Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

注和警告

注： "注"表示可以帮助您更好地使用计算机的重要信息。

警告： "警告"表示如果不遵循说明，就有可能损坏硬件或导致数据丢失。

本说明文件中的信息如有更改，恕不另行通知。
© 2009 Dell Inc. 版权所有，翻印必究。

未经 Dell Inc. 书面许可，严禁以任何形式复制这些材料。

本文中使用的商标：*Dell*、*DELL* 徽标、*Dell OpenManage* 和 *PowerEdge* 是 Dell Inc. 的商标；*Microsoft*、*Windows*、*Windows Server*、*Windows Vista* 和 *Active Directory* 是 Microsoft Corporation 在美国和/或其它国家/地区的商标或注册商标；*Red Hat* 和 *Linux* 是 Red Hat, Inc. 在美国和其它国家/地区的注册商标；*SUSE* 是 Novell Corporation 的注册商标。*Intel* 和 *Pentium* 是 Intel Corporation 在美国和其它国家/地区的注册商标；*UNIX* 是 The Open Group 在美国和其它国家/地区的注册商标；VMware 是 VMware, Inc. 在美国和/或其它管辖区域的注册商标。

版权 1998-2009 The OpenLDAP Foundation。版权所有，翻印必究。无论修改与否，以源代码和二进制的形式重新分发或使用都必须经过 OpenLDAP Public License 的授权许可。此许可证的副本包括在分发目录顶层中的 LICENSE 文件中，您也可以在 **www.OpenLDAP.org/license.html** 中找到。OpenLDAP 是 The OpenLDAP Foundation 的注册商标。一些单独文件和/或附送软件包的版权可能归其它方所有，受其它条款的制约。此软件根据 University of Michigan LDAP v3.3 分发版本开发出来。此软件还包含来自公共来源的材料。有关 OpenLDAP 的信息可以从 **www.openldap.org/** 获得。部分版权 1998-2004 Kurt D.Zeilenga。部分版权 1998-2004 Net Boolean Incorporated。部分版权 2001-2004 IBM Corporation。版权所有，翻印必究。无论修改与否，以源代码和二进制的形式重新分发或使用都必须经过 OpenLDAP Public License 的授权许可。部分版权 1999-2003 Howard Y.H.Chu。部分版权 1999-2003 Symas Corporation。部分版权 1998-2003 Hallvard B.Furuseth。版权所有，翻印必究。只要保留此通告，无论修改与否，都允许以源代码和二进制的形式重新分发和使用。在没有得到版权所有者事先书面许可的情况下，所有者的名称不得用于标记或宣传那些根据本软件开发出来的产品。本软件按"原样"提供，不带任何明示或暗示的保证。部分版权 (c) 1992-1996 Regents of the University of Michigan。版权所有，翻印必究。只要保留此通告并且应有权归属于 Ann Arbor 的 University of Michigan 所有，则允许以源代码和二进制的形式重新分发或使用。在没有得到事先书面许可的情况下，该大学的名称不得用于标记或宣传那些根据本软件开发出来的产品。本软件按"原样"提供，不带任何明示或暗示的保证。本说明文件中述及的其它商标和产品名称是指拥有相应商标和产品名称的公司或其制造的产品。Dell Inc. 对本公司的商标和产品名称之外的其它商标和产品名称不拥有任何专有权。

2009 年 6 月

目录

词汇表

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

Active Directory

Active Directory 一种集中且标准化的系统，能够自动化网络管理用户数据、安全和分布式资源，并能够保证与其它目录的互操作。Active Directory 的设计专门针对分布式网络环境。

ARP

地址解析协议 (Address Resolution Protocol) 的缩略词，是一种通过主机的 Internet 地址查找其以太网地址的方法。

ASCII

美国信息交换标准代码 (American Standard Code for Information Interchange) 的缩略词，是一种代码表示法，用于显示或打印字母、数字和其它字符。

BIOS

基本输入/输出系统 (basic input/output system) 的缩略词，是系统软件的一部分，系统软件用于提供与外围设备的最低级界面，并控制系统引导过程的第一阶段，包括将操作系统安装到内存中。

CA

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

CD

压缩光盘 (compact disc) 的缩写。

CHAP

质询握手验证协议 (Challenge-Handshake Authentication Protocol) 的缩略词，PPP 服务器使用的一种验证方法，用于验证连接创始者的身份。

CIM

公用信息模型 (Common Information Model) 的缩略词，是一个用于在网络上管理系统的协议。

CLI

命令行界面 (command-line interface) 的缩写。

CLP

命令行协议 (command-line protocol) 的缩写。

CSR

证书签名请求 (Certificate Signing Request) 的缩写。

DDNS

动态域名系统 (Dynamic Domain Name System) 的缩写。

DHCP

动态主机配置协议 (Dynamic Host Configuration Protocol) 的缩写，是一种可以为局域网中计算机动态分配 IP 地址的协议。

DLL

动态链接库 (Dynamic Link Library) 的缩写，是一个小程序的库，其中的任何小程序都可以由系统中运行的大程序在需要时调用。这种小程序可以帮助大程序与特定设备（比如打印机或扫描仪）通信，通常打包为 DLL 程序（或文件）。

DMTF

分布式管理综合小组 (Distributed Management Task Force) 的缩写。

DNS

域名系统 (Domain Name System) 的缩写。

DSU

磁盘存储单元 (disk storage unit) 的缩写。

FQDN

完全限定域名 (Fully Qualified Domain Names) 的缩略词。Microsoft® Active Directory® 仅支持 64 字节或更少的 FQDN。

FSMO

灵活单主机操作 (Flexible Single Master Operation)。这是 Microsoft 用于保证扩展操作原子性的方法。

GMT

格林尼治标准时间 (Greenwich Mean Time) 的缩写，是世界上所有地区通用的标准时间。GMT 是指经过英国伦敦市外格林尼治天文台的本初子午线（0 经度）的平均太阳时。

GPIO

通用输入/输出 (general purpose input/output) 的缩写。

GRUB

GRand 统一引导加载程序 (DRand Unified Bootloader) 的缩略词，这是一个新的常用 Linux 加载程序。

GUI

图形用户界面 (graphical user interface) 的缩写。相对于以文本显示和键入所有用户交互活动的命令提示符界面，图形用户界面是指使用窗口、对话框和按钮等元素的计算机显示界面。

iAMT

Intel® Active Management Technology — 提供了更安全的系统管理功能，无论计算机是否开机，或者操作系统是否响应。

ICMB

智能机柜管理总线 (Intelligent enclosure Management Bus) 的缩写。

ICMP

Internet 控制报文协议 (Internet control message protocol) 的缩写。

ID

标识符 (identifier) 的缩写，通常用于表示用户标识符（用户 ID）或对象标识符（对象 ID）。

iDRAC6

Integrated Dell Remote Access Controller 的缩略词，Dell 11G PowerEdge 服务器的集成系统芯片监测/控制系统。

IP

Internet 协议 (Internet Protocol) 的缩写，是 TCP/IP 的网络层。IP 可提供信息包路径、分段和重组。

IPMB

智能平台管理总线 (intelligent platform management bus) 的缩写，一种用于系统管理技术的总线。

IPMI

智能平台管理界面 (Intelligent Platform Management Interface) 的缩写，是系统管理技术的一部分。

Kbps

千位/秒 (kilobits per second) 的缩写，表示数据传输速率。

LAN

局域网 (local area network) 的缩写。

LDAP

轻量目录访问协议 (Lightweight Directory Access Protocol) 的缩写。

LED

发光二极管 (light-emitting diode) 的缩写。

LOM

主板上局域网 (Local area network On Motherboard) 的缩写。

LUN

逻辑单元 (logical unit) 的缩略词。

MAC

介质访问控制 (media access control) 的缩略词，是网络节点和网络物理层之间的网络子层。

MAC 地址

介质访问控制地址 (media access control address) 的缩略词，是嵌入 NIC 物理组件的唯一地址。

Managed System

由 Management Station 监测的系统称为 Managed System。

Management Station

Management Station 是一个系统，管理员从该系统可远程管理配有 iDRAC6 的 Dell 系统。

MAP

管理访问点 (Manageability Access Point) 的缩写。

Mbps

兆位/秒 (megabits per second) 的缩写，表示数据传输速率。

MIB

管理信息库 (management information base) 的缩写。

MII

介质独立接口 (Media Independent Interface) 的缩写。

NAS

网络连接存储 (network attached storage) 的缩写。

NIC

网络接口卡 (network interface card) 的缩写。计算机中安装的适配器电路板，提供了到网络的物理连接。

OID

对象标识符 (Object Identifiers) 的缩写。

PCI

外围组件互连 (Peripheral Component Interconnect) 的缩写，是一种标准界面和总线技术，用于将外围设备连接至系统并与外围设备进行通信。

POST

开机自检 (power-on self-test) 的缩略词，是在系统开机时自动运行的一系列诊断检测。

PPP

点对点协议 (Point-to-Point Protocol) 的缩写，是 Internet 标准协议，通过串行点对点链接传输网络层数据报（例如 IP 数据包）。

RAC

远程访问控制器 (remote access controller) 的缩写。

RAM

随机存取存储器 (random-access memory) 的缩略词。RAM 是系统和 iDRAC6 上的通用可读可写存储器。

RAM 磁盘

模拟硬盘驱动器的内存驻留程序。iDRAC6 在其内存中保留 RAM 磁盘。

ROM

只读存储器 (read-only memory) 的缩略词，可以从中读取数据，但不能向其中写入数据。

RPM

Red Hat® Package Manager 的缩写，是一种用于 Red Hat Enterprise Linux® 操作系统的软件包管理系统，可帮助安装软件包。它与安装程序类似。

SAC

Microsoft 的 Special Administration Console 的缩略词。

SAP

服务访问点 (Service Access Point) 的缩写。

SEL

系统事件日志 (system event log) 的缩略词。

SM-CLP

服务器管理命令行协议 (Server Management-Command Line Protocol) 的缩写。SM-CLP 是 DMTF SMASH 标准的子组件，用于简化跨多个平台的服务器管理。SM-CLP 规范，与受管元件寻址规范 (Managed Element Addressing Specification) 以及 SM-CLP 映射规范配合使用，可说明各种管理任务执行的标准 verb 和目标。

SMI

系统管理中断 (systems management interrupt) 的缩写。

SMTP

简单邮件传输协议 (Simple Mail Transfer Protocol) 的缩写，是一种用于在系统间传输（通常通过以太网）电子邮件的协议。

SMWG

系统管理工作组 (Systems Management Working Group) 的缩写。

SNMP 陷阱

由 iDRAC6 生成的通知（事件），包含有关受管服务器状态更改或潜在硬件故障的信息。

SSH

安全外壳 (Secure SHell) 的缩写。

SSL

安全套接字层 (secure sockets layer) 的缩写。

TAP

远程定位器字母数字协议 (Telelocator Alphanumeric Protocol) 的缩写，是用于向寻呼机服务提交请求的协议。

TCP/IP

传输控制协议/网际协议 (Transmission Control Protocol/Internet Protocol) 的缩写，表示一组标准以太网协议，其中包括网络层协议和传输层协议。

TFTP

小型文件传输协议 (Trivial File Transfer Protocol) 的缩写，用于向无磁盘设备或系统下载引导代码的简单文件传输协议。

Unified Server Configurator

Dell Unified Server Configurator (USC) 是嵌入式配置公用程序，它允许在系统的整个生命周期中从嵌入式环境执行系统和存储管理任务。

UPS

不间断电源设备 (uninterruptible power supply) 的缩写。

USB

通用串行总线 (Universal Serial Bus) 缩写。

USC

Unified Server Configurator 的缩写

UTC

协调世界时 (Universal Coordinated Time) 的缩写。*请参阅* GMT。

VLAN

虚拟局域网 (Virtual Local Area Network) 的缩写。

VNC

虚拟网络计算 (virtual network computing) 的缩写。

VT-100

视频终端 100 (Video Terminal 100) 的缩写，用于大多数普通终端仿真程序。

WAN

广域网 (wide area network) 的缩写。

WS-MAN

Web 管理服务 (WS-MAN) 协议的缩写。WS-MAN 是交换信息的传输机制。WS-MAN 为设备提供通用语言来共享数据，从而使其更易于管理。

受管服务器

受管服务器是嵌入 iDRAC6 的系统。

回滚

可恢复上一软件或固件版本。

总线

连接计算机中各种功能装置的一组导体。总线根据其传输的数据的类型来命名，例如数据总线、地址总线或 PCI 总线。

扩展模式

一种解决方案，与 Active Directory 配合使用来决定用户对 iDRAC6 的访问权限；使用 Dell 定义的 Active Directory 对象。

控制台重定向

控制台重定向功能可将受管服务器的显示器屏幕、鼠标功能和键盘功能转至 Management Station 上的相应设备。这样您便可以使用 Management Station 的系统控制台来控制受管服务器。

标准模式

一种解决方案，与 Active Directory 配合使用来决定用户对 iDRAC6 的访问权限；只使用 Active Directory 组对象。

硬件日志

记录 iDRAC6 生成的事件。

目录

目录

RACADM 子命令概览

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节提供了 RACADM 命令行界面中可用子命令的说明。

警告： Racadm 设置对象的值，而不对其执行任何功能验证。例如，RACADM 允许设置证书验证对象为 1 而 Active Directory 对象为 0，即使只有在 Active Directory® 启用的情况下才进行证书验证。同样，即使 cfgADEnable 对象为 0，cfgADSSOEnable 对象也可以设置为 0 或 1，不过只有在 Active Directory 启用的情况下才生效。

---

help

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-1 说明了 **help** 命令。

表 A-1. Help 命令

命令	定义
help	列出可以与 **RACADM** 配合使用的所有子命令，并提供每个命令的简短说明。

提要

```
racadm help

racadm help <子命令>
```

说明

help 子命令列出了可以与 **racadm** 命令一起使用的所有子命令，以及对每个子命令的一行说明。还可以在 **help** 后键入子命令以得到有关特定子命令的语法。

输出

racadm help 命令显示子命令的完整列表。

racadm help <*子命令*> 命令只显示指定的子命令的信息。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

arp

注： 要使用此命令，必须具有**"Execute Diagnostic Commands"（执行诊断命令）**权限。

表 A-2 说明了 **arp** 命令。

表 A-2. arp 命令

命令	定义
arp	显示 ARP 表的内容。不能添加或删除 ARP 表条目。

提要

```
racadm arp
```

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

clearasrscreen

注： 要使用此命令，必须具有**"Clear Logs"（清除日志）**权限。

表 A-3 说明了 **clearasrscreen** 子命令。

表 A-3. clearasrscreen

子命令	定义
clearasrscreen	清除内存中的上次崩溃屏幕。

提要

```
racadm clearasrscreen
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

config

注： 要使用 **getconfig** 命令，必须具有**"Log In iDRAC"（登录到 iDRAC）**权限。

表 A-4 说明了 **config** 和 **getconfig** 子命令。

表 A-4. config/getconfig

子命令	定义
config	配置 iDRAC6。
getconfig	获取 iDRAC6 配置数据。

提要

```
racadm config [-c|-p] -f <文件名>

racadm config -g <组名> -o <对象名> [-i <索引>] <值>
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

说明

config 子命令允许用户分别设置 iDRAC6 配置参数或作为配置文件的一部分批量设置。如果数据不同，会为该 iDRAC6 对象写入新值。

输入

表 A-5 说明了 **config** 子命令选项。

注： serial/telnet/ssh 控制台不支持 **-f** 和 **-p** 选项。

表 A-5. config 子命令选项和说明

选项	说明
-f	**-f <*文件名*>** 选项会使 **config** 读取由 **<*文件名*>** 指定的文件内容并配置 iDRAC6。该文件必须包含在"分析规则"中所指定格式的数据。
-p	**-p**，或密码选项，指示 **config** 在配置完成后删除 config 文件 **-f <*文件名*>** 中包含的密码条目。
-g	**-g <*组名*>**（即组选项）必须与 **-o** 选项配合使用。<*组名*> 用于指定包含要设置的对象的组。
-o	**-o <*对象名*> <*值*>**（即对象选项）必须与 **-g** 选项配合使用。此选项指定与字符串 <*值*> 写在一起的对象名。
-i	**-i <*索引*>**（即索引选项）只对索引组有效并且可用于指定唯一组。<*索引*> 是从 1 至 16 的十进制整数。在此处该索引由索引值指定，而不由"命名的"值指定。
-c	**-c**，或检查选项，与 **config** 子命令配合使用，使用户可以分析 **.cfg** 文件以查找语法错误。如果找到错误，则显示行号和简短的错误说明。不会对 iDRAC6 执行写入操作。此选项只是一种检查。

输出

此子命令将在出现以下任一情况时生成错误输出：

- 无效的语法、组名、对象名称、索引或其它无效的数据库组成部分
- racadm CLI 故障

该子命令将返回一则提示，注明 **.cfg** 文件中的对象总数，以及其中被写入的配置对象的数量。

示例

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100`

  设置 **cfgNicIpAddress** 配置参数（对象）为值 10.35.10.110。此 IP 地址对象包含在 **cfgLanNetworking** 组中。

- racadm config -f myrac.cfg

  配置或重新配置 iDRAC6。**myrac.cfg** 文件可以从 **getconfig** 命令创建。只要遵循分析规则，也可以手动编辑 **myrac.cfg** 文件。

  注： **myrac.cfg** 文件中未包含密码信息。要在文件中包含此信息，则必须手动输入。如果您想在配置期间从 **myrac.cfg** 文件中删除密码信息，请使用 **-p** 选项。

---

getconfig

getconfig 子命令说明

getconfig 子命令允许用户分别检索 iDRAC6 配置参数，或者检索所有的 iDRAC6 配置组并保存到文件中。

输入

表 A-6 说明了 **getconfig** 子命令选项。

注： 未指定文件的 **-f** 选项会将文件内容输出到终端屏幕。

表 A-6. getconfig 子命令选项

选项	说明
-f	**-f <*文件名*>** 选项会指示 getconfig 将整个 iDRAC6 配置写入配置文件。此文件可用于通过 **config** 子命令进行批配置操作。 **注：** **-f** 选项不会为 **cfgIpmiPet** 和 **cfgIpmiPef** 组创建条目。必须至少设置一个陷阱目标以将 **cfgIpmiPet** 组捕获到文件中。
-g	**-g <*组名*>** 或**组**选项可以用于显示单个组的配置。组**名**为 **racadm.cfg** 文件中所使用的组的名称。如果组为索引组，则使用 **-i** 选项。
-h	**-h** 或 **help** 选项显示可以使用的所有可用配置组的列表。如果用户不记得确切的组名，此选项将十分有用。
-i	**-i <*索引*>**（即**索引**选项）只对索引组有效并且可用于指定唯一组。<*索引*> 是从 1 至 16 的十进制整数。如果没有指定 **-i <*索引*>**，将假设组的值为 1，表示具有多个条目的表。索引由索引值指定，不由"命名的"值指定。
-o	-o **<*对象名*>**，或对象选项，指定在查询中使用的对象名称。此选项是可选的，并可与 -g 选项一起使用。
-u	**-u <*用户名*>**（即**用户名**选项）可用于显示指定用户的配置。**<*用户名*>** 选项为该用户的登录名称。
-v	**-v** 选项显示所显示属性的其它详情，并与 **-g** 选项一起使用。

输出

此子命令将在出现以下任一情况时生成错误输出：

- 无效的语法、组名、对象名、索引或其它无效的数据库组成部分
- racadm CLI 传送故障

如果没有遇到错误，此子命令将显示指定配置的内容。

示例

- racadm getconfig -g cfgLanNetworking

  显示组 **cfgLanNetworking** 中包含的所有配置属性（对象）。

- racadm getconfig -f myrac.cfg

  将所有组配置对象从 iDRAC6 保存到 **myrac.cfg**。

- racadm getconfig -h

  显示 iDRAC6 上可用配置组的列表。

- racadm getconfig -u root

  显示用户命名为 root 的配置属性。

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  显示索引 2 处的用户组实例，并提供属性值的详细信息。

提要

`racadm getconfig -f <文件名>`

`racadm getconfig -g <组名> [-i <索引>]`

`racadm getconfig -u <用户名>`

`racadm getconfig -h`

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

coredump

注： 要使用此命令，必须具有**"Execute Debug Commands"（执行调试命令）**权限。

表 A-7 说明了 **coredump** 子命令。

表 A-7. coredump

子命令	定义
coredump	显示最后一次 iDRAC6 信息转储。

提要

`racadm coredump`

说明

coredump 子命令显示有关 RAC 最近出现的重要问题的详细信息。coredump 信息可用于诊断这些重要问题。

如果出现的话，coredump 信息在整个 iDRAC6 关机后再开机过程中都保持不变，并且只有在出现以下某种情况时才会清除：

- 使用 **coredumpdelete** 子命令清除 coredump 信息。
- 在 RAC 上出现其它重要情况。如果出现这种情况，coredump 信息将与最新出现的严重错误相关。

请参阅 **coredumpdelete** 子命令了解有关清除 **coredump** 的详情。

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

coredumpdelete

注： 要使用此命令，必须具有**"Clear Logs"（清除日志）**或**"Execute Debug Commands"（执行调试命令）**权限。

表 A-8 说明了 **coredumpdelete** 子命令。

表 A-8. coredumpdelete

子命令	定义
coredumpdelete	删除 iDRAC6 中存储的信息转储。

提要

```
racadm coredumpdelete
```

说明

coredumpdelete 子命令可用于清除 RAC 中最近存储的 **coredump** 数据。

注： 如果发出 **coredumpdelete** 命令并且 RAC 中没有存储任何 coredump，此命令将会显示一条成功信息。这是预期的行为。

请参阅 **coredump** 子命令查看 coredump 的有关详情。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

fwupdate

注： 要使用此命令，必须具有**"Configure iDRAC6"（配置 iDRAC6）**权限。

注： 开始固件更新前，请参阅"高级 iDRAC6 配置"了解其它信息。

表 A-9 说明了 **fwupdate** 子命令。

表 A-9. fwupdate

子命令	定义
fwupdate	更新 iDRAC6 上的固件

提要

```
racadm fwupdate -s

racadm fwupdate -g -u -a <TFTP_服务器_IP_地址> [-d <路径>]

racadm fwupdate -p -u -d <路径>

racadm fwupdate -r
```

说明

fwupdate 子命令使用户能够更新 iDRAC6 上的固件。用户可以：

- 检查固件更新过程状态
- 通过提供 IP 地址和可选路径从 TFTP 服务器更新 iDRAC6 固件
- 使用本地 RACADM 从本地文件系统更新 iDRAC6 固件
- 回滚到待机固件

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

输入

表 A-10 说明了 **fwupdate** 子命令选项。

注： **-p** 选项只在本地 RACADM 中受支持，并且不受远程或 serial/telnet/ssh 控制台支持。**-p** 选项在 Linux 操作系统中也不受支持。

表 A-10. fwupdate 子命令选项

选项	说明
-u	**"update"（更新）**选项，对固件更新文件执行校验和，并启动实际更新进程。此选项可与 **-g** 或 **-p** 选项配合使用。在更新结束后，iDRAC6 会执行软重设。
-s	**"status"（状态）**选项，返回所在更新进程中的当前状态。此选项始终为自动运行。
-g	**"get"（获取）**选项指示固件从 TFTP 服务器获取固件更新文件。用户还必须指定 **-a** 和 **-d** 选项。如果没有 **-a** 选项，则使用属性 **cfgRhostsFwUpdateIpAddr** 和 **cfgRhostsFwUpdatePath** 从 **cfgRemoteHosts** 组中包含的属性读取默认设置。
-a	**"IP Address"（IP 地址）**选项指定 TFTP 服务器的 IP 地址。
-d	**-d**（即**目录**）选项指定固件更新文件在 TFTP 服务器或 iDRAC6 主机服务器上所在的目录。
-p	**-p**（即**放置**）选项可用于从 Managed System 向 iDRAC6 更新固件文件。**-u** 选项必须与 **-p** 选项配合使用。
-r	**"rollback"（回滚）**选项用于回滚到待机固件。

输出

显示信息，表明正在执行的操作。

示例

- `racadm fwupdate -g -u - a 143.166.154.143 -d <路径>`

  在本示例中，**-g** 选项指示固件从 TFTP 服务器上的位置（由 **-d** 选项指定）下载固件更新文件，该服务器位于指定的 IP 地址（由 **-a** 选项指定）。从 TFTP 服务器下载映像文件后，更新过程开始。更新完成后，iDRAC6 会重设。

- `racadm fwupdate -s`

  此选项将读取固件更新的当前状态。

- `racadm fwupdate -p -u -d <路径>`

  在本示例中，由主机的文件系统来提供更新的固件映像。

注： **-p** 选项在远程 RACADM 接口中不支持 fwupdate 子命令。Linux 操作系统上不支持通过本地路径进行远程 RACADM 固件更新。

---

getssninfo

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-11 说明了 **getssninfo** 子命令。

表 A-11. getssninfo 子命令

子命令	定义
getssninfo	从会话管理器的会话表中检索当前活动或挂起的一个或多个会话的会话信息。

提要

```
racadm getssninfo [-A] [-u <用户名> | *]
```

说明

getssninfo 命令会返回已连接到 iDRAC6 的用户的列表。摘要信息提供了以下信息：

- "Username"（用户名）
- "IP address"（IP 地址）（如果可用）
- "Session type"（会话类型）（例如，Serial 或 Telnet）
- "Consoles in use"（使用的控制台）（例如，虚拟介质或虚拟 KVM)

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

输入

表 A-12 说明了 **getssninfo** 子命令选项。

表 A-12. getssninfo 子命令选项

选项	说明
-A	**-A** 选项可取消打印数据标头。
-u	**-u <用户名>** 选项将显示输出限制为只显示所给用户名的详细会话记录。如果将 "*" 符号作为所给用户名，则列出所有用户。指定此选项时将不打印摘要信息。

示例

- racadm getssninfo

表 A-13 提供了一个从 **racadm getssninfo** 命令输出的示例。

表 A-13. getssninfo 子命令输出示例

用户	IP 地址	类型	控制台
root	192.168.0.10	Telnet	虚拟 KVM

- racadm getssninfo -A

  "root" "143.166.174.19" "Telnet" "NONE"

- racadm getssninfo -A -u *

  "root" "143.166.174.19" "Telnet" "NONE"

  "bob" "143.166.174.19" "GUI" "NONE"

---

getsysinfo

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-14 说明了 **racadm getsysinfo** 子命令。

表 A-14. getsysinfo

命令	定义
getsysinfo	显示 iDRAC6 信息、系统信息和监护程序状态信息。

提要

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6] [-r]
```

说明

getsysinfo 子命令显示了有关 RAC、Managed System 和监督配置的信息。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

输入

表 A-15 说明了 **getsysinfo** 子命令选项。

表 A-15. getsysinfo 子命令选项

选项	说明
-4	显示 IPv4 设置
-6	显示 IPv6 设置
-c	显示常见设置
-d	显示 iDRAC6 信息
-s	显示系统信息
-w	显示监督信息
-A	消除打印页眉/标签

如果没有指定 **-w** 选项，则使用其它选项作为默认值。

输出

getsysinfo 子命令显示了有关 RAC、Managed System 和监督配置的信息。

示例输出

```
RAC Information（RAC 信息）:
RAC Date/Time（RAC 日期/时间）= 10/01/2008 09:39:53
Firmware Version（固件版本）= 0.32
Firmware Build（固件版次）= 55729
Last Firmware Update（上次固件更新）= 09/25/2008 18:08:31
Hardware Version（硬件版本）= 0.01
MAC Address（MAC 地址）= 00:1e:c9:b2:c7:1f

常见设置:
Register DNS RAC Name（注册 DNS RAC 名称）= 0
DNS RAC Name（DNS RAC 名称）= iDRAC6
Current DNS Domain（当前 DNS 域）=
Domain Name from DHCP（来自 DHCP 的域名）= 0

IPv4 设置:
Enabled（已启用）= 1
Current IP Address（当前 IP 地址）= 192.168.0.120
Current IP Gateway（当前 IP 网关）= 192.168.0.1
```

```
Current IP Netmask（当前 IP 网络掩码）= 255.255.255.0
DHCP Enabled（DHCP 已启用）= 0
Current DNS Server 1（当前 DNS 服务器 1）= 0.0.0.0
Current DNS Server 2（当前 DNS 服务器 2）= 0.0.0.0
DNS Servers from DHCP（来自 DHCP 的 DNS 服务器）= 0

IPv6 设置：
Enabled（已启用）= 0
Current IP Address 1（当前 IP 地址）= 2002:0000:0000::0001
Current IP Gateway（当前 IP 网关）= ::
Prefix Length（前缀长度）= 64
Autoconfig（自动配置）= 1
DNS Server from DHCPv6（从 DHCPv6 获得 DNS 服务器）= 0
Current DNS Server 1（当前 DNS 服务器 1）= ::
Current DNS Server 2（当前 DNS 服务器 2）= ::

系统信息：
System Model（系统型号）= PowerEdge 2800
System BIOS Version（系统 BIOS 版本）= 0.2.4
BMC Firmware Version（BMC 固件版本）= 0.32
Service Tag（服务标签）= AC056
Host Name（主机名）=
OS Name（操作系统名称）=
Power Status（电源状态）= ON

Watchdog information（监督信息）：
Recovery Action（恢复操作）= None
Present countdown value（当前倒计数值）= 15 seconds
Initial countdown value（初始倒计数值）= 15 seconds
```

示例

- `racadm getsysinfo -A -s`

  `"系统信息:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "主机名"`

  `"Microsoft Windows 2000 版本 5.0, 版次号 2195, Service Pack 2" "ON"`

- `racadm getsysinfo -w -s`

```
系统信息：
System Model（系统型号）= PowerEdge 2900
System BIOS Version（系统 BIOS 版本）= 0.2.3
BMC Firmware Version（BMC 固件版本）= 0.17
Service Tag（服务标签）= 48192
Host Name（主机名）= racdev103
OS Name（操作系统名称）= Microsoft Windows Server 2003
Power Status（电源状态）= OFF


Watchdog information（监督信息）：
Recovery Action（恢复操作）= None
Present countdown value（当前倒计数值）= 0 seconds
Initial countdown value（初始倒计数值）= 0 seconds
```

限制

只有 Managed System 上装有 Dell™ OpenManage™ 系统软件时，**getsysinfo** 输出中的"Hostname"（主机名）和"OS Name"（操作系统名称）字段才会显示准确的信息。如果 Managed System 上没有安装 OpenManage，这些字段将会为空白或显示错误的信息。

---

getractime

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-16 说明了 **getractime** 子命令。

表 A-16. getractime

子命令	定义
getractime	显示 Remote Access Controller 的当前时间。

提要

```
racadm getractime [-d]
```

说明

如果不带选项，**getractime** 子命令会以通用可读格式显示时间。

使用 **-d** 选项时，**getractime** 会以如下格式显示时间，*yyyymmddhhmmss.mmmmmms*，这与 UNIX **date** 命令返回的格式相同。

输出

getractime 子命令将输出显示在一行上。

示例输出

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

ifconfig

注： 要使用此命令，必须具有**"Execute Diagnostic Commands"（执行诊断命令）**或**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-17 说明了 **ifconfig** 子命令。

表 A-17. ifconfig

子命令	定义
ifconfig	显示网络接口表的内容。

提要

```
racadm ifconfig
```

---

netstat

注： 要使用此命令，必须具有**"Execute Diagnostic Commands"（执行诊断命令）**权限。

表 A-18 说明了 **netstat** 子命令。

表 A-18. netstat

子命令	定义
netstat	显示路径选择表和当前连接。

提要

```
racadm netstat
```

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

ping

注： 要使用此命令，必须具有**"Execute Diagnostic Commands"（执行诊断命令）**或**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-19 说明了 **ping** 子命令。

表 A-19. ping

子命令	定义
ping	验证目标 IP 地址是否可以使用当前路径选择表内容从 iDRAC6 进行访问。需要目标 IP 地址。ICMP 回音数据包根据当前的路径选择表内容会被发送到目标 IP 地址。

提要

```
racadm ping <ip 地址>
```

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

setniccfg

注： 要使用 **setniccfg** 命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-20 说明了 **setniccfg** 子命令。

表 A-20. setniccfg

子命令	定义
setniccfg	设置控制器的 IP 配置。

注： NIC 和以太网管理端口这两个术语可以互换使用。

提要

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <IPv4 地址> <网络掩码> <IPv4 网关>

racadm setniccfg -s6 <IPv6 地址> <IPv6 前缀长度> <IPv6 网关>

racadm setniccfg -o
```

说明

setniccfg 子命令设置控制器 IP 地址。

- **-d** 选项为以太网管理端口启用 DHCP（默认是禁用 DHCP）。
- **-d6** 选项为以太网管理端口启用"AutoConfig"（自动配置）。默认为启用。
- **-s** 选项可启用静态 IP 设置。IPv4 地址、网络掩码和网关可以指定。否则，会使用现有的静态设置。*<IPv4 地址>*、*<网络掩码>* 和 *<网关>* 必须键入为点分隔的字符串。
- **-s6** 选项可启用静态 IPv6 设置。IPv6 地址、前缀长度和 IPv6 网关可以指定。
- **-o** 选项完全禁用以太网管理端口。

输出

如果操作没有成功，**setniccfg** 子命令会显示相应的错误信息。如果成功，将会显示信息。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

getniccfg

注： 要使用 **getniccfg** 命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-21 说明了 **setniccfg** and **getniccfg** 子命令。

表 A-21. setniccfg/getniccfg

子命令	定义
getniccfg	显示控制器的当前 IP 配置。

提要

```
racadm getniccfg
```

说明

getniccfg 子命令显示当前以太网管理端口设置。

示例输出

如果操作没有成功，**getniccfg** 子命令会显示相应的错误信息。如果操作成功，输出会按下面的格式显示：

```
NIC Enabled（NIC 已启用）= 1

DHCP Enabled（DHCP 已启用）= 1

IP Address（IP 地址）= 192.168.0.1

Subnet Mask（子网掩码）= 255.255.255.0

Gateway（网关）= 192.168.0.1
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

getsvctag

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-22 说明了 **getsvctag** 子命令。

表 A-22. getsvctag

子命令	定义
getsvctag	显示服务标签。

提要

```
racadm getsvctag
```

说明

getsvctag 子命令显示主机系统的服务标签。

示例

在命令提示符下键入 `getsvctag`。输出显示如下：

```
Y76TP0G
```

命令在成功时返回 `0`，在错误时返回非零值。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

racdump

注： 要使用此命令，必须具有**"Debug"（调试）**权限。

表 A-23 说明了 **racdump** 子命令。

表 A-23. racdump

子命令	定义
racdump	显示状态和 iDRAC6 的一般信息。

提要

```
racadm racdump
```

说明

racdump 子命令提供的单个命令可以获取转储、状态和 iDRAC6 板的一般信息。

运行 **racdump** 子命令时会显示以下信息：

- 常规系统/RAC 信息
- 信息转储
- 会话信息
- 进程信息
- 固件版次信息

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

racreset

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-24 说明了 **racreset** 子命令。

表 A-24. racreset

子命令	定义
racreset	重设 iDRAC6。

注： 发出 racreset 子命令后，iDRAC6 可能需要长达一分钟来返回可用状态。

提要

```
racadm racreset [hard | soft]
```

说明

racreset 子命令发出对 iDRAC6 的重设。重设事件会写入 iDRAC6 日志。

硬重设会对 RAC 执行深层重设操作。硬重设只应作为恢复 RAC 的最后尝试的手段。

注： 按表 A-25 中所述执行 iDRAC6 硬重设后，必须重新引导系统。

表 A-25 说明了 **racreset** 子命令选项。

表 A-25. racreset 子命令选项

选项	说明
hard	*硬*重设会对 Remote Access Controller 执行深层重设操作。硬重设只应作为重设 iDRAC6 控制器的最后尝试的手段。
soft	*软*重设会对 RAC 执行正常重新引导操作。

示例

- `racadm racreset`

  启动 iDRAC6 软重设序列。

- `racadm racreset hard`

  启动 iDRAC6 硬重设序列。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

racresetcfg

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-26 说明了 **racresetcfg** 子命令。

表 A-26. racresetcfg

子命令	定义
racresetcfg	将全部 iDRAC6 配置重设为工厂默认值。

提要

```
racadm racresetcfg
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

说明

racresetcfg 命令将删除所有已由用户配置的数据库属性条目。数据库具有所有条目的默认属性，这些属性用于将控制器恢复为原始默认设置。重设数据库属性后，iDRAC6 会自动重设。

注： 此命令会删除当前 iDRAC6 配置并将 iDRAC6 和串行配置重设为原始默认设置。重设后，默认名称和密码会分别变为 **root** 和 **calvin**，而 IP 地址会变为 192.168.0.120。如果从网络客户端（例如，支持的 Web 浏览器、telnet/ssh 或远程 RACADM）发出 **racresetcfg**，则必须使用默认的 IP 地址。

注： 重设为默认完成后，某些 iDRAC6 固件进程需要停止并重新启动。iDRAC6 将有大约 30 秒的不响应时间，直到本操作完成。

---

serveraction

注： 要使用此命令，必须具有**"Execute Server Control Commands"（执行服务器控制命令）**权限。

表 A-27 说明了 **serveraction** 子命令。

表 A-27. serveraction

子命令	定义
serveraction	对 Managed System 执行重设或开机/关机/关机后再开机操作。

提要

```
racadm serveraction <操作>
```

说明

serveraction 子命令使用户能够在主机系统上执行电源管理操作。 表 A-28 说明了 **serveraction** 电源控制选项。

表 A-28. serveraction 子命令选项

字符串	定义
<*操作***>**	指定操作。以下为 <*操作*> 字符串的选项： • **powerdown** — 关闭 Managed System 电源。 • **powerup** — 打开 Managed System 电源。 • **powercycle** — 在 Managed System 上发出关机后再开机操作。此操作类似于按下系统前面板的电源按钮关闭然后再打开系统电源。 • **powerstatus** — 显示服务器的当前电源状态（"ON"[开] 或"OFF"[关]）。 • **hardreset** — 在 Managed System 上执行重设（重新引导）操作。

输出

如果无法执行所请求的操作，**serveraction** 子命令将会显示错误信息，如果成功完成操作，将会显示成功信息。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

getraclog

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-29 说明了 **racadm getraclog** 命令。

表 A-29. getraclog

命令	定义
getraclog -i	显示 iDRAC6 日志中的条目数。
getraclog	显示 iDRAC6 日志条目。

提要

```
racadm getraclog -i
```

```
racadm getraclog [-A] [-o] [-c 计数] [-s 起始记录] [-m]
```

说明

getraclog -i 命令显示 iDRAC6 日志中的条目数。

以下选项允许 **getraclog** 命令读取条目：

- **-A** — 不带页眉或标签显示输出。
- **-c** — 提供要被返回的最大条目数。
- **-m** — 一次显示一屏信息并提示用户继续（类似于 UNIX **more** 命令）。
- **-o** — 以一行显示输出。

- **-s** — 指定要显示的起始记录。

  注： 如果没有提供选项，将显示整个日志。

输出

默认输出显示有记录号、时间戳、源和说明。时间戳会从 1 月 1 日午夜开始并一直增加到系统引导。系统引导后，就会使用系统的时间戳。

示例输出

```
Record（记录）: 1
Date/Time（日期/时间）: Dec 8 08:10:11
Source（来源）: login[433]
Description（说明）: root login from 143.166.157.103
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

clrraclog

注： 要使用此命令，必须具有**"Clear Logs"（清除日志）**权限。

提要

```
racadm clrraclog
```

说明

clrraclog 子命令会从 iDRAC6 日志删除所有现有的记录。会创建一条新记录来记录清除日志的日期和时间。

---

getsel

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-30 说明了 **getsel** 命令。

表 A-30. getsel

命令	定义
getsel -i	显示系统事件日志中的条目数。
getsel	显示 SEL 条目。

提要

```
racadm getsel -i

racadm getsel [-E] [-R] [-A] [-o] [-c 计数] [-s 计数] [-m]
```

说明

getsel -i 命令显示 SEL 中的条目数。

以下 **getsel** 选项（不含 **-i** 选项）用于读取条目。

-A — 指定不带页眉或标签显示输出。

-c — 提供要被返回的最大条目数。

-o — 以一行显示输出。

-s — 指定要显示的起始记录。

-E — 将 16 字节的原始 SEL 放在每行输出的最后作为十六进制值的顺序。

-R — 只打印原始数据。

-m — 一次显示一屏信息并提示用户继续（类似于 UNIX **more** 命令）。

注： 如果没有指定参数，将显示整个日志。

输出

默认输出显示有记录号、时间戳、严重性和说明。

例如：

```
Record（记录）：1
Date/Time（日期/时间）：05-11-16 22:40:43
Severity（严重性）：Ok
Description（说明）：System Board SEL: event log sensor for System Board, log cleared was asserted
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

clrsel

注： 要使用此命令，必须具有**"Clear Logs"（清除日志）**权限。

提要

```
racadm clrsel
```

说明

clrsel 命令会从系统事件日志 (SEL) 删除所有现有的记录。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

gettracelog

注： 要使用此命令，必须具有**"Log In To iDRAC"（登录到 iDRAC）**权限。

表 A-31 说明了 **gettracelog** 子命令。

表 A-31. gettracelog

命令	定义
gettracelog -i	显示 iDRAC6 跟踪日志中的条目数。
gettracelog	显示 iDRAC6 跟踪日志。

提要

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c 计数] [-s 起始记录] [-m]
```

说明

gettracelog（不带 **-i** 选项）命令可读取条目。以下 **gettracelog** 条目用于读取条目：

-i — 显示 iDRAC6 跟踪日志中的条目数

-m — 一次显示一屏信息并提示用户继续（类似于 UNIX **more** 命令）。

-o — 以一行显示输出。

-c — 指定要显示的记录数

-s — 指定要显示的起始记录

-A — 不显示页眉或标签

输出

默认输出显示有记录号、时间戳、源和说明。时间戳会从 1 月 1 日午夜开始并一直增加到系统引导。系统引导后，就会使用系统的时间戳。

例如：

```
Record（记录）：1
```

```
Date/Time（日期/时间）：Dec 8 08:21:30
```

```
Source（源）：ssnmgrd[175]
```

```
Description（说明）：root from 143.166.157.103: session timeout sid 0be0aef4
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

sslcsrgen

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-32 说明了 **sslcsrgen** 子命令。

表 A-32. sslcsrgen

子命令	说明
sslcsrgen	从 RAC 生成并下载 SSL 证书签名请求 (CSR)。

提要

```
racadm sslcsrgen [-g] [-f <文件名>]

racadm sslcsrgen -s
```

说明

sslcsrgen 子命令可以用于生成 CSR 并将该文件下载到客户端的本地文件系统。CSR 可用来创建自定义 SSL 证书以在 RAC 上进行 SSL 事务处理。

选项

注： serial/telnet/ssh 控制台不支持 **-f** 选项。

表 A-33 说明了 **sslcsrgen** 子命令选项。

表 A-33. sslcsrgen 子命令选项

选项	说明
-g	生成新的 CSR。
-s	返回 CSR 生成过程的状态（正在生成、活动或无）。
-f	指定下载位置的文件名 <*文件名*>，CSR 将被下载至该文件。

注： 如果未指定 **-f** 选项，当前目录中的 **sslcsr** 将作为文件名默认值。

如果没有指定任何选项，默认情况下会生成 CSR 并作为 **sslcsr** 下载到本地文件系统。 **-g** 选项不能与 **-s** 选项一起使用，而 **-f** 选项只能与 **-g** 选项一起使用。

sslcsrgen -s 子命令将返回以下状态代码之一：

- CSR 成功生成。
- CSR 不存在。
- CSR 生成正在进行。

限制

sslcsrgen 子命令只能从本地或远程 RACADM 客户端执行并且不能用在 Serial、Telnet 或 SSH 接口中。

注： 生成 CSR 前，必须在 RACADM **cfgRacSecurity** 组中配置 CSR 字段。例如：racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany

示例

```
racadm sslcsrgen -s
```

或

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

sslcertupload

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-34 说明了 **sslcertupload** 子命令。

表 A-34. sslcertupload

子命令	说明
sslcertupload	将自定义 SSL 服务器或 CA 证书从客户端上载到 RAC。

提要

```
racadm sslcertupload -t <类型> [-f <文件名>]
```

选项

表 A-35 说明了 **sslcertupload** 子命令选项。

表 A-35. sslcertupload 子命令选项

选项	说明
-t	指定要上载的证书类型，CA 证书或服务器证书。 1 = 服务器证书 2 = CA 证书
-f	指定要上载的证书文件名。如果没有指定文件，将会选择当前目录中的 **sslcert** 文件。

如果成功，**sslcertupload** 命令将返回 0，不成功则返回非零数字。

限制

sslcertupload 子命令只能从本地或远程 RACADM 客户端执行。**sslcsrgen** 子命令不能用在 Serial、Telnet 或 SSH 接口中。

示例

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

支持的接口

- 本地 RACADM
- 远程 RACADM

---

sslcertdownload

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-36 说明了 **sslcertdownload** 子命令。

表 A-36. sslcertdownload

子命令	说明
sslcertupload	将 SSL 证书从 iDRAC6 下载到客户端的文件系统。

提要

```
racadm sslcertdownload -t <类型> [-f <文件名>]
```

选项

表 A-37 说明了 **sslcertdownload** 子命令选项。

表 A-37. sslcertdownload 子命令选项

选项	说明
-t	指定要下载的证书类型，即 Microsoft® Active Directory® 证书或服务器证书。 1 = 服务器证书 2 = Microsoft Active Directory 证书
-f	指定要上载的证书文件名。如果没有指定 **-f** 选项或文件名，将会选择当前目录中的 **sslcert** 文件。

如果成功，**sslcertdownload** 命令将返回 0，不成功则返回非零数字。

限制

sslcertdownload 子命令只能从本地或远程 RACADM 客户端执行。**sslcsrgen** 子命令不能用在 Serial、Telnet 或 SSH 接口中。

示例

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

支持的接口

- 本地 RACADM
- 远程 RACADM

---

sslcertview

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-38 说明了 **sslcertview** 子命令。

表 A-38. sslcertview

子命令	说明
sslcertview	显示 RAC 上存在的 SSL 服务器或 CA 证书。

提要

```
racadm sslcertview -t <类型> [-A]
```

选项

表 A-39 说明了 **sslcertview** 子命令选项。

表 A-39. sslcertview 子命令选项

选项	说明
-t	指定要查看的证书类型，即 Microsoft Active Directory 证书或服务器证书。 1 = 服务器证书

	2 = Microsoft Active Directory 证书
-A	不显示标头/标签。

输出示例

```
racadm sslcertview -t 1

Serial Number（序列号）: 00

Subject Information（主题信息）:
Country Code (CC)（国家/地区代码）: US
State (S)（州/省 [S]）: Texas
Locality (L)（地区）: Round Rock
Organization (O)（组织）: Dell Inc.
Organizational Unit (OU)（组织单位）: Remote Access Group
Common Name (CN)（常用名）: iDRAC6 default certificate（iDRAC6 默认证书）

Issuer Information（颁发者信息）:
Country Code (CC)（国家/地区代码）: US
State (S)（州/省 [S]）: Texas
Locality (L)（地区）: Round Rock
Organization (O)（组织）: Dell Inc.
Organizational Unit (OU)（组织单位）: Remote Access Group
Common Name (CN)（常用名）:iDRAC6 default certificate（iDRAC6 默认证书）

Valid From（有效期自）: Jul 8 16:21:56 2005 GMT
Valid To（有效期至）: Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 默认证书
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 默认证书
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

sslkeyupload

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-40 说明了 **sslkeyupload** 子命令。

表 A-40. sslkeyupload

子命令	说明
sslkeyupload	将 SSL 密钥从客户端上载到 DRAC6。

提要

