适用于 PowerEdge M1000e 的 Dell Chassis Management Controller 6.10 版

用户指南

DELL EMC

注、小心和警告

注：“注”表示帮助您更好地使用该产品的重要信息。

小心：“小心”表示可能会损坏硬件或导致数据丢失，并说明如何避免此类问题。

警告：“警告”表示可能会造成财产损失、人身伤害甚至死亡。

2018 - 06

Rev. A01

目录

1

概览

适用于 Dell EMC PowerEdge M1000e 机箱的 Dell Chassis Management Controller (CMC) 是系统管理硬件和软件解决方案，用于管理多个 Dell 服务器机箱。它是安装在 Dell PowerEdge M1000e 机箱背面的可热插拔插卡。CMC 具有自己的微处理器和内存，由插入其中的模块化机箱供电。

IT 管理员使用 CMC 可以：

- 查看资源清册
- 执行配置并监测任务
- 远程打开或关闭服务器
- 支持发出有关 M1000e 机箱中服务器和组件的事件警报

您可以将 M1000e 机箱配置为使用一个 CMC 或冗余 CMC。在冗余 CMC 配置中，如果主要 CMC 与 M1000e 机箱或管理网络失去通信，则待机 CMC 会接管机箱管理。

CMC 为服务器提供多个系统管理功能。电源和散热管理是 CMC 的主要功能。

- 机柜级别电源和温度实时自动管理。
  - CMC 可监测系统电源需求，并支持可选的动态电源设备接入模式。此模式使 CMC 可以提高电源效率，方法是根据负载和冗余要求设置待机状态中的电源设备。
  - CMC 报告实时功耗，包括用时间戳记录的高点和低点。
  - CMC 支持对可选机柜的电源上限进行设置，一旦超过该限制就将触发警报或采取措施（例如，节流服务器模块和/或防止打开新刀片服务器的电源），使机柜电源保持在规定的电源上限之内。
  - CMC 将监测并根据实际环境温度和内部温度测量值自动控制冷却风扇。
  - CMC 提供全面的机柜资源清册和状态或错误报告。
- CMC 具有集中配置以下设置的机制：
  - M1000e 机柜的网络和安全设置。
  - 电源冗余和电源上限设置。
  - I/O 交换机和 iDRAC 网络设置。
  - 服务器上的第一引导设备。
  - I/O 模块和服务器之间的 I/O 结构一致性检查。CMC 还根据需要禁用组件，以保护系统硬件。
  - 用户访问安全。

您可以将 CMC 配置为在发生温度、硬件配置错误、断电和风扇速度相关的警告或错误时发送电子邮件警报或 SNMP 陷阱警报。

主题：

本发行版中的新增功能

此版本适用于 Dell PowerEdge M1000e 的 CMC 支持：

- 更新 Linux 内核开放源代码软件包至版本 4.9.31。
- 带有 24 个字符长度的插槽名称可标识单个服务器。
- 128 位会话标识符。
- 为 TMP8501 警报启用 SNMP 陷阱。
- 机箱配置文件 xml 文件中的扩展结构 Flex Address 配置支持。
- 联邦信息处理标准 (FIPS) 140-2 加密功能。
- 启用 Windows 文件共享协议版本 SMBv2 和 SMBv3。
- 更新 OpenSSH 开放源代码软件包到版本 7.6p1。SSH 的最短密钥长度为 1024 位。

主要功能

CMC 功能分为管理功能和安全保护功能。

管理功能

CMC 提供以下管理功能：

- 冗余 CMC 环境。
- IPv4 和 IPv6 的动态域名系统 (DDNS) 注册。
- 使用 SNMP、Web 界面、iKVM、Telnet 或 SSH 连接进行远程系统管理和监测。
- 监测 - 允许访问系统信息和组件状态。
- 访问系统事件日志 - 允许访问硬件日志和 CMC 日志。
- 不同机箱组件的固件更新 - 支持更新 CMC、服务器、iKVM 和 I/O 模块基础结构设备的固件。
- 使用 Lifecycle Controller，在机箱中的多个服务器上进行 BIOS、网络控制器和存储控制器等服务器组件的固件更新。
- 服务器组件更新 - 使用“网络共享”模式一键更新所有刀片。
- Dell OpenManage 软件集成 - 使您能够从 Dell OpenManage Server Administrator 或 IT Assistant 启动 CMC Web 界面。
- CMC 警报 - 通过电子邮件信息或 SNMP 陷阱针对潜在管理节点问题发出警报。
- 远程电源管理 - 从管理控制台提供远程电源管理功能，如关机和重设任意机箱组件。
- 电源使用情况报告。
- 安全套接字层 (SSL) 加密 - 通过 Web 界面提供安全的远程系统管理。
- Integrated Dell Remote Access Controller (iDRAC) Web 界面的启动点。
- 支持 WS-Management。
- FlexAddress 功能 - 使用机箱为特定插槽分配的 WWN/MAC ID 替换出厂配置的全球名称/介质访问控制 (WWN/MAC) ID ；可选升级。
- iDRAC IO 标识功能支持增强的 WWN/MAC 地址资源清册。

- 机箱组件状态和运行状况的图形显示。
- 支持一个和多个插槽的服务器。
- LCD iDRAC 配置向导支持 iDRAC 网络配置。
- iDRAC 单点登录。
- 网络时间协议 (NTP) 支持。
- 增强的服务器摘要、电源报告和电源控制页面。
- 强制 CMC 故障转移以及服务器的虚拟重置。
- 无需重新引导操作系统重设 iDRAC。
- 支持使用 RACADM 配置存储阵列 — 使您可以使用 RACADM 配置 IP、加入或创建组、并选择存储阵列结构。
- 多机箱管理：
  - 从主机箱可查看最多八个组成员机箱。
  - 从主机箱选择机箱配置属性并将其推送至组成员的功能。
  - 组成员保持其机箱设置与主机箱同步的功能。
- 支持将服务器设置和配置信息保存到硬盘并将其还原至相同或不同的服务器。

安全功能

CMC 提供以下安全功能：

- 密码级别安全性管理 - 防止未经授权访问远程系统。
- 通过以下方式集中进行用户验证：
  - 使用标准方案或扩展方案（可选）的 Active Directory。
  - 存储于硬件的用户 ID 和密码。
- 基于角色的授权，使管理员能为每位用户配置特定权限。
- 通过 Web 界面配置用户 ID 和密码。

  注: Web 界面支持 128 位 SSL 3.0 加密和 40 位 SSL 3.0 加密（适用于不接受 128 位加密的国家/地区）。

  注: Telnet 不支持 SSL 加密技术。
- 可配置 IP 端口（如适用）。
- 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。
- 可配置会话自动超时和一个以上并发会话。
- 限制连接到 CMC 的客户端的 IP 地址范围。
- 使用加密层的 Secure Shell (SSH) 实现更高的安全保护。
- 单点登录、双重验证和公共密钥验证。

机箱概览

下图展示了 CMC（插图）的正面和 CMC 插槽在机箱中的位置。

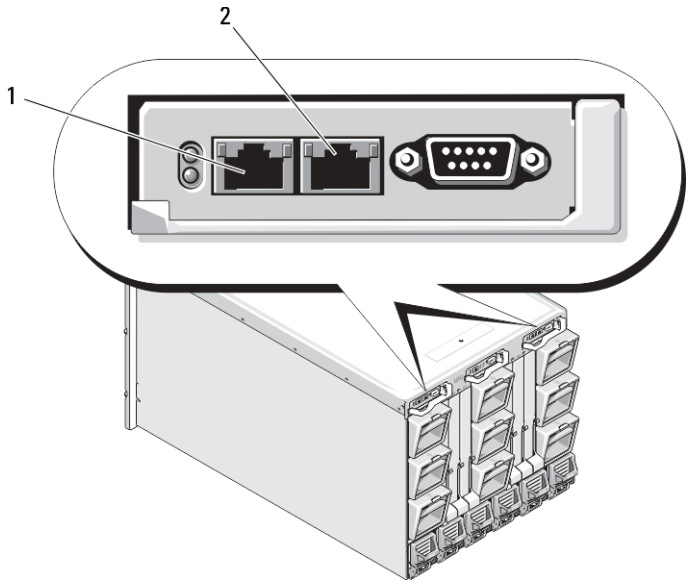


图 1: 机箱中的 CMC 插槽位置

表. 1: CMC 插槽位置详细信息

1	GB 端口
2	STK 端口

CMC 端口信息

通过防火墙远程访问 CMC 需要以下 TCP/IP 端口。这些是 CMC 用于侦听连接的端口。

表. 2: CMC 服务器侦听端口

端口号	功能
22*	SSH
23*	Telnet
80*	HTTP
161	SNMP 代理
443*	HTTPS

* 可配置端口

下表列出了 CMC 用作客户端的端口。

表. 3: CMC 客户端端口

端口号	功能
25	SMTP
53	DNS
68	DHCP 分配的 IP 地址

端口号	功能
69	TFTP
162	SNMP 陷阱
514*	远程系统日志
636	LDAPS
3269	全局编录 (GC) LDAPS

* 可配置端口

最低 CMC 版本

下表列出了启用罗列的刀片服务器所需的最低 CMC 版本。

表. 4: 刀片服务器的最低 CMC 版本

服务器	CMC 的最低版本
PowerEdge M600	CMC 1.0
PowerEdge M605	CMC 1.0
PowerEdge M805	CMC 1.2
PowerEdge M905	CMC 1.2
PowerEdge M610	CMC 2.0
PowerEdge M610x	CMC 3.0
PowerEdge M710	CMC 2.0
PowerEdge M710HD	CMC 3.0
PowerEdge M910	CMC 2.3
PowerEdge M915	CMC 3.2
PowerEdge M420	CMC 4.1
PowerEdge M520	CMC 4.0
PowerEdge M620	CMC 4.0
PowerEdge M820	CMC 4.11
PowerEdge PSM4110	CMC 4.11
PowerEdge M630	CMC 5.0
PowerEdge M830	CMC 5.0
PowerEdge M640	CMC 6.0

