Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 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： "注意"表示如果不遵循说明，就有可能损坏硬件或导致数据丢失。

2010 年 7 月

目录

iDRAC6 Enterprise 概览

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

Integrated Dell Remote Access Controller (iDRAC6) Enterprise 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，与受管 Dell PowerEdge 服务器共存于系统板上。服务器操作系统执行应用程序；iDRAC6 监测并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。

受管服务器安装在 Dell M1000e 系统机壳（机箱）中，装有模块化电源设备、冷却风扇和机箱管理控制器 (CMC)。CMC 监测和管理机箱中安装的所有组件。可以添加冗余 CMC 以在主要 CMC 出现故障时进行热故障转移。机箱通过 LCD 显示屏、本地控制台连接及其 Web 界面提供到 iDRAC6 设备的访问。机箱中的每个刀片都有一个 iDRAC6。M1000e 中总共可以安装 16 个刀片。

所有到 iDRAC6 的网络连接都通过 CMC 网络接口（标有"GB1"的 CMC RJ45 连接端口）。CMC 通过专用内部网络发送通信到 iDRAC6 设备。此专用管理网络在服务器数据通路之外并且在操作系统的控制外，即*带外*。受管服务器的*带内*网络接口通过机箱内安装的输入/输出模块 (IOM) 来访问。

注： 建议将 iDRAC6 和 CMC 使用的机箱管理网络与生产网络隔离或分开。混合管理和生产或应用网络通信会造成拥塞或网络饱和，从而导致 CMC 和 iDRAC6 通信延迟。延迟会造成无法预料的机箱行为，比如即使运行正常，CMC 也会显示 iDRAC6 脱机。还会造成其它意外行为。

iDRAC6 网络接口默认情况下已禁用。必须对其进行配置，才能访问 iDRAC6。当 iDRAC6 已启用且在网络上配置后，可以通过 iDRAC6 Web 界面、Telnet 或 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。

IPv6 Ready 徽标认证

IPv6 Ready 徽标委员会的任务是定义 IPv6 符合性和互操作检测规范，提供自检测工具资源，并颁发 IPv6 Ready 徽标。

iDRAC6 通过了**第 2 阶段 IPv6 Ready 徽标**认证，徽标 ID 为 **02-C-000380**。有关 IPv6 Ready 徽标计划的信息，请参阅 **http://www.ipv6ready.org/**。

---

iDRAC6 安全功能

- 通过 Microsoft Active Directory、常规 LDAP Directory Service 或由本地管理的用户 ID 和密码对用户进行验证。
- 双重验证，由 SmartCCard 登录功能提供。双重验证基于用户*拥有*的设备 (Smart Card) 和*所知*的内容 (PIN)。
- 基于角色的权限，使管理员能够为每个用户配置特定权限
- 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
- 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 IP 地址范围可以配置

---

iDRAC6 Enterprise 和 vFlash 介质

iDRAC6 Enterprise 为 vFlash 介质提供 SD 卡槽。有关 iDRAC6 Enterprise 和 vFlash 介质的详情，请参阅 **support.dell.com\manuals** 上的*《硬件用户手册》*。

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

表 1-1. iDRAC6 功能列表

部件	iDRAC6 Enterprise	适用于 vFlash 介质的 iDRAC6 Enterprise
接口和标准支持		
IPMI 2.0	✓	✓
Web GUI	✓	✓
SNMP	✓	✓
WSCMAN	✓	✓
SM-CLP	✓	✓
RACADM 命令行	✓	✓
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		
基于角色授权	✓	✓
本地用户	✓	✓
Active Directory	✓	✓
双重验证	✓	✓
单一登录	✓	✓
SSL 加密	✓	✓
远程管理和补救		
远程固件更新	✓	✓
服务器功率控制	✓	✓
LAN 上串行（有代理）	✓	✓
LAN 上串行（无代理）	✓	✓
功率封顶	✓	✓
上次崩溃屏幕捕获	✓	✓
引导捕获	✓	✓
虚拟介质	✓	✓
远程文件共享	✓	✓
虚拟控制台	✓	✓
虚拟控制台共享	✓	✓
vFlash	✗	✓
监测		
传感器监测和警报	✓	✓
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	✓	✓

跟踪日志	✔	✔
远程系统日志	✔	✔
✔ = 支持；✖ = 不支持		

支持的平台

要了解最新的支持平台，请查阅 iDRAC6 自述文件和 *《Dell 系统软件支持值表》*（位于 **support.dell.com / manuals**）。

支持的操作系统

要了解最新信息，请查阅 iDRAC6 自述文件和 *《Dell 系统软件支持值表》*（位于 **support.dell.com / manuals**）。

支持的 Web 浏览器

要了解最新信息，请查阅 iDRAC6 自述文件和 *《Dell 系统软件支持值表》*（位于 **support.dell.com / manuals**）。

注： 由于安全缺陷，已停止对 SSL 2.0 的支持。确保浏览器已配置为启用 SSL 3.0。

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	• 10Mbps/100Mbs/1Gbps 以太网，通过 CMC Gb 以太网端口。 • DHCP 支持。 • SNMP 陷阱和电子邮件事件通知。 • 通过 SSH 和 Telnet 支持 SMCCLP shell 和 RACADM 命令，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。

小心： iDRAC6 不检查配置端口之间的冲突。在进行端口配置时，确保各个端口分配之间互不冲突。

表 1-3. iDRAC6 服务器侦听端口

"Port Number"（端口号）	功能
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668, 3669	虚拟介质服务
3670, 3671	虚拟介质安全服务
3672	vFlash 服务
5900*	虚拟控制台键盘/鼠标
5901*	Virtual Console 视频
5988*	用于 WSMAN

* 可配置端口

表 1-4. iDRAC6 客户端端口

"Port Number"（端口号）	功能
25	SMTP
53	DNS
68	DHCP 分配的 IP 地址
69	TFTP
162	SNMP 陷阱
636	LDAPS
3269	全局编录 (GC) LDAPS

您可能需要的其它说明文件

除了本指南以外，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。您可以在 Dell 支持网站 **support.dell.com/manuals** 上访问这些指南。在**"Manuals"（手册）**页上，单击**"Software"（软件）→"Systems Management**"（系统管理）。单击右侧的相应产品链接以访问文档。

- iDRAC6 联机帮助提供了有关使用 Web 界面的信息。
- *《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 Chassis Management Controller 用户指南》*和*《Dell 机箱管理控制器管理员参考指南》*提供了有关使用控制器（管理含有 Dell PowerEdge 服务器的机箱中的所有模块）的信息。
- *《Dell OpenManage IT Assistant 用户指南》*提供了有关使用 IT Assistant 的信息。
- *《Dell Management Console 用户指南》*提供了有关使用 Dell Management Console 的信息。
- *《Dell OpenManage Server Administrator 用户指南》*提供了有关安装和使用 Server Administrator 的信息。
- *《Dell Update Package 用户指南》*介绍了如何获取 Dell Update Package 以及如何将其用于系统更新策略中。
- *《Dell Lifecycle Controller 用户指南》*介绍了有关 Unified Server Configurator (USC)、Unified Server Configurator C Lifecycle Controller Enabled (USC C LCE) 和 Remote Services 的信息。
- Dell Enterprise 技术中心 **www.delltechcenter.com** 上提供的*《iDRAC6 CIM 组件映射》*和*《iDRAC6 SM-CLP 属性数据库》*说明文件介绍了 iDRAC6 SMCCLP 属性数据库、WSCMAN 类和 SMCCLP 目标间的映射以及 Dell 实施详情等信息。
- *《iDRAC6 管理员参考指南》*提供了有关下列内容的信息，即刀片式服务器中 iDRAC6 Enterprise 及架式或塔式服务器中 iDRAC6 Enterprise 或 Express 的 RACADM 子命令、支持的 RACADM 界面、属性数据库组和对象定义。
- *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：

- 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 **www.dell.com/regulatory_compliance** 上的"Regulatory Compliance"（管制遵循）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。
- *《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。

- 系统可能附带版本注释或自述文件，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。

目录

目录

配置 iDRAC6 Enterprise

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

本节介绍了如何建立 iDRAC6 访问以及如何配置管理环境以使用 iDRAC6。

开始之前

配置 iDRAC6 前收集以下项目：

- *Dell Chassis Management Controller Firmware 用户指南*
- *Dell Systems Management Tools and Documentation* DVD

Dell Systems Management Tools and Documentation DVD 包含以下部分：

- 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

有关详情，请参阅 Dell 支持网站 **support.dell.com / manuals** 上的《*Dell OpenManage Server Administrator 安装指南*》和《*Dell OpenManage Management Station 软件安装指南*》。

用于配置 iDRAC6 的界面

可以使用 iDRAC6 配置公用程序、iDRAC6 Web 界面、Chassis Management Controller (CMC) Web 界面、机箱 LCD 面板、本地和远程 RACADM CLI、iVMCLI 或 SM-CLP CLI 配置 iDRAC6。在受管服务器上安装操作系统和 Dell OpenManage 软件后，本地 RACADM CLI 就可用。表 2-1 说明了这些界面。

为了提高安全性，通过 iDRAC6 配置公用程序或本地 RACADM CLI 对 iDRAC6 配置的权限可使用 RACADM 命令（请参阅 **support.dell.com / manuals** 上的《*iDRAC6 管理员参考指南*》）或从 GUI（请参阅"启用或禁用本地配置访问"）禁用。

注： 同时使用一个以上的配置界面可能会产生意外的结果。

表 2-1. 配置界面

接口	说明
iDRAC6 配置公用程序	在启动时访问，iDRAC6 配置公用程序在安装新的 Dell PowerEdge 服务器时很有用。用来设置网络和基本安全功能以及启用其它功能。
iDRAC6 Web 界面	iDRAC6 Web 界面是基于浏览器的管理应用程序，可以用来交互式管理 iDRAC6 和监控受管服务器。这是日常任务（如监控系统运行状况、查看系统事件日志、管理本地 iDRAC6 用户以及启动 CMC Web 界面和虚拟控制台会话）的主要界面。
CMC Web 界面	除了监控和管理机箱外，CMC Web 界面还可用来查看受管服务器的状态，更新 iDRAC6 固件，配置 iDRAC6 网络设置，登录 iDRAC6 Web 界面以及启动、停止或重设受管服务器。
机箱 LCD 面板	可使用 iDRAC6 所在机箱上的 LCD 面板来查看机箱中服务器的高级别状态。在 CMC 初始配置期间，配置向导会允许启用 iDRAC6 网络的 DHCP 配置。
本地和远程 RACADM	本地 RACADM 命令行界面在受管服务器上运行。可以从 iDRAC6 Web 界面启动虚拟控制台会话来进行访问。当您安装 Dell OpenManage Server Administrator 时，RACADM 被安装在受管服务器上。 远程 RACADM 是运行在 Management Station 上的客户端公用程序。它在受管服务器上使用带外网络接口运行 RACADM 命令。 **–r** 选项可在网络上运行 RACADM 命令。 通过 RACADM 命令可以访问几乎所有 iDRAC6 功能。可以检查传感器数据、系统事件日志记录以及 iDRAC6 中维护的当前状态和配置值。可以变更 iDRAC6 配置值、管理本地用户、启用和禁用功能，以及执行电源功能，如关闭或重新引导受管服务器。
iVMCLI	通过 iDRAC6 虚拟介质命令行界面 (iVMCLI)，受管服务器可以访问 Management Station 上的介质。这非常有助于开发在多个受管服务器上安装操作系统的脚本。
SM-CLP	SM-CLP 是 iDRAC6 中结合的服务器管理工作组服务器管理命令行协议 (SM-CLP)。可使用 Telnet 或 SSH 登录 iDRAC6 并在 CLI 提示符处键入 `smclp` 来访问 SM-CLP 命令行。 SM-CLP 命令提供了有用的本地 RACADM 命令子集。这些命令对脚本编写很有用，因为它们可以从 Management Station 命令行执行。命令的输出可以用定义明确的格式（包括 XML）进行检索，因此非常有助于脚本编写以及与现有报告和管理工具进行集成。

IPMI	IPMI 为嵌入式管理子系统（如 iDRAC6）定义了一种与其它嵌入式系统和管理应用程序进行通信的标准方式。 可以使用 iDRAC6 Web 界面、SM-CLP 或 RACADM 命令配置 IPMI 平台事件筛选器 (PEF) 和平台事件陷阱 (PET)。 PEF 使 iDRAC6 在检测到情况时执行特定的操作（比如重新引导受管服务器）。PET 指示 iDRAC6 在检测到指定事件或情况时发送电子邮件或 IPMI 警报。 在启用 LAN 上 IPMI 后，还可以与 iDRAC6 配合使用标准 IPMI 工具，如 **IPMItool** 和 **ipmish**。

配置任务

本节概括介绍 Management Station、iDRAC6 以及受管服务器的配置任务。要执行的任务包括配置 iDRAC6 以供远程访问、配置要使用的 iDRAC6 功能、在受管服务器上安装操作系统，以及在 Management Station 和受管服务器上安装管理软件。

可以用来执行每个任务的配置任务列在任务之下。

注： 执行本指南中的配置过程之前，必须在机箱中安装并配置 CMC 和输入/输出模块，且 Dell PowerEdge 服务器必须实际安装在机箱中。

配置 Management Station

通过安装 Dell OpenManage 软件、Web 浏览器以及其它软件公用程序来设置 Management Station。请参阅"配置 Management Station"。

配置 iDRAC6 网络

启用 iDRAC6 网络并配置 IP、网络掩码、网关和 DNS 地址。

注： 为了提高安全性，通过 iDRAC6 配置公用程序或本地 RACADM CLI 对 iDRAC6 配置的权限可使用 RACADM 命令（请参阅 **support.dell.com / manuals** 上的的《*iDRAC6 管理员参考指南*》）或从 GUI（请参阅"启用或禁用本地配置访问"）禁用。

注： 更改 iDRAC6 网络设置会终止当前所有到 iDRAC6 的网络连接。

注： *只有*在 CMC 初始配置期间才可以选择使用 LCD 面板配置服务器。部署机箱后，LCD 面板不能用于重新配置 iDRAC6。

注： LCD 面板只能用来启用 DHCP 以配置 iDRAC6 网络。

- 机箱 LCD 面板 — 请参阅《*Dell Chassis Management Controller Firmware 用户指南*》
- iDRAC6 配置公用程序 — 请参阅"使用 iDRAC6 配置公用程序"
- CMC Web 界面 - 请参阅"使用 CMC Web 界面配置网络设置"
- 远程和本地 RACADM — 请参阅 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》中的 **cfgLanNetworking**。

配置 iDRAC6 用户

设置本地 iDRAC6 用户和权限。iDRAC6 在固件中设置了一个有 16 个本地用户的表。可以为这些用户设置用户名、密码和角色。

- iDRAC6 配置公用程序（仅配置管理用户）- 请参阅"LAN 用户配置"
- iDRAC6 Web 界面 — 请参阅"添加和配置 iDRAC6 用户"
- 远程和本地 RACADM - 请参阅"添加 iDRAC6 用户"

注： 在 Active Directory / 通用 LDAP Directory Service 环境中使用 iDRAC6 时，确保用户名符合生效的 Active Directory / 通用 LDAP Directory Service 命名惯例。

配置目录服务

除了本地 iDRAC6 用户，您也可以使用 Microsoft Active Directory 或常规 LDAP 目录服务验证 iDRAC6 用户登录。

有关详情，请参阅"使用 iDRAC6 目录服务"。

配置 IP 筛选和 IP 阻塞

除了用户验证，您还可以通过拒绝定义范围以外的 IP 地址连接尝试以及临时阻止在可配置时间范围内多次验证失败的 IP 地址连接来防止未授权访问。

- iDRAC6 Web 界面 — 请参阅"配置 IP 筛选和 IP 阻塞"
- RACADM — 请参阅"配置 IP 筛选（IP 范围）"和"配置 IP 阻塞"

配置平台事件

当 iDRAC6 从某个受管服务器的传感器中检测到警告或严重情况时会发生平台事件。

配置平台事件筛选器 (PEF) 以选择要检测的事件，如在检测到事件时重新启动受管服务器。

- iDRAC6 Web 界面 — 请参阅"配置平台事件筛选器 (PEF)"
- RACADM — 请参阅"配置 PEF"

配置平台事件陷阱 (PET) 以向 IP 地址发送警报通知，比如装有 IPMI 软件的 Management Station 或向指定电子邮件地址发送电子邮件。

- iDRAC6 Web 界面 — 请参阅"配置平台事件陷阱 (PET)"
- RACADM — 请参阅"配置 PET"

启用或禁用本地配置访问

可以禁用对重要配置参数的访问，例如网络配置和用户权限。一旦禁用，重新引导后该设置仍将持续保留。本地 RACADM 程序和 iDRAC6 配置公用程序（引导时）都禁止配置写入访问。Web 访问配置参数不受限制，并且可以随时查看配置数据。有关 iDRAC6 Web 界面的信息，请参阅"启用或禁用本地配置访问"。对于 RACADM 命令，请参阅 **support.dell.com / manuals** 提供的*《iDRAC6 管理员参考指南》*中的 **cfgRacTuning**。

配置 iDRAC6 服务

启用或禁用 iDRAC6 网络服务 — 如 Telnet、SSH 和 Web 服务器界面 — 并重新配置端口和其它服务参数。

- iDRAC6 Web 界面 — 请参阅"配置 iDRAC6 服务"
- RACADM — 请参阅"使用本地 RACADM 配置 iDRAC6 Telnet 和 SSH 服务"

配置安全套接字层 (SSL)

为 iDRAC6 Web Server 配置 SSL。

- iDRAC6 Web 界面 — 请参阅"安全套接字层 (SSL)"
- RACADM — 请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》中的 cfgRacSecurity、sslcsrgen、sslcertupload、sslcertdownload 和 sslcertview。

配置虚拟介质

配置虚拟介质功能以便可以在 Dell PowerEdge 服务器上安装操作系统。虚拟介质允许受管服务器访问 Management Station 上的介质设备或者网络共享的 ISO CD/DVD 映像，就好像是受管服务器上的设备一样。

- iDRAC6 Web 界面 — 请参阅"配置并使用虚拟介质"
- iDRAC6 配置公用程序 — 请参阅"Virtual Media Configuration"（虚拟介质配置）"

配置 VFlash 介质卡

安装和配置用于 iDRAC6 的 VFlash 介质卡。

- iDRAC6 Web 界面及使用 RACADM — 请参阅"配置 vFlash SD 卡及管理 vFlash 分区"

安装受管服务器软件

使用虚拟介质在 Dell PowerEdge 服务器上安装操作系统，然后在受管 Dell PowerEdge 服务器上安装 Dell OpenManage 软件并设置上次崩溃屏幕功能。

- 虚拟控制台 - 请参阅"在受管服务器上安装软件"
- iVMCLI - 请参阅"使用虚拟介质命令行界面公用程序"

配置受管服务器的上次崩溃屏幕功能

设置受管服务器以使 iDRAC6 可以在操作系统崩溃或冻结后捕获屏幕图像。

- 受管服务器 — 请参阅"配置受管服务器以捕获上次崩溃屏幕"和"禁用 Windows 自动重新引导选项"

使用 CMC Web 界面配置网络设置

注： 必须具有机箱配置管理员权限才能从 CMC 设置 iDRAC6 网络设置。

注： 默认 CMC 用户名为 **root**，密码为 **calvin**。

注： CMC IP 地址可以在 iDRAC6 Web 界面中找到，方法是单击**"System"（系统）→"Remote Access"（远程访问）→ CMC**。还可以从此屏幕启动 CMC Web 界面。

从 CMC 启动 iDRAC6 Web 界面

CMC 提供单独机箱组件（例如服务器）的有限管理。为了全面管理这些单独组件，CMC 为服务器 iDRAC6 Web 界面提供一个启动点。

从 CMC 启动 iDRAC6：

1. 登录到 CMC Web 界面。
2. 从系统树中选择**"Server Overview"（服务器概览）**。**"Servers Status"（服务器状态）**屏幕显示可用服务器的列表。
3. 单击您要管理的服务器的**"iDRAC"**。在新浏览器窗口中启动 iDRAC GUI。

从 CMC 启动单个服务器的 iDRAC6 Web 界面：

1. 登录到 CMC Web 界面。
2. 展开系统树中的**"Server Overview"（服务器概览）**。展开的**"Servers"（服务器）**列表中显示所有服务器。
3. 单击想要查看的服务器。您选择显示的服务器的**"Server Status"（服务器状况）**屏幕出现。
4. 单击**"Launch iDRAC6 GUI"（启动 iDRAC6 GUI）**。

单一登录

您可以使用单一登录功能从 CMC 启动 iDRAC6 Web 界面，而无需第二次登录。下面介绍单次登录策略。

- 拥有**"Server Administrator"（服务器管理员）**权限（在**"User Privileges"（用户权限）**下设置）的 CMC 用户会通过单一登录自动登录到 iDRAC6 Web 界面。登录后，用户被自动授予 iDRAC6 管理员权限。即便同一位用户在 iDRAC6 上没有帐户，或如果该帐户没有管理员权限，这也同样适用。
- 没有**"Server Administrator"（服务器管理员）**权限（在**"User Privileges"（用户权限）**下设置）但在 iDRAC6 上有相同帐户的 CMC 用户会通过单一登录自动登录到 iDRAC6。一旦登录到 iDRAC6 Web 界面，此用户会被授予为 iDRAC6 帐户创建的权限。

  注： 在此情况下，*相同帐户*意味着用户拥有的 CMC 用户名和密码与 iDRAC6 相同。用户名相同但密码不同的用户将被视为无效用户。

- 没有**"Server Administrator"（服务器管理员）**权限（在**"User Privileges"（用户权限）**下设置）或在 iDRAC6 上没有相同帐户的 CMC 用户不会通过单一登录自动登录到 iDRAC6。此用户在单击**"Launch iDRAC6 GUI"（启动 iDRAC6 GUI）**后会被定向到 iDRAC6 登录屏幕。

  注： 在此情况下，将提示用户登录到 iDRAC6。

  注： 如果禁用 iDRAC6 网络 LAN（LAN 已启用 = 否），单一登录不可用。

  注： 如果从机箱卸下服务器、iDRAC6 IP 地址被更改或 iDRAC6 网络连接出现问题，则单击**"Launch iDRAC6 GUI"（启动 iDRAC6 GUI）**图标将显示一个错误屏幕。

为 iDRAC6 配置网络

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6。**
2. 单击**"Network/Security"（网络/安全性）**选项卡：

   要启用或禁用 LAN 上串行：

   a. 单击**"Serial Over LAN"（LAN 上串行）**。

      "Serial Over LAN"（LAN 上串行）屏幕出现。

b. 选择**"Enable Serial Over LAN"（启用 LAN 上串行）**复选框。您也可更改**"Baud Rate"（波特率）**和**"Channel Privilege Level Limit"（信道权限级别限制）**设置。

c. 单击**"Apply"（应用）**。

要启用或禁用 LAN 上 IPMI：

a. 单击**"Network"（网络）**。

此时会出现**"Network"（网络）**屏幕。

b. 单击**"IPMI Settings"（IPMI 设置）**。

c. 选中**"Enable IPMI Over LAN"（启用 LAN 上 IPMI）**复选框。您也可更改**"Channel Privilege Level Limit"（信道权限级别限制）**和**"Encryption Key"（密钥）**设置。

d. 单击**"Apply"（应用）**。

要启用或禁用 DHCP：

a. 单击**"Network"（网络）**。

此时会出现**"Network"（网络）**屏幕。

b. 在**"IPv4 Settings"（IPv4 设置）**部分选择**"DHCP Enable"（启用 DHCP）**复选框，在**"IPv6 Settings"（IPv6 设置）**部分选择**"Autoconfiguration Enable"（启用自动配置）**复选框来启用 DHCP。要使用 DHCP 获得 DNS 服务器地址，请选择**"Use DHCP to obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**复选框。

c. 单击**"Apply"（应用）**。

注： 如果您选择不启用 DHCP，则必须输入服务器的静态 IP 地址、网络掩码和默认网关。

查看 FlexAddress 夹层卡光纤连接

M1000e 包括 FlexAddress，它是一种先进的多级、多标准网络系统。FlexAddress 允许为每个受管服务器端口连接使用永久、机箱分配的全球名称和 MAC 地址 (WWN/MAC)。

注： 为了避免可能导致无法开启受管服务器的错误，每个端口和光纤连接都*必须*安装正确类型的夹层卡。

使用 CMC Web 界面执行 FlexAddress 功能的配置。有关 FlexAddress 功能及其配置的详情，请参阅*《Dell Chassis Management Controller 用户指南》*和*《Chassis Management Controller (CMC) Secure Digital (SD) Card 技术规范》*说明文件。

为机箱启用并配置 FlexAddress 功能后，单击**"System"（系统）→"Properties"（属性）**选项卡 → **WWN/MAC** 查看所安装的夹层卡列表、它们所连接的光纤、光纤类型，以及每个已安装的嵌入式以太网和可选夹层卡端口的服务器分配或机箱分配的 MAC 地址。

"ServerCAssigned"（服务器分配）列显示嵌入控制器硬件的服务器分配的 WWN/MAC 地址。WWN/MAC 地址显示**"N/A"（无）**，表示没有为指定结构安装接口。

"ChassisCAssigned"（机箱分配）列显示用于特定插槽的机箱分配的 WWN/MAC 地址。WWN/MAC 地址显示**"N/A"（无）**，表示没有安装 FlexAddress 功能。**"ServerCAssigned"（服务器分配）**和**"ChassisCAssigned"（机箱分配）**列中的复选标记表示活动的地址。

iDRAC6 的 FlexAddress MAC

FlexAddress 功能用机箱分配的 MAC 地址代替服务器分配的 MAC 地址，并随同刀片 LOM、夹层卡和输入/输出模块一起使用于 iDRAC6。iDRAC6 FlexAddress 功能支持为机箱中 iDRAC6 保留插槽特定的 MAC 地址。机箱分配的 MAC 地址保存在 CMC 非易失性内存中，并在 iDRAC6 引导期间或更改 CMC FlexAddress 页设置的情况下发送给 iDRAC6。

如果 CMC 启用了机箱分配的 MAC 地址，iDRAC6 会在以下屏幕的**"MAC Address"（MAC 地址）**字段中显示该值：

- **"System"（系统）→"Properties"（属性）**选项卡 →**"System Details"（系统详情）→"iDRAC6 Information"（iDRAC6 信息）**
- **"System"（系统）→ "Properties"（属性）**选项卡 → **WWN/MAC**
- **"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 → "Properties"（属性）**选项卡 →**"Remote Access Information"（远程访问信息）→"Network Settings"（网络设置）**
- **"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）**选项卡 →**"Network"（网络）→"Network Interface Card Settings"（网络接口卡设置）**

小心： 启用 FlexAddress 后，如果从服务器分配的 MAC 地址切换到机箱分配的 MAC 地址或者相反，iDRAC6 IP 地址也会变化。

注： 只能通过 CMC 启用或禁用 FlexAddress 功能。iDRAC6 GUI 只报告状态。如果在 CMC FlexAddress 页中更改 FlexAddress 设置，任何现有的虚拟控制台或虚拟介质会话都会终止。

通过 RACADM 启用 FlexAddress

不能从 iDRAC6 启用 FlexAddress。从 CMC 在插槽和结构级别启用 FlexAddress。

1. 从 CMC 控制台，使用以下 RACADM 命令在插槽级别启用受管服务器的 FlexAddress：

   `racadm setflexaddr -i <slot_no> 1，<slot_no> 为要启用 FlexAddress 的插槽编号。`

2. 然后，从 CMC 控制台，通过执行以下 RACADM 命令在结构级别启用 FlexAddress：

   `racadm setflexaddr -f <fabric_name> 1，<fabric_name> 为 A、B 或 C。`

3. 要从 CMC 控制台启用机箱中所有 iDRAC6 的 FlexAddress，则执行以下 RACADM 命令：

   `racadm setflexaddr -f idrac 1`

请参阅《*Dell Chassis Management Controller 管理员参考指南*》了解有关 CMC RACADM 子命令的详情。

远程系统日志

iDRAC6 远程系统日志功能允许远程写入 RAC 日志和系统事件日志 (SEL) 到外部系统日志服务器。可以从一个中央日志中读取整个服务器场的所有日志。

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。远程系统日志条目包含在 UDP 数据包中一起传输，该数据包发送到远程系统日志服务器的系统日志端口。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。还可以通过 CMC 更改 iDRAC6 远程系统日志设置。

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 2-2 列出远程系统日志设置。

表 2-2. 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 1C3	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。
"Port Number"（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 Cg cfgRemoteHosts Co cfgRhostsSyslogEnable [1/0] ; default is 0

racadm config Cg cfgRemoteHosts Co cfgRhostsSyslogServer1 <服务器名 1> ; default is blank

racadm config Cg cfgRemoteHosts Co cfgRhostsSyslogServer2 <服务器名 2>; default is blank

racadm config Cg cfgRemoteHosts Co cfgRhostsSyslogServer3 <服务器名 3>; default is blank

racadm config Cg cfgRemoteHosts Co cfgRhostsSyslogPort <端口号>; default is 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。如果启用了引导一次，则系统只在选中的设备引导一次，且不会在引导顺序中针对性地继续做为首个引导设备。

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）**选项卡 **→"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 2-3 列出**"First Boot Device"（第一个引导设备）**设置。

表 2-3. "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。
引导一次	选中 = 启用；取消选中 = 禁用。选中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。

远程文件共享

iDRAC6 远程文件共享 (RFS) 功能允许指定网络共享上的 CD/DVD ISO 映像文件，并通过 NFS 或 CIFS 像 CD 或 DVD 一样装载它，使其作为受管服务器操作系统的虚拟驱动器。

注： 该功能只能用于 IPv4 地址。目前不支持 IPv6 地址。

注： 对于 Linux 发行版本，操作 runlevel init 3 时该功能可能会要求手动装入命令。
该命令的语法为：
mount /dev/OS_specific_device /<用户定义的装入点>
其中，<用户定义的装入点>是您选择的与任何装入命令类似的用于装入的任何目录。
对于 RHEL，CD 设备（**.iso** 虚拟设备）是 **/dev/scd0**，软盘设备（**.img** 虚拟设备）是 **/dev/sdc**。
对于 SLES，CD 设备是 **/dev/sr0**，软盘设备是 **/dev/sdc**。
为确保使用的是正确的设备（对于 SLES 或 RHEL 二者），当您连接虚拟设备时，在 Linux 操作系统上您必须立即运行该命令：
tail /var/log/messages | grep SCSI
这将显示识别该设备（如 SCSI 设备 sdc）的文本。
使用 Linux 发行版本运行 runlevel init 3 时，此过程也适用于虚拟介质。默认情况下，虚拟介质不会自动装入 init 3。

CIFS 共享映像路径的格式应为：

```
//<IP 地址或域名>/<共享名>/<映像路径>
```

NFS 共享映像路径的格式应为：

```
<IP 地址>:/<映像路径>
```

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。

以 IMG 扩展名为结尾的文件名被重定向为虚拟软盘，而以 ISO 扩展名为结尾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。

在 iDRAC6 中，远程文件共享 (RFS) 功能利用基本的虚拟介质操作。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。CMC 和 iDRAC6 中的 GUI 和命令行选项也可以关闭 RFS 连接。CMC 中的 RFS 连接始终会覆盖 iDRAC6 中已有的 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 2-4 列出远程文件共享设置。

表 2-4. 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。

Status（状态）	**"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）**建立文件共享连接。成功建立连接后，**"Connect"（连接）**按钮禁用。

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

小心： 所有字符，包括字母数字和特殊字符，都允许用于用户名、密码和映像位置，但以下字符除外：'（单引号）、"（双引号）、,（逗号）、<（小于号）和 >（大于号）。使用远程文件共享时，不允许上面列出的字符用于用户名、密码和映像位置中。

内部双 SD 模块

内部双 SD 模块 (IDSDM) 只能用于相应平台。通过使用镜像第一块 SD 卡内容的其他 SD 卡，IDSDM 对 Hypervisor SD 卡提供冗余。在系统 BIOS 设置的 **Integrated Devices（集成设备）**屏幕中将**冗余**选项设置为**镜像模式**，可将带有第二块 SD 卡的 iDRAC6 vFlash SD 卡设置为 IDSDM。启用 IDSDM 功能时，iDRAC6 vFlash SD 卡的 vFlash 功能不可用，且该卡在 IDSDM 中被设置为备用 SD 卡。有关 IDSDM 的 BIOS 选项的更多信息，请参阅 Dell 支持网站 **support.dell.com/manuals** 中的《*硬件用户手册*》。

注： 在 BIOS 设置中的**"Integrated Devices"（集成设备）**屏幕中，必须将**"Internal USB Port"（内部 USB 端口）**选项设置为**"On"（开启）**。如将该选项设置为**"Off"（关闭）**，则系统无法将 IDSDM 视为引导设备。

两块 SD 卡中的任意一块都可做为主卡。例如，如果在 IDSDM 中安装有两块新的 SD 卡，SD1 将成为"活动"或主卡。SD2 将是备份卡，并且向两块卡中进行所有文件系统 IDSDM 写入，但仅从 SD1 读取。任何时候如 SD1 发生故障或被拆除，SD2 将自动成为"活动（主）"卡。

表 2-5. IDSDM 状态

IDSDM - 镜像模式	SD 卡	vFlash SD 卡
已启用	活动（SD2 卡）	vFlash 不活动，切换为活动 SD2 卡
已禁用	活动（SD2 卡）	仅 vFlash 活动

使用 iDRAC，您可查看 IDSDM 的状态、运行状况及可用性。

SD 卡冗余状况及故障事件被记录到 SEL 中，显示在 LCD 中，其如已启用警报将生成 PET 警报。

使用 GUI 查看内部双 SD 模块状态

1. 登录至 iDRAC Web GUI。
2. 在**系统**树中，单击**"Removable Flash Media"（可移动闪速更新介质）**。显示"Removable vFlash Media"（**可移动 vFlash 介质**）页面。该页面显示以下两部分：
   - **内部双 SD 模块** — 仅当 IDSDM 为冗余模式时显示 **冗余状况**显示为**完全**。如未显示此部分，则该卡为非冗余模式状态。有效的**冗余状况**提示为：
     - **完全** — SD 卡 1 和 2 工作正常。
     - **掉失** — 其中一块或两块 SD 卡工作不正常。
   - **内部 SD 模块状况** — 通过下列信息显示 SD1 和 SD2 的 SD 卡状态：
     - 状况：

-  — 表示该卡工作正常。
-  — 表示该卡为脱机或写保护。
-  — 表示已发出一个警报。

- 位置 — SD 卡的位置。
- 联机状况 — SD1 和 SD2 卡可以为 表 2-6 中列出的状态之一。

表 2-6. SD1 和 SD2 卡状态

状态	说明
引导	正在启动控制器。
活动	该卡接收所有 SD 写入并用于 SD 读取。
等待	该卡为备用卡。正在接收所有 SD 写入的副本。
失败	在 SD 卡读取或写入期间报告一个错误
未配备	未检测到 SD 卡
脱机	在引导时，该卡的 CID 签名与 NV 存储值不同，或该卡是正在运行的复制操作的目标。
写保护	该卡由 SD 卡上的物理锁写保护。IDSDM 无法使用写保护卡。

更新 iDRAC6 固件

更新 iDRAC6 固件会在闪存中安装一个新固件映像。可以用以下任何方法更新固件：

- iDRAC6 Web 界面
- RACADM CLI
- Dell Update Package（用于 Linux 或 Microsoft Windows）
- DOS iDRAC6 固件更新公用程序
- CMC Web 界面

下载固件或更新软件包

从 **support.dell.com** 下载固件。固件映像有几种不同格式，可支持不同的更新方法。

要使用 iDRAC6 Web 界面更新 iDRAC6 固件，或使用 CMC Web 界面恢复 iDRAC6，请下载作为自解压压缩包打包的二进制映像。

要从受管服务器更新 iDRAC6 固件，为要更新的 iDRAC6 所在服务器的操作系统下载特定的 Dell Update Package (DUP)。

要使用 DOS iDRAC6 固件更新公用程序更新 iDRAC6 固件，请下载作为自解压压缩包文件打包的更新公用程序和二进制映像。

执行固件更新

注： iDRAC6 固件更新开始后，全部现有的 iDRAC6 会话都会断开连接并且不允许进行新会话，直到更新过程完成为止。

注： iDRAC6 固件更新期间，机箱风扇以 100% 速率运行。当更新完成后，会恢复为正常的风扇速度。这是正常的行为，目的为避免服务器在无法向 CMC 发送传感器信息期间过热。

要使用 Linux 或 Microsoft Windows 的 Dell Update Package，应在受管服务器上执行操作系统特定的 DUP。

使用 iDRAC6 Web 界面或 CMC Web 界面时，将固件二进制映像放在运行 Web 界面的 Management Station 可以访问的磁盘上。请参阅"更新 iDRAC6 固件"。

注： iDRAC6 Web 界面还允许将 iDRAC6 配置重设为工厂默认值。

您可以使用 CMC Web 界面或 CMC RACADM 来更新 iDRAC6 固件。此功能在 iDRAC6 固件处于正常模式和损坏时都可使用。请参阅"使用 CMC 更新 iDRAC6 固件"。

注： 如果在固件更新期间没有保留配置，iDRAC6 会为 SSL 证书生成新的 SHA1 和 MD5 密钥。因为该密钥与打开的 Web 浏览器中的密钥不同，所以连接到 iDRAC6 的所有浏览器窗口都必须在固件更新完成后关闭。如果没有关闭浏览器窗口，将显示**"Invalid Certificate"（证书无效）**错误信息。

注： 如果将 iDRAC6 固件回滚到较早版本，则删除基于 Windows 的任何 Management Station 上的现有 Internet Explorer ActiveX 浏览器插件，以允许固件安装 ActiveX 插件的兼容版本。

验证 Linux DUP 的数字签名

数字签名用于验证文件签署者的身份以及确认文件的内容自签署以来未进行修改。

如果系统上还没有安装，必须安装 Gnu Privacy Guard (GPG) 来验证数字签名。

要使用标准验证程序，请执行下列步骤：

1. 通过访问 **lists.us.dell.com** 并单击**"Dell Public GPG key"（Dell 公共 GPG 密钥）**链接来下载 Dell Linux 公共 GPG 密钥。将文件保存到本地系统。默认名称是 **linux-security- publickey.txt**。

2. 通过运行以下命令，将公共密钥导入 GPG 可信数据库：

   `gpg --import <公共密钥文件名>`

注： 必须提供私人密钥来完成此过程。

3. 为避免出现不信任密钥警告，请更改 Dell 公共 GPG 密钥的信任级别。

   a. 输入以下命令：

      `gpg --edit-key 23B66A9D`

   b. 在 GPG 密钥编辑器内，输入 `fpr`。系统将显示以下信息：

      ```
      pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group(产品组)) <linux-security@dell.com>
      Primary key fingerprint (主要密钥指纹)：4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
      ```

      如果导入密钥的指纹与以上完全相同，则说明是正确的密钥。

   c. 仍在 GPG 密钥编辑器中，输入 `trust`。以下菜单会出现：

      ```
      Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from different sources, etc.)（请确定您信任此用户的程度以正确验证其他用户的密钥[通过检查通行证，核对不同来源的指纹等]。）


        1 = I don't know or won't say (我不知道或不想说)
        2 = I do NOT trust (我不信任)
        3 = I trust marginally (我不太信任)
        4 = I trust fully (我完全信任)
        5 = I trust ultimately (我绝对信任)
        m = back to the main menu (返回主菜单)

      Your decision (您的决定)?
      ```

   d. 输入 5，然后按 <Enter> 键。以下提示会出现：

      `Do you really want to set this key to ultimate trust?（是否确定要将此密钥设置为绝对信任？） [y/n]`

   e. 输入 y <Enter> 确认选择。

   f. 输入 quit <Enter> 退出 GPG 密钥编辑器。

   必须且只能导入并验证公共密钥一次。

4. 获得所需软件包（例如 Linux DUP 或自解压压缩包）以及相关的签名文件，来源是 Dell 支持网站 **support.dell.com/support/downloads**。

   注： 每个 Linux 更新软件包均具有独立的签名文件，与更新软件包显示在同一 Web 页面上。进行验证时同时需要更新软件包及其关联签名文件。默认情况下，签名文件的名称与 DUP 文件名相同，带有 **.sign** 扩展名。例如，iDRAC6 固件映像具有关联 **.sign** 文件（**IDRAC_FRMW_LX_2.2.BIN.sign**），这与固件映像（**IDRAC_FRMW_LX_2.2.BIN**）一起包括在自解压压缩包中。要下载该文件，右击**" Download"（下载）**链接并使用**"Save Target As"（目标另存为）**选项。

5. 验证更新软件包：

   `gpg --verify <Linux Update Package 签名文件名> <Linux Update Package 文件名>`

以下示例说明了验证 Dell PowerEdge M610 iDRAC6 更新软件包时必须执行的步骤：

1. 从 **support.dell.com** 下载以下两个文件：

   - IDRAC_FRMW_LX_2.2.BIN.sign
   - IDRAC_FRMW_LX_2.2.BIN

2. 通过运行以下命令行导入公共密钥：

   `gpg --import <linux-security-publickey.txt>`

以下输出信息会出现：

```
gpg: key 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed（gpg: key 23B66A9D:
("Dell Computer Corporation (Linux 系统组) <linux-security@dell.com>" 没有更改
gpg: Total number processed: 1（gpg: 处理的总数: 1））
gpg: unchanged: 1（gpg: 未更改: 1）
```

3. 如果以前没有为 Dell 公共密钥设置 GPG 信任水平，则执行此操作。

   a. 输入以下命令：

   ```
   gpg --edit-key 23B66A9D
   ```

   b. 在命令提示符处，输入以下命令：

   ```
   fpr
   trust
   ```

   c. 输入 5，然后按 <Enter>，从菜单中选择"I trust ultimately"（我绝对信任）。

   d. 输入 y <Enter> 确认选择。

   e. 输入 quit <Enter> 退出 GPG 密钥编辑器。

   这将完成 Dell 公共密钥的验证。

4. 通过运行以下命令验证 Dell PowerEdge M610 iDRAC6 软件包数字签名：

   ```
   gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign IDRAC_FRMW_LX_2.2.BIN
   ```

   以下输出信息会出现：

   ```
   gpg: Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D (gpg: 签名时间 2008 星期五七月 11 日 15:03:47 CDT，使用 DSA
   秘钥 ID 23B66A9D)
   gpg: Good signature from "Dell, Inc. (Product Group) <linux-security@dell.com>" (gpg: 来自 "Dell, Inc.(产品组） <linux-
   security@dell.com>" 的有效签名)
   ```

如果没有按步骤 3 所示验证密钥，将会收到更多信息：

```
gpg: WARNING: This key is not certified with a trusted signature!（警告：此密钥未经可信签名确认！）
gpg: There is no indication that the signature belongs to the owner.（没有迹象显示此签名属于所有者。）
Primary key fingerprint (主要密钥指纹)：4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
```

使用 iDRAC6 Web 界面

注： 如果 iDRAC6 固件更新进度在完成前被中断，iDRAC6 固件可能损坏。在这种情况下，可以使用 CMC 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，可以选择将 iDRAC6 配置重设为工厂默认值。如果将配置设置为工厂默认值，外部网络访问会在更新完成后被禁用。必须使用 iDRAC6 配置公用程序启用并配置网络。

1. 启动 iDRAC6 Web 界面。

2. 在系统树中选择**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6**。

3. 单击**"Update"（更新）**选项卡。

   "**Firmware Update"（固件更新）**屏幕出现。

   注： 要更新固件，必须将 iDRAC6 置于更新模式。在该模式中，即使取消更新过程，iDRAC6 也会自动重设。

4. 在"**Upload"（上载）**部分中，单击**"Browse"（浏览）找到**下载的固件映像。也可在文本字段中输入路径。例如：

   C:\Updates\V2.2\<*映像名称*>。

   默认固件映像名称为 **firmimg.imc**。

5. 单击**"Upload"（上载）**。

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

   注： 在上载过程中，您可单击**"Cancel"（取消）**中止固件升级过程。单击**"Cancel"（取消）**会将 iDRAC6 重设到正常工作模式。

   上载完成后，显示**"Upload (Step 2 of 3)"（上载[第 2 步，共 3 步]）**屏幕。

- 如果映像文件成功上载并通过所有验证检查，会出现一条说明固件映像已验证的信息。
- 如果映像未成功上载，或未能通过验证检查，则固件更新将返回到**"Firmware Update"（固件更新）**屏幕。您可尝试再次升级 iDRAC6 或单击**"Cancel"（取消）**将 iDRAC6 重设为正常工作模式。

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 被禁用，且您不能登录到 iDRAC6 Web 界面。必须在 BIOS 开机自检期间使用 **iDRAC6 配置公用程序**或通过 CMC 重新配置 LAN 设置。

6. 在默认情况下，**"Preserve Configuration"（保留配置）**选项被启用（选中），以便在升级后将当前设置保留在 iDRAC6 上。如果不想保留这些设置，则清除**"Preserve Configuration"（保留配置）**复选框。
7. 单击**"Begin Update"（开始更新）**开始升级过程。请不要中断升级过程。
8. 在**"Upload (Step 3 of 3)"（上载 [第 3 步，共 3 步]）**窗口中，将看到更新状况。固件升级操作的进度以百分比形式衡量，将显示在**"Progress"（进度）**列中。
9. 固件更新完成后，**"Upload (Step 3 of 3)"（上载[第 3 步，共 3 步]）**窗口将刷新结果，iDRAC6 将自动重设。必须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。

使用 RACADM 更新 iDRAC6 固件

可以使用远程 RACADM 更新 iDRAC6 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.imc
   ```

2. 运行以下 RACADM 命令：

   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.imc** 的位置。

使用 DOS 更新公用程序

要使用 DOS 更新公用程序更新 iDRAC6 固件，请引导受管服务器进入 DOS，然后执行 **idrac16d** 命令。该命令的语法为：