```
racadm sslkeyupload -t <类型> [-f <文件名>]
```

选项

表 A-41 说明了 **sslkeyupload** 子命令选项。

表 A-41. sslkeyupload 子命令选项

选项	说明
-t	指定要上载的密钥。 1 = SSL 密钥用于生成服务器证书。
-f	指定要上载的 SSL 密钥文件名。

如果成功，**sslkeyupload** 命令将返回 0，不成功则返回非零数字。

限制

sslkeyupload 子命令只能从本地或远程 RACADM 客户端执行。不能用于 Serial、Telnet 或 SSH 接口。

示例

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

支持的接口

- 本地 RACADM
- 远程 RACADM

---

testemail

表 A-42 说明了 **testemail** 子命令。

表 A-42. testemail 配置

子命令	说明
testemail	检测 RAC 的电子邮件警报功能。

提要

```
racadm testemail -i <索引>
```

说明

从 iDRAC6 向指定目标发送检测电子邮件。

执行 testemail 命令前，确保 RACADM **cfgEmailAlert** 组中的指定索引已启用并正确配置。 表 A-43 提供了 **cfgEmailAlert** 组的列表和相关命令。

表 A-43. testemail 配置

操作	命令
启用警报	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
设置目标电子邮件地址	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
设置要发送到目标电子邮件地址的自定义消息	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"

确保 SNMP IP 地址配置正确	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152
查看当前电子邮件警报设置	racadm getconfig -g cfgEmailAlert -i <*索引*> 其中 <*索引*> 是一个 1 到 4 之间的数字

选项

表 A-44 说明了 **testemail** 子命令选项。

表 A-44. testemail 子命令

选项	说明
-i	指定要检测的电子邮件警报的索引。

输出

无。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

testtrap

注： 要使用此命令，必须具有**"Test Alerts"（检测警报）**权限。

表 A-45 说明了 **testtrap** 子命令。

表 A-45. testtrap

子命令	说明
testtrap	检测 RAC 的 SNMP 陷阱警报功能。

提要

```
racadm testtrap -i <索引>
```

说明

testtrap 子命令通过从 iDRAC6 向网络上的指定目标陷阱侦听程序发送检测陷阱来检测 RAC 的 SNMP 陷阱警报功能。

执行 **texttrap** 子命令前，确保 RACADM **cfgIpmiPet** 组中的指定索引正确配置。

表 A-46 提供了 **cfgIpmiPet** 组的列表和相关命令。

表 A-46. cfgEmailAlert 命令

操作	命令
启用警报	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
设置目标电子邮件 IP 地址	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
查看当前检测陷阱设置	racadm getconfig -g cfgIpmiPet -i <*索引*>

	其中 <*索引*> 是一个 1 到 4 之间的数字

输入

表 A-47 说明了 **testtrap** 子命令选项。

表 A-47. testtrap 子命令选项

选项	说明
-i	指定检测要使用的陷阱配置的索引。有效值为 1 到 4 之间的数字。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

vmdisconnect

注： 要使用此命令，必须具有**"Access Virtual Media"（访问虚拟介质）**权限。

表 A-48 说明了 **vmdisconnect** 子命令。

表 A-48. vmdisconnect

子命令	说明
vmdisconnect	关闭所有来自远程客户端的现有 iDRAC6 虚拟介质连接 。

提要

```
racadm vmdisconnect
```

说明

vmdisconnect 子命令允许用户断开另一个用户的虚拟介质会话连接。断开连接后，基于 Web 的界面将会反映正确的连接状态。只有通过使用本地或远程 RACADM 才可用。

vmdisconnect 子命令使 iDRAC6 用户能够断开所有活动的虚拟介质会话连接。通过使用 RACADM **getsysinfo** 子命令，或者可以在 iDRAC6 基于 Web 的界面中显示活动虚拟介质会话。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

vmkey

注： 要使用此命令，必须具有**"Access Virtual Media"（访问虚拟介质）**权限。

表 A-49 说明了 **vmkey** 子命令。

表 A-49. vmkey

子命令	说明
vmkey	执行虚拟介质密钥相关的操作。

提要

racadm vmkey <*操作*>

如果 <*操作*> 配置为 reset，虚拟闪速更新内存就会重设为默认大小 256 MB。

说明

将自定义虚拟介质密钥映像上载到 RAC 后，密钥大小就会变为映像大小。vmkey 子命令可用于将密钥重设回初始默认大小，在 iDRAC6 上为 256 MB。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

usercertupload

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-50 说明了 **usercertupload** 子命令。

表 A-50. usercertupload

子命令	说明
usercertupload	将用户证书或用户 CA 证书从客户端上载到 iDRAC6。

提要

racadm usercertupload -t <*类型*> [-f <*文件名*>] -i <*索引*>

选项

表 A-51 说明了 **usercertupload** 子命令选项。

表 A-51. usercertupload 子命令选项

选项	说明
-t	指定要上载的证书类型，CA 证书或服务器证书。 1 = 用户证书 2 = 用户 CA 证书
-f	指定要上载的证书文件名。如果没有指定文件，将会选择当前目录中的 **sslcert** 文件。
-i	用户的索引号。有效值为 1-16。

如果成功，**usercertupload** 命令将返回 0，不成功则返回非零数字。

限制

usercertupload 子命令只能从本地或远程 RACADM 客户端执行。

示例

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

支持的接口

- 本地 RACADM
- 远程 RACADM

---

usercertview

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-52 说明了 **usercertview** 子命令。

表 A-52. usercertview

子命令	说明
usercertview	显示 iDRAC6 上的用户证书或用户 CA 证书。

提要

```
racadm sslcertview -t <类型> [-A] -i <索引>
```

选项

表 A-53 说明了 **sslcertview** 子命令选项。

表 A-53. sslcertview 子命令选项

选项	说明
-t	指定要查看的证书类型，即用户证书或用户 CA 证书。 1 = 用户证书 2 = 用户 CA 证书
-A	不显示标头/标签。
-i	用户的索引号。有效 1-16。

支持的接口

- 本地 RACADM
- 远程 RACADM
- telnet/ssh/serial RACADM

---

localConRedirDisable

注： 只有本地 RACADM 用户可以执行此命令。

表 A-54 说明了 **localConRedirDisable** 子命令。

表 A-54. localConRedirDisable

子命令	说明
localConRedirDisable	禁用控制台重定向到 Management Station。

提要

racadm localConRedirDisable <*选项*>

如果 <*选项*> 设置为 1，控制台重定向将禁用。

如果 <*选项*> 设置为 0，控制台重定向将启用。

支持的接口

- 本地 RACADM

---

krbkeytabupload

注： 要使用此命令，必须具有**"Configure iDRAC"（配置 iDRAC）**权限。

表 A-55 说明了 **krbkeytabupload** 子命令。

表 A-55. kerbkeytabupload

子命令	说明
krbkeytabupload	上载 Kerberos keytab 文件。

提要

racadm krbkeytabupload [-f <*文件名*>]

<文件名>是包括路径的文件名称。

选项

表 A-56 说明了 **krbkeytabupload** 子命令选项。

表 A-56. kerbkeytabupload 子命令选项

选项	说明
-f	指定要上载的 keytab 文件名。如果没有指定文件，将会选择当前目录中的 keytab 文件。

如果成功，**krbkeytabupload** 命令将返回 0，不成功则返回非零数字。

限制

krbkeytabupload 子命令只能从本地或远程 RACADM 客户端执行。

示例

racadm krbkeytabupload -f *c:\keytab\krbkeytab.tab*

支持的接口

- 本地 RACADM
- 远程 RACADM

目录

目录

iDRAC6 属性数据库组和对象定义

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

iDRAC6 属性数据库包含 iDRAC6 的配置信息。数据按相关对象组织，而对象按对象组来组织。本节列出了属性数据库支持的组和对象的 ID。

借助 RACADM 公用程序使用组和对象 ID 来配置 iDRAC6。随后各节说明各个对象并指出对象是否可读、可写或可以读写。

△ **警告： Racadm 设置对象的值，而不对其执行任何功能验证。例如，RACADM 允许设置 Certificate Validation 对象为 1 而 Active Directory 对象设置为 0，即使只有在 Active Directory® 启用的情况下才进行证书验证。同样，即使 cfgADEnable 对象为 0，cfgADSSOEnable 对象也可以设置为 0 或 1，不过只有在 Active Directory 启用的情况下才生效。**

除非另外说明，所有字符串值都限于可显示 ASCII 字符。

可显示字符

可显示字符包括以下字符集：

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#$%^&*()_+-={}[]|\:";'<>,.?/
```

---

idRacInfo

该组包含显示参数以提供有关所查询 iDRAC6 的特定信息。

该组允许有一个实例。以下小节介绍该组中的对象。

idRacProductInfo（只读）

有效值

字符串，最多 63 个 ASCII 字符

默认值

Integrated Dell Remote Access Controller

说明

可标识产品的文本字符串

idRacDescriptionInfo（只读）

有效值

字符串，最多 255 个 ASCII 字符

默认值

此系统组件提供了一套完整的 Dell PowerEdge 服务器远程管理功能。

说明

iDRAC 类型的文本说明

idRacVersionInfo（只读）

有效值

字符串，最多 63 个 ASCII 字符

默认值

<当前版本号>

说明

包含当前产品固件版本的字符串

idRacBuildInfo（只读）

有效值

字符串，最多 16 个 ASCII 字符

默认值

当前 iDRAC6 固件内部版本

说明

包含当前产品内部版本的字符串

idRacName（只读）

有效值

字符串，最多 15 个 ASCII 字符

默认值

iDRAC

说明

用户指定用于标识此控制器的名称

idRacType（只读）

有效值

产品 ID

默认值

10

说明

将 Remote Access Controller 类型标识为 iDRAC6

---

cfgLanNetworking

该组包含的参数用于配置 iDRAC6 NIC。

该组允许有一个实例。该组中的某些对象可能需要重设 iDRAC6 NIC，这会导致短暂的连接中断。更改 iDRAC6 NIC IP 地址设置的对象将关闭所有活动的用户会话，并要求用户使用更新的 IP 地址设置来重新连接。

cfgNicIPv4Enable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 iDRAC6 IPv4 堆栈

cfgNicSelection（读/写）

有效值

0 = 共享

1 = 与故障转移 LOM2 共享

2 = 专用

3= 与故障转移所有 LOM 共享（仅限 iDRAC6 Enterprise）

默认值

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

说明

为 RAC 网络接口控制器 (NIC) 指定当前操作模式。 表 B-1 说明支持的模式。

表 B-1. cfgNicSelection 支持的模式

模式	说明
共享	如果主机服务器集成 NIC 与主机服务器上的 RAC 共享，则使用此模式。此模式使各个配置使用主机服务器上的相同 IP 地址和 RAC 以实现网络上的通用访问。
与故障转移 LOM2 共享	启用主机服务器 LOM2 集成网络接口控制器间的组功能。
专用	指定将 RAC NIC 用作远程访问的专用 NIC。
与故障转移所有 LOM 共享	启用主机服务器集成网络接口控制器上的所有 LOM 间的组功能。 当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1 和 NIC 2 接收数据，但是只通过 NIC 1 发送数据。从 NIC 2 到 NIC 3 然后到 NIC 4 执行故障转移。如果 NIC 4 出现故障，远程访问设备会通过故障转移，将所有数据传输转移回 NIC 1，但前提条件是 NIC 1 故障已得到修复。

cfgNicVLanEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC/BMC 的 VLAN 功能。

cfgNicVLanId（读 / 写）

有效值

1-4094

默认值

1

说明

为网络 VLAN 配置指定 VLAN ID。此属性只有在 **cfgNicVLanEnable** 设置为 **1**（已启用）时才有效。

cfgNicVLanPriority（读/写）

有效值

0 – 7

默认值

0

说明

为网络 VLAN 配置指定 VLAN 优先权。此属性只有在 cfgNicVLanEnable 设置为 1（已启用）时才有效。

cfgDNSDomainNameFromDHCP（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定 iDRAC6 DNS 域名应从网络 DHCP 服务器分配

cfgDNSDomainName（读/写）

有效值

字符串，最多 254 个 ASCII 字符。至少一个字符必须是字母。字符限制为字母数字、'-' 和 '.'。

注： Microsoft® Active Directory® 只支持不超过 64 个字节的完全限定域名 (FQDN)。

默认值

<空白>

说明

这是 DNS 域名。

cfgDNSRacName（读/写）

有效值

字符串，最多 63 个 ASCII 字符。至少一个字符必须为字母。

注： 有些 DNS 服务器只注册 31 个或更少字符的名称。

默认值

idrac-<服务标签>

说明

显示 iDRAC6 名称，默认情况下它是 rac-*服务标签*。此参数只有在 **cfgDNSRegisterRac** 设置为 1 (TRUE) 时才有效。

cfgDNSRegisterRac（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

在 DNS 服务器上注册 iDRAC6 名称

cfgDNSServersFromDHCP（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定是否应从网络上的 DHCP 服务器分配 DNS 服务器 IPv4 地址

cfgDNSServer1（读 / 写）

有效值

表示有效 IPv4 地址的字符串。例如：192.168.0.20。

默认值

0.0.0.0

说明

指定 DNS 服务器 1 的 IPv4 地址

cfgDNSServer2（读 / 写）

有效值

表示有效 IPv4 地址的字符串。例如：192.168.0.20。

默认值

0.0.0.0

说明

检索 DNS 服务器 2 的 IPv4 地址

cfgNicEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 iDRAC6 网络接口控制器。如果禁用 NIC，就不能再访问至 iDRAC6 的远程网络接口。

cfgNicIpAddress（读 / 写）

注： 此参数只有在 **cfgNicUseDhcp** 参数设置为 0 (FALSE) 时才可配置。

有效值

表示有效 IPv4 地址的字符串。例如：192.168.0.20。

默认值

192.168.0.120

说明

指定分配给 iDRAC6 的 IPv4 地址

cfgNicNetmask（读 / 写）

注： 此参数只有在 **cfgNicUseDhcp** 参数设置为 0 (FALSE) 时才可配置。

有效值

表示有效子网掩码的字符串。例如，255.255.255.0。

默认值

255.255.255.0

说明

用于 iDRAC6 IP 地址的子网掩码

cfgNicGateway（读 / 写）

注： 此参数只有在 **cfgNicUseDhcp** 参数设置为 0 (FALSE) 时才可配置。

有效值

表示有效网关 IPv4 地址的字符串。例如：192.168.0.1。

默认值

192.168.0.1

说明

iDRAC6 网关 IPv4 地址

cfgNicUseDhcp（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定是否使用 DHCP 分配 iDRAC6 IPv4 地址。如果此属性设置为 1 (TRUE)，则会从网络上的 DHCP 服务器分配 iDRAC6 IPv4 地址、子网掩码和网关。如果此属性设置为 **0** (FALSE)，用户就能配置 **cfgNicIpAddress**、**cfgNicNetmask** 和 **cfgNicGateway** 属性。

cfgNicMacAddress（只读）

有效值

表示 iDRAC6 NIC MAC 地址的字符串

默认值

iDRAC6 NIC 的当前 MAC 地址。例如，00:12:67:52:51:A3。

说明

iDRAC6 NIC MAC 地址

---

cfgRemoteHosts

此组提供允许针对电子邮件警报配置 SMTP 服务器的属性。

cfgRhostsFwUpdateTftpEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用从网络 TFTP 服务器更新 iDRAC6 固件的操作

cfgRhostsFwUpdateIpAddr（读/写）

有效值

表示有效 IPv4 地址的字符串。例如 192.168.0.61

默认值

0.0.0.0

说明

指定用于 TFTP iDRAC6 固件更新操作的网络 TFTP 服务器 IPv4 地址

cfgRhostsFwUpdatePath（读/写）

有效值

字符串，长度不超过 255 个 ASCII 字符

默认值

<空白>

说明

指定 TFTP 服务器上存在 iDRAC6 固件映像文件的 TFTP 路径。TFTP 路径相对于 TFTP 服务器上的 TFTP 根路径。

注： 服务器可能还要求您指定驱动器（例如 **C:**）。

cfgRhostsSmtpServerIpAddr（读/写）

有效值

表示有效 SMTP 服务器 IPv4 地址的字符串。例如，192.168.0.55

默认值

0.0.0.0

说明

网络 SMTP 服务器或 TFTP 服务器的 IPv4 地址。如果已配置并启用警报，SMTP 服务器会从 iDRAC6 发送电子邮件警报。TFTP 服务器与 iDRAC6 相互传送文件。

---

cfgUserAdmin

此组提供了有关那些可通过可用远程接口访问 iDRAC6 的用户的配置信息。

允许多达 16 个用户组实例。每个实例表示一个用户的配置。

cfgUserAdminIndex（只读）

有效值

1 – 16

默认值

<实例>

说明

该数字表示用户实例。

cfgUserAdminIpmiLanPrivilege（读/写）

有效值

2（用户）

3（操作员）

4（管理员）

15（无权限）

默认值

4（用户 2）

15（所有其他）

说明

IPMI LAN 信道上的最大权限

cfgUserAdminPrivilege（读/写）

有效值

0x00000000 到 0x000001ff，以及 0x0

默认值

0x00000000

说明

此属性指定允许的用户基于角色的权限。该值用位掩码来表示，允许设置各种权限值组合。 表 B-2 说明了可以为创建位掩码而组合的用户权限位值。

表 B-2. 用户权限位掩码

用户权限	权限位掩码
"Login to iDRAC"（登录到 iDRAC）	0x0000001
"Configure iDRAC"（配置 iDRAC）	0x0000002
"Configure Users"（配置用户）	0x0000004
"Clear Logs"（清除日志）	0x0000008
"Execute Server Control Commands"（执行服务器控制命令）	0x0000010
"Access Console Redirection"（访问控制台重定向）	0x0000020
"Access Virtual Media"（访问虚拟介质）	0x0000040
"Test Alerts"（检测警报）	0x0000080
"Execute Debug Commands"（执行调试命令）	0x0000100

示例

表 B-3 提供了具有一项或多项权限的用户的权限位掩码示例。

表 B-3. 用户权限位掩码示例

用户权限	权限位掩码
不允许用户访问 iDRAC。	0x00000000
用户只能登录到 iDRAC 并查看 iDRAC 和服务器配置信息。	0x00000001
用户可以登录到 iDRAC 并更改配置。	0x00000001 + 0x00000002 = 0x00000003
用户可以登录到 iDRAC、访问虚拟介质，并访问控制台重定向。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName（读/写）

注： 此属性值必须在用户名中唯一。

有效值

字符串，最多 16 个 ASCII 字符

默认值

根目录（用户 2）

<空白>（所有其他）

说明

此索引的用户名。如果索引为空，则在此名称字段中写入字符串将创建用户索引。写入双引号字符串 ("") 将删除该索引处的用户。字符串不能包含 /（正斜线）、\（反斜线）、.（句点）、@（at 符号）或问号。

注： 此属性值必须在用户名中唯一。

cfgUserAdminPassword（只写）

有效值

字符串，最多 20 个 ASCII 字符

默认值

****

说明

该用户的密码。写入此属性之后，用户密码将被加密，不能查看或显示。

cfgUserAdminEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1（用户 2）

0（所有其他）

说明

启用或禁用一个用户

cfgUserAdminSolEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

为该用户启用或禁用 LAN 上串行 (SOL) 用户访问

cfgUserAdminIpmiSerialPrivilege（读/写）

有效值

2（用户）

3（操作员）

4（管理员）

15（无权限）

默认值

4（用户 2）

15（所有其他）

说明

IPMI LAN 信道上的最大权限

---

cfgEmailAlert

此组包含用来配置 iDRAC6 电子邮件警报功能的参数。

以下小节介绍该组中的对象。允许该用户组的多达四个实例。

cfgEmailAlertIndex（只读）

有效值

1 – 4

默认值

<实例>

说明

警报实例的唯一索引

cfgEmailAlertEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用警报实例

cfgEmailAlertAddress（读 / 写）

有效值

电子邮件地址格式，最大长度为 64 个 ASCII 字符

默认值

<空白>

说明

指定电子邮件警报的目标电子邮件地址，例如 user1@company.com

cfgEmailAlertCustomMsg（读 / 写）

有效值

字符串，最多 32 个字符

默认值

<空白>

说明

指定构成警报主题的自定义信息

---

cfgSessionManagement

此组包含的参数用于配置可以连接到 iDRAC6 的会话数。

该组允许有一个实例。以下小节介绍该组中的对象。

cfgSsnMgtRacadmTimeout（读 / 写）

有效值

10 – 1920

默认值

60

说明

定义远程 RACADM 接口的空闲超时（秒）。如果远程 RACADM 会话保持不活动超过了指定会话，该会话将会关闭。

cfgSsnMgtConsRedirMaxSessions（读 / 写）

有效值

1 – 4

默认值

2

说明

指定 iDRAC6 上允许的最大控制台重定向会话数。

cfgSsnMgtWebserverTimeout（读 / 写）

有效值

60 – 10800

默认值

1800

说明

定义 Web 服务器超时。此属性设置允许连接保持空闲（没有用户输入）的时间量（秒）。如果达到了此属性设置的时间限制，就会取消会话。对此设置所做的更改不会影响当前会话；必须注销并再次登录才能使新设置生效。

cfgSsnMgtSshIdleTimeout（读 / 写）

有效值

0（无超时）

60 – 1920

默认值

300

说明

定义 SSH 空闲超时。此属性设置允许连接保持空闲（没有用户输入）的时间量（秒）。如果达到了此属性设置的时间限制，就会取消会话。对此设置所做的更改不会影响当前会话；必须注销并再次登录才能使新设置生效。

过期的 SSH 会话将显示以下错误信息：

"Connection timed out"（连接超时）

出现此信息后，系统会返回到生成 SSH 会话的 Shell。

cfgSsnMgtTelnetTimeout（读/写）

有效值

0（无超时）

60 – 1920

默认值

300

说明

定义 Telnet 空闲超时。此属性设置允许连接保持空闲（没有用户输入）的时间量（秒）。如果达到了此属性设置的时间限制，就会取消会话。对此设置的更改不会影响当前会话（必须注销并再次登录才能使新设置生效）。

过期的 Telnet 会话将显示以下错误信息：

"Connection timed out"（连接超时）

出现此信息后，系统会返回到生成 Telnet 会话的 Shell。

---

cfgSerial

此组包含 iDRAC6 服务的配置参数。

该组允许有一个实例。以下小节介绍该组中的对象。

cfgSerialBaudRate（读/写）

有效值

9600, 28800, 57600, 115200

默认值

57600

说明

设置 iDRAC6 串行端口上的波特率。

cfgSerialConsoleEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 串行控制台接口。

cfgSerialConsoleQuitKey（读 / 写）

有效值

字符串，最多 4 个字符

默认值

^\ (<Ctrl><\>)

注： "^" 是 <Ctrl> 键。

说明

在使用 **console com2** 命令时，此键或组合键会终止文本控制台重定向。**cfgSerialConsoleQuitKey** 值可以由以下某一值表示：

- 十进制值 — 例如："95"
- 十六进制值 — 例如："0x12"
- 八进制值 — 例如："007"
- ASCII 值 — 例如："^a"

  ASCII 值可以使用以下 Esc 键代码来表示：

  (a) ^ 后跟任何字母 (a-z, A-Z)

  (b) ^ 后跟列出的特殊字符：[ ] \ ^ _

cfgSerialConsoleIdleTimeout（读 / 写）

有效值

0 = 无超时

60 – 1920

默认值

300

说明

断开空闲串行会话连接前等待的最大秒数。

cfgSerialConsoleNoAuth（读 / 写）

有效值

0（启用串行登录验证）

1（禁用串行登录验证）

默认值

0

说明

启用或禁用 RAC 串行控制台登录验证。

cfgSerialConsoleCommand（读 / 写）

有效值

字符串，最多 128 个字符

默认值

<空白>

说明

指定在用户登录串行控制台接口后执行的串行命令。

cfgSerialHistorySize（读 / 写）

有效值

0 – 8192

默认值

8192

说明

指定串行历史记录缓冲区的最大大小。

cfgSerialCom2RedirEnable（读 / 写）

默认值

1

有效值

1 (TRUE)

0 (FALSE)

说明

启用或禁用控制台进行 COM 2 端口重定向。

cfgSerialSshEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 iDRAC6 上的 SSH 接口

cfgSerialTelnetEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 上的 Telnet 控制台接口

---

cfgOobSnmp

该组包含的参数用于配置 iDRAC6 的 SNMP 代理和陷阱功能。

该组允许有一个实例。以下小节介绍该组中的对象。

cfgOobSnmpAgentCommunity（读 / 写）

有效值

字符串，最多 31 个字符

默认值

public

说明

指定 SNMP 陷阱使用的 SNMP 团体名称

cfgOobSnmpAgentEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 中的 SNMP 代理

---

cfgRacTuning

此组用于配置各种 iDRAC6 配置属性，比如有效端口和安全端口限制。

cfgRacTuneConRedirPort（读 / 写）

有效值

1 – 65535

默认值

5900

说明

指定发送至 RAC 的键盘、鼠标、视频和虚拟介质通信使用的端口。

cfgRacTuneRemoteRacadmEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 iDRAC 中的远程 RACADM 接口

cfgRacTuneCtrlEConfigDisable

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用本地用户从 BIOS POST option-ROM 配置 iDRAC 的能力。

cfgRacTuneHttpPort（读 / 写）

有效值

1 – 65535

默认值

80

说明

指定用来与 iDRAC6 进行 HTTP 网络通信的端口号

cfgRacTuneHttpsPort（读 / 写）

有效值

1 – 65535

默认值

443

说明

指定用来与 iDRAC6 进行 HTTPS 网络通信的端口号

cfgRacTuneIpRangeEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 的 IPv4 地址范围验证功能

cfgRacTuneIpRangeAddr（读/写）

有效值

IPv4 地址格式的字符串，例如 192.168.0.44

默认值

192.168.1.1

说明

指定可接受的 IPv4 地址位模式，其位置由范围掩码属性 (**cfgRacTuneIpRangeMask**) 中的那些 "1" 来确定。

cfgRacTuneIpRangeMask（读/写）

有效值

IPv4 地址格式的字符串，例如 255.255.255.0

默认值

255.255.255.0

说明

带有左对齐位的标准 IP 掩码值。例如：255.255.255.0

cfgRacTuneIpBlkEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 的 IPv4 地址阻塞功能

cfgRacTuneIpBlkFailCount（读/写）

有效值

2 – 16

默认值

5

说明

在拒绝从该 IP 地址发出的登录尝试前，在特定时限 (**cfgRacTuneIpBlkFailWindow**) 内允许登录失败的最多次数

cfgRacTuneIpBlkFailWindow（读/写）

有效值

10 – 65535

默认值

60

说明

定义对失败尝试进行计数的时间长度（秒）。当达到失败尝试的限制数后，将不对失败计数。

cfgRacTuneIpBlkPenaltyTime（读/写）

有效值

10 – 65535

默认值

300

说明

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 地址发出的会话请求

cfgRacTuneSshPort（读 / 写）

有效值

1 – 65535

默认值

22

说明

指定用于 iDRAC6 SSH 接口的端口号

cfgRacTuneTelnetPort（读 / 写）

有效值

1 – 65535

默认值

23

说明

指定用于 iDRAC6 Telnet 接口的端口号

cfgRacTuneConRedirEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用控制台重定向

cfgRacTuneConRedirEncryptEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

加密控制台重定向会话中的视频

cfgRacTuneAsrEnable（读/写）

注： 此对象需要重设 iDRAC6 方可变为活动状态。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 的上次崩溃屏幕捕获功能。

cfgRacTuneDaylightOffset（读/写）

有效值

0 – 60

默认值

0

说明

为 RAC 时间指定使用的夏令时时差（分钟）。

cfgRacTuneTimezoneOffset（读/写）

有效值

– 720 – 780

默认值

0

说明

为 RAC 时间指定使用的 GMT/UTC 时区时差（分钟）

。以下显示美国的一些常见时差：

-480（PST — 太平洋标准时间）

-420（MST — 山地标准时间）

-360（CST — 中部标准时间）

-300（EST — 东部标准时间）

cfgRacTuneLocalServerVideo（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用（打开）或禁用（关闭）本地服务器视频。

cfgRacTuneLocalConfigDisable（读 / 写）

有效值

0 (TRUE)

1 (FALSE)

默认值

0

说明

将该项设置为 1，即可禁用对 iDRAC6 配置数据的写访问

cfgRacTuneWebserverEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 iDRAC Web Server。如果禁用此属性，将无法使用客户端 Web 浏览器访问 iDRAC6。此属性对于 Telnet/SSH 或 RACADM 接口无效。

---

ifcRacManagedNodeOs

此组包含说明受管服务器操作系统的有关属性。

该组允许有一个实例。以下小节介绍该组中的对象。

ifcRacMnOsHostname（只读）

有效值

字符串，最多 255 个字符

默认值

<空白>

说明

受管服务器的主机名

ifcRacMnOsOsName（只读）

有效值

字符串，最多 255 个字符

默认值

<空白>

说明

受管服务器的操作系统名称

---

cfgRacSecurity

此组用于配置与 iDRAC6 SSL 证书签名请求 (CSR) 功能相关的设置。在从 iDRAC6 生成 CSR 前，必须配置此组中的属性。

请参阅 RACADM sslcsrgen 子命令了解有关生成证书签名请求的详情。

cfgRacSecCsrCommonName（读/写）

有效值

字符串，最多 254 个字符

默认值

<空白>

说明

指定 CSR 公用名称 (CN)，必须是证书中给定的 IP 或 iDRAC 名称

cfgRacSecCsrOrganizationName（读/写）

有效值

字符串，最多 254 个字符

默认值

<空白>

说明

指定 CSR 组织名称 (O)

cfgRacSecCsrOrganizationUnit（读/写）

有效值

字符串，最多 254 个字符

默认值

<空白>

说明

指定 CSR 组织部门 (OU)

cfgRacSecCsrLocalityName（读/写）

有效值

字符串，最多 254 个字符

默认值

<空白>

说明

指定 CSR 地点 (L)

cfgRacSecCsrStateName（读 / 写）

有效值

字符串，最多 254 个字符

默认值

<空白>

说明

指定 CSR 州/省名称 (S)

cfgRacSecCsrCountryCode（读 / 写）

有效值

字符串，最多 2 个字符

默认值

<空白>

说明

指定 CSR 国家（地区）代码 (CC)

cfgRacSecCsrEmailAddr（读 / 写）

有效值

字符串，最多 254 个字符

默认值

<空白>

说明

指定 CSR 电子邮件地址

cfgRacSecCsrKeySize（读 / 写）

有效值

1024

2048

4096

默认值

1024

说明

指定 CSR 的 SSL 非对称密钥大小

---

cfgRacVirtual

该组包含的参数用于配置 iDRAC6 虚拟介质功能。该组允许有一个实例。以下小节介绍该组中的对象。

cfgVirMediaAttached（读 / 写）

有效值

0 = 分离

1 = 附加

2 = 自动附加

默认值

0

说明

此对象用于通过 USB 总线将虚拟设备连接到系统。连接设备后，服务器会识别出连接到系统的有效 USB 海量存储设备。这相当于将本地 USB CDROM/软盘驱动器连接到系统上的 USB 端口。当附加设备后，可以使用 iDRAC6 Web 界面或 CLI 远程连接至虚拟设备。将此对象设置为 **0** 会造成设备与 USB 总线分离。

cfgVirtualBootOnce（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 的虚拟介质一次引导功能。

cfgVirMediaFloppyEmulation（读 / 写）

注： 要使此更改生效，必须重新附加虚拟介质（使用 cfgVirMediaAttached）。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

如果设置为 0，Windows 操作系统会将虚拟软盘驱动器认作可移动磁盘。Windows 操作系统会在重新枚举期间分配驱动器号 C: 或更高。设置为 1 时，虚拟软盘驱动器被 Windows 操作系统认作软盘驱动器。Windows 操作系统将会分配驱动器号 A: 或 B:。

cfgVirMediaKeyEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 的虚拟介质密钥功能

---

cfgActiveDirectory

该组包含的参数用于配置 iDRAC6 Active Directory 功能。

cfgADRacDomain（读/写）

有效值

任何可打印的不超过 254 个字符的文本字符串，不含空格

默认值

<空白>

说明

iDRAC6 所在的 Active Directory 域

cfgADRacName（读/写）

有效值

任何可打印的不超过 254 个字符的文本字符串，不含空格

默认值

<空白>

说明

Active Directory 目录林中记录的 iDRAC6 的名称

cfgADEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 上的 Active Directory 用户验证。如果此属性已禁用，则仅使用本地 iDRAC6 验证进行用户登录。

cfgADSSOEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 上 Active Directory 单一登录验证。

cfgADSmartCardLogonEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 上的 Smart Card 登录。

cfgADCRLEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

为基于 Active Directory 的 Smart Card 用户启用或禁用证书撤回列表 (CRL) 检查。

cfgADDomainController1（读/写）

有效值

不超过 254 个 ASCII 字符的字符串，表示有效 IP 地址或完全限定域名 (FQDN)

默认值

<空白>

说明

iDRAC6 使用指定的值，在 LDAP 服务器中搜索用户名。

cfgADDomainController2（读/写）

有效值

不超过 254 个 ASCII 字符的字符串，表示有效 IP 地址或完全限定域名 (FQDN)

默认值

<空白>

说明

iDRAC6 使用指定的值，在 LDAP 服务器中搜索用户名。

cfgADDomainController3（读 / 写）

有效值

不超过 254 个 ASCII 字符的字符串，表示有效 IP 地址或完全限定域名 (FQDN)

默认值

<空白>

说明

iDRAC6 使用指定的值，在 LDAP 服务器中搜索用户名。

cfgADAuthTimeout（读 / 写）

有效值

15 – 300 秒

默认值

120

说明

指定等待 Active Directory 验证请求完成多少秒后便超时

cfgADType（读 / 写）

有效值

1（扩展模式）

2（标准模式）

默认值

1

说明

确定与 Active Directory 一起使用的模式类型。

cfgADGlobalCatalog1（读 / 写）

有效值

不超过 254 个 ASCII 字符的字符串，表示有效 IP 地址或完全限定域名 (FQDN)

默认值

<空白>

说明

iDRAC6 使用指定的值，在全局编录服务器中搜索用户名。

cfgADGlobalCatalog2（读 / 写）

有效值

不超过 254 个 ASCII 字符的字符串，表示有效 IP 地址或完全限定域名 (FQDN)

默认值

<空白>

说明

iDRAC6 使用指定的值，在全局编录服务器中搜索用户名。

cfgADGlobalCatalog3（读 / 写）

有效值

不超过 254 个 ASCII 字符的字符串，表示有效 IP 地址或完全限定域名 (FQDN)

默认值

<空白>

说明

iDRAC6 使用指定的值，在全局编录服务器中搜索用户名。

cfgADCertValidationEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用在 Active Directory 配置过程中执行的 Active Directory 证书验证。

---

cfgStandardSchema

该组包含的参数用于配置 Active Directory 标准模式设置。

cfgSSADRoleGroupIndex（只读）

有效值

介于 1 和 5 之间的整数

默认值

<实例>

说明

Active Directory 中记录的角色组的索引

cfgSSADRoleGroupName（读/写）

有效值

最多 254 个字符的任何可打印文本字符串。

默认值

<空白>

说明

Active Directory 目录林中记录的角色组的名称

cfgSSADRoleGroupDomain（读/写）

有效值

任何可打印的不超过 254 个字符的文本字符串，不含空格

默认值

<空白>

说明

角色组所在的 Active Directory 域

cfgSSADRoleGroupPrivilege（读/写）

有效值

0x00000000 到 **0x000001ff**

默认值

<空白>

说明

使用表 B-4 中的位掩码数字为角色组设置基于角色的权限。

表 B-4. 角色组权限的位掩码

角色组权限	位掩码
"Login to iDRAC"（登录到 iDRAC）	0x00000001
"Configure iDRAC"（配置 iDRAC）	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
"Access Console Redirection"（访问控制台重定向）	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

---

cfgIpmiSol

此组用于配置系统的 LAN 上串行 (SOL) 功能。

cfgIpmiSolEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 SOL

cfgIpmiSolBaudRate（读/写）

有效值

9600, 19200, 57600, 115200

默认值

115200

说明

LAN 上串行通信的波特率

cfgIpmiSolMinPrivilege（读/写）

有效值

2（用户）

3（操作员）

4（管理员）

默认值

4

说明

指定 SOL 访问所需的最小权限级别

cfgIpmiSolAccumulateInterval（读/写）

有效值

1 – 255

默认值

10

说明

指定一般情况下，在发送部分 SOL 字符数据包前 iDRAC6 等待的时间。该值是基于 1 的 5ms 增量。

cfgIpmiSolSendThreshold（读/写）

有效值

1 – 255

默认值

255

说明

SOL 阈值限制值。指定发送 SOL 数据包前缓冲的最大字节数。

---

cfgIpmiLan

此组用于配置系统的 LAN 上 IPMI 功能。

cfgIpmiLanEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用通过 LAN 上 IPMI 接口

cfgIpmiLanPrivilegeLimit（读/写）

有效值

2（用户）

3（操作员）

4（管理员）

默认值

4

说明

指定 LAN 上 IPMI 访问允许的最大权限级别

cfgIpmiLanAlertEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用全局电子邮件警报。此属性会覆盖所有单独的电子邮件警报启用/禁用属性。

cfgIpmiEncryptionKey（读/写）

有效值

0 到 40 个字符的十六进制数的字符串，不含空格。只允许偶数位。

默认值

00000000000000000000

说明

IPMI 密钥。

cfgIpmiPetCommunityName（读/写）

有效值

字符串，最多 18 个字符

默认值

public

说明

陷阱的 SNMP 团体名称

---

cfgIpmiPetIpv6

此组用于在受管服务器上配置 IPv6 平台事件陷阱。

cfgIpmiPetIPv6Index（只读）

有效值

1 – 4

默认值

<索引值>

说明

与陷阱对应的索引的唯一标识符

cfgIpmiPetIPv6AlertDestIpAddr

有效值

IPv6 地址

默认值

<空白>

说明

配置陷阱的 IPv6 警报目标 IP 地址

cfgIpmiPetIPv6AlertEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用陷阱的 IPv6 警报目标

---

cfgIpmiPef

此组用于配置受管服务器上的平台事件筛选器。

事件筛选器可用于控制与操作相关的策略，在受管服务器上出现重要事件时将触发这些操作。

cfgIpmiPefName（只读）

有效值

字符串，最多 255 个字符

默认值

索引筛选器的名称

说明

指定平台事件筛选器的名称

cfgIpmiPefIndex（读/写）

有效值

1 – 19

默认值

平台事件筛选器对象的索引值

说明

指定特定平台事件筛选器的索引

cfgIpmiPefAction（读/写）

有效值

0（无）

1（断电）

2（重设）

3（关机后再开机）

默认值

0

说明

指定触发警报后在受管服务器上执行的操作

cfgIpmiPefEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用特定的平台事件筛选器

---

cfgIpmiPet

此组用于在受管服务器上配置平台事件陷阱。

cfgIpmiPetIndex（只读）

有效值

1 – 4

默认值

特定平台事件陷阱的索引值

说明

与陷阱对应的索引的唯一标识符

cfgIpmiPetAlertDestIpAddr（读/写）

有效值

表示有效 IPv4 地址的字符串。例如，192.168.0.67。

默认值

0.0.0.0

说明

指定网络上陷阱接收器的目标 IPv4 地址。在受管服务器上触发事件时，陷阱接收器会接收到 SNMP 陷阱。

cfgIpmiPetAlertEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用特定陷阱

---

cfgUserDomain

此组用于配置 Active Directory 用户域名。在任何给定时间都能配置不超过 40 个域名。

cfgUserDomainIndex（只读）

有效值

1 – 40

默认值

索引值

说明

表示特定域

cfgUserDomainName（只读）

有效值

字符串，最多 255 个 ASCII 字符

默认值

<空白>

说明

指定 Active Directory 用户域名

---

cfgServerPower

此组提供几个电源管理功能。

cfgServerPowerStatus（只读）

有效值

1 (ON)

0 (OFF)

默认值

<当前服务器电源状态>

说明

表示服务器电源状态，为 ON 或 OFF

cfgServerPowerAllocation（只读）

注： 当有多个电源时，此属性表示最小容量电源。

有效值

字符串，最多 32 个字符

默认值

<空白>

说明

表示可用的供服务器使用的已分配电源

cfgServerActualPowerConsumption（只读）

有效值

字符串，最多 32 个字符

默认值

<空白>

说明

表示当前时刻服务器消耗的功率

cfgServerMinPowerCapacity（只读）

有效值

字符串，最多 32 个字符

默认值

<空白>

说明

表示最小服务器功率容量

cfgServerMaxPowerCapacity（只读）

有效值

字符串，最多 32 个字符

默认值

<空白>

说明

表示最大服务器功率容量

cfgServerPeakPowerConsumption（只读）

有效值

字符串，最多 32 个字符

默认值

<当前服务器功耗峰值>

说明

表示当前时刻之前服务器消耗的最大功率

cfgServerPeakPowerConsumptionTimestamp（只读）

有效值

字符串，最多 32 个字符

默认值

最大功耗时间戳

说明

当记录最大功耗时的时间

cfgServerPowerConsumptionClear（只写）

有效值

1 (TRUE)

0 (FALSE)

默认值

****

说明

将 cfgServerPeakPowerConsumption（读/写）属性重设为 0，将 cfgServerPeakPowerConsumptionTimestamp 属性重设为当前 iDRAC 时间。

cfgServerPowerCapWatts（读/写）

有效值

字符串，最多 32 个字符

默认值

服务器功率阈值（瓦）

说明

用瓦特表示服务器功率阈值

cfgServerPowerCapBtuhr（读/写）

有效值

字符串，最多 32 个字符

默认值

服务器功率阈值 (BTU/hr)

说明

用 BTU/hr 表示服务器功率阈值

cfgServerPowerCapPercent（读/写）

有效值

字符串，最多 32 个字符

默认值

服务器功率阈值（百分比）

说明

用百分比表示服务器功率阈值

---

cfgIPv6LanNetworking

此组用于通过 LAN 联网功能配置 IPv6。

cfgIPv6Enable

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC6 IPv6 堆栈

cfgIPv6Address1（读/写）

有效值

表示有效 IPv6 输入项的字符串

默认值

::

说明

iDRAC6 IPv6 地址

cfgIPv6Gateway（读/写）

有效值

表示有效 IPv6 输入项的字符串

默认值

::

说明

iDRAC6 网关 IPv6 地址

cfgIPv6PrefixLength（读/写）

有效值

1-128

默认值

64

说明

iDRAC6 IPv6 地址 1 的前缀长度

cfgIPv6AutoConfig（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用"IPv6 Auto Config"（IPv6 自动配置）选项

cfgIPv6LinkLocalAddress（只读）

有效值

表示有效 IPv6 输入项的字符串

默认值

::

说明

iDRAC6 IPv6 链路本地地址

cfgIPv6Address2（只读）

有效值

表示有效 IPv6 输入项的字符串

默认值

::

说明

iDRAC6 IPv6 地址

cfgIPv6DNSServersFromDHCP6（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定 cfgIPv6DNSServer1 和 cfgIPv6DNSServer2 是静态地址还是 DHCP IPv6 地址

cfgIPv6DNSServer1（读/写）

有效值

表示有效 IPv6 输入项的字符串

默认值

::

说明

IPv6 DNS 服务器地址

cfgIPv6DNSServer2（读/写）

有效值

表示有效 IPv6 输入项的字符串

默认值

::

说明

IPv6 DNS 服务器地址

---

cfgIPv6URL

此组指定用于配置 iDRAC6 IPv6 URL 的属性。

cfgIPv6URLstring（只读）

有效值

字符串，最多 80 个字符

默认值

<空白>

说明

iDRAC6 IPv6 URL

---

cfgIpmiSerial

此组指定用于配置 BMC IPMI 串行接口的属性。

cfgIpmiSerialConnectionMode（读/写）

有效值

0（终端）

1（基本）

默认值

1

说明

当 iDRAC6 **cfgSerialConsoleEnable** 属性设置为 0（已禁用）时，iDRAC6 串行端口会变成 IPMI 串行端口。此属性确定串行端口的 IPMI 定义模式。

在基本模式中，端口使用二进制数据来试图与串行客户端上的应用程序通信。在终端模式中，端口假定连有 dumb ASCII 终端并允许输入非常简单的命令。

cfgIpmiSerialBaudRate（读/写）

有效值

9600, 19200, 57600, 115200

默认值

57600

说明

指定 IPMI 上的串行连接的波特率

cfgIpmiSerialChanPrivLimit（读/写）

有效值

2（用户）

3（操作员）

4（管理员）

默认值

4

说明

指定 IPMI 串行信道上允许的最大权限级别

cfgIpmiSerialFlowControl（读/写）

有效值

0（无）

1 (CTS/RTS)

2 (XON/XOFF)

默认值

1

说明

指定 IPMI 串行端口的流控制设置

cfgIpmiSerialHandshakeControl（读/写）

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 IPMI 终端模式握手控制

cfgIpmiSerialLineEdit（读/写）

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 IPMI 串行接口上的行编辑

cfgIpmiSerialEchoControl（读/写）

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 IPMI 串行接口上的回音控制

cfgIpmiSerialDeleteControl（读/写）

有效值

0 (FALSE)

1 (TRUE)

默认值

0

说明

启用或禁用 IPMI 串行接口上的删除控制

cfgIpmiSerialNewLineSequence（读/写）

有效值

0（无）

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

默认值

1

说明

指定 IPMI 串行接口的新行序列规范

cfgIpmiSerialInputNewLineSequence（读 / 写）

有效值

0 (<ENTER>)

1 (NULL)

默认值

1

说明

指定 IPMI 串行接口的输入新行序列规范

---

cfgSmartCard

该组指定用于为使用智能卡访问 iDRAC6 的操作提供支持的属性。

cfgSmartCardLogonEnable（读 / 写）

有效值

0（已禁用）

1（已启用）

2（已启用并提供远程 RACADM）

默认值

0

说明

针对使用智能卡访问 iDRAC6 的操作执行启用、禁用，或执行启用并提供远程 RACADM 支持

cfgSmartCardCRLEnable（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用证书撤回列表 (CRL)

---

cfgNetTuning

此组使用户能够配置 RAC NIC 的高级网络接口参数。配置后，更新的设置可能需要长达一分钟才能生效。

△ **警告： 修改此组中的属性时应特别小心。不正确地修改此组中的属性会造成 RAC NIC 不能运行。**

cfgNetTuningNicAutoneg（读 / 写）

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用物理链路速度和双工的自动协商。如果为启用，则自动协商会优先于 **cfgNetTuningNic100MB** 和 **cfgNetTuningNicFullDuplex** 对象中设置的值。

cfgNetTuningNic100MB（读 / 写）

有效值

0 (10 MBit)

1 (100 MBit)

