Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

DRAC 5 概览
DRAC 5 使用入门
DRAC 5 的基本安装
DRAC 5 的高级配置
添加和配置 DRAC 5 用户
将 DRAC 5 用于 Microsoft Active Directory
配置 Smart Card 验证
启用 Kerberos 验证
使用 GUI 控制台重定向
使用并配置虚拟介质
配置安全功能
使用 DRAC 5 SM-CLP 命令行界面
监控和警报管理
配置智能平台管理接口 (IPMI)
对 Managed System 进行恢复和故障排除
恢复并故障排除 DRAC 5
传感器
RACADM 子命令概览
DRAC 5 属性数据库组和对象定义
支持的 RACADM 接口
词汇表

"注"和"注意"

注： "注"表示可以帮助您更好地使用计算机的重要信息。

注意： "注意"表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

"注"和"注意"

注： "注"表示可以帮助您更好地使用计算机的重要信息。

注意： "注意"表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

2008 年 7 月

本说明文件中的信息如有更改，恕不另行通知。
© 2008 Dell Inc. 版权所有，翻印必究。

目录

RACADM 子命令概览

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- help
- arp
- clearasrscreen
- config
- getconfig
- coredump
- coredumpdelete
- fwupdate
- getssninfo
- getsysinfo
- getractime
- ifconfig
- netstat
- ping
- setniccfg
- getniccfg
- getsvctag
- racdump
- racreset
- racresetcfg
- serveraction
- getraclog
- clrraclog
- getsel
- clrsel
- gettracelog
- sslcsrgen
- sslcertupload
- sslcertdownload
- sslcertview
- sslkeyupload
- krbkeytabupload
- 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 DRAC 5”（登录 DRAC 5）**权限。

表 A-1 说明了 **help** 命令。

表 A-1。 Help 命令

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

提要

```
racadm help
```

```
racadm help <子命令>
```

说明

help 子命令列出了可以同 **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

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

---

arp

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

表 A-2 说明了 **arp** 命令。

表 A-2。 arp 命令

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

提要

```
racadm arp
```

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

clearasrscreen

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

表 A-3 说明了 **clearasrscreen** 子命令。

表 A-3。 clearasrscreen

子命令	定义
clearasrscreen	清除内存中的上次崩溃屏幕。

提要

```
racadm clearasrscreen
```

支持的接口

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

---

config

注： 要使用 **getconfig** 命令，必须具有 **“Log In DRAC 5”（登录 DRAC 5）**权限。

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

表 A-4。 config/getconfig

子命令	定义
config	配置 DRAC 5。
getconfig	获取 DRAC 5 配置数据。

提要

```
racadm config [-c|-p] -f <文件名>
```

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

支持的接口

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

说明

config 子命令允许用户分别设置 DRAC 5 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 DRAC 5 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 DRAC 5。该文件必须包含在“分析规则”中所指定格式的数据。

-p	**-p**，或密码选项，指示 **config** 在配置完成后删除 config 文件 **-f <*文件名*>** 中包含的密码条目。
-g	**-g <*组名*>**（即组选项）必须与 **-o** 选项配合使用。<*组名*> 用于指定包含要设置的对象的组。
-o	**-o <*对象名*> <*值*>**（即对象选项）必须与 **-g** 选项配合使用。此选项指定与字符**串** <*值*>写在一起的对象名。
-i	**-i <*索引*>**（即索引选项）只对索引组有效并且可用于指定唯一组。<*索引*> 是从 1 至 16 的十进制整数。在此处该索引由索引值指定，而不由“命名的”值指定。
-c	**-c**，或检查选项，与 **config** 子命令配合使用，并使用户可以分析 **.cfg** 文件以查找语法错误。如果找到错误，则显示行号和简短的错误说明。不会对 DRAC 5 执行写入操作。此选项只是一种检查。

输出

此子命令将在出现以下任一情况时生成错误输出：

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

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

示例

- racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100

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

- racadm config -f myrac.cfg

  配置或重新配置 DRAC 5。**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 DRAC 5 配置参数，或者检索所有 RAC 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 RAC 配置写入配置文件。此文件可用于通过 **config** 子命令进行批配置操作。 **注：** **-f** 选项不会为 **cfgIpmiPet** 和 **cfgIpmiPef** 组创建条目。必须至少设置一个陷阱目标以将 **cfgIpmiPet** 组捕获到文件中。
-g	**-g <*组名*>**（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：

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

如果没有遇到错误，此子命令将显示指定配置的内容。

示例

- racadm getconfig -g cfgLanNetworking

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

- racadm getconfig -f myrac.cfg

  将所有组配置对象从 RAC 保存到 **myrac.cfg**。

- racadm getconfig -h

  显示 DRAC 5 上可用配置组的列表。

- racadm getconfig -u root

  显示用户命名为 root 的配置属性。

- racadm getconfig -g cfgUserAdmin -i 2 -v

  显示索引 2 处的用户组实例，并提供属性值的详细信息。

提要

racadm getconfig -f <*文件名*>

racadm getconfig -g <*组名*> [-i <*索引*>]

racadm getconfig -u <*用户名*>

racadm getconfig -h

支持的接口

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

---

coredump

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

表 A-7 说明了 **coredump** 子命令。

表 A-7。 coredump

子命令	定义
coredump	显示最后一次 DRAC 5 内核转储。

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 RAC 关机后再开机过程中都保持不变，并且只有在出现以下某种情况时才会清除：

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

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

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

coredumpdelete

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

表 A-8 说明了 **coredumpdelete** 子命令。

表 A-8。 coredumpdelete

子命令	定义
coredumpdelete	删除 DRAC 5 中存储的内核转储。

提要

```
racadm coredumpdelete
```

说明

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

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

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

支持的接口

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

---

fwupdate

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

注： 开始固件更新前，请参阅 "启动文本控制台" 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
fwupdate	更新 DRAC 5 上的固件。

提要

```
racadm fwupdate -s
```

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

```
racadm fwupdate -p -u -d <路径>
```

说明

fwupdate 子命令使用户能够更新 DRAC 5 上的固件。用户可以：

- 检查固件更新进程状况

- 通过提供 IP 地址和可选路径从 TFTP 服务器更新 DRAC 5 固件
- 使用本地 RACADM 从本地文件系统更新 DRAC 5 固件

支持的接口

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

输入

表 A-10 说明了 **fwupdate** 子命令选项。

注： **-p** 选项只在本地 RACADM 中受支持，并且不受 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，DRAC 5 会执行软重设。
-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**，或**目录**，选项指定固件更新文件在 TFTP 服务器或 DRAC 5 主服务器上所在的目录。
-p	**-p**，或**放置**，选项可用于从 Managed System 向 DRAC 5 更新固件文件。**-u** 选项必须与 **-p** 选项配合使用。

输出

显示信息，表明正在执行的操作。

示例

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

  在本示例中，**-g** 选项告诉固件从 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。完成后，DRAC 5 将会重设。

  如果下载超过 15 分钟并且超时，则将固件闪速更新映像传输到服务器上的本地驱动器。然后，使用控制台重定向，连接到远程系统并使用本地 racadm 本地安装固件。

- `racadm fwupdate -s`

  此选项将读取固件更新的当前状况。

- `racadm fwupdate -p -u -d c:\ <映像>`

  在本示例中，由主机的文件系统来提供更新的固件映像。

- `racadm -r 192.168.0.120 -u root -p racpassword fwupdate -g -u -a 192.168.0.120 -d <映像>`

  在本示例中，RACADM 用于使用提供的 DRAC 用户名和密码远程更新指定 DRAC 的固件。此映像从 TFTP 服务器中检索。

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 DRAC 5”（登录 DRAC 5）**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 DRAC 的用户的列表。摘要信息提供了以下信息：

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

支持的接口

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

输入

表 A-12 说明了 **getssninfo** 子命令选项。

表 A-12。 getssninfo 子命令选项

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

示例

- racadm getssninfo

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

表 A-13。 getssninfo 子命令输出示例

用户	IP 地址	类型	控制台
root	192.168.0.10	Telnet	Virtual KVM

```
racadm getssninfo -A

"root" 143.166.174.19 "Telnet" "NONE"

racadm getssninfo -A -u *

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

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

---

getsysinfo

注： 要使用此命令，必须具有 **“Log In To DRAC 5”（登录 DRAC 5）**权限。

表 A-14 说明了 **racadm getsysinfo** 子命令。

表 A-14。 getsysinfo

命令	定义
getsysinfo	显示 DRAC 5 信息、系统信息和监督状况信息。

提要

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

说明

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

支持的接口

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

输入

表 A-15 说明了 **getsysinfo** 子命令选项。

表 A-15。 getsysinfo 子命令选项

选项	说明
-d	显示 DRAC 5 信息
-s	显示系统信息
-w	显示监督信息
-A	消除打印页眉/标签。

如果没有指定 **-w** 选项，则使用其它选项作为默认值。

输出

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

示例输出

```
RAC Information（RAC 信息）：
RAC Date/Time（RAC 日期/时间）= Thu Dec 8 20:01:33 2005
Firmware Version（固件版本）= 1.0
Firmware Build（固件构建）= 05.12.08
Last Firmware Update（上次固件更新）= Thu Dec 8 08:09:36 2005


Hardware Version（硬件版本）= A00
Current IP Address（当前 IP 地址）= 192.168.0.120
Current IP Gateway（当前 IP 网关）= 192.168.0.1
Current IP Netmask（当前 IP 网络掩码）= 255.255.255.0
DHCP Enabled（DHCP 已启用）= 0
MAC Address（MAC 地址）= 00:14:22:18:cd:f9
Current DNS Server 1（当前 DNS 服务器 1）= 0.0.0.0
Current DNS Server 2（当前 DNS 服务器 2）= 0.0.0.0
DNS Servers from DHCP（来自 DHCP 的 DNS 服务器）= 0
Register DNS RAC Name（注册 DNS RAC 名称）= 0
DNS RAC Name（DNS RAC 名称）= rac-48192
Current DNS Domain（当前 DNS 域）=


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


Watchdog information（监护程序信息）
Recovery Action（恢复操作）= None
Present countdown value（当前倒计数值）= 0 seconds
Initial countdown value（初始倒计数值）= 0 seconds
```

示例

```
racadm getsysinfo -A -s


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


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

```
racadm getsysinfo -w -s
```

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



Watchdog information（监护程序信息）
Recovery Action（恢复操作）= None
Present countdown value（当前倒计数值）= 0 seconds
Initial countdown value（初始倒计数值）= 0 seconds
```

限制

只有 Managed System 上装有 Dell OpenManage 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 DRAC 5”（登录 DRAC 5）**权限。

表 A-16 说明了 **getractime** 子命令。

表 A-16。 getractime

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

提要

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

说明

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

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

输出

getractime 子命令将输出显示在一行上。

示例输出

```
racadm getractime

Thu Dec 8 20:15:26 2005


racadm getractime -d

20051208201542.000000
```

支持的接口

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

---

ifconfig

注： 要使用此命令，必须具有“**Execute Diagnostic Commands**”（**执行诊断命令**）或“**Configure DRAC 5**”（**配置 DRAC 5**）权限。

表 A-17 说明了 **ifconfig** 子命令。

表 A-17。 ifconfig

子命令	定义
ifconfig	显示网络接口表的内容。

提要

```
racadm ifconfig
```

---

netstat

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

表 A-18 说明了 **netstat** 子命令。

表 A-18。 netstat

子命令	定义
netstat	显示路径选择表和当前连接。

提要

```
racadm netstat
```

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

ping

注： 要使用此命令，必须具有 **“Execute Diagnostic Commands”（执行诊断命令）**或 **“Configure DRAC 5”（配置 DRAC 5）**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选择表的内容从 DRAC 5 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

- 远程 RACADM
- telnet/ssh/serial RACADM

---

setniccfg

注： 要使用 **setniccfg** 命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**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 -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 子命令设置控制器 IP 地址。

- **-d** 选项为以太网管理端口启用 DHCP（默认是启用 DHCP）。
- **-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*>必须键入为圆点分隔的字符串。

  ```
  racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
  ```
- **-o** 选项完全禁用以太网管理端口。<*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

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

---

getniccfg

注： 要使用 **getniccfg** 命令，必须具有 **“Log In To DRAC 5”（登录 DRAC 5）**权限。

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

表 A-21。 setniccfg/getniccfg

子命令	定义
getniccfg	显示控制器的当前 IP 配置。

提要

```
racadm getniccfg
```

说明

getniccfg 子命令显示当前以太网管理端口设置。

示例输出

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

```
NIC Enabled（NIC 已启用） = 1

DHCP Enabled（DHCP 已启用） = 1

IP Address（IP 地址） = 192.168.0.1

Subnet Mask（子网掩码） = 255.255.255.0

Gateway（网关） = 192.168.0.1
```

支持的接口

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

---

getsvctag

注： 要使用此命令，必须具有**“Log In To DRAC 5”（登录 DRAC 5）**权限。

表 A-22 说明了 **getsvctag** 子命令。

表 A-22。 getsvctag

子命令	定义
getsvctag	显示服务标签。

提要

```
racadm getsvctag
```

说明

getsvctag 子命令显示主机系统的服务标签。

示例

在命令提示符下键入 getsvctag。输出显示如下：

```
Y76TP0G
```

命令在成功时返回 0，在错误时返回非零值。

支持的接口

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

---

racdump

注： 要使用此命令，必须具有“**Debug**”（**调试**）权限。

表 A-23 说明了 **racdump** 子命令。

表 A-23。 racdump

子命令	定义
racdump	显示状况和一般 DRAC 5 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、状况和常规 DRAC 5 板信息。

运行 **racdump** 子命令时会显示以下信息：

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

支持的接口

- 远程 RACADM
- telnet/ssh/serial RACADM

---

racreset

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-24 说明了 **racreset** 子命令。

表 A-24。 racreset

子命令	定义
racreset	重设 DRAC 5。

注意： 发出 racreset 子命令后，DRAC 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 DRAC 5 的重设。重设事件会写入 DRAC 5 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。

注意： 在执行表 A-25 中说明的 DRAC 5 硬重设后必须重新引导系统。

表 A-25 说明了 **racreset** 子命令选项。

表 A-25。 racreset 子命令选项

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

示例

- `racadm racreset`

  启动 DRAC 5 软重设序列。

- `racadm racreset hard`

  启动 DRAC 5 硬重设序列。

支持的接口

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

racresetcfg

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-26 说明了 **racresetcfg** 子命令。

表 A-26。 racresetcfg

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

提要

```
racadm racresetcfg
```

支持的接口

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

说明

racresetcfg 命令将删除所有已由用户配置的数据库属性条目。数据库具有所有条目的默认属性，这些属性用于将插卡恢复为原始默认设置。重设数据库属性后，DRAC 5 会自动重设。

注意： 此命令会删除当前 RAC 配置并将 RAC 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： 此子命令还会将串行接口重设为默认波特率 (57600) 和 COM 端口。可能需要通过 BIOS 设置屏幕为服务器重新配置串行设置以通过串行端口访问 RAC。

---

serveraction

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

表 A-27 说明了 **serveraction** 子命令。

表 A-27。 serveraction

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

提要

```
racadm serveraction <操作>
```

说明

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

表 A-28。 serveraction 子命令选项

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

输出

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

支持的接口

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

---

getraclog

注： 要使用此命令，必须具有 **“Log In DRAC 5”（登录 DRAC 5）**权限。

表 A-29 说明了 **racadm getraclog** 命令。

表 A-29。 getraclog

命令	定义
getraclog -i	显示 DRAC 5 日志中的条目数。
getraclog	显示 DRAC 5 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 DRAC 5 日志中的条目数。

以下选项允许 **getraclog** 命令读取条目：

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

注： 如果没有提供选项，将显示整个日志。

输出

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

示例输出

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

支持的接口

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

---

clrraclog

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

提要

```
racadm clrraclog
```

说明

clrraclog 子命令会从 RAC 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 DRAC 5”（登录 DRAC 5）**权限。

表 A-30 说明了 **getsel** 命令。

表 A-30。 getsel

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

提要

```
racadm getsel -i
```

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

说明

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

支持的接口

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

---

clrsel

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

提要

```
racadm clrsel
```

说明

clrsel 命令会从系统事件日志 (SEL) 删除全部现有的记录。

支持的接口

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

---

gettracelog

注： 要使用此命令，必须具有 **“Log In To DRAC 5”（登录 DRAC 5）**权限。

表 A-31 说明了 **gettracelog** 子命令。

表 A-31。 gettracelog

命令	定义
gettracelog -i	显示 DRAC 5 跟踪日志中的条目数。
gettracelog	显示 DRAC 5 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 DRAC 5 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（记录）: 1

Date/Time（日期/时间）: Dec 8 08:21:30

Source（源）: ssnmgrd[175]

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

支持的接口

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

---

sslcsrgen

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**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 可用来创建自定义 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
-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：

- CSR 成功生成。
- CSR 不存在。
- CSR 生成正在进行。

限制

sslcsrgen 子命令只能从本地或远程 RACADM 客户端执行并且不能用在串行、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

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

---

sslcertupload

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-34 说明了 **sslcertupload** 子命令。

表 A-34。 sslcertupload

子命令	说明
sslcertupload	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 **sslcertupload** 子命令选项。

表 A-35。 sslcertupload 子命令选项

选项	说明
-t	指定要上载的认证类型，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 **sslcert** 文件。

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

限制

sslcertupload 子命令只能从本地或远程 RACADM 客户端执行。**sslcsrgen** 子命令不能用在串行、远程登录或 SSH 接口中。

示例

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

支持的接口

- 本地 Racadm：
- 远程 RACADM

---

sslcertdownload

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-36 说明了 **sslcertdownload** 子命令。

表 A-36。 sslcertdownload

子命令	说明
sslcertupload	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-37 说明了 **sslcertdownload** 子命令选项。

表 A-37。 sslcertdownload 子命令选项

选项	说明
-t	指定要下载的认证类型，Microsoft® Active Directory® 认证或服务器认证。 1 = 服务器认证 2 = Microsoft Active Directory 认证
-f	指定要上载的认证文件名。如果没有指定 **-f** 选项或文件名，将会选择当前目录中的 **sslcert** 文件。

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

限制

sslcertdownload 子命令只能从本地或远程 RACADM 客户端执行。**sslcsrgen** 子命令不能用在串行、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

- 本地 Racadm：
- 远程 RACADM

---

sslcertview

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-38 说明了 **sslcertview** 子命令。

表 A-38。 sslcertview

子命令	说明
sslcertview	显示 RAC 上存在的 SSL 服务器或 CA 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
-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（序列号） : 00


Subject Information（主题信息）
Country Code (CC)（国家/地区代码）: US
State (S)（州/省 [S]）: Texas
Locality (L)（地区）: Round Rock
Organization (O)（组织）: Dell Inc.
Organizational Unit (OU)（组织单位）: Remote Access Group
```

```
Common Name (CN)（常用名）: DRAC5 default certificate


Issuer Information（颁发者信息）:
Country Code (CC)（国家/地区代码）: US
State (S)（州/省 [S]）: Texas
Locality (L)（地区）: Round Rock
Organization (O)（组织）: Dell Inc.
Organizational Unit (OU)（组织单位）: Remote Access Group
Common Name (CN)（常用名）: DRAC5 default certificate


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


racadm sslcertview -t 1 -A



00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

支持的接口

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

---

sslkeyupload

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-40 说明了 **sslkeyupload** 子命令。

表 A-40。 sslkeyupload

子命令	说明
sslkeyupload	将 SSL 密钥从客户端上载到 DRAC 5。

提要

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

选项

表 A-41 说明了 **sslkeyupload** 子命令选项。

表 A-41。 sslkeyupload 子命令选项

选项	说明
-t	指定要上载的密钥。 1 = 服务器认证
-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 **sslcert** 文件。

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。**sslcsrgen** 子命令不能用在串行、远程登录或 SSH 接口中。

示例

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

支持的接口

- 本地 Racadm：
- 远程 RACADM

---

krbkeytabupload

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-42 说明了 **krbkeytabupload** 子命令。

表 A-42。 kerbkeytabupload

子命令	说明
krbkeytabupload	上载 Kerberos keytab 文件。

提要

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

选项

表 A-43 说明了 **krbkeytabupload** 子命令选项。

表 A-43。 krbkeytabupload 子命令选项

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

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

限制

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

示例

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

支持的接口

- 本地 Racadm：
- 远程 RACADM

---

testemail

表 A-44 说明了 **testemail** 子命令。

表 A-44。 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 RAC 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-45 提供了 **cfgEmailAlert** 组的列表和相关命令。

表 A-45。 testemail 配置

措施	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 cfgRhostsSmptServerIpAddr -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-46 说明了 **testemail** 子命令选项。

表 A-46。 testemail 子命令

选项	说明
-i	指定要检测的电子邮件警报的索引。

输出

无。

支持的接口

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

---

testtrap

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

表 A-47 说明了 **testtrap** 子命令。

表 A-47。 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 RAC 向网络上的指定目标陷阱侦听程序发送检测陷阱来检测 RAC 的 SNMP 陷阱警报功能。

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

表 A-48 提供了**cfgIpmiPet** 组的列表和相关命令。

表 A-48。 cfgEmailAlert 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-49 说明了 **testtrap** 子命令选项。

表 A-49。 testtrap 子命令选项

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

支持的接口

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

---

vmdisconnect

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

表 A-50 说明了 vmdisconnect 子命令。

表 A-50。 vmdisconnect

子命令	说明
vmdisconnect	关闭所有来自远程客户端的现有 RAC 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 RAC 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 RAC 基于 Web 的界面中显示活动虚拟介质会话。

支持的接口

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

---

vmkey

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

表 A-51 说明了 vmkey 子命令。

表 A-51。 vmkey

子命令	说明
vmkey	执行虚拟介质密钥相关的操作。

提要

```
racadm vmkey <操作>
```

如果 <*操作*> 配置为 reset，虚拟闪速更新内存就会重设为默认大小 16 MB。

说明

将自定义虚拟介质密钥映像上载到 RAC 后，密钥大小就会变为映像大小。vmkey 子命令可用于将密钥重设回初始默认大小，在 DRAC 5 上为 16 MB。

支持的接口

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

---

usercertupload

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-52 说明了 **usercertupload** 子命令。

表 A-52。 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 DRAC。

提要

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

选项

表 A-53 说明了 **usercertupload** 子命令选项。

表 A-53。 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。 1 = 用户认证 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 **sslcert** 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

- 本地 Racadm：
- 远程 RACADM

---

usercertview

注： 要使用此命令，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

表 A-54 说明了 **usercertview** 子命令。

表 A-54。 usercertview

子命令	说明
usercertview	显示 DRAC 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-55 说明了 **sslcertview** 子命令选项。

表 A-55。 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。 1 = 用户认证 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

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

---

localConRedirDisable

注： 只有本地 racadm 用户可以执行此命令。

表 A-56 说明了 localConRedirDisable 子命令。

表 A-56。 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。

支持的接口

- 本地 Racadm：

目录

目录

DRAC 5 属性数据库组和对象定义

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 可显示字符
- idRacInfo
- cfgLanNetworking
- cfgRemoteHosts
- cfgUserAdmin
- cfgEmailAlert
- cfgSessionManagement
- cfgSerial
- cfgNetTuning
- cfgOobSnmp
- cfgRacTuning
- ifcRacManagedNodeOs
- cfgRacSecurity
- cfgRacVirtual
- cfgActiveDirectory
- cfgStandardSchema
- cfgIpmiSerial
- cfgIpmiSol
- cfgIpmiLan
- cfgIpmiPef
- cfgIpmiPet

DRAC 5 属性数据库包含 DRAC 5 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 DRAC 5。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：

```
abcdefghijklmnopqrstuvwxwz
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

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

---

idRacInfo

该组包含显示参数以提供有关所查询 DRAC 5 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

"Dell Remote Access Controller 5"

说明

使用文本字符串标识产品。

idRacDescriptionInfo（只读）

有效值

字符串，最多 255 个 ASCII 字符。

默认值

"This system component provides a complete set of remote management functions for Dell PowerEdge servers."（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

DRAC 5

说明

用户指定用于标识此控制器的名称。

idRacType（只读）

默认值

6

说明

将 Remote Access Controller 类型标识为 DRAC 5。

---

cfgLanNetworking

该组包含的参数用于配置 DRAC 5 NIC。

该组允许有一个实例。对该组中对象的所有更改/更新都需要重设 DRAC 5 NIC，这会导致短暂的连接中断。更改 DRAC 5 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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

指定 RAC DNS 域名应从网络 DHCP 服务器分配。

cfgDNSDomainName（读/写）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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

“”

说明

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

cfgDNSRacName（读/写）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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

cfgDNSRegisterRac（读 / 写）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

在 DNS 服务器上注册 DRAC 5 名称。

cfgDNSServersFromDHCP（读 / 写）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

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

cfgNicIpAddress（读 / 写）

注： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。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

192.168.0.120

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： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。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 RAC 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： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。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）

注： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

指定是否使用 DHCP 分配 RAC 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 RAC 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。

注： 如果远程更新系统，则使用**setniccfg** 命令。

cfgNicSelection（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0（共享）

1（与故障转移共享）

2（专用）

默认值

2

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。
与故障转移共享	启用主机服务器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。

cfgNicMacAddress（只读）

有效值

表示 RAC NIC MAC 地址的字符串。

默认值

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

说明

RAC NIC MAC 地址。

cfgNicVLanEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0 ®C 4094

默认值

0

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

---

cfgRemoteHosts

此组提供了用于配置各种远程组件的属性，其中包括用于电子邮件警报的 SMTP 服务器和用于固件更新的 TFTP 服务器 IP 地址。

cfgRhostsSmtpServerIpAddr（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

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

默认值

0.0.0.0

说明

网络 SMTP 服务器的 IP 地址。如果已配置并启用了警报，SMTP 服务器会从 RAC 发送电子邮件警报。

cfgRhostsFwUpdateTftpEnable（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用从网络 TFTP 服务器进行 RAC 固件更新。

cfgRhostsFwUpdateIpAddr（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

表示有效 TFTP 服务器 IP 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 RAC 固件更新操作的网络 TFTP 服务器 IP 地址。

cfgRhostsFwUpdatePath（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 255。

默认值

“”

说明

指定 RAC 固件映像文件在 TFTP 服务器上的 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**）。

---

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）

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

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。

cfgUserAdminIpmiSerialPrivilege（读/写）

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

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 串行信道上的最大权限。

cfgUserAdminPrivilege（读/写）

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

有效值

0x0000000 至 0x00001ff 和 0x0

默认值

0x0000000

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 说明允许的用户权限的位掩码。

表 B-2。 用户权限位掩码

用户权限	权限位掩码
登录 DRAC 5	0x0000001
配置 DRAC 5	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 RAC。	0x00000000
用户只能登录到 RAC 并查看 RAC 和服务器配置信息。	0x00000001
用户可以登录到 RAC 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

cfgUserAdminUserName（读/写）

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

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。字符串不能包含“/”（正斜杠）、“\”（反斜杠）、“.”（句点）、“@”（AT 符号）或引号。

注： 此属性值必须不同于其它用户实例。

cfgUserAdminPassword（只写）

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

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

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

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用一个用户。

cfgUserAdminSolEnable

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

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®C4

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（只读）

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（只读）

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 DRAC 5 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 2

默认值

2

说明

指定 RAC 上允许的最大控制台重定向会话数。

cfgSsnMgtRacadmTimeout（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

10 ®C1920

默认值

30

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。

cfgSsnMgtWebserverTimeout（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

60 ®C 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0（无超时）

60 ®C 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> 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。

cfgSsnMgtTelnetTimeout（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0（无超时）

60 ®C 1920

默认值

0

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>，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

该组包含用于 DRAC 5 串行端口的配置参数。

该组允许有一个实例。以下小节介绍该组中的对象。

cfgSerialBaudRate（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

9600, 28800, 57600, 115200

默认值

57600

说明

设置 DRAC 5 串行端口的波特率。

cfgSerialConsoleEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串

MaxLen = 2

默认值

^\ (<Ctrl><\>)

注： "^" 是 <Ctrl> 键。

说明

在使用 **connect com2** 命令时，此键或组合键会终止文本控制台重定向。 **cfgSerialConsoleQuitKey** 值可以用以下方式表示：

- 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）

注： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

说明

指定在用户登录串行控制台接口后执行的串行命令。

默认值

“”

示例

"connect com2"

cfgSerialHistorySize（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

cfgSerialSshEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 DRAC 5 上的 SSH 接口。

cfgSerialTelnetEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 上的远程登录控制台接口。

cfgSerialCom2RedirEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

---

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。

注意： 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1（已启用）

0（已禁用）

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

576 ®C 1500

默认值

1500

说明

DRAC 5 NIC 所用的最大传输单位的字节大小。

cfgNetTuningTcpSrttDflt（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

6 ®C 384

默认值

6

说明

TCP 重新传输往返时间的顺利往返超时基础默认值，以 秒为单位。（输入十六进制值。）

---

cfgOobSnmp

该组包含的参数用于配置 DRAC 5 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 31。

默认值

public

说明

指定 SNMP 陷阱使用的 SNMP 团体名称。

cfgOobSnmpAgentEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 中的 SNMP 代理。

---

cfgRacTuning

此组用于配置各种 RAC 配置属性，比如有效端口和安全端口限制。

cfgRacTuneHttpPort（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

10 ®C 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

10 ®C 65535

默认值

443

说明

指定用来与 RAC 进行 HTTPS 网络通信的端口号。

cfgRacTuneIpRangeEnable

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 的 IP 地址范围验证功能。

cfgRacTuneIpRangeAddr

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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

cfgRacTuneIpBlkEnable

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

cfgRacTuneIpBlkFailcount

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

有效值

2 ®C 16

默认值

5

说明

在从 IP 地址进行的登录尝试被拒绝前，在窗口内发生的最大登录故障数。

cfgRacTuneIpBlkFailWindow

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

有效值

2 ®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，将不计数失败。

cfgRacTuneIpBlkPenaltyTime

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

有效值

2 ®C 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 65535

默认值

22

说明

指定用于 RAC SSH 接口的端口号。

cfgRacTuneTelnetPort（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 65535

默认值

23

说明

指定用于 RAC telnet 接口的端口号。

cfgRacTuneRemoteRacadmEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

1

说明

启用或禁用 RAC 中的远程 RACADM 接口。

cfgRacTuneConRedirEncryptEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

加密控制台重定向会话中的视频。

cfgRacTuneConRedirPort（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 65535

默认值

5901

说明

指定在与 RAC 进行控制台重定向活动期间要为键盘和鼠标通信使用的端口。

注： 此对象在变活动前要求 DRAC 5 重设。

cfgRacTuneConRedirVideoPort（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 65535

默认值

5901

说明

指定在与 RAC 进行控制台重定向活动期间要为视频通信使用的端口。

注： 此对象在变活动前要求 DRAC 5 重设。

cfgRacTuneAsrEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 RAC 的崩溃屏幕捕获功能。

注： 此对象在变活动前要求 DRAC 5 重设。

cfgRacTuneDaylightOffset（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0 ®C 60

默认值

0

说明

为 RAC 时间指定使用的夏令时时差（分钟）。

cfgRacTuneTimezoneOffset（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

-720 ®C 780

默认值

0

说明

为 RAC 时间指定使用的 GMT/UTC 时区时差（分钟）。美国的一些常用时区时差如下：

-480（PST — 太平洋标准时间）

-420（山地标准时间）

-360（CST — 中部标准时间）

-300（EST — 东部标准时间）

cfgRacTuneWebserverEnable（读 / 写）

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用和禁用 RAC Web 服务器。如果禁用此属性，将无法使用客户 Web 浏览器或远程 RACADM 访问 RAC。此属性对于 telnet/ssh/serial 或本地 RACADM 接口无效。

cfgRacTuneLocalServerVideo（读 / 写）

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

有效值

1 (Enables)

