Integrated Dell Remote Access Controller 6 (iDRAC6)

版本 1.95

用户指南

注和小心

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”表示如果不遵循说明，就有可能损坏硬件或导致数据丢失。

2013 - 03

目录

1

iDRAC6 概览

Integrated Dell Remote Access Controller6 (iDRAC6) 是一种系统管理硬件和软件解决方案，用于为 Dell PowerEdge 系统提供远程管理功能、崩溃系统恢复和电源控制功能。

iDRAC6 在远程监测 / 控制系统中使用集成的片上系统微处理器。iDRAC6 与受管 PowerEdge 服务器共存于系统板上。服务器操作系统负责执行应用程序； iDRAC6 负责监测和管理操作系统之外的服务器环境和状态。

可以配置 iDRAC6 向您发送电子邮件或简单网络管理协议 (SNMP) 陷阱警报来通知警告或错误。为帮助诊断系统崩溃的可能原因， iDRAC6 可以在检测到系统崩溃时记录事件数据并捕获屏幕图像。

默认情况下，启用的 iDRAC6 网络界面使用静态 IP 地址 192.168.0.120。必须对其进行配置，才能访问 iDRAC6。当在网络上配置 iDRAC6 后，可以通过 iDRAC6 Web 界面、 Telnet 或 Secure Shell (SSH) 和支持的网络管理协议 （如智能平台管理接口 [IPMI]）以分配的 IP 地址对其进行访问。

此版本有何新功能

- 支持 DIMM 配置和 PCI 卡 （请参阅 《发行说明》了解详情。）
- 支持 Internet Explorer 10 浏览器。
- 默认的证书签名请求 (CSR) 密钥长度已更改为 2048 位。

iDRAC6 Express 管理功能

iDRAC6 Express 提供以下管理功能：

- 提供动态域名系统 (DDNS) 注册。
- 使用 Web 界面和服务器管理命令行协议 (SM-CLP) 命令行通过串行、Telnet 或 SSH 连接进行远程系统管理和监控。
- 支持 Microsoft Active Directory 验证 — 使用扩展架构或标准架构将 iDRAC6 用户 ID 和密码集中在 Active Directory 中。
- 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。
- 提供对系统信息和组件状况的访问以进行监控。

- 提供对系统事件日志、iDRAC6 日志和崩溃或无响应系统的上次崩溃屏幕的访问 （与操作系统状态无关）。
- 提供选项通过 GUI 或 CLI 将工作注释添加到 Lifecycle Controller 日志。
- 使您能够从 Dell OpenManage Server Administrator 或 Dell OpenManage IT Assistant 启动 iDRAC6 Web 界面。
- 通过电子邮件或 SNMP 陷阱警告潜在受管节点问题。
- 提供远程电源管理功能，例如，从管理控制台关机和重设。
- 提供智能平台管理接口 (IPMI) 支持。
- 通过 Web 界面提供安全远程系统管理。
- 通过密码级安全管理阻止对远程系统的未授权访问。
- 通过基于角色的授权为不同的系统管理任务提供可分配权限。
- 增加 IPv6 支持，例如：允许使用 IPv6 地址访问 iDRAC6 Web 界面、指定 iDRAC NIC 的 IPv6 地址、指定目标号码以配置 IPv6 SNMP 警报目标。
- 通过使用 Web Services for Management (WS-MAN) 协议提供网络可访问管理。
- 增加服务器管理命令行协议 (SM-CLP) 支持，这提供了系统管理 CLI 实施的标准。
- 可以从通过固件回滚和恢复选择的固件映像引导 （或回滚到该固件映像）。

有关 iDRAC6 Express 的详情，请参阅 **dell.com/support/manuals** 上的《硬件用户手册》。

iDRAC6 Enterprise 和 vFlash 介质

iDRAC6 Enterprise （带有 vFlash 介质）增加了对 RACADM、虚拟控制台、虚拟介质功能、专用 NIC 和 vFlash （带可选 Dell vFlash 介质卡）的支持。 vFlash 允许在 vFlash 介质上保存应急引导映像和诊断工具。有关 iDRAC6 Enterprise 和 vFlash 介质的详情，请参阅 **dell.com/support/manuals** 上的 《硬件用户手册》。

表 1-1 列出了 BMC、iDRAC6 Express、iDRAC6 Enterprise 和 vFlash 介质的可用功能。

表 1-1. iDRAC6 功能列表

部件	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise（支持 vFlash）
接口和标准支持				
IPMI 2.0	✓	✓	✓	✓
基于 Web 的 GUI	✗	✓	✓	✓
SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP（仅限于 SSH）	✗	✓	✓	✓
RACADM 命令行（SSH 和本地）	✗	✓	✓	✓
RACADM 命令行（远程）	✗	✗	✓	✓
连接性				
共享 / 故障转移网络模式	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN 标记	✓	✓	✓	✓
IPv6	✗	✓	✓	✓
动态 DNS	✗	✓	✓	✓
专用 NIC	✗	✗	✓	✓
安全和验证				
基于角色的权限	✓	✓	✓	✓
本地用户	✓	✓	✓	✓
SSL 加密	✓	✓	✓	✓

表 1-1. iDRAC6 功能列表 *（续）*

部件	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise（支持 vFlash）
Active Directory	✗	✓	✓	✓
通用 LDAP 支持	✗	✓	✓	✓
双重验证 [1]	✗	✓	✓	✓
单一登录	✗	✓	✓	✓
PK 验证（适用于 SSH）	✗	✗	✓	✓
远程管理和补救				
远程固件更新	✓[2]	✓	✓	✓
服务器功率控制	✓[2]	✓	✓	✓
LAN 上串行（有代理）	✓	✓	✓	✓
LAN 上串行（无代理）	✓	✓	✓	✓
功率上限	✓	✓	✓	✓
上次崩溃屏幕捕获	✗	✓	✓	✓
引导捕获	✗	✓	✓	✓
虚拟介质 [3]	✗	✗	✓	✓
虚拟控制台 [3]	✗	✗	✓	✓
虚拟控制台共享 [3]	✗	✗	✓	✓
远程虚拟控制台启动	✗	✗	✓	✓
vFlash	✗	✗	✗	✓

表 1-1. iDRAC6 功能列表 *（续）*

部件	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise（支持 vFlash）
监测				
传感器监测和警报	✓[2]	✓	✓	✓
实时功率监测	✓	✓	✓	✓
实时功率图表	✗	✓	✓	✓
历史功率计数器	✗	✓	✓	✓
日志记录				
系统事件日志 (SEL)	✓	✓	✓	✓
RAC 日志	✗	✓	✓	✓
远程系统日志	✗	✗	✓	✓
Lifecycle Controller				
Unified Server Configurator	✓[4]	✓	✓	✓
远程服务（通过 WS-MAN）	✗	✓	✓	✓
部件更换	✗	✗	✗	✓

[1] 双重验证需要 Internet Explorer。

[2] 功能只能通过 IPMI 使用，而不是通过 Web GUI 使用。

[3] 虚拟控制台和虚拟介质通过 Java 和 Active-X 插件可用。

[4] 通过 BMC 可用的 Unified Server Configurator 仅限于操作系统安装和诊断。

✓ = 支持；✗ = 不支持

iDRAC6 提供以下安全功能：

- 单一登录、双重验证和公共密钥验证。
- 通过 Active Directory （可选）、 LDAP 验证 （可选）或硬件存储的用户 ID 和密码对用户进行验证。
- 基于角色的权限，使管理员能够为每位用户配置特定权限。
- 通过基于 Web 界面或 SM-CLP 进行用户 ID 和密码配置。
- SM-CLP 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。
- 通过 Web 界面或 SM-CLP 进行会话超时配置 （以秒为单位）。
- 可配置 IP 端口 （适用时）。

  注：Telnet 不支持 SSL 加密技术。
- SSH 使用加密传输层实现更高的安全性。
- 每个 IP 地址的登录失败限制，在超过此限制时阻塞来自该 IP 地址的登录。
- 能够限制连接到 iDRAC6 的客户端的 IP 地址范围。

支持的平台

有关最新的受支持平台，请参阅 **dell.com/support/manuals** 上的 iDRAC6 自述文件和 《Dell 系统软件支持值表》。

支持的操作系统

有关最新信息，请参阅 **dell.com/support/manuals** 上的 iDRAC6 自述文件和 《Dell 系统软件支持值表》。

支持的 Web 浏览器

有关最新信息，请参阅 **dell.com/support/manuals** 上的 *iDRAC6 1.95 发行说明*和 《Dell 系统软件支持值表》。

注：由于存在严重的安全缺陷，已停止对 SSL 2.0 的支持。浏览器必须配置为启用 SSL 3.0 以便能够正常工作。不支持 Internet Explorer 6.0。

支持的远程访问连接

表 1-2 列出连接功能。

表 1-2. 支持的远程访问连接

连接	功能
iDRAC6 NIC	• 10 Mbps/100 Mbps 以太网 • DHCP 支持 • SNMP 陷阱和电子邮件事件通知 • 支持 SM-CLP （Telnet、 SSH 和 RACADM）命令 Shell，进行诸如 iDRAC6 配置、系统引导、重设、开机和关机命令等操作 • 支持 IPMI 公用程序，比如 IPMItool 和 ipmish

iDRAC6 端口

表 1-3 列出 iDRAC6 侦听连接的端口。表 1-4 标识 iDRAC6 用作客户端的端口。当打开防火墙以远程访问 iDRAC6 时，需要此信息。

表 1-3. iDRAC6 服务器侦听端口

端口号	功能
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	虚拟控制台键盘 / 鼠标、虚拟介质服务、虚拟介质安全服务和虚拟控制台视频

* 可配置端口

表 1-4. iDRAC6 客户端端口

端口号	功能
25	SMTP
53	DNS
68	DHCP 分配的 IP 地址
69	TFTP
162	SNMP 陷阱
636	LDAPS
3269	全局目录 (GC) LDAPS

您可能需要的其他说明文件

除了本指南以外， Dell 支持网站 **dell.com/support/manuals** 上的以下说明文件提供了关于在系统中设置和操作 iDRAC6 的其它信息。

- iDRAC6 联机帮助提供了有关使用基于 Web 界面的详情。
- 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》提供有关 RACADM 子命令、支持的界面以及 iDRAC6 属性数据库组和对象定义的信息。
- 《Dell Lifecycle Controller 用户指南》介绍 Unified Server Configurator (USC)、 Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE) 和 Remote Services。
- 有关 iDRAC6 和 IPMI 接口的信息，请参阅 《Dell OpenManage 底板管理控制器公用程序用户指南》。
- 《Dell 系统软件支持值表》介绍了有关各种 Dell 系统的信息，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。
- 《Dell OpenManage Server Administrator 安装指南》包含帮助安装 Dell OpenManage Server Administrator 的说明。
- 《Dell OpenManage Management Station 软件安装指南》包含帮助安装 Dell OpenManage Management Station 软件的说明，该软件中包括 Baseboard Management Utility， DRAC 工具和 Active Directory 管理单元。

- 《Dell OpenManage Server Administrator 用户指南》提供有关安装和使用 Server Administrator 的信息。
- 《Dell Update Package 用户指南》提供如何获取 Dell Update Package 以及如何将其用于系统更新策略中。
- *词汇表*介绍本说明文件中使用的术语。

以下系统说明文件还提供了有关安装 iDRAC6 的系统的详情：

- 有关安装 iDRAC6 的信息，请参阅 《硬件用户手册》。
- 系统附带的安全说明提供了重要的安全与管制信息。有关其它管制信息，请参阅 **dell.com/regulatory_compliance** 上的 "Regulatory Compliance"（管制标准）主页。保修信息可能包括在该说明文件中，也可能作为单独的说明文件提供。
- 机架解决方案附带的 《机架安装说明》介绍了如何将系统安装到机架中。
- 《使用入门指南》概述了系统功能、系统设置以及技术规格。
- 《硬件用户手册》提供了有关系统功能的信息，并说明了如何排除系统故障以及安装或更换系统组件。
- 系统管理软件说明文件介绍了软件的功能、要求、安装和基本操作。
- 操作系统说明文件介绍了如何安装 （如果有必要）、配置和使用操作系统软件。
- 单独购买的任何组件所附带的说明文件均提供有关配置和安装这些选件的信息。
- 系统有时附带更新，用于说明对系统、软件和 / 或说明文件所做的更改。

  注：请始终先阅读这些更新，因为这些更新通常会取代其它说明文件中的信息。
- 系统可能附带发行说明或自述文件，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。

通过 Dell 支持站点访问说明文件

要通过 Dell 支持站点访问这些文件：

1. 进入 **dell.com/support/manuals**。
2. 在 **Tell us about your Dell system** （向我们介绍您的戴尔系统）部分，在 **No** （否）下面，选择 **Choose from a list of all Dell products** （从戴尔产品的完整列表中选择）并单击 **Continue** （继续）。

3 在 **Select your product type**（选择产品类型）部分，单击 **Software, Monitors, Electronics & Peripherals**（软件、显示器、电子设备和外围设备）。

4 在 **Choose your Dell Software, Monitors, Electronics & Peripherals**（选择您的戴尔产品：软件、显示器、电子设备和外围设备）部分，单击 **Software**（软件）。

5 在 **Choose your Dell Software**（选择您的戴尔产品：软件）部分，从以下项中单击所需的链接：

- Client System Management （客户端系统管理）
- Enterprise System Management （企业系统管理）
- Remote Enterprise System Management （远程企业系统管理）
- Serviceability Tools （可服务性工具）

6 要查看相应的说明文件，请单击所需的产品版本。

您也可以使用以下链接直接访问这些说明文件：

- 有关客户端系统管理说明文件 —**dell.com/OMConnectionsClient**
- 有关企业系统管理说明文件 — **dell.com/openmanagemanuals**
- 有关远程企业系统管理说明文件 — **dell.com/esmmanuals**
- 有关可服务性工具说明文件 — **dell.com/serviceabilitytools**

2

iDRAC6 使用入门

iDRAC6 使您能够远程监控、故障排除以及修复 Dell 系统，即使系统已关闭。 iDRAC6 提供了虚拟控制台、虚拟介质、智能卡验证和单一登录 (SSO) 等功能。

Management Station 是一个系统，管理员从该系统可远程管理配有 iDRAC6 的 Dell 系统。在这种方式下被监控的系统叫做 *Managed System*。

或者，您可以在 Management Station 和 Managed System 上安装 Dell OpenManage 软件。没有 Managed System Software，将不能在本地使用 RACADM，并且 iDRAC6 无法捕获上次崩溃屏幕。

要设置 iDRAC6，应遵循这些常规步骤：

注：在各种系统中，此步骤可能有所不同。请参阅 Dell 支持网站 dell.com/support/manuals 上特定系统的《硬件用户手册》了解关于如何执行此过程的准确说明。

1. 配置 iDRAC6 属性、网络设置和用户 — 可以通过使用 iDRAC6 配置公用程序、基于 Web 的界面或 RACADM 来配置 iDRAC6。
2. **（可选）**对于 Windows 系统，配置 Microsoft Active Directory 以提供对 iDRAC6 的访问，从而能够为 Active Directory 软件中的现有用户添加和控制 iDRAC6 用户权限。
3. **（可选）**配置智能卡验证 — 智能卡为您的企业额外添加了一层安全保护。
4. 配置远程访问点，比如虚拟控制台和虚拟介质。
5. 配置安全设置。
6. 配置警报实现高效的系统管理能力。
7. 配置 iDRAC6 智能平台管理接口 (IPMI) 设置使用基于标准的 IPMI 工具管理网络上的系统。

3

iDRAC6 的基本安装

本节介绍了如何安装和设置 iDRAC6 硬件和软件。

开始之前

在安装和配置 iDRAC6 软件之前，确保具备系统随附的以下项目：

- iDRAC6 硬件 （已安装或在可选套件中）
- iDRAC6 安装过程 （在本章中）
- *Dell Systems Management Tools and Documentation* DVD

安装 iDRAC6 Express/Enterprise 硬件

注：iDRAC6 连接仿真 USB 键盘连接。因此，重新启动系统后，即使没有连接键盘，系统也不会通知用户。

iDRAC6 Express/Enterprise 可以预装在系统上，也可以单独提供。要开始使用已安装在系统上的 iDRAC6，请参阅第 33 页上的 “软件安装和配置概览”。

如果在系统上没有安装 iDRAC6 Express/Enterprise，请参阅平台的 《硬件用户手册》，了解硬件安装说明。

配置系统使用 iDRAC6

要配置系统使用 iDRAC6，请使用 iDRAC6 配置公用程序。

要运行 iDRAC6 配置公用程序：

1. 打开或重新启动系统。
2. 在 POST 期间出现提示时，请按 <Ctrl><E> 组合键。

   如果按 <Ctrl><E> 之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并再试一次。
3. 配置 LOM。
   a. 使用箭头键选择 **“LAN Parameters”**（LAN 参数），然后按 <Enter> 。随即显示 **“NIC Selection”**（NIC 选择）。
   b. 使用箭头键选择以下某个 NIC 模式：

- **"Dedicated"**（专用）— 选择此选项可以使远程访问设备能够使用 iDRAC6 Enterprise 上的专用网络接口。此接口不与主机操作系统共享并会将管理通信路由到单独的物理网络，从而能够与应用程序通信分开。此选项只有在系统中装有 iDRAC6 Enterprise 时才可用。安装 iDRAC6 Enterprise 卡后，确保更改 **"NIC Selection"**（NIC 选择）为 **"Dedicated"**（专用）。这可以通过 iDRAC6 配置公用程序、 iDRAC6 Web 界面或通过 RACADM 完成。
- **"Shared"**（共享）— 选择此选项可以与主机操作系统共享网络接口。当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1 和 NIC 2 接收数据，但是只通过 NIC 1 发送数据。如果 NIC 1 出现故障，远程访问设备将不可访问。
- **"Shared with Failover LOM2"**（与故障转移 LOM2 共享）— 选择此选项可以与主机操作系统共享网络接口。当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1 和 NIC 2 接收数据，但是只通过 NIC 1 发送数据。如果 NIC 1 出现故障，远程访问设备会故障转移到 NIC 2 进行所有数据发送。远程访问设备会继续使用 NIC 2 进行数据发送。如果 NIC 2 出现故障，远程访问设备会故障转移回 NIC 1 来进行所有数据发送，但前提是 NIC 1 中的故障已经得以纠正。
- **"Shared with Failover All LOMs"**（与故障转移所有 LOM 共享）— 选择此选项可以与主机操作系统共享网络接口。当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1、NIC 2、NIC 3 和 NIC 4 接收数据；但是只通过 NIC 1 发送数据。如果 NIC 1 出现故障，远程访问设备会故障转移到 NIC 2 来进行所有数据发送。如果 NIC 2 出现故障，远程访问设备会故障转移到 NIC 3 来进行所有数据发送。如果 NIC 3 出现故障，远程访问设备会故障转移到 NIC 4 来进行所有数据发送。如果 NIC 4 出现故障，远程访问设备会故障转移回 NIC 1 来进行所有数据发送 （仅当 NIC 1 故障已修复时）。

4 配置网络控制器 LAN 参数使用 DHCP 或静态 IP 地址源。

a 使用下箭头键，选择 **"LAN Parameters"**（LAN 参数）并按 <Enter>。

b 使用上箭头和下箭头键，选择 **"IP Address Source"**（IP 地址源）。

c 使用右箭头和左箭头键，选择 DHCP、“Auto Config”（自动配置）或 “Static”（静态）。

d 如果选择了 “Static”（静态），请配置 “IP Address”（IP 地址）、“Subnet Mask”（子网掩码）和 “Default Gateway”（默认网关）设置。

e 按 <Esc> 键。

5 按 <Esc> 键。

6 选择 Save Changes and Exit （保存更改并退出）。

软件安装和配置概览

本节高度概述了 iDRAC6 软件安装和配置过程。有关 iDRAC6 软件组件的详情，请参阅第 34 页上的 “在 Managed System 上安装软件”。

安装 iDRAC6 软件

要安装 iDRAC6 软件：

1 在 Managed System 上安装 iDRAC6 软件。请参阅第 34 页上的 “在 Managed System 上安装软件”。

2 在 Management Station 上安装 iDRAC6 软件。请参阅第 34 页上的 “在 Management Station 上安装软件”。

配置 iDRAC6

要配置 iDRAC6：

1 使用下面一个配置工具：

- 基于 Web 的界面 （请参阅第 41 页上的 “使用 Web 界面配置 iDRAC6”）
- RACADM CLI （请参阅 dell.com/support/manuals 上的 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》）
- Telnet 控制台 （请参阅第 79 页上的 “使用 Telnet 控制台”）

注：同时使用一个以上的 iDRAC6 配置工具可能会产生意外的结果。

2 配置 iDRAC6 网络设置。请参阅第 98 页上的 “配置 iDRAC6 网络设置”。

3 添加并配置 iDRAC6 用户。请参阅第 115 页上的 “添加和配置 iDRAC6 用户”。

4 配置 Web 浏览器以访问基于 Web 的界面。请参阅第 38 页上的“配置支持的 Web 浏览器”。

5 禁用 Microsoft Windows 自动重新引导选项。请参阅第 284 页上的“禁用 Windows 自动重新引导选项”。

6 更新 iDRAC6 固件。请参阅第 35 页上的 “更新 iDRAC6 固件”。

在 Managed System 上安装软件

在 Managed System 上安装软件是可选项。没有 Managed System Software，将不能在本地使用 RACADM，并且 iDRAC6 无法捕获上次崩溃屏幕。

要安装 Managed System Software，请使用 *Dell Systems Management Tools and Documentation* DVD 在 Managed System 上安装软件。有关安装此软件的说明，请参阅 Dell 支持网站 **support.dell.com\manuals** 上提供的 《软件快速安装指南》。

Managed System Software 将您选择的相应版本的 Dell OpenManage Server Administrator 安装在 Managed System 上。

注：请勿在同一系统上安装 iDRAC6 Management Station Software 和 iDRAC6 Managed System Software。

如果 Managed System 上没有安装 Server Administrator，您将无法查看系统的上次崩溃屏幕或使用 **“Auto Recovery”**（自动恢复）功能。

有关上次崩溃屏幕的详情，请参阅第 302 页上的 “查看上次系统崩溃屏幕”。

在 Management Station 上安装软件

您的系统包括 *Dell Systems Management Tools and Documentation* DVD。此 DVD 具有以下组件：

- DVD 根目录 - 包含 Dell Systems Build and Update Utility，这提供了服务器设置和系统安装的信息
- SYSMGMT - 包含系统管理软件产品，其中包括 Dell OpenManage Server Administrator

有关 Server Administrator、 IT Assistant 和 Unified Server Configurator 的信息，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《Server Administrator 用户指南》、《IT Assistant 用户指南》和 《Lifecycle Controller 用户指南》。

在 Linux Management Station 上安装和删除 RACADM

要使用远程 RACADM 功能，请在运行 Linux 的 Management Station 上安装 RACADM。

注：运行 *Dell Systems Management Tools and Documentation* DVD 上的**安装程序**时，支持的所有操作系统的 RACADM 公用程序都安装到 Management Station 上。

安装 RACADM

1. 以 root 身份登录至您想在其中安装 Management Station 组件的系统。
2. 如果有必要，使用以下命令或类似命令安装 *Dell Systems Management Tools and Documentation* DVD：

   ```
   mount /media/cdrom
   ```

3. 导航到 **/linux/rac** 目录并执行以下命令：

   ```
   rpm -ivh *.rpm
   ```

要获得关于 RACADM 命令的帮助，请在发出前面的命令后键入 **racadm help**。

卸载 RACADM

要卸载 RACADM，请打开命令提示符并键入：

```
rpm -e <racadm_软件包_名称>
```

其中 <*racadm_软件包_名称*> 是用于安装 RAC 软件的 RPM 软件包。

例如，如果 RPM 软件包名称是 **srvadmin-racadm5**，则键入：

```
rpm -e srvadmin-racadm5
```

更新 iDRAC6 固件

使用以下某一方法更新 iDRAC6 固件。

- 基于 Web 的界面 （请参阅第 36 页上的 “使用基于 Web 的界面更新 iDRAC6 固件”）
- RACADM CLI （请参阅第 36 页上的 “使用 RACADM 更新 iDRAC6 固件”）
- Dell Update Package（请参阅第 37 页上的“使用针对所支持 Windows 和 Linux 操作系统的 Dell Update Package 更新 iDRAC6 固件”）

开始之前

使用本地 RACADM 或 Dell Update Package 更新 iDRAC6 固件前，应执行以下过程。否则，固件更新操作可能会失败。

1. 安装并启用相应的 IPMI 和受管节点驱动程序。
2. 如果系统正在运行 Windows 操作系统，则启用并启动 **Windows Management Instrumentation** (WMI) 服务。
3. 如果您使用 iDRAC6 Enterprise 且系统正在运行 SUSE Linux Enterprise Server （版本 10） for Intel? EM64T，请启动 **Raw** 服务。
4. 断开连接并卸下虚拟介质。

   注：如果 iDRAC6 固件更新因故中断，可能最多需要等待 30 分钟，才可以再次进行固件更新。
5. 确保 USB 已启用。

下载 iDRAC6 固件

要更新 iDRAC6 固件，从 Dell 支持网站 **support.dell.com** 下载最新固件并将该文件保存到本地系统。

iDRAC6 固件包中含有以下软件组件：

- 编译的 iDRAC6 固件代码和数据
- 基于 Web 的界面、JPEG 和其它用户界面数据文件
- 默认配置文件

使用基于 Web 的界面更新 iDRAC6 固件

有关详细信息，请参阅第 67 页上的 “更新 iDRAC6 固件 / 系统服务恢复映像”。

使用 RACADM 更新 iDRAC6 固件

可以使用基于 CLI 的 RACADM 工具来更新 iDRAC6 固件。如果在 Managed System 上装有 Server Administrator，则使用本地 RACADM 更新固件。

1. 从 Dell 支持网站 **support.dell.com** 下载 iDRAC6 固件映像到 Managed System。

   例如：

   ```
   C:\downloads\firmimg.d6
   ```

2 运行以下 RACADM 命令：

```
racadm fwupdate -pud c:\downloads\
```

还可以使用远程 RACADM 和 TFTP 服务器更新固件。

例如：

```
racadm -r <iDRAC6 IP 地址> -u <用户名> -p <密码>
fwupdate -g -u -a <路径>
```

其中*路径*是 TFTP 服务器上存储 **firmimg.d6** 的位置，包括 TFTP 服务器 IP 地址。

路径：<*TFTP 服务器 IP*> -d <*TFTP 服务器上的固件映像路径*>

- 情况 1：如果 firmimg.d6 映像位于 tftp 根目录文件夹中，路径为：<*TFTP 服务器 IP*>
- 情况 2：如果 firmimg.d6 映像位于 tftp 根目录的子文件夹中，路径为：<*TFTP 服务器 IP*> -d /< *子文件夹路径* >

使用针对所支持 Windows 和 Linux 操作系统的 Dell Update Package 更新 iDRAC6 固件

从 Dell 支持网站 **support.dell.com** 下载并运行针对所支持 Windows 和 Linux 操作系统的 Dell Update Package。有关详情，请参阅 Dell 支持网站 **support.dell.com\manuals** 上的 《Dell Update Package 用户指南》。

注：在使用 Linux 中的 Dell Update Package 公用程序更新 iDRAC6 固件时，可看到控制台上显示的这些信息：

“usb 5-2: device descriptor read/64, error -71”（usb 5-2：设备描述符读取 /64，错误 -71）

“usb 5-2: device descriptor not accepting address 2, error -7”（usb 5-2：设备描述符不能接受地址 2，错误 -71）

这些错误在性质上并不严重，应予以忽略。这些信息是由于固件更新过程中重设 USB 设备而造成的，并且无害。

配置支持的 Web 浏览器

以下各节提供了有关配置支持的 Web 浏览器的说明。

配置 Web 浏览器以连接到 iDRAC6 基于 Web 的界面

如果从通过代理服务器连接到 Internet 的 Management Station 连接到 iDRAC6 基于 Web 的界面，则必须配置 Web 浏览器才能从该服务器访问 Internet。

要配置 Internet Explorer Web 浏览器访问代理服务器：

1. 打开 Web 浏览器窗口。
2. 单击 **"Tools"**（工具）并单击 **"Internet Options"**（Internet 选项）。
3. 从 **"Internet Options"**（Internet 选项）窗口中，单击 **"Connections"**（连接）选项卡。
4. 在 **"Local Area Network (LAN) settings"**（局域网 [LAN] 设置）下，单击 **"LAN Settings"**（局域网设置）。
5. 如果选中了 **"Use a proxy server"**（使用代理服务器）框，则选择 **"Bypass proxy server for local addresses"**（对于本地地址不使用代理服务器）框。
6. 单击 **"OK"**（确定）两次。

可信域列表

通过 Web 浏览器访问 iDRAC6 基于 Web 的界面时，如果可信域列表中缺少 iDRAC6 IP 地址，将提示您将该 IP 地址添加到列表中。完成后，单击 **"Refresh"**（刷新）或重新启动 Web 浏览器以重新连接到 iDRAC6 基于 Web 的界面。

查看基于 Web 界面的本地化版本

Windows

以下 Windows 操作系统语言支持 iDRAC6 基于 Web 的界面：

- 英语
- 法语
- 德语
- 西班牙语

- 日语
- 简体中文

要在 Internet Explorer 中查看 iDRAC6 基于 Web 界面的本地化版本：

1. 单击 **"Tools"**（工具）菜单并选择 **"Internet Options"**（Internet 选项）。
2. 在 **"Internet Options"**（Internet 选项）窗口中，单击 **"Languages"**（语言）。
3. 在 **"Language Preference"**（语言首选项）窗口中，单击 **"Add"**（添加）。
4. 在 **"Add Language"**（添加语言）窗口中，选择支持的语言。

   要选择一种以上的语言，按 <Ctrl>。
5. 选择首选语言并单击 **"Move Up"**（上移）将语言移动到列表顶部。
6. 单击 **OK**（确定）。
7. 在 **"Language Preference"**（语言首选项）窗口中，单击 **"OK"**（确定）。

Linux

如果在具有简体中文图形用户界面 (GUI) 的 Red Hat Enterprise Linux（版本 4）客户端上运行虚拟控制台， Viewer 菜单和标题可能会显示随机字符。此问题是由于 Red Hat Enterprise Linux （版本 4）简体中文操作系统中的编码不正确引起的。要修复此问题，通过执行以下步骤访问并修改当前编码设置：

1. 打开命令终端。
2. 键入 "locale" 并按 <Enter>。系统将显示以下输出。

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
```

```
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3 如果这些值包括 “zh_CN.UTF-8”，则无需任何更改。如果值中不包括 “zh_CN.UTF-8”，则转至步骤 4。

4 导航至 /etc/sysconfig/i18n 文件。

5 在文件中，应用以下更改：

当前项：

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

更新项：

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-
8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

6 注销，然后登录操作系统。

7 重新启动 iDRAC6。

从其它语言切换到简体中文时，应确保此修复仍然有效。否则，应重复此过程。

有关 iDRAC6 的高级配置，请参阅第 77 页上的 “高级 iDRAC6 配置”。

4

使用 Web 界面配置 iDRAC6

iDRAC6 提供了 Web 界面供您配置 iDRAC6 属性和用户、执行远程管理任务以及排除远程 （受管）系统的问题。对于日常系统管理，请使用 iDRAC6 Web 界面。本章介绍如何使用 iDRAC6 Web 界面来执行常规系统管理任务，并提供了指向相关信息的链接。

大多数 Web 界面配置任务还可以使用 RACADM 命令或服务器管理命令行协议 (SM-CLP) 命令来执行。

本地 RACADM 命令从受管服务器执行。

SM-CLP 和 SSH/Telnet RACADM 命令在 Shell 中执行，可通过 Telnet 或 SSH 连接远程使用。有关使用 SM-CLP 的详情，请参阅第 209 页上的“使用 iDRAC6 SM-CLP 命令行界面”。有关 RACADM 命令的详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《RACADM iDRAC6 和 CMC 命令行参考指南》。

小心：通过单击 “Refresh”（刷新）或按 F5 刷新浏览器时，会从 Web 图形用户界面 (GUI) 会话中注销或重定向到 “System Summary”（系统摘要）页。

访问 Web 界面

要访问 iDRAC6 Web 界面，请执行以下步骤：

1. 打开支持的 Web 浏览器窗口。

   要使用 IPv4 地址访问 Web 界面，请转至步骤 2。

   要使用 IPv6 地址访问 Web 界面，请转至步骤 3。

2. 使用 IPv4 地址访问 Web 界面；必须启用 IPv4：

   在浏览器的 **“Address”**（地址）栏中，键入：

   `https://<iDRAC-IPv4 地址>`

   然后按 <Enter>。

3. 使用 IPv6 地址访问 Web 界面；必须启用 IPv6。

   在浏览器的 **“Address”**（地址）栏中，键入：

   `https://[<iDRAC-IPv6 地址>]`

   然后按 <Enter>。

4 如果默认 HTTPS 端口号 （端口 443）已更改，请键入：

`https://<iDRAC-IP-` **地址** `>:<` **端口号** `>`

其中 *iDRAC-IP-**地址***是 iDRAC6 **的** IP **地址，而***端口号***是** HTTPS **端口号。**

5 在 **"Address"**（地址）字段中，键入 `https://<`*iDRAC-IP- 地址* `>` 并按 <Enter>。

如果默认 HTTPS 端口号 （端口 443）已更改，请键入：

`https://<`*iDRAC-IP- **地址** >:< **端口号***`>`

其中 *iDRAC-IP- **地址***是 iDRAC6 的 IP 地址，而***端口号***是 HTTPS 端口号。

将显示 iDRAC6 **"Login"**（登录）窗口。

登录

您可以以 iDRAC6 用户或 Microsoft Active Directory 用户的身份登录。iDRAC6 用户的默认用户名为 **root**，默认密码为 **calvin**。

必须得到管理员授予的 **"Login to iDRAC"**（登录到 iDRAC）权限才能登录到 iDRAC6。

要登录，执行下列步骤：

1 在 **"Username"**（用户名）字段中键入下面的内容之一：

- 您的 iDRAC6 用户名。

  本地用户的用户名区分大小写。比如 `root`、`it_user` 或 john_doe。

- 您的 Active Directory 用户名。

  Active Directory 名称可以用以下任何形式输入：< *用户名* >、< *域* >\< *用户名* >、< *域* >/< *用户名* > 或 < *用户* >@< *域* >。它们不区分大小写。比如 `dell.com\john_doe` 或 `JOHN_DOE@DELL.COM`。

2 在 **"Password"**（密码）字段中，键入 iDRAC6 用户密码或 Active Directory 用户密码。密码区分大小写。

3 从 **"Domain"**（域）下拉框中，选择 *"This iDRAC"（此 iDRAC）* 则以 iDRAC6 用户身份登录，或选择任何可用域则以 Active Directory 用户身份登录。

注：对于 Active Directory 用户，如果指定了域名作为用户名的一部分，则从下拉菜单中选择 *"This iDRAC"（此 iDRAC）*。

4 单击 OK （确定）或按 <Enter>。

注销

1 在主窗口的右上角，单击 **"Logout"**（注销）关闭会话。

2 关闭浏览器窗口。

注："**Logout**"（注销）按钮在您登录后才出现。

注：如果在未注销的情况下关闭浏览器，将会导致会话保持打开状态，直至超时为止。强烈建议您单击注销按钮结束会话；否则，该会话将在会话超时之前一直保持活动状态。

注：在 Microsoft Internet Explorer 中使用窗口右上角的关闭按钮（"x"）关闭 iDRAC6 Web 界面可能会生成应用程序错误。要解决这个问题，请从 Microsoft 支持网站 **support.microsoft.com** 下载最新的 Internet Explorer 累积安全更新。

小心：如果通过 <Ctrl+T> 或 <Ctrl+N> 打开了多个 Web GUI 会话来从同一个 Management Station 访问同一个 iDRAC6，接着注销了其中一个会话，则所有 Web GUI 会话都会终止。

使用多个浏览器选项卡和窗口

打开新选项卡和窗口时，不同版本的 Web 浏览器会表现出不同的行为。Microsoft Internet Explorer 版本 7 和版本 8 提供打开选项卡和窗口的选择。

选项卡会继承最近打开的选项卡的特征。

按 <Ctrl - T> 从活动会话打开新选项卡，然后再次登录。

按 <Ctrl - N> 从活动会话打开新的浏览器窗口。您将通过已验证的凭据登录。

关闭一个选项卡会使所有 iDRAC6 Web 界面选项卡过期。

此外，如果您使用高级用户权限在一个选项卡上登录，而在另一个选项卡上以管理员身份登录，则两个选项卡均获得第一次登录的权限。

Mozilla Firefox 3 的选项卡行为与 Microsoft Internet Explorer 版本 7 和版本 8 相同。

表 4-1. 受支持浏览器中的用户权限行为

浏览器	选项卡行为	窗口行为
Microsoft Internet Explorer 6	不适用	新会话
Microsoft IE7 和 IE8	从最后打开的会话	新会话

配置 iDRAC6 NIC

本节假定 iDRAC6 已经配置好并能够在网络上访问。如需初始 iDRAC6 网络配置的帮助，请参阅第 33 页上的 “配置 iDRAC6”。

配置网络和 IPMI LAN 设置

注：您必须具有 “**Configure iDRAC**”（配置 iDRAC）权限才能执行以下步骤。

注：大部分 DHCP 服务器需要一个服务器来将客户端标识符令牌存储在其保留表中。客户端 （例如 iDRAC）在 DHCP 协议过程中必须提供此令牌。 iDRAC6 以单字节接口编号 (0) 后跟六字节 MAC 地址来提供客户端标识符选项。

注：如果运行时启用了生成树协议 (STP)，请保证还按以下方式打开了 PortFast 或类似技术：
- 在连接到 iDRAC6 的交换机的端口上
- 在连接到运行 iDRAC 虚拟控制台会话的 Management Station 的端口上

注：如果系统在开机自检过程中停机，可能会看到以下信息：“`Strike the F1 key to continue, F2 to run the system setup program`”（按 `F1` 键继续，按 `F2` 键运行系统设置程序）
该错误的一个可能原因是出现网络风暴事件，导致失去与 iDRAC6 的通信。网络风暴平息后，重新启动系统。

1. 单击 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）→ **“Network”**（网络）。
2. 在 **“Network”**（网络）页上，可以输入网络设置、常见 iDRAC6 设置、IPv4 设置、IPv6 设置、IPMI 设置和 VLAN 设置。请参阅表 4-2、表 4-3、表 4-4、表 4-5、表 4-6 和表 4-7 了解这些设置的说明。
3. 输入所需的设置后，单击 **“Apply”**（应用）。

   对 “Network”（网络）页进行的新设置将被保存。

   注：对 NIC IP 地址设置的更改将关闭所有用户会话并且用户必须使用更新的 IP 地址设置重新连接到 iDRAC6 Web 界面。对于所有其它更改，必须重设 NIC，这可能导致短暂的连接中断。

表 4-2. 网络设置

设置	说明
NIC 选择	配置四种可能模式中的当前模式： • 专用 • 共享 (LOM1) • 与故障转移 LOM2 共享 • 与故障转移所有 LOM 共享 **注：“Dedicated”（专用）选项仅对于 iDRAC Enterprise 卡可用，“Shared with Failover All LOMs”（与故障转移所有 LOM 共享）选项仅对几个系统可用。** 如果 NIC 选择设置为 **“Shared”**（共享）或 **“Shared with Failover”**（与故障转移共享）模式，iDRAC6 将不会通过同一物理端口进行本地通信。这是因为网络交换机不会通过收到数据包的同一端口来发送数据包。 如果 NIC 选择设置为 **“Shared with Failover”**（与故障转移共享）（LOM 2 或所有 LOM），建议不要将 LOM 连接到不同网络广播域。 将 iDRAC 配置为任何共享模式时，建议不要将 LOM 与添加式网络控制器组合。无论 NIC 选择模式是什么，各 LOM 之间任何类型的组合都可以接受 （共享 / 与故障转移 LOM2 共享 / 与故障转移所有 LOM 共享）。
“MAC Address”（MAC 地址）	显示唯一标识网络中各个节点的 “Media Access Control (MAC) Address”（介质访问控制 [MAC] 地址）。
“Enable NIC”（启用 NIC）	选中后，表示 NIC 已启用并激活此组中剩余的控制。当 NIC 被禁用时，通过网络往来于 iDRAC6 的所有通信均被阻止。 默认值为 **“On”**（开）。

表 4-2. 网络设置 *（续）*

设置	说明
"Auto Negotiation"（自动协商）	如果设置为 **"On"**（开），则通过与最近的路由器或交换机通信来显示网络速度和模式。如果设置为 **"Off"**（关），则允许手动设置网络速度和双工模式。 如果 **"NIC Selection"**（NIC 选择）*不是*设置为 **"Dedicated"**（专用），则总是启用 "Auto Negotiation"（自动协商）设置（**"On"** [开]）。 **注：服务器关闭时，嵌入式 LOM 端口最多支持速度 100Mbps。因此，配置 LOM 和交换机以支持自动协商将保证在系统电源转换期间始终连接到 iDRAC。**
Network Speed（网络速度）	使您能够根据网络环境将网络速度设置为 100 Mb 或 10 Mb。如果 "Auto Negotiation"（自动协商）设置为 **"On"**（开），此选项将不可用。
Duplex Mode（双工模式）	使您能够根据网络环境将双工模式设置为全双工或半双工。如果 **"Auto Negotiation"**（自动协商）设置为 **"On"**（开），此选项将不可用。
NIC MTU	允许设置 NIC 上的最大传输单元 (MTU) 大小。

表 4-3. 常见设置

设置	说明
"Register iDRAC on DNS"（在 DNS 上注册 iDRAC）	在 DNS 服务器上注册 iDRAC6 名称。 默认为 **"Disabled"**（已禁用）。
"DNS iDRAC Name"（DNS iDRAC 名称）	只有在选中 **"Register iDRAC on DNS"**（在 DNS 上注册 iDRAC）后才会显示 iDRAC6 名称。默认名称为 idrac- *服务标签*，其中*服务标签*是 Dell 服务器的服务标签号码，例如：idrac-00002。
"Auto Config Domain Name"（自动配置域名）	使用默认 DNS 域名。如果没有选中该复选框并且选择了 **"Register iDRAC on DNS"**（在 DNS 上注册 iDRAC）选项，则可以在 **"DNS Domain Name"**（DNS 域名）字段中修改 DNS 域名。 默认为 **"Disabled"**（已禁用）。

表 4-3. 常见设置 *（续）*

设置	说明
DNS Domain Name（DNS 域名）	默认 **"DNS Domain Name"**（DNS 域名）为空白。选中 **"Auto Config Domain Name"**（自动配置域名）复选框后，此选项禁用。

表 4-4. IPv4 设置

设置	说明
Enable IPv4（启用 IPv4）	如果启用了 NIC，此操作将选择 IPv4 协议支持并将此部分中的其它字段设置为启用。
DHCP Enable（启用 DHCP）	提示 iDRAC6 从动态主机配置协议 (DHCP) 服务器获取 NIC 的 IP 地址。默认值为 **"off"**（关）。
IP Address（IP 地址）	指定 iDRAC6 NIC IP 地址。
子网掩码	允许用户输入或编辑 iDRAC6 NIC 的静态 IP 地址。要更改此设置，请取消选择 "Use DHCP (For NIC IP Address)"（使用 DHCP [对于 NIC IP 地址]）复选框。
网关	路由器或交换机的地址。该值采用 "点分隔" 格式，比如 192.168.0.1。
"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）	通过选择 **"Use DHCP to obtain DNS server addresses"**（使用 DHCP 获取 DNS 服务器地址）复选框启用 DHCP 获取 DNS 服务器地址。如果没有使用 DHCP 获取 DNS 服务器地址，应在 **"Preferred DNS Server"**（首选 DNS 服务器）和 **"Alternate DNS Server"**（备用 DNS 服务器）字段中提供 IP 地址。 默认值为 **"off"**（关）。 **注：如果选中 "Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）复选框，将不能在 "Preferred DNS Server"（首选 DNS 服务器）和 "Alternate DNS Server"（备用 DNS 服务器）字段中输入 IP 地址。**
首选 DNS 服务器	DNS 服务器 IP 地址。
备用 DNS 服务器	备用 DNS 服务器 IP 地址。

表 4-5. IPv6 设置

设置	说明
Enable IPv6（启用 IPv6）	如果选中该复选框，则启用 IPv6。如果没有选中该复选框，则禁用 IPv6。默认为 “Disabled”（已禁用）。
“Autoconfiguration Enable”（启用自动配置）	选择此框允许 iDRAC6 从动态主机配置协议 (DHCPv6) 服务器获取 iDRAC6 NIC 的 IPv6 地址。启用自动配置还将取消激活并清除 “IP Address 1”（IP 地址 1）、“Prefix Length”（前缀长度）和 “IP Gateway”（IP 网关）的静态值。
“IP Address 1”（IP 地址 1）	为 iDRAC NIC 配置 IPv6 地址。要更改此设置，必须先通过取消选择相关复选框来禁用 **“AutoConfig”**（自动配置）。
前缀长度	配置 IPv6 地址的前缀长度。可以是介于 1 和 128 （含）之间的值。要更改此设置，必须先通过取消选择相关复选框来禁用 **“AutoConfig”**（自动配置）。
网关	为 iDRAC NIC 配置静态网关。要更改此设置，必须先通过取消选择相关复选框来禁用 **“AutoConfig”**（自动配置）。
链路本地地址	指定 iDRAC6 NIC 链路本地 IPv6 地址。
“IP Address 2...15”（IP 地址 2...15）	如果有的话，指定附加 iDRAC6 NIC IPv6 地址。
“Use DHCP to obtain DNS server addresses”（使用 DHCP 获取 DNS 服务器地址）	通过选择 **“Use DHCP to obtain DNS server addresses”**（使用 DHCP 获取 DNS 服务器地址）复选框启用 DHCP 获取 DNS 服务器地址。如果没有使用 DHCP 获取 DNS 服务器地址，应在 **“Preferred DNS Server”**（首选 DNS 服务器）和 **“Alternate DNS Server”**（备用 DNS 服务器）字段中提供 IP 地址。 默认值为 “Off”（关）。 **注：如果选中 “Use DHCP to obtain DNS server addresses”（使用 DHCP 获取 DNS 服务器地址）复选框，将不能在 “Preferred DNS Server”（首选 DNS 服务器）和 “Alternate DNS Server”（备用 DNS 服务器）字段中输入 IP 地址。**

表 4-5. IPv6 设置 *（续）*

设置	说明
首选 DNS 服务器	配置首选 DNS 服务器的静态 IPv6 地址。要更改此设置，必须先清除 **"Use DHCP to obtain DNS Server Addresses"**（使用 DHCP 获取 DNS 服务器地址）。
备用 DNS 服务器	配置备用 DNS 服务器的静态 IPv6 地址。要更改此设置，必须先清除 **"Use DHCP to obtain DNS Server Addresses"**（使用 DHCP 获取 DNS 服务器地址）。

表 4-6. IPMI 设置

设置	说明
启用 LAN 上 IPMI	选中后表示 IPMI LAN 信道已启用。默认值为 **"Off"**（关）。
信道权限级别限制	配置 LAN 信道上可接受的用户最低权限级别。选择以下选项之一：**"Administrator"**（管理员）、**"Operator"**（操作员）或 **"User"**（用户）。默认为 **"Administrator"**（管理员）。
Encryption Key（加密密钥）	配置密钥：0 至 20 个十六进制字符 （不允许空白）。默认值是全零。

表 4-7. VLAN 设置

设置	说明
启用 VLAN ID	如果启用，将仅接受匹配的虚拟 LAN (VLAN) ID 通信。
VLAN ID	802.1g 字段中的 VLAN ID 字段。为 VLAN ID 输入有效值（必须为 1 到 4094 之间的数字）。
Priority （优先级）	802.1g 字段中的 "Priority"（优先权）字段。输入一个从 0 到 7 之间的数字以设置 VLAN ID 的优先权。

配置 IP 筛选和 IP 阻塞

注：您必须具有 **"Configure iDRAC"**（配置 iDRAC）权限才能执行以下步骤。

1. 单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性），然后单击 **"Network"**（网络）选项卡打开 **"Network"**（网络）页。
2. 单击 **"Advanced Settings"**（高级设置）配置网络安全性设置。

   表 4-8 说明了 **"Network Security"**（网络安全性）**页设置**。

3 配置设置后，单击 **"Apply"**（应用）。

保存 "Network Security"（网络安全性）页上所做的任何新设置。

表 4-8. 网络安全性页设置

设置	说明
IP Range Enabled（IP 范围已启用）	启用 IP 范围检查功能，定义了可以访问 iDRAC 的 IP 地址范围。默认值为 **"off"**（关）。
IP Range Address（IP 范围地址）	根据子网掩码中的 1，确定可接受的 IP 地址位样式。该值是含 IP 范围子网掩码的按位 "与"，可确定所允许的 IP 地址的高端。允许在高位包含此位样式的任何 IP 地址建立 iDRAC6 会话。从该范围外的 IP 地址登录都会失败。各属性中的默认值允许从 192.168.1.0 到 192.168.1.255 的地址范围建立 iDRAC6 会话。
"IP Range Subnet Mask"（IP 范围子网掩码）	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。默认为 **255.255.255.0**。
IP Blocking Enabled（IP 阻塞已启用）	启用 IP 地址阻塞功能，该功能限制在预先选择的时间范围内从特定 IP 地址尝试登录失败的次数。默认值为 **"off"**（关）。
IP Blocking Fail Count（IP 阻塞失败计数）	设置拒绝某个 IP 地址的登录尝试前允许登录失败的次数。默认为 **10**。
IP Blocking Fail Window（IP 阻塞失败时间范围）	决定一个时间范围（以秒为单位），在该范围内必须发生 IP 阻塞失败计数的失败次数才会触发 IP 阻塞惩罚时间。默认为 **3600**。
IP Blocking Penalty Time（IP 阻塞惩罚时间）	一个时间范围（以秒为单位），在该范围内拒绝失败次数过多的某个 IP 地址的登录尝试。默认为 **3600**。

配置平台事件

平台事件配置提供了用于配置 iDRAC6 以便针对某些事件信息执行所选操作的机制。操作包括无操作、重新引导系统、系统关机后再开机、关闭系统电源和生成警报 （平台事件陷阱 [PET] 和 / 或电子邮件）。

表 4-9 中列出了可筛选平台事件。

表 4-9. 平台事件筛选器

索引	平台事件
1	风扇危急声明
2	电池警告声明
3	电池危急声明
4	电压危急声明
5	温度警告声明
6	温度危急声明
7	侵入危急声明
8	已降级冗余
9	冗余丢失
10	处理器警告声明
11	处理器危急声明
12	没有处理器危急声明
13	电源设备警告声明
14	电源设备危急声明
15	没有电源设备危急声明
16	事件日志危急声明
17	监督危急声明
18	系统电源警告声明
19	系统电源危急声明
20	没有可移动闪速更新介质通知声明
21	可移动闪速更新介质危急声明
22	可移动闪速更新介质警告声明

出现平台事件时 （例如，电池警告声明），会生成系统事件并记录在系统事件日志 (SEL) 中。如果该事件与某个已启用的平台事件筛选器 (PEF) 相匹配且已将该筛选器配置为生成警报 （PET 或电子邮件），则会将 PET 或电子邮件警报发送到一个或多个配置目标。

如果还将同一平台事件筛选器配置为执行操作 （比如重新引导系统），则将执行该操作。

配置平台事件筛选器 (PEF)

注：配置平台事件陷阱或电子邮件警报设置前配置平台事件筛选器。

1. 使用支持的 Web 浏览器登录远程系统。请参阅第 41 页上的 “访问 Web 界面”。
2. 单击 **“System”**（系统）→ **“Alerts”**（警报）→ **“Platform Events”**（平台事件）。
3. 在 **“Platform Event Filters Configuration”**（平台事件筛选器配置）下，选择 **“Enabled”**（已启用）选项以**启用平台事件筛选器警报**。

   注：必须启用 “**Enable Platform Event Filter Alerts**”（启用平台事件筛选器警报）才能将警报发送到任何有效的配置目标 （PET 或电子邮件）。
4. 在 **“Platform Event Filters List”**（平台事件筛选器列表）表中，对于要配置的筛选器执行以下操作：
   - 选择以下一项措施：
     - 重新引导系统
     - 关闭系统电源后再开启
     - 关闭系统电源
     - No Action （无操作）
   - 在 **“Generate Alert”**（生成警报）列中，选择复选框允许警报生成，或取消选中复选框禁止选定操作的警报生成。

   注：必须启用 “**Generate Alert**”（生成警报）才能将警报发送到任何有效的配置目标 （PET）。
5. 单击 **“Apply”**（应用）。将保存设置。

配置平台事件陷阱 (PET)

注：必须具有 “**Configure iDRAC**”（配置 iDRAC）权限才能添加或启用 / 禁用 SNMP 警报。如果不具有 “**Configure iDRAC**”（配置 iDRAC）权限，以下选项将不可用。

1 使用支持的 Web 浏览器登录远程系统。

2 确保已执行第 52 页上的 “配置平台事件筛选器 (PEF)”中的过程。

3 单击 **“System”**（系统）→ **“Alerts”**（警报）→ **“Traps Settings”**（陷阱设置）。

4 在 **“IPv4 Destination List”**（IPv4 目标列表）或 **“IPv6 Destination List”**（IPv6 目标列表）中，对于**目标号码**执行以下操作以配置 IPv4 或 IPv6 SNMP 警报目标：

   a 选择或取消选择 **“State”**（状态）复选框。选中的复选框表示允许 IP 地址接收警报。取消选择的复选框表示禁止 IP 地址接收警报。

   b 在 **“Destination IPv4 Address”**（目标 IPv4 地址）或 **“Destination IPv6 Address”**（目标 IPv6 地址）中，输入有效的平台事件陷阱目标 IP 地址。

   c 在 **“Test Trap”**（检测陷阱）中，单击 **“Send”**（发送）检测配置的警报。

   注：用户帐户必须具有 “Test Alerts”（检测警报）权限才能发送检测陷阱。有关详情，请参阅表 6-6。

   指定的更改显示在 IPv4 或 IPv6 **“Destination List”**（目标列表）中。

5 在 **“Community String”**（团体字符串）字段中，输入 iDRAC SNMP 团体名称。

   注：目标团体字符串必须与 iDRAC6 团体字符串相同。

6 单击 **“Apply”**（应用）。将保存设置。

注：如果禁用平台事件筛选器，与状态为 °× 不好 °± 的传感器相关的陷阱也会禁用。如果 “Enable Platform Event Filter Alerts”（启用平台事件筛选器警报）选项已启用，始终会生成与 °× 不良到良好 °± 过渡关联的陷阱。例如，如果禁用 “Removable Flash MEdia Absent Informational Assert Filter”（没有可移动快擦写介质通知声明筛选器）的 “Generate Alert”（生成警报）选项并卸下 SD 卡，将不会显示相关陷阱。如果再次插入 SD 卡，将生成陷阱。但如果启用 “Enable Platform Event Filter Alerts”（启用平台事件筛选器警报）选项，则卸下或插入 SD 卡时会生成陷阱。

配置电子邮件警报

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

注：电子邮件警报支持 IPv4 和 IPv6 地址。

1 使用支持的 Web 浏览器登录远程系统。

2 确保已执行第 52 页上的“配置平台事件筛选器 (PEF)”中的过程。

3 单击 **“System”**（系统）→ **“Alerts”**（警报）→ **“Email Alert Settings”**（电子邮件警报设置）。

4 在 **“Destination Email Addresses”**（目标电子邮件地址）表中，执行以下操作，为 **“Email Alert Number”**（电子邮件警报号码）配置目标地址：

   a 选择或取消选择 **“State”**（状态）复选框。选中的复选框表示允许电子邮件地址接收警报。取消选择的复选框表示禁止电子邮件地址接收警报信息。

   b 在 **“Destination E-mail Address”**（目标电子邮件地址）字段中，键入有效电子邮件地址。

   c 在 **“E-mail Description”**（电子邮件说明）字段中，键入简短说明。

5 在 **“Test Email”**（检测电子邮件）中，单击 **“Send”**（发送）检测配置的电子邮件警报设置。

6 在 **“SMTP (e-mail) Server IP Address”**（SMTP （电子邮件）服务器 IP 地址）字段中，输入要在配置中使用的 SMTP 服务器的有效 IP 地址或 FQDN （完全限定域名）。

   注：要成功发送检测电子邮件，必须在 “Email Alert Settings”（电子邮件警报设置）页中配置 “SMTP (email) Server IP Address”（SMTP [电子邮件] 服务器 IP 地址）。在出现平台事件时， SMTP 服务器使用设置的 IP 地址与 iDRAC6 进行通信，以发送电子邮件警报。

7 单击 **“Apply”**（应用）。将保存设置。

使用 Web 界面配置 IPMI

1 使用支持的 Web 浏览器登录远程系统。

2 配置 LAN 上 IPMI。

   a 在 **“System”**（系统）树中，单击 **“iDRAC Settings”**（iDRAC 设置）。

   b 单击 **“Network/Security”**（网络 / 安全性）选项卡，然后单击 **“Network”**（网络）。

c 在 **"Network"**（网络）页的 **"IPMI Settings"**（IPMI 设置）下，选择 **"Enable IPMI Over LAN"**（启用 LAN 上 IPMI）并单击 **"Apply"**（应用）。

d 如果需要，更新 IPMI LAN 信道权限。

注：此设置确定可以从 LAN 上 IPMI 接口执行的 IPMI 命令。有关详情，请参阅 IPMI 2.0 规范。

在 **"IPMI Settings"**（IPMI 设置）下，单击 **"Channel Privilege Level Limit"**（信道权限级别限制）下拉菜单，选择 **"Administrator"**（管理员）、**"Operator"**（操作员）或 **"User"**（用户）并单击 **"Apply"**（应用）。

e 如果需要，设置 IPMI LAN 信道密钥。

注：iDRAC6 IPMI 支持 RMCP+ 协议。

在 **"IPMI LAN Settings"**（IPMI LAN 设置）下的 **"Encryption Key"**（密钥）字段中，键入密钥并单击 **"Apply"**（应用）。

