是否吊销：清除
- 检查下载的程序的签名：选中
- 使用 SSL 2.0：选中
- 使用 SSL 3.0：选中
- 使用 TLS 1.0：选中
- 对无效站点证书发出警告：选中
- 在安全和非安全模式之间转换时发出警告：选中
- 重定向提交的表单时发出警告：选中

注: 要修改该设置，建议您了解并理解后果。例如，如果您阻止弹出窗口，则部分 iDRAC Web 界面可能无法正常工作。

7. 单击**应用**，然后单击**确定**。
8. 单击**连接**选项卡。
9. 在**局域网 (LAN) 设置**下，单击**局域网设置**。
10. 如果您使用 IE9 和 IPv6 地址访问 iDRAC，请清除**使用自动配置脚本**选项。
11. 如果选中了**使用代理服务器**框，则选择**对于本地地址不使用代理服务器**框。
12. 单击**确定**两次。
13. 关闭并重新启动浏览器，确保所有更改都生效。

注: 使用 Internet Explorer 9.x 登录 iDRAC Web 界面时，有时一些页面中的内容可能无法正确显示。要解决此问题，请按 <F12> 键。在 **Internet Explorer 9 调试**窗口中，将**文档模式**选择为 **Internet Explorer 7**。浏览器将会刷新，并且 iDRAC **登录**页面将会显示。

相关概念

[查看 Web 界面的本地化版本]

相关任务

[将 iDRAC 添加到受信域列表中]
[禁用 Firefox 中的白名单功能]

将 iDRAC 添加到受信域列表中

当您访问 iDRAC Web 界面时，如果受信域列表中没有 iDRAC IP 地址，系统会提示您将该地址添加到该列表中。完成后，请单击**刷新**或者重新启动 Web 浏览器以建立指向 iDRAC Web 界面的连接。

在某些操作系统上，如果受信域列表中缺少 iDRAC IP 地址，Internet Explorer (IE) 8 可能不会提示您将该 IP 地址添加到列表中。

注: 如果使用浏览器不信任的证书连接到 iDRAC Web 界面，则当您确认第一条警告后，系统会再次显示浏览器的证书错误警告。这是出于安全考虑的预期行为。

要在 IE 8 中将 iDRAC IP 添加到受信域列表中，请执行以下操作：

1. 选择 **Tools**（工具） → **Internet Options**（Internet 选项） → **Security**（安全） → **Trusted sites**（受信站点） → **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。

禁用 Firefox 中的白名单功能

对于每个具有插件的不同网站，Firefox 的"白名单"安全功能要求具备用户权限才能安装插件。如果启用，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，即使查看器版本相同也是如此。

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）的值将变成粗体文本。**Status**（状态）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，请双击 **xpinstall.enabled**，将 **Value**（值）设置为 **True**。

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)

附带的 ISO 标识符表示支持的语言变体。对于某些支持的语言，需要将浏览器大小调整为 1024 像素宽才能查看所有功能。

iDRAC Web 界面设计用于与本地化的键盘一起使用，以提供对各种语言版本的支持。iDRAC Web 界面的某些功能（如虚拟控制台）可能需要执行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: 请参阅浏览器文档了解如何配置或设置不同的语言并查看本地化版本的 iDRAC Web 界面。

更新设备固件

使用 iDRAC 可以更新 iDRAC、BIOS 和所有通过 Lifecycle Controller 更新进行支持的设备固件，例如：

- Lifecycle Controller
- 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)
- PCIe 固态驱动器 (SSD)
- SAS 硬盘驱动器

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。

在固件更新后，**System Inventory**（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)
- **.d7** — 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 System Control（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 **.d7** 的文件，您必须具有"配置"权限。

注: 在第 13 代 PowerEdge 服务器上，可以从 2.*xx*.*xx*.*xx* 直接升级到固件版本 2.10.10.10，在第 12 代 PowerEdge 服务器上，可以从 1.5*x*.5*x* 或 1.6*x*.6*x* 直接升级到固件版本 2.10.10.10。

注: 在升级 iDRAC 固件后，您可能会发现 Lifecycle Controller 日志中显示的时间戳不同，直至使用 NTP 重置 iDRAC 时间。在重置 iDRAC 时间之前，Lifecycle 日志显示 BIOS 时间。

您可以使用以下方法执行固件更新：

- 使用本地系统或网络共享上的固件映像文件。
- 连接到其中包含可用更新目录的 FTP、TFTP 或 HTTP 站点或网络存储库。可以使用 Dell Repository Manager 创建自定义存储库。有关更多信息，请参阅 *Dell Repository Manager Data Center User's Guide*（Dell Repository Manager 数据中心用户指南）。iDRAC 会自动提供安装在服务器上的 BIOS 和固件与存储库位置或 FTP 站点上的 BIOS 和固件之间的区别。存储库中包含的所有适用更新也适用于系统。在具有 iDRAC Enterprise 许可证的情况下，此功能可用。
- 计划使用 FTP 站点或网络存储库位置中的目录文件定期自动更新固件。

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: 当通过带外方式应用多个固件更新时，将以尽可能高效的顺序排列这些更新，以减少不必要的系统重新启动。

表. 7: 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

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？
Lifecycle Controller	否	否	否	是
BIOS	是	是	是	是
RAID 控制器	是	是	是	是
背板	是	是	是	是
机柜	是	是	否	是
NIC	是	是	是	是
iDRAC	是	**否	*否	*否
电源设备	是	是	是	是
CPLD	否	是	是	是
FC 卡	是	是	是	是
PCIe SSD	否	否	否	否
SAS 硬盘驱动器	否	是	是	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。iDRAC 通信和监测功能可能暂时中断。

** 当从 1.30.30 或更高版本更新 iDRAC 时，无需重新启动系统。但是，在使用带外接口应用早于 1.30.30 的 iDRAC 固件版本时，需要重新启动系统。

相关概念

[下载设备固件]

相关任务

[更新单个设备固件]
[使用存储库更新固件]
[使用 FTP 更新固件]
[使用 TFTP 更新设备固件]
[使用 HTTP 更新设备固件]
[使用 RACADM 更新设备固件]
[计划自动固件更新]
[使用 CMC Web 界面更新固件]
[使用 DUP 更新固件]
[使用远程 RACADM 更新固件]
[使用 Lifecycle Controller 远程服务更新固件]

下载设备固件

您下载的映像文件格式取决于更新方法：

- iDRAC Web 界面 - 下载打包为自解压存档的二进制映像。默认的固件映像文件是 firmimg.d7。

注: 相同的文件格式用于使用 CMC Web 界面恢复 iDRAC。

- 受管系统 - 下载特定于操作系统的 Dell 更新包 (DUP)。Linux 操作系统文件扩展名是 .bin，而 Windows 操作系统的文件扩展名是 .exe。
- Lifecycle Controller - 下载最新目录文件和 DUP，并使用 Lifecycle Controller 中的 *Platform Update*（平台更新）功能来更新设备固件。有关平台更新的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。

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 或 NFS）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: 确保用于单个组件 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 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Update and Rollback（更新和回滚）**。
   此时将显示 **Firmware Update**（固件更新）页面。
2. 在 **Update**（更新）选项卡中，选择 **Local**（本地）作为 **File Location**（文件位置）。
3. 单击 **Browse**（浏览），为所需组件选择固件映像文件，然后单击 **Upload**（上载）。
4. 上载完成后，将在 **Update Details**（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，**Contents**（内容）列将显示一个 ⊞ 图标，其位于该固件映像文件名的旁边。展开该名称可查看**设备名**、**当前固件版本**和**可用固件版本**的信息。
5. 选择要更新的固件文件并执行以下任一操作：
   - 对于不需要主机系统重新引导的固件映像，请单击 **Install**（安装）。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 **Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）。
   - 要取消固件更新，请单击 **Cancel**（取消）。

   在您单击 **Install**（安装）、**Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）时，将显示消息 `Updating Job Queue`（正在更新作业队列）。
6. 单击 **Job Queue**（作业队列）显示 **Job Queue**（作业队列）页面，在此可以查看和管理分阶段的固件更新，或单击 **OK**（确定）刷新当前页面并查看固件更新的状态。

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

相关概念

更新设备固件
查看和管理分阶段更新
下载设备固件

使用存储库更新固件

您可以通过指定网络共享（其中包含有效的 DUP 存储库以及用于描述可用 DUP 的目录）执行多个固件更新。当 iDRAC 连接到网络共享位置并检查可用更新时，将生成一个比较报告，其中列出了所有可用更新。然后，您可以选择并向系统应用所需的包含在存储库中的更新。

在使用存储库执行更新之前，请确保：

- 在网络共享（CIFS 或 NFS）中创建存储库（其中包含基于 Windows 的更新软件包 (DUP) 以及目录文件）。如果不存在用户定义的目录文件，则默认情况下将使用 Catalog.xml。
- 已启用 Lifecycle Controller。
- 您拥有服务器控制权限以更新除 iDRAC 外的设备的固件。

要使用存储库更新设备固件，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **更新和回滚**。
   此时将显示 **Firmware Update**（固件更新）页面。
2. 在 **Update**（更新）选项卡中，选择 **Network Share**（网络共享）作为 **File Location**（文件位置）。
3. 在 **Catalog Location**（目录位置）部分中，输入网络设置的详细信息。
   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）。
4. 单击 **Check for Update**（检查更新）。
   将在 **Update Details**（更新详细信息）部分中将显示一个比较报告，其中列出了当前固件版本和存储库中的可用固件版本。

   注: 在此比较报告中不包含存储库中不适用于系统或已安装硬件的任何更新，或不受支持的任何更新。
5. 选择所需更新并执行以下操作之一：
   - 对于不需要主机系统重新引导的固件映像，请单击 **Install**（安装）。例如，.d7 固件文件。
   - 对于需要主机系统重新引导的固件映像，请单击 **Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）。
   - 要取消固件更新，请单击 **Cancel**（取消）。

   在您单击 **Install**（安装）、**Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）时，将显示消息 `Updating Job Queue`（正在更新作业队列）。
6. 单击 **Job Queue**（作业队列）显示 **Job Queue**（作业队列）页面，在此可以查看和管理分阶段的固件更新，或单击 **OK**（确定）刷新当前页面并查看固件更新的状态。

相关概念

更新设备固件
查看和管理分阶段更新
下载设备固件
计划自动固件更新

使用 FTP 更新固件

您可以直接从 iDRAC 连接到 Dell FTP 站点或任何其他 FTP 站点以执行固件更新。可使用 FTP 站点上提供的基于 Windows 的更新软件包 (DUP) 和目录文件，而不必创建自定义存储库。
在使用存储库执行更新之前，请确保：

- 已启用 Lifecycle Controller。
- 您拥有服务器控制权限以更新除 iDRAC 外的设备的固件。

要使用 FTP 更新固件，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **更新和回滚**。

此时将显示 **Firmware Update**（固件更新）页面。

2. 在 **Update**（更新）选项卡中，选择 **FTP** 作为 **File Location**（文件位置）。
3. 在 **FTP Server Settings**（FTP 服务器设置）部分中，输入 FTP 详细信息。

   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击 **Check for Update**（检查更新）。
5. 上载完成后，**Update Details**（更新详细信息）部分将显示一个比较报告，其中显示了当前固件版本和存储库中的可用固件版本。

   注: 在此比较报告中不包含存储库中不适用于系统或已安装硬件的任何更新，或不受支持的任何更新。
6. 选择所需更新并执行以下操作之一：
   - 对于不需要主机系统重新引导的固件映像，请单击 **Install**（安装）。例如，.d7 固件文件。
   - 对于需要主机系统重新引导的固件映像，请单击 **Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）。
   - 要取消固件更新，请单击 **Cancel**（取消）。

   在您单击 **Install**（安装）、**Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）时，将显示消息 `Updating Job Queue`（正在更新作业队列）。
7. 单击 **Job Queue**（作业队列）显示 **Job Queue**（作业队列）页面，在此可以查看和管理分阶段的固件更新，或单击 **OK**（确定）刷新当前页面并查看固件更新的状态。

相关概念

更新设备固件
查看和管理分阶段更新
下载设备固件
计划自动固件更新

使用 TFTP 更新设备固件

您可以直接从 iDRAC 连接到 TFTP 站点以执行固件更新。可使用 TFTP 站点上提供的基于 Windows 的更新软件包 (DUP) 和目录文件，而不必创建自定义存储库。

执行更新前，请确保：

- 已启用 Lifecycle Controller。
- 您拥有服务器控制权限以更新除 iDRAC 外的设备的固件。

要使用 TFTP 更新设备固件：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **更新和回滚**。

   此时将显示 **Firmware Update**（固件更新）页面。
2. 在**更新**选项卡中，选择 **TFTP** 作为**文件位置**。
3. 在 **TFTP 服务器设置**部分中，输入 TFTP 详细信息。

   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击 **Check for Update**（检查更新）。
5. 上载完成后，**Update Details**（更新详细信息）部分将显示一个比较报告，其中显示了当前固件版本和存储库中的可用固件版本。

   注: 在此比较报告中不包含存储库中不适用于系统或已安装硬件的任何更新，或不受支持的任何更新。
6. 选择所需更新并执行以下操作之一：

- 对于不需要主机系统重新引导的固件映像，请单击 **Install**（安装）。例如，.d7 固件文件。
- 对于需要主机系统重新引导的固件映像，请单击 **Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）。
- 要取消固件更新，请单击 **Cancel**（取消）。

在您单击 **Install**（安装）、**Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）时，将显示消息 `Updating Job Queue`（正在更新作业队列）。

7. 单击 **Job Queue**（作业队列）显示 **Job Queue**（作业队列）页面，在此可以查看和管理分阶段的固件更新，或单击 **OK**（确定）刷新当前页面并查看固件更新的状态。

相关概念

下载设备固件
更新设备固件
查看和管理分阶段更新
下载设备固件
计划自动固件更新

使用 HTTP 更新设备固件

您可以直接从 iDRAC 连接到 HTTP 站点以执行固件更新。可使用 HTTP 站点上提供的基于 Windows 的更新软件包 (DUP) 和目录文件，而不必创建自定义存储库。
在使用存储库执行更新之前，请确保：

- 已启用 Lifecycle Controller。
- 您拥有服务器控制权限以更新除 iDRAC 外的设备的固件。

要使用 HTTP 更新设备固件：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **更新和回滚**。
   此时将显示 **Firmware Update**（固件更新）页面。
2. 在**更新**选项卡中，选择 **HTTP** 作为**文件位置**。
3. 在 **HTTP 服务器设置**部分中，输入 HTTP 详细信息。
   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
4. 单击 **Check for Update**（检查更新）。
5. 上载完成后，**Update Details**（更新详细信息）部分将显示一个比较报告，其中显示了当前固件版本和存储库中的可用固件版本。

   注: 在此比较报告中不包含存储库中不适用于系统或已安装硬件的任何更新，或不受支持的任何更新。
6. 选择所需更新并执行以下操作之一：
   - 对于不需要主机系统重新引导的固件映像，请单击 **Install**（安装）。例如，.d7 固件文件。
   - 对于需要主机系统重新引导的固件映像，请单击 **Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）。
   - 要取消固件更新，请单击 **Cancel**（取消）。

   在您单击 **Install**（安装）、**Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）时，将显示消息 `Updating Job Queue`（正在更新作业队列）。
7. 单击 **Job Queue**（作业队列）显示 **Job Queue**（作业队列）页面，在此可以查看和管理分阶段的固件更新，或单击 **OK**（确定）刷新当前页面并查看固件更新的状态。

输入完成此任务后用户应执行的任务（可选）。

相关概念

[下载设备固件](#)
[更新设备固件](#)
[查看和管理分阶段更新](#)
[下载设备固件](#)
[计划自动固件更新](#)

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 **dell.com/idracmanuals** 上提供的 *RACADM Reference Guide for iDRAC and CMC*（适用于 iDRAC 和 CMC 的 RACADM 参考指南）。

示例：

- 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
  ```

计划自动固件更新

您可以创建定期执行的重复计划以使 iDRAC 检查新的固件更新。DRAC 将在计划的日期和时间连接到指定的网络共享（CIFS 或 NFS）或 FTP，检查新的更新并应用和暂存所有适用的更新。远程服务器上的日志文件中包含关于服务器访问权限和已暂存的固件更新的信息。

只有在拥有 iDRAC Enterprise 许可证的情况下才可使用自动更新。

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 地址计划自动固件更新。

相关概念

[下载设备固件](#)
[更新设备固件](#)
[查看和管理分阶段更新](#)

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: 如果已计划了自动更新作业，请勿创建下一个计划自动更新作业。新创建的作业会覆盖当前计划的作业。

1. 在 iDRAC Web 界面中，转至**概览 → iDRAC 设置 → 更新和回滚**。
   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：
   - **网络 —** 使用来自网络共享（CIFS 或 NFS）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 FTP 站点中的目录文件。输入 FTP 站点详细信息。
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 **Schedule Update**（计划更新）。

   将在作业队列中创建下一个计划的作业。重复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 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 **Server**（服务器） → **Overview**（概述） → **<server name>**。
   此时将显示**服务器状态**页面。
3. 单击 **Launch iDRAC**（启动 iDRAC）Web 界面并执行 **iDRAC Firmware Update**（iDRAC 固件更新）。

相关概念

更新设备固件
下载设备固件
使用 iDRAC Web 界面更新固件

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 公用程序更新 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`

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

要使用远程 RACADM 进行更新：

1. 将固件映像下载到 TFTP 或 FTP 服务器，例如：C:\downloads\firmimg.d7
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>`

     其中 *path* 是 TFTP 服务器上存储 firmimg.d7 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 <ftpsrever IP> <ftpserver username> <ftpserver password> –d <path>`

     其中 *path* 是 FTP 服务器上存储 firmimg.d7 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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（ iDRAC8 RACADM 命令行界面参考指南）中的 **fwupdate** 命令。

使用 Lifecycle Controller 远程服务更新固件

有关使用 Lifecycle Controller–Remote Services 更新固件的信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller Remote Services Quick Start Guide*（Lifecycle Controller Remote Services 快速入门指南）。

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. 导航至**机箱概览** → **设置** → **常规** 。
3. 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**。

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. 在 iDRAC Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Update and Rollback（更新和回滚）** → **Settings（设置）**。

   此时将显示 **Chassis Management Controller Firmware Update Settings**（Chassis Management Controller 固件更新设置）页面。
2. 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。
3. 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

您可以查看并删除计划的作业，包括配置和更新作业。这是一个许可功能。在下次重新引导期间可以删除排队的所有作业。

相关任务

[更新设备固件]

使用 iDRAC Web 界面查看和管理分阶段更新

要使用 iDRAC Web 界面查看计划作业的列表，请转至**概览** → **服务器** → **作业队列**。**作业队列**页面将会显示 Lifecycle Controller 作业队列中作业的状态。有关所显示字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

要删除作业，请选择相应作业并单击 **Delete**（删除）。系统会刷新页面并且从 Lifecycle Controller 作业队列中移除所选作业。您可以在下次重新引导期间删除所有排队运行的作业。您不能删除活动作业，即状态为 *Running*（正在运行）或 *Downloading*（正在下载）的作业。

您必须具有 Server Control（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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

回滚设备固件

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

在具有单一 iDRAC 和 Lifecycle Controller 固件的 Dell 第 13 代 PowerEdge 服务器上，回滚 iDRAC 固件时也会回滚 Lifecycle Controller 固件。但是，在具有固件版本 2.*xx.xx.xx* 的第 12 代 PowerEdge 服务器上，将 iDRAC 回滚到 1.*xx.xx* 等之前的版本时，不会回滚 Lifecycle Controller 固件版本。建议在回滚 iDRAC 后将 Lifecycle Controller 回滚到之前的版本。

注: 在具有固件版本 2.10.10.10 的第 12 代 PowerEdge 服务器上，在不回滚 iDRAC 的情况下，不能将 Lifecycle Controller 回滚到 1.*xx.xx*。必须先将 iDRAC 回滚到 1.*xx.xx* 版本，然后才能回滚 Lifecycle Controller。

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: 不能对诊断程序、驱动程序包和 CPLD 执行固件回滚。

注: 第 13 代 PowerEdge 系统不支持固件版本 1.*xx*.*xx*。

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
- RACADM CLI（iDRAC 和 CMC）
- Lifecycle Controller
- Lifecycle Controller 远程服务

相关任务

使用 iDRAC Web 界面回滚固件
使用 CMC Web 界面回滚固件
使用 RACADM 回滚固件
使用 Lifecycle Controller 回滚固件
使用 Lifecycle Controller 远程服务回滚固件

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**概览** → **iDRAC 设置** → **更新和回滚** → **回滚**。
   Rollback（回滚）页面将显示您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以及可用的固件回滚版本。
2. 选择一个或多个要为其回滚固件的设备。
3. 根据所选设备，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）。如果仅选择了 iDRAC，则单击 **Install**（安装）。
   在您单击 **Install and Reboot**（安装并重新引导）或 **Install Next Reboot**（下次重新引导时安装）时，将显示消息“Updating Job Queue（正在更新作业队列）”。
4. 单击 **Job Queue**（作业队列）。
   将显示 **Job Queue**（作业队列）页面，您可在其中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。
   - 如果将 iDRAC 配置重设为默认值，将会把 iDRAC IP 地址重设为 192.168.0.120。您可以使用此 IP 访问 iDRAC，或者使用本地 RACADM 或 F2（远程 RACADM 需要网络访问权限）重新配置 iDRAC 地址。

   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 **Server Overview（服务器概览） → <服务器名称>**。
   随即会显示 **Server Status**（服务器状态）页面。
3. 单击**启动 iDRAC** 并执行设备固件回滚，如使用 iDRAC Web 界面回滚固件一节中所述。

使用 RACADM 回滚固件

要使用 racadm 回滚设备固件，请执行以下操作：

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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

使用 Lifecycle Controller 回滚固件

有关信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。

使用 Lifecycle Controller 远程服务回滚固件

有关信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller Remote Services Quick Start Guide*（Lifecycle Controller Remote Services 快速入门指南）。

恢复 iDRAC

iDRAC 支持两个操作系统映像，以确保 iDRAC 可引导。如果出现无法预见的灾难性错误，您将丢失两个引导路径：

- 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 指示灯会以大约 1/2 秒的频率闪烁。（LED 指示灯位于机架式和塔式服务器的背面，但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.d7** 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.d7，重新编程 iDRAC，然后重新引导 iDRAC。

使用 TFTP 服务器

您可以使用简单文件传输协议 (TFTP) 服务器来升级或降级 iDRAC 固件或安装证书。该协议在 SM-CLP 和 RACADM 命令行界面中用于为 iDRAC 收发文件。TFTP 服务器必须使用 iDRAC IP 地址或 DNS 名称进行访问。

注: 如果使用 iDRAC Web 界面来传输证书和更新固件，则无需 TFTP 服务器。

在 Windows 或 Linux 操作系统上，您可以使用 `netstat -a` 命令来查看 TFTP 服务器是否正在运行。TFTP 的默认端口为 69。如果 TFTP 服务器未运行，请执行以下操作之一：

- 在网络上查找其他运行 TFTP 服务的计算机。
- 在操作系统上安装 TFTP 服务器。

备份服务器配置文件

您可以备份系统配置，包括已在各组件（例如 BIOS、RAID、NIC、iDRAC、Lifecycle Controller 和网络子卡 (NDC)）上安装的固件映像，以及这些组件的配置设置。备份操作还包括硬盘配置数据、主板和已更换部件。备份过程将创建一个文件。可以将该文件保存到 vFlash SD 卡或网络共享（CIFS 或 NFS）。

还可以启用和计划基于某一天、周或月的固件和服务器配置的定期备份。

备份功能已获得许可，iDRAC Enterprise 许可证提供此功能。

注: 在第 13 代服务器中，此功能将自动启用。

在执行备份操作之前，请确保：

- 启用 Collect System Inventory on Reboot (CSIOR)（重新引导时收集系统资源清册 (CSIOR)）选项。如果 CSIOR 处于禁用状态，并且您启动备份操作，则会显示以下消息：

  `System Inventory with iDRAC may be stale,start CSIOR for updated inventory`
- 要在 vFlash SD 卡上执行备份，请执行以下操作：
  - 插入、启用和初始化 Dell 支持的 vFlash SD 卡。
  - vFlash SD 卡具有足够的空间存储备份文件。

备份文件包含已加密的用户敏感数据、配置信息，以及可用于导入服务器配置文件操作的固件映像。

备份事件已记录在 Lifecycle 日志中。

相关概念

计划自动备份服务器配置文件
导入服务器配置文件

使用 iDRAC Web 界面备份服务器配置文件

要使用 iDRAC Web 界面备份服务器配置文件：

1. 转至 **概览** → **iDRAC 设置** → **服务器配置文件**。
   此时将显示 **Backup and Export Server Profile**（备份和导出服务器配置文件）页面。
2. 选择以下选项之一保存备份文件映像：
   - **Network（网络）**，以在 CIFS 或 NFS 共享上保存备份文件映像。
   - **vFlash**，以在 vFlash 卡上保存备份文件映像。
3. 输入备份文件名和加密密码（可选）。
4. 如果选择 **Network**（网络）作为文件位置，请输入网络设置。

   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）。
5. 单击 **立即备份**。
   备份操作启动，您可以在 **Job Queue**（作业队列）页面上查看状态。在成功操作后，即会在指定的位置创建备份文件。

使用 RACADM 备份服务器配置文件

要使用 RACADM 备份服务器配置文件，请使用 systemconfig backup 子命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

计划自动备份服务器配置文件

可以启用和计划基于某一天、周或月执行的固件和服务器配置定期备份。

在计划服务器配置文件自动备份之前，请确保：

- 已启用 Lifecycle Controller 和 Collect System Inventory on Reboot (CSIOR) 选项。
- 已启用网络时间协议 (NTP)，使得时间偏移不会影响已计划作业的实际运行时间以及下一个计划作业的创建时间。
- 要在 vFlash SD 卡上执行备份，请执行以下操作：
  – 插入、启用和初始化 Dell 支持的 vFlash SD 卡。
  – vFlash SD 卡具有足够的空间存储备份文件。

注: 不支持使用 IPv6 地址计划服务器配置文件自动备份。

使用 Web 界面计划服务器配置文件自动备份

要计划服务器配置文件自动备份，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **服务器配置文件**。
   此时将显示 **Backup and Export Server Profile**（备份和导出服务器配置文件）页面。
2. 单击 **Automatic Backup**（自动备份）选项卡。
3. 选择 **Enable Automatic Backup**（启用自动备份）选项。

4. 选择以下选项之一保存备份文件映像：
   - **Network**（网络），以在 CIFS 或 NFS 共享上保存备份文件映像。
   - **vFlash**，以在 vFlash 卡上保存备份文件映像。
5. 输入备份文件名和加密密码（可选）。
6. 如果选择 **Network**（网络）作为文件位置，请输入网络设置。

   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）
7. 在 **Backup Window Schedule**（备份窗口计划）部分中，指定备份操作的开始时间和频率（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 **Schedule Backup**（计划备份）。

   在作业队列中，将为重复作业显示下一个计划备份操作的起始日期和时间。在重复作业的第一个实例启动五分钟后，将创建下一个时间段的作业。将在计划的日期和时间执行服务器配置文件备份操作。

使用 RACADM 计划服务器配置文件自动备份

要启用自动备份，请使用以下命令：

```
racadm set lifecyclecontroller.lcattributes.autobackup Enabled
```

要计划服务器配置文件备份，请使用以下命令：

```
racadm systemconfig backup –f <filename> <target> [-n <passphrase>] -time
<hh:mm> -dom <1-28,L,’*’> -dow<*,Sun-Sat> -wom <1-4, L,’*’> -rp <1-366>-mb
<Max Backups>
```

要查看当前的备份计划，请使用以下命令：

```
racadm systemconfig getbackupscheduler
```

要禁用自动备份功能，请使用以下命令：

```
racadm set LifeCycleController.lcattributes.autobackup Disabled
```

要清除备份计划，请使用以下命令：

```
racadm systemconfig clearbackupscheduler
```

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 iDRAC8 RACADM Command Line Interface Reference Guide（iDRAC8 RACADM 命令行界面参考指南）。

导入服务器配置文件

可使用备份映像文件导入（还原）同一台服务器的配置和固件而无需重新引导服务器。

在第 13 代服务器中，此功能自动执行整个主板更换过程。在更换主板并重新安装内存、HDD 和其他硬件后，将显示一个特殊的引导屏幕，提供一个选项，用于还原所有保存的配置、服务标签和许可设置以及诊断程序。新主板上的 iDRAC 会读取此信息并还原保存的配置。

导入功能尚未授权。

注: 对于还原操作，系统服务标签和备份文件中的服务标签必须相同。还原操作应用于与在备份文件中捕获的相同且位于同一位置（例如相同插槽）的所有系统组件。如果组件不同或位于不同的位置，则不会对其进行修改并且将还原故障记录到 Lifecycle 日志中。

执行导入操作之前，确保已启用了 Lifecycle Controller。如果在禁用 Lifecycle Controller 时启动导入操作，将显示以下消息：

`Lifecycle Controller is not enabled, cannot create Configuration job.`
`（Lifecycle Controller 未启用，无法创建配置作业。）`

当导入操作在进行中时，如果您再次启动导入操作，将显示以下错误消息：

`Restore is already running（还原已在运行）`

导入事件已记录在 Lifecycle 日志中。

相关任务

还原操作顺序

使用 iDRAC Web 界面导入服务器配置文件

要使用 iDRAC Web 界面导入服务器配置文件：

1. 转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Server Profile（服务器配置文件）** → **Import（导入）**。

   将显示 **Import Server Profile**（导入服务器配置文件）页面。
2. 选择以下任一项指定备份文件的位置：
   - **Network（网络）**
   - **vFlash**
3. 输入备份文件名和解密密码（可选）。
4. 如果选择 **Network**（网络）作为文件位置，请输入网络设置。

   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）。
5. 为 **Virtual disks configuration and hard disk data**（虚拟磁盘配置和硬盘数据）选择以下其中一项：
   - **Preserve**（保留）— 保留 RAID 级别、虚拟磁盘、控制器属性和系统中的硬盘数据，并利用备份映像文件将系统还原到先前的已知状态。
   - **Delete and Replace**（删除并替换）— 将 RAID 级别、虚拟磁盘、控制器属性和系统中的硬盘配置信息删除，并用备份映像文件中的数据替换。
6. 单击**导入**。

   服务器配置文件导入操作已启动。

使用 RACADM 导入服务器配置文件

要使用 RACADM 导入服务器配置文件，请使用 **systemconfig restore** 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

还原操作顺序

还原操作顺序为：

1. 主机系统关闭。
2. 备份文件信息用于还原 Lifecycle Controller。
3. 主机系统打开。
4. 设备的固件和配置还原过程完成。
5. 主机系统关闭。
6. iDRAC 固件和配置还原过程完成。
7. iDRAC 重新启动。
8. 还原的主机系统打开以恢复正常工作。

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。您还可以使用 Dell Remote Access Configuration Tool (DRACT) 来查找 iDRAC、更新固件以及设置 Active Directory。有关更多信息，请参阅相应的用户指南。

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，请参阅管理许可证。

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 User's Guide*（Lifecycle Controller Remote Services 用户指南））
- IPMITool（请参阅 *Baseboard Management Controller Management Utilities User's Guide*（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 Serial Over LAN（IPMI LAN 上串行）
   - LAN 上 IPMI
   - SSH 或 Telnet 客户端
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。

相关概念

登录 iDRAC
修改网络设置
配置服务
配置前面板显示屏
设置受管系统位置
配置时区和 NTP
设置 iDRAC 通信
配置用户帐户和权限
监测和管理电源
启用上次崩溃屏幕
配置并使用虚拟控制台
管理虚拟介质
管理 vFlash SD 卡
设置第一引导设备
启用或禁用 OS 到 iDRAC 直通

相关任务

配置 iDRAC 以发送警报

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，转到**概览 → iDRAC 设置 → 属性**，查看与 iDRAC 相关的以下信息。有关各属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

- 硬件和固件版本
- 最新固件更新
- RAC 时间
- IPMI 版本
- 用户界面标题栏信息
- 网络设置
- IPv4 设置
- IPv6 设置

使用 RACADM 查看 iDRAC 信息

要使用 RACADM 查看 iDRAC 信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）中的 `getsysinfo` 或 `get` 子命令详细信息。

修改网络设置

使用 iDRAC 设置公用程序配置 iDRAC 网络设置后，您还可以通过 iDRAC Web 界面、RACADM、Lifecycle Controller、Dell Deployment Toolkit 和 Server Administrator（引导至操作系统后）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: 更改网络设置可能会使指向 iDRAC 的当前网络连接中断。

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**概览** → **iDRAC 设置** → **网络**。
   随即会显示 **Network**（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 **Apply**（应用）。
   如果您选择 **Network Settings**（网络设置）下的 **Auto Dedicated NIC**（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。可以使用 RACADM 或 WS-MAN 配置此超时值。

   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用本地 RACADM 修改网络设置

要生成可用网络属性列表，请键入以下命令：

注: 您可以将 getconfig 和 config 命令或者 get 和 set 命令与 RACADM 对象配合使用。

- 使用 getconfig 命令：`racadm getconfig -g cfgLanNetworking`
- 使用 get 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 **cfgNicUseDhcp** 或 DHCPEnable 并启用此功能：

- 使用 config 命令：`racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1`
- 使用 set 命令：`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：

- 使用 config 命令：

  ```
  racadm config -g cfgLanNetworking -o cfgNicEnable 1 racadm config -g
  cfgLanNetworking -o cfgNicIpAddress 192.168.0.120 racadm config -g
  cfgLanNetworking -o cfgNicNetmask 255.255.255.0 racadm config -g
  cfgLanNetworking -o cfgNicGateway 192.168.0.120 racadm config -g
  cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g cfgLanNetworking -o
  cfgDNSServersFromDHCP 0 racadm config -g cfgLanNetworking -o cfgDNSServer1
  192.168.0.5 racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
  racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1 racadm config -g
  ```

```
cfgLanNetworking -o cfgDNSRacName RAC-EK00002 racadm config -g
cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0 racadm config -g
cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

- 使用 set 命令：

```
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 cfgNicEnable 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。如果您两次未成功登录，则只能在 30 秒后才能重新登录。如果登录失败次数超过两次，则只能在 60 秒后重新登录。

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: 如果来自客户端 IP 地址的登录尝试被阻止，少数 SSH 客户端会显示以下信息：`ssh exchange identification: Connection closed by remote host`。

注: 如果您使用 Dell Deployment Toolkit (DTK)，有关权限的信息请参阅*《Dell Deployment Toolkit 用户指南》*。

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**概览** → **iDRAC 设置** → **网络** → **网络**。
   随即会显示 **Network**（网络）页面。
2. 单击 **Advanced Settings**（高级设置）。
   随即会显示 **Network Security（网络安全性）**页面。
3. 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。

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。

要配置 IP 筛选，请使用以下 RACADM 对象：

- 使用 config 命令：
  – cfgRacTuneIpRangeEnable

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask
- 将 set 命令与 iDRAC.IPBlocking 组中的对象配合使用：
  - RangeEnable
  - RangeAddr
  - RangeMask

cfgRacTuneIpRangeMask 或 RangeMask 属性对接入 IP 地址和 cfgRacTuneIpRangeAddr 或 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。

如果以下表达式等于零，登录将会继续：

- 使用传统语法：`cfgRacTuneIpRangeMask & (<incoming-IP-address> ^ cfgRacTuneIpRangeAddr)`
- 使用新语法：`RangeMask & (<incoming-IP-address> ^ RangeAddr)`

其中 & 是数量的按位“与”，而 ^ 是按位“异或”。

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：
  - 使用 config 命令：

    ```
    racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1 racadm config -
    g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57 racadm config -g
    cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
    ```
  - 使用 set 命令：

    ```
    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：
  - 使用 set 命令：

    ```
    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 **dell.com/idracmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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。
- Web Server - 启用对 iDRAC Web 界面的访问。如果您禁用该选项，请使用本地 RACADM 重新启用 Web Server，因为禁用 Web Server 会同时禁用远程 RACADM。
- SSH - 通过固件 RACADM 访问 iDRAC。

- Telnet - 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 — 启用上次系统崩溃屏幕。
- VNC 服务器 - 启用支持或不支持 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**概览** → **iDRAC 设置** → **网络** → **服务**。
   将显示 **Services**（**服务**）页面。
2. 指定所需信息，然后单击 **Apply**（**应用**）。
   有关各设置的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 配置服务

要使用 RACADM 启用和配置各服务，请执行以下操作：

- 将以下对象与 config 命令配合使用：
  - cfgRacTuneLocalConfigDisable
  - cfgRacTuneCtrlEConfigDisable
  - cfgSerialSshEnable
  - cfgRacTuneSshPort
  - cfgSsnMgtSshIdleTimeout
  - cfgSerialTelnetEnable
  - cfgRacTuneTelnetPort
  - cfgSsnMgtTelnetIdleTimeout
  - cfgRacTuneWebserverEnable
  - cfgSsnMgtWebserverTimeout
  - cfgRacTuneHttpPort
  - cfgRacTuneHttpsPort
  - cfgRacTuneRemoteRacadmEnable
  - cfgSsnMgtRacadmTimeout
  - cfgOobSnmpAgentEnable
  - cfgOobSnmpAgentCommunity
- 将以下对象组中的对象与 set 命令配合使用：
  - iDRAC.LocalSecurity
  - iDRAC.LocalSecurity
  - iDRAC.SSH
  - iDRAC.Webserver
  - iDRAC.Telnet
  - iDRAC.Racadm

– iDRAC.SNMP

有关这些对象的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

启用或禁用 HTTPs 重定向

如果因为默认 iDRAC 证书中的证书警告问题，或作为一项用于调试目的的临时设置，不需要从 HTTP 自动重定向到 HTTPs，您可以对 iDRAC 进行配置，以禁止从 http 端口（默认值为 80）重定向到 https 端口（默认为 443）。默认情况下，该选项已启用。您必须注销然后登录 iDRAC 以使此设置生效。如果禁用此功能，会显示警告消息。

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
```

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 功能是已获得许可的功能，在 iDRAC Enterprise 许可证中提供。

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。

在任何时间只能有一个 VNC 客户端会话处于活动状态。

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:

- 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。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**概览** → **iDRAC 设置** → **网络** → **服务**。

   将显示 **Services**（**服务**）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，请对 `VNCserver` 对象使用 `set` 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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

一般来说，所有兼容 Remote Frame Buffer (RFB) 的 VNC 查看器均连接到 VNC 服务器（使用 iDRAC IP 地址和为 VNC 服务器配置的端口号）。如果在配置 iDRAC 中的 VNC 服务器设置时禁用了 SSL 加密选项，则连接到 VNC 查看器可执行以下操作：

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 并且 VNC 端口号为 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。

相关概念

[配置 LCD 设置]
[配置系统 ID LED 设置]

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**概览** → **硬件** → **前面板**。
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）
   - Asset Tag（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 前面板显示屏，请使用 System.LCD 组中的对象。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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**概览 → 硬件 → 前面板**。将显示**前面板**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，请使用 setled 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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. 转至 **Overview**（概述） → **iDRAC Settings**（**iDRAC** 设置） → **Properties**（属性） → **Settings**（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

要使用 RACADM 配置时区和 NTP，请将 iDRAC.Time 和 iDRAC.NTPConfigGroup 组中的对象与 set 命令配合使用。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

设置第一引导设备

您可以设置第一引导设备，使其仅用于下次引导或用于所有后续重新引导。根据此选择，您可以为系统设置第一引导设备。系统在下次和后续重新引导时会从选定设备引导，并保持作为 BIOS 引导顺序中的第一引导设备，直到从 iDRAC Web 界面或从 BIOS 引导顺序再次进行更改为止。您可以将第一引导设备设置为以下选项之一：

- 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
- vFlash
- Lifecycle Controller
- BIOS 引导管理器

注:

- BIOS 设置 (F2)、Lifecycle Controller (F10)、BIOS Boot Manager (F11) 仅支持启用一次性引导。
- 虚拟控制台不支持永久引导配置。其始终仅会引导一次。
- 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 **Overview**（概览） → **Server**（服务器） → **Setup**（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. 要仅在下次引导时从选定设备引导，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，请使用 cfgServerFirstBootDevice 对象。
- 要启用为设备引导一次，请使用 cfgServerBootOnce 对象。

有关这些对象的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

使用虚拟控制台设置第一引导设备

在服务器通过其引导顺序运行之前，您可以在虚拟控制台查看器中查看服务器时选择要从中引导的设备。可以执行一次引导即引导至设置第一引导设备中列出的所有支持设备。

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。

启用上次崩溃屏幕：

1. 从 *Dell Systems Management Tools and Documentation* DVD 中，在受管系统上安装 Server Administrator。

   有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Dell OpenManage Server Administrator Installation Guide*（Dell OpenManage Server Administrator 安装指南）。

