# 集成式 Dell Remote Access Controller 7 (iDRAC7) 1.30.30 版用户指南

# 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。**



2012 - 12

Rev. A00

# 目录

1

# 概述

集成式 Dell Remote Access Controller 7 (iDRAC7) 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。iDRAC7 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 iDRAC7 是大型数据中心解决方案的组成部分，可帮助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、修正和修复 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 iDRAC7 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

iDRAC7 有以下型号：

- 带 IPMI 的 Basic Management（默认在 200-500 系列服务器上提供）
- iDRAC7 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）
- iDRAC7 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 *iDRAC7 Overview and Feature Guide*（iDRAC7 概述和功能指南）。

## 结合使用 iDRAC7 与 Lifecycle Controller 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/support/manuals** 上提供的 *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller Remote Services 用户指南）。

# 主要功能

iDRAC7 中的主要功能包括：

**注:** 某些功能仅限 iDRAC7 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 gets。
- 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 iDRAC7 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）。

**部署**

- 管理 vFlash SD 卡分区。
- 配置前面板显示设置。
- 启动 Lifecycle Controller，通过该控制器可以配置和更新 BIOS 以及支持的网络和存储适配器。
- 管理 iDRAC7 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）。

**更新**

- 管理 iDRAC7 许可证。
- 为 Lifecycle Controller 支持的设备更新 BIOS 和设备固件
- 更新或回滚 iDRAC7 固件。
- 管理分阶段更新。
- 备份和还原服务器配置文件

**维护和故障排除**

- 执行与电源相关的操作和监测电能消耗。
- 生成警报不依赖于服务器管理员。
- 记录事件数据：Lifecycle 和 RAC 日志。
- 设置电子邮件警报、IPMI 警报、远程系统日志、WS 事件日志、事件的 SNMP 陷阱（v1 和 v2c）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。

**保护连接性**

保护对关键网络资源的访问权限非常重要。iDRAC7 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。
- 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 iDRAC7 的客户端的有限 IP 地址范围。
- 具有 Enterprise 许可证的机架式和塔式服务器上的专用千兆位以太网适配器。

# 此发行版中的新功能

以下是此发行版中的新功能：

- 为 Lifecycle Controller 支持的所有设备更新设备固件
- 查看和管理分阶段固件更新。
- 备份和还原服务器配置文件。
- 导出硬件资源清册。
- 查看附加组件的硬件和固件资源清册信息。
- 虚拟控制台：
  - 自动锁定操作系统。
  - 缩放虚拟控制台查看器。
  - 修改的键盘宏。
  - 使用虚拟控制台查看器设置第一引导设备。
- 允许 iDRAC 基于链接状态自动选择网络接口卡 (NIC)（专用 NIC 或共享 LOM）的设置。
- 查看当前活动的 NIC。
- 在前面板 LCD 上启用虚拟控制台指示。
- 将 Lifecycle Controller 或 BIOS Boot Manager 设置为第一引导设备。
- 设置时区和网络时间协议 (NTP)。
- 启用 OS 至 iDRAC 直通。
- 改进的安全性功能，例如：

  - 在使用默认凭据登录 iDRAC 时警告用户。
  - 生成和使用自定义签名 SSL 签名证书。
- 查看 CPU 详细信息，例如处理器自动调节和预测性故障信息。
- 查看双列内存模块 (DIMM) 的运行状况和状态信息。
- 监测运行状况并查看光纤信道主机总线适配器 (FC HBA) 设备的资源清册。
- 为在 iDRAC 中本地存储的用户帐户启用 SNMPv3 验证。
- 支持使用 v1 和 v2 格式的 SNMP 陷阱。支持使用 v1、v2 或 v3 格式或仅限 v3 格式的 SNMP Gets。
- 将警报远程发送到外部服务器。
- 发送 WS 事件通知。此功能当前限于作业控制警报类型。
- 使用诊断控制台将 iDRAC7 重设为出厂默认值。
- 对于 RACADM 命令，键入开始字母并按 <TAB> 键补齐命令，使用 **cd** 可在各个级别之间遍历。
- 通过 RACADM 和 WS-MAN 使用导出或导入 XML 配置文件执行服务器配置。
- 支持 Safari、Chrome 和 Mac OS X。

**相关链接**

更新设备固件
查看和管理分阶段更新
备份和还原服务器配置文件
查看系统资源清册
使用虚拟控制台查看器
配置 LCD 设置
设置第一引导设备
配置时区和 NTP
启用或禁用 OS 到 iDRAC 直通
更改默认登录密码
SSL 服务器证书
查看传感器信息
资源清册和监测 FC HBA 设备
配置本地用户
使用 iDRAC7 Web 界面将 iDRAC7 重设为出厂默认设置

# 支持的 Web 浏览器

下面的浏览器支持 iDRAC7：

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

对于版本的列表，请参阅 **dell.com/support/manuals** 上提供的 *Readme*（自述文件）。

# 管理许可证

iDRAC7 的功能根据购买的许可证（Basic Management、iDRAC7 Express 或 iDRAC7 Enterprise）提供。界面上只会提供获得许可证的功能，您可以使用这些功能来配置或使用 iDRAC7。例如，iDRAC7 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。

iDRAC7 许可证管理和固件更新功能可通过 iDRAC7 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

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 iDRAC7 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的许可证。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 iDRAC7、RACADM、WS-MAN 和 Lifecycle Controller 远程服务，对于一对多许可证管理，您可以使用 Dell License Manager，来执行下列许可证操作：

- 查看 - 查看当前许可证信息。
- 导入 - 获取许可证后，将许可证存储到本地存储位置，并使用支持的界面之一将其导入 iDRAC7。如果许可证通过验证检查，则会导入。

  **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，则删除分配给组件的许可证。将许可证删除后，它不会存储在 iDRAC7 中，并且基本产品功能会启用。
- 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 iDRAC7 Enterprise 许可证（没有网络连接）并激活专用 NIC，可以使用本地 iDRAC7 Enterprise 许可证安装工具。此公用程序安装 30 天试用版 iDRAC7 Enterprise 许可证，允许您将 iDRAC 重设为从共享 NIC 到专用 NIC 进行使用。

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 |
| 当前许可证 | 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 |

### 使用 iDRAC7 Web 界面管理许可证

要使用 iDRAC7 Web 界面管理许可证，请转至 **Overview（概述）** → **Server（服务器）** → **Licenses（许可证）**。**Licensing**（许可证）页面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 *iDRAC7 Online Help*（iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# iDRAC7 中的可授权功能

下表提供了基于购买的许可证启用的 iDRAC7 功能。

**表. 2: iDRAC7 可获得许可的功能**

| 功能 | Basic Management with IPMI | iDRAC7 Express（机架式和塔式服务器） | iDRAC7 Express（适用于刀片服务器） | iDRAC7 Enterprise |
|---|---|---|---|---|
| **接口和标准支持** | | | | |
| IPMI 2.0 | 是 | 是 | 是 | 是 |
| 基于 Web 的界面 [1] | 否 | 是 | 是 | 是 |
| SNMP | 否 | 是 | 是 | 是 |
| WS-MAN | 是 | 是 | 是 | 是 |
| SMASH-CLP (SSH) | 否 | 是 | 是 | 是 |
| RACADM（SSH、本地和远程）[1] | 否 | 是 | 是 | 是 |
| Telnet | 否 | 是 | 是 | 是 |

| 功能 | Basic Management with IPMI | iDRAC7 Express（机架式和塔式服务器） | iDRAC7 Express（适用于刀片服务器） | iDRAC7 Enterprise |
|---|---|---|---|---|
| **连接性** | | | | |
| 共享或故障转移网络模式（仅限机架和塔式服务器） | 是 | 是 | 否 | 是 |
| 专用 NIC | 否 | 否 | 是 [ 2] | 是 [2,6] |
| DNS | 是 | 是 | 是 | 是 |
| VLAN 标记 | 是 | 是 | 是 | 是 |
| IPv4 | 是 | 是 | 是 | 是 |
| IPv6 | 否 | 是 | 是 | 是 |
| 动态 DNS | 否 | 是 | 是 | 是 |
| **安全和验证** | | | | |
| 基于角色的权限 | 是 | 是 | 是 | 是 |
| 本地用户 | 是 | 是 | 是 | 是 |
| 目录服务（Active Directory 和通用 LDAP） | 否 | 否 | 否 | 是 |
| SSL 加密 | 是 | 是 | 是 | 是 |
| 双重验证 [3] | 否 | 否 | 否 | 是 |
| 单一登录 (SSO) | 否 | 否 | 否 | 是 |
| PK 验证（适用于 SSH） | 否 | 否 | 否 | 是 |
| 安全锁定 | 否 | 是 | 是 | 是 |
| **远程管理和补救** | | | | |
| 嵌入式诊断 | 是 | 是 | 是 | 是 |
| LAN 上串行（有代理） | 是 | 是 | 是 | 是 |
| LAN 上串行（无代理） | 否 | 是 | 是 | 是 |
| 崩溃屏幕捕获 | 否 | 是 | 是 | 是 |
| 崩溃视频捕获 | 否 | 否 | 否 | 是 |
| 引导捕获 | 否 | 否 | 否 | 是 |
| 虚拟介质 [4] | 否 | 否 | 是 | 是 |
| 虚拟控制台 [4] | 否 | 否 | 是 [5] | 是 |
| 控制台协作 [4] | 否 | 否 | 否 | 是 |
| 虚拟文件夹 | 否 | 否 | 否 | 是 |
| 虚拟控制台聊天 | 否 | 否 | 否 | 是 |
| 远程文件共享 | 否 | 否 | 否 | 是 |
| vFlash [6] | 否 | 否 | 否 | 是 |
| vFlash 分区 [6] | 否 | 否 | 否 | 是 |
| 自动查找 | 否 | 是 | 是 | 是 |
| 备份服务器配置文件 | 否 | 否 | 否 | 是 |
| 零件更换 [8] | 否 | 是 | 是 | 是 |

| 功能 | Basic Management with IPMI | iDRAC7 Express（机架式和塔式服务器） | iDRAC7 Express（适用于刀片服务器） | iDRAC7 Enterprise |
|---|---|---|---|---|
| 网络时间协议 (NTP) | 否 | 是 | 是 | 是 |
| **监测和功率** | | | | |
| 传感器监测和警报 | 是 | 是 | 是 | 是 |
| 设备监测 | 否 | 是 | 是 | 是 |
| 存储监测 | 否 | 是 | 是 | 是 |
| 单个 CPU 和内存传感器 | 是 | 是 | 是 | 是 |
| 电子邮件警报 | 否 | 是 | 是 | 是 |
| 历史功率计数器 | 是 | 是 | 是 | 是 |
| 功率限额 | 否 | 否 | 否 | 是 |
| 实时功率监测 | 是 | 是 | 是 | 是 |
| 实时功率图表 | 否 | 是 | 是 | 是 |
| **日志记录** | | | | |
| 系统事件日志 | 是 | 是 | 是 | 是 |
| RAC 日志 [7] | 否 | 是 | 是 | 是 |
| 跟踪日志 [7] | 否 | 是 | 是 | 是 |
| 远程系统日志 | 否 | 否 | 否 | 是 |

[1]通过 iDRAC7 Web 界面和 RACADM 始终可使用 iDRAC7 许可证管理和固件更新功能。

[2] 所有刀片服务器都一直使用 iDRAC7 专用的 NIC，但速度限制为 100 Mbps。由于机箱的限制，GIGABYTE 以太网卡无法在刀片服务器上使用，但可在具有 Enterprise 许可证的机架和塔式服务器上使用。刀片服务器未启用共享 LOM。

[3] 双重验证可通过 Active-X 使用，因此仅支持 Internet Explorer。

[4] 虚拟控制台和虚拟介质可通过 Java 和 Active-X 插件使用。

[5] 带远程启动功能的单一用户虚拟控制台。

[6] 在一些系统中，需要可选的 iDRAC7 端口卡。

[7] 可通过 WS-MAN 以基本版本使用 RAC 和跟踪日志。

[8] 部件更换是一个 Lifecycle Controller 功能，该功能通过为更换部件还原固件级别和配置来简化更换失败部件的过程。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Dell Lifecycle Controller User's Guide*（Dell Lifecycle Controller 用户指南）。

# 访问 iDRAC7 的界面和协议

下表列出了访问 iDRAC7 的界面。

**注:** 同时使用一个以上的界面可能会产生意外的结果。

**表. 3: 访问 iDRAC7 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 iDRAC7 Web 界面与其他功能一起使用。 |

| 界面或协议 | 说明 |
| --- | --- |
| | 要访问 iDRAC 设置公用程序，请在引导过程中按 <F2>，然后在 **System Setup Main Menu**（系统设置主菜单）页面上单击 **iDRAC Settings**（iDRAC 设置）。 |
| iDRAC7 Web 界面 | 使用 iDRAC7 Web 界面可管理 iDRAC7 和监控受管系统。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。管理员可通过 SSL CSR 生成流程上载其 SSL 证书以保护 Web 服务器。默认 HTTP 和 HTTPS 端口可更改。用户访问权限基于用户权限。 |
| RACADM | 使用此命令行公用程序可执行 iDRAC7 和服务器管理。您可以在本地和远程使用 RACADM。<br>• 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 iDRAC7 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根用户才能使用此公用程序。<br>• 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。<br>• 固件 RACADM 可通过使用 SSH 或 telnet 登录到 iDRAC7 进行访问。您可以在不指定 iDRAC7 IP、用户名和密码的情况下运行固件 RACADM 命令。<br>• 您无须指定 iDRAC7 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）。 |
| 服务器 LCD 面板/机箱 LCD 面板 | 使用服务器前面板上的 LCD 可以：<br>• 查看警报、iDRAC7 IP 或 MAC 地址、用户可编程字符串。<br>• 设置 DHCP<br>• 配置 iDRAC7 静态 IP 设置。<br>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。<br>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 | 除监控和管理机箱外，使用 CMC Web 界面还可以：<br>• 查看受管系统的状态<br>• 更新 iDRAC7 固件<br>• 配置 iDRAC7 网络设置<br>• 登录到 iDRAC7 Web 界面。<br>• 启动、停止或重设受管系统<br>• 更新 BIOS、PERC 和支持的网络适配器 |
| Lifecycle Controller | 使用 Lifecycle Controller 可执行 iDRAC7 配置。要访问 Lifecycle Controller，请在引导过程中按 <F10> 并转到 **System Setup（系统设置）** → **Advanced Hardware Configuration（高级硬件配置）** → **iDRAC Settings（iDRAC 设置）**。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。 |
| Telnet | 使用 Telnet 可访问 iDRAC7，您可以在 iDRAC7 上运行 RACADM 和 SMCLP 命令。有关 RACADM 的详细信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。有关 SMCLP 的详细信息，请参阅使用 SMCLP。<br>**注:** Telnet 不是加密协议，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 接口。 |

| 界面或协议 | 说明 |
|---|---|
| SSH | 使用 SSH 可运行 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 iDRAC7 上，SSH 服务在默认情况下已启用。iDRAC7 中的 SSH 服务可以禁用。iDRAC7 仅支持具有 DSA 和 RSA 主机密钥算法的 SSH 版本 2。当您首次启动 iDRAC7 时，系统会生成独特的 1024 位 DSA 和 1024 位 RSA 主机密钥。 |
| IPMITool | 通过 iDRAC7 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/support/manuals** 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）。 |
| 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。 |
| WS-MAN | LC 远程服务基于一对多系统管理任务的 WS-Management 协议。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。<br>管理 Web 服务 (WS-Management) 是基于简单对象访问协议 (SOAP) 的系统管理协议。iDRAC7 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 信息定义在受管系统中可修改的语义和信息类型。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 iDRAC7 设备接口提供。<br>有关更多信息，请参阅以下内容：<br>• **dell.com/support/manuals** 上提供的 Lifecycle Controller-Remote Services User's Guide（Lifecycle Controller Remote Services 用户指南）。<br>• **dell.com/support/manuals** 上提供的 Lifecycle Controller Integration Best Practices Guide（Lifecycle Controller 集成最佳实践指南）。<br>• Dell TechCenter 上的 Lifecycle Controller 页面 — **delltechcenter.com/page/Lifecycle+Controller**<br>• Lifecycle Controller WS-Management 脚本中心 — **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller**<br>• MOF 和配置文件 - **delltechcenter.com/page/DCIM.Library**<br>• DTMF 网站 - dmtf.org/standards/profiles/ |

# iDRAC7 端口信息

穿过防火墙远程访问 iDRAC7 需要以下端口。下面是 iDRAC7 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. 4: iDRAC7 用于监听连接的端口**

| 端口号 | 功能 |
|---|---|
| 22* | SSH |
| 23* | Telnet |
| 80* | HTTP |
| 443* | HTTPS |
| 623 | RMCP/RMCP+ |
| 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 |

* 可配置端口

下表列出了 iDRAC7 用作客户端的端口。

**表. 5: iDRAC7 用作客户端的端口**

| 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 |

# 您可能需要的其他说明文件

除本指南外，Dell 支持网站 **dell.com/support/manuals** 上的以下说明文件提供关于在您的系统中设置和操作 iDRAC7 的附加信息。在 **Manuals**（手册）页面上，单击 **Software（软件）→ Systems Management（系统管理）**。在右侧单击相应的产品链接以访问说明文件。

- *iDRAC7 Online Help*（iDRAC7 联机帮助）提供关于 iDRAC7 Web 界面上可用字段的详细信息及其描述。安装 iDRAC7 后，您可以访问联机帮助。
- *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）提供关于 RACADM 子命令、支持的界面以及 iDRAC7 属性数据库组和对象定义的信息。
- *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 User's Guide*（Dell Lifecycle Controller 用户指南）提供有关使用 Lifecycle Controller 图形用户界面 (GUI) 的信息。
- *Dell Lifecycle Controller Remote Services Quick Start Guide*（Lifecycle Controller Remote Services 快速入门指南）提供远程服务功能的概述、有关远程服务、Lifecycle Controller API 的入门信息，以及提供对 Dell 技术中心中各种资源的参考。
- *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。
- *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。
- 系统可能附带自述文件，提供对系统或说明文件所做的最新更新，或者为有经验的用户或技术人员提供高级技术参考资料。
- *Glossary*（词汇表）将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：

- *iDRAC7 Overview and Feature Guide*（iDRAC7 概述和功能指南）提供关于 iDRAC、它可获得许可的功能以及许可证升级选项信息。
- 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。

# 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. 请访问 **www.dell.com/support**。
2. 选择您的支持类别。
3. 在页面顶部的“Choose a Country/Region”（选择国家/地区）下拉式菜单中，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。

2

# 登录 iDRAC7

您可以使用 iDRAC7 用户、Microsoft Active Directory 用户或轻型目录服务协议 (LDAP) 用户的身份登录 iDRAC7。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 iDRAC7。

**相关链接**

以本地用户、Active Directory 用户或 LDAP 用户身份登录 iDRAC7
使用智能卡登录 iDRAC7
使用单一登录来登录 iDRAC7
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 iDRAC7

在使用 Web 界面登录 iDRAC7 之前，请确保已配置支持的 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 Active Directory 外，基于 openLDAP、openDS、Novell eDir 和 Fedora 的目录服务均受支持。用户名中不允许使用“<”和“>”字符。

要以本地用户、Active Directory 用户或 LDAP 用户身份登录 iDRAC7，请执行以下操作：

1. 打开支持的 Web 浏览器。
2. 在 **Address**（地址）字段中，输入 `https://[iDRAC7-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://[iDRAC7-IP-address]:[port-number]`，其中，`[iDRAC7-IP-address]` 是 iDRAC7 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 **Username**（用户名）和 **Password**（密码）字段中，输入您的 iDRAC7 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 **Submit**（提交）。您就可使用所需的用户权限登录 iDRAC7。

   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。

**相关链接**

[配置用户帐户和权限]
[更改默认登录密码]
[配置支持的 Web 浏览器]

# 使用智能卡登录 iDRAC7

您可以使用智能卡登录 iDRAC7。智能卡提供双重验证 (TFA)，该功能可实现双层安全性：

- 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。

**相关链接**

[使用智能卡作为本地用户登录 iDRAC7]
[使用智能卡作为 Active Directory 用户登录 iDRAC7]