默认值

1

说明

指定 RAC NIC 使用的速度。如果 **cfgNetTuningNicAutoNeg** 设置为 **1**（已启用），则不使用此属性。

cfgNetTuningNicFullDuplex（读 / 写）

有效值

0（半双工）

1（全双工）

默认值

1

说明

指定 RAC NIC 的双工设置。如果 **cfgNetTuningNicAutoNeg** 设置为 **1**（已启用），则不使用此属性。

cfgNetTuningNicMtu（读 / 写）

有效值

576 – 1500

默认值

1500

说明

iDRAC6 NIC 所用的最大传输单位的字节大小。

目录

目录

支持的 RACADM 接口

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

下表提供了 RACADM 子命令及其相应接口支持的概览。

表 C-1. RACADM 子命令接口支持

子命令	Telnet/SSH/Serial	本地 RACADM	远程 RACADM
arp	✔	✘	✔
clearasrscreen	✔	✔	✔
clrraclog	✔	✔	✔
clrsel	✔	✔	✔
coredump	✔	✘	✔
coredumpdelete	✔	✔	✔
fwupdate	✔	✔	✔
getconfig	✔	✔	✔
getniccfg	✔	✔	✔
getraclog	✔	✔	✔
getractime	✔	✔	✔
getsel	✔	✔	✔
getssninfo	✔	✔	✔
getsvctag	✔	✔	✔
getsysinfo	✔	✔	✔
gettracelog	✔	✔	✔
help	✔	✔	✔
ifconfig	✔	✘	✔
netstat	✔	✘	✔
ping	✔	✘	✔
racdump	✔	✘	✔
racreset	✔	✔	✔
racresetcfg	✔	✔	✔
serveraction	✔	✔	✔
setniccfg	✔	✔	✔
sslcertdownload	✘	✔	✔
sslcertupload	✘	✔	✔
sslcertview	✔	✔	✔
sslcsrgen	✘	✔	✔
sslkeyupload	✘	✔	✔
testemail	✔	✔	✔
testtrap	✔	✔	✔
vmdisconnect	✔	✔	✔
vmkey	✔	✔	✔

usercertupload	✗	✓	✓
usercertview	✓	✓	✓
localConRedirDisable	✗	✓	✗
✓ = 支持; ✗ =不支持			

目录

目录

iDRAC6 概览

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

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

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

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

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

---

iDRAC6 Express 管理功能

iDRAC6 Express 提供以下管理功能：

- 动态域名系统 (DDNS) 注册
- 使用 Web 界面和 SM-CLP 命令行通过 Serial、Telnet 或 SSH 连接进行远程系统管理和监控
- 支持 Microsoft® Active Directory® 验证 — 使用扩展模式或标准模式将 iDRAC6 用户 ID 和密码集中在 Active Directory 中
- 监控 — 提供对系统信息和组件状态的访问
- 访问系统日志 — 能够访问系统事件日志、iDRAC6 日志和崩溃或无响应系统的上次崩溃屏幕，而不受操作系统状态的影响
- Dell OpenManage™ 软件集成 — 使您能够从 Dell OpenManage Server Administrator 或 Dell OpenManage IT Assistant 启动 iDRAC6 Web 界面
- iDRAC6 警报 — 通过电子邮件信息或 SNMP 陷阱提示潜在受管节点问题
- 远程电源管理 — 从管理控制台提供远程电源管理功能，比如关机和重设
- 智能平台管理接口 (IPMI) 支持
- 安全套接字层 (SSL) 加密 — 通过 Web 界面提供安全的远程系统管理
- 密码级别安全性管理 — 防止未授权访问远程系统
- 基于角色的权限 — 为不同的系统管理任务提供可分配的权限
- IPv6 支持 — 增加 IPv6 支持，例如：允许使用 IPv6 地址访问 iDRAC6 Web 界面、指定 iDRAC NIC 的 IPv6 地址、指定目标号码以配置 IPv6 SNMP 警报目标。
- WS-MAN 支持 — 使用 Web Services for Management (WS-MAN) 协议提供网络可访问管理。
- SM-CLP 支持 — 增加服务器管理命令行协议 (SM-CLP) 支持，这提供了系统管理 CLI 实施的标准。
- 固件回滚和恢复 — 允许从选定的固件映像引导或回滚到选定的固件映像。

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

---

iDRAC6 Enterprise 和 vFlash 介质

增加对 RACADM、虚拟 KVM、虚拟介质功能、专用 NIC 和虚拟闪速更新（带可选 Dell vFlash 介质卡）的支持。虚拟闪速更新允许在 vFlash 介质上保存应急引导映像和诊断工具。有关 iDRAC6 Enterprise 和 vFlash 介质的详情，请参阅 **support.dell.com\manuals** 上的*《硬件用户手册》*。

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

表 1-1. iDRAC6 功能列表

功能	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash 介质
接口和标准支持				
IPMI 2.0	✔	✔	✔	✔
基于 Web 的 GUI	✘	✔	✔	✔

SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP	✗	✓	✓	✓
RACADM 命令行	✗	✗	✓	✓
传导性				
共享/故障转移网络模式	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN 标记	✓	✓	✓	✓
IPv6	✗	✓	✓	✓
动态 DNS	✗	✓	✓	✓
专用 NIC	✗	✗	✓	✓
安全和验证				
基于角色的权限	✓	✓	✓	✓
本地用户	✓	✓	✓	✓
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	✓ [1]	✓	✓	✓
服务器功率控制	✓ [1]	✓	✓	✓
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	✗	✗	✓	✓
虚拟控制台	✗	✗	✓	✓
虚拟控制台共享	✗	✗	✓	✓
虚拟闪速更新	✗	✗	✗	✓
监视				
传感器监视和警报	✓ [1]	✓	✓	✓
实时功率监视	✗	✓	✓	✓
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	✗	✓	✓	✓

[1] - 功能只能通过 IPMI 使用，而不是通过 Web GUI 使用

✓ = 支持；✗ = 不支持

iDRAC6 提供以下安全保护功能：

- 通过 Active Directory（可选）或硬件存储的用户 ID 和密码对用户进行验证
- 基于角色的权限，使管理员能为每个用户配置特定权限
- 通过基于 Web 的界面或 SM-CLP 进行用户 ID 和密码配置
- SM-CLP 和 Web 界面支持 128 位和 40 位加密（针对某些不支持 128 位加密的国家），并使用 SSL 3.0 标准
- 通过 Web 界面或 SM-CLP 进行会话超时配置（以秒为单位）
- 可配置 IP 端口（在相应情况下）

  注： Telnet 不支持 SSL 加密技术。

- SSH，其使用加密传输层增强安全保护
- 每个 IP 地址的登录失败限制，在超过此限制时阻止来自该 IP 地址的登录
- 能够限制连接到 iDRAC6 的客户端的 IP 地址范围
- Smart Card 验证

支持的平台

有关最新的支持平台，请参阅 **support.dell.com\manuals** 和系统随附 *Dell Systems Management Tools and Documentation* DVD 上的 iDRAC6 自述文件和《*Dell 系统软件支持值表*》。

支持的操作系统

有关最新信息，请参阅 **support.dell.com\manuals** 和系统随附 *Dell Systems Management Tools and Documentation* DVD 上的 iDRAC6 自述文件和《*Dell 系统软件支持值表*》。

支持的 Web 浏览器

有关最新信息，请参阅 **support.dell.com\manuals** 和系统随附 *Dell Systems Management Tools and Documentation* DVD 上的 iDRAC6 自述文件和《*Dell 系统软件支持值表*》。

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

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

iDRAC6 端口

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

表 1-3. iDRAC6 服务器侦听端口

端口号	功能

22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	控制台重定向键盘/鼠标、虚拟介质服务、虚拟介质安全服务、控制台重定向视频
* 可配置端口	

表 1-4. iDRAC6 客户端端口

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

您可能需要的其它说明文件

除了本*《用户指南》*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。可从 Dell 支持网站 **support.dell.com\manuals** 获取这些说明文件。

- iDRAC6 联机帮助提供了有关使用基于 Web 界面的详情。
- 有关 iDRAC 硬件和系统服务配置的详情，请参阅*《Dell Unified Server Configurator 用户指南》*。
- 有关使用 IT Assistant 的信息，请参阅*《Dell OpenManage IT Assistant 用户指南》*。
- 有关安装 iDRAC6 的信息，请参阅*《硬件用户手册》*。
- 有关安装和使用 Server Administrator 的信息，请参阅*《Dell OpenManage Server Administrator 用户指南》*。
- 有关最新的支持平台、操作系统和 Web 浏览器，请参阅 iDRAC6 自述文件和*《Dell 系统软件支持值表》*。
- 有关如何获取 Dell Update Package 以及如何将其用于系统更新策略的信息，请参阅*《Dell Update Package 用户指南》*。
- 有关 iDRAC6 和 IPMI 接口的信息，请参阅*《Dell OpenManage 底板管理控制器公用程序用户指南》*。

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。
- 机架解决方案附带的*《机架安装说明》*介绍了如何将系统安装到机架中。
- *《使用入门指南》*概述了系统功能、系统设置以及技术规格。
- *《硬件用户手册》*提供了有关系统功能的信息，并说明了如何排除系统故障以及安装或更换系统组件。
- 系统管理软件说明文件介绍了软件的功能、要求、安装和基本操作。
- 操作系统说明文件介绍了如何安装（如有必要）、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

使用 WS-MAN 界面

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

支持的 CIM 配置文件

iDRAC6 固件通过使用 Web Services for Management (WS-MAN) 协议提供网络可访问管理。WS-MAN 是交换信息的传输机制。WS-MAN 为设备提供通用语言来共享数据，从而使其更易于管理。WS-MAN 是远程系统管理解决方案的重要部分，但其还有其它部分。

WS-MAN 使用 HTTPS 保持管理通信安全。客户端必须使用本地或 Microsoft® Active Directory® 用户权限登录，以验证会话。HTTPS 使用在 IP 端口 443 上的安全套接字层 (SSL)，确保通信安全。

通过 WS-MAN 提供的数据为 iDRAC6 工具界面（映射到下列分布式管理综合小组 (DMTF) 配置文件和 Dell 扩展配置文件）提供的数据子集。

用于传送基于 DMTF CIM 的管理信息是 WS-MAN 的最常见用途。CIM 定义可在 Managed System 中操作的管理信息类型。其提供客户端和服务通过电线讨论的对象。WS-MAN 指定可对管理对象执行的某些标准操作。例如，使用 WS-MAN，客户端系统可查找一组管理对象，获取管理对象的内容，并将其内容设置为新值。WS-MAN 提供管理对话的动词；CIM 类和属性是名词，而对象是动词操作针对的对象。

为确保客户端与服务之间的互操作性，DMTF 和 Dell 进一步指定各方必须了解的 CIM 类、属性和行为的标准最低 *词汇*。这些 DMTF 和 Dell 特有的配置文件定义一组所有符合标准的服务必须实施的惯例。因此，所有客户端均可以根据这些惯例正确地运行。

支持的 CIM 配置文件

表 11-1. 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. 服务处理器： 包含表示 iDRAC6 的 CIM 类定义。 **注：** 基础服务器配置文件（上述者）和服务处理器配置文件在某种意义上是独立的，其说明的对象汇集组件配置文件中定义的所有其它 CIM 对象。
3. 物理资产： 定义表示受管元素的物理方面的 CIM 类。iDRAC6 使用此配置文件表示主机服务器及其组件的 FRU 信息以及物理拓扑。
4. SM CLP 管理员域 定义表示 CLP 配置的 CIM 类。iDRAC6 使用此配置文件自行实施 CLP。
5. 电源状态管理 定义用于电源控制操作的 CIM 类。iDRAC6 使用此配置文件进行主机服务器的电源控制操作。
6. 电源设备（版本 1.1） 定义表示电源设备的 CIM 类。iDRAC6 使用此配置文件表示主机服务器的电源设备，以说明功耗（如高低功耗水印）。
7. CLP 服务 定义表示 CLP 配置的 CIM 类。iDRAC6 使用此配置文件自行实施 CLP。
8. IP 界面
9. DHCP 客户端
10. DNS 客户端
11. 以太网端口 上述配置文件定义表示网络堆栈的 CIM 类。iDRAC6 使用这些配置文件表示 iDRAC6 NIC 的配置。
12. 记录日志 定义表示不同类型的日志的 CIM 类。iDRAC6 使用此配置文件表示系统事件日志 (SEL) 和 iDRAC6 RAC 日志。
13. 软件资源清册 定义已安装或可用软件的资源清册的 CIM 类。通过 TFTP 协议，iDRAC6 使用此配置文件对当前安装的 iDRAC6 固件版本进行资源清册。
14. 基于角色授权 定义表示角色的 CIM 类。iDRAC6 使用此配置文件配置 iDRAC6 帐户权限。

15. 软件更新 定义对可用软件更新进行资源清册的 CIM 类。通过 TFTP 协议，iDRAC6 使用此配置文件对固件更新进行资源清册。
16. SMASH 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。
17. 配置文件注册 定义通告配置文件实施的 CIM 类。按本表所述，iDRAC6 使用此配置文件通告其自行实施的配置文件。
18. 基础度量 定义表示度量的 CIM 类。iDRAC6 使用此配置文件表示主机服务器说明功耗的度量（如高低功耗水印）。
19. 简单标识管理 定义表示标识的 CIM 类。iDRAC6 使用此配置文件配置 iDRAC6 帐户。
20. USB 重定向 定义表示本地 USB 端口远程重定向的 CIM 类。iDRAC6 将此配置文件与虚拟介质配置文件结合使用，以配置虚拟介质。
Dell 扩展
1. Dell® Active Directory 客户端版本 2.0.0 定义用于配置 iDRAC6 Active Directory 客户端和 Active Directory 组本地权限的 CIM 类和 Dell 扩展类。
2. Dell 虚拟介质 定义用于配置 iDRAC6 虚拟介质的 CIM 类和 Dell 扩展类。扩展 USB 重定向配置文件。
3. Dell 以太网端口 定义用于为 iDRAC6 NIC 配置 NIC 边带界面的 CIM 类和 Dell 扩展类。扩展以太网端口配置文件。
4. Dell 电源利用管理 定义表示主机服务器电源预算和配置/监测主机服务器电源预算的 CIM 类和 Dell 扩展类。

有关详情，请参阅 **www.dmtf.org/standards/profiles/**。有关配置文件列表或信息的更新，请参阅 WS-MAN 版本注释或自述文件。

WS-MAN 的实施符合 DMTF WS-MAN 规范版本 1.0.0。支持 WS-MAN 协议的已知兼容工具包括（但不限于）Microsoft Windows® 远程管理 (WinRM)、open wsman 和 wsmancli 工具。

目录

目录

使用 iDRAC6 SM-CLP 命令行界面

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节提供了有关 iDRAC6 中纳入的分布式管理综合小组 (DMTF) 的服务器管理命令行协议 (SM-CLP) 的信息。

注： 本节假定用户熟悉服务器硬件系统管理体系结构 (SMASH) 标准和 SM-CLP 规范。有关这些规范的详情，请参阅 DMTF 网站 **www.dmtf.org**。

iDRAC6 SM-CLP 是一项提供系统管理 CLI 实施标准的协议。SM-CLP 是 DMTF SMASH 标准的一部分，可跨多个平台简化服务器管理。SM-CLP 规范，与受管元件寻址规范 (Managed Element Addressing Specification) 以及 SM-CLP 映射规范配合使用，可说明各种管理任务执行的标准 verb 和目标。

---

iDRAC6 SM-CLP 支持

SM-CLP 由 DRAC6 控制器固件承载，并且支持 Telnet、SSH 和基于串行的接口。iDRAC6 SM-CLP 界面基于由 DMTF 组织提供的 SM-CLP 规范版本 1.0。iDRAC6 SM-CLP 支持表 11-1"支持 CIM 配置文件"中说明的所有配置文件。

以下各节提供了 iDRAC6 上 SM-CLP 功能的概览。

SM-CLP 功能

SM-CLP 提供了 verb 的概念，并旨在通过 CLI 提供系统管理功能。verb 表示要执行的操作，而目标确定了要运行操作的实体（或对象）。

以下是 SM-CLP 命令行语法的示例。

<verb> [<选项>] [<目标>] [<属性>]

在典型的 SM-CLP 会话期间，您可以用表 12-1 中所列的 verb 执行操作。

表 12-1. 系统支持的 CLI Verb

Verb	定义
cd	使用 shell 导航映射
set	将属性设定为特定值
help	显示指定目标的帮助
reset	重设目标
show	显示目标属性、verb 和子目标
start	打开目标
stop	关闭目标
exit	从 SM-CLP shell 会话退出
version	显示目标的版本属性
load	将二进制映像从一个 URL 地址移至指定目标地址

使用 SM-CLP

SSH（或 telnet）到 DRAC6，使用正确的凭据。

SMCLP 提示符 (/admin1->) 将会显示。

SM-CLP 目标

表 12-2 提供通过 SM-CLP 提供的目标列表，支持上述表 12-1 中所述的操作。

表 12-2. SM-CLP 目标

目标	定义
admin1	管理员域
admin1/profiles1	iDRAC6 中的注册配置文件
admin1/hdwr1	硬件
admin1/system1	Managed System 目标
admin1/system1/redundancyset1	电源设备
admin1/system1/redundancyset1/pwrsupply*	Managed System 电源设备
admin1/system1/sensors1	Managed System 传感器
admin1/system1/capabilities1	Managed System SMASH 收集功能
admin1/system1/capabilities1/ pwrcap1	Managed System 电源利用功能
admin1/system1/capabilities1/ elecap1	Managed System 目标功能
admin1/system1/logs1	记录日志收集目标
admin1/system1/logs1/log1	系统事件日志 (SEL) 记录条目
admin1/system1/logs1/log1/ record*	Managed System 上的单独 SEL 记录实例
admin1/system1/settings1	Managed System SMASH 收集设置
admin1/system1/settings1/ pwrmaxsetting1	Managed System 最大电源分配设置
admin1/system1/settings1/ pwrminsetting1	Managed System 最小电源分配设置
admin1/system1/capacities1	Managed System 容量 SMASH 收集
admin1/system1/consoles1Internet Explorer	Managed System 控制台 SMASH 收集
admin1/system1/usbredirectsap1	虚拟介质 USB 重定向 SAP
admin1/system1/usbredirectsap1/remotesap1	虚拟介质目标 USB 重定向 SAP
admin1/system1/sp1	服务处理器
admin1/system1/sp1/timesvc1	服务处理器时间服务
admin1/system1/sp1/capabilities1	服务处理器功能 SMASH 收集
admin1/system1/sp1/capabilities1/clpcap1	CLP 服务功能
admin1/system1/sp1/capabilities1/pwrmgtcap1	系统中电源状态管理服务功能
admin1/system1/sp1/capabilities1/ipcap1	IP 接口功能
admin1/system1/sp1/capabilities1/dhcpcap1	DHCP 客户端功能
admin1/system1/sp1/capabilities1/NetPortCfgcap1	网络端口配置功能
admin1/system1/sp1/capabilities1/usbredirectcap1	虚拟介质功能 USB 重定向 SAP
admin1/system1/sp1/capabilities1/vmsapcap1	虚拟介质 SAP 功能
admin1/system1/sp1/capabilities1/swinstallsvccap1	软件安装服务功能
admin1/system1/sp1/capabilities1/acctmgtcap*	帐户管理服务功能
admin1/system1/sp1/capabilities1/adcap1	Active Directory 功能
admin1/system1/sp1/capabilities1/rolemgtcap*	基于本地角色的管理功能
admin1/system1/sp1/capabilities/PwrutilmgtCap1	电源利用管理功能
admin1/system1/sp1/capabilities/metriccap1	跃点服务功能
admin1/system1/sp1/capabilities1/elecap1	多因素验证功能
admin1/system1/sp1/capabilities1/lanendptcap1	LAN（以太网端口）端点功能
admin1/system1/sp1/logs1	服务处理器日志收集
admin1/system1/sp1/logs1/log1	系统记录日志
admin1/system1/sp1/logs1/log1/record*	系统日志条目
admin1/system1/sp1/settings1	服务处理器设置收集
admin1/system1/sp1/settings1/ clpsetting1	CLP 服务设置数据
admin1/system1/sp1/settings1/ ipsettings1	IP 接口分配设置数据（静态）
admin1/system1/sp1/settings1/ ipsettings1/staticipsettings1	静态 IP 接口分配设置数据
admin1/system1/sp1/settings1/ ipsettings1/dnssettings1	DNS 客户端设置数据
admin1/system1/sp1/settings1/ ipsettings2	IP 接口分配设置数据 (DHCP)
admin1/system1/sp1/settings1/ ipsettings2/dhcpsettings1	DHCP 客户端设置数据
admin1/system1/sp1/clpsvc1	CLP 服务协议服务
admin1/system1/sp1/clpsvc1/	CLP 服务协议端点

clpendpt*	
admin1/system1/sp1/clpsvc1/ tcpendpt*	CLP 服务协议 TCP 端点
admin1/system1/sp1/jobq1	CLP 服务协议作业队列
admin1/system1/sp1/jobq1/job*	CLP 服务协议作业
admin1/system1/sp1/pwrmgtsvc1	电源状态管理服务
admin1/system1/sp1/ipcfgsvc1	IP 接口配置服务
admin1/system1/sp1/ipendpt1	IP 接口协议端点
admin1/system1/sp1/ ipendpt1/gateway1	IP 接口网关
admin1/system1/sp1/ ipendpt1/dhcpendpt1	DHCP 客户端协议端点
admin1/system1/sp1/ ipendpt1/dnsendpt1	DNS 客户端协议端点
admin1/system1/sp1/ipendpt1/ dnsendpt1/dnsserver*	DNS 客户端服务器
admin1/system1/sp1/NetPortCfgsvc1	网络端口配置服务
admin1/system1/sp1/lanendpt1	LAN 端点
admin1/system1/sp1/ lanendpt1/enetport1	以太网端口
admin1/system1/sp1/VMediaSvc1	虚拟介质服务
admin1/system1/sp1/ VMediaSvc1/tcpendpt1	虚拟介质 TCP 协议端点
admin1/system1/sp1/swid1	软件标识
admin1/system1/sp1/ swinstallsvc1	软件安装服务
admin1/system1/sp1/ account1-16	多因素验证 (MFA) 帐户
admin1/sysetm1/sp1/ account1-16/identity1	本地用户身份帐户
admin1/sysetm1/sp1/ account1-16/identity2	IPMI 身份 (LAN) 帐户
admin1/sysetm1/sp1/ account1-16/identity3	IPMI 身份（串行）帐户
admin1/sysetm1/sp1/ account1-16/identity4	CLP 身份帐户
admin1/system1/sp1/acctsvc1	MFA 帐户管理服务
admin1/system1/sp1/acctsvc2	IPMI 帐户管理服务
admin1/system1/sp1/acctsvc3	CLP 帐户管理服务
admin1/system1/sp1/group1-5	Active Directory 组
admin1/system1/sp1/ group1-5/identity1	Active Directory 身份
admin1/system1/sp1/ADSvc1	Active Directory 服务
admin1/system1/sp1/rolesvc1	本地角色基础授权 (RBA) 服务
admin1/system1/sp1/rolesvc1/ Role1-16	本地角色
admin1/system1/sp1/rolesvc1/ Role1-16/privilege1	本地角色权限
admin1/system1/sp1/rolesvc1/ Role17-21/	Active Directory 角色
admin1/system1/sp1/rolesvc1/ Role17-21/privilege1	Active Directory 权限
admin1/system1/sp1/rolesvc2	IPMI RBA 服务
admin1/system1/sp1/rolesvc2/ Role1-3	IPMI 角色
admin1/system1/sp1/rolesvc2/ Role4	IPMI LAN 上串行 (SOL) 角色
admin1/system1/sp1/rolesvc3	CLP RBA 服务
admin1/system1/sp1/rolesvc3/ Role1-3	CLP 角色
admin1/system1/sp1/rolesvc3/ Role1-3/privilege1	CLP 角色权限
admin1/system1/sp1/ pwrutilmgtsvc1	电源利用管理服务
admin1/system1/sp1/ pwrutilmgtsvc1/pwrcurr1	电源利用管理服务当前电源分配设置数据
admin1/system1/sp1/metricsvc1	跃点服务
/admin1/system1/sp1/metricsvc1/cumbmd1	累计基础跃点定义

/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	累计基础跃点数
/admin1/system1/sp1/metricsvc1/cumwattamd1	累计瓦特聚合跃点定义
/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	累计瓦特聚合跃点数
/admin1/system1/sp1/metricsvc1/cumampamd1	累计安培聚合跃点定义
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	累计安培聚合跃点数
/admin1/system1/sp1/metricsvc1/loamd1	低聚合跃点定义
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	低聚合跃点数
/admin1/system1/sp1/metricsvc1/hiamd1	高聚合跃点定义
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	高聚合跃点数
/admin1/system1/sp1/metricsvc1/avgamd1	平均聚合跃点定义
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	平均聚合跃点数

目录

目录

使用 VMCLI 部署操作系统

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

虚拟介质命令行界面 (VMCLI) 公用程序是一个命令行界面，从 Management Station 向远程系统中的 iDRAC6 提供虚拟介质功能。使用 VMCLI 和脚本化方法，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 VMCLI 公用程序集成到公司网络的信息。

准备工作

开始使用 VMCLI 公用程序前，应确保目标远程系统和公司网络符合以下各节所列的要求。

远程系统要求

iDRAC6 在各个远程系统上配置。

网络要求

网络共享必须包含以下组件：

- 操作系统文件
- 需要的驱动程序
- 操作系统引导映像文件

  映像文件必须是一个操作系统 CD，也可以是具有工业标准的可引导格式的 CD/DVD ISO 映像。

创建可引导映像文件

将映像文件部署到远程系统前，应确保所支持系统可以从该文件引导。要检测映像文件，使用 iDRAC6 Web 用户界面将映像文件传输到检测系统，然后重新引导该系统。

以下各节提供了有关为 Linux 和 Microsoft® Windows® 系统创建映像文件的特定信息。

为 Linux 系统创建映像文件

使用数据复制器 (dd) 公用程序为 Linux 系统创建可引导映像文件。

要运行该公用程序，打开命令提示符并键入以下命令：

```
dd if=<输入设备> of=<输出文件>
```

例如：

```
dd if=/dev/sdc0 of=mycd.img
```

为 Windows 系统创建映像文件

为 Windows 映像文件选择数据复制器公用程序时，选择一个复制映像文件和 CD/DVD 引导扇区的公用程序。

准备部署

配置远程系统

1. 创建可以由 Management Station 访问的网络共享。
2. 将操作系统文件复制到网络共享。
3. 如果有可引导的预配置部署映像文件将操作系统部署到远程系统，则应跳过此步骤。

   如果没有可引导的预配置部署映像文件，应创建该文件。包括任何用于操作系统部署过程的程序和/或脚本。

   例如，要部署 Windows 操作系统，映像文件可能要包括类似于 Microsoft Systems Management Server (SMS) 所用部署方法的程序。

   创建映像文件时，执行以下操作：

   - 遵循标准基于网络的安装过程
   - 将部署映像标记为"*只读*"以确保各个目标系统引导并执行相同的部署过程

- 执行以下一个过程：
  - 将 **IPMItool** 和 VMCLI 集成到现有操作系统部署应用程序。使用示例 **vm6deploy** 脚本作为使用公用程序的指南。
  - 使用现有 **vm6deploy** 脚本部署操作系统。

部署操作系统

使用 VMCLI 公用程序和该公用程序包含的 **vm6deploy** 脚本将操作系统部署到远程系统。

开始之前，应查看 VMCLI 公用程序包含的示例 **vm6deploy** 脚本。该脚本显示了将操作系统部署到网络中远程系统的详细步骤。

以下过程提供了在目标远程系统上部署操作系统的高级别概览。

1. 在 **ip.txt** 文本文件中列出将要部署的远程系统的 iDRAC6 IPv4 地址，每行一个 IPv4 地址。
2. 在客户端介质驱动器中插入可引导操作系统 CD 或 DVD。
3. 在命令行运行 **vm6deploy**。

要运行 **vm6deploy** 脚本，在命令提示符处输入以下命令：

```
vm6deploy -r ip.txt -u <idrac-用户> -p <idrac-密码> -c {<iso9660-映像> | <路径>} -f {<软盘映像>|<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、DVD 或软盘的设备路径
- *<floppy-img>* 是有效软盘映像的路径

vm6deploy 脚本将其命令行选项传递给 **VMCLI** 公用程序。请参阅"命令行选项"了解有关这些选项的详情。脚本处理 **-r** 选项与 **vmcli -r** 选项略有不同。如果 **-r** 选项的参数是现有文件的名称，脚本会从指定文件读取 iDRAC6 IPv4 地址并每行运行一次 **VMCLI** 公用程序。如果 **-r** 选项的参数不是文件名，则应是单个 iDRAC6 的地址。在这种情况下，**-r** 按 **VMCLI** 公用程序中的说明运行。

使用 VMCLI 公用程序

VMCLI 公用程序是一个可编写脚本的命令行界面，从 Management Station 向 iDRAC6 提供虚拟介质功能。

VMCLI 公用程序提供以下功能：

注： 虚拟化只读映像文件时，多个会话可能共享同一映像介质。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结
- 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。

如果操作系统支持管理员权限或操作系统特定的权限或组成员资格，还将需要管理员权限来运行 VMCLI 命令。

客户端系统的管理员控制用户组和权限，从而控制可运行公用程序的用户。

对于 Windows 系统，必须具有高级用户权限才能运行 VMCLI 公用程序。

对于 Linux 系统，可以使用 **sudo** 命令访问 VMCLI 公用程序，无需管理员权限。此命令提供集中化非管理员访问的方法并记录所有用户命令。要添加或编辑 VMCLI 组中的用户，管理员可以使用 **visudo** 命令。没有管理员权限的用户可以将 **sudo** 命令作为前缀添加到 VMCLI 命令行（或 VMCLI 脚本）来获取对远程系统上 iDRAC6 的访问和运行公用程序。

安装 VMCLI 公用程序

VMCLI 公用程序位于 *Dell Systems Management Tools and Documentation* DVD 上，该 DVD 随 Dell OpenManage System Management 软件套件提供。要安装该公用程序，请将 *Dell Systems Management Tools and Documentation* DVD 插入系统 DVD 驱动器并按照屏幕上的说明操作。

Dell Systems Management Tools and Documentation DVD 包含最新系统管理软件产品，包括诊断、存储管理、远程访问服务和 IPMItool 公用程序。此 DVD 还包含自述文件，提供最新系统管理软件产品信息。

Dell Systems Management Tools and Documentation DVD 包含 **vm6deploy** — 这是一个说明如何使用 VMCLI 和 IPMItool 公用程序将软件部署到多个远程系统的示例脚本。

注： **vm6deploy** 脚本依赖于安装时目录中存在的其它文件。如果想从另一个目录使用脚本，必须随之复制所有的文件。如果并未安装 IPMItool 公用程序，则除其它文件外，还须复制该公用程序。

命令行选项

VMCLI 界面在 Windows 和 Linux 系统上相同。

VMCLI 命令格式如下：

`VMCLI [参数] [操作_系统_shell_选项]`

命令行语法区分大小写。有关详情，请参阅"VMCLI 参数"。

如果远程系统接受了命令，并且 iDRAC6 授权连接，则命令将继续运行，直至出现以下任何一种情况：

- VMCLI 连接因任何原因终止。
- 使用操作系统控制手动终止进程。例如，在 Windows 中，可以使用任务管理器终止进程。

VMCLI 参数

IP 地址

`-r <iDRAC-IP-地址>[:<iDRAC-SSL-端口>]`

此参数提供 iDRAC6 IPv4 地址和 SSL 端口，公用程序用来与目标 iDRAC6 建立虚拟介质连接。如果输入无效 IPv4 地址或 DDNS 名称，将会显示错误信息并且终止命令。

<iDRAC-IP-地址> 是有效、唯一的 IPv4 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，将会显示错误信息并且终止命令。

iDRAC6 用户密码

`-p <iDRAC-用户-密码>`

此参数提供指定 iDRAC6 用户的密码。

如果 iDRAC6 验证失败，将会显示错误信息并且终止命令。

软盘/磁盘设备或映像文件

`-f {<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（对于 Linux 系统）；<*映像-文件*> 是有效映像文件的文件名和路径。

注： VMCLI 公用程序不支持安装点。

此参数指定提供虚拟软盘/磁盘介质的设备或文件。

例如，映像文件指定如下：

`-f c:\temp\myfloppy.img`（Windows 系统）

`-f /tmp/myfloppy.img`（Linux 系统）

如果文件没有写保护，虚拟介质将会写入映像文件。配置操作系统来写保护不应改写的软盘映像文件。

例如，设备指定如下：

`-f a:\`（Windows 系统）

`-f /dev/sdb4 # 4th partition on device /dev/sdb`（Linux 系统）

注： Red Hat® Enterprise Linux® 版本 4 不提供且将不提供对多个 LUN 的支持。然而内核支持此功能，但必须按下列步骤启用 Red Hat Enterprise Linux 版本 4 来识别含多个 LUN 的 SCSI 设备：

1. 编辑 **/etc/modprobe.conf** 并添加以下行：
   options scsi_mod max_luns=8
   （可以指定 8 个或大于 1 的任意数量的 LUN。）

2. 在命令行键入以下命令，获取内核映像的名称：

   uname -r

3. 转至 **/boot** 目录，删除步骤 2 中所指定名称的内核映像文件，名称为：

   mkinitrd /boot/initrd-'uname -r'.img `uname -r'

4. 重新引导服务器。

5. 运行以下命令，确认已为步骤 1 中所指定的 LUN 数量添加对多个 LUN 的支持：

   cat /sys/modules/scsi_mod/max_luns

如果设备提供了写保护功能，请使用该功能确保虚拟介质不会写介质。

如果不虚拟化软盘介质，请在命令行上省略此参数。如果检测到无效值，将会显示错误信息并且会终止命令。

CD/DVD 设备或映像文件

`-c {<设备-名称> | <映像-文件>}`

其中 <*设备名称*> 是有效 CD/DVD 驱动器号（Windows 系统）或有效 CD/DVD 设备文件名（Linux 系统），<*映像文件*> 是有效 ISO-9660 映像文件的文件名和路径。

此参数指定将提供虚拟 CD/DVD-ROM 介质的设备或文件：

例如，映像文件指定如下：

`-c c:\temp\mydvd.img`（Windows 系统）

`-c /tmp/mydvd.img`（Linux 系统）

例如，设备指定如下：

`-c d:\`（Microsoft® Windows® 系统）

`-c /dev/cdrom`（Linux 系统）

如果不虚拟化 CD/DVD 介质，请在命令行上省略此参数。如果检测到无效值，将会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。

版本显示

-v

此参数用于显示 VMCLI 公用程序版本。如果没有提供其它非开关选项，此命令将会终止，但不会显示错误信息。

帮助显示

-h

此参数显示 VMCLI 公用程序参数的摘要。如果没有提供其它非开关选项，此命令将会终止，但不会显示错误。

加密的数据

-e

如果命令行中包括此参数，VMCLI 将使用 SSL 加密的信道在 Management Station 和远程系统中的 iDRAC6 之间传输数据。如果命令行中不包括此参数，数据传输将不加密。

注： 使用此选项不会在 RACADM 或 Web 界面等其它 iDRAC6 配置界面将显示的虚拟介质加密状态更改为*已启用*。

VMCLI 操作系统 Shell 选项

VMCLI 命令行中可使用以下操作系统功能：

- stderr/stdout 重定向 — 将任何打印的公用程序数据重定向至文件。

  例如，使用大于号字符 (>) 后接文件名将以 VMCLI 公用程序打印的输出覆盖指定的文件。

  注： VMCLI 公用程序不从标准输入 (**stdin**) 读取。因此不需要 **stdin** 重定向。

- 后台执行 — 默认情况下 VMCLI 公用程序在前台运行。使用操作系统的命令 Shell 功能可以使该公用程序在后台运行。例如，在 Linux 操作系统下，命令后面的 (&) 字符会使程序生成为一个新后台进程。

后一种技术在脚本程序中很有用，因为它允许脚本在为 VMCLI 命令启动新进程后继续执行（否则，脚本将保持阻止直至 VMCLI 程序终止）。当有多个 VMCLI 实例以这种方式启动，并且必须手动终止一个或多个命令实例时，使用操作系统特定的功能来列出并终止进程。

VMCLI 返回代码

每当出错时，会将文本信息（仅有英文）发送到标准错误输出。

目录

目录

配置智能平台管理接口 (IPMI)

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

配置 IPMI

本节提供有关配置和使用 iDRAC6 IPMI 接口的信息。接口包括以下：

- LAN 上 IPMI
- 串行 IPMI
- LAN 上串行

iDRAC6 完全兼容 IPMI 2.0。可以通过以下途径配置 iDRAC6 IPMI：

- 浏览器中的 iDRAC6 GUI
- 开放源代码公用程序，比如 *ipmitool*
- Dell® OpenManage® IPMI Shell，即 *ipmish*
- RACADM

有关使用 IPMI Shell (ipmish) 的详情，请参阅 **support.dell.com\manuals** 上的《*Dell OpenManage 底板管理控制器公用程序用户指南*》。

有关使用 RACADM 的详情，请参阅"远程使用 RACADM"。

使用基于 Web 的界面配置 IPMI

有关详细信息，请参阅"配置 IPMI"。

使用 RACADM CLI 配置 IPMI

1. 使用任何 RACADM 接口登录远程系统。请参阅"远程使用 RACADM"。
2. 配置 LAN 上 IPMI。

   打开命令提示符，键入以下命令并按 <Enter>：

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

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

   a. 更新 IPMI 信道权限。

      在命令提示符下，键入以下命令并按 <Enter>：

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <级别>
      ```

      其中 <*级别*> 是以下某个值：

      - 2（用户）
      - 3（操作员）
      - 4（管理员）

      例如，要设置 IPMI LAN 信道权限为 2（用户），键入以下命令：

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. 如果需要，设置 IPMI LAN 信道密钥。

   注： iDRAC6 IPMI 支持 RMCP+ 协议。有关详情，请参阅 IPMI 2.0 规范。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <密钥>
```

其中 <*密钥*> 是一个有效十六进制格式的 20 字符密钥。

3. 配置 IPMI LAN 上串行 (SOL)。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. 更新 IPMI SOL 最小权限级别。

注： IPMI SOL 最小权限级别确定了激活 IPMI SOL 所需的最小权限。有关详情，请参阅 IPMI 2.0 规范。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <级别>
```

其中 <*级别*> 是以下某个值：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要配置 IPMI 权限为 2（用户），键入以下命令：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. 更新 IPMI SOL 波特率。

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

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <波特率>
```

其中 <*波特率*> 为 9600、19200、57600 或 115200 bps。

例如：

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. 为单个用户启用 SOL。

注： 可以为每个用户启用或禁用 SOL。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2
```

其中 <*id*> 是用户的唯一 ID。

4. 配置 IPMI 串行。

a. 将 IPMI 串行连接模式更改为相应的设置。

在命令提示符下，键入以下命令并按 <Enter>：

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

b. 设置 IPMI 串行波特率。

打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <波特率>
```

其中 <*波特率*> 为 9600、19200、57600 或 115200 bps。

例如：

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. 启用 IPMI 串行硬件流控制。

在命令提示符下，键入以下命令并按 <Enter>：

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

d. 设置 IPMI 串行信道最小权限级别。

在命令提示符下，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <级别>
```

其中 *<级别>* 是以下某个值：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要设置 IPMI 串行信道权限为 2（用户），键入以下命令：

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. 确保在 BIOS 设置程序中正确设置了串行 MUX。

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

IPMI 配置完成。

如果 IPMI 串行处于终端模式，可以使用 **racadm config cfgIpmiSerial** 命令配置以下其它设置：

- 删除控制
- 回声控制
- 行编辑
- 新行序列
- 输入新行序列

有关这些属性的详情，请参阅 IPMI 2.0 规范。

使用 IPMI 远程访问串行接口

在 IPMI 串行接口中，以下模式可用：

- **"IPMI terminal mode"（IPMI 终端模式）**— 支持从串行终端提交的 ASCII 命令。命令集仅有有限的命令（包括电源控制）并支持作为十六进制 ASCII 字符输入的原始 IPMI 命令。
- **"IPMI basic mode"（IPMI 基本模式）**— 支持二进制接口以进行程序访问，比如底板管理公用程序 (BMU) 附带的 IPMI Shell (IPMISH)。

要使用 RACADM 配置 IPMI 模式：

1. 禁用 RAC 串行接口。

   在命令提示符下键入：

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

2. 启用相应的 IPMI 模式。

   例如，在命令提示符下键入：

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

有关详情，请参阅**"**iDRAC6 属性数据库组和对象定义**"**。

配置 LAN 上串行使用基于 Web 的界面

有关详细信息，请参阅"配置 IPMI"。

注： LAN 上串行可与以下 Dell OpenManage 工具一起使用：SOLProxy 和 IPMItool。有关详情，请参阅 **support.dell.com\manuals** 上的《*Dell OpenManage 底板管理控制器公用程序用户指南*》。

目录

目录

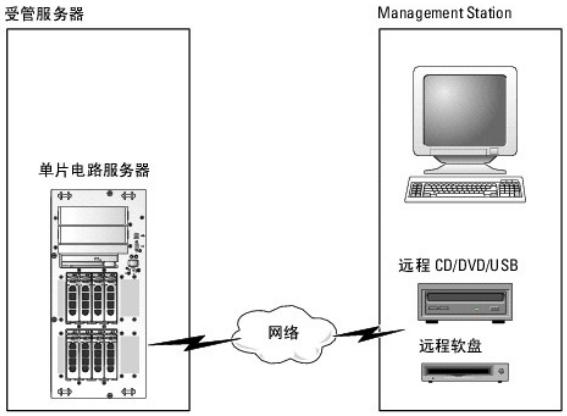
配置并使用虚拟介质

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

概览

虚拟介质功能可通过控制台重定向查看器访问，提供了受管服务器对网络上远程系统所连介质的访问。 图 15-1 显示了**虚拟介质**的整体结构。

图 15-1. 虚拟介质的整体结构



使用**虚拟介质**，管理员可以远程引导其受管服务器，安装应用程序，更新驱动程序，甚至从虚拟 CD/DVD 和软盘驱动器远程安装新操作系统。

注： **虚拟介质**至少需要 128 Kbps 的可用网络带宽。

虚拟介质为受管服务器的操作系统和 BIOS 定义了两种设备：软盘设备和光盘设备。

Management Station 通过网络提供物理介质或映像文件。附加或自动附加**虚拟介质**后，来自受管服务器的所有虚拟 CD/软盘驱动器访问请求都会通过网络定向到 Management Station。连接**虚拟介质**相当于将介质插入 Managed System 的物理设备。当**虚拟介质**处于连接状态时，Managed System 上的虚拟设备会显示为未装有介质的两个驱动器。

表 15-1 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 15-1. 支持的驱动器连接

支持的虚拟软盘驱动器连接	支持的虚拟光盘驱动器连接
带有 1.44 软盘的传统 1.44 软盘驱动器	带有 CD-ROM 介质的 CD-ROM、DVD、CDRW 组合驱动器
带有 1.44 软盘的 USB 软盘驱动器	ISO9660 格式的 CD-ROM/DVD 映像文件
1.44 软盘映像	带有 CD-ROM 介质的 USB CD-ROM 驱动器
USB 可移动磁盘	

基于 Windows 的 Management Station

要在运行 Microsoft® Windows® 操作系统的 Management Station 上运行**虚拟介质**功能，请安装支持版本的带有 Java Runtime Environment (JRE) 的 Internet Explorer 或 Firefox。有关详情，请参阅"支持的 Web 浏览器"。

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。有关详情，请参阅"支持的 Web 浏览器"。

需要安装 Java Runtime Environment (JRE) 才能运行控制台重定向插件。可以从 **java.sun.com** 下载 JRE。推荐 JRE 版本 1.6 或更高版本。

配置虚拟介质

1. 登录到 iDRAC6 Web 界面。
2. 选择**"System"（系统）→"Console/Media"（控制台/介质）**。
3. 单击**"Configuration"（配置）→"Virtual Media"（虚拟介质）**以配置虚拟介质设置。

   表 15-2 说明**虚拟介质**配置值。
4. 配置完设置后，单击**"Apply"（应用）**。
5. 单击相应按钮继续。请参阅表 15-3。

表 15-2. 虚拟介质配置属性

属性	值
远程介质连接状态	**"Attach"（附加）**- 立刻将**"Virtual Media"（虚拟介质）**附加到服务器。 **"Detach"（分离）**- 立刻从服务器上分离**"Virtual Media"（虚拟介质）**。 **"Auto-Attach"（自动附加）**- 只有当虚拟介质会话启动时才将**"Virtual Media"（虚拟介质）**附加到服务器。
"Max Sessions"（最大会话数）	显示**"Virtual Media"（虚拟介质）**会话的最大允许数目，此值始终为 1。
"Active Sessions"（激活的会话数）	显示"Virtual Media"（虚拟介质）当前会话的数目。
"Virtual Media Encryption Enabled"（虚拟介质加密已启用）	选择或取消选择此复选框以启用或禁用**"Virtual Media"（虚拟介质）**连接上的加密。如果选择，则启用加密；如果取消选择，则禁用加密。
"Floppy Emulation"（软盘仿真）	表示**"Virtual Media"（虚拟介质）**对于服务器显示为软盘驱动器还是 USB 闪存盘。如果选中**"Floppy Emulation"（软盘仿真）**，则**"Virtual Media"（虚拟介质）**设备显示为服务器上的软盘设备。如果不选中此项，则显示为 USB 闪存盘驱动器。
"Enable Boot Once"（启用引导一次）	选中此框可以启用**"Boot Once"（引导一次）**选项。使用此属性在下次引导时从虚拟介质引导；系统将从引导顺序中的下一项引导。系统引导一次后，此选项将自动终止**"Virtual Media"（虚拟介质）**会话。

表 15-3. 配置页按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的**"Configuration"（配置）**值。
"Refresh"（刷新）	重新载入**"Configuration"（配置）**页。
"Apply Changes"（应用更改）	保存**"Configuration"（配置）**页上的所有新设置。

运行虚拟介质

警告： 运行虚拟介质会话时不要发出 racreset 命令。否则可能发生意外情况，例如丢失数据。

注： 访问虚拟介质时，Console Viewer 窗口应用程序必须保持活动。

注： 执行以下步骤启用 Red Hat® Enterprise Linux®（第 4 版），以识别带多个逻辑单元 (LUN) 的 SCSI 设备：

1. 将以下行添加至 **/ect/modprobe**：

   ```
   options scsi_mod max_luns=256

