

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

[iDRAC6 概览](#)

[iDRAC6 使用入门](#)

[iDRAC6 的基本安装](#)

[使用 Web 界面配置 iDRAC6](#)

[iDRAC6 的高级配置](#)

[添加和配置 iDRAC6 用户](#)

[将 iDRAC6 用于 Microsoft Active Directory](#)

[配置 Smart Card 验证](#)

[使用 GUI 控制台重定向](#)

[配置并使用虚拟介质](#)

[使用 WS-MAN 界面](#)

[使用 iDRAC6 SM-CLP 命令行界面](#)

[使用 VMCLI 部署 操作系统](#)

[配置智能平台管理接口 \(IPMI\)](#)

[使用 iDRAC 配置公用程序](#)

[监控和警报管理](#)

[对 Managed System 进行恢复和故障排除](#)

[对 iDRAC6 进行恢复和故障排除](#)

[传感器](#)

[电源监控和管理](#)

[配置安全功能](#)

[RACADM 子命令概览](#)

[iDRAC6 属性数据库组和对象定义](#)

[支持的 RACADM 接口](#)

[词汇表](#)

注和小心

 **注：**“注”表示可以帮助您更好地使用计算机的重要信息。

 **小心：**“注意”表示如果不遵循说明，就有可能损坏硬件或导致数据丢失。

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/或其它国家的商标或注册商标；Red Hat 和 Linux Red Hat, Inc. 在美国和其他国家的的注册商标；SUSE 是 Novell Corporation 的注册商标。Intel 和 Pentium 是 Intel Corporation 在美国和其它国家的注册商标；UNIX 是 The Open Group 在美国和其它国家的注册商标；VMware 是 VMware, Inc. 在美国 / 或其它管辖区的注册商标。

版权 1998-2006 The OpenLDAP Foundation. All rights reserved (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顶层目录中的 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/或赠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资源的材料。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. All rights reserved (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 Halvard B. Furuseth. All rights reserved (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，需要保留此通告才行。在没有得到版权所有者的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，不帶任何明示或暗示的保证。部分版权 (c) 1992-1996 Regents of the University of Michigan. All rights reserved (版权所有，翻印必究)。只要保留此通告并且应有权利归属于 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，不帶任何明示或暗示的保证。本说明文件中提及的其它商标和名称是指拥有相应商标和名称的公司或其制造的产品。Dell Inc. 对本公司的商标和名称之外的其它商标和名称不拥有任何专有权。

2009 年 3 月 修订 A00

RACADM 子命令概览

Integrated Dell™ Remote Access Controller固件版本1.2
用户指南

- [help](#)
- [config](#)
- [getconfig](#)
- [getssninfo](#)
- [getsysinfo](#)
- [getractime](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [clrtraclog](#)
- [getsel](#)
- [clrsel](#)
- [gettracelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)

本节提供了 RACADM 命令行界面中可用子命令的说明。

help

[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，并且为每个子命令提供了一行说明。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

- 1 本地 RACADM

config

[表 A-2](#) 说明了 **config** 和 **getconfig** 子命令。

表 A-2. config/getconfig

命令	定义
----	----

子命令	定义
config	配置 iDRAC。
getconfig	获取 iDRAC 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

- 1 本地 RACADM

说明

`config` 子命令允许用户分别设置 iDRAC 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 iDRAC 对象写入新值。

输入

表 A-3 说明了 `config` 子命令选项。

表 A-3. `config` 子命令选项和说明

选项	说明
-f	-f <文件名> 选项会使 <code>config</code> 读取由 <文件名> 指定的文件内容并配置 iDRAC。该文件必须包含在 配置文件语法 中所指定格式的数据。
-p	-p, 或密码, 选项指示 <code>config</code> 在配置完成后删除 <code>config</code> 文件 -f <文件名> 中包含的密码条目。
-g	-g <组名>, 或组, 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>, 或对象, 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> (或索引选项) 只对索引组有效, 可用于指定唯一组。在此处该索引由索引值指定, 而不由“命名”值指定。
-c	-c, 或检查, 选项与 <code>config</code> 子命令配合使用, 并使用用户可以分析 .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 iDRAC 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:

- 1 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
- 1 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

```
1 racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.110
```

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。

```
1 racadm config -f myrac.cfg
```

配置或重新配置 iDRAC。`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。要在文件中包括密码, 必须手工输入。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` 子命令允许用户分别检索 iDRAC 配置参数, 或者检索所有 iDRAC 配置组并保存到文件中。

输入

表 A-4 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-4. `getconfig` 子命令选项

选项	说明
<code>-f</code>	<code>-f <文件名></code> 选项会指示 <code>getconfig</code> 将整个 iDRAC 配置写入配置文件。此文件可随后用于通过 <code>config</code> 子命令进行批配置操作。 注： <code>-f</code> 选项不会为 <code>cfglpmiPet</code> 和 <code>cfglpmiPef</code> 组创建条目。必须至少设置一个陷阱目标以将 <code>cfglpmiPet</code> 组捕获到文件中。
<code>-g</code>	<code>-g <组名></code> ，或组，选项可以用于显示单个组的配置。组名为 <code>racadm.cfg</code> 文件中所使用的组的名称。如果组为索引组，则应使用 <code>-i</code> 选项。
<code>-h</code>	<code>-h</code> 或 <code>help</code> 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。
<code>-i</code>	<code>-i <索引></code> （或索引选项）只对索引组有效，可用于指定唯一组。如果没有指定 <code>-i <索引></code> ，将对组采用值 1，这些组是具有多个条目的表。索引由索引值指定，不由命名的值指定。
<code>-o</code>	<code>-o <对象名></code> ，或对象，选项指定在查询中使用的对象名称。此选项可与 <code>-g</code> 选项一起使用。
<code>-u</code>	<code>-u <用户名></code> ，或用户名，选项可用于显示指定用户的配置。 <code><用户名></code> 选项为该用户的登录名称。
<code>-v</code>	<code>-v</code> 或详情选项显示所显示属性的其它详情，并与 <code>-g</code> 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：

- 1 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
- 1 `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

```
1 racadm getconfig -g cfgLanNetworking
   显示组 cfgLanNetworking 中包含的所有配置属性（对象）。

1 racadm getconfig -f myrac.cfg
   将所有组配置对象从 iDRAC 保存到 myrac.cfg。

1 racadm getconfig -h
   显示 iDRAC 上可用配置组的列表。

1 racadm getconfig -u root
   显示用户命名为 root 的配置属性。

1 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

- 1 本地 RACADM

getssninfo

[表 A-5](#) 说明了 `getssninfo` 子命令。

表 A-5. getssninfo 子命令

子命令	定义
<code>getssninfo</code>	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 iDRAC 的用户的列表。摘要信息提供了以下信息：

- 1 "Username" (用户名)
- 1 "IP address" (IP 地址) (如果可用)
- 1 "Session type" (会话类型) (例如, SSH 或远程登录)
- 1 "Consoles in use" (使用的控制台) (例如, Virtual Media 或 Virtual KVM)

支持的接口

- 1 本地 RACADM

输入

[表 A-6](#) 说明了 `getssninfo` 子命令选项。

表 A-6. getssninfo 子命令选项

选项	说明
<code>-A</code>	<code>-A</code> 选项可取消打印数据标头。
<code>-u</code>	<code>-u <用户名></code> 用户名选项将打印输出限制为只打印所给用户名的详细会话记录。如果将 "*" 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

```
1 racadm getssninfo
```

[表 A-7](#) 提供了一个从 `racadm getssninfo` 命令输出的示例。

表 A-7. getssninfo 子命令输出示例

用户	IP 地址	类型	控制台
root	192.168.0.10	Telnet	Virtual KVM

```
1 racadm getssninfo -A
```

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

```
1 racadm getssninfo -A -u *  
  
"root" "143.166.174.19" "Telnet" "NONE"  
  
1 "bob" "143.166.174.19" "GUI" "NONE"
```

getsysinfo

[表 A-8](#) 说明了 `racadm getsysinfo` 子命令。

表 A-8. getsysinfo

命令	定义
<code>getsysinfo</code>	显示 iDRAC 信息、系统信息和监护程序状况信息。

提要

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

说明

`getsysinfo` 子命令显示了有关 iDRAC、Managed Server 和监护程序配置的信息。

支持的接口

```
1 本地 RACADM
```

输入

[表 A-9](#) 说明了 `getsysinfo` 子命令选项。

表 A-9. getsysinfo 子命令选项

选项	说明
<code>-d</code>	显示 iDRAC 信息。
<code>-s</code>	显示系统信息
<code>-w</code>	显示监督信息
<code>-A</code>	消除打印页眉/标签。

输出

`getsysinfo` 子命令显示了有关 iDRAC、Managed Server 和监护程序配置的信息。

示例输出

```
RAC Information:  
RAC Date/Time           = Wed Aug 22 20:01:33 2007  
Firmware Version        = 0.32  
Firmware Build          = 13661  
Last Firmware Update    = Mon Aug 20 08:09:36 2007  
  
Hardware Version         = NA  
Current IP Address       = 192.168.0.120  
Current IP Gateway       = 192.168.0.1  
Current IP Netmask       = 255.255.255.0  
DHCP Enabled            = 1  
MAC Address              = 00:14:22:18:cd:f9  
Current DNS Server 1    = 10.32.60.4
```

```
Current DNS Server 2 = 10.32.60.5
DNS Servers from DHCP = 1
Register DNS RAC Name = 1
DNS RAC Name = iDRAC-783932693338
Current DNS Domain = us.dell.com
```

```
System Information:
System Model = PowerEdge M600
System BIOS Version = 0.2.1
BMC Firmware Version = 0.32
Service Tag = 48192
Host Name = dell-x92i38xc2n
OS Name =
Power Status = OFF
```

```
Watchdog Information:
Recovery Action = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

示例

```
l racadm getsysinfo -A -s

"System Information:" ("系统信息") "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"

l racadm getsysinfo -w -s

System Information:
System Model = PowerEdge M600
System BIOS Version = 0.2.1
BMC Firmware Version = 0.32
Service Tag = 48192
Host Name = dell-x92i38xc2n
OS Name =
Power Status = ON

Watchdog Information:
Recovery Action = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

限制

只有 managed server 上装有 Dell OpenManage 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 server 上没有安装 OpenManage，这些字段将会为空白或显示错误的信息。

getractive

[表 A-10](#) 说明了 `getractive` 子命令。

表 A-10. getractive

子命令	定义
<code>getractive</code>	显示 Remote Access Controller 的当前时间。

提要

```
racadm getractive [-d]
```

说明

如果不带选项，`getractive` 子命令会以通用可读格式显示时间。

使用 `-d` 选项时，`getractive` 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

getractive 子命令将输出显示在一行上。

示例输出

```
racadm getractive
Thu Dec 8 20:15:26 2005
racadm getractive -d
20071208201542.000000
```

支持的接口

- 1 本地 RACADM
-

setniccfg

[表 A-11](#) 说明了 setniccfg 子命令。

表 A-11. setniccfg

子命令	定义
setniccfg	设置控制器的 IP 配置。

提要

```
racadm setniccfg -d
racadm setniccfg -s [<ip 地址> <网络掩码> <网关>]
racadm setniccfg -o [<ip 地址><网络掩码><网关>]
```

说明

setniccfg 子命令设置 iDRAC IP 地址。

- 1 -d 选项为 NIC 启用 DHCP（默认是启用 DHCP）。
- 1 -s 选项启用静态 IP 设置。IP 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。<ip 地址>、<网络掩码> 和 <网关> 必须键入为点分隔的字符串。

```
racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
```

- 1 -o 选项完全禁用 NIC。<ip 地址>、<网络掩码>和<网关>必须键入为圆点分隔的字符串。

```
racadm setniccfg -o 192.168.0.120 255.255.255.0 192.168.0.1
```

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

- 1 本地 RACADM
-

getniccfg

[表 A-12](#) 说明 `getniccfg` 子命令。

表 A-12. getniccfg

子命令	定义
<code>getniccfg</code>	显示 iDRAC 的当前 IP 配置。

提要

```
racadm getniccfg
```

说明

`getniccfg` 子命令显示当前 NIC 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      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway         = 192.168.0.1
```

支持的接口

- 1 本地 RACADM
-

getsvctag

[表 A-13](#) 说明了 `getsvctag` 子命令。

表 A-13. getsvctag

子命令	定义
<code>getsvctag</code>	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

1 本地 RACADM

racreset

[表 A-14](#) 说明了 `racreset` 子命令。

表 A-14. racreset

子命令	定义
<code>racreset</code>	重置 iDRAC。

 **注意：** 发出 `racreset` 子命令后，iDRAC 可能需要长达一分钟来返回可用状态。

提要

```
racadm racreset
```

说明

`racreset` 子命令发出对 iDRAC 的重置。重置事件会写入 iDRAC 日志。

示例

```
1 racadm racreset
   启动 iDRAC 软重置序列。
```

支持的接口

1 本地 RACADM

racresetcfg

[表 A-15](#) 说明了 `racresetcfg` 子命令。

表 A-15. racresetcfg

子命令	定义
<code>racresetcfg</code>	将全部 RAC 配置重置为工厂默认值。

提要

```
racadm racresetcfg
```

支持的接口

1 本地 RACADM

说明

`racresetcfg` 命令会删除所有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 iDRAC 恢复为默认设置。



注意： 此命令会删除当前 iDRAC 配置并将 iDRAC 配置重设为默认设置。重设后，默认名称和密码分别为 `root` 和 `calvin`，而 IP 地址为 `192.168.0.120` 加上服务器在机箱中所在的插槽号。

serveraction

表 A-16 说明了 `serveraction` 子命令。

表 A-16. `serveraction`

子命令	定义
<code>serveraction</code>	对 Managed Server 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-17 说明了 `serveraction` 电源控制选项。

表 A-17. `serveraction` 子命令选项

字符串	定义
<code><操作></code>	指定操作。以下为 <code><操作></code> 字符串的选项： <ul style="list-style-type: none">1 <code>powerdown</code> — 关闭 Managed Server 电源。1 <code>powerup</code> — 打开 Managed Server 电源。1 <code>powercycle</code> — 在 Managed Server 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后再打开系统电源。1 <code>powerstatus</code> — 显示服务器的当前电源状况（"ON"（开）或"OFF"（关））1 <code>hardreset</code> — 在 Managed Server 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

- 1 本地 RACADM

getraclog

表 A-18 说明了 `racadm getraclog` 命令。

表 A-18. `getraclog`

命令	定义
<code>getraclog -i</code>	显示 iDRAC 日志中的条目数。
<code>getraclog</code>	显示 iDRAC 日志条目。

提要

```
racadm gettraclog -i
```

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

说明

`gettraclog -i` 命令显示 iDRAC 日志中的条目数。

 **注：** 如果没有提供选项，将显示整个日志。

以下选项允许 `gettraclog` 命令读取条目：

表 A-19. gettraclog 子命令选项

选项	说明
-A	显示不带页眉或标签的输出。
-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 <code>more</code> 命令）。
-o	以一行显示输出。
-s	指定要显示的起始记录。

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 日午夜开始并一直持续到 managed server 引导。Managed Server 引导后，Managed Server 的系统时间被用于时间戳。

示例输出

```
Record:      1
Date/Time:   Dec 8 08:10:11
Source:      login[433]
Description: root login from 143.166.157.103
```

支持的接口

- 1 本地 RACADM
-

clrraclog

提要

```
racadm clrraclog
```

说明

`clrraclog` 子命令会从 iDRAC 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

[表 A-20](#) 说明了 `getsel` 命令。

表 A-20. getsel

--	--

命令	定义
<code>getsel -i</code>	显示系统事件日志中的条目数。
<code>getsel</code>	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 日志中的条目数。

以下 `getsel` 选项（不含 `-i` 选项）用于读取条目。

 **注：** 如果没有指定参数，将显示整个日志。

表 A-21. `getsel` 子命令选项

选项	说明
<code>-A</code>	指定不带页眉或标签显示输出。
<code>-c</code>	提供要被返回的最大条目数。
<code>-o</code>	以一行显示输出。
<code>-s</code>	指定要显示的起始记录。
<code>-E</code>	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。
<code>-R</code>	只打印原始数据。
<code>-m</code>	一次显示一屏信息并提示用户继续（类似于 UNIX <code>more</code> 命令）。

输出

默认输出显示有记录号、时间戳、严重性和说明。

例如：

```
Record:      1
Date/Time:  11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

支持的接口

- 1 本地 RACADM

clrsel

提要

```
racadm clrsel
```

说明

`clrsel` 命令会从系统事件日志 (SEL) 删除全部现有的记录。

支持的接口

1 本地 RACADM

gettracelog

[表 A-22](#) 说明了 `gettracelog` 子命令。

表 A-22. `gettracelog`

命令	定义
<code>gettracelog -i</code>	显示 iDRAC 跟踪日志中的条目数。
<code>gettracelog</code>	显示 iDRAC 跟踪日志。

提要

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c count] [-s startrecord] [-m]
```

说明

`gettracelog` (不带 `-i` 选项) 命令读取条目。以下 `gettracelog` 条目用于读取条目:

表 A-23. `gettracelog` 子命令选项

选项	说明
<code>-i</code>	显示 iDRAC 跟踪日志中的条目数。
<code>-m</code>	一次显示一屏信息并提示用户继续 (类似于 UNIX <code>more</code> 命令)。
<code>-o</code>	以一行显示输出。
<code>-c</code>	指定要显示的记录数。
<code>-s</code>	指定要显示的起始记录
<code>-A</code>	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 日午夜开始并一直持续到 managed system 引导。Managed System 引导后, Managed System 的系统时间用于时间戳。

例如:

```
Record: 1
```

```
Date/Time: Dec 8 08:21:30
```

```
Source: ssmgrd[175]
```

```
Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

支持的接口

1 本地 RACADM

sslcsrgen

[表 A-24](#) 说明了 `sslcsrgen` 子命令。

表 A-24. sslcsrgen

子命令	说明
sslcsrgen	从 RAC 生成并下载 SSL 认证签名请求 (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 可用于创建自定义 SSL 认证以在 RAC 上进行 SSL 事务处理。

选项

[表 A-25](#) 说明了 sslcsrgen 子命令选项。

表 A-25. sslcsrgen 子命令选项

选项	说明
-g	生成新的 CSR。
-s	返回 CSR 生成进程的状况（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况代码之一：

- 1 CSR 成功生成。
- 1 CSR 不存在。
- 1 CSR 生成正在进行。

 **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

- 1 本地 RACADM

sslcertupload

[表 A-26](#) 说明了 sslcertupload 子命令。

表 A-26. sslcertupload

子命令	说明
sslcertupload	

子命令	说明
sslcertupload	从客户端到 iDRAC 上载自定义 SSL 服务器或 CA 认证。

提要

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

选项

[表 A-27](#) 说明了 `sslcertupload` 子命令选项。

表 A-27. sslcertupload 子命令选项

选项	说明
-t	指定要上载的认证类型，CA 认证或服务器认证。 1 = 服务器认证 2 = CA 认证
-f	指定要上载的认证文件名。如果没有指定文件，将会选择当前目录中的 <code>sslcert</code> 文件。

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

示例

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

支持的接口

- 1 本地 RACADM

sslcertdownload

[表 A-28](#) 说明了 `sslcertdownload` 子命令。

表 A-28. sslcertdownload

子命令	说明
sslcertdownload	从 RAC 将 SSL 认证下载到客户的文件系统。

提要

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

选项

[表 A-29](#) 说明了 `sslcertdownload` 子命令选项。

表 A-29. sslcertdownload 子命令选项

选项	说明
-t	指定要下载的认证类型，Microsoft® Active Directory® 认证或服务器认证。 1 = 服务器认证

	2 = Microsoft Active Directory 认证
-f	指定要下载的证书文件名。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。

示例

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

支持的接口

- 1 本地 RACADM

sslcertview

[表 A-30](#) 说明了 **sslcertview** 子命令。

表 A-30. sslcertview

子命令	说明
sslcertview	显示 iDRAC 上存在的 SSL 服务器或 CA 认证。

提要

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

选项

[表 A-31](#) 说明了 **sslcertview** 子命令选项。

表 A-31. sslcertview 子命令选项

选项	说明
-t	指定要查看的认证类型，Microsoft Active Directory 认证或服务器认证。 1 = 服务器认证 2 = Microsoft Active Directory 认证
-A	不显示标头/标签。

输出示例

```
racadm sslcertview -t 1

Serial Number           : 00

Subject Information:
Country Code (CC)      : US
State (S)              : Texas
Locality (L)           : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)       : iDRAC default certificate

Issuer Information:
Country Code (CC)      : US
State (S)              : Texas
Locality (L)           : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : Remote Access Group
```

```

Common Name (CN)      : iDRAC default certificate
Valid From            : Jul 8 16:21:56 2005 GMT
Valid To              : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

```

```

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT

```

支持的接口

- 1 本地 RACADM

testemail

[表 A-32](#) 说明了 `testemail` 子命令。

表 A-32. testemail 配置

子命令	说明
testemail	检测 iDRAC 的电子邮件警报功能。

提要

```
racadm testemail -i <索引>
```

说明

从 iDRAC 向指定目标发送检测电子邮件。

在执行 `testemail` 命令前，确保在 RACADM [cfgEmailAlert](#) 组中指定的索引已被启用并进行了正确的配置。[表 A-33](#) 提供了 `cfgEmailAlert` 组命令示例。

表 A-33. testemail 配置

措施	命令
启用警报	<code>racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1</code>
设置目标电子邮件地址	<code>racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com</code>
设置要发送到目标电子邮件地址的自定义消息	<code>racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"</code>
确保 SNMP IP 地址配置正确	<code>racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr -i 192.168.0.152</code>
查看当前电子邮件警报设置	<code>racadm getConfig -g cfgEmailAlert -i <索引></code>
	其中 <索引> 是一个 1 到 4 之间的数字

选项

[表 A-34](#) 说明了 `testemail` 子命令选项。

表 A-34. testemail 子命令选项

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

- 1 本地 RACADM
-

testtrap

表 A-35 说明了 testtrap 子命令。

表 A-35. testtrap

子命令	说明
testtrap	检测 iDRAC 的 SNMP 陷阱警报功能。

提要

```
racadm testtrap -i <索引>
```

说明

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

执行 testtrap 子命令前，确保 RACADM [cfgIpmiPet](#) 组中的指定索引正确配置。

表 A-36 提供了 [cfgIpmiPet](#) 组的列表和相关命令。

表 A-36. cfg 电子邮件警报命令

措施	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-37 说明了 testtrap 子命令选项。

表 A-37. 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

- 1 本地 RACADM
-

[目录](#)

[目录](#)

iDRAC 属性数据库组和对象定义

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [可显示字符](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgIpmiSol](#)
- [cfgIpmiLan](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)

iDRAC 属性数据库包含 iDRAC 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 iDRAC。以下部分说明各个对象并指出对象是否可读、可写或可以读写。

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：

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

idRacInfo

该组包含显示参数以提供有关所查询 iDRAC 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

RAC 类型的文本描述。

idRacVersionInfo（只读）

有效值

字符串，最多 63 个 ASCII 字符。

默认值

1.0

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 RAC 固件版本。例如，"05.12.06"。

说明

包含当前产品版本的字符串。

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)

默认值

8

说明

将远程访问控制器类型标识为 iDRAC。

cfgLanNetworking

该组包含的参数用于配置 iDRAC NIC。

该组允许有一个实例。该组中的所有对象均需重置 iDRAC NIC，这会导致短暂连接中断。更改 iDRAC 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。

cfgDNSDomainNameFromDHCP (读/写)

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定 iDRAC DNS 域名应从网络 DHCP 服务器分配。

cfgDNSDomainName (读/写)

有效值

字符串，最多 250 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

""

说明

DNS 域名。此参数只有在 `cfgDNSDomainNameFromDHCP` 设置为 0 (FALSE) 时才有效。

cfgDNSRacName (读/写)

有效值

字符串，最多 63 个 ASCII 字符。必须至少一个字符为字母。

 **注：** 有些 DNS 服务器只注册 31 个或更少字符的名称。

默认值

rac-服务标签

说明

显示 RAC 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 iDRAC 名称。

cfgDNSServersFromDHCP (读/写)

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定 DNS 服务器 IP 地址应从网络上的 DHCP 服务器分配。

cfgDNSServer1 (读/写)

有效值

表示有效 IP 地址的字符串。例如：192.168.0.20。

说明

指定 DNS 服务器 1 的 IP 地址。此属性只有在 `cfgDNSServersFromDHCP` 设置为 0 (FALSE) 时才有效。

 **注：** 在交换地址期间，`cfgDNSServer1` 和 `cfgDNSServer2` 可以设置为相同的值。

cfgDNSServer2（读/写）

有效值

表示有效 IP 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 IP 地址。此参数只有在 `cfgDNSServersFromDHCP` 设置为 0 (FALSE) 时才有效。

 **注：** 在交换地址期间，`cfgDNSServer1` 和 `cfgDNSServer2` 可以设置为相同的值。

cfgNicEnable（读/写）

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC 网络接口控制器。如果 NIC 已禁用，到 iDRAC 的远程网络接口将不再可访问，并且 iDRAC 将只能通过本地 RACADM 接口使用。

cfgNicIpAddress（读/写）

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

有效值

表示有效 IP 地址的字符串。例如：192.168.0.20。

默认值

192.168.0.*n*

其中 *n* 是 120 加上服务器插槽号。

说明

指定要分配给 RAC 的静态 IP 地址。此属性只有在 `cfgNicUseDhcp` 设置为 0 (FALSE) 时才有效。

cfgNicNetmask (读/写)

 **注：** 此参数只有在 `cfgNicUseDhcp` 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 iDRAC IP 地址静态分配的子网掩码。此属性只有在 `cfgNicUseDhcp` 设置为 0 (FALSE) 时才有效。

cfgNicGateway (读/写)

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

有效值

表示有效网关 IP 地址的字符串。例如：192.168.0.1。

默认值

192.168.0.1

说明

用于 RAC IP 地址静态分配的网关 IP 地址。此属性只有在 `cfgNicUseDhcp` 设置为 0 (FALSE) 时才有效。

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 iDRAC IP 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 iDRAC IP 地址、子网掩码和网关。如果此属性设置为 0 (FALSE)，则会从 `cfgNicIpAddress`、`cfgNicNetmask` 和 `cfgNicGateway` 属性分配静态 IP 地址、子网掩码和网关。

cfgNicMacAddress (只读)

有效值

表示 RAC NIC MAC 地址的字符串。

默认值

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

说明

iDRAC NIC MAC 地址。

cfgUserAdmin

此组提供了有关那些可通过可用远程接口访问 RAC 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。

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

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-1](#) 说明了可以组合创建位掩码的用户权限位值。

表 B-1. 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
配置用户	0x0000004
清除日志	0x0000008
执行服务器控制命令	0x0000010
访问控制台重定向	0x0000020
访问虚拟介质	0x0000040
检测警报	0x0000080
执行调试命令	0x0000100

示例

[表 B-2](#) 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-2. 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。	0x0000000
用户只能登录到 iDRAC 并查看 iDRAC 和服务器配置信息。	0x0000001
用户可以登录到 iDRAC 并更改配置。	0x0000001 + 0x0000002 = 0x0000003
用户可以登录到 iDRAC、访问虚拟介质和访问控制台重定向。	0x0000001 + 0x0000040 + 0x0000080 = 0x00000C1

cfgUserAdminUserName (读/写)

有效值

字符串。最大长度 = 16。

默认值

""

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。您不能更改名称，而必须删除名称后再重新创建。字符串必须包含 / (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

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用一个用户。

cfgUserAdminSolEnable

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 LAN 上串行 (SOL) 用户访问。

cfgEmailAlert

此组包含用来配置 RAC 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

此参数根据现有实例设置。

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

为电子邮件警报指定目标电子邮件地址。例如，user1@company.com。

cfgEmailAlertAddress

有效值

电子邮件地址格式，最大长度为 64 个 ASCII 字符。

默认值

""

说明

警报源的电子邮件地址。

cfgEmailAlertCustomMsg

有效值

字符串。最大长度 = 32。

默认值

""

说明

指定随警报发出的自定义消息。

cfgSessionManagement

此组包含的参数用于配置可以连接到 iDRAC 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。

cfgSsnMgtConsRedirMaxSessions (读/写)

有效值

1 - 2

默认值

2

说明

指定 iDRAC 上允许的最大控制台重定向会话数。

cfgSsnMgtWebserverTimeout (读/写)

有效值

60 - 1920

默认值

300

说明

定义 Web Server 超时。此属性设置允许连接保持闲置（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以使新设置生效）。

过期的 Web Server 会话注销当前会话。

cfgSsnMgtSshIdleTimeout (读/写)

有效值

0 (无超时)
60 - 1920

默认值

300

说明

定义 Secure Shell 闲置超时。此属性设置允许连接保持闲置（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以使新设置生效）。

只有在按下 <"Enter" (输入) > 后，过期的 SSH 会话才会显示以下错误信息：

Warning: Session no longer valid, may have timed out (警告：会话不再有效，可能已超时)

出现此信息后，系统会返回到生成 SSH 会话的 shell。

cfgSsnMgtTelnetIdleTimeout (读取/写入)

有效值

0 (无超时)

60 - 1920

默认值

300

说明

定义远程登录空闲超时。此属性设置允许连接保持闲置（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以使新设置生效）。

只有按下 <"Enter"（输入）>，过期的远程登录会话才会显示以下错误信息：

Warning: Session no longer valid, may have timed out (警告：会话不再有效，可能已超时)

出现此信息后，系统会返回到生成远程登录会话的 shell。

cfgSerial

此组包含 iDRAC 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。

cfgSerialSshEnable (读/写)

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 iDRAC 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 iDRAC 上的远程登录控制台接口。

cfgRacTuning

此组用于配置各种 iDRAC 配置属性，比如有效端口和安全端口限制。

cfgRacTuneHttpPort (读/写)

有效值

10 - 65535

默认值

80

说明

指定用来与 RAC 进行 HTTP 网络通信的端口号。

cfgRacTuneHttpsPort (读/写)

有效值

10 - 65535

默认值

443

说明

指定用来与 iDRAC 进行 HTTPS 网络通信的端口号。

cfgRacTuneIpRangeEnable

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC 的 IP 地址范围验证功能。

cfgRacTuneIpRangeAddr

有效值

字符串，IP 地址格式。例如，192.168.0.44。

默认值

192.168.1.1

说明

指定可接受的 IP 地址位模式，其位置由范围掩码属性 (cfgRacTuneIpRangeMask) 中的各个 1 来确定。

cfgRacTuneIpRangeMask

有效值

带有左对齐位的标准 IP 掩码值

默认值

255.255.255.0

说明

字符串，IP 地址格式。例如：255.255.255.0

cfgRacTuneIpBIKEnable

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 的 IP 地址阻塞功能。

cfgRacTuneIpBIKFailCount

有效值

2 - 16

默认值

5

说明

在从 IP 地址进行的登录尝试被拒绝前，在窗口 (cfgRacTuneIpBlkFailWindow) 内发生的最大登录故障数。

cfgRacTuneIpBlkFailWindow

有效值

10 – 65535

默认值

60

说明

定义计数失败尝试的时间长度（秒）。当达到失败尝试的限制数后，将不计失败。

cfgRacTuneIpBlkPenaltyTime

有效值

10 – 65535

默认值

300

说明

定义具有过多失败的来自某 IP 地址的会话请求被拒绝的时间长度（秒）。

cfgRacTuneSshPort（读/写）

有效值

1 – 65535

默认值

22

说明

指定用于 iDRAC 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 iDRAC telnet 接口的端口号。

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。

cfgRacTuneConRedirPort (读/写)

有效值

1 - 65535

默认值

5900

说明

指定在与 iDRAC 进行控制台重定向活动期间键盘和鼠标通信要使用的端口。

cfgRacTuneConRedirVideoPort (读/写)

有效值

1 - 65535

默认值

5901

说明

指定在与 iDRAC 进行控制台重定向活动期间视频通信使用的端口。

 **注：** 此对象在变为活动前要求 iDRAC 重置。

cfgRacTuneAsrEnable (读/写)

有效值

0 (FALSE)

1 (TRUE)

默认值

0

说明

启用或禁用 iDRAC 的上次崩溃屏幕捕获功能。

 **注：** 此对象在变为活动前要求 iDRAC 重置。

cfgRacTuneWebserverEnable (读/写)

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用和禁用 iDRAC Web Server。如果禁用此属性，将无法使用客户 Web 浏览器访问 iDRAC。此属性对于 telnet/SSH 或本地 RACADM 接口无效。

cfgRacTuneLocalServerVideo (读/写)

有效值

1 (启用)

0 (禁用)

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（启用）

1（禁用）

默认值

0

说明

禁用写入访问 iDRAC 配置数据。默认启用访问。

 **注：** 可以使用本地 RACADM 或 iDRAC Web 界面禁用访问，但禁用后，只有通过 iDRAC Web 界面才能重新启用访问。

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（读/写）

有效值

字符串。最大长度 = 255。

默认值

...

说明

受管服务器的主机名。

ifcRacMnOsOsName（读/写）

有效值

字符串。最大长度 = 255。

默认值

...

说明

受管服务器的操作系统名称。

cfgRacSecurity

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

请参阅 RACADM [sslcsrgen](#) 子命令详情了解有关生成认证签名请求的详情。

cfgSecCsrCommonName (读取/写入)

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 常用名 (CN)。

cfgSecCsrOrganizationName (读取/写入)

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 组织名称 (O)。

cfgSecCsrOrganizationUnit (读取/写入)

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 组织部门 (OU)。

cfgSecCsrLocalityName (读取/写入)

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 地点 (L)。

cfgSecCsrStateName (读取/写入)

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 州/省名称 (S)。

cfgSecCsrCountryCode (读取/写入)

有效值

字符串。最大长度 = 2。

默认值

""

说明

指定 CSR 国家 (地区) 代码 (CC)

cfgSecCsrEmailAddr (读取/写入)

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 电子邮件地址。

cfgSecCsrKeySize (读取/写入)

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 iDRAC 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

1 (TRUE)

0 (FALSE)

默认值

1

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。当连接设备时，可以随后使用 iDRAC 基于 Web 的界面或 CLI 远程连接到虚拟设备。将此对象设置为 0 会造成设备与 USB 总线分离。

 **注：** 必须重新启动系统才能启用所有更改。

cfgVirAtapiSrvPort (读/写)

有效值

1 - 65535

默认值

3668

说明

指定 iDRAC 加密虚拟介质连接所用的端口号。

cfgVirAtapiSrvPortSsl (读/写)

有效值

任何介于 0 和 65535 十进制数的未用端口号。

默认值

3670

说明

设置 SSL 虚拟介质连接所用的端口。

cfgVirMediaBootOnce (读/写)

有效值

1 (已启用)

0 (已禁用)

默认值

0

说明

启用或禁用 iDRAC 的虚拟介质一次引导功能。如果在主机服务器重新引导时已启用此属性，此功能会尝试从虚拟介质设备引导—如果设备中装有相应介质。

cfgFloppyEmulation (读/写)

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盘符 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 操作系统将会分配盘符 A: 或 B:。

cfgActiveDirectory

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

cfgADracDomain (读/写)

有效值

任何不带空格的可打印文本字符串。长度限制为 254 个字符。

默认值

""

说明

iDRAC 所在的 Active Directory 域。

cfgADracName (读/写)

有效值

任何不带空格的可打印文本字符串。长度限制为 254 个字符。

默认值

""

说明

Active Directory 目录林中记录的 iDRAC 的名称。

cfgADEnable (读/写)

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 iDRAC 上的 Active Directory 用户验证。如果此属性已禁用，则会相应使用本地 iDRAC 验证进行用户登录。

cfgADAuthTimeout (读/写)

 **注：** 要修改此属性，必须具有“Configure iDRAC”（配置 iDRAC）权限。

有效值

15 – 300

默认值

120

说明

指定在超时前等待 Active Directory 验证请求完成的秒数。

cfgADRootDomain (读/写)

有效值

任何不带空格的可打印文本字符串。长度限制为 254 个字符。

默认值

""

说明

域目录林的根域。

cfgADSpecifyServerEnable (读/写)

有效值

1 或 0 (True 或 False)。

默认值

0

说明

1 (True) 允许指定 LDAP 或全局编目服务器。0 (False) 禁用此选项。

cfgADDomainController (读/写)

有效的 IP 地址或完全限定域名 (FQDN)

默认值

无默认值

说明

iDRAC 使用指定的值搜索 LDAP 服务器查找用户名。

cfgADGlobalCatalog (读/写)

有效值

有效的 IP 地址或完全限定域名 (FQDN)

默认值

无默认值

说明

iDRAC 使用指定的值搜索全局编录服务器查找用户名。

cfgADType (读/写)

有效值

1 = 启用 Active Directory 扩展架构。

2 = 启用 Active Directory 标准架构。

默认值

1 = 扩展架构

说明

确定与 Active Directory 一起使用的架构类型。

cfgStandardSchema

该组包含的参数用于配置 Active Directory 标准架构设置。

cfgSSADRoleGroupIndex (只读)

有效值

从 1 到 5 的整数。

说明

Active Directory 中记录的角色组索引。

cfgSSADRoleGroupName (读/写)

有效值

任何不带空格的可打印文本字符串。长度限制为 254 个字符。

默认值

(空白)

说明

Active Directory 中记录的角色组名称。

cfgSSADRoleGroupDomain (读/写)

有效值

任何不带空格的可打印文本字符串。长度限制为 254 个字符。

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-3](#) 中的位掩码数字为角色组设置基于角色的权限。

表 B-3. 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
配置用户	0x00000004
清除日志	0x00000008
执行服务器控制命令	0x00000010

访问控制台重定向	0x00000020
访问虚拟介质	0x00000040
检测警报	0x00000080
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

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 SOL。

cfgIpmiSolBaudRate (读/写)

有效值

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 存取所需的最小权限级别。

cfgIpmiSolAccumulateInterval (读/写)

有效值

1– 255。

默认值

10

说明

指定发送部分 SOL 字符数据包前 iDRAC 一般等待的时间。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

0 (FALSE)

1 (TRUE)

默认值

0

说明

启用或禁用 LAN 上 IPMI 接口。

cfgIpmiLanPrivLimit (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 访问所需的最大权限。

cfgIpmiLanAlertEnable (读/写)

有效值

- 0 (FALSE)
- 1 (TRUE)

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

不带空格的 0 到 20 字符的十六进制字符串。

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。

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。最大长度 = 255。

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（只读）

有效值

1 - 17

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

- 0 (FALSE)
- 1 (TRUE)

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 (读/写)

有效值

1 - 4

默认值

相应的索引值。

说明

与陷阱相应的索引的唯一标识符。

cfgIpmiPetAlertDestIpAddr (读/写)

有效值

表示有效 IP 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 IP 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

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用特定陷阱。

[目录](#)

iDRAC SMCLP 属性数据库

Integrated Dell™ Remote Access Controller固件版本1.2
用户指南

- [/system1/sp1/account<1-16>](#)
- [/system1/sp1/enetport1/*](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse_ndpt1](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse_ndpt1/remotesap1](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse_ndpt1/remotesap2](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1](#)
- [/system1/sp1/group<1-5>](#)
- [/system1/sp1/oemdelld_adservice1](#)
- [/system1/sp1/oemdelld_racsecurity1](#)
- [/system1/sp1/oemdelld_ssl1](#)
- [/system1/sp1/oemdelld_vmsservice1](#)
- [/system1/sp1/oemdelld_vmsservice1/tcpendpt1](#)

/system1/sp1/account<1-16>

此目标提供了有关那些可通过可用远程接口访问 RAC 的本地用户的配置信息。允许多达 16 个用户组实例。每个实例 <1-16> 代表单个本地用户的配置。

userid (只读)

有效值

1-16

默认值

取决于访问的帐户实例。

说明

指定实例 ID 或本地用户 ID。

username (读/写)

有效值

字符串。最大长度 = 16

默认值

""

说明

包含此帐户本地用户姓名的文本字符串。字符串不能包含正斜线 (/)、句号 (.)、at 符号 (@) 或引号 (")。删除此帐户即可删除该用户。(删除帐户 <1-16>)。

 **注：** 此属性值必须在用户名中唯一。

oemdelld_ipmilsanprivileges (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。

密码 (只写)

有效值

长度在 4 到 20 个字符之间的文本字符串。

默认值

""

说明

保存此本地用户的密码。写入此属性之后，用户密码将被加密，不能查看或显示。

enabledstate (读/写)

有效值

0 (已禁用)

1 (已启用)

默认值

0

说明

帮助启用或禁用个人用户。

solenabled (读/写)

有效值

0 (已禁用)

1 (已启用)

默认值

0

说明

启用或禁用 LAN 上串行 (SOL) 用户访问。

oemdel_l_extendedprivileges (读/写)

有效值

0x00000000 到 0x000001ff

默认值

0x00000000

说明

指定此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 C-1](#) 说明了可以组合创建位掩码的用户权限位值。

表 C-1. 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
配置用户	0x0000004
清除日志	0x0000008
执行服务器控制命令	0x0000010
访问控制台重定向	0x0000020
访问虚拟介质	0x0000040
检测警报	0x0000080
执行调试命令	0x0000100

示例

[表 C-2](#) 提供了具有一项或多项权限的用户的权限位掩码示例。

表 C-2. 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 RAC、访问虚拟介质和访问控制台重定向。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

/system1/sp1/enetport1/*

该组包含的参数用于配置 iDRAC NIC。该组允许有一个实例。该组中的所有对象均需要重设 iDRAC NIC，这会导致短暂的连接中断。更改 iDRAC 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。

macaddress (只读)

有效值

表示 RAC NIC MAC 地址的字符串。

默认值

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

说明

保存 iDRAC NIC MAC 地址。

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_nicenable (读/写)

有效值

0 (已禁用)

1 (已启用)

默认值

0

说明

启用或禁用 iDRAC 网络接口控制器。如果禁用 NIC，则远程网络接口无法连接到 iDRAC，只有通过本地 RACADM 界面才能显示 iDRAC 的可用情况。

ipaddress (读/写)

有效值

表示有效 IP 地址的字符串。例如：192.168.0.20。

默认值

192.168.0.n (其中 n 等于 120 加上服务器插槽编号)

说明

指定要分配给 RAC 的静态 IP 地址。此属性只在 oemdell_usedhcp 设置为 0 (已禁用) 时有效。

subnetmask (读/写)

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 iDRAC IP 地址静态分配的子网掩码。此属性只在 oem Dell_usedhcp 设置为 0（已禁用）时有效。

oem Dell_usedhcp（读/写）

有效值

0（已禁用）

1（已启用）

默认值

0

说明

指定是否使用 DHCP 分配 iDRAC IP 地址。如果此属性设置为 1（已启用），则从网络上的 DHCP 服务器分配 iDRAC IP 地址、子网掩码和网关。如果此属性设置为 0（已禁用），则用户需要手动插入静态 IP 地址、子网掩码和网关增益值。

committed（读/写）

有效值

0（待提交）

1（已提交）

默认值

1

说明

使用户能够更改 IP 地址和/或子网掩码而无需终止当前会话。如果此属性设置为 1（已提交），则 IP 地址和子网掩码有效。更改 IP 地址或子网掩码将自动使该属性变为 0（待提交）。为了使网络设置生效，该属性必须设置为 1。

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1

oem Dell_domainnamefromdhcp（读/写）

有效值

0（已禁用）

1 (已启用)

默认值

0

说明

指定 iDRAC DNS 域名应从网络 DHCP 服务器分配。

oemdelldnsdomainname (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。

默认值

""

说明

保存 DNS 域名。此参数只在 oemdelldomainnamefromdhcp 设置为 0 (已禁用) 时有效。

oemdelldnsregisterrac (读/写)

有效值

0 (未注册)

1 (已注册)

默认值

0

说明

在 DNS 服务器上注册 iDRAC 名称。

oemdelldnsracname (读/写)

有效值

字符串，最多 63 个 ASCII 字符。必须至少一个字符为字母。

 **注：** 有些 DNS 服务器只能注册最多 31 个字符的名称。

默认值

rac-服务标签

说明

显示 RAC 名称，默认情况下是 RAC 服务标签。此参数只在 oemdelldnsregisterrac 设置为 1（已注册）时有效。

oemdelldnsregisterrac（读/写）

有效值

0（已禁用）

1（已启用）

默认值

0

说明

指定 DNS 服务器 IP 地址应从网络上的 DHCP 服务器分配。

`/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1`

dnsserveraddress（读/写）

有效值

表示有效 IP 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 IP 地址。此属性只在 oemdelldnsregisterrac 设置为 0（已禁用）时有效。

`/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap2`

dnsserveraddress（读/写）

有效值

表示有效 IP 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 2 的 IP 地址。此属性只在 oemdelI_serversfromdhcp 设置为 0（已禁用）时有效。

/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1

defaultgatewayaddress（读/写）

有效值

表示有效网关 IP 地址的字符串。例如：192.168.0.1。

默认值

192.168.0.1

说明

用于 RAC IP 地址静态分配的网关 IP 地址。此属性只在 oemdelI_usedhcp 设置为 0（已禁用）时有效。

/system1/sp1/group<1-5>

这些组包含配置 Active Directory 标准模式设置的参数。

oemdelI_groupname（读/写）

有效值

长度最多 254 个字符的任何可打印文本字符串，不包含空格。

默认值

""

说明

保存 Active Directory 目录林中记录的角色组名称。

oemdelI_groupdomain（读/写）

有效值

长度最多 254 个字符的任何可打印文本字符串，不包含空格。

默认值

""

说明

保存角色组所在的 Active Directory 域。

oemdel_l_groupprivilege (读/写)

有效值

0x00000000 到 0x000001ff

默认值

""

说明

使用表 B-3 中的位掩码数字为角色组设置基于角色的权限。

表 C-3. 角色组权限的位掩码

"Role Group" (角色组)	权限位掩码
"Login to iDRAC" (登录到 iDRAC)	0x00000001
"Configure iDRAC" (配置 iDRAC)	0x00000002
配置用户	0x00000004
清除日志	0x00000008
执行服务器控制命令	0x00000010
访问控制台重定向	0x00000020
访问虚拟介质	0x00000040
检测警报	0x00000080
执行调试命令	0x00000100

/system1/sp1/oemdel_l_adservice1

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

enabledstate (读/写)

有效值

0 (已禁用)

1 (已启用)

默认值

0

说明

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

oemdel_l_adracname (读/写)

有效值

长度最多 254 个字符的任何可打印文本字符串，不包含空格。

默认值

""

说明

Active Directory 目录林中记录的 iDRAC 的名称。

oem Dell_adracdomain (读/写)

有效值

长度最多 254 个字符的任何可打印文本字符串，不包含空格。

默认值

""

说明

iDRAC 所在的 Active Directory 域。

oem Dell_adrootdomain (读/写)

有效值

长度最多 254 个字符的任何可打印文本字符串，不包含空格。

默认值

""

说明

域目录林的根域。

oem Dell_timeout (读/写)

有效值

15 - 300

默认值

120

说明

指定在超时前等待 Active Directory 验证请求完成的秒数。

oem Dell_schematype (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 一起使用的架构类型。

oem Dell_adspecifyserverenable (读/写)

有效值

0 (已禁用)

1 (已启用)

默认值

0

说明

使用户能够指定 LDAP 或全局目录服务器。

oem Dell_addomaincontroller (读/写)

有效值

有效的 IP 地址或完全限定域名 (FQDN)。

默认值

""

说明

用户指定的值，iDRAC 使用该值在 LDAP 服务器上搜索用户名。

oemhell_adglobalcatalog (读/写)

有效值

有效的 IP 地址或 FQDN。

默认值

无默认值

说明

用户指定的值，iDRAC 使用该值在全局目录服务器上搜索用户名。

/system1/sp1/oemhell_racsecurity1

此组用于配置与 iDRAC SSL 认证签名请求 (CSR) 功能相关的设置。在从 iDRAC 生成 CSR 前，必须配置此组中的所有属性。

commonname (读/写)

有效值

字符串，最多 254 个字符。

默认值

""

说明

指定 CSR 常用名。

organizationname (读/写)

有效值

字符串，最多 254 个字符。

默认值

""

说明

指定 CSR 组织名称。

oemhell_organizationunit (读/写)

有效值

字符串，最多 254 个字符。

默认值

""

说明

指定 CSR 组织部门。

oemdellocalityname (读/写)

有效值

字符串，最多 254 个字符。

默认值

""

说明

指定 CSR 地点。

oemdelstate (读/写)

有效值

字符串，最多 254 个字符。

默认值

""

说明

指定 CSR 州/省名称。

oemdelcountrycode (读/写)

有效值

字符串，最多 2 个字符。

默认值

""

说明

指定 CSR 国家（地区）代码。

oemdel_emailaddress (读/写)

有效值

字符串，最多 254 个字符。

默认值

""

说明

指定 CSR 电子邮件地址。

oemdel_keysize (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。

/system1/sp1/oemdel_ssl1

包括生成证书签名请求 (CSR) 和查看证书所需的参数。

generate (读/写)

有效值

0 (不生成)

1 (生成)

默认值

0

说明

当设置为 1 时生成 CSR。生成 CSR 之前设置 oem Dell_racsecurity1 目标中的属性。

oem Dell_status (只读)

有效值

未找到 CSR

已生成 CSR

默认值

未找到 CSR

说明

在当前会话过程中，显示发出的前一个生成命令（如果有）的执行状态。

oem Dell_certtype (读/写)

有效值

SSL

AD

CSR

默认值

SSL

说明

指定需要查看的证书类型（AD 或 SSL），并借助于 **generate** 属性帮助生成 CSR。

/system1/sp1/oem Dell_vm service 1

该组包含的参数用于配置 iDRAC 虚拟介质功能。

enabledstate (读/写)

有效值

VMEDIA_DETACH

VMEDIA_ATTACH

VMEDIA_AUTO_ATTACH

默认值

VMEDIA_ATTACH

说明

用于通过 USB 总线将虚拟设备连接到系统，允许服务器识别连接到系统的有效 USB 大容量存储设备。这相当于将本地 USB CDROM/软盘驱动器连接到系统上的 USB 端口。设备连接后，随即可使用 iDRAC Web 界面或 CLI 远程连接到虚拟设备。将此属性设置为 0 会造成设备与 USB 总线分离。

oem Dell_singleboot (读/写)

有效值

0 (已禁用)

1 (已启用)

默认值

0

说明

启用或禁用 iDRAC 的虚拟介质一次引导功能。如果当重新引导主机服务器时已启用此属性，那么服务器将尝试从虚拟介质设备中引导。

oem Dell_floppyemulation (读/写)

有效值

0 (已禁用)

1 (已启用)

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盘符 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 操作系统会分配驱动器号 A: 或 B:

`/system1/sp1/oem Dell_vm service1/tcp end pt1`

port number (读/写)

有效值

1 - 65535

默认值

3668

说明

指定 iDRAC 加密虚拟介质连接所用的端口号。

oemdelI_sslenabled (只读)

有效值

FALSE

默认值

FALSE

说明

表明此端口已禁用 SSL。

portnumber (读/写)

有效值

1 - 65535

默认值

3670

说明

指定 iDRAC 加密虚拟介质连接所用的端口号。

oemdelI_sslenabled (只读)

有效值

TRUE

默认值

TRUE

说明

表明此端口已启用 SSL。

[目录](#)

RACADM 和 SM-CLP 等价

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

表 D-1 列出了 RACADM 组和对象以及它们的位置，SM-SLP 在 SM-CLP MAP 中的等价位置。

表 D-1. RACADM 组/对象和 SM-CLP 等价

RACADM 组/对象	SM-CLP	说明
idRacInfo		
idRacName		字符串，最多 15 个 ASCII 字符。默认： IDRAC 。
idRacProductInfo		字符串，最多 63 个 ASCII 字符。默认： Integrated Dell Remote Access Controller 。
idRacDescriptionInfo		字符串，最多 255 个 ASCII 字符。默认： 此系统组件提供了一套完整的 Dell PowerEdge 服务器远程管理功能
idRacVersionInfo		字符串，最多 63 个 ASCII 字符。默认： 1
idRacBuildInfo		字符串，最多 16 个 ASCII 字符。
idRacType		默认： 8
cfgActiveDirectory	/system1/sp1/oemdel_adservice1	
cfgADEnable	enablestate	0 禁用，1 启用。默认： 0
cfgADRacName	oemdel_adracname	字符串，最多 254 个字符。
cfgADRacDomain	oemdel_adracdomain	字符串，最多 254 个字符。
cfgADRootDomain	oemdel_adrootdomain	字符串，最多 254 个字符。
cfgADAuthTimeout	oemdel_timeout	15 到 300 秒。默认： 120
cfgADType	oemdel_schematype	1 为标准架构，2 为扩展架构。默认： 1
cfgADSpecifyServerEnable	oemdel_adspecifyserverenable	启用时，指定一台 LDAP 或全局编目服务器。 0 禁用，1 启用。默认： 0
cfgADDomainController	oemdel_addomaincontroller	LDAP 搜索中使用的域控制器的 DNS 名称或 IP 地址。
cfgADGlobalCatalog	oemdel_adglobalcatalog	LDAP 搜索中使用的全局编目服务器的 DNS 名称或 IP 地址。
cfgStandardSchema		
cfgSSADRoleGroupIndex	/system1/sp1/group1 至 /system1/sp1/group5	RACADM — 组索引 ID (1-5)。 SM-CLP — 用地址路径选择。
cfgSSADRoleGroupName	oemdel_groupname	字符串，最多 254 个字符。
cfgSSADRoleGroupDomain	oemdel_groupdomain	字符串，最多 254 个字符。
cfgSSADRoleGroupPrivilege	oemdel_groupprivilege	值在 0x00000000 和 0x000001ff 之间的位掩码。
cfgLanNetworking	/system1/sp1/enetport1	
cfgNicMacAddress	macaddress	接口的 MAC 地址。不可编辑。
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicEnable	oemdel_nicenable	0 禁用 NIC，1 启用 NIC。默认： 0
cfgNicUseDHCP	oemdel_usedhcp	0 配置静态网络地址，1 使用 DHCP。默认： 0
cfgNicIpAddress	ipaddress	iDRAC IP 地址。默认： 192.168.0.120 加服务器插槽号。
cfgNicNetmask	subnetmask	iDRAC 网络子网掩码。默认： 255.255.255.0
	committed	当组值更改后， committed 设置为 0 以表示新值尚未保存。设置值为 1 保存新配置。默认： 1

	/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdelldnsdomainname	字符串，最多 250 个 ASCII 字符。必须至少一个字符为字母。
cfgDNSDomainNameFromDHCP	oemdelldnsdomainnamefromdhcp	设置为 1 从 DHCP 获得域名。默认：0
cfgDNSRacName	oemdelldnsracname	字符串，最多 63 个 ASCII 字符。必须至少一个字符为字母。默认：IDRAC- 加 Dell 服务标签。
cfgDNSRegisterRac	oemdelldnsregisterrac	设置为 1 在 DNS 中注册 IDRAC 名称。默认：0
cfgDNSServersFromDHCP	oemdelldnsserversfromdhcp	设置为 1 从 DHCP 获得 DNS 服务器地址。默认：0
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	表示 DNS 服务器 IP 地址的字符串。
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1/remotesap2	
cfgDNSServer2	dnsserveraddresses2	表示 DNS 服务器 IP 地址的字符串。
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	表示默认网关 IP 地址的字符串。默认：192.168.0.1
cfgRacVirtual	/system1/sp1/oemdelldvmservice1	
cfgFloppyEmulation	oemdelldfloppyemulation	设置为 1 启用软盘仿真。默认：0
cfgVirMediaAttached	enabledstate	设置为 1 (RACADM)/ VMEDIA_ATTACH (SM-CLP) 以附加 介质。默认：1 (RACADM)/ VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdelldsingleboot	设置为 1 从所选介质执行下一次引导。默认：0。
	/system1/sp1/oemdelldvmservice1/ tcpendpt1	
	oemdelldsslenabled	如果启用 SSL 用于第一个虚拟介质设备，则设置为 1，否则设置为 0。不可编辑。
cfgVirAtapiSvrPort	portnumber	用于第一个虚拟介质设备的端口。默认：3668
	/system1/sp1/oemdelldvmservice1/ tcpendpt2	
	oemdelldsslenabled	如果启用 SSL 用于第二个虚拟介质设备，则设置为 1，否则设置为 0。不可编辑。
cfgVirAtapiSvrPortSsl	portnumber	用于第二个虚拟介质设备的端口。默认：3670
cfgUserAdmin	/system1/sp1/account1 至 /system1/sp1/account16	
cfgUserAdminEnable	enabledstate	设置为 1 启用用户。默认：0
cfgUserAdminIndex	userid	从 1 到 16 的用户索引。
cfgUserAdminIpmiLanPrivilege	oemdelldipmilanprivileges	2 (用户)、3 (操作员)、4 (管理员) 或 15 (无权限)。默认：4
cfgUserAdminPassword	密码	字符串，最多 20 个 ASCII 字符。
cfgUserAdminPrivilege	oemdelldextendedprivileges	值在 0x00000000 和 0x000001ff 之间的位掩码。默认：0x00000000
cfgUserAdminSolEnable	solenabled	设置为 1 允许用户使用“LAN 上串行”。默认：0
cfgUserAdminUserName	username	字符串，最多 16 个字符。
cfgEmailAlert		
cfgEmailAlertAddress		电子邮件目标地址，最多 64 个字符。
cfgEmailAlertCustomMsg		要在电子邮件中发送的信息，最多 32 个字符。
cfgEmailAlertEnable		设置为 1 启用电子邮件警报。默认：0
cfgEmailAlertIndex		电子邮件警报实例的索引。1 到 4 之间的数。
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		允许的并发控制台重定向会话数 (1 或 2)。默认：2

cfgSsnMgtSshIdleTimeout		SSH 会话超时前空闲的秒数。0 禁用超时或 60-1920 秒。默认: 300
cfgSsnMgtTelnetIdleTimeout		telnet 会话超时前空闲的秒数。0 禁用超时或 60-1920 秒。默认: 300
cfgSsnMgtWebserverTimeout		Web 界面会话超时前空闲的秒数。60 到 1920 秒。默认: 300
cfgRacTuning		
cfgRacTuneConRedirEnable		设置为 1 启用控制台重定向, 0 为禁用。默认: 1
cfgRacTuneConRedirEncrypt 启用		设置为 1 启用控制台重定向网络通信量加密, 0 为禁用。默认: 1
cfgRacTuneConRedirPort		用于控制台重定向的端口。默认: 5900
cfgRacTuneConRedirVideoPort		用于控制台视频重定向的端口。默认: 5901
cfgRacTuneHttpPort		用于 Web 界面 HTTP 的端口。默认: 80
cfgRacTuneHttpsPort		用于安全 Web 界面 HTTPS 的端口。默认: 443
cfgRacTuneIpBlkEnable		设置为 1 启用 IP 阻止。默认: 0
cfgRacTuneIpBlkFailCount		阻止 IP 前计数的失败登录尝试次数 (2 到 16)。默认: 5
cfgRacTuneIpBlkFailWindow		不进行失败登录尝试计数的时间秒数 (10 到 65535)。默认: 60
cfgRacTuneIpBlkPenaltyTime		阻止 IP 保持阻止状态的时间秒数 (10 到 65535)。默认: 300
cfgRacTuneIpRangeAddr		IP 范围筛选器的基本 IP 地址。默认: 192.168.0.1
cfgRacTuneIpRangeEnable		设置为 1 允许 IP 范围筛选。默认: 0
cfgRacTuneIpRangeMask		应用到地址来选择有效 IP 地址的位掩码。默认: 255.255.255.0
cfgRacTuneLocalServerVideo		设置为 1 启用本地 iKVM 控制台。默认: 1
cfgRacTuneSshPort		SSH 服务所用的端口。默认: 22
cfgRacTuneTelnetPort		telnet 服务所用的端口。默认: 23
cfgRacTuneWebserverEnable		设置为 1 启用 iDRAC Web 接口。默认: 1
ifcRacManagedNodeOS		
ifcRacMnOsHostname		受管服务器的主机名。最多 255 个字符的字符串。
ifcRacMnOsOsName		受管服务器的操作系统名称。最多 255 个字符的字符串。
cfgRacSecurity		/system1/sp1/oemdel_l_racsecurity1
cfgRacSecCsrCommonName	commonname	Active Directory 常用名。字符串, 最多 254 个字符。
cfgRacSecCsrCountryCode	oemdel_l_countrycode	Active Directory 国家 (地区) 代码。2 个字符。
cfgRacSecCsrEmailAddr	oemdel_l_emailaddress	用于认证签名请求的电子邮件地址。字符串, 最多 254 个字符。
cfgRacSecCsrKeySize	oemdel_l_keysize	密钥的长度 (512、1024 或 2048)。默认: 1024 。
cfgRacSecCsrLocalityName	oemdel_l_localityname	Active Directory 地点名称。字符串, 最多 254 个字符。
cfgRacSecCsrOrganizationName	organizationname	Active Directory 组织名称。字符串, 最多 254 个字符。
cfgRacSecCsrOrganizationUnit	oemdel_l_organisationunit	Active Directory 组织部门名称。字符串, 最多 254 个字符。
cfgRacSecCsrStateName	oemdel_l_statename	Active Directory 国家名称。字符串, 最多 254 个字符。
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		发送部分"LAN 上串行"数据包前等待的最大毫秒数 (1 到 255)。默认: 10
cfgIpmiSolBaudRate		"LAN 上串行"使用的波特率 (19200, 57600, 115200)。默认: 115200
cfgIpmiSolEnable		设置为 1 启用"LAN 上串行"功能。默认: 0
cfgIpmiSolSendThreshold		发送 SOL 数据前收集的最大字符数 (1 到 255)。默认: 255
cfgIpmiSolMinPrivilege		使用 SOL 所需的最小权限。2 (用户)、3 (操作员) 或 4 (管理员)。默认: 4
cfgIpmiLan		
cfgIpmiEncryptionKey		0 到 40 个十六进制数的字符串。默认: 00
cfgIpmiLanAlertEnable		设置为 1 启用 IPMI LAN 警报。默认: 0
cfgIpmiLanEnable		设置为 1 启用 IPMI over LAN 接口。默认: 0
cfgIpmiPetCommunityName		最多 18 个字符的字符串。默认: public
cfgIpmiPef		
cfgIpmiPefAction		检测到事件时要采取的操作。0 (无)、1 (关机)、2 (重置)、3 (关机后再开机)。

		默认: 0
cfglpmiPefEnable		设置为 1 启用平台事件筛选。默认: 0
cfglpmiPefIndex		平台事件筛选器的索引号。 (1 - 17)
cfglpmiPefName		平台事件的名称, 最多 254 个字符的字符串。不可编辑。
cfglpmiPet		
cfglpmiPetAlertDestIpAddr		平台事件陷阱接收器的 IP 地址。默认: 0.0.0.0
cfglpmiPetAlertEnable		设置为 1 启用平台事件陷阱。默认: 1
cfglpmiPetIndex		平台事件陷阱的索引号 (1-4)。

表 D-2. RACADM 子命令和 SM-CLP 等价

RACADM 子命令	SM-CLP	说明
sslcsrgen -g	set /system1/sp1/oemdel_ssl1 oemdel_certtype=CSR set /system1/sp1/oemdel_ssl1 generate=1 dump -destination <iDRAC-CertificateSigningRequest-TFTP-URI> /system1/sp1/oemdel_ssl1	生成并下载 SSL 认证签名请求 (CSR)。
sslcsrgen -s	show /system1/sp1/oemdel_ssl1 oemdel_status	返回 CSR 生成过程的状态。
sslcertupload -t 1	set /system1/sp1/oemdel_ssl1 oemdel_certtype=SSL load -source <iDRAC-server-certificate-TFTP-URI> /system1/sp1/oemdel_ssl1	将 iDRAC 服务器认证上传到 iDRAC。
sslcertupload -t 2	set /system1/sp1/oemdel_ssl1 oemdel_certtype=AD load -source <ActiveDirectory-certificate-TFTP-URI> /system1/sp1/oemdel_ssl1	将 Active Directory 认证上传到 iDRAC。
sslcertdownload -t 1	set /system1/sp1/oemdel_ssl1 oemdel_certtype=SSL load -source <iDRAC-server-certificate-TFTP-URI> /system1/sp1/oemdel_ssl1	从 iDRAC 下载 iDRAC 服务器认证。
sslcertdownload -t 2	set /system1/sp1/oemdel_ssl1 oemdel_certtype=AD load -source <ActiveDirectory-certificate-TFTP-URI> /system1/sp1/oemdel_ssl1	从 iDRAC 下载 Active Directory 认证。

[目录](#)

iDRAC 概览

Integrated Dell™ Remote Access Controller 固件版本 1.2 用户指南

- [iDRAC 管理功能](#)
- [iDRAC 安全功能](#)
- [支持的平台](#)
- [支持的操作系统](#)
- [支持的 Web 浏览器](#)
- [支持的远程访问连接](#)
- [iDRAC 端口](#)
- [您可能需要的其它说明文件](#)

Integrated Dell™ Remote Access Controller (iDRAC) 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。

iDRAC 在远程监测/控制系统中使用集成的片上系统微处理器。iDRAC 共存于受管 PowerEdge 服务器的系统板上。服务器操作系统与正在执行的应用程序相关；iDRAC 与监测和管理操作系统之外的服务器环境和状态相关。

可以配置 iDRAC 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，iDRAC 可以在检测到系统崩溃时记录事件数据并捕获屏幕图像。

Managed Servers 安装在 Dell M1000e 系统机柜（机箱）中，装有模块化电源设备、冷却风扇和机箱管理控制器 (CMC)。CMC 监控和管理机箱中安装的所有组件。可以添加冗余 CMC 以在主要 CMC 失败时进行热故障转移。机箱通过 LCD 显示屏、本地控制台连接及其 web 界面提供到 iDRAC 的访问。

所有到 iDRAC 的网络连接都通过 CMC 网络接口（标有“GB1”的 CMC RJ45 连接端口）。CMC 通过专用内部网络将通信路由到服务器上的 iDRAC。此专用管理网络在服务器数据通路之外并且在操作系统的控制外，即带外。受管服务器的带内 网络接口通过机箱内安装的输入/输出模块 (IOM) 来访问。

iDRAC 网络接口默认情况下已禁用。必须对其进行配置，才能访问 iDRAC。当 iDRAC 已启用且在网络上配置后，可以通过 iDRAC web 接口、telnet 或 SSH 和 supported 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。

iDRAC 管理功能

iDRAC 提供以下管理功能：

- 1 动态域名系统 (DDNS) 注册
- 1 使用 Web 接口、本地 RACADM 命令行界面通过控制台重定向以及 SM-CLP 命令行通过 telnet/SSH 连接进行远程系统管理和监控
- 1 支持 Microsoft Active Directory® 验证 — 使用标准架构或扩展架构将 iDRAC 用户 ID 和密码集中在 Active Directory 中进行管理
- 1 控制台重定向 — 提供远程系统键盘、视频和鼠标功能
- 1 虚拟介质 — 允许受管服务器访问 Management Station 上的本地介质驱动器或网络共享的 ISO CD/DVD 映像
- 1 监控 — 提供对系统信息和组件状态的访问
- 1 访问系统日志 — 能够访问系统事件日志、iDRAC 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
- 1 Dell OpenManage™ 软件集成 — 使您能够从 Dell OpenManage Server Administrator 或 IT Assistant 启动 iDRAC Web 界面
- 1 iDRAC 警报 — 通过电子邮件或 SNMP 陷阱发出潜在受管节点问题的警报
- 1 远程电源管理 — 从管理控制台提供远程电源管理功能，比如关闭系统和重置
- 1 智能平台管理接口 (IPMI) 支持
- 1 安全套接层 (SSL) 加密 — 通过 Web 界面提供安全的远程系统管理
- 1 密码级别安全性管理 — 防止未经授权访问远程系统
- 1 基于角色的授权 — 为不同的系统管理任务提供可分配的权限

iDRAC 安全功能

iDRAC 提供以下安全功能：

- 1 通过 Microsoft Active Directory（可选）或硬件保存的用户 ID 和密码为用户提供验证
- 1 基于角色的授权，使管理员能为每个用户配置特定权限
- 1 通过 Web 界面或 SM-CLP 进行用户 ID 和密码配置
- 1 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

- 1 通过 Web 界面或 SM-CLP 进行会话超时配置（以秒为单位）
- 1 可配置 IP 端口（在相应情况下）

 **注：** Telnet 不支持 SSL 加密技术。

- 1 Secure Shell (SSH)，其使用加密传输层实现更高的安全保护
- 1 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
- 1 限制连接到 iDRAC 的客户端的 IP 地址范围

支持的平台

iDRAC 在 Dell PowerEdge M1000e 系统机柜中支持以下 PowerEdge 系统：

- 1 PowerEdge M600
- 1 PowerEdge M605
- 1 PowerEdge M805
- 1 PowerEdge M905

查看 iDRAC 自述文件和《Dell PowerEdge 兼容性指南》（位于 Dell 支持网站 support.dell.com）以了解最新支持的平台。

支持的操作系统

[表 1-1](#) 列出支持 iDRAC 的操作系统。

请参阅 Dell 支持网站 support.dell.com 上的《Dell OpenManage Server Administrator 兼容性指南》了解最新信息。

表 1-1. 支持的操作系统

操作系统系列	操作系统
Microsoft Windows	Microsoft® Windows Server® 2003 R2 Standard 和 Enterprise (32-bit x86) Editions, 带有 SP2 Microsoft Windows Server 2003 Web、Standard 和 Enterprise (32 位 x86) Edition, 带有 SP2 Microsoft Windows Server 2003 标准版和企业版 (x64) (含 SP2) Microsoft Windows Storage Server 2003 R2 Express、Workgroup、Standard 和 Enterprise x64 Edition Microsoft Windows Server 2008 Web、Standard 和 Enterprise (32 位 x86) Editions Microsoft Windows Server 2008 Web、Standard、Enterprise 和 Datacenter (x64) Editions 注： 安装 Windows Server 2003 with Service Pack 1 时，应注意更改 DCOM 安全设置。有关详情，请参阅 Microsoft 支持网站文章 903220 support.microsoft.com/kb/903220 。
Red Hat® Linux®	Red Hat Enterprise Linux WS、ES 和 AS (版本 4) (x86 和 x86_64) Enterprise Linux 5 (x86 和 x86-64)
SUSE® Linux	Enterprise Server 9, 带有 Update 2 和 Update 3 (x86_64) Enterprise Server 10 (Gold) (x86_64)

支持的 Web 浏览器

[表 1-2](#) 列出了作为 iDRAC 客户端支持的 Web 浏览器。

请参阅 iDRAC 自述文件和《Dell OpenManage Server Administrator 兼容性指南》（位于 Dell 支持网站 support.dell.com）了解最新信息。

 **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。

表 1-2. 支持的 Web 浏览器

--	--

操作系统	支持的 Web 浏览器
Windows	Internet Explorer 6.0, 带有 Service Pack 2 (SP2), 只用于 Windows XP 和 Windows 2003 R2 SP2 Internet Explorer 7.0, 只用于 Windows Vista、Windows XP、Windows 2003 R2 SP2 和 Windows Server 2008 Mozilla Firefox 2.0 for Windows (只用于 Java vKVM/vMedia 控制台)
Linux	Mozilla Firefox 1.5, 只用于 SUSE Linux (版本 10) Red Hat Enterprise Linux 4 和 5 (32 位或 64 位) 和 Suse Linux Enterprise Server 10 (32 位或 64 位) 上的 Mozilla Firefox 2.0

支持的远程访问连接

[表 1-3](#) 列出连接功能。

表 1-3. 支持的远程访问连接

连接	功能
iDRAC NIC	<ul style="list-style-type: none"> 10Mbps/100Mbps/1Gbps 以太网, 通过 CMC Gb 以太网端口 DHCP 支持 SNMP 陷阱和电子邮件事件通知 支持 SM-CLP (telnet 或 SSH) 命令 shell, 进行诸如 iDRAC 配置、系统启动、重置、开机和关机命令等操作 支持 IPMI 公用程序, 比如 ipmitool 和 ipmishell

iDRAC 端口

[表 1-4](#) 列出 iDRAC 侦听连接的端口。 [表 1-5](#) 标识 iDRAC 用作客户端的端口。当打开防火墙以远程访问 iDRAC 时, 需要此信息。

表 1-4. iDRAC 服务器侦听端口

"Port Number" (端口号)	功能
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668*, 3669*	虚拟介质服务
3770*, 3771*	虚拟介质安全服务
5900*	控制台重定向: 键盘/鼠标
5901*	控制台重定向: 视频
* 可配置端口	

表 1-5. iDRAC 客户端端口

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

您可能需要的其它说明文件

除了本《用户指南》以外，以下说明文件提供了在系统中设置和操作 iDRAC 的其它信息：

- 1 iDRAC 联机帮助提供了有关使用 Web 界面的信息。
- 1 《Dell Chassis Management Controller 用户指南》提供有关使用控制器（管理含有 PowerEdge 服务器的机箱中的所有模块）的信息。
- 1 《Dell OpenManage IT Assistant 用户指南》提供了关于使用 IT Assistant 的信息。
- 1 《Dell OpenManage Server Administrator 用户指南》提供了有关安装和使用 Server Administrator 的信息。
- 1 《Dell Update Packages 用户指南》介绍了如何获取 Dell Update Package 以及如何将其用于系统更新策略中。

以下系统说明文件还提供了更多有关安装 iDRAC 的系统的信息：

- 1 《产品信息指南》提供了重要的安全与管制信息。保修信息可能在该说明文件中附带，也可能作为单独的说明文件提供。
- 1 机架解决方案中的《机架安装指南》和《机架安装说明》介绍如何将系统安装到机架中。
- 1 《使用入门指南》概述了系统配置、如何设置系统以及技术规格。
- 1 《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。
- 1 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。
- 1 操作系统说明文件介绍了如何安装（如果有必要）、配置和使用操作系统软件。
- 1 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项的信息。
- 1 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。

- 1 可能还会提供版本注释或自述文件以说明对系统、说明文件或针对高级用户或技术人员的高级技术参考资料的最新更新。

[目录](#)

配置 iDRAC

Integrated Dell™ Remote Access Controller固件版本1.2 用户指南

- [开始之前](#)
- [用于配置 iDRAC 的界面](#)
- [配置任务](#)
- [配置网络 \(使用 CMC Web 界面\)](#)
- [查看 FlexAddress 夹层卡光纤连接](#)
- [更新 iDRAC 固件](#)

本部分介绍了如何建立 iDRAC 访问以及如何配置管理环境以使用 iDRAC。

开始之前

配置 iDRAC 前收集以下项目：

- 1 *Dell Chassis Management Controller Firmware 用户指南*
- 1 *Dell PowerEdge Installation and Server Management CD*
- 1 *Dell Systems Management Consoles CD*
- 1 *Dell PowerEdge Service and Diagnostic Utilities CD*
- 1 *Dell PowerEdge Documentation CD*

用于配置 iDRAC 的界面

可以使用 iDRAC 配置公用程序、iDRAC Web 界面、本地 RACADM CLI 或 SM-CLP CLI 配置 iDRAC。在受管服务器上安装操作系统和 Dell PowerEdge 服务器管理软件后，本地 RACADM CLI 才可用。 [表 2-1](#) 说明这些界面。

要获得更好的安全保护，请通过 iDRAC 配置公用程序访问 iDRAC 配置，或使用 RACADM 命令（请参阅[RACADM 子命令概览](#)）或从 GUI（请参阅[启用或禁用本地配置访问](#)）禁用本地 RACADM CLI。

 **注意：** 同时使用一个以上的配置界面可能会产生意外的结果。

表 2-1. 配置界面

接口	说明
iDRAC 配置公用程序	在启动时访问，iDRAC 配置公用程序在安装新 PowerEdge 服务器时有用。用来设置网络和基本安全功能以及启用其它功能。
iDRAC Web 界面	iDRAC Web 界面是基于浏览器的管理应用程序，可以用来交互式管理 iDRAC 和监控。这是日常任务（如监控系统运行状况、查看系统事件日志、管理本地 iDRAC 用户以及启动 CMC Web 界面和控制台重定向会话）的主要界面。
CMC Web 界面	除了监控和管理机箱，CMC Web 界面可用于查看受管服务器的状态、配置 iDRAC 网络设置，以及启动、停止或重置受管服务器。
机箱 LCD 面板	iDRAC 所在机箱上的 LCD 面板可用于查看机箱中服务器的高级别状态。在 CMC 初始配置期间，配置向导会允许启用 iDRAC 网络的 DHCP 配置。
本地 Racadm:	本地 RACADM 命令行界面在受管服务器上运行。可以从 iKVM 访问或从 iDRAC Web 界面启动控制台重定向会话来进行访问。当您安装 Dell OpenManage Server Administrator 时，RACADM 被安装在受管服务器上。 通过 RACADM 命令可以访问几乎所有 iDRAC 功能。可以检查传感器数据、系统事件日志记录以及 iDRAC 中维护的当前状态和配置值。可以变更 iDRAC 配置值、管理本地用户、启用和禁用功能，以及执行电源功能，如关闭或重新启动受管服务器。
IVM-CLI	通过 iDRAC 虚拟介质命令行界面 (IVM-CLI)，受管服务器可以访问 Management Station 上的介质。这非常有助于开发脚本在多个受管服务器上安装操作系统。
SM-CLP	SM-CLP 是 iDRAC 中结合的服务器管理工作组服务器管理命令行协议 (SM-CLP)。使用 telnet 或 SSH 登录 iDRAC 可访问 SM-CLP 命令行。 SM-CLP 命令提供了有用的本地 RACADM 命令子集。这些命令对脚本编写很有用，因为它们可以从 Management Station 命令行执行。命令的输出可以用定义明确的格式（包括 XML）进行检索，因此非常有助于脚本编写以及与现有报告和管理工具进行集成。 请参阅 RACADM 和 SM-CLP 等价查看 RACADM 和 SM-CLP 命令之间的对比。
IPMI	IPMI 为嵌入式管理子系统（如 iDRAC）定义了一种与其它嵌入式系统和管理应用程序进行通信的标准方式。 可以使用 iDRAC Web 界面、SM-CLP 或 RACADM 命令配置 IPMI 平台事件筛选器 (PEF) 和平台事件陷阱 (PET)。 PEF 使 iDRAC 在检测到情况时执行可选的操作（比如重新启动受管服务器）。PET 指示 iDRAC 在检测到指定事件或情况时发送电子邮件或 IPMI 警报。

在启用 IPMI Over LAN 后，还可以与 iDRAC 配合使用标准 IPMI 工具，如 [ipmitool](#) 和 [ipmishell](#)。

配置任务

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

可以用来执行每个任务的配置任务列在任务之下。

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

配置 Management Station

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

- 1 请参阅[配置 Management Station](#)

配置 iDRAC 网络

启用 iDRAC 网络并配置 IP、网络掩码、网关和 DNS 地址。

 **注：** 通过 iDRAC 配置公用程序访问 iDRAC 配置，或使用 RACADM 命令（请参阅[RACADM 子命令概览](#)）或从 GUI（请参阅[启用或禁用本地配置访问](#)）禁用本地 RACADM CLI。

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

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

 **注：** LCD 面板可用于启用 DHCP 以配置 iDRAC 网络。如果要分配静态地址，必须使用 iDRAC 配置公用程序或 CMC Web 界面。

- 1 机箱 LCD 面板 — 请参阅 *Dell Chassis Management Controller Firmware 用户指南*。
- 1 iDRAC 配置公用程序 — 请参阅 [LAN](#)
- 1 CMC Web 界面 — 请参阅 "[配置网络（使用 CMC Web 界面）](#)"
- 1 RACADM — 请参阅 "[cfgLanNetworking](#)"

配置 iDRAC 用户

设置本地 iDRAC 用户和权限。iDRAC 在固件中设置了一个有十六个本地用户的表。可以为这些用户设置用户名、密码和角色。

- 1 iDRAC 配置公用程序（仅配置管理用户） — 请参阅 [LAN 用户配置](#)
- 1 iDRAC Web 界面 — 请参阅 [添加和配置 iDRAC 用户](#)
- 1 RACADM — 请参阅 "[添加 iDRAC 用户](#)"

"Configure Active Directory"（配置 Active Directory）

除了本地 iDRAC 用户，您也可以使用 Microsoft® Active Directory® 验证 iDRAC 用户登录。

- 1 请参阅[将 iDRAC 用于 Microsoft Active Directory](#)

配置 IP 筛选和 IP 阻止

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

- 1 iDRAC Web 界面 — 请参阅 [配置 IP 筛选和 IP 阻塞](#)
- 1 RACADM — 请参阅[配置 IP 筛选 \(IpRange\)](#)、[配置 IP 阻塞](#)

配置平台事件

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

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

- 1 IDRAC Web 界面 — 请参阅 [配置平台事件筛选器 \(PEF\)](#)
- 1 RACADM — 请参阅“[配置 PEF](#)”

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

- 1 IDRAC Web 界面 — 请参阅 [配置平台事件陷阱 \(PET\)](#)
- 1 RACADM — [配置 PET](#)

启用或禁用本地配置访问

可以禁用对重要配置参数的访问，例如网络配置和用户权限。一旦禁用，重新引导后该设置仍将持续保留。本地 RACADM 程序和 IDRAC 配置公用程序（引导时）都禁止配置写入访问。Web 访问配置参数不受限制，并且可以随时查看配置数据。有关 IDRAC Web 界面的信息，请参阅[启用或禁用本地配置访问](#)。有关 cfgRac Tuning 命令的信息，请参阅[cfgRacTuning](#)。

配置“LAN 上串行”

“LAN 上串行”(SOL) 是一种 IPMI 功能，允许通过网络重新定向受管服务器的串行端口 I/O。SOL 支持 IDRAC 控制台重新定向功能。

- 1 IDRAC Web 界面 — 请参阅 [启用或禁用本地配置访问](#)
- 1 另请参阅[使用 GUI 控制台重新定向](#)

配置 iDRAC 服务

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

- 1 IDRAC Web 界面 — 请参阅 [配置 iDRAC 服务](#)
- 1 RACADM — 请参阅“[使用本地 RACADM 配置 iDRAC Telnet 和 SSH 服务](#)”

配置安全套接层 (SSL)

为 iDRAC Web 服务器配置 SSL。

- 1 IDRAC Web 界面 — 请参阅 [安全套接层 \(SSL\)](#)
- 1 RACADM — 请参阅[cfgRacSecurity](#)、[sslcsrqn](#)、[sslcertupload](#)、[sslcertdownload](#)、[sslcertview](#)

配置虚拟介质

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

- 1 IDRAC Web 界面 — 请参阅 [配置并使用虚拟介质](#)
- 1 IDRAC 配置公用程序 — 请参阅 [虚拟介质](#)

安装受管服务器软件

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

- 1 控制台重新定向 — 请参阅[在受管服务器上安装软件](#)
- 1 IVM-CLI — 请参阅[使用虚拟介质命令行界面公用程序](#)

配置受管服务器的上次崩溃屏幕功能

设置受管服务器以使 iDRAC 可以在操作系统崩溃或冻结后捕获屏幕图像。

- 1 受管服务器 — 请参阅[配置受管服务器以捕获上次崩溃屏幕](#)、[禁用 Windows 自动重新引导选项](#)

配置网络（使用 CMC Web 界面）

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

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

 **注：** CMC IP 地址可以在 iDRAC Web 界面中找到，方法是单击“**System**”（系统）→“**Remote Access**”（远程访问）→**CMC**。还可以从此页启动 CMC Web 界面。

1. 使用 web 浏览器通过表单 URL `https://<CMC-IP-address>` 或 `https://<CMC-DNS-name>` 登录 CMC web 用户界面。
2. 输入 CMC 用户名和密码并单击“**OK**”（确定）。
3. 单击左侧列“**Chassis**”（机箱）旁的加号 (+)，然后单击“**Servers**”（服务器）。
4. 单击“**Setup**”（设置）→“**Deploy Network**”（部署网络）。
5. 为服务器启用 LAN，方法是选中“**Enable Lan**”（启用 Lan）标题下服务器旁边的复选框。
6. 启用或禁用 IPMI over LAN，方法是选中或取消选取“**Enable IPMI over LAN**”（启用 IPMI over LAN）标题下服务器旁的复选框。
7. 为服务器启用或禁用 DHCP，方法是选中或取消选取“**DHCP Enabled**”（已启用 DHCP）标题下服务器旁的复选框。
8. 如果 DHCP 已禁用，则为服务器输入静态 IP 地址、网络掩码和默认网关。
9. 单击页面底部的“**Apply**”（应用）。

查看 FlexAddress 夹层卡光纤连接

M1000e 包括 FlexAddress，它是一种先进的多级、多标准网络系统。FlexAddress 允许为每个 Managed Server 端口连接使用永久、机箱分配的 World Wide 名称和 MAC 地址 (WWN/MAC)。

 **注意：** 为了避免可能导致无法开启 Managed Server 的错误，每个端口和光纤连接必须安装正确类型的夹层卡。

使用 CMC Web 界面执行 FlexAddress 功能的配置。有关 FlexAddress 功能及其配置的更多详情，请参阅《*Dell Chassis Management Controller Firmware Version 1.20 用户指南*》。

为机箱启用并配置 FlexAddress 功能后，单机**System**→**Properties**→**WWN/MAC** 查看所安装的夹层卡列表、它们所连接的光纤和端口、光纤端口位置、光纤类型，以及每个已安装的嵌入式以太网和可选夹层卡路口的服务器配置或机箱分配的 MAC 地址。

要查看已安装的夹层卡的列表、已安装的夹层卡类型，以及是否配置了 FlexAddress，单击“**System**”（系统）→“**Properties**”（属性）→“**Summary**”（摘要）。

更新 iDRAC 固件

更新 iDRAC 固件会在 iDRAC 闪存中安装新的固件映像。可以用以下任何方法更新固件：

1. SM-CLP `load` 命令
1. iDRAC Web 界面
1. Dell Update Package（用于 Linux 或 Microsoft Windows）
1. DOS iDRAC 固件更新公用程序
1. CMC Web 界面（仅在 iDRAC 固件损坏时）

下载固件或更新软件包

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

要使用 iDRAC Web 界面或 SM-CLP 更新 iDRAC 固件，或使用 CMC Web 界面恢复 iDRAC，请下载二进制映像，作为自解压压缩包打包。

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

要使用 DOS iDRAC 固件更新公用程序更新 iDRAC 固件，请下载更新公用程序和二进制映像，这些都打包在自解压压缩包中。

执行固件更新

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

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

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

使用 SM-CLP `load` 命令时，将固件二进制映像放在小型文件传输协议 (TFTP) 服务器可向 iDRAC 提供的目录中。请参阅[使用 SM-CLP 更新 iDRAC 固件](#)。

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

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

只有在 CMC 检测到 iDRAC 固件损坏（如果 iDRAC 固件更新进程在完成前中断会发生这种情况）时，才可以使用 CMC Web 界面更新固件。请参阅[使用 CMC 恢复 iDRAC 固件](#)。

 **注：** CMC 更新 iDRAC 的固件后，iDRAC 将为 SSL 证书生成新的 SHA1 和 MD5 密钥。因为该密钥与打开的 Web 浏览器中的密钥不同，所以连接到 iDRAC 的所有浏览器窗口都必须在固件更新完成后关闭。如果没有关闭浏览器窗口，将显示“Invalid Certificate”（证书无效）错误消息。

 **注：** 如果将 iDRAC 固件从版本 1.20 还原到较早版本，则必须删除基于 Windows 的 Management Station 上所有现有的 Internet Explorer ActiveX 浏览器插件，以便安装 ActiveX 插件的兼容版本。要删除 ActiveX 插件，可以导航至 `c:\WINNT\Downloaded Program Files` 并删除文件 `DELL IMC KVM Viewer`。

使用 DOS 更新公用程序

要使用 DOS 更新公用程序更新 iDRAC 固件，请启动受管服务器到 DOS，然后执行 `idrac16d` 命令。该命令的语法为：

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

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

其选项有：

-f — 强制更新。-f 选项可用将来将固件降级为较早的映像。

-i=<文件名> — 指定包含固件映像的文件名映像。如果固件文件名已从默认名称 `firmimg.imc` 更改，则本选项是必需的。

-l=<日志文件> — 记录来自更新活动的输出。此选项用于调试。

 **注意：** 如果为 `idrac16d` 命令输入了错误参数，或提供了 -h 选项，则会在用法输出中看到另外的选项 `-nopresconfig`。此选项用于不保留任何配置信息来更新固件。不应使用此选项，因为它会删除全部现有的 iDRAC 配置信息，如 IP 地址、用户和密码。

验证数字签名

数字签名用于验证文件签署者的身份以及确认文件的内容自签署以来未进行修改。

如果系统上还没有安装，必须安装 Gnu Privacy Guard (GPG) 来验证数字签名。要使用标准验证程序，应执行下列步骤：

1. 下载 Dell Linux 公共 GnuPG 密钥（如果还没有），方法是导航到 lists.us.dell.com 并单击 [Dell Public GPG key](#) 链接。将文件保存到本地系统。默认名称是 `linux-security-publickey.txt`。
2. 通过运行以下命令，将公共密钥导入 gpg 可信数据库：