## 使用智能卡作为本地用户登录 iDRAC7

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信任的认证机构 (CA) 证书上载到 iDRAC7
- 启用智能卡登录。

iDRAC7 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。

使用智能卡作为本地用户登录 iDRAC7：

1. 使用链接 `https://[IP 地址]` 访问 iDRAC7 Web 界面。
   将显示 **iDRAC7 Login（登录）**页面，提示插入智能卡。

   **注:** 如果默认 HTTPS 端口号（端口 443）已更改，键入：`https://[IP 地址]:[端口号]` 其中，`[IP 地址]` 是 iDRAC7 的 IP 地址而 `[端口号]` 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 iDRAC7。

   **注:** 如果您是已启用 **Enable CRL check for Smart Card Logon（启用智能卡登录的 CRL 检查）**功能的本地用户，则 iDRAC7 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。

**相关链接**

[启用或禁用智能卡登录]
[为本地用户配置 iDRAC7 智能卡登录]

## 使用智能卡作为 Active Directory 用户登录 iDRAC7

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 iDRAC7。

- 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 iDRAC7：

1. 使用链接 `https://[IP address]` 登录 iDRAC7。
   **iDRAC7 Login（登录）**页会显示出来，提示插入智能卡。

   **注:** 如果默认的 HTTPS 端口号（端口 443）变更，键入：`https://[IP address]:[port number]`，其中 `[IP address]` 是 iDRAC7 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 **Submit（提交）**。
   您便使用您的 Active Directory 凭据登录到了 iDRAC7。

   **注:**

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

**相关链接**

启用或禁用智能卡登录
为 Active Directory 用户配置 iDRAC7 智能卡登录

# 使用单一登录来登录 iDRAC7

启用单一登录 (SSO) 后，您可以直接登录 iDRAC7 而无需输入您的域用户验证凭据（例如用户名和密码）。

**相关链接**

为 Active Directory 用户配置 iDRAC7 SSO 登录

## 使用 iDRAC7 Web 界面登录 iDRAC7 SSO

使用单一登录功能登录 iDRAC7 之前，请确保：

- 您已使用有效的 Active Directory 用户帐户登录系统。
- 单点登录选项在 Active Directory 配置过程中已启用。

使用 Web 界面登录 iDRAC7：

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 iDRAC7 FQDN (iDRAC7dnsname.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。

   iDRAC7 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 iDRAC7 SSO

通过 SSO 功能，您可以从 CMC Web 界面启动 iDRAC7 Web 界面。CMC 用户从 CMC 启动 iDRAC7 时具有 CMC 用户权限。如果 CMC 中存在该用户帐户而 iDRAC 中不存在，则用户仍可从 CMC 启动 iDRAC7。

如果禁用 iDRAC7 网络 LAN（LAN Enabled = No（LAN 已启用 = 否）），则 SSO 不可用。

如果服务器已从机箱中卸下，iDRAC7 IP 地址发生变化，或 iDRAC7 网络连接中存在问题，则启动 iDRAC7 的选项在 CMC Web 界面中会变灰。

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 iDRAC7

您可以通过 RACADM 公用程序使用远程 RACADM 访问 iDRAC7。

有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 参考指南）。

如果管理站没有将 iDRAC7 的 SSL 证书存储到其默认证书存储中，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:** iDRAC7 证书是 iDRAC7 发送给 RACADM 客户端以建立安全会话的证书。此证书通过 CA 发出或自签名。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。

**相关链接**

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 Management Station 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` 命令：`- cat testcacert.pem >> cert.pem`
4. 生成服务器证书并将其上传到 iDRAC7。

# 使用本地 RACADM 访问 iDRAC7

有关使用本地 RACADM 访问 iDRAC7 的信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 使用固件 RACADM 访问 iDRAC7

您可以使用 SSH 或 Telnet 界面访问 iDRAC7 并运行固件 RACADM 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 使用 SMCLP 访问 iDRAC7

当您使用 Telnet 或 SSH 登录 iDRAC7 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 iDRAC7

您可以通过 SSH 登录 iDRAC7（不输入密码）。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@<域>
```

或

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

其中，`IP_address` 是 iDRAC7 的 IP 地址。

**发送 RACADM 命令：**

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

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

**相关链接**

对 SSH 使用公共密钥验证

# 多个 iDRAC7 会话

下表提供了可能使用各种界面的多个 iDRAC7 会话的列表。

**表. 6: 多个 iDRAC7 会话**

| 界面 | 会话数 |
|---|---|
| iDRAC7 Web 界面 | 4 |
| 远程 RACADM | 4 |
| 固件 RACADM / SMCLP | SSH - 2<br>Telnet - 2<br>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 Configure Users（配置用户）权限登录到 iDRAC7。
- 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。

如果使用 Active Directory 或 LDAP 登录，则显示同一条警告消息。在确定是否有任何（本地）帐户将 root/calvin 作为凭据时，不考虑 Active Directory 和 LDAP 帐户。在使用 SSH、Telnet、远程 RACADM 或 Web 界面登录 iDRAC 时，还会显示警告消息。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。

要更改凭据，必须拥有 Configure Users（配置用户）权限。

**相关链接**

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 iDRAC7 Web 界面时，如果显示 **Default Password Warning**（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：+、&、?、>、-、}、|、.、!、(、'、,、_、[、"、@、#、)、*、;、$、]、/、§、%、=、<、:、{、l、\
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 *iDRAC7 Online Help*（iDRAC7 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 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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**（上一步）、**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 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户验证）** → **Local Users（本地用户）**。

   将显示 **Users**（用户）页面。
2. 在 **Default Password Warning**（默认密码警告）部分，选择 **Enable**（启用），然后单击 **Apply**（应用）启用在登录 iDRAC7 时显示 **Default Password Warning**（默认密码警告）页面。否则，请选择 **Disable**（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 启用显示警告消息以更改默认登录密码，请使用 `idrac.tuning.DefaultCredentialWarning` 对象。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

3

# 设置受管系统和 Management Station

要使用 iDRAC7 执行带外系统管理，您必须配置 iDRAC7 的远程访问功能，设置 Management Station 和受管系统，并且配置支持的 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。

**相关链接**


设置 iDRAC7 IP 地址
设置受管系统
更新设备固件
回滚 iDRAC7 固件
设置管理站
配置支持的 Web 浏览器


## 设置 iDRAC7 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 iDRAC7 之间的通信。您可以使用以下界面中的一个来设置 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 iDRAC7。
- 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 iDRAC7 IP 地址 192.168.0.120 来配置初始网络设置，包括为 iDRAC7 设置 DHCP 或静态 IP。

对于刀片服务器，默认情况下会禁用 iDRAC7 网络界面。

当您配置了 iDRAC7 IP 地址之后：

- 确保*在设置 iDRAC7 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：
  - 使用支持浏览器（Internet Explorer、Firefox、Chrome 或 Safari）的 iDRAC7 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）

**相关链接**

使用 iDRAC 设置公用程序设置 iDRAC IP
使用 CMC Web 界面设置 iDRAC7 IP
启用自动查找

## 使用 iDRAC 设置公用程序设置 iDRAC IP

要设置 iDRAC7 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：
   - Network Settings（网络设置）
   - 常见设置
   - IPv4 设置
   - IPv6 设置
   - IPMI 设置
   - VLAN 设置
6. 回到 **System Setup Main Menu（系统设置主菜单）**页面并单击 **Finish（完成）**。
   网络信息即会保存并且系统会重新引导。

**相关链接**

Network Settings（网络设置）
常见设置
IPv4 设置
IPv6 设置
IPMI 设置
VLAN 设置

### Network Settings（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：
   - Dedicated（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，Dedicated（专用）选项允许从与分配给主机 LOM 或 NIC 端口的 IP 地址所在的相同或不同的子网中，为 iDRAC 分配 IP 地址。

   **注:** 该选项只能用在具有 iDRAC7 Enterprise 许可证的机架式或塔式系统上。对于刀片式系统，它在默认情况下即可用。

- LOM1
- LOM2
- LOM3
- LOM4

**注:** 对于机架式和塔式服务器，根据服务器型号，可使用全部四种 LOM 选项或使用其中的中的两种（LOM1 和 LOM2）。刀片服务器不使用 LOM 进行 iDRAC7 通信。

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。

   **注:** 如果您在 **NIC Selection（NIC 选择）**下拉菜单中选择了 **Dedicated（专用）**，则该选项将变灰。

   例如，要在 LOM1 故障时通过 LOM2 路由 iDRAC7 网络流量，则对 **NIC Selection（NIC 选择）**选择 **LOM1**，对 **Failover Network（故障转移网络）**选择 **LOM2**。
4. 如果 iDRAC7 必须自动设置双工模式和网络速度，则在 **Auto Negotiation（自动协商）**下，选择 **On（打开）**。该选项仅用于专用模式。如果启用，iDRAC7 会根据网络速度将网络速度设置为 10、100 或 1000 Mbps。
5. 在 **Network Speed（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 iDRAC7。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。

注册 iDRAC7：

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 **Auto Config Domain Name（自动配置域名）**自动从 DHCP 获取域名。否则，提供 **DNS Domain Name（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 **Enable DHCP**（启用 DHCP）下选择 **Enabled**（启用）选项，以便 DHCP 能够将 IP 地址、网关和子网掩码自动分配给 iDRAC7。否则，选择 **Disabled**（禁用）并输入以下各项的值：
   - 静态 IP 地址
   - 静态网关
   - 静态子网掩码
3. 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 iDRAC7，请在 **Enable Auto-configuration**（启用自动配置）下选择 **Enabled**（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

可将 iDRAC7 配置到 VLAN 基础架构中。要配置 VLAN 设置：

1. 在 **Enable VLAN ID（启用 VLAN ID）**下，选择 **Enabled（已启用）**。
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。

## 使用 CMC Web 界面设置 iDRAC7 IP

要使用 CMC Web 界面设置 iDRAC7 IP 地址：

**注:** 必须具有机箱配置管理员权限才能从 CMC 设置 iDRAC7 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 *iDRAC7 Online Help*（iDRAC7 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）。

## 启用自动查找

自动查找功能允许新安装的服务器自动查找托管配置服务器的远程管理控制台。*配置服务器*向 iDRAC7 提供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。有关自动查找的更多信息，请参阅 **ell.com/support/manuals** 上提供的 *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller Remote Services 用户指南）。

自动查找可结合静态 IP 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 DNS 已指定，则从 DNS 检索配置服务器 IP 并且无需 DHCP 设置。如果配置服务器已指定，则将跳过查找，因此 DHCP 和 DNS 都不需要。

您可以使用 iDRAC7 设置公用程序或使用 Lifecycle Controller 启用自动查找。有关使用 Lifecycle Controller 的信息，请参阅 **dell.com/support/manuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。

如果在出厂运送的系统上未启用自动查找功能，则会启用默认管理员帐户（用户名为 root，密码为 calvin）。在启用自动查找之前，请确保禁用此管理员帐户。如果已启用 Lifecycle Controller 中的自动查找，则在*查找*配置服务器之前，所有 iDRAC 用户帐户都被禁用。

使用 iDRAC 设置公用程序启用自动查找：

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。

# 设置管理站

管理站是用于访问 iDRAC7 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，请参阅自述文件。
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 iDRAC7，则需要）。
4. 从 *Dell Systems Management Tools and Documentation* DVD 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。
5. 根据要求安装下列组件：
   - Telnet
   - SSH 客户端
   - TFTP
   - Dell OpenManage Essentials

**相关链接**

安装和使用 VMCLI 公用程序
配置支持的 Web 浏览器

## 远程访问 iDRAC7

要从管理站远程访问 iDRAC7 Web 界面，请确保管理站与 iDRAC7 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 iDRAC7 NIC 设置为 LOM1 并确保管理站与 iDRAC7 位于同一网络中。

  **注:** 如果将系统升级到 iDRAC7 Enterprise，则可将 iDRAC7 NIC 设置为 **Dedicated**（专用）。

要从管理站访问受管系统的控制台，请通过 iDRAC7 Web 界面使用虚拟控制台。

**相关链接**

启动虚拟控制台
Network Settings（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
- Server Administrator

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）。

**相关链接**

修改本地管理员帐户设置

## 修改本地管理员帐户设置

设置 iDRAC7 IP 地址后，您可以修改使用 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，转到 **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 **Username（用户名）**、**LAN User Privileges（LAN 用户权限）**、**Serial Port User Privileges（串行端口用户权限）**和 **Password（密码）**。
   有关各选项的信息，请参阅 *iDRAC 设置公用程序联机帮助*。
3. 依次单击 **Back（返回）**、**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 iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Properties（属性）** → **Details（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 *《iDRAC7 联机帮助》*。
3. 单击 **Apply（应用）**。系统位置详细信息即保存到 iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 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（返回）**、**Finish（完成）**和 **Yes（是）**。
   该详细信息即会保存。

## 优化系统性能和功率消耗

您可以使用 iDRAC 设置公用程序优化受管系统的性能，设置最高排气温度和风扇速度。要执行此操作：

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. 指定温度、用户选项和风扇设置。
   有关详细信息，请参阅*《iDRAC 设置联机帮助》*。
3. 单击 **Back（上一步）**，单击 **Finish（完成）**，然后单击 **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 iDRAC7。有关版本的信息，请参阅 **dell.com/support/manuals** 上提供的 *Readme*（自述文件）。

如果从通过代理服务器连接到 Internet 的管理站连接到 iDRAC7 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. 在 Web 浏览器中，转至**工具 → Internet 选项 → 安全 → 本地网络**。
2. 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。
3. 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

4. 转至**工具** → **Internet 选项** → **高级**。
5. 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：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 iDRAC7 Web 界面可能无法正常工作。
6. 单击**应用**，然后单击**确定**。
7. 单击**连接**选项卡。
8. 在**局域网 (LAN) 设置**下，单击**局域网设置**。
9. 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。
10. 单击**确定**两次。
11. 关闭并重新启动浏览器，确保所有更改都生效。

**相关链接**

查看 Web 界面的本地化版本

## 将 iDRAC7 添加到受信域列表中

当您访问 iDRAC7 Web 界面时，如果受信域列表中没有 iDRAC7 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 **Refresh（刷新）**或者重新启动 Web 浏览器以建立指向 iDRAC7 Web 界面的连接。

在某些操作系统上，如果受信域列表中缺少 iDRAC7 IP 地址，Internet Explorer (IE) 8 不会提示用户将该 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 iDRAC7 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 iDRAC7 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 **Add this website to the zone（将该网站添加到区域）**中输入 iDRAC7 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 iDRAC7 安装 Virtual Console 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

iDRAC7 Web 界面提供以下语言的版本：

- 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。

iDRAC7 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。iDRAC7 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 iDRAC7 Web 界面。

# 更新设备固件

使用 iDRAC7 可以更新 iDRAC7、BIOS 和所有通过 Lifecycle Controller 更新支持的设备固件，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

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 更新包 (DUP)
- **.d7**
- **.usc**
- **.pm**

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**、**.usc** 以及 **.pm** 的文件，您必须具有 Configure（配置）权限。

**相关链接**

下载设备固件
使用 iDRAC7 Web 界面更新设备固件
使用 RACADM 更新设备固件
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：

- iDRAC7 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 iDRAC7。
- 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 - 下载最新的编录文件和 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/support/manuals** 上提供的 *Lifecycle Controller User's Guide*（Lifecycle Controller 用户指南）。

## 使用 iDRAC7 Web 界面更新设备固件

要使用 iDRAC7 Web 界面更新设备固件，请执行以下操作：

1. 转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Update and Rollback（更新和回滚）** → **Update（更新）**。
   此时将显示 **Firmware Update**（固件更新）页面。
2. 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）。
3. 在上载完成后，**Update Details**（更新详细信息）部分显示上载到 iDRAC 的每个固件文件及其状态。有关字段的信息，请参阅 *iDRAC7 Online Help*（iDRAC7 联机帮助）。
4. 选择需要更新的固件文件并单击以下任一选项：
   - 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 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`（更新作业队列）。
5. 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。

**相关链接**

更新设备固件
查看和管理分阶段更新
下载设备固件

## 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/support/manuals** 上提供的 *RACADM Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 参考指南）。

## 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 iDRAC7 固件。

使用 CMC Web 界面更新 iDRAC7 固件：

1. 登录到 CMC Web 界面。
2. 转至 **Server（服务器）** → **Overview（概述）** → **<server name>**。
   随即会显示 **Server Status**（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）。

**相关链接**

更新设备固件
下载设备固件
使用 iDRAC7 Web 界面更新设备固件

## 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 iDRAC7 固件时，如果看到控制台中显示如 `usb 5-2: device descriptor read/64, error -71`（`usb 5-2：设备描述符读取/64，错误 -71`）之类的错误信息，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`

使用 DUP 更新 iDRAC7：

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 <iDRAC7 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 <iDRAC7 IP address> -u <username> -p <password> update —f <filename>`

   FTP 服务器：

   - 使用 **fwupdate** 命令：`racadm -r <iDRAC7 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 <iDRAC7 IP address> -u <username> -p <password> update —f <filename>`

   有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）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/support/manuals** 上提供的 *Lifecycle Controller Remote Services Quick Start Guide*（Lifecycle Controller Remote Services 快速入门指南）。

# 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。

**相关链接**

更新设备固件

## 使用 iDRAC7 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 **Overview（概述）** → **Server（服务器）** → **Job Queue（作业队列）**。**Job Queue**（作业队列）页面显示 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 *iDRAC7 Online Help*（iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 回滚 iDRAC7 固件

您可以使用下列方法将固件回滚到之前安装的版本：

- iDRAC7 Web 界面
- CMC Web 界面
- RACADM CLI（iDRAC7 和 CMC）
- Lifecycle Controller
- Lifecycle Controller 远程服务

**相关链接**

使用 iDRAC7 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-Remote Services 回滚固件

## 使用 iDRAC7 Web 界面回滚固件

要使用 iDRAC7 Web 界面回滚固件，请执行以下操作：

**注:** 当前仅支持对 iDRAC7 固件的回滚，不支持任何其他设备固件。

1. 在 iDRAC7 Web 界面中，转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Update and Rollback（更新和回滚）** → **Rollback（回滚）**。

**Rollback**（回滚）页面显示当前和以前的固件版本。

2. 单击 **Next**（下一步）。
   在应用回滚后，iDRAC7 重新引导。

   **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。

   **注:** 如果将 iDRAC7 配置重设为默认值，则会将 iDRAC7 IP 地址重设为 192.168.0.120。您可以使用此 IP 访问 iDRAC7，或者使用本地 RACADM 或 F2（远程 RACADM 需要网络访问权限）重新配置 iDRAC7 地址。

3. 回滚完成后，iDRAC7 会重设。要使用 iDRAC7，您必须关闭当前浏览器窗口并使用新的浏览器窗口重新连接。
4. 要查看 iDRAC7 固件版本，请转至下列任何页面：
   - 转至 **Overview（概述）** → **Server（服务器）** → **Properties（属性）** → **Summary（摘要）**并在 **Server Information**（服务器信息）部分下查看固件版本。
   - 转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Properties（属性）**并在 **Integrated Dell Remote Access Controller 7**（集成 Dell Remote Access Controller 7）部分下查看固件版本。

## 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 **Launch iDRAC（启动 iDRAC）**Web 界面并执行 iDRAC7 固件回滚。

## 使用 RACADM 回滚固件

您只能使用 RACADM 将 iDRAC 固件回滚到以前的固件版本。要实现这一点，请使用 **fwupdate** 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 使用 Lifecycle Controller 回滚固件

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

## 使用 Lifecycle Controller-Remote Services 回滚固件

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

## 恢复 iDRAC7

iDRAC7 支持两个操作系统映像，以确保 iDRAC7 可引导。如果出现无法预见的灾难性错误，导致您丢失两个引导路径：

- iDRAC7 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 iDRAC7，然后重新引导 iDRAC7。

### 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 iDRAC7 固件或安装证书。该协议在 SM-CLP 和 RACADM 命令行界面中用于为 iDRAC7 收发文件。TFTP 服务器必须使用 iDRAC7 IP 地址或 DNS 名称进行访问。

**注:** 如果您使用 iDRAC7 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。

## 备份和还原服务器配置文件

您可以备份系统配置，包括各个组件上安装的固件映像和这些组件的配置设置。备份创建可保存到 vFlash SD 卡或网络共享（CIFS 或 NFS）的单个文件。

在对 vFlash SD 卡执行备份操作之前，请确保：

- 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。

备份文件包含加密的用户敏感数据、配置信息和固件映像，您可以对其执行还原操作。

在执行还原操作之前，确保已启用了 Lifecycle Controller。

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。还原操作适用于相同且位于同一位置（例如相同插槽）的所有系统组件（已在备份文件中捕获）。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。

### 使用 iDRAC7 Web 界面备份服务器配置文件

要使用 iDRAC7 Web 界面备份服务器配置文件，请执行以下操作：

1. 转至 **Overview（概述）→ iDRAC Settings（iDRAC 设置）→ Backup and Restore（备份和还原）**。
   此时将显示 **Backup and Restore Server Profile**（备份和还原服务器配置文件）页面。
2. 选择 **Backup**（备份）。
3. 选择以下选项之一保存备份文件映像：
   - 网络共享，在 CIFS 或 NFS 共享上保存备份文件映像。
   - VFLASH
4. 输入备份文件名和加密密码（可选）。
5. 如果选择 **Network**（网络）作为文件位置，请输入网络设置。

有关各字段的信息，请参阅 *iDRAC7 Online Help*（iDRAC7 联机帮助）。

6. 单击 **Backup Server Profile**（备份服务器配置文件）。
   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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 使用 iDRAC7 Web 界面还原服务器配置文件

备份文件用于还原系统。
要使用 iDRAC7 Web 界面备份和还原服务器配置文件，请执行以下操作：

1. 转至 **Overview（概述）→ iDRAC Settings（iDRAC 设置）→ Backup and Restore（备份和还原）**。
   此时将显示 **Backup and Restore Server Profile**（备份和还原服务器配置文件）页面。
2. 选择 **Restore**（还原）。
3. 选择以下任一项指定备份文件的位置：
   - 网络共享
   - VFLASH
4. 输入备份文件名和解密密码（可选）。
5. 如果选择 **Network**（网络）作为文件位置，请输入网络设置。
   有关各字段的信息，请参阅 *iDRAC7 Online Help*（iDRAC7 联机帮助）。
6. 选择以下一项：
   - **Preserve**（保留）- 保留现有的虚拟磁盘配置和硬盘数据。
   - **Delete and Replace**（删除并替换）- 使用备份映像文件中的数据替换系统。
7. 单击 **Restore Server Profile**（还原服务器配置文件）。
   还原操作即得到启动。

## 使用 RACADM 还原服务器配置文件

要使用 RACADM 还原服务器配置文件，请使用 **systemconfig restore** 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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 iDRAC7

您可以使用 Dell Management Console 或 Dell OpenManage Essentials 查找和监测 iDRAC7。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 iDRAC7

通过 iDRAC7 可配置 iDRAC7 属性、设置用户以及设置警报，以执行远程管理任务。

在配置 iDRAC7 之前，请确保已配置 iDRAC7 网络设置和支持的浏览器，并且已更新需要的许可证。有关 iDRAC7 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 iDRAC7：

- iDRAC7 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 iDRAC7，请执行以下操作：

1. 登录到 iDRAC7。
2. 如有必要，修改网络设置。

   **注:** 如果您已配置 iDRAC7 网络设置，请在 iDRAC7 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 iDRAC7 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 iDRAC7 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 iDRAC7 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。

**相关链接**

登录 iDRAC7

修改网络设置

# 查看 iDRAC7 信息

您可以查看 iDRAC7 的基本属性。

## 使用 Web 界面查看 iDRAC7 信息

在 iDRAC7 Web 界面中，请转到 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Properties（属性）**，查看与 iDRAC7 相关的以下信息。有关各属性的信息，请参阅 *iDRAC7 联机帮助*。

- 设备类型
- 硬件和固件版本
- 最新固件更新
- RAC 时间
- 可能激活的会话数
- 目前会话数
- LAN 处于启用或禁用状态
- 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 iDRAC7 信息

要使用 RACADM 查看 iDRAC7 信息，请参阅 **dell.com/support/manuals** 上 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）中提供的 `getsysinfo` 或 `get` 子命令详细信息。

# 修改网络设置

使用 iDRAC 设置公用程序配置 iDRAC7 网络设置后，您还可以通过 iDRAC7 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 iDRAC7 Web 界面或 RACADM 修改网络设置，您必须具有 **Configure**（配置）权限。

**注:** 更改网络设置可能会使指向 iDRAC7 的当前网络连接中断。

## 使用 Web 界面修改网络设置

要修改 iDRAC7 网络设置，请执行以下操作：

1. 在 iDRAC7 Web 界面中，转至 **Overview**（概述） → **iDRAC Settings**（iDRAC 设置） → **Network**（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 *iDRAC7 Online Help*（iDRAC7 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，iDRAC7 LAN 也会处于禁用状态。

## 配置 IP 筛选和 IP 阻塞

除了用户验证之外，访问 iDRAC7 时使用以下选项可提供更高的安全性：

- IP 筛选限制访问 iDRAC7 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 Management Station（其 IP 地址位于该范围内）的 iDRAC7 访问。所有其他登录请求都将被拒绝。
- IP 阻塞可动态确定来自特定 IP 地址的登录失败次数上限，并防止（或阻止）该地址在预选的时间范围内登录 iDRAC7。包括：
  - 允许的登录失败次数。
  - 这些失败必须发生的时间范围（以秒为单位）。
  - 被阻塞 IP 地址在超过允许失败次数后不能建立会话的时间（以秒为单位）。

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`（ssh exchange 标识：连接被远程主机关闭）。

**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 iDRAC7 Web 界面配置 IP 过滤和 IP 封锁

您必须具有配置 iDRAC7 的权限才能执行这些步骤。

配置 IP 过滤和 IP 封锁：

1. 在 iDRAC7 Web 界面中，转至 **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. 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 过滤和封锁设置。
   有关各选项的信息，请参阅 *《iDRAC7 联机帮助》*。
4. 单击 **Apply（应用）**保存设置。

### 使用 RACADM 配置 IP 筛选和 IP 阻塞

您必须具有配置 iDRAC7 的权限才能执行这些步骤。

要配置 IP 筛选和 IP 阻塞，请使用以下 RACADM 对象：

- 使用 **config** 命令：
  - cfgRacTuneIpRangeEnable
  - cfgRacTuneIpRangeAddr
  - cfgRacTuneIpRangeMask
  - cfgRacTuneIpBlkEnable
  - cfgRacTuneIpBlkFailCount

- cfgRacTuneIpBlkFailWindow

- 将 **set** 命令与 **iDRAC.IPBlocking** 组中的对象配合使用：
  - RangeEnable
  - RangeAddr
  - RangeMask
  - BlockEnable
  - FailCount
  - FailWindow
  - PenaltyTime

**cfgRacTuneIpRangeMask** 或 **RangeMask** 属性对接入 IP 地址和 **cfgRacTuneIpRangeAddr** 或 **RangeAddr** 属性的 IP 地址均适用。如果结果相同，则允许接入登录请求访问 iDRAC7。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。

**IP 阻塞的示例**

- 以下示例说明，如果在一分钟内连续五次尝试登录失败，则会阻止管理站 IP 地址建立会话五分钟。
  - 使用 **config** 命令：

    ```
    racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1 racadm
    config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5 racadm config -
    g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
    ```

  - 使用 **set** 命令：

    ```
    racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set
    iDRAC.IPBlocking.FailCount 5 racadm set iDRAC.IPBlocking.FailWindow
    60
    ```

- 以下示例会阻止一分钟内三次以上的失败尝试，并阻止附加登录尝试一小时；

- 使用 **config** 命令：

  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1 racadm
  config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3 racadm config -
  g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60 racadm config -g
  cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
  ```