   cd /boot

   mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
   ```
2. 重新引导服务器。

3. 运行以下命令以查看虚拟 CD/DVD 和/或虚拟软盘：

   cat /proc/scsi/scsi

注： 通过使用虚拟介质，在 Management Station 上只能虚拟化一个软盘/USB 驱动器/映像/闪存盘和一个光盘驱动器，用作受管服务器上的（虚拟）驱动器。

支持的虚拟介质配置

可以为一个软盘驱动器和一个光盘驱动器启用虚拟介质。对每种介质类型一次只能虚拟化一个驱动器。

支持的软盘驱动器包括软盘映像或一个可用软盘驱动器。支持光盘驱动器包括最多一个可用光盘驱动器或一个 ISO 映像文件。

连接虚拟介质

执行以下步骤以运行虚拟介质：

1. 在 Management Station 上打开支持的 Web 浏览器。有关详情，请参阅"支持的 Web 浏览器"。
2. 启动 iDRAC6 Web 界面。有关详情，请参阅"访问 Web 界面"。
3. 选择**"System"（系统）→"Console/Media"（控制台/介质）**。

   将出现**"Console Redirection and Virtual Media"（控制台重定向和虚拟介质）**页。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。可以同时选择一个光盘驱动器和一个软盘/USB 快擦写驱动器进行虚拟化。

   注： 受管服务器上的虚拟设备驱动器号与 Management Station 上的物理驱动器号不一致。

   注： **虚拟介质**可能无法在配置有 Internet Explorer Enhanced Security 的 Windows 操作系统客户端上正常运行。要解决此问题，请参阅 Microsoft 操作系统说明文件或联系系统管理员。

4. 单击**"Launch Viewer"（启动查看器）**。

   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。

   iDRAC KVM 代理应用程序会在单独窗口中启动。

5. 单击**"Tools"（工具）→"Launch Virtual Media"（启动虚拟介质）**。

   将显示"Media Redirection"（介质重定向）向导。

   注： 除非希望终止虚拟介质会话，否则请勿关闭此向导。

6. 如果介质已连接，必须断开连接，然后再连接到其它介质源。取消选中要断开连接的介质左边的框。
7. 选中要连接的介质类型旁边的框。

   如果希望连接软盘映像或 ISO 映像，输入映像的路径（在本地计算机上），或单击**"Add Image..."（添加映像...）**按钮并浏览到映像。

   介质将会连接并且**"Status"（状态）**窗口将会更新。

断开虚拟介质连接

1. 单击**"Tools"（工具）→"Launch Virtual Media"（启动虚拟介质）**。
2. 取消选中要断开连接的介质旁边的框。

   介质将会断开连接并且**"Status"（状态）**窗口将会更新。

3. 单击**"Exit"（退出）**以终止"Media Redirection"（介质重定向）向导。

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 CD 插入到 Management Station 的 CD 驱动器中。
   - 选择了本地 CD 驱动器。
   - 已与虚拟驱动器连接。
2. 按照"从虚拟介质引导"一节的步骤从虚拟介质引导以确保 BIOS 已设置为从进行安装的 CD 驱动器引导。
3. 按照屏幕上的说明完成安装。

多磁盘的安装请务必遵循以下步骤：

1. 从虚拟介质控制台取消映射虚拟化（重定向）的 CD/DVD。
2. 将下一张 CD/DVD 插入到远程光盘驱动器中。
3. 从虚拟介质控制台映射（重定向）此 CD/DVD。

   将新 CD/DVD 插入到远程光盘驱动器中而不重新映射可能会无法正常运行。

一次引导功能

一次引导功能有助于临时更改引导顺序以便从远程虚拟介质设备引导。通常在安装操作系统时，可以结合使用此功能和虚拟介质。

注： 必须有**"Configure iDRAC6"（配置 iDRAC6）**权限才能使用此功能。

注： 必须使用虚拟介质重定向远程设备才能使用此功能。

使用一次引导功能：

1. 打开服务器电源并进入 BIOS 引导管理器。
2. 将引导顺序更改为从远程虚拟介质设备引导。
3. 通过 Web 界面登录到 iDRAC6，单击**"System"（系统）→ "Console/Media"（控制台/介质）→"Configuration"（配置）**。
4. 选中虚拟介质下的**"Enable Boot Once "（启用一次引导）**选项。
5. 对服务器执行关机后再开机操作。

服务器从远程虚拟介质设备引导。服务器下次重新引导时，将断开远程虚拟介质连接。

注： 虚拟介质应处在**"Attached"（连接）**状态，虚拟驱动器才能显示在引导顺序中。确保可引导介质存在于虚拟驱动器中以启用**"Boot Once"（一次引导）**。

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（如果已附加）并配置有驱动器号。

在 Windows 中使用虚拟驱动器类似于使用物理驱动器。使用虚拟介质向导连接到介质后，只需单击该驱动器并浏览其内容就可在系统上使用该介质。

基于 Linux 的系统

根据系统上软件的配置，虚拟介质驱动器可能不自动安装。如果驱动器没有自动安装，则使用 Linux **mount** 命令手动安装驱动器。

关于虚拟介质的常见问题

表 15-4 列出常见问题和解答。

表 15-4. 使用虚拟介质：常见问题

问题	解答
有时会发现虚拟介质客户端连接中断。为什么？	出现网络超时后，iDRAC6 固件会断开连接，断开服务器和虚拟驱动器之间的链接。 如果虚拟介质配置设置在 iDRAC6 基于 Web 界面中或使用本地 RACADM 命令更改，当配置更改应用后，任何连接的介质都会断开连接。 要重新连接虚拟驱动器，使用虚拟介质向导。
哪些操作系统支持 iDRAC6？	请参阅"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之间的链接。另外，有些人会在 Web 界面或输入 RADACM 命令变更虚拟介质配置设置。要重新连接虚拟驱动器，使用**虚拟介质**功能。
通过 vMedia 安装 Windows 操作系统所用时间似乎太长了。为什么？	如果使用 *Dell Systems Management Tools and Documentation* DVD 和慢速网络连接安装 Windows 操作系统，安装过程可能会由于网络延迟而需要更多的时间访问 iDRAC6 Web 界面。虽然安装窗口没有显示安装进程，安装仍在进行。
如何将虚拟设备配置为可引导设备？	在受管服务器上，访问 BIOS 设置并单击引导菜单。找到虚拟 CD、虚拟软盘或虚拟闪速更新并根据需要更改设备引导顺序。另外，通过在 CMOS 设置的引导顺序中按"空格"键使虚拟设备可以引导。例如，要从 CD 驱动器引导，将 CD 驱动器配置为引导顺序中的第一个驱动器。
我可以从何种介质引导？	iDRAC6 允许从以下可引导介质引导： • CDROM/DVD 数据介质 • ISO 9660 映像 • 1.44 软盘或软盘映像 • 被操作系统认作可移动磁盘的 USB 闪存盘 • USB 闪存盘映像
如何使 USB 闪存盘可引导？	搜索 **support.dell.com** 寻找 Dell 引导公用程序，这是一种可以使 Dell USB 闪存盘可引导的 Windows 程序。 还可以使用 Windows 98 启动盘引导并将系统文件从启动盘复制到 USB 闪存盘。例如，从 DOS 提示符处键入以下命令： `sys a: x: /s` 其中 *x* 是要使其可引导的 USB 闪存盘。
无法在运行 Red Hat Enterprise Linux 或 SUSE® Linux 操作系统的系统上找到虚拟软盘/虚拟 CD 设备。已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 在第一步返回消息的时间戳。 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。
无法在运行 Red Hat Enterprise Linux 或 SUSE Linux 操作系统的系统上找到虚拟软盘/虚拟 CD 设备。已连接虚拟介质并且也已经连接到远程软盘。我应该怎么做？	*（解答 [续]）* 为了安装虚拟 CD 驱动器，请找到 Linux 分配给虚拟 CD 驱动器的设备节点。执行以下步骤以找到并安装虚拟 CD 驱动器： 1. 打开 Linux 命令提示符并运行以下命令： grep "Virtual CD" /var/log/messages 2. 找到该信息的最新条目并记下时间。 3. 在 Linux 提示符处运行以下命令： grep "hh:mm:ss" /var/log/messages 其中 hh:mm:ss 是 grep 在步骤 1 所返回信息的时间戳。 4. 在步骤 3 中，查看 grep 命令的结果并找到赋予 "Dell Virtual CD" 的设备名。 5. 确保已连接到虚拟 CD 驱动器。 6. 在 Linux 提示符处运行以下命令： mount */dev/sdx* /mnt/CD 其中 */dev/sdx* 是在第 4 步发现的设备名称 /mnt/floppy 是安装点。
当我使用 iDRAC6 Web 界面远程执行固件更新时，服务器上的虚拟驱动器已卸下。为什么？	固件更新造成 iDRAC6 重设，删除远程连接，并卸下虚拟驱动器。
在我连接了 USB 设备之后，所有的 USB 设备都分离了，为什么？	虚拟介质设备和虚拟闪速更新设备都是作为组合 USB 设备连接到主机 USB 总线的，且它们共享同一个 USB 端口。每当任何虚拟介质或虚拟闪速更新 USB 设备连接到主机 USB 总线或从该总线断开时，将从主机 USB 总线短暂地断开所有虚拟介质和虚拟闪速更新设备，然后重新连接这些设备。如果某个虚拟介质设备正被主机操作系统使用，必须避免附加或分离一个或多个虚拟介质或虚拟闪速更新设备。建议先连接所有必需 USB 设备，然后再使用这些设备。
USB 重设按钮有什么用？	它可重设连接到服务器的远程 USB 设备和本地 USB 设备。

目录

目录

使用 iDRAC 配置公用程序

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

概览

iDRAC 配置公用程序是一个引导前配置环境，允许您查看并设置 iDRAC6 和受管服务器的参数。具体说来，可以：

- 查看 iDRAC6 和主背板固件的固件版本号
- 启用或禁用 iDRAC6 局域网
- 启用或禁用 LAN 上 IPMI
- 配置 LAN 参数
- 配置虚拟介质
- 配置 Smart Card
- 更改管理用户名和密码
- 重设 iDRAC 配置为工厂默认值
- 查看系统事件日志 (SEL) 信息或从日志清除信息
- 配置 LCD
- 配置系统服务

使用 iDRAC 配置公用程序执行的任务也可以通过 iDRAC 或 Dell™ OpenManage™ 软件提供的其它公用程序执行，其中包括基于 Web 的界面、SM-CLP 命令行界面、本地 RACADM 命令行界面。

启动 iDRAC 配置公用程序

1. 通过按服务器正面的电源按钮打开或重新启动服务器。
2. 如果看到**"Press <Ctrl-E> for Remote Access Setup within 5 sec....."（在 5 秒内按 <Ctrl-E> 进行远程访问设置.....）** 信息，应立即按 <Ctrl><E>。

注： 如果操作系统在您按 <Ctrl><E> 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。

将显示显示 iDRAC 配置公用程序。前两行提供了有关 iDRAC6 固件和主背板固件版本的信息。在确定是否需要升级固件时，版本级别很有用。

iDRAC6 固件是信息中与外部界面（比如基于 Web 的界面、SM-CLP 和 Web 界面）相关的部分。主背板固件是固件中与服务器硬件环境交互并监测服务器硬件环境的部分。

使用 iDRAC 配置公用程序

在固件版本信息下面，iDRAC 配置公用程序的其余部分是可以用 <上箭头> 和 <下箭头> 访问的菜单项。

- 如果菜单项引出子菜单或可编辑文本字段，应按 <Enter> 访问项目，在完成配置后按 <Esc> 离开。
- 如果项目具有可选值，比如"Yes"（是）/"No"（否）或"Enabled"（已启用）/"Disabled"（已禁用），则按 <左箭头>、<右箭头> 或 <空格键> 选择一个值。
- 如果项目不可编辑，会呈蓝色显示。有些项目会根据所做的其它选择而变得可编辑。
- 屏幕底部显示当前项目的说明。可以按 <F1> 显示当前项目的帮助。
- 使用 iDRAC 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 iDRAC 配置公用程序的菜单项。

iDRAC6 LAN

使用 <左箭头>、<右箭头> 和空格键可以选择**"On"（开）**和**"Off"（关）**。

在默认配置中，iDRAC6 LAN 处于启用状态。必须启用 LAN 才能允许使用 iDRAC6 功能，比如基于 Web 的界面、Telnet/SSH、控制台重定向和虚拟介质。

如果选择禁用 LAN，以下警告将会显示：

"iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF."（如果 LAN 信道关闭，iDRAC6 带外界面将会禁用。）

Press any key to clear the message and continue.（按任意键清除信息并继续。）

该信息告诉您，在禁用 LAN 时，除了通过直接连接到 iDRAC HTTP、HTTPS、Telnet 或 SSH 端口访问的功能外，并不接收带外管理网络通信，比如从 Management Station 发送到 iDRAC6 的 IPMI 信息。本地 RACADM 界面仍然可用，可用来重新配置 iDRAC6 LAN。

"IPMI Over LAN"（LAN 上 IPMI）

按 <左箭头>、<右箭头> 和空格键选择**"On"（开）**和**"Off"（关）**。如果选中**"Off"（关）**，iDRAC6 将不会接收通过 LAN 界面抵达的 IPMI 信息。

如果选择**"Off"（关）**，以下警告将会显示：

"iDRAC IPMI Over LAN Out-of-Band interface will be disabled if the LAN Channel is OFF."（如果 LAN 信道关闭，iDRAC 的 LAN 上 IPMI 带外界面将会禁用。）

按任意键清除信息并继续。 请参阅"iDRAC6 LAN"了解该信息的解释。

LAN 参数

按 <Enter> 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
一般设置	
"NIC Selection"（NIC 选择）	按 <右箭头>、<左箭头> 和空格键，在模式之间切换。 可用模式包括**"Dedicated"（专用）**、**"Shared"（共享）**、**"Shared with Failover LOM2"（与故障转移 LOM2 共享）**以及**"Shared with Failover All LOMs"（与故障转移所有 LOM 共享）**。 这些模式允许 iDRAC6 使用对应接口与外界通信。
"MAC Address"（MAC 地址）	这是 iDRAC6 网络接口的不可编辑 MAC 地址。
"VLAN Enable"（VLAN 启用）	选择**"On"（开）**，为 iDRAC6 启用虚拟 LAN 筛选。
VLAN ID	如果**"VLAN Enable"（VLAN 启用）**设置为**"On"（开）**，输入 1-4094 的任意 VLAN ID 值。
VLAN	如果**"VLAN Enable"（VLAN 启用）**设置为**"On"（开）**，选择 0-7 的 VLAN 优先级。
"Register iDRAC6 Name"（注册 iDRAC6 名称）	选择**"On"（开）**可在 DNS 服务中注册 iDRAC6 名称。如果不想用户能够在 DNS 中查找 iDRAC6 名称，则选择**"Off"（关）**。
"iDRAC6 Name"（iDRAC6 名称）	如果**"Register iDRAC Name"（注册 iDRAC 名称）**设置为**"On"（开）**，按 <Enter> 可以编辑**"Current DNS iDRAC Name"（当前 DNS iDRAC 名称）**文本字段。完成编辑 iDRAC6 名称后按 <Enter>。按 <Esc> 返回上一个菜单。iDRAC6 名称必须是有效的 DNS 主机名。
"Domain Name from DHCP"（从 DHCP 获取域名）	如果想从网络上的 DHCP 服务获取域名，则选择**"On"（开）**。如果想指定域名，则选择**"Off"（关）**。
"Domain Name"（域名）	如果**"Domain Name from DHCP"（从 DHCP 获取域名）**设置为**"Off"（关）**，则按 <Enter> 可以编辑**"Current Domain Name"（当前域名）**文本字段。完成编辑后按 <Enter>。按 <Esc> 返回上一个菜单。域名必须是有效 DNS 域，例如 mycompany.com。
"Host Name String"（主机名字符串）	按 <Enter> 可以编辑。为平台事件陷阱 (PET) 警报输入主机名。
"LAN Alert Enabled"（LAN 警报已启用）	选择**"On"（开）**，可以启用 PET LAN 警报。
"Alert Policy Entry 1"（警报策略条目 1）	选择**"Enable"（启用）**或**"Disable"（禁用）**，可以激活第一个警报目标。
"Alert Destination 1"（警报目标 1）	如果**"LAN Alert Enabled"（LAN 警报已启用）**设置为**"On"（开）**，输入要转发 PET LAN 警报到的 IP 地址。
"IPv4 Settings"（IPv4 设置）	启用或禁用对 IPv4 连接的支持。
IPv4	选择**"Enabled"（已启用）**或**"Disabled"（已禁用）**IPv4 协议支持。
"RMCP+ Encryption Key"（RMCP+ 密钥）	按 <Enter> 可以编辑值，完成后按 <Esc>。RMCP+ 密钥是一个 40 字符的十六进制字符串（字符 0-9、a-f 和 A-F）。RMCP+ 是一种 IPMI 扩展，为 IPMI 添加了验证和加密功能。默认值为包含 40 个 0（零）的字符串。
"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**。
"Default Gateway"（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 Settings"（IPv6 设置）	启用或禁用对 IPv6 连接的支持。
"IP Address Source"（IP 地址源）	选择**"AutoConfig"（自动配置）**或**"Static"（静态）**。当选择**"AutoConfig"（自动配置）**后，会从 DHCP 获取**"IPv6 Address 1"（IPv6 地址 1）**、**"Prefix Length"（前缀长度）**和**"Default Gateway"（默认网关）**字段。 当选择**"Static"（静态）**后，**"IPv6 Address 1"（IPv6 地址 1）**、**"Prefix Length"（前缀长度）**和**"Default Gateway"（默认网关）**都会变成可编辑项。
"IPv6 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。
"Default Gateway"（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 iDRAC 网络接口的不可编辑的 **IPv6 链路本地地址**。
"IPv6 Address 2"（IPv6 地址 2）	这是 iDRAC 网络接口的不可编辑的 **IPv6 地址 2**。
"DNS Servers from DHCP"（从 DHCP 获得 DNS 服务器）	选择**"On"（开）**可从网络上的 DHCP 服务检索 DNS 服务器地址。选择**"Off"（关）**可指定以下 DNS 服务器地址。
"DNS Server 1"（DNS 服务器 1）	如果**"DNS Servers from DHCP"（从 DHCP 获得 DNS 服务器）**为**"Off"（关）**，则输入第一个 DNS 服务器的 IP 地址。
"DNS Server 2"（DNS 服务器 2）	如果**"DNS Servers from DHCP"（从 DHCP 获得 DNS 服务器）**为**"Off"（关）**，则输入第一个 DNS 服务器的 IP 地址。
高级 LAN 配置	
"Auto-Negotiate"（自协商）	如果**"NIC Selection"（NIC 选择）**设置为**"Dedicated"（专用）**，请选择**"Enabled"（已启用）**或**"Disabled"（已禁用）**。 当选择**"Enabled"（已启用）**时，将自动配置**"LAN Speed Setting"（LAN 速度设置）**和**"LAN Duplex Setting"（LAN 双工设置）**。
"LAN Speed Setting"（LAN 速度设置）	如果**"Auto-Negotiate"（自协商）**设置为**"Disabled"（已禁用）**，请选择 10 Mbps 或 100 Mbps。
"LAN Duplex Setting"（LAN 双工设置）	如果**"Auto-Negotiate"（自协商）**设置为**"Disabled"（已禁用）**，请选择**"Half Duplex"（半双工）**或**"Full Duplex"（全双工）**。

虚拟介质配置

"Virtual Media"（虚拟介质）

按 <Enter>，选择**"Detached"（分离）**、**"Attached"（附加）**或**"Auto-Attached"（自动附加）**。如果选择**"Attached"（附加）**，虚拟介质设备会附加到 USB 总线，从而可以在**控制台重定向**会话期间使用。

如果选择**"Detached"（分离）**，用户将不能在**控制台重定向**会话期间访问虚拟介质设备。

注： 要使用具有**"Virtual Media"（虚拟介质）**功能的 USB 快擦写驱动器，必须在 BIOS 设置公用程序中将**"USB Flash Drive Emulation Type"（USB 快擦写驱动器仿真类型）**设置为**"Hard disk"（硬盘）**。在服务器启动期间按 <F2> 可访问 BIOS 设置公用程序。如果**"USB Flash Drive Emulation Type"（USB 快擦写驱动器仿真类型）**设置为**"Auto"（自动）**，快擦写驱动器将显示为系统软盘驱动器。

"Virtual Flash"（虚拟闪速更新）

按 <Enter>，选择**"Disabled"（已禁用）**或**"Enabled"（已启用）**。

"Disable"（禁用）/"Enable"（启用）将导致从 USB 总线上**分离**所有虚拟介质设备，或将所有虚拟介质设备**附加**到 USB 总线上。

"Disable"（禁用）将导致虚拟闪速更新被删除，变成不可用状态。

注： 如果 iDRAC6 Express 卡插槽中没有容量大于 256 MB 的 SD 卡，该字段就是只读字段。

"Smart Card Logon"（Smart Card 登录）

按 <Enter>，选择**"Enabled"（已启用）**或**"Disabled"（已禁用）**。该选项配置 Smart Card 登录功能。可用选项有**"Enabled"（已启用）**、**"Disabled"（已禁用）**和**"Enabled with RACADM"（已启用并提供 RACADM）**。

注： 当选择**"Enabled"（已启用）**后，会关闭**"IPMI Over LAN"（LAN 上 IPMI）**并阻止编辑。

系统服务配置

"System Services"（系统服务）

按 <Enter>，选择**"Enabled"（已启用）**或**"Disabled"（已禁用）**。有关详情，请参阅 Dell 支持网站 **support.dell.com\manuals** 上的《*Dell Unified Server Configurator 用户指南*》。

注： 修改此选项后，如果选择**"Save"（保存）**和**"Exit"（退出）**以应用新设置，将会重新启动服务器。

取消系统服务

按 <Enter>，选择**"No"（否）**或**"Yes"（是）**。

当选择**"Yes"（是）**后，如果选择**"Save"（保存）**和**"Exit"（退出）**以应用新设置，会关闭所有 Unified Server Configurator 会话并重新启动服务器。

"LCD Configuration"（LCD Configuration）

按 <Enter>，显示**"LCD Configuration"（LCD 配置）**子菜单。配置完 LAN 参数后，按 <Esc> 返回上一个菜单。

表 18-2. LCD 用户配置

"LCD Line 1"（LCD 行 1）	按 <右箭头>、<左箭头> 和空格键，在选项之间切换。 该功能将 LCD 上的**主**显示设置为以下选项之一： **"Ambient Temp"（环境温度）**、**"Asset Tag"（资产标签）**、**"Host Name"（主机名）**、**"iDRAC6 IPv4 Address"（iDRAC6 IPv4 地址）**、**"iDRAC6 IPv6 Address"（iDRAC6 IPv6 地址）**、**"iDRAC6 MAC Address"（iDRAC6 MAC 地址）**、**"Model Number"（型号）**、**"None"（无）**、**"Service Tag"（服务标签）**、**"System Power"（系统功率）**、**"User-Defined String"（用户定义字符串）**。
"LCD User-Defined String"（LCD 用户定义字符串）	如果**"LCD Line 1"（LCD 行 1）**设置为**"User-Defined String"（用户定义字符串）**，则查看或输入要在 LCD 上显示的字符串。 字符串最大长度为 62 个字符。
"LCD System Power Units"（LCD 系统电源单位）	如果**"LCD Line 1"（LCD 行 1）**设置为**"System Power"（系统功率）**，则选择**"Watt"（瓦特）**或 **BTU/hr**，来指定 LCD 上显示的功率单位。
"LCD Ambient Temp Units"（LCD 环境温度单位）	如果**"LCD Line 1"（LCD 行 1）**设置为**"Ambient Temp"（环境温度）**，则选择**"Celsius"（摄氏）**或**"Fahrenheit"（华氏）**，来指定 LCD 上显示的温度单位。
"LCD Error Display"（LCD 错误显示）	选择**"Simple"（简单）**或 **SEL**（系统事件日志）。 该功能允许采用以下两种格式之一，在 LCD 上显示错误信息： "Simple"（简单）格式用英语提供事件说明。 SEL 格式显示系统事件日志文本字符串。
"LCD Remote KVM Indication"（LCD 远程 KVM 指示）	选择**"Enabled"（已启用）**后，当设备上存在活动的虚拟 KVM 时即会显示文本 *KVM*。
"LCD Front Panel Access"（LCD 前面板访问）	按 <右箭头>、<左箭头> 和空格键，在选项**"Disabled"（已禁用）**、**"View/Modify"（查看/修改）**和**"View Only"（仅查看）**之间切换。 该设置为 LCD 定义用户访问级别。

LAN 用户配置

LAN 用户是 iDRAC 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 18-3. LAN 用户配置

项目	说明

"Account Access"（帐户访问）	选择**"Enabled"（已启用）**可启用管理员帐户。选择**"Disabled"（已禁用）**可禁用管理员帐户。
"Account Privilege"（帐户权限）	选择**"Admin"（管理员）**、**"User"（用户）**、**"Operator"（操作员）**和**"No Access"（无权限）**。
"Account User Name"（帐户用户名）	按 <Enter> 以编辑用户名并在完成后按 <Esc>。默认用户名为 **root**。
"Enter Password"（输入密码）	键入管理员帐户的新密码。键入时字符不会显示出来。
"Confirm Password"（确认密码）	重新键入管理员帐户的新密码。如果输入的字符与**"Enter Password"（输入密码）**字段中输入的字符不同，将会显示信息，必须重新输入密码。

重设为默认值

使用**"Reset to Default"（重设为默认值）**菜单项可以将所有 iDRAC6 配置项重设为工厂默认值。例如，如果忘记了管理用户密码或者想从默认设置重新配置 iDRAC6，可能就需要这样做。

按 <Enter> 以选择项目。系统将显示以下警告信息：

"Resetting to factory defaults will restore remote Non-Volatile user settings.Continue?"（重设为工厂默认值会恢复远程非易失用户设置。是否要继续？）

< "NO"（否）（取消） >

< "YES"（是）（继续） >

选择**"YES"（是）**并按 <Enter> 会将 iDRAC 重设为默认值。

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 最多保持 512 条信息。

要查看 SEL 信息，请选择**"View System Event Log"（查看系统事件日志）**并按 <Enter>。使用 <左箭头> 可移动到上一条（较旧）信息，使用 <右箭头> 可移动到下一条（较新）信息。输入记录号可跳到该记录。查看完 SEL 信息后按 <Esc>。

要清除 SEL，请选择**"Clear System Event Log"（清除系统事件日志）**并按 <Enter>。

使用完 SEL 菜单后，按 <Esc> 返回上一个菜单。

退出 iDRAC 配置公用程序

完成 iDRAC 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> 可以保留更改。

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> 可以返回 iDRAC 配置公用程序。

目录

目录

监控和警报管理

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节介绍如何监控 iDRAC6，以及如何将系统和 iDRAC6 配置为可接收警报。

配置 Managed System 以获取上次崩溃屏幕

在 iDRAC6 可以捕获上次崩溃屏幕前，必须将 Managed System 配置成满足以下前提条件。

1. 安装 Managed System Software。有关安装 Managed System Software 的详情，请参阅《*Server Administrator 用户指南*》。
2. 运行支持的 Microsoft® Windows® 操作系统，并且在**"Windows Startup and Recovery Settings"（Windows 启动和恢复设置）**中取消选中 Windows 的"自动重新引导"功能。
3. 启用上次崩溃屏幕（默认情况下已禁用）。

   要使用本地 RACADM 启用上次崩溃屏幕，请打开命令提示符，并键入以下命令：

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

4. 启用自动恢复计时器并将**"Auto Recovery"（自动恢复）**操作设置为**"Reset"（重设）**、**"Power Off"（关机）**或**"Power Cycle"（关机后再开机）**。要配置**"Auto Recovery"（自动恢复）**计时器，必须使用 Server Administrator 或 IT Assistant。

   有关如何配置**"Auto Recovery"（自动恢复）**计时器的信息，请参阅《*Server Administrator 用户指南*》。要确保能够捕获上次崩溃屏幕，**"Auto Recovery"（自动恢复）**计时器必须设置为 60 秒或更大。默认设置为 480 秒钟。

   当"Auto Recovery"（自动恢复）操作设置为**"Shutdown"（关机）**或**"Power Cycle"（关机后再开机）**时，如果 Managed System 崩溃，上次崩溃屏幕将不可用。

禁用 Windows 自动重新引导选项

为了确保在 iDRAC6 基于 Web 的界面上，上次崩溃屏幕功能能够正常工作，请在运行 Microsoft Windows Server® 2008 和 Windows Server 2003 操作系统的 Managed System 上禁用**"Automatic Reboot"（自动重新引导）**选项。

在 Windows 2008 Server 中禁用"Automatic Reboot"（自动重新引导）选项

1. 打开 Windows**"Control Panel"（控制面板）**并双击**"System"（系统）**图标。
2. 在左侧单击**"Tasks"（任务）**下的**"Advanced System Setting"（高级系统设置）**。
3. 单击**"Advanced"（高级）**选项卡。
4. 在**"Startup and Recovery"（启动和恢复）**下，单击**"Settings"（设置）**。
5. 取消选择**"Automatically Restart"（自动重新启动）**复选框。
6. 单击**"OK"（确定）**两次。

在 Windows Server 2003 中禁用自动重新引导选项

1. 打开 Windows**"Control Panel"（控制面板）**并双击**"System"（系统）**图标。
2. 单击**"Advanced"（高级）**选项卡。

3. 在**"Startup and Recovery"（启动和恢复）**下，单击**"Settings"（设置）**。
4. 取消选择**"Automatically Reboot"（自动重新引导）**复选框。
5. 单击**"OK"（确定）**两次。

配置平台事件

平台事件配置提供了用于配置远程访问设备针对某些事件信息执行所选操作的机制。这些操作包括重新引导、关机后再开机、关机以及触发警报（平台事件陷阱 [PET] 和/或电子邮件）。

可筛选的平台事件包括以下：

- 风扇危急声明筛选器
- 电池警告声明筛选器
- 电池危急声明筛选器
- 不连续电压危急声明筛选器
- 温度警告声明筛选器
- 温度危急声明筛选器
- 侵入危急声明筛选器
- 冗余降级筛选器
- 冗余丧失筛选器
- 处理器警告声明筛选器
- 处理器危急声明筛选器
- 处理器缺失筛选器
- 处理器电源警告声明筛选器
- 处理器电源危急声明筛选器
- 处理器电源缺失声明筛选器
- 事件日志危急声明筛选器
- 监控软件危急声明筛选器
- 系统电源警告声明筛选器
- 系统电源危急声明筛选器

出现平台事件时（例如，风扇探测器故障），会生成系统事件并在系统事件日志 (SEL) 中记录。如果该事件匹配基于 Web 的界面中平台事件筛选器列表中的平台事件筛选器 (PEF)，并且已配置该筛选器生成警报（PET 或电子邮件），则会将 PET 或电子邮件警报发送到一个或多个配置目标。

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

配置平台事件筛选器 (PEF)

在配置平台事件陷阱或电子邮件警报设置之前，配置平台事件筛选器。

使用基于 Web 的界面配置 PEF

有关详细信息，请参阅"配置平台事件筛选器 (PEF)"。

使用 RACADM CLI 配置 PEF

1. 启用 PEF。

   打开命令提示符，键入以下命令并按 <Enter>：

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   其中 1 和 1 分别是 PEF 索引和启用/禁用选择。

   PEF 索引可以是 1 到 19 的值。启用/禁用选择可以设置为 1（已启用）或 0（已禁用）。

例如，要启用具有索引 5 的 PEF，键入以下命令：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. 配置 PEF 操作。

   在命令提示符下，键入以下命令并按 <Enter>：

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <操作>
   ```

   其中 <*操作*> 值位如下所示：

   - 0 = 无警报操作
   - 1 = 关闭服务器
   - 2 = 重新引导服务器
   - 3 = 关闭后重新打开服务器

   例如，要使 PEF 能重新引导服务器，请键入以下命令：

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
   ```

   其中 1 是 PEF 索引，而 2 是执行重新引导的 PEF 操作。

配置 PET

使用 Web 用户界面配置 PET

有关详细信息，请参阅"配置平台事件陷阱 (PET)"。

使用 RACADM CLI 配置 PET

1. 启用全局警报。

   打开命令提示符，键入以下命令并按 <Enter>：

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

2. 启用 PET。

   在命令提示符下，键入下列命令，并在键入每个命令后按 <Enter>：

   ```
   IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
   ```

   ```
   IPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 1 1
   ```

   其中 1 和 1 分别是 PET 目标索引和启用/禁用选择

   PET 目标索引可以是 1 到 4 之间的一个值。启用/禁用选择可以设置为 1（已启用）或 0（已禁用）。

   例如，要启用具有索引 4 的 PET，键入以下命令：

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

   ```
   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 4 1
   ```

3. 配置 PET 策略。

   在命令提示符下，键入以下命令并按 <Enter>：

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IPv4 地址>
   ```

   ```
   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6 地址>
   ```

   其中，1 表示 PET 目标索引，<*IPv4 地址*> 和 <*IPv6 地址*> 表示接收平台事件警报的系统的目标 IP 地址。

4. 配置团体名称字符串。

   在命令提示符下键入：

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名称>
```

配置电子邮件警报

使用 Web 用户界面配置电子邮件警报

有关详细信息，请参阅"配置电子邮件警报"。

使用 RACADM CLI 配置电子邮件警报

1. 启用全局警报。

   打开命令提示符，键入以下命令并按 <Enter>：

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

2. 启用电子邮件警报。

   在命令提示符下，键入下列命令，并在键入每个命令后按 <Enter> 键：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
   ```

   其中 1 和 1 分别是电子邮件目标索引和启用/禁用选择。

   电子邮件目标索引可以是 1 到 4 之间的一个值。启用/禁用选择可以设置为 1（已启用）或 0（已禁用）。

   例如，要启用具有索引 4 的电子邮件，键入以下命令：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. 配置电子邮件设置。

   在命令提示符下，键入以下命令并按 <Enter>：

   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <*电子邮件地址*>

   其中 1 是电子邮件目标索引，而 <*电子邮件地址*> 是接收平台事件警报的目标电子邮件地址。

   要配置自定义信息，请在命令提示符下键入以下命令并按 <Enter>：

   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <*自定义信息*>

   其中，1 表示电子邮件目标索引，<*自定义信息*> 表示电子邮件警报上显示的信息。

检测电子邮件警报

RAC 电子邮件警报功能允许用户在 Managed System 上发生重要事件时接收电子邮件警报。下面的示例说明如何测试电子邮件警报功能以确保 RAC 在网络上正确发送电子邮件警报。

```
racadm testemail -i 2
```

注： 确保在测试电子邮件警报功能前 **SMTP** 和**电子邮件警报**设置已配置。有关详情，请参阅"配置电子邮件警报"。

测试 RAC SNMP 陷阱警报功能

RAC SNMP 陷阱警报功能允许 SNMP 陷阱侦听器配置接收 Managed System 上发生的系统事件陷阱。

下面的示例说明用户如何测试 RAC 的 SNMP 陷阱警报功能。

```
racadm testtrap -i 2
```

测试 RAC SNMP 陷阱警报功能前，请确保正确配置了 SNMP 和陷阱设置。请参阅 "testtrap" 和 "sslkeyupload" 子命令说明来配置这些设置。

有关 SNMP 验证的常见问题

为什么显示以下信息：

"Remote Access: SNMP Authentication Failure"（远程访问：SNMP 验证故障）

在查找过程中，IT Assistant 会尝试验证设备的 get 和 set 团体名称。在 IT Assistant 中，get **团体名称 = public** 而 set **团体名称 = private**。默认情况下，iDRAC6 代理的团体名称是 **public**。当 IT Assistant 发出 set 请求时，iDRAC6 代理会生成 SNMP 验证错误，因为它只接受来自**团体 = public** 的请求。

注： 这是供查找使用的 SNMP 代理团体名称。

可以使用 RACADM 更改 iDRAC6 团体名称。

要查看 iDRAC6 团体名称，请使用以下命令：

```
racadm getconfig -g cfgOobSnmp
```

要设置 iDRAC6 团体名称，请使用以下命令：

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <团体名称>
```

要使用基于 Web 的界面访问/配置 iDRAC6 SNMP 代理团体名称，请转至**"Remote Access"（远程访问）→"Configuration"（配置）→"Services"（服务），**单击**"SNMP Agent"（SNMP 代理）**。

为了防止出现 SNMP 验证错误，必须输入代理接受的团体名称。由于 iDRAC6 只允许一个团体名称，因此必须对 IT Assistant 查找设置使用相同的 **get** 和 **set** 团体名称。

目录

目录

对 Managed System 进行恢复和故障排除

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节介绍如何使用 iDRAC6 基于 Web 的界面，执行与崩溃的远程系统的恢复和故障排除工作有关的任务。

- "排除远程系统故障时首先需要执行的步骤"
- "管理远程系统上的电源"
- "IPv6 信息"
- "查看上次系统崩溃屏幕"

排除远程系统故障时首先需要执行的步骤

以下是在排除 Managed System 高级别故障时常见的一些问题：

1. 系统开机还是关机？
2. 如果是开机，操作系统是运作正常、崩溃，或者只是冻结？
3. 如果是关机，电源是意外关闭的吗？

对于崩溃的系统，请检查上次崩溃屏幕（请参阅"查看上次系统崩溃屏幕"），使用控制台重定向和远程电源管理（请参阅"管理远程系统上的电源"）重新启动系统，并监控重新引导过程。

管理远程系统上的电源

iDRAC6 允许在 Managed System 上远程执行几种电源管理操作，以便在出现系统崩溃或其它系统事件后进行恢复。

从 iDRAC6 基于 Web 的界面上选择电源控制操作

要使用基于 Web 的界面执行电源管理操作，请参阅"执行服务器电源控制操作"。

从 iDRAC6 CLI 上选择电源控制操作

使用 `racadm serveraction` 命令在主机系统上执行电源管理操作。

`racadm serveraction <操作>`

以下为 *<操作>* 字符串的选项：

- **powerdown** — 关闭 Managed System 电源。
- **powerup** — 打开 Managed System 电源。
- **powercycle** — 在 Managed System 上发出关机后再开机操作。此操作类似于按下系统前面板的电源按钮关闭然后再打开系统电源。
- **powerstatus** — 显示服务器的当前电源状态（"ON"或"OFF"）。
- **hardreset** — 在 Managed System 上执行重设（重新引导）操作。

查看系统信息

"System Summary"（系统摘要）页显示关于以下系统组件的信息：

- Main System Chassis（主系统机箱）
- Integrated Dell Remote Access Controller 6 - Enterprise

要访问系统信息，请展开**系统**树并单击**"Properties"（属性）**。

Main System Chassis（主系统机箱）

表 20-1 和表 20-2 说明主系统机箱属性。

注： 要接收**主机名**和**操作系统名称**信息，Managed System 上必须安装有 iDRAC6 服务。

表 20-1. 系统信息字段

字段	说明
"Description"（说明）	系统说明。
"BIOS Version"（BIOS 版本）	系统 BIOS 版本。
"Service Tag"（服务标签）	系统服务标签号码。
"Host Name"（主机名）	主机系统的名称。
"OS Name"（操作系统名称）	系统上运行的操作系统。

表 20-2. 自动恢复字段

字段	说明
"Recovery Action"（恢复操作）	可以将 iDRAC6 配置为在检测到"系统挂起"时执行以下操作之一："No Action"（无操作）、"Hard Reset"（硬重设）、"Power Down"（关闭电源）或"Power Cycle"（关机后再开机）。
"Initial Countdown"（初始倒计数）	当检测到"系统挂起"后，一旦经过这些秒数，iDRAC6 将执行恢复操作。
"Present Countdown"（当前倒计数）	倒计数计时器的当前值，以秒为单位。

Integrated Dell Remote Access Controller 6 Enterprise

表 20-3 说明 iDRAC6 Enterprise 属性。

表 20-3. iDRAC6 Enterprise 信息字段

字段	说明
"Date/Time"（日期/时间）	采用以下格式表示的当前时间： 日 月 DD HH:MM:SS:YYYY
"Firmware Version"（固件版本）	iDRAC 固件版本。
"Firmware Updated"（固件更新）	上次对固件刷写的日期，采用以下格式： 日 月 DD HH:MM:SS:YYYY
"Hardware Version"（硬件版本）	Remote Access Controller 版本。
"MAC Address"（MAC 地址）	显示唯一标识网络中各个节点的介质访问控制 (MAC) 地址

IPv4 信息

表 20-4 说明 IPv4 属性。

表 20-4. IPv4 信息字段

字段	说明
"Enabled"（已启用）	"Yes"（是）或"No"（否）

"IP Address"（IP 地址）	标识主机的网络接口卡 (NIC) 的 32 位地址。该值采用点分隔格式，比如 143.166.154.127。
"Subnet Mask"（子网掩码）	子网掩码标识 IP 地址的组成部分：扩展网络前缀和主机号。该值采用点分隔格式，比如 255.255.0.0。
"Gateway"（网关）	路由器或交换机的地址。该值采用点分隔格式，比如 143.166.154.1。
"DHCP Enabled"（是否已启用 DHCP）	"Yes"（是）或"No"（否）。指示是否启用了动态主机配置协议 (DHCP)。

IPv6 信息

表 20-5 说明 IPv6 属性。

表 20-5. IPv6 信息字段

字段	说明
"Enabled"（已启用）	指示是否启用了 Ipv6 堆栈。
"IP Address 1"（IP 地址 1）	指定 iDRAC6 NIC IPv6 地址。
"Prefix Length"（前缀长度）	指定 IPv6 地址前缀长度的整数。可以是介于 1 和 128（含）之间的值。
"IP Gateway"（IP 网关）	指定 iDRAC6 NIC 网关。
"Link Local Address"（链路本地地址）	指定 iDRAC6 NIC IPv6 地址。
"IP Address 2"（IP 地址 2）	如果有的话，指定 iDRAC6 NIC 的附加 IPv6 地址。
"Auto Config"（自动配置）	"AutoConfig"（自动配置）可让 Server Administrator 从动态主机配置协议 (DHCPv6) 服务器获取 iDRAC NIC 的 IPv6 地址。此外，请取消激活并删除"Static IP Address"（静态 IP 地址）、"Prefix Length"（前缀长度）和"Static Gateway"（静态网关）的值。

使用系统事件日志 (SEL)

SEL 页显示 Managed System 上发生的系统重要事件。

要查看系统事件日志：

1. 在**系统**树中单击**"System"（系统）**。
2. 单击**"Logs"（日志）**选项卡，然后单击**"System Event Log"（系统事件日志）**。

   "System Event Log"（系统事件日志）页显示事件严重性并提供其它信息，如表 20-6 所示。
3. 单击相应的**"System Event Log"（系统事件日志）**页按钮以继续（请参阅表 20-6）。

表 20-6. 状态指示器图标

图标/类别	说明
	绿色复选标记表示健康（正常）状况。
	黄色带有感叹号的三角表示警告（不严重）状况。
	红色 X 表示严重（故障）状况。
	问号图标指示状态未知。
日期/时间	事件发生的日期和时间。如果日期为空白，则事件发生在系统引导时。格式为 mm/dd/yyyy hh:mm:ss，按照 24 小时表示。
说明	事件的简要说明

表 20-7. SEL 页按钮

按钮	操作
"Print"（打印）	按**窗口中显示的排序顺序打印 SEL。**
"Refresh"（刷新）	重新载入 **SEL** 页。
"Clear Log"（清除日	清除 **SEL**。

志）	**注：** 仅当您有**"Clear Logs"（清除日志）**权限时，才会显示**"Clear Log"（清除日志）**按钮。
"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。

使用命令行查看系统日志

`racadm getsel -i`

getsel -i 命令显示 SEL 中的条目数。

`racadm getsel <选项>`

注： 如果没有指定参数，将显示整个日志。

注： 请参阅"getsel"了解有关可用选项的详情。

clrsel 命令会从系统事件日志 (SEL) 删除全部现有的记录。

`racadm clrsel`

使用开机自检引导日志

注： 重新引导 iDRAC6 后，所有日志都将清除。

iDRAC6 的这种功能使用户能够回放 BIOS 开机自检引导的最后三个实例的停止运动视频。

要查看开机自检引导捕获日志：

1. 在**系统**树中单击**"System"（系统）**。
2. 单击**"Logs"（日志）**选项卡并随后单击**"BOOT Capture"（引导捕获）**选项卡。
3. 选择开机自检引导捕获日志的日志编号，然后单击**"Play"（播放）**。

   随即在新屏幕上打开日志的视频。

   注： 必须先关闭打开的开机自检引导捕获日志视频，之后才能播放另一个日志视频。不能同时播放两个日志。
4. 单击**"Playback"（回放）→"Play"（播放）**，启动开机自检引导捕获日志视频。
5. 单击**"STOP"（停止）**以停止视频。

在引导期间按 **F10** 进入 Unified Server Configurator (USC) 应用程序后，iDRAC6 Express Card 会绑定到 iDRAC6。如果绑定成功，会在 SEL 和 LCD 中记录以下信息 — `iDRAC6 Upgrade Successful`（iDRAC6 升级成功）。如果绑定失败，会在 SEL 和 LCD 中记录以下信息 — `iDRAC6 Upgrade Failed`（iDRAC6 升级失败）。另外，如果在主板上插入的 iDRAC6 Express Card 包含不支持特定平台的旧或过期 iDRAC6 固件并且引导系统，会在开机自检屏幕上生成记录 — `iDRAC firmware is out-of-date`（iDRAC 固件过期）。请更新至最新的固件。使用特定平台的最新 iDRAC6 固件更新 iDRAC6 Express Card。有关详情，请参阅*《Dell Unified Server Configurator 和 Dell Unified Server Configurator®C 已启用生命周期控制器用户指南》*。

查看上次系统崩溃屏幕

注： 上次崩溃屏幕功能要求 Managed System 在 Server Administrator 中配置**"Auto Recovery"（自动恢复）**功能。此外，确保使用 iDRAC6 启用了**"Automated System Recovery"（自动系统恢复）**功能。导航至**"Remote Access"（远程访问）**部分中**"Configuration"（配置）**选项卡下**"Services"（服务）**页以启用此功能。

"Last Crash Screen"（上次崩溃屏幕）页显示最新的崩溃屏幕。上次系统崩溃信息保存在 iDRAC6 内存中，并且可以远程访问。

要查看**"Last Crash Screen"（上次崩溃屏幕）**页：

1. 在**系统**树中单击**"System"（系统）**。

2. 单击**"Logs"（日志）**选项卡，然后单击**"Last Crash"（上次崩溃）屏幕**。

"Last Crash Screen"（上次崩溃屏幕）页在屏幕右上角提供以下按钮（请参阅表 20-8）：

表 20-8. 上次崩溃屏幕页按钮

按钮	操作
"Print"（打印）	打印**"Last Crash Screen"（上次崩溃屏幕）**页。
"Refresh"（刷新）	重新载入**"Last Crash Screen"（上次崩溃屏幕）**页。

注： 由于自动恢复计时器的波动，当系统重设计时器设置为小于 30 秒的值时可能无法捕获**上次崩溃屏幕**。使用 Server Administrator 或 IT Assistant 将系统重设计时器设置为至少 30 秒，并确保**上次崩溃屏幕**运行正常。有关其它信息，请参阅"配置 Managed System 以获取上次崩溃屏幕"。

目录

目录

对 iDRAC6 进行恢复和故障排除

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节介绍如何对崩溃的 iDRAC6 进行恢复和故障排除。

可以使用以下任一工具来排除 iDRAC6 的故障：

- RAC 日志
- 诊断控制台
- 跟踪日志
- racdump
- coredump

使用 RAC 日志

RAC 日志是 iDRAC6 固件中的一个持续存在的日志。日志中的列表记录了用户操作（比如登录、注销和安全策略更改）以及由 iDRAC6 发出的警报。当日志已满后，会将最早的条目覆盖掉。

要从 iDRAC6 用户界面 (UI) 访问 RAC 日志，请执行以下操作：

1. 在**系统**树中，单击**"Remote Access"（远程访问）**。
2. 单击**"Logs"（日志）**选项卡，然后单击**"RAC Log"（RAC 日志）**。

RAC 日志提供表 21-1 中所列的信息。

表 21-1. RAC 日志页信息

字段	说明
"Date/Time"（日期/时间）	日期和时间（例如 Dec 19 16:55:47）。 当 iDRAC6 刚开始启动并且无法与 Managed System 通信时，该时间将会显示为系统引导。
"Source"（来源）	引起事件的接口。
"Description"（说明）	iDRAC6 中记录的事件和用户名的简要说明。

使用 RAC 日志页按钮

"RAC Log"（RAC 日志）页提供表 21-2 中所列的按钮。

表 21-2. RAC 日志按钮

按钮	操作
"Print"（打印）	打印**"RAC Log"（RAC 日志）**页。
"Clear Log"（清除日志）	清除**"RAC Log"（RAC 日志）**条目。 **注：** 仅当您有**"Clear Logs"（清除日志）**权限时，才会显示**"Clear Log"（清除日志）**按钮。
"Save As"（另存为）	打开一个弹出窗口，使您能够将 **RAC 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**"RAC Log"（RAC 日志）**页。

使用命令行

可以使用 `getraclog` 命令查看 RAC 日志条目。