下表列出了启用罗列的 IOM 所需的最低 CMC 版本。

表. 5: IOM 的最低 CMC 版本

IOM 交换机	CMC 的最低版本
PowerConnect M6220	CMC 1.0
PowerConnect M6348	CMC 2.1
PowerConnect M8024	CMC 1.2
PowerConnect M8024-k	CMC 3.2
PowerConnect M8428-k	CMC 3.1
Dell 10/100/1000Mb 以太网直通	CMC 1.0
Dell 4Gbps FC 直通模块	CMC 1.0
Dell 8/4Gbps FC SAN 模块	CMC 1.2
Dell 10Gb 以太网直通	CMC 2.1
Dell 10Gb 以太网直通 II 型	CMC 3.0
Dell 10Gb 以太网直通-k	CMC 3.0
Brocade M4424	CMC 1.0
Brocade M5424	CMC 1.2
Cisco Catalyst CBS 3130X-S	CMC 1.0
Cisco Catalyst CBS 3130G	CMC 1.0
Cisco Catalyst CBS 3032	CMC 1.0
Dell Force10 MXL 10/40GbE	CMC 4.11
Dell PowerEdge M I/O 聚合器	CMC 4.2
Mellanox M2401G DDR Infiniband 交换机	CMC 1.0
Mellanox M3601Q QDR Infiniband 交换机	CMC 2.0
Mellanox M4001F/M4001Q FDR/QDR Infiniband 交换机	CMC 4.0
Mellanox M4001T FDR10 Infiniband 交换机	CMC 4.1
Brocade M6505	CMC 4.3
Cisco Nexus B22DELL	CMC 4.3

此发行版的最新固件版本

下表列出了支持下列服务器的 BIOS、iDRAC 和 Lifecycle Controller 的最新固件版本：

表. 6: BIOS、iDRAC 和 Lifecycle Controller 的最新固件版本

服务器	BIOS	iDRAC	Lifecycle Controller
PowerEdge M600	2.4.0	1.65	不适用
PowerEdge M605	5.4.1	1.65	不适用
PowerEdge M805	2.3.3	1.65	不适用
PowerEdge M905	2.3.3	1.65	不适用

服务器	BIOS	iDRAC	Lifecycle Controller
PowerEdge M610	6.3.0	3.50	1.6
PowerEdge M610x	6.3.0	3.50	1.6
PowerEdge M710	6.4.0	3.80	1.7.5.4
PowerEdge M710HD	7.0.0	3.50	1.6
PowerEdge M910	2.9.0	3.50	1.6
Power Edge M915	3.2.2	3.80	1.7.5.4
PowerEdge M420	2.3.3	2.40.40.40	2.40.40.40
PowerEdge M520	2.4.2	2.40.40.40	2.40.40.40
PowerEdge M620	2.5.4	2.40.40.40	2.40.40.40
PowerEdge M820	2.3.3	2.40.40.40	2.40.40.40
PowerEdge M630	2.7.1	2.52.52.52	2.52.52.52
PowerEdge M830	2.7.1	2.52.52.52	2.52.52.52
PowerEdge M640	1.0.0	3.10.10.10	3.10.10.10

注: 阵列软件版本 6.0.4 支持 PowerEdge PSM4110。

支持的远程访问连接

下表列出支持的远程访问控制器。

表. 7: 支持的远程访问连接

连接	功能
CMC 网络接口端口	• GB 端口：CMC Web 界面专用网络接口。两个 10/100/1000 Mbps 端口，一个用于管理，另一个用于机箱到机箱的电缆整合。 • STK：机箱到机箱管理网络电缆整合的上行链路端口。 • 10 Mbps/100 Mbps/1 Gbps 以太网，通过 CMC GbE 端口。 • DHCP 支持。 • SNMP 陷阱和电子邮件事件通知。 • iDRAC 和 I/O 模块 (IOM) 的网络接口。 • 支持 Telnet/SSH 命令控制台和 RACADM CLI 命令，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。 • 支持专门设计使用二进制协议与特定类型 IOM 通信的应用程序进行二进制交换。 • 通过 connect（或 racadm connect）命令，可将串行端口连接到内部服务器的串行控制台或 I/O 模块。
其他连接	• 通过 Avocent 集成 KVM 交换机模块 (iKVM) 访问 Dell CMC 控制台。

支持的平台

CMC 支持为 PowerEdge M1000e 平台设计的模块化系统。有关 CMC 兼容性的信息，请参阅设备的说明文件。

有关最新支持的平台，请参阅 **dell.com/cmcmanuals** 上的 *Chassis Management Controller Version 6.0 Release Notes（Chassis Management Controller 6.0 版发行说明）*。

支持的 Management Station Web 浏览器

有关支持的 Web 浏览器的最新信息，请参阅 **dell.com/cmcmanuals** 上的 *Chassis Management Controller Version 6.1 Release Notes*（Chassis Management Controller 6.1 版发行说明）。

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari 版本 8.0.8
- Safari 版本 9.0.3
- Mozilla Firefox 57
- Mozilla Firefox 58
- Google Chrome 62
- Google Chrome 63

注: 默认情况下，此发行版支持 TLS 1.1 和 TLS 1.2。但是，要启用 TLS 1.0，请使用以下 RACADM 命令：

```
$ racadm config -g cfgRacTuning -o cfgRacTuneTLSProtocolVersionEnable TLSv1.0+
```

查看 CMC Web 界面的本地化版本

要查看 CMC Web 界面的本地化版本：

1 打开 Windows **控制面板**。
2 双击**区域选项**图标。
3 从 **您的区域设置 [位置]**下拉菜单选择所需区域设置。

支持的管理控制台应用程序

CMC 支持与 Dell OpenManage IT Assistant 集成。有关更多信息，请参阅 Dell 支持网站 **dell.com/support/manuals** 上的 IT Assistant 说明文件集。

您可能需要的其他说明文件

除了本指南以外，您可以在此网站获取以下指南：**dell.com/support/manuals**。选择 **Choose from a list of all Dell products（从所有 Dell 产品列表中选择）**，然后单击 **Continue（继续）**。单击 **Software , Monitors , Electronics & Peripherals（软件、显示器、电子设备及外围设备）** > **Software（软件）**：

- 单击 **Remote Enterprise System Management**（远程企业系统管理），然后单击 **Dell Chassis Management Controller Version 6.0**（Dell Chassis Management Controller 版本 4.45）以查看：
  - *CMC Online Help*（CMC 联机帮助）提供了有关使用 Web 界面的信息。
  - *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*（Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范）提供最低 BIOS 和固件版本、安装和使用情况的信息。
  - *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）提供了关于 RACADM 子命令、支持的界面、属性数据库组和对象定义的信息。
  - **dell.com/cmcmanuals** 上提供的 *Chassis Management Controller Version 6.0 Release Notes*（Chassis Management Controller 5.2 版发行说明）为有经验的用户或技术人员提供了系统、说明文件或高级技术参考资料的最新更新。

- 单击 **Remote Enterprise System Management**（远程企业系统管理），然后单击所需的 iDRAC 版本号以查看 *Integrated Dell Remote Access Controller 7 (iDRAC) User's Guide*（Integrated Dell Remote Access Controller 7 (iDRAC7) 用户指南），该指南提供了在管理系统上安装、配置和维护 iDRAC 的信息。
- 单击 **Enterprise System Management**（企业系统管理），然后单击产品名称以查看下列说明文件：
  - *Dell OpenManage Server Administrator's User's Guide*（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 SNMP Reference Guide for iDRAC and Chassis Management Controller*（Dell OpenManage SNMP for iDRAC and Chassis Management Controller 参考指南）提供了有关 SNMP MIB 的信息。
  - *Dell Update Packages User's Guide*（Dell Update Package 用户指南）提供了有关获取和作为系统更新策略的一部分使用 Dell Update Package 的信息。

以下系统说明文件在以下网站可用：**dell.com/support/manuals**，这些文件提供了有关安装了 CMC 的系统的更多信息。

- 系统随附的安全说明提供了重要的安全和法规信息。其他法规信息请参阅法规合规性主页，网址是 **dell.com/regulatory_compliance**。保修信息可能包含于此说明文件中，也可能为单独的说明文件。
- 机架解决方案中的 *Rack Installation Guide*（机架安装指南）和 *Rack Installation Instructions*（机架安装说明）介绍如何将系统安装到机架中。
- *Hardware Owner's Manual*（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。
- 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。
- 系统可能附带 Chassis Management Controller 6.0 版发行说明或自述文件，这些文件为有经验的用户或技术人员提供了系统、说明文件或高级技术参考资料的最新更新。
- 有关 IOM 网络设置的更多信息，请参阅 *Dell PowerConnect M6220 Switch Important Information*（Dell PowerConnect M6220 交换机重要信息）说明文件和 *Dell PowerConnect 6220 Series Port Aggregator White Paper*（Dell PowerConnect 6220 系列端口聚合器白皮书）。
- 针对第三方管理控制台应用程序的说明文件。

联系戴尔

注: 如果没有可用的互联网连接，可在购货发票、装箱单、帐单或戴尔产品目录上查找联系信息。

戴尔提供了几种在线以及基于电话的支持和服务选项。可用性会因国家和地区以及产品的不同而有所差异，某些服务可能在您所在的国家/地区不可用。有关销售、技术支持或客户服务问题，请联系戴尔：

1. 请转至 **Dell.com/support**。
2. 选择您的支持类别。
3. 在页面底部的**选择国家/地区**下拉列表中，确认您所在的国家或地区。
4. 根据您的需要选择相应的服务或支持链接。