0 (Disables)

默认值

1

说明

启用（打开）或禁用（关闭）本地服务器视频。

cfgRacTuneLocalConfigDisable

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用本地用户使用本地 racadm 或 Dell OpenManage Server Administrator Utilities 配置 DRAC 5 的能力。

cfgRacTuneCtrlEConfigDisable

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用本地用户从 BIOS POST option-ROM 配置 DRAC 5 的能力。

---

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 255。

默认值

“”

说明

Managed System 的主机名。

ifcRacMnOsOsName（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 255。

默认值

“”

说明

Managed System 的操作系统名称。

---

cfgRacSecurity

此组用于配置与 RAC SSL 认证签名请求 (CSR) 功能相关的设置。在从 RAC 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。

cfgRacSecCsrCommonName（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 254。

默认值

“”

说明

指定 CSR 常用名 (CN)。

cfgRacSecCsrOrganizationName（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 254。

默认值

“”

说明

指定 CSR 组织名称 (O)。

cfgRacSecCsrOrganizationUnit（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 254。

默认值

“”

说明

指定 CSR 组织部门 (OU)。

cfgRacSecCsrLocalityName（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 地点 (L)。

cfgRacSecCsrStateName（读/写）

注： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。

有效值

字符串。最大长度 = 254。

默认值

""

说明

指定 CSR 州/省名称 (S)。

cfgRacSecCsrCountryCode（读/写）

注： 要修改此属性，必须具有 **"Configure DRAC 5"（配置 DRAC 5）**权限。

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)

cfgRacSecCsrEmailAddr（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

cfgRacSecCsrKeySize（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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 DRAC 5 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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

有效值

1 (TRUE)

0 (FALSE)

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。当连接设备时，可以随后使用 DRAC5 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）

注： 要修改此属性，必须具有**“Access Virtual Media”（访问虚拟介质）**权限。

有效值

1 ®C 65535

默认值

3669

说明

指定 RAC 加密虚拟介质连接所用的端口号。

cfgVirAtapiSrvPortSsl（读/写）

注： 要修改此属性，必须具有**“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

任何介于 0 和 65535 十进制数的未用端口号。

默认值

3669

说明

设置 SSL 虚拟介质连接所用的端口。

cfgVirMediaKeyEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

cfgVirMediaBootOnce（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1（已启用）

0（已禁用）

默认值

0

说明

启用或禁用 RAC 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一如果设备中装有相应介质。

注： 要启用一次引导功能，在系统重新引导期间转至 BIOS 设置并手工更改引导顺序。

cfgFloppyEmulation（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

设置为 0 时，虚拟软盘驱动器被 Windows 操作系统认作可移动磁盘。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 DRAC 5 Active Directory 功能。

cfgADRacDomain（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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

DRAC 所在的 Active Directory 域。

cfgADRacName（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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 DRAC 的名称。

cfgADEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

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

cfgADSpecifyServerEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

有效 IP 地址或完全限定域名 (FQDN)

默认值

无默认值

说明

DRAC 5 使用指定的值搜索 LDAP 服务器查找用户名。

cfgADGlobalCatalog（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

有效 IP 地址或 FQDN

默认值

无默认值

说明

DRAC 5 使用指定的值搜索全局编目服务器查找用户名。

cfgAODomain（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

有效 IP 地址或 FQDN

格式

<域>:<IP 或 FQDN>

默认值

无默认值

说明

DRAC 5 使用指定的值搜索关联对象查找用户名。

cfgADSmartCardLogonEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 DRAC 5 上的 Smart Card 登录。

cfgADCRLEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

为基于 Active Directory 的 Smart Card 用户启用或禁用认证撤回列表 (CRL) 检查。

cfgADAuthTimeout（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

15 ®C 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

cfgADType（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 = 启用扩展架构与 Active Directory 一起使用。

2 = 启用标准架构与 Active Directory 一起使用。

默认值

1 = 扩展架构

说明

确定与 Active Directory 一起使用的架构类型。

cfgADSSOEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 (TRUE)

0 (FALSE)

默认值

0

说明

启用或禁用 RAC 上 Active Directory 单一式身份验证。

---

cfgStandardSchema

此组包含用于配置标准架构设置的参数。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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 DRAC 5	0x00000001
配置 DRAC 5	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

---

cfgIpmiSerial

此组指定用于配置 BMC IPMI 串行接口的属性。

cfgIpmiSerialConnectionMode（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0（终端）

1（基本）

默认值

1

说明

当 DRAC 5 **cfgSerialConsoleEnable** 属性设置为 0（已禁用），DRAC 5 串行端口会成为 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

9600, 19200, 57600, 115200

默认值

57600

说明

指定 IPMI 上串行连接的波特率。

cfgIpmiSerialChanPrivLimit（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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。

cfgIpmiSerialFlowControl（读/写）

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

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）

注： 要修改此属性，必须具有“**Configure DRAC 5**”（配置 **DRAC 5**）权限。

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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 IPMI 串行接口上的回声控制。

cfgIpmiSerialDeleteControl（读/写）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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）

注： 要修改此属性，必须具有**“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0（无）

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

默认值

1

说明

指定 IPMI 串行接口的新行序列指定。

cfgIpmiSerialInputNewLineSequence（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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指定。

---

cfgIpmiSol

此组用于配置系统的 LAN 上串行功能。

cfgIpmiSolEnable（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 LAN 上串行 (SOL)。

cfgIpmiSolBaudRate（读 / 写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

9600, 19200, 57600, 115200

默认值

57600

说明

LAN 上串行通信的波特率。

cfgIpmiSolMinPrivilege（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

2（用户）

3（操作员）

4（管理员）

默认值

4

说明

指定 LAN 上串行访问所需的最小权限。

cfgIpmiSolAccumulateInterval（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 255。

默认值

10

说明

指定发送部分 SOL 字符数据包前 BMC 一般等待的时间。该值是基于 1 的 5ms 增量。

cfgIpmiSolSendThreshold（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 255

默认值

255

说明

SOL 阈值限制值。

---

cfgIpmiLan

此组用于配置系统的 LAN 上 IPMI 功能。

cfgIpmiLanEnable（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用 LAN 上 IPMI 接口。

cfgIpmiLanPrivLimit（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

2（用户）

3（操作员）

4（管理员）

默认值

0

说明

指定 LAN 上 IPMI 访问所需的最大权限。

cfgIpmiLanAlertEnable（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

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）

注： 要查看或修改此属性，必须具有**“Configure DRAC 5”（配置 DRAC 5）**权限和管理员权限。

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）

注： 要修改此属性，必须具有**“Configure DRAC 5”（配置 DRAC 5）**权限。

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 Managed System 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 ®C 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）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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 Managed System 上执行的操作。

cfgIpmiPefEnable（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

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 Managed System 上配置平台事件陷阱。

cfgIpmiPetIndex（读/写）

注： 要修改此属性，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**权限。

有效值

1 ®C 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）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

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 Managed System 上触发事件时，陷阱接收器会接收到 SNMP 陷阱。

cfgIpmiPetAlertEnable（读/写）

注： 要修改此属性，必须具有“Configure DRAC 5”（配置 DRAC 5）权限。

有效值

0 (FALSE)

1 (TRUE)

默认值

1

说明

启用或禁用特定陷阱。

目录

目录

支持的 RACADM 接口

Dell™ Remote Access Controller 5 固件版本 1.40 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

DRAC 5 概览

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- DRAC 5 本次发布的新功能
- DRAC 5 规格和功能
- 您可能需要的其它说明文件

Dell™ Remote Access Controller 5 (DRAC 5) 是一种系统管理硬件和软件解决方案，专门用于为 Dell 系统提供远程管理功能、崩溃系统恢复和电源控制功能。

通过与系统底板管理控制器 (BMC) 通信，可以将 DRAC 5（如果安装）配置为给您发送有关电压、温度、侵入和风扇速度警告或错误的电子邮件警报。DRAC 5 还会记录事件数据和最近的崩溃屏幕（只适用于运行 Microsoft® Windows® 操作系统的系统）以帮助诊断造成系统崩溃的可能原因。

DRAC 5 具有自己的微处理器和内存，由所安装的系统供电。DRAC 5 可以预装在系统上，也可以通过单独的套件提供。

要开始使用 DRAC 5，请参阅 "DRAC 5 使用入门"。

DRAC 5 本次发布的新功能

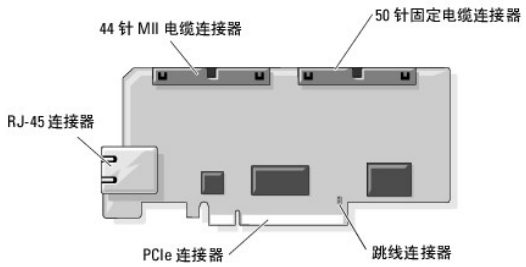
本次发布，DRAC 5 固件版本 1.40：

- 支持使用 Smart Card 进行 Microsoft Active Directory® 身份验证
- 支持使用单一式登录来登录 DRAC 5
- 提供监测功耗的传感器。DRAC 5 使用此数据通过图表和统计来描述系统功耗。
- 提供视频回放功能帮助管理员查看 managed system 的 POST 和操作系统引导日志
- 增强了 SM®CCLP 支持

DRAC 5 规格和功能

图 1-1显示 DRAC 5 硬件。

图 1-1。 DRAC 5 硬件功能



DRAC 5 规格

电源规格

表 1-1 列出 DRAC 5 的电源要求。

表 1-1。 DRAC 5 电源规格

系统电源
+3.3 V 辅助电压条件下 1.2 A（最大）
+3.3 V 主电压条件下 550 mA（最大）
+5 V 主电压条件下 0 mA（最大）

连接器

注： DRAC 5 硬件的安装说明可以在*安装远程访问卡*说明文件或系统随附的*《安装与故障排除指南》*中找到。

DRAC 5 包括一个机载 10/100 Mbps RJ-45 NIC、一根 50 针管理电缆，以及一根 44 针 MII 电缆。请参阅 图 1-1 了解 DRAC 5 电缆连接器。

50 针管理电缆是 DRAC 主接口，可以连接 USB、串行、视频和内置集成电路 (I2C) 总线。44 针 MII 电缆将 DRAC NIC 连接到系统主板。当 DRAC 5 配置为 **“Dedicated NIC”（专用 NIC）**模式时，RJ-45 连接器将 DRAC NIC 连接到带外连接。

根据要求，可以使用管理和 MII 电缆以三种不同模式配置 DRAC。有关详情，请参阅“DRAC 模式”。

DRAC 5 端口

表 1-2 标识 DRAC 5 用来侦听服务器连接的端口。 表 1-3 标识 DRAC 5 用作客户端的端口。当打开防火墙以远程访问 DRAC 5 时，需要此信息。

表 1-2。 DRAC 5 服务器侦听端口

“Port Number”（端口号）	功能
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
161	SNMP 代理
443*	HTTPS
623	RMCP/RMCP+
3668*	虚拟介质服务器
3669*	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 1-3。 DRAC 5 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

支持的远程访问连接

表 1-4 列出连接功能。

表 1-4。 支持的远程访问连接

连接	功能
DRAC 5 NIC	• 10/100 Mbps 以太网 • DHCP 支持 • SNMP 陷阱和电子邮件事件通知 • 用于 DRAC 5 基于 Web 界面的专用网络接口 • 对 telnet/ssh 控制台和 Racadm CLI 命令的支持，包括系统引导、重设、开机和关机命令
串行端口	• 支持串行控制台和 Racadm CLI 命令，包括系统引导、重设、开机和关机命令 • 支持纯文本控制台重定向到 VT-100 终端或终端仿真器

DRAC 5 标准功能

DRAC 5 提供以下功能：

- 双重验证，由 Smart Card 登录提供。双重验证基于用户拥有的设备 (Smart Card) 和所知的内容 (PIN)。
- 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
- 基于角色的授权，使管理员能为每个用户配置特定权限
- 通过基于 Web 的界面或 Racadm CLI 进行用户 ID 和密码配置
- 动态域名系统 (DNS) 注册
- 使用基于 Web 的界面、串行连接、远程 RACADM 或远程登录连接来远程管理和监视系统。
- 支持 Active Directory 验证 — 使用标准架构和扩展架构将所有 DRAC 5 用户 ID 和密码集中到 Active Directory 中。
- 控制台重定向 — 提供远程系统键盘、视频和鼠标功能。
- 虚拟介质 — 使 Managed System 能够访问 Management Station 上的介质驱动器。
- 访问系统事件日志 — 能够访问系统事件日志 (SEL)、DRAC 5 日志和崩溃或无响应系统的上次崩溃屏幕，而不受操作系统状态的影响。
- Dell OpenManage 软件集成 — 使您能够从 Dell OpenManage Server Administrator 或 IT Assistant 启动 DRAC5 基于 Web 的界面。
- RAC 警报 — 使用**“Dedicated”（专用）**、**“Shared with Failover”（与故障转移共享）**或**“Shared”（共享）** NIC 设置，通过电子邮件信息或 SNMP 陷阱向您发出有关潜在管理型节点问题的警报。
- 本地和远程配置 — 使用 RACADM 命令行公用程序提供本地和远程配置。
- 远程电源管理 — 从管理控制台提供远程电源管理，比如关机和重设。
- IPMI 支持。
- 基于标准的 IPMI over LAN 和 SM-CLP 管理。
- 监测功耗的传感器。DRAC 5 使用此数据通过图表和统计来描述系统功耗。
- 安全套接层 (SSL) 加密 — 通过基于 Web 的界面提供安全远程系统管理。
- 密码级别安全性管理 — 防止未授权访问远程系统。
- 基于角色的授权可以为不同的系统管理任务提供可分配的权限。

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有关设置和运行系统中 DRAC 5 的其它信息：

- DRAC 5 联机帮助提供了有关使用基于 Web 界面的信息。
- *《Dell OpenManage™ IT Assistant 用户指南》*提供有关 IT Assistant 的信息。
- *《Dell OpenManage Server Administrator 用户指南》*提供了有关安装和使用 Server Administrator 的信息。
- *《Dell OpenManage Server Administrator SNMP 参考指南》*介绍了 SNMP 管理信息库 (MIB)。MIB 定义了标准 MIB 之外的变量，以涵盖系统管理代理程序功能。
- *《Dell OpenManage 底板管理控制器公用程序用户指南》*提供了有关使用 BMC 管理公用程序配置底板管理控制器 (BMC)、配置 Managed System 的信息以及其它 BMC 信息。
- *《Dell Update Packages 用户指南》*提供了有关作为系统更新战略的一部分获取和使用 Dell Update Packages 的信息。
- *《Dell 系统软件支持值表》*介绍了有关各种 Dell 系统的信息，这些系统支持的操作系统以及可以安装在这些系统上的 Dell OpenManage 组件。

以下系统说明文件还提供了更多有关 DRAC 5 所安装的系统的信息：

- *《产品信息指南》*提供了重要的安全与管制信息。有关其它管制信息，请参阅 **www.dell.com/regulatory_compliance** 上的 Regulatory Compliance Homepage（管制标准主页）。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。
- 机架解决方案提供的*《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。
- *《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。
- *《硬件用户手册》*提供了有关系统功能的信息，并说明了如何排除系统故障以及安装或更换系统组件。
- 系统管理软件说明文件介绍了软件的功能、要求、安装和基本操作。
- 操作系统说明文件介绍了如何安装（如果有必要）、配置和使用操作系统软件。
- 单独购买的任何组件所附带的说明文件均提供有关配置和安装这些选件的信息。
- 系统有时附带更新，用于说明对系统、软件和/或说明文件所做的更改。

  注： 请始终先阅读这些更新，因为这些更新通常会取代其它说明文件中的信息。

- 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

目录

使用并配置虚拟介质

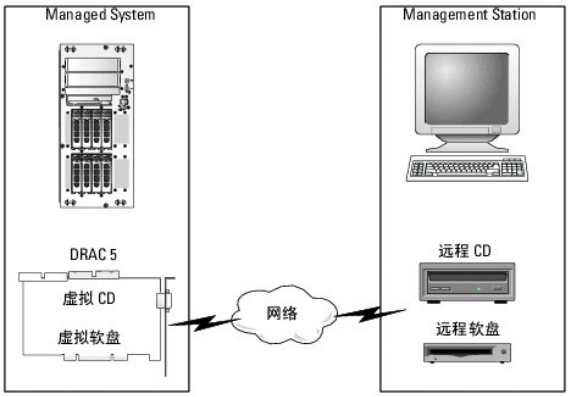
Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 概览
- 安装虚拟介质插件
- 运行虚拟介质
- 使用闪速更新
- 使用虚拟介质命令行界面公用程序
- 使用 VM-CLI 部署操作系统
- 开始之前
- 创建可引导映像文件
- 准备部署
- 部署操作系统
- 常见问题

概览

虚拟介质功能给 Managed System 提供了虚拟 CD 驱动器，该驱动器可以在网络上的任何位置使用标准介质。 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 System，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。

managed system 配置有 DRAC 5 卡。虚拟 CD 和软盘驱动器是两个嵌入 DRAC 5 的电子设备并由 DRAC 5 固件控制。无论是否连接有虚拟介质，这两个设备都始终存在于 managed system 的操作系统和 BIOS 中。

Management Station 通过网络提供物理介质或映像文件。第一次启动 RAC 浏览器并访问虚拟介质页时，将会从 DRAC 5 Web Server 下载虚拟介质插件并自动安装在 Management Station 上。为了使虚拟介质功能正常运行，必须在 management station 上安装虚拟介质插件。

连接虚拟介质后，所有来自 Managed System 的虚拟 CD/软盘驱动器存取请求都会通过网络定向到 Management Station。连接虚拟介质就好比将介质插入虚拟设备。没有连接虚拟介质时，Managed System 上的虚拟设备就像两个没有介质的驱动器。

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 映像文件
1.44 软盘映像	带有 CD-ROM 介质的 USB CD-ROM 驱动器

安装虚拟介质插件

必须在 management station 上安装虚拟介质插件才能使用虚拟介质功能。打开 DRAC 5 用户界面并启动虚拟介质页后，浏览器将自动下载插件（如果需要）。如果成功安装插件，虚拟介质页将会显示虚拟驱动器可以连接的软盘和光盘列表。

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，请安装带有 ActiveX 控件插件的 Internet Explorer。将浏览器安全性设置为**中**或更低设置以允许 Internet Explorer 下载和安装已签名的 ActiveX 控件。

要了解受支持的 Web 浏览器列表，请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。

此外，必须具有管理员权限才能安装和使用虚拟介质功能。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 Mozilla 或 Firefox。如果尚未安装虚拟介质插件，或者有更新的版本，则在安装过程中会显示一个对话框要求您确认 management station 上的插件安装。请确保运行浏览器的用户 ID 具有在浏览器的目录树中的写入权限。如果用户 ID 没有写入权限，则无法安装虚拟介质插件。

请参阅 Dell 支持网站 **support.dell.com** 上的*《Dell 系统软件支持值表》*了解详情。

运行虚拟介质

注意： 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。

使用虚拟介质可以“虚拟化”软盘映像或驱动器，使管理控制台上的软盘映像、软盘驱动器或光盘驱动器成为远程系统上的可用驱动器。

支持的虚拟介质配置

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

支持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。

使用 Web 用户界面运行虚拟介质

连接虚拟介质

1. 在 management station 打开一个支持的 Web 浏览器。请参阅 Dell 支持网站 **support.dell.com** 上的*《Dell 系统软件支持值表》*了解详情。

   控制台重定向和虚拟介质只支持 32 位 Web 浏览器。使用 64 位 Web 浏览器可能会产生无法预料的结果或操作故障。

2. 连接并登录至 DRAC 5。有关详情，请参阅“访问基于 Web 的界面”。
3. 单击**“Media”（介质）**选项卡，然后单击**“Virtual Media”（虚拟介质）**。

   虚拟介质页显示可虚拟化的客户端驱动器。

   注： **软盘驱动器**下的**软盘映像文件**（如果可用）可能显示，只要该设备可虚拟化为虚拟软盘。同时可以选择一个光盘驱动器和一个软盘，或者单个驱动器。

   注： managed system 上的虚拟设备驱动器号与 management station 上的物理驱动器号不一致。

4. 如果提示，请按照屏幕上的说明安装虚拟介质插件。
5. 在**“Attribute”（属性）**框中执行以下步骤：
   a. 在**值**列确保**连接 / 断开**状态值为**已连接**。

      如果值为**已分离**，请执行以下步骤：

      - 在**“Media”（介质）**选项卡中单击**“Configuration”（配置）**。
      - 在**值**列中确保选中了**“Attach Virtual Media”（连接虚拟介质）**复选框。
      - 单击**“Apply Changes”（应用更改）**。
      - 在**“Virtual Media”（虚拟介质）**选项卡中单击**“Virtual Media”（虚拟介质）**。
      - 在**值**列确保**连接 / 断开**状态值为**已连接**。

   - 确保**当前状态**值为**没有连接**。如果值字段显示已连接，则必须与映像或驱动器断开连接，然后重新连接。此状态只在当前 Web 界面上表示虚拟介质连接的当前状态。
   - 确保“Active Session”（激活的会话）值为“Available”（可用）。如果“Value”（值）字段显示为“In Use”（占用），必须等待现有虚拟介质会话释放或使用 Remote Access 下的“Session Management”（会话管理）选项卡并终止活动的虚拟介质会话。一次只允许一个活动的虚拟介质会话。此会话可以由任何 Web 界面或 VM-CLI 公用程序创建。
   - 选中**“Encryption Enabled”（加密已启用）**复选框以在远程系统和 management station 之间建立加密的连接（如果需要）。

- 如果虚拟化软盘映像或 ISO 映像，请选择**“Floppy Image File”（软盘映像文件）**或**“ISO Image File”（ISO 映像文件）**，并输入或浏览至要虚拟化的映像文件。

   如果虚拟化软盘驱动器或光盘驱动器，请选择要虚拟化的驱动器旁的按钮。

7. 单击**“Connect”（连接）**。

   如果此连接经过验证，连接状态将变为**已连接**并会显示所有连接驱动器的列表。所选择的所有可用软盘映像将在 managed system 的控制台上出现，就像真实的驱动器。

   注： 分配的虚拟驱动器号（对于 Microsoft® Windows® 系统）或设备特殊文件（对于 Linux 系统）可能与管理控制台上的驱动器号不同。

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

断开虚拟介质连接

单击**“Disconnect”（断开连接）**从 management station 上断开所有虚拟化的映像和驱动器。**所有**虚拟化的映像或驱动器将断开，不再出现在 managed system 上。

连接和断开虚拟介质连接功能

DRAC 5 虚拟介质功能基于 USB 技术，可以利用 USB 即插即用功能。DRAC 5 增加了从 USB 总线连接和断开虚拟设备连接的功能。设备断开连接后，操作系统或 BIOS 将无法看到任何连接的设备。虚拟设备连接后，设备将可见。与 DRAC 4 不同（设备只有下次系统引导后才能启用或禁用），DRAC 5 虚拟设备可在任意时候连接或断开连接。

可以使用 Web 浏览器、本地 racadm、远程 racadm、telnet 和串行端口连接或断开虚拟设备连接。要使用 Web 浏览器配置虚拟介质，可以导航到“Media”（介质）页，然后进入“Configuration”（配置）页，您可以在这里更改设置并进行应用。您还可指定“Virtual Media Port Number”（虚拟介质端口号）和“Virtual Media SSL Port Number”（虚拟介质

SSL 端口号）。此外，可以启用或禁用“Virtual Flash”（虚拟闪速更新）和“Boot Once”（引导一次）功能。

注： 要启用一次引导功能，在系统重新引导期间转至 BIOS 设置并手工更改引导顺序。

自动连接虚拟介质

DRAC 5 固件 1.30 和更高版本支持自动连接虚拟介质功能。启用此功能后，只要在支持的客户端上虚拟化（连接）了设备，DRAC 5 都会自动将虚拟设备连接到系统。

DRAC 5 会在虚拟介质会话断开连接后断开虚拟介质设备

使用 Web 浏览器连接、自动连接和分离虚拟介质

要使用连接虚拟介质功能，执行以下操作：

1. 单击“System”（系统）->“Media”（介质）->“Configuration”（配置）
2. 选择“Attach Virtual Media”（连接虚拟介质）的“Value”（值）复选框
3. 单击“Apply Changes”（应用更改）。

要使用分离虚拟介质功能，执行以下操作：

1. 单击“System”（系统）→“Media”（介质）→“Configuration”（配置）
2. 取消选择“Attach Virtual Media”（连接虚拟介质）的“Value”（值）复选框
3. 单击“Apply Changes”（应用更改）。

使用 RACADM 连接、自动连接和断开虚拟介质连接功能

要连接虚拟介质功能，请打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 1
```

要断开虚拟介质连接，请打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 0
```

要自动连接虚拟介质功能，请打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 2
```

从虚拟介质引导

在支持的系统上，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：

1. 引导 Managed System。
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 System 重新引导。

   Managed System 尝试根据引导顺序从可引导设备引导。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“使用 VM-CLI 部署操作系统”。

1. 验证以下内容：
   - 操作系统安装 CD 插入到 management station 的 CD 驱动器中。
   - 选择了本地 CD 驱动器。
   - 已与虚拟驱动器连接。
2. 按照从虚拟介质引导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。连接到 Management Station 上的介质后，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

在 Linux 系统上，虚拟介质驱动器没有配置驱动器号。根据系统上安装的软件，虚拟介质驱动器可能不自动安装。如果驱动器不自动安装，请手动安装驱动器。

使用闪速更新

DRAC 5 提供持续闪速更新 — 位于 DRAC 5 文件系统的16 MB 快速闪存，系统可使用它进行持续存储和访问。启用后，虚拟闪速更新配置为第三个虚拟驱动器并出现在 BIOS 引导顺序中，允许用户从虚拟闪速更新引导。

注： 要从虚拟闪速更新引导，虚拟闪速更新映像必须是可引导映像。

与需要外部客户端连接或主机系统内作用设备的 CD 或软盘驱动器不同，实现虚拟闪速更新只需要 DRAC 5 持续虚拟闪速更新功能。16 MB 快速闪存在主机环境中作为未格式化的可移动 USB 设备出现。

实现虚拟闪速更新时请使用以下原则：

- 连接或断开虚拟闪速更新连接将执行 USB 重新枚举，会分别连接和断开所有虚拟介质设备连接（例如 CD 驱动器和软盘驱动器）。
- 启用或禁用虚拟闪速更新时，虚拟介质 CD/软盘驱动器连接状况不更改。

注意： 断开连接和连接过程中断正在进行的虚拟介质读取和写入操作。

启用虚拟闪速更新

要启用虚拟闪速更新，请打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 1
```

禁用虚拟闪速更新

要禁用虚拟闪速更新，请打开命令提示符，键入以下命令并按 <Enter>：

```
racadm config -gcfgRacVirtual -o cfgVirMediaKeyEnable 0
```

在虚拟闪速更新中保存映像

虚拟闪速更新可从 managed 主机格式化。如果运行 Windows 操作系统，请右击设备图标并选择 **"Format"（格式化）**。如果运行 Linux，类似 format 和 fdisk 的系统工具可分区和格式化 USB。

从 RAC Web 浏览器向虚拟闪速更新上载映像前，请确保映像文件大小在 1.44 MB 至 16 MB 之间（包含），并且已禁用虚拟闪速更新。下载映像并重新启用虚拟闪速更新驱动器后，系统和 BIOS 将可以识别虚拟闪速更新。

配置可引导的虚拟闪速更新

1. 将可引导软盘插入软盘驱动器或将可引导 CD 插入光盘驱动器。
2. 重新启动系统并引导至选择的介质驱动器。
3. 向虚拟闪速更新添加分区并启用分区。

   如果虚拟闪速更新仿真硬盘驱动器请使用 **fdisk**。如果虚拟闪速更新配置为驱动器 B:，则虚拟闪速更新仿真软盘，不需要分区来将虚拟闪速更新配置为可引导驱动器。
4. 请使用 **format** 命令和 /s 参数格式化驱动器来将系统文件传送至虚拟闪速更新。

   例如：

   ```
   format /s x
   ```

   其中 *x* 是分配给虚拟闪速更新的驱动器号。
5. 关闭系统并从相应驱动器中取出可引导软盘或 CD。
6. 打开系统并验证系统是否从虚拟闪速更新引导至 C:\ 或 A:\ 提示符。

使用虚拟介质命令行界面公用程序

虚拟介质命令行界面 (VM-CLI) 公用程序是一个脚本化命令行界面，提供从 management station 到远程系统中的 DRAC 5 的虚拟介质功能。

VM-CLI 公用程序提供以下功能：

- 支持多个同时激活的会话。

  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。

- 与虚拟介质插件一致的可移动介质设备或映像文件
- 启用 DRAC 固件引导一次选项后自动终结。
- 使用安全套接字层 (SSL) 确保与 DRAC 5 的通信安全

运行公用程序前，请确保具有远程系统上 DRAC 5 的虚拟介质用户权限。

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 VM-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 VM-CLI 公用程序。

对于 Linux 系统，可以使用 **sudo** 命令访问 VM-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 VM-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 VM-CLI 命令行（或 VM-CLI 脚本）来获取对远程系统上 DRAC 5 的访问和运行公用程序。

公用程序安装

VM-CLI 公用程序位于 *Dell Systems Management Tools and Documentation* DVD 上，该 DVD 随 Dell OpenManage System Management 软件包提供。要安装该公用程序，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，包括诊断、存储管理、远程访问服务和 RACADM 公用程序。本 DVD 还包含自述文件，提供最新 systems management software 产品信息。

此外，*Dell Systems Management Tools and Documentation* DVD 还包含 **vmdeploy**—演示如何使用 VM-CLI 和 RACADM 公用程序将软件部署到多个远程系统的示例脚本。有关详情，请参阅 “使用 VM-CLI 部署操作系统”。

命令行选项

VM-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 DRAC 5 IP 地址的选项采用的语法对于 RACADM 和 VM-CLI 公用程序都一样。

VM-CLI 命令格式如下：

```
racvmcli [参数] [操作系统 shell 选项]
```

注： 需要**管理员**权限来运行 racvmcli 命令。

所有命令行语法区分大小写。有关详情，请参阅“VM-CLI 参数”。

如果远程系统接受了命令，并且 DRAC 5 授权连接，则命令将继续运行，直至出现以下任何一种情况：

- VM-CLI 连接因任何原因终止。
- 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。

VM-CLI 参数

DRAC 5 IP 地址

`-r <RAC-IP-地址>[:<RAC-SSL-端口>]`

其中 *<RAC-IP-地址>* 是有效的唯一 IP 地址或者 DRAC 5 动态域名系统 (DDNS) 名称（如果支持）。

此参数提供 DRAC 5 IP 地址和 SSL 端口。VM-CLI 公用程序需要此信息与目标 DRAC 5 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。