2. 在 **Windows** 启动和恢复窗口中，确保未选择自动重新引导选项。

   有关更多信息，请参阅 Windows 说明文件。

3. 使用 Server Administrator 可启用 **Auto Recovery**（自动恢复）定时器、将 Auto Recovery（自动恢复）操作设置为 **Reset**（重设）、**Power Off**（关机）或 **Power Cycle**（关机后开机），并以秒为单位设置定时器（60 - 480 之间的值）。

   有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Dell OpenManage Server Administrator Installation Guide*（Dell OpenManage Server Administrator 安装指南）。

4. 使用以下选项之一启用 **Auto Shutdown and Recovery (ASR)**（自动关闭和恢复 (ASR)）选项：

   - Server Administrator - 请参阅 **dell.com/support/manuals** 上提供的 *Dell OpenManage Server Administrator User's Guide*（Dell OpenManage Server Administrator 用户指南）。
   - 本地 RACADM - 使用以下命令：

     ```
     racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
     ```

5. 启用 **Automated System Recovery Agent**（自动系统恢复代理）。要实现这一点，请转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Services（服务）**，选择 **Enabled**（启用），然后单击 **Apply**（应用）。

启用或禁用 OS 到 iDRAC 直通

在包含网络子卡 (NDC) 或嵌入式主板内置局域网 (LOM) 设备的服务器中，可以启用 OS 到 iDRAC 直通功能，该功能通过共享 LOM（机架或塔式服务器）、专用 NIC（机架、塔式或刀片服务器），或通过 USB NIC 在 iDRAC 和主机操作系统之间提供高速双向带内通信。iDRAC Enterprise 许可证提供此功能。

如果通过专用 NIC 启用，则可以在主机操作系统中启动浏览器，然后访问 iDRAC Web 界面。刀片服务器的专用 NIC 通过 Chassis Management Controller 提供。

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 WS-MAN（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 或 WS-MAN 使用 XML 配置文件，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 Configure（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。
- 在专用模式下，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，请输入第一个 LOM 的 IP 地址。

在启用 OS 到 iDRAC 直通功能后，如果此功能不起作用：

- 检查是否正确连接了 iDRAC 的专用 NIC 电缆。
- 确保至少一个 LOM 处于活动状态。

相关参考资料

[支持 OS 到 iDRAC 直通功能的卡]
[支持 USB NIC 的操作系统]
[使用 Web 界面启用或禁用 OS 到 iDRAC 直通]
[使用 RACADM 启用或禁用 OS 到 iDRAC 直通]
[使用 iDRAC 设置公用程序启用或禁用 OS 到 iDRAC 直通]

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. 8: ：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 • 57810S DP bNDC KR • 57800S QP rNDC (10G BASE-T + 1G BASE-T) • 57800S QP rNDC (10G SFP+ + 1G BASE-T) • 57840 4x10G KR • 57840 rNDC
	Intel	• i540 QP rNDC (10G BASE-T + 1G BASE-T) • i350 QP rNDC 1G BASE-T • x520/i350 rNDC 1GB
	Qlogic	QMD8262 刀片式服务器 NDC

内置的 LOM 卡也支持 OS 到 iDRAC 直通功能。

以下各卡不支持 OS 到 iDRAC 直通功能：

- Intel 10 GB NDC。
- 包含两个控制器的 Intel rNDC – 10G 控制器不支持。
- Qlogic bNDC
- PCIe、夹层卡和网络接口卡。

支持 USB NIC 的操作系统

支持 USB NIC 的操作系统包括：

- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2（64 位）
- Windows Server 2012
- Windows Server 2012 R2
- SUSE Linux Enterprise Server 10 SP4（64 位）
- SUSE Linux Enterprise Server 11 SP2（64 位）
- SUSE Linux Enterprise Server 11 SP4
- RHEL 5.9（32 位和 64 位）
- RHEL 6.4
- RHEL 6.7
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U3
- vSphere v5.1 U1 ESXi
- vSphere v5.5 ESXi
- vSphere v5.5 U3

- vSphere 6.0
- vSphere 6.0 U1
- CentOS 6.5
- CentOS 7.0
- Ubuntu 14.04.1 LTS
- Ubuntu 12.04.04 LTS
- Debian 7.6 (Wheezy)
- Debian 8.0

在使用 Windows 2008 SP2 64 位操作系统的服务器上，不会自动发现（或启用）iDRAC 虚拟 CD USB 设备。您必须手动启用此设备。有关更多信息，请参阅 Microsoft 推荐的步骤以手动更新此设备的远程网络驱动程序接口规范 (RNDIS) 驱动程序。

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。

如果主机上的操作系统是 SUSE Linux Enterprise Server 11、CentOS 6.5、CentOS 7.0、Ubuntu 14.04.1 LTS 或 Ubuntu 12.04.4 LTS，则在 iDRAC 中启用 USB NIC 后，必须在主机操作系统上手动启用 DHCP 客户端。有关启用 DHCP 的信息，请参阅 SUSE Linux Enterprise Server、CentOS 和 Ubuntu 操作系统的文档。

对于 vSphere，必须安装 VIB 文件，然后再启用 USB NIC。

对于以下操作系统，如果安装 Avahi 和 nss-mdns 软件包，则可以从主机操作系统使用 **https://idrac.local** 启动 iDRAC。如果未安装这些软件包，请使用 **https://169.254.0.1** 启动 iDRAC。

Operating System（操作系统）	**防火墙状态**	**Avahi 软件包**	**nss-mdns 软件包**
RHEL 5.9 32 位	Disable（禁用）	作为独立软件包安装 (avahi-0.6.16-10.el5_6.i386.rpm)	作为独立软件包安装 (nss-mdns-0.10-4.el5.i386.rpm)
RHEL 6.4 64 位	Disable（禁用）	作为独立软件包安装 (avahi-0.6.25-12.el6.x86_64.rpm)	作为独立软件包安装 (nss-mdns-0.10-8.el6.x86_64.rpm)
SLES 11 SP3 64 位	Disable（禁用）	Avahi 软件包在操作系统 DVD 中提供	将在安装 Avahi 期间安装 nss-mdns

在主机系统上安装 RHEL 5.9 操作系统时、USB NIC 直通模式处于禁用状态。如果在完成安装后启用该选项，不会自动激活与 USB NIC 设备对应的网络接口。您可以执行以下任一操作以激活 USB NIC 设备：

- 使用 Network Manager 工具配置 USB NIC 接口。导航至 **System（系统）** → **Administrator（管理员）** → **Network** → **Devices（网络设备）** → **New** → **Ethernet Connection（新建以太网连接）**并选择 **Dell computer corp.iDRAC Virtual NIC USB Device（Dell 计算机 corp.iDRAC 虚拟 NIC USB 设备）**。单击 Activate（激活）图标可激活设备。有关更多信息，请参阅 RHEL 5.9 说明文件。
- 在 /etc/sysconfig/network-script/ 目录中创建对应接口的配置文件 ifcfg-ethX。添加基本条目 DEVICE、BOOTPROTO、HWADDR、ONBOOT。在 ifcfg-ethX 文件中添加 TYPE，然后使用命令 `service network restart` 重新启动网络服务。
- 重新引导系统。
- 关闭和打开系统电源。

在使用 RHEL 5.9 操作系统的系统上，如果已禁用 USB NIC，并且您关闭系统（或反之），则在打开系统时（并且已启用 USB NIC），USB NIC 设备不会自动激活。要使其处于活动状态，请检查 /etc/sysconfig/

network-script 目录中是否存在对应于 USB NIC 接口的 ifcfg-ethX.bak 文件。如果存在，则将其重命名为 ifcfg-ethX，然后使用 `ifup ethX` 命令。

相关任务

[安装 VIB 文件](#)

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 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **OS to iDRAC Pass-through（OS 到 iDRAC 直通）**。

   此时将显示 **OS to iDRAC Pass-through**（OS 到 iDRAC 直通）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。

   要禁用此功能，请选择 **Disabled**（禁用）。
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，请输入 USB NIC 的 IP 地址。

   默认值为 169.254.0.1。建议使用该默认 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。

   请不要输入 169.254.0.3 和 169.254.0.4 IP。这些 IP 是当使用 A/A 电缆时，为位于前面板上的 USB NIC 端口保留的。
5. 单击**应用**应用设置。
6. 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，请使用 iDRAC.OS-BMC 组中的对象。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。

   要禁用此功能，请选择 **Disabled**（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，请输入 USB NIC 的 IP 地址。

   默认值为 169.254.0.1。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。请不要输入 IP 169.254.0.3 和 169.254.0.4。使用 A/A 电缆时，这些 IP 地址保留用于用前面板上的 USB NIC 端口。
5. 依次单击 **Back**（上一步）、**Finish**（完成）和 **Yes**（是）。详细信息即得到保存。

获取证书

下表列出了基于登录类型的证书类型。

表. 9: 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。

登录类型	证书类型	获取方法
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 自带默认的自签名 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。

相关概念

SSL 服务器证书
生成新的证书签名请求

SSL 服务器证书

iDRAC 包含 Web 服务器，该服务器配置为使用行业标准的 SSL 安全协议通过网络来传输加密数据。SSL 建立在非对称加密技术基础之上，是一种广泛接受的加密技术，用于在客户端与服务器之间提供经过验证和加密的通信，防止遭到网络上的窃听。

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

该加密进程提供高级数据保护。iDRAC 采用 128 位 SSL 加密标准，这是北美普遍使用的最安全的 Internet 浏览器加密形式。

默认情况下，iDRAC Web 服务器包含 Dell 自签名的唯一 SSL 数字证书。您可以用知名证书颁发机构 (CA) 签名的证书替换默认的 SSL 证书。证书颁发机构是一个企业实体，在信息技术行业中满足可靠的筛选、标识和其他重要安全标准方面得到认可。CA 的示例包括 Thawte 和 VeriSign。要启动用于获取 CA 签名证书的过程，请使用 iDRAC Web 界面或 RACADM 界面生成包含您公司信息的证书签名请求 (CSR)。然后，将生成的 CSR 提交给 CA，例如 VeriSign 或 Thawte。CA 可以是根 CA 或中间 CA。在收到 CA 签名的 SSL 证书后，将其上载到 iDRAC。

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

您也可以上载自定义的签名证书来对 SSL 证书签名，而不是依赖此功能的默认签名证书。通过将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 都是可信的。如果在自定义 SSL 证书已在使用时上载自定义签名证书，则自定义 SSL 证书被禁用，而使用自定义签名证书签名的一次性自动生成的 SSL 证书。您可以下载自定义签名证书（没有私钥）。您还可以删除现有的自定义签名证书。在删除自定义签名证书后，iDRAC 重设并自动生成新的自签名 SSL 证书。如果重新生成自签名证书，则必须在 iDRAC 和管理站之间重建信任。自动生成的 SSL 证书是自签名证书，到期日为七年零一天，并且这一天的开始日期位于过去（适用于管理站和 iDRAC 的不同时区设置）。

在生成证书签名请求 (CSR) 时，iDRAC Web 服务器 SSL 证书支持将星号字符 (*) 作为公用名称最左侧的组成部分。例如，“*.qa.com”或“*.company.qa.com”。这称为通配符证书。如果在 iDRAC 外部生成通配符 CSR，

您将具有一个已签名的单通配符 SSL 证书，可上载该证书以用于多个 iDRAC，并且所有 iDRAC 将受支持的浏览器的信任。在使用受支持的浏览器（支持通配符证书）连接到 iDRAC Web 界面时，浏览器将会信任 iDRAC。在启动查看器时，查看器客户端将会信任 iDRAC。

相关概念

生成新的证书签名请求
上载服务器证书
查看服务器证书
上载自定义签名证书
下载自定义 SSL 证书签名证书
删除自定义 SSL 证书签名证书

生成新的证书签名请求

CSR 是向 SSL 服务器证书的证书认证机构 (CA) 发出的数字请求。SSL 服务器证书允许服务器的客户端信任服务器的身份，并与服务器协调加密会话。

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。

相关概念

SSL 服务器证书

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**概览** → **iDRAC 设置** → **网络** → **SSL**，选择**生成一个新证书签名请求 (CSR)**，然后单击**下一步**。

   将显示 **Generate a New Certificate Signing Request**（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 Online Help*（iDRAC 联机帮助）。
3. 单击 **Generate**（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，请将 cfgRacSecurity 组中的对象与 config 命令配合使用，或将 iDRAC.Security 组中的对象与 set 命令配合使用，然后使用 sslcsrgen 命令生成 CSR。有关更多信息，请参阅 **ddell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

上载服务器证书

生成 CSR 之后，您可以将已签名的 SSL 服务器证书上载到 iDRAC 固件。必须重设 iDRAC 才能应用证书。iDRAC 仅接受 X509、Base 64 编码的 Web 服务器证书。SHA-2 证书也受支持。

△ **小心: 重设期间，iDRAC 在几分钟内不可用。**

相关概念

SSL 服务器证书

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**概览** → **iDRAC 设置** → **网络** → **SSL**，选择**上载服务器证书**，然后单击**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，提示您立即重设 iDRAC 或在稍后执行。根据需要单击**重设 iDRAC** 或**稍后重设 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: 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。

使用 RACADM 上载服务器证书

要上载 SSL 服务器证书，请使用 sslcertupload 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC*（适用于 iDRAC 的 RACADM 命令行参考指南）。

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: 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。

相关概念

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**概览** → **iDRAC 设置** → **网络** → **SSL**。**SSL** 页面将会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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

上载自定义签名证书

您可以上载自定义签名证书以签署 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 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **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 **Upload Custom SSL Certificate Signing Certificate**（上载自定义 SSL 证书签名证书）并单击 **Next（下一步）**。
   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 **Browse**（浏览）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，提示您立即重设 iDRAC 或在稍后执行。根据需要单击**重设 iDRAC** 或**稍后重设 iDRAC**。
   重设 iDRAC 之后，将会应用新证书。重设期间，iDRAC 在几分钟内不可用。

   注: 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。

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 子命令，然后使用 racreset 命令重设 iDRAC。有关更多信息，请参阅 **www.dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **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 **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）。

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 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **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，提示您立即重设 iDRAC 或在稍后执行。根据需要单击**重设 iDRAC** 或**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 **www.dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

使用 RACADM 配置多个 iDRAC

您可以使用 RACADM 配置具有相同属性的一个或多个 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。文件名由用户指定。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出到其他 iDRAC。

您还可以借助 RACADM 使用系统配置 XML 文件配置多个 iDRAC。系统配置 XML 文件包含组件配置信息，并且通过将此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 **dell.com/support/manuals** 上或 Dell 技术中心提供的 *XML Configuration Workflow*（XML 配置工作流）白皮书。

要使用 .cfg 文件配置多个 iDRAC：

1. 使用以下命令查询包含所需配置的目标 iDRAC：`racadm getconfig -f myfile.cfg`。

该命令请求 iDRAC 配置并生成 **myfile.cfg** 文件。如果需要，您可以使用另一个名称配置该文件。

注: 使用 `getconfig -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 .cfg 文件不包含用户密码。

getconfig 命令显示组（通过组名称和索引指定）中的所有配置属性并按用户名显示用户的所有配置属性。

2. 使用简单文本编辑器修改配置文件（可选）。

   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. 通过以下命令使用新的配置文件修改目标 iDRAC：`racadm config -f myfile.cfg`

   这会将信息加载到其他 iDRAC。您可以使用 **config** 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`

创建 iDRAC 配置文件

配置文件 **.cfg** 可以：

- 创建
- 从 `racadm getconfig -f <filename>.cfg` 命令或 `racadm get -f <filename>.cfg` 命令获取
- 从 `racadm getconfig -f <filename>.cfg` 命令或 `racadm get -f <filename>.cfg` 获取，然后进行编辑

  有关 **getconfig** 和 **get** 命令的信息，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）。

.cfg 文件首先经过解析以验证存在有效的组和对象名称以及符合基本的语法规则。错误中将会标记检测到错误的行号，并显示一条消息解释该问题。整个文件都会经过解析以检查正确性，并且显示所有的错误。如果在 **.cfg** 文件中发现错误，则不会将写命令传送至 iDRAC。在使用该文件配置 iDRAC 之前，用户必须更正所有错误。请在 `config` 子命令中使用 `-c` 选项，该选项可以验证语法并且不会对 iDRAC 执行写操作。

请在创建 **.cfg** 文件时使用以下原则：

- 如果解析器遇到索引组，则会将组的索引用作锚点。对索引组中的对象执行的任何修改也会与索引值相关联。

  例如：

  – 如果您已经使用 **getconfig** 命令：

  ```
  [cfgUserAdmin] # cfgUserAdminIndex=11 cfgUserAdminUserName= #
  cfgUserAdminPassword=******** (Write-Only) cfgUserAdminEnable=0
  cfgUserAdminPrivilege=0x00000000 cfgUserAdminIpmiLanPrivilege=15
  cfgUserAdminIpmiSerialPrivilege=15 cfgUserAdminSolEnable=0
  ```

  – 如果您已经使用 **get** 命令：

  ```
  [idrac.users.16] Enable=Disabled IpmiLanPrivilege=15
  IpmiSerialPrivilege=15 !!Password=******** (Write-Only) Privilege=0x0
  SNMPv3AuthenticationType=SHA SNMPv3Enable=Disabled SNMPv3PrivacyType=AES
  SolEnable=Disabled UserName=
  ```

- 该索引是只读索引，并且不可修改。索引组的对象会绑定到索引并且列出在该索引下，该对象值的任何有效配置仅适用于这种特定的索引。

- 每个索引组都有一个预定义的索引集。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。
- 使用 `racresetcfg` 子命令将 iDRAC 重设为默认设置，然后运行 `racadm config -f <filename>.cfg` 或 `racadm set -f <filename>.cfg` 命令。确保 **.cfg** 文件包含所有所需的对象、用户、索引和其他参数。

小心: 使用 `racresetcfg` 子命令将数据库和 iDRAC NIC 设置重设为默认设置，并移除所有用户和用户配置。当根用户可用时，还会将其他用户设置重设为默认设置。

分析规则

- 以"#"开头的所有行都将被视为注释。注释行必须在第一列开始。"#"字符位于任何其他列都将被视为"#"字符。一些调制解调器参数在其字符串中可能包含 # 字符。不需要转义字符。您可能希望从 `racadm getconfig -f <filename> .cfg` 命令生成 **.cfg**，然后对不同的 iDRAC 执行 `racadm config -f <filename> .cfg` 命令，而不添加转义字符。例如：

```
#

# This is a comment

[cfgUserAdmin]

cfgUserAdminPageModemInitString=<Modem init # not a comment>
```

- 所有组条目必须包含在"[" 和"]" 字符对中。表示组名称的起始字符"[" *必须*在第一列开始。此组名称*必须*在该组中的任何对象之前指定。未包含相关组名称的对象会生成错误。配置数据按照 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）中的定义组织成组。下例显示了组名称、对象和对象的属性值。

```
[cfgLanNetworking] -{group name}

cfgNicIpAddress=143.154.133.121 {object name}
```

- 所有参数都指定为"对象=值"对，在对象、= 或值之间不留空格。

  值后的空格将被忽略。值字符串内的空格保持不变。"="右侧的任何字符都将原样保留（例如，第二个"="或"#"、"["、"]"等等）。这些字符是有效的调制解调器聊天脚本字符。

  请参阅上一个圆点符号后面的示例。

  `racadm getconfig -f <filename> .cfg` 命令将注释放置在索引对象前，允许用户查看包含的注释。

  要查看索引组的内容，请使用以下命令：

  `racadm getconfig -g <groupName> -i <index 1-16>`

- 对于索引组，对象定位器必须是"[ ]"对后的第一个对象。以下是当前索引组的示例：

```
[cfgUserAdmin]

cfgUserAdminIndex=11
```

  如果您键入 `racadm getconfig -f` *<myexample>*`.cfg`，命令将建立当前 iDRAC 配置的 **.cfg** 文件。此配置文件可用作示例并用作唯一的 **.cfg** 文件的起点。

修改 iDRAC IP 地址

在配置文件中修改 iDRAC IP 地址时，删除所有不必要的 <*变量*>=**值**条目。只有实际变量组标签带有 "[" 和 "]" 的保持不变，包括与 IP 地址更改有关的两个 <*变量*>=**值**条目。

例如：

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

此文件更新如下：

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

cfgNicGateway=10.35.9.1
```

命令 `racadm config -f myfile.cfg` 分析文件并通过行号标识任何错误。正确的文件会更新适当的条目。此外，您可以使用与上一示例相同的 `getconfig` 命令确认更新。

使用此文件下载企业范围内的更改或通过网络配置新系统。

注: “定位器”是一个内部术语，它不会在文件中使用。

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。要实现这一点：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **网络** → **服务**。
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，您无法使用 Server Administrator 或 IPMITool 执行 iDRAC 配置。但是，您可以使用 LAN 上 IPMI。

5

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 FlexAddress 信息。

相关概念

[查看受管系统运行状况和属性](#)
[查看系统资源清册](#)
[查看传感器信息](#)
[监测 CPU、内存和 I/O 模块的性能指标](#)
[检查系统的新鲜空气符合性](#)
[查看历史温度数据](#)
[资源清册和监测存储设备](#)
[资源清册和监测网络设备](#)
[资源清册和监测 FC HBA 设备](#)
[查看 FlexAddress 夹层卡光纤连接](#)
[查看或终止 iDRAC 会话](#)

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**概览 → 服务器 → 属性 → 摘要**。随即会显示**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 **System Summary**（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）。

查看系统资源清册

您可以查看关于受管系统上安装的硬件和固件组件的信息。要实现此操作，请在 iDRAC Web 界面中转至**概览 → 服务器 → 属性 → 系统资源清册**。有关显示的属性的信息，请参阅 *iDRAC Online Help*（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

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
- 电源设备
- NIC
- 光纤信道
- 背板
- Enclosure（机柜）
- PCIe SSD

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。

单击 **Export**（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 **Disabled**（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。

    注: 在 Dell 第 13 代 PowerEdge 服务器上，IDSDM 重建操作在后台执行，并且系统在重建过程中不会停止。您可以检查 Lifecycle Controller 日志，以查看重建操作的状态。在 Dell 第 12 代 PowerEdge 服务器上，在执行重建操作时，系统会停止。

  - 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。
- **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。

下表说明如何利用 iDRAC Web 界面和 RACADM 查看传感器信息。有关在 Web 界面上显示的属性的信息，请参阅相应页面的 *iDRAC Online Help*（iDRAC 联机帮助）。

表. 10: 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	**概览 → 硬件 → 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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。
风扇	**概览 → 硬件 → 风扇**	

查看传感器信息	使用 Web 界面	使用 RACADM
CPU	**概览 → 硬件 → CPU**	
内存	**概览 → 硬件 → 内存**	
侵入	**概览 → 服务器 → 侵入**	
电源设备	**概览 → 硬件 → 电源设备**	
可移除闪存介质	**概览 → 硬件 → 可移除闪存介质**	
温度	**概览 → 服务器 → 电源/散热 → 温度**	
电压	**概览 → 服务器 → 电源/散热 → 电压**	

监测 CPU、内存和 I/O 模块的性能指标

在 Dell 第 13 代 PowerEdge 服务器中，Intel ME 支持每秒计算使用 (CUPS) 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。由于此功能是通过 Intel ME 实现的，所以它独立于操作系统，不会占用 CPU 资源。Intel ME 具有一个系统 CUPS 传感器，可提供计算、内存和 I/O 资源的利用率值，作为 CUPS 指标。iDRAC 针对总体系统利用率来监测此 CUPS 指标，同时监测 CPU、内存和 I/O 利用率指标的瞬时值。

通过从 CPU 和芯片组所提供的一组专用计数器查询数据，可获取系统资源利用率信息。这些计数器称为资源监测计数器或 RMC。这些计数器由节点管理器汇总，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）。

由于 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** - 每个 CPU 核心具有独立的资源监测计数器 (RMC)，这些计数器将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** - 有单独的计数器 (RMC) 测量每个内存通道或内存控制器实例中发生的内存流量。这些计数器将聚合以测量系统中所有内存通道的累积内存流量。这是内存带宽消耗的量度，而不是内存占用量。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 中的每个根端口有单独的计数器 (RMC)，以测量从根端口和更低段传出或传入的 PCI Express 流量。然后，将聚合这些计数器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 IO 带宽利用率的量度。
- **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运行的工作负载的性质。因此，在任何给定时间，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 利用率指标将一分钟进行一次聚合。因此，如果在这些指标中存在任何瞬时峰值，这些峰值可能会隐藏。它们用于表示工作负载模式而非资源利用量。

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。
- 读取历史统计数据时所需的登录权限和 Enterprise 许可证。

使用 Web 界面监测 CPU、内存和 I/O 模块的性能指标

要监测 CPU、内存和 I/O 模块的性能指标，请在 iDRAC Web 界面中转至**概览** → **硬件**。**硬件概览**页面将显示以下内容：

- **硬件**部分 - 单击所需的链接可查看组件的运行状况。
- **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 利用率和系统级 CUPS 指标的统计数据。如果主机系统已关闭电源，则图形将显示低于 0% 的关闭电源线。
  - 可以重设特定传感器的峰值利用率。为此，可单击**重设历史峰值**。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
  - 显示或指定警告阈值利用率限值。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 I/O 模块的性能指标

可使用 **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 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

检查系统的新鲜空气符合性

新鲜空气冷却功能直接使用外部空气来冷却数据中心的系统。新鲜空气符合性系统可以在其正常环境工作范围（温度高达 113 °F（ 45 °C）以上工作。

注: 某些服务器或服务器配置可能不具备新鲜空气符合性。要获取有关新鲜空气符合性的详细信息，请参阅具体的服务器手册或联系 Dell 以获取更多详细信息。

检查系统的新鲜空气符合性：

1. 在 iDRAC Web 界面中，转至**概览** → **服务器** → **电源/散热** → **温度**。
   随即会显示 **温度**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

您可以监测系统在高于通常受支持的新鲜空气温度阈值的环境温度下工作的时间的百分比。系统板温度传感器读数在一段时间内得到收集，以便监测温度。数据收集在系统从出厂后首次通电时开始，并且在整个系统通电期间收集和显示数据。您可以跟踪和存储过去七年的受监测温度。

注: 即使系统不具备新鲜空气符合性，您也可以跟踪其温度历史记录。但是，将根据新鲜空气支持的限制条件生成阈值限制和新鲜空气相关警告。这些限制条件是，42ºC 时发出警告，47ºC 时发出严重警报。这些值对应于 40 º C 和 45ºC 的新鲜空气限制（具有 2ºC 的差数，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：

- 警告范围 — 包括系统在超过温度传感器警告阈值 (42ºC) 的温度条件下工作的持续时间。在为期 12 个月的周期内，系统可以在 10% 的时间内在警告范围内工作。
- 严重范围 — 包括系统在超过温度传感器严重阈值 (47ºC) 的温度条件下工作的持续时间。在为期 12 个月的周期内，系统可以在 1% 的时间内在严重范围内工作。严重范围也增加了警告范围的时间。

所收集的数据以图形格式表示，以便跟踪 10% 和 1% 水平。所记录的温度数据只能在从工厂发货之前清除。

如果系统在超过通常受支持的温度阈值的条件下持续工作指定的工作时间，则生成一个事件。如果指定工作时间内的平均温度大于或等于警告水平（> = 8%）或严重水平（> = 0.8%），则会在 Lifecycle 日志中记录一个事件，并且生成相应的 SNMP 陷阱。这些事件包括：

- 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**概览** → **服务器** → **电源/散热** → **温度**。
   随即会显示 **温度**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。

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** 子命令。有关更多信息，请参阅 *iDRAC8 RACADM Command Line Reference Guide*（iDRAC8 RACADM 命令行参考指南）。

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。如果执行重设为默认值的操作，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**概览** → **服务器** → **电源/散热** → **温度**。
   随即会显示 **温度**页面。
2. 在**温度探测器**部分中，对于**系统板入口温度**，以摄氏度或华氏度为单位输入**警告阈值**的最小和最大值。如果以摄氏度输入值，系统将自动计算并显示华氏度值。类似地，如果输入华氏度值，将显示摄氏度值。
3. 单击**应用**。
   值已配置。

   注: 对默认阈值的更改不会反映在历史记录数据图表中，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消息不同于有关超出新鲜空气阈值的警告消息。

查看主机操作系统上可用的网络接口

您可以查看主机操作系统上可用的所有网络接口的相关信息，例如分配给服务器的 IP 地址。iDRAC Service Module 为 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、网络接口说明、网络接口状态、网络接口类型（以太网、隧道、环回等）、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 Enterprise 许可证提供。

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**概览** → **服务器** → **服务模块**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. 转到**概览** → **主机操作系统** → **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。

   将在**硬件 → 网络设备**部分中显示相应的设备页面，其中会显示设备的详细信息。有关属性的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

4. 对于每个网络设备，请单击 ⊞ 图标可显示其他详细信息。

   同样，可以从**硬件 → 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。请单击**查看主机操作系统的网络接口**。

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 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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 FlexAddress 信息，请在 Chassis Management Controller (CMC) 中配置并启用 FlexAddress 功能。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Dell Chassis Management Controller User Guide*（Dell Chassis Management Controller 用户指南）。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: 要避免可能导致无法开启受管系统的错误，每个端口和光纤连接都*必须*安装正确类型的夹层卡。

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**：

- **Overview（概述） → Server（服务器） → Properties（属性） Details（详细信息） → iDRAC Information（iDRAC 信息）**。
- **Overview（概述） → Server（服务器） → Properties（属性）WWN/MAC**。
- **Overview（概述） → iDRAC Settings（iDRAC 设置） → Properties（属性） iDRAC Information（iDRAC 信息） → Current Network Settings（当前网络设置）**。
- **Overview（概述） → iDRAC Settings（iDRAC 设置） → Network（网络） Network（网络） → Network Settings（网络设置）** 。

小心: 启用 FlexAddress 后，如果从服务器分配的 MAC 地址切换到机箱分配的 MAC 地址或者相反，iDRAC IP 地址也会变化。

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**概览** → **iDRAC 设置** → **会话**。
   随即**会话**页面会显示会话 ID、用户名、IP 地址以及会话类型。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。

有关这些命令的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

6

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 Serial Over LAN（IPMI LAN 上串行）
- IPMI Over LAN（LAN 上 IPMI）
- 远程 RACADM
- 本地 RACADM
- 远程服务

有关支持协议、命令和前提条件的概述，请参阅下表。

表. 11: 通信模式 — 摘要

通信模式	支持的协议	支持的命令	前提条件
iDRAC Web 界面	Internet 协议 (https)	不适用	Web Server
使用串行通信 DB9 电缆的串行接口	串行协议	RACADM SMCLP IPMI	iDRAC 固件的组成部分 RAC 串行或 IPMI 串行已启用。
IPMI Serial Over LAN（IPMI LAN 上串行）	智能平台管理总线协议 SSH Telnet	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。
SMCLP	SSH Telnet	SMCLP	iDRAC 上的 SSH 或 Telnet 已启用。
远程 RACADM	https	远程 RACADM	远程 RACADM 已安装并启用。
固件 RACADM	SSH Telnet	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。

通信模式	支持的协议	支持的命令	前提条件
远程服务 [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM 已安装 (Windows) 或 OpenWSMAN 已安装 (Linux)。

[1] 有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller Remote Services 用户指南）。

相关概念

使用 DB99 电缆通过串行连接与 iDRAC 进行通信
使用 DB9 电缆时在 RAC 串行和串行控制台之间切换
使用 IPMI SOL 与 iDRAC 进行通信
使用 LAN 上 IPMI 与 iDRAC 通信
启用或禁用远程 RACADM
禁用本地 RACADM
启用受管系统上的 IPMI
在引导期间为串行控制台配置 Linux
支持的 SSH 加密方案

使用 DB99 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: 如果是刀片服务器，则串行连接通过机箱建立。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Chassis Management Controller User's Guide*（Chassis Management Controller 用户指南）。

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。
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。

相关概念

针对串行连接配置 BIOS
启用 RAC 串行连接
启用 IPMI 串行连接基本和终端模式

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> 键。
3. 转至 **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: 这仅适用于机架和塔式服务器中的 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**概览** → **iDRAC 设置** → **网络** → **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，请使用以下选项之一：

- 将 cfgSerial 组中的对象与 config 命令配合使用。
- 将 iDRAC.Serial 组中的对象与 set 命令配合使用。

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: 这仅适用于机架和塔式服务器中的 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 root -p calvin sel get
  ```
- 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。

相关概念

[针对串行连接配置 BIOS]

[IPMI 串行终端模式的附加设置]

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**概览** → **iDRAC 设置** → **网络** → **串行**。
2. 在 **IPMI 串行**下，指定该属性的值。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，然后使用以下任一命令启用 IPMI 模式：

- 使用 config 命令：

  `racadm config -g cfgSerial -o cfgSerialConsoleEnable 0`

  `racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode < 0 or 1>`

  其中，*0* 表示终端模式而 *1* 表示基本模式。
- 使用 set 命令：

  `racadm set iDRAC.Serial.Enable 0`

  `racadm set iDRAC.IPMISerial.ConnectionMode < 0 or 1>`

  其中，*0* 表示终端模式而 *1* 表示基本模式。

使用 RACADM 启用串行连接 IPMI 串行设置

要配置 IPMI 串行设置，可以使用 set 或 config 命令：

1. 使用以下命令将 IPMI 串行连接模式更改为相应的设置：
   - 使用 config 命令：`racadm config -g cfgSerial -o cfgSerialConsoleEnable 0`
   - 使用 set 命令：`racadm set iDRAC.Serial.Enable 0`
2. 设置 IPMI 串行波特率：
   - 使用 config 命令：`racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <baud_rate>`
   - 使用 set 命令：`racadm set iDRAC.IPMISerial.BaudRate <baud_rate>`

   其中 `<baud_rate>` 为 9600、19200、57600 或 115200 bps。
3. 启用 IPMI 串行硬件流控制：
   - 使用 config 命令：`racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1`
   - 使用 set 命令：`racadm set iDRAC.IPMISerial.FlowControl 1`
4. 设置 IPMI 串行信道最低权限级别：
   - 使用 config 命令：`racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <level>`
   - 使用 set 命令：`racadm set iDRAC.IPMISerial.ChanPrivLimit <level>`

   其中，`<level>` 为 2（用户）、3（操作员）或 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**概览** → **iDRAC 设置** → **网络** → **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，请运行命令：`racadm config cfgIpmiSerial`

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

要在串行控制台模式中切换到 RAC 串行接口通信模式，请使用以下键序列：

```
<Esc> +<Shift> <9>
```

以上键序列会定向到 iDRAC Login（iDRAC 登录）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 串行接口通信模式下切换到串行控制台模式，请使用以下键序列：

```
<Esc> +<Shift> <q>
```

在终端模式下，要将连接切换为串行控制台模式，请使用：

```
<Esc> +<Shift> <q>
```

在串行控制台模式下时，要返回终端模式用途，请使用：

```
<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。通过 SOL，您可以：

- 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、Telnet、IPMItool）。

相关概念

[针对串行连接配置 BIOS](#)
[配置 iDRAC 以使用 SOL](#)
[启用支持的协议](#)

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> 键。
3. 转至 **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 以 25 x 80 的格式发送屏幕串行数据。用于调用 `console com2` 命令的 SSH 窗口必须设置为 25 x 80。这样，重定向之后的屏幕就可以正常显示。

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**概览** → **iDRAC 设置** → **网络** → **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. 启用 IPMI LAN 上串行：
   - 使用 **config** 命令：`racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`
   - 使用 **set** 命令：`racadm set iDRAC.IPMISol.Enable 1`
2. 更新 IPMI SOL 最低权限级别：
   - 使用 **config** 命令：`racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <level>`
   - 使用 **set** 命令：`racadm set iDRAC.IPMISol.MinPrivilege 1`

   其中，`<level>` 是 2（用户）、3（操作员）、4（管理员）。

   注: IPMI SOL 最低权限级别确定激活 IPMI SOL 的最低权限级别。有关详细信息，请参阅 IPMI 2.0 规范。
3. 更新 IPMI SOL 波特率：
   - 使用 **config** 命令：`racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <baud_rate>`
   - 使用 **set** 命令：`racadm set iDRAC.IPMISol.BaudRate <baud_rate>`

   其中 `<baud_rate>` 为 9600、19200、57600 或 115200 bps。

   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。
4. 为每位用户启用 SOL：
   - 使用 **config** 命令：`racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2`

- 使用 set 命令：`racadm set iDRAC.Users.<id>.SolEnable 2`

其中 `<id>` 是用户的唯一 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

支持的协议为 IPMI、SSH 和 Telnet。

使用 Web 界面启用支持的协议

要启用 SSH 或 Telnet，请转到 **Overview**（概览） → **iDRAC Settings**（iDRAC 设置） → **Network**（网络） → **Services**（服务），然后为 SSH 或 Telnet 分别选择 **Enabled**（启用）。

要启用 IPMI，请转到**概览** → **iDRAC 设置** → **网络**，并选择**启用 LAN 上 IPMI**。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 或 Telnet，请运行以下命令：

- Telnet：
  - 使用 config 命令：`racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
  - 使用 set 命令：`racadm set iDRAC.Telnet.Enable 1`
- SSH：
  - 使用 config 命令：`racadm config -g cfgSerial -o cfgSerialSshEnable 1`
  - 使用 set 命令：`racadm set iDRAC.SSH.Enable 1`

  要更改 SSH 端口，请执行以下操作：

  - 使用 config 命令：`racadm config -g cfgRacTuning -o cfgRacTuneSshPort <port number>`
  - 使用 set 命令：`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 或 Telnet 协议）

相关任务

使用 IPMI 协议的 SOL
使用 SSH 或 Telnet 协议的 SOL

使用 IPMI 协议的 SOL

IPMItool <--> LAN/WAN 连接 <--> iDRAC

基于 IPMI 的 SOL 公用程序和 IPMItool 使用 RMCP+（使用 UDP 数据报发送到端口 623）。当使用 IPMI 2.0 时，RMCP+ 提供改进的身份验证、数据完整性检查、加密机制以及携带多个有效负荷的能力。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。

指向 iDRAC 的 RMCP+ 连接必须使用加密密钥（Key Generator (KG) 密钥）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，您可以在**概览** → **iDRAC 设置** → **网络** → **服务**中更改 SOL 的默认超时值。

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. 在命令提示符下（Windows 或 Linux），运行此命令以从 iDRAC 启动 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，请轮流按下 <~> 和 <.>。SOL 会话即关闭。

   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。

使用 SSH 或 Telnet 协议的 SOL

Secure Shell (SSH) 和 Telnet 是用于与 iDRAC 执行命令行通信的网络协议。您可以通过任一接口分析远程 RACADM 和 SMCLP 命令。
SSH 相对于 Telnet 拥有增强的安全性。iDRAC 仅支持带有密码验证的 SSH 版本 2，并且在默认情况下已启用。iDRAC 同时最多支持两个 SSH 会话和两个 Telnet 会话。建议使用 SSH，因为 Telnet 并非安全协议。仅当无法安装 SSH 客户端或网络基础架构安全时才必须使用 Telnet。

使用在管理站上支持 SSH 和 Telnet 网络协议的开源程序（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 或 Telnet 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 或 Telnet。
   Telnet（端口 23）/SSH（端口 22）客户端 <--> WAN 连接 <--> iDRAC

   基于 IPMI 的 SOL 使用 SSH 或 Telnet 协议从而无需另外公用程序，因为串行到网络转换在 iDRAC 内发生。您使用的 SSH 或 Telnet 控制台必须能够解释和响应从受管系统的串行端口到达的数据。串行端口通常附加到仿真 ANSI- 或 VT100/VT220 终端的 shell。串行控制台将自动重定向到 SSH 或 Telnet 控制台。

相关任务

[从 Windows 上的 Putty 使用 SOL](#)
[从 Linux 上的 OpenSSH 或 Telnet 使用 SOL](#)

从 Windows 上的 Putty 使用 SOL

从 Windows Management Station 上的 Putty 启动 IPMI SOL：

注: 如有必要，您可以在 **Overview**（**概览**） → **iDRAC Settings**（**iDRAC 设置**） → **Network**（**网络**） → **Services**（**服务**）下更改默认的 SSH 或 Telnet 超时。

1. 运行以下命令连接到 iDRAC：`putty.exe [-ssh | -telnet] <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 或 Telnet 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。

相关概念

在 iDRAC 命令行控制台中断开 SOL 会话连接

从 Linux 上的 OpenSSH 或 Telnet 使用 SOL

从 Linux 管理站上的 OpenSSH 或 Telnet 启动 SOL：

注: 如有必要，您可以在 **Overview**（概述） → **iDRAC Settings**（iDRAC 设置） → **Network**（网络） → **Services**（服务）下更改默认 SSH 或 Telnet 会话超时。

1. 启动 shell。
2. 使用以下命令连接到 iDRAC：
   - 对于 SSH：ssh <*iDRAC-ip-address*> -l <*login name*>
   - 对于 Telnet：telnet <*iDRAC-ip-address*>

   注: 如果更改了 Telnet 服务的默认端口号（端口 23），则将端口号添加到 Telnet 命令结尾。

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 config -g cfgSerial -o cfgSerialHistorySize <number>
   ```