社交媒体参考

要了解有关 Dell 解决方案和服务的产品、最佳做法和信息的更多详情，可访问社交媒体平台，如 Dell TechCenter 和 YouTube。您也可以访问 **www.delltechcenter.com/cmc**，查看 CMC wiki 页面上的博客、论坛、白皮书和实际操作视频等。以下是适用于 CMC 5.0 的实际操作视频：

- 在 PowerEdge M1000E 机箱中复制服务器配置配置文件
- 使用快速部署功能将配置文件分配给服务器插槽
- 重设 iDRAC 而无需重新引导操作系统
- 多机箱管理

这些实际操作视频也可以在 YouTube 上找到。

若要获取 CMC 说明文件和其他相关固件说明文件，请参阅 **www.dell.com/esmmanuals**

2

安装和设置 CMC

这部分介绍如何安装 PowerEdge M1000e Chassis Management Controller (CMC) 硬件、建立对 CMC 的访问、配置您的管理环境以使用 CMC 并引导您完成随后的 CMC 配置步骤：

- 设置对 CMC 的初始访问。
- 通过网络访问 CMC。
- 添加并配置 CMC 用户。
- 更新 CMC 固件。

有关安装和设置冗余 CMC 环境的更多信息，请参阅了解冗余 CMC 环境。

主题：

开始之前

设置 CMC 环境之前，请从 **support.dell.com** 下载最新版本的 CMC 固件。

此外，确保您拥有系统随附的 *ell Systems Management Tools and Documentation* DVD。

安装 CMC 硬件

CMC 已预先安装在机箱中，因此无需安装。可以安装第二个 CMC 作为活动 CMC 的备用。

相关链接

了解冗余 CMC 环境

设置机箱一览表

使用以下步骤可准确设置机箱：

1 确保 CMC 与使用浏览器的管理站位于相同的网络中，即管理网络。将以太网网络电缆从标记为 **GB** 的 CMC 端口连接至管理网络。

注: 不要将电缆插入标有 STK 的 CMC 以太网端口。有关用电缆连接 STK 端口的更多信息，请参阅了解冗余 CMC 环境。

2 在机箱中安装 I/O 模块，并连接电缆。

3 在机箱中插入服务器。

4 将机箱与电源相连。

5 按下机箱左下角的电源按钮，或者在完成步骤 7 后，从 CMC Web 界面打开机箱电源。

注: 不要打开服务器电源。

6 使用系统前端的 LCD 面板，为 CMC 提供静态 IP 地址或配置为 DHCP。

7 连接至 CMC IP 地址并提供默认用户名 (root) 和密码 (calvin)。

8 在 CMC Web 界面中为每个 iDRAC 提供一个 IP 地址并启用 LAN 和 IPMI 接口。

注: 有些服务器上的 iDRAC LAN 接口默认为禁用。

9 在 CMC Web 界面中为每个 I/O 模块提供一个 IP 地址。

10 连接到各 iDRAC 并提供 iDRAC 的最终配置。默认用户名是 *root*，密码是 *calvin*。

11 通过 Web 浏览器连接至每个 I/O 模块，并提供 I/O 模块的最终配置。

12 打开服务器电源并安装操作系统。

注: 如果控制面板未正确安装到机箱上，CMC 将重新启动。

基本 CMC 网络连接

小心: 将 STK 端口连接到管理网络可以获得意想不到的结果。将 GB 和 STK 布线到相同的网络（广播域）会造成广播风暴。

为了提供最高的冗余度，请将每个可用的 CMC 连接到您的管理网络。

每个 CMC 都有两个 RJ-45 以太网端口，分别标记为 **GB**（上行链路端口）和 **STK**（堆栈或缆线集合端口）。利用基本的布线，您可以将 GB 端口连接到管理网络并保持 STK 端口闲置。

菊花链式 CMC 网络连接

如果一个机架中有多个机箱，则可以通过以菊花链式连接最多四个机箱来减少与管理网络之间的连接数。如果 4 个机箱中各包含一个冗余 CMC，则通过菊花链式连接，您可以将必需的管理网络连接数从 8 个减少到 2 个。如果每个机箱只有一个 CMC，则您可以将必需的连接数从 4 个减少到 1 个。

当采用菊花链式连接机箱时，GB 是上行端口，而 STK 是堆栈（电缆合并）端口。将 GB 端口连接到管理网络或机箱中 CMC 的更接近网络的的 STK 端口。将 STK 端口仅连接到离链或网络更远的 GB 端口。

在活动的 CMC 插槽和第二 CMC 插槽中为 CMC 创建单独的链。

下图显示四个菊花链式连接机箱的线缆布置，每个机箱都具有活动和待机 CMC。

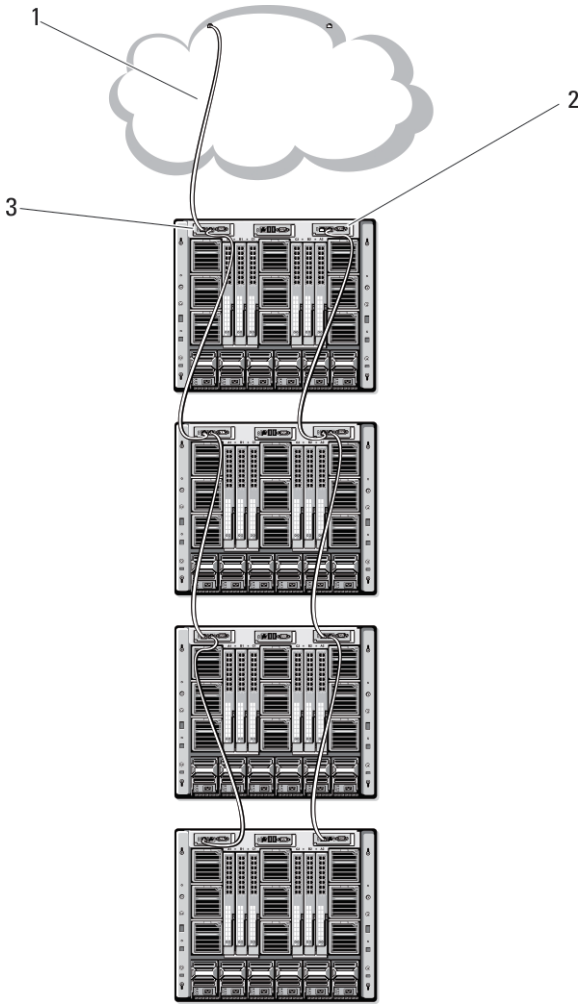


图 2: 菊花链式 CMC 网络

1	管理网络
2	待机 CMC
3	活动 CMC

下图提供不正确的 CMC 电缆连接的示例。

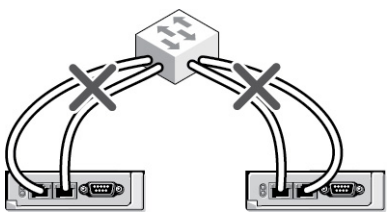


图 3: CMC 网络布线错误 - 2 个 CMC

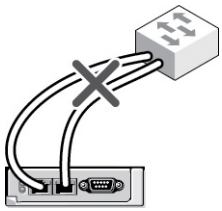


图 4: CMC 网络布线错误 - 单个 CMC

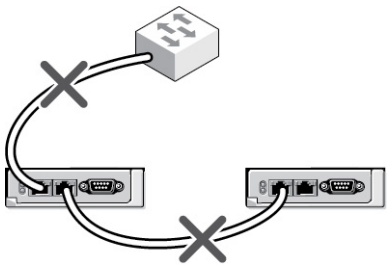


图 5: CMC 网络布线错误 - 2 个 CMC

将最多四个机箱使用菊花链式连接：

1 将第一个机箱活动 CMC 的 GB 端口连接到管理网络。
2 将第二个机箱活动 CMC 的 GB 端口连接到第一个机箱活动 CMC 的 STK 端口。
3 如果有第三个机箱，请将其活动 CMC 的 GB 端口连接到第二个机箱活动 CMC 的 STK 端口。
4 如果有第四个机箱，请将其活动 CMC 的 GB 端口连接到第三个机箱的 STK 端口。
5 如果机箱中有冗余 CMC，请使用相同的方式进行连接。

小心: 任何 CMC 的 STK 端口永远都不会连接到管理网络。它只能连接到其他机箱的 GB 端口。将 STK 端口连接到管理网络会中断网络并导致数据丢失。用电缆将 GB 和 STK 端口连接到相同网络（广播域）会引发广播风暴。

注: 请勿将活动 CMC 连接到待机 CMC。

注: 重设 STK 端口链接至另一个 CMC 的 CMC 可能会中断链接后面的 CMC 的网络。子 CMC 可能会记录消息表明网络链接已丢失，且它们可能故障切换到冗余 CMC。

6 要开始使用 CMC，请参阅在管理站上安装远程访问软件。

在管理站上安装远程访问软件

可使用远程访问软件（例如 Telnet、Secure Shell (SSH) 或操作系统上提供的串行控制台公用程序）或使用 Web 界面从管理工作站上访问 CMC。

若要从管理站使用远程 RACADM，则使用系统随附的 *Dell Systems Management Tools and Documentation* DVD 安装远程 RACADM。这张 DVD 包括以下 Dell OpenManage 组件：

- DVD 根目录 - 包含 Dell Systems Build and Update Utility。
- SYSMGMT - 包含系统管理软件产品，其中包括 Dell OpenManage Server Administrator。
- DOCS - 包含系统、系统管理软件产品、外设和 RAID 控制器的说明文件。
- SERVICE - 包含配置系统所需的工具，并提供最新的诊断程序和 Dell 专为您的系统优化的驱动程序。

有关安装 Dell OpenManage 软件组件的信息，请参阅 DVD 或 **dell.com/support/manuals** 上提供的 *Dell OpenManage Installation and Security User's Guide*（Dell OpenManage 安装和安全用户指南）。您还可以从 **dell.com/support** 下载最新版本的 Dell DRAC 工具。