```
gpg --import <公共密钥文件名>
```

 **注：** 必须提供私人密钥来完成此过程。

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

e. 键入以下命令：

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

f. 在 GPG 密钥编辑器内，键入 `fpr`。系统将显示以下信息：

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

如果导入密钥的指纹与以上完全相同，则说明是正确的密钥。

g. 仍在 GPG 密钥编辑器中，键入 `trust`。以下菜单会出现：

```
Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
```

different sources, etc.)

```
1 = I don't know or won't say
2 = I do NOT trust
3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
m = back to the main menu
```

Your decision?

h. 键入 5 <按 Enter 键>。以下提示会出现：

```
Do you really want to set this key to ultimate trust?
```

i. 键入 y <按 Enter 键> 确认选择。

j. 键入 quit <按 Enter 键> 退出 GPG 密钥编辑器。

必须且只能导入并验证公共密钥一次。

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

 **注：** 每个 Linux 更新软件包均具有独立的签名文件，与更新软件包显示在同一 web 页面上。进行验证时同时需要更新软件包及其关联签名文件。默认情况下，签名文件与 DUP 文件名相同，带有 .sign 扩展名。例如，如果 Linux DUP 命名为 PEM600_BIOS_LX_2.1.2.BIN，那么其签名文件是 PEM600_BIOS_LX_2.1.2.BIN.sign。iDRAC 固件映像也具有关联 .sign 文件，包括在固件映像的自解压压缩包中。要下载该文件，右击下载链接并使用“Save Target As”（目标另存为）... 文件选项。

5. 验证更新软件包：

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

以下示例说明了验证 PowerEdge M600 BIOS 更新软件包所遵循的步骤：

1. 从 support.dell.com 下载以下两个文件：

```
1 PEM600_BIOS_LX_2.1.2.BIN.sign
```

```
1 PEM600_BIOS_LX_2.1.2.BIN
```

2. 通过运行以下命令行导入公共密钥：

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

以下输出信息会出现：

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

3. Set the GPG trust level for the Dell public key. (为 Dell 公共密钥设置 GPG 信任水平。) if you haven't done so previously. (如果以前没有执行此操作。)

a. 键入以下命令：

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

b. 在命令提示符处，键入以下命令：

```
fpr
trust
```

c. 键入 5 <按 Enter 键> 从菜单选择 I trust ultimately (我绝对信任)。

d. 键入 y <按 Enter 键> 确认选择。

e. 键入 quit <按 Enter 键> 退出 GPG 密钥编辑器。

这将完成 Dell 公共密钥的验证。

4. 通过运行以下命令验证 PEM600 BIOS 软件包数字签名：

```
gpg --verify PEM600_BIOS_LX_2.1.2.BIN.sign PEM600_BIOS_LX_2.1.2.BIN
```

以下输出信息会出现：

```
gpg: Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D
gpg: Good signature from "Dell, Inc. (Product Group) <linux-security@dell.com>"
```

 **注：** 如果没有验证密钥（如[步骤 3](#)所示），将会收到其它信息：

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

清除浏览器的高速缓存

为了能够使用最新 iDRAC 中的功能，必须清除浏览器高速缓存以移除/删除可能存储在系统中的旧网页。

Internet Explorer

1. 启动 Internet Explorer。
2. 单击“Tools”（工具），然后单击“Internet Options”（Internet 选项）。
屏幕将显示“Internet Options”（Internet 选项）窗口。
3. 单击 General（常规）选项卡。
4. 在“Temporary Internet files”（Internet 临时文件）中单击“Delete Files”（删除文件）。
屏幕将显示“Delete Files”（删除文件）窗口。
5. 单击选中“Delete all offline content”（删除所有脱机内容），然后单击“OK”（确定）。
6. 单击“OK”（确定）关闭“Internet Options”（Internet 选项）窗口。

Firefox

1. 启动 Firefox。
2. 单击“Edit”（编辑）→ “Preferences”（首选项）。
3. 单击“Privacy”（隐私）选项卡。
4. 单击“Clear Cache Now”（立即清除高速缓存）。
5. 单击 Close（关闭）。

[目录](#)

[目录](#)

配置 Management Station

Integrated Dell™ Remote Access Controller固件版本1.2
用户指南

- [Management Station 设置步骤](#)
- [Management Station 网络要求](#)
- [配置支持的 Web 浏览器](#)
- [安装 Java Runtime Environment \(JRE\)](#)
- [安装 Telnet 或 SSH 客户端](#)
- [安装 TFTP 服务器](#)
- [安装 Dell OpenManage IT Assistant](#)

management station 是用于监控和管理 PowerEdge 服务器及机箱中其它模块的计算机。本部分说明了设置 Management Station 以与 iDRAC 配合使用的软件安装和配置任务。开始配置 iDRAC 之前，遵循此部分中的步骤确保已安装并配置了所需工具。

Management Station 设置步骤

要设置 Management Station，应执行下列步骤：

1. 设置 management station 网络。
2. 安装并配置一个支持的 Web 浏览器。
3. 安装 Java Runtime Environment (JRE)（对于 Windows 可选）。
4. 安装 telnet 或 SSH 客户端（如果需要）。
5. 安装 TFTP 服务器（如果需要）。
6. 安装 Dell OpenManage IT Assistant（可选）。

Management Station 网络要求

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

使用 iDRAC 控制台重定向功能（请参阅[使用 GUI 控制台重定向](#)），可以访问受管服务器的控制台，即使不能从服务器端口进行网络访问。还可以使用 iDRAC 功能在受管服务器上执行几种管理功能，比如重新启动计算机。但是，要访问网络和受管服务器上托管的应用程序服务，可能需要在管理计算机中有另外的 NIC。

配置支持的 Web 浏览器

以下部分介绍如何配置支持的 Web 浏览器来使用 iDRAC Web 界面。关于支持的 Web 浏览器列表，请参阅[支持的 Web 浏览器](#)。

打开 Web 浏览器

iDRAC Web 界面设计用于在受支持的 Web 浏览器中以至少 800（宽）x 600（高）像素的屏幕分辨率进行查看。为了能够查看该界面并访问所有功能，请确保将分辨率设置为至少 800 x 600 像素，和/或根据需要调整浏览器的大小。

 **注：** 在某些情况下，通常在固件更新后第一次会话期间，Internet Explorer 6 用户会看到在浏览器的状态栏中出现“Done, with errors”（已完成，但网页上有错误）的消息，同时主浏览器窗口中仅显示部分页面。遇到连接问题时也会出现此错误。这是 Internet Explorer 6 的已知问题。请关闭浏览器并重启。

配置 Web 浏览器以连接到 Web 界面

如果从通过代理服务器连接到因特网的 management station 连接到 iDRAC Web 界面，则必须配置 Web 浏览器以从该服务器访问因特网。

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

1. 打开 Web 浏览器窗口。

- 单击“Tools”（工具）并单击“Internet Options”（Internet 选项）。

随即将出现“Internet Options”（Internet 选项）窗口。

 **注：**不同 Internet Explorer 版本的默认安全级别各不相同。为了确保系统能够正常工作，请单击“Advanced”（高级）选项卡，并确认已选中“Enable Install-On-Demand (Other)”（启用即需安装[其它]）、“Enable third-party browser extensions”（启用第三方浏览器扩展）、“Sun Java Enabled”（启用 Sun Java）和“Use SSL 3.0”（使用 SSL 3.0）（选项名称可能会随版本而有所不同）。如果对这些设置进行了任何更改，请重新启动 Internet Explorer。

- 单击“Connections”（连接性）选项卡。
- 在“Local Area Network (LAN) settings”（局域网 [LAN] 设置）下，单击“LAN Settings”（局域网设置）。
- 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。
- 单击“OK”（确定）两次。

将 iDRAC 添加到可信域列表

通过 Web 浏览器访问 iDRAC Web 界面时，会在可信域列表中缺少 iDRAC IP 地址的情况下提示您将 IP 地址添加到列表中。完成后，单击“Refresh”（刷新）或重新启动 Web 浏览器以连接到 iDRAC Web 界面。

查看 Web 界面的本地化版本

iDRAC Web 界面支持以下操作系统语言：

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

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

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

Internet Explorer 6.0 (Windows)

要在 Internet Explorer 中查看 iDRAC Web 界面的本地化版本，应执行下列步骤：

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. 在“语言首选项”窗口中，单击“确定”。
7. 单击 OK（确定）。

Firefox 1.5 (Linux)

要在 Firefox 1.5 中查看 iDRAC Web 界面的本地化版本，请执行以下步骤：

1. 单击"Edit"（编辑）→ "Preferences"（首选项），然后单击"Advanced"（高级）选项卡。
2. 在"Language"（语言）部分，单击"Choose"（选择）。
3. 单击"Select a language to add"（选择要添加的语言）...
4. 选择支持的语言并单击"Add"（添加）。
5. 选择首选语言并单击"Move Up"（上移）移动到列表顶部。
6. 在语言菜单中，单击"OK"（确定）。
7. 单击 OK（确定）。

Firefox 2.0 (Linux 或 Windows)

要在 Firefox 2.0 中查看 iDRAC Web 界面的本地化版本，请执行以下步骤：

1. 单击"Tools"（工具）→ "Options"（选项），然后单击"Advanced"（高级）选项卡。
2. 在"Language"（语言）下，单击"Choose"（选择）。
屏幕将显示"Languages"（语言）窗口。
3. 在"Select a language to add..."（选择要添加的语言...）下拉菜单中，单击以高亮度显示一种受支持的语言，然后单击"Add"（添加）。
4. 单击选择首选语言，然后单击"Move Up"（上移）直到该语言出现在列表顶部。
5. 单击"OK"（确定）关闭"Languages"（语言）窗口。
6. 单击"OK"（确定）关闭"Options"（选项）窗口。

在 Linux 中设置区域

控制台重定向查看器需要 UTF-8 字符集才能正确显示。如果显示乱码，应检查区域设置并根据需要重置字符集。

以下步骤显示如何在 Red Hat® Enterprise Linux® 客户端上设置简体中文 GUI 的字符集：

1. 打开命令终端。
2. 键入 locale（本地）并按 <Enter>。类似以下的输出将会显示：

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

3. 如果这些值包括"zh_CN.UTF-8"，则无需任何更改。如果值中不包括"zh_CN.UTF-8"，则转至步骤 4。
4. 用文本编辑器编辑 /etc/sysconfig/i18n 文件。
5. 在文件中，应用以下更改：

当前项：

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

更新项:

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

6. 注销，然后登录操作系统。

从其它语言切换时，应确保此修补仍然有效。如果不行，应重复此程序。

禁用 Firefox 中的白名单功能

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

要禁用白名单功能并避免重复不必要的插件安装，应执行下列步骤：

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

“Preference Name”（**首选项名称**）、“Status”（**状况**）、“Type”（**类型**）和“Value”（**值**）的值会更改为粗体文本。“Status”（**状况**）值会更改为“user set”（**用户设置**），而“Value”（**值**）的值会更改为 `false`。

4. 在“Preferences Name”（**首选项名称**）列中，找到 `xpinstall.enabled`。

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

安装 Java Runtime Environment (JRE)

 **注：** 如果使用 Internet Explorer 浏览器，则会为控制台查看器提供 ActiveX 控件。如果安装了 JRE 并且在启动查看器前在 iDRAC web 界面中配置了控制台查看器，则还可以将 Java 控制台查看器用于 Internet Explorer。有关详情，请参阅在 [iDRAC Web 界面中配置控制台重定向](#)。

可以选择在启动查看器前使用 Java 查看器作为替代。

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

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

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

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

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

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

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

安装 Telnet 或 SSH 客户端

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

 **注：** 一次只能有一个到 iDRAC 的活动 telnet 或 SSH 连接。当有活动连接时，其它连接尝试会被拒绝。

与 iDRAC 配合使用 Telnet

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

如果 management station 运行 Windows XP 或 Windows 2003，则可能会在 iDRAC telnet 会话中遇到字符问题。此问题会以冻结登录的方式发生，在这种状况下，回车键不响应并且不显示密码提示。

要解决此问题，从 Microsoft Support 网站 support.microsoft.com 下载热修复 824810。请参阅 Microsoft 知识库文章 824810 了解有关详情。

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，会话可能会回音 ^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 客户端以使用 <Backspace> 键，应执行下列步骤：

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

```
Telnet
```

如果运行 telnet 会话，应按 <Ctrl><]>。

3. 在提示符后，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 会话以使用 <Backspace> 键，应执行下列步骤：

1. 打开 shell 并键入：