4. 退出 SOL 会话以关闭活动的 SOL 会话。

相关任务

使用 Telnet 虚拟控制台
为 Telnet 会话配置 Backspace 键
在 iDRAC 命令行控制台中断开 SOL 会话连接

使用 Telnet 虚拟控制台

当 BIOS 虚拟控制台设为 VT100/VT220 仿真时，Microsoft 操作系统上的某些 Telnet 客户端可能不会正确显示 BIOS 设置屏幕。如果发生此问题，请将 BIOS 控制台更改为 ANSI 模式以更新显示。要在 BIOS 设置菜单中执行此程序，请选择**虚拟控制台 → 远程终端类型 → ANSI**。

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。

要使用 Telnet 虚拟控制台：

1. 在 **Windows Component Services**（**Windows 组件服务**）中启用 **Telnet**。
2. 使用以下命令连接到 iDRAC：`telnet <IP address>:<port number>`，其中 `IP address` 是 iDRAC 的 IP 地址，而 `port number` 是 Telnet 端口号（如果您使用新端口）。

为 Telnet 会话配置 Backspace 键

根据 Telnet 客户端，使用 <Backspace>（退格）键可能会产生意外的结果。例如，会话可能会回应 `^h`。不过，大多数 Microsoft 和 Linux Telnet 客户端均可配置使用 <Backspace> 键。

要配置 Linux Telnet 会话使用 <Backspace> 键，打开命令提示符并键入 `stty erase ^h`。在提示符下，键入 `telnet`。

配置 Microsoft Telnet 客户端使用 <Backspace> 键：

1. 打开命令提示符窗口（如果需要）。
2. 如果没有运行 Telnet 会话，请键入 `telnet`。如果正在运行 Telnet 会话，请按 `<Ctrl><]>`。
3. 在提示符下，键入 `set bsasdel`。

   将显示信息 `Backspace will be sent as delete`。

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，请依次按 <Enter> 键、<Esc> 键和 <t> 键。SOL 会话将关闭。
- 要从 Linux 上的 Telnet 退出 SOL 会话，请按住 <Ctrl>+]。将显示 Telnet 提示符。输入 `quit` 退出 Telnet。
- 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 界面的 **Overview**（**概览**） → **iDRAC Settings**（**iDRAC 设置**） → **Sessions**（**会话**）下终止命令行控制台。

使用 LAN 上 IPMI 与 iDRAC 通信

您必须为 iDRAC 配置 LAN 上 IPMI，才能对任何外部系统的 LAN 信道启用或禁用 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。

使用 Web 界面配置 LAN 上 IPMI

配置 LAN 上 IPMI：

1. 在 iDRAC Web 界面中，转至**概览 → iDRAC 设置 → 网络**。

   随即会显示 **Network**（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

要配置 LAN 上 IPMI，请使用 set 或 config 命令：

1. 启用 LAN 上 IPMI：
   - 使用 config 命令：racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   - 使用 set 命令：racadm set iDRAC.IPMILan.Enable 1

   注: 该设置确定使用 LAN 上 IPMI 界面执行的 IPMI 命令。有关更多信息，请参阅 **intel.com** 上的 IPMI 2.0 规范。
2. 更新 IPMI 信道权限：
   - 使用 config 命令：racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <level>
   - 使用 set 命令：racadm set iDRAC.IPMILan.PrivLimit <level>

   其中，<level> 是以下任一项：2（用户）、3（操作员）或 4（管理员）
3. 如果需要，请设置 IPMI LAN 信道加密密钥：
   - 使用 config 命令：racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <key>
   - 使用 set 命令：racadm set iDRAC.IPMILan.EncryptionKey <key>

   其中 <key> 是一个有效的十六进制格式的 20 字符加密密钥。

   注: iDRAC IPMI 支持 RMCP+ 协议。有关更多信息，请参阅 **intel.com** 上的 IPMI 2.0 规范。

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。最多可并行运行五个远程 RACADM 会话。

使用 Web 界面启用或禁用远程 RACADM

启用或禁用远程 RACADM：

1. 在 iDRAC Web 界面中，转至**概览** → **iDRAC 设置** → **网络** → **服务**。

将显示 **Services**（**服务**）页面。

2. 在**远程 RACADM** 下，选择**启用**。否则，选择**禁用**。
3. 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

默认启用 RACADM 远程功能。如果禁用此功能，请键入以下命令之一：

- 使用 config 命令：`racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1`
- 使用 set 命令：`racadm set iDRAC.Racadm.Enable 1`

要禁用远程功能，请键入以下命令之一：

- 使用 config 命令：`racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0`
- 使用 set 命令：`racadm set iDRAC.Racadm.Enable 0`

注: 建议在本地系统上运行这些命令。

禁用本地 RACADM

本地 RACADM 默认启用。要禁用，请参阅禁用访问以修改主机系统上的 iDRAC 配置设置。

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 **dell.com/support/manuals** 上提供的 *Dell Open Manage Server Administrator's User Guide*（Dell Open Manage Server Administrator 用户指南）。

在引导期间为串行控制台配置 Linux

以下步骤专用于 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。

按照以下说明编辑 **/etc/grub.conf** 文件：

1. 找到文件的 General Setting（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 屏幕不会在 RAC 虚拟控制台中显示。要禁用图形界面，请注释掉以 `splashimage` 开头的行。

   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` 添加到第一个选项。

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
```

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. 12: SSH 密码方案

方案类型	方案
非对称加密	Diffie-Hellman DSA/DSS 512-1024（随机）位/NIST 规范
对称加密	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
消息完整性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
验证	密码
PKA 身份验证	公-私密钥对

对 SSH 使用公共密钥验证

iDRAC 支持 SSH 上的公共密钥验证 (PKA)。这是一个获得许可证的功能。如果正确设置和使用 SSH 上的 PKA，则当登录到 iDRAC 时，您无需输入用户名或密码。这对设置执行各种功能的自动化脚本非常有用。上载的密钥必须使用 RFC 4716 或 openssh 格式。否则，您必须将密钥转换为该格式。

在任何情况下，必须在管理站上生成一对私有和公共密钥。将公共密钥上载到 iDRAC 本地用户，同时 SSH 客户端会使用私有密钥来建立管理站与 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: 在 iDRAC 上，该权限通常保留为属于管理员用户组成员的用户使用。但是，可以向位于“自定义”用户组中的用户分配此权限。具有此权限的用户可修改任何用户的配置。这包括创建或删除任何用户，为任何用户管理 SSH 密钥等。由于这些原因，因此，请谨慎分配此权限。

小心: 上载、查看和/或删除 SSH 密钥的能力取决于“配置用户”用户权限。该权限允许用户配置其他用户的 SSH 密钥。您需要谨慎分配此权限。

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. 启动该应用程序并选择要生成的 SSH-2 RSA 或 SSH-2 DSA 密钥类型（SSH-1 不受支持）。支持的密钥生成算法仅包括 RSA 和 DSA。
2. 输入密钥的位数。对于 RSA，密钥位数为 768 和 4096 位，而对于 DSA，则为 1024 位。
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 1024 –C testing`

其中：

- `-t` 是 *dsa* 或 *rsa*。
- –b 选项指定介于 768 和 4096 之间的加密位数。
- `–c` 选项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。

请按照指示进行操作。命令执行后，请上载公共文件。

小心: 使用 ssh-keygen 从 Linux Management Station 生成的密钥是非 4716 格式。请使用 `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` 将该密钥转换为 4716 格式。请勿更改该密钥文件的权限。该转换必须使用默认权限执行。

注: iDRAC 不支持密钥的 ssh-agent 转发。

上载 SSH 密钥

您可以为*每位用户*上载最多四个公共密钥通过 SSH 接口使用。添加公共密钥之前，请确保查看密钥是否已设置，以便密钥不会被意外覆盖。

添加新公共密钥时，请确保现有的密钥不会在添加新密钥位置的索引中。iDRAC 不支持在添加新密钥之前执行检查以确保以前的密钥删除。当添加新密钥时，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**概览** → **iDRAC 设置** → **网络** → **用户验证** → **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 **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，请执行：`racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- 对于远程 RACADM，请使用 Telnet 或 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 telnet/ssh/serial 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，转到 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **User Authentication（用户身份验证）** → **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 **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。

使用 RACADM 查看 SSH 密钥

要查看 SSH 密钥，请运行以下命令：

- 特定密钥 - `racadm sshpkauth -i <2 to 16> -v -k <1 to 4>`
- 所有密钥 - `racadm sshpkauth -i <2 to 16> -v -k all`

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，转到 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **User Authentication（用户身份验证）** → **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。

   随即会显示 **User 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**。

   随即会显示包含密钥详细信息的 **View/Remove SSH Key(s)（查看/删除 SSH 密钥）**页面。

4. 选择 **Remove（删除）要删除的密钥，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`

7

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 管理系统和维护系统安全。默认情况下，使用本地管理员帐户配置 iDRAC。此默认用户名为 *root*，并且密码为 *calvin*。作为管理员，您可以设置用户帐户以允许其他用户访问 iDRAC。

您可以设置本地用户或用户目录服务（例如 Microsoft Active Directory 或 LDAP）以设置用户帐户。使用目录服务可提供一个集中的位置用于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。

相关概念

配置本地用户
配置 Active Directory 用户
配置通用 LDAP 用户

配置本地用户

您可以使用特定的访问权限在 iDRAC 中配置多达 16 个本地用户。在创建 iDRAC 用户之前，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来设置用户名、密码和角色。这些用户名和密码可以通过任何 iDRAC 的安全保护界面（即 Web 界面、RACADM 或 WS-MAN）进行更改。您还可以为每个用户启用或禁用 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**概览** → **iDRAC 设置** → **用户验证** → **本地用户**。
   此时将显示 **Users**（用户）页面。
2. 在 **User ID**（用户 ID）列中，单击用户 ID 编号。

   注: 用户 1 用于 IPMI 匿名用户，您无法更改此配置。

   显示 **User Main Menu**（用户主菜单）页面。
3. 选择 **Configure User**（配置用户），然后单击 **Next**（下一步）。
   显示 **User Configuration**（用户配置）页面。
4. 启用用户 ID 并为用户指定用户名、密码和访问权限。您还可以为用户启用 SNMPv3 验证。有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
5. 单击 **Apply**（应用）。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。

要配置多个具有相同配置设置的 iDRAC 用户，请执行以下步骤之一：

- 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个受管系统上创建 iDRAC 配置文件并执行 racadm config 或 racadm set 子命令。

如果您正在配置新的 iDRAC 或者您已经使用了 **racadm racresetcfg** 命令，则唯一的当前用户是 `root`，密码为 `calvin`。**racresetcfg** 子命令会将会把 iDRAC 重设为默认值。

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，请在命令提示符下输入以下命令：

- 使用 config 命令：`racadm getconfig -u <username>`

或

输入以下命令，每次仅查找索引 1 至 16 中的一个：

- 使用 config 命令：`racadm getconfig -g cfgUserAdmin -i <index>`
- 使用 get 命令：`racadm get iDRAC.Users.<index>.UserName`

注: 您还可以键入 `racadm getconfig -f <myfile.cfg>` 或 `racadm get -f <myfile.cfg>`，并查看或编辑 **myfile.cfg** 文件，该文件包含所有 iDRAC 配置参数。

多个参数和对象 ID 会与其当前值一起显示。其中重要的对象是：

- 如果您已经使用 getconfig 命令：

  ```
  # cfgUserAdminIndex=XX
  cfgUserAdminUserName=
  ```
- 如果您已经使用 get 命令：

  ```
  iDRAC.Users.UserName=
  ```

如果 **cfgUserAdminUserName** 对象没有值，则可以使用 **cfgUserAdminIndex** 对象指示的索引编号。如果 “=”后显示了名称，该索引即会被此用户名使用。

使用 **racadm config** 子命令手动启用或禁用用户时，*必须*以 **-i** 选项指定索引。

请注意，上述示例中显示的 **cfgUserAdminIndex** 对象包含“#”字符。它表示这是一个只读对象。同样，如果您使用 **racadm config -f racadm.cfg** 命令来指定需要写入的任意数量的组/对象，将无法指定索引。这种行为允许使用相同设置配置多个 iDRAC 时具备更大的灵活性。

要为用户启用 SNMP v3 验证，请使用 **SNMPv3AuthenticationType**、**SNMPv3Enable**、**SNMPv3PrivacyType** 对象。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *RACADM Command Line Interface Guide*（RACADM 命令行界面指南）。

如果您使用的是 XML 配置文件，请使用 **AuthenticationProtocol**、**ProtocolEnable** 和 **PrivacyProtocol** 属性来启用 SNMPv3 验证。

使用 RACADM 添加 iDRAC 用户

要添加新用户到 RAC 配置，请执行以下操作：

1. 设置用户名。
2. 设置密码。
3. 设置以下用户权限：
   - iDRAC
   - LAN
   - Serial Port
   - LAN 上串行
4. 启用用户。

示例：

下面的示例说明如何添加新用户 "John" 密码 "123456"，该用户对 RAC 具有“登录”权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 3 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 123456
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiLanPrivilege 2
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiSerialPrivilege 2
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminSolEnable 1
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminEnable 1
```

要进行验证，请使用以下命令之一：

```
racadm getconfig -u john
racadm getconfig –g cfgUserAdmin –i 3
```

有关 RACADM 命令的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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）：

注: 您可以使用 **getconfig** 和 **config** 命令或者使用 **get** 和 **set** 命令。

1. 使用命令语法找到可用的用户索引：
   - 使用 **getconfig** 命令：racadm getconfig -g cfgUserAdmin -i <index>
   - 使用 **get** 命令：racadm get iDRAC.Users <index>
2. 使用新用户名和密码键入以下命令。
   - 使用 **config** 命令：racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <user privilege bitmask value>

- 使用 set 命令：`racadm set iDRAC.Users.<index>.Privilege <user privilege bitmask value>`

注: 有关特定用户权限的有效位掩码值的列表，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。默认权限值为 0，即表示用户未启用任何权限。

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。这是已许可的功能。

注: Microsoft Windows 2000、Windows Server 2003 和 Windows Server 2008 操作系统支持使用 Active Directory 来识别 iDRAC 用户。

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权限，从而使管理员可以为每位用户配置特定的权限。

与上一代服务器的 iDRAC 角色和权限名称相比，现在已发生更改。角色名称为：

表. 13: iDRAC 角色

目前这一代	前一代	Privileges（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
Read Only（只读）	来宾用户	登录
无	无	无

表. 14: 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。
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	使用户可以清除系统事件日志 (SEL)。
系统控制	执行服务器控制命令	可对主机系统关机后再开机。
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）	使用户可以运行虚拟控制台。

目前这一代	前一代	说明
	访问虚拟控制台（适用于机架式和塔式服务器）	
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。
Debug（调试）	执行诊断命令	使用户可以运行诊断命令。

相关概念

[对 iDRAC 使用 Active Directory 验证的前提条件](#)
[支持的 Active Directory 验证机制](#)

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 Active Directory 架构。有关详细信息，请参阅 Microsoft 网站。
- 将 PKI 集成到 Active Directory 架构中。iDRAC 使用标准公共密钥架构 (PKI) 机制来验证 Active Directory 的安全性。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。

相关任务

[在域控制器上启用 SSL](#)

在域控制器上启用 SSL

当 iDRAC 使用 Active Directory 域控制器验证用户时，会启动与域控制器之间的 SSL 会话。此时，域控制器必须发布由认证机构 (CA) 签署的证书 — 其根证书也上载到 iDRAC 中。对于*任何*要使用域控制器验证的 iDRAC — 不管它是根域控制器还是子域控制器 — 该域控制器必须具有由域的认证机构签发的启用了 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。

相关任务

[安装每个域控制器的 SSL 证书](#)
[将域控制器根 CA 证书导出至 iDRAC](#)
[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

注: 如果系统运行 Windows 2000 或您使用独立的 CA，以下步骤可能不同。

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 **OK**（**确定**）。
4. 在 **Console 1**（**控制台 1**）(MMC) 窗口中，单击 **File**（**文件**）（在 Windows 2000 系统上则单击 **Console**（**控制台**））并选择 **Add/Remove Snap-in**（**添加/删除管理单元**）。
5. 在 **Add/Remove Snap-in**（**添加/删除管理单元**）窗口中，单击 **Add**（**添加**）。
6. 在 **Standalone Snap-in**（**独立管理单元**）窗口中，选择 **Certificates**（**证书**）并单击 **Add**（**添加**）。
7. 选择 **Computer**（**计算机**）并单击 **Next**（**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 **Certificate Export Wizard**（**证书导出向导**）中，单击 **Next**（**下一步**）并选择 **No do not export the private key**（**不，不导出私有密钥**）。
12. 单击 **Next**（**下一步**）并选择 **Base-64 encoded X.509 (.cer)**（**基于 64 位编码的 X.509 [.cer]**）作为格式。
13. 单击 **Next**（**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 控制器都附带一个默认的自签名证书。

如果 Active Directory 服务器设置为在 SSL 会话初始化阶段期间验证客户端，您需要将 iDRAC 服务器证书上载到 Active Directory 域控制器。如果 Active Directory 不在 SSL 会话的初始化阶段期间执行客户端验证，则无需此附加步骤。

注: 如果系统运行 Windows 2000，以下步骤可能不同。

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 0x1 -f <RAC SSL certificate>
   ```

2. 在域控制器上，打开 **MMC Console**（**MMC 控制台**）窗口并选择 **Certificates**（**证书**） → **Trusted Root Certification Authorities**（**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 **Next**（**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。

如果您已安装自己的证书，请确保 CA 签名位于 **Trusted Root Certification Authority**（受信任的根认证机构）列表中的您的证书。如果该机构不在列表中，则您必须在所有域控制器上安装它。

6. 单击 **Next**（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**，然后单击**确定**。iDRAC 固件 SSL 证书已导入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，拥有自定义的 Active Directory 对象。所有访问控制对象都在 Active Directory 中维护。它为在具有各种权限级别的不同 iDRAC 上配置用户访问权限提供了最大的灵活性。

相关概念

[标准架构 Active Directory 概览](#)
[扩展架构 Active Directory 概览](#)

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。

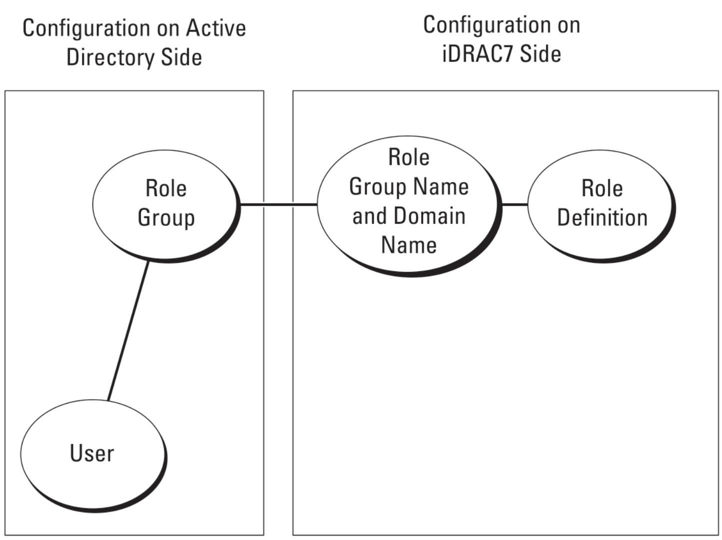


图 1: 使用 Active Directory 标准架构配置 iDRAC

在 Active Directory 中，一个标准组对象用作角色组。具有 iDRAC 访问权限的用户为该角色组的成员。要为此用户分配访问特定 iDRAC 的权限，需要在特定 iDRAC 上配置角色组名称及其域名。角色及权限级别在每个 iDRAC（而不是 Active Directory 中）上进行定义。在每个 iDRAC 中，最多可以定义五个角色组。表参考编号显示默认角色组的权限。

表. 15: 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	0x000001ff

角色组	默认权限级别	授予的权限	位掩码
		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	
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: “位掩码”值只有在用 RACADM 设置标准架构时才使用。

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（或任何嵌套组）来自多个域，则必须在 iDRAC 上配置全局编录服务器地址。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

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. 创建一个组或选择现有的组。将 Active Directory 用户添加为 Active Directory 组的成员以访问 iDRAC。
3. 在 iDRAC 上使用 iDRAC Web 界面或 RACADM 配置组名、域名和角色权限。

相关任务

使用 iDRAC Web 界面配置具有标准架构的 Active Directory
使用 RACADM 配置具有标准架构的 Active Directory

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**概览** → **iDRAC 设置** → **用户验证** → **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**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. 或者，当与 Active Directory (AD) 服务器通信时，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。为此，必须指定域控制器和全局编录 FQDN。该操作将在后面的步骤中完成。因此 DNS 应在网络设置中正确进行配置。
5. 单击下一步。

   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 Active Directory 响应的时长。

   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。
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

使用 RACADM 配置具有标准架构的 iDRAC Active Directory：

1. 在 racadm 命令提示符下，运行以下命令：
   - 使用 config 命令：

     ```
     racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
     cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -i
     <index> -o cfgSSADRoleGroupName <common name of the role group> racadm
     config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully
     qualified domain name> racadm config -g cfgStandardSchema -i <index> -o
     cfgSSADRoleGroupPrivilege <Bit Mask Value for specific RoleGroup
     permissions> racadm config -g cfgActiveDirectory -o
     cfgADDomainController1 <fully qualified domain name or IP address of the
     domain controller> racadm config -g cfgActiveDirectory -o
     cfgADDomainController2 <fully qualified domain name or IP address of the
     domain controller> racadm config -g cfgActiveDirectory -o
     cfgADDomainController3 <fully qualified domain name or IP address of the
     domain controller> racadm config -g cfgActiveDirectory -o
     cfgADGlobalCatalog1 <fully qualified domain name or IP address of the
     domain controller> racadm config -g cfgActiveDirectory -o
     cfgADGlobalCatalog2 <fully qualified domain name or IP address of the
     domain controller> racadm config -g cfgActiveDirectory -o
     cfgADGlobalCatalog3 <fully qualified domain name or IP address of the
     domain controller>
     ```

- 使用 set 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>
  ```

  有关特定角色组权限的位掩码值，请参阅默认角色组权限。

  输入域控制器的 FQDN，而不是域的 FQDN。例如，输入 `servername.dell.com` 而不是 `dell.com`。

  三个地址中至少有一个需要进行配置。iDRAC 逐一尝试连接到每个配置的地址，直到成功建立连接。使用标准架构时，这些是用户帐户和角色组所在域控制器的地址。

  只有用户帐户和角色组位于不同的域中时，标准架构才需要全局编录服务器。在多个域的情况下，只能使用通用组。

  如果您启用了证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的 Subject（主题）或 Subject Alternative Name（主题备用名称）字段相符。

如果要禁用 SSL 握手过程中的证书验证，请输入以下 RACADM 命令：

- 使用 config 命令：`racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- 使用 set 命令：`racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

在此情况下，无需上载认证机构 (CA) 证书。

在 SSL 握手过程中强制执行证书验证（可选）：

- 使用 config 命令：`racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- 使用 set 命令：`racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

在此情况下，必须使用以下 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全局编录 FQDN。确保 DNS 已在 **Overview**（概述） → **iDRAC Settings**（**iDRAC 设置**） → **Network**（网络）下正确配置。

以下 RACADM 命令可选用。

```
racadm sslcertdownload -t 0x1 -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，请输入以下 RACADM 命令：
   - 使用 **config** 命令：`racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
   - 使用 **set** 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：
   - 使用 **config** 命令：

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
     config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP
     address>
     ```
   - 使用 **set** 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：
   - 使用 **config** 命令：`racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>`
   - 使用 **set** 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。

Active Directory 架构扩展

Active Directory 数据是*属性*和*类*的分布式数据库。Active Directory 架构包括用于确定可在数据库中添加或包括的数据类型的规则。用户类是数据库中存储的*类*的一个示例。一些示例用户类属性可能包括用户的名字、姓氏、电话号码等等。您可以通过添加自己唯一的*属性*和*类*来扩展 Active Directory 数据库以用于特定需求。Dell 已扩展架构以包括使用 Active Directory 支持远程管理验证和授权的必要更改。

添加到现有 Active Directory 架构的每个*属性*或*类*都必须使用唯一的 ID 定义。为了在整个行业内维护唯一的 ID，Microsoft 将维护 Active Directory 对象标识符 (OID) 的数据库，以便公司添加架构扩展时，可以保证这些扩展唯一并且不会彼此冲突。要在 Microsoft 的 Active Directory 中扩展架构，对于添加到目录服务中的属性和类，Dell 将收到唯一的 OID、唯一的扩展名和唯一链接的属性 ID：

- 扩展是：`dell`
- 基础 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 已扩展架构以包括*关联*、*设备*和*权限*属性。*关联*属性用于将用户或组与一组特定的权限一起链接到一个或多个 iDRAC 设备。此模型为网络上有各种用户、iDRAC 权限和 iDRAC 设备组合的管理员提供了最大的灵活性，而无需繁琐操作。

对于网络上您要与 Active Directory 集成进行验证和授权的每个物理 iDRAC 设备，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，并且每个关联对象可根据需要链接到尽可能多的用户、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。

但是，每个关联对象只能链接到一个权限对象（可链接用户、用户组或 iDRAC 设备对象）。本示例允许管理员控制特定 iDRAC 设备上每位用户的权限。

iDRAC 设备对象是指向 iDRAC 固件的链接，用于查询 Active Directory 以进行验证和授权。当 iDRAC 添加到网络后，管理员必须配置 iDRAC、其设备对象及 Active Directory 名称，以便用户能够通过 Active Directory 执行验证和授权。此外，管理员必须将 iDRAC 添加到至少一个关联对象以便用户进行验证。

下图显示为提供验证和授权所需连接的关联对象。

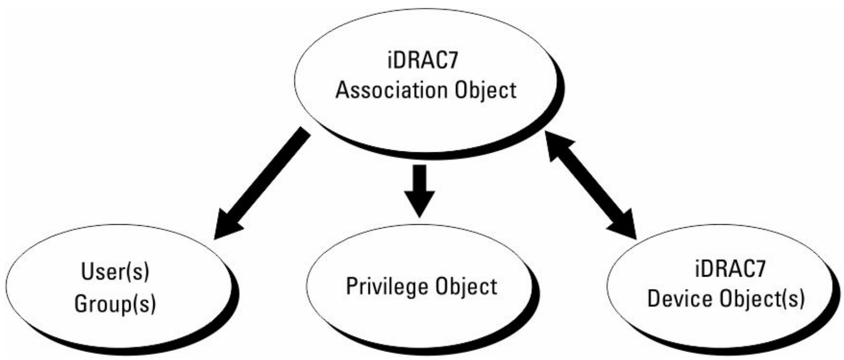


图 2: Active Directory 对象的典型设置

您可以根据需要创建任意数目的关联对象。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。

关联对象允许任意数目的用户和/或组以及 iDRAC 设备对象。但是，每个关联对象仅包括一个权限对象。关联对象可连接在 iDRAC 设备上拥有权限的用户。

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 对象与关联对象相关联。Dell 扩展不允许来自其他域的组或 iDRAC 对象作为关联对象的产品成员添加。

添加来自不同域的通用组时，将创建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，并且不能与来自其他域的通用组一起使用。

来自任何域的用户、用户组或嵌套用户组均可添加到关联对象中。扩展架构解决方案支持 Microsoft Active Directory 允许的任何用户组类型和跨多个域嵌套的任何用户组。

累积使用扩展架构的权限

扩展架构验证机制支持从不同的权限对象中进行权限累积（这些权限对象通过不同的关联对象与相同用户相关联）。换句话说，扩展架构验证累计权限以允许用户获得所有已分配权限，这些已分配权限对应于与相同用户相关联的不同权限对象。

下图提供了一个使用扩展架构累积权限的示例。

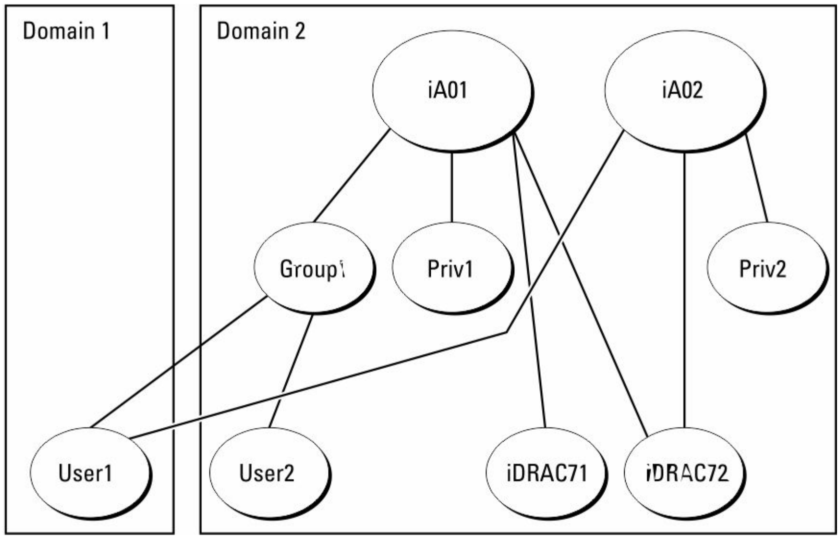


图 3: 用户权限累积

该图展示了两个关联对象 — A01 和 A02。通过这两个关联对象，用户 1 关联到 iDRAC2。

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，用户 1 拥有 iDRAC2 上的 Priv1 和 Priv2 权限。用户 1 仅拥有 iDRAC1 上的 Priv1 权限。用户 2 拥有 iDRAC1 和 iDRAC2 上的 Priv1 权限。此外，该图还展示了用户 1 可以在不同的域中，并且可以是某个组的成员。

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。

相关概念

扩展架构 Active Directory 概览
安装用于 Active Directory 用户和计算机管理单元的 Dell 扩展
将 iDRAC 用户和权限添加到 Active Directory

相关任务

使用 iDRAC Web 界面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

扩展 Active Directory 架构

通过扩展您的 Active Directory 架构，可向 Active Directory 架构添加 Dell 组织单元、架构类和属性，以及示例权限与关联对象。在您扩展架构之前，确保您对域目录林的架构主机灵活单主机操作 (FSMO) 角色拥有者具有架构管理员权限。

注: 确保该产品使用的架构扩展不同于之前的 RAC 产品。早期的架构不适用于该产品。

注: 扩展新架构不会影响之前版本的产品。

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**。
   架构已扩展。要验证架构扩展，请使用 MMC 和 Active Directory 架构管理单元验证类和属性[类和属性](#)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. 16: 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
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. 17: DelliDRACdevice 类

OID	1.2.840.113556.1.8000.1280.1.7.1.1
说明	代表 Dell iDRAC 设备。在 Active Directory 中必须将 iDRAC 配置为 delliDRACDevice。这种配置使 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. 18: 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. 19: 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

OID	1.2.840.113556.1.8000.1280.1.1.1.3
	dellIsTestAlertUser
	dellIsDebugCommandAdmin

表. 20: 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. 21: 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. 22: 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	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE
属于此属性的 dellPrivilege 对象的列表。	可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers	1.2.840.113556.1.8000.1280.1.1.2.2	FALSE
属于此角色的 dellRacDevice 和 DelliDRACDevice 对象的列表。该属性是 dellAssociationMembers 后退链接的前进链接。 链接 ID：12070	可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellIsLoginUser	1.2.840.113556.1.8000.1280.1.1.2.3	TRUE
如果用户具有设备的登录权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

属性名称/说明	分配的 OID/语法对象标识符	单值
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 如果用户具有设备的日志清除权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
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	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

属性名称/说明	分配的 OID/语法对象标识符	单值
dellAssociationObjectMembers 前进链接的后退链接。		
dellAssociationMembers 属于此产品的 dellAssociationObjectMembers 的列表。该属性是 dellProductMembers 链接属性的后退链接。 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，您可以通过在安装程序过程中选择 **Active Directory Users and Computers Snap-in（Active Directory 用户和计算机管理单元）**选项扩展管理单元。有关安装系统管理软件的其他说明，请参阅《Dell OpenManage 软件快速安装指南》。对于 64 位 Windows 操作系统，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

相关概念

将对象添加到关联对象

相关任务

创建 iDRAC 设备对象
创建权限对象
创建关联对象

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. 输入新对象的名称。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。

相关任务

　　为关联对象提供用户访问权限

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）。随即会显示 **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. 输入 `Authenticated Users`（验证的用户），单击 **Check Names**（检查名称），然后单击 **OK**（确定）。验证的用户即会添加到 **Groups and user names**（组和用户名）列表中。
5. 单击**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。

相关任务

　　添加用户或用户组
　　添加权限
　　添加 iDRAC 设备或 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**权限对象**选项卡以向关联添加权限对象，该关联定义了针对 iDRAC 设备验证时，用户或用户组的权限。一个关联对象只能添加一个权限对象。

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**权限对象**选项卡以向关联添加权限对象，该关联定义了针对 iDRAC 设备验证时，用户或用户组的权限。一个关联对象只能添加一个权限对象。

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**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**概览** → **iDRAC 设置** → **用户验证** → **目录服务** → **Microsoft Active Directory**。

   随即显示 **Active Directory** 摘要页面。
2. 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。
3. 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。
4. 单击**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。
5. 指定关于 Active Directory (AD) 服务器和用户帐户的位置信息。此外，指定在登录期间 iDRAC 必须等待 AD 响应的时长。

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 DNS 已在**概览 → iDRAC 设置 → 网络**下正确配置。
- 如果用户和 iDRAC 对象位于不同的域中，请勿选择**登录时的用户域**选项。而是选择**指定域**选项并输入可以提供 iDRAC 对象的域名。

6. 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。
7. 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。
8. 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. 打开命令提示符并输入以下 RACADM 命令：
   - 使用 config 命令：
     ```
     racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
     cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
     cfgADRacName <RAC common name> racadm config -g cfgActiveDirectory -o
     cfgADRacDomain <fully qualified rac domain name> racadm config -g
     cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain name
     or IP Address of the domain controller> racadm config -g
     cfgActiveDirectory -o cfgADDomainController2 <fully qualified domain name
     or IP Address of the domain controller> racadm config -g
     cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain name
     or IP Address of the domain controller>
     ```
   - 使用 set 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>
     ```

   注: 您必须至少配置三个地址之一。iDRAC 逐一尝试连接到每个配置的地址，直到成功建立连接。使用扩展架构时，这些是此 iDRAC 设备所在位置域控制器的 FQDN 或 IP 地址。

   在 SSL 握手过程中禁用证书验证（可选）：

   - 使用 config 命令：`racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
   - 使用 set 命令：`racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

   注: 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）：

   - 使用 config 命令：`racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`

- 使用 **set** 命令：`racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

在此情况下，您必须上载 CA 证书：

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

注: 如果启用了证书验证，则指定域控制器服务器地址和 FQDN。请确保在 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）**下正确配置 DNS。

以下 RACADM 命令可选：

```
racadm sslcertdownload -t 0x1 -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 RACADM 命令：
   - 使用 **config** 命令：`racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
   - 使用 **set** 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 RACADM 命令：
   - 使用 **config** 命令：

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
     config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP
     address>
     ```
   - 使用 **set** 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，请输入以下命令：
   - 使用 **config** 命令：`racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>`
   - 使用 **set** 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。
5. 按 **Enter** 完成配置具有扩展架构的 Active Directory 的过程。

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**概览** → **iDRAC 设置** → **用户验证** → **目录服务** → **Microsoft Active Directory**。

   随即显示 **Active Directory** 摘要页面。
2. 单击 **Test Settings（测试设置）**。
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）**。将显示详细的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: 在选中“启用证书验证”的情况下测试 Active Directory 设置时，iDRAC 要求 Active Directory 服务器通过 FQDN 而不是 IP 地址进行标识。如果 Active Directory 服务器通过 IP 地址标识，则证书验证失败，原因是 iDRAC 无法与 Active Directory 服务器通信。

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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。此功能不需要在您的目录服务上进行任何架构扩展。

为了使 iDRAC LDAP 实施能够通用，应当利用不同目录服务之间的共性对用户进行分组，然后映射用户-组关系。特定于目录服务的操作是架构。例如，它们对于组、用户以及用户和组之间的链接可能具有不同的属性名称。这些操作可以在 iDRAC 中进行配置。

注: 通用 LDAP 目录服务不支持基于智能卡的双重验证 (TFA) 和单一登录 (SSO)。

相关任务

使用 iDRAC 基于 Web 的界面配置通用 LDAP 目录服务
使用 RACADM 配置通用 LDAP 目录服务

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**概览** → **iDRAC 设置** → **用户验证** → **目录服务** → **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 **Configure Generic LDAP**（**配置通用 LDAP**）。
3. 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 LDAP。
4. 单击**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。
5. 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 **Overview**（**概览**） → **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。固件将搜索该组的直接成员以匹配用户 DN。此外，仅支持单个域，不支持跨域。
6. 单击**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。

7. 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。

8. 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。

9. 如果要配置其他角色组，请重复第 7 步和第 8 步。
10. 单击 **Finish（完成）**。通用 LDAP 目录服务即配置完成。

使用 RACADM 配置通用 LDAP 目录服务

要配置 LDAP 目录服务，请执行以下操作：

- 将 **cfgLdap** 和 **cfgLdapRoleGroup** 组中的对象与 config 命令配合使用。
- 将 iDRAC.LDAP 和 iDRAC.LDAPRole 组中的对象与 set 命令配合使用。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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，转到**概览 → iDRAC 设置 → 用户验证 → 目录服务 → 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 **Test Settings（测试设置）**。
3. 输入测试 LDAP 的所选目录用户的用户名和密码。使用的格式取决于 *Attribute of User Login（用户登录的属性）*，且输入的用户名必须与所选属性的值匹配。

   注: 如果在选中**启用证书验证**的情况下测试 LDAP 设置，iDRAC 要求用 FQDN（而不是 IP 地址）来标识 LDAP 服务器。如果用 IP 地址来标识 LDAP 服务器，证书验证会失败，这是因为 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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

8

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，请访问 Microsoft 网站。

相关任务

为 Active Directory 用户配置 iDRAC SSO 登录
为本地用户配置 iDRAC 智能卡登录
为 Active Directory 用户配置 iDRAC 智能卡登录

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：

- 将 iDRAC 时间与 Active Directory 域控制器时间同步。如果不同步，iDRAC 上的 kerberos 验证失败。您可以使用时区和 NTP 功能同步时间。要实现这一点，请参阅配置时区和 NTP。
- 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**委派**选项卡上为 keytab 用户选中了**对任何服务的委派均信任此用户（仅限 Kerberos）**。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。

相关概念

配置浏览器以启用 Active Directory SSO

相关任务

将 iDRAC 注册为 Active Directory 根域中的计算机
生成 Kerberos Keytab 文件
创建 Active Directory 对象并提供权限

将 iDRAC 注册为 Active Directory 根域中的计算机

在 Active Directory 根域中注册 iDRAC：

1. 单击 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Network（网络）**。

随即会显示 **Network**（网络）页面。

2. 提供有效的 **Preferred/Alternate DNS Server（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。
3. 选择 **Register iDRAC on DNS（向 DNS 注册 iDRAC）**。
4. 提供有效 **DNS Domain Name（DNS 域名）**。
5. 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 Online Help*（iDRAC 联机帮助）。

生成 Kerberos Keytab 文件

要支持 SSO 和智能卡登录验证，iDRAC 应支持在 Windows Kerberos 网络中启用自身作为 Kerberos 服务的的配置。iDRAC 上的 Kerberos 配置涉及的步骤与配置非 Windows Server Kerberos 服务作为 Windows Server Active Directory 中安全主体的步骤相同。

ktpass 工具（可作为服务器安装 CD/DVD 的组成部分从 Microsoft 获得）用于创建用户帐户的服务主体名称 (SPN) 绑定并将信任信息导出到 MIT 格式的 Kerberos *keytab* 文件中，这将允许外部用户或系统与密钥分发中心 (KDC) 之间建立信任关系。keytab 文件包含加密密钥，用于加密服务器和 KDC 之间的信息。ktpass 工具允许支持 Kerberos 验证的基于 UNIX 的服务，从而可使用 Windows Server Kerberos KDC 服务提供的互操作性功能。有关 **ktpass** 公用程序的详细信息，请访问 Microsoft 网站：**technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

生成 keytab 文件之前，您必须创建一个 Active Directory 用户帐户与 `ktpass` 命令的 **-mapuser** 选项一起使用。此外，您必须拥有与上载生成的 keytab 文件使用的 iDRAC DNS 名称相同的名称。