在 Linux 管理站上安装 RACADM

1 以根用户身份登录到运行支持的 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统，从而在该系统中安装管理系统组件。

2 将 *Dell Systems Management Tools and Documentation* DVD 插入 DVD 驱动器中。

3 若要将 DVD 装载到所需位置，则使用 mount 命令或类似命令。

注: 在 Red Hat Enterprise Linux 5 操作系统中，DVD 光盘是使用 `-noexec mount` 选项自动挂载。该选项不允许从 DVD 光盘运行任何可执行程序。您需要手动挂载 DVD-ROM，然后运行可执行程序。

4 导航至 **SYSMGMT/ManagementStation/linux/rac** 目录。要安装 RAC 软件，请输入以下命令：

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

5 要查看 RACADM 命令帮助，请在运行前面的命令后键入 `racadm help`。有关 RACADM 的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

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 <file name>`

从 Linux 管理站卸载 RACADM

1 以根用户身份登录到要卸载管理站功能的系统上。

2 使用以下 rpm 查询命令确定已安装的是哪个版本的 DRAC 工具：

```
rpm -qa | grep mgmtst-racadm
```

3 验证要卸载的软件包版本，并使用 rpm 卸载该功能。

```
-e rpm -qa | grep mgmtst-racadm command
```

配置 Web 浏览器

您可以通过 Web 浏览器来配置和管理 CMC、服务器、以及安装在机箱中的模块。请参阅 *Readme*（自述文件）中的*支持的浏览器*部分，网址：**dell.com/support/manuals**。

CMC 与使用浏览器的管理站必须位于相同的网络中，即*管理网络*。根据安全性要求，管理网络应该是隔离的、高度安全的网络。

注: 确保管理网络上的安全措施（如防火墙和代理服务器）不会阻止 Web 浏览器访问 CMC。

一些浏览器功能会干扰连接或性能，特别是当管理网络没有到 Internet 的路由时。如果管理站在 Windows 操作系统上运行，有些 Internet Explorer 设置会干扰连接，即使使用命令行界面访问管理网络时也会如此。

相关链接

代理服务器
Microsoft Phishing Filter
证书吊销列表访存
使用 Internet Explorer 从 CMC 下载文件
允许在 Internet Explorer 中播放动画

代理服务器

要通过对管理网络无访问权限的代理服务器进行浏览，可以将管理网络地址添加到浏览器的例外列表中。这样可以使浏览器在访问管理网络时绕过代理服务器。

Internet Explorer

要编辑 Internet Explorer 中的例外列表，请执行以下操作：

1 启动 Internet Explorer。
2 单击**工具** > **Internet 选项** > **连接**。
3 在**局域网 (LAN) 设置**部分，单击 **LAN 设置**。
系统会显示**局域网 (LAN) 设置**对话框。
4 在**局域网 (LAN) 设置**对话框中，转至**代理服务器**部分，选中**为 LAN 使用代理服务器**选项。
高级选项将变为启用状态。
5 单击**高级**。
6 在**例外**部分，将管理网络上的 CMC 和 iDRAC 地址作为分号分隔的列表进行添加。您可以在条目中使用 DNS 名称和通配符。

Mozilla Firefox

要在 Mozilla Firefox 版本 3.0 中编辑例外列表，请执行以下操作：

1 启动 Mozilla Firefox。
2 单击**工具** > **选项**（对于运行 Windows 的系统）或单击**编辑** > **首选项**（对于运行 Linux 的系统）。
3 单击**高级**，然后单击**网络**选项卡。
4 单击**设置**。
5 选择**手动配置代理**。
6 在**不使用代理**字段中，以逗号分隔形式输入管理网络上的 CMC 和 iDRAC 地址。可以在条目中使用 DNS 名称和通配符。

Microsoft Phishing Filter

如果在管理系统上的 Internet Explorer 7 中启用 Microsoft Phishing Filter 且 CMC 不能访问 Internet，则对 CMC 的访问可能会延迟几秒钟。在使用浏览器或远程 RACADM 等其他接口时会发生这种延迟。执行以下步骤可禁用 Phishing Filter：

1 启动 Internet Explorer。
2 单击**工具** > **Phishing Filter**，然后单击 **Phishing Filter** 设置。
3 选中**禁用 Phishing Filter** 复选框，然后单击**确定**。

证书吊销列表访存

如果 CMC 无权访问 Internet，请禁用 Internet Explorer 中的证书撤回列表 (CRL) 访存功能。该功能将检测服务器（例如 CMC Web 服务器）是否使用从 Internet 检索的证书撤回列表 (CRL) 中的证书。如果 Internet 无法访问，使用浏览器或远程 RACADM 等命令行界面访问 CMC 时，此功能可能导致几秒钟的延迟。

要禁用 CRL 访存，请执行以下操作：

1 启动 Internet Explorer。
2 单击**工具** > **Internet 选项**，然后单击**高级**。
3 滚动到**安全**部分，清除**检查发行商的证书是否吊销**复选框，然后单击**确定**。

使用 Internet Explorer 从 CMC 下载文件

当使用 Internet Explorer 从 CMC 下载文件时，如果未启用**不将加密的页面存入硬盘**选项，您可能会遇到问题。
要启用**不将加密的页面存入硬盘**选项，请执行以下操作：

1 启动 Internet Explorer。
2 单击**工具** > **Internet 选项** > **高级**。
3 滚动到**安全**部分，选中**不将加密的页存盘**。

允许在 Internet Explorer 中播放动画

当与 Web 界面互传文件时，文件传输图标会旋转以指示存在传输活动。使用 Internet Explorer 时，必须将浏览器配置为允许播放动画。
要将 Internet Explorer 配置为播放动画，请执行以下操作：

1 启动 Internet Explorer。
2 单击**工具** > **Internet 选项** > **高级**。
3 滚动到**多媒体**部分，选中**在网页中播放动画**选项。

设置对 CMC 的初始访问

要远程管理 CMC，请将 CMC 连接到您的管理网络，然后配置 CMC 网络设置。

注: 若要管理 M1000e 解决方案，它必须连接到管理网络。

有关配置 CMC 网络设置的信息，请参阅配置初始 CMC 网络。此初始配置分配可启用对 CMC 访问的 TCP/IP 网络参数。

确保各服务器上的 CMC 和 iDRAC 以及所有交换机 I/O 模块上的网络管理端口都连接到 M1000e 机箱内的公共内部网络。这样可以将管理网络与服务器数据网络隔离。流量隔离对于机箱管理的不间断访问非常重要。

CMC 已连接到管理网络。所有对 CMC 和 iDRAC 的外部访问都通过 CMC 完成。对受管服务器的访问则通过与输入/输出模块 (IOM) 的网络连接完成。这使应用程序网络能够与管理网络相互隔离。

建议您将机箱管理与数据网络相隔离。Dell 不支持或保证不正确集成到环境中的机箱的正常运行时间。由于数据网络上存在潜在的流量，因而内部管理网络上的管理接口可能会因发送到服务器的流量而处于饱和状态。这将导致 CMC 和 iDRAC 通信发生延迟。这些延迟可能会使机箱发生意想不到的行为，例如，即使 iDRAC 启动并在运行，CMC 也会将其显示为脱机，这又会导致其他不期望的行为。如果物理隔离管理网络的做法不切实际，可以将 CMC 和 iDRAC 流量分离到单独的 VLAN。CMC 和各个 iDRAC 网络接口可配置为使用 VLAN。

如果您有一个机箱，请将 CMC 和待机 CMC 连接到管理网络。如果有一个冗余 CMC，则使用另一条网络电缆并将 **GB** CMC 端口连接到管理网络的第二个端口。

如果有多个机箱，您可以在基本连接（将每个 CMC 连接到管理网络）或菊花链式机箱连接（多个机箱串联起来，只有一个 CMC 连接到管理网络）之间选择。基本连接类型使用管理网络上更多的端口，并提供更好的冗余。菊花链式连接类型使用管理网络上较少的端口，但增加了 CMC 间的相关性，降低了系统的冗余。

注: 在冗余配置中不正确连接 CMC 的电缆会导致无法管理并可能引发广播风暴。

相关链接

基本 CMC 网络连接
菊花链式 CMC 网络连接
配置初始 CMC 网络

配置初始 CMC 网络

注: 更改 CMC 网络设置可能会断开当前网络连接。

可以在 CMC 得到 IP 地址之前或之后执行 CMC 初始网络配置。要在得到 IP 地址之前配置 CMC 的初始网络设置，您可以使用以下任一界面：

- 机箱前面的 LCD 面板
- Dell CMC 串行控制台

要在 CMC 得到 IP 地址之后配置初始网络设置，可以使用以下任意界面：

- 命令行界面 (CLI)，如串行控制台、Telnet、SSH 或通过 iKVM 连接的 Dell CMC 控制台
- 远程 RACADM
- CMC Web 界面

CMC 同时支持 IPv4 和 IPv6 寻址模式。IPv4 和 IPv6 的配置设置相互独立。

使用 LCD 面板界面配置 CMC 网络

注: 只有部署 CMC 或更改默认密码后，使用 LCD 面板配置 CMC 的选项才可用。如果密码未更改，您可以继续使用 LCD 重设 CMC 的配置，但可能会导致安全风险。

LCD 面板位于机箱前面的左下角。

要使用 LCD 面板界面设置网络，请执行以下操作：

1 按下机箱电源按钮将其打开。
通电时，LCD 屏幕将显示一系列初始化屏幕。准备就绪后，**Language Setup（语言设置）**屏幕将会显示。

2 使用箭头按钮选择语言，然后按下中央按钮以选择**接受/是**，并再次按下中央按钮。
机柜屏幕显示以下问题：是否**配置机柜**？

- 按下中央按钮继续到 CMC **网络设置**屏幕。请参阅步骤 4。
- 要退出 **Configure Enclosure（配置机柜）**菜单，请选择“否”图标并按下中央按钮。请参阅步骤 9。