```
idrac16d [-f] [-i=<文件名>] [-l=<日志文件>]
```

当不带选项执行时，**idrac16d** 命令会使用当前目录中的固件映像文件 **firmimg.imc** 更新 iDRAC6 固件。

其选项有：

- `-f` — 强制更新。`-f` 选项可用来将固件*降级*为较早的映像。
- `-i=<文件名>` — 指定固件映像的文件名。如果固件文件名已从默认名称 **firmimg.imc** 更改，则本选项是必需的。
- `-l=<日志文件>` — 记录来自更新活动的输出。此选项用于调试。

注： 如果为 **idrac16d** 命令输入了错误参数，或提供了 `-h` 选项，则会在用法输出中看到另外的选项 `-nopresconfig`。此选项用于在不保留任何配置信息的情况下更新固件。建议**不**使用此选项，因为它会*删除*现有的所有 iDRAC6 配置信息，包括 IP 地址、用户和密码。

更新 USC 修复软件包

请参阅《*Dell Lifecycle Controller 用户指南*》了解从 iDRAC6 Web 界面更新 USC 修复软件包的信息。

配置 iDRAC6 与 IT Assistant 配合使用

Dell OpenManage IT Assistant 可查找符合简单网络管理协议 (SNMP) 版本 1 和版本 2c 以及智能平台管理接口 (IPMI) 版本 2.0 的受管理设备。

iDRAC6 符合 IPMI 版本 2.0。本节说明将 iDRAC6 配置为可被 IT Assistant 查找和监控的必要步骤。有两种方法可完成此操作：通过 iDRAC6 配置公用程序和通过 iDRAC6 的图形 Web 界面。

使用 iDRAC6 配置公用程序启用查找和监控

要在 iDRAC6 配置公用程序级别设置 iDRAC6 以进行 IPMI 查找和警报陷阱发送，请重新启动受管服务器（刀片），并使用虚拟控制台，以及远程监控器和控制台键盘或 LAN 上串行 (SOL) 连接观察启动过程。当显示"Press <Ctrl-E> for Remote Access Setup"（按 <Ctrl-E> 进行远程访问设置）时，按 <Ctrl><E>。

当出现**"iDRAC6 Configuration Utility"（iDRAC6 配置公用程序）**屏幕时，使用箭头键向下滚动。

1. 启用 **LAN 上 IPMI**。
2. 输入站点的**"RMCP+ Encryption Key"（RMCP+ 密钥）**（如果已使用）。

注： 请与高级网络管理员或 CIO 联系，讨论此选项的实施，因为这样会增加宝贵的安全保护，必须在整个站点实施才能正常运行。

3. 在**"LAN Parameters"（LAN 参数）**中，按 <Enter> 以进入子屏幕。使用上下箭头导航。
4. 使用空格键将**"LAN Alert Enabled"（LAN 警报已启用）**切换到**"On"（开）**。
5. 将 Management Station 的 IP 地址输入到**"Alert Destination 1"（警报目标 1）**中。
6. 按照在数据中心生效的统一命名惯例在**"iDRAC6 Name"（iDRAC6 名称）**中输入名称字符串。默认值是 iDRAC6-{*服务标签*}。

通过按 <Esc>、<Esc>，然后按 <Enter> 退出 iDRAC6 配置公用程序，以保存所做的更改。服务器现在将引导到正常运行，IT Assistant 在预定的下次查找过程中将发现该服务器。

注： 还可以使用 Dell Management Console 这个下一代一对多系统管理应用程序来启用查找和监控。请参阅 Dell 支持网站 **support.dell.com / manuals** 上的《*Dell Management Console 用户指南*》了解详情。

使用 iDRAC6 Web 界面启用查找和监控

还可以通过远程 Web 界面启用 IPMI 查找：

1. 打开支持的 Web 浏览器窗口。
2. 使用具有管理员权限的登录名和密码登录到 iDRAC6 Web 界面。
3. 在系统树中选择**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6**。
4. 单击**"Network / Security"（网络 / 安全性）**选项卡。

   此时会出现**"Network"（网络）**屏幕。
5. 单击**"IPMI Settings"（IPMI 设置）**。
6. 确保**"Enable IPMI Over LAN"（启用 LAN 上 IPMI）**复选框已选中。
7. 从**"Channel Level Privileges"（信道级别权限）**下拉式菜单中选择**"Administrator"（管理员）**。
8. 输入站点的**"RMCP+ Encryption Key"（RMCP+ 密钥）**（如果已使用）。
9. 如果在此屏幕上做出了任何修改，单击**"Apply"（应用）**。
10. 在系统树中选择**"System"（系统）**。
11. 单击**"Alert Management"（警报管理）**选项卡，然后单击**"Platform Events"（平台事件）**。

    此时出现**"Platform Events"（平台事件）**屏幕，显示您可配置 iDRAC6 生成电子邮件警报的事件列表。
12. 选择**"Generate Alerts"（生成警报）** 列中的复选框，启用一个或多个事件的电子邮件警报。
13. 如果在此屏幕上做出了任何修改，单击**"Apply"（应用）**。
14. 单击**"Trap Settings"（陷阱设置）**。

将会显示**"Trap Settings"（陷阱设置）**屏幕。

15. 在**"IPv4 Destination List"（IPv4 目标列表）**部分的第一个可用**"Destination IP Address"（目标 IP 地址）**字段中，选择**"Enabled"（已启用）**复选框，然后输入 Management Station 的 IP 地址。

16. 如果在此屏幕上做出了任何修改，单击**"Apply"（应用）**。

现在可以单击**"Test Trap"（检测陷阱）**列中的**"Send"（发送）**链接发送一个检测陷阱。

Dell 强烈建议，为了安全起见，使用自己的用户名、LAN 上 IPMI 权限和密码为 IPMI 命令创建单独的用户：

1. 在系统树中选择**"System"（系统）**→**"Remote Access"（远程访问）**→ **iDRAC6**。

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

   此时**"Users"（用户）**屏幕出现，显示所有用户（已定义或未定义）的列表。

3. 单击一个未定义用户的**"User ID"（用户 ID）**。

   将显示已选定用户 ID 的**"User Configuration"（用户配置）**屏幕。

4. 选择**"Enable User"（启用用户）**复选框，然后输入用户名和密码。

5. 在**"IPMI LAN Privilege"（IPMI LAN 权限）**部分中，确保**"Maximum LAN User Privilege Granted"（授予的最大 LAN 用户权限）**设置为**"Administrator"（管理员）**。

6. 根据需要设置其它用户权限。

7. 单击**"Apply"（应用）**保存新用户设置。

使用 IT Assistant 查看 iDRAC6 状态和事件

完成查找后，iDRAC6 设备将显示在 **"ITA Devices detail"（ITA 设备详情）**屏幕的 **"Servers"（服务器）**类别中，而且可以通过单击 iDRAC6 名称来查看 iDRAC6 信息。这与 DRAC 5 系统不同，在 DRAC 5 系统中，管理卡显示在 RAC 组中。

现在，可以在 IT Assistant 的主要**"Alert Log"（警报日志）**中看到 iDRAC6 错误和警告陷阱。这些内容显示在**"Unknown"（未知）**类别中，但陷阱说明和严重性将是准确的。

有关使用 IT Assistant 管理数据中心的详情，请参阅*《Dell OpenManage IT Assistant 用户指南》*。

注： 还可以使用 Dell Management Console 这个下一代一对多系统管理应用程序来查看 iDRAC6 状态和事件。请参阅 Dell 支持网站 **support.dell.com/manuals** 上的*《Dell Management Console 用户指南》*了解详情。

目录

目录

配置 Management Station

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

Management Station 是用于监控和管理 Dell PowerEdg 服务器及机箱中其它模块的计算机。本节说明了设置 Management Station 以与 iDRAC6 Enterprise 配合使用的软件安装和配置任务。开始配置 iDRAC6 之前，遵循本节中的步骤确保已安装并配置了所需工具。

Management Station 设置步骤

要设置 Management Station，应执行下列步骤：

1. 设置 Management Station 网络。
2. 安装并配置一个支持的 Web 浏览器。
3. 安装 Java Runtime Environment (JRE)（如果使用 Firefox，则必须安装）。
4. 安装 Telnet 或 SSH 客户端（如果需要）。
5. 安装 TFTP 服务器（如果需要）。
6. 安装 Dell OpenManage IT Assistant（可选）。
7. 安装 Dell Management Console（可选）。

Management Station 网络要求

要访问 iDRAC6，Management Station 必须与标有"GB1"的 CMC RJ45 连接端口位于同一网络。有可能将 CMC 网络与受管服务器所在的网络隔离开，以便 Management Station 可以对 iDRAC6 而不是受管服务器进行 LAN 访问。

使用 iDRAC6 虚拟控制台功能（请参阅"配置和使用 LAN 上串行"），可以访问受管服务器的控制台，即使不能从网络访问服务器端口。还可以使用 iDRAC6 功能在受管服务器上执行几种管理功能，比如重新引导计算机。但是，要访问网络和受管服务器上托管的应用程序服务，可能需要在受管服务器中有另外的 NIC。

配置支持的 Web 浏览器

以下各节介绍如何配置所支持的 Web 浏览器以用于 iDRAC6 Web 界面。

打开 Web 浏览器

iDRAC6 Web 界面设计为在所支持的 Web 浏览器中查看，屏幕最小分辨率为 800（宽）x 600（高）像素。为了能够查看该界面并访问所有功能，请确保将分辨率设置为至少 800 x 600 像素，和/或根据需要调整浏览器的大小。

注： 某些情况下，通常在固件更新后的第一次会话期间，Internet Explorer 用户在浏览器的状态栏中会看到信息**"Done, with errors"（已完成，但网页上有错误）**，同时主浏览器窗口仅显示部分屏幕。遇到连接问题时也会出现此错误。这是 Internet Explorer 的已知问题。请关闭浏览器并重启。

配置 Web 浏览器以连接到 Web 界面

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

要配置 Internet Explorer Web 浏览器来访问代理服务器，应执行下列步骤：

1. 打开 Web 浏览器窗口。

2. 单击**"Tools"（工具）**并单击**"Internet Options"（Internet 选项）**。

   屏幕将显示**"Internet Options"（Internet 选项）**窗口。

3. 选择**"Tools"（工具）**→**"Internet Options"（Internet 选项）**→**"Security"（安全）**→**"Local Network"（本地网络）**。

4. 单击**"Custom Level"（自定义级别）**。

5. 从下拉式菜单中选择**"Medium-Low"（中低）**，然后单击**"Reset"（重设）**。单击**"OK"（确定）**以确认配置。需要通过单击**"Custom Level"（自定义级别）**按钮重新进入此对话框。

6. 然后向下滚动到标记为"ActiveX controls and plug-ins"（ActiveX 控件和插件）的部分，检查每项设置，因为不同的 IE 版本在**"Medium-Low"（中低）**状态下具有不同的设置：

   - Automatic prompting for ActiveX controls（ActiveX 控件自动提示）：Enable（启用）
   - Binary and script behaviors（二进制和脚本行为）：Enable（启用）
   - Download signed ActiveX controls（下载已签名的 ActiveX 控件）：Prompt（提示）
   - Initialize and script ActiveX controls not marked as safe（对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本）：Prompt（提示）
   - Run ActiveX controls and plug-ins（运行 ActiveX 控件和插件）：Enable（启用）
   - 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）：Enable（启用）

   在**"Downloads"（下载）**部分中：

   - Automatic prompting for file downloads（文件下载的自动提示）：Enable（启用）
   - File download（文件下载）：Enable（启用）
   - Font download（字体下载）：Enable（启用）

   在**"Miscellaneous"（其他）**部分中：

   - Allow META-REFRESH（允许 META REFRESH）：Enable（启用）
   - Allow scripting of Internet Explorer Web browser control（允许 Internet Explorer 网页浏览器控件的脚本）：Enable（启用）
   - Allow script-initiated windows without size or position constraints（允许由脚本初始化的窗口，不受大小和位置限制）：Enable（启用）
   - Don't prompt for client certificate selection when no certificates or only one certificate exists（没有证书或只有一个证书时不提示进行客户端证书选择）：Enable（启用）
   - Launching programs and files in an IFRAME（在 IFRAME 中启动程序和文件）：Enable（启用）
   - Open files based on content, not file extension（基于内容打开文件，而不是基于文件扩展名）：Enable（启用）
   - Software channel permissions（软件频道权限）：Low safety（安全级 - 低）
   - Submit nonencrypted form data（提交非加密表单数据）：Enable（启用）
   - Use Pop-up Blocker（使用弹出窗口阻止程序）：Disable（禁用）

   在**"Scripting"（脚本）**部分中：

   - Active scripting（活动脚本）：Enable（启用）
   - Allow paste operations via script（允许通过脚本进行粘贴操作）：Enable（启用）
   - Scripting of Java applets（Java 小程序脚本）：Enable（启用）

- 选择**"Tools"（工具）**→**"Internet Options"（Internet 选项）**→**"Advanced"（高级）**。
- 确保选中或取消选中以下各项：

  在**"Browsing"（浏览）**部分中：

  - Always send URLs as UTF-8（总是以 UTF-8 发送 URL）：选中
  - Disable script debugging (Internet Explorer)（禁用脚本调试 (Internet Explorer)）：选中
  - Disable script debugging: (Other)（禁用脚本调试（其他））：选中
  - Display a notification about every script error（显示每个脚本错误的通知）：取消选中
  - Enable Install On demand (Other)（启用即需安装（其他））：选中
  - Enable page transitions（允许页面转换）：选中
  - Enable third-party browser extensions（启用第三方浏览器扩展）：选中
  - Reuse windows for launching shortcuts（再次使用窗口来启动快捷方式）：取消选中

在**"HTTP 1.1 settings"（HTTP 1.1 设置）**部分中：

- Use HTTP 1.1（使用 HTTP 1.1）：选中
- Use HTTP 1.1 through proxy connections（通过代理连接使用 HTTP 1.1）：选中

在 **Java (Sun)** 部分中：

- Use JRE 1.6.x_yz（使用 JRE 1.6.x_yz）：选中（可选，版本可能不同）

在**"Multimedia"（多媒体）**部分中：

- Enable automatic image resizing（启用自动图像大小调整）：选中
- Play animations in Web pages（播放网页中的动画）：选中
- Play videos in Web pages（播放网页中的视频）：选中
- Show pictures（显示图片）：选中

在**"Security"（安全）**部分中：

- Check for publishers' certificate revocation（检查发行商的证书是否吊销）：取消选中
- Check for signatures on downloaded programs（检查下载的程序的签名）：取消选中
- Check for signatures on downloaded programs（检查下载的程序的签名）：选中
- Use SSL 2.0（使用 SSL 2.0）：取消选中
- Use SSL 3.0（使用 SSL 3.0）：选中
- Use TLS 1.0（使用 TLS 1.0）：选中
- Warn about invalid site certificates（对无效站点证书发出警告）：选中
- Warn if changing between secure and not secure mode（在安全和非安全模式之间转换时发出警告）：选中
- Warn if forms submittal is being redirected（重定向提交的表单时发出警告）：选中

注： 如果选择更改以上任何设置，建议您先了解这样做的后果。例如，如果选择阻止弹出窗口，iDRAC6 Web 界面的某些部分将无法正常运行。

9. 单击**"Apply"（应用）**，然后单击**"OK"（确定）**。
10. 单击**"Connections"（连接）**选项卡。
11. 在**"Local Area Network (LAN) settings"（局域网 [LAN] 设置）**下，单击**"LAN Settings"（局域网设置）**。
12. 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。
13. 单击**"OK"（确定）**两次。
14. 关闭并重新启动浏览器，确保所有更改都生效。

将 iDRAC6 添加到可信域列表

通过 Web 浏览器访问 iDRAC6 Web 界面时，如果可信域列表中缺少 iDRAC6 IP 地址，则系统会提示用户将该 IP 地址添加到列表中。完成后，单击**"Refresh"（刷新）**或重新启动 Web 浏览器即可连接到 iDRAC6 Web 界面。

在有些操作系统上，如果可信域列表中缺少 iDRAC6 IP 地址，Internet Explorer (IE) 8 系统不会提示用户将该 IP 地址添加到列表中。

注： 当连接至带有浏览器不信任证书的 iDRAC Web 界面时，在确认首次警告后，可能会再次显示浏览器证书错误警告。这是为确保安全而采取的预期行为。

要在 IE 8 中将 iDRAC6 IP 添加到可信域列表中，请执行以下操作：

1. 选择**"Tools"（工具）→ "Internet Options"（Internet 选项）→ "Security"（安全）→ "Trusted sites"（信任的站点）→ Sites（站点）**。
2. 在**"Add this website to the zone"（将该网站添加到区域）**中输入 iDRAC6 IP 地址 。
3. 单击**"Add"**（添加）。
4. 单击**"OK"（确定）**。
5. 单击**"Close"**（关闭）。

6. 单击**"OK"（确定）**然后刷新浏览器。

第一次通过装有 Active-X 插件的 IE 8 启动虚拟控制台时，会显示"Certificate Error: Navigation Blocked"（证书错误：导航被阻止）信息。

1. 单击**"Continue to this website"（继续转至本网站）**。

2. 在**"Security Warning"（安全警告）**窗口中单击**"Install"（安装）**可安装 Active-X 控件。

启动虚拟控制台会话。

查看 Web 界面的本地化版本

iDRAC6 Web 界面支持以下操作系统语言：

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

括号中的 ISO 标识符表示受支持的特定语言变量。使用其它方言或语言的界面不受支持，并有可能无法按照预期方式工作。对某些受支持的语言，要查看全部功能，可能需要将浏览器窗口的大小调整为 1024 像素宽。

iDRAC6 Web 界面设计用于与上面列出的特定语言变量的本地化键盘配合工作。iDRAC6 Web 界面的某些功能（例如虚拟控制台）可能需要额外的步骤才能访问特定功能/字母。有关在这些情况下如何使用本地化键盘的信息，请参阅"使用 Video Viewer"。使用其它键盘不受支持，并有可能导致异常问题。

注： 请参阅浏览器文档了解如何配置或设置不同的语言并查看本地化版本的 iDRAC6 Web 界面。

在 Linux 中设置区域

虚拟控制台查看器需要 UTF-8 字符集才能正确显示。如果显示乱码，应检查区域设置并根据需要重设字符集。

要在 Linux 客户端上设置简体中文 GUI 的字符集：

1. 打开命令终端。

2. 输入 locale 并按 <Enter> 键。类似以下的输出将会显示：

```
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. 用文本编辑器编辑 **/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。

从其它语言切换时，应确保此修补仍然有效。如果不行，请重复此步骤。

禁用 Firefox 中的白名单功能

Firefox 具有"白名单"安全功能，需要用户权限才能为各个运行插件程序的不同站点安装插件程序。如果已启用，白名单功能会要求为访问的每个 iDRAC6 安装虚拟控制台查看器，即使查看器版本都一样。

要禁用白名单功能并避免重复不必要的插件安装，应执行下列步骤：

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

   "Preference Name"（首选项名称）、**"Status"（状态）**、**"Type"（类型）**和**"Value"（值）**的值会更改为粗体文本。**"Status"（状态）**值会更改为**"user set"（用户设置）**，而**"Value"（值）**的值会更改为 **false**。
4. 在**"Preferences Name"（首选项名称）**列中，找到 **xpinstall.enabled**。

   确保**"Value"（值）**为 **true**。如果不是，双击 **xpinstall.enabled** 以将**"Value"（值）**设置为 **true**。

在 Management Station 上安装 iDRAC6 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

在 Management Station 上安装和卸载 RACADM

要使用远程 RACADM 功能，请在 Management Station 上安装 RACADM。请参阅 **support.dell.com/manuals** 上的 *《Dell OpenManage Management Station 软件安装指南》*，了解有关如何在运行 Microsoft Windows 操作系统的 Management Station 上安装 DRAC 工具的信息。

在 Linux 上安装和卸载 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**。

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 iDRAC6 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
```

安装 Java Runtime Environment (JRE)

注： 如果使用 Internet Explorer，则会为虚拟控制台查看器提供 ActiveX 控件。如果安装了 JRE 并且在启动查看器前在 iDRAC6 Web 界面中配置了虚拟控制台查看器，则还可以将 Java 虚拟控制台查看器用于 Firefox。有关详情，请参阅"在 iDRAC6 Web 界面上配置虚拟控制台和虚拟介质"。

可以选择在启动查看器前使用 Java 查看器作为替代。

如果使用 Firefox 浏览器，则必须安装 JRE（或 Java Development Kit [JDK]）以使用虚拟控制台功能。虚拟控制台查看器是一个 Java 应用程序，从 iDRAC6 Web 界面下载到 Management Station，然后用 Management Station 上的 Java Web Start 启动。

转至 **java.sun.com** 安装 JRE 或 JDK。推荐版本 1.6 (Java 6.0) 或更高。

Java Web Start 程序将自动与 JRE 或 JDK 一同安装。文件 **jviewer.jnlp** 将下载到桌面，并出现对话框提示如何完成后续操作。可能需要将 **.jnlp** 扩展名类型与浏览器中的 Java Web Start 应用程序相关联。否则，单击**"Open with"（打开方式）**，然后选择 javaws 应用程序，该程序位于 JRE 安装目录的 bin 子目录中。

注： 如果安装 JRE 或 JDK 后没有将 **.jnlp** 文件类型与 Java Web Start 相关联，可以手动设置关联。对于 Windows (**javaws.exe**)，单击**"Start"（开始）→"Control Panel"（控制面板）→"Appearance and Themes"（外观和主题）→"Folder Options"（文件夹选项）**。在**"File Types"（文件类型）**选项卡中，在**"Registered file types"（已注册的文件类型）**下高亮度显示 **.jnlp**，然后单击**"Change"（更改）**。对于 Linux (**javaws**)，启动 Firefox 并单击**"Edit"（编辑）→"Preferences"（首选项）→"Downloads"（下载）**，然后单击**"View and Edit Actions"（查看和编辑操作）**。

对于 Linux，安装 JRE 或 JDK 后，可以将指向 Java bin 目录的路径添加到系统 PATH 前面。例如，如果 Java 安装在 /usr/java，则在本地 .bashrc 或 /etc/profile 中添加下面这行内容：

```
PATH=/usr/java/bin:$PATH; export PATH
```

注： 文件中可能已经存在 PATH-modification 行。确保输入的路径信息不会产生冲突。

安装 Telnet 或 SSH 客户端

默认情况下，iDRAC6 Telnet 服务已禁用而 SSH 服务已启用。由于 Telnet 是一种不安全的协议，因此只应在无法安装 SSH 客户端或者网络连接有安全保障时才使用。

注： iDRAC6 支持同时多达 4 个 Telnet 会话和 4 个 SSH 会话。

与 iDRAC6 配合使用 Telnet

Telnet 包括在 Windows 和 Linux 操作系统中，可以从命令 shell 运行。还可以选择安装其它商用或免费提供的比操作系统标准版本具有更多方便功能的 Telnet 客户端。

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。

要将 Microsoft Telnet 客户端配置为使用 <Backspace> 键，请执行下列步骤：

1. 打开命令提示符窗口（如果需要）。
2. 如果没有运行 Telnet 会话，应输入：

   ```
   telnet
   ```

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

   ```
   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 会话以使用 <Backspace> 键，应执行下列步骤：

1. 打开 shell 并输入：

   ```
   stty erase ^h
   ```
2. 在提示符下输入：

   ```
   telnet
   ```

与 iDRAC6 配合使用 SSH

Secure Shell (SSH) 是一种命令行连接，具有与 Telnet 会话相同的功能，但具有会话协议和加密功能以加强安全性。iDRAC6 支持具有密码验证的 SSH 版本 2。SSH 默认情况下在 iDRAC6 上已启用。

可以在 Management Station 上使用 PuTTY 或 OpenSSH 等免费程序连接到受管服务器的 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。此信息文本取决于客户端，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）。

iDRAC6 支持同时多达 4 个 Telnet 会话和 4 个 SSH 会话。不过，8 个会话中只有一个可以使用 SM-CLP。即，iDRAC6 一次只支持一个 SM-CLP 会话。会话超时由 cfgSsnMgtSshIdleTimeout 属性（请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》）控制。

iDRAC6 SSH 实现支持多种密码模式，如表 3-1 中所示。

注： 不支持 SSHv1。

表 3-1. 密码模式

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
信息完整性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
验证	• "Password"（密码）

安装 TFTP 服务器

注： 如果只使用 iDRAC6 Web 界面传输 SSL 证书和上载新 iDRAC6 固件，则不需要 TFTP 服务器。

小型文件传输协议 (TFTP) 是一种简化的文件传输协议 (FTP)。用于 SM-CLP 和 RACADM 命令行界面与 iDRAC6 相互传输文件。

只有在更新 iDRAC6 固件或在 iDRAC6 上安装证书时，才需要将文件复制到 iDRAC6 或从 iDRAC6 复制文件。如果在执行这些任务时选择使用 RACADM，TFTP 服务器必须在 iDRAC6 可以通过 IP 地址或 DNS 名称访问的计算机上运行。

可以在 Windows 或 Linux 操作系统上使用 netstat -a 命令查看 TFTP 服务器是否已在侦听。端口 69 是 TFTP 默认端口。如果没有服务器运行，则可做以下选择：

- 在网络上查找另一个运行 TFTP 服务的计算机。
- 如果正在使用 Linux，则从分发包中安装 TFTP 服务器。
- 如果正在使用 Windows，则安装商用或免费 TFTP 服务器

安装 Dell OpenManage IT Assistant

系统包括了 Dell OpenManage System Management 软件套件。此套件包括但不限于以下组件：

- *Dell Systems Management Tools and Documentation* DVD
- Dell 支持网站和自述文件 — 检查自述文件和 Dell 支持网站 **support.dell.com / manuals** 以了解有关 Dell 产品的最新信息。

有关安装 IT Assistant 的信息，请参阅《*Dell OpenManage IT Assistant 用户指南*》，网址为 **support.dell.com / manuals**。

安装 Dell Management Console

Dell Management Console (DMC) 是新一代一对多系统管理应用程序，提供类似于 Dell OpenManage IT Assistant 的功能，并且还提供增强的查找、资源清册、监控和报告功能。它是基于 Web 的 GUI，安装在网络环境中的 Management Station 上。

可以从 *Dell Management Console* DVD 安装 DMC 或从 Dell 网站 **www.dell.com/openmanage** 下载并安装。

请参阅 **support.dell.com/manuals** 上的《*Dell Management Console 用户指南*》了解如何安装该软件。

目录

目录

配置受管服务器

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

本节介绍了设置受管服务器以增强远程管理能力的各种任务。这些任务包括安装 Dell Open Manage Server Administrator 软件以及配置受管服务器以捕获上次崩溃屏幕。

在受管服务器上安装软件

Dell 管理软件包括以下功能：

- RACADM CLI — 允许配置和管理 iDRAC6。这是一种用于脚本配置和管理任务的强大工具。
- Server Administrator — 使用 iDRAC6 上次崩溃屏幕功能所必需的软件。
- Server Administrator Instrumentation Service — 能够访问由业界标准系统管理代理程序收集的故障和性能详细信息，并允许远程管理所监控的系统，包括关机、启动和安全性。
- Server Administration Storage Management Service — 以综合的图形化视图提供存储管理信息。
- Server Administrator 日志 — 显示各种信息日志，如系统发出或收到的命令、监测的硬件事件、POST 事件以及系统警报。您可以在主页上查看日志，打印日志或将日志保存为报告，以及通过电子邮件将其发送到指定服务联络地址。

使用 *Dell Systems Management Tools and Documentation* DVD 安装 Dell OpenManage Server Administrator。有关安装此软件的说明，请参阅《*Dell OpenManage Server Administrator 安装指南*》，网址为：**support.dell.com / manuals**。

配置受管服务器以捕获上次崩溃屏幕

iDRAC6 可以捕获上次崩溃屏幕以便用户在 Web 界面中查看，从而帮助诊断受管服务器崩溃的原因。请按照以下步骤启用上次崩溃屏幕功能。

1. 安装受管服务器软件。有关详情，请参阅《*Dell OpenManage Server Administrator 安装指南*》和《*Dell OpenManage Management Station 软件安装指南*》。您可以在 Dell 支持网站 **support.dell.com / manuals** 上访问这些文档。

2. 如果运行的是 Windows，确保在**"Windows Startup and Recovery Settings"（Windows 启动和恢复设置）**中取消选择**"Automatically Reboot"（自动重新引导）**。请参阅"禁用 Windows 自动重新引导选项"。

3. 在 iDRAC6 Web 界面中启用**上次崩溃屏幕**（默认已禁用）。

   要在 iDRAC6 Web 界面中启用**"Last Crash Screen"（上次崩溃屏幕）**，请单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network / Security"（网络 / 安全性）**选项卡 **→"Services"（服务）**，然后选中**"Automatic System Recovery Agent Settings"（自动系统恢复代理设置）**标题下的**"Enabled"（启用）**复选框。

   要使用本地 RACADM 启用上次崩溃屏幕，在受管服务器上打开命令提示符并输入以下命令：

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

4. 在 Server Administrator Web 界面中，启用**"Auto Recovery"（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）**。

   有关如何配置**"Auto Recovery"（自动恢复）**计时器的信息，请参阅《*Dell OpenManage 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）**计时器应设置为 60 秒。默认设置为 480 秒钟。

   "Auto Recovery"（自动恢复）操作设置为**"Shutdown"（关机）**或**"Power Cycle"（关机后再开机）**时，如果受管服务器电源关闭，则上次崩溃屏幕将不可用。

禁用 Windows 自动重新引导选项

为确保 iDRAC6 可以捕获上次崩溃屏幕，应在运行 Windows Server 或 Windows Vista 的受管服务器上禁用**"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. 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。

目录

目录

使用 Web 界面配置 iDRAC6 Enterprise

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

iDRAC6 提供了 Web 界面，使您能够配置 iDRAC6 属性和用户、执行远程管理任务以及排除远程（受管）系统的故障。一般使用 Web 界面执行日常系统管理任务。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。

使用 Web 界面进行的大多数配置任务还可以用本地或远程 RACADM 命令或 SM-CLP 命令来执行。

本地 RACADM 命令从受管服务器执行。远程 RACADM 是在 Management Station 上运行的客户端公用程序，利用带外接口与受管服务器通信。该公用程序使用 **–r** 选项在网络上执行命令。有关使用 RACADM 的详情，请参阅"使用 RACADM 命令行界面"。

SM-CLP 命令在 shell 中执行，可通过 Telnet 或 Secure Shell (SSH) 连接远程使用。有关使用 SM-CLP 的详情，请参阅 "使用 iDRAC6 Enterprise SM-CLP 命令行界面"。

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。
2. 在**"Address"（地址）**字段中，输入 `https://<iDRAC6-IP-地址>` 并按 <Enter>。

   如果默认 HTTPS 端口号（端口 443）已更改，请输入：

   `https://<iDRAC6-IP-地址>:<端口号>`

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

   iDRAC6**"Login"（登录）**窗口将会出现。

登录

您可以以 iDRAC6 用户、Microsoft Active Directory 用户或 LDAP 用户的身份登录。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）**字段中输入下面的内容之一：
   - 您的 iDRAC6 用户名。

   注： 本地用户的用户名*区分小写*。比如 root、it_user、IT_user 或 john_doe。

   - 您的 Active Directory (AD) 用户名。也可从下拉菜单中选择 AD 域名。

     对于 Active Directory 用户名，可使用以下任意形式：<*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` 即 `JOHN_DOE@DELL.COM`。或者，也可以在**"Domain"（域）**字段中输入域。

   - LDAP 用户名（不含域名）。
2. 在**"Password"（密码）**字段中，输入 iDRAC6 用户密码、Active Directory 用户密码或 LDAP 密码。密码区分大小写。
3. 单击**"OK"（确定）**或按 <Enter>。

注销

1. 在主窗口的右上角，单击**"Log out"（注销）**关闭会话。

2. 关闭浏览器窗口。

注： **"Log out"（注销）**按钮在您登录后才出现。

注： 不正常注销关闭浏览器会造成会话一直活动直到会话超时为止。建议单击 **"Log out"（注销）**按钮结束会话。

注： 在 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。Internet Explorer (IE) 7 和 IE 8 提供选项来打开选项卡和窗口。每个选项卡将继承最新打开的选项卡的特性。按 <CtrlCT> 可打开新选项卡，按 <CtrlCN> 可从活动会话打开新浏览器窗口。将用已验证的凭据登录。关闭其中任何一个选项卡都会使所有 iDRAC6 Web 界面选项卡过期。此外，如果用户在一个选项卡上使用"Power User"（超级用户）权限登录，然后在另一个选项卡上以"Administrator"（管理员）权限登录，那么这两个打开的选项卡都将具有"Administrator"（管理员）权限。

Firefox 2 和 Firefox 3 中的选项卡行为与 IE 7 和 IE 8 中的一样；新选项卡是新的会话。但是，Firefox 中的窗口行为不同。Firefox 窗口将以与最后打开的窗口相同的权限运行。例如，如果打开了一个 Firefox 窗口并用"Power User"（超级用户）权限登录，用"Administrator"（管理员）权限打开了另一个窗口，则**两个**用户现在都有"Administrator"（管理员）权限。

表 5-1. 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 IE7 和 IE8	从最后打开的会话	新会话
Firefox 2 和 Firefox 3	从最后打开的会话	从最后打开的会话

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"配置 iDRAC6 网络"。

配置网络、IPMI 和 VLAN 设置

注： 您必须具有**"Configure iDRAC6"（配置 iDRAC6）**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 iDRAC6）在 DHCP 协商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。

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6**。
2. 单击**"Network/Security"（网络/安全性）**选项卡。

   此时会出现**"Network"（网络）**屏幕。
3. 根据需要配置网络、IPMI 和 VLAN 设置。请参阅表 5-2、表 5-3 和表 5-4 了解**"Network"（网络）、IPMI** 和 **"VLAN Settings"（VLAN 设置）**选项的说明。
4. 单击**"Apply"（应用）**。
5. 单击相应按钮继续。

表 5-2. 网络设置

设置	说明
网络接口插卡设置	
"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）。MAC 地址不能更改。
"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 的所有通信均被封锁。 默认为**不选中**。
常见设置	
"Register iDRAC6 on DNS"（在 DNS 上注册 iDRAC6）	在 DNS 服务器上注册 iDRAC6 名称。

	默认为**不选中**。
DNS iDRAC6 Name（名称）	显示 iDRAC6 名称。默认名称为 idrac-*service_tag*，其中 *service_tag* 是 Dell 服务器的服务标签号码。例如：iDRAC-HM8912S。
"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）	**选中**：启用从 DHCP 获取 DNS。 **不选中**：禁用从 DHCP 获取 DNS。
"DNS Domain Name"（DNS 域名）	默认**"DNS Domain Name"（DNS 域名）**为空白。如果选中**"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）**复选框，此选项就会呈灰色显示并且无法修改此字段。
IPv4 设置	
已启用	启用（**选中**）或禁用（**不选中**）IPv4 协议支持。应选中**"Enable NIC"（启用 NIC）**选项激活此设置。
"DHCP Enable"（启用 DHCP）	如果**选中**，Server Administrator 会从 DHCP 服务器获取 iDRAC6 NIC 的 IP 地址。还会取消激活**"IP Address"（IP 地址）**、**"Subnet Mask"（子网掩码）**和**"Gateway"（网关）**字段。
"IP Address"（IP 地址）	允许用户输入或编辑 iDRAC6 NIC 的静态 IP 地址。要更改此设置，取消选择**"DHCP Enable"（启用 DHCP）**选项。
"Subnet Mask"（子网掩码）	允许用户输入或编辑 iDRAC6 NIC 的子网掩码。要更改此设置，取消选择**"DHCP Enable"（启用 DHCP）**选项。
"Gateway"（网关）	允许用户输入或编辑 iDRAC6 NIC 的静态 IPv4 网关。要更改此设置，取消选择**"DHCP Enable"（启用 DHCP）**选项。
"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，选择**"DHCP Enable"（启用 DHCP）**选项以获取 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。
"Preferred DNS Server"（首选 DNS 服务器）	允许用户输入或编辑首选 DNS 服务器的静态 IP 地址。要更改此设置，首先取消选择**"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**选项。
"Alternate DNS Server"（备用 DNS 服务器）	当**未选择"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**时使用次要 DNS 服务器 IP 地址。如果没有备用 DNS 服务器，则输入 IP 地址 0.0.0.0。
IPv6 设置	
已启用	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**不选中**。
"Autoconfiguration Enable"（启用自动配置）	选中此选项将允许 iDRAC6 从动态主机配置协议 (DHCPv6) 服务器获取 iDRAC6 NIC 的 IPv6 地址。启用**"Autoconfiguration Enable"（启用自动配置）**也会禁用并清空**"IPv6 Address"（IPv6 地址）**、**"Prefix Length"（前缀长度）**和**"Gateway"（网关）**的静态值。
"IPv6 Address"（IPv6 地址）	配置 iDRAC6 NIC 的 IPv6 地址。要更改此设置，必须先通过取消选中相关复选框来禁用**"Autoconfiguration Enable"（启用自动配置）**。 **注：** 如果网络配置了 IPv6 DHCP，则只显示两个 IPv6 地址（链路本地地址和全局地址），如果配置了网络路由器发送路由器通告信息，则会显示所有 16 个 IPv6 地址。 **注：** 如果输入包含 8 个以上组的 IPv6 地址，iDRAC6 将不会允许保存设置。
"Prefix Length"（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，必须先通过取消选中相关复选框来禁用**"Autoconfiguration Enable"（启用自动配置）**。
"Gateway"（网关）	配置 iDRAC6 NIC 的静态 IPv6 网关。要更改此设置，必须先通过取消选中相关复选框来禁用**"Autoconfiguration Enable"（启用自动配置）**。
"Use DHCPv6 to obtain DNS server addresses"（使用 DHCPv6 获取 DNS 服务器地址）	通过选择**"Use DHCPv6 to obtain DNS server addresses"（使用 DHCPv6 获取 DNS 服务器地址）**复选框启用 DHCP 获取 IPv6 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**取消选中**。 **注：** 如果选中**"Use DHCPv6 to obtain DNS server addresses"（使用 DHCPv6 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。
"Preferred DNS Server"（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，取消选中**"Use DHCPv6 to obtain DNS server addresses"（使用 DHCPv6 获取 DNS 服务器地址）**。
"Alternate DNS Server"（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，取消选中**"Use DHCPv6 to obtain DNS server addresses"（使用 DHCPv6 获取 DNS 服务器地址）**。

表 5-3. IPMI 设置

设置	**说明**
"Enable IPMI Over LAN"（启用 LAN 上 IPMI）	选中后表示 IPMI LAN 信道已启用。默认为**不选中**。
"Channel Privilege Level Limit"（信道权限级别限制）	配置 LAN 信道上可接受的用户最大权限级别。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"（密钥）	配置密钥。密钥必须包含不超过 40 个字符的偶数个十六进制字符（不含空格）。默认 IPMI 密钥是全零。

表 5-4. VLAN 设置

按钮	说明
"Enable VLAN ID"（启用 VLAN ID）	**"Yes"（是）**- 启用。**"No"（否）**- 禁用。如果启用，将仅接受匹配的虚拟 LAN (VLAN) ID 通信。 **注：** VLAN 设置只能通过 CMC Web 界面配置。iDRAC6 只显示当前启用状态；不能在此屏幕上修改设置。
VLAN ID	802.1g 字段中的 VLAN ID 字段。显示从 1 到 4094 的值，但是 4001 到 4020 除外。
优先级	802.1g 字段中的"Priority"（优先权）字段。这用于标识 VLAN ID 的优先权并显示从 0 到 7 的 VLAN 优先权值。

表 5-5. 网络配置按钮

按钮	说明
"Advanced Settings"（高级设置）	显示**"Network Security"（网络安全）**屏幕，允许输入"IP Range"（IP 范围）和"IP Blocking"（IP 阻塞）属性。
"Print"（打印）	打印屏幕上显示的**"Network"（网络）**配置值。
"Refresh"（刷新）	重新载入**"Network"（网络）**屏幕。
"Apply"（应用）	保存网络配置屏幕上所做的任何新设置。 **注：** 对 NIC IP 地址设置的更改将关闭所有用户会话并要求用户使用更新的 IP 地址设置重新连接到 iDRAC6 Web 界面。所有其它更改将要求重设 NIC，这可能导致短暂的连接中断。

配置 IP 筛选和 IP 阻塞

注： 您必须具有**"Configure iDRAC6"（配置 iDRAC6）**权限才能执行以下步骤。

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6** 。
2. 单击**"Network/Security"（网络/安全性）**选项卡。

   此时会出现**"Network"（网络）**屏幕。
3. 单击**"Advanced Settings"（高级设置）**。

   随即出现**"Network Security"（网络安全性）**屏幕。
4. 根据需要配置 IP 筛选和阻塞设置。有关 **IP 筛选和阻塞设置**的说明，请参阅表 5-6。
5. 单击**"Apply"（应用）**。
6. 单击相应按钮继续。请参阅表 5-7。

表 5-6. IP 筛选和阻塞设置

设置	说明
"IP Range Enabled"（IP 范围已启用）	启用 IP 范围检查功能，该功能定义了可以访问 iDRAC6 的 IP 地址的范围。默认为**"Disabled"（已禁用）**。
"IP Range Address"（IP 范围地址）	决定可接受的 IP 子网地址。默认为 **192.168.1.0**。
"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。默认为**"Disabled"（已禁用）**。
"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**。

表 5-7. 网络安全性按钮

按钮	说明

"Print"（打印）	打印屏幕上显示的**"Network Security"（网络安全性）**值。
"Refresh"（刷新）	重新载入**"Network Security"（网络安全性）**屏幕。
"Apply"（应用）	保存**"Network Security"（网络安全性）**屏幕上所做的任何新设置。
"Go Back to Network Configuration Page"（退回到网络配置页）	返回到**"Network"（网络）**屏幕。

配置平台事件

平台事件配置提供了用于配置 iDRAC6 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 5-8 中列出了可筛选平台事件。

表 5-8. 可筛选平台事件

索引	平台事件
1	电池探测器警告
2	电池探测器故障
3	分离电压探测器故障
4	温度探测器警告
5	温度探测器故障
6	处理器故障
7	处理器不存在
8	硬件日志故障
9	自动系统恢复
10	SD 卡发生故障
11	冗余掉失

发生平台事件时（例如，*电池探测器警告*），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. 登录到 iDRAC6 Web 界面。
2. 单击**"System"（系统）**，然后单击**"Alert Management"（警报管理）**选项卡。

   随即出现**"Platform Events"（平台事件）**屏幕。
3. 选择**"Enable Paltform Event Filter Alerts"（启用平台事件筛选器警报）**复选框。您必须为要发送至有效目标的任何平台警报选择该选项。
4. 选择要为各个事件启用的以下操作之一：
   - 重新引导系统 - 发生事件时，系统重新启动（温引导）。
   - 系统关机后再开机 - 发生事件时，系统关闭、关闭电源，然后重新启动（冷引导）。
   - 关闭系统电源 - 发生事件时，系统关闭并关闭电源。
   - 无操作 - 发生事件时，不进行任何操作。这是事件的默认设置。
5. 对于您想生成警报的每个事件，选中其旁边的**"Generate Alert"（生成警报）**选项。

注： 可通过选中或取消选中**"Generate Alert"（生成警报）**列标题旁边的复选框启用或禁用所有事件的警报生成。

6. 单击**"Apply"（应用）**。

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. 登录到 iDRAC6 Web 界面。
2. 确保遵循"配置平台事件筛选器 (PEF)"中的步骤。
3. 单击**"System"（系统）**，然后单击**"Alert Management"（警报管理）**选项卡。

   随即出现**"Platform Events"（平台事件）**屏幕。
4. 单击**"Trap Settings"（陷阱设置）**。

   将会显示 **"Trap Settings"（陷阱设置）** 屏幕。
5. 配置 PET 目标 IP 地址：
   a. 选中要激活的**"Destination Number"（目标号码）**的**"Enabled"（启用）**复选框。
   b. 在相应的 IPv4 或 IPv6**"Destination IP Address"（目标 IP 地址）**框中输入 IP 地址。
   c. 单击**"Apply"（应用）**。

   注： 要成功发送陷阱，配置**"Community String"（团体字符串）**值。**"Community String"（团体字符串）**值表示从 iDRAC6 发送的简单网络管理协议 (SNMP) 警报陷阱中使用的团体字符串。在发生平台事件时，iDRAC6 就会发送 SNMP 警报陷阱。**"Community String"（团体字符串）**的默认设置为 **Public**。

   d. 要检测所配置的警报，单击**"Send"（发送）**。
   e. 要添加其它目标 IP 地址，请重复执行步骤 a 至步骤 d。可以指定最多 4 个 IPv4 和 4 个 IPv6 目标地址。

配置电子邮件警报

1. 登录到 iDRAC6 Web 界面。
2. 确保遵循"配置平台事件筛选器 (PEF)"中的步骤。
3. 单击**"System"（系统）**，然后单击**"Alert Management"（警报管理）**选项卡。

   随即出现**"Platform Events"（平台事件）**屏幕。
4. 单击**"Email Alert Settings"（电子邮件警报设置）**。

   随即出现 **"Email Alert Settings"（电子邮件警报设置）** 屏幕。
5. 配置电子邮件警报目标。
   a. 选中第一个未定义的电子邮件警报的**"Enabled"（启用）**复选框。
   b. 在**"Destination Email Address"（目标电子邮件地址）**字段中输入有效的电子邮件地址。
   c. 单击**"Apply"（应用）**。

   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）**屏幕上的**"SMTP (e-mail) Server Address Settings"（SMTP [电子邮件] 服务器地址设置）**部分配置 SMTP [电子邮件] 服务器。使用点分隔格式（如 192.168.1.1）或 DNS 名称在字段中指定 SMTP 服务器。在发生平台事件时，"SMTP Server"（SMTP 服务器）的 IP 地址与 iDRAC6 进行通信，发送电子邮件警报。

   d. 在**"Modify Source Email Name"（修改源电子邮件名称）**字段中，输入使用的警报发件人电子邮件，或保持空白以使用默认电子邮件发件人 默认为 blade_slot@iDRAC6 IP 地址。
      - 如果**"Modify Source Email Name"（修改源电子邮件名称）**字段为空，iDRAC6 主机名已配置且 DNS 域名处于活动状态，则源电子邮件地址为：<iDRAC6 主机名>@<DNS 域名>。
      - 如果此字段为空，iDRAC6 主机名为空且 DNS 域名处于活动状态，则源电子邮件地址为：<iDRAC6 Slot*x*>@<DNS 域名>。
      - 如果此字段为空，iDRAC6 主机名为空且 DNS 域名也为空，则源电子邮件地址为：<iDRAC6 Slot*x*>@<iDRAC6 IP 地址>。
      - 如果此字段为"不含 @ 的字符串"，且 DNS 域名处于活动状态，则源电子邮件地址为：<不含 @ 的字符串>@<DNS 域名>。
      - 如果此字段为"不含 @ 的字符串"，且 DNS 域名为空，则源电子邮件地址为：<不含 @ 的字符串>@<iDRAC6 IP 地址>。
      - 如果此字段为"含 @ 的字符串"，且 DNS 域名处于活动状态，则源电子邮件地址为：<含 @ 的字符串>@<DNS 域名>。

- 如果此字段为"含 @ 的字符串"，且 DNS 域名为空，则源电子邮件地址为：<含 @ 的字符串>@<iDRAC6 IP 地址>。

e. 单击**"Send"（发送）**检测配置的电子邮件警报（如果需要）。

f. 要添加其它电子邮件警报目标，请重复执行 步骤 a 至 步骤 e。最多可以指定四个电子邮件警报目标。

配置 LAN 上 IPMI

1. 登录到 iDRAC6 Web 界面。

2. 配置 LAN 上 IPMI：

   a. 单击**"System"（系统）**→**"Remote Access"（远程访问）**→ **iDRAC6**，然后单击**"Network/Security"（网络/安全性）**选项卡。

   此时会出现**"Network"（网络）**屏幕。

   b. 单击**"IPMI Settings"（IPMI 设置）**。

   c. 选中**"Enable IPMI Over LAN"（启用 LAN 上 IPMI）**复选框。

   d. 如果需要，更新**"Channel Privilege Level Limit"（信道权限级别限值）**：

   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）**下拉式菜单，选择**"Administrator"（管理员）**、**"Operator"（操作员）**或**"User"（用户）**，然后单击**"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 Settings"（IPMI 设置）**下的**"Encryption Key"（密钥）**字段中，输入密钥。

   f. 单击**"Apply"（应用）**。

3. 配置 IPMI LAN 上串行 (SOL)：

   a. 单击**"System"（系统）**→**"Remote Access"（远程访问）**→ **iDRAC6**，然后单击**"Network/Security"（网络/安全性）**选项卡。

   此时会出现**"Network"（网络）**屏幕。

   b. 单击**"Serial Over LAN"（LAN 上串行）**选项卡。

   c. 选择**"Enable Serial Over LAN"（启用 LAN 上串行）**。

   d. 如果需要，通过从**"Baud Rate"（波特率）**下拉式菜单中选择数据速度来更新 IPMI SOL **波特率**。

   注： 要重定向 LAN 上串行控制台，确保 SOL **波特率**与受管服务器的波特率相同。

   e. 单击**"Apply"（应用）**。

   f. 根据需要在**"Advanced Settings"（高级设置）**页配置 IP 过滤和阻塞设置。

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*基于角色的授权*）的唯一用户。

要添加和配置 iDRAC6 用户，请执行以下步骤：

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

1. 单击**"System"（系统）**→**"Remote Access"（远程访问）**→ **iDRAC6** →**"Network/Security"（网络/安全性）**→**"Users"（用户）**。

   "Users"（用户）屏幕显示各个用户的**"User ID"（用户 ID）**、**"State"（状态）**、**"User Name"（用户名）**、**"IPMI LAN Privileges"（IPMI LAN 权限）**、"iDRAC6 Privileges"（iDRAC6 权限）和**"Serial Over LAN"（LAN 上串行）**功能。

   注： User-1 为 IPMI 匿名用户保留，不可配置。

2. 在**"User ID"（用户 ID）**列单击用户 ID 编号。

3. 在 **"User Main Menu"（用户主菜单）** 页（请参阅 表 5-9、表 5-10 和 表 5-11）上，您可以配置用户、上载 SSH 公共密钥文件、查看或删除指定的 SSH 密钥或所有 SSH 密钥。