- 使用 **set** 命令：

  ```
  racadm set iDRAC.IPBlocking.BlockEnable 1 racadm set
  iDRAC.IPBlocking.FailCount 3 racadm set iDRAC.IPBlocking.FailWindow
  60 racadm set iDRAC.IPBlocking.PenaltyTime 3600
  ```

有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 配置服务

您可以在 iDRAC7 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 iDRAC7 配置。
- Web Server - 启用对 iDRAC7 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 时会同时禁用远程 RACADM。
- SSH - 通过固件 RACADM 访问 iDRAC7。
- Telnet - 通过固件 RACADM 访问 iDRAC7
- 远程 RACADM - 远程访问 iDRAC7。
- SNMP 代理 - 启用对 iDRAC7 中 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。

## 使用 Web 界面配置服务

使用 iDRAC7 Web 界面配置服务：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Services（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*《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 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。

**相关链接**

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 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Hardware（硬件）** → **Front Panel（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）
   - 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 **Apply**（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 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**（上一步）、**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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Hardware（硬件）** → **Front Panel（前面板）**。将显示 **Front Panel（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：

   - Blink Off（闪烁关闭）
   - Blink On（闪烁开启）

- Blink On 1 Day Timeout（闪烁开启 1 天超时）
- Blink On 1 Week Timeout（闪烁开启 1 周超时）
- Blink On 1 Month Timeout（闪烁开启 1 个月超时）

3. 单击 **Apply（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 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 *iDRAC7 Online Help*（iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 设置第一引导设备

您可以设置第一引导设备仅用于下次引导或用于所有后续重新引导。根据此选择，您可以设置系统的第一引导设备。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 iDRAC7 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设备之一：

- 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
- 远程文件共享
- 本地 SD 卡

- VFLASH
- Lifecycle Controller
- BIOS Boot Manager

**注:** iDRAC7 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

使用 iDRAC7 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。
   有关选项的详细信息，请参阅*《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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。您可以对 Setting First Boot Device（设置第一引导设备）中列出的所有支持设备执行一次引导。

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 iDRAC7 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 Card (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）或专用 NIC（机架、塔式或刀片服务器），在 iDRAC7 和主机操作系统之间提供高速双向带内通信。iDRAC7 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：

- 主机操作系统和 iDRAC7 位于同一子网。
- 已配置主机操作系统 IP 地址。
- 您具有 Configure（配置）权限。

在启用此功能时：

- 在共享模式下，主机操作系统的 IP 地址自动填充。
- 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。

下表提供支持 OS 到 iDRAC 直通功能的卡的列表。

**表. 7: ：OS 到 iDRAC 直通 - 支持的卡**

| 类别 | 制造商 | 类型 |
|---|---|---|
| NDC | Broadcom | • 57800S QP rNDC (10G BASE-T + 1G BASE-T) |

| 类别 | 制造商 | 类型 |
| --- | --- | --- |
| | | • 57800S QP rNDC (10G SFP+ + 1G BASE-T)<br>• 5720 QP rNDC 1G BASE-T<br>• 57810S DP bNDC KR<br>• 57840 4x10G SFP+ (Sirius)<br>• 57840 4x10G KR (Regulus) |
| | Intel | • i540 QP rNDC (10G BASE-T + 1G BASE-T)<br>• i350 QP rNDC 1G BASE-T<br>• i520 DP bNDC KR<br>• x520 2X10G SFP+ / i350 2X1G Base-T (Saiph) |
| | QLogic | 10G DP bNDC KR |
| 夹层卡 | Broadcom | • 5719 QP 1G Mezz<br>• 57810S DP 10G KR Mezz |
| | Intel | • DP 10Gb KR Mezz<br>• i350 QP 1G Mezz |
| | QLogic | • DP 10Gb SFP+/DA CNA Mezz<br>• QME2662 FC16<br>• QME2572 FC8 |
| | Emulex | LPM16002 |
| NIC | Broadcom | • 57810 DP 10G SFP+ ADAPTER<br>• 57810C DP 10G BASE-T ADAPTER<br>• 5720 DP 1G ADAPTER<br>• 5719 QP 1G ADAPTER |
| | Intel | • X540 DP 10G BASE-T ADAPTER<br>• I350 DP 1G ADAPTER<br>• I350 QP 1G ADAPTER<br>• X520 DP 10G SFP+ ADAPTER |
| | QLogic | DP 10Gb SFP+/DA CNA ADAPTER |
| PCIe | Emulex | LPe16000 |
| | Qlogic | • QLE2660 FC16<br>• QLE2662 FC16<br>• QLE2560 FC8<br>• QLE2562 FC8 |

以下各卡不支持 OS 到 iDRAC 直通功能：

- Intel 10 Gig bNDC。
- 包含两个控制器的 Intel rNDC (Elk Flat rNDC) – 10G 控制器不支持。

- Qlogic bNDC Part # D90TX。

## 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 **Enable**（启用）。配置的主机 OS IP 地址显示在 **OS IP Address**（OS IP 地址）字段中。要禁用，请选择 **Disable**（禁用）并转至步骤 4。
3. 单击 **Test Network Connection**（测试网络连接）验证 iDRAC 是否能连接到此 IP 地址。
4. 单击 **Apply**（应用）。OS 到 iDRAC 直通已启用。

## 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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 **OS to iDRAC Pass-Through**（OS 到 iDRAC 直通）。
   随即显示 **iDRAC Settings.OS to iDRAC Pass-through**（iDRAC 设置 OS 到 iDRAC 直通）页面。
2. 选择 **Enabled**（启用）以启用 OS 到 iDRAC 直通。否则，请选择 **Disabled**（禁用）。配置的主机 OS IP 地址显示在 **OS IP Address**（OS IP 地址）字段中。
3. 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. 8: 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 的单一登录 | 可信 CA 证书 | 生成 CSR 并从证书认证机构获取签名 |
| 本地或 Active Directory 用户的智能卡登录 | • 用户证书<br>• 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。<br>• 可信 CA 证书 — 此证书由 CA 颁发。 |
| Active Directory 用户登录 | 可信 CA 证书 | 此证书由 CA 颁发。 |
| 本地用户登录 | SSL 证书 | 生成 CSR 并从可信 CA 获取签名 |

| 登录类型 | 证书类型 | 获取方法 |
| --- | --- | --- |
| | | **注:** iDRAC7 自带默认的自签名 SSL 服务器证书。iDRAC7 Web 服务器、虚拟介质和虚拟控制台使用此证书。 |

**相关链接**

SSL 服务器证书
生成新的证书签名请求

## SSL 服务器证书

iDRAC7 包含 Web 服务器，该服务器配置为使用工业标准的 SSL 安全协议在网络上传输加密数据。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

该加密进程可提供高级数据保护。iDRAC7 采用 128 位 SSL 加密标准，这是北美常用的 Internet 浏览器最安全的加密形式。

iDRAC7 Web 服务器默认包含 Dell 自签名的唯一 SSL 数字证书。您可以用已知证书颁发机构 (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。要启动获得 CA 签名的证书的过程，请使用 iDRAC7 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。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）。

**相关链接**

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 iDRAC7。用于生成 CSR（存储在 iDRAC7 固件）上的信息必须与 SSL 服务器证书中包含的信息匹配，也就是说，该证书必须通过 iDRAC7 创建的 CSR 生成。

**相关链接**

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，iDRAC7 不会接受该证书。

1. 在 iDRAC7 Web 界面中，转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **SSL**，选择 **Generate a New Certificate Signing Request (CSR)**（生成一个新证书签名请求 (CSR)），然后单击 **Next**（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 *iDRAC7 Online Help*（iDRAC7 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 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 上载服务器证书

生成 CSR 后，您可以将签名的 SSL 服务器证书上载到 iDRAC7 固件。iDRAC7 会在证书上载后重设。iDRAC7 仅接受 X509，Base 64 编码的 Web 服务器证书。

**小心: 在重设期间，iDRAC7 在几分钟内不可用。**

**相关链接**

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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **SSL**，选择 **Upload Server Certificate（上载服务器证书）**，然后单击 **Next（下一步）**。

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

2. 在 **File Path（文件路径）**下，单击 **Browse（浏览）**并选择 Management Station 上的证书。

3. 单击 **Apply（应用）**。

   SSL 服务器证书即会上载到 iDRAC7 固件，并替换现有的证书。

### 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 查看服务器证书

您可以查看当前在 iDRAC7 中使用的 SSL 服务器证书。

**相关链接**

SSL 服务器证书

### 使用 Web 界面查看服务器证书

在 iDRAC7 Web 界面中，转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **SSL**。**SSL** 页面当前会在此页面的顶部显示 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 上载自定义签名证书

您可以上载自定义签名证书来签署 SSL 证书。

### 使用 Web 界面上载自定义签名证书

要使用 iDRAC7 Web 界面上载自定义签名证书，请执行以下操作：

1. 转至 **Overview（概述）** → **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 **Apply**（应用）。
   证书即上载到 iDRAC 并且 iDRAC 重设。在重设期间，iDRAC 会有几分钟不可用。

### 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。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 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 iDRAC7 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 iDRAC7 Web 界面下载自定义签名证书，请执行以下操作：

1. 转至 **Overview（概述）→ 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 删除自定义 SSL 证书签名证书

您还可以使用 iDRAC7 Web 界面或 RACADM 删除现有的自定义签名证书。

### 删除自定义签名证书

要使用 iDRAC7 Web 界面删除自定义签名证书，请执行以下操作：

1. 转至 **Overview（概述）→ 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）。
   自定义签名证书即从 iDRAC 中删除。iDRAC 重设以使用 Web 服务器自动生成的默认自签名 SSL 证书。在重设期间，iDRAC 不可用。

### 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。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 使用 RACADM 配置多个 iDRAC7

您可以使用 RACADM 配置具有相同属性的一个或多个 iDRAC7。当您使用其组 ID 和对象 ID 查询特定 iDRAC7 时，RACADM 会从检索的信息创建 **.cfg** 配置文件。文件名是用户指定的。将文件导入其他 iDRAC7 可进行方式相同的配置。

**注:** 少数配置文件包含唯一的 iDRAC7 信息（例如静态 IP 地址），您必须修改然后才能将文件导出到其他 iDRAC7。

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 iDRAC7，请执行以下操作：

1. 使用以下命令查询包含所需配置的目标 iDRAC7：`racadm getconfig -f myfile.cfg`。

该命令请求 iDRAC7 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 iDRAC7 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 iDRAC7：`racadm config -f myfile.cfg`

   这会将信息加载到其他 iDRAC7。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 iDRAC7：`racadm racreset`

## 创建 iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

**.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。错误会使用检测到错误的行号进行标记，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 iDRAC7。在使用该文件配置 iDRAC7 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 iDRAC7 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。
- 每个索引组都提供预定义的索引集。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

- 使用 racresetcfg 子命令将 iDRAC7 重置为默认设置，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 子命令可将数据库和 iDRAC7 NIC 设置重设为默认设置，并移除所有用户和用户配置。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 iDRAC7 执行 racadm config -f <filename> .cfg 命令，而不添加转义字符。例如：

  ```
  #
  # 这是一条注释
  [cfgUserAdmin]
  cfgUserAdminPageModemInitString=<调制解调器初始化字符串中的 # 不是注释>
  ```

- 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。没有包括相关组名称的对象会生成错误。配置数据组织成组，如 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）中所定义。以下示例显示组名称、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 iDRAC7 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 iDRAC7 IP 地址

在配置文件中修改 iDRAC7 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 地址编号有关的两个 *<变量>*=**值**条目。

例如：

```
#
# 对象组 "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
```

```
cfgNicGateway=10.35.10.1
```