```
stty erase ^h
```

2. 在提示符后，键入：

```
Telnet
```

与 iDRAC 配合使用 SSH

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

可以在 management station 上使用 PuTTY (Windows) 或 OpenSSH (Linux) 连接到受管服务器的 iDRAC。如果在登录过程中出现错误，ssh 客户端就会发出一条错误信息。此信息文本取决于客户端，不受 iDRAC 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，只支持一个 telnet 或 SSH 会话。会话超时由 `cfgSsnMgtSshIdleTimeout` 属性控制，如“[iDRAC 属性数据库组和对象定义](#)”中所述。

iDRAC SSH 实现支持多种密码模式，如[表 3-1](#)中所示。

 **注：** SSHv1 不支持。

表 3-1. 密码模式

模式类型	模式
非对称加密	Diffie-Hellman DSA/DSS 512-1024（随机）位/NIST 规范
对称加密	1 AES256-CBC 1 RIJNDAEL256-CBC 1 AES192-CBC 1 RIJNDAEL192-CBC 1 AES128-CBC 1 RIJNDAEL128-CBC 1 BLOWFISH-128-CBC 1 3DES-192-CBC 1 ARCFOUR-128

信息完整性	<ul style="list-style-type: none">1 HMAC-SHA1-1601 HMAC-SHA1-961 HMAC-MD5-1281 HMAC-MD5-96
验证	<ul style="list-style-type: none">1 密码

安装 TFTP 服务器

 **注：** 如果只使用 iDRAC Web 界面传输 SSL 认证并上传新 iDRAC 固件，则不需要 TFTP 服务器。

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

只有在更新 iDRAC 固件或在 iDRAC 上安装认证时才需要与 iDRAC 相互传输文件。如果在执行这些任务时选择使用 SM-CLP 或 RACADM，TFTP 服务器必须在 iDRAC 可以通过 IP 号或 DNS 名称访问的计算机上运行。

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

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

安装 Dell OpenManage IT Assistant

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

- 1 *Dell Systems Management Consoles* CD — 包含所有最新的 Dell 系统管理控制台产品，包括 Dell OpenManage IT Assistant。
- 1 *Dell PowerEdge Service and Diagnostic Utilities* CD — 提供配置系统所需的工具并提供固件、诊断程序和 Dell 针对您系统优化的驱动程序。
- 1 *Dell PowerEdge Documentation* CD — 帮助您获得最新系统、系统管理软件产品、外围设备和 RAID 控制器的说明文件。
- 1 Dell 支持网站和自述文件 — 检查自述文件和 Dell 支持网站 support.dell.com 以了解有关 Dell 产品的最新信息。

使用 *Dell System Management Consoles* CD 在 Management Station 上安装管理控制台软件，包括 Dell OpenManage IT Assistant。有关安装该软件的说明，请参阅《快速安装指南》。

[目录](#)

配置受管服务器

Integrated Dell™ Remote Access Controller固件版本1.2 用户指南

- [在受管服务器上安装软件](#)
- [配置受管服务器以捕获上次崩溃屏幕](#)
- [禁用 Windows 自动重新引导选项](#)

本部分介绍了设置受管服务器以加强远程管理功能的任务。这些任务包括安装 Dell Open Manage Server Administrator 软件以及配置受管服务器以捕获上次崩溃屏幕。

在受管服务器上安装软件

Dell 管理软件包括以下功能：

- 1 本地 RACADM CLI — 允许从受管系统配置和管理 iDRAC。这是一种用于脚本配置和管理任务的强大工具。
- 1 必需 Server Administrator 才能使用 iDRAC 上次崩溃屏幕功能。
- 1 Server Administrator — 一种 Web 界面，允许从网络上的远程主机管理远程系统。
- 1 Server Administrator Instrumentation Service — 能够存取由业界标准系统管理代理程序收集的故障和性能详细信息，并允许远程管理监测的系统，包括关闭系统、启动系统和安全保护。
- 1 Server Administration Storage Management Service — 用集成的图形化视图提供存储管理信息。
- 1 Server Administrator 记录 — 显示各种信息的记录，如系统发出或收到的命令、监测的硬件事件、POST 事件以及系统警报。您可以在主页上查看记录，打印记录或将记录保存为报告，以及通过电子邮件将其发送到指定服务联络地址。

使用 *Dell PowerEdge Installation and Server Management* CD 安装 Server Administrator。有关安装该软件的说明，请参阅《快速安装指南》。

配置受管服务器以捕获上次崩溃屏幕

iDRAC 可以捕获上次崩溃屏幕以便您可以在 Web 界面中查看来帮助诊断受管系统崩溃的原因。按照这些步骤启用上次崩溃屏幕功能。

1. 安装受管服务器软件。有关安装受管服务器软件的详情，请参阅《Server Administrator 用户指南》。
2. 如果正在运行 Microsoft® Windows® 操作系统，确保在“Windows Startup and Recovery Settings”（Windows 启动和故障恢复设置）中取消选择“自动重新启动”功能。请参阅[禁用 Windows 自动重新引导选项](#)。
3. 在 iDRAC Web 界面中启用上次崩溃屏幕（默认已禁用）。

要在 iDRAC Web 界面中启用上次崩溃屏幕，单击 **System** → **Remote Access** → **iDRAC** → **Network/Security** → **Services**（服务），然后选中“自动系统恢复代理设置”标题下的“**Enable**”（启用）复选框。

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

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

4. 在 Server Administrator web 界面中，启用“Auto Recovery”（自动恢复）计时器并将“Auto Recovery”（自动恢复）操作设置为“Reset”（重置）、“Power Off”（关机）或“Power Cycle”（关机后再开机）。

有关如何配置“Auto Recovery”（自动恢复）计时器的信息，请参阅《Server Administrator 用户指南》。要确保能够捕获上次崩溃屏幕，“Auto Recovery”（自动恢复）计时器应设置为 60 秒。默认设置为 480 秒钟。

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

禁用 Windows 自动重新引导选项

为确保 iDRAC 可以捕获上次崩溃屏幕，在运行 Microsoft Windows Server® 或 Windows Vista® 的受管服务器上禁用“Automatic Reboot”（自动重新启动）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。

[目录](#)

使用 Web 界面配置 iDRAC

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [访问 Web 界面](#)
- [配置 iDRAC NIC](#)
- [配置平台事件](#)
- [配置 IPMI](#)
- [添加和配置 iDRAC 用户](#)
- [使用 SSL 和数字认证确保 iDRAC 通信](#)
- [配置和管理 Active Directory 认证](#)
- [启用或禁用本地配置访问](#)
- [配置 LAN 上串行](#)
- [配置 iDRAC 服务](#)
- [更新 iDRAC 固件](#)

iDRAC 提供了 Web 界面供您配置 iDRAC 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 iDRAC Web 界面。本章介绍了如何使用 iDRAC Web 界面来执行常规系统管理任务，并提供了一些相关信息的链接。

大多数 Web 界面配置任务还可以使用本地 RACADM 命令或 SM-CLP 命令来执行。

本地 RACADM 命令从受管服务器执行。有关使用本地 RACADM 的详情，请参阅[使用本地 RACADM 命令行界面](#)。

SM-CLP 命令在 shell 中执行，可通过 telnet 或 SSH 连接远程使用。有关使用 SM-CLP 的详情，请参阅[使用 iDRAC SM-CLP 命令行界面](#)。

访问 Web 界面

要访问 iDRAC Web 界面，请执行以下步骤：

1. 打开一个支持的 Web 浏览器窗口。

有关详情，请参阅[支持的 Web 浏览器](#)。

2. 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 iDRAC 的 IP 地址，而 *端口号* 是 HTTPS 端口号。

iDRAC“Login”（登录）窗口将会出现。

登录

您可以作为 iDRAC 用户或 Microsoft® Active Directory® 用户登录。默认用户名为 **root**，默认密码为 **calvin**。

必须得到管理员授予“Login to iDRAC”（登录到 iDRAC）权限才能登录到 iDRAC。

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：

- 1 您的 iDRAC 用户名。

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

- 1 您的 Active Directory 用户名。

Active Directory 名称可以用以下任何形式输入：`<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，输入您的 iDRAC 用户密码或 Active Directory 用户密码。密码区分大小写。

3. 单击“OK”（确定）或按 <Enter>。

注销

1. 在主窗口的右上角，单击“Logout”（**注销**）关闭会话。
2. 关闭浏览器窗口。

 **注：** “Log Out”（**注销**）按钮在您登录后才出现。

 **注：** 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 iDRAC 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。

使用多个浏览器选项卡和窗口

打开新选项卡和窗口时，不同版本的 web 浏览器会表现出不同的行为。每个窗口都是一个新会话，但每个新选项卡则不是新会话。Microsoft Internet Explorer 6 不支持选项卡；因此，每个打开的浏览器窗口都是一个新的 iDRAC Web 界面会话。Internet Explorer 7 具有打开选项卡和窗口的选项。每个选项卡将继承最新打开的选项卡的特性。例如，如果用户在一个选项卡上使用“Power User”（超级用户）权限登录，然后在另一个选项卡上以“Administrator”（管理员）权限登录，那这两个打开的选项卡都将具有“Administrator”（管理员）权限。关闭其中任何一个选项卡都会使所有 iDRAC Web 界面选项卡过期。

Firefox 中的选项卡和窗口行为与 Internet Explorer 7 相似。

配置 iDRAC NIC

本节假定 iDRAC 已经配置好并能够在网络上访问。请参阅[配置 iDRAC 网络](#)配置 iDRAC 网络获得有关初始 iDRAC 网络配置的帮助。

配置网络和 IPMI LAN 设置

 **注：** 您必须具有**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保留表中。客户端（例如 iDRAC）在 DHCP 协议过程中必须提供此令牌。iDRAC 以单字节接口编号 (0) 后跟六字节 MAC 地址来提供客户端标识符选项。

1. 单击“System”（**系统**）→ “Remote Access”（**远程存取**）→ iDRAC。
2. 单击“Network/Security”（**网络/安全性**）选项卡打开“Network Configuration”（**网络配置**）页。

[表 5-1](#) 和 [表 5-2](#) 说明了网络页上的**网络设置**和**IPMI LAN 设置**。

3. 完成输入所需设置后，单击“Apply”（**应用**）。
4. 单击相应按钮继续。请参阅[表 5-3](#)。

表 5-1. 网络设置

设置	说明
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 iDRAC 的所有通信均被封锁。 默认为 off。
"Media Access Control (MAC) Address"（ 介质访问控制 [MAC] 地址 ）	显示唯一标识网络中各个节点的"Media Access Control (MAC) Address"（介质访问控制 [MAC] 地址）。MAC 地址不能更改。
"Use DHCP (For NIC IP Address)"（ 使用 DHCP [对于 NIC IP 地址] ）	提示 iDRAC 从动态主机配置协议 (DHCP) 服务器获取 NIC 的 IP 地址。同时，禁用"Static IP Address"（ 静态 IP 地址 ）、"Static Subnet Mask"（ 静态子网掩码 ）和"Static Gateway"（ 静态网关 ）控制。 默认为 off。
"Static IP Address"（ 静态 IP 地址 ）	允许用户输入或编辑 iDRAC NIC 的静态 IP 地址。要更改此设置，请取消选择"Use DHCP"（ 使用 DHCP [用于 NIC IP 地址] ）复选框。
"Static Subnet Mask"（ 静态子网掩码 ）	允许用户输入或编辑 iDRAC NIC 的子网掩码。要更改此设置，首先取消选择"Use DHCP"（ 使用 DHCP [用于 NIC IP 地址] ）复选框。
"Static Gateway"（ 静态网关 ）	允许用户输入或编辑 iDRAC NIC 的静态网关。要更改此设置，首先取消选择"Use DHCP"（ 使用 DHCP [用于 NIC IP 地址] ）复选框。
"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"Static Preferred DNS Server"（ 静态首选 DNS 服务器 ）

服务器地址)	器)和"Static Alternate DNS Server" (静态备用 DNS 服务器) 字段中提供 IP 地址。 默认为 off。 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"Static Preferred DNS Server" (静态首选 DNS 服务器) 和"Static Alternate DNS Server" (静态备用 DNS 服务器) 字段中输入 IP 地址。
"Static Preferred DNS Server" (静态首选 DNS 服务器)	允许用户输入或编辑首选 DNS 服务器的静态 IP 地址。要更改此设置, 首先取消选择"Use DHCP to obtain DNS server addresses" (使用 DHCP 获取 DNS 服务器地址) 复选框。
"Static Alternate DNS Server" (静态备用 DNS 服务器)	仅当未选择"Use DHCP to obtain DNS server addresses" (使用 DHCP 获得 DNS 服务器地址) 时使用备用 DNS 服务器 IP 地址。如果没有备用 DNS 服务器, 则输入 IP 地址 0.0.0.0。
"Register iDRAC on DNS" (向 DNS 注册 iDRAC)	在 DNS 服务器上注册 iDRAC 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" (向 DNS 注册 iDRAC) 后才会显示 iDRAC 名称。默认名称为 idrac-service_tag, 其中 service_tag 是 Dell 服务器的服务标签号码。例如: idrac-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中了"Register iDRAC on DNS" (在 DNS 上注册 iDRAC) 复选框, 则可以在"DNS Domain Name" (DNS 域名) 字段修改 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 [用于 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。
"Community String" (团体字符串)	包含在从 iDRAC 发送的"Simple Network Management Protocol (SNMP)" (简单网络管理协议 [SNMP]) 警报陷阱中使用的团体字符串。在出现平台事件时 SNMP 警报陷阱由 iDRAC 传输。默认为 public。
"SMTP Server Address" (SMTP 服务器地址)	在出现平台事件时, iDRAC 为了发送电子邮件警报而与之通信的"Simple Mail Transfer Protocol (SMTP)" (简单邮件传输协议 [SMTP]) 服务器的 IP 地址。默认为 127.0.0.1。

表 5-2. IPMI LAN 设置

设置	说明
"Enable IPMI Over LAN" (启用 LAN 上 IPMI)	选中后表示 IPMI LAN 信道已启用。默认为 off。
"Channel Privilege Level Limit" (信道权限级别限制)	配置 LAN 信道上可接受的用户最大权限级别。选择以下选项之一: Administrator (管理员)、Operator (操作员) 或 User (用户)。默认为 Administrator (管理员)。
"Encryption Key" (密钥)	配置密钥: 0 至 20 十六进制字符 (不允许空白)。默认为空白。

表 5-3. 网络配置页按钮

按钮	说明
"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。
"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。
"Apply" (应用)	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 iDRAC Web 界面。所有其他更改将要求重设 NIC, 这可能导致丢失连接。

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

表 5-4 说明了“Network Security”（网络安全性）页设置。

- 配置完设置后，单击“Apply”（应用）。
- 单击相应按钮继续。请参阅表 5-5。

表 5-4. 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。默认为 off。
"IP Range Address"（IP 范围地址）	决定可接受的 IP 子网地址。默认为 192.168.1.0。
"IP Range Subnet Mask"（IP 范围子网掩码）	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。默认为 255.255.255.0。
"IP Blocking Enabled"（IP 阻塞已启用）	启用 IP 地址阻止功能，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。默认为 off。
"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 阻塞故障窗口）	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过多的某个 IP 地址的登录尝试。默认为 3600。

表 5-5. 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"（应用）	保存“Network Security”（网络安全性）页上所做的任何新设置。
"Go Back to Network Page"（返回到网络页）	返回到“Network”（网络）页。

配置平台事件

平台事件配置提供了用于配置 iDRAC 针对某些事件消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）。

可筛选平台事件在表 5-6 中列出。

表 5-6. 可筛选平台事件

索引	平台事件
1	电池警告声明
2	电池临界声明
3	分离电压临界声明
4	温度警告声明
5	温度临界声明
6	已降级冗余
7	冗余掉失
8	处理器警告声明
9	处理器临界声明
10	没有处理器声明
11	事件日志临界声明
12	监督临界声明

出现平台事件时（例如，电池警告声明），会生成系统事件并在系统事件日志（SEL）中记录。如果该事件匹配某个已启用的平台事件筛选器（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。

如果该平台事件筛选器还配置为执行操作（比如重新引导系统），则将执行操作。

配置平台事件筛选器（PEF）

 **注：** 配置平台事件陷阱或电子邮件警报设置前配置平台事件筛选器。

1. 登录 iDRAC Web 界面。请参阅[访问 Web 界面](#)。
2. 单击“System”（系统）然后“Alert Management”（警报管理）选项卡。
3. 在平台事件页上，通过单击事件对应的“Generate Alert”（生成警报）复选框为事件启用“Alert Generation”（警报生成）。

 **注：** 可通过单击“Generate Alert”（生成警报）列标题旁边的复选框启用或禁用所有事件的“Alert Generation”（警报生成）。

4. 单击要为各个事件启用操作下方的单选按钮。每个事件只能设置一个操作。
5. 单击“Apply”（应用）。

 **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）。

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. 配置 PET 目标 IP 地址：
 - a. 单击要激活的“Destination Number”（目标号码）旁边的“Enable”（启用）复选框。
 - b. 在“Destination IP Address”（目标 IP 地址）框中输入 IP 地址。

 **注：** 目标团体字符串必须与 iDRAC 团体字符串相同。

- c. 单击“Apply”（应用）。

 **注：** 要成功发送陷阱，先配置“Network Configuration”（网络配置）页上的“Community String”（团体字符串）值。“Community String”（团体字符串）值表示从 iDRAC 发送的简单网络管理协议（SNMP）警报陷阱中使用的团体字符串。在出现平台事件时 SNMP 警报陷阱由 iDRAC 传输。“Community String”（团体字符串）的默认设置为 Public。

- d. 单击“Send”（发送）检测配置的警报（如果需要）。
- e. 为任何其它目标号码重复步骤 a 到 d。

配置电子邮件警报

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. 配置电子邮件警报设置。
 - a. 在“Alert Management”（警报管理）选项卡中，单击“Email Alert Settings”（电子邮件警报设置）。
4. 配置电子邮件警报目标。
 - a. 在“Email Alert Number”（电子邮件警报号码）列中，单击目标号码。有四个可能接收警报的目标。
 - b. 确保选中“Enabled”（已启用）复选框。
 - c. 在“Destination Email Address”（目标电子邮件地址）字段中，键入有效电子邮件地址。
 - d. 单击“Apply”（应用）。

 **注：** 要成功发送检测电子邮件，必须在“Network Configuration”（网络配置）页上配置“SMTP Server Address”（SMTP 服务器地址）。在出现平台事件时，“SMTP Server”（SMTP 服务器）的 IP 地址与 iDRAC 进行通信，发送电子邮件警报。

- e. 单击“Send”（发送）检测配置的电子邮件警报（如果需要）。

- f. 为其它电子邮件警报设置重复步骤 a 到步骤 e。

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. 单击"System" (系统) → "Remote Access" (远程访问) → iDRAC，然后单击"Network/Security" (网络/安全性)。
 - b. 在"Network Configuration" (网络配置) 页，"IPMI LAN Settings" (IPMI LAN 设置) 下，选择"Enable IPMI Over LAN" (启用 LAN 上 IPMI)。
 - c. 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) 下拉菜单，选择"Administrator" (管理员)、"Operator" (操作员) 或"User" (用户) 并单击"Apply" (应用)。

- d. 如果需要，设置 IPMI LAN 信道密钥。

 **注：** iDRAC IPMI 支持 RMCP+ 协议。

 **注：** 密钥必须包含不超过 20 个字符的偶数个十六进制字符。

在"IPMI LAN Settings" (IPMI LAN 设置) 下"Encryption Key" (密钥) 字段中，键入密钥。

- e. 单击"Apply" (应用)。

3. 配置 IPMI LAN 上串行 (SOL)。
 - a. 单击"System" (系统) → "Remote Access" (远程存取) → iDRAC。
 - b. 单击"Network Security" (网络安全) 选项卡，然后单击"Serial Over LAN" (LAN 上串行)。
 - c. 在"Serial Over LAN Configuration" (LAN 上串行配置) 页上，单击"Enable Serial Over LAN" (启用 LAN 上串行) 复选框启用 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 波特率与受管服务器的波特率相同。

单击"Baud Rate" (波特率) 下拉菜单选择数据速度 19.2 kbps、57.6 kbps 或 115.2 kbps。

- e. 单击"Apply" (应用)。

添加和配置 iDRAC 用户

要用 iDRAC 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 iDRAC 用户，请执行以下步骤：

 **注：** 您必须具有配置 iDRAC 权限才能执行以下步骤。

1. 单击"System" (系统) → "Remote Access" (远程访问) → iDRAC，然后单击"Network/Security" (网络/安全性) 选项卡。
2. 打开"Users" (用户) 页配置用户。

"Users" (用户) 页显示各个用户的"User ID" (用户 ID)、"State" (状态)、"Username" (用户名)、"IPMI LAN Privileges" (IPMI LAN 权限)、"iDRAC Privileges" (iDRAC 权限) 和"Serial Over LAN" (LAN 上串行)。

 **注：** User-1 为 IPMI 匿名用户保留，不可配置。

3. 在"User ID" (用户 ID) 列单击用户 ID 编号。
4. 在"User Configuration" (用户配置) 页中配置用户的属性和权限。

[表 5-7](#) 说明配置 iDRAC 用户名和密码的"General" (常规) 设置。

[表 5-8](#) 说明"IPMI User Privileges" (IPMI 用户权限) 以供配置用户 LAN 权限。

表 5-9 说明用于"IPMI User Privileges " (IPMI 用户权限) 和"DRAC User Privileges " (DRAC 用户权限) 设置的"User Group permissions" (用户组权限)。

表 5-10 说明"iDRAC Group" (iDRAC 组) 权限。如果将"iDRAC User Privilege" (iDRAC 用户权限) 添加给 Administrator (管理员)、Power User (高级用户) 或 Guest User (客用户), iDRAC Group (iDRAC 组) 将会更改为 Custom (自定义) 组。

5. 完成后, 单击"Apply" (应用)。
6. 单击相应按钮继续。请参阅表 5-11。

表 5-7. 常规属性

属性	说明
用户 ID	包含 16 个预置用户 ID 编号之一。此字段不能编辑。
启用用户	选中后表示用户到 iDRAC 的权限已启用。取消选取后, 用户的权限会被禁用。
"Username" (用户名)	指定一个 iDRAC 用户名, 最多 16 个字符。每个用户必须具有唯一用户名。 注: iDRAC 上的用户名不能包含 / (正斜杠) 或 . (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。
"Change Password" (更改密码)	启用"New Password" (新密码) 和"Confirm New Password" (确认新密码) 字段。取消选取时, 无法更改用户的密码。
"New Password" (新密码)	启用编辑 iDRAC 用户密码。输入多达 20 个字符的"Password" (密码)。这些字符将不会显示。
"Confirm New Password" (确认新密码)	重新输入 iDRAC 用户的密码以进行确认。

表 5-8. IPMI LAN 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: None (无)、Administrator (管理员)、Operator (操作员) 或 User (用户)。
启用 LAN 上串行	允许用户使用"Serial over LAN " (LAN 上 IPMI 串行)。选取后, 将启用此权限。

表 5-9. iDRAC 用户权限

属性	说明
iDRAC 组	指定用户的最大 iDRAC 用户权限为以下之一: Administrator (管理员)、Power User (高级用户)、Guest User (客用户)、Custom (自定义) 或 None (无)。 请参阅 表 5-10 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。
配置用户	使用户可以允许特定用户访问系统。
清除日志	允许用户清除 iDRAC 日志。
执行服务器控制命令	允许用户执行 RACADM 命令。
访问控制台重定向	允许用户运行控制台重定向。
访问虚拟介质	允许用户运行和使用虚拟介质。
检测警报	允许用户将测试警报 (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 5-10. iDRAC 组权限

用户组	授予的权限
管理员	"Login to iDRAC" (登录到 iDRAC)、"Configure iDRAC" (配置 iDRAC)、"Configure Users" (配置用户)、"Clear Logs" (清除日志)、"Execute Server Control Commands" (执行服务器控制命令)、"Access 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)
高级用户	"Login to iDRAC" (登录到 iDRAC)、"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)

客用户	"Login to iDRAC" (登录到 iDRAC)
"Custom" (自定义)	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)
无	没有分配权限

表 5-11. 用户配置页按钮

按钮	措施
"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。
"Apply" (应用)	保存用户配置页上所做的任何新设置。
"Go Back To Users Page" (返回到用户页)	返回"Users Page" (用户页)。

使用 SSL 和数字认证确保 iDRAC 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:

- 1 安全套接字层 (SSL)
- 1 认证签名请求 (CSR)
- 1 访问 SSL 主菜单
- 1 生成新 CSR
- 1 上传服务器认证
- 1 查看服务器认证

安全套接字层 (SSL)

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

启用 SSL 的系统可以执行以下任务:

- 1 向启用 SSL 的客户端验证自身
- 1 允许客户端向服务器验证自身
- 1 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。iDRAC 使用 128 位 SSL 加密标准, 北美互联网浏览器常用的最安全加密方式。

默认情况下, iDRAC Web 服务器包括 Dell 自我签名的 SSL 数字证书 (服务器 ID)。为确保因特网的高安全性, 使用公认证机构签署的认证更换 Web Server SSL 认证。要开始获取签署认证, 可以使用 iDRAC Web 界面提供公司信息来生成认证签名请求 (CSR)。可以随后将生成的 CSR 提交给 CA, 比如 VeriSign 或 Thawte。

认证签名请求 (CSR)

CSR 是认证机构 (CA) 对安全服务器认证的数字请求。安全服务器认证使服务器客户机能够信任所选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, Thawte 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 将向申请者颁发数字签名的认证, 以在通过网络和因特网进行事务处理时唯一标识该申请者。

CA 批准了 CSR 并向用户颁发认证后, 应将认证上载到 iDRAC 固件。iDRAC 固件上存储的 CSR 信息必须与认证中包含的信息一致。

访问 SSL 主菜单

1. 单击"System" (系统) → "Remote Access" (远程访问) → iDRAC, 然后单击"Network/Security" (网络/安全性) 选项卡。
2. 单击 SSL 打开"SSL Main Menu" (SSL 主菜单) 页。

使用"SSL Main Menu" (SSL 主菜单) 页生成准备发送给 CA 的 CSR。CSR 信息存储在 iDRAC 固件中。

[表 5-12](#) 说明了生成 CSR 时可用的选项。

表 5-13 说明了 SSL 主菜单页上的可用按钮。

表 5-12. SSL 主菜单选项

字段	说明
"Generate a New Certificate Signing Request (CSR)" (生成新的认证签名请求 [CSR])	选择选项并单击"Next" (下一步) 打开"Generate Certificate Signing Request (CSR)" (生成认证签名请求 [CSR]) 页。 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 返回的认证匹配。
"Upload Server Certificate" (上传服务器认证)	选择选项并单击"Next" (下一步) 打开"Certificate Upload" (认证上传) 页并上传 CA 发送给您的认证。 注: 只有 X509, Base 64 编码认证才能被 iDRAC 接受。不接受 DER 编码认证。
"View Server Certificate" (查看服务器认证)	选择选项并单击"Next" (下一步) 打开"View Server Certificate" (查看服务器认证) 页并查看现有的服务器认证。

表 5-13. SSL 主菜单按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"SSL Main Menu" (SSL 主菜单) 值。
"Refresh" (刷新)	重载"SSL Main Menu" (SSL 主菜单) 页。
Next	处理"SSL Main Menu" (SSL 主菜单) 页上的信息并继续下一步。

生成新的认证签名请求

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

- 在 SSL 主菜单页上选择 "Generate a New Certificate Signing Request (CSR)" (生成新的认证签名请求 [CSR]), 并单击"Next" (下一步)。
- 在生成认证签名请求 (CSR) 页上输入每个 CSR 属性值。

[表 5-14](#)说明了生成认证签名请求 (CSR) 页选项。
- 单击"Generate" (生成) 创建 CSR。
- 单击"Download" (下载) 将 CSR 文件保存到本地计算机。
- 单击相应按钮继续。请参阅[表 5-15](#)。

表 5-14. 生成认证签名请求 (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、下划线和句点有效。空格无效。
"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)	认证实体的城市或其它位置 (例如, 朗得洛克 [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。
国家和地区代码	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 5-15. 生成认证签名请求 (CSR) 页按钮

--	--

按钮	说明
"Print" (打印)	打印屏幕上显示的"Generate Certificate Signing Request" (生成认证签名请求) 值。
"Refresh" (刷新)	重载"Generate Certificate Signing Request" (生成认证签名请求) 页。
"Generate" (生成)	生成 CSR 并随后提示用户保存到指定目录。
"Download" (下载)	下载认证到本地计算机。
"Go Back to SSL Main Menu" (返回 SSL 主菜单)	使用户返回到"SSL Main Menu" (SSL 主菜单) 页。

上传服务器认证

1. 在 SSL 主菜单项中选择"Upload Server Certificate" (上传服务器认证) 并单击"Next" (下一步)。

显示"Certificate Upload" (认证上传) 页。

2. 在"File Path" (文件路径) 字段中, 键入认证的路径或单击"Browse" (浏览) 导航到认证文件。

 **注:** "File Path" (文件路径) 值显示上传的认证的相对文件路径。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. 单击相应按钮继续。请参阅表 5-16。

表 5-16. 认证上传页按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"Certificate Upload" (认证上传) 值。
"Refresh" (刷新)	重新加载"Certificate Upload" (认证上传) 页。
"Apply" (应用)	应用认证到 iDRAC 固件。
"Go Back to SSL Main Menu" (返回 SSL 主菜单)	使用户返回到"SSL Main Menu" (SSL 主菜单) 页。

查看服务器认证

1. 在 SSL 主菜单项中选择"View Server Certificate" (查看服务器认证) 并单击"Next" (下一步)。

[表 5-17](#) 说明认证窗口中列出的字段及相关说明。

2. 单击相应按钮继续。请参阅表 5-18。

表 5-17. 认证信息

字段	说明
"Serial Number" (序列号)	认证序列号
"Subject Information" (主题信息)	按照主题输入的认证属性
"Issuer Information" (颁发者信息)	按照颁发者返回的认证属性
"Valid From" (有效期至)	认证的颁发日期
"Valid To" (有效期至)	认证的期满日期

表 5-18. 查看服务器认证页按钮

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

配置和管理 Active Directory 认证

 **注：** 您必须具有“Configure iDRAC”（配置 iDRAC）权限才能配置 Active Directory 以及上传、下载和查看 Active Directory 认证。

 **注：** 有关 Active Directory 配置和如何配置标准架构和扩展架构的 Active Directory 的详情，请参阅[将 iDRAC 用于 Microsoft Active Directory](#)。

访问 Active Directory 主菜单：

1. 单击“System”（系统）→ “Remote Access”（远程访问）→ iDRAC，然后单击“Network/Security”（网络/安全性）选项卡。
2. 单击 Active Directory 打开“Active Directory Main Menu”（Active Directory 主菜单）页。

[表 5-19](#)列出 Active Directory 主菜单页选项。

3. 单击相应按钮继续。请参阅表 5-20。

表 5-19. Active Directory 主菜单页选项

字段	说明
"Configure Active Directory"（配置 Active Directory）	配置 Active Directory "ROOT Domain Name"（ROOT 域名）、"Active Directory Authentication Timeout"（Active Directory 验证超时）、"Active Directory Schema Selection"（Active Directory 架构选择）、"iDRAC Name"（iDRAC 名称）、"iDRAC Domain Name"（iDRAC 域名）、"Role Groups"（角色组）、"Group Name"（组名）和"Group Domain"（组域）设置。
"Upload Active Directory CA Certificate"（上传 Active Directory CA 认证）	将 Active Directory 认证上传到 iDRAC。
"Download iDRAC Server Certificate"（下载 iDRAC 服务器认证）	Windows Download Manager 将 iDRAC 服务器认证下载到系统。
"View Active Directory CA Certificate"（查看 Active Directory CA 认证）	显示已上传到 iDRAC 的 Active Directory 认证。

表 5-20. Active Directory 主菜单页按钮

按钮	定义
"Print"（打印）	打印屏幕上显示的“Active Directory Main Menu”（Active Directory 主菜单）页。
"Refresh"（刷新）	重新加载“Active Directory Main Menu”（Active Directory 主菜单）页。
Next	处理“Active Directory Main Menu”（Active Directory 主菜单）页上的信息并继续下一步。

配置 Active Directory（标准架构和扩展架构）

1. 在 Active Directory 主菜单页中选择“Configure Active Directory”（配置 Active Directory）并单击“Next”（下一步）。
2. 在“Active Directory Configuration”（Active Directory 配置）页上，输入 Active Directory 设置。
[表 5-21](#)说明了“Active Directory Configuration and Management”（Active Directory 配置和管理）页设置。
3. 单击“Apply”（应用）保存设置。
4. 单击相应按钮继续。请参阅[表 5-22](#)。
5. 要配置 Active Directory 标准架构角色组，单击各个角色组（1-5）。请参阅[表 5-23](#)和[表 5-24](#)。

 **注：** 要保存 Active Directory 配置页上的设置，单击“Apply”（应用），然后再进入自定义角色组页。

表 5-21. Active Directory 配置页设置

设置	说明
"Enable Active Directory"（启用 Active	选中后，启用 Active Directory。默认为“Disabled”（已禁用）。

Directory)	
"ROOT Domain Name" (ROOT 域名)	Active Directory ROOT 域名。此默认为空白。 名称必须是 x.y 格式的有效域名, 其中 x 是 1-254 个字符的 ASCII 字符串, 字符之间没有空格, 而 y 是有效域类型, 例如 com、edu、gov、int、mil、net 或 org。默认为空白。
"Timeout" (超时)	等待 Active Directory 查询完成的秒数。最小值等于或大于 15 秒。默认设置为 120。
"Use Standard Schema" (使用标准架构)	使用 Active Directory 标准架构
"Use Extended Schema" (使用扩展架构)	使用 Active Directory 扩展架构。
"iDRAC Name" (iDRAC 名称)	唯一识别 Active Directory 中 iDRAC 的名称。此默认为空白。 名称必须是 1-254 个字符的 ASCII 字符串, 字符之间没有空格。
"iDRAC Domain Name" (iDRAC 域名)	Active Directory iDRAC 对象所在的域的 DNS 名称。此默认为空白。 名称必须是 x.y 格式的有效域名, 其中 x 是 1-254 个字符的 ASCII 字符串, 字符之间没有空格, 而 y 是有效域类型, 例如 com、edu、gov、int、mil、net 或 org。
"Role Groups" (角色组)	iDRAC 相关角色组列表。 要更改角色组的设置, 在角色组列表中单击角色组编号。
"Group Name" (组名称)	标识 iDRAC 相关 Active Directory 角色组的名称。此默认为空白。
"Group Domain" (组域)	角色组所在的域类型。

表 5-22. Active Directory 配置页按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"Active Directory Configuration" (Active Directory 配置) 值。
"Refresh" (刷新)	重新加载"Active Directory Configuration" (Active Directory 配置) 页。
"Apply" (应用)	保存 "Active Directory Configuration" (Active Directory 配置) 页上所做的任何新设置。
"Go Back to Active Directory Main Menu" (返回到 Active Directory 主菜单)	返回 "Active Directory Main Menu" (Active Directory 主菜单) 页。

表 5-23. 角色组权限

设置	说明
"Role Group Privilege Level" (角色组权限级别)	指定用户的最大 iDRAC 用户权限为以下之一: Administrator (管理员)、Power User (高级用户)、Guest User (客用户)、None (无) 或 Custom (自定义)。 请参阅表 5-24 了解"Role Group" (角色组) 权限
"Login to iDRAC" (登录到 iDRAC)	允许组登录 iDRAC。
"Configure iDRAC" (配置 iDRAC)	授予配置 iDRAC 的组权限。
"Configure Users" (配置用户)	授予配置用户的组权限。
"Clear Logs" (清除日志)	授予清除日志的组权限。
"Execute Server Control Commands" (执行服务器控制命令)	授予执行服务器控制命令的组权限。
"Access Console Redirection" (访问控制台重定向)	允许组进行控制台重定向。
"Access Virtual Media" (访问虚拟介质)	允许组访问虚拟介质。
"Test Alerts" (检测警报)	允许组将测试警报 (电子邮件或 PET) 发送到特定用户。
"Execute Diagnostic Commands" (执行诊断命令)	授予执行诊断命令的组权限。

表 5-24. 角色组权限

属性	说明
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)
高级用户	"Login to iDRAC" (登录到 iDRAC)、"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)
客用户	"Login to iDRAC" (登录到 iDRAC)
"Custom" (自	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

定义)	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)
无	没有分配权限

上载 Active Directory CA 认证

1. 在"Active Directory Main Menu" (Active Directory 主菜单) 页中选择"Upload Active Directory CA Certificate" (上载 Active Directory CA 认证) 并单击"Next" (下一步)。
2. 在认证上载页"File Path" (文件路径) 字段中, 键入认证的文件路径或单击"Browse" (浏览) 导航至认证文件。

注: "File Path" (文件路径) 值显示上载的认证的相对文件路径。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。

确保域控制器的 SSL 认证得到同一个认证机构的签署且此认证在访问 iDRAC 的 management station 上可用。

3. 单击"Apply" (应用)。
4. 单击相应按钮继续。请参阅表 5-25。

表 5-25. 认证上载页按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"Certificate Upload" (认证上载) 值。
"Refresh" (刷新)	重新加载"Certificate Upload" (认证上载) 页。
"Apply" (应用)	应用认证到 iDRAC 固件。
"Go Back to Active Directory Main Menu" (退回到 Active Directory 主菜单)	返回 Active Directory 主菜单页。

下载 iDRAC 服务器认证

1. 在"Active Directory Main Menu" (Active Directory 主菜单) 页中选择"Download iDRAC Server Certificate" (下载 iDRAC 服务器认证) 并单击"Next" (下一步)。
2. 保存文件到系统上的目录。
3. 在"Download Complete" (下载完成) 窗口中单击"Close" (关闭)。

查看 Active Directory CA 认证

使用"Active Directory Main Menu" (Active Directory 主菜单) 页查看 iDRAC 的 CA 服务器认证。

1. 在"Active Directory Main Menu" (Active Directory 主菜单) 页中选择"View Active Directory CA Certificate" (查看 Active Directory CA 认证) 并单击"Next" (下一步)。

表 5-26 说明认证窗口中列出的字段及相关说明。

2. 单击相应按钮继续。请参阅表 5-27。

表 5-26. Active Directory CA 认证信息

字段	说明
"Serial Number" (序列号)	认证序列号
"Subject Information" (主题信息)	按照主题输入的认证属性。
"Issuer Information" (颁发者信息)	按照颁发者返回的认证属性。
"Valid From" (有效期自)	认证发出日期。
"Valid To" (有效期至)	认证有效日期。

表 5-27. 查看 Active Directory CA 认证页按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"Active Directory CA Certificate" (Active Directory CA 认证) 值。
"Refresh" (刷新)	重新加载"View Active Directory CA Certificate" (查看 Active Directory CA 认证) 页。
"Go Back to Active Directory Main Menu" (返回到 Active Directory 主菜单)	使用户返回到"Active Directory Main Menu" (Active Directory 主菜单) 页。

启用或禁用本地配置访问

 **注：** 本地配置访问的默认配置为"Enabled" (启用)。

启用本地配置访问

1. 单击System→Remote Access→iDRAC →"Network/Security" (网络/安全性)。
2. 在"Local Configuration" (本地配置) 下，单击以取消选中"Disable iDRAC local USER Configuration Updates" (禁用 iDRAC 本地 USER 配置更新) 启用访问。
3. 单击"Apply" (应用)。
4. 单击相应按钮继续。

禁用本地配置访问

1. 单击"System" (系统) →"Remote Access" (远程访问) → iDRAC →"Network/Security" (网络/安全性)。
2. 在"Local Configuration" (本地配置) 下，单击以选中"Disable iDRAC local USER Configuration Updates" (禁用 iDRAC 本地 USER 配置更新) 禁用访问。
3. 单击"Apply" (应用)。
4. 单击相应按钮继续。

配置 LAN 上串行

1. 单击System→ Remote Access→ iDRAC→ "Network/Security" (网络安全)。
2. 单击"Serial Over LAN" (LAN 上串行) 打开"Serial Over LAN Configuration" (LAN 上串行配置) 页。
[表 5-28](#) 提供关于 "Serial Over LAN Configuration" (LAN 上串行配置) 页设置的信息。
3. 单击"Apply" (应用)。
4. 如果需要，配置高级设置。否则，单击相应按钮继续 (请参阅[表 5-29](#))。
要配置高级设置，请执行以下步骤：
 - a. 单击"Advanced Settings" (高级设置)。
 - b. 在"Serial Over LAN Configuration Advanced Settings" (LAN 上串行配置高级设置) 页中配置所需的高级设置 (请参阅[表 5-30](#))。
 - c. 单击"Apply" (应用)。
 - d. 单击相应按钮继续 (请参阅[表 5-31](#))。

表 5-28. LAN 上串行配置页设置

设置	说明

"Enable Serial Over LAN" (启用 LAN 上串行)	选中后, 复选框表示 LAN 上串行已启用。
"Baud Rate" (波特率)	表示数据速度。选择数据速度 19.2 kbps、57.6 kbps 或 115.2 kbps。

表 5-29. LAN 上串行配置页按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"Serial Over LAN Configuration" (LAN 上串行配置) 值。
"Refresh" (刷新)	重新载入"Serial Over LAN Configuration" (LAN 上串行配置) 页。
"Advanced Settings" (高级设置)	打开 "Serial Over LAN Configuration Advanced Settings" (LAN 上串行配置高级设置) 页。
"Apply" (应用)	查看"Serial Over LAN Configuration" (LAN 上串行配置) 页时保存所作的任何新设置。

表 5-30. LAN 上串行配置高级设置页设置

设置	说明
"Character Accumulate Interval" (字符积累间隔时间)	iDRAC 传输部分 SOL 字符数据信息包前等待时间。该时间按秒衡量。
"Character Send Threshold" (字符发送阈值)	只要接收到此数量 (或大于此数量) 的字符, iDRAC 就会发送包含这些字符的 SOL 字符数据信息包。阈值按字符衡量。

表 5-31. LAN 上串行配置高级设置页按钮

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

配置 iDRAC 服务

-  **注:** 要修改这些设置, 必须具有"Configure iDRAC" (配置 iDRAC) 权限。
-  **注:** 向服务应用更改时, 更改会立即生效。现有连接可能会没有警告而终止。
-  **注:** Microsoft Windows 附带的远程登录客户端与 BMU 通信时存在一个已知的问题。使用其它远程登录客户端, 例如 HyperTerminal 或 PuTTY。

1. 单击 System→ Remote Access→ iDRAC, 然后单击 "Network/Security" (网络/安全性) 选项卡。
2. 单击"Services" (服务) 打开"Services" (服务) 配置页。
3. 根据需要配置以下服务:
 - 1 Web server — 请参阅表 5-32 了解 Web server 设置
 - 1 SSH — 请参阅表 5-33 了解 SSH 设置
 - 1 Telnet — 请参阅表 5-34 了解 telnet 设置
 - 1 Automated System Recovery Agent — 请参阅表 5-35 了解 Automated System Recovery Agent 设置
4. 单击"Apply" (应用)。
5. 单击相应按钮继续。请参阅表 5-36。

表 5-32. Web 服务器设置

设置	说明
"Enabled" (已启用)	启用或禁用 iDRAC Web Server。选中后, 复选框表示 web server 已启用。默认"enabled" (已启用)。

"Max Sessions" (最大会话)	此系统允许的最大同时会话数。此字段不可编辑。可以有四个并发会话。
"Current Sessions" (当前会话)	系统上当前会话数，小于等于"Max Sessions" (最大会话)。此字段不可编辑。
"Timeout" (超时)	允许连接保持闲置的秒数。达到超时时将取消会话。对超时设置的更改会立即生效并将重设 Web Server。超时范围为 60 至 1920 秒。默认设置为 300 秒钟。
"HTTP Port Number" (HTTP 端口号)	iDRAC 侦听浏览器连接的端口。默认为 80。
"HTTPS Port Number" (HTTPS 端口号)	iDRAC 侦听安全浏览器连接的端口。默认为 443。

表 5-33. SSH 设置

设置	说明
"Enabled" (已启用)	启用或禁用 SSH。选中后，表示 SSH 已启用。
"Max Sessions" (最大会话)	此系统允许的最大同时会话数。只支持一个会话。
"Active Sessions" (激活的会话)	系统上的当前会话数。
"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)	iDRAC 侦听 SSH 连接的端口。默认为 22。

表 5-34. Telnet 设置

设置	说明
"Enabled" (已启用)	启用或禁用 Telnet。选中后，telnet 已启用。
"Max Sessions" (最大会话)	此系统允许的最大同时会话数。只支持一个会话。
"Active Sessions" (激活的会话)	系统上的当前会话数。
"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 0。
"Port Number" (端口号)	iDRAC 侦听 telnet 连接的端口。默认为 23。

表 5-35. 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 5-36. 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 iDRAC 固件

 **注意：** 如果 iDRAC 固件出现损坏（如果 iDRAC 固件更新进程在完成前被中断则有可能发生），则可以使用 CMC 恢复 iDRAC。请参阅《CMC 固件用户指南》了解相关说明。

 **注：** 按默认，固件更新将保留当前 iDRAC 设置。在更新过程中，可以选择重设 iDRAC 配置为工厂默认值。如果设置配置为工厂默认值，外部网络访问会在更新完成后被禁用。必须使用 iDRAC 配置公用程序或 CMC Web 界面启用并配置网络。

1. 启动 iDRAC Web 界面。
2. 单击 System → Remote Access → iDRAC，然后单击"Update" (更新) 选项卡。

 **注：** 要更新固件，必须将 iDRAC 置于更新模式。在该模式中，iDRAC 会自动重设，即使取消更新进程。
3. 在"Firmware Update" (固件更新) 页上，单击"Next" (下一步) 开始更新过程。
4. 在"Firmware Update - Upload (page 1 of 4)" (固件更新 - 上传【第 1 页/共 4 页】) 窗口中，单击"Browse" (浏览) 或输入所下载固件映像的路径。

例如：

C:\Updates\V1.0\<映像名称>。

默认固件映像名称为 **firmimg.imc**。

5. 单击**"Next"（下一步）**。

- 1 该文件将被上传到 iDRAC。This may take several minutes to complete.（完成此过程可能需要几分钟。）

或

- 1 如果要终止固件升级过程，可在此时单击**"Cancel"（取消）**。单击**"Cancel"（取消）**将使 iDRAC 重设为正常工作模式。

1 在**"Firmware Update - Validation (page 2 of 4)"（固件更新 - 验证 [第 2 页/共 4 页]**）窗口中，您将看到对上载的映像文件进行的验证结果。

- 1 如果映像文件成功上载并通过所有验证检查，会出现一条说明固件映像已验证的信息。

或

- 1 如果映像未成功上载，或未能通过验证检查，则固件更新将返回到**"Firmware Update - Upload (page 1 of 4)"（固件更新 - 上载(第 1 页/共 4 页)**窗口。您可尝试再次升级 iDRAC 或单击**"Cancel"（取消）**将 iDRAC 重设为正常工作模式。

 **注：** 如果取消选择**"Preserve Configuration"（保留配置）**复选框，iDRAC 将会重设为默认设置。在默认设置中，LAN 已禁用。将不能登录到 iDRAC Web 界面。必须使用 CMC Web 界面或在 BIOS POST 期间通过 iDRAC 配置公用程序使用 iKVM 重新配置 LAN 设置。

7. 在默认情况下，**"Preserve Configuration"（保留配置）**复选框被勾选，以便在升级后将当前设置保留在 iDRAC 上。如果不想保留这些设置，则取消选择**"Preserve Configuration"（保留配置）**复选框。

8. 单击**"Begin Update"（开始更新）**开始升级过程。请不要中断升级过程。

9. 在**"Firmware Update - Updating (page 3 of 4)"（固件更新 - 更新 [第 3 页/共 4 页]**）窗口中，将看到升级状况。固件升级操作的进程以百分比形式衡量，将显示在**"Progress"（进程）**列中。

10. 一旦固件更新完成，**"Firmware Update - Update Results (page 4 of 4)"（固件更新 - 更新结果 [第 4 页/共 4 页]**）窗口将出现且 iDRAC 将自动重设。必须关闭当前浏览器窗口，再使用新的浏览器窗口重新连接到 iDRAC。

使用 CMC 恢复 iDRAC 固件

iDRAC 固件一般使用 iDRAC 工具更新，比如 iDRAC Web 界面，或者从 support.dell.com 下载的操作系统特定的更新软件包。

如果 iDRAC 固件出现损坏（如果 iDRAC 固件更新进程在完成前被中断则有可能发生），则可以使用 CMC Web 界面更新固件。

如果 CMC 检测到损坏的 iDRAC 固件，iDRAC 会列在 CMC Web 界面的**"Updatable Components"（可更新组件）**页。

 **注：** 请参阅《*CMC 固件用户指南*》了解使用 CMC Web 界面的说明。

要更新 iDRAC 固件，应执行下列步骤：

1. 从 support.dell.com 将最新的 iDRAC 固件下载到管理计算机上。
2. 登录到 CMC Web 界面。
3. 单击**系统树**中的**"Chassis"（机箱）**。
4. 单击**"Update"（更新）**选项卡。**"Updatable Components"（可更新组件）**页将会显示。如果可以从 CMC 恢复，带有可恢复 iDRAC 的服务器会包括在列表中。
5. 单击 **server-n**，其中 **n** 是要恢复 iDRAC 的服务器的编号。
6. 单击**"Browse"（浏览）**浏览到所下载的 iDRAC 固件映像，并单击**"Open"（打开）**。
7. 单击**"Begin Firmware Update"（开始固件更新）**。

将固件映像文件上载到 CMC 后，iDRAC 会用映像更新自己。

[目录](#)

将 iDRAC 用于 Microsoft Active Directory

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [扩展架构和标准架构的优缺点](#)
- [扩展架构 Active Directory 概述](#)
- [Active Directory 标准架构概述](#)
- [在域控制器上启用 SSL](#)
- [使用 Active Directory 登录到 iDRAC](#)
- [常见问题](#)

目录服务维护一个公用数据库，在其中存储用于在网络上控制用户、计算机、打印机和其它设备的所有必需信息。如果公司使用 Microsoft® Active Directory® 服务软件，则可以配置软件提供对 iDRAC 的访问，以允许控制和将 iDRAC 用户权限添加到 Active Directory 软件中的现有用户。

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

您可使用 Active Directory 定义 iDRAC 上的用户访问权限：您可使用采用 Dell 定义的 Active Directory 对象的扩展架构解决方案，或只采用 Active Directory 组对象的标准架构解决方案。

扩展架构和标准架构的优缺点

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

使用扩展架构解决方案的优势有：

- 1 所有权限控制对象都在 Active Directory 中。
- 1 非常自由地使用不同权限级别配置不同 iDRAC 卡上的用户权限。

使用标准架构解决方案的优势有：

- 1 无需架构扩展，因为标准架构只使用 Active Directory 对象。
- 1 Active Directory 端的配置简单。

扩展架构 Active Directory 概述

有三种方式启用 Active Directory 使用扩展架构：

- 1 iDRAC Web 界面（请参阅[通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC](#)）。
- 1 RACADM CLI 工具（请参阅[使用扩展架构 Active Directory 和 RACADM 配置 iDRAC](#)）。
- 1 SM-CLP 命令行（请参阅[使用扩展架构 Active Directory 和 SM-CLP 配置 iDRAC](#)）。

Active Directory 架构扩展

Active Directory 数据是属性和类的分布式数据库。Active Directory 架构包含确定可添加或包含在数据库中的数据类型的规则。用户类是数据库中存储的类的一个示例。一些示例用户类属性包括用户的名字、姓氏和电话号码等。公司可以通过添加自己独特的属性和类扩展 Active Directory 数据库以解决特定环境下的需求。Dell 扩展了该架构以包括属性和类，支持远程管理验证和授权。

每个添加到现有 Active Directory 架构的属性或类都必须定义一个唯一的 ID。要在整个行业中保证唯一的 ID，Microsoft 维护了一个 Active Directory 对象标识符 (OID) 数据库，从而在各公司向该架构添加扩展时能够保证唯一性并且相互不冲突。为扩展 Microsoft Active Directory 中的架构，对于我们添加到目录服务的属性和分类，Dell 收到唯一的 OID、唯一名称扩展以及唯一链接属性 ID，如[表 6-1](#)。

表 6-1. Dell Active Directory 对象标识符

Active Directory 服务分类	Active Directory OID
Dell 扩展	dell
Dell 基础 OID	1.2.840.113556.1.8000.1280
RAC LinkID 范围	12070 至 12079

RAC 架构扩展概览

为在各种客户环境中提供最大的灵活性，Dell 提供了一组属性，可以由用户根据所需结果进行配置。Dell 扩展了该架构以包括关联、设备和权限属性。关联属性用于将具有一组特定权限的用户或组与一个或多个 RAC 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、RAC 权限和 RAC 设备进行各种组合而无需增加太多的复杂性。

Active Directory 对象概览

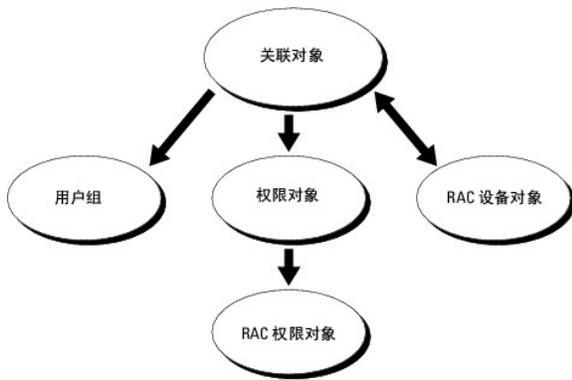
对于网络上每一个想与 Active Directory 集成以进行验证和授权的物理 RAC 来说，请创建至少一个关联对象和一个 RAC 设备对象。可以创建多个“关联”对象，每个“关联”对象都可以链接到任意多个用户、用户组或 RAC“设备”对象。用户和 RAC 设备对象可以是企业任何域中的成员。

不过，每个“关联”对象只能链接（或者可能链接用户、用户组或 RAC“设备”对象）到一个“权限”对象。此示例允许管理员控制特定 RAC 上的每个用户权限。

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

图 6-1 说明关联对象提供了进行所有验证和授权所需的连接。

图 6-1. Active Directory 对象的典型设置



注： RAC 权限对象适用于 DRAC 4 和 iDRAC。

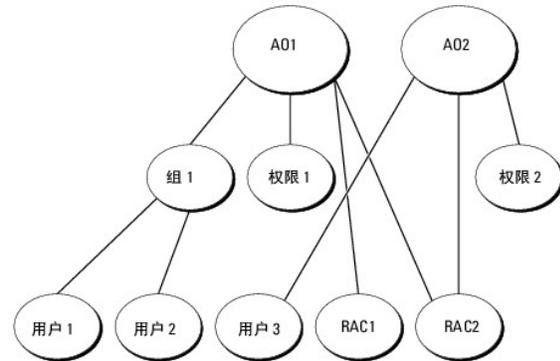
可以根据需要创建任意数量的关联对象。不过，对于网络上每一个想与 Active Directory 集成以使用 RAC (iDRAC) 验证和授权的 RAC 来说，必须创建至少一个“关联对象”和一个 RAC“设备对象”。

关联对象允许任意数量的用户和/或组以及 RAC 设备对象。然而，每个“关联”对象只有一个“权限”对象。“关联对象”连接那些对 RAC 具有“权限”的“用户”。

可以在一个域或多个域中配置 Active Directory 对象。例如，已有两个 iDRAC 卡 (RAC1 和 RAC2) 和三个 Active Directory 现有用户 (用户 1、用户 2 和用户 3)。想要授予用户 1 和用户 2 对两个 iDRAC 的管理员权限并授予用户 3 对 RAC2 卡的登录权限。图 6-2 显示了如何在此情况下设置 Active Directory 对象。

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

图 6-2. 在一个域中设置 Active Directory 对象



要为单个域情况配置对象，请执行以下任务：

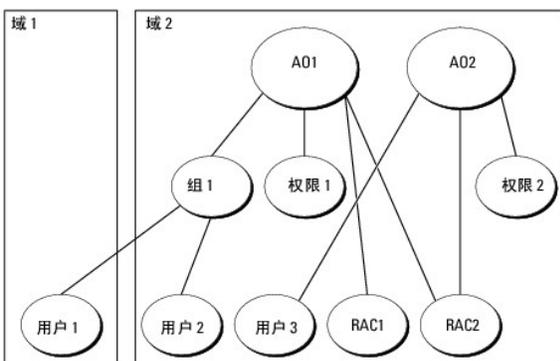
1. 创建两个关联对象。

2. 创建两个 RAC“设备对象”，RAC1 和 RAC2，用以代表两个 iDRAC。
3. 创建两个权限对象，权限 1 和权限 2，其中权限 1 具有所有权限（管理员），而权限 2 具有登录权限。
4. 将用户 1 和用户 2 归到组 1。
5. 将组 1 添加为关联对象 1 (AO1) 的成员，权限 1 作为 AO1 的权限对象，而 RAC1 和 RAC2 作为 AO1 中的 RAC 设备。
6. 将用户 3 添加为关联对象 2 (AO2) 的成员，权限 2 作为 AO2 的权限对象，而 RAC2 作为 AO2 中的 RAC 设备。

有关详细说明，请参阅[将 iDRAC 用户和权限添加到 Active Directory](#)。

[图 6-3](#) 提供多个域中 Active Directory 对象的示例。在这种情况下，已有两个 iDRAC (RAC1 和 RAC2) 和三个 Active Directory 现有用户 (用户 1、用户 2 和 用户 3)。用户 1 位于域 1 中，用户 2 和用户 3 位于域 2 中。在此情况下，配置用户 1 和用户 2 具有对两个 iDRAC 的管理员权限，配置用户 3 具有对 RAC2 卡的登录权限。

图 6-3. 在多个域中设置 Active Directory 对象



要为多个域情况配置对象，请执行以下任务：

1. 确保域目录林功能处在本机或 Windows 2003 模式。
 2. 在任何域中创建两个关联对象 AO1（通用范围）和 AO2。
- [图 6-3](#) 显示域 2 中的对象。
3. 创建两个 RAC“设备对象”，RAC1 和 RAC2，用以代表两个 iDRAC。
 4. 创建两个权限对象，权限 1 和权限 2，其中权限 1 具有所有权限（管理员），而权限 2 具有登录权限。
 5. 将用户 1 和用户 2 归到组 1。组 1 的组范围必须是通用。
 6. 将组 1 添加为关联对象 1 (AO1) 的成员，权限 1 作为 AO1 的权限对象，而 RAC1 和 RAC2 作为 AO1 中的 RAC 设备。
 7. 将用户 3 添加为关联对象 2 (AO2) 的成员，权限 2 作为 AO2 的权限对象，而 RAC2 作为 AO2 中的 RAC 设备。

配置扩展架构 Active Directory 访问 iDRAC

在使用 Active Directory 访问 iDRAC 之前，必须配置 Active Directory 软件和 iDRAC，方法是按照编号顺序执行下列步骤：

1. 扩展 Active Directory 架构（请参阅[“扩展 Active Directory 架构”](#)）。
2. 扩展 Active Directory 用户和计算机管理单元（请参阅[“安装 Dell 对 Active Directory 用户和计算机管理单元的扩展”](#)）。
3. 将 iDRAC 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 iDRAC Web 界面或 RACADM 配置 iDRAC Active Directory 属性（请参阅[“通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC”](#) 或 [“使用扩展架构 Active Directory 和 RACADM 配置 iDRAC”](#)）。

扩展 Active Directory 架构

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

可以使用以下方法之一扩展架构：

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

如果使用 LDIF 脚本，将不会把 Dell 组织单元添加到架构。

LDIF 文件和 Dell Schema Extender 分别位于 *Dell Systems Management Consoles* CD 的以下目录中：

- 1 *CD 驱动器:\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files*
- 1 *CD 驱动器:\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender*

要使用 LDIF 文件，请参阅 **LDIF_Files** 目录中自述文件中的说明。要使用 Dell Schema Extender 扩展 Active Directory 架构，请参阅 [“使用 Dell Schema Extender”](#)。

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

使用 Dell Schema Extender

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

1. 在“Welcome”（欢迎）屏幕中单击“Next”（下一步）。
2. 阅读并了解警告，单击“Next”（下一步）。
3. 选择“Use Current Log In Credentials”（使用当前登录凭据）或输入具有架构管理员权限的用户名和密码。
4. 单击“Next”（下一步）运行 Dell Schema Extender。
5. 单击 **Finish**（完成）。

架构将会扩展。要验证架构扩展，请使用 Microsoft 管理控制台 (MMC) 和 Active Directory 架构管理单元验证以下内容是否存在：

- 1 类（请参阅 [表 6-2](#) 到 [表 6-7](#)）
- 1 属性（[表 6-8](#)）

请参阅 Microsoft 说明文件详细了解如何在 MMC 中启用和使用 Active Directory 架构管理单元。

表 6-2. 添加到 Active Directory 架构的类的类定义

类名称	分配的对象标识号 (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 6-3. dellRacDevice 类

OID	1.2.840.113556.1.8000.1280.1.1.1.1
说明	表示 Dell RAC 设备。RAC 设备必须在 Active Directory 中配置为 dellRacDevice。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 6-4. dellAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.1.1.2
说明	表示 Dell 关联对象。关联对象提供用户和设备之间的连接。
类的类型	结构类
超类	组
属性	dellProductMembers dellPrivilegeMember

表 6-5. dellRAC4Privileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.3
说明	用于为 iDRAC 设备定义权限（授权权利）。
类的类型	辅助类
超类	无
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 6-6. dellPrivileges 类

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

表 6-7. dellProduct 类

OID	1.2.840.113556.1.8000.1280.1.1.1.5
说明	所有 Dell 产品派生所依据的主类。
类的类型	结构类
超类	计算机
属性	dellAssociationMembers

表 6-8. 添加到 Active Directory 架构的属性的列表

属性名称/说明	分配的 OID/语法对象标识符	单值
dellPrivilegeMember 属于此属性的 dellPrivilege 对象的列表。	1.2.840.113556.1.8000.1280.1.1.2.1 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers 属于此角色的 dellRacDevices 对象的列表。此属性是到 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置权限，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 当前架构版本用于更新架构。	1.2.840.113556.1.8000.1280.1.1.2.12 不区分大小写的字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType 此属性是 dellRacDevice 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 中的架构时，还必须扩展 Active Directory 用户和计算机管理单元以使管理员能够管理 RAC (iDRAC) 设备、用户和用户组、RAC 关联和 RAC 权限。

使用 *Dell Systems Management Consoles* CD 安装 systems management software 时，可以通过在安装过程中选择“**Dell Extension to the Active Directory User's and Computers Snap-In**”（到 Active Directory 用户和计算机管理单元的 Dell 扩展）选项来扩展管理单元。请参阅《*Dell OpenManage 软件快速安装指南*》进一步了解如何安装 Systems Management 软件。

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 RAC 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，应执行以下步骤：

1. 如果登录到域控制器，则单击"Start"（开始）→ "Admin Tools"（管理工具）→ "Active Directory Users and Computers"（Active Directory 用户和计算机）。
如果没有登录到域控制器上，则必须在本地系统上安装相应的 Microsoft Administrator Pack。要安装此 Administrator Pack，单击"Start"（开始）→ "Run"（运行），键入 MMC 并按 Enter。
Microsoft 管理控制台 (MMC) 显示。
2. 在"Console 1"（控制台 1）窗口中单击"File"（文件）（或"Console"（控制台），如果是运行 Windows 2000 的系统）。
3. 单击"Add/Remove Snap-in"（添加/删除管理单元）。
4. 选择"Active Directory Users and Computers"（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

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

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

创建 RAC 设备对象

1. 在"MMC Console Root"（MMC 控制台根目录）窗口中，右击一个容器。
2. 选择"New"（新建）→ "Dell RAC Object"（Dell RAC 对象）。
系统将显示"New Object"（新对象）窗口。
3. 为新对象键入名称。该名称必须与准备在["通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC"](#)的[步骤 a](#)中键入的 iDRAC 名称相同。
4. 选择"RAC Device Object"（RAC 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，右击一个容器。
2. 选择"New"（新建）→ "Dell RAC Object"（Dell RAC 对象）。
系统将显示"New Object"（新对象）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. 右击创建的权限对象并选择"Properties"（属性）。
7. 单击"RAC Privileges"（RAC 权限）选项卡并选择希望用户具有的权限（有关详情请参阅[iDRAC 用户权限](#)）。

创建关联对象

关联对象从组派生而来，必须包含组类型。关联范围为关联对象指定安全组类型。创建关联对象时，请选择适用于要添加对象的类型的关联范围。

例如，如果选择“Universal”（通用），则关联对象仅当 Active Directory 域以本机模式或更高模式运行时才可用。

1. 在“Console Root”（控制台根节点）(MMC) 窗口中，右击一个容器。
2. 选择“New”（新建）→“Dell RAC Object”（Dell RAC 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）。

将对象添加到关联对象

使用“Association Object Properties”（关联对象属性）窗口，可以关联用户或用户组、权限对象和 RAC 设备或 RAC 设备组。如果系统运行 Windows 2000 模式或更高模式，请使用通用组以跨越用户或 RAC 对象的域。

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

添加用户或用户组

1. 右击“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 RAC 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）选项卡将一个或多个 RAC 设备添加到关联。关联设备指定连接到网络的 RAC 设备，这些设备对于所定义的用户或用户组可用。可以将多个 RAC 设备添加到关联对象。

添加 RAC 设备或 RAC 设备组

要添加 RAC 设备或 RAC 设备组：

1. 选择“Products”（产品）选项卡并单击“Add”（添加）。
2. 键入 RAC 设备或 RAC 设备组名称并单击“OK”（确定）。
3. 在“Properties”（属性）窗口中单击“Apply”（应用），并单击“OK”（确定）。

通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC

1. 打开一个支持的 Web 浏览窗口。
2. 登录 iDRAC Web 界面。

3. 单击"System" (系统) → "Remote Access" (远程访问)。
4. 单击"Configuration" (配置) 选项卡并选择 Active Directory。
5. 在 Active Directory 主菜单项中选择"Configure Active Directory" (配置 Active Directory) 并单击"Next" (下一步)。
6. 在"Common Settings" (常用设置) 部分:
 - e. 选择"Enable Active Directory" (启用 Active Directory) 复选框。
 - f. 键入"Root Domain Name" (Root 域名)。**"Root Domain Name" (Root 域名)** 是目录林的完全限定 Root 域名。
 - g. 键入**超时**时间, 以秒为单位。
7. 在 Active Directory 架构选择部分单击"Use Extended Schema" (使用扩展架构)。
8. 在"Extended Schema Settings" (扩展架构设置) 部分:
 - a. 键入"DRAC Name" (DRAC 名称)。此名称必须与在域控制器中新建的 RAC 对象的常用名相同 (请参阅[创建 RAC 设备对象的步骤 3](#))。
 - b. 键入"DRAC Domain Name" (DRAC 域名) (例如 idrac.com)。请勿使用 NetBIOS 名称。**"DRAC Domain Name" (DRAC 域名)** 是 RAC 设备对象所在子域的完全限定域名。
9. 单击"Apply" (应用) 保存 Active Directory 设置。
10. 单击"Go Back To Active Directory Main Menu" (退回到 Active Directory 主菜单)。
11. 将域目录根 CA 认证上载到 iDRAC。
 - a. 选择"Upload Active Directory CA Certificate" (上载 Active Directory CA 认证) 单选按钮, 然后单击"Next" (下一步)。
 - b. 在"Certificate Upload" (认证上载) 页中键入认证的文件路径或浏览至认证文件。

 **注:** "File Path" (文件路径) 值显示上载的认证的相对文件路径。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。

域控制器的 SSL 认证应已得到根 CA 的签署。在访问 iDRAC 的 management station 上准备好根 CA 认证 (请参阅[导出域控制器根 CA 认证](#))。
 - c. 单击"Apply" (应用)。

iDRAC Web server 将在单击"Apply" (应用) 后自动重新启动。
12. 注销, 然后登录 iDRAC 以完成 iDRAC Active Directory 功能配置。
13. 单击"System" (系统) → "Remote Access" (远程访问)。
14. 单击"Configuration" (配置) 选项卡并单击"Network" (网络)。
15. 如果在"Network Settings" (网络设置) 下选择了"Use DHCP" (使用 DHCP) (用于 NIC IP 地址), 则选择"Use DHCP to obtain server address" (使用 DHCP 获取服务器地址)。

要手动输入 DNS 服务器 IP 地址, 取消选中"Use DHCP to obtain DNS server address" (使用 DHCP 获取 DNS 服务器地址) 并键入主要和备用 DNS 服务器 IP 地址。

16. 单击"Apply Changes" (应用更改)。

iDRAC 扩展架构 Active Directory 功能配置完成。

使用扩展架构 Active Directory 和 RACADM 配置 iDRAC

使用以下命令, 通过 RACADM CLI 工具而不是 Web 界面配置采用扩展架构的 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 cfgADRacDomain <rac-FQDN>
racadm config -g cfgActiveDirectory -o cfgADRootDomain <root-FQDN>
```

```
racadm config -g cfgActiveDirectory -o cfgADracName <RAC 常用名>

racadm sslcertupload -t 0x2 -f <根-CA-认证-TFTP-URI>

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

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. 按“Enter”（输入）完成 iDRAC Active Directory 功能配置。

使用扩展架构 Active Directory 和 SM-CLP 配置 iDRAC

 **注：** 必须运行 TFTP 服务器，从中检索根 CA 认证并向其保存 iDRAC 服务器认证。

使用以下命令用 SM-CLP 配置采用扩展架构的 iDRAC Active Directory 功能。

1. 使用 telnet 或 SSH 登录 iDRAC 并输入以下 SM-CLP 命令：

```
cd /system/spl/oem Dell_ adservice1

set enablestate=1

set oem Dell_ schematype=1

set oem Dell_ adracdomain=<rac-FQDN>

set oem Dell_ adrootdomain=<root-FQDN>

set oem Dell_ adracname=<RAC 常用名>

set /system1/spl/oem Dell_ ssl1 oem Dell_ certtype=AD

load -source <ActiveDirectory-certificate-TFTP-URI> /system1/spl/oem Dell_ ssl1

set /system1/spl/oem Dell_ ssl1 oem Dell_ certtype=SSL

dump -destination <DRAC-服务器-认证-TFTP-URI> /system1/spl/oem Dell_ ssl1
```

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 SM-CLP 命令：

```
set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oem Dell_ serversfromdhcp=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 SM-CLP 命令：

```
set /system1/spl/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oem Dell_ serversfromdhcp=0

set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesapl dnsserveraddress=<主-DNS-IP-地址>

set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesapl dnsserveraddress=<辅-DNS-IP-地址>
```

Active Directory 标准架构概览

如 [图 6-4](#) 中所示，为 Active Directory 集成使用标准架构需要在 Active Directory 和 iDRAC 上都进行配置。在 Active Directory 端，标准组对象用作角色组。具有 iDRAC 权限的用户将是该角色组的成员。为了授予该用户对特定 iDRAC 的权限，需要在特定 iDRAC 上配置角色组名称及其域名。与扩展架构解决方案不同，角色和权限级别定义在各个 iDRAC 上，而不是 Active Directory 中。每个 iDRAC 中可配置和定义多达五个角色组。[表 5-10](#) 显示了角色组的权限级别而 [表 6-9](#) 显示了默认角色组设置。

图 6-4. 使用 Microsoft Active Directory 和标准架构配置 iDRAC

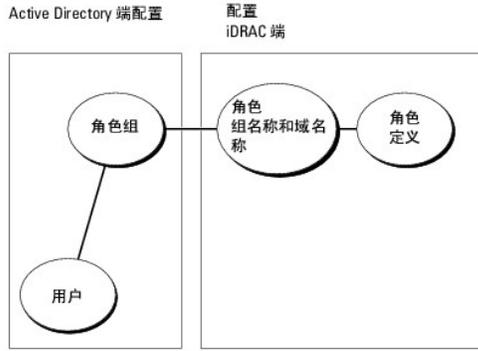


表 6-9. 默认角色组权限

默认权限级别	授予的权限	位掩码
管理员	"Login to iDRAC" (登录到 iDRAC)、"Configure iDRAC" (配置 iDRAC)、"Configure Users" (配置用户)、"Clear Logs" (清除日志)、"Execute Server Control Commands" (执行服务器控制命令)、"Access 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
高级用户	"Login to iDRAC" (登录到 iDRAC)、"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)	0x000000f9
客用户	"Login to iDRAC" (登录到 iDRAC)	0x00000001
无	没有分配权限	0x00000000
无	没有分配权限	0x00000000

注： 位掩码值只有在设置 RACADM 标准架构时才使用。

有两种方式启用 标准架构 Active Directory :

- 1 使用 iDRAC Web 用户界面。请参阅[用标准架构 Active Directory 和 Web 界面配置 iDRAC](#)。
- 1 用 RACADM CLI 工具。请参阅[使用标准架构 Active Directory 和 RACADM 配置 iDRAC](#)。

配置标准架构 Active Directory 访问 iDRAC

在 Active Directory 用户可以访问 iDRAC 前，需要执行下列步骤配置 Active Directory:

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。组名称和这个域的名称需要在 iDRAC 上使用 Web 界面、RACADM 或 SM-CLP 配置 (请参阅[用标准架构 Active Directory 和 Web 界面配置 iDRAC](#)或[用标准架构 Active Directory 和 RACADM 配置 iDRAC](#))。
3. 添加作为 Active Directory 组成员访问 iDRAC 的 Active Directory 用户。

用标准架构 Active Directory 和 Web 界面配置 iDRAC

1. 打开一个支持的 Web 浏览窗口。
2. 登录 iDRAC Web 界面。
3. 单击"System" (系统) → "Remote Access" (远程访问) ? iDRAC，然后单击"Configuration" (配置) 选项卡。
4. 选择 Active Directory 打开"Active Directory Main Menu" (Active Directory 主菜单) 页。
5. 在 Active Directory 主菜单中选择"Configure Active Directory" (配置 Active Directory) 并单击"Next" (下一步)。
6. 在"Common Settings" (常用设置) 部分:

- a. 选择"Enable Active Directory" (启用 Active Directory) 复选框。
 - b. 键入"Root Domain Name" (Root 域名)。**"Root Domain Name" (Root 域名)** 是目录林的完全限定 Root 域名。
 - c. 键入**超时**时间, 以秒为单位。
7. 在 Active Directory 架构选择部分单击"Use Standard Schema" (使用标准架构)。
8. 单击"Apply" (应用) 保存 Active Directory 设置。
9. 在标准架构设置部分的"Role Groups" (角色组) 列中, 单击"Role Group" (角色组)。
- "Configure Role Group" (配置角色组) 页将会显示, 其中包括角色组的"Group Name" (组名称)、"Group Domain" (组域) 和"Role Group Privileges" (角色组权限)。
10. 键入"Group Name" (组名称)。标识 iDRAC 关联的 Active Directory 角色组的名称。
11. 键入"Group Domain" (组域)。**"Group Domain" (组域)** 是目录林的完全限定 Root 域名。
12. 在"Role Group Privileges" (角色组权限) 页, 设置组权限。
- [表 5-10](#) (在 [page 72](#)上) 说明了"Role Group Privileges" (角色组权限)。
- 如果修改任何权限, 现有**角色组权限** (管理员、高级用户或客用户) 将会根据修改的权限更改为自定义组或相应**角色组权限**。
13. 单击"Apply" (应用) 保存角色组设置。
14. 单击"Go Back To Active Directory Configuration and Management" (退回到 Active Directory 配置和管理)。
15. 单击"Go Back To Active Directory Main Menu" (退回到 Active Directory 主菜单)。
16. 将域目录林根 CA 认证上载到 iDRAC。
- a. 选择"Upload Active Directory CA Certificate" (上传 Active Directory CA 认证) 单选按钮, 然后单击"Next" (下一步)。
 - b. 在"Certificate Upload" (认证上载) 页中键入认证的文件路径或浏览至认证文件。
-  **注:** "File Path" (文件路径) 值显示上载的认证的相对文件路径。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。
- 域控制器的 SSL 认证应已得到根 CA 的签署。在访问 iDRAC 的 management station 上准备好根 CA 认证 (请参阅 ["导出域控制器根 CA 认证"](#))。
- c. 单击"Apply" (应用)。
- iDRAC Web server 将在单击"Apply" (应用) 后自动重新启动。
17. 注销, 然后登录 iDRAC 以完成 iDRAC Active Directory 功能配置。
18. 单击"System" (系统) → "Remote Access" (远程访问)。
19. 单击"Configuration" (配置) 选项卡, 然后单击"Network" (网络)。
20. 如果在"Network Settings" (网络设置) 下选择了"Use DHCP" (使用 DHCP) (用于 NIC IP 地址), 则选择"Use DHCP to obtain DNS server address" (使用 DHCP 获取 DNS 服务器地址)。
- 要手动输入 DNS 服务器 IP 地址, 取消选中"Use DHCP to obtain DNS server address" (使用 DHCP 获取 DNS 服务器地址) 并键入主要和备用 DNS 服务器 IP 地址。
21. 单击"Apply Changes" (应用更改)。
- iDRAC 标准架构 Active Directory 功能配置完成。

使用标准架构 Active Directory 和 RACADM 配置 iDRAC

使用以下命令, 通过 RACADM CLI 工具而不是 Web 界面配置采用扩展架构的 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 cfgActiveDirectory -o cfgADRootDomain <root-FQDN>

racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupName <角色-组-常用-名称>

racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupDomain <RAC-FQDN>

racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupPrivilege <许可-位-掩码>

racadm sslcertupload -t 0x2 -f <根-CA-认证-TFTP-URI>

racadm sslcertdownload -t 0x1 -f <RAC-SSL-认证-TFTP-URI>

```

 **注：** 有关位掩码编号值，请参阅 [表 B-1](#)。

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>

```

使用标准架构 Active Directory 和 SM-CLP 配置 iDRAC

 **注：** 不能使用 SM-CLP 上载认证。而应使用 iDRAC Web 界面或本地 RACADM 命令。

使用以下命令用 SM-CLP 配置 iDRAC Active Directory 标准架构。

1. 使用 telnet 或 SSH 登录 iDRAC 并输入以下 SM-CLP 命令：

```

cd /system/spl/oem Dell_adservice1

set enablestate=1

set oem Dell_schematype=2

set oem Dell_adracdomain=<RAC-FQDN>

```

2. 分别为五个 Active Directory 角色组输入以下命令：

```

set /system1/spl/groupN oem Dell_groupname=<角色组 N 常用名>

set /system1/spl/groupN oem Dell_groupdomain=<rac-FQDN>

set /system1/spl/groupN oem Dell_groupprivilege=<用户-权限-位-掩码>

```

其中 N 是 1 到 5。

3. 输入以下命令设置 Active Directory SSL 认证。

```

set /system1/spl/oem Dell_ssl1 oem Dell_certtype=AD
load -source <ActiveDirectory-certificate-TFTP-URI> /system1/spl/oem Dell_ssl1

set /system1/spl/oem Dell_ssl1 oem Dell_certtype=SSL

dump -destination <iDRAC-服务器-认证-TFTP-URI> /system1/spl/oem Dell_ssl1

```

4. 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 SM-CLP 命令：

```

set /system1/spl/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oem Dell_serversfromdhcp=1

```

5. 如果 iDRAC 上已禁用 DHCP 或者想手动输入 DNS IP 地址，则键入以下 SM-CLP 命令：

```

set /system1/spl/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oem Dell_serversfromdhcp=0

```

```
set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesapl dnsserveraddress=<主-DNS-IP-地址>

set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesapl dnsserveraddress=<辅-DNS-IP-地址>
```

在域控制器上启用 SSL

如果使用 Microsoft Enterprise Root CA 将所有域控制器自动分配到 SSL 认证, 请执行下列步骤以在各个域控制器上启用 SSL。

1. 在域控制器上安装 Microsoft 企业根 CA。
 - a. 选择"Start" (开始) → "Control Panel" (控制面板) → "Add or Remove Programs" (添加或删除程序)。
 - b. 选择"Add/Remove Windows Components" (添加/删除 Windows 组件)。
 - c. 在"Windows Components Wizard" (Windows 组件向导) 中, 选择"Certificate Services" (认证服务) 复选框。
 - d. 选择"Enterprise root CA" (企业根 CA) 作为"CA Type" (CA 类型) 并单击"Next" (下一步)。
 - e. 输入"Common name for this CA" (此 CA 的常用名), 单击"Next" (下一步) 并单击"Finish" (完成)。
2. 通过安装每个控制器的 SSL 认证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, 右击"Automatic Certificate Request Settings" (自动认证申请设置) 并单击"Automatic Certificate Request" (自动认证申请)。
 - c. 在"Automatic Certificate Request Setup Wizard" (自动认证申请设置向导) 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)。

导出域控制器根 CA 认证

 **注:** 如果系统运行 Windows 2000, 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. 在运行字段中键入 mmc 并单击"OK" (确定)。
4. 在控制台 1 (MMC) 窗口中单击"File" (文件) 或在 Windows 2000 计算机上单击"Console" (控制台), 并选"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" (认证) 并单击"Add" (添加)。
7. 选择"Computer" (计算机) 帐户并单击"Next" (下一步)。
8. 选择"Local Computer" (本地计算机) 并单击"Finish" (完成)。
9. 单击 OK (确定)。
10. 在"Console 1" (控制台 1) 窗口中, 展开"Certificates" (认证) 文件夹, 展开"Personal" (个人) 文件夹并单击"Certificates" (认证) 文件夹。
11. 找到并右击根 CA 认证, 选择"All Tasks" (所有任务) 并单击"Export" (导出)。
12. 在"Certificate Export Wizard" (认证导出向导) 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) 并保存认证至系统上的目录。
15. 将保存在 [步骤 14](#) 中的认证上载到 IDRAC。

要使用 RACADM 上载认证, 请参阅 [通过扩展架构 Active Directory 使用 Web 界面配置 IDRAC](#)。

要使用 Web 界面上载认证，请执行下面的过程：

- a. 打开一个支持的 Web 浏览器窗口。
- b. 登录 iDRAC Web 界面。
- c. 单击"System"（系统）→ "Remote Access"（远程访问），然后单击"Configuration"（配置）选项卡。
- d. 单击"Security"（安全性）打开"Security Certificate Main Menu"（安全认证主菜单）页。
- e. 在安全认证主菜单页中选"Upload Server Certificate"（上传服务器认证）并单击"Apply"（应用）。
- f. 在认证上传屏幕中执行以下过程之一：
 - o 单击"Browse"（浏览）并选择认证。
 - o 在值字段中键入认证的路径。
- g. 单击"Apply"（应用）。

导入 iDRAC 固件 SSL 认证

使用下面的过程将 iDRAC 固件 SSL 认证导入到所有域控制器受信任的认证列表。

 **注：** 如果系统运行 Windows 2000，以下步骤可能不同。

 **注：** 如果 iDRAC 固件 SSL 认证是由公认的 CA 签署的，则不需要执行本节说明的步骤。

iDRAC SSL 认证就是用于 iDRAC Web Server 的认证。所有 iDRAC 都带有默认自签证书。

要使用 iDRAC Web 界面访问认证，选择"Configuration"（配置）→ Active Directory→ "Download iDRAC Server Certificate"（下载 iDRAC 服务器认证）。

1. 在域控制器上，打开"MMC Console"（MMC 控制台）窗口并选择"Certificates"（认证）→ "Trusted Root Certification Authorities"（受信任的根认证颁发机构）。
2. 右击"Certificates"（认证），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 认证文件。
4. 在每个域控制器的"Trusted Root Certification Authority"（受信任的根认证颁发机构）中安装 RAC SSL 认证。

如果已安装自己的认证，应确保签署您的认证的 CA 位于"Trusted Root Certification Authority"（可信根认证颁发机构）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 根据认证类型自动选择认证存储，或浏览到所选存储。
6. 单击"Finish"（完成）并单击"OK"（确定）。

使用 Active Directory 登录到 iDRAC

可以通过 Web 界面使用 Active Directory 登录 iDRAC。使用以下某一格式输入用户名：

<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。

常见问题

[表 6-10](#) 列出常见问题和解答。

表 6-10. 将 iDRAC 用于 Active Directory: 常见问题

问题	解答
是否可以使用 Active Directory 跨越多个树登录 iDRAC?	是。iDRAC 的 Active Directory 查询算法支持单个目录林中的多个树。
使用 Active Directory 登录到 iDRAC 的操作是否可以在混合模式下进行 (也就是说, 目录林中的域控制器运行着不同的操作系统, 比如 Microsoft Windows NT® 4.0、Windows 2000 或 Windows Server 2003) ?	是。在混合模式中, iDRAC 查询过程使用的所有对象 (比如用户、RAC 设备对象和关联对象) 都必须处于同一域中。 如果处于混合模式, Dell 扩展的 Active Directory 用户和计算机管理单元将会检查模式并限制用户以跨多个域创建对象。
将 iDRAC 用于 Active Directory 是否支持多个域环境?	是。域目录林功能级别必须处在本机 (Native) 或 Windows 2003 模式。此外, 关联对象、RAC 用户对象和 RAC 设备对象 (包括关联对象) 的组必须是通用组。
这些 Dell 扩展的对象 (Dell 关联对象、Dell RAC 设备和 Dell 权限对象) 是否可以位于不同的域?	关联对象和权限对象必须位于相同的域。Dell 扩展的 Active Directory 用户和计算机管理单元强制您在相同的域中创建这两个对象。其它对象可以位于不同的域。
域控制器 SSL 配置是否有任何限制?	是。目录林中的所有 Active Directory 服务器的 SSL 认证都必须由相同的根 CA 签署, 因为 iDRAC 只允许上传一个可信 CA SSL 认证。
我创建并上传了一个新 RAC 认证, 然而现在 Web 界面不启动。	如果使用 Microsoft Certificate Services 生成 RAC 认证, 有一种可能是您在创建认证时不小心选择了 "User Certificate" (用户认证), 而不是 "Web Certificate" (Web 认证)。 通过以下 racadm 命令从受管服务器使用 RACADM CLI 恢复、生成 CSR 并随后从 Microsoft Certificate Services 创建新的 Web 认证并进行加载: racadm sslcsrgen [-g] [-u] [-f {文件名}] racadm sslcertupload -t 1 -f {web_sslcert}
如果不能使用 Active Directory 验证登录到 iDRAC, 应该怎么办? 我如何排除这个故障?	<ol style="list-style-type: none"> 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 iDRAC 用户帐户, 请使用本地凭据登录 iDRAC。 <p>登录后, 执行以下步骤:</p> <ol style="list-style-type: none"> a. 确保已选中 "iDRAC Active Directory Configuration" (iDRAC Active Directory 配置) 页上的 "Enable Active Directory" (启用 Active Directory) 框。 b. 确保 iDRAC "Networking Configuration" (网络配置) 页上的 DNS 设置正确。 c. 确保已从 Active Directory 根 CA 将 Active Directory 认证上传到 iDRAC。 d. 检查域控制器 SSL 认证以确保没有过期。 e. 确保 "DRAC Name" (DRAC 名称)、"Root Domain Name" (Root 域名) 和 "DRAC Domain Name" (DRAC 域名) 与 Active Directory 环境配置相匹配。 f. 确保 iDRAC 密码最多有 127 个字符。虽然 iDRAC 可以支持多达 256 个字符的密码, Active Directory 只支持最大长度为 127 个字符的密码。

[目录](#)

查看 Managed Server 的配置和运行状况

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [System Summary \(系统摘要\)](#)
- [WWN/MAC 摘要](#)
- [系统运行状况](#)

System Summary (系统摘要)

单击 "System" (系统) → "Properties" (属性) → "Summary" (摘要) 获取有关系统主机柜和 Integrated Dell Remote Access Controller 的信息。

系统主机柜

系统信息

本部分 iDRAC Web 界面提供有关 Managed Server 的以下基本信息：

- 1 说明 — Managed Server 的型号或名称。
- 1 BIOS 版本 — Managed Server 的 BIOS 版本号。
- 1 服务标签 — Managed Server 的服务标签号码。
- 1 主机名 — 与 Managed Server 相关联的 DNS 主机名。
- 1 操作系统名称 — 安装在 Managed Server 上的操作系统名称。

I/O 夹层卡

本部分 iDRAC Web 界面提供有关安装在 Managed Server 上的 I/O 夹层卡和存储控制器插卡的以下信息：

- 1 IO 夹层卡 — 列出安装在 Managed Server 上的 I/O 夹层卡。
- 1 插卡类型 — 已安装的夹层卡/连接的物理类型。
- 1 型号名称 — 已安装的夹层卡的型号、类型或说明。
- 1 集成存储卡 — 已安装的存储控制器插卡的型号或名称。