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。

准备工作

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基于 SSH 的 PKA，在登录 iDRAC6 时，您不必输入密码。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. 输入密钥的位数。密钥生成算法仅支持 RSA 和 DSA。对于 RSA，加密位数必须介于 768 和 4096 位之间，而 DSA 则为 1024 位。
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. 您可以使用**"Save public key"（保存公共密钥）**选项将公共密钥保存到文件中，以便稍后上载。所有上载的密钥必须采用 RFC 4716 或 openSSH 格式。否则，必须转换格式。

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 Ct rsa Cb 1024 CC testing
```

注： 选项区分小写。

其中，

-t 可以是 *dsa* 或 *rsa*。

Cb 选项指定介于 768 和 4096 之间的加密位数。

CC 选项允许修改公共密钥注释，该选项是可选的。

执行此命令后，上载公共文件。

注： 使用 ssh-keygen 从 Linux management station 生成的密钥不采用 RFC4716 格式，而是采用 openSSH 格式。openSSH 公共密钥可以上载到 iDRAC6。iDRAC6 公共密钥算法可验证 openSSH 和 FC4716 密钥、内部转换 RFC4716 密钥为 openSSH 格式，然后内部保存密钥。

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，您不必输入密码就能够通过 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_address>
```

其中，IP_address 是 iDRAC6 的 IP 地址。

发送 RACADM 命令：

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

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

请参阅"使用 RACADM 上载、查看和删除 SSH 密钥"了解有关使用 RACADM 上载、查看和删除 SSH 密钥的信息。

表 5-9. 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 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。
"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。

"**pload SSH Key(s)"（上载 SSH 密钥）**页允许您上载 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**"View/Remove SSH Key(s)"（查看/删除 SSH 密钥）**页的不可编辑文本框中。

小心： 上载、查看和/或删除 SSH 密钥的能力基于"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。授予此权限时应谨慎。有关详情，请参阅表 5-14。

表 5-10. 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。 **注：** openSSH 格式的公共密钥支持密钥文本粘贴选项。RFC4716 格式的密钥不支持文本粘贴选项。
"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 5-11. 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）**可删除已有密钥。

1. 如果选择**"Configure User"（配置用户）并**单击 **"Next"（下一步）**， 则显示 **"User Configuration"（用户配置）** 页。
2. 在**"User Configuration"（用户配置）**屏幕中配置用户的属性和权限。

   表 5-12 说明配置 iDRAC6 用户名和密码的**"General"（常规）**设置。

   表 5-13 说明用于配置用户 LAN 权限的**"IPMI User Privileges "（IPMI 用户权限）**。

   表 5-14 说明用于**"IPMI LAN Privileges "（IPMI LAN 权限）**和 iDRAC6"User Privileges "（用户权限）设置的**"User Group"（用户组）**权限。

   表 5-15 说明 **iDRAC6 组**权限。如果添加**"iDRAC6 User Privilege"（iDRAC6 用户权限）**到**"Administrator"（管理员）**、**"Power User"（超级用户）**或**"Guest User"（客用户）**，iDRAC6 **组**会更改为**"Custom"（自定义）**组。
3. 完成后，单击**"Apply"（应用）**。
4. 单击相应按钮继续。请参阅表 5-16。

表 5-12. 常规属性

<table>
<tr><th>属性</th><th>说明</th></tr>
<tr><td>"User ID"（用户 ID）</td><td>包含 16 个预置用户 ID 编号之一。此字段不能编辑。</td></tr>
<tr><td>"Enable User"（启用用户）</td><td>选中后，表示启用用户对于 iDRAC6 的访问权限。取消选中后，表示禁用用户的访问权限。</td></tr>
<tr><td>用户名</td><td>指定一个 iDRAC6 用户名，最多 16 个字符。每个用户必须具有唯一用户名。

• 0-9
• A-Z
• a-z
• 特殊字符：

<table><tr><td>+</td><td>%</td><td>=</td><td>,</td><td>-</td><td>{</td><td>]</td><td>§</td></tr><tr><td>!</td><td>(</td><td>?</td><td>;</td><td>_</td><td>}</td><td>I</td><td></td></tr><tr><td>#</td><td>中所示）</td><td>*</td><td>:</td><td>$</td><td>[</td><td>|</td><td></td></tr></table>
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。</td></tr>
<tr><td>"Change Password"（更改密码）</td><td>启用"New Password"（新密码）和"Confirm New Password"（确认新密码）字段。取消选中时，无法更改用户的"Password"（密码）。</td></tr>
<tr><td>"New Password"（新密码）</td><td>允许编辑 iDRAC6 用户密码。输入多达 20 个字符的"Password"（密码）。这些字符将不会显示。

• 0-9
• A-Z
• a-z
• 特殊字符：

<table><tr><td>+</td><td>%</td><td>=</td><td>,</td><td>-</td><td>{</td><td>]</td><td>。</td></tr><tr><td>!</td><td>(</td><td>?</td><td>;</td><td>_</td><td>}</td><td>I</td><td>|</td></tr><tr><td>#</td><td>中所示）</td><td>*</td><td>:</td><td>$</td><td>[</td><td>/</td><td>@</td></tr></table></td></tr>
<tr><td>"Confirm New Password"（确认新密码）</td><td>重新输入 iDRAC6 用户的密码以进行确认。</td></tr>
</table>

表 5-13. IPMI LAN 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：**"None"（无）**、**"Administrator"（管理员）**、**"Operator"（操作员）**或**"User"（用户）**。
"Enable Serial Over LAN"（启用 LAN 上串行）	允许用户使用 IPMI LAN 上串行。**选中**后，将启用此权限。

表 5-14. 其它权限

属性	说明
"iDRAC6 Group"（iDRAC6 组）	指定用户的最大 iDRAC6 用户权限为以下之一：**"Administrator"（管理员）**、**"Power User"（高级用户）**、**"Guest User"（客用户）**、**"Custom"（自定义）**或**"None"（无）**。 请参阅表 5-15 了解 **DRAC6 组**权限。
"Login to iDRAC6"（登录到 iDRAC6）	允许用户登录到 iDRAC6。
"Configure iDRAC6"（配置 iDRAC6）	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。 **小心： 通常为 iDRAC 的管理员用户组的成员保留该权限。但也可将该权限分配给"Custom"（自定义）用户组中的用户。具有该权限的用户可修改任何用户的配置。其中包括创建或删除任何用户、用户的 SSH 密钥管理等。出于这些原因，应谨慎分配该权限。**
"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。
访问虚拟控制台	允许用户运行虚拟控制台。 **小心： 通常为 iDRAC 的管理员组或 Power User（高级用户）组的成员保留该权限。除了能使用虚拟控制台，还允许具有访问虚拟控制台权限的用户在 iDRAC6 Web 界面中查看任何虚拟控制台使用人员的活动。出于这些原因，应谨慎分配该权限。**

"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）	允许用户发送检测警报（电子邮件和 PET）到当前配置的所有警报收件人。
"Execute Diagnostic Commands"（执行诊断命令）	允许用户运行诊断命令。

表 5-15. iDRAC6 组权限

用户组	授予的权限
管理员	**"Login to iDRAC6"（登录到 iDRAC6）、"Configure iDRAC6"（配置 iDRAC6）、"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）**
高级用户	**"Login to iDRAC6"（登录到 iDRAC6）、"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）**
客用户	**"Login to iDRAC6"（登录到 iDRAC6）**
自定义	选择以下权限的任意组合：**"Login to iDRAC6"（登录到 iDRAC6）、"Configure iDRAC6"（配置 iDRAC6）、"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）**
None（无）	没有分配权限

表 5-16. 用户配置按钮

按钮	操作
"Print"（打印）	打印屏幕上显示的**"User Configuration"（用户配置）**值。
"Refresh"（刷新）	重新载入**"User Configuration"（用户配置）**屏幕。
"Apply"（应用）	保存对用户配置所做的任何新设置。
"Go Back To User Main Menu"（返回用户主菜单）	返回**"User Main Menu"（用户主菜单）屏幕**。

使用 SSL 和数字证书保证 iDRAC6 通信安全

本节提供关于 iDRAC6 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)
- 访问 SSL 主菜单
- 生成新 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，服务器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窃听。

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，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 (CA) 签署的证书更换 Web Server SSL 证书。认证机构是信息技术行业认可的企业实体，可满足高标准的可靠性审查、识别和其它重要安全标准。例如，Thwate 和 VeriSign 均为 CA。要开始获取签署的证书，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 CA，比如 VeriSign 或 Thawte。

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。安全服务器证书使服务器客户端能够信任服务器的身份并能够与服务器协商加密会话。

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，以在通过网络和因特网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，将证书上载到 iDRAC6 固件。iDRAC6 固件中保存的 CSR 信息必须与证书中的信息一致，即，必须对应 iDRAC6 创建的 CSR 生成证书。

访问 SSL 主菜单

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）**选项卡。
2. 单击 **SSL** 以打开 **SSL** 屏幕。

表 5-17 说明了生成 CSR 时可用的选项。

表 5-18 说明了**"SSL Main Menu"（SSL 主菜单）**屏幕上的可用按钮。

表 5-17. SSL 主菜单选项

字段	说明
"Generate a New Certificate Signing Request (CSR)"（生成新的证书签名请求 [CSR]）	选择此选项并单击**"Next"（下一步）**将打开**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**屏幕。 **注：** 每个新 CSR 会覆盖固件上以前的 CSR。为了使 CA 接受您的 CSR，固件中的 CSR 必须与 CA 返回的证书匹配。
"Upload Server Certificate"（上载服务器证书）	选择此选项并单击**"Next"（下一步）**将打开**"Certificate Upload"（证书上载）**屏幕并上载 CA 发送给您的证书。 **注：** iDRAC6 仅接受 Base 64 编码的 X509 证书。不接受 DER 编码证书。
"View Server Certificate"（查看服务器证书）	选择此选项并单击**"Next"（下一步）**将打开**"View Server Certificate"（查看服务器证书）**屏幕并查看现有的服务器证书。

表 5-18. SSL 主菜单按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的 **SSL** 值。
"Refresh"（刷新）	重新载入 **SSL** 屏幕。
"Next"（下一步）	处理 **SSL** 屏幕上的信息并继续下一步。

生成新的证书签名请求

注： 每个新的 CSR 都会改写固件上存储的任何原有的 CSR 数据。固件中的 CSR 必须匹配 CA 返回的证书。否则，iDRAC6 将不会接受证书。

1. 在 **SSL** 屏幕上选择**"Generate a New Certificate Signing Request (CSR)"（生成新的证书签名请求 [CSR]）**，并单击**"Next"（下一步）**。
2. 在**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**屏幕上输入每个 CSR 属性值。

   表 5-19 说明了**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**屏幕选项。
3. 单击**"Generate"（生成）**创建 CSR。
4. 单击**"Download"（下载）**将 CSR 文件保存到远程 Management Station。
5. 单击相应按钮继续。请参阅表 5-20。

表 5-19. 生成证书签名请求 (CSR) 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，**www.xyzcompany.com**）。只有字母数字字符、空格、连字符、下划线和句点有效。
"Organization Name"（组织名称）	与组织相关的名称（例如，XYZ 公司）。只有字母数字字符、连字符、下划线、句点和空格有效。
"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）。只有字母数字字符、连字符、下划线、句点和空格有效。
"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]）。只有字母数字字符和空格有效。不要使用下划线或其它字符分隔字词。
"State Name"（州/省名称）	申请认证的实体所在的州或省（例如，德克萨斯州 [Texas]）。只有字母数字字符和空格有效。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。输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。
"Key Size"（密钥大小）	要生成的证书签名请求 (CSR) 密钥的大小。大小应为 1024 KB 或 2048 KB。

表 5-20. 生成证书签名请求 (CSR) 按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**值。
"Refresh"（刷新）	重新载入**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**屏幕。
"Generate"（生成）	生成 CSR，然后提示用户保存到指定目录。
"Download"（下载）	下载证书到本地计算机。
"Go Back to SSL Main Menu"（返回 SSL 主菜单）	使用户返回到 **SSL** 屏幕。

上载服务器证书

1. 在 **SSL** 屏幕中选择**"Upload Server Certificate"（上载服务器证书）**，然后单击**"Next"（下一步）**。

   随即出现**"Certificate Upload"（证书上载）**屏幕。

2. 在**"File Path"（文件路径）**字段中，输入证书的路径或单击**"Browse"（浏览）**导航到 Management Station 上的证书文件。

注： **"File Path"（文件路径）**值显示要上载的证书的文件路径。必须输入此文件路径，包括完整路径和完整文件名及文件扩展名。

3. 单击**"Apply"（应用）**。

4. 单击相应按钮继续。请参阅表 5-21。

表 5-21. 证书上载按钮

按钮	说明
"Print"（打印）	打印**"Certificate Upload"（证书上载）**屏幕上显示的值
"Refresh"（刷新）	重新载入**"Certificate Upload"（证书上载）**屏幕
"Apply"（应用）	将证书应用到 iDRAC6 固件
"Go Back to SSL Main Menu"（返回 SSL 主菜单）	使用户返回到**"SSL Main Menu"（SSL 主菜单）**屏幕

查看服务器证书

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

   表 5-22 说明**"View Server Certificate"（查看服务器证书）**窗口中列出的字段及相关说明。

2. 单击相应按钮继续。请参阅表 5-23。

表 5-22. 查看服务器证书信息

字段	说明
"Serial Number"（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

表 5-23. 查看服务器证书按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的**"View Server Certificate"（查看服务器证书）**值。
"Refresh"（刷新）	重新载入**"View Server Certificate"（查看服务器证书）**屏幕。
"Go Back to SSL Main Menu"（返回 SSL 主菜单）	返回**"SSL Main Menu"（SSL 主菜单）**屏幕。

配置和管理 Microsoft Active Directory 认证

注： 您必须具有**"Configure iDRAC"（配置 iDRAC）**权限才能配置 Active Directory 以及上载、下载和查看 Active Directory 证书。

注： 有关 Active Directory 配置和如何配置标准架构和扩展架构的 Active Directory 的详情，请参阅 "使用 iDRAC6 目录服务"。

要访问 **Microsoft Active Directory** 摘要屏幕，请单击 **"System"（系统）→ "Remote Access"（远程访问）→ iDRAC6→ "Network/Security"（网络/安全性）**选项卡 **→ "Directory Service"（目录服务）→ Microsoft Active Directory**。

表 5-24 列出 **Active Directory** 摘要选项。单击相应按钮继续。

表 5-24. Active Directory 选项

字段	说明
常见设置	显示通常配置的 Active Directory 设置。
"Active Directory CA Certificate"（Active Directory CA 证书）	显示签署域控制器的所有 SSL 服务器证书的 CA 证书。
"Standard Schema Settings"（标准架构设置）/"Extended Schema Settings"（扩展架构设置）	根据当前 Active Directory 配置，将会显示"Extended Schema Settings"（扩展架构设置）或"Standard Schema Settings"（标准架构设置）。
"Configure Active Directory"（配置 Active Directory）	单击此选项配置 Active Directory 设置共 4 步中的第 1 步。**"Step 1 of 4 Active Directory"（Active Directory 第 1 步，共 4 步）**页允许上载 Active Directory CA 证书到 iDRAC6，查看当前已上载到 iDRAC6 的 Active Directory CA 证书，或启用证书验证。
"Test Settings"（检测设置）	单击此选项允许您使用指定的设置检测 Active Directory 配置。
"Kerberos Keytab Upload"（Kerberos Keytab 上载）	单击此选项可将 Kerberos Keytab 上载到 iDRAC6。有关如何创建 Keytab 文件的信息，请参阅"配置 iDRAC6 为单一式登录和智能卡登录"。

表 5-25. Active Directory 按钮

按钮	定义
"Print"（打印）	打印屏幕上显示的 **Active Directory** 值。
"Refresh"（刷新）	重新载入 **Active Directory** 屏幕。

配置 Active Directory（标准架构和扩展架构）

1. 在 **Active Directory** 摘要屏幕上，单击**"Configure Active Directory"（配置 Active Directory）**。
2. 在**"Step 1 of 4 Active Directory"（Active Directory 第 1 步，共 4 步）**屏幕上，可以启用证书验证，上载 Active Directory CA 证书到 iDRAC6，或查看当前的 Active Directory CA 证书。

   表 5-26 介绍了 **Active Directory 配置与管理**过程中各步骤的设置和选项。单击相应按钮继续。

表 5-26. Active Directory 配置设置

设置	说明

Active Directory 配置与管理第 1 步，共 4 步	
"Certificate Validation Enabled"（启用证书验证）	指定是启用还是禁用证书验证。如果**选中，**则启用证书验证。连接到 Active Directory 期间，iDRAC6 使用安全套接字层 (SSL) 上 LDAP。默认情况下，iDRAC6 在 SSL 握手期间通过使用载入 iDRAC6 的 CA 证书来验证域控制器的 SSL 服务器证书，提供强大的安全性。检测时可以禁用证书验证。
"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）	要上载 Active Directory CA 证书，单击**"Browse"（浏览）**，选择文件，并单击**"Upload"（上载）**。请确保域控制器的 SSL 证书是同一认证机构签署的，且访问 iDRAC6 的 Management Station 上有此证书。**"File Path"（文件路径）**值显示要上载的证书的文件路径。如果选择不浏览到证书，则输入包括完整路径、完整文件名和文件扩展名的文件路径。
"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）	显示上载到 iDRAC6 的 Active Directory CA 证书。
Active Directory 配置与管理第 2 步，共 4 步	
"Active Directory Enabled"（启用 Active Directory）	如果想启用 Active Directory，则选择此选项。
"Enable SmartCCard Login"（启用智能卡登录）	选择此选项启用智能卡登录。以后使用 GUI 尝试登录时都会提示进行智能卡登录。 **注：** 只有装有 Internet Explorer 的 Microsoft Windows 操作系统才支持基于智能卡的双重验证 (TFA) 和单一登录。另外，Windows XP 下的 Terminal Services（远程桌面）不支持智能卡操作。不过，Windows Vista 支持这种操作。
"Enable Single Sign-on"（启用单一登录）	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，则选择此选项。如果启用了单一登录 (SSO) 后注销，则可以使用 SSO 再登录回来。如果已使用 SSO 登录，然后注销，或者如果 SSO 失败，则将会显示正常的登录网页。 **注：** 启用智能卡登录**或**单一登录不会禁用任何命令行带外接口，包括 SSH、Telnet、远程 RACADM 和 LAN 上 IPMI。 **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。标准和扩展架构均支持单一登录 (SSO) 功能。
"User Domain Name"（用户域名）	输入用户域名条目。如果已配置，会在登录页以下拉式菜单的形式显示用户域名列表。如果未配置，Active Directory 用户仍可以通过输入以下格式的用户名来登录：用户名@域名或域名\用户名。**"Add"（添加）**：向列表添加新的用户域名条目。**"Edit"（编辑）**：修改现有用户域名条目。**"Delete"（删除）**：从列表删除用户域名条目。
"Timeout"（超时）	输入等待 Active Directory 查询完成需要的最长时间（秒）。
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。
指定域控制器地址	选择**"Specify Domain Controller Addresses"（指定域控制器地址）**选项则允许 iDRAC6 使用 Active Directory 域控制器服务器地址。选择此选项后，不执行 DNS 查找。指定域控制器的 IP 地址或完全限定域名 (FQDN)。当选择**"Specify Domain Controller Addresses"（指定域控制器地址）**选项时，要求至少配置三个地址之一。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**"Standard Schema"（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。如果选择**"Extended Schema"（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。
Active Directory 配置与管理第 3 步，共 4 步	
扩展架构选择	如果想为 Active Directory 使用扩展架构，则选择此选项。 单击**"Next"（下一步）**以显示**"Step 4 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 4 步，共 4 步）**。 **"iDRAC6 Name"（iDRAC6 名称）**：指定唯一识别 Active Directory 中 iDRAC6 的名称。该值默认为 NULL。 **"iDRAC6 Domain Name"（iDRAC6 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 iDRAC6 配置为使用扩展 Active Directory 架构时，才会显示这些设置。
标准架构选择	如果想为 Active Directory 使用标准架构，则选择此选项。 单击**"Next"（下一步）**以显示**"Step 4a of 4 Active Directory"（Active Directory 第 4a 步，共 4 步）**页。 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** 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。 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)。选择此选项后，不执行 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。 **"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）**：指定角色组所在的组域类型。

	"Role Groups Privileges"（角色组权限）：指定组权限级别。（请参阅表 5-27） 只有 iDRAC6 配置为使用标准 Active Directory 架构时，才会显示这些设置。

表 5-27. 角色组权限

设置	说明
"Role Group Privilege Level"（角色组权限级别）	指定用户的最大 iDRAC6 用户权限为以下之一：**"Administrator"（管理员）**、**"Power User"（高级用户）**、**"Guest User"（客用户）**、**"None"（无）**或**"Custom"（自定义）**。 请参阅表 5-28 了解**角色组**权限
"Login to iDRAC6"（登录到 iDRAC6）	允许组登录 iDRAC6。
"Configure iDRAC6"（配置 iDRAC6）	授予配置 iDRAC6 的组权限。
"Configure Users"（配置用户）	授予配置用户的组权限。
"Clear Logs"（清除日志）	授予清除日志的组权限。
"Execute Server Control Commands"（执行服务器控制命令）	授予执行服务器控制命令的组权限。
访问虚拟控制台	允许组访问虚拟控制台。
"Access Virtual Media"（访问虚拟介质）	允许组访问虚拟介质。
"Test Alerts"（检测警报）	允许组将检测警报（电子邮件和 PET）发送给特定用户。
"Execute Diagnostic Commands"（执行诊断命令）	授予执行诊断命令的组权限。

表 5-28. 角色组权限

属性	说明
管理员	"Login to iDRAC6"（登录到 iDRAC6）、"Configure iDRAC6"（配置 iDRAC6）、"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）
高级用户	"Login to iDRAC6"（登录到 iDRAC6）、"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）
客用户	"Login to iDRAC6"（登录到 iDRAC6）
自定义	选择以下权限的任意组合："Login to iDRAC6"（登录到 iDRAC6）、"Configure iDRAC6"（配置 iDRAC6）、"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）
None（无）	没有分配权限

查看 Active Directory CA 证书

在 **Active Directory** 摘要页上，单击**"Configure Active Directory"（配置 Active Directory）**。将会显示**"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）**部分。请参阅表 5-29。

表 5-29. Active Directory CA 证书信息

字段	说明
"Serial Number"（序列号）	证书序列号。
"Subject Information"（主题信息）	按照主题输入的证书属性。
"Issuer Information"（颁发者信息）	按照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。

启用或禁用本地配置访问

注： 本地配置访问的默认设置为**"Enabled"（启用）**。

启用本地配置访问

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**。
2. 在**"Local Configuration"（本地配置）**下，单击以**取消选中"Disable iDRAC6 local USER Configuration Updates"（禁用 iDRAC6 本地用户配置更新）**启用访问。
3. 单击**"Apply"（应用）**。

禁用本地配置访问

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**。
2. 在**"Local Configuration"（本地配置）**下，单击以选中**"Disable iDRAC6 local USER Configuration Updates"（禁用 iDRAC6 本地用户配置更新）**禁用访问。
3. 单击**"Apply"（应用）**。

配置 iDRAC6 服务

注： 要修改这些设置，必须具有**"Configure iDRAC6"（配置 iDRAC6）**权限。

注： 向服务应用更改时，更改会立即生效。现有连接可能会没有警告而终止。

注： Microsoft Windows 附带的 Telnet 客户端存在一个已知的问题。使用其它 Telnet 客户端，例如 HyperTerminal 或 PuTTY。

1. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6**，然后单击**"Network/Security"（网络/安全性）**选项卡。
2. 单击**"Services"（服务）**打开**"Services"（服务）**配置屏幕。
3. 根据需要配置以下服务：
   - Web Server — 请参阅表 5-30 了解 Web Server 设置
   - SSH — 请参阅表 5-31 了解 SSH 设置
   - Telnet — 请参阅表 5-32 了解 Telnet 设置
   - SNMP Agent — 请参阅表 5-33 了解 SNMP Agent 设置
   - Automated System Recovery Agent — 请参阅表 5-34 了解 Automated System Recovery Agent 设置
4. 单击**"Apply"（应用）**。

表 5-30. Web Server 设置

设置	说明
已启用	启用或禁用 iDRAC6 Web Server。**选中**后，表示 Web Server 已启用。默认值为**选中**。
"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。可以同时有 4 个 Web Server 会话。
"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）**。此字段不可编辑。
"Timeout"（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立即生效并将重设 Web Server。超时范围为 60 至 10800 秒。默认为 **1800** 秒。
"HTTP Port Number"（HTTP 端口号）	iDRAC6 侦听浏览器连接的端口。默认为 **80**。
"HTTPS Port Number"（HTTPS 端口号）	iDRAC6 侦听安全浏览器连接的端口。默认为 **443**。

表 5-31. SSH 设置

设置	说明
已启用	启用或禁用 SSH。**选中**复选框表示 SSH 已启用。
"Max Sessions"（最大会话数）	此系统允许的最大同时 SSH 会话数。支持同时 4 个 SSH 会话。不能编辑此字段。
"Active Sessions"（激活的会话数）	系统上的当前会话数。不能编辑此字段。
"Timeout"（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**。

"Port Number"（端口号）	iDRAC6 侦听 SSH 连接的端口。默认为 **22**。

表 5-32. Telnet 设置

设置	说明
已启用	启用或禁用 Telnet。**选中**后，就启用 Telnet。默认值为**取消选中**。
"Max Sessions"（最大会话数）	此系统允许的最大同时 Telnet 会话数。支持同时 4 个 Telnet 会话。不能编辑此字段。
"Active Sessions"（激活的会话数）	系统上的当前 Telnet 会话数。不能编辑此字段。
"Timeout"（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**。
"Port Number"（端口号）	iDRAC6 侦听 Telnet 连接的端口。默认为 **23**。

表 5-33. SNMP 设置

设置	说明
已启用	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。包含 SNMP 警报目标的 IP 地址的团体名称。团体名称长度最多为 31 个非空白字符。默认为 **public**。

表 5-34. 自动系统恢复代理

设置	说明
已启用	启用自动系统恢复代理。

更新 iDRAC6 固件

注： 如果 iDRAC6 固件损坏（例如 iDRAC6 固件更新在完成前被中断时可能发生），则可以使用 CMC 恢复 iDRAC6。请参阅《*CMC 固件用户指南*》了解相关说明。

注： 默认情况下，固件更新将保留当前 iDRAC6 设置。在更新过程中，可以选择将 iDRAC6 配置重设为工厂默认值。如果将配置设置为工厂默认值，外部网络访问会在更新完成后被禁用。必须使用 iDRAC6 配置公用程序或 CMC Web 界面启用并配置网络。

1. 启动 iDRAC6 Web 界面。
2. 单击**"System"（系统）**→**"Remote Access"（远程访问）**→ **iDRAC6**，然后单击**"Update"（更新）**选项卡。

   "**Firmware Update"（固件更新）**屏幕出现。

   注： 要更新固件，必须将 iDRAC6 置于更新模式。在该模式中，即使取消更新过程，iDRAC6 也会自动重设。
3. 在**"Upload"（上载）**部分中，单击**"Browse"（浏览）**并选择固件映像。

   例如：

   `C:\Updates\V2.2\`*<映像名称>*。

   默认固件映像名称为 **firmimg.imc**。
4. 单击**"Upload"（上载）**。该文件将被上载到 iDRAC6。This may take several minutes to complete.（完成此过程可能需要几分钟。）
5. 在**"Upload (Step 2 of 3)"（上载 [第 2 步，共 3 步]）**屏幕中，您将看到对上载的映像文件进行的验证结果。
   - 如果映像文件成功上载并通过所有验证检查，会出现一条说明固件映像已验证的信息。
   - 如果映像没有上载成功，或者没有通过验证检查，则重设 iDRAC6，关闭当前会话，然后尝试再次更新。

注： 如果取消选中**"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 已禁用。您将不能登录到 iDRAC6 Web 界面。必须使用 CMC Web 界面或在 BIOS 开机自检期间通过 iDRAC6 配置公用程序使用虚拟控制台重新配置 LAN 设置。

6. 默认情况下，**"Preserve Configuration"（保留配置）**复选框已**选中**，以便在升级后将当前设置保留在 iDRAC6 上。如果不想保留这些设置，则取消选中**"Preserve Configuration"（保留配置）**复选框。
7. 单击**"Begin Update"（开始更新）**开始升级过程。请不要中断升级过程。

8. 在**"Upload (Step 3 of 3)"（上载 [第 3 步，共 3 步]）**窗口中，将看到升级状态。固件升级操作的进度以百分比形式衡量，将显示在**"Progress"（进度）**列中。

9. 固件更新完成后，**"Upload (step 3 of 3)"（上载[第 3 步，共 3 步]）**窗口将刷新结果，iDRAC6 将自动重设。要继续通过 Web 界面访问 iDRAC6，关闭当前浏览器窗口并使用新浏览器窗口重新连接到 iDRAC6。

使用 CMC 更新 iDRAC6 固件

iDRAC6 固件一般使用 iDRAC6 公用程序更新，比如 iDRAC6 Web 界面，或者从 **support.dell.com** 下载的操作系统特定的更新软件包。

您可以使用 CMC Web 界面或 RACADM 来更新 iDRAC6 固件。此功能在 iDRAC6 固件处于正常模式和损坏时都可使用。

注： 请参阅《*Chassis Management Controller Firmware 用户指南*》了解使用 CMC Web 界面的说明。

要更新 iDRAC6 固件，请执行下列步骤：

1. 从 **support.dell.com** 将最新的 iDRAC6 固件下载到管理站上。

2. 登录到 CMC Web 界面。

3. 单击**系统树**中的**"Chassis"（机箱）**。

4. 单击 **Update**（更新）选项卡。**"Firmware Update"（固件更新）**屏幕出现。

5. 通过选择**"Update Targets"（更新目标）**复选框，选择要更新的一个 iDRAC6 或多个型号相同的 iDRAC6。

6. 单击 iDRAC6 组件列表下的**"Apply iDRAC6 Enterprise Update"（应用 iDRAC6 Enterprise 更新）**按钮。

7. 单击**"Browse"（浏览）**，浏览到下载的 iDRAC6 固件映像，并单击**"Open"（打开）**。

8. 单击**"Begin Firmware Update"（开始固件更新）**。

将固件映像文件上载到 CMC 后，iDRAC6 会用映像更新自己。

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 Web 界面并登录到远程系统。

   单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6**，然后单击**"Update"（更新）**选项卡。

2. 单击**"Rollback"（回滚）**。**"Rollback (Step 2 of 3)"（回滚 [第 2 步，共 3 步]）**页中显示当前固件版本和回滚固件版本。

3. 单击**"Next"（下一步）**开始固件回滚过程。

   在**"Rollback (Step 3 of 3)"（回滚 [第 3 步，共 3 步]）**页中，将看到回滚操作状态。成功完成后，会显示过程成功完成。

   如果固件回滚成功，iDRAC6 将自动重设。要继续通过 Web 界面访问 iDRAC6，关闭当前浏览器并使用新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。

   注： 如果想将 iDRAC6 固件从版本 2.2 回滚到版本 2.1，**"Preserve Configuration"（保留配置）**功能将不起作用。

目录

目录

使用 iDRAC6 目录服务

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

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。

您可通过 Microsoft Active Directory 登录至 iDRAC6 配置用户验证。您也可提供基于角色的授权，使得管理员可为各个用户配置特定权限。请参阅后续各部分获取更多信息。

表 6-1 显示 iDRAC6 Active Directory 用户权限。

表 6-1. iDRAC6 用户权限

权限	说明
"Login to iDRAC6"（登录到 iDRAC6）	允许用户登录到 iDRAC6
"Configure iDRAC6"（配置 iDRAC6）	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
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：

- Web 界面
- 本地 RACADM
- 用于 SM-CLP CLI 的 SSH 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 Web 界面登录且配置了用户域，则 Web 界面登录屏幕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"将 iDRAC6 用于 Microsoft Active Directory"中的上述登录语法，仍能够以 Active Directory 用户的身份登录。

为 iDRAC6 启用 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"在域控制器上启用 SSL"。

在域控制器上启用 SSL

当 iDRAC6 针对 Active Directory 域控制器验证用户，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 iDRAC6 中。换句话说，要使 iDRAC6 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：

1. 通过安装每个控制器的 SSL 证书启用每个域控制器上的 SSL。
   a. 单击**"Start"（开始）**→**"Administrative Tools"（管理工具）**→**"Domain Security Policy"（域安全策略）**。
   b. 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）**。
   c. 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）**。
   d. 单击**"Next"（下一步）**并单击**"Finish"（完成）**。

域控制器根 CA 证书导出到 iDRAC6

注： 如果系统运行 Windows 2000，以下步骤可能不同。

注： 如果使用单机版 CA，则以下步骤可能不同。

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，输入 mmc，然后单击**"OK"（确定）**。
4. 在**"Console 1"（控制台 1）**(MMC) 窗口中，单击**"File"（文件）**（在 Windows 2000 系统上则单击**"Console"[控制台]**）并选择**"Add/Remove Snap-in"（添加/删除管理单元）**。
5. 在**"Add/Remove Snap-in"（添加/删除管理单元）**窗口中，单击**"Add"（添加）**。
6. 在**"Standalone Snap-in"（独立管理单元）**窗口中，选择**"Certificates"（证书）**并单击**"Add"（添加）**。
7. 选择**"Computer"（计算机）**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）**并单击**"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 中保存的证书上载到 iDRAC6。

    要使用 RACADM 上载认证，请参阅 "使用 RACADM 以标准架构配置 Active Directory"。

    要使用 Web 界面上载证书，请参阅"使用 iDRAC6 Web 界面以标准架构配置 Active Directory"。

导入 iDRAC6 固件 SSL 证书

注： 如果 Active Directory Server 设置为在 SSL 会话初始化期间验证客户端，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 iDRAC6 控制器都配备有默认自签署证书。

要下载 iDRAC6 SSL 证书，请运行以下 RACADM 命令：

racadm sslcertdownload -t 0x1 -f <RAC SSL ÷§þÈ>

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

您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，该解决方案采用 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。
- 在不同 iDRAC6 卡上用不同权限级别配置用户权限时具有最大的灵活性。

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 在整个业界是唯一的，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，能够确保唯一性并且相互间不会冲突。为了扩展 Microsoft Active Directory 中的架构，Dell 为我们添加到目录服务的属性和类申请了唯一的 OID、唯一的名称扩展以及唯一链接的属性 ID。

- Dell 扩展名是：`dell`
- Dell 基础 OID 是：`1.2.840.113556.1.8000.1280`
- RAC LinkID 范围是：`12070` 到 `12079`

iDRAC6 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 iDRAC6 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、iDRAC6 权限和 iDRAC6 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

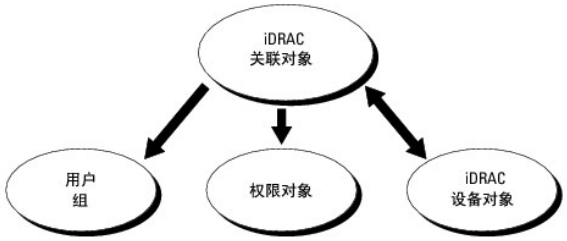
对于网络上每一个想与 Active Directory 集成以进行验证和授权的物理 iDRAC6 来说，请创建至少一个关联对象和一个 iDRAC6 设备对象。可以创建多个关联对象，每个关联对象都可以链接到任意多个用户、用户组或 iDRAC6 设备对象。用户和 iDRAC6 用户组可以是企业任何域中的成员。

不过，每个关联对象只能链接（或者可能链接用户、用户组或 iDRAC6 设备对象）到一个权限对象。此示例允许管理员控制特定 iDRAC6 设备上的每个用户权限。

iDRAC6 设备对象就是到 iDRAC6 固件的链接，用于查询 Active Directory 以进行验证和授权。将 iDRAC6 添加到网络后，管理员必须使用 Active Directory 名称配置 iDRAC6 及其设备对象，以便用户可以使用 Active Directory 执行验证和授权。管理员还必须将 iDRAC6 添加到至少一个关联对象以使用户能够验证。

图 6-1 说明关联对象提供了进行所有验证和授权所需的连接。

图 6-1. 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，对于网络上每一个想与 Active Directory 集成以使用 iDRAC6 验证和授权的 iDRAC6 设备来说，必须创建至少一个关联对象和一个 iDRAC6 设备对象。

关联对象允许任意数量的用户和/或组以及 iDRAC6 设备对象。然而，每个关联对象只有一个权限对象。关联对象连接那些对 iDRAC6 设备具有*权限*的*用户*。

ADUC MMC 管理单元的 Dell 扩展仅允许关联来自相同域的权限对象和 iDRAC6 对象到关联对象。Dell 扩展不允许来自其它域的 iDRAC6 对象添加为关联对象的产品成员。

添加来自不同域的通用组时，请创建一个具有通用范围的关联对象。Dell Schema Extender 公用程序创建的默认关联对象是域本地组，不能与来自其它域的通用组一起使用。

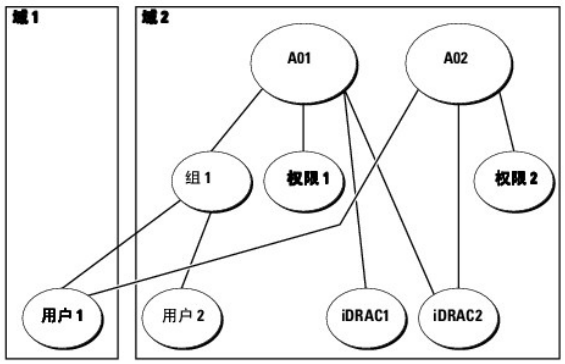
来自任何域的用户、用户组或嵌套的用户组都可以添加到关联对象中。扩展架构解决方案支持任何用户组类型和 Microsoft Active Directory 允许的多个域之间嵌入的任何用户组。

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 6-2 提供了使用扩展架构累积权限的示例。

图 6-2. 用户权限累积



该图显示两个关联对象 - A01 和 A02。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 现在拥有权限集：登录到 iDRAC、虚拟介质、清除日志、配置 iDRAC 和检测警报，即权限 1 和权限 2 权限的组合。

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。另外，此图显示用户 1 可在其它域，而且可以是组成员。

配置扩展架构 Active Directory 访问 iDRAC6

在使用 Active Directory 访问 iDRAC6 之前，按顺序执行下列步骤配置 Active Directory 软件和 iDRAC6：

1. 扩展 Active Directory 架构（请参阅"扩展 Active Directory 架构"）。
2. 扩展 Active Directory 用户和计算机管理单元（请参阅"安装 Dell 对 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"将 iDRAC6 用户和权限添加到 Active Directory"）。
4. 使用 iDRAC6 Web 界面或 RACADM 配置 iDRAC6 Active Directory 属性（请参阅"使用 iDRAC6 Web 界面以扩展架构配置 Microsoft Active Directory"或"使用 RACADM 以扩展架构配置 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**安装到您的目录中。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此产品的之前版本无影响。

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。有关安装信息，请参阅"安装 Dell 对 Active Directory 用户和计算机管理单元的扩展"。有关 iDRAC6 扩展架构和安装 Active Directory 用户和计算机 MMC 管理单元的进一步详情，请参阅 **support.dell.com/manuals** 提供的《*Dell OpenManage 安装和安全性用户指南*》。

注： 在您创建 iDRAC6 关联对象或 iDRAC6 设备对象时，选择**"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

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 "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

小心： 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 6-2 到表 6-7）
- 属性（表 6-8）

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 6-2. 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 6-3. dellRacDevice 类

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
说明	表示 Dell iDRAC6 设备。iDRAC6 必须在 Active Directory 中配置为 delliDRACDevice。这种配置使 iDRAC6 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 6-4. 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 6-5. dellRAC4Privileges 类

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
说明	为 iDRAC6 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 6-6. dellPrivileges 类

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

表 6-7. 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 6-8. 添加到 Active Directory 架构的属性的列表

属性名称/说明	分配的 OID/语法对象标识符	单值
dellPrivilegeMember 属于此属性的 dellPrivilege 对象的列表。	1.2.840.113556.1.8000.1280.1.1.2.1 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers 属于此角色的 dellRacDevice 和 DelliDRACDevice 对象的列表。此属性是指向 dellAssociationMembers 后退链接的前进链接。 链接 ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser 如果用户具有设备的登录权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin 如果用户具有设备的卡配置权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin 如果用户具有设备的用户配置权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin 如果用户具有设备的日志清除权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser 如果用户具有设备的服务器重设权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser 如果用户具有设备的虚拟控制台权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser 如果用户具有设备的虚拟介质权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser 如果用户具有设备的检测警报用户权限，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	1.2.840.113556.1.8000.1280.1.1.2.13	TRUE

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。	不区分大小写的字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
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 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 iDRAC6 设备、用户和用户组、iDRAC6 关联和 iDRAC6 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）**选项来扩展管理单元。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 64 位 Windows 操作系统来说，管理单元安装程序位于：

<DVD 驱动器>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

有关 Active Directory 用户和计算机管理单元的详情，请参阅 Microsoft 说明文件。

安装 Administrator Pack

必须在管理 Active Directory iDRAC6 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 iDRAC6 对象。

有关详情，请参阅"打开 Active Directory 用户和计算机管理单元"。

打开 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，单击**"Start"（开始）→"Run"（运行）**，输入 `MMC`，然后按 **Enter**。

   此时 MMC 会出现。

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 iDRAC6 用户和权限添加到 Active Directory

使用 Dell 扩展的 Active Directory 用户和计算机管理单元，您能够通过创建 iDRAC6、关联和权限对象添加 iDRAC6 用户和权限。要添加每种对象类型，请执行以下过程：

- 创建 iDRAC6 设备对象
- 创建权限对象
- 创建关联对象
- 将对象添加到关联对象

创建 iDRAC6 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）**。

   系统将显示**"New Object"（新建对象）**窗口。

3. 为新对象输入名称。该名称必须与准备在"使用 iDRAC6 Web 界面以扩展架构配置 Microsoft Active Directory"的步骤 A 中输入的 iDRAC6 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"（控制台根目录）**(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）**。

   系统将显示**"New Object"（新建对象）**窗口。
3. 为新对象输入名称。
4. 选择**"Privilege Object"（权限对象）**。
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）**选项卡并选择您希望用户或组拥有的权限（请参阅表 5-14）。

创建关联对象

注： iDRAC6 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"（控制台根目录）**(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. 为新对象输入名称。
4. 选择**"Association Object"（关联对象）**。
5. 选择**"Association Object"（关联对象）**的范围。
6. 单击**"OK"（确定）**。
7. 向验证用户提供访问创建的关联对象的访问权限。要执行此操作：
   a. 转到**"Administrative Tools"（管理工具）→ "ADSI Edit"**。此时将显示**"ADSI Edit"**窗口。
   b. 在右侧窗格中，导航至创建的关联对象，右键单击并选择**"Properties"（属性）**。
   c. 在**"Security"（安全）**选项卡中，单击**"Add"（添加）**。
   d. 键入"验证用户"，单击**"Check Names"（检查姓名）**，然后单击**"OK"（确定）**。"**验证用户**"被添加至**组和用户名称**列表中。
   e. 单击**"OK"（确定）**。

将对象添加到关联对象

使用**"Association Object Properties"（关联对象属性）**窗口，可以关联用户或用户组、权限对象和 iDRAC6 设备或 iDRAC6 设备组。

可以添加用户组和 iDRAC6 设备组。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. 输入用户或用户组名称并单击**"OK"（确定）**。

添加权限

1. 选择**"Privileges Object"（权限对象）**选项卡并单击**"Add"（添加）**。
2. 输入权限对象名称并单击**"OK"（确定）**。

单击**"Privilege Object"（权限对象）**选项卡，将权限对象添加到验证 iDRAC6 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 iDRAC6 设备或 iDRAC6 设备组。

要添加 iDRAC6 设备或 iDRAC6 设备组：

1. 选择**"Products"（产品）**选项卡并单击**"Add"（添加）。**
2. 输入 iDRAC6 设备或 iDRAC6 设备组名称并单击**"OK"（确定）**。
3. 在**"Properties"（属性）**窗口中，单击**"Apply"（应用）**，并单击**"OK"（确定）**。

单击**"Products"（产品）**选项卡，添加一个连接到网络的 iDRAC6 设备，供所定义的用户或用户组使用。您可将多个 iDRAC6 设备添加到一个关联对象。

使用 iDRAC6 Web 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 Web 界面。
3. 在系统树中选择**"System"（系统）→ "Remote Access"（远程访问）→ iDRAC6→ "Network/Security"（网络/安全性）**选项卡**→ "Directory Service"（目录服务）**？**Microsoft Active Directory**。

   随即显示 **Active Directory** 摘要屏幕。
4. 滚动到屏幕底部并单击**"Configure Active Directory"（配置 Active Directory）**。

   此时会显示 **"Step 1 of 4 Active Directory"（Active Directory 第 1 步，共 4 步）**屏幕。
5. 要验证 Active Directory 服务器的 SSL 证书，请选择**"Certificate Settings"（证书设置）**下的**"Certificate Validation Enabled"（启用证书验证）**复选框。

   如果不想验证 Active Directory 服务器的 SSL 证书，应跳至第 7 步 。
6. 在**"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）**下输入证书文件路径或浏览找到证书文件，然后单击**"Upload"（上载）**。

   注： 必须输入绝对文件路径，包括完整路径、完整文件名及文件扩展名。

   您上载的 Active Directory CA 证书的证书信息会在**"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）**部分出现。
7. 单击**"Next"（下一步）**。

   此时会出现 **"Step 2 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 2 步，共 4 步）**屏幕。
8. 选择**"Active Directory Enabled"（启用 Active Directory）**复选框。

   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。标准和扩展架构均支持单一登录 (SSO) 功能。

9. 单击**"Add"（添加）**以输入**用户域名**。在文本字段中输入域名，然后单击**"OK"（确定）**。 请注意，此步骤可选。如果您配置用户域列表，则会在 Web 界面登录屏幕上显示该列表。您可从列表中选择，然后只需输入用户名。

10. 在**"Timeout"（超时）**字段中输入您要让 iDRAC6 等待 Active Directory 应答的秒数。

11. 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。如果已配置，则忽略**"Domain Controller Server Addresses 1-3"（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。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。

    注： 当 DNS 查找失败或未返回任何服务器时，iDRAC6 不会将故障转移到指定的域控制器。

12. 选择**"Specify Domain Controller Addresses"（指定域控制器地址）**选项则允许 iDRAC6 使用 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 FQDN。当选择**"Specify Domain Controller Addresses"（指定域控制器地址）**选项时，要求至少配置三个地址之一。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**"Extended Schema"（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： 如果您启用证书验证，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"（主题替代名称）**字段相符。

13. 单击**"Next"（下一步）**。

    此时会出现 **"Step 3 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 3 步，共 4 步）**屏幕。

14. 在**"Schema Selection"（架构选择）**下选择**"Extended Schema Selection"（扩展架构选择）**复选框。

15. 单击**"Next"（下一步）**。

    此时会显示 **"Step 4 of 4 Active Directory"（Active Directory 第 4 步，共 4 步）**屏幕。

16. 在**"Extended Schema Settings"（扩展架构设置）**下输入 **iDRAC6 名称**和 **iDRAC6 域名**以配置 iDRAC6 设备对象及其在 Active Directory 中的位置。

17. 单击**"Finish"（完成）**保存更改，然后单击**"Done"（完成）**。

    此时会出现主**"Active Directory Configuration and Management"（Active Directory 配置与管理）**摘要页。接下来检测刚配置的 Active Directory 设置。

18. 滚动到屏幕底部并单击**"Test Settings"（检测设置）**。

    显示**"Test Active Directory Settings"（检测 Active Directory 设置）**屏幕。

19. 输入您的 iDRAC6 用户名和密码，然后单击**"Start Test"（开始检测）**。

    将显示检测结果和检测日志。有关其它信息，请参阅"检测配置"。

    注： 您必须拥有在 iDRAC6 上正确配置的 DNS 服务器才能支持 Active Directory 登录。导航至**"Network"（网络）**屏幕（单击**"System"[系统]** →**"Remote Access"[远程访问]**→ **iDRAC**6，然后单击**"Network/Security"[网络/安全性]** →**"Network"[网络]**选项卡）手动配置 DNS 服务器或使用 DHCP 获取 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 Active Directory