此文件更新如下：

```
#
# 对象组 "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# 注释，此行的其余部分将被忽略
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 iDRAC7 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 iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Services（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 **Apply（应用）**。

   **注:** 如果访问已禁用，您无法使用 Server Administrator 或 IPMITool 执行 iDRAC7 配置。但您可以使用 LAN 上 IPMI。

5

# 查看 iDRAC7 和受管系统信息

您可以查看 iDRAC7 和受管系统的运行状况和属性、硬件和固件资源清册、传感器运行状况、存储设备、网络设备以及查看和终止用户会话。对于刀片服务器，您还可以查看 flex address 信息。

**相关链接**



## 查看受管系统运行状况和属性

在登录 iDRAC7 Web 界面时，通过 **System Summary**（系统摘要）页面可以查看管理系统的运行状况、iDRAC7 的基本信息，预览虚拟控制台，添加和查看工作注释，以及快速启动如开启或关闭、关闭后再启动、查看日志、更新和回滚固件以及重设 iDRAC7 等任务。

要访问 **System Summary**（系统摘要）页面，请转至 **Overview（概述）→ Server（服务器）→ Properties（属性）→ Summary（摘要）**。随即会显示 **System Summary**（系统摘要）页面。有关更多信息，请参阅 *iDRAC7 Online Help*（iDRAC7 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

您可以查看关于管理系统上安装的硬件和固件组件的信息。要实现这一点，在 iDRAC7 Web 界面中，转至 **Overview（概述）→ Server（服务器）→ Properties（属性）→ System Inventory（系统资源清册）**。有关显示的属性的信息，请参阅 *iDRAC7 Online Help*（iDRAC7 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
- NIC（集成的和嵌入的）
- 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
- 机柜

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 **Collect System Inventory on Reboot (CSIOR)**（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 iDRAC7，然后导航至 **System Inventory**（系统资源清册）页面查看详细信息。信息可能需要长达五分钟才能可用，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。
- 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** - 提供关于系统板进气温度和排气温度（仅适用于机架式和塔式服务器）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报和临界阈值范围内。
- **电压** - 指示多个系统组件上电压传感器的状态和读数。

下表提供如何利用 iDRAC7 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 *iDRAC7 Online Help*（iDRAC7 联机帮助）。

**表. 9: 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 | **Overview（概述）→ Hardware（硬件）→ Batteries（电池）** | 使用 **getsensorinfo** 命令。<br>对于电源设备，您还可以使用 **System.Power.Supply** 命令和 **get** 子命令。<br>有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。 |
| 风扇 | **Overview（概述）→ Hardware（硬件）→ Fans（风扇）** | |
| CPU | **Overview（概述）→ Hardware（硬件）→ CPU** | |
| 内存 | **Overview（概述）→ Hardware（硬件）→ Memory（内存）** | |
| 侵入 | **Overview（概述）→ Server（服务器）→ Intrusion（侵入）** | |
| 电源设备 | **Overview（概述）→ Hardware（硬件）→ Power Supplies（电源设备）** | |
| 可移动闪存介质 | **Overview（概述）→ Hardware（硬件）→ Removable Flash Media（可移动闪存介质）** | |
| 温度 | **Overview（概述）→ Server（服务器）→ Power/Thermal（电源/耐热）→ Temperatures（温度）** | |
| 电压 | **Overview（概述）→ Server（服务器）→ Power/Thermal（电源/耐热）→ Voltages（电压）** | |

# 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:** 对于 135W CPU、PCIe SSD、GPU 卡和 LR DIMM，不支持新鲜空气配置。若要了解服务器的受支持新鲜空气配置，请与 Dell 联系。

检查系统的新鲜空气符合性：

1. 在 iDRAC7 Web 界面中，转至**概述 → 服务器 → 功率/热力 → 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温度阈值的环境温度下工作的时间的百分比。系统板入口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入口温度。

**注:** 您甚至可以跟踪不具有新鲜空气符合性的系统的入口温度历史。

共有两个温度范围被跟踪：

- 警告范围 — 包括系统在超过入口温度传感器警告阈值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 — 包括系统在超过入口温度传感器严重阈值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，入口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，入口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，入口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，入口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 iDRAC7 Web 界面查看历史温度数据

查看历史温度数据：

1. 在 iDRAC7 Web 界面中，转至**概述 → 服务器 → 功率/热力 → 温度**。
   随即会显示 **温度**页面。
2. 请参阅**系统板入口温度历史数据**部分，其中提供了过去一天、过去 30 天和过去一年的存储入口温度（平均值和峰值）的图形显示。
   有关更多信息，请参阅*《iDRAC7 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*《适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南》*。

# 资源清册和监测存储设备

您可以使用 iDRAC7 Web 界面或 RACADM 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（包括电池）。
- 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

不过，WS-MAN 显示系统中大多数存储设备的信息。

iDRAC7 可盘点和监测 PERC 8 系列的 RAID 控制器，包括 H310、H710、H710P 和 H810。不支持综合嵌入式管理的控制器为内部磁带适配器 (ITA) 和 SAS 6Gbps HBA。

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。

有关概念性信息，请参阅 **dell.com/support/manuals** 上提供的 *OpenManage Storage Management User's Guide*（OpenManage Storage Management 用户指南）。

## 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 **Overview（概览）** → **Storage（存储）** → **Summary（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 **Overview（概览）** → **Storage（存储）** → **Topology（拓扑）**查看重要存储组件的分层物理防护视图。
- 转至 **Overview（概览）** → **Storage（存储）** → **Physical Disks（物理磁盘）**查看物理磁盘信息。将显示 **Physical Disks（物理磁盘）**页面。
- 转至 **Overview（概览）** → **Storage（存储）** → **Virtual Disks（虚拟磁盘）**查看虚拟磁盘信息。将显示 **Virtual Disks（虚拟磁盘）**页面。
- 转至 **Overview（概览）** → **Storage（存储）** → **Controllers（控制器）**查看 RAID 控制器信息。将显示 **Controllers（控制器）**页面。
- 转至 **Overview（概览）** → **Storage（存储）** → **Enclosures（机柜）**查看机柜信息。将显示 **Enclosures（机柜）**页面。

您还可以使用筛选器查看特定的设备信息。

有关显示的属性和使用筛选器选项的详细信息，请参阅*《iDRAC7 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** 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 资源清单和监控网络设备

您可以远程监控受管系统中下列网络设备的运行状况并查看其资源清单。

- 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 (Network Daughter Cards, NDC)
- 夹层卡（Mezzanine cards，仅适用于刀片式服务器）

对于每个设备，您可以查看端口和支持分区的以下信息：

- Link Status（连接状态）
- Properties（属性）
- Settings and Capabilities（设置和功能）
- Receive and Transmit Statistics（接收和传送统计数据）

## 使用 Web 界面监控网络设备

要使用 Web 界面查看网络设备信息，请转至 **Overview（概览）** → **Hardware（硬件）** → **Network Devices（网络设备）**。随即会显示 **Network Devices（网络设备）**页面。有关所显示属性的详细信息，请参阅*《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

除了 iDRAC7 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

您可以远程监测运行状况并查看受管系统中光纤信道主机总线适配器 (FC HBA) 设备的资源清册。Emulex 和 QLogic（FC8 除外）FC HBA 受到支持。对于每台 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）

## 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 **Overview（概述）** → **Hardware（硬件）** → **Fibre Channel（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 *iDRAC7 Online Help*（iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 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 iDRAC7 中的 Flex 地址信息，请在 Chassis Management Controller 中配置并启用 Flex 寻址功能。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 iDRAC7 实施。iDRAC7 FlexAddress 功能支持为机箱中的 iDRAC7 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，如果启用 FlexAddress，该 MAC 地址会在 iDRAC7 引导过程中发送到 iDRAC7。

如果 CMC 启用机箱分配的 MAC 地址，iDRAC7 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，iDRAC7 IP 地址也会变化。**

# 查看或终止 iDRAC7 会话

您可以查看当前登录 iDRAC7 的用户数并终止用户会话。

## 使用 Web 界面终止 iDRAC7 会话

没有管理权限的用户必须先具备 Configure iDRAC7（配置 iDRAC7）权限才能使用 iDRAC7 Web 界面终止 iDRAC7 会话。

要查看和终止 iDRAC7 会话：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）→ iDRAC Settings（iDRAC 设置）→ Sessions（会话）**。

随即 **Sessions（会话）**页面会显示会话 ID、用户名、IP 地址以及会话类型。有关这些属性的详细信息，请参阅*《iDRAC7 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 iDRAC7 会话

您必须具有管理员权限才能使用 RACADM 终止 iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

6

# 设置 iDRAC7 通信

您可以使用下列模式之一与 iDRAC7 通信：

- iDRAC7 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. 10: 通信模式 — 摘要**

| 通信模式 | 支持的协议 | 支持的命令 | 前提条件 |
|---|---|---|---|
| **iDRAC7 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<br>SMCLP<br>IPMI | iDRAC7 固件的部分<br>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<br>SSH<br>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<br>Telnet | SMCLP | iDRAC7 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<br>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。 |
| **远程服务 [1]** | WS-MAN | WinRM (Windows)<br>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/support/manuals** 上提供的 *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller Remote Services 用户指南）。

**相关链接**

使用 DB9 电缆通过串行连接与 iDRAC7 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 iDRAC7 通信

使用 LAN 上 IPMI 与 iDRAC7 通信
启用或禁用远程 RACADM
禁用本地 RACADM
启用受管系统上的 IPMI
为引导期间的串行控制台配置 Linux
支持的 SSH 加密方案

# 使用 DB9 电缆通过串行连接与 iDRAC7 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 iDRAC7 中启用 RAC 串行连接或 IPMI 串行连接。

**相关链接**

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 iDRAC7。

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（返回）**、**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 iDRAC7 中启用 RAC 串行。

**注:** 这仅适用于机架式服务器和塔式服务器上的 iDRAC7。

### 使用 Web 界面启用 RAC 串行连接

启用 RAC 串行连接：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Serial（串行）**。
   随即会显示 **Serial（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 **Apply（应用）**。
   IPMI 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 iDRAC7 的 IPMI 串行路由，请在以下任意模式的 iDRAC7 中配置 IPMI 串行：

**注:** 这仅适用于机架和塔式服务器中的 iDRAC7。

- 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 iDRAC7 时查看操作系统引导顺序上至 BIOS。

**相关链接**

针对串行连接配置 BIOS
IPMI 串行终端模式的其他设置

### 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。

要配置 IPMI 串行接口设置：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Serial（串行）**。
2. 在 **IPMI Serial（IPMI 串行）**下，指定该属性的值。有关该选项的信息，请参阅*《iDRAC7 联机帮助》*。
3. 单击 **Apply（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 串行终端模式的其他设置

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 串行终端模式的其他设置*

要设置终端模式设置：

1. 在 iDRAC7 Web 界面中，转到 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Serial（串行）**。

   随即会显示 **Serial（串行）**页面。
2. 启用 IPMI 串行。
3. 单击 **Terminal Mode Settings（终端模式设置）** 。

   随即会显示 **Terminal Mode Settings（终端模式设置）**页面。
4. 指定以下值：
   - Line Editing（行编辑）

- Delete control（删除控制）
- Echo Control（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 *iDRAC7 联机帮助*。

5. 单击 **Apply（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

iDRAC7 支持退出键序列(Escape key sequences)，该序列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 iDRAC7 通信

IPMI LAN 上串行 (SOL) 允许受管系统基于文本的控制台串行数据通过 iDRAC7 的专用或共享带外以太网管理网络重定向。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 iDRAC7 以使用 SOL。
3. 启用支持的协议（SSH、Telnet、IPMItool）。

**相关链接**

针对串行连接配置 BIOS
配置 iDRAC7 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 iDRAC7。

1. 开启或重新启动系统。
2. 按 <F2> 键。
3. 转到 **System BIOS Settings（系统 BIOS 设置）** → **Serial Communication（串行通信）**。
4. 指定以下值：
   - Serial Communication（串行通信）— On With Console Redirection
   - Serial Port Address（串行端口地址）— COM2。

     **注:** 如果 **serial port address（串行端口地址）**字段中的 **serial device2（串行设备 2）**设置为 com1，则可将 **serial communication（串行通信）**字段设置为 **On with serial redirection via com1（开，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）**。

## 配置 iDRAC7 以使用 SOL

您可以使用 Web 界面、RACADM 或 iDRAC 设置公用程序指定 iDRAC7 中的 SOL 设置。

### 使用 iDRAC7 Web 界面配置 iDRAC7 以使用 SOL

要配置 IPMI LAN 上串行 (SOL)：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Serial Over LAN（LAN 上串行）**。

   随即会显示 **Serial Over LAN（LAN 上串行）**页面。
2. 启用 SOL，指定各值，然后单击 **Apply（应用）**。

   IPMI SOL 设置即配置完成。
3. 要设置字符积累间隔时间和字符发送阈值，请选择 **Advanced Settings（高级设置）**。

   随即会显示 **Serial Over LAN Advanced Settings（LAN 上串行高级设置）**页面。
4. 指定各属性的值并单击 **Apply（应用）**。

IPMI SOL 高级设置即配置完成。这些值有助于提升性能。

有关各选项的信息，请参阅*《iDRAC7 联机帮助》*。

### 使用 RACADM 配置 iDRAC7 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 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）**，并选择 **Enable IPMI Over LAN（启用 LAN 上 IPMI）**。请确保 **Encryption Key（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）

**相关链接**

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 <—> iDRAC7

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。有关详细信息，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 iDRAC7 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 iDRAC7 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 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Services（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），运行从 iDRAC7 启动 SOL 的命令：`ipmitool -H <iDRAC7-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，请重置 iDRAC7 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 iDRAC7 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 在 Telnet 上拥有增强的安全性。iDRAC7 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。iDRAC7 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 Management Station 上支持 SSH 和 Telnet 网络协议的开源程序（例如 PuTTY 或 OpenSSH）连接到 iDRAC7。

**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 iDRAC7 通信之前，请确保：

1. 配置 BIOS 以启用串行控制台。
2. 在 iDRAC7 中配置 SOL。
3. 使用 iDRAC7 Web 界面或 RACADM 启用 SSH 或 Telnet。

   Telnet（端口 23）/SSH（端口 22）客户端 <—> WAN 连接 <—> iDRAC7

   基于 IPMI 的 SOL 使用 SSH 或 Telnet 协议从而无需其他公用程序，因为串行到网络转换在 iDRAC7 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。

**相关链接**

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 iDRAC7：`putty.exe [-ssh | -telnet] <登录名>@<iDRAC7 ip 地址> <端口号>`

   **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 Management Station 到受管系统的、使用 SSH 或 Telnet 协议的 SOL 会话。要访问 iDRAC7 命令行控制台，请按照 ESC 键序列进行操作。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。

**相关链接**

在 iDRAC7 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 iDRAC7：
   - 对于 SSH：ssh *<iDRAC7-ip-address>* -l *<iDRAC7-ip-address>*
   - 对于 Telnet：telnet *<iDRAC7-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 iDRAC7 连接到受管系统的 SOL 端口。一旦建立 SOL 会话后，iDRAC7 命令行控制台将不可用。按照转义序列正确操作以打开 iDRAC7 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。

**相关链接**

使用 Telnet 虚拟控制台
为 Telnet 会话配置 Backspace 键
在 iDRAC7 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 **Virtual Console（虚拟控制台）** → **Remote Terminal Type（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. 使用命令连接到 iDRAC7：`telnet <IP 地址>:<端口号>`，其中 `IP 地址`是 iDRAC7 的 IP 地址，而`端口号`是 Telnet 端口号（如果你使用新端口）。

### *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`（`Backspace 将用 delete 代替`）。

### *在 iDRAC7 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，从 iDRAC7 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 iDRAC7 通信

您必须为 iDRAC7 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。如果该配置未完成，则外部系统无法使用 IPMI 命令与 iDRAC7 服务器通信。

## 使用 Web 界面配置 LAN 上 IPMI

配置 LAN 上 IPMI：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）**。
   将显示 **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 *iDRAC7 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 设置公用程序联机帮助*。
3. 依次单击 **Back（返回）**、**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:** iDRAC7 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 iDRAC7 Web 界面或 RACADM 启用或禁用远程 RACADM。您可以并行运行最多五个远程 RACADM 会话。

## 使用 Web 界面启用或禁用远程 RACADM

启用或禁用远程 RACADM：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Services（服务）**。
   将显示 **Services（服务）**页面。
2. 在 **Remote RACADM（远程 RACADM）**下，选择 **Enabled（已启用）**。否则，选择 **Disabled（已禁用）**。
3. 单击 **Apply（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 默认情况下已启用。要禁用，请参阅禁用访问以修改主机系统上的 iDRAC7 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）。

# 为引导期间的串行控制台配置 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。

   ```
   # 通过 anaconda 生成的 grub.conf # 请注意，您对此文件进行更改后无需重新运行 grub # 注意：您没有 /boot 分区。这意味着所有 # 内核和 initrd 路径都与 / 相关，例如 # root (hd0,0) # kernel /boot/vmlinuz-version ro root=/dev/sda1 # 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
```

以下示例显示新增了一行的示例文件。