如果忽略 *<RAC-SSL-端口>*，将会使用端口 443（默认端口）。除非更改了 DRAC 5 的默认 SSL 端口，否则不需要可选的 SSL 端口。

DRAC 5 用户名

`-u <DRAC-用户名>`

此参数提供将运行虚拟介质的 DRAC 5 用户名。

*<DRAC-用户名>*必须具有以下属性：

- 有效用户名
- DRAC 虚拟介质用户权限

如果 DRAC 5 验证失败，错误信息将会显示并且命令会终止。

DRAC 用户密码

`-p <DRAC-用户密码>`

此参数提供指定 DRAC 5 用户的密码。

如果 DRAC 5 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。

此外，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）

此外，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 VM-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 VM-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。

加密的数据

-e

如果命令行中包括此参数，VM-CLI 将使用 SSL 加密的信道在 management station 和远程系统中的 DRAC 5 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。

VM-CLI 操作系统外壳选项

VM-CLI 命令行中可使用以下操作系统功能：

- 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 VM-CLI 公用程序打印的输出覆盖指定的文件。

  注： VM-CLI 公用程序不从标准输入读取 (stdin)。因此不需要 stdin 重定向。

- 后台执行 — 默认情况下 VM-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 VM-CLI 命令启动新进程后继续执行（否则，脚本将保持阻塞直至 VM-CLI 程序终止）。当有多个 VM-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。

VM-CLI 返回代码

0 = 无错误

1 = 无法连接

2 = VM-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。

使用 VM-CLI 部署操作系统

虚拟介质命令行界面 (VM-CLI) 公用程序是一个命令行界面，从 Management Station 向远程系统中的 DRAC 5 提供虚拟介质功能。使用 VM-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。

本部分提供了有关将 VM-CLI 公用程序集成到公司网络的信息。

开始之前

开始使用 VM-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

- DRAC 5 卡安装在各个远程系统中
- 各个远程系统中的虚拟设备是 BIOS 引导序列中的第一个设备。

Dell 自定义工厂集成

使用 Dell 自定义工厂集成 (CFI) 选项订购 Dell™ 系统时，Dell 可以为带有 DRAC 5 卡的系统进行预配置，其中包括 DDNS 名称以及允许使用虚拟介质的预配置系统 BIOS。借助这种配置，系统在装入公司网络时就可以从虚拟介质设备引导。

有关详情，请参阅 Dell 网站 **www.dell.com**。

网络要求

必须具有包含以下内容的网络共享：

- 操作系统文件
- 需要的驱动程序
- 操作系统引导映像文件

  映像文件必须是一个软盘映像，也可以是 CD/DVD ISO 映像，具有工业标准的可引导格式。

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 DRAC 5 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/fd0 of=myfloppy.img
```

为 Windows 系统创建映像文件

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

准备部署

配置远程系统

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

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

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

   创建映像文件时应确保：

   - 遵循标准基于网络的安装步骤
   - 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

- 执行以下某一程序：
  - 将 RACADM 和虚拟介质命令行界面 (VM-CLI) 集成到现有操作系统部署应用程序。将 DRAC 5 公用程序集成到现有操作系统部署应用程序中时把示例部署脚本作为指导参考。
  - 使用现有 **vmdeploy** 脚本部署操作系统。

部署操作系统

使用 VM-CLI 和该公用程序包括的 vmdeploy 脚本将操作系统部署到远程系统。

开始之前，应查看 VM-CLI 公用程序包括的示例 vmdeploy 脚本。该脚本提供了将操作系统部署到网络中的远程系统的详细要求。

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. 识别要部署的远程系统。
2. 记录目标远程系统上 DRAC 5 名称和 IP 地址。
3. 为每个目标远程系统执行以下步骤：
   a. 配置包括以下目标系统参数的 VM-CLI 过程：
      - DRAC 5 IP 地址或 DDNS 名称
      - 可引导部署映像文件名称
      - DRAC 5 用户名
      - DRAC 5 用户密码
   b. 使用 RACADM，设置目标 DRAC 5 **"boot once"（引导一次）**选项。
   c. 使用 RACADM，重新引导 DRAC 5 系统。

常见问题

有时我发现虚拟介质客户端连接会断开。为什么？

出现网络超时后，DRAC 5 固件会断开连接，断开服务器和虚拟驱动器间的链接。要重新连接虚拟驱动器，使用虚拟介质功能。

哪些操作系统支持 DRAC 5？

请参阅 Dell 支持网站 support.dell.com 上的《Dell 系统软件支持值表》了解所支持操作系统的列表。

哪些 Web 浏览器支持 DRAC 5？

请参阅 Dell 支持网站 **support.dell.com** 上的*《Dell 系统软件支持值表》*了解所支持 Web 浏览器的列表。

为什么有时丢失客户端连接？

- 如果网络缓慢或更改客户端系统 CD 驱动器中的 CD，有时可能丢失客户端连接。例如，如果更改客户端系统的 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。
- 出现网络超时后，DRAC 5 固件会断开连接，断开服务器和虚拟驱动器间的链接。要重新连接虚拟驱动器，使用虚拟介质功能。

如果带有 Service Pack 4 的 Windows 2000 不能正确安装，我应该怎么做？

如果使用虚拟介质和 Windows 2000 操作系统 CD 安装带有 Service Pack 4 的 Windows 2000，在安装期间系统可能会偶然失去与 CD 驱动器的连接，因此操作系统可能未能正确安装。要解决此问题，从 Microsoft 支持网站 **support.microsoft.com** 下载文件 usbstor.sys 并仅在遇到该问题的系统上运行。请参阅 Microsoft 知识库文章 823086 了解有关详情。

我为什么不能在本地或远程安装 Windows 2000？

如果虚拟闪速更新已启用并且不包含有效映像；例如，虚拟闪速更新包含损坏的或随机映像，则可能无法本地或远程安装 Windows 2000。要解决此问题，在虚拟闪速更新上安装有效映像或禁用虚拟闪速更新（如果在安装期间不使用）。

为什么在配置为共享 NIC 模式时虚拟介质连接会断开？

在配置为共享 NIC 模式时，在服务器上安装网络和芯片组驱动程序会造成虚拟介质连接断开。安装网络或芯片组驱动程序会造成 LOM 重设，从而导致网络数据包超时以及虚拟介质连接超时并断开。要解决此问题，将驱动程序从虚拟驱动器复制到服务器本地硬盘驱动器。要防止断开的虚拟介质连接干扰驱动程序安装过程，应直接从服务器启动驱动程序安装。

Windows 操作系统安装所用时间似乎太长了。 为什么？

如果使用 *Dell Systems Management Tools and Documentation* DVD 和慢速网络连接安装 Windows 操作系统，安装过程可能会由于网络延迟而需要更多的时间访问 DRAC 5 基于 Web 的界面。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 System 上，访问 BIOS 设置并导航到引导菜单。找到虚拟 CD、虚拟软盘或虚拟闪速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？

DRAC 5 允许从以下可引导介质引导：

- CDROM/DVD 数据介质
- ISO 9660 映像
- 1.44 软盘或软盘映像
- DRAC 5 嵌入式虚拟闪速更新
- 被操作系统认作可移动磁盘的 USB 闪存盘
- USB 闪存盘映像

如何使 USB 闪存盘可引导？

只有装了 Windows 98 DOS 的 USB 闪存盘才可以从虚拟软盘引导。要配置自己的可引导 USB 闪存盘，引导至 Windows 98 启动盘并将系统文件从启动盘复制到 USB 闪存盘。例如，从 DOS 提示符处键入以下命令：

```
sys a: x: /s
```

其中 "x:" 是要使其可引导的 USB 闪存盘。

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，打开支持的 Web 浏览器，导航到 Dell 支持网站 support.dell.com，并搜索 "R122672.exe"。

是否需要管理员权限来安装 ActiveX 插件？

在 Windows 系统上必须具有管理员或高级用户权限才能安装虚拟介质插件。

在 Red Hat Linux Management Station 上需要什么权限才能安装和使用虚拟介质插件？

必须在浏览器的目录树上具有写权限才能成功安装虚拟介质插件。

无法在运行 Red Hat Enterprise Linux 或 SUSE Linux 操作系统的系统上找到虚拟软盘设备。已连接虚拟介质并且也已经连接到远程软盘。我应该怎么做？

有些 Linux 版本不会以相同的方式自动安装虚拟软盘驱动器和虚拟 CD 驱动器。为了安装虚拟软盘驱动器，找到 Linux 分配给虚拟软盘驱动器的设备节点。执行下列步骤正确查找并安装虚拟软盘驱动器：

1. 打开 Linux 命令提示符并运行以下命令：

   grep "Virtual Floppy" /var/log/messages

2. 找到该信息的最新条目并记下时间。
3. 在 Linux 提示符处运行以下命令：

   grep "hh:mm:ss" /var/log/messages
   其中

   hh:mm:ss 是 grep 在第一步返回消息的时间戳。

4. 在步骤 3 中，查看 grep 命令的结果并找到赋予 "Dell Virtual Floppy" 的设备名。
5. 确保已连接到虚拟软盘驱动器。
6. 在 Linux 提示符处运行以下命令：

   mount /dev/sdx /mnt/floppy

   其中

   /dev/sdx 是在第 4 步发现的设备名称

   /mnt/floppy 是安装点。

在虚拟软盘驱动器或虚拟闪速更新上支持何种文件系统？

虚拟软盘驱动器或虚拟闪速更新支持 FAT16 或 FAT32 文件系统。

当我使用 DRAC 5 基于 Web 的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 DRAC 5 重设，删除远程连接，并卸下虚拟驱动器。当 DRAC 重设完成后，这些驱动器会重新出现。

当启用或禁用虚拟闪速更新时，我注意到我的所有虚拟驱动器消失并随后又重新出现。为什么？

禁用或启用虚拟闪速更新会造成 USB 重设并造成所有虚拟驱动器从 USB 总线断开并随后又重新连接。

如何在具有只读文件系统的 management station 上安装 Web 浏览器？

如果正在运行 Linux 并且 Management Station 具有只读文件系统，则可以在客户系统上安装浏览器而无需连接到 DRAC 5。通过使用本机插件安装软件包，浏览器可以在客户端设置期间手动安装。

注意： 在只读客户端环境中，如果 DRAC 5 固件更新到较新版本的插件，则已装的 VM 插件将不能运行。这是因为当固件包含较新版本的插件时，不允许运行较早版本插件的功能。在这种情况下，将会提示客户进行插件安装。由于文件系统是只读的，安装将会失败并且插件功能将不可用。

要获得插件安装软件包：

1. 登录到现有的 DRAC5
2. 更改浏览器地址栏中的 URL，从：

   ```
   https://<RAC_IP>/cgi-bin/webcgi/main
   ```

   更改为：

   ```
   https://<RAC_IP>/plugins/ # 请确保包括斜杠。
   ```

3. 注意两个子目录 vm 和 vkvm。 导航到相应的子目录，在 rac5XXX.xpi 文件上单击鼠标右键，并选择 “Save Link Target As...”（将链接目标另存为...）。
4. 选择一个位置来保存插件安装软件包文件。

要安装插件安装软件包：

1. 将安装软件包复制到可以由客户端访问的客户端本机文件系统共享。
2. 在客户系统上打开浏览器的一个实例。
3. 在浏览器的地址栏中输入插件安装软件包的文件路径。例如：

   file:///tmp/rac5vm.xpi

4. 浏览器会引导用户完成插件安装过程。

安装完成后，只要目标 DRAC5 固件不包含较新版本的插件，浏览器都不会再次提示安装插件。

目录

目录

配置安全功能

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- DRAC 管理员的安全选项
- 使用 SSL 和数字认证确保 DRAC 5 通信
- 使用 Secure Shell (SSH)
- 配置服务
- 启用其它 DRAC 5 安全选项

DRAC 5 提供以下安全功能

- 针对 DRAC 管理员的高级安全选项：
  - "Console Redirection disable"（控制台重定向禁用）选项使*本地*系统用户能够使用 DRAC 5 控制台重定向功能禁用控制台重定向。
  - 本地配置禁用功能使*远程* DRAC 管理员能够有选择地禁用 DRAC 5 的配置：
    - BIOS POST option-ROM
    - 操作系统使用本地 racadm 和 Dell OpenManage Server Administrator utilities
- RACADM CLI 和基于 Web 的界面操作，支持 128 位和 40 位（用于不允许 128 位加密的国家/地区）SSL 加密技术

  注： Telnet 不支持 SSL 加密技术。
- 通过基于 Web 的界面或 Racadm CLI 进行会话超时配置（以秒为单位）
- 可配置 IP 端口（在相应情况下）
- 使用加密传输层的 Secure Shell (SSH) 实现更高的安全保护。
- 每个 IP 地址的登录失败限制，在超过此限制时阻塞来自该 IP 地址的登录。
- 连接 DRAC 5 客户端的有限 IP 地址范围

DRAC 管理员的安全选项

禁用 DRAC 5 本地配置

管理员可以通过 DRAC 5 图形用户界面 (GUI) 选择 **Remote Access**→"**Configuration**"（**配置**）→"**Services**"（**服务**）来禁用本地配置。选中 "**Disable the DRAC local Configuration using option ROM**"（使用 option ROM 禁用 DRAC 本地配置）复选框后，远程访问配置公用程序—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 DRAC local Configuration using RACADM**"（使用 RACADM 禁用 DRAC 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 DRAC 5，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 GUI 启用外，管理员可以使用本地 racadm 命令执行。

系统重新引导期间禁用本地配置

此功能禁用 managed system 用户在系统重新引导期间配置 DRAC 5 的能力。

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

注： 此选项只在 Remote Access Configuration Utility 1.13 和更高版本上受支持。要升级此版本，使用来自 *Dell Server Updates* DVD 或 Dell 支持网站 **support.dell.com** 上的 BIOS 更新软件包更新 BIOS。

从本地 racadm 禁用本地配置

此功能禁用 managed system 用户使用本地 racadm 或 Dell OpenManage Server Administrator utilities 配置 DRAC 5 的能力。

```
racadm config -g cfgRacTune -o cfgRacTuneLocalConfigDisable 1
```

注意： 此功能极大地限制了本地用户从本地系统配置 DRAC 5 的能力，包括执行配置默认重设。Dell 建议谨慎使用这些功能，并且应该一次只禁用一个接口以防止一下子失去所有登录权限。

注： 请参阅 Dell 支持网站 **support.dell.com** 上有关*禁用 DRAC 中的本地配置和远程虚拟 KVM* 的白皮书了解详情。

尽管管理员可以使用本地 racadm 命令设置本地配置选项，然而出于安全原因，可以只从带外 DRAC 5 GUI 或命令行界面进行重设。 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，在有多个管理员管理服务器和远程访问设备的数据中心，负责维护服务器软件的管理员可能不需要远程访问设备的管理权限。同样，技术人员在日常系统维护时会实际接触到服务器—可以重新引导系统并访问密码保护的 BIOS—但是不应能够配置远程访问设备。在这样的情况下，远程访问设备管理员可能希望禁用本地配置。

管理员应记住，由于禁用本地配置会极大地限制本地配置权限—包括重设 DRAC 5 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 DRAC 5 用户并且只允许 Microsoft Active Directory® 目录服务用户登录 DRAC 5，则 Active Directory 验证基础架构会随后失败，而管理员将可能无法登录。同样，如果管理员已禁用所有本地配置并在已有动态主机配置协议 (DHCP) 服务器的网络上为 DRAC 5 设置静态 IP 地址，而 DHCP 服务器随后将该 DRAC 5 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 DRAC 5 远程虚拟 KVM

管理员可以有选择地禁用 DRAC 5 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。使用此功能要求在服务器上安装 DRAC 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 DRAC 5 远程 vKVM。例如，管理员不希望远程 DRAC 5 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** 上有关*禁用 DRAC 中的本地配置和远程虚拟 KVM* 的白皮书了解详情。

有关登录脚本的详情，请参阅 **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx**。

使用 SSL 和数字认证确保 DRAC 5 通信

本小节提供关于 DRAC 5 中包括的以下数据安全性功能的信息：

- "安全套接字层 (SSL)"
- "认证签名请求 (CSR)"
- "访问 SSL 主菜单"
- "生成新的认证签名请求"
- "上载服务器认证"
- "上载服务器认证"

安全套接字层 (SSL)

DRAC 包括一个 Web 服务器，服务器配置为使用业界标准的 SSL 安全协议以通过互联网传输加密数据。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 的系统固件

- 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。DRAC 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。

DRAC Web 服务器包括 Dell 自我签名的 SSL 数字证书（服务器 ID）。要确保互联网上的高安全性，请向 DRAC 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，然后上载从 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，以在通过网络和 Internet 进行事务处理时唯一标识该申请者。

CA 批准 CSR 并向您发送认证后，您必须将认证上载至 DRAC 固件。保存在 DRAC 固件上的 CSR 信息必须与认证中包含的信息相匹配。

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**页选项（参阅表 11-1）生成 CSR 以发送到 CA。CSR 信息存储在DRAC 5 固件上。 表 11-2 说明了 **SSL 主菜单**页上的按钮。

表 11-1。 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]）	单击**"Next"（下一步）**打开**"Certificate Signing Request Generation"（认证签名请求生成）**页，可以生成 CSR 发送给 CA 以请求安全 Web 认证。 **注意：** 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）	单击 **"Next"（下一步）**上载公司拥有的现有认证并用来控制对 DRAC 5 的访问。 **注意：** DRAC 5 仅接受 X509 基于 64 编码的认证。DER 编码的认证不被接受。上载新认证会替换 DRAC 5 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 11-2。 SSL 主菜单按钮

按钮	说明
"Print"（打印）	打印 **SSL 主菜单**页。
Next	导航至下一页。

生成新的认证签名请求

注： 每个新的 CSR 都会改写固件上任何原有的 CSR。认证机构 (CA) 接受 CSR 前，固件中的 CSR 必须与 CA 返回的认证匹配。否则，DRAC 5 将不会上载认证。

1. 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）**。
2. 在**生成认证签名请求 (CSR)** 页上键入每个 CSR 属性值。

   表 11-3说明了**生成认证签名请求 (CSR)** 页选项。
3. 单击 **"Generate"（生成）**保存或查看 CSR。
4. 单击相应的**生成认证签名请求 (CSR)** 页按钮继续。 表 11-4 说明了 "**Generate Certificate Signing Request (CSR)"（生成认证签名请求 [CSR]）**上的按钮。

表 11-3。 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 11-4。 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。
"Go Back to Security Main Menu"（退回到安全性主菜单）	返回 **SSL 主菜单**页。
"Generate"（生成）	生成 CSR。

上载服务器认证

1. 在 **SSL 主菜单**页中选择 **"Upload Server Certificate"（上载服务器认证）**并单击 **"Next"（下一步）**。

   显示 **"Certificate Upload"（认证上载）**页。
2. 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。

3. 单击**“Apply”（应用）**。
4. 单击相应页按钮继续。

查看服务器认证

1. 在 **SSL 主菜单**页中选择**“View Server Certificate”（查看服务器认证）**并单击**“Next”（下一步）**。

   表 11-5 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 11-5。 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)

在任何时刻，只支持四个 SSH 会话。会话超时由 `cfgSsnMgtSshIdleTimeout` 属性控制，如 "DRAC 5 属性数据库组和对象定义" 中所述。

可以使用以下命令在 DRAC 5 上启用 SSH：

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

可以使用以下命令更改 SSH 端口：

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

有关 `cfgSerialSshEnable` 和 `cfgRacTuneSshPort` 属性的详情，请参阅 "DRAC 5 属性数据库组和对象定义"。

DRAC 5 SSH 实现支持多种密码模式，如表 11-6 中所示。

表 11-6。 密码模式

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

	• HMAC-MD5-128 • HMAC-MD5-96
验证	• 密码

注： SSHv1 不支持。

配置服务

注： 要修改这些设置，必须具有 **“Configure DRAC 5”（配置 DRAC 5）**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：
   - 本地配置 (表 11-7)
   - Web 服务器 (表 11-8)
   - SSH (表 11-9)
   - Telnet (表 11-10)
   - 远程 RACADM (表 11-11)
   - SNMP 代理 (表 11-12)
   - 启用自动系统恢复代理 (表 11-13)

   使用自动系统恢复代理启用 DRAC 5 的上次崩溃屏幕功能。

   注： 必须安装Server Administrator 并启用其“Auto Recovery”（自动恢复）功能，方法是将“Action”（动作）设置为：“Reboot System”（重新引导系统）、“Power Off System”（关闭系统电源）或“Power Cycle System”（系统关机或再开机），这样才能使上次崩溃屏幕在 DRAC 5 中运作。
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 11-14。

表 11-7。 本地配置设置

设置	说明
“Disable the DRAC local configuration using option ROM”（使用 option ROM 禁用 DRAC 本地配置）	使用 option ROM 禁用 DRAC 5 的本地配置。option ROM 会在系统重新引导期间提示按 <Ctrl+E> 进入设置模块。
“Disable the DRAC local configuration using RACADM”（使用 RACADM 禁用 DRAC 本地配置）	使用本地 RACADM 禁用 DRAC 5 的本地配置。

表 11-8。 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时间，以秒为单位。达到超时时将取消会话。对超时设置的更改不影响当前会话。更改超时设置时，必须注销并再次登录以使新设置生效。超时范围为 60 至 1920 秒。
“HTTP Port Number”（HTTP 端口号）	侦听服务器连接的 DRAC 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 DRAC 使用的端口。默认设置为 **443**。

表 11-9。 SSH 设置

设置	说明
已启用	启用或禁用 SSH。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。最多支持 4 个会话。
“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）	Secure Shell 闲置超时，以秒为单位。范围 = 60 至 1920 秒。输入 0 秒将禁用超时功能。默认设置为 300。
“Port Number”（端口号）	侦听服务器连接的 DRAC 使用的端口。默认设置为 22。

表 11-10。 Telnet 设置

设置	说明
已启用	启用或禁用 Telnet。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。最多支持 4 个会话。
“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）	Secure Shell 闲置超时，以秒为单位。范围 = 60 至 1920 秒。输入 0 秒将禁用超时功能。默认设置为 0。
“Port Number”（端口号）	侦听服务器连接的 DRAC 使用的端口。默认设置为 23。

表 11-11。 远程 RACADM 设置

设置	说明
已启用	启用或禁用远程 RACADM。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。最多支持 4 个会话。
“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 11-12。 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 11-13。 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 11-14。 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。

启用其它 DRAC 5 安全选项

要防止未授权访问远程系统，DRAC 5 提供了以下功能：

- IP 地址筛选 (IPRange) — 定义可以访问 DRAC 5 的特定范围的 IP 地址。
- IP 地址阻塞 — 限制特定 IP 地址的失败登录尝试次数。

这些功能在 DRAC 5 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 DRAC 5 进行访问。所有其它登录都将被拒绝。

IP 筛选将接入登录的 IP 地址与以下 **cfgRacTuning** 属性中指定的 IP 地址范围相比较：

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

c**fgRacTuneIpRangeMask** 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 DRAC 5。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 "DRAC 5 属性数据库组和对象定义" 查看 **cfgRacTune** 属性的完整列表。

表 11-15。 IP 地址筛选 (IpRange) 属性

属性	说明
cfgRacTuneIpRangeEnable	启用 IP 范围检查功能。
cfgRacTuneIpRangeAddr	根据子网掩码中的 1，确定可接受的 IP 地址位样式。 此属性是与 **cfgRacTuneIpRangeMask** 的按位“与”，确定所允许 IP 地址的高端。在高位包含此位样式的任何 IP 地址都允许建立 DRAC 5 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 DRAC 5 会话。
cfgRacTuneIpRangeMask	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。

启用 IP 筛选

以下是 IP 筛选设置的示例命令。

请参阅“远程使用 RACADM”了解有关 RACADM 和 RACADM 命令的详情。

注： 以下 RACADM 命令会阻塞除 192.168.0.57 以外的所有 IP 地址

要将登录限制到一个 IP 地址（例如，192.168.0.57），则使用全掩码，如下所示。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

要将登录限制到一小组四个相邻 IP 地址（例如，192.168.0.212 到 192.168.0.215），则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：

- 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。
- 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 DRAC 5。

IP 阻塞参数使用 **cfgRacTuning** 组功能，其中包括：

- 允许的登录失败次数
- 按秒计算的必须出现这些失败的时间范围
- 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，这些值会由内部计数器“增加”。当用户成功登录后，失败历史记录就会清除并且内部计数器将重设。

注： 如果客户端 IP 地址的登录尝试遭到拒绝，有些 SSH 客户端会显示以下信息：ssh exchange identification: Connection closed by remote host.（ssh exchange 标识：连接被远程主机关闭。）

请参阅 "DRAC 5 属性数据库组和对象定义" 查看 **cfgRacTune** 属性的完整列表。

表 11-16 列出了用户定义的参数。

表 11-16。 登录重试限制属性

属性	定义
cfgRacTuneIpBlkEnable	启用 IP 阻塞功能。 如果在一段时间内 (**cfgRacTuneIpBlkFailWindow**) 某 IP 地址出现连续的失败 (**cfgRacTuneIpBlkFailCount**)，则在一段时间内 (**cfgRacTuneIpBlkPenaltyTime**) 来自该地址的其它建立会话尝试都会遭到拒绝。
cfgRacTuneIpBlkFailCount	设置拒绝某 IP 地址的登录尝试前允许的登录失败次数。

cfgRacTuneIpBlkFailWindow	计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。
crgRacTuneIpBlkPenaltyTime	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 DRAC 5 GUI 配置网络安全设置

注： 您必须具有**配置 DRAC 5** 权限才能执行以下步骤。

1. 在**系统**树中，单击**“Remote Access”（远程访问）**。
2. 单击**“Configuration”（配置）**选项卡，然后单击**“Network”（网络）**。
3. 在**“Network Configuration”（网络配置）**页中单击**“Advanced Settings”（高级设置）**。
4. 在**“Network Security”（网络安全性）**页中配置属性值，然后单击**“Apply Changes”（应用更改）**。

   表 11-17 说明了“**Network Security”（网络安全性）**页设置。
5. 单击相应的**“Network Security”（网络安全性）**页按钮继续。请参阅 表 11-18 了解“**Network Security”（网络安全性）**页按钮的说明。

表 11-17。 网络安全性页设置

设置	说明
“IP Range Enabled”（IP 范围已启用）	启用 IP 范围检查功能，该功能定义可以访问 DRAC 5 的特定 IP 地址范围。
“IP Range Address”（IP 范围地址）	决定可接受的 IP 子网地址。
“IP Range Subnet Mask”（IP 范围子网掩码）	定义 IP 地址中的高位位置。子网掩码应采用网络掩码的格式，其中较高位全部为 1，较低位全部为零。 例如，"**255.255.255.0**"。
“IP Blocking Enabled”（IP 阻塞已启用）	启用 IP 地址阻止功能，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 11-18。 网络安全性页按钮

按钮	说明
"Print"（打印）	打印**"Network Security"（网络安全性）**页
"Refresh"（刷新）	重载**"Network Security"（网络安全性）**页
"Apply Changes"（应用更改）	保存对**"Network Security"（网络安全性）**页的更改。
"Go Back to Network Configuration Page"（退回到网络配置页 ）	返回**"Network Configuration"（网络配置）**页。

目录

目录

使用 DRAC 5 SM-CLP 命令行界面

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- DRAC 5 SM-CLP 支持
- SM-CLP 功能

本部分提供了有关 DRAC 5 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，请参阅分布式管理综合小组 (DMTF) 网站 **www.dmtf.org**。

DRAC 5 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。SMWG SM-CLP 是 DMTF 推动的整个 SMASH 工作中的一部分。

DRAC 5 SM-CLP 支持

DRAC 5 是提供 SM-CLP 基于标准的命令行协议的第一个 RAC 产品。SM-CLP 由 DRAC 5 控制器固件承载并且支持远程登录、SSH 和基于串行的接口。DRAC 5 SM-CLP 接口基于由 DMTF 组织提供的 SM-CLP 规范版本 1.0。

以下部分提供了 DRAC 5 上 SM-CLP 功能的概览。

SM-CLP 功能

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

以下是 SM-CLP 命令行语法的示例。

```
<verb> [<选项>] [<目标>] [<属性>]
```

在典型的 SM-CLP 会话期间，用户可以使用表 12-1 和表 12-2 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。
delete	删除对象实例。
help	显示特定目标的帮助。
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。

表 12-2。 支持的 CLI Verb，用于风扇、电池、侵入、硬件性能、电源设备、温度和电压

Verb	定义
cd	使用 shell 导航映射。
help	显示特定目标的帮助。
show	显示目标属性、verb 和子目标。
exit	从 SM-CLP shell 会话退出。
version	显示目标的版本属性。

使用 SM-CLP

1. SSH（或 telnet）到 DRAC 5，使用正确的凭据。
2. 在命令提示符下键入 `smclp`。

SMCLP 提示符 (->) 将会显示。

SM-CLP 管理操作和目标

管理操作

DRAC 5 SM-CLP 使用户能够管理以下操作：

- 服务器电源管理 — 打开、关闭或重新引导系统
- 系统事件日志 (SEL) 管理 — 显示或清除 SEL 记录

选项

表 12-3 列出支持的 SM-CLP 选项。

表 12-3。 支持的 SM-CLP 选项

SM-CLP 选项	说明
-all	指示 verb 执行所有可能的功能。
-display	显示用户定义数据。
-examine	指示命令处理器在不执行命令的情况下验证命令语法。
-help	显示命令 verb 帮助。
-version	显示命令 verb 版本。

目标

表 12-4 提供了通过 SM-CLP 提供的支持这些操作的目标列表。

表 12-4。 SM-CLP 目标

目标	定义
/system1	Managed System 目标。
/system1/logs1	日志收集目标
/system1/logs1/log1	Managed System 上的系统事件日志 (SEL) 目标。

/system1/logs1/log1/ record1	Managed System 上的单独 SEL 记录实例。
/system1/pwrmgtsvc1	系统的电源管理服务。
/system1/pwrmgtsvc1/ pwrmgtcap1	系统的电源管理服务功能。
/system1/fan1	managed system 上的风扇目标。
/system1/fan1/ tachsensor1	managed system 上风扇目标的传感器目标。
/system1/batteries1	managed system 上的电池目标。
/system1/batteries1/ sensor1	managed system 上电池目标的传感器目标。
/system1/intrusion1	managed system 上的机箱侵入目标。
/system1/intrusion1/ sensor1	managed system 上机箱侵入目标的传感器目标。
/system1/hardwareperformance1	managed system 上的硬件性能目标。
/system1/hardwareperformance1/sensor1	managed system 上硬件性能目标的传感器目标。
/system1/powersupplies1	managed system 上的电源设备目标。
/system1/powersupplies1/sensor1	managed system 上电源设备目标的传感器目标。
/system1/temperatures1	managed system 上的温度目标。
/system1/temperatures1/tempsensor1	managed system 上温度目标的传感器目标。
/system1/voltages1	managed system 上的电压目标。
/system1/voltages1/voltsensor1	managed system 上电压目标的传感器目标。
/system1/chassis1	系统的机箱目标。

SM-CLP 输出格式

DRAC 5 当前支持 SM-CLP 规范中说明的基于文本的输出。

DRAC 5 SM-CLP 示例

以下小节提供了使用 SM-CLP 执行以下操作的示例情况：

- 服务器电源管理
- SEL 管理
- 映射目标导航
- 显示系统属性

服务器电源管理

表 12-5 提供了使用 SM-CLP 在 Managed System 上执行电源管理操作的示例。

表 12-5。 服务器电源管理操作

操作	语法
使用 telnet/SSH 接口登录 RAC	 >ssh 192.168.0.120 >login: root >password:
启动 SM-CLP 管理 shell	 - >smclp DRAC5 SM-CLP System Management Shell, version 1.0 Copyright (c) 2004-2008 Dell, Inc. All rights reserved（版权所有，翻印必究） ->

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 已成功重设

SEL 管理

表 12-6 提供了使用 SM-CLP 在 Managed System 上执行 SEL 相关操作的示例。

表 12-6。 SEL 管理操作

操作	语法
查看 SEL	->show /system1/logs1/log1 /system1/logs1/log1 目标: Record1 Record2 Record3 Record4 Record5 属性: InstanceID = IPMI:BMC1 SEL Log MaxNumberOfRecords = 512 CurrentNumberOfRecords = 5 Name = IPMI SEL EnabledState = 2 OperationalState = 2 HealthState = 2 Caption = IPMI SEL Description = IPMI SEL ElementName = IPMI SEL 命令: cd show help exit version
查看 SEL 记录	->show /system1/logs1/log1/record4 /system1/logs1/log1/record4 属性: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 20050620100512.000000-000 Description = FAN 7 RPM: fan sensor, detected a failure（风扇传感器，检测到故障） ElementName = IPMI SEL Record 命令: cd show help exit version
清除 SEL	->delete /system1/logs1/log1/record* 所有记录成功删除

电池管理

表 12-7 提供了使用 SM-CLP 在电池上执行操作的示例。

表 12-7。 电池管理操作

操作	语法
查看电池状态	->show system1/batteries1/sensor1 /system1/batteries1/sensor1: 属性: SystemCreationClassName = CIM_ComputerSystem SystemName = F196P1S CreationClassName = CIM_Sensor DeviceID = BATTERY 1 SensorType = 1 PossibleStates = {"Good" "Bad" "Unknown"} CurrentState = good ElementName = System Board CMOS Battery OtherSensorTypeDescription = CMOS battery sensor. EnabledState = 1 Verb: cd exit help show version

映射目标导航

表 12-8 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 12-8。 映射目标导航操作

操作	语法
导航到系统目标并重新引导	->cd system1 ->reset **注：** 当前默认目标为 /。
导航到 SEL 目标并显示日志记录	->cd system1 ->cd logs1/log1 ->show
	->cd system1/logs1/log1 ->show
显示当前目标	->cd .
上移一级	->cd ..
退出 shell	->exit

系统属性

表 12-9 列出了在用户键入以下命令时显示的系统属性：