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 **iDRACname** 和**服务主体名称**使用小写字母，对域名使用大写字母，如示例中所示。
3. 运行以下命令：

   ```
   C:\>setspn -a HTTP/iDRACname.domainname.com username
   ```

   将生成一个 keytab 文件。

   注: 如果发现为之创建 keytab 文件的 iDRAC 用户有任何问题，请创建新用户和新 keytab 文件。如果再次执行最初创建的同一 keytab 文件，则无法正确配置。

创建 Active Directory 对象并提供权限

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。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。

相关概念

[将 iDRAC 用户和权限添加到 Active Directory]

配置浏览器以启用 Active Directory SSO

本节提供 Internet Explorer 和 Firefox 的浏览器设置以启用 Active Directory SSO。

注: Google Chrome 和 Safari 不支持使用 Active Directory 进行 SSO 登录。

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**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。

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）。

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。

相关概念

[Active Directory 单一登录或智能卡登录的前提条件]

相关任务

[使用 iDRAC Web 界面配置具有标准架构的 Active Directory]
[使用 RACADM 配置具有标准架构的 Active Directory]
[使用 iDRAC Web 界面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]

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 名称是否匹配 iDRAC 完全限定域名。要实现此操作，请在 iDRAC Web 界面中，转至**概览 → iDRAC 设置 → 网络 → 网络**，然后查看 **DNS 域名**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 **Enable Single Sign-On**（**启用单一登录**）选项。

使用 RACADM 为 Active Directory 用户配置 iDRAC SSO 登录

除了配置 Active Directory 时执行的步骤之外，要启用 SSO，还需运行以下命令之一：

- 使用 config 命令：

  ```
  racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
  ```

- 使用 set 命令：

  ```
  racadm set iDRAC.ActiveDirectory.SSOEnable 1
  ```

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。

相关概念

获取证书
上载智能卡用户证书
启用或禁用智能卡登录

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。

相关概念

获取证书

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**概览 → iDRAC 设置 → 网络 → 用户验证 → 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 User Certificate**（**上载用户证书**），然后单击 **Next**（**下一步**）。

   将显示 **User Certificate Upload**（**用户证书上载**）页面。

4. 浏览并选择 Base64 用户证书，然后单击 **Apply**（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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。

相关概念

获取证书

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**概览** → **iDRAC 设置** → **网络** → **用户验证** → **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

要为智能卡登录上载受信 CA 证书，请使用 **usercertupload** 对象。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。有关选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

相关概念

启用或禁用智能卡登录
获取证书
生成 Kerberos Keytab 文件
使用 iDRAC Web 界面配置具有标准架构的 Active Directory
使用 RACADM 配置具有标准架构的 Active Directory

使用 iDRAC Web 界面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

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: 如果智能卡登录已启用，则 SSH、Telnet、LAN 上 IPMI、LAN 上串行和远程 RACADM 均已禁用。此外，如果您禁用智能卡登录，则接口不会自动启用。

相关概念

获取证书
为 Active Directory 用户配置 iDRAC 智能卡登录
为本地用户配置 iDRAC 智能卡登录

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**概览** → **iDRAC 设置** → **用户验证** → **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（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，请使用以下选项之一：

- 将 cfgSmartCard 组中的对象与 config 命令配合使用。
- 将 iDRAC.SmartCard 组中的对象与 set 命令配合使用。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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）**启用智能卡登录。否则，选择 **Disabled（已禁用）**。有关选项的详细信息，请参阅 *《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。

9

配置 iDRAC 以发送警报

您可以为受管系统上发生的特定事件设置警报和操作。当系统组件的状态超过预定义的条件时，就会发生某个事件。如果某个事件与已配置此筛选器生成警报（电子邮件、SNMP 陷阱、IPMI 警报、远程系统日志或 WS 事件）的事件筛选器相符，则会将警报发送到一个或多个配置的目标。如果还配置了让此筛选器执行某个操作（如重新引导、关机后再开机或关闭系统），则会执行该操作。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、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、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。

相关概念

启用或禁用警报
筛选警报
设置事件警报
设置警报复现事件
配置电子邮件警报、SNMP 陷阱或 IPMI 陷阱设置
配置远程系统日志记录
配置 WS 事件
警报消息 ID

启用或禁用警报

为了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。

相关概念

筛选警报
配置电子邮件警报、SNMP 陷阱或 IPMI 陷阱设置

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**概览** → **服务器** → **警报**。随即会显示**警报**页面。
2. 在 **Alerts**（警报）部分：
   - 选择 **Enable**（启用）以启用警报生成或执行事件操作。

- 选择 **Disable**（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。

使用 RACADM 启用或禁用警报

要启用或禁用生成警报或事件操作，请使用 config 命令：

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

要启用或禁用生成警报或事件操作，请使用 set 命令：

```
racadm set iDRAC.IPMILan.AlertEnable 1
```

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**平台事件**下，选择**启用**以启用警报或事件生成操作。否则，选择**禁用**。有关各选项的更多信息，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。

相关概念

[启用或禁用警报]
[配置电子邮件警报、SNMP 陷阱或 IPMI 陷阱设置]

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**概览** → **服务器** → **警报**。将显示**警报**页面。
2. 在 **Alerts Filter（警报过滤）**部分，选择下列一个或多个类别：
   - 系统运行状况
   - 存储
   - 配置
   - 审核
   - 更新
   - 工作注释
3. 选择下列一个或多个严重性等级：
   - 通知
   - 警告
   - Critical（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，可以使用 **eventfilters** 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。

相关概念

[启用或禁用警报](#)
[配置电子邮件警报、SNMP 陷阱或 IPMI 陷阱设置](#)
[筛选警报](#)
[配置远程系统日志记录](#)
[配置 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. 转至 **Overview（概述）** → **Server（服务器）** → **Alerts（警报）**。

   随即会显示 **Alerts**（警报）页面。
3. 在 **Alerts Results**（警报结果）下，选择以下所需事件的一个或所有警报：
   - 电子邮件警报
   - SNMP 陷阱
   - IPMI 警报
   - 远程系统日志
   - 操作系统日志
   - WS 事件
4. 单击应用。

   设置即会保存。
5. 在 **Alerts**（警报）部分，选择 **Enable**（启用）选项，将警报发送到配置的目标。
6. （可选）您可以发送测试事件。在 **Message ID to Test Event**（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 **Test**（测试）。有关消息 ID 的列表，请参阅 **dell.com/support/manuals** 上提供的 *Event Messages Guide*（事件消息指南）。

使用 RACADM 设置事件警报

要设置事件警报，可以使用 **eventfilters** 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

设置警报复现事件

如果系统持续在大于入口温度阈值限制的温度条件下工作，您可以配置 iDRAC 以便按照特定时间间隔生成附加事件。默认时间间隔是 30 天。有效范围是 0 到 366 天。值“0”指示无事件复现。

注: 您必须具有“配置 iDRAC”权限，才能设置警报复现值。

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**概览** → **服务器** → **警报** → **警报复现**。
   此时将显示**警报复现**页面。
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。

使用 RACADM 设置警报复现事件

要使用 RACADM 设置警报复现事件，可以使用 **eventfilters** 子命令。有关更多信息，请参阅 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。

相关概念

筛选警报
启用或禁用警报

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**概览** → **服务器** → **警报**。将显示**警报**页面。
2. 在**警报结果**下，从**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，请使用以下选项之一：

- eventfilters 命令。
- 将 cfgIpmiPefAction 对象与 config 命令配合使用。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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) 和智能平台管理界面 (IPMI) 陷阱接收 iDRAC 的数据。对于具有大量节点的系统，管理站对于可能发生的每种情况轮询每个 iDRAC 时，效率可能比较低下。例如，事件陷阱可以通过平衡节点之间的负载或在发生验证故障时发出警报来帮助管理站。可支持 SNMP v1、v2 和 v3 格式。

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。也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。

相关概念

[配置 IP 警报目标]
[配置电子邮件警报设置]

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.com/support/manuals** 上提供的 *SNMP Reference Guide for iDRAC8*（适用于 iDRAC8 的 SNMP 参考指南）。

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. 转至 **Overview（概述）** → **Server（服务器）** → **Alerts（警报）** → **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。
   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 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。请确保目的地团体字符串与 iDRAC 团体字符串相同。默认值为 Public。
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，而不适用于 IPMI 陷阱。IPMI 陷阱始终以 SNMP v1 格式而不是基于配置的 **SNMP Trap Format**（SNMP 陷阱格式）选项发送。

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：
   - 对于 IPv4 地址：
     `racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i (索引) (0|1)`
   - 对于 IPv6 地址：
     `racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i (索引) (0|1)`

   其中，(索引) 是目标索引，0 或 1 分别禁用或启用陷阱。

   例如，要启用具有索引 4 的陷阱，请输入以下命令：

   `racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1`
2. 配置陷阱目标地址：

   `racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i [索引] [IP 地址]`

   其中 `[索引]` 是陷阱目标索引，而 `[IP-address]` 是接收平台事件警报的系统的目标 IP 地址。
3. 配置 SNMP 公共名称字符串：

   `racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [名称]`

   其中 `[name]` 是 SNMP 公共名称。
4. 要配置 SNMP 目标：
   - 要设置 SNMPv3 的 SNMP 陷阱目标：

     `racadm set idrac.SNMP.Alert.[index].DestAddr [Ip address]`

     例如：

     `racadm set idrac.SNMP.Alert.1.DestAddr 1.2.3.4`
   - 要为陷阱目标设置 SNMPv3 用户：

     `racadm set idrac.SNMP.Alert.1.SNMPv3Username root`
   - 要为用户启用 SNMPv3：

     `racadm set idrac.users.2.SNMPv3Enable Enabled`
5. 如有必要，请测试陷阱：

   `racadm testtrap -i [索引]`

   其中 `[索引]` 是要测试的陷阱目标索引。

   有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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）。要实现这一点，请：

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

您可以配置电子邮件地址以接收电子邮件警报。还可以配置 SMTP 服务器地址设置。

注: 如果邮件服务器是 Microsoft Exchange Server 2007，请确保为邮件服务器配置 iDRAC 域名，以便从 iDRAC 接收电子邮件警报。

注: 电子邮件警报支持 IPv4 和 IPv6 地址。使用 IPv6 时必须指定 DRAC DNS 域名。

相关概念

[配置 SMTP 电子邮件服务器地址设置]

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. 转至 **Overview**（概述） → **Server**（服务器） → **Alerts**（警报） → **SNMP and Email Settings**（SNMP 和电子邮件设置）。
2. 选择**状态**选项以启用要接收警报的电子邮件地址并键入有效的电子邮件地址。有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击 **Test Email**（测试电子邮件）下的 **Send**（发送）测试配置的电子邮件警报设置。
4. 单击**应用**。

使用 RACADM 配置电子邮件警报设置

要配置电子邮件警报设置，请执行以下操作：

1. 要启用电子邮件警报，请执行以下操作：
   - 使用 config 命令：

     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [index] [0|1]
     ```

     其中，`[index]` 是电子邮件目标索引。0 会禁用电子邮件警报，1 会启用警报。

     电子邮件目标索引可以是 1 到 4 的值。例如，要使用索引 4 启用电子邮件，请输入以下命令：

     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
     ```
   - 使用 set 命令：

     ```
     racadm set iDRAC.EmailAlert.Enable.[index] 1
     ```

     其中，`[index]` 是电子邮件目标索引。0 会禁用电子邮件警报，1 会启用警报。

     电子邮件目标索引可以是 1 到 4 的值。例如，要使用索引 4 启用电子邮件，请输入以下命令：

     ```
     racadm set iDRAC.EmailAlert.Enable.4 1
     ```
2. 要配置电子邮件设置，请执行以下操作：
   - 使用 config 命令：

     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 [email-
     address]
     ```

其中，1 是电子邮件目标索引，`[email-address]` 是接收平台事件警报的目标电子邮件地址。

- 使用 **set** 命令：

  ```
  racadm set iDRAC.EmailAlert.Address.1 [email-address]
  ```

  其中，1 是电子邮件目标索引，`[email-address]` 是接收平台事件警报的目标电子邮件地址。

3. 配置自定义信息：

   - 使用 **config** 命令：

     ```
     racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i [index]
     [custom-message]
     ```

     其中 `[index]` 是电子邮件目标索引，而 `[custom-message]` 是自定义消息。

   - 使用 **set** 命令：

     ```
     racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
     ```

     其中 `[index]` 是电子邮件目标索引，而 `[custom-message]` 是自定义消息。

4. 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]
   ```

   其中 `[index]` 是要测试的电子邮件目标索引。

   有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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**概览** → **服务器** → **警报** → **SNMP 和电子邮件设置**。
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，请使用以下命令之一：

- 使用 **set** 命令：

  ```
  racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP
  Address>
  ```

- 使用 **config** 命令：

  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP E-mail
  Server IP Address>
  ```

配置 WS 事件

WS 事件协议用于客户端服务（订阅者）向服务器（事件来源）注册感兴趣的项目（订阅），以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 事件消息的客户端可以使用 iDRAC 订阅并接收与 Lifecycle Controller 作业相关的事件。

配置 WS 事件功能以接收与 Lifecycle Controller 作业有关的更改的 WS 事件消息所需的步骤将在 iDRAC 1.30.30 规范说明文件中的“Web 服务事件支持”中进行介绍。除了此规范之外，有关 WS 事件协议的完整信息，请参阅 DSP0226（DMTF WS 管理规范）第 10 部分“通知（事件）”说明文件。与 Lifecycle Controller 有关的作业在“DCIM 作业控制配置文件”说明文件中进行介绍。

监测机箱事件

在 PowerEdge FX2/FX2s 机箱上，您可以在 iDRAC 中启用**机箱管理和监测**设置来执行机箱管理和监测任务，例如监测机箱组件、配置警报、使用 iDRAC RACADM 传递 CMC RACADM 命令以及更新机箱管理固件。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**，以便转发机箱事件。默认情况下，此设置已设置为**已启用**。

注: 为让此设置生效，必须确保在 CMC 中，将**服务器模式下的机箱管理**设置设为**监测**或**管理和监测**。

当**机箱管理和监测**选项设置为**已启用**时，iDRAC 会生成和记录机箱事件。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 还可将生成的事件转发到 iDRAC。如果服务器上的 iDRAC 不起作用，则 CMC 会对前 16 个事件排队，并在 CMC 日志中记录其余的事件。在将**机箱监测**设置为“已启用”后，系统会立即将这 16 个事件发送到 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。

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**机箱概览 → 设置 → 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**概览 → 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

注: 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 监测机箱事件，请运行 `racadm get system.chassiscontrol.chassismanagementmonitoring` 命令。有关更多信息，请参阅 **dell.com/**

idracmanuals 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

警报消息 ID

下表提供了显示警报的信息 ID 的列表。

表. 23: 警报信息 ID

信息 ID	说明
AMP	Amperage
ASR	自动系统重设
BAR	备份/还原
BAT	电池事件
BIOS	BIOS 管理
BOOT	引导控制
CBL	电缆
CPU	处理器
CPUA	处理器不存在
CTL	存储控制
DH	证书管理
DIS	自动查找
ENC	存储机柜
FAN	风扇事件
FSD	Debug（调试）
HWC	硬件配置
IPA	DRAC IP 更改
ITR	侵入
JCP	作业控制
LC	Lifecycle Contr（Lifecycle 控制器）

信息 ID	说明
LIC	许可
LNK	链路状态
LOG	日志事件
MEM	内存
NDR	NIC 操作系统驱动程序
NIC	NIC 配置
OSD	操作系统部署
OSE	操作系统事件
PCI	PCI 设备
PDR	物理磁盘
PR	部件交换
PST	BIOS 开机自检
PSU	电源设备
PSUA	PSU 不存在
PWR	电源使用
RAC	RAC 事件
RDU	冗余
RED	固件下载
RFL	IDSDM 介质
RFLA	IDSDM 不存在
RFM	FlexAddress SD
RRDU	IDSDM 冗余
RSI	远程服务
SEC	安全事件
系统事件日志	系统事件日志

信息 ID	说明
SRD	软件 RAID
SSD	PCIe SSD
STOR	存储
SUP	固件更新作业
SWC	软件配置
SWU	软件更改
SYS	系统信息
TMP	温度
TST	测试警报
UEFI	UEFI 事件
USR	用户跟踪
VDR	虚拟磁盘
VF	vFlash SD 卡
VFL	vFlash 事件
VFLA	vFlash 不存在
VLT	电压
VME	虚拟介质
VRM	虚拟控制台
WRK	工作注释

10 管理日志

iDRAC 提供包含系统、存储设备、网络设备、固件更新、配置更改、许可证信息等相关事件的 Lifecycle 日志。不过，系统事件同时作为名为系统事件日志 (SEL) 的单独日志提供。Lifecycle 日志通过 iDRAC Web 界面、RACADM 和 WS-MAN 界面可访问。

Lifecycle 日志的大小达到 800 KB 时，日志将压缩并存档。您只能查看未存档的日志条目，并对未存档日志应用筛选器和注释。要查看存档的日志，您必须将整个 Lifecycle 日志导出到系统中的某一位置。

相关概念

- 查看系统事件日志
- 查看 Lifecycle 日志
- 导出 Lifecycle Controller 日志
- 添加工作注释
- 配置远程系统日志记录

查看系统事件日志

当受管系统上发生系统事件时，将记录在 System Event Log（系统事件日志，SEL） 中。相同的 SEL 条目还可以在 LC 日志中找到。

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**概览 → 服务器 → 日志**。

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: 如果使用的是 Internet Explorer，并且在保存时遇到问题，请下载 Internet Explorer 的累积安全更新。您可以从 Microsoft 支持网站 **support.microsoft.com** 下载。

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，将在 Lifecycle Controller 日志中记录一个条目。该日志条目中包含已从中清除 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，请使用命令：`racadm getsel -i`

要清除 SEL 条目，请使用命令：`racadm clrsel`

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。要实现这一点，请：

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。它提供以下各项相关事件的日志：

- 存储设备
- 系统事件
- 网络设备
- 配置
- 审核
- 更新
- 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：

- Telnet
- SSH
- Web 界面
- RACADM
- SM-CLP
- IPMI Over LAN（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筛选日志，查看、导出工作注释并将其添加到日志事件。

相关任务

筛选 Lifecycle 日志

[使用 Web 界面导出 Lifecycle Controller 日志](#)
[将备注添加到 Lifecycle 日志](#)

使用 Web 界面查看 Lifecycle 日志

要查看 Lifecycle 日志，请单击**概览** → **服务器** → **日志** → **Lifecycle** 日志。随即会显示 **Lifecycle** 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**。
   筛选的日志条目将在 **Log Results**（日志结果）中显示。

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 **ddell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

导出 Lifecycle Controller 日志

您可以将单个压缩 XML 文件中的全部 Lifecycle Controller 日志（活动条目和存档条目）导出到网络共享或本地系统。压缩的 XML 文件的扩展名为 .xml.gz。文件条目将按照其序列号顺序（从最低序列号到最高序列号）排序。

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

要使用 RACADM 导出 Lifecycle Controller 日志，请使用 `lclog export` 命令。有关更多信息，请参阅 **dell.com/support/manuals** 或 **dell.com/esmmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

添加工作注释

登录到 iDRAC 的每个用户都可以添加工作注释，工作注释会作为事件存储在 lifecycle 日志中。您必须具有 iDRAC 日志权限才能添加工作注释。每条新的工作注释最多支持 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**概览** → **服务器** → **属性** → **摘要**。
   随即会显示 **System Summary（系统摘要）**页面。
2. 在 **Work Notes（工作注释）**下，在空白文本框中输入文本。

   注: 建议不要使用过多特殊字符。
3. 单击 **Add**（添加）。
   工作注释即会添加到日志。有关详细信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

配置远程系统日志记录

您可以向远程系统发送 Lifecycle 日志。执行此操作之前，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**概览** → **服务器** → **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，并指定服务器地址以及端口号。有关各选项的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
3. 单击**应用**。
   设置即会保存。写入 lifecycle 日志的所有日志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 syslog 服务器设置，请使用以下选项之一：

- 将 cfgRemoteHosts 组中的对象与 config 命令配合使用。
- 将 iDRAC.SysLog 组中的对象与 set 命令配合使用。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

11

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：

- **Power Monitoring（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。
- **Power Capping（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。
- **Power Control（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。

相关概念

监测功率
执行电源控制操作
功率限额
配置电源设备选项
启用或禁用电源按钮
设置功耗的警告阈值

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: 系统功耗趋势（每小时、每天、每周）直方图仅当 iDRAC 运行时才绘制。如果 iDRAC 重新启动，现有功耗数据将丢失，直方图重新开始绘制。

使用 Web 界面监测功率

要查看电源监测信息，请在 iDRAC Web 界面中，转至**概览 → 服务器 → 电源/散热 → 电源监测**。随即会显示**电源监测**页面。有关更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

使用 RACADM 监测功率

要查看功率监测信息，请将 **System.Power** 组对象与 **get** 命令配合使用，或者将 **cfgServerPower** 对象与 **getconfig** 命令配合使用。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

设置功耗的警告阈值

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。

对应于刀片服务器系统的功率警告阈值将设置为 CMC 电源分配。

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: 执行 racreset 或 iDRAC 更新后，警告阈值的值重设为默认值。

使用 Web 界面设置功耗警告阈值

1. 在 iDRAC Web 界面中，转至**概览 → 服务器 → 电源/散热 → 电源监测**。
   此时将显示**功率监测**页面。
2. 在**现有功耗读数和阈值**部分的**警告阈值**列中，输入以**瓦特**或 **BTU/hr** 为单位的值。
   这些值必须低于**故障阈值**。这些值将舍入到最接近的可被 14 整除的值。如果输入**瓦特**，系统将自动计算并显示 **BTU/hr** 值。类似地，如果输入 BTU/hr，则会显示**瓦特**值。
3. 单击**应用**。已配置值。

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 WS-Management 执行这些操作。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *Lifecycle Controller Remote Services Quick Start Guide*（Lifecycle Controller Remote Services 快速入门指南）和 **delltechcenter.com** 上提供的 *Dell Power State Management*（Dell 电源状态管理）配置文件说明文件。

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**概览 → 服务器 → 电源/散热 → 电源配置 → 电源控制**。随即会显示**电源控制**页面。
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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。这是一个获得许可证的功能。

刀片服务器中的功率上限

在 PowerEdge M1000e 或 PowerEdge VRTX 机箱中的刀片服务器启动前，iDRAC 提供 CMC 所需要的功率要求。该功率高于刀片消耗的实际功率，并且根据有限的硬件资源清册信息进行计算。当服务器启动后，根据服务器的实际功耗，它需要的功率范围可能会变小。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 可能会请求增加最大可能功耗，从而增大功率范围。iDRAC 仅增加 CMC 的最大可能功耗请求。如果功耗减少，它不会请求减小最小可能功率。如果功耗超出 CMC 分配的功率，iDRAC 会继续请求增加功率。

系统启动并初始化后，iDRAC 会根据实际刀片配置计算新的功率要求。即使 CMC 分配新的功率要求失败，刀片仍然会保持电源开启。

CMC 从低优先级服务器回收任何未用功率，然后分配给较高优先级的基础架构模块或服务器。

如果分配的功率不足，刀片服务器不会开启。如果分配给刀片的功率足够，iDRAC 会开启系统电源。

查看和配置功率上限策略

如果启用功率封顶策略，它会对系统强制执行用户定义的功率限制。如果不启用，它会使用默认实施的硬件功率保护策略。该功率保护策略与用户定义的策略相互独立。系统性能会进行动态调整，以保持功率消耗与指定的阈值相近。

对于小负荷，实际功耗可能较小，但瞬时功率可能超出阈值，直到性能调整完成。例如，对于给定的系统配置，最大可能功率消耗为 700W，而最小可能功率消耗为 500W。您可以指定并启用 Power Budget Threshold（功率预算阈值），从而将消耗从当前的 650W 降低到 525W。从此时起，系统的性能会进行动态调整，从而保持功率消耗，以免超出用户指定的阈值 525W。

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 设置功率封顶阈值时，转换为以瓦特为单位的值会舍入为最接近的整数。当读回功率封顶阈值时，从瓦特转换为 BTU/hr 会再次以这种方式进行舍入。因此，写入的值通常与读取的值不同，例如，设置为 600 BTU/hr 的阈值在读回时为 601 BTU/hr。

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**概览** → **服务器** → **电源/散热** → **电源配置** → **电源配置**。随即会显示**电源配置**页面。

   显示 **Power Configuration**（电源配置）页面后，当前电源策略限制会显示在 **Currently Active Power Cap Policy**（当前活动电源限额策略）部分下。
2. 在 **iDRAC Power Cap Policy（iDRAC 电源限额策略）**下选择 **Enable（启用）**。
3. 在 **User-Defined Limits**（用户定义的限制）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 **Apply**（应用）以应用该值。

使用 RACADM 配置功率上限策略

查看和配置当前功率限额值：

- 将以下对象配合 **config** 子命令使用：
  - cfgServerPowerCapWatts
  - cfgServerPowerCapBTUhr
  - cfgServerPowerCapPercent
  - cfgServerPowerCapEnable
- 将以下对象配合 **set** 子命令使用：
  - 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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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。

热备用是电源设备功能，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。

在包含两个 PSU 的系统中，PSU1 或 PSU2 都可以配置为主 PSU。在包含四个 PSU 的系统中，必须设置 PSU (1+1 或 2+2) 对作为主 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。

功率因数是消耗的实际功率与视在功率之比。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**概览** → **服务器** → **电源/散热** → **电源配置** → **电源配置**。将显示**电源配置**页面。
2. 在**电源设备选项**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 **Apply（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 **set** 子命令使用：

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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 power factor correction（功率因数校正）。有关此选项的更多信息，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**（启用）以启用电源按钮。否则，请选择 **Disabled**（禁用）。
3. 依次单击 **Back**（上一步）、**Finish**（完成）和 **Yes**（是）。设置即保存。

12 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）

相关概念

[资源清册和监测 FC HBA 设备]
[动态配置虚拟地址、启动器和存储目标设置]

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，您可以查看端口和支持分区的以下信息：

- 链路状态
- 属性
- 设置和功能
- Receive and Transmit Statistics（接收和传送统计数据）

相关概念

[对网络设备执行资源清册、监测和配置操作]
[动态配置虚拟地址、启动器和存储目标设置]

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**概览** → **硬件** → **网络设备**。随即会显示**网络设备**页面。有关所显示属性的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

注: 如果 **OS Driver State**（**操作系统驱动程序状态**）显示的状态为 Operational（可操作），它会指示操作系统驱动程序状态或 UEFI 驱动程序状态。

使用 RACADM 监测网络设备

要查看网络设备信息，请使用 **hwinventory** 和 **nicstatistics** 命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

除了 iDRAC Web 界面中显示的属性以外，使用 RACADM 或 WS-MAN 时还可能显示其他属性。

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信道主机总线适配器 (FC HBA) 设备的运行状况并查看其资源清册。系统支持 Emulex 和 QLogic FC HBA。对于每个 FC HBA 设备，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）

相关概念

[对网络设备执行资源清册、监测和配置操作]

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**概览** → **硬件** → **光纤信道**。此时将显示 FC 页面。有关所显示属性的更多信息，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** 子命令。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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，以及应用持久性策略。此功能允许应用程序根据电源状态变更（即，操作系统重新启动、热重设、冷重设或 AC 重启），以及根据该电源状态对应的持久性策略设置来应用设置。通过此功能，可为需要向另一个系统快速重新配置系统负载的部署提供更高的灵活性。

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，所有虚拟地址将重设为出厂设置的默认永久地址。

注: 在具有虚拟 FIP、虚拟 WWN 和虚拟 WWPN MAC 属性的卡上，虚拟 WWN 和虚拟 WWPN MAC 属性会在您配置虚拟 FIP 时自动配置。

通过使用 IO 标识功能，您可以执行以下操作：

- 查看和配置网络设备的虚拟地址（例如，NIC、CNA、FC HBA）
- 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。

仅当已启用 I/O 标识功能时，持久性策略才会生效。在系统每次重设或开机时，将根据策略设置保留或清除值。

相关概念

[对网络设备执行资源清册、监测和配置操作]
[支持 I/O 标识优化功能的卡]
[支持 I/O 标识优化功能的 BIOS 版本]
[支持 I/O 标识优化功能的 NIC 固件版本]
[启用或禁用 I/O 标识优化功能]
[配置持久性策略设置]

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。

制造商	类型
Broadcom	• 5720 PCIe 1 GB • 5719 PCIe 1 GB • 57810 PCIe 10 GB • 57810 bNDC 10 GB • 57800 rNDC 10 GB + 1 GB • 57840 rNDC 10 GB • 57840 bNDC 10 GB • 5720 rNDC 1 GB • 5719 夹层卡 1 GB • 57810 夹层卡 10 GB • 5720 bNDC 1 GB
Intel	• i350 夹层卡 1 GB • x520+i350 rNDC 10GB+1GB • I350 bNDC 1GB • x540 PCIe 10GB • x520 PCIe 10GB • i350 PCIe 1GB • x540+i350 rNDC 10GB+1GB • i350 rNDC 1GB • x520 bNDC 10GB • 40G 2P XL710 QSFP+ rNDC
Mellanox	• ConnectX-3 10G • ConnectX-3 40G • ConnectX-3 10G • ConnectX-3 Pro 10G • ConnectX-3 Pro 40G

制造商	类型
	• ConnectX-3 Pro 10G
Qlogic	• QME2662 夹层卡 FC16 • QLE2660 PCIe FC16 • QLE2662 PCIe FC16
Emulex	• LPM16002 夹层卡 FC16 • LPe16000 PCIe FC16 • LPe16002 PCIe FC16 • LPM16002 夹层卡 FC16 • LPM15002 • LPe15000 • LPe15002 • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104-UX-D rNDC 10GB • OCm14102-U2-D bNDC 10GB • OCm14102-U3-D 夹层卡 10GB • Ce14102-UX-D PCIe 10GB

注: 以下插卡不支持 I/O 标识优化：

- Intel x520 夹层卡 10 GB

支持 I/O 标识优化功能的 BIOS 版本

在第 13 代 Dell PowerEdge 服务器中，默认情况下已提供必需的 BIOS 版本。

下表提供了在第 12 代 PowerEdge 服务器上支持的最低 BIOS 版本。

Dell PowerEdge 第 12 代服务器	支持的最低 BIOS 版本
R720、R720xd、R620、T620 和 M620	2.1.0
R820	2.0.15
R520、R320、R420、T420、T320、M520 和 M420	2.0.19
M820	1.7.0

支持 I/O 标识优化功能的 NIC 固件版本

在第 13 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。

制造商	支持的 NIC 固件版本
Broadcom 卡	7.8.x
Intel 卡	15.0.x
QLogic 82xx (CNA)	6.0.0.x 1.13.x/

iDRAC 设置为 Flex Address 模式或控制台模式时的虚拟地址/Flex Address 和持久性策略行为

下表根据 CMC 中的 Flex Address 功能状态、iDRAC 中设置的模式、iDRAC 中的 IO 标识 功能状态以及 XML 配置，描述虚拟地址管理 (VAM) 配置和持久性策略行为。

CMC 中的 Flex Address 功能状态	**iDRAC 中设置的模式**	**IO 标识在 iDRAC 中的功能状态**	**XML 配置**	**持久性策略**	**清除持久性策略 - 虚拟地址**
Flex Address 已启用	FlexAddress 模式	Enabled（已启用）	虚拟地址管理 (VAM) 已配置	配置的 VAM 仍然存在	设置为 Flex Address
Flex Address 已启用	FlexAddress 模式	Enabled（已启用）	未配置 VAM	设置为 Flex Address	无持久性 - 设置为 Flex Address
Flex Address 已启用	FlexAddress 模式	已禁用	使用 Lifecycle Controller 中提供的路径配置	设置为该周期的 Flex Address	无持久性 - 设置为 Flex Address
Flex Address 已启用	FlexAddress 模式	已禁用	未配置 VAM	设置为 Flex Address	设置为 Flex Address
Flex Address 已禁用	FlexAddress 模式	Enabled（已启用）	VAM 已配置	配置的 VAM 仍然存在	仅限持久性 - 不能清除
Flex Address 已禁用	FlexAddress 模式	Enabled（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
Flex Address 已禁用	FlexAddress 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
Flex Address 已禁用	FlexAddress 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
Flex Address 已启用	控制台模式	Enabled（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
Flex Address 已启用	控制台模式	Enabled（已启用）	未配置 VAM	设置为硬件 MAC 地址	设置为硬件 MAC 地址
Flex Address 已启用	控制台模式	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

CMC 中的 Flex Address 功能状态	iDRAC 中设置的模式	IO 标识在 iDRAC 中的功能状态	XML 配置	持久性策略	清除持久性策略 - 虚拟地址
Flex Address 已禁用	控制台模式	Enabled（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
Flex Address 已禁用	控制台模式	Enabled（已启用）	未配置 VAM	设置为硬件 MAC 地址	设置为硬件 MAC 地址
Flex Address 已禁用	控制台模式	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
Flex Address 已启用	控制台模式	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 I/O 标识的系统行为

	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	Enabled（已启用）	已禁用		从 CMC FlexAddress	根据 FlexAddress 规格
	不适用，已启用或已禁用	Enabled（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	Enabled（已启用）	已禁用		从 CMC FlexAddress	根据 FlexAddress 规格
	Enabled（已启用）	Enabled（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	Enabled（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

通常将在系统引导后配置设备，然后在重新引导后初始化设备。您可以启用“I/O 标识优化”功能以实现引导优化。如果此功能已启用，它会在设备重设之后和初始化之前设置虚拟地址、发起程序和存储目标属性，因而无需第二次重新启动 BIOS。设备配置和引导操作通过启动一次系统完成，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 和网卡已更新至最新固件。有关受支持的版本信息，请参阅支持 I/O 标识优化功能的 BIOS 版本和支持 I/O 标识优化功能的 NIC 固件版本。

启用 I/O 标识优化功能后，从 iDRAC 导出 XML 配置文件，在 XML 配置文件中修改所需的 I/O 属性，然后将此文件重新导入 iDRAC。

有关 XML 配置文件中可修改的 I/O 标识优化功能属性的列表，请参阅 **delltechcenter.com/idrac** 上提供的 *NIC Profile*（NIC 配置文件）说明文件。

注: 不要修改非 I/O 标识优化功能属性。

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 **Overview**（概览） → **Hardware**（硬件） → **Network Devices**（网络设备）。