3 按下中央按钮继续到 CMC **网络设置**屏幕。

4 使用向下箭头按钮选择网络速度（10Mbps、100Mbps、自动 (1 Gbps)）。
“网络速度”设置必须与您的网络配置相匹配才能实现有效的网络吞吐量。将“网络速度”设置为低于网络配置的速度会增加带宽消耗，并使网络通信变慢。**您必须确定网络是否支持以上网络速度并进行相应的设置**。如果您的网络配置与此处的任何值不匹配，则建议您使用“自动协商”（**Auto（自动）**选项）或咨询网络设备制造商。

按中央按钮继续到下一个 **CMC 网络设置**屏幕。

5 选择匹配网络环境的双工模式（半双工或全双工）。

注：如果“自动协商”设置为“开启”或选择 1000MB (1Gbps)，则网络速度和双工模式设置不可用。

如果为一个设备打开了自动协商，但没有为另一个设备打开，则使用自动协商的设备可以确定其他设备的网络速度，但不能确定双工模式；此时，双工模式将在自动协商期间默认为半双工设置。这种双工模式的不匹配会造成网络连接变慢。

按中央按钮继续到下一个 **CMC 网络设置**屏幕。

6 选择要用于 CMC 的 Internet 协议（IPv4、IPv6 或两者），然后按下中央按钮继续到下一个 **CMC 网络设置**屏幕。

7 选择希望 CMC 以何种方式获得 NIC IP 地址：

动态主机配置协议 (DHCP)	CMC 会自动从网络上的 DHCP 服务器检索 IP 配置（IP 地址、掩码和网关）。CMC 将获得在您的网络上分配的唯一 IP 地址。如果已选择 DHCP 选项，请按下中央按钮。随即出现 **Configure iDRAC（配置 iDRAC）**屏幕；转至步骤 9。
静态	在随即出现的屏幕中手动输入 IP 地址、网关和子网掩码： 如果已经选择**静态**选项，请按下中央按钮继续到下一个 **CMC 网络设置**屏幕，然后： • 您可以使用以下方法设置 **Static IP Address（静态 IP 地址）**：使用左右箭头键可以在位置之间移动，使用上下箭头键可以为每个位置选择编号。完成 **Static IP Address（静态 IP 地址）**设置后，按下中央按钮以继续。 • 设置子网掩码，然后按中央按钮。 • 设置网关，然后按中央按钮。随即显示 **Network Summary（网络摘要）**屏幕。 **Network Summary（网络摘要）**屏幕列出了您输入的 **Static IP Address（静态 IP 地址）**、**Subnet Mask（子网掩码）**和 **Gateway（网关）**设置。检查设置的准确性。要更正设置，可以导航至左箭头按钮，然后按下中央键以返回该设置屏幕。更正后，按下中央按钮。 • 确认所输入的设置的准确性后，按下中央按钮。**Register DNS?（是否注册 DNS？）**屏幕将显示。

注：如果为 CMC IP 配置选择动态主机配置协议 (DHCP) 模式，则在默认情况下还将启用 DNS 注册。

8 如果在上一步中选择了 **DHCP**，请转至步骤 10。

要注册 DNS 服务器的 IP 地址，按下中央按钮以继续。如果没有 DNS，按右箭头键。**Register DNS?（是否注册 DNS？）**屏幕将出现；转至步骤 10。

您可以使用以下方法设置 **DNS IP Address（DNS IP 地址）**：使用左右箭头键可以在位置之间移动，使用上下箭头键可以为每个位置选择编号。完成 DNS IP Address（DNS IP 地址）设置后，按下中央按钮以继续。

9 表明您是否希望配置 iDRAC：

- **否**：请跳至步骤 13。
- **是**：请按下中央按钮继续。

您也可以从 CMC GUI 配置 iDRAC。

10 选择要用于服务器的 Internet 协议（IPv4、IPv6 或两者）。

动态主机配置协议 (DHCP)	iDRAC 会自动从网络上的 DHCP 服务器检索 IP 配置（IP 地址、掩码和网关）。iDRAC 将获得在您的网络上分配的唯一 IP 地址。按中央按钮。
静态	必须在随即出现的屏幕中手动输入 IP 地址、网关和子网掩码。 如果已经选择**静态**选项，请按下中央按钮继续到下一个 **iDRAC 网络设置**屏幕，然后： • 您可以使用以下方法设置 **Static IP Address（静态 IP 地址）**：使用左右箭头键可以在位置之间移动，使用上下箭头键可以为每个位置选择编号。此地址是第一个插槽中 iDRAC 的静态 IP。随后各个 iDRAC 的静态 IP 地址将基于该 IP 地址与插槽号增量计算得出。完成 **Static IP Address（静态 IP 地址）**设置后，按下中央按钮以继续。 • 设置子网掩码，然后按中央按钮。 • 设置网关，然后按中央按钮。

- 选择是否**启用**或**禁用** IPMI LAN 通道。按下中央按钮以继续。

- 在 **iDRAC Configuration（iDRAC 配置）**屏幕上，要将所有 iDRAC 网络设置应用到已安装的服务器，则高亮显示 **Accept/Yes（接受/是）**图标并按中央按钮。如果不打算将 iDRAC 网络设置应用到已安装的服务器，则高亮显示 **No（否）**图标并按下中央按钮，然后继续步骤 c。
- 在下一个 **iDRAC Configuration（iDRAC 配置）**屏幕上，要将所有 iDRAC 网络设置应用到新安装的服务器，则高亮显示 Accept/Yes（接受/是）图标并按中央按钮；将新服务器插入机箱时，LCD 将提示用户是否使用之前配置的网络设置/策略自动部署服务器。如果不打算将 iDRAC 网络设置应用到新安装的服务器，则高亮显示 **No（否）**图标并按下中央按钮；将新服务器插入机箱时，不会配置 iDRAC 网络设置。

11 在 **Enclosure（机柜）**屏幕上，要应用所有机柜设置，则高亮显示 **AAccept/Yes（接受/是）**图标并按中央按钮。如果不打算应用机柜设置，则高亮显示 **No（否）**图标并按下中央按钮。

12 在 **IP Summary（IP 摘要）**屏幕上，检查您提供的 IP 地址以确保地址准确无误。要更正设置，可以导航至左箭头按钮，然后按下中央键以返回该设置屏幕。更正后，按下中央按钮。如果需要，可以导航至右箭头按钮，然后按下中央键以返回 **IP Summary（IP 摘要）**屏幕。

当您确认输入的设置正确之后，按下中央按钮。配置向导将关闭并返回到 **Main Menu（主菜单）**屏幕。

注: 如果您选择了是/接受，在显示 IP 摘要屏幕之前，将显示等待屏幕。

现在可以在网络上使用 CMC 和 iDRAC。您可以使用 Web 界面或诸如串行控制台、Telnet 和 SSH 等 CLI 通过分配的 IP 地址访问 CMC。

注: 通过 LCD 配置向导完成网络设置后，该向导将不再可用。

访问 CMC 的界面和协议

配置完 CMC 网络设置后，您可以通过各种界面远程访问 CMC。下表列出您可用于远程访问 CMC 的界面。

注: 因 Telnet 没有其他接口安全，所以默认禁用。启用使用 Web、ssh 或远程 RACADM 的 Telnet。

注: 同时使用一个以上的界面可能会产生意外的结果。

表. 8: CMC 界面

界面	说明
Web 界面	可使用图形用户界面远程访问 CMC。Web 界面构建在 CMC 固件中并从管理站上的受支持 Web 浏览器通过 NIC 接口访问。 有关支持的 Web 浏览器的列表，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller Version 5.0 Release Notes*（Chassis Management Controller 5.0 版发行说明）中的“支持的浏览器”部分。
远程 RACADM 命令行界面	使用此命令行公用程序管理 CMC 及其组件。您可以使用远程或固件 RACADM： • 远程 RACADM 是在管理站上运行的客户端公用程序。它使用带外网络接口在受管系统上运行 RACADM 命令，并且使用 HTTPs 通道。`-r` 选项在网络上运行 RACADM 命令。 • 固件 RACADM 可以通过使用 SSH 或 Telnet 登录 CMC 进行访问。您可以在不指定 CMC IP、用户名或密码的情况下运行固件 RACADM 命令。在输入 RACADM 提示符时，您可以在不加 racadm 前缀的情况下直接运行命令。
机箱 LCD 面板	使用前面板上的 LCD 可以： • 查看警报、CMC IP 或 MAC 地址、用户可编程字符串。 • 设置 DHCP • 配置 CMC 静态 IP 设置。 • 查看活动 CMC 的 CMC MAC 地址。 • 查看附加到 CMC IP 结尾的 CMC VLAN ID（如果已配置 VLAN）。
Telnet	提供命令行界面，用于通过网络访问 CMC。CMC 命令行提供 RACADM 命令行界面和 connect 命令，用于连接到服务器或 IO 模块的串行控制台。