```
show /system1
```

这些属性来源于标准组织提供的基础系统配置文件，并基于 CIM 架构定义的 **CIM_ComputerSystem** 类。

有关其它信息，请参阅 DMTF CIM 架构定义。

表 12-9。 系统属性

对象	属性	说明
CIM_ComputerSystem	名称	企业环境中存在的系统实例的唯一标识符。 最大长度 = 256
	ElementName	系统的用户友好名称。 最大长度 = 64
	NameFormat	标识生成名称的方法。 值： Other, IP, Dial, HID, NWA, HWA, X25, ISDN, IPX, DCC, ICD, E.164, SNA, OID/OSI, WWN, NAA
	专用	指示系统是特殊用途系统还是一般用途系统的枚举。 值： 0=非专用 1=未知 2=其它 3=存储

		4=路由器 5=交换机 6=第 3 层交换机 7=中央交换机 8=集线器 9=存取服务器 10=防火墙 11=打印 12=I/O 13=Web 高速缓存 14=管理 15=阻塞服务器
		16=文件服务器 17=移动用户设备 18=中继器 19=网桥/扩展器 20=网关 21=存储虚拟器 22=介质库 23=扩展器节点 24=NAS 机头 25=自带 NAS 26=UPS 27=IP 电话 28=管理控制器 29=机箱管理器
	ResetCapability	定义系统中的重设方法 值: 1=其它 2=未知 3=已禁用 4=已启用 5=未实现
	CreationClassName	派生此实例的超类。
	EnabledState	表示系统的启用/禁用状态。 值: 0=未知 1=其它 2=已启用 3=已禁用 4=关闭

		5=暂无 6=已启用，但是脱机 7=检测中 8=推迟 9=静默 10=启动
	EnabledDefault	表示系统已启用状态的默认启动配置。默认情况下，系统为“已启用”（值=2）。 值： 2=已启用 3=已禁用 4=暂无 5=已启用，但是脱机 6=无默认
	RequestedState	表示系统上次请求或所需的状态。 值： 2=已启用 3=已禁用 4=关闭 5=无更改 6=脱机 7=检测 8=推迟 9=静默 10=重新引导 11=重设 12=暂无
	HealthState	表示系统的当前运行状况。 值： 0=未知 5=良好 10=降级/警告 15=次要故障 20=主要故障 30=严重故障 35=不可恢复错误
	OperationalStatus	表示系统的当前状况。 值： 0=未知 1=其它 2=良好 3=降级

		4=繁忙 5=预测故障 6=错误 7=不可恢复错误 8=启动 9=停止 10=已停止 11=服务中 12=无联络 13=掉失通信 14=异常中断 15=休眠 16=支持实体错误 17=完成 18=电源模式
	说明	系统基于文本的描述。

风扇、温度、数字电压、功耗和安培传感器的属性名

支持的风扇、温度、数字电压、功耗和安培传感器的属性名

表 12-10。 传感器

对象	属性	说明
CIM_NumericSensor	SystemCreationClassName	系统创建类的名称— CIM_ComputerSystem)
	SystemName	系统的服务标签，是企业环境中系统的唯一标识符
	CreationClassName	创建类名 —CIM_NumericSensor
	DeviceID	系统中传感器的唯一 ID fan1…n（用于 tachsensor） temp 1…n（用于 tempsensor） numeric voltage 1…n) 用于 numericsensor（电压）（仅限 PMBus 系统）） power consumption 1…n（用于 power consumption（仅限 PMBus 系统）） amperage 1…n（用于 amperage（仅限 PMBus 系统））
	BaseUnits	传感器测量单位 RPM=Tachometer（用于 tachsensor） C=Temperature（用于 tempsensor） V=电压（用于 numericsensor）Watts=功耗（用于 powerconsumption） Amp=安培（用于 amperage）
	CurrentReading	传感器的当前读数。
	LowerThresholdNonCritical	非临界阈值下限
	UpperThresholdNonCritical	非临界阈值上限
	LowerThresholdCritical	临界阈值下限
	UpperThresholdCritical	临界阈值上限
	SupportedThreshold	支持的传感器阈值。 { "LowerThresholdCritical" }（用于 tachsensor） { "LowerThresholdNonCritical", "UpperThresholdNonCritical", "UpperThresholdCritical", "LowerThresholdCritical" }（用于 tempsensor） { }（用于 voltsensor（数字传感器）） {"UpperThresholdNonCritical", "UpperThresholdCritical"}（用于 powerconsumption { } 用于 amperage）

	SettableThreshold	可以为传感器设置的阈值级别。 { }（没有传感器支持设置阈值）
	SensorTypes	传感器类型： 5=Tachometer（用于 tachsensor） 2=Temperature（用于 temperature） 3=Voltage（用于 voltage） 1=Power Consumption（用于 powerconsumption） 1=Ampereage（用于 amperage）
	PossibleStates	传感器可能的状态。 { "unknown", "warning", "failed", "non-recoverable" }
	CurrentState	传感器报告的当前状态
	ElementName	传感器的名称
	OtherSensorTypeDescription	如果 sensortype 属性包含值 "1"（其它），此属性会提供有关传感器的更多说明。 "Power consumption sensor."用于 powerconsumption "Amperage sensor." 用于 amperage
	EnabledState	表示传感器是已启用还是已禁用。 1=Enabled

电源设备传感器属性名

表 12-11。 支持的电源设备传感器属性名

对象	属性	说明
CIM_NumericSensor	SystemCreationClassName	系统创建类的名称 CIM_ComputerSystem)
	SystemName	系统的服务标签，是企业环境中系统的唯一标识符
	CreationClassName	创建类名 —CIM_PowerSupply
	DeviceID	系统中传感器的唯一 ID。 pwrsupply 1...n
	TotalOutputPower	DRAC 用户界面上显示的总电源输出
	ElementName	特定传感器的名称。
	OperationalStatus	电源设备的当前运行状态。
	HealthState	电源设备的运行状态。
	EnabledState	表示传感器是已启用还是已禁用。 1=Enabled

侵入、电池、电压和硬件性能传感器的属性名

表 12-12。 支持的侵入、电池、电压和硬件性能传感器的属性名

对象	属性	说明
CIM_NumericSensor	SystemCreationClassName	系统创建类的名称— CIM_ComputerSystem)
	SystemName	系统的服务标签，是企业环境中系统的唯一标识符
	CreationClassName	创建类名 —CIM_Sensor
	DeviceID	系统中传感器的唯一 ID Intrusion1...n（用于侵入传感器） Battery1...n（用于电池传感器） Voltage1...n（用于电压传感器） Hardware performance sensor1...n（用于硬件性能传感器）
	SensorType	1=其它 3=Voltage（用于电压传感器）
	PossibleStates	传感器可能的状态 { "no intrusion", "chassis intrusion," "drive bay intrusion," "I/O card area intrusion," "processor area intrusion," "LAN disconnect," "unauthorized dock," "FAN area intrusion" }（用于侵入传感器）

		{ "absent," "low," "failed," "good" }（用于电池传感器） { "good," "bad," "unknown" }（用于电压传感器） { "Normal," "Others," "Thermal Protection," "Cooling Capacity changed," "Power Capacity changed," "User Configuration" }（用于硬件性能传感器）
	CurrentState	传感器报告的当前状态。
	ElementName	传感器的名称
	OtherSensorTypeDescription	如果 sensortype 属性包含值 "1"（其它），此属性会提供有关传感器的更多说明。 "Chassis intrusion sensor"（用于侵入传感器） "CMOS battery sensor"（用于电池传感器） "Hardware performance sensor"（用于硬件性能）
	EnabledState	表示传感器是已启用还是已禁用 1=Enabled（用于所有传感器）

风扇和电源设备冗余设置传感器的属性名

表 12-13。 支持的风扇和电源设备冗余设置传感器的属性名

对象	属性	说明
CIM_RedundancySet	InstanceID	实例号
	RedundancyStatus	冗余状态。
	TypeOfSet	3=负载平衡（用于风扇冗余） 4=备用（用于电源设备冗余）
	MinNumberNeeded	0=未知
	ElementName	传感器的名称

机箱传感器属性名

表 12-14。 支持的机箱传感器属性名

对象	属性	说明
CIM_Chassis	CreationClassName	创建类名—CIM_Chassis
	PackageType	封装类型 3=机箱
	ChassisPackageType	机箱封装类型 17=主系统机箱
	制造商	制造商 "Dell"
	Model（型号）	系统的型号名称
	ElementName	元素名称

电源管理服务属性名

表 12-15。 支持的电源管理服务属性名

对象	属性	说明
CIM_PowerManagementService	CreationClassName	创建类的名称— CIM_PowerManagementService
	名称	IPMI Power Service
	ElementName	Dell Server Power Management Service

	powerstate	系统的当前电源状态。 2=On 6=Off 可以设置为以下值： 2=打开电源 6=关闭电源 5=电源重置 9=先关闭再打开系统电源

使用 set verb，可以设置系统的电源状态。例如，如果要打开关闭系统的电源：

```
set powerstate=2
```

电源功能的属性名

表 12-16。 支持的电源功能的属性名

对象	属性	说明
CIM_PowerManagementCapabilities	InstanceID	电源功能的唯一实例 ID
	PowerChangeCapabilities	3=电源状态可设置
	ElementName	Dell Server Power Management Service
	PowerStatesSupported	2=打开电源 6=关闭电源 5=电源重置 9=先关闭再打开系统电源

目录

目录

监控和警报管理

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 配置平台事件
- 常见问题

本节介绍如何监控 DRAC 5 以及如何配置系统和 DRAC 5 来接收警报。

配置 Managed System 以获取上次崩溃屏幕

在 DRAC 5 可以捕获上次崩溃屏幕前，必须将 managed system 配置成满足以下前提条件。

1. 安装 managed system software。有关安装 managed system software 的详情，请参阅《*Server Administrator 用户指南*》。
2. 运行支持的 Microsoft® Windows® 操作系统，并且在 **“Windows Startup and Recovery Settings”（Windows 启动和恢复设置）**中取消选中 Windows“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）。

   要启用本地 RACADM，打开命令提示符并键入以下命令：

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

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

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

   “Auto Recovery”（自动恢复）操作设置为 **“Shutdown”（关机）**或 **“Power Cycle”（关机后再开机）**时，如果 managed system 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

为了确保 DRAC 5 基于 Web 的界面中上次崩溃屏幕功能正常工作，必须在运行 Microsoft Windows Server 2003 和 Windows 2000 Server 操作系统的 managed system 上禁用 **“Automatic Reboot”（自动重新引导）**选项。

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。

在 Windows 2000 Server 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. 单击“**启动和恢复...**”按钮。
4. 取消选择“ **自动重新引导**”复选框。

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：

- 风扇探测器故障
- 电池探测器警告
- 电池探测器故障
- 分离电压探测器故障
- 温度探测器警告
- 温度探测器故障
- 检测到机箱侵入
- 已降级冗余
- 冗余掉失
- 处理器警告
- 处理器故障
- 处理器不存在
- PS/VRM/D2D 警告
- PS/VRM/D2D 故障
- 电源不存在
- 硬件日志故障
- 自动系统恢复

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)

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 Web 用户界面配置 PEF

1. 使用支持的 Web 浏览器登录远程系统。请参阅“访问基于 Web 的界面”。
2. 单击“**Alert Management**”（**警报管理**）选项卡，然后单击“**Platform Events**”（**平台事件**）。
3. 启用全局警报。
   a. 单击“**Alert Management**”（**警报管理**）并选择“**Platform Events**”（**平台事件**）。
   b. 选择“**Enable Platform Event Filter Alert**”（**启用平台事件筛选器警报**）复选框。
4. 在“**Platform Events Filters Configuration**”（**平台事件筛选器配置**）下，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**）。
5. 在“**Platform Event Filters List**”（**平台事件筛选器列表**）下，双击要配置的筛选器。

6. 在“**Set Platform Events**”（设置平台事件）页中，进行相应选择并单击“**Apply Changes**”（应用更改）。

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）。

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 17 间的一个值。启用/禁用选择可以设置为 1（已启用）或 0（已禁用）。

   例如，要启用具有索引 5 的 PEF，键入以下命令：

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

2. 配置 PEF 操作。

   在命令提示符处，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：

   - <*操作*> 值位 0 ®C 1 = 启用警报操作，0 = 禁用警报
   - <*操作*> 值位 1 ®C 1 = 关机；0 = 不关机
   - <*操作*> 值位 2 ®C 1 = 重新引导；0 = 不重新引导
   - <*操作*> 值位 3 ®C 1 = 关机后再开机；0 = 不关机后再开机

   例如，要启用 PEF 重新引导系统，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

1. 使用支持的 Web 浏览器登录远程系统。请参阅“访问基于 Web 的界面”。
2. 确保遵循"使用 Web 用户界面配置 PEF"中的步骤。
3. 配置 PET 策略。
   a. 在“**Alert Management**”（警报管理）选项卡中，单击“**Traps Settings**”（陷阱设置）。

b. 在“**Destination Configuration Settings**”（**目标配置设置**）下，使用相应信息配置“**Community String**”（**团体字符串**）字段，然后单击“**Apply Changes**”（**应用更改**）。

4. 配置 PET 目标 IP 地址

a. 在“**Destination Number**”（**目标号码**）列中，单击目标号码。

b. 确保选中“**Enable Destination**”（**启用目标**）复选框。

c. 在“**Destination IP Address**”（**目标 IP 地址**）字段中，键入有效 PET 目标 IP 地址。

d. 单击“**Apply Changes**”（**应用更改**）。

e. 单击“**Send Test Trap**”（**发送检测陷阱**）检测配置的警报（如果需要）。

注： 用户帐户必须具有“**Test Alerts**”（**检测警报**）权限才能执行此步骤。请参阅表 5-4。

f. 为其它目标号码重复步骤 a 到 e。

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：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -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：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
```

3. 配置 PET 策略。

在命令提示符处，键入以下命令并按 <Enter>：

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IP 地址>
```

其中 1 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>
```

配置电子邮件警报

使用 Web 用户界面配置电子邮件警报

1. 使用支持的 Web 浏览器登录远程系统。请参阅“访问基于 Web 的界面”。
2. 确保遵循"使用 Web 用户界面配置 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）**。
   b. 在**“SMTP (Email) Server Address settings”（SMTP [电子邮件] 服务器地址设置）**下，使用相应信息配置**“SMTP (Email) Server IP address”（SMTP [电子邮件] 服务器 IP 地址）**字段，然后单击**“Apply Changes”（应用更改）**。
4. 配置电子邮件警报目标。
   a. 在**“Email Alert Number”（电子邮件警报号）**列中，单击电子邮件警报号。
   b. 确保选中**“Enable Email Alert”（启用电子邮件警报）**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. 在**“Email Description”（电子邮件说明）**字段中，输入说明（如果需要）。
   e. 单击**“Apply Changes”（应用更改）**。
   f. 单击**“Send Test Email”（发送检测电子邮件）**检测配置的电子邮件警报（如果需要）。

   注： 用户帐户必须具有**“Test Alerts”（检测警报）**权限才能执行此步骤。请参阅表 5-4。

   g. 为其余电子邮件警报设置重复 步骤 a 到 步骤 e。
5. 启用全局警报。
   a. 单击**“Alert Management”（警报管理）**并选择**“Platform Events”（平台事件）**。
   b. 选择**“Enable Platform Event Filter Alert”（启用平台事件筛选器警报）**复选框。

使用 RACADM CLI 配置电子邮件警报

1. 启用全局警报。

   打开命令提示符，键入以下命令并按 <Enter>：

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

2. 启用电子邮件警报。

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

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

   其中 1 和 1 分别是电子邮件目标索引和启用/禁用选择。

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

   例如，要启用具有索引 4 的电子邮件，键入以下命令：

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

3. 配置电子邮件设置。

在命令提示符处，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 是电子邮件目标索引，而 <*自定义消息*> 是自定义消息。

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 "**testemail**" 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，DRAC 5 代理的团体名称是 public。当 IT Assistant 发出 set 请求时，DRAC 5 代理会生成 SNMP 验证错误，因为它只接受来自团体 = public 的请求。

可以使用 RACADM 更改 DRAC 5 团体名称。

要查看 DRAC 5 团体名称，请使用以下命令：

```
racadm getconfig -g cfgOobSnmp
```

要设置 DRAC 5 团体名称，请使用以下命令：

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

要防止生成 SNMP 验证陷阱，必须输入将由代理接受的团体名称。由于 DRAC 5 只允许一个团体名称，因此必须为 IT Assistant 查找设置输入相同的 get 和 set 团体名称。

目录

目录

配置智能平台管理接口（IPMI）

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 配置 IPMI
- 配置 LAN 上串行

配置 IPMI

本部分提供有关配置和使用 DRAC 5 IPMI 接口的信息。接口包括以下：

- LAN 上 IPMI
- 串行 IPMI
- LAN 上串行

DRAC 5 完全兼容 IPMI 2.0。可以通过以下途径配置 DRAC IPMI：

- 浏览器
- 开发源代码公用程序，比如 *ipmitool*
- Dell OpenManage IPMI shell, **ipmish**
- RACADM。

有关使用 IPMI Shell, ipmish 的详情，请参阅 Dell Support 网站 **support.dell.com** 上的《*Dell OpenManage™ BMC 用户指南*》。

有关使用 RACADM 的详情，请参阅“远程使用 RACADM”。

使用基于 Web 的界面配置 IPMI

1. 使用支持的 Web 浏览器登录远程系统。请参阅“访问基于 Web 的界面”。
2. 配置 LAN 上 IPMI。
   a. 在**系统**树中，单击**“Remote Access”（远程访问）**。
   b. 单击**“Configuration”（配置）**选项卡并单击**“Network”（网络）**。
   c. 在**“Network Configuration”（网络配置）**页的**“IPMI LAN Settings”（IPMI LAN 设置）**下，选择**“Enable IPMI Over LAN”（启用 LAN 上 IPMI）**并单击**“Apply Changes”（应用更改）**。
   d. 如果需要，更新 IPMI LAN 信道权限。

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

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

   e. 如果需要，设置 IPMI LAN 信道密钥。

   注： DRAC 5 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。

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

如果 IPMI 串行处于终端模式，可以配置以下其它设置：

- 删除控制
- 回声控制
- 行编辑
- 新行序列
- 输入新行序列

有关这些属性的详情，请参阅 IPMI 2.0 规范。

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： DRAC 5 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 cfgIpmiLan -o cfgIpmiEncryptionKey <密钥>
```

其中 <*密钥*> 是一个有效十六进制格式的 20 字符密钥。

3. 配置 IPMI LAN 上串行 (SOL)。

在命令提示符处，键入以下命令并按 <Enter>：

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

a. 更新 IPMI SOL 最小权限级别。

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 cfgIpmiSol -o cfgIpmiSolMinPrivilege <级别>
```

其中<*级别*> 是以下某个值：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要配置 IPMI 权限为 2（用户），键入以下命令：

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

b. 更新 IPMI SOL 波特率。

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

在命令提示符处，键入以下命令并按 <Enter>：

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

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

例如：

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

c. 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 cfgIpmiSerial -o cfgIpmiSerialBaudRate <波特率>
```

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

例如：

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

c. 启用 IPMI 串行硬件流控制。

在命令提示符处，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：

- 2（用户）
- 3（操作员）
- 4（管理员）

例如，要设置 IPMI 串行信道权限为 2（用户），键入以下命令：

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

e. 确保串行 MUX 在 BIOS 设置程序中正确设置。

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

IPMI 配置完成。

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

- 删除控制
- 回声控制
- 行编辑
- 新行序列
- 输入新行序列

有关这些属性的详情，请参阅 IPMI 2.0 规范。

使用 IPMI 远程访问串行接口

在 IPMI 串行接口中，以下模式可用：

- **"IPMI terminal mode"（IPMI 终端模式）** — 支持从串行终端提交的 ASCII 命令。命令集仅限于有限的命令（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。
- **"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 **"**DRAC 5 属性数据库组和对象定义**"**。

配置 LAN 上串行

注： 有关完整 LAN 上串行信息请参阅 *Dell OpenManage 底板管理控制器用户指南*。

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 Over LAN"（LAN 上串行）**。
3. 配置 LAN 上串行设置。

   表 14-1 提供关于 **LAN 上串行配置**页设置的信息。

4. 单击 **"Apply Changes"（应用更改）**。
5. 如果需要，配置高级设置。否则，单击相应的 **LAN 上串行配置**页按钮继续（参阅表 14-2）。

   要配置高级设置：

   a. 单击 **"Advanced Settings"（高级设置）**。

   b. 在 **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 14-3。

   c. 单击 **"Apply Changes"（应用更改）**。

   d. 单击相应的 **LAN 上串行配置高级设置**页按钮继续。请参阅 表 14-4 或 **LAN 上串行配置高级设置**页按钮的说明。

表 14-1。 LAN 上串行配置页设置

设置	说明
启用 LAN 上串行	启用 LAN 上串行。选中=启用；未选中=禁用。
波特率	IPMI 数据速度。选择 **9600 bps**、**19.2 kbps**、**57.6 kbps** 或 **115.2 kbps**。
信道权限级别限制	设置 IPMI LAN 上串行最小用户权限：**管理员**、**操作员**或**用户**。

表 14-2。 LAN 上串行配置页按钮

按钮	说明
"Print"（打印）	打印**LAN 上串行配置**页。
"Refresh"（刷新）	刷新 **LAN 上串行配置**页。
"Advanced Settings"（高级设置）	打开 **LAN 上串行配置高级设置**页。
"Apply Changes"（应用更改）	应用 **LAN 上串行配置**页设置。

表 14-3。 LAN 上串行配置高级设置页设置

设置	说明
字符积累间隔时间	传输部分 SOL 字符数据包之前 BMC 需要等待的时间。从 1 开始，每 5ms 递增。
字符发送阈值	接收到此数量的字符（或更多）时，BMC 将发送一个包含字符的 SOL 字符数据包。从 1 开始。

表 14-4。 LAN 上串行配置高级设置页按钮

按钮	说明
"Print"（打印）	打印 **LAN 上串行配置高级设置**页。
"Refresh"（刷新）	刷新 **LAN 上串行配置高级设置**页。
"Go Back To Serial Over LAN Configuration Page"（退回到 LAN 上串行配置页）	返回 **LAN 上串行配置**页。
"Apply Changes"（应用更改）	应用 **LAN 上串行配置高级设置**页设置。

目录

目录

对 Managed System 进行恢复和故障排除

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 排除远程系统故障首先需要进行的步骤
- 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 和 操作系统引导日志
- 查看上次系统崩溃屏幕

本节介绍了如何使用 DRAC 5 基于 Web 的界面执行与远程崩溃系统恢复和故障排除有关的任务。

- "排除远程系统故障首先需要进行的步骤"
- "管理远程系统上的电源"
- "使用系统事件日志 (SEL)"
- "查看上次系统崩溃屏幕"

排除远程系统故障首先需要进行的步骤

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，应检查上次崩溃屏幕（参见 "查看上次系统崩溃屏幕"），并使用控制台重定向（参见 "Managed System 上支持的屏幕分辨率刷新率"）以及远程电源管理（参见 "管理远程系统上的电源"）来重新启动系统并观察重新引导过程。

管理远程系统上的电源

DRAC 5 允许在 Managed System 上远程执行几种电源管理操作，以在系统崩溃或出现其它系统事件后尝试恢复。

使用**电源管理**页执行以下操作：

- 当重新引导、打开或关闭系统电源时，通过操作系统执行秩序关机。
- 查看系统当前的**电源状况**—**打开**或**关闭**。

要从**系统**树访问**电源管理**页，请单击 **"System"（系统）**，然后单击 **"Power Management"（电源管理）**选项卡。

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。

从 DRAC 5 GUI 选择电源控制操作

1. 选择以下**电源控制操作**之一。
   - **"Power On System"（打开系统电源）**— 打开系统电源（相当于系统电源关闭时按电源按钮）。
   - **"Power Off System"（关闭系统电源）**— 关闭系统电源（与系统电源打开时按电源按钮等效）。

- **"Reset System"（重设系统）**— 重设系统（相当于按重启动按钮）；使用此功能不关闭电源。
- **"Power Cycle System"（系统关机后再开机）**— 关闭系统电源，然后重新引导（冷引导）系统。

2. 单击**"Apply"（应用）**执行电源管理操作（例如，使系统关机后再开机）。
3. 单击相应的**电源管理**页按钮继续（请参阅表 15-1）。

表 15-1。 电源管理页按钮（右上）

按钮	措施
"Print"（打印）	打印**电源管理**页
"Refresh"（刷新）	重载**电源管理**页

从 DRAC 5 CLI 选择电源控制操作

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

`racadm serveraction <操作>`

以下为 *<操作>* 字符串的选项：

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

- 主系统机箱
- Remote Access Controller
- 底板管理控制器

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

主系统机箱

表 15-2 和 表 15-3 说明主系统机箱属性。

注： 要接收**主机名**和**操作系统名称**信息，managed system 上必须安装有 DRAC 5 服务。

表 15-2。 系统信息字段

字段	说明
说明	系统说明。
"BIOS Version"（BIOS 版本）	系统 BIOS 版本。
"Service Tag"（服务标签）	系统服务标签号码。

"Host Name"（主机名）	主机系统的名称。
"OS Name"（操作系统名称）	系统上运行的操作系统。

表 15-3。 自动恢复字段

字段	说明
"Recovery Action"（恢复操作）	检测到“系统挂起”时，DRAC 可配置为执行以下操作之一：无操作、硬重设、断电或关机后再开机。
"Initial Countdown"（初始倒计数）	在 DRAC 将执行恢复操作时检测“系统挂起”后经过的秒数。
"Present Countdown"（当前倒计数）	倒计数计时器的当前值，以秒为单位。

Remote Access Controller

表 15-4 说明了 Remote Access Controller 属性。

表 15-4。 RAC 信息字段

字段	说明
名称	短名称。
产品信息	详细名称。
"Hardware Version"（硬件版本）	Remote Access Controller 卡版本，或“未知”。
固件版本	DRAC 5 当前固件版本级别。
"Firmware Updated"（固件更新）	固件上次更新的日期和时间。
"RAC Time"（RAC 时间）	系统时钟设置。

底板管理控制器

表 15-5 说明了底板管理控制器的属性。

表 15-5。 BMC 信息字段

字段	说明
名称	底板管理控制器。
IPMI 版本	智能平台管理接口 (IPMI) 版本。
可能激活的会话数	同时可激活的最大会话数。
目前激活的会话数	目前激活的总会话数。
固件版本	BMC 固件版本。
LAN 已启用	LAN 已启用或 LAN 已禁用。

使用系统事件日志 (SEL)

SEL 日志页显示 managed system 上发生的系统重要事件。

要查看系统事件日志：

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

系统事件日志页显示事件严重性并提供其他信息，如表 15-6 所示。

3. 单击相应的**“System Event Log”（系统事件日志）**页按钮以继续（参阅表 15-7）。

表 15-6。 状况标志图标

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 15-7。 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。

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。

clrsel 命令会从系统事件日志 (SEL) 删除全部现有的记录。