   将显示**网络设备**页面。
2. 单击 **I/O 标识优化**选项卡，选择 **I/O 标识优化**选项以启用此功能。要禁用此功能，请清除此选项。
3. 单击**应用**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
```

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。对于辅助供电设备与非辅助供电设备，设备的行为将有所不同。

注: Dell PowerEdge FX2/FX2s 机箱中的 PCIe 设备不支持 IO 标识及 IO 标识持久性策略配置。

注: 如果在 iDRAC 上将 **VirtualAddressManagement** 属性设置为 **FlexAddress** 模式，并且在 CMC 中禁用 FlexAddress 功能，则在**持久性策略**被设置为默认值时，该功能可能不起作用。请确保在 iDRAC 中将 **VirtualAddressManagement** 属性设置为**控制台**模式，或者在 CMC 中启用 FlexAddress 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。

为 SNMP、电子邮件或 WS 事件处理通知启用事件操作。日志也包括在远程系统日志中。

持久性策略的默认值

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

相关概念

启用或禁用 I/O 标识优化功能

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 **Overview（概览）** → **Hardware（硬件）** → **Network Devices（网络设备）**。

   将显示**网络设备**页面。
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：
   - **AC 断电** - 在发生 AC 断电情况时保留虚拟地址或目标设置。
   - **冷引导** - 在发生冷重设时保留虚拟地址或目标设置。
   - **热引导** - 在发生热重设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 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC RACADM 命令行界面参考指南）。

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. 24: iSCSI 启动器 - 默认值

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
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

iSCSI 启动器	IPv4 模式下的默认值	IPv6 模式下的默认值
IscsiInitiatorChapPwd	已清除值	已清除值
IPVer	Ipv4	

表. 25: 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	

13

管理存储设备

在 iDRAC 2.00.00.00 版本中，iDRAC 扩展了其无代理管理，其中包括直接配置新 PERC9 控制器的功能。通过该功能，您可以远程配置在运行时连接到系统的存储组件。这些组件包括 RAID 和非 RAID 控制器、信道、端口、机柜、端口和已连接到它们的磁盘。

综合嵌入式管理 (CEM) 框架中随附了完整的存储子系统查找、拓扑、运行状况监测和配置，这是通过使用 I2C 接口上的 MCTP 协议与内外部 PERC 控制器交互实现的。对于实时配置，CEM 支持 PERC9 控制器。PERC9 控制器的固件版本必须为 9.1 或更高版本。

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。

您可以配置和管理控制器功能，而无需访问 BIOS。这些功能包括配置虚拟磁盘，以及应用 RAID 级别和热备用以保护数据。您可以启动许多其他控制器功能（例如重建及故障排除）。您可通过配置数据冗余和分配热备用来保护数据。

存储设备包括：

- 控制器 - 大多数操作系统不直接从磁盘中读写数据，而会向控制器发送读写指令。系统中的控制器硬件直接与磁盘交互以写入和检索数据。控制器具有一些连接器（信道或端口），这些连接器连接到一个或多个物理磁盘或含有物理磁盘的机柜。RAID 控制器可跨越磁盘边界以创建更多存储空间容量（或虚拟磁盘），以使用多个磁盘的容量。控制器还能执行其他任务，例如启动重建操作和初始化磁盘等。要完成任务，控制器需要一些称为固件和驱动程序的特殊软件。要正常工作，控制器必须安装所需的最低固件和驱动程序版本。不同的控制器在读写数据和执行任务方面具有不同的特性。这将有助于您了解这些功能，以便最高效地管理存储。
- 物理磁盘或物理设备 - 位于机柜内部或与控制器相连。在 RAID 控制器上，物理磁盘或设备用于创建虚拟磁盘。
- 虚拟磁盘 - 是 RAID 控制器从一个或多个物理磁盘创建的存储空间。虽然虚拟磁盘可能由多个物理磁盘创建，但是操作系统将它视为一个磁盘。根据所用的 RAID 级别，虚拟磁盘可以在发生磁盘故障时保留冗余数据或者具有特定的性能属性。虚拟磁盘仅能在 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 - 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，但不具备与外部机柜相关的管理功能（如温度探测器和警报等）。物理磁盘可以包含在机柜中，也可以连接到系统背板上。

除了管理机柜中包含的物理磁盘，您还可以监测机柜中风扇、电源设备和温度探测器的状态。可以热插拔机柜。热插拔指的是在操作系统仍在运行的情况下将组件添加到系统。

连接到控制器的物理设备必须具有最新的固件。有关最新支持的固件，请联系您的服务提供商。

PERC 中的存储事件将映射到 SNMP 陷阱和 WSMAN 事件（如果适用）。将在 Lifecycle 日志中记录对存储配置所做的任何更改。

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	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。 如果该控制器具有挂起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”方式不需要重新引导系统。	将应用配置。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

相关概念

- 理解 RAID 概念
- 资源清册和监测存储设备
- 查看存储设备拓扑
- 管理控制器
- 管理物理磁盘
- 管理机柜或背板
- 管理 PCIe SSD
- 管理虚拟磁盘
- 闪烁或取消闪烁组件 LED

相关参考资料

- 支持的控制器
- 支持的机柜
- 支持的存储设备功能的摘要

理解 RAID 概念

Storage Management 采用独立磁盘冗余阵列 (RAID) 技术提供存储管理功能。要理解 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系统上的磁盘空间。

什么是 RAID？

RAID 是管理将存在的或连接到系统的物理磁盘上数据存储的技术。RAID 的一个重要特点是能够跨接多个物理磁盘，以使多个物理磁盘的合并存储容量可以视为一个扩展的磁盘空间。RAID 的另一个重要特点是能够保存冗余数据，可以在磁盘故障的时候用来恢复数据。RAID 使用不同的技术（比如分条、镜像和奇偶校验）来存储和重新构建数据。有各种不同的 RAID 级别使用不同的方法来存储和重新构建数据。各个 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点。并不是所有的 RAID 级别都存有冗余数据，这意味着有些 RAID 级别在丢失数据后无法恢复。您选择的 RAID 级别取决于您侧重于性能、保护，还是存储容量。

注: RAID Advisory Board (RAB) 定义实现 RAID 所用的规格。虽然 RAB 定义了 RAID 级别，但不同供应商的 RAID 级别商业实现与实际 RAID 规格可能有所不同。由特定供应商提供的实现方案可能会影响到读写性能和数据冗余的程度。

硬件和软件 RAID

RAID 既可以使用硬件也可以使用软件来实现。使用硬件 RAID 的系统具有一个 RAID 控制器，在物理磁盘上实现 RAID 级别并处理数据读写。使用操作系统提供的软件 RAID 时，操作系统实施 RAID 级别。因此，只是本身使用软件 RAID 会降低该系统的性能。但是，可以结合硬件 RAID 卷使用软件 RAID，从而提供更好的性能并且在 RAID 卷配置方面具有更大的灵活性。例如，可以跨越两个 RAID 控制器来镜像一对硬件 RAID 5 卷，从而提供 RAID 控制器冗余。

RAID 概念

RAID 使用特定的技术来将数据写到磁盘。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 — 从一个物理磁盘复制数据到另一个物理磁盘。镜像通过在不同物理磁盘上保存相同数据的两个备份来实现数据冗余。如果镜像中的一个磁盘发生故障，系统可以通过使用未受影响的磁盘来继续工作。镜像的两端始终保存相同的数据。镜像的任何一端都可充当可运行端。镜像 RAID 磁盘组与 RAID 5 磁盘组在读操作方面性能相当，但是在写操作方面性能更好。
- 分条 — 磁盘分条在虚拟磁盘中的所有物理磁盘上写入数据。每个条带都包含连续的虚拟磁盘数据地址，使用顺序模式以固定大小单位映射到虚拟磁盘中的各个物理磁盘。例如，如果虚拟磁盘包含五个物理磁盘，条带会将数据写入物理磁盘一至五而不重复在某个物理磁盘上写入。条带在每个物理磁盘上使用的空间大小相同。物理磁盘上的条带部分是一个元素带。分条自身并不提供数据冗余。分条与奇偶校验同时使用就能够实现数据冗余。
- 条带大小 — 条带使用的总磁盘空间（不包括奇偶校验磁盘）。例如，假设条带包含 64 KB 磁盘空间并且条带中每个磁盘上有 16 KB 数据。在这种情况下，条带大小是 64 KB，而元素带大小是 16 KB。
- 元素带 — 元素带是位于单个物理磁盘上的条带部分。
- 元素带大小 — 元素带使用的磁盘空间量。例如，假设条带包含 64 KB 磁盘空间并且条带中每个磁盘上有 16 KB 数据。在这种情况下，元素带大小是 16 KB，而条带大小是 64 KB。
- 奇偶校验 — 奇偶校验是指通过使用某个算法与分条一起保存的冗余数据。如果其中的一个分条磁盘发生故障，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 级别都采用镜像、分条和奇偶校验的一定组合，从而实现数据冗余或提高读写性能。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 提供了各种不同的方法或 RAID 级别来组织磁盘存储。有些 RAID 级别保存冗余数据，因此可以在磁盘发生故障后恢复数据。不同的 RAID 级别可能也意味着在系统输入/输出（读和写）性能方面有某种程度的提高或降低。

保存冗余数据需要使用额外的物理磁盘。随着使用更多的磁盘，某个磁盘出现故障的可能也就会增加。由于在输入/输出性能和冗余方面存在差异，所以根据操作系统中的应用程序和所存储数据的性质来挑选，某个 RAID 级别可能比另一种更适合。

选择某个 RAID 级别后，需要注意以下性能和成本问题：

- 可用性或容错性—可用性或容错性是指系统即使在一个组件出现故障时保持运行并允许访问数据的能力。在 RAID 卷中，可用性或容错性是通过保存冗余数据来实现的。冗余数据包括镜像（复制数据）和奇偶校验信息（使用某种算法重新构建数据）。
- 性能—根据所选的 RAID 级别，读写性能可能会有所提高或降低。有些 RAID 级别可能更适合于某些应用程序。

- 成本效率—保存与 RAID 卷相关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、容易重新生成的或者不太重要，那么在数据冗余方面增加的成本可能就不太合算。
- 平均故障间隔时间 (MTBF) — 使用额外磁盘保持数据冗余还会在任何特定时刻增加磁盘故障的可能性。虽然这个选项在那些需要冗余数据的环境中是不可避免的，但确实给公司的系统支持人员增加了工作负担。
- 卷- 卷是指单磁盘非 RAID 虚拟磁盘。使用 O-ROM <Ctrl> <r> 等外部公用程序可以创建卷。Storage Management 不支持创建卷。但只要有可用空间，即可查看卷，以及使用这些卷中的驱动器创建新虚拟磁盘或现有虚拟磁盘的联机容量扩展 (OCE)。

选择 RAID 级别

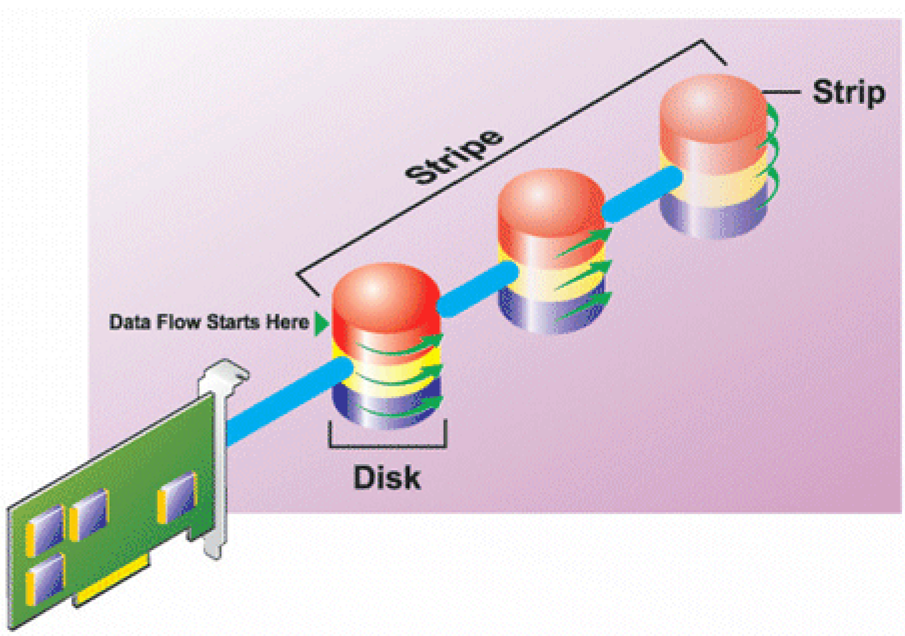
您可以使用 RAID 在多个磁盘上控制数据存储。每种 RAID 级别或连锁都具有不同的性能和数据保护特点。

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，将数据写入各个物理磁盘上的相等大小区段上。RAID 0 不提供数据冗余。



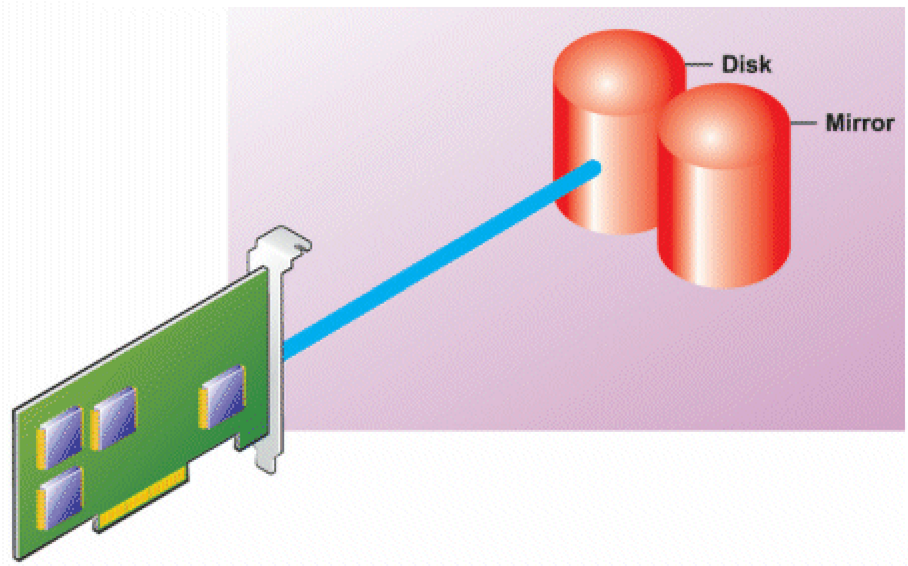
RAID 0 特点：

- 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。
- 不会存储冗余数据。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 是保持冗余数据的最简单形式。在 RAID 1 中，数据在一个或多个物理磁盘上被镜像或复制。如果一个物理磁盘失败，则可使用镜像另一端的数据对该数据进行重建。

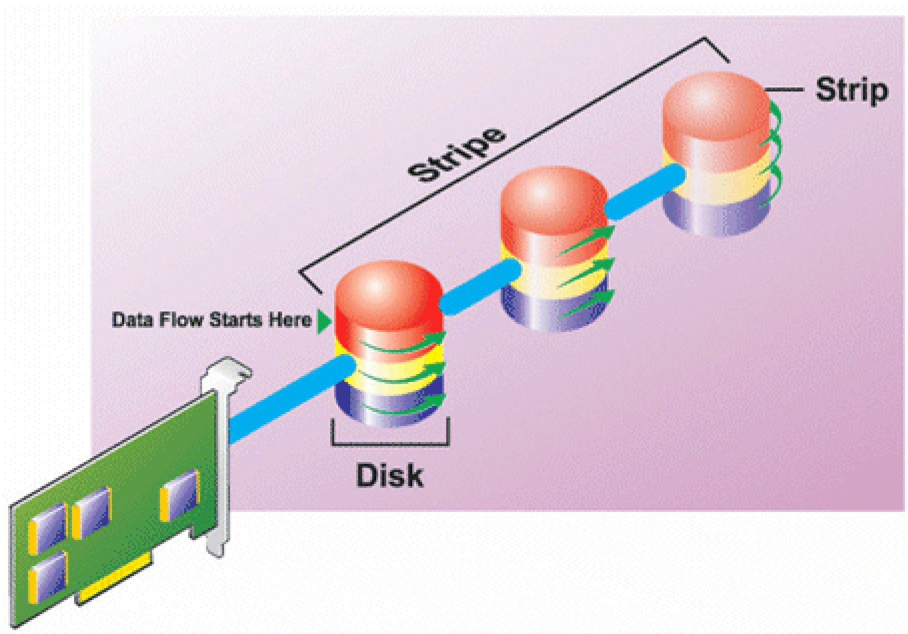


RAID 1 特点：

- 将 *n* + *n* 个磁盘组合为一个虚拟磁盘，具有 *n* 个磁盘的容量。当前由 Storage Management 支持的控制器在创建 RAID 1 时允许选择两个磁盘。由于这两个磁盘互为镜像，总存储容量相当于一个磁盘。
- 数据同时复制到这两个磁盘。
- 一个磁盘发生故障时，虚拟磁盘仍然可以工作。数据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（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来提供数据冗余。但并不是专门用某个物理磁盘进行奇偶校验，而是在磁盘组中的所有物理磁盘上对奇偶校验信息进行分条。

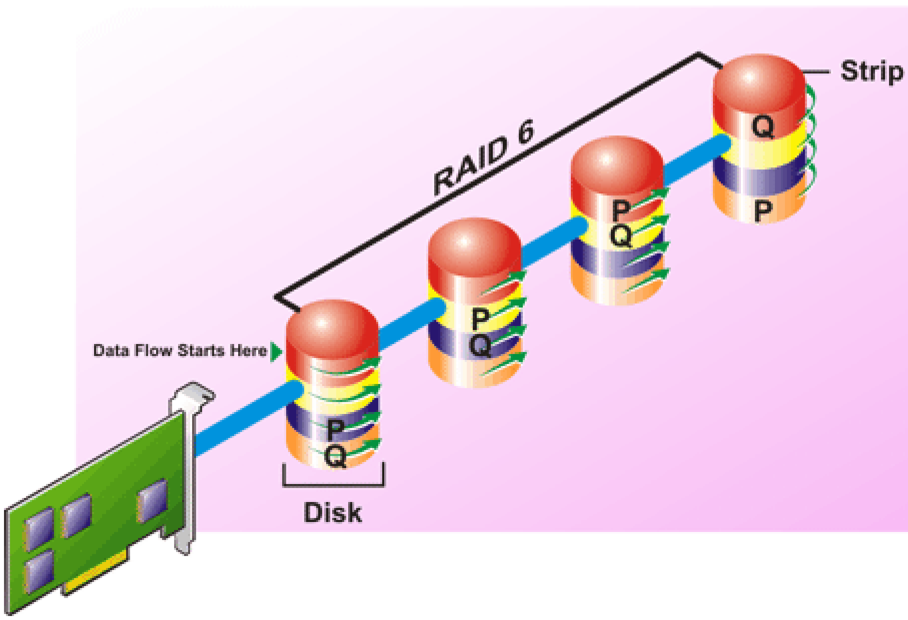


RAID 5 特点：

- 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。将从剩下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条和奇偶校验信息来提供数据冗余。与 RAID 5 类似，奇偶校验在各条带上分布。然而，RAID 6 使用额外的物理磁盘存放奇偶校验，这样磁盘组中的每个条带都有两个具有奇偶校验信息的磁盘块。额外的奇偶校验在两个磁盘失败时提供数据保护。在下面的图像中，两组奇偶校验信息表示为 **P** 和 **Q**。



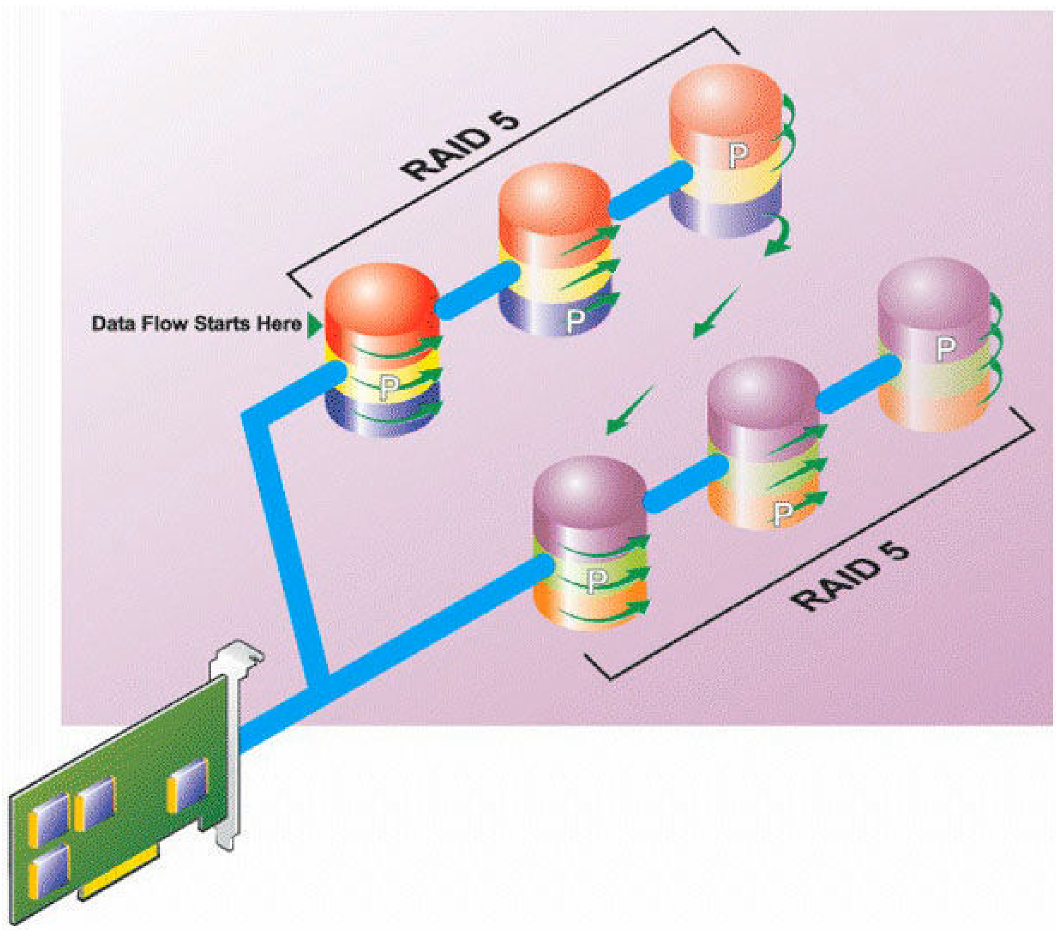
RAID 6 特点：

- 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。
- 虚拟磁盘在多达两个磁盘失败时仍保持正常运行。将从剩下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。
- 需要每个跨接有两个磁盘以实现奇偶校验。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 是一个以上物理磁盘跨接分条。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，也有可能实现 RAID 50。在这种情况下，可以实现多个 RAID 5 虚拟磁盘，然后将这些 RAID 5 磁盘转换为动态磁盘。可以随后创建一个跨接所有 RAID 5 虚拟磁盘的动态卷。

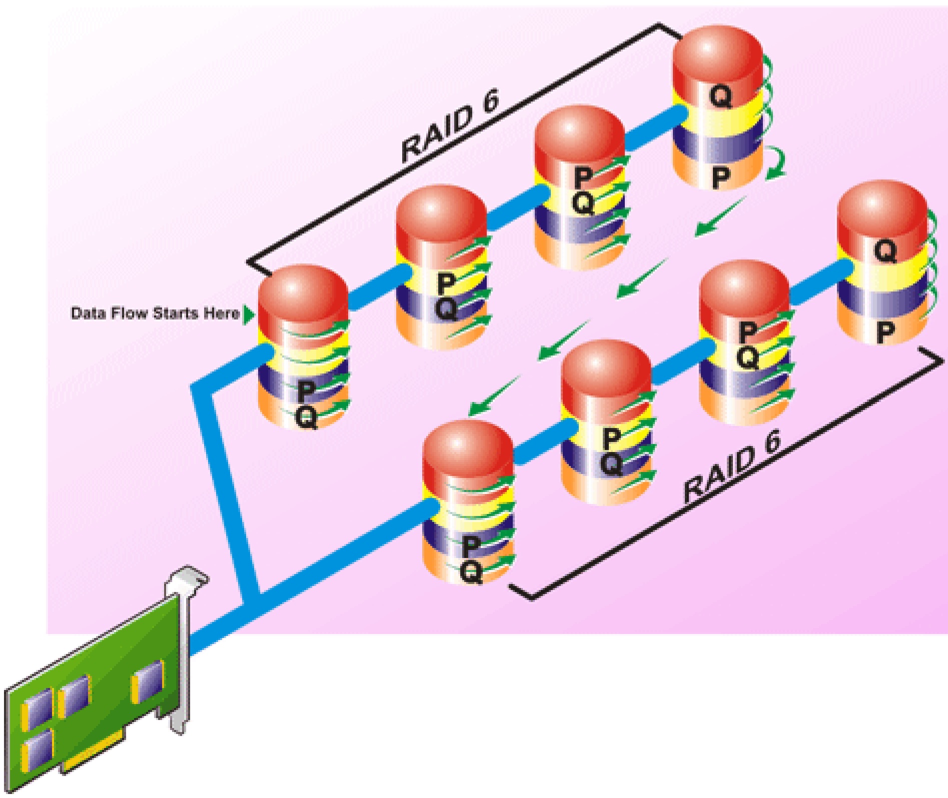


RAID 50 特点：

- 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。
- 数据在所有跨接上进行分条。RAID 50 在磁盘空间方面成本较高。

RAID 级别 60（在 RAID 6 组上分条）

RAID 60 是在多个配置为 RAID 6 的物理磁盘的跨接上分条。例如，一个用四个物理磁盘实施的 RAID 6 磁盘组，随后与另外四个物理磁盘的磁盘组继续实施，即成为 RAID 60。

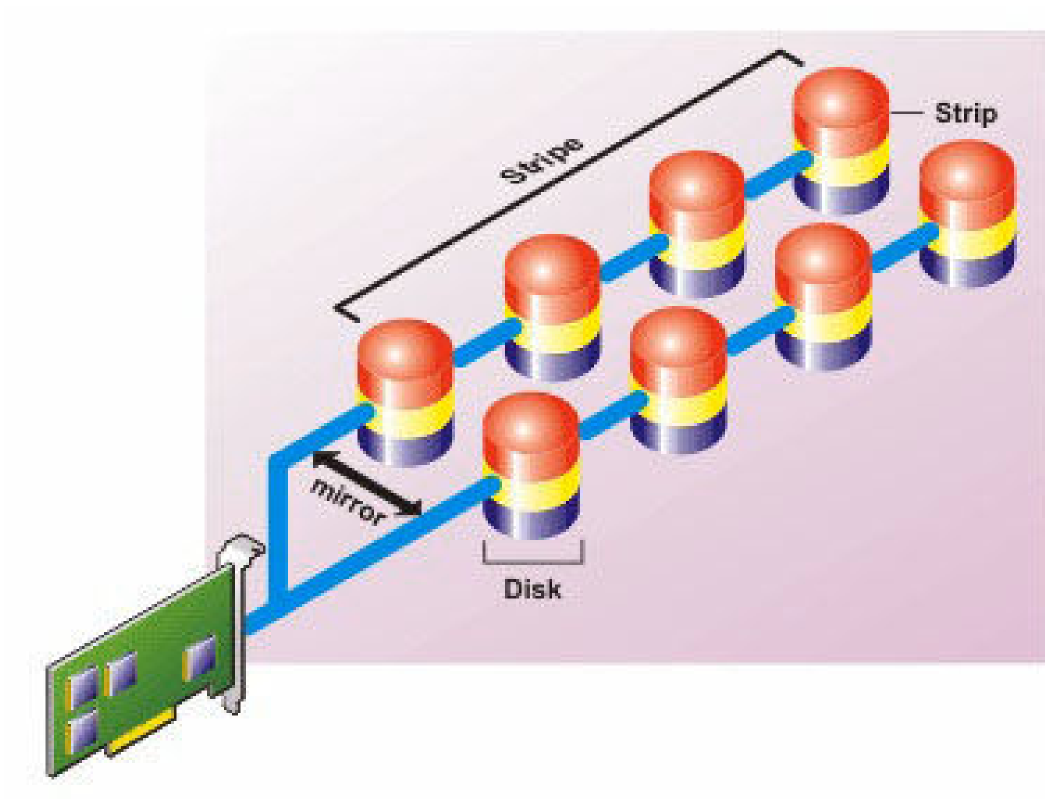


RAID 60 特点：

- 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。
- 需要每个跨接有两个磁盘以实现奇偶校验。RAID 60 在磁盘空间方面成本较高。

RAID 级别 10（分条的镜像）

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。对于 RAID 10，数据在多个物理磁盘上分条。分条的磁盘组随后会镜像到另一组物理磁盘。RAID 10 可以视为*条带的镜像*。



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。
- 数据的镜像映像在物理磁盘组上进行分条。此级别通过镜像提供冗余。
- 一个磁盘发生故障时，虚拟磁盘仍然可以工作。从没有故障的镜像磁盘中读取数据。
- 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. 26: RAID 级别性能比较

RAID 级别	数据可用性	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	N	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 级别	数据可用性	读性能	写性能	重建性能	所需的最小磁盘	建议的用途
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）	严重信息。数据库和其他读密集型事务性使用。
RAID 60	极好	很好	一般	差	X x (N + 2)（N = 至少为 2）	严重信息。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 接口支持以下 PERC9 控制器：

- PERC H830
- PERC H730P
- PERC H730
- PERC H330

iDRAC 接口支持以下 PERC8 控制器：

- PERC H810
- PERC H710P
- PERC H710
- PERC H310

iDRAC 接口支持以下模块化 PERC 控制器：

- PERC FD33xS
- PERC FD33xD

注: 有关在 PERC FD33xS 和 PERC FD33xD 控制器上配置和更改控制器模式的更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Dell Chassis Management Controller Version 1.2 for PowerEdge FX2/FX2s User's Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller 版本 1.2 用户指南）。

支持的非 RAID 控制器

iDRAC 接口支持 12 Gbps SAS HBA 外部适配器。

支持的机柜

iDRAC 支持 MD1400 和 MD1420 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。

注: 准备卸下以及组件 LED 闪烁或取消闪烁等功能不适用于 HHHL PCIe SSD 卡。

功能名称	PERC 9 控制器						PERC 8 控制器				PCIe SSD
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
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	分阶段	分阶段	分阶段	分阶段	不适用
创建虚拟磁盘	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
编辑虚拟磁盘高速缓存策略	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
检查虚拟磁盘一致性	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
取消检查一致性	实时	实时	实时	实时	实时	实时	不适用	不适用	不适用	不适用	不适用
初始化虚拟磁盘	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
取消初始化	实时	实时	实时	实时	实时	实时	不适用	不适用	不适用	不适用	不适用
加密虚拟磁盘	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
分配和取消分配专用热备用	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
删除虚拟磁盘	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
设置巡检读取模式	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用

功能名称	PERC 9 控制器						PERC 8 控制器				PCIe SSD
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
巡检读取未配置区域	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）	实时（仅限 Web 界面中）	分阶段（仅限 Web 界面中）	分阶段（仅限 Web 界面中）	分阶段（仅限 Web 界面中）	分阶段（仅限 Web 界面中）	不适用
检查一致性模式	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
回写模式	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
负载平衡模式	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
检查一致性率	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
重建率	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
后台初始化 (BGI) 率	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
重构率	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
导入外部配置	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
自动导入外部配置	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
清除外部配置	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
重设控制器配置	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	不适用
创建或更改安全密钥	实时	实时	实时	实时	实时	实时	分阶段	分阶段	分阶段	分阶段	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	实时
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	实时

功能名称	PERC 9 控制器						PERC 8 控制器				PCIe SSD
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
安全地擦除数据	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	分阶段
配置背板模式	实时	实时	实时	实时	实时	实时	不适用	不适用	不适用	不适用	不适用
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	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

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

但是，RACADM 和 WS-MAN 将显示系统中大多数存储设备的信息。

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。

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**概览** → **存储** → **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**概览** → **存储** → **拓扑**查看重要存储组件的分层物理防护视图。
- 转至**概览** → **存储** → **物理磁盘** → **属性**查看物理磁盘信息。将显示**物理磁盘属性**页面。
- 转至**概览** → **存储** → **虚拟磁盘** → **属性**查看虚拟磁盘信息。将显示**虚拟磁盘属性**页面。
- 转至**概览** → **存储** → **控制器** → **属性**查看 RAID 控制器信息。将显示**控制器属性**页面。
- 转至**概览** → **存储** → **机柜** → **属性**查看机柜信息。将显示**机柜属性**页面。

您还可以使用筛选器查看特定的设备信息。

有关所示属性以及如何使用筛选器选项的更多信息，请参阅 *iDRAC Online Help*（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 **raid** 或 **storage** 子命令。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）。

使用 iDRAC 设置公用程序监测背板

在 iDRAC 设置公用程序中，转到**系统摘要**。将显示 **iDRAC 设置系统摘要**页面。**背板资源清册**部分将显示背板信息。有关这些字段的信息，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。还会显示物理磁盘直接连接到控制器。

要查看存储设备拓扑，请转至**概览 → 存储 → 拓扑**。**拓扑**页面将显示系统中存储组件的分层表示形式。

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（仅在 RACADM 中受支持，并且是分阶段操作）
- 转换为非 RAID 磁盘（仅在 RACADM 中受支持，并且是分阶段操作）
- 闪烁或取消闪烁 LED

相关概念

资源清册和监测存储设备
分配或取消分配物理磁盘作为全局热备用

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。热备份保持在待机模式中。如果虚拟磁盘中的某个物理磁盘发生故障，会激活分配的热备份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。如果激活热备份，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。

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份的分配。用户也可以将一个以上的物理磁盘分配为全局热备份。

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。如果想要将热备用分配给一个虚拟磁盘（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。
- 如果不存在虚拟磁盘，请至少创建一个虚拟磁盘。
- 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、WS-MAN）或 <CTRL+R> 将它们转换为 RAID 模式。

如果已在"添加到挂起操作"模式中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，如果您尝试将此相同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。

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**概览** → **存储** → **物理磁盘** → **设置**。
   此时将显示**设置物理磁盘**页面。
2. 从**控制器**下拉菜单中，选择控制器以查看关联的物理磁盘。
3. 要分配为全局热备用，请从**操作-分配到全部**列中的下拉菜单中，对一个或多个物理磁盘选择**全局热备用**。
4. 要取消分配热备用，请从**操作-分配到全部**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**。
5. 在**应用操作模式**下拉菜单中，选择要应用设置的时间。
6. 单击**应用**。
   将根据选定的操作模式应用这些设置。

相关任务

[使用 Web 界面选择操作模式]

使用 RACADM 分配或取消分配全局热备用

使用存储**子命令**，并将类型指定为全局热备用。有关更多信息，请参阅 **dell.com/esmmanuals** 上的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

相关任务

[使用 RACADM 选择操作模式]

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。

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 或 WS-MAN。
- 在重新启动服务器时，按 Ctrl+R 组合键并选择所需控制器。

注: 在 HBA 模式下运行的 PERC 硬件控制器不支持转换模式。

注: PERC H310 和 H330 控制器仅支持转换为 PERC 8 控制器的非 RAID 模式。

注: 如果连接到 PERC 控制器的物理驱动器处于非 RAID 模式，则 iDRAC 界面（例如 iDRAC GUI、RACADM 和 WS-MAN）中显示的磁盘大小可能略小于磁盘的实际大小。但是，您可以使用整个磁盘容量来部署操作系统。

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**概览** → **存储** → **物理磁盘** → **设置**。
   此时将显示**设置**页面。
2. 从**控制器**下拉菜单中选择一个控制器。
   此时将显示与所选控制器相关联的物理磁盘。
3. 从**操作 - 分配至所有**下拉列表框中，为所有磁盘选择所需选项（**转换为 RAID** 或**转换为非 RAID**），或从**操作**下拉菜单中为特定磁盘选择选项。
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**应用**。
   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。

有关命令的更多信息，请参阅 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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

相关概念

[创建虚拟磁盘]
[编辑虚拟磁盘高速缓存策略]
[删除虚拟磁盘]
[检查虚拟磁盘一致性]
[初始化虚拟磁盘]
[加密虚拟磁盘]

[分配或取消分配专用热备用](#)
[使用 Web 界面管理虚拟磁盘](#)
[使用 RACADM 管理虚拟磁盘](#)

创建虚拟磁盘

要实施 RAID 功能，必须创建虚拟磁盘。虚拟磁盘是 RAID 控制器从一个或多个物理磁盘创建的存储空间。虽然虚拟磁盘可能由多个物理磁盘创建，但是操作系统会将它视为一个磁盘。

创建虚拟磁盘之前，您应当熟悉创建虚拟磁盘之前的注意事项中的信息。

可以使用连接到 PERC 控制器的物理磁盘来创建虚拟磁盘。要创建虚拟磁盘，您必须具有服务器控制用户权限。最多可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：

- 创建虚拟磁盘的物理磁盘驱动器不可用。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。
- 已创建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，然后创建新的虚拟磁盘。
- 作业当前正在运行或已在选定的控制器上计划。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。您可以在作业队列页中查看和管理已计划作业的状态。
- 物理磁盘处于非 RAID 模式。必须使用 iDRAC 界面（例如 iDRAC Web 界面、RACADM、WS-MAN）或 <CTRL+R> 将其转换为 RAID 模式。

注: 如果在"添加到挂起操作"模式下创建虚拟磁盘且未创建作业，如果之后删除该虚拟磁盘，则针对该虚拟磁盘的"创建挂起操作"将被清除。

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。
- 磁盘组是连接到其上已创建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阻止混合磁盘组。
- 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。
- 无法在 PCIe SSD 上创建虚拟磁盘。

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**概览 → 存储 → 虚拟磁盘 → 创建**。

将显示**创建虚拟磁盘**页面。

2. 在**设置**选项卡中，执行下列操作：
   a. 输入虚拟磁盘的名称。
   b. 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。
   c. 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。
   d. 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**、**T10 PI 容量**。

      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。
   e. 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。
   f. 此时将根据所选的物理磁盘（步骤 3）显示**跨越计数**字段。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。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。
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 Online Help*（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。

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 **dell.com/esmmanuals** 上的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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读取或写入策略。因此，在应用策略时，将显示一条错误消息。

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** - 只有最近的两次读取请求顺序访问磁盘扇区时，控制器才会启动预读。如果后续的读取请求随机访问磁盘各个扇区，控制器将恢复为不预读策略。控制器继续评估读取请求是否在顺序访问磁盘扇区，并在需要时启动预读。

  注: 上几代 PERC 控制器支持 **不预读**、**预读**和**自适应预读**读取策略设置。对于 PERC 8 和 PERC 9，**预读**和**自适应预读**设置在控制器级别其功能是等同的。就向后兼容目的而言，一些系统管理接口和 PERC 8 及 PERC 9 控制器仍然允许读取策略设置为**自适应预读**。虽然在 PERC 8 或 PERC 9 上可以设置**预读**或**自适应预读**，但二者在功能上无任何区别。
- **预读** - 控制器在搜寻数据时读取虚拟磁盘的连续扇区。如果将数据写入虚拟磁盘的连续扇区，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** - 控制器只在数据写入磁盘后发送写入请求完成信号。直写高速缓存的数据安全性要高于回写高速缓存，因为只有在数据安全地写入磁盘后，系统才会假定数据可用。
- **回写** — 在数据进入控制器高速缓存但尚未写入磁盘时，控制器会发送写入请求完成信号。回写高速缓存可以改善性能，因为后续的读取请求可以更快地从高速缓存然后从磁盘检索数据。但是，在发生系统故障、

使数据无法被写入磁盘时也可能发生数据丢失。其他应用程序如果假定数据在磁盘上而采取相应的操作，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。
- 预读和回写操作需要使用高速缓存。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

删除虚拟磁盘将会破坏所有信息（包括虚拟磁盘上的文件系统和卷），并会将虚拟磁盘从控制器配置中移除。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。在删除磁盘组中的最后一个虚拟磁盘时，所有已分配的专用热备用将自动变为全局热备用。

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。

当允许执行此操作时，您可以删除引导虚拟驱动器。这是通过边带实现的，并且独立于操作系统。因此，在删除虚拟驱动器之前将出现一条警告消息。

如果删除某个虚拟磁盘并立即创建一个新虚拟磁盘，并且所有特性与删除的磁盘完全一样，那么控制器将会像根本没删除第一个虚拟磁盘一样识别数据。在这种情况下，如果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

此操作将验证冗余（奇偶校验）信息的准确性。此任务只适用于冗余虚拟磁盘。在必要时，一致性检查任务将重建冗余数据。如果虚拟驱动器具有已降级的状态，则运行一致性检查操作可能会使虚拟驱动器恢复至就绪状态。您也可以取消一致性检查操作。

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。

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。必须初始化所配置的虚拟磁盘，然后才能使用虚拟磁盘。

注: 当尝试重新创建现有配置时，请勿初始化虚拟磁盘。

可以执行快速初始化、完全初始化或取消初始化操作。

注: 取消初始化的操作是实时操作。只能使用 iDRAC Web 界面（而非 RACADM）取消初始化。

快速初始化

快速初始化操作将初始化虚拟磁盘中包括的所有物理磁盘。该操作将更新物理磁盘上的元数据，以使所有磁盘空间都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并未擦除，尽管以后的写操作会覆盖物理磁盘上保留的任何信息。

快速初始化操作仅会删除引导扇区和条带信息。仅在时间有限或硬盘驱动器是新驱动器或未使用的驱动器时，才应执行快速初始化。快速初始化过程所需的时间更少（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。

快速初始化任务并不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较低。

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（也称为慢速初始化）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之后执行完全初始化。与快速初始化操作相比，如果您的物理磁盘有问题或者怀疑磁盘有坏块，则可能更需要执行完全初始化。完全初始化操作会重新映射坏块，并向所有磁盘块写入零。

如果对虚拟磁盘执行完全初始化，则无需执行后台初始化。在完全初始化过程中，主机不能访问虚拟磁盘。如果系统在完全初始化过程中重新引导，则操作将终止，并且会在虚拟磁盘上启动后台初始化过程。

建议始终对以前包含数据的驱动器执行完全初始化。针对每 GB 的完全初始化可能需要长达 1-2 分钟。初始化速度取决于控制器型号、硬盘驱动器速度和固件版本。

完全初始化任务一次将初始化一个物理磁盘。

注: 仅支持执行实时完全初始化。只有少数控制器支持完全初始化。

加密虚拟磁盘

当控制器上已禁用加密功能（即，已删除安全密钥）时，可为通过 SED 驱动器创建的虚拟磁盘手动启用加密功能。如果虚拟磁盘是在控制器启用加密功能后创建的，则会自动加密虚拟磁盘。虚拟磁盘将自动配置为加密虚拟磁盘，除非在虚拟磁盘创建期间已禁用所启用的加密选项。

注: 此任务只能分阶段进行，不支持实时操作。

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。

分配或取消分配专用热备用

专用热备用是已分配给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。

只有 T10 PI (DIF) 型的物理磁盘才能作为热备用分配给已启用 T10 PI (DIF) 的虚拟磁盘。如果之后在虚拟磁盘上启用了 T10 PI，任何已分配为专用热备用的非 T10 PI (DIF) 驱动器磁盘将不是热备用。

只能向 4K 虚拟磁盘分配 4K 驱动器以作为热备用。

如果您已在"添加到挂起操作"模式中将虚拟磁盘分配为专用热备用，将创建挂起操作，但不会创建任务。因此，如果您尝试取消分配此专用热备用，将会清除"分配专用热备用挂起操作"。

如果已在"添加到挂起操作"模式中取消将虚拟磁盘分配为专用热备用，将创建挂起操作，但不会创建任务。因此，如果您尝试分配此专用热备用，将会清除"取消分配专用热备用挂起操作"。

使用 Web 界面管理虚拟磁盘

1. 在 iDRAC Web 界面中，转至**概览** → **存储** → **虚拟磁盘** → **管理**。
   此时将显示**管理虚拟磁盘**页面。
2. 从**控制器**下拉菜单中，选择您想要管理其虚拟磁盘的控制器。
3. 对于一个或多个虚拟磁盘，从每个**操作**下拉菜单中选择一个操作。
   可以为虚拟驱动器指定多个操作。当选择某个操作时，将显示一个附加的**操作**下拉菜单。从该下拉菜单中选择另一个操作。之前已选择的操作不会显示在附加**操作**下拉菜单中。此外，所选操作旁边将显示**删除**链接。单击此链接可删除所选操作。
   - **删除**
   - **编辑策略：读高速缓存** - 将读高速缓存策略更改为以下选项之一：
     - **不预读**
     - **预读**
     - **自适应预读**

     注: 上几代 PERC 控制器支持 **不预读**、**预读**和**自适应预读**读取策略设置。对于 PERC 8 和 PERC 9，**预读**和**自适应预读**设置在控制器级别其功能是等同的。 就向后兼容目的而言，一些系统管理接口和 PERC 8 及 PERC 9 控制器仍然允许读取策略设置为**自适应预读**。虽然在 PERC 8 或 PERC 9 上可以设置**预读**或**自适应预读**，但二者在功能上无任何区别。
   - **编辑策略：写高速缓存** - 将写高速缓存策略更改为以下选项之一：
     - **直写**
     - **回写**
     - **强制回写**
   - **编辑策略：磁盘高速缓存** - 将磁盘高速缓存策略更改为以下选项之一：
     - **Default（默认值）**
     - **Enabled（已启用）**
     - **Disabled（已禁用）**
   - **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**

- **加密虚拟磁盘** - 加密虚拟磁盘驱动器。如果控制器具有加密功能，则可以创建、更改或删除安全密钥。

  注: 只有在使用 Self-Encrypting Drive (SED) 驱动器创建虚拟磁盘时，**加密虚拟磁盘**选项方可用。
- **管理专用热备用** - 分配或取消分配用作专用热备用的物理磁盘。仅显示有效的专用热备用。如果没有有效的专用热备用，则下拉菜单中不会显示此部分。

有关这些选项的更多信息，请参阅 *iDRAC Online Help*（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**应用**。
   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 RACADM 命令管理虚拟磁盘：

- 删除虚拟磁盘：`racadm storage deletevd:<VD FQDD>`
- 初始化虚拟磁盘：`racadm storage init:<VD FQDD> -speed {fast|full}`
- 检查虚拟磁盘一致性：`racadm storage ccheck:<vdisk fqdd>`
- 加密虚拟磁盘：`racadm storage encryptvd:<VD FQDD>`
- 分配或取消分配专用热备用：`racadm storage hotspare:<Physical Disk FQDD> -assign yes -type dhs -vdkey: <FQDD of VD>`
- 取消检查一致性：`racadm storage cancelcheck: <vdisks fqdd>`

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

相关概念

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
支持的控制器
支持的存储设备功能的摘要
将物理磁盘转换为 RAID 或非 RAID 模式

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

注: 可以使用 iDRAC Web 界面而非 RACADM 配置“巡检读取未配置区域”属性。

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。

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: 如果控制器中没有可用的虚拟磁盘，则不支持**启动**和**停止**等巡检读取模式操作。尽管可以使用 iDRAC 界面成功调用操作，但在关联作业启动时，操作会失败。

负载平衡

通过“负载平衡”属性，可自动使用两个连接到同一机柜的控制器端口或连接器来路由 I/O 请求。此属性仅在 SAS 控制器上可用。

后台初始化 (BGI) 率

在 PERC 控制器上，冗余虚拟磁盘的后台初始化会在创建虚拟磁盘后 0 至 5 分钟内自动开始。冗余虚拟磁盘的后台初始化准备虚拟磁盘保存冗余数据，改善写性能。例如，在 RAID 5 虚拟磁盘的后台初始化完成后，奇偶校验信息就已初始化。在 RAID 1 虚拟磁盘的后台初始化完成后，物理磁盘就会镜像。

后台初始化过程可帮助控制器识别并更正以后可能会出现的冗余数据问题。在这方面，后台初始化过程与一致性检查过程类似。用户应允许后台初始化完成运行。如果取消运行，后台初始化会在 0 到 5 分钟内自动重新

启动。在后台初始化运行过程中，可以执行读写操作等过程。其他过程（如创建虚拟磁盘）不能与后台初始化过程同时进行。这些过程会导致后台初始化被取消。

后台初始化率（可在范围 0 % 至 100% 之间配置）表示专用于运行后台初始化任务的系统资源百分比。设为 0 % 时，后台初始化对于控制器具有最低优先级，需要最长的时间才能完成，并且对系统性能的影响最小。后台初始化率为 0 % 并不表示后台初始化已停止或暂停。设置为 100 % 时，后台初始化对于控制器具有最高优先级。只需最短的时间即可完成后台初始化，但对系统性能的影响最大。

检查一致性

检查一致性任务验证冗余（奇偶校验）信息的准确性。此任务只适用于冗余虚拟磁盘。在必要时，检查一致性任务将重建冗余数据。当虚拟磁盘处于“失败的冗余”状态时，执行“检查一致性”可能会将虚拟磁盘返回到“就绪”状态。

一致性检查率（可在范围 0 % 和 100% 之间配置）表示专用于运行一致性检查任务的系统资源百分比。设为 0% 时，一致性检查对于控制器具有最低优先级，需要最长的时间才能完成，并且对系统性能的影响最小。一致性检查率为 0% 并不表示一致性检查已停止或暂停。设置为 100 % 时，一致性检查对于控制器具有最高优先级。只需最短的时间即可完成一致性检查，但对系统性能的影响最大。

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锁定或解锁对 SED 的访问。只能为每个具有加密功能的控制器创建一个加密密钥。安全密钥通过本地密钥管理 (LKM) 功能进行管理。LKM 用于生成在保护虚拟磁盘时所需的密钥 ID 和密码或密钥。如果使用 LKM，必须通过提供安全密钥标识符和密码短语来创建加密密钥。

在 HBA 模式下运行的 PERC 硬件控制器上不支持该任务。

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。

使用 Web 界面配置控制器属性

1. 在 iDRAC Web 界面中，转至**概览** → **存储** → **控制器** → **设置**。
   此时会显示**设置控制器**页面。
2. 在**配置控制器属性**部分中，从**控制器**下拉菜单中选择要配置的控制器。
3. 为各个属性指定所需的信息。
   当前值列将显示每个属性的现有值。您可以通过在**操作**下拉菜单中选择选项来为每个属性修改此值。
   有关各字段的信息，请参阅 *iDRAC Online Help*（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**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: 如果控制器中没有可用的虚拟磁盘，则不支持启动和停止等巡检读取模式操作。尽管可以使用 iDRAC 界面成功调用操作，但在关联作业启动时，操作会失败。

- 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

外部配置是从一个控制器移至另一个控制器的物理磁盘上的数据。位于已移动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，以便在移动物理磁盘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，如果外部配置只包含 RAID 1 虚拟磁盘镜像的一端，则虚拟磁盘处于降级状态并且可以导入。如果外部配置只包含原先配置为 RAID 5 的三个物理磁盘中的一个，则 RAID 5 虚拟磁盘将会出现故障状态且不能导入。

除了虚拟磁盘，外部配置可能包含在一个控制器上分配为热备份，但随后转移到另一控制器的物理磁盘。导入外部配置任务会将新物理磁盘导入为热备份。如果物理磁盘在前一个控制器上被设为专用热备份，但是在外部配置中该热备份分配的虚拟磁盘不再存在，则该物理磁盘会作为全局热备份导入。

如果检测到使用本地密钥管理器 (LKM) 锁定的任何外部配置，则在此版本中，不能在 iDRAC 中导入外部配置。您必须通过 CTRL-R 解锁驱动器，然后继续从 iDRAC 导入外部配置。

导入外部配置任务只有在控制器检测到外部配置时才会显示。通过检查物理磁盘状态还可以识别物理磁盘是否包含外部配置（虚拟磁盘或热备份）。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有热备份。

注: 导入外部配置任务会导入已添加到控制器中的物理磁盘上的所有虚拟磁盘。如果有一个以上的外部虚拟磁盘，则将导入所有配置。

PERC9 控制器支持在无需用户交互的情况下自动导入外部配置。可以启用或禁用该自动导入功能。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: 操作系统正在系统上运行时，建议不要移除外部机柜电缆。重新建立连接时，移除电缆会导致出现外部配置。

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会更改。只有在处于"未配置 - 良好"状态的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

要导入外部配置，请执行以下操作：

1. 在 iDRAC Web 界面中，转至**概览** → **存储** → **控制器** → **设置**。
   此时会显示**设置控制器**页面。
2. 在**外部配置**部分中，从**控制器**下拉菜单中选择要配置的控制器。
3. 在**应用操作模式**下拉菜单中，选择导入操作时间。
4. 单击**导入外部配置**。
   将根据选定的操作模式导入配置。

   要自动导入外部配置，请在**配置控制器属性** 部分中启用 **增强的自动导入外部配置**选项，选择**应用操作模式**，然后单击**应用**。

   注: 在启用**增强的自动导入外部配置**选项之后，必须重新引导系统以导入外部配置。

使用 RACADM 导入外部配置

要导入外部配置，请使用以下命令：