```
racadm getraclog -i
```

getraclog -i 命令显示 iDRAC6 日志中的条目数。

```
racadm getraclog [选项]
```

注： 有关详情，请参阅"getraclog"。

可以使用 `clrraclog` 命令从 RAC 日志清除所有条目。

```
racadm clrraclog
```

使用诊断控制台

iDRAC6 提供一组标准网络诊断工具（请参阅表 21-3），与基于 Microsoft® Windows® 或 Linux 的系统提供的工具类似。使用 iDRAC6 基于 Web 的界面，可以访问网络调试工具。

要访问**"Diagnostic Console"（诊断控制台）**页：

1. 在**系统**树中，单击**"Remote Access"（远程访问）**。
2. 单击**"Diagnostics"（诊断）**选项卡。

表 21-3 说明**"Diagnostic Console"（诊断控制台）**页上可用的选项。键入命令并单击**"Submit"（提交）**。调试结果显示在**"Diagnostic Console"（诊断控制台）**页中。

要刷新**"Diagnostic Console"（诊断控制台）**页，请单击**"Refresh"（刷新）**。要执行其它命令，请单击**"Go Back to Diagnostics Page"（退回到诊断页）**。

表 21-3. 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	打印路径选择表的内容。如果在 **netstat** 选项右边的文本字段中提供可选接口号，netstat 将输出与通过该接口的通信量有关的其它信息、缓冲区的使用情况以及其它网络接口信息。
ping <*IP 地址*>	验证目标 IP 地址是否可以使用当前路径选择表内容从 iDRAC6 进行访问。必须在该选项右侧的字段中输入目标 IP 地址。根据当前的路径选择表内容，将 Internet 控制报文协议 (ICMP) 回音数据包发送到目标 IP 地址。
gettracelog	显示 iDRAC6 跟踪日志。有关详情，请参阅"gettracelog"。

使用跟踪日志

内部 iDRAC6 跟踪日志由管理员用于调试 iDRAC6 警报和网络问题。

要从 iDRAC6 基于 Web 的界面访问跟踪日志：

1. 在**系统**树中，单击**"Remote Access"（远程访问）**。
2. 单击**"Diagnostics"（诊断）**选项卡。
3. 将 **gettracelog** 命令或 **racadm gettracelog** 命令键入**命令**字段。

   注： 还可以从命令行界面使用此命令。有关详情，请参阅"gettracelog"。

跟踪日志跟踪以下信息：

- DHCP — C 跟踪发送到 DHCP 服务器和从 DHCP 服务器接收的数据包。
- IP — C 跟踪发送和接收的 IP 数据包。

跟踪日志还可能包含 iDRAC6 固件特定的错误代码，与内部 iDRAC6 固件有关，而不是 Managed System 的操作系统。

注： iDRAC6 不会回送数据包大小超过 1500 字节的 ICMP (ping)。

使用 racdump

racadm racdump 命令使用户可以通过一个命令就获得转储、状态以及 iDRAC6 板的一般信息。

注： 此命令只能在 Telnet 和 SSH 接口上使用。有关详情，请参阅 "racdump" 命令。

使用 coredump

racadm coredump 命令显示有关 RAC 最近出现的重要问题的详细信息。coredump 信息可用于诊断这些重要问题。

如果出现的话，coredump 信息在整个 RAC 关机后再开机过程中都保持不变，并且只有在出现以下某种情况时才会清除：

- 使用 **coredumpdelete** 子命令清除 coredump 信息。
- 在 RAC 上出现其它重要情况。如果出现这种情况，coredump 信息将与最新出现的严重错误相关。

racadm coredumpdelete 命令可用于清除 RAC 中最近存储的 **coredump** 数据。

有关详情，请参阅 "coredump" 和 "coredumpdelete" 子命令。

目录

目录

传感器

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

硬件传感器或探测器帮助用户以更有效的方式监测网络上的系统，使用户可以采取相应的措施来防止灾难，比如系统不稳定或损坏。

可以使用 iDRAC6 监视相应的硬件传感器来监测电池、风扇探测器、机箱侵入、电源设备、功耗、温度和电压。

电池探测器

电池探测器提供有关系统板 CMOS 和母板存储 RAM (ROMB) 电池的信息。

注： 只有在系统具有 ROMB 时，存储 ROMB 电池设置才可用。

风扇探测器

风扇探测器传感器提供的信息有：

- 风扇冗余 — 如果主风扇不能以预设置的速度散热，第二个风扇将替换主风扇。
- 风扇探测器列表 — 提供系统所有风扇的速度信息。

机箱侵入探测器

机箱侵入探测器提供机箱状态的信息，即机箱是打开还是关闭。

电源设备探测器

电源设备探测器提供的信息有：

- 电源设备状态
- 电源设备冗余，即，在主电源设备故障的情况下由冗余电源设备替换主电源设备。

注： 如果系统中只有一个电源设备，电源设备冗余将设置为**已禁用**。

电源监测探测器

电源监测提供有关*实时*功耗（瓦和安培）的信息。

还可以查看 iDRAC6 中设置的当前时间的上一分钟、上一小时、昨天或上周功耗的图形化表示。

温度探测器

温度传感器提供有关系统板环境温度的信息。温度探测器表示探测器状态是否在预置警告和临界阈值内。

电压探测器

以下是典型的电压探测器。系统可能有这些和/或其它。

- CPU [n] VCORE
- System Board 0.9V PG
- System Board 1.5V ESB2
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

电压探测器表示探测器状态是否在预置警告和临界阈值内。

目录

目录

iDRAC6 使用入门

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

iDRAC6 使您能够远程监控、故障排除以及修复 Dell 系统，即使系统已关闭。iDRAC6 提供了丰富的功能，比如控制台重定向、虚拟介质、虚拟 KVM、Smart Card 验证和单一登录等。

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

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

要设置 iDRAC6，应遵循这些常规步骤：

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

1. 配置 iDRAC6 属性、网络设置和用户 — 可以通过使用 iDRAC6 配置公用程序、基于 Web 的界面或 RACADM 来配置 iDRAC6。
2. 如果通过使用 Windows 系统配置 Microsoft® Active Directory® 以提供对 iDRAC6 的访问，能够使您为 Active Directory 软件中的现有用户添加和控制 iDRAC6 用户权限。
3. 配置 Smart Card 验证 — Smart Card 为您的企业额外添加了一层安全保护。
4. 配置远程访问点，比如控制台重定向和虚拟介质。
5. 配置安全设置。
6. 配置警报实现高效的系统管理能力。
7. 配置 iDRAC6 智能平台管理界面 (IPMI) 设置使用基于标准的 IPMI 工具管理网络上的系统。

目录

目录

启用 Kerberos 验证

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

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 Smart Card 和单一登录。

Microsoft® Windows® 2000、Windows XP、Windows Server® 2003、Windows Vista® 和 Windows Server 2008 使用 Kerberos 作为默认验证方法。

iDRAC6 使用 Kerberos 支持两种验证机制 — Active Directory 单一登录和 Active Directory Smart Card 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 Smart Card 登录，iDRAC6 使用基于 Smart Card 的双重验证 (TFA) 作为凭据来启用 Active Directory 登录。这是本地 Smart Card 验证随附的功能。

如果 iDRAC6 时间与域控制器时间不同，iDRAC6 上的 Kerberos 验证将会失败。最多允许 5 分钟偏差。要进行成功验证，请同步服务器与域控制器的时间，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 <偏差值>
```

使用 Smart Card 进行单一登录和 Active Directory 验证的前提条件

- 配置 iDRAC6 进行 Active Directory 登录。有关详情，请参阅"使用 Active Directory 登录到 iDRAC6"。
- 注册 iDRAC6 作为 Active Directory 根域中的计算机。
  a. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**选项卡→**"Network"（网络）**子选项卡。
  b. 提供有效的**"Preferred"（首选）/"Alternate DNS Server"（备用 DNS 服务器）**IP 地址。该值是根域中 DNS 的 IP 地址，验证用户的 Active Directory 帐户。
  c. 选择**"Register iDRAC on DNS"（向 DNS 注册 iDRAC）**。
  d. 提供有效**"DNS Domain Name"（DNS 域名）**。

  请参阅 ***iDRAC6 联机帮助***了解有关详情。

为支持两种新的验证机制，iDRAC6 支持配置以使自身作为 Windows Kerberos 网络上的加密服务。iDRAC6 上的 Kerberos 配置步骤与配置非 Windows Server Kerberos 服务作为 Windows Server Active Directory 安全原则的步骤一样。

使用 Microsoft 工具 **ktpass**（由 Microsoft 服务器安装 CD/DVD 提供）创建用户帐户 Service Principal Name (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 文件包含加密密钥，用于对服务器和 KDC 间的信息进行加密。ktpass 工具使那些支持 Kerberos 验证的基于 UNIX 的服务能够使用 Windows Server Kerberos KDC 服务提供的交互功能。

从 ktpass 公用程序获得的 keytab 作为文件上载提供给 iDRAC6 并作为网络上的加密服务。

由于 iDRAC6 是一种非 Windows 操作系统设备，在想将 iDRAC6 映射到 Active Directory 用户帐户的域控制器（Active Directory 服务器）上，运行 **ktpass** 公用程序（Microsoft Windows 的一部分）。

例如，使用以下 **ktpass** 命令创建 Kerberos keytab 文件：

```
C:\>ktpass -princ HOST/dracname.domainname.com@DOMAINNAME.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out
c:\krbkeytab
```

iDRAC6 用于 Kerberos 验证的加密类型是 DES-CBC-MD5。基本类型是 KRB5_NT_PRINCIPAL。服务基本名称映射到的用户帐户的属性应启用以下帐户属性：

- 为此帐户使用 DES 加密类型
- 不要求 Kerberos 预验证

注： 建议使用最新的 **ktpass** 公用程序创建 Keytab 文件。

此步骤会生成一个 keytab 文件，应将该文件上载到 iDRAC6。

注： keytab 包含加密密钥，因此应保管好。

有关 **ktpass** 公用程序的详情，请参阅 Microsoft 网站：**http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-**

d576a8db0d051033.mspx?mfr=true

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

配置 iDRAC6 成为使用 Smart Card 进行单一登录和 Active Directory 验证

将从 Active Directory 根域获得的 keytab 上载到 iDRAC6：

1. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**选项卡→ **Active Directory** 子选项卡 → 单击**"Configure Active Directory"（配置 Active Directory）**。
2. 选择**"Upload Kerberos Keytab"（上载 Kerberos Keytab）**并单击**"Next"（下一步）**。
3. 在**"Kerberos Keytab Upload"（Kerberos Keytab 上载）**页上，选择要上载的 Keytab 文件并单击**"Apply"（应用）**。

还可以使用 CLI racadm 命令将文件上载到 iDRAC6。以下命令将 keytab 文件上载到 iDRAC6：

```
racadm krbkeytabupload -f <文件名>
```

其中 <文件名> 是 keytab 文件的名称。本地和远程 racadm 都支持 racadm 命令。

配置 Active Directory 用户进行单一登录

开始使用 Active Directory 单一登录功能前，应确保已配置 iDRAC6 进行 Active Directory 登录并且准备用来登录系统的域用户帐户已启用可进行 iDRAC6 Active Directory 登录。

另外确保已启用 Active Directory 登录设置。请参阅"将 iDRAC6 用于 Microsoft Active Directory"了解如何设置 Active Directory 用户的详情。还必须通过上载从 Active Directory 根域获得的有效 *keytab* 文件到 iDRAC6 来启用 iDRAC6 作为加密服务。

请参阅"配置 iDRAC6 以使用单一登录"了解如何使用 GUI 和 CLI 启用单一登录。

使用 Active Directory 用户的单一登录来登录到 iDRAC6

注： 要登录到 iDRAC6，应确保具有 Microsoft Visual C++ 2005 程序库的最新运行时组件。有关详情，请参阅 Microsoft 网站。

1. 使用有效 Active Directory 帐户登录到系统。
2. 在浏览器的地址栏中键入 iDRAC6 的网址。

   注： 根据浏览器设置的不同，在第一次使用此功能时可能会提示下载并安装单一登录 ActiveX 插件。

   可以使用相应的 Microsoft Active Directory 权限登录到 iDRAC6，但要求：

   - 是 Microsoft Active Directory 用户。
   - 在 iDRAC6 中配置进行 Active Directory 登录。
   - 启用 iDRAC6 进行 Kerberos Active Directory 验证。

为 Smart Card 登录配置 Active Directory 用户

开始使用 Active Directory Smart Card 登录功能前，确保已配置 iDRAC6 进行 Active Directory 登录并且已颁发 Smart Card 的用户帐户已启用 iDRAC6 Active Directory 登录。

另外确保已启用 Active Directory 登录设置。有关如何设置 Active Directory 用户的详情，请参阅"将 iDRAC6 用于 Microsoft Active Directory"。还必须通过上载从 Active Directory 根域获得的有效 *keytab* 文件到 iDRAC6 来启用 iDRAC6 作为加密服务。

目录

目录

配置用于 iDRAC6 的 VFlash 介质卡

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

VFlash 介质卡是一种安全数字 (SD) 卡，可插入系统背面的可选 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。有关如何安装和从系统拆下 vFlash 介质卡的信息，请参阅 **support.dell.com\manuals** 上的*《硬件用户手册》*。

使用 iDRAC6 Web 界面配置 VFlash 介质卡

启用或禁用 VFlash 介质卡

注： 只有在 vFlash 介质卡存在时，**"Virtual Flash Enable"（虚拟闪速更新启用）**选项才可用。如卡不存在，则显示以下信息：

`SD Card not inserted`（未插入 SD 卡）。`Please insert an SD card of size greater than 256MB`（请插入大于 256MB 的 SD 卡）。

1. 确保 VFlash 介质卡已安装。
2. 打开支持的 Web 浏览器窗口并登录 iDRAC6 Web 界面。
3. 在系统树中选择**"System"（系统）**。
4. 单击**"Virtual Flash"（虚拟闪速更新）**选项卡。

   将显示**"Virtual Flash"（虚拟闪速更新）**屏幕。
5. 选择**"Virtual Flash Enable"（虚拟闪速更新启用）**选项启用 vFlash 介质卡。启用虚拟闪速更新会将 SD 卡上创建的映像文件 **ManagedStore.IMG** 公开为所选大小的 USB 闪存盘。只有当 SD 卡上存在有效 **ManagedStore.IMG** 映像时，虚拟闪速更新才能启用。要禁用，清除此选项。

   注： *"Virtual Flash"（虚拟闪速更新）*GUI 页上的 ManagedStore.IMG 和 ManagedStore.ID 文件在主机服务器的操作系统上不可见，但在 SD 卡上可见。
6. 单击**"Apply Changes"（应用更改）**。

格式化 vFlash 介质卡

注： **"Format"（格式化）**选项仅在 vFlash 介质卡存在时才可用。另外，只有在虚拟闪速更新禁用时，SD 卡才能格式化。

1. 登录到 iDRAC6 Web 界面。
2. 在系统树中选择**"System"（系统）**。
3. 单击**"Virtual Flash"（虚拟闪速更新）**选项卡。

   将显示**"Virtual Flash"（虚拟闪速更新）**屏幕。
4. 清除**"Virtual Flash Enable"（虚拟闪速更新启用）**选项。
5. 单击**"Format"（格式化）**在 SD 卡上创建虚拟闪速更新映像文件 **ManagedStore.IMG**。文本文件 **ManagedStore.ID** 也会在 SD 卡上创建并且提供有关虚拟闪速更新映像的信息。

   出现警报对话框，警告卡上任何现有映像都会在格式化过程中清除并请求确认。单击**"OK"（确定）**继续。

   显示状态栏，指示格式化进度。

上载磁盘映像

1. 确保映像文件大小不超过 256 MB。

   注： 虽然您的 VFlash 卡可能大于 256 MB，但此时仅可访问 256 MB。

   注： 虚拟闪速更新允许直接在 vFlash 介质上存储紧急引导映像和诊断工具。映像文件可以是 DOS 可引导软盘映像，即 ***.img** 文件（对于 Windows）或来自 Red Hat® Enterprise Linux® 介质的 **diskboot.img** 文件（对于 Linux）。**diskboot.img** 可用于创建应急磁盘或创建用于执行网络安装的磁盘。可以使用虚拟闪速更新保存持久映像供平时使用或以后应急之用。

2. 登录到 iDRAC6 Web 界面。

3. 在系统树中选择**"System"（系统）**。

4. 单击**"Virtual Flash"（虚拟闪速更新）**选项卡。

   将显示**"Virtual Flash"（虚拟闪速更新）**屏幕。

5. 清除**"Virtual Flash Enable"（虚拟闪速更新启用）**选项。

6. 在**"Virtual Flash Drive"（虚拟闪速更新驱动器）**部分，输入映像文件路径或单击**"Browse"（浏览）**导航至其在系统中的位置。

   单击**"Upload"（上载）**。

   显示状态栏，指示上载进度。

注： 可以上载可引导 ISO 映像到虚拟闪速更新分区，但是不再可引导。转换 ISO 映像为 IMG 映像以使 IMG 映像可以引导。

查看虚拟闪存盘大小

"Virtual Flash Key Size"（虚拟闪存盘大小）下拉式菜单显示当前的大小设置。

使用 RACADM 配置 VFlash 介质卡

启用或禁用 VFlash 介质卡

打开到服务器的本地控制台，登录并输入：

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 或 0 ]
```

其中 1 为启用，0 为禁用。

注： 有关 cfgRacVirtual 的详情（包括输出详情），请参阅"cfgRacVirtual"。

注： RACADM 命令只有在 vFlash 介质卡存在时有用。如果没有卡，将会显示以下信息：*"ERROR: Unable to perform the requested operation."（错误：无法执行请求的操作。）* *"Ensure that a non®Cwrite protected SD Card is inserted."（确保插入无写保护的 SD 卡）*。

重设 vFlash 介质卡

打开到服务器的 Telnet/SSH 文本控制台，登录并输入：

```
racadm vmkey reset
```

警告： 使用 RACADM 命令重设 vFlash 介质卡会将闪存盘的大小重设为 256MB 并删除全部现有数据。

注： 有关 vmkey 的详情，请参阅"vmkey"。RACADM 命令只有在 vFlash 介质卡存在时才有用。如果没有卡，将会显示以下信息：*"ERROR: Unable to perform the requested operation."（错误：无法执行请求的操作。）* *"Ensure that a SD Card is inserted."（确保插入 SD 卡）*。

目录

目录

电源监控和管理

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 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。

从电源角度上看，基础硬件设计已优化：

- 高效电源设备和稳压器已整合到设计当中。
- 如适用，选用最低的电源组件。
- 机箱设计已通过系统优化空气流通，从而将风扇的功率降至最低。

PowerEdge 系统提供各种功能，以控制和管理电源：

- **"Power Inventory and Budgeting"（电源资源清册和预算）：**在引导时，系统资源清册允许计算当前配置的系统电源预算。
- **"Power Capping"（功率封顶）：**可对系统进行节流，以维持指定的功率限额。
- **"Power Monitoring"（电源监控）：**iDRAC6 对电源设备进行状况轮询，以收集功率测量数据。iDRAC6 采集功耗测量历史并计算运行平均值、峰值等。您可使用 iDRAC6 基于 Web 的界面在**"Power Monitoring"（电源监控）**页上查看信息。

电源资源清册、电源预算和封顶

从使用的角度上看，机架层上的冷却数量可能有限。通过用户定义的功率限额，可以随心分配所需的功率，从而满足您的性能需求。

iDRAC6 监控功耗并动态调节处理器，从而满足您定义的功率限额水平，在满足功率需求的同时尽量提高性能。

电源监控

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

- 累计功率
- 平均、最小和最大功率
- 功率余量值
- 功耗（也在基于 Web 的界面中以图形形式显示）

配置和管理电源

您可使用 iDRAC6 基于 Web 的界面和 RACADM 命令行界面 (CLI) 在 PowerEdge 系统上管理和配置电源控制。具体说来，可以：

- 查看服务器的电源状态
- 在服务器上执行电源控制操作（例如打开电源、关闭电源、系统重设、关机后再开机）
- 查看服务器和已安装电源设备的电源预算信息，例如最小和最大潜在功耗
- 查看和配置服务器的电源预算阈值

查看电源设备的运行状态

"Power Supplies"（电源设备）页显示服务器上所安装电源设备的状态和额定值。

使用基于 Web 的界面

要查看电源设备的运行状况：

1. 登录到 iDRAC6 基于 Web 的界面。
2. 选择系统树中的**"Power Supplies"（电源设备）**。**"Power Supplies"（电源设备）**页显示和提供下列信息：
   - **"Power Supplies Redundancy Status"（电源设备冗余状态）**：可能值为：
     - **"Full"（完全）**：电源设备 PS1 和 PS2 的类型相同，且均正常工作。
     - **"Lost"（掉失）**：电源设备 PS1 和 PS2 的类型不同，或者其中一台电源设备发生故障。不存在冗余情况。
     - **"Disabled"（已禁用）**：两台电源设备中只有一台可供使用。不存在冗余情况。
   - **"Individual Power Supply Elements"（各个电源设备组件）**可能值为：
   - **"Status"（状态）**显示如下：
     - **"OK"（良好）**表示电源设备存在且正在与服务器通信。
     - **"Warning"（警告）**表示只发出警告警报并且必须由管理员采取纠正措施。如果没有采取纠正措施，将可能发生影响服务器完整性的严重电源故障。
     - **"Severe"（严重）**表示已至少发出一个故障警报。故障状态表示服务器上发生电源故障，必须立即采取纠正措施。
   - **"Location"（位置）** 显示电源设备名称：PS-n，其中 n 为电源设备编号。
   - **"Type"（类型）**显示电源设备的类型，例如 AC 或 DC（AC 至 DC 或 DC 至 DC 电压转换）。
   - **"Input Wattage"（输入功率）** 显示电源设备的输入功率，其为系统可放置在数据中心的最大 AC 电源负载。
   - **"Maximum Wattage"（最大功率）**显示电源设备的最大功率，为系统可用的直流电源。此值用于确定电源设备容量足以供系统配置使用。
   - **"Online Status"（联机状态）**表示电源设备的电源状态：存在和良好、输入掉失、不存在或预测故障。
   - **"FW Version"（FW 版本）**显示电源设备的固件版本。

   注： 由于电源设备的效率，导致最大功率与输入功率不同。例如，如果电源设备的效率为 89%，最大功率则为 717W，而输入功率估计为 797W。

使用 RACADM

打开到 iDRAC 的 Telnet/SSH 文本控制台，登录并键入：

```
racadm getconfig -g cfgServerPower
```

查看电源预算

服务器在**"Power Budget Information"（电源预算信息）**页上提供电源子系统的电源预算状态概览。

使用 Web 界面

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

1. 登录到 iDRAC6 基于 Web 的界面。
2. 单击**"Power Management"（电源管理）**选项卡。
3. 选择**"Power Budget"（电源预算）**选项。
4. 将显示**"Power Budget Information"（电源预算信息）**页。

第一张表中显示当前系统配置用户指定功率封顶阈值的最小和最大限制。这些表示您可设定作为系统上限的 AC 功耗的范围。一旦选中，此上限将为系统可放置在数据中心的最大 AC 电源负载。

"Minimum Potential Power Consumption"（最小潜在功耗）显示您可指定的最低电源预算阈值。

"Maximum Potential Power Consumption"（最大潜在功耗）显示您可指定的最高电源预算阈值。此值也是当前系统配置的绝对最大功耗。

使用 RACADM

打开到 iDRAC 的 Telnet/SSH 文本控制台，登录并键入：

```
racadm getconfig -g cfgServerPower
```

注： 有关 cfgServerPower 的详情（包括输出详情），请参阅"cfgServerPower"。

电源预算阈值

如果启用电源预算阈值，则可设定系统的功率封顶限制。系统性能会被动态调整以保持功耗接近指定阈值。在性能调整完成之前，工作负载轻时实际功耗可能较低，且可能会短暂地超过阈值。

如果您选中电源预算阈值的**"Enabled"（已启用）**，系统将强制执行用户指定的阈值。如果您取消选中电源预算阈值，**系统不会达到**功率限额。例如，指定系统配置的最大潜在功耗为 700W，最小潜在功耗为 500W。您可指定和启用电源预算阈值，将其 650W 的电流功耗降低至 525W。自此，系统性能将被动态调整以保持功耗，从而不会超过用户指定 525W 的阈值。

使用基于 Web 的界面

1. 登录到 iDRAC6 基于 Web 的界面。
2. 单击**"Power Management"（电源管理）**选项卡。
3. 选择**"Power Budget"（电源预算）**选项。将显示**"Power Budget Information"（电源预算信息）**页。
4. 在**"Power Budget Threshold"（电源预算阈值）**表中输入以瓦特、BTU/小时或百分比为单位的值。您指定以瓦特或 BTU/小时为单位的值将为电源预算阈值限制值。如果您指定以百分比为单位的值，其将为最大至最小潜在功耗间隔的百分比。例如，100% 阈值表示最大潜在功耗，而 0% 表示最小潜在功耗。

   注： 电源预算阈值不得超过最大潜在功耗或低于最小潜在功耗。

5. 选中**"Enabled"（已启用）**以启用阈值，或保持取消选中。如果您指定**"Enabled"（已启用）**，系统将强制执行用户指定阈值。如果您**取消选中**，系统将不会达到功率限额。
6. 单击**"Apply Changes"（应用更改）**。

使用 RACADM

```
racadm config -g cfgServerPower -o cfgServerPowerCapWatts <功率限额瓦特值>

racadm config -g cfgServerPower -o cfgServerPowerCapBTUhr <功率限额 BTU/小时值>

racadm config -g cfgServerPower -o - cfgServerPowerCapPercent <功率限额百分比值 >
```

注： 如果将电源预算阈值设定以 BTU/小时为单位，转换成瓦特则为最接近整数的值。重新读取以 BTU/小时为单位的电源预算阈值时，瓦特转换成 BTU/小时则再次使用此方式。因此，书写的值名义上是与读取的值不同，例如，600 BTU/小时的阈值将转回为 601 BTU/小时。

查看电源监控

使用 Web 界面

要查看电源监控数据：

1. 登录到 iDRAC6 Web 界面。
2. 选择系统树中的**"Power Monitoring"（电源监控）**。将显示**"Power Monitoring"（电源监控）**页。

"Power Monitoring"（电源监控）页上提供的信息如下：

电源监控

- **"Status"（状态）："OK"（良好）**表示电源设备存在并正在与服务器通信，**"Warning"（警告）**表示已发出警告警报，**"Severe"（严重）**表示已发出故障警报。
- **"Probe Name"（探测器名称）**：系统板系统级别。此描述表明探测器在系统中按其位置受到监控。
- **"Reading"（读数）**：当前功耗，以瓦特/BTU/小时表示。

Amperage（安培）

- **"Location"（位置）** 显示电源设备名称：PS-n，其中 n 为电源设备编号
- **"Reading"（读数）**：当前功耗，以安培表示

Power Tracking Statistics（功率跟踪统计数据）

注： 列出当前时间和峰值时间时出现明显错误。根据当前时间列出的值实际为峰值时间，而根据峰值时间列出的值实际为当前时间。

- **"Cumulative"（累计）** 显示从电源设备输入端测量得到的服务器的当前累计能耗。此值以千瓦时显示，且表示系统所用总能量的累计值。您可以使用**"Reset Cumulative"（重设累计）**按钮，重设此值。
- **"Max Peak Amps"（最大峰值安培）**是指开始和当前时间所指定间隔内的最高电流值。您可以使用**"Reset Max Peaks"（重设最大峰值）**按钮，重设此值。
- **"Max Peak Watts"（最大峰值瓦数）**是指开始和当前时间所指定间隔内的最高功率值。您可以使用**"Reset Max Peaks"（重设最大峰值）**按钮，重设此值。
- **"Start Time"（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"（累计）**，您可以使用**"Reset Cumulative"（重设累计）按钮**重设此值，但系统重设或出现故障操作时其将保持原值。对于**"Max Peak Amps"（最大峰值安培）**和**"Max Peak Watts"（最大峰值瓦数）**，您可以使用**"Reset Max Peaks"（重设最大峰值）**按钮重设此值，但系统重设或出现故障操作时其将保持原值。
- **"Cumulative"（累计）**的**"Finish Time"（完成时间）**显示计算系统能耗时的当前日期和时间。对于**"Max Peak Amps"（最大峰值安培）**和**"Max Peak Watts"（最大峰值瓦数）**，**"Finish Time"（完成时间）**字段显示出现这些峰值时的时间。

注： 功率跟踪统计数据在系统重置时保持不变，因此会反映开始和结束时间间隔内的所有活动。**"Reset Max Peaks"（重置最大峰值）**按钮会将相应字段重置为零。在下一个表中，功耗数据在系统重设时不会保持不变，所以在这些时候会重设为零。显示的功率值是相应时间间隔（前一分钟、前一小时、昨天和上周）内的累计平均值。因为这里的开始到完成时间间隔可能与功率跟踪统计数据间隔不同，所以峰值功率值（最大峰值瓦数对最大功耗）可能有所不同。

Power Consumption（功耗）

- 显示系统在上一分钟、上一小时、昨天和上周的平均、最大和最小功耗。
- "Average Power Consumption"（平均功耗）：前一分钟、前一小时、昨天和上周内的平均值。
- "Max and Min Power Consumption"（最大功耗和最小功耗）：给定时间间隔内的实测最大和最小功耗。
- "Max and Min Time"（最大和最小时间）：出现最大和最小功耗时的时间。

"Headroom"（余量）

"System Instantaneous Headroom"（系统瞬间余量）显示电源设备可用电源与系统当前功耗之间的差额。

"System Peak Headroom"（系统峰值余量）显示电源设备可用电源与系统峰值功耗之间的差额。

"Show Graph"（显示图形）

单击这个按钮可显示上一小时分别以瓦特和安培为单位的 iDRAC6 功率和电流消耗图形。用户可使用图形上所提供的下拉式菜单，选择查看上周的这些统计数据。

注： 图上绘制的各数据点代表 5 分钟内读数的平均值。因此，这些图形可能无法反映功率或电流消耗中的短暂波动。

执行服务器电源控制操作

注： 要执行电源管理操作，必须具有**"Chassis Control Administrator"（机箱控制管理员）**权限。

iDRAC6 使您能够远程执行多个电源管理操作，如有序关机。

使用 Web 界面

1. 登录到 iDRAC6 Web 界面。
2. 单击**"Power Management"（电源管理）**选项卡。随即出现**"Power Control"（电源控制）**页。
3. 通过单击单选按钮选择以下**电源控制操作**中的一项：
   - **"Power On System"（打开系统电源）**可打开服务器电源（相当于服务器电源关闭时按电源按钮）。如果系统电源已经打开，则该选项被禁用。

- **"Power Off System"（关闭系统电源）**可关闭服务器电源。如果系统电源已经关闭，则该选项被禁用。
- **"NMI (Non-Masking Interrupt)"（NMI [非屏蔽中断]）**生成一条 NMI 指令导致系统停机。
- **"Graceful Shutdown"（正常关机）**可关闭系统。
- **"Reset System"（重设系统）**（温引导）可重设系统而不断电。如果系统电源已经关闭，则该选项被禁用。
- **"Power Cycle System"（系统关机后再开机）**（冷引导）可关机然后重新引导系统。如果系统电源已经关闭，则该选项被禁用。

4. 单击**"Apply"（应用）**。会显示要求确认的对话框。
5. 单击**"OK"（确定）**执行您所选的电源管理操作（例如，使系统重设）。

使用 RACADM

打开到服务器的 Telnet/SSH 文本控制台，登录并键入：

```
racadm serveraction <操作>
```

其中 <操作> 为开机、关机、关机后再开机、硬重设或电源状况。

目录

目录

配置安全功能

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

iDRAC6 提供以下安全保护功能：

- 针对 iDRAC6 管理员的高级安全选项：
  - "Console Redirection disable"（控制台重定向禁用）选项使*本地*系统用户能够使用 iDRAC6 控制台重定向功能禁用控制台重定向。
  - 本地配置禁用功能使*远程* iDRAC6 管理员能够有选择地禁用 iDRAC6 的配置：
  - BIOS POST option-ROM
  - 操作系统（使用本地 RACADM 和 Dell OpenManage Server Administrator 公用程序）
- RACADM CLI 和基于 Web 的界面操作，支持 128 位和 40 位（用于不允许 128 位加密的国家/地区）SSL 加密技术

  注： Telnet 不支持 SSL 加密技术。
- 通过基于 Web 的界面或 Racadm CLI 进行会话超时配置（以秒为单位）
- 可配置 IP 端口（在相应情况下）
- 使用加密传输层的 Secure Shell (SSH) 实现更高的安全保护。
- 每个 IP 地址的登录失败限制，在超过此限制时阻塞来自该 IP 地址的登录。
- 连接到 iDRAC6 的客户端的有限 IP 地址范围

针对 iDRAC6 管理员的安全选项：

禁用 iDRAC6 本地配置

管理员可以通过 iDRAC6 图形用户界面 (GUI) 选择**"Remote Access"（远程访问）→"Configuration"（配置）→"Services"（服务）**来禁用本地配置。选中**"Disable the iDRAC Local Configuration using option ROM"（使用 option ROM 禁用 iDRAC 本地配置）**复选框后，iDRAC6 配置公用程序—在系统引导期间按 <Ctrl+E> 访问—以只读模式运行，防止本地用户配置设备。管理员选择**"Disable the iDRAC Local Configuration using RACADM"（使用 RACADM 禁用 iDRAC 本地配置）**复选框后，本地用户不能通过 RACADM 公用程序或 Dell OpenManage Server Administrator 配置 iDRAC6，尽管这些程序仍可读取配置设置。

管理员可以启用一个或同时启用这两个选项。除了通过基于 Web 的界面启用外，管理员可以使用本地 RACADM 命令执行。

系统重新引导期间禁用本地配置

此功能禁用 Managed System 用户在系统重新引导期间配置 iDRAC6 的能力。

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

注： 仅在 iDRAC6 配置公用程序上支持此选项。要升级到此版本，请使用 Dell 支持网站 **support.dell.com** 上的 BIOS 更新软件包升级 BIOS。

从本地 RACADM 禁用本地配置

此功能禁用 Managed System 用户使用本地 RACADM 或 Dell OpenManage Server Administrator 公用程序配置 iDRAC6 的能力。

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

警告： 此功能极大地限制了本地用户从本地系统配置 iDRAC6 的能力，包括执行配置默认重设。Dell 建议谨慎使用这些功能，并且应该一次只禁用一个接口以防止一下子失去所有登录权限。

注： 请参阅 Dell 支持网站 **support.dell.com** 上有关*禁用 DRAC 中的本地配置和远程虚拟 KVM* 的白皮书了解详情。

尽管管理员可以使用本地 RACADM 命令设置本地配置选项，然而出于安全原因，可以只从带外 iDRAC6 基于 Web 的界面或命令行界面进行重设。cfgRacTuneLocalConfigDisable 选项在系统开机自检完成并且引导到操作系统环境后应用。操作系统可以是 Microsoft® Windows Server® 或 Enterprise Linux 等可以运行本地 RACADM 命令的操作系统，或者是用来运行 Dell OpenManage Deployment Toolkit 本地 RACADM 命令的 Microsoft Windows® 预安装环境或 vmlinux 的有限使用操作系统。

有几种情况可能需要管理员禁用本地配置。例如，在有多个管理员管理服务器和远程访问设备的数据中心，负责维护服务器软件的管理员可能不需要远程访问设备的管理权限。同样，技术人员在日常系统维护时会实际接触到服务器—可以重新引导系统并访问密码保护的 BIOS—但是不应能够配置远程访问设备。在这样的情况下，远程访问设备管理员可能希望禁用本地配置。

管理员应记住，由于禁用本地配置会极大地限制本地配置权限—包括重设 iDRAC6 为默认配置的能力—所以应该只在必要时使用这些选项，并且一般情况下应一次只禁用一个接口以避免一下失去所有登录权限。例如，如果管理员已禁用所有本地 iDRAC6 用户并且只允许 Microsoft Active Directory® 目录服务用户登录 iDRAC6，则 Active Directory 验证基础架构随后会出现故障，而管理员将可能无法登录。同样，如果管理员已禁用所有本地配置并在已有动态主机配置协议 (DHCP) 服务器的网络上为 iDRAC6 设置静态 IP 地址，而 DHCP 服务器随后将该 iDRAC6 IP 地址分配给网络上的另一个设备，则随后出现的冲突会禁用 DRAC 的带外连接，要求管理员通过串行连接将固件重设为默认设置。

禁用 iDRAC6 远程虚拟 KVM

管理员可以有选择地禁用 iDRAC6 远程 KVM，为本地用户在系统上工作提供了一个灵活安全的机制，防止其他人通过控制台重定向查看该用户的操作。为了使用此功能，必须在服务器上安装 iDRAC 受管节点软件。管理员可以使用以下命令禁用远程 vKVM：

```
racadm LocalConRedirDisable 1
```

命令 LocalConRedirDisable 在带参数 1 执行时会禁用现有的远程 vKVM 会话窗口

要帮助防止远程用户重写本地用户设置，此命令只对本地 RACADM 可用。管理员可以在支持 RACADM 的操作系统中使用此命令，包括 Microsoft Windows Server 2003 和 SUSE Linux Enterprise Server 10。由于此命令在整个系统重新引导过程中持续有效，管理员必须明确撤销后才能重新启用远程 vKVM。可以使用参数 0 来设置：

```
racadm LocalConRedirDisable 0
```

有几种情况可能需要禁用 iDRAC6 远程 vKVM。例如，管理员可能不希望远程 iDRAC6 用户查看系统上配置的 BIOS 设置，在这种情况下可以通过使用 LocalConRedirDisable 命令在系统开机自检期间禁用远程 vKVM。可能还希望每次管理员登录系统时都自动禁用远程 vKVM 来提高安全性，在这种情况下可以从用户登录脚本执行 LocalConRedirDisable 命令来实现。

注： 请参阅 Dell 支持网站 **support.dell.com** 上有关*禁用 DRAC 中的本地配置和远程虚拟 KVM* 的白皮书了解详情。

有关登录脚本的详情，请参阅 **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx。**

使用 SSL 和数字证书保证 iDRAC6 通信安全

本小节提供关于 iDRAC6 中包括的以下数据安全性功能的信息：

- "安全套接字层 (SSL)"
- "证书签名请求 (CSR)"
- "访问 SSL 主菜单"
- "生成证书签名请求"

安全套接字层 (SSL)

iDRAC6 包括 Web 服务器，通过配置 Web 服务器可使用行业标准的 SSL 安全协议在 Internet 上传输加密数据。基于公共密钥和私人密钥加密技术构建的 SSL 是广泛接受的技术，用于在客户端和服务器之间提供验证和加密的通信以防止网络上的窃听现象。

启用 SSL 的系统：

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

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

iDRAC6 Web 服务器包括 Dell 自签 SSL 数字证书 (Server ID)。要确保 Internet 上的高安全性，请向 iDRAC6 提交请求生成新的证书签名请求 (CSR) 来更换 Web 服务器 SSL 证书。

证书签名请求 (CSR)

CSR 是向认证机构 (CA) 请求安全服务器证书的数字请求。安全服务器证书可以保护远程系统的身份，并确保与远程系统交换的信息不会被他人查看或更改。要确保 DRAC 的安全，强烈建议您生成 CSR，将 CSR 提交至 CA，然后上载从 CA 返回的证书。

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

CA 批准 CSR 并向您发送证书后，您必须将证书上载至 iDRAC6 固件。存储在 iDRAC6 固件中的 CSR 信息必须与证书中包含的信息匹配。

访问 SSL 主菜单

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击 **SSL**。

使用 **SSL 主菜单**（请参阅表 23-1）生成 CSR，上载现有服务器证书，或查看现有服务器证书。CSR 信息存储在 iDRAC6 固件中。 表 23-2 说明了 **SSL** 页上的可用按钮。

表 23-1. SSL 主菜单

字段	说明
生成证书签名请求 (CSR)	单击**"Next"（下一步）**打开该页，可以生成 CSR 发送给 CA 以请求安全 Web 证书。
"Upload Server Certificate"（上载服务器证书）	单击**"Next"（下一步）**，上载您公司拥有的现有证书并用来控制对 iDRAC6 的访问。 **注：** 只有 Base 64 编码的 X509 证书才能被 iDRAC6 接受。不接受 DER 编码的证书。上载新证书会替换 iDRAC6 中原有的默认证书。
"View Server Certificate"（查看服务器证书）	单击**"Next"（下一步）**查看现有服务器证书。

表 23-2. SSL 主菜单按钮

按钮	说明
"Print"（打印）	打印**"SSL Main Menu"（SSL 主菜单）**页。
"Refresh"（刷新）	重载**"SSL Main Menu"（SSL 主菜单）**页。
"Next"（下一步）	导航至下一页。

生成证书签名请求

注： 每个 CSR 都会改写固件上任何原有的 CSR。在 iDRAC 能够接受已签名的 CSR 前，固件中的 CSR 必须匹配 CA 返回的证书。

1. 在**"SSL Main Menu"（SSL 主菜单）**上，选择**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**并单击**"Next"（下一步）**。
2. 在**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**页上键入每个 CSR 属性的值。

   表 23-3 说明了**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**页选项。
3. 单击**"Generate"（生成）**打开或保存 CSR。
4. 单击相应的**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**页按钮继续。 表 23-4 说明了**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**页上的可用按钮。

表 23-3. 生成证书签名请求 (CSR) 页选项

字段	说明
"Common Name"（常用名）	认证的确切名（通常是 Web Server 的域名，例如，**www.xyzcompany.com**）。只有字母数字字符、连字符、下划线、空格和句点有效。
"Organization Name"（组织名称）	与此组织相关的名称（例如，XYZ 公司）。只有字母数字字符、连字符、下划线、句点和空格有效。
"Organization Unit"（组织部门）	与组织部门相关的名称（例如，事业组）。只有字母数字字符、连字符、下划线、句点和空格有效。
"Locality"（地点）	认证实体的城市或其它位置（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。使用下拉式菜单选择国家/地区。
"Email"（电子邮件）	与 CSR 相关的电子邮件地址。可以键入公司的电子邮件地址，或任何想与 CSR 关联的电子邮件地址。此字段可选。

表 23-4. 生成证书签名请求 (CSR) 页按钮

按钮	说明
"Print"（打印）	打印"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）页。
"Refresh"（刷新）	重载"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）页。
"Go Back to SSL Main Menu"（返回 SSL 主菜单）	返回"SSL Main Menu"（SSL 主菜单）页。
"Generate"（生成）	生成 CSR。

查看服务器证书

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

   表 23-5 说明"Certificate"（证书）窗口中列出的字段及相关说明。

2. 单击相应的"View Server Certificate"（查看服务器证书）页按钮继续。

表 23-5. 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

使用 Secure Shell (SSH)

有关使用 SSH 的信息，请参阅"使用 Secure Shell (SSH)"。

配置服务

注： 要修改这些设置，必须具有"Configure iDRAC"（配置 iDRAC）权限。此外，仅当用户作为 **root** 登录时，才可以启用远程 RACADM 命令行公用程序。

1. 展开**系统**树并单击"Remote Access"（远程访问）。
2. 单击"Configuration"（配置）选项卡，然后单击"Services"（服务）。
3. 根据需要配置以下服务：
   - 本地配置（表 23-6）
   - Web Server（表 23-7）
   - SSH（表 23-8）
   - Telnet（表 23-9）
   - 远程 RACADM（表 23-10）
   - SNMP 代理（表 23-11）
   - 自动系统恢复代理（表 23-12）

   使用**自动系统恢复代理**启用 iDRAC6 的**上次崩溃屏幕**功能。

   注： 必须安装 **Server Administrator** 并启用其**自动恢复**功能，方法是将"Action"（动作）设置为："Reboot System"（重新引导系统）、"Power Off System"（关闭系统电源）或"Power Cycle System"（系统关机再开机），这样才能使**上次崩溃屏幕**在 iDRAC6 中运行。

4. 单击"Apply Changes"（应用更改）。

5. 单击相应的**"Services"（服务）页**按钮继续。请参阅表 23-13。

表 23-6. 本地配置设置

设置	说明
使用 option ROM 禁用 iDRAC 的本地配置	使用 option ROM 禁用 iDRAC 的本地配置。option ROM 会在系统重新引导期间提示按 <Ctrl+E> 进入设置模块。
使用 RACADM 禁用 iDRAC 的本地配置	使用本地 RACADM 禁用 iDRAC 的本地配置。

表 23-7. Web Server 设置

设置	说明
"Enabled"（已启用）	启用或禁用 Web Server。选中=启用；未选中=禁用。
"Max Sessions"（最大会话数）	此系统允许的最大同时会话数。
"Active Sessions"（激活的会话数）	系统上的当前会话数，小于等于**"Max Sessions"（最大会话数）**。
"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直接影响并终止当前的 Web 界面会话。Web Server 也可进行重设。请等待几分钟，然后再打开新的 Web 界面会话。超时范围为 60 至 10800 秒。默认值为 1800 秒。
"HTTP Port Number"（HTTP 端口号）	侦听服务器连接的 iDRAC 使用的端口。默认设置为 **80**。
"HTTPS Port Number"（HTTPS 端口号）	侦听服务器连接的 iDRAC 使用的端口。默认设置为 **443**。

表 23-8. SSH 设置

设置	说明
"Enabled"（已启用）	启用或禁用 SSH。选中后，复选框表示 SSH 已启用。
"Timeout"（超时）	Secure Shell 闲置超时，以秒为单位。超时范围为 60 至 1920 秒。输入 0 秒将禁用超时功能。默认为 **300**。
"Port Number"（端口号）	iDRAC6 侦听 SSH 连接所在的端口。默认为 **22**。

表 23-9. Telnet 设置

设置	说明
"Enabled"（已启用）	启用或禁用 Telnet。选中后，就启用 Telnet。
"Timeout"（超时）	Telnet 闲置超时，以秒为单位。超时范围为 60 至 1920 秒。输入 0 秒将禁用超时功能。默认为 **300**。
"Port Number"（端口号）	iDRAC6 侦听 Telnet 连接所在的端口。默认为 **23**。

表 23-10. 远程 RACADM 设置

设置	说明
"Enabled"（已启用）	启用/禁用远程 RACADM。选中后，就启用远程 RACADM。
"Active Sessions"（激活的会话数）	系统上的当前会话数。
"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）**。

表 23-11. SNMP 代理设置

设置	说明
"Enabled"（已启用）	启用或禁用 SNMP 代理。选中=启用；未选中=禁用。
"Community Name"（团体名称）	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。默认设置为 **public**。

表 23-12. 自动系统恢复代理设置

设置	说明
"Enabled"（已启用）	启用自动系统恢复代理。

表 23-13. 服务页按钮

按钮	说明
"Print"（打印）	打印**"Services"（服务）**页。
"Refresh"（刷新）	刷新**"Services"（服务）**页。
"Apply Changes"（应用更改）	应用**"Services"（服务）**页设置。

启用其它 iDRAC6 安全选项

要防止未授权访问远程系统，iDRAC6 提供了以下功能：

- IP 地址筛选 (IPRange) — 定义可以访问 iDRAC6 的特定范围的 IP 地址。
- IP 地址阻塞 — 限制特定 IP 地址的失败登录尝试次数。

这些功能在 iDRAC6 默认配置中禁用。使用以下子命令或基于 Web 的界面启用这些功能。