```
racadm clrsel
```

使用 POST 和 操作系统引导日志

DRAC 5 的这种功能使用户能够回放 BIOS POST 和操作系统引导的最后三个实例的停止动作视频。

要查看 POST 和操作系统引导捕获日志：

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 或操作系统引导捕获日志的日志号。

   日志的视频显示在新屏幕上。
4. 单击“**STOP”（停止）**停止视频。

查看上次系统崩溃屏幕

注意： 上次崩溃屏幕功能要求 managed system 配置了 Server Administrator 中的**“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 DRAC 5 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）**。

上次崩溃屏幕页提供屏幕右上角的以下按钮（参阅表 15-8）：

表 15-8。 上次崩溃屏幕页按钮

按钮	措施
“Print”（打印）	打印**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保存到所选的目录。
“Delete”（删除）。	删除**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，当系统重设计时器设置为小于 30 秒时**上次崩溃屏幕**可能无法捕获。使用 Server Administrator 或 IT Assistant 将系统重设计时器设置为至少 30 秒，并确保**上次崩溃屏幕**运行正常。有关其它信息，请参阅“配置 Managed System 以获取上次崩溃屏幕”。

目录

目录

恢复并故障排除 DRAC 5

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 使用 RAC 日志
- 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 DRAC 5 进行恢复和故障排除。

可以使用以下某一工具来排除 DRAC 5 的故障：

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

使用 RAC 日志

RAC 日志是 DRAC 5 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 DRAC 5 发出的警报。当日志已满后，会将最早的条目覆盖掉。

要从 DRAC 5 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 16-1 中所列信息。

表 16-1。 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）。 当 DRAC 5 刚开始启动并且无法与 managed system 通信时，该时间将会显示为系统引导。
来源	引起事件的接口。
说明	DRAC 5 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 16-2 中所列的按钮。

表 16-2。 RAC 日志按钮

按钮	措施
“Print”（打印）	打印**“RAC Log”（RAC 日志）**页。

"Clear Log"（清除日志）	清除 **"RAC Log"（RAC 日志）**条目。 **注：** 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。 **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 DRAC 5 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

DRAC 5 提供一组标准网络诊断工具（参阅表 16-3），与基于 Microsoft® Windows® 或 Linux 的系统提供的工具类似。使用 DRAC 5 基于 Web 的接口，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 16-3 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"（退回到诊断页）**。

表 16-3。 诊断命令

命令	说明
arp	显示地址解析协议 (ARP) 表的内容。ARP 条目不能添加或删除。
ifconfig	显示网络接口表的内容。
netstat	打印路由选择表的内容。如果在 **netstat** 选项右边的文本字段中提供可选接口号，netstat 将输出与通过该接口的通信量有关的其它信息、缓冲区的使用情况以及其它网络接口信息。
ping <*IP 地址*>	验证目标 IP 地址是否可以使用当前路由选择表的内容从 DRAC 5 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 DRAC 5 跟踪日志。有关详情，请参阅 "gettracelog"。

使用跟踪日志

内部 DRAC 5 跟踪日志可以由管理员用来调试 DRAC 5 警报或网络连接问题。

要从 DRAC 5 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：

- DHCP ®C 跟踪发送到 DHCP 服务器和从 DHCP 服务器接收的信息包。
- IP ®C 跟踪发送和接收的 IP 信息包。

跟踪日志还可能包含 DRAC 5 固件特定的错误代码，与内部 DRAC 5 固件有关，而不是 Managed System 的操作系统。

注： DRAC 5 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 DRAC 5 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：

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

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

有关详情，请参阅coredump和coredumpdelete。

目录

目录

传感器

Dell™ Remote Access Controller 5 固件版本 1.40 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
- 硬件性能探测器
- 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 DRAC 5 监视相应的硬件传感器来监测电池、风扇探测器、机箱入侵、电源设备、功耗、温度和电压。

电池探测器

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

注： 只有在系统具有 ROMB 时，存储 ROMB 电池设置才可用。

风扇探测器

风扇探测器传感器提供的信息有：

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

机箱入侵探测器

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：

- 电源设备的状态，是在正常阈值范围内，还是超过阈值。

  注： 只能从 Dell™ OpenManage™ Server Administrator 设置阈值。请参阅《*Dell OpenManage Server Administrator 用户指南*》了解详情。

- 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，“Power Supply Redundancy”（电源设备冗余）部分将不会显示。

硬件性能探测器

硬件性能探测器提供中央处理器 (CPU) 的性能状态，是降级还是正常。当 CPU 处于限制状态时，硬件性能传感器的状态显示为降级。

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。此信息通过底板管理控制器 (BMC) 固件传感器提供给 DRAC 5。

注： 此功能只在有限的 Dell PowerEdge™ *x*9*xx* 和 *xx*0*x* 系统上提供。

还可以查看距 DRAC 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

以下是典型的电源探测器。系统可能有这些和/或其他。

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

电压探测器表示探测器状态是否在预置警告和严重阈值内。

目录

目录

DRAC 5 使用入门

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

DRAC 5 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。DRAC 5 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。

管理员使用 Management station 远程管理装有 DRAC 卡的 Dell 系统。相应的被监控的系统称为 managed system。

要能够使用 DRAC 卡，应遵循这些步骤：

1. 在 Dell 系统中安装 DRAC 5 卡 — DRAC 5 可能预装在系统中或在套件中单独提供。

   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** 上特定系统的*硬件用户手册*详细了解如何执行此步骤。

   必须在 management station 和 managed system 上安装 DRAC 5 软件。没有 managed system software，将不能在本地使用 RACADM，并且 DRAC 不能捕获上次崩溃屏幕。

2. 配置 DRAC 5 属性、网络设置和用户 — 可以通过使用远程访问配置公用程序、基于 Web 的界面或 RACADM 来配置 DRAC 5。
3. 配置 Microsoft® Active Directory® 访问 DRAC 5，从而能在 Active Directory 软件中为现有用户添加和控制 DRAC 5 用户权限。
4. 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。
5. 配置远程访问点，比如控制台重定向和虚拟介质。
6. 配置安全设置。
7. 使用基于标准的服务器管理命令行协议 (SM-CLP) 管理网络上的系统。
8. 配置警报实现高效的系统管理。
9. 配置 DRAC 5 智能平台管理接口 (IPMI) 设置使用基于标准的 IPMI 工具管理网络上的系统。

目录

目录

DRAC 5 的基本安装

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 开始之前
- 安装 DRAC 5 硬件
- 配置系统使用 DRAC 5
- 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 DRAC 5 固件
- 配置支持的 Web 浏览器

本部分介绍了如何安装并设置 DRAC 5 硬件和软件。

开始之前

在安装和配置 DRAC 5 软件前检查一下系统随附的项目：

- DRAC 5 硬件（已安装或在可选套件中）
- DRAC 5 安装步骤（在本章中）
- *Dell Systems Management Tools and Documentation* DVD

安装 DRAC 5 硬件

注： DRAC 5 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。

DRAC 5 可以预装在系统上，也可以通过单独的套件提供。要开始使用已安装在系统上的 DRAC 5，请参阅“软件安装和配置概览”。

如果在系统上没有安装 DRAC 5，请参阅 DRAC 5 套件随附的*安装远程访问卡*说明文件或参阅平台的*《安装与故障排除指南》*了解硬件安装说明。

注： 请参阅系统包括的*《安装与故障排除指南》*了解有关如何删除 DRAC 5 的信息。另外，如果使用扩展架构，应查看与所删除 DRAC 5 相关的所有 Microsoft® Active Directory® RAC 属性以确保相应的安全。

配置系统使用 DRAC 5

要配置系统使用 DRAC 5，使用 Dell™ Remote Access 配置公用程序（以前为 BMC 设置模块）。

要运行 Dell Remote Access 配置公用程序：

1. 打开或重新启动系统。
2. 系统完成 POST 后提示您时，请按 <Ctrl><E> 组合键。

   如果按 <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 NIC。

a. 使用下箭头键，高亮度显示“**NIC Selection**”（**NIC 选择**）。

b. 使用左箭头和右箭头键，选择以下某个 NIC 选择：

- “**Dedicated**”（**专用**） — 选择此选项使远程访问设备能够使用 Remote Access Controller (RAC) 上的专用网络接口。此接口不与主机操作系统共享并会将管理通信路由到单独的物理网络，从而能够与应用程序通信分开。此选项只有在系统中装有 DRAC 卡时才可用。
- “**Shared**”（**共享**） — 选择此选项与主机操作系统共享该网络接口。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。
- “**Failover**”（**故障转移**） — 选择此选项与主机操作系统共享该网络接口。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 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。

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** 或 “**Static**”（**静态**）。

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

e. 按 <Esc>。

5. 按 <Esc>。

6. 选择“**Save Changes and Exit**”（**保存更改并退出**）。

系统会自动重新引导。

注： 在配有一个 NIC 的 Dell PowerEdge™ 1900 系统上查看 Web 用户界面时，NIC 配置页会显示两个 NIC（NIC1 和 NIC2）。这是正常的行为。PowerEdge 1900 系统（以及其它在主板上配有单独 LAN 的 PowerEdge 系统）可以配置 NIC 组。共享和组模式可以在这些系统上独立运行。

请参阅《*Dell OpenManage 底板管理控制器公用程序用户指南*》了解有关 Dell 远程访问配置公用程序的详情。

软件安装和配置概览

本节从较高的级别概述了 DRAC 5 软件安装和配置过程。使用基于 Web 的界面、RACADM CLI 或 Serial/Telnet/SSH 控制台配置 DRAC 5。

有关 DRAC 5 软件组件的详情，请参阅 "在 Managed System 上安装软件"。

安装 DRAC 5 软件

要安装 DRAC 5 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 Management Station 上安装软件”。

配置 DRAC 5

要配置 DRAC 5：

1. 选择以下某个配置工具：
   - 基于 Web 的界面
   - RACADM CLI
   - Serial/Telnet/SSH 控制台

注意： 同时使用一个以上的 DRAC 5 配置工具可能会产生意外的结果。

2. 配置 DRAC 5 网络设置。请参阅“配置 DRAC 5 属性”。
3. 添加和配置 DRAC 5 用户。请参阅“添加和配置 DRAC 5 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 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 DRAC 5 固件。请参阅“启动文本控制台”。
7. 通过网络访问 DRAC 5。请参阅“启动文本控制台”。

在 Managed System 上安装软件

在 managed system 上安装软件是可选项。没有 managed system software，将不能在本地使用 RACADM，并且 DRAC 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。有关如何安装此软件的说明，请参阅《*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 DRAC 5 management station software 和 DRAC 5 managed system software。

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

有关上次崩溃屏幕的详情，请参阅 "查看上次系统崩溃屏幕"。

在 Management Station 上安装软件

系统包括了 Dell OpenManage Systems Management 软件套件 。此套件包括但不限于，*Dell Systems Management Tools and Documentation* DVD。此 DVD 具有以下组件：

- *Dell Systems Build and Update Utility* — 一种可引导公用程序，可优化 Dell 系统的部署和重新部署，并且还提供了所需的工具来配置和更新 Dell 系统。
- *Dell Systems Console and Agent* — 包含所有最新的 Dell 系统管理软件产品，比如 Dell OpenManage Server Administrator 和控制台产品，包括 Dell OpenManage IT Assistant。
- *Dell Systems Service and Diagnostics Tools* — 提供配置系统所需的工具并提供最新的 BIOS、固件、诊断程序和 Dell 针对您系统优化的驱动程序。

有关安装 Server Administrator 软件的信息，请参阅《*Server Administrator 用户指南*》。

配置 Red Hat Enterprise Linux（版本 4）Management Station

Dell Digital KVM Viewer 需要额外配置才能在 Red Hat Enterprise Linux（版本 4）management station 上运行。在 management station 上安装 Red Hat Enterprise Linux（版本 4）操作系统时，执行以下步骤：

- 提示添加或删除软件包时，安装可选的 **Legacy Software Development** 软件。此软件包包括在 management station 上运行 Dell Digital KVM 查看器所需的软件组件。
- 要确保 Dell Digital KVM Viewer 运作正常，在防火墙上打开以下端口：
  - 键盘和鼠标端口（默认为端口 5900）
  - 视频端口（默认为端口 5901）

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 **"Setup"（安装）**时，所有所支持操作系统的 RACADM 公用程序都安装到 management station 上。

安装 RACADM

1. 以 root 身份登录至您想在其中安装 Management Station 组件的系统。
2. 如果必要，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 DRAC 5 固件

使用以下某一方法更新 DRAC 5 固件。

- 基于 Web 的界面
- RACADM CLI
- Dell Update Packages

开始之前

使用本地 RACADM 或 Dell Update Packages 更新 DRAC 5 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. 如果系统正在运行 SUSE Linux Enterprise Server（版本 10）for Intel EM64T，则启动 Raw 服务。
4. 确保 RAC 虚拟闪速更新已卸下或者操作系统或其它应用程序或用户没有在使用。
5. 断开连接并卸下虚拟介质。
6. 确保 USB 已启用。

下载 DRAC 5 固件

要更新 DRAC 5 固件，从 Dell Support 网站 **support.dell.com** 下载最新固件并将该文件保存到本地系统。

以下软件组件包括在 DRAC 5 固件包中：

- 编译的 DRAC 5 固件代码和数据
- 扩充 ROM 映像
- 基于 Web 的界面、JPEG 和其它用户界面数据文件
- 默认配置文件

使用 **“Firmware Update”（固件更新）**页将 DRAC 5 固件更新为最新修订版本。运行固件更新时，更新会保留当前的 DRAC 5 设置。

使用基于 Web 的界面更新 DRAC 5 固件

1. 打开基于 Web 的界面并登录到远程系统。

   请参阅“访问基于 Web 的界面”。

2. 在 **“System”（系统）**树中，单击 **“Remote Access”（远程访问）**并单击 **“Update”（更新）**选项卡。
3. 在 **“Firmware Update”（固件更新）**页的 **“Firmware Image”（固件映像）**字段中，键入从 **support.dell.com** 下载的固件映像的路径或单击 **“Browse”（浏览）**导航到该映像。

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

   例如：

   `C:\Updates\V1.0\<映像名称>`。

   默认固件映像名称是 **firmimg.d5**。

4. 单击 **“Update”（更新）**。

   更新可能需要几分钟才能完成。完成后，将会出现一个对话框。

5. 单击 **“OK”（确定）**关闭会话并自动注销。
6. DRAC 5 重设后，单击 **“Log In”（登录）**登录到 DRAC 5。

使用 racadm 更新 DRAC 5 固件

可以使用基于 CLI 的 racadm 工具来更新 DRAC 5 固件。如果在 managed system 上装有 Server Administrator，则使用 local racadm 更新固件。

1. 从 Dell 支持网站 **support.dell.com** 下载 DRAC 5 固件映像到 managed system

例如：

```
C:\downloads\firmimg.d5
```

2. 运行以下 racadm 命令：

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

还可以使用 remote racadm 更新固件。

例如：

```
racadm -r <DRAC5 IP 地址> U <用户名> -p <密码> fwupdate -p -u -d <路径>
```

其中*路径*是 managed system 上保存 **firmimg.d5** 的位置。

使用针对所支持 Windows 和 Linux 操作系统的 Dell Update Packages 更新 DRAC 5 固件

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

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

要了解受支持的 Web 浏览器列表，请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。。

配置 Web 浏览器以连接到基于 Web 的界面

如果从通过代理服务器连接到因特网的 management station 连接到 DRAC 5 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 DRAC 5 基于 Web 的界面时，会在可信域列表中缺少 DRAC 5 IP 地址的情况下提示您将该 IP 地址添加到列表中。完成后，单击“Refresh”（刷新）或重新启动 Web 浏览器重新连接到 DRAC 5 基于 Web 的界面。

32 位和 64 位 Web 浏览器

DRAC 5 基于 Web 的界面在 64 位 Web 浏览器上不受支持。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，即使插件安装已失败，Web 浏览器也会将插件信息存储在配置文件目录。要修复此问题，安装并运行支持的 32 位 Web 浏览器，并登录 DRAC 5。

查看本地化版本的基于 Web 的界面

Windows

DRAC 5 基于 Web 的界面获得以下 Windows 操作系统语言支持：

- 英语
- 法语
- 德语
- 西班牙语
- 日语
- 简体中文

要在 Internet Explorer 中查看 DRAC 5 基于 Web 界面的本地化版本，应执行下列步骤：

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. 导航到 /etc/sysconfig/i18n 文件。
5. 在文件中，应用以下更改：

   当前项：

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

   更新项：

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

6. 注销并随后登录操作系统。
7. 重新启动 DRAC 5。

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 DRAC 5 的高级配置，请参阅"DRAC 5 的高级配置"。

目录

目录

DRAC 5 的高级配置

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 开始之前
- 配置 DRAC 5 属性
- 使用 Web 用户界面配置 DRAC 5
- 启用并配置 Managed System 使用串行或 Telnet 控制台
- 使用串行或 Telnet 控制台
- 配置串行模式和终端模式
- 通过本地串行端口或 Telnet Management Station（客户系统）连接到 Managed System
- 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
- 使用串行或 Telnet 控制台
- 使用 Secure Shell (SSH)
- 配置 DRAC 5 网络设置
- 通过网络访问 DRAC 5
- 配置 DRAC 5 NIC
- 远程使用 RACADM
- RACADM 提要
- 启用和禁用 racadm 远程功能
- 配置多个 DRAC 5 卡
- 常见问题

本部分提供有关高级 DRAC 5 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 DRAC 环境的用户进行阅读。

开始之前

应已完成 DRAC 5 硬件和软件的基本安装和设置。有关详情，请参阅“DRAC 5 的基本安装”。

配置 DRAC 5 属性

可以通过基于 Web 的界面或 RACADM 配置 DRAC 5 属性（网络、用户等）。

DRAC 5 提供了基于 Web 的界面和 RACADM（命令行界面），使您能够配置 DRAC 5 属性和用户，执行远程管理任务并对远程（管理型）系统进行故障排除。对于日常系统管理，请使用 DRAC 5 基于 Web 的界面。本章介绍了如何使用 DRAC 5 基于 Web 的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。

所有基于 Web 界面的配置任务也可以通过 RACADM 执行。

使用 Web 用户界面配置 DRAC 5

有关每个基于 Web 的界面页面的上下文敏感信息，请参阅 DRAC 5 联机帮助。

访问基于 Web 的界面

访问 DRAC 5 基于 Web 的界面。

1. 打开一个支持的 Web 浏览窗口。

   请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。

2. 在 **"Address"（地址）**字段中键入下面的内容，并按 <Enter>：

   `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 DRAC 5 的 IP 地址，而*端口号*是 HTTPS 端口号。

   将会显示 DRAC 5 **登录**窗口。

注： 如果使用 Internet Explorer 版本 6 SP2 或版本 7 登录 DRAC 5 Web GUI 并且客户端在专用网络上，但是不能访问 Internet，则可能会遇到长达 30 秒的延迟。要解决此问题：

1. 禁用钓鱼网站过滤器。

   https://phishingfilter.microsoft.com/faq.aspx.

2. 禁用 CRL 提取：

   a.单击 "**Tools"（工具）**→ "**Options"（选项）**→ "**Advanced"（高级）**选项卡→ "**Security"（安全性）**。

   b.取消选择 "**Check for publisher's certificate revocation"（检查发布者认证撤销）**。

登录

您可以作为 DRAC 5 用户或 Microsoft® Active Directory® 用户登录。默认用户名为 **root**，默认密码为 **calvin**。

登录 DRAC 5 前，请验证您具有 **"Log In to DRAC 5"（登录 DRAC 5）**权限。请询问企业的 DRAC 或网络管理员确认访问权限。

要登录：

1. 在 **"User Name"（用户名）**字段中键入下面的内容之一：
   - 您的 DRAC 5 用户名。

     例如，<*用户名*>

     本地用户的 DRAC 5 用户名区分大小写
   - 您的 Active Directory 用户名。

例如，<*域*>\<*用户名*>、<*域*>/<*用户名*> 或 <*用户*>@<*域*>。

Active Directory 用户名示例：**dell.com\john_doe** 或 **john_doe@dell.com**。

Active Directory 用户名不区分大小写。

2. 在 **“Password”（密码）**字段中，键入 DRAC 5 用户密码或 Active Directory 用户密码。

此字段区分大小写。

3. 单击 **“OK”（确定）**或按 <Enter>。

注销

1. 在 DRAC 5 基于 Web 的界面窗口右上角单击 **“Log Out”（注销）**关闭会话。
2. 关闭浏览器窗口。

注： **“Log Out”（注销）**按钮在您登录后才出现。

注： 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 DRAC 5 基于 Web 的界面可能会生成应用程序错误。要修复此问题，从 Microsoft 支持站点 support.microsoft.com 下载最新的 Internet Explorer 累积安全更新。

启用并配置 Managed System 使用串行或 Telnet 控制台

以下小节介绍如何在 Managed System 上启用和配置 serial/telnet/ssh 控制台。

使用 connect com2 串行命令

使用 **connect com2** 串行命令时，应确保以下配置正确：

- BIOS 设置程序中的 **“Serial Communication”（串行通信）→ “Serial Port”（串行端口）**设置。
- DRAC 配置设置。

如果 telnet 会话建立到 DRAC 5 时这些设置不正确，**connect com2** 可能会显示空白屏幕。

为 Managed System 上的串行连接配置 BIOS 设置程序

执行下列步骤配置 BIOS 设置程序以将输出重定向到串行端口。

注： 必须将系统设置程序与 **connect com2** 命令一起配置。

1. 打开或重新启动系统。
2. 系统显示以下信息时立即按 <F2> 键：

```
<F2> = System Setup（<F2> = 系统设置）
```

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

   “External Serial Connector”（外部串行连接器） — **“Remote Access Device”（远程访问设备）**

   “Redirection After Boot”（启动后重定向） ®C **“Disabled”（已禁用）**
5. 按 <Esc> 退出系统设置程序以完成系统设置程序配置。

使用远程访问串行接口

向 RAC 设备建立串行连接时，以下接口可用：

- IPMI 串行接口。请参阅 “使用 IPMI 远程访问串行接口”。
- RAC 串行接口

RAC 串行接口

RAC 还支持提供了 RAC CLI 的串行控制台接口（或 *RAC 串行控制台*），RAC CLI 不由 IPMI 定义。如果系统包括已启用 **“Serial Console”（串行控制台）**的 RAC 卡，该 RAC 卡将会覆盖 IPMI 串行设置并显示 RAC CLI 串行接口。

要启用 RAC 串行终端接口，设置 **cfgSerialConsoleEnable** 属性为 **1** (TRUE)。

例如：

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

有关详情，请参阅 “cfgSerialConsoleEnable（读/写）”。

表 4-1 提供了串行接口设置。

表 4-1。 串行接口设置

IPMI 模式	RAC 串行控制台	接口
基本	已禁用	基本模式
基本	已启用	RAC CLI
终端	已禁用	IPMI 终端模式
终端	已启用	RAC CLI

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. 在内核行上追加两个选项：

```
kernel .............console=ttyS1,57600
```

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

表 4-2 提供了示例 **/etc/grub.conf** 文件，显示在此步骤中说明的更改。

表 4-2。 示例文件：/etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE: You do not have a /boot partition. This means that
# all kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sdal
# initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,57600
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/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

编辑 **/etc/grub.conf** 文件时，应遵循以下原则：

1. 禁用 GRUB 的图形界面并使用基于文本的界面；否则，GRUB 屏幕将不会显示在 RAC 控制台重定向中。要禁用图形界面，注释掉以 splashimage 开头的行。
2. 要使用多个 GRUB 选项来通过 RAC 串行连接启动控制台会话，将以下行添加到所有选项：

   ```
   console=ttyS1,57600
   ```

   表 4-2 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 4-3 显示具有新行的示例文件。

表 4-3。 示例文件：/etc/innitab

```
#
# inittab This file describes how the INIT process should set up
# the system in a certain run-level.
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel.The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have
# networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left.Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

按照以下说明编辑文件 **/etc/securetty**：

添加新行，带有 COM2 的串行 tty 名称：

```
ttyS1
```

表 4-4 显示具有新行的示例文件。

表 4-4。 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**

启用 DRAC 5 Serial/Telnet/SSH 控制台

可以本地或远程启用 serial/telnet/ssh 控制台。

本地启用 Serial/Telnet/SSH 控制台

注： 您（当前用户）必须具有 “Configure DRAC 5”（配置 DRAC 5）权限，才能执行本节的步骤。

要从 Managed System 启用 serial/telnet/ssh 控制台，在命令提示符处键入以下本地 RACADM 命令：

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

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

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

远程启用 Serial/Telnet/SSH 控制台

要远程启用 serial/telnet/ssh 控制台，在命令提示符处键入以下远程 **RACADM** 命令：

```
racadm -u <用户名> -p <密码> -r <DRAC 5 IP 地址> config -g cfgSerial -o cfgSerialConsoleEnable 1
```

```
racadm -u <用户名> -p <密码> -r <DRAC 5 IP 地址> config -g cfgSerial -o cfgSerialTelnetEnable 1
```

```
racadm -u <用户名> -p <密码> -r <DRAC 5 IP 地址> config -g cfgSerial -o cfgSerialTelnetEnable 1
```

注： 使用 Internet Explorer 版本 6 SP2 或版本 7 登录专用网络上的 managed system，但不能访问 Internet，则在使用 remote RACADM 命令期间可能会遇到长达 30 秒的延迟。

使用 RACADM 配置串行和 Telnet 控制台的设置

本小节提供了步骤来为 serial/telnet/ssh 控制台重定向配置默认配置设置。

要配置设置，请输入 RACADM **config** 命令并带有对应于所需设置的组、属性和属性值。

可以从本地或远程键入 RACADM 命令。远程使用 RACADM 命令时，必须包括用户名、密码和 Managed System DRAC 5 IP 地址。

在本地使用 RACADM

要本地键入 RACADM 命令，在 Managed System 上从命令提示符处键入以下命令：

```
racadm config -g <组> -o <属性> <值>
```

要查看属性列表，在 Managed System 上从命令提示符处键入以下命令：

```
racadm getconfig -g <组>
```

远程使用 RACADM

要远程使用 RACADM 命令，在 Management Station 上从命令提示符处键入以下命令：

```
racadm -u <用户名> -p <密码> -r <DRAC 5 IP 地址> config -g <组> -o <属性> <值>
```

远程使用 RACADM 前，应确保 Web Server 配置有 DRAC 5 卡。否则，RACADM 将超时并显示以下信息：

无法按照指定 IP 地址连接到 RAC。

要使用 Secure Shell (SSH)、telnet 或本地 RACADM 启用 Web Server，在 Management Station 上的命令提示符处键入以下命令：

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

显示配置设置

表 4-5 提供了用于显示配置设置的操作和相关命令。要运行命令，在 Managed System 上打开命令提示符，键入命令并按 <Enter>。

表 4-5。 显示配置设置

措施	命令
列出可用组。	racadm getconfig -h
显示特定组的当前设置。	racadm getconfig -g <组> 例如，要显示所有 **cfgSerial** 组设置的列表，输入以下命令：

	racadm getconfig -g cfgSerial
远程显示特定组的当前设置。	racadm -u <*用户*> -p <*密码*> -r <*DRAC 5 IP 地址*> getconfig -g cfgSerial 例如，要远程显示 **cfgSerial** 组的所有设置的列表，输入以下内容： racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial

配置 Telnet 端口号

键入以下命令更改 DRAC 5 上的 Telnet 端口号。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <新端口号>
```

使用串行或 Telnet 控制台

可以使用 RACADM 或从串行 /telnet/ssh 控制台命令提示符远程运行表 4-19 中的串行命令。

登录 DRAC 5

配置完 management station 终端仿真软件和管理型节点 BIOS 后，执行下列步骤登录到 DRAC 5：

1. 使用 Management Station 终端仿真软件连接到 DRAC 5。
2. 输入 DRAC 5 用户名并按 <Enter>。

   您已登录 DRAC 5。

启动文本控制台

通过 management station 终端软件以 Telnet 或 SSH 登录 DRAC 5 后，可以使用 telnet/SSH 命令 **connect com2** 重定向 managed system 文本控制台。一次只支持一个 **connect com2** 客户端。

要连接到 managed system 文本控制台，请打开 DRAC 5 命令提示符（通过 telnet 或 SSH 会话显示）并键入：

```
connect com2
```

从串行会话，可以通过按 <Esc><Shift><Q> 连接 managed system 的串行控制台，该命令将 managed system 的串行端口直接连接到服务器的 COM2 端口并且不经过 DRAC 5。要将 DRAC 5 重新连接到串行端口，请按 <Esc><Shift><9>。管理型节点 COM2 端口和 DRAC 5 串行端口的波特率必须相同。

connect -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。

注： 使用 **-h** 选项时，客户端和服务器终端仿真类型（ANSI 或 VT100）必须相同；否则，输出可能混乱。此外，将客户端终端行设置为 **25**。

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>
```

配置串行模式和终端模式

配置 IPMI 和 RAC 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 4-6 了解 IPMI 串行设置的说明。
4. 配置 RAC 串行设置。

   请参阅 表 4-7 了解 RAC 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 4-8 了解串行配置页设置的说明。

表 4-6。 IPMI 串行设置

设置	说明
连接模式设置	• 直接连接基本模式 - IPMI 串行基本模式 • 直接连接终端模式 - IPMI 串行终端模式
波特率	设置数据速度。选择 **9600 bps**、**19.2 kbps**、**57.6 kbps** 或 **115.2 kbps**。
数据流控制	• 无 — 硬件流控制关闭 • RTS/CTS — 硬件流控制打开
信道权限级别限制	• 管理员 • 操作员 • 用户

表 4-7。 RAC 串行设置

设置	说明
已启用	启用或禁用 RAC 串行控制台。选中=启用；未选中=禁用。
“Maximum Sessions”（最大会话）	此系统允许的最大同时会话数。
“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 **9600 bps**、**28.8 kbps**、**57.6 kbps** 和 **115.2 kbps**。默认值为 **57.6 kbps**。
“Escape Key”（Esc 键）	指定 <Esc> 键。默认为 ^\ 字符。
“History Buffer Size”（历史记录缓冲区大小）	串行历史记录缓冲区大小，保持上次写入控制台的字符。最大值和默认值 = 8192 字符。
“Login Command”（登录命令）	有效登录时执行的 DRAC 命令行。

表 4-8。 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 RAC 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 4-9 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。请参与 表 4-10 了解终端模式设置页按钮的说明。

表 4-9。 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： • **BMC 在收到 <bksp> 或 <del> 时输出 <bksp><sp><bksp> 字符** — • **BMC 在收到 <bksp> 或 <del> 时输出 <del> 字符** —
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 4-10。 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”（退回到串行端口配置 ）	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。

通过本地串行端口或 Telnet Management Station（客户系统）连接到 Managed System

Managed System 提供了系统上 DRAC 5 和串行端口之间的访问，从而可以开机、关机、重设 Managed System 以及访问日志。

串行控制台可以通过 Managed System 外部串行连接器在 DRAC 5 上使用。任何时刻只有一个串行客户系统（management station）可以活动。telnet 和 SSH 控制台在 DRAC 5 上可通过 DRAC 模式使用（请参阅“DRAC 模式”）。任何时刻可以有多达四个 Telnet 客户系统和四个 SSH 客户端连接。到 Managed System serial 或 telnet 控制台的 Management Station 连接需要 Management Station 终端仿真软件。有关详情，请参阅“配置管理站终端仿真软件”。

以下小节解释了如何使用以下方法将 Management Station 连接到 Managed System：

- 使用终端软件和 DB-9 或零调制解调器电缆的 Managed System 外部串行端口
- 通过 Managed System DRAC 5 NIC 或共享、组 NIC 使用终端软件的 telnet 连接

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。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 4-11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 4-11。 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

DRAC 5 支持在运行以下某种终端仿真软件的 management station 上使用串行或 telnet 文本控制台：

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

执行以下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**”（**重设**）、“**connect**”（**连接**）和“**hangup**”（**挂断**）设置以使它们保留为空白。
12. 要保存每个空白值，按 <Enter>。
13. 清除完所有指定字段后，按 <Enter> 退出“**Modem Dialing and Parameter Setup**”（**调制解调器拨号和参数设置**）菜单。
14. 选择“**Save setup as config_name**”（**将设置另存为 config_name**）并按 <Enter>。
15. 选择“**Exit From Minicom**”（**从 Minicom 退出**）并按 <Enter>。
16. 在命令解释程序提示符处键入 `minicom <Minicom config 文件名>`。
17. 要将 Minicom 窗口展开为 80 x 25，拖动窗角。
18. 按 <Ctrl+a>, <z>, <x> 退出 Minicom。

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

确保 Minicom 窗口显示命令提示符，比如 `[DRAC 5\root]#`。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 4-12 配置任何版本的 Minicom。

表 4-12。 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 4-13 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 4-13。 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

确保 HyperTerminal 窗口显示命令提示符，比如 `[DRAC 5\root]#`。命令提示符出现后，表示连接成功并且您可以使用 **connect com2** serial 命令连接到 Managed System 控制台。

配置 Linux XTerm 进行 Telnet 控制台重定向

执行此部分中的步骤时应遵循以下原则：

- 通过 telnet 控制台使用 **connect com2** 命令显示系统设置屏幕时，在系统设置中将终端类型设置为 **ANSI** 并用于 telnet 会话。
- 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。

要在 Linux 中运行 telnet：

1. 启动新的 Xterm 会话。

   在命令提示符处，键入 `xterm &`

2. 单击 XTerm 窗口的右下角并将窗口的大小重新调整为 80 x 25。
3. 连接到 Managed System 中的 DRAC 5。

   在 Xterm 提示符处，键入 `telnet <DRAC 5 IP 地址>`

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 Management Station 中的 DRAC 5。