```
racadm storage importconfig:<Controller FQDD>
```

有关更多信息，请参阅 **dell.com/esmmanuals** 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到另一个控制器，可能会发现物理磁盘包含所有或部分虚拟磁盘（外部配置）。通过检查物理磁盘状态可以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。可以从新连接的物理磁盘上清除或擦除虚拟磁盘信息。

"清除外部配置"操作将永久擦除已添加到控制器的物理磁盘上的所有数据。如果存在一个以上的外部虚拟磁盘，将会删除所有配置。您可能更希望导入虚拟磁盘而非破坏数据。要删除外部数据，必须执行初始化。如果您具有无法导入的不完整的外部配置，可使用"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**概览** → **存储** → **控制器** → **设置**。
   此时会显示**设置控制器**页面。
2. 在**外部配置**部分中，从**控制器**下拉菜单中选择要为其清除外部配置的控制器。
3. 在**应用操作模式**下拉菜单中，选择要清除数据的时间。
4. 单击**清除**。
   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，请使用以下命令：

```
racadm storage clearconfig:<Controller FQDD>
```

有关更多信息，请参阅 **dell.com/esmmanuals** 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

可以重设控制器的配置。此操作会删除虚拟磁盘驱动器，并取消分配控制器上的所有热备用。除了从配置中移除磁盘外，此操作不会删除任何数据。重设配置时不会移除任何外部配置。仅 PERC 9.1 固件可实时支持此功能。重设配置不会擦除任何数据。您可以在不执行初始化操作（这会导致恢复数据）的情况下重新创建完全相同的配置。您必须具有服务器控制权限。

注: 重设控制器配置不会移除外部配置。要移除外部配置，请执行清除配置操作。

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**概览** → **存储** → **控制器** → **故障排除**。
   此时会显示**控制器故障排除**页面。
2. 从**操作**下拉菜单中，为一个或多个控制器选择**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，请使用以下命令：

```
racadm storage resetconfig:<Controller FQDD>
```

有关更多信息，请参阅 **dell.com/esmmanuals** 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。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。
- 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: 请确保在切换模式之前先备份外部配置、安全密钥、虚拟磁盘和热备用，因为这些数据将被删除。

注: 请确保在更改控制器模式之前，对 PERC FD33xS 和 FD33xD 存储底座提供 CMC 许可证。有关存储底座 CMC 许可证的更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Dell Chassis Management Controller Version 1.2 for PowerEdge FX2/FX2s User's Guide*（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 WS-MAN）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**已启用**。

以下列表提供使用服务器配置文件功能通过 WS-MAN 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在设置控制器模式的同时配置多个 RAID 操作。例如，如果 PERC 控制器处于 HBA 模式，则可以编辑导出 xml 以将控制器模式更改为 RAID，将驱动器状态转换为就绪，并创建虚拟磁盘。
- 在将模式从 RAID 更改为 HBA 时，**RAIDaction pseudo** 属性会设置为更新（默认行为）。该属性可运行和创建故障虚拟磁盘。控制器模式虽已更改，但完成作业时出错。要避免出现此问题，必须在 XML 文件中将 RAIDaction 属性注释掉。

- 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 xml 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**概览** → **存储** → **控制器**。
2. 在**控制器**页面上，单击**设置** → **控制器模式**。

   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**应用**。

   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：

- 要查看控制器的当前模式，在 RACADM 提示符处，运行 `$ racadm get Storage.Controller.1.RequestedControllerMode [key =<Controller_FQDD>]` 命令。系统将显示以下输出：`RequestedControllerMode = NONE`。
- 要将控制器模式设置为 HBA，请运行 `$ racadm set Storage.Controller.1.RequestedControllerMode HBA [Key=< Controller_FQDD >]` 命令。

有关 RACADM 命令的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

12Gbps SAS HBA 适配器操作

非 RAID 控制器是具有较少 RAID 功能的 HBA。它们不支持虚拟磁盘。

在此版本中，iDRAC 界面仅支持 12 Gbps SAS HBA 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，可查看与机柜关联的 EMM、风扇、电源设备和温度探测器属性。这些属性按控制器类型显示。
- 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:

- 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。
- 在执行固件更新后重新引导系统。
- 仅会为 12 Gbps SAS HBA 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。

相关概念

资源清册和监测存储设备
查看系统资源清册
更新设备固件

[监测驱动器上的预测性故障分析](#)
[闪烁或取消闪烁组件 LED](#)

监测驱动器上的预测性故障分析

Storage Management 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 会对每个磁盘执行预测性故障分析，并在预计到会发生磁盘故障时发出警报。控制器会针对预计的故障检查物理磁盘，如果发现这样的预计故障，会将此信息传递给 iDRAC。iDRAC 将立即记录一个警报。

非 RAID (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。
- 配置以下属性：
  - 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
- 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，会显示一条错误消息。

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 PCIe SSD

外围设备组件快速互连 (PCIe) 固态设备(SSD) 是一种高性能存储设备，设计用于要求低延迟、较高的每秒输入输出操作数 (IOPS) 以及企业级存储可靠性和可维护性的解决方案。PCIe SSD 的设计基于单层单元 (SLC) 和多层单元 (MLC) NAND 闪存技术与高速 PCIe 2.0 或 PCIe 3.0 兼容接口。在第 13 代 Dell PowerEdge 机架式和塔式服务器以及 Dell PowerEdge R920 服务器上，iDRAC 2.20.20.20 及以上版本支持 Half-Height Half-Length (HHHL) PCIe SSD 卡。对于未配备 PCIe SSD 支持的背板的服务器，HHHL SSD 卡可以直接插入此类服务器中的 PCI 插槽。在配备有受支持背板的服务器上，同样可以使用这些插卡。

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

PCIe SSD 子系统由背板、连接到系统背板的 PCIe 扩展卡（可为机箱前部的最多四个或八个 PCIe SSD 提供 PCIe 连接）以及 PCIe SSD 组成。

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
- 闪烁或取消闪烁设备 LED

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
- 报告驱动器状态，例如联机、故障和脱机
- 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

注: 热插拔功能、卸下准备以及设备 LED 指示灯闪烁或取消闪烁不适用于 HHHL PCIe SSD 设备。

相关概念

对 PCIe SSD 进行资源清册和监测
准备移除 PCIe SSD
擦除 PCIe SSD 设备数据

对 PCIe SSD 进行资源清册和监测

在分阶段或实时模式中，将为 PCIe SSD 提供以下资源清册和监测信息：

- 硬件信息：
  - PCIe SSD 扩展卡

– PCIe SSD 背板

- 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，请在 iDRAC Web 界面中转至**概览** → **存储** → **物理磁盘**。此时将显示**属性**页面。对于 PCIe SSD，**名称**列中将显示 **PCIe SSD**。展开可查看各个属性。

使用 RACADM 对 PCIe SSD 进行资源清册和监测

可使用 `racadm storage get controllers:<PcieSSD controller FQDD>` 命令对 PCIe SSD 进行资源清册和监测

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/esmmanuals** 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

PCIe SSD 支持有序的热交换操作，允许您添加或移除设备，而不必停止或重新引导安装了这些设备的系统。为防止数据丢失，必须先使用“准备移除”操作，然后再物理地移除设备。

注:

- 只有在运行受支持操作系统的受支持系统中安装了 PCIe SSD 时，才支持有序热交换操作。为了确保 PCIe SSD 的配置正确，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任务。

  注: 使用 ESXi 6.0 和 iDRAC Service Module 2.1 版本的系统支持准备移除任务。
- 准备移除任务是一项分阶段的操作。但是，该任务可以通过 iDRAC Service Module 实时执行。

“准备移除”操作将停止所有后台活动和所有正在运行的 I/O 活动，以便安全地移除设备。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。
- 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**概览** → **存储** → **物理磁盘** → **设置**。
   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。
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**立即应用**选项可用。此操作不支持分阶段模式。
5. 单击**应用**。
   如果作业未创建，将会显示一条消息，指示作业创建未成功。此外，还会显示消息 ID 和建议的响应操作。
   如果作业创建成功，将会显示一条信息，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 准备移除 PCIe SSD

要准备移除 PCIe SSD 驱动器，请运行以下命令：

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

要在执行 **preparetoremove** 命令后创建目标作业，请运行以下命令：

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

要查询所返回的作业 ID，请运行以下命令：

```
racadm jobqueue view -i <job ID>
```

有关更多信息，请参阅 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

擦除 PCIe SSD 设备数据

“安全擦除”功能将永久擦除磁盘上的所有现有数据。在 PCIe SSD 上执行加密擦除操作将会覆盖所有块，并导致 PCIe SSD 上的所有数据永久丢失。在执行加密擦除过程中，主机无法访问 PCIe SSD。将在重新引导系统后应用更改。

如果在加密擦除期间系统重新引导或遇到断电，则该操作将取消。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:

- 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。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**概览 → 存储 → 物理磁盘 → 设置**。

   此时将显示**设置物理磁盘**页面。
2. 从**控制器**下拉菜单中，选择控制器以查看关联的 PCIe SSD。
3. 从下拉菜单中，对一个或多个 PCIe SSD 选择**安全擦除**选项。

   如果您已选择**安全擦除**，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：
   - **在下次重新引导时** - 选择此选项可在下次系统重新引导时应用操作。这是 PERC 8 控制器的默认选项。
   - **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）

     注: 对于 PERC 8 或更早版本的控制器，**正常关机**是默认选项。对于 PERC 9 控制器，**不重新引导（手动重新引导系统）**是默认选项。
5. 单击**应用**。

   如果作业未创建，将会显示一条消息，指示作业创建未成功。此外，还会显示消息 ID 和建议的响应操作。

   如果作业创建成功，将显示一条信息，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 PCIe SSD 设备数据

要在 PCIe SSD 设备上执行安全擦除，请运行以下命令：

```
racadm storage secureerase:<PCIeSSD FQDD>
```

要在执行 secureerase 命令后创建目标作业，请运行以下命令：

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

要查询所返回的作业 ID，请运行以下命令：

```
racadm jobqueue view -i <job ID>
```

有关更多信息，请参阅 **dell.com/esmmanuals** 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

相关概念

支持的存储设备功能的摘要
支持的机柜
配置背板模式
查看通用插槽
设置 SGPIO 模式

配置背板模式

Dell 第 13 代 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。此配置用于高性能模式，没有故障转移或高可用性 (HA) 功能。扩展器可在两个存储控制器之间划分内部驱动器阵列。在这种模式下，虚拟磁盘创建仅会显示已连接到特定控制器的驱动器。此功能对于许可没有要求。此功能仅在少数系统上受支持。

背板支持以下两种模式：

- 统一模式 - 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。此拆分是不可配置的。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。

默认情况下，将使用统一模式。

如果扩展器支持该配置，iDRAC 允许拆分模式设置。您可能需要在安装第二个控制器之前启用此模式。在允许配置此模式之前，iDRAC 会首先检查扩展器功能，且不会检查是否存在第二个 PERC 控制器。

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。

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**概览 → 存储 → 机柜 → 设置**。
   此时将显示**机柜设置**页面。
2. 从**控制器**下拉菜单中，选择要配置其关联机柜的控制器。
3. 在**值**列中，为所需的背板或机柜选择所需模式：
   - 一体化
   - 拆分
4. 从**应用操作模式**下拉菜单中，选择**立即应用**来立即应用操作，然后单击**应用**。
   将创建作业 ID。
5. 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”。
6. 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，请将 `BackplaneMode` 对象与 `set` 子命令一起使用。

例如，要将 BackplaneMode 属性设置为拆分模式，请执行以下操作：

1. 在 RACADM 命令提示符处，运行以下命令来查看当前背板模式：
   ```
   get storage.enclosure.1.backplanecurrentmode
   ```
   输出为：
   ```
   BackplaneCurrentMode=UnifiedMode
   ```
2. 运行以下命令来查看所需模式：
   ```
   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：
   ```
   set storage.enclosure.1.backplanerequestedmode "splitmode"
   ```
   系统将显示成功消息。
4. 运行以下命令来验证是否已将 `backplanerequestedmode` 属性设置为拆分模式：
   ```
   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：
   ```
   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：
   `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：
   `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：
   `serveraction powercycle`
10. 当系统完成 POST 和 CSIOR 之后，键入以下命令来验证 `backplanerequestedmode`：
   `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：
   `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：
   `storage get pdisks`

   有关 racadm 命令的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）

查看通用插槽

某些第 13 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。这些插槽连接至主要存储控制器 (PERC) 和 PCIe 扩展卡。这些插槽称为“通用”插槽。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：

- 如果插槽为空，会对插槽显示**空插槽**。
- 如果没有可支持 PCIe 的插槽，将不会显示**支持 PCIe** 列。
- 如果是在其中一个插槽中安装了 PCIe SSD 的通用背板，则**总线协议**列会显示 **PCIe**。
- **热备用**列不适用于 PCIe SSD。

注: 通用插槽不支持热交换功能。如果要移除 PCIe SSD 驱动器并将其更换为 SAS/SATA 驱动器，请确保先对 PCIe SSD 驱动器完成“准备移除”任务。如果不执行该任务，主机操作系统可能会遇到问题，如蓝屏、内核错误等。

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 界面设置 SGPIO 模式。

使用 RACADM 设置 SGPIO 模式

要配置 SGPIO 模式，请将 SGPIOMode 对象与 set 子命令配合使用。如果将其设置为禁用，则为 I2C 模式。如果启用，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）。

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：
   - **概览 → 存储 → 物理磁盘 → 设置**。
   - **概览 → 存储 → 虚拟磁盘 → 创建**
   - **概览 → 存储 → 虚拟磁盘 → 管理**
   - **概览 → 存储 → 控制器 → 设置**
   - **概览 → 存储 → 控制器 → 故障排除**
   - **概览 → 存储 → 机柜 → 设置**

- **概览 → 存储 → 挂起操作**

2. 从**应用操作模式**下拉菜单中选择下列任一项：
   - **立即应用** - 选择此选项将立即应用设置。此选项仅可用于 PERC 9 控制器。如果存在要完成的作业，则此选项将灰显。完成此作业至少需要 2 分钟。
   - **在下次重新引导时** - 选择此选项可在下次系统重新引导时应用设置。这是 PERC 8 控制器的默认选项。
   - **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）

     注: 对于 PERC 8 或更早版本的控制器，**正常关机**是默认选项。对于 PERC 9 控制器，**不重新引导（手动重新引导系统）**是默认选项。
   - **添加到挂起操作** - 选择此选项可创建要应用设置的挂起操作。您可以在**概览 → 存储 → 挂起操作**页面中查看控制器的所有挂起操作。

   注:

   - **添加到挂起操作**选项不适用于**挂起操作**页面，以及**物理磁盘 → 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

可使用 `jobqueue` 子命令选择操作模式。有关更多信息，请参阅 **dell.com/esmmanuals** 上的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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挂起操作。根据选定的选项，所有设置将立即应用、在下次重新引导时应用或在计划的时间应用。可以删除控制器的所有挂起操作，但不能删除单个挂起操作。

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**概览 → 存储 → 挂起操作**。
   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：
   - **立即应用** - 选择此选项可立即提交所有操作。此选项适用于具有最新固件版本的 PERC 9 控制器。
   - **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。这是 PERC 8 控制器的默认选项。此选项适用于 PERC 8 和更高版本。
   - **在计划的时间** - 选择此选项可在计划的日期和时间提交操作。此选项适用于 PERC 8 和更高版本。
     – **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）

     注: 对于 PERC 8 或更早版本的控制器，**正常关机**是默认选项。对于 PERC 9 控制器，**不重新引导（手动重新引导系统）**是默认选项。
5. 如果提交作业未创建，将会显示一条消息，指示作业创建未成功。此外，还会显示消息 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挂起状态，并且如果只有这些操作是挂起操作，则不能从**挂起操作**页中创建作业。您必须执行任何其他存储配置操作，或使用 RACADM 或 WSMAN 在所需控制器上创建所需的配置作业。

   您无法在**挂起操作**页面中查看或清除 PCIe SSD 的挂起操作。可使用 racadm 命令清除 PCIe SSD 的挂起操作。

使用 RACADM 查看和应用挂起操作

可使用 **jobqueue** 子命令应用挂起操作。有关更多信息，请参阅 **dell.com/esmmanuals** 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**创建作业**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。您无法查看 PCIe SSD 的挂起操作，因此**添加到挂起操作**选项不可用。请使用 racadm 命令清除 PCIe SSD 的挂起操作。

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。只有 PERC 9.1 和更高版本固件才实时支持此功能。

注: 对于不带背板的服务器，不支持执行闪烁或取消闪烁操作。

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：
   - **概览 → 存储 → 识别** - 显示**识别组件 LED** 页面，您可以在该页面中闪烁或取消闪烁物理磁盘、虚拟磁盘和 PCIe SSD。
   - **概览 → 存储 → 物理磁盘 → 识别**– 显示**识别物理磁盘**页面，您可以在该页面中闪烁或取消闪烁物理磁盘和 PCIe SSD。
   - **概览 → 存储 → 物理磁盘 → 识别**- 显示**识别虚拟磁盘**页面，您可以在该页面中闪烁或取消闪烁虚拟磁盘。
2. 如果位于**识别组件 LED** 页面上：
   - 选择或取消选择所有组件的 LED - 选择**全选/取消全选**选项，然后单击**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. 如果位于**识别物理磁盘**页面上：
   - 选择或取消选择所有物理磁盘驱动器或 PCIe SSD - 选择**全选/取消全选**选项，然后单击**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**全选/取消全选**选项，然后单击**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。

Blinking or unblinking component LEDs using RACADM

To blink or unblink component LEDs, use the following commands:

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at **dell.com/esmmanuals**.

14 配置并使用虚拟控制台

您可以使用虚拟控制台管理远程系统，通过 Management Station 上的键盘、视频和鼠标控制受管服务器上相应的设备。这是适用于机架和塔式服务器的一项得到许可的功能。默认情况下，该功能在刀片服务器中可用。

主要功能有：

- 同时支持最多六个虚拟控制台会话。所有会话可同时查看同一受管服务器控制台。
- 您可以在支持的 Web 浏览器（使用 Java 或 ActiveX 插件）中启动虚拟控制台。如果 Management Station 上运行的操作系统并非 Windows，则必须使用 Java 查看器。
- 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。
- 您不能使用相同的插件打开从 Management Station 到受管服务器的两个虚拟控制台会话。
- 如果第二个用户请求虚拟控制台会话，将通知第一个用户并提供拒绝访问、允许只读访问或允许完全共享访问的选项。系统将通知第二个用户另一个用户已经得到控制权。第一个用户必须在三十秒内响应，否则将基于默认设置授予第二个用户访问权限。当两个会话并行活动时，第一个用户会在屏幕右上角看到一条信息，表明第二个用户有正在进行的会话。如果第一个用户和第二个用户都没有管理员权限，终止第一个用户的会话时会自动终止第二个用户的会话。

相关概念

配置 Web 浏览器以使用虚拟控制台
配置虚拟控制台
启动虚拟控制台

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. 27: 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

建议将显示器的显示分辨率配置为 1280x1024 像素或更高。

注: 如果您将活动虚拟控制台会话和较低分辨率的显示器连接到虚拟控制台，则服务器控制台分辨率当在本地控制台上选择服务器时可能会重设。如果系统运行 Linux 操作系统，则 X11 控制台可能在本地显示器中无法查看。在 iDRAC 虚拟控制台中按下 <Ctrl><Alt><F1> 以将 Linux 切换到文本控制台。

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 **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 或 Java 插件。

   ActiveX 查看器仅支持 Internet Explorer。Java 查看器支持任何浏览器。
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。

相关概念

配置 Web 浏览器以使用 Java 插件
配置 IE 以使用 ActiveX 插件
将 CA 证书导入管理站

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 位操作系统上可安装 32 位或 64 位 JRE 版本，或在 32 位操作系统上可安装 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）*。

相关概念

配置虚拟控制台

配置 IE 以使用 ActiveX 插件

您必须先配置 IE 浏览器设置，然后再启动和运行基于 ActiveX 的虚拟控制台和虚拟介质应用程序。ActiveX 应用程序将以签名的 CAB 文件形式从 iDRAC 服务器提供。如果在虚拟控制台中将插件类型设置为"本机 ActiveX"，则当您尝试启动虚拟控制台时，该 CAB 文件会下载至客户端系统并启动基于 ActiveX 的虚拟控制台。Internet Explorer 需进行一些配置来下载、安装和运行这些基于 ActiveX 的应用程序。

在 64 位浏览器上，Internet Explorer 具有 32 位和 64 位版本。您可以使用任一版本。但是，如果在 64 位版本中安装插件，然后尝试在 32 位浏览器中运行查看器，则必须重新安装插件。

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 2003、Windows XP、Windows Vista、Windows 7 和 Windows 2008 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**受信站点**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. 允许浏览器下载加密的内容并启用第三方浏览器扩展。要实现此操作，请转至**工具** → **Internet 选项** → **高级**，清除**不将加密的页存盘**选项，然后选择**启用第三方浏览器扩展**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**工具** → **Internet 选项** → **安全**，并选择您要运行该应用程序的区域。
6. 单击**自定义级别**。在**安全设置**窗口中执行以下操作：
   - 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**工具** → **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 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 控件之前，Internet Explorer 可能会显示安全警告。要完成 ActiveX 控件安装步骤，请在 Internet Explorer 发出安全警告时接受 ActiveX 控件。

相关概念

清除浏览器高速缓存
Windows Vista 或更新的 Microsoft 操作系统的附加设置

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. 确保没有为“可信站点”区域选择**启用保护模式**选项。或者，您可以将 iDRAC 地址添加到 Intranet 区域中的站点。默认情况下，保护模式对“Intranet 区域”和“可信站点”区域中的站点已关闭。

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 IE7 中的早期 ActiveX 版本

要清除 IE7 中早期版本的 ActiveX 查看器，请执行以下操作：

1. 关闭 Video Viewer（视频查看器）和 Internet Explorer 浏览器。
2. 重新打开 Internet Explorer 浏览器并转至 **Internet Explorer** → **工具** → **管理加载项**，然后单击**启用或禁用加载项**。随即会显示**管理加载项**窗口。
3. 从 **Show**（**显示**）下拉菜单中选择 **Add-ons that have been used by Internet Explorer**（**Internet Explorer 使用的加载项**）。
4. 删除 *Video Viewer*（*视频查看器*）插件。

清除 IE8 中的 ActiveX 早期版本

要清除 IE8 中早期版本的 ActiveX 查看器，请执行以下操作：

1. 关闭 Video Viewer（视频查看器）和 Internet Explorer 浏览器。
2. 重新打开 Internet Explorer 浏览器并转至 **Internet Explorer** → **工具** → **管理加载项**，然后单击**启用或禁用加载项**。随即会显示**管理加载项**窗口。
3. 从**显示**下拉菜单中选择**所有加载项**。
4. 选择*视频查看器*插件并单击**更多信息**链接。
5. 选择 **More Information**（**更多信息**）窗口中的 **REMOVE**（**删除**）。
6. 关闭 **More Information**（**更多信息**）和 **Manage Add-ons**（**管理插件**）窗口。

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. 在命令提示符处，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

当您启动虚拟控制台或虚拟介质时，系统会显示提示来验证证书。如果您具有自定义 Web 服务器证书，则可以将 CA 证书导入 Java 或 ActiveX 的可信证书库，从而避免这些提示。

相关概念

[将 CA 证书导入到 Java 受信证书库](#)
[将 CA 证书导入 ActiveX 受信证书库](#)

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 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 命令行工具创建使用 Secure Hash Algorithm（安全散列算法，SHA）的证书散列值。由于它在默认情况下使用 SHA，因此，建议使用 OpenSSL 工具 1.0.x 及更新版本。CA 证书必须为 Base64 encoded PEM（64 位编码的 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 Management Station 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. 将重命名后的 CA 证书复制到主目录，例如，**C:\Documents and Settings\<user> directory**。

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。

相关概念

[配置 Web 浏览器以使用虚拟控制台]
[启动虚拟控制台]

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 **Overview（概览）** → **Server（服务器）** → **Virtual Console（虚拟控制台）**。将显示 **Virtual Console（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 Online Help*（iDRAC 联机帮助）。
3. 单击 **Apply（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，请使用以下选项之一：

- 将 iDRAC.VirtualConsole 组中的对象与 set 命令配合使用。
- 将以下对象与 config 命令配合使用：
  - cfgRacTuneConRedirEnable
  - cfgRacTuneConRedirPort
  - cfgRacTuneConRedirEncryptEnable
  - cfgRacTunePluginType
  - cfgRacTuneVirtualConsoleAuthorizeMultipleSessions

有关这些对象的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

预览虚拟控制台

启动虚拟控制台之前，您可以预览 **System（系统）** → **Properties（属性）** → **System Summary（系统摘要）**页面中虚拟控制台的状态。**Virtual Console Preview（虚拟控制台预览）**区域显示一个图像，表明虚拟控制台的状态。该图像每隔 30 秒刷新一次。这是 licensed feature（许可的功能）。

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: 不要从受管系统上的 Web 浏览器启动虚拟控制台会话。

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 Java 或 ActiveX 插件。
- 可用的最小网络带宽为 1 MB/秒。

注: 如果嵌入式视频控制器在 BIOS 中已禁用，同时启动虚拟控制台，则虚拟控制台查看器为空白。

使用 32 位或 64 位 IE 浏览器启动虚拟控制台时，对两类浏览器分别都有所需的插件（Java 或 ActiveX）可用。"Internet 选项"设置对两种浏览器通用。

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 control panel（Java 控制面板）** → **General（常规）** → **Network Settings（网络设置）**并选择 **Direct Connection（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。

初次使用带有 ActiveX 插件的 IE8 启动虚拟控制台时，可能会显示 `Certificate Error: Navigation Blocked`（证书错误：导航已阻止）信息。单击 **Continue to this website（继续浏览此网站）**，然后单击 **Install**（安装）在 **Security Warning**（安全警告）窗口中安装 ActiveX 控件。虚拟控制台会话已启动。

相关概念

[使用 URL 启动虚拟控制台](#)
[配置 Web 浏览器以使用 Java 插件](#)
[配置 IE 以使用 ActiveX 插件](#)
[使用 Web 界面启动虚拟控制台](#)
[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](#)
[同步鼠标指针](#)

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 **Overview（概览）** → **Server**（服务器） → **Virtual Console（虚拟控制台）**。随即会显示 **Virtual Console**（虚拟控制台）页面。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。
- 转至 **Overview（概览）** → **Server**（服务器） → **Properties（属性）**。随即会显示 **System Summary**（系统摘要）页面。在 **Virtual Console Preview**（虚拟控制台预览）部分，单击 **Launch**（启动）。**Virtual Console Viewer**（虚拟控制台查看器）即会启动。

Virtual Console Viewer（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。

启动应用程序后，可能会显示多个消息框。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 Yes（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。要同步这两个光标，请参阅[同步鼠标指针](#)。

从 Windows Vista 管理站启动虚拟控制台可能会导致显示重新启动虚拟控制台的消息。要避免此问题，请在下列位置设置合适的超时值：

- **Control Panel**（控制面板） → **Power Options**（电源选项） → **Power Saver**（节能程序） → **Advanced Settings**（高级设置） → **Hard Disk**（硬盘） → **Turnoff Hard Disk After <time_out>（<time_out> 秒后关闭硬盘）**
- **Control Panel**（控制面板） → **Power Options**（电源选项） → **High–Performance**（高性能） → **Advanced Settings**（高级设置） → **Hard Disk**（硬盘） → **Turnoff Hard Disk After <time_out>（<time_out> 秒后关闭硬盘）**

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) 登录和单一登录 (SSO)。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。

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 **Yes**（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 **Continue**（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: 如果远程服务器关闭，则会显示消息“No Signal”（无信号）。

虚拟控制台查看器标题栏显示从管理站连接到 iDRAC 的 DNS 名称或 IP 地址。如果 iDRAC 没有 DNS 名称，则会显示 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>`

虚拟控制台查看器有时候会显示低质量视频。这是由于当您启动虚拟控制台会话时，网络连接速度过慢导致一两个视频帧丢失。要传输所有视频帧并改进后续视频质量，请执行以下任一操作：

- 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）。

同步鼠标指针

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。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 **Tools**（工具）菜单中选择 **Single Cursor**（单个指针）。
- 要设置鼠标加速，请转至 **Tools（工具） → Session Options（会话选项） → Mouse（鼠标）**。在 **Mouse Acceleration**（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: 这对运行 Windows 操作系统的受管系统不适用，因为该操作系统支持绝对定位。

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 **Tools（工具） → Session Options（会话选项） → Mouse（鼠标）**。在 **Mouse Acceleration（鼠标加速）**选项卡中，选择 **None**（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 **Virtual Console**（虚拟控制台）页面上将 **Max Sessions**（最大会话数）重新配置为 `1`。

通过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按键组合从管理站发送到受管系统。如果禁用此功能，它会将所有按键组合定向到虚拟控制台会话正在运行的管理站。要将所有键击传递到服务器，请在 Virtual Console Viewer（虚拟控制台查看器）中，转至 **Tools**（工具） **→ Session Options（会话选项） → General（常规）**选项卡并选择 **Pass all keystrokes to server**（将所有键击传递到服务器）选项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，必须加载本机库，Pass all keystrokes to server（将所有键击传递到服务器）和 Single Cursor（单个鼠标）模式才能起作用。如果未加载本机库，则 **Pass all keystrokes to server**（将所有键击传递到服务器）和 **Single Cursor**（单个鼠标）选项取消选中。如果您尝试选择任一选项，则会显示一条错误消息，指示不支持所选的选项。

  对于 ActiveX 客户端，必须加载本机库，Pass all keystrokes to server（将所有键击传递到服务器）功能才会起作用。如果未加载本机库，则 **Pass all keystrokes to server** （将所有键击传递到服务器）选项取消选择。如果您尝试选择任一选项，则会显示一条错误消息，指示不支持该功能。

  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。
- 管理站和受管系统上运行的操作系统。对管理站上的操作系统有意义的按键组合不会传递到受管系统。
- 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。

相关概念

[在 Windows 操作系统上运行的基于 Java 的虚拟控制台会话]
[在 Linux 操作系统上运行的基于 Java 的虚拟控制台会话]
[在 Windows 操作系统上运行的基于 ActiveX 的虚拟控制台会话]

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

- 系统始终会将所有单独的按键（不是不同按键的组合，而是一次单独的键击）发送到受管系统。这包括所有功能键、Shift、Alt、Ctrl 键和菜单键。这些按键中的一部分对 Management Station 和受管系统都有影响。

  例如，如果管理站和受管系统运行的是 Windows 操作系统，并且已禁用“传递所有按键”，则当您按下 Windows 按键来打开**开始**菜单时，管理站和受管系统上的**开始**菜单都会打开。但是，如果启用“传递所有按键”，则只有受管系统上的**开始**菜单会打开，管理站上不会打开。

- 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 键是由 Linux 内核进行解释的按键组合。如果 Management Station 或受管系统上的操作系统失去响应，您需要恢复系统，这会很有用。您可以使用下列方法之一在 Linux 操作系统上启用 Magic SysRq 按键。
  - 将一个条目添加到 **/etc/sysctl.conf**
  - echo "1" > /proc/sys/kernel/sysrq
- 如果 Pass all keystrokes to server（将所有按键传递给服务器）已启用，系统会将 Magic SysRq 按键发送到受管系统上的操作系统。重置操作系统（在取消安装或同步的情况下重新引导）的按键序列行为取决于 Management Station 上是否启用了 Magic SysRq：
  - 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/Telnet 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，将显示登录提示 `localhost.localdomain`。请使用操作系统用户名和密码登录。
3. 如果未启用 SysRq，请使用 `echo 1 >/proc/sys/kernel/sysrq` 启用。
4. 运行中断顺序 `~ B`。
5. 使用 SysRq 魔术键启用 SysRq 功能。例如，使用以下命令将显示控制台上的内存信息：

   ```
   echo m > /proc/sysrq-trigger displays
   ```

使用 SSH/Telnet 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`。随即将显示 `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。

15

管理虚拟介质

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。

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

对于机架式和塔式服务器，这是一个获得许可证的功能。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)、软盘驱动器（包括基于 USB 的驱动器）和 USB 闪存盘。
- 您只能在受管系统的 Management Station 上附加一个软盘、USB 闪存盘、映像、密钥或一个光盘驱动器。支持的软盘驱动器包括软盘映像或一个可用软盘驱动器。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。
- 无法从虚拟机访问 iDRAC 的虚拟软盘介质。
- 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。

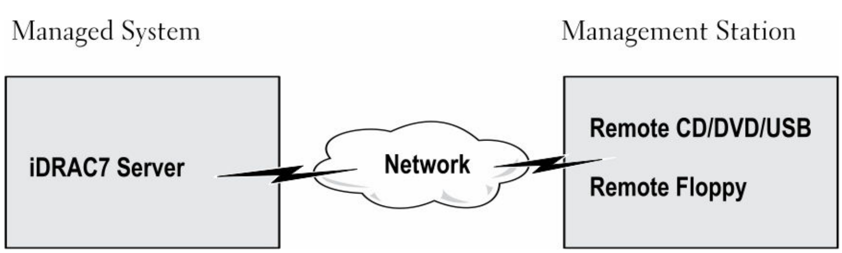


图 4: 虚拟介质设置

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. 28: 支持的驱动器和设备

驱动器	支持的存储介质
虚拟光驱	• 带有 1.44 软盘的传统 1.44 软盘驱动器 • CD-ROM • DVD • CD-RW • 带有 CD-ROM 介质的复合驱动器
虚拟软盘驱动器	• ISO9660 格式的 CD-ROM/DVD 映像文件 • ISO9660 格式的软盘映像文件
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。

相关概念

[配置 Web 浏览器以使用虚拟控制台]

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不要重设 iDRAC。否则，可能发生意外结果，包括丢失数据。**

1. 在 iDRAC Web 界面中，转至**概览** → **服务器** → **已附加介质**。
2. 指定所需设置。有关详细信息，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，请执行以下操作：

- 将 iDRAC.VirtualMedia 组中的对象与 set 命令配合使用。
- 将 cfgRacVirtual 组中的对象与 config 命令配合使用。

有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC*（适用于 iDRAC 的 RACADM 命令行参考指南）。

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**虚拟介质**部分中，根据需要选择**分离**、**附加**或**自动附加**。有关各选项的更多信息，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. 29: 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

必须在管理站中配置以下设置，以便显示空驱动器。要执行此操作，请在 Windows 资源管理器中，从**组织**菜单中单击**文件夹和搜索选项**。在**查看**选项卡上，取消选中**隐藏计算机文件夹中的空驱动器**选项，然后单击**确定**。

访问虚拟介质

可使用或不使用虚拟控制台访问虚拟介质。访问虚拟介质前，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，并且您尝试启动虚拟介质客户端，则会显示以下错误消息：*Virtual Media is currently unavailable. A Virtual Media or Remote File Share session is in use* （虚拟介质当前不可用。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。

相关概念

[配置 Web 浏览器以使用虚拟控制台]
[配置虚拟介质]

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**概览** → **服务器** → **虚拟控制台**。