注：密钥必须包含不超过 40 个字符的偶数个十六进制字符。

3 配置 IPMI LAN 上串行 (SOL)。

a 在 **"System"**（系统）树中，单击 **"iDRAC Settings"**（iDRAC 设置）。

b 单击 **"Network/Security"**（网络 / 安全性）选项卡，然后单击 **"Serial Over LAN"**（LAN 上串行）。

c 在 **"Serial Over LAN"**（LAN 上串行）页，选择 **"Enable Serial Over LAN"**（启用 LAN 上串行）。

d 更新 IPMI SOL 波特率。

注：要重定向 LAN 上串行控制台，应确保 SOL 波特率与 Managed System 的波特率相同。

e 单击 **"Baud Rate"**（波特率）下拉菜单，选择相应的波特率，并单击 **"Apply"**（应用）。

f 更新需要的最小权限。此属性定义使用 **"Serial Over LAN"**（LAN 上串行）功能所需的最小用户权限。

单击 **"Channel Privilege Level Limit"**（信道权限级别限制）下拉菜单，并随后选择 **"User"**（用户）、**"Operator"**（操作员）或 **"Administrator"**（管理员）。

g 单击 **"Apply"**（应用）。

4 配置 IPMI 串行。

a 在 **"Network/Security"**（网络 / 安全性）选项卡中，单击 **"Serial"**（串行）。

b 在 **"Serial"**（串行）菜单中，将 IPMI 串行连接模式更改为相应设置。

在 **"IPMI Serial"**（IPMI 串行）下，单击 **"Connection Mode Setting"**（连接模式设置）下拉菜单，选择相应的模式。

c 设置 IPMI 串行波特率。

单击 **"Baud Rate"**（波特率）下拉菜单，选择相应的波特率，并单击 **"Apply"**（应用）。

d 设置 **"Channel Privilege Level Limit"**（信道权限级别限制）和 **"Flow Control"**（流控制）。

e 单击 **"Apply"**（应用）。

f 确保在 Managed System 的 BIOS 设置程序中正确设置了串行 MUX。

- 重新启动系统。
- 在开机自检期间，按 <F2> 进入 BIOS 设置程序。
- 导航到 **"Serial Communication"**（串行通信）。
- 在 **"Serial Connection"**（串行连接）菜单中，确保 **"External Serial Connector"**（外部串行连接器）设置为 **"Remote Access Device"**（远程访问设备）。
- 保存并退出 BIOS 设置程序。
- 重新启动系统。

如果 IPMI 串行处于终端模式，可以配置以下其它设置：

- 删除控制
- 回声控制
- 行编辑
- 新行序列
- 输入新行序列

有关这些属性的详情，请参阅 IPMI 2.0 规范。有关终端模式命令的其它信息，请参阅 **dell.com/support/manuals** 上的《Dell OpenManage Baseboard Management Controller 公用程序用户指南》。

配置 iDRAC6 用户

有关详细信息，请参阅 “第 115 页上的 “添加和配置 iDRAC6 用户””。

使用 SSL 和数字证书保证 iDRAC6 通信安全

本节提供关于 iDRAC 中包括的以下数据安全性功能的信息：

- 安全套接字层 (SSL)
- 证书签名请求 (CSR)
- 通过基于 Web 的界面访问 SSL
- 生成 CSR
- 上载服务器证书
- 查看服务器证书

安全套接字层 (SSL)

iDRAC6 包括一个 Web Server，它配置为使用业界标准的 SSL 安全协议以通过网络传输加密数据。基于公共密钥和私人密钥加密技术构建的 SSL 是广泛接受的技术，用于在客户端和服务器之间提供验证和加密的通信以防止网络上的窃听现象。

启用 SSL 的系统可以执行以下任务：

- 向启用 SSL 的客户端验证自身
- 允许客户端向服务器验证自身
- 允许两个系统建立加密连接

此加密过程提供高级别数据保护。iDRAC6 使用 128 位 SSL 加密标准，这是北美 Internet 浏览器常用的最安全加密方式。

默认情况下， iDRAC6 Web Server 包括 Dell 自签名的 SSL 数字证书 （服务器 ID）。为确保 Internet 的高安全性，使用公认认证机构签署的证书更换 Web Server SSL 证书。要开始获取签署证书，可以使用 iDRAC6 Web 界面提供公司信息来生成证书签名请求 (CSR)。随后可以将生成的 CSR 提交给认证机构 (CA)，比如 VeriSign 或 Thawte。

证书签名请求 (CSR)

CSR 是发送至 CA 的数字请求，用于获得安全服务器证书。安全服务器证书使服务器客户端能够信任所连服务器的身份并能够与服务器协商加密会话。

认证机构是 IT 行业认可的企业实体，可满足高标准的可靠性审查、识别和其它重要安全标准。例如，Thwate 和 VeriSign 均为 CA。CA 收到 CSR 后，将对 CSR 中包含的信息进行检查和验证。如果申请者符合 CA 的安全标准， CA 将向申请者颁发数字签名的证书，以在通过网络和 Internet 进行事务处理时唯一标识该申请者。

CA 批准了 CSR 并发送证书后，应将证书上载到 iDRAC6 固件。存储在 iDRAC6 固件中的 CSR 信息必须与证书中包含的信息匹配。

通过基于 Web 的界面访问 SSL

1. 单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）。
2. 单击 **SSL** 以打开 **SSL** 页。

使用 **SSL** 页执行以下一个选项：

- 生成证书签名请求 (CSR) 以发送到 CA。 CSR 信息存储在 iDRAC6 固件中。
- 上载服务器证书。
- 查看服务器证书。

表 4-10 说明了 **SSL** 页的以上选项。

表 4-10. SSL 页选项

字段	说明
"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）	使用此选项可以生成 CSR 发送给 CA 以请求安全 Web 证书。 **注：**每个新的 CSR 都会改写固件上任何原有的 CSR。固件中的 CSR 必须匹配 CA 返回的证书。
"Upload Server Certificate"（上载服务器证书）	使用此选项可以上载您公司拥有的现有证书并用来控制对 iDRAC6 的访问。 **注：**iDRAC6 仅接受 Base 64 编码的 X509 证书。不接受 DER 编码证书。上载新证书会替换 iDRAC6 中原有的默认证书。
View Server Certificate（查看服务器证书）	使用此选项可以查看现有服务器证书。

生成证书签名请求

1 在 SSL 页上，选择 **"Generate Certificate Signing Request (CSR)"**（生成证书签名请求 [CSR]）并单击 **"Next"**（下一步）。

2 在 **"Generate Certificate Signing Request (CSR)"**（生成证书签名请求 [CSR]）页上输入每个 CSR 属性值。表 4-11 说明了 CSR 属性。

3 单击 **"Generate"**（生成）创建 CSR 并将其下载到本地计算机，然后保存到指定目录。

4 单击 **"Go Back to SSL Main Menu"**（返回 SSL 主菜单）返回到 SSL 页。

表 4-11. 生成证书签名请求 (CSR) 属性

字段	说明
Common Name（常用名）	认证的确切名称 （通常是 iDRAC 的域名，例如，xyzcompany.com）。字母数字字符、连字符和句点有效。
Organization Name（组织名称）	与组织相关的名称 （例如， XYZ 公司）。字母数字字符、连字符和句点有效。
Organization Unit（组织单位）	与诸如部门等组织单位相关的名称 （例如，信息技术）。字母数字字符、连字符和句点有效。
Locality （地点）	认证的实体所在的城市或其它位置 （例如，朗得罗克 [Round Rock]）。字母数字字符、连字符和句点有效。
状态名称	申请认证的实体所在的州或省 （例如，德克萨斯州 [Texas]）。字母数字字符、连字符和句点有效。不要使用缩写。
"Country Code"（国家 / 地区代码）	申请认证的实体所在的国家 / 地区名。
Email （电子邮件）	与 CSR 相关的电子邮件地址。键入公司的电子邮件地址或与 CSR 相关的任何电子邮件地址。此字段可选。

上载服务器证书

1 在 SSL 页中，选择 **"Upload Server Certificate"**（上载服务器证书）并单击 **"Next"**（下一步）。

将显示 **"Upload Server Certificate"**（上载服务器证书）页。

2 在 **"File Path"**（文件路径）字段的 **"Value"**（值）字段中键入证书路径，或单击 **"Browse"**（浏览）导航至证书文件。

注：File Path （文件路径）值显示上载的证书的相对文件路径。必须键入绝对文件路径，包括全路径和完整文件名及文件扩展名。

3 单击 **"Apply"**（应用）。

4 单击 **"Go Back to SSL Main Menu"**（返回 SSL 主菜单）返回到 **"SSL Main Menu"**（SSL 主菜单）页。

查看服务器证书

1 在 SSL 页中，选择 **"View Server Certificate"**（查看服务器证书）并单击 **"Next"**（下一步）。

"View Server Certificate"（查看服务器证书）页显示已上载到 iDRAC 的服务器证书。

表 4-12 说明了 **"Certificate"**（证书）表中列出的字段及相关说明。

2 单击 **"Go Back to SSL Main Menu"**（返回 SSL 主菜单）返回到 **"SSL Main Menu"**（SSL 主菜单）页。

表 4-12. 认证信息

字段	说明
序列号	证书序列号
"Subject Information"（主题信息）	按主题输入的证书属性
"Issuer Information"（颁发者信息）	按颁发者返回的证书属性
"Valid From"（有效期自）	证书的颁发日期
"Valid To"（有效期至）	证书的期满日期

配置和管理 Active Directory

使用该页可以配置和管理 Active Directory 设置。

注：您必须具有 “**Configure iDRAC**”（配置 iDRAC）权限才能使用或配置 Active Directory。

注：配置或使用 Active Directory 功能之前，确保配置 Active Directory 服务器以便与 iDRAC6 进行通信。

注：有关 Active Directory 配置和如何配置扩展架构或标准架构的 Active Directory 的详细信息，请参阅第 129 页上的 “使用 iDRAC6 Directory Service”。

要访问 **“Active Directory Configuration and Management”**（Active Directory 配置和管理）页：

1. 单击 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）。
2. 单击 **Active Directory** 以打开 **“Active Directory Configuration and Management”**（Active Directory 配置和管理）页。

   表 4-13 列出了 **“Active Directory Configuration and Management”**（Active Directory 配置和管理）页选项。
3. 单击 **“Configure Active Directory”**（配置 Active Directory）配置 Active Directory。有关配置信息的详情，请参阅第 143 页上的 “使用 iDRAC6 目录服务”。
4. 单击 **“Test Settings”**（检测设置）使用您指定的设置检测 Active Directory 配置。有关使用 “Test Settings”（检测设置）选项的详情，请参阅第 143 页上的 “使用 iDRAC6 目录服务”。

表 4-13. Active Directory 配置和管理页选项

属性	说明
常见设置	
“Active Directory Enabled”（启用 Active Directory）	指定是启用还是禁用 Active Directory。
“Single Sign-On Enabled”（单一登录已启用）	指定是启用还是禁用单一登录。如果启用，则不用输入域用户验证凭据，比如用户名和密码，就可登录 iDRAC6。选中该复选框以启用登录。

表 4-13. Active Directory 配置和管理页选项 *（续）*

属性	说明
"Schema Selection"（架构选择）	指定配合 Active Directory 使用标准架构还是扩展架构。 **注：在此版本中，如果 Active directory 配置为使用扩展架构，则不支持基于智能卡的双重验证 (TFA) 功能。对于标准架构和扩展架构都支持单一登录 (SSO) 功能。**
"User Domain Name"（用户域名）	该值最多含有 40 个用户域条目。如果已配置，用户域名列表将显示在登录页中，作为登录用户可从中选择的下拉式菜单。如果不配置， Active Directory 用户仍然能够通过按 user_name@domain_name、domain_name/user_name 或 domain_name\user_name 格式输入用户名进行登录。
超时	指定等待 Active Directory 查询完成需要的秒数。默认值为 120 秒钟。
利用 DNS 查找域控制器	选择 **"Look Up Domain Controllers with DNS"**（利用 DNS 查找域控制器）选项可从 DNS 查找中获得 Active Directory 域控制器。选择此选项后，域控制器服务器地址 1-3 被忽略。选择 **"User Domain from Login"**（登录的用户域）可使用登录用户的域名进行 DNS 查找。否则，选择 **"Specify a Domain"**（指定一个域）并输入 DNS 查找所使用的域名。 iDRAC6 会逐一尝试连接每个地址 （前 4 个地址由 DNS 查找返回），直到成功建立连接为止。 如果选择 **"Extended Schema"**（扩展架构），域控制器是 iDRAC6 设备对象和关联对象所在的地址。如果选择 **"Standard Schema"**（标准架构），域控制器是用户帐户和角色组所在的地址。
"Domain Controller Server Address 1-3 (FQDN or IP)"（域控制器服务器地址 1-3 [FQDN 或 IP]）	指定域控制器的完全限定域名 (FQDN) 或 IP 地址。要求至少配置 3 个地址之一。iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。如果选择扩展架构，这些地址是 iDRAC6 设备对象和关联对象所在的域控制器的地址。如果选择标准架构，这些地址是用户帐户和角色组所在的域控制器的地址。

表 4-13. Active Directory 配置和管理页选项 *（续）*

属性	说明
“Certificate Validation Enabled”（启用证书验证）	连接到 Active Directory 期间， iDRAC6 使用安全套接字层 (SSL)。默认情况下，在安全套接字层 (SSL) 握手过程中，iDRAC6 使用在 iDRAC6 中载入的 CA 证书验证域控制器的安全套接字层 (SSL) 服务器证书，并提供强大的安全保护。如果要进行检测或系统管理员选择信任安全边界内的域控制器而不验证其安全套接字层 (SSL) 证书，则可以禁用证书验证。此选项指定是启用还是禁用证书验证。
“Active Directory CA Certificate”（Active Directory CA 证书）	
“Certificate”（证书）	签署所有域控制器的安全套接字层 (SSL) 服务器证书的认证机构的证书。
Extended Schema Settings（扩展架构设置）	**“iDRAC Name”**（iDRAC 名称）：指定唯一识别 Active Directory 中 iDRAC 的名称。该值默认为 NULL。 **“iDRAC Domain Name”**（iDRAC 域名）：Active Directory iDRAC 对象所在的域的 DNS 名称 （字符串）。该值默认为 NULL。 只有 iDRAC 配置为使用扩展 Active Directory 架构时，才会显示这些设置。

表 4-13. Active Directory 配置和管理页选项 *（续）*

属性	说明
Standard Schema Settings（标准架构设置）	**"Global Catalog Server Address 1-3 (FQDN or IP)"**（全局编录服务器地址 1-3 [FQDN 或 IP]）：指定全局编录服务器的完全限定域名 (FQDN) 或 IP 地址。要求至少配置 3 个地址之一。 iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。仅当用户帐户和角色组位于不同域中时，标准架构才需要全局编录服务器。 **"Role Groups"**（角色组）：指定与 iDRAC6 关联的角色组的列表。 **"Group Name"**（组名称）：指定标识 Active Directory 中与 iDRAC6 关联的角色组的名称。 **"Group Domain"**（组域）：指定组域。 **"Group Privilege"**（组权限）：指定组权限级别。 只有 iDRAC 配置为使用标准 Active Directory 架构时，才会显示这些设置。 选择 **"Look Up Global Catalog Servers with DNS"**（使用 DNS 查找全局编录服务器）选项并输入用于 DNS 查找的 **"Root Domain Name"**（根域名）来获取 Active Directory 全局编录服务器。选择此选项后，**全局编录服务器地址 1-3** 将被忽略。 iDRAC6 会尝试逐一连接到每个地址 （由 DNS 查找返回的前 4 个地址），直到成功建立连接为止。仅当用户帐户和角色组位于不同域中时，标准架构才需要全局编录服务器。

配置并管理通用 LDAP

iDRAC6 提供了一个通用方案，支持基于轻型目录访问协议 (LDAP) 的验证。此功能无需服务目录的任何架构扩展。有关配置通用 LDAP 目录服务的信息，请参阅第 161 页上的 "通用 LDAP 目录服务"。

配置 iDRAC6 服务

注：要修改这些设置，必须具有 "Configure iDRAC"（配置 iDRAC）权限。

1 单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）。然后，单击 **"Services"**（服务）选项卡以显示 **"Services"**（服务）配置页。

2 根据需要配置以下服务：

- 本地配置 — 请参阅表 4-14。
- Web Server — 请参阅表 4-15 了解 Web Server 设置。
- SSH — 请参阅表 4-16 了解 SSH 设置。
- Telnet — 请参阅表 4-17 了解 Telnet 设置。
- 远程 RACADM — 请参阅表 4-18 了解远程 RACADM 设置。
- SNMP 代理 — 请参阅表 4-19 了解 SNMP 设置。
- 自动系统恢复 (ASR) 代理 — 请参阅表 4-20 了解 ASR 代理设置。

3 单击 **"Apply"**（应用）应用 **"Service"**（服务）页设置。

表 4-14. 本地配置

设置	说明
"Disable the iDRAC Local Configuration using option ROM"（使用 option ROM 禁用 iDRAC 的本地配置）	使用 option ROM 禁用 iDRAC 的本地配置。 Option ROM 位于 BIOS 中，提供了用户界面引擎以允许 BMC 和 iDRAC 配置。option ROM 会提示按 <Ctrl+E> 以进入设置模块。
"Disable the iDRAC Local Configuration using RACADM"（使用 RACADM 禁用 iDRAC 的本地配置）	使用本地 RACADM 禁用 iDRAC 的本地配置。

表 4-15. Web Server 设置

设置	说明
Enabled（启用）	启用或禁用 iDRAC6 Web Server。选中后，复选框表示 Web Server 已启用。默认值为**已启用**。
Max Sessions（最大会话数）	此系统允许的最大 Web Server 同时会话数。此字段不可编辑。可以同时进行的最大会话数是五。
"Active Sessions"（激活的会话数）	系统上的当前会话数，小于等于 **"Max Sessions"**（最大会话数）的值。此字段不可编辑。

表 4-15. Web Server 设置 *（续）*

设置	说明
超时	允许连接保持闲置的秒数。达到超时时将取消会话。对超时设置的更改会直接影响并终止当前的 Web 界面会话。 Web Server 也将进行重设。请等待几分钟，然后再打开新的 Web 界面会话。超时范围为 60 至 10800 秒。默认值为 1800 秒。
HTTP Port Number（HTTP 端口号）	iDRAC6 侦听浏览器连接所在的端口。默认为 80。
HTTPS Port Number（HTTPS 端口号）	iDRAC6 侦听安全浏览器连接所在的端口。默认为 443。

表 4-16. SSH 设置

设置	说明
Enabled（启用）	启用或禁用 SSH。选中后，就启用 SSH。
Max Sessions（最大会话数）	此系统允许的最大同时 SSH 会话数。不能编辑此字段。 **注：**iDRAC6 支持同时最多 2 个 SSH 会话。
"Active Sessions"（激活的会话数）	系统上的当前 SSH 会话数，小于等于 **"Max Sessions"**（最大会话数）的设置。不能编辑此字段。
超时	Secure Shell 闲置超时，以秒为单位。超时范围为 60 至 10800 秒。输入 0 秒将禁用超时功能。默认为 1800。
端口号	iDRAC6 侦听 SSH 连接所在的端口。默认为 22。

表 4-17. Telnet 设置

设置	说明
Enabled（启用）	启用或禁用 Telnet。选中后，就启用 Telnet。
Max Sessions（最大会话数）	此系统允许的最大同时 Telnet 会话数。不能编辑此字段。 **注：**iDRAC6 支持同时最多 2 个 Telnet 会话。
"Active Sessions"（激活的会话数）	系统上的当前 Telnet 会话数，小于等于 **"Max Sessions"**（最大会话数）的设置。不能编辑此字段。
超时	Telnet 闲置超时，以秒为单位。超时范围为 60 至 10800 秒。输入 0 秒将禁用超时功能。默认为 1800。
端口号	iDRAC6 侦听 Telnet 连接所在的端口。默认为 23。

表 4-18. 远程 RACADM 设置

设置	说明
Enabled （启用）	启用 / 禁用远程 RACADM。选中后，就启用远程 RACADM。
“Active Sessions” （激活的会话数）	系统上的当前远程 RACADM 会话数。不能编辑此字段。

表 4-19. SNMP 设置

设置	说明
Enabled （启用）	启用 / 禁用 SNMP。选中后，就启用 SNMP。
“SNMP Community Name” （SNMP 团体名称）	启用 / 禁用 SNMP 团体名称。选中后，就启用 SNMP 团体名称。定义要使用的 SNMP 团体字符串。团体名称长度最多为 31 个字符 （不带空格）。默认为 public。

表 4-20. 自动系统恢复代理设置

设置	说明
Enabled （启用）	启用 / 禁用自动系统恢复代理。选中后，就启用自动系统恢复代理。

更新 iDRAC6 固件 / 系统服务恢复映像

注：如果 iDRAC6 固件出现损坏 （如果 iDRAC6 固件更新进度在完成前被中断，则有可能会发生），则可以使用 iDRAC6 Web 界面恢复 iDRAC6。

注：默认情况下，固件更新将保留当前 iDRAC6 设置。在更新过程中，可以选择重设 iDRAC6 配置为工厂默认值。如果将配置设置为工厂默认值，必须使用 iDRAC6 配置公用程序配置网络。

1. 打开 iDRAC6 基于 Web 的界面并登录到远程系统。
2. 单击 **“iDRAC Settings”**（iDRAC 设置），然后单击 **“Update”**（更新）选项卡。
3. 在 **“Upload/Rollback (Step 1 of 3)”**（上载 / 回滚（第 1 步，共 3 步））页中，单击 **“Browse”**（浏览）选择从 support.dell.com 下载的固件映像或系统服务恢复映像。

注：如果运行 Firefox，文本光标不会显示在 “**Firmware Image**”（固件映像）字段中。

例如：

`C:\Updates\V1.0\<`*映像名称*`>`。

或

`\\192.168.1.10\Updates\V1.0\<`*映像名称*`>`

默认固件映像名称是 **firmimg.d6**。

4 单击 **“Upload”**（上载）。

该文件将上载到 iDRAC6。 This process may take several minutes to complete.（完成此过程可能需要几分钟。）

在该过程完成之前，将显示以下信息：

“`File upload in progress...`”（正在上载文件 ...）

5 在 **“Status (page 2 of 3)”**（状况 [第 2 页，共 3 页]）页上，您将看到对上载的映像文件进行的验证结果。

- 如果系统恢复映像文件成功上载并通过所有验证检查，将显示系统恢复映像文件名称。如果固件映像已上载，将显示当前固件版本和新固件版本。

  或

- 如果映像没有成功上载，或没有通过验证检查，将显示相应错误信息，而且更新将返回到 **“Upload/Rollback (Step 1 of 3)”**（上载 / 回滚 [第 1 步，共 3 步]）页。您可尝试再次更新 iDRAC6 或单击 **“Cancel”**（取消）将 iDRAC6 重设为正常工作模式。

6 在固件映像的情况下，使用 **“Preserve Configuration”**（保留配置）可以选择保留或清除现有 iDRAC6 配置。默认情况下会选择此选项。

注：如果取消选择 “**Preserve Configuration**”（保留配置）复选框，iDRAC6 将会重设为默认设置。在默认设置中， LAN 已启用并具有静态 IPv4 地址。用户将不能登录到 iDRAC6 Web 界面。必须在 BIOS 开机自检过程中使用 iDRAC6 配置公用程序重新配置 LAN 设置。

7 单击 **“Update”**（更新）开始更新过程。

8 在 **“Updating (Step 3 of 3)”**（正在更新 [第 3 步，共 3 步]）页中，将看到更新状况。更新进度以百分比衡量，将显示在 **“Progress”**（进度）列中。

注：处于更新模式时，即使退出此页，更新过程也继续在后台进行。

如果固件更新成功，iDRAC6 将自动重设。应关闭当前浏览器窗口，再使用新的浏览器窗口重新连接到 iDRAC6。如果出现错误，将显示相应错误信息。

如果系统服务恢复更新成功 / 失败，将显示相应状况信息。

iDRAC6 固件回滚

iDRAC6 具有保留两个同时固件映像的预防措施。可以选择从选定的固件映像引导或回滚到选定的固件映像。

1 打开 iDRAC6 基于 Web 的界面并登录到远程系统。

单击 **"System"**（系统）→ **"iDRAC Settings"**（iDRAC 设置），然后单击 **"Update"**（更新）选项卡。

2 在 **"Upload/Rollback (Step 1 of 3)"**（上载 / 回滚 [第 1 步，共 3 步]）页中，单击 **"Rollback"**（回滚）。**"Status (Step 2 of 3)"**（状况 [第 2 步，共 3 步]）页中显示当前固件版本和回滚固件版本。

使用 **"Preserve Configuration"**（保留配置）可以选择保留或清除现有 iDRAC6 配置。默认情况下会选择此选项。

注：如果取消选择 **"Preserve Configuration"**（保留配置）复选框，iDRAC6 将会重设为默认设置。在默认设置中，LAN 已启用。您将不能登录到 iDRAC6 Web 界面。您必须在 BIOS 开机自检过程中使用 iDRAC6 配置公用程序或使用 RACADM 命令 （在服务器本地上提供）重新配置 LAN 设置。

3 单击 **"Update"**（更新）开始固件更新过程。

在 **"Updating (Step 3 of 3)"**（正在更新 [第 3 步，共 3 步]）页中，将看到回滚操作状况。进度以百分比衡量，将显示在 **"Progress"**（进度）列中。

注：处于更新模式时，即使退出此页，更新过程也继续在后台进行。

如果固件更新成功，iDRAC6 将自动重设。应关闭当前浏览器窗口，再使用新的浏览器窗口重新连接到 iDRAC6。

远程系统日志

iDRAC6 Enterprise 提供远程系统日志功能，该功能允许您远程写入 RAC 日志和系统事件日志 (SEL) 到外部系统日志服务器。您可以从中央日志读取整个服务器场日志。

远程系统日志协议不需要任何用户验证。要使日志输入远程系统日志服务器中，应确保在 iDRAC6 和远程系统日志服务器间有正确的网络连接，并且远程系统日志服务器运行在 iDRAC6 所在的网络上。远程系统日志的条目是发送到远程系统日志服务器系统日志端口的用户数据报协议 (UDP) 数据包。如果出现网络故障，iDRAC6 将不会再次发送相同日志。当 iDRAC6 的 RAC 日志和 SEL 日志记录日志时，远程日志记录也会实时进行。

可以通过远程 Web 界面启用远程系统日志：

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 Web 界面。
3. 在系统树中，选择 **"System"**（系统）→ **"Setup"**（设置）选项卡 → **"Remote Syslog Settings"**（远程系统日志设置）。将会显示 **"Remote Syslog Settings"**（远程系统日志设置）屏幕。

表 4-21 列出远程系统日志设置。

表 4-21. 远程系统日志设置

属性	说明
"Remote Syslog Enabled"（已启用远程系统日志）	选择此选项可启用指定服务器上系统日志的传送和远程捕获。启用系统日志后，新的日志条目会发送到系统日志服务器。
系统日志服务器 1 - 3	输入远程系统日志服务器地址以记录 iDRAC6 信息，比如 SEL 日志和 RAC 日志。系统日志服务器地址允许字母数字、-、 .、 : 和 _ 符号。
端口号	输入远程系统日志服务器的端口号。端口号应介于 1 到 65535 之间。默认为 514。

注：远程系统日志协议定义的严重性级别有别于标准 IPMI 系统事件日志 (SEL) 的严重性级别。因此报告的所有 iDRAC6 远程系统日志条目在系统日志服务器中都带有严重性级别注意。

以下示例说明更改远程系统日志设置的配置对象和 RACADM 命令用法：

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogEnable [1/0] ; 默认为 0

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer1 <服务器名 1> ; 默认为空

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer2 <服务器名 2>; 默认为空
```

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer3 <服务器名 3>; 默认为空

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPort <端口号>; 默认为 514
```

“First Boot Device”（第一个引导设备）

此功能允许选择系统的第一个引导设备并启用 **“Boot Once”**（引导一次）。在下一次以及以后的重新引导时，系统会从所选设备引导，并且该设备会一直是 BIOS 引导次序的第一个引导设备，直到从 iDRAC6 GUI 或 BIOS 引导顺序中再次更改为止。

可以通过远程 Web 界面选择第一个引导的设备：

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 Web 界面。
3. 在系统树中，选择 **“System”**（系统）→ **“Setup”**（设置）→ **“First Boot Device”**（第一个引导设备）。将会显示 **“First Boot Device”**（第一个引导设备）屏幕。

表 4-22 列出 **“First Boot Device”**（第一个引导设备）设置。

表 4-22. “First Boot Device”（第一个引导设备）

属性	说明
“First Boot Device”（第一个引导设备）	从下拉列表选择第一个引导设备。在下一次以及以后的重新引导时，系统会从所选设备引导。
“Boot Once”（引导一次）	选中 = 启用；取消选中 = 禁用。选择此选项在下一次引导时从所选设备引导。因此，系统会从 BIOS 引导次序的第一个引导设备引导。

Remote File Share （远程文件共享）

iDRAC6 的远程文件共享 (RFS) 功能允许指定网络共享上的 ISO 或 IMG 映像文件，并通过网络文件系统 (NFS) 或通用因特网文件系统 (CIFS) 像 CD/DVD 或软盘一样安装它，使其作为受管服务器操作系统的虚拟驱动器。

CIFS 共享映像路径的格式为：

//<IP 地址或域名>/<映像路径>

NFS 共享映像路径的格式为：

<*IP 地址*>:/<*映像路径*>

注：如果使用 NFS，确保提供包括映像文件扩展名的确切 <*映像路径*>，因为它区分大小写。

注：<*IP 地址*> 必须是 IPv4 地址。目前不支持 IPv6 地址。

如果用户名包含域名，则输入的用户名必须采用 <*用户名*>@<*域*> 格式。例如， user1@dell.com 是有效的用户名，而 dell\user1 不是。

带有 IMG 扩展名的文件名被重定向为虚拟软盘，而带有 ISO 扩展名的文件名被重定向为虚拟 CDROM。远程文件共享只支持 .IMG 和 .ISO 映像文件格式。

RFS 功能利用 iDRAC6 中的基本虚拟介质实施。必须拥有虚拟介质权限才能安装 RFS。如果虚拟驱动器已被虚拟介质所使用，则该驱动器不能作为 RFS 安装，反之亦然。要让 RFS 正常工作， iDRAC6 中的虚拟介质必须处于*连接*或*自动连接*模式。

RFS 连接状态可在 iDRAC6 日志中找到。一旦连接后，即使注销 iDRAC6，已安装虚拟驱动器的 RFS 也不会断开。如果 iDRAC6 重置或网络连接故障，则 RFS 连接关闭。 iDRAC6 中的 GUI 和命令行选项也可以关闭 RFS 连接。

注：iDRAC6 vFlash 功能与 RFS 没有关联。

要通过 iDRAC6 Web 界面启用远程文件共享，请执行以下操作：

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 Web 界面。
3. 选择 **"System"**（系统）→ **"Remote File Share"**（远程文件共享）选项卡。

   此时将显示 **"Remote File Share"**（远程文件共享）屏幕。

表 4-23 列出远程文件共享设置。

表 4-23. 远程文件服务器设置

属性	说明
用户名	NFS/CIFS 文件系统的连接用户名。
Password（密码）	NFS/CIFS 文件系统的连接密码。
Image File Path（映像文件路径）	要通过远程文件共享功能共享的文件路径。

表 4-23. 远程文件服务器设置 *（续）*

属性	说明
状况	“Connected”（已连接）：文件已共享。 “Not Connected”（未连接）：文件未共享。 “Connecting”（正在连接）：正在连接到共享。

单击 **“Connect”**（连接）可连接到 RFS。成功建立连接后，**“Connect”**（连接）就处于禁用状态。

注：即使已配置远程文件共享，鉴于安全原因，GUI 也不会显示此信息。

对于远程文件共享，远程 RACADM 命令是：

`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：“User Name”（用户名）和 “Password”（密码）支持的最大字符数是 40，“Image File Path”（映像文件路径）的最大字符数是 511。所有字符，包括字母数字和特殊字符，都允许用于这三个字段，但以下字符除外：

- '（单引号）
- "（双引号）
- ,（逗号）
- <（小于号）
- >（大于号）

内部双 SD 模块

内部双 SD 模块 (IDSDM) 使用另一个 SD 卡镜像第一个 SD 卡的内容，在管理程序 SD 卡上提供冗余。通过在系统 BIOS 设置的 **"Integrated Devices"**（集成设备）屏幕中将 **"Redundancy"**（冗余）选项设置为 **"Mirror mode"**（镜像模式），可以将第二个 SD 卡与其它 SD 卡一起设置为 IDSDM。有关 IDSDM 的 BIOS 选项的详情，请参阅 Dell 支持网站 dell.com/support/manuals 上的 《硬件用户手册》。

注：在 BIOS 设置的 "Integrated Devices"（集成设备）屏幕中，"Internal USB Port"（内部 USB 端口）选项必须设置为 "On"（开）。如果此选项设置为 "Off"（关），IDSDM 不会对系统显示为引导设备。

两个 SD 卡之一可以是主卡。例如，如果在 IDSDM 中安装了两个 SD 卡，将系统的交流电源断开，则 SD1 视为活动卡或主卡。 SD2 是备用卡，所有文件系统 IDSDM 写入将写入这两个卡，但仅从 SD1 读取。任何时候 SD1 出现故障或卸下时， SD2 都会自动变为活动 （主）卡。vFlash SD 卡在镜像模式时处于禁用状态。

表 4-24. IDSDM 状态

IDSDM - 镜像模式	SD1 卡	SD2 卡	vFlash SD 卡
Enabled （启用）	活动	活动	非活动
Disabled （禁用）	活动	非活动	活动

使用 iDRAC 可以查看 IDSDM 的状况、运行状况和可用性。

SD 卡冗余状况和故障事件记录到 SEL，显示在 LCD 上，如果启用了警报，将生成 PET 警报。

使用 GUI 查看内部双 SD 模块状况

1. 登录 iDRAC Web GUI。
2. 单击 **"Removable Flash Media"**（可移动闪速更新介质）。将会显示 **"Removable vFlash Media"**（可移动 vFlash 介质）页。此页显示以下两部分：

- **"Internal Dual SD Module"**（内部双 SD 模块）— 仅当 IDSDM 处于冗余模式时显示。**"Redundancy Status"**（冗余状况）显示为 **"Full"**（完全）。如果此部分不存在，则卡处于非冗余模式状态。有效的 **"Redundancy Status"**（冗余状况）指示是：

- **"Full"**（完全）— SD 卡 1 和 2 正常工作。
- **"Lost"**（掉失）— 任一 SD 卡或两个 SD 卡工作不正常。

- **"Internal SD Module Status"**（内部 SD 模块状况）— 显示 SD1、SD2 和 vFlash 卡的 SD 卡状态，提供以下信息：
  - "Status"（状态）：
    -  — 表示卡正常。
    -  — 表示卡脱机或写保护。
    -  — 表示发出了警报。
  - "Location"（位置）— SD 卡的位置。
  - "Online Status"（联机状况）— SD1、 SD2 和 vFlash 卡可以处于表 4-25 中列出的一种状态。

表 4-25. SD 卡状态

SD 卡	State（状态）	说明
SD1 和 SD2	Boot（引导）	控制器正在加电。
	活动	该卡已准备好接受 SD 读 / 写请求。
	待机	卡是辅助卡。正在接收所有 SD 写入的副本。
	故障	在 SD 卡读取或写入过程中报告了错误。
	不存在	没有检测到 SD 卡。
	脱机	在引导时，卡的卡标识 (CID) 签名与非易失性 (NV) 存储值不同，或卡是正在进行的复制操作的目标。
	写保护	卡已通过 SD 卡上的物理闩锁进行写保护。IDSDM 不能使用写保护的卡。
vFlash	活动	该卡已准备好接受 SD 读 / 写请求。
	不存在	没有检测到 SD 卡。

5

高级 iDRAC6 配置

本节提供有关高级 iDRAC6 配置的信息，推荐具备高级系统管理知识的用户以及那些希望根据特定需要自定义 iDRAC6 环境的用户进行阅读。

开始之前

应已完成 iDRAC6 硬件和软件的基本安装和设置。有关详情，请参阅第 31 页上的 “iDRAC6 的基本安装”。

配置 iDRAC6 以通过 SSH/Telnet 远程查看串行输出

您可以通过执行以下步骤，为远程串行控制台配置 iDRAC6：

首先，配置 BIOS 以启用串行控制台：

1. 打开或重新启动系统。
2. 看到下列信息时立即按 <F2>：

   `<F2> = System Setup`

3. 向下滚动并通过按 <Enter> 选择 **“Serial Communication”**（串行通信）。
4. 如下设置 **“Serial Communication”**（串行通信）屏幕选项：

   串行通信 . . . . 开，通过 `com2` 进行串行重定向

   注：只要串行端口地址字段中的串行设备 2 也设置为 com1，您就可以将串行通信设置为 **“On with serial redirection via com1”**（开，通过 com1 进行串行重定向）。

   串行端口地址 . . . . 串行设备 `1 = com1`、串行设备 `2 = com2`

   外部串行连接器 . . . . 串行设备 `1`

   故障安全波特率 . . . .`115200`

   远程终端类型 . . . .`vt100/vt220`

   引导后重定向 . . . . 已启用

然后，选择 **"Save Changes"**（保存更改）。

5 按 <Esc> 退出**系统设置**程序，并完成系统设置程序配置。

配置 iDRAC6 设置以启用 SSH/Telnet

接下来，配置 iDRAC6 设置，以启用 SSH/Telnet，而这可通过 RACADM 或 iDRAC6 Web 界面实现。

要配置 iDRAC6 设置以通过 RACADM 启用 SSH/Telnet，请运行以下命令：

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

您也可以远程运行 RACADM 命令；请参阅第 100 页上的 "远程使用 RACADM"。

要配置 iDRAC6 设置以通过 iDRAC6 Web 界面启用 SSH/Telnet，请执行以下步骤：

1 展开 **"System"**（系统）树并单击 **"iDRAC Settings"**（iDRAC 设置）。

2 单击 **"Network Security"**（网络 / 安全性）选项卡，然后单击 **"Services"**（服务）。

3 在 **SSH** 或 **Telnet** 部分下选择 **"Enabled"**（已启用）。

4 单击 **"Apply Changes"**（应用更改）。

下一步是通过 Telnet 或 SSH 连接到 iDRAC6。

通过 Telnet 或 SSH 启动文本控制台

通过 Management Station 终端软件使用 Telnet 或 SSH 登录 iDRAC6 后，可以使用 Telnet/SSH 命令 **console com2** 重定向 Managed System 文本控制台。一次只支持一个 **console com2** 客户端。

要连接到 Managed System 文本控制台，请打开 iDRAC6 命令提示符（通过 Telnet 或 SSH 会话显示）并键入：

```
console com2
```

`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 （以及最大）大小为 8192 个字符。可以使用以下命令将此数设置为更小的值：

```
racadm config -g cfgSerial -o cfgSerialHistorySize
<数字>
```

要配置 Linux 在引导期间进行控制台重定向，请参阅第 82 页上的 “为引导期间的串行控制台配置 Linux”。

使用 Telnet 控制台

使用 Microsoft Windows XP 或 Windows 2003 运行 Telnet

如果 Management Station 运行 Windows XP 或 Windows 2003，可能会在 iDRAC6 Telnet 会话中遇到字符问题。此问题可能表现为冻结登录，即回车键没有反应且密码提示符不出现。

要解决此问题，请从 Microsoft 支持网站 **support.microsoft.com** 下载热修复程序 824810。请参阅 Microsoft 知识库文章 824810 了解有关详情。

使用 Windows 2000 运行 Telnet

如果 Management Station 运行 Windows 2000，则无法通过按 <F2> 键访问 BIOS 设置。要解决此问题，推荐使用可从 Microsoft 免费下载的 Windows Services for UNIX 3.5 所带的 Telnet 客户端。转至 **microsoft.com/downloads/** 并搜索 *Windows Services for UNIX 3.5*。

为 Telnet 虚拟控制台启用 Microsoft Telnet

注：为 VT100/VT220 仿真设置 BIOS 虚拟控制台后，Microsoft 操作系统上的有些 Telnet 客户端可能不会正常显示 BIOS 设置屏幕。如果出现此问题，可以通过将 BIOS 虚拟控制台更改为 ANSI 模式来更新显示。要在 BIOS 设置菜单中执行此步骤，选择 “**Virtual Console**”（虚拟控制台）→ “**Remote Terminal Type**”（远程终端类型）→ ANSI。

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。

1. 在 **“Windows Component Services”**（Windows 组件服务）中启用 **Telnet**。
2. 连接到 Management Station 中的 iDRAC6。

   打开命令提示符，键入以下命令并按 <Enter>：

   ```
   telnet <IP 地址>:<端口号>
   ```

   其中 *IP 地址*是 iDRAC6 的 IP 地址，而*端口号*是 Telnet 端口号码（如果使用新端口）。

为 Telnet 会话配置 Backspace 键

根据 Telnet 客户端的不同，使用 <Backspace> 键可能会产生无法预料的结果。例如，会话可能会回应 ^h。不过，大多数 Microsoft 和 Linux Telnet 客户端可配置为使用 <Backspace> 键。

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

1. 打开命令提示符窗口 （如果需要）。
2. 如果尚未运行 Telnet 会话，则键入：

   ```
   telnet
   ```

   如果运行 Telnet 会话，则按 <Ctrl><]>。
3. 在提示符下键入：

   ```
   set bsasdel
   ```

   系统将显示以下信息：

   ```
   Backspace will be sent as delete.(Backspace 会作为
   Delete 发送。)
   ```

要配置 Linux Telnet 会话使用 <Backspace> 键：

1. 打开命令提示符并键入：

   ```
   stty erase ^h
   ```
2. 在提示符下键入：

   ```
   telnet
   ```

使用 Secure Shell (SSH)

保持系统设备和设备管理安全是非常重要的。嵌入式连接设备是许多业务流程的核心。如果这些设备出现问题，业务就会承担风险，这对命令行界面 (CLI) 设备管理软件提出了新的安全要求。

Secure Shell (SSH) 是一个命令行会话，具有与 Telnet 会话相同的功能，不过安全性更高。iDRAC6 支持具有密码验证功能的 SSH 版本 2。安装或更新 iDRAC6 固件时，会在 iDRAC6 上启用 SSH。

在 Management Station 上既可以使用 PuTTY 也可以使用 OpenSSH 连接到 Managed System 的 iDRAC6。如果在登录过程中出现错误， SSH 客户端就会发出一条错误信息。此信息文本依赖于客户端，不受 iDRAC6 控制。

注：OpenSSH 应该从 Windows 上的 VT100 或 ANSI 终端仿真程序中运行。在 Windows 命令提示符处运行 OpenSSH 不会得到完整的功能 （即，有些键不响应并且不显示任何图形）。

在任何时刻，只支持两个 SSH 会话。会话超时由 `cfgSsnMgtSshIdleTimeout` 属性控制，如 Dell 支持网站 **dell.com/support/manuals** 上的 《RACADM iDRAC6 和 CMC 命令行参考指南》中所述。

要在 iDRAC6 上启用 SSH，键入：

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

要更改 SSH 端口，键入：

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort
<端口号>
```

有关 `cfgSerialSshEnable` 和 `cfgRacTuneSshPort` 属性的详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《RACADM iDRAC6 和 CMC 命令行参考指南》。

iDRAC6 SSH 实现支持多种加密模式，如表 5-1 中所示。

表 5-1. 加密模式

模式类型	模式
非对称加密	Diffie-Hellman DSA/DSS 512-1024 （随机）位 / NIST 规范
对称加密	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
消息完整性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
验证	• Password （密码）

注：不支持 SSHv1。

为引导期间的串行控制台配置 Linux

以下步骤特定于 Linux GRand Unified Bootloader (GRUB)。如果使用其它引导装载程序，则需要相似的更改。

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. 找到文件的常规设置部分并添加以下两行新命令：

```
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. 如果 /etc/grub.conf 包含 splashimage 指令，应将其注释掉。

表 5-2 提供了示例 /etc/grub.conf 文件，显示在此过程中说明的更改。

表 5-2. 示例文件：/etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after
making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This
means that
#          all kernel and initrd paths are relative
to /, e.g.
```

表 5-2. 示例文件：/etc/grub.conf *（续）*

```
#          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
```

编辑 /etc/grub.conf 文件时，应遵循以下原则：

1. 禁用 GRUB 的图形界面并使用基于文本的界面；否则， GRUB 屏幕将不会显示在 RAC 虚拟控制台中。要禁用图形界面，注释掉以 `splashimage` 开头的行。
2. 要使用多个 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
   ```

   表 5-2 显示 `console=ttyS1,57600` 仅添加到第一个选项。

允许在引导后登录到虚拟控制台

按照以下说明编辑文件 /etc/inittab：

添加新行以在 COM2 串行端口上配置 agetty：

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

表 5-3 显示具有新行的示例文件。

表 5-3. 示例文件：/etc/innitab

```
#
# 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
```

表 5-3. 示例文件：/etc/innitab *（续）*

```
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

# 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"
```

表 5-3. 示例文件：/etc/innitab *（续）*

```
# 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
```

按照以下说明编辑文件 /etc/securetty：

添加新行，带有 COM2 的串行 tty 名称：

```
ttyS1
```

表 5-4 显示具有新行的示例文件。

表 5-4. 示例文件：/etc/securetty

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

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。

配置串行连接的 iDRAC6

您可以使用下列任何一种界面通过串行连接连接到 iDRAC6：

- iDRAC6 CLI
- 直接连接基本模式
- 直接连接终端模式

要将系统设置为使用这些界面中的任何一种，请执行以下步骤。

1. 配置 BIOS 以启用串行连接：
   a. 打开或重新启动系统。
   b. 看到下列信息时立即按 <F2>：
      ```
      <F2> = System Setup
      ```
   c. 向下滚动并通过按 <Enter> 选择 **"Serial Communication"**（串行通信）。
   d. 如下设置 **"Serial Communication"**（串行通信）屏幕：
      外部串行连接器 . . . . 远程访问设备
   e. 选择 **"Save Changes"**（保存更改）。
   f. 按 <Esc> 退出**系统设置**程序，并完成系统设置程序配置。
2. 将 DB-9 或零调制解调器电缆从 Management Station 连接到受管节点服务器。请参阅第 92 页上的 "为串行控制台连接 DB-9 或零调制解调器电缆"。
3. 确保管理终端仿真软件已配置串行连接。请参阅第 92 页上的 "配置 Management Station 终端仿真软件"。
4. 配置 iDRAC6 设置以启用串行连接，这可通过 RACADM 或 iDRAC6 Web 界面实现。

要配置 iDRAC6 设置以通过 RACADM 启用串行连接，请运行以下命令：

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

要配置 iDRAC6 设置以通过 iDRAC6 Web 界面启用串行连接，请执行以下步骤：

1. 展开 **"System"**（系统）树并单击 **"iDRAC Settings"**（iDRAC 设置）。
2. 单击 **"Network Security"**（网络 / 安全性）选项卡，然后单击 **"Serial"**（串行）。

3 在 **"RAC Serial"**（RAC 串行）部分下选择 **"Enabled"**（已启用）。

4 单击 **"Apply Changes"**（应用更改）。

当您通过原来的设置串行连接时，将看到一个登录提示。输入 iDRAC6 用户名和密码（默认值分别为 `root`、`calvin`）。

您可以从这个界面执行 RACADM 等功能。例如，要打印系统事件日志，请输入下列 RACADM 命令：

```
racadm getsel
```

将 iDRAC 配置为使用直接连接基本模式和直接连接终端模式

使用 RACADM，运行下列命令，以禁用 iDRAC6 命令行界面：

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

然后，运行下列 RACADM 命令，以启用直接连接基本模式：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 1
```

或运行下列 RACADM 命令，以启用直接连接终端模式：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 0
```

您可以用 iDRAC6 Web 界面执行相同操作：

1 展开 **"System"**（系统）树并单击 **"iDRAC Settings"**（iDRAC 设置）。

2 单击 **"Network Security"**（网络 / 安全性）选项卡，然后单击 **"Serial"**（串行）。

3 在 **"RAC Serial"**（RAC 串行）部分下取消选择 **"Enabled"**（已启用）。

直接连接基本模式：

在 **"IPMI Serial"**（IPMI 串行）部分下，将 **"Connection Mode Settings"**（连接模式设置）下拉式菜单更改为 **"Direct Connect Basic Mode"**（直接连接基本模式）。

直接连接终端模式：

在 **"IPMI Serial"**（IPMI 串行）部分下，将 **"Connection Mode Settings"**（连接模式设置）下拉式菜单更改为 **"Direct Connect Terminal Mode"**（直接连接终端模式）。

4 单击 **"Apply Changes"**（应用更改）。有关直接连接基本模式和直接连接终端模式的详情，请参阅第 96 页上的"配置串行模式和终端模式"。

直接连接基本模式使您能够直接通过串行连接使用 ipmish 等工具。例如，要通过 IPMI 基本模式用 ipmish 打印系统事件日志，请运行下列命令：

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin
sel get
```

直接连接终端模式使您能够向 iDRAC6 发出 ASCII 命令。例如，通过直接连接终端模式打开 / 关闭服务器：

1 通过终端仿真软件连接至 iDRAC6。

2 键入以下命令进行登录：

```
[SYS PWD -U root calvin]
```

您将看到以下响应：

```
[SYS]