界面	说明
	注: Telnet 不是安全协议，并且在默认情况下处于禁用状态。Telnet 可传输所有数据，包括纯文本形式的密码。当传输敏感信息时，请使用 SSH 界面。
SSH	使用 SSH 运行 RACADM 命令。它所提供的功能与使用加密传输层的 Telnet 控制台相同，可提供更高的安全性。SSH 服务默认在 CMC 上处于启用状态，可以被禁用。
WSMan	CMC 远程服务基于一对多系统管理任务的 WS-Management 协议。您必须使用 WSMan 客户端（如 WinRM 客户端 (Windows) 或 Open WSMan 客户端 (Linux)）来使用 CMC 远程服务功能。您也可以使用 Power Shell 和 Python 来编写 WSMan 界面脚本。 Web Services for Management (WS-Management) 是基于简单对象访问协议 (SOAP) 的系统管理协议。CMC 使用 WS - Management 传递分布式管理综合小组 (DMTF) 基于公用信息模型 (CIM) 的管理信息。CIM 信息定义了可在管理系统中修改的语义和信息类型。 CMC WSMan 实施在端口 443 上采用 SSL 实现传输安全性，并且支持基本验证。通过 WS-Management 获得的数据由映射到 DMTF 配置文件和扩展名配置文件的 CMC 工具界面提供。 有关更多信息，请参阅以下内容： • MOF 和配置文件 - **delltechcenter.com/page/DCIM.Library** • DTMF 网站 - **dmtf.org/standards/profiles/** • WSMan 发行说明或自述文件。 • **www.wbemsolutions.com/ws_management.html** • DMTF WS-Management 规范：**www.dmtf.org/standards/wbem/wsman** 可以通过利用 Windows WinRM、Powershell CLI 等客户端基础结构、WSMANCLI 等开放源代码公用程序、以及 Microsoft .NET 等应用程序编程环境来使用 Web 服务界面。 WinRM 工具为其发送的所有 WSMan 命令设置 60 秒的默认响应超时。WinRM 不允许改变此超时间隔时间。 由于 WinRM 工具中的一个错误，使用 “winrm set winrm/config @{MaxTimeoutms ="80000"}” 不会更改超时。因此，建议 WinRM 不被用于需要超过一分钟才能完成执行的命令。 因为用户可以使用这些库配置超时持续时间，建议使用创建 SOAP-XML 数据包的库。 对于使用 Microsoft WinRM 的客户端连接，最低要求为 2.0 版本。有关更多信息，请参阅 <**support.microsoft.com/kb/968929**> 上的 Microsoft 文章。

注: CMC 默认用户名是 root，默认密码是 calvin。

使用其他系统管理工具启动 CMC

您还可以从 Dell Server Administrator 或 Dell OpenManage IT Assistant 启动 CMC。

要使用 Dell Server Administrator 访问 CMC 界面，请启动管理站上的 Server Administrator。从 Server Administrator 主页左窗格的系统树上，单击**系统** > **主系统机箱** > **Remote Access Controller**。有关更多信息，请参阅 *Dell Server Administrator User's Guide*（Dell Server Administrator 用户指南）。

下载和更新 CMC 固件

要下载 CMC 固件，请参阅下载 CMC 固件。

要更新 CMC 固件，请参阅更新 CMC 固件。

设置机箱物理位置和机箱名称

您可在数据中心设置机箱位置和机箱名称，以识别网络上的机箱（默认名称为 **Dell Rack System**）。例如，对机箱名称的 SNMP 查询将返回您所配置的名称。

使用 Web 界面设置机箱物理位置和机箱名称

要使用 CMC Web 界面设置机箱物理位置和机箱名称，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**设置** > **常规**。
此时将显示**常规机箱设置**页。
2 键入位置属性和机箱名称。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注：“机箱位置”字段是可选字段。建议使用数据中心、通道、机架和机架插槽字段来表示机箱的物理位置。

3 单击**应用**。将保存设置。

使用 RACADM 设置机箱物理位置和机箱名称

要使用命令行界面设置机箱名称、位置、日期和时间，请使用 **setsysinfo** 和 **setchassisname** 命令。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

设置 CMC 的日期和时间

可手动设置日期和时间，也可将日期和时间与网络时间协议 (NTP) 服务器同步。

使用 CMC Web 界面设置 CMC 的日期和时间

要使用 CMC Web 界面设置 CMC 的日期和时间，请执行以下操作：

1 在系统树中，转至“机箱概览”，然后单击**设置** > **日期/时间**。
此时将显示**日期/时间**页。
2 要将日期和时间与网络时间协议 (NTP) 服务器同步，请选择**启用 NTP** 并最多指定三个 NTP 服务器。
3 要手动设置日期和时间，请清除**启用 NTP** 并编辑**日期**和**时间**字段，从下拉菜单选择**时区**，然后单击**应用**。

使用 RACADM 设置 CMC 的日期和时间

要使用命令行界面设置日期和时间，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 config 命令和 `cfgRemoteHosts` 数据库属性组部分。

配置 LED 以识别机箱上的组件

可以为全部或单个组件（机箱、服务器和 IOM）设置组件 LED 闪烁作为识别机箱上组件的一种方法。

注: **要修改这些设置，必须具备机箱配置管理员权限。**

使用 CMC Web 界面配置 LED 闪烁

要使用 CMC Web 界面为一个、多个或所有组件 LED 启用闪烁，请执行以下操作：

1 转至以下任一页：
- **机箱概述** > **故障排除** > **标识**。
- **机箱概述** > **机箱控制器** > **故障排除** > **标识**。
- **机箱概述** > **服务器概述** > **故障排除** > **标识**。

  注: **只能在此页上选择服务器。**
- **机箱概述** > **I/O 模块概述** > **故障排除** > **标识**。

  此时将显示**标识**页。

2 要为组件 LED 启用闪烁，请选择所需的组件并单击**闪烁**。

3 要为组件 LED 禁用闪烁，请清除所需的组件并单击**取消闪烁**。

使用 RACADM 配置 LED 闪烁

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm setled -m <module> [-l <ledState>]
```

其中 *<module>* 指定想要配置 LED 的模块。配置选项有：

- `server-nx`，其中 *n* = 1-8 并且 *x* = a、b、c 或 d
- `switch-n`，其中 *n*=1-6
- `cmc-active`

和 *<ledState>* 指定 LED 是否应该闪烁。配置选项有：

- 0 - 不闪烁（默认）
- 1 - 闪烁

配置 CMC 属性

可以使用 Web 界面或 RACADM 配置 CMC 属性，如电源预算、网络设置、用户，以及 SNMP 和电子邮件警报。

使用 CMC Web 界面配置 iDRAC 启动方法

要在**常规机箱设置**页面上配置 iDRAC 启动方法，请执行以下操作：

1 在系统树中，单击**机箱概览** > **设置**。

系统将显示**常规机箱设置**页面。

2 在 **iDRAC 启动方法**属性的下拉菜单中，选择 **IP 地址**或 **DNS**。

3 单击**应用**。

注: 仅在以下情况下需要使用基于 DNS 的方法来启动任何特定 iDRAC：

- 机箱设置为 DNS。
- CMC 检测到特定 iDRAC 是使用 DNS 名称配置的。

使用 RACADM 配置 iDRAC 启动方法

要使用 RACADM 更新 CMC 固件，请使用 `cfgRacTuneIdracDNSLaunchEnable` 子命令。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

使用 CMC Web 界面配置登录闭锁策略属性

注: 要执行以下步骤，必须具备机箱配置管理员权限。

安全登录功能允许您使用 CMC Web 界面配置 CMC 登录的 IP 范围属性。要使用 CMC Web 界面配置 IP 范围属性，请执行以下操作：

1 在系统树中，转至**机箱概览**并单击**网络 > 网络**。
将显示**网络配置**页面。

2 在“IPv4 设置”部分，单击**高级设置**。此外，要访问**安全登录**页面，请在系统树中，转至**机箱概览**，然后单击**安全 > 登录**。
将显示**安全登录**页面。

3 要启用拦截用户或拦截 IP 功能，请在**登录锁定策略**部分，选中**按用户名锁定**或**按 IP 地址 (IPV4) 锁定**。
设置其他登录闭锁策略属性的选项将激活。

4 在激活的字段 - **锁定失败次数**、**锁定失败窗口**和**锁定惩罚时间**中输入登录锁定策略属性必填值。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

5 要保存这些设置，请单击**应用**。

使用 RACADM 配置登录锁定策略属性

您可以针对以下功能使用 RACADM 配置登录锁定策略属性：

- 用户阻止
- IP 地址阻止
- 允许的登录尝试次数
- 锁定失败次数超限后的间隔时间
- 锁定惩罚时间

- 要启用用户阻止功能，请使用：
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneUserBlkEnable <0|1>
  ```
- 要启用 IP 阻止功能，请使用：
  ```
  racadm config –g cfgRacTuning –o cfgRacTuneIPBlkEnable <0|1>
  ```
- 要指定登录尝试次数，请使用：
  ```
  racadm config –g cfgRacTuning –o cfgRacTuneIpBlkFailCount
  ```
- 要指定锁定失败次数超限后的间隔时间，请使用：
  ```
  racadm config –g cfgRacTuning –o cfgRacTuneIpBlkFailWindow
  ```

- 要指定锁定惩罚时间的值，请使用：

```
racadm config –g cfgRacTuning –o cfgRacTuneIpBlkPenaltyTime
```

有关这些对象的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

了解冗余 CMC 环境

如果活动 CMC 失败，可以安装待机 CMC 接替。冗余 CMC 可预先安装或随后安装。CMC 网络电缆连接正确对确保完全冗余或最佳性能至关重要。

故障转移发生在以下时候：

- 运行 RACADM **cmcchangeover** 命令（请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（Chassis Management Controller for Dell PowerEdge M1000e RACADM 命令行参考指南）中的 **cmcchangeover** 命令部分）。
- 在活动 CMC 上运行 RACADM racreset 命令。请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（Chassis Management Controller for Dell PowerEdge M1000e RACADM 命令行参考指南）中的 **racreset** 命令部分。
- 从 Web 界面重设活动 CMC。（请参阅**电源控制操作**的**重设 CMC** 选项，如执行电源控制操作中所述。）
- 从活动 CMC 上卸下网络电缆。
- 从机箱中卸下活动 CMC。
- 在活动 CMC 上初始化 CMC 固件闪存。
- 有不再工作的活动 CMC。