   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 DRAC 5 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
   ```

使用串行或 Telnet 控制台

Serial 和 **telnet** 命令以及 RACADM CLI 可以键入 serial 或 telnet 控制台并在服务器上本地或远程执行。本地 RACADM CLI 只安装供根用户使用。

使用 Windows XP 或 Windows 2003 运行 Telnet

如果 Management Station 运行 Windows XP 或 Windows 2003，会在 DRAC 5 telnet 会话中遇到字符问题。此问题会显示为冻结登录，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。

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/** 并搜索 "*Windows Services for UNIX 3.5*"。

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。DRAC 5 支持具有密码验证的 SSH 版本 2。安装或更新 DRAC 5 固件时，会在 DRAC 5 上启用 SSH。

在 Management Station 上既可以使用 PuTTY 也可以使用 OpenSSH 连接 Managed System 的 DRAC 5。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 DRAC 5 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 "DRAC 5 属性数据库组和对象定义" 中所述。

要在 DRAC 5 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 "DRAC 5 属性数据库组和对象定义"。

DRAC 5 SSH 实现支持多种密码模式，如表 4-14 中所示。

表 4-14。 密码模式

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

注： SSHv1 不支持。

配置 DRAC 5 网络设置

注意： 更改 DRAC 5 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 DRAC 5 网络设置：

- 基于 Web 的接口 — 请参阅 "配置 DRAC 5 NIC"
- RACADM CLI — 请参阅 “cfgLanNetworking”。
- Dell Remote Access 配置公用程序 — 请参阅 "配置系统使用 DRAC 5"

注： 如果准备在 Linux 环境中部署 DRAC 5，请参阅 “安装 RACADM”。

通过网络访问 DRAC 5

配置完 DRAC 5 后，可以使用以下某一界面来远程访问 managed system：

- 基于 Web 的界面
- RACADM
- Telnet 控制台
- SSH
- IPMI

表 4-15 说明了各个 DRAC 5 界面。

表 4-15。 DRAC 5 界面

接口	说明
基于 Web 的界面	提供了使用图形用户界面到 DRAC 5 的远程访问。基于 Web 的界面构建在 DRAC 5 固件中并从 management station 上的受支持 Web 浏览器通过 NIC 接口访问。 要了解受支持的 Web 浏览器列表，请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。
RACADM	提供了使用命令行界面到 DRAC 5 的远程访问。RACADM 使用 managed system 的 IP 地址执行 RACADM 命令（RACADM 远程功能选项 [-r]）。 **注：** racadm 远程功能只在 management station 上受支持。要了解受支持的 Web 浏览器列表，请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。 **注：** 使用 racadm 远程功能时，在使用涉及文件操作的 racadm 子命令的文件夹上必须具有写权限，例如： `racadm getconfig -f <文件名>` 或： `racadm sslcertupload -t 1 -f c:\cert\cert.txt` 子命令
Telnet 控制台	提供通过 DRAC 5 到服务器 RAC 端口的访问以及通过 DRAC 5 NIC 到硬件管理接口的访问，并提供对 serial 和 RACADM 命令的支持，包括 **powerdown**、**powerup**、**powercycle** 和 **hardreset** 命令。 **注：** Telnet 是一种以明文传送所有数据（包括密码）的非安全协议。发送敏感信息时，应使用 SSH 接口。
SSH 接口	使用更高安全保护的加密传输层，提供与 Telnet 控制台相同的功能。
IPMI 接口	提供通过 DRAC 5 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。请参阅《*Dell OpenManage 底板管理控制器用户指南*》了解有关详情。

注： DRAC 5 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 DRAC 5 NIC 访问 DRAC 5 基于 Web 的界面。

要了解受支持的 Web 浏览器列表，请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。

要使用 Server Administrator 访问 DRAC 5 远程访问接口，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》。

配置 DRAC 5 NIC

配置网络和 IPMI LAN 设置

注： 您必须具有**配置 DRAC 5** 权限才能执行以下步骤。

注： 大部分 DHCP 服务器需要一个服务器来将客户端标识符令牌存储在其保留表中。客户端（例如 DRAC 5）在 DHCP 协议过程中必须提供此令牌。对于 RAC，DRAC 5 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： 如果您的 managed system DRAC 在**"Shared"（共享）**或**"Shared with Failover"（与故障转移共享）**模式下配置，并且 DRAC 连接到启用了生成树协议 (STP) 的交换机，则当 STP 汇聚期间 Management Station 的 LOM 链路状态更改时，网络客户端将经历 20-30 秒连接延迟。

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）**页配置 DRAC 5 NIC 设置。

   表 4-16 和 表 4-17 说明了**网络配置**页上的**网络设置**和 **IPMI 设置**。
4. 完成后单击**"Apply Changes"（应用更改）**。
5. 单击相应的**"Network Configuration"（网络配置）**页按钮继续。请参阅表 4-18。

表 4-16。 网络设置

设置	说明
NIC 选择	显示选定的 NIC 模式（**"Dedicated"（专用）**、**"Shared with Failover"（与故障转移共享）**或**"Shared"（共享）**）。 默认设置为**"Dedicated"（专用）**。
MAC Address（MAC 地址）	显示 DRAC 5 MAC 地址。
启用 NIC	启用 DRAC 5 NIC 并激活此组中的其它控件。 默认设置为**已启用**。
"Use DHCP (For NIC IP Address)"（使用 DHCP [对于 NIC IP 地址]）	启用 Dell OpenManage™ Server Administrator 从动态主机配置协议 (DHCP) 服务器获得 DRAC 5 NIC IP 地址。选中复选框取消激活**" Static IP Address "（静态 IP 地址）**、**"Static Gateway"（静态网关）**和**"Static Subnet Mask"（静态子网掩码）**控件。 默认设置为**已禁用**。
"Static IP Address"（静态 IP 地址）	指定或编辑 DRAC 5 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 Gateway"（静态网关）	指定或编辑 DRAC 5 NIC 的静态网关。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）	指定或编辑 DRAC 5 NIC 的静态子网掩码。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。
"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）	从 DHCP 服务器获得主要 DNS 服务器地址和备用 DNS 服务器地址，而不是静态设置。 默认设置为**已禁用**。
"Static Preferred DNS Server"（静态首选 DNS 服务器）	仅当**未选择"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**时使用主要 DNS 服务器 IP 地址。
"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，则可以为该 IP 地址输入 0.0.0.0。
"Register DRAC on DNS"（向 DNS 注册 DRAC）	在 DNS 服务器上注册 DRAC 5 名称。 默认设置为**已禁用**。
"DNS DRAC Name"（DNS DRAC 名称）	只有选中**"Register DRAC 5 on DNS"（在 DNS 上注册 DRAC 5）**后才显示 DRAC 5 名称。默认 DRAC 5 名称是 RAC-服务标签，其中服务标签 是 Dell 服务器的服务标签编号（例如 RAC-EK00002）。
"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 DRAC 5 on DNS"（在 DNS 上注册 DRAC 5）**复选框，则可以在**"DNS Domain Name"（DNS 域名）**字段修改 DNS 域名。 默认设置为**已禁用**。

"DNS Domain Name"（DNS 域名）	默认 DNS 域名是 **MYDOMAIN**。如果选中 **"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）**复选框，此选项将会灰显并且将无法修改此字段。
"Auto Negotiation"（自动协商）	确定 DRAC 5 是否会通过与最近的路由器或集线器通信来自动设置 **"Duplex Mode"（双工模式）**和 **"Network Speed"（网络速度）**(**On**)，或者允许手动设置 **"Duplex Mode"（双工模式）**和 **"Network Speed"（网络速度）**(**Off**)。
"Network Speed"（网络速度）	将网络速度设置为 100 Mb 或 10 Mb 以满足网络环境。如果 **"Auto Negotiation"（自动协商）**设为 **On**，此选项将不可用。
"Duplex Mode"（双工模式）	将双工模式设置为全双工或半双工以满足网络环境。如果 **"Auto Negotiation"（自动协商）**设为 **On**，此选项将不可用。

表 4-17。 IPMI LAN 设置

设置	说明
启用 LAN 上 IPMI	启用 IPMI LAN 信道。
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）。
"Encryption Key"（密钥）	配置密钥字符格式：0 至 20 十六进制字符（不允许空白）。 默认设置为 **00000000000000000000**。
启用 VLAN ID	启用 VLAN ID。如果启用，将仅接受匹配的 VLAN ID 通信。
VLAN ID	802.1g 字段中的 VLAN ID 字段。
优先权	802.1g 字段中的优先权字段。

表 4-18。 网络配置页按钮

按钮	说明
"Print"（打印）	打印 **"Network Configuration"（网络配置）**页。
"Refresh"（刷新）	重新载入 **"Network Configuration"（网络配置）**页。
"Advanced Settings"（高级设置）	显示 **"Network Security "（网络安全性）**页。
"Apply Changes"（应用更改）	将所做更改保存到网络配置。 **注：** 更改 NIC IP 地址设置将关闭所有用户会话，并要求用户使用更新的 IP 地址设置重新连接到 DRAC 5 基于 Web 的界面。所有其他更改将要求重设 NIC，这可能导致丢失连接。

有关详情，请参阅 "使用 DRAC 5 GUI 配置网络安全设置"。

远程使用 RACADM

注： 使用 racadm 远程功能前请配置 DRAC 5 上的 IP 地址。有关设置 DRAC 5 的详情以及相关文档的列表，请参阅 "DRAC 5 的基本安装"。

RACADM 提供远程功能选项 (**-r**)，可以允许连接 managed system 和从远程控制台和 management station 执行 **racadm** 子命令。要使用远程功能，您需要有效用户名（**-u** 选项）和密码（**-p** 选项）和 DRAC 5 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 DRAC 认证，则在键入 racadm 命令时会显示一条消息。

```
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）
```

```
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。

EORROR：无法按照指定 IP 地址连接到 RAC。

注： racadm 远程功能只在 management station 上受支持。有关详情，请参阅 Dell 支持网站 support.dell.com 上的 Dell 系统软件支持值表。

注： 使用 racadm 远程功能时，在使用涉及文件操作的 racadm 子命令的文件夹上必须具有写权限，例如：

racadm getconfig -f <文件名>

或

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

RACADM 提要

racadm -r <*RAC IP 地址*> -u <*用户名*> -p <*密码*> <*子命令*> <*子命令选项*>

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

racadm -i -r <*RAC IP 地址*>:<*端口*> <*子命令*> <*子命令选项*>

RACADM 选项

表 4-19 列出 **racadm** 命令的选项。

表 4-19。 racadm 命令选项

选项	说明
-r <raclpAddr> **-r <raclpAddr>:<**端口号**>**	指定控制器的远程 IP 地址。 用法：<端口号> 如果 DRAC 5 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 4-20 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”。

输入 RACADM 子命令时，请在命令前加上 racadm。例如：

```
racadm help
```

表 4-20。 RACADM 子命令

命令	说明
help	列出 DRAC 5 子命令。
help <子命令>	列出指定子命令的用法语句。
arp	显示 ARP 表的内容。ARP 表条目不能被添加或删除。
clearasrscreen	清除上一个 ASR（崩溃）屏幕（上一个蓝色屏幕）。
clrraclog	清除 DRAC 5 日志。单个条目被用来指示清除日志的用户和时间。
config	配置 RAC。
getconfig	显示当前 RAC 配置属性。
coredump	显示最后一次 DRAC 5 信息转储。
coredumpdelete	删除 DRAC 5 中存储的信息转储。
fwupdate	执行或显示 DRAC 5 固件更新的状况。
getssninfo	显示关于活动会话的信息。
getsysinfo	显示一般 DRAC 5 和系统信息。
getractime	显示 DRAC 5 时间。
ifconfig	显示当前 RAC IP 配置。
netstat	显示路径选择表和当前连接。
ping	验证目标 IP 地址是否可以使用当前路由选择表的内容从 DRAC 5 访问。
setniccfg	设置控制器的 IP 配置。
getniccfg	显示控制器的当前 IP 配置。
getsvctag	显示服务标签。
racdump	转储 DRAC 5 状况和状态信息以进行调试。
racreset	重设 DRAC 5。

racresetcfg	将 DRAC 5 重设为默认配置。
serveraction	在 managed system 上执行电源管理操作。
getraclog	显示 RAC 日志。
clrsel	清除系统事件日志条目。
gettracelog	显示 DRAC 5 跟踪日志。如果随 -i 使用，则命令显示 DRAC 5 跟踪日志中的条目数。
sslcsrgen	生成并下载 SSL CSR。
sslcertupload	将 CA 认证或服务器认证上载至 DRAC 5。
sslcertdownload	下载 CA 认证。
sslcertview	查看 DRAC 5 中的 CA 认证或服务器认证。
testemail	强制 DRAC 5 通过 DRAC 5 NIC 发送检测电子邮件来检查电子邮件配置。
testtrap	强制 DRAC 5 通过 DRAC 5 NIC 发送检测 SNMP 陷阱来检查陷阱配置。
vmdisconnect	强制关闭虚拟介质连接。
vmkey	将虚拟闪速更新大小重设为默认大小 (16 MB)。

有关 RACADM 错误消息的常见问题

执行 DRAC 5 重设后（使用 racadm racreset 命令），我发出了一个命令，结果显示以下信息：

racadm <命令名称> Transport: ERROR: (RC=-1)

这条信息是什么意思？

必须等待 DRAC 5 完成重设，然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：

- Local racadm 错误信息 — 类似语法、拼写错误和错误名称的问题。
- Remote 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。

当从我的系统 ping DRAC IP 地址然后在 ping 响应过程中在专用和共享模式之间切换 DRAC 5 卡时，我没有收到响应。

清除系统上的 ARP 表。

配置多个 DRAC 5 卡

使用 RACADM 可以配置一个或多个具有相同属性的 DRAC 5 卡。使用组 ID 和对象 ID 查询特定 DRAC 5 卡时，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 DRAC 5 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 DRAC 5 信息（如静态 IP 地址），在将文件导出到其他 DRAC 5 卡之前必须修改这些信息。

要配置多个 DRAC 5 卡，请执行以下过程：

1. 使用 RACADM 查询包含相应配置的目标 DRAC 5。

   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 RAC 配置重定向至文件仅对本地和远程 RACADM 界面支持。

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 RAC。

在命令提示符处键入：

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

4. 重设已配置的目标 RAC。

在命令提示符处键入：

```
racadm reset
```

getconfig -f racadm.cfg 子命令请求 DRAC 5 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：

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

config 子命令将信息加载到其他 DRAC 5 中。使用 **config** 与 Server Administrator 同步用户和密码数据库

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
```

注意： 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，都可能损坏 racadm 数据库。

创建 DRAC 5 配置文件

DRAC 5 配置文件 <文件名>**.cfg** 用于 racadm config -f <文件名>.cfg 命令。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 DRAC 5。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：

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

注： 请参阅 “getconfig”了解关于 **getconfig** 命令的信息。

将首先分析 **.cfg** 文件以验证有效的组和对象名称是否存在，然后实施一些简单的语法规则。错误标记有在其中检测到错误的行号，并且有一条简单的信息解释该问题。将分析整个文件的正确性，并显示所有错误。如果在 **.cfg** 文件中找到错误，写入命令将不传输到 DRAC 5。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 DRAC 5 执行写入操作。

创建 **.cfg** 文件时请使用以下原则：

- 如果分析器遇到索引组，区分各个索引的将是锚定对象的值。

  分析器将从 DRAC 5 读入该组的所有索引。配置 DRAC 5 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 DRAC 5 上创建。

- 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 DRAC 5 上可以正确分析和运行的 **.cfg** 文件可能无法在其它 DRAC 5 上正确运行。

- 使用 **racresetcfg** 子命令配置所有具有相同属性的 DRAC 5 卡。

  使用 **racresetcfg** 子命令将 DRAC 5 重设为初始默认值，然后运行 `racadm config -f <文件名>.cfg` 命令。确保 **.cfg** 文件中包含所有所需的对象、用户、索引和其它参数。

注意： 使用 **racresetcfg** 子命令将数据库和 DRAC 5 NIC 设置重设为初始默认设置并删除所有用户和用户配置。尽管根用户可用，但也会将其他用户的设置重设为默认设置。

分析规则

- 所有以“#”开头的行将被视为注释。

  注释行必须在第一列中开始。任何其他列中的“#”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 DRAC 5 执行 `racadm config -f <文件名>.cfg` 命令，而不添加转义字符。

  示例：

  ```
  #

  # 这是一条注释。

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<调制解调器初始化字符串中的 # 不是注释>
  ```

- 所有组条目必须括在“**[**”和“**]**”字符中。

  表示组名称的开头“**[**”字符*必须*在第一列中开始。此组名称*必须*在该组中的任何对象之前指定。没有关联组名的对象将导致错误。配置数据按 "DRAC 5 属性数据库组和对象定义" 中的定义分组。

  以下示例显示了组名称、对象以及对象的属性值。

  示例：

  ```
  [cfgLanNetworking] -{组名称}
  ```

cfgNicIpAddress=143.154.133.121 {*对象名称*}

- 所有参数都指定为“对象=值”对，在对象、= 或值之间不留空格。

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

请参见上一列表项中的实例。

- **.cfg** 分析器忽略索引对象条目。

用户无法指定使用哪个索引。如果索引已存在，则使用该索引，否则将在该组的第一个可用索引中创建新条目。

racadm getconfig -f <*文件名*>.cfg 命令将注释放置在索引对象前，允许用户查看包含的注释。

注： 可以使用以下命令手动创建索引组：
racadm config -g <组名称> -o <锚定对象> -i <索引 1-16> <唯一定位标记名称>

- 无法从 **.cfg** 文件中删除索引组的行。

用户必须使用以下命令手动删除索引对象：

racadm config -g <*组名称*> -o <*对象名称*> -i <*索引 1-16*> ""

注： 空字符串（两个 "" 字符表示）指示 DRAC 5 删除指定组的索引。

要查看索引组的内容，请使用以下命令：

racadm getconfig -g <*组名称*> -i <*索引 1-16*>

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

[cfgUserAdmin]

cfgUserAdminUserName=<用户名>

如果键入 racadm getconfig -f <myexample>.cfg，则命令为当前 DRAC 5 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 DRAC 5 IP 地址

修改配置文件中的 DRAC 5 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 DRAC 5 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输入 <Ctrl><e> 时 option ROM 所提供的功能一样。有关使用 option ROM 配置网络属性的详情，请参阅 "配置 DRAC 5 网络属性"。

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**，则禁用 DRAC 5 LAN，即使启用了 DHCP。

DRAC 模式

DRAC 5 可以配置为三种模式：

- 专用
- 共享
- 与故障转移共享

表 4-21 提供了各种模式的说明。

表 4-21。 DRAC 5 NIC 配置

模式	说明
专用	DRAC 使用自己的 NIC（RJ-45 连接器）和 BMC MAC 地址用于网络通信。
共享	DRAC 在平台上使用 Broadcom LOM1。
与故障转移共享	DRAC 使用 Broadcom LOM1 和 LOM2 作为故障转移组。该组使用 BMC MAC 地址。

常见问题

访问 DRAC 5 基于 Web 的界面时，得到一个安全警告，指出 SSL 认证的主机名与 DRAC 5 的主机名不匹配。

DRAC 5 包括了一个默认的 DRAC 5 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 **DRAC5 默认认证**的，它与 DRAC 5 的主机名不匹配（例如，IP 地址）。

要解决这个安全问题，应上载一个颁发给 DRAC 5 IP 地址的 DRAC 5 服务器认证。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 DRAC 5 的 IP 地址（例如，192.168.0.120）或注册的 DNS DRAC 名称匹配。

要确保 CSR 匹配注册的 DNS DRAC 名称：

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 Settings”（网络设置）**页：
   a. 选中**“Register DRAC on DNS”（向 DNS 注册 DRAC）**复选框。
   b. 在**“DNS DRAC Name”（DNS DRAC 名称）**字段，输入 DRAC 名称。
4. 单击**“Apply Changes”（应用更改）**。

请参阅 "使用 SSL 和数字认证确保 DRAC 5 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？

重设 DRAC 5 Web Server 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。

DRAC 5 Web Server 会在发生以下情况后重设：

- 使用 DRAC 5 Web 用户界面更改网络配置或网络安全性属性时
- 更改 **cfgRacTuneHttpsPort** 属性时（包括 config -f 配置文件> 更改它时）
- 使用 **racresetcfg** 时
- 重设 DRAC 5 时
- 上载新的 SSL 服务器认证时

为什么我的 DNS 服务器没有注册 DRAC 5？

有些 DNS 服务器只注册 31 个或更少字符的名称。

访问 DRAC 5 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。

DRAC 5 包括了一个默认的 DRAC 5 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 Thawte 或 Verisign）颁发的 DRAC 5 服务器认证。请参阅 "使用 SSL 和数字认证确保 DRAC 5 通信" 了解有关颁发认证的详情。

目录

目录

添加和配置 DRAC 5 用户

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 使用 RACADM 公用程序配置 DRAC 5 用户

要用 DRAC 5 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*。要实现更多安全性，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。

添加和配置 DRAC 5 用户：

注： 您必须具有配置 DRAC 5 权限才能执行以下步骤。

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**“Users”（用户）**。

   “Users”（用户）页将会显示，其中包括每个用户的**“State”（状态）**、**“User Name”（用户名）**、**“RAC Privilege”（RAC 权限）**、**“IPMI LAN Privilege”（IPMI LAN 权限）**、**“IPMI Serial Privilege”（IPMI 串行权限）**和**“Serial Over LAN”（LAN 上串行）**。
3. 在**“User ID”（用户 ID）**列单击用户 ID 编号。
4. 在**“User Main Menu”（用户主菜单）**页，可以配置用户，上载用户认证，查看现有用户认证，上载可信认证机构 (CA) 认证或查看可信 CA 认证。

   如果选择**“Configure User”（配置用户）**并单击**“Next”（下一步）**，“User Configuration”（用户配置）页将会显示。有关详情，请参阅步骤 5。

   如果选择**“Smart Card Configuration”（Smart Card 配置）**部分下的选择，则请参阅表 5-1。
5. 在**“User Configuration”（用户配置）**页中配置用户的属性和权限。

   表 5-2 说明配置新的或现有 DRAC 用户名和密码的**“General”（常规）**设置。

   表 5-3 说明**“IPMI User Privileges ”（IPMI 用户权限）**以供配置用户 LAN 权限。

   表 5-4 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 5-5 说明 **“**DRAC Group”（DRAC 组）权限。如果将 DRAC 用户权限添加到管理员、高级用户或客用户，**“DRAC Group”（DRAC 组）**将更改为**“Custom”（自定义）**组。
6. 完成后单击**“Apply Changes”（应用更改）**。
7. 单击相应的**“User Configuration”（用户配置）**页按钮继续。请参阅表 5-6。

表 5-1。 Smart Card 配置部分中的选项

选项	说明
上载用户认证	使您能够将用户认证上载到 DRAC 并导入用户配置文件。
查看用户认证	显示已上载到 DRAC 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 DRAC 并导入用户配置文件。
查看可信 CA 认证	显示已上载到 DRAC 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 5-2。 常规属性

属性	说明
用户 ID	指定 16 个预置用户 ID 编号之一。 如果您编辑用户 root 的信息，则此字段为静态字段。不能编辑 root 的用户名。
启用用户	启用用户访问 DRAC 5。取消选取后，不能更改用户名。
用户名	指定一个 DRAC 5 用户名，最多 16 个字符。每个用户必须具有唯一用户名。 **注：** 本地 DRAC 5 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）	指定或编辑 DRAC 5 用户密码。
"Confirm New Password"（确认新密码）	要求重新输入 DRAC 5 用户的密码进行确认。

表 5-3。 IPMI 用户权限

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

表 5-4。 DRAC 用户权限

属性	说明
"DRAC Group"（DRAC 组）	指定用户的最大 DRAC 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 5-5 了解 **DRAC 组**权限。
"Login to DRAC"（登录到 DRAC）	允许用户登录到 DRAC。
"Configure DRAC"（配置 DRAC）	允许用户配置 DRAC。
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 DRAC 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 5-5。 DRAC 组权限

用户组	授予的权限
管理员	登录到 DRAC、配置 DRAC、配置用户、清除日志、执行服务器控制命令、访问控制台重定向、访问虚拟介质、测试警报、执行诊断命令
高级用户	登录到 DRAC、清除日志、执行服务器控制命令、访问控制台重定向、访问虚拟介质、测试警报
客用户	"Login to DRAC"（登录到 DRAC）
"Custom"（自定义）	选择以下权限的任意组合：登录到 DRAC、配置 DRAC、配置用户、清除日志、执行服务器动作命令、访问控制台重定向、访问虚拟介质、测试警报、执行诊断命令
无	没有分配权限

表 5-6。 用户配置页按钮

按钮	措施
"Print"（打印）	打印 **"User Configuration"（用户配置）**页
"Refresh"（刷新）	重载 **"User Configuration"（用户配置）**页

"Go Back To Users Page"（退回到用户页）	返回 **"Users Page"（用户页）**。
"Apply Changes"（应用更改）	将所做更改保存到网络配置。

使用 RACADM 公用程序配置 DRAC 5 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。

DRAC 5 基于 Web 的界面是配置 DRAC 5 的最快方式。如果选择命令行或脚本配置或需要配置多个 DRAC 5，请使用随 DRAC 5 代理安装在 managed system 上的 RACADM。

要配置多个具有相同配置设置的 DRAC 5，请执行以下过程之一：

- 参考本节中的 RACADM 示例，创建一个 **racadm** 命令的批处理文件，然后在各个 managed system 上执行该批处理文件。
- 按 "RACADM 子命令概览" 中所述创建 DRAC 5 配置文件并使用同一配置文件在各个 managed system 上执行 **racadm config** 子命令。

开始之前

最多可以在 DRAC 5 属性数据库中配置多达 16 个用户。手动启用 DRAC 5 用户前，请验证当前用户是否存在。如果配置新 DRAC 5 或运行 **racadm racresetcfg** 命令，则当前唯一用户为 root 密码 calvin。**racresetcfg** 子命令将 DRAC 5 重设回原始默认值。

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

注： 可以随时启用和禁用用户。因此，用户在各个 DRAC 5 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 DRAC 5 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 DRAC 5。

添加 DRAC 5 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. 设置用户权限。
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 cfgUserPrivilege 0x00000001
```

```
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 DRAC 5 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 DRAC 5 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

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 "**testemail**" 子命令说明来配置这些设置。

启用带有权限的 DRAC 5 用户

要启用带有特定管理权限（基于角色授权）的用户，首先按照 "开始之前" 中的步骤找到可用用户索引。接着，键入以下带有新用户名和密码的命令行。

注： 请参阅 表 B-2 查看特定用户权限的有效位掩码值列表。默认权限值为 0，表示用户没有启用任何权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <索引> <用户权限位掩码值>
```

目录

目录

将 DRAC 5 用于 Microsoft Active Directory

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 为 DRAC 5 启用 Active Directory 身份验证的前提条件
- 支持的 Active Directory 身份验证机制
- 标准架构 Active Directory 概述
- 扩展架构 Active Directory 概述
- 配置和管理 Active Directory 认证
- 在域控制器上启用 SSL
- 支持的 Active Directory 配置
- 使用 Active Directory 登录到 DRAC 5
- 使用 Active Directory 单一式登录
- 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。如果公司已在使用 Microsoft® Active Directory® 服务软件，则可以配置软件提供对 DRAC 5 的访问，以允许控制和将 DRAC 5 用户权限添加到 Active Directory 软件中的现有用户。

注： 使用 Active Directory 识别 DRAC 5 用户在 Microsoft Windows® 2000、Windows Server® 2003 和 Windows Server 2008 操作系统上受支持。

为 DRAC 5 启用 Active Directory 身份验证的前提条件

要使用 DRAC 5 的 Active Directory 身份验证功能，必须已部署有 Active Directory 基础架构。DRAC 5 Active Directory 身份验证支持单个目录林中多个树间的身份验证。请参阅 "支持的 Active Directory 配置" 了解支持的对应于域功能级别、组、对象等的 Active Directory 配置。

请参阅 Microsoft 网站了解如何设置 Active Directory 基础架构（如果尚未有）。

DRAC 5 使用标准公共密钥基础架构 (PKI) 机制来安全验证 Active Directory，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

可以使用 Active Directory 通过两种方法在 DRAC 5 上定义用户权限：可以使用*标准架构*解决方案，该方案只使用 Active Directory 组对象，或者可以使用*扩展架构*解决方案，该方案经过 Dell 自定义加入 Dell 定义的 Active Directory 对象。有关这些解决方案的详情，请参阅以下部分。

使用 Active Directory 配置 DRAC 5 权限时，必须选择扩展架构或标准架构解决方案。

使用标准架构解决方案的优势有：

- 无需架构扩展，因为标准架构只使用 Active Directory 对象。
- Active Directory 一端的配置很简单。

使用扩展架构解决方案的优势有：

- 所有权限控制对象都在 Active Directory 中。
- 在不同 DRAC 5 卡上用不同权限级别配置用户权限的最大灵活性。

标准架构 Active Directory 概述

如 图 6-1 中所示，为 Active Directory 集成使用标准架构需要在 Active Directory 和 DRAC 5 上都进行配置。在 Active Directory 端，标准组对象用作角色组。具有 DRAC 5 权限的用户将是角色组的一员。为了将该用户权限授予特定 DRAC 5 卡，需要在特定 DRAC 5 上配置角色组名称及其域名称。与扩展架构解决方案不同，角色和权限级别在各个 DRAC 5 卡上定义，而不是在 Active Directory 中。每个 DRAC 5 中最多可以配置和定义五个角色组。 表 6-12 显示了角色组的权限级别而 表 6-1 显示了默认角色组设置。

图 6-1。 用 Microsoft Active Directory 和 Standard Schema 配置 DRAC 5

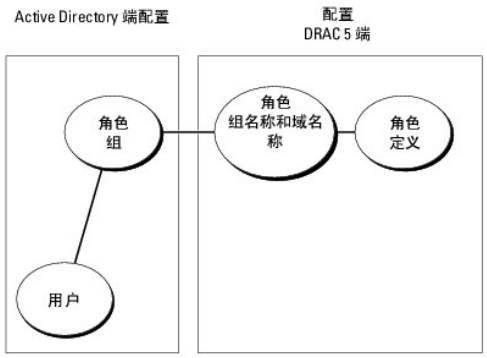


表 6-1。 默认角色组权限

角色组	默认权限级别	授予的权限	位掩码
角色组 1	管理员	登录到 DRAC、配置 DRAC、配置用户、清除日志、执行服务器控制命令、访问控制台重定向、访问虚拟介质、测试警报、执行诊断命令	0x000001ff
角色组 2	高级用户	登录到 DRAC、清除日志、执行服务器控制命令、访问控制台重定向、访问虚拟介质、测试警报	0x000000f9
角色组 3	客用户	"Login to DRAC"（登录到 DRAC）	0x00000001
角色组 4	无	没有分配权限	0x00000000
角色组 5	无	没有分配权限	0x00000000

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

有两种方式启用标准架构 Active Directory：

- 用 DRAC 5 基于 web 的用户界面。请参阅 "配置 DRAC 5 使用标准架构 Active Directory 和 基于 Web 的界面"。
- 用 RACADM CLI 工具。请参阅 "配置 DRAC 5 使用标准架构 Active Directory 和 RACADM"。