使用以下命令以通过 RACADM 命令行界面 (CLI) 工具而不是 Web 界面配置 iDRAC6 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： 您必须配置这三个地址中的至少一个。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。对于扩展架构来说，这些是此 iDRAC6 设备所在域控制器的 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。

如果要禁用 SSL 握手过程中的证书验证，请输入以下 RACADM 命令：

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

在此情况下，您无需上载 CA 证书。

如果要在 SSL 握手过程中执行证书验证，请输入以下 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 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"导入 iDRAC6 固件 SSL 证书"。

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

2. 如果 iDRAC6 上已启用 DHCP 并且希望使用 DHCP 服务器提供的 DNS，则输入以下 RACADM 命令：

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

3. 如果 iDRAC6 上已禁用 DHCP 或希望手动输入 DNS IP 地址，则输入以下 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>
```

4. 如果要配置用户域列表以便在登录到 iDRAC6 Web 界面时只需输入用户名，则输入以下命令：

```
racadm config -g cfgUserDomain -o cfgUserDomainName <域控制器的完全限定域名或 IP 地址> -i <索引>
```

您最多可配置 40 个用户域，其索引编号为 1 至 40。

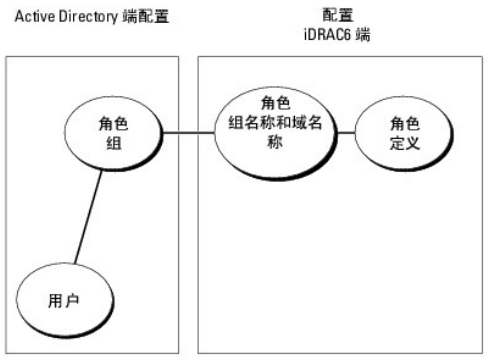
请参阅"将 iDRAC6 用于 Microsoft Active Directory"了解关于用户域的详情。

5. 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 6-3 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 6-3. 用 Microsoft Active Directory 和标准架构配置 iDRAC6



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 卡的权限，需要在特定 iDRAC6 卡上配置角色组名称及其域名。与扩展架构解决方案不同的是，角色和权限级别定义在各个 iDRAC6 卡上，而不是 Active Directory 中。每个 iDRAC6 中可配置和定义多达五个角色组。表 6-9 显示默认的角色组权限。

表 6-9. 默认角色组权限

角色组	默认权限级别	授予的权限	位掩码
角色组 1	None（无）	"**Login to iDRAC"（登录到 iDRAC）**、**"**Configure iDRAC"（配置 iDRAC）、"Configure Users"（配置用户）、**"Clear Logs"（清除日志）**、**"Execute Server Control Commands"（执行服务器控制命令）**、**"Access Virtual Console"（访问虚拟控制台）**、**"Access Virtual Media"（访问虚拟介质）**、**"Test Alerts"（检测警报）**、**"Execute Diagnostic Commands"（执行诊断命令）**	0x000001ff
角色组 2	None（无）	**"Login to iDRAC"（登录到 iDRAC）**、**"Configure iDRAC"（配置 iDRAC）**、**"Execute Server Control Commands"（执行服务器控制命令）**、**"Access Virtual Console"（访问虚拟控制台）**、**"Access Virtual Media"（访问虚拟介质）**、**"Test Alerts"（检测警报）**、**"Execute Diagnostic Commands"（执行诊断命令）**	0x000000f9
角色组 3	None（无）	"Login to iDRAC"（登录到 iDRAC）	0x00000001
角色组 4	None（无）	没有分配权限	0x00000000
角色组 5	None（无）	没有分配权限	0x00000000

注： "Bit Mask"（位掩码）值只有在用 RACADM 设置标准架构时才使用。

单域和多域情况

如果所有登录用户和角色组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以及嵌套组来自多个域，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）必须为通用组类型。

配置标准架构 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。添加作为 Active Directory 组成员访问 iDRAC6 的 Active Directory 用户。
3. 使用 Web 界面或 RACADM 在 iDRAC6 上配置组名称和域名（请参阅"使用 iDRAC6 Web 界面以标准架构配置 Active Directory"或"使用 RACADM 以标准架构配置 Active Directory"）。

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

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）→ "Remote Access"（远程访问）→ iDRAC6→ "Network/Security"（网络/安全性）**选项卡→ **"Directory Service"（目录服务）→ Microsoft Active Directory**。

   随即显示 **Active Directory** 摘要页。
4. 滚动到屏幕底部并单击**"Configure Active Directory"（配置 Active Directory）**。

   此时会显示 **"Step 1 of 4 Active Directory"（Active Directory 第 1 步，共 4 步）**屏幕。
5. 在**"Certificate Settings"（证书设置）**下，选择**"Certificate Validation Enabled"（启用证书验证）**。
6. 在**"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）**下输入证书文件路径或浏览找到证书文件，然后单击**"Upload"（上载）**。

   注： 必须输入绝对文件路径，包括完整路径、完整文件名及文件扩展名。

   您上载的 Active Directory CA 证书的证书信息会在**"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）**部分出现。
7. 单击**"Next"（下一步）**。

   此时会出现 **"Step 2 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 2 步，共 4 步）**屏幕。

8. 选择**"Active Directory Enabled"（启用 Active Directory）**复选框。

9. 选择**"Enable smart card Login"（启用智能卡登录）**会启用智能卡登录。以后使用 GUI 尝试登录时都会提示进行智能卡登录。

10. 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）**。

11. 单击**"Add"（添加）**以输入**用户域名**。在文本字段中输入域名，然后单击**"OK"（确定）**。 请注意，此步骤可选。如果您配置用户域列表，则会在 Web 界面登录屏幕上显示该列表。您可从列表中选择，然后只需输入用户名。

12. 在**"Timeout"（超时）**字段中输入您要让 iDRAC6 等待 Active Directory 应答的秒数。

13. 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。如果已配置，则忽略**"Domain Controller Server Addresses 1-3"（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。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**"Standard Schema"（标准架构）**，域控制器是用户帐户和角色组所在的地址。

14. 选择**"Specify Domain Controller Addresses"（指定域控制器地址）**选项则允许 iDRAC6 使用 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 FQDN。当选择**"Specify Domain Controller Addresses"（指定域控制器地址）**选项时，要求至少配置三个地址之一。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**"Standard Schema"（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。

    注： 当 DNS 查找失败或未返回任何服务器时，iDRAC6 不会将故障转移到指定的域控制器。

15. 单击**"Next"（下一步）**。

    此时会出现 **"Step 3 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 3 步，共 4 步）**屏幕。

16. 在**"Schema Selection"（架构选择）**下选择**"Standard Schema Selection"（标准架构选择）**复选框。

17. 单击**"Next"（下一步）**。

    此时会显示**"Step 4a of 4 Active Directory"（Active Directory 第 4a 步，共 4 步）**屏幕。

18. 在**"Standard Schema Settings"（标准架构设置）**下，选择**"Look Up Global Catalog Servers with DNS"（利用 DNS 查找全局编录服务器**）选项并输入要在 DNS 查找中使用的**"Root Domain Name"（根域名）**以获得 Active Directory 全局编录服务器。如果已配置，则忽略"Global Catalog Server Addresses 1-3"（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。

    注： 当 DNS 查找失败或未返回任何服务器时，iDRAC6 不会将故障转移到指定的全局编录服务器。

19. 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。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。

    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。如果使用 iDRAC6 Web GUI 配置 Active Directory，则需要输入全局地址，即使用户和组都处于同一域。

20. 单击**"Role Group"（角色组）**按钮添加一个角色组。

    此时会出现**"Step 4b of 4 Configure Role Group"（配置角色组第 4b 步，共 4 步）**屏幕。

21. 输入**"Group name"（组名称）**。组名称标识与 iDRAC6 关联的 Active Directory 角色组。

22. 输入**"Group Domain"（组域）**。**"Group Domain"（组域）**是目录林的完全限定 Root 域名。

23. 在**"Role Group Privileges"（角色组权限）**部分中，设置组权限。请参阅表 5-14 了解角色组权限的信息。

    注： 如果修改任何权限，现有角色组权限（管理员、高级用户或客用户）将会根据修改的权限更改为自定义组或相应角色组权限。

24. 单击**"OK"（确定）**保存角色组设置。

    此时会显示一个警报对话框，表明您的设置已经更改。单击**"OK"（确定）**返回到**"Step 4a of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 4a 步，共 4 步）**屏幕。

25. 要添加额外角色组，请重复步骤 20 到步骤 24。

26. 单击**"Finish"（完成）**，然后单击**"Done"（完成）**。

    此时会出现主**"Active Directory Configuration and Management"（Active Directory 配置与管理）**摘要屏幕。检测刚配置的 Active Directory 设置。

27. 滚动到屏幕底部并单击**"Test Settings"（检测设置）**。

    此时会出现**"Test Active Directory Settings"（检测 Active Directory 设置）**屏幕。

28. 输入您的 iDRAC6 用户名和密码，然后单击**"Start Test"（开始检测）**。

    将显示检测结果和检测日志。有关其它信息，请参阅"检测配置"。

    注： 您必须拥有在 iDRAC6 上正确配置的 DNS 服务器才能支持 Active Directory 登录。导航至**"Network"（网络）**屏幕（单击**"System"[系统] → "Remote Access"[远程访问] → iDRAC6**，然后单击**"Network / Security"[网络 / 安全性] → "Network"[网络]**选项卡）手动配置 DNS 服务器或使用 DHCP 获取 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 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 iDRAC6 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 <特定角色组权限的位掩码值>
   ```

   注： 有关特定角色组权限位掩码值的信息，请参阅表 6-9。

   ```
   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： 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。

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

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

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

   注： 标准架构仅在用户帐户和角色组位于不同域时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"（主题替代名称）**字段相符。

   如果要禁用 SSL 握手过程中的证书验证，请输入以下 RACADM 命令：

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

   在此情况下，无需上载认证机构 (CA) 证书。

   如果要在 SSL 握手过程中执行证书验证，请输入以下 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"导入 iDRAC6 固件 SSL 证书"。

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

2. 如果 iDRAC6 上已启用 DHCP 并且希望使用 DHCP 服务器提供的 DNS，则输入以下 RACADM 命令：

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

3. 如果 iDRAC6 上已禁用 DHCP 或者想手动输入 DNS IP 地址，则输入以下 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>
```

4. 如果要配置用户域列表以便在登录到 Web 界面时只需输入用户名，则输入以下命令：

```
racadm config -g cfgUserDomain -o cfgUserDomainName <域控制器的完全限定域名或 IP 地址> -i <索引>
```

最多可配置 40 个用户域，其索引编号为 1 至 40。

请参阅"将 iDRAC6 用于 Microsoft Active Directory"了解关于用户域的详情。

检测配置

如果要验证您的配置是否有效或需要诊断失败 Active Directory 登录的问题，您都可从 iDRAC6 Web 界面检测设置。

在 iDRAC6 Web 界面中完成配置设置后，单击屏幕底部的**"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屏幕底部显示。

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"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。

将 iDRAC6 和 LDAP 目录服务一起使用

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。

要使 iDRAC6 LDAP 实施变为通用，须将不同目录服务之间的共同性用于组用户，并映射用户组关系。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。登录用户必须输入用户名，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。在启用通用 LDAP 后，GUI 登录页面的下菜单中仅显示**"This iDRAC"（此 iDRAC）**。

注： 在此版本中，仅支持 openLDAP 和基于 openDS 的目录服务。"<"和">"字符不允许在 openLDAP 和 OpenDS 的用户名中使用。

使用 iDRAC6 基于 Web 的界面配置通用 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. 展开**"System"（系统）**树并单击**"Remote Access"（远程访问）**→ **iDRAC6**→ **"Network/Security"（网络/安全性）**选项卡→ **"Directory Service"（目录服务）** → **"Generic LDAP Directory Service"（通用 LDAP 目录服务）**。

4. "**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）**。

   注： 在此版本中，仅支持不带扩展的标准架构 Active Directory (SSAD)。

   此时会出现**"Step 1 of 3 Generic LDAP Configuration and Management"（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。

5. 在**"Certificate Settings"（证书设置）**下面，选中**"Enable Certificate Validation"（启用证书验证）**可启用证书验证。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）。服务器证书中的 CN 字段设置应与 iDRAC6 的 LDAP 服务器地址字段相匹配，证书验证才能正常进行。

6. 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。

7. 单击**"Upload"（上载）**。

   随即上载签署域控制器的所有安全套接字层 (SSL) 服务器证书的根 CA 证书。

8. 单击**"Next"（下一步）**以转至**"Step 2 of 3 Generic LDAP Configuration and Management"（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，通用 LDAP 目录服务不支持基于双重验证 (TFA) 的智能卡和单一登录 (SSO) 功能。

9. 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。

10. 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。如果未选中，则使用由登录用户提供的用户名与组成员进行比较。

11. 在**"LDAP Server Address"（LDAP 服务器地址）**字段中，输入LDAP 服务器的 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。

12. 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。

13. 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。

14. 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。

15. 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。

16. 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 中此值应是唯一的，否则，必须配置搜索筛选器以确保登录用户的唯一性。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。

17. 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 member 和 uniquemember 属性。

18. 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。

19. 单击**"Next"（下一步）**以转至**"Step 3a of 3 Generic LDAP Configuration and Management"（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。

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

    此时会出现**"Step 3b of 3 Generic LDAP Configuration and Management"（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。

21. 输入**"Group Distinguished Name (DN)"（组可分辨名称）**，以识别与 iDRAC6 相关的通用 LDAP 目录服务中的角色组。

22. 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。

23. 单击**"Apply"（应用）**以保存角色组设置。

    iDRAC6 Web 服务器自动返回**"Step 3a of 3 Generic LDAP Configuration and Management"（通用 LDAP 配置和管理第 3a 步，共 3 步）**页，该页显示了您的角色组设置。

24. 如需要，配置其它角色组。

25. 单击**"Finish"（完成）**返回**"Generic LDAP Configuration and Management"（通用 LDAP 配置和管理）** 摘要**页**。

26. 单击**"Test Settings"（检测设置）**检查 LDAP 设置。

27. 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。

    注： 在选中**"Enable Certificate Validation"（启用证书验证）**时检测 LDAP 设置，iDRAC6 要求 LDAP 服务器通过 FQDN 而不是通过 IP 地址识别。如果 LDAP 服务器通过 IP 地址识别，则证书验证失败，这是因为 iDRAC6 无法与 LDAP 服务器通信。

将显示检测结果和检测日志。您已完成**"Generic LDAP Directory Service"（通用 LDAP 目录服务）** 配置。

常见问题

Active Directory 登录问题

使用 Active Directory 单一登录 iDRAC6 需要将近 4 分钟。

正常 Active Directory 单一登录通常用不到 10 秒，但是如果在 iDRAC6 **"Network"（网络）**页指定了**"Preferred DNS Server"（首选 DNS 服务器）**和 **"Alternate DNS Server"（备用 DNS 服务器）**并且首选 DNS 服务器出现故障，则使用 Active Directory 单一登录功能登录 iDRAC6 可能需要将近 4 分钟。DNS 服务器停机时会出现 DNS 超时。iDRAC6 使用备用 DNS 服务器登录。

我已为 Windows Server 2008 Active Directory 中的域配置了 Active Directory 并已进行这些配置。该域中有一个子域，用户和组位于同一子域，并且用户是组的成员。现在如果用子域中的用户尝试登录 iDRAC6，Active Directory 单一登录将会失败。

这可能是错误的组类型造成的。Active Directory 服务器中有两种组类型：

- **安全** - 安全组允许管理用户和计算机到共享资源的访问并过滤组策略设置。
- **分发** - 分发组仅供用于电子邮件分发列表。

应始终确保组类型是**安全**。不能使用分发组在任何对象上分配权限并用来筛选组策略设置。

我的 Active Directory 登录失败。我应该怎么做？

iDRAC6 在 Web 界面中提供诊断工具。

1. 从 Web 界面以拥有管理员权限的本地用户身份登录。

2. 在系统树中，选择**"System"（系统）**→ **"Remote Access"（远程访问）**→ **iDRAC6**→ **"Network/Security"（网络/安全性）**选项卡→ **"Directory Service"（目录服务）**→ **Microsoft Active Directory**。

   随即显示 **Active Directory** 摘要屏幕。

3. 滚动到屏幕底部并单击**"Test Settings"（检测设置）**。

   显示"**Test Active Directory Settings"（检测 Active Directory 设置）**屏幕。

4. 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。iDRAC6 也会记录详细的检测结果以帮助您解决任何问题。

   如果问题仍然存在，请配置 Active Directory 设置，更改用户配置并重新运行检测，直到检测用户通过授权步骤。

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。问题是什么以及如何修复？

```
ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.（错误：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。)

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：

- iDRAC6 日期不在服务器证书或 CA 证书的有效期内。检查 iDRAC6 时间和证书的有效期。
- 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。
  - 如果您使用 IP 地址，请参阅"我使用域控制器地址的 IP 地址且不能通过证书验证。是什么问题？"。
  - 如果您使用 FQDN，请保证您使用域控制器的 FQDN 而不是域本身。例如，使用 servername.example.com，而*不是* example.com。

如果不能使用 Active Directory 登录到 iDRAC6，应检查什么？

首先用检测设置功能诊断问题。有关说明，请参阅"我的 Active Directory 登录失败。我应该怎么做？"。

然后，解决检测结果所指明的具体问题。有关其它信息，请参阅"检测配置"。

本节解释最常见的问题。但一般来说，您应检查如下内容：

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。
   a. 确保在**"Step 2 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 2 步，共 4 步）**页中选中**"Active Directory Enabled"（启用 Active Directory）**复选框。
   b. 如果已启用证书验证，确保已将正确的 Active Directory 根 CA 证书上载到 iDRAC6。此证书在**"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）**区域中显示。确保 iDRAC6 时间在 CA 证书的有效期内。
   c. 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，则确保**组名称**和**组域**与 Active Directory 配置相符。
   d. 导航至**"Network"（网络）**屏幕。选择**"System"（系统）→ "Remote Access"（远程访问）→ iDRAC6 → "Network/Security"（网络/安全性）→"Network"（网络）**。
      确保 DNS 设置正确。
   e. 检查域控制器 SSL 证书以确保 iDRAC6 时间在证书的有效期内。

Active Directory 证书验证

我使用域控制器地址的 IP 地址且不能通过证书验证。是什么问题？

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）字段使用域控制器的主机名而不是 IP 地址。您可通过以下措施解决此问题：

- 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。
- 重新签发服务器证书，使用在"Subject"（主题）或"Subject Alternative Name"（主题备用名称）字段中的 IP 地址，以便与 iDRAC6 中配置的 IP 地址相符。
- 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。

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。

扩展架构和标准架构

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？

使用 iDRAC6 对象所在域中域控制器的主机名称 (FQDN) 或 IP 地址。

需要配置全局编录地址吗？

如果使用扩展架构，就不能配置全局编录地址，因为扩展架构不使用此地址。

如果使用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，您只能使用通用组。

如果使用标准架构且所有用户和所有角色组都在相同域中，则不要求配置全局编录地址。

标准架构的查询方式是什么？

iDRAC6 首先连接到配置的域控制器地址。如果用户和角色组在该域内，则保存权限。

如果配置了全局控制器地址，则 iDRAC6 会继续查询全局编录。如果从全局编录检索到额外的权限，则会累加这些权限。

其它

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*期间，iDRAC6 执行 LDAP CONNECT 操作仅是为了找出问题，而不会对不安全的连接执行 LDAP BIND 操作。

iDRAC6 支持 NetBIOS 名称吗？

此版本不支持。

目录

目录

配置 iDRAC6 为单一式登录和智能卡登录

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

本节提供了将 iDRAC6 配置为本地用户和 Active Directory 用户智能卡登录及 Active Directory 用户单一登录 (SSO) 的信息。

iDRAC6 支持基于 Kerberos 的 Active Directory 验证来支持 Active Directory 智能卡和单一 (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标准，iDRAC6 现在支持基于 Kerberos 的 Active Directory 验证来支持 Active Directory 智能卡和单一 (SSO) 登录。

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 将 Kerberos 用作默认的验证方法。

iDRAC6 使用 Kerberos 支持两种验证机制 — Active Directory 单一登录和 Active Directory 智能卡登录。对于单一登录，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。

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，请同步服务器与域控制器的时间，然后**重设** iDRAC6。

还可以使用以下 RACADM 时差命令同步时间：

```
racadm config -g cfgRacTuning -o

cfgRacTuneTimeZoneOffset <offset value>
```

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为：

- 配置 iDRAC6 进行 Active Directory 登录。有关详情，请参阅"使用 iDRAC6 目录服务"。
- 注册 iDRAC6 作为 Active Directory 根域中的计算机。
  a. 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"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 iDRAC6 on DNS"（在 DNS 上注册 iDRAC6）**。
  d. 提供有效**"DNS Domain Name"（DNS 域名）**。
  e. 验证网络 DNS 配置与 Active Directory DNS 信息匹配。

  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.exe -princ HTTP/idracname.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype
  KRB5_NT_PRINCIPAL -pass <密码> +DesOnly -out c:\krbkeytab
  ```

  注： 如果发现 keytab 文件创建所针对的 iDRAC6 用户有问题，应创建新的用户和新的 keytab 文件。如果再执行原来创建的 keytab 文件，将不会正确配置。

成功执行以上命令后，运行以下命令：

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

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 property"（为此帐户使用 DES 加密类型）。

注： 必须创建 Active Directory 用户帐户以供 **ktpass** 命令的 -mapuser 选项使用。另外，应将同一名称作为要上载所生成 keytab 文件的 iDRAC6 DNS 名称。

注： 建议使用最新的 **ktpass** 公用程序创建 Keytab 文件。此外，生成 keytab 文件期间，应使用小写字母用于 **idracname** 和**服务主体名称**。

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://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

- iDRAC6 时间应与 Active Directory 域控制器同步。

浏览器设置为启用 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 **Sites（站点）**。
4. 仅选择以下选项：
   - 包含在其他区域中未列出的所有本地 (intranet) 站点。
   - 包含不适用代理服务器的所有站点。
5. 单击 **Advanced（高级）**。
6. 向将用作 SSO 配置一部分的 iDRAC 实例添加所有要使用的相关域名（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 enter network.negotiate。
4. 将 iDRAC 名称添加至 network.negotiate-auth.trusted-uris（使用逗号分隔列表）。
5. 将 iDRAC 名称添加至 network.negotiate-auth.delegation-uris（使用逗号分隔列表）。

使用 Active Directory SSO

可以使 iDRAC6 能够使用 Kerberos（一种网络验证协议）来启用单一登录。有关设置 iDRAC6 以使用 Active Directory 单一登录功能的详情，请参阅"Active Directory SSO 和智能卡验证的前提条件"。

配置 iDRAC6 使用 SSO

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）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）**选项卡→ **"Network"（网络）**。
在**"Network"（网络）**页中，验证**"DNS iDRAC6 Name"（DNS iDRAC6 名称）**是否正确并匹配 iDRAC6 完全限定域名。

4. 在系统树中，选择**"System"（系统）→ "Remote Access"（远程访问）→ iDRAC6→ "Network/Security"（网络/安全性）**选项卡→ **"Directory Service"（目录服务）→ Microsoft Active Directory**。

   随即显示 **Active Directory** 摘要屏幕。

5. 滚动到屏幕底部并单击**"Configure Active Directory"（配置 Active Directory）**。

   显示**"Active Directory Configuration and Management Step 1 of 4"（Active Directory 配置与管理第 1 步，共 4 步）**屏幕。

6. 要验证 Active Directory 服务器的 SSL 证书，请选择**"Certificate Settings"（证书设置）**下的"**Enable** Certificate Validation"（启用证书验证）复选框。

   如果不想验证 Active Directory 服务器的 SSL 证书，则无需采取任何措施，并跳到步骤 8。

7. 在**"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）**下输入证书文件路径或浏览找到证书文件，然后单击**"Upload"（上载）**。

   注： 必须输入绝对文件路径，包括完整路径、完整文件名及文件扩展名。

   您上载的 Active Directory CA 证书的证书信息会在**"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）**部分出现。

8. 单击**"Next"（下一步）**。

   显示**"Active Directory Configuration and Management Step 2 of 4**"（Active Directory 配置与管理第 2 步，共 4 步）屏幕。

9. 选择**"Enable Active Directory"（启用 Active Directory**）复选框。

10. 如果要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）就直接登录 iDRAC6，选择**"Enable Single Sign-on"（启用单一登录）**。

    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。

    将 iDRAC6 配置为使用单一登录 (SSO) 之前，确保已执行下列步骤：

    a. 在 Active Directory 服务器中已创建设备对象、权限对象和关联对象。

    b. 为创建的权限对象设置访问权限。建议不要提供管理员权限，因为管理员权限会绕过某些安全检查。

    c. 使用关联对象关联设备对象和权限对象。

    d. 将之前的 SSO 用户（登录用户）添加至设备对象。

    e. 为*验证用户*提供访问权限，以访问创建的关联对象。

       有关如何执行这些步骤的信息，请参阅" 将 iDRAC6 用户和权限添加到 Active Directory"。

    要使用 CLI 启用 SSO，请运行 RACADM 命令：

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

11. 添加**"User Domain Name"（用户域名）**，并输入域控制器服务器地址的 IP 地址。选择**"Look Up Domain Controllers with DNS"（利用 DNS 查找域控制器）**或**"Specify Domain Controller Addresses"（指定域控制器地址）**。选择**"Next"（下一步）**。显示**"Active Directory Configuration and Management Step 3 of 4**"（Active Directory 配置与管理第 3 步，共 4 步）屏幕。

12. 选择**"Standard Schema"（标准架构）**或**"Extended Schema"（扩展架构）**选项，然后单击**"Next"（下一步）**。

    如已选择**"Standard Schema"（标准架构）**，请转至第 13 步。如已选择**"Extended Schema"（扩展架构）**，请转至第 14 步。

13. 对于标准架构：

    a. 在**"Active Directory Step 4a of 4"**（Active Directory 第 4a 步，共 4 步）页中，输入**"Global Catalog Server"（全局编录服务器）**的 IP 地址或选择**"Look Up Global Catalog Servers with DNS"（利用 DNS 查找全局编录服务器）**选项并输入 DNS 查找所使用的**"Root Domain Name"（根域名）**以获得 Active Directory 全局编录服务器。

    b. 单击任意角色组，并添加有效 Active Directory 用户所属角色组的信息。显示"**Active Directory Step 4b of 4"（Active Directory 第 4b 步，共 4 步）**屏幕。

    c. 输入角色组名称、组域名、角色组权限级别以及要求的权限，然后单击**"Finish"（完成）**。显示"Configuration set successfully (成功设置配置)"（配置成功设置）消息。单击 **OK（确定）**。**"Step 4a of 4"（第 4a 步，共 4 步）**屏幕显示创建的角色组名称、组域和组权限级别。

    d. 单击 **Finish**（完成）。系统将显示成功信息。

14. 对于扩展架构，在**"Active Directory Step 4 of 4"（Active Directory 第 4 步，共 4 步）**屏幕中，输入 **iDRAC6 名称**和 **iDRAC6 域名**，然后单击**"Finish"（完**

成）。系统将显示成功信息。

使用 SSO 登录至 iDRAC6

1. 使用有效 Active Directory 网络帐户登录 Management Station。
2. 使用 iDRAC6 完全限定域名登录 iDRAC6 Web 页面：

   http://idracname.domain.com。

iDRAC6 会使用在用户使用有效 Active Directory 网络帐户登录时缓存在操作系统中的凭据来使用户登录。

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。

在 iDRAC6 中配置智能卡登录

要从 Web 界面启用 iDRAC6 智能卡登录功能：

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 Web 界面。
3. 转到**"Step 1 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 1 步，共 4 步）**屏幕。
4. 要验证 Active Directory 服务器的 SSL 证书，请选择**"Certificate Settings"（证书设置）**下的**"Certificate Validation Enabled"（启用证书验证）**复选框。如果不想验证 Active Directory 服务器的 SSL 证书，应跳至 步骤 6。
5. 在**"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）**下输入证书文件路径或浏览找到证书文件，然后单击**"Upload"（上载）**。必须输入绝对文件路径，包括完整路径、完整文件名及文件扩展名。您上载的 Active Directory CA 证书的证书信息会在**"Current Active Directory CA Certificate"（当前 Active Directory CA 证书）**部分出现。
6. 单击"Next"（下一步）。此时会出现**"Step 2 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 2 步，共 4 步）**屏幕。
7. 选择**"Active Directory Enabled"（启用 Active Directory）**复选框。
8. 选择**"Enable SmartCCard Login"（启用智能卡登录）**启用智能卡登录。以后使用 GUI 尝试登录时都会提示进行智能卡登录。
9. 添加**"User Domain Name"（用户域名）**，并输入域控制器服务器地址的 IP 地址。选择**"Next"（下一步）**。
10. 在**"Step 3 of 4 Active Directory Configuration and Management"（Active Directory 配置与管理第 3 步，共 4 步）**页上选择**"Standard Schema Settings"（标准架构设置）**。选择**"Next"（下一步）**。
11. 在**"Step 4a of 4 Active Directory"（Active Directory 第 4a 步，共 4 步）**上，输入**全局编录服务器**的 IP 地址。通过选择一个角色组（**"Step 4B of 4 Configure Role Group"[配置角色组第 4B 步，共 4 步]** 页）添加有效 Active Directory 用户所属角色组的信息。输入**"Group Name"（组名称）**、**"Group Domain"（组域）**和**"Role Group Privileges"（角色组权限）**。选择**"OK"（确定）**，然后选择**"Finish"（完成）**。选择**"Done"（完成）**后，回滚到 **Active Directory** 摘要页的底部并选择**"Kerberos Keytab Upload"（Kerberos Keytab 上载）**。
12. 上载有效的 Kerberos Keytab 文件。确保 Active Directory Server 和 iDRAC6 时间同步。上载 keytab 文件前验证时间和时区都正确。有关创建 Keytab 文件的详情，请参阅"配置 iDRAC6 为单一式登录和智能卡登录"。

清除**"Enable SmartCCard Login"（启用智能卡登录）**选项以禁用 TFA 智能卡登录功能。下次登录 iDRAC6 GUI 时，会提示输入 Microsoft Active Directory 或本地登录用户名和密码，这是 Web 界面的默认登录提示。

使用 Active Directory 智能卡验证登录 iDRAC6

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 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 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. 插入智能卡。

3. 输入 PIN，并单击**"Log in"（登录）**。

   将会使用在 Active Directory 中设置的凭据登录 iDRAC6。

   注： 无需将智能卡 一直留在读卡器中来保持登录。

有关 SSO 的常见问题

在 Windows 7 和 Windows Server 2008 R2 中 SSO 登录失败。

必须为 Windows 7 和 Windows Server 2008 R2 启用加密类型 DES_CBC_CRC 和 DES_CBC_MD5。要启用加密类型：

1. 以管理员或具有管理员权限的用户身份登录。
2. 前往**"Start"（开始）**并运行 **gpedit**。显示**"Local Group Policy Editor"（本地组策略编辑器）**窗口。
3. 前往**"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）**。

对 iDRAC6 中的智能卡登录进行故障排除

参考以下提示帮助调试无法访问的智能卡：

差不多需要 4 分钟使用 Active Directory 智能卡登录 iDRAC6。

正常 Active Directory 智能卡登录通常用不到 10 秒，但是如果在 iDRAC6 **"Network"（网络）**页中指定**"Preferred DNS Server"（首选 DNS 服务器）**和**"Alternate DNS Server"（备用 DNS 服务器）**，并且首选 DNS 服务器失败，则使用 Active Directory 智能卡登录 iDRAC6 差不多需要 4 分钟。DNS 服务器停机时会出现 DNS 超时。iDRAC6 使用备用 DNS 服务器登录。

ActiveX 插件无法检测到智能卡阅读器

确保 Microsoft Windows 操作系统支持 Smart Card。Windows 支持有限的几种智能卡加密服务提供程序 (CSP)。

提示：作为常规检查看智能卡 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。可以使用以下命令通过 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 验证插件不会正确安装。需要部署 32 位版本的"Microsoft Visual C++ 2005 Redistributable Package"才能正确安装并运行插件。

- 如果收到以下错误信息"Not able to load the Smart Card PlugCin.Please check your IE settings or you may have insufficient privileges to use the Smart Card PlugCin"（无法载入智能卡插件。请检查 IE 设置或是否有足够权限使用智能卡插件），然后再安装"Microsoft Visual C++ 2005 Redistributable Package"。该文件位于 Microsoft 网站 **www.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：

表 7-1. 分发版本的 C++ Redistributable Package

Redistributable Package 文件名	Version（版本）	发布日期	Size（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互在 5 分钟之内以确保 Kerberos 验证。请查阅**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Properties"（属性）→"Remote Access Information"（远程访问信息）**页上的 **iDRAC6 时间**，以及通过右键单击屏幕右下角的时间显示的域控制器时间。时差显示在弹出框中。对于美国中部标准时间 (CST)，该值为 C6。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 Co cfgRacTuneTimeZoneOffset <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，设置 iDRAC6 时间为 GMT 时间 18:00 将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"。

目录

目录

查看受管服务器的配置和运行状况

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

系统摘要

"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）**选项卡→ **"System Summary"（系统摘要）**。请参阅 iDRAC6 联机帮助，了解**"System Summary"（系统摘要）**页中每个部分的详细信息。

系统详细信息

"System Details"（系统详细信息）页显示关于以下系统组件的信息：

- 系统主机柜
- Integrated Dell Remote Access Controller 6 - Enterprise

系统主机柜

系统信息

iDRAC6 Web 界面的该部分提供有关受管服务器的以下基本信息：

- 说明 — 受管服务器的型号或名称
- BIOS 版本 — 受管服务器的 BIOS 版本号
- 服务标签 — 服务器的服务标签号码
- 主机名 — 与受管服务器相关联的 DNS 主机名
- 操作系统名称 — 安装在受管服务器上的操作系统名称

  注： 只有当 Managed System 上装有 Dell OpenManage Server Administrator 时，**"OS Name"（操作系统名称）**字段才会显示。例外就是 VMware 操作系统名称，即使 Managed System 上没有安装 Server Administrator 也会显示该名称。

- 系统修订版本 — 机箱版本号。

I/O 夹层卡

iDRAC6 Web 界面的本部分提供有关安装在受管服务器上的 I/O 夹层卡的以下信息：

- 位置 — 列出安装在 Managed Server 上的输入/输出夹层卡。该列表还显示了支持扩充卡的平台的 I/O 夹层卡。
- 存在状态 — 表示是否存在夹层卡，或是否为其他结构的夹层卡槽的扩展。
- 插卡类型 — 已安装的夹层卡/连接的物理类型
- 型号名称 — 已安装的夹层卡的型号、类型或说明

集成的存储卡

iDRAC6 Web 界面的本部分提供有关安装在受管服务器上的集成存储控制器卡的信息：

- 插卡类型 — 显示已安装存储卡的型号名称，如 SAS6/iR

集成网卡

iDRAC6 Web 界面的本部分提供有关安装在受管服务器上的集成网卡的以下信息： 仅为适用的平台显示。

- 卡类型 — 显示安装在主板上的集成网卡的类型，例如千兆位以太网
- 模块名称 — 显示集成网卡的型号名称。

有关集成网卡的更多信息，请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*硬件用户手册*》。

自动恢复

iDRAC6 Web 界面的本部分详细介绍通过 Open Manage Server Administrator 设置的受管服务器自动恢复功能的当前工作模式：

- 恢复操作 — 当检测到系统故障或*挂起*时执行的操作。可用操作有**"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）**。
- 初始倒计数 — 检测到系统挂起后执行 iDRAC6 恢复操作前所需的时间（以秒为单位）。
- 当前倒计数 — 倒计数计时器的当前值（以秒为单位）。

Integrated Dell Remote Access Controller 6 - Enterprise

iDRAC6 信息

iDRAC6 Web 界面的本部分提供有关 iDRAC6 自身的以下信息：

- 日期/时间 — 显示 iDRAC6 的当前日期和时间（即屏幕最后刷新时间）
- 固件版本 — 显示 Managed System 上安装的 iDRAC6 固件的当前版本
- CPLD 版本 — 显示板卡的复杂可编程逻辑设备 (CPLD) 版本。
- 扩展 CPLD 版本 — 显示扩展版 CPLD 版本。
- 固件更新 — 显示上次成功更新 iDRAC6 固件的日期和时间
- MAC 地址 — 显示与 iDRAC6 的 LOM（母板上的 LAN）网络接口控制器相关联的 MAC 地址

IPv4 设置

- 启用 — 显示 IPv4 协议支持是已启用还是禁用

  注： IPv4 协议选项默认为启用。

- DHCP 已启用 — 如果 iDRAC6 设置为从 DHCP 服务器获取其 IP 地址和相关信息则启用
- IP 地址 — 显示与 iDRAC6（非受管服务器）相关的 IP 地址
- 子网掩码 — 显示为 iDRAC6 配置的 TCP/IP 子网掩码
- 网关 — 显示为 iDRAC6 配置的网络网关的 IP 地址
- 使用 DHCP 获取 DNS 服务器地址 — 显示是否使用 DHCP 获取 DNS 服务器地址
- 首选 DNS 服务器 — 显示当前活动的主要 DNS 服务器
- 备用 DNS 服务器 — 显示备用 DNS 服务器地址

IPv6 设置

- 启用 — 显示 IPv6 协议支持是已启用还是禁用
- 启用自动配置 — 显示是否已启用或禁用自动配置
- 链接本地地址 — 显示 iDRAC6 NIC 的 IPv6 地址
- IPv6 地址 1-16 — 显示 iDRAC6 NIC 的 16 个 IPv6 地址（IPv6 地址 1 至 IPv6 地址 16）。
- 网关 — 显示为 iDRAC6 配置的网络网关的 IP 地址
- 使用 DHCPv6 获取 DNS 服务器地址 — 显示是否使用 DHCP 获取 DNS 服务器地址

- 首选 DNS 服务器 — 显示当前活动的主要 DNS 服务器
- 备用 DNS 服务器 — 显示备用 DNS 服务器地址

注： 此信息可从 **iDRAC6 →"Properties"（属性）→"Remote Access Information"（远程访问信息）**获得。

嵌入式 NIC MAC 地址

- NIC 1 — 显示嵌入式网络接口控制器 (NIC) 1 的介质访问控制 (MAC) 地址。

  在介质访问控制层， MAC 地址唯一识别网络中的每个节点。

  Internet 小型计算机系统接口 (iSCSI) NIC 是在主机计算机上运行的带有 iSCSI 堆栈的网络接口控制器。

  Ethernet NIC 支持有线以太网标准，并插入到服务器的系统总线中。
- NIC 2 — 显示嵌入式 NIC 2 的 MAC 地址，可在网络中唯一识别。
- NIC 3 — 显示嵌入式 NIC 3 的 MAC 地址，可在网络中唯一识别。并非所有系统上都显示嵌入式 NIC 3 MAC 地址。
- NIC 4 — 显示嵌入式 NIC 4 的 MAC 地址，可在网络中唯一识别。并非所有系统上都显示有嵌入式 NIC 4 MAC 地址。

WWN / MAC

单击**"System"（系统）→"Properties"（属性）→ WWN / MAC** 查看已安装 I/O 夹层卡及与之相关联的网络结构的当前配置。如果 CMC 中已启用 FlexAddress 功能，则全局分配的（机箱分配的）永久 MAC 地址将取代每个 LOM 的硬接线值。

服务器运行状况

单击**"System"（系统）→"Properties"（属性）选项卡 →"System Summary"（系统摘要）→"Server Health"（服务器运行状况）**部分可查看 iDRAC6 和 iDRAC6 所监控组件运行状况的重要信息。**"Status"（状态）**列显示每个组件的状态。有关状态图标及其含义的列表，请参阅表 19-3。单击**"Component"（组件）**列中的组件名称，了解有关该组件的更多详细信息。

注： 还可以通过单击该窗口左侧窗格中的组件名称获取组件信息。左侧窗格中出现的组件与选定哪个选项卡/屏幕无关。

iDRAC6

"Remote Access Information"（远程访问信息）屏幕列出大量有关 iDRAC6 的详细信息，例如名称、固件版本、固件更新、iDRAC6 时间、IPMI 版本、CPLD 版本、服务器类型和网络参数。还可以通过单击屏幕顶部相应的选项卡获得更多详细信息。

CMC

CMC 屏幕显示 Chassis Management Controller 的运行状况、固件版本和 IP 地址。也可以通过单击**"Launch the CMC Web Interface"（启动 CMC Web 界面）**按钮启动 CMC Web 界面。请参阅《*Chassis Management Controller Firmware 用户指南*》了解详情。

注： 从 iDRAC6 启动 CMC Web GUI 会用相同的 IP 地址格式定向搜索。例如，如果用 IPv6 地址格式打开 iDRAC6 Web GUI，CMC Web 页也会用有效 IPv6 地址打开。

电池

"Batteries"（电池）屏幕显示系统主板币形电池的状态，该电池用于维持 Managed System 的实时时钟 (RTC) 和 CMOS 配置数据存储。

温度

"Temperatures"（温度）屏幕显示板载环境温度探测器的状态和读数。显示*"warning"（警告）*或*"failure"（故障）*状态的最小和最大温度阈值，以及探测器的当前运行状况。

注： 根据服务器的型号不同，可能不会显示*"warning"（警告）*或*"failure"（故障）*状态的温度阈值和/或探测器的运行状况。

电压

"Voltage Probes"（电压探测器）屏幕显示电压探测器的状态和读数，提供诸如机载电压轨和 CPU 核心传感器状态等信息。

电源监控

"Power Monitoring"（电源监控）屏幕显示以下监控和电源统计信息：

- 电源监控 — 显示系统板电流监视器报告的服务器所用功率（以交流瓦特计的一分钟平均功率值）。
- 安培 — 显示活动电源设备的电流消耗量（以安培计的交流电）。
- 电源跟踪统计 — 显示从上次重设读数开始系统所用电量的信息。
- 峰值统计 — 显示从上次重设读数开始系统所用峰值电量的信息。
- 功耗 — 显示系统上一分钟、上一小时、昨天和上周的平均、最小和最大功耗，以及最大和最小功率时间。
- 显示图表 — 显示 1 小时、24 小时、3 天和 1 周功耗的图形化表示。

注： 功率和安培按交流测量。

CPU

CPU 屏幕报告受管服务器上每个 CPU 的运行状况。此运行状况是多个独立温度、电源和功能测试的累计信息。

POST

"Post Code"（开机自检代码）屏幕显示引导受管服务器操作系统前，上次系统开机自检代码（以十六进制表示）。

综合运行状况

"Misc Health"（综合运行状况）屏幕提供对以下系统日志的访问：

- 系统事件日志 — 显示 Managed System 发生的系统关键事件。
- 开机自检代码 — 显示引导受管服务器操作系统前，上次系统开机自检代码（以十六进制表示）。
- 上次崩溃 — 显示最近一次的崩溃屏幕和时间。
- 引导捕获 — 提供前三次引导屏幕的回放。

注： 该信息还可从**"System"（系统）→"Logs"（日志）**选项卡 →**"System Event Log"（系统事件日志）**获得。

目录

目录

电源监控和电源管理

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

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。

注： iDRAC6 电源管理逻辑使用刀片服务器中的复杂可编程逻辑设备 (CPLD)。一些平台还支持扩展的 CPLD。CPLD 设备的更新可从 Dell 支持网站 **support.dell.com** 的**"System Firmware"（系统固件）**或**"System Board"（系统板）**部分获得。建议用最新的 CPLD 固件版本更新刀片服务器。最新的 CPLD 和扩展的 CPLD 固件版本（用于适用平台）显示在 iDRAC6 Web GUI 中。

Dell PowerEdge 系统提供多项电源监控和管理功能：

- **电源监控：**iDRAC6 收集功耗测量历史并计算运行平均值、峰值等。您可使用 iDRAC6 Web 界面在**"Power Monitoring"（电源监控）**屏幕上查看信息。您也可通过单击**"Show Graph"（显示图形）**（**"Power Monitoring"（电源监控）**屏幕底部）查看以图形形式给出的信息。有关详情，请参阅"电源监控"。
- **电源预算：**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。有关详情，请参阅"电源预算"。
- **电源控制：**iDRAC6 允许您远程执行 Managed System 上的多个电源管理操作。有关详情，请参阅"电源控制"。

配置和管理电源

您可使用 iDRAC6 Web 界面和 RACADM 命令行界面 (CLI) 在 Dell 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态。请参阅"查看电源监控"。
- 查看服务器的电源预算信息，包括最小和最大潜在功耗。请参阅"查看电源预算"。
- 查看服务器的电源预算阈值。请参阅"电源预算阈值"。
- 查看分配给服务器的 PCIe 扩展卡的功率。请参阅"查看并修改 PCIe 功率分配"。
- 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、关机后再开机以及正常关机）。请参阅"执行服务器电源控制操作"。

电源监控

iDRAC6 会连续监控 Dell PowerEdge 服务器的功耗。iDRAC6 会计算以下功率值并通过其 Web 界面或 RACADM CLI 提供信息：

- 累计系统功率
- 系统峰值功率和系统峰值安培
- 平均、最小和最大功耗
- 功耗（也在 Web 界面中以图形形式显示）
- 最大和最小功率时间

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. 在系统树中，选择**"Power Monitoring"（电源监控）**。

   此时会出现**"Power Monitoring"（电源监控）**屏幕并显示以下信息：

电源监控

- **"Status"（状态）：绿色复选标记**表示电源状况正常，**"Warning"（警告）**表示发出了警告警报，而**"Severe"（严重）**表示发出了故障警报。
- **"Probe Name"（探测器名称）**：列出传感器的名称。
- **"Reading"（读数）**：探测器报告的瓦特。
- **"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。

Amperage（安培）

- **"Location"（位置）**：显示系统板传感器的名称。
- **"Reading"（读数）**：当前功耗，以安培表示。

功率跟踪统计和峰值统计

- **统计信息：**
  - **"Cumulative System Power"（累计系统功率）**显示服务器的当前累计能耗（千瓦时）。此值代表系统使用的总能量。您可单击表格行末尾的**"Reset"（重设）**重设此值为 0。
  - **"System Peak Power"（系统峰值功率）**指定系统峰值（瓦特）。
  - **"System Peak Amperage"（系统峰值安培）**指定系统峰值安培。峰值是从**"Measurement Start Time"（测量开始时间）**到现在记录的最高值。峰值时间是出现峰值的时间点。单击表行结尾的**"Reset"（重设）**设置恢复为当前即时值（如果服务器运行，这个值将不会为 0）。单击重设还会将测量开始时间重设为当前时间。
  - **"Measurement Start Time"（测量开始时间）**显示上次清除系统能耗值并开始新的测量周期时记录的日期和时间。对于**"Cumulative System Power"（累计系统功率）**、**"System Peak Amperage"（系统峰值安培）**和**"System Peak Power"（系统峰值功率）**统计，重设时的峰值将会立即反映为当前即时值。
  - **"Cumulative System Power"（累计系统功率）**使用的**"Measurement Current Time"（测量当前时间）**显示计算系统能耗时的当前日期和时间。对于**"System Peak Amperage"（系统峰值安培）**和**"System Peak Power"（系统峰值功率）**来说，**"Peak Time"（峰值时间）**字段显示这些峰值出现时的时间。
  - **"Reading"（读数）**：自计数器启动以来**"Cumulative System Power"（累计系统功率）**、**"System Peak Power"（系统峰值功率）**和**"System Peak Amperage"（系统峰值安培）**的相应统计值。

注： 功率跟踪统计数据在系统重置时保持不变，因此会反映开始和当前时间间隔内的所有活动。功耗表中显示的功率值是在相应时间间隔（前一分钟、小时、天和周）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）

- **"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 Power Consumption"（最大功耗）**和**"Min Power Consumption"（最小功耗）**：给定时间间隔内的实测最大和最小功耗。
- **"Max Power Time"（最大功率时间）**和**"Min Power Time"（最小功率时间）**：最大和最小功耗出现时的时间（按分钟、小时、天和周）。

"Show Graph"（显示图形）

单击**"Show Graph"（显示图形）**显示描绘过去一小时、24 小时、三天和一周内的 iDRAC6 功耗（瓦）的图形。使用图上方的下拉菜单可选择时间段。