[OK]
```

3 键入以下命令，确认已成功登录：

```
[SYS TMODE]
```

您将看到以下响应：

```
[OK TMODE]
```

4 键入以下命令，关闭服务器电源 （服务器电源会立即关闭）：

```
[SYS POWER OFF]
```

5 打开服务器电源 （服务器电源会立即打开）：

```
[SYS POWER ON]
```

在 RAC 串行接口通信模式和串行控制台间切换

iDRAC6 支持 Esc 键序列，从而允许在 RAC 串行接口通信和串行控制台间切换。

要将系统设置为允许此行为，请执行以下步骤：

1 打开或重新启动系统。

2 看到下列信息时立即按 <F2>：

<F2> = System Setup

3 向下滚动并通过按 <Enter> 选择 **"Serial Communication"**（串行通信）。

4 如下设置 **"Serial Communication"**（串行通信）屏幕：

串行通信 -- 开，通过 com2 进行串行重定向

注：只要 "serial port address"（串行端口地址）字段中的 "serial device2"（串行设备 2）设置为 com1，您就可以将 "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）。

串行端口地址 -- 串行设备 1 = com1、串行设备 2 = com2

外部串行连接器 -- 串行设备 2

故障安全波特率 115200

远程终端类型 ...vt100/vt220

引导后重定向 ... 已启用

然后，选择 **"Save Changes"**（保存更改）。

5 按 <Esc> 退出**系统设置**程序，并完成系统设置程序配置。

连接 Managed System 外部串行连接器和 Management Station 串行端口间的零调制解调器电缆。

在 Management Station 上使用终端仿真程序 （hyperterminal 或 Tera Term）并根据受管服务器在引导过程的位置，将会看到开机自检屏幕或操作系统屏幕。这基于配置：SAC （对于 Windows）和 Linux 文本模式屏幕 （对于 Linux）。设置 Management Station 的终端设置为波特率 - 115200, 数据 - 8 bit，奇偶校验 - none，停止 - 1 bit 以及流控制 - None。

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>

以上键序列会导向到 "iDRAC Login"（iDRAC 登录）提示符 （如果 RAC 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 RAC 设置为 "IPMI Serial Direct Connect Terminal Mode"（IPMI 串行直接连接终端模式））。

要在 RAC 串行接口通信模式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，要将连接切换为系统 COM2 端口，请使用：

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

连接到系统 COM2 端口时，要返回终端模式，请使用：

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

为串行控制台连接 DB-9 或零调制解调器电缆

要使用串行文本控制台访问 Managed System，请将 DB-9 零调制解调器电缆连接到 Managed System 上的 COM 端口。为使连接能用于零调制解调器电缆，须在 CMOS 设置中设置相应的串行通信设置。并不是所有 DB-9 电缆都能传送此连接所需的插针输出 / 信号。此连接所用的 DB-9 电缆必须符合表 5-5 中所示的规格。

注：DB-9 电缆还可以用于 BIOS 文本虚拟控制台。

表 5-5. DB-9 零调制解调器电缆所需的插针输出

信号名称	DB-9 插针（服务器插针）	DB-9 插针（工作站插针）
FG （Frame Ground [机架地线]）	–	–
TD （Transmit data [传输数据]）	3	2
RD （Receive Data [接收数据]）	2	3
RTS （Request To Send [请求发送]）	7	8
CTS （Clear To Send [清除发送]）	8	7
SG （Signal Ground [信号接地]）	5	5
DSR （Data Set Ready [数据设备就绪]）	6	4
CD （Carrier Detect [载波检测]）	1	4
DTR （Data Terminal Ready [数据终端就绪]）	4	1 和 6

配置 Management Station 终端仿真软件

iDRAC6 支持在运行以下一种终端仿真软件的 Management Station 上使用串行或 Telnet 文本控制台：

- Xterm 中的 Linux Minicom
- Hilgraeve's HyperTerminal Private Edition （版本 6.3）
- Xterm 中的 Linux Telnet
- Microsoft Telnet

执行以下小节中的步骤以配置所用终端软件。如果使用 Microsoft Telnet，则无需配置。

为串行控制台仿真配置 Linux Minicom

Minicom 是 Linux 的串行端口访问公用程序。以下步骤可用于配置 Minicom 版本 2.0。其它 Minicom 版本可能略有不同，但需要相同的基本设置。使用 第 94 页上的 “串行控制台仿真所需的 Minicom 设置”中的信息配置其它版本的 Minicom。

为串行控制台仿真配置 Minicom 版本 2.0

注：要确保文本正确显示，建议使用 Xterm 窗口来显示 Telnet 控制台，而不是 Linux 安装提供的默认控制台。

1. 要启动新 Xterm 会话，在命令提示符处键入 `xterm &`。
2. 在 Xterm 窗口中，将鼠标箭头移到窗口的右下角并将窗口的大小调整为 80 x 25。
3. 如果没有 Minicom 配置文件，则转至下一步。

   如果有 Minicom 配置文件，则键入 `minicom <Minicom config 文件名>` 并跳至步骤 17。
4. 在 Xterm 命令提示符处，键入 `minicom -s`。
5. 选择 Serial Port Setup （串行端口设置）并按 <Enter> 键。
6. 按 <a> 并选择相应的串行设备 （例如， /dev/ttyS0）。
7. 按 <e> 并将 **“Bps/Par/Bits”**（速率 / 奇偶校验位 / 数据位和停止位）选项设置为 57600 8N1。
8. 按 <f> 并将 **“Hardware Flow Control”**（硬件流控制）设置为 **“Yes”**（是），将 **“Software Flow Control”**（软件流控制）设置为 **“No”**（否）。
9. 要退出 Serial Port Setup （串行端口设置）菜单，按 <Enter>。
10. 选择 Modem and Dialing （调制解调器和拨号）并按 <Enter>。
11. 在 **“Modem Dialing and Parameter Setup”**（调制解调器拨号和参数设置）菜单中，按 <Backspace> 清除 **“init”**（初始化）、**“reset”**（重设）、**“connect”**（连接）和 **“hangup”**（挂断）设置以使它们保留为空白。
12. 要保存每个空白值，按 <Enter>。

13 清除完所有指定字段后，按 <Enter> 退出 **Modem Dialing and Parameter Setup**（调制解调器拨号和参数设置）菜单。

14 选择 **Save setup as config_name**（将设置另存为 config_name）并按 <Enter>。

15 选择 **Exit From Minicom**（从 Minicom 退出）并按 <Enter>。

16 在命令 Shell 提示符处键入 `minicom <Minicom config 文件名>`。

17 要将 Minicom 窗口展开为 80 x 25，拖动窗角。

18 按 <Ctrl+a>、<z>、<x> 退出 Minicom。

注：如果使用串行文本虚拟控制台的 Minicom 来配置 Managed System BIOS，则建议打开 Minicom 中的颜色。要打开颜色，键入以下命令：`minicom -c on`

确保 Minicom 窗口显示一个命令提示符。命令提示符出现后，表示连接成功并且您可以使用 **connect** serial 命令连接到 Managed System 控制台。

串行控制台仿真所需的 Minicom 设置

根据表 5-6 配置任何版本的 Minicom。

表 5-6. 串行控制台仿真所需的 Minicom 设置

设置说明	所需设置
Bps/Par/Bits（速率 / 奇偶校验位 / 数据位和停止位）	57600 8N1
Hardware flow control（硬件流量控制）	是
Software flow control（软件流量控制）	否
Terminal emulation（终端仿真）	ANSI
Modem dialing and parameter settings（调制解调器拨号和参数设置）	清除 **init**（初始化）、**reset**（重设）、**connect**（连接）和 **hangup**（挂断）设置以使它们保留为空白
“Window size”（窗口大小）	80 x 25（要重新调整大小，拖动窗角）

为串行控制台配置 HyperTerminal

HyperTerminal 是 Microsoft Windows 串行端口访问公用程序。要设置虚拟控制台屏幕为合适大小，请使用 Hilgraeve 的 HyperTerminal Private Edition 版本 6.3。

小心：所有版本的 Microsoft Windows 操作系统都包括有 Hilgraeve 的 HyperTerminal 终端仿真软件。但是，包括的版本没有提供在虚拟控制台期间需要的许多功能。因此，使用版本 6.3 或支持 VT100/VT220 或 ANSI 仿真模式的任何终端仿真软件代替。Hilgraeve 的 HyperTerminal Private 就是支持系统上虚拟控制台的一种完全 VT100/VT220 或 ANSI 终端仿真程序示例。

要为串行控制台配置 HyperTerminal：

1. 启动 HyperTerminal 程序。
2. 键入新连接的名称并单击 **"OK"**（确定）。
3. 在 **"Connect using:"**（连接所用端口：），选择 Management Station 上连有 DB-9 零调制解调器电缆的 COM 端口（例如，COM2）并单击 **"OK"**（确定）。
4. 如表 5-7 中所示配置 COM 端口设置。
5. 单击 OK（确定）。
6. 单击 **"File"**（文件）→ **"Properties"**（属性）并单击 **"Settings"**（设置）选项卡。
7. 将 **"Telnet terminal ID:"**（Telnet 终端 ID：）设置为 **ANSI**。
8. 单击 **"Terminal Setup"**（终端设置）并将 **"Screen Rows"**（屏幕行数）设置为 **26**。
9. 将 **"Columns"**（列数）设置为 80 并单击 **"OK"**（确定）。

表 5-7. Management Station COM 端口设置

设置说明	所需设置
"Bits per second"（每秒位数）	57600
"Data bits"（数据位）	8
奇偶校验	None（无）
"Stop bits"（停止位）	1
Flow control（流控制）	硬件

配置串行模式和终端模式

配置 IPMI 和 iDRAC6 串行

1. 展开 **"System"**（系统）树并单击 **"iDRAC Settings"**（iDRAC 设置）。
2. 单击 **"Network Security"**（网络 / 安全性）选项卡，然后单击 **"Serial"**（串行）。
3. 配置 IPMI 串行设置。

   请参阅表 5-8 了解 IPMI 串行设置的说明。
4. 配置 iDRAC6 串行设置。

   请参阅表 5-9 了解 iDRAC6 串行设置的说明。
5. 单击 **"Apply Changes"**（应用更改）应用 IPMI 和 iDRAC6 串行更改。
6. 单击相应的 **"Serial"**（串行）页按钮继续。有关 **"Serial Configuration"**（串行配置）页设置的说明，请参阅 *iDRAC6 联机帮助*。

表 5-8. IPMI 串行设置

设置	说明
"Connection Mode Settings"（连接模式设置）	• 直接连接基本模式 - IPMI 串行基本模式 • 直接连接终端模式 - IPMI 串行终端模式
波特率	• 设置数据速度。选择 9600 bps、 19.2 kbps、 57.6 kbps 或 115.2 kbps。
Flow Control（流控制）	• "None"（无）— 硬件流控制关闭 • RTS/CTS — 硬件流控制打开
信道权限级别限制	• 管理员 • "Operator"（操作员） • User （用户）

表 5-9. iDRAC6 串行设置

设置	说明
Enabled （启用）	启用或禁用 iDRAC6 串行控制台。选中 = 启用；未选中 = 禁用。

表 5-9. iDRAC6 串行设置 *（续）*

设置	说明
超时	线路断开之前的最大线路闲置时间（以秒为单位）。范围是 60 至 1920 秒。默认值为 300 秒。 0 秒表示禁用超时功能。
Redirect Enabled（已启用重定向）	启用或禁用虚拟控制台。选中 = 启用；未选中 = 禁用。
波特率	外部串行端口的数据速度。值包括 9600 bps、 19.2 kbps、57.6 kbps 和 115.2 kbps。默认值为 57.6 kbps。
Escape Key （Esc 键）	指定 <Esc> 键。默认为 ^\ 字符。
"History Buffer Size"（历史记录缓冲区大小）	串行历史记录缓冲区大小，保持上次写入虚拟控制台的字符。最大值和默认值 = 8192 个字符。
Login Command（登录命令）	有效登录后执行的 iDRAC6 命令行。

配置终端模式

1. 展开 **"System"**（系统）树并单击 **"iDRAC Settings"**（iDRAC 设置）。
2. 单击 **"Network Security"**（网络 / 安全性）选项卡，然后单击 **"Serial"**（串行）。
3. 在 **"Serial"**（串行）页中单击 **"Terminal Mode Settings"**（终端模式设置）。
4. 配置终端模式设置。

   请参阅表 5-10 了解终端模式设置的说明。
5. 单击 **"Apply Changes"**（应用更改）。
6. 单击相应的 **"Terminal Mode Settings"**（终端模式设置）页按钮继续。有关 **"Terminal Mode Settings"**（终端模式设置）页按钮的说明，请参阅 *iDRAC6 联机帮助*。

表 5-10. 终端模式设置

设置	说明
行编辑	启用或禁用行编辑。

表 5-10. 终端模式设置 *（续）*

设置	说明
删除控制	选择以下选项之一： • **“iDRAC outputs a <bksp><sp><bksp> character when <bksp> or <del> is received”（iDRAC 在收到 <bksp> 或 <del> 时输出 <bksp><sp><bksp> 字符）—** • **“iDRAC outputs a <del> character when <bksp> or <del> is received”（iDRAC 在收到 <bksp> 或 <del> 时输出 <del> 字符）—**
回声控制	启用或禁用回声。
信号交换控制	启用或禁用符号交换。
新行序列	选择 **“None”**（无）、 **<CR-LF>**、 **<NULL>**、 **<CR>**、 **<LF-CR>** 或 **<LF>**。
输入新行序列	选择 **<CR>** 或 **<NULL>**。

配置 iDRAC6 网络设置

小心：更改 iDRAC6 网络设置可能会断开当前网络连接。

使用以下一个工具配置 iDRAC6 网络设置：

- 基于 Web 的界面 — 请参阅第 44 页上的 “配置 iDRAC6 NIC”。
- RACADM CLI — 请参阅 Dell 支持网站 **dell.com/support/manuals** 上《RACADM iDRAC6 和 CMC 命令行参考指南》中的 cfgLanNetworking。
- iDRAC6 配置公用程序 — 请参阅第 31 页上的 “配置系统使用 iDRAC6”。

注：如果要在 Linux 环境中部署 iDRAC6，请参阅第 35 页上的 “安装 RACADM”。

通过网络访问 iDRAC6

配置完 iDRAC6 后，可以使用下述一种界面来远程访问 Managed System：

- 基于 Web 的界面
- RACADM

- Telnet 控制台
- SSH
- IPMI

表 5-11 描述各种 iDRAC6 界面。

表 5-11. iDRAC6 界面

接口	说明
基于 Web 的界面	允许使用图形用户界面远程访问 iDRAC6。基于 Web 的界面构建在 iDRAC6 固件中并从 Management Station 中支持的 Web 浏览器通过 NIC 接口访问。
RACADM	允许通过命令行界面远程访问 iDRAC6。 RACADM 使用 iDRAC6 IP 地址执行 RACADM 命令。 **注：**racadm 远程功能选项只在 Management Station 上受支持。有关详情，请参阅第 100 页上的 “远程使用 RACADM”。 **注：**使用 racadm 远程功能时，须在使用有关文件操作的 RACADM 子命令的文件夹上具有写权限，例如： `racadm getconfig -f <文件名>` 或： `racadm sslcertupload -t 1 -f c:\cert\cert.txt` 子命令
Telnet 控制台	提供对 iDRAC6 的访问并支持串行和 RACADM 命令，包括 **powerdown**、 **powerup**、 **powercycle** 和 **hardreset** 命令。 **注：**Telnet 并非安全协议， Telnet 会传输所有数据，包括明文形式的密码。发送敏感信息时，应使用 SSH 接口。
SSH 接口	使用更高安全保护的加密传输层，提供与 Telnet 控制台相同的功能。
IPMI 接口	允许通过 iDRAC6 使用远程系统的基本管理功能。接口包括 LAN 上 IPMI、串行 IPMI 以及 LAN 上串行。有关详情，请参阅 **support.dell.com\manuals** 上的 《Dell OpenManage 底板管理控制器公用程序用户指南》。

注：iDRAC6 默认用户名是 `root`，默认密码是 `calvin`。

可以使用支持的 Web 浏览器，或使用 Server Administrator 或 IT Assistant，通过 iDRAC6 NIC 访问 iDRAC6 基于 Web 的界面。

要使用 Server Administrator 访问 iDRAC6 远程访问界面，请执行以下操作：

- 启动 Server Administrator。
- 从 Server Administrator 主页左窗格的系统树上，单击 **System** （系统）→ **Main System Chassis** （主系统机箱）→ **Remote Access Controller**。

有关详情，请参阅 《Server Administrator 用户指南》。

远程使用 RACADM

注：使用 RACADM 远程功能前请配置 iDRAC6 上的 IP 地址。有关设置 iDRAC6 的详情以及相关说明文件的列表，请参阅第 31 页上的 “iDRAC6 的基本安装”。

RACADM 提供远程功能选项 (**-r**)，可以允许连接 Managed System 和从远程虚拟控制台或 Management Station 执行 RACADM 子命令。要使用远程功能，需要有效的用户名 （**-u** 选项）和密码 （**-p** 选项），以及 iDRAC6 的 IP 地址。

注：如果用来访问远程系统的系统在默认证书存储区中没有 iDRAC6 证书，则在键入 RACADM 命令时会显示一条信息。有关 iDRAC6 证书的详情，请参阅第 57 页上的 “使用 SSL 和数字证书保证 iDRAC6 通信安全”。

“Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name”（安全警告：证书无效 - 证书上的名称无效或与站点名称不匹配）

继续执行。为 racadm 使用 -S 选项可以在出现证书相关错误时停止执行。

RACADM 继续执行命令。不过，如果使用 ®CS 选项，RACADM 会停止执行命令并显示以下信息：

“Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name”（安全警告：证书无效 - 证书上的名称无效或与站点名称不匹配）

Racadm 不继续执行命令。

“ERROR: Unable to connect to iDRAC6 at specified IP address”（错误：无法按照指定 IP 地址连接到 iDRAC6）

在 Linux 系统上，确保使用远程 RACADM 执行以下中间步骤以便成功验证证书：

1 将 DER 格式的证书转换为 PEM 格式 （使用 openssl cmdline 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 证书捆绑的位置。例如，对于 RHEL5 64 位，位置为 /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
```

RACADM 提要

```
racadm -r <iDRAC6 IP 地址> -u <用户名> -p <密码>
<子命令> <子命令选项>
racadm -i -r <iDRAC6 IP 地址> <子命令> <子命令选项>
```

例如：

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
racadm -i -r 192.168.0.120 getsysinfo
```

如果 iDRAC6 的 HTTPS 端口号已更改为除默认端口 (443) 之外的自定义端口，则必须使用下面的语法：

```
racadm -r <iDRAC6 IP 地址>:<端口> -u <用户名> -p
<密码> <子命令> <子命令选项>
racadm -i -r <iDRAC6 IP 地址>:<端口> <子命令>
<子命令选项>
```

RACADM 选项

表 5-12 列出 RACADM 命令的选项。

表 5-12. racadm 命令选项

选项	说明
-r <*racIpAddr*>	指定控制器的远程 IP 地址。
-r <*racIpAddr*>: < *端口号* >	如果 iDRAC6 端口号不是默认端口 (443)，则使用 : < *端口号* >
-i	指示 RACADM 向用户交互查询用户名和密码。
-u < *用户名* >	指定用于验证命令事务处理的用户名。如果使用 -u 选项，则必须使用 -p 选项，并且不允许使用 -i 选项（交互）。
-p < *密码* >	指定用于验证命令事务处理的密码。如果使用 -p 选项，则不允许使用 -i 选项。
-S	指定 RACADM 应检查是否有无效证书错误。如果检测到无效证书， RACADM 会停止执行命令并显示错误信息。

启用和禁用 RACADM 远程功能

注：建议在本地系统上运行这些命令。

RACADM 远程功能默认启用。如果禁用，请键入下面的 RACADM 命令启用：

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

要禁用远程功能，请键入：

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 0
```

RACADM 子命令

表 5-13 提供可在 RACADM 中运行的每个 RACADM 子命令的说明。有关 RACADM 子命令的详细列表 （包括语法和有效条目），请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《RACADM iDRAC6 和 CMC 命令行参考指南》。

输入 RACADM 子命令时，请在命令前加上 RACADM，例如：

```
racadm help
```

表 5-13. RACADM 子命令

命令	说明
help	列出 iDRAC6 子命令。
help < *子命令* >	列出指定子命令的用法语句。
arp	显示 ARP 表的内容。 ARP 表条目不能被添加或删除。
clearasrscreen	清除上一个 ASR （崩溃）屏幕 （上一个蓝屏）。
clrraclog	清除 iDRAC6 日志。单个条目被用来指示清除日志的用户和时间。
config	配置 iDRAC6。
getconfig	显示当前 iDRAC6 配置属性。
coredump	显示上次 iDRAC6 内核转储。
coredumpdelete	删除 iDRAC6 中存储的内核转储。
fwupdate	执行或显示 iDRAC6 固件更新的状况。
getssninfo	显示关于活动会话的信息。
getsysinfo	显示 iDRAC6 和系统的一般信息。
getractime	显示 iDRAC6 时间。
ifconfig	显示当前 iDRAC6 的 IP 配置。
netstat	显示路由表和当前连接。
ping	验证目标 IP 地址是否可以使用当前路由表内容从 iDRAC6 进行访问。
setniccfg	设置控制器的 IP 配置。
sshpkauth	允许上载最多 4 个不同的 SSH 公共密钥，删除现有密钥和查看 iDRAC6 中已有的密钥。
getniccfg	显示控制器的当前 IP 配置。
getsvctag	显示系统服务标签。
racdump	转储 iDRAC6 状况和状态信息以进行调试。
racreset	重设 iDRAC6。
racresetcfg	将 iDRAC6 重设为默认配置。
serveraction	在受管系统上执行电源管理操作。
getraclog	显示 iDRAC6 日志。
clrsel	清除系统事件日志条目。

表 5-13. RACADM 子命令 *（续）*

命令	说明
gettracelog	显示 iDRAC6 跟踪日志。如果与 -i 一起使用，则命令显示 iDRAC6 跟踪日志中的条目数。
sslcsrgen	生成并下载 SSL CSR。
sslcertupload	将 CA 证书或服务器证书上载至 iDRAC6。
sslcertdownload	下载 CA 证书。
sslcertview	查看 iDRAC6 中的 CA 证书或服务器证书。
sslkeyupload	将 SSL 密钥从客户端上载到 DRAC6。
testtrap	强制 DRAC6 通过 DRAC6 NIC 发送检测 SNMP 陷阱来检查陷阱配置。
vmdisconnect	强制关闭虚拟介质连接。
closessn	关闭设备上的通信会话。
getsel	显示 SEL 条目。
krbkeytabupload	上载 Kerberos keytab 文件。
localConRedirDisable	禁用服务器控制台。服务器视频端口没有视频输出。
testemail	检测 RAC 的电子邮件警报功能。
usercertupload	将用户证书或用户 CA 证书从客户端上载到 iDRAC6。
usercertview	显示 iDRAC6 上的用户证书或用户 CA 证书。
vflashsd	初始化 vflash SD 卡或获取此卡的状态。
vflashpartition	创建、删除、列出初始化的 vFlash SD 卡上的分区或查看其状况。

有关 RACADM 错误信息的常见问题

执行 iDRAC6 重设后 （使用 racadm racreset 命令），我发出了一个命令，结果显示以下信息：

“ERROR: Unable to connect to RAC at specified IP address”（错误：无法按照指定 IP 地址连接到 RAC）

这条信息是什么意思？

必须等到 iDRAC6 完成重设后，才能发出另一个命令。

使用 racadm 命令和子命令时，我得到了并不理解的错误。

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 — 类似语法、印刷错误和错误名称等问题。
- 远程 RACADM 错误信息 — 类似错误 IP 地址、错误用户名或错误密码等问题。

当从系统中 ping iDRAC6 IP 地址并在 ping 响应过程中在专用和共享模式之间切换 iDRAC6 时，没有收到响应。

清除系统上的 ARP 表。

远程 RACADM 无法从 SUSE Linux Enterprise Server (SLES) 11 SP1 连接到 iDRAC

确保已安装正式的 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
```

配置多个 iDRAC6 控制器

使用 RACADM 可以配置一个或多个具有相同属性的 iDRAC6 控制器。使用组 ID 和对象 ID 查询特定 iDRAC6 控制器时，RACADM 会从检索到的信息创建 **.cfg** 配置文件。文件名是用户指定的，例如，**racadm.cfg**。通过将文件导出到一个或多个 iDRAC6，可以在最短时间内以相同属性配置控制器。

注：某些配置文件包含独特的 iDRAC6 信息 （如静态 IP 地址），在将文件导出到其它 iDRAC 之前必须修改这些信息。

要配置多个 iDRAC6 控制器，请执行以下步骤：

1 使用 RACADM 查询包含相应配置的目标 iDRAC6。

注：生成的 .cfg 文件不包含用户密码。

打开命令提示符并键入：

```
racadm getconfig -f myfile.cfg
```

注：使用 getconfig -f 将 iDRAC6 配置重定向至文件仅在本地和远程 RACADM 接口中受支持。

2 使用简单文本编辑器 **（可选）**修改配置文件。

3 使用新配置文件修改目标 iDRAC6。

在命令提示符处键入：

```
racadm config -f myfile.cfg
```

4 重设已配置的目标 iDRAC6。

在命令提示符处键入：

```
racadm racreset
```

`getconfig -f racadm.cfg` 子命令请求 iDRAC6 配置并生成 **racadm.cfg** 文件。如果需要，可以用其它名称配置该文件。

可以使用 **getconfig** 命令来执行以下操作：

- 显示组中的所有配置属性（用组名称和索引指定）
- 按用户名显示用户的所有配置属性

config 子命令将信息载入其它 iDRAC6 中。使用 **config** 将用户和密码数据库与 Server Administrator 同步。

初始配置文件 **racadm.cfg** 是由用户命名的。在以下示例中，配置文件被命名为 **myfile.cfg**。要创建此文件，请在命令提示符处键入以下命令：

```
racadm getconfig -f myfile.cfg
```

小心：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。任何格式都会使分析器混淆，都有可能损坏 RACADM 数据库。

创建 iDRAC6 配置文件

iDRAC6 配置文件 < *文件名* >.cfg 和 `racadm config -f` < ***文件名*** >`.cfg` 命令一起使用。可以使用配置文件构建配置文件（类似于 **.ini** 文件）并用该文件配置 iDRAC6。可以使用任何文件名，并且该文件不需要 **.cfg** 扩展名（尽管本小节中的该名称引用了此扩展名）。

可通过以下方式建立 **.cfg** 文件：

- 创建
- 通过 `racadm getconfig -f` < ***文件名*** >`.cfg` 命令获取
- 通过 `racadm getconfig -f` < ***文件名*** >`.cfg` 命令获取，然后进行编辑

注：有关 getconfig 命令的信息，请参阅 Dell 支持网站 dell.com/support/manuals 上 《RACADM iDRAC6 和 CMC 命令行参考指南》中的 getconfig 命令。

将首先分析 .cfg 文件以验证有效的组和对象名称是否存在，然后实施一些简单的语法规则。错误标记有在其中检测到错误的行号，并且有一条简单的信息解释该问题。将分析整个文件的正确性，并显示所有错误。如果在 .cfg 文件中找到错误，写入命令将不传输到 iDRAC6。用户必须纠正*所有*错误，然后才能进行任何配置。 -c 选项可以用于 config 子命令，它仅验证语法，而*不会*对 iDRAC6 执行写入操作。

创建 .cfg 文件时请使用以下原则：

- 如果分析器遇到索引组，则该组的索引用作定位标记。对索引组内对象的任何修改也与索引值关联。

  例如：

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

- 索引是只读的，不能修改。索引组的对象在哪个索引下面列出，这些对象就绑定到哪个索引，对象值的任何有效配置仅适用于该特定索引。
- 为每个索引组提供了一组预定义的索引。有关详情，请参阅 Dell 支持网站 dell.com/support/manuals 上的 《RACADM iDRAC6 和 CMC 命令行参考指南》。
- 使用 racresetcfg 子命令将 iDRAC6 重设为初始默认值，然后运行 `racadm config -f <`*文件名*`>.cfg` 命令。确保 .cfg 文件中包含所有所需的对象、用户、索引和其它参数。

小心：使用 racresetcfg 子命令将数据库和 iDRAC6 NIC 设置重设为初始默认设置并删除所有用户和用户配置。尽管根用户可用，但也会将其他用户的设置重设为默认设置。

分析规则

- 所有以 '#' 开头的行将被视为注释。

  注释行*必须*在第一列中开始。任何其它列中的 '#' 字符将被视为 '#' 字符。

  一些调制解调器参数可能在其字符串中包含 # 字符。不需要转义字符。可能需要通过 `racadm getconfig -f <`***文件名***`>.cfg` 命令生成 .cfg，然后对另一个 iDRAC6 执行 `racadm config -f <`***文件名***`>.cfg` 命令，而不添加转义字符。

  示例：

  ```
  #

  # 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 >
  ```

- 所有组条目必须括在 "[" 和 "]" 字符中。

  表示组名称的开头 "[" 字符*必须*在第一列中开始。此组名称*必须*在该组中的任何对象之前指定。没有关联组名称的对象将导致错误。配置数据将归入各组，如 Dell 支持网站 **dell.com/support/manuals** 上的《RACADM iDRAC6 和 CMC 命令行参考指南》中所定义。

  以下示例显示了组名称、对象以及对象的属性值。

  示例：

  ```
  [cfgLanNetworking] -{group name}

  cfgNicIpAddress=143.154.133.121 { 对象名称 }
  ```

- 所有参数都指定为“对象 = 值”对，在对象、 = 或值之间不留空格。

  值后的空格将忽略。值字符串内的空格保持不变。将按原样采用 '=' 右边的任何字符（例如，第二个 '=' 或 '#'、'['、']' 等）。这些字符都是有效的调制解调器对话脚本字符。

  请参见上一个圆点符号后面的示例。

  `racadm getconfig -f <`***文件名***`>.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 <组名称> -i <索引 1-16>
```

- 对于索引组，对象定位标记*必须*是 "[ ]" 对后的第一个对象。下面是当前索引组的示例：

  ```
  [cfgUserAdmin]
  cfgUserAdminIndex=11
  ```

  如果键入 `racadm getconfig -f <myexample>.cfg`，则命令为当前 iDRAC6 配置生成一个 .cfg 文件。此配置文件可用作一个示例，依据该文件开始创建独特的 .cfg 文件。

修改 iDRAC6 IP 地址

修改配置文件中的 iDRAC6 IP 地址时，请删除所有不需要的“< *变量* >= **值**”条目。只有带有 "[" 和 "]" 的实际变量组标签保留，包括两个与 IP 地址更改相关的 “< *变量* >= **值**”条目。

例如：

```
#
#    对象组 "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

此文件将更新为如下内容：

```
#
#    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 分析文件并用行号标识任何错误。正确的文件将更新适当的条目。此外，可以使用上面示例中的 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：“定位标记”是内部术语，不应在文件中使用。

配置 iDRAC6 网络属性

要生成可用网络属性的列表，请键入以下命令：

```
racadm getconfig -g cfgLanNetworking
```

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

此命令提供的配置功能与引导期间提示您键入 <Ctrl><E> 时 iDRAC6 配置公用程序所提供的功能一样。有关使用 iDRAC6 配置公用程序配置网络属性的详情，请参阅第 31 页上的 “配置系统使用 iDRAC6”。

以下示例介绍如何使用命令配置所需的 LAN 网络属性。

```
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
```

注：如果 cfgNicEnable 设置为 0，则即使启用了 DHCP，也会禁用 iDRAC6 LAN。

iDRAC6 模式

iDRAC6 可配置为四种模式：

- 专用
- 共享
- 与故障转移 LOM2 共享
- 与故障转移所有 LOM 共享

表 5-14 提供了各种模式的说明。

表 5-14. iDRAC6 NIC 配置

模式	说明
专用	iDRAC6 将自己的 NIC （RJ-45 连接器）和 iDRAC MAC 地址用于网络通信。
共享	iDRAC6 在平台上使用 LOM1。
与故障转移 LOM2 共享	iDRAC6 使用 LOM1 和 LOM2 作为故障转移组。该组使用 iDRAC6 MAC 地址。
与故障转移所有 LOM 共享	iDRAC6 使用 LOM1、LOM2、LOM3 和 LOM4 作为故障转移组。该组使用 iDRAC6 MAC 地址。

关于网络安全的常见问题

访问 iDRAC6 基于 Web 的界面时，我得到一个安全警告，指出 SSL 证书的主机名与 iDRAC6 的主机名不匹配。

iDRAC6 包括了一个默认的 iDRAC6 服务器证书以确保基于 Web 的界面和远程 RACADM 功能的网络安全。如果使用该证书， Web 浏览器就会显示一个安全警告，因为默认的证书是颁发给 **iDRAC6 默认证书**的，它与 iDRAC6 的主机名不匹配 （例如， IP 地址）。

要解决这个安全问题，应上载一个颁发给 IP 地址或 iDRAC6 的 iDRAC 名称的 iDRAC6 服务器证书。生成用于颁发证书的证书签名请求 (CSR) 时，应确保 CSR 的常用名 (CN) 与 iDRAC6 的 IP 地址 （如果是颁发给 IP 的证书）（例如， 192.168.0.120）或注册的 DNS iDRAC6 名称 （如果是颁发给 iDRAC 注册名称的证书）匹配。

要确保 CSR 与注册 DNS iDRAC6 名称匹配：

1 在 **"System"**（系统）树中，单击 **"iDRAC Settings"**（iDRAC 设置）。

2 单击 **"Network/Security"**（网络 / 安全性）选项卡，然后单击 **"Network"**（网络）。

3 在 **"Common Settings"**（常见设置）表中：

   a 选择 **"Register iDRAC on DNS"**（在 DNS 上注册 iDRAC）复选框。

   b 在 **"DNS iDRAC Name"**（DNS iDRAC 名称）字段中，输入 iDRAC6 名称。

4 单击 **"Apply Changes"**（应用更改）。

请参阅第 312 页上的 "使用 SSL 和数字证书保证 iDRAC6 通信安全" 了解有关生成 CSR 和颁发证书的详情。

为什么在属性更改后，远程 RACADM 和基于 Web 的服务会变得不可用?

重设 iDRAC6 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。

iDRAC6 Web 服务器会在发生以下情况后重设：

- 使用 iDRAC6 Web 用户界面更改网络配置或网络安全性属性时
- 更改 **cfgRacTuneHttpsPort** 属性时（包括 config -f *配置文件* > 更改它时）
- 使用 **racresetcfg** 时
- iDRAC6 重设时
- 上载新的 SSL 服务器证书时

为什么我的 DNS 服务器没有注册 iDRAC6?

有些 DNS 服务器只注册 31 个或更少字符的名称。

访问 iDRAC6 基于 Web 的界面时，我得到一个安全警告，指出该 SSL 证书是由一个不可信的认证机构 (CA) 颁发的。

iDRAC6 包括了一个默认的 iDRAC6 服务器证书以确保基于 Web 的界面和远程 RACADM 功能的网络安全。此证书不是由可信 CA 颁发的。要解决这个安全问题，请上载一个由可信 CA （例如 Microsoft 认证机构、 Thawte 或 Verisign）颁发的 iDRAC6 服务器证书。请参阅第 312 页上的“使用 SSL 和数字证书保证 iDRAC6 通信安全”了解有关颁发证书的详情。

6

添加和配置 iDRAC6 用户

要用 iDRAC6 管理系统并维护系统安全性，请创建多个具有特定管理权限（或基于角色的权限）的独特*用户*。要增强安全性，还可以配置警报以便在发生特定系统事件时通过电子邮件通知特定用户。

使用 Web 界面配置 iDRAC6 用户

添加和配置 iDRAC6 用户

要用 iDRAC6 管理系统并维护系统安全性，请创建多个具有特定管理权限（或*基于角色的权限*）的独特用户。

要添加和配置 iDRAC6 用户，请执行以下步骤：

注：您必须具有 "Configure Users"（配置用户）权限才能配置 iDRAC 用户。

1 单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）→ **"Users"**（用户）。

"Users"（用户）页 （请参阅表 6-1）显示 iDRAC6 用户的以下信息：**"User ID"**（用户 ID）、"**State** (Enabled/Disabled)"（状态 [已启用 / 已禁用]）、**"User Name"**（用户名）、**iDRAC**、**LAN**、**"Serial Port"**（串行端口）和 "**Serial Over LAN** (Enabled/Disabled)"（LAN 上串行 [已启用 / 已禁用]）。

注：用户 1 保留用于 IPMI 匿名用户，您无法更改此配置。

2 在 **"User ID"**（用户 ID）列单击用户 ID 编号。

在 **"User Main Menu"**（用户主菜单）页 （请参阅表 6-2 和表 6-7），可以配置用户、查看或上载用户证书、上载可信认证机构 (CA) 证书、查看可信 CA 证书、上载 Secure Shell (SSH) 公共密钥文件或者查看或删除特定的 SSH 密钥或所有 SSH 密钥。

如果选择 **"Configure User"**（配置用户）并单击 **"Next"**（下一步），将会显示 **"User Configuration"**（用户配置）页。

3 在 **"User Configuration"**（用户配置）页上，配置以下内容：

- 用户名、密码，以及新 iDRAC 用户或现有 iDRAC 用户的访问权限。表 6-3 说明 **"General User Settings"**（常规用户设置）。

- 用户的 IPMI 权限。表 6-4 说明配置用户 LAN 权限的 **"IPMI User Privileges"**（IPMI 用户权限）。
- iDRAC 用户权限。表 6-5 说明 **iDRAC 用户权限**。
- iDRAC 组访问权限。表 6-6 说明 **iDRAC 组权限**。

4 完成后，单击 **"Apply Changes"**（应用更改）。

5 单击 **"Go Back To Users Page"**（退回到用户页）可返回到 "Users"（用户）页。

表 6-1. 用户状态和权限

设置	说明
User ID （用户 ID）	显示用户 ID 号顺序列表。**"User ID"**（用户 ID）下的每个字段都包含 16 个预设用户 ID 号中的一个。此字段不能编辑。
State （状态）	显示用户的登录状态："Enabled"（已启用）或 "Disabled"（已禁用）。（默认为已禁用。） **注：默认启用用户 2。**
用户名	显示用户的登录名称。指定一个 iDRAC6 用户名，最多 16 个字符。每个用户必须具有独特用户名。 **注：如果更改用户名，则在下次用户登录前新用户名将不显示在用户界面上。**
iDRAC	显示用户所分配的组 （权限级别），包括 "Administrator"（管理员）、"Operator"（操作员）、"Read Only"（只读）或 "None"（无）。
LAN	显示用户所分配的 IPMI LAN 权限级别，包括 "Administrator"（管理员）、"Operator"（操作员）、"Read Only"（只读）或 "None"（无）。
串行端口	显示用户所分配的 IPMI 串行端口权限级别，包括 "Administrator"（管理员）、"Operator"（操作员）、"Read Only"（只读）或 "None"（无）。
Serial Over Lan （LAN 上串行）	允许或不允许用户使用 IPMI LAN 上串行。

表 6-2. Smart Card 配置选项

选项	说明
"Upload User Certificate"（上载用户证书）	允许用户上载用户证书到 iDRAC6 并导入用户配置文件。
查看用户认证	显示已上载到 iDRAC 的用户证书页。
上载可信 CA 认证	使您能够将可信 CA 证书上载到 iDRAC 并导入用户配置文件。
"View Trusted CA Certificate"（查看可信 CA 证书）	显示已上载到 iDRAC 的可信 CA 证书。可信 CA 证书由得到授权可向用户颁发证书的 CA 颁发。

表 6-3. 常规用户设置

User ID（用户 ID）	16 个预设用户 ID 编号之一。
Enable User（启用用户）	选中后，表示用户的 iDRAC6 访问权限已启用。清空后，表示禁用用户的访问权限。
用户名	用户名称，最多 16 个字符。支持以下字符： • 0-9 • A-Z • a-z • 特殊字符： + %) ' > : $ [| ! & = * , - {] § # (? < ; _ } I
Change Password（更改密码）	启用 **"New Password"**（新密码）和 **"Confirm New Password"**（确认新密码）字段。清除时，无法更改用户的 "Password"（密码）。

表 6-3. 常规用户设置 *（续）*

"New Password"（新密码）	输入多达 16 个字符的 **"Password"**（密码）。这些字符将被屏蔽，而不会显示出来。支持以下字符： • 0-9 • A-Z • a-z • 特殊字符：

+	&	?	>	-	}	|	.
!	(	'	,	_	[	"	@
#	)	*	;	$	]	/	§
%	=	<	:	{	I	\	

"Confirm New Password"（确认新密码）	重新键入 iDRAC 用户的密码以进行确认。

表 6-4. IPMI 用户权限

属性	说明
"Maximum LAN User Privilege Granted"（授予的最大 LAN 用户权限）	指定 IPMI LAN 信道上的用户最大权限为以下用户组之一：**"Administrator"**（管理员）、**"Operator"**（操作员）、**"User"**（用户）或 **"None"**（无）。
"Maximum Serial Port User Privilege Granted"（授予的最大串行端口用户权限）	指定 IPMI 串行信道上的用户最大权限为以下用户组之一：**"Administrator"**（管理员）、**"Operator"**（操作员）、**"User"**（用户）或 **"None"**（无）。
启用 LAN 上串行	允许用户使用 IPMI LAN 上串行。选中后，此权限将启用。

表 6-5. iDRAC 用户权限

属性	说明
角色	指定用户的最大 iDRAC 用户权限为以下权限之一：**"Administrator"**（管理员）、**"Operator"**（操作员）、**"Read Only"**（只读）或 **"None"**（无）。请参阅表 6-6 了解 **iDRAC 组权限**。

表 6-5. iDRAC 用户权限 *（续）*

属性	说明
"Login to iDRAC"（登录到 iDRAC）	允许用户登录到 iDRAC。
"Configure iDRAC"（配置 iDRAC）	允许用户配置 iDRAC。
Configure Users（配置用户）	使用户可以允许特定用户访问系统。 **小心：此权限通常为属于 iDRAC 上的管理员角色的成员保留。但是，可以给 Operator （操作员）角色中的用户分配此权限。具有此权限的用户可以修改任何用户的配置。这包括创建和删除任何用户、用户的 SSH 密钥管理等。因此，应谨慎分配此权限。**
清除日志	允许用户清除 iDRAC 日志。
"Execute Server Control Commands"（执行服务器控制命令）	使用户能够执行服务器控制命令。
"Access Virtual Console"（访问虚拟控制台）	允许用户运行虚拟控制台。
"Access Virtual Media"（访问虚拟介质）	允许用户运行和使用虚拟介质。
"Test Alerts"（检测警报）	允许用户将检测警报 （电子邮件或 PET）发送到特定用户。
"Execute Diagnostic Commands"（执行诊断命令）	允许用户运行诊断命令。

表 6-6. iDRAC 组权限

用户组	授予的权限
管理员	"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"（检测警报）、"Execute Diagnostic Commands"（执行诊断命令）
"Operator"（操作员）	选择以下权限的任意组合："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 Action Commands"（执行服务器操作命令）、"Access Virtual Console"（访问虚拟控制台）、"Access Virtual Media"（访问虚拟介质）、"Test Alerts"（检测警报）、"Execute Diagnostic Commands"（执行诊断命令）
只读	"Login to iDRAC"（登录到 iDRAC）
None （无）	没有分配权限

通过 SSH 的公共密钥验证

iDRAC6 支持通过 SSH 的公共密钥验证 (PKA)。此验证方法不再需要嵌入或提供用户 ID/ 密码，从而提高了 SSH 脚本编写的自动化程度。

开始之前

通过 SSH 界面*每个用户*最多可以配置 4 个公共密钥来使用。添加或删除公共密钥之前，务必使用查看命令查看已设置了什么密钥，这样就不会无意改写或删除密钥。如果正确设置和使用了通过 SSH 的 PKA，在登录 iDRAC6 时，您不必输入用户名和密码。对于设置自动脚本来执行各种功能，这颇为有用。

准备好设置此功能时，注意以下事项：

- 您可以使用 RACADM 或从 GUI 管理此功能。
- 添加新公共密钥时，确保现有密钥不位于添加新密钥的索引处。iDRAC6 不检查在添加新密钥之前是否删除了以前的密钥。添加了新密钥后，只要启用了 SSH 接口，新密钥就自动生效。

生成在 Windows 中使用的公共密钥

在添加帐户之前，在将通过 SSH 访问 iDRAC6 的系统中必须有公共密钥。有两种常用方法可生成公共 / 私人密钥对：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。默认情况下，所有标准安装均包含 *ssh-keygen* CLI 公用程序。

本节介绍使用这两个应用程序生成公共 / 私人密钥对的简单说明。有关这些工具的其它用法或高级用法，请参阅应用程序帮助。

要使用适用于 Windows 客户端的 *PuTTY Key Generator* 创建基本密钥：

1. 启动应用程序，根据要生成的密钥类型选择 SSH-2 RSA 或 SSH-2 DSA。（不支持 SSH-1）。
2. 密钥生成算法仅支持 RSA 和 DSA。输入密钥的位数。对于 RSA，该数字应介于 768 和 4096 位之间，而对于 DSA，则为 1024。
3. 单击 **Generate**（生成），按指示在窗口中移动鼠标。创建密钥后，您可以修改密钥注释字段。还可以输入密码短语，来保证密钥的安全。确保将私人密钥保存起来。
4. 可以使用“Save public key”（保存公共密钥）选项将公共密钥保存为文件供以后上载。所有上载的密钥必须采用 RFC 4716 或 openssh 格式。如果不是，必须转换为该格式。

生成在 Linux 中使用的公共密钥

适用于 Linux 客户端的 *ssh-keygen* 应用程序是不带图形用户界面的命令行工具。

打开终端窗口，然后在 Shell 提示符中键入：

```
ssh-keygen - t rsa - b 1024 - C testing
```

注：选项区分大小写。

其中，

-t 选项可以是 *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。

请按照说明进行操作。执行此命令后，上载公共文件。

小心：Linux Management Station 通过 ssh-keygen 生成的密钥不是 4716 格式。将密钥转换为 4716 格式，方法为 `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`。**不要更改密钥文件的权限。以上转换应使用默认权限进行。**

注：iDRAC6 不支持密钥的 ssh-agent 转发。

使用公共密钥验证方法登录

上载公共密钥后，可以不输入密码通过 SSH 登录 iDRAC6。您还可以选择以命令行参数的形式发送单个 RACADM 命令到 SSH 应用程序。命令行选项的效果就像远程 RACADM 一样，因为会话在命令完成之后结束。

例如：

登录：

```
ssh username@<域>
```

或

```
ssh username@<IP 地址>
```

其中， IP 地址 是 iDRAC6 的 IP 地址。

发送 racadm 命令：

```
ssh username@<域> racadm getversion
ssh username@<域> racadm getsel
```

使用 iDRAC6 基于 Web 的界面上载、查看和删除 SSH 密钥

1. 单击 **"iDRac Settings"**（iDRac 设置）→ **"Network/Security"**（网络 / 安全性）→ **"Users"**（用户）。将会显示 **"Users"**（用户）页。
2. 在 **"User ID"**（用户 ID）列单击用户 ID 编号。将会显示 **"User Main Menu"**（用户主菜单）页。
3. 使用 **"SSH Key Configurations"**（SSH 密钥配置）选项上载、查看或删除 SSH 密钥。

小心：上载、查看和 / 或删除 SSH 密钥的能力取决于 "Configure Users"（配置用户）用户权限。此权限允许用户配置其他用户的 SSH 密钥。应谨慎授予此权限。有关用户权限的详情，请参阅第 115 页上的 "添加和配置 iDRAC6 用户"。

表 6-7. SSH 密钥配置

选项	说明
"Upload SSH Key(s)"（上载 SSH 密钥）	允许本地用户上载 Secure Shell (SSH) 公共密钥文件。如果密钥已上载，则密钥文件的内容会显示在 **"User Configuration"**（用户配置）页的不可编辑文本框中。

表 6-7. SSH 密钥配置 *（续）*

选项	说明
"View/Remove SSH Key(s)"（查看 / 删除 SSH 密钥）	允许本地用户查看或删除指定的 SSH 密钥或所有 SSH 密钥。

"Upload SSH Key(s)"（上载 SSH 密钥）页允许上载 Secure Shell (SSH) 公共密钥文件。如果上载了密钥，密钥文件的内容会显示在 **"View/Remove SSH Key(s)"**（查看 / 删除 SSH 密钥）页上的不可编辑文本框中。

表 6-8. "Upload SSH Key(s)"（上载 SSH 密钥）

选项	说明
文件 / 文本	选择 **"File"**（文件）选项并键入密钥所在的路径。也可以选择 **"Text"**（文本）选项并在框中粘贴密钥文件的内容。您可以上载新密钥或改写已有密钥。要上载密钥文件，单击 **"Browse"**（浏览），选择文件然后单击 **"Apply"**（应用）按钮。
Browse （浏览）	单击此按钮可定位密钥的完整路径和文件名。

"View/Remove SSH Key(s)"（查看 / 删除 SSH 密钥）页允许您查看或删除用户的 SSH 公共密钥。

表 6-9. "View/Remove SSH Key(s)"（查看 / 删除 SSH 密钥）

选项	说明
删除	上载的密钥显示在此框中。选择 "Remove"（删除）选项并单击 **"Apply"**（应用）可删除现有密钥。

使用 RACADM 上载、查看和删除 SSH 密钥

"Upload"（上载）

上载模式允许上载密钥文件或将密钥文本复制到命令行。上载和复制密钥不能同时进行。

本地和远程 RACADM：

```
racadm sshpkauth -i <2 到 16> -k <1 到 4> -f < 文件名 >
racadm sshpkauth -i <2 到 16> -k <1 到 4> -t
```

< 密钥文本 >

Telnet/SSH/Serial RACADM：

```
racadm sshpkauth -i <2 到 16> -k <1 到 4> -t
< 密钥文本 >
```

示例：

使用文件将有效密钥上载到第一个密钥空间中的 iDRAC6 用户 2：

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

PK SSH 验证密钥文件已成功上载到 RAC。

小心：“key text”（密钥文本）选项在本地和远程 RACADM 上受支持。“file”（文件）选项在 Telnet/ssh/serial RACADM 上不受支持。

查看

视图模式允许用户查看指定的密钥或所有密钥。

```
racadm sshpkauth -i <2 到 16> -v -k <1 到 4>
racadm sshpkauth -i <2 到 16> -v -k all
```

删除

删除模式允许用户删除指定的密钥或所有密钥。

```
racadm sshpkauth -i <2 到 16> -d -k <1 到 4>
racadm sshpkauth -i <2 到 16> -d -k all
```

有关子命令选项的信息，请参阅 Dell 支持网站 **dell.com/support/manuals** 上 《iDRAC6 和 CMC 命令行参考指南》中的 `sshpkauth` 子命令。

使用 RACADM 公用程序配置 iDRAC6 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。

可以使用 Managed System 上同 iDRAC6 代理一起安装的 RACADM 命令行来配置单一或多个 iDRAC6 用户。

要配置多个具有相同配置设置的 iDRAC6，请执行以下一个过程：

- 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 Managed System 上执行该批处理文件。
- 如 Dell 支持网站 **dell.com/support/manuals** 上的 《iDRAC6 和 CMC 命令行参考指南》中所述，创建 iDRAC6 配置文件并使用相同的配置文件在每个 Managed System 上执行 **racadm config** 子命令。

开始之前

最多可以在 iDRAC6 属性数据库中配置 16 个用户。手动启用 iDRAC6 用户前，请验证当前用户是否存在。如果配置新 iDRAC6 或运行 racadm racresetcfg 命令，则当前唯一用户为 root，密码为 calvin。 racresetcfg 子命令将 iDRAC6 重设回原始默认值。

小心：使用 racresetcfg 命令时请小心，因为*所有*配置参数将重设为默认值。任何之前的更改将丢失。

注：在一段时间后，可以启用和禁用用户。因此，用户在各个 iDRAC6 上可能会有不同的索引号。

要验证用户是否存在，请在命令提示符处键入以下命令：

```
racadm getconfig -u <用户名>
```

或

键入以下命令，每次仅查找索引 1 至 16 中的一个：

```
racadm getconfig -g cfgUserAdmin -i <索引>
```

注：还可以键入 racadm getconfig -f <*myfile.cfg*> 并查看或编辑 myfile.cfg 文件，该文件包含所有 iDRAC6 配置参数。

系统将显示有些参数和对象 ID 以及它们的当前值。受关注的两个对象为：

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

如果 cfgUserAdminUserName 对象没有值，则可以使用由 cfgUserAdminIndex 对象表示的索引编号。如果 “=”后有名称，则该索引由该用户名占用。

注：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，上一实例中显示的 **cfgUserAdminIndex** 对象带有 '#' 字符。并且如果使用 **racadm config -f racadm.cfg** 命令指定任意数量的要写入的组 / 对象，将无法指定索引。新用户将被添加至第一个可用的索引。这便可以更灵活地使用相同设置配置 多个 iDRAC6。

添加 iDRAC6 用户

要将新用户添加到 RAC 配置，可以使用一些基本命令。通常，执行以下过程：

1. 设置用户名。
2. 设置密码。

3 设置以下用户权限：
- iDRAC
- LAN
- 串行端口
- Serial Over Lan （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”，对 RAC 具有登录权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2 123456
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiLanPrivilege 4
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiSerialPrivilege 4
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminSolEnable 1
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

要验证，请使用以下命令之一：

```
racadm getconfig -u john
racadm getconfig - g cfgUserAdmin - i 2
```

删除 iDRAC6 用户

使用 RACADM 时，必须手动逐个禁用用户。不能使用配置文件删除用户。

下面的示例说明可用于删除 iDRAC6 用户的命令语法：

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <索引> ""
```

双引号空字符串 ("") 指示 iDRAC6 删除指定索引处的用户配置，并将用户配置重设为初始出厂默认值。

启用 iDRAC6 用户权限

要启用具有特定管理权限 （基于角色授权）的用户，首先请通过执行第 125 页上的 “开始之前”中的步骤找到一个可用用户索引。然后输入以下命令行，并在其中输入新的用户名和密码。

注：有关特定用户权限的有效位掩码值的列表，请参阅 Dell 支持网站 dell.com/support/manuals 上的 《iDRAC6 和 CMC 命令行参考指南》。默认权限值为 0，表示用户没有启用任何权限。

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <index> <user privilege
bitmask value>
```

7

使用 iDRAC6 Directory Service

目录服务维护一个公用数据库，在其中存储网络上的用户、计算机、打印机等相关的信息。如果公司使用 Microsoft Active Directory 或 LDAP Directory Service 软件，则可以配置软件提供对 iDRAC6 的访问，以允许将 iDRAC6 用户权限添加到目录服务中的现有用户并对这些权限进行控制。

将 iDRAC6 用于 Microsoft Active Directory

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 iDRAC6 用户。

可以配置通过 Microsoft Active Directory 的用户验证以登录 iDRAC6。还可以提供基于角色的权限，使管理员能够为每个用户配置特定权限。有关详情，请参阅随后各节。

表　显示 iDRAC6 Active Directory 用户权限。

iDRAC6 用户权限

权限	说明
"Login to iDRAC"（登录到 iDRAC）	允许用户登录到 iDRAC6
"Configure iDRAC"（配置 iDRAC）	允许用户配置 iDRAC6
Configure Users（配置用户）	使用户可以允许特定用户访问系统
Clear Logs（清除日志）	允许用户清除 iDRAC6 日志
"Execute Server Control Commands"（执行服务器控制命令）	允许用户执行 RACADM 命令
"Access Virtual Console"（访问虚拟控制台）	允许用户运行虚拟控制台
"Access Virtual Media"（访问虚拟介质）	允许用户运行和使用虚拟介质

iDRAC6 用户权限 *（续）*

权限	说明
"Test Alerts"（检测警报）	允许用户将检测警报（电子邮件和 PET）发送给特定用户
"Execute Diagnostic Commands"（执行诊断命令）	允许用户运行诊断命令

您可使用以下方法之一通过 Active Directory 登录到 iDRAC6：

- 基于 Web 的界面
- 远程 RACADM
- Serial 或 Telnet 控制台

登录语法对于所有这三种方法都是一致的：

< *用户名* @ *域* >

或

< *域* >\< *用户名* > 或 < *域* >/< *用户名* >

其中*用户名*是含有 1-256 个字节的 ASCII 字符串。

用户名和域名中不能使用空格和特殊字符（例如 \、/ 或 @）。

注：不能指定 NetBIOS 域名，比如 Americas，因为这些名称无法解析。

如果从基于 Web 的界面登录且配置了用户域，则基于 Web 的界面登录页会在下拉式菜单中列出所有用户域供您选择。如果从下拉式菜单中选择一个用户域，则只需输入用户名。如果选择 **"This iDRAC"**（此 iDRAC），则只要您使用本节前文所述的登录语法，就能够以 Active Directory 用户的身份登录。

还可以使用智能卡或单一登录功能登录 iDRAC6。有关详情，请参阅第 169 页上的"配置 iDRAC6 进行单一登录或智能卡登录"。

注：Windows 2008 Active Directory 服务器仅支持最大长度为 256 个字符的 < *用户名* >@< *域名* > 字符串。

为 iDRAC6 启用 Microsoft Active Directory 验证的前提条件

要使用 iDRAC6 的 Active Directory 验证功能，必须已部署有 Active Directory 基础架构。请参阅 Microsoft 网站了解如何设置 Active Directory 基础架构 （如果尚未有）。

iDRAC6 使用标准公共密钥基础架构 (PKI) 机制来安全验证 Active Directory，因此，另外还需要 Active Directory 基础架构的集成 PKI。请参阅 Microsoft 网站了解有关 PKI 设置的详情。

要正确验证所有域控制器，还需要在 iDRAC6 连接的所有域控制器上启用安全套接字层 (SSL)。有关具体信息，请参阅第 131 页上的“在域控制器上启用 SSL”。

在域控制器上启用 SSL

当 iDRAC 针对 Active Directory 域控制器验证用户时，会启动与域控制器的 SSL 会话。此时，域控制器应发布由认证机构 (CA) 签署的证书 — 其根证书也上载到 iDRAC 中。换言之，要使 DRAC 能够验证到*任何*域控制器 — 无论是根还是子域控制器 — 该域控制器都应具有由域 CA 签署的启用了 SSL 的证书。

如果使用 Microsoft Enterprise Root CA *自动*分配所有域控制器到 SSL 证书，请执行下列步骤以在各个域控制器上启用 SSL：

通过安装每个控制器的 SSL 证书启用每个域控制器上的 SSL。

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）。
3. 在 **“Automatic Certificate Request Setup Wizard”**（自动证书申请设置向导）中，单击 **“Next”**（下一步）并选择 **“Domain Controller”**（域控制器）。
4. 单击 **“Next”**（下一步）并单击 **“Finish”**（完成）。

将域控制器根 CA 证书导出到 iDRAC6

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。

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. 在 **"Run"**（运行）字段中键入 `mmc` 并单击 **"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 account"**（计算机帐户）并单击 **"Next"**（下一步）。
8. 选择 **"Local Computer"**（本地计算机）并单击 **"Finish"**（完成）。
9. 单击 **OK**（确定）。
10. 在 **"Console 1"**（控制台 1）窗口中，展开 **"Certificates"**（证书）文件夹，展开 **"Personal"**（个人）文件夹并单击 **"Certificates"**（证书）文件夹。
11. 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 ...）。
12. 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，不导出私人密钥）。
13. 单击 **"Next"**（下一步）并选择 **"Base-64 encoded X.509 (.cer)"**（Base-64 编码 X.509 [.cer]）作为格式。
14. 单击 **"Next"**（下一步）并将证书保存至系统上的目录。
15. 将在步骤 14 保存的证书上载到 iDRAC。

    要使用 RACADM 上载证书，请参阅第 147 页上的 "使用 iDRAC6 基于 Web 的界面以扩展架构配置 Microsoft Active Directory" 或第 157 页上的 "使用 RACADM 以标准架构配置 Microsoft Active Directory"。

要使用基于 Web 的界面上载证书，请参阅第 147 页上的 “使用 iDRAC6 基于 Web 的界面以扩展架构配置 Microsoft Active Directory” 或第 154 页上的 “使用 iDRAC6 基于 Web 的界面以标准架构配置 Microsoft Active Directory”。

导入 iDRAC6 固件 SSL 证书

注：如果 Active Directory Server 设置为在 SSL 会话初始化阶段验证客户端，则还需要将 iDRAC6 Server 证书上载到 Active Directory 域控制器。如果 Active Directory 在 SSL 会话初始化期间不验证客户端，则不需要这一额外步骤。