配置标准架构 Active Directory 访问 DRAC 5

需要执行以下步骤来配置 Active Directory，然后 Active Directory 用户才能访问 DRAC 5：

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。组的名称和该域的名称需要使用基于 web 的界面或 RACADM 在 DRAC 5 上配置（请参阅 "配置 DRAC 5 使用标准架构 Active Directory 和 基于 Web 的界面" 或 "配置 DRAC 5 使用标准架构 Active Directory 和 RACADM"）。
3. 将 Active Directory 用户添加为 Active Directory 组的成员以访问 DRAC 5。

配置 DRAC 5 使用标准架构 Active Directory 和 基于 Web 的界面

1. 打开一个支持的 Web 浏览窗口。
2. 登录到 DRAC 5 基于 Web 的界面。

3. 展开**系统**树并单击**“Remote Access”（远程访问）**。
4. 单击**“Configuration”（配置）**选项卡并选择 **Active Directory**。
5. 在 **Active Directory 主菜单**页中选择**“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）**。组名称标识 Active Directory 中与 DRAC 5 卡相关联的角色组。
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 6-12 说明了“Role Group Privileges”（角色组权限）。

    表 6-13 说明了“Role Group Permissions”（角色组特权）。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 Root CA 认证上载到 DRAC 5。
    a. 选中**“Upload Active Directory CA Certificate”（上载 Active Directory CA 认证）**复选框，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。确保根 CA 认证位于用来访问 DRAC 5 的 management station 上（请参阅 "导出域控制器根 CA 认证到 DRAC 5"）。
    c. 单击“Apply”（应用）。

    DRAC 5 Web server 将在单击**“Apply”（应用）**后自动重新启动。
17. 注销，然后登录 DRAC 5 以完成 DRAC 5 Active Directory 功能配置。
18. 在**系统**树中，单击**“Remote Access”（远程访问）**。
19. 单击“Configuration”（配置）选项卡，然后单击“Network”（网络）。

    系统将显示**“Network Configuration”（网络配置）**页。
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）**。

    DRAC 5 标准架构 Active Directory 功能配置完成。

配置 DRAC 5 使用标准架构 Active Directory 和 RACADM

通过 RACADM CLI 而不是基于 Web 的界面，使用以下命令配置 DRAC 5 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 <完全限定的 root 域名>

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号>

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

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

   注： 有关位掩码编号值，请参阅 表 B-4。

2. 如果 DRAC 5 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 DRAC 5 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>
```

扩展架构 Active Directory 概述

有两种方式启用扩展架构 Active Directory：

- 用 DRAC 5 基于 web 的用户界面。请参阅“配置 DRAC 5 使用扩展架构 Active Directory 和 基于 Web 的界面”。
- 用 RACADM CLI 工具。请参阅“配置 DRAC 5 使用扩展架构 Active Directory 和 RACADM”。

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。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

Microsoft 维护的 Active Directory OID 数据库可以在 http://msdn.microsoft.com/certification/ADAcctInfo.asp 通过输入我们的扩展 Dell 来查看。

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

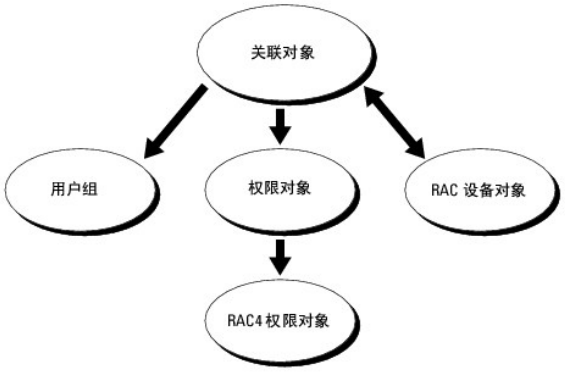
对于网络上每一个想与 Active Directory 集成以进行验证和授权的物理 RAC 来说，请创建至少一个关联对象和一个 RAC 设备对象。可以创建多个“关联”对象，每个“关联”对象都可以链接到任意多个用户、用户组或 RAC“设备”对象。用户和 RAC 设备对象可以是企业任何域中的成员。

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 6-2说明关联对象提供了进行所有验证和授权所需的连接。

图 6-2。 Active Directory 对象的典型设置



注： RAC 权限对象适用于 DRAC 4 和 DRAC 5。

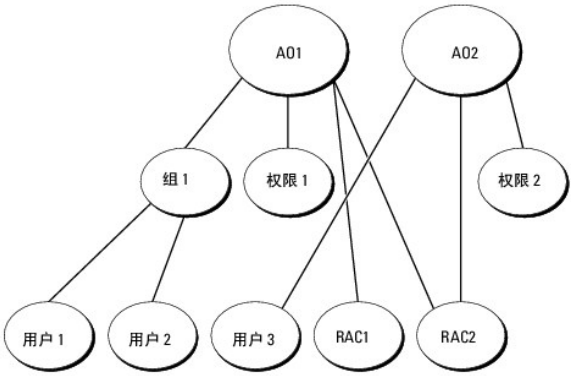
可以根据需要创建任意数量的关联对象。不过，对于网络上每一个想与 Active Directory 集成以使用 RAC (DRAC 5) 验证和授权的 RAC (DRAC 5) 来说，必须创建至少一个“关联”对象和一个 RAC“设备”对象。

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 (DRAC 5) 具有“权限”的“用户”。

此外，可以在一个域或多个域中配置 Active Directory 对象。例如，已有两个 DRAC 5 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 DRAC 5 卡的管理员权限并授予用户 3 对 RAC2 卡的登录权限。 图 6-3 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 6-3。 在一个域中设置 Active Directory 对象



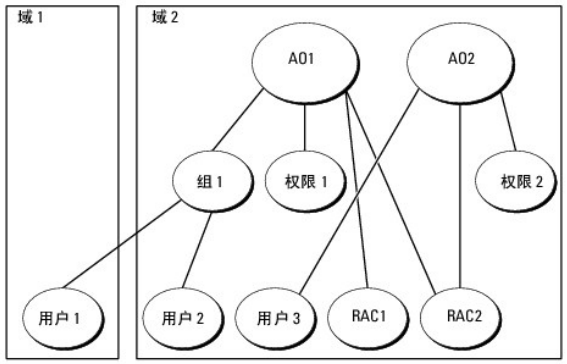
要为单个域情况配置对象，请执行以下任务：

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 DRAC 5 卡。
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 DRAC 5 用户和权限添加到 Active Directory”。

图 6-4 提供多个域中 Active Directory 对象的示例。在这种情况下，已有两个 DRAC 5 卡（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 DRAC 5 卡的管理员权限，配置用户 3 具有对 RAC2 卡的登录权限。

图 6-4。 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 6-4 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 DRAC 5 卡。
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 DRAC 5

在使用 Active Directory 访问 DRAC 5 之前，必须配置 Active Directory 软件和 DRAC 5，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 DRAC 5 用户及其权限添加到 Active Directory（请参阅"将 DRAC 5 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 DRAC 5 基于 Web 的界面或 RACADM 配置 DRAC 5 Active Directory 属性（请参阅"配置 DRAC 5 使用扩展架构 Active Directory 和 基于 Web 的界面"或"配置 DRAC 5 使用扩展架构 Active Directory 和 RACADM"）。

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：

- Dell Schema Extender 公用程序

- LDIF 脚本文件

如果使用 LDIF 脚本，将不会把 Dell 组织单元添加到架构。

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

- DVD 驱动器：**\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- DVD 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**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：

- 类（请参阅 表 6-2 到 表 6-7）
- 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 DRAC 5 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 DRAC 5 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设权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser 如果用户具有设备的控制台重定向权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser 如果用户具有设备的虚拟介质权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser 如果用户具有设备的检测警报用户权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin 如果用户具有设备的调试命令管理员权限，则为 TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion 当前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 (DRAC 5) 设备、用户和用户组、RAC 关联和 RAC 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 **“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 DRAC 5 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：

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 DRAC 5 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 DRAC 5 用户和权限。要添加每个对象类型，请执行以下过程：

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

创建 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"配置 DRAC 5 使用扩展架构 Active Directory 和 基于 Web 的界面 "的步骤 a中键入的 DRAC 5 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（有关详情请参阅表 5-4）。

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**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）。

配置 DRAC 5 使用扩展架构 Active Directory 和基于 Web 的界面

1. 打开一个支持的 Web 浏览窗口。
2. 登录到 DRAC 5 基于 Web 的界面。
3. 展开**系统**树并单击**“Remote Access”（远程访问）**。
4. 单击**“Configuration”（配置）**选项卡并选择 **Active Directory**。
5. 在 **Active Directory 主菜单**页中选择**“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 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创建的 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 drac5.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. 将域目录林 Root CA 认证上载到 DRAC 5。
    a. 选中**“Upload Active Directory CA Certificate”（上载 Active Directory CA 认证）**复选框，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 DRAC 5 的 management station 上准备好根 CA 认证（请参阅 "导出域控制器根 CA 认证到 DRAC 5"）。
    c. 单击“Apply”（应用）。

    DRAC 5 Web server 将在单击**“Apply”（应用）**后自动重新启动。
12. 注销，然后登录 DRAC 5 以完成 DRAC 5 Active Directory 功能配置。
13. 在**系统**树中，单击**“Remote Access”（远程访问）**。
14. 单击“Configuration”（配置）选项卡，然后单击“Network”（网络）。

    系统将显示**“Network Configuration”（网络配置）**页。
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）**。

    DRAC 5 扩展架构 Active Directory 功能配置完成。

配置 DRAC 5 使用扩展架构 Active Directory 和 RACADM

使用以下命令以通过 RACADM CLI 工具而不是基于 Web 的界面配置 DRAC 5 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 <完全限定的 rac 域名>
```

```
racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全限定的 root 域名>
```

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

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

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

2. 如果想指定 LDAP、全局编目服务器或关联对象域，而不是使用 DNS 服务器返回的服务器来搜索用户名，则键入以下命令启用“**Specify Server”（指定服务器）**选项：

```
racadm config -g cfgActive Directory -o cfgADSpecifyServer Enable 1
```

注： 如果使用此选项，CA 认证中的主机名将不会与指定服务器的名称进行匹配。这对于 DRAC 管理员特别有用，因为既可以输入主机名，也可以输入 IP 地址。

启用“**Specify Server”（指定服务器）**选项后，可以用服务器的 IP 地址或完全限定域名 (FQDN) 来指定 LDAP 服务器或全局编目服务器。FQDN 包含服务器的主机名和域名。

注： 如果在使用基于 Kerberos 的 Active Directory 身份验证，则只指定服务器的 FQDN；不支持指定 IP 地址。有关详情，请参阅“启用 Kerberos 验证”。

要使用命令行接口 (CLI) 指定 LDAP 服务器，则键入：

```
racadm config -g cfgActive Directory -o cfgADDomainController <完全限定域名或 IP 地址>
```

要使用命令行接口 (CLI) 指定全局编目服务器，则键入：

```
racadm config -g cfgActive Directory -o cfgGlobalCatalog <完全限定域名或 IP 地址>
```

要使用命令行接口 (CLI) 指定关联对象域，则键入：

```
racadm config -g cfgActive Directory -o cfgAODomain <域>:<完全限定域名或 IP 地址>
```

其中 <域> 是关联对象所在的域，而 IP/FQDN 是 DRAC 5 所连指定主机（域的域控制器）的 IP 地址或 FQDN。

要指定关联对象，应确保还提供全局编目的 IP 或 FQDN。

注： 如果指定 IP 地址 0.0.0.0，DRAC 5 将不会搜索任何服务器。

可以用逗号分隔来指定一列 LDAP、全局编目服务器或关联对象。DRAC 5 允许指定多达四个 IP 地址或主机名。

如果没有为所有域和应用程序正确配置 LDAPS，启用该功能会在现有应用程序/域运行期间产生难以预料的结果。

如果在 DRAC 上的“**Specify Server**”（**指定服务器**）选项下配置域控制器，并且如果关联对象包含同一个域上的用户和 RAC 对象，使用扩展架构的 Active Directory 登录将会成功。不过，如果关联上的用户或 RAC 对象来自不同域，并且如果只提供域控制器信息，使用扩展架构的 Active Directory 登录将会失败。在这种情况下，应配置全局编目选项以便能够登录。

3. 如果 DRAC 5 上已启用 DHCP 并且希望使用 DHCP 服务器提供的 DNS，则键入以下 racadm 命令：

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

4. 如果 DRAC 5 上已禁用 DHCP 或者想手动输入 DNS IP 地址，则键入以下 racadm 命令：

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

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

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

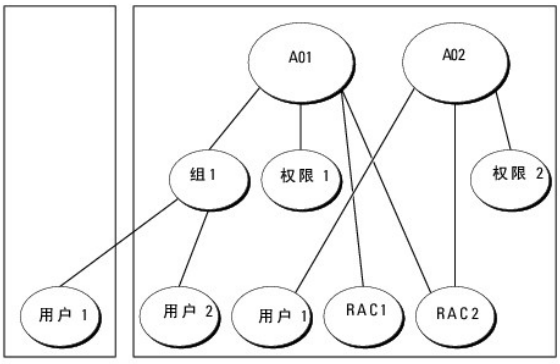
5. 按“**Enter**”（**输入**）完成 DRAC 5 Active Directory 功能配置。

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 6-5提供了使用扩展架构累积权限的示例。

图 6-5。 用户权限累积



该图显示两个关联对象—A01 和 A02。这些关联对象可能属于相同或不同的域。用户 1 通过关联对象与 RAC1 和 RAC2 关联。因此，用户 1 具有累积权限，将权限 1 和权限 2 的权限合并起来。

例如，权限 1 具有这些权限：登录、虚拟介质和清除日志，而权限 2 具有的权限：登录、配置 DRAC 和检测警报。用户 1 现在就具有权限：登录、虚拟介质、清除日志、配置 DRAC 和检测警报，这是权限 1 和权限 2 的权限合集

扩展架构验证，因此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。

配置和管理 Active Directory 认证

访问 Active Directory 主菜单：

1. 展开**系统**树并单击**“Remote Access”（远程访问）**。
2. 单击**“Configuration”（配置）**选项卡并单击 **Active Directory**。

表 6-9列出 **Active Directory 主菜单**页选项。

表 6-9。 Active Directory 主菜单页选项

字段	说明
“Configure Active Directory”（配置 Active Directory）	配置 Active Directory 的 DRAC 名称、ROOT 域名、DRAC 域名、Active Directory 验证超时、Active Directory 架构选择和角色组设置。
“Upload Active Directory CA Certificate”（上载 Active Directory CA 认证）	将 Active Directory 认证上载到 DRAC。
“Download DRAC Server Certificate”（下载 DRAC 服务器认证）	使用 Windows 下载管理器可将 DRAC 服务器认证下载到系统。
“View Active Directory CA Certificate”（查看 Active Directory CA 认证）	显示已上载到 DRAC 的 Active Directory 认证。

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 and Management”（Active Directory 配置和管理）**页中输入 Active Directory 设置。

   表 6-10 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. 单击相应的**“Active Directory Configuration”（Active Directory 配置）**页按钮继续。请参阅表 6-11。
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 6-12和表 6-13。

注： 要保存“Active Directory Configuration and Management”（Active Directory 配置和管理）页上的设置，必须单击“ Apply”（应用）然后才能进入“Custom Role Group”（自定义角色组）页。

表 6-10。 Active Directory 配置和管理页设置

设置	说明
“Enable Active Directory”（启用 Active Directory）	启用 Active Directory。选中=启用；未选中=禁用。
“ROOT Domain Name”（ROOT 域名）	Active Directory ROOT 域名。该值默认为 **NULL**。 名称必须是包含 *x.y* 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、org。
“Timeout”（超时）	等待 Active Directory 查询完成需要的秒数。最小值等于或大于 15 秒。默认值为 120 秒。
使用标准架构	为 Active Directory 使用标准架构
使用扩展架构	为 Active Directory 使用扩展架构
“DRAC Name”（DRAC 名称）	在 Active Directory 中唯一标识 DRAC 5 卡的名称。该值默认为 **NULL**。 名称必须是 1-254 个字符的 ASCII 字符串，字符之间没有空格。
“DRAC Domain Name”（DRAC 域名）	Active Directory DRAC 5 对象所在的域的 DNS 名称（字符串）。该值默认为 **NULL**。

	名称必须是包含 *x.y* 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、org。
角色组	与 DRAC 5 卡关联的角色组的列表。 要更改角色组的设置，在角色组列表中单击角色组编号。“Configure Role Group”（配置角色组）窗口将会显示。 **注：** 如果在应用 Active Directory 配置和管理页设置前单击角色组链接，将会失去这些设置。
组名称	该名称标识 Active Directory 中与 DRAC 5 卡相关联的角色组。
组域	组所在的域。
组权限	组的权限级别。

表 6-11。 Active Directory 配置和管理页按钮

按钮	说明
“Print”（打印）	打印 **“Active Directory Configuration and Management”（Active Directory 配置和管理）**页。
“Apply”（应用）	保存对 **“Active Directory Configuration and Management”（Active Directory 配置和管理）**页的更改。
“Go Back to Active Directory Main Menu”（退回到 Active Directory 主菜单）	返回 **Active Directory 主菜单**页。

表 6-12。 角色组权限

设置	说明
角色组权限级别	指定用户的最大 DRAC 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 6-13了解**角色组**权限
“Login to DRAC”（登录到 DRAC）	允许用户登录到 DRAC。
“Configure DRAC”（配置 DRAC）	允许用户配置 DRAC。
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 DRAC 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 6-13。 角色组权限

属性	说明
管理员	登录到 DRAC、配置 DRAC、配置用户、清除日志、执行服务器控制命令、访问控制台重定向、访问虚拟介质、测试警报、执行诊断命令
高级用户	登录到 DRAC、清除日志、执行服务器控制命令、访问控制台重定向、访问虚拟介质、测试警报
客用户	“Login to DRAC”（登录到 DRAC）
“Custom”（自定义）	选择以下权限的任意组合：登录到 DRAC、配置 DRAC、配置用户、清除日志、执行服务器动作命令、访问控制台重定向、访问虚拟介质、测试警报、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。

3. 单击 **“Apply”（应用）**。

4. 单击相应的**“Certificate Upload”（认证上载）**页按钮继续。请参阅表 6-11。

下载 DRAC 服务器认证

1. 在**“Active Directory Main Menu”（Active Directory 主菜单）**页中选择**“Download DRAC Server Certificate”（下载 DRAC 服务器认证）**并单击**“Next”（下一步）**。
2. 在**“File Download”（文件下载）**窗口中单击**“Save”（保存）**，将文件保存到系统中的目录。
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 DRAC 5 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 6-14 说明**认证**窗口中列出的字段及相关说明。

2. 单击相应的**“View Active Directory CA Certificate”（查看 Active Directory CA 认证）**页按钮继续。请参阅表 6-11。

表 6-14。 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。
有效期自	认证发出日期。
有效期至	认证有效日期。

在域控制器上启用 SSL

当 DRAC 5 针对 Active Directory 域控制器验证用户，会启动与域控制器的 SSL 会话。此时，域控制器应发布由认证颁发机构 (CA) 签署的认证 — 其根认证也上载到 DRAC 5 中。换句话说，要使 DRAC 5 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 SSL 的认证。

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）**。

导出域控制器根 CA 认证到 DRAC 5

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）→ R**un（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. 上载在 步骤 14 中保存的认证到 DRAC 5。

要使用 RACADM 上载认证，请参阅 "配置 DRAC 5 使用扩展架构 Active Directory 和 基于 Web 的界面"。

要使用基于 Web 的界面上载认证，请执行下面的过程：

a. 打开一个支持的 Web 浏览窗口。
b. 登录到 DRAC 5 基于 Web 的界面。
c. 展开**系统**树并单击**“Remote Access”（远程访问）**。
d. 单击**“Configuration”（配置）**选项卡，然后单击**“Security”（安全性）**。
e. 在**安全性认证主菜单**页中选**“Upload Server Certificate”（上载服务器认证）**并单击**“Apply”（应用）**。
f. 在**认证上载**屏幕中执行以下过程之一：
   - 单击**“Browse”（浏览）**并选择认证。
   - 在值字段中键入认证的路径。
g. 单击**“Apply”（应用）**。

导入 DRAC 5 固件 SSL 认证

注： 如果 Active Directory Server 设置为在 SSL 会话初始化期间验证客户端，则还需要将 DRAC 5 Server 认证上载到 Active Directory 域控制器。如果 Active Directory 在 SSL 会话初始化期间不验证客户端，则不需要这一额外步骤。

使用下面的过程将 DRAC 5 固件 SSL 认证导入到所有域控制器信任的认证列表。

注： 如果系统运行 Windows 2000，以下步骤可能不同。

注： 如果 DRAC 5 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。

DRAC 5 SSL 认证就是用于 DRAC 5 Web Server 的认证。所有的 DRAC 5 控制器都配备有默认的自签署认证。

要使用 DRAC 5 基于 Web 的界面访问认证，请选择“Configuration”（配置） **Active Directory “Download DRAC 5 Server Certificate”（下载 DRAC 5 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）。

在 DRAC 5 上设置 SSL 时间

当 DRAC 5 验证 Active Directory 用户时，DRAC 5 还会验证由 Active Directory 服务器发布的认证以确保 DRAC 与授权 Active Directory 服务器通信。

该检查还会确保认证在 DRAC 5 指定的时间范围内有效。不过，认证和 DRAC 5 上指定的时区之间可能会不匹配。当 DRAC 5 时间是本地系统时间而认证是 GMT 时间时就有可能发生这样的情况。

要确保 DRAC 5 使用 GMT 时间来比照认证时间，必须设置时差对象。

```
racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <时差值>
```

有关详情，请参阅“cfgRacTuneTimezoneOffset（读/写）”。

支持的 Active Directory 配置

DRAC 5 的 Active Directory 查询算法支持单个目录林中有多个树。

DRAC 5 Active Directory 验证支持混合模式（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）。不过，DRAC 5 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。

如果域目录林运行级别是本地模式或 Windows 2003 模式，DRAC 5 Active Directory 支持多域环境。此外，关联对象、RAC 用户对象和 RAC 设备对象（包括关联对象）的组都必须是通用组。

注： 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。

使用 Active Directory 登录到 DRAC 5

可以使用以下方法之一以 Active Directory 登录到 DRAC 5：

- 基于 Web 的界面
- 远程 RACADM
- 串行或 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。

还可以使用 Smart Card 登录 DRAC 5。有关详情，请参阅“使用 Smart Card 登录 DRAC 5”。

使用 Active Directory 单一式登录

可以启用 DRAC 5 使用 Kerberos（一种网络身份验证协议）启用单一式登录并登录到 DRAC 5。有关设置 DRAC 5 以使用 Active Directory 单一式登录功能的详情，请参阅 "启用 Kerberos 验证。"

配置 DRAC 5 以使用单一式登录

1. 导航到“**Remote Access”（远程访问）**→“**Configuration”（配置）**选项卡→ **Active Directory** 子选项卡? 选择“ **Configure Active Directory”（配置 Active Directory）**。
2. 在“**Active Directory Configuration and Management”（Active Directory 配置和管理）**页上，选择“**Single Sign-On”（单一式登录）**。

   此选项使用户能够在登录到工作站后直接登录 DRAC 5。

使用单一式登录来登录 DRAC 5

1. 使用网络帐户登录工作站。
2. 使用 https 访问 DRAC 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 DRAC 5 的 IP 地址，而*端口号*是 HTTPS 端口号。

   DRAC 5 单一式登录页面将会显示。
3. 单击 **“Login”（登录）**。

   凭借用户使用有效 Active Directory 帐户登录时缓存在操作系统中的凭据，DRAC 5 会使用户登录。

常见问题

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 DRAC 5 只允许上载一个可信 CA SSL 认证。