```
#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
```

以下示例显示新增了一行的示例文件。

**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 iDRAC7 通信，它支持下表中列出的多种密码方案。

**表. 11: 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<br>• RIJNDAEL256-CBC<br>• AES192-CBC<br>• RIJNDAEL192-CBC<br>• AES128-CBC<br>• RIJNDAEL128-CBC<br>• BLOWFISH-128-CBC<br>• 3DES-192-CBC<br>• ARCFOUR-128 |
| 信息完整性 | • HMAC-SHA1-160<br>• HMAC-SHA1-96<br>• HMAC-MD5-128<br>• HMAC-MD5-96 |
| 身份验证 | 密码 |
| PKA 身份验证 | 公-私密钥对 |

## 对 SSH 使用公共密钥验证

iDRAC7 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 iDRAC7 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 Management Station 上生成一对私有和公共密钥。将公共密钥上载到 iDRAC7 本地用户，同时 SSH 客户端会使用私有密钥来建立 Management Station 与 iDRAC7 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 iDRAC7 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 **Generate（生成）**，根据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:** iDRAC7 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。

添加新的公共密钥时，请确保现有的密钥不会在添加新密钥位置的索引中。iDRAC7 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 iDRAC7 Web 界面中，请转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **User Authentication（用户验证）** → **Local Users（本地用户）**。

   将显示 **Users（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。

   有关详细信息，请参阅《iDRAC7 联机帮助》。
5. 单击 **Apply（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，要使用文件将有效的密钥上载到第一个密钥空间中的 iDRAC7 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

您可以查看上载到 iDRAC7 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）**。

   将显示 **Users（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 **View/Remove SSH Key(s)（查看/删除 SSH 密钥）**，然后单击 **Next（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）**。

   将显示 **Users（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 Key Configurations（SSH 密钥配置）**下，选择 **View/Remove SSH Key(s)（查看/删除 SSH 密钥）**，然后单击 **Next（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 iDRAC7 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 iDRAC7。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从而允许其他用户访问 iDRAC7。

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。

iDRAC7 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。

**相关链接**

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 iDRAC7 上配置多达 16 个本地用户。在创建 iDRAC7 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设置用户名、密码和角色。这些用户名和密码可通过任何 iDRAC7 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。

**注:** SNMPv3 功能已获得许可，iDRAC7 Enterprise 许可证提供此功能。

## 使用 iDRAC7 Web 界面配置本地用户

添加和配置本地 iDRAC7 用户：

**注:** 您必须具有 Configure Users（配置用户）权限才能创建 iDRAC7 用户。

1. 在 iDRAC7 Web 界面中，请转至 **Overview（概述）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户验证）** → **Local Users（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。有关这些选项的更多信息，请参阅 *iDRAC7 Online Help*（iDRAC7 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 配置单个或多个 iDRAC7 用户。

要配置多个具有相同配置设置的 iDRAC7 用户，请执行以下程序之一：

- 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 iDRAC7 配置文件并执行 **racadm config** 或 **racadm set** 子命令。

如果您正在配置新的 iDRAC7 或者您已经使用 **racadm racresetcfg** 命令，则唯一的当前用户是 `root`，密码为 `calvin`。**racresetcfg** 子命令会将 iDRAC7 重设为默认值。

**注:** 用户随后可以被启用，也可以被禁用。因此，在每个 iDRAC7 上，用户可能具有不同的索引编号。

要验证用户是否存在，请在命令提示符处键入以下命令之一：

- 使用 **config** 命令：`racadm getconfig -u <username>`
- 使用 **get** 命令：`racadm get ―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 iDRAC7 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** 命令来指定任意数量要写入的组/对象，则无法指定索引。这种行为允许使用相同设置配置多个 iDRAC7 时具备更大的灵活性。

### 使用 RACADM 添加 iDRAC7 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：

- iDRAC7
- LAN
- 串行端口
- 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 启用具有权限的 iDRAC7 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列表，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。默认权限值为 0，即表示用户没有启用权限。

# 配置 Active Directory 用户

如果您的公司使用 Microsoft Active Directory 软件，则可以配置该软件以提供访问 iDRAC7 的权限，从而允许添加和控制目录服务中现有用户的 iDRAC7 用户权限。这是获得许可证的功能。

**注:** 在 Microsoft Windows® 2000、Windows Server 2003 和 Windows Server 2008 操作系统上支持使用 Active Directory 来识别 iDRAC7 用户。

您可以通过 Active Directory 配置用户身份验证以登录到 iDRAC7。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。

从服务器生成后，iDRAC7 角色和权限的名称已发生更改。角色名称为：

**表. 12: iDRAC7 角色**

| 目前这一代 | 前一代 | 权限 |
|---|---|---|
| 管理员 | 管理员 | 登录、配置、配置用户、日志、系统控制、访问虚拟控制台、访问虚拟介质、系统操作、调试 |
| 操作员 | 高级用户 | 登录、配置、系统控制、访问虚拟控制台、访问虚拟介质、系统操作、调试 |
| 只读 | 来宾用户 | 登录 |
| 无 | 无 | 无 |

**表. 13: iDRAC7 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）<br>访问虚拟控制台（适用于机架式和塔式服务器） | 使用户可以运行虚拟控制台。 |
| 访问虚拟介质 | 访问虚拟介质 | 使用户可以运行和使用虚拟介质。 |
| 系统操作 | 测试警报 | 允许以异步通知的方式发送用户发起和生成的事件以及信息并进行记录。 |
| 调试 | 执行诊断命令 | 使用户可以运行诊断命令。 |

**相关链接**

对 iDRAC7 使用 Active Directory 验证的前提条件

支持的 Active Directory 验证机制

## 对 iDRAC7 使用 Active Directory 验证的前提条件

要使用 iDRAC7 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。iDRAC7 使用标准公共密钥架构 (PKI) 机制来验证 Active Directory 的安全性。有关详细信息，请参阅 Microsoft 网站。
- 在 iDRAC7 连接到的所有域控制器上启用安全套接字曾 (SSL)，以验证所有域控制器的安全性。

**相关链接**

在域控制器上启用 SSL

## 在域控制器上启用 SSL

当 iDRAC7 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 iDRAC7 中。对于*任何*要使用域控制器验证的 iDRAC7 — 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 iDRAC7。
3. 导入 iDRAC7 固件 SSL 证书。

**相关链接**

安装每个域控制器的 SSL 证书
将域控制器根 CA 证书导出至 iDRAC7
导入 iDRAC7 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 iDRAC7

**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 iDRAC7：

1. 找到运行 Microsoft Enterprise CA 服务的域控制器。
2. 单击 **Start（开始）** → **Run（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 **Local Computer（本地计算机）**，单击 **Finish（完成）**，然后单击 **OK（确定）**。
9. 在 **Console 1（控制台 1）**窗口中，转到 **Certificates（证书）Personal（个人）Certificates（证书）文件夹**。
10. 找到并右键单击根 CA 证书，选择 **All Tasks（所有任务）**，然后单击 **Export...（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. 将第 13 步保存的证书上载到 iDRAC7。

### 导入 iDRAC7 固件 SSL 证书

iDRAC7 SSL 证书是用于 iDRAC7 Web 服务器的相同证书。所有 iDRAC7 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 iDRAC7 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 iDRAC7 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 Trusted Root Certificate Authority（受信任的根认证机构）列表中，请勿执行本节中的步骤。

将 iDRAC7 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 iDRAC7 SSL 证书：

   ```
   racadm sslcertdownload -t 0x1 -f <RAC SSL 证书>
   ```
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 **Certificates（证书）**，选择 **All Tasks（所有任务）**并单击 **Import（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 **Trusted Root Certification Authority（受信任的根认证机构）**中安装 iDRAC7 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 **Finish（完成）**，然后单击 **OK（确定）**。iDRAC7 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 iDRAC7 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 iDRAC7 上配置用户访问权限提供了最大的灵活性。

**相关链接**

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 iDRAC7 上都进行配置。

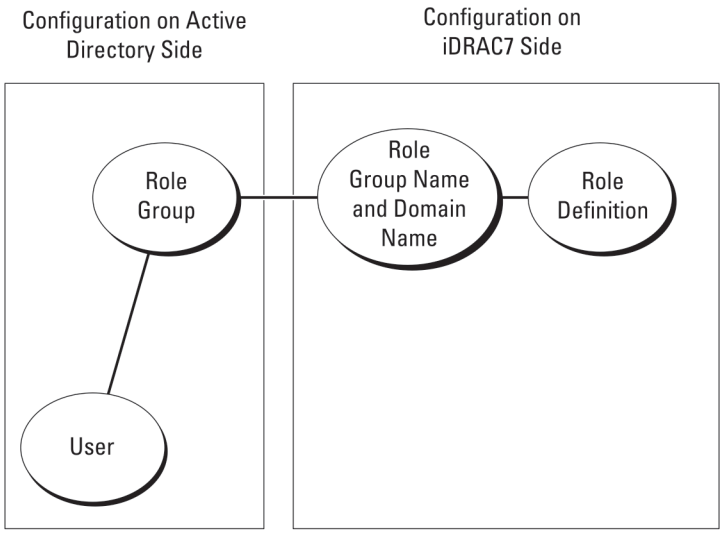


**图 1: 使用 Active Directory 标准架构配置 iDRAC7**

在 Active Directory 中，标准组对象用作角色组。具有 iDRAC7 访问权限的用户属于角色组的成员。要为此用户分配访问特定 iDRAC7 的权限，需要在特定 iDRAC7 上配置角色组名称及其组名。角色及权限级别在每个 iDRAC7（而不是 Active Directory 中）上进行定义。在每个 iDRAC7 中，您最多可以定义五个角色组。表参考编号显示了默认角色组的权限。

**表. 14: 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 | Login to iDRAC（登录到 iDRAC）、Configure iDRAC（配置 iDRAC）、Configure Users（配置用户）、Clear Logs（清除日志）、Execute Server Control Commands（执行服务器控制命令）、Access Virtual Console（访问虚拟控制台）、Access Virtual Media（访问虚拟介质）、Test Alerts（测试警报）、Execute Diagnostic Commands（执行诊断命令） | 0x000001ff |
| 角色组 2 | 无 | Login to iDRAC（登录到 iDRAC）、Configure iDRAC（配置 iDRAC）、Execute Server Control Commands（执行服务器控制命令）、Access Virtual Console（访问虚拟控制台）、Access Virtual Media（访问虚拟介质）、Test Alerts（测试警报）、Execute Diagnostic Commands（执行诊断命令） | 0x000000f9 |

| 角色组 | 默认权限级别 | 授予的权限 | 位掩码 |
|---|---|---|---|
| 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:** Bit Mask（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 iDRAC7 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 iDRAC7 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 Universal Group（通用组）类型。

## 配置标准架构 Active Directory

配置 iDRAC7 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 用户作为 Active Directory 组的成员添加以访问 iDRAC7。
3. 在 iDRAC7 上使用 iDRAC7 Web 界面或 RACADM 配置组名、域名和角色权限。

**相关链接**

使用 iDRAC7 Web 界面以标准架构配置 Active Directory
使用 RACADM 配置具有标准架构的 Active Directory

### 使用 iDRAC7 Web 界面以标准架构配置 Active Directory

**注:** 有关各字段的信息，请参阅*《iDRAC7 联机帮助》*。

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户验证）** → **Directory Services（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. 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。
4. 请单击 **Next（下一步）**。

   将显示 **Active Directory Configuration and Management Step 2 of 4（Active Directory 配置和管理第 2 步，共 4 步）**页面。
5. 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 iDRAC7 登录过程中 iDRAC7 必须等待 Active Directory 响应的时间。

   **注:** 如果证书验证已启用，请指定域控制器服务器地址和全局编录 FQDN。确保 DNS 已在 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）**下正确配置。
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 **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。

8. 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。
9. 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。
10. 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。
11. 单击 **Finish（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 iDRAC7 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。iDRAC7 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 证书>
```

2. 如果 iDRAC7 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 iDRAC7 上已禁用 DHCP 或者想手动输入 DNS IP 地址，则输入以下 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

要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 到 12079`

### iDRAC7 架构扩展概览

Dell 已扩展架构以包括 *Association（关联）*、*Device（设备）*和 *Privilege（权限）*属性。*Association（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 iDRAC7 设备。此模型为网络上有各种用户、iDRAC7 权限和 iDRAC7 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 iDRAC7 设备，创建至少一个关联对象和一个 iDRAC7 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 iDRAC7 设备对象。用户和 iDRAC7 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 iDRAC7 设备对象）。本示例允许管理员控制特定 iDRAC7 设备上每位用户的权限。

iDRAC7 设备对象是指向 iDRAC7 固件的链接，用于查询 Active Directory 以进行验证和授权。当 iDRAC7 添加到网络后，管理员必须配置 iDRAC7、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 iDRAC7 添加到至少一个关联对象以便用户进行验证。

下图所示为提供验证和授权所需连接的的关联对象。

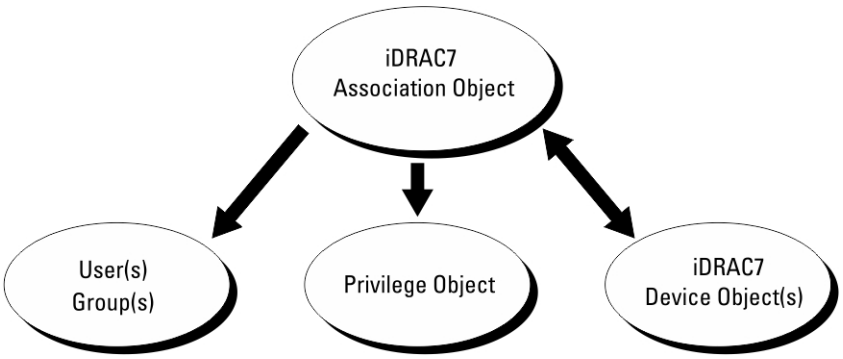


**图 2: Active Directory 对象的典型设置**

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 iDRAC7 验证和授权的每个 iDRAC7 设备必须有一个 iDRAC7 设备对象。

关联对象允许任意数目的用户和/或组以及 iDRAC7 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 iDRAC7 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 iDRAC7 对象与关联对象相关联。Dell 扩展不允许来自其他域的组或 iDRAC7 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。

### 使用扩展架构累积权限

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。

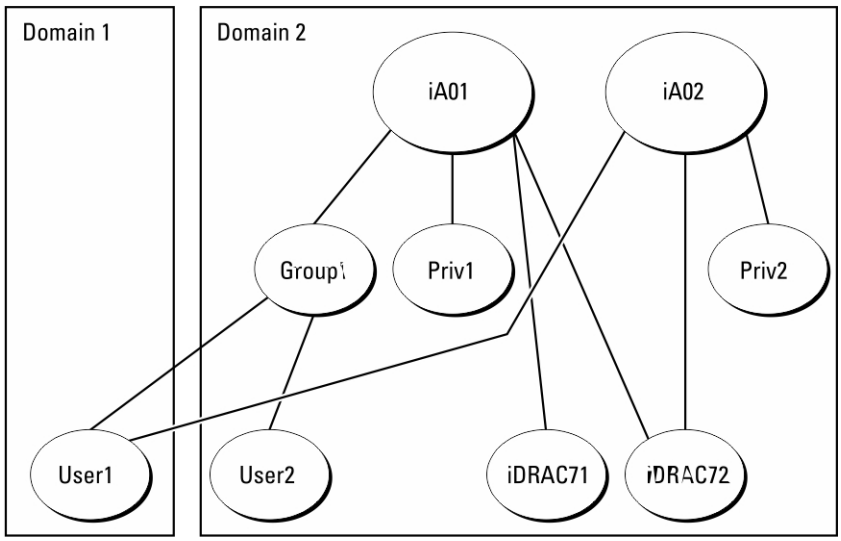


**图 3: 用户权限累积**

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 iDRAC72。

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 iDRAC72 上的 Priv1 和 Priv2 权限。用户 1 仅拥有 iDRAC71 上的 Priv1 权限。用户 2 拥有 iDRAC71 和 iDRAC72 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

配置 Active Directory 以访问 iDRAC7：

1. 扩展 Active Directory 架构。
2. 扩展 Active Directory 用户和计算机管理单元。
3. 将 iDRAC7 用户及其权限添加到 Active Directory。
4. 使用 iDRAC7 Web 界面或 RACADM 配置 iDRAC7 Active Directory 属性。

**相关链接**

扩展架构 Active Directory 概览

安装用于 Microsoft Active Directory 用户和计算机管理单元的 Dell 扩展

将 iDRAC7 用户和权限添加到 Active Directory
使用 iDRAC7 Web 界面以扩展架构配置 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、架构类别以及属性，以及示例权限和关联对象。在您扩展架构之前，确保您对域森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。

可以使用以下方法之一扩展架构：

- Dell Schema Extender 公用程序
- LDIF 脚本文件

如果使用 LDIF 脚本文件，将不会把 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 **Next（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 **Next（下一步）**运行 Dell Schema Extender。
5. 单击 **Finish（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. 15: 添加到活动目录架构的类的类定义**

| 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 |

| 类名称 | 分配的对象标识号 (OID) |
| --- | --- |
| dellProduct | 1.2.840.113556.1.8000.1280.1.1.1.5 |

**表. 16: dellRacDevice 类**

| OID | 1.2.840.113556.1.8000.1280.1.7.1.1 |
| --- | --- |
| 说明 | 代表 Dell iDRAC7 设备。在 Active Directory 中必须将 iDRAC7 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<br>dellRacType |

**表. 17: 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<br>dellPrivilegeMember |

**表. 18: dellRAC4Privileges 类**

| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
| --- | --- |
| 说明 | 为 iDRAC7 定义权限（授权权限） |
| 类的类型 | 辅助类 |
| 超类 | 无 |
| 属性 | dellIsLoginUser<br>dellIsCardConfigAdmin<br>dellIsUserConfigAdmin<br>dellIsLogClearAdmin<br>dellIsServerResetUser<br>dellIsConsoleRedirectUser<br>dellIsVirtualMediaUser<br>dellIsTestAlertUser<br>dellIsDebugCommandAdmin |

**表. 19: 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 |

| | |
|---|---|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.4 |
| 超类 | 用户 |
| 属性 | dellRAC4Privileges |

**表. 20: 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. 21: 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**<br>属于此属性的 dellPrivilege 对象的列表。 | 1.2.840.113556.1.8000.1280.1.1.2.1<br>可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellProductMembers**<br>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。<br>链接 ID: 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2<br>可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellIsLoginUser**<br>如果用户具有设备的登录权限，则为 TRUE。 | 1.2.840.113556.1.8000.1280.1.1.2.3<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsCardConfigAdmin**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsUserConfigAdmin**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsLogClearAdmin**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsServerResetUser**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsConsoleRedirectUser**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsVirtualMediaUser**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsTestAlertUser** | 1.2.840.113556.1.8000.1280.1.1.2.10 | TRUE |

| 属性名称/说明 | 分配的 OID/语法对象标识符 | 单值 |
| --- | --- | --- |
| 如果用户具有设备的测试警报用户权限，则为 TRUE。 | 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | |
| **dellIsDebugCommandAdmin**<br>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<br>布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellSchemaVersion**<br>当前架构版本用于更新架构。 | 1.2.840.113556.1.8000.1280.1.1.2.12<br>忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellRacType**<br>此属性是 delliDRACDevice 对象的当前 RAC 类型以及到 dellAssociationObjectMembers 前进链接的后退链接。 | 1.2.840.113556.1.8000.1280.1.1.2.13<br>忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellAssociationMembers**<br>属于此产品的 dellAssociationObjectMembers 的列表。该属性是 dellProductMembers 链接属性的后退链接。<br>链接 ID：12071 | 1.2.840.113556.1.8000.1280.1.1.2.14<br>可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |

## 安装用于 Microsoft 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 iDRAC7 设备、用户和用户组、iDRAC7 关联和 iDRAC7 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详细信息，请参阅 Microsoft 说明文件。

## 将 iDRAC7 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 iDRAC7 用户和权限。要添加每个对象，请执行以下操作：

- 创建 iDRAC7 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

**相关链接**

将对象添加到关联对象
创建 iDRAC7 设备对象
创建权限对象
创建关联对象

### *创建 iDRAC7 设备对象*

创建 iDRAC7 设备对象：

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 iDRAC7 Web 界面配置 Active Directory 属性时输入的 iDRAC7 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 **Console Root（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. 右键单击创建的权限对象并选择 **Properties（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：

**注:** iDRAC7 关联对象从组派生而来，其范围设置为 Domain Local（本地域）。

1. 在 **Console Root（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）**。
   随即会显示 **New Object （新建对象）**窗口。
3. 输入新对象的名称并选择 **Association Object（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。

**相关链接**

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 **Security（安全）**选项卡中，单击 **Add（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 **OK**（确定）。

### *将对象添加到关联对象*

使用 **Association Object Properties（关联对象属性）**窗口，可以关联用户或用户组、权限对象和 iDRAC7 设备或 iDRAC7 设备组。

可以添加用户组和 iDRAC7 设备组。

**相关链接**

添加用户或用户组
添加权限
添加 iDRAC7 设备或设备组

### *添加用户或用户组*

添加用户或用户组：

1. 右键单击 **Association Object（关联对象）**并选择 **Properties （属性）**。
2. 选择 **Users（用户）**选项卡并单击 **Add（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：

单击 **Privilege Object（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 iDRAC7 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 **OK（确定）**。
3. 单击 **Privilege Object（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 iDRAC7 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 iDRAC7 设备或设备组*

要添加 iDRAC7 设备或设备组：

1. 选择 **Products（产品）**选项卡并单击 **Add（添加）**。
2. 输入 iDRAC7 设备或 iDRAC7 设备组名称并单击 **OK（确定）**。
3. 在 **Properties（属性）**窗口中，单击 **Apply（应用）**，并单击 **OK（确定）**。
4. 单击 **Products（产品）**选项卡以添加一个已连接到可用于定义的用户或用户组的网络的 iDRAC7 设备。您可以将多个 iDRAC7 设备添加到单个关联对象。

## 使用 iDRAC7 Web 界面以扩展架构配置 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*《iDRAC7 联机帮助》*。

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户验证）** → **Directory Services（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. 请单击 **Next（下一步）**。

   将显示 **Active Directory Configuration and Management Step 2 of 4（Active Directory 配置和管理第 2 步，共 4 步）**页面。
5. 指定关于 Active Directory (AD) 服务器和用户帐户的位置信息。同时，还指定在登录流程期间，iDRAC7 必须等待 AD 响应的时长。

**注:** 如果启用了证书验证，指定 Domain Controller 服务器地址和 FQDN。确保 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）**下的 DNS 正确配置。

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 **Extended Schema（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 iDRAC7 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。iDRAC7 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 iDRAC7 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 根 CA 证书>
   ```

**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 证书>
```

2. 如果 iDRAC7 上已启用 DHCP 并且希望使用 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 iDRAC7 上已禁用 DHCP 或希望手动输入 DNS IP 地址，则输入以下 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 iDRAC7 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。
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 iDRAC7 Web 界面测试 Active Directory 设置

测试 Active Directory 设置：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）→ iDRAC Settings（iDRAC 设置）→ User Authentication（用户验证）→ Directory Services（目录服务）→ Microsoft Active Directory**。

   将显示 **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 Enable Certificate Validation（启用证书验证）的情况下测试 Active Directory 设置时，iDRAC7 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 iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 配置通用 LDAP 用户

iDRAC7 提供通用解决方案来支持基于轻量级目录访问协议 (LDAP) 的验证。此功能不需要在目录服务上进行任何架构扩展。

要使 iDRAC7 LDAP 实施通用，组用户应利用不同目录服务之间的共同性然后映射用户-组关系。目录服务特定的操作为架构。例如，他们可能有不同的属性名称用于组、用户以及用户和组之间的链接。这些操作可在 iDRAC7 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)。

**相关链接**

使用 iDRAC7 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 iDRAC7 基于 Web 的界面配置通用 LDAP 目录服务

使用 Web 界面配置通用 LDAP 目录服务：

**注:** 有关各字段的信息，请参阅《*iDRAC7 联机帮助*》。

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户验证）** → **Directory Services（目录服务）** → **Generic LDAP Directory Service（通用 LDAP 目录服务）**。

   **Generic LDAP Configuration and Management（通用 LDAP 配置和管理）**页面显示当前的通用 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. 请单击 **Next（下一步）**。