使用下面的过程将 iDRAC6 固件 SSL 证书导入到域控制器信任的所有证书列表中。

注：如果系统运行 Windows 2000，以下步骤可能不同。

注：如果 iDRAC6 固件 SSL 证书是由公认的 CA 签署的，且该 CA 证书已经列入域控制器 “Trusted Root Certification Authority”（受信任的根认证机构）列表中，则无需执行本节的步骤。

iDRAC6 SSL 证书就是用于 iDRAC6 Web Server 的证书。所有 iDRAC 控制器都配备有默认自签证书。

要下载 iDRAC6 SSL 证书，请运行以下 RACADM 命令：

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 证书>
```

1. 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）。
2. 右键单击 **“Certificates”**（证书），选择 **“All Tasks”**（所有任务）并单击 **“Import”**（导入）。
3. 单击 **“Next”**（下一步）并浏览查找到 SSL 证书文件。
4. 在每个域控制器的 **“Trusted Root Certification Authority”**（受信任的根认证机构）中安装 iDRAC6 SSL 证书。

   如果已安装自己的证书，应确保签署您的证书的 CA 位于 **“Trusted Root Certification Authority”**（可信根认证机构）列表中。如果该机构不在列表中，必须在所有的域控制器上安装它。
5. 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。
6. 单击 **“Finish”**（完成）并单击 **“OK”**（确定）。

支持的 Active Directory 验证机制

可以通过两种方法使用 Active Directory 定义对 iDRAC6 的用户访问：一种方法是使用*扩展架构*解决方案，该解决方案经过 Dell 自定义后加入 Dell 定义的 Active Directory 对象。另一种方法是使用*标准架构*解决方案，该解决方案仅采用 Active Directory 组对象。有关这些解决方案的详情，请参阅随后各节。

当使用 Active Directory 配置对 iDRAC6 访问权限时，必须选择扩展架构解决方案或标准架构解决方案。

使用扩展架构解决方案的优势有：

- 所有权限控制对象都在 Active Directory 中设置。
- 支持用各种权限级别在不同 iDRAC6 上配置用户权限。

使用标准架构解决方案的优势是无需架构扩展，因为 Microsoft 的默认 Active Directory 架构配置已经提供所有必需的对象类。

扩展架构 Active Directory 概述

使用扩展架构解决方案要求 Active Directory 架构扩展，如以下一节所述。

Active Directory 架构扩展

Active Directory 数据是属性和类的分布式数据库。Active Directory 架构包含确定可添加或包含在数据库中的数据类型的规则。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以包括用户的名字、姓氏、电话号码等。公司可以通过添加自己独特的属性和类扩展 Active Directory 数据库以解决特定环境下的需求。Dell 扩展了该架构，包括必要的更改以支持远程管理验证和授权。

每个添加到现有 Active Directory 架构的属性或类都必须定义唯一的 ID。为了保证 ID 在整个业界是独特的，Microsoft 维护着一个 Active Directory 对象标识符 (OID) 数据库，从而在各公司向架构中添加扩展时，能够确保独特性并且相互间不会冲突。为了扩展 Microsoft Active Directory 中的架构， Dell 为添加到目录服务的属性和类申请了独特的 OID、独特的名称扩展以及独特链接的属性 ID。

Dell 扩展名：dell

Dell 基础 OID ：1.2.840.113556.1.8000.1280

RAC LinkID 范围：12070 到 12079

iDRAC 架构扩展概览

为了在各种客户环境中提供最大的灵活性，Dell 提供了一组属性，可以由用户根据所需结果进行配置。Dell 扩展了该架构以包括关联、设备和权限属性。关联属性用于将具有一组特定权限的用户或组与一个或多个 iDRAC 设备链接起来。这种模式给管理员提供了极大的灵活性，可以对网络上的用户、iDRAC 权限和 iDRAC 设备进行各种组合而无需增加太多的复杂性。

Active Directory 对象概览

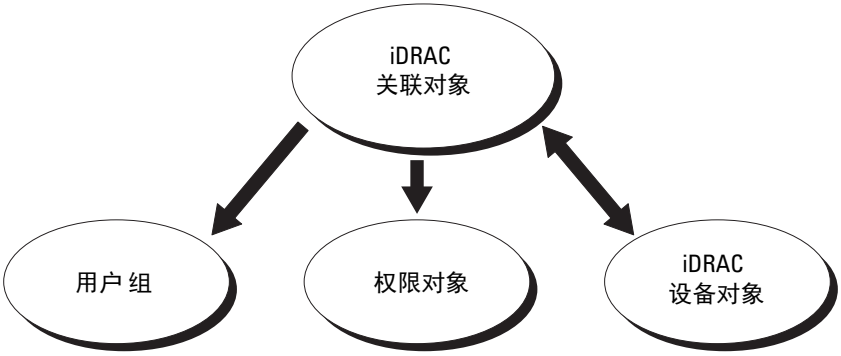
对于网络上每一个要与 Active Directory 集成以进行验证和授权的物理 iDRAC 来说，请创建至少一个关联对象和一个 iDRAC 设备对象。可以创建多个关联对象，每个关联对象都可以链接到任意多个用户、用户组或 iDRAC 设备对象。用户和 iDRAC 用户组可以是企业中任何域的成员。

不过，每个关联对象只能链接（或者可能链接用户、用户组或 iDRAC 设备对象）到一个权限对象。此示例允许管理员控制每个用户对特定 iDRAC 的权限。

iDRAC 设备对象就是指向 iDRAC 固件的链接，用于查询 Active Directory 以进行验证和授权。将 iDRAC 添加到网络后，管理员必须使用 Active Directory 名称配置 iDRAC 及其设备对象，以便用户可以使用 Active Directory 执行验证和授权。此外，管理员还必须将 iDRAC 添加到至少一个关联对象以使用户能够验证。

图 7-1 说明关联对象提供了进行所有验证和授权所需的连接。

图 7-1. Active Directory 对象的典型设置



可以根据需要创建任意数量的关联对象。不过，对于网络上每一个要与 Active Directory 集成以使用 iDRAC 验证和授权的 iDRAC 来说，必须创建至少一个关联对象和一个 iDRAC 设备对象。

关联对象允许任意数量的用户和 / 或组以及 iDRAC 设备对象。然而，每个关联对象只有一个权限对象。关联对象连接对 iDRAC 拥有*权限*的*用户*。

Active Directory 用户和计算机 MMC 管理单元的 Dell 扩展仅允许将来自相同域的权限对象和 iDRAC 对象与关联对象关联。 Dell 扩展不允许将其它域中的组或 iDRAC 对象添加为关联对象的产品成员。

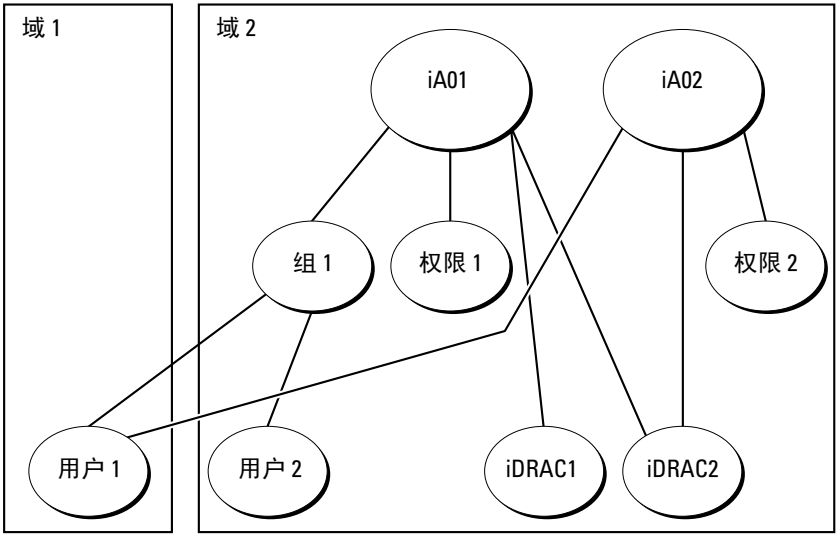
来自任何域的用户、用户组或嵌套的用户组都可以添加到关联对象中。扩展架构解决方案支持任何用户组类型和 Microsoft Active Directory 允许的多个域之间嵌入的任何用户组。

使用扩展架构累积权限

扩展架构验证机制支持对通过不同关联对象与同一用户相关的不同权限对象进行权限累积。换言之，扩展架构验证可以累积权限，使用户能够拥有与同一用户关联的不同权限对象对应的所有已分配权限的超级集合。

图 7-2 提供了使用扩展架构累积权限的示例。

图 7-2. 用户权限累积



该图显示了两个关联对象 — iA01 和 iA02。用户 1 通过两个关联对象与 iDRAC2 关联。因此，用户 1 具有累积权限，即在 iDRAC2 上将权限 1 和权限 2 的权限合并起来。

例如，权限 1 有如下权限：登录、虚拟介质和清除日志，而权限 2 有如下权限：登录到 iDRAC、配置 iDRAC 和检测警报。因此，用户 1 现在的权限集为：登录到 iDRAC、虚拟介质、清除日志、配置 iDRAC 和检测警报，这是权限 1 和权限 2 的权限集合的合并结果。

扩展架构验证利用同一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。

在此配置中，用户 1 对 iDRAC2 拥有权限 1 和权限 2 权限。用户 1 对 iDRAC1 仅拥有权限 1 权限。用户 2 对 iDRAC1 和 iDRAC2 都拥有权限 1 权限。此外，该图还表明用户 1 可位于不同的域并可以由嵌套组关联。

配置扩展架构 Active Directory 以访问 iDRAC6

在使用 Active Directory 访问 iDRAC6 之前，必须执行下列步骤配置 Active Directory 软件和 iDRAC6：

1. 扩展 Active Directory 架构 （请参阅第 138 页上的 “扩展 Active Directory 架构”）。
2. 扩展 Active Directory 用户和计算机管理单元 （请参阅第 143 页上的 “安装 Dell 对 Microsoft Active Directory 用户和计算机管理单元的 扩展”）。
3. 将 iDRAC6 用户及其权限添加到 Active Directory （请参阅第 145 页上的 “将 iDRAC 用户和权限添加到 Microsoft Active Directory”）。
4. 使用 iDRAC6 基于 Web 的界面或 RACADM 配置 iDRAC6 Active Directory 属性 （请参阅第 147 页上的 “使用 iDRAC6 基于 Web 的界面以扩展架构配置 Microsoft Active Directory”或第 149 页上的 “使用 RACADM 以扩展架构配置 Microsoft Active Directory”）。

扩展 Active Directory 架构

重要信息：此产品的架构扩展与前几代 Dell 远程管理产品不同。您必须扩展新架构并将新 Active Directory 用户和计算机 Microsoft 管理控制台 (MMC) 管理单元安装到目录中。旧架构不能用于此产品。

注：扩展新架构或将新扩展安装到 Active Directory 用户和计算机管理单元对以前的产品无影响。

Dell Systems Management Tools and Documentation DVD 上提供了 Schema Extender 和 Active Directory 用户和计算机 MMC 管理单元扩展。有关安装这些扩展的信息，请参阅第 143 页上的 “安装 Dell 对 Microsoft Active Directory 用户和计算机管理单元的 扩展”。有关扩展 iDRAC6 的架构和安装 Active Directory 用户和计算机 MMC 管理单元的进一步详情，请参阅 **dell.com/support/manuals** 上的 《Dell OpenManage 安装和安全用户指南》。

注：在您创建 iDRAC 关联对象或 iDRAC 设备对象时，请确保选择了 “Dell Remote Management Object Advanced”（Dell 高级远程管理对象）。

扩展 Active Directory 架构将会在 Active Directory 架构中添加一个 Dell 组织单元、架构类和属性以及示例权限和关联对象。扩展架构前，确保在域目录林的 “架构主机灵活单主机操作 (FSMO) 角色所有者”上具有 “Schema Admin”（架构管理员）权限。

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，将不会把 Dell 组织单元添加到架构。

LDIF 文件和 Dell Schema Extender 分别位于 *Dell Systems Management Tools and Documentation* DVD 的以下目录中：

- *DVD 驱动器*:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <DVD *驱动器*>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender

注：Remote_Management 文件夹用于在较早的远程访问产品如 DRAC 4 和 DRAC 5 上扩展架构，而 Remote_Management_Advanced 文件夹用于在 iDRAC6 上扩展架构。

要使用 LDIF 文件，请参阅 **LDIF_Files** 目录中自述文件中的说明。要使用 Dell Schema Extender 扩展 Active Directory 架构，请参阅第 139 页上的“使用 Dell Schema Extender”。

可以从任意位置复制并运行 Schema Extender 或 LDIF 文件。

使用 Dell Schema Extender

注：Dell Schema Extender 使用 SchemaExtenderOem.ini 文件。要确保 Dell Schema Extender 公用程序运行正常，请勿修改该文件的名称。

1. 在 **Welcome**（欢迎）屏幕中单击 **Next**（下一步）。
2. 阅读并了解警告，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）。

   架构将会扩展。要验证架构扩展情况，请使用 MMC 和 Active Directory 架构管理单元验证以下项是否存在：

   - 类（请参阅表 7-1 到表 7-6）
   - 属性（表 7-7）

有关使用 MMC 和 Active Directory 架构管理单元的详情，请参阅 Microsoft 说明文件。

表 7-1. 添加到 Active Directory 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
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 7-2. dellRacDevice 类

OID	1.2.840.113556.1.8000.1280.1.7.1.1
说明	表示 Dell iDRAC 设备。 iDRAC 设备必须在 Active Directory 中配置为 delliDRACDevice。这种配置使 iDRAC 能够向 Active Directory 发送轻量级目录访问协议 (LDAP) 查询。
类的类型	结构类
超类	dellProduct
属性	dellSchemaVersion dellRacType

表 7-3. delliDRACAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.7.1.2
说明	表示 Dell 关联对象。关联对象提供用户和设备之间的连接。
类的类型	结构类
超类	组
属性	dellProductMembers dellPrivilegeMember

表 7-4. dellRAC4Privileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.3
说明	用于为 iDRAC 设备定义权限 （授权权限）。
类的类型	辅助类
超类	None （无）
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 7-5. dellPrivileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.4
说明	用作 Dell 权限 （授权权限）的容器类。
类的类型	结构类
超类	User （用户）
属性	dellRAC4Privileges

表 7-6. 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 7-7. 添加到 Active Directory 架构的属性的列表

属性名称 / 说明	分配的 OID/ 语法对象标识符	单值
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE
属于此属性的 dellPrivilege 对象的列表。	可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers	1.2.840.113556.1.8000.1280.1.1.2.2	FALSE
属于此角色的 dellRacDevice 和 DelliDRACDevice 对象的列表。此属性是指向 dellAssociationMembers 后退链接的前进链接。 链接 ID: 12070	可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellIsLoginUser	1.2.840.113556.1.8000.1280.1.1.2.3	TRUE
如果用户具有设备的登录权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsCardConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.4	TRUE
如果用户具有设备的卡配置权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	TRUE
如果用户具有设备的用户配置权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
delIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
如果用户具有设备的日志清除权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
如果用户具有设备的服务器重设权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE
如果用户具有设备的虚拟控制台权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9	TRUE
如果用户具有设备的虚拟介质权限，则为 TRUE。	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

表 7-7. 添加到 Active Directory 架构的属性的列表 *（续）*

属性名称 / 说明	分配的 OID/ 语法对象标识符	单值
dellIsTestAlertUser 如果用户具有设备的检测警报用户权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin 如果用户具有设备的调试命令管理员权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion 当前架构版本用于更新架构。	1.2.840.113556.1.8000.1280.1.1.2.12 不区分大小写的字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType 此属性是 delliDRACDevice 对象的当前 RAC 类型以及到 dellAssociationObjectMembers 前进链接的后退链接。	1.2.840.113556.1.8000.1280.1.1.2.13 不区分大小写的字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers 属于此产品的 dellAssociationObjectMembers 的列表。此属性是到 dellProductMembers 链接属性的后退链接。 链接 ID：12071	1.2.840.113556.1.8000.1280.1.1.2.14 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

扩展 Active Directory 中的架构时，还必须扩展 Active Directory 用户和计算机管理单元，以使管理员能够管理 iDRAC 设备、用户和用户组、iDRAC 关联和 iDRAC 权限。

使用 *Dell Systems Management Tools and Documentation* DVD 安装系统管理软件时，可以通过在安装过程中选择 **"Active Directory Users and Computers Snap-in"**（Active Directory 用户和计算机管理单元）选项来安装管理单元。请参阅 《Dell OpenManage 软件快速安装指南》进一步了解如何安装系统管理软件。对于 x64 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情，请参阅 Microsoft 说明文件。

安装 Administrator Pack

必须在管理 Active Directory iDRAC 对象的每个系统上安装 Administrator Pack。如果不安装 Administrator Pack，将无法在容器中查看 Dell iDRAC 对象。

有关更多信息，请参阅第 144 页上的 "打开 Microsoft Active Directory 用户和计算机管理单元"。

打开 Microsoft Active Directory 用户和计算机管理单元

要打开 Active Directory 用户和计算机管理单元：

1. 如果登录到域控制器，则单击 **Start**（开始）→ **Admin Tools**（管理工具）→ **Active Directory Users and Computers**（Active Directory 用户和计算机）。

   如果没有登录到域控制器上，则必须在本地系统上安装相应的 Microsoft Administrator Pack。要安装此 Administrator Pack，请单击 **"Start"**（开始）→ **"Run"**（运行），键入 `MMC` 并按 **Enter**。

   将显示 MMC。

2. 在 **Console 1**（控制台 1）窗口中，单击 **File**（文件）（如果是运行 Windows 2000 的系统，则单击 **Console**（控制台））。
3. 单击 **Add/Remove Snap-in**（添加 / 删除管理单元）。
4. 选择 **"Active Directory Users and Computers Snap-in"**（Active Directory 用户和计算机管理单元）并单击 **"Add"**（添加）。
5. 单击 **Close**（关闭）并单击 **OK**（确定）。

将 iDRAC 用户和权限添加到 Microsoft Active Directory

通过使用 Dell 扩展的 Active Directory 用户和计算机管理单元，您能够通过创建 iDRAC、关联和权限对象添加 iDRAC 用户和权限。要添加每种对象类型，请执行以下过程：

- 创建 iDRAC 设备对象
- 创建权限对象
- 创建关联对象
- 配置关联对象

创建 iDRAC 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 远程管理高级对象）。

   将显示 New Object （新建对象）窗口。
3. 为新对象键入名称。该名称必须与准备在第 147 页上的 "使用 iDRAC6 基于 Web 的界面以扩展架构配置 Microsoft Active Directory" 的步骤 A 中键入的 iDRAC 名称相同。
4. 选择 **"iDRAC Device Object"**（iDRAC 设备对象）。
5. 单击 OK （确定）。

创建权限对象

注：权限对象必须和相关关联对象创建在同一个域中。

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 远程管理高级对象）。

   将显示 New Object （新建对象）窗口。
3. 为新对象键入名称。
4. 选择 **"Privilege Object"**（权限对象）。
5. 单击 OK （确定）。

6 右键单击创建的权限对象并选择 Properties （属性）。

7 单击 **"Remote Management Privileges"**（远程管理权限）选项卡并选择要让用户具有的权限。

创建关联对象

注：iDRAC 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 远程管理高级对象）。

这将打开 New Object （新建对象）窗口。

3 为新对象键入名称。

4 选择 Association Object （关联对象）。

5 单击 OK （确定）。

配置关联对象

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 iDRAC 设备。

可以添加用户组。创建 Dell 相关的组和非 Dell 相关的组的过程相同。

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 键入用户或用户组名称并单击 OK （确定）。

单击 **"Privilege Object"**（权限对象）选项卡将权限对象添加到验证 iDRAC 设备时定义用户或用户组权限的关联。只能将一个权限对象添加到关联对象。

添加权限

1 选择 Privileges Object （权限对象）选项卡，并单击 Add （添加）。

2 键入权限对象名称并单击 OK （确定）。

单击 **"Products"**（产品）选项卡添加一个连接到网络的 iDRAC 设备，供所定义的用户或用户组使用。可以将多个 iDRAC 设备添加到关联对象。

添加 iDRAC 设备

要添加 iDRAC 设备：

1. 选择 Products （产品）选项卡并单击 Add （添加）。
2. 键入 iDRAC 设备名称并单击 **"OK"**（确定）。
3. 在 Properties （属性）窗口中，单击 Apply （应用），并单击 OK （确定）。

使用 iDRAC6 基于 Web 的界面以扩展架构配置 Microsoft Active Directory

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 基于 Web 的界面。
3. 转至 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）选项卡 → **"Directory Service"**（目录服务）选项卡 → Microsoft Active Directory。
4. 滚动到 **"Active Directory Configuration and Management"**（Active Directory 配置和管理）页底部，然后单击 **"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。
5. 在 **"Certificate Settings"**（证书设置）下面，如果要验证 Active Directory 服务器的 SSL 证书，则选择 **"Enable Certificate Validation"**（启用证书验证）；否则，转至步骤 9。
6. 在 **"Upload Active Directory CA Certificate"**（上载 Active Directory CA 证书）下面，键入证书文件路径或浏览找到证书文件。

   注：必须键入绝对文件路径，包括全路径和完整文件名及文件扩展名。
7. 单击 **"Upload"**（上载）。

   将显示上载的 Active Directory CA 证书的证书信息。
8. **（可选：用于 AD 验证）**在 **"Upload Kerberos Keytab"**（上载 Kerberos Keytab）下，键入 Keytab 文件的路径或浏览查找该文件。单击 **"Upload"**（上载）。 Kerberos Keytab 将会上载到 iDRAC6。
9. 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。
10. 选择 **"Enable Active Directory"**（启用 Active Directory）。

小心：在此版本中，如果 Active Directory 配置为使用扩展架构，则不支持基于智能卡的双重验证 (TFA) 功能。对于标准架构和扩展架构都支持单一登录 (SSO) 功能。

11 单击 **"Add"**（添加）以输入用户域名。

12 在提示符处键入用户域名并单击 **"OK"**（确定）。

注：此步骤是可选的。如果您配置用户域列表，则会在 Web 界面登录屏幕上显示。您可从列表中选择，然后只需键入用户名。

13 在 **"Timeout"**（超时）字段中，键入 iDRAC 必须等待 Active Directory 应答的时间 （秒）。默认值为 120 秒钟。

14 选择以下选项之一：

a **"Look Up Domain Controllers with DNS"**（利用 DNS 查找域控制器）选项，可从 DNS 查找中获得 Active Directory 域控制器。忽略域控制器服务器地址 1-3。选择 **"User Domain from Login"**（登录的用户域）可使用登录用户的域名进行 DNS 查找。或者，选择 **"Specify a Domain"**（指定域）并输入要在 DNS 查找中使用的域名。 iDRAC6 会逐一尝试连接每个地址 （前 4 个地址由 DNS 查找返回），直到成功建立连接为止。对于**扩展架构**，这些是 iDRAC6 设备对象和关联对象所在的域控制器。

b **"Specify Domain Controller Addresses"**（指定域控制器地址）选项，允许 iDRAC6 使用指定的 Active Directory 域控制器服务器地址。未执行 DNS 查找。指定域控制器的 IP 地址或完全限定域名 (FQDN)。如果选择 **"Specify Domain Controller Addresses"**（指定域控制器地址）选项，则三个地址必须至少配置一个。iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。对于**扩展架构**，这些地址是 iDRAC6 设备对象和关联对象所在的域控制器的地址。

注：在 "Domain Controller Server Address"（域控制器服务器地址）字段中指定的 FQDN 或 IP 地址应与域控制器证书 （如果已启用证书验证）的 "Subject"（主题）或 "Subject Alternative Name"（主题备用名称）字段相符。

15 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。

16 在 **"Schema Selection"**（架构选择）下，单击 **"Extended Schema"**（扩展架构）。

17 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。

18 在 **"Extended Schema Settings"**（扩展架构设置）下，键入 **iDRAC 名称**和 **iDRAC 域名**以配置 iDRAC 设备对象。 iDRAC 域名是创建 iDRAC 对象所在的域的名称。

19 单击 **"Finish"**（完成）以保存 Active Directory 扩展架构设置。

iDRAC6 Web Server 自动返回 **"Active Directory Configuration and Management"**（Active Directory 配置和管理）页。

20 单击 **"Test Settings"**（检测设置）以检查 Active Directory 扩展架构设置。

21 键入 Active Directory 用户名和密码。

将显示检测结果和检测日志。有关其它信息，请参阅第 160 页上的"检测配置"。

注：您必须在 iDRAC 上正确配置 DNS 服务器，才能支持 Active Directory 登录。单击 "iDRAC Settings"（iDRAC 设置）→ "Network/Security"（网络 / 安全性）→ "Network"（网络）页，手动配置 DNS 服务器或使用 DHCP 获得 DNS 服务器。

现在完成了以扩展架构配置 Active Directory 的过程。

使用 RACADM 以扩展架构配置 Microsoft Active Directory

使用以下命令，通过 RACADM CLI 工具而不是 Web 界面以扩展架构配置 iDRAC6 Microsoft Active Directory 功能。

1 打开命令提示符并键入以下 RACADM 命令：

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

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o
cfgADRacName <RAC 常用名>

racadm config -g cfgActiveDirectory -o
cfgADRacDomain <完全限定的 rac 域名>

racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <域控制器的完全限定域名或 IP 地址>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <域控制器的完全限定域名或 IP 地址>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <域控制器的完全限定域名或 IP 地址>
```

注：要求至少配置 3 个地址之一。 iDRAC 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。选择扩展架构选项时，这些地址是此 iDRAC 设备所在的域控制器的 FQDN 或 IP 地址。在扩展架构模式下根本不使用全局编录服务器。

注：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。

小心：在此版本中，如果 Active Directory 配置为使用扩展架构，则不支持基于智能卡的双重验证 (TFA) 功能。对于标准架构和扩展架构都支持单一登录 (SSO) 功能。

如果要使用 DNS 查找获取 Active Directory 域控制器服务器地址，键入以下命令：

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable=1
```

- 要使用登录用户的域名执行 DNS 查找：

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain=1
  ```

- 要指定在 DNS 查找中使用的域名：

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <在 DNS 查找中使用的域名>
  ```

如果要禁用 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

在此情况下，您无需上载 CA 证书。

如果要执行 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

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

在此情况下，您需要使用以下 RACADM 命令上载 CA 证书：

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

```
racadm sslcertupload -t 0x2 -f <ADS 根 CA 证书>
```

以下 RACADM 命令可选。有关其它信息，请参阅第 133 页上的“导入 iDRAC6 固件 SSL 证书”。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 证书>
```

2 如果要指定 Active Directory (AD) 查询完成前需等待多少秒才超时，键入以下命令：

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <以秒为单位的时间>
```

3 如果 iDRAC 上已启用 DHCP 并且希望使用 DHCP 服务器提供的 DNS，则键入以下 RACADM 命令：

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 1
```

4 如果 iDRAC 上已禁用 DHCP 或者想手动输入 DNS IP 地址，则键入以下 RACADM 命令：

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<主要 DNS IP 地址>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
<次要 DNS IP 地址>
```

5 如果要配置用户域列表，以便在登录到 iDRAC6 基于 Web 的界面时只需输入用户名，则键入以下命令：

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <索引>
```

您最多可配置 40 个用户域，其索引编号为 1 至 40。

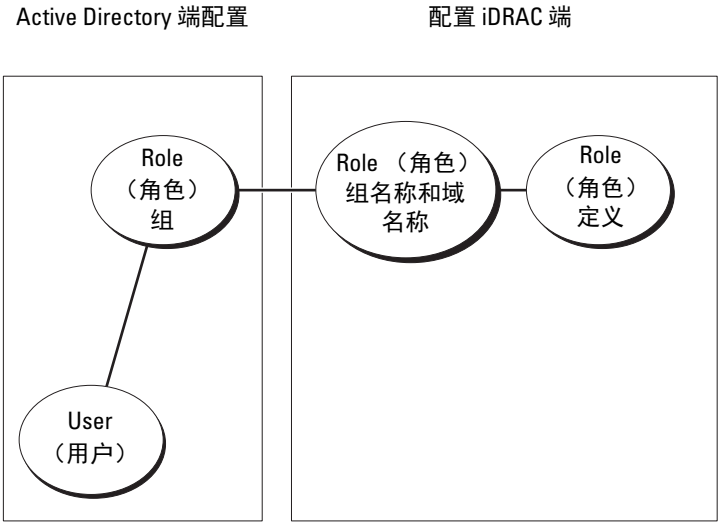
请参阅第 161 页上的 “通用 LDAP 目录服务”了解关于用户域的详情。

6 按 Enter 完成以扩展架构配置 Active Directory 的过程。

标准架构 Active Directory 概述

如图 7-3 中所示，为 Active Directory 集成而使用标准架构时需要在 Active Directory 和 iDRAC6 上都进行配置。

图 7-3. 使用 Microsoft Active Directory 和标准架构配置 iDRAC



在 Active Directory 端，标准组对象用作角色组。具有 iDRAC6 权限的用户将是该角色组的成员。为了授予该用户对特定 iDRAC6 的权限，需要在特定 iDRAC6 上配置角色组名称及其域名。与扩展架构解决方案不同，角色和权限级别在各个 iDRAC6 上定义，而不是在 Active Directory 中定义。每个 iDRAC 中可配置和定义多达五个角色组。表 7-8 显示默认的角色组权限。

注：所有五个角色组的 “Default Role Group Privilege Level”（默认角色组权限级别）均为 “None”（无）。您必须从下拉列表框中选择一个默认角色组权限。

表 7-8. 默认角色组权限

权限级别	授予的权限	位掩码
管理员	“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”（检测警报）、“Execute Diagnostic Commands”（执行诊断命令）	0x000001ff
“Operator”（操作员）	“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”（检测警报）、“Execute Diagnostic Commands”（执行诊断命令）	0x000000f9
只读	“Login to iDRAC”（登录到 iDRAC）	0x00000001
None （无）	没有分配权限	0x00000000

注：“位掩码”值只有在用 RACADM 设置标准架构时才使用。

单域和多域情况

如果所有登录用户和角色组以及嵌套组都在相同域中，则只须在 iDRAC6 上配置域控制器地址。在此单域情况下，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，则要求在 iDRAC6 上配置全局编录服务器地址。在此多域情况下，所有角色组和嵌套组（如有）都必须为通用组类型。

配置标准架构 Microsoft Active Directory 访问 iDRAC6

必须执行下列步骤配置 Active Directory， Active Directory 用户才能访问 iDRAC6：

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. 创建组或选择现有组。添加 Active Directory 用户作为 Active Directory 组的成员以访问 iDRAC6。
3. 使用基于 Web 的界面或 RACADM 在 iDRAC6 上配置组名称和域名。有关更多信息，请参阅第 154 页上的“使用 iDRAC6 基于 Web 的界面以标准架构配置 Microsoft Active Directory”或第 157 页上的 “使用 RACADM 以标准架构配置 Microsoft Active Directory”。

使用 iDRAC6 基于 Web 的界面以标准架构配置 Microsoft Active Directory

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 基于 Web 的界面。
3. 转至 **“iDRAC Settings”**（iDRAC 设置） → **“Network/Security”**（网络 / 安全性）选项卡 → **“Directory Service”**（目录服务）选项卡 → **Microsoft Active Directory**。
4. 滚动到 **“Active Directory Configuration and Management”**（Active Directory 配置和管理）页底部，然后单击 **“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。
5. 在 **“Certificate Settings”**（证书设置）下面，如果要验证 Active Directory 服务器的 SSL 证书，则选择 **“Enable Certificate Validation”**（启用证书验证）；否则，转至步骤 9。
6. 在 **“Upload Active Directory CA Certificate”**（上载 Active Directory CA 证书）下，浏览以查找证书文件。
7. 单击 **“Upload”**（上载）。

   将显示有效 Active Directory CA 证书的证书信息。

8 （可选：用于 AD 验证）在 **"Upload Kerberos Keytab"**（上载 Kerberos Keytab）下，键入 Keytab 文件的路径或浏览查找该文件。单击 **"Upload"**（上载）。 Kerberos Keytab 将会上载到 iDRAC6。

9 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。

10 选择 **"Enable Active Directory"**（启用 Active Directory）。

11 如果想不输入域用户验证凭据 （比如用户名和密码）就登录 iDRAC6，则选择 **"Enable Single Sign-On"**（启用单一登录）。

12 单击 **"Add"**（添加）以输入用户域名。

13 在提示符处键入用户域名并单击 **"OK"**（确定）。

14 在 **"Timeout"**（超时）字段中，键入 iDRAC 必须等待 Active Directory 应答的时间 （秒）。默认值为 120 秒钟。

15 选择以下选项之一：

a **"Look Up Domain Controllers with DNS"**（利用 DNS 查找域控制器）选项，可从 DNS 查找中获得 Active Directory 域控制器。忽略域控制器服务器地址 1-3。选择 **"User Domain from Login"**（登录的用户域）可使用登录用户的域名进行 DNS 查找。或者，选择 **"Specify a Domain"**（指定域）并输入要在 DNS 查找中使用的域名。 iDRAC6 会逐一尝试连接每个地址 （前 4 个地址由 DNS 查找返回），直到成功建立连接为止。对于**标准架构**，域控制器是用户帐户和角色组所在的地址。

b 选择 **"Specify Domain Controller Addresses"**（指定域控制器地址）选项，允许 iDRAC6 使用指定的 Active Directory 域控制器服务器地址。未执行 DNS 查找。指定域控制器的 IP 地址或完全限定域名 (FQDN)。如果选择 **"Specify Domain Controller Addresses"**（指定域控制器地址）选项，则三个地址必须至少配置一个。iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。对于**标准架构**，这些是用户帐户和角色组所在域控制器的地址。

注：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。

16 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。

17 在 **"Schema Selection"**（架构选择）下，选择 **"Standard Schema"**（标准架构）。

18 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。

19 选择以下选项之一：

- 选择 **"Look Up Global Catalog Servers with DNS"**（使用 DNS 查找全局编录服务器）选项并输入用于 DNS 查找的 **"Root Domain Name"**（根域名）来获取 Active Directory 全局编录服务器。将会忽略全局编录服务器地址 1-3。iDRAC6 会尝试逐一连接到每个地址（由 DNS 查找返回的前 4 个地址），直到成功建立连接为止。仅当用户帐户和角色组位于不同域中时，标准架构才需要全局编录服务器。
- 选择 **"Specify Global Catalog Server Addresses"**（指定全局编录服务器地址）选项，并输入全局编录服务器的 IP 地址或完全限定域名 (FQDN)。未执行 DNS 查找。必须至少配置 3 个地址之一。iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。仅当用户帐户和角色组位于不同域中时，才需要为标准架构设置全局编录服务器。

注：在 "Global Catalog Server Addresses"（全局编录服务器地址）字段中指定的 FQDN 或 IP 地址应与域控制器证书（如果已启用证书验证）的 "Subject"（主题）或 "Subject Alternative Name"（主题备用名称）字段相符。

注：仅当用户帐户和角色组位于不同域中时，标准架构才需要全局编录服务器。而在此多域情况下，仅可使用通用组。

20 在 **"Role Groups"**（角色组）下，单击 **"Role Groups"**（角色组）。

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。

21 指定 **"Role Group Name"**（角色组名称）。

"Role Group Name"（角色组名称）标识与 iDRAC 关联的 Active Directory 角色组。

22 指定 **"Role Group Domain"**（角色组域），这是角色组的域。

23 通过选择 **"Role Group Privilege Level"**（角色组权限级别），指定 **"Role Group Privileges"**（角色组权限）。例如，如果选择 **"Administrator"**（管理员），则为该权限级别选择所有权限。

24 单击 **"Apply"**（应用）保存角色组设置。

iDRAC6 Web Server 自动返回 **"Step 4a of 4 Active Directory Configuration and Management"**（第 4a 步，共 4 步 Active Directory 配置和管理）页，该页显示了设置。

25 如果需要，配置其它角色组。

26 单击 **"Finish"**（完成）返回 **"Active Directory Configuration and Management"**（Active Directory 配置和管理）页。

27 单击 **"Test Settings"**（检测设置）以检查 Active Directory 标准架构设置。

28 键入 iDRAC6 用户名和密码。

将显示检测结果和检测日志。有关其它信息，请参阅第 160 页上的"检测配置"。

注：您必须在 iDRAC 上正确配置 DNS 服务器，才能支持 Active Directory 登录。单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）→ **"Network"**（网络）页，手动配置 DNS 服务器或使用 DHCP 获得 DNS 服务器。

现在完成了以标准架构配置 Active Directory 的过程。

使用 RACADM 以标准架构配置 Microsoft Active Directory

通过 RACADM CLI 而不是基于 Web 的界面，使用以下命令以标准架构配置 iDRAC Active Directory 功能。

1 打开命令提示符并键入以下 RACADM 命令：

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <索引> -o
cfgSSADRoleGroupName <角色组常用名>
racadm config -g cfgStandardSchema -i <索引> -o
cfgSSADRoleGroupDomain <完全限定域名>
racadm config -g cfgStandardSchema -i <索引> -o
cfgSSADRoleGroupPrivilege <特定用户权限的位掩码编号>
```

注：有关位掩码编号值，请参阅 Dell 支持网站 dell.com/support/manuals 上的《RACADM iDRAC6 和 CMC 命令行参考指南》。

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <域控制器的完全限定域名或 IP 地址>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <域控制器的完全限定域名或 IP 地址>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <域控制器的完全限定域名或 IP 地址>
```

注：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。

注：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`。

注：要求至少配置 3 个地址之一。iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。对于标准架构来说，这些是用户帐户和角色组所在域控制器的地址。

如果要使用 DNS 查找获取 Active Directory 域控制器服务器地址，键入以下命令：

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

- 要使用登录用户的域名执行 DNS 查找：

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

- 要指定在 DNS 查找中使用的域名：

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <在 DNS 查找中使用的域名>
  ```

要指定全局编录服务器地址，请键入以下命令：

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog1 <域控制器的完全限定域名或 IP 地址>
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog2 <域控制器的完全限定域名或 IP 地址>
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog3 <域控制器的完全限定域名或 IP 地址>
```

注：仅当用户帐户和角色组位于不同域中时，标准架构才需要全局编录服务器。而在此多域情况下，仅可使用通用组。

注：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。

如果要使用 DNS 查找获取 Active Directory 全局编录服务器地址，键入以下命令：

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

```
racadm config -g cfgActiveDirectory -o
cfgADGcRootDomain <域名>
```

如果要禁用 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

在此情况下，无需上载认证机构 (CA) 证书。

如果要执行 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

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

在此情况下，也必须使用以下 RACADM 命令上载 CA 证书：

```
racadm sslcertupload -t 0x2 -f <ADS 根 CA 证书>
```

以下 RACADM 命令可选。有关其它信息，请参阅第 133 页上的 “导入 iDRAC6 固件 SSL 证书”。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 证书>
```

2 如果要指定 Active Directory (AD) 查询完成前需等待多少秒才超时，键入以下命令：

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <以秒为单位的时间>
```

3 如果 iDRAC6 上已启用 DHCP 并且希望使用 DHCP 服务器提供的 DNS，则键入以下 RACADM 命令：

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 1
```

4 如果 DRAC6 上已禁用 DHCP 或者想手动输入 DNS IP 地址，则键入以下 RACADM 命令：

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<主要 DNS IP 地址>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
<次要 DNS IP 地址>
```

5 如果要配置用户域列表以便在登录到基于 Web 的界面时只需输入用户名，则键入以下命令：

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <索引>
```

可以配置最多 40 个用户域，索引编号为 1 到 40。有关用户域的详情，请参阅第 161 页上的 “通用 LDAP 目录服务”。

检测配置

如果要验证配置是否正确，或需要诊断 Active Directory 登录失败问题，则可以在 iDRAC6 基于 Web 的界面上检测设置。

在 iDRAC6 基于 Web 的界面中完成配置设置后，单击页面底部的 **“Test Settings”**（检测设置）。必须输入检测用户的名称 （例如 username@domain.com）和密码才能运行检测。根据您的配置，完成所有检测步骤和显示每步结果可能需要一些时间。详细的检测日志将在结果页面底部显示。

如果任何步骤失败，请查看检测日志中的详情以识别问题和可能的解决方案。关于最常见的错误，请参阅第 165 页上的 “关于 Active Directory 的常见问题”。

如果需要对设置做出更改，请单击 **Active Directory** 选项卡并逐步更改配置。

通用 LDAP 目录服务

iDRAC6 提供了一个通用的解决方案，支持基于轻型目录访问协议 (LDAP) 的验证。此功能无需服务目录的任何架构扩展。

为使 iDRAC6 LDAP 实施能够通用化，借助了不同目录服务间的共同之处来归类用户并建立用户和组关系映射。目录服务的特定操作是架构。例如，用户和组之间的组、用户和链接有不同的属性名称。这些操作可在 iDRAC6 中配置。

登录语法 （目录用户与本地用户）

与 Active Directory 不同，特殊字符 （“@”、“\” 和 “/”）不能用于区分 LDAP 用户和本地用户。登录用户只应输入用户名，不包括域名。iDRAC6 保持用户名的现状，不会分开用户名和用户域。在启用通用 LDAP 后， iDRAC6 首先尝试作为目录用户登录。如果失败，则启用本地用户查找。

注：在 Active Directory 登录语法中不做任何更改。如果启用通用 LDAP，GUI 登录页会在下拉菜单只显示 “This iDRAC”（此 iDRAC）。

注：对于基于 openLDAP 和 OpenDS 的目录服务，不允许在用户名中使用 “< “和” >”字符。

使用 iDRAC6 Web 界面配置通用 LDAP 目录服务

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 基于 Web 的界面。
3. 转至 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）选项卡 → **“Directory Service”**（目录服务）选项卡 → **“Generic LDAP Directory Service”**（通用 LDAP 目录服务）。

   “Generic LDAP Configuration and Management”（通用 LDAP 配置和管理）页中显示当前的 iDRAC6 通用 LDAP 设置。滚动到 **“Generic LDAP Configuration and Management”**（通用 LDAP 配置和管理）页的底部，并单击 **“Configure Generic LDAP”**（配置通用 LDAP）。

   将显示 **“Generic LDAP Configuration and Management Step 1 of 3”**（通用 LDAP 配置和管理第 1 步，共 3 步）页。使用此页配置在与通用 LDAP 服务器通信时， SSL 连接初始化中所使用的数字证书。这些通信使用 SSL 上的 LDAP (LDAPS)。如果启用证书验证，则上载由认证机构 (CA) 颁发、LDAP 服务器在初始化 SSL 连接时所使用的证书。认证机构 (CA) 的证书用于验证由 LDAP 服务器在 SSL 初始化时提供的证书的真实性。

注：在此版本中，不支持基于 LDAP 绑定的非 SSL 端口。仅支持 SSL 上的 LDAP。

4 在 **"Certificate Settings"**（证书设置）下，选择 **"Enable Certificate Validation"**（启用证书验证）启用证书验证。如果启用， iDRAC6 在安全套接字层 (SSL) 握手过程中使用 CA 证书来验证 LDAP 服务器证书；如果禁用，则 iDRAC6 跳过 SSL 握手的证书验证步骤。在测试期间或者如果系统管理员选择信任安全边界内的域控制器而无需验证他们的 SSL 证书，则禁用证书验证。

小心：确保在证书生成时，LDAP 服务器证书主题字段中的 "CN = 打开 LDAP FQDN" 已设置 （例如 CN= openldap.lab）。 iDRAC6 中的 LDAP 服务器地址字段应设置为使证书验证能够起作用的 FQDN 地址。

5 在 **"Upload Directory Service CA Certificate"**（上载目录服务 CA 证书）下面，键入证书文件路径或浏览找到证书文件。

注：必须键入绝对文件路径，包括全路径和完整文件名及文件扩展名。

6 单击 **"Upload"**（上载）。

上载根 CA 的证书，该证书用于签署所有域控制器的安全套接字层 (SSL) 服务器证书。

7 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。使用此页可配置通用 LDAP 和用户帐户的位置信息。

注：在此版本中，不支持基于智能卡的双重验证 (TFA) 和单一登录 (SSO) 功能用于通用 LDAP 目录服务。

8 输入以下信息：

- 选择 **"Enable Generic LDAP"**（启用通用 LDAP）。

注：在此版本中，不支持嵌套组。固件将搜索与用户 DN 相匹配的组的直接成员。并且仅支持单域。不支持交叉域。

- 选择 **"Use Distinguished Name to Search Group Membership"**（使用可分辨名称搜索组成员）选项将可分辨名称 (DN) 用于组成员。 iDRAC6 将从目录中检索的用户 DN 与组成员进行比较。如果已清除，则使用由登录用户提供的用户名与组成员进行比较。
- 在 **"LDAP Server Address"**（LDAP 服务器地址）字段中，输入 LDAP 服务器的完全限定域名 (FQDN) 或 IP 地址。要指定位于相同域的多个冗余 LDAP 服务器，请提供所有服务器的列表 （用逗号隔开）。 iDRAC6 会尝试依次连接到每个服务器，直到建立连接为止。

- 在 **"LDAP Server Port"**（LDAP 服务器端口）字段中输入 SSL 上的 LDAP 所使用的端口。默认为 636。
- 在 **"绑定 DN"**（Bind DN）字段中，输入在搜索登录用户 DN 时用于绑定服务器的用户 DN。如果未指定，则使用匿名绑定。
- 输入 **"Bind DN"**（绑定 DN）所使用的 **"Bind Password"**（绑定密码）。如果不允许匿名绑定，则此项为必填项。
- 在 **"Base DN to Search"**（要搜索的基本 DN）字段中，输入开始所有搜索所在目录的分支 DN。
- 在 **"Attribute of User Login"**（用户登录属性）字段中，输入要搜索的用户属性。默认为 UID。建议：在选定的基本 DN 中此值应是独特的，否则，必须配置搜索筛选器以确保登录用户的独特性。如果用户 DN 无法通过搜索属性组合和搜索筛选器唯一识别，则登录失败。
- 在 **"Attribute of Group Membership"**（组成员属性）字段中，指定使用哪个 LDAP 属性来检查组成员。它应是一个组类属性。如果未指定， iDRAC6 使用*成员*和*独特成员*属性。
- 在 **"Search Filter"**（搜索筛选器）字段中，输入有效的 LDAP 搜索筛选器。如果用户属性无法唯一识别选定的基本 DN 中的登录用户，则使用筛选器。如果未指定，默认为 *objectClass*=*，表示搜索树中的所有对象。由用户配置的附加搜索筛选器仅适用于用户 DN 搜索，而不能用于组成员搜索。

9 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。使用此页配置授予用户权限所使用的权限组。启用通用 LDAP 后，角色组用于指定 iDRAC6 用户的授权策略。

注：在此版本中，与 AD 不同的是，无需使用特殊字符（"@"、"\" 和 "/"）来区分 LDAP 用户和本地用户。只应输入用户名登录，不应包括域名。

10 在 **"Role Groups"**（角色组）下，单击 **"Role Groups"**（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。使用此页配置控制用户的授权策略所使用的每个角色组。

11 在 **"Group DN"**（组 DN）字段中，输入在与 iDRAC6 相关的通用 LDAP 目录服务中标识角色组的组可分辨名称。

12 在 **"Role Group Privileges"**（角色组权限）部分，通过选择 **"Role Group Privilege Level"**（角色组权限级别）指定与组相关的权限。例如，如果选择 **"Administrator"**（管理员），则为该权限级别选择所有权限。

13 单击 **"Apply"**（应用）以保存角色组设置。

iDRAC6 Web Server 会自动返回到 **"Generic LDAP Configuration and Management Step 3a of 3"**（通用 LDAP 配置和管理第 3a 步，共 3 步）页，其中显示角色组设置。

14 如需要，配置其它角色组。

15 单击 **"Finish"**（完成）返回 **"Generic LDAP Configuration and Management"**（通用 LDAP 配置和管理）摘要页。

16 单击 **"Test Settings"**（检测设置）检查 LDAP 设置。

17 输入选择检测 LDAP 设置的目录用户的用户名和密码。此格式取决于 *"Attribute of User Login"*（用户登录属性）所使用的格式，且输入的用户名必须与选定的属性值相匹配。

将显示检测结果和检测日志。现在已完成通用 LDAP 目录服务配置。

使用 RACADM 配置通用 LDAP 目录服务

```
racadm config -g cfgldap -o cfgLdapEnable 1
racadm config -g cfgldap -o cfgLdapServer <FQDN 或 IP 地址>
racadm config -g cfgldap -o cfgLdapPort <端口号>
racadm config -g cfgldap -o cfgLdapBaseDN dc=common,dc=com
racadm config -g cfgldap -o cfgLdapCertValidationenable 0
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupDN 'cn=everyone, ou=groups, dc=common,
dc=com'
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupPrivilege 0x0001
```

使用以下命令查看设置

```
racadm getconfig -g cfgldap
racadm getconfig -g cfgldaprolegroup -i 1
```

使用 RACADM 确认是否能登录

```
racadm -r <iDRAC6 - IP> -u user.1 -p password getractime
```

检测 BindDN 选项的其它设置

```
racadm config -g cfgldap -o cfgLdapBindDN "cn=idrac_admin,
ou=iDRAC_admins,ou=People,dc=common,dc=com"
```

```
racadm config -g cfgldap -o cfgLdapBindPassword password
```

注：将 iDRAC6 配置为使用域名服务器，用于解析 iDRAC6 配置为在 LDAP 服务器地址中使用的 LDAP 服务器主机名。主机名必须匹配 LDAP 服务器证书中的 “CN”或 “Subject”（主题）。

关于 Active Directory 的常见问题

我的 Active Directory 登录失败。我该如何排除此问题?

iDRAC6 在基于 Web 的界面中提供了一个诊断工具。从基于 Web 的界面以拥有管理员权限的本地用户身份登录。单击 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）**选项卡** → **“Directory Service”**（目录服务）→ **Microsoft Active Directory**。滚动到 **“Active Directory Configuration and Management”**（Active Directory 配置和管理）页底部，然后单击 **“Test Settings”**（检测设置）。输入检测用户名和密码，然后单击 **“Start Test”**（开始检测）。 iDRAC6 会逐步运行检测并显示每个步骤的结果。还会记录详细的检测结果，以帮助您解决问题。返回 **“Active Directory Configuration and Management”**（Active Directory 配置和管理）页：滚动到页面底部，然后单击 **“Configure Active Directory”**（配置 Active Directory）以更改配置并再次运行检测，直到检测用户通过授权步骤为止。

我启用了证书验证，但我的 Active Directory 登录失败了。我从 GUI 运行诊断，检测结果显示以下错误信息：

ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. **（错误：不能联系 LDAP 服务器，错误：14090086：SSL 例程：SSL3_GET_SERVER_CERTIFICATE：证书验证失败：请检查正确的认证机构 (CA) 证书是否已上载到 iDRAC。）另请检查 iDRAC 日期是否在证书有效期内，且 iDRAC 中配置的域控制器地址是否与目录服务器证书的主题相符。**

可能出现了什么问题，我应该如何解决？

如果启用证书验证，则 iDRAC6 在与目录服务器建立 SSL 连接时会使用上载的 CA 证书验证目录服务器证书。证书验证失败的最常见原因是：

1. iDRAC6 日期不在服务器证书或 CA 证书的有效期内。请检查 iDRAC6 时间和证书的有效期。
2. 在 iDRAC6 中配置的域控制器地址与目录服务器证书的主题或主题备用名称不相符。如果使用的是 IP 地址，请阅读以下问题和解答。如果使用的是 FQDN，请确保使用的是域控制器的 FQDN，而不是域的 FQDN，例如，是 `servername.example.com`，而不是 `example.com`。

我使用 IP 地址作为域控制器地址，未能通过证书验证。问题在哪里？

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， Active Directory 在域控制器证书的 “Subject”（主题）或 “Subject Alternative Name”（主题备用名称）字段中使用域控制器的主机名，而不是 IP 地址。可以使用多种方法解决此问题：

1. 在 iDRAC6 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相符。
2. 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 iDRAC6 中配置的 IP 地址匹配。
3. 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。

我在多域环境中使用扩展架构。我该如何配置域控制器地址？

这应该是 iDRAC6 对象所在域中域控制器的主机名 (FQDN) 或 IP 地址。

何时需要配置全局编录地址？

如果使用的是扩展架构，则不使用全局编录地址。

如果使用的是标准架构且用户和角色组来自不同的域，则必须配置全局编录地址。在此情况下，仅可使用通用组。

如果使用的是标准架构且所有用户和所有角色组都在相同域中，则不必配置全局编录地址。

标准架构的查询方式是什么？

iDRAC6 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，将保存权限。

如果配置了全局控制器地址，则 iDRAC6 会继续查询全局编录。如果从全局编录中检索到其它权限，则会累积这些权限。

iDRAC6 总在 SSL 上使用 LDAP 吗?

是。所有传输都通过安全端口 636 和 / 或 3269。

在*检测设置*过程中， iDRAC6 仅执行 LDAP CONNECT 操作以便隔离问题，而不会对不安全的连接执行 LDAP BIND 操作。

为什么 iDRAC6 默认启用证书验证?

iDRAC6 执行严格的安全策略以确保其所连接域控制器的身份。如果不验证证书，黑客可欺骗域控制器和劫持 SSL 连接。如果您选择信任您安全边界内的所有域控制器而无需验证证书，您可通过 GUI 或 CLI 将其禁用。

iDRAC6 支持 NetBIOS 名称吗?

此版本不支持。

如果不能使用 Active Directory 登录到 iDRAC6，应检查什么?

可以在 iDRAC6 基于 Web 的界面中的 **"Active Directory Configuration and Management"**（Active Directory 配置和管理）页底部单击 **"Test Settings"**（检测设置），从而诊断问题。然后根据测试结果修复具体问题。有关其它信息，请参阅第 160 页上的 "检测配置"。

本节说明了最常见的问题，但一般而言，您应检查以下各项：

1. 确保在登录期间使用正确的用户域名，而不是 NetBIOS 名称。
2. 如果具有本地 iDRAC6 用户帐户，请使用本地凭据登录 iDRAC6。

   登录后：

   a. 确保已选中 iDRAC6 的 **"Active Directory Configuration and Management"**（Active Directory 配置和管理）页上的 **"Enable Active Directory"**（启用 Active Directory）选项。

   b. 确保 iDRAC6 网络配置页上的 DNS 设置正确。

   c. 如果启用了证书验证，请确保已将正确的 Active Directory 根 CA 证书上载到 iDRAC6。确保 iDRAC6 时间在 CA 证书的有效期内。

   d. 如果使用扩展架构，则确保 **iDRAC6 名称**和 **iDRAC6 域名**与 Active Directory 环境配置相符。

      如果使用标准架构，确保**组名称**和**组域名**与 Active Directory 配置相符。

3. 检查域控制器 SSL 证书以确保 iDRAC6 时间在证书的有效期内。

8

配置 iDRAC6 进行单一登录或智能卡登录

本节介绍如何配置 iDRAC6 使本地用户和 Active Directory 用户进行智能卡登录和使 Active Directory 用户进行单一登录 (SSO)。

iDRAC6 支持基于 Kerberos 的 Active Directory 验证以支持 Active Directory 智能卡和 SSO 登录。

关于 Kerberos 验证

Kerberos 是一种网络验证协议，使系统能够通过非安全网络安全地通信。通过让系统验证真实性来实现这一目的。为了达到更高的验证执行标准，iDRAC6 现在支持基于 Kerberos 的 Active Directory 验证来支持 Active Directory 智能卡和 SSO 登录。

Microsoft Windows 2000、 Windows XP、 Windows Server 2003、 Windows Vista 和 Windows Server 2008 将 Kerberos 用作默认验证方法。

iDRAC6 使用 Kerberos 支持两种验证机制 — Active Directory SSO 登录和 Active Directory 智能卡登录。对于 Active Directory SSO 登录，在用户使用有效 Active Directory 帐户登录后，iDRAC6 使用在操作系统中缓存的用户凭据。

对于 Active Directory 智能卡登录， iDRAC6 使用基于智能卡的双重验证 (TFA) 作为凭据来启用 Active Directory 登录。这是本地智能卡验证随附的功能。

如果 iDRAC6 时间与域控制器时间不同，iDRAC6 上的 Kerberos 验证将会失败。最多允许 5 分钟偏差。要进行成功验证，请同步服务器时间与域控制器时间，然后**重设** iDRAC6。

Active Directory SSO 和智能卡验证的前提条件

Active Directory SSO 和智能卡验证的前提条件是：

- 配置 iDRAC6 进行 Active Directory 登录。有关详情，请参阅第 129 页上的 “使用 iDRAC6 Directory Service”。
- 注册 iDRAC6 作为 Active Directory 根域中的计算机。要执行此操作：
  a 单击 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）选项卡 → **“Network”**（网络）子选项卡。
  b 提供有效的**首选 / 备用 DNS 服务器** IP 地址。该值是根域中 DNS 的 IP 地址，验证用户的 Active Directory 帐户。
  c 选择 **“Register iDRAC on DNS”**（向 DNS 注册 iDRAC）。
  d 提供有效 **“DNS Domain Name”**（DNS 域名）。
  请参阅 *iDRAC6 联机帮助*了解有关详情。
- 为支持两种新的验证机制， iDRAC6 支持配置以使自身作为 Windows Kerberos 网络上的加密服务。iDRAC6 上的 Kerberos 配置步骤与配置非 Windows Server Kerberos 服务作为 Windows Server Active Directory 安全原则的步骤一样。

  使用 Microsoft 工具 **ktpass** （由 Microsoft 服务器安装 CD/DVD 提供）创建用户帐户服务主体名称 (SPN) 绑定并将可信信息导出到 MIT 样式的 Kerberos *keytab* 文件，这将确定外部用户或系统与 Key Distribution Centre (KDC) 之间的可信关系。该 keytab 文件包含密钥，用于对服务器和 KDC 之间的信息进行加密。 ktpass 工具使那些支持 Kerberos 验证的基于 UNIX 的服务能够使用 Windows Server Kerberos KDC 服务提供的交互功能。

  从 ktpass 公用程序获得的 keytab 作为文件上载提供给 iDRAC6 并作为网络上的加密服务。

  由于 iDRAC6 是一种非 Windows 操作系统设备，在想将 iDRAC6 映射到 Active Directory 用户帐户的域控制器 （Active Directory 服务器）上，运行 **ktpass** 公用程序 （Microsoft Windows 的一部分）。

  例如，使用以下 **ktpass** 命令创建 Kerberos keytab 文件：

```
C:\>ktpass -princ
HOST/dracname.domainname.com@DOMAINNAME.COM -
mapuser dracname -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

iDRAC6 用于 Kerberos 验证的加密类型是 DES-CBC-MD5。主体类型是 KRB5_NT_PRINCIPAL。服务主体名称映射到的用户帐户的属性应启用 **"Use DES encryption types for this account"**（为此帐户使用 DES 加密类型）属性。

注：建议使用最新的 ktpass 公用程序创建 Keytab 文件。

此步骤会生成一个 Keytab 文件，应将该文件上载到 iDRAC6。

注：keytab 包含加密密钥，因此应保管好。

有关 **ktpass** 公用程序的详情，请参阅 Microsoft 网站：**http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

- iDRAC6 时间应与 Active Directory 域控制器同步。还可以使用以下 RACADM 时差命令同步时间：

  ```
  racadm config -g cfgRacTuning -o

  cfgRacTuneTimeZoneOffset <offset value>
  ```

- 要为扩展架构启用单一登录，确保在 Keytab 用户的 **"Delegation"**（委派）选项卡中选择 **"Trust this user for delegation to any service (Kerberos only)"**（信任此用户委派到任何服务 [仅限于 Kerberos]）选项。仅在使用 **ktpass** 公用程序创建 Keytab 文件之后，此选项卡才可用。

浏览器设置以启用 Active Directory SSO

要配置 Internet Explorer 的浏览器设置：

1. 打开 Internet Explorer Web 浏览器
2. 选择 **"Tools"**（工具）→ **"Internet Options"**（Internet 选项）→ **"Security"**（安全）→ **"Local Intranet"**（本地 Intranet）。
3. 单击**站点**。
4. 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）。
5. 单击 **Advanced**（高级）。

6 添加所有相对域名，这些域名将用于属于 SSO 配置一部分的 Weblogic Server 实例 （例如 myhost.example.com）

7 单击 **Close** （关闭）并单击 **OK** （确定）。

8 单击 **OK** （确定）。

要配置 Firefox 的浏览器设置：

1 打开 Firefox Web 浏览器。

2 在地址栏中，输入 `about:config`。

3 在 **"Filter"**（过滤器）中，输入 `network.negotiate`。

4 将 iDRAC 名称添加到 network.negotiate-auth.trusted-uris （使用逗号分隔列表）。

5 将 iDRAC 名称添加到 network.negotiate-auth.delegation-uris （使用逗号分隔列表）。

使用 Microsoft Active Directory SSO

SSO 功能允许在登录到工作站后不输入域用户验证凭据 （比如用户名和密码），即可直接登录 iDRAC6。要使用此功能登录 iDRAC6，应已使用有效 Active Directory 用户帐户登录到系统。另外，应已配置用户帐户使用 Active Directory 凭据登录 iDRAC6。 iDRAC6 使用缓存的 Active Directory 凭据登录。

可以使 iDRAC6 能够使用 Kerberos （一种网络验证协议）来启用 SSO。有关详情，请参阅第 169 页上的 "关于 Kerberos 验证"。配置 iDRAC6 进行 SSO 登录之前，确保已执行第 170 页上的 "Active Directory SSO 和智能卡验证的前提条件"一节中列出的步骤。

配置 iDRAC6 使用 SSO

执行以下步骤，使用 iDRAC Web 界面配置 iDRAC6 进行 SSO：

1 登录 iDRAC Web 界面。

2 转至 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）选项卡 → **"Directory Service"**（目录服务）选项卡 → **Microsoft Active Directory**。

3 单击 **"Configure Active Directory"**（配置 Active Directory）。将会显示 **"Active Directory Configuration and Management Step 1 of 4"**（Active Directory 配置和管理第 1 步，共 4 步）页。

4 将从 Active Directory 根域获得的 Keytab 上载到 iDRAC6。为此，在 **"Upload Kerberos Keytab"**（上载 Kerberos Keytab）下，键入 Keytab 文件的路径或单击 **"Browse"**（浏览）查找该文件。单击 **"Upload"**（上载）。Kerberos Keytab 将会上载到 iDRAC6。Keytab 就是在执行第 170 页上的 "Active Directory SSO 和智能卡验证的前提条件" 中列出的任务时创建的文件。