注: 当 CMC 故障转移时，所有 iDRAC 连接和所有活动 CMC 会话都将丢失。丢失会话的用户必须重新连接到新的活动 CMC。

相关链接

关于待机 CMC
CMC 故障保护模式
活动 CMC 自举过程
获得冗余 CMC 的运行状况

关于待机 CMC

待机 CMC 等同于活动 CMC 的镜像，并作为镜像进行维护。活动和待机 CMC 都必须安装相同的固件版本。如果固件版本不同，系统将报告为冗余已降级。

待机 CMC 采用与活动 CMC 相同的设置和属性。必须在两个 CMC 上维护相同的固件版本，但不需要在待机 CMC 上复制配置设置。

注: 有关安装待机 CMC 的信息，请参阅 *Hardware Owner's Manual*（硬件用户手册）。有关在待机 CMC 上安装 CMC 固件的说明，请遵照更新固件中的说明操作。

CMC 故障保护模式

M1000e 机柜可启用故障保护模式，以防止刀片服务器和 I/O 模块出现故障。当没有 CMC 控制机箱时，便会启用故障保护模式。在 CMC 故障转移期间或单 CMC 管理中断时：

- 您无法打开新安装的刀片服务器。
- 您无法远程访问现有刀片服务器。
- 机箱冷却风扇满负荷运行，以实现组件的温度保护。

- 刀片服务器性能降低以限制功耗，直到 CMC 的管理恢复。

以下是可能导致 CMC 管理丢失的一些情况：

- CMC 移除 - 机箱管理会在更换 CMC 或故障转移至待机 CMC 之后恢复。
- 拔下 CMC 网络电缆或网络连接中断 - 机箱管理在机箱故障转移到待机 CMC 后恢复。网络故障转移只有在冗余 CMC 模式下才能启用。
- CMC 重设 - 机箱管理会在 CMC 重新引导或机箱故障转移至待机 CMC 之后恢复。
- CMC 故障转移命令已发出 - 机箱管理会在机箱故障转移至待机 CMC 之后恢复。
- CMC 固件更新 - 机箱管理会在 CMC 重新引导或机箱故障转移至待机 CMC 之后恢复。建议您首先更新待机 CMC，以便仅发生一次故障转移事件。
- CMC 错误检测和纠正 - 机箱管理会在 CMC 重设或机箱故障转移至待机 CMC 之后恢复。

注: 您可以将机柜配置为使用一个 CMC 或冗余 CMC。在冗余 CMC 配置中，如果主要 CMC 与机柜或管理网络失去通信，则待机 CMC 会接管机箱管理。

活动 CMC 自举过程

两个 CMC 插槽之间没有任何区别，即插槽并不表明优先级。而首先安装或引导的 CMC 将担任活动 CMC 的角色。如果打开交流电源时已安装了两个 CMC，则安装在 CMC 机箱插槽 1（左侧）的 CMC 通常担任活动角色。活动 CMC 由蓝色 LED 表示。

如果将两个 CMC 插入已经打开电源的机箱，将需要最多两分钟来进行自动的活动/待机协商。协商完后，将恢复正常的机箱运行。

获得冗余 CMC 的运行状况

可以在 Web 界面中查看待机 CMC 的运行状况。有关在 Web 界面中访问 CMC 运行状况的更多信息，请参阅查看机箱信息和监测机箱与组件运行状况。

3

登录 CMC

您可以使用 CMC 本地用户、Microsoft Active Directory 用户或 LDAP 用户身份登录 CMC。默认用户名和密码分别是 root 和 calvin。您还可以使用单点登录或智能卡进行登录。

主题：

相关链接

访问 CMC Web 界面
以本地用户、Active Directory 用户或 LDAP 用户身份登录 CMC
使用智能卡登录 CMC
使用单点登录来登录 CMC
使用串行、Telnet 或 SSH 控制台登录 CMC
使用 RACADM 访问 CMC
使用公共密钥验证登录 CMC

访问 CMC Web 界面

在使用 Web 界面登录 CMC 之前，请确保已配置支持的 Web 浏览器（Internet Explorer 或 Firefox），并且已创建具有所需权限的用户帐户。

注: 如果使用 Microsoft Internet Explorer，请通过代理连接，如果看到“无法显示 XML 页”错误，则需要禁用代理才能继续。

要访问 CMC Web 界面，请执行以下操作：

1 打开支持的 Web 浏览器窗口。
有关支持的 Web 浏览器的最新信息，请参阅 *Readme*（自述文件），网址：**dell.com/support/manuals**。

2 在**地址**字段中键入下面的 URL 并按 Enter：
- 要访问使用 IPv4 地址的 CMC，请输入：`https://<CMC IP address>`
  如果默认的 HTTPS 端口号（端口 443）已更改，请键入：`https://<CMC IP address>:<port number>`
- 要访问使用 IPv6 地址的 CMC，请输入：`https://[<CMC IP address>]`
  如果默认的 HTTPS 端口号（端口 443）已更改，请键入：`https://[<CMC IP address>]:<port number>`

注: 使用 IPv6 时，必须用方括号 ([ ]) 将 *<CMC IP address>* 括起来。

其中 *<CMC IP address>* 是 CMC 的 IP 地址，而 *<port number>* 是 HTTPS 端口号。

随即显示 CMC 的 **Login**（登录）页面。

相关链接

配置 Web 浏览器
以本地用户、Active Directory 用户或 LDAP 用户身份登录 CMC
使用智能卡登录 CMC
使用单点登录来登录 CMC

以本地用户、Active Directory 用户或 LDAP 用户身份登录 CMC

要登录 CMC，您必须具有**登录 CMC** 权限的 CMC 帐户。默认 CMC 用户名是 root，密码是 calvin。根帐户是随 CMC 一起提供的默认管理帐户。

注:

- 为增加安全性，强烈建议您在首次设置时更改根帐户的默认密码。
- 如果启用了证书验证，应提供系统的完全限定域名 (FQDN)。如果启用了证书验证并且为域控制器提供了 IP 地址，登录将失败。

CMC 不支持扩展的 ASCII 字符（如 ß、å、é、ü）或主要在非英语语言中使用的其他字符。

不能在单个工作站上的多个浏览器窗口中使用不同的用户名登录到 Web 界面。

注: CMC 的多域配置：

- 林中所有子域均须扩展该架构。
- 应将用户添加至每个域，并在每个域中创建 CMC 设备。
- 在配置 CMC 的扩展架构时，必须提及所配置的域。例如，如果根域为 **fwad2.lab**，用户为 **cmcuser5@NodeA.GrandChildA.SubChildA.ChildA.fwad2.lab**，则用于配置该用户的域为 **NodeA.GrandChildA.SubChildA.ChildA.fwad2.lab**。用户 **cmcuser5@NodeA.GrandChildA.SubChildA.ChildA.fwad2.lab** 可从 CMC 进行验证。

要以本地用户、Active Directory 用户或 LDAP 用户身份登录，请执行以下操作。

1 在**用户名**字段中，键入您的用户名：
   - CMC 用户名：<user name>
   - Active Directory 用户名：<domain>\<user name>、<domain>/<user name> 或 <user>@<domain>。
   - LDAP 用户名：<user name>

   注: 对于 Active Directory 用户，用户名区分大小写。
2 在**密码**字段中，键入用户密码。

   注: 此字段区分大小写。
3 在**域**字段中，从下拉菜单中选择所需的域。
4 另外，可选择会话超时。这是您在被自动注销前可保持登录状态但不进行任何操作的时间。默认值为 Web 服务会话空闲超时。
5 单击**确定**。
   您便以所需的用户权限登录 CMC。

注: 如果 LDAP 验证已启用并且您尝试使用本地凭据登录 CMC，凭证首先在 LDAP 服务器中检查，然后在 CMC 中检查。

注: 对于带有 OPEN-DS 的 LDAP 验证，DH 密钥必须大于 768 位。

相关链接

配置用户帐户和权限
访问 CMC Web 界面

使用智能卡登录 CMC

您可以使用智能卡登录 CMC。智能卡提供双重验证 (TFA)，该功能可实现双层安全性：

- 物理智能卡设备。
- 加密代码（例如密码或 PIN）。

用户必须使用智能卡和 PIN 验证其凭据。

注: 您不能使用 IP 地址通过智能卡登录来登录 CMC。Kerberos 基于完全限定域名 (FQDN) 验证您的凭据。

当您使用智能卡作为 Active Directory 用户登录之前，请确保：

- 将可信证书颁发机构 (CA) 证书（CA 签发的 Active Directory 证书）上载到 CMC。
- 配置 DNS 服务器。
- 启用 Active Directory 登录。
- 启用智能卡登录。

要使用智能卡作为 Active Directory 用户登录 CMC：

1 使用链接 `https://<cmcname.domain-name>` 登录 CMC。
此时将显示 **CMC 登录**页，提示插入智能卡。

注: 如果您更改了默认 HTTPS 端口号（端口 80），则使用 `<cmcname.domain-name>:<port number>` 访问 CMC Web 页，其中 cmcname 是 CMC 的 CMC 主机名，domain-name 是域名，port number 是 HTTPS 端口号。

2 插入智能卡并单击**登录**。
此时将显示 PIN 弹出窗口。

3 输入 PIN，并单击**提交**。

注: 如果 Active Directory 中存在该智能卡用户，则不需要输入 Active Directory 密码。

您已使用 Active Directory 凭据登录到 CMC。

相关链接

为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

使用单点登录来登录 CMC

启用单点登录 (SSO) 后，您可以登录 CMC 而无需输入您的域用户验证凭据（例如用户名和密码）。

注: 您不能使用 IP 地址登录单点登录。Kerberos 会根据 FQDN 验证您的凭据。

使用单点登录功能登录 CMC 之前，请确保：

- 您已使用有效的 Active Directory 用户帐户登录到系统。
- 单点登录选项在 Active Directory 配置过程中已启用。

使用单点登录登录到 CMC：

1 使用网络帐户登录客户端系统。

2 使用 `https://<cmcname.domain-name>` 登录 CMC Web 界面
例如，cmc-6G2WXF1.cmcad.lab，其中 cmc-6G2WXF1 是 cmc-name，cmcad.lab 是 domain-name。