   将显示 **Generic LDAP Configuration and Management Step 2 of 3（通用 LDAP 配置和管理第 2 步，共 3 步）**页面。
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. 请单击 **Next（下一步）**。

   将显示 **Generic LDAP Configuration and Management Step 3a of 3（通用 LDAP 配置和管理第 3a 步，共 3 步）**页面。
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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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 iDRAC7 Web 界面测试 LDAP 目录服务设置

要测试 LDAP 目录服务设置：

1. 在 iDRAC7 Web 界面中，转到 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户身份验证）** → **Directory Services（目录服务）** → **Generic LDAP Directory Service（通用 LDAP 目录服务）**。

   **Generic LDAP Configuration and Management（通用 LDAP 配置和管理）**页面中显示当前的通用 LDAP 设置。
2. 单击 **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 **Enable Certificate Validation（启用证书验证）** 的情况下测试 LDAP 设置，iDRAC7 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 iDRAC7 无法与 LDAP 服务器通信。

   **注:** 如果启用通用 LDAP，iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

8

# 配置 iDRAC7 进行单一登录或智能卡登录

本节提供配置 iDRAC7 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 和智能卡登录是可获得许可的功能。

iDRAC7 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。

**相关链接**

为 Active Directory 用户配置 iDRAC7 SSO 登录
为本地用户配置 iDRAC7 智能卡登录
为 Active Directory 用户配置 iDRAC7 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 iDRAC7 时间与 Active Directory 域控制器时间同步。如果不同步，iDRAC7 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 iDRAC7 注册为 Active Directory 根域中的计算机。
- 使用 ktpass 工具生成 keytab 文件。
- 要为扩展架构启用单一登录，请确保在 **Delegation**（委派）选项卡上为 keytab 用户选中了 **Trust this user for delegation to any service (Kerberos only)**（对任何服务的委派均信任此用户（仅限 Kerberos））。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 iDRAC7 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。

**相关链接**

配置浏览器以启用 Active Directory SSO
将 iDRAC7 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 iDRAC7 注册为 Active Directory 根域中的计算机

在 Active Directory 根域中注册 iDRAC7：

1. 单击 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Network（网络）**。
   将显示 **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。
   有关各选项的详细信息，请参阅 *iDRAC7 联机帮助*。

## 生成 Kerberos Keytab 文件

要支持 SSO 和智能卡登录验证，iDRAC7 应支持在 Windows Kerberos 网络中启用自身作为 Kerberos 服务的的配置。iDRAC7 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 iDRAC7 DNS 名称相同的名称。

使用 ktpass 工具生成 keytab 文件：

1. 在希望将 iDRAC7 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 DES-CBC-MD5 -ptype
   KRB5_NT_PRINCIPAL -pass [密码] +DesOnly -out c:\krbkeytab
   ```

   加密类型为 DES-CBC-MD5。主体类型为 KRB5_NT_PRINCIPAL。服务主体名称映射至其上的用户帐户的属性应采用“使用 DES”加密类型方可启用此帐户属性。

   **注:** 对 **iDRAC7name** 和 **Service Principal Name（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/iDRAC7name.domainname.com username
   ```

   将生成一个 keytab 文件。

   **注:** 如果发现为之创建 keytab 文件的 iDRAC7 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。

**相关链接**

将 iDRAC7 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 **Advanced**（高级）。
4. 向将用作 SSO 配置一部分的 iDRAC7 实例添加所有要使用的相关域名（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 iDRAC7 名称添加至 network.negotiate-auth.trusted-uris（使用逗号分隔的列表）。
4. 将 iDRAC7 名称添加至 network.negotiate-auth.delegation-uris（使用逗号分隔的列表）。

# 为 Active Directory 用户配置 iDRAC7 SSO 登录

为 Active Directory SSO 登录配置 iDRAC7 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 iDRAC7。

**相关链接**

Active Directory 单一登录或智能卡登录的前提条件
使用 iDRAC7 Web 界面以标准架构配置 Active Directory
使用 RACADM 配置具有标准架构的 Active Directory
使用 iDRAC7 Web 界面以扩展架构配置 Active Directory
使用 RACADM 配置具有扩展架构的 Active Directory

## 使用 Web 界面配置 Active Directory 用户的 iDRAC7 SSO 登录

配置 iDRAC7 以进行 Active Directory SSO 登录：

**注:** 有关各选项的信息，请参阅*《iDRAC7 联机帮助》*。

1. 验证 iDRAC7 DNS 名称是否匹配 iDRAC7 完全限定域名。要实现此操作，在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **Network（网络）**，然后查看 **DNS Domain Name（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 iDRAC7 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 iDRAC7 智能卡登录

配置 iDRAC7 本地用户进行智能卡登录：

1. 将智能卡用户证书和信任的 CA 证书上载到 iDRAC7。
2. 启用智能卡登录。

**相关链接**

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。

**相关链接**

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 iDRAC7 Web 界面中，请转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **User Authentication（用户验证）** → **Local Users（本地用户）**。
   将显示 **Users（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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。

**相关链接**

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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）** → **User Authentication（用户验证）** → **Local Users（本地用户）**。
   将显示 **Users（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 **Apply（应用）**。

### 为使用 RACADM 的智能卡上载受信 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 为 Active Directory 用户配置 iDRAC7 智能卡登录

为 Active Directory 用户配置 iDRAC7 智能卡登录之前，请确保您已完成所需的前提条件。

配置 iDRAC7 进行智能卡登录：

1. 在 iDRAC7 Web 界面中，配置 Active Directory 设置基于标准架构或扩展架构的用户帐户时，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：
   - 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*《iDRAC7 联机帮助》*。

**相关链接**

启用或禁用智能卡登录
获取证书
生成 Kerberos Keytab 文件
使用 iDRAC7 Web 界面以标准架构配置 Active Directory
使用 RACADM 配置具有标准架构的 Active Directory
使用 iDRAC7 Web 界面以扩展架构配置 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

启用或禁用 iDRAC7 的智能卡登录之前，请确保：

- 您已配置 iDRAC7 权限。
- 具有相应证书的 iDRAC7 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。

**相关链接**

获取证书
为 Active Directory 用户配置 iDRAC7 智能卡登录
为本地用户配置 iDRAC7 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 iDRAC7 Web 界面中，转到 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **User Authentication（用户身份验证）** → **Smart Card（智能卡）**。
   随即会显示 **Smart Card（智能卡）**页面。
2. 从 **Configure Smart Card Logon（配置智能卡登录）**下拉菜单中，请选择 **Enabled（启用）**以启用智能卡登录，或者选择 **Enabled With Remote RACADM（使用远程 RACADM 启用）**。否则，选择 **Disabled（禁用）**。
   有关各选项的详细信息，请参阅 *iDRAC7 联机帮助*。
3. 单击 **Apply（应用）**以应用设置。
   使用 iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 使用 iDRAC 设置公用程序启用或禁用智能卡登录

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（返回）**、**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 iDRAC7 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 iDRAC7 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、远程系统日志或 WS 事件发送到配置的目标。
   - 对受管系统执行重新引导、关机或关机后再开机操作。

**相关链接**

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
警报信息 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。

**相关链接**

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 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Server（服务器）** → **Alerts（警报）**。随即会显示 **Alerts**（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 **Apply**（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 **Platform Events（平台事件）**下，选择 **Enabled（启用）**启用警报或事件生成操作。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（返回）**、**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。

**相关链接**

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 iDRAC7 Web 界面过滤警报

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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Alerts（警报）**。将显示 **Alerts（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：
   - Informational（信息）
   - Warning（警告）
   - Critical（严重）
4. 单击 **Apply（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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、远程系统日志和 WS 事件。

**相关链接**

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
   - 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，请使用 **eventfilters** 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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 365 天。值“0”指示禁用事件复现。

**注:** 您必须具有“配置 iDRAC”权限，才能设置警报复现值。

### 使用 iDRAC7 Web 界面设置警报复现事件

设置警报复现值：

1. 在 iDRAC7 Web 界面中，转至**概述 → 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*《iDRAC7 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，请使用 **eventfilters** 子命令。有关更多信息，请参阅*《适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南》*。

## 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。

**相关链接**

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 iDRAC7 Web 界面中，转至 **Overview（概览） → Server（服务器） → Alerts（警报）**。将显示 **Alerts（警报）**页面。
2. 在 **Alerts Results（警报结果）**下，从 **Actions（操作）**下拉式菜单中，为每个事件选择一个操作：
   - Reboot（重新引导）
   - Power Cycle（关机后再开机）
   - Power Off（关闭电源）
   - No Action（无操作）
3. 单击 **Apply（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 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 iDRAC7 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 iDRAC7 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 。

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。

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。

**相关链接**

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。

### 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。
   您最多可以指定八个目标地址。有关选项的更多信息，请参阅 *iDRAC7 Online Help*（iDRAC7 联机帮助）。
3. 输入 iDRAC7 SNMP community string（团体字符串）。
   有关选项的更多信息，请参阅 *iDRAC7 Online Help*（iDRAC7 联机帮助）。

   **注:** Community String （团体字符串）值表示 iDRAC7 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 iDRAC7 团体字符串相同。默认值为 Public。
4. 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）。
5. 单击 **Apply**（应用）。
   警报目标即完成配置。
6. 在 **SNMP Trap Format**（SNMP 陷阱格式）部分，选择要用于发送陷阱目标上陷阱的协议版本 - **SNMP v1** 或 **SNMP v2**，然后单击 **Apply**（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 地址] 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 [名称] 是 SNMP 公共名称。

4. 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 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**（上一步）、**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，确保为邮件服务器配置 iDRAC7 域名，以便从 iDRAC7 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。

**相关链接**

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 **State**（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。有关选项的更多信息，请参阅 *iDRAC7 Online Help*（iDRAC7 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 **Apply**（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 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 iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Alerts（警报）** → **SNMP and E-mail Settings（SNMP 和电子邮件设置）**。
2. 选择 **Enable Authentication（启用验证）**选项，指定用户名和密码（拥有 SMTP 服务器访问权限的用户），然后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)。

   有关选项的详细信息，请参阅*《iDRAC7 联机帮助》*。
3. 单击 **Apply（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 iDRAC7 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。

# 警报信息 ID

下表提供了显示警报的信息 ID 的列表。

**表. 22: 警报信息 ID**

| 信息 ID | 说明 |
|---|---|
| AMP | 安培 |
| 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 |

| 信息 ID | 说明 |
| --- | --- |
| 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 | 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） |
| LIC | 许可 |
| LNK | 链接状态 |
| 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 |

| 信息 ID | 说明 |
| --- | --- |
| SEC | 安全事件 |
| SEL | 系统事件日志 |
| SRD | 软件 RAID |
| SSD | PCIe SSD |
| STOR | 存放时 |
| 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 | Virtual Media（虚拟介质） |
| VRM | 虚拟控制台 |
| WRK | 工作注释 |

10

# 管理日志

iDRAC7 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 iDRAC7 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。

**相关链接**

查看系统事件日志
查看 Lifecycle 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 iDRAC7 Web 界面中查看 SEL，请转至 **Overview（概览）** → **Server（服务器）** → **Logs（日志）**选项卡。

**System Event Log（系统事件日志）**页面显示系统运行状况指示灯、时间戳和每个记录事件的说明。有关更多信息，请参阅*《iDRAC7 联机帮助》*。

单击 **Save As（另存为）**将 **SEL** 保存到您所选的位置。

**注:** 如果正在使用 Internet Explorer 并且在保存时遇到问题，请确保下载 Internet Explorer 的累积安全更新，下载位置是 Microsoft 支持网站 **support.microsoft.com**。

## 使用 RACADM 查看系统事件日志

查看 SEL：

```
racadm getsel <选项>
```

如果没有指定参数，将显示整个日志。

显示 SEL 条目数：

```
racadm getsel -i
```

有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

## 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 **System Event Log**（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. 依次单击 **Back**（上一步）、**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
- Configuration（配置）
- 审核
- 更新
- 工作注释

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。

**相关链接**

筛选 Lifecycle 日志
导出 Lifecycle 日志结果
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 **Overview（概述）** → **Server（服务器）** → **Logs（日志）** → **Lifecycle Log（Lifecycle 日志）**。随即会显示 **Lifecycle Log**（Lifecycle 日志）页面。有关各选项的更多信息，请参阅 *iDRAC7 Online Help*（iDRAC7 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。

### 导出 Lifecycle 日志结果

要导出 Lifecycle 日志结果，请在 **Lifecycle Log（Lifecycle 日志）**页面的 **Log Results（日志结果）**区域中，单击 **Export（导出）**。将显示一个对话框，允许您以 XML 格式将日志条目保存到所选的位置。

### 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 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 添加工作注释

登录到 iDRAC7 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 iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Properties Details（属性）** → **Summary（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*《iDRAC7 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：

- iDRAC7 和远程系统之间有网络连接。
- 远程系统和 iDRAC7 位于同一网络。

## 使用 Web 界面配置远程系统日志

要配置远程系统日志服务器设置：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Logs（日志）** → **Settings（设置）**。
   随即会显示 **Remote Syslog Settings（远程系统日志设置）**屏幕。
2. 启用远程系统日志，指定服务器地址以及端口号。有关各选项的详细信息，请参阅*《iDRAC7 联机帮助》*。
3. 单击 **Apply（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 配置远程系统登录

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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

11

# 监控和管理电源

您可以使用 iDRAC7 监控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。

**相关链接**

监控功率
执行电源控制操作
功率封顶
配置电源设备选项
启用或禁用电源按钮

# 监控功率

iDRAC7 会持续监控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）。

## 使用 Web 界面监控功率

要查看功率监控信息，请在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Power/Thermal（电源/耐热）** → **Power Monitoring（功率监控）**。随即会显示 **Power Monitoring（功率监控）**页面。有关详细信息，请参阅*《iDRAC7 联机帮助》*。

## 使用 RACADM 监测电源

要查看电源监测信息，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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）*。

# 执行电源控制操作

使用 Web 界面或 RACADM，您可以对 iDRAC7 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/support/manuals** 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 界面执行功率控制操作

要执行功率控制操作：

1. 在 iDRAC7 Web 界面中，转至 **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）**。随即会显示 **Power Control（电源控制）** 页面。
2. 选择所需电源操作：
   - Power On Sysytem（打开系统电源）
   - Power Off System（关闭系统电源）
   - NMI (Non-Masking Interrupt)（NMI [非屏蔽中断]）
   - Graceful Shutdown（正常关机）
   - Reset System (warm boot)（重启系统 [热启动]）
   - Power Cycle System (cold boot)（使系统关机后再开机 [冷启动]）
3. 单击 **Apply（应用）**。有关详细信息，请参阅 *《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 功率封顶

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。

## 刀片式服务器中的功率封顶

刀片式服务器启动前，iDRAC7 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，iDRAC7 可能会请求增加最大可能功耗，从而增大功率范围。iDRAC7 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，iDRAC7 会继续请求增加功率。

系统启动并初始化后，iDRAC7 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，刀片仍然会保持启动。

CMC 从低优先级服务器回收任何未用功率，随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，刀片式服务器不会启动。如果分配给刀片的功率足够，iDRAC7 会启动系统电源。

## 查看和配置功率封顶策略

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。

如果设置的功率封顶值低于推荐的最小阈值，iDRAC7 可能无法保持请求的功率封顶值。

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 界面配置电源限额策略

要查看和配置电源策略，请执行以下操作：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Server（服务器）** → **Power/Thermal（电源/耐热）** → **Power Configuration（电源配置）** → **Power Configuration（电源配置）**。随即会显示 **Power Configuration**（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 配置功率限额策略

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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 使用 iDRAC 设置公用程序配置电源限额策略

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 **Enabled**（启用）以启用 **iDRAC Power Limit Policy**（iDRAC 电源限制策略）。否则，选择 **Disabled**（禁用）。
3. 使用建议的设置，或在 **User Defined Limits**（用户定义的限制）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**（上一步）、**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 可以根据负载而进入活动或睡眠模式。

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

配置电源设备选项：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Power/Thermal（电源/耐热）** → **Power Configuration（电源配置）** → **Power Configuration（电源配置）**。将显示 **Power Configuration（电源配置）**页面。
2. 在 **Power Supply Options（电源设备选项）**下，选择所需的选项。有关详细信息，请参阅*《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

### 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 Power Supply（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**（上一步）、**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

# 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：

- 同时支持最多四个虚拟控制台会话。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。

**相关链接**

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. 23: 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:** 如果您将活动的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 iDRAC7 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。

   有关支持浏览器版本的更多信息，请参阅 **dell.com/support/manuals** 上提供的 *Readme*（自述文件）。
2. 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。
3. 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。
4. 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。
5. 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。

**相关链接**

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 Management Station

## 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）*。

**相关链接**

配置虚拟控制台

## 配置 IE 以使用 ActiveX 插件

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

配置 IE 以使用 ActiveX 插件：

1. 清除浏览器的高速缓存。
2. 将 iDRAC7 IP 或主机名添加到 **Trusted Sites（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. 启用浏览器以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 **Tools（工具）** → **Internet Options（Internet 选项）** → **Advanced（高级）**，清除 **Do not save encrypted pages to disk（不将加密的页存盘）**选项，然后选择 **Enable third-party browser extensions（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 **Tools（工具）** → **Internet Options（Internet 选项）** → **Security（安全）**并选择您要运行该应用程序的区域。
6. 单击 **Custom level（自定义级别）**。在 **Security Settings（安全设置）**窗口中，执行以下操作：

   – 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 **Run ActiveX controls and plugins（运行 ActiveX 控件和插件）**选择 **Enable（启用）**或 **Prompt（提示）**。
- 对 **Script ActiveX controls marked safe for scripting（对标记为可安全执行脚本的 ActiveX 控件执行脚本）**选择 **Enable（启用）**或 **Prompt（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:** 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。

**相关链接**

清除浏览器高速缓存
Windows Vista 或更新的 Microsoft 操作系统的其他设置

## Windows Vista 或更新的 Microsoft 操作系统的其他设置

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 Trusted Sites（可信站点）区域选择 **Enable Protected Mode（启用保护模式）**选项。或者，您可以将 iDRAC7 地址添加到 Intranet 区域中的站点。默认情况下，保护模式对 Intranet Zone（Intranet 区域）和 Trusted Sites（可信站点）区域中的站点已关闭。
4. 单击 **Sites（站点）**。
5. 在 **Add this website to the zone（将该网站添加到区域）**字段中，添加 iDRAC7 的地址，然后单击 **Add（添加）**。
6. 单击 **Close（关闭）**，然后单击 **OK（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 Active-X 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 → Tools（工具）→ Manage Add-ons（管理加载项）**，然后单击 **Enable or Disable Add-ons（启用或禁用加载项）**。随即会显示 **Manage Add-ons（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 旧版本

要清除 IE8 中旧版本的 Active-X 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 → Tools（工具）Manage Add-ons（管理加载项），然后**单击 **Enable or Disable Add-ons（启用或禁用加载项）**。随即会显示 **Manage Add-ons（管理加载项）**窗口。
3. 从 **Show（显示）**下拉菜单中选择 **All Add-ons（所有加载项）**。
4. 选择 *Video Viewer（视频查看器）*插件并单击 **More Information（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 旧版本

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 *iDRAC7 Virtual Console Client（iDRAC7 虚拟控制台客户端）*的项目。

## 将 CA 证书导入 Management Station

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。

**相关链接**

将 CA 证书导入到 Java 信任证书存储区
将 CA 证书导入 ActiveX 可信证书库

### 将 CA 证书导入到 Java 信任证书存储区

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 **Security（安全）**选项卡，然后单击 **Certificates（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 **Close（关闭）**，然后单击 **OK（确定）**。**Java Control Panel（Java 控制面板）**窗口将关闭。

### 将 CA 证书导入 ActiveX 可信证书库

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 (CA 证书名称) -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 iDRAC7 Web 界面或 RACADM 命令行界面配置虚拟控制台。

**相关链接**

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

使用 iDRAC7 Web 界面配置虚拟控制台：

1. 转至 **Overview（概览）** → **Server（服务器）** → **Console（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。有关选项的信息，请参阅 *《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