5 单击 **"Next"**（下一步）。将会显示 **"Active Directory Configuration and Management Step 2 of 4"**（Active Directory 配置和管理第 2 步，共 4 步）页。

6 选择 **"Enable Single Sign-On"**（启用单一登录）启用 SSO 登录。

7 单击 **"Next"**（下一步），直到显示最后一页为止。如果 Active Directory 配置为使用标准架构，则显示 **"Active Directory Configuration and Management Step 4a of 4"**（Active Directory 配置和管理第 4a 步，共 4 步）页。如果 Active Directory 配置为使用扩展架构，则显示 **"Active Directory Configuration and Management Step 4 of 4"**（Active Directory 配置和管理第 4 步，共 4 步）页。

8 单击 **"Finish"**（完成）以应用设置。

使用 RACADM：

可以使用以下 CLI racadm 命令将 Keytab 文件上载到 iDRAC6：

```
racadm krbkeytabupload -f < 文件名 >
```

其中 < 文件名 > 是 keytab 文件的名称。本地和远程 racadm 都支持 racadm 命令。

要使用 CLI 启用单一登录，请运行 racadm 命令：

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

使用 SSO 登录到 iDRAC6

1 使用有效 Active Directory 帐户登录到系统。

2 要访问 iDRAC6 网页，请键入：

```
https://<FQDN 地址 >
```

如果默认 HTTPS 端口号 （端口 443）已更改，请键入：

```
https://<FQDN 地址 >:< 端口号 >
```

其中 *FQDN 地址*是 iDRAC FQDN (idracdnsname.domain name)，*端口号*是 HTTPS 端口号。

注：如果使用 IP 地址而不是 FQDN， SSO 将失败。

iDRAC6 会使用在用户使用有效 Active Directory 帐户登录时缓存在操作系统中的凭据来使用户登录。

在以下情况下，可以使用相应的 Microsoft Active Directory 权限登录到 iDRAC6：

- 您是 Microsoft Active Directory 用户。
- 您在 iDRAC6 中配置进行 Active Directory 登录。
- 启用 iDRAC6 进行 Kerberos Active Directory 验证。

配置智能卡验证

iDRAC6 启用**智能卡登录**支持双重验证 (TFA) 功能。

传统的验证架构使用用户名和密码来验证用户。这提供了最低的安全性。

TFA 让用户提供双重验证，提供了更高的安全性，双重验证是您拥有和您知道的东西，您拥有的是物理设备智能卡，您知道的是密码或 PIN 等机密代码。

双重验证要求用户通过提供*两方面*的凭据来验证身份。

配置本地 iDRAC6 用户进行智能卡登录

您可配置本地 iDRAC6 用户，使用智能卡登录到 iDRAC6。单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）→ **"Users"**（用户）。

但是，在用户可以使用智能卡登录到 iDRAC6 之前，必须将用户的智能卡证书和可信认证机构 (CA) 证书上载到 iDRAC6。

注：在配置智能卡之前，确保 CA 证书验证已启用。

导出智能卡证书

可以通过使用卡管理软件 (CMS) 将智能卡证书从智能卡导出为 Base64 编码格式的文件来获得用户证书。通常可以从智能卡供应商处获得 CMS。该编码文件应作为用户证书上载到 iDRAC6。颁发智能卡用户证书的可信认证机构也应将 CA 证书导出为 Base64 编码格式的文件。应将此文件作为用户的可信 CA 证书进行上载。用智能卡证书中组成用户基本名 (UPN) 的用户名来配置用户。

注：要登录 iDRAC6，在 iDRAC6 中配置的用户名应与智能卡证书中的用户基本名 (UPN) 大小写一致。

例如，如果已给用户 “sampleuser@domain.com”颁发智能卡证书，用户名应配置为 “sampleuser”。

配置 Active Directory 用户进行智能卡登录

使用 Active Directory 智能卡登录功能之前，确保已配置 iDRAC6 进行 Active Directory 登录并且已颁发智能卡的用户帐户已启用 iDRAC6 Active Directory 登录。

另外确保已启用 Active Directory 登录设置。请参阅第 129 页上的 “使用 iDRAC6 Directory Service”了解如何设置 Active Directory 用户的详情。还必须通过将从 Active Directory 根域获得的有效 *Keytab* 文件上载到 iDRAC6 来启用 iDRAC6 作为加密服务。

要配置 Active Directory 用户使用智能卡登录 iDRAC6，iDRAC6 管理员应配置 DNS 服务器，上载 Active Directory CA 证书到 iDRAC6，并启用 Active Directory 登录。请参阅第 129 页上的 “使用 iDRAC6 Directory Service”了解如何设置 Active Directory 用户的详情。

可以从 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）→ **“Directory Service”**（目录服务）→ **Microsoft Active Directory** 配置 Active Directory。

注：在配置智能卡之前，确保 CA 证书验证已启用。

使用 iDRAC6 配置智能卡

注：要修改这些设置，必须具有 “Configure iDRAC”（配置 iDRAC）权限。

1. 在 iDRAC6 Web 界面中，转至 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）→ **“Smart Card”**（智能卡）选项卡。
2. 配置智能卡登录设置。

   表 8-1 提供了有关 **“Smart Card”**（智能卡）页设置的信息。
3. 单击 **“Apply”**（应用）。

表 8-1. 智能卡设置

设置	说明
“Configure Smart Card Logon”（配置智能卡登录）	• **“Disabled”（已禁用）**— 禁用智能卡登录。随后从图形用户界面 (GUI) 进行的登录会显示常规登录页。所有命令行带外接口，包括 Secure Shell (SSH)、Telnet、Serial 和远程 RACADM 都会保持其状态。 • **“Enabled”（已启用）**— 启用智能卡登录。应用更改后，注销，插入智能卡，然后单击 **“Login”**（登录）并输入智能卡 PIN。启用智能卡登录会禁用所有 CLI 带外接口，包括 SSH、Telnet、Serial、远程 RACADM 和 LAN 上 IPMI，这是因为这些服务只支持单重验证。 • **“Enabled with Remote Racadm”（随远程 Racadm 启用）**— 随远程 RACADM 启用智能卡登录。其它所有 CLI 带外接口都会禁用。 如果选择 **“Enabled”**（已启用）或 **“Enabled with Remote Racadm”**（随远程 Racadm 启用），会在随后使用基于 Web 的界面尝试登录时提示进行智能卡登录。 建议 iDRAC6 管理员将 **“Enable with Remote Racadm”**（随远程 Racadm 启用）设置只用来访问 iDRAC6 基于 Web 的界面以便使用远程 RACADM 命令运行脚本。如果管理员不需要使用远程 RACADM，建议使用智能卡登录的 **“Enabled”**（已启用）设置。启用智能卡登录前，确保完成了 iDRAC6 本地用户配置和 / 或 Active Directory 配置。 **注：**智能卡登录要求用适当的证书配置本地 iDRAC6 用户。如果使用智能卡登录来登录 Microsoft Active Directory 用户，则必须确保为该用户配置 Active Directory 用户证书。可以在 “Users”（用户）→ “User Main Menu”（用户主菜单）页配置用户证书。

表 8-1. 智能卡设置 *（续）*

设置	说明
“Enable CRL check for Smart Card Logon”（启用 CRL 检查进行智能卡登录）	此检查仅供智能卡本地用户使用。如果希望 iDRAC6 检查证书撤回列表 (CRL) 撤回用户智能卡证书，则选择此选项。会对从证书撤回列表 (CRL) 分发服务器下载的用户 iDRAC 证书进行检查以在 CRL 中撤回。 CRL 分发服务器列在用户的智能卡证书中。 为了使 CRL 功能起作用，iDRAC6 的网络配置中必须配置了有效的 DNS IP 地址。可以在 iDRAC6 中的 **“iDRAC Settings”**（iDRAC 设置）→ **“Network/Security”**（网络 / 安全性）→ **“Network”**（网络）下配置 DNS IP 地址。 在以下情况下，用户将无法登录： • 用户证书在 CRL 文件中列为已撤回。 • iDRAC6 无法与 CRL 分发服务器通信。 • iDRAC6 无法下载 CRL。 **注：必须在 “Network/Security”（网络 / 安全性）→ “Network”（网络）页中正确配置 DNS 服务器的 IP 地址，此检查才能成功。**

使用智能卡登录 iDRAC6

iDRAC6 Web 界面会向所有配置为使用智能卡的用户显示智能卡登录页。

注：为用户启用智能卡登录之前，确保完成了 iDRAC6 本地用户配置和 / 或 Active Directory 配置。

注：根据浏览器设置的不同，第一次使用此功能时，可能会提示下载并安装智能卡阅读器 ActiveX 插件。

1 使用 https 访问 iDRAC6 Web 页面。

`https://<IP 地址>`

如果默认 HTTPS 端口号 （端口 443）已更改，请键入：

`https://<IP 地址>:<端口号>`

其中 *IP 地址*是 iDRAC6 的 IP 地址，而*端口号*是 HTTPS 端口号。

iDRAC6 “Login”（登录）页会显示出来，提示插入智能卡。

2 将智能卡插入阅读器并单击 **“Login”**（登录）。

iDRAC6 会提示输入智能卡的 PIN。

3 输入本地智能卡用户的智能卡 PIN，如果未在本地创建用户，则 iDRAC6 将提示输入用户 Active Directory 帐户的密码。

注：如果是已选中 “Enable CRL check for Smart Card Logon”（启用 CRL 检查进行智能卡登录）的 Active Directory 用户，iDRAC6 会尝试下载 CRL 并在 CRL 中检查用户证书。如果证书在 CRL 中列为已撤回或由于某些原因不能下载 CRL，则通过 Active Directory 登录会失败。

您已登录 iDRAC6。

使用 Active Directory 智能卡验证登录 iDRAC6

1 使用 https 登录 iDRAC6。

`https://<IP 地址>`

如果默认 HTTPS 端口号 （端口 443）已更改，请键入：

`https://<IP 地址>:<端口号>`，其中 `IP 地址`是 `iDRAC6 IP` 地址，而*端口号*是 `HTTPS` 端口号。

iDRAC6 “Login”（登录）页会显示出来，提示插入智能卡。

2 插入智能卡并单击 **“Login”**（登录）。

将显示 PIN 弹出对话框。

3 输入 PIN，并单击 **OK** （确定）。

将会使用在 Active Directory 中设置的凭据登录 iDRAC6。

对 iDRAC6 中的智能卡登录进行故障排除

参考以下提示调试无法访问的智能卡：

ActiveX 插件无法检测到智能卡阅读器

确保 Microsoft Windows 操作系统支持 Smart Card。Windows 支持有限的几种智能卡加密服务提供程序 (CSP)。

提示：作为常规检查，了解智能卡 CSP 是否位于特定客户端上，在出现 Windows 登录 (Ctrl-Alt-Del) 屏幕时将智能卡插入阅读器并查看 Windows 是否检测到智能卡并显示 PIN 对话框。

不正确的智能卡 PIN

检查智能卡是否因为用不正确的 PIN 尝试太多次而已锁定。在这种情况下，组织中的智能卡颁发者应能够帮助获得新的智能卡。

无法登录本地 iDRAC6

如果本地 iDRAC6 用户无法登录，检查上载到 iDRAC6 的用户名和用户证书是否已经过期。iDRAC6 跟踪日志可能会提供有关错误的重要日志信息；尽管有时由于安全考虑，错误信息可能会有意模棱两可。

无法以 Active Directory 用户的身份登录 iDRAC6

- 如果无法以 Active Directory 用户的身份登录 iDRAC6，则尝试不启用智能卡登录来登录 iDRAC6。如果已启用 CRL 检查，则尝试不启用 CRL 检查来进行 Active Directory 登录。CRL 失败时，iDRAC6 跟踪日志应能够提供重要信息。
- 还可以选择使用以下命令通过本地 racadm 禁用智能卡登录：`racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0`
- 对于 64 位 Windows 平台，如果部署了 64 位版本的 Microsoft Visual C++ 2005 Redistributable Package，iDRAC6 验证 Active - X 插件不会安装。要正确安装并运行 Active - X 插件，请部署 32 位版本的 Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)。需要该软件包以在 Internet Explorer 浏览器上启动虚拟控制台会话。
- 如果收到以下错误信息“`Not able to load the Smart Card Plug-in.Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in`”（无法载入智能卡插件。请检查 IE 设置或是否没有足够权限使用智能卡插件），然后再安装 Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)。该文件位于 Microsoft 网站 **microsoft.com**。两种分发版本的 C++ Redistributable Package 已经过测试，允许 Dell 智能卡插件载入。有关详情，请参阅表 8-2。

表 8-2. 分发版本的 C++ Redistributable Package

Redistributable Package 文件名	Version（版本）	发布日期	大小	说明
vcredist_x86.exe	6.0.2900.2180	2006 年 3 月 21 日	2.56 MB	MS Redistributable 2005
vcredist_x86.exe	9.0.21022.8	2007 年 11 月 7 日	1.73 MB	MS Redistributable 2008

- 请确保 iDRAC6 时间和域控制器服务器上的域控制器时间相差在 5 分钟之内，以确保 Kerberos 验证能够正常进行。请查看 **"System"**（系统）→ **"iDRAC Settings"**（iDRAC 设置）→ **"Properties"**（属性）→ **"iDRAC Information"**（iDRAC 信息）页上的 **"RAC Time"**（RAC 时间），以及通过右键单击屏幕右下角的时间查看域控制器时间。时差在弹出框中显示。对于美国中部标准时间 (CST)，该值为 - 6。使用以下 RACADM 时差命令同步 iDRAC6 时间 （通过 Remote 或 Telnet/SSH RACADM）：`racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <以分钟计的时差值>`。例如，如果系统时间为 GMT -6 (US CST) 并且时间为下午 2 点，将 iDRAC6 时间设置为 GMT 时间 18:00，需要在以上命令中为时差输入 360。还可以使用 *cfgRacTuneDaylightoffset* 设置夏令时变体。这样就不必在每年两次调整夏令时的时候更改时间，或者还可以在以上示例的时差中使用 300。

SSO 常见问题

在 Windows Server 2008 R2 x64 上 SSO 登录失败。应怎样做才能使 SSO 在 Windows Server 2008 R2 x64 上成功。

1. 为域控制器和域策略执行 **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** 中介绍的操作。将计算机配置为使用 DES-CBC-MD5 加密方案。这些设置可能会影响与环境中的客户端计算机或服务和应用程序的兼容性。**"Configure encryption types allowed for Kerberos"**（配置 Kerberos 允许的加密类型）策略设置位于 **Computer Configuration\Security Settings\Local Policies\Security Options**。
2. 域客户端必须具有更新的 GPO。在命令行处，键入 `gpupdate /force` 并用 `klist purge` 命令删除旧 Keytab。
3. 更新 GPO 后，创建新 Keytab。
4. 上载 Keytab 到 iDRAC6。

现在可以使用 SSO 登录 iDRAC。

Windows 7 和 Windows Server 2008 R2 上的 AD 用户 SSO 登录失败。应该执行什么操作解决此问题?

必须为 Windows 7 和 Windows Server 2008 R2 启用加密类型。要启用加密类型：

1. 以管理员或具有管理权限的用户的身份登录。
2. 转至 **"Start"**（开始）并运行 **gpedit.msc**。将显示 **"Local Group Policy Editor"**（本地组策略编辑器）窗口。

3 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）。

4 右键单击 **"Network Security: Configure encryption types allowed for kerberos"**（网络安全：配置 Kerberos 允许的加密类型）并选择 **"Properties"**（属性）。

5 启用所有选项。

6 单击 **OK**（确定）。现在可以使用 SSO 登录 iDRAC。

对于扩展架构，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：发往远程服务器的外出 NTLM 通信量）并选择 **"Properties"**（属性）。

3 选择 **"Allow all"**（全部允许）。

4 单击 **"OK"**（确定），然后关闭 **"Local Group Policy Editor"**（本地组策略编辑器）窗口。

5 转至 **"Start"**（开始）并运行 cmd。此时将显示**命令提示符**窗口。

6 运行命令 `gpupdate /force`。将更新组策略。关闭**命令提示符**窗口。

7 转至 **"Start"**（开始）并运行 regedit。此时将显示 **"Registry Editor"**（注册表编辑器）窗口。

8 导航至 HKEY_LOCAL_MACHINE → **"System"**（系统）→ CurrentControlSet → **"Control"**（控件）→ LSA。

9 在右窗格中，右键单击并选择 **"New"**（新建）→ **"DWORD (32-bit) Value"**（DWORD [32 位] 值）。

10 将新项命名为 SuppressExtendedProtection。

11 右键单击 SuppressExtendedProtection 并单击 **"Modify"**（修改）。

12 在 **"Value data"**（值数据）字段中键入 1 并单击 **"OK"**（确定）。

13 关闭 **"Registry Editor"**（注册表编辑器）窗口。现在可以使用 SSO 登录 iDRAC。

如果为 iDRAC 启用了 SSO 并且使用 Internet Explorer 登录 iDRAC，SSO 将失败并提示输入用户名和密码。如何解决此问题?

确保 **"Tools"**（工具）→ **"Internet Options"**（Internet 选项）→ **"Security"**（安全）→ **"Trusted sites"**（可信站点）中列出了 iDRAC IP 地址。如果未列出， SSO 将失败并提示输入用户名和密码。单击 **"Cancel"**（取消）并继续。

9

使用 GUI 虚拟控制台

本节提供关于使用 iDRAC6 虚拟控制台功能的信息。

概览

iDRAC6 虚拟控制台功能使您能够以图形或文本模式远程访问本地控制台。您可以利用虚拟控制台在一个位置控制一个或多个已启用 iDRAC6 的系统。

不用再坐在每台服务器前执行各种日常维护。而是可以在任何地方从台式机或膝上型计算机管理服务器。还可以与他人共享信息 — 无论多么遥远，都可以迅速共享。

使用虚拟控制台

注：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。

注：如果虚拟控制台会话已从 Management Station 打开用于特定 iDRAC6，则从相同 Management Station 打开新会话用于该 iDRAC6 的任何尝试都将失败。

注：可同时打开多个从单个 Management Station 至多个 iDRAC6 控制器的虚拟控制台会话。

"Virtual Console"（虚拟控制台）页使您能够通过使用本地 Management Station 上的键盘、视频和鼠标管理远程系统，从而控制远程受管服务器上相应的设备。此功能可以与虚拟介质功能配合使用以执行远程软件安装。

以下规则适用于虚拟控制台会话：

- 最多可同时支持四个虚拟控制台会话。所有会话同时查看同一个受管服务器控制台。
- 从 1.5 版开始，可以按照打开会话的顺序从同一客户端向多个远程服务器发出多个会话。如果打开了使用 Java 插件的虚拟控制台会话，可以打开另一个使用 ActiveX 插件的虚拟控制台会话。但是，如果打开了基于 ActiveX 的虚拟控制台会话，则无法打开另一个使用 Java 插件的虚拟控制台会话。必须先关闭第一个虚拟控制台会话，才能打开第二个虚拟控制台会话。
- 不应从 Managed System 上的 Web 浏览器启动虚拟控制台会话。
- 最低要求 1 MB/sec 可用网络带宽。

- 对 iDRAC6 的第一个虚拟控制台会话为完全访问会话。如果第二位用户请求虚拟控制台会话，第一位用户会收到通知并可以选择 （批准、拒绝或允许作为只读）向第二位用户发送共享请求。第二位用户也将被告知另一用户享有控制权。第一位用户在 30 秒的超时时限内对于随后每位用户的共享请求没有应答时，根据为 `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions` 对象设置的值授予虚拟控制台访问权限。此对象与设置用于第二 / 第三 / 第四个会话中的插件类型 （ActiveX 或 Java）无关。有关此对象的详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》。

  注：此规则仅适用于远程或固件 （SSH 或 Telnet） RACADM，而不适用于本地 RACADM。

配置 Management Station

要在 Management Station 上使用虚拟控制台，请执行以下过程：

1. 安装并配置一个支持的 Web 浏览器。有关详情，请参阅以下章节：
   - 第 24 页上的 “支持的 Web 浏览器”
   - 第 38 页上的 “配置支持的 Web 浏览器”
2. 如果使用 Firefox 或想配合使用 Internet Explorer 和 Java 查看器，则安装 Java Runtime Environment (JRE)。如果使用 Internet Explorer 浏览器，则会为控制台查看器提供 ActiveX 控件。如果安装了 JRE 并且在启动查看器前在 iDRAC6 Web 界面中配置了控制台查看器，则还可以将 Java 控制台查看器用于 Firefox。
3. 如果使用 Internet Explorer (IE)，请按以下方式确保浏览器能够下载加密内容：
   - 转至 Internet Explorer 选项或设置，并选择 **“Tools”**（工具） → **“Internet Options”**（Internet 选项） → **“Advanced”**（高级）。
   - 滚动至 **“Security”**（安全性）并清除此选项：

     `Do not save encrypted pages to disk`（不将加密的页存盘）
4. 如果使用 Internet Explorer 启动带有 Active-X 插件的虚拟控制台会话，确保已将 iDRAC6 IP 地址或主机名添加到 **“Trusted Sites”**（可信站点）列表。还应重设自定义设置为 **“Medium-low”**（中低）或更改设置以允许安装签名的 Active-X 插件。有关详情，请参阅第 186 页上的 “基于 ActiveX 的虚拟控制台和虚拟介质应用程序的 Internet Explorer 浏览器配置”。

注：不支持 64 位 ActiveX 插件使用 Internet Explorer 启动虚拟控制台会话。

5 建议将显示器的显示分辨率配置为 1280x1024 像素或更高。

注：如果系统运行的是 Linux 操作系统，本地显示器上可能无法查看 X11 控制台。在 iDRAC6 虚拟控制台按 <Ctrl><Alt><F1>，将 Linux 切换到文本控制台。

注：有时可能遇到以下 Java 脚本编译错误："Expected: ;"（预期的：；）。要解决此问题，请调整网络设置，使用 JavaWebStart 中的 "Direct connection"（直接连接）："Edit"（编辑）→ "Preferences"（首选项）→ "General"（常规）→ "Network Settings"（网络设置），并选择 "Direct connection"（直接连接），而非 "Use browser settings"（使用浏览器设置）。

清除浏览器的高速缓存

如果运行虚拟控制台时出现问题（超出范围错误，同步问题等等），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：必须拥有管理员权限才能清除浏览器的高速缓存。

要清除 IE7 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，转到 **Internet Explorer→ "Tools"**（工具）→ **"Manage Add-ons"**（管理插件）并单击 **"Enable or Disable Add-ons"**（启用或禁用插件）。显示 **"Manage Add-ons"**（管理插件）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。

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，转到 **Internet Explorer→ "Tools"**（工具）→ **"Manage Add-ons"**（管理插件）并单击 **"Enable or Disable Add-ons"**（启用或禁用插件）。显示 **"Manage Add-ons"**（管理插件）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。

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`

2 此时会显示 **"Java Cache viewer"**（Java 高速缓存查看器）。

3 删除标为 *"iDRAC6 Virtual Console Client"*（iDRAC6 虚拟控制台客户端）的项。

基于 ActiveX 的虚拟控制台和虚拟介质应用程序的 Internet Explorer 浏览器配置

本节介绍启动和运行基于 ActiveX 的虚拟控制台和虚拟介质应用程序所需的 Internet Explorer 浏览器设置。

注：清除浏览器的高速缓存，然后执行浏览器配置设置。有关详情，请参阅第 185 页上的 "清除浏览器的高速缓存"。

Microsoft Windows 操作系统的常见设置

1 在 Internet Explorer 中，转至 **"Tools"**（工具）→ **"Internet Options"**（Internet 选项）→ **"Security"**（安全）选项卡。

2 选择要用于运行应用程序的区域。

3 单击 **"Custom"**（自定义）。如果使用的是 Internet Explorer 8，单击 **"Custom level"**（自定义级别）。将显示 **"Security Settings"**（安全设置）窗口。

4 在 **"ActiveX controls and plug-ins"**（ActiveX 控件和插件）下面：

- 选择 **"Download signed ActiveX controls"**（下载已签名的 ActiveX 控件）的 **"Prompt"**（提示）选项
- 选择 **"Run ActiveX controls and plug-ins"**（运行 ActiveX 控件和插件）的 **"Enable"**（启用）或 **"Prompt"**（提示）选项
- 选择 **"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）的 **"Enable"**（启用）或 **"Prompt"**（提示）选项
- 单击 **"OK"**（确定），然后再次单击 **"OK"**（确定）。

Windows Vista 或更新的 Microsoft 操作系统的其它设置

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

可以采用以下一种方法在具有“保护模式”的 Internet Explorer 浏览器中启动和运行 ActiveX 应用程序：

- 转至 **“Program Files”**（程序文件）→ **Internet Explorer**。右键单击 **iexplore.exe** 并单击 **“Run as administrator”**（以管理员身份运行）。
- 将 iDRAC IP 地址添加到“Trusted Sites”（可信站点）。要执行此操作：

1. 在 Internet Explorer 中，转至 **“Tools”**（工具）→ **“Internet Options”**（Internet 选项）→ **“Security”**（安全）→ **“Trusted Sites”**（可信站点）。
2. 确保没有为“Trusted Sites”（可信站点）区域选中 **“Enable Protected Mode”**（启用保护模式）选项。或者，可以将 iDRAC 地址添加到 Intranet 区域中的站点。默认情况下，为 Intranet 区域和“Trusted Sites”（可信站点）区域中的站点关闭了保护模式。
3. 单击**站点**。
4. 在 **“Add this website to the zone”**（将该网站添加到区域）字段中，添加 iDRAC 的地址，然后单击 **“Add”**（添加）。
5. 单击 **“Close”**（关闭），然后单击 **“OK”**（确定）。
6. 关闭并重新启动浏览器使设置生效。

支持的屏幕分辨率和刷新率

表 9-1 列出了受管服务器上运行的虚拟控制台会话支持的屏幕分辨率和相应的刷新率。

表 9-1. 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

在 iDRAC6 Web 界面中配置虚拟控制台

要在 iDRAC6 Web 界面中配置虚拟控制台，请执行下列步骤：

1. 单击 **"System"**（系统）→ **"Console/Media"**（控制台 / 介质）→ **"Configuration"**（配置）以配置 iDRAC6 虚拟控制台设置。
2. 配置虚拟控制台属性。表 9-2 说明虚拟控制台的设置。
3. 完成时，请单击 **"Apply"**（应用）保存新设置。

表 9-2. 虚拟控制台配置属性

属性	说明
Enabled （启用）	单击可以启用或禁用虚拟控制台。如果选中此选项，则表示启用虚拟控制台。默认值为 **"enabled"**（已启用）。 **注：在启动虚拟控制台后选择或取消选择 "Enabled"（已启用）选项会断开所有现有的虚拟控制台会话连接。**
Max Sessions （最大会话数）	选择允许的虚拟控制台会话的最大数目，为 1 至 4。默认值为 2。
"Active Sessions" （激活的会话数）	显示活动控制台会话数目。此字段为只读。
"Remote Presence Port" （远程存在端口）	用于连接到 "Virtual Console"（虚拟控制台）键盘 / 鼠标选项的网络端口号。此通信量始终加密。如果其它程序正在使用默认端口，可能需要更改此编号。默认值为 5900。 **注：在启动虚拟控制台后修改 "Remote Presence Port"（远程存在端口）值会断开所有现有的虚拟控制台会话连接。**
"Video Encryption Enabled" （视频加密已启用）	**选中**表示视频加密已启用。进入视频端口的所有通信量均被加密。 **取消选中**表示视频加密已禁用。进入该视频端口的通信量均未加密。 默认值为 **"Encrypted"**（加密）。禁用加密可以提高较慢网络上的性能。 **注：在启动虚拟控制台后启用或禁用 "Video Encryption Enabled"（视频加密已启用）选项会断开所有现有的虚拟控制台会话连接。**

表 9-2. 虚拟控制台配置属性 *（续）*

属性	说明
"Local Server Video Enabled"（本地服务器视频已启用）	选中表示在虚拟控制台期间到 iDRAC6 虚拟控制台显示器的输出已禁用。这可确保使用 **"Virtual Console"**（虚拟控制台）所执行的任务不会在受管服务器的本地显示器上被看到。
"Plug-in Type"（插件类型）	要配置插件的类型。 • **"Native"**（本机）（Windows 为 ActiveX，而 Linux 为 Java 插件）— ActiveX Viewer 只能在 Internet Explorer 上运行。 • **Java** — 将启动 Java 查看器。

注：有关借助虚拟控制台使用虚拟介质的信息，请参阅第 231 页上的 "配置并使用虚拟介质"。

打开虚拟控制台会话

打开虚拟控制台会话时，会启动 Dell 虚拟控制台 Viewer 应用程序，并且在 Viewer 中会显示远程系统的桌面。使用虚拟控制台 Viewer 应用程序，可以从本地 Management Station 控制远程系统的鼠标和键盘功能。

注：虚拟控制台从 Windows Vista Management Station 启动会导致虚拟控制台重新启动信息。为避免这种情况，在以下位置设置相应的超时值："Control Panel"（控制面板）→ "Power Options"（电源选项）→ "Power Saver"（节电程序）→ "Advanced Settings"（高级设置）→ "Hard Disk"（硬盘）→ "Turnoff Hard Disk After <time_out>"（< 超时 > 后关闭硬盘），以及在 "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>"（< 超时 > 后关闭硬盘）。

要在 Web 界面中打开虚拟控制台会话，请执行下列步骤：

1. 单击 **"System"**（系统）→ **"Console/Media"**（控制台 / 介质）→ **"Virtual Console and Virtual Media"**（虚拟控制台和虚拟介质）。
2. 使用表 9-3 中的信息确保虚拟控制台会话可用。

   如果想要重新配置显示的任何属性值，请参阅第 188 页上的 "在 iDRAC6 Web 界面中配置虚拟控制台"。

注：有关借助虚拟控制台使用虚拟介质的信息，请参阅第 231 页上的 "配置并使用虚拟介质"。

表 9-3. 虚拟控制台

属性	说明
"Virtual Console Enabled"（虚拟控制台已启用）	"Yes"（是）/ "No"（否）（选中 / 取消选中）
"Video Encryption Enabled"（视频加密已启用）	"Yes"（是）/ "No"（否）（选中 / 取消选中）
Max Sessions **（最大会话数）**	显示支持的最大虚拟控制台会话数。
"Active Sessions"（激活的会话数）	显示当前活动虚拟控制台会话数。
"Local Server Video Enabled"（本地服务器视频已启用）	"Yes"（是）= 已启用；"No"（否）= 已禁用。
"Remote Presence Port"（远程存在端口）	用于连接到 "Virtual Console"（虚拟控制台）键盘 / 鼠标选项的网络端口号。此通信量始终加密。如果其它程序正在使用默认端口，可能需要更改此编号。默认值为 5900。
"Plug-in Type"（插件类型）	显示在 **"Configuration"**（配置）页选择的插件的类型。 **注：**对于 64 位 Windows 平台，如果部署了 64 位版本的 Microsoft Visual C++ 2005 Redistributable Package，iDRAC6 验证 Active – X 插件不会正确安装。要正确安装并运行 Active – X 插件，请部署 32 位版本的 Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)。需要该软件包以在 Internet Explorer 浏览器上启动虚拟控制台会话。

3 如果虚拟控制台会话可用，请单击 **"Virtual Console and Virtual Media"**（虚拟控制台和虚拟介质）页上的 **"Launch Virtual Console"**（启动虚拟控制台）。

注：启动应用程序后会出现多个信息框。为了防止未授权访问应用程序，在三分钟内浏览这些信息框。否则，将会提示重新启动应用程序。

注：如果在随后步骤中出现一个或多个 "Security Alert"（安全警报）窗口，请阅读窗口中的信息并单击 "Yes"（是）继续。

Management Station 连接到 iDRAC6，在 iDRAC6 虚拟控制台 Viewer 应用程序中显示远程系统的桌面。

4 两个鼠标指针出现在查看器窗口中：一个是远程系统的指针，一个是本地系统的指针。可通过选择 iDRAC6 虚拟控制台菜单中 **"Tools"**（工具）下的 **"Single Cursor"**（单光标）选项更改为单光标。

Virtual Console Preview （虚拟控制台预览）

在启动虚拟控制台之前，可以在 **"System"**（系统）→ **"Properties"**（属性）→ **"System Summary"**（系统摘要）页上预览虚拟控制台的状态。**"Virtual Console Preview"**（虚拟控制台预览）部分显示一个图像，表明虚拟控制台的状态。该图像每 30 秒钟自动刷新一次。

注：仅当启用了虚拟控制台并且存在 iDRAC6 Enterprise 卡时，虚拟控制台图像才可用。

表 9-4 提供了关于可用选项的信息。

表 9-4. 虚拟控制台预览选项

选项	说明
启动	单击此链接可启动虚拟控制台。 如果仅启用了虚拟介质，则单击此链接将直接启动虚拟介质。 如果您没有虚拟控制台权限或虚拟控制台和虚拟介质都已禁用，则不显示此链接。
设置	单击此链接可在 **"Console/Media Configuration"**（控制台 / 介质配置）页上查看或编辑虚拟控制台配置设置。 **注：您必须有配置 iDRAC 的权限才能编辑虚拟控制台配置设置。**
Refresh （刷新）	单击此链接可刷新显示的虚拟控制台图像。

使用 iDRAC6 虚拟控制台 (Video Viewer)

iDRAC6 虚拟控制台 (Video Viewer) 在 Management Station 和受管服务器之间提供了一个用户界面，使用户能够从 Management Station 查看受管服务器的桌面并控制其鼠标和键盘功能。连接到远程系统时， iDRAC6 虚拟控制台在单独窗口中启动。

注：您必须有管理员权限才能启动 iDRAC6 虚拟控制台 (Video Viewer)。

注：如果切断远程服务器电源，将显示 “No Signal”（无信号）信息。

注：虚拟控制台标题栏显示从 Management Station 连接的 iDRAC 的 DNS 名称或 IP 地址。如果 iDRAC 没有 DNS 名称，则显示 IP 地址。格式为：
<DNS 名称 / IPv6 地址 / IPv4 地址>, <型号>, User: <用户名>, <fps>

iDRAC6 虚拟控制台提供了各种控制调整，比如鼠标同步、快照、键盘宏指令和虚拟介质访问。有关这些功能的详情，请单击 **“System”**（系统）→ **“Console/Media”**（控制台 / 介质），并单击 **“Virtual Console and** Virtual Media”（虚拟控制台和虚拟介质） GUI 页上的 **“Help”**（帮助）。

当启动虚拟控制台会话并显示 iDRAC6 虚拟控制台时，可能需要同步鼠标指针。

表 9-5 说明了查看器中可以使用的菜单选项。

表 9-5. Viewer 菜单栏选择

菜单项	项	说明
“别针”图标	NA	单击 “别针” 图标可以锁定 iDRAC6 虚拟控制台菜单栏。这可以防止工具栏自动隐藏。 **注：**这只适用于 Active-X 查看器，而不适用于 Java 插件。

表 9-5. Viewer 菜单栏选择 *（续）*

菜单项	项	说明
虚拟介质	**"Launch Virtual Media"**（启动虚拟介质）	将会显示 **"Virtual Media Session"**（虚拟介质会话），其中列出可用于在主窗口中映射的设备。要虚拟化 ISO 或 IMG 映像，请单击 **"Add"**（添加）并选择一个映像文件。将会显示选定的映像文件，同时列出可用于在主窗口中映射的设备。要虚拟化设备或映像，选择表中 **"Mapped"**（已映射）列中的选项。此时设备或映像将会映射到服务器。要取消映射，取消选择该复选框。 单击 **"Details"**（详情）会显示一个列出虚拟设备和映像的面板。还会显示各设备或映像的读 / 写活动。
"File"（文件）	**"Capture to File"**（捕获到文件）	捕获当前远程系统屏幕为 Windows 上的 .bmp 文件或 Linux 上的 .png 文件。将显示一个对话框，使您可以将文件保存到指定位置。 **注：**Windows 上的 .bmp 文件格式或 Linux 上的 .png 文件格式只适用于本机插件。 Java 插件只支持 .jpg 和 .jpeg 文件格式。
	退出	控制台使用结束并已注销后 （使用远程系统的注销过程），从 **"File"**（文件）菜单中选择 **"Exit"**（退出）关闭 **iDRAC6 虚拟控制台**窗口。
查看	Refresh （刷新）	刷新视图虚拟控制台的视图。虚拟控制台请求服务器的参考视频帧。
	"Full Screen/Windowed"（全屏 / 窗口）	以全屏模式查看视频虚拟控制台。要退出全屏模式，请单击 **"Windowed"**（窗口）。
	"Fit"（适应）	将视频虚拟控制台窗口的大小调整为显示服务器视频所需的最小大小。此菜单项在全屏模式中不可用。

表 9-5. Viewer 菜单栏选择 *（续）*

菜单项	项	说明
“Macros”（宏）	• Alt+Ctrl+Del • Alt+Tab • Alt+Esc • Ctrl+Esc • Alt+Space • Alt+Enter • Alt+Hyphen • Alt+F4 • PrtScrn • Alt+PrtScrn • F1 • Pause （暂停） • Tab • Ctrl+Enter • SysRq • Alt+LShift+RShift+Esc • Ctrl+Alt+Backspace • Alt+F? （其中 F? 代表 F1-F12 键） • Ctrl+Alt+F? （其中 F? 代表 F1-F12 键）	在选择了宏或者输入为宏指定的热键之后，该操作将在远程系统上执行。

表 9-5. Viewer 菜单栏选择 *（续）*

菜单项	项	说明
"Tools"（工具）	**"Session Options"**（会话选项）	"Session Options"（会话选项）窗口提供额外的会话查看器控制调整。此窗口提供 **"General"**（常规）和 **"Mouse"**（鼠标）选项卡。 可以从 "General"（常规）选项卡控制 **"Keyboard pass through mode"**（键盘通过模式）。选择 **"Pass all keystrokes to target"**（将所有按键传递到目标），将 Management Station 的按键传递到远程系统。 鼠标选项卡包含两部分：**"Single Cursor"**（单光标）和 **"Mouse Acceleration"**（鼠标加速度）。**"Single Cursor"**（单光标）功能是为了解决某些远程操作系统上鼠标不一致的问题。当查看器进入 **"Single Cursor"**（单光标）模式后，鼠标指针就会限制在 Viewer 窗口内。按终止键可退出此模式。使用此控制来选择可退出单光标模式的键。 **"Mouse Acceleration"**（鼠标加速度）可以根据操作系统优化鼠标的性能。
	"Single Cursor"（单光标）	在 Viewer 中启用单光标模式。在此模式中，客户端光标隐藏起来，只能看到服务器的光标。客户端光标也限制在 Viewer 框内。用户将无法在 Viewer 窗口之外使用光标，直到按下 **"Session Options - Mouse"**（会话选项 - 鼠标）选项卡中指定的**终止键**。
	"Stats"（统计数据）	此菜单选项启动一个对话框，其中显示 Viewer 的性能统计数据。显示的值有： • "Frame Rate"（帧速率） • "Bandwidth"（带宽） • "Compression"（压缩 ） • "Packet Rate"（数据包速率）

表 9-5. Viewer 菜单栏选择 *（续）*

菜单项	项	说明
电源	**"Power ON System"**（打开系统电源）	打开系统电源。
	"Power OFF System"（关闭系统电源）	关闭系统电源。
	"Graceful Shutdown"（正常关机）	关闭系统。 **注：**使用此选项执行正常关机之前，确保为操作系统配置了关机选项。如果没在操作系统上配置此选项就使用此选项，此选项将会重新引导 Managed System，而不是执行关机操作。
	"Reset System (warm boot)"（重设系统 [温引导]）	在不关闭电源的情况下重新引导系统。
	"Power Cycle System (cold boot)"（使系统关机后再开机 [冷引导]）	关闭系统电源，然后重新引导系统。
帮助	**"Contents and Index"**（目录和索引）	说明如何查看联机帮助。
	关于 iDRAC6 虚拟控制台	显示 **iDRAC6 虚拟控制台**版本。

禁用或启用本地服务器视频

可以使用 iDRAC6 Web 界面将 iDRAC6 配置为禁用 iDRAC6 虚拟控制台连接。

如果想保证对受管服务器控制台有独占访问权限，必须在 **"Virtual Console Configuration"**（虚拟控制台配置）页上禁用本地控制台*并*重新配置 **"Max Sessions"**（最大会话数）为 1。

注：禁用 （关闭）服务器上的本地视频后，连接到 iDRAC6 虚拟控制台的显示器、键盘和鼠标仍然启用。

要禁用或启用本地控制台，请执行以下过程：

1 在 Management Station 上，打开支持的 Web 浏览器并登录 iDRAC6。

2 单击 **"System"**（系统）→ **"Console/Media"**（控制台 / 介质）？**"Configuration"**（配置）。

3 要禁用 （关闭）服务器上的本地视频，请清除 **"Configuration"**（配置）页上的 **"Local Server Video Enabled"**（本地服务器视频已启用）复选框，然后单击 **"Apply"**（应用）。默认值为 "OFF"（关）。

注：如果开启本地服务器视频，将需 15 秒关闭。

4 要启用 （打开）服务器上的本地视频，请选择 **"Configuration"**（配置）页上的 **"Local Server Video Enabled"**（本地服务器视频已启用）复选框，然后单击 **"Apply"**（应用）。

远程启动虚拟控制台和虚拟介质

通过在支持的浏览器上输入单个 URL 可以启动虚拟控制台 / 虚拟介质，而不是从 iDRAC6 Web GUI 启动。根据系统配置，会进行手动验证过程（登录页）或自动定向到虚拟控制台 / 虚拟介质 Viewer。

如果 SSO 在系统上已配置，则您不能使用 URL 格式启动虚拟控制台 / 虚拟介质。

您可以使用在 iDRAC6、LDAP 和 Active Directory 中本地创建的用户帐户启动虚拟控制台。

注：Internet Explorer 支持本地、 Active Directory (AD)、智能卡 (SC) 和单一登录 (SSO) 登录。Firefox 在基于 Windows 的操作系统上仅支持本地、AD 和 SSO 登录。它不支持 SC 登录。

使用 URL 格式启动控制台

如果您在浏览器中输入 `link<IP>/console`，则通过正常手动登录程序进行登录取决于登录配置。如果登录成功，虚拟控制台 / 虚拟介质视图将启动。否则，您会重定向到 iDRAC6 GUI 主页。

iDRAC Web GUI 会话在 vKVM 页的背景中显示。

一次只能启动一个虚拟控制台会话。

如果您拥有 "Read Only"（只读）权限，可使用 URL 格式仅启动 "Virtual Console"（虚拟控制台）页，不启动 "Virtual Media"（虚拟介质）页。

如果 iDRAC6 中禁用 “Virtual Console”（虚拟控制台），则用户或管理员权限足够时仍可启动 “Virtual Media”（虚拟介质）。有关足够权限的详情，请参阅第 197 页上的 “远程启动虚拟控制台和虚拟介质”。

一般错误情况

表 9-6 列出了一般错误情况、这些错误的原因和 iDRAC6 表现的行为。

表 9-6. 错误情况

错误情况	原因	行为
登录失败	输入的用户名无效或密码不正确。	与指定 *https://<IP>* 时登录失败的行为一样。
iDRAC6 Enterprise 卡不存在	iDRAC6 Enterprise 卡不存在。因此虚拟控制台 / 虚拟介质功能不能用。	iDRAC6 虚拟控制台 Viewer 没有启动。重定向到 iDRAC6 GUI 主页。
权限不足	您没有虚拟控制台和虚拟介质权限。	iDRAC6 虚拟控制台 Viewer 没有启动，系统重定向到控制台 / 介质配置 GUI 页。
虚拟控制台被禁用	系统中的虚拟控制台已禁用。	iDRAC6 虚拟控制台 Viewer 没有启动，系统重定向到控制台 / 介质配置 GUI 页。
检测到未知的 URL 参数	输入的 URL 包含未定义的参数。	显示 “Page Not Found”（页面未找到） (404) 信息。

虚拟控制台常见问题

表 9-7 列出常见问题和解答。

表 9-7. 使用虚拟控制台：常见问题

问题	解答
带外 Web GUI 注销后，虚拟控制台未能注销。	即使 Web 会话已注销，虚拟控制台和虚拟介质会话仍保持活动。关闭虚拟介质和虚拟控制台 Viewer 应用程序以注销相应会话。
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。

表 9-7. 使用虚拟控制台：常见问题 *（续）*

问题	解答
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，iDRAC6 收到本地视频打开请求后，视频就立刻**打开**。
本地用户还可以关闭视频吗？	当本地控制台禁用时，本地用户不能关闭视频。
本地用户还可以打开视频吗？	当本地控制台禁用时，本地用户不能打开视频。
关闭本地视频是否也会关闭本地键盘和鼠标？	否。
关闭本地控制台是否会关闭远程控制台会话上的视频？	不会，打开或关闭本地视频与远程控制台会话无关。
iDRAC6 用户打开或关闭本地服务器视频需要什么权限？	任何具有 iDRAC6 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？	该状况显示在 iDRAC6 Web 界面的 **“Virtual Console Configuration”**（虚拟控制台配置）页上。 RACADM CLI 命令 `racadm getconfig -g cfgRacTuning` 在对象 **cfgRacTuneLocalServerVideo** 中显示状况。
从 “Virtual Console”（虚拟控制台）窗口看不到系统屏幕的底部。	确保 Management Station 的显示器分辨率设置为 1280x1024。另外，还可尝试使用 iDRAC6 虚拟控制台客户端上的滚动栏。
控制台窗口显示乱码。	Linux 上的控制台查看器需要 UTF-8 字符集。检查区域设置并根据需要重设字符集。

表 9-7. 使用虚拟控制台：常见问题 *（续）*

问题	解答
为什么鼠标在 Linux 文本控制台下不同步 （在 Dell Unified Server Configurator (USC)、 Dell Lifecycle Controller 或 Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)）？	虚拟控制台需要 USB 鼠标驱动程序，但是 USB 鼠标驱动程序只在 X-Windows 操作系统下可用。
我的鼠标同步还是有问题。	启动虚拟控制台会话前，确保为操作系统选择正确的鼠标。 请确保在 iDRAC6 虚拟控制台客户端上选择 iDRAC6 虚拟控制台菜单中 **"Tools"**（工具）下的 **"Single Cursor"**（单光标）选项。默认为双光标模式。
为什么使用 iDRAC6 虚拟控制台远程安装 Microsoft 操作系统期间不能使用键盘或鼠标？	在 BIOS 中启用了虚拟控制台的系统上远程安装支持的 Microsoft 操作系统时，将会收到一则 EMS 连接信息，要求您选择 **"OK"**（确定）后才能继续。无法使用鼠标远程选择 **"OK"**（确定）。必须要么在本地系统上选择 **"OK"**（确定），要么重新启动远程管理的服务器，重新安装，然后在 BIOS 中关闭虚拟控制台。 此信息由 Microsoft 生成，用来提醒用户，虚拟控制台已启用。为了确保不显示此信息，远程安装操作系统前，应始终在 BIOS 中关闭虚拟控制台。
为什么 Management Station 上的 Num Lock 指示灯不反映远程服务器上 Num Lock 的状况？	当通过 iDRAC6 访问时， Management Station 上的 Num Lock 指示灯不一定与远程服务器上的 Num Lock 状态保持一致。 Num Lock 的状态取决于连接远程会话时远程服务器上的设置，而与 Management Station 上 Num Lock 的状态无关。
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？	您在从本地系统配置虚拟控制台会话。这不受支持。
如果我正在运行虚拟控制台会话时本地用户访问受管服务器，会收到警告信息吗？	否。如果本地用户访问系统，两人都有系统控制权。

表 9-7. 使用虚拟控制台：常见问题 *（续）*

问题	解答
我需要多少带宽来运行虚拟控制台会话？	建议具有 5 MB/ 秒连接确保良好性能。最低性能需要 1 MB/sec 连接。
Management Station 运行虚拟控制台有什么最低系统要求？	Management Station 需要 Intel Pentium III 500 MHz 处理器和至少 256 MB 的 RAM。
为什么我在 iDRAC6 虚拟控制台 Video Viewer 上看到一则 **“No Signal”**（无信号）信息？	您看到此信息可能是因为 iDRAC6 虚拟控制台插件未接收到远程服务器桌面视频。通常，在远程服务器被切断电源时可能发生此行为。有时此信息可能由于远程服务器桌面视频接收故障而显示。
为什么我在 iDRAC6 虚拟控制台 Video Viewer 上看到一则 **“Out of Range”**（超出范围）信息？	您看到此信息可能是因为捕获视频所需的参数超出 iDRAC6 能够捕获视频的范围。显示分辨率或刷新率等参数过高将导致出现超过范围状况。通常，参数的最大范围由视频内存大小或带宽等物理限制设置。

10

使用 WS-MAN 界面

Web Services for Management (WS – MAN) 是用于系统管理的基于简单对象访问协议 (SOAP) 的一种协议。 WS – MAN 提供设备互操作协议，供设备在网络间共享和交换数据。 iDRAC6 使用 WS – MAN 提供基于分布式管理综合小组 (DMTF) 公用信息模型 (CIM) 的管理信息； CIM 信息定义可以在 Managed System 上操作的语义和信息类型。 Dell 嵌入式服务器平台管理接口划分到多个配置文件中，每个配置文件定义特定管理域或功能区的特定接口。此外， Dell 定义了多个模型和配置文件扩展，为接口提供更多功能。

通过 WS-MAN 提供的数据通过映射到下列 DMTF 配置文件和 Dell 扩展配置文件的 iDRAC6 工具界面提供：

支持的 CIM 配置文件

表 10-1. 标准 DMTF

标准 DMTF
1 基础服务器 定义表示主机服务器的 CIM 类。
2 服务处理器： 包含表示 iDRAC6 的 CIM 类定义。
3 物理资产： 定义表示受管元素的物理方面的 CIM 类。 iDRAC6 使用此配置文件表示主机服务器的 FRU 信息。
4 SM CLP 管理员域 定义表示 CLP 配置的 CIM 类。 iDRAC6 使用此配置文件自行实施 CLP。
5 电源状态管理 定义用于电源控制操作的 CIM 类。 iDRAC6 使用此配置文件进行主机服务器的电源控制操作。
6 电源设备 （版本 1.1） 定义表示电源设备的 CIM 类。 iDRAC6 使用此配置文件表示主机服务器的电源设备，以说明功耗 （如高低功耗水印）。

表 10-1. 标准 DMTF *（续）*

标准 DMTF
7 CLP 服务 定义表示 CLP 配置的 CIM 类。 iDRAC6 使用此配置文件自行实施 CLP。
8 IP 界面
9 DHCP 客户端
10 DNS 客户端
11 以太网端口 上述配置文件定义表示网络堆栈的 CIM 类。 iDRAC6 使用这些配置文件表示 iDRAC6 NIC 的配置。
12 记录日志 定义表示不同类型的日志的 CIM 类。 iDRAC6 使用此配置文件表示系统事件日志 (SEL) 和 iDRAC6 RAC 日志。
13 软件资源清册 定义已安装或可用软件的资源清册的 CIM 类。通过 TFTP 协议， iDRAC6 使用此配置文件对当前安装的 iDRAC6 固件版本进行资源清册。
14 基于角色授权 定义表示角色的 CIM 类。 iDRAC6 使用此配置文件配置 iDRAC6 帐户权限。
15 软件更新 定义对可用软件更新进行资源清册的 CIM 类。通过 TFTP 协议， iDRAC6 使用此配置文件对固件更新进行资源清册。
16 SMASH 收集 定义表示 CLP 配置的 CIM 类。 iDRAC6 使用此配置文件自行实施 CLP。
17 配置文件注册 定义通告配置文件实施的 CIM 类。按本表所述， iDRAC6 使用此配置文件通告其自行实施的配置文件。
18 基础度量 定义表示度量的 CIM 类。 iDRAC6 使用此配置文件表示主机服务器说明功耗的度量 （如高低功耗水印）。
19 简单标识管理 定义表示标识的 CIM 类。 iDRAC6 使用此配置文件配置 iDRAC6 帐户。
20 USB 重定向 定义表示本地 USB 端口远程重定向的 CIM 类。 iDRAC6 将此配置文件与虚拟介质配置文件结合使用，以配置虚拟介质。

表 10-1. 标准 DMTF *（续）*

Dell 扩展
1 Dell Active Directory 客户端版本 2.0.0 定义用于配置 iDRAC6 Active Directory 客户端和 Active Directory 组本地权限的 CIM 类和 Dell 扩展类。
2 Dell 虚拟介质 定义用于配置 iDRAC6 虚拟介质的 CIM 类和 Dell 扩展类。扩展 USB 重定向配置文件。
3 Dell 以太网端口 定义用于为 iDRAC6 NIC 配置 NIC 边带界面的 CIM 类和 Dell 扩展类。扩展以太网端口配置文件。
4 Dell 电源利用管理 定义表示主机服务器电源预算和配置 / 监测主机服务器电源预算的 CIM 类和 Dell 扩展类。
5 Dell 操作系统部署 定义表示操作系统部署功能配置的 CIM 和 Dell 扩展类。通过使用服务处理器提供的操作系统部署功能支持操作系统部署，扩展了引用配置文件的管理功能。
6 Dell 作业控制 定义用于管理配置作业的 CIM 类和 Dell 扩展类。
7 Dell LC 管理配置文件 定义 Dell Lifecycle Controller 的配置属性的 CIM 类和 Dell 扩展类，例如自动查找。此配置文件还可以管理部件更换、母板更换、系统配置文件的导出和导入、从网络共享引导和加密证书管理。
8 Dell 永久存储 定义用于管理 Dell 平台的 vFlash SD 卡上分区的 CIM 类和 Dell 扩展类。
9 Dell 简单 NIC 定义表示 NIC 网络控制器配置的 CIM 类和 Dell 扩展类。
10 Dell BIOS 和引导管理配置文件 定义表示 Dell BIOS 属性和用于配置主机的引导顺序的 CIM 类和 Dell 扩展类。
11 Dell RAID 配置文件 定义表示主机 RAID 存储配置的 CIM 类和 Dell 扩展类。
12 Dell 电源配置文件 定义表示主机电源设备资源清册信息的 CIM 类和 Dell 扩展类。

表 10-1. 标准 DMTF *（续）*

Dell 扩展
13 Dell iDRAC 卡配置文件 定义表示 iDRAC6 资源清册信息的 CIM 类和 Dell 扩展类。此配置文件还提供用于配置 iDRAC 属性和用户帐户的表示和方法。
14 Dell 风扇配置文件 定义表示主机风扇资源清册信息的 CIM 类和 Dell 扩展类。
15 Dell 内存配置文件 定义表示主机 DIMM 资源清册信息的 CIM 类和 Dell 扩展类。
16 Dell CPU 配置文件 定义表示主机 CPU 资源清册信息的 CIM 类和 Dell 扩展类。
17 Dell 系统信息配置文件 定义表示主机平台资源清册信息的 CIM 类和 Dell 扩展类。
18 Dell PCI 设备配置文件 定义表示主机 PCI 设备资源清册信息的 CIM 类和 Dell 扩展类。
19 Dell 视频配置文件 定义表示主机视频卡资源清册信息的 CIM 类和 Dell 扩展类。

iDRAC6 WS – MAN 实施在端口 443 上使用 SSL 实现传输安全性，并支持基本验证和摘要验证。可通过 Windows WinRM 和 Powershell CLI 等客户端基础架构、WSMANCLI 等开放源代码公用程序、Microsoft .NET 等应用程序编程环境利用 Web 服务接口。

有关 Dell Lifecycle Controller 远程服务的详情，请参阅以下说明文件：

- 用户指南
- 发行说明
- 错误信息和故障排除列表

访问这些说明文件：

1. 进入 **dell.com/support/manuals**。
2. 单击 “**Software**”（软件）→ “**Systems Management**”（系统管理）→ “**Dell Unified Server Configurator and Lifecycle Controller**”（Dell Unified Server Configurator 和 Lifecycle Controller）。

3 单击相关版本查看特定版本的所有文档。

有关 Web 服务界面指南 （Windows 和 Linux）、配置文件说明文件、代码示例、白皮书和其它有用的信息，请导航至 **delltechcenter.com** 上的 **“OpenManage Systems Management”**（OpenManage 系统管理） → **Lifecycle Controller**。

有关详情，请参阅以下内容：

- DMTF 网站 **dmtf.org/standards/profiles/**
- WS – MAN 发行注释或自述文件。

11

使用 iDRAC6 SM-CLP 命令行界面

本节提供了有关 iDRAC6 中纳入的分布式管理综合小组 (DMTF) 的服务器管理命令行协议 (SM-CLP) 的信息。

注：本节假定用户熟悉服务器硬件系统管理体系结构 (SMASH) 标准和 SM-CLP 规范。有关这些规范的详情，请参阅 DMTF 网站 dmtf.org。

iDRAC6 SM-CLP 是一项提供系统管理 CLI 实施标准的协议。SM-CLP 是 DMTF SMASH 标准的一部分，可跨多个平台简化服务器管理。 SM-CLP 规范，与受管元件寻址规范 (Managed Element Addressing Specification)、众多配置文件以及 SM-CLP 映射规范配合使用，可说明各种管理任务执行的标准 verb 和目标。

iDRAC6 SM-CLP 支持

SM-CLP 由 iDRAC6 控制器固件承载，并且支持 Telnet、SSH 和基于串行的接口。 iDRAC6 SM-CLP 界面基于由 DMTF 组织提供的 SM-CLP 规范版本 1.0。 iDRAC6 SM-CLP 支持表 10-1 中所述的所有配置文件。