```
racadm config -g cfgRacTuning -o <对象名> <值>
```

此外，将这些功能与相应的会话空闲超时值以及定义的网络安全计划结合使用。

以下小节提供了有关这些功能的其它信息。

IP 筛选 (IpRange)

IP 地址筛选（或 *IP 范围检查*）只允许 IP 地址在用户特定范围内的客户端或管理工作站对 iDRAC6 进行访问。所有其它登录都将被拒绝。

IP 筛选将接入登录的 IP 地址与以下 **cfgRacTuning** 属性中指定的 IP 地址范围相比较：

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

cfgRacTuneIpRangeMask 属性既应用于接入 IP 地址，也应用于 **cfgRacTuneIpRangeAddr** 属性。如果两个属性的结果相同，则允许接入登录请求访问 iDRAC6。从该范围以外的 IP 地址登录将收到一个错误。

如果以下表达式等于零，登录将会继续：

```
cfgRacTuneIpRangeMask & (<进入的 IP 地址> ^ cfgRacTuneIpRangeAddr)
```

其中 & 是数量的按位"与"，而 ^ 是按位"异或"。

请参阅"iDRAC6 属性数据库组和对象定义"查看 **cfgRacTuning** 属性的完整列表。

表 23-14. IP 地址筛选 (IpRange) 属性

属性	说明
cfgRacTuneIpRangeEnable	启用 IP 范围检查功能。
cfgRacTuneIpRangeAddr	根据子网掩码中的 1，确定可接受的 IP 地址位样式。 此属性是与 **cfgRacTuneIpRangeMask** 的按位"与"，确定所允许 IP 地址的高端。允许在高位包含此位样式的任何 IP 地址建立 iDRAC6 会话。从该范围外的 IP 地址登录都会失败。各属性中的默认值允许从 192.168.1.0 到 192.168.1.255 的地址范围建立 iDRAC6 会话。
cfgRacTuneIpRangeMask	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。

启用 IP 筛选

以下是 IP 筛选设置的示例命令。

请参阅"远程使用 RACADM"了解有关 RACADM 和 RACADM 命令的详情。

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

要将登录限制到一个 IP 地址（例如，192.168.0.57），则使用全掩码，如下所示。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

要将登录限制到一小组四个相邻 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
```

IP 筛选原则

启用 IP 筛选时应遵循以下原则：

- 确保 **cfgRacTuneIpRangeMask** 配置为网络掩码的形式，所有的高位为 1（定义掩码中的子网），在低位都变为 0。
- 用所要的范围基础地址作为 **cfgRacTuneIpRangeAddr** 的值。此地址的 32 位二进制值应将掩码中为零的所有低位都设为零。

IP 阻塞

IP 阻塞动态确定来自特定 IP 地址的额外登录失败，并阻塞（或防止）该地址在预选的时间长度内登录 iDRAC6。

IP 阻塞参数使用 **cfgRacTuning** 组功能，其中包括：

- 允许的登录失败次数
- 按秒计算的必须出现这些失败的时间范围
- 在超过允许失败总数后阻止"有问题"IP 地址建立会话的时间（秒）

随着特定 IP 地址的登录失败次数不断累积，这些值会由内部计数器"增加"。当用户成功登录后，失败历史记录就会清除并且内部计数器将重设。

注： 如果客户端 IP 地址的登录尝试遭到拒绝，有些 SSH 客户端会显示以下信息：ssh exchange identification: Connection closed by remote host.（ssh exchange 标识：连接被远程主机关闭。）

请参阅"iDRAC6 属性数据库组和对象定义"查看 **cfgRacTuning** 属性的完整列表。

表 23-15 列出了用户定义的参数。

表 23-15. 登录重试限制属性

属性	定义
cfgRacTuneIpBlkEnable	启用 IP 阻塞功能。 如果在一段时间内 (**cfgRacTuneIpBlkFailWindow**) 某 IP 地址出现连续的失败 (**cfgRacTuneIpBlkFailCount**)，则在一段时间内 (**cfgRacTuneIpBlkPenaltyTime**) 来自该地址的其它建立会话尝试都会遭到拒绝。
cfgRacTuneIpBlkFailCount	设置拒绝某 IP 地址的登录尝试前允许的登录失败次数。
cfgRacTuneIpBlkFailWindow	计算失败尝试次数的时间范围（秒）。当失败次数超出此限制，将不会记入计数器。
cfgRacTuneIpBlkPenaltyTime	定义来自失败次数过多的某 IP 地址的所有登录尝试被拒绝的时间长度（秒）。

启用 IP 阻塞

以下示例显示，如果客户端在一分钟内超过五次登录尝试失败，将阻止该客户 IP 地址建立会话五分钟。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

以下示例在一分钟内阻止三次以上的失败尝试，并阻止其它登录尝试一小时。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

使用 iDRAC6 GUI 配置网络安全设置

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

1. 在**系统**树中，单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Network"（网络）**。
3. 在**"Network Configuration"（网络配置）**页中，单击**"Advanced Settings"（高级设置）**。
4. 在**"Network Security"（网络安全性）**页中，配置属性值，然后单击**"Apply Changes"（应用更改）**。

   表 23-16 说明了**"Network Security"（网络安全性）**页设置。
5. 单击相应的**"Network Security"（网络安全性）**页按钮继续。请参阅表 23-17 了解**"Network Security"（网络安全性）**页按钮的说明。

表 23-16. 网络安全性页设置

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

表 23-17. 网络安全性页按钮

按钮	说明
"Print"（打印）	打印**"Network Security"（网络安全性）**页
"Refresh"（刷新）	重载**"Network Security"（网络安全性）**页
"Apply Changes"（应用更改）	保存对**"Network Security"（网络安全性）**页所做的更改。
"Go Back to Network Configuration Page"（退回到网络配置页）	返回**"Network Configuration"（网络配置）**页。

目录

目录

iDRAC6 的基本安装

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节介绍了如何安装和设置 iDRAC6 硬件和软件。

准备工作

在安装和配置 iDRAC6 软件之前，检查一下系统随附的项目：

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

安装 iDRAC6 Express/Enterprise 硬件

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

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

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

配置系统使用 iDRAC6

要配置系统使用 iDRAC6，请使用 iDRAC6 配置公用程序。

要运行 iDRAC6 配置公用程序：

1. 打开或重新启动系统。
2. 在开机自检期间出现提示时，请按 <Ctrl><E>。

   如果按 <Ctrl><E> 之前已开始载入操作系统，请让系统完成引导过程，然后重新启动系统并再试一次。

3. 配置 LOM。
   a. 使用箭头键选择 LAN 参数，然后按 <Enter>。随即显示"NIC Selection"（NIC 选择）。
   b. 使用箭头键选择以下某个NIC 模式：
      - **"Dedicated"（专用）**— 选择此选项可以使远程访问设备能够使用 iDRAC Enterprise 上的专用网络接口。此接口不与主机操作系统共享并会将管理通信路由到单独的物理网络，从而能够与应用程序通信分开。此选项只有在系统中装有 iDRAC6 Enterprise 时才可用。
      - **"Shared"（共享）**— 选择此选项可以与主机操作系统共享网络接口。当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1 和 NIC 2 接收数据，但是只通过 NIC 1 发送数据。如果 NIC 1 出现故障，远程访问设备将不可访问。
      - **"Shared with Failover LOM2"（与故障转移 LOM2 共享）**— 选择此选项可以与主机操作系统共享网络接口。当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1 和 NIC 2 接收数据，但是只通过 NIC 1 发送数据。如果 NIC 1 出现故障，远程访问设备会故障转移到 NIC 2 进行所有数据发送。远程访问设备会继续使用 NIC 2 进行数据发送。如果 NIC 2 出现故障，远程访问设备会故障转移回 NIC 1 来进行所有数据发送，但前提是 NIC 1 中的故障已经得以纠正。
      - **"Shared with Failover All LOMs"（与故障转移所有 LOM 共享）**— 选择此选项可以与主机操作系统共享网络接口。当主机操作系统针对 NIC 组配置后，远程访问设备网络接口将具有全部功能。远程访问设备通过 NIC 1、NIC 2、NIC 3 和 NIC 4 接收数据，但是只通过 NIC 1 发送数据。如果 NIC 1 出现故障，远程访问设备会故障转移回 NIC 2 来进行所有数据发送。如果 NIC 2 出现故障，远程访问设备会故障转移回 NIC 3 来进行所有数据发送。如果 NIC 3 出现故障，远程访问设备会故障转移回 NIC 4 来进行所有数据发送。如果 NIC 4 出现故障，远程访问设备会故障转移回 NIC 1 来进行所有数据发送，但前提是原来的 NIC 1 故障已经得以纠正。此选项可能在 iDRAC6 Enterprise 上不可用。
4. 配置网络控制器 LAN 参数使用 DHCP 或静态 IP 地址源。
   a. 使用下箭头键，选择**"LAN Parameters"（LAN 参数）**并按 <Enter>。

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

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

d. 如果选择了**"Static"（静态）**，则配置**"Ethernet IP Address"（以太网 IP 地址）**、**"Subnet Mask"（子网掩码）**和**"Default Gateway"（默认网关）**设置。

e. 按 <Esc>。

5. 按 **<Esc>。**

6. 选择**"Save Changes and Exit"（保存更改并退出）**。

软件安装和配置概览

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

安装 iDRAC6 软件

要安装 iDRAC6 软件：

1. 在 Managed System 上安装软件。请参阅"在 Managed System 上安装软件"。

2. 在 Management Station 上安装软件。请参阅"在 Managed System 上安装软件"。

配置 iDRAC6

要配置 iDRAC6：

1. 选择以下某个配置工具：
   - 基于 Web 的界面（请参阅"使用 Web 界面配置 iDRAC6"）
   - RACADM CLI（请参阅"使用 iDRAC6 SM-CLP 命令行界面"）
   - Telnet 控制台（请参阅"使用 Telnet 控制台"）

   注： 同时使用一个以上的 iDRAC6 配置工具可能会产生意外的结果。

2. 配置 iDRAC6 网络设置。请参阅"配置 iDRAC6 网络设置"。

3. 添加并配置 iDRAC6 用户。请参阅"添加和配置 iDRAC6 用户"。

4. 配置 Web 浏览器以使用基于 Web 的界面。请参阅"配置支持的 Web 浏览器"。

5. 禁用 Microsoft® Windows® 自动重新启动选项。请参阅"禁用 Windows 自动重新引导选项"。

6. 更新 iDRAC6 固件。请参阅"更新 iDRAC6 固件"。

在 Managed System 上安装软件

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

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

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

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

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

有关上次崩溃屏幕的详情，请参阅"查看上次系统崩溃屏幕"。

在 Management Station 上安装软件

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

- DVD 根目录 - 包含 Dell Systems Build and Update Utility，这提供了服务器设置和系统安装的信息
- SYSMGMT - 包含系统管理软件产品，其中包括 Dell OpenManage Server Administrator
- Docs - 包含系统管理软件产品、外围设备和 RAID 控制器的说明文件
- SERVICE - 包含配置系统所需的工具并提供最新诊断程序和 Dell 针对系统优化的驱动程序

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

在 Linux Management Station 上安装和删除 RACADM

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

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

安装 RACADM

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

   ```
   mount /media/cdrom
   ```

3. 导航到 **/linux/rac** 目录并执行以下命令：

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

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

卸载 RACADM

要卸载 RACADM，请打开命令提示符并键入：

```
rpm -e <racadm_软件包_名称>
```

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

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

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

更新 iDRAC6 固件

使用以下某一方法更新 iDRAC6 固件。

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

准备工作

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

1. 安装并启用相应的 IPMI 和受管节点驱动程序。
2. 如果系统正在运行 Windows 操作系统，则启用并启动 **Windows Management Instrumentation** (WMI) 服务。

3. 如果您使用 iDRAC6 Enterprise 且您的系统正在运行 SUSE® Linux Enterprise Server（版本 10）for Intel® EM64T，请启动**原始** 服务。
4. 断开连接并卸下虚拟介质。

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

5. 确保 USB 已启用。

下载 iDRAC6 固件

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

iDRAC6 固件包中含有以下软件组件：

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

使用基于 Web 的界面更新 iDRAC6 固件

有关详细信息，请参阅"更新 iDRAC6 固件/系统服务恢复映像"。

使用 RACADM 更新 iDRAC6 固件

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

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

   例如：

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

2. 运行以下 RACADM 命令：

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

   还可以使用远程 RACADM 和 TFTP 服务器更新固件。

   例如：

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

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

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

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

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

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

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

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

清除浏览器高速缓存

固件升级后，清除 Web 浏览器高速缓存。

请参阅 Web 浏览器的联机帮助了解有关详情。

配置支持的 Web 浏览器

以下各节提供了有关配置支持的 Web 浏览器的说明。

配置 Web 浏览器以连接到 iDRAC6 基于 Web 的界面

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

要配置 Internet Explorer Web 浏览器访问代理服务器：

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

可信域列表

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

32 位和 64 位 Web 浏览器

64 位 Web 浏览器不支持 iDRAC6 基于 Web 的界面。如果打开 64 位浏览器，则会访问"Console Redirection"（控制台重定向）页并尝试安装插件，安装过程将会失败。如果此错误未得到确认并且重复此过程，即使在第一次尝试期间插件安装失败，"Console Redirect"（控制台重定向）页也会载入。出现此问题的原因在于，即使插件安装过程已失败，Web 浏览器也会将插件信息存储在配置文件目录中。要修复此问题，安装并运行支持的 32 位 Web 浏览器，并登录 iDRAC6。

查看本地化版本的基于 Web 的界面

Windows

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

- 英语
- 法语
- 德语
- 西班牙语
- 日语
- 简体中文

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

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

要选择一种以上的语言，按 <Ctrl>。

5. 选择首选语言并单击**"Move Up"（上移）**将语言移动到列表顶部。

6. 单击**"OK"（确定）**。

7. 在**"Language Preference"（语言首选项）**窗口中，单击**"OK"（确定）**。

Linux

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

1. 打开命令终端。

2. 键入 "locale" 并按 <Enter>。系统将显示以下输出。

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

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

4. 导航至 **/etc/sysconfig/i18n** 文件。

5. 在文件中，应用以下更改：

   当前项：

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

   更新项：

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

6. 注销，然后登录操作系统。

7. 重新启动 iDRAC6。

从其它语言切换到简体中文时，应确保此修复仍然有效。否则，应重复此过程。

有关 iDRAC6 的高级配置，请参阅"高级 iDRAC6 配置"。

目录

目录

使用 Web 界面配置 iDRAC6

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

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

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

本地 RACADM 命令从受管服务器执行。

SM-CLP 和 SSH/Telnet RACADM 命令在 Shell 中执行，可通过 Telnet 或 SSH 连接远程使用。有关 SM-CLP 的详情，请参阅"使用 iDRAC6 SM-CLP 命令行界面"。有关 RACADM 命令的详情，请参阅"RACADM 子命令概览"和"iDRAC6 属性数据库组和对象定义"。

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。

   有关详情，请参阅"支持的 Web 浏览器"。

   要使用 IPv4 地址访问 Web 界面，请转至步骤 2。

   要使用 IPv6 地址访问 Web 界面，请转至步骤 3。

2. 使用 IPv4 地址访问 Web 界面：必须启用 IPv4：

   在浏览器的**"Address"（地址）**栏中，键入：

   https://<iDRAC-IPv4 地址>

   然后按 <Enter>。

3. 使用 IPv6 地址访问 Web 界面：必须启用 IPv6：

   在浏览器的**"Address"（地址）**栏中，键入：

   https://[<iDRAC-IPv6 地址>]

   然后按 <Enter>。

4. 如果默认 HTTPS 端口号（端口 443）已更改，请键入：

   https://<iDRAC-IP-地址>:<端口号>

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

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

   如果默认 HTTPS 端口号（端口 443）已更改，请键入：

   https://*<iDRAC-IP-地址>*:*<端口号>*

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

将显示 iDRAC6**"Login"（登录）**窗口。

登录

您可以作为 iDRAC6 用户或 Microsoft® Active Directory® 用户登录。iDRAC6 用户的默认用户名为 **root**，默认密码为 **calvin**。

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

要登录，执行下列步骤：

1. 在**"Username"（用户名）**字段中键入下面的内容之一：

   - 您的 iDRAC6 用户名。

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

   - 您的 Active Directory 用户名。

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

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

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

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

4. 单击**"OK"（确定）**或按 <Enter>。

注销

1. 在主窗口的右上角，单击**"Logout"（注销）**关闭会话。
2. 关闭浏览器窗口。

注： **"Logout"（注销）**按钮在您登录后才出现。

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

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

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"。

配置网络和 IPMI LAN 设置

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

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

注： 如果运行时启用了生成树协议 (STP)，请保证还按以下方式打开了 PortFast 或类似技术：

- 在连接到 iDRAC6 的交换机的端口上
- 在连接到运行 iDRAC KVM 会话的 Management Station 的端口上

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

1. 单击**"Remote Access"（远程访问）→"Configuration"（配置）→"Network"（网络）。**
2. 在**"Network"（网络）**页上，可以输入网络接口卡设置、常见 iDRAC 设置、IPv4 设置、IPv6 设置、IPMI 设置和 VLAN 设置。请参阅表 4-1、表 4-2、表 4-3、表 4-4、表 4-5 和表 4-6 了解这些设置的说明。
3. 完成输入所需设置后，单击**"Apply Changes"（应用更改）**。
4. 单击相应按钮继续。请参阅表 4-7。

表 4-1. 网络接口插卡设置

设置	说明
"NIC Selection"（NIC 选择）	配置四种可能模式中的当前模式： * "Dedicated (iDRAC NIC)"（专用 [iDRAC NIC]） **注：** 只有 iDRAC6 Enterprise 才提供此选项。 * "Shared (LOM1)"（共享 [LOM1]） * "Shared with Failover LOM2"（与故障转移 LOM2 共享） * "Shared with Failover All LOMs"（与故障转移所有 LOM 共享） **注：** 此选项可能在 iDRAC6 Enterprise 上不可用。 **注：** 如果**"NIC Selection"（NIC 选择）**设置为**"Shared"（共享）**或**"Shared with Failover"（与故障转移共享）**模式，iDRAC6 将不会通过同一物理端口本地通信。这是因为网络交换机不会通过收到数据包的同一端口来发送数据包。
"MAC Address"（MAC 地址）	显示唯一标识网络中各个节点的"Media Access Control (MAC) Address"（介质访问控制 [MAC] 地址）。
"Enable NIC"（启用 NIC）	选中后，表示 NIC 已启用并激活此组中剩余的控制。当 NIC 被禁用时，通过网络往来于 iDRAC6 的所有通信均被阻止。 默认值为**"On"（开）**。
"Auto Negotiation"（自动协商）	如果设置为**"On"（开）**，则通过与最近的路由器或集线器通信显示网络速度和模式。如果设置为**"Off"（关）**，则允许手动设置网络速度和双工模式（"Off"[关]） 如果**"NIC Selection"（NIC 选择）***不是*设置为**"Dedicated"（专用）**，则总是启用"Auto Negotiation"（自动协商）设置（**"On"[开]）**。
"Network Speed"（网络速度）	使您能够根据网络环境将网络速度设置为 100 Mb 或 10 Mb。如果"Auto Negotiation"（自动协商）设置为**"On"（开）**，此选项将不可用。
"Duplex Mode"（双工模式）	使您能够根据网络环境将双工模式设置为全双工或半双工。如果**"Auto Negotiation"（自动协商）**设置为**"On"（开）**，此选项将不可用。

表 4-2. 常用 iDRAC 设置

设置	说明
"Register iDRAC on DNS"（在 DNS 上注册 iDRAC）	在 DNS 服务器上注册 iDRAC6 名称。 默认为**"Disabled"（已禁用）**。
"DNS iDRAC Name"（DNS iDRAC 名称）	只有在选中**"Register iDRAC on DNS"（在 DNS 上注册 iDRAC）**后才会显示 iDRAC6 名称。默认名称为 idrac-*服务标签*，其中 *服务标签*是 Dell 服务器的服务标签号码，例如：idrac-00002。
"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）	使用默认 DNS 域名。如果没有选中该复选框并且选择了**"Register iDRAC on DNS"（在 DNS 上注册 iDRAC）**选项，则可以在**"DNS Domain Name"（DNS 域名）**字段中修改 DNS 域名。 默认为**"Disabled"（已禁用）**。 **注：** 要选择**"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）**复选框，还应选择**"Use DHCP (For NIC IP Address)"（使用 DHCP [对于 NIC IP 地址]）**复选框。
"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用户将不能修改此字段。

表 4-3. IPv4 设置

设置	说明
"Enabled"（已启用）	如果启用了 NIC，此操作将选择 IPv4 协议支持并将此部分中的其它字段设置为启用。
"Use DHCP (For NIC IP Address)"（使用 DHCP [对于 NIC IP 地址]）	提示 iDRAC6 从动态主机配置协议 (DHCP) 服务器获取 NIC 的 IP 地址。默认值为**"off"（关）**。
"IP Address"（IP 地址）	指定 iDRAC6 NIC IP 地址。
"Subnet Mask"（子网掩码）	允许用户输入或编辑 iDRAC6 NIC 的静态 IP 地址。要更改此设置，请取消选择"Use DHCP (For NIC IP Address)"（使用 DHCP [对于 NIC IP 地址]）复选框。
"Gateway"（网关）	路由器或交换机的地址。该值采用"点分隔"格式，比如 192.168.0.1。

"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）	通过选择**"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**复选框启用 DHCP 获取 DNS 服务器地址。如果没有使用 DHCP 获取 DNS 服务器地址，应在**"Preferred DNS Server"（首选 DNS 服务器）**和**"Alternate DNS Server"（备用 DNS 服务器）**字段中提供 IP 地址。 默认值为**"off"（关）**。 **注：** 如果选中**"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**复选框，将不能在**"Preferred DNS Server"（首选 DNS 服务器）**和**"Alternate DNS Server"（备用 DNS 服务器）**字段中输入 IP 地址。
"Preferred DNS Server"（首选 DNS 服务器）	DNS 服务器 IP 地址。
"Alternate DNS Server"（备用 DNS 服务器）	备用 IP 地址。

表 4-4. IPv6 设置

设置	**说明**
"Enabled"（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"Disabled"（已禁用）。
"Auto Config"（自动配置）	选中此框将允许 iDRAC6 从动态主机配置协议 (DHCPv6) 服务器获取 iDRAC6 NIC 的 IPv6 地址。启用**"Auto Config"（自动配置）**还将取消激活并清除"IP Address 1"（IP 地址 1）、"Prefix Length"（前缀长度）和"IP Gateway"（IP 网关）的静态值。
"IP Address 1"（IP 地址 1）	为 iDRAC NIC 配置 IPv6 地址。要更改此设置，必须先通过取消选中相关复选框来禁用**"AutoConfig"（自动配置）**。
"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**"AutoConfig"（自动配置）**。
"IP Gateway"（IP 网关）	为 iDRAC NIC 配置静态网关。要更改此设置，必须先通过取消选中相关复选框来禁用**"AutoConfig"（自动配置）**。
"Link Local Address"（链路本地地址）	指定 iDRAC6 NIC IPv6 地址。
"IP Address 2"（IP 地址 2）	如果有的话，指定附加 iDRAC6 NIC IPv6 地址。
"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）	通过选择**"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**复选框启用 DHCP 获取 DNS 服务器地址。如果没有使用 DHCP 获取 DNS 服务器地址，应在**"Preferred DNS Server"（首选 DNS 服务器）**和**"Alternate DNS Server"（备用 DNS 服务器）**字段中提供 IP 地址。 默认值为"Off"（关）。检查审核副本 注：如果选中**"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**复选框，将不能在**"Preferred DNS Server"（首选 DNS 服务器）**和**"Alternate DNS Server"（备用 DNS 服务器）**字段中输入 IP 地址。
"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，必须先取消选中**"Use DHCP to obtain DNS Server Addresses"（使用 DHCP 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，必须先取消选中**"Use DHCP to obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**。

表 4-5. 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。默认值为**"Off"（关）**。
"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低权限级别。选择以下选项之一：**"Administrator"（管理员）**、**"Operator"（操作员）**或**"User"（用户）**。默认为**"Administrator"（管理员）**。
"Encryption Key"（密钥）	配置密钥：0 至 20 个十六进制字符（不允许空白）。默认为空白。

表 4-6. VLAN 设置

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

表 4-7. 网络配置页按钮

按钮	**说明**
"Print"（打印）	打印屏幕上显示的**"Network Configuration"（网络配置）**值。
"Refresh"（刷新）	重新载入**"Network Configuration"（网络配置）**页。

"Advanced Settings"（高级设置）	打开**"Network Security"（网络安全性）**页，使用户能够输入 IP 范围和 IP 阻塞属性。
"Apply Changes"（应用更改）	保存网络配置页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需要用户使用更新的 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 iDRAC"（配置 iDRAC）**权限才能执行以下步骤。

1. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**，然后单击**"Network"（网络）**选项卡以打开**"Network"（网络）**页。
2. 单击**"Advanced Settings"（高级设置）**配置网络安全性设置。

   表 4-8 说明了**"Network Security"（网络安全性）页设置**。配置完设置后，单击**"Apply"（应用）**。
3. 单击相应按钮继续。请参阅表 4-9。

表 4-8. 网络安全性页设置

设置	说明
"IP Range Enabled"（IP 范围已启用）	启用 IP 范围检查功能，定义了可以访问 iDRAC 的 IP 地址范围。默认值为**"off"（关）**。
"IP Range Address"（IP 范围地址）	根据子网掩码中的 1，确定可接受的 IP 地址位样式。该值是含 IP 范围子网掩码的按位"与"，可确定所允许的 IP 地址的高端。允许在高位包含此位样式的任何 IP 地址建立 iDRAC6 会话。从该范围外的 IP 地址登录都会失败。各属性中的默认值允许从 192.168.1.0 到 192.168.1.255 的地址范围建立 iDRAC6 会话。
"IP Range Subnet Mask"（IP 范围子网掩码）	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。默认为 **255.255.255.0**。
"IP Blocking Enabled"（IP 阻塞已启用）	启用 IP 地址阻塞功能，该功能限制在预先选择的时间范围内尝试从特定 IP 地址登录失败的次数。默认值为**"off"（关）**。
"IP Blocking Fail Count"（IP 阻塞故障计数）	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 阻塞故障时间范围）	决定一个时间范围（以秒为单位），在该范围内必须发生 IP 阻塞故障计数的故障才能触发 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 4-9. 网络安全性页按钮

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）**页。
"Apply Changes"（应用更改）	保存**"Network Security"（网络安全性）**页上所做的任何新设置。
"Return to the Network Configuration Page"（返回网络配置页）	返回**"Network Configuration"（网络配置）**页。

配置平台事件

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

表 4-10 中列出了可筛选平台事件。

表 4-10. 平台事件筛选器

索引	平台事件
1	风扇临界声明

2	电池警告声明
3	电池临界声明
4	分离电压临界声明
5	温度警告声明
6	温度临界声明
7	侵入临界声明
8	风扇冗余已降级
9	风扇冗余已丢失
10	处理器警告声明
11	处理器临界声明
12	处理器不存在
13	电源设备警告声明
14	电源设备临界声明
15	电源设备不存在
16	事件日志临界声明
17	监督临界声明
18	系统电源警告声明
19	系统电源临界声明

。

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

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

配置平台事件筛选器 (PEF)

注： 配置平台事件陷阱或电子邮件警报设置前配置平台事件筛选器。

1. 使用支持的 Web 浏览器登录远程系统。请参阅"访问 Web 界面"。
2. 单击**"System"（系统）**→ **"Alert Management"（警报管理）**→ **"Platform Events"（平台事件）**。
3. 在第一个表中，选择**"Enable Platform Event Filter Alerts"（启用平台事件筛选器警报）**复选框，然后单击**"Apply Changes"（应用更改）**。

   注： 必须启用**"Enable Platform Event Filter Alerts"（启用平台事件筛选器警报）**才能将警报发送到任何有效的配置目标（PET 或电子邮件）。
4. 在下一个表，即**"Platform Event Filters List"（平台事件筛选器列表）**中，单击要配置的筛选器。
5. 在**"Set Platform Events"（设置平台事件）**页中，选择相应的**"Shutdown Action"（关机操作）**或选择**"None"（无）**。
6. 选择或取消选择**"Generate Alert"（生成警报）**以启用或禁用此操作。

   注： 必须启用**"Generate Alert"（生成警报）**才能将警报发送到任何有效的配置目标（PET 或电子邮件）。
7. 单击**"Apply Changes"（应用更改）**。

   将返回到**"Platform Events"（平台事件）**页，其中应用的更改显示在**"Platform Event Filters List"（平台事件筛选器列表）。**
8. 重复步骤 4 至 7 以配置其它平台事件筛选器。

配置平台事件陷阱 (PET)

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

1. 使用支持的 Web 浏览器登录远程系统。请参阅"访问 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）→"Alert Management"（警报管理）→ "Traps Settings"（陷阱设置）**。

4. 在**"IPv4 Destination List"（IPv4 目标列表）**或**"IPv6 Destination List"（IPv6 目标列表）**中，单击目标号码以配置 IPv4 或 IPv6 SNMP 警报目标。

5. 在**"Set Platform Event Alert Destination"（设置平台事件警报目标）**页上，选择或取消选择**"Enable Destination"（启用目标）**。选中的框表示允许 IP 地址接收警报。取消选中的框表示禁止 IP 地址接收警报。

6. 输入有效的平台事件陷阱目标 IP 地址并单击**"Apply Changes"（应用更改）**。

7. 单击**"Send Test Trap"（发送检测陷阱）**检测配置的警报或单击**"Go Back to the Platform Event Destination Page"（退回到平台事件目标页）**。

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

   在**"Platform Event Alert Destinations"（平台事件警报目标）**页上，应用的更改显示在 IPv4 或 IPv6**"Destination List"（目标列表）**中**。**

8. 在**"Community String"（团体字符串）**字段中，输入相应的 iDRAC SNMP 团体名称。单击**"Apply Changes"（应用更改）**。

   注： 目标团体字符串必须与 iDRAC6 团体字符串相同。

9. 重复步骤 4 至 7 以配置其它 IPv4 或 IPv6 目标号码。

配置电子邮件警报

注： 电子邮件警报支持 IPv4 和 IPv6 地址。

1. 使用支持的 Web 浏览器登录远程系统。

2. 确保遵循"配置平台事件筛选器 (PEF)"中的步骤。

3. 单击**"System"（系统）→"Alert Management"（警报管理）→ "Email Alert Settings"（电子邮件警报设置）**。

4. 在**"Destination Email Addresses"（目标电子邮件地址）**下的表中，单击要配置目标地址的**"Email Alert Number"（电子邮件警报号码）**。

5. 在**"Set Email Alert"（设置电子邮件警报）**页上，选择或取消选择**"Enable E-mail Alert"（启用电子邮件警报）**。选中的框表示允许电子邮件地址接收警报。取消选中的框表示禁止电子邮件地址接收警报信息。

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

7. 在**"E-mail Description"（电子邮件说明）**字段中，键入要在电子邮件中显示的简短说明。

8. 单击**"Apply Changes"（应用更改）**。

9. 如果要检测配置的电子邮件警报，请单击**"Send Test Email"（发送检测电子邮件）**。否则，单击**"Go Back to the E-mail Alert Destination Page"（退回到电子邮件警报目标页）**。

10. 单击**"Go Back to the E-mail Alert Destination Page"（退回到电子邮件警报目标页）**，在**"SMTP (e-mail) Server IP Address"（SMTP [电子邮件] 服务器 IP 地址）**字段中输入有效的 SMTP IP 地址。

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

11. 单击**"Apply Changes"（应用更改）**。

12. 重复步骤 4 至 9 以配置其它电子邮件警报目标。

配置 IPMI

1. 使用支持的 Web 浏览器登录远程系统。

2. 配置 LAN 上 IPMI。

   a. 在**系统**树中，单击**"Remote Access"（远程访问）**。

b. 单击**"Configuration"（配置）**选项卡并单击**"Network"（网络）**。

c. 在**"Network Configuration"（网络配置）**页的**"IPMI LAN Settings"（IPMI LAN 设置）**下，选择**"Enable IPMI Over LAN"（启用 LAN 上 IPMI）**并单击**"Apply Changes"（应用更改）**。

d. 如果需要，更新 IPMI LAN 信道权限。

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

在**"IPMI LAN Settings"（IPMI LAN 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）**并单击**"Apply Changes"（应用更改）**。

e. 如果需要，设置 IPMI LAN 信道密钥。

注： iDRAC6 IPMI 支持 RMCP+ 协议。

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

注： 密钥必须包含不超过 40 个字符的偶数个十六进制字符。

3. 配置 IPMI LAN 上串行 (SOL)。

a. 在**系统**树中，单击**"Remote Access"（远程访问）**。

b. 在**"Configuration"（配置）**选项卡中，单击**"Serial Over LAN"（LAN 上串行）**。

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

d. 更新 IPMI SOL 波特率。

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

e. 单击**"Baud Rate"（波特率）**下拉式菜单，选择相应的波特率，并单击**"Apply Changes"（应用更改）**。

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

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

g. 单击**"Apply Changes"（应用更改）**。

4. 配置 IPMI 串行。

a. 在**"Configuration"（配置）**选项卡中，单击**"Serial"（串行）**。

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

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

c. 设置 IPMI 串行波特率。

单击**"Baud Rate"（波特率）**下拉式菜单，选择相应的波特率，并单击**"Apply Changes"（应用更改）**。

d. 设置信道权限级别限制。

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）**。

e. 单击**"Apply Changes"（应用更改）**。

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

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

如果 IPMI 串行处于终端模式，可以配置以下其它设置：

- 删除控制
- 回声控制
- 行编辑
- 新行序列

- 输入新行序列

有关这些属性的详情，请参阅 IPMI 2.0 规范。有关终端模式命令的其它信息，请参阅 **support.dell.com\manuals** 上的*《Dell OpenManage 底板管理控制器公用程序用户指南》*。

配置 iDRAC6 用户

有关详细信息，请参阅"添加和配置 iDRAC6 用户"。

使用 SSL 和数字证书确保 iDRAC6 通信

本节提供关于 iDRAC 中包括的以下数据安全性功能的信息：

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

安全套接字层 (SSL)

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

启用 SSL 的系统可以执行以下任务：

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

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

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

证书签名请求 (CSR)

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

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

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

通过基于 Web 的界面访问 SSL

1. 单击**"Remote Access"（远程访问）→"Configuration"（配置）**。
2. 单击 **SSL** 以打开 **SSL** 页。

使用 **SSL** 页执行以下一个选项：

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

表 4-11 说明了 **SSL** 页的以上选项。

表 4-11.

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

SSL 页选项

生成证书签名请求

注： 每个新的 CSR 都会改写固件上存储的任何以前的 CSR 数据。在 iDRAC 能够接受已签名的 CSR 前，固件中的 CSR 必须匹配 CA 返回的证书。

1. 在 **SSL** 页上，选择**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**并单击**"Next"（下一步）**。
2. 在**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**页上输入每个 CSR 属性值。 表 4-12 说明了 CSR 属性。
3. 单击**"Generate"（生成）**以创建 CSR 并将其下载到本地计算机上。
4. 单击相应按钮继续。请参阅表 4-13。

表 4-12. 生成证书签名请求 (CSR) 属性

字段	说明
"Common Name"（常用名）	证书的确切名称（通常是 iDRAC 的域名，例如，**www.xyzcompany.com**）。字母数字字符、连字符、下划线、空格和句点有效。
"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"（组织部门）	与组织部门相关的名称（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）	证书实体的城市或其它位置（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。键入公司的电子邮件地址或与 CSR 相关的任何电子邮件地址。此字段可选。

表 4-13. 生成证书签名请求 (CSR) 页按钮

按钮	说明
"Print"（打印）	打印屏幕上显示的**"Generate Certificate Signing Request"（生成证书签名请求）**值。
"Refresh"（刷新）	重载**"Generate Certificate Signing Request"（生成证书签名请求）**页。
"Generate"（生成）	生成 CSR 并随后提示用户保存到指定目录。
"Go Back to SSL Main Menu"（返回 SSL 主菜单）	使用户返回到 **SSL** 页。

上载服务器证书

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

   将显示**"Upload Server Certificate"（上载服务器证书）**页。
2. 在**"File Path"（文件路径）**字段的**"Value"（值）**字段中键入证书路径，或单击**"Browse"（浏览）**导航至证书文件。

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

3. 单击**"Apply"（应用）**。

4. 单击相应页按钮继续。请参阅表 4-14。

表 4-14. 证书上载页按钮

按钮	说明
"Print"（打印）	打印**"Certificate Upload"（证书上载）**页。
"Go Back to SSL Main Menu"（返回 SSL 主菜单）	返回**"SSL Main Menu"（SSL 主菜单）**页。
"Apply"（应用）	将证书应用于 iDRAC6 固件。

查看服务器证书

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

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

   表 4-15 说明了**"Certificate"（证书）**表中列出的字段及相关说明。

2. 单击相应按钮继续。请参阅表 4-16。

表 4-15. 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 4-16. 查看服务器证书页按钮

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

配置和管理 Active Directory 证书

使用该页可以配置和管理 Active Directory 设置。

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

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

注： 有关 Active Directory 配置和如何配置扩展模式或标准模式的 Active Directory 的详情，请参阅"将 iDRAC6 用于 Microsoft Active Directory"。

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

1. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**。

2. 单击 **Active Directory** 以打开**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页。

   表 4-17 列出了**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页选项。

3. 单击相应按钮继续。请参阅表 4-18。

表 4-17. Active Directory 配置和管理页选项

属性	说明
一般设置	
"Active Directory Enabled"（Active Directory 已启用）	指定是启用还是禁用 Active Directory。
"Single Sign-On Enabled"（单一登录已启用）	指定是启用还是禁用单一登录。如果启用，则不用输入域用户验证凭据，比如用户名和密码，就可登录 iDRAC6。值有**"Yes"（是）**和**"No"（否）**。
"Schema Selection"（模式选择）	指定配合 Active Directory 使用标准模式还是扩展模式。 **注：** 在此版本中，如果 Active directory 配置为使用扩展模式，则不支持基于智能卡的双重验证 (TFA) 和单一登录 (SSO) 功能。
"User Domain Name"（用户域名）	该值最多含有 40 个用户域条目。如果已配置，用户域名列表将显示在登录页中，作为登录用户可从中选择的下拉式菜单。如果不配置，Active Directory 用户仍然能够通过按 user_name@domain_name、domain_name/user_name 或 domain_name\user_name 格式输入用户名进行登录。
"Timeout"（超时）	指定等待 Active Directory 查询完成需要的秒数。默认值为 120 秒钟。
"Domain Controller Server Address 1-3 (FQDN or IP)"（域控制器服务器地址 1-3 [FQDN 或 IP]）	指定域控制器的完全限定域名 (FQDN) 或 IP 地址。要求至少配置 3 个地址之一。iDRAC 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。如果选择扩展模式，这些地址是 iDRAC 设备对象和关联对象所在的域控制器的地址。如果选择标准模式，这些地址是用户帐户和角色组所在的域控制器的地址。
"Certificate Validation Enabled"（启用证书验证）	连接 Active Directory 时，iDRAC 使用安全套接字层 (SSL) 上的轻量级目录访问协议 (LDAP)。默认情况下，在安全套接字层 (SSL) 握手过程中，iDRAC 使用在 iDRAC 中载入的 CA 证书验证域控制器的安全套接字层 (SSL) 服务器证书，并提供强大的安全保护。如果要进行检测或系统管理员选择信任安全边界内的域控制器而不验证其安全套接字层 (SSL) 证书，则可以禁用证书验证。此选项指定是启用还是禁用证书验证。
Active Directory CA 证书	
"Certificate"（证书）	签署所有域控制器的安全套接字层 (SSL) 服务器证书的认证机构的证书。
"Extended Schema Settings"（扩展模式设置）	**"iDRAC Name"（iDRAC 名称）**：指定唯一识别 Active Directory 中 iDRAC 的名称。该值默认为 NULL。 **"iDRAC Domain Name"（iDRAC 域名）**：Active Directory iDRAC 对象所在的域的 DNS 名称（字符串）。该值默认为 NULL。 只有 iDRAC 配置为使用扩展 Active Directory 模式时，才会显示这些设置。
"Standard Schema Settings"（标准模式设置）	**"Global Catalog Server Address 1-3 (FQDN or IP)"（全局编录服务器地址 1-3 [FQDN 或 IP]）**：指定全局编录服务器的完全限定域名 (FQDN) 或 IP 地址。要求至少配置 3 个地址之一。iDRAC 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。仅当用户帐户和角色组位于不同域中时，标准模式才需要全局编录服务器。 **"Role Groups"（角色组）**：指定与 iDRAC6 关联的角色组的列表。 **"Group Name"（组名称）**：指定标识 Active Directory 中与 iDRAC6 关联的角色组的名称。 **"Group Domain"（组域）**：指定组域。 **"Group Privilege"（组权限）**：指定组权限级别。 只有 iDRAC 配置为使用标准 Active Directory 模式时，才会显示这些设置。

表 4-18. Active Directory 配置和管理页按钮

按钮	定义
"Print"（打印）	打印"Active Directory Configuration and Management"（Active Directory 配置和管理）页上显示的值。
"Refresh"（刷新）	重新载入"Active Directory Configuration and Management"（Active Directory 配置和管理）页。
"Configure Active Directory"（配置 Active Directory）	使您可以配置 Active Directory。有关详细的配置信息，请参阅"将 iDRAC6 用于 Microsoft Active Directory"。
"Test Settings"（检测设置）	允许您使用指定的设置检测 Active Directory 配置。有关使用**"Test Settings"（检测设置）**选项的详情，请参阅"将 iDRAC6 用于 Microsoft Active Directory"。

配置 iDRAC6 服务

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

1. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**。然后，单击**"Services"（服务）**选项卡以显示**"Services"（服务）**配置页。

2. 根据需要配置以下服务：
   - 本地配置 — 请参阅表 4-19
   - Web Server — 请参阅表 4-20 了解 Web Server 设置
   - SSH — 请参阅表 4-21 了解 SSH 设置
   - Telnet — 请参阅表 4-22 了解 Telnet 设置。
   - 远程 RACADM — 请参阅表 4-23 了解远程 RACADM 设置。
   - SNMP Agent — 请参阅表 4-24 了解 SNMP 设置。
   - 自动系统恢复 (ASR) 代理 — 请参阅表 4-25 了解 ASR 代理设置。
3. 单击**"Apply"（应用）**。
4. 单击相应按钮继续。请参阅表 4-26。

表 4-19. 本地配置

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

表 4-20. Web Server 设置

设置	说明
"Enabled"（已启用）	启用或禁用 iDRAC6 Web Server。选中后，复选框表示 Web Server 已启用。默认值为**"enabled"（已启用）**。
"Max Sessions"（最大会话数）	此系统允许的最大同时会话数。此字段不可编辑。可以同时进行的最大会话数是五。
"Active Sessions"（激活的会话数）	系统上的当前会话数，小于等于**"Max Sessions"（最大会话数）**的值。此字段不可编辑。
"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直接影响并终止当前的 Web 界面会话。Web Server 也可进行重设。请等待几分钟，然后再打开新的 Web 界面会话。超时范围为 60 至 10800 秒。默认值为 1800 秒。
"HTTP Port Number"（HTTP 端口号）	iDRAC6 侦听浏览器连接所在的端口。默认为 **80**。
"HTTPS Port Number"（HTTPS 端口号）	iDRAC6 侦听安全浏览器连接所在的端口。默认为 **443**。

表 4-21. SSH 设置

设置	说明
"Enabled"（已启用）	启用或禁用 SSH。选中后，复选框表示 SSH 已启用。
"Timeout"（超时）	Secure Shell 闲置超时，以秒为单位。超时范围为 60 至 1920 秒。输入 0 秒将禁用超时功能。默认为 **300**。
"Port Number"（端口号）	iDRAC6 侦听 SSH 连接所在的端口。默认为 **22**。

表 4-22. Telnet 设置

设置	说明
"Enabled"（已启用）	启用或禁用 Telnet。选中后，就启用 Telnet。
"Timeout"（超时）	Telnet 闲置超时，以秒为单位。超时范围为 60 至 1920 秒。输入 0 秒将禁用超时功能。默认为 **300**。
"Port Number"（端口号）	iDRAC6 侦听 Telnet 连接所在的端口。默认为 **23**。

表 4-23. 远程 RACADM 设置

设置	说明
"Enabled"（已启用）	启用/禁用远程 RACADM。选中后，就启用远程 RACADM。

"Active Sessions"（激活的会话数）	系统上的当前会话数。

表 4-24. SNMP 设置

设置	说明
"Enabled"（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 4-25. 自动系统恢复代理设置

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

表 4-26. 服务页按钮

按钮	说明
"Print"（打印）	打印**"Services"（服务）**页。
"Refresh"（刷新）	刷新**"Services"（服务）**页。
"Apply Changes"（应用更改）	应用**"Services"（服务）**页设置。

更新 iDRAC6 固件/系统服务恢复映像

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

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

1. 打开 iDRAC6 基于 Web 的界面并登录到远程系统。
2. 单击**"Remote Access"（远程访问）**，然后单击**"Update"（更新）**选项卡。
3. 在**"Upload/Rollback (Step 1 of 3)"（上载/回滚 [第 1 步，共 3 步]）**页中，单击**"Browse"（浏览）**，或键入从 **support.dell.com** 下载的固件映像或系统服务恢复映像的路径。

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

   例如：

   `C:\Updates\V1.0\<`*映像名称*`>`。

   或

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

   默认固件映像名称是 **firmimg.d6**。
4. 单击**"Upload"（上载）**。

   该文件将上载到 iDRAC6。完成此过程可能需要几分钟。

   在该过程完成之前，将显示以下信息：

   `"File upload in progress..."`（正在上载文件...）
5. 在**"Status (page 2 of 3)"（状态 [第 2 页，共 3 页]）**页上，您将看到对上载的映像文件进行的验证结果。
   - 如果映像文件成功上载并通过所有验证检查，将显示映像文件名称。如果固件映像已上载，将显示当前固件版本和新固件版本。

     或

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

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

  注： 如果取消选择**"Preserve Configuration"（保留配置）**复选框，iDRAC6 将会重设为默认设置。在默认设置中，LAN 已启用。用户将不能登录到 iDRAC6 Web 界面。您必须在 BIOS 开机自检期间使用 iDRAC6 配置公用程序重新配置 LAN 设置。