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。

电源预算

"Power Budget"（电源预算）屏幕显示功率限制，其中包含重负荷下的系统向数据中心提交的交流功耗的范围。

服务器开机前，iDRAC6 向 CMC 提供功率电路要求。服务器开机后，根据服务器实际消耗的功率，可能会要求较小的功率电路。如果功耗越来越大并且服务器消耗的功率接近其最大分配，iDRAC6 会要求增加最大潜在功耗，因此增大功率电路。iDRAC6 只向 CMC 要求增加最大潜在功耗。如果功耗降低，将不会要求较小的潜在功率。

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

如果没有分配到足够的功率，刀片服务器不会开机。如果刀片分配到足够的功率，iDRAC 会打开系统电源。

iDRAC6 还支持为适用平台的 PCIe 扩展卡分配功率。可以更改分配给安装在服务器扩展槽中的 PCIe 扩展卡的功率。两个 PCIe 卡可以安装在适用平台上。iDRAC 动态调整包络功率以贴近刀片的实际系统要求，增加分配给扩展卡插槽的功率，向 CMC 请求组合功率。有关扩展卡的详细信息，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的 *硬件用户手册*。有关修改 PCIe 功率分配的信息，请参阅 "查看并修改 PCIe 功率分配"。

在刀片开机后，BIOS 将引导并检测安装的 PCIe 扩展卡的实际功耗。这在开机自检期间完成。如果两个卡都已安装，iDRAC 会保持扩展卡在预初始化阶段时使用的值。在获得当前已安装的 PCIe 卡的更新值时，iDRAC 会将该值与 扩展卡估测功耗相组合，并报告整个刀片的新功率值。如果 CMC 未分配足够的功率，iDRAC 将会切断刀片电源。如果 CMC 分配足够功率，BIOS 可以继续引导，服务器可以启动。

例如，如果分到的功率值为 500W，则 iDRAC 会假设在预初始化期间将使用此值，除非为 PCIe 扩展槽设置了不同的值。如果设置为不同的值，则将在预初始化期间一直使用该值。该值

在交流电源周期内一直保存。然后会在系统开机自检时，将输入值与安装的扩展卡数量进行比较。

查看电源预算

服务器在**"Power Budget"（电源预算）**屏幕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 Web 界面。
2. 在系统树中选择**"System"（系统）。**
3. 单击**"Power Management"（电源管理）**选项卡，然后单击**"Power Budget"（电源预算）**。

   将出现**"Power Budget"（电源预算）**屏幕。

"Power Budget Information"（电源预算信息）表显示了当前系统配置的最小和最大功率阈值。其中包含重负荷下阈值设定系统向数据中心提交的交流功耗的范围。

- **"Minimum Potential Power Consumption"（最小潜在功耗）**代表最低的电源预算阈值。
- **"Maximum Potential Power Consumption"（最大潜在功耗）**代表最高的电源预算阈值。此值也是当前系统配置的绝对最大功耗。

使用 RACADM

在受管服务器上，打开命令行界面并输入：

```
racadm getconfig -g cfgServerPower
```

注： 有关 cfgServerPower 的详细信息（含输出细节），请参阅 Dell 支持网站 s**upport.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》中的 cfgServerPower 。

电源预算阈值

电源预算阈值在启用时会执行系统的功率限制。系统性能会被动态调整以保持功耗接近指定阈值。

实际功耗可能在较轻负荷下较低并可能暂时超过阈值直到完成性能调整。

注： iDRAC6 中的电源预算阈值信息是只读模式且不能启用或配置。

使用 Web 界面

1. 登录到 iDRAC6 Web 界面。
2. 在系统树中选择**"System"（系统）。**
3. 单击**"Power Management"（电源管理）**选项卡，然后单击**"Power Budget"（电源预算）**。

   将出现**"Power Budget"（电源预算）**屏幕。**电源预算阈值** 表显示系统的下列功率限制信息：

   - **"Enabled"（已启用）**指示系统是否强制执行电源预算阈值。
   - **"Threshold in Watts"（瓦特阈值）**和**"Threshold in BTU / hr"（BTU / 小时 阈值）**分别以瓦特和 BTU/小时为单位显示限制值。
   - **"Threshold in Percentage(of Maximum)"（阈值百分比 [占最大值]）**显示功率限值范围百分比。

使用 RACADM

要从本地 RACADM 查看电源预算阈值数据， 在受管服务器上，打开命令行界面并输入 ：

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts
```

returns <*瓦特表示的功率限值*>

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr
```

returns <*BTU/小时表示的功率限值*>

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent
```

returns <*% 表示的功率限值*>

注： 有关 cfgServerPower 的详细信息（含输出细节），请参阅 Dell 支持网站 **support.dell.com/manuals** 提供的《*iDRAC6 管理员参考指南*》中的 cfgServerPower。

查看并修改 PCIe 功率分配

PCIe 功率分配允许查看并修改分配给 PCIe 扩展卡的最大功率。分配的功率应介于 100W 和 500W 之间。分配的功率太大可能导致刀片不开机，或可能阻止机箱中的其他刀片开机。如果 PCIe 扩展卡消耗的功率多于分配的功率，则刀片将会关机。修改 PCIe 功率分配值后，系统在启动时将使用新的功率分配值。

注： PCIe 功率分配信息并不适用于所有平台，不会为不适用的平台显示此信息。

注： 必须具有管理员权限（配置 iDRAC 和执行服务器控制命令）才可编辑 PCIe 功率分配值。

使用 Web 界面

1. 登录到 iDRAC6 Web 界面。
2. 在系统树中选择**"System"（系统）**。
3. 单击**"Power Management"（电源管理）**选项卡，然后单击**"Power Budget"（电源预算）**。**PCIe 功率分配**表的**"Power Threshold in Watts"（瓦特功率阈值）**字段显示最新的功率分配值。
4. 输入所需的值，或单击**"Default Value"（默认值）**指定默认值。有效值介于 100W 至 500W。默认值是 500W。
5. 单击**"Apply"（应用）**保存新值。系统启动时将使用新值。

使用 RACADM

要查看为使用远程 RACADM 的 PCIe 扩展卡分配的最新功率，在远程系统上，打开命令提示符 并输入以下命令：

```
racadm -r <idracip> -u <用户名> -p <密码> config -g cfgServerPower -o cfgServerPowerPCIeAllocation
```

Returns <*以交流瓦特或 BTU/小时表示的功率限值*>。默认值是 500W。

要更改功率分配值（例如改为 250W）：

```
racadm -r <idracip> -u <用户名> -p <密码> config -g cfgServerPower -o cfgServerPowerPCIeAllocation 250
```

将值设置为 250W

注： 仅在远程而非本地 RACADM 上支持 cfgServerPowerPCIeAllocation 对象。

注： 有关详细信息，请参阅 Dell 支持网站 **support.dell.com/manuals** 提供的《*iDRAC6 管理员参考指南*》中的 cfgServerPowerPCIeAllocation。

电源控制

iDRAC6 允许您远程执行开机、关机、重设、正常关机、非屏蔽中断 (NMI) 或关机后再开机操作。使用**"Power Control"（电源控制）**屏幕在重新引导、开机或关机时通过操作系统执行有序关机。

执行服务器电源控制操作

注： 要执行电源管理操作，您必须拥有**"Administrative"（管理）**权限。

iDRAC6 允许您远程执行开机、重设、正常关机、NMI 或打开电源再关闭电源操作。

使用 Web 界面

1. 登录到 iDRAC6 Web 界面。

2. 在系统树中选择**"System"（系统）**。

3. 单击**"Power Management"**（电源管理）选项卡。

   随即出现**"Power Control"（电源控制）**屏幕。

4. 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（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。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。NMI 向操作系统发送一个高级中断指令，使系统暂停运行以进行紧急诊断或故障排除工作。如果系统电源已经关闭，则该选项被禁用。
   - **"Graceful Shutdown"（正常关机）**尝试关闭操作系统，然后关闭系统电源。正常关机需要能识别 ACPI （高级配置和电源接口）的操作系统，以允许进行系统指导的电源管理。如果系统电源已经关闭，则该选项被禁用。
   - **"Reset System (warm boot)"（重设系统 [温引导]）**可重新引导系统而不断电。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。

5. 单击**"Apply"（应用）**。

   对话框会显示要求确认。

6. 单击**"OK"（确定）**执行您选择的电源管理操作。

使用 RACADM

要从本地 RACADM 执行电源操作，在命令提示符处输入以下命令：

```
racadm serveraction <操作>
```

其中 <操作> 为"powerup"、"powerdown"、"powercycle"、"hardreset"或"powerstatus"。

注： 有关 serveraction 的详细信息（含输出细节），请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《 *iDRAC6 管理员参考指南*》中的 serveraction。

目录

目录

配置和使用 LAN 上串行

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

LAN 上串行 (SOL) 是一项 IPMI 功能，允许受管服务器的基于文本的控制台数据（传统上发送到串行 I/O 端口）通过 iDRAC6 的专用带外以太网管理网络重定向。SOL 带外控制台使系统管理员能够从可访问网络的任何位置远程管理刀片服务器的基于文本的控制台。SOL 的优势如下：

- 远程访问操作系统而不会发生超时现象。
- 在 Windows 的紧急管理服务 (EMS) 或 Special Administrator Console (SAC) 上或在 Linux Shell 中诊断主机系统。
- 在开机自检过程中查看刀片服务器的进度并重新配置 BIOS 设置程序（同时重定向到串行端口）。

在 BIOS 中启用 LAN 上串行

要为 LAN 上串行配置服务器，要求执行以下配置步骤，在此将详细说明这些步骤。

1. 在 BIOS 中配置 LAN 上串行（默认情况下已禁用）
2. 为 LAN 上串行 (SOL) 配置 iDRAC6
3. 选择初始化 LAN 上串行的方法（SSH、Telnet、SOL Proxy 或 IPMI Tool）
4. 为 SOL 配置操作系统

默认情况下，BIOS 中的串行通信**关闭**。要将主机文本控制台数据重定向到 LAN 上串行，必须启用通过 COM1 的虚拟控制台。要更改 BIOS 设置，执行下列步骤：

1. 引导受管服务器。
2. 在开机自检过程中，按 <F2> 进入 BIOS 设置公用程序。
3. 向下滚动到"Serial Communication"（串行通信）并按 <Enter>。

   在弹出窗口中，显示串行通信列表和以下选项：

   - Off（断开）
   - On without Virtual Console（开，不启用虚拟控制台）
   - On with Virtual Console（开，启用虚拟控制台）

   使用箭头键在选项之间导航。
4. 确保启用了**"On with Virtual Console"（开，启用虚拟控制台）**。确保**"Serial Port Address"（串行端口地址）**为 COM1。
5. 确保**"Failsafe Baud Rate"（故障安全波特率）**与 iDRAC6 上配置的 SOL 波特率相同。故障安全波特率和 iDRAC6 的 SOL 波特率设置的默认值都是 115.2 kbps。
6. 确保启用了**"Redirection After Boot"（引导后重定向）**。此选项可启用随后重新引导中的 BIOS SOL 重定向。BIOS 的**"Remote Terminal Type"（远程终端类型）**值为 VT100/VT220 和 ANSI。
7. 保存更改并退出。

   受管服务器重新引导。

在 iDRAC6 Web GUI 中配置 LAN 上串行

1. 打开**"Serial Over LAN Configuration"（LAN 上串行配置）**屏幕，方法是选择**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Serial Over LAN"（LAN 上串行）**。
2. 保证选择了**"Enable Serial Over LAN"（启用 LAN 上串行）**选项（已启用）。默认情况下，该选项已启用。

3. 通过从**"Baud Rate"（波特率）**下拉菜单中选择数据速度来更新 IPMI SOL 波特率。选项是 9600 bps、19.2 kbps、57.6 kbps 和 115.2 kbps。默认值是 115.2 kbps。

4. 为 LAN 上串行选择权限级别限制。

   注： 确保 SOL 波特率与在 BIOS 中设置的故障安全波特率相同。

5. 如果已经做出更改，单击**"Apply"（应用）**。

表 9-1. LAN 上串行配置设置

设置	说明
"Enable Serial Over LAN"（启用 LAN 上串行）	该复选框选中后表示 LAN 上串行已启用。
"Baud Rate"（波特率）	表示数据速度。选择数据速度 **9600 bps**、**19.2 kbps**、**57.6 kbps** 或 **115.2 kbps**。
"Channel Privilege Level Limit"（信道权限级别限制）	为 LAN 上串行选择权限级别限制。

表 9-2. LAN 上串行配置按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的**"Serial Over LAN"（LAN 上串行）**配置值。
"Refresh"（刷新）	重新载入**"Serial Over LAN"（LAN 上串行）**屏幕。
"Advanced Settings"（高级设置）	打开**"Serial Over LAN Configuration Advanced Settings"（LAN 上串行配置高级设置）**屏幕。
"Apply"（应用）	应用在查看**"Serial Over LAN"（LAN 上串行）**屏幕时所做的任何新设置。

6. 如有必要，更改**"Serial Over LAN Configuration Advanced Settings"（LAN 上串行配置高级设置）**屏幕上的配置。建议使用默认值。**"Advanced Settings"（高级设置）**使用户可以通过更改**"Character Accumulate Interval"（字符积累间隔时间）**和**"Character Send Threshold"（字符发送阈值）**值调整 SOL 性能。为了达到最佳性能，分别使用默认设置 10 毫秒和 255 个字符。

表 9-3. LAN 上串行配置高级设置

设置	说明
"Character Accumulate Interval"（字符积累间隔时间）	iDRAC6 发送部分 SOL 数据包之前等待的典型时间长度。此参数用毫秒指定。
"Character Send Threshold"（字符发送阈值）	指定每个 SOL 数据包的字符数。iDRAC6 接受的字符数一旦等于或大于"Character Send Threshold"（字符发送阈值）值，iDRAC6 就开始发送包含的字符数等于或小于"Character Send Threshold"（字符发送阈值）值的 SOL 数据包。如果数据包包含的字符数小于此值，该数据包就称为部分 SOL 数据包。

注： 如果减小这些值，SOL 的虚拟控制台功能的性能可能会降低。此外，对于每个数据包，SOL 会话必须等待接收确认，才能发送下一个数据包。因此，性能将显著降低。

表 9-4. LAN 上串行配置高级设置按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的**"Serial Over LAN Configuration Advanced Settings"（LAN 上串行配置高级设置）**值。
"Refresh"（刷新）	重新载入**"Serial Over LAN Configuration Advanced Settings"（LAN 上串行配置高级设置）**屏幕。
"Apply"（应用）	保存在查看**"Serial Over LAN Configuration Advanced Settings"（LAN 上串行配置高级设置）**屏幕时所做的任何新设置。
"Go Back To Serial Over LAN Configuration Page"（退回到 LAN 上串行配置页）	使用户返回到**"Serial Over LAN"（LAN 上串行）**屏幕。

7. 在**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）**选项卡 **→"Services"（服务）**，为 SOL 配置 SSH 和 Telnet。

   注： 每个刀片服务器只支持一个活动 SOL 会话。

   注： SSH 协议默认为启用。Telnet 协议默认为禁用。

8. 单击**"Services"（服务）**打开**"Services"（服务）**屏幕。

注： SSH 和 Telnet 程序都提供对远程机器的访问。

9. 根据需要，单击 **SSH** 或 **Telnet** 的**"Enabled"（启用）**。

10. 单击**"Apply"（应用）**。

注： 由于 SSH 具有更好的安全性和加密机制，因此建议使用 SSH 方法。

注： 只要超时值设置为 0，SSH/Telnet 会话持续时间就可以无限长。默认超时值为 1800 秒。

11. 通过选择**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Network"（网络）**，启用 iDRAC6 带外接口（LAN 上 IPMI）。

12. 在**"IPMI Settings"（IPMI 设置）**下选择**"Enable IPMI Over LAN"（启用 LAN 上 IPMI）**选项。

13. 单击**"Apply"（应用）**。

使用 LAN 上串行 (SOL)

本节提供了几种初始化 LAN 上串行会话的方法，包括 Telnet 程序、SSH 客户端、IPMItool 和 SOL Proxy。LAN 上串行功能的用途是通过 iDRAC6 将受管服务器的串行端口重定向到 Management Station 的控制台。

通过 Telnet 或 SSH 重定向 SOL 的模型

Telnet（端口 23）/SSH（端口 22）客户端↔WAN 连接↔iDRAC6 服务器

通过 SSH/Telnet 实施基于 IPMI 的 SOL 无需使用额外的公用程序，因为串行到网络转换是在 iDRAC6 中进行的。使用的 SSH 或 Telnet 控制台应该能解释并响应来自受管服务器串行端口的数据。串行端口通常连接到仿真 ANSI 或 VT100/VT220 终端的 Shell 上。串行控制台自动重定向到 SSH 或 Telnet 控制台。

要启动 SOL 会话，通过 SSH/Telnet 连接到 iDRAC6，这会转至 iDRAC6 命令行控制台。然后在美元提示符处输入 connect。

请参阅"安装 Telnet 或 SSH 客户端"了解有关使用带有 iDRAC6 的 Telnet 和 SSH 客户端的详情。

SOL Proxy 模型

Telnet 客户端（端口 623）↔WAN 连接↔SOL 代理↔iDRAC6 服务器

当 SOL Proxy 与 Management Station 上的 Telnet 客户端通信时，它使用 TCP/IP 协议。但是，SOL Proxy 通过 RMCP/IPMI/SOL 协议与受管服务器的 iDRAC6 通信，该协议是基于 UDP 的协议。因此，如果通过 WAN 连接从 SOL Proxy 与 Managed System 的 iDRAC6 通信，可能会遇到网络性能问题。建议的使用模式是让 SOL Proxy 和 iDRAC6 服务器在同一个 LAN 中。具有 Telnet 客户端的 Management Station 随后可以通过 WAN 连接连接到 SOL Proxy。在此使用模型中，SOL Proxy 将按要求运行。

通过 IPMItool 重定向 SOL 的模型

IPMItool↔WAN 连接↔iDRAC6 服务器

基于 IPMI 的 SOL 公用程序 IPMItool 使用 RMCP+ 协议，该协议通过 UDP 数据报发送到端口 623。iDRAC6 要求将此 RMCP+ 连接加密。密钥（KG 密钥）必须包含零或 NULL 字符，可以在 iDRAC6 Web GUI 或 iDRAC6 配置公用程序中进行配置。还可以通过按 Backspace 键删除密钥，这样 iDRAC6 将默认提供 NULL 字符作为密钥。使用 RMCP+ 的优势是改善了验证、数据完整性检查、加密和能够承载多种类型的有效载荷。有关详情，请参阅"通过 IPMItool 使用 SOL"或 IPMItool 网站：**http://ipmitool.sourceforge.net/manpage.html**。

在 iDRAC6 命令行控制台中断开 SOL 会话连接

用于断开 SOL 会话的命令是面向公用程序的。只有 SOL 会话完全终止后才可以退出公用程序。要断开 SOL 会话连接，从 iDRAC6 命令行控制台终止 SOL 会话。

准备退出 SOL 重定向时，按 <Enter>、<Esc>，然后按 <t>（按顺序逐个按这些键）。SOL 会话将相应关闭。连接 SOL 会话后，转义序列也会显示在屏幕上。受管服务器关闭后，需要较长时间建立 SOL 会话。

注： 如果在公用程序中没有成功关闭 SOL 会话，可能会有更多 SOL 会话不可用。解决这种问题的途径就是在 Web GUI 的**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Sessions"（会话）**下终止命令行控制台。

通过 PuTTY 使用 SOL

要从 Windows Management Station 上的 PuTTY 启动 SOL，请执行以下步骤：

注： 如果需要，可以在**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**更改默认 SSH/Telnet 超时时间。

1. 在命令提示符处使用以下命令连接到 iDRAC6：

   ```
   putty.exe [-ssh | -telnet] <登录名称>@<iDRAC IP 地址> <端口号>
   ```

   注： 端口号可选。仅在重新分配端口号时是必需的。

2. 在命令提示符处输入以下命令启动 SOL：

   ```
   connect
   ```

   注： 这会连接到受管服务器的串行端口。成功建立 SOL 会话后，iDRAC6 命令行控制台将不再可用。正确按照转义序列到达 iDRAC6 命令行控制台。使用"在 iDRAC6 命令行控制台中断开 SOL 会话连接"中详细说明的命令序列退出 SOL 会话并启动新会话。

   注： 在 Windows 中，如果在主机重新引导后立即打开"Emergency Management System (EMS)"（紧急管理系统） 控制台，Special Admin Console (SAC) 终端可能会损坏。按"在 iDRAC6 命令行控制台中断开 SOL 会话连接"中所述退出 SOL 会话，关闭终端，打开其他终端，并使用上述相同命令启动 SOL 会话。

将 SOL Over Telnet 用于 Linux

注： 如果需要，可在**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**更改默认 Telnet 超时时间。

要从 Linux Management Station 上的 Telnet 启动 SOL，请执行这些步骤：

1. 启动 shell。

2. 使用以下命令连接到 iDRAC6：

   ```
   telnet <iDRAC6-ip-地址>
   ```

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

3. 在命令提示符处输入以下命令启动 SOL：

   ```
   connect
   ```

4. 要从 Linux 上的 Telnet 退出 SOL 会话，请按 <Ctrl>+]（按住 <Ctrl> 键并按右方括号键，然后释放）。Telnet 提示符将会显示。输入 quit 以退出 Telnet。

在 Linux 中通过 OpenSSH 使用 SOL

OpenSSH 是一个使用 SSH 协议的开放源代码公用程序。要从 Linux Management Station 上的 OpenSSH 启动 SOL，请执行以下步骤：

注： 如果需要，可以在**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**更改默认 SSH 会话超时时间。

1. 启动 shell。

2. 使用以下命令连接到 iDRAC6：

   ```
   ssh <iDRAC IP 地址> -l <登录名称>
   ```

3. 在命令提示符处输入以下命令启动 SOL：

   ```
   connect
   ```

   注： 这会连接到受管服务器的串行端口。成功建立 SOL 会话后，iDRAC6 命令行控制台将不再可用。正确按照转义序列到达 iDRAC6 命令行控制台。退出 SOL 会话（请参阅 "在 iDRAC6 命令行控制台中断开 SOL 会话连接" 了解如何关闭活动的 SOL 会话）。

通过 IPMItool 使用 SOL

Dell Systems Management Tools and Documentation DVD 提供了可在各个操作系统上安装的 IPMItool。请参阅《*软件快速安装指南*》了解安装详情。要在 Management Station

上使用 IPMItool 启动 SOL，请执行以下步骤：

注： 如果需要，可以在**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**更改默认 SOL 超时时间。

1. 在正确的目录下找到 **IPMItool.exe**。

   Windows 32 位操作系统中的默认路径是 **C:\Program Files\Dell\SysMgt\bmc**，而在 Windows 64 位操作系统中的默认路径是 **C:\Program Files (x86)\Dell\SysMgt\bmc**。

2. 在**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Network"（网络）→ "IPMI Settings"（IPMI 设置）**确保**密钥**全部为零。

3. 在 Windows 命令提示符或 Linux Shell 提示符中输入以下命令，从 iDRAC 启动 SOL：

   ```
   ipmitool -H <iDRAC IP 地址> -I lanplus -U <登录名称> -P <登录密码> sol activate
   ```

   这会连接到受管服务器的串行端口。

4. 要从 IPMItool 退出 SOL 会话，请按 <~> 和 <.>（按顺序逐个按波浪号和句点键）。请多试几次，因为 iDRAC6 可能会由于太忙而无法接受这些键。SOL 会话将关闭。

   注： 如果用户没有正确终止 SOL 会话，则输入以下命令以重新引导 iDRAC。允许 iDRAC6 长达 2 分钟完成引导。有关详情，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的*《iDRAC6 管理员参考指南》*。

   ```
   racadm racreset
   ```

用 SOL Proxy 打开 SOL

LAN 上串行代理 (SOL Proxy) 是一个远程登录守护程序，允许使用 LAN 上串行 (SOL) 和 IPMI 协议对远程系统进行基于 LAN 的管理。任何标准 Telnet 客户端应用程序，如 Microsoft Windows 上的 HyperTerminal 或 Linux 上的 Telnet 都可以用来访问此守护程序的功能。SOL 既可以在菜单模式，也可以在命令模式中使用。配合远程系统 BIOS 虚拟控制台的 SOL 协议允许管理员通过 LAN 远程查看和更改 Managed System 的 BIOS 设置。使用 SOL 也可以通过 LAN 访问 Linux 串行控制台和 Microsoft 的 EMS/SAC 界面。

注： 所有版本的 Windows 操作系统都包括有 HyperTerminal 终端仿真软件。但是，包括的版本没有提供虚拟控制台期间需要的许多功能。这时，可以使用支持 VT100/VT220 或 ANSI 仿真模式的任何终端仿真软件。Hilgraeve 的 HyperTerminal Private Edition 6.1 或更高版本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。另外，使用命令行窗口执行 Telnet 串行虚拟控制台可能会显示乱码。

注： 请参阅系统的用户指南以了解有关虚拟控制台的详情，其中包括硬件和软件要求以及如何配置主机和客户端系统以使用虚拟控制台。

注： HyperTerminal 和 Telnet 设置必须与 Managed System 上的设置一致。例如，波特率和终端模式应相符。

注： 从 MS-DOS 提示符运行的 Windows telnet 命令支持 ANSI 终端仿真，并且需要为 ANSI 仿真设置 BIOS 以正确显示所有屏幕。

使用 SOL Proxy 之前

使用 SOL Proxy 之前，请参阅*《底板管理控制器公用程序用户指南》*，了解如何配置 Management Station。默认情况下，BMC 管理公用程序安装在 Windows 操作系统上的以下目录中：

C:\Program Files\Dell\SysMgt\bmc —（32 位操作系统）

C:\Program Files (x86)\Dell\SysMgt\bmc —（64 位操作系统）

安装程序将文件复制到 Linux Enterprise 操作系统上的以下位置：

/etc/init.d/SOLPROXY.cfg

/etc/solproxy.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/ipmish

启动 SOL Proxy 会话

对于 Windows 2003

要在安装后在 Windows 系统上启动 SOL Proxy 服务，可以重新引导系统（SOL Proxy 会在重新引导后自动启动）。或者，可以通过完成以下步骤手动启动 SOL Proxy 服务：

1. 右键单击**"My Computer"（我的电脑）**并单击**"Manage"（管理）**。

将显示**"Computer Management"（计算机管理）**窗口。

2. 单击**"Services and Applications"（服务和应用程序）**，然后单击**"Services"（服务）**。

   可用服务会显示在右边。

3. 在服务列表中找到 **DSM_BMU_SOLProxy** 并右键单击以启动服务。

根据所使用的控制台，访问 SOL Proxy 有不同的步骤。在本节中，正在运行 SOL Proxy 的 Management Station 称为 SOL Proxy 服务器。

对于 Linux

在系统启动时，SOL Proxy 会自动启动。另外，您也可以转到目录 **/etc/init.d**，并且使用以下命令管理 SOL Proxy 服务：

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

结合使用 Telnet 和 SOL Proxy

假定 SOL Proxy 服务已经在 Management Station 上正常运行。

对于 Windows 2003：

1. 在 Management Station 上打开一个命令提示符窗口。
2. 在命令行中输入 `telnet` 命令，如果 SOL Proxy 服务器在同一机器上运行，提供 `localhost` 作为 IP 地址并提供在安装 SOL Proxy 时指定的端口号（默认值为 623）。例如：

   ```
   telnet localhost 623
   ```

对于 Linux：

1. 在 Management Station 上打开 Linux Shell。
2. 输入 `telnet` 命令，并提供 `localhost` 作为 SOL Proxy 服务器的 IP 地址，以及在安装 SOL Proxy 时指定的端口号（默认值为 623）。例如：

   ```
   telnet localhost 623
   ```

   注： 无论主机操作系统是 Windows 还是 Linux，如果 SOL Proxy 服务器是在除 Management Station 之外的机器上运行，则输入 SOL Proxy 服务器的 IP 地址，而不输入 localhost。

   ```
   telnet <SOL Proxy 服务器 IP 地址> 623
   ```

结合使用 HyperTerminal 和 SOL Proxy

1. 从远程站打开 **HyperTerminal.exe**。
2. 选择 **TCPIP(Winsock)**。
3. 输入主机地址 `localhost` 和端口号 623。

连接到远程 Managed System 的 BMC

成功建立 SOL Proxy 会话后，将显示以下各个选项：

```
1. Connect to the Remote Server's BMC（连接到远程服务器的 BMC）
```

2. Configure the Serial-Over-LAN for the Remote Server（为远程服务器配置 LAN 上串行）

3. Activate Virtual Console（激活虚拟控制台）

4. Reboot and Activate Virtual Console（重新引导并激活虚拟控制台）

5. Help（帮助）

6. Exit（退出）

注： 尽管同时可以有多个 SOL 会话处于活动状态，但在任何给定的时间，用于 Managed System 的虚拟控制台会话只有一个可以处于活动状态。

注： 要退出活动的 SOL 会话，请使用 <~><.> 字符序列。这个序列会终止 SOL，并返回到顶层菜单。

1. 在主菜单中选择选项 1。

2. 输入远程 Managed System 的 iDRAC6 **IP 地址**。

3. 提供 Managed System 上 iDRAC6 的 iDRAC6 **用户名**和**密码**。必须分配 iDRAC6 用户名和密码并存储在 iDRAC6 非易失性存储器中。

注： 一次仅允许一个使用 iDRAC6 的 SOL 虚拟控制台会话。

注： 如果需要，在 iDRAC6 Web GUI 中的**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Services"（服务）**下面将 Telnet **超时值**更改为零，从而将 SOL 会话持续时间延长到无限长。

4. 提供 IPMI 密钥（如果已在 iDRAC6 中配置）。

注： 可以在 iDRAC6 GUI 的**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全性）→"Network"（网络）→"IPMI Settings"（IPMI 设置）→"Encryption Key"（密钥）**中找到 IPMI 密钥。

注： 默认 IPMI 密钥是全零。如果对加密选项按 <Enter>，iDRAC6 将使用此默认密钥。

5. 在主菜单中选择**"Configure the Serial-Over-LAN for the Remote Server"（为远程服务器配置 LAN 上串行）**（选项 2）。

SOL 配置菜单会出现。根据当前的 SOL 状态，SOL 配置菜单的内容会不同：

- 如果已经启用 SOL，则当前设置会显示出来，并为您提供三个选项：

  1. Disable Serial-Over-LAN（禁用 LAN 上串行）

  2. Change Serial-Over-LAN settings（更改 LAN 上串行设置）

  3. Cancel（取消）

- 如果已经启用 SOL，确保 SOL 波特率与 iDRAC6 的保持一致，且用户拥有管理员权限。
- 如果目前已禁用 SOL，则输入 Y 可以启用 SOL，输入 N 可以使 SOL 保持在禁用状态。

6. 在主菜单中选择**"Activate Virtual Console"（激活虚拟控制台）**（选项 3）。

远程 Managed System 的文本控制台会重定向到 Management Station。

7. 在主菜单中选择**"Reboot and Activate Virtual Console"（重新引导并激活虚拟控制台）**（选项 4）（可选）。

远程 Managed System 的电源状态会被确认。如果电源为开，则会要求用户决定是正常关机，还是强制关机。

之后，会一直监视电源状态，直到状态变为**"On"（开）**。虚拟控制台会开始，远程 Managed System 文本控制台被重定向到 Management Station。

在 Managed System 重新引导时，您可以进入 BIOS 系统设置程序来查看或配置 BIOS 设置。

8. 在主菜单中选择**"Help"（帮助）**（选项 5）可以显示每个选项的详细说明。

9. 在主菜单中选择**"Exit"（退出）**（选项 6）可以终止 Telnet 会话并从 SOL Proxy 断开。

注： 如果用户没有正确终止 SOL 会话，则发出以下命令以重新引导 iDRAC。请允许 iDRAC6 花 1-2 分钟完成引导。有关详情，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的*《iDRAC6 管理员参考指南》*。

```
racadm racreset
```

操作系统配置

完成以下步骤以配置类似 UNIX 的一般操作系统。此配置基于 Red Hat Enterprise Linux 5.0、SUSE Linux Enterprise Server 10 SP1 和 Windows 2003 Enterprise 的默认安装。

Linux Enterprise 操作系统

1. 编辑 **/etc/inittab** 文件以启用硬件流控制并允许用户通过 SOL 控制台登录。将以下一行添加到 #Run gettys in standard runlevels 部分的结尾。

   7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220

原始 /etc/inittab **示例：**

```
_____________________________________________________________________

#

# inittab      This file describes how the INIT process should set up
               the system in a certain run-level. (该文件描述了 init 进
               程如何在一定的运行水平上建立系统。)

#

SKIP this part of file (跳过文件的这个部分)

# Run gettys in standard runlevels (在标准运行级别运行 gettys)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1

# Run xdm in runlevel 5 (在运行级别 5 运行 xdm)

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

修改后的 **/etc/inittab** 示例：

```
_____________________________________________________________________

#

# inittab      This file describes how the INIT process should set up
               the system in a certain run-level. (该文件描述了 init 进
               程如何在一定的运行水平上建立系统。)

#

SKIP this part of file (跳过文件的这个部分)

# Run gettys in standard runlevels (在标准运行级别运行 gettys)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1

7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Run xdm in runlevel 5 (在运行级别 5 运行 xdm)

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

2. 编辑 **/etc/securetty** 文件以允许用户通过 SOL 控制台以 root 用户的身份登录。将以下一行添加在 console 后面：

   ttyS0

原始 **/etc/securetty** 示例：

```
console
vc/1
vc/2
vc/3
vc/4
SKIP the rest of file (跳过文件的这个部分)
```

修改后的 **/etc/securetty** 示例：

```
控制台
ttyS0
vc/1
vc/2
vc/3
vc/4
SKIP the rest of file (跳过文件的这个部分)
```

---

3. 编辑 **/boot/grub/grub.conf** 或 **/boot/grub/menu.list** 文件，以便为 SOL 添加引导选项：

   e. 注释掉类似 Unix 的各个操作系统中的图形显示行：

      - RHEL 5 中的 splashimage=(had0,0)/grub/splash.xpm.gz
      - SLES 10 中的 gfxmenu (hda0,5)/boot/message

   f. 在第一 title= ... 行前面添加以下一行：

      # Redirect OS boot via SOL

   g. 将以下项附加到第一 title= ... 行：

      SOL redirection

   h. 将以下文本附加到第一个 title= ... 的 kernel/... 行：

      console=tty1 console=ttyS0,115200

注： Red Hat Enterprise Linux 5 中的 **/boot/grub/grub.conf** 是指向 **/boot/grub/menu.list** 的符号链接。可以更改两者中任一项中的设置。

RHEL 5 中的原始 **/boot/grub/grub.conf** 示例：

```
# grub.conf generated by anaconda (grub.conf 由 anaconda 生成)
#
# Note that you do not have to return grub after making changes
  to this file (请注意更改文件后，您必要没有返回 grub)
# NOTICE: You have a /boot partition.This means that all kernel
  and initrd paths are relative to /boot/, eg. root (hd0,0)
  (注意：您有一个/ boot 分区。这意味着所有的内核和 initrd 路径是相对到
  /boot/，例如 root (hd0,0))
# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00
  (内核 /vmlinux-版本 ro root=/dev/VolGroup00/LogVol00
```

initrd /initrd-version.img#boot=/dev/sda)

```
# initrd /initrd-version.img

#boot=/dev/sda

default=0

timeout=5

splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu

title Red Hat Enterprise Linux 5

root (hd0,0)

kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet

initrd /initrd-2.6.18-8.el5.img
```

修改后的 /boot/grub/grub.conf 示例：

```
# grub.conf generated by anaconda (grub.conf 由 anaconda 生成)

#

# Note that you do not have to return grub after making changes
  to this file (请注意更改文件后，您必要没有返回 grub)

# NOTICE: You have a /boot partition.This means that all kernel
  and initrd paths are relative to /boot/, eg. root (hd0,0)
  (注意：您有一个/ boot 分区。这意味着所有的内核和 initrd 路径是相对到
  /boot/，例如 root (hd0,0))

# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

# initrd /initrd-version.img

#boot=/dev/sda

default=0

timeout=5

#splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu

# Redirect the OS boot via SOL (通过 SOL 重定向操作系统引导)

title Red Hat Enterprise Linux 5 SOL redirection

root (hd0,0)

kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet console=tty1 console=ttyS0,115200

initrd /initrd-2.6.18-8.el5.img
```

SLES 10 中的原始 **/boot/grub/menu.list** 示例：

```
#Modified by YaST2.Last modification on Sat Oct 11 21:52:09 UTC 2008
(YaST2 已修改。上次修改时间 2008 星期六十月 11 日 21:52:09 UTC)

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux
(请不要改变此命令 - YaST2 标识符: 初始名称: linux)###

title SUSE Linux Enterprise Server 10 SP1
```

```
root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

SLES 10 中修改后的 **/boot/grub/menu.list** 示例：

```
#Modified by YaST2.Last modification on Sat Oct 11 21:52:09 UTC 2008
(YaST2 已修改。上次修改时间星期六十月 11 日 21:52:09)

Default 0

Timeout 8

#gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux
(请不要改变此命令 - YaST2 标识符: 初始名称: linux)###

title SUSE Linux Enterprise Server 10 SP1 SOL redirection

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts console=tty1
console=ttyS0,115200

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Windows 2003 Enterprise

1. 在 Windows 命令提示符中输入 bootcfg，找出引导项 ID。找到操作系统友好名称 **Windows Server 2003 Enterprise** 部分的引导项 ID。按 <Enter> 以在 Management Station 上显示引导选项。

2. 通过输入以下内容，在 Windows 命令提示符中启用 EMS：

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <引导 ID>
   ```

   注： <引导 ID> 是步骤 1 中的引导项 ID。

3. 按 <Enter> 以验证 EMS 控制台设置是否生效。

原始 bootcfg 设置示例：

```
Boot Loader Settings

--------------------

timeout:30

default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Boot Entries

------------

Boot entry ID: 1

Os Friendly Name: Winodws Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

修改后的 bootcfg 设置示例：

```
      Boot Loader Settings
      --------------------
      timeout: 30
      default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
      redirect: COM1
      redirectbaudrate:115200
      Boot Entries
      ------------
      Boot entry ID: 1
      Os Friendly Name: Windows Server 2003, Enterprise
      Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
      OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

目录

目录

使用 GUI 虚拟控制台

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

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，从而可以从一个位置控制一个或多个启用了 iDRAC6 的系统。

使用虚拟控制台

"Virtual Console"（虚拟控制台）屏幕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：

- 每个刀片支持最多两个并发虚拟控制台会话。两个会话同时查看同一个受管服务器控制台。
- 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。

如果另一用户请求虚拟控制台会话，第一位用户将收到通知并可选择拒绝访问、仅允许视频或完全共享访问。第二位用户也将被告知另一用户享有控制权。第一位用户必须在 30 秒内响应，否则将不会给第二位用户授予访问权。两个会话同时处于活动状态时，第一位用户在屏幕右上角看到消息，表明另一用户正在进行会话。

如果第一位或第二位用户都不具有管理员权限，第一位用户的活动会话的终止将自动导致第二位用户的会话终止。

清除浏览器的高速缓存

如果在运行虚拟控制台时遇到问题（超出范围错误、同步问题等），则清除浏览器的高速缓存，以移除/删除系统中存储的查看器的所有旧版本，然后重试。

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 已使用的插件）**。
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"（所有插件）**。
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. 在命令提示符下，运行 `javaws -viewer`
2. 显示**"Java Cache Viewer"（Java 高速缓存查看器）**。
3. 删除标题为*"iDRAC6 Virtual Console Client"（iDRAC6 虚拟控制台客户端）*和 *JViewer* 的项。

也可以在命令提示符下运行 `javaws -uninstall` 以删除高速缓存中的所有应用程序。

支持的屏幕分辨率和刷新率

表 10-1 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 10-1. 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

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。请参阅"支持的 Web 浏览器" 和"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)。请参阅"安装 Java Runtime Environment (JRE)"。
3. 建议将显示器的显示分辨率配置为 1280x1024 像素。

   注： 如果有活动虚拟控制台会话，并且虚拟控制台连接了较低分辨率的显示器，在通过本地控制台选择服务器的情况下，可重设服务器控制台分辨率。如果服务器运行 Linux 操作系统，本地显示器上可能无法查看 X11 控制台。在虚拟控制台上按 <Ctrl><Alt><F1> 会将 Linux 切换到文本控制台。

4. 如使用 Internet Explorer 启动带有 Java 插件的虚拟控制台会话，请执行以下操作：
   a. 在 Internet Explorer 中，转至**"Tools"（工具）→"Internet Options"（Internet 选项）→"Security"（安全）→"Trusted sites"（受信任的站点）→"Custom level"（自定义级别）**。

   注： 对于 64 位的 Windows 7，单击**"Tools"（工具）→"Internet Options"（Internet 选项）→"Security"（安全）→"Internet"→"Custom level"（自定义级别）**。

   b. 在**"Security Settings"（安全设置）**窗口中，选择**"Automatic prompting for file downloads"（文件下载自动提示）**的**"Disable"（禁用）**选项。
   c. 单击**"OK"（确定）**，然后再次单击**"OK"（确定）**。

在 iDRAC6 Web 界面上配置虚拟控制台和虚拟介质

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）**，然后单击**"Virtual Console / Media"（虚拟控制台 / 介质）**选项卡。
2. 单击**"Configuration"（配置）**打开**"Configuration"（配置）**屏幕。
3. 配置虚拟控制台属性。表 10-2 说明虚拟控制台的设置。
4. 完成后，单击**"Apply"（应用）**。
5. 单击相应按钮继续。请参阅表 10-3。

表 10-2. 虚拟控制台配置属性

属性	说明
已启用	选择启用或禁用虚拟控制台。 **选中**表示"Virtual Console"（虚拟控制台）已启用。 **取消选中**表示"Virtual Console"（虚拟控制台）已禁用。 默认值为**已启用**。
"Max Sessions"（最大会话数）	显示可能的虚拟控制台会话的最大数目，为 **1** 或 **2**。使用下拉式菜单可以更改允许的虚拟控制台会话的最大数目。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。
"Keyboard and Mouse Port Number"（键盘和鼠标端口号）	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**。
"Video Port Number"（视频端口号）	用于连接到"Virtual Console Screen Service"（虚拟控制台屏幕服务）的网络端口号。如果其它程序正在使用默认端口，可能需要更改此设置。默认为 **5901**。
"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。**
"Mouse Mode"（鼠标模式）	如果 managed server 运行在 Windows 操作系统上，选择 **Windows**。 如果受管服务器运行在 Linux 上，则选择 **Linux**。 如果服务器不是运行在 Windows 或 Linux 操作系统上，选择 **USC/Diags**。 **注：** 在 HyperV、Dell Diagnostics 或 USC（系统服务）中必须选择 **USC/Diags**。 默认为 **Windows**。
"Console Plug-In Type for IE"（IE 的控制台插件类型）	当在 Windows 操作系统上使用 Internet Explorer 时，用户可在以下查看器中进行选择： **ActiveX** - *ActiveX 虚拟控制台*查看器 **Java** - *Java 虚拟控制台*查看器 **注：** 根据 Internet Explorer 版本不同，可能需要关闭其它安全保护限制（请参阅"配置并使用虚拟介质"）。 **注：** 客户端系统上必须装有 Java 运行时环境才能使用 Java 查看器。
"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启用输出至虚拟控制台显示器。**取消选中**表示您使用**"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。

注： 有关借助虚拟控制台使用虚拟介质的信息，请参阅"配置并使用虚拟介质"。

表 10-5 中的按钮在**"Virtual Console Configuration"（虚拟控制台配置）**屏幕上可用。

表 10-3. 虚拟控制台配置按钮

按钮	定义
"Print"（打印）	打印**"Configuration"（配置）**屏幕
"Refresh"（刷新）	重新载入**"Configuration"（配置）**屏幕
"Apply"（应用）	保存对虚拟控制台所做的任何新设置

打开虚拟控制台会话

打开虚拟控制台会话时，启动 Dell Virtual Console Viewer (**iDRACView**) 应用程序 ，并且在查看器中会出现远程系统的桌面。使用 **iDRACView**，可以从本地 Management Station 控制远程系统的鼠标和键盘功能。

注： 从 Windows Vista Management Station 中启动虚拟控制台可能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）→"HighCPerformance"（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）→ "Virtual Console / Media"（虚拟控制台 / 介质）**选择卡**→ "Virtual Console and Virtual Media"（虚拟控制台和虚拟介质）**。
2. 在**"Virtual Console and Virtual Media"（虚拟控制台和虚拟介质）**屏幕中，使用表 10-4 中的信息确保有一个虚拟控制台会话可用。

   如果希望重新配置显示的任何属性值，请参阅 "在 iDRAC6 Web 界面上配置虚拟控制台和虚拟介质"。

表 10-4. 虚拟控制台信息

属性	说明
启用虚拟控制台	**"Yes"（是）/"No"（否）**
"Video Encryption Enabled"（视频加密已启用）	**"Yes"（是）/"No"（否）**
"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。
"Mouse Mode"（鼠标模式）	显示当前生效的鼠标加速度。应根据受管服务器上安装的操作系统的类型选择**"Mouse Mode"（鼠标模式）**。
"Console Plug-in Type"（控制台插件类型）	显示当前配置的插件类型。 **ActiveX** — 将启动 Active-X 查看器。在 Windows 操作系统上运行时，Active-X 查看器只能在 Internet Explorer 上工作。 **Java** — 将启动 Java 查看器。Java 查看器可在 Internet Explorer 等任何浏览器上使用。如果客户端运行的操作系统不是 Windows，必须使用 Java 查看器。如果在 Windows 操作系统上运行时使用 Internet Explorer 访问 iDRAC6，则既可选择 **Active-X**,，也可选择 **Java** 插件类型。 **注：** 如果选择 **Java** 作为插件类型，对于 Internet Explorer 8，虚拟控制台第一次可能不会启动。
"Local Server Video Enabled"（本地服务器视频已启用）	**"Yes"（是）**表示在虚拟控制台期间启用输出至虚拟控制台显示器。**"No"（否）**表示您使用**"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。

注： 有关借助虚拟控制台使用虚拟介质的信息，请参阅 "配置并使用虚拟介质"。

表 10-5 中的按钮在**"Virtual Console"（虚拟控制台）**屏幕上可用。

表 10-5. 虚拟控制台按钮

按钮	定义
"Refresh"（刷新）	重新载入**"Virtual Console Configuration"（虚拟控制台配置）**屏幕
启动虚拟控制台	在目标远程系统上打开一个虚拟控制台会话
"Print"（打印）	打印**"Virtual Console Configuration"（虚拟控制台配置）**屏幕

3. 如一个虚拟控制台会话可用，单击**"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，必须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 并且远程系统桌面显示在 **iDRACView** 中。

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。必须同步两个鼠标指针，使远程鼠标指针跟随本地鼠标指针。请参阅"同步鼠标指针"。

虚拟控制台预览

启动虚拟控制台之前，可以通过**"System"（系统）→"Properties"（属性）→"System Summary"（系统摘要）**页预览虚拟控制台的状态。**"Virtual Console Preview"（虚拟控制台预览）**部分显示一张展示虚拟控制器状态的图像。该图像每 30 秒自动刷新。

注： 此虚拟控制台图像仅在您启用虚拟控制台时可用。

表 10-6 提供了有关可用选项的信息。

表 10-6. 虚拟控制台预览选项

选项	描述
启动	单击该按钮启动虚拟控制台。 如果仅启用了虚拟介质，则直接单击该链接启动虚拟介质。 如您不具有虚拟控制台权限或禁用虚拟控制台和虚拟介质，则该按钮为禁用；
设置	在**"Virtual Console / Media Configuration"（虚拟控制台 / 介质配置）**页上单击该链接查看或编辑虚拟控制台配置设置。
"Refresh"（刷新）	单击该按钮刷新显示的虚拟控制台图像。

使用 Video Viewer

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，Video Viewer 在单独窗口中启动。

注： 虚拟控制台标题栏显示从 Management Station 中连接的 iDRAC 的 DNS 名称或 IP 地址。如果 iDRAC 不具有 DNS 名称，则显示 IP 地址。命令格式是：<DNS 名称 / IPv6 地址 / IPv4 地址>, <型号>, <插槽号>, User: <用户名>, <fps>