以下各节提供了 iDRAC6 上 SM-CLP 功能的概览。

SM-CLP 功能

SM-CLP 提供了 verb 的概念，并旨在通过 CLI 提供系统管理功能。 verb 表示要执行的操作，而目标确定了要运行操作的实体 （或对象）。

请参阅 SM-CLP 命令行语法的以下示例。

```
<verb> [< 选项 >] [< 目标 >] [< 属性 >]
```

在典型的 SM-CLP 会话期间，您可以用表 11-1 中所列的 verb 执行操作。

表 11-1. 系统支持的 CLI Verb

Verb	定义
cd	使用 Shell 导航映射
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

表 11-1. 系统支持的 CLI Verb *（续）*

Verb	定义
show	显示目标属性、 verb 和子目标
启动	打开目标
stop	关闭目标
exit	从 SM-CLP 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 地址移至指定目标地址

使用 SM-CLP

SSH （或 Telnet）到 iDRAC6，使用正确的凭据。

SMCLP 提示符 (/admin1–>) 将会显示。

SM-CLP 目标

表 11-2 提供通过 SM-CLP 提供的目标列表，支持上述表 11-1 中所述的操作。

表 11-2. SM-CLP 目标

目标	定义
admin1	管理员域
admin1/profiles1	iDRAC6 中的注册配置文件
admin1/hdwr1	硬件
admin1/system1	Managed System 目标
admin1/system1/redundancyset1	电源设备
admin1/system1/redundancyset1/pwrsupply*	Managed System 电源设备
admin1/system1/sensors1	Managed System 传感器
admin1/system1/capabilities1	Managed System SMASH 收集功能
admin1/system1/capabilities1/pwrcap1	Managed System 电源利用功能
admin1/system1/capabilities1/elecap1	Managed System 目标功能

表 11-2. SM-CLP 目标 *（续）*

目标	定义
admin1/system1/logs1	记录日志收集目标
admin1/system1/logs1/log1	系统事件日志 (SEL) 记录条目
admin1/system1/logs1/log1/record*	Managed System 上的单独 SEL 记录实例
admin1/system1/settings1	Managed System SMASH 收集设置
admin1/system1/settings1/pwrmaxsetting1	Managed System 最大电源分配设置
admin1/system1/settings1/pwrminsetting1	Managed System 最小电源分配设置
admin1/system1/capacities1	Managed System 容量 SMASH 收集
admin1/system1/consoles1Internet Explorer	Managed System 控制台 SMASH 收集
admin1/system1/usbredirectsap1	虚拟介质 USB 重定向 SAP
admin1/system1/usbredirectsap1/remotesap1	虚拟介质目标 USB 重定向 SAP
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/ipcap1	IP 接口功能
admin1/system1/sp1/capabilities1/dhcpcap1	DHCP 客户端功能
admin1/system1/sp1/capabilities1/NetPortCfgcap1	网络端口配置功能
admin1/system1/sp1/capabilities1/usbredirectcap1	虚拟介质功能 USB 重定向 SAP

表 11-2. SM-CLP 目标 *（续）*

目标	定义
admin1/system1/sp1/capabilities1/vmsapcap1	虚拟介质 SAP 功能
admin1/system1/sp1/capabilities1/swinstallsvccap1	软件安装服务功能
admin1/system1/sp1/capabilities1/acctmgtcap*	帐户管理服务功能
admin1/system1/sp1/capabilities1/adcap1	Active Directory 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/capabilities/metriccap1	跃点服务功能
admin1/system1/sp1/capabilities1/elecap1	多重验证功能
admin1/system1/sp1/capabilities1/lanendptcap1	LAN （以太网端口）端点功能
admin1/system1/sp1/logs1	服务处理器日志收集
admin1/system1/sp1/logs1/log1	系统记录日志
admin1/system1/sp1/logs1/log1/record*	系统日志条目
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/settings1/ipsettings1	IP 接口分配设置数据 （静态）
admin1/system1/sp1/settings1/ipsettings1/staticipsettings1	静态 IP 接口分配设置数据
admin1/system1/sp1/settings1/ipsettings1/dnssettings1	DNS 客户端设置数据

表 11-2. SM-CLP 目标 *（续）*

目标	定义
admin1/system1/sp1/settings1/ipsettings2	IP 接口分配设置数据 (DHCP)
admin1/system1/sp1/settings1/ipsettings2/dhcpsettings1	DHCP 客户端设置数据
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/ipcfgsvc1	IP 接口配置服务
admin1/system1/sp1/ipendpt1	IP 接口协议端点
admin1/system1/sp1/ipendpt1/gateway1	IP 接口网关
admin1/system1/sp1/ipendpt1/dhcpendpt1	DHCP 客户端协议端点
admin1/system1/sp1/ipendpt1/dnsendpt1	DNS 客户端协议端点
admin1/system1/sp1/ipendpt1/dnsendpt1/dnsserver*	DNS 客户端服务器
admin1/system1/sp1/NetPortCfgsvc1	网络端口配置服务
admin1/system1/sp1/lanendpt1	LAN 端点
admin1/system1/sp1/lanendpt1/enetport1	以太网端口
admin1/system1/sp1/VMediaSvc1	虚拟介质服务
admin1/system1/sp1/VMediaSvc1/tcpendpt1	虚拟介质 TCP 协议端点

表 11-2. SM-CLP 目标 *（续）*

目标	定义
admin1/system1/sp1/swid1	软件标识
admin1/system1/sp1/ swinstallsvc1	软件安装服务
admin1/system1/sp1/ account1-16	多重验证 (MFA) 帐户
admin1/sysetm1/sp1/ account1-16/identity1	本地用户身份帐户
admin1/sysetm1/sp1/ account1-16/identity2	IPMI 身份 (LAN) 帐户
admin1/sysetm1/sp1/ account1-16/identity3	IPMI 身份 （串行）帐户
admin1/sysetm1/sp1/ account1-16/identity4	CLP 身份帐户
admin1/system1/sp1/acctsvc1	MFA 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/group1-5	Active Directory 组
admin1/system1/sp1/ group1-5/identity1	Active Directory 身份
admin1/system1/sp1/ADSvc1	Active Directory 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/rolesvc1/ Role17-21/	Active Directory 角色
admin1/system1/sp1/rolesvc1/ Role17-21/privilege1	Active Directory 权限
admin1/system1/sp1/rolesvc2	IPMI RBA 服务

表 11-2. SM-CLP 目标 *（续）*

目标	定义
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
admin1/system1/sp1/pwrutilmgtsvc1	电源利用管理服务
admin1/system1/sp1/pwrutilmgtsvc1/pwrcurr1	电源利用管理服务当前电源分配设置数据
admin1/system1/sp1/metricsvc1	跃点服务
/admin1/system1/sp1/metricsvc1/cumbmd1	累计基础跃点定义
/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	累计基础跃点数
/admin1/system1/sp1/metricsvc1/cumwattamd1	累计瓦特聚合跃点定义
/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	累计瓦特聚合跃点数
/admin1/system1/sp1/metricsvc1/cumampamd1	累计安培聚合跃点定义
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	累计安培聚合跃点数
/admin1/system1/sp1/metricsvc1/loamd1	低聚合跃点定义
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	低聚合跃点数

表 11-2. SM-CLP 目标 *（续）*

目标	定义
/admin1/system1/sp1/metricsvc1 /hiamd1	高聚合跃点定义
/admin1/system1/sp1/metricsvc1 /hiamd1/hiamv*	高聚合跃点数
/admin1/system1/sp1/metricsvc1 /avgamd1	平均聚合跃点定义
/admin1/system1/sp1/metricsvc1 /avgamd1/avgamv*	平均聚合跃点数

12

使用 VMCLI 部署操作系统

虚拟介质命令行界面 (VMCLI) 公用程序是一个命令行界面，从 Management Station 向远程系统中的 iDRAC6 提供虚拟介质功能。使用 VMCLI 和脚本方法，可以在网络中的多个远程系统上部署操作系统。

本节提供了有关将 VMCLI 公用程序集成到公司网络的信息。

开始之前

开始使用 VMCLI 公用程序前，应确保目标远程系统和公司网络符合以下各节所列的要求。

远程系统要求

iDRAC6 在各个远程系统上配置。

网络要求

网络共享必须包含以下组件：

- 操作系统文件
- 需要的驱动程序
- 操作系统引导映像文件

  映像文件必须是一个操作系统 CD，也可以是具有工业标准的可引导格式的 CD/DVD ISO 映像。

创建可引导映像文件

将映像文件部署到远程系统前，应确保所支持系统可以从该文件引导。要检测映像文件，使用 iDRAC6 Web 用户界面将映像文件传输到检测系统，然后重新引导该系统。

以下各节提供了有关为 Linux 和 Microsoft Windows 系统创建映像文件的特定信息。

为 Linux 系统创建映像文件

使用数据复制器 (dd) 公用程序为 Linux 系统创建可引导映像文件。

要运行该公用程序，打开命令提示符并键入以下命令：

```
dd if=< 输入设备 > of=< 输出文件 >
```

例如：

```
dd if=/dev/sdc0 of=mycd.img
```

为 Windows 系统创建映像文件

为 Windows 映像文件选择数据复制器公用程序时，选择一个复制映像文件和 CD/DVD 引导扇区的公用程序。

准备部署

配置远程系统

1. 创建可以由 Management Station 访问的网络共享。
2. 将操作系统文件复制到网络共享。
3. 如果有可引导的预配置部署映像文件将操作系统部署到远程系统，则应跳过此步骤。

   如果没有可引导的预配置部署映像文件，应创建该文件。包括任何用于操作系统部署过程的程序和 / 或脚本。

   例如，要部署 Windows 操作系统，映像文件可能要包括类似于 Microsoft Systems Management Server (SMS) 所用部署方法的程序。

   创建映像文件时，执行以下操作：

   - 遵循标准基于网络的安装过程
   - 将部署映像标记为*只读*以确保各个目标系统引导并执行相同的部署过程
4. 请执行以下过程之一：
   - 将 **IPMItool** 和 VMCLI 集成到现有操作系统部署应用程序。使用示例 **vm6deploy** 脚本作为使用公用程序的指南。
   - 使用现有 **vm6deploy** 脚本部署操作系统。

部署操作系统

使用 VMCLI 公用程序和该公用程序包含的 **vm6deploy** 脚本将操作系统部署到远程系统。

开始之前，应查看 VMCLI 公用程序包含的示例 **vm6deploy** 脚本。该脚本显示了将操作系统部署到网络中远程系统的详细步骤。

以下过程提供了在目标远程系统上部署操作系统的高级别概览。

1. 在 **ip.txt** 文本文件中列出将要部署的远程系统的 iDRAC6 IPv4 或 IPv6 地址，每行一个 IPv4 或 IPv6 地址。
2. 在客户端介质驱动器中插入可引导操作系统 CD 或 DVD。
3. 在命令行运行 **vm6deploy**。

要运行 **vm6deploy** 脚本，在命令提示符处输入以下命令：

```
vm6deploy -r ip.txt -u <idrac 用户> -p <idrac 用户密码> -
c {<iso9660 映像> | <路径>} -f {<软盘设备> 或 <软盘映像>}
```

其中

- *<idrac 用户>* 是 iDRAC6 用户名，例如 **root**
- *<idrac 用户密码>* 是 iDRAC6 用户的密码，例如 **calvin**
- *<iso9660- 映像>* 是操作系统安装 CD 或 DVD 的 ISO9660 映像路径
- -f {*< 软盘设备 >*} 是包含操作系统安装 CD、 DVD 或软盘的设备的路径
- *< 软盘映像 >* 是有效软盘映像的路径

vm6deploy 脚本将其命令行选项传递给 **VMCLI** 公用程序。请参阅 “命令行选项”了解有关这些选项的详情。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，脚本会从指定文件读取 iDRAC6 IPv4 或 IPv6 地址并每行运行一次 **VMCLI** 公用程序。如果 **-r** 选项的参数不是文件名，则应是单个 iDRAC6 的地址。在这种情况下，**-r** 按 **VMCLI** 公用程序中的说明运行。

使用 VMCLI 公用程序

VMCLI 公用程序是一个可编写脚本的命令行界面，从 Management Station 向 iDRAC6 提供虚拟介质功能。

VMCLI 公用程序提供以下功能：

注：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。

- 与虚拟介质插件一致的可移动介质设备或映像文件
- 启用 iDRAC6 固件引导一次选项后自动终止
- 使用安全套接字层 (SSL) 确保与 iDRAC6 的通信安全

运行公用程序前，确保对 iDRAC6 有虚拟介质用户权限。

小心：建议在启动 VMCLI 命令行公用程序时使用交互式标志 '-i' 选项。通过保护用户名和密码安全可以加强安全性，因为在许多 Windows 和 Linux 操作系统上，当其他用户检查进程时用户名和密码可见。

如果操作系统支持管理员权限或操作系统特定的权限或组成员资格，还将需要管理员权限来运行 VMCLI 命令。

客户端系统的管理员控制用户组和权限，从而控制可运行公用程序的用户。

对于 Windows 系统，必须具有高级用户权限才能运行 VMCLI 公用程序。

对于 Linux 系统，可以使用 **sudo** 命令访问 VMCLI 公用程序，无需管理员权限。此命令提供集中化非管理员访问的方法并记录所有用户命令。要添加或编辑 VMCLI 组中的用户，管理员可以使用 **visudo** 命令。没有管理员权限的用户可以将 **sudo** 命令作为前缀添加到 VMCLI 命令行 （或 VMCLI 脚本）来获取对远程系统上 iDRAC6 的访问和运行公用程序。

安装 VMCLI 公用程序

VMCLI 公用程序位于 *Dell Systems Management Tools and Documentation* DVD 上，该 DVD 随 Dell OpenManage System Management 软件套件提供。要安装该公用程序，请将 *Dell Systems Management Tools and Documentation* DVD 插入系统 DVD 驱动器并按照屏幕上的说明操作。

Dell Systems Management Tools and Documentation DVD 包含最新系统管理软件产品，包括存储管理、远程访问服务和 IPMItool 公用程序。此 DVD 还包含自述文件，提供最新系统管理软件产品信息。

Dell Systems Management Tools and Documentation DVD 包含 **vm6deploy** — 这是一个说明如何使用 VMCLI 和 IPMItool 公用程序将软件部署到多个远程系统的示例脚本。

注：vm6deploy 脚本依赖于安装时目录中存在的其它文件。如果想从另一个目录使用脚本，必须随之复制所有的文件。如果并未安装 IPMItool 公用程序，则除其它文件外，还须复制该公用程序。

命令行选项

VMCLI 界面在 Windows 和 Linux 系统上相同。

VMCLI 命令格式如下：

`VMCLI [ 参数 ] [ 操作系统外壳程序选项 ]`

命令行语法区分大小写。有关详情，请参阅第 221 页上的 “VMCLI 参数”。

如果远程系统接受了命令，并且 iDRAC6 授权连接，则命令将继续运行，直至出现以下任何一种情况：

- VMCLI 连接因任何原因终止。
- 使用操作系统控制手动终止进程。例如，在 Windows 中，可以使用任务管理器终止进程。

VMCLI 参数

iDRAC6 IP 地址

`-r <iDRAC IP 地址 >[:<iDRAC SSL 端口 >]`

此参数提供 iDRAC6 IPv4 或 IPv6 地址和 SSL 端口，公用程序用来与目标 iDRAC6 建立虚拟介质连接。如果输入无效 IPv4 或 IPv6 地址或 DDNS 名称，将会显示错误信息并且终止命令。

<iDRAC IP 地址 > 是有效、独特的 IPv4 或 IPv6 地址或 iDRAC6 动态域名系统 (DDNS) 名称 （如果支持）。如果省略 *<iDRAC SSL 端口 >*，则使用端口 443 （默认端口）。除非更改了 iDRAC6 的默认 SSL 端口，否则不需要可选的 SSL 端口。

iDRAC6 用户名

`-u <iDRAC 用户 >`

此参数提供将运行虚拟介质的 iDRAC6 用户名。

<iDRAC 用户 > 必须具有以下属性：

- 有效用户名
- iDRAC6 虚拟介质用户权限

如果 iDRAC6 验证失败，将会显示错误信息并且终止命令。

iDRAC6 用户密码

`-p <iDRAC 用户密码>`

此参数提供指定 iDRAC6 用户的密码。

如果 iDRAC6 验证失败，将会显示错误信息并且终止命令。

软盘 / 磁盘设备或映像文件

`-f {<软盘设备> 或 <软盘映像>}` 和 / 或

`-c {<CD-DVD 设备> 或 <CD-DVD 映像>}`

其中 <软盘设备> 或 `<CD-DVD 设备>` 是有效的驱动器号（对于 Windows 系统）或有效的设备文件名（对于 Linux 系统），而 <**软盘映像**> 或 `<CD-DVD 映像>` 是有效映像文件的文件名和路径。

注：VMCLI 公用程序不支持安装点。

此参数指定提供虚拟软盘 / 磁盘介质的设备或文件。

例如，映像文件指定如下：

`-f c:\temp\myfloppy.img`（Windows 系统）

`-f /tmp/myfloppy.img`（Linux 系统）

如果文件没有写保护，虚拟介质将会写入映像文件。配置操作系统来写保护不应改写的软盘映像文件。

例如，设备指定如下：

`-f a:\`（Windows 系统）

`-f /dev/sdb4 # 4th partition on device /dev/sdb`（Linux 系统）

注：Red Hat Enterprise Linux 版本 4 不支持多个 LUN。不过，内核支持此功能。通过以下步骤使 Red Hat Enterprise Linux 版本 4 能够识别具有多个 LUN 的 SCSI 设备：

1. 编辑 **/etc/modprobe.conf** 并添加以下行：
   `options scsi_mod max_luns=8`
   （可以指定 8 个或大于 1 的任意数量的 LUN。）
2. 在命令行键入以下命令，获取内核映像的名称：
   `uname -r`
3. 转至 **/boot** 目录，删除步骤 2 中所指定名称的内核映像文件，名称为：
   `mkinitrd /boot/initrd-’ uname -r’ .img ‘uname -r’`

4 重新引导服务器。

5 运行以下命令，确认已为步骤 1 中所指定的 LUN 数量添加对多个 LUN 的支持：

```
cat /sys/modules/scsi_mod/max_luns
```

如果设备提供了写保护功能，请使用该功能确保虚拟介质不会写介质。

如果不虚拟化软盘介质，请在命令行上省略此参数。如果检测到无效值，将会显示错误信息并且会终止命令。

CD/DVD 设备或映像文件

`-c {<` *设备名称* `> | <` *映像文件* `>}`

其中 < *设备名称* > 是有效 CD/DVD 驱动器号 （Windows 系统）或有效 CD/DVD 设备文件名 （Linux 系统）， < *映像文件* > 是有效 ISO-9660 映像文件的文件名和路径。

此参数指定将提供虚拟 CD/DVD-ROM 介质的设备或文件：

例如，映像文件指定如下：

`-c c:\temp\mydvd.img` （Windows 系统）

`-c /tmp/mydvd.img` （Linux 系统）

例如，设备指定如下：

`-c d:\` （Microsoft Windows 系统）

`-c /dev/cdrom` （Linux 系统）

如果不虚拟化 CD/DVD 介质，请在命令行上省略此参数。如果检测到无效值，将会显示错误信息并且会终止命令。

用此命令指定至少一种介质类型 （软盘或 CD/DVD 驱动器），除非只提供了开关选项。否则，将会显示错误信息并且命令将终止并生成错误。

版本显示

`-v`

此参数用于显示 VMCLI 公用程序版本。如果没有提供其它非开关选项，此命令将会终止，但不会显示错误信息。

帮助显示

`-h`

此参数显示 VMCLI 公用程序参数的摘要。如果没有提供其它非开关选项，此命令将会终止，但不会显示错误。

加密的数据

-e

如果命令行中包括此参数， VMCLI 将使用 *SSL 加密的信道*在 Management Station 和远程系统中的 iDRAC6 之间传输数据。如果命令行中不包括此参数，数据传输将不加密。

注：使用此选项不会在 RACADM 或 Web 界面等其它 iDRAC6 配置界面将显示的虚拟介质加密状况更改为*已启用*。

VMCLI 操作系统 Shell 选项

VMCLI 命令行中可使用以下操作系统功能：

- 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 公用程序不从标准输入 (stdin) 读取。因此不需要 stdin 重定向。

- 后台执行 — 默认情况下 VMCLI 公用程序在前台运行。使用操作系统的命令 Shell 功能可以使该公用程序在后台运行。例如，在 Linux 操作系统下，命令后面的 (&) 字符会使程序生成为一个新后台进程。

后一种技术在脚本程序中很有用，因为它允许脚本在为 VMCLI 命令启动新进程后继续执行 （否则，脚本将保持阻止直至 VMCLI 程序终止）。当有多个 VMCLI 实例以这种方式启动，并且必须手动终止一个或多个命令实例时，使用操作系统特定的功能来列出并终止进程。

VMCLI 返回代码

每当出错时，会将文本信息 （仅有英文）发送到标准错误输出。

13

配置智能平台管理接口

本节提供有关配置和使用 iDRAC6 IPMI 接口的信息。接口包括以下：

- “IPMI over LAN”（LAN 上 IPMI）
- 串行 IPMI
- LAN 上串行

iDRAC6 完全兼容 IPMI 2.0。可以通过以下途径配置 iDRAC6 IPMI：

- 浏览器中的 iDRAC6 GUI
- 开放源代码公用程序，比如 *ipmitool*
- Dell OpenManage IPMI shell, *ipmish*
- RACADM

有关使用 IPMI Shell (ipmish) 的详情，请参阅 **support.dell.com\manuals** 上的 《Dell OpenManage 底板管理控制器公用程序用户指南》。

有关使用 RACADM 的详情，请参阅 第 100 页上的 “远程使用 RACADM”。

使用基于 Web 的界面配置 IPMI

有关详细信息，请参阅第 54 页上的 “使用 Web 界面配置 IPMI”。

使用 RACADM CLI 配置 IPMI

1. 使用任何 RACADM 接口登录远程系统。请参阅第 100 页上的 “远程使用 RACADM”。
2. 配置 LAN 上 IPMI。

   打开命令提示符，键入以下命令并按 <Enter>：

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

   注：此设置确定可以从 LAN 上 IPMI 接口执行的 IPMI 命令。有关详情，请参阅 IPMI 2.0 规范。

   a 更新 IPMI 信道权限。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit <级别>
```

其中 <*级别*> 是以下一个值：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要设置 IPMI LAN 信道权限为 2（用户），键入以下命令：

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit 2
```

b 如果需要，设置 IPMI LAN 信道密钥。

注：iDRAC6 IPMI 支持 RMCP+ 协议。有关详情，请参阅 IPMI 2.0 规范。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <密钥>
```

其中 <*密钥*> 是一个有效十六进制格式的 20 字符密钥。

3 配置 IPMI LAN 上串行 (SOL)。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a 更新 IPMI SOL 最低权限级别。

注：IPMI SOL 最低权限级别确定了激活 IPMI SOL 所需的最小权限。有关详情，请参阅 IPMI 2.0 规范。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege <级别>
```

其中 <*级别*> 是以下一个值：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要配置 IPMI 权限为 2（用户），键入以下命令：

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

b 更新 IPMI SOL 波特率。

注：要重定向 LAN 上串行控制台，应确保 SOL 波特率与 Managed System 的波特率相同。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <波特率>
```

其中 <*波特率*> 为 9600、19200、57600 或 115200 bps。

例如：

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

c 为单个用户启用 SOL。

注：可以为每个用户启用或禁用 SOL。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <id> 2
```

其中 <*id*> 是用户的独特 ID。

4 配置 IPMI 串行。

a 将 IPMI 串行连接模式更改为相应的设置。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgSerial -o
cfgSerialConsoleEnable 0
```

b 设置 IPMI 串行波特率。

打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate <波特率>
```

其中 <*波特率*> 为 9600、19200、57600 或 115200 bps。

例如：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate 57600
```

c 启用 IPMI 串行硬件流控制。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialFlowControl 1
```

d 设置 IPMI 串行信道最低权限级别。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit <级别>
```

其中 <*级别*> 是以下一个值：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要设置 IPMI 串行信道权限为 2（用户），键入以下命令：

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit 2
```

e 确保在 BIOS 设置程序中正确设置了串行 MUX。

- 重新启动系统。
- 在开机自检期间，按 <F2> 进入 BIOS 设置程序。
- 单击“Serial Communication”（串行通信）。
- 在“Serial Connection”（串行连接）菜单中，确保“External Serial Connector”（外部串行连接器）设置为“Remote Access Device”（远程访问设备）。
- 保存并退出 BIOS 设置程序。
- 重新启动系统。

IPMI 配置完成。

如果 IPMI 串行处于终端模式，可以使用 **racadm config cfgIpmiSerial** 命令配置以下其它设置：

- 删除控制
- 回声控制
- 行编辑

- 新行序列
- 输入新行序列

有关这些属性的详情，请参阅 IPMI 2.0 规范。

使用 IPMI 远程访问串行接口

在 IPMI 串行接口中，以下模式可用：

- “IPMI terminal mode”（IPMI 终端模式）— 支持从串行终端提交的 ASCII 命令。命令集仅有有限数量的命令 （包括电源控制）并支持作为十六进制 ASCII 字符输入的原始 IPMI 命令。
- “IPMI basic mode”（IPMI 基本模式）— 支持二进制接口以进行程序访问，比如底板管理公用程序 (BMU) 附带的 IPMI Shell (IPMISH)。

要使用 RACADM 配置 IPMI 模式：

1 禁用 RAC 串行接口。

在命令提示符下键入：

```
racadm config -g cfgSerial -o
cfgSerialConsoleEnable 0
```

2 启用相应的 IPMI 模式。

例如，在命令提示符下键入：

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

有关详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 iDRAC6 属性数据库组和对象定义。

配置 LAN 上串行使用基于 Web 的界面

有关详细信息，请参阅第 54 页上的 “使用 Web 界面配置 IPMI”。

注：LAN 上串行可与以下 Dell OpenManage 工具一起使用：SOLProxy 和 IPMItool。有关详情，请参阅 **support.dell.com\manuals** 上的 《Dell OpenManage 底板管理控制器公用程序用户指南》。

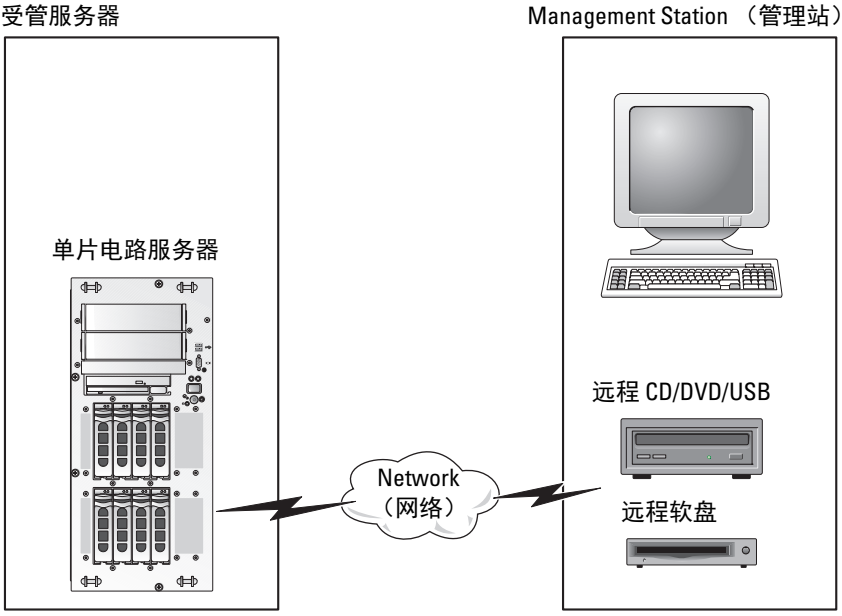
14

配置并使用虚拟介质

概览

虚拟介质功能可通过虚拟控制台 Viewer 访问，提供了受管服务器对网络上远程系统所连介质的访问。图 14-1 显示了**虚拟介质**的整体结构。

图 14-1. 虚拟介质的整体结构



使用**虚拟介质**，管理员可以远程引导其受管服务器，安装应用程序，更新驱动程序，甚至从虚拟 CD/DVD 和软盘驱动器远程安装新操作系统。

注：虚拟介质至少需要 128 Kbps 的可用网络带宽。

虚拟介质为受管服务器的操作系统和 BIOS 定义了两种设备：软盘设备和光盘设备。

Management Station 通过网络提供物理介质或映像文件。附加或自动附加**虚拟介质**后，来自受管服务器的所有虚拟 CD/ 软盘驱动器访问请求都会通过网络定向到 Management Station。连接**虚拟介质相**当于将介质插入 Managed System 的物理设备。当**虚拟介质**处于已附加状态时， Managed System 上的虚拟设备会显示为未装有介质的两个驱动器。

表 14-1 列出了虚拟软盘和虚拟光盘驱动器支持的驱动器连接。

注：在连接期间更改**虚拟介质**会停止系统引导顺序。

表 14-1. 支持的驱动器连接

支持的虚拟软盘驱动器连接	支持的虚拟光盘驱动器连接
带有 1.44 软盘的传统 1.44 软盘驱动器	带有 CD-ROM 介质的 CD-ROM、DVD、 CDRW 组合驱动器
带有 1.44 软盘的 USB 软盘驱动器	ISO9660 格式的 CD-ROM/DVD 映像文件
1.44 软盘映像	带有 CD-ROM 介质的 USB CD-ROM 驱动器
USB 可移动磁盘	

基于 Windows 的 Management Station

要在运行 Microsoft Windows 操作系统的 Management Station 上运行**虚拟介质**功能，请安装支持版本的带有 Java Runtime Environment (JRE) 的 Internet Explorer 或 Firefox。

基于 Linux 的 Management Station

要在运行 Linux 操作系统的 Management Station 上运行虚拟介质功能，请安装支持版本的 Firefox。

需要安装 32 位 Java Runtime Environment (JRE) 才能运行虚拟控制台插件。可以从 **java.sun.com** 下载 JRE。

警告：为了成功启动虚拟介质，确保在 64 位操作系统上已安装 32 位或 64 位 JRE 版本，或在 32 位操作系统上已安装 32 位 JRE 版本。iDRAC6 不支持 64 位 ActiveX 版本。同样对于 Linux，确保必须安装 "compat-libstdc++-33-3.2.3-61" 相关软件包才能启动虚拟介质。在 Windows 上，该软件包可能包含在 .NET Framework 软件包中。

配置虚拟介质

1 登录到 iDRAC6 Web 界面。

2 选择 “System”（系统） → “Console/Media”（控制台 / 介质）选项卡 → “Configuration”（配置） → “Virtual Media”（虚拟介质）来配置虚拟介质设置。

表 14-2 说明**虚拟介质**配置值。

3 配置完设置后，单击 “Apply”（应用）。

表 14-2. 虚拟介质配置属性

属性	值
状况	“Attach”（附加） - 立刻将 “Virtual Media”（虚拟介质）附加到服务器。 “Detach”（分离） - 立刻从服务器上分离 “Virtual Media”（虚拟介质）。 “Auto-Attach”（自动附加） - 只有当虚拟介质会话启动时才将 “Virtual Media”（虚拟介质）附加到服务器。
Max Sessions （最大会话数）	显示 “Virtual Media”（虚拟介质）会话的最大允许数目，此值始终为 1。
“Active Sessions”（激活的会话数）	显示 “Virtual Media”（虚拟介质）当前会话的数目。
“Virtual Media Encryption Enabled”（虚拟介质加密已启用）	选择或取消选择此复选框以启用或禁用 “Virtual Media”（虚拟介质）连接上的加密。如果选择，则启用加密；如果取消选择，则禁用加密。
“Floppy Emulation”（软盘仿真）	表示 “Virtual Media”（虚拟介质）对于服务器显示为软盘驱动器还是 USB 闪存盘。如果选中 “Floppy Emulation”（软盘仿真），则 “Virtual Media”（虚拟介质）设备显示为服务器上的软盘设备。如果清空此项，则显示为 USB 闪存盘驱动器。 **注：在某些 Windows Vista 和 Red Hat 环境上，可能无法虚拟化已启用 “Floppy Emulation”（软盘仿真）的 USB。**

表 14-2. 虚拟介质配置属性 *（续）*

属性	值
连接状态	“Connected”（已连接） - 虚拟介质会话正在进行。 “Not connected”（未连接） - 虚拟介质会话不在进行。
“Enable Boot Once”（启用引导一次）	选择此框可以启用 “Boot Once”（引导一次）选项。使用此属性从虚拟介质引导。在下次引导时，从 BIOS 引导菜单中选择引导设备。系统引导一次后，此选项将自动断开 “Virtual Media”（虚拟介质）设备连接。

运行虚拟介质

警告：运行虚拟介质会话时不要发出 racreset 命令。否则可能发生意外情况，例如丢失数据。

注：访问虚拟介质时， Console Viewer 窗口应用程序必须保持活动。

注：执行以下步骤以启用 Red Hat Enterprise Linux （版本 4）来识别含多个逻辑单元 (LUN) 的 SCSI 设备：

1 将以下行添加至 /ect/modprobe：

```
options scsi_mod max_luns=256

cd /boot

mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
```

2 重新引导服务器。

3 运行以下命令以查看虚拟 CD/DVD 和 / 或虚拟软盘：

```
cat /proc/scsi/scsi
```

注：通过使用虚拟介质，在 Management Station 上只能虚拟化一个软盘 /USB 驱动器 / 映像 / 闪存盘和一个光盘驱动器，用作受管服务器上的 （虚拟）驱动器。

支持的虚拟介质配置

可以为一个软盘驱动器和一个光盘驱动器启用虚拟介质。对每种介质类型一次只能虚拟化一个驱动器。

支持的软盘驱动器包括软盘映像或一个可用软盘驱动器。支持光盘驱动器包括最多一个可用光盘驱动器或一个 ISO 映像文件。

连接虚拟介质

执行以下步骤以运行虚拟介质：

1. 在 Management Station 上打开支持的 Web 浏览器。
2. 启动 iDRAC6 Web 界面。有关详情，请参阅第 41 页上的 “访问 Web 界面”。
3. 选择 “System”（系统） → “Console/Media”（控制台 / 介质） → “Virtual Console and Virtual Media”（虚拟控制台和虚拟介质）。
4. 将显示 “Virtual Console and Virtual Media”（虚拟控制台和虚拟介质）页。如果要更改任何显示属性的值，请参阅第 233 页上的 “配置虚拟介质”。

   注：软盘驱动器下的软**盘映像文件**（如果可用）可能显示，只要该设备可虚拟化为虚拟软盘。可以同时选择一个光盘驱动器和一个软盘 /USB 快擦写驱动器进行虚拟化。

   注：受管服务器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：虚拟介质可能无法在配置有 Internet Explorer Enhanced Security 的 Windows 操作系统客户端上正常运行。要解决此问题，请参阅 Microsoft 操作系统说明文件或联系系统管理员。

5. 单击 “Launch Virtual Console”（启动虚拟控制台）。

   注：在 Linux 上，文件 jviewer.jnlp 会下载到桌面，并且会出现一个对话框，询问对该文件执行什么操作。选择选项 “Open with program”（用程序打开），然后选择 javaws 应用程序，该程序位于 JRE 安装目录的 bin 子目录。

   iDRAC6 **虚拟控制台**应用程序会在单独窗口中启动。

6. 单击 “Virtual Media”（虚拟介质） → “Launch Virtual Media”（启动虚拟介质）。

   将会显示 “Virtual Media Session”（虚拟介质会话）向导。

   注：除非希望终止虚拟介质会话，否则请勿关闭此向导。

7 如果介质已连接，必须断开连接，然后再连接到其它介质源。清除要断开连接的介质左边的框。

8 选择您要连接的介质类型。

如果希望连接软盘映像或 ISO 映像，输入映像的路径 （在本地计算机上），或单击 “Add Image”（添加映像）按钮并浏览到映像。

介质将会连接并且 “Status”（状态）窗口将会更新。

断开虚拟介质连接

1 单击 “Tools”（工具） → “Launch Virtual Media”（启动虚拟介质）。

2 清除要断开连接的介质旁边的框。

介质将会断开连接并且 “Status”（状态）窗口将会更新。

3 单击 “Exit”（退出）终止 “Virtual Media Session”（虚拟介质会话）向导。

注：每当启动虚拟介质会话或连接 vFlash 时，主机操作系统和 BIOS 中会显示名为 "LCDRIVE" 的附加驱动器。当 vFlash 或虚拟介质会话断开连接时，此附加驱动器消失。

从虚拟介质引导

系统 BIOS 使用户能够从虚拟光盘驱动器或虚拟软盘驱动器引导。开机自检过程中，进入 BIOS 设置窗口，验证虚拟驱动器已启用并按正确顺序列出。

要更改 BIOS 设置，执行下列步骤：

1 引导受管服务器。

2 按 <F2> 进入 BIOS 设置窗口。

3 滚动到引导顺序并按 <Enter>。

在弹出窗口中，虚拟光盘驱动器和虚拟软盘驱动器与标准引导设备列在一起。

4 确保虚拟驱动器已启用并作为第一个带有可引导介质的设备列出。如果需要，请遵循屏幕上的说明修改引导顺序。

5 保存更改并退出。

受管服务器重新引导。

受管服务器将会根据引导顺序尝试从可引导设备引导。如果虚拟设备已连接并且有可引导介质，系统会引导至该虚拟设备。否则，系统会忽略此设备，就像没有可引导介质的物理设备。

使用虚拟介质安装操作系统

本节说明在 Management Station 上安装操作系统的手动交互方法，可能需要数小时来完成。使用**虚拟介质**的脚本化操作系统安装过程可能需要不到 15 分钟来完成。有关详情，请参阅第 219 页上的 “部署操作系统”。

1. 验证以下内容：
   - 操作系统安装 CD 插入到 Management Station 的 CD 驱动器中。
   - 选择了本地 CD 驱动器。
   - 已与虚拟驱动器连接。
2. 按照第 236 页上的 “从虚拟介质引导”一节中的步骤从虚拟介质引导以确保 BIOS 已设置为从进行安装的 CD 驱动器引导。
3. 按照屏幕上的说明完成安装。

多磁盘的安装请务必遵循以下步骤：

1. 从虚拟介质控制台取消映射虚拟化 （重定向）的 CD/DVD。
2. 将下一张 CD/DVD 插入到远程光盘驱动器中。
3. 从虚拟介质控制台映射 （重定向）此 CD/DVD。

   将新 CD/DVD 插入到远程光盘驱动器中而不重新映射可能会无法正常运行。

引导一次功能

引导一次功能有助于临时更改引导次序以便从远程虚拟介质设备引导。通常在安装操作系统时，可以结合使用此功能和虚拟介质。

注：必须有 “Configure iDRAC6”（配置 iDRAC6）权限才能使用此功能。

注：必须使用虚拟介质重定向远程设备才能使用此功能。

要使用 “Boot Once”（引导一次）功能，应执行以下操作：

1. 通过 Web 界面登录到 iDRAC6，单击 “System”（系统） → “Console/Media”（控制台 / 介质） → “Configuration”（配置）。
2. 选择**虚拟介质**下的 “Enable Boot Once ”（启用引导一次）选项。
3. 打开服务器电源并进入 BIOS 引导管理器。
4. 将引导顺序更改为从远程虚拟介质设备引导。
5. 对服务器执行关机后再开机操作。

   服务器从远程虚拟介质设备引导。服务器下次重新引导时，将断开远程虚拟介质连接。

注：虚拟介质应处在 “Attached”（已附加）状态，虚拟驱动器才能显示在引导顺序中。确保可引导介质存在于虚拟驱动器中以启用 “Boot Once”（引导一次）。

服务器的操作系统运行时使用虚拟介质

基于 Windows 的系统

在 Windows 系统上，虚拟介质驱动器已自动安装 （如果已连接）并配置有驱动器号。

在 Windows 中使用虚拟驱动器类似于使用物理驱动器。使用虚拟介质向导连接到介质后，只需单击该驱动器并浏览其内容就可在系统上使用该介质。

基于 Linux 的系统

根据系统上软件的配置，虚拟介质驱动器可能不自动安装。如果驱动器没有自动安装，则使用 Linux **mount** 命令手动安装驱动器。

关于虚拟介质的常见问题

表 14-3 列出常见问题和解答。

表 14-3. 使用虚拟介质：常见问题

问题	解答
有时会发现虚拟介质客户端连接中断。为什么？	出现网络超时后， iDRAC6 固件会断开连接，断开服务器和虚拟驱动器之间的链接。 如果虚拟介质配置设置在 iDRAC6 基于 Web 界面中或使用本地 RACADM 命令更改，当配置更改应用后，任何连接的介质都会断开连接。 要重新连接虚拟驱动器，使用虚拟介质向导。
哪些操作系统支持 iDRAC6？	请参阅第 24 页上的 “支持的操作系统”查看所支持操作系统的列表。
哪些 Web 浏览器支持 iDRAC6？	请参阅第 24 页上的 “支持的 Web 浏览器”查看所支持 Web 浏览器的列表。

表 14-3. 使用虚拟介质：常见问题 *（续）*

问题	解答
为什么有时丢失客户端连接？	• 如果网络缓慢或更改客户端系统 CD 驱动器中的 CD，有时可能丢失客户端连接。例如，如果更换客户端系统的 CD 驱动器中的 CD，则新 CD 可能具有自动开始功能。在这种情况下，如果客户端系统准备读取 CD 前花了过多时间，固件可能超时，连接可能丢失。如果连接丢失，请从 GUI 重新连接并继续之前的操作。 • 出现网络超时后，iDRAC6 固件会断开连接，断开服务器和虚拟驱动器之间的链接。另外，有些人会在 Web 界面或输入 RADACM 命令变更虚拟介质配置设置。要重新连接虚拟驱动器，使用**虚拟介质**功能。
通过虚拟介质安装 Windows 操作系统所用时间似乎太长了。为什么？	如果使用 *Dell Systems Management Tools and Documentation* DVD 和慢速网络连接安装 Windows 操作系统，安装过程可能会由于网络延迟而需要更多的时间访问 iDRAC6 Web 界面。虽然安装窗口没有显示安装进程，安装仍在进行。
如何将虚拟设备配置为可引导设备？	在受管服务器上，访问 BIOS 设置并单击引导菜单。找到虚拟 CD、虚拟软盘或 vFlash 并根据需要更改设备引导顺序。另外，通过在 CMOS 设置的引导顺序中按 “空格” 键使虚拟设备可以引导。例如，要从 CD 驱动器引导，将 CD 驱动器配置为引导顺序中的第一个驱动器。
我可以从何种介质引导？	iDRAC6 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

表 14-3. 使用虚拟介质：常见问题 *（续）*

问题	解答
如何使 USB 闪存盘可引导？	搜索 **support.dell.com** 寻找 Dell 引导公用程序，这是一种可以使 Dell USB 闪存盘可引导的 Windows 程序。 还可以使用 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，从 DOS 提示符处键入以下命令： `sys a: x: /s` 其中 *x* 是要使其可引导的 USB 闪存盘。

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。已附加虚拟介质并且也已经连接到远程软盘。我应该怎么做？	有些 Linux 版本不会以相同的方式自动安装虚拟软盘驱动器和虚拟 CD 驱动器。为了安装虚拟软盘驱动器，找到 Linux 分配给虚拟软盘驱动器的设备节点。执行下列步骤正确查找并安装虚拟软盘驱动器：
	
	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`
	其中
	`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 Virtual Floppy 的设备名。
	
	5 确保已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` 是在第 4 步发现的设备名称
	`/mnt/floppy` 是安装点。

表 14-3. 使用虚拟介质：常见问题 *（续）*

问题	解答

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。已连接虚拟介质并且也已经连接到远程软盘。我应该怎么做？	*（解答 [续]）*
	为了安装虚拟 CD 驱动器，请找到 Linux 分配给虚拟 CD 驱动器的设备节点。执行以下步骤以找到并安装虚拟 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`
	其中
	`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 Virtual CD* 的设备名称。
	5 确保已连接到虚拟 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` 是在第 4 步发现的设备名称
	`/mnt/floppy` 是安装点。

当我使用 iDRAC6 Web 界面远程执行固件更新时，服务器上的虚拟驱动器已卸下。为什么？	固件更新造成 iDRAC6 重设，删除远程连接，并卸下虚拟驱动器。
在我连接了 USB 设备之后，所有的 USB 设备都分离了，为什么？	虚拟介质设备和 vFlash 设备都是作为组合 USB 设备连接到主机 USB 总线的，且它们共享同一个 USB 端口。每当任何虚拟介质或 vFlash USB 设备连接到主机 USB 总线或从该总线断开时，将从主机 USB 总线短暂地断开所有虚拟介质和 vFlash 设备，然后重新连接这些设备。如果某个虚拟介质设备正被主机操作系统使用，必须避免附加或分离一个或多个虚拟介质或 vFlash 设备。建议先连接所有必需 USB 设备，然后再使用这些设备。

表 14-3. 使用虚拟介质：常见问题 *（续）*

问题	解答
USB 重设按钮有什么用？	它可重设连接到服务器的远程 USB 设备和本地 USB 设备。
如何获得虚拟介质的最高性能？	要获得虚拟介质的最高性能，请在禁用了虚拟控制台时启动虚拟介质或执行以下一项操作： • 尽可能地降低虚拟控制台屏幕的视频分辨率和颜色深度。 • 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和虚拟控制台的 iDRAC 之间的数据传输不受保护。** • 如果使用的是任何 Windows 服务器操作系统，停止名称为 Windows Event Collector 的 Windows 服务。为此，转至 “**Start**”（开始）> “**Administrative Tools**”（管理工具）> “**Services**”（服务）。右键单击 **Windows Event Collector** 并单击 “**Stop**”（停止）。

15

配置 vFlash SD 卡和管理 vFlash 分区

vFlash SD 卡是一种安全数字 (SD) 卡，可插入系统背面的可选 iDRAC6 Enterprise 卡插槽中。它提供像普通 USB 闪存盘设备一样的存储空间。它是用户定义分区的存储位置，可配置为向系统显示为 USB 设备，还可以用于创建可引导 USB 设备。分区将向系统公开为软盘驱动器和硬盘驱动器或 CD/DVD 驱动器，具体视选定的仿真模式而定。可以将任何这些驱动器设置为可引导设备。

有关如何安装和从系统拆下卡的信息，请参阅 **dell.com/support/manuals** 上系统的 《硬件用户手册》。

支持 vFlash SD 卡和标准 SD 卡。*vFlash SD 卡*是指支持新的增强 vFlash 功能的卡。*标准 SD 卡*是指仅支持有限的 vFlash 功能的普通现成 SD 卡。

使用 vFlash SD 卡时，最多可以创建 16 个分区。创建分区时，可以为该分区提供卷标名称，可以执行一系列操作来管理和使用分区。 vFlash SD 卡的大小可以是不超过 8GB 的任意大小。每个分区的大小最多是 4GB。

标准 SD 卡的大小可以是任意大小，但仅支持一个分区。分区大小限制为 256MB。默认情况下，分区的卷标名称是 VFLASH。

注：确保在 iDRAC6 Enterprise 卡插槽中仅插入 vFlash SD 卡或标准 SD 卡。如果插入任何其它格式的卡 （例如，多媒体卡 (MMC)），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 卡时出错）。

如果您是管理员，可以对 vFlash 分区执行所有操作。如果不是，则必须有 "Access Virtual Media"（访问虚拟介质）权限才能创建、删除、格式化、附加、分离或复制该分区的内容。

使用 iDRAC6 Web 界面配置 vFlash 或标准 SD 卡

安装 vFlash 或标准 SD 卡之后，可以查看其属性、启用或禁用 vFlash 和初始化该卡。必须启用 vFlash 功能才能执行分区管理。卡被禁用时，只能查看其属性。初始化操作可删除现有分区并将卡重设。

注：必须具有 "Configure iDRAC"（配置 iDRAC）权限才能启用或禁用 vFlash 或初始化该卡。

如果系统的 iDRAC6 Enterprise 卡插槽中没有该卡，将显示以下错误信息。SD card not detected（未检测到 SD 卡）。Please insert an SD card of size 256MB or greater（请插入 256MB 或更大的 SD 卡）。

要查看和配置 vFlash 或标准 SD 卡：

1 打开支持的 Web 浏览器窗口并登录 iDRAC6 Web 界面。

2 在系统树中选择 “System”（系统）。

3 单击 **vFlash** 选项卡。将显示 “**SD Card Properties**”（SD 卡属性）页。

表 15-1 列出为 SD 卡显示的属性。

表 15-1. SD 卡属性

属性	说明
Name （名称）	显示插入到服务器的 iDRAC6 Enterprise 卡插槽中的卡名称。如果该卡支持新的增强 vFlash 功能，将显示 *“vFlash SD Card ”*（vFlash SD 卡）。如果该卡支持有限的 vFlash 功能，将显示 *“SD Card ”*（SD 卡）。
大小	以千兆字节 (GB) 为单位显示卡的大小。
Available Space （总空间）	显示 vFlash SD 卡上的未使用空间 (MB)。可以使用此空间在 vFlash SD 卡上创建更多分区。 如果插入的 vFlash SD 卡未初始化，则可用空间显示该卡未初始化。 对于标准 SD 卡，不显示可用空间。
Write-protected （写保护）	显示该卡是否受写保护。
运行状况	显示 vFlash SD 卡的整体运行状况。运行状况可以是： • OK （正常） • 警告 • Critical （严重） 如果是警告，重新初始化该卡。 如果是严重，重新安装并重新初始化该卡。 对于标准 SD 卡，不显示运行状况。

表 15-1. SD 卡属性 *（续）*

属性	说明
“vFlash Enabled”（已启用 vFlash）	选择该复选框可对卡执行 vFlash 分区管理。取消选择该复选框可禁止 vFlash 分区管理。

4 单击 “Apply”（应用）可允许或禁止对卡执行 vFlash 分区管理。

如果附加了任何 vFlash 分区，则无法禁用 vFlash 并将显示错误信息。

注：如果禁用了 vFlash，仅显示 “SD Card Properties”（SD 卡属性）子选项卡。

5 单击 “Initialize”（初始化）。将删除所有现有分区并重设该卡。此时将显示一条确认消息。

6 单击 OK （确定）。初始化操作完成后，会显示成功信息。

注：仅当选择了 “vFlash Enabled”（已启用 vFlash）选项时，才会启用 “Initialize”（初始化）。

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。

如果在诸如 WSMAN 提供程序、iDRAC6 配置公用程序或 RACADM 等应用程序正使用 vFlash 时单击 vFlash 页上的任何选项，或者如果导航到 GUI 中的其它页， iDRAC6 可能会显示以下错误信息

“vFlash is currently in use by another process”（vFlash 当前正被另一个进程使用）。 Try again after some time （请稍后重试）。

使用 RACADM 配置 vFlash 或标准 SD 卡

可以从本地、远程或 Telnet/SSH 控制台使用 RACADM 命令查看和配置 vFlash 或标准 SD 卡。

注：必须具有 “Configure iDRAC”（配置 iDRAC）权限才能启用或禁用 vFlash 和初始化该卡。

显示 vFlash 或标准 SD 卡属性

打开到服务器的 Telnet/SSH/ 串行控制台，登录并输入以下命令：

```
racadm getconfig -g cfgvFlashSD
```

显示以下只读属性：

- `cfgvFlashSDSize`

- cfgvFlashSDLicense
- cfgvFlashSDAvailableSize
- cfgvFlashSDHealth

启用或禁用 vFlash 或标准 SD 卡

打开到服务器的 Telnet/SSH/ 串行控制台，登录并输入以下命令：

- 要启用 vFlash 或标准 SD 卡：

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable
  1
  ```

- 要禁用 vFlash 或标准 SD 卡：

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable
  0
  ```

注：RACADM 命令只有在 vFlash 或标准 SD 卡存在时才有用。如果没有卡，将会显示以下信息：*"ERROR: SD Card not present"*（错误：SD 卡不存在）。

初始化 vFlash 或标准 SD 卡

打开到服务器的 Telnet/SSH/ 串行控制台，登录并输入以下命令以初始化该卡：

```
racadm  vflashsd  initialize
```

将删除所有现有分区并重设该卡。

获取 vFlash 或标准 SD 卡的最新状况

打开到服务器的 Telnet/SSH/ 串行控制台，登录并输入以下命令以获取发送到 vFlash 或标准 SD 卡的最后一个初始化命令的状况：

```
racadm vFlashsd status
```

注：此命令仅显示发送到 SD 卡的命令的状况。要获取发送到 SD 卡上的各个分区的命令的状况，请使用以下命令：

```
racadm vflashpartition status
```

重设 vFlash 或标准 SD 卡

打开到服务器的 Telnet/SSH/ 串行控制台，登录并输入：

```
racadm vflashsd initialize
```

有关 `vflashsd` 的详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》。

注：从 1.5 版开始， `racadm vmkey reset` **命令已弃用。此命令的功能现在由** `vflashsd initialize` **提供。虽然执行** `vmkey reset` **命令将会成功，但建议使用** `vflashsd initialize` **命令。有关详情，请参阅第 246 页上的 “初始化 vFlash 或标准 SD 卡”。**

使用 iDRAC6 Web 界面管理 vFlash 分区

可以执行以下任务：

- 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 / 分离分区
- 删除现有分区
- 下载分区内容
- 引导至分区

创建空白分区

空白分区类似于空白 USB 闪存盘。可以在 vFlash 或标准 SD 卡上创建空白分区。可以选择创建类型为*软盘*或*硬盘*的分区。不支持使用分区类型 CD 创建空白分区。

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能创建空白分区。

在创建空白分区之前，确保符合以下条件：

- 卡已初始化。
- 卡没有受写保护。
- 尚未对卡执行初始化操作。

要创建空白 vFlash 分区：

1. 在 iDRAC6 Web 界面上，选择“System”（系统）→ vFlash 选项卡 → “Create Empty Partition”（创建空白分区）子选项卡。将会显示“Create Empty Partition”（创建空白分区）页。
2. 输入表 15-2 中所述的信息。
3. 单击“Apply”（应用）。将创建一个新分区。会显示一个说明进度百分比的页面。

   在以下情况下，将显示错误信息：

   - 卡受写保护。
   - 卷标名称与现有分区的卷标匹配。
   - 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 4GB。
   - 已经对卡执行初始化操作。

   注：新分区未格式化 (RAW)。

表 15-2. 创建空白分区页面选项

字段	说明
索引	选择分区索引。下拉列表中仅显示未使用的索引。默认情况下选中最小可用索引。可以从下拉列表中将其更改为任何其它索引值。 **注：对于标准 SD 卡，只有索引 1 可用。**
Label （卷标）	为新分区输入独特的卷标。卷标名称最多可以包含六个字母数字字符。在卷标名称中不要包括任何空格。字符以大写字体显示。 **注：对于标准 SD 卡，默认情况下卷标名称是 VFLASH，无法修改此名称。**
仿真 类型	从下拉列表中选择分区的仿真类型。可用选项是“Floppy”（软盘）和“Hard Disk”（硬盘）。

表 15-2. 创建空白分区页面选项 *（续）*

字段	说明
大小	输入以兆字节 (MB) 表示的分区大小。最大分区大小是 4GB，或小于或等于 vFlash SD 卡上的可用空间。 **注：**对于标准 SD 卡，分区大小是 256MB，无法更改。

使用映像文件创建分区

可以使用映像文件 （以 .img 或 .iso 格式提供）在 vFlash 或标准 SD 卡上创建新分区。可以创建类型为软盘、硬盘或 CD 的分区。

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能创建分区。

如果使用 .iso 映像文件 （对于 CD），将创建只读分区。如果使用 .img 映像文件 （对于软盘和硬盘），将创建读写分区。

新创建分区的大小等于映像文件大小。映像文件大小必须是：

- 小于或等于卡上的可用空间。
- 小于或等于 4GB。最大分区大小是 4GB。

使用 Web 界面时，可以上载到 vFlash SD 卡的映像大小在 32 位和 64 位浏览器 （Internet Explorer 和 FireFox）上最大都限制为 2GB。

使用 RACADM 和 WSMAN 界面时，可以上载到 vFlash SD 卡的映像大小最大为 4 GB。

对于标准 SD 卡，映像大小应小于或等于 256MB。

在使用映像文件创建分区之前，确保符合以下条件：

- 卡已初始化。
- 卡没有受写保护。
- 尚未对卡执行初始化操作。

注：在使用映像文件创建分区时，确保映像类型和仿真类型匹配。iDRAC 将映像仿真为指定的映像类型。上载的映像和仿真类型不匹配时，可能会出现问题。例如，如果分区是使用 ISO 映像创建的，并且仿真类型指定为 “Hard Disk”（硬盘），则 BIOS 无法从该映像引导。

要使用映像文件创建 vFlash 分区：

1 在 iDRAC6 Web 界面上，选择 “System”（系统） → vFlash 选项卡 → “Create From Image”（从映像创建）子选项卡。将显示 “Create Partition from Image File”（从映像文件创建分区）页。

2 输入表 15-3 中所述的信息。

3 单击 “Apply”（应用）。将创建一个新分区。

在以下情况下，将显示错误信息：

- 卡受写保护。
- 卷标名称与现有分区的卷标匹配。
- 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。
- 已经对卡执行初始化操作。

表 15-3. 使用映像文件页面选项创建分区

字段	说明
索引	选择分区索引。下拉列表中仅显示未使用的索引。默认情况下选中最小可用索引。可以从下拉列表中将其更改为任何其它索引值。 **注：对于标准 SD 卡，只有索引 1 可用。**
Label （卷标）	为新分区输入独特的卷标。卷标最多可以包含六个字母数字字符。在卷标名称中不要包括空格。字符以大写字体显示。 **注：对于标准 SD 卡，卷标名称是 VFLASH，无法修改。**
仿真 类型	从下拉列表中选择分区的仿真类型。可用选项是 “Floppy”（软盘）、“Hard Disk”（硬盘）和 CD。
映像位置	单击 “Browse”（浏览）并指定映像文件位置。仅支持 .img 或 .iso 文件类型。