7. 单击**"Update"（更新）**开始更新过程。

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

   注： 处于更新模式时，即使退出此页，更新过程也继续在后台进行。

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

   如果系统服务恢复更新成功/失败，将显示相应状态信息。

iDRAC6 固件回滚

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

1. 打开 iDRAC6 基于 Web 的界面并登录到远程系统。

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

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

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

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

3. 单击**"Update"（更新）**开始固件更新过程。

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

   注： 处于更新模式时，即使退出此页，更新过程也继续在后台进行。

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

目录

目录

高级 iDRAC6 配置

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

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

准备工作

应已完成 iDRAC6 硬件和软件的基本安装和设置。有关详情，请参阅"iDRAC6 的基本安装"。

配置 iDRAC6 以通过 SSH/Telnet 远程查看串行输出

您可以通过执行以下步骤，为远程串行控制台重定向配置 iDRAC6：

首先，配置 BIOS 以启用串行控制台重定向：

1. 打开或重新启动系统。
2. 看到下列信息时立即按 <F2>：

   <F2> = System Setup（<F2> = 系统设置）
3. 向下滚动并通过按 <Enter> 选择**"Serial Communication"（串行通信）**。
4. 如下设置**"Serial Communication"（串行通信）**屏幕选项：

   串行通信....带有 COM2 串行重定向打开

   注： 您可以将串行通信设置为**带有 COM1 串行重定向打开**，只要串行端口地址字段中的串行设备 2 也设置为 com1。

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

   外部串行连接器....串行设备 1

   故障保护波特率....115200

   远程终端类型....vt100/vt220

   引导后重定向....已启用

   然后，选择**"Save Changes"（保存更改）**。
5. 按 <Esc> 退出**系统设置**程序，并完成系统设置程序配置。

配置 iDRAC6 设置以启用 SSH/Telnet

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

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

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

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

您也可以远程运行 RACADM 命令，请参阅"远程使用 RACADM"。

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

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Services"（服务）**。
3. 在 **SSH** 或 **Telnet** 部分下选择**"Enabled"（已启用）**。
4. 单击**"Apply Changes"（应用更改）**。

下一步是通过 Telnet 或 SSH 连接到 iDRAC6。

通过 Telnet 或 SSH 启动文本控制台

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

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

```
console com2
```

`console -h com2` 命令显示等待键盘输入或来自串行端口的新字符前串行历史记录缓冲区的内容。

历史记录缓冲区的默认（以及最大）大小为 8192 个字符。可以使用以下命令将此数设置为更小的值：

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

要配置 Linux 在引导期间进行控制台重定向，请参阅"配置 Linux 在引导期间进行串行控制台重定向"。

使用 Telnet 控制台

使用 Microsoft® Windows® XP 或 Windows 2003 运行 Telnet

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

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

使用 Windows 2000 运行 Telnet

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

为 Telnet 控制台重定向启用 Microsoft Telnet

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

注： 在配置客户 VT100 仿真窗口时，将显示重定向控制台的窗口或应用程序设置为 25 行 x 80 列以确保文本正确显示；否则，有些文本屏幕可能会出现乱码。

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

   打开命令提示符，键入以下命令并按 <Enter>：

   ```
   telnet <IP 地址>:<端口号>
   ```

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

为 Telnet 会话配置 Backspace 键

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

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

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

   `telnet`

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

   `set bsasdel`

   系统将显示以下信息：

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

要配置 Linux Telnet 会话使用 <Backspace> 键：

1. 打开命令提示符并键入：

   `stty erase ^h`
2. 在提示符下键入：

   `telnet`

使用 Secure Shell (SSH)

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

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

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

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

在任何时刻，只支持四个 SSH 会话。会话超时由 cfgSsnMgtSshIdleTimeout 属性控制，如"iDRAC6 属性数据库组和对象定义"中所述。

要在 iDRAC6 上启用 SSH，键入：

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

要更改 SSH 端口，键入：

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

有关 cfgSerialSshEnable 和 cfgRacTuneSshPort 属性的详情，请参阅"iDRAC6 属性数据库组和对象定义"。

iDRAC6 SSH 实现支持多种密码模式，如表 5-1 中所示。

表 5-1. 加密模式

模式类型	模式
非对称加密	Diffie-Hellman DSA/DSS 512-1024（随机）位/NIST 规范
对称加密	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128

信息完整性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
验证	• 密码

注： 不支持 SSHv1。

配置 Linux 在引导期间进行串行控制台重定向

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

注： 在配置客户端 VT100 仿真窗口时，将显示重定向控制台的窗口或应用程序设置为 25 行 x 80 列以确保文本正确显示；否则，有些文本屏幕可能会出现乱码。

按照以下说明编辑 **/etc/grub.conf** 文件：

1. 找到文件的常规设置部分并添加以下两行新命令：

   ```
   serial --unit=1 --speed=57600
   terminal --timeout=10 serial
   ```

2. 在内核行上追加两个选项：

   ```
   kernel .............console=ttyS1,115200n8r console=tty1
   ```

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

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

表 5-2. 示例文件：/etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

编辑 **/etc/grub.conf** 文件时，应遵循以下原则：

1. 禁用 GRUB 的图形界面并使用基于文本的界面；否则，GRUB 屏幕将不会显示在 RAC 控制台重定向中。要禁用图形界面，注释掉以 splashimage 开头的行。

2. 要使用多个 GRUB 选项来通过 RAC 串行连接启动控制台会话，将以下行添加到所有选项：

   ```
   console=ttyS1,115200n8r console=tty1
   ```

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

启用引导后登录到控制台

按照以下说明编辑文件 **/etc/inittab**：

添加新行以在 COM2 串行端口上配置 agetty：

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

表 5-3 显示具有新行的示例文件。

表 5-3. 示例文件：/etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel.The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left.Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

按照以下说明编辑文件 **/etc/securetty**：

添加新行，带有 COM2 的串行 tty 名称：

```
ttyS1
```

表 5-4 显示具有新行的示例文件。

表 5-4. 示例文件：/etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
```

```
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

配置串行连接的 iDRAC6

您可以通过下列任何一种界面通过串行连接连接到 iDRAC6：

- iDRAC6 CLI
- 直接连接基本模式
- 直接连接终端模式

要将系统设置为使用任何一种界面，请执行以下步骤。

配置 **BIOS** 以启用串行连接：

1. 打开或重新启动系统。
2. 看到下列信息时立即按 <F2>：

   <F2> = System Setup（<F2> = 系统设置）
3. 向下滚动并通过按 <Enter> 选择**"Serial Communication"（串行通信）**。
4. 如下设置**"Serial Communication"（串行通信）**屏幕：

   外部串行连接器....远程访问设备

   然后，选择**"Save Changes"（保存更改）**。
5. 按 <Esc> 退出**系统设置**程序，并完成系统设置程序配置。

接下来，将 DB-9 或零调制解调器电缆从 Management Station 连接到受管节点服务器。请参阅"为串行控制台连接 DB-9 或零调制解调器电缆"。

接着，确认管理终端仿真软件已配置串行连接。请参阅"配置 Management Station 终端仿真软件"。

最后，配置 iDRAC6 设置以启用串行连接，而这可通过 RACADM 或 iDRAC6 Web 界面实现。

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

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

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

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Serial"（串行）**。
3. 在**"RAC Serial"（RAC 串行）**部分下选择**"Enabled"（已启用）**。
4. 单击**"Apply Changes"（应用更改）**。

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

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

```
racadm getsel
```

在 iDRAC 上配置直接连接基本模式和直接连接终端模式

使用 RACADM，运行下列命令，以禁用 iDRAC6 命令行界面：

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

然后，运行下列 RACADM 命令，以启用直接连接基本模式：

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

或运行下列 RACADM 命令，以启用直接连接终端模式：

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

您可以用 iDRAC6 Web 界面执行相同操作：

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Serial"（串行）**。
3. 在**"RAC Serial"（RAC 串行）**部分下取消选择**"Enabled"（已启用）**。

   直接连接基本模式：

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

   直接连接终端模式：

   在**"IPMI Serial"（IPMI 串行）**部分下，将**"Connection Mode Settings"（连接模式设置）**下拉式菜单更改为**"Direct Connect Terminal Mode"（直接连接终端模式）**。
4. 单击**"Apply Changes"（应用更改）**。有关直接连接基本模式和直接连接终端模式的详情，请参阅"配置串行模式和终端模式"。

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

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

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

1. 通过终端仿真软件连接至 iDRAC6
2. 键入以下命令进行登录：

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

   您将看到以下响应：

   ```
   [SYS]
   [OK]
   ```
3. 键入以下命令，确认已成功登录：

   ```
   [SYS TMODE]
   ```

   您将看到以下响应：

   ```
   [OK TMODE]
   ```
4. 键入以下命令，关闭服务器电源（服务器电源会立即关闭）：

   ```
   [SYS POWER OFF]
   ```
5. 打开服务器电源（服务器电源会立即打开）：

   ```
   [SYS POWER ON]
   ```

在 RAC 串行接口通信模式和串行控制台重定向间切换

iDRAC6 支持转义键序列，从而允许在 RAC 串行接口通信和串行控制台重定向间切换。

要将系统设置为允许此行为，请执行以下步骤：

1. 打开或重新启动系统。

2. 看到下列信息时立即按 <F2>：

   <F2> = System Setup（<F2> = 系统设置）

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

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

   串行通信 -- 开，通过 com2 进行串行重定向

   注： 只要**"serial port address"（串行端口地址）**字段中的**"serial device2"（串行设备 2）**设置为 com1，您就可以将**"serial communication"（串行通信）**字段设置为**"On with serial redirection via com1"（开，通过 com1 进行串行重定向）**。

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

   外部串行连接器 -- 串行设备 2

   故障保护波特率....115200

   远程终端类型...vt100/vt220

   引导后重定向 ... 已启用

   然后，选择**"Save Changes"（保存更改）**。

5. 按 <Esc> 退出**系统设置**程序，并完成系统设置程序配置。

连接 Managed System 外部串行接口和 Management Station 串行端口间的零调制解调器电缆。

在 Management Station 上使用终端仿真程序（hyperterminal 或 teraterm）并根据受管服务器在引导过程的位置，将会看到开机自检屏幕或操作系统屏幕。这基于配置：SAC（对于 Windows）和 Linux 文本模式屏幕（对于 Linux）。设置 Management Station 的终端设置为波特率®C115200, 数据®C8 bit，奇偶校验®Cnone，停止®C1 bit 以及流控制®CNone。

要在串行控制台重定向模式中切换到 RAC 串行接口通信模式，使用以下键序列：

<Esc> +<Shift> <9>

以上键序列会导向到"iDRAC Login"（iDRAC 登录）提示符（如果 RAC 设置为"RAC Serial"（RAC 串行）模式或"Serial Connection"（串行连接）模式，在该模式可以发送终端命令（如果 RAC 设置为"IPMI Serial Direct Connect Terminal Mode"（IPMI 串行直接连接终端模式））。

要将 RAC 串行接口通信模式切换为串行控制台重定向模式，使用以下键序列：

<Esc> +<Shift> <q>

为串行控制台连接 DB-9 或零调制解调器电缆

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

注： DB-9 电缆还可以用于 BIOS 文本控制台重定向。

表 5-5. DB-9 零调制解调器电缆所需的插针输出

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

配置 Management Station 终端仿真软件

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

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

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

为串行控制台仿真配置 Linux Minicom

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

为串行控制台仿真配置 Minicom 版本 2.0

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

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

   如果有 Minicom 配置文件，则键入 `minicom <Minicom config 文件名>` 并跳至步骤 17。
4. 在 Xterm 命令提示符处，键入 `minicom -s`。
5. 选择**"Serial Port Setup"（串行端口设置）**并按 <Enter> 键。
6. 按 <a> 并选择相应的串行设备（例如，**/dev/ttyS0**）。
7. 按 <e> 并将**"Bps/Par/Bits"（速率/奇偶校验位/数据位和停止位）**选项设置为 **57600 8N1**。
8. 按 <f> 并将**"Hardware Flow Control"（硬件流控制）**设置为**"Yes"（是）**，将**"Software Flow Control"（软件流控制）**设置为**"No"（否）**。
9. 要退出**"Serial Port Setup"（串行端口设置）**菜单，按 <Enter>。
10. 选择**"Modem and Dialing"（调制解调器和拨号）**并按 <Enter>。
11. 在**"Modem Dialing and Parameter Setup"（调制解调器拨号和参数设置）**菜单中，按 <Backspace> 清除**"init"（初始化）**、**"reset"（重设）**、**"connect"（连接）**和**"hangup"（挂断）**设置以使它们保留为空白。
12. 要保存每个空白值，按 <Enter>。
13. 清除完所有指定字段后，按 <Enter> 退出**"Modem Dialing and Parameter Setup"（调制解调器拨号和参数设置）**菜单。
14. 选择**"Save setup as config_name"（将设置另存为 config_name）**并按 <Enter>。
15. 选择**"Exit From Minicom"（从 Minicom 退出）**并按 <Enter>。
16. 在命令解释程序提示符处键入 `minicom <Minicom config 文件名>`。
17. 要将 Minicom 窗口展开为 80 x 25，拖动窗角。
18. 按 <Ctrl+a>、<z>、<x> 退出 Minicom。

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

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

串行控制台仿真所需的 Minicom 设置

根据表 5-6 配置任何版本的 Minicom。

表 5-6. 串行控制台仿真所需的 Minicom 设置

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

为串行控制台重定向配置 HyperTerminal

HyperTerminal 是 Microsoft Windows 串行端口访问公用程序。要合适地设置控制台屏幕的大小，使用 Hilgraeve 的 HyperTerminal Private Edition 版本 6.3。

警告： 所有版本的 Microsoft Windows 操作系统都包括有 Hilgraeve 的 HyperTerminal 终端仿真软件。但是，包括的版本没有提供控制台重定向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 6.3 就是支持系统上控制台重定向的一种完全 VT100/VT220 或 ANSI 终端仿真程序。另外，使用命令行窗口执行 Telnet 串行控制台重定向可能会显示乱码。

要为串行控制台重定向配置 HyperTerminal：

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

表 5-7. Management Station COM 端口设置

设置说明	所需设置
每秒位数：	57600
数据位数	8
奇偶校验	无
停止位	1
流控制	硬件

配置串行模式和终端模式

配置 IPMI 和 iDRAC6 串行

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Serial"（串行）**。
3. 配置 IPMI 串行设置。

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

   请参阅表 5-9 了解 iDRAC6 串行设置的说明。
5. 单击**"Apply Changes"（应用更改）**。
6. 单击相应的**"Serial Configuration"（串行配置）**页按钮继续。请参阅表 5-10 了解串行配置页设置的说明。

表 5-8. IPMI 串行设置

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

表 5-9. iDRAC6 串行设置

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

表 5-10. 串行配置页设置

按钮	说明
"Print"（打印）	打印**"Serial Configuration"（串行配置）**页。
"Refresh"（刷新）	刷新**"Serial Configuration"（串行配置）**页。
"Apply Changes"（应用更改）	应用 IPMI 和 iDRAC6 串行更改。
"Terminal Mode Settings"（终端模式设置）	打开**"Terminal Mode Settings"（终端模式设置）**页。

配置终端模式

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Serial"（串行）**。
3. 在**"Serial"（串行）**页中单击**"Terminal Mode Settings"（终端模式设置）**。

4. 配置终端模式设置。

   请参阅表 5-11 了解终端模式设置的说明。

5. 单击**"Apply Changes"（应用更改）**。

6. 单击相应的**"Terminal Mode Settings"（终端模式设置）**页按钮继续。请参阅表 5-12 了解终端模式设置页按钮的说明。

表 5-11. 终端模式设置

设置	说明
"Line Editing"（行编辑）	启用或禁用行编辑。
"Delete Control"（删除控制）	选择以下选项之一： • **"iDRAC outputs a <bksp><sp><bksp> character when <bksp> or <del> is received"（iDRAC 在收到 <bksp> 或 <del> 时输出 <bksp><sp><bksp> 字符）**— • **"iDRAC outputs a <del> character when <bksp> or <del> is received"（iDRAC 在收到 <bksp> 或 <del> 时输出 <del> 字符）**—
"Echo Control"（回声控制）	启用或禁用回声。
"Handshaking Control"（符号交换控制）	启用或禁用符号交换。
"New Line Sequence"（新行序列）	选择**"None"（无）**、**<CR-LF>**、**<NULL>**、**<CR>**、**<LF-CR>** 或 **<LF>**。
"Input New Line Sequence"（输入新行序列）	选择 **<CR>** 或 **<NULL>**。

表 5-12. 终端模式设置页按钮

按钮	说明
"Print"（打印）	打印**"Terminal Mode Settings"（终端模式设置）**页。
"Refresh"（刷新）	刷新**"Terminal Mode Settings"（终端模式设置）**页。
"Return to Serial Port Configuration"（返回串行端口配置）	返回**"Serial Port Configuration"（串行端口配置）**页。
"Apply Changes"（应用更改）	应用终端模式设置更改。

配置 iDRAC6 网络设置

警告： 更改 iDRAC6 网络设置可能会断开当前网络连接。

使用以下一个工具配置 iDRAC6 网络设置：

- 基于 Web 的接口 — 请参阅"配置 iDRAC6 NIC"
- RACADM CLI — 请参阅"cfgLanNetworking"
- iDRAC6 配置公用程序 — 请参阅"配置系统使用 iDRAC6"

注： 如果要在 Linux 环境中部署 iDRAC6，请参阅"安装 RACADM"。

通过网络访问 iDRAC6

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

- 基于 Web 的界面
- RACADM
- Telnet 控制台
- SSH
- IPMI

表 5-13 描述各种 iDRAC6 界面。

表 5-13. iDRAC6 界面

接口	说明
基于 Web 的界面	允许使用图形用户界面远程访问 iDRAC6。基于 Web 的界面构建在 iDRAC6 固件中并从 Management Station 中支持的 Web 浏览器通过 NIC 接口访问。 有关支持的 Web 浏览器列表，请参阅"支持的 Web 浏览器"。
RACADM	允许通过命令行界面远程访问 iDRAC6。RACADM 使用 iDRAC6 IP 地址执行 RACADM 命令。 **注：** racadm 远程功能选项只在 Management Station 上受支持。有关详情，请参阅"远程使用 RACADM"。 **注：** 使用 racadm 远程功能时，须在使用有关文件操作的 RACADM 子命令的文件夹上具有写权限，例如： `racadm getconfig -f <文件名>` 或： `racadm sslcertupload -t 1 -f c:\cert\cert.txt` 子命令
Telnet 控制台	提供对 iDRAC6 的访问并支持串行和 RACADM 命令，包括 **powerdown**、**powerup**、**powercycle** 和 **hardreset** 命令。 **注：** Telnet 是一种以明文传送所有数据（包括密码）的非安全协议。发送敏感信息时，应使用 SSH 接口。
SSH 接口	使用更高安全保护的加密传输层，提供与 Telnet 控制台相同的功能。
IPMI 接口	允许通过 iDRAC6 使用远程系统的基本管理功能。接口包括 LAN 上 IPMI、串行 IPMI 以及 LAN 上串行。有关详情，请参阅 **support.dell.com\manuals** 上的《*Dell OpenManage 底板管理控制器公用程序用户指南*》。

注： iDRAC6 默认用户名是 root，默认密码是 calvin。

可以通过使用支持的 Web 浏览器或通过 Server Administrator 或 IT Assistant，通过 iDRAC6 NIC 访问 iDRAC6 基于Web 的界面。

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

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

有关详情，请参阅《*Server Administrator 用户指南*》。

远程使用 RACADM

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

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

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

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

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

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

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

Racadm 不继续执行命令。

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

注： RACADM 远程功能只在 Management Station 上受支持。有关详情，请参阅 Dell 支持网站 **support.dell.com\manuals** 上 **Dell OpenManage 软件**下的《*Dell 系统软件支持值表*》。

注： 使用 RACADM 远程功能时，须在使用有关文件操作的 RACADM 子命令的文件夹上具有写权限，例如：

```
racadm getconfig -f <文件名>
```

或

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt 子命令
```

RACADM 提要

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

```
racadm -i -r <iDRAC6 IP 地址> <子命令> <子命令选项>
```

例如：

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

```
racadm -i -r 192.168.0.120 getsysinfo
```

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

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

```
racadm -i -r <iDRAC6 IP 地址>:<端口> <子命令> <子命令选项>
```

RACADM 选项

表 5-14 列出 RACADM 命令的选项。

表 5-14. 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的密码。如果使用 **-p** 选项，则不允许使用 **-i** 选项。
-S	指定 RACADM 应检查是否有无效证书错误。如果检测到无效证书，RACADM 会停止执行命令并显示错误信息。

启用和禁用 RACADM 远程功能

注： 建议在本地系统上运行这些命令。

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

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

要禁用远程功能，请键入：

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

RACADM 子命令

表 5-15 提供可在 RACADM 中运行的每个 RACADM 子命令的说明。有关 RACADM 子命令（包括语法和有效条目）的详细列表，请参阅"RACADM 子命令概览"。

输入 RACADM 子命令时，请在命令前加上 RACADM，例如：

```
racadm help
```

表 5-15. RACADM 子命令

命令	说明
help	列出 iDRAC6 子命令。

help <*子命令*>	列出指定子命令的用法语句。
arp	显示 ARP 表的内容。ARP 表条目不能被添加或删除。
clearasrscreen	清除上一个 ASR（崩溃）屏幕（上一个蓝屏）。
clrraclog	清除 iDRAC6 日志。单个条目被用来指示清除日志的用户和时间。
config	配置 iDRAC6。
getconfig	显示当前 iDRAC6 配置属性。
coredump	显示最新 iDRAC6 信息转储。
coredumpdelete	删除 iDRAC6 中存储的信息转储。
fwupdate	执行或显示 iDRAC6 固件更新的状态。
getssninfo	显示关于活动会话的信息。
getsysinfo	显示一般 iDRAC6 和系统信息。
getractime	显示 iDRAC6 时间。
ifconfig	显示当前 iDRAC6 的 IP 配置。
netstat	显示路径选择表和当前连接。
ping	验证目标 IP 地址是否可以使用当前路径选择表内容从 iDRAC6 进行访问。
setniccfg	设置控制器的 IP 配置。
getniccfg	显示控制器的当前 IP 配置。
getsvctag	显示服务标签。
racdump	转储 iDRAC6 状况和状态信息以进行调试。
racreset	重设 iDRAC6。
racresetcfg	将 iDRAC6 重设为默认配置。
serveraction	在 Managed System 上执行电源管理操作。
getraclog	显示 iDRAC6 日志。
clrsel	清除系统事件日志条目。
gettracelog	显示 iDRAC6 跟踪日志。如果与 -i 一起使用，则命令显示 iDRAC6 跟踪日志中的条目数。
sslcsrgen	生成并下载 SSL CSR。
sslcertupload	将 CA 证书或服务器证书上载至 iDRAC6。
sslcertdownload	下载 CA 证书。
sslcertview	查看 iDRAC6 中的 CA 证书或服务器证书。
sslkeyupload	强制 DRAC6 通过 DRAC6 NIC 发送检测电子邮件来检查电子邮件配置。
testtrap	强制 DRAC6 通过 DRAC6 NIC 发送检测 SNMP 陷阱来检查陷阱配置。
vmdisconnect	强制关闭虚拟介质连接。
vmkey	将虚拟闪速更新大小重设为默认大小 (256 MB)。

有关 RACADM 错误消息的常见问题

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

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

这条信息是什么意思？

必须等到 iDRAC6 完成重设后，才能发出另一个命令。

使用 racadm 命令和子命令时，我得到了并不理解的错误。

使用 RACADM 命令和子命令时，可能会遇到以下一个或多个错误：

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

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

清除系统上的 ARP 表。

配置多个 iDRAC6 控制器

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

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

要配置多个 iDRAC6 控制器，请执行以下步骤：

1. 使用 RACADM 查询包含相应配置的目标 iDRAC6。

   注： 生成的 **.cfg** 文件不包含用户密码。

   打开命令提示符并键入：

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

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

2. 使用简单文本编辑器（可选）修改配置文件。

3. 使用新配置文件修改目标 iDRAC6。

   在命令提示符处键入：

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

4. 重设已配置的目标 iDRAC6。

   在命令提示符处键入：

   ```
   racadm racreset
   ```

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

可以使用 **getconfig** 命令来执行以下操作：

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

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

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

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

警告： 建议使用简单文本编辑器编辑此文件。RACADM 公用程序使用 ASCII 文本分析器。任何格式都会使分析器混淆，都有可能损坏 RACADM 数据库。

创建 iDRAC6 配置文件

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

可通过以下方式建立 **.cfg** 文件：

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

注： 请参阅"getconfig"了解关于 **getconfig** 命令的信息。

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

创建 **.cfg** 文件时请使用以下原则：

- 如果分析器遇到索引组，区分各个索引的将是锚定对象的值。

  分析器将从 iDRAC6 读入该组的所有索引。配置 iDRAC6 时，该组内的任何对象均为都是简单修改。如果修改的对象代表新的索引，则将在配置过程中在 iDRAC6 上创建该索引。

- 不能在 **.cfg** 文件中指定选择的索引。

  由于可以创建和删除索引，因此，在一段时间后，组可能会变得支离破碎，并且带有已使用和未使用的索引。如果索引存在，则修改该索引。如果索引不存在，则使用第一个可用的索引。此方法在添加索引条目时更加灵活，因为用户不需要在所有管理的 CMC 之间进行精确索引匹配。新用户将被添加至第一个可用的索引。如果所有索引均已满并且必须添加新的用

户，则在一个 iDRAC6 上可以正确分析和运行的 **.cfg** 文件可能无法在其它 iDRAC6 上正确运行。

- 可以使用 **racresetcfg** 子命令为多个 iDRAC6 配置相同的属性。

  使用 **racresetcfg** 子命令将 iDRAC6 重设为初始默认值，然后运行 `racadm config -f <文件名>.cfg` 命令。确保 **.cfg** 文件中包含所有所需的对象、用户、索引和其它参数。

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

分析规则

- 所有以 '#' 开头的行将被视为注释。

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

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

  示例：

  ```
  #

  # 这是一条注释。

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<调制解调器初始化字符串中的 # 不是注释>
  ```

- 所有组条目必须括在 "**[**" 和 "**]**" 字符中。

  表示组名称的开头 "**[**" 字符*必须*在第一列中开始。此组名称*必须*在该组中的任何对象之前指定。没有关联组名的对象将导致错误。配置数据按"iDRAC6 属性数据库组和对象定义"中的定义分组。

  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=143.154.133.121 {对象名称}
  ```

- 所有参数都指定为"对象=值"对，在对象、= 或值之间不留空格。

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

  请参见上一列表项中的示例。

- **.cfg** 分析器忽略索引对象条目。

  用户*无法*指定使用哪个索引。如果索引已存在，则使用该索引，否则将在该组的第一个可用索引中创建新条目。

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

注： 可以使用以下命令手动创建索引组：
`racadm config -g <组名称> -o <锚定对象> -i <索引 1-16> <唯一定位标记名称>`

- *无法*从 **.cfg** 文件中删除索引组的行。

  用户必须使用以下命令手动删除索引对象：

  ```
  racadm config -g <组名称> -o <对象名称> -i <索引 1-16> ""
  ```

注： 空字符串（两个 "" 字符表示）指示 iDRAC6 删除指定组的索引。

要查看索引组的内容，请使用以下命令：

```
racadm getconfig -g <组名称> -i <索引 1-16>
```

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

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<用户名>
  ```

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

修改 iDRAC6 IP 地址

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

例如：

```
#

# 对象组 "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

此文件将更新为如下内容：

```
#

# 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
```

命令 **racadm config -f myfile.cfg** 分析文件并用行号标识任何错误。正确的文件将更新适当的条目。此外，可以使用上面示例中的 **getconfig** 命令确认更新。

使用此文件下载企业范围内的更改或通过网络配置新系统。

注： "定位标记"是内部术语，不应在文件中使用。

配置 iDRAC6 网络属性

要生成可用网络属性的列表，请键入以下命令：

```
racadm getconfig -g cfgLanNetworking
```

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

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

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

以下示例介绍如何使用命令配置所需的 LAN 网络属性。

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

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

iDRAC6 模式

iDRAC6 可配置为四种模式：

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

表 5-16 提供了各种模式的说明。

表 5-16. iDRAC6 NIC 配置

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

常见问题 关于网络安全

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

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

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

要确保 CSR 与注册 DNS iDRAC6 名称匹配：

1. 在**系统**树中，单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击**"Network"（网络）**。
3. 在**"Common Settings"（常见设置）**表中：
   a. 选择**"Register iDRAC on DNS"（在 DNS 上注册 iDRAC）**复选框。
   b. 在**"DNS iDRAC Name"（DNS iDRAC 名称）**字段中，输入 iDRAC6 名称。
4. 单击**"Apply Changes"（应用更改）**。

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

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

重设 iDRAC6 Web 服务器后，可能需要等待几分钟，远程 RACADM 服务和基于 Web 的界面才会可用。

iDRAC6 Web 服务器会在发生以下情况后重设：

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

为什么我的 DNS 服务器没有注册 iDRAC6？

有些 DNS 服务器只注册 31 个或更少字符的名称。

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

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

目录

目录

添加和配置 iDRAC6 用户

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

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*。要增强安全性，还可以配置警报以便在发生特定系统事件时通过电子邮件通知特定用户。

使用 Web 界面配置 iDRAC6 用户

添加和配置 iDRAC6 用户

要用 iDRAC6 管理系统并维护系统安全性，请创建多个具有特定管理权限（或*基于角色的授权*）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 Users"（配置用户）**权限才能配置 iDRAC 用户。

1. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**→**"Users"（用户）**。

   用户页面显示以下 iDRAC 用户信息：**用户 ID、状态（启用 /禁用）、用户名、RAC 权限、IPMI LAN 权限、IPMI 串行权限**和 **LAN 上串行状态（启用 /禁用）**。 表 6-1 说明配置 iDRAC 用户所需的用户状态和权限。

   注： 用户 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。

   在**"User Main Menu"（用户主菜单）**页上，您可以配置用户、查看用户证书、上载可信认证机构 (CA) 证书或查看可信 CA 证书。

   如果选择**"Configure User"（配置用户）**并单击**"Next"（下一步）**， **"User Configuration"（用户配置）**页将会显示。继续到步骤 4。

   如果在**"Smart Card Configuration"（Smart Card 配置）**选择某个选项，请参阅表 6-2。

3. 在**"User Configuration"（用户配置）**页上，配置以下内容：
   - 用户名、密码，以及新 iDRAC 用户或现有 iDRAC 用户的访问权限。 表 6-3 说明**"General User Settings"（常规用户设置）**。
   - 用户的 IPMI 权限。 表 6-4 说明配置用户 LAN 权限的**"IPMI User Privileges"（IPMI 用户权限）**。
   - iDRAC 用户权限。 表 6-5 说明 **iDRAC 用户权限**。
   - "iDRAC Group"（iDRAC 组）访问权限。 表 6-6 说明**"iDRAC Group Permissions"（iDRAC 组权限）**。

4. 完成后，单击**"Apply Changes"（应用更改）**。

5. 单击相应按钮继续。请参阅表 6-7。

表 6-1. 用户状态和权限

设置	说明
"User ID"（用户 ID）	显示用户 ID 号顺序列表。**"User ID"（用户 ID）**下的每个字段都包含 16 个预设用户 ID 号中的一个。此字段不能编辑。
"State"（状态）	显示用户的登录状态："Enabled"（已启用）或"Disabled"（已禁用）。（默认为已禁用。） **注：** 默认启用用户 2。
"User Name"（用户名）	显示用户的登录名称。指定一个 iDRAC6 用户名，最多 16 个字符。每个用户必须具有唯一用户名。 **注：** iDRAC6 上的用户名不能包含 **/**（正斜杠）和 **.**（句点）字符。

	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。
"RAC Privilege"（RAC 权限）	显示用户所分配的组（权限级别），包括"Administrator"（管理员）、"Operator"（操作员）、"Read Only"（只读）或"None"（无）。
"IPMI LAN Privilege"（IPMI LAN 权限）	显示用户所分配的 IPMI LAN 权限级别，包括"Administrator"（管理员）、"Operator"（操作员）、"Read Only"（只读）或"None"（无）。
"IPMI Serial Privilege"（IPMI 串行权限）	显示用户所分配的 IPMI 串行端口权限级别，包括"Administrator"（管理员）、"Operator"（操作员）、"Read Only"（只读）或"None"（无）。
"Serial Over LAN"（LAN 上串行）	允许/不允许用户使用 LAN 上 IPMI 串行。

表 6-2. Smart Card 配置选项

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

表 6-3. 常规用户设置

"User ID"（用户 ID）	16 个预设用户 ID 编号之一。
"Enable User"（启用用户）	选中后，表示用户的 iDRAC6 访问权限已启用。取消选中后，用户的访问权限会被禁用。
"User Name"（用户名）	用户名称，最多 16 个字符。
"Change Password"（更改密码）	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**密码**。
"New Password"（新密码）	输入多达 20 个字符的**"Password"（密码）**。密码字符不会显示出来。
"Confirm New Password"（确认新密码）	重新键入 iDRAC 用户的密码以进行确认。

表 6-4. IPMI 用户权限

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

表 6-5. iDRAC 用户权限

属性	**说明**
"Roles"（角色）	指定用户的最大 iDRAC 用户权限为以下权限之一：**"Administrator"（管理员）**、**"Operator"（操作员）**、**"Read Only"（只读）**或**"None"（无）**。请参阅表 6-6 了解 **DRAC 组权限**。
"Login to iDRAC"（登录到 iDRAC）	允许用户登录到 iDRAC。
"Configure iDRAC"（配置 iDRAC）	允许用户配置 iDRAC。
"Configure Users"（配置用户）	使用户可以允许特定用户访问系统。
"Clear Logs"（清除日志）	允许用户清除 iDRAC 日志。
"Execute Server Control Commands"（执行服务器控制命令）	使用户能够执行服务器控制命令。
"Access Console Redirection"（访问控制台重定向）	允许用户运行控制台重定向。
"Access Virtual Media"（访问虚拟介质）	允许用户运行和使用虚拟介质。
"Test Alerts"（检测警报）	允许用户将检测警报（电子邮件或 PET）发送到特定用户。
"Execute Diagnostic Commands"（执行诊断命令）	允许用户运行诊断命令。

表 6-6. iDRAC 组权限

用户组	**授予的权限**

"Administrator"（管理员）	**"Login to iDRAC"（登录到 iDRAC）、"Configure iDRAC"（配置 iDRAC）、"Configure Users"（配置用户）、"Clear Logs"（清除日志）、"Execute Server Control Commands"（执行服务器控制命令）、"Access Console Redirection"（访问控制台重定向）、"Access Virtual Media"（访问虚拟介质）、"Test Alerts"（检测警报）、"Execute Diagnostic Commands"（执行诊断命令）**
"Operator"（操作员）	选择以下权限的任意组合：**"Login to iDRAC"（登录到 iDRAC）、"Configure iDRAC"（配置 iDRAC）、"Configure Users"（配置用户）、"Clear Logs"（清除日志）、"Execute Server Action Commands"（执行服务器操作命令）、"Access Console Redirection"（访问控制台重定向）、"Access Virtual Media"（访问虚拟介质）、"Test Alerts"（检测警报）、"Execute Diagnostic Commands"（执行诊断命令）**
"Read Only"（只读）	**登录到 iDRAC**
"None"（无）	没有分配权限

表 6-7. 用户配置页按钮

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）**页。
"Go Back To Users Page"（退回到用户页）	返回**"Users Page"（用户页）**。
"Apply Changes"（应用更改）	保存对用户配置所做的任何新设置。

使用 RACADM 公用程序配置 iDRAC6 用户

注： 必须以用户 **root** 登录才能在远程 Linux 系统上执行 RACADM 命令。

可以使用 iDRAC6 代理安装在 Managed System 上的 RACADM 命令行来配置单一或多个 iDRAC6 用户。

要配置多个具有相同配置设置的 iDRAC6，请执行以下程序之一：

- 参考本节中的 RACADM 示例，创建 RACADM 命令的批处理文件，然后在各个 Managed System 上执行该批处理文件。
- 按"RACADM 子命令概览"中所述创建 iDRAC6 配置文件并使用同一配置文件在各个 Managed System 上执行 **racadm config** 子命令。

准备工作

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

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

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

要验证用户是否存在，请在命令提示符处键入以下命令：

```
racadm getconfig -u <用户名>
```

或

键入以下命令，每次仅查找索引 1 至 16 中的一个：

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

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

系统将显示有些参数和对象 ID 以及它们的当前值。受关注的两个对象为：

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

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

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

添加 iDRAC6 用户

要将新用户添加到 RAC 配置，可以使用一些基本命令。通常，执行以下过程：

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

示例

下面的示例说明如何添加新用户 "John" 密码 "123456"，对 RAC 具有登录权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

要验证，请使用以下命令之一：

```
racadm getconfig -u john

racadm getconfig ◎Cg cfgUserAdmin ◎Ci 2
```

删除 iDRAC6 用户

使用 RACADM 时，必须手动逐个禁用用户。不能使用配置文件删除用户。

下面的示例说明可用于删除 RAC 用户的命令语法：

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

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

启用 iDRAC6 用户权限

要启用带有特定管理权限（基于角色授权）的用户，首先按照"准备工作"中的步骤找到可用用户索引。接着，键入以下带有新用户名和密码的命令行。

注： 请参阅表 B-2 查看特定用户权限的有效位掩码值列表。默认权限值为 0，表示用户没有启用任何权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <索引> <用户权限位掩码值>
```

目录

目录

将 iDRAC6 用于 Microsoft Active Directory

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

目录服务维护一个公用数据库，在其中存储在网络上控制用户、计算机、打印机等所需的所有信息。如果公司已使用 Microsoft® Active Directory® 服务软件，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 Active Directory 软件中的现有用户并对这些权限进行控制。

注： 使用 Active Directory 识别 DRAC6 用户在 Microsoft Windows® 2000、Windows Server® 2003 和 Windows Server 2008 操作系统上受支持。

表 7-1 显示九个 iDRAC6 Active Directory 用户权限。

表 7-1. iDRAC6 用户权限

权限	说明
"Login to iDRAC"（登录到 iDRAC）	允许用户登录到 iDRAC6
"Configure iDRAC"（配置 iDRAC）	允许用户配置 iDRAC6
"Configure Users"（配置用户）	使用户可以允许特定用户访问系统
"Clear Logs"（清除日志）	允许用户清除 iDRAC6 日志
"Execute Server Control Commands"（执行服务器控制命令）	允许用户执行 RACADM 命令
"Access Console Redirection"（访问控制台重定向）	允许用户运行控制台重定向
"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（电子邮件和 PET）发送给特定用户
"Execute Diagnostic Commands"（执行诊断命令）	允许用户运行诊断命令

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"。

支持的 Active Directory 验证机制

可以通过两种方法使用 Active Directory 定义对 iDRAC6 的用户访问：一种方法是使用*扩展模式*解决方案，该解决方案经过 Dell 自定义后加入 Dell 定义的 Active Directory 对象。另一种方法是使用*标准模式*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 的访问权限时，必须选择扩展模式解决方案或标准模式解决方案。

使用扩展模式解决方案的优势有：

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

使用标准模式解决方案的优势是无需模式扩展，因为 Microsoft 的默认 Active Directory 模式配置已经提供所有必需的对象类。

扩展模式 Active Directory 概览

使用扩展模式解决方案要求 Active Directory 模式扩展，如以下一节所述。

扩展 Active Directory 模式

重要信息：此产品的模式扩展与前几代 Dell 远程管理产品不同。您必须扩展新模式并将新 Active Directory 用户和计算机 Microsoft 管理控制台 (MMC) 管理单元安装到目录中。旧模式不能用于此产品。

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

在 *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。有关详情，请参阅"扩展 Active Directory 模式"和"安装 Dell 对 Active Directory 用户和计算机管理单元的扩展"。有关为 iDRAC6 扩展模式和安装 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** 上的*《Dell OpenManage 安装和安全性用户指南》*。

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

Active Directory 模式扩展

Active Directory 数据是属性和类的分布式数据库。Active Directory 模式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 扩展了该模式，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 模式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，从而在各公司向模式中添加扩展时，能够确保唯一性并且相互间不会冲突。为了扩展 Microsoft Active Directory 中的模式，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

iDRAC 模式扩展概览

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 扩展了该模式以包括关联、设备和权限属性。关联属性用于将具有一组特定权限的用户或组与一个或多个 iDRAC 设备链接起来。这种模式给管理员提供了极大的灵活性，可以对网络上的用户、iDRAC 权限和 iDRAC 设备进行各种组合而无需增加太多的复杂性。

Active Directory 对象概览

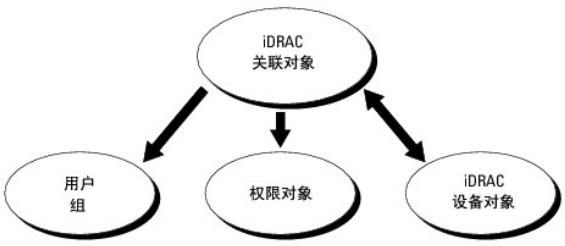
对于网络上每一个要与 Active Directory 集成以进行验证和授权的物理 iDRAC 来说，请创建至少一个关联对象和一个 iDRAC 设备对象。可以创建多个关联对象，每个关联对象都可以链接到任意多个用户、用户组或 iDRAC 设备对象。用户和 iDRAC 用户组可以是企业中任何域的成员。

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

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

图 7-1 说明关联对象提供了进行所有验证和授权所需的连接。

图 7-1. Active Directory 对象的典型设置



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

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

Active Directory 用户和计算机 MMC 管理单元的 Dell 扩展仅允许将来自相同域的权限对象和 iDRAC6 对象与关联对象关联。Dell 扩展不允许将其它域中的组或 iDRAC 对象添加为关联对象的产品成员。

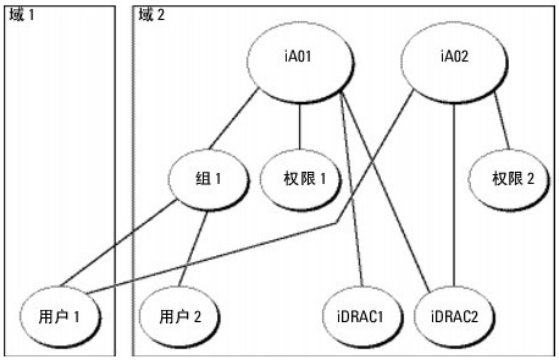
来自任何域的用户、用户组或嵌套的用户组可添加到关联对象中。扩展模式解决方案支持任何用户组类型和 Microsoft Active Directory 允许的多个域之间嵌入的任何用户组。

使用扩展模式累积权限

扩展模式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，扩展模式验证可以累积权限，使用户能够拥有与同一用户关联的不同权限对象对应的所有已分配权限的超级集合。

图 7-2 提供了使用扩展模式累积权限的示例。

图 7-2. 用户权限累积



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

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

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

配置扩展模式 Active Directory 以访问 iDRAC

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

1. 扩展 Active Directory 模式（请参阅"扩展 Active Directory 模式"）。
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 iDRAC 用户和权限添加到 Active Directory"）。
4. 在各个域控制器上启用 SSL（请参阅"在域控制器上启用 SSL"）。
5. 使用 iDRAC6 基于 Web 的界面或 RACADM 配置 iDRAC6 Active Directory 属性（请参阅"使用 iDRAC6 基于 Web 的界面以扩展模式配置 Active Directory"或"使用 RACADM 以扩展模式配置 Active Directory"）。

扩展 Active Directory 模式将会在 Active Directory 模式中添加一个 Dell 组织单元、模式类和属性以及示例权限和关联对象。扩展模式前，必须在域目录林的"模式主机灵活单主机操作 (FSMO) 角色所有者"上具有"Schema Admin"（模式管理员）权限。

可以使用以下方法之一扩展模式：

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

如果使用 LDIF 脚本，将不会把 Dell 组织单元添加到模式。

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 模式，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

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

1. 在**"Welcome"（欢迎）**屏幕中单击**"Next"（下一步）**。
2. 阅读并了解警告，单击**"Next"（下一步）**。
3. 选择**"Use Current Log In Credentials"（使用当前登录凭据）**或输入具有模式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）**。

   模式将会扩展。要验证模式扩展情况，请使用 MMC 和 Active Directory 模式管理单元验证以下项是否存在：

   - 类（请参阅表 7-2 到表 7-7）
   - 属性（表 7-8）

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

表 7-2. 添加到 Active Directory 模式的类的类定义

类名称	分配的对象标识号 (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 7-3. dellRacDevice 类

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

表 7-4. 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 7-5. dellRAC4Privileges 类

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
说明	用于为 iDRAC 设备定义权限（授权权限）。
类的类型	辅助类
超类	无
属性	**dellIsLoginUser**

	dellIsCardConfigAdmin **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

表 7-6. 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 7-7. 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 7-8. 添加到 Active Directory 模式的属性的列表

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控制台重定向权限，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 当前模式版本用于更新模式。	1.2.840.113556.1.8000.1280.1.1.2.12 不区分大小写的字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType 此属性是 delliDRACDevice 对象的当前 RAC 类型以及到 dellAssociationObjectMembers 前进链接的后退链接。	1.2.840.113556.1.8000.1280.1.1.2.13 不区分大小写的字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers 属于此产品的 dellAssociationObjectMembers 的列表。此属性是到 dellProductMembers 链接属性的后退链接。 链接 ID：12071	1.2.840.113556.1.8000.1280.1.1.2.14 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

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

使用 *Dell Systems Management Tools and Documentation* DVD 安装系统管理软件时，可以通过在安装过程中选择**"Active Directory Users and Computers Snap-in"（Active Directory 用户和计算机管理单元）**选项来安装管理单元。请参阅《*Dell OpenManage 软件快速安装指南*》进一步了解如何安装系统管理软件。对于 x64 位 Windows 操作系统，管理单元安装程序位于 **<DVD 驱动器>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**

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

安装 Administrator Pack

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

有关详情，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，请单击**"Start"（开始）→"Run"（运行）**，键入 `MMC` 并按 **Enter**。

   将显示 MMC。

2. 在**"Console 1"（控制台 1）**窗口中，单击**"File"（文件）**（如果是运行 Windows 2000 的系统，则单击**"Console"（控制台）**）。

3. 单击**"Add/Remove Snap-in"（添加/删除管理单元）**。

4. 选择**"Active Directory Users and Computers Snap-in"（Active Directory 用户和计算机管理单元）**并单击**"Add"（添加）**。

5. 单击**"Close"（关闭）**并单击**"OK"（确定）**。

将 iDRAC 用户和权限添加到 Active Directory

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

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

创建 iDRAC 设备对象

1. 在 MMC 的**"Console Root"**（控制台根目录）窗口中，右键单击一个容器。
2. 选择**"New"（新建）→"Dell Remote Management Object Advanced"（Dell 远程管理高级对象）**。

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

创建权限对象

注： 权限对象必须和相关关联对象创建在同一个域中。

1. 在**"Console Root"（控制台根节点）**(MMC) 窗口中，右键单击一个容器。
2. 选择**"New"（新建）→"Dell Remote Management Object Advanced"（Dell 远程管理高级对象）**。

   将显示**"New Object"（新建对象）**窗口。
3. 为新对象键入名称。
4. 选择**"Privilege Object"（权限对象）**。
5. 单击**"OK"（确定）**。
6. 右键单击创建的权限对象并选择**"Properties"（属性）**。
7. 单击**"Remote Management Privileges"（远程管理权限）**选项卡并选择要让用户具有的权限。

创建关联对象

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

1. 在**"Console Root"（控制台根节点）**(MMC) 窗口中，右键单击一个容器。
2. 选择**"New"（新建）→"Dell Remote Management Object Advanced"（Dell 远程管理高级对象）**。

   这将打开**"New Object"（新建对象）**窗口。
3. 为新对象键入名称。
4. 选择**"Association Object"（关联对象）**。
5. 选择**"Association Object"（关联对象）**的范围。
6. 单击**"OK"（确定）**。

配置关联对象

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

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

添加用户或用户组

1. 右键单击**"Association Object"（关联对象）**并选择**"Properties"（属性）**。
2. 选择**"Users"（用户）**选项卡并单击**"Add"（添加）**。
3. 键入用户或用户组名称并单击**"OK"（确定）**。

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

添加权限

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

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

添加 iDRAC 设备

要添加 iDRAC 设备：

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

使用 iDRAC6 基于 Web 的界面以扩展模式配置 Active Directory

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 基于 Web 的界面。
3. 展开**系统**树并单击**"Remote Access"（远程访问）**。
4. 单击**"Configuration"（配置）**选项卡并选择 **Active Directory**。
5. 滚动到**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页底部，然后单击**"Configure Active Directory"（配置 Active Directory）**。

   此时会出现**"Step 1 of 4 Active Directory Configuration and Management"（第 1 步，共 4 步 Active Directory 配置和管理）**页。
6. 在**"Certificate Settings"（证书设置）**下面，如果要验证 Active Directory 服务器的 SSL 证书，则选中**"Enable Certificate Validation"（启用证书认证）**；否则，转至步骤 9。
7. 在**"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）**下面，键入证书文件路径或浏览找到证书文件。

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

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

10. 单击**"Next"（下一步）**以转至**"Step 2 of 4 Active Directory Configuration and Management"（第 2 步，共 4 步 Active Directory 配置和管理）**。

11. 单击**"Enable Active Directory"（启用 Active Directory）**。

警告： 在此版本中，如果 Active Directory 配置为扩展模式，将不支持基于 Smart Card 的双重验证 (TFA) 和单一登录 (SSO) 功能。

12. 单击**"Add"（添加）**以输入用户域名。

13. 在提示符处输入用户域名并单击**"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。您可从列表中选择，然后只需键入用户名。

14. 键入**超时**时间（以秒为单位），指定 iDRAC6 等待 Active Directory 响应的时间。默认值为 120 秒钟。

15. 键入"Domain Controller Server Address"（域控制器服务器地址）。您可为登录处理最多输入三个 Active Directory 服务器，但必须通过输入 IP 地址或完全限定域名 (FQDN) 配置至少一个服务器。iDRAC6 会尝试连接到每个配置的服务器，直到建立连接为止。

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

16. 单击**"Next"（下一步）**以转至**"Step 3 of 4 Active Directory Configuration and Management"（第 3 步，共 4 步 Active Directory 配置和管理）**。

17. 在**"Schema Selection"（模式选择）**下，单击**"Extended Schema"（扩展模式）**。

18. 单击**"Next"（下一步）**以转至**"Step 4 of 4 Active Directory Configuration and Management"（第 4 步，共 4 步 Active Directory 配置和管理）**。

19. 在**"Extended Schema Settings"（扩展模式设置）**下，键入 iDRAC 名称和域名以配置 iDRAC 设备对象。iDRAC 域名是创建 iDRAC 对象所在的域的名称。

20. 单击**"Finish"（完成）**以保存 Active Directory 扩展模式设置。

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

21. 单击**"Test Settings"（检测设置）**以检查 Active Directory 扩展模式设置。

22. 键入 Active Directory 用户名和密码。

将显示检测结果和检测日志。有关详情，请参阅"检测配置"。

注： 您必须拥有在 iDRAC 上正确配置的 DNS 服务器才能支持 Active Directory 登录。单击**"Remote Access"（远程访问）→"Configuration"（配置）→"Network"（网络）**页以手动配置 DNS 服务器或使用 DHCP 获得 DNS 服务器。

现在完成了以扩展模式配置 Active Directory 的过程。

使用 RACADM 以扩展模式配置 Active Directory

使用以下命令，通过 RACADM CLI 工具而不是 Web 界面以扩展模式配置 iDRAC Active Directory 功能。

1. 打开命令提示符并键入以下 RACADM 命令：

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

racadm config -g cfgActiveDirectory -o cfgADType 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 cfgDomainController1 <域控制器的完全限定域名或 IP 地址>

racadm config -g cfgActiveDirectory -o cfgDomainController2 <域控制器的完全限定域名或 IP 地址>

racadm config -g cfgActiveDirectory -o cfgDomainController3 <域控制器的完全限定域名或 IP 地址>
```