Video Viewer 提供了各种控制调整，比如颜色模式、鼠标同步、快照、键盘宏指令、电源操作和虚拟介质访问。单击**"Help"（帮助）**了解有关这些功能的详情。

启动虚拟控制台会话并且 Video Viewer 出现后，可能需要调整颜色模式并同步鼠标指针。

表 10-7 说明了查看器中可以使用的菜单选项。

表 10-7. Viewer 菜单栏选择

菜单项	项目	说明
显卡	**"Pause"（暂停）**	临时暂停虚拟控制台。
	"Resume"（恢复）	恢复虚拟控制台。
	"Refresh"（刷新）	刷新查看器屏幕图像。
	"Capture Current Screen"（捕获当前屏幕）	将当前的远程系统屏幕捕获为 **.bmp** 文件。将显示一个对话框，使您可以将文件保存到指定位置。
	"Full Screen"（全屏）	要使"Video Viewer"（视频查看器）扩展为全屏幕模式，请单击查看器右上角以获得全屏幕。
	"Exit"（退出）	控制台使用结束并已注销后（使用远程系统的注销步骤），从**"Video"（视频）**菜单中选择**"Exit"（退出）**关闭"Video Viewer"（视频查看器） 窗口。
Keyboard（键盘）	"Hold Right Alt Key"（按住右 Alt 键）	选择此项，然后再键入想和右 <Alt> 键组合的键。
	"Hold Left Alt Key"（按住左 Alt 键）	选择此项，然后再键入想和左 <Alt> 键组合的键。
	"Left Windows Key"（左 Windows 键）	选择**"Hold Down"（按住）**，然后再键入想和左 Windows 键组合的字符。选择**"Press and Release"（按住并松开）**发送左 Windows 按键。
	"Right Windows Key"（右 Windows 键）	选择**"Hold Down"（按住）**，然后再键入想和右 Windows 键组合的字符。选择**"Press and Release"（按住并松开）**发送右 Windows 按键。
	"Macros"（宏）	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。Video Viewer 提供以下宏： • Alt+Ctrl+删除 • Alt+选项卡 • Alt+Esc • Ctrl+Esc • Alt+空格 • Alt+输入 • Alt+下划线 • Alt+F4 • PrtScrn • Alt+PrtScrn • F1 • 暂停 • Alt+M • Alt+D • Alt+PrtScrn+M • Alt+PrtScrn+P
	"Keyboard Pass-through"（键盘通过）	键盘通过模式可使客户端上所有键盘功能重定向到服务器。
Mouse（鼠标）	**"Synchronize Cursor"（同步光标）**	同步光标以便将客户端上的鼠标重定向到服务器上的鼠标。
	"Hide Local Cursor"（隐藏本地光标）	只显示来自虚拟控制台的光标。建议在虚拟控制台中运行 USC 时使用此设置。
"Options"（选项）	**"Color Mode"（颜色模式）**	允许选择颜色深度以提高网络上的性能。例如，如果正在从虚拟介质安装软件，可以选择最低的颜色深度，以便虚拟控制台查看器可以使用较少的网络带宽，用更多的带宽从介质传输数据。 颜色模式可以设置为 15 位彩色和 7 位彩色。

"Power"（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。
	"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。
"Media"（介质）	**"Virtual Media Wizard"（虚拟介质向导）**	**"Media"（介质）**菜单提供对"Virtual Media Wizard"（虚拟介质向导）的访问，使用户能够重定向到诸如以下的设备或映像： • 软盘驱动器 • CD • DVD • ISO 格式映像 • USB 闪存盘 有关虚拟介质功能的信息，请参阅 "配置并使用虚拟介质"。 使用虚拟介质时必须保持 Virtual Console Viewer 窗口活动。
"Help"（帮助）	**"About iDRACView"（关于 iDRACView）**	显示 iDRACView 版本。

同步鼠标指针

使用虚拟控制台连接到远程 Dell PowerEdge 系统时，远程系统上的鼠标加速度可能与 Management Station 上的鼠标指针不同步，从而造成 Video Viewer 窗口中出现两个鼠标指针。

要同步鼠标指针，单击**"Mouse"（鼠标）→"Synchronize cursor"（同步光标）**或按 <Alt><M>。

"Synchronize cursor"（同步光标）菜单项是一个切换。确保菜单项旁边有复选标记以便光标同步活动。

使用 Red Hat Enterprise Linux 或 Novell SUSE Linux 时，在启动查看器前务必配置鼠标模式。请参阅"在 iDRAC6 Web 界面上配置虚拟控制台和虚拟介质"获得配置帮助。操作系统的默认鼠标设置用于在 iDRAC6**"Virtual Console"（虚拟控制台）**屏幕中控制鼠标箭头。

禁用或启用本地控制台

使用 iDRAC6 Web 界面，可以配置 iDRAC6 以禁用 虚拟控制台连接。当本地控制台已禁用后，一个黄色状况点会出现在服务器 (OSCAR) 列表中，表示控制台已在 iDRAC6 中锁定。当本地控制台已启用时，状况点会变绿。

如果想确定对受管服务器控制台有独占访问，必须在**"Virtual Console"（虚拟控制台）屏幕**上禁用本地控制台*并重新配置***"Max Sessions"（最大会话数）**为 1。

注： 通过禁用（关闭）服务器上的本地视频，将禁用连接到虚拟控制台的显示器、键盘和鼠标。

要禁用或启用本地控制台，请执行以下过程：

1. 在 Management Station 上打开一个支持的 Web 浏览器并登录 iDRAC6。有关详情，请参阅"访问 Web 界面"。
2. 单击**"System"（系统）**，单击**"Virtual Console / Media"（虚拟控制台 / 介质）**选项卡，然后单击**"Configuration"（配置）**。
3. 如果想在服务器上禁用（关闭）本地视频，在**"Configuration"（配置）**屏幕中取消选择**"Local Server Video Enabled"（本地服务器视频已启用）**，然后单击**"Apply"（应用）**。默认值为**"Enabled"（已启用）**（选中）。
4. 如果想在服务器上启用（打开）本地视频，在**"Configuration"（配置）**屏幕中选择**"Local Server Video Enabled"（本地服务器视频已启用）**，然后单击**"Apply"（应用）**。

"**Virtual Console"（虚拟控制台）**屏幕显示本地服务器视频的状态。

远程启动虚拟控制台及虚拟介质

通过在支持的浏览器上输入单个 URL 可启动虚拟控制台或虚拟介质，而不必从 iDRAC6 Web GUI 启动。根据系统配置，可以通过手动验证过程（登录页）或自动定向到虚拟控制台或虚拟介质查看器 (iDRACView)。

注： Internet Explorer 支持本地、Active Directory (AD)、智能卡 (SC) 和单一登录 (SSO) 登录。Firefox 支持 SSO、本地和 AD 登录。

URL 格式

如果在浏览器中输入链接 **https: / / <idrac6_ip> / console**，则需要完成正常手动登录过程，这取决于登录配置。如果 SSO 未启用而启用本地、AD 或 SC 登录，则显示相应的登录

页。如果登录成功，将不启动虚拟控制台或虚拟介质视图。而是重定向到 iDRAC6 GUI 首页。

注： 用于启动 **iDRACView** 的 URL 区分大小写，只能采用小写方式输入。

一般错误情况

表 10-8 列出了一般错误情况、这些错误产生的原因及 iDRAC6 行为。

表 10-8. 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。	指定 *https://<ip>* 时的行为相同且登录失败。
权限不足	您没有虚拟控制台和虚拟介质权限。	iDRACView 未启动，将重定向到虚拟控制台/介质配置 GUI 页。
虚拟控制台已禁用	系统中的虚拟控制台已禁用。	iDRACView 未启动，将重定向到虚拟控制台/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。

常见问题

表 10-9 列出常见问题和解答。

表 10-9. 使用虚拟控制台：常见问题

问题	解答
带外 Web GUI 注销后，虚拟控制台不能注销。	即使注销 Web 会话，虚拟控制台和虚拟介质会话也将保持活动。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。
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 一收到本地视频打开请求，视频就立刻**打开**。
本地用户还可以关闭视频吗？	是的，本地用户可以使用 RACADM CLI（本地）关闭视频。
本地用户还可以打开视频吗？	否。本地控制台禁用后，本地用户的键盘和鼠标会禁用并且无法更改任何设置。
关闭本地视频是否也会关闭本地键盘和鼠标？	是。
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 and Virtual Media"（虚拟控制台和虚拟介质）**屏幕上。 RACADM CLI 命令 `racadm getconfig Cg cfgRacTuning` 在对象 **cfgRacTuneLocalServerVideo** 中显示状况。该 `racadm` 命令可以从 Telnet/SSH 执行或从 iDRAC6 的远程会话执行。 远程 RACADM 命令为： `racadm -r <idracip> -u <用户> -p <密码> getconfig -g cfgRacTuning` 该状况还可以在 虚拟控制台 OSCAR 显示中看到。当本地控制台已启用后，绿色状况会出现在服务器名称旁边。禁用后，黄点表示本地控制台已被 iDRAC6 锁定。
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。
控制台窗口显示乱码。	Linux 上的虚拟控制台查看器需要 UTF-8 字符集。检查区域设置并根据需要重设字符集。有关详情，请参阅"在 Linux 中设置区域"。
为什么在载入 Windows 2000 操作系统时受管服务器上出现空白屏幕？	受管服务器没有正确的 ATI 视频驱动程序。更新视频驱动程序。
执行虚拟控制台时，为什么鼠标在 DOS 中不同步？	Dell BIOS 仿真 PS/2 鼠标的驱动程序。根据设计，PS/2 鼠标为鼠标指针使用相对位置，这会造成同步的延迟。iDRAC6 带有 USB 鼠标驱动程序，该驱动程序允许使用绝对位置并且能够提供更紧密的鼠标指针跟踪。即使 iDRAC6 将 USB 的绝对鼠标位置传递给 Dell BIOS，BIOS 仿真程序依然会将它转换回相对位置，所以行为依旧。要修复此问题， 在**"Configuration"（配置）**屏幕中将鼠标模式设置为 **USC/Diags**。
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 (LC) 或启用生命周期控制器的 Dell Unified Server Configurator (USC-LCE) 中）？	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。 确保在**"Mouse"（鼠标）**菜单中选中**"Synchronize Mouse"（同步鼠标）**。按 <Alt><M> 或选择**"Mouse"（鼠标）→"Synchronize mouse"（同步鼠标）**以切换鼠标同步。同步启用后，复选标记会出现在**"Mouse"（鼠标）**菜单选项

	的旁边。
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，用以警告用户，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 指示灯不需要与远程服务器上的 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。
我需要多少带宽来运行虚拟控制台会话？	建议使用 5 MB/秒连接以获得良好性能。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。
启动虚拟控制台后，只能在虚拟控制台中使用鼠标，在本地系统中无法使用鼠标。为什么会出现这种情况，我应该怎样做才能在虚拟控制台和本地系统中使用鼠标？	如果将**"Mouse Mode"（鼠标模式）**设置为 **USC/Diags** 就会发生这种情况。按 <Alt><M> 热键，可在本地系统中使用鼠标。再次按 <Alt><M>，可在虚拟控制台中使用鼠标。

目录

目录

配置 vFlash SD 卡及管理 vFlash 分区

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

vFlash SD 卡是一种安全数字 (SD) 卡，可插入系统背面边角的可选 iDRAC6 企业卡插槽中。它提供像普通 USB 闪存盘设备一样的存储空间。它是用户定义的分区的存储位置，可作为 USB 设备配置提供给系统，也可用来创建可引导 USB 设备。取决于所选的仿真模式，这些分区可作为软盘驱动器、硬盘驱动器或 CD/DVD 驱动器提供给系统。可以将任何这些分区设置为可引导设备。

vFlash SD 卡和标准 SD 卡受支持。*vFlash SD 卡*指支持新的增强 vFlash 功能的卡。*标准 SD 卡*指通常的市售 SD 卡，仅支持有限的 vFlash 功能。

通过 vFlash SD 卡，可以创建最多 16 个分区。在创建分区时可以为其指定卷标名称，并可执行一系列的操作来管理和使用分区。vFlash SD 卡可以为 8GB（含）以下 的任意大小。每个分区最大可为 4GB。

标准 SD 卡可为任意大小，但只支持一个分区。分区的大小限制为 256MB。分区的卷标名称默认为"VFLASH"。

注： 确保只将一个 vFlash SD 卡或标准 SD 卡插入到 iDRAC6 企业卡插槽中。如果插入任何其他格式化的卡（例如多媒体卡 (MMC)），则在初始化卡时会显示下列错误信息：*An error has occurred while initializing SD card（初始化 SD 卡时出现错误）*。

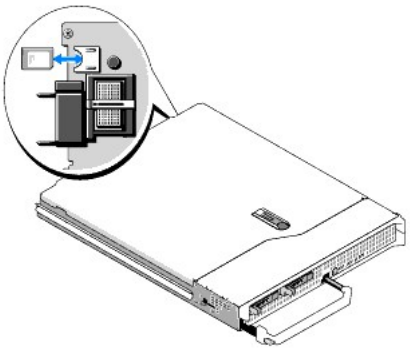
如果您是管理员，则可以对 vFlash 分区执行所有操作。如果不是，则您必须拥有"访问虚拟介质"权限，才可创建、删除、格式化、附加、分离或复制分区的内容。

注： 一次只能执行一项 vFlash 操作。必须先完成第一个操作，才可执行另一个 vflash 操作。例如，如果通过 RACADM 启动从映像创建操作，则无法通过 RACADM 或 GUI 执行创建、下载或格式化操作。必须等到该操作完成，才可执行下一个 vFlash 操作。

安装 vFlash 或标准 SD 卡

1. 从机箱上卸下刀片。
2. 找到位于系统背面边角的 vFlash 介质插槽。

   注： 您无需卸下刀片盖即可安装或取出卡。



3. 带标签的一面朝上，将 SD 卡的触针一端插入模块上的卡插槽中。

   注： 为确保卡的正确插入，插槽设置了键锁。

4. 向内按压卡，使其完全进入插槽并锁定。
5. 重新将刀片安装到机箱中。

卸下 vFlash 或标准 SD 卡

要卸下 VFlash 或标准 SD 卡，请向内推动卡使其松脱，然后从卡插槽中取出该卡。

通过 iDRAC6 Web 界面配置 vFlash 或标准 SD 卡

在安装完 vFlash 或标准 SD 卡后，可以查看其属性，启用或禁用 vFlash，以及初始化卡。必须启用卡才能执行分区管理操作。当卡被禁用时，只能查看其属性。初始化操作将删除现有的分区并重置卡。

注： 必须拥有"配置 iDRAC"权限才可启用或禁用 vFlash 或初始化卡。

如果系统的 iDRAC6 企业卡插槽上没有卡，则会显示下列错误信息。

`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）。

查看并配置 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。**"SD Card Properties"（SD 卡属性）** 页显示。

   表 11-1 列出了为 SD 卡所显示的属性。

表 11-1. SD 卡属性

属性	说明
Name（名称）	显示安装在服务器 iDRAC6 企业卡插槽上的卡的名称。如果该卡支持新的增强 vFlash 功能，则显示为 *vFlash SD 卡*。如果支持有限的 vFlash 功能，则显示为 *SD 卡*。
Size（大小）	显示千兆字节表示的卡大小 (GB)。
可用空间	显示 SD 卡上的未用空间 (MB)。此空间可用于在 vFlash SD 卡上创建更多分区。 如果插入的 SD 卡未初始化，则可用空间会显示该卡未初始化。
写保护	显示卡是否写保护。
运行状况	显示 SD 卡的整体运行状况。分为： • OK（良好） • Warning（警告） • Critical（严重） 如果为 Warning（警告），重新初始化卡。 如果为 Critical（严重），重新安装卡并重新初始化。
vFlash Enable（vFlash 启用）	选择该复选框可在卡上执行 vFlash 分区管理。清除该复选框可禁用 vFlash 分区管理。

4. 单击**"Apply"（应用）**以启用或禁用卡上的 vFlash 分区管理。

   如果附加了任何 vFlash 分区，则无法禁用 vFlash，并显示错误信息。

   注： 如果 vFlash 已禁用，则只能查看 SD 卡属性， 不能执行其他 vFlash 操作，如使用映像文件创建空分区，管理分区，格式化分区及下载分区内容。

5. 单击**"Initialize"（初始化）**。所有现有分区都将被删除并重设卡。此时将显示一条确认消息。
6. 单击**"OK"（确定）**。在初始化操作完成后，会显示一条已成功完成信息。

   注： 只有选定 **"vFlash Enable（vFlash 启用）**选项，才可使用**"Initialize"（初始化）**。

   如果已附加任何 vFlash 分区，则初始化操作会失败并显示错误信息。

如果在应用程序（如 WSMAN 提供程序、 iDRAC6 配置公用程序或 RACADM）使用 vFlash 时单击 vFlash 页面上的任何选项 ，或如果要 导航至 GUI 中的其他页面，iDRAC6 可能会显示以下信息。

`SD card is temporarily unavailable. To retry, click Refresh.` (SD 卡暂时无法使用。要重试，单击刷新。)

通过 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 命令查看及配置 vFlash 或标准 SD 卡。

注： 必须拥有"配置 iDRAC"权限才可启用或禁用 vFlash 或初始化卡。

显示 vFlash 或标准 SD 卡属性

打开到服务器的 telnet/SSH/Serial 控制台，登录并输入以下命令：

```
racadm getconfig -g cfgvFlashSD
```

此时显示下列只读属性：

- cfgvFlashSDSize
- cfgvFlashSDLicense
- cfgvFlashSDAvailableSize
- cfgvFlashSDHealth

启用或禁用 vFlash 或标准 SD 卡

打开到服务器的 telnet/SSH/Serial 控制台，登录并输入以下命令：

- 启用 vFlash 或标准 SD 卡：

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
  ```

- 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。如果卡不存在，显示以下消息：*"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/Serial 控制台，登录并输入以下命令：

```
racadm vflashsd initialize
```

所有现有分区都将被删除并重设卡。

获取 vFlash 或标准 SD 卡的最新状态

打开服务器的 telnet/SSH/Serial 控制台，登录并输入以下命令以查看向 vFlash 或标准 SD 卡发送的最新命令的状态：

```
racadm vFlashsd status
```

重设 vFlash 或标准 SD 卡

打开到服务器的 telnet/SSH/Serial 控制台，登录并输入：

```
racadm vflashsd initialize
```

有关 vflashsd 的详细信息，请参阅Dell 支持网站 **support.dell.com / manuals** 上可用的《 *iDRAC 管理员参考指南* 》。

注： 从 1.5 版本起，`racadm vmkey reset` 命令被取代。现在的 `vflashsd initialize` 命令包含该命令功能。虽然可成功执行 `vmkey reset` 命令，但建议使用 `vflashsd initialize` 命令。有关详情，请参阅"初始化 vFlash 或标准 SD 卡"。

通过 iDRAC6 Web 界面管理 vFlash 分区

可以执行以下任务：

- 创建空分区
- 使用映像文件创建分区
- 格式化分区
- 查看可用的分区

- 修改分区
- 附加/分离分区
- 删除现有的分区
- 下载分区内容
- 引导至分区

创建 空分区

空分区类似于空 USB 闪盘。可以在 vFlash 或标准 SD 卡上创建空分区。可以选择创建的分区类型有*软盘*或*硬盘*。分区类型 CD 不支持创建空分区。

注： 必须拥有"访问虚拟介质"权限才可创建空分区。

在创建 空分区之前，确保：

- 卡已初始化。
- 卡没有写保护。
- 未在卡上执行初始化操作。

创建空 vFlash 分区：

1. 在 iDRAC6 Web 界面上，选择**"System"（系统）**→ **"vFlash"**选项卡→ **"Create Empty Partition"（创建空分区）**子选项卡。此时显示 **"Create Empty Partition"（创建空分区）**页面。
2. 输入 表 11-2 中提供的信息。
3. 单击**"Apply"（应用）**。新分区已创建。

   注： 在创建分区过程中，不会显示进程或状态。

   若显示错误信息可能是以下原因之一：

   - 卡有写保护。
   - 卷标名称与某个现有分区的卷标相同。
   - 为分区大小输入的值为非整数，输入的值超过卡上的可用空间，或者所请求的分区大小大于 4GB。
   - 已在卡上执行初始化操作。

   注： 新的分区未格式化 (RAW)。

表 11-2. "Create Empty Partition "（创建空分区）页面选项

字段	说明
Index（索引）	选择分区索引。只有未使用的索引显示在下拉列表中。默认选择最低的可用索引值。可以将其更改为下拉列表中任何其他的索引值。 **注：** 对于标准 SD 卡，仅索引 1 是可用的。
Label（卷标）	为新分区输入唯一的卷标。卷标名称可以包含多达六个字母数字字符。卷标名称中不得包括空格。卷标名称字符显示为大写。 **注：** 对于标准 SD 卡，卷标名称必须是"VFLASH"。如果不是，会显示错误信息。
Emulation Type（仿真类型）	从下拉列表中为分区选择仿真类型。可用的选项为**软盘**和 **HDD** 。
Size（大小）	输入兆字节表示的分区大小 (MB)。分区大小最大为 4 GB， 或小于等于 vFlash SD 卡上的可用空间。 **注：** 对于标准 SD 卡，分区大小可高达 256MB。

使用映像文件创建分区

可使用映像文件（可为 **.img** 或 **.iso** 格式）在 vFlash 或标准 SD 卡上创建新分区。可以创建的分区类型有软盘、硬盘或 CD。创建的分区为只读。

注： 必须拥有" 访问虚拟介质"权限才可创建分区。

新创建的分区大小等于映像文件大小 。映像文件的大小必须：

- 小于或等于卡上的可用空间。
- 小于或等于 4GB。分区大小最大值为 4GB。

使用 Web 界面时， 对于 32 位和 64 位浏览器（Internet Explorer 和 FireFox），可以上传到 vFlash SD 卡上的映像文件大小的最大限值为 2GB。

使用 RACADM 和 WSMAN 界面时，可以上传到 vFlash SD 卡上的映像文件大小的最大值为 4 GB。

对于标准 SD 卡，映像文件大小必须小于或等于 256MB。

在基于映像文件创建分区之前，确保：

- 卡已初始化。
- 卡没有写保护。
- 未在卡上执行初始化操作。

注： 在基于映像文件创建分区时，确保映像类型和仿真类型匹配。iDRAC 基于指定的映像类型仿真设备。上传的映像文件与仿真类型不匹配时会出现问题。例如，如果是使用 ISO 映像创建的分区但仿真类型指定为硬盘 ，则 BIOS 将无法从此映像引导。

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。此时显示**"Create Partition from Image File"（从映像文件创建分区）** 页面。
2. 输入 表 11-3 中提供的信息。
3. 单击**"Apply"（应用）**。至此已使用映像文件创建了新分区。

   注： 在创建分区过程中，不会显示进程或状态。

   若显示错误信息可能是以下原因之一：

   - 卡有写保护。
   - 卷标名称与某个现有分区的卷标相同。
   - 映像文件的大小大于 4GB 或超过卡上的可用空间。
   - 映像文件不存在，或映像文件的扩展名既不是 **.img** 也不是 **.iso**。
   - 已在卡上执行初始化操作。

表 11-3. 通过"映像文件"页面选项创建分区

字段	说明
索引	选择分区索引。只有未使用的索引显示在下拉列表中。默认选择最低的可用索引值。可以将其更改为下拉列表中任何其他的索引值。 **注：** 对于标准 SD 卡，仅索引 1 是可用的。
Label（卷标）	为新分区输入唯一的卷标。可以包含多达 6 个字母数字字符。卷标名称中不得包括空格。卷标名称字符显示为大写。 **注：** 对于标准 SD 卡，卷标名称必须是"VFLASH"。如果不是，会显示错误信息。
Emulation Type（仿真类型）	从下拉列表中为分区选择仿真类型。可用的选项为**软盘**、**HDD** 和 **CDROM** 。
映像位置	单击**"Browse"（浏览）**并指定映像文件的位置。仅支持 **.img** 或 **.iso** 文件类型。

格式化分区

可以基于文件系统类型格式化 vFlash SD 卡上的现有分区。支持的 文件系统类型有 EXT2、EXT3、FAT16 和 FAT32。带有限 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 CD 分区。不能格式化只读分区。

注： 必须拥有" 访问虚拟介质"权限才可格式化分区。

在格式化分区之前，应确保：

- 卡已启用。
- 分区未附加。
- 卡没有写保护。
- 未在卡上执行初始化操作。

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。此时会显示**"Format"（格式化）**页面。
2. 输入 表 11-4 中提供的信息。
3. 单击**"Apply"（应用）**。此时会显示一条关于分区上的所有数据将被删除的警告消息。单击**"OK"（确定）**。至此已根据指定的文件系统类型格式化了所选分区。

   若显示错误信息可能是以下原因之一：

   - 卡有写保护。
   - 已在卡上执行初始化操作。

表 11-4. "格式化分区"页面选项

字段	说明
Label（卷标）	选择您要格式化的分区卷标。默认选择第一个可用的分区。 类型为软盘或硬盘的所有现有分区在下拉列表中均可用。附加分区或只读分区在下拉列表中不可用。
Type to Format to（格式化为何种类型）	选择要将分区格式化为何种文件系统类型。可用的选项有 EXT2、EXT3、FAT16 和 FAT32。对于标准 SD 卡，仅 FAT32 可用。

查看可用分区

要查看可用分区列表，必须确保 vFlash 或标准 SD 卡已启用。

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 Partition"（管理分区）**页面列出了可用分区。
2. 关于每个分区，可以查看 表 11-5 中提供的信息。

表 11-5. 查看可用分区

字段	说明
Index（索引）	是按 1 至 16 为分区编索引的。一个分区索引对应一个唯一的特定分区。在创建分区时指定。
Label（卷标）	标识分区。在创建分区时指定。
Size（大小）	分区大小以兆字节 (MB) 为单位。
Read Only（只读）	分区的读写访问状态。 - 选中 = 只读分区 - 未选中 = 读写分区 **注：** 对于标准 SD 卡，分区是读写模式， 此列不会显示。
Attached（已附加）	指出分区是否作为 USB 设备对操作系统可见。要附加或分离分区，请参阅章节" 附加和分离分区"。
Emulation Type（仿真类型）	显示分区类型是软盘、硬盘还是 CD。
Type（类型）	显示分区类型是软盘、硬盘还是 CD。

修改分区

要修改分区，必须确保卡已启用。

注： 必须拥有"访问虚拟介质"权限才可修改 vFlash 分区。

可以将只读分区更改为读写，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。此时显示 **"Manage Partitions"（管理分区）**页面。
2. 在 **"Read Only"（只读）**列，为要更改为只读的分区选中该复选框，或者为要更改为读写的分区清除该复选框。

   注： 如果分区类型是 CD，则其状态为只读且该复选框被选中。无法将其状态更改为读写。
   如果分区是附加的，则该复选框呈灰色显示。
   对于标准 SD 卡，分区是读写模式，**"Read Only"（只读）**列不会显示。

3. 单击**"Apply"（应用）**。至此基于所选项分区已更改为只读或读写。

附加和分离分区

可以 附加一个或多个分区作为虚拟的 USB 大容量存储设备，从而作为大容量存储设备对操作系统和 BIOS 可见。同时附加多个分区时， 会基于索引按升序将它们呈现给主机操作系统。相应的驱动器号分配是由操作系统控制。

若分离了某个分区，则主机操作系统不再视其为虚拟的 USB 大容量存储设备，并会从 BIOS 引导次序菜单中将其删除。

在附加或分离分区时，系统的 USB 总线会重设。这会影响正在使用 vFlash 的任何应用程序（如操作系统），并将断开所有 iDRAC 虚拟介质会话。

注： 必须拥有"访问虚拟介质"权限才可附加或分离分区。

在附加或分离分区之前，必须确保：

- 卡已启用。
- 未在卡上执行初始化操作。

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。此时显示 **"Manage Partitions"（管理分区）**页面。
2. 在 **"Attached"（附加）**列，为要附加的分区选中此复选框，或为要分离的分区清除此复选框。

   注： 分离的分区不会显示在引导顺序中。

3. 单击**"Apply"（应用）**。至此已基于所选项附加或分离了分区。

操作系统针对附加的分区的行为

当分区已附加且主机操作系统是 Windows，则分配给附加分区的驱动器号由操作系统控制。

如果分区为只读，则在主机操作系统中会显示为只读。

如果主机操作系统不支持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，分区类型 EXT2 无法从 Windows 操作系统中读取。

从主机操作系统更改附加的分区的卷标名称时，不会影响 iDRAC 为该分区存储的卷标名称。

删除现有的分区

注： 可以删除 vFlash 或标准 SD 上的现有分区。

在 删除现有分区之前，必须确保：

- 卡没有写保护。
- 分区未附加。
- 未在卡上执行初始化操作。

  注： 必须拥有"访问虚拟介质"权限才可修改分区。

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。此时显示 **"Manage Partitions"（管理分区）**页面。

2. 在**"Delete"（删除）**列，单击要删除的分区的删除图标，然后单击**"Apply"（应用）**。至此分区已删除。

下载分区内容

可以将 vFlash 分区内容作为 **.img** 或 **.iso** 格式的映像文件下载到本地或远程位置。本地位置在 iDRAC6 Web 界面所在的管理系统上。远程位置是指 Managed System。

注： 必须拥有" 访问虚拟介质"权限才可下载分区。

在将内容下载到本地或远程位置之前，必须确保：

- 卡已启用。
- 未在卡上执行初始化操作。
- 对于读写分区，不得附加它。

下载 vFlash 分区内容到系统某个位置：

1. 在 iDRAC6 Web 界面上，选择**"System"（系统）**→ **"vFlash"**选项卡→ **"Download"（下载）** 子选项卡。此时显示**" Download Partition"（下载分区）**页面。
2. 从**"Label"（卷标）**下拉菜单上，选择要下载的分区。所有现有分区都显示在列表上，附加的分区除外。默认选择第一个分区。
3. 单击**"Download"（下载）**。
4. 指定要保存文件的位置。

   如果只指定文件夹位置，则分区卷标将用作为文件名，且扩展名为 **.iso**（对于 CD 类型分区）或 **.img**（对于软盘和硬盘类型分区）。
5. 单击"**Save"**（保存）。所选分区的内容将下载到指定的位置。

引导到分区

可以将附加的 vFlash 分区设置为下一个引导操作的引导设备。vFlash 分区必须包含可引导的映像（**.img** 或 **.iso** 格式）才可将其设置为引导设备。要将分区设置为引导设备以及执行引导操作，必须确保卡已启用。

注： 必须拥有"访问虚拟介质"权限才可将分区设置为引导设备。

可以对 vFlash 或标准 SD 卡执行引导操作。关于各个步骤，请参阅 "First Boot Device（第一个引导设备）" 部分。

注： 如果系统 BIOS 不支持 vFlash 作为第一个引导设备，则附加的 vFlash 分区不会列入**"First Boot Device"（第一个引导设备）** 下拉菜单上。因此，必须确保将 BIOS 更新到可支持将 vFlash 分区设置为第一个引导设备的最新版本。如果 BIOS 是最新的版本， 则重新启动服务器时，BIOS 会提示 iDRAC 它支持 vFlash 作为第一个引导设备，这样 iDRAC 就会将 vFlash 分区列入**"First Boot Device"（第一个引导设备）**下拉菜单。

使用 RACADM 管理 vFlash 分区

可以使用 vFlashPartition 子命令在已初始化的 vFlash 或标准 SD 卡上创建、删除、列出或查看分区状态 。命令格式是：

```
racadm vflashpartition <create | delete | status | list> <选项>
```

注： 必须拥有"访问虚拟介质"权限才可执行 vFlash 分区管理。

有效选项：

-i <索引>	适用于此命令的分区索引。 <索引> 必须是介于 1 到 16 的整数。 **注：** 对于标准 SD 卡，索引值限制为 1，因为只支持一个大小 256MB 的分区。

仅适用于创建操作的选项：

-o <卷标>	将分区安装到操作系统时所显示的卷标。 <卷标> 必须是一个包含最多 6 个字母数字字符的字符串，并且不能含有空格。
-e <类型>	分区的仿真类型。<类型> 必须是软盘、CDROM 或 HDD。
-t <类型>	创建 <类型> 类型的分区。<类型> 必须是：

	• 空 - 创建空分区。
	  ○ -s <大小> - MB 表示的分区大小。
	  ○ -f <类型>- 基于文件系统类型的分区的格式化类型。有效选项包括 RAW、FAT16、FAT32、EXT2 或 EXT3。
	• 映像 - 使用映像文件创建分区。下列选项适用于映像类型：
	  ○ -l <路径> - 指定相对于 iDRAC 的远程路径。路径可以位于安装的驱动器上或共享：
	SMB 路径： //<ip 或域>/<共享名称> /<映像路径>
	NFS 路径：<ip 地址>:/<映像路径>
	  ○ -u <用户> - 访问远程映像的用户名。
	
	-p <密码> - 访问远程映像的密码。

仅适用于状态操作的选项：

-i	显示分区索引的状态。

创建分区

- 创建 20MB 的空分区：

  ```
  racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20
  ```

- 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： 使用本地 RACADM 不支持的映像文件创建分区。

删除分区

- 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 "初始化 vFlash 或标准 SD 卡"。

获取分区状态

- 获取分区 1 的操作状态：

  ```
  racadm vflashpartition status -i 1
  ```

- 获取所有现有分区的状态：

  ```
  racadm vflashpartition status -a
  ```

查看分区信息

列出所有现有分区及其属性：

```
racadm vflashpartition list
```

引导到分区

- 列出引导列表中可用的设备：

  ```
  racadm getconfig -g cfgServerInfo -o cfgServerFirstBootDevice
  ```

  如果是 vFlash SD 卡，则附加的分区的卷标名称会出现在引导列表中。如果是标准 SD 卡且分区是附加的，则"VFLASH"会出现在引导列表中。

- 将 vFlash 分区设置为引导设备：

  ```
  racadm config -g cfgServerInfo -o cfgServerFirstBootDevice "<vFlash 分区名称>"
  ```

  其中，对 vFlash SD 卡，<vFlash 分区名称> 是其卷标名称，而对于标准 SD 卡，它是"VFLASH"。

  在运行此命令时，vFlash 分区卷标被自动设置为引导一次，即 **cfgserverBootOnce** 设置为 1。引导一次仅将设备引导到分区一次， 不会在引导次序中始终将其保持第一。

附加或分离分区

- 附加分区：

  ```
  racadm config –g cfgvflashpartition –i 1 –o cfgvflashPartitionAttachState 1
  ```

- 分离分区：

  ```
  racadm config –g cfgvflashpartition –i 1 –o cfgvflashPartitionAttachState 0
  ```

修改分区

- 将只读分区更改为读写：

  ```
  racadm config –g cfgvflashpartition –i 1 –o cfgvflashPartitionAccessType 1
  ```

- 将读写分区更改为只读：

  ```
  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细信息，请参阅 Dell 支持网站 **support.dell.com / manuals** 上的《 *iDRAC 管理员参考指南*》。

常见问题

什么时候锁定 vFlash 或标准 SD 卡？

当正在执行的操作需要独占访问介质时，iDRAC 会锁定虚拟闪速更新介质。例如，在初始化操作期间。

目录

目录

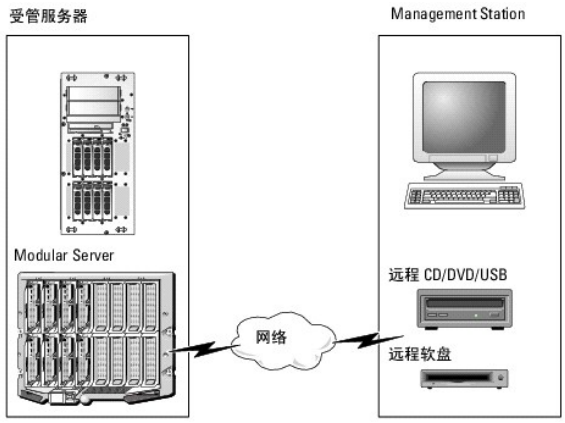
配置并使用虚拟介质

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

概览

虚拟介质功能可通过虚拟控制台查看器访问，提供了受管服务器对网络上远程系统所连介质的访问。图 12-1 显示了虚拟介质的整体结构。

图 12-1. 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。连接虚拟介质后，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。当虚拟介质处于连接状态时，Managed System 上的虚拟设备会显示为未装有介质的两个驱动器。

表 12-1 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 12-1. 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（最小大小为 128 MB）	

基于 Windows 的 Management Station

要在运行 Windows 操作系统的 Management Station 上运行虚拟介质功能，请安装所支持版本的带有 ActiveX 控件插件的 Internet Explorer。将浏览器安全性设置为**中**或更低设置以允许 Internet Explorer 下载和安装已签名的 ActiveX 控件。

根据 Internet Explorer 的版本，可能需要自定义 ActiveX 的安全设置：

1. 启动 Internet Explorer。
2. 单击**"Tools"（工具）→"Internet Options"（Internet 选项）**，然后单**"Security"（安全）**选项卡。
3. 在**"Select a Web content zone to specify its security settings"（选择 Web 内容区域以指定其安全设置）**中，单击选择所需的区域。
4. 在**"Security level for this zone"（此区域的安全级别）**中，单击**"Custom Level"（自定义级别）**。

   屏幕将显示**"Security Settings"（安全设置）**窗口。
5. 在**"ActiveX controls and plugins"（ActiveX 控件和插件）**中，确保将以下设置设置为**"Enable"（启用）**：
   - 允许脚本
   - 自动提示 ActiveX 控件
   - 下载已签名的 ActiveX 控件
   - 下载未签名的 ActiveX 控件
6. 单击**"OK"（确定）**保存所有更改，并关闭**"Security Settings"（安全设置）**窗口。
7. 单击**"OK"（确定）**关闭**"Internet Options"（Internet 选项）**窗口。
8. 重新启动 Internet Explorer。

必须具有管理员权限才能安装 ActiveX。安装 ActiveX 控件前，Internet Explorer 可能会显示一条安全警告。要完成 ActiveX 控件安装过程，必须在 Internet Explorer 显示安全警告提示时接受该控件。

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 Java Runtime Environment (JRE) 才能运行虚拟控制台插件。可以从 **java.sun.com** 下载 JRE。

配置虚拟介质

1. 登录到 iDRAC6 Web 界面。
2. 单击**"System"（系统）→"Virtual Console / Media"（虚拟控制台 / 介质）→"Configuration"（配置）**。
3. 在"Virtual Media"（虚拟介质）部分选择设置值。请参阅 表 12-2 了解关于"Virtual Media"（虚拟介质）配置值的信息。
4. 单击**"Apply"（应用）**保存设置。

   将会显示警报对话框，显示以下信息："You are about to change device configuration. All existing redirection sessions will be closed.Do you want to continue?"（您将要更改设备配置。将关闭所有现有的重定向会话。要继续吗？）
5. 单击 **OK**（确定）继续。

   此时会出现显示以下信息的提示对话框："Virtual Media Configuration successfully set."（虚拟介质配置成功设置。）

表 12-2. 虚拟介质配置值

属性	值
"Attach Virtual Media"（连接虚拟介质）	**"Attach"（连接）** - 立刻将"Virtual Media"（虚拟介质）连接到服务器。 **"Detach"（分离）** - 立刻从服务器上分离"Virtual Media"（虚拟介质）。 **"Auto-Attach"（自动连接）** - 只有当虚拟介质会话启动时才将"Virtual Media"（虚拟介质）连接到服务器。
"Maximum Sessions"（最大会话）	显示"Virtual Media"（虚拟介质）会话的最大允许数目。此值始终为 **1**。 **注：** 只允许一个虚拟介质用户会话；但一个会话中可连接多个设备。请参阅"运行虚拟介质"。
"Active Sessions"（激活的会话数）	显示当前活动的虚拟介质会话数。

"Virtual Media Encryption Enabled"（虚拟介质加密已启用）	启用（选中）或禁用（未选中）"Virtual Media"（虚拟介质）连接的加密。
"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。如果不选中此项，则显示为 USB 闪存盘驱动器。 **注：** 在某些 Windows Vista 和 Red Hat Enterprise Linux 环境中，不能启用 **"Floppy Emulation"（软盘仿真）**来虚拟化 USB。
"Enable Boot Once"（启用引导一次）	启用（选中）或禁用（未选中）引导一次选项，会在服务器引导一次后自动终止"Virtual Media"（虚拟介质）会话。使用此属性从虚拟介质引导。在下次引导时，系统会从引导顺序中的下一个设备引导。此选项对于自动部署有用。

运行虚拟介质

小心： 运行虚拟介质会话时不要发出 racreset 命令。否则会产生不良后果，包括数据丢失。

注： 访问虚拟介质时，Virtual Console Viewer 窗口应用程序必须保持活动。

1. 在 Management Station 上打开支持的 Web 浏览器。
2. 登录到 iDRAC6 Web 界面。
3. 单击**"Virtual Console / Media"（虚拟控制台 / 介质）**选项卡。

   此时会出现**"Virtual Console and Virtual Media"（虚拟控制台和虚拟介质）**屏幕。

   如果要更改任何显示属性的值，请参阅"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。同时可以选择一个光盘驱动器和一个软盘，或者单个驱动器。

   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络管理员。

4. 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。

   iDRACView 应用程序会以单独的窗口启动。

5. 选择**"Media"（介质）→"Virtual Media Wizard"（虚拟介质向导）**。

   此时会出现**"Media Redirection"（介质重定向）**窗口。

6. 查看**"Media Redirection"（介质重定向）**窗口底部的**"Status"（状态）**部分。如果介质已连接，可以断开该介质，然后再连接其它介质源。要断开介质，请单击**"Disconnect"（断开）**按钮（位于**"Status"（状态）**窗口中的介质旁）。
7. 选择位于希望连接的介质类型旁边的单选按钮。
8. 您可选择**"Floppy Image"（软盘映像）**单选按钮和 **CD / DVD 驱动器**部分中的单选按钮之一。

   注： 当 Management Station CD/DVD 介质已由 iDRAC6 刀片使用时，相同介质可以重定向并提供给另一个 iDRAC6 刀片。换句话说，iDRAC6 支持向两个不同 iDRAC6 刀片重定向相同介质（只读）。但是对于 USB 介质，将无法连接到两个 iDRAC6 刀片。iDRAC6 显示警告信息提示这一情况。

   要连接软盘映像或 ISO 映像，请在本地计算机上输入到映像位置的路径或单击**"Browse"（浏览）**按钮导航至映像位置。

   注： 如果使用基于 Java 的虚拟介质插件，将不能装载远程 ISO 映像。例如，Linux 客户端不会允许装载映像，因为它们使用基于 Java 的插件。为避免这种情况，将 ISO 映像复制到本地系统以使映像文件在本地可用。基于 Java 的虚拟介质插件不允许使用 **\\computer\share** 格式指定共享名称。

9. 单击各个所选介质类型旁边的**"Connect"（连接）按钮。**

   介质将会连接并且**"Status"（状态）**窗口将会更新。

10. 单击**"Close"（关闭）。**

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。

断开虚拟介质连接

1. 选择**"Media"（介质）→"Virtual Media Wizard"（虚拟介质向导）**。

   此时会出现**介质重定向向导**。

2. 单击希望断开连接的介质旁边的**"Disconnect"（断开连接）**。

   介质将会断开连接并且**"Status"（状态）**窗口将会更新。

3. 单击 **Close（关闭）**。

注： 启动 **iDRACview** 并随后注销 Web GUI，**iDRACView** 将不会终止并保持活动。

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"部署操作系统"。

1. 验证以下内容：
   - 操作系统安装 DVD/CD 插入到 Management Station 的 DVD/CD 驱动器中。
   - 选择了本地 DVD/CD 驱动器。
   - 已与虚拟驱动器连接。
2. 按照"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 DVD/CD 驱动器引导。
3. 按照屏幕上的说明完成安装。

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。

常见问题

表 12-3 列出常见问题和解答。

表 12-3. 使用虚拟介质：常见问题

问题	解答
有时，我发现虚拟介质客户端连接断开。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间的链接。 如果虚拟介质配置设置在 iDRAC6 Web 界面或本地 RACADM 命令中更改，当配置更改应用后，任何所连介质都会断开连接。 要重新连接虚拟驱动器，使用虚拟介质向导。
哪些操作系统支持 iDRAC6？	请参阅"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"支持的 Web 浏览器"查看所支持 Web 浏览器的列表。
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。
Windows 操作系统安装所用时间似乎太长了。为什么？	如果正在安装 Windows 操作系统并且网络连接很慢，则由于网络延迟，安装过程会需要更多时间访问 iDRAC6 Web 界面。虽然安装窗口没有显示安装进程，安装仍在进行。
我正在查看软盘驱动器或 USB 闪存盘的内容。如果尝试使用同一驱动器建立虚拟介质连接，我会收到连接故障信息并要求我重试。为什么？	不允许同时访问虚拟软盘驱动器。尝试虚拟化驱动器前，关闭用于查看驱动器内容的应用程序。
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 设置并导航到引导菜单。找到虚拟 CD、虚拟软盘或 vFlash 并根据需要更改设备引导顺序。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 • 被操作系统识别为可移动磁盘（最小大小为 128 MB）的 USB 闪存盘 • USB 闪存盘映像
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 提示符处输入以下命令： `sys a: x: /s` 其中 *x* 是要使其可引导的 USB 闪存盘。
我的虚拟软盘驱动器上支持何种文件系统类型？	虚拟软盘驱动器支持 FAT16 或 FAT32 文件系统。
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，断开远程连接，并卸下虚拟驱动器。当 iDRAC6 重设完成后，这些驱动器会重新出现。

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？	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。

目录

目录

使用 RACADM 命令行界面

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

RACADM 命令行界面 (CLI) 允许从受管服务器使用 iDRAC6 管理功能。RACADM 允许访问 iDRAC6 Web 界面上的大部分功能。不过，可以在脚本中使用 RACADM 以简化多个服务器的配置，而不使用对于交互式管理更有用的 Web 界面。

RACADM 有以下界面可用：

- 本地 RACADM
- 远程 RACADM
- Telnet/SSH RACADM

本地 RACADM 命令不使用网络连接从受管服务器访问 iDRAC6。这意味着可以使用本地 RACADM 命令配置初始 iDRAC6 网络。远程 RACADM 是一种客户端公用程序，可用于从 Management Station 通过带外网络接口执行。使用 SSH/Telnet RACADM 来从 SSH 或 Telnet 提示符下使用 RACADM 命令。

本节提供以下信息：

- RACADM 命令和支持的 RACADM 界面
- 从命令提示符使用本地 RACADM
- 远程 RACADM
- SSH/Telnet RACADM
- 使用 **racadm** 命令配置 iDRAC6
- 使用 RACADM 配置文件配置多个 iDRAC6

小心： 最新的 iDRAC6 固件只支持最新的 RACADM 版本。如果使用较旧版本的 RACADM 查询具有最新固件的 iDRAC6，可能会出错。安装随最新 Dell OpenManage DVD 介质提供的 RACADM 版本。

RACADM 子命令

表 13-1 提供可在 RACADM 中运行的每个 RACADM 子命令的说明。有关 RACADM 子命令及语法和有效条目的详细列表，请参阅 Dell 支持网站 **support.dell.com/manuals** 提供的《*iDRAC6 管理员参考指南*》。