   随即会显示 **Virtual Console**（**虚拟控制台**）页面。

2. 单击 **Launch**（**启动**）**Virtual Console**（**虚拟控制台**）。

   随即会启动 **Virtual Console Viewer**（**虚拟控制台查看器**）。

   注: 在 Linux 中，Java 是用于访问虚拟控制台的默认插件类型。在 Windows 中，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。

相关概念

配置 Web 浏览器以使用虚拟控制台
配置虚拟介质
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

不使用虚拟控制台启动虚拟介质

当禁用 **Virtual Console**（**虚拟控制台**）时，在启动虚拟介质前，请确保：

- 虚拟介质处于 *Attach*（*附加*）状态。
- 将系统配置为显示空驱动器。要执行此操作，请在 Windows 资源管理器中导航至 **Folder Options**（**文件夹选项**），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**）。

当禁用 Virtual Console（虚拟控制台）时，要启动虚拟介质：

1. 在 iDRAC Web 界面中，转至**概览** → **服务器** → **虚拟控制台**。

   随即会显示 **Virtual Console**（**虚拟控制台**）页面。

2. 单击 **Launch**（**启动**）**Virtual Console**（**虚拟控制台**）。

   随即显示以下消息：

   ```
   Virtual Console has been disabled. Do you want to continue using Virtual
   Media redirection?
   ```

3. 单击**确定**。

   此时将显示 **Virtual Media**（**虚拟介质**）窗口。

4. 在 **Virtual Media**（**虚拟介质**）菜单中，单击 **MAP CD/DVD**（**映射 CD/DVD**）或 **Map Removable Disk**（**映射可移动磁盘**）。

   有关更多信息，请参阅映射虚拟驱动器。

   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 Windows 操作系统客户端上，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。

相关概念

[配置虚拟介质](#)

[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](#)

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）并浏览至要用作映像文件的源的文件夹或目录。映像文件位于管理站或者受管系统的 C: 驱动器中。
3. 在 **Image File Name**（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）并浏览到一个位置。
4. 单击 **Create Image**（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，则会继续进行映像创建。

   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。

   文件夹作为映像添加时，将在使用此功能的管理站桌面上创建一个 **.img** 文件。如果移动或删除此 **.img** 文件，则 **Virtual Media**（虚拟介质）菜单中此文件夹对应的条目将不起作用。因此，使用*映像*时建议不要移动或删除 **.img** 文件。不过，可在首先取消选定相关条目然后使用 **Remove Image**（删除映像）删除该条目后删除该 **.img** 文件。

查看虚拟设备详细信息

要查看虚拟设备的详细信息，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）**部分将显示已映射的虚拟设备以及每个设备的读/写活动。如果已连接虚拟介质，将显示此信息。如果未连接虚拟介质，将显示“Virtual Media is not connected”（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。

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: 使用基于 ActiveX 的虚拟介质时必须具有管理权限才能映射操作系统 DVD 或 USB 闪存盘（已连接到管理站）。要映射驱动器，请以管理员身份启动 IE 或将 iDRAC IP 地址添加到受信任的站点列表中。

1. 要建立虚拟介质会话，请从 **Virtual Media**（虚拟介质）菜单中单击 **Connect Virtual Media**（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
   - 映射软盘

   注: 如果已在 **Attached Media**（已附加介质）页中启用 **Floppy Emulation**（软盘仿真）选项，将在列表中显示 **Map Floppy Disk**（映射软盘）菜单项。如果已启用 **Floppy Emulation**（软盘仿真），将使用 **Map Floppy Disk**（映射软盘）替换 **Map Removable Disk**（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。

2. 单击您要映射的设备类型。

   注: 如果虚拟介质会话目前在当前 Web 接口会话、另一个 Web 接口会话或在 VMCLI 中处于活动状态，则会显示活动会话。

3. 在 **Drive/Image File**（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、软盘）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；对于可移动磁盘和软盘，则为 IMG。

   如果在默认路径（桌面）中创建映像，当您选择 **Map Removable Disk**（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 **Map Removable Disk**（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 **Browse**（浏览）以指定映像。

4. 选择 **Read-only**（只读）将可写设备映射为只读。

   对于 CD/DVD 设备，默认情况下此选项处于启用状态，并且不能禁用。

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 **Virtual Media**（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 Virtual Media（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。

相关概念

[显示正确的虚拟驱动器用于映射]
[添加虚拟介质映像]

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和软盘，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。在开机自检期间按下 <F2> 进入 **System Setup（系统设置）**。
2. 转至 **SATA settings（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 **Client（客户端）**窗口。该窗口显示可映射的正确驱动器。

相关概念

[映射虚拟驱动器]

取消映射虚拟驱动器

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）。

   将显示一条消息，要求您进行确认。
2. 单击**是**。
   该菜单项的复选标记没有出现，表明其未映射至主机服务器。

   注: 从运行 Macintosh 操作系统的客户端系统中取消映射连接到 vKVM 的 USB 设备后，所取消映射的设备可能不可用于此客户端。通过重新启动系统或在客户端系统上手动挂载此设备可查看此设备。

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. 确保虚拟驱动器已经启用并列为带有可引导介质的首个设备。如果需要，请按照屏幕说明修改引导顺序。
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。

   受管系统将根据引导顺序尝试从可引导设备引导。如果已经连接虚拟设备并且具有可引导介质，系统将引导至虚拟设备。否则，系统将忽略设备，与处理没有可引导介质的物理设备时类似。

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。

相关概念

[映射虚拟驱动器]
[配置虚拟介质]

16

安装和使用 VMCLI 公用程序

虚拟介质命令行界面 (VMCLI) 公用程序是一个界面，它提供从管理站到受管系统上的 iDRAC 的虚拟介质功能。通过此公用程序，您可以访问虚拟介质功能，包括映像文件和物理驱动器，从而在网络中的多个远程系统上部署操作系统。

注: 只能在安装有 32 位操作系统的管理站上运行 VMCLI 公用程序。

VMCLI 公用程序支持以下功能：

- 管理可通过虚拟介质访问的可移动设备或映像。
- 启用 iDRAC 固件的**引导一次**选项之后将会自动终止会话。
- 使用安全套接字层 (SSL) 确保与 iDRAC 的通信安全。
- 执行 VMCLI 命令，直到：
  - 连接将自动终止。
  - 操作系统终止该进程。

  注: 要终止 Windows 中的进程，请使用任务管理器。

安装 VMCLI

VMCLI 公用程序包含在 *Dell Systems Management Tools and Documentation* DVD 中。

要安装 VMCLI 公用程序：

1. 将 *Dell Systems Management Tools and Documentation* DVD 插入 Management Station 的 DVD 驱动器。
2. 遵循屏幕上的说明安装 DRAC 工具。
3. 安装成功后，检查 **install\Dell\SysMgt\rac5** 文件夹以确保 **vmcli.exe** 存在。同样地，检查 UNIX 的各个路径。

   VMCLI 公用程序即已安装在系统上。

运行 VMCLI 公用程序

- 如果操作系统需要特定权限或组成员，则您需要相似的权限才能运行 VMCLI 命令。
- 在 Windows 系统上，非管理员必须具有 Power User（**高级用户**）权限才能运行 VMCLI 公用程序。
- 在 Linux 系统上，要访问 iDRAC，请运行 VMCLI 公用程序，并记录用户命令，非管理员用户必须在 VMCLI 命令前加上 `sudo`。但是，要添加或编辑 VMCLI 管理员组中的用户，请使用 `visudo` 命令。

VMCLI 语法

Windows 和 Linux 系统上的 VMCLI 界面完全相同。VMCLI 语法为：

`VMCLI [parameter] [operating_system_shell_options]`

例如，`vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

*参数*使 VMCLI 能够连接到指定的服务器，访问 iDRAC 并映射到指定虚拟介质。

注: VMCLI 语法区分大小写。

为了确保安全，推荐使用下列 VMCLI 参数：

- `vmcli -i` — 启用启动 VMCLI 的交互式方法。它可以确保当其他用户查看进程时用户名和密码不可见。
- vmcli `-r <iDRAC IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {< device-name > | < image-file >}` — 指示 iDRAC CA 证书是否有效。如果证书无效，运行此命令时将显示警告信息。但是，此命令可以成功执行，并将建立 VMCLI 会话。有关 VMCLI 参数的更多信息，请参阅 *VMCLI 帮助*或 *VMCLI 管理页面*。

相关概念

[访问虚拟介质的 VMCLI 命令]
[VMCLI 操作系统 Shell 选项]

访问虚拟介质的 VMCLI 命令

下列表格提供访问不同虚拟介质所需要的 VMCLI 命令。

表. 30: VMCLI 命令

虚拟介质	命令
软盘驱动器	`vmcli -r [RAC IP or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]`
可引导软盘或 USB 闪存盘映像	`vmcli -r [iDRAC IP address] [iDRAC user name] -p [iDRAC password] -f [floppy.img]`
CD 驱动器使用 -f 选项	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -f [device name]|[image file]-f [cdrom - dev ]`
可引导 CD/DVD 映像	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -c [DVD.img]`

如果文件不受写保护，虚拟介质可能会写入映像文件。要确保虚拟介质不会写入介质：

- 配置操作系统来写保护不应改写的软盘映像文件。
- 使用设备的写保护功能。

虚拟化只读映像文件时，多个会话可以共享同一映像介质。

虚拟化物理驱动器时，一次只能有一个会话访问一个给定物理驱动器。

VMCLI 操作系统 Shell 选项

VMCLI 使用 Shell 选项来启用下列操作系统功能：

- stderr/stdout 重定向 — 将任何打印的公用程序输出重定向至文件。

  例如，使用大于号字符 (>) 后接文件名将以 VMCLI 公用程序打印的输出覆盖指定的文件。

  注: VMCLI 公用程序不会从标准输入 (stdin) 读取数据。因此，不需要 stdin 重定向。

- 后台执行 — 在默认情况下，VMCLI 公用程序在前台执行。使用操作系统的命令 Shell 功能可让公用程序在后台运行。

  例如，在 Linux 操作系统下，在命令后接上 & 字符可以让程序变成一个新的后台进程。这种技术在脚本程序中非常有用，为 VMCLI 命令启动新的进程后，它可以让脚本继续执行（否则，脚本会停止执行，直到 VMCLI 程序终止）。

  如果启动多个 VMCLI 会话，请使用操作系统特定的工具来列出和终止进程。

17

管理 vFlash SD 卡

vFlash SD 卡是一个安全数字 (SD) 卡，插在系统 vFlash SD 卡插槽中。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 是获得许可证的功能。

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: 确保仅在 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，则初始化该卡时将显示以下错误消息：*An error has occurred while initializing SD card.（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。

配置 vFlash SD 卡

在配置 vFlash 之前，请确保系统上已安装 vFlash SD 卡。关于如何从系统安装和移除卡的信息，请参阅 **dell.com/support/manuals** 上系统的 *Hardware Owner's Manual*（硬件用户手册）。

注: 必须具有"访问虚拟介质"权限才能启用或禁用 vFlash 功能，以及对卡执行初始化操作。

相关概念

[查看 vFlash SD 卡属性](#)
[启用或禁用 vFlash 功能](#)
[初始化 vFlash SD 卡](#)

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**概览** → **服务器** → **vFlash**。随即会显示 **SD 卡属性**页面。有关所显示属性的信息，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，请使用以下方法之一：

- 将 `cfgvFlashSD` 对象与 `getconfig` 命令配合使用。将显示以下只读属性：
  - cfgvFlashSDSize
  - cfgVFlashSDLicensed
  - cfgvFlashSDAvailableSize
  - cfgvFlashSDHealth
  - cfgVFlashSDEnable
  - cfgVFlashSDWriteProtect
  - cfgVFlashSDInitialized
- 将以下对象与 `get` 命令配合使用：
  - 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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

使用 iDRAC 设置公用程序查看 vFlash SD 卡属性

要查看 vFlash SD 卡属性，请在 **iDRAC 设置公用程序**中转至**介质和 USB 端口设置**。**介质和 USB 端口设置**页面将显示属性。关于所显示的属性的信息，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**概览** → **服务器** → **vFlash**。

   随即会显示 **SD Card Properties**（**SD 卡属性**）页面。
2. 选中 **vFLASH Enabled**（**启用 vFLASH**）选项可启用 vFlash 功能，清除该选项则可禁用 vFlash 功能。如果已附加任何 vFlash 分区，则无法禁用 vFlash，并且会显示一条错误消息。

   注: 如果禁用 vFlash 功能，则不会显示 SD 卡属性。
3. 单击 **Apply**（**应用**）。vFlash 功能即会启用或禁用，具体取决于您的选择。

使用 RACADM 启用或禁用 vFlash 功能

要使用 RACADM 启用或禁用 vFlash 功能，请使用以下方法之一：

- 使用 `config` 命令：
  - 要启用 vFlash：
    ```
    racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
    ```
  - 要禁用 vFlash：
    ```
    racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
    ```
- 使用 `set` 命令：
  - 要启用 vFlash：
    ```
    racadm set iDRAC.vflashsd.Enable 1
    ```
  - 要禁用 vFlash：
    ```
    racadm set iDRAC.vflashsd.Enable 0
    ```

注: 只有存在 vFlash SD 卡时，RACADM 命令才能有用。如果没有卡，则显示以下消息：*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**。
   将会显示 **iDRAC 设置.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 卡处于写保护状态，将会禁用“初始化”选项。

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**概览 → 服务器 → 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，请使用以下方法之一：

- 使用 `vFlashSD` 命令：

```
racadm vflashsd initialize
```

- 使用 set 命令：

```
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。

有关这些命令的更多信息，请参阅 **dell.com/support/manuals** 和 **dell.com/esmmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

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**。
   将会显示 **iDRAC 设置.介质和 USB 端口设置**页面。
2. 单击 **Initialize vFlash（初始化 vFlash）**。
3. 单击 **Yes（是）**。初始化操作将开始。
4. 单击 **Back（后退）**并导航至同一 **iDRAC Settings . Media and USB Port Settings（iDRAC 设置.介质和 USB 端口设置）**页面查看成功消息。
   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 telnet、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，请使用以下命令：`racadm vflashpartition status -a`
4. 要获取特定分区的上次状态，请使用以下命令：`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: 管理员可在 vFlash 分区上执行所有操作。否则，您必须拥有 **Access Virtual Media（访问虚拟介质）**权限才能创建、删除、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: 如果在应用程序（例如 WS-MAN、iDRAC 设置公用程序或 RACADM）使用 vFlash 时单击 vFlash 页面上的任何选项，或导航到 GUI 中的其他一些页面，iDRAC 可能会显示以下消息：`vFlash is currently in use by another process. Try again after some time`（vFlash 当前正被另一个进程使用。请一段时间后再次尝试）。

vFlash 能够在没有其他正在进行的 vFlash 操作（例如格式化、附加分区等）时执行快速分区创建。因此，建议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

空白分区附加到系统时类似于空白 USB 闪存盘。可在 vFlash SD 卡上创建空白分区。可创建*软盘*或*硬盘*类型的分区。分区类型 CD 仅在使用映像创建分区时受支持。

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**概览** → **服务器** → **vFlash** → **创建空白分区**。

   将会显示 **Create Empty Partition（创建空白分区）**页面。
2. 指定所需的信息，然后单击**应用**。有关各选项的更多信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

   将默认创建新的未格式化的空白分区，该分区为只读。将显示表示进度百分比的页面。如果发生下列情况，将显示错误信息：

   - 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

创建 20 MB 空白分区：

1. 打开系统的 telnet、SSH 或串行控制台并登录。
2. 输入以下命令：`racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20`

   将创建 FAT16 格式的 20 MB 空白分区。默认情况下，空白分区将创建为读写分区。

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: 上载的映像和模拟类型必须匹配。iDRAC 模拟映像类型不正确的设备时会出现问题。例如，如果使用 ISO 映像创建分区并且模拟类型指定为“硬盘”，将无法从此映像引导 BIOS。
- 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，因为支持的最大分区大小为 4 GB。不过，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 文件系统上的映像文件。因此，图像文件具有 4 GB 的限制。

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**概览** → **服务器** → **vFlash** → **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. 输入所需信息，然后单击**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 模拟类型，将创建只读的分区。对于 Floppy（软盘）或 Hard Disk（硬盘）模拟类型，将创建读写分区。如果出现以下情况，将显示错误信息：

   - 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. 打开系统的 telnet、SSH 或串行控制台并登录。
2. 输入以下命令：`racadm vflashpartition create –i 1 –o drive1 –e HDD –t image –l //myserver/sharedfolder/foo.iso –u root –p mypassword`

   将创建一个新分区。默认情况下，创建的分区为只读。此命令对映像文件扩展名要区分大小写。如果文件扩展名为大写，例如 FOO.ISO 而不是 FOO.iso，则命令会返回语法错误。

   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。

格式化分区

您可以根据文件系统的类型格式化 vFlash SD 卡上的现有分区。支持的文件系统类型为 EXT2、EXT3、FAT16 和 FAT32。您只能格式化硬盘或软盘类型的文件分区，不能格式化 CD。您无法格式化只读分区。

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。

要格式化 vFlash 分区：

1. 在 iDRAC Web 界面中，转至**概览** → **服务器** → **vFlash** → **格式化**。
   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**确定**。
   所选分区将格式化为指定的文件系统类型。如果发生下列情况将显示错误信息：
   - 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**概览** → **服务器** → **vFlash** → **管理**。随即会显示**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 Telnet、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

可以将只读分区更改为读/写分区，反之亦然。修改分区前，请确保：

- vFlash 功能已启用。
- 具有 **Access Virtual Media（访问虚拟介质）**的权限。

注: 默认创建只读分区。

使用 Web 界面修改分区

要修改分区：

1. 在 iDRAC Web 界面中，转至**概览** → **服务器** → **vFlash** → **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: 如果分区为 CD 类型，状态将为只读。您无法将状态更改为读写。如果分区已附加，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. 打开系统的 telnet、SSH 或串行控制台并登录。
2. 使用以下任一方法：
   - 使用 `config` 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 config -g cfgvflashpartition -i 1 -o
       cfgvflashPartitionAccessType 1
       ```
     - 要将读写分区更改为只读分区：
       ```
       racadm config -g cfgvflashpartition -i 1 -o
       cfgvflashPartitionAccessType 0
       ```
   - 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，这些分区会以 USB 大容量存储设备显示在操作系统和 BIOS 中。当您附加多个分区时，根据分配的索引，这些分区在操作系统和 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**概览** → **服务器** → **vFlash** → **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. 打开系统的 telnet、SSH 或串行控制台并登录。
2. 使用以下任一方法：
   - 使用 `config` 命令：
     – 要连接分区：
     ```
     racadm config -g cfgvflashpartition -i 1 -o
     cfgvflashPartitionAttachState 1
     ```
     – 要断开分区连接：
     ```
     racadm config -g cfgvflashpartition -i 1 -o
     cfgvflashPartitionAttachState 0
     ```
   - 使用 `set` 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。
- 操作系统必须支持附加分区的文件系统。否则，您将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。同样，在 Linux 环境中，操作系统也无法读取 Windows 系统原生的 NTFS 分区类型。
- vFlash 分区卷标与模拟 USB 设备上的文件系统卷名不同。您可以从操作系统更改模拟 USB 设备的卷名。但是，这不会更改存储在 iDRAC 中的分区卷标名称。

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**概览 → 服务器 → vFlash → 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**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 telnet、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**概览 → 服务器 → vFlash → 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: 所有现有分区（附加分区除外）都将显示在列表中。第一个分区为默认选中。
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，请参阅设置第一引导设备。

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 分区设置为第一引导设备，请使用 `cfgServerInfo`。有关更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

注: 运行此命令时，vFlash 分区标签自动设置为引导一次 - `cfgserverBootOnce` 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。

18

使用 SMCLP

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 Common Information Model Object Manager（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（服务器硬件的系统管理架构，SMASH）标准以及 Server Management Working Group (SMWG) SMCLP 规范。

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 Telnet、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 **delltechcenter.com** 上提供了关于配置文件、扩展和 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。

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
- 管理 iDRAC 用户帐户
- 查看系统属性

运行 SMCLP 命令

您可以使用 SSH 或 Telnet 界面运行 SMCLP 命令。打开 SSH 或 Telnet 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 `-$` 的脚本可将这些用于 yx1x 系统；但从 yx2x 系统开始，使用 `admin->` 的脚本可用于刀片、机架和塔式服务器。

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，而目标确定运行该操作的实体（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. 31: SMCLP 动词

动词	定义
cd	使用 Shell 导航 MAP
set	将属性设定为特定值
help	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
version	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. 32: 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/pwrcap1	受管系统电源利用功能
admin1/system1/capabilities1/elecap1	受管系统目标功能
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/capabilities/PwrutilmgtCap1	电源利用管理功能
admin1/system1/sp1/capabilities1/elecap1	验证功能
admin1/system1/sp1/settings1	服务处理器设置收集

目标	定义
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
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	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/acctsvc1	本地用户帐户管理服务
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

目标	定义
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP 角色权限

相关概念

运行 SMCLP 命令
用法示例

导航 MAP 地址空间

可通过 SM-CLP 管理的对象通过在名为可管理接入点 (MAP) 地址空间的分层空间中排列的目标表示。地址路径可指定从地址空间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。这是您登录 iDRAC 时的默认起点。使用 `cd` 动词可从根向下导航。

注: 斜线 (/) 和反斜线 (\) 在 SM-CLP 地址路径中可互换。但是，命令行结尾的反斜线表示命令在下一行继续并将在分析命令时被忽略。

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` 动词可查找您在地址空间中的当前位置。`..` 和 `.` 缩写与它们在 Windows 和 Linux 中的作用相同：`..` 指父代级别而 `.` 指当前级别。

使用 show 动词

了解关于使用 `show` 动词的目标的详细信息。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` 选项使您可以将命令的输出限制为一个或多个属性、目标、关联和动词。例如，要仅显示当前位置的属性和目标，请使用以下命令：

```
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` 选项会在指定目标的附加级别运行状况上执行 `show` 命令。要查看地址空间中的所有目标和属性，请使用 `-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**。

默认格式为 **text**，并且是可读性最高的输出。**clpcsv** 格式是逗号分隔的值格式，适合加载到电子表格程序中。**keyword** 格式以每行一个"关键字=值"对列表的格式输出信息。**clpxml** 格式是一个包含 **response** XML 元素的 XML 文档。DMTF 已指定 **clpcsv** 和 **clpxml** 格式及其规格，可在 DMTF 网站 **dmtf.org** 上找到这些内容。

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
- SEL 管理
- 映射目标导航

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
  ```

  随即显示以下消息：

  ```
  system1 has been stopped successfully
  ```

- 要开启服务器：

  ```
  start /system1
  ```

  随即显示以下消息：

  ```
  system1 has been started successfully
  ```

- 要重新引导服务器：

  ```
  reset /system1
  ```

  随即显示以下消息：

  ```
  system1 has been reset successfully
  ```

SEL 管理

以下示例显示如何使用 SMCLP 在受管系统上执行 SEL 相关操作。在 SMCLP 命令提示符下键入以下命令：

- 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
```

- 清除 SEL：

  ```
  delete /system1/logs1/log1/record*
  ```

  系统将显示以下输出：

  ```
  All records deleted successfully
  ```

映射目标导航

以下示例显示如何使用 cd 动词导航 MAP。在所有示例中，初始默认目标假定为 /。

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：
  输入 `cd .`

- 要向上移动一级：
  输入 `cd ..`
- 要退出：
  `exit`

19

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。它没有界面，但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。

注: 仅在已安装 iDRAC Express 或 iDRAC Enterprise 许可证之后，才能使用 iDRAC 服务模块。

在使用 iDRAC 服务模块之前，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 服务模块功能。
- 操作系统到 iDRAC 的直通功能可在 iDRAC 中通过内部 USB 总线启用。

  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。

安装 iDRAC 服务模块

您可以从 **dell.com/support** 下载和安装 iDRAC Service Module。必须在服务器的操作系统上拥有管理员权限才能安装 iDRAC Service Module。有关如何进行安装的信息，请参阅 **dell.com/support/manuals** 上的 *iDRAC Service Module Installation Guide*（iDRAC Service Module 安装指南）。

注: 此功能不适用于 Dell Precision PR7910 系统。

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 **dell.com/openmanagemanuals.com** 上提供的 *iDRAC Service Module Installation Guide*（iDRAC Service Module 安装指南）。

iDRAC Service Module 监测功能

iDRAC 服务模块提供以下监测功能：

- 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
- 与技术支持报告集成。仅在已安装 iDRAC Service Module 2.0 或更高版本时才适用。有关更多信息，请参阅生成技术支持报告。
- 准备移除 NVMe PCIe SSD。有关更多信息，请参阅 iDRACUG_准备移除 NVMe PCIe SSD。

注: Windows Management Instrumentation 提供程序、通过 iDRAC 准备移除 NVMe 设备、技术支持报告操作系统自动收集等功能仅在最低固件版本为 2.00.00.00 或更高版本的 Dell PowerEdge 服务器上受支持。

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 提供相似的信息，例如在 iDRAC 中的操作系统名称、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，将不会禁用此功能。

iDRAC Service Module 2.0 已通过操作系统网络接口监测功能修订操作系统信息功能。如果将 iDRAC Service Module 2.0 版与 iDRAC 2.00.00.00 一起使用，它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。有关更多信息，请参阅查看主机操作系统上可用的网络接口。

在将 iDRAC Service Module 2.0 版与低于 2.00.00.00 的 iDRAC 版本一起使用时，操作系统信息功能不会提供操作系统网络接口监测功能。

将 Lifecycle 日志复制到操作系统日志

您可以在 iDRAC 中启用此功能时将 Lifecycle Controller 日志复制到操作系统日志。这类似于 OpenManage Server Administrator 所执行的系统事件日志 (SEL) 复制。将使用 iDRAC 服务模块在操作系统日志中复制已将 **OS Log**（操作系统日志）选项选作目标（在 **Alerts**（警报）页面，或等效的 RACADM 或 WSMAN 界面中）的所有事件日志。在操作系统日志中包含的默认日志集与为 SNMP 警报或陷阱配置的日志集相同。

iDRAC Service Module 还将记录在操作系统未处于运行状态时发生的事件。由 iDRAC Service Module 执行的操作系统日志记录操作将遵循基于 Linux 的操作系统所使用的 IETF 系统日志标准。

注: 从 iDRAC Service Module 2.1 版本开始，Lifecycle Controller 日志在 Windows 操作系统日志中的复制位置可以使用 iDRAC Service Module 安装程序配置。可在安装 iDRAC Service Module 时或修改 iDRAC Service Module 安装程序时，配置此位置。

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。

系统自动恢复选项

ASR 功能是一种基于硬件的计时器。如果发生硬件故障，有可能不会调用 Health Monitor，但服务器会如同激活电源开关时一样进行重设。ASR 使用连续递减的“心跳”计时器实现。Health Monitor 频繁重新加载计数器，以防止计数器递减至零。如果 ASR 计数至零，则认定为操作系统已锁定，系统将自动尝试重新引导。

您可以执行系统自动恢复操作，例如在指定时间后重新引导、重启或关闭服务器。仅在已禁用操作系统监视程序计时器之后，才会启用此功能。如果已安装 OpenManage Server Administrator，将禁用此监测功能，以避免重复的监视程序计时器。

Windows Management Instrumentation 提供程序

WMI 是对 Windows Driver Model 的一组扩展，它提供了一个操作系统接口，所配备的组件通过此接口提供信息和通知。WMI 是 Microsoft 对基于 Web 的企业管理 (WBEM) 和通用信息模型 (CIM) 标准的实现，它从 Distributed Management Task Force (DMTF) 管理服务器硬件、操作系统和应用程序。WMI 提供程序有助于集成系统管理控制台（例如 Microsoft System Center），并启用脚本以管理 Microsoft Windows Server。

可以在 iDRAC 中启用或禁用 WMI 选项。iDRAC 将通过 iDRAC Service Module 显示 WMI 类，以提供服务器运行状况信息。默认情况下，WMI 信息功能已启用。iDRAC Service Module 在 iDRAC 中通过 WMI 提供 WSMAN 所监测的类。这些类在 **root/cimv2/dcim** 命名空间中提供。

可以通过使用任何标准的 WMI 客户端界面访问这些类。有关更多信息，请参阅配置文件说明文件。

以下示例使用 DCIM_account 类演示 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细信息，请参阅 Dell TechCenter 提供的 WSMAN 配置文件说明文件。

CIM 接口	WinRM	WMIC	PowerShell
枚举类实例	`winrm e wmi/root/cimv2/dcim/dcim_account`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account`	`Get-WmiObject dcim_account -namespace root/cimv2/dcim`
获取类的特定实例	`winrm g wmi/root/cimv2/dcim/DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name="iDRAC.Embedded.1#Users.16"`	`Get-WmiObject -Namespace root\cimv2\dcim -Class dcim_account -filter "Name='iDRAC.Embedded.1#Users.16'"`
获取实例的关联实例	`winrm e wmi/root/cimv2/dcim/* -dialect:association -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name='iDRAC.Embedded.1#Users.2' ASSOC`	`Get-Wmiobject -Query "ASSOCIATORS OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`
获取实例的引用	`winrm e wmi/root/cimv2/dcim/* -dialect:association –associations -filter:`	不适用	`Get-Wmiobject -Query "REFERENCES OF {DCIM_Account.CreationClassName='DCI`

CIM 接口	WinRM	WMIC	PowerShell
	{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}		M_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim

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。

如果已在 iDRAC 服务模块安装期间启用监测功能，则在安装完成后，如果 iDRAC 服务模块检测到存在 OpenManage Server Administrator，它将禁用重叠的监测功能集。如果 OpenManage Server Administrator 正在运行，则 iDRAC 服务模块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 **Overview**（**概览**）**Server**（**服务器**）**Service Module**（**服务模块**）。
   将显示 **iDRAC Service Module Setup**（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。
3. 要执行带外监测功能，请选择以下一个或多个选项：
   - **OS Information**（操作系统信息）- 查看操作系统的信息。
   - **Replicate Lifecycle Log in OS Log**（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。如果系统上已安装 OpenManage Server Administrator，将禁用此选项。
   - **WMI 信息** - 包括 WMI 信息。
   - **Auto System Recovery Action**（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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

20

使用 USB 端口进行服务器管理

在第 12 代 Dell PowerEdge 服务器中，所有 USB 端口都专用于服务器。在第 13 代服务器中，其中一个前面板 USB 端口供 iDRAC 用于管理用途（如预配置和故障排除）。此端口有一个图标用于指示其为管理端口。所有配备有 LCD 面板的第 13 代服务器都支持此功能。此端口在订购的少数几个不带 LCD 面板的 200-500 型号中不可用。在此情况下，您最好将这些端口用于服务器操作系统。

此 USB 端口由 iDRAC 使用时：

- 通过使用连接到 iDRAC 的 USB 型 A/A 电缆，此 USB 网络接口允许从便携式设备（例如膝上型计算机）使用现有的远程带外管理工具。将为 iDRAC 分配 IP 地址 (169.254.0.3)，为膝上型计算机分配 IP 169.254.0.4。
- 您可以将服务器配置文件存储在 USB 设备中，并从此 USB 设备更新服务器配置。

注: 此功能在以下设备中受支持：

- 具有 FAT 文件系统和单个分区的 USB 设备。
- 所有 Dell Windows 8 和 Windows RT 平板电脑，包括 XPS 10 和 Venue Pro 8。对于具有微型 USB 端口的设备（如 XPS 10 和 Venue Pro 8），必须结合使用 On-The-Go (OTG) 适配器和 A/A 型电缆才能使其工作。

相关概念

使用 USB 设备上的服务器配置文件配置 iDRAC

相关任务

通过直接 USB 连接访问 iDRAC 界面

通过直接 USB 连接访问 iDRAC 界面

在 13 代服务器中，新引入的 iDRAC Direct 功能允许用户直接将膝上型计算机或 PC 的 USB 端口连接到 iDRAC 的 USB 端口。这样，您就可以直接与 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。
必须使用 A/A 型电缆将膝上型计算机（USB 主机控制器）连接到服务器中的 iDRAC（USB 设备）。

在 iDRAC 充当 USB 设备并且管理端口模式已设置为“自动”时，此 USB 端口将始终由 iDRAC 使用。此端口不会自动切换到操作系统。

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. 确保该 USB 端口已启用。有关更多信息，请参阅配置 USB 管理端口设置。
3. 用一条 A/A 型电缆将膝上型计算机连接到 iDRAC 的 USB 端口。
   管理 LED（如果存在）将呈绿色亮起，并保持亮起两秒钟。
4. 等待为膝上型计算机 (169.254.0.4) 和 iDRAC (169.254.0.3) 分配 IP 地址。完成此操作可能需要几秒钟。

5. 开始使用 iDRAC 网络界面，例如 Web 界面、RACADM 或 WS-Man。
6. 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。
7. 在使用之后，断开电缆连接。

   然后 LED 将关闭。

使用 USB 设备上的服务器配置文件配置 iDRAC

通过新的 iDRAC Direct 功能，您可以对 iDRAC 进行服务器配置。首先在 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 设备连接服务器时，才能使用 iDRAC 接口设定 USB 管理端口设置。

注: 未配备 LCD 和 LED 面板的 PowerEdge 服务器不支持 USB 密钥。

相关概念

配置 USB 管理端口设置

相关任务

从 USB 设备导入服务器配置文件

配置 USB 管理端口设置

可以在 iDRAC 中配置 USB 端口：

- 可使用 BIOS 设置来启用或禁用服务器的 USB 端口。如果将其设置为**关闭所有端口**或**关闭前部端口**，iDRAC 会同时禁用受管的 USB 端口。可以使用 iDRAC 界面查看端口状态。如果状态为“禁用”：
  - iDRAC 不处理已连接至受管 USB 端口的 USB 设备或主机。
  - 可以修改受管的 USB 配置，但是只有已在 BIOS 中启用前面板 USB 端口之后，所执行的设置才会生效。
- 设置 USB 管理端口模式，该模式将确定 USB 端口是由 iDRAC 还是由服务器操作系统使用：
  - 自动（默认）：如果 USB 设备不受 iDRAC 支持或者设备上不存在服务器配置文件，USB 端口将从 iDRAC 断开连接，并连接到服务器。当从服务器移除设备时，端口配置将重设，并由 iDRAC 使用。
  - 标准操作系统使用：USB 设备始终由操作系统使用。
  - 仅限 iDRAC Direct：USB 设备始终由 iDRAC 使用。

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**概览** → **硬件** → **USB 管理端口**。
   将显示**配置 USB 管理端口**页面。
2. 从 **USB 管理端口模式**下拉菜单中，选择下列任一选项：
   - **自动** - USB 端口由 iDRAC 或服务器操作系统使用。
   - **标准操作系统使用** - USB 端口由服务器操作系统使用。
   - **仅限 iDRAC Direct** - USB 端口由 iDRAC 使用。
3. 从"iDRAC 管理：USB XML 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 XML 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**
   - **Enabled**（已启用）

   有关各字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
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.ManagementPortStatus`
- 要查看 USB 端口配置：
  `racadm get iDRAC.USB.ManagementPortMode`
- 要修改 USB 端口配置：
  `racadm set iDRAC.USB.ManagementPortMode <Automatic|Standard OS Use|iDRAC|>`

  注: 确保使用 RACADM set 命令时将标准操作系统使用属性括在单引号中。
- 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 **dell.com/esmmanuals.com** 上提供的 *iDRAC RACADM Command Line Interface Reference Guide*（iDRAC RACADM 命令行界面参考指南）。

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 **USB 管理端口模式**下拉菜单中，执行以下操作：
   - **自动** - USB 端口由 iDRAC 或服务器操作系统使用。
   - **标准操作系统使用** - USB 端口由服务器操作系统使用。
   - **仅限 iDRAC Direct** - USB 端口由 iDRAC 使用。
3. 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**
   - **Enabled**（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）。
4. 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.xml 和 control.xml 文件：

- 服务器配置文件位于 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。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、<modelnumber> -config.xml 或 config.xml。
- 控制 XML 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: 在导入服务器配置文件时，如更改 XML 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 XML 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。
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
   - <modelnum>-config.xml
   - config.xml
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

如果 USB LED 存在，它表示以下内容：

- 呈绿色稳定亮起 - 正在从 USB 设备复制服务器配置文件时。
- 呈绿色闪烁 - 正在执行作业时。
- 呈绿色稳定亮起 - 作业已成功完成时。

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。

21

使用 iDRAC 快速同步功能

数个 Dell 第 13 代 PowerEdge 服务器具有可支持快速同步功能的快速同步板。该功能允许通过移动设备进行服务器处管理。这允许您使用移动设备查看资源清册和监测信息，并配置基本 iDRAC 设置（如设置根用户凭据和配置第一引导设备）。

您可以在 iDRAC 中为移动设备（例如 OpenManage Mobile）配置 iDRAC 快速同步访问。您必须在移动设备上安装 OpenManage Mobile 应用，才能使用 iDRAC 快速同步界面管理服务器。

注: 此功能目前在采用 Android 操作系统的移动设备上受支持。

在当前版本中，此功能仅对 Dell PowerEdgeR730xd、R630 和 R730 机架式服务器可用。对于这些服务器，您可以选择订购此功能板。因此，这是一种追加销售的硬件，其功能不依赖于 iDRAC 软件许可。

iDRAC 快速同步硬件包括：

- 激活按钮 - 必须按此按钮才能激活快速同步界面。在密集堆叠的机架式基础架构中，这有助于确定和启用要与之通信的目标服务器。当空闲状态达到所配置的时间（默认值为 30 秒）或在按下相应按钮以取消激活之后，快速同步功能将变为非活动状态。
- 活动 LED - 如果快速同步功能被禁用，此 LED 会闪烁几次，然后熄灭。此外，如果触发了可配置的非活动计时器，此 LED 也将熄灭，并取消激活界面。

在 iDRAC 上配置 iDRAC 快速同步设置后，将移动设备移近服务器（即距离小于两厘米），读取关于服务器的相关信息并执行 iDRAC 配置设置。

通过 OpenManage Mobile，可以执行以下操作：

- 查看资源清册信息：
- 查看监测信息：
- 配置基本 iDRAC 网络设置

有关 OpenManage Mobile 的更多信息，请参阅 **dell.com/support/manuals** 上提供的 *OpenManage Mobile User's Guide*（OpenManage Mobile 用户指南）。

相关概念

[配置 iDRAC 快速同步功能](#)
[使用移动设备查看 iDRAC 信息](#)

配置 iDRAC 快速同步功能

通过使用 iDRAC Web 界面或 RACADM，可以配置 iDRAC 快速同步功能以访问移动设备：

- 访问 - 您可以指定以下任意一个选项来配置 iDRAC 快速同步功能的访问状态：
  - 读写 - 默认状态。

- 读写访问 - 允许您配置基本的 iDRAC 设置。
- 只读访问 - 允许您查看资源清册和监测信息。
- 禁止访问 - 不允许您查看信息和配置设置。

- 超时 - 您可以启用或禁用 iDRAC 快速同步非活动计时器：
  - 如果已启用，您可以指定多久后关闭快速同步模式。要打开，请再次按激活按钮。
  - 如果已禁用，计时器将不允许您输入超时的时长。
- 超时限制 - 您可以指定多久后禁用快速同步模式。默认值为 30 秒。

必须具有服务器控制权限才能配置设置。无需重新引导服务器即可使设置生效。

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 快速同步设置

要配置 iDRAC 快速同步：

1. 在 iDRAC Web 界面中，转至**概览 → 硬件 → 前面板**。
2. 在 **iDRAC 快速同步**部分中，从**访问**下拉菜单中选择下列选项之一以访问 Android 移动设备：
   - 读写
   - 只读
   - 已禁用
3. 启用计时器。
4. 指定超时值。
   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 快速同步设置

要配置 iDRAC 快速同步功能，请使用 **System.QuickSync** 组中的 racadm 对象。有关更多信息，请参阅 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

使用 iDRAC 设置公用程序配置 iDRAC 快速同步设置

要配置 iDRAC 快速同步：

1. 在 iDRAC 设置公用程序中，转至**前面板安全性**。
   此时将显示 **iDRAC 设置前面板安全性**页面。
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（15 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 **dell.com/support/manuals** 上提供的 *OpenManage Mobile User's Guide*（OpenManage Mobile 用户指南）中的相应步骤。

22

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：

- Virtual Media Command Line Interface（虚拟介质命令行界面，CLI）
- Virtual Media Console（虚拟介质控制台）
- 远程文件共享

相关任务

使用 VMCLI 部署操作系统
使用远程文件共享部署操作系统
使用虚拟介质部署操作系统

使用 VMCLI 部署操作系统

使用 vmdeploy 脚本部署操作系统之前，请确保：

- 在 Management Station 上安装 VMCLI 公用程序。
- 为用户启用 iDRAC 的**配置用户**和**访问虚拟介质**权限。
- 在 Management Station 上安装 IPMItool。