格式化分区

可以根据文件系统类型格式化 vFlash SD 卡上的现有分区。支持的文件系统类型是 EXT2、EXT3、FAT16 和 FAT32。具有有限 vFlash 功能的标准 SD 卡仅支持 FAT32 格式。

只能格式化硬盘或软盘分区。不支持格式化类型为 CD 的分区。只读分区无法格式化。

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能格式化分区。

在格式化分区之前，确保符合以下条件：

- 卡已启用。
- 分区未附加。
- 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 iDRAC6 Web 界面上，选择 “System”（系统） → vFlash 选项卡 → “Format”（格式化）子选项卡。将会显示 “Format Partition”（格式化分区）页。

2 输入表 15-4 中所述的信息。

3 单击 “Apply”（应用）。将显示警告信息，表明分区中的所有数据将被清除。单击 OK （确定）。选定分区即格式化为指定的文件系统类型。

在以下情况下，将显示错误信息：

- 卡受写保护。
- 已经对卡执行初始化操作。

表 15-4. 格式化分区页面选项

字段	说明
Label （卷标）	选择要格式化的分区卷标。默认情况下选择第一个可用分区。 下拉列表中显示类型为软盘或硬盘的所有现有分区。下拉列表中不显示已附加或只读的分区。
Format Type （格式化类型）	选择要将分区格式化到的文件系统类型。可用选项有 EXT2、 EXT3、 FAT16 和 FAT32。

查看可用分区

确保 vFlash 或标准 SD 卡已启用以查看可用分区列表。

要查看卡上的可用分区：

1 在 iDRAC6 Web 界面上，选择 “System”（系统） → vFlash → “Manage”（管理）子选项卡。“Manage Partitions”（管理分区）页列出可用分区。

2 对于每个分区，可以查看表 15-5 中所述的信息。

表 15-5. 查看可用分区

字段	说明
索引	分区的索引从 1 到 16。分区索引对于特定分区是独特的。它是在创建分区时指定的。
Label （卷标）	标识分区。它是在创建分区时指定的。
大小	以兆字节 (MB) 为单位的分区大小。
Read-Only （只读）	分区的读写访问状态。 • 选中 = 只读分区。 • 取消选中 = 读写分区 **注：对于标准 SD 卡，分区是读写分区，此列不显示。**
Attached （已附加）	指明分区是否作为 USB 设备对操作系统可见。要附加或分离分区，请参阅第 253 页上的 “附加和分离分区”一节。
类型	显示分区类型是软盘、硬盘还是 CD。
状况	对分区正在执行或上一次执行的操作的状况，显示进度百分比。状况值为： • “Idle”（空闲） - 没有执行操作。 • “Formatting”（正在格式化） - 正在格式化分区。 • “Creating”（正在创建） - 正在创建分区。

修改分区

确保卡已启用以便修改分区。

可以将只读分区更改为读写分区，反之亦然。要执行此操作：

1 在 iDRAC6 Web 界面上，选择 “System”（系统） → vFlash 选项卡 → “Manage”（管理）子选项卡。将会显示 “Manage Partitions”（管理分区）页。

2 在 “Read-Only”（只读）列中，如果要将分区更改为只读，则选择分区的复选框，如果要将分区更改为读写，则取消选择分区的复选框。

注：如果分区的类型为 CD，则默认情况下状态为只读并选中了此复选框。无法将状态更改为读写。如果分区已附加，此复选框呈灰色显示。对于标准 SD 卡，分区是读写分区，“Read-Only”（只读）列不显示。

3 单击 “Apply”（应用）。分区根据所做的选择更改为只读或读写。

附加和分离分区

可以将一个或多个分区作为一个虚拟 USB 大容量存储设备附加，以便它们对操作系统和 BIOS 作为大容量存储设备呈现。同时附加多个分区时，将根据索引按升序向主机操作系统呈现这些分区。相应的驱动器号分配由操作系统控制。

如果分离分区，分区在主机操作系统中不再显示为虚拟 USB 大容量存储设备，而且该分区从 BIOS 引导顺序菜单中删除。

如果附加或分离分区，将重设系统的 USB 总线。这可能会影响正使用 vFlash 的任何应用程序 （例如操作系统），并将断开 iDRAC 虚拟介质会话的连接。

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能附加或分离分区。

在附加或分离分区之前，确保符合以下条件：

- 卡已启用。
- 尚未对卡执行初始化操作。

要附加或分离分区：

1. 在 iDRAC6 Web 界面上，选择 “System”（系统） → vFlash 选项卡 → “Manage”（管理）子选项卡。将会显示 “Manage Partitions”（管理分区）页。
2. 在 “Attached”（已附加）列中，如果要附加分区，则选择分区的复选框，如果要分离分区，则取消选择分区的复选框。

   注：分离的分区不显示在引导顺序中。
3. 单击 “Apply”（应用）。分区根据所做的选择附加或分离。

已附加分区的操作系统行为

分区已附加并且主机操作系统是 Windows 时，分配给已附加分区的驱动器号由操作系统控制。

如果分区为只读，它将按主机操作系统中所示为只读。

如果主机操作系统不支持已附加分区的文件系统，则无法从主机操作系统读取或修改分区内容。例如，无法从 Windows 操作系统读取分区类型 EXT2。

从主机操作系统更改已附加分区的卷标名称时，不会影响 iDRAC 为该分区存储的卷标名称。

删除现有分区

注：可以删除 vFlash 或标准 SD 卡的现有分区。

在 删除现有分区之前，必须确保：

- 卡已启用。
- 卡没有受写保护。
- 分区未附加。
- 尚未对卡执行初始化操作。

要删除现有分区：

1. 在 iDRAC6 Web 界面上，选择 “System”（系统）→ vFlash 选项卡 → “Manage”（管理）子选项卡。将会显示 “Manage Partitions”（管理分区）页。
2. 在 “Delete”（删除）列中，单击要删除的分区的删除图标，然后单击 “Apply”（应用）。分区被删除。

下载分区内容

可以将 vFlash 分区的内容以 .img 或 .iso 格式的映像文件下载到本地或远程位置。本地位置是操作 iDRAC6 Web 界面所在的管理系统。远程位置是映射到 Management Station 的网络位置。

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能下载分区。

在将内容下载到本地或远程位置之前，确保符合以下条件：

- 卡已启用。
- 尚未对卡执行初始化操作。
- 读写分区不能附加。

要将 vFlash 分区的内容下载到系统上：

1. 在 iDRAC6 Web 界面上，选择 “System”（系统）→ vFlash 选项卡 → “Download”（下载）子选项卡。将会显示 “Download Partition”（下载分区）页。
2. 从 “Label”（卷标）下拉菜单中，选择要下载的分区。除已附加分区之外的所有现有分区都显示在列表中。默认情况下选择第一个分区。
3. 单击 “Download”（下载）。

4 指定保存文件的位置。

如果仅指定文件夹位置，则分区卷标用作文件名，扩展名为 .iso（CD 类型的分区）和 .img（软件和硬盘类型的分区）。

5 单击 Save（保存）。选定分区的内容下载到指定位置。

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。vFlash 分区必须含有可引导映像（格式为 .img 或 .iso），才能将其设置为引导设备。确保卡已启用以便将分区设置为引导设备和执行引导操作。

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能将分区设置为引导设备。

可以为 vFlash 或标准 SD 卡执行引导操作。有关步骤，请参阅第 71 页上的 ““First Boot Device”（第一个引导设备）”一节。

注：如果系统 BIOS 不支持 vFlash 用作第一个引导设备，则已附加的 vFlash 分区不在 “First Boot Device”（第一个引导设备）下拉菜单中列出。因此，确保将 BIOS 更新到支持将 vFlash 分区设置为第一个引导设备的最新版本。如果 BIOS 是最新版本，则重新引导服务器将导致 BIOS 通知 iDRAC 它支持 vFlash 用作第一个引导设备，iDRAC 在 “First Boot Device”（第一个引导设备）下拉菜单中列出 vFlash 分区。

使用 RACADM 管理 vFlash 分区

可以使用 `vFlashPartition` 子命令在已经初始化的 vFlash 或标准 SD 卡上创建、删除、列出或查看分区状况。格式为：

```
racadm vflashpartition <create | delete | status |
list> < 选项 >
```

注：必须具有 “Access Virtual Media”（访问虚拟介质）权限才能执行 vFlash 分区管理。

有效选项：

-i < 索引 >	此命令适用的分区的索引。 < 索引 > 必须是从 1 到 16 的整数。 **注：**对于标准 SD 卡，索引值限制为 1，因为仅支持一个大小为 256MB 的分区。

仅对 create 操作有效的选项：

-o < 卷标 >	分区安装在操作系统上时显示的卷标。 < 卷标 > 必须是最多含有六个字母数字字符的字符串，不能包含空格。
-e < 类型 >	分区的仿真类型。 < 类型 > 必须是软盘、 cddvd 或 HDD。
-t < 类型 >	创建类型为 < 类型 > 的分区。 < 类型 > 必须是： • empty - 创建空白分区。 • -s < 大小 > - 以 MB 为单位的分区大小。 • -f < 类型 >- 根据文件系统类型的分区格式化类型。有效选项为 RAW、 FAT16、 FAT32、 EXT2 或 EXT3。 • image - 使用相对于 iDRAC 的映像创建分区。以下选项对于映像类型有效： • -l < 路径 > - 指定相对应 iDRAC 的远程路径。路径可以位于安装的驱动器上： SMB 路径：//<IP 地址或域 >/< 共享名称 > /< 映像路径 > NFS 路径：<IP 地址 >:/< 映像路径 > • -u < 用户 > - 用于访问远程映像的用户名。 • -p < 密码 > - 用于访问远程映像的密码。

仅对 status 操作有效的选项：

-a	显示对所有现有分区的操作的状况。

创建分区

- 要创建 20MB 空白分区：

```
racadm vflashpartition create -i 1 -o drive1 -t
empty -e HDD -f fat16 -s 20
```

- 要使用远程系统上的映像文件创建分区：

```
racadm vflashpartition create -i 1 -o drive1 -e
HDD -t image -l //myserver/sharedfolder/foo.iso
-u root -p mypassword
```

注：此命令要区分映像文件扩展名的大小写。如果文件扩展名为大写，例如为 FOO.ISO 而不是 FOO.iso，则命令会返回语法错误。

注：在本地 RACADM 中不支持使用映像文件创建分区。

删除分区

- 要删除分区：

  ```
  racadm vflashpartition delete -i 1
  ```

- 要删除所有分区，请重新初始化 vFlash SD 卡。有关详情，请参阅第 246 页上的 “初始化 vFlash 或标准 SD 卡”。

获取分区状况

- 要获取对分区 1 的操作的状况：

  ```
  racadm vflashpartition status -i 1
  ```

- 要获取所有现有分区的状况：

  ```
  racadm vflashpartition status -a
  ```

查看分区信息

要列出所有现有分区及其属性：

```
racadm vflashpartition list
```

引导至分区

- 要在引导列表中列出可用设备：

  ```
  racadm  getconfig  -g cfgServerInfo  -o
  cfgServerFirstBootDevice
  ```

  如果是 vFlash SD 卡，已附加分区的卷标名称将出现在引导列表中。如果是标准 SD 卡并且分区已附加，则 VFLASH 出现在引导列表中。

- 要将 vFlash 分区设置为引导设备：

  ```
  racadm  config  -g cfgServerInfo  -o
  cfgServerFirstBootDevice  “<vFlash 分区名称 >”
  ```

  其中， <vFlash 分区名称 > 是 vFlash SD 卡的卷标名称， VFLASH 是标准 SD 卡的卷标名称。

  注：运行此命令时， vFlash 分区卷标自动设置为引导一次，即 cfgserverBootOnce 设置为 1。引导一次操作仅将设备引导至分区一次，而且不将它永久保留在引导顺序的第一位。

附加或分离分区

- 要附加分区：

```
racadm config -g cfgvflashpartition -i 1 -o
cfgvflashPartitionAttachState 1
```

- 要分离分区：

```
racadm config -g cfgvflashpartition -i 1 -o
cfgvflashPartitionAttachState 0
```

修改分区

- 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
```

有关 RACADM 子命令和 iDRAC6 属性数据库组和对象定义的详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》。

常见问题

vFlash 或标准 SD 卡何时锁定?

当 iDRAC 执行的操作需要介质的独占访问时， iDRAC 就锁定虚拟闪速更新介质。例如，在初始化操作过程中。

16

电源监控和管理

Dell PowerEdge 系统整合了众多全新和增强的电源管理功能。整个平台（从硬件到固件再到系统管理软件）的设计均以电源效率、电源监控和电源管理为重点。

从电源角度上看，基础硬件设计已优化：

- 高效电源设备和稳压器已整合到设计当中。
- 如适用，选用最低的电源组件。
- 机箱设计已通过系统优化空气流通，从而将风扇的功率降至最低。

PowerEdge 系统提供各种功能，以控制和管理电源：

- **"Power Inventory and Budgeting"（电源资源清册和预算）**：在引导时，系统资源清册允许计算当前配置的系统电源预算。
- **"Power Capping"（功率封顶）**：可对系统进行节流，以维持指定的功率限额。
- **"Power Monitoring"（电源监控）**：iDRAC6 对电源设备进行状况轮询，以收集功率测量数据。iDRAC6 采集功率测量历史记录并计算运行平均值、峰值等。您可使用 iDRAC6 基于 Web 的界面在 **"Power Monitoring"**（电源监控）页上查看信息。

电源资源清册、电源预算和封顶

从使用的角度上看，机架层上的冷却数量可能有限。通过用户定义的功率限额，可以随心分配所需的功率，从而满足您的性能需求。

iDRAC6 监控功耗并动态调节处理器，从而满足您定义的功率限额水平，在满足功率需求的同时尽量提高性能。

电源监控

iDRAC6 会连续监控 PowerEdge 服务器的功耗。 iDRAC6 会计算以下功率值并通过其基于 Web 的界面或 RACADM CLI 提供信息：

- 累计功率
- 平均、最小和最大功率
- 功率余量值
- 功耗 （也在基于 Web 的界面中以图形形式显示）

配置和管理电源

您可使用 iDRAC6 基于 Web 的界面和 RACADM 命令行界面 (CLI) 在 PowerEdge 系统上管理和配置电源控制。具体说来，可以：

- 查看服务器的电源状况
- 在服务器上执行电源控制操作 （例如打开电源、关闭电源、系统重设、关机后再开机）
- 查看服务器和已安装电源设备的电源预算信息，例如最小和最大潜在功耗
- 查看和配置服务器的电源预算阈值

查看电源设备的运行状况

"Power Supplies"（电源设备）页显示服务器上所安装电源设备的状况和额定值。

使用基于 Web 的界面

要查看电源设备的运行状况：

1. 登录到 iDRAC6 基于 Web 的界面。
2. 选择系统树中的 **"Power Supplies"**（电源设备）。**"Power Supplies"**（电源设备）页显示和提供下列信息：
   - **"Power Supplies Redundancy Status"（电源设备冗余状况）**：可能值为：
     - **"Full"（完全）**：系统中安装的电源设备的类型相同，且均正常工作。

– **"Lost"（掉失）**：在安装了两台电源设备的系统中，系统中安装的电源设备属于不同类型或其中一台设备出现故障或被拆下。在安装了四台电源设备的系统中，系统中安装的电源设备属于不同类型或其中两台或三台设备出现故障或被拆下。

– **"Disabled"（已禁用）**：各电源设备中只有一台可供使用。不存在冗余情况。

– **"Degraded"（降级）**（仅限于安装了四台电源设备的系统中）：系统中安装了四台电源设备，但其中一台设备出现故障或被拆下。

• **"Individual Power Supply Elements"（各个电源设备组件）**可能值为：

– **"Status"（状况）**显示如下：

  • **"OK"**（良好）表示电源设备存在且正在与服务器通信。

  • **"Warning"**（警告）表示只发出警告警报并且必须由管理员采取纠正措施。如果没有采取纠正措施，将可能发生影响服务器完整性的严重电源故障。

  • **"Severe"**（严重）表示已至少发出一个故障警报。故障状况表示服务器上发生电源故障，必须立即采取纠正措施。

– **"Location"**（位置）显示电源设备名称：PS-n，其中 n 为电源设备编号。

– **"Type"**（类型）显示电源设备的类型，例如交流或直流 （交流至直流或直流至直流电压转换）。

– **"Input Wattage"**（输入功率）显示电源设备的输入功率，其为系统可放置在数据中心的最大交流电源负载。

– **"Max Wattage"**（最大功率）显示电源设备的最大功率，这是系统可用的直流电源。此值用于确定电源设备容量足以供系统配置使用。

– **"Online Status"**（联机状况）表示电源设备的电源状态：存在和良好、输入掉失、不存在或预测故障。

– **"FW Version"**（固件版本）显示电源设备的固件版本。

注：由于电源设备具有一定的效率，**最大功率**与**输入功率**存在差额。例如，如果电源设备的效率为 89%，**最大功率**为 717W，则**输入功率**估计为 797W。

使用 RACADM

打开到 iDRAC 的 Telnet/SSH 文本控制台，登录并键入：

```
racadm getconfig -g cfgServerPower
```

查看电源预算

服务器在 **"Power Budget Information"**（电源预算信息）页上提供电源子系统的电源预算状况概览。

使用 Web 界面

注：要执行电源管理操作，您必须拥有 "Administrative"（管理）权限。

1. 登录到 iDRAC6 基于 Web 的界面。
2. 单击 Power （电源）选项卡。
3. 选择 **"Power Budget"**（电源预算）选项。
4. 将显示 **"Power Budget Information"**（电源预算信息）页。

第一张表中显示当前系统配置用户指定功率封顶阈值的最小和最大限制。这些表示您可设定作为系统上限的交流功耗的范围。一旦选中，此上限将是系统可放置在数据中心的最大交流电源负载。

"System Minimum Power Consumption"（系统最小功耗）显示默认最小功率限额值。

"System Maximum Power Consumption"（系统最大功耗）显示默认最大功率限额值。此值也是当前系统配置的绝对最大功耗。

使用 RACADM

打开到 iDRAC 的 Telnet/SSH 文本控制台，登录并键入：

```
racadm getconfig -g cfgServerPower
```

注：有关 cfgServerPower 的详情 （包括输出详情），请参阅 Dell 支持网站 dell.com/support/manuals 上 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 cfgServerPower。

电源预算阈值

如果启用电源预算阈值，则可设定系统的功率封顶限制。系统性能会被动态调整以保持功耗接近指定阈值。在性能调整完成之前，工作负载轻时实际功耗可能较低，且可能会短暂地超过阈值。

如果您选择电源预算阈值的 **"Enabled"**（已启用），系统将强制执行用户指定的阈值。如果您取消选择电源预算阈值，**系统不会达到**功率限额。例如，指定系统配置的最大潜在功耗为 700W，最小潜在功耗为 500W。您可指定和启用电源预算阈值，将其 650W 的电流功耗降低至 525W。自此，系统性能将被动态调整以保持功耗，从而不会超过用户指定 525W 的阈值。

使用基于 Web 的界面

1. 登录到 iDRAC6 基于 Web 的界面。
2. 单击 **Power**（电源）选项卡。
3. 选择 **"Power Budget"**（电源预算）选项。将显示 **"Power Budget Information"**（电源预算信息）页。
4. 在 **"Power Budget"**（电源预算）表中输入以瓦特、 BTU/ 小时或百分比为单位的值。您指定以瓦特或 BTU/ 小时为单位的值将为电源预算阈值限制值。如果您指定以百分比为单位的值，其将为最大至最小潜在功耗间隔的百分比。例如， 100% 阈值表示最大潜在功耗，而 0% 表示最小潜在功耗。

   注：电源预算阈值不得超过最大潜在功耗或低于最小潜在功耗。
5. 选择 **"Enabled"**（启用）可启用该阈值。系统会强制执行用户指定的阈值。如果取消选择此复选框，系统将不会实施功率限额。
6. 单击 **"Apply Changes"**（应用更改）。

使用 RACADM

```
racadm config -g cfgServerPower -o
cfgServerPowerCapWatts <功率限额瓦特值>

racadm config -g cfgServerPower -o
cfgServerPowerCapBTUhr <功率限额 BTU/ 小时值>

racadm config -g cfgServerPower -o
cfgServerPowerCapPercent <功率限额百分比值 >
```

```
racadm config -g cfgServerPower -o
cfgServerPowerCapEnable <1 表示启用， 0 表示禁用 >
```

注：如果将电源预算阈值设定以 BTU/ 小时为单位，转换成瓦特则舍入为最接近整数的值。重新读取电源预算阈值时，瓦特转换成 BTU/ 小时再次使用此方式舍入。因此，书写的值名义上是与读取的值不同，例如， 600 BTU/ 小时的阈值将转回为 601 BTU/ 小时。

查看电源监控

使用 Web 界面

要查看电源监控数据：

1. 登录到 iDRAC6 Web 界面。
2. 选择系统树中的 **"Power Monitoring"**（电源监控）。将显示 **"Power Monitoring"**（电源监控）页。

以下各节介绍 **"Power Monitoring"**（电源监控）页上提供的信息：

电源监控

- **"Status"（状况）**：**"OK"**（良好）表示电源设备存在并正在与服务器通信，**"Warning"**（警告）表示已发出警告警报，**"Severe"**（严重）表示已发出故障警报。
- **"Probe Name"（探测器名称）**：系统板系统级别。此描述表明探测器在系统中按其位置受到监控。
- **"Reading"（读数）**：当前功耗，以瓦特 /BTU/ 小时表示。
- **"Warning Threshold"（警告阈值）**：显示系统运行建议的可接受功耗（以瓦特和 BTU/ 小时为单位）。功耗超过此值会产生警告事件。
- **"Failure Threshold"（故障阈值）**：显示系统运行所需的最高可接受功耗 （以瓦特和 BTU/ 小时为单位）。功耗超过此值会产生严重 / 故障事件。

安培

- **"Location"（位置）**：显示电源设备名称：PS-n，其中 n 为电源设备编号
- **"Reading"（读数）**：当前功耗，以安培表示

Power Tracking Statistics （功率跟踪统计数据）

- **"Energy Consumption"**（能耗）表示从电源输入端测量得到的服务器当前累积能耗。此值以千瓦时显示，且表示系统所用总能量的累计值。您可以使用 **"Reset"**（重设）按钮，重设此值。
- **"System Peak Power"**（系统峰值功率）指定自测量开始时间以来系统功率的最高 1 分钟平均值。您可以使用 **"Reset"**（重设）按钮，重设此值。
- **"System Peak Amperage"**（系统峰值安培）指定开始和高峰时段之间的峰值电流值。您可以使用 **"Reset"**（重设）按钮，重设此值。
- **"Measurement Start Time"**（测量开始时间）显示上次清除统计数据并开始新的测量周期时记录的日期和时间。对于 **"Energy Consumption"**（能耗），您可以使用 **"Reset"**（重设）按钮重设此值，但系统重设或出现故障操作时其将保持原值。对于 **"System Peak Power"**（系统峰值功率）和 **"System Peak Amperage"**（系统峰值安培），您可以使用 **"Reset"**（重设）按钮重设此值，但系统重设或出现故障操作时其将保持原值。
- **"Measurement Finish Time"**（测量完成时间）显示计算系统能耗时的当前日期和时间。**"Peak Time"**（峰值时间）显示出现峰值的时间。

注：功率跟踪统计数据在系统重设时保持不变，因此会反映开始和结束时间间隔内的所有活动。"Reset"（重设）按钮会将相应字段重设为零。在下一个表中，功耗数据在系统重设时不会保持不变，所以在这些时候会重设为零。显示的功率值是相应时间间隔（前一分钟、前一小时、昨天和上周）内的累计平均值。因为这里的开始到完成时间间隔可能与功率跟踪统计数据间隔不同，所以峰值功率值（最大峰值瓦数对最大功耗）可能有所不同。

Power Consumption （功耗）

- 显示系统在上一分钟、上一小时、昨天和上周的平均、最大和最小功耗。
- "Average Power Consumption"（平均功耗）：前一分钟、前一小时、昨天和上周内的平均值。
- "Max and Min Power Consumption"（最大功耗和最小功耗）：给定时间间隔内的实测最大和最小功耗。
- "Max and Min Power Time"（最大和最小功率时间）：出现最大和最小功耗时的时间。

“Headroom”（余量）

- **“System Instantaneous Headroom”**（系统瞬间余量）显示电源设备可用电源与系统当前功耗之间的差额。
- **“System Peak Headroom”**（系统峰值余量）显示电源设备可用电源与系统峰值功耗之间的差额。

“Show Graph”（显示图形）

单击 **“Show Graph”**（显示图形）可显示上一小时分别以瓦特和安培为单位的 iDRAC6 功率和电流消耗图形。用户可使用图形上所提供的下拉式菜单，选择查看上周的这些统计数据。

注：图上绘制的各数据点代表 5 分钟内读数的平均值。因此，这些图形可能无法反映功率或电流消耗中的短暂波动。

使用 RACADM

打开到 iDRAC 的 Telnet/SSH 文本控制台，登录并键入：

```
racadm getconfig -g cfgServerPower
```

有关 **cfgServerPower** 的详情 （包括输出详情），请参阅 Dell 支持网站 **dell.com/support/manuals** 上 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 **cfgServerPower**。

执行服务器电源控制操作

注：要执行电源管理操作，必须具有 “Chassis Control Administrator”（机箱控制管理员）权限。

iDRAC6 使您能够远程执行多个电源管理操作，如有序关机。

使用 Web 界面

1. 登录到 iDRAC6 Web 界面。
2. 单击 **Power** （电源）选项卡。随即出现 **Power Control** （电源控制）页。
3. 通过单击单选按钮选择以下**电源控制操作**中的一项：
   - **“Power On System”**（打开系统电源）可打开服务器电源 （相当于服务器电源关闭时按电源按钮）。如果系统电源已经打开，则该选项被禁用。

- **"Power Off System"**（关闭系统电源）可关闭服务器电源。如果系统电源已经关闭，则该选项被禁用。
- **"NMI (Non-Masking Interrupt)"**（NMI [非屏蔽中断]）生成一条 NMI 指令导致系统停机。
- **"Graceful Shutdown"**（正常关机）可关闭系统。

注：使用此选项执行正常关机之前，确保为操作系统配置了关机选项。如果没在操作系统上配置此选项就使用此选项，此选项将会重新引导 Managed System，而不是执行关机操作。

- **"Reset System"**（重设系统 [温引导]）可重设系统而不断电。如果系统电源已经关闭，则该选项被禁用。
- **"Power Cycle System"**（系统关机后再开机 [冷引导]）可将系统关机，然后重新引导系统。如果系统电源已经关闭，则该选项被禁用。

4 单击 **"Apply"**（应用）。会显示要求确认的对话框。

5 单击 **"OK"**（确定）执行您所选的电源管理操作 （例如，使系统重设）。

使用 RACADM

打开到服务器的 Telnet/SSH 文本控制台，登录并键入：

```
racadm serveraction < 操作 >
```

其中 < **操作** > 为开机、关机、关机后再开机、硬重设或电源状况。

17

使用 iDRAC6 配置公用程序

概览

iDRAC6 配置公用程序是一个引导前配置环境，允许您查看并设置 iDRAC6 和受管服务器的参数。具体说来，可以：

- 查看 iDRAC6 和主背板固件的固件版本号
- 启用或禁用 iDRAC6 局域网
- 启用或禁用 LAN 上 IPMI
- 配置 LAN 参数
- 启用或禁用 “Auto – Discovery”（自动查找）并配置预配置服务器
- 配置虚拟介质
- 配置智能卡
- 更改管理用户名和密码
- 重设 iDRAC6 配置为工厂默认值
- 查看系统事件日志 (SEL) 信息或从日志清除信息
- 配置 LCD
- 配置系统服务

使用 iDRAC6 配置公用程序执行的任务也可以通过 iDRAC6 或 Dell OpenManage 软件提供的其它公用程序执行，其中包括基于 Web 的界面、 SM-CLP 命令行界面以及本地和远程 RACADM 命令行界面。

启动 iDRAC6 配置公用程序

1. 通过按服务器正面的电源按钮打开或重新启动服务器。
2. 如果看到 **“Press <Ctrl-E> for Remote Access Setup within 5 sec.....”**（在 5 秒内按 <Ctrl-E> 进行远程访问设置 .....）信息，应立即按 **<Ctrl><E>**。

注：如果操作系统在您按 <Ctrl><E> 前开始载入，应让系统完成引导，然后重新启动服务器并重试。

将显示 **iDRAC6 配置公用程序**窗口。前两行提供了有关 iDRAC6 固件和主背板固件版本的信息。在确定是否需要升级固件时，版本级别很有用。

iDRAC6 固件是信息中与外部界面 （比如基于 Web 的界面、 SM-CLP 和 Web 界面）相关的部分。主背板固件是固件中与服务器硬件环境交互并监测服务器硬件环境的部分。

使用 iDRAC6 配置公用程序

在固件版本信息下面， iDRAC6 配置公用程序的其余部分是可以用 < 上箭头 > 和 < 下箭头 > 访问的菜单项。

- 如果菜单项引出子菜单或可编辑文本字段，应按 <Enter> 访问项目，在完成配置后按 <Esc> 离开。
- 如果项目具有可选值，比如 “Yes”（是） / “No”（否）或 “Enabled”（已启用） / “Disabled”（已禁用），则按 < 左箭头 >、< 右箭头 > 或 < 空格键 > 选择一个值。
- 如果项目不可编辑，会呈蓝色显示。有些项目会根据所做的其它选择而变得可编辑。
- 屏幕底部显示当前项目的说明。可以按 <F1> 显示当前项目的帮助。
- 使用 iDRAC6 配置公用程序完成后，按 <Esc> 查看退出菜单，可以在这里选择保存或放弃更改或返回公用程序。

以下各节说明了 iDRAC6 配置公用程序的菜单项。

iDRAC6 LAN

使用 < 左箭头 >、 < 右箭头 > 和空格键可以选择 **“On”**（开）和 **“Off”**（关）。

在默认配置中， iDRAC6 LAN 处于启用状态。必须启用 LAN 才能允许使用 iDRAC6 功能，比如基于 Web 的界面、 Telnet/SSH、虚拟控制台和虚拟介质。

如果选择禁用 LAN，以下警告将会显示：

“iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF.”（如果 LAN 信道关闭，iDRAC6 带外界面将会禁用。）

Press any key to clear the message and continue.（按任意键清除信息并继续。）

该信息告诉您，在禁用 LAN 时，除了通过直接连接到 iDRAC6 HTTP、HTTPS、 Telnet 或 SSH 端口访问的功能外，并不接收带外管理网络通信，比如从 Management Station 发送到 iDRAC6 的 IPMI 信息。本地 RACADM 接口仍然可用，可用来重新配置 iDRAC6 LAN。

IPMI Over LAN （LAN 上 IPMI）

按 < 左箭头 >、 < 右箭头 > 和空格键选择 **"On"**（开）和 **"Off"**（关）。如果选中 **"Off"**（关）， iDRAC6 将不会接收通过 LAN 接口抵达的 IPMI 信息。

如果选择 **"Off"**（关），以下警告将会显示：

"iDRAC6 Out-of-Band IPMI interface will be disabled if IPMI Over LAN is OFF."（如果 LAN 上 IPMI 关闭，iDRAC6 带外 IPMI 接口将会禁用。）

Press any key to clear the message and continue.（按任意键清除信息并继续。）请参阅第 270 页上的 "iDRAC6 LAN" 了解该信息的解释。

LAN Parameters （LAN 参数）

按 <Enter> 可以显示 "LAN Parameters"（LAN 参数）子菜单。配置完 LAN 参数后，按 <Esc> 返回上一个菜单。

表 17-1. LAN Parameters （LAN 参数）

项	说明
常见设置	
NIC 选择	按 < 右箭头 >、 < 左箭头 > 和空格键，在模式之间切换。 可用模式包括 **"Dedicated"**（专用）、**"Shared"**（共享）、**"Shared with Failover LOM2"**（与故障转移 LOM2 共享）以及 **"Shared with Failover All LOMs"**（与故障转移所有 LOM 共享）。 这些模式允许 iDRAC6 使用对应接口与外界通信。
"MAC Address"（MAC 地址）	这是 iDRAC6 网络接口的不可编辑 MAC 地址。
VLAN Enable（VLAN 启用）	选择 **"On"**（开），为 iDRAC6 启用虚拟 LAN 筛选。
VLAN ID	如果 **"VLAN Enable"**（VLAN 启用）设置为 **"On"**（开），输入 1-4094 的任意 VLAN ID 值。

表 17-1. LAN Parameters （LAN 参数） *（续）*

项	说明
“VLAN Priority”（VLAN 优先级）	如果 **“VLAN Enable”**（VLAN 启用）设置为 **“On”**（开），选择 0-7 的 VLAN 优先级。
“Register iDRAC6 Name”（注册 iDRAC6 名称）	选择 **On**（开）可在 DNS 服务中注册 iDRAC6 名称。如果不想用户能够在 DNS 中查找 iDRAC6 名称，则选择 **“Off”**（关）。
“iDRAC6 Name”（iDRAC6 名称）	如果 **“Register iDRAC Name”**（注册 iDRAC 名称）设置为 **“On”**（开），按 <Enter> 可以编辑 **“Current DNS iDRAC Name”**（当前 DNS iDRAC 名称）文本字段。完成编辑 iDRAC6 名称后按 <Enter>。按 <Esc> 返回上一个菜单。 iDRAC6 名称必须是有效的 DNS 主机名。
Domain Name from DHCP（从 DHCP 获取域名）	如果想从网络上的 DHCP 服务获取域名，则选择 **“On”**（开）。如果想指定域名，则选择 **“Off”**（关）。
Domain Name（域名）	如果 **“Domain Name from DHCP”**（从 DHCP 获取域名）设置为 **“Off”**（关），则按 <Enter> 可以编辑 **“Current Domain Name”**（当前域名）文本字段。完成编辑后按 <Enter>。按 <Esc> 返回上一个菜单。域名必须是有效 DNS 域，例如 `mycompany.com`。
Host Name String（主机名字符串）	按 <Enter> 可以编辑。为平台事件陷阱 (PET) 警报输入主机名。
LAN Alert Enabled（LAN 警报已启用）	选择 **“On”**（开），可以启用 PET LAN 警报。
Alert Policy Entry 1（警报策略条目 1）	选择 **“Enable”**（启用）或 **“Disable”**（禁用），可以激活第一个警报目标。
Alert Destination 1（警报目标 1）	如果 **“LAN Alert Enabled”**（LAN 警报已启用）设置为 **“On”**（开），输入要转发 PET LAN 警报到的 IP 地址。
IPv4 设置	启用或禁用对 IPv4 连接的支持。
IPv4	选择 **“Enabled”**（已启用）或 **“Disabled”**（已禁用）IPv4 协议支持。
RMCP+ Encryption Key（RMCP+ 密钥）	按 <Enter> 可以编辑值，完成后按 <Esc>。 RMCP+ 密钥是一个 40 字符的十六进制字符串（字符 0-9、a-f 和 A-F）。RMCP+ 是一种 IPMI 扩展，为 IPMI 添加了验证和加密功能。默认值为包含 40 个 0（零）的字符串。

表 17-1. LAN Parameters （LAN 参数） *（续）*

项	说明
IP 地址源	选择 **DHCP** 或 **"Static"**（静态）。如果选择 DHCP，则 **"Ethernet IP Address"**（以太网 IP 地址）、**"Subnet Mask"**（子网掩码）和 **"Default Gateway"**（默认网关）字段均从 DHCP 服务器获得。如果在网络上没有找到 DHCP 服务器，这些字段将会设置为零。 如果选择 **"Static"**（静态），**"Ethernet IP Address"**（以太网 IP 地址）、**"Subnet Mask"**（子网掩码）和 **"Default Gateway"**（默认网关）项目都会变为可编辑。
Ethernet IP Address（以太网 IP 地址）	如果 **"IP Address Source"**（IP 地址源）设置为 **DHCP**，此字段将会显示从 DHCP 获得的 IP 地址。 如果 **"IP Address Source"**（IP 地址源）设置为 **"Static"**（静态），则输入想分配给 iDRAC6 的 IP 地址。 默认值为 **192.168.0.120**。
子网掩码	如果 **"IP Address Source"**（IP 地址源）设置为 **DHCP**，此字段将会显示从 DHCP 获得的子网掩码。 如果 **"IP Address Source"**（IP 地址源）设置为 **"Static"**（静态），则输入 iDRAC6 的子网掩码。默认为 **255.255.255.0**。
默认网关	如果 **"IP Address Source"**（IP 地址源）设置为 **DHCP**，此字段将会显示从 DHCP 获得的默认网关 IP 地址。 如果 **"IP Address Source"**（IP 地址源）设置为 **"Static"**（静态），则输入默认网关的 IP 地址。默认值为 **192.168.0.1**。
DNS Servers from DHCP（从 DHCP 获得 DNS 服务器）	选择 **"On"**（开）可从网络上的 DHCP 服务检索 DNS 服务器地址。选择 **"Off"**（关）可指定以下 DNS 服务器地址。
DNS Server 1（DNS 服务器 1）	如果 **"DNS Servers from DHCP"**（从 DHCP 获得 DNS 服务器）为 **"Off"**（关），则输入第一个 DNS 服务器的 IP 地址。
DNS Server 2（DNS 服务器 2）	如果 **"DNS Servers from DHCP"**（从 DHCP 获得 DNS 服务器）为 **"Off"**（关），则输入第二个 DNS 服务器的 IP 地址。

表 17-1. LAN Parameters （LAN 参数） *（续）*

项	说明
IPv6 设置	启用或禁用对 IPv6 连接的支持。
IP 地址源	选择 **“AutoConfig”**（自动配置）或 **“Static”**（静态）。当选择 **“AutoConfig”**（自动配置）后，会从 DHCP 获取 **“IPv6 Address 1”**（IPv6 地址 1）、**“Prefix Length”**（前缀长度）和 **“Default Gateway”**（默认网关）字段。 当选择 **“Static”**（静态）后，**“IPv6 Address 1”**（IPv6 地址 1）、**“Prefix Length”**（前缀长度）和 **“Default Gateway”**（默认网关）都会变成可编辑项。
IPv6 地址 1	如果 **“IP Address Source”**（IP 地址源）设置为 **“AutoConfig”**（自动配置），此字段将会显示从 DHCP 获得的 IP 地址。 如果 **“IP Address Source”**（IP 地址源）设置为 **“Static”**（静态），则输入想分配给 iDRAC6 的 IP 地址。
前缀长度	配置 IPv6 地址的前缀长度。可以是 1 到 128 之间 （含）的值。
默认网关	如果 **“IP Address Source”**（IP 地址源）设置为 **“AutoConfig”**（自动配置），此字段将会显示从 DHCP 获得的默认网关的 IP 地址。 如果 **“IP Address Source”**（IP 地址源）设置为 **“Static”**（静态），则输入默认网关的 IP 地址。
“IPv6 Link-local Address”（IPv6 链路本地地址）	这是 iDRAC6 网络接口的不可编辑的 **IPv6 链路本地地址**。
IPv6 地址 2	这是 iDRAC6 网络接口的不可编辑的 **IPv6 地址 2**。
DNS Servers from DHCP （从 DHCP 获得 DNS 服务器）	选择 **“On”**（开）可从网络上的 DHCP 服务检索 DNS 服务器地址。选择 **“Off”**（关）可指定以下 DNS 服务器地址。
DNS Server 1 （DNS 服务器 1）	如果 **“DNS Servers from DHCP”**（从 DHCP 获得 DNS 服务器）为 **“Off”**（关），则输入第一个 DNS 服务器的 IP 地址。
DNS Server 2 （DNS 服务器 2）	如果 **“DNS Servers from DHCP”**（从 DHCP 获得 DNS 服务器）为 **“Off”**（关），则输入第一个 DNS 服务器的 IP 地址。

表 17-1. LAN Parameters （LAN 参数） *（续）*

项	说明
高级 LAN 配置	
Auto-Negotiate（自动协商）	如果 **"NIC Selection"**（NIC 选择）设置为 **"Dedicated"**（专用），请选择 **"Enabled"**（已启用）或 **"Disabled"**（已禁用）。 当选择 **"Enabled"**（已启用）时，将自动配置 **"LAN Speed Setting"**（LAN 速度设置）和 **"LAN Duplex Setting"**（LAN 双工设置）。
LAN Speed Setting（LAN 速度设置）	如果 **"Auto-Negotiate"**（自动协商）设置为 **"Disabled"**（已禁用），请选择 10 Mbps 或 100 Mbps。
LAN Duplex Setting （LAN 双工设置）	如果 **"Auto-Negotiate"**（自动协商）设置为 **"Disabled"**（已禁用），请选择 **"Half Duplex"**（半双工）**或 "Full Duplex"**（全双工）。

"Virtual Media Configuration"（虚拟介质配置）

虚拟介质

按 <Enter>，选择 **"Detached"**（分离）、**"Attached"**（附加）或 **"Auto-Attached"**（自动附加）。如果选择 **"Attached"**（附加），虚拟介质设备会附加到 USB 总线，从而可以在**虚拟控制台**会话期间使用。

如果选择 **"Detached"**（分离），用户将不能在**虚拟控制台**会话期间访问虚拟介质设备。

注：要使用具有 "Virtual Media"（虚拟介质）功能的 USB 快擦写驱动器，必须在 BIOS 设置公用程序中将 "USB Flash Drive Emulation Type"（USB 快擦写驱动器仿真类型）设置为 "Hard disk"（硬盘）。在服务器启动期间按 <F2> 可访问 BIOS 设置公用程序。如果 "USB Flash Drive Emulation Type"（USB 快擦写驱动器仿真类型）设置为 "Auto"（自动），快擦写驱动器将显示为系统软盘驱动器。

vFlash

按 <Enter>，选择 **"Enabled"**（已启用）或 **"Disabled"**（已禁用）。

- **"Enabled"（已启用）** - vFlash 可用于分区管理。
- **"Disabled"（已禁用）** - vFlash 不可用于分区管理。

警告：如果一个或多个分区正在使用或已附加，则 vFlash 无法禁用。

初始化 vFlash

选择此选项可初始化 vFlash 卡。初始化操作将擦除 SD 卡上的现有数据，而且会删除所有现有分区。如果一个或多个分区正在使用或已附加，则无法执行初始化操作。只有 iDRAC Enterprise 卡插槽中的卡大小大于 256 MB 并且启用了 vFlash 时，才可以访问此选项。

按 <Enter> 可初始化 vFlash SD 卡。

以下原因可能会造成初始化操作失败：

- SD 卡当前不存在。
- “vFlash is currently in use by another process”（vFlash 当前正被另一个进程使用）。
- vFlash 未启用。
- SD 卡写保护。
- 一个或多个分区当前正在使用中。
- 一个或多个分区当前已附加。

vFlash 属性

按 <Enter> 可查看以下 vFlash SD 卡属性：

- **“Name”（名称）** - 显示插入到服务器的 vFlash SD 卡插槽中的 vFlash SD 卡名称。如果是 Dell SD 卡，将显示 “vFlash SD Card”（vFlash SD 卡）。如果不是 Dell SD 卡，将显示 “SD Card”（SD 卡）。
- **“Size”（大小）** - 以千兆字节 (GB) 为单位显示 vFlash SD 卡的大小。
- **“Available Space”（可用空间）** - 以兆字节 (MB) 为单位显示 vFlash SD 卡上的未使用空间。可以使用此空间在 vFlash SD 卡上创建更多分区。对于 SD 卡，可用空间显示为 256MB。
- **“Write Protected”（写保护）** - 显示 vFlash SD 卡是否受写保护。
- **“Health”（运行状况）** - 显示 vFlash SD 卡的整体运行状况。运行状况可以是：
  - OK （正常）
  - 警告
  - Critical （严重）

按 <Esc> 键退出。

Smart Card 登录

按 <Enter>，选择 **"Enabled"**（已启用）或 **"Disabled"**（已禁用）。该选项可配置智能卡登录功能。可用选项有 **"Enabled"**（已启用）、**"Disabled"**（已禁用）和 **"Enabled with RACADM"**（与 RACADM 一起启用）。

注：当选择 "Enabled"（已启用）或 "Enabled with RACADM"（与 RACADM 一起启用）后，会关闭 "IPMI Over LAN"（LAN 上 IPMI）并阻止编辑。

系统服务配置

System Services （系统服务）

按 <Enter>，选择 **"Enabled"**（已启用）或 **"Disabled"**（已禁用）。有关详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《Dell Lifecycle Controller 用户指南》。

注：修改此选项后，如果选择 "Save"（保存）和 "Exit"（退出）以应用新设置，将会重新启动服务器。

注：如果选择恢复为工厂默认值，"System Services"（系统服务）的设置不会变化。

取消系统服务

按 <Enter>，选择 **"No"**（否）或 **"Yes"**（是）。

当选择 **"Yes"**（是）后，如果选择 **"Save"**（保存）和 **"Exit"**（退出）以应用新设置，会关闭所有 Unified Server Configurator 会话并重新启动服务器。

重新启动时收集系统资源清册

选择 **"Enabled"**（已启用）允许在引导时收集资源清册。有关详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《Dell Lifecycle Controller 用户指南》。

注：修改此选项会在您保存设置并从 iDRAC6 配置公用程序退出后重新启动服务器。

注：如果选择恢复为工厂默认值，"Collect System Inventory on Restart"（重新启动时收集系统资源清册）的设置不会变化。

LCD 配置

按 <Enter>，显示 **"LCD Configuration"**（LCD 配置）子菜单。配置完 LCD 参数后，按 <Esc> 返回上一个菜单。

表 17-2. LCD 用户配置

"LCD Line 1"（LCD 行 1）	按 < 右箭头 >、< 左箭头 > 和空格键，在选项之间切换。 该功能将 LCD 上的主屏幕设置为以下选项之一： **"Ambient Temp"**（环境温度）、**"Asset Tag"**（资产标签）、**"Host Name"**（主机名）、**"iDRAC6 IPv4 Address"**（iDRAC6 IPv4 地址）、**"iDRAC6 IPv6 Address"**（iDRAC6 IPv6 地址）、**"iDRAC6 MAC Address"**（iDRAC6 MAC 地址）、**"Model Number"**（型号）、**"None"**（无）、**"Service Tag"**（服务标签）、**"System Power"**（系统电源）、**"User-Defined String"**（用户定义字符串）。
"LCD User-Defined String"（LCD 用户定义字符串）	查看或输入要在 LCD 上显示的字符串。字符串最大长度为 62 个字符。
LCD System Power Units（LCD 系统电源单位）	选择 **"Watt"**（瓦特）或 **"BTU/hr"**（BTU/ 小时）以指定要在 LCD 上显示的单位。
LCD Ambient Temp Units（LCD 环境温度单位）	选择 **"Celsius"**（摄氏度）或 **"Fahrenheit"**（华氏度）以指定要在 LCD 上显示的单位。
LCD Error Display（LCD 错误显示）	选择 **"Simple"**（简单）或 **SEL**（系统事件日志）。 该功能允许采用以下两种格式之一，在 LCD 上显示错误信息： "Simple"（简单）格式用英语提供事件说明。 SEL 格式显示系统事件日志文本字符串
"LCD Remote Virtual Console Indication"（LCD 远程虚拟控制台指示）	选择 **"Enabled"**（已启用）后，当设备上存在活动的虚拟控制台时即会显示文本 *"Virtual Console "*（虚拟控制台）。
LCD Front Panel Access（LCD 前面板访问）	按 < 右箭头 >、< 左箭头 > 和空格键，在选项 **"Disabled"**（已禁用）、**"View And Modify"**（查看和修改）和 **"View Only"**（仅查看）之间切换。 该设置为 LCD 定义用户访问级别。

LAN 用户配置

LAN 用户是 iDRAC6 管理员帐户，默认为 **root**。按 <Enter> 以显示“LAN User Configuration”（LAN 用户配置）子菜单。配置完 LAN 用户后，按 <Esc> 返回上一个菜单。

重设为默认值

使用 **“Reset to Default”**（重设为默认值）菜单项可以将所有 iDRAC6 配置项重设为工厂默认值。例如，如果忘记了管理用户密码或者想从默认设置重新配置 iDRAC6，可能就需要这样做。

按 <Enter> 以选择项目。系统将显示以下警告信息：

“Resetting to factory defaults will restore remote Non-Volatile user settings.Continue?”（重设为工厂默认值会恢复远程非易失用户设置。是否要继续？）

< “NO”（否）（取消） >

< “YES”（是）（继续） >

选择 **“YES”**（是）并按 <Enter> 会将 iDRAC6 重设为默认值。

如果此操作失败，将显示以下任何错误信息：

- “Reset command was not successful.”（重设命令不成功。）
  “Please try later- iDRAC is busy.”（请稍后尝试 - iDRAC 正忙。）
- “Failed to restore settings to default values - Timeout.”（将设置恢复为默认值失败 - 超时。）
- “Not able to send Reset command.”（无法发送重设命令。）
  “Please try later- iDRAC is busy.”（请稍后尝试 - iDRAC 正忙。）

表 17-3. LAN 用户配置

项	说明
自动查找	自动查找功能允许在网络上自动查找未配置的系统；另外，还会*安全*建立初始凭据，以便可以管理这些被发现的系统。此功能使 iDRAC6 可以找到预配置服务器。iDRAC6 和预配置服务器会互相验证。远程预配置服务器发送用户凭据以使 iDRAC6 使用这些凭据创建用户帐户。创建用户帐户后，远程控制台可以使用查找过程中指定的凭据建立 WS-MAN 与 iDRAC6 的通信，并随后向 iDRAC6 发送安全指令以远程部署操作系统。 有关远程操作系统部署的信息，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《Dell Lifecycle Controller 用户指南》。 *手动启用自动查找前，应在独立*的 **iDRAC6 配置公用程序** 会话中执行以下必要操作： • “Enable NIC”（启用 NIC） • Enable IPv4 （启用 IPv4） • DHCP 启用 • 从 DHCP 获取域名 • 禁用管理帐户 （第 2 个帐户） • 从 DHCP 获取 DNS 服务器地址 • 从 DHCP 获取 DNS 域名 选择 **“Enabled”**（已启用）可启用自动查找功能。默认情况下，此选项为 **“Disabled”**（禁用）。如果订购了**已启用**自动查找功能的 Dell 系统，则 Dell 系统上的 iDRAC6 会启用 DHCP 并且没有用于远程登录的默认凭据。
“Auto – Discovery”（自动查找）*（续...）*	添加 Dell 系统到网络并使用自动查找功能前，确保： • 已配置动态主机配置协议 (DHCP) 服务器 / 域名系统 (DNS)。 • 已安装、配置并注册预配置 Web 服务。

表 17-3. LAN 用户配置 *（续）*

项	说明
预配置服务器	此字段用于配置预配置服务器。配置服务器的地址可以由 IPv4 地址或主机名组成，并且不应超过 255 个字符。各个地址应用逗号分开。 如果启用了自动查找功能，并且在自动查找过程成功完成后，会从设置好的配置服务器检索用户凭据供以后远程配置。 有关详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《Dell Lifecycle Controller 用户指南》。
Account Access （帐户访问）	选择 **"Enabled"**（启用）可启用管理员帐户。选择 **"Disabled"**（已禁用）禁用管理员帐户，或当自动查找已启用时选择此项。
"Account Privilege"（帐户权限）	选择 **"Admin"**（管理员）、**"User"**（用户）、**"Operator"**（操作员）和 **"No Access"**（无权限）。
Account User Name（帐户用户名）	按 <Enter> 以编辑用户名并在完成后按 <Esc>。默认用户名为 **root**。
Enter Password（输入密码）	键入管理员帐户的新密码。键入时字符不会显示出来。
Confirm Password（确认密码）	重新键入管理员帐户的新密码。如果输入的字符与 **"Enter Password"**（输入密码）字段中输入的字符不同，将会显示信息，必须重新输入密码。

系统事件日志菜单

"System Event Log"（系统事件日志）菜单允许查看系统事件日志 (SEL) 信息以及清除日志信息。按 <Enter> 以显示 **"System Event Log Menu"**（系统事件日志菜单）。系统会计数日志条目并显示总记录数和最新的信息。 SEL 最多保留 512 条信息。

要查看 SEL 信息，请选择 **"View System Event Log"**（查看系统事件日志）并按 <Enter>。使用 < 左箭头 > 可移动到上一条 （较旧）信息，使用 < 右箭头 > 可移动到下一条 （较新）信息。输入记录号可跳到该记录。查看完 SEL 信息后按 <Esc>。

要清除 SEL，请选择 **"Clear System Event Log"**（清除系统事件日志）并按 <Enter>。

使用完 SEL 菜单后，按 <Esc> 返回上一个菜单。

退出 iDRAC6 配置公用程序

完成 iDRAC6 配置更改后，按 <Esc> 键显示退出菜单。

- 选择 **"Save Changes and Exit"**（保存更改并退出）并按 <Enter> 以保留更改。如果此操作失败，将显示以下一则信息：
  - "iDRAC6 Communication Failure"（iDRAC6 通信失败）— iDRAC 不可访问时显示。
  - "Some of the settings cannot be applied"（有些设置无法应用）— 有设置无法应用时显示。
- 选择 **"Discard Changes and Exit"**（放弃更改并退出）并按 <Enter> 可以忽略所做的更改。
- 选择 **"Return to Setup"**（返回设置）并按 <Enter> 以返回 iDRAC6 配置公用程序。

18

监控和警报管理

本节介绍如何监控 iDRAC6，以及如何将系统和 iDRAC6 配置为可接收警报。

配置 Managed System 以捕获上次崩溃屏幕

在 iDRAC6 可以捕获上次崩溃屏幕前，必须对 Managed System 进行配置以满足以下前提条件。

1. 安装 managed system software。有关安装 Managed System Software 的详情，请参阅 《Server Administrator 用户指南》。
2. 运行支持的 Microsoft Windows 操作系统，并且在 **"Windows Startup and Recovery Settings"**（Windows 启动和恢复设置）中取消选择 Windows 的*自动重新引导*功能。
3. 启用上次崩溃屏幕 （默认情况下已禁用）。

   要使用本地 RACADM 启用上次崩溃屏幕，请打开命令提示符，并键入以下命令：

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

4. 启用自动恢复计时器并将 **"Auto Recovery"**（自动恢复）操作设置为 **"Reset"**（重设）、**"Power Off"**（关机）或 **"Power Cycle"**（关机后再开机）。要配置 **"Auto Recovery"**（自动恢复）计时器，必须使用 Server Administrator 或 IT Assistant。

   有关如何配置 **"Auto Recovery"**（自动恢复）计时器的信息，请参阅 《Server Administrator 用户指南》。要确保能够捕获上次崩溃屏幕，**"Auto Recovery"**（自动恢复）计时器必须设置为 60 秒或更大。默认设置为 480 秒钟。

   当 **"Auto Recovery"**（自动恢复）操作设置为 **"Shutdown"**（关机）或 **"Power Cycle"**（关机后再开机）时，如果 Managed System 崩溃，上次崩溃屏幕将不可用。

禁用 Windows 自动重新引导选项

为了确保在 iDRAC6 基于 Web 的界面上，上次崩溃屏幕功能能够正常工作，请在运行 Microsoft Windows Server 2008 和 Windows Server 2003 操作系统的 Managed System 上禁用 **"Automatic Reboot"**（自动重新引导）选项。

在 Windows 2008 Server 中禁用 "Automatic Reboot"（自动重新引导）选项

1. 打开 Windows **"Control Panel"**（控制面板）并双击 **"System"**（系统）图标。
2. 在左侧单击 **"Tasks"**（任务）下的 **"Advanced System Setting"**（高级系统设置）"。
3. 单击 **"Advanced"**（高级）选项卡。
4. 在 **"Startup and Recovery"**（启动和恢复）下，单击 **"Settings"**（设置）。
5. 取消选择 **"Automatically Restart"**（自动重新启动）复选框。
6. 单击 **"OK"**（确定）两次。

在 Windows Server 2003 中禁用自动重新引导选项

1. 打开 Windows **"Control Panel"**（控制面板）并双击 **"System"**（系统）图标。
2. 单击 **"Advanced"**（高级）选项卡。
3. 在 **"Startup and Recovery"**（启动和恢复）下，单击 **"Settings"**（设置）。
4. 取消选择 **"自动重新引导"** 复选框。
5. 单击 **"OK"**（确定）两次。

配置平台事件

平台事件配置提供了用于配置远程访问设备针对某些事件信息执行所选操作的机制。这些操作包括重新引导、关机后再开机、关机以及触发警报（平台事件陷阱 [PET] 和 / 或电子邮件）。

可筛选的平台事件包括以下：

1 风扇危急声明筛选器
2 电池警告声明筛选器
3 电池危急声明筛选器
4 电压危急声明筛选器
5 温度警告声明筛选器
6 温度危急声明筛选器
7 侵入危急声明筛选器
8 冗余降级筛选器
9 冗余丧失筛选器
10 处理器警告声明筛选器
11 处理器危急声明筛选器
12 没有处理器危急声明筛选器
13 电源警告声明筛选器
14 电源危急声明筛选器
15 没有电源设备危急声明筛选器
16 事件日志危急声明筛选器
17 监控软件危急声明筛选器
18 系统电源警告声明筛选器
19 系统电源危急声明筛选器
20 没有可移动闪速更新介质通知声明筛选器
21 可移动闪速更新介质危急声明筛选器
22 可移动闪速更新介质警告声明筛选器

出现平台事件时 （例如，风扇探测器故障），会生成系统事件并在系统事件日志 (SEL) 中记录。如果该事件匹配平台事件筛选器列表中的平台事件筛选器 (PEF)，并且已配置该筛选器生成警报 （PET 或电子邮件），则会将 PET 或电子邮件警报发送到一个或多个配置目标。

如果还将同一平台事件筛选器配置为执行操作 （比如重新引导系统），则将执行该操作。

配置平台事件筛选器 (PEF)

在配置平台事件陷阱或电子邮件警报设置之前，配置平台事件筛选器。

使用基于 Web 的界面配置 PEF

有关详细信息，请参阅第 52 页上的 “配置平台事件筛选器 (PEF)”。

使用 RACADM CLI 配置 PEF

1 启用 PEF。

打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
1 1
```