表 13-1. RACADM 子命令

命令	说明
arp	显示 ARP 表的内容。不能添加或删除 ARP 表条目。
clearasrscreen	删除上次崩溃 (ASR) 屏幕
closessn	关闭设备中的通信会话。
coredump	显示最后一次 iDRAC6 信息转储。
coredumpdelete	删除 iDRAC6 中存储的信息转储。
clrraclog	清除 iDRAC6 日志。清除后，会有一个条目用来指示清除日志的用户和时间。
clrsel	清除受管服务器的系统事件日志条目。
config	配置 iDRAC6。
fwupdate	更新 iDRAC6 固件。
getconfig	显示当前 iDRAC6 配置属性。
getniccfg	显示控制器的当前 IP 配置。
getraclog	显示 iDRAC6 日志。
getractime	显示 iDRAC6 时间。
getsel	显示 SEL 条目。
getssninfo[1]	显示关于活动会话的信息。
getsvctag	显示服务标签。

getsysinfo	显示有关 iDRAC6 和受管服务器的信息，包括 IP 配置、硬件型号、固件版本和操作系统信息。
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。
help	列出 iDRAC6 子命令。
help <*子命令*>	列出指定子命令的用法语句。
ifconfig	显示网络接口表的内容。
krbkeytabupload	上载 Kerberos keytab 文件。
localconredirdisable	从本地系统执行本地虚拟控制台禁用。
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。需要目标 IP 地址。ICMP 回音数据包根据当前的路由表内容发送到目标 IP 地址。
ping6	验证目标 IPv6 地址是否可以使用当前路由表内容从 iDRAC6 进行访问。需要目标 IPv6 地址。根据当前的路由表内容将 ICMP 回音数据包发送到目标 IPv6 地址。
racdump	显示状态和 iDRAC6 的一般信息。
racreset	重设 iDRAC6。
racresetcfg	将 iDRAC6 重设为默认配置。
remoteimage	远程文件共享
serveraction	在受管服务器上执行电源管理操作。
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。
sslcertdownload	下载 CA 证书。
sslcertupload	将 CA 证书或服务器证书上载至 iDRAC6。
sslcertview	查看 iDRAC6 中的 CA 证书或服务器证书。
sslcsrgen	生成并下载 SSL CSR。
testemail	强制 iDRAC6 通过 iDRAC6 NIC 发送电子邮件。
testtrap	强制 iDRAC6 通过 iDRAC6 NIC 发送 SNMP 警报。
traceroute	跟踪数据包从系统转发到目标 IPv4 地址的过程中历经的路由器网络路径。
traceroute6	跟踪数据包从系统转发到目标 IPv6 地址的过程中历经的路由器网络路径。
version	显示 iDRAC6 版本信息。
vflashsd	初始化或获取 vflash SD 卡的状态。
vflashpartition	创建、删除、列出或查看初始化的 vFlash SD 卡上分区的状态。
vmdisconnect	关闭所有打开的与远程客户端的 iDRAC6 虚拟介质连接。
vmkey	将 vFlash 分区重设为 256 MB 的默认大小，并删除分区的全部数据。
[1] 对 getssninfo 命令的响应中不包含 SOL 会话信息。	

使用本地 RACADM 命令

从命令提示符或 shell 提示符本地运行 RACADM 命令（在受管服务器上）。

登录受管服务器，启动命令 shell，然后按以下一种格式输入本地 RACADM 命令：

- `racadm <子命令> [参数]`
- `racadm <getconfig|config> [-g <组>] [-o <对象> <值>]`

不带选项的 RACADM 命令显示常规用法信息。要显示 RACADM 子命令列表，输入：

```
racadm help
```

或

```
racadm getconfig -h
```

子命令列表包括 iDRAC6 支持的所有 RACADM 命令。

要获得子命令帮助，输入：

```
racadm help <子命令>
```

该命令显示子命令的语法和命令行选项。

使用 RACADM 公用程序配置 iDRAC6

本节介绍如何使用 RACADM 执行各种 iDRAC6 配置任务。

显示当前 iDRAC6 设置

RACADM **getconfig** 子命令从 iDRAC6 检索当前配置设置。配置值归入各*组*中，其中包含一个或多个*对象*，而对象具有*值*。

请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》了解组和对象的完整说明。

要显示所有 iDRAC6 组的列表，输入此命令：

```
racadm getconfig -h
```

要显示特定组的对象和值，输入此命令：

```
racadm getconfig -g <组>
```

例如，要显示所有 **cfgLanNetworking** 组对象设置的列表，输入以下命令：

```
racadm getconfig -g cfgLanNetworking
```

使用 RACADM 管理 iDRAC6 用户

注： 使用 **racresetcfg** 命令时请小心，因为*所有*配置参数都会重设为初始默认值。任何之前的更改将丢失。

注： 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**。

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。

注： 为 Active Directory 环境创建的用户和组必须符合 Active Directory 命名惯例。

最多可以在 iDRAC6 属性数据库中配置 15 个用户。（第十六位用户保留作为 IPMI LAN 用户。）手动启用 iDRAC6 用户前，验证是否存在任何当前用户。

要验证用户是否存在，请在命令提示符处输入以下命令：

```
racadm getconfig -u <用户名>
```

或

输入以下命令，每次仅查找索引 1 至 16 中的一个：

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

注： 还可以输入 racadm getconfig -f <*文件名*> 并查看生成的 <*文件名*> 文件，其中包括所有用户和所有其它 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=nn
```

```
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，则该索引将分配给该用户。

注： 为 Active Directory 环境创建的用户和组必须符合 Active Directory 命名惯例。

添加 iDRAC6 用户

要在 iDRAC6 中添加用户，请按以下步骤进行：

1. 设置用户名。
2. 设置密码。
3. 设置登录到 iDRAC6 用户权限。
4. 启用用户。

示例

下面的示例说明如何添加密码为"123456"的新用户"John"，以及 iDRAC6 的登录权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

为验证新用户，使用以下某一命令：

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

启用 iDRAC6 用户权限

要给用户授予特定的管理（基于角色）权限，请将 **cfgUserAdminPrivilege** 属性设置为表 13-2 所示的值组成的位掩码：

表 13-2. 用户权限位掩码

用户权限	权限位掩码
"Login to iDRAC6"（登录到 iDRAC6）	0x00000001
"Configure iDRAC6"（配置 iDRAC6）	0x00000002
"Configure Users"（配置用户）	0x00000004
"Clear Logs"（清除日志）	0x00000008
"Execute Server Control Commands"（执行服务器控制命令）	0x00000010
访问虚拟控制台	0x00000020
"Access Virtual Media"（访问虚拟介质）	0x00000040
"Test Alerts"（检测警报）	0x00000080
"Execute Debug Commands"（执行调试命令）	0x00000100

例如，要给用户授予**"Configure iDRAC6"（配置 iDRAC6）**、**"Configure Users"（配置用户）**、**"Clear Logs"（清除日志）**和**"Access Virtual Console"（访问虚拟控制台）**权限，添加值 0x00000002、0x00000004、0x00000008 和 0x00000010 组成位掩码 0x0000002E。然后输入以下命令以设置权限：

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

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。

从本地 RACADM：

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

从 telnet/ssh RACADM：

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

<密钥文本>
```

示例：

使用文件向 iDRAC6 用户 2 的第一个密钥空间中上载一个有效密钥：

```
$ 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： telnet/ssh/serial RACADM 不支持"file"（文件）选项。**

视图

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
```

"Delete"（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
```

小心： 通常为 iDRAC 的管理员用户组的成员保留该权限。但也可将该权限分配给"Custom"（自定义）用户组中的用户。具有该权限的用户可修改任何用户的配置。其中包括创建或删除任何用户、用户的 SSH 密钥管理等。出于这些原因，应谨慎分配该权限。

请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》中的 sshpkauth，了解子命令选项的信息。

删除 iDRAC6 用户

使用 RACADM 时，无法删除 iDRAC 用户。仅可使用 **cfgUserAdminEnable** 对象禁用该用户。该命令的语法为：

```
racadm config Cg cfgUserAdmin Co cfgUserAdminEnable CI <索引>
```

要了解管理用户管理的信息，请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》。

检测电子邮件警报

iDRAC6 电子邮件警报功能允许用户在受管服务器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检测电子邮件警报功能以确保 iDRAC6 可以在网络上正确发送电子邮件警报。

```
racadm testemail -i 2
```

（-i 2 表示电子邮件警报表中的第 2 个索引条目）

注： 确保在检测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"配置电子邮件警报"。

检测 iDRAC6 SNMP 陷阱警报功能

iDRAC6 SNMP 陷阱警报功能允许 SNMP 陷阱侦听器配置为接收受管服务器上发生的系统事件陷阱。

下面的示例说明用户如何检测 SNMP 陷阱警报功能。

```
racadm testtrap -i 2
```

（-i 2 表示电子邮件警报表中的第 2 个索引条目）

注： 检测 iDRAC6 SNMP 陷阱警报功能之前，请确保正确配置了 SNMP 和陷阱设置。请参阅 **testtrap** 和 **testemail** 子命令说明来配置这些设置。有关详情，请参阅"配置平台事件陷阱 (PET)"。

配置 iDRAC6 网络属性

要生成可用网络属性的列表，请输入以下命令：

```
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提示您按下 <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"iDRAC6 LAN"。

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。

配置 LAN 上 IPMI

1. 通过输入以下命令，配置 LAN 上 IPMI：

   ```
   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. 通过输入以下命令更新 IPMI 信道权限：

      ```
      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，要将 IPMI LAN 信道权限设置为 2（用户），输入以下命令：

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. 如果需要，使用如下的命令设置 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。

      ```
      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。

2. 使用以下命令配置 IPMI LAN 上串行 (SOL)：

   ```
   racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
   ```

   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。

   a. 使用以下命令更新 IPMI SOL 最低权限级别：

      ```
      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，要将 IPMI 权限配置为 2（用户），输入以下命令：

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
      ```

   注： 要重定向 LAN 上串行控制台，确保 SOL 波特率与受管服务器的波特率相同。

   b. 使用以下命令更新 IPMI SOL 波特率：

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <波特率>
      ```

      其中 <*波特率*> 为 19200、57600 或 115200 bps。

例如：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. 通过在命令提示符处键入以下命令启用 SOL。

注： 可以为每个用户启用或禁用 SOL。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable 1 -i <id>
```

其中 <*id*> 是用户的唯一 ID。

配置 PEF

可以配置希望 iDRAC6 对每个平台警报采取的措施。表 13-3 列出了可能的操作和在 RACADM 中标识的值。

表 13-3. 平台事件操作

操作	值
无操作	0
电源关闭	1
重新引导	2
关机后再开机	3

使用以下命令配置 PEF 操作：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <索引> <操作值>
```

其中，<*索引*> 是 PEF 索引（表 5-8），而 <*操作值*> 是来自表 13-3 的值。

例如，要使 PEF 能够在检测到处理器严重事件时重新引导系统并发送 IPMI 警报，输入以下命令：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
```

配置 PET

1. 使用以下命令启用全局警报：

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

2. 使用以下命令启用 PET：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <索引> <0|1>
```

其中 <*索引*> 是 PET 目标索引，而 0 或 1 分别禁用 PET 或启用 PET。

例如，要启用具有索引 4 的 PET，输入以下命令：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

3. 使用以下命令配置 PET 策略：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <索引> <IP-地址>
```

其中 <*索引*> 是 PET 目标索引，而 <*IP-地址*> 是接收平台事件警报的系统的目标 IP 地址。

4. 配置团体名称字符串。

在命令提示符下输入：

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名称>
```

其中 <*名称*> 是 PET 团体名称。

配置电子邮件警报

1. 输入以下命令启用全局警报：

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

2. 输入以下命令启用电子邮件警报：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <索引> <0|1>
   ```

   其中 <*索引*> 是电子邮件目标索引，0 禁用电子邮件警报，1 启用警报。电子邮件目标索引可以是 1 到 4 之间的一个值。

   例如，要启用具有索引 4 的电子邮件，输入以下命令：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. 通过输入以下命令配置电子邮件设置：

   ```
   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。

4. 要配置 SMTP 电子邮件服务器，输入以下命令：

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP 电子邮件服务器 IP 地址>
   ```

5. 要配置自定义信息，请输入以下命令：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <索引> <自定义信息>
   ```

   其中 <*索引*> 是电子邮件目标索引，而 <*自定义信息*> 是自定义信息。

6. 如果需要，通过输入以下命令检测配置的电子邮件警报：

   ```
   racadm testemail -i <索引>
   ```

   其中 <*索引*> 是要检测的电子邮件目标索引。

配置 IP 筛选（IP 范围）

IP 地址筛选（或 *IP 范围检查*）只允许从 IP 地址在用户指定范围内的客户端或管理工作站对 iDRAC6 进行访问。其它所有登录请求都会被拒绝。

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。如果结果相同，接入的登录请求就能够访问 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-IP-地址> ^ cfgRacTuneIpRangeAddr)
```

其中 & 是数量的按位"与"，而 ^ 是按位"异或"。

请参阅 Dell 支持网站 **support.dell.com/manuals** 提供的《*iDRAC6 管理员参考指南*》中的 cfgRacTuning，了解 cfgRacTuning 属性的完整列表。

表 13-4. 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。在高位包含此位样式的任何 IP 地址都允许登录。从此范围外的 IP 地址登录都会失败。各个属性的默认值允许 192.168.1.0 到 192.168.1.255 范围的地址登录。
cfgRacTuneIpRangeMask	定义 IP 地址中的高位位置。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。

以下是使用本地 RACADM 设置 IP 筛选的示例。

注： 请参阅"使用 RACADM 命令行界面"了解有关 RACADM 和 RACADM 命令的详情。

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

   ```
   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
   ```

2. 要将登录限制到一小组四个相邻 IP 地址（例如，192.168.0.212 到 192.168.0.215），则选择掩码中除最低的两个位以外的所有位，如下所示：

   ```
   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
   ```

   范围掩码的最后字节设置为 252，十进制数字为 11111100b。

IP 筛选原则

启用 IP 筛选时应遵循以下原则：

- 确保 **cfgRacTuneIpRangeMask** 以网络掩码的形式配置，所有的重要位为 1（定义掩码中的子网），在低位都变为 0。
- 使用所需范围的基地址作为 **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。

配置 IP 阻塞

IP 阻塞可动态确定来自特定 IP 地址的登录失败次数何时过多，并阻塞（或防止）该地址在预选的时间长度内登录 iDRAC6。

IP 阻塞功能包括：

- 允许的登录失败次数 (**cfgRacTuneIpBlkFailcount**)
- 按秒计的这些失败必须发生的时间范围 (**cfgRacTuneIpBlkFailWindow**)
- 被阻塞 IP 地址在超过允许失败次数后不能建立会话的时间（秒）(**cfgRacTuneIpBlkPenaltyTime**)

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"登记"。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）。

请参阅 Dell 支持网站 **support.dell.com/manuals** 提供的《*iDRAC6 管理员参考指南*》，了解 **cfgRacTune** 属性的完整列表。

表 13-5 列出了用户定义的参数。

表 13-5. 登录重试限制（IP 阻塞）属性

属性	定义
cfgRacTuneIpBlkEnable	启用 IP 阻塞功能。 如果在一段时间内 (**cfgRacTuneIpBlkFailWindow**) 一个 IP 地址出现连续的失败 (**cfgRacTuneIpBlkFailCount**)，则在一段时间内 (**cfgRacTuneIpBlkPenaltyTime)** 来自该地址的所有其它建立会话的尝试都会遭到拒绝。
cfgRacTuneIpBlkFailCount	设置拒绝某 IP 地址的登录尝试前允许的登录失败次数。
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时，将不会记入计数器。
cfgRacTuneIpBlkPenaltyTime	定义一个时间范围（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。

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，将在五分钟内阻止该客户端 IP 地址建立会话。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 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 cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

使用本地 RACADM 配置 iDRAC6 Telnet 和 SSH 服务

Telnet/SSH 控制台可以使用 RACADM 命令在本地配置（在受管服务器上）。

注： 必须具有**"Configure iDRAC"（配置 iDRAC6）**权限才能执行本节中的命令。

注： 在 iDRAC6 中重新配置 Telnet 或 SSH 设置时，任何当前会话都会终止而没有警告。

要从本地 RACADM 启用 Telnet 和 SSH，登录受管服务器并在命令提示符处输入以下命令：

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

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

要禁用 Telnet 或 SSH 服务，将值从 1 更改为 0：

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

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

输入以下命令更改 iDRAC6 上的 Telnet 端口号。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <新端口号>
```

例如，要将 Telnet 端口从默认 23 更改为 8022，输入此命令：

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

有关可用 RACADM CLI 命令的完整列表，请参阅"使用 RACADM 命令行界面"。

远程和 SSH/Telnet RACADM

远程 RACADM 是一种客户端公用程序，可用于从 Management Station 通过带外网络接口执行。提供了远程功能选项 (**-r**)，可以允许连接到 Managed System 和从远程控制台或 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。使用 SSH/Telnet RACADM 来从 SSH 或 Telnet 提示符下使用 RACADM 命令。

最大的并发远程 RACADM 会话数是 4。这些会话相互独立且与 Telnet 和 SSH 会话并存。iDRAC6 可以同时支持 4 个 SSH 会话和 4 个 Telnet 会话，以及 4 个 RACADM 会话。

注： 使用 RACADM 远程功能前请配置 iDRAC6 上的 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。

```
"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）

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.(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 not continuing execution of the command. (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）
```

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 sslcertdownload -t <类型> [-f <文件名>]
```

远程 RACADM 用法

```
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>
```

远程 RACADM 选项

表 13-6 列出远程 RACADM 命令的选项。

表 13-6. RACADM 命令选项

选项	说明
-r <*racIpAddr***>** **-r <***racIpAddr***>:<***端口号***>**	指定控制器的远程 IP 地址。 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。

使用 iDRAC6 配置文件

iDRAC6 配置文件是一个包含 iDRAC6 数据库值表示的文本文件。可以使用 RACADM **getconfig** 子命令生成包含 iDRAC6 当前值的配置文件。随后可以编辑该文件并使用 RACADM **config -f** 子命令将文件载入 iDRAC6，或将配置复制到其它 iDRAC6。

创建 iDRAC6 配置文件

配置文件是一个纯文本文件。可以使用任何有效的文件名；但 **.cfg** 文件扩展名是推荐的格式。

配置文件可以：

- 使用文本编辑器创建
- 使用 RACADM **getconfig** 子命令从 iDRAC6 获得
- 使用 RACADM **getconfig** 子命令从 iDRAC6 获得并随后编辑

要用 RACADM **getconfig** 命令获取配置文件，输入以下命令：

```
racadm -r <远程 iDRAC6 IP> -u <用户> -p <密码> getconfig -f myconfig.cfg
```

此命令在当前目录中创建文件 **myconfig.cfg**。

配置文件语法

注： 使用纯文本编辑器编辑配置文件，比如 Windows 上的**记事本**或 Linux 上的 **vi**。**racadm** 公用程序只分析 ASCII 文本。任何格式都会造成分析器混乱，并可能损坏 iDRAC6 数据库。

本节说明配置文件的格式。

- 以 # 开头的行是注释。

  注释*必须*从第一列开始。所有其它列中的 # 字符均视为正常 # 字符。

  示例：

  ```
  #
  # This is a comment (这是一条注释。)
  [cfgUserAdmin]
  cfgUserAdminPrivilege=4
  ```

- 组条目必须用 ***[*** 和 ***]*** 字符括起来。

  表示组名称的起始 ***[*** 字符*必须*从第一列开始。此组名称*必须*在该组中的任何对象之前指定。没有关联组名称的对象将导致错误。配置数据是根据 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》中的定义进行分组的。

  以下示例显示了组名称、对象以及对象的属性值。

  示例：

  ```
  [cfgLanNetworking]（组名称）
  cfgNicIpAddress=192.168.1.1（对象名称）
  ```

- 参数指定为*对象*=*值*对，在对象、= 和值之间不留空格。

  值后的空格将忽略。值字符串内的空格保持不变。= 右侧的所有字符都将保留原样（例如另一个=，或 #、*[*、*]* 等等）。

  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>
  ```

- 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
  ```

- 如果分析器遇到索引组，则将组的索引做为定位标记使用。该索引组内对象的任何修改项也与索引值相关联。

  例如：

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

- 该索引为只读，无法修改。索引组的对象被绑定到索引，在该索引下会列出这些对象，且该对象值的任何有效配置仅适用于该特定索引
- 各个索引组可使用一组预定义索引。要了解更多信息，请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的*《iDRAC 管理员参考指南》*。

修改配置文件中的 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：

```
#
# Object Group (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：

```
#

# Object Group (对象组) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (注释，此行的其余部分将被忽略)

cfgNicGateway=10.35.9.1
```

载入配置文件到 iDRAC6

命令 `racadm config -f <文件名>` 分析配置文件以验证有效组和对象名称存在并且遵守语法规则。如果文件没有任何错误，则该命令使用文件内容更新 iDRAC6 数据库。

注： 要只验证语法而不更新 iDRAC6 数据库，将 **-c** 选项添加到 **config** 子命令。

配置文件中的错误标记有行号以及一条简单的信息解释该问题。必须更正所有错误，然后才可以用配置文件更新 iDRAC6。

注： 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。

执行 `racadm config -f <文件名>` 命令前，可以运行 `racresetcfg` 子命令将 iDRAC6 重设为默认设置。确保要加载的配置文件包括所有需要的对象、用户、索引和其它参数。

要用配置文件更新 iDRAC6，执行以下命令：

```
racadm -r <远程 iDRAC6 IP> -u <用户> -p <密码> config -f myconfig.cfg
```

在命令完成后，可以执行 RACADM **getconfig** 子命令确定更新成功。

配置多个 iDRAC6

使用配置文件，可以用相同属性配置其它 iDRAC6。按照这些步骤配置多个 iDRAC6：

1. 从希望复制到其它设置的 iDRAC6 设置中创建配置文件。输入以下命令：

   ```
   racadm -r <远程 iDRAC6 IP> -u <用户> -p <密码> getconfig -f <文件名>
   ```

   其中 *<文件名>* 是保存 iDRAC6 属性的文件的名称，比如 **myconfig.cfg**。

   以下示例说明如何使用远程 RACADM 命令配置多个 iDRAC6。在 Management Station 上创建批处理文件并从批处理文件调用远程 racadm 命令。

   例如：

   ```
   racadm -r <服务器 IP 1> -u <用户> -p <密码> config -f myconfig.cfg

   racadm -r <服务器 IP 2> -u <用户> -p <密码> config -f myconfig.cfg

   ...
   ```

   有关详情，请参阅"创建 iDRAC6 配置文件"。

   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 iDRAC6 之前必须修改这些信息。

2. 编辑在上一步创建的配置文件，并删除或注释掉任何*不想*复制的设置。

3. 将编辑的配置文件复制到网络驱动器，要配置 iDRAC6 的各个受管服务器可以访问此文件。

4. 对于要配置的每个 iDRAC6：

   a. 登录受管服务器并启动命令提示符。

b. 如果要从默认设置重新配置 iDRAC6，输入以下命令：

```
racadm racreset
```

c. 用以下命令加载配置文件到 iDRAC6：

```
racadm -r <远程 iDRAC6 IP> -u <用户> -p <密码> config -f <文件名>
```

其中 <*文件名*> 是创建的配置文件的名称。如果文件不在工作目录中，还包括完整路径。

d. 通过输入以下命令重设已配置的 iDRAC6：

```
racadm reset
```

目录

目录

使用 WS-MAN 界面

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

Web Services for Management (WSCMAN) 是用于系统管理的基于简单对象访问协议 (SOAP) 的一种协议。WSCMAN 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 WSCMAN 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。用多个配置文件来组织管理 Dell 嵌入式服务器平台管理接口，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。

WS-MAN 的数据是由映射到 DMTF 配置文件和 Dell 扩展配置文件的 iDRAC6 工具接口提供的。

WS-Management 功能

WSCManagement 规范促进了管理应用程序和所管理资源间的互操作性。通过确定一组核心的 Web 服务规范和使用要求来提供对与所有系统管理都非常重要的通用操作，WSCManagement 能够：

- 查找并浏览管理资源
- 获取、设置、创建和删除各个管理资源，比如设置和动态值
- 枚举容器和集合中的内容，比如大型表和日志
- 执行特定管理方法，带有强制输入和输出参数

支持的 CIM 配置文件

表 16-1. 支持的 CIM 配置文件

标准 DMTF
1. 基础服务器 定义表示主机服务器的 CIM 类。
2. 基础度量 定义提供用于构建和控制受管元素度量的 CIM 类。
3. 服务处理器 定义用于构建服务处理器的 CIM 类。
4. USB 重定向 定义用于描述关于 USB 重定向的信息的 CIM 类。对于键盘、视频和鼠标设备，如果要作为 USB 设备来管理，则应使用此配置文件。
5. 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及其组件的 FRU 信息以及物理拓扑。
6. 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。
7. 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。
8. 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。
9. IP 界面 定义表示 Managed System IP 接口的 CIM 类。
10. DHCP 客户端 定义表示 DHCP 客户端及其相关功能和配置的 CIM 类。
11. DNS 客户端 定义表示 Managed System 中 DNS 客户端的 CIM 类。
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. 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。

14. SMASH 集合
定义表示 CLP 配置的 CIM 类。iDRAC6 使用此配置文件自行实施 CLP。

15. 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。

16. 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。

17. 以太网端口
定义表示 Managed System 中以太网端口、相关控制器和以太网接口的 CIM 类。端口物理方面关联以及配置文件实施版本信息在此配置文件中构建。

18. 传感器
定义用于描述受管系统中传感器的 CIM 类。还可以定义描述传感器与受监控设备之间关系的关联类。

Dell 扩展

1. Active Directory 客户端
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. 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. 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。

4. 软件资源清册
定义 CIM 和 Dell 扩展，用于表示当前已安装的 BIOS、组件固件、诊断、Unified Server Configurator 和驱动程序包版本。此外，还可表示"Lifecycle Controller"（生命周期控制器）中的 BIOS 版本和可用固件升级映像，以用于回滚和重新安装。

5. 软件更新
定义 CIM 和 Dell 扩展，用于表示更新 BIOS、诊断、驱动程序包、组件和生命周期控制器固件的服务类和方法。更新方法支持从 CIFS、NFS、FTP 和 HTTP 网络共享位置和从生命周期控制器中的更新映像进行更新。更新请求用作业来表示，可以立即预定或稍后选择一种重新引导操作来应用更新。

6. 作业控制
定义 CIM 和 Dell 扩展，用于管理由更新请求生成的作业。可以创建、删除、修改作业，以及将作业合并到作业队列中，并在一次重新引导时执行多个更新。

7. LC 管理
定义 CIM 和 Dell 扩展，用于获取和设置管理自动发现和部件更换生命周期控制器功能的属性。

8. 永久存储
定义用于管理 Dell 平台的虚拟闪速更新介质分区的 CIM 和 Dell 扩展类。

9. 简单 NIC
定义代表 NIC 网络控制器配置的 CIM 和 Dell 扩展类。

10. BIOS 和引导管理
定义代表 Dell BIOS 属性及配置主机引导顺序的 CIM 和 Dell 扩展类。

11. 简单 RAID
定义代表主机 RAID 存储配置的 CIM 和 Dell 扩展类。

12. iDRAC 卡
定义代表 iDRAC6 资源清册信息的 CIM 和 Dell 扩展类。

13. 内存
定义代表主机 DIMM 资源清册信息的 CIM 和 Dell 扩展类。

14. CPU
定义代表主机 CPU 资源清册信息的 CIM 和 Dell 扩展类。

15. 系统信息
定义代表主机平台资源清册信息的 CIM 和 Dell 扩展类。

16. PCI 设备
定义代表主机 PCI 设备资源清册信息的 CIM 和 Dell 扩展类。

17. 显卡
定义代表主机视频卡资源清册信息的 CIM 和 Dell 扩展类。

iDRAC6 WSCMAN 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。可以通过利用客户端基础架构来使用 Web 服务接口，比如 Windows WinRM 和 Powershell CLI，诸如 WSMANCLI 等开放源公用程序，以及应用程序编程环境诸如 Microsoft .NET。

还有更多实施指南、白皮书、配置文件、MOF 和代码示例可从 Dell Enterprise Technology Center **www.delltechcenter.com** 获得。有关详情，另请参阅以下内容：

- DMTF 网址：**www.dmtf.org/standards/profiles/**
- WSCMAN 发行说明或自述文件。

目录

目录

使用 iDRAC6 Enterprise SM-CLP 命令行界面

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

本节提供了有关 iDRAC6 中服务器管理工作组 (SMWG) 服务器管理命令行协议 (SM-CLP) 的信息。

注： 本节假定您熟悉服务器硬件系统管理体系结 (SMASH) 标准和 SMWG SM-CLP 规范。有关这些规范的详情，请参阅分布式管理任务小组 (DMTF) 网站 **www.dmtf.org**。

iDRAC6 SM-CLP 是由 DMTF 和 SMWG 推动的一项协议，提供了系统管理 CLI 实施的标准。定义的 SMASH 体系结构做了很多工作，旨在为更多标准系统管理组件建立基础。SMWG SM-CLP 是 DMTF 推动的整个 SMASH 工作中的一部分。

SM-CLP 提供了本地 RACADM 命令行界面的一部分功能，只不过访问路径不同。SM-CLP 在 iDRAC6 中执行，而 RACADM 在受管服务器上执行。另外，RACADM 是一种 Dell 专用界面，而 SM-CLP 是业界标准界面。

注： 有关 iDRAC6 SMCCLP 属性数据库、WS-MAN 类和 SMCCLP 目标间映射以及 Dell 实施细节的信息，请参阅 *iDRAC6 CIM 元素映射*和 *iDRAC6 SM-CLP 属性数据库*说明文件，这些说明文件可从 Dell Enterprise Technology Center **www.delltechcenter.com** 获得。在 DMTF 配置文件及 Dell 扩展配置文件中指明了《*iDRAC6 CIM 组件映射*》文档中包含的信息。WSMAN 结构在 **http://www.dmtf.org/standards/profiles/** 上的 DMTF 配置文件和 MOF 中说明。另外，Dell 扩展可从 **http://www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions** 获得。

使用 SM-CLP 进行系统管理

iDRAC6 SM-CLP 使用户能够从命令行管理以下系统功能：

- 服务器电源管理 — 打开、关闭或重新引导系统
- 系统事件日志 (SEL) 管理 — 显示或清除 SEL 记录
- iDRAC6 用户帐户管理
- Active Directory 配置
- iDRAC6 LAN 配置
- SSL 证书签名请求 (CSR) 生成
- 虚拟介质配置

---

iDRAC6 SM-CLP 支持

SM-CLP 承载在 iDRAC6 固件中并支持 Telnet 和 SSH 连接。iDRAC6 SM-CLP 界面基于由 DMTF 组织提供的 SM-CLP 规范版本 1.0。

以下各节提供了 iDRAC6 上 SM-CLP 功能的概览。

注： 如果通过 Telnet/SSH 建立了 SMCCLP 会话，并且此会话由于网络连接断开而未能成功关闭，将会显示消息指出已达到最大连接数。要解决此问题，在 Web GUI **"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Network/Security"（网络/安全）→"Sessions"（会话）**下终止 SMCCLP 会话，然后再尝试建立新会话。

注： iDRAC6 支持同时多达 4 个 Telnet 会话和 4 个 SSH 会话。不过，8 个会话中只有一个可以使用 SM-CLP。即，iDRAC6 一次只支持一个 SM-CLP 会话。

如何启动 SMCCLP 会话

- 通过 SSH/Telnet 连接到 iDRAC6，会转至 CLI（控制台）。
- 在美元符号提示符处输入"smclp"启动 SMCCLP 控制台。

语法：

```
telnet <iDRAC6-ip-地址>

$（the CLI prompt is displayed（显示 CLI 提示符））
```

$smclp（at the CLI prompt, type (在 CLI 提示符中，键入) smclp）

SM-CLP 功能

SM-CLP 规范提供了一组常用标准 SM-CLP verb，可通过 CLI 用于简单系统管理。

SM-CLP 提供了 verb 的概念，并旨在通过 CLI 提供系统配置功能。verb 表示要执行的操作，而目标为执行操作的实体（或对象）。

以下是 SM-CLP 命令行的语法：

<verb> [<选项>] [<目标>] [<属性>]

表 15-1 提供了 iDRAC6 CLI 支持的 verb 的列表，各个命令的语法，以及 verb 支持的选项列表。

表 15-1. 支持的 SM-CLP CLI Verb

Verb	说明	"Options"（选项）
cd	使用 shell 导航 Managed System 地址空间。 语法： cd [*选项*] [*目标*]	-default, -examine, -help, -output, -version
delete	删除对象实例。 语法： delete [*选项*] [*目标*]	-examine, -help, -output, -version
exit	从 SM-CLP shell 会话退出。 语法： exit [*选项*]	-help, -output, -version
help	显示 SM-CLP 命令帮助。 help	-examine, -help, -output, -version
reset	重设目标。 语法： reset [*选项*] [*目标*]	-examine, -help, -output, -version
set	设置目标属性 语法： set [*选项*] [*目标*] <*属性名称*>=<*值*>	-examine, -help, -output, -version
show	显示目标属性、verb 和子目标。 语法： show [*选项*] [*目标*] <*属性名称*>=<*值*>	-all, -default, -display, -examine, -help, -level, -output, -version
start	启动目标。 语法： start [*选项*] [*目标*]	-examine, -force, -help, -output, -version
stop	关闭目标。 语法： stop [*选项*] [*目标*]	-examine, -force, -help, -output, -version, -wait
version	显示目标的版本属性。 语法： version [*选项*]	-examine, -help, -output, -version

表 15-2 说明 SM-CLP 选项。有些选项有简写格式，如表中所示。

表 15-2. 支持的 SM-CLP 选项

SM-CLP 选项	说明
-all, -a	指示 verb 执行所有可能的功能。
-destination	在 dump 命令中指定存储映像的位置。 语法： -destination <URI>
-display, -d	筛选命令输出。 语法： -display <属性 | 目标 | verb>[, <属性 | 目标 | verb>]*
-examine, -x	指示命令处理器在不执行命令的情况下验证命令语法。
-force, -f	如无法正常关闭，请使用该选项对目标系统执行强制关机。 语法： stop -force <目标>
-help, -h	显示 verb 帮助。
-level, -l	指示 verb 处理在指定目标下面的附加级别的目标。 语法： -level <*n* | all>
-output, -o	指定输出的格式。 语法： -output format=<text | clpcsv | keyword | clpxml> 或 -o format=<text | clpcsv | keyword | clpxml>
-version, -v	显示 SMCCLP 版本号。

导航 MAP 地址空间

注： 斜杠 (/) 和反斜杠 (\) 在 SM-CLP 地址路径中可以互换。不过，命令行末尾的反斜杠会使命令在下一行继续并在命令分析中忽略。

可以使用 SM-CLP 管理的对象由称为可管理性访问点 (MAP) 地址层次空间排列的目标表示。地址路径指定从地址空间根到对象的路径。

根目标由斜杠 (/) 或反斜杠 (\) 表示。这是登录 iDRAC6 时的默认起始点。使用 cd verb 从根向下导航。

例如，要导航到系统事件日志 (SEL) 中的第三个记录，输入以下命令：

```
->cd /admin1/system1/logs1/log1/record3
```

输入不带目标的 cd verb 以查找在地址空间中的当前位置。..和 .缩写的作用与在 Windows 以及 Linux 中相同：..指父级，而 .指当前级。

目标

有关通过 SM-CLP 可用目标的列表，请参阅 SMCCLP 映射说明文件，该说明文件可从 Dell Enterprise Technology Center **www.delltechcenter.com** 获得。

使用 Show Verb

要了解有关目标的详情，请使用 show verb。此 verb 显示目标的属性、子目标、关联和该位置允许的 SM-CLP verb 的列表。

使用 -display 选项

show -display 选项允许限制命令的输出为一个或多个属性、目标、关联和 verb。例如，要只显示当前位置的属性和目标，使用以下命令：

```
show - 显示属性、目标
```

要只列出某些属性，按以下命令予以限定：

```
show -d properties=(userid,name) /admin1/system1/sp1/oemdcim_mfaaccount1
```

如果只想显示一个属性，可以省略括号。

使用 -level 选项

show -level 选项在指定目标以下的级别执行 **show**。要查看地址空间中的所有目标和属性，使用 **-l all** 选项。

使用 -output 选项

-output 选项指定 SM-CLP verb 输出的四种格式之一：**text**、**clpcsv**、**keyword** 和 **clpxml**。

默认格式为 **text**，是最可读的输出。**clpcsv** 格式是逗号分隔值格式，适合于载入电子表格程序。**keyword** 格式以每行关键字=值对列表输出信息。**clpxml** 格式是 XML 文档，包含 **response**XML 元素。DMTF 指定了 **clpcsv** 和 **clpxml** 格式，其规范可以在 DMTF 网站 **www.dmtf.org** 找到。

以下示例显示了如何以 XML 输出 SEL 内容：

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

---

iDRAC6 SM-CLP 示例

以下小节通过示例介绍如何使用 SSH 界面登录 iDRAC6 以及启动 SM-CLP 会话执行以下操作：

- 服务器电源管理
- SEL 管理
- 映射目标导航
- 显示系统属性

服务器电源管理

表 15-3 提供了使用 SM-CLP 在受管服务器上执行电源管理操作的示例。

输入"smclp"启动 SM-CLP 控制台。

表 15-3. 服务器电源管理操作

操作	语法
使用 SSH 界面登录到 iDRAC6	>ssh 192.168.0.120 >login: root >password: 输入"smclp"启动 SMCCLP 控制台。
关闭服务器的电源	->stop /admin1/system1 system1 successfully stopped
将服务器从电源关闭状态打开	->start /admin1/system1 system1 successfully started
重新引导服务器	->reset /admin1/system1 RESET successful for system1

SEL 管理

表 15-4 提供了使用 SM-CLP 在 Managed System 上执行 SEL 相关操作的示例。

映射目标导航

表 15-4. SEL 管理操作

操作	语法

查看 SEL	->show -d targets,properties,verbs /admin1/system1/logs1/log1 **可能返回：** Targets: record1/ record2/... Properties: OverwritePolicy=7 LogState=4 CurrentNumberOfRecords=60 MaxNumberOfRecords=512 ElementName=Record Log 1 HealthState=5 EnabledState=2 RequestedState=12 EnabledDefault=2 TransitioningToState=12 InstanceID=DCIM: SEL Log OperationalStatus={2} Verb: show exit version cd help
查看 SEL 记录	->show /admin1/system1/logs1/log1/record4 **可能返回：** ufip=/admin1/system1/logs1/log1/record4 Associations:LogManagesRecord=>/admin1/system1/logs1/log1 Properties: RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255* RecordFormat=*IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*IPMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI_GeneratorID*IPMI_EvMRev*IPMI_Se Description=:0:Assert:OEM specific ElementName=DCIM System Event Log Entry InstanceID=DCIM:SEL LOG:4 LogInstanceID=idrac:Unknown:Unknown SEL Log LogName=DCIM System Event Log Entry RecordID=DCIM:SEL LOG:4 CreationTimeStamp=20090616114341.000000+000
	Verb: show exit version cd help delete
清除 SEL	->delete /admin1/system1/logs1/log1/record* **返回：** Records deleted successfully.(记录删除成功。)

表 15-5 提供了使用 **cd** verb 导航映射的示例。在所有示例中，假定初始的默认目标为 /。

表 15-5. 映射目标导航操作

操作	语法
导航到系统目标并重新引导	->cd admin1/system1 ->reset **注：** 当前默认目标为 **/**。
导航到 SEL 目标并显示日志记录	->cd admin1 ->cd system1 ->cd logs1 ->cd log1 ->show **相当于** ->cd admin1/system1/logs1/log1 ->show
显示当前目标	->cd .
上移一级	->cd ..
退出 shell	->exit

目录

目录

使用 iVM-CLI 部署操作系统

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

集成虚拟介质命令行界面 (iVM-CLI) 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 iVM-CLI 和脚本化方法，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 iVM-CLI 公用程序集成到公司网络的信息。

开始之前

开始使用 iVM-CLI 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 在各远程系统中配置。

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 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，打开命令提示符并输入以下命令：

```
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 Microsoft 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：

   - 执行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。

- 请执行以下过程之一：
  - 将 **IPMItool** 和虚拟介质命令行界面 (iVM-CLI) 集成到现有操作系统部署应用程序。使用示例 **ivmdeploy** 脚本作为使用公用程序的指南。
  - 使用现有 **ivmdeploy** 脚本部署操作系统。

注： **ivmdeploy** 内部使用 **iVMCLI** 和 **ipmitool**。应具有*"IPMI over LAN"（LAN 上 IPMI）*权限才能使用此工具。另外，使用 **ivmdeploy** 脚本时，虚拟介质应处于连接状态。

部署操作系统

使用 iVM-CLI 公用程序和该公用程序包含的 **ivmdeploy** 脚本将操作系统部署到远程系统。

开始之前，应查看 iVM-CLI 公用程序包含的示例 **ivmdeploy** 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 IP 地址，每行一个 IP 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 **ivmdeploy**。

要运行 ivmdeploy 脚本，在命令提示符处输入以下命令：