自动恢复

本部分 iDRAC Web 界面详细介绍通过 Open Manage Server Administrator 设置的 Managed Server 自动恢复功能的当前工作模式：

- 1 恢复操作 — 当检测到系统故障或挂起时执行的操作。可选操作有 "No Action" (无操作)、"Hard Reset" (硬重置)、"Power Down" (关闭电源) 或 "Power Cycle" (循环加电)。
- 1 初始倒计时 — 检测到系统挂起后执行 iDRAC 恢复操作所需的时间 (以秒为单位)。
- 1 当前倒计时 — 倒计时计时器的当前值 (以秒为单位)。

Integrated Dell Remote Access Controller

iDRAC 信息

本部分 iDRAC Web 界面提供有关 iDRAC 自身的以下信息：

- 1 时期/时间 — iDRAC 的当前日期和时间 (即页面最后刷新时间)。
- 1 固件版本 — Managed Server 上安装的 iDRAC 固件的当前版本。
- 1 固件更新 — 上次成功更新 iDRAC 固件的日期和时间。
- 1 硬件版本 — Managed Server 主平面 (电路板) 的版本号。

- 1 IP 地址 — 与 iDRAC（并非 Managed Server）相关联的 IP 地址。
- 1 网关 — 为 iDRAC 配置的网络网关的 IP 地址。
- 1 子网掩码 — 为 iDRAC 配置的 TCP/IP 子网掩码。
- 1 MAC 地址 — 与 iDRAC 的 LOM（母板上的 LAN）网络接口控制器相关联的 MAC 地址。
- 1 DHCP 已启用 — 如果 iDRAC 设置为从 DHCP 服务器获取其 IP 地址和相关信息则启用。
- 1 首选 DNS 地址 1 — 设置为当前活动的主要 DNS 服务器。
- 1 备用 DNS 地址 2 — 设置为备用 DNS 服务器地址。

 **注：** 此信息还可以从 iDRAC → "Properties"（属性） → "iDRAC Information"（iDRAC 信息）中获得。

WWN/MAC 摘要

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

系统运行状况

单击"System"（系统） → "Properties"（属性） → "Health"（运行状况）查看有关 iDRAC 和 iDRAC 监控组件的运行状况。在"Severity"（严重性）列显示每个组件的状态。有关状态图标及其含义的列表，请参阅表 14-3。单击"Component"（组件）列中的组件名称，了解有关该组件的更多详细信息。

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

iDRAC

iDRAC 信息页列出大量有关 iDRAC 的详细信息，例如运行状况、名称、固件版本和网络参数。还可以通过单击页面顶部相应的选项卡获得更多详细信息。

CMC

CMC 页面显示 Chassis Management Controller 的运行状况、固件版本和 IP 地址。也可以通过单击"Launch the CMC Web Interface"（启动 CMC Web 界面）按钮启动 CMC Web 界面。

电池

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

温度

"Temperature Probes Information"（温度探测器信息）页面显示机载环境温度探测器的状态和读数。显示"warning"（警告）或"failure"（故障）状态的最小和最大温度阈值，以及探测器的当前运行状况。

Voltages（电压）

"Voltage Probes Information"（电压探测器信息）页面显示电压探测器的状态和读数，这些信息将提供机载电压轨和 CPU 核心传感器的状态。

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

电源监控

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

- 1 电源监控 — 显示由 System Board Current Monitor 报告的服务器用电量（以瓦特为单位）。
- 1 电源跟踪统计 — 显示从上次重置"Measurement Start Time"（测量开始时间）开始系统所用电量的信息。
- 1 峰值统计 — 显示从上次重置"Measurement Start Time"（测量开始时间）开始系统用电峰值的信息。

CPU

"CPU Information" (CPU 信息) 页面报告 Managed Server 上每个 CPU 的运行状况。此运行状况是多个独立温度、电源和功能测试的累计信息。

POST

"Post Codes" (开机自检代码) 页显示引导 Managed Server 操作系统前，上次系统开机自检代码 (以十六进制表示)。

综合运行状况

"Misc Health" (综合运行状况) 页提供对以下系统日志的访问：

系统事件日志 — 显示 Managed System 发生的系统关键事件。

开机自检代码 — 显示引导 Managed Server 操作系统前，上次系统开机自检代码 (以十六进制表示)。

上次崩溃 — 显示最近一次的崩溃屏幕和时间。

引导捕获 — 提供前三次引导屏幕的回放。

 **注：** 此信息也可从"System" (系统) → "Properties" (属性) → "Logs" (日志) 中获得。

[目录](#)

[目录](#)

使用 GUI 控制台重定向

Integred Dell™ Remote Access Controller固件版本1.2
用户指南

- [概览](#)
- [使用控制台重定向](#)
- [使用 Video Viewer](#)
- [常见问题](#)

本节提供关于使用 iDRAC 控制台重定向功能的信息。

概览

iDRAC 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。使用控制台重定向，可以从一个位置控制一个或多个已启用 iDRAC 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，managed server 不会指示控制台已经重定向。

"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 managed server 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：

- 1 支持最多两个并发控制台重定向会话。两个会话同时查看同一个 managed server 控制台。
- 1 控制台重定向会话不应从 Managed System 上的 web 浏览器启动。
- 1 最低要求 1 MB/sec 可用网络带宽。

如果另一用户请求控制台重定向会话，第一位用户将收到通知并可选择拒绝访问、仅允许视频或完全共享访问。第二位用户也将被告知另一用户享有控制权。第一位用户必须在 30 秒内响应，否则将自动授予第二位用户完全访问权。两个会话同时处于活动状态时，每个用户均可在屏幕右上角看到消息，表明另一用户正在进行会话。不允许第三个活动的会话。如果第三位用户请求控制台重定向会话，访问将被拒绝并且不会中断第一位或第二位用户的会话。

如果第一位或第二位用户都不具有管理员权限，第一位用户的活动会话的终结将自动导致第二位用户的会话终结。

支持的屏幕分辨率和刷新率

[表 8-1](#) 列出了 managed server 上运行的控制台重定向会话支持的屏幕分辨率和相应的刷新率。

表 8-1. 支持的屏幕分辨率和刷新率

屏幕分辨率	刷新率 (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

配置 Management Station

要在 management station 上使用控制台重定向，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：
 - 1 [支持的 Web 浏览器](#)
 - 1 [配置支持的 Web 浏览器](#)

2. 如果使用 Firefox 或想使用 Internet Explorer 的 Java 查看器，则安装 Java Runtime Environment (JRE)。请参阅[安装 Java Runtime Environment \(JRE\)](#)。
3. 建议将显示器分辨率配置为 1280x1024 像素或更高。

注意： 如果有活动控制台重定向会话并且 iKVM 连接了较低分辨率的显示器，在本地控制台选择了服务器的情况下，可能会重设服务器控制台分辨率。如果服务器运行在 Linux 操作系统上，本地显示器上可能无法查看 X11 控制台。在 iKVM 上按 <Ctrl><Alt><F1> 会将 Linux 切换为文本控制台。

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，应执行下列步骤：

1. 单击“System”（系统），然后单击“Console”（控制台）选项卡。
2. 单击“Configuration”（配置）打开“Console Redirection Configuration”（控制台重定向配置）页。
3. 配置控制台重定向属性。表 8-2 说明控制台重定向的设置。
4. 完成后，单击“Apply”（应用）。
5. 单击相应按钮继续。请参阅表 8-3。

表 8-2. 控制台重定向配置属性

属性	说明
已启用	单击以启用或禁用“Console Redirection”（控制台重定向）。 “Checked”（选中）表示“Console Redirection”（控制台重定向）已启用。 “Unchecked”（取消选中）表示“Console Redirection”（控制台重定向）已禁用。 默认“enabled”（已启用）。
“Max Sessions”（最大会话）	显示可能的“Console Redirection”（控制台重定向）会话的最大数目，1 或 2。使用下拉菜单更改允许的“Console Redirection”（控制台重定向）会话的最大允许数目。默认为 2。
“Active Sessions”（激活的会话）	显示“Active Console”（活动控制台）会话数目。此字段为只读。
“Keyboard and Mouse Port Number”（键盘和鼠标端口号）	用于连接到“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。默认为 5900。
“Video Port Number”（视频端口号）	用于连接到“Console Redirection Screen Service”（控制台重定向屏幕服务）的网络端口号。如果其它程序正在使用默认端口，可能需要更改此设置。默认为 5901。
“Video Encryption Enabled”（视频加密已启用）	“Checked”（选中）表示视频加密已启用。进入该视频端口的所有通信量均被加密。 “Unchecked”（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。 默认为“Encrypted”（加密）。禁用加密可以提高较慢网络上的性能。
“Mouse Mode”（鼠标模式）	如果 managed server 运行在 Windows 操作系统上，选择 Windows。 如果服务器运行在 Linux 上，则选择 Linux。 如果服务器不是运行在 Windows 或 Linux 操作系统上，选择 “None”（无）。 默认为 Windows。
“Console Plug-In Type for IE”（IE 的控制台插件类型）	当在 Windows 操作系统上使用 Internet Explorer 时，用户可在以下查看器中进行选择： ActiveX - ActiveX 控制台重定向查看器 Java - Java 控制台重定向查看器 注： 根据 Internet Explorer 版本不同，可能需要关闭其它安全保护限制（请参阅 配置并使用虚拟介质 ）。 注： 客户机系统上必须装有 Java 运行时环境才能使用 Java 查看器。
“Disable Local Console”（禁用本地控制台）	选中表示在控制台重定向期间到 iKVM 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 managed server 的本地显示器上看到。

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 8-5 中的按钮在“Console Redirection Configuration”（控制台重定向配置）页上可用。

表 8-3. 控制台重定向配置页按钮

按钮	定义
"Print"（打印）	打印"Console Redirection Configuration"（控制台重定向配置）页
"Refresh"（刷新）	重载"Console Redirection Configuration"（控制台重定向配置）页
"Apply"（应用）	保存对控制台重定向所做的任何新设置。

在 SM-CLP 命令行界面配置控制台重定向

打开控制台重定向会话

打开控制台重定向会话时，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，应执行下列步骤：

1. 单击"System"（系统），然后单击"Console"（控制台）选项卡。
2. 在"Console Redirection"（控制台重定向）页中使用表 8-4 中的信息确保有一个控制台重定向会话可用。

如果希望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 8-4. 控制台重定向页信息

属性	说明
"Console Redirection Enabled"（控制台重定向已启用）	是/否
"Video Encryption Enabled"（视频加密已启用）	是/否
"Max Sessions"（最大会话）	显示支持的最大控制台重定向会话数
"Current Sessions"（当前会话）	显示当前活动控制台重定向会话数
"Mouse Mode"（鼠标模式）	显示当前生效的鼠标加速度。应根据 managed server 上安装的操作系统的类型选择"Mouse Acceleration"（鼠标加速度）模式。
"Console Plug-in Type"（控制台插件类型）	显示当前配置的插件类型。 ActiveX — 将启动 Active-X 查看器。在 Windows 操作系统上运行时，Active-X 查看器只能在 Internet Explorer 上工作。 Java — 将启动 Java 查看器。Java viewer 可在 Internet Explorer 等任何浏览器上使用。如果客户机运行的操作系统不是 Windows，必须使用 Java 查看器。如果在 Windows 操作系统上运行时使用 Internet Explorer 访问 iDRAC，则既可选择 Active-X 也可选择 Java 插件类型。
"Local Console"（本地控制台）	如果本地控制台没有已禁用，则没有选中。如果选中，控制台不能由任何人使用机箱上的 iKVM 连接访问。

 **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 8-5 中的按钮在“Console Redirection”（控制台重定向）页上可用。

表 8-5. 控制台重定向页按钮

按钮	定义
"Refresh"（刷新）	重载"Console Redirection Configuration"（控制台重定向配置）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 Configuration"（控制台重定向配置）页

3. 如果控制台重定向会话可用，则单击"Launch Viewer"（启动查看器）。

 **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 iDRAC，在 Dell Digital KVM Viewer 应用程序中显示远程系统的桌面。

4. 两个鼠标光标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。必须同步两个鼠标光标以使远程鼠标光标跟随本地鼠标光标。请参阅[同步鼠标光标](#)。

使用 Video Viewer

Video Viewer 在 management station 和 managed server 之间提供了一个用户界面，使用户能够从 management station 查看 managed server 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。

Video Viewer 提供了各种控制调整，比如颜色模式、鼠标同步、快照、键盘宏指令和虚拟介质访问。单击“**Help**”（帮助）了解有关这些功能的详情。

启动控制台重定向会话并且 Video Viewer 出现后，可能需要调整颜色模式并同步鼠标光标。

[表 8-6](#) 说明了查看器中可以使用的菜单选项。

表 8-6. Viewer 菜单栏选择

菜单项	项目	说明
视频	"Pause" (暂停)	临时暂停控制台重定向。
	"Resume" (恢复)	恢复控制台重定向。
	"Refresh" (刷新)	刷新查看器屏幕图像。
	"Capture Current Screen" (捕获当前屏幕)	捕获当前远程系统屏幕为 Windows 上的 .bmp 文件或 Linux 上的 .png 文件。将显示一个对话框，使您可以将文件保存到指定位置。
	"Full Screen" (全屏)	要将 Video Viewer 展开成全屏模式，从"Video" (视频) 菜单中选择"Full Screen" (全屏)。
	"Exit" (退出)	控制台使用结束并已注销后 (使用远程系统的注销步骤)，从"Video" (视频) 菜单中选择"Exit" (退出) 关闭"Video Viewer" (视频查看器) 窗口。
Keyboard (键盘)	按住右 Alt 键	选择此项，然后再键入想和右 <Alt> 键组合的键。
	"Hold Left Alt Key" (按住左 Alt 键)	选择此项，然后再键入想和左 <Alt> 键组合的键。
	"Left Windows Key" (左 Windows 键)	选择"Hold Down" (按住)，然后再键入想和左 Windows 键组合的字符。选择"Press and Release" (按住并松开) 发送左 Windows 按键。
	"Right Windows Key" (右 Windows 键)	选择"Hold Down" (按住)，然后再键入想和右 Windows 键组合的字符。选择"Press and Release" (按住并松开) 发送右 Windows 按键。
	"Macros" (宏)	在选择了宏或者输入为宏指定的热键之后，该操作将在远程系统上执行。Video Viewer 提供以下宏： <ul style="list-style-type: none"> 1 Ctrl-Alt-Del 1 Alt-Tab 1 Alt-Esc 1 Ctrl-Esc 1 Alt-空格 1 Alt-Enter 1 Alt-连字号 1 Alt-F4 1 PrtScn 1 Alt-PrtScn 1 F1 1 "Pause" (暂停) 1 Alt+m
	"Keyboard Pass-through" (键盘通过)	键盘通过模式可使客户机上所有键盘功能重定向到服务器。
鼠标	同步光标	"Mouse" (鼠标) 菜单使用户能够同步光标，以便将客户机上的鼠标重定向到服务器上的鼠标。
选项	"Color Mode" (颜色模式)	允许选择颜色深度提高网络性能。例如，如果正在从虚拟介质安装软件，可以选择最低的颜色深度 (3 位灰色)，因此控制台查看器可以使用较少的网络带宽，用更多的带宽从介质传输数据。 模式颜色可以设置为 15 位彩色、7 位彩色、4 位彩色、4 位灰色和 3 位灰色。
介质	虚拟介质向导	"Media" (介质) 菜单提供对虚拟介质向导的访问，使用户能够重定向到诸如以下的设备或映像： <ul style="list-style-type: none"> 1 软盘驱动器 1 CD 1 DVD 1 ISO 格式映像 1 USB 快擦写驱动器 <p>有关虚拟介质功能的信息，请参阅配置并使用虚拟介质。</p> <p>使用虚拟介质时必须保持 Console Viewer 窗口活动。</p>
帮助	无	激活"Help" (帮助) 菜单。

同步鼠标光标

使用控制台重定向连接到远程 PowerEdge 系统时，远程系统上的鼠标加速度可能与 Management Station 上的鼠标光标不同步，从而造成 Video Viewer 窗口中出现两个鼠标光标。

要同步鼠标指针，单击“Mouse”（鼠标）→“Synchronize cursor”（同步光标）或按 <Alt><M>。

“Synchronize cursor”（同步光标）菜单项是一个切换。确保菜单项旁边有复选标记以便光标同步活动。

使用 Red Hat® Linux® 或 Novell® SUSE® Linux 时，在启动查看器前务必为 Linux 配置鼠标模式。请参阅在 [iDRAC Web 界面中配置控制台重定向](#) 获得配置帮助。操作系统的默认鼠标设置用于在 iDRAC 控制台重定向屏幕中控制鼠标箭头。

禁用或启用本地控制台

使用 iDRAC Web 界面，可以配置 iDRAC 以禁用 iKVM 连接。当本地控制台已禁用后，一个黄色状况点会出现在服务器 (OSCAR) 列表中，表示控制台已在 iDRAC 中锁定。当本地控制台已启用，状况点会变绿。

如果想确定对 managed server 控制台有独占访问，必须在 **控制台重定向页** 上禁用本地控制台并重新配置“Max Sessions”（最大会话数）为 1。

 **注：** 除 PowerEdge SC1435 和 6950 以外的所有 x9xx PowerEdge 系统都支持本地控制台功能。

 **注：** 通过禁用（关闭）服务器上的本地视频，将禁用连接到 iKVM 的显示器、键盘和鼠标。

要禁用或启用本地控制台，应执行以下程序：

1. 在 management station 上打开一个支持的 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），单击“Console”（控制台）选项卡，然后单击“Configuration”（配置）。
3. 如果希望禁用服务器上的本地视频（关闭），在“Console Redirect Configuration”（控制台重定向配置）页中，选择“Disable Local Console”（禁用本地控制台）复选框并随后单击“Apply”（应用）。默认值为 OFF。
4. 如果希望启用（打开）服务器上的本地视频，在“Console Redirect Configuration”（控制台重定向配置）页中，取消选择“Disable Local Console”（禁用本地控制台）复选框，然后单击“Apply”（应用）。

“Console Redirection”（控制台重定向）页显示本地服务器视频的状态。

常见问题

[表 8-7](#) 列出常见问题和解答。

表 8-7. 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后可以启动新的远程控制台视频会话吗？	是。
为什么要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延迟吗？	没有，iDRAC 一收到本地视频打开请求，视频就立刻 打开 。
本地用户还可以关闭视频吗？	是的，本地用户可以使用 RACADM CLI（本地）关闭视频。
本地用户还可以打开视频吗？	否。本地控制台禁用后，本地用户的键盘和鼠标会禁用并且无法更改任何设置。
关闭本地视频是否也会关闭本地键盘和鼠标？	是。
关闭本地控制台是否会关闭远程控制台会话上的视频？	不会，打开关闭本地视频与远程控制台会话无关。
iDRAC 用户打开或关闭本地服务器视频需要什么权限？	任何具有 iDRAC 配置权限的用户都可以打开或关闭本地控制台。
如何获得本地服务器视频的最新状况？	该状况显示在 iDRAC Web 界面的“Console Redirection Configuration”（控制台重定向配置）页上。 RACADM CLI 命令 <code>racadm getconfig @Cg cfgRacTuning</code> 在对象 <code>cfgRacTuneLocalServerVideo</code> 中显示状态。 该状况还可以在 iKVM OSCAR 显示中看到。当本地控制台已启用后，绿色状况会出现在服务器名称旁边。已禁用后，黄色点表示本地控制台已被 iDRAC 锁定。
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。
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。检查区域并根据需要重设字符集。有关详情，请参阅在 Linux 中设置区域 。
为什么在载入 Windows 2000 操作系统时 managed server 上出现空白屏	managed server 没有正确的 ATI 视频驱动程序。必须使用 <i>Dell PowerEdge Installation and Server Management</i> CD 更新视频驱动程序。

幕?	
执行控制台重定向时，为什么鼠标在 DOS 中不同步?	Dell BIOS 仿真 PS/2 鼠标的驱动程序。根据设计，PS/2 鼠标为鼠标指针使用相对位置，这会造成同步的延迟。iDRAC 带有 USB 鼠标驱动程序，该驱动程序允许使用绝对位置并且能够提供更紧密的鼠标指针跟踪。即使 iDRAC 将 USB 的绝对鼠标位置传递给 Dell BIOS，BIOS 仿真程序依然会将其转换回相对位置，所以行为依旧。为解决此问题，在控制台重定向配置中将鼠标模式设置为 NONE (无) 。
为什么鼠标在 Linux 文本控制台下不同步?	虚拟 KVM 要求 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。 确保在"Mouse" (鼠标) 菜单中选中"Synchronize Mouse" (同步鼠标)。按 <Alt><M> 或选择"Mouse" (鼠标) →"Synchronize mouse" (同步鼠标) 以切换鼠标同步。同步启用后，复选标记会出现在"Mouse" (鼠标) 菜单选项的旁边。
为什么使用 iDRAC 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，将会收到一个 EMS 连接信息，需要您选择"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 managed server，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的 Num Lock 的状态?	当通过 iDRAC 访问时，management station 上的 Num Lock 指示灯不需要与远程服务器上的 Num Lock 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 managed server，会收到警告消息吗?	否。如果本地用户访问系统，两人都有系统控制权。
我需要多少带宽来运行控制台重定向会话?	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 运行控制台重定向的最低系统要求是多少?	Management Station 要求 Intel Pentium III 500 MHz 处理器和至少 256 MB 的 RAM。

[目录](#)

配置并使用虚拟介质

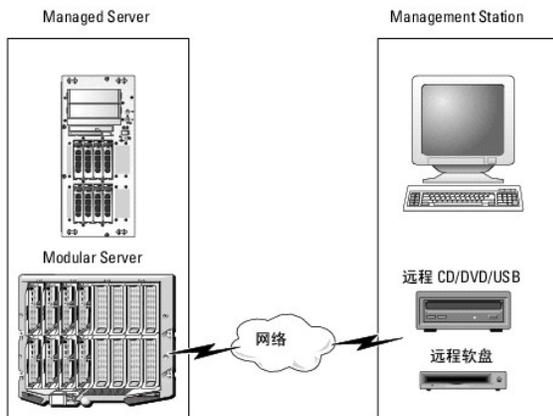
Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [概览](#)
- [配置虚拟介质](#)
- [运行虚拟介质](#)
- [常见问题](#)

概览

"Virtual Media" (虚拟介质) 功能, 可从控制台重定向查看器使用, 提供了 managed server 对网络上远程系统所选介质的访问。图 9-1 显示了 "Virtual Media" (虚拟介质) 的整体结构。

图 9-1. 虚拟介质的整体结构



使用 "Virtual Media" (虚拟介质), 管理员可以远程引导其 managed server, 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: "Virtual Media" (虚拟介质) 至少需要 128 Kbps 的可用网络带宽。

"Virtual Media" (虚拟介质) 为 managed server 的操作系统和 BIOS 定义了两种设备: 软盘设备和光盘设备。

Management Station 通过网络提供物理介质或映像文件。连接 "Virtual Media" (虚拟介质) 后, 来自 managed server 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 "Virtual Media" (虚拟介质) 与将介质插入物理设备看起来一样。没有连接虚拟介质时, managed server 上的虚拟设备就像两个没有介质的驱动器。

表 9-1 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 "Virtual Media" (虚拟介质) 会停止系统引导顺序。

表 9-1. 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 Management Station 上运行 "Virtual Media" (虚拟介质) 功能 (Management Station 运行 Microsoft® Windows® 操作系统), 请安装支持的带有 ActiveX 控件插件的 Internet Explorer (请参阅支持的 [Web 浏览器](#))。将浏览器安全性设置为中或更低设置以允许 Internet Explorer 下载和安装已签名的 ActiveX 控件。

根据 Internet Explorer 的版本, 可能需要自定义 ActiveX 的安全设置:

1. 启动 Internet Explorer。
2. 单击"Tools" (工具) → "Internet Options" (Internet 选项)，然后单击"Security" (安全) 选项卡。
3. 在"Select a Web content zone to specify its security settings" (选择 Web 内容区域以指定其安全设置) 中，单击选择所需的区域。
4. 在"Security level for this zone" (此区域的安全级别) 中，单击"Custom Level" (自定义级别)。

屏幕将显示"Security Settings" (安全设置) 窗口。

5. 在"ActiveX controls and plugins" (ActiveX 控件和插件) 中，确保将以下设置设置为"Enable" (启用)：
 - 1 允许脚本
 - 1 自动提示 ActiveX 控件
 - 1 下载已签名的 ActiveX 控件
 - 1 下载未签名的 ActiveX 控件
6. 单击"OK" (确定) 保存所有更改，并关闭"Security Settings" (安全设置) 窗口。
7. 单击"OK" (确定) 关闭"Internet Options" (Internet 选项) 窗口。
8. 重新启动 Internet Explorer。

必须具有管理员权限才能安装 ActiveX。安装 ActiveX 控件前，Internet Explorer 可能会显示一条安全警告。要完成 ActiveX 控件安装过程，必须在 Internet Explorer 显示安全警告提示时接受该控件。

基于 Linux 的 Management Station

要在运行 Linux 操作系统的 management station 上运行虚拟介质功能，请安装支持版本的 Firefox。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。

配置虚拟介质

1. 登录 iDRAC Web 界面。
2. 在导航树中选择"System" (系统) 并单击"Console" (控制台) 选项卡。
3. 单击"Configuration" (配置) → "Virtual Media" (虚拟介质) 以配置虚拟介质设置。
[表 9-2](#) 说明"Virtual Media" (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 9-3](#)。

表 9-2. 虚拟介质配置值

属性	值
"Attach Virtual Media" (连接虚拟介质)	Attach - 立刻将"Virtual Media" (虚拟介质) 附加到服务器。 Detach - 立刻从服务器上分离"Virtual Media" (虚拟介质)。 Auto-Attach - 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。
"Maximum Sessions" (最大会话)	显示"Virtual Media" (虚拟介质) 会话的最大允许数目。此值始终为 1。
"Active Sessions" (激活的会话)	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)	单击此复选框启用或禁用"Virtual Media" (虚拟介质) 连接上的加密。选中会启用加密；取消选取会禁用加密。
"Virtual Media Port Number" (虚拟介质端口号)	用于不加密连接到"Virtual Media" (虚拟介质) 服务的网络端口号。从指定端口号开始的两个连续端口用于连接到"Virtual Media" (虚拟介质) 服务。指定端口后面的端口号不能配置给其它 iDRAC 服务。默认为 3668。
"Virtual Media SSL Port Number" (虚拟	用于加密连接到"Virtual Media" (虚拟介质) 服务的网络端口号。从指定端口号开始的两个连续端口用于连接到"Virtual Media" (虚拟

拟介质 SSL 端口号)	介质) 服务。指定端口后面的端口号不能配置给其它 iDRAC 服务。默认为 3670。
"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 密钥驱动器。
"Enable Boot Once" (启用引导一次)	选中此复选框启用引导一次选项。服务器引导一次后, 此选项将自动终止"Virtual Media" (虚拟介质) 会话。此选项对于自动部署有用。

表 9-3. 虚拟介质配置页按钮

按钮	说明
"Print" (打印)	打印屏幕上显示的"Console Configuration" (控制台配置) 值。
"Refresh" (刷新)	重新载入"Console Configuration" (控制台配置) 页。
"Apply" (应用)	保存"Console Configuration" (控制台配置) 页上所做的任何新设置。

运行虚拟介质

- 🔔 **注意:** 运行"Virtual Media" (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。
- 🔔 **注意:** 访问虚拟介质时, Console Viewer 窗口应用程序必须保持活动。

- 在 management station 打开一个支持的 Web 浏览器。请参阅[支持的 Web 浏览器](#)。
- 启动 iDRAC Web 界面。访问[Web 界面](#)。
- 在导航树中选择"System" (系统) 并单击"Console" (控制台) 选项卡。

"Console Redirection" (控制台重定向) 页出现。如果要更改任何显示属性的值, 请参阅[配置虚拟介质](#)。

- 🔔 **注:** "Floppy Image File" (软盘驱动器) 下的"Floppy Drive" (软盘映像文件) (如果可用) 可能显示, 只要该设备可虚拟化为虚拟软盘。同时可以选择一个光盘驱动器和一个软盘, 或者单个驱动器。
- 🔔 **注:** managed server 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:** "Virtual Media" (虚拟介质) 可能无法在配置有 Internet Explorer Enhanced Security 的 Windows 操作系统客户端上正常运行。要解决此问题, 请参阅 Microsoft 操作系统说明文件或联络管理员。

- 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。

iDRACView 应用程序会以另外的窗口启动。

- 单击"Media" (介质) → "iVrtual Media Wizard..." (虚拟介质向导...)

介质重定向向导会出现。

- 查看状况窗口。如果介质已连接, 必须断开连接, 然后再连接到其它介质源。单击位于要断开连接的介质右侧的"Disconnect" (断开连接) 按钮。

- 选择位于希望连接的介质类型旁边的单选按钮。

可以在"Floppy/USB Drive" (软盘/USB 驱动器) 部分选择一个单选按钮, 在"CD/DVD Drive" (CD/DVD 驱动器) 部分选择一个。

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"Browse" (浏览) 按钮并浏览到映像。

- 单击各个所选介质类型旁边的"Connect" (连接) 按钮。

介质将会连接并且状况窗口将会更新。

- 单击"Close" (关闭) 按钮。

断开虚拟介质连接

- 单击"Media" (介质) → "iVrtual Media Wizard..." (虚拟介质向导...)

2. 单击希望断开连接的介质旁边的“Disconnect”（**断开连接**）。

介质将会断开连接并且状况窗口将会更新。

3. 单击 **Close**（**关闭**）。

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 managed server。
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其它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。

managed server 重新引导。

managed server 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非交互方法，可能需要数小时来完成。使用“Virtual Media”（**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：
 - 1 操作系统安装 CD 插入到 management station 的 CD 驱动器中。
 - 1 选择了本地 CD 驱动器。
 - 1 已与虚拟驱动器连接。
2. 按照[从虚拟介质引导](#)部分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。

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装入（如果已附加）并分配有驱动器号。

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装入。如果驱动器没有自动装入，则使用 Linux **mount** 命令手工装入驱动器。

常见问题

[表 9-4](#) 列出常见问题和解答。

表 9-4. 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连接中断。为什么？	<p>出现网络超时后，iDRAC 固件会断开连接，断开服务器和虚拟驱动器间的链接。</p> <p>如果虚拟介质配置设置在 iDRAC Web 界面或本地 RACADM 命令中更改，当配置更改应用后，任何所连介质都会断开连接。</p> <p>要重新连接虚拟驱动器，使用虚拟介质向导。</p>
哪些操作系统支持 iDRAC？	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 iDRAC？	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？	<ol style="list-style-type: none"> 1 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，如果更改客户端系统的 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。 1 出现网络超时后，iDRAC 固件会断开连接，断开服务器和虚拟驱动器间的链接。另外，有些人会在 Web 界面或输入 RACADM 命令变更虚拟介质配置设置。要重新连接虚拟驱动器，使用“Virtual Media”（虚拟介质）功能。
Windows 操作系统安装所用时间似乎太长了。为什么？	如果使用 <i>Dell PowerEdge Installation and Server Management</i> CD 和慢速网络连接安装 Windows 操作系统，安装程序可能因为网络延迟而需要更多时间访问 iDRAC Web 界面。虽然安装窗口没有显示安装进程，安装仍在进行。
我正在查看软盘驱动器或 USB 闪存盘的内容。如果尝试使用同一驱动器建立虚拟介质连接，我会收到连接故障消息并要求我重试。为什么？	不允许同时访问虚拟软盘驱动器。尝试虚拟化驱动器前，关闭用于查看驱动器内容的应用程序。
如何将虚拟设备配置为可引导设备？	在 managed server 上，访问 BIOS 设置并导航到引导菜单。找到虚拟 CD、虚拟软盘或虚拟闪存更新并根据需要更改设备引导顺序。例如，要从 CD 驱动器引导，将 CD 驱动器配置为引导顺序中的第一个驱动器。
我可以从何种介质引导？	<p>iDRAC 允许从以下可引导介质引导：</p> <ol style="list-style-type: none"> 1 CDROM/DVD 数据介质 1 ISO 9660 映像 1 1.44 软盘或软盘映像 1 被操作系统认作可移动磁盘的 USB 闪存盘 1 USB 闪存盘映像
如何使 USB 闪存盘可引导？	<p>搜索 support.dell.com 寻找 Dell 引导公用程序，这是一种可用来制作 Dell USB 引导盘的 Windows 程序。</p> <p>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：</p> <pre>sys a: x: /s</pre> <p>其中 x 是要使其可引导的 USB 闪存盘。</p> <p>还可以使用 Dell 引导公用程序创建可引导 USB 闪存盘。此公用程序只与 Dell 品牌的 USB 闪存盘兼容。要下载该公用程序，请打开 Web 浏览器，导航到 Dell 支持网站 support.dell.com 并搜索 R122672.exe。</p>
无法在运行 Red Hat® Enterprise Linux® 或 SUSE® Linux 操作系统的系统上找到虚拟软盘设备。已连接虚拟介质并且也已经连接到远程软盘。我应该怎么做？	<p>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：</p> <ol style="list-style-type: none"> 1. 打开 Linux 命令提示符并运行以下命令： <pre>grep "Virtual Floppy" /var/log/messages</pre> 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： <pre>grep "hh:mm:ss" /var/log/messages</pre> <p>其中</p> <pre>hh:mm:ss</pre> <p>是 grep 在第一步返回消息的时间戳。</p> 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： <pre>mount /dev/sdx /mnt/floppy</pre> <p>其中</p> <pre>/dev/sdx</pre> <p>是在第 4 步发现的设备名称</p> <pre>/mnt/floppy</pre> <p>是安装点。</p>
在虚拟软盘驱动器上支持何种文件系统类型？	虚拟软盘驱动器支持 FAT16 或 FAT32 文件系统。
当我使用 iDRAC 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 iDRAC 重设，删除远程连接，并卸下虚拟驱动器。当 iDRAC 重设完成后，这些驱动器会重新出现。

使用本地 RACADM 命令行界面

Integrated Dell™ Remote Access Controller固件版本1.2 用户指南

- [使用 RACADM 命令](#)
- [RACADM 子命令](#)
- [使用 RACADM 公用程序配置 iDRAC](#)
- [使用 iDRAC 配置文件](#)
- [配置多个 iDRAC](#)

本地 RACADM 命令行界面 (CLI) 提供从 managed server 到 iDRAC 的管理功能。RACADM 提供了与 iDRAC Web 界面一样的功能。不过，可以在脚本中使用 RACADM 以简化多个服务器和 iDRAC 的配置，而 Web 界面对于交互式管理更实用。

本地 RACADM 命令不使用网络连接从 managed server 访问 iDRAC。这意味着可以使用本地 RACADM 命令配置初始 iDRAC 网络。

有关配置多个 iDRAC 的详情，请参阅[配置多个 iDRAC](#)。

本节提供以下信息：

- 1 从命令提示符使用 RACADM
- 1 使用 `racadm` 命令配置 iDRAC
- 1 使用 RACADM 配置文件配置多个 iDRAC

使用 RACADM 命令

从命令提示符或 shell 提示符本地运行 RACADM 命令（在 managed server 上）。

登录 managed server，启动命令 shell，然后按以下格式输入本地 RACADM 命令：

```
racadm <子命令> -g <组> -o <对象> <值>
```

不带选项的 RACADM 命令显示常规用法信息。要显示 RACADM 子命令列表，键入：

```
racadm help
```

子命令列表包括 iDRAC 支持的所有命令。

要获得子命令帮助，键入：

```
racadm help <子命令>
```

该命令显示子命令的语法和命令行选项。

RACADM 子命令

[表 10-1](#) 提供可在 RACADM 中运行的每个 RACADM 子命令的说明。有关 RACADM 子命令及语法和有效条目的详细列表，请参阅[RACADM 子命令概览](#)。

表 10-1. RACADM 子命令

命令	说明
clrraclog	清除 iDRAC 日志。清除后，会有一个条目用来指示清除日志的用户和时间。
clrse1	清除 managed server 的系统事件日志条目。
config	配置 iDRAC。
getconfig	显示当前 iDRAC 配置属性。
getniccfg	显示控制器的当前 IP 配置。
getraclog	显示 iDRAC 日志。
getractime	显示 iDRAC 时间。
getssninfo	显示关于活动会话的信息。
getsvctag	显示服务标签。
getsysinfo	显示有关 iDRAC 和 managed server 的信息，包括 IP 配置、硬件型号、固件版本和操作系统信息。
gettracelog	显示 iDRAC 跟踪日志。如果与 <code>-i</code> 一起使用，则命令显示 iDRAC 跟踪日志中的条目数。

help	列出 iDRAC 子命令。
help <子命令>	列出指定子命令的用法语句。
racreset	重设 iDRAC。
racresetcfg	将 iDRAC 重设为默认配置。
serveraction	在 managed server 上执行电源管理操作。
setniccfg	设置控制器的 IP 配置。
sslcertdownload	下载 CA 认证。
sslcertupload	将 CA 认证或服务器认证上载至 iDRAC。
sslcertview	查看 iDRAC 中的 CA 认证或服务器认证。
sslcsrgen	生成并下载 SSL CSR。
testemail	强制 iDRAC 通过 iDRAC NIC 发送电子邮件。
testtrap	强制 iDRAC 通过 iDRAC NIC 发送 SNMP 警报。

使用 RACADM 公用程序配置 iDRAC

本节介绍如何使用 RACADM 执行各种 iDRAC 配置任务。

显示当前 iDRAC 设置

RACADM `getconfig` 子命令从 iDRAC 检索当前配置设置。配置值组织为组，其中包含一个或多个对象，而对象具有值。

请参阅[iDRAC 属性数据库组和对象定义](#)了解组和对象的完整说明。

要显示所有 iDRAC 组的列表，输入此命令：

```
racadm getconfig -h
```

要显示特定组的对象和值，输入此命令：

```
racadm getconfig -g <组>
```

例如，要显示所有 `cfgLanNetworking` 组对象设置的列表，输入以下命令：

```
racadm getconfig -g cfgLanNetworking
```

使用 RACADM 管理 iDRAC 用户

 **注意：** 使用 `racresetcfg` 命令时请小心，因为所有配置参数都会重设为初始默认值。任何之前的更改将丢失。

 **注：** 如果配置新 iDRAC 或运行 `racadm racresetcfg` 命令，则当前唯一用户为 `root`，密码为 `calvin`。

 **注：** 可以随时启用和禁用用户。因此，用户在各个 iDRAC 上可能会有不同的索引号。

最多可以在 iDRAC 属性数据库中配置 15 个用户。（第十六位用户保留作为 IPMI LAN 用户。）手动启用 iDRAC 用户前，验证是否存在任何当前用户。

要验证用户是否存在，请在命令提示符处键入以下命令：

```
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 <文件名>` 并查看生成的 `<文件名>` 文件，其中包括所有用户和所有其它 iDRAC 配置参数。

系统将显示有些参数和对象 ID 以及它们的当前值。受关注的两个对象为：

```
# cfgUserAdminIndex=nn
```

```
cfgUserAdminUserName=
```

如果 `cfgUserAdminUserName` 对象没有值，则可以使用由 `cfgUserAdminIndex` 对象表示的索引编号。如果 = 后有名称，则该索引将分配给该用户。

添加 iDRAC 用户

要添加新用户到 iDRAC，应执行下列步骤：

1. 设置用户名。
2. 设置密码。
3. 设置登录到 iDRAC 用户权限。
4. 启用用户。

示例

下面的示例说明如何添加密码为“123456”的新用户“John”，以及 iDRAC 的登录权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001
racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

为验证新用户，使用以下某一命令：

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

启用 iDRAC 用户权限

要给用户授予特定的管理（基于角色）权限，请将 `cfgUserAdminPrivilege` 属性设置为表 10-2 所示的值组成的位掩码：

表 10-2. 用户权限位掩码

用户权限	权限位掩码
"Login to iDRAC"（登录到 iDRAC）	0x00000001
"Configure iDRAC"（配置 iDRAC）	0x00000002
配置用户	0x00000004
清除日志	0x00000008
执行服务器控制命令	0x00000010
访问控制台重定向	0x00000020
访问虚拟介质	0x00000040
检测警报	0x00000080
执行调试命令	0x00000100

例如，要允许用户“Configure iDRAC”（配置 iDRAC）、“Configure Users”（配置用户）、“Clear Logs”（清除日志）和“Access Console Redirection”（访问控制台重定向）权限，添加值 0x00000002、0x00000004、0x00000008 和 0x00000010 组成位掩码 0x0000002E。然后输入以下命令以设置权限：

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

删除 iDRAC 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 iDRAC 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。

检测电子邮件警报

iDRAC 电子邮件警报功能允许用户在 managed server 上发生重要事件时接收电子邮件警报。下面的示例演示如何测试电子邮件警报功能以确保 iDRAC 在网络上正确发送电子邮件警报。

```
racadm testemail -i 2
```

 **注：** 确保检测电子邮件警报功能前 SMTP 和电子邮件警报设置已配置。有关详情，请参阅[配置电子邮件警报](#)。

检测 iDRAC SNMP 陷阱警报功能

iDRAC SNMP 陷阱警报功能允许 SNMP 陷阱侦听器接收 managed server 上发生的系统事件陷阱。

下面的示例演示用户如何测试 SNMP 陷阱警报功能。

```
racadm testtrap -i 2
```

 **注：** 检测 iDRAC SNMP 陷阱警报功能之前，请确保正确配置了 SNMP 和陷阱设置。请参阅 `testtrap` 和 `testemail` 子命令说明配置这些设置。

配置 iDRAC 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提示您输入 <Ctrl><E> 时 iDRAC 配置公用程序所提供的功能一样。有关使用 iDRAC 配置公用程序配置网络属性的详情，请参阅[LAN](#)。

以下实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 iDRAC LAN。

配置 IPMI

1. 通过输入以下命令，配置 LAN 上 IPMI：

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

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

- a. 通过输入以下命令更新 IPMI 信道权限：

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

其中<级别>是以下某个值：

- o 2 (用户)

- o 3 (操作员)
- o 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 cfgIpmlan -o cfgIpmlanPrivilegeLimit 2
```

- b. 如果需要, 使用如下的命令设置 IPMI LAN 信道加密密钥:

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

```
racadm config -g cfgIpmlan -o cfgIpmlanEncryptionKey <密钥>
```

其中<密钥>是一个有效十六进制格式的 20 字符密钥。

2. 使用以下命令配置 IPMI LAN 上串行 (SOL):

```
racadm config -g cfgIpmlan -o cfgIpmlanSolEnable 1
```

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。

- a. 使用以下命令更新 IPMI SOL 最低权限级别:

```
racadm config -g cfgIpmlan -o cfgIpmlanSolMinPrivilege <级别>
```

其中<级别>是以下某个值:

- o 2 (用户)
- o 3 (操作员)
- o 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 cfgIpmlan -o cfgIpmlanSolMinPrivilege 2
```

注: 要重新定向 LAN 上串行控制台, 应确保 SOL 波特率与 managed server 的波特率相同。

- b. 使用以下命令更新 IPMI SOL 波特率:

```
racadm config -g cfgIpmlan -o cfgIpmlanSolBaudRate <波特率>
```

其中<波特率>为 19200、57600 或 115200 bps。

例如:

```
racadm config -g cfgIpmlan -o cfgIpmlanSolBaudRate 57600
```

- c. 通过在命令提示符处键入以下命令启用 SOL。

注: SOL 可以为每个用户启用或禁用。

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

其中 <id> 是用户的唯一 ID。

配置 PEF

可以配置希望 iDRAC 对每个平台警报采取的措施。表 10-3 列出了可能的操作和在 RACADM 中标识的值。

表 10-3. 平台事件操作

措施	值
无操作	0
电源关闭	1
重新引导	2
关机后再开机	3

1. 使用以下命令配置 PEF 操作:

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

其中，<索引> 是 PEF 索引（请参阅表 5-6），<操作值> 是来自表 10-3 的值。

例如，当检测到处理器严重事件时要 PEF 重新引导系统并发送 IPMI 警报，键入以下命令：

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
```

配置 PET

1. 使用以下命令启用全局警报：

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

2. 使用以下命令启用 PET：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <索引> <0|1>
```

其中 <索引> 是 PET 目标索引，而 0 或 1 分别禁用 PET 或启用 PET。

例如，要启用具有索引 4 的 PET，键入以下命令：

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

3. 使用以下命令配置 PET 策略：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <索引> <IP-地址>
```

其中 <索引> 是 PET 目标索引，而 <IP-地址> 是接收平台事件警报的系统的目标 IP 地址。

4. 配置团体名称字符串。

在命令提示符下键入：

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

其中 <名称> 是 PET 团体名称。

配置电子邮件警报

1. 输入以下命令启用全局警报：

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

2. 输入以下命令启用电子邮件警报：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <索引> <0|1>
```

其中 <索引> 是电子邮件目标索引，0 禁用电子邮件警报，1 启用警报。电子邮件目标索引可以是 1 到 4 之间的一个值。

例如，要启用具有索引 4 的电子邮件，键入以下命令：

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

3. 通过输入以下命令配置电子邮件设置：

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

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

4. 要配置自定义消息，请输入以下命令：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <索引> <自定义消息>
```

其中 <索引> 是电子邮件目标索引，而 <自定义消息> 是自定义消息。

5. 如果需要，通过输入以下命令检测配置的电子邮件警报：

```
racadm testemail -i <索引>
```

其中 <索引> 是要检测的电子邮件目标索引。

配置 IP 筛选 (IpRange)

IP 地址筛选 (或 IP 范围检查) 只允许 IP 地址在用户指定范围内的客户端或 management workstation 对 iDRAC 进行访问。其它所有登录请求都会拒绝。

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：

```
1 cfgRacTuneIpRangeAddr
1 cfgRacTuneIpRangeMask
```

`cfgRacTuneIpRangeMask` 属性既应用于接入 IP 地址，也应用于 `cfgRacTuneIpRangeAddr` 属性。如果结果相同，接入的登录请求就能够访问 iDRAC。从该范围以外的 IP 地址登录将收到一条错误。

如果以下表达式等于零，登录将会继续：

```
cfgRacTuneIpRangeMask & (<接入-IP-地址> ^ cfgRacTuneIpRangeAddr)
```

其中 `&` 是数量的按位“与”，而 `^` 是按位“异或”。

请参阅 [cfgRacTuning](#) 了解 `cfgRacTuning` 属性的完整列表。

表 10-4. IP 地址筛选 (IpRange) 属性

属性	说明
<code>cfgRacTuneIpRangeEnable</code>	启用 IP 范围检查功能。
<code>cfgRacTuneIpRangeAddr</code>	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 <code>cfgRacTuneIpRangeMask</code> 的按位“与”。确定所允许 IP 地址的高端。在高位包含此位样式的任何 IP 地址都允许登录。从此范围外的 IP 地址登录都会失败。各个属性的默认值允许 192.168.1.0 到 192.168.1.255 范围的地址登录。
<code>cfgRacTuneIpRangeMask</code>	定义 IP 地址中的高位位置。掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。

配置 IP 筛选

要在 Web 界面中配置 IP 筛选，应按照这些步骤：

1. 单击“System”（系统）→“Remote Access”（远程访问）→ iDRAC →“Network/Security”（网络安全性）。
2. 在“Network Configuration”（网络配置）页上，单击“Advanced Settings”（高级设置）。
3. 选中“IP Range Enabled”（IP 范围已启用）复选框并输入“IP Range Address”（IP 范围地址）和“IP Range Subnet Mask”（IP 范围子网掩码）。
4. 单击“Apply”（应用）。

以下是使用本地 RACADM 设置 IP 筛选的示例。

 **注：** 请参阅 [使用本地 RACADM 命令行界面](#) 了解有关 RACADM 和 RACADM 命令的详情。

1. 以下 RACADM 命令会阻塞除 192.168.0.57 以外的所有 IP 地址：

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

2. 要将登录限制到一小组四个相邻 IP 地址（例如，192.168.0.212 到 192.168.0.215），则在掩码中除最低的两个位以外选中所有位，如下所示：

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

范围掩码的最后字节设置为 252，十进制数字为 11111100b。

IP 筛选原则

启用 IP 筛选时应遵循以下原则：

- 1 确保 `cfgRacTuneIpRangeMask` 以网络掩码的形式配置，所有的重要位为 1（定义掩码中的子网），在低位都变为 0。
- 1 使用所需范围的基地址作为 `cfgRacTuneIpRangeAddr` 的值。此地址的 32 位二进制值应将掩码中为零的所有低位都设为零。

配置 IP 阻塞

IP 阻塞动态确定来自特定 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 iDRAC。

IP 阻塞功能包括：

- 1 允许的登录失败次数 (`cfgRacTuneIpBlkFailCount`)
- 1 按秒计的这些失败必须发生的时间框架 (`cfgRacTuneIpBlkFailWindow`)
- 1 阻止被阻塞 IP 地址在超过允许失败总数后不能建立会话的时间（秒） (`cfgRacTuneIpBlkPenaltyTime`)

随着特定 IP 地址的登录失败次数不断累积，这些值会由内部计数器“登记”。当用户成功登录后，失败历史记录就会清除并且内部计数器将重置。

 **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[iDRAC 属性数据库组和对象定义](#)了解 `cfgRacTune` 属性的完整列表。

[登录重试限制属性](#) 列出了用户定义的参数。

表 10-5. 登录重试限制属性

属性	定义
<code>cfgRacTuneIpBlkEnable</code>	启用 IP 阻塞功能。 如果在一段时间内 (<code>cfgRacTuneIpBlkFailWindow</code>) 某 IP 地址出现连续的失败 (<code>cfgRacTuneIpBlkFailCount</code>)，则在一段时间内 (<code>cfgRacTuneIpBlkPenaltyTime</code>) 来自该地址的其它建立会话尝试都会遭到拒绝。
<code>cfgRacTuneIpBlkFailCount</code>	设置拒绝某 IP 地址的登录尝试前允许的登录失败次数。
<code>cfgRacTuneIpBlkFailWindow</code>	计数失败的时间框架（秒）。当失败次数超出此限制，将不会记入计数器。
<code>cfgRacTuneIpBlkPenaltyTime</code>	定义一个时间范围（以秒为单位），在该范围内拒绝失败过多的某个 IP 地址的登录尝试。

启用 IP 阻塞

以下示例显示，如果客户端在一分钟内超过五次登录尝试失败，将阻止该客户 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 cfgRacTuneIpBlkFailWindow 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

以下示例在一分钟内阻止三次以上的失败尝试，并阻止其它登录尝试一小时。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

使用本地 RACADM 配置 iDRAC Telnet 和 SSH 服务

telnet/SSH 控制台可以使用 RACADM 命令在本地配置（在 managed server 上）。

 **注：** 必须具有“Configure iDRAC”（配置 iDRAC）权限才能执行本部分中的命令。

 **注：** 在 iDRAC 中重新配置 telnet 或 SSH 设置时，任何当前会话都会终止而没有警告。

要从本地 RACADM 启用 telnet 和 SSH，登录 managed server 并在命令提示符处键入以下命令：

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

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

要禁用 telnet 或 SSH 服务，将值从 1 更改为 0：

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

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

键入以下命令更改 iDRAC 上的 Telnet 端口号。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <新端口号>
```

例如，要更改 telnet 端口从默认 22 到 8022，键入此命令：

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

有关可用 RACADM CLI 命令的完整列表，请参阅[使用本地 RACADM 命令行界面](#)。

使用 iDRAC 配置文件

iDRAC 配置文件是一个包含 iDRAC 数据库值表示的文本文件。可以使用 RACADM `getconfig` 子命令生成包含 iDRAC 当前值的配置文件。可以随后编辑该文件并使用 RACADM `config -f` 子命令将文件载入 iDRAC，或将配置复制到其它 iDRAC。

创建 iDRAC 配置文件

配置文件是一个纯文本文件（无格式）。可以使用任何有效文件名；`.cfg` 文件扩展是推荐的格式。

配置文件可以：

- 1 使用文本编辑器创建
- 1 使用 RACADM `getconfig` 子命令从 iDRAC 获得
- 1 使用 RACADM `getconfig` 子命令从 iDRAC 获得并随后编辑

要使用 RACADM `getconfig` 命令获得配置文件，在 managed server 命令提示符处输入以下命令：

```
racadm getconfig -f myconfig.cfg
```

此命令在当前目录中创建文件 `myconfig.cfg`。

配置文件语法

 **注意：** 使用纯文本编辑器编辑配置文件，比如 Windows 上的**记事本**或 Linux 上的 **vi**。racadm 公用程序只分析 ASCII 文本。格式会造成分析器混乱，并可能损坏 iDRAC 数据库。

本部分说明配置文件的格式。

- 1 以 `#` 开头的行是注释。

注释必须从第一列开始。所有其它列中的 `#` 字符均只被视为正常 `#` 字符。

示例：

```
#  
  
# This is a comment (这是一条注释)  
  
[cfgUserAdmin]  
  
cfgUserAdminPrivilege=4
```

- 1 组条目必须用 `[` 和 `]` 字符括起来。

表示组名的起始 `[` 字符必须从第一列开始。此组名称必须在该组中的任何对象之前指定。没有关联组名的对象将导致错误。配置数据按[iDRAC 属性数据库组和对象定义](#)中所述分组。

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)
```

- 1 参数都指定为对象=值对，在对象、= 和值之间不留空格。

值后的空格将忽略。值字符串内的空格保持不变。= 右侧的所有字符都将保留原样（例如另一个=，或 #、[、] 等等）。

- 1 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>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> <唯一定位标记名称>
```

- 1 索引组的行无法从配置文件中删除。

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> ""
```



注： 空字符串（两个 "" 字符表示）指示 iDRAC 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> -i <索引>
```

- 1 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>
```

- 1 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 iDRAC 读入该组的所有索引。配置 iDRAC 时，该组内的任何对象都是简单修改。如果修改的对象代表新的索引，则该索引将在配置过程中在 iDRAC 上创建。

- 1 不能在配置文件中指定想要的索引。

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。此方法在用户不需要的地方添加索引条目以在所有管理的 RAC 之间实现精确索引匹配方面更加灵活。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 iDRAC 上可以正确分析和运行的配置文件可能无法在其它 iDRAC 上正确运行。

修改配置文件中的 iDRAC IP 地址

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

例如：

```
#  
  
# Object Group "cfgLanNetworking" (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 "cfgLanNetworking" (对象组 "cfgLanNetworking")  
  
#  
  
[cfgLanNetworking]  
  
cfgNicIpAddress=10.35.9.143  
  
# comment, the rest of this line is ignored (注释，此行的其余部分将被忽略)
```

cfgNicGateway=10.35.9.1

载入配置文件到 iDRAC

命令 `racadm config -f <文件名>` 分析配置文件以验证有效组和对象名称存在并且遵守语法规则。如果文件没有任何命令错误，则使用文件内容更新 iDRAC 数据库。

 **注：** 要只验证语法而不更新 iDRAC 数据库，将 `-c` 选项添加到 `config` 子命令。

配置文件中的错误标记有行号以及一条简单的信息解释该问题。必须更正所有错误，然后才可以用配置文件更新 iDRAC。

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

执行 `racadm config -f <文件名>` 命令前，可以运行 `racreset` 子命令重设 iDRAC 为默认设置。确保要加载的配置文件包括所有需要的对象、用户、索引和其它参数。

要使用配置文件更新 iDRAC，请在 `managed server` 的命令提示符处执行以下命令：

```
racadm config -f <文件名>
```

在命令完成后，可以执行 `RACADM getconfig` 子命令确定更新成功。

配置多个 iDRAC

使用配置文件，可以用相同属性配置其它 iDRAC。按照这些步骤配置多个 iDRAC：

1. 从希望参考设置的 iDRAC 创建配置文件。在 `managed server` 的命令提示符处，输入以下命令：

```
racadm getconfig -f <文件名>
```

其中 `<文件名>` 是保存 iDRAC 属性的文件的名称，比如 `myconfig.cfg`。

有关详情，请参阅[创建 iDRAC 配置文件](#)。

 **注：** 某些配置文件包含独特的 iDRAC 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。

2. 编辑在上一步创建的配置文件并删除或注释掉任何不想复制的设置。
3. 将编辑的配置文件复制到网络驱动器，供要配置 iDRAC 的各个 `managed server` 可以访问此文件。
4. 对于要配置的每个 iDRAC：

- a. 登录 `managed server` 并启动命令提示符。
- b. 如果要从默认设置重新配置 iDRAC，输入以下命令：

```
racadm racreset
```

- c. 使用以下命令将配置文件载入 iDRAC：

```
racadm config -f <文件名>
```

其中 `<文件名>` 是创建的配置文件的名称。如果文件不在工作目录中，还包括完整路径。

- d. 通过输入以下命令重设已配置的 iDRAC：

```
racadm reset
```

[目录](#)

[目录](#)

使用 iDRAC SM-CLP 命令行界面

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [使用 SM-CLP 进行系统管理](#)
- [iDRAC SM-CLP 支持](#)
- [SM-CLP 功能](#)
- [导航 MAP 地址空间](#)
- [使用 Show Verb](#)
- [iDRAC SM-CLP 示例](#)
- [用 Telnet 或 SSH 使用 LAN 上串行 \(SOL\)](#)

本部分提供了有关 iDRAC 中 Server Management Workgroup (SMWG) Server Management Command Line Protocol (SM-CLP) 的信息。

 **注：** 本部分假定您熟悉 Systems Management Architecture for Server Hardware (SMASH) 标准和 SMWG SM-CLP 规范。有关这些规范的详情，请参阅分布式管理任务小组 (DMTF) 网站 www.dmtf.org。

iDRAC SM-CLP 是由 DMTF 和 SMWG 推动的一项协议，提供了系统管理 CLI 实施的标准。定义的 SMASH 体系结构做了很多工作，旨在为更多标准系统管理组件建立基础。SMWG SM-CLP 是 DMTF 推动的整个 SMASH 工作中的一部分。

SM-CLP 提供了本地 RACADM 命令行界面的一部分功能，只不过访问路径不同。SM-CLP 在 iDRAC 中执行，而 RACADM 在 managed server 上执行。另外，RACADM 是一种 Dell 专用界面，而 SM-CLP 是业界标准界面。请参阅[RACADM 和 SM-CLP 等价](#)了解 RACADM 和 SM-CLP 命令的映射。

使用 SM-CLP 进行系统管理

iDRAC SM-CLP 使用户能够从命令行或脚本管理以下系统功能：

- 1 服务器电源管理 — 打开、关闭或重新引导系统
- 1 系统事件日志 (SEL) 管理 — 显示或清除 SEL 记录
- 1 iDRAC 用户帐户管理
- 1 Active Directory 配置
- 1 iDRAC LAN 配置
- 1 SSL 认证签名请求 (CSR) 生成
- 1 虚拟介质配置
- 1 在 Telnet 或 SSH 上 LAN 上串行 (SOL) 重定向

iDRAC SM-CLP 支持

SM-CLP 承载在 iDRAC 固件中并支持 telnet 和 SSH 连接。iDRAC SM-CLP 界面基于由 DMTF 组织提供的 SM-CLP 规范版本 1.0。

以下部分提供了 iDRAC 上 SM-CLP 功能的概览。

SM-CLP 功能

SM-CLP 规范提供了一组常用标准 SM-CLP verb，可通过 CLI 用于简单系统管理。

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

以下是 SM-CLP 命令行的语法：

<verb> [<选项>] [<目标>] [<属性>]

[表 11-1](#) 提供了 iDRAC CLI 支持的 verb 的列表，各个命令的语法，以及 verb 支持的选项列表。

表 11-1. 支持的 SM-CLP CLI Verb

Verb	说明	选项
cd	使用 shell 导航 Managed System 地址空间。	- Cdefault, -Cexamine, -Chelp, -Coutput, -Cversion

	语法: cd [选项] [目标]	
delete	删除对象实例。 语法: delete [选项] 目标	- Cexamine, -Chelp, -Coutput, -Cversion
dump	将二进制映像从 MAP 移至 URI。 dump -destination <URI> [选项] [目标]	- Cdestination, -Cexamine, -Chelp, -Coutput, -Cversion
exit	从 SM-CLP shell 会话退出。 语法: exit [选项]	- Chelp, -Coutput, -Cversion
help	显示 SM-CLP 命令帮助。 help	-examine, -help, -output, -version
load	将二进制映像从 URI 移至 MAP。 语法: load -source <URI> [选项] [目标]	- Cexamine, -Chelp, -Coutput, -Csource, -Cversion
reset	重设目标。 语法: reset [选项] [目标]	- Cexamine, -Chelp, -Coutput, -Cversion
set	设置目标属性 语法: set [选项] [目标] <属性名称>=<值>	- Cexamine, -Chelp, -Coutput, -Cversion
show	显示目标属性、verb 和子目标。 语法: show [选项] [目标] <属性名称>=<值>	-all, -default, -Cdisplay, -Cexamine, -Chelp, -Clevel, -Coutput, -Cversion
start	启动目标。 语法: start [选项] [目标]	- Cexamine, -Cforce, -Chelp, -Coutput, -Cversion
stop	关闭目标。 语法: stop [选项] [目标]	- Cexamine, -Cforce, -Chelp, -Coutput, -Cstate, -Cversion, -Cwait
version	显示目标的版本属性。 语法: version [选项]	- Cexamine, -Chelp, -Coutput, -Cversion

表 11-2 说明 SM-CLP 选项。有些选项有简写格式，如表中所示。

表 11-2. 支持的 SM-CLP 选项

SM-CLP 选项	说明
- Call, -Ca	指示 verb 执行所有可能的功能。
-destination	在 dump 命令中指定存储映像的位置。 语法: -destination <URI >
-display, -d	筛选命令输出。 语法: -display <属性 目标 verb>[, <属性 目标 verb>]*
-examine, -x	指示命令处理器在不执行命令的情况下验证命令语法。

- Chelp, -Ch	显示 verb 帮助。
- Clevel, -l	指示 verb 在目标上以指定目标以下的级别操作。 语法： -level <n all>
- Coutput, -Co	指定输出的格式。 语法： -output <text clpcsv clpxml>
-source	在 load 命令中指定映像的位置。 语法： -source <URI>
- Cversion, -Cv	显示 SMASH-CLP 版本号。

导航 MAP 地址空间

 **注：** 斜杠 (/) 和反斜杠 (\) 在 SM-CLP 地址路径中可以互换。不过，命令行末尾的反斜杠会使命令在下一行继续并在命令分析中忽略。

可以使用 SM-CLP 管理的对象由称为可管理性访问点 (MAP) 地址层次空间排列的目标表示。地址路径指定从地址空间根到对象的路径。

根目标由斜杠 (/) 或反斜杠 (\) 表示。这是登录 iDRAC 时的默认起始点。使用 cd verb 从根向下导航。例如，要导航到系统事件日志 (SEL) 中的第三个记录，输入以下命令：

```
->cd /system1/sp1/logs1/record3
```

输入不带目标的 cd verb 以查找在地址空间中的当前位置。..和 .缩写的作用与在 Windows 以及 Linux 中相同：..指父级，而 .指当前级。

目标

表 11-3 提供了 SM-CLP 可用的目标列表。

表 11-3. SM-CLP 目标

目标	定义
/system1/	Managed System 目标。
/system1/sp1	服务处理器。
/system1/sol1	LAN 上串行目标。
/system1/sp1/account1 through /system1/sp1/account16	十六个本地 iDRAC 用户帐户。account1 是根帐户。
/system1/sp1/enetport1	iDRAC NIC MAC 地址。
/system1/sp1/enetport1/lanendpt1/ ipendpt1	iDRAC IP、网关和网络掩码设置。
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	iDRAC DNS 服务器设置。
/system1/sp1/group1 through /system1/sp1/group5	Active Directory 标准架构组。
/system1/sp1/logs1	日志收集目标。
/system1/sp1/logs1/record1	Managed System 上的单独 SEL 记录实例。
/system1/sp1/logs1/records	Managed System 上的 SEL 目标。
/system1/sp1/oemdel_l_racsecurity1	用来生成认证签名请求的参数存储。
/system1/sp1/oemdel_l_ssl1	SSL 认证请求状态。
/system1/sp1/oemdel_l_vmservice1	虚拟介质配置和状态。