其中 1 和 1 分别是 PEF 索引和启用 / 禁用选择。

PEF 索引可以是 1 到 22 之间的一个值。启用 / 禁用选择可以设置为 1（已启用）或 0 （已禁用）。

例如，要启用具有索引 5 的 PEF，键入以下命令：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
5 1
```

2 配置 PEF 操作。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 <操作>
```

其中 <*操作*> 值位如下所示：

- 0 = 无警报操作
- 1 = 关闭服务器
- 2 = 重新引导服务器
- 3 = 关闭后重新打开服务器

例如，要使 PEF 能重新引导服务器，请键入以下命令：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 2
```

其中 1 是 PEF 索引，而 2 是执行重新引导的 PEF 操作。

配置 PET

使用 Web 用户界面配置 PET

有关详细信息，请参阅第 52 页上的 “配置平台事件陷阱 (PET)”。

使用 RACADM CLI 配置 PET

1 启用全局警报。

打开命令提示符，键入以下命令并按 <Enter>：

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

2 启用 PET。

在命令提示符下，键入下列命令，并在键入每个命令后按 <Enter>：

```
IPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 1 1
```

```
IPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 1 1
```

其中 1 和 1 分别是 PET 目标索引和启用 / 禁用选择

PET 目标索引可以是 1 到 4 之间的一个值。启用 / 禁用选择可以设置为 1（已启用）或 0（已禁用）。

例如，要启用具有索引 4 的 PET，键入以下命令：

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 4 1
```

3 配置 PET 策略。

在命令提示符下，键入以下命令并按 <Enter>：

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i 1 <IPv4 地址>
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6 地址>
```

其中， 1 表示 PET 目标索引， *<IPv4 地址>* 和 *<IPv6 地址>* 表示接收平台事件警报的系统的目标 IP 地址。

4 配置团体名称字符串。

在命令提示符下键入：

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <名称>
```

配置电子邮件警报

使用 Web 用户界面配置电子邮件警报

有关详细信息，请参阅第 53 页上的 “配置电子邮件警报”。

使用 RACADM CLI 配置电子邮件警报

1 启用全局警报。

打开命令提示符，键入以下命令并按 <Enter>：

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

2 启用电子邮件警报。

在命令提示符下，键入下列命令，并在键入每个命令后按 <Enter>：

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 1 1
```

其中 1 和 1 分别是电子邮件目标索引和启用 / 禁用选择。

电子邮件目标索引可以是 1 到 4 之间的一个值。启用 / 禁用选择可以设置为 1（已启用）或 0（已禁用）。

例如，要启用具有索引 4 的电子邮件，键入以下命令：

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 配置电子邮件设置。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1 <电子邮件地址>
```

其中 1 是电子邮件目标索引，而 <*电子邮件地址*> 是接收平台事件警报的目标电子邮件地址。

要配置自定义信息，请在命令提示符下键入以下命令并按 <Enter>：

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i 1 <自定义信息>
```

其中，1 表示电子邮件目标索引，<*自定义信息*> 表示电子邮件警报上显示的信息。

检测电子邮件警报

RAC 电子邮件警报功能允许用户在 Managed System 上发生重要事件时接收电子邮件警报。下面的示例说明如何测试电子邮件警报功能以确保 RAC 在网络上正确发送电子邮件警报。

```
racadm testemail -i 2
```

注：确保在测试电子邮件警报功能前 SMTP 和电子邮件警报设置已配置。有关详情，请参阅第 288 页上的 “配置电子邮件警报”。

测试 RAC SNMP 陷阱警报功能

RAC SNMP 陷阱警报功能允许 SNMP 陷阱侦听器配置接收 Managed System 上发生的系统事件陷阱。

下面的示例说明用户如何测试 RAC 的 SNMP 陷阱警报功能。

```
racadm testtrap -i 2
```

测试 RAC SNMP 陷阱警报功能前，请确保正确配置了 SNMP 和陷阱设置。要配置这些设置，请参阅 Dell 支持网站 **dell.com/support/manuals** 上《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 testtrap 和 testemail 子命令说明。

有关 SNMP 验证的常见问题

为什么显示以下信息：

```
Remote Access: SNMP Authentication Failure
```

在发现过程中，IT Assistant 会尝试验证设备的 get 和 set 团体名称。在 IT Assistant 中， get **团体名称 = public** 而 set **团体名称 = private**。默认情况下， iDRAC6 代理的团体名称是 **public**。当 IT Assistant 发出 set 请求时，iDRAC6 代理会生成 SNMP 验证错误，因为它只接受来自**团体 = public** 的请求。

注：这是 SNMP 代理团体名称。

可以使用 RACADM 更改 iDRAC6 团体名称。

要查看 iDRAC6 团体名称，请使用以下命令：

```
racadm getconfig -g cfgOobSnmp
```

要设置 iDRAC6 团体名称，请使用以下命令：

```
racadm config -g cfgOobSnmp -o
cfgOobSnmpAgentCommunity <团体名称>
```

要使用基于 Web 的界面访问 / 配置 iDRAC6 SNMP 代理团体名称，请转至 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）→ **"Services"**（服务），然后单击 **"SNMP Agent"**（SNMP 代理）。

为了防止出现 SNMP 验证错误，必须输入代理接受的团体名称。由于 iDRAC6 只允许一个团体名称，因此必须对 IT Assistant 发现设置使用相同的 **get** 和 **set** 团体名称。

19

对 Managed System 进行恢复和故障排除

本节介绍如何使用 iDRAC6 基于 Web 的界面，执行与崩溃的远程系统的恢复和故障排除工作有关的任务。

- 。第 291 页上的 “排除远程系统故障时首先需要执行的步骤”
- 。第 291 页上的 “管理远程系统上的电源”
- 。第 301 页上的 “使用开机自检引导日志”
- 。第 302 页上的 “查看上次系统崩溃屏幕”

排除远程系统故障时首先需要执行的步骤

以下是在排除 Managed System 高级别故障时常见的一些问题：

1. 系统开机还是关机？
2. 如果是开机，操作系统是运作正常、崩溃，或者只是冻结？
3. 如果是关机，电源是意外关闭的吗？

对于崩溃的系统，请检查上次崩溃屏幕 （请参阅第 302 页上的 “查看上次系统崩溃屏幕”），使用虚拟控制台和远程电源管理 （请参阅第 291 页上的 “管理远程系统上的电源”）重新启动系统，并观察重新引导过程。

管理远程系统上的电源

iDRAC6 允许在 Managed System 上远程执行几种电源管理操作，以便在出现系统崩溃或其它系统事件后进行恢复。

从 iDRAC6 基于 Web 的界面上选择电源控制操作

要使用基于 Web 的界面执行电源管理操作，请参阅第 266 页上的 “执行服务器电源控制操作”。

从 iDRAC6 CLI 上选择电源控制操作

使用 `racadm serveraction` 命令在主机系统上执行电源管理操作。

`racadm serveraction <`*操作*`>`

以下为 < *操作* > 字符串的选项：

- **powerdown** — 关闭 Managed System 电源。
- **powerup** — 打开 Managed System 电源。
- **powercycle** — 发出对 Managed System 的关机后再开机操作。此操作类似于按下系统前面板的电源按钮关闭然后再打开系统电源。
- **powerstatus** — 显示服务器的当前电源状况 （“ON”或 “OFF”）
- **hardreset** — 对 Managed System 执行重设 （重新引导）操作。

查看系统信息

“System Summary”（系统摘要）页允许快速查看系统的运行状况及其它的基本 iDRAC6 信息，并为您提供访问系统运行状况和信息页面的链接。此外，还可从此页面快速启动常规任务并查看系统事件日志 (SEL) 中记录的最近事件。

要访问 **“System Summary”**（系统摘要）页，请单击 **“System”**（系统）→ **“Properties”**（属性）→ **“System Summary”**（系统摘要）选项卡。有关详情，请参阅 *iDRAC6 联机帮助*。

“System Details”（系统详细信息）页显示关于以下系统组件的信息：

- 主系统机箱
- Remote Access Controller

要访问 **“System Details”**（系统详情）页，展开 **“System”**（系统）树并单击 **“Properties”**（属性）→ **“System Details”**（系统详情）选项卡。

主系统机箱

注：要接收**主机名**和**操作系统名称**信息， Managed System 上必须安装有 iDRAC6 服务。

表 19-1. 系统信息

字段	说明
说明	系统说明。
BIOS 版本	系统 BIOS 版本。
Service Tag （服务标签）	系统服务标签号码。
快速服务代码	系统的服务代码。
Host Name （主机名）	主机系统的名称。
操作系统名称	系统上运行的操作系统。
OS Version （操作系统版本）	系统上运行的操作系统的版本。
“System Revision” （系统修订版本）	系统修订版本号。
“Lifecycle Controller Firmware” （Lifecycle Controller 固件）	Lifecycle Controller 固件的版本。

表 19-2. 自动恢复

字段	说明
恢复操作	可以将 iDRAC6 配置为在检测到*系统挂起*时执行以下操作之一：“No Action”（无操作）、“Hard Reset”（硬重设）、“Power Down”（关闭电源）或 “Power Cycle”（关机后再开机）。
“Initial Countdown” （初始倒计数）	当检测到*系统挂起*后，一旦经过这些秒数， iDRAC6 将执行恢复操作。
“Present Countdown” （当前倒计数）	倒计数计时器的当前值，以秒为单位。

表 19-3. 嵌入式 NIC MAC 地址

字段	说明
“Virtual MAC”（虚拟 MAC）	显示虚拟介质访问控制 (MAC) 地址。 vMAC 数据可从硬件资源清册获得，因此查看 VMAC 数据之前需要收集一次硬件资源清册。 单击 **“System Inventory”**（系统资源清册）。资源清册数据已更新并且将在 **“System Inventory”**（系统资源清册）页上显示。再次单击 **“System Details”**（系统详情）。每个嵌入式 LAN 端口的虚拟 MAC 现在都显示在 **“System Details”**（系统详情）页中。 **注：**vMAC 功能将被未来发行版本中的 Dell Advanced Infrastructure Manager (AIM) 使用。如果 Dell AIM 当前不管理服务器，则以太网 MAC 地址和虚拟 MAC 地址相同。
NIC 1	显示嵌入式网络接口控制器 (NIC) 1 的以太网、 Internet 小型计算机系统接口 (iSCSI) 和虚拟 MAC 地址。 Ethernet NIC 支持有线以太网标准，并插入到服务器的系统总线中。 iSCSI NIC 是主机计算机上运行 iSCSI 堆栈的网络接口控制器。 在介质访问控制层，MAC 地址唯一识别网络中的每个节点。
NIC 2	显示网络中唯一标识的嵌入式网络接口控制器 NIC 2 的以太网、 iSCSI 和虚拟 MAC 地址。
NIC 3	显示网络中唯一标识的嵌入式网络接口控制器 NIC 3 的以太网、 iSCSI 和虚拟 MAC 地址。
NIC 4	显示网络中唯一标识的嵌入式网络接口控制器 NIC 4 的以太网、 iSCSI 和虚拟 MAC 地址。

Remote Access Controller

表 19-4. RAC 信息

字段	说明
Name （名称）	iDRAC6
产品信息	Integrated Dell Remote Access Controller 6 – Enterprise
Date/Time （日期 / 时间）	采用以下格式表示的当前时间： Day Month DD HH:MM:SS YYYY 示例：Fri Jan 28 16:27:29 2011
Firmware Version （固件版本）	iDRAC6 固件版本
“Firmware Updated”（固件更新）	上次对固件刷写的日期，采用以下格式： Day Month DD HH:MM:SS YYYY 示例：Sat Jan 29 2011 13:31:50
Hardware Version （硬件版本）	Remote Access Controller 版本
“MAC Address” （MAC 地址）	显示唯一标识网络中各个节点的介质访问控制 (MAC) 地址

表 19-5. IPv4 信息

字段	说明
“IPv4 Enabled” （已启用 IPv4）	“Yes”（是）或 “No”（否）
IP Address （IP 地址）	标识主机的网络接口卡 (NIC) 的 32 位地址。该值采用点分隔格式，比如 143.166.154.127。
子网掩码	子网掩码标识 IP 地址的组成部分：扩展网络前缀和主机号。该值采用点分隔格式，比如 255.255.0.0。
网关	路由器或交换机的地址。该值采用点分隔格式，比如 143.166.154.1。
DHCP Enabled （已启用 DHCP）	“Yes”（是）或 “No”（否）。指示是否启用了动态主机配置协议 (DHCP)。

表 19-5. IPv4 信息 *（续）*

字段	说明
"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）	**"Yes"**（是）或 **"No"**（否）。表示是否要使用 DHCP 获取 DNS 服务器地址。
首选 DNS 服务器	表示首选 DNS 服务器的静态 IPv4 地址。
备用 DNS 服务器	表示备用 DNS 服务器的静态 IPv4 地址。

表 19-6. IPv6 信息字段

字段	说明
"IPv6 Enabled"（启用 IPv6）	表示是否启用了 Ipv6 堆栈。
"IP Address 1"（IP 地址 1）	指定 iDRAC6 NIC 的 IPv6 地址 / 前缀长度。*"prefix length"*（前缀长度）结合 IP 地址 1。这是指定 IPv6 地址前缀长度的整数。可以是介于 1 和 128 之间的值。
IP 网关	指定 iDRAC6 NIC 的网关。
链路本地地址	指定 iDRAC6 NIC 链路本地 IPv6 地址。
"IP Address 2...15"（IP 地址 2...15）	如果有的话，指定 iDRAC6 NIC 额外的 IPv6 地址。
"AutoConfig Enabled"（启用自动配置）	**"Yes"**（是）或 **"No"**（否）。"AutoConfig"（自动配置）可让 Server Administrator 从动态主机配置协议 (DHCPv6) 服务器获取 iDRAC NIC 的 IPv6 地址。
"Use DHCPv6 to obtain DNS server addresses"（使用 DHCPv6 获取 DNS 服务器地址）	**"Yes"**（是）或 **"No"**（否）。表示是否要使用 DHCPv6 获取 DNS 服务器地址。
首选 DNS 服务器	表示首选 DNS 服务器的静态 IPv6 地址。
备用 DNS 服务器	表示备用 DNS 服务器的静态 IPv6 地址。

“System Inventory”（系统资源清册）

“System Inventory”（系统资源清册）页显示关于系统上所安装硬件和固件组件的信息。

要访问 **“System Inventory”**（系统资源清册）页，展开 **“System”**（系统）树并单击 **“Properties”**（属性）→ **“System Inventory”**（系统资源清册）。

硬件资源清册

此部分显示关于系统上当前显示的硬件组件的信息。如果 “Hardware Inventory”（硬件资源清册）数据不可用，当您单击 **“System Inventory”**（系统资源清册）选项卡时，将显示以下消息：

“Hardware Inventory is unavailable.”（硬件资源清册不可用。）

刷新页面以查看详情。

固件资源清册

此部分显示所安装的 Dell 组件的固件版本。如果 “Firmware inventory”（固件资源清册）数据不可用，当您单击 **“System Inventory”**（系统资源清册）选项卡时，将显示以下消息：

“Hardware Inventory is unavailable.”（硬件资源清册不可用。）

刷新页面以查看详情。

注：如果没有启用 CSIOR （“Collect System Inventory on Reboot”（重新引导时收集系统资源清册）），则可能需要一些时间来收集数据，因此建议先运行 CSIOR 并在重新引导时收集系统资源清册，然后再单击 “System Inventory”（系统资源清册）选项卡。

向系统添加新硬件或从系统中删除硬件后，**“System Inventory”**（系统资源清册）页可能不会自动更新更改。这是因为制造过程中收集的资源清册数据可能无法更新为新的更改。

要解决此问题，请在 BIOS 开机自检期间，选择 **Cntl+E** 选项并启用 **“Collect system Inventory on reboot”**（重新引导时收集系统资源清册）。保存并从 **Cntl+E** 选项中退出。

系统会重新引导以收集新的系统资源清册。资源清册收集完成后，**“System Inventory”**（系统资源清册）页会显示正确的硬件和软件资源清册数据。

有关详情，请参阅 *iDRAC6 联机帮助*。

使用系统事件日志 (SEL)

SEL 页显示 Managed System 上发生的系统重要事件。

要查看系统事件日志：

1. 在**系统**树中单击 **"System"**（系统）。
2. 单击 **"Logs"**（日志）选项卡，然后单击 **"System Event Log"**（系统事件日志）。

   "System Event Log"（系统事件日志）页显示事件严重性并提供其它信息，如表 19-7 所示。
3. 单击相应的 **"System Event Log"**（系统事件日志）页按钮以继续。有关详情，请参阅 iDRAC6 联机帮助。
4. 单击 **"Clear Log"**（清除日志）清除 SEL。

   注：仅当您有 "Clear Logs"（清除日志）权限时，才会显示 "Clear Log"（清除日志）按钮。
5. 单击 **"Save As"**（另存为）将 SEL 保存到您所选的目录。

表 19-7. 状况指示器图标

图标 / 类别	说明
	绿色复选标记表示健康 （正常）状况。
	黄色带有感叹号的三角表示警告 （不严重）状况。
	红色 X 表示严重 （故障）状况。
	问号图标指示状态未知。
Date/Time（日期 / 时间）	事件发生的日期和时间。如果日期为空白，则事件发生在系统引导时。格式为 <day> <mon> dd yyyy hh:mm:ss，基于 24 小时制。
说明	事件的简要说明。

启用 / 禁用 OEM 事件日志

OEM 事件日志会在 **"System Event Log"**（系统事件日志）页上自动显示。**"Systems"**（系统）→ **"Logs"**（日志）选项卡中的 **"Advanced Settings"**（高级设置）按钮可以启用 / 禁用 Managed System 的 OEM 事件消息在 **"System Event Log"**（系统事件日志）页上的显示。

要禁用 OEM 事件日志在 **"System Event Log"**（系统事件日志）页上的显示，请选择 **"OEM SEL Event Filter Enabled"**（OEM SEL 事件筛选器已启用）选项。

注：默认情况下，"OEM SEL Event Filter Enabled"（OEM SEL 事件筛选器已启用）选项未选中。

使用命令行查看系统日志

```
racadm getsel -i
```

getsel -i 命令显示 SEL 中的条目数。

```
racadm getsel <选项>
```

注：如果没有指定参数，将显示整个日志。

注：有关您可以使用的选项的详情，请参阅 Dell 支持网站 dell.com/support/manuals 上《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 getsel 子命令。

clrsel 命令会从系统事件日志 (SEL) 删除全部现有的记录。

```
racadm clrsel
```

使用工作注释

工作注释是用户可添加的说明或注释。任何 iDRAC 用户均可添加工作注释。工作注释无法删除。您可以一次查看最多 1000 个工作注释。要快速参考，最新的十个工作注释可在 iDRAC 主页上显示。

注：如果添加的工作注释数超过 800 个，则 GUI 页可能需要额外数秒才能载入该页面。这是由于有相对大量的数据在 GUI 和 iDRAC6 之间进行处理。新添加的工作注释在页面载入后可能不会显示。要解决此问题，请单击"Refresh"（刷新）。

"Work Notes"（工作注释）页可让您在 Lifecycle 日志中输入工作注释。会自动记录注释的时间戳。

要访问 **"Work Notes"**（工作注释）页，展开 **"System"**（系统）树并单击 **"Systems"**（系统）→ **"Logs"**（日志）→ **"Work Notes"**（工作注释）。

"Work Notes"（工作注释）页可让您输入工作注释并提供其它信息，如表 19-8 中所示。

输入工作注释：

1 在 **"Work Notes"**（工作注释）页中的 **"Add Work Notes"**（添加工作注释）部分下，在显示的字段中输入工作注释。

注：工作注释支持最多 50 个字母数字字符。

2 单击 Save （保存）。

新的工作注释在 **"Add Work Notes"**（添加工作注释）部分下的工作注释表中显示。

表 19-8. 工作注释

字段	说明
Date/Time（日期 / 时间）	显示为每个工作注释条目记录的时间戳。格式为 yyyy-mm-ddThh:mm:ssZ，基于 24 小时制，其中， yyyy：年 mm：月 dd：日 T：时间 hh : 小时 mm : 分 ss：秒 Z：时区指示符。 **注：如果时间为 UTC，直接在时间后添加 Z （不带空格）即可。Z 是零 UTC 时差的时区指示符。因此， 09:30 UTC 表示为 09:30Z 或 0930Z。 14:45:15 UTC 将为 14:45:15Z 或 144515Z。**
Notes（注释）	显示工作注释条目内容。

使用开机自检引导日志

注：重新引导 iDRAC6 后，所有日志都会清除。

"Boot Capture"（引导捕获）页使用户能够看到最近三次可用引导循环的记录。这些记录按从新到旧的顺序排列。如果服务器没有出现引导循环，则会显示 **"No Recording Available"**（没有可用记录）。选择显示的引导循环后单击 **"Play"**（播放）在新窗口中显示。

注：查看引导捕获仅在 Java 上支持，在 Active-X 上不支持。

要查看引导捕获日志：

1. 在**系统**树中单击 **"System"**（系统）。
2. 单击 **"Logs"**（日志）选项卡，然后单击 **"BOOT Capture"**（引导捕获）选项卡。
3. 选择引导循环并单击 **"Play"**（播放）。

   随即在新屏幕上打开日志的视频。

   注：必须先关闭打开的引导捕获日志视频，之后才能播放另一个日志视频。不能同时播放两个日志。
4. 单击 **"Playback"**（回放）→ **"Play"**（播放），启动引导捕获日志视频。
5. 单击 **"Playback"**（回放）→ **"Media Controls"**（介质控制）停止视频。

注：显示信息要求保存 data.jnlp 文件而不是打开查看器。要修复此问题，请在 Internet Explorer 中执行以下操作：转至 "Tools"（工具）→ "Internet Options"（Internet 选项）→ "Advanced"（高级）选项卡并取消选择 *"Do not save encrypted pages to disk"*（不将加密的页存盘）。

注：如果 iDRAC 已重设，引导捕获视频将不可用，因为它存储在 RAM 中并且会在 iDRAC 重设时删除。

在引导期间按 F10 进入 Unified Server Configurator (USC) 应用程序后，iDRAC6 Express 卡会绑定到 iDRAC6。如果绑定成功，会在 SEL 和 LCD 中记录以下信息 — "`iDRAC6 Upgrade Successful`"（`iDRAC6` 升级成功）。如果绑定失败，会在 SEL 和 LCD 中记录以下信息 — "`iDRAC6 Upgrade Failed`"（`iDRAC6` 升级失败）。另外，如果在主板上插入的 iDRAC6 Express 卡包含不支持特定平台的旧或过期 iDRAC6 固件并且引导系统，会在开机自检屏幕上生成日志 — "`iDRAC firmware is out-of-date.Please update to the latest firmware`"（`iDRAC` 固件过期。请更新至最新的固件）。使用特定平台的最新 iDRAC6 固件更新 iDRAC6 Express 卡。有关详情，请参阅《Dell Lifecycle Controller 用户指南》。

查看上次系统崩溃屏幕

注：上次崩溃屏幕功能要求 Managed System 在 Server Administrator 中配置“Auto Recovery”（自动恢复）功能。此外，确保使用 iDRAC6 启用了“Automated System Recovery”（自动系统恢复）功能。导航至 “iDRAC Settings”（iDRAC 设置）部分中 “Network/Security”（网络 / 安全性）选项卡下的 “Services”（服务）页以启用此功能。

要查看 **“Last Crash Screen”**（上次崩溃屏幕）页：

1. 在**系统**树中单击 **“System”**（系统）。
2. 单击 **“Logs”**（日志）选项卡，然后单击 **“Last Crash”**（上次崩溃）**屏幕**。

   “Last Crash Screen”（上次崩溃屏幕）页显示最新的崩溃屏幕。上次系统崩溃信息保存在 iDRAC6 内存中，并且可以远程访问。

   有关 **“Last Crash Screen”**（上次崩溃屏幕）页上所显示按钮的详情，请参阅 *iDRAC6 联机帮助*。

注：由于自动恢复计时器的波动，当系统重设计时器设置为小于 30 秒的值时可能无法捕获**上次崩溃屏幕**。使用 Server Administrator 或 IT Assistant 将系统重设计时器设置为至少 30 秒，并确保**上次崩溃屏幕**运行正常。有关其它信息，请参阅第 283 页上的 “配置 Managed System 以捕获上次崩溃屏幕”。

20

对 iDRAC6 进行恢复和故障排除

本节介绍如何执行与崩溃的 iDRAC6 的恢复和故障排除有关的任务。

可以使用以下任一工具来排除 iDRAC6 的故障：

- RAC 日志
- 诊断控制台
- 标识服务器
- 跟踪日志
- racdump
- coredump

使用 RAC 日志

RAC 日志是 iDRAC6 固件中的一个持续存在的日志。日志中的列表记录了用户操作 （比如登录、注销和安全策略更改）以及由 iDRAC6 发出的警报。当日志已满后，会将最早的条目覆盖掉。

要从 iDRAC6 用户界面 (UI) 访问 RAC 日志，请执行以下操作：

1. 在 **"System"**（系统）树中，单击 **"iDRAC Settings"**（iDRAC 设置）。
2. 单击 **"Logs"**（日志）选项卡，然后单击 **"iDRAC Log"**（iDRAC 日志）。

"iDRAC Log"（iDRAC 日志）页显示表 20-1 中列出的信息。

表 20-1. iDRAC 日志页面信息

字段	说明
"Date/Time"（日期 / 时间）	日期和时间 （例如 `Dec 19 16:55:47`）。 当 iDRAC6 刚开始启动并且无法与 Managed System 通信时，该时间将会显示为 "`System Boot`"（系统引导）。
Source	引起事件的接口。
说明	iDRAC6 中记录的事件和用户名的简要说明。

注：有关使用 "iDRAC Log"（iDRAC 日志）页按钮的详情，请参阅 *iDRAC6 联机帮助*。

使用命令行

使用 `getraclog` 命令查看 iDRAC6 日志条目。

`racadm getraclog [` **选项** `]`

`racadm getraclog -i`

getraclog -i 命令显示 iDRAC6 日志中的条目数。

注：有关详情，请参阅 Dell 支持网站 dell.com/support/manuals 上《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 getraclog。

可以使用 `clrraclog` 命令从 iDRAC 日志清除所有条目。

`racadm clrraclog`

使用诊断控制台

iDRAC6 提供一组标准网络诊断工具（请参阅表 20-2），与基于 Microsoft Windows 或 Linux 的系统提供的工具类似。使用 iDRAC6 基于 Web 的界面，可以访问网络调试工具。

单击 **"Reset iDRAC6"**（重设 iDRAC6）以重设 iDRAC。将对 iDRAC 执行普通引导操作。

要访问 **"Diagnostic Console"**（诊断控制台）页：

1. 在 **"System"**（系统）树中，单击 **"iDRAC Settings"**（iDRAC 设置）→ **"Troubleshooting"**（故障排除）选项卡 → **"Diagnostics Console"**（诊断控制台）。
2. 键入命令并单击 **"Submit"**（提交）。表 20-2 说明可以使用的命令。调试结果显示在 **"Diagnostics Console"**（诊断控制台）页中。
3. 要刷新 **"Diagnostics Console"**（诊断控制台）页，请单击 **"Refresh"**（刷新）。要执行其它命令，请单击 **"Go Back to Diagnostics Page"**（退回到诊断页）。

表 20-2. 诊断命令

命令	说明
arp	显示地址解析协议 (ARP) 表的内容。ARP 条目不能添加或删除。
ifconfig	显示网络接口表的内容。
netstat	打印路由表的内容。如果在 **netstat** 选项右边的文本字段中提供可选接口号，netstat 将输出与通过该接口的通信量有关的其它信息、缓冲区的使用情况以及其它网络接口信息。

表 20-2. 诊断命令 *（续）*

命令	说明
ping <*IP 地址*>	验证目标 IP 地址是否可以使用当前路由表内容从 iDRAC6 进行访问。必须在该选项右侧的字段中输入目标 IP 地址。根据当前的路由表内容，将 Internet 控制报文协议 (ICMP) 回音数据包发送到目标 IP 地址。
gettracelog	显示 iDRAC6 跟踪日志。有关详情，请参阅 Dell 支持网站 dell.com/support/manuals 上 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 gettracelog。

使用标识服务器

"Identify"（标识）页允许启用系统标识功能。

要识别服务器：

1. 单击 **"System"**（系统）→ **"iDRAC Settings"**（iDRAC 设置）→ **"Troubleshooting"**（故障排除）→ **"Identify"**（标识）。
2. 在 **"Identify"**（标识）屏幕上，选择 **"Identify Server"**（标识服务器）复选框启用 LCD 及背后标识服务器 LED 的闪烁。
3. **"Identify Server Timeout"**（标识服务器超时）字段显示 LCD 闪烁的秒数。输入要让 LCD 闪烁的时间 （秒）。超时范围为 1 到 255 秒。如果将超时设为 0 秒， LCD 会连续闪烁。
4. 单击 **"Apply"**（应用）。

如果输入 0 秒，则通过这些步骤禁用：

1. 单击 **"System"**（系统）→ **"iDRAC Settings"**（iDRAC 设置）→ **"Troubleshooting"**（故障排除）→ **"Identify"**（标识）。
2. 在 **"Identify"**（标识）屏幕上，取消选择 **"Identify Server"**（标识服务器）选项，然后单击 **"Apply"**（应用）。

使用跟踪日志

内部 iDRAC6 跟踪日志由管理员用于调试 iDRAC6 警报和网络问题。

要从 iDRAC6 基于 Web 的界面访问跟踪日志：

1. 在 **"System"**（系统）树中，单击 **"iDRAC Settings"**（iDRAC 设置）。
2. 单击 **"Diagnostics"**（诊断）选项卡。

3 将 gettracelog 命令或 racadm gettracelog 命令键入**命令**字段。

注：还可以从命令行界面使用此命令。有关详情，请参阅 Dell 支持网站 dell.com/support/manuals 上 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 gettracelog。

跟踪日志跟踪以下信息：

- DHCP - 跟踪发送到 DHCP 服务器和从 DHCP 服务器接收的数据包。
- IP - 跟踪发送和接收的 IP 数据包。

跟踪日志还可能包含 iDRAC6 固件特定的错误代码，与内部 iDRAC6 固件有关，而不是 Managed System 的操作系统。

注：iDRAC6 不会回送数据包大小超过 1500 字节的 ICMP (ping)。

使用 racdump

`racadm racdump` 命令使用户可以通过一个命令就获得转储、状态以及 iDRAC6 板的一般信息。

注：此命令仅可用于 Telnet、 SSH 和远程 racadm 界面。有关详情，请参阅 Dell 支持网站 dell.com/support/manuals 上 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 racdump 命令。

使用 coredump

`racadm coredump` 命令显示有关 RAC 最近出现的重要问题的详细信息。 coredump 信息可用于诊断这些重要问题。

如果出现的话，coredump 信息在整个 RAC 关机后再开机过程中都保持不变，并且只有在出现以下某种情况时才会清除：

- 使用 `coredumpdelete` 子命令清除 coredump 信息。
- 在 RAC 上出现其它重要情况。如果出现这种情况， coredump 信息将与最新出现的严重错误相关。

`racadm coredumpdelete` 命令可用于清除 RAC 中任何最近存储的 **coredump** 数据。有关详情，请参阅 Dell 支持网站 **dell.com/support/manuals** 上 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》中的 `coredump` 和 `coredumpdelete` 子命令。

21

传感器

硬件传感器或探测器帮助用户以更有效的方式监测网络上的系统，使用户可以采取相应的措施来防止灾难，比如系统不稳定或损坏。

可以使用 iDRAC6 监测相应的硬件传感器来监测电池、风扇探测器、机箱侵入、电源设备、功耗、温度和电压。

电池探测器

电池探测器提供有关系统板 CMOS 和主板存储 RAM (ROMB) 电池的信息。

注：只有在系统具有 ROMB 时，存储 ROMB 电池设置才可用。

风扇探测器

风扇探测器传感器提供的信息有：

- 风扇冗余 — 如果主风扇不能以预设置的速度散热，第二个风扇将替换主风扇。
- 风扇探测器列表 — 提供系统所有风扇的速度信息。

机箱侵入探测器

机箱侵入探测器提供机箱状况的信息，即机箱是打开还是关闭。

电源设备探测器

电源设备探测器提供的信息有：

- 电源设备状况
- 电源设备冗余，即，在主电源设备故障的情况下由冗余电源设备替换主电源设备。

  注：如果系统中只有一个电源设备，电源设备冗余将设置为“Disabled”（已禁用）。

可移动闪速更新介质探测器

可移动闪速更新介质传感器提供关于 vFlash SD 卡状况 （活动或不存在）的信息。有关 vFlash SD 卡的详情，请参阅第 243 页上的 “配置 vFlash SD 卡和管理 vFlash 分区”。

电源监测探测器

电源监测提供有关*实时*功耗 （瓦和安培）的信息。

还可以查看 iDRAC6 中设置的当前时间的上一分钟、上一小时、昨天或上周功耗的图形化表示。

温度探测器

温度传感器提供有关系统板环境温度的信息。温度探测器表示探测器状况是否在预设警告和临界阈值内。

电压探测器

以下是典型的电压探测器。系统可能有这些和 / 或其它。

- CPU [n] VCORE
- System Board 0.9V PG
- System Board 1.5V ESB2 PG
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

电压探测器表示探测器状况是否在预设警告和临界阈值内。

22

配置安全功能

iDRAC6 提供以下安全功能：

- 针对 iDRAC6 管理员的高级安全选项：
  - “Virtual Console disable”（虚拟控制台禁用）选项使*本地*系统用户能够使用 iDRAC6 虚拟控制台功能禁用虚拟控制台。
  - 本地配置禁用功能使*远程* iDRAC6 管理员能够有选择地禁用 iDRAC6 的配置：
    - BIOS POST option-ROM
    - 操作系统使用本地 RACADM 和 Dell OpenManage Server Administrator 公用程序
- RACADM CLI 和基于 Web 的界面操作，支持 128 位和 40 位 （用于不接受 128 位加密的国家 / 地区） SSL 加密技术

  注：Telnet 不支持 SSL 加密技术。
- 通过基于 Web 的界面或 RACADM CLI 进行会话超时配置 （以秒为单位）
- 可配置 IP 端口 （在相应情况下）
- Secure Shell (SSH)，其使用加密传输层实现更高的安全性
- 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 iDRAC6 的客户端的有限 IP 地址范围

针对 iDRAC6 管理员的安全选项

禁用 iDRAC6 本地配置

管理员可以通过 iDRAC6 图形用户界面 (GUI) 选择 **"iDRAC Settings"**（iDRAC 设置）→ **"Network/Security"**（网络 / 安全性）→ **"Services"**（服务）来禁用本地配置。选中 **"Disable the iDRAC Local Configuration using option ROM"**（使用 option ROM 禁用 iDRAC 本地配置）复选框后，iDRAC6 配置公用程序—在系统引导期间按 <Ctrl+E> 访问—以只读模式运行，防止本地用户配置设备。管理员选择 **"Disable the iDRAC Local Configuration using RACADM"**（使用 RACADM 禁用 iDRAC 本地配置）复选框后，本地用户不能通过 RACADM 公用程序或 Dell OpenManage Server Administrator 配置 iDRAC6，尽管这些程序仍可读取配置设置。

管理员可以使用基于 Web 的界面启用其中一个或同时启用这两个选项。

系统重新引导期间禁用本地配置

此功能禁用 Managed System 用户在系统重新引导期间配置 iDRAC6 的能力。

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

注：仅在 iDRAC6 配置公用程序上支持此选项。要升级到此版本，您必须升级 BIOS。使用 Dell 支持网站 **support.dell.com** 上的 BIOS 更新软件包升级 BIOS。

从本地 RACADM 禁用本地配置

此功能禁用 Managed System 用户使用本地 RACADM 或 Dell OpenManage Server Administrator 公用程序配置 iDRAC6 的能力。

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

警告：此功能极大地限制了本地用户从本地系统配置 iDRAC6 的能力，包括执行配置默认重设。建议您根据情况使用这些功能。一次只禁用一个接口以防一下失去所有登录权限。

注：请参阅 Dell 支持网站 **support.dell.com** 上有关*禁用 DRAC 中的本地配置和远程虚拟 KVM* 的白皮书了解详情。

尽管管理员可以使用本地 RACADM 命令设置本地配置选项，然而出于安全原因，可以只从带外 iDRAC6 基于 Web 的界面或命令行界面进行重设。 `cfgRacTuneLocalConfigDisable` 选项在系统开机自检完成并且引导到操作系统环境后应用。操作系统可以是 Microsoft Windows Server 或 Enterprise Linux 等可以运行本地 RACADM 命令的操作系统，或者是用来运行 Dell OpenManage Deployment Toolkit 本地 RACADM 命令的 Microsoft Windows 预安装环境或 vmlinux 等有限使用操作系统。

有几种情况可能需要管理员禁用本地配置。例如，在有多个管理员管理服务器和远程访问设备的数据中心，负责维护服务器软件的管理员可能不需要远程访问设备的管理权限。同样，技术人员在日常系统维护时会实际接触到服务器—可以重新引导系统并访问密码保护的 BIOS—但是不应能够配置远程访问设备。在这样的情况下，远程访问设备管理员可能希望禁用本地配置。

管理员应记住，由于禁用本地配置会极大地限制本地配置权限—包括重设 iDRAC6 为默认配置的能力—所以应该只在必要时使用这些选项，并且一般情况下应一次只禁用一个接口以避免一下失去所有登录权限。例如，如果管理员已禁用所有本地 iDRAC6 用户并且只允许 Microsoft Active Directory 目录服务用户登录 iDRAC6，则 Active Directory 验证基础架构随后会出现故障，而管理员将可能无法登录。同样，如果管理员已禁用所有本地配置并在已有动态主机配置协议 (DHCP) 服务器的网络上为 iDRAC6 设置静态 IP 地址，而 DHCP 服务器随后将该 iDRAC6 IP 地址分配给网络上的另一个设备，则随后出现的冲突会禁用 DRAC 的带外连接，要求管理员通过串行连接将固件重设为默认设置。

禁用 iDRAC6 虚拟控制台

管理员可以有选择地禁用 iDRAC6 远程虚拟控制台，为本地用户在系统上工作提供了一个灵活安全的机制，防止其他人通过虚拟控制台查看该用户的操作。为了使用此功能，必须在服务器上安装 iDRAC 受管节点软件。管理员可以使用以下命令禁用虚拟控制台：

```
racadm LocalConRedirDisable 1
```

命令 LocalConRedirDisable 在带参数 1 执行时会禁用现有的虚拟控制台会话窗口

要帮助防止远程用户重写本地用户设置，此命令只对本地 RACADM 可用。管理员可以在支持 RACADM 的操作系统中使用此命令，包括 Microsoft Windows Server 2003 和 SUSE Linux Enterprise Server 10。由于此命令在整个系统重新引导过程中持续有效，管理员必须明确撤销此命令后才能重新启用虚拟控制台。可以使用参数 0 来设置：

```
racadm LocalConRedirDisable 0
```

有几种情况可能需要禁用 iDRAC6 虚拟控制台。例如，管理员可能不希望远程 iDRAC6 用户查看系统上配置的 BIOS 设置，在这种情况下可以通过使用 `LocalConRedirDisable` 命令在系统开机自检期间禁用虚拟控制台。可能还希望每次管理员登录系统时都自动禁用虚拟控制台来提高安全性，在这种情况下可以从用户登录脚本执行 `LocalConRedirDisable` 命令来实现。

注：请参阅 Dell 支持网站 support.dell.com 上有关*禁用 DRAC 中的本地配置和远程虚拟 KVM* 的白皮书了解详情。

有关登录脚本的详情，请参阅 **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx**。

使用 SSL 和数字证书保证 iDRAC6 通信安全

本小节提供关于 iDRAC6 中包括的以下数据安全功能的信息：

- 第 312 页上的 “安全套接字层 (SSL)”
- 第 313 页上的 “证书签名请求 (CSR)”
- 第 313 页上的 “访问 SSL 主菜单”
- 第 314 页上的 “生成证书签名请求”

安全套接字层 (SSL)

iDRAC6 包括 Web Server，通过配置 Web Server 可使用行业标准的 SSL 安全协议在 Internet 上传输加密数据。基于公共密钥和私人密钥加密技术构建的 SSL 是广泛接受的技术，用于在客户端和服务器之间提供验证和加密的通信以防止网络上的窃听现象。

启用 SSL 的系统：

- 向启用 SSL 的客户端验证自身
- 允许客户端向服务器验证自身
- 允许两个系统建立加密连接

此加密过程提供高级别数据保护。 iDRAC6 使用 128 位 SSL 加密标准，这是北美 Internet 浏览器常用的最安全加密方式。

iDRAC6 Web Server 包括 Dell 自签 SSL 数字证书 （服务器 ID）。确保 Internet 上的高安全性：

1 将默认的 Web Server SSL 证书替换为来自认证机构 (CA) 的有效证书。

2 通过将请求提交至 iDRAC6 生成证书签名请求 (CSR)。

3 向认证机构 (CA) 提供 CSR 以获得有效证书。

证书签名请求 (CSR)

CSR 是向认证机构 (CA) 请求安全服务器证书的数字请求。安全服务器证书可以保护远程系统的身份，并确保与远程系统交换的信息不会被他人查看或更改。要确保 DRAC 的安全，强烈建议您生成 CSR，将 CSR 提交至 CA，然后上载从 CA 返回的证书。

CA 是 IT 行业认可的企业实体，可满足高标准的可靠性审查、识别和其它重要安全标准。例如，Thwate 和 VeriSign 均为 CA。CA 收到您的 CSR 后，将对 CSR 中包含的信息进行检查和验证。如果申请者符合 CA 的安全标准， CA 将向申请者颁发认证，以便在通过网络和 Internet 进行交易时唯一标识该申请者。

CA 批准 CSR 并向您发送证书后，您必须将证书上载至 iDRAC6 固件。存储在 iDRAC6 固件中的 CSR 信息必须与证书中包含的信息匹配。

访问 SSL 主菜单

1 展开 **"System"**（系统）树并单击 **"iDRAC Settings"**（iDRAC 设置）。

2 单击 **"Network Security"**（网络 / 安全性）选项卡，然后单击 **SSL**。

使用 **SSL 主菜单** （请参阅表 22-1）生成 CSR，上载现有服务器证书，或查看现有服务器证书。 CSR 信息存储在 iDRAC6 固件中。有关 **SSL** 页上可用按钮的信息，请参阅 *iDRAC6 联机帮助*。

表 22-1. SSL 主菜单

字段	说明
"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）	单击 **"Next"**（下一步）打开该页，可以生成 CSR 发送给 CA 以请求安全 Web 证书。

表 22-1. SSL 主菜单 *(续)*

字段	说明
"Upload Server Certificate"（上载服务器证书）	单击 "Next"（下一步），上载您公司拥有的现有证书并用来控制对 iDRAC6 的访问。 **注：**只有 Base 64 编码的 X509 证书才能被 iDRAC6 接受。不接受 DER 编码的证书。上载新证书会替换 iDRAC6 中原有的默认证书。
View Server Certificate（查看服务器证书）	单击 "Next"（下一步）查看现有服务器证书。

生成证书签名请求

注：每个 CSR 都会改写固件上任何原有的 CSR。在 iDRAC 能够接受已签名的证书前，固件中的 CSR 必须匹配从 CA 返回的证书。

1. 在 "SSL Main Menu"（SSL 主菜单）上，选择 "Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）并单击 "Next"（下一步）。
2. 在 "Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）页上键入每个 CSR 属性的值。

   表 22-2 说明了 "Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）页选项。
3. 单击 "Generate"（生成）打开或保存 CSR。
4. 单击相应的 "Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）页按钮继续。有关 "Generate Certificate Signing Request (CSR)"（生成证书签名请求 (CSR)]）页上可用按钮的详情，请参阅 *iDRAC6 联机帮助*。

表 22-2. 生成证书签名请求 (CSR) 页选项

字段	说明
Common Name（常用名）	认证的确切名 （通常是 Web Server 的域名，例如，xyzcompany.com）。字母数字字符、连字符和句点有效。
Organization Name（组织名称）	与此组织相关的名称 （例如， XYZ 公司）。字母数字字符、连字符和句点有效。

表 22-2. 生成证书签名请求 (CSR) 页选项 *（续）*

字段	说明
Organization Unit（组织单位）	与组织部门相关的名称 （例如，事业组）。字母数字字符、连字符和句点有效。
Locality（地点）	认证实体的城市或其它位置 （例如，朗得罗克 [Round Rock]）字母数字字符、连字符和句点有效。
状态名称	申请认证的实体所在的州或省 （例如，德克萨斯州 [Texas]）字母数字字符、连字符和句点有效。
“Country Code”（国家 / 地区代码）	申请认证的实体所在的国家 / 地区名。使用下拉式菜单选择国家 / / 地区。
Email（电子邮件）	与 CSR 相关的电子邮件地址。可以键入公司的电子邮件地址，或任何想与 CSR 关联的电子邮件地址。此字段可选。

查看服务器证书

1 在 **“SSL Main Menu”**（SSL 主菜单）页中，选择 **“View Server Certificate”**（查看服务器证书）并单击 **“Next”**（下一步）。

表 22-3 说明 **Certificate** （证书）窗口中列出的字段及相关说明。

2 单击相应的 **“View Server Certificate”**（查看服务器证书）页按钮继续。

表 22-3. 认证信息

字段	说明
序列号	证书序列号
“Subject Information”（主题信息）	按主题输入的证书属性
“Issuer Information”（颁发者信息）	按颁发者返回的证书属性
“Valid From”（有效期自）	证书的颁发日期
“Valid To”（有效期至）	证书的期满日期

使用 Secure Shell (SSH)

有关使用 SSH 的信息，请参阅第 80 页上的 “使用 Secure Shell (SSH)”。

配置服务

注：要修改这些设置，必须具有 “Configure iDRAC”（配置 iDRAC）权限。此外，仅当用户作为 root 登录时，才可以启用远程 RACADM 命令行公用程序。

1. 展开 System （系统）树并单击 iDRAC Settings （iDRAC 设置）。
2. 单击 **“Network Security”**（网络 / 安全性）选项卡，然后单击 **“Services”**（服务）。
3. 根据需要配置以下服务：
   - 本地配置 （表 22-4）
   - Web Server （表 22-5）
   - SSH （表 22-6）
   - Telnet （表 22-7）
   - 远程 RACADM （表 22-8）
   - SNMP 代理 （表 22-9）
   - 自动系统恢复代理 （表 22-10）

   使用**自动系统恢复代理**启用 iDRAC6 的**上次崩溃屏幕**功能。

   注：必须安装 Server Administrator 并激活其**自动恢复**功能，方法是将 “Action”（操作）设置为：“Reboot System”（重新引导系统）、“Power Off System”（关闭系统电源）或 “Power Cycle System”（系统关机再开机），这样才能使**上次崩溃屏幕**在 iDRAC6 中运行。
4. 单击 **“Apply Changes”**（应用更改）应用 “Services”（服务）页设置。

表 22-4. 本地配置设置

设置	说明
“Disable the iDRAC local configuration using option ROM”（使用 option ROM 禁用 iDRAC 本地配置）	使用 option ROM 禁用 iDRAC 的本地配置。option ROM 会在系统重新引导期间提示按 <Ctrl+E> 进入设置模块。
“Disable the iDRAC local configuration using RACADM”（使用 RACADM 禁用 iDRAC 本地配置）	使用本地 RACADM 禁用 iDRAC 的本地配置。

表 22-5. Web Server 设置

设置	说明
Enabled （启用）	启用或禁用 Web Server。选中 = 启用；未选中 = 禁用。
Max Sessions （最大会话数）	此系统允许的最大同时会话数。
“Active Sessions” （激活的会话数）	系统上的当前会话数，小于等于 **“Max Sessions”**（最大会话数）。
超时	允许连接保持闲置的秒数。达到超时时将取消会话。对超时设置的更改会直接影响并终止当前的 Web 界面会话。 Web Server 也将进行重设。请等待几分钟，然后再打开新的 Web 界面会话。超时范围为 60 至 10800 秒。默认值为 1800 秒。
HTTP Port Number （HTTP 端口号）	侦听服务器连接的 iDRAC 使用的端口。默认设置为 80。
HTTPS Port Number （HTTPS 端口号）	侦听服务器连接的 iDRAC 使用的端口。默认设置为 443。

表 22-6. SSH 设置

设置	说明
Enabled （启用）	启用或禁用 SSH。选中后，会启用 SSH。
超时	Secure Shell 闲置超时，以秒为单位。超时范围为 60 至 1920 秒。输入 0 秒将禁用超时功能。默认为 300。
端口号	iDRAC6 侦听 SSH 连接所在的端口。默认为 22。

表 22-7. Telnet 设置

设置	说明
Enabled （启用）	启用或禁用 Telnet。选中后，就启用 Telnet。
超时	Telnet 闲置超时，以秒为单位。超时范围为 60 至 1920 秒。输入 0 秒将禁用超时功能。默认为 300。
端口号	iDRAC6 侦听 Telnet 连接所在的端口。默认为 23。

表 22-8. 远程 RACADM 设置

设置	说明
Enabled （启用）	启用 / 禁用远程 RACADM。选中后，就启用远程 RACADM。
“Active Sessions” （激活的会话数）	系统上的当前会话数。

表 22-9. SNMP 代理设置

设置	说明
Enabled （启用）	启用或禁用 SNMP 代理。选中 = 启用；未选中 = 禁用。
Community Name （团体名称）	定义要使用的 SNMP 团体字符串。团体名称长度最多为 31 个非空白字符。默认设置为 public。

表 22-10. 自动系统恢复代理设置

设置	说明
Enabled （启用）	启用自动系统恢复代理。

启用其它 iDRAC6 安全选项

要防止未授权访问远程系统， iDRAC6 提供了以下功能：

- IP 地址筛选 (IPRange) — 定义可以访问 iDRAC6 的特定范围的 IP 地址。
- IP 地址阻塞 — 限制特定 IP 地址的失败登录尝试次数。

这些功能在 iDRAC6 默认配置中禁用。使用以下子命令或基于 Web 的界面启用这些功能。

```
racadm config -g cfgRacTuning -o <对象名> <值>
```

此外，将这些功能与相应的会话空闲超时值以及定义的网络安全计划结合使用。

以下小节提供了有关这些功能的其它信息。

IP 筛选 (IpRange)

IP 地址筛选 （或 *IP 范围检查*）只允许 IP 地址在用户特定范围内的客户端或管理工作站对 iDRAC6 进行访问。所有其它登录都将被拒绝。

IP 筛选将接入登录的 IP 地址与以下 **cfgRacTuning** 属性中指定的 IP 地址范围相比较：

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

cfgRacTuneIpRangeMask 属性既应用于接入 IP 地址，也应用于 **cfgRacTuneIpRangeAddr** 属性。如果两个属性的结果相同，则允许接入登录请求访问 iDRAC6。从该范围以外的 IP 地址登录将收到一个错误。

如果以下表达式等于零，登录将会继续：

```
cfgRacTuneIpRangeMask & (<接入的 IP 地址> ^
cfgRacTuneIpRangeAddr)
```

其中 & 是数量的按位 “与”，而 ^ 是按位 “异或”。

有关 **cfgRacTuning** 属性的完整列表，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》。

表 22-11. IP 地址筛选 (IpRange) 属性

属性	说明
cfgRacTuneIpRangeEnable	启用 IP 范围检查功能。
cfgRacTuneIpRangeAddr	根据子网掩码中的 1，确定可接受的 IP 地址位样式。 此属性是与 **cfgRacTuneIpRangeMask** 的按位“与”，确定所允许 IP 地址的高端。允许在高位包含此位样式的任何 IP 地址建立 iDRAC6 会话。从该范围外的 IP 地址登录都会失败。各属性中的默认值允许从 192.168.1.0 到 192.168.1.255 的地址范围建立 iDRAC6 会话。
cfgRacTuneIpRangeMask	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。

启用 IP 筛选

请参阅以下用于 IP 筛选设置的示例命令。

请参阅第 100 页上的“远程使用 RACADM”了解有关 RACADM 和 RACADM 命令的详情。

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

要将登录限制到一个 IP 地址 （例如， 192.168.0.57），则使用全掩码，如以下部分中所示。

```
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
```

要将登录限制到一组四个相邻的 IP 地址 （例如， 192.168.0.212 到 192.168.0.215），则选择掩码中除最低的两个位以外的所有位，如以下部分中所示：

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.252
```

IP 筛选原则

启用 IP 筛选时应遵循以下原则：

- 确保 **cfgRacTuneIpRangeMask** 配置为网络掩码的形式，所有的高位为 1 （定义掩码中的子网），在低位都变为 0。
- 用所要的范围基础地址作为 **cfgRacTuneIpRangeAddr** 的值。此地址的 32 位二进制值应将掩码中为零的所有低位都设为零。

IP 阻塞

IP 阻塞动态确定来自特定 IP 地址的额外登录失败，并阻塞 （或防止）该地址在预选的时间长度内登录 iDRAC6。

IP 阻塞参数使用 **cfgRacTuning** 组功能，其中包括：

- 允许的登录失败次数
- 按秒计算的必须出现这些失败的时间范围
- 在超过允许失败总数后阻止*有问题的* IP 地址建立会话的时间 （秒）

随着特定 IP 地址的登录失败次数不断累积，这些值会由内部计数器*增加*。当用户成功登录后，失败历史记录就会清除并且内部计数器将重设。

注：如果客户端 IP 地址的登录尝试遭到拒绝，有些 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。）**

有关 **cfgRacTuning** 属性的完整列表，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 《适用于 iDRAC6 和 CMC 的 RACADM 命令行参考指南》。

表 22-12 列出了用户定义的参数。

表 22-12. 登录重试限制属性

属性	定义
cfgRacTuneIpBlkEnable	启用 IP 阻塞功能。 如果在一段时间内 (**cfgRacTuneIpBlkFailWindow**) 某 IP 地址出现连续的失败 (**cfgRacTuneIpBlkFailCount**)，则在一段时间内 (**cfgRacTuneIpBlkPenaltyTime**) 来自该地址的其它建立会话尝试都会遭到拒绝。
cfgRacTuneIpBlkFailCount	设置拒绝某 IP 地址的登录尝试前允许的登录失败次数。

表 22-12. 登录重试限制属性 *（续）*

属性	定义
cfgRacTuneIpBlkFailWindow	计算失败尝试次数的时间范围 （秒）。当失败次数超出此限制，将不会记入计数器。
cfgRacTuneIpBlkPenaltyTime	定义来自失败次数过多的某 IP 地址的所有登录尝试被拒绝的时间长度 （秒）。

启用 IP 阻塞

以下示例显示，如果客户端在一分钟内超过五次登录尝试失败，将阻止该客户端 IP 地址建立会话五分钟。

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

以下示例在一分钟内阻止三次以上的失败尝试，并阻止其它登录尝试一小时。

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

使用 iDRAC6 GUI 配置网络安全设置

注：您必须具有 “Configure iDRAC6”（配置 iDRAC6）权限才能执行以下步骤。

1. 在 **“System”**（系统）树中，单击 **“iDRAC Settings”**（iDRAC 设置）。
2. 单击 **“Network/Security”**（网络 / 安全性）选项卡，然后单击 **“Network”**（网络）。
3. 在 **“Network Configuration”**（网络配置）页中，单击 **“Advanced Settings”**（高级设置）。
4. 在 **“Network Security”**（网络安全性）页中，配置属性值，然后单击 **“Apply Changes”**（应用更改）。

   表 22-13 说明了 **“Network Security”**（网络安全性）页设置。
5. 单击相应的 **“Network Security”**（网络安全性）页按钮继续。有关 Network Security （网络安全性）页按钮的详情，请参阅 *iDRAC6 联机帮助*。

表 22-13. 网络安全性页设置

设置	说明
IP Range Enabled（IP 范围已启用）	启用 IP 范围检查功能，该功能定义可以访问 iDRAC6 的特定 IP 地址范围。
IP Range Address（IP 范围地址）	根据子网掩码中的 1，确定可接受的 IP 地址位样式。该值是含 IP 范围子网掩码的按位 “与”，可确定所允许的 IP 地址的高端。允许在高位包含此位样式的任何 IP 地址建立 iDRAC6 会话。从该范围外的 IP 地址登录都会失败。各属性中的默认值允许从 192.168.1.0 到 192.168.1.255 的地址范围建立 iDRAC6 会话。
“IP Range Subnet Mask”（IP 范围子网掩码）	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。 例如：255.255.255.0
IP Blocking Enabled （IP 阻塞已启用）	启用 IP 地址阻塞功能，该功能限制在预先选择的时间范围内从特定 IP 地址尝试登录失败的次数。
IP Blocking Fail Count （IP 阻塞失败计数）	设置拒绝某个 IP 地址的登录尝试前允许登录失败的次数。

表 22-13. 网络安全性页设置 *（续）*

设置	说明
IP Blocking Fail Window（IP 阻塞失败时间范围）	决定一个时间范围（以秒为单位），在该范围内必须发生 IP 阻塞失败计数的失败次数才会触发 IP 阻塞惩罚时间。
IP Blocking Penalty Time（IP 阻塞惩罚时间）	一个时间范围（以秒为单位），在该范围内拒绝失败次数过多的某个 IP 地址的登录尝试。

索引

A

C

I

L

M

N

P

R

S

T

U

V

W

Z