我创建并上载了一个新 RAC 认证，然而现在基于 Web 的界面不启动。

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）**。

要恢复、生成 CSR 并随后从 Microsoft Certificate Services 创建新 web 认证并从 managed system 用 RACADM CLI 使用以下 racadm 命令载入：

```
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 DRAC 5，应该怎么办？我如何排除这个故障？

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 DRAC 用户帐户，请使用本地凭据登录 DRAC 5。

   登录后：

   a. 确保已选中 DRAC 5 Active Directory 配置页上的**“Enable Active Directory”（启用 Active Directory）**框。

   b. 确保 DRAC 5 联网配置页上的 DNS 设置正确。

   c. 确保已从 Active Directory 根 CA 将 Active Directory 认证上载到 DRAC 5。

   d. 检查域控制器 SSL 认证以确保没有过期。

   e. 确保 **DRAC 名称**、**Root 域名**和 **DRAC 域名**与 Active Directory 环境配置相匹配。

   f. 确保 DRAC 5 密码最多有 127 个字符。虽然 DRAC 5 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

目录

配置 Smart Card 验证

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 在 DRAC 5 中配置 Smart Card 登录
- 配置本地 DRAC 5 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 DRAC 5
- 使用 Active Directory Smart Card 身份验证登录 DRAC 5
- 排除 DRAC 5 中 Smart Card 登录故障

Dell™ Remote Access Controller 5 (DRAC 5) 1.30 和更高版本支持*双重验证*登录 DRAC 5 Web 界面。这种支持由 DRAC 5 上的“**Smart Card Logon**”（**Smart Card 登录**）功能提供。

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。

而双重验证则提供了更高的安全性，要求用户具有密码或 PIN 以及数字认证的专用密钥。

双重验证要求用户通过提供*两方面*的凭据来验证身份。

在 DRAC 5 中配置 Smart Card 登录

从“**Remote Access**”（**远程访问**）→“**Configuration**”（**配置**）→ **Smart Card** 启用 DRAC 5 Smart Card 登录。

如果您：

- **禁用** Smart Card 配置，会提示您输入 Microsoft® Active Directory® 或本地登录用户名和密码。
- **启用**或**随远程 Racadm 启用**，会在随后使用 GUI 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。这是因为这些服务只支持单重验证。

  选择“**Enable with Remote Racadm**”（**随远程 Racadm 启用**）后，所有 CLI 带外接口，除远程 racadm 以外，都会禁用。

  注： Dell 建议 DRAC 5 管理员将“**Enable with Remote Racadm**”（**随远程 Racadm 启用**）设置只用来访问 DRAC 5 用户界面来使用远程 racadm 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“**Enabled**”（**已启用**）设置。另外，应确保启用“**Smart Card Logon**”（**Smart Card 登录**）前完成 DRAC 5 本地用户配置和/或 Active Directory 配置。

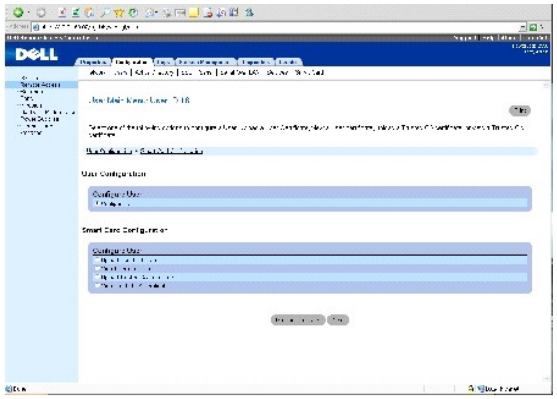
- “**Enable CRL check for Smart Card Logon**”（**启用 CRL 检查进行 Smart Card 登录**），会对从认证撤回表 (CRL) 分发服务器下载的用户 DRAC 认证进行检查以在 CRL 中撤回。

  注： CRL 分发服务器列在用户的 Smart Card 认证中。

配置本地 DRAC 5 用户进行 Smart Card 登录

可以配置本地 DRAC 5 用户使用 Smart Card 登录 DRAC 5。导航到 **Remote Access**→“**Configuration**”（**配置**）→“**Users**”（**用户**）。

图 7-1。 Smart Card 用户管理页



不过，在用户可以使用 Smart Card 登录 DRAC 5 前，必须将用户的 Smart Card 认证和可信认证机构 (CA) 认证上载到 DRAC 5。

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 DRAC 5。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 DRAC 5，在 DRAC 5 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 DRAC 5，DRAC 5 管理员应配置 DNS 服务器，上载 Active Directory CA 认证到 DRAC 5，并启用 Active Directory 登录。请参阅 "将 DRAC 5 用于 Microsoft Active Directory" 详细了解如何设置 Active Directory 用户。

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 DRAC 5"（配置 DRAC 5）**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 7-1 提供了有关 **Smart Card** 页设置的信息。
4. 单击 **"Apply Changes"（应用更改）**。

表 7-1。 Smart Card 设置

设置	说明
配置 Smart Card 登录	• "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。 • "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、Serial、远程 RACADM 和 IPMI over LAN。 • "Enabled with Remote Racadm"（随远程 Racadm 启用） — 随远程 RACADM 启用 Smart Card 登录。其它所有 CLI 带外接口都会禁用。 **注：** Smart Card 登录要求用适当的认证配置本地 DRAC 5 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。
"Enable CRL check for Smart Card Logon"（为 Smart Card 登录启用 CRL 检查）	本检查仅供 Active Directory 登录用户使用。如果希望 DRAC 5 检查认证撤回表 (CRL) 撤回用户 Smart Card 认证，则选择此选项。 在以下情况下，用户将无法登录： • 用户认证在 CRL 文件中列为已撤回。 • DRAC 无法与 CRL 分发服务器通讯。 • DRAC 无法下载 CRL。 **注：** 必须在 **"Configuration"（配置）→"Network"（网络）**页中正确配置 DNS 服务器的 IP 地址，检查才能成功。

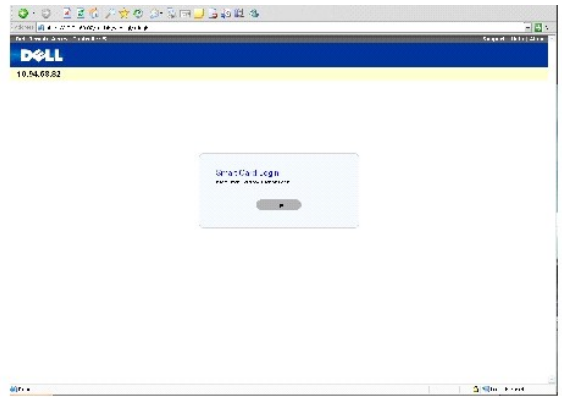
使用 Smart Card 登录 DRAC 5

DRAC 5 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 Logon"（Smart Card 登录）前完成 DRAC 5 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。

图 7-2。 使用 Smart Card 登录 DRAC 5



1. 使用 https 访问 DRAC 5 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 DRAC 5 的 IP 地址，而*端口号*是 HTTPS 端口号。

DRAC 5 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）**。

DRAC 5 会提示输入 Smart Card 的 PIN。

3. 输入 Smart Card PIN 并单击“**OK”（确定）**。

注： 如果是已选中“**Enable CRL check for Smart Card Logon”（启用 CRL 检查进行 Smart Card 登录）** 的 Active Directory 用户，DRAC 5 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 DRAC 5。

不过，如果 Smart Card 登录失败，并且如果：

- 已为用户帐户启用 Active Directory 登录，而且
- 是有效的 Active Directory 用户
- 应已配置 Active Directory 使用 Smart Card 身份验证。（有关详情，请参阅“启用 Kerberos 验证”。）

DRAC 5 将会自动使用户登录。

使用 Active Directory Smart Card 身份验证登录 DRAC 5

1. 使用 https 登录 DRAC 5。

`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 DRAC 5 的 IP 地址，而*端口号*是 HTTPS 端口号。

DRAC 5 登录页会显示出来，提示插入 Smart Card。

2. 插入 Smart Card 并单击“**Login”（登录）**。

PIN 弹出对话框将会显示。

3. 输入 PIN，并单击“**OK”（确定）**。

将会使用跟 Active Directory 中设置一样的凭据让用户登录 DRAC 5。

有关详情，请参阅“启用 Kerberos 验证”。

排除 DRAC 5 中 Smart Card 登录故障

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 DRAC 5

如果本地 DRAC 5 用户不能登录，检查上载到 DRAC 5 的用户名和用户认证是否已经过期。DRAC 5 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 DRAC 5

如果无法作为 Active Directory 用户登录 DRAC 5，应尝试不启用 Smart Card 登录来登录 DRAC 5。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，DRAC 5 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

目录

启用 Kerberos 验证

Dell™ Remote Access Controller 5 固件版本 1.40 用户指南

- 使用 Smart Card 进行单一式登录和 Active Directory 验证的前提条件
- 配置 DRAC 5 成为使用 Smart Card 进行单一式登录和 Active Directory 验证
- 使用单一式登录来登录到 DRAC 5

Kerberos 是一种网络验证协议，使系统能够通过不安全网络安全通信。通过让系统验证真实性来实现这一目的。

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

从 DRAC 5 版本 1.40 开始，DRAC 5 使用 Kerberos 支持两种验证机制 — 单一式登录和 Active Directory Smart Card 登录。

对于单一式登录，在用户使用有效 Active Directory登录后 DRAC 5 使用操作系统缓存的用户凭据。

从 DRAC 5 版本 1.40 开始，Active Directory 验证将使用基于 Smart Card 的双元验证 (TFA) 以及用户名密码组合作为有效凭据。

使用 Smart Card 进行单一式登录和 Active Directory 验证的前提条件

- 配置 DRAC 5 进行 Active Directory 登录。有关详情，请参阅“使用 Active Directory 登录到 DRAC 5”。
- 注册 DRAC 5 作为 Active Directory 根域中的计算机。
  a. 导航至“**Remote Access**”（**远程访问**）→“**Configuration**”（**配置**）选项卡→“**Network**”（**网络**）子选项卡→“**Network Settings**”（**网络设置**）。
  b. 提供有效的“**Preferred**”（**首选**）/“**Static DNS Server**”（**静态 DNS 服务器**）IP 地址。该值是根域中 DNS 的 IP 地址，验证用户的 Active Directory 帐户。
  c. 选择“**Register DRAC on DNS**”（**向 DNS 注册 DRAC**）。
  d. 提供有效“**DNS Domain Name**”（**DNS 域名**）。

  请参阅 *DRAC 5 联机帮助*了解详情。

  由于 DRAC 5 是一种非 Windows 操作系统设备，在想将 DRAC 5 映射到 Active Directory 用户帐户的域控制器（Active Directory 服务器）上，运行 **ktpass** 公用程序的 Microsoft® Windows® 程序部分。例如：

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

  注： DRAC 5 支持的 Kerberos 验证的加密类型是 DES-CBC-MD5。

  此步骤会生成一个 keytab 文件，应将该文件上载到 DRAC 5。

注： keytab 包含加密密钥，因此应保管好。

有关 **ktpass** 公用程序的详情，请参阅 Microsoft 网站： **http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

- DRAC 5 时间应与 Active Directory 域控制器同步。

配置 DRAC 5 成为使用 Smart Card 进行单一式登录和 Active Directory 验证

将从 Active Directory 根域获得的 keytab 文件上载到 DRAC 5：

1. 导航到“**Remote Access”（远程访问）**→“**Configuration”（配置）**选项卡→ **Active Directory** 子选项卡。
2. 选择“**Upload Kerberos Keytab”（上载 Kerberos Keytab）**并单击“**Next”（下一步）**。
3. 在“**Kerberos Keytab Upload”（Kerberos Keytab 上载）**页上，导航到保存 keytab 的文件夹并单击“**Upload”（上载）**。

使用单一式登录来登录到 DRAC 5

注： 要登录到 DRAC 5，应确保具有 Microsoft Visual C++ 2005 程序库的最新运行时组件。有关详情，请参阅 Microsoft 网站。

1. 使用有效 Active Directory 帐户登录到系统。
2. 在浏览器的地址栏中键入 DRAC 5 的网址。

   注： 根据浏览器的不同，在第一次使用此功能时可能会提示下载并安装单一式登录 ActiveX 插件。

   您已登录 DRAC 5。

目录

目录

使用 GUI 控制台重定向

Dell™ Remote Access Controller 5 固件版本 1.40 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 DRAC 5 控制台重定向功能的信息。

概览

DRAC 5 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 DRAC 5 的系统。

现今，借助网络和因特网的强大力量，您再也不用坐到每一台服务器的前面去执行所有的日常维护。您可以从另一个城市或者甚至从地球的另一边通过您的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 — 无论多么遥远但总是迅速及时。

使用控制台重定向

注： 打开控制台重定向会话时，Managed System 不会指示控制台已经重定向。

“Console Redirection”（控制台重定向）页使用户能够管理远程系统，通过使用本地 Management Station 上的键盘、视频和鼠标控制远程 Managed System 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：

- 仅支持两个同时控制台重定向会话。
- 控制台重定向会话只能连接到一个远程目标系统。
- 不能在本地系统上配置控制台重定向会话。
- 最低要求 1 MB/sec 可用网络带宽。

Managed System 上支持的屏幕分辨率刷新率

表 9-1 列出了 Managed System 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 9-1。 支持的屏幕分辨率和刷新率

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

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：
   - 请参阅 Dell 支持网站 **support.dell.com** 上的 Dell 系统软件支持值表。

     控制台重定向和虚拟介质只支持 32 位 Web 浏览器。使用 64 位 Web 浏览器可能会产生无法预料的结果或操作故障。
   - "配置支持的 Web 浏览器"
2. 显示器显示分辨率至少配置为 1280 x 1024 像素 60 Hz 128 色。否则，可能无法以**全屏模式**查看控制台。
3. 如果使用 Java 插件连接，应确保系统装有 Java 虚拟机 (JVM) 1.4 或更高版本。

配置控制台重定向

1. 在 management station 上打开一个支持的 Web 浏览器并登录 DRAC 5。有关详情，请参阅"访问基于 Web 的界面"。
2. 在**系统**树中单击**"System"（系统）**。
3. 单击**"Console"（控制台）**选项卡，然后单击**"Configuration"（配置）**。
4. 在**控制台重定向配置页**中使用表 9-2中的信息配置控制台重定向会话。
5. 在 DRAC 5 版本 1.40 和更高版本中，可以选择要安装的**本机**或 **Java** 插件类型。

单击**"Apply Changes"（应用更改）**。

表 9-2。 控制台重定向配置页信息

Information（信息）	说明
已启用	选中 = 启用；未选中=禁用
"Max Sessions"（最大会话）	显示可用的控制台重定向会话数。
"Active Sessions"（激活的会话）	显示活动控制台重定向会话数。
"Keyboard and Mouse Port Number"（键盘和鼠标端口号）	默认值 = 5900
"Video Port Number"（视频端口号）	默认值 = 5901
"Video Encryption Enabled"（视频加密已启用）	选中 = 启用；未选中=禁用
"Local Server Video Enabled"（本地服务器视频已启用）	选中 = 启用；未选中=禁用
插件类型	允许选择**本机**（Windows 为 ActiveX，而 Linux 为 XPI 插件）或 **Java** 插件。 **注：** 如果选择 Java 插件，应确保系统已装有 Java 虚拟机 (JVM) 1.4 或更高版本。

表 9-3 中的按钮在**控制台重定向配置**页上可用。

表 9-3。 控制台重定向配置页按钮

属性	说明
"Print"（打印）	打印**控制台重定向配置**页
"Refresh"（刷新）	重载**控制台重定向配置**页
"Apply Changes"（应用更改）	保存配置设置。

注： 对于 DRAC 5 版本 1.30 和更高，可以为远程用户禁用控制台重定向。有关详情，请参阅"禁用 DRAC 5 远程虚拟 KVM"。

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 viewer 中会出现远程系统的桌面。使用虚拟 KVM Viewer 应用程序，可以从本地或远程 Management Station 控制系统的鼠标和键盘功能。

要打开控制台重定向会话：

1. 在 management station 上打开一个支持的 Web 浏览器并登录 DRAC 5。有关详情，请参阅“访问基于 Web 的界面”。
2. 在**系统**树中，单击**“System”（系统）**和**“Console”（控制台）**选项卡，单击**“Console Redirect”（控制台重定向）**。

注： 如果收到安全警告，提示您安装并运行控制台重定向插件，应验证插件的真实性，然后单击**“Yes”（是）**安装并运行插件。如果运行 Firefox，请重新启动浏览器然后转至步骤 步骤 1。

3. 在**控制台重定向**页中使用表 9-4 中的信息确保有一个控制台重定向会话可用。

表 9-4。 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
“Local Server Video Enabled”（本地服务器视频已启用）	是/否
“Status”（状态）	已连接或已断开连接
“Max Sessions”（最大会话）	支持的最大控制台重定向会话数
“Active Sessions”（激活的会话）	当前激活的控制台重定向会话数
插件类型	在**“Console Redirect Configuration”（控制台重定向配置）**页中选择的插件类型。

表 9-5 中的按钮在**控制台重定向**页上可用。

表 9-5。 控制台重定向页按钮

按钮	定义
“Refresh”（刷新）	重载**控制台重定向配置**页
“Connect”（连接）	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**控制台重定向配置**页。

4. 如果控制台重定向会话可用，则单击**“Connect”（连接）**。

如果系统运行 Linux 并且已在**“Console Redirect Configuration”（控制台重定向配置）**页选择安装 Java 插件，将会显示一条信息提示**“Open”（打开）**或**“Save”（保存）** **.jnlp** 文件到系统。如果选择保存 **.jnlp** 文件，则双击手工运行保存的文件。如果下载了 **.jnlp** 文件但是不运行，控制台重定向的状态将始终显示**“Connecting”（正在连接）**。

如果系统运行 Windows 并且已在**“Console Redirect Configuration”（控制台重定向配置）**页选择安装 Java 插件，系统将会保存 **.jnlp** 文件并自动运行。

注： 如果 JVM 没有安装在系统上，则单击**“Connect”（连接）**时，控制台重定向的状态会显示为**“Connecting”（正在连接）**直至单击**“Disconnect”（断开连接）**。

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 DRAC 5，在 Dell Digital KVM Viewer 应用程序中显示远程系统的桌面。

5. 如果两个鼠标光标出现在远程系统的桌面上，则同步 Management Station 和远程系统上的鼠标光标。请参阅“同步鼠标光标”。

禁用或启用本地视频

要禁用或启用本地视频，应执行以下步骤：

1. 在 management station 上打开一个支持的 Web 浏览器并登录 DRAC 5。有关详情，请参阅“访问基于 Web 的界面”。

2. 在**系统**树中单击**“System”（系统）** 。
3. 单击**“Console”（控制台）** 选项卡，然后单击**“Configuration”（配置）** 。
4. 如果想在服务器上启用（打开）本地视频，在**“Console Redirect Configuration”（控制台重定向配置）**页中选择“Local Server Video Enabled”（本地服务器视频已启用）复选框并随后单击“Apply Changes”（应用更改）。默认值为 ON。
5. 如果想在服务器上禁用（关闭）本地视频，在**“Console Redirect Configuration”（控制台重定向配置）**页中取消选择“Local Server Video Enabled”（本地服务器视频已启用）复选框并随后单击“Apply Changes”（应用更改）。

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

注： “local server video enabled”（本地服务器视频已启用）功能在除 PowerEdge SC1435 和 6950 以外的所有 x9xx PowerEdge 系统上受支持。

注： 禁用（关闭）服务器上的本地视频，只有连接到本地服务器的显示器会禁用。

注： 对于 DRAC 5 版本 1.30 和更高，可以为远程用户禁用控制台重定向。有关详情，请参阅“禁用 DRAC 5 远程虚拟 KVM”。

使用 Video Viewer

Video Viewer 在 Management Station 和远程系统之间提供了一个用户界面，使用户能够从 Management Station 查看远程系统的桌面并控制其鼠标和键盘运作。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，比如视频校准、鼠标加速度和快照。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，可能需要调整以下控制以正确查看并控制远程系统。这些调整包括：

- 访问 Viewer 菜单栏
- 调整视频质量
- 同步鼠标光标

访问 Viewer 菜单栏

Viewer 菜单栏是一个隐藏菜单栏。要访问菜单栏，将光标移到 Viewer 桌面窗口的中上方。

另外，该菜单栏还可以通过按默认功能键 <F9> 来激活。要为该功能键重新分配新功能：

1. 按 <F9> 或将鼠标光标移到 Video Viewer 的顶部。
2. 按“按钉”锁定 Viewer 菜单栏。
3. 在 Viewer 菜单栏，单击**“Tools”（工具）**并选择**“Session”（会话）选项。**
4. 在**会话选项**窗口中单击**“General”（常规）**选项卡。
5. 在**“General”（常规）**选项卡窗口的**“Menu Activation Keystroke”（菜单激活按键）**框中，单击下拉菜单并选择另一个功能键。
6. 单击**“Apply”（应用）**，然后单击**“OK”（确定）**。

表 9-6 提供 Viewer 菜单栏中可以使用的主要功能。

表 9-6。 Viewer 菜单栏选择

菜单项	项目	说明
文件	“Capture to File”（捕获到文件）	将当前远程系统屏幕捕获到本地系统上的 **.bmp** (Windows) 或 **.png** (Linux) 文件。将显示一个对话框，使您可以将文件保存到指定位置。
	“Exit”（退出）	退出**“Console Redirection”（控制台重定向）**页。
查看	“Refresh”（刷新）	更新整个远程系统屏幕视区。

	“Full Screen”（全屏）	将会话屏幕从窗口扩展到全屏。
“Macros”（宏）	各个键盘快捷键	在远程系统上执行按键组合。 要将 management station 的键盘连接到远程系统并运行宏： 1. 单击**“Tools”（工具）**。 2. 在**会话选项**窗口中单击“General”（常规）选项卡。 3. 选择**“Pass all keystrokes to target”（将所有按键传递到目标）**。 4. 单击 **OK（确定）**。 5. 单击**“Macros”（宏）**。 6. 在**“Macros”（宏）**菜单中单击要在目标系统上执行的按键组合。
“Tools”（工具）	自动视频调节	重新校准 session viewer 视频输出。
	“Manual Video Adjust”（手动视频调节）	提供各种控制以手动调节 session viewer 视频输出。 **注：** 调整水平位置偏离中心将取消鼠标光标同步。
	“Session Options”（会话选项）	提供其他 session viewer 控制调节。 **“Mouse”（鼠标）**选项卡允许选择用于优化控制台重定向鼠标性能的操作系统。请选择 **Windows**、**Linux** 或**无**。 **“General”（常规）**选项卡提供以下选项： • **键盘通过模式** — 选择**“Pass all keystrokes to target”（将所有按键传递到目标）**将 management station 的按键传递到远程系统。 • **菜单激活按键** — 选择激活 viewer 菜单栏的功能键。 **“Toolbar”（工具栏）**选项卡允许在 1 至 10 秒间调整**工具栏隐藏延迟**时间。
帮助	无	激活**“Help”（帮助）**菜单。

调整视频质量

Video Viewer 提供了视频调整，使用户能够为达到最佳效果而优化视频。单击**“Help”（帮助）**了解有关详情。

要自动调整视频质量：

1. 访问 Viewer 菜单栏。请参阅“访问 Viewer 菜单栏”。
2. 单击**“Tools”（工具）**并选择**“Automatic Video Adjust”（自动视频调节）**。

将重新调节视频质量并重新显示 session viewer。

要手动调整视频质量：

1. 访问 Viewer 菜单栏。请参阅“访问 Viewer 菜单栏”。
2. 单击**“Tools”（工具）**并选择**“Manual Video Adjust”（手动视频调节）**。
3. 在**视频调节**窗口中单击每个视频调节按钮根据需要调整控制。

手动调整视频质量时，请遵守以下原则：

- 要避免鼠标光标取消同步，请调整水平设置使远程系统的桌面位于会话窗口中央。
- 像素噪声比率设置降低为零将导致多个视频刷新命令造成过量网络通信量，并且视频在 Video Viewer 窗口中闪烁。Dell 建议将“Pixel Noise Ratio”（像素噪声比率）设置调整为达到最佳系统性能和像素效果的水平，同时尽量减少网络通信量。

同步鼠标光标

使用控制台重定向连接到远程 Dell 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。

要同步鼠标光标：

1. 访问 Viewer 菜单栏。请参阅“访问 Viewer 菜单栏”。
2. 单击“**Tools**”（工具）并选择“**Session Options**”（会话选项）。
3. 单击“**Mouse**”（鼠标）选项卡，选择 management station 的操作系统，并单击“**OK**”（确定）。
4. 单击“**Tools**”（工具）并选择“**Manual Video Adjust**”（手动视频调节）。
5. 调整水平控制使远程系统的桌面显示在会话窗口的中央。
6. 单击 **OK**（确定）。

使用 Linux（Red Hat® 或 Novell®）时，会使用操作系统的默认鼠标设置来控制 DRAC 5 控制台重定向屏幕中的鼠标箭头。

注： 在 Linux（Red Hat 或 Novell）系统上，存在已知的鼠标同步问题。要避免鼠标同步问题，应确保所有用户都使用默认鼠标设置。

有关禁用控制台重定向的信息，请参阅 "禁用 DRAC 5 远程虚拟 KVM"。

常见问题

当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。

请求关闭本地会话后，为什么需要 15 秒钟才能关闭服务器上的本地视频？

使用户能够在视频关闭前有机会采取行动。

打开本地视频是否有时间延迟？

没有，DRAC 5 一收到本地视频打开请求就会立即打开视频。

本地用户也可以关闭视频吗？

是，本地用户可以使用 racadm CLI（本地）关闭视频。

本地用户也可以打开视频吗？

是，用户应在服务器上装有 racadm CLI 并且只有在用户能够通过 RDP 连接（比如终端服务、 telnet 或 SSH）访问服务器时。用户可以随后登录到服务器并运行 racadm（本地）打开视频。

我的本地视频已关闭并且由于某些原因， DRAC 5 不能远程访问并且服务器不能通过 RDP、telnet 或 SSH 访问。如何恢复本地视频？

在这种情况下，唯一恢复本地视频的方式是从服务器拔下交流电源线，耗尽服务器余电并重新连接交流电源线；这会将本地视频恢复到服务器显示器上。另外，DRAC 5 配置也会更改为打开本地视频（默认）。如果需要再次关闭本地视频，DRAC 5 需要重新配置。

关闭本地视频也会关闭本地键盘和鼠标吗？

不，关闭本地视频只会关闭服务器显示器输出连接的视频；不会关闭服务器本地连接的键盘和鼠标。

关闭本地服务器视频是否会关闭远程 vKVM 会话上的视频？

不，打开或关闭本地视频与远程控制器会话无关。

DRAC 5 用户打开或关闭本地服务器视频需要哪些权限？

任何具有 DRAC 5 配置权限的用户都可以打开或关闭本地服务器视频。

如何获得本地服务器视频的最新状况？

状况信息显示在 DRAC 5 web 界面的“Console Redirection Configuration”（控制台重定向配置）页。racadm CLI 命令 racadm getconfig ®Cg cfgRacTuning 在对象 cfgRacTuneLocalServerVideo 中显示状态。本地用户还可以在服务器 LCD 屏幕上看到状态，比如 “Video OFF”（视频关闭）或 “Video OFF in 15”（视频在 15 秒后关闭）。

为什么有时在服务器 LCD 屏幕上看不到 “Video OFF”（视频关闭）或 “Video OFF in 15”（视频在 15 秒后关闭）状态？

本地视频状态是一种低优先级消息，在同时出现更高优先级的服务器事件时会被屏蔽。LCD 消息基于优先级，必须关闭所有高优先级 LCD 消息并解决事件后，较低优先级的消息才会显示出来。LCD 屏幕上的服务器视频消息仅作提供信息之用。

如何获得有关本地服务器视频功能的更多信息？

请参阅 Dell 支持网站 **support.dell.com** 查看有关此功能的白皮书。

我在屏幕上看到视频损坏。怎么解决这个问题？

在**控制台重定向**窗口中单击**“Refresh”（刷新）**以刷新屏幕。

注： 可能需要单击几次**“Refresh”（刷新）**才能纠正视频损坏。

在控制台重定向期间，在 Windows 2000 系统上，键盘和鼠标从休眠返回后会锁定。是什么原因造成这种情况？

要解决此问题，必须通过运行 **racadm racreset** 命令重设 DRAC 5。

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。

在控制台重定向期间，在 Windows Server 2003 系统上，鼠标从休眠返回后会锁定。为什么会发生这种情况？

要解决此问题，请从虚拟 KVM (vKVM) 窗口下拉式菜单中选择 Windows 以外的操作系统设置鼠标加速度，等待 5 到 10 秒，然后再次选择 Windows。如果问题仍然没有解决，必须通过运行 **racadm racreset** 命令重设 DRAC 5。

如果问题仍然没有解决，必须通过运行 **racadm racreset hard** 命令重设 DRAC 5。

为什么 vKVM 键盘和鼠标不工作？

必须在 Managed System 的 BIOS 设置中将 USB 控制器设置为“**On with BIOS support**”（**启动具有 BIOS 支持**）。重新启动 Managed System 并按 <F2> 进入设置。选择“**Integrated Devices**”（**集成设备**），然后选择“**USB Controller**”（**USB 控制器**）。保存更改并重新启动系统。

为什么当 Windows 出现蓝色屏幕时，Managed System 控制台屏幕变为空白？

Managed System 没有正确的 ATI 视频驱动程序。必须用 *Dell Systems Management Tools and Documentation* DVD 更新视频驱动程序。

为什么完成 Windows 2000 操作系统安装后在远程控制台上出现空白屏幕？

Managed System 没有正确的 ATI 视频驱动程序。DRAC 5 控制台重定向在使用 Windows 2000 分发 CD 中的 SVGA 视频驱动程序时运行不正常。必须使用 *Dell Systems Management Tools and Documentation* DVD 安装 Windows 2000 以确保 managed system 具有最新受支持的驱动程序。

为什么在载入 Windows 2000 操作系统时 Managed System 上出现空白屏幕？

Managed System 没有正确的 ATI 视频驱动程序。必须用 *Dell Systems Management Tools and Documentation* DVD 更新视频驱动程序。

为什么在 Managed System 上的 Windows 全屏幕 DOS 窗口中出现空白屏幕？

Managed System 没有正确的 ATI 视频驱动程序。必须用 *Dell Systems Management Tools and Documentation* DVD 更新视频驱动程序。

为什么无法通过按 <F2> 键进入 BIOS 设置？

这种情况在 Windows 环境中很普遍。使用鼠标单击“Console Redirection”（控制台重定向）窗口上的某个区域以调整焦点。要将焦点移到“Console Redirection”（控制台重定向）窗口的底部菜单栏，使用鼠标并单击底部菜单栏的某个对象。

使用 Dell Systems Management Tools and Documentation DVD 远程安装操作系统时，为什么 vKVM 鼠标不同步？

为目标系统上运行的操作系统配置控制台重定向。

1. 在 vKVM 工具栏菜单中单击“**Tools**”（**工具**）并选择“**Session Options**”（**会话选项**）。
2. 在“**Session Options**”（**会话选项**）窗口中单击“**Mouse**”（**鼠标**）选项卡。
3. 在“**Mouse Acceleration**”（**鼠标加速度**）框中选择目标系统上运行的操作系统并单击“**OK**”（**确定**）。

在 Windows 系统上从休眠状态唤醒后，为什么 vKVM 鼠标不同步？

在 vKVM 窗口下拉式菜单上为鼠标加速度选择不同的操作系统。然后，返回原来的操作系统以初始化 USB 鼠标设备。

1. 在 vKVM 工具栏中单击“**Tools**”（**工具**）并选择“**Session Options**”（**会话选项**）。
2. 在“**Session Options**”（**会话选项**）窗口中单击“**Mouse**”（**鼠标**）选项卡。
3. 在“**Mouse Acceleration**”（**鼠标加速度**）框中选择另一个操作系统并单击“**OK**”（**确定**）。
4. 初始化 USB 鼠标设备。

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 鼠标为鼠标光标使用相对位置，这会造成同步的延迟。DRAC 5 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光标跟踪。即使 DRAC 5 将 USB 的绝对鼠标位置传递给 Dell BIOS，BIOS 仿真程序依然会将它转换回相对位置，所以行为依旧。

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。

请确保目标系统的桌面在控制台重定向窗口的中央。

1. 在 vKVM 工具栏中单击**“Tools”（工具）**并选择**“Manual Video Adjustment”（手动视频调节）**。
2. 根据需要调整水平和垂直控制以在控制台重定向窗口中对齐桌面。
3. 单击 **Close（关闭）**。
4. 将目标系统的鼠标光标移动至控制台重定向窗口的左上角，然后将光标移动回窗口中央。
5. 重复步骤 2 至步骤 4 直到两个鼠标同步。

为什么为不同操作系统更改鼠标加速度时，vKVM 鼠标和键盘不工作？

更改鼠标加速度后，USB vKVM 键盘和鼠标将保持非活动 5 到 10 秒。网络负载有时会使此操作比正常要长（超过 10 秒）。

为什么从 vKVM 窗口看不到服务器屏幕的底部？

请确保服务器屏幕分辨率为 1280 x 1024 像素 60 Hz 128 色。

为什么使用 DRAC5 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 System，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。

为什么在中文、日文和韩文版本的 Microsoft Windows 2000 中，控制台重定向无法显示操作系统引导菜单？

在可以引导多个操作系统的运行 Windows 2000 的系统上，通过执行下列步骤来更改默认引导操作系统：

1. 右击**“My Computer”（我的电脑）**图标并选择**“Properties”（属性）**。
2. 单击**“高级”**选项卡。
3. 单击**“Startup and Recovery”（启动和故障恢复）**。
4. 从**“Startup”（启动）**列表选择新的默认操作系统。
5. 在**“Show”（显示）**列表框中，键入默认操作系统自动引导之前选择列表应显示的秒数。

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 DRAC 5 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。

为什么建立控制台重定向会话时显示多个 Session Viewer 窗口？

您在将控制台重定向会话配置到本地系统。请将会话重新配置到远程系统。

如果我运行控制台重定向会话而本地用户访问远程系统，会收到警告消息吗？

否。如果本地用户访问系统，他可以改写您的动作而不发出警告。

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 RAM。

远程系统上可运行的控制台重定向会话的最大数量是多少？

DRAC 5 支持最多 2 个同时控制台重定向会话。

为什么出现鼠标同步问题?

在 Linux（Red Hat 或 Novell）系统上，存在已知的鼠标同步问题。要避免鼠标同步问题，应确保所有用户都使用默认鼠标设置。

如何在具有只读文件系统的 management station 上安装 Web 浏览器？

如果正在运行 Linux 并且 Management Station 具有只读文件系统，则可以在客户系统上安装浏览器而无需连接到 DRAC 5。通过使用本机插件安装软件包，浏览器可以在客户端设置期间手动安装。

注意： 在只读客户端环境中，如果 DRAC 5 固件更新到较新版本的插件，则已装的 VM 插件将不能运行。这是因为当固件包含较新版本的插件时，不允许运行较早版本插件的功能。在这种情况下，将会提示客户进行插件安装。由于文件系统是只读的，安装将会失败并且插件功能将不可用。

要获得插件安装软件包：

1. 登录到现有 DRAC 5。
2. 更改浏览器地址栏中的 URL，从：

   ```
   https://<RAC_IP>/cgi-bin/webcgi/main
   ```

   更改为：

   ```
   https://<RAC_IP>/plugins/ # 请确保包括斜杠。
   ```

3. 注意两个子目录 vm 和 vkvm 。 导航到相应的子目录，在 rac5XXX.xpi 文件上单击鼠标右键，并选择“Save Link Target As...”（将链接目标另存为...）。
4. 选择一个位置来保存插件安装软件包文件。

要安装插件安装软件包：

1. 将安装软件包复制到可以由客户端访问的客户端本机文件系统共享。
2. 在客户系统上打开浏览器的一个实例。
3. 在浏览器的地址栏中输入插件安装软件包的文件路径。例如：

   file:///tmp/rac5vm.xpi
4. 浏览器会引导用户完成插件安装过程。

安装完成后，只要目标 DRAC5 固件不包含较新版本的插件，浏览器都不会再次提示安装插件。

当重新引导终端时，为什么控制台重定向会话结束。

当 DRAC 5 NIC 设置处于 "shared"（共享）或 "shared with failover"（ 共享故障切换）模式时，系统重置会造成母板 LAN (LOM) 重置。在具有启用生成树协议 (STP) 的交换机的网络上，这会造成 management station 和客户端之间的连接在大约十到十五秒后重新建立。因此，与远程系统的连接会丢失并且在控制台重定向和虚拟介质客户端上会显示连接丢失错误信息。如果在此时访问 DRAC GUI，会收到 "Page Not Found"（页面未找到）错误信息。

要解决此问题：

- 在网络上使用 DRAC 5 专用 NIC 连接。
- 禁用网络交换机上的 STP。

目录

Back to Contents Page

词汇表

Dell™ Remote Access Controller 5 固件版本 1.40 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。

AGP

加速图形端口 (accelerated graphics port) 的缩写，是一种总线规范，使图形卡可以更快地访问主系统内存。

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。

BMC

底板管理控制器 (baseboard management controller) 的缩写，是 DRAC 5 和 Managed System 的 BMC 之间的控制器接口。

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，以在通过网络和 Internet 进行事务处理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。

DRAC 5

Dell 远程访问控制器 5 (Dell Remote Access Controller 5) 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 (DRand 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。

ICMB

智能机箱管理总线 (Intelligent Chassis 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）。

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。

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

Managed System 是安装或嵌入 DRAC 5 的系统。

Management Station

Management Station 是远程访问 DRAC 5 的系统。

MAP

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

Mbps

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

MIB

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

MII

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

NAS

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

NIC

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

OID

对象标识符 (Object Identifiers) 的缩写。

PCI

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

PKI

公用密钥基础架构 (Public Key Infrastructure) 的缩写。PKI 使非安全公共网络（比如 Internet）用户能够通过使用从可信机构获得并共享的公共和专用密钥对来安全保密地交换数据。

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) 的缩略词。RAM 是系统和 DRAC 5 上的通用可读可写存储器。

RAM 磁盘

模拟硬盘驱动器的内存驻留程序。DRAC 5 在其内存中维护 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。

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

简单网络管理协议 (Simple Network Management Protocol) 的缩写，是用于管理 IP 网络节点的协议。DRAC 5 是 SNMP 管理的设备（节点）。

SNMP 陷阱

由 DRAC 5 或 BMC 生成的通知（事件），包含有关 Managed System 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。

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。

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。

标准架构

一种与 Active Directory 一起使用的解决方案，用来确定用户的 DRAC 5 权限；只使用 Active Directory 组对象。

控制台重定向

控制台重定向功能可将 managed system 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 managed system。

扩展架构

一种与 Active Directory 一起使用的解决方案，用来确定用户的 DRAC 5 权限；使用 Dell 定义的 Active Directory 对象。

硬件日志

记录由 DRAC 5 和 BMC 生成的事件。

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。

Back to Contents Page