使用 Show Verb

要了解有关使用目标的详情，请使用 show verb。此 verb 显示目标的属性、子目标和该位置允许的 SM-CLP verb 的列表。

使用 -display 选项

show @Cdisplay 选项允许限制命令的输出为一个或多个属性、目标和 **verb**。例如，要只显示当前位置的属性和目标，使用以下命令：

```
show -d properties,targets /system1/sp1/account1
```

要只列出某些属性，按以下命令予以限定：

```
show -d properties=(userid,username) /system1/sp1/account1
```

如果只想显示一个属性，可以省略括号。

使用 **-level** 选项

show -level 选项在指定目标以下的级别执行 **show**。例如，如果想查看 **/system1/sp1** 下帐户 1 到帐户 16 的 **username** 和 **userid** 属性，可以输入以下命令：

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

要查看地址空间的所有目标和属性，使用 **-l all** 选项，如以下命令：

```
show -l all -d properties /
```

使用 **-output** 选项

-output 选项指定 SM-CLP **verb** 输出的四种格式之一：**text**、**clpcsv**、**keyword** 和 **clpxml**。

默认格式为 **text**，是最可读的输出。**clpcsv** 格式是逗号分隔值格式，适合于载入电子表格程序。**keyword** 格式以每行关键字=值对列表输出信息。**clpxml** 格式是 XML 文档，包含 **response** XML 元素。DMTF 指定了 **clpcsv** 和 **clpxml** 格式，其规范可以在 DMTF 网站 www.dmtf.org 找到。

以下示例显示了如何以 XML 输出 SEL 内容：

```
show -l all -output format=clpxml /system1/sp1/logs1
```

iDRAC SM-CLP 示例

以下小节提供了使用 SM-CLP 执行以下操作的示例：

- 1 服务器电源管理
- 1 SEL 管理
- 1 映射目标导航
- 1 显示系统属性
- 1 设置 iDRAC IP 地址、子网掩码和网关地址

有关使用 iDRAC SM-CLP 界面的信息，请参阅[iDRAC SMCLP 属性数据库](#)。

服务器电源管理

[表 11-4](#) 提供了使用 SM-CLP 在 Managed Server 上执行电源管理操作的示例。

表 11-4. 服务器电源管理操作

操作	语法
使用 SSH 界面登录 iDRAC	>ssh 192.168.0.120 >login: root >password:
关闭服务器的电源	->stop /system1 system1 已成功停止
将服务器从电源关闭状态打开	->start /system1 system1 已成功启动
重新引导服务器	->reset /system1 system1 已成功重置

SEL 管理

表 11-5 提供了使用 SM-CLP 在 Managed System 上执行 SEL 相关操作的示例。

表 11-5. SEL 管理操作

操作	语法
查看 SEL	<pre>->show /system1/sp1/logs1</pre> <p>Targets: record1 record2 record3 record4 record5</p> <p>Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5</p> <p>Verbs: cd delete exit help show version</p>
查看 SEL 记录	<pre>->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4</pre> <p>Properties: Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007</p> <p>Verbs: cd exit help show version</p>
清除 SEL	<pre>->delete /system1/sp1/logs1</pre> <p>All records deleted successfully</p>

映射目标导航

表 11-6 提供了使用 cd verb 导航映射的示例。在所有示例中，假定初始的默认目标为 /。

表 11-6. 映射目标导航操作

操作	语法
导航到系统目标并重新引导	<pre>->cd system1 ->reset</pre> <p>注： 当前默认目标为 /。</p>
导航到 SEL 目标并显示日志记录	<pre>->cd system1 ->cd sp1 ->cd logs1 ->show</pre> <pre>->cd system1/sp1/logs1 ->show</pre>
显示当前目标	<pre>->cd .</pre>
上移一级	<pre>->cd ..</pre>
退出 shell	<pre>->exit</pre>

设置 iDRAC IP 地址、子网掩码和网关地址

使用 SM-CLP 更新 iDRAC 网络属性是一个两部分过程：

1. 设置 NIC 属性新值，位置为 `/system1/sp1/enetport1/lanendpt1/ipendpt1`：
 - o `oemdellicenable` — 设置为 1 启用 iDRAC 网络，0 禁用
 - o `ipaddress` — IP 地址
 - o `subnetmask` — 子网掩码
 - o `oemdellicusedhcp` — 设置为 1 启用使用 DHCP 设置 `ipaddress` 和 `subnetmask` 属性，0 设置静态值
2. 通过将 `committed` 属性设置为 1 提交新值。

无论何时 `commit` 属性的值为 1，属性的当前设置都活动。如果更改任何属性，`commit` 属性会重设为 0，表示值尚未提交。

 **注：** `commit` 属性只影响在 `/system1/sp1/enetport1/lanendpt1/ipendpt1` MAP 位置的属性。所有其它 SM-CLP 命令会立即生效。

 **注：** 如果使用本地 RACADM 设置 iDRAC 网络属性，您的更改会立即生效，因为本地 RACADM 不依赖于网络连接。

提交更改后，新网络设置会生效，造成 telnet 或 ssh 会话终止。通过引入提交步骤，可以延迟会话的终结直至完成所有 SM-CLP 命令。

[表 11-7](#) 提供了使用 SM-CLP 设置 iDRAC 属性的示例。

表 11-7. 使用 SM-CLP 设置 iDRAC 网络属性

操作	语法
导航到 iDRAC NIC 属性位置	<code>->cd /system1/sp1/enetport1/lanendpt1/ipendpt1</code>
设置新 IP 地址	<code>->set ipaddress=10.10.10.10</code>
设置子网掩码	<code>->set subnetmask=255.255.255.255</code>
打开 DHCP 标志	<code>->set oemdellicusedhcp=1</code>
启用 NIC	<code>->set oemdellicenable=1</code>
提交更改	<code>->set committed=1</code>

使用 SM-CLP 更新 iDRAC 固件

要使用 SM-CLP 更新 iDRAC 固件，必须知道 Dell 更新软件包的 TFTP URI。

按照这些步骤使用 SM-CLP 更新固件：

1. 使用 telnet 或 SSH 登录 iDRAC。
2. 通过输入以下命令检查当前固件版本：

```
version
```

3. 输入以下命令：

```
load -source tftp://<tftp-服务器>/<更新-路径> /system1/sp1
```

其中 `<tftp-服务器>` 是 TFTP 服务器的 DNS 名称或 IP 地址，而 `<更新-路径>` 是 TFTP 服务器上更新软件包的路径。

telnet 或 SSH 会话将会终止。可能需要等待几分钟固件更新才能完成。

4. 要验证写入新固件，请启动新 telnet 或 SSH 会话并再次重新输入 `version` 命令。

用 Telnet 或 SSH 使用 LAN 上串行 (SOL)

在 Management Station 上使用 Telnet 或 SSH 控制台连接到 iDRAC 并随后重定向 managed server 的串行端口到控制台中。此功能是 IPMI SOL 的替代，该方式要求 `solproxy` 一类的公用程序在网络数据包间转换串行数据流。iDRAC SOL 方式消除了额外公用程序的需要，因为串行到网络转换是在 iDRAC 中进行的。

使用的 Telnet 或 SSH 控制台应该能解释并响应来自 Managed Server 串行端口的数据。串行端口通常附加到仿真 ANSI- 或 VT100- 终端的 Shell 上。

使用 Telnet，连接到 IPMI LAN SOL 端口—端口 2100。串行控制台自动重定向到 Telnet 控制台。

使用 SSH 或 Telnet，按照连接到 SM-CLP 的方式连接到 iDRAC。SOL 重定向可以随后从 `/system1/sol1` 目标启动。

请参阅[安装 Telnet 或 SSH 客户端](#)了解有关使用带有 iDRAC 的 Telnet 和 SSH 客户端的详情。

将 SOL Over Telnet 用于 Microsoft Windows 上的 HyperTerminal

1. 选择"Start" (开始) → "All Programs" (所有程序) → "Accessories" (附件) → "Communications" (通讯) → "HyperTerminal" (超级终端)。
2. 为连接输入名称, 选择图标, 并单击"OK" (确定)。
3. 从"Connect using" (连接使用) 字段的列表中选择 TCP/IP (Winsock)。
4. 在"Host address" (主机地址) 字段中输入 iDRAC 的 DNS 名称或 IP 地址。
5. 在"Port number" (端口号) 字段中输入 Telnet 端口号。
6. 单击 OK (确定)。

要结束 SOL 会话, 单击 HyperTerminal 断开连接图标。

将 SOL Over Telnet 用于 Linux

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

1. 启动 shell。
2. 使用以下命令连接到 iDRAC:

```
telnet <iDRAC-ip-地址>
```

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

3. 输入以下命令以启动 SOL:

```
start /system1/sol1
```

这会连接到 Managed Server 的串行端口。

准备好退出 SOL 后, 键入 <Ctrl>+] (按住 Ctrl 并键入右方括号, 然后松开)。Telnet 提示符将会显示。键入 quit 退出 Telnet。

使用 SOL Over SSH

/system1/sol1 目标允许将 Managed Server 的串行端口重定向到 SSH 控制台。

1. 使用 OpenSSH 或 PuTTY 连接到 iDRAC。
2. 输入以下命令以启动 SOL:

```
start /system1/sol1
```

这会连接到 Managed Server 的串行端口。SM-CLP 命令不再可用。

准备退出 SOL 重定向时, 按 <Enter>、<Esc>, 然后按 <T> (按顺序逐个按这些键)。将关闭 SSH 会话。

一旦启动 SOL, 就不能返回 SM-CLP。必须退出 SSH 会话并启动新会话以使用 SM-CLP。

[目录](#)

[目录](#)

使用 iVM-CLI 部署操作系统

Integrated Dell™ Remote Access Controller固件版本1.2
用户指南

- [开始之前](#)
- [创建可引导映像文件](#)
- [准备部署](#)
- [部署操作系统](#)
- [使用虚拟介质命令行界面公用程序](#)

虚拟介质命令行界面 (iVM-CLI) 公用程序是一个命令行界面，从 management station 向远程系统中的 iDRAC 提供虚拟介质功能。使用 iVM-CLI 和脚本化方法，可以在网络中的多个远程系统上部署操作系统。

本节提供了有关将 iVM-CLI 公用程序集成到公司网络的信息。

开始之前

开始使用 iVM-CLI 公用程序前，应确保目标远程系统和公司网络符合以下部分所列的要求。

远程系统要求

- 1 iDRAC 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：

- 1 操作系统文件
- 1 需要的驱动程序
- 1 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 iDRAC 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。

以下部分提供了有关为 Linux 和 Windows 系统创建映像文件的特定信息。

为 Linux 系统创建映像文件

使用数据复制器 (dd) 公用程序为 Linux 系统创建可引导映像文件。

要运行该公用程序，打开命令提示符并键入以下命令：

```
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 Microsoft® Windows® 操作系统，映像文件可包括类似于 Microsoft Systems Management Server (SMS) 所用部署方法的程序。

创建映像文件时，应执行以下规则：

- 1 遵循标准基于网络的安装步骤
 - 1 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步骤
- 1 执行以下某一程序：
- 1 将 **ipmitool** 和虚拟介质命令行界面 (IVM-CLI) 集成到现有操作系统部署应用程序。使用示例 **ivmdeploy** 脚本作为使用公用程序的指南。
 - 1 使用现有 **ivmdeploy** 脚本部署操作系统。

部署操作系统

使用 IVM-CLI 和该公用程序包含的 **ivmdeploy** 脚本将操作系统部署到远程系统。

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

以下步骤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 iDRAC IP 地址，每行一个 IP 地址。
2. 在客户端介质驱动器中插入可引导操作系统 CD 或 DVD。
3. 在命令行运行 **ivmdeploy**。

要运行 **ivmdeploy** 脚本，在命令提示符处输入以下命令：

```
ivmdeploy -r ip.txt -u <idrac-用户> -p <idrac-密码> -c {<iso9660-映像> | <路径>}
```

其中

- 1 <idrac-用户> 是 iDRAC 用户名，例如 **root**
- 1 <idrac-密码> 是 iDRAC 用户的密码，例如 **calvin**
- 1 <iso9660-映像> 是操作系统安装 CD 或 DVD 的 ISO9660 映像路径
- 1 <路径> 是包含操作系统安装 CD 或 DVD 的设备路径

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

ivmdeploy 脚本只支持从 CD/DVD 或 CD/DVD ISO9660 映像安装。如果需要从软盘或软盘映像安装，可以修改脚本以使用 **IVMCLI -f** 选项。

使用虚拟介质命令行界面公用程序

虚拟介质命令行界面 (IVM-CLI) 公用程序是一个可编写脚本的命令行界面，从 management station 向 iDRAC 提供虚拟介质功能。

IVM-CLI 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，一个会话一次只能访问一个给定物理驱动器。

- 1 与虚拟介质插件一致的可移动介质设备或映像文件
- 1 启用 iDRAC 固件引导一次选项后自动终结。

- 1 使用安全套接字层 (SSL) 确保与 iDRAC 的通信安全

运行公用程序前，确保对 iDRAC 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 iVM-CLI 命令。

客户端系统的管理员控制用户组和权限，从而控制可运行公用程序的用户。

对于 Windows 系统，必须具有高级用户权限来运行 iVM-CLI 公用程序。

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

安装 iVM-CLI 公用程序

iVM-CLI 公用程序位于 *Dell OpenManage™ Systems Management Consoles CD* 上，该 CD 随 Dell OpenManage System Management 软件套件提供。要安装公用程序，请将 *System Management Consoles CD* 插入到系统的 CD 驱动器中并按屏幕上的说明操作。

Systems Management Consoles CD 包含最新系统管理软件，包括诊断、存储管理、远程访问服务和 RACADM 公用程序。本 CD 还包含自述文件，提供最新 *systems management software* 产品信息。

Systems Management Consoles CD 还包含 `ivmdeploy` — 这是一个演示如何使用 iVM-CLI 和 RACADM 公用程序将软件部署到多个远程系统的示例脚本。

 **注：** `ivmdeploy` 脚本依赖于安装时目录中的其它文件。如果想从另一个目录使用脚本，必须随之复制所有的文件。

命令行选项

iVM-CLI 界面在 Windows 和 Linux 系统上相同。公用程序使用的选项与 RACADM 公用程序选项一致。例如，指定 iDRAC IP 地址的选项采用的语法对于 RACADM 和 iVM-CLI 公用程序都一样。

iVM-CLI 命令格式如下：

```
ivmcli [参数] [操作_系统_shell_选项]
```

命令行语法区分大小写。有关详情，请参阅“[iVM-CLI 参数](#)”。

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

- 1 iVM-CLI 连接因任何原因终止。
- 1 使用操作系统控制手动终止过程。例如，在 Windows 中，可以使用“任务管理器”终止进程。

iVM-CLI 参数

iDRAC IP 地址

```
-r <iDRAC-IP-地址>[:<iDRAC-SSL-端口>]
```

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

<iDRAC-IP-地址>是有效、唯一的 IP 地址或 iDRAC 动态域名系统 (DDNS) 名称（如果支持）。如果省略 <iDRAC-SSL-port>，则使用端口 443（默认端口）。除非更改了 iDRAC 的默认 SSL 端口，否则不需要可选的 SSL 端口。

iDRAC 用户名

```
-u <iDRAC-用户-名称>
```

此参数提供将运行虚拟介质的 iDRAC 用户名。

<iDRAC-用户-名称> 必须具有以下属性：

- 1 有效用户名
- 1 iDRAC 虚拟介质用户权限

如果 iDRAC 验证失败，错误信息将会显示并且命令会终止。

iDRAC 用户密码

-p <iDRAC-用户-密码>

此参数提供指定 iDRAC 用户的密码。

如果 iDRAC 验证失败，错误信息将会显示并且命令会终止。

软盘/磁盘设备或映像文件

-f {<设备名称> | <映像文件>}

其中 <设备-名称> 是有效驱动器号（对于 Windows 系统）或有效设备文件名，包括可安装文件系统分区号，如果可用（对于 Linux 系统）；<映像-文件> 是有效映像文件的文件名和路径。

此参数指定提供虚拟软盘/磁盘介质的设备或文件。

例如，映像文件指定如下：

-f c:\temp\myfloppy.img (Windows 系统)

-f /tmp/myfloppy.img (Linux 系统)

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

例如，设备指定如下：

-f a:\ (Windows 系统)

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

如果设备提供了写保护功能，请使用该功能确保虚拟介质不会写介质。

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

CD/DVD 设备或映像文件

-c {<设备-名称> | <映像-文件>}

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

此参数指定将提供虚拟 CD/DVD-ROM 介质的设备或文件：

例如，映像文件指定如下：

-c c:\temp\mydvd.img (Windows 系统)

-c /tmp/mydvd.img (Linux 系统)

例如，设备指定如下：

-c d:\ (Windows 系统)

-c /dev/cdrom (Linux 系统)

如果不虚拟化 CD/DVD 介质，请在命令行上省略此参数。如果检测到无效值，错误信息将会列出并且命令会终止。

用此命令指定至少一个介质类型（软盘或 CD/DVD 驱动器），除非只提供了开关选项。否则，错误信息将会显示并且命令将终止并生成错误。

版本显示

-v

此参数用于显示 iVM-CLI 公用程序版本。如果没有提供其它非开关选项，此命令将会不显示错消息而终止。

帮助显示

-h

此参数显示 iVM-CLI 公用程序参数的摘要。如果没有提供其它非开关选项，此命令将会无错终止。

手动显示

-m

此参数显示 iVM-CLI 公用程序的详细“man 页”，包括所有可能选项的说明。

加密的数据

-e

如果命令行中包括此参数，iVM-CLI 公用程序将使用 SSL 加密的信道在 management station 和远程系统中的 iDRAC 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。

iVM-CLI 操作系统 Shell 选项

iVM-CLI 命令行中可使用以下操作系统功能：

- 1 `stderr/stdout redirection` — 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 iVM-CLI 公用程序打印的输出覆盖指定的文件。

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

- 1 `后台执行` — 默认情况下 iVM-CLI 公用程序在前台运行。使用操作系统的命令外壳功能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 iVM-CLI 命令启动新进程后继续执行（否则，脚本将保持阻塞直至 iVM-CLI 程序终止）。当有多个 iVM-CLI 实例以这种方式启动，必须手动终止一个或多个命令实例，使用操作系统特定的功能来列出并终止进程。

iVM-CLI 返回代码

0 = 无错误

1 = 无法连接

2 = iVM-CLI 命令行错误

3 = RAC 固件连接已删除

当遇到错误时，文本信息（仅有英文）也会发送到标准错误输出。

[目录](#)

使用 iDRAC 配置公用程序

Integrated Dell™ Remote Access Controller固件版本1.2
用户指南

- [概览](#)
- [启动 iDRAC 配置公用程序](#)
- [使用 iDRAC 配置公用程序](#)

概览

iDRAC 配置公用程序是一个引导前配置环境，允许查看并设置 iDRAC 和 Managed Server 的参数。具体说来，可以：

- 1 查看 iDRAC 和主背板固件的固件版本号
- 1 配置、启用或禁用 iDRAC 局域网
- 1 启用或禁用 LAN 上 IPMI
- 1 启用 LAN 平台事件陷阱 (PET) 目标
- 1 附加或分离虚拟介质设备
- 1 更改管理用户名和密码
- 1 重设 iDRAC 配置为工厂默认值
- 1 查看系统事件日志 (SEL) 信息或从日志清除信息

可以使用 iDRAC 配置公用程序执行的任务还可以用 iDRAC 或 OpenManage 软件提供的其它公用程序执行，包括 Web 界面、SM-CLP 命令行界面、本地 RACADM 命令行界面以及基本网络配置情况下在初始 CMC 配置期间的 CMC LCD。

启动 iDRAC 配置公用程序

必须使用 iKVM 连接的控制台在最初或在重设 iDRAC 为默认设置后访问 iDRAC 配置公用程序。

1. 在连接到 iKVM 控制台的键盘上，按 <Print Screen> 显示 iKVM 的“On Screen Configuration and Reporting (OSCAR)”（屏幕配置和报告 [OSCAR]）菜单。使用 <上箭头> 和 <下箭头> 高亮度显示包含服务器的插槽，然后按 <Enter>。
2. 通过按服务器正面的电源按钮打开或重新启动服务器。
3. 如果看到 **Press <Ctrl-E> for Remote Access Setup within 5 sec.....（在 5 秒内按 <Ctrl-E> 进行远程访问设置.....）** 信息，应立即按 <Ctrl><E>。

 **注：** 如果操作系统在您按 <Ctrl><E> 前开始载入，应让系统完成引导，然后重新启动服务器并重试。

iDRAC 配置公用程序显示。前两行提供了有关 iDRAC 固件和主背板固件修订的信息。在确定是否需要固件升级时，修订级别很有用。

iDRAC 固件是与外部界面相关的部分，比如 SM-CLP 和 Web 界面。主背板固件是监测并交互服务器硬件环境的部分。

使用 iDRAC 配置公用程序

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

- 1 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。
- 1 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。
- 1 如果项目不可编辑，会显示为蓝色。有些项目会根据您所做的其它选择而变得可编辑。
- 1 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。
- 1 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。

LAN

使用<左箭头>、<右箭头>和空格键选择"Enabled"（已启用）和"Disabled"（已禁用）。

在默认配置中，iDRAC LAN 已禁用。必须启用 LAN 来允许使用 iDRAC 功能，比如 Web 界面，telnet/SSH 访问 SM-CLP 命令行界面，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：

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

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

该消息告诉您，除了直接连接 iDRAC HTTP、HTTPS、telnet 或 SSH 端口可以访问的功能外，带外管理网络通信量，比如从 Management Station 发送到 iDRAC 的 IPMI 信息，在 LAN 禁用时也不会收到。本地 RACADM 界面保持可用并且可用来重新配置 iDRAC LAN。

LAN 上 IPMI (On/Off)

按 <左箭头>、<右箭头>和空格键选择 On (开) 和 Off (关)。如果选中 Off (关)，iDRAC 将不会通过 LAN 界面接收 IPMI 信息。

如果选择 Off (关)，以下警告将会显示：

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

Press any key to clear the message and continue. (按任意键清除信息并继续。) 请参阅[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 13-1. LAN 参数

项目	说明
"RMCP+ Encryption Key" (RMCP+ 密钥)	按 <Enter> 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。默认值为 40 个 0 的字符串。
"IP Address Source" (IP 地址源)	选择 DHCP 或"Static"（静态）。如果选中 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），则输入想为 iDRAC 分配的 IP 地址。 默认为 192.168.0.120 加上包含服务器的插槽号。
MAC Address (MAC 地址)	这是 iDRAC 网络接口的不可编辑 MAC 地址。
"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），应输入 iDRAC 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。 默认为 192.168.0.1。
"LAN Alert Enabled" (LAN 警报已启用)	选择 On 启用平台事件陷阱 (PET) LAN 警报。
"Alert Policy Entry 1" (警报策略条目 1)	选择"Enable"（启用）或"Disable"（禁用）激活第一个警报目标。
"Alert Destination 1" (警报目标 1)	输入将要转发 PET LAN 警报的 IP 地址。
"Host Name String" (主机名字符串)	按 <Enter> 以编辑。输入 PET 警报的主机名称。
"DNS Servers from DHCP" (来自 DHCP 的 DNS 服务器)	选择 On (开) 从网络上的 DHCP 服务检索 DNS 服务器地址。选择 Off (关) 指定以下 DNS 服务器地址。
"DNS Server 1" (DNS 服务器 1)	如果"DNS Servers from DHCP" (来自 DHCP 的 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" (来自 DHCP 的 DNS 服务器) 为 Off (关)，则输入第二个 DNS 服务器的 IP 地址。
"Register iDRAC Name" (注册 iDRAC 名称)	选择 On (开) 在 DNS 服务中注册 iDRAC 名称。如果不想用户能够在 DNS 中查找 iDRAC 名称，则选择 Off (关)。

"iDRAC Name" (iDRAC 名称)	如果"Register iDRAC Name" (注册 iDRAC 名称) 设置为 On (开), 按 <Enter> 以编辑"Current DNS iDRAC Name" (当前 DNS iDRAC 名称) 文本字段。完成编辑 iDRAC 名称后按 <Enter>。按 <Esc> 返回上一个菜单。iDRAC 名称必须是有效的 DNS 主机名。
"Domain Name from DHCP" (来自 DHCP 的域名)	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" (来自 DHCP 的域名) 为 Off (关), 则按 <Enter> 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。

虚拟介质

使用 <左箭头> 和 <右箭头> 来选择"Attached" (附加) 或"Detached" (分离)。如果选择"Attached" (附加), 虚拟介质设备会附加到 USB 总线, 从而可以在**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 闪存盘, 在 BIOS 设置公用程序中"USB Flash Drive Emulation Type" (USB 闪存盘仿真类型) 必须设置为"Hard disk" (硬盘)。在服务器启动期间按 <F2> 可访问 BIOS 设置公用程序。如果"USB Flash Drive Emulation Type" (USB 闪存盘仿真类型) 设置为"Auto" (自动), 闪存盘将显示为系统软盘驱动器。

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 13-2. Lan 用户配置页

项目	说明
"Account Access" (帐户访问)	选择"Enabled" (启用) 启用管理员帐户。选择"Disabled" (禁用) 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, 将会显示消息, 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) 菜单项将所有 iDRAC 配置项重设为工厂默认值。如果忘记了管理用户密码或者想从默认设置重新配置 iDRAC, 可能需要这样做。

 **注:** 在默认配置中, iDRAC 网络已禁用。不能在网络上重新配置 iDRAC 直到已在 iDRAC 配置公用程序中启用了 iDRAC 网络。

按 <Enter> 以选择项目。以下警告信息会出现:

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?

< 否 (取消) >

< 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)。系统会显示日志条目并显示总记录数和最新的信息。SEL 保持最多 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> 移动到上一条 (较旧) 信息, <右箭头> 移动到下一条 (较新) 信息。输入记录号跳到该记录。查看完 SEL 信息后按 <Esc>。

 **注:** 只能在 iDRAC 配置公用程序或 iDRAC Web 界面中清除 SEL。

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

使用完 SEL 菜单后, 按 <Esc> 返回上一个菜单。

退出 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> 以保留更改。

选择"Discard Changes and Exit"（**放弃更改并退出**）并按 <Enter> 以忽略所作更改。

选择"Return to Setup"（**返回设置**）并按 <Enter> 以返回 iDRAC 配置公用程序。

[目录](#)

[目录](#)

对 Managed Server 进行恢复和故障排除

Integrated Dell™ Remote Access Controller 固件版本 1.2
用户指南

- [安全第一@C您以及系统](#)
- [故障指示灯](#)
- [问题解决工具](#)
- [故障排除和常见问题](#)

此部分解释如何使用 iDRAC 功能执行与诊断和排除远程 Managed Server 故障相关的任务。包含以下小节：

- 1 故障提示 — 帮助查找可以有助诊断问题的信息和其它系统提示
- 1 问题解决工具 — 说明可以用于排除系统故障的 iDRAC 工具
- 1 故障排除和常见问题 — 有关可能遇到的常见问题的答案

安全第一@C您以及系统

要执行此部分的某些程序，必须是在维护机箱、PowerEdge 服务器或其它硬件模块。不要尝试维修本指南以及系统说明文件介绍之外的系统硬件。

警告： 多数维修只能由经认证的维修技术人员进行。用户只能执行产品说明文件中授权的故障排除和简单维修工作或按照联机或电话服务和支持团队的指示操作。未经 Dell 授权的维修所造成的损坏不在保修范围之内。请阅读并遵循产品附带的安全说明。

故障指示灯

本节介绍可能预示系统出现问题的提示。

LED 指示灯

系统问题的最初提示可能是机箱或机箱组件上的 LED。以下组件和模块具有状态 LED：

- 1 机箱 LCD 显示
- 1 服务器
- 1 风扇
- 1 CMC
- 1 I/O 模块
- 1 电源设备

机箱 LCD 上单一的 LED 汇总了系统中所有组件的状况。LCD 上的稳定蓝色 LED 表示系统中没有检测到错误状况。LCD 上闪烁的琥珀色 LED 表示检测到一个或多个错误状况。

如果机箱 LCD 有闪烁的琥珀色 LED，可以使用 LCD 菜单找出发生错误的组件。请参阅《Dell CMC 固件用户指南》获得 LCD 使用帮助。

[表 14-1](#) 说明了 PowerEdge Server 上 LED 的含义：

表 14-1. 服务器 LED 指示灯

LED 指示灯	含义
稳定绿色	服务器开机。没有绿色 LED 表示服务器没有开机。
稳定蓝色	iDRAC 运行良好。
闪烁琥珀色	iDRAC 检测到错误状况或正在更新固件。
闪烁蓝色	用户已激活此服务器的定位 ID。

硬件故障指示灯

提示模块有硬件问题，包括以下：

- 1 未能通电

- 1 风扇有噪音
- 1 网络连接掉失
- 1 电池、温度、电压或电源监控传感器警报
- 1 硬盘驱动器故障
- 1 USB 介质故障
- 1 由于摔落、浸水或其它外部压力导致的物理损坏

当出现这些问题后，可以尝试用这些方法解决问题：

- 1 重新安置模块并重新启动
- 1 尝试将模块插入机箱中的其它托架
- 1 尝试更换硬盘驱动器或 USB 闪存盘
- 1 重新连接或更换电源和网络电缆

如果这些步骤没有解决问题，请参阅《硬件用户手册》了解硬件设备的特定故障排除信息。

其它故障指示灯

表 14-2. 故障指示灯

查看：	操作：
系统管理软件发出的警报信息	请参阅系统管理软件的说明文件。
系统事件日志信息	请参阅 检查系统事件日志 (SEL) 。
启动开机自检代码中的信息	请参阅 检查开机自检代码 。
上次崩溃屏幕上的信息	请参阅 查看上次系统崩溃屏幕 。
LCD 中服务器状态屏幕上的警报信息	请参阅 在服务器状态屏幕上检查错误信息 。
iDRAC 日志中的信息	请参阅 查看 iDRAC 日志 。

问题解决工具

本部分介绍可以用来诊断系统问题的 iDRAC 功能，特别是尝试远程解决问题时。

- 1 检查系统运行状况
- 1 在系统事件日志中检查错误信息
- 1 检查开机自检代码
- 1 查看上次崩溃屏幕
- 1 在 LCD 上的服务器状态屏幕上检查错误信息
- 1 查看 iDRAC 日志
- 1 访问系统信息
- 1 识别机箱中的 Managed Server
- 1 使用诊断控制台
- 1 管理远程系统上的电源

检查系统运行状况

登录到 iDRAC Web 界面后，显示的第一页说明系统组件的运行状况。[表 14-3](#) 说明系统运行状况指示灯的含义。

表 14-3. 系统运行状况指示灯

指示灯	说明
	绿色复选标记表示健康（正常）状况。

	黄色带有感叹号的三角表示警告（不严重）状况。
	红色 X 表示严重（故障）状况。
	问号图标指示状态未知。

单击“Health”（运行状况）页上的任何组件查看有关组件的信息。会显示电池、温度、电压和电源监控的传感器读数，帮助诊断有些问题。iDRAC 和 CMC 信息页提供了有用的当前状况和配置信息。

检查系统事件日志（SEL）

“SEL Log”（SEL 日志）页显示 managed server 上发生的事件信息。

要查看“System Event Log”（系统事件日志），请执行以下步骤：

1. 单击“System”（系统），然后单击“Logs”（日志）选项卡。
2. 单击“System Event Log”（系统事件日志）以显示“System Event Log”（系统事件日志）页。

“System Event Log”（系统事件日志）页显示系统运行状况指示灯（请参阅表 14-3）、时间戳和事件说明。

3. 单击相应的“System Event Log”（系统事件日志）页按钮以继续（参阅表 14-4）。

表 14-4. SEL 页按钮

按钮	措施
“Print”（打印）	按窗口中显示的排序顺序打印 SEL。
“Clear Log”（清除日志）	清除 SEL。 注： “Clear Log”（清除日志）按钮仅当具有“Clear Logs”（清除日志）权限时显示。
“Save As”（另存为）	打开一个弹出窗口，使您能够将 SEL 保存到所选的目录。 注： 如果正在使用 Internet Explorer 并且在保存时遇到问题，请确保下载 Internet Explorer 的累积安全更新，下载位置是 Microsoft® 支持网站 support.microsoft.com。
“Refresh”（刷新）	重新载入 SEL 页。

检查开机自检代码

“Post Codes”（开机自检代码）页在引导操作系统前显示上次系统开机自检代码。开机自检代码是来自系统 BIOS 的进度指示，表示自打开电源重设的引导顺序的各个阶段，使用户能够诊断与系统引导相关的任何故障。

 **注：** 查看 LCD 显示屏或《硬件用户手册》中的文本，以查找开机自检代码信息编号。

要查看开机自检代码，执行下列步骤：

1. 单击“System”（系统）、“Logs”（日志）选项卡，然后单击“Post Codes”（开机自检代码）。

“Post Codes”（开机自检代码）页显示系统运行状况指示灯（请参阅表 14-3）、十六进制代码和代码说明。

2. 单击相应的“Post Code”（开机自检代码）页按钮以继续（参阅表 14-5）。

表 14-5. 开机自检代码按钮

按钮	措施
“Print”（打印）	打印“Post Codes”（开机自检代码）页。
“Refresh”（刷新）	重载“Post Codes”（开机自检代码）页。

查看上次系统崩溃屏幕

 **注意：** 必须在 Server Administrator 和 iDRAC Web 界面中配置上次崩溃屏幕功能。请参阅[配置受管服务器以捕获上次崩溃屏幕](#)了解配置此功能的说明。

"Last Crash Screen" (上次崩溃屏幕) 页显示最近的崩溃屏幕，包含系统崩溃前发生的事件的信息。上次系统崩溃映像保存在 iDRAC 持续存储中并且可以远程访问。

要查看"Last Crash Screen" (上次崩溃屏幕) 页，请执行以下步骤：

- 1 单击"System" (系统)、"Logs" (日志) 选项卡，然后单击"Last Crash" (上次崩溃)。

"Last Crash Screen" (上次崩溃屏幕) 页提供[表 14-6](#) 中所示的按钮：

 **注：** 如果没有保存的崩溃屏幕，"Save" (保存) 和"Delete" (删除) 按钮不会出现。

表 14-6. 上次崩溃屏幕页按钮

按钮	措施
"Print" (打印)	打印"Last Crash Screen" (上次崩溃屏幕) 页。
"Save" (保存)	打开一个弹出窗口，使您能够将上次崩溃屏幕页保存到所选的目录。
"Delete" (删除)。	删除"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，当系统重设计器配置为太高的值时，"Last Crash Screen" (上次崩溃屏幕) 可能无法捕获。默认设置为 480 秒钟。使用 Server Administrator 或 IT Assistant 将系统重设计器设置为 60 秒，并确保"Last Crash Screen" (上次崩溃屏幕) 运行正常。有关其它信息，请参阅[配置受管服务器以捕获上次崩溃屏幕](#)。

查看最新引导顺序"

如果遇到引导故障，可以从"Boot Capture" (引导捕获) 页面查看前三次引导顺序期间发生的屏幕活动。引导屏幕以每秒钟 1 帧的速率回放。[表 14-7](#)列出可用的控制操作。

 **注：** 必须具有管理员权限才能查看引导捕获顺序的回放。

表 14-7. 引导捕获选项

按钮/选项	说明
选择引导顺序	允许选择待载入和播放的引导顺序。 <ol style="list-style-type: none">1 引导捕获 1 — 载入最新的引导顺序。1 引导捕获 2 — 载入引导捕获 1 之前发生的引导顺序 (第二个最新的引导顺序)。1 引导捕获 3 — 载入引导捕获 2 之前发生的引导顺序 (第三个最新的引导顺序)。
"Save As" (另存为)	创建包含当前顺序所有引导捕获图像的压缩 .zip 文件。用户必须具有管理员权限才能执行此操作。
"Previous Screen" (上一个屏幕)	转到回放控制台的上一个屏幕 (如果有)。
"Play" (播放)	从回放控制台的当前屏幕启动屏幕播放。
"Pause" (暂停)	在回放控制台正在播放的当前屏幕暂停显示屏幕播放。
"Stop" (停止)	停止屏幕播放，并载入引导顺序的第一个屏幕。
"Next Screen" (下一个屏幕)	转到回放控制台的下一个屏幕 (如果有)。
"Print" (打印)	打印出现在屏幕上的引导捕获图像。
"Refresh" (刷新)	重新载入引导捕获页。

在服务器状态屏幕上检查错误信息

如果闪烁的琥珀色 LED 亮起，并且特定服务器出现一个错误，则 LCD 上的主服务器状态屏幕将使用橙色高亮度显示受影响的服务器。使用 LCD 导航按钮高亮度显示受影响的服务器，然后单击中间按钮。将在第二行显示错误和警告信息。下表列出所有错误信息及其严重性。

表 14-8. 服务器状态屏幕

严重性	信息	原因
"Warning" (警告)	系统板环境温度：系统板的温度传感器，警告事件	服务器环境温度越过警告阈值

Critical (严重)	系统板环境温度: 系统板的温度传感器, 故障事件	服务器环境温度越过故障阈值
Critical (严重)	系统板 CMOS 电池: 系统板的电池传感器, 故障已声明	CMOS 电池不存在或没有电压
"Warning" (警告)	系统板系统水平: 系统板的电流传感器, 警告事件	电流越过警告阈值
Critical (严重)	系统板系统水平: 系统板的电流传感器, 故障事件	电流越过故障阈值
Critical (严重)	CPU<编号> <电压传感器名称>: CPU<编号> 的电压传感器, 声明的状态已声明	电压超出范围
Critical (严重)	系统板<电压传感器名称>: 系统板的电压传感器, 声明的状态已声明	电压超出范围
Critical (严重)	CPU<编号> <电压传感器名称>: CPU<编号> 的电压传感器, 声明的状态已声明	电压超出范围
Critical (严重)	CPU<编号> 状态: CPU<编号> 的处理器传感器, IERR 已声明	CPU 故障
Critical (严重)	CPU<编号> 状态: CPU<编号> 的处理器传感器, 热断路已声明	CPU 过热
Critical (严重)	CPU<编号> 状态: CPU<编号> 的处理器传感器配置错误已声明	处理器类型不正确或位置错误
Critical (严重)	CPU<编号> 状态: CPU<编号> 的处理器传感器, 存在已取消声明	所需的 CPU 丢失或不正确
Critical (严重)	系统板视频升降器: 系统板的模块传感器, 拆卸的设备已声明	已拆卸所需模块
Critical (严重)	Mezz B<插槽编号> 状态: Mezz B<插槽编号> 的添加式插卡传感器, 安装错误已声明	为 I/O 结构安装的 Mezzanine 卡不正确
Critical (严重)	Mezz C<插槽编号> 状态: Mezz C<插槽编号> 的添加式插卡传感器, 安装错误已声明	为 I/O 结构安装的 Mezzanine 卡不正确
Critical (严重)	背板驱动器 <编号>: 背板的驱动器插槽传感器, 驱动器已拆卸	存储驱动器已拆卸
Critical (严重)	背板驱动器 <编号>: 背板的驱动器插槽传感器, 驱动器故障已声明	存储驱动器故障
Critical (严重)	系统板 PFault 故障防护: 系统板的电压传感器, 声明的状态已声明	在系统板电压未处于正常水平时生成此事件。
Critical (严重)	系统板操作系统监护程序: 系统板的监护程序传感器, 过期的计时器已声明	IDRAC 监护程序计时器已过期并且没有设置操作。
Critical (严重)	系统板操作系统监护程序: 系统板的监护程序传感器, 重新引导已声明	IDRAC 监护程序检测到系统已崩溃 (由于没有从主机收到响应, 因此计时器过期), 并且操作设置为重新引导。
Critical (严重)	系统板操作系统监护程序: 系统板的监护程序传感器, 关机已声明	IDRAC 监护程序检测到系统已崩溃 (由于没有从主机收到响应, 因此计时器过期), 并且操作设置为关机。
Critical (严重)	系统板操作系统监护程序: 系统板的监护程序传感器, 关机并重新打开电源已声明	IDRAC 监护程序检测到系统已崩溃 (由于没有从主机收到响应, 因此计时器过期), 并且操作设置为关机并重新打开电源。
Critical (严重)	系统板 SEL: 系统板的事件日志传感器, 日志已满已声明	SEL 设备检测到再向 SEL 添加一个条目后就已满。
"Warning" (警告)	ECC 校正错误: 内存传感器, 可校正的 ECC (<DIMM 位置>) 已声明	可校正的 ECC 错误达到严重水平。
Critical (严重)	ECC 不可校正错误: 内存传感器, 不可校正的 ECC (<DIMM 位置>) 已声明	已检测到一个不可校正的 ECC 错误。
Critical (严重)	I/O 信道检查: 严重事件传感器, I/O 信道检查 NMI 已声明	I/O 信道中生成一个严重中断。
Critical (严重)	PCI 奇偶校验错误: 严重事件传感器, PCI PERR 已声明	在 PCI 总线上检测到奇偶校验错误。
Critical (严重)	PCI 系统错误: 严重事件传感器, PCI SERR (<插槽编号或 PCI 设备 ID>) 已声明	设备检测到 PCI 错误
Critical (严重)	SBE 日志禁用: 事件日志传感器, 禁用的可校正内存错误记录已声明	如果记录的 SBE 太多, 会禁用单位错误记录
Critical (严重)	记录禁用: 事件日志传感器, 禁用的所有事件记录已声明	禁用了所有错误记录
不可恢复	CPU 协议错误: 处理器传感器, 到不可恢复的过渡已声明	处理器协议已进入一种不可恢复的状态。
不可恢复	CPU 总线 PERR: 处理器传感器, 到不可恢复的过渡已声明	处理器总线 PERR 已进入一种不可恢复的状态。
不可恢复	CPU 初始化错误: 处理器传感器, 到不可恢复的过渡已声明	处理器初始化已进入一种不可恢复的状态。
不可恢复	CPU 机器检查: 处理器传感器, 到不可恢复的过渡已声明	处理器机器检查已进入一种不可恢复的状态。
Critical (严重)	内存空闲: 内存传感器, 冗余丢失 (<DIMM 位置>) 已声明	内存空闲不再冗余。
Critical (严重)	内存镜像: 内存传感器, 冗余丢失 (<DIMM 位置>) 已声明	镜像内存不再冗余
Critical (严重)	内存 RAID: 内存传感器, 冗余丢失 (<DIMM 位置>) 已声明	RAID 内存不再冗余
"Warning" (警告)	添加的内存: 内存传感器, 存在 (<DIMM 位置>) 已声明	已拆卸添加的内存模块。
"Warning" (警告)	拆卸的内存: 内存传感器, 存在 (<DIMM 位置>) 已取消声明	已拆卸内存模块。
Critical (严重)	内存配置错误: 内存传感器, 配置错误 (<DIMM 位置>) 已声明	系统的内存配置不正确。
"Warning" (警告)	内存冗余增益: 内存传感器, 冗余降级 (<DIMM 位置>) 已声明	内存冗余已降级但未丢失
Critical (严重)	PCIE 严重错误: 严重事件传感器, 总线严重错误已声明	在 PCIE 总线上检测到严重错误。
Critical (严重)	芯片组错误: 严重事件传感器, PCI PERR 已声明	检测到芯片错误。
"Warning" (警告)	内存 ECC 警告: 内存传感器, 从良好到非严重的过渡 (<DIMM 位置>) 已声明	可校正 ECC 错误数已经超出正常水平。
Critical (严重)	内存 ECC 警告: 内存传感器, 从严重到不太严重的过渡 (<DIMM 位置>) 已声明	可校正的 ECC 错误数已达到严重水平。

Critical (严重)	POST 错误: POST 传感器, 没有安装内存	板上没有检测到内存
Critical (严重)	POST 错误: POST 传感器, 内存配置错误	检测到内存, 但是内存不可配置
Critical (严重)	POST 错误: POST 传感器, 不可使用的内存错误	已配置内存, 但内存不可用
Critical (严重)	POST 错误: POST 传感器, 遮罩 BIOS 故障	系统 BIOS 遮罩故障
Critical (严重)	POST 错误: POST 传感器, CMOS 出现故障	CMOS 出现故障
Critical (严重)	POST 错误: POST 传感器, DMA 控制器出现故障	DMA 控制器出现故障
Critical (严重)	POST 错误: POST 传感器, 中断控制器出现故障	中断控制器出现故障
Critical (严重)	POST 错误: POST 传感器, 计时器刷新故障	计时器刷新故障
Critical (严重)	POST 错误: POST 传感器, 可编程间隔计时器错误	可编程间隔计时器错误
Critical (严重)	POST 错误: POST 传感器, 奇偶校验错误	奇偶校验错误
Critical (严重)	POST 错误: POST 传感器, SIO 出现故障	SIO 出现故障
Critical (严重)	POST 错误: POST 传感器, 键盘控制器出现故障	Keyboard controller failure (键盘控制器出现故障)
Critical (严重)	POST 错误: POST 传感器, 系统管理中断初始化失败	系统管理中断初始化失败
Critical (严重)	POST 错误: POST 传感器, BIOS 关闭检测失败	BIOS 关闭检测失败
Critical (严重)	POST 错误: POST 传感器, BIOS POST 内存检测失败	BIOS POST 内存检测失败
Critical (严重)	POST 错误: POST 传感器, Dell 远程访问控制器配置失败	Dell 远程访问控制器配置失败
Critical (严重)	POST 错误: POST 传感器, CPU 配置失败	CPU 配置失败
Critical (严重)	POST 错误: POST 传感器, 内存配置不正确	内存配置不正确
Critical (严重)	POST 错误: POST 传感器, POST 故障	视频后出现一般故障
Critical (严重)	硬件版本错误: 版本更改传感器, 硬件不兼容性已声明	检测到不兼容的硬件
Critical (严重)	硬件版本错误: 版本更改传感器, 硬件不兼容性 (BMC 固件) 已声明	硬件和固件不兼容
Critical (严重)	硬件版本错误: 版本更改传感器, 硬件不兼容性 (BMC 固件和 CPU 不匹配) 已声明	CPU 和固件不兼容
Critical (严重)	内存温度过高: 内存传感器, 可校正的 ECC <DIMM 位置> 已声明	内存模块过热
Critical (严重)	内存严重 SB CRC: 内存传感器, 不可校正的 ECC 已声明	南桥内存故障
Critical (严重)	内存严重 NB CRC: 内存传感器, 不可校正的 ECC 已声明	北桥内存故障
Critical (严重)	监护程序计时器: 监护程序传感器, 重新引导已声明	监护程序计时器已造成系统重新引导
Critical (严重)	监护程序计时器: 监护程序传感器, 计时器过期已声明	监护程序计时器过期但没有采取操作
"Warning" (警告)	链接调节: 版本更改传感器, 成功的软件或 F/W 更改已取消声明	无法为正确的 NIC 操作更新链接调节
"Warning" (警告)	链接调节: 版本更改传感器, 成功的硬件更改 <设备插槽编号> 已取消声明	无法为正确的 NIC 操作更新链接调节
Critical (严重)	LinkT/ FlexAddr: 链接调节传感器, 无法对虚拟 MAC 地址进行编程 (总线 # 设备 # 功能 #) 已声明	无法为此设备进行弹性地址编程
Critical (严重)	LinkT/FlexAddr: 链接调节传感器, 设备选项 ROM 无法支持链接调节或弹性地址 (Mezz <位置>) 已声明	选项 ROM 不支持弹性地址或链接调节。
Critical (严重)	LinkT/ FlexAddr: 链接调节传感器, 无法从 BMC/iDRAC 获得链接调节或弹性地址数据已声明	无法从 BMC/iDRAC 获得链接调节或弹性地址信息
Critical (严重)	LinkT/FlexAddr: 链接调节传感器, 设备选项 ROM 无法支持链接调节或弹性地址 (Mezz XX) 已声明	当 NIC 的 PCI 设备选项 ROM 不支持链接调节或弹性地址功能时产生此事件。
Critical (严重)	LinkT/FlexAddr: 链接调节传感器, 无法对虚拟 MAC 地址 (<位置>) 进行编程已声明	当 BIOS 无法在指定 NIC 设备上对虚拟 MAC 地址进行编程时产生此事件。
Critical (严重)	I/O 严重错误: 严重 IO 组传感器, 严重 IO 错误 (<位置>)	此事件的生成与 CPU IERR 存在关联, 并可指明哪个设备导致 CPU IERR。
"Warning" (警告)	PCIE 非严重错误: 非严重 I/O 组传感器, PCIE 错误 (<位置>)	此事件的生成与 CPU IERR 存在关联。

查看 iDRAC 日志

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

其中"System Event Log" (系统事件日志) (SEL) 包含 Managed Server 中发生的事件记录, "iDRAC Log" (iDRAC 日志) 包含 iDRAC 中发生的事件记录。

要访问 iDRAC 日志, 请执行以下步骤:

- 1 单击"System" (系统) → "Remote Access" (远程访问) → iDRAC, 然后单击"iDRAC Log" (iDRAC 日志)。

iDRAC 日志提供表 14-9 中所列的信息。

表 14-9. iDRAC 日志页面信息

--	--

字段	说明
"Date/Time" (日期/时间)	日期和时间 (例如 Dec 19 16:55:47)。 iDRAC 根据 Managed Server 的时钟设置其时钟。当 iDRAC 最初启动并且无法与 Managed Server 通信时, 时间将会显示为字符串 System Boot。
"Source" (来源)	引起事件的接口。
"Description" (说明)	iDRAC 中记录的事件和用户名的简要说明。

使用 iDRAC 日志页按钮

"iDRAC Log" (iDRAC 日志) 页提供以下按钮 (请参阅表 14-10)。

表 14-10. iDRAC 日志按钮

按钮	措施
"Print" (打印)	打印 "iDRAC Log" (iDRAC 日志) 页。
"Clear Log" (清除日志)	清除 "iDRAC Log" (iDRAC 日志) 条目。 注: 只有您具有 "Clear Logs" (清除日志) 权限时, 才会显示 "Clear Log" (清除日志) 按钮。
"Save As" (另存为)	打开一个弹出窗口, 使您能够将 "iDRAC Log" (iDRAC 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 "iDRAC Log" (iDRAC 日志) 页。

查看系统信息

系统摘要页显示关于以下系统组件的信息:

- 1 系统主机壳
- 1 Integrated Dell Remote Access Controller

要访问系统信息, 请单击 "System" (系统) → "Properties" (属性)。

系统主机壳

表 14-11 和表 14-12 说明系统主机壳属性。

表 14-11. 系统信息字段

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

表 14-12. 自动恢复字段

字段	说明
"Recovery Action" (恢复操作)	当检测到 "系统挂起" 时, iDRAC 可能配置为执行以下某一操作: "No Action" (无操作)、"Hard Reset" (硬重置)、"Power Down" (断电) 或 "Power Cycle" (关机后再开机)。
"Initial Countdown" (初始倒计时)	检测到 "系统挂起" 后经过多少秒 iDRAC 将会执行恢复操作。
"Present Countdown" (当前倒计时)	倒计时计数器的当前值, 以秒为单位。

计数)

Integrated Dell Remote Access Controller

表 14-13 说明 iDRAC 属性。

表 14-13. iDRAC 信息字段

字段	说明
日期/时间	提供 iDRAC 上 GMT 标准的当前日期和时间。
固件版本	列出 iDRAC 固件的版本。
"Firmware Updated" (固件更新)	列出固件上次更新的时间。日期按 UTC 格式显示, 例如: Tue, 8 May 2007, 22:18:21 UTC。
"IP Address" (IP 地址)	标识网络接口的 32-位地址。该值采用“点分隔”格式显示, 比如 143.166.154.127。
"Gateway" (网关)	作为至其它网络网桥的网关 IP 地址。该值采用“点分隔”格式, 比如 143.166.150.5。
子网掩码	标识组成扩展网络前缀和主机号的 IP 地址部分的子网掩码。该值采用“点分隔”格式显示, 比如 255.255.0.0。
MAC Address (MAC 地址)	唯一标识网络中各个 NIC 的介质访问控制 (MAC) 地址, 例如 00-00-0c-ac-08。这是 Dell 分配的 ID 并且不能编辑。
"DHCP Enabled" (是否已启用 DHCP)	Enabled 表示动态主机配置协议 (DHCP) 已启用。 Disabled 表示 DHCP 没有启用。

识别机箱中的 managed server

PowerEdge M1000e 机箱最多可装有十六个服务器。要找到机箱中的特定服务器, 可以使用 iDRAC Web 界面打开服务器上的蓝色闪烁 LED。打开 LED 后, 可以指定想要 LED 闪烁的秒数以确保在 LED 依然闪烁时可以找到机箱。输入 0 会使 LED 一直闪烁直到禁用它。

要识别服务器:

1. 单击"System" (系统) → "Remote Access" (远程访问) → iDRAC → "Troubleshooting" (故障排除)。
2. 在"Identify" (识别) 页上, 选中"Identify Server" (识别服务器) 旁边的值框。
3. 在"Identify Server Timeout" (标识服务器超时) 字段中, 输入想要 LED 闪烁的秒数。如果想要 LED 一直闪烁直到禁用它, 应输入 0。
4. 单击"Apply" (应用)。

服务器上的蓝色 LED 会闪烁指定的秒数。

如果输入 0 保持 LED 闪烁, 应按照这些步骤来禁用它:

1. 单击"System" (系统) → "Remote Access" (远程访问) → iDRAC → "Troubleshooting" (故障排除)。
2. 在"Identify" (识别) 页上, 取消选中"Identify Server" (识别服务器) 旁边的值框。
3. 单击"Apply" (应用)。

使用诊断控制台

iDRAC 提供一组标准网络诊断工具 (参阅表 14-14), 与基于 Microsoft® Windows® 或 Linux 的系统提供的工具类似。使用 iDRAC Web 界面, 可以访问网络调试工具。

要访问"Diagnostics Console" (诊断控制台) 页, 请执行以下步骤:

1. 单击"System" (系统) → iDRAC → "Troubleshooting" (故障排除)。
2. 单击"Diagnostics" (诊断) 选项卡。

表 14-14 说明可以在"Diagnosics Console" (诊断控制台) 页上输入的命令。键入命令并单击"Submit" (提交)。调试结果显示在"Diagnosics Console" (诊断控制台) 页中。

单击"Clear" (清除) 按钮清除上一个命令显示的结果。

要刷新"Diagnosics Console" (诊断控制台) 页, 请单击"Refresh" (刷新)。

表 14-14. 诊断命令

命令	说明
arp	显示地址解析协议 (ARP) 表的内容。ARP 条目不能添加或删除。
ifconfig	显示网络接口表的内容。
netstat	打印路由选择表的内容。
ping <IP 地址>	验证目标 IP 地址是否可以使用当前路由表内容从 iDRAC 进行访问。必须在该选项右侧的字段中输入目标 IP 地址。根据当前的路由选择表内容, 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 iDRAC 跟踪日志。有关详情, 请参阅 gettracelog 。

管理远程系统上的电源

iDRAC 允许在 Managed server 上远程执行几种电源管理操作。使用“Power Management”（电源管理）页在重新引导、开机或关机时通过操作系统执行有序关机。

 **注：** 必须具有“Execute Server Action Commands”（执行服务器操作命令）权限才能执行电源管理操作。请参阅[添加和配置 iDRAC 用户](#)查看配置用户权限的帮助。

1. 单击“System”（系统），然后单击“Power Management”（电源管理）选项卡。
2. 选择“Power Control Action”（电源控制操作），例如，“Reset System (warm boot)”（重设系统 [温引导]）。

[表 14-15](#) 提供有关电源控制操作的信息。

3. 单击“Apply”（应用）以执行所选操作。
4. 单击相应按钮继续。请参阅[表 14-16](#)。

表 14-15. 电源控制操作

“Power On Sysytem”（打开系统电源）	打开系统电源（相当于在系统电源关闭时按电源按钮）。
“Powers Off System”（关闭系统电源）	打开系统电源（相当于在系统电源关闭时按电源按钮）。
“NMI (Non-Masking Interrupt)”（NMI [非屏蔽中断]）	向操作系统发送一个高级中断指令, 使系统暂停运行以进行紧急诊断或故障排除工作。
“Graceful Shutdown”（正常关机）	尝试正常关闭操作系统, 然后关闭系统电源。它需要能识别 ACPI（高级配置和电源接口）的操作系统, 允许系统指导的电源管理。
“Reset System (warm boot)”（重设系统 [温引导]）	重新引导系统而不断电（温引导）。
关闭并打开系统电源	关机并随后重新引导系统（冷引导）。

表 14-16. 电源管理页按钮

按钮	措施
“Print”（打印）	打印屏幕上显示的“Power Management”（电源管理）值。
“Refresh”（刷新）	重新装载“Power Management”（电源管理）页。
“Apply”（应用）	查看“Power Management”（电源管理）页时保存所作的任何新设置。

故障排除和常见问题

[表 14-17](#) 包含有关故障排除问题的常见问题。

表 14-17. 常见问题/故障排除

问题	解答
服务器上的 LED 为闪烁琥珀色。	<p>检查 SEL 信息并随后清除 SEL 以停止闪烁 LED。</p> <p>从 iDRAC Web 界面:</p> <ol style="list-style-type: none"> 1 请参阅检查系统事件日志 (SEL) <p>从 SM-CLP:</p>

	<p>1 请参阅SEL 管理</p> <p>从 iDRAC 配置公用程序:</p> <p>1 请参阅系统事件日志菜单</p>
服务器上有闪烁蓝色 LED。	用户已激活服务器的定位 ID。这是帮助识别机箱中服务器的信号。请参阅 识别机箱中的 managed server 了解有关此功能的信息。
我如何找到 iDRAC 的 IP 地址?	<p>从 CMC Web 界面:</p> <ol style="list-style-type: none"> 单击"Chassis" (机箱) → "Servers" (服务器), 然后单击"Setup" (设置) 选项卡。 单击"Deploy" (部署)。 从显示的表中读出服务器的 IP 地址。 <p>从 iKVM:</p> <ol style="list-style-type: none"> 重新引导服务器并通过按 <Ctrl><E> 进入 iDRAC 配置公用程序 <p>或</p> <ol style="list-style-type: none"> 在 BIOS POST 期间观察显示的 IP 地址。 <p>或</p> <ol style="list-style-type: none"> 在 OSCAR 中选择 "Dell CMC" 控制台以通过本地串行连接登录到 CMC。 <p>CMC RACADM 命令可以从该连接发出。请参阅《CMC 固件用户指南》获得 CMC RACADM 子命令的完整列表。</p>
我如何找到 iDRAC 的 IP 地址? (续)	<p>例如:</p> <pre>\$ racadm getniccfg -m server-1</pre> <p>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</p> <p>从本地 RACADM:</p> <ol style="list-style-type: none"> 在命令提示符处输入以下命令: <pre>racadm getsysinfo</pre> <p>从 LCD:</p> <ol style="list-style-type: none"> 在主菜单上, 高亮度显示"Server" (服务器) 并按选中按钮。 选择寻找 IP 地址的服务器并按选中按钮。
我如何找到 CMC 的 IP 地址?	<p>从 iDRAC Web 界面:</p> <ol style="list-style-type: none"> 单击"System" (系统) → "Remote Access" (远程访问) → CMC。 <p>CMC IP 地址显示在"Summary" (摘要) 页上。</p> <p>或</p> <ol style="list-style-type: none"> 在 OSCAR 中选择 "Dell CMC" 控制台以通过本地串行连接登录到 CMC。CMC RACADM 命令可以从该连接发出。请参阅《CMC 固件用户指南》获得 CMC RACADM 子命令的完整列表。 <pre>\$ racadm getniccfg -m chassis</pre> <p>NIC Enabled (NIC 已启用) = 1 DHCP Enabled (DHCP 已启用) = 1 Static IP Address (静态 IP 地址) = 192.168.0.120 Static Subnet Mask (静态子网掩码) = 255.255.255.0 Static Gateway (静态网关) = 192.168.0.1 Current IP Address (当前 IP 地址) = 10.35.155.151 Current Subnet Mask (当前子网掩码) = 255.255.255.0 Current Gateway (当前网关) = 10.35.155.1 Speed (速度) = Autonegotiate Duplex (双工) = Autonegotiate</p>
iDRAC 网络连接不工作。	<ol style="list-style-type: none"> 确保 LAN 电缆已连接到 CMC。 确保 iDRAC LAN 已启用。
我将服务器插入机箱并按下电源按钮, 但是没有任何反应。	<ol style="list-style-type: none"> iDRAC 需要大约 30 秒初始化, 然后服务器才能通电。等待 30 秒, 然后再次按电源按钮。 检查 CMC 电源预算。机箱电源预算可能超支。
我忘记了 iDRAC 管理用户名和密码。	<p>必须将 iDRAC 恢复为默认设置。</p> <ol style="list-style-type: none"> 重新引导服务器并在提示时按 <Ctrl><E> 并进入 iDRAC 配置公用程序

	<p>2. 在配置公用程序菜单上，高亮度显示“Reset to Default”（重设为默认值）并按 <Enter>。</p> <p>有关详情，请参阅重设为默认值。</p>
如何更改服务器的插槽名称？	<ol style="list-style-type: none"> 1. 登录 CMC Web 界面。 2. 打开“Chassis”（机箱）树并单击“Servers”（服务器）。 3. 单击“Setup”（设置）选项卡。 4. 在服务器的行中键入插槽的新名称。 5. 单击“Apply”（应用）。
从 iDRAC Web 界面启动控制台重定向会话时，ActiveX 安全弹出窗口将会出现。	<p>从客户端浏览器看，iDRAC 可能不是受信任的站点。</p> <p>要防止每次启动控制台重定向会话都出现安全弹出窗口，应将 iDRAC 添加到受信任的站点列表：</p> <ol style="list-style-type: none"> 1. 单击“Tools”（工具）→“Internet Options...”（Internet 选项...）→“Security”（安全）→“Trusted sites”（信任的站点）。 2. 单击“Sites”（站点）并输入 iDRAC 的 IP 地址或 DNS 名称。 3. 单击 Add（添加）。
启动控制台重定向会话时，查看器屏幕为空白。	<p>如果具有“Virtual Media”（虚拟介质）权限但没有“Console Redirection”（控制台重定向）权限，将能够启动查看器以便可以访问虚拟介质功能，但是 Managed Server 的控制台将不显示。</p>
iDRAC 不引导。	<p>卸下并重新插入服务器。</p> <p>检查 CMC Web 界面查看 iDRAC 是否显示为可升级组件。如果是，请按使用 CMC 恢复 iDRAC 固件的说明操作。</p> <p>如果没有解决问题，请联络技术支持部门。</p>
尝试引导 Managed Server 时，电源指示灯为绿色，但是根本没有 POST 或视频。	<p>如果出现以下情况，可能会发生此现象：</p> <ol style="list-style-type: none"> 1 内存未安装或不可访问。 1 CPU 未安装或不可访问。 1 视频提升卡缺失或连接不正确。 <p>另外，在 iDRAC Web 界面或 LCD 的 iDRAC 日志中查找错误信息。</p>

[目录](#)

词汇表

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

Active Directory

Active Directory 是一种集中标准化的系统，能够自动化用户数据、安全性和分布式资源的网络管理，并支持与其它目录系统的互操作。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) 的缩写，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) 的缩写，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) 的缩写，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，并控制系统引导进程的初始阶段，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 将向申请者颁发认证，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

竞争握手验证协议 (Challenge-Handshake Authentication Protocol) 的缩写，PPP 服务器使用的一种验证方法，用于确认连接创始者的身份。

CIM

公用信息模型 (Common Information Model) 的缩写，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

认证签名请求 (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

格林尼治平均时 (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）的标准太阳时间。

GPIO

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

GRUB

GRand 统一引导加载程序 (GRand Unified Bootloader) 的缩写，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 控制信息协议 (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 的缩写，集成的系统芯片监测/控制 Dell 11G PowerEdge 服务器系统。

IP

网际协议 (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) 的缩写。

MAC

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

Managed System

由"Management station" (管理站) 监测的系统称为 Managed System。

Management Station

"Management station" (管理站) 是一种系统, 从该系统管理员可远程管理带有 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。

MI

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

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

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文报 (例如 IP 信息包)。

RAC

Remote Access Controller 的缩写。

RAM

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

RAM

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) 的缩写，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 的缩写。

SAP

服务访问点 (Service Access Point) 的缩写。

SEL

系统事件日志 (system event log) 的缩写。

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，用以优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 是交换信息的运送机制。WS-MAN 提供用于设备的通用语言来共享数据，由此使数据管理更加简单。

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。

扩展架构

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。

标准架构

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](#)

RACADM 子命令概览

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [help](#)
- [arp](#)
- [clearasrscreen](#)
- [config](#)
- [getconfig](#)
- [coredump](#)
- [coredumpdelete](#)
- [fwupdate](#)
- [getssninfo](#)
- [getsysinfo](#)
- [gettractime](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racdump](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [clrraclog](#)
- [getsel](#)
- [clrsel](#)
- [gettracelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [_sslcertview](#)
- [sslkeyupload](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)
- [vmkey](#)
- [usercertupload](#)
- [usercertview](#)
- [localConRedirDisable](#)

本节提供了 RACADM 命令行界面中可用子命令的说明。

help

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

[表 A-1](#) 说明了 `help` 命令。

表 A-1. Help 命令

命令	定义
<code>help</code>	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` 子命令列出了可以同 `racadm` 命令一起使用的所有子命令，并且为每个子命令提供了一行说明。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

- 1 本地 RACADM
- 1 远程 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

- 1 远程 RACADM
 - 1 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

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

config

 **注：** 要使用 getconfig 命令，必须具有“Log In iDRAC”（登录 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
-----	----

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

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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”值指定。
-c	-c, 或检查选项, 与 config 子命令配合使用, 并使用用户可以分析 .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:

- 1 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
- 1 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