# 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 iDRAC7 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。

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。

**相关链接**

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
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（概述）** → **Server（服务器）** → **Console（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（概述）** → **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. 打开支持的 Web 浏览器并在地址栏中输入以下 URL（小写）：**https://iDRAC7_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 *iDRAC7 Online Help*（iDRAC7 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 Management Station 连接到 iDRAC7 的 DNS 名称或 IP 地址。如果 iDRAC7 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>, 用户： <username>、<fps>`
- 对于刀片式服务器：
  `<DNS name / IPv6 address / IPv4 address>、<Model>、<Slot number>，用户：<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 <Esc> 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 Predictable Pointer Acceleration（可预测指针加速）功能所导致的。要在 iDRAC7 虚拟控制台上正确同步鼠标，必须禁用此功能。要禁用可预测鼠标加速，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）。

为了独占访问管理服务器控制台，您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。

**相关链接**

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 Management Station 和受管系统运行的是 Windows 操作系统，并且已禁用 Pass All Keys（传递所有按键），则当您按下 Windows 按键来打开 **Start（开始）**菜单时，Management Station 和受管系统上的 **Start（开始）**菜单都会打开。但是，如果启用 Pass All Keys（传递所有按键），则只有受管系统上的 **Start（开始）**菜单会打开，Management Station 上的不会打开。
- 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。

### 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：

  单击 Virtual Console（虚拟控制台）页面上的 Help（帮助）可查看在线帮助
- 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。

13

# 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。
- 从虚拟机无法访问 iDRAC7 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。

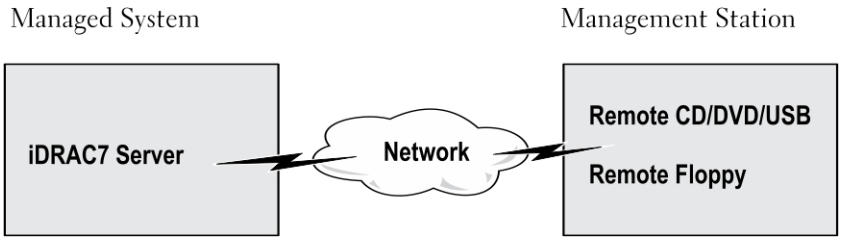


**图 4: 虚拟介质设置**

## 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. 24: 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<br>• CD-ROM<br>• DVD<br>• CD-RW<br>• 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<br>• 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<br>• 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。

**相关链接**

配置 Web 浏览器以使用虚拟控制台

## 使用 iDRAC7 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能重置 iDRAC7。否则，可能发生意外结果，包括丢失数据。**

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** **Attached Media（附加介质）**。
2. 指定所需设置。有关详细信息，请参阅 *《iDRAC7 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 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 Settings（iDRAC 设置）公用程序中，转至 **Virtual Media**（虚拟介质）。

随即会显示 **iDRAC Settings Virtual Media**（iDRAC 设置虚拟介质）页面。

2. 根据需要选择 **Detach**（分离）、**Attach**（附加）或 **Auto attach**（自动附加）。有关这些选项的更多信息，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**（上一步）、**Finish**（完成）和 **Yes**（是）。

虚拟介质设置即完成配置。

## 附加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. 25: 附加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。 |

# 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，一定要配置 Web 浏览器。

**相关链接**

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。
- 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）**。

要使用虚拟控制台访问虚拟介质：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Console（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 上，JAVA 是访问虚拟控制台的默认插件类型。在 Windows 上，要使用 JAVA 访问虚拟控制台，请打开 **.jnlp** 文件以启动虚拟控制台。3 点击
3. 单击 **Virtual Media（虚拟介质）** → **Launch Virtual Media（启动虚拟介质）**。

   随即会显示虚拟介质 **Client View（客户端视图）**窗口，其中列出可用于映射的设备。

   **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。

   。

**相关链接**

配置 Web 浏览器以使用虚拟控制台
配置虚拟介质

## 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Console（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）**。
   此时将显示以下消息：
   虚拟控制台已禁用。是否要继续使用虚拟介质重定向？
3. 单击 **OK（确定）**以连接到虚拟介质。
   随即会显示虚拟介质 **Client View（客户端视图）**窗口，其中列出可用于映射的设备。

   **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。

**相关链接**

配置虚拟介质

## 添加虚拟介质映像

要添加虚拟介质映像，在虚拟介质 **Client View（客户端视图）**窗口中：

- 要添加映像，单击 **Add Image（添加映像）**，然后从 Management Station 或受管系统的 C: 驱动器选择映像文件。
  ISO 或软盘映像将添加到可用设备的列表中。
- 要添加文件夹作为 ISO 和软盘映像，请单击 **Add Folder as Image（添加文件夹作为映像）**。此功能将创建远程文件夹的介质映像并将其作为服务器操作系统的 USB 附加设备安装。
  该介质将连接并信息在 **Client View（客户端视图）**窗口中更新。
  文件夹作为映像添加时，将在使用此功能的 Management Station 桌面上创建一个 **.iso** 文件。如果移动或删除此 **.iso** 文件，则虚拟介质 **Client View（客户端视图）**窗口中此文件夹对应的条目将不起作用。因此，使用 *已添加文件夹*时建议不要移动或删除 **.iso** 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 **.iso** 文件。

## 删除虚拟介质映像

要删除该映像，在虚拟介质 **Client View（客户端视图）**窗口中，选择所需的映射映像，然后单击 **Remove Image（删除映像）**。

选定的映像将从 **Client View（客户端视图）**窗口的设备列表中删除。

## 查看虚拟设备详细信息

要查看虚拟设备详细信息，请在虚拟介质 **Client View（客户端视图）**窗口中，单击 **Details（详细信息）**。将显示 **Details（详细信息）**区域，表明可用的虚拟设备和每个设备的读/写活动。

## 重置 USB

要重置 USB 设置：

1. 在虚拟介质 **Client View（客户端视图）**窗口中，单击 **Details（详细信息）**，然后单击 **USB Reset（USB 重置）**。

   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。
2. 单击 **Yes（是）**。

   USB 随即会重置。

   **注:** 即使您注销 iDRAC7 Web 界面会话，iDRAC7 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 的虚拟驱动器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或将 iDRAC7 IP 地址添加到受信任的站点列表中。

1. 断开所有现有映射的驱动器，然后将其映射到另外的介质源。
2. 在虚拟介质 **Client View（客户端视图）**窗口，添加映像或含有映像的文件夹。
3. 在 **Mapped（已映射）**列下，选择与驱动器相关的具有所需映像的复选框。要将可写入设备映射为只读设备，请在映射前选择该设备的 **Read-only（只读）**选项。

   该设备即映射到受管系统。

**相关链接**

显示映射的正确虚拟驱动器
添加虚拟介质映像

### 显示映射的正确虚拟驱动器

在基于 Linux 的 Management Station 上，虚拟介质 **Client（客户端）**窗口可显示可移动磁盘和软盘，它们不属于 Management Station。要确保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 Management Station 上的操作系统。在开机自检（POST）期间按下 <F2> 或 <F12> 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。

**相关链接**

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. 在虚拟介质 **Client View（客户端视图）**窗口的 **Mapped（已映射）**列下，清除驱动器的复选框。
   虚拟驱动器将从受管系统中取消映射。
2. 单击 **Exit（退出）**终止 **Virtual Media（虚拟介质）**会话。
   虚拟介质 **Client View（客户端视图）**窗口将关闭。

## 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 **OK（确定）**返回 **System BIOS Settings（系统 BIOS 设置）**页面，然后单击 **Finish（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 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Server（服务器）** → **Attached Media（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。

**相关链接**

14

# 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 Management Station 到受管系统上的 iDRAC7 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:** 您只能在 Management Station 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 iDRAC7 固件 **Boot Once（引导一次）**选项时自动终止会话。
- 使用安全套接字层 (SSL) 确保与 iDRAC7 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 iDRAC7，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 [参数] [操作系统_shell_选项]
```

例如，`vmcli -r iDRAC7-IP-address:iDRAC7-SSL-port`

*参数*使 VMCLI 能够连接到指定的服务器，访问 iDRAC7 并映射到指定的虚拟介质。

**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 <iDRAC7-IP-address[:iDRAC7-SSL-port]> -S -u <iDRAC7-用户名> -p <iDRAC7-用户密码> -c {< 设备名称 > | < 映像文件 >}` — 指示 iDRAC7 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 Man（VMCLI 管理）页面*。

**相关链接**

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. 26: VMCLI 命令**

| 虚拟介质 | 命令 |
|---|---|
| 软盘驱动器 | `vmcli -r [RAC IP 或主机名] -u [iDRAC7 用户名] -p [iDRAC7 用户密码] -f [设备名]` |
| 可引导软盘或 USB 闪存盘映像 | `vmcli -r [iDRAC7 IP 地址] [iDRAC7 用户名] -p [iDRAC7 密码] -f [floppy.img]` |
| CD 驱动器使用 -f 选项 | `vmcli -r [iDRAC7 IP 地址] -u [iDRAC7 用户名] -p [iDRAC7 密码] -f [设备名]\|[映像文件]-f [cdrom - dev ]` |
| 可引导 CD/DVD 映像 | `vmcli -r [iDRAC7 IP 地址] -u [iDRAC7 用户名] -p [iDRAC7 密码] -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。

15

# 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 iDRAC7 Web 界面的 **Overview（概览）** → **Server（服务器）** → **vFlash** 下显示以下错误信息：

`SD card not detected. Please insert an SD card of size 256MB or greater.（未检测到 SD 卡。请插入大小为 256MB 或更大的 SD 卡。）`

**注:** 确保仅在 iDRAC7 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信息：*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 Configure iDRAC（配置 iDRAC）权限才能启用或禁用 vFlash 功能和初始化该卡。

**相关链接**

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 iDRAC7 Web 界面或 RACADM 来查看 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash**。随即会显示 **SD Card Properties（SD 卡属性）**页面。有关所显示属性的信息，请参阅 *《iDRAC7 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：

1. 打开系统的 telnet、SSH 或串行控制台并登录。
2. 输入命令：`racadm getconfig -g cfgvFlashSD`
   显示以下只读属性：
   - cfgvFlashSDSize
   - cfgVFlashSDLicensed
   - cfgvFlashSDAvailableSize
   - cfgvFlashSDHealth
   - cfgVFlashSDEnable
   - cfgVFlashSDWriteProtect
   - cfgVFlashSDInitialized

### 使用 iDRAC 设置公用程序查看 vFlash SD 卡属性

要查看 vFlash SD 卡属性，在 **iDRAC Settings Utility（iDRAC 设置公用程序）**中，转至 **vFlash Media（vFlash 介质）**。**iDRAC Settings vFlash Media（iDRAC 设置 vFlash 介质）**页面随即会显示属性。关于所显示属性的详细信息，请参阅 *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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（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：

1. 打开系统的 telnet、SSH 或串行控制台并登录。
2. 输入以下命令：
   - 要启用 vFlash，输入：
     `racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1`
   - 要禁用 vFlash，输入：
     `racadm config -g cfgvFlashsd -o cfgvflashSDEnable 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 **vFlash Media（vFlash 介质）**。

随即会显示 **iDRAC Settings vFlash Media（iDRAC 设置 vFlash 介质）**。

2. 选择 **Enabled（启用）**启用 vFlash 功能或选择 **Disabled（禁用）**禁用 vFlash 功能。
3. 依次单击 **Back（返回）**、**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。

### 使用 Web 界面初始化 vFlash SD 卡

要初始化 vFlash SD 卡：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（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。
   如果附加了任何 vFlash 分区，则初始化操作将失败并显示错误信息。

### 使用 RACADM 初始化 vFlash SD 卡

要使用 RACADM 初始化 vFlash SD 卡：

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 initialize`
   系统随即会删除所有现有分区并重新格式化该卡。

### 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 **vFlash Media（vFlash 介质）**。
   随即会显示 **iDRAC Settings vFlash Media（iDRAC 设置 vFlash 介质）**。
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（返回）**浏览至同一 **iDRAC Settings vFlash Media（iDRAC 设置 vFlash 介质）**页面查看成功信息。
   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:** 如果重置 iDRAC7，上次分区操作的状态会丢失。

# 管理 vFlash 分区

您可以使用 iDRAC7 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
- 附加或分离分区
- 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，iDRAC7 可能会显示以下信息：`vFlash is currently in use by another process. Try again after some time.`（vFlash 当前正被其他进程使用。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。使用映像创建分区时仅支持分区类型 CD。

创建空白分区前，请确保：

- 具有 **Access Virtual Media（访问虚拟介质）**权限。
- 卡已初始化。
- 卡没有受写保护。
- 尚未对卡执行初始化操作。

### 使用 Web 界面创建空白分区

要创建空白 vFlash 分区：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Create Empty Partition（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 **Apply（应用）**。有关这些选项的更多信息，请参阅*《iDRAC7 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：

   - 卡受写保护。
   - 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 **.iso**）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。iDRAC7 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 Hard Disk（硬盘），则 BIOS 无法从此映像引导。
- 映像文件大小小于或等于卡上的可用空间。
- 映像文件大小小于或等于 4 GB，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。

### 通过 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 iDRAC7 Web 界面中，转至 **Overview（概览）→ Server（服务器）→ vFlash → Create From Image（从映像创建）**。

   将显示 **Create Partition from Image File（从映像文件创建分区）**页面。
2. 输入所需信息，然后单击 **Apply（应用）**。有关选项的信息，请参阅 *《iDRAC7 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名既不是 .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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Format（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*《iDRAC7 联机帮助》*。
   将显示警告信息，提示分区中的所有数据将被清除。
3. 单击 **OK**（确定）。
   所选分区将格式化为指定的文件系统类型。如果发生下列情况将显示错误信息：
   - 卡受写保护。
   - 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，在 iDRAC7 Web 界面中转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Manage（管理）**。随即会显示 **Manage Partitions（管理分区）**页面，其中列出可用分区和每个分区的相关信息。有关分区的信息，请参阅*《iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Manage（管理）**。
   将会显示 **Manage Partitions（管理分区）**页面。
2. 在 **Read-Only（只读 ）**列中：
   - 选择分区的复选框，然后单击 **Apply（应用）**更改为 read-only（只读）。
   - 清除分区的复选框，然后单击 **Apply（应用）**更改为 read-write（读写）。
     分区根据所做的选择更改为只读或读写。

   **注:** 如果分区为 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. 输入以下命令：
   - 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
     ```

## 附加或分离分区

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 总线会重置。这会影响使用 vFlash 卡的应用程序，并且会断开 iDRAC7 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 界面附加或分离分区

要附加或分离分区：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Manage（管理）**。
   将会显示 **Manage Partitions（管理分区）**页面。
2. 在 **Attached（已附加）**列中：
   - 选中分区的复选框，然后单击 **Apply（应用）**附加分区。
   - 清除分区的复选框，然后单击 **Apply（应用）**分离分区。
     分区根据所做的选择附加或分离。

### 使用 RACADM 连接或断开分区连接

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. 输入以下命令：
   - 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
     ```

### 已附加分区的操作系统行为

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 iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Manage（管理）**。
   将会显示 **Manage Partitions（管理分区）**页面。
2. 在 **Delete（删除）**列中，单击您要删除的分区的删除图标。
   将显示一条信息，表明此操作会永久删除该分区。
3. 单击 **OK**（确定）。
   分区即被删除。

### 使用 RACADM 删除现有分区

删除分区：

1. 打开系统的 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（iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **vFlash** → **Download（下载）**。
   将会显示 **Download Partition（下载分区）**页面。
2. 从 **Label（卷标）**下拉菜单中，选择要下载的分区，然后单击 **Download（下载）**。

   **注:** 所有现有分区（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 分区设置为第一个引导设备，请参阅设置第一个引导设备。

**注:** 如果 **First Boot Device（第一个引导设备）**下拉菜单中未列出附加的 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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

**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。

16

# 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管理命令的协议。此协议使用 human-oriented（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 倡导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:** 本文假定您熟悉 Systems Management Architecture for Server Hardware（服务器硬件的系统管理架构，SMASH）标准以及 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 iDRAC7 控制器固件开始托管 SMCLP 并支持 Telnet、SSH 和基于串口的界面。iDRAC7 SMCLP 界面基于 DMTF 组织提供的 SMCLP 规范版本 1.0。

**注:** 关于配置文件、扩展和 MOF 的信息在 **delltechcenter.com** 上提供，所有 DMTF 信息在 **dmtf.org/standards/profiles/** 上提供。

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

iDRAC7 SMCLP 让您可以：

- 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 iDRAC7 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 iDRAC7。将显示 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。

# iDRAC7 SMCLP 语法

iDRAC7 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：

<动词> [<选项>] [<目标>] [<属性>]

下表提供了动词及其定义。

**表. 27: 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. 28: SMCLP 目标**

| 目标 | 定义 |
|---|---|
| admin1 | 管理员域 |
| admin1/profiles1 | iDRAC7 中的已注册配置文件 |
| 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 |

| 目标 | 定义 |
| --- | --- |
| 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 |
| 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 |

| 目标 | 定义 |
| --- | --- |
| 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 |
| admin1/system1/sp1/rolesvc3/Role1-3/privilege1 | CLP 角色权限 |

**相关链接**

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 iDRAC7 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/oemdcim_mfaaccount1
```

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**，并且是最具可读性的输出。**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
  ```

  此时将显示以下消息：

  ```
  system1 has been stopped successfully（system1 已成功停止）
  ```

- 要开启服务器：

  ```
  start /system1
  ```

  此时将显示以下消息：

  ```
  system1 has been started successfully（system1 已成功启动）
  ```

- 要重新引导服务器：

reset /system1

此时将显示以下消息：

system1 has been reset successfully（system1 已成功重设）

## 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

  目标：

  Record1
  Record2
  Record3
  Record4
  Record5

  属性：

  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

  命令：

  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

  属性：

  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
```

命令：

```
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`（所有记录成功删除）

## 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`

17

# 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）
- Remote File Share（远程文件共享）

**相关链接**

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 iDRAC7 的 **Configure User（配置用户）**和 **Access Virtual Media（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 iDRAC7。
- 系统能够从映像文件引导。
- 在 iDRAC7 中启用 LAN 上 IPMI。
- 网络共享包含业界标准格式（例如 **.img** 或 **.iso**）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 iDRAC7 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 <iDRAC7 IP 地址或文件> -u <iDRAC7 用户> -p <iDRAC7 用户密码> [ -f {<软盘映像> | <设备名称>} | -c { <设备名称>|<映像文件>} ] [-i <设备 ID>]
   ```

   **注:** vmdeploy 不支持 IPv6，因为 IPv6 不支持 IPMI 工具。

**注:** vmdeploy 脚本处理 `-r` 选项与 `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 iDRAC7 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 iDRAC7 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. 29: vmdeploy 命令参数**

| 参数 | 说明 |
|---|---|
| `<iDRAC7 用户>` | iDRAC7 用户名。该参数必须有以下属性：<br>- 有效用户名<br>- iDRAC7 虚拟介质用户权限<br>如果 iDRAC7 验证失败，将会显示错误信息并且终止命令。 |
| `<iDRAC7 ip \| 文件>` | iDRAC7 IP 地址或包含 iDRAC7 IP 地址的文件。 |
| `<iDRAC7 用户密码>`或 `<iDRAC7 密码>` | iDRAC7 用户的密码。<br>如果 iDRAC7 验证失败，将会显示错误信息并且终止命令。 |
| `-c {<设备名称> \| <映像文件>}` | 指向操作系统安装 CD 或 DVD 的 ISO9660 映像的路径。 |
| `<软盘设备>` | 指向包含操作系统安装 CD、DVD 或软盘的设备的路径。 |
| `<软盘映像>` | 指向有效软盘映像的路径。 |
| `<设备 ID>` | 引导一次的设备的 ID。 |

**相关链接**

配置虚拟介质
配置 iDRAC7

# 使用远程文件共享部署操作系统

使用 Remote File Share（远程文件共享）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。
- 为用户启用 iDRAC7 的 **Configure User（配置用户）**和 **Access Virtual Media（访问虚拟介质）**权限。
- Remote File Share（远程文件共享）已启用。
- 网络共享包含业界标准格式（例如 **.img** 或 **.iso**）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。