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

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

警告： 在此版本中，如果 Active Directory 配置为扩展模式，将不支持基于 Smart Card 的双重验证 (TFA) 和单一登录 (SSO) 功能。

如果要禁用 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

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

在此情况下，您无需上载 CA 证书。

如果要执行 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

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

在此情况下，您需要使用以下 RACADM 命令上载 CA 证书：

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
racadm sslcertupload -t 0x2 -f <ADS 根 CA 证书>
```

以下 RACADM 命令可选。有关其它信息，请参阅"导入 iDRAC6 固件 SSL 证书"。

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

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

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

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

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 <主要 DNS IP 地址>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <次要 DNS IP 地址>
```

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

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

您最多可配置 40 个用户域，其索引编号为 1 至 40。

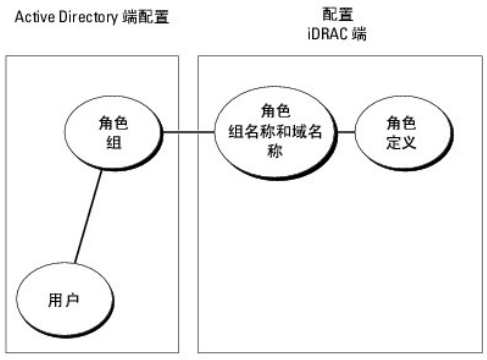
请参阅"使用 Active Directory 登录到 iDRAC6"了解关于用户域的详情。

5. 按 **Enter** 完成以扩展模式配置 Active Directory 的过程。

标准模式 Active Directory 概览

如图 7-3 中所示，为 Active Directory 集成使用标准模式需要在 Active Directory 和 iDRAC6 上都进行配置。

图 7-3. 使用 Microsoft Active Directory 和标准模式配置 iDRAC



在 Active Directory 端，标准组对象用作角色组。具有 iDRAC6 权限的用户将是该角色组的成员。为了授予该用户对特定 iDRAC6 的权限，需要在特定 iDRAC6 上配置角色组名称及其域名。与扩展模式解决方案不同，角色和权限级别在各个 iDRAC6 上定义，而不是在 Active Directory 中定义。每个 iDRAC 中可配置和定义多达五个角色组。 表 7-9 显示默认的角色组权限。

表 7-9. 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	"Administrator"（管理员）	**"Login to iDRAC"（登录到 iDRAC）、"Configure iDRAC"（配置 iDRAC）、"Configure Users"（配置用户）、"Clear Logs"（清除日志）、"Execute Server Control Commands"（执行服务器控制命令）、"Access Console Redirection"（访问控制台重定向）、"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	"Operator"（操作员）	**"Login to iDRAC"（登录到 iDRAC）、"Configure iDRAC"（配置 iDRAC）、"Execute Server Control Commands"（执行服务器控制命令）、"Access Console Redirection"（访问控制台重定向）、"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	"Read Only"（只读）	"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	无	没有分配权限	0x00000000

注： "位掩码"值只有在用 RACADM 设置标准模式时才使用。

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。

配置标准模式 Active Directory 以访问 iDRAC

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。必须使用基于 Web 的界面或 RACADM 在 iDRAC6 上配置组名称和此域的名称（请参阅"使用 iDRAC6 基于 Web 的界面以标准模式配置 Active Directory"或"使用 RACADM 以标准模式配置 Active Directory"）。
3. 添加作为 Active Directory 组成员访问 iDRAC 的 Active Directory 用户。

使用 iDRAC6 基于 Web 的界面以标准模式配置 Active Directory

1. 打开支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 基于 Web 的界面。
3. 展开**系统**树并单击**"Remote Access"（远程访问）**。
4. 单击**"Configuration"（配置）**选项卡并选择 **Active Directory**。
5. 滚动到**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页底部，然后单击**"Configure Active Directory"（配置 Active Directory）**。

   此时会出现**"Step 1 of 4 Active Directory Configuration and Management"（第 1 步，共 4 步 Active Directory 配置和管理）**页。
6. 在**"Certificate Settings"（证书设置）**下面，如果要验证 Active Directory 服务器的 SSL 证书，则选中**"Enable Certificate Validation"（启用证书认证）**；否则，转至步骤 9**。**
7. 在**"Upload Active Directory CA Certificate"（上载 Active Directory CA 证书）**下面，键入证书文件路径或浏览找到证书文件。

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

   将显示有效 Active Directory CA 证书的证书信息。
9. 在**"Upload Kerberos Keytab"（上载 Kerberos Keytab）**下，键入 Keytab 文件的路径或浏览查找该文件。单击**"Upload"（上载）**。Kerberos Keytab 将会上载到 iDRAC6。

10. 单击**"Next"（下一步）**以转至**"Step 2 of 4 Active Directory Configuration and Management"（第 2 步，共 4 步 Active Directory 配置和管理）**。

11. 选择**"Enable Active Directory"（启用 Active Directory）**。

12. 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）**。

13. 单击**"Add"（添加）**以输入用户域名。

14. 在提示符处输入用户域名并单击**"OK"（确定）**。

15. 键入**超时**时间（以秒为单位），指定 iDRAC6 等待 Active Directory 响应的时间。默认值为 120 秒钟。

16. 键入"Domain Controller Server Address"（域控制器服务器地址）。您可为登录处理最多输入三个 Active Directory 服务器，但必须通过输入 IP 地址或 FQDN 配置至少一个服务器。iDRAC6 会尝试连接到每个配置的服务器，直到建立连接为止。

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

17. 单击**"Next"（下一步）**以转至**"Step 3 of 4 Active Directory Configuration and Management"（第 3 步，共 4 步 Active Directory 配置和管理）**。

18. 在**"Schema Selection"（模式选择）**下，单击**"Standard Schema"（标准模式）**。

19. 单击**"Next"（下一步）**以转至**"Step 4a of 4 Active Directory Configuration and Management"（第 4a 步，共 4 步 Active Directory 配置和管理）页。**

20. 在**"Standard Schema Settings"（标准模式设置）**下，键入全局编录服务器地址以指定它在 Active Directory 中的位置。至少必须配置一个全局编录服务器的位置。

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

    注： 仅当用户帐户和角色组位于不同域中时，标准模式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。

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

    将显示**"Step 4b of 4"（步骤 4b，共 4 步）**页。

22. 指定**"Role Group Name"（角色组名称）**。

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

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

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

25. 单击**"Apply"（应用）**以保存角色组设置。

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

26. 重复步骤 20 至步骤 25 以配置其它角色组。

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

28. 单击**"Test Settings"（检测设置）**以检查 Active Directory 标准模式设置。

29. 键入 iDRAC6 用户名和密码。

    将显示检测结果和检测日志。有关详情，请参阅"检测配置"。

注： 您必须拥有在 iDRAC 上正确配置的 DNS 服务器才能支持 Active Directory 登录。单击**"Remote Access"（远程访问）→"Configuration"（配置）→"Network"（网络）**页以手动配置 DNS 服务器或使用 DHCP 获得 DNS 服务器。

现在完成了以标准模式配置 Active Directory 的过程。

使用 RACADM 以标准模式配置 Active Directory

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

1. 打开命令提示符并键入以下 RACADM 命令：

   racadm config -g cfgActiveDirectory -o cfgADEnable 1

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g cfgStandardSchema -i <索引> -o
   cfgSSADRoleGroupName <角色组常用名>

   racadm config -g cfgStandardSchema -i <索引> -o
   cfgSSADRoleGroupDomain <完全限定域名>

   racadm config -g cfgStandardSchema -i <索引> -o
   cfgSSADRoleGroupPrivilege <特定用户权限的位掩码编号>

   注： 有关位掩码编号值，请参阅表 B-2。

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <域控制器的完全限定域名或 IP 地址>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <域控制器的完全限定域名或 IP 地址>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <域控制器的完全限定域名或 IP 地址>

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

   注： 输入域控制器的 FQDN，而*不是*域的 FQDN。例如，输入 servername.dell.com 而不是 dell.com。

   注： 要求至少配置 3 个地址之一。iDRAC6 会尝试逐一连接到每个配置的地址，直到成功建立连接为止。对于标准模式来说，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： 仅当用户帐户和角色组位于不同域中时，标准模式才需要全局编录服务器。而在此多域情况下，仅可使用通用组。

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

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

   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0

   在此情况下，无需上载认证机构 (CA) 证书。

   如果要执行 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

   在此情况下，也必须使用以下 RACADM 命令上载 CA 证书：

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

   以下 RACADM 命令可选。有关其它信息，请参阅"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，则键入以下 RACADM 命令：

   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1

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

   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

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

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

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

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

最多可以配置 40 个用户域，索引编号介于 1 和 40 之间。

请参阅"使用 Active Directory 登录到 iDRAC6"了解关于用户域的详情。

检测配置

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

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

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

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

在域控制器上启用 SSL

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

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

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）**。

将域控制器根 CA 证书导出到 iDRAC

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）**字段中键入 mmc 并单击**"OK"（确定）**。
4. 在**"Console 1"（控制台 1）**(MMC) 窗口中，单击**"File"（文件）**（在 Windows 2000 系统上则单击**"Console"[控制台]**）并选择**"Add/Remove Snap-in"（添加/删除管理单元）**。
5. 在**"Add/Remove Snap-in"（添加/删除管理单元）**窗口中，单击**"Add"（添加）**。
6. 在**"Standalone Snap-in"（独立管理单元）**窗口中，选择**"Certificates"（证书）**并单击**"Add"（添加）**。
7. 选择**"Computer account"（计算机帐户）**并单击**"Next"（下一步）**。
8. 选择**"Local Computer"（本地计算机）**并单击**"Finish"（完成）**。
9. 单击**"OK"（确定）**。
10. 在**"Console 1"（控制台 1）**窗口中，展开**"Certificates"（证书）**文件夹，展开**"Personal"（个人）**文件夹并单击**"Certificates"（证书）**文件夹。
11. 找到并右键单击根 CA 证书，选择**"All Tasks"（所有任务）**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，不导出私钥）**。
13. 单击**"Next"（下一步）**并选择**"Base-64 encoded X.509 (.cer)"（ Base-64 编码 X.509 [.cer]）**作为格式。

14. 单击**"Next"（下一步）**并将证书保存至系统上的目录。

15. 将在步骤 14 保存的证书上载到 iDRAC 。

    要使用 RACADM 上载证书，请参阅"使用 iDRAC6 基于 Web 的界面以扩展模式配置 Active Directory"或"使用 RACADM 以标准模式配置 Active Directory"。

    要使用基于 Web 的界面上载证书，请参阅"使用 iDRAC6 基于 Web 的界面以扩展模式配置 Active Directory"或"使用 iDRAC6 基于 Web 的界面以标准模式配置 Active Directory"。

导入 iDRAC6 固件 SSL 证书

注： 如果 Active Directory 服务器设置为在 SSL 会话初始化期间验证客户端，则还需要将 iDRAC 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 iDRAC 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。

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

要下载 iDRAC SSL 证书，请运行以下 RACADM 命令：

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

1. 在域控制器上，打开**"MMC Console"（MMC 控制台）**窗口并选择**"Certificates"（证书）→"Trusted Root Certification Authorities"（受信任的根认证机构）**。

2. 右键单击**"Certificates"（证书）**，选择**"All Tasks"（所有任务）**并单击**"Import"（导入）**。

3. 单击**"Next"（下一步）**并浏览查找到 SSL 证书文件。

4. 在每个域控制器的**"Trusted Root Certification Authority"（受信任的根认证机构）**中安装 iDRAC 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）**。

使用 Active Directory 登录到 iDRAC6

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

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

登录语法对于所有这三种方法都是一致的：

<*用户名@域*>

或

<*域*>\<*用户名*> 或 <*域*>/<*用户名*>

其中*用户名*是 1-256 字节的 ASCII 字符串。

用户名和域名中不能使用空格和特殊字符（例如 \、/ 或 @）。

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

如果从基于 Web 的界面登录且配置了用户域，则基于 Web 的界面登录页会在下拉式菜单中列出所有用户域供您选择。如果从下拉式菜单中选择一个用户域，则只需输入用户名。如果选择**"This iDRAC"（此 iDRAC）**，则只要您使用"使用 Active Directory 登录到 iDRAC6"中的上述登录语法，仍可作为 Active Directory 用户登录。

还可以使用 Smart Card 登录 DRAC6。有关详情，请参阅"使用 Smart Card 登录 iDRAC6"。

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

使用 Active Directory 单一登录

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"启用 Kerberos 验证"。

配置 iDRAC6 以使用单一登录

1. 单击**"Remote Access"（远程访问）**→**"Configuration"（配置）**选项卡→ **Active Directory** 子选项卡 → 选择**"Configure Active Directory"（配置 Active Directory）**。

2. 在**"Step 2 of 4 Active Directory Configuration and Management"（步骤 2，共 4 步 Active Directory 配置和管理）**页上，选择**"Enable Single Sign-On"（启用单一登录）**。只有在选中**"Enable Active Directory"（启用 Active Directory）**后，**"Enable Single Sign-On"（启用单一登录）**选项才启用。

   "Enable Single Sign-On"（启用单一登录）选项允许在登录到工作站后不输入域用户验证凭据（比如用户名和密码）直接登录 iDRAC6。要使用此功能登录 iDRAC6，应已使用有效 Active Directory 用户帐户登录到系统。另外，应已配置用户帐户使用 Active Directory 凭据登录 iDRAC6。iDRAC6 使用缓存的 Active Directory 凭据登录。

   要使用 CLI 启用单一登录，请运行 racadm 命令：

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

使用单一登录来登录到 iDRAC6

1. 使用网络帐户登录工作站。

2. 要访问 iDRAC6 网页，请键入：

   `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。

   将显示 iDRAC6 单一登录页。

3. 单击**"Login"（登录）**。

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

关于 Active Directory 的常见问题

我的 Active Directory 登录失败，我该如何排除此问题？

iDRAC6 在基于 Web 的界面中提供了一个诊断工具。从基于 Web 的界面以拥有管理员权限的本地用户身份登录。单击**"Remote Access**"（远程访问）→**"Configuration"（配置）** → **Active Directory**。滚动到**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页底部，然后单击**"Test Settings"（检测设置）**。输入检测用户名和密码，然后单击**"Start Test"（开始检测）**。iDRAC6 会逐步运行测试并显示每个步骤的结果。还会记录详细的检测结果，以帮助您解决问题。单击 **Active Directory** 选项卡以返回到**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页。滚动到页面底部，然后单击**"Configure Active Directory"（配置 Active Directory）**以更改配置并再次运行检测，直到检测用户通过授权步骤为止。

我启用了证书验证，但我的 Active Directory 登录失败了。我从 GUI 运行诊断，检测结果显示以下错误信息：

ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC.（错误：不能联系 LDAP 服务器，错误：14090086：SSL 例程：SSL3_GET_SERVER_CERTIFICATE：证书验证失败：请检查正确的认证机构 (CA) 证书是否已上载到 iDRAC。）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.（另请检查 iDRAC 日期是否在证书有效期内，且 iDRAC 中配置的域控制器地址是否与目录服务器证书的主题相符。）

可能出现了什么问题，我应该如何解决？

如果启用证书验证，则 iDRAC6 在与目录服务器建立 SSL 连接时会使用上载的 CA 证书验证目录服务器证书。证书验证失败的最常见原因是：

1. iDRAC6 日期不在服务器证书或 CA 证书的有效期内。请检查 iDRAC6 时间和证书的有效期。

2. iDRAC 中配置的域控制器地址与目录服务器证书的主题或主题备用名称不相符。如果使用的是 IP 地址，请阅读以下问题和解答。如果使用的是 FQDN，请确保使用的是域控制器的

FQDN，而不是域的 FQDN，例如，是 servername.example.com，而不是 example.com。

我使用域控制器地址的 IP 地址且不能通过证书验证。问题在哪里？

请检查域控制器证书的"Subject"（主题）或"Subject Alternative Name"（主题备用名称）字段。通常 Active Directory 在域控制器证书的"Subject"（主题）或"Subject Alternative Name"（主题备用名称）字段中使用域控制器的主机名而不是 IP 地址。可以使用多种方法解决此问题：

1. 在 iDRAC6 上将域控制器的主机名称 (FQDN) 配置为*域控制器地址*，以与服务器证书的主题或主题备用名称相符。
2. 重新颁发服务器证书以在"Subject"（主题）或"Subject Alternative Name"（主题备用名称）字段中使用 IP 地址，从而与在 iDRAC6 中配置的 IP 地址匹配。
3. 如果选择信任此域控制器而无需在 SSL 握手过程中验证证书，请禁用证书验证。

我目前在多域环境中使用扩展模式，我该如何配置域控制器地址？

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

何时需要配置全局编录地址？

如果使用的是扩展模式，则不使用全局编录地址。

如果使用的是标准模式且用户和角色组来自不同的域，则必须配置全局编录地址。在此情况下，仅可使用通用组。

如果使用的是标准模式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。

标准模式的查询方式是什么？

iDRAC6 先连接到所配置的域控制器地址，如果用户和角色组位于该域，将保存权限。

如果配置了全局控制器地址，则 iDRAC6 会继续查询全局编录。如果从全局编录中检索到其它权限，则会累积这些权限。

iDRAC6 总在 SSL 上使用 LDAP 吗？

是。所有传输都通过安全端口 636 和/或 3269。

在*检测设置*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。

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证书验证，您可通过 GUI 或 CLI 将其禁用。

iDRAC6 支持 NetBIOS 名称吗？

此版本不支持。

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

可以在 iDRAC6 基于 Web 的界面中的**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页底部单击**"Test Settings"（检测设置）**，从而诊断问题。然后根据检测结果修复具体问题。有关详情，请参阅"检测配置"。

本节说明了多数常见问题，但一般而言，您应检查以下各项：

1. 确保在登录期间使用正确的用户域名，而不是 NetBIOS 名称。
2. 如果具有本地 iDRAC6 用户帐户，请使用本地凭据登录 iDRAC6。

   登录后：

   a. 确保已选中 iDRAC6 的**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页上的**"Enable Active Directory"（启用 Active Directory）**框。
   b. 确保 iDRAC6 网络配置页上的 DNS 设置正确。
   c. 如果启用了证书验证，请确保已将正确的 Active Directory 根 CA 证书上载到 iDRAC6。确保 iDRAC6 时间在 CA 证书的有效期内。
   d. 如果使用扩展模式，则确保 **iDRAC6 名称**和 **iDRAC6 域名**与 Active Directory 环境配置相符。

      如果使用标准模式，则确保**组名称**和**组域名**与 Active Directory 配置相符。
3. 检查域控制器 SSL 证书以保证 iDRAC6 时间在证书的有效期内。

目录

目录

配置 Smart Card 验证

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

iDRAC6 启用 **Smart Card 登录**支持双重验证 (TFA) 功能。

传统的验证模式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 Smart Card，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 Smart Card 登录

要从基于 Web 的界面启用 iDRAC6 Smart Card 登录功能，请进入**"Remote Access"（远程访问）→"Configuration"（配置）→ Smart Card**，然后选择**"Enable"（启用）**。

如果您：

- **启用**或**随远程 Racadm 启用**，会在随后使用基于 Web 的界面尝试登录时提示进行 Smart Card 登录。

  选择**"Enable"（启用）**后，所有命令行界面 (CLI) 带外接口，比如 Telnet、SSH、Serial、远程 racadm 和 LAN 上 IPMI 都会禁用，因为这些服务只支持单重验证。

  选择**"Enable with Remote Racadm"（随远程 Racadm 启用）**后，除远程 racadm 以外的所有 CLI 带外接口都会禁用。

  注： Dell 建议 iDRAC6 管理员将**"Enable with Remote Racadm"（随远程 Racadm 启用）**设置只用来访问 iDRAC6 基于 Web 的界面来使用远程 RACADM 命令运行脚本。如果管理员不需要使用远程 RACADM，Dell 会建议使用 Smart Card 登录的**"Enabled"（已启用）**设置。另外，启用 **Smart Card 登录**前，确保完成了 iDRAC6 本地用户配置和/或 Active Directory 配置。

- **禁用** Smart Card 配置（默认）。此选项禁用 TFA Smart Card 登录功能，当您下次登录到 iDRAC6 GUI 时，将提示输入 Microsoft® Active Directory® 或本地登录用户名和密码，这是从 Web 界面出现的默认登录提示。
- **"Enable CRL check for Smart Card Logon"（启用 CRL 检查进行 Smart Card 登录）**，会对从证书撤回列表 (CRL) 分发服务器下载的用户 iDRAC 证书进行检查以在 CRL 中撤回。

  注： CRL 分发服务器列在用户的 Smart Card 证书中。

配置本地 iDRAC6 用户进行 Smart Card 登录

您可配置本地 iDRAC6 用户，使用 Smart Card 登录到 iDRAC6。单击**"Remote Access"（远程访问）→"Configuration"（配置）→"Users"（用户）**。

但是，在用户可以使用 Smart Card 登录到 iDRAC6 之前，必须将用户的 Smart Card 证书和可信认证机构 (CA) 证书上载到 iDRAC6。

导出 Smart Card 证书

可以通过使用卡管理软件 (CMS) 将 Smart Card 证书从 Smart Card 导出为 Base64 编码格式的文件来获得用户证书。通常可以从 Smart Card 供应商处获得 CMS。该编码文件应作为用户证书上载到 iDRAC6。颁发 Smart Card 用户证书的可信认证机构也应将 CA 证书导出为 Base64 编码格式的文件。应将此文件作为用户的可信 CA 证书进行上载。用 Smart Card 证书中组成用户基本名 (UPN) 的用户名来配置用户。

注： 要登录 iDRAC6，在 iDRAC6 中配置的用户名应与 Smart Card 证书中的用户基本名 (UPN) 大小写一致。

例如，如果已给用户 "sampleuser@domain.com" 颁发 Smart Card 证书，用户名应配置为 "sampleuser"。

为 Smart Card 登录配置 Active Directory 用户

要配置 Active Directory 用户使用 Smart Card 登录 iDRAC6，iDRAC6 管理员应配置 DNS 服务器，上载 Active Directory CA 证书到 iDRAC6，并启用 Active Directory 登录。有关如何设置 Active Directory 用户的详情，请参阅"将 iDRAC6 用于 Microsoft Active Directory"。

注： 如果 Smart Card 用户在 Active Directory 内，则需要 Active Directory 密码连同 Smart Card PIN。

可以从**"Remote Access"（远程访问）**→**"Configuration"（配置）**→ **Active Directory** 来配置 Active Directory。

配置 Smart Card

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

1. 展开**系统**树并单击**"Remote Access"（远程访问）**。
2. 单击**"Configuration"（配置）**选项卡，然后单击 **Smart Card**。
3. 配置 Smart Card 登录设置。

   表 8-1 提供了有关 **Smart Card** 页设置的信息。
4. 单击**"Apply Changes"（应用更改）**。

表 8-1. Smart Card 设置

设置	说明
配置 Smart Card 登录	• **"Disabled"（已禁用）** — 禁用 Smart Card 登录。随后从图形用户界面 (GUI) 进行的登录会显示常规登录页。所有命令行带外接口，包括 secure shell (SSH)、 Telnet、Serial 和远程 RACADM 都会设置为默认状态。 • **"Enabled"（启用）** — 启用 Smart Card 登录。应用更改后，注销，插入 Smart Card，然后单击**"Login"（登录）**并输入 Smart Card PIN。启用 Smart Card 登录会禁用所有 CLI 带外接口，包括 SSH、Telnet、Serial、远程 RACADM 和 LAN 上 IPMI。 • **"Enabled with Remote Racadm"（随远程 Racadm 启用）**— 随远程 RACADM 启用 Smart Card 登录。其它所有 CLI 带外接口都会禁用。 **注：** Smart Card 登录要求用适当的证书配置本地 iDRAC6 用户。如果使用 Smart Card 登录来登录 Microsoft Active Directory 用户，则必须确保为该用户配置 Active Directory 用户证书。可以在**"Users"（用户）**→**"User Main Menu"（用户主菜单）**页配置用户证书。
"Enable CRL check for Smart Card Logon"（启用 CRL 检查进行 Smart Card 登录）	此检查仅供 Smart Card 本地用户使用。如果希望 iDRAC6 检查证书撤回列表 (CRL) 撤回用户 Smart Card 证书，则选择此选项。为了使 CRL 功能起作用，iDRAC6 的网络配置中必须配置了有效的 DNS IP 地址。可以在 iDRAC6 中的**"Remote Access"（远程访问）**→**"Configuration"（配置）**→**"Network"（网络）**下配置 DNS IP 地址。 在以下情况下，用户将无法登录： • 用户证书在 CRL 文件中列为已撤回。 • iDRAC6 无法与 CRL 分发服务器通信。 • iDRAC6 无法下载 CRL。 **注：** 必须在**"Configuration"（配置）**→**"Network"（网络）**页中正确配置 DNS 服务器的 IP 地址，此检查才能成功。

使用 Smart Card 登录 iDRAC6

iDRAC6 Web 界面会向所有配置为使用 Smart Card 的用户显示 Smart Card 登录页。

注： 为用户启用 Smart Card 登录之前，确保完成了 iDRAC6 本地用户配置和/或 Active Directory 配置。

注： 根据浏览器设置的不同，第一次使用此功能时，可能会提示下载并安装 Smart Card 阅读器 ActiveX 插件。

1. 使用 https 访问 iDRAC6 Web 页面。

   `https://<IP 地址>`

   如果默认 HTTPS 端口号（端口 443）已更改，请键入：

   `https://<IP 地址>:<端口号>`

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

   iDRAC6"Login"（登录）页会显示出来，提示插入 Smart Card。

2. 将 Smart Card 插入阅读器并单击**"Login"（登录）**。

   iDRAC6 会提示输入 Smart Card 的 PIN。

3. 输入本地 Smart Card 用户的 Smart Card PIN，如果未在本地创建用户，则 iDRAC6 将提示输入用户 Active Directory 帐户的密码。

注： 如果是已选中**"Enable CRL check for Smart Card Logon"（启用 CRL 检查进行 Smart Card 登录）**的 Active Directory 用户，iDRAC6 会尝试下载 CRL 并在 CRL 中检查用户证书。如果证书在 CRL 中列为已撤回或由于某些原因不能下载 CRL，则通过 Active Directory 登录会失败。

您已登录 iDRAC6。

使用 Active Directory Smart Card 验证登录 iDRAC6

1. 使用 https 登录 iDRAC6。

   `https://<IP 地址>`

   如果默认 HTTPS 端口号（端口 443）已更改，请键入：

   `https://<IP 地址>:<端口号>`

   其中 *IP 地址*是 iDRAC6 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 Smart Card。

2. 插入 Smart Card 并单击**"Login"（登录）**。

   将显示 PIN 弹出对话框。

3. 输入 PIN，并单击**"OK"（确定）**。

4. 输入用户的 Active Directory 密码验证用户，然后单击**"OK"（确定）**。

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

注： 如果 Smart Card 用户在 Active Directory 内，则需要 Active Directory 密码连同 SC PIN。在以后的版本中，可能不需要 Active Directory 密码。

对 iDRAC6 中的 Smart Card 登录进行故障排除

参考以下提示帮助调试无法访问的 Smart Card：

ActiveX 插件无法检测到 Smart Card 阅读器

确保 Smart Card 在 Microsoft Windows® 操作系统上受支持。Windows 支持有限的几种 Smart Card 加密服务提供程序 (CSP)。

提示：作为常规检查看 Smart Card CSP 是否位于特定客户端上，在出现 Windows 登录 (Ctrl-Alt-Del) 屏幕时将 Smart Card 插入阅读器并查看 Windows 是否检测到 Smart Card 并显示 PIN 对话框。

不正确的 Smart Card PIN

检查 Smart Card 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 Smart Card 颁发者应能够帮助获得新的 Smart Card。

无法登录本地 iDRAC6

如果本地 iDRAC6 用户不能登录，检查上载到 iDRAC6 的用户名和用户证书是否已经过期。iDRAC6 跟踪日志可能会提供有关错误的重要日志信息；尽管有时由于安全考虑，错误信息可能会有意模棱两可。

无法以 Active Directory 用户的身份登录 iDRAC6

如果无法以 Active Directory 用户的身份登录 iDRAC6，则尝试不启用 Smart Card 登录来登录 iDRAC6。如果已启用 CRL 检查，则尝试不启用 CRL 检查来进行 Active Directory 登录。CRL 失败时，iDRAC6 跟踪日志应能够提供重要信息。

还可以选择用以下命令通过本地 racadm 禁用 Smart Card 登录：

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

目录

目录

使用 GUI 控制台重定向

Integrated Dell® Remote Access Controller 6 (iDRAC6) 版本 1.1 用户指南

本节提供关于使用 iDRAC6 控制台重定向功能的信息。

概览

iDRAC6 控制台重定向功能使您能够以图形或文本模式远程访问本地控制台。您可以利用控制台重定向在一个位置控制一个或多个已启用 iDRAC6 的系统。

不用再坐在每台服务器前执行各种日常维护。而是可以在任何地方从台式机或膝上型计算机管理服务器。还可以与他人共享信息 — 无论多么遥远，都可以迅速共享。

使用控制台重定向

注： 打开控制台重定向会话时，受管服务器不会指示控制台已经重定向。

注： 如果已经打开从 Management Station 至 iDRAC6 的控制台重定向会话，则试图打开从同一 Management Station 至此 iDRAC6 的新会话将激活现有的会话。不会生成新的会话。

注： 可同时打开多个从单个 Management Station 至多个 iDRAC6 控制器的控制台重定向会话。

"Console Redirection"（控制台重定向）页使您能够通过使用本地 Management Station 上的键盘、视频和鼠标管理远程系统，从而控制远程受管服务器上相应的设备。此功能可以与虚拟介质功能配合使用以执行远程软件安装。

以下规则适用于控制台重定向会话：

- 最多可同时支持四个控制台重定向会话。所有会话同时查看同一个受管服务器控制台。
- 从同一客户端控制台（Management Station）至远程服务器 (iDRAC6) 仅可打开一个会话。然而，同一客户端可向多个远程服务器发出多个会话。
- 不应从 Managed System 上的 Web 浏览器启动控制台重定向会话。
- 最低要求 1 MB/sec 可用网络带宽。

对 iDRAC 的第一个控制台重定向会话为完全访问会话。如果第二位用户请求控制台重定向会话，第一位用户将被告知并可选择拒绝、**允许只读**或**批准**。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，否则将拒绝第二位用户的访问。

如上次的完全访问会话终止，所有的**允许只读**会话亦会自动终止。

配置 Management Station

要在 Management Station 上使用控制台重定向，请执行以下过程：

1. 安装并配置一个支持的 Web 浏览器。有关详情，请参阅以下章节：
   - "支持的 Web 浏览器"
   - "配置支持的 Web 浏览器"

   注： 必须在 Management Station 上安装 Java Run Time Environment，才能使用控制台重定向功能。

2. 如果使用 Internet Explorer，请按以下方式确保浏览器能够下载加密内容：
   - 转至 Internet Explorer 选项或设置，并选择**"Tools"（工具）→"Internet Options"（Internet 选项）→"Advanced"（高级）**。
   - 滚动至**"Security"（安全性）**并取消选中此选项：

     请勿将加密页面保存在磁盘中

3. 建议将显示器的显示分辨率配置为 1280x1024 像素或更高。

注： 如果系统运行的是 Linux 操作系统，本地显示器上可能无法查看 X11 控制台。在 iDRAC KVM 上按 <Ctrl><Alt><F1> 会将 Linux 切换到文本控制台。

注： 有时可能遇到以下 Java 脚本编译错误："Expected: ;"（预期的：；） 。要解决此问题，请调整网络设置，使用 JavaWebStart 中的"Direct connection"（直接连接）："Edit"（编辑）→"Preferences"（首选项）→"General"（常规）→"Network Settings"（网络设置），并选择"Direct connection"（直接连接）而非"Use browser settings"（使用浏览器设置）。

在 iDRAC Web 界面中配置控制台重定向

要在 iDRAC Web 界面中配置控制台重定向，请执行下列步骤：

1. 单击**"System"（系统）→"Console/Media"（控制台/介质）→ "Configuration"（配置）**以配置 iDRAC 控制台重定向设置。
2. 配置控制台重定向属性。 表 10-1 说明控制台重定向的设置。
3. 完成后，单击**"Apply Changes"（应用更改）**。
4. 单击相应按钮继续。请参阅表 10-2。

表 10-1. 控制台重定向配置属性

属性	说明
"Enabled"（已启用）	单击可以启用或禁用控制台重定向。如果选中此选项，则表示启用控制台重定向。默认值为**"enabled"（已启用）**。 **注：** 在启动虚拟 KVM 后选中或清除**"Enabled"（已启用）**选项会断开所有现有的虚拟 KVM 会话连接。
"Max Sessions"（最大会话数）	显示可能打开的控制台重定向会话的最大数目，为 1 至 4。使用下拉式菜单可以更改允许的控制台重定向会话的最大允许数目。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。
"Remote Presence Port"（远程存在端口）	用于连接到"Console Redirection"（控制台重定向）键盘/鼠标选项的网络端口号。此通信量始终加密。如果其它程序正在使用默认端口，可能需要更改此编号。默认值为 **5900**。 **注：** 在启动虚拟 KVM 后修改**"Remote Presence Port"（远程存在端口）**值会断开所有现有的虚拟 KVM 会话连接。
"Video Encryption Enabled"（视频加密已启用）	**选中**表示视频加密已启用。进入视频端口的所有通信量均被加密。 **取消选中**表示视频加密已禁用。进入该视频端口的通信量均未加密。 默认值为**"Encrypted"（加密）。禁用加密可以提高较慢网络上的性能。** **注：** 在启动虚拟 KVM 后启用或禁用**"Video Encryption Enabled"（视频加密已启用）**选项会断开所有现有的虚拟 KVM 会话连接。
"Local Server Video Enabled"（本地服务器视频已启用）	选中表示在控制台重定向期间到 iDRAC KVM 显示器的输出已禁用。这可确保用户使用**"Console Redirection"（控制台重定向）**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： 有关借助控制台重定向使用虚拟介质的信息，请参阅"配置并使用虚拟介质"。

表 10-2 中的按钮在**"Configuration"（配置）**页上可用。

表 10-2. 配置页按钮

按钮	定义
"Print"（打印）	打印页面
"Refresh"（刷新）	重新载入**"Configuration"（配置）**页
"Apply Changes"（应用更改）	保存任何新的或已更改设置

打开控制台重定向会话

打开控制台重定向会话时，会启动 Dell™ 虚拟 KVM Viewer 应用程序，并且在查看器中会出现远程系统的桌面。使用虚拟 KVM Viewer 应用程序，可以从本地 Management Station 控制远程系统的鼠标和键盘功能。

要在 Web 界面中打开控制台重定向，请执行下列步骤：

1. 单击**"System"（系统）→"Console/Media"（控制台/介质）→ "Console Redirection and Virtual Media"（控制台重定向和虚拟介质）**。

2. 使用表 10-3 中的信息确保控制台重定向会话可用。

   如果想要重新配置显示的任何属性值，请参阅"在 iDRAC Web 界面中配置控制台重定向"。

表 10-3. 控制台重定向

属性	说明
"Console Redirection Enabled"（控制台重定向已启用）	是/否（选中/取消选中）
"Video Encryption Enabled"（视频加密已启用）	是/否（选中/取消选中）
"Max Sessions"（最大会话数）	显示支持的最大控制台重定向会话数
"Active Sessions"（激活的会话数）	显示当前活动控制台重定向会话数
"Local Server Video Enabled"（本地服务器视频已启用）	"Yes"（是）= 已启用；"No"（否）= 已禁用。
"Remote Presence Port"（远程存在端口）	用于连接到"Console Redirection"（控制台重定向）键盘/鼠标选项的网络端口号。此通信量始终加密。如果其它程序正在使用默认端口，可能需要更改此编号。默认值为 5900。

注： 有关借助控制台重定向使用虚拟介质的信息，请参阅"配置并使用虚拟介质"。

表 10-4 中的按钮可以在**"Console Redirection and Virtual Media"（控制台重定向和虚拟介质）**页使用。

表 10-4. 控制台重定向和虚拟介质页按钮

按钮	定义
"Refresh"（刷新）	重新载入**"Console Redirection and Virtual Media"（控制台重定向和虚拟介质）**页
"Launch Viewer"（启动 Viewer）	在目标远程系统上打开一个控制台重定向会话
"Print"（打印）	打印**"Console Redirection and Virtual Media"（控制台重定向和虚拟介质）**页

3. 如果控制台重定向会话可用，则单击**"Launch Viewer"（启动 Viewer）**。

   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： 如果在以下步骤中出现一个或多个**"Security Alert"（安全警报）**窗口，请阅读窗口中的信息并单击**"Yes"（是）**继续。

   Management Station 连接到 iDRAC6，在 iDRAC KVM Viewer 应用程序中显示远程系统的桌面。

4. 两个鼠标指针出现在查看器窗口中：一个是远程系统的，一个是本地系统的。可通过选择 iDRAC KVM 菜单中**"Tools"（工具）**下的**"Single Cursor"（单光标）**选项更改为单光标。

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： 如果切断远程服务器电源，将显示**"No Signal"（无信号）**信息。

Video Viewer 提供了各种控制调整，比如鼠标同步、快照、键盘宏指令和虚拟介质访问。有关这些功能的详情，请单击**"System"（系统）**→**"Console/Media"（控制台/介质）**，并单击**"Console Redirection and Virtual Media"（控制台重定向和虚拟介质）**页上的**"Help"（帮助）**。

当启动控制台重定向会话并出现 Video Viewer 时，可能需要同步鼠标指针。

禁用或启用本地服务器视频

可以使用 iDRAC6 Web 界面将 iDRAC6 配置为禁用 iDRAC KVM 连接。

如果想保证对受管服务器控制台有独占访问，必须在**"Console Redirection Configuration"（控制台重定向配置）页**上禁用本地控制台*并重新配置***"Max Sessions"（最大会话数）**为 1。

注： 禁用（关闭）服务器上的本地视频后，连接到 iDRAC KVM 的显示器、键盘和鼠标仍然启用。

要禁用或启用本地控制台，请执行以下过程：

1. 在 Management Station 上，打开支持的 Web 浏览器并登录 iDRAC。有关详情，请参阅"访问 Web 界面"。

2. 单击**"System"（系统）→"Console/Media"（控制台/介质）→ "Configuration"（配置）**。

3. 要禁用（关闭）服务器上的本地视频，请取消选中**"Configuration"（配置）**页上的**"Local Server Video Enabled"（本地服务器视频已启用）**复选框，然后单击**"Apply"（应用）**。默认值为"OFF"（关）。

   注： 如果开启本地服务器视频，将需 15 秒关闭。

4. 要启用（打开）服务器上的本地视频，请选中**"Configuration"（配置）**页上的**"Local Server Video Enabled"（本地服务器视频已启用）**复选框，然后单击**"Apply"（应用）**。

关于控制台重定向的常见问题

表 10-5 列出常见问题和解答。

表 10-5. 使用控制台重定向：常见问题

问题	解答
在服务器上的本地视频关闭时可以启动新的远程控制台视频会话吗？	可以。
为什么请求关闭本地视频后需要 15 秒才能关闭服务器上的本地视频？	使本地用户有机会在视频关闭前采取某些操作。
打开本地视频时有时间延迟吗？	没有，iDRAC6 收到本地视频打开请求后，视频就立刻**打开**。
本地用户还可以关闭视频吗？	当本地控制台禁用时，本地用户不能关闭视频。
本地用户还可以打开视频吗？	当本地控制台禁用时，本地用户不能打开视频。
关闭本地视频是否也会关闭本地键盘和鼠标？	不会。
关闭本地控制台是否会关闭远程控制台会话上的视频？	不会，打开或关闭本地视频与远程控制台会话无关。
iDRAC 用户打开或关闭本地服务器视频需要什么权限？	任何具有 iDRAC 配置权限的用户都可以打开或关闭本地控制台。
如何获得本地服务器视频的最新状态？	该状态显示在 iDRAC Web 界面的**"Console Redirection Configuration"（控制台重定向配置）**页上。 RACADM CLI 命令 **racadm getconfig -g cfgRacTuning** 在对象 **cfgRacTuneLocalServerVideo** 中显示状态。
从控制台重定向窗口不能看到系统屏幕的底部。	确保 Management Station 的显示器分辨率设置为 1280x1024。另外，还可尝试使用 iDRAC KVM 客户端的滚动栏。
控制台窗口显示乱码。	Linux 上的控制台查看器要求 UTF-8 字符集。检查区域设置并根据需要重设字符集。
为什么鼠标在 Linux 文本控制台下不同步？	虚拟 KVM 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。	启动控制台重定向会话前，确保为操作系统选择正确的鼠标。 请确保在 iDRAC KVM 客户端上选择 iDRAC KVM 菜单中**"Tools"（工具）**下的**"Single Cursor"（单光标）**选项。
为什么使用 iDRAC6 控制台重定向远程安装 Microsoft 操作系统期间不能使用键盘或鼠标？	在 BIOS 中启用了控制台重定向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 中关闭控制台重定向。 此信息由 Microsoft 生成，用以警告用户，控制台重定向已启用。为了确保不显示此信息，远程安装操作系统前，应始终在 BIOS 中关闭控制台重定向。
为什么 Management Station 上的 Num Lock 指示灯不反映远程服务器上 Num Lock 的状态？	当通过 iDRAC 访问时，Management Station 上的 Num Lock 指示灯不一定与远程服务器上的 Num Lock 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控制台重定向会话时显示多个 Session Viewer 窗口？	您在从本地系统配置控制台重定向会话。这不受支持。
如果我正在运行控制台重定向会话时本地用户访问受管服务器，会收到警告信息吗？	不会。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控制台重定向会话？	Dell 建议 5 MB/sec 连接以获得良好性能。最低性能要求 1 MB/sec 连接。
Management Station 运行控制台重定向有什么最低系统要求？	Management Station 需要 Intel® Pentium® III 500 MHz 处理器，且 RAM 至少为 256 MB。
为什么我在 iDRAC KVM Video Viewer 上看到一则**"No Signal"（无信号）**信息？	您看到此信息可能是因为 iDRAC 虚拟 KVM 插件未接收到远程服务器桌面视频。通常，在远程服务器被切断电源时可能发生此行为。有时此信息可能由于远程服务器桌面视频接收故障而显示。
为什么我在 iDRAC KVM Video Viewer 上看到一则**"Out of Range"（超出范围）**信息？	您看到此信息可能是因为捕获视频所需的参数超出 iDRAC 能够捕获视频的范围。显示分辨率或刷新率等参数过高将导致出现超过范围状况。通常，参数的最大范围由视频内存大小或带宽等物理限制设置。