```
1 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。

```
1 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 cfglpmiPet 和 cfglpmiPef 组创建条目。必须至少设置一个陷阱目标以将 cfglpmiPet 组捕获到文件中。
-g	-g <组名> (即组选项) 可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，则应使用 -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用户名。
-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：

- 1 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
- 1 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

```
1 racadm getconfig -g cfgLanNetworking  
  
显示组 cfgLanNetworking 中包含的所有配置属性（对象）。  
  
1 racadm getconfig -f myrac.cfg  
  
将所有组配置对象从 iDRAC6 保存到 myrac.cfg。  
  
1 racadm getconfig -h  
  
显示 iDRAC6 上可用配置组的列表。  
  
1 racadm getconfig -u root  
  
显示用户命名为 root 的配置属性。  
  
1 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

- 1 本地 RACADM
 - 1 远程 RACADM
 - 1 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
<code>coredump</code>	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：

- 1 使用 `coredumpdelete` 子命令清除 `coredump` 信息。
- 1 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

- 1 远程 RACADM
 - 1 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

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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“[iDRAC6 的高级配置](#)”了解其他说明。

[表 A-9](#) 说明了 `fwupdate` 子命令。

表 A-9. fwupdate

子命令	定义
<code>fwupdate</code>	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 -r
```

说明

`fwupdate` 子命令使用户能够更新 iDRAC6 上的固件。用户可以：

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

支持的接口

- 1 本地 RACADM
- 1 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。

表 A-10. fwupdate 子命令选项

选项	说明
-u	更新 选项，对固件更新文件执行检查和，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 会执行软重置。
-s	状况 选项，返回所在更新进程中的当前状况。此选项始终为自动运行。
-g	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	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

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

在本示例中，-g 选项告诉固件从 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 会重置。

```
1 racadm fwupdate -s
```

此选项将读取固件更新的当前状况。

```
1 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。

getssninfo

 **注：** 要使用此命令，必须具有“Log In To iDRAC”（登录 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：

- 1 "Username" (用户名)
- 1 "IP address" (IP 地址) (如果可用)
- 1 "Session type" (会话类型) (例如, 串行或远程登录)
- 1 "Consoles in use" (使用的控制台) (例如, Virtual Media 或 Virtual KVM)

支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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 "*" 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

```
1 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	Type (类型)	控制台
root	192.168.0.10	Telnet	Virtual KVM

```
1 racadm getssninfo -A
"root" "143.166.174.19" "Telnet" "NONE"
1 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 iDRAC) 权限。

[表 A-14](#) 说明了 `racadm getsysinfo` 子命令。

表 A-14. `getsysinfo`

命令	定义
<code>getsysinfo</code>	显示 iDRAC6 信息、系统信息和监护程序状况信息。

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

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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 Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
Last Firmware Update = 09/25/2008 18:08:31
Hardware Version = 0.01
MAC Address = 00:1e:c9:b2:c7:1f

Common settings:
Register DNS RAC Name = 0
DNS RAC Name = iDRAC6
Current DNS Domain =
Domain Name from DHCP = 0

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
Current IP Gateway = 192.168.0.1
Current IP Netmask = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0

IPv6 settings:
Enabled = 0
Current IP Address 1 = 2002:0000:0000::0001
Current IP Gateway = ::
Prefix Length = 64
Autoconfig = 1
```

```
DNS Server from DHCPv6 = 0
Current DNS Server 1 = ::
Current DNS Server 2 = ::
```

```
System Information:
System Model = PowerEdge R610
System BIOS Version = 0.2.4
BMC Firmware Version = 0.32
Service Tag = AC056
Host Name =
OS Name =
Power Status = ON
```

```
Watchdog Information:
Recovery Action = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

示例

```
l racadm getsysinfo -A -s

"System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"

"Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"

l racadm getsysinfo -w -s
```

```
System Information:
System Model           = PowerEdge 2900
System BIOS Version   = 0.2.3
BMC Firmware Version  = 0.17
Service Tag           = 48192
Host Name              = racdev103
OS Name                = Microsoft Windows Server 2003
Power Status           = OFF
```

```
Watchdog Information:
Recovery Action       = None
Present countdown value = 0 seconds
Initial countdown value = 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 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

`getractive` 子命令将输出显示在一行上。

示例输出

```
racadm getractive
Thu Dec 8 20:15:26 2005

racadm getractive -d
20051208201542.000000
```

支持的接口

- 1 本地 RACADM
 - 1 远程 RACADM
 - 1 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
<code>ifconfig</code>	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
<code>netstat</code>	显示路径选择表和当前连接。

提要

```
racadm netstat
```

支持的接口

- 1 远程 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由表内容从 iDRAC6 进行访问。需要目标 IP 地址。ICMP 回送数据包根据当前的路由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

- 1 远程 RACADM
- 1 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：** 术语 NIC 和以太网管理端口可以互换使用。

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。

- 1 -d 选项为以太网管理端口启用 DHCP（默认是禁用 DHCP）。
- 1 -d6 选项为以太网管理端口启用“AutoConfig”（自动配置）。默认为启用。
- 1 -s 选项启用静态 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。
- 1 -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。

- 1 -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

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

getniccfg

 **注：** 要使用 `getniccfg` 命令，必须具有“Log In To iDRAC”（登录 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
<code>getniccfg</code>	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      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway          = 192.168.0.1
```

支持的接口

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

getsvctag

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

[表 A-22](#) 说明了 `getsvctag` 子命令。

表 A-22. getsvctag

子命令	定义
<code>getsvctag</code>	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

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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
<code>racdump</code>	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：

- 1 常规系统/RAC 信息
- 1 内核转储
- 1 会话信息

- 1 进程信息
- 1 固件版次信息

支持的接口

- 1 远程 RACADM
- 1 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
<code>racreset</code>	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
<code>hard</code>	硬重设会对 Remote Access Controller 执行深层重设操作。硬重设只应作为恢复 iDRAC6 控制器的最后尝试的手段。
<code>soft</code>	软重设会对 RAC 执行正常重新引导操作。

示例

- ```
1 racadm racreset
 启动 iDRAC6 软重设序列。

1 racadm racreset hard
 启动 iDRAC6 硬重设序列。
```

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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                     |
|--------------------------|------------------------|
| <code>racresetcfg</code> | 将全部 iDRAC6 配置重设为工厂默认值。 |

## 提要

```
racadm racresetcfg
```

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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，这些属性用于将插卡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 和串行配置重设为初始默认设置。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（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                                    |
|---------------------------|---------------------------------------|
| <code>serveraction</code> | 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 |
|-----|----|
|-----|----|

|                   |                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;操作&gt;</b> | 指定操作。以下为 <操作> 字符串的选项： <ul style="list-style-type: none"> <li>1 <b>powerdown</b> — 关闭 Managed System 电源。</li> <li>1 <b>powerup</b> — 打开 Managed System 电源。</li> <li>1 <b>powercycle</b> — 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后再打开系统电源。</li> <li>1 <b>powerstatus</b> — 显示服务器的当前电源状况（“ON”或“OFF”）</li> <li>1 <b>hardreset</b> — 在 Managed System 上执行重置（重新引导）操作。</li> </ul> |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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

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

## getraclog

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

[表 A-29](#) 说明了 **racadm getraclog** 命令。

**表 A-29. getraclog**

| 命令                  | 定义                 |
|---------------------|--------------------|
| <b>getraclog -i</b> | 显示 iDRAC6 日志中的条目数。 |
| <b>getraclog</b>    | 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：

- 1 **-A** — 不带页眉或标签显示输出。
- 1 **-c** — 提供要被返回的最大条目数。
- 1 **-m** — 一次显示一屏信息并提示用户继续（类似于 UNIX **more** 命令）。
- 1 **-o** — 以一行显示输出。
- 1 **-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 日午夜开始并一直持续到系统引导。系统引导后，就会使用系统的时间戳。

## 示例输出

```
Record: 1
Date/Time: Dec 8 08:10:11
Source: login[433]
Description: 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 iDRAC）权限。

[表 A-30](#) 说明了 `getsel` 命令。

**表 A-30. getsel**

| 命令                     | 定义             |
|------------------------|----------------|
| <code>getsel -i</code> | 显示系统事件日志中的条目数。 |
| <code>getsel</code>    | 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 日志中的条目数。

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: 1
Date/Time: 11/16/2005 22:40:43
Severity: Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

## 支持的接口

- 1 本地 RACADM
  - 1 远程 RACADM
  - 1 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) 删除全部现有的记录。

## 支持的接口

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

## gettracelog

 **注：** 要使用此命令，必须具有“Log In To iDRAC”（登录 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 日午夜开始并一直持续到系统引导。系统引导后, 就会使用系统的时间戳。

例如:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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 认证签名请求 (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 可用于创建自定义 SSL 认证以在 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                             |
|-----------|--------------------------------|
| <b>-g</b> | 生成新的 CSR。                      |
| <b>-s</b> | 返回 CSR 生成进程的状况（正在生成、活动或无）。     |
| <b>-f</b> | 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况代码之一：

- 1 CSR 成功生成。
- 1 CSR 不存在。
- 1 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串行、远程登录或 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

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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                              |
|----------------------|---------------------------------|
| <b>sslcertupload</b> | 从客户端到 RAC 上载自定义 SSL 服务器或 CA 认证。 |

## 提要

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

## 选项

[表 A-35](#) 说明了 `sslicertupload` 子命令选项。

**表 A-35. sslicertupload 子命令选项**

| 选项 | 说明                                                        |
|----|-----------------------------------------------------------|
| -t | 指定要上传的认证类型，CA 认证或服务器认证。<br>1 = 服务器认证<br>2 = CA 认证         |
| -f | 指定要上传的认证文件名。如果没有指定文件，将会选择当前目录中的 <code>sslicert</code> 文件。 |

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

## 限制

`sslicertupload` 子命令只能从本地或远程 RACADM 客户端执行。`sslicsrngen` 子命令不能用在串行、远程登录或 SSH 接口中。

## 示例

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

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM

---

## sslicertdownload

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

[表 A-36](#) 说明了 `sslicertdownload` 子命令。

**表 A-36. sslicertdownload**

| 子命令                         | 说明                           |
|-----------------------------|------------------------------|
| <code>sslicertupload</code> | 将 SSL 认证从 iDRAC6 下载到客户的文件系统。 |

## 提要

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

## 选项

[表 A-37](#) 说明了 `sslicertdownload` 子命令选项。

**表 A-37. sslicertdownload 子命令选项**

| 选项 | 说明                                                |
|----|---------------------------------------------------|
| -t | 指定要下载的认证类型，Microsoft® Active Directory® 认证或服务器认证。 |

|           |                                                                   |
|-----------|-------------------------------------------------------------------|
|           | 1 = 服务器认证                                                         |
|           | 2 = Microsoft Active Directory 认证                                 |
| <b>-f</b> | 指定要上传的认证文件名。如果没有指定 <b>-f</b> 选项或文件名，将会选择当前目录中的 <b>sslcert</b> 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** 子命令不能用在串行、远程登录或 SSH 接口中。

## 示例

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

## 支持的接口

- 1 本地 RACADM
- 1 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                          |
|--------------------|-----------------------------|
| <b>sslcertview</b> | 显示 RAC 上存在的 SSL 服务器或 CA 认证。 |

## 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                                                                                                |
|-----------|---------------------------------------------------------------------------------------------------|
| <b>-t</b> | 指定要查看的认证类型，Microsoft Active Directory 认证或服务器认证。<br>1 = 服务器认证<br>2 = Microsoft Active Directory 认证 |
| <b>-A</b> | 不显示标头/标签。                                                                                         |

## 输出示例

```
racadm sslcertview -t 1
Serial Number : 00
```

```
Subject Information:
Country Code (CC) : US
State (S) : Texas
Locality (L) : Round Rock
Organization (O) : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN) : iDRAC6 default certificate
```

```
Issuer Information:
Country Code (CC) : US
State (S) : Texas
Locality (L) : Round Rock
Organization (O) : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN) : iDRAC6 default certificate
```

```
Valid From : Jul 8 16:21:56 2005 GMT
Valid To : Jul 7 16:21:56 2010 GMT
```

```
racadm sslcertview -t 1 -A
```

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

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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                     |
|---------------------------|------------------------|
| <code>sslkeyupload</code> | 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        |
|-----------------|-----------|
| <code>-t</code> | 指定要上载的密钥。 |

|    |                      |
|----|----------------------|
|    | 1 = SSL 密钥用于生成服务器证书。 |
| -f | 指定要上传的 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。不能用于串行、远程登录或 SSH 接口。

## 示例

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

## 支持的接口

- 1 本地 RACADM
- 1 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 cfgRhostsSmtServerIpAddr -i 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

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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 testtrap 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><br>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

- 1 本地 RACADM
  - 1 远程 RACADM
  - 1 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况。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

- 1 本地 RACADM
  - 1 远程 RACADM
  - 1 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传到 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置回初始默认大小，在 iDRAC6 上为 256 MB。

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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 | 将用户认证或用户 CA 认证从客户端上载到 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 | 指定要上载的认证类型，CA 认证或服务器认证。<br>1 = 用户认证<br>2 = 用户 CA 认证 |
| -f | 指定要上载的认证文件名。如果没有指定文件，将会选择当前目录中的 <b>sslicert</b> 文件。 |
| -i | 用户的索引号。有效 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

- 1 本地 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 上的用户认证或用户 CA 认证。 |

## 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 | 指定要查看的认证类型，用户认证或用户 CA 认证。<br>1 = 用户认证<br>2 = 用户 CA 认证 |
| -A | 不显示标头/标签。                                             |
| -i | 用户的索引号。有效 1-16。                                       |

## 支持的接口

- 1 本地 RACADM
- 1 远程 RACADM
- 1 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

- 1 本地 RACADM
- 

[目录](#)

[目录](#)

## iDRAC6 属性数据库组和对象定义

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [可显示字符](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgRemoteHosts](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgOobSnmpp](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgIpmiSsl](#)
- [cfgIpmiLan](#)
- [cfgIpmiPetIpv6](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)
- [cfgUserDomain](#)
- [cfgServerPower](#)
- [cfgIpv6LanNetworking](#)
- [cfgIpv6URL](#)
- [cfgIpmiSerial](#)
- [cfgSmartCard](#)
- [cfgNetTuning](#)

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。以下部分说明各个对象并指出对象是否可读、可写或可以读写。

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：

abcdefghijklmnopqrstuvwxyz

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 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@/-©

### 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)

**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 作为远程访问的专用 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。<br><br>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 @C 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。必须至少一个字符为字母。

 **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，就不能访问至 iDRAC6 的远程网络接口。

## cfgNicIpAddress (读/写)

 **注：** 此参数只有在 `cfgNicUseDhcp` 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` 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` 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:）。

## cfgRhostsSntpServerIpAddr（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 传送电子邮件警报。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 @C 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](#) 说明了可以组合创建位掩码的用户权限位值。

表 B-2. 用户权限位掩码

| 用户权限      | 权限位掩码     |
|-----------|-----------|
| 登录到 iDRAC | 0x0000001 |
| 配置 iDRAC  | 0x0000002 |
| 配置用户      | 0x0000004 |
| 清除日志      | 0x0000008 |
| 执行服务器控制命令 | 0x0000010 |
| 访问控制台重定向  | 0x0000020 |
| 访问虚拟介质    | 0x0000040 |
| 检测警报      | 0x0000080 |
| 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>（其他所有）

### 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（其他所有）

### 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 Serial Over LAN (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@C4

### 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 @C 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 @C 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 @C 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闲置（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以使新设置生效）。

## cfgSsnMgtSshIdleTimeout（读/写）

### 有效值

0（无超时）

60 @C 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闲置（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以使新设置生效）。

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 @C 1920

### 默认值

300

## 说明

定义远程登录空闲超时。此属性设置允许连接保持闲置（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以使新设置生效）。

过期的远程登录会话将显示以下错误信息：

"Connection timed out"（连接超时）

出现此信息后，系统会返回到生成远程登录会话的 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 串行接口上的波特率。

## 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：

- 1 十进制值 — 例如：“95”
- 1 十六进制值 — 例如：“0x12”
- 1 八进制值 — 例如：“007”
- 1 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 @C 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 @C 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 上的远程登录控制台接口

---

## 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@/-©

### 有效值

1 C 65535

### 默认值

5900

### 说明

指定供至 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

### cfgRacTuneCtrlIEConfigDisable

#### 有效值

1 (TRUE)

0 (FALSE)

#### 默认值

0

#### 说明

启用该选项后，即可禁用本地用户从 BIOS POST 选项-ROM 配置 iDRAC 的能力。

### cfgRacTuneHttpPort (读/写)

#### 有效值

1 @C 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 @C 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

## cfgRacTuneIpBIKEnable (读/写)

#### 有效值

1 (TRUE)

0 (FALSE)

#### 默认值

0

#### 说明

启用或禁用 iDRAC6 的 IPv4 地址阻止功能

### cfgRacTuneIpBlkFailCount (读/写)

#### 有效值

2 @C 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 @C 65535

#### 默认值

60

#### 说明

定义计数失败尝试的时间长度 (秒)。当达到失败尝试的限制数后，将不计失败。

### cfgRacTuneIpBlkPenaltyTime (读/写)

#### 有效值

10 @C 65535

#### 默认值

300

### 说明

如果在定义的秒数内来自某 IP 地址的会话请求失败次数过多，请求则会被拒绝

## cfgRacTuneSshPort (读/写)

### 有效值

1 @C 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 @C 65535

### 默认值

23

### 说明

指定用于 iDRAC6 远程登录接口的端口号

## 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

## 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 服务器。如果禁用此属性，将无法使用客户端 Web 浏览器访问 iDRAC6。此属性对于远程登录/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](#) 子命令详细了解有关生成认证签名请求的详情。

## 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：** 要使其更改生效，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盘符 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 操作系统将会分配盘符 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。

## cfgAD RacDomain (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

## cfgAD RacName (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

## cfgAD Enable (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。

## cfgAD DomainController1 (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 @C 300 秒

### 默认值

120

### 说明

如果在指定秒数后，Active Directory 验证请求仍未完成，则显示超时。

## 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 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 标准架构设置。

## cfgSSADRoleGroupIndex (只读)

### 有效值

1 到 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

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        |
|-----------|------------|
| 登录到 iDRAC | 0x00000001 |
| 配置 iDRAC  | 0x00000002 |
| 配置用户      | 0x00000004 |
| 清除日志      | 0x00000008 |
| 执行服务器控制命令 | 0x00000010 |
| 访问控制台重定向  | 0x00000020 |
| 访问虚拟介质    | 0x00000040 |
| 检测警报      | 0x00000080 |
| 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 @C 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 @C 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 个字符的十六进制字符串，不带空格。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 @C 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 警报目的地 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 警报目的地

---

## 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 @C 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（重置）

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 @C 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。任何给定时间都能配置不超过 40 个域名。

### cfgUserDomainIndex (只读)

#### 有效值

1 @C 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，此属性控制最小容量电源的增长情况。

### 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 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 链接本地地址**

**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 串行接口的换行序列规范

## 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

启用或禁用证书撤销列表 (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。

 **小心：** 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

启用物理链接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 @C 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](#)

## 支持的 RACADM 接口

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 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             | ✓                 | ✗         | ✓         |
| clearascreen    | ✓                 | ✓         | ✓         |
| 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

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [iDRAC6 Express 管理功能](#)
- [iDRAC6 Enterprise](#)
- [iDRAC6 安全 功能](#)
- [支持的平台](#)
- [支持的操作系统](#)
- [支持的 Web 浏览器](#)
- [支持的远程访问连接](#)
- [iDRAC6 端口](#)
- [您可能需要的其它说明文件](#)

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。服务器操作系统与正在执行的应用程序相关；iDRAC6 与监测和管理操作系统之外的服务器环境和状态相关。

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 iDRAC6 在网络上配置后，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：

- 1 动态域名系统 (DDNS) 注册
- 1 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
- 1 支持 Microsoft® Active Directory® 验证 — 使用扩展架构或标准架构将 iDRAC6 用户 ID 和密码集中在 Active Directory 中
- 1 监控 — 提供对系统信息和组件状态的访问
- 1 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
- 1 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
- 1 iDRAC6 警报 — 通过电子邮件信息或 SNMP 陷阱提示潜在管理节点问题
- 1 远程电源管理 — 从管理控制台提供远程电源管理功能，比如关闭系统和重置
- 1 智能平台管理接口 (IPMI) 支持
- 1 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
- 1 密码级别安全性管理 — 防止未授权访问远程系统
- 1 基于角色的授权 — 为不同的系统管理任务提供可分配的权限
- 1 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
- 1 WS-MAN 支持 — 使用 Web Services for Management (WS-MAN) 协议提供网络可访问管理。
- 1 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。
- 1 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](http://support.dell.com/manuals) 上的《硬件用户手册》。

---

## iDRAC6 Enterprise

增加对 RACADM、虚拟 KVM、虚拟介质功能、专用 NIC 和虚拟闪存更新（带可选 Dell vFlash 介质卡）的支持。有关 iDRAC6 Enterprise 的详情，请参阅 [support.dell.com/manuals](http://support.dell.com/manuals) 上的《硬件用户手册》。

---

## iDRAC6 安全 功能

iDRAC6 提供以下安全保护功能：

- 1 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
- 1 基于角色的授权，使管理员能为每个用户配置特定权限
- 1 通过基于 Web 的界面或 SM-CLP 进行用户 ID 和密码配置

- 1 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
- 1 通过 Web 界面或 SM-CLP 进行会话超时配置（以秒为单位）
- 1 可配置 IP 端口（在相应情况下）

 **注：** Telnet 不支持 SSL 加密技术。

- 1 SSH，其使用加密传输层增强安全保护
- 1 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
- 1 能够限制连接到 iDRAC6 的客户端的 IP 地址范围
- 1 Smart Card 验证

## 支持的平台

iDRAC6 支持以下 PowerEdge 系统：

- 1 PowerEdge R710
- 1 PowerEdge R610
- 1 PowerEdge T610

要了解最新支持的平台，请查阅 [support.dell.com/manuals](http://support.dell.com/manuals) 上和系统随附的 *Dell Systems Management Tools and Documentation* DVD 上的 iDRAC6 自述文件和《*Dell OpenManage Server Administrator 兼容性指南*》。

## 支持的操作系统

[表 1-1](#) 列出支持 iDRAC6 的操作系统。

要了解最新信息，请参阅 Dell 支持网站 [support.dell.com/manuals](http://support.dell.com/manuals) 上和系统随附的 *Dell Systems Management Tools and Documentation* DVD 上的《*Dell OpenManage Server Administrator 兼容性指南*》。

**表 1-1. 支持的 Managed Server 操作系统**

| 操作系统系列            | 操作系统                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Windows | <p>Windows Server® 2003 系列，包括：</p> <p>Windows Server 2003 R2 (Web、Standard 和 Enterprise 版本) (含 SP2) (x86)</p> <p>Windows Server 2003 R2 (Standard、Enterprise 和 DataCenter 版本) (含 SP2) (x64)</p> <p>Windows Server 2003 (SBS、Standard 和 Premium 版本) (含 SP2)</p> <p><b>注：</b> 安装 Windows Server 2003 with Service Pack 1 时，应注意更改 DCOM 安全设置。有关详情，请参阅 Microsoft 支持网站文章 903220 <a href="http://support.microsoft.com/kb/903220">support.microsoft.com/kb/903220</a>。</p> <p>Windows Server 2008 Core (Web、Standard 和 Enterprise 版本) (x86)</p> <p>Windows Server 2008 Core (Standard、Enterprise 和 DataCenter 版本) (x64)</p> <p>Windows Server 2008 SBS、EBS、Standard 和 Premium 版本</p> |
| SUSE® Linux       | Enterprise Server 10 SP2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Red Hat® Linux®   | <p>Enterprise Linux 4.7 (x86_32、x86_64)</p> <p>Enterprise Linux 5 U2 (x86_32、x86_64)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| VMware®           | <p>ESX 3.5 U4</p> <p>ESXi 3.5 U4 Flash</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## 支持的 Web 浏览器

[表 1-2](#) 列出了作为 iDRAC6 客户端支持的 Web 浏览器。

要了解最新信息，请参阅 iDRAC6 自述文件和《Dell OpenManage Server Administrator 兼容性指南》（位于 Dell 支持网站 [support.dell.com/manuals](http://support.dell.com/manuals)）。

 **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。

**表 1-2. 支持的 Web 浏览器**

| 支持的 Web 浏览器                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 适用于 Windows XP、Windows 2000 Server、Windows 2000 Pro、Windows 2003 Server Gold、Windows 2003 Server SP1 和 Windows 2003 Server SP2 的 Microsoft Internet Explorer 6.0 SP2                                                   |
| 适用于 Windows 2003 Server Gold、Windows 2003 Server SP1、Windows 2003 Server SP2、Windows Server 2008 和 Windows Vista 的 Microsoft Internet Explorer 7.0                                                                     |
| SUSE Linux Enterprise Server (SLES) 10 SP1 上的 Mozilla Firefox 2.0                                                                                                                                                      |
| Windows 2003 Server Gold、Windows 2003 Server SP1、Windows 2003 Server SP2、Windows 2000 Pro、Windows XP、Windows Server 2008、Windows Vista、Red Hat Enterprise Linux 4 和 5、SLES 9 和 10 及 SLES 10 SP1 上的 Mozilla Firefox 3.0 |

## 支持的远程访问连接

[表 1-3](#) 列出连接功能。

**表 1-3. 支持的远程访问连接**

| 连接         | 功能                                                                                                                                                                                                                                                                |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iDRAC6 NIC | <ul style="list-style-type: none"> <li>1 10Mbps/100Mbps/以太网</li> <li>1 DHCP 支持</li> <li>1 SNMP 陷阱和电子邮件事件通知</li> <li>1 支持 SM-CLP (Telnet 或 SSH) 命令 Shell，进行诸如 iDRAC6 配置、系统引导、重置、开机和关机命令等操作</li> <li>1 支持 IPMI 公用程序，比如 IPMITool 和 ipmish</li> <li>1 串行连接</li> </ul> |

## iDRAC6 端口

[表 1-4](#) 列出 iDRAC6 侦听连接的端口。[表 1-5](#) 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 1-4. iDRAC6 服务器侦听端口**

| "Port Number" (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 1-5. iDRAC6 客户端端口**

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

---

## 您可能需要的其它说明文件

除了本《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](http://support.dell.com/manuals) 获取这些说明文件。

- 1 iDRAC6 联机帮助提供了有关使用基于 Web 界面的详情。
- 1 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*》。
- 1 有关使用 IT Assistant 的信息，请参阅《*Dell OpenManage IT Assistant 用户指南*》。
- 1 有关安装 iDRAC6 的信息，请参阅《*硬件用户手册*》。
- 1 有关安装和使用 Server Administrator 的信息，请参阅《*Dell OpenManage Server Administrator 用户指南*》。
- 1 要了解最新支持的平台，请查阅 iDRAC6 自述文件和《*Dell OpenManage Server Administrator 兼容性指南*》。
- 1 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*》。
- 1 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：

- 1 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。
- 1 《*使用入门指南*》概述了系统功能、系统设置以及技术规格。
- 1 《*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。
- 1 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。
- 1 操作系统说明文件介绍了如何安装（如果有必要）、配置和使用操作系统软件。
- 1 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。
- 1 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。

- 1 系统可能附带的版本注释或自述文件，提供了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了高级技术参考资料。

---

[目录](#)

## 配置并使用虚拟介质

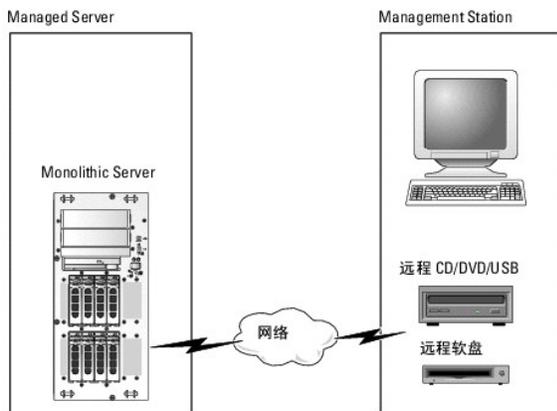
集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [概览](#)
- [配置虚拟介质](#)
- [运行虚拟介质](#)
- [常见问题](#)

### 概览

虚拟介质功能，可从控制台重定向查看器使用，提供了 managed server 对网络上远程系统所连介质的访问。图 10-1 显示了虚拟介质的整体结构。

图 10-1. 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 managed server，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 managed server 的操作系统和 BIOS 定义了两种设备：软盘设备和光盘设备。

Management Station 通过网络提供物理介质或映像文件。连接或自动连接虚拟介质后，来自 managed server 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。连接虚拟介质与将介质插入物理设备看起来一样。未连接虚拟介质时，虚拟设备不会显示在 managed server 上。

表 10-1 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 10-1. 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，请安装支持的带有 Java Runtime Environment (JRE) 的 Internet Explorer 或 Firefox。有关详细信息，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](http://java.sun.com) 下载 JRE。推荐 JRE 版本 1.6 或更高。

## 配置虚拟介质

1. 登录 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 10-2](#) 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 10-3](#)。

表 10-2. 虚拟介质配置属性

| 属性                                            | 值                                                                                                                                                |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 远程介质连接状态                                      | Attach - 立刻将“Virtual Media”（虚拟介质）附加到服务器。<br>Detach - 立刻从服务器上分离“Virtual Media”（虚拟介质）。<br>Auto-Attach - 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）                          | 显示“Virtual Media”（虚拟介质）会话所允许的最大数目，这个数目通常为 1。                                                                                                     |
| “Active Sessions”（激活的会话）                      | 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。选择启用加密，取消选择禁用加密。                                                                                    |
| “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 密钥驱动器。         |
| “Enable Boot Once”（启用引导一次）                    | 选中此复选框启用引导一次选项。服务器引导一次后，此选项将自动终止“Virtual Media”（虚拟介质）会话。此选项对于自动部署有用。                                                                             |

表 10-3. 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

 **小心：** 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. 向 `/ect/modprobe` 添加以下行：

```
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. 运行以下命令查看"Virtual CD/DVD" (虚拟 CD/DVD) 和/或"Virtual Floppy" (虚拟软盘):

```
cat /proc/scsi/scsi
```

 **注:** 使用虚拟介质, 仅能虚拟化一个软盘/USB 驱动器/映像/密钥, 且来自"Management Station" (管理站) 的光盘驱动器将作为受管服务器上的 (虚拟) 驱动器使用。

## 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。

支持软盘驱动器包括软盘映像或可用软盘驱动器。支持光盘驱动器包括最多 1 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 打开一个支持的 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)。

随即显示"Console Redirection" (控制台重定向) 和"Virtual Media" (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。可同时选择一个光盘驱动器和一个软盘/USB 闪存驱动器进行虚拟化。

 **注:** managed server 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网络管理员。

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 Agent 应用程序会以另外的窗口启动。

5. 单击"Tools" (工具) → "Launch Virtual Media" (连接虚拟介质)。

介质重定向向导会出现。

 **注:** 除非要终止虚拟介质会话, 否则请勿关闭本向导。

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" (连接虚拟介质)。
2. 取消选中想断开的介质旁边的框。

介质将会断开连接并且"Status" (状态) 将会更新。
3. 单击"Exit" (退出) 以终止介质重定向向导。

## 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 managed server。
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其它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。

managed server 重新引导。

managed server 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非交互方法，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：
  - 1 操作系统安装 CD 插入到 management station 的 CD 驱动器中。
  - 1 选择了本地 CD 驱动器。
  - 1 已与虚拟驱动器连接。
2. 按照[从虚拟介质引导](#)部分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. 取消从虚拟介质控制台到虚拟化（已重定向）CD/DVD 的映射。
2. 将下张 CD/DVD 插入远程光盘驱动器。
3. 从虚拟介质控制台映射（重定向）到此 CD/DVD。  
不重新映射就将新 CD/DVD 插入远程光盘驱动器可能不会起作用。

## 一次引导功能

一次引导功能可帮助将引导顺序临时更改为“从远程虚拟介质设备引导”。此功能与虚拟介质结合使用，通常用于安装操作系统。

 **注：** 必须有**配置 iDRAC6** 的权限才能使用此功能。

 **注：** 远程设备必须使用虚拟介质重定向才能使用此功能。

使用一次引导功能

1. 为服务器加电，并进入 BIOS Boot Manager。
2. 将引导顺序更改为“boot from the remote Virtual Media device”（从远程虚拟介质设备引导）。
3. 通过 Web 界面登录 iDRAC6 并单击 **"System"（系统）** → **"Console/Media"（控制台/介质）** → **"Configuration"（配置）**。
4. 选中虚拟介质下的**"Boot Once Enabled"（启用一次引导）选项**。
5. 对服务器执行关机后再开机操作。

随即服务器将从远程虚拟介质设备引导。下次服务器重新引导时，远程虚拟介质连接将断开。

## 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装入（如果已附加）并分配有驱动器号。

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装入。如果驱动器没有自动装入，则使用 Linux `mount` 命令手工装入驱动器。

## 常见问题

表 10-4 列出常见问题和解答。

表 10-4. 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间的链接。<br><br>如果虚拟介质配置设置在 iDRAC6 Web 界面或本地 RACADM 命令中更改，当配置更改应用后，任何所连介质都会断开连接。<br><br>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 <a href="#">支持的操作系统</a> 查看所支持操作系统的列表。                                                                                                                                                                                                                                                                                                                                                                                        |
| 哪些 Web 浏览器支持 iDRAC6？                                                                             | 请参阅 <a href="#">支持的 Web 浏览器</a> 查看所支持 Web 浏览器的列表。                                                                                                                                                                                                                                                                                                                                                                                |
| 为什么有时丢失客户端连接？                                                                                    | <ol style="list-style-type: none"><li>1 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，如果更改客户端系统的 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。</li><li>1 出现网络超时后，iDRAC6 固件会断开连接，断开服务器和虚拟驱动器间的链接。另外，有些人会在 Web 界面或输入 RACADM 命令变更虚拟介质配置设置。要重新连接虚拟驱动器，使用 <b>虚拟介质</b> 功能。</li></ol>                                                                                                |
| 通过虚拟介质安装 Windows 操作系统所用时间似乎太长了。为什么？                                                              | 如果使用 <i>Dell Systems Management Tools and Documentation</i> 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时延而需要很长时间访问 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 managed server 上，访问 BIOS 设置并导航到引导菜单。找到虚拟 CD、虚拟软盘或虚拟闪存更新并根据需要更改设备引导顺序。例如，要从 CD 驱动器引导，将 CD 驱动器配置为引导顺序中的第一个驱动器。                                                                                                                                                                                                                                                                                                                   |
| 我可以从何种介质引导？                                                                                      | iDRAC6 允许从以下可引导介质引导： <ol style="list-style-type: none"><li>1 CDROM/DVD 数据介质</li><li>1 ISO 9660 映像</li><li>1 1.44 软盘或软盘映像</li><li>1 被操作系统认作可移动磁盘的 USB 闪存盘</li><li>1 USB 闪存盘映像</li></ol>                                                                                                                                                                                                                                           |
| 如何使 USB 闪存盘可引导？                                                                                  | 搜索 <a href="http://support.dell.com">support.dell.com</a> 寻找 Dell 引导公用程序，这是一种可用来制作 Dell USB 引导盘的 Windows 程序。<br><br>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：<br><br><code>sys a: x: /s</code><br><br>其中 <code>x</code> 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： <ol style="list-style-type: none"><li>1. 打开 Linux 命令提示符并运行以下命令：<br/><br/><code>grep "Virtual Floppy" /var/log/messages</code></li><li>2. 找到该信息的最新条目并记下时间。</li><li>3. 在 Linux 提示符处运行以下命令：<br/><br/><code>grep "hh:mm:ss" /var/log/messages</code><br/>其中</li></ol><br><code>hh:mm:ss</code> 是 <code>grep</code> 在第一步返回消息的时间戳。 |

|                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                           | <p>4. 在步骤 3 中，查看 <code>grep</code> 命令的结果并找到赋予 Dell Virtual Floppy 的设备名。</p> <p>5. 确保已连接到虚拟软盘驱动器。</p> <p>6. 在 Linux 提示符处运行以下命令：</p> <pre>mount /dev/sdx /mnt/floppy</pre> <p>其中</p> <p><code>/dev/sdx</code> 是在第 4 步发现的设备名称</p> <p><code>/mnt/floppy</code> 是安装点。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p>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？</p> | <p>(继续回答)</p> <p>要安装虚拟软盘驱动器，找到 Linux 分配给虚拟 CD 驱动器的设备节点。按照以下步骤查找和安装虚拟 CD 设备：</p> <ol style="list-style-type: none"> <li>1. 打开 Linux 命令提示符并运行以下命令：</li> </ol> <pre>grep "Virtual Floppy" /var/log/messages</pre> <ol style="list-style-type: none"> <li>2. 找到该信息的最新条目并记下时间。</li> <li>3. 在 Linux 提示符处运行以下命令：</li> </ol> <pre>grep "hh:mm:ss" /var/log/messages</pre> <p>其中</p> <p>hh:mm:ss 是 <code>grep</code> 在步骤 1 返回消息的时间戳。</p> <ol style="list-style-type: none"> <li>4. 在步骤 3 中，查看 <code>grep</code> 命令的结果并找到赋予“Dell Virtual CD”的设备名。</li> <li>5. 确保已连接到虚拟 CD 驱动器。</li> <li>6. 在 Linux 提示符处运行以下命令：</li> </ol> <pre>mount /dev/sdx /mnt/floppy</pre> <p>其中</p> <p><code>/dev/sdx</code> 是在第 4 步发现的设备名称</p> <p><code>/mnt/floppy</code> 是安装点。</p> |
| <p>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？</p>                                                     | <p>固件更新造成 iDRAC6 重置，删除远程连接，并卸下虚拟驱动器。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>在我连接了 USB 设备之后，所有的 USB 设备都分离了，为什么？</p>                                                                 | <p>虚拟介质设备和虚拟闪存更新设备都是作为组合 USB 设备连接到 Host USB BUS（主机 USB 总线）的，且它们共享同一个 USB 端口。无论何时只要任意虚拟介质或虚拟闪存更新 USB 设备从主机 USB 总线连接或是断开，所有的虚拟介质和虚拟闪存更新设备都会短暂地从主机 USB 总线断开，然后他们会再次连接。如果主机操作系统正在使用虚拟介质设备，必须避免连接或断开一个或多个虚拟介质或虚拟闪存更新设备。建议在使用所需 USB 设备前线连接它们。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <p>USB 重置按钮有什么用？</p>                                                                                      | <p>它可重置连接到服务器的远程 USB 设备和本地 USB 设备。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## 使用 WS-MAN 界面

### 集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

#### ● [支持 CIM 配置文件](#)

使用 Web 服务管理 (WS-MAN) 协议, iDRAC6 固件提供网络访问管理。WS-MAN 是用于信息交换的传输机制。WS-MAN 为设备提供一种通用语言共享数据, 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组成部分, 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, 以进行身份验证会话。HTTPS 使用在 IP 端口 443 上的安全套接字层 (SSL), 确保通信安全。

WS-MAN 中可用的数据为 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) 提供的数据集。

用于转让 DMTF 基于 CIM 管理信息是 WS-MAN 最常见的用途。CIM 定义可于受管系统中操作的管理信息类型。其提供客户端和服务在线上讨论的对象。WS-MAN 指定可于管理对象上实施的某些标准操作。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, 并设置其内容至新值。WS-MAN 提供管理对话的动词、CIM 类和属性名词, 而对对象通过动词操作。

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标准最低词汇。这些 DMTF 和 Dell 指定配置文件定义一组对话, 其必须由所有符合标准的服务实施。因此, 所有客户端可根据这些对话正确地运行。

## 支持 CIM 配置文件

表 11-1. 支持 CIM 配置文件

| 标准 DMTF                                                                                                        |
|----------------------------------------------------------------------------------------------------------------|
| 1. 基础服务器<br>定义表示主机服务器的 CIM 类。                                                                                  |
| 2. 服务处理器:<br>包含表示 iDRAC6 的 CIM 类定义。                                                                            |
| <b>注:</b> 基础服务器配置文件 (上述者) 和服务处理器配置文件在传感中自治, 从而其说明的对象集合于组件配置文件所定义的所有其它 CIM 对象中。                                 |
| 3. 物理资产:<br>定义表示受管元素的物理方面的 CIM 类。iDRAC6 使用本配置文件表示主服务器和其组件的 FRU 信息以及物理拓扑。                                       |
| 4. SM CLP 管理区域<br>定义表示 CLP 配置的 CIM 类。iDRAC6 使用本配置文件, 进行其自身 CLP 实施。                                             |
| 5. 电源状态管理<br>定义电源控制操作的 CIM 类。iDRAC6 使用本配置文件进行主服务器的电源控制操作。                                                      |
| 6. 电源设备 (版本 1.1)<br>定义表示电源设备的 CIM 类。iDRAC6 使用本配置文件表示主服务器的电源设备, 以说明功耗 (如高低功耗水印)。                                |
| 7. CLP 服务<br>定义表示 CLP 配置的 CIM 类。iDRAC6 使用本配置文件, 进行其自身 CLP 实施。                                                  |
| 8. IP 界面<br>9. DHCP 客户端<br>10. DNS 客户端<br>11. 以太网端口<br>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<br>定义表示日志的不同类型的 CIM 类。iDRAC6 使用本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<br>定义已安装或可用软件资源清册的 CIM 类。通过 TFTP 协议, iDRAC6 使用本配置文件作为当前安装 iDRAC6 固件版本的资源清册。                         |
| 14. 基于角色授权<br>定义表示角色的 CIM 类。iDRAC6 使用本配置文件配置 iDRAC6 帐户权限。                                                      |
| 15. 软件更新<br>定义可用软件更新资源清册的 CIM 类。通过 TFTP 协议, iDRAC6 使用本配置文件作为固件更新的资源清册。                                         |

|                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------|
| 16. SMASH 集合<br>定义表示 CLP 配置的 CIM 类。iDRAC6 使用本配置文件，进行其自身 CLP 实施。                                                    |
| 17. 配置文件注册<br>定义通告配置文件实施的 CIM 类。按本表所述，iDRAC6 使用本配置文件作为通告其自身已实施的配置文件。                                               |
| 18. 基础度量<br>定义表示度量的 CIM 类。iDRAC6 将本配置文件用于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<br>定义表示标识的 CIM 类。iDRAC6 使用本配置文件配置 iDRAC6 帐户。                                                            |
| 20. USB 重定向<br>定义表示本地 USB 端口远程重定向的 CIM 类。iDRAC6 将本配置文件与虚拟介质配置文件配合使用，以配置虚拟介质。                                       |
| Dell ©'                                                                                                            |
| 1. Dell™ Active Directory 客户端版本 2.0.0<br>定义配置 iDRAC6 Active Directory 客户和本地 Active Directory 组权限的 CIM 类和 Dell 扩展类。 |
| 2. Dell 虚拟介质<br>定义配置 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<br>定义为 iDRAC6 NIC 配置的 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<br>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/](http://www.dmtf.org/standards/profiles/)。有关本列表配置文件或信息的更新，请参阅 WS-MAN 版本注释或自述文件。

WS-MAN 的实施符合 DMTF WS-MAN 指定版本 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)、打开 wsman 和 wsmancli 工具。

---

[目录](#)

[目录](#)

## 使用 iDRAC6 SM-CLP 命令行界面

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [iDRAC6 SM-CLP 支持](#)
- [SM-CLP 功能](#)

本节提供了有关 iDRAC6 中纳入的分布式管理任务小组 (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](http://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，可跨平台优化服务器管理。SM-CLP 规范与受管元素寻址规范和多个 SM-CLP 映射规范配置文件结合使用，可描述各种管理任务执行的标准化 verb 和目标。

---

## iDRAC6 SM-CLP 支持

SM-CLP 由 DRAC6 控制器固件承载，并且支持远程登录、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"中说明的各种配置文件。

以下部分提供了 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，您可以使用 [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    | 将二进制图像由一个 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 | 描述 |
|----|----|
|----|----|

| 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                                             | 受管系统目标              |
| admin1/system1/redundancysct1                              | 电源设备                |
| admin1/system1/redundancysct1/pwrsupply*                   | 受管系统电源设备            |
| admin1/system1/sensors1                                    | 受管系统传感器             |
| admin1/system1/capabilities1                               | 受管系统 SMASH 收集功能     |
| admin1/system1/capabilities1/pwrcap1                       | 受管系统电源利用功能          |
| admin1/system1/capabilities1/elec1                         | 受管系统目标功能            |
| admin1/system1/logs1                                       | 记录日志收集目标            |
| admin1/system1/logs1/log1                                  | 系统事件日志 (SEL) 记录条目   |
| admin1/system1/logs1/log1/<br>记录*                          | 受管系统上的单独 SEL 记录实例   |
| admin1/system1/settings1                                   | 受管系统 SMASH 收集设置     |
| admin1/system1/settings1/pwrmaxsetting1                    | 受管系统最大电源分配设置        |
| admin1/system1/settings1/pwrminsetting1                    | 受管系统最小电源分配设置        |
| admin1/system1/capacities1                                 | 受管系统容量 SMASH 收集     |
| admin1/system1/console1Internet Explorer                   | 受管系统控制台 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/dhccap1                   | 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/capabilities1/PwrutilmgtCap1            | 电源利用管理功能            |
| admin1/system1/sp1/capabilities1/metriccap1                | 跃点服务功能              |
| admin1/system1/sp1/capabilities1/elec1                     | 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/clpendpt*                       | CLP 服务协议端点          |
| admin1/system1/sp1/clpsvc1/tcpendpt*                       | CLP 服务协议 TCP 端点     |
| admin1/system1/sp1/jobq1                                   | CLP 服务协议作业队列        |
| admin1/system1/sp1/jobq1/job*                              | CLP 服务协议作业          |
| admin1/system1/sp1/pwrmtgsvc1                              | 电源状态管理服务            |
| admin1/system1/sp1/pcfgsvc1                                | IP 接口配置服务           |

|                                                        |                       |
|--------------------------------------------------------|-----------------------|
| admin1/system1/sp1/pendpt1                             | IP 接口协议端点             |
| admin1/system1/sp1/pendpt1/gateway1                    | IP 接口网关               |
| admin1/system1/sp1/pendpt1/dhcpndpt1                   | DHCP 客户端协议端点          |
| admin1/system1/sp1/pendpt1/dnsndpt1                    | DNS 客户端协议端点           |
| admin1/system1/sp1/pendpt1/dnsndpt1/dnsserver*         | DNS 客户端服务器            |
| admin1/system1/sp1/NetPortCfgsvc1                      | 网络端口配置服务              |
| admin1/system1/sp1/lanndpt1                            | LAN 端点                |
| admin1/system1/sp1/lanndpt1/enetport1                  | 以太网端口                 |
| admin1/system1/sp1/VMediaSvc1                          | 虚拟介质服务                |
| admin1/system1/sp1/VMediaSvc1/tcpndpt1                 | 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](#)

## 使用 VMCLI 部署 操作系统

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [准备工作](#)
- [创建可引导映像文件](#)
- [准备部署](#)
- [部署操作系统](#)
- [使用 VMCLI 公用程序](#)

虚拟介质命令行界面 (VMCLI) 公用程序是一个命令行界面，从管理站向远程系统中的 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部分所列的要求。

### 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：

- 1 操作系统文件
- 1 需要的驱动程序
- 1 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。

以下部分提供了有关为 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，应执行以下规则：

- 1 遵循标准基于网络的安装步骤
  - 1 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步骤
- 1 执行以下某一程序：
- 1 将 IPMI tool 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。
  - 1 使用现有 **vm6deploy** 脚本部署操作系统。

---

## 部署操作系统

使用 VMCLI 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。

以下步骤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-user> -p <idrac-passwd> -c {<iso9660-img> | <path>} -f {<floppy-img>|<path>}
```

其中

- 1 <idrac-用户> 是 iDRAC6 用户名，例如 **root**
- 1 <idrac-密码> 是 iDRAC6 用户的密码，例如 **calvin**
- 1 <iso9660-映像>是操作系统安装 CD 或 DVD 的 ISO9660 映像路径
- 1 <路径>是包含操作系统安装 CD、DVD 或软盘的设备路径
- 1 <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，从管理站向 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，一个会话一次只能访问一个给定物理驱动器。

- 1 与虚拟介质插件一致的可移动介质设备或映像文件
- 1 启用 iDRAC6 固件引导一次选项后自动终结。
- 1 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来运行 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 软件包提供。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指示操作。

*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。本 DVD 还包含自述文件，提供最新 systems management software 产品信息。

*Dell Systems Management Tools and Documentation DVD* 包含 `vm6deploy`—演示如何使用 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，则除安装其它文件外，还须安装该公用程序。

## 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：

- 1 VMCLI 连接因任何原因终止。
- 1 使用操作系统控制手动终止过程。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，将显示错误信息并终止命令。

`<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-名称>`

此参数提供将运行虚拟介质的 iDRAC6 用户名。

`<iDRAC-用户-名称>` 必须具有以下属性：

- 1 有效用户名
- 1 iDRAC6 虚拟介质用户权限

如果 iDRAC6 验证失败，错误信息将会显示并且命令会终止。

### iDRAC6 用户密码

`-p <iDRAC-用户-密码>`

此参数提供指定 iDRAC6 用户的密码。

如果 iDRAC6 验证失败，错误信息将会显示并且命令会终止。

## 软盘/磁盘设备或映像文件

-f {<设备名称> | <映像文件>}

其中 <设备-名称> 是有效驱动器号 (对于 Windows 系统) 或有效设备文件名 (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：  
选项 `scsi_mod max_luns=8`  
(您可指定 8 个或任意数量 (大于 1) 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，确认多个 LUN 支持已添加步骤 1 中所指定的 LUN 个数：

```
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，错误信息将会显示并且命令会终止。

## 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，错误信息将会列出并且命令会终止。

用此命令指定至少一个介质类型（软盘或 CD/DVD 驱动器），除非只提供了开关选项。否则，错误信息将会显示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，此命令将会无错终止。

## 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，此命令将会无错终止。

## 加密的数据

-e

如果命令行中包括此参数，VMCLI 公用程序将使用 SSL 加密的信道在 管理站和远程系统中的 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：** 使用此选项不会将显示的虚拟介质加密状态更改为已启用 RACADM 或 Web 界面等其它 iDRAC6 配置界面。

## VMCLI 操作系统 Shell 选项

VMCLI 命令 行中可使用以下操作系统功能：

- 1 stderr/stdout redirection — 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。

- 1 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外壳功能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，必须手动终止一个或多个命令实例，使用操作系统特定的功能来列出并终止进程。

## VMCLI 返回代码

当遇到错误时，文本信息（仅有英文）会发送到标准错误输出。

---

[目录](#)

[目录](#)

## 配置智能平台管理接口 (IPMI)

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [配置 IPMI](#)
- [配置 LAN 上串行使用基于 Web 的界面](#)

---

### 配置 IPMI

本部分提供有关配置和使用 iDRAC6 IPMI 接口的信息。接口包括以下：

- 1 LAN 上 IPMI
- 1 串行 IPMI
- 1 LAN 上串行

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

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

有关使用 IPMI Shell, *ipmish* 的更多详细信息，请参阅《Dell OpenManage 基板管理控制器公用程序用户指南》，网址为 [support.dell.com/manuals](http://support.dell.com/manuals)。

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。

在命令提示符处，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。

在命令提示符处，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmlan -o cfgIpmlenEncryptionKey <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)。

在命令提示符处，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmlsol -o cfgIpmlsolEnable 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。

在命令提示符处，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmlsol -o cfgIpmlsolMinPrivilege <级别>
```

其中<级别> 是以下某个值：

- o 2 (用户)
- o 3 (操作员)
- o 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 cfgIpmlsol -o cfgIpmlsolMinPrivilege 2
```

#### b. 更新 IPMI SOL 波特率。

 **注：** 要重新定向 LAN 上串行控制台，应确保 SOL 波特率与 managed system 的波特率相同。

在命令提示符处，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmlsol -o cfgIpmlsolBaudRate <波特率>
```

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

例如：

```
racadm config -g cfgIpmlsol -o cfgIpmlsolBaudRate 57600
```

#### c. 为单个用户启用 SOL。

 **注：** SOL 可以为每个用户启用或禁用。

在命令提示符处，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. 更改 IPMI 串行连接模式为相应的设置。

在命令提示符处，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 cfgIpmlserial -o cfgIpmlserialBaudRate <波特率>
```

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

例如：

```
racadm config -g cfgIpmlserial -o cfgIpmlserialBaudRate 57600
```

#### c. 启用 IPMI 串行硬件流控制。

在命令提示符处，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。

在命令提示符处，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:

- o 2 (用户)
- o 3 (操作员)
- o 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. 确保串行 MUX 在 BIOS 设置程序中正确设置。

- o 重新启动系统。
- o 在开机自检期间，按 <F2> 进入 BIOS 设置程序。
- o 导航到“Serial Communication” (串行通信)。
- o 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)。
- o 保存并退出 BIOS 设置程序。
- o 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:

- o 删除控制
- o 回声控制
- o 行编辑
- o 新行序列
- o 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:

- 1 “IPMI terminal mode” (IPMI 终端模式) — 支持从串行终端提交的 ASCII 命令。命令集仅限于有限的命令 (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。
- 1 “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《Dell OpenManage 基板管理控制器公用程序用户指南》，网址为 [support.dell.com/manuals](http://support.dell.com/manuals)。

---

[目录](#)

[目录](#)

## 使用 iDRAC 配置公用程序

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [概览](#)
- [启动 iDRAC 配置公用程序](#)
- [使用 iDRAC 配置公用程序](#)

---

### 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 和管理型服务器的参数。具体说来，可以：

- 1 查看 iDRAC6 和主背板固件的固件版本号
- 1 启用或禁用 iDRAC6 局域网
- 1 启用或禁用 LAN 上 IPMI
- 1 配置 LAN 参数
- 1 配置虚拟介质
- 1 配置智能卡
- 1 更改管理用户名和密码
- 1 重设 iDRAC 配置为工厂默认值
- 1 查看系统事件日志 (SEL) 信息或从日志清除信息
- 1 配置 LCD
- 1 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™ 软件提供的其他公用程序执行，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。

iDRAC 配置公用程序显示。前两行提供了有关 iDRAC6 固件和主背板固件修订的信息。在确定是否需要固件升级时，修订级别很有用。

iDRAC6 固件是固件中与外界界面（比如基于 Web 的界面、SM-CLP 和 Web 界面）相关的部分。主背板固件是监测并交互服务器硬件环境的部分。

---

### 使用 iDRAC 配置公用程序

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

- 1 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。
- 1 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。
- 1 如果项目不可编辑，会显示为蓝色。有些项目会根据您所做的其它选择而变得可编辑。
- 1 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。
- 1 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，方可使用 iDRAC6 功能，比如基于 Web 的界面、远程登录/SSH 和对 SM-CLP 命令行界面的 RAC 串行访问、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。)

该消息告诉您，在禁用 LAN 时，除了通过直接连接 iDRAC HTTP、HTTPS、远程登录或 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，可用于重新配置 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。)

Press any key to clear the message and continue. (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 15-1. LAN 参数

| 项目                                    | 说明                                                                                                                                                                                                                                                               |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一般设置                                  |                                                                                                                                                                                                                                                                  |
| NIC 选择                                | 按 <右箭头>、<左箭头> 和空格键，在模式之间切换。<br><br>可用模式包括 <b>专用</b> 、 <b>共享</b> 、 <b>与故障转移 LOM2 共享</b> 以及 <b>与故障转移所有 LOM 共享</b> 。<br><br>这些模式允许 iDRAC6 使用对应接口与外界通信。                                                                                                              |
| 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 iDRAC 名称)  | 选择 "On" (开) 在 DNS 服务中注册 iDRAC6 名称。如果不想让用户在 DNS 中查找 iDRAC6 名称，则选择 "Off" (关)。                                                                                                                                                                                      |
| "iDRAC6 Name" (iDRAC 名称)              | 如果 "Register iDRAC6 Name" (注册 iDRAC 名称) 设置为 On (开)，按 <Enter> 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" (来自 DHCP 的域名) | 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" (来自 DHCP 的域名) 设置为 "Off" (关)，则按 <Enter> 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> 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)，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)，激活第一个警报目的地。                                                                                                                                                                                                                    |
| "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 警报的 IP 地址。                                                                                                                                                                                         |
| IPv4 设置                               | 启用或禁用对 IPv4 连接的支持。                                                                                                                                                                                                                                               |
| IPv4                                  | 选择 "Enabled" (已启用) 或 "Disabled" (已禁用) IPv4 协议支持。                                                                                                                                                                                                                 |
| "RMCP+ Encryption Key" (RMCP+ 密钥)     | 按 <Enter> 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。默认值为包含 40 个 0 (零) 的字符串。                                                                                                                                 |
| IP 地址源                                | 选择 DHCP 或 "Static" (静态)。如果选中 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。<br><br>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。<br>如果"IP Address Source" (IP 地址源) 设置为"Static" (静态), 则输入想为 iDRAC6 分配的 IP 地址。<br>默认值为 192.168.0.120。                                                                                                      |
| 子网掩码                                        | 如果"IP Address Source" (IP 地址源) 设置为 DHCP, 此字段将会显示从 DHCP 获得的子网掩码。<br>如果"IP Address Source" (IP 地址源) 设置为"Static" (静态), 则输入 iDRAC6 的子网掩码。默认为 255.255.255.0。                                                                                                                   |
| 默认网关                                        | 如果"IP Address Source" (IP 地址源) 设置为 DHCP, 此字段将会显示从 DHCP 获得的默认网关 IP 地址。<br>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。默认为 192.168.0.1。                                                                                                                 |
| "DNS Servers from DHCP" (来自 DHCP 的 DNS 服务器) | 选择 On (开) 从网络上的 DHCP 服务检索 DNS 服务器地址。选择 Off (关) 指定以下 DNS 服务器地址。                                                                                                                                                                                                            |
| "DNS Server 1" (DNS 服务器 1)                  | 如果"DNS Servers from DHCP" (来自 DHCP 的 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" (来自 DHCP 的 DNS 服务器) 为 Off (关), 则输入第二个 DNS 服务器的 IP 地址。                                                                                                                                                                                           |
| IPv6 设置                                     | 启用或禁用对 IPv6 连接的支持。                                                                                                                                                                                                                                                        |
| IP 地址源                                      | 选择"AutoConfig" (自动配置) 或"Static" (静态)。当选择"AutoConfig" (自动配置) 后, 会从 DHCP 获取"IPv6 Address 1" (IPv6 地址 1)、"Prefix Length" (前缀长度) 和"Default Gateway" (默认网关) 字段。<br>当选择"Static" (静态) 后, "IPv6 Address 1" (IPv6 地址 1)、"Prefix Length" (前缀长度) 和"Default Gateway" (默认网关) 都会变成可编辑项。 |
| IPv6 地址 1                                   | 如果"IP Address Source" (IP 地址源) 设置为"AutoConfig" (自动配置), 此字段将会显示从 DHCP 获得的 IP 地址。<br>如果"IP Address Source" (IP 地址源) 设置为"Static" (静态), 则输入想为 iDRAC6 分配的 IP 地址。                                                                                                               |
| 前缀长度                                        | 配置 IPv6 地址的前缀长度。可以是 1 到 128 之间 (含) 的值。                                                                                                                                                                                                                                    |
| 默认网关                                        | 如果"IP Address Source" (IP 地址源) 设置为"AutoConfig" (自动配置), 此字段将会显示从 DHCP 获得的默认网关的 IP 地址。<br>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 链接本地地址                                 | 这是 iDRAC 网络接口的不可编辑的 IPv6 链接本地地址。                                                                                                                                                                                                                                          |
| 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" (来自 DHCP 的 DNS 服务器) | 选择 On (开) 从网络上的 DHCP 服务检索 DNS 服务器地址。选择 Off (关) 指定以下 DNS 服务器地址。                                                                                                                                                                                                            |
| "DNS Server 1" (DNS 服务器 1)                  | 如果"DNS Servers from DHCP" (来自 DHCP 的 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" (来自 DHCP 的 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)。<br>当选择"Enabled" (已启用) 后, 会自动配置"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)。                                                                                                                                                                                |

## "Virtual Media Configuration" (虚拟介质配置)

### 虚拟介质

按 <Enter>, 选择"Detached" (分离)、"Attached" (附加) 或"Auto-Attached" (自动附加)。如果选择"Attached" (附加), 虚拟介质设备会附加到 USB 总线, 从而可以在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 闪存盘, 在 BIOS 设置公用程序中"USB Flash Drive Emulation Type" (USB 闪存盘仿真类型) 必须设置为"Hard disk" (硬盘)。在服务器启动期间按 <F2> 可访问 BIOS 设置公用程序。如果"USB Flash Drive Emulation Type" (USB 闪存盘仿真类型) 设置为"Auto" (自动), 闪存盘将显示为系统软盘驱动器。