```
ivmdeploy -r ip.txt -u <idrac-用户> -p <idrac-密码> -c {<iso9660-映像> | <路径>}
```

其中

- <*idrac-用户*> 是 iDRAC6 用户名 - 例如，**root**
- <*idrac-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
- <*路径*> 是包含操作系统安装 CD 或 DVD 的设备路径

ivmdeploy 脚本将其命令行选项传递给 **iVMCLI** 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 **iVMCLI -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 IP 地址并每行运行 **iVMCLI** 公用程序一次。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 **iVMCLI** 公用程序中的说明运行。

ivmdeploy 脚本只支持从 CD/DVD 或 CD/DVD ISO9660 映像安装。如果需要从软盘或软盘映像安装，可以修改脚本以使用 **iVMCLI -f** 选项。

使用虚拟介质命令行界面公用程序

虚拟介质命令行界面 (iVM-CLI) 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。

iVMCLI 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 iVMCLI 命令行公用程序时使用交互标志"-i"选项。这样可保护用户名和密码隐私，确保更高的安全性。因为在许多 Windows 和 Linux 操作系统上，当其他用户检查进程时，用户名和密码以明文形式可见。

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 iVM-CLI 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来运行 iVM-CLI 公用程序。

对于 Linux 系统，可以使用 **sudo** 命令访问 iVM-CLI 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 iVM-CLI 组中的用户，管理员使用 **visudo** 命令。无管理员权限的用户可将 **sudo** 命令添加为 iVMCLI 命令行（或 iVMCLI 脚本）的前缀以获得对远程系统中 iDRAC6 的访问和运行公用程序。

安装 iVMCLI 公用程序

iVM-CLI 公用程序位于 *Dell Systems Management Tools and Documentation DVD* 上，该 DVD 随 Dell OpenManage System Management 软件包提供。要安装该公用程序，请将 *DVD* 插入您的系统并按屏幕说明操作。

Dell Systems Management Tools and Documentation DVD 包含最新系统管理软件产品，包括诊断、存储管理、远程访问服务和 RACADM 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 还包含 **ivmdeploy** - 演示如何使用 iVM-CLI 和 RACADM 公用程序将软件部署到多个远程系统的示例脚本。

注： ivmdeploy 脚本依赖于安装时目录中的其它文件。如果想从另一个目录使用脚本，随之复制所有的文件。

命令行选项

iVM-CLI 界面在 Windows 和 Linux 系统上相同。公用程序使用的选项与 RACADM 公用程序选项一致。例如，指定 iDRAC6 IP 地址的选项采用的语法对于 RACADM 和 iVMCLI 公用程序都一样。

iVMCLI 命令格式如下：

`iVMCLI [参数] [操作_系统_shell_选项]`

命令行语法区分大小写。有关详情，请参阅"iVMCLI 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：

- iVMCLI 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。

注： 使用 iVMCLI 命令时，如参数值在词与词之间有空格，则必须使用引号将完整的参数值括起来。例如，以将系统中的 DVD 映像附加至服务器操作系统的命令为例：
F:\idrac>ivmcli -r 10.35.155.117 -u root -p calvin -c c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso

其中 -c 是参数之一，**c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso** 是参数值，其中的"documents and settings"和"my documents"含有空格。因此，要为完整的映像文件路径使用引号。如不使用引号，该命令将无效。下列命令也是无效的：

C:\"documents and settings"\.....

iVMCLI 参数

iDRAC6 IP 地址

`-r <iDRAC IP 地址>[:<iDRAC SSL 端口>]`

此参数提供 iDRAC6 IP 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 IP 地址或 DDNS 名称，将显示错误信息并终止命令。

<iDRAC IP 地址> 是有效、唯一的 IP 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 用户名>`

此参数提供将运行虚拟介质的 iDRAC6 用户名。

<iDRAC 用户名> 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，错误信息将会显示并且命令会终止。

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，错误信息将会显示并且命令会终止。

软盘/磁盘设备或映像文件

`-f {<设备名称> | <映像文件>}`

其中 *<设备名称>* 是有效驱动器号（对于 Windows 系统）或有效设备文件名，在适用的情况下包括可安装文件系统分区号（对于 Linux 系统）；*<映像文件>* 是有效映像文件的文件名和路径。

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 (`设备第 4 分区 `/dev/sdb)`（Linux 系统）

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:\`（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，将会列出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。

Root CA 证书验证

`-S`

该参数用来表示 iDRAC CA 证书是否有效。如证书无效，iVMCLI 会话终止，并显示一条错误消息表示该证书无效。如该证书有效，将建立 iVMCLI 会话。

版本显示

-v

此参数用于显示 iVM-CLI 公用程序版本。如果没有提供其它非开关选项，此命令将会不显示错信息就终止。

帮助显示

-h

此参数显示 iVM-CLI 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。

手动显示

-m

此参数显示 iVM-CLI 公用程序的详细"man 页"，包括所有可能选项的说明。

加密的数据

-e

如果命令行中包括此参数，iVMCLI 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。

iVMCLI 操作系统 Shell 选项

iVM-CLI 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 iVMCLI 公用程序打印的输出覆盖指定的文件。

  注： iVMCLI 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，iVMCLI 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 iVMCLI 命令启动新进程后继续执行（否则，脚本将保持阻塞直至 iVMCLI 程序终止）。当有多个 iVMCLI 实例以这种方式启动，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。

iVMCLI 返回代码

0 = 无错误

1 = 无法连接

2 = iVMCLI 命令行错误

3 = RAC 固件连接已删除

每当遇到错误时，文本信息（仅有英文）也会发送到标准错误输出。

目录

目录

使用 iDRAC6 配置公用程序

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

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 Managed System 的参数。具体说来，可以：

- 查看 iDRAC6 和主背板固件的固件版本号
- 配置、启用或禁用 iDRAC6 局域网 (LAN)
- 启用或禁用 LAN 上 IPMI
- 配置 LAN 参数
- 启用、禁用或取消系统服务
- 启用或禁用"Auto-Discovery"（自动发现）并配置预配置服务器
- 附加或分离虚拟介质设备
- 启用或禁用 vFlash
- 启用或禁用智能卡登录和单一登录
- 配置系统服务
- 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

可以使用 iDRAC6 配置公用程序执行的任务还可以用 iDRAC6 或 Dell OpenManage 软件提供的其它公用程序执行，包括 Web 界面、SM-CLP 命令行界面、本地和远程 RACADM 命令行界面，以及基本网络配置情况下在初始 iDRAC6 配置期间的 iDRAC6 LCD。

启动 iDRAC6 配置公用程序

必须使用 iDRAC6 虚拟控制台连接的控制台在最初或在重设 iDRAC6 为默认设置后访问 iDRAC6 配置公用程序。

1. 在连接到 iDRAC6 虚拟控制台的键盘上，按 <Print Screen> 显示 iDRAC6 **虚拟控制台的"On Screen Configuration and Reporting (OSCAR)"（屏幕配置和报告 [OSCAR]）**菜单。使用 <上箭头> 和 <下箭头> 高亮度显示包含服务器的插槽，然后按 <Enter>。
2. 通过按服务器正面的电源按钮打开或重新启动服务器。
3. 在看到信息"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.....）时，立即按 <Ctrl><E>。此时将显示 iDRAC6 配置公用程序。

注： 如果操作系统在您按 <Ctrl><E> 之前已开始载入，请让系统完成引导，然后重新启动服务器并重试。

配置公用程序的前两行提供关于 iDRAC6 固件和主背板固件修订的信息。在确定是否需要升级固件时，版本级别很有用。

iDRAC6 固件是固件中与外部界面相关的部分，比如 SM-CLP 和 Web 界面。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

在固件修订信息下面，iDRAC6 配置公用程序的其余部分是可以用上箭头和下箭头键访问的菜单项。

- 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，会显示为蓝色。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、右箭头和空格键选择**"On"（开）**和**"Off"（关）**。

在默认配置中，iDRAC6 LAN 已禁用。必须启用 LAN 来允许使用 iDRAC6 功能，比如 Web 界面、Telnet/SSH 访问 SM-CLP 命令行界面、虚拟控制台和虚拟介质。

如果选择禁用 LAN，将会显示以下警告：

`iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.`（如果 LAN 信道关闭，iDRAC 带外界面将会禁用。）

该信息告诉您，除了直接连接 iDRAC6 HTTP、HTTPS、Telnet 或 SSH 端口可以访问的功能外，带外管理网络通信量，比如从 Management Station 发送到 iDRAC6 的 IPMI 信息，在 LAN 禁用时也不会收到。本地 RACADM 界面仍然可用，可用来重新配置 iDRAC6 LAN。

按任意键清除信息并继续。

LAN 上 IPMI

按左箭头、右箭头和空格键选择**"On"（开）**和**"Off"（关）**。如果选择**"Off"（关）**，iDRAC6 将不会通过 LAN 界面接收 IPMI 信息。

如果选择**"Off"（关）**，将会显示警告信息。

按任意键清除信息并继续。有关此信息的说明，请参阅"iDRAC6 LAN"。

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 18-1. LAN 参数

项目	说明
常见设置	
"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）	显示**"On"（开）/"Off"（关）**。选择**"On"（开）**会启用 iDRAC6 的虚拟 LAN 过滤。
VLAN ID	显示 1-4094 之间的任何 VLAN ID 值。
VLAN	显示 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。 默认值为已启用。
"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。
"IP Address Source"（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**。
Subnet Mask（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。
IPv6 设置	
IPv6	启用或禁用对 IPv6 连接的支持。
"IPv6 Address Source"（IPv6 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 Address 1"（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。
"Prefix Length"（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 2-15	这是 iDRAC6 网络接口的不可编辑的 **IPv6 地址 2...IPv6 地址 15**。
"DNS Servers from DHCPv6"（从 DHCPv6 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。

"Virtual Media Configuration"（虚拟介质配置）

虚拟介质

使用左箭头和右箭头键来选择**"Auto-Attached"（自动附加）**、**"Attached"（附加）**或**"Detached"（分离）**。

- 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。
- 如果选择**"Auto-Attached"（自动附加）**，虚拟介质设备会在虚拟介质会话启动时自动附加到服务器。

注： 要使用具有虚拟介质功能的 USB 闪存盘，BIOS 设置公用程序中的**"USB Flash Drive Emulation Type"（USB 闪存盘仿真类型）**必须设置为**"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 闪存盘仿真类型）**设置为**"Auto"（自动）**，闪存盘将显示为系统软盘驱动器。

vFlash

使用左箭头和右箭头键选择**"Enabled"（已启用）**或**"Disabled"（已禁用）**。

- **"Enabled"（已启用）** - 可对 vFlash 进行分区管理。
- **"Disabled"（已禁用）** - 不可对 vFlash 进行分区管理。

小心： 如一个或多个分区正在使用中或被附加，则无法禁用 vFlash。

"Initialize vFlash"（初始化 vFlash）

选择该选项初始化 vFlash 卡。初始化操作会删除 SD 卡中现有数据，并会删除所有现有分区。如一个或多个分区正在使用中或被附加，则无法执行初始化操作。仅当 iDRAC Enterprise 卡槽中的卡超过 256 MB 且启用了 vFlash 时，该选项才可用。

按 <Enter> 初始化 vFlash SD 卡。

由于以下原因导致初始化操作可能失败：

- 当前不存在 SD 卡。
- 当前另一进程正在使用 vFlash。
- 未启用 vFlash。
- SD 卡受写保护。
- 一个或多个分区当前正在使用中。
- 当前附加有一个或多个分区。

"vFlash Properties"（vFlash 属性）

按 <Enter> 查看下列 vFlash SD 卡属性：

- **"Name"（名称）** - 显示插入服务器 vFlash SD 卡槽的 vFlash SD 卡的名称。如是 Dell SD 卡，则显示为 vFlash SD 卡。如是非 Dell SD 卡，则显示为 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 卡中未使用的空间。此空间可用于在 vFlash SD 卡上创建更多分区。对于 SD 卡而言，可用空间显示为 256MB。
- **"Write Protected"（写保护）** - 显示 vFlash SD 卡是否为写保护状态。
- **"Health"（运行状况）** - 显示 vFlash SD 卡的整体运行状况。分为：
  - OK（良好）
  - Warning（警告）
  - Critical（严重）

按 <Esc> 键退出。

Smart Card / SSO

此选项配置 **"Smart Card Logon"（智能卡登录）**和**"Single Sign-on"（单一登录）** 功能。可用的选项有**"Enabled"（已启用）**和**"Disabled"（已禁用）**。

注： 如果启用**"Single Sign-on"（单一登录）**功能，则禁用**"Smart Card Logon"（智能卡登录）**功能。

系统服务

系统服务

使用左箭头和右箭头键选择**"Enabled"（已启用）**或**"Disabled"（已禁用）**。如果已启用，某些 iDRAC6 功能可通过 Lifecycle Controller 配置。有关详情，请参阅 Dell 支持网站 **support.dell.com / manuals** 上的*《Lifecycle Controller 用户指南》*。

注： 修改此选项会在您**"Save"（保存）**和**"Exit"（退出）**以应用新设置时重新启动服务器。

取消系统服务

使用上箭头和下箭头键选择**"Yes"（是）**或**"No"（否）**。

在选择**"Yes"（是）**时，所有 Lifecycle Controller 会话都会关闭，且服务器在您**"Save"（保存）**和**"Exit"（退出）**以应用新设置时重新启动。

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 *support.dell.com/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 配置公用程序退出时重新启动服务器。

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。

表 18-2. LAN 用户配置屏幕

项目	说明
自动查找	自动发现功能允许在网络上自动发现未配置的系统；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发现过程中指定的凭据建立与 iDRAC6 的 WSMAN 通信，并随后发送安全指令给 iDRAC6 来远程部署操作系统。 有关远程操作系统部署的信息，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的*《Dell Lifecycle Controller 用户指南》*。 *手动启用自动发现前*，应在独立的 **iDRAC6 配置公用程序**会话中执行以下必要操作： • 启用 NIC（刀片服务器） • 启用 IPv4（刀片服务器） • 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）**可启用自动发现功能。默认情况下，此选项为**"Disabled"（禁用）**。如果订购了**已启用**自动发现功能的 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"（自动发现） *（续...）*	添加 Dell 系统到网络并使用自动发现功能前，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。
预配置服务器	此字段用于配置预配置服务器。预配置服务器地址可以是 IPv4 地址或主机名的组合，并且不应超过 255 个字符。每个主机名地址使用逗号分隔。 如果启用了自动发现功能，在自动发现过程成功完成后，可从已配置的预配置服务器检索用户凭据，以便进行以后的远程预配置。 有关详情，请参阅 Dell 支持网站 **support.dell.com/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。当自动发现已启用时，选择**"Disabled"（禁用）**可禁用管理员帐户。
"IPMI LAN Privilege"（IPMI LAN 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）	输入管理员帐户的新密码。输入时字符不会显示出来。
"Confirm Password"（确认密码）	重新输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。

"Reset To Default"（重设为默认值）

使用**"Reset To Default"（重设为默认值）**菜单项可将所有 iDRAC6 配置项重设为工厂默认值。如果忘记了管理用户密码或者想从默认设置重新配置 iDRAC6，可能需要这样做。

注： 在默认配置中，iDRAC6 网络已禁用。直到在 iDRAC6 配置公用程序中启用了 iDRAC6 网络之后，才能在网络上重新配置 iDRAC6。

按 <Enter> 以选择项目。以下警告信息会出现：

"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 (Cancel)"（否（取消））>

< "YES (Continue)"（是（继续））>

要将 iDRAC6 重设为默认值，请选择**"YES"（是）**并按 <Enter>。

如该操作失败，则会显示以下任意错误消息：

- 重设命令不成功。请稍候再试 - iDRAC 正忙。
- 恢复设置为默认值失败 - 超时。
- 无法发送重设命令。请稍候再试 - iDRAC 正忙。

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>。要导航：

- 使用左箭头键移动到上一条（较旧）信息，使用右箭头键移动到下一条（较新）信息。
- 输入特定记录号跳到该记录。

按 <Esc> 退出系统事件日志。

注： 只能在 iDRAC6 配置公用程序或 iDRAC6 Web 界面中清除 SEL。

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。如该操作失败，则显示以下消息之一：
  - iDRAC6 Communication Failure—isplayed if iDRAC is not accessible. (iDRAC6 通信故障—无法访问 iDRAC 时显示)。
  - Some of the settings cannot be applied—isplayed when few settings cannot be applied. (无法应用某些设置—无法应用某些设置时显示)。
- 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。

目录

目录

对 Managed System 进行恢复和故障排除

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers 版本 3.0 用户指南

本节介绍如何使用 iDRAC6 公用程序执行与诊断和排除远程 Managed System 故障相关的任务。包含以下小节：

- 故障提示 — 帮助查找可以有助诊断问题的信息和其它系统提示
- 问题解决工具 — 说明可以用于排除系统故障的 iDRAC6 工具
- 故障排除和常见问题 — 有关可能遇到的常见问题的答案

安全第一 您以及系统

要执行本节中的某些过程，必须是在维护机箱、Dell PowerEdge 系统或其它硬件模块。不要尝试维修本指南以及系统说明文件介绍之外的系统硬件。

△ **小心： 多数维修只能由经认证的维修技术人员进行。用户只能执行产品说明文件中授权的故障排除和简单维修工作或按照联机或电话服务和支持团队的指示操作。未经 Dell 授权的维修所造成的损坏不在保修范围之内。请阅读并遵循产品附带的安全说明。**

故障指示灯

本节介绍可能预示系统出现问题的提示。

LED 指示灯

机箱上或机箱中所安装组件上的 LED 一般是系统故障的第一指示器。以下组件和模块具有状态 LED：

- 机箱 LCD 显示
- 服务器
- 风扇
- CMC
- I/O 模块
- 电源设备

机箱 LCD 上单一的 LED 汇总了系统中所有组件的状况。LCD 上的稳定蓝色 LED 表示系统中没有检测到错误状况。LCD 上闪烁的琥珀色 LED 表示检测到一个或多个错误状况。

如果机箱 LCD 有闪烁的琥珀色 LED，可以使用 LCD 菜单找出发生错误的组件。请参阅《*Dell Chassis Management Controller Firmware 用户指南*》获得 LCD 使用帮助。

表 19-1 说明了 Dell PowerEdge 系统上 LED 的含义：

表 19-1. 刀片 服务器 LED 指示灯

LED 指示灯	含义
稳定绿色（*仅用于电源按钮*）	服务器开机。没有绿色 LED 表示服务器没有开机。
稳定蓝色	iDRAC6 运行正常。
闪烁琥珀色	iDRAC6 检测到错误状况或正在更新固件。
闪烁蓝色	用户已激活此服务器的定位 ID。

硬件故障指示灯

提示模块有硬件问题，包括以下：

- 未能通电

- 风扇有噪音
- 网络连接掉失
- 电池、温度、电压或电源监控传感器警报
- 硬盘驱动器故障
- USB 介质故障
- 由于摔落、浸水或其它外部压力导致的物理损坏

当出现此类问题时，请检查是否有损坏，然后尝试使用以下策略修正问题：

- 重新安置模块并重新启动
- 尝试将模块插入机箱中的其它托架
- 尝试更换硬盘驱动器或 USB 闪存盘
- 重新连接或更换电源和网络电缆

如果这些步骤没有解决问题，请参阅《*硬件用户手册*》了解硬件设备的特定故障排除信息。

其它故障指示灯

表 19-2. 故障指示灯

查看：	**操作：**
Systems Management Software 发出警报信息	请参阅 Systems Management Software 的说明文件。
系统事件日志信息	请参阅"检查系统事件日志 (SEL)"。
启动开机自检代码中的信息	请参阅"检查开机自检代码"。
上次崩溃屏幕上的信息	请参阅"查看上次系统崩溃屏幕"。
LCD 中服务器状态屏幕上的警报信息	请参阅"在服务器状态屏幕上检查错误信息"。
iDRAC6 日志中的信息	请参阅"查看 iDRAC6 日志"。

问题解决工具

本节介绍可以用来诊断系统问题的 iDRAC6 公用程序，特别是尝试远程解决问题时。

- 检查系统运行状况
- 在系统事件日志中检查错误信息
- 检查开机自检代码
- 查看上次崩溃屏幕
- 查看最新引导顺序
- 在 LCD 上的服务器状态屏幕上检查错误信息
- 查看 iDRAC6 日志
- 查看系统信息
- 识别机箱中的受管服务器
- 使用诊断控制台
- 管理远程系统上的电源

检查系统运行状况

登录到 iDRAC6 Web 界面后，**"System Summary"（系统摘要）**屏幕会显示系统组件的运行状况。表 19-3 说明系统运行状况指示灯的含义。

表 19-3. 服务器运行状况指示灯

指示灯	**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。

单击**"Server Health"（服务器运行状况）**屏幕上的任何组件查看有关组件的信息。会显示电池、温度、电压和电源监控的传感器读数，帮助诊断有些问题。iDRAC6 和 CMC 信息屏幕提供了有用的当前状况和配置信息。

检查系统事件日志 (SEL)

"SEL Log"（SEL 日志）屏幕显示受管服务器上发生的事件信息。

要查看**系统事件日志**，请执行以下步骤：

1. 单击**"System"（系统）**，然后单击**"Logs"（日志）**选项卡。
2. 单击**"System Event Log"（系统事件日志）**以显示**"System Event Log"（系统事件日志）**屏幕。

   "System Event Log"（系统事件日志）屏幕显示系统运行状况指示灯（请参阅表 19-3）、时间戳和事件说明。
3. 单击相应的**"System Event Log"（系统事件日志）**按钮继续（请参阅表 19-4）。

表 19-4. SEL 按钮

按钮	操作
"Print"（打印）	按**窗口中显示的排序顺序打印 SEL**。
"Clear Log"（清除日志）	清除 **SEL**。 **注：** **"Clear Log"（清除日志）**按钮仅当具有**"Clear Logs"（清除日志）**权限时显示。
"Save As"（另存为）	打开一个弹出窗口，使您能够将 **SEL** 保存到所选的目录。 **注：** 如果正在使用 Internet Explorer 并且在保存时遇到问题，请确保下载 Internet Explorer 的累积安全更新，下载位置是 Microsoft 支持网站 **support.microsoft.com**。 **注：** 使用 Internet Explorer 时，如无法使用**"Save As"（另存为）**保存 SEL 日志，这可能是由于浏览器设置造成的。要解决的问题： 1. 在 Internet Explorer 中，转至**"Tools"（工具）→"Internet Options"（Internet 选项）→"Security"（安全）**，选择要下载至的区域。例如，如果 iDRAC 设备位于本地内部网中，则选择**"Local Intranet"（本地 Intranet）**，然后单击**"Custom level...."（自定义级别...）** 2. 在**"Security Settings"（安全设置）**窗口中**"Downloads"（下载）**下，确保启用了以下选项： o "Automatic prompting for file downloads"（文件下载自动提示） o "File download"（文件下载） **小心：** **要确保使用的计算机可安全访问 iDRAC，必须禁用*"Miscellaneous"（其他）*下的*"Launching applications and unsafe files"（加载应用程序和不安全文件）*。**
"Refresh"（刷新）	重新载入 **SEL** 屏幕。

检查开机自检代码

"Post Codes"（开机自检代码）屏幕在引导操作系统前显示上次系统开机自检代码。开机自检代码是来自系统 BIOS 的进度指示，表示自打开电源重设的引导顺序的各个阶段，使用户能够诊断与系统引导相关的任何故障。

注： 查看 LCD 显示屏或《硬件用户手册》中的文本，以查找开机自检代码信息编号。

要查看开机自检代码，执行下列步骤：

1. 单击**"System"（系统）**、**"Logs"（日志）**选项卡，然后单击**"Post Codes"（开机自检代码）**。

   "Post Codes"（开机自检代码）屏幕显示系统运行状况指示灯（请参阅表 19-3）、十六进制代码和代码说明。

2. 单击相应的**"Post Code"（开机自检代码）**按钮继续（参阅表 19-5）。

表 19-5. 开机自检代码按钮

按钮	操作
"Print"（打印）	打印**"Post Code"（开机自检代码）屏幕。**
"Refresh"（刷新）	重新载入**"Post Code"（开机自检代码）屏幕。**

查看上次系统崩溃屏幕

注： 必须在 Server Administrator 和 iDRAC6 Web 界面中配置上次崩溃屏幕功能。请参阅"配置受管服务器以捕获上次崩溃屏幕"了解配置此功能的说明。

"Last Crash Screen"（上次崩溃屏幕）屏幕显示最近的崩溃屏幕，包含系统崩溃前发生的事件的信息。上次系统崩溃映像保存在 iDRAC6 持续存储中并且可以远程访问。

要查看**"Last Crash Screen"（上次崩溃屏幕）**屏幕，请执行以下步骤：

- 单击**"System"（系统）**、**"Logs"（日志）**选项卡，然后单击**"Last Crash Screen"（上次崩溃屏幕）**。

"Last Crash Screen"（上次崩溃屏幕）屏幕提供表 19-6 中所示的按钮：

注： 如果没有保存的崩溃屏幕，**"Save"（保存）**和**"Delete"（删除）**按钮不会出现。

表 19-6. 上次崩溃屏幕按钮

按钮	操作
"Print"（打印）	打印**"Last Crash Screen"（上次崩溃屏幕）**屏幕。
"Save"（保存）	打开一个弹出窗口，使您能够将**上次崩溃屏幕**保存到所选的目录。
"Delete"（删除）	删除**"Last Crash Screen"（上次崩溃屏幕）**屏幕。
"Refresh"（刷新）	重新载入**"Last Crash Screen"（上次崩溃屏幕）**屏幕。

注： 由于自动恢复计时器的波动，当系统重设计时器配置为太高的值时，**上次崩溃屏幕**可能无法捕获。默认设置为 480 秒钟。使用 Server Administrator 或 IT Assistant 将系统重设计时器设置为 60 秒，并确保**上次崩溃屏幕**运行正常。有关其它信息，请参阅"配置受管服务器以捕获上次崩溃屏幕"。

查看最新引导顺序

如果遇到引导问题，可以从**"Boot Capture"（引导捕获）**屏幕查看前三次引导顺序期间发生的屏幕活动。引导屏幕以每秒钟 1 帧的速率回放。iDRAC6 在引导期间记录 50 个帧。

表 19-7 列出可用的控制操作。

注： 必须具有管理员权限才能查看引导捕获顺序的回放。

表 19-7. 引导捕获选项

按钮/选项	说明
"Select the boot sequence"（选择引导顺序）	允许选择待载入和播放的引导顺序。 - 引导捕获 1 — 载入最新的引导顺序。 - 引导捕获 2 — 载入引导捕获 1 之前发生的引导顺序（第二个最新的引导顺序）。 - 引导捕获 3 — 载入引导捕获 2 之前发生的引导顺序（第三个最新的引导顺序）。
"Save As"（另存为）	创建包含当前顺序所有引导捕获图像的压缩 .zip 文件。用户必须具有管理员权限才能执行此操作。
"Previous Screen"（上一个屏幕）	转到重放控制台的上一个屏幕（如果有）。
"Play"（播放）	从重放控制台的当前屏幕启动屏幕播放。
"Pause"（暂停）	在重放控制台正在播放的当前屏幕暂停显示屏幕播放。
"Stop"（停止）	停止屏幕播放，并载入引导顺序的第一个屏幕。
"Next Screen"（下一个屏幕）	转到重放控制台的下一个屏幕（如果有）。
"Print"（打印）	打印出现在屏幕上的引导捕获图像。
"Refresh"（刷新）	重新载入引导捕获屏幕。

在服务器状态屏幕上检查错误信息

如果闪烁的琥珀色 LED 亮起，并且特定服务器出现一个错误，则 LCD 上的主服务器状态屏幕将使用橙色高亮度显示受影响的服务器。使用 LCD 导航按钮高亮度显示受影响的服务器，然后单击中间按钮。将在第二行显示错误和警告信息。下表列出所有错误信息及其严重性。

表 19-8. 服务器状况屏幕

严重性	信息	原因
Warning（警告）	System Board Ambient Temp: Temperature sensor for System Board, warningevent (系统板环境温度：系统板的温度传感器，警告事件)	服务器环境温度越过警告阈值
Critical（严重）	System Board Ambient Temp: Temperature sensor for System Board, failure event (系统板环境温度：系统板的温度传感器，故障事件)	服务器环境温度越过故障阈值
Critical（严重）	System Board CMOS Battery: Battery sensor for System Board, failed wasasserted (系统板 CMOS 电池：系统板的电池传感器，故障已声明)	CMOS 电池不存在或没有电压
Warning（警告）	System Board System Level: Current sensor for System Board, warning event (系统板系统水平：系统板的电流传感器，警告事件)	电流越过警告阈值
Critical（严重）	System Board System Level: Current sensor for System Board, failure event (系统板系统水平：系统板的电流传感器，故障事件)	电流越过故障阈值
Critical（严重）	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU<编号> <电压传感器名称>：CPU<编号> 的电压传感器，声明的状态已声明)	电压超出范围
Critical（严重）	System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted (系统板<电压传感器名称>：系统板的电压传感器，声明的状态已声明)	电压超出范围
Critical（严重）	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU<编号> <电压传感器名称>：CPU<编号> 的电压传感器，声明的状态已声明)	电压超出范围
Critical（严重）	CPU<number> Status: Processor sensor for CPU<number, IERR was asserted (CPU<编号> 状态：CPU<编号> 的处理器传感器，IERR 已声明)	CPU 故障
Critical（严重）	CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted (CPU<编号> 状态：CPU<编号> 的处理器传感器，热断路已声明)	CPU 过热
Critical（严重）	CPU<number> Status: Processor sensor for CPU<number, configuration error was asserted (CPU<编号> 状态：CPU<编号> 的处理器传感器配置错误已声明)	处理器类型不正确或位置错误
Critical（严重）	CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted (CPU<编号> 状态：CPU<编号> 的处理器传感器，存在已取消声明)	所需 CPU 缺少或不存在
Critical（严重）	System Board Video Riser: Module sensor for System Board, device removed was asserted (系统板视频升降器：系统板的模块传感器，拆卸的设备已声明)	已拆卸所需模块
Critical（严重）	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted (Mezz B<插槽编号> 状态：Mezz B<插槽编号> 的添加式插卡传感器，安装错误已声明)	为 IO 结构安装的夹层卡不正确
Critical（严重）	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted (Mezz C<插槽编号> 状态：Mezz C<插槽编号> 的添加式插卡传感器，安装错误已声明)	为 I/O 结构安装的夹层卡不正确
Critical（严重）	Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed (背板驱动器 <编号>：背板的驱动器插槽传感器，驱动器已拆卸)	存储驱动器已拆卸
Critical（严重）	Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted (背板驱动器 <编号>：背板的驱动器插槽传感器，驱动器故障已声明)	存储驱动器故障
Critical（严重）	System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted (系统板 PFault 故障防护：系统板的电压传感器，声明的状态已声明)	在系统板电压未处于正常水平时生成此事件
Critical（严重）	System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted (系统板操作系统监护程序：系统板的监护程序传感器，过期的计时器已声明)	iDRAC6 监护程序计时器已过期并且没有设置操作
Critical（严重）	System Board OS Watchdog: Watchdog sensor for System Board, reboot was asserted (系统板操作系统监护程序：系统板的监护程序传感器，重新引导已声明)	iDRAC6 监护程序检测到系统已崩溃（由于没有从主机收到响应，因此计时器过期），并且操作设置为重新引导
Critical（严重）	System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted (系统板操作系统监护程序：系统板的监护程序传感器，关机已声明)	iDRAC6 监护程序检测到系统已崩溃（由于没有从主机收到响应，因此计时器过期），并且操作设置为关机
Critical（严重）	System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted (系统板操作系统监护程序：系统板的监护程序传感器，关机后再开机已声明)	iDRAC6 监护程序检测到系统已崩溃（由于没有从主机收到响应，因此计时器过期），并且操作设置为关机后再开机
Critical（严重）	System Board SEL: Event Log sensor for System Board, log full was asserted (系统板 SEL：系统板的事件日志传感器，日志已满已声明)	SEL 设备检测到再向 SEL 添加一个条目后它就已满
Warning（警告）	ECC Corr Err: Memory sensor, correctable ECC (ECC 校正错误：内存传感器，可校正 ECC) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	可校正的 ECC 错误达到严重水平
Critical（严重）	ECC Uncorr Err: Memory sensor, uncorrectable ECC (ECC 不可校正错误：内存传感器，不可校正的 ECC) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	已检测到一个不可校正的 ECC 错误
Critical（严重）	I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted (I/O 信道检查：严重事件传感器，I/O 信道检查 NMI 已声明)	I/O 信道中生成一个严重中断
Critical（严重）	PCI Parity Err: Critical Event sensor, PCI PERR was asserted (PCI 奇偶校验错误：严重事件传感器，PCI PERR 已声明)	在 PCI 总线上检测到奇偶校验错误
Critical（严重）	PCI System Err: Critical Event sensor, PCI SERR (PCI 系统错误：关键事件传感器，PCI SERR) (<Slot number or PCI Device ID>) was asserted (（<插槽编号或 PCI 设备 ID>）已声明)	设备检测到 PCI 错误

Critical（严重）	SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted (SBE 日志禁用：事件日志传感器，禁用的可校正内存错误记录已声明)	如果记录的 SBE 太多，会禁用单位错误记录
Critical（严重）	Logging Disabled: Event Log sensor, all event logging disabled was asserted (记录禁用：事件日志传感器，禁用的所有事件记录已声明)	禁用了所有错误记录
不可恢复	CPU Protocol Err: Processorsensor, transition to non-recoverable was asserted (CPU 协议错误：处理器传感器，到不可恢复的过渡已声明)	处理器协议已进入一种不可恢复的状态
不可恢复	CPU Bus PERR: Processor sensor, transition to non-recoverable wasasserted (CPU 总线 PERR：处理器传感器，到不可恢复的过渡已声明)	处理器总线 PERR 已进入一种不可恢复的状态
不可恢复	CPU Init Err: Processor sensor, transition to non-recoverable wasasserted (CPU 初始化错误：处理器传感器，到不可恢复的过渡已声明)	处理器初始化已进入一种不可恢复的状态
不可恢复	CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted (CPU 机器检查：处理器传感器，到不可恢复的过渡已声明)	处理器机器检查已进入一种不可恢复的状态
Critical（严重）	Memory Spared: Memory sensor, redundancy lost (内存空闲：内存传感器，冗余丢失) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	内存空闲不再冗余
Critical（严重）	Memory Mirrored: Memory sensor, redundancy lost (内存镜像：内存传感器，冗余丢失) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	镜像内存不再冗余
Critical（严重）	Memory RAID: Memory sensor, redundancy lost (内存 RAID：内存传感器，冗余丢失) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	RAID 内存不再冗余
Warning（警告）	Memory Added: Memory sensor, presence (<DIMM Location>) was deasserted (添加的内存：内存传感器，存在（<DIMM 位置>）已取消声明)	已拆卸添加的内存模块
Warning（警告）	Memory Removed: Memory sensor, presence (<DIMM Location>) was deasserted (拆卸的内存：内存传感器，存在（<DIMM 位置>）已取消声明)	已拆卸内存模块
Critical（严重）	Memory Cfg Err: Memory sensor, configuration error (内存配置错误：内存传感器，配置错误) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	系统的内存配置不正确
Warning（警告）	Mem Redun Gain: Memory sensor, redundancy degraded (内存冗余增益：内存传感器，冗余降级) (<DIMM Location>) was asserted ((<DIMM 位置>) 已声明)	内存冗余已降级但未丢失
Critical（严重）	PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted (PCIE 严重错误：严重事件传感器，总线严重错误已声明)	在 PCIE 总线上检测到严重错误
Critical（严重）	Chipset Err: Critical Event sensor, PCI PERR was asserted (芯片组错误：严重事件传感器，PCI PERR 已声明)	检测到芯片错误
Warning（警告）	Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location>) was asserted (内存 ECC 警告：内存传感器，从良好到非严重的过渡（<DIMM 位置>）已声明)	可校正 ECC 错误数已经超出正常水平
Critical（严重）	Mem ECC Warning: Memory sensor, transition to critical from less severe (<DIMM Location>) was asserted (内存 ECC 警告：内存传感器，从不太严重到严重的过渡（<DIMM 位置>）已声明)	可校正的 ECC 错误数已达到严重水平
Critical（严重）	POST Err: POST sensor, Nomemory installed (开机自检错误：开机自检传感器，没有安装内存)	板上没有检测到内存
Critical（严重）	POST Err: POST sensor, Memory configuration error (开机自检错误：开机自检传感器，内存配置错误)	检测到内存，但是内存不可配置
Critical（严重）	POST Err: POST sensor, Unusable memory error (开机自检错误：开机自检传感器，不可使用的内存错误)	已配置内存，但内存不可用
Critical（严重）	POST Err: POST sensor, Shadow BIOS failed (开机自检错误：开机自检传感器，遮罩 BIOS 故障)	系统 BIOS 遮罩故障
Critical（严重）	POST Err: POST sensor, CMOS failed (开机自检错误：开机自检传感器，CMOS 出现故障)	CMOS 出现故障
Critical（严重）	POST Err: POST sensor, DMA controller failed (开机自检错误：开机自检传感器，DMA 控制器出现故障)	DMA 控制器出现故障
Critical（严重）	POST Err: POST sensor, Interrupt controller failed (开机自检错误：开机自检传感器，中断控制器出现故障)	中断控制器出现故障
Critical（严重）	POST Err: POST sensor, Timer refresh failed (开机自检错误：开机自检传感器，计时器刷新故障)	计时器刷新故障
Critical（严重）	POST Err: POST sensor, Programmable interval timer error (开机自检错误：开机自检传感器，可编程间隔计时器错误)	可编程间隔计时器错误
Critical（严重）	POST Err: POST sensor, Parity error (开机自检错误：开机自检传感器，奇偶校验错误)	奇偶校验错误
Critical（严重）	POST Err: POST sensor, SIO failed (开机自检错误：开机自检传感器，SIO 出现故障)	SIO 出现故障
Critical（严重）	POST Err: POST sensor, Keyboard controller failed (开机自检错误：开机自检传感器，键盘控制器出现故障)	Keyboard controller failure
Critical（严重）	POST Err: POST sensor, Systemmanagement interrupt initialization failed (开机自检错误：开机自检传感器，系统管理中断初始化失败)	系统管理中断初始化失败
Critical（严重）	POST Err: POST sensor, BIOSshutdown test failed (开机自检错误：开机自检传感器，BIOS 关闭检测失败)	BIOS 关闭检测失败
Critical（严重）	POST Err: POST sensor, BIOSPOST memory test failed (开机自检错误：开机自检传感器，BIOS 开机自检内存检测失败)	BIOS 开机自检内存检测失败
Critical（严重）	POST Err: POST sensor, Dellremote access controller configuration failed (开机自检错误：开机自检传感器，Dell Remote Access Controller 配置失败)	Dell Remote Access Controller 配置失败
Critical（严重）	POST Err: POST sensor, CPU configuration failed (开机自检错误：开机自检传感器，CPU 配置失败)	CPU 配置失败
Critical（严	POST Err: POST sensor, Incorrect memory configuration (开机自检错误：开机自检传感器，内存配置不正	内存配置不正确

重）	确)	
Critical（严重）	POST Err: POST sensor, POST failure (开机自检错误：开机自检传感器，开机自检故障)	视频后出现一般故障
Critical（严重）	Hdwar version err: Version Change sensor, hardware incompatibility was asserted (硬件版本错误：版本更改传感器，硬件不兼容性已声明)	检测到不兼容的硬件
Critical（严重）	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted (硬件版本错误：版本更改传感器，硬件不兼容性（BMC 固件）已声明)	硬件和固件不兼容
Critical（严重）	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted (硬件版本错误：版本更改传感器，硬件不兼容性（BMC 固件和 CPU 不匹配）已声明)	CPU 和固件不兼容
Critical（严重）	Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted (内存温度过高：内存传感器，可校正的 ECC <DIMM 位置> 已声明)	内存模块过热
Critical（严重）	Mem Fatal SB CRC: Memory sensor, uncorrectable ECC wasasserted (内存严重 SB CRC：内存传感器，不可校正的 ECC 已声明)	南桥内存故障
Critical（严重）	Mem Fatal NB CRC: Memory sensor, uncorrectable ECC wasasserted (内存严重 NB CRC：内存传感器，不可校正的 ECC 已声明)	北桥内存故障
Critical（严重）	WatchDog Timer: Watchdog sensor, reboot was asserted (监护程序计时器：监护程序传感器，重新引导已声明)	监护程序计时器已造成系统重新引导
Critical（严重）	WatchDog Timer: Watchdog sensor, timer expired was asserted (监护程序计时器：监护程序传感器，计时器过期已声明)	监护程序计时器过期但没有采取操作
Warning（警告）	Link Tuning: Version Change sensor, successful software or F/W change was deasserted (链接调节：版本更改传感器，成功的软件或 F/W 更改已取消声明)	无法为正确的 NIC 操作更新链接调节设置
Warning（警告）	Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted (链接调节：版本更改传感器，成功的硬件更改 <设备插槽编号> 已取消声明)	无法为正确的 NIC 操作更新链接调节设置
Critical（严重）	LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Function #) was asserted (LinkT/FlexAddr：链接调节传感器，无法对虚拟 MAC 地址进行编程（总线 # 设备 # 功能 #）已声明)	无法为此设备进行 FlexAddress 编程
Critical（严重）	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) wasasserted (LinkT/FlexAddr：链接调节传感器，设备选项 ROM 无法支持链接调节或 FlexAddress（Mezz <位置>）已声明)	选项 ROM 不支持 FlexAddress 或链接调节
Critical（严重）	LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted (LinkT/FlexAddr：链接调节传感器，无法从 BMC/iDRAC6 获得链接调节或 FlexAddress 数据已声明)	无法从 BMC/iDRAC6 获得链接调节或 FlexAddress 信息
Critical（严重）	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or FlexAddress (Mezz XX) was asserted (LinkT/FlexAddr：链接调节传感器，设备选项 ROM 无法支持链接调节或 FlexAddress (Mezz XX) 已声明)	当 NIC 的 PCI 设备选项 ROM 不支持链接调节或 FlexAddress 功能时产生此事件
Critical（严重）	LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted (LinkT/FlexAddr：链接调节传感器，无法对虚拟 MAC 地址（<位置>）进行编程已声明)	当 BIOS 无法在指定 NIC 设备上对虚拟 MAC 地址进行编程时产生此事件
Critical（严重）	I/O Fatal Err: Fatal IO Group sensor, fatal IO error (<location>) (I/O 严重错误：严重 IO 组传感器，严重 IO 错误（<位置>）)	此事件的生成与 CPU IERR 存在关联，并可指明哪个设备导致 CPU IERR
Warning（警告）	PCIE NonFatal Er: Non Fatal I/O Group sensor, PCIe error (<location>) (PCIE 非严重错误：非严重 I/O 组传感器，PCIe 错误（<位置>）)	此事件的生成与 CPU IERR 存在关联

查看 iDRAC6 日志

iDRAC6 日志是 iDRAC6 固件中的一个持续日志。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。iDRAC6 固件更新后清除日志。

其中**系统事件日志** (SEL) 包含受管服务器中发生的事件记录，iDRAC6 **日志**包含 iDRAC6 中发生的事件记录。

要访问 iDRAC6 **日志**，应执行以下步骤：

- 单击**"System"（系统）→"Remote Access"（远程访问）→ iDRAC6 →"Logs"（日志）** 。显示 **iDRAC6 日志** 屏幕。该屏幕提供列在 表 19-9 中的信息。

表 19-9. iDRAC6 日志信息

字段	说明
"Date/Time"（日期/时间）	日期和时间（例如 Dec 19 16:55:47）。 在 iDRAC6 初始化时，iDRAC6 的时钟根据受管服务器的时钟进行设置。如果在启动 iDRAC6 时受管服务器处于关闭状态，则 iDRAC6 将根据刀片所在机箱中的 CMC 设置其时钟。 **注：** 由于 iDRAC6 的时间源会根据受管服务器电源状态（iDRAC6 初始化时）的不同而有所不同，受管服务器时间应设置为与 CMC 时间一致。如果系统与 CMC 时间不一致，iDRAC 初始化事件后可能会在 iDRAC6 日志中报告不一致时间。
"Source"（来源）	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。

使用 iDRAC6 日志按钮

iDRAC6 **日志**屏幕提供以下按钮（请参阅 表 19-10）。

表 19-10. iDRAC6 日志按钮

按钮	操作
"Print"（打印）	打印 iDRAC6 **日志**屏幕。
"Clear Log"（清除日志）	清除 iDRAC6 **日志**条目。 **注：** 只有您具有**"Clear Logs"（清除日志）**权限时，才会显示**"Clear Log"（清除日志）**按钮。
"Save As"（另存为）	打开一个弹出窗口，使您能够将iDRAC6 **日志** 保存到所选的目录。 **注：** 如果正在使用 Internet Explorer 并且在保存时遇到问题，请确保下载 Internet Explorer 的累积安全更新，下载位置是 Microsoft 支持网站 **support.microsoft.com**。
"Refresh"（刷新）	重新载入 iDRAC6 **日志**屏幕。

查看系统信息

"System Details"（系统详细信息）屏幕显示关于以下系统组件的信息：

- 系统主机柜
- Integrated Dell Remote Access Controller 6—Enterprise

要访问系统信息，单击**"System"（系统）**→**"Properties"（属性）**→**"System Details"（系统详细信息）**。

请参阅 "对 Managed System 进行恢复和故障排除" 了解有关系统摘要、系统主机柜和 iDRAC6 的信息。

识别机箱中的受管服务器

Dell PowerEdge M1000e 机箱最多可装有十六个服务器。要找到机箱中的特定服务器，可以使用 iDRAC6 Web 界面打开服务器上的蓝色闪烁 LED。打开 LED 后，可以指定想要 LED 闪烁的秒数以确保在 LED 依然闪烁时可以找到机箱。输入 **0** 会使 LED 一直闪烁直到禁用它。

要识别服务器：

1. 单击**"System"（系统）**→**"Remote Access"（远程访问）**→**iDRAC6** →**"Troubleshooting"（故障排除）**。
2. 在**"Identify"（识别）**屏幕上，选中**"Identify Server"（识别服务器）**。
3. 在**"Identify Server Timeout"（标识服务器超时）**字段中，输入想要 LED 闪烁的秒数。如果想要 LED 一直闪烁直到禁用它，应输入 **0**。
4. 单击**"Apply"（应用）**。

服务器上的蓝色 LED 会闪烁指定的秒数。

如果输入 **0** 保持 LED 闪烁，应按照这些步骤来禁用它：

1. 单击**"System"（系统）**→**"Remote Access"（远程访问）**→**iDRAC6** →**"Troubleshooting"（故障排除）**。
2. 在**"Identify"（识别）**屏幕上，取消选中**"Identify Server"（识别服务器）**。
3. 单击**"Apply"（应用）**。

使用诊断控制台

iDRAC6 提供一组标准网络诊断工具（参阅表 19-11），与基于 Microsoft Windows 或 Linux 的系统提供的工具类似。使用 iDRAC6 Web 界面，可以访问网络调试工具。

单击**"Reset iDRAC6"（重设 iDRAC6）**重设 iDRAC。在 iDRAC 上执行正常引导操作。

要访问**"Diagnostics Console"（诊断控制台）**屏幕，请执行以下步骤：

1. 单击**"System"（系统）→ iDRAC6 →"Troubleshooting"（故障排除）**。

2. 选择**"Diagnostics Console"（诊断控制台）**选项卡。

表 19-11 说明可以在**"Diagnostics Console"（诊断控制台）**屏幕上输入的命令。输入命令并单击**"Submit"（提交）**。调试结果显示在**"Diagnostics Console"（诊断控制台）**屏幕中。

单击**"Clear"（清除）**按钮清除上一个命令显示的结果。

要刷新**"Diagnostics Console"（诊断控制台）**屏幕，请单击**"Refresh"（刷新）**。

表 19-11. 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。
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。
ping6 <*IPv6 地址*>	验证目标 IPv6 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 IPv6 地址。ICMP（Internet 控制报文协议）回音数据包根据当前的路由表内容发送到目标 IPv6 地址。
traceroute <*IP 地址*>	用来确定 IP 网络上数据包使用的路由。
traceroute6 <*IPv6 地址*>	用来确定 IPv6 网络上数据包使用的路由。
gettracelog	显示 iDRAC6 跟踪日志。要获取更多信息，请参阅 Dell 支持网站 **support.dell.com / manuals** 提供的《*iDRAC6 管理员参考指南*》中的 gettracelog。

管理远程系统上的电源

iDRAC6 允许在受管服务器上远程执行几种电源管理操作。使用**"Power Management"（电源管理）**屏幕在重新引导、开机或关机时通过操作系统执行有序关机。

注： 必须具有**"Execute Server Action Commands"（执行服务器操作命令）**权限才能执行电源管理操作。请参阅"添加和配置 iDRAC6 用户"查看配置用户权限的帮助。

1. 单击**"System"（系统）**，然后单击**"Power Management"（电源管理）→"Power Control"（电源控制）**选项卡。

2. 选择**"Power Control Operation"（电源控制操作）**，例如，**"Reset System (warm boot)"（重设系统 [温引导]）**。

   表 19-12 提供有关电源控制操作的信息。

3. 单击**"Apply"（应用）**以执行所选操作。

表 19-12. 电源控制操作

"Power On Sysytem"（打开系统电源）	打开系统电源（相当于在系统电源关闭时按电源按钮）。
"Power Off System"（关闭系统电源）	关闭系统电源（相当于在系统电源打开时按电源按钮）。
"NMI (Non-Masking Interrupt)"（NMI [非屏蔽中断]）	向操作系统发送一个高级中断指令，使系统暂停运行以进行紧急诊断或故障排除工作。
"Graceful Shutdown"（正常关机）	尝试正常关闭操作系统，然后关闭系统电源。它需要能识别 ACPI （高级配置和电源接口）的操作系统，允许系统指导的电源管理。 **注：** 当服务器软件停止响应或您未在本地 Windows 控制台以管理员身份登录时，可能无法正常关闭服务器操作系统。在这些情况下，必须指定对 Windows 强制重新引导，而不是正常关机。另外，根据您主机上运行的 Windows 操作系统版本，有可能配置了在 iDRAC6 触发时修改关机行为的关于关机过程的策略。要了解本地计算机策略"Shutdown: Allow system to be shut down without having to login"（关机：允许在没有登录的情况下关闭系统），请参阅 Microsoft 说明文件。
"Reset System (warm boot)"（重设系统 [温引导]）	重新引导系统而不关闭系统电源（温引导）。
"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（冷引导）。

有关详情，请参阅"电源监控和电源管理"。

故障排除和常见问题

表 19-13 包含有关故障排除问题的常见问题。

表 19-13. 常见问题/故障排除

问题	解答
服务器上的 LED 为闪烁琥珀色。	检查 SEL 信息并随后清除 SEL 以停止闪烁 LED。 从 iDRAC6 Web 界面： • 请参阅"检查系统事件日志 (SEL)" 从 SM-CLP： • 请参阅"SEL 管理" 从 iDRAC6 配置公用程序： • 请参阅"系统事件日志菜单"
服务器上有闪烁蓝色 LED。	用户已激活服务器的定位 ID。这是帮助识别机箱中服务器的信号。请参阅"识别机箱中的受管服务器"了解有关此 功能的信息。
我如何找到 iDRAC6 的 IP 地址？	**从 CMC Web 界面：** 1. 单击**"Chassis"（机箱）→"Servers"（服务器）**，然后单击**"Setup"（设置）**选项卡。 2. 单击**"Deploy"（部署）**。 3. 从显示的表中读出服务器的 IP 地址。 **从虚拟控制台：** • 重新引导服务器并通过按 <Ctrl><E> 进入 **iDRAC6 配置公用程序**。 • 在 BIOS 开机自检期间观察显示的 IP 地址。 • 在 OSCAR 中选择 "Dell CMC" 控制台以通过本地串行连接登录到 CMC。CMC RACADM 命令可以从该连接发出。请参阅 *《Dell Chassis Management Controller 管理员参考指南》*了解完整的 CMC RACADM 子命令列表。 • 使用本地 RACADM **getsysinfo** 命令查看 iDRAC6 IP 地址。
	例如： $ racadm getniccfg -m server-1 DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1 **从本地 RACADM：** 在命令提示符处输入以下命令： racadm getsysinfo **从 LCD：** 1. 在主菜单上，高亮度显示**"Server"（服务器）**并按选中按钮。 2. 选择寻找 IP 地址的服务器并按选中按钮。
我如何找到 CMC 的 IP 地址？	**从 iDRAC6 Web 界面：** • 单击**"System"（系统）→"Remote Access"（远程访问）→ CMC**。 CMC IP 地址显示在 CMC **"Summary"（摘要）**屏幕上。 **从虚拟控制台：** • 在 OSCAR 中选择 "Dell CMC" 控制台以通过本地串行连接登录到 CMC。CMC RACADM 命令可以从该连接发出。请参阅 *《Dell Chassis Management Controller 管理员参考指南》*了解完整的 CMC RACADM 子命令列表。 $ racadm getniccfg -m chassis NIC Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate

	注： 以上操作还可以用远程 RACADM 执行。
iDRAC6 网络连接不工作。	• 确保 LAN 电缆已连接到 CMC。 • 确保已为网络启用 NIC 设置、IPv4 或 IPv6 设置，以及静态或 DHCP。
我将服务器插入机箱并按下电源按钮，但是没有任何反应。	• iDRAC6 需要大约 2 分钟初始化，然后服务器才能开机。 • 检查 CMC 电源预算。机箱电源预算可能超支。
我忘记了 iDRAC6 管理用户名和密码。	必须将 iDRAC6 恢复为默认设置。 1. 重新引导服务器并在提示时按 <Ctrl><E> 进入 **iDRAC6 配置公用程序**。 2. 在 **iDRAC6 配置公用程序**菜单上，高亮度显示**"Reset to Default"（重设为默认值）**并按 <Enter>。 **注：** 还可以通过发出 `racadm racresetcfg` 从本地 RACADM 重设 iDRAC6。 有关详情，请参阅""Reset To Default"（重设为默认值）"。
如何更改服务器的插槽名称？	1. 登录到 CMC Web 界面。 2. 打开**机箱**树并单击**"Servers"（服务器）**。 3. 单击**"Setup"（设置）**选项卡。 4. 在服务器的行中输入插槽的新名称。 5. 单击**"Apply"（应用）**。
从 iDRAC6 Web 界面启动虚拟控制台会话时， ActiveX 安全弹出窗口将会出现。	iDRAC6 可能不是可信站点。要防止每次启动虚拟控制台会话都出现安全弹出窗口，应在客户端浏览器中将 iDRAC6 添加到受信任的站点列表： 1. 单击**"Tools"（工具）→"Internet Options"（Internet 选项）→"Security"（安全）→"Trusted sites"（信任的站点）**。 2. 单击**"Sites"（站点）**并输入 iDRAC6 的 IP 地址或 DNS 名称。 3. 单击 **Add**（添加）。 4. 单击**"Custom Level"（自定义级别）**。 5. 在**"Security Settings"（安全设置）**窗口中，在**"Download unsigned ActiveX Controls"（下载未签名的 ActiveX 控件）**下选择**"Prompt"（提示）**。
启动虚拟控制台会话时，查看器屏幕为空白。	如果具有**"Virtual Media"（虚拟介质）**权限但没有**"Virtual Console"（虚拟控制台）**权限，将能够启动查看器以便可以访问虚拟介质功能，但是受管服务器的控制台将不显示。
iDRAC6 在引导期间不响应。	卸下并重新插入服务器。 检查 CMC Web 界面查看 iDRAC6 是否显示为可升级组件。如果是，请按"使用 CMC 更新 iDRAC6 固件"的说明操作。 如果没有解决问题，请联系技术支持部门。
尝试引导受管服务器时，电源指示灯为绿色，但是根本没有开机自检或视频。	如果出现以下情况，可能会发生此现象： • 内存未安装或不可访问。 • CPU 未安装或不可访问。 • 视频提升卡缺失或连接不正确。 另外，在 iDRAC6 Web 界面或 LCD 的 iDRAC6 日志中查找错误信息。

目录