使用远程文件共享部署操作系统：

1. 使用 NFS 或 CIFS 将 ISO 或 IMG 映像文件安装到受管系统。
2. 转至 **Overview（概览）** → **Setup（设置）** → **First Boot Device（第一引导设备）**。
3. 在 **First Boot Device（第一引导设备）**下拉式列表中将引导顺序设置为 **Remote File Share（远程文件共享）**。
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 **Apply（应用）**。

6. 重新引导受管系统并按照屏幕上的说明完成部署。

**相关链接**

配置虚拟介质
设置第一引导设备
管理远程文件共享

## 管理远程文件共享

使用 Remote File Share（远程文件共享，RFS）功能，您可以设置位于网络共享上的 ISO 或 IMG 映像文件，并使用 NFS 或 CIFS 将其作为 CD 或 DVD 进行加载，从而将其作为虚拟驱动器供受管服务器的操作系统使用。

**注:** CIFS 和 NFS 都支持 IPv4 地址。CIFS 仅支持 IPv6 地址。

远程文件共享仅支持 **.img** 和 **.iso** 映像文件。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加载 RFS。

**注:** 如果 ESXi 在受管系统上运行，并且如果您使用远程文件共享加载软盘映像 (**.img**)，则 ESXi 操作系统不能使用连接的软盘映像。

RFS 的连接状态在 iDRAC7 日志中提供。一旦连接，即使您从 iDRAC7 注销，加载 RFS 的虚拟驱动器也不会断开连接。如果重置 iDRAC7 或者网络连接丢失，RFS 连接会关闭。在 CMC 和 iDRAC7 中也可以通过 Web 界面和命令行选项来关闭 RFS 连接。CMC 的 RFS 连接始终会覆盖现有 iDRAC7 中的 RFS 加载。

**注:** iDRAC7 vFlash 功能与 RFS 没有关联。

## 使用 Web 界面配置远程文件共享

启用远程文件共享：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Server（服务器）** → **Attached Media（已附加介质）**。
   将显示 **Attached Media**（已附加介质）页面。
2. 在 **Remote File Share**（远程文件共享）下，选择附加或自动附加并指定映像文件路径、域名、用户名和密码。有关这些字段的信息，请参阅 *iDRAC7 Online Help*（iDRAC7 联机帮助）。
3. 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加载命令。命令的语法如下：

   ```
   mount /dev/OS_specific_device / user_defined_mount_point
   ```

   其中，`user_defined_mount_point` 是您选择的与任何加载命令类似的用于加载的任何目录。

   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 中并非自动加载。

## 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 <选项>
```

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>`：映像在网络共享上的位置；使用双引号将位置括起来
- `-s`：显示当前状态

**注:** 用户名、密码和映像位置可使用所有字符（包括字母数字和特殊字符），但以下字符除外：’（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。
- 网络共享包含业界标准格式（例如 **.img** 或 **.iso**）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. 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 iDRAC7 Web 界面将引导顺序设置为从 **Virtual Floppy（虚拟软盘）**或 **Virtual CD/DVD/ISO（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。

**相关链接**

配置虚拟介质
设置第一引导设备
配置 iDRAC7

## 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。

**相关链接**

关于 IDSDM
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 **Internal USB Port（内部 USB 端口）**设置为 **On（开）**。如果设置为 **Off（关）**，则 IDSDM 无法用作引导设备。
4. 如果不需要冗余（单 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 **Disabled（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 iDRAC7 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，并在前面板上显示，如果启用警报，则会生成 PET 警报。

**相关链接**

查看传感器信息

18

# 使用 iDRAC7 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

**相关链接**

使用诊断控制台
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

## 使用诊断控制台

iDRAC7 提供了标准的网络诊断工具集合，这与 Microsoft Windows 或基于 Linux 的系统中包含的工具类似。使用 iDRAC7 Web 界面，您可以访问网络调试工具。

要访问诊断控制台：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Troubleshooting（故障排除）** → **Diagnostics（诊断）**。
2. 在 **Command（命令）**文本框中，输入命令，然后单击 **Submit（提交）**。有关各命令的详细信息，请参阅 *《iDRAC7 联机帮助》*。

   随即结果会显示在同一页面上。

## 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。

iDRAC7 记录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。如果重置 iDRAC7，引导捕获视频将不再可用，因为该视频存储在 RAM 中，所以已删除。

**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 **Boot Capture（引导捕获视频）**屏幕，请单击 **Overview（概览）** → **Server（服务器）** → **Troubleshooting（故障排除）** → **Video Capture（视频捕获）**。

**Video Capture（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*《iDRAC7 联机帮助》*。

# 查看日志

您可以查看系统事件日志 (SEL) 和 Lifecycle 日志。有关详细信息，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 iDRAC7 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 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Server（服务器）** → **Troubleshooting（故障排除）** → **Last Crash Screen（上次崩溃屏幕）**。

   **Last Crash Screen**（上次崩溃屏幕）页面显示受管系统上最新保存的崩溃屏幕。

   单击 **Clear（清除）**可删除上次崩溃屏幕。

**相关链接**

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
- 可移动闪存介质
- 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，在 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Hardware（硬件）** → **Front Panel（前面板）**。将显示 **Front Panel**（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/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

**相关链接**

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 iDRAC7 Web 界面中，转至 **Overview（概述）** → **Hardware（硬件）** → **Front Panel（前面板）**。**Live Front Panel Feed**（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，可以使用 **getled** 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上提供的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

**相关链接**

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

iDRAC7 和 CMC（适用于刀片服务器）Web 界面将显示下列各项的状态信息：

- 电池
- 风扇
- 侵入
- 电源设备
- 可移动闪存介质
- 温度
- 电压
- CPU

在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **System Summary（系统摘要）** → **Server Health（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。

# 在服务器状态屏幕上检查错误信息

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 iDRAC7

您可以执行软/硬 iDRAC7 重启动而无需关闭服务器：

- 硬重启动 — 在服务器中，按住 LED 按钮 15 秒。
- 软重启动 — 使用 iDRAC7 Web 界面或 RACADM。

## 使用 iDRAC7 Web 界面重设 iDRAC7

要重新启动 iDRAC7，请在 iDRAC7 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 iDRAC7

要重新启动 iDRAC7，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 iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 参考指南）。

# 将 iDRAC7 重设为出厂默认设置

您可以使用 iDRAC 设置公用程序或 iDRAC7 Web 界面将 iDRAC7 重设为出厂默认设置。

## 使用 iDRAC7 Web 界面将 iDRAC7 重设为出厂默认设置

要使用 iDRAC7 Web 界面将 iDRAC7 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）。
   iDRAC7 重新引导并恢复为出厂默认值。iDRAC7 IP 重设并且无法访问。您可以使用前面板或 BIOS 配置 IP。

## 使用 iDRAC 设置公共程序将 iDRAC7 重设为出厂默认设置

要使用 iDRAC 设置公用程序将 iDRAC7 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 **Yes**（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。

19

# 常见问题解答

本部分列出了下列常见问题：



## System Event Log（系统事件日志）

**通过 Internet Explorer 使用 iDRAC7 Web 界面时，为什么 SEL 没有使用 Save As（另存为）选项保存？**

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 iDRAC7 设备位于本地内部网中，则选择 **Local Intranet（本地 Intranet）**，然后单击 **Custom level...（自定义级别...）**。
2. 在 **Security Settings（安全设置）**窗口中 **Downloads（下载）**下，确保启用了以下选项：
   - 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 iDRAC7 的计算机的安全，请不要在 Miscellaneous（其他）下启用 Launching applications and unsafe files（启动应用程序和不安全文件）选项。**

## 网络安全

**访问 iDRAC7 Web 界面时，系统会显示一条安全警告来声明证书认证机构 (CA) 颁发的 SSL 证书不可信。**

iDRAC7 包含一个默认的 iDRAC7 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 iDRAC7 服务器证书。

**为什么 DNS 服务器不注册 iDRAC7？**

某些 DNS 服务器注册包含多达 31 个字符的 iDRAC7 名称。

**访问 iDRAC7 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 iDRAC7 主机名不匹配。**

iDRAC7 包含一个默认的 iDRAC7 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 iDRAC7 的默认证书与 iDRAC7 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 iDRAC7 主机名的 iDRAC7 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 iDRAC7 IP 地址（如果证书颁发给 IP）或注册的 DNS iDRAC7 名称（如果证书颁发给 iDRAC7 注册的名称）匹配。

要确保 CSR 与注册的 DNS iDRAC7 名称匹配：

1. 在 iDRAC7 Web 界面中，转至 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **Network（网络）**。随即会显示 **Network（网络）**页面。
2. 在 **Common Settings（常见设置）**部分：
   - 选择 **Register iDRAC on DNS（向 DNS 注册 iDRAC）**选项。
   - 在 **DNS iDRAC Name（DNS iDRAC 名称）**字段中，输入 iDRAC7 名称。
3. 单击 **Apply（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 iDRAC7 用户帐户，请使用本地凭据登录到 iDRAC7。登录后，请确保：
  - 在 **Active Directory Configuration and Management**（Active Directory 配置和管理）页面上已选中 **Enable Active Directory**（启用 Active Directory）选项。
  - **iDRAC7 Networking configuration**（iDRAC7 网络配置）页面上的 DNS 设置正确。
  - 如果已启用证书验证，则会将正确的 Active Directory 根 CA 证书上载到 iDRAC7。
  - 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。
- 检查域控制器 SSL 证书以确保 iDRAC7 时间在证书的有效期内。

**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 iDRAC7.
Please also check if the iDRAC7 date is within the valid period of the
certificates and if the Domain Controller Address configured in iDRAC7 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：：请检查是否已经正确的证书认证机构 (CA) 证书上载到 iDRAC7。请同时检查 iDRAC7 日期是否在证书的有效期内，并且在 iDRAC7 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 iDRAC7 与目录服务器建立 SSL 连接时，iDRAC7 使用上载的 CA 证书验证目录服务器证书。证书验证失败最常见的原因包括：

- iDRAC7 日期超出服务器证书或 CA 证书的有效期。检查 iDRAC7 时间和证书的有效期。

- 在 iDRAC7 中配置的域控制器地址与目录服务器证书的 Subject（主题）或 Subject Alternative Name（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 iDRAC7 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 Subject（主题）或 Subject Alternative Name（主题备用名称）字段中使用 IP 地址，从而与在 iDRAC7 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 iDRAC7 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？**

iDRAC7 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 Global Controller Address（全局控制器地址），iDRAC7 会继续查询 Global Catalog（全局编录）。如果从全局编录中检索到附加权限，这些权限会累积。

**iDRAC7 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，iDRAC7 仅执行 LDAP CONNECT（LDAP 连接）以隔离该问题，而不是在非安全连接上执行 LDAP BIND（LDAP 绑定）。

**为什么 iDRAC7 默认启用证书验证？**

iDRAC7 强制实行强大的安全机制来确保 iDRAC7 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。

**iDRAC7 支持 NetBIOS 名称吗？**

此版本不支持。

**为什么使用 Active Directory 单一登录或智能卡登录需要四分钟才能登录到 iDRAC7？**

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，iDRAC7 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 iDRAC7 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 更新到 iDRAC7。

现在可以使用 SSO 登录 iDRAC7。

**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 **Local Computer Settings（本地计算机设置）** → **Windows Settings（Windows 设置）** → **Security Settings（安全设置）** → **Local Policies（本地策略）** → **Security Options（安全选项）**。
4. 右键单击 **Network Security: Configure encryption types allowed for kerberos（网络安全：配置 Kerberos 允许的加密类型）**并选择 **Properties（属性）**。
5. 启用所有选项。
6. 单击 **OK（确定）**。现在可以使用 SSO 登录 iDRAC7。

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 **Registry Editor（注册表编辑器）**窗口。现在可以使用 SSO 登录 iDRAC7。

**如果为 iDRAC7 启用了 SSO 并且使用 Internet Explorer 登录 iDRAC7，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 iDRAC7 IP 地址列于 **Tools（工具）** → **Internet Options（Internet 选项）** → **Security（安全）** → **Trusted sites（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 **Cancel（取消）**并继续。

# 智能卡登录

**使用 Active Directory 智能卡登录功能登录 iDRAC7 需要最多四分钟时间。**

正常的 Active Directory 智能卡登录通常不超过 10 秒，但如果您在 **Network（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。iDRAC7 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

**即使您登出 iDRAC7 Web 界面，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？**

是。

**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，iDRAC7 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。

**iDRAC7 用户打开或关闭本地服务器视频需要什么权限？**

任何具有 iDRAC7 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 -p 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 iDRAC7 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 **Tools（工具）** → **Session Options（会话选项）** → **Mouse（鼠标）**选项卡。在 **Mouse Acceleration（鼠标加速）**下，选择 **Linux**。
- 在 **Tools（工具）**菜单下，选择 **Single Cursor（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 iDRAC7 虚拟控制台客户端上的 **Single Cursor（单一光标）**选项（位于 iDRAC7 虚拟控制台菜单的 **Tools（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 iDRAC7 访问时，Management Station 上的 Num Lock 指示灯不需要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 Management Station 上的 Num Lock 状态无关。

**为什么从本地主机建立虚拟控制台会话时显示多个 Session Viewer 窗口？**

您正在从本地系统配置虚拟控制台。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。

**Management Station 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 Virtual Console Viewer 窗口有时会显示“No Signal”（无信号）的信息？**

显示该消息是因为 iDRAC7 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 iDRAC7 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，可能会导致超出范围。通常情况下，物理限制（例如视频内存大小或带宽）决定了参数的最大范围。

**从 iDRAC7 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？**

iDRAC7 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 iDRAC7 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 **Sites（站点）**并输入 iDRAC7 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。iDRAC7 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 iDRAC7 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，行为保持不变。要修复这个问题，请在 Configuration（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 **Mouse Mode（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 iDRAC7 Web 界面时，为什么 GUI 会话会超时？**

从 CMC Web 界面启动 iDRAC7 的虚拟控制台时，将打开弹出窗口，提示您启动虚拟控制台。弹出窗口将在虚拟控制台打开后不久关闭。

启动 management station 上同一 iDRAC7 系统的 GUI 和虚拟控制台时，如果在关闭弹出窗口之前启动 GUI，会发生 iDRAC7 GUI 会话超时。如果在关闭包含虚拟控制台的弹出窗口之后，再从 CMC Web 界面启动 iDRAC7 GUI，将不会出现该问题。

**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** 键同时按下 **Print Screen** 键，然后松开。要在使用 Internet Explorer 时，通过 iDRAC7 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，iDRAC7 固件会断开连接，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 Virtual Media（虚拟介质）配置设置在 iDRAC7 Web 界面或通过本地 RACADM 命令更改，当配置更改应用后，任何所连介质都会断开连接。

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 iDRAC7 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？**

iDRAC7 允许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？**

在 **support.dell.com** 搜索 Dell Boot Utility

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。

**为什么使用 iDRAC7 Web 界面执行远程固件更新之后，连接了服务器的虚拟驱动器会被删除？**

固件更新会导致 iDRAC7 重置，断开远程连接并卸载虚拟驱动器。iDRAC7 完成重置后，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。无论任何虚拟介质或 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，请不要附加或分离一个或多个虚拟介质或 vFlash 设备。推荐您在使用之前，首先连接所有所需的 USB 设备。

**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 iDRAC7 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 iDRAC7 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，iDRAC7 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。

要阻止生成 SNMP 验证错误，您必须输入代理程序接受的团体名称。由于 iDRAC7 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都没有显示，并且 OpenManage Storage Management (OpenManage 存储管理) 显示的存储设备比 iDRAC7 多，为什么？**

iDRAC7 仅显示 Comprehensive Embedded Management（综合嵌入式管理，CEM）支持的设备的信息。

# RACADM

**执行 iDRAC7（使用 racadm racreset 命令）重置后，如果发出任何命令，则会显示以下消息。这表示什么意思？**

`ERROR: Unable to connect to RAC at specified IP address`（错误：无法连接到指定 IP 地址的 RAC）

此消息表示您必须等到 iDRAC7 完成重置后，才能发出其他命令。

**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 iDRAC7 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 iDRAC7。**

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 <文件名>
```

其中，文件名是 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？**

重置 iDRAC7 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。

以下情况下重置 iDRAC7 Web 服务器：

- 使用 iDRAC7 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`（配置文件）进行更改时）。
- 使用 racresetcfg 命令时。
- 重置 iDRAC7 时。
- 上载新的 SSL 服务器证书时。

**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 **Chassis（机箱）** → **Servers（服务器）** → **Setup（设置）** → **Deploy（部署）**。在显示的表格中查看服务器的 IP 地址。

**使用虚拟控制台**：开机自检（POST）期间重新启动服务器查看 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。参阅 CMC RACADM 子命令完整列表的*《适用于 iDRAC7 和 CMC 的 RACADM 命令行参考手册》*。

**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 iDRAC7 Web 界面中**：单击 **Overview（概览）** → **iDRAC Settings（iDRAC 设置）** → **CMC**。**CMC Summary（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。参阅 CMC RACADM 子命令完整列表的*《适用于 iDRAC7 和 CMC 的 RACADM 命令行参考手册》*

```
$ 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 iDRAC7 Web 界面中**：转至 **Overview（概览）** → **Server（服务器）** → **Properties（属性）** → **Summary（摘要）**。**System Summary（系统摘要）**页面随即会显示 iDRAC7 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 显示器导航按钮查看 iDRAC7 IP 地址。转至 **Setup View（设置视图）** → **View（视图）** → **iDRAC IP** → **IPv4** 或 **IPv6** → **IP**。

**在 OpenManage Server Administrator（OpenManage 服务器管理员）中**：在 Server Administrator Web（服务器管理员 Web）界面中，转至 **Modular Enclosure（模块化机箱）** → **System/Server Module（系统/服务器模块）** → **Main System Chassis/Main System（主系统机箱/主系统）Remote Access（远程访问）**。

**iDRAC7 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，iDRAC7 需要多达两分钟进行初始化。
- 检查 CMC 功率预算，机箱功率预算可能已超出。

**如何检索 iDRAC7 管理的用户名和密码？**

您必须将 iDRAC7 恢复到默认设置。有关详细信息，请参阅将 iDRAC7 恢复为出厂默认设置。

**如何更改机箱中系统的插槽名称？**

1. 登录 CMC Web 界面并转至 **Chassis（机箱）** → **Servers（服务器）** → **Setup（设置）** 。
2. 在服务器的行中输入插槽的新名称并单击 **Apply（应用）**。

**刀片式服务器上的 iDRAC7 在启动期间未响应。**

卸下并重新插入服务器。

检查 CMC Web 界面以查看 iDRAC7 是否显示为可升级组件。如果是，则遵循使用 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 iDRAC7 Web 界面参阅 iDRAC7 日志中的错误消息或服务器 LCD 中的错误消息。

20

# 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 iDRAC7 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
- iDRAC7 上的警报已启用

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：转至 Sever（服务器），访问 LCD 显示器，记下 IP 地址或主机名，然后使用管理台中的 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。

## 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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **System Summary（系统摘要）**，查看系统信息，访问该页面上的各链接查看系统运行状况。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。

## 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的操作。
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 iDRAC7 Web 界面中，转至 **Overview（概览）** → **Server（服务器）** → **Logs（日志）**查看 SEL 和 **Overview（概览）** → **Server（服务器）** → **Logs（日志）** → **Lifecycle Log（Lifecycle 日志）**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。

# 用于更新 iDRAC 固件的界面

使用以下界面更新 iDRAC 固件：

- iDRAC7 Web 界面
- RACADM CLI（iDRAC7 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（Dell 远程访问配置工具，DRACT）

# 执行正常关机

要执行正常关机，在 iDRAC7 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）**。
- **Overview（概览）** → **Server（服务器）** → **Power/Thermal（电源/耐热）** → **Power Monitoring（电源监控）**。在 **Power Control（电源控制）**下拉菜单中，选择 **Graceful Shutdown（正常关机）**，然后单击 **Apply（应用）**。

有关更多信息，请参阅*《iDRAC7 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加载 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 iDRAC7 Web 界面启动虚拟控制台：
   - 转至 **Overview（概览）** → **Server（服务器）** → **Console（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。

# 使用附带的虚拟介质和远程文件共享安装 Bare Metal OS

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

目前，一个机架上安装两台服务器。要增加两个额外的服务器，需要确定在机架上留下多少空间。

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。