### "Virtual Flash" (虚拟闪存更新)

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) 将导致虚拟闪存被删除, 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 登录

按 <Enter>，选择“Enabled”（已启用）或“Disabled”（已禁用）。该选项配置智能卡登录功能。可用选项有“Enabled”（已启用）、“Disabled”（已禁用）和“Enabled with RACADM”（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）。有关更多信息，请参阅《Dell Unified Server Configurator 用户指南》（在 Dell 支持网站 support.dell.com/manuals 上提供）。

 **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 15-2. LCD 用户配置

|                                            |                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LCD 行 1                                    | 按 <右箭头>、<左箭头> 和空格键，在选项之间切换。<br><br>该功能将 LCD 上的主显示设置为以下选项之一：<br><br>"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 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。<br><br>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 上的功率显示单位。                                                                                                                                                                                                                                                           |
| "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 上的温度显示单位。                                                                                                                                                                                                                                               |
| "LCD Error Display"（LCD 错误显示）              | 选择“Simple”（简单）或 SEL（系统事件日志）。<br><br>该功能允许采用以下两种格式之一，在 LCD 上显示错误信息：<br><br>"Simple"（简单）格式用英语提供事件说明。<br><br>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。<br><br>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 15-3. LAN 用户配置

|  |  |
|--|--|
|  |  |
|--|--|

| 项目                          | 说明                                                                         |
|-----------------------------|----------------------------------------------------------------------------|
| "Account Access" (帐户访问)     | 选择"Enabled" (启用) 启用管理员帐户。选择"Disabled" (禁用) 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, 将会显示消息, 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, 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。以下警告信息会出现:

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

< NO (Cancel) >  
(< 否 (取消) >)

< YES (Continue) >  
(< 是 (继续) >)

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 保持最多 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> 移动到上一条 (较旧) 信息, <右箭头> 移动到下一条 (较新) 信息。输入记录号跳到该记录。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> 以保留更改。

选择"Discard Changes and Exit" (放弃更改并退出) 并按 <Enter> 以忽略所作更改。

选择"Return to Setup" (返回设置) 并按 <Enter> 以返回 iDRAC 配置公用程序。

---

[目录](#)

[目录](#)

## 监控和警报管理

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [配置 Managed System 以获取上次崩溃屏幕](#)
- [禁用 Windows 自动重新引导选项](#)
- [配置平台事件](#)
- [常见问题](#)

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，必须将受控系统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“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，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”（重置）、“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，如果受控系统崩溃，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，请在受控系统上禁用“Automatic Reboot”（自动重新引导）选项（受控系统运行的是 Microsoft Windows Server® 2008 和 Windows Server 2003 操作系统）。

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

1. 打开 Windows“控制面板”并双击“系统”图标。
2. 在左侧单击“Advanced System Setting”（高级系统设置）（在“Tasks”（任务）下）。
3. 单击“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“控制面板”并双击“系统”图标。
2. 单击“高级”选项卡。

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

---

## 配置平台事件

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

可筛选的平台事件包括以下：

- 1 风扇危急声明筛选器
- 1 电池警告声明筛选器
- 1 电池危急声明筛选器
- 1 不连续电压危急声明筛选器
- 1 温度警告声明筛选器
- 1 温度危急声明筛选器
- 1 入侵危急声明筛选器
- 1 冗余降级筛选器
- 1 冗余丧失筛选器
- 1 处理器警告声明筛选器
- 1 处理器危急声明筛选器
- 1 处理器缺失筛选器
- 1 处理器电源警告声明筛选器
- 1 处理器电源危急声明筛选器
- 1 处理器电源缺失声明筛选器
- 1 事件日志危急声明筛选器
- 1 监控软件危急声明筛选器
- 1 系统电源警告声明筛选器
- 1 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），则将执行操作。

## 配置平台事件筛选器（PEF）

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。

### 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。

在命令提示符处，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：

- 1 0 = 无警报操作
- 1 1 = 关闭服务器
- 1 2 = 重新引导服务器
- 1 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> 键：

```
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。

在命令提示符处，键入以下命令并按 <Enter>：

```
IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IPv4_address>
```

```
IPv6:racadm config -g cfgIpmiPetIPv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6_address>
```

其中，1 表示 PET 目的地索引，<IPv4\_address> 和 <IPv6\_address> 表示接收平台事件警报的系统的 IP 地址目的地。

#### 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 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。

在命令提示符处，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。

要配置自定义消息，在命令提示符处，键入以下命令并按 <Enter>：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <自定义消息>
```

其中，1 表示电子邮件目的地的索引，<custom\_message> 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。下面的示例演示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。

下面的示例演示用户如何测试 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 SNMP 和陷阱设置。请参阅 [testtrap](#) 和 [sslkeyupload](#) 子命令说明来配置这些设置。

---

## 常见问题

**为什么显示以下消息：**

**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 cfgOobSnmpp
```

要设置 iDRAC6 团体名称，请使用以下命令：

```
racadm config -g cfgOobSnmpp -o cfgOobSnmppAgentCommunity <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，必须输入会被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

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [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](#)
- [查看系统信息](#)
- [使用系统事件日志 \(SEL\)](#)
- [使用 POST 引导日志](#)
- [查看上次系统崩溃屏幕](#)

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。

- 1 ["排除远程系统故障时首先需要执行的步骤"](#)
- 1 ["管理远程系统上的电源"](#)
- 1 ["IPv6 信息"](#)
- 1 ["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 允许在受控系统上远程执行几种电源管理操作，以便在出现系统崩溃或其他系统事件后进行恢复。

" iDRAC6 " Web ...` ` ÷

要使用基于 Web 的界面执行电源控制操作，请参阅["执行服务器电源控制操作"](#)。

" iDRAC6 CLI ...` ` ÷

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：

- 1 **powerdown** — 关闭 Managed System 电源。
- 1 **powerup** — 打开 Managed System 电源。
- 1 **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后再打开系统电源。
- 1 **powerstatus** — 显示服务器的当前电源状态 ("ON"或 "OFF")
- 1 **hardreset** — 在 Managed System 上执行重设（重新引导）操作。

---

### 查看系统信息

**系统摘要**页显示关于以下系统组件的信息：

- 1 Main System Chassis (主系统机箱)
- 1 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 17-1 和 表 17-2 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，受控系统上必须安装有 iDRAC6 服务。

表 17-1. 系统信息字段

| 字段                  | 说明          |
|---------------------|-------------|
| 说明                  | 系统说明。       |
| BIOS 版本             | 系统 BIOS 版本。 |
| "Service Tag"（服务标签） | 系统服务标签号码。   |
| 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 17-2. 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：无操作、硬重设、关机或关机后再开机。 |
| "Initial Countdown"（初始倒计时） | 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"（当前倒计时） | 倒计时计时器的当前值，以秒为单位。                                     |

## Integrated Dell Remote Access Controller 6 Enterprise

表 17-3 说明 iDRAC6 Enterprise 属性。

表 17-3. iDRAC6 Enterprise 信息字段

| 字段                       | 说明                                          |
|--------------------------|---------------------------------------------|
| 日期/时间                    | 采用以下格式表示的当前时间：<br>日 月 DD HH:MM:SS:YYYY      |
| 固件版本                     | iDRAC 固件版本。                                 |
| "Firmware Updated"（固件更新） | 上次对固件执行闪存日期，采用以下格式：<br>日 月 DD HH:MM:SS:YYYY |
| "Hardware Version"（硬件版本） | Remote Access Controller 版本。                |
| 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 17-4 说明 IPv4 属性。

表 17-4. IPv4 信息字段

| 字段                         | 说明                                                      |
|----------------------------|---------------------------------------------------------|
| 已启用                        | "Yes"（是）或"No"（否）                                        |
| IP 地址                      | 标识主机的网络接口卡 (NIC) 的 32 位地址。该值采用点分隔格式，比如 143.166.154.127。 |
| 子网掩码                       | 子网掩码标识 IP 地址的组成部分；扩展网络前缀和主机号。该值采用点分隔格式，比如 255.255.0.0。  |
| 网关                         | 路由器或交换机的地址。该值采用点分隔格式，比如 143.166.154.1。                  |
| "DHCP Enabled"（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 17-5 说明 IPv6 属性。

表 17-5. IPv6 信息字段

| 字段                     | 说明                                                                                                                                                                                        |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 已启用                    | 指示是否启用了 IPv6 堆栈。                                                                                                                                                                          |
| IP Address 1 (IP 地址 1) | 为 iDRAC NIC 指定 IPv6 地址。                                                                                                                                                                   |
| 前缀长度                   | 指定 IPv6 地址前缀长度的整数。可以是 1 到 128 (含) 的值。                                                                                                                                                     |
| IP 网关                  | 指定 iDRAC NIC 的网关。                                                                                                                                                                         |
| 链接本地地址                 | 为 iDRAC NIC 指定 IPv6 地址。                                                                                                                                                                   |
| IP Address 2 (IP 地址 2) | 为 iDRAC NIC 指定其他 IPv6 地址 (若有)。                                                                                                                                                            |
| Auto Config (自动配置)     | "AutoConfig" (自动配置) 可从 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 页显示受控系统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)。

系统事件日志页显示事件严重性并提供其他信息, 如表 17-6 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 17-6)。

表 17-6. 状况指示器图标

| 图标/类别                                                                               | 说明                                                                   |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------|
|  | 绿色复选标记表示健康 (正常) 状况。                                                  |
|  | 黄色带有感叹号的三角表示警告 (不严重) 状况。                                             |
|  | 红色 X 表示严重 (故障) 状况。                                                   |
|  | 问号图标指示状态未知。                                                          |
| 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 17-7. 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" (清除日志) | 清除 SEL。<br><br><b>注:</b> "Clear Log" (清除日志) 按钮仅当具有 "Clear Logs" (清除日志) 权限时显示。                                                                                    |
| "Save As" (另存为)    | 打开一个弹出窗口, 使您能够将 SEL 保存到所选的目录。<br><br><b>注:</b> 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 日志中的条目数。

```
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。

`clrssel` 命令会从系统事件日志 (SEL) 删除全部现有的记录。

```
racadm clrssel
```

---

## 使用 POST 引导日志

 **注：** 重新引导 iDRAC6 后，所有日志都会被清除掉。

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

要查看 POST 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 POST 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 POST 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 POST 引导捕获日志视频。
  5. 单击 "STOP" (停止) 停止视频。
- 

## 查看上次系统崩溃屏幕

 **注：** 上次崩溃屏幕功能要求受控系统在 Server Administrator 中配置 "Auto Recovery" (自动恢复) 功能。此外，确保使用 DRAC 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。

**上次崩溃屏幕** 页显示最近的崩溃屏幕，包含系统崩溃前发生的事件的信息。上次系统崩溃信息保存在 iDRAC6 内存中，并且可以远程访问。

要查看 **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。

**上次崩溃屏幕** 页提供屏幕右上角的以下按钮 (参阅 [表 17-8](#))：

表 17-8. 上次崩溃屏幕页按钮

| 按钮             | 操作           |
|----------------|--------------|
| "Print" (打印)   | 打印上次崩溃屏幕页。   |
| "Refresh" (刷新) | 重新载入上次崩溃屏幕页。 |

 **注：** 由于自动恢复计时器的波动，当系统重置计时器设置为小于 30 秒时 **上次崩溃屏幕** 可能无法捕获。使用 Server Administrator 或 IT Assistant 将系统重置计时器设置为至少 30 秒，并确保 **上次崩溃屏幕** 运行正常。有关其他信息，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

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [使用 RAC 日志](#)
- [使用命令行](#)
- [使用诊断控制台](#)
- [使用跟踪日志](#)
- [使用 racdump](#)
- [使用 coredump](#)

本节介绍如何对崩溃的 iDRAC6 进行恢复和故障排除。

可以使用以下某一工具来排除 iDRAC6 的故障：

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

---

## 使用 RAC 日志

**RAC 日志** 是 iDRAC6 固件中的一个持续日志。日志中的列表记录了用户操作（比如登录、注销和安全策略更改）以及由 iDRAC6 发出的警报。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：

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 18-1](#) 中所列信息。

**表 18-1. RAC 日志页信息**

| 字段    | 说明                                                                     |
|-------|------------------------------------------------------------------------|
| 日期/时间 | 日期和时间（例如 Dec 19 16:55:47）。<br>当 iDRAC6 刚开始启动并且无法与受管系统通信时，该时间将会显示为系统引导。 |
| 来源    | 引起事件的接口。                                                               |
| 说明    | iDRAC6 中记录的事件和用户名的简要说明。                                                |

## 使用 RAC 日志页按钮

RAC 日志页提供 [表 18-2](#) 中所列的按钮。

**表 18-2. 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。<br><b>注：</b> 只有您具有 "Clear Logs" (清除日志) 权限时，才会显示 "Clear Log" (清除日志) 按钮。                                                  |
| "Save As" (另存为)    | 打开一个弹出窗口，使您能够将 "RAC Log" (RAC 日志) 保存到所选的目录。<br><b>注：</b> 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) | 重新加载"RAC Log" (RAC 日志) 页。 |

## 使用命令行

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 18-3](#)），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**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 18-3](#) 说明**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**诊断控制台**页中。

要刷新**诊断控制台**页，请单击“Refresh”（刷新）。要执行其他命令，请单击“Go Back to Diagnostics Page”（返回到诊断页）。

**表 18-3. 诊断命令**

| 命令                              | 说明                                                                                                                   |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>arp</code>                | 显示地址解析协议 (ARP) 表的内容。ARP 条目不能添加或删除。                                                                                   |
| <code>ifconfig</code>           | 显示网络接口表的内容。                                                                                                          |
| <code>netstat</code>            | 打印路由选择表的内容。如果在 <code>netstat</code> 选项右边的文本字段中提供可选接口号， <code>netstat</code> 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。 |
| <code>ping &lt;IP 地址&gt;</code> | 验证目标 IP 地址是否可以使用当前路由表内容从 iDRAC6 进行访问。必须在该选项右侧的字段中输入目标 IP 地址。根据当前的路由选择表内容，将 Internet 控制报文协议 (ICMP) 回音数据包发送到目标 IP 地址。  |
| <code>gettracelog</code>        | 显示 iDRAC6 跟踪日志。有关详情，请参阅“ <a href="#">gettracelog</a> ”。                                                              |

## 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` 命令输入**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：

1. DHCP @C 跟踪发送到 DHCP 服务器和从 DHCP 服务器接收的信息包。

- 1 IP @C 跟踪发送和接收的 IP 信息包。

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，而不是受管系统的操作系统。

 **注：** iDRAC6 不会回送信息包大小超过 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 卡的一般信息。

 **注：** 此命令只能在 Telnet 和 SSH 接口上使用。有关详细信息，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：

- 1 使用 `coredumpdelete` 子命令清除 coredump 信息。
- 1 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。

请参阅 "[coredump](#)" 和 "[coredumpdelete](#)" 子命令查看更多信息。

---

[目录](#)

[目录](#)

## 传感器

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [电池探测器](#)
- [风扇探测器](#)
- [机箱入侵探测器](#)
- [电源设备探测器](#)
- [电源监测探测器](#)
- [温度探测器](#)
- [电压探测器](#)

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

可以使用 iDRAC6 监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 motherboard 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：

- 1 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。
- 1 风扇探测器列表 — 提供系统所有风扇的速度信息。

---

### 机箱入侵探测器

机箱入侵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：

- 1 电源设备状态
- 1 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。

 **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。

还可以查看距 iDRAC6 当前时间一小时、一天或一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严重阈值内。

---

### 电压探测器

以下是典型的电压探测器。系统可能有这些和/或其他。

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

电压探测器表示探测器状态是否在预置警告和严重阈值内。

---

[目录](#)

[目录](#)

## iDRAC6 使用入门

### 集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 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 身份验证等。

管理站是指管理员远程管理配有 iDRAC6 的 Dell 系统的系统。在这种方式下被监测的系统叫做受管系统。

或者，您可以在管理站和受管系统上安装 Dell™ OpenManage™ 软件。没有受管系统软件，将不能在本地使用 RACADM，并且 iDRAC6 无法捕获上次崩溃的屏幕。

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](http://support.dell.com/manuals) 上特定系统的**硬件用户手册**详细了解如何执行此步骤。

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，能够使您超越 Active Directory 软件的现有用户对 iDRAC6 进行添加和控制。
3. 配置 Smart Card 身份验证 — 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。
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](#)

## 电源监控和管理

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [电源资源清册、电源预算和封顶](#)
- [电源监控](#)
- [配置和管理电源](#)
- [查看电源设备的运行状态。](#)
- [查看电源预算](#)
- [电源预算阈值](#)
- [查看电源监控](#)
- [执行服务器电源控制操作](#)

Dell™ PowerEdge™ 系统整合了众多全新并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：

- 1 高性能电源设备和稳压器已整合到设计当中。
- 1 如适用，选用最低的电源组件。
- 1 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：

- 1 “Power Inventory and Budgeting”（**电源资源和预算**）：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。
- 1 “Power Capping”（**功率封顶**）：可对系统进行限制，以维持指定的功率限额。
- 1 “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**）屏幕上查看信息。

---

## 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需求，到您所需功率需求的同时最大化性能。

---

## 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：

- 1 累计功率
- 1 平均、最小和最大功率
- 1 功率余量值
- 1 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：

- 1 查看服务器的电源状态
- 1 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、打开电源再关闭电源）
- 1 查看服务器的电源预算信息，例如最小和最大可能功耗
- 1 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**）屏幕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）屏幕显示和提供下列信息：
  - 1 “Power Supplies Redundancy Status”（电源设备冗余状态）：可能值为：
    - o “Full”（完全）：电源设备 PS1 和 PS2 的型号相同，且均正常工作。
    - o “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。
    - o “Disabled”（禁用）：仅有其中一台电源设备可供使用。不存在冗余情况。
  - 1 “Individual Power Supply Elements”（各个电源设备组件）：可能值为：
    - o “Status”（状态）显示如下：
      - o “OK”（良好）表示电源设备存在且正在与服务器通信。
      - o “Warning”（警告）表示仅发出警告，并且必须在管理员设定的时间内采取补救操作。如果没有在管理员指定的时间内采取补救操作，将可能发生影响机箱完整性的严重电源故障。
      - o “Severe”（严重）表示已至少发出一个故障警报。故障状况表示服务器上发生电源故障，必须立即采取补救措施。
    - o Location（位置）显示电源设备名称：PS-n，其中 n 为电源编号。
    - o 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）。
    - o “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。
    - o “Maximum Wattage”（最大功率）显示电源设备的最大功率，为系统可用的 DC 功率。此值用于确定电源设备容量足以供系统配置使用。
    - o “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。
    - o “FW Version” FW（版本）表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 的远程登录/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）屏幕上提供电源子系统的电源预算状况概览。

## 使用 Web 界面

 **注：** 要执行电源管理操作，您必须拥有“Administrative”（管理员）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. 显示“Power Budget Information”（电源预算状态）屏幕。

第一张表中显示当前系统配置用户特定功率封顶的最小和最大限制。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”（最小潜在功耗）显示您可指定的最低电源预算阈值。

“Maximum Potential Power”（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 的远程登录/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。实际功耗可能在较轻负荷下较低并可能暂时超过阈值直到完成性能调整。

如果您选中**启用**电源预算阈值，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，最低潜在功率为 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。显示 **“Power Budget Information”（电源预算状态）** 屏幕。
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。您设定以瓦特或 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：** 功耗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”（启用）** 以启用阈值，或取消选中。如果您指定 **“Enabled”（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，600 BTU/小时的阈值则转回为 601 BTU/小时。

---

## 查看电源监控

### 使用 Web 界面

若要查看电源监控数据：

1. 登录到 iDRAC6 基于 Web 的界面。
2. 选择系统树中的 **“Power Monitoring”（电源监控）**。随即显示 **“Power Monitoring”（电源监控）** 屏幕。

**“Power Monitoring”（电源监控）** 屏幕上提供的信息如下：

### 电源监控

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

### Amperage（安培）

- 1 Location (位置) 显示电源设备名称: PS-n, 其中 n 为电源编号
- 1 "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。

- 1 "Cumulative" (累计) 显示从电源设备输入端测量得到的服务器的电流累积能耗。此值以千瓦时显示, 且表示系统所用总能量的累计值。您可以使用 "Reset Cumulative" (重设累计) 按钮, 重设此值。
- 1 "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。
- 1 "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。
- 1 "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。
- 1 "Finish Time" (累计) 的 "Cumulative" (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) 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设时保持不变, 所以可反映指定开始和完成时间间隔内的所有活动。"Reset Max Peaks" (重设最大峰值) 按钮将相应字段的峰值重设为零。在下一个表中, 功耗数据在系统重设时不会保持不变, 所以在这些时候会重设为零。显示的功率值是相应时间间隔 (前一分钟、小时、天和周) 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)

- 1 显示系统在上一分钟、小时、天和周的平均、最大和最小功耗。
- 1 平均功耗: 前一分钟、小时、天和周内的平均值。
- 1 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。
- 1 最大和最小时间: 出现最大和最小功耗时的时间。

## 余量

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。

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。

## 显示图形

单击这个按钮可显示上一小时以瓦特和安培为单位的 iDRAC6 功耗和电流功耗图形。用户可使用图形上所提供的下列菜单, 选择查看上周的这些数据。

 **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 **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 基于 Web 的界面。
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 "Power Control Operations" (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”（**重置系统**）（温引导）可重置系统而不断电。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服务器。如果系统电源已经关闭，则该选项被禁用。
4. 单击“Apply”（**应用**）。对话框会显示要求确认。
  5. 单击“OK”（**确定**）执行您所选的电源管理操作（例如，使系统重置）。

## 使用 RACADM

打开到服务器的远程登录/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、硬重置或电源状况。

---

[目录](#)

## 配置安全功能

### 集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [针对 iDRAC6 管理员的安全选项：](#)
- [使用 SSL 和数字认证确保 iDRAC6 通信](#)
- [使用 Secure Shell \(SSH\)](#)
- [配置服务](#)
- [启用其它 iDRAC6 安全选项](#)

iDRAC6 提供以下安全保护功能：

- 1 针对 iDRAC6 管理员的高级安全选项：
    - 1 “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。
    - 1 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：
      - o BIOS POST option-ROM
      - o 操作系统使用本地 RACADM 和 Dell OpenManage Server Administrator 公用程序
    - 1 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。
- 1 通过基于 Web 的界面或 Racadm CLI 进行会话超时配置（以秒为单位）
  - 1 可配置 IP 端口（在相应情况下）
  - 1 使用加密传输层的 Secure Shell (SSH) 实现更高的安全保护。
  - 1 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。
  - 1 连接 iDRAC6 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 ROM 选项禁用 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

此功能禁用受管系统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](http://support.dell.com) 上的 BIOS 更新软件包升级 BIOS。

#### 从本地 RACADM 禁用本地配置

此功能禁用受管系统用户使用本地 RACADM 或 Dell OpenManage Server Administrator 公用程序配置 iDRAC6 的能力。

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

 **小心：** 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置。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](http://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置。cfgRacTuneLocalConfigDisable

选项在系统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，这样可以运行本地 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，在有多名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

管理员可以选择地禁用 iDRAC6 远程 KVM，为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 管理型节点软件。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。管理员可以在支持本地 RACADM 的操作系统中使用此命令，包括 Microsoft Windows Server 2003 和 SUSE Linux Enterprise Server 10。由于此命令在系统重新引导后依然有效，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 POST 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设置执行 LocalConRedirDisable 命令来实现。

 **注：** 请参阅 Dell 支持网站 [support.dell.com](http://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](http://technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx)。

---

## 使用 SSL 和数字认证确保 iDRAC6 通信

本小节提供关于 iDRAC6 中包括的以下数据安全性功能的信息：

- 1 [“安全套接字层 \(SSL\)”](#)
- 1 [“认证签名请求 \(CSR\)”](#)
- 1 [“访问 SSL 主菜单”](#)
- 1 [“生成认证签名请求”](#)

### 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 安全协议在因特网上传输加密数据。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端之间提供验证和加密的通信以防止网络上窃听。

启用 SSL 的系统固件

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

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

iDRAC6 Web 服务器包括 Dell 自签名的 SSL 数字认证 (Server ID)。要确保互联网上的高安全性，请向 iDRAC6 提交请求生成新的认证签名请求 (CSR) 来更换 Web 服务器 SSL 认证。

### 认证签名请求 (CSR)

CSR 是认证机构 (CA) 对安全服务器认证的数字请求。安全服务器认证可以确保远程系统的身份，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，并将 CSR 提交至 CA，然后从 CA 返回的认证。

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 将向申请者颁发认证，以便在通过网络和 Internet 进行交易时唯一标识该申请者。

CA 批准 CSR 并向您发送认证后，您必须将认证上载至 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（参阅表 21-1）生成 CSR，上载现有服务器认证，或查看现有服务器认证。CSR 信息存储在 iDRAC6 固件中。表 21-2 说明了 SSL 页上的可用按钮。

表 21-1. SSL 主菜单

| 字段                                   | 说明                                                                                                                               |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 生成认证签名请求 (CSR)                       | 单击下一步打开该页，可以生成 CSR 发送给 CA 以请求安全 Web 认证。                                                                                          |
| "Upload Server Certificate"（上载服务器认证） | 单击下一步，上载您公司拥有的现有认证并用来控制对 iDRAC6 的访问。<br><br><b>注：</b> 只有 X509, Base 64 编码认证才能被 iDRAC6 接受。DER 编码的认证不被接受。上载新认证会替换 iDRAC6 中原有的默认认证。 |
| "View Server Certificate"（查看服务器认证）   | 单击“Next”（下一步）查看现有服务器认证。                                                                                                          |

表 21-2. SSL 主菜单按钮

| 按钮            | 说明           |
|---------------|--------------|
| "Print"（打印）   | 打印 SSL 主菜单页。 |
| "Refresh"（刷新） | 重载 SSL 主菜单页。 |
| Next          | 导航至下一页。      |

## 生成认证签名请求

**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 CR 前，固件中的 CSR 必须匹配 CA 返回的认证。

1. 在 SSL 主菜单上，选择生成认证签名请求 (CSR) 并单击下一步。
2. 在生成认证签名请求 (CSR) 页上输入每个 CSR 属性值。  
  
表 21-3 说明了生成认证签名请求 (CSR) 页选项。
3. 单击生成或保存 CSR。
4. 单击相应的生成认证签名请求 (CSR) 页按钮继续。表 21-4 说明了生成认证签名请求 (CSR) 页上的可用按钮。

表 21-3. 生成认证签名请求 (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、下划线和句点有效。空格无效。 |
| "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，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。                         |
| 国家和地区代码                   | 申请认证的实体所在的国家/地区名。使用下拉菜单选择国家/地区。                                              |
| "Email"（电子邮件）             | 与 CSR 相关的电子邮件地址。可以输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 21-4. 生成认证签名请求 (CSR) 页按钮

|  |  |
|--|--|
|  |  |
|--|--|

| 按钮                                      | 说明                  |
|-----------------------------------------|---------------------|
| "Print" (打印)                            | 打印生成认证签名请求 (CSR) 页。 |
| "Refresh" (刷新)                          | 重载生成认证签名请求 (CSR) 页。 |
| "Go Back to SSL Main Menu" (返回 SSL 主菜单) | 返回 SSL 主菜单页。        |
| "Generate" (生成)                         | 生成 CSR。             |

## 查看服务器认证

1. 在 SSL 主菜单项中选择"View Server Certificate" (查看服务器认证) 并单击"Next" (下一步)。

[表 21-5](#) 说明认证窗口中列出的字段及相关说明。

2. 单击相应的查看服务器认证页按钮继续。

表 21-5. 认证信息

| 字段                           | 说明           |
|------------------------------|--------------|
| "Serial Number" (序列号)        | 认证序列号        |
| "Subject Information" (主题信息) | 按照主题输入的认证属性  |
| "Issuer Information" (颁发者信息) | 按照颁发者返回的认证属性 |
| 有效期自                         | 认证的颁发日期      |
| 有效期至                         | 认证的期满日期      |

## 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:
  - 1 本地配置 ([表 21-6](#))
  - 1 Web 服务器 ([表 21-7](#))
  - 1 SSH ([表 21-8](#))
  - 1 Telnet ([表 21-9](#))
  - 1 远程 RACADM ([表 21-10](#))
  - 1 SNMP 代理 ([表 21-11](#))
  - 1 启用自动系统恢复代理 ([表 21-12](#))

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, 方法是将动作设置为: 重新引导系统、关闭系统电源或系统关机后再开机, 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. 单击相应的服务页按钮继续。请参阅[表 21-13](#)。

表 21-6. 本地配置设置

| 设置                       | 说明                                                                |
|--------------------------|-------------------------------------------------------------------|
| 使用 ROM 选项禁用 iDRAC 的本地配置  | 使用 ROM 选项禁用 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 21-7. Web 服务器设置

| 设置                              | 说明                                                                                                                        |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 已启用                             | 启用或禁用 Web 服务器。选中=启用；未选中=禁用。                                                                                               |
| "Max Sessions" (最大会话)           | 此系统允许的最大同时会话数。                                                                                                            |
| "Active Sessions" (激活的会话)       | 系统上当前会话数，小于等于"Max Sessions" (最大会话)。                                                                                       |
| "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 服务器也可进行重设。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 21-8. SSH 设置

| 设置                  | 说明                                                               |
|---------------------|------------------------------------------------------------------|
| 已启用                 | 启用或禁用 SSH。选中后，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 连接的端口。默认为 22。                                      |

表 21-9. Telnet 设置

| 设置                  | 说明                                                         |
|---------------------|------------------------------------------------------------|
| 已启用                 | 启用或禁用 Telnet。选中后，telnet 已启用。                               |
| "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 连接的端口。默认为 23。                             |

表 21-10. 远程 RACADM 设置

| 设置                        | 说明                                  |
|---------------------------|-------------------------------------|
| 已启用                       | 启用 / 禁用远程 RACADM。选中后，远程 RACADM 启用。  |
| "Active Sessions" (激活的会话) | 系统上的当前会话数。                          |
| "Active Sessions" (激活的会话) | 系统上当前会话数，小于等于"Max Sessions" (最大会话)。 |

表 21-11. SNMP 代理设置

| 设置                      | 说明                                                         |
|-------------------------|------------------------------------------------------------|
| 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 21-12. 自动系统恢复代理设置

| 设置  | 说明          |
|-----|-------------|
| 已启用 | 启用自动系统恢复代理。 |

表 21-13. 服务页按钮

| 设置 | 说明 |
|----|----|
|    |    |

| 按钮                     | 说明       |
|------------------------|----------|
| "Print" (打印)           | 打印服务页。   |
| "Refresh" (刷新)         | 刷新服务页。   |
| "Apply Changes" (应用更改) | 应用服务页设置。 |

## 启用其它 iDRAC6 安全选项

要防止未经授权访问远程系统，iDRAC6 提供了以下功能：

- 1 IP 地址筛选 (IPRange) — 定义可以访问 iDRAC6 的特定范围的 IP 地址。
- 1 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：

- 1 `cfgRacTuneIpRangeAddr`
- 1 `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 地址登录将收到一条错误。

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 21-14. IP 地址筛选 (IpRange) 属性**

| 属性                                   | 说明                                                                                                                                                                                                            |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cfgRacTuneIpRangeEnable</code> | 启用 IP 范围检查功能。                                                                                                                                                                                                 |
| <code>cfgRacTuneIpRangeAddr</code>   | 根据子网掩码中的 1，确定可接受的 IP 地址位样式。<br>此属性是与 <code>cfgRacTuneIpRangeMask</code> 的按位“与”，确定所允许 IP 地址的高端。在高位包含此位样式的任何 IP 地址都允许建立 iDRAC6 会话。从此范围外的 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。 |
| <code>cfgRacTuneIpRangeMask</code>   | 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），则在掩码中除最低的两个位以外选中所有位，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：

- 1 确保 `cfgRacTuneIpRangeMask` 配置为网络掩码的形式，所有的重要位为 1（定义掩码中的子网），在低位都变为 0。
- 1 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：

- 1 允许的登录失败次数
- 1 按秒计算的必须出现这些失败的时间范围
- 1 阻止“有问题”IP 地址在超过允许失败总数后不能建立会话的时间（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置。

 **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 21-15](#) 列出了用户定义参数。

**表 21-15. 登录重试限制属性**

| 属性                                      | 定义                                                                                                                                                                                                    |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cfgRacTuneIpBlkEnable</code>      | 启用 IP 阻塞功能。<br>如果在一段时间内 ( <code>cfgRacTuneIpBlkFailWindow</code> ) 某 IP 地址出现连续的失败 ( <code>cfgRacTuneIpBlkFailCount</code> )，则在一段时间内 ( <code>cfgRacTuneIpBlkPenaltyTime</code> ) 来自该地址的其它建立会话尝试都会遭到拒绝。 |
| <code>cfgRacTuneIpBlkFailCount</code>   | 设置拒绝某 IP 地址的登录尝试前允许的登录失败次数。                                                                                                                                                                           |
| <code>cfgRacTuneIpBlkFailWindow</code>  | 计数失败尝试的时间范围（秒）。当失败次数超出此限制，将不会记入计数器。                                                                                                                                                                   |
| <code>cfgRacTuneIpBlkPenaltyTime</code> | 定义具有过多失败的来自某 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 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**）页中配置属性值，然后单击“Apply Changes”（**应用更改**）。

[表 21-16](#) 说明了“Network Security”（**网络安全**）页设置。

5. 单击相应的“Network Security”（**网络安全**）页按钮继续。请参阅 [表 21-17](#) 了解“Network Security”（**网络安全**）页按钮的说明。

**表 21-16. 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，定义了可以访问 iDRAC6 的特定范围 IP 地址。                                                                                                                                        |
| "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”，确定所允许的 IP 地址的高端。在高位包含此位样式的任何 IP 地址都允许建立 iDRAC6 会话。从此范围外的 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。<br>例如，“255.255.255.0”。                                                                                                        |
| "IP Blocking Enabled" (IP 阻塞已启用)       | 启用 IP 地址阻止功能，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 阻塞故障窗口)  | 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过多的某个 IP 地址的登录尝试。                                                                                                                                        |

**表 21-17. 网络安全性页按钮**

| 按钮                                                 | 说明                                         |
|----------------------------------------------------|--------------------------------------------|
| "Print" (打印)                                       | 打印“Network Security”（ <b>网络安全</b> ）页       |
| "Refresh" (刷新)                                     | 重载“Network Security”（ <b>网络安全</b> ）页       |
| "Apply Changes" (应用更改)                             | 保存对“Network Security”（ <b>网络安全</b> ）页的更改。  |
| "Go Back to Network Configuration Page" (退回到网络配置页) | 返回“Network Configuration”（ <b>网络配置</b> ）页。 |

[目录](#)

## iDRAC6 的基本安装

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [准备工作](#)
- [安装 iDRAC6 Express/Enterprise 硬件](#)
- [配置系统使用 iDRAC6](#)
- [软件安装和配置概览](#)
- [在 Managed System 上安装软件](#)
- [在 Management Station 上安装软件](#)
- [更新 iDRAC6 固件](#)
- [配置支持的 Web 浏览器](#)

本部分介绍了如何安装并设置 iDRAC6 硬件和软件。

---

### 准备工作

在安装和配置 iDRAC6 软件前检查一下系统随附的项目：

- 1 iDRAC6 硬件（已安装或在可选套件中）
- 1 iDRAC6 安装步骤（在本章中）
- 1 *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，重新引导系统后，如果没有连接键盘，系统也不会通知您。

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，使用 iDRAC6 配置 公用程序。

要运行 iDRAC6 配置公用程序：

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

如果按 <Ctrl><E> <Ctrl><E> 组合键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> 键。NIC 选择随即显示。
  - b. 使用箭头键选择以下某个 NIC 模式：
    - **专用** — 选择此选项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。
    - **共享** — 选择此选项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 失败，远程访问设备将不可访问。
    - **与故障转移 LOM2 共享** — 选择此选项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 失败，远程访问设备会故障转移到 NIC 2 来进行所有数据发送。远程访问设备会继续使用 NIC 2 进行数据发送。如果 NIC 2 失败，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。
    - **与故障转移所有 LOM 共享** — 选择此选项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 失败，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 失败，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 失败，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 失败，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。
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、自动配置或静态**。
  - 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

本节从较高的级别概述了 iDRAC6 软件安装和配置过程。有关 iDRAC6 软件组件的详细信息，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：
    - 1 基于 Web 的界面（请参阅“[使用 Web 界面配置 iDRAC6](#)”）
    - 1 RACADM CLI（请参阅“[使用 iDRAC6 SM-CLP 命令行界面](#)”）
    - 1 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。没有受管系统软件，将不能在本地使用 RACADM，并且 iDRAC6 不能捕获上次崩溃屏幕。

要安装 managed system software，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](http://support.dell.com/manuals) 上提供的 *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 管理工作站软件和 iDRAC6 受管系统软件。

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 系统建立和更新公用程序，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 - 此目录包含系统管理软件产品、外设和 RAID 控制器的说明文件
- SERVICE - 包含配置系统所需的工具、提供最新的诊断程序和专为 Dell 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 *Server Administrator 用户指南*、*IT Assistant 用户指南* 和 *Unified Server Configurator 用户指南*，可访问 Dell 支持网站 [support.dell.com/manuals](http://support.dell.com/manuals) 获取这些资料。

## 在 Linux Management Station 上安装和删除 RACADM

要使用远程 RACADM 功能，在运行 Linux 的 management station 上安装 RACADM。

 **注：** 在 *Dell Systems Management Tools and Documentation* DVD 上运行**安装**时，所有所支持操作系统的 RACADM 公用程序都安装到管理工作站上。

### 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. 如果必要，使用以下命令或类似命令将 *Dell Systems Management Tools and Documentation* DVD 装入：

```
mount /media/cdrom
```

3. 导航到 `/linux/rac` 目录并执行以下命令：

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

有关 RACADM 命令的帮助，在发出上个命令后键入 `racadm help`。

### 卸载 RACADM

要卸载 RACADM，打开命令提示符并键入：

```
rpm -e <racadm_package_name>
```

其中 `<racadm_package_name>` 是用于安装 RAC 软件包的 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。

1. 基于 Web 的界面（请参阅[“使用基于 Web 的界面更新 iDRAC6 固件”](#)）
1. RACADM CLI（请参阅[“使用 RACADM 更新 iDRAC6 固件”](#)）
1. Dell Update Packages（请参阅[“使用针对所支持 Windows 和 Linux 操作系统的 Dell Update Packages 更新 iDRAC6 固件”](#)）

### 准备工作

使用本地 RACADM 或 Dell Update Packages 更新 iDRAC6 固件前，应执行以下程序。否则，固件更新操作会失败。

1. 安装并启用相应的 IPMI 和管理型节点驱动程序。
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) 的 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](http://support.dell.com) 下载最新固件并将该文件保存到本地系统。

iDRAC6 固件包包含以下软件组件:

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

## 使用基于 Web 的界面更新 iDRAC6 固件

有关详情, 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。如果在受管系统上装有 Server Administrator, 则使用本地 RACADM 更新固件。

1. 从 Dell 支持网站 [support.dell.com](http://support.dell.com) 下载 iDRAC6 固件映像到受管系统。

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 服务器上保存 **firmimg.d6** 的位置。

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

从 Dell 支持网站 [support.dell.com](http://support.dell.com) 下载并运行针对所支持 Windows 和 Linux 操作系统的 Dell Update Packages。有关详情, 请参阅 *Dell Update Package 用户指南*, 可访问 Dell 支持网站 [support.dell.com/manuals](http://support.dell.com/manuals) 获取相关资料。

 **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: 设备描述符读取 / 64, 错误 -71
```

```
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

以下部分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因特网的管理工作站连接到 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因特网。

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，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，会在可信域列表中缺少 iDRAC6 IP 地址的情况下提示您将 IP 地址添加到列表中。完成后，单击刷新或重新启动 Web 浏览器重新连接到 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，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：

- 1 英语
- 1 法语
- 1 德语
- 1 西班牙语
- 1 日语
- 1 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“工具”菜单并选择“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“语言 首选项”窗口中，单击“确定”。

## Linux

如果在具有简体中文界面 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。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> 键。以下输出会出现。

```
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_CN.GB2312:zh_CN:zh"
```

更新项：

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CN.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。如果不行，应重复此程序。

有关 iDRAC6 的高级配置，请参阅“[iDRAC6 的高级配置](#)。”

---

[目录](#)

[目录](#)

## 使用 Web 界面配置 iDRAC6

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [访问 Web 界面](#)
- [配置 iDRAC6 NIC](#)
- [配置平台事件](#)
- [配置 iDRAC6 用户](#)
- [使用 SSL 和数字认证确保 iDRAC6 通信](#)
- [配置和管理 Active Directory 认证](#)
- [配置 iDRAC6 服务](#)
- [更新 iDRAC6 固件/系统服务恢复映像](#)

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, 并提供了到相关信息的链接。

大多数 Web 界面配置任务还可以使用本地 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. 打开一个支持的 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。

iDRAC6“Login” (登录) 窗口将会出现。

## 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：

- 1 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。

- 1 您的 Active Directory 用户名。

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

2. 在“Password”（**密码**）字段中，键入 iDRAC6 用户密码或 Active Directory 用户密码。密码区分大小写。
3. 从“Domain”（**域**）下拉框中，选择“This iDRAC”（*此 iDRAC*）则以 iDRAC6 用户身份登录，或选择任何可用域则以 Active Directory 用户身份登录。

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

4. 单击“OK”（**确定**）或按 <Enter>。

## 注销

1. 在主窗口的右上角，单击“Logout”（**注销**）关闭会话。
2. 关闭浏览器窗口。

 **注：** “Log Out”（**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](http://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**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：

- n 在连接到 iDRAC6 的交换机的端口上
- n 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. 网络接口卡设置**

| 设置                        | 说明                                                                                                                                                                                                                                                          |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NIC 选择                    | 配置四种可能模式中的当前模式：<br><br>"Dedicated (iDRAC NIC)" (专用 [iDRAC NIC])<br><br><b>注：</b> 只有 iDRAC6 Enterprise 才提供此选项。<br><br>"Shared (LOM1)" (共享 [LOM1])<br><br>"Shared with Failover LOM2" (与故障转移 LOM2 共享)<br><br>"Shared with Failover All LOMs" (与故障转移所有 LOM 共享) |
| 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)。                                                                                                                                                                                       |
| 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。<br><br>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])<br><br>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) 设为 On，此选项将不可用。                                                                                                                                                                                        |

表 4-2. 常见 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。<br><br>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-service_tag，其中 service_tag 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。<br><br>默认为"Disabled" (已禁用)。<br><br><b>注：</b> 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 [用于 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                                                                                                                                                                                                                            |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 地址                                                            | 为 iDRAC NIC 指定 IP 地址。                                                                                                                                                                                                         |
| 子网掩码                                                             | 允许用户输入或编辑 iDRAC6 NIC 的静态 IP 地址。要更改此设置，请取消选择"Use DHCP" (使用 DHCP [用于 NIC IP 地址]) 复选框。                                                                                                                                           |
| 网关                                                               | 路由器或交换机的地址。该值采用"点分隔"格式，比如 192.168.0.1。                                                                                                                                                                                        |
| "Use DHCP to obtain DNS server addresses" (使用 DHCP 获取 DNS 服务器地址) | 通过选择"Use DHCP to obtain DNS server addresses" (使用 DHCP 获取 DNS 服务器地址) 复选框启用 DHCP 获取 DNS 服务器地址。如果没有使用 DHCP 获取 DNS 服务器地址，应在"Preferred DNS Server" (首选 DNS 服务器) 和"Alternate DNS Server" (备用 DNS 服务器) 字段中提供 IP 地址。<br><br>默认为 off。 |

|            |                                                                                                                                                                        |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <b>注：</b> 如果选中"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）复选框，将不能在"Preferred DNS Server"（首选 DNS 服务器）和"Alternate DNS Server"（备用 DNS 服务器）字段中输入 IP 地址。 |
| 首选 DNS 服务器 | DNS 服务器 IP 地址。                                                                                                                                                         |
| 次要 DNS 服务器 | 备用 IP 地址。                                                                                                                                                              |

表 4-4. IPv6 设置

| 设置                                                              | 说明                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 (DHCP) 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）。                                                                                                                                                                                                                                                                                                                                               |
| 前缀长度                                                            | 配置 IPv6 地址的前缀长度。可以是 1 到 128（含）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 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）。                                                                                                                                                                                                                                                                                                                                                   |
| 链接本地地址                                                          | 为 iDRAC NIC 指定 IPv6 地址。                                                                                                                                                                                                                                                                                                                                                                                          |
| IP Address 2（IP 地址 2）                                           | 为 iDRAC NIC 指定其他 IPv6 地址（若有）。                                                                                                                                                                                                                                                                                                                                                                                    |
| "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。<br><br>默认值为"Off"（关）。检查审核副本<br><br><b>注：</b> 如果选中"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）复选框，将不能在"Preferred DNS Server"（首选 DNS 服务器）和"Alternate DNS Server"（备用 DNS 服务器）字段中输入 IP 地址。 |
| 首选 DNS 服务器                                                      | 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）。                                                                                                                                                                                                                                                                                                           |
| 次要 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                                                                                                 |
|----------------------|----------------------------------------------------------------------------------------------------|
| 启用 LAN 上 IPMI        | 选中后表示 IPMI LAN 信道已启用。默认值为"Off"（关）。                                                                 |
| 信道权限级别限制             | 配置 LAN 信道上可接受的用户最低权限级别。选择以下选项之一：Administrator（管理员）、Operator（操作员）或 User（用户）。默认为 Administrator（管理员）。 |
| "Encryption Key"（密钥） | 配置密钥：0 至 20 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                                                              |
|------------|-----------------------------------------------------------------|
| 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）。     |
| 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) 配置网络安全设置。

[表 4-8](#) 说明了"Network Security" (网络安全) 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，定义了可以访问 iDRAC 的 IP 地址范围。默认为 off。                                                                                                                                  |
| "IP Range Address" (IP 范围地址)           | 根据子网掩码中的 1，确定可接受的 IP 地址样式。该值是含 IP 范围子网掩码的按位"与"，确定所允许的 IP 地址的高端。在高位包含此位样式的任何 IP 地址都允许建立 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 地址阻止功能，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。默认为 off。                                                                                                                       |
| "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 阻塞故障窗口)  | 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. 网络安全页按钮**

| 按钮                                                   | 说明                                      |
|------------------------------------------------------|-----------------------------------------|
| "Print" (打印)                                         | 打印屏幕上显示的"Network Security" (网络安全) 值。    |
| "Refresh" (刷新)                                       | 重新载入"Network Security" (网络安全) 页。        |
| "Apply Changes" (应用更改)                               | 保存"Network Security" (网络安全) 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)。

可筛选平台事件在[表 4-10](#)中列出。

**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）。

- 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" (返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。

- 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。

- 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。

- 使用支持的 Web 浏览器登录远程系统。
- 确保遵循"配置平台事件筛选器 (PEF)"中的步骤。
- 单击"System" (系统) → "Alert Management" (警报管理) → "Email Alert Settings" (电子邮件警报设置)。
- 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)。
- 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。
- 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。
- 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。
- 单击"Apply Changes" (应用更改)。
- 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" (返回到电子邮件警报目标页)。
- 单击"Go Back to the E-mail Alert Destination Page" (返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。

- 单击"Apply Changes" (应用更改)。
- 重复步骤 4 至 9 以配置其它电子邮件警报目标。

## 配置 IPMI

- 使用支持的 Web 浏览器登录远程系统。
- 配置 LAN 上 IPMI。
  - 在系统树中，单击"Remote Access" (远程访问)。
  - 单击"Configuration" (配置) 选项卡并单击"Network" (网络)。
  - 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)。
  - 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)。

- 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“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）下拉菜单，选择相应的模式。

- c. 设置 IPMI 串行波特率。

单击“Baud Rate”（波特率）下拉菜单，选择相应的波特率，并单击“Apply 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. 确保串行 MUX 在 managed system 的 BIOS 设置程序中正确设置。
  - o 重新启动系统。
  - o 在开机自检期间，按 <F2> 进入 BIOS 设置程序。
  - o 导航到“Serial Communication”（串行通信）。
  - o 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）。
  - o 保存并退出 BIOS 设置程序。
  - o 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：

- 1 删除控制
- 1 回声控制
- 1 行编辑
- 1 新行序列
- 1 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/](http://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

有关详情，请参阅 [添加和配置 iDRAC6 用户](#)。

---

## 使用 SSL 和数字认证确保 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
- 上载服务器认证
- 查看服务器认证

### 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端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，北美互联网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，使用公认证机构签署的认证更换 Web Server SSL 认证。要开始获取签署认证，可以使用 iDRAC6 Web 界面提供公司信息来生成认证签名请求 (CSR)。随后可以将生成的 CSR 提交给认证机构 (CA)，比如 VeriSign 或 Thawte。

### 认证签名请求 (CSR)

CSR 是发送至 CA 的数字请求，用于获得安全服务器认证。安全服务器认证使服务器客户机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 将向申请者颁发数字签名的认证，以在通过网络和因特网进行事务处理时唯一标识该申请者。

CA 批准了 CSR 并向用户颁发认证后，应将认证上载到 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                                                                                                                     |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 生成认证签名请求 (CSR)                       | 使用此选项可以生成 CSR 发送给 CA 以请求安全 Web 证书。<br><br><b>注：</b> 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 返回的认证匹配。 |
| “Upload Server Certificate”（上载服务器认证） | 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。                                                                                  |

|                                     |                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------|
|                                     | <b>注：</b> iDRAC6 仅接受 Base 64 编码的 X509 证书。不接受 DER 编码认证。上载新认证会替换 iDRAC6 中原有的默认认证。 |
| "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

## 生成认证签名请求

**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。

- 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)。
- 在生成认证签名请求 (CSR) 页上输入每个 CSR 属性值。表 4-12 说明了 CSR 属性。
- 单击"Generate" (生成) 以创建 CSR 并将其下载到本地计算机上。
- 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)        | 认证的确切名 (通常是 iDRAC 的域名，例如，www.xyzcompany.com)。只有字母数字字符、连字符、下划线和句点有效。空格无效。 |
| "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)            | 认证实体的城市或其它位置 (例如，朗得洛克 [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。                   |
| 国家和地区代码                    | 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. 生成认证签名请求 (CSR) 页按钮

| 按钮                                      | 说明                                                           |
|-----------------------------------------|--------------------------------------------------------------|
| "Print" (打印)                            | 打印屏幕上显示的"Generate Certificate Signing Request" (生成认证签名请求) 值。 |
| "Refresh" (刷新)                          | 重载"Generate Certificate Signing Request" (生成认证签名请求) 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。                                                |

## 上载服务器认证

- 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。

- 在"File Path" (文件路径) 字段中的"Value" (值) 字段中键入认证路径，或单击"Browse" (浏览) 导航至认证文件。

**注：** "File Path" (文件路径) 值显示上载的认证的相对文件路径。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。

- 单击"Apply" (应用)。
- 单击相应页按钮继续。请参阅表 4-14。

表 4-14. 认证上载页按钮

| 按钮 | 说明 |
|----|----|
|    |    |

|                                         |                                  |
|-----------------------------------------|----------------------------------|
| "Print" (打印)                            | 打印"Certificate Upload" (证书上传) 页。 |
| "Go Back to SSL Main Menu" (返回 SSL 主菜单) | 返回 SSL 主菜单页。                     |
| "Apply" (应用)                            | 将证书应用于 iDRAC6 固件。                |

## 查看服务器认证

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. 认证信息

| 字段                           | 说明           |
|------------------------------|--------------|
| "Serial Number" (序列号)        | 认证序列号        |
| "Subject Information" (主题信息) | 按照主题输入的认证属性  |
| "Issuer Information" (颁发者信息) | 按照颁发者返回的认证属性 |
| 有效期至                         | 认证的颁发日期      |
| 有效期至                         | 认证的期满日期      |

表 4-16. 查看服务器认证页按钮

| 按钮                                      | 说明                                             |
|-----------------------------------------|------------------------------------------------|
| "Print" (打印)                            | 打印屏幕上显示的"View Server Certificate" (查看服务器认证) 值。 |
| "Refresh" (刷新)                          | 重新载入"View Server Certificate" (查看服务器认证) 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 认证

使用该页可以配置和管理 Active Directory 设置。

-  **注：** 您必须具有"Configure iDRAC" (配置 iDRAC) 权限才能使用或配置 Active Directory。
-  **注：** 配置或使用 Active Directory 功能之前，确保配置 Active Directory 服务器以便与 iDRAC6 进行通信。
-  **注：** 有关 Active Directory 配置和如何配置扩展架构或标准架构的 Active Directory 的详情，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" (启用 Active Directory) | 指定是启用还是禁用 Active Directory |

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directory)                                                                      |                                                                                                                                                                                                                                                                                                                                                                                  |
| "Schema Selection" (架构选择)                                                       | 指定配合 Active Directory 使用标准架构还是扩展架构                                                                                                                                                                                                                                                                                                                                               |
| "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。默认设置为 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 会逐一尝试连接到各配置地址直到成功连接。如果选择扩展架构, 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。如果选择标准架构, 这些地址是用户帐户和角色组所在的域控制器的地址。                                                                                                                                                                                                                               |
| "Certificate Validation Enabled" (启用证书验证)                                       | 连接 Active Directory 时, iDRAC 总是使用安全套接字层 (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 中载入的认证 CA 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                                                          |                                                                                                                                                                                                                                                                                                                                                                                  |
| 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。                                                                                                                                                                                                                                                                                                                                             |
| 扩展架构设置                                                                          | "iDRAC Name" (iDRAC 名称): 指定唯一识别 Active Directory 中 iDRAC 的名称。该值默认为 NULL。<br>"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。                                                                                                                                                                                                              |
| 标准架构设置                                                                          | "Global Catalog Server Address 1-3 (FQDN or IP)" (全局编录服务器地址 1-3 [FQDN 或 IP]): 指定全局编录服务器的完全限定域名 (FQDN) 或 IP 地址。要求至少配置 3 个地址之一。iDRAC 会逐一尝试连接到各配置地址直到成功连接。仅当用户帐户和角色组位于不同域中时, 标准架构才需要全局编录服务器。<br>"Role Groups" (角色组): 指定与 iDRAC6 关联的角色组的列表。<br>"Group Name" (组名称): 指定标识 Active Directory 中与 iDRAC6 关联的角色组的名称。<br>"Group Domain" (组域): 指定组所在的域。<br>"Group Privilege" (组权限): 指定组的权限级别。 |

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"。                                 |
| 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:
  - 1 本地配置 — 请参阅表 4-19
  - 1 Web Server — 请参阅表 4-20 了解 Web Server 设置
  - 1 SSH — 请参阅表 4-21 了解 SSH 设置
  - 1 Telnet — 请参阅表 4-22 了解 Telnet 设置。
  - 1 远程 RACADM — 请参阅表 4-23 了解远程 RACADM 设置。

- 1 SNMP Agent — 请参阅[表](#) 了解 SNMP 设置。
- 1 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 iDRAC Local Configuration using option ROM"（使用 option ROM 禁用 iDRAC 本地配置） | 使用 option ROM 禁用 iDRAC 的本地配置。Option ROM 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 iDRAC Local Configuration using RACADM"（使用 RACADM 禁用 iDRAC 本地配置）         | 使用本地 RACADM 禁用 iDRAC 的本地配置。                                                                                     |

**表 4-20. Web 服务器设置**

| 设置                             | 说明                                                                                                                        |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 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 <b>已启用</b> 。                                                          |
| "Max Sessions"（最大会话）           | 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）       | 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 服务器也可进行重置。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                                                               |
|--------------------|------------------------------------------------------------------|
| 已启用                | 启用或禁用 SSH。选中后，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                                                         |
|--------------------|------------------------------------------------------------|
| 已启用                | 启用或禁用 Telnet。选中后，telnet 已启用。                               |
| "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 连接的端口。默认为 23。                             |

**表 4-23. 远程 RACADM 设置**

| 设置                       | 说明                                 |
|--------------------------|------------------------------------|
| 已启用                      | 启用 / 禁用远程 RACADM。选中后，远程 RACADM 启用。 |
| "Active Sessions"（激活的会话） | 系统上的当前会话数。                         |

**表 4-24. SNMP 设置**

| 设置                               | 说明                                                                                           |
|----------------------------------|----------------------------------------------------------------------------------------------|
| 已启用                              | 启用/禁用 SNMP。选中后，表示 SNMP 已启用。                                                                  |
| "SNMP Community Name"（SNMP 团体名称） | 启用/禁用 SNMP 团体名称。选中后，表示 SNMP 团体名称已启用。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                               |
|-----|----------------------------------|
| 已启用 | 启用/禁用自动系统恢复代理。选中后，表示自动系统恢复代理已启用。 |

表 4-26. 服务页按钮

| 按钮                     | 说明       |
|------------------------|----------|
| "Print" (打印)           | 打印服务页。   |
| "Refresh" (刷新)         | 刷新服务页。   |
| "Apply Changes" (应用更改) | 应用服务页设置。 |

## 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，则有可能发生），则可以使用 iDRAC6 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，可以选择重置 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)" (上传/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" (上传)。
 

该文件将上传到 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..." (正在上传文件...)
5. 在"Status (page 2 of 3)" (状态 [第 2 页, 共 3 页]) 页上，您将看到对上传的映像文件进行的验证结果。
  - 1 如果映像文件成功上传并通过所有验证检查，将显示映像文件名称。如果固件映像已上传，将显示当前固件版本和新固件版本。
  - 或
    - 1 如果映像没有成功上传，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)" (上传/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 重置为正常工作模式。

o 在固件映像的情况下，使用"Preserve Configuration" (保留配置) 可以选择保留或删除现有 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 将会重置为默认设置。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 将自动重置。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)" (上传/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) 可以选择保留或删除现有 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 将会重置为默认设置。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 将自动重置。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](#)

## iDRAC6 的高级配置

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [准备工作](#)
- [配置 iDRAC6，查看通过 SSH / Telnet 的远程串行输出](#)
- [配置串行连接的 iDRAC6](#)
- [为串行控制台连接 DB-9 或零调制解调器电缆](#)
- [配置管理站终端仿真软件](#)
- [配置串行模式和终端模式](#)
- [配置 iDRAC6 网络设置](#)
- [通过网络访问 iDRAC6](#)
- [远程使用 RACADM](#)
- [RACADM 提要](#)
- [启用和禁用 RACADM 远程功能](#)
- [配置多个 iDRAC6 控制器](#)
- [常见问题](#)

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，查看通过 SSH / Telnet 的远程串行输出

您可以为远程串行控制台重定向配置 iDRAC6，步骤如下：

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**串行通信**。
4. 如下设置**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**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

下一步，配置 iDRAC6 设置，以启用 ssh / telnet，而这可通过 RACADM 或 iDRAC6 Web 界面实现。

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** 章节下选择**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

通过管理站终端软件以 telnet 或 SSH 登录 iDRAC6 后，可以使用 telnet / SSH 命令 **connect com2** 重定向到受管系统文本控制台。一次只支持一个 **console com2** 客户端。

要连接到受管系统文本控制台，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 <号码>
```

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

如果管理站运行 Windows XP 或 Windows 2003，则可能会在 iDRAC6 telnet 会话中遇到字符问题。此问题会以冻结登录的方式发生，在这种状况下，回车键不响应并且不显示密码提示。

要解决此问题，从 Microsoft Support 网站 [support.microsoft.com](http://support.microsoft.com) 下载热修复 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 Windows Services for UNIX® 3.5 所带的 Telnet 客户端，从 Microsoft 免费下载。转至 [www.microsoft.com/downloads/](http://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 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**。

1. 在**"Windows Component Services"（Windows 组件服务）**中启用 Telnet。
2. 连接到管理站中的 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，会话可能会回音 ^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, 应键入:

```
Telnet
```

如果运行 telnet 会话, 应按 <Ctrl><]>。

3. 在提示符后, 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. 在提示符后, 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, 客户的业务就会承担风险, 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, 不过安全保护级别更高。iDRAC6 支持具有密码验证的 SSH 版本 2。安装或更新 iDRAC6 固件时, 会在 iDRAC6 上启用 SSH。

在管理站上既可以使用 PuTTY 也可以使用 OpenSSH 连接到受管系统的 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. 密码模式**

| 模式类型  | 模式                                                                                                                                                                   |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 非对称加密 | Diffie-Hellman DSA / DSS 512-1024 (随机) 位 / NIST 规范                                                                                                                   |
| 对称加密  | 1 AES256-CBC<br>1 RIJNDAEL256-CBC<br>1 AES192-CBC<br>1 RIJNDAEL192-CBC<br>1 AES128-CBC<br>1 RIJNDAEL128-CBC<br>1 BLOWFISH-128-CBC<br>1 3DES-192-CBC<br>1 ARCFOUR-128 |
| 信息完整性 | 1 HMAC-SHA1-160<br>1 HMAC-SHA1-96<br>1 HMAC-MD5-128                                                                                                                  |

|    |               |
|----|---------------|
|    | 1 HMAC-MD5-96 |
| 验证 | 1 密码          |

 **注：** SSHv1 不支持。

## 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 VT100 仿真窗口中，将显示重定向控制台的窗口或应用程序设置为 25 行 x 80 列以确保正确的文本显示；否则，有些文本屏幕可能会混乱。

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. 在内核上追加两个选项：

```
kernelconsole=ttyS1,57600
```

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，显示在此步骤中说明的更改。

**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                                                            |
| <b>serial --unit=1 --speed=57600</b>                                                               |
| <b>terminal --timeout=10 serial</b>                                                                |
| 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/sdal hda=ide-scsi console=ttyS0 console=ttyS1,57600 |
| 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/sdal 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=ttyS1,57600
```

[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/inittab**

```
#
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

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6: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串行连接到 iDRAC6:

- 1 iDRAC6 CLI
- 1 直接连接基本模式
- 1 直接连接终端模式

将系统设置为可使用任何一种界面, 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**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**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。

下一步, 将 DB-9 或零调制解调器电缆从管理站连接到管理型节点服务器。请参阅[为串行控制台连接 DB-9 或零调制解调器电缆](#)。

下一步, 确认您的管理站终端仿真软件已配置串行连接。请参阅[配置管理站终端仿真软件](#)。

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。

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 串行** 一节下选择**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, 您可看到一个登录提示。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
```

## 配置直接连接基本模式和直接连接终端模式的 iDRAC

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 串行** 一节下取消选择**启用**。

直接连接基本模式：

在 **IPMI 串行** 一节下，将**连接模式设置**下拉菜单更改为**直接连接基本模式**。

直接连接终端模式：

在 **IPMI 串行** 一节下，将**连接模式设置**下拉菜单更改为**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或关闭服务器：

1. 终端仿真软件连接至 iDRAC6

2. 键入以下登录命令：

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

您将看到以下响应：

```
[SYS]
```

```
[良好]
```

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]
```

## 在直接连接终端模式与串行控制台重定向之间切换

iDRAC6 支持 Escape 键序列，允许在直接连接终端模式与串行控制台重定向之间切换。

为系统设置允许此行为的步骤如下：

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**串行通信**。

4. 如下设置“Serial Communication”（**串行通信**）屏幕：

串行通信 -- 带有 com2 串行重定向打开

 **注：** 您可以将 serial 串行通信字段设置为 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 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**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。