  注: 如果在受管系统或 Management Station 上配置了 IPv6，则 IPMItool 不起作用。

- 在目标远程系统上配置 iDRAC。
- 系统能够从映像文件引导。
- 在 iDRAC 中启用 LAN 上 IPMI。
- 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，按照基于标准网络的安装步骤进行操作，并将部署映像标记为只读，从而确保每个目标系统引导并执行相同的部署步骤。

- 虚拟介质状态为附加状态。
- 在 Management Station 中安装 **vmdeploy** 脚本。查看 VMCLI 附带的此示例 vmdeploy 脚本。该脚本介绍如何将操作系统部署到网络中的远程系统。它在内部使用 VMCLI 和 IPMItool。

  注: **vmdeploy** 脚本在安装过程中依赖于目录中的一些支持文件。要从其他目录使用脚本，请一并复制所有文件。如果没有安装 IPMItool 公用程序，请复制该公用程序及其他文件。

在目标远程系统上部署操作系统：

1. 在 **ip.txt** 文本文件中列出目标远程系统的 iDRAC IPv4 地址。每行列出一个 IPv4 地址。
2. 在 Management Station 驱动器中插入可引导操作系统 CD 或 DVD。
3. 使用管理员权限打开命令提示符并运行 **vmdeploy** 脚本：

```
vmdeploy.bat -r <iDRAC-IPAddress or file> -u <iDRAC-user> -p <iDRAC-user-passwd> [ -f {<floppy-image> | < device-name>} | -c { <device-name>|<image-file>} ] [-i <DeviceID>]
```

注: vmdeploy 不支持 IPv6，因为 IPv6 不支持 IPMI 工具。

注: vmdeploy 脚本处理 `-r` 选项的方式与 `vmcli -r` 选项略有不同。如果 `-r` 选项的参数是现有文件的名称，脚本将从指定文件读取 iDRAC IPv4 或 IPv6 地址，并对每行运行该公用程序一次。如果 `-r` 选项的参数并非文件名，则应为单一 iDRAC 地址。在这种情况下，**-r** 将如 VMCLI 公用程序所述工作。

下表介绍 vmdeploy 命令参数。

表. 33: vmdeploy 命令参数

参数	说明
`<iDRAC-user>`	iDRAC 用户名。该参数必须有以下属性： • 有效用户名 • iDRAC 虚拟介质用户权限 如果 iDRAC 验证失败，将会显示错误信息并且终止命令。
`<iDRAC-ip | file>`	iDRAC IP 地址或包含 iDRAC IP 地址的文件。
`<iDRAC-user-password>` 或 `<iDRAC-passwd>`	iDRAC 用户的密码。 如果 iDRAC 验证失败，将会显示错误信息并且终止命令。
`-c {<device-name> | <image-file>}`	指向操作系统安装 CD 或 DVD 的 ISO9660 映像的路径。
`<floppy-device>`	指向包含操作系统安装 CD、DVD 或软盘的设备的路径。
`<floppy-image>`	指向有效软盘映像的路径。
`<Device ID>`	引导一次的设备的 ID。

相关概念

配置虚拟介质

相关任务

配置 iDRAC

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 或 CIFS 将 ISO 或 IMG 映像文件挂载到受管系统。
2. 转至**概览** → **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 **Boot Once（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。

相关概念

管理远程文件共享
设置第一引导设备

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 或 CIFS 将其作为 CD 或 DVD 进行挂载）。RFS 是一种许可的功能。

注: CIFS 支持 IPv4 和 IPv6 地址，但 NFS 仅支持 IPv4 地址。

远程文件共享仅支持 **.img** 和 **.iso** 映像文件格式。系统会将 **.img** 文件重定向为虚拟软盘，而将 **.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。

注: 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。

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：

  Virtual Media is detached or redirected for the selected virtual drive.（虚拟介质与所选虚拟驱动器断开连接或重定向。）

RFS 的连接状态在 iDRAC 日志中提供。一旦连接，即使您从 iDRAC 注销，挂载 RFS 的虚拟驱动器也不会断开连接。如果重设 iDRAC 或者网络连接丢失，RFS 连接会关闭。在 CMC 和 iDRAC 中也可以通过 Web 界面和命令行选项来关闭 RFS 连接。CMC 的 RFS 连接始终会覆盖 iDRAC 中的现有 RFS 挂载。

注: iDRAC vFlash 功能与 RFS 没有关联。

如果将 iDRAC 固件从版本 1.30.30 更新到 1.50.50 固件时，存在活动的 RFS 连接并且已将虚拟介质附加模式设置为 **Attach（附加）**或 **Auto Attach（自动附加）**，则 iDRAC 会在固件升级完成和 iDRAC 重新引导后尝试重新建立 RFS 连接。

如果将 iDRAC 固件从版本 1.30.30 更新到 1.50.50 固件时，存在活动的 RFS 连接并且已将虚拟介质附加模式设置为 **Detach**（**断开**），则 iDRAC 不会在固件升级完成和 iDRAC 重新引导后尝试重新建立 RFS 连接。

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**概览** → **服务器** → **已附加介质**。
   将显示 **Attached Media**（已附加介质）页面。
2. 在 **Attached Media**（已附加介质）下，选择 **Attach**（附加）或 **Auto Attach**（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。有关这些字段的信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。
   映像文件路径示例：
   - CIFS —//<用于连接 CIFS 文件系统的 IP>/<文件路径>/<映像名称>
   - NFS - <用于连接 NFS 文件系统的 IP>/<文件路径>/<映像名称>

   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> 。

   映像文件路径、用户名和密码支持以下字符：
   - 大写字符
   - 小写字符
   - 数字 0-9
   - _、-、?、<、>、/、\、:、*、|、@
   - 空格

   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。
4. 单击 **Apply**（应用），然后单击 **Connect**（连接）。
   在建立连接后，**Connection Status**（连接状态）显示为 **Connected**（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。

   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` 而软盘设备是 /dev/sdc。要确保使用正确的设备（用于 SLES 或 RHEL），当您连接虚拟设备时，必须在 Linux OS 上立即运行该命令：

   ```
   tail /var/log/messages | grep SCSI
   ```

   这将显示标识设备的文本（例如，SCSI 设备 sdc）。在运行级别 init 3 中使用 Linux 发行版时，此程序也适用于虚拟介质。默认情况下，虚拟介质在 init 3 中并非自动挂载。

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>
```

选项可为：

–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>: 网络共享上的映像位置；在位置周围使用双引号。请参阅使用 Web 界面配置远程文件共享部分中的映像文件路径示例。

–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）。

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. 请执行以下操作之一：
   - 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。

相关概念

配置虚拟介质
设置第一引导设备

相关任务

[配置 iDRAC]

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。

相关概念

[关于 IDSDM]

相关任务

[在 BIOS 中启用 SD 模块和冗余]

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**内部 USB 端口**设置为**开**。如果设置为关，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) 仅在适用的平台上提供。IDSDM 通过使用作为第一个 SD 卡内容的镜像的另一个 SD 卡的管理程序 SD 卡来提供冗余性。

这两个 SD 卡都可以作为主卡。例如，如果在 IDSDM 中安装两个新的 SD 卡，SD1 是活动（主）卡，SD2 是备用卡。系统会将数据会写入两个卡上，但是只从 SD1 进行读取。无论何时，如何移除 SD1 或者 SD1 发生故障，SD2 会自动变成活动（主）卡。

您可以使用 iDRAC Web 或 RACADM 查看状态、运行状况和 IDSDM 的可用性。系统会将 SD 卡冗余状态和故障事件记录到 SEL 中，并显示在前面板上。如果启用警报，会生成 PET 警报。

相关概念

查看传感器信息

23

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

相关任务

使用诊断控制台
计划远程自动诊断
查看开机自检代码
查看引导和崩溃捕获视频
查看日志
查看上次系统崩溃屏幕
查看前面板状态
硬件故障指示灯
查看系统运行状况
生成技术支持报告

使用诊断控制台

iDRAC 提供了标准的网络诊断工具集，这与 Microsoft Windows 或基于 Linux 的系统中包含的工具类似。通过使用 iDRAC Web 界面，您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**概览** → **服务器** → **故障排除** → **诊断程序**。
2. 在**命令**文本框中输入命令，然后单击**提交**。有关各命令的详细信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

   随即结果会显示在同一页面上。

计划远程自动诊断

您可以在服务器上以一次性事件形式远程调用自动脱机诊断程序并返回结果。如果诊断程序需要重新引导，您可以立即重新引导，或计划为在以后的重新引导或维护周期（类似于更新）中执行。在运行诊断程序时，会收

集结果并将其存储在内部 iDRAC 存储设备中。然后，可以使用 `diagnostics export` racadm 命令将结果导出到 NFS 或 CIFS 网络共享。您也可以使用相应的 WSMAN 命令运行诊断程序。有关更多信息，请参阅 WSMAN 文档。

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。如果您指定“当前时间”，将在下次重新引导时运行诊断程序。
- 结束时间 - 在开始时间之后的日期和时间运行诊断。如果诊断未在结束时间前启动，则它会被标记为失败，并且结束时间已过期。如果指定“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：

- 系统电源关闭后重启
- 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，iDRAC 将重启操作系统）

一次只能计划或运行一个诊断作业。诊断作业的状态可为成功完成、完成但出错或未成功。将在 Lifecycle Controller 日志中记录诊断事件，其中包含结果信息。您可以使用远程 RACADM 和 WSMAN 检索上一个执行的诊断作业的结果。

可以将已远程计划的上一个已完成诊断作业的诊断结果导出到网络共享（例如 CIFS 或 NFS）。最大文件大小为 5 MB。

当诊断作业的状态为“未计划”或“已计划”时，您可以取消诊断作业。如果正在运行诊断，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 share> -u <username> -p
<password>
```

有关各选项的更多信息，请参阅 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

查看开机自检代码

开机自检代码是系统 BIOS 提供的进度指示器，表示通电重设的引导顺序的各个阶段，并且可让您诊断与系统引导相关的各种故障。**Post Codes（开机自检代码）**页面显示引导操作系统前的最新系统开机自检代码。

要查看开机自检代码，请转至 **Overview（概览）** → **Server（服务器）** → **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。引导循环视频按照从新到旧的顺序进行排列。
- 最后一次崩溃视频 — 崩溃视频记录导致故障的事件序列。

这是一个获得许可证的功能。

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。

要查看**引导捕获**屏幕，请单击**概览** → **服务器** → **故障排除** → **视频捕获**。

视频捕获屏幕随即会显示录制的视频。有关详细信息，请参阅 *iDRAC Online Help*（iDRAC 联机帮助）。

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**概览** → **服务器** → **故障排除** → **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 Lifecycle 日志。有关更多信息，请参阅查看系统事件日志和查看 Lifecycle 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。这是一个获得许可证的功能。

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**概览** → **服务器** → **故障排除** → **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。

相关概念

启用上次崩溃屏幕

查看前面板状态

受管系统上的前面板概要显示系统中下列组件的状态：

- 电池
- 风扇
- 侵入
- 电源设备
- 可移除闪存介质
- 温度
- 电压

您可以查看受管系统的前面板状态：

- 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**概览** → **硬件** → **前面板**。将显示**前面板**页面。

Live Front Panel Feed（前面板实时信息）区域显示当前在 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 **Hide Error**（隐藏错误）和 **UnHide Error**（取消隐藏错误）灰显。您只能隐藏或取消隐藏机架和塔式服务器的错误。

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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

相关概念

配置 LCD 设置

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**概览** → **硬件** → **前面板**。**前面板实时信息**部分将显示前面板当前的状态：

- 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），**Hide Error**（隐藏错误）和 **UnHide Error**（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。

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 **dell.com/idracmanuals** 上提供的 *iDRAC8 RACADM Command Line Interface Reference Guide*（iDRAC8 RACADM 命令行界面参考指南）。

相关概念

配置系统 ID LED 设置

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 *Hardware Owner's Manual（硬件用户手册）* 中关于硬件设备的特定故障排除信息。

小心: 您只能执行产品文档中授权的故障排除和简单修复操作，或者根据在线或电话服务以及支持团队的指示进行操作。由于非 Dell 授权的维修而导致的损坏不在保修之列。请阅读并遵循产品随附的安全说明。

查看系统运行状况

iDRAC 和 CMC（适用于刀片服务器）Web 界面将显示下列项的状态信息：

- 电池
- 风扇
- 侵入
- 电源设备
- 可移除闪存介质
- 温度
- 电压
- CPU

在 iDRAC Web 界面中，转至**概览** → **服务器** → **系统摘要** → **服务器运行状况**部分。

要查看 CPU 运行状况，请转至 **Overview（概览）** → **Hardware（硬件）** → **CPU**。

系统运行状况指示灯为：

- — 表示处于正常状态。
- — 表示处于警告状态。
- — 表示处于故障状态。
- — 表示处于未知状态。

单击 **Server Health（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。

生成技术支持报告

如果您必须与技术支持人员一起处理服务器问题，但是因为安全策略导致无法直接访问 Internet，则您可以向技术支持人员提供必要的数据，以帮助进行故障排除，而无需安装软件或从 Dell 下载工具，并且无需从服务器操作系统或 iDRAC 访问 Internet。您可以从其他系统发送报告，并确保在向技术支持人员传输从您服务器收集的数据时这些数据不会被未授权人员看到。

您可以生成服务器的运行状况报告，然后将此报告导出到管理站（本地）中的位置或导出到共享网络位置（例如通用 Internet 文件系统 (CIFS) 或网络文件共享 (NFS)）。然后，您可以直接与技术支持人员共享此报告。要导出到 CIFS 或 NFS 等网络共享，必须直接通过网络连接到 iDRAC 共享或专用网络端口。

将生成标准 ZIP 格式的报告。此报告包含与 DSET 报告中信息相似的信息，例如：

- 所有组件的硬件资源清册
- 系统、Lifecycle Controller 和组件属性
- 操作系统和应用程序信息
- 活动的 Lifecycle Controller 日志（不包括已归档的日志条目）
- PCIe SSD 日志
- 存储控制器日志

注: Dell 第 12 代 PowerEdge 服务器不支持 TTYLog 使用 TSR 功能收集 PCIe SSD 数据。

生成报告后，您可以查看此报告。报告包含一组 XML 文件和日志文件。必须与技术支持人员共享此报告以对问题进行故障排除。

在每次执行数据收集操作时，将在 Lifecycle Controller 日志中记录一个事件。此事件包括诸如所用界面、导出日期和时间及 iDRAC 用户名等信息。

可通过以下两种方式生成“操作系统应用程序和日志”报告：

- 自动 — 使用自动调用 OS Collector 工具的 iDRAC 服务模块。
- 手动 - 从服务器操作系统手动执行 OS Collector 可执行文件。iDRAC 会向服务器操作系统提供 OS Collector 可执行文件（以标记为 DRACRW 的 USB 设备形式提供）。

注:

- OS Collector 工具不适用于 Dell Precision PR7910 系统。
- 操作系统日志收集功能在 CentOS 操作系统上不受支持。

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。

相关概念

[自动生成技术支持报告]
[手动生成技术支持报告]

自动生成技术支持报告

如果已安装 iDRAC Service Module，您可以自动生成技术支持报告。iDRAC Service Module 会调用主机操作系统上的相应 OS Collector 文件，收集数据，并将此数据传输到 iDRAC。然后，可以将该报告保存至所需的位置。

使用 iDRAC Web 界面自动生成技术支持报告

要自动生成技术支持报告，请执行以下操作：

1. 在 iDRAC Web 界面中，转至 **Overview**（概览） → **Server**（服务器） → **Troubleshooting** （故障排除） → **Tech Support Report**（技术支持报告）。

   将显示 **Tech Support Report**（技术支持报告）页面。
2. 选择要为其收集数据的选项：
   - **硬件**
   - **操作系统和应用程序数据**

     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。
   - 单击**高级导出选项**以选择下列其他选项：
     - **RAID 控制器日志**
     - **操作系统和应用程序数据**下的**启用报告筛选**

   根据选定的选项，收集数据所需的时间显示在这些选项的旁边。
3. 选择**我同意允许技术支持部门使用此数据**选项，然后单击**导出**。
4. 在 iDRAC Service Module 完成向 iDRAC 传输操作系统和应用程序数据后，会将其与硬件数据一起打包并生成最终报告。将显示一条消息，用于保存报告。

5. 指定用于保存技术支持报告的位置。

手动生成技术支持报告

当未安装 iSM 时，您可以手动运行 OS Collector 工具以生成技术支持报告。必须在服务器操作系统上运行 OS Collector 工具以导出操作系统和应用程序数据。将在服务器操作系统中显示一个标记为 DRACRW 的虚拟 USB 设备。此设备包含特定于主机操作系统的 OS Collector 文件。可从服务器操作系统运行特定于操作系统的文件以收集数据，并将数据传输到 iDRAC。然后，您可以将报告导出到本地或网络共享位置。

在 Dell 第 13 代 PowerEdge 服务器中，出厂时已安装 OS Collector DUP。但是，如果您确定 iDRAC 中没有 OS Collector，则可以从 Dell 支持网站下载 DUP 文件，然后通过固件更新过程将该文件上载到 iDRAC。

在使用 OS Collector 工具手动生成技术支持报告之前，请在主机操作系统中执行以下操作：

- 在 Linux 操作系统中：检查 IPMI 服务是否正在运行。如果未运行，必须手动启动该服务。下表提供了在每种 Linux 操作系统可用于检查 IPMI 服务状态以及启动该服务（如果需要）的命令。

Linux 操作系统	用于检查 IPMI 服务状态的命令	用于启动 IPMI 服务的命令
Red Hat Enterprise Linux 5 64 位	`$ service ipmi status`	`$ service ipmi start`
Red Hat Enterprise Linux 6		
SUSE Linux Enterprise Server 11		
CentOS 6		
Oracle VM		
Oracle Linux 6.4		
Red Hat Enterprise Linux 7	`$ systemctl status ipmi.service`	`$ systemctl start ipmi.service`

  注:

  - CentOS 仅受 iDRAC Service Module 2.0 或更高版本支持。
  - 如果 IPMI 模块已不存在，则可以从操作系统分发介质中安装相应的模块。在安装完成后，服务将立即启动。

- 在 Windows 操作系统中：
  - 检查 WMI 服务是否正在运行：
    - 在停止 WMI 之后，OS Collector 将自动启动 WMI 并继续执行收集操作。
    - 如果 WMI 已禁用，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未导致无法获取注册表或软件数据。

使用 iDRAC Web 界面手动生成技术支持报告

要手动生成技术支持报告：

1. 在 iDRAC Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Troubleshooting （故障排除）** → **Tech Support Report（技术支持报告）**。
   将显示 **Tech Support Report**（技术支持报告）页面。
2. 选择要为其收集数据的选项：

- **硬件**，将报告导出到本地系统上的位置。
- **操作系统和应用程序数据**，将报告导出到网络共享并指定网络设置。

  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。
- 单击**高级导出选项**以选择下列其他选项：
  - **RAID 控制器日志**
  - **操作系统和应用程序数据**下的**启用报告筛选**

根据选定的选项，收集数据所需的时间显示在这些选项的旁边。

如果系统上未运行 OS Collector 工具，则操作系统和应用程序数据选项将呈灰色而不可选择。系统显示消息 OS and Application Data (Timestamp Never)。

如果系统上曾运行过 OS Collector 工具，则显示上次收集操作系统和应用程序数据的时间戳：Last Collected: <timestamp>。

3. 单击**连接 OS Collector**。

   将引导您访问主机操作系统。此时会出现一条消息，要求您启动虚拟控制台。
4. 启动虚拟控制台后，单击弹出式消息以运行和使用 OS Collector 工具来收集数据。
5. 导航至由 iDRAC 为系统提供的 DRACRW 虚拟 USB 设备。
6. 调用适用于主机操作系统的 OS Collector 文件：
   - 对于 Windows，运行 **Windows_OSCollector_Startup.bat**。
   - 对于 Linux，运行 **Linux_OSCollector_Startup.exe**。
7. 在 OS Collector 将数据传输到 iDRAC 后，iDRAC 会自动删除 USB 设备。
8. 返回到**技术支持报告**页面，单击**刷新**图标，以反映新的时间戳。
9. 要导出数据，请在**导出位置**下选择**本地**或**网络**。
10. 如果已选择**网络**，请输入网络位置的详细信息。
11. 选择**我同意允许技术支持部门使用此数据**选项，然后单击**导出**以将数据导出到指定位置。

使用 RACADM 手动生成技术支持报告

要使用 RACADM 生成 TSR ，请使用 **techsupreport** 子命令。有关更多信息，请参阅 **dell.com/esmmanuals.com** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

在服务器状态屏幕上检查错误消息

琥珀色 LED 闪烁，并且特定服务器有错误时，LCD 上的主要 Server Status Screen（服务器状态屏幕）会以橙色突出显示受影响的服务器。使用 LCD 导航按钮突出显示受影响的服务器，然后单击中间的按钮。错误和警告信息将在第二行中显示。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。

使用 iDRAC Web 界面重设 iDRAC

要重新启动 iDRAC，请在 iDRAC Web 界面中执行以下操作之一：

- 转至 **Overview**（**概述**） → **Server**（**服务器**） → **Summary**（**摘要**）。在 **Quick Launch Tasks**（快速启动任务）中，单击 **Reset iDRAC**（重设 iDRAC）。
- 转至 **Overview**（**概述**） → **Server**（**服务器**） → **Troubleshooting**（**故障排除**） → **Diagnostics**（**诊断**）。单击 **Reset iDRAC**（重设 iDRAC）。

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 **dell.com/support/manuals** 上提供的 *RACADM Reference Guide for iDRAC and CMC*（适用于 iDRAC 和 CMC 的 RACADM 参考指南）。

擦除系统和用户数据

您可以擦除系统组件和这些组件的用户数据。这些系统组件包括：

- Lifecycle Controller 数据
- 嵌入式诊断程序
- 嵌入式操作系统驱动程序包
- BIOS 重设为默认值
- iDRAC 重设为默认值

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。以前的信息将不存在。

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

有关更多信息，请参阅 **dell.com/esmmanuals** 上提供的 *iDRAC RACADM Command Line Reference Guide*（iDRAC RACADM 命令行参考指南）。

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 **Overview（概述）** → **Server（服务器）** → **Troubleshooting（故障排除）** → **Diagnostics（诊断）**。

   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）。

   将以百分比形式显示完成状态。iDRAC 将重新引导并恢复为出厂默认值。iDRAC IP 将重设且无法访问。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。

24

常见问题

本部分列出了下列常见问题：

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：

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。

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 **Common Settings（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**。

Active Directory

Active Directory 登录失败。如何解决此问题？

要诊断此问题的故障，请在 **Active Directory Configuration and Management**（Active Directory 配置和管理）页面上，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：

- 当登录时，请确保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到 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**来自登录的用户域**选项。而应选择**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。

即使已启用证书验证，Active Directory 登录也会失败。测试结果会显示以下错误消息。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.（错误：无法连接到 LDAP 服务器，错误：14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE：证书验证失败：请检查是否已将正确的证书认证机构 (CA) 证书上载到 iDRAC。请同时检查 iDRAC 日期是否在证书的有效期内，并且在 iDRAC 中配置的域控制器地址与目录服务器证书的主题匹配。）

如果已启用证书验证，当 iDRAC 与目录服务器建立 SSL 连接时，iDRAC 将使用已上载的 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 日期超出服务器证书或 CA 证书的有效期。检查 iDRAC 时间和证书的有效期。
- 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（而不是域）的 FQDN。例如 **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。如果解决此问题？

请检查域控制器证书的 Subject（主题）或 Subject Alternative Name（主题备用名称）字段。通常，在域控制器证书的 Subject（主题）或 Subject Alternative Name（主题备用名称）字段中，Active Directory 使用主机名而不是 IP 地址。要解决此问题，请执行以下操作：

- 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。在这种情况下，您仅可以使用 Universal Group（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 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，将保存权限。

如果已配置"全局控制器地址"，iDRAC 会继续查询"全局编录"。如果从全局编录中检索到其他权限，这些权限会累积。

iDRAC 始终在 SSL 上使用 LDAP 吗？

是的。所有数据都通过安全端口 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机制来确保 iDRAC 连接到的域控制器的身份。如果不实行证书验证，黑客可以欺骗域控制器并劫持 SSL 连接。在安全区域内，如果您选择信任所有没有证书验证的域控制器，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。当 DNS 服务器关闭时，预计会出现 DNS 超时。在这种情况下，iDRAC 会使用备用 DNS 服务器进行登录。

Active Directory 针对 Windows Server 2008 Active Directory 中存在的域进行配置。该域包含子域，用户和组位于同一子域中，并且用户是该组的成员。当您尝试使用子域中的用户登录到 iDRAC 时，Active Directory 单一登录会失败。

这可能是由于组类型不正确。Active Directory 服务器中包括两种组类型：

- 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。

请始终确保组类型为“安全”。您不能使用分发组来在任何对象上分配权限，但是可以使用它们来过滤组策略设置。

单一登录

SSO 登录在 Windows Server 2008 R2 x64 上失败。需要执行哪些设置才能解决此问题？

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环境中客户端计算机或服务以及应用程序的兼容性。Kerberos 策略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）**下。
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 **Start**（开始）并运行 **gpedit.msc**。随即会显示 **Local Group Policy Editor**（本地组策略编辑器）窗口。
3. 转至**本地计算机设置** → **Windows 设置** → **安全设置** → **本地策略** → **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**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 **Start**（开始）并运行 cmd。随即会显示命令提示窗口。
5. 运行命令 `gpupdate /force`。组策略即会更新。完成后，请关闭命令提示窗口。
6. 转至 **Start**（开始）并运行 regedit。随即会显示 **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**注册表编辑器**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？

请确保 iDRAC IP 地址列于**工具** → **Internet 选项** → **安全** → **受信任的站点**中。如果未列于其中，SSO 会失败并提示您输入用户名和密码。请单击**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 支持有限数量的智能卡加密服务提供商 (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。

检查智能卡是否由于不正确的 PIN 尝试次数过多而锁定。在这种情况下，联系组织中的智能卡发行商以获取新智能卡。

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？

是。关闭 Virtual Console Viewer （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？

不会。

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 Virtual Console（虚拟控制台）页面上。

使用 RACADM 命令 `racadm getconfig –g cfgRacTuning` 可以在对象 `cfgRacTuneLocalServerVideo` 中显示状态信息。

或者从 Telnet、SSH 或远程会话使用下列 RACADM 命令：

```
racadm -r (iDrac IP) -u (username) -p (password) getconfig -g cfgRacTuning
```

您也可以在虚拟控制台 OSCAR 显示器中查看状态信息。启用本地控制台时，绿色状态将显示在服务器名称旁边。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。请检查您的语言环境，如果需要请重新设置字符集。

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 Virtual Console Viewer 中，请执行下列任一操作：

- 转至**工具** → **会话选项** → **鼠标**选项卡。在 **鼠标加速**下，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？

不能。对于已经在 BIOS 中启用了虚拟控制台的系统，远程安装受支持的 Microsoft 操作系统时，将发送 EMS 连接信息，需要您远程选择 **OK（确定）**。或者必须在本地系统上选择 **OK（确定）**，或者远程重新启动受管的服务器、重新安装，然后在 BIOS 中关闭虚拟控制台。

该消息由 Microsoft 生成，用于警告用户虚拟控制台已启用。要确保不显示该消息，请确保在远程安装操作系统之前，始终在 iDRAC 设置公用程序中关闭虚拟控制台。

为什么 Management Station 上的 Num Lock（数字锁定）指示灯不能反映远程服务器上 Num Lock 的状态？

通过 iDRAC 访问时，管理站上的数字锁定指示灯不一定与远程服务器上的数字锁定状态相同。连接远程会话时，数字锁定状态取决于远程服务器的设置，与管理站上的数字锁定状态无关。

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。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？

不会。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？

为了实现良好的性能，推荐使用 5 MBPS 连接。为了确保最低性能，需要 1 MBPS 连接。

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？

显示该消息是因为 iDRAC 虚拟控制台插件没有接收远程服务器桌面视频。通常情况下，当远程服务器关闭时会发生这种情况。有时，远程服务器桌面视频接收故障也会导致显示该信息。

为什么 Virtual Console Viewer 窗口有时会显示"Out of Range"（超出范围）的信息？

显示该消息是因为捕获视频所需的参数超出 iDRAC 能够捕获视频的范围。某些参数（例如显示分辨率或刷新率）过高会导致超出范围。通常情况下，物理限制（例如视频内存大小或带宽）决定参数的最大范围。

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 **Tools**（工具） → **Internet Options**（Internet 选项） → **Security**（安全） → **Trusted sites**（受信站点）。
2. 单击**站点**并输入 iDRAC 的 IP 地址或 DNS 名称
3. 单击 **Add**（添加）。
4. 单击 **Custom Level**（自定义级别）。
5. 在 **Security Settings**（安全设置）窗口中，在 **Download unsigned ActiveX Controls**（下载未签名的 ActiveX 控件）下选择 **Prompt**（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。在设计方面，PS/2 鼠标使用鼠标指针的相对位置，这导致在同步时发生延迟。iDRAC 具有 USB 鼠标驱动程序，允许绝对位置和更密切的鼠标指针跟踪。即使 iDRAC 将 USB 绝对鼠标位置传送到 Dell BIOS，BIOS 模拟仍然将其转换回相对位置，而行为保持不变。要修复这个问题，请在“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**鼠标模式**设置为 **USC/Diags**，会发生这种情况。按下 **Alt + M** 热键可以在本地系统使用鼠标。再次按下 **Alt + M** 可以在虚拟控制台中使用鼠标。

启动虚拟控制台之后立刻从 CMC Web 界面启动 iDRAC Web 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。

在管理站上同时启动 GUI 和虚拟控制台至相同的 iDRAC 系统时，如果 GUI 在弹出窗口关闭之前启动，会发生 iDRAC GUI 会话超时。如果在包含虚拟控制台的弹出窗口关闭之后，再从 CMC Web 界面启动 iDRAC GUI，不会出现该问题。

为什么 Linux SysRq 键在 Internet Explorer 上无法使用？

从 Internet Explorer 使用虚拟控制台时，Linux SysRq 键的行为将会不同。要发送 SysRq 键，按住 **Ctrl** 和 **Alt** 键并同时按下 **Print Screen** 键，然后松开。要在使用 Internet Explorer 时通过 iDRAC 将 SysRq 键发送到远程 Linux 服务器：

1. 激活远程 Linux 服务器上的魔法键功能。您可以使用下列命令在 Linux 终端上将其激活：
   ```
   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"Link Interrupted"（“连接中断”）的信息？

在服务器重新引导期间使用共享的网络端口时，当 BIOS 重置网卡时，iDRAC 将会断开。断开时间在 10 Gb 卡上会更长，并且如果所连接的网络交换机启用了 Spanning Tree Protocol（生成树协议 ，STP），断开时间会格外长。在这种情况下，建议对连接到服务器的交换机端口启用“portfast”（端口快速）。大多数情况下，虚拟控制台将自动恢复连接。

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 **Client View（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 Setup （BIOS 设置）并转至引导菜单。找到虚拟 CD、虚拟软盘或 vFlash，然后根据需要更改设备的引导顺序。此外，还可以在 CMOS 设置的引导顺序中按“spacebar”（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。如何解决这个问题？

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 Reset（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 **Start**（开始） → **Administrative Tools**（管理工具） → **Services**（服务）。右键单击 **Windows Event Collector** 然后单击 **Stop**（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 Remote File Share（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。

vFlash SD 卡

vFlash SD 卡何时锁定？

当操作正在执行时，系统会锁定 vFlash SD 卡。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）？

作为查找功能的组成部分，IT Assistant 尝试验证设备的 get 和 set 团体名称。在 IT Assistant 中，您的 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 代理程序团体名称为 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为 public 的请求。

要防止发生 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，因此您必须对 IT Assistant 查找设置使用相同的 get 和 set 团体名称。

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。

iDRAC Service Module

在安装或运行 iDRAC Service Module 前，是否应卸载 OpenManage Server Administrator？

不需要。无需卸载 Server Administrator。在安装或运行 iDRAC Service Module 之前，请确保已停止 iDRAC Service Module 所提供的 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，则状态显示为**已安装**。

注: 可使用 `systemctl status dcismeng.service` 命令而非 `init.d` 命令检查是否已在 Red Hat Enterprise Linux 7 操作系统上安装 iDRAC Service Module。

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：

- 单击**开始** → **控制面板** → **程序和功能**。已安装的 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 和更早的版本上，在安装 iDRAC Service Module 时，将显示错误消息此服务器不是支持的服务器。有关支持的服务器的更多信息，请参阅 User Guide（用户指南）。如何解决此问题？

安装 iDRAC Service Module 之前，请确保服务器是第 12 代或更高世代的 PowerEdge 服务器。此外，请确保使用的是 64 位系统。

将在操作系统日志中显示以下消息，即使已正确配置“通过 USBNIC 从操作系统到 iDRAC 的直通”功能也是如此。原因是什么？

```
The iDRAC Service Module is unable to communicate with iDRAC using the OS to
iDRAC Pass-through channel
```

iDRAC Service Module 使用“通过 USB NIC 从操作系统到 iDRAC 的直通”功能来建立与 iDRAC 的通信。有时，虽然已为 USB NIC 接口配置正确的 IP 地址，但仍未建立此通信。如果主机操作系统路由表具有针对同一目标掩码的多个条目，并且 USB NIC 目标未列为路由中的第一个目标，则可能会发生此情况。

目标	Gateway（网关）	子网掩码	标志	度量指标	参考	使用接口
默认	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

在此示例中，**enp0s20u12u3** 是 USB NIC 接口。本地链路目标掩码重复，并且 USB NIC 不是顺序中的第一项。这会导致 iDRAC Service Module 和 iDRAC 之间发生连接问题（通过“操作系统到 iDRAC 直通”功能）。要解决此连接问题，请确保可从主机操作系统访问 iDRAC USB NIC IPv4 地址（默认为 169.254.0.1）。

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 将创建虚拟交换机和端口组，以在 USB NIC 模式下通过“操作系统到 iDRAC 直通”功能与 iDRAC 通信。在卸载后，虚拟交换机 **vSwitchiDRACvusb** 和端口组 **iDRAC Network** 不会删除。要手动删除它们，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”`
  - 要删除虚拟交换机：`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：

Operating System（操作系统）	Location（位置）
Microsoft Windows	**事件查看器** → **Windows** 日志 → **系统**。将在源名称 **iDRAC Service Module** 下复制所有 iDRAC Service Module Lifecycle 日志。

Operating System（操作系统）	Location（位置）
	注: 在 iSM 2.1 和更高的版本中，Lifecycle 日志复制于 Lifecycle Controller Log 源名称下 。在 iSM 2.0 和更早的版本中，这些日志复制于 iDRAC Service Module 源名称下。 注: Lifecycle 日志的位置可以使用 iDRAC Service Module 安装程序进行配置。在安装 iDRAC Service Module 或修改此安装程序时，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 Installation Guide*（iDRAC Service Module 安装指南）中的 *Linux Dependencies*（Linux 相关性）一节。

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 命令和子命令时，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。

确保已安装官方的 openssl 和 libopenssl 版本。运行以下命令安装 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。
- 更改 cfgRacTuneHttpsPort 时（包括通过 `config -f (config file)`进行更改时）。
- 使用 racresetcfg 命令时。
- 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？

这会发生是因为正在创建分区。但是，该分区过一段时间后会删除并显示“已删除分区”的消息。如果没有显示，请等到创建分区的操作完成，然后删除分区。

其他

如何查找刀片式服务器的 iDRAC IP 地址？

可使用以下任何一种方法查找 iDRAC IP 地址：

使用 CMC Web 界面：转至**机箱** → **服务器** → **设置** → **部署**并在显示的表中查看服务器的 IP 地址。

使用虚拟控制台：在开机自检期间重新引导服务器以查看 iDRAC IP 地址。通过本地串行连接选择 OSCAR 中的“Dell CMC”控制台登录 CMC。可从此连接发送 CMC RACADM 命令。请参阅 *iDRAC8 RACADM Command Line Interface Reference GuideiDRAC*（iDRAC8 RACADM 命令行界面参考指南）以了解 CMC RACADM 子命令的完整列表。

在本地 RACADM 中，使用命令：`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 Main Menu（主菜单）上，高亮显示 Server（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？

在 iDRAC Web 界面中：单击**概览** → **iDRAC 设置** → **CMC**。**CMC 摘要**页面随即会显示 CMC IP 地址。

在虚拟控制台中：通过本地串行连接选择 OSCAR 中的“Dell CMC”控制台登录 CMC。可从此连接中发布 CMC RACADM 命令。请参阅 *iDRAC8 RACADM Command Line Interface Reference GuideiDRAC*（iDRAC8 RACADM 命令行界面参考指南）以了解 CMC RACADM 子命令完整列表

```
$ 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。

如何查找机架式服务器和塔式服务器的 iDRAC IP 地址？

在 iDRAC Web 界面中：转至**概览** → **服务器** → **属性** → **摘要**。**系统摘要**页面随即会显示 iDRAC IP 地址。

在本地 RACADM 中，使用命令 `racadm getsysinfo`。

在 LCD 中：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**。

在 OpenManage Server Administrator 中：在“服务器管理员 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。
- 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。

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 功率预算，机箱功率预算可能已超出。

如何检索 iDRAC 管理用户名和密码？

您必须将 iDRAC 恢复到默认设置。有关更多信息，请参阅将 iDRAC 重设为出厂默认设置。

如何更改机箱中系统的插槽名称？

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 **Apply**（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 Web 界面以查看 iDRAC 是否显示为可升级组件。如果是，则按照使用 CMC Web 界面升级固件中的说明进行升级。

如果问题仍然存在，请与技术支持部门联系。

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。

25 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。

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。需要查明原因以进行故障排除，从而使使用 iDRAC 的服务器恢复。

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: 如果您不能访问 iDRAC Web 界面，请转至服务器，访问 LCD 面板，并记下 IP 地址或主机名，然后使用管理站中的 iDRAC Web 界面执行以下操作：

- 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。
- 可在虚拟控制台中查看操作系统映像。如果可以看到映像，则重置系统（热启动）并再次登录。如果能够登录，则已解决此问题。
- 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

相关任务

预览虚拟控制台
查看引导和崩溃捕获视频
查看系统运行状况
查看日志
生成技术支持报告
资源清册和监测存储设备
使用 iDRAC 服务模块

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**概览** → **服务器** → **系统摘要**以查看系统信息，访问该页面上的各链接以查看系统运行状况。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。

相关任务

[查看系统运行状况]
[使用 iDRAC 服务模块]
[生成技术支持报告]

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 Lifecycle 日志和系统事件日志

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**概览** → **服务器** → **日志**以查看 SEL，以及**概览** → **服务器** → **日志** → **Lifecycle 日志**以查看 Lifecycle 日志。

   注: SEL 也会在 Lifecycle 日志中记录。使用筛选选项可查看 SEL。
2. 将 SEL 或 Lifecycle 日志以 XML 格式导出到外部位置（Management Station、USB、网络共享等等）。或者，您可以启用远程系统日志记录，以便写入到 Lifecycle 日志的所有日志也同时写入已配置的远程服务器。
3. 如果您正在使用 iDRAC Service Module，则将 Lifecycle 日志导出到操作系统日志。有关更多信息，请参阅[使用 iDRAC Service Module]。

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
- RACADM CLI（iDRAC 和 CMC）
- Dell Update Package（Dell 更新软件包，DUP)
- CMC Web 界面
- Lifecycle Controller–Remote Services（远程服务）
- Lifecycle Controller

- Dell Remote Access Configuration Tool（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：

- **Overview**（概览） → **Server**（服务器） → **Power/Thermal**（电源/耐热） → **Power Configuration**（电源配置） → **Power Control**（电源控制）。将显示 **Power Control**（电源控制）页面。选择 **Graceful Shutdown**（正常关机）然后单击 **Apply**（应用）。
- **概览** → **服务器** → **电源/散热** → **电源监测**。在**电源控制**下拉菜单中，选择**正常关机**，然后单击**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

启动服务器的远程控制台和挂载 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. 使用下列方法之一通过 iDRAC Web 界面启动虚拟控制台：
   - 转至 **Overview**（概览） → **Server**（服务器） → **Virtual Console**（虚拟控制台），然后单击 **Launch Virtual Console**（启动虚拟控制台）。
   - 转至 **Overview**（概览） → **Server**（服务器） → **Properties**（属性），然后在 **Virtual Console Preview**（虚拟控制台预览）下单击 **Launch**（启动）。

   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

要执行此操作，请参阅使用远程文件共享部署操作系统。

管理机架密度

假定一个机架上安装了两台服务器。要增加两个额外的服务器，需要确定机架中余下的空间量。

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 导出 XML 配置文件。
4. 在 XML 文件中编辑 I/O 标识优化功能设置。
5. 将 XML 配置文件导入 iDRAC。

相关概念

更新设备固件
启用或禁用 I/O 标识优化功能