要将直接连接终端模式切换为串行控制台重定向模式，使用以下的 Escape 键序列：

<Esc> + <Shift> <q>

要将串行控制台重定向模式切换为直接连接终端模式，使用以下的 Escape 键序列：

<Esc> + <Shift> <9>

---

## 为串行控制台连接 DB-9 或零调制解调器电缆

要使用串行文本控制台访问 Managed System，请将 DB-9 零调制解调器电缆连接到 Managed System 上的 COM 端口。为使连接能用于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          |

---

## 配置管理站终端仿真软件

iDRAC6 支持在运行以下某种终端仿真软件的管理站上使用串行或 telnet 文本控制台：

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

执行以下子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，在提示符处输入 `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重新调整为 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，输入 `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" (重置)**、**"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

使用 [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

超级终端是 Microsoft Windows 串行端口访问公用程序。要按比例设置控制台屏幕的大小，使用 Hilgraeve 的 HyperTerminal Private Edition 版本 6.3。

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     |
| 数据流控制 | 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                                                                                                                                   |
|----------|--------------------------------------------------------------------------------------------------------------------------------------|
| 连接模式设置   | <ul style="list-style-type: none"> <li>1 直接连接基本模式 - IPMI 串行基本模式</li> <li>1 直接连接终端模式 - IPMI 串行终端模式</li> </ul>                         |
| 波特率      | <ul style="list-style-type: none"> <li>1 设置数据速度。选择 <b>9600 bps</b>、<b>19.2 kbps</b>、<b>57.6 kbps</b> 或 <b>115.2 kbps</b>。</li> </ul> |
| 数据流控制    | <ul style="list-style-type: none"> <li>1 无 — 硬件流控制关闭</li> <li>1 RTS/CTS — 硬件流控制打开</li> </ul>                                         |
| 信道权限级别限制 | <ul style="list-style-type: none"> <li>1 管理员</li> <li>1 操作员</li> <li>1 用户</li> </ul>                                                 |

表 5-9. iDRAC6 串行设置

| 设置                                | 说明                                                                                                                 |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 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。                                                                                          |
| 波特率                               | 外部串行端口的数据速度。值包括 <b>9600 bps</b> 、 <b>28.8 kbps</b> 、 <b>57.6 kbps</b> 和 <b>115.2 kbps</b> 。默认值为 <b>57.6 kbps</b> 。 |
| "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 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)           | 打印串行配置页。               |
| "Refresh" (刷新)         | 刷新串行配置页。               |
| "Apply Changes" (应用更改) | 应用 IPMI 和 iDRAC6 串行更改。 |
| 终端模式设置                 | 打开终端模式设置页。             |

## 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. 在串行配置页中单击"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        |
|------|-----------|
| 行编辑  | 启用或禁用行编辑。 |
| 删除控制 | 选择以下选项之一： |

|        |                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>1 iDRAC 在收到 &lt;bksp&gt; 或 &lt;del&gt; 时输出 &lt;bksp&gt;&lt;sp&gt;&lt;bksp&gt; 字符—</li> <li>1 iDRAC 在收到 &lt;bksp&gt; 或 &lt;del&gt; 时输出 &lt;del&gt; 字符—</li> </ul> |
| 回声控制   | 启用或禁用回声。                                                                                                                                                                                                |
| 符号交换控制 | 启用或禁用符号交换。                                                                                                                                                                                              |
| 新行序列   | 选择 None、<CR-LF>、<NULL>、<CR>、<LF-CR> 或 <LF>。                                                                                                                                                             |
| 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)                                       | 打印终端模式设置页。  |
| "Refresh" (刷新)                                     | 刷新终端模式设置页。  |
| "Go Back to Serial Port Configuration" (返回到串行端口配置) | 返回串行端口配置页。  |
| "Apply Changes" (应用更改)                             | 应用终端模式设置更改。 |

## 配置 iDRAC6 网络设置

 **小心：** 更改 iDRAC6 网络设置可能会断开当前网络连接。

使用以下任一工具配置 iDRAC6 网络设置：

- 1 基于 Web 的接口 — 请参阅 [“配置 iDRAC6 NIC”](#)
- 1 RACADM CLI — 请参阅 [“cfgLanNetworking”](#)。
- 1 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，可以使用下述任何一种界面来远程访问受管系统：

- 1 基于 Web 的界面
- 1 RACADM
- 1 Telnet 控制台
- 1 SSH
- 1 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 | <p>提供了使用图形用户界面到 iDRAC6 的远程访问。基于 Web 的界面构建在 iDRAC6 固件中并从管理站中支持的 Web 浏览器通过 NIC 接口访问。</p> <p>关于支持的 Web 浏览器列表，请参阅 <a href="#">“支持的 Web 浏览器。”</a></p>                                                                                                                             |
| RACADM     | <p>提供通过命令行界面到 iDRAC6 的远程访问。RACADM 使用 iDRAC6 IP 地址执行 RACADM 命令。</p> <p><b>注：</b> racadm 远程功能选项只在管理站上受支持。有关详情，请参阅 <a href="#">“远程使用 RACADM。”</a></p> <p><b>注：</b> 使用 racadm 远程功能时，须在使用有关文件操作的 RACADM 子命令的文件夹上写明权限，例如：</p> <pre>racadm getconfig -f &lt;文件名&gt;</pre> <p>或：</p> |

|            |                                                                                                                                                                                     |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | 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 <b>powerdown</b> 、 <b>powerup</b> 、 <b>powercycle</b> 和 <b>hardreset</b> 命令。<br><br><b>注：</b> 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    | 提供通过 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 <a href="http://support.dell.com/manuals">support.dell.com/manuals</a> 上的《Dell OpenManage 基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。

请参阅“支持的 Web 浏览器”查看支持的 Web 浏览器的列表。

要使用 Server Administrator 访问 iDRAC6 远程访问界面，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 的详情以及相关文档的列表，请参阅“[iDRAC6 的基本安装](#)。”

RACADM 提供远程功能选项 (-r)，可以允许连接受管系统和从远程控制台或管理站执行 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认证存储中没有 iDRAC6 认证，则在键入 RACADM 命令时会显示一条消息。有关 iDRAC6 认证的详情，请参阅“[使用 SSL 和数字认证确保 iDRAC6 通信](#)。”

Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (安全警告: 认证无效 - 认证名称无效或与站点名称不匹配)

继续执行。为 racadm 使用 -s 选项以停止认证相关错误的执行。

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消息：

Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (安全警告: 认证无效 - 认证名称无效或与站点名称不匹配)

Racadm 不继续执行命令。

错误：无法按照指定 IP 地址连接到 iDRAC6

**注：** RACADM 远程功能只在管理站上受支持。有关详情，请参阅 Dell 支持网站 [support.dell.com/manuals](http://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 子命令的文件夹上写明权限，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 端口号更改为非默认端口 (443) 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>       | 指定控制器的远程 IP 地址。                                           |
| -r <racIpAddr>:<端口号> | 用法: <端口号> 如果 iDRAC6 端口号不是默认端口 (443)                       |
| -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 -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 应检查是否有无效认证错误。如果检测到无效认证, 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                                    |
|----------------------------------|---------------------------------------|
| <a href="#">help</a>             | 列出 iDRAC6 子命令。                        |
| <a href="#">help &lt;子命令&gt;</a> | 列出指定子命令的用法语句。                         |
| <a href="#">arp</a>              | 显示 ARP 表的内容。ARP 表条目不能被添加或删除。          |
| <a href="#">clearasrscreen</a>   | 清除上一个 ASR (崩溃) 屏幕 (上一个蓝色屏幕)。          |
| <a href="#">clrraclog</a>        | 清除 iDRAC6 日志。单个条目被用来指示清除日志的用户和时间。     |
| <a href="#">config</a>           | 配置 iDRAC6。                            |
| <a href="#">getconfig</a>        | 显示当前 iDRAC6 配置属性。                     |
| <a href="#">coredump</a>         | 显示最新 iDRAC6 信息转储。                     |
| <a href="#">coredumpdelete</a>   | 删除 iDRAC6 中存储的信息转储。                   |
| <a href="#">fwupdate</a>         | 执行或显示 iDRAC6 固件更新的状况。                 |
| <a href="#">getssninfo</a>       | 显示关于活动会话的信息。                          |
| <a href="#">getsysinfo</a>       | 显示一般 iDRAC6 和系统信息。                    |
| <a href="#">getrctime</a>        | 显示 iDRAC6 时间。                         |
| <a href="#">ifconfig</a>         | 显示当前 iDRAC6 的 IP 配置。                  |
| <a href="#">netstat</a>          | 显示路径选择表和当前连接。                         |
| <a href="#">ping</a>             | 验证目标 IP 地址是否可以使用当前路由表内容从 iDRAC6 进行访问。 |
| <a href="#">setniccfg</a>        | 设置控制器的 IP 配置。                         |
| <a href="#">getniccfg</a>        | 显示控制器的当前 IP 配置。                       |
| <a href="#">getsvctag</a>        | 显示服务标签。                               |

|                                 |                                                    |
|---------------------------------|----------------------------------------------------|
| <a href="#">racdump</a>         | 转储 iDRAC6 状况和状态信息以进行调试。                            |
| <a href="#">racreset</a>        | 重置 iDRAC6。                                         |
| <a href="#">racresetcfg</a>     | 将 iDRAC6 重置为默认配置。                                  |
| <a href="#">serveraction</a>    | 在 managed system 上执行电源管理操作。                        |
| <a href="#">getraclog</a>       | 显示 iDRAC6 日志。                                      |
| <a href="#">clrsl</a>           | 清除系统事件日志条目。                                        |
| <a href="#">gettracelog</a>     | 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。 |
| <a href="#">sslcsrgen</a>       | 生成并下载 SSL CSR。                                     |
| <a href="#">sslcertupload</a>   | 将 CA 认证或服务器认证上传至 iDRAC6。                           |
| <a href="#">sslcertdownload</a> | 下载 CA 认证。                                          |
| <a href="#">sslcertview</a>     | 查看 iDRAC6 中的 CA 认证或服务器认证。                          |
| <a href="#">sslkeyupload</a>    | 强制 DRAC6 通过 DRAC6 NIC 发送检测电子邮件来检查电子邮件配置。           |
| <a href="#">testtrap</a>        | 强制 DRAC6 通过 DRAC6 NIC 发送检测 SNMP 陷阱来检查陷阱配置。         |
| <a href="#">vmdisconnect</a>    | 强制关闭虚拟介质连接。                                        |
| <a href="#">vmkey</a>           | 将虚拟闪存更新大小重置为默认大小 (256 MB)。                         |

## 有关 RACADM 错误消息的常见问题

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

**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 完成重置后，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：

- 1 本地 RACADM 错误信息—类似语法、拼写错误和错误名称的问题。
- 1 远程 RACADM 错误信息—类似错误 IP 地址、错误用户名或错误密码的问题。

当从系统输入 iDRAC6 IP 地址并在 输入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 卡，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 iDRAC6 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. 重置已配置的目标 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，可以用其他名称配置该文件。

可以使用 `getconfig` 命令来执行以下操作：

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

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

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

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

 **小心：** 建议使用简单文本编辑器编辑此文件。RACADM 公用程序使用 ASCII 文本分析器。任何格式混淆分析器，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，并且该文件不要求 `.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：

- 1 创建
- 1 通过 `racadm getconfig -f <文件名>.cfg` 命令获取
- 1 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：

- 1 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，则该索引将在配置过程中在 iDRAC6 上创建。
- 1 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。

- 1 使用 `racresetcfg` 子命令配置所有具有相同属性的 iDRAC6 卡。

使用 `racresetcfg` 子命令将 iDRAC6 重置为初始默认值，然后运行 `racadm config -f <文件名>.cfg` 命令。确保 `.cfg` 文件中包含所有所需的对象、用户、索引和其它参数。

 **小心：** 使用 `racresetcfg` 子命令将数据库和 iDRAC6 NIC 设置重置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置为默认设置。

## 分析规则

- 1 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。任何其他列中的“#”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>
```

- 1 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}
```

- 1 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实例。

- 1 .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>
```

- 1 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>
```

- 1 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：

对象组 "cfgLanNetworking"

#
```

```
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
注释, 此行的其余部分将被忽略
cfgNicGateway=10.35.9.1
```

命令 `racadm config -f myfile.cfg` 分析文件并按行号识别错误。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。”](#)

以下实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：

- 1 专用
- 1 共享
- 1 与故障转移 LOM2 共享
- 1 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 iDRAC MAC 地址。  |

## 常见问题

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

iDRAC6 包括了一个默认的 iDRAC6 服务器认证以确保基于 Web 的界面和远程 RACADM 配置的网络安全。如果使用该认证，Web 浏览器就会显示一个安全警告，因为默认的认证是颁发给 **iDRAC6 默认认证**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，应上载一个办法给 IP 地址的 iDRAC6 服务器认证，或 iDRAC6 的 iDRAC 名称。生成用于颁发认证的认证签名请求 (CSR) 时，应确保 CSR 的常用名 (CN) 与 iDRAC6 的 IP 地址（**如果是颁发给 IP 的认证**）（例如，192.168.0.120）或注册的 DNS iDRAC6 名称（**如果是颁发给 iDRAC 注册名称的认证**）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**常见设置表**：
  - a. 选择**在 DNS 上注册 iDRAC**复选框。
  - b. 在**DNS iDRAC 名称**字段，输入 iDRAC6 名称。
4. 单击"Apply Changes"（**应用更改**）。

请参阅 ["使用 SSL 和数字认证确保 iDRAC6 通信"](#) 了解有关生成 CSR 和颁发认证的详情。

**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？**

重置 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置：

- 1 使用 iDRAC6 Web 用户界面更改网络配置或网络安全属性时
- 1 更改 `cfgRacTuneHttpsPort` 属性时（包括 `config -f 配置文件` 更改它时）
- 1 使用 `racresetcfg` 时
- 1 iDRAC6 重置时
- 1 上载新的 SSL 服务器认证时

**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 认证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 服务器认证以确保基于 Web 的界面和远程 RACADM 配置的网络安全。此认证不是由可信 CA 颁发的。要解决这个安全问题，上载一个由可信 CA（例如微软认证机构、Thawte 或 Verisign）颁发的 iDRAC6 服务器认证。请参阅 ["使用 SSL 和数字认证确保 iDRAC6 通信"](#) 了解有关颁发认证的详情。

---

[目录](#)

## 添加和配置 iDRAC6 用户

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [使用 Web 界面配置 iDRAC6 用户](#)
- [使用 RACADM 公用程序配置 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：** 您须拥有**配置用户**权限来配置 iDRAC 用户。

1. 单击**远程访问** → **配置** → **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](#)描述配置 iDRAC 用户的用户状态和权限。

 **注：** User 1 为 IPMI 匿名用户保留，不可配置。

2. 在“User ID”（**用户 ID**）列单击用户 ID 编号。

在**用户主菜单**项，您可配置用户、查看用户认证、上传可信认证机构（CA）认证或查看可信 CA 认证。

如果选择**配置用户**并单击**下一步**，则 **用户配置**页将会显示。请继续执行步骤 4。

若您在 **Smart Card 配置**项下选择一个选项，请参阅 [表 6-2](#)。

3. 在**用户配置**页，配置以下项目：

- 1 新的或现有的 iDRAC 用户的用户名、密码和访问权限。 [表 6-3](#) 说明 **常规用户设置**。
- 1 用户的 IPMI 权限。 [表 6-4](#) 说明 **IPMI 用户权限**以供配置用户 LAN 权限。
- 1 iDRAC 用户权限。 [表 6-5](#) 说明 **iDRAC 用户权限**。
- 1 iDRAC 组访问权限。 [表 6-6](#) 说明 **iDRAC 组权限**。

4. 完成后单击“Apply Changes”（**应用更改**）。

5. 单击相应按钮继续。请参阅 [表 6-7](#)。

**表 6-1. 用户状态和权限**

| 设置         | 说明                                                                                                    |
|------------|-------------------------------------------------------------------------------------------------------|
| 用户 ID      | 显示用户 ID 编号顺序列表。在 <b>用户 ID</b> 下的每个字段包含 16 个预设用户 ID 编号之一。此字段不能编辑。                                      |
| State (状态) | 显示用户的登录状态：启用或禁用。（禁用为默认。）<br><br><b>注：</b> User 2 默认为启用。                                               |
| 用户名        | 显示用户登陆名称。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。<br><br><b>注：</b> iDRAC6 上的用户名不能包含 /（正斜杠） 或 .（句点）字符。 |

|             |                                            |
|-------------|--------------------------------------------|
|             | <b>注：</b> 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 权限      | 显示将用户分配至的组（权限级别）（管理员、操作员、只读或无）。            |
| IPMI LAN 权限 | 显示将用户分配至的 IPMI LAN 权限级别（管理员、操作员、只读或无）。     |
| IPMI 串行权限   | 显示将用户分配至的 IPMI 串行端口权限级别（管理员、操作员、只读或无）。     |
| 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                                                   |
|------------|------------------------------------------------------|
| 查看用户认证     | 显示已上载到 iDRAC 的用户认证页。                                 |
| 上载可信 CA 认证 | 使您能够将可信 CA 认证上载到 iDRAC 并导入用户配置文件。                    |
| 查看可信 CA 认证 | 显示已上载到 iDRAC 的可信 CA 认证。可信 CA 认证由得到授权可向用户颁发认证的 CA 颁发。 |

表 6-3. 常规用户设置

|                               |                                                                        |
|-------------------------------|------------------------------------------------------------------------|
| 用户 ID                         | 16 个预设用户 ID 编号之一。                                                      |
| 启用用户                          | 选中后表示用户访问 iDRAC6 的权限已启用。取消选取后，用户的权限会被禁用。                               |
| 用户名                           | 用户名最多 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。取消选取时，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）。字符将不显示。                                     |
| "Confirm New Password"（确认新密码） | 重新输入 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： <b>管理员、操作员、用户或无</b> 。 |
| "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： <b>管理员、操作员、用户或无</b> 。   |
| 启用 LAN 上串行                                                  | 允许用户使用"Serial over LAN"（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                                                                                       |
|---------------------------------------|------------------------------------------------------------------------------------------|
| 角色                                    | 指定用户最大的 iDRAC 用户权限为以下用户组之一： <b>管理员、操作员、用户或无</b> 。请参阅 <a href="#">表 6-6</a> 了解 iDRAC 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。                                                                            |
| 配置用户                                  | 使用户可以允许特定用户访问系统。                                                                         |
| 清除日志                                  | 允许用户清除 iDRAC 日志。                                                                         |
| 执行服务器控制命令                             | 使用户执行服务器控制命令。                                                                            |
| 访问控制台重定向                              | 允许用户运行控制台重定向。                                                                            |
| 访问虚拟介质                                | 允许用户运行和使用虚拟介质。                                                                           |
| 检测警报                                  | 允许用户将测试警报（电子邮件或 PET）发送到特定用户。                                                             |
| "Execute Diagnostic Commands"（执行诊断命令） | 允许用户运行诊断命令。                                                                              |

表 6-6. iDRAC 组权限

| 用户组 | 授予的权限                                                                                                                                                                                                                                                                                      |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理员 | "Login to iDRAC"（登录到 iDRAC）、"Configure iDRAC"（配置 iDRAC）、"Configure Users"（配置用户）、"Clear Logs"（清除日志）、"Execute Server Control Commands"（执行服务器控制命令）、"Access 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）            |
| 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） |
| 只   | "Login to iDRAC"（登录到 iDRAC）                                                                                                                                                                                                                                                                |

|   |        |
|---|--------|
| 读 |        |
| 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 屏幕上显示的用户配置值。                    |
| "Refresh" (刷新)                   | 重新载入"User Configuration" (用户配置) 页。 |
| "Go Back To Users Page" (返回到用户页) | 返回"Users Page" (用户页)。              |
| "Apply Changes" (应用更改)           | 保存用户配置页上所做的任何新设置。                  |

## 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。

iDRAC6 基于 Web 的界面是配置 iDRAC6 用户的最快方式。如果选择命令行或脚本配置或需要配置多个 iDRAC6 卡，请使用随 iDRAC6 代理安装在受管系统上的 RACADM。

要配置多个具有相同配置设置的 iDRAC6 卡，请执行以下程序之一：

- 1 参考本节中的 RACADM 示例，创建 RACADM 命令的批处理文件，然后在各个受管系统上执行该批处理文件。
- 1 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受管系统上执行 `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 重置回原始默认值。

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

 **注：** 可以随时启用和禁用用户。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：

- 1 iDRAC 权限
- 1 IPMI LAN 权限
- 1 IPMI 串行权限
- 1 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 cfgUserAdminIpmlanPrivilege 4
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmlSerialPrivilege 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。

 **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](#)

## 将 iDRAC6 用于 Microsoft Active Directory

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [为 iDRAC6 启用 Active Directory 验证的前提条件](#)
- [支持的 Active Directory 身份验证机制](#)
- [扩展架构 Active Directory 概述](#)
- [标准架构 Active Directory 概述](#)
- [测试您的配置](#)
- [在域控制器上启用 SSL](#)
- [使用 Active Directory 登录到 iDRAC6](#)
- [常见问题](#)

目录服务维护一个公用数据库，在其中存储用于在网络上控制用户、计算机、打印机等的所有必需信息。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，以允许控制和将 iDRAC6 用户权限添加到 Active Directory 软件中的现有用户。

 **注：** 使用 Active Directory 识别 iDRAC6 用户在 Microsoft Windows® 2000、Windows Server® 2003 和 Windows Server 2008 操作系统上受支持。

表 7-1 显示了九种 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                 |
| 配置用户                                   | 使用户可以允许特定用户访问系统               |
| 清除日志                                   | 允许用户清除 iDRAC6 日志              |
| 执行服务器控制命令                              | 允许用户执行 RACADM 命令              |
| 访问控制台重定向                               | 允许用户运行控制台重定向                  |
| 访问虚拟介质                                 | 允许用户运行和使用虚拟介质                 |
| 检测警报                                   | 允许用户将测试警报 (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                    |

## 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层 (SSL)。有关详情，请参阅“[在域控制器上启用 SSL](#)”。

## 支持的 Active Directory 身份验证机制

可以通过两种方法使用 Active Directory 定义对 iDRAC6 的用户访问：一种方法是使用扩展架构解决方案，该解决方案采用 Dell 定义的 Active Directory 对象。另一种方法是使用标准架构解决方案，该解决方案仅采用 Active Directory 组对象。关于这些方案的详细信息，请参阅下面的部分。

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

使用扩展架构解决方案的优势有：

- 1 所有权限控制对象都在 Active Directory 中。
- 1 在不同 iDRAC6 卡上用不同权限级别配置用户权限时具有最大的灵活性。

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

## 扩展架构 Active Directory 概述

使用扩展架构解决方案要求 Active Directory 架构扩展，如下面部分所述。

## 扩展 Active Directory 架构

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

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

Schema Extender 和 Active Directory 用户和计算机 MMC 管理单元扩展在 *Dell Systems Management Tools and Documentation DVD* 上提供。有关详情，请参阅“扩展 Active Directory 架构”和“安装 Dell 对 Active Directory 用户和计算机管理单元的扩展”。有关为 iDRAC6 扩展架构和安装 Active Directory 用户和计算机 MMC 管理单元的进一步详情，请参阅 [support.dell.com/manuals](http://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 架构扩展

Active Directory 数据是属性和类的分布式数据库。Active Directory 架构包含确定可添加或包含在数据库中的数据类型的规则。用户类是数据库中存储的类的一个示例。一些示例用户类属性包括用户的名字、姓氏和电话号码等。公司可以通过添加自己独特的属性和类扩展 Active Directory 数据库以解决特定环境下的需求。Dell 扩展了该架构包括必要的更改以支持远程管理验证和授权。

每个添加到现有 Active Directory 架构的属性或类都必须定义一个唯一的 ID。为了保证整个业界 ID 的唯一，Microsoft 维护着一个 Active Directory 对象标识符 (OID) 数据库，从而在各公司向架构中添加扩展时，能够确保唯一性并且相互间不会冲突。为了扩展 Microsoft Active Directory 中的架构，Dell 为我们添加到目录服务的属性和类申请了唯一的 OID、唯一的名称扩展以及唯一链接的属性 ID。

Dell 扩展名是： dell

Dell 基础 OID 是： 1.2.840.113556.1.8000.1280

RAC LinkID 范围是： 12070 到 12079

## iDRAC 架构扩展概览

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

## Active Directory 对象概览

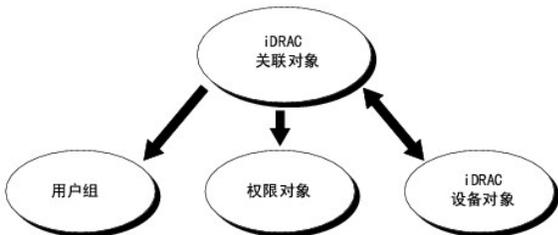
对于网络上每一个要与 Active Directory 集成以进行验证和授权的物理 iDRAC 来说，请创建至少一个关联对象和一个 iDRAC 设备对象。可以创建多个关联对象，每个关联对象都可以链接到任意多个用户、用户组或 iDRAC 设备对象。用户和 iDRAC 用户组可以是企业中任何域的成员。

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

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。

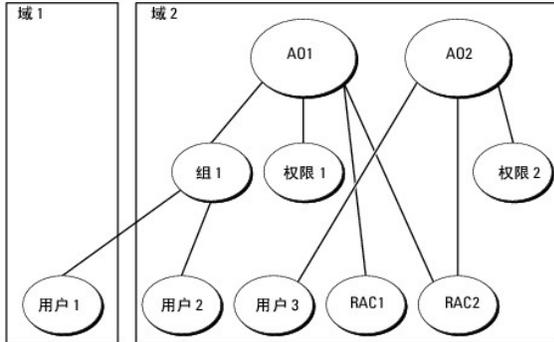
来自任何域的用户、用户组或嵌套的用户组可添加到关联对象中。扩展架构解决方案支持 Microsoft Active Directory 允许的任何用户组类型和跨多个域的任何用户组嵌套。

## 使用扩展架构累积权限

扩展架构验证机制支持对通过不同关联对象与同一用户相关的不同权限对象进行权限累积。换句话说，扩展架构验证累积权限使用户能够超越拥有与同一用户关联的不同权限对象的所有已分配权限。

图 7-2 提供了使用扩展架构累积权限的示例。

图 7-2. 用户权限累积



该图显示两个关联对象—A01 和 A02。用户1 通过两个关联对象与 iDRAC2 关联。因此，用户1 具有累积权限，即在 iDRAC2 上将权限 1 和权限 2 的权限合并起来。

例如，Priv1 有如下权限：登录、虚拟介质和清除日志，而 Priv2 有如下权限：登录到 iDRAC、配置 iDRAC 和测试警报。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 的权限集的合并结果。

扩展架构验证利用同一用户关联的不同权限对象的已分配权限，累积权限可实现最大的权限合集。

在此配置中，用户1 在 iDRAC2 上拥有 Priv1 和 Priv2 权限。用户1 仅在 iDRAC2 上拥有 Priv1 权限。用户2 在 iDRAC1 和 iDRAC2 上都拥有 Priv1 权限。此外，该图还表明用户 1 可位于不同的域并由嵌套组关联。

## 配置扩展架构 Active Directory 访问 iDRAC

在使用 Active Directory 访问 iDRAC6 之前，必须配置 Active Directory 软件和 iDRAC6。方法是按顺序执行下列步骤：

1. 扩展 Active Directory 架构（请参阅[“扩展 Active Directory 架构”](#)）。
2. 扩展 Active Directory 用户和计算机管理单元（请参阅[“安装 Dell 对 Active Directory 用户和计算机管理单元的扩展”](#)）。
3. 将 iDRAC6 用户及其权限添加到 Active Directory（请参阅[“将 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[“通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC6”](#)或[“通过扩展架构使用 RACADM 配置 Active Directory”](#)）。

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

可以使用以下方法之一扩展架构：

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

如果使用 LDIF 脚本，将不会把 Dell 组织单元添加到架构。

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

- 1 DVD 驱动器:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory\_Tools\Remote\_Management\_Advanced\LDIF\_Files
- 1 <DVD 驱动器>:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory\_Tools\Remote\_Management\_Advanced\Schema Extender

要使用 LDIF 文件，请参阅 *LDIF\_Files* 目录中自述文件中的说明。要使用 Dell Schema Extender 扩展 Active Directory 架构，请参阅[“使用 Dell Schema Extender”](#)。

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

## 使用 Dell Schema Extender

**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**欢迎**屏幕中单击“Next”（下一步）。
2. 阅读并了解警告，单击“Next”（下一步）。
3. 选择“Use Current Log In Credentials”（使用当前登录凭据）或输入具有架构管理员权限的用户名和密码。
4. 单击“Next”（下一步）运行 Dell Schema Extender。
5. 单击 **Finish**（完成）。

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

- 1 类（请参阅 [表 7-2](#) 到 [表 7-7](#)）
- 1 属性（[表 7-8](#)）

请参阅 Microsoft 说明文件，详细了解如何使用 MMC 和 Active Directory 架构管理单元。

**表 7-2. 添加到 Active Directory 架构的类的类定义**

| 类名称                  | 分配的对象标识号 (OID)                     |
|----------------------|------------------------------------|
| dellIDRACDevice      | 1.2.840.113556.1.8000.1280.1.7.1.1 |
| dellIDRACAssociation | 1.2.840.113556.1.8000.1280.1.7.1.2 |
| dellIRAC4Privileges  | 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<br>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<br>dellPrivilegeMember |

**表 7-5. dellIRAC4Privileges 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（授权利）。                                                                   |
| 类的类型 | 辅助类                                                                                      |
| 超类   | 无                                                                                        |
| 属性   | dellIsLoginUser<br>dellIsCardConfigAdmin<br>dellIsUserConfigAdmin<br>dellIsLogClearAdmin |

|                         |
|-------------------------|
| dellServerResetUser     |
| dellConsoleRedirectUser |
| dellVirtualMediaUser    |
| dellTestAlertUser       |
| dellDebugCommandAdmin   |

表 7-6. dellPrivileges 类

|      |                                    |
|------|------------------------------------|
| OID  | 1.2.840.113556.1.8000.1280.1.1.1.4 |
| 说明   | 用作 Dell 权限（授权权利）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 架构的属性的列表

| 属性名称/说明                                                                                                                            | 分配的 OID/语法对象标识符                                                                              | 单值    |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------|
| <b>dellPrivilegeMember</b><br>属于此属性的 dellPrivilege 对象的列表。                                                                          | 1.2.840.113556.1.8000.1280.1.1.2.1<br>可分辨名称 (LDAPTYPE_DN<br>1.3.6.1.4.1.1466.115.121.1.12)   | FALSE |
| <b>dellProductMembers</b><br>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。<br>链接 ID: 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2<br>可分辨名称 (LDAPTYPE_DN<br>1.3.6.1.4.1.1466.115.121.1.12)   | FALSE |
| <b>dellLoginUser</b><br>如果用户具有设备的登录权限，则为 TRUE。                                                                                     | 1.2.840.113556.1.8000.1280.1.1.2.3<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |
| <b>dellCardConfigAdmin</b><br>如果用户具有设备的卡配置权限，则为 TRUE。                                                                              | 1.2.840.113556.1.8000.1280.1.1.2.4<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |
| <b>dellUserConfigAdmin</b><br>如果用户具有设备的用户配置权限，则为 TRUE。                                                                             | 1.2.840.113556.1.8000.1280.1.1.2.5<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |
| <b>dellLogClearAdmin</b><br>如果用户具有设备的日志清除权限，则为 TRUE。                                                                               | 1.2.840.113556.1.8000.1280.1.1.2.6<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |
| <b>dellServerResetUser</b><br>如果用户具有设备的服务器重置权限，则为 TRUE。                                                                            | 1.2.840.113556.1.8000.1280.1.1.2.7<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |
| <b>dellConsoleRedirectUser</b><br>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<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |
| <b>dellVirtualMediaUser</b><br>如果用户具有设备的虚拟介质权限，则为 TRUE。                                                                            | 1.2.840.113556.1.8000.1280.1.1.2.9<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7) | TRUE  |

|                                                                                                                              |                                                                                                            |       |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-------|
| <b>dellIsTestAlertUser</b><br>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<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7)              | TRUE  |
| <b>dellIsDebugCommandAdmin</b><br>如果用户具有设备的调试命令管理员权限，则为 TRUE。                                                                | 1.2.840.113556.1.8000.1280.1.1.2.11<br>布尔值 (LDAPTYPE_BOOLEAN<br>1.3.6.1.4.1.1466.115.121.1.7)              | TRUE  |
| <b>dellSchemaVersion</b><br>当前架构版本用于更新架构。                                                                                    | 1.2.840.113556.1.8000.1280.1.1.2.12<br>不区分大小写的字符串<br>(LDAPTYPE_CASEIGNORESTRING<br>1.2.840.113556.1.4.905) | TRUE  |
| <b>dellRacType</b><br>此属性是 dellIDRACDevice 对象的"当前 RAC 类型"以及到 dellAssociationObjectMembers 前进链接的后退链接。                         | 1.2.840.113556.1.8000.1280.1.1.2.13<br>不区分大小写的字符串<br>(LDAPTYPE_CASEIGNORESTRING<br>1.2.840.113556.1.4.905) | TRUE  |
| <b>dellAssociationMembers</b><br>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。<br>链接 ID: 12071 | 1.2.840.113556.1.8000.1280.1.1.2.14<br>可分辨名称 (LDAPTYPE_DN<br>1.3.6.1.4.1.1466.115.121.1.12)                | FALSE |

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

扩展 Active Directory 中的架构时，还必须扩展 Active Directory 用户和计算机管理单元，以使管理员能够管理 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 Systems Management 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**。

此时 MMC 会出现。

2. 在“**Console 1**”（**控制台 1**）窗口中单击“**File**”（**文件**）（或“**Console**”（**控制台**），如果是运行 Windows 2000 的系统）。
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。要添加每个对象类型，请执行以下过程：

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

- 1 配置关联对象

## 创建 iDRAC 设备对象

1. 在"MMC Console Root" (MMC 控制台根目录) 窗口中, 右击一个容器。
2. 选择"New" (新建) → "Dell Remote Management Object Advanced" (Dell 高级远程管理对象)。  
系统将显示"New Object" (新对象) 窗口。
3. 为新对象键入名称。该名称必须与准备在[通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC6](#)的步骤 A 中键入的 iDRAC 名称相同。
4. 选择 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, 右击一个容器。
2. 选择"New" (新建) → "Dell Remote Management Object Advanced" (Dell 高级远程管理对象)。  
系统将显示"New Object" (新对象) 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, 右击一个容器。
2. 选择"New" (新建) → "Dell Remote Management Object Advanced" (Dell 高级远程管理对象)。  
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)。

## 通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC6

1. 打开一个支持的 Web 浏览窗口。
2. 登录到 iDRAC6 的 Web 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" (上传 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" (上传)。

将显示上传的 Active Directory CA 证书的证书信息。

9. 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)。
10. 单击"Enable Active Directory" (启用 Active Directory)。
11. 单击"Add" (添加) 以输入用户域名。

- 在提示符处输入用户名并单击“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。
- 键入**超时**时间（以秒为单位），指定 iDRAC6 等待 Active Directory 响应的的时间。默认设置为 120 秒钟。
- 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：** 如果您启用证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的“Subject”（主题）或“Subject Alternative Name”（主题替代名称）字段相符。

- 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）。
- 在“Schema Selection”（架构选择）下，单击“Extended Schema”（扩展架构）。
- 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）。
- 在“Extended Schema Settings”（扩展架构设置）下，键入 iDRAC 名称和域名以配置 iDRAC 设备对象。iDRAC 域名是创建 iDRAC 对象所在的域的域名。
- 单击“Finish”（完成）以保存 Active Directory 扩展架构设置。

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

- 单击“Test Settings”（检测设置）以检查 Active Directory 扩展架构设置。
- 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[“测试您的配置”](#)。

 **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。导航至“Remote Access”（远程访问）→“Configuration”（配置）→“Network”（网络）页面手动配置 DNS 服务器或使用 DHCP 获得 DNS 服务器。

您已完成 Active Directory 配置，架构已扩展。

## 通过扩展架构使用 RACADM 配置 Active Directory

使用以下命令，通过 RACADM CLI 工具而不是 Web 界面配置采用扩展架构的 iDRAC Active Directory 功能。

- 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。选择扩展架构选项时，这些地址是此 iDRAC 设备所在的域控制器的 FQDN 或 IP 地址。扩展架构模式完全不使用全局编录服务器。

 **注：** 如果您启用证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的“Subject”（主题）或“Subject Alternative Name”（主题替代名称）字段相符。

如果要禁用 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

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

在此情况下，您无需上传 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 命令上传 CA 证书：

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

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

以下 RACADM 命令可选。有关其它信息，请参阅“[导入 iDRAC6 固件 SSL 认证](#)”。

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

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 Web 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。

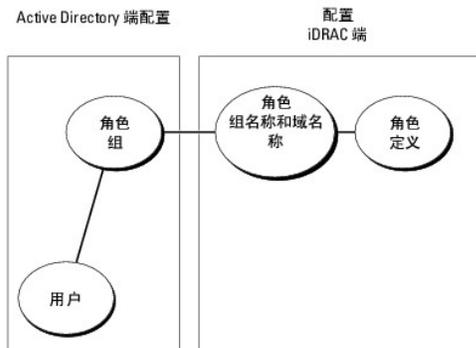
请参阅“[使用 Active Directory 登录到 iDRAC6](#)”了解关于用户域的详情。

5. 按 **Enter** 键完成扩展架构的 Active Directory 配置。

## 标准架构 Active Directory 概述

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

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



在 Active Directory 端，标准组对象用作角色组。具有 iDRAC6 权限的用户将是该角色组的成员。为了授予该用户对特定 iDRAC6 的权限，需要在特定 iDRAC6 上配置角色组名称及其域名。与扩展架构解决方案不同，角色和权限级别在各个 iDRAC6 上定义，而不是在 Active Directory 中定义。每个 iDRAC 中可配置和定义多达五个角色组。[表 7-9](#) 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 | 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 | 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   | 只读     | "Login to iDRAC" (登录到 iDRAC)                                                                                                                                                                                                                                                             | 0x00000001 |

|       |   |        |            |
|-------|---|--------|------------|
| 3     |   |        |            |
| 角色组 4 | 无 | 没有分配权限 | 0x00000000 |
| 角色组 5 | 无 | 没有分配权限 | 0x00000000 |

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

## 单域和多域情况

如果所有登录用户和角色组以及嵌套组都在相同域中，则只须在 iDRAC6 上配置域控制器地址。在此单域情况下，支持所有组类型。

如果所有登录用户和角色组以及嵌套组来自多个域，则要求在 iDRAC6 上配置全局编录服务器地址。在此多域情况下，所有角色组和嵌套组（如有）必须为通用组类型。

## 配置标准架构 Active Directory 访问 iDRAC

在 Active Directory 用户可以访问 iDRAC6 前，必须执行下列步骤配置 Active Directory：

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 Web 界面或 RACADM 在 iDRAC6 上配置组名称和此域的名称（请参阅[“通过标准架构 Active Directory 使用 Web 界面配置 iDRAC6”](#)或[“通过标准架构使用 RACADM 配置 Active Directory”](#)）。
3. 添加作为 Active Directory 组成员访问 iDRAC 的 Active Directory 用户。

## 通过标准架构 Active Directory 使用 Web 界面配置 iDRAC6

1. 打开一个支持的 Web 浏览器窗口。
2. 登录到 iDRAC6 的 Web 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”（**上传 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”（**上传**）。

将显示上传的 Active Directory CA 证书的证书信息。

9. 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**）。
10. 单击“Enable Active Directory”（**启用 Active Directory**）。

11. 单击“Add”（添加）以输入用户名。
12. 在提示符处输入用户名并单击“OK”（确定）。
13. 键入超时时间（以秒为单位），指定 iDRAC6 等待 Active Directory 响应的的时间。默认设置为 120 秒钟。
14. 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：** 如果您启用证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的“Subject”（主题）或“Subject Alternative Name”（主题替代名称）字段相符。
15. 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）。
16. 在“Schema Selection”（架构选择）下，单击“Standard Schema”（标准架构）。
17. 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。
18. 在“Standard Schema Settings”（标准架构设置）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：** 如果您启用证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的“Subject”（主题）或“Subject Alternative Name”（主题替代名称）字段相符。

 **注：** 仅当用户帐户和角色组位于不同域中时，标准架构才需要全局编录服务器。而在此多域情况下，仅可使用通用组。
19. 在“Role Groups”（角色组）下，单击“Role Groups”（角色组）。
 

将出现“Step 4b of 4”（第 4b 步，共 4 步）页。
20. 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。
21. 指定“Role Group Domain”（角色组域），这是角色组的域。
22. 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。
23. 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。
24. 重复步骤 18 至 22 以配置其它角色组，或单击“Finish”（完成）以返回“Active Directory Configuration and Management”（Active Directory 配置和管理）页，该页显示了所有标准架构配置设置。
25. 单击“Test Settings”（检测设置）以检查 Active Directory 标准架构设置。
26. 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[测试您的配置](#)。

 **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。导航至“Remote Access”（远程访问）→“Configuration”（配置）→“Network”（网络）页面手动配置 DNS 服务器或使用 DHCP 获得 DNS 服务器。

您已完成标准架构的 Active Directory 配置。

## 通过标准架构使用 RACADM 配置 Active Directory

通过 RACADM CLI 而不是基于 Web 的界面，使用以下命令配置标准架构的 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：** 如果您启用证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的“Subject”（主题）或“Subject Alternative Name”（主题替代名称）字段相符。

 **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 会逐一尝试连接到各配置地址直到成功连接。对于标准架构来说，这些是用户帐户和角色组所在域控制器的地址。

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

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

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

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

 **注：** 如果您启用证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的“Subject”（主题）或“Subject Alternative Name”（主题替代名称）字段相符。

如果要禁用 SSL 握手过程中的证书验证，请键入以下 RACADM 命令：

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

在此情况下，无需上传认证机构 (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 命令上传 CA 证书：

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

以下 RACADM 命令可选。有关其它信息，请参阅“[导入 iDRAC6 固件 SSL 认证](#)”。

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

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。

---

## 测试您的配置

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**”（**测试设置**）。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。详细的测试日志将在结果页面底部显示。

如果任何步骤失败，请查看测试日志中的详情以识别问题和可能的解决方案。关于最常见的错误，请参阅[常见问题](#)。

若要修改设置，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。换句话说，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 认证，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 认证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，右击“Automatic Certificate Request Settings”（自动认证申请设置）并单击“Automatic Certificate Request”（自动认证申请）。
  - c. 在“Automatic Certificate Request Setup Wizard”（自动认证申请设置向导）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 系统上为“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”（认证）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”（认证）文件夹，展开“Personal”（个人）文件夹并单击“Certificates”（认证）文件夹。
11. 找到并右击根 CA 认证，选择“All Tasks”（所有任务）并单击“Export...”（导出...）
12. 在“Certificate Export Wizard”（认证导出向导）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）并保存认证至系统上的目录。
15. 将保存在 [步骤 14](#) 中的认证上载到 iDRAC。

要使用 RACADM 上载证书，请参阅[通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC6](#)或[通过标准架构使用 RACADM 配置 Active Directory](#)。

要使用基于 Web 的界面上载证书，请参阅[通过扩展架构 Active Directory 使用 Web 界面配置 iDRAC6](#)或[通过标准架构 Active Directory 使用 Web 界面配置 iDRAC6](#)。

## 导入 iDRAC6 固件 SSL 认证

 **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。

使用下面的程序将 iDRAC6 固件 SSL 认证导入到所有域控制器受信任的认证列表。

 **注：** 如果系统运行 Windows 2000，以下步骤可能不同。

 **注：** 如果 iDRAC 固件 SSL 认证是由公认的 CA 签署且该 CA 认证已经列入域控制器“Trusted Root Certification Authority”（受信任的根认证颁发机构）列表中，则无需执行本部分的步骤。

iDRAC SSL 认证就是用于 iDRAC Web Server 的认证。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 认证>
```

1. 在域控制器上，打开“MMC Console”（MMC 控制台）窗口并选择“Certificates”（认证）→“Trusted Root Certification Authorities”（受信任的根认证颁发机构）。
2. 右击“Certificates”（认证），选择“All Tasks”（所有任务）并单击“Import”（导入）。
3. 单击“Next”（下一步）并浏览查找找到 SSL 认证文件。
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。

如果已安装自己的认证，应确保签署您的认证的 CA 位于“Trusted Root Certification Authority”（可信根认证颁发机构）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 根据认证类型自动选择认证存储，或浏览到所选存储。
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：

- 1 基于 Web 的界面
- 1 远程 RACADM
- 1 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菜单中列出所有用户域供您选择。如果从下拉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。

---

## 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 Web 界面以拥有管理员权限的本地用户身份登录。导航到“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 子选项卡以返回到“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，直到检测用户通过验证步骤为止。

**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 (错误)：Can't contact LDAP server (不能联系 LDAP 服务器)，error:14090086:SSL routines:SSL3\_GET\_SERVER\_CERTIFICATE:certificate verify failed (证书验证失败)：Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC (请检查正确的认证机构 (CA) 证书是否已上传到 iDRAC)。另请检查 iDRAC 日期是否在证书有效期内，且 iDRAC 中配置的域控制器地址是否与目录服务器证书的主题相符。

可能出现了什么问题，我应该如何解决？

如果启用证书验证，则 iDRAC6 在与目录服务器建立 SSL 连接时会使用上传的 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替代名称不相符。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替代名称相符。
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. 禁用证书验证，如果您选择信任此域控制器且在 SSL 握手中无需证书验证。

我目前在多域环境中使用扩展架构，我该如何配置域控制器地址？

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

何时需要配置全局编录地址？

如果使用的是扩展架构，则不使用全局编录地址。

如果使用的是标准架构且用户和角色组来自不同的域，则必须配置全局编录地址。在此情况下，仅可使用通用组。

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

标准架构的查询方式是什么？

iDRAC6 先连接到所配置的域控制器地址，如果用户和角色组位于该域，将保存权限。

如果配置了全局编录地址，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。

在测试设置中，iDRAC6 进行 LDAP CONNECT 仅是为了找出问题，而不是对不安全的连接进行 LDAP BIND。

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。如果无证书验证，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) 页面底部单击"Test Settings" (检测设置)，从而诊断问题。然后，可以解决检测结果指明的具体问题。有关详情，请参阅"测试您的配置"。**

**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) 页面上的"Enable Active Directory" (启用 Active Directory) 框。
- b. 确保 iDRAC6 网络配置页面上的 DNS 设置正确。

- c. 如果启用了证书验证，请确保已将正确的 Active Directory 根 CA 证书上载到 iDRAC6。确保 iDRAC6 时间在 CA 证书的有效期内。
- d. 如果使用扩展架构，则确保 **iDRAC6 名称** 和 **iDRAC6 域名** 与 Active Directory 环境配置相符。

如果使用标准架构，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

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [在 iDRAC6 中配置 Smart Card 登录](#)
- [配置本地 iDRAC6 用户进行 Smart Card 登录](#)
- [为 Smart Card 登录配置 Active Directory 用户](#)
- [配置 Smart Card](#)
- [使用 Smart Card 登录 iDRAC6](#)
- [使用 Active Directory Smart Card 身份验证登录 iDRAC6](#)
- [对 iDRAC6 中的 Smart Card 登录进行故障排除](#)

iDRAC6 支持双重验证 (TFA) 功能，是通过启用 **Smart Card 登录** 实现。

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。

另一方面，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 **远程访问** → **配置** → **Smart Card**，然后 **选择启用**。

如果您：

- 1 **启用**或**随远程 Racadm 启用**后，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**启用**后，所有命令行界面 (CLI) 带外接口，比如 telnet、SSH、串行、远程 racadm 和 IPMI over LAN 都会禁用，因为这些服务只支持单重验证。  
选择**随远程 Racadm 启用**后，所有 CLI 带外接口，除远程 racadm 以外，都会禁用。

 **注：** Dell 建议 iDRAC6 管理员将**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 Smart Card 登录的**已启用**设置。另外，应确保启用 **Smart Card 登录**前完成 iDRAC6 本地用户配置和 / 或 Active Directory 配置。

- 1 **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，将提示您输入 Microsoft® Active Directory® 或本地登录用户名和密码，这是从 Web 界面的默认登录提示。
- 1 **启用 CRL 检查进行 Smart Card 登录**，会对从认证撤回表 (CRL) 分发服务器下载的用户 iDRAC 认证进行检查以在 CRL 中撤回。

 **注：** CRL 分发服务器列在用户的 Smart Card 认证中。

---

## 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。导航到 **Remote Access** → **"Configuration" (配置)** → **"Users" (用户)**。

不过，在用户可以使用 Smart Card 登录到 iDRAC6 前，必须将用户的 Smart Card 认证和可信认证机构 (CA) 认证上载到 iDRAC6。

## 导出 Smart Card 认证

可以通过使用卡管理软件 (CMS) 将 Smart Card 认证从 Smart Card 导出为 Base64 编码格式的文件来获得用户认证。通常可以从 Smart Card 供应商处获得 CMS。该编码文件应作为用户认证上载到 iDRAC6。颁发 Smart Card 用户认证的 **可信认证机构** 也应将 CA 认证导出为 Base64 编码格式的文件。应将此文件作为用户的可信 CA 认证进行上载。用 Smart Card 认证中组成 **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 认证中的用户基本名 (UPN) 大小写一致。

例如，如果已颁发给用户 Smart Card 认证，"sampleuser@domain.com"，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 认证到 iDRAC6，并启用 Active Directory 登录。请参阅 [将 iDRAC6 用于 Microsoft Active Directory](#) 详细了解如何设置 Active Directory 用户。

 **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。

可以从 Remote Access → "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                                                   | <ul style="list-style-type: none"><li>1 "Disabled" (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。</li><li>1 "Enabled" (启用) — 启用 Smart Card 登录。在进行完更改后，注销，插入 Smart Card 并接着单击"Login" (登录) 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、串行、远程 RACADM 和 IPMI over LAN。</li><li>1 "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。</li></ul> <p><b>注：</b> Smart Card 登录要求用适当的认证配置本地 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 用户认证。可以在"Users" (用户) → "User Main Menu" (用户主菜单) 页配置用户认证。</p> |
| "Enable CRL check for Smart Card Logon" (为 Smart Card 登录启用 CRL 检查) | <p>本检查仅供 Active Directory 登录用户使用。如果希望 iDRAC6 检查认证撤回表 (CRL) 撤回用户 Smart Card 认证，则选择此选项。</p> <p>在以下情况下，用户将无法登录：</p> <ul style="list-style-type: none"><li>1 用户认证在 CRL 文件中列为已撤回。</li><li>1 iDRAC6 无法与 CRL 分发服务器通讯。</li><li>1 iDRAC6 无法下载 CRL。</li></ul> <p><b>注：</b> 必须在"Configuration" (配置) → "Network" (网络) 页中正确配置 DNS 服务器的 IP 地址，检查才能成功。</p>                                                                                                                                                                                                                                                                                                                                       |

## 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：** 确保为用户启用 Smart Card 登录前完成 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 登录页会显示出来，提示插入 Smart Card。

2. 将 Smart Card 插入读取器并单击"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，如果未创建本地用户，则 iDRAC6 将提示输入用户 Active Directory 帐户的密码。

 **注：** 如果是已选中**启用 CRL 检查进行 Smart Card 登录**的 Active Directory 用户，iDRAC6 会尝试下载 CRL 并检查用户认证的 CRL。如果认证在 CRL 中列为已撤回或由于某些原因不能下载 CRL，则通过 Active Directory 的登录会失败。

您已登录 iDRAC6。

---

## 使用 Active Directory Smart Card 身份验证登录 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 登录页面会显示出来，提示插入 Smart Card。

2. 插入 Smart Card 并单击“Login”（**登录**）。

PIN 弹出对话框将会显示。

3. 输入 PIN，并单击“OK”（**确定**）。

4. 输入用户的 Active Directory 密码验证 Smart Card，然后单击**确定**。

将会使用跟 Active Directory 中设置一样的凭据让用户登录 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 读取器

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：作为常规检查查看是否 Smart Card CSP 位于特定客户机上，在出现 Windows 登录 (Ctrl-Alt-Del) 屏幕时将 Smart Card 插入读取器并查看 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 是否因为太多次数不正确 PIN 尝试而已锁定。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 的用户名和用户认证是否已经过期。iDRAC6 跟踪日志可能会提供有关错误的重要日志消息；尽管有时由于安全考虑，错误消息可能会有意不太明确。

### 无法作为 Active Directory 用户登录 iDRAC6

如果无法作为 Active Directory 用户登录 iDRAC6，应尝试不启用 Smart Card 登录来登录 iDRAC6。如果已启用 CRL 检查，应尝试不启用 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消息。

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](#)

## 使用 GUI 控制台重定向

集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

- [概览](#)
- [使用控制台重定向](#)
- [使用 Video Viewer](#)
- [常见问题](#)

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，managed server 不会指示控制台已经重定向。

 **注：** 如果已经打开从管理站至 iDRAC6 的控制台重定向会话，则试图打开从同一管理站至此 iDRAC6 的新会话将激活现有的会话。不会生成新的会话。

 **注：** 多个控制台重定向会话可从单一的管理站同时打开至多个 iDRAC6 卡。

"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 managed server 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：

- 1 最高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。
- 1 从同一客户端控制台（管理站）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。
- 1 不应从受管系统上的 Web 浏览器启动控制台重定向会话。
- 1 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：

- 1 "[支持的 Web 浏览器](#)"
- 1 "[配置支持的 Web 浏览器](#)"

 **注：** Java 运行时间环境必须在管理站上安装，使控制台重定向功能工作。

2. 如果您使用 Internet Explorer，请确保浏览器能够下载下列加密内容：

- 1 转至 Internet Explorer 选项或设置，并选择 **工具**→ **Internet 选项**→ **高级**。
- 1 滚动至**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. 建议将显示器分辨率配置为 1280x1024 像素或更高。

 **注：** 如果有活动控制台重定向会话，并且 iDRAC KVM 连接了较低分辨率的显示器，在通过本地控制台选择服务器的情况下，可重设服务器控制台分辨率。如果服务器运行在 Linux 操作系统上，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 切换为文本控制台。

**注：** 有时可能遇到以下 Java 脚本编译错误：“预期的：；”。要解决此问题，请调整网络设置，使用 JavaWebStart 中的“直接连接”：“编辑->首选项->常规->网络设置”，并选择“直接连接”而非“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，应执行下列步骤：

1. 单击**系统**→**控制台 / 介质**→**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 9-1 说明控制台重定向的设置。
3. 完成后，单击“Apply”（应用）。
4. 单击相应按钮继续。请参阅表 9-2。

表 9-1. 控制台重定向配置属性

| 属性                                       | 说明                                                                                                                                                          |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 已启用                                      | 单击以启用或禁用“Console Redirection”（控制台重定向）。<br><b>选中</b> 表示“Console Redirection”（控制台重定向）已启用。<br><b>取消选中</b> 表示“Console Redirection”（控制台重定向）已禁用。<br><b>默认已启用。</b> |
| “Max Sessions”（最大会话）                     | 显示可能打开的控制台重定向会话的最大数目，1 至 4。使用下拉菜单更改允许的“Console Redirection”（控制台重定向）会话的最大允许数目。默认为 <b>2</b> 。                                                                 |
| “Active Sessions”（激活的会话）                 | 显示“Active Console”（活动控制台）会话数目。此字段为只读。                                                                                                                       |
| 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。默认为 <b>5900</b> 。                                                         |
| “Video Encryption Enabled”（视频加密已启用）      | <b>选中</b> 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。<br><b>取消选中</b> 表示视频加密已禁用。进入该视频端口的通信量均未加密。<br><b>默认为加密。禁用加密可以提高较慢网络上的性能。</b>                                           |
| “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 managed server 的本地显示器上看到。                                                 |

**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 9-2 中的按钮在**控制台 / 介质配置**页上可用。

表 9-2. 配置页按钮

| 按钮                    | 定义           |
|-----------------------|--------------|
| “Print”（打印）           | 打印此页         |
| “Refresh”（刷新）         | 重新载入配置页      |
| “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，会开启 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，应执行下列步骤：

1. 单击**系统**→**控制台 / 介质**→**配置**。
2. 使用表 9-3 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 9-3. Console Redirection（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)                     | 显示支持的最大控制台重定向会话数                                                                                |
| "Active Sessions" (激活的会话)                 | 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) | 如果本地控制台没有已禁用, 则没有选中。如果选中, 且本地 iDRAC KVM 连接当前处于远程使用, 任何人将无法访问控制台。                                |
| 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 9-4](#) 中的按钮可以在 [控制台重定向和虚拟介质](#) 页使用。

**表 9-4. 控制台重定向和虚拟介质 页按钮**

| 按钮                          | 定义                            |
|-----------------------------|-------------------------------|
| "Refresh" (刷新)              | 重载 <a href="#">控制台重定向配置</a> 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 <a href="#">控制台重定向配置</a> 页 |

- 如果控制台重定向会话可用, 则单击 "Launch Viewer" (启动查看器)。

 **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。

管理站连接到 iDRAC6, 在 iDRAC KVM Viewer 应用程序中显示远程系统的桌面。

- 两个鼠标光标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。您可通过选择 iDRAC KVM 菜单 **工具栏** 下的 **单光标** 选项更改为单光标。

## 使用 Video Viewer

Video Viewer 在 management station 和 managed server 之间提供了一个用户界面, 使用户能够从 management station 查看 managed server 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后, 将显示 **无信号** 的信息。

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。有关这些功能的更多详情, 请单击 **系统** → **控制台 / 媒介**, 并单击 [控制台重定向和虚拟介质](#) 页上的 **帮助**。

当您启动控制台重定向会话并出现 Video Viewer 时, 您可能需要同步鼠标指针。

## 禁用或启用本地服务器视频

您可使用 iDRAC6 Web 界面配置 iDRAC6 禁用 iDRAC KVM 连接。

如果想确定对受管服务器控制台有独占访问, 必须在 [控制台重定向配置](#) 页上禁用本地控制台并重新配置 **最大会话数** 为 1。

 **注:** 通过禁用 (关闭) 服务器上的本地视频, 将启用连接到 iDRAC KVM 的显示器、键盘和鼠标。

要禁用或启用本地控制台, 应执行以下程序:

- 在管理站上打开一个支持的 Web 浏览器并登录 iDRAC。有关详情, 请参阅 [访问 Web 界面](#)。
- 单击 **系统** → **控制台 / 媒介** → **配置**。
- 要禁用 (关闭) 服务器上的本地视频, 请取消选中 [配置](#) 页上的 **本地服务器视频已启用** 复选框, 然后单击 **应用**。默认值为 OFF。

 **注：** 如果开启本地服务器视频，将需 15 秒关闭。

- 要启用（打开）服务器上的本地视频，请选中配置页上的**本地服务器视频已启用**复选框，然后单击**应用**。

## 常见问题

表 9-5 列出常见问题和解答。

**表 9-5. 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？                                | 是。                                                                                                                                                                                                                                                                                     |
| 为什么要求关闭本地视频后需要 15 秒才能关闭服务器上的本地视频？                             | 使本地用户有机会在视频关闭前采取某些操作。                                                                                                                                                                                                                                                                  |
| 打开本地视频时有时间延迟吗？                                                | 没有，iDRAC 收到本地视频打开请求后，视频就立刻 <b>打开</b> 。                                                                                                                                                                                                                                                 |
| 本地用户还可以关闭视频吗？                                                 | 当本地控制台禁用时，本地用户不能打开视频。                                                                                                                                                                                                                                                                  |
| 本地用户还可以打开视频吗？                                                 | 当本地控制台禁用时，本地用户不能打开视频。                                                                                                                                                                                                                                                                  |
| 关闭本地视频是否也会关闭本地键盘和鼠标？                                          | 否。                                                                                                                                                                                                                                                                                     |
| 关闭本地控制台是否会关闭远程控制台会话上的视频？                                      | 不会，打开关闭本地视频与远程控制台会话无关。                                                                                                                                                                                                                                                                 |
| iDRAC 用户打开或关闭本地服务器视频需要什么权限？                                   | 任何具有 iDRAC 配置权限的用户都可以打开或关闭本地控制台。                                                                                                                                                                                                                                                       |
| 如何获得本地服务器视频的最新状况？                                             | 该状态显示在 iDRAC Web 界面的 <b>控制台重定向配置</b> 页上。<br><br>RACADM CLI 命令 <code>racadm getconfig @Cg cfgRacTuning</code> 在对象 <code>cfgRacTuneLocalServerVideo</code> 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 要求 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。<br><br>请确保在 iDRAC KVM 客户端上选择 iDRAC KVM 菜单 <b>工具栏</b> 下的 <b>单光标</b> 选项。                                                                                                                                                                                     |
| 为什么使用 iDRAC 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，将会收到一个 EMS 连接信息，需要您选择“OK”（ <b>确定</b> ）后才能继续。无法使用鼠标远程选择“OK”（ <b>确定</b> ）。必须要么在本地系统上选择“OK”（ <b>确定</b> ），要么重新启动远程 managed server，重新安装，然后在 BIOS 中关闭控制台重定向。<br><br>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，管理站上的 Num Lock 指示灯不需要与远程服务器上的 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 managed server，会收到警告消息吗？               | 否。如果本地用户访问系统，两人都有系统控制权。                                                                                                                                                                                                                                                                |
| 我需要多少带宽来运行控制台重定向会话？                                           | 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 运行控制台重定向的最低系统要求是多少？                        | 管理站要求 Intel® Pentium® III 500 MHz 处理器，且 RAM 至少为 256 MB。                                                                                                                                                                                                                                |
| 为什么我在 iDRAC KVM Video Viewer 上看到一个 <b>无信号</b> 信息？             | 您看到此信息可能因为 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 上看到一个 <b>超出范围</b> 信息？            | 您看到此信息可能因为捕获视频的的必要参数超出 iDRAC 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出范围状态。通常，参数范围的最大值由视频内存大小或带宽等物理限制设置。                                                                                                                                                                                           |

[目录](#)

## [目录](#)

### 集成 Dell™ Remote Access 控制器 6 (iDRAC6) 版本 1.0 用户指南

 **注：**“注”表示可以帮助您更好地使用计算机的重要信息。

 **小心：**“注意”表示如果不遵循说明，就有可能损坏硬件或导致数据丢失。

**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/或其它国家的商标或注册商标；Red Hat 和 Linux Red Hat, Inc. 在美国和其他国家的的注册商标；SUSE 是 Novell Corporation 的注册商标。Intel 和 Pentium 是 Intel Corporation 在美国和其它国家的注册商标；UNIX 是 The Open Group 在美国和其它国家的注册商标；VMware 是 VMware, Inc. 在美国 / 或其它管辖区的注册商标。

版权 1998-2006 The OpenLDAP Foundation. All rights reserved (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顶层目录中的 LICENSE 文件中，您可以在 [www.OpenLDAP.org/license.html](http://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资源的材料。有关 OpenLDAP 的信息可以从 [www.openldap.org/](http://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. All rights reserved (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 Halvard B. Furuseth. All rights reserved (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，需要保留此通告才行。在没有得到版权所有者优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，不帶任何明示或暗示的保证。部分版权 (c) 1992-1996 Regents of the University of Michigan. All rights reserved (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，不帶任何明示或暗示的保证。本说明文件中提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 3 月 修订 A00

---

## [目录](#)