注: 如果您更改了默认 HTTPS 端口号（端口 80），则使用 <cmcname.domain-name>:<port number> 访问 CMC Web 界面，其中 cmcname 是 CMC 的 CMC 主机名，domain-name 是域名，port number 是 HTTPS 端口号。

CMC 会使用在您使用有效 Active Directory 帐户登录时浏览器高速缓存的 Kerberos 凭据来使您登录。如果登录失败，浏览器将重定向至正常的 CMC 登录页。

注: 如果您没有登录到 Active Directory 域，而且使用的是除 Internet Explorer 以外的浏览器，则登录将失败，而且浏览器仅显示空白页。

相关链接

为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

使用串行、Telnet 或 SSH 控制台登录 CMC

您可以通过串行、Telnet 或 SSH 连接、或者通过 iKVM 上的 Dell CMC 控制台登录 CMC。

当您配置完管理站终端仿真软件和受管节点 BIOS 后，执行下列任务以登录到 CMC：

1 使用管理站终端仿真软件连接到 CMC。

2 键入 CMC 用户名和密码，然后按 <Enter>。

您即登录到 CMC。

还请参阅以下主题：

- 将 Telnet 控制台与 CMC 配合使用
- 将 SSH 与 CMC 配合使用
- 必需的 Minicom 设置

相关链接

配置 CMC 以使用命令行控制台

从 Dell CMC 控制台启用对 iKVM 的访问

使用 RACADM 访问 CMC

RACADM 提供一组可以通过基于文本的界面配置和管理 CMC 的命令。RACADM 可以通过 Telnet/SSH 或串行连接访问、通过 iKVM 上的 Dell CMC 控制台访问，或者使用安装在管理站上的 RACADM 命令行界面远程访问。

RACADM 接口的分类如下：

- 远程 RACADM - 允许使用 -r 选项和 CMC 的 DNS 名称或 IP 地址在管理站上运行 RACADM 命令。
- 固件 RACADM - 允许使用 Telnet、SSH、串行连接或 iKVM 登录到 CMC。使用固件 RACADM 后，可运行作为 CMC 固件一部分的 RACADM 实现。

注: 远程 RACADM 包含在 Dell Systems Management Tools and Documentation DVD 中，并已安装在管理站上。

您可以在脚本中使用远程 RACADM 命令来配置多个 CMC。CMC 不支持脚本，所以不能直接在 CMC 上运行脚本。

有关 RACADM 的更多信息，请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（Chassis Management Controller for Dell PowerEdge M1000e RACADM 命令行参考指南）。

有关配置多个 CMC 的更多信息，请参阅使用 RACADM 配置多个 CMC。

使用公共密钥验证登录 CMC

您可以通过 SSH 登录 CMC，不输入密码。您还可以将单一的 RACADM 命令作为命令行参数发送到 SSH 应用程序。由于该会话在命令完成时结束，因此命令行选项的行为与远程 RACADM 类似。

在通过 SSH 登录 CMC 前，确保已上载公共密钥。

例如：

- **登录**：`ssh service@<domain>` 或 `ssh service@<IP_address>`，其中 IP_address 是 CMC IP 地址。
- **发送 RACADM 命令**：`ssh service@<domain> racadm getversion` 和 `ssh service@<domain> racadm getsel`

使用服务帐户登录时，如果在创建公共/私人密钥对时设置了密码短语，可能会提示您再次输入该密码短语。如果密码短语与密钥结合使用，Windows 和 Linux 客户端都提供相应方法来使之自动实现。在 Windows 客户端上，您可以使用 Pageant 应用程序。该应用程序在后台运行，使密码短语的输入变得透明。在 Linux 客户端上，您可以使用 sshagent。有关如何设置和使用上述任一应用程序，请参阅该应用程序提供的说明文件。

相关链接

配置通过 SSH 的公共密钥验证

多个 CMC 会话

下表提供了可能使用各种界面的多个 CMC 会话的列表。

表. 9: 多个 CMC 会话

界面	每个界面的最大会话数
CMC Web 界面	4
RACADM	4
Telnet	4
SSH	4
WS-MAN	4
iKVM	1
串行	1

更改默认登录密码

在以下情况下，系统会发送警告消息提示您更改默认密码：

- 您以**配置用户**权限登录到 CMC。
- 默认密码警告功能已启用。
- 当前启用的任何帐户的默认用户名和密码都分别是 `root` 和 `calvin`。

如果使用 Active Directory 或 LDAP 登录，会显示同一条警告消息。在确定是否有任何（本地）帐户将 `root` 和 `calvin` 作为凭据时，不考虑 Active Directory 和 LDAP 帐户。在使用 SSH、Telnet、远程 RACADM 或 Web 界面登录 CMC 时，也会显示警告消息。对于 Web 界面、SSH 和 Telnet，会为每个会话显示一条警告消息。对于远程 RACADM，会为每个命令显示警告消息。

要更改凭据，您必须拥有**配置用户**权限。

注: 如果在 CMC 登录页面上选中不再显示该警告选项，则会生成 CMC 日志消息。

使用 Web 界面更改默认登录密码

当您登录 CMC Web 界面时，如果显示**默认密码警告**页面，您可以更改密码。要更改密码，请执行以下操作：

1 选择 **Change Default Password**（更改默认密码）选项。

2 在**新密码**字段中，输入新密码。

密码的最大字符数为 20。字符进行屏蔽处理。支持使用以下字符：

- 0-9
- A-Z
- a-z
- 特殊字符：+、&、?、>、-、}、|、.、!、(、'、,、_、[、"、@、#、)、*、;、$、]、/、§、%、=、<、:、{、|、\

3 在**确认密码**字段中，再次输入密码。

4 单击**继续**。新密码即配置好并且您随后登录到 CMC。

注: 只有在新密码和确认密码字段匹配的情况下才会继续。

有关其他字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

使用 RACADM 更改默认登录密码

要更改密码，请运行以下 RACADM 命令：

```
racadm config –g cfgUserAdmin –o cfgUserAdminPassword –i <index> <newpassword>
```

其中，`<index>` 是从 1 至 16 的值（代表用户帐户），`<newpassword>` 是新的用户定义的密码。

有关更多信息，请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

启用或禁用默认密码警告消息

您可以启用或禁用默认密码警告消息的显示。要实现这一点，您必须拥有 Configure Users（配置用户）权限。

使用 Web 界面启用或禁用默认密码警告消息

要在登录 iDRAC 后启用或禁用默认密码警告消息的显示，请执行以下操作：

1 转至**机箱控制器** > **用户验证** > **本地用户**。

此时将显示**用户**页面。

2 在**默认密码警告**部分，选择**启用**，然后单击**应用**以在登录到 CMC 时启用显示**默认密码警告**页面。否则，请选择**禁用**。

或者，如果此功能已启用并且您不希望为后续登录操作显示警告消息，请在**默认密码警告**页面上，选择**不再显示此警告**选项，然后单击**应用**。

使用 RACADM 启用或禁用警告消息以更改默认登录密码

要使用 RACADM 启用显示警告消息以更改默认登录密码，请使用 `racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>` 对象。有关更多信息，请参阅 **dell.com/support/manuals** 上的

Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

4

更新固件

您可以为以下各项更新固件：

- CMC - 活动和待机
- iKVM
- IOM

您可以更新以下服务器组件的固件：

- iDRAC - 必须使用恢复界面更新早于 iDRAC6 的 iDRAC。iDRAC6 固件也可使用恢复界面更新，但是不宜用于 iDRAC6 和未来版本。
- BIOS
- Unified Server Configurator
- 32 位诊断程序
- 操作系统驱动程序包
- 网络接口控制器
- RAID 控制器

主题：

相关链接

下载 CMC 固件
查看当前安装的固件版本
更新 CMC 固件
更新 iKVM 固件
更新服务器组件固件
使用 CMC 恢复 iDRAC 固件
更新 IOM 基础结构设备固件

下载 CMC 固件

在开始固件更新之前，请从 **support.dell.com** 下载最新的固件版本，然后将其保存到本地系统。

CMC 固件包中包含以下软件组件：

- 编译的 CMC 固件代码和数据
- Web 界面、JPEG 和其他用户界面数据文件
- 默认配置文件

或者，您也可以使用 Dell Repository Manager (DRM) 查看是否有可用的最新固件更新。Dell Repository Manager (DRM) 可确保 Dell 系统具有最新 BIOS、驱动程序、固件和软件。您可根据品牌和型号或服务标签，从支持站点 (**support.dell.com**) 为支持的平台搜索可用的最新更新。您可以下载更新，或根据搜索结果构建一个存储库。有关使用 DRM 搜索最新固件更新的更多信息，请参阅 Dell Tech Center 中的“在 Dell 支持站点上使用 Dell Repository Manager 搜索最新更新”。有关保存 DRM 用作输入以创建存储库的资源清册文件的更多信息，请参阅使用 CMC Web 界面保存机箱资源清册报告。建议按以下顺序更新 M1000e 机箱固件：

- 刀片服务器组件固件
- CMC 固件

有关 M1000e 机箱的更新顺序的更多信息，请参阅支持站点上的 *CMC Firmware 5.0 Release Notes*（CMC 固件 5.0 版发行说明）。

签名的 CMC 固件映像

M1000e CMC 5.0 版和更高版本的固件包含签名。CMC 固件将执行签名验证步骤，以确保已上载固件的真实性。只有固件映像经 CMC 验证为服务提供商的有效映像且未被更改过，固件更新过程才会成功。如果 CMC 无法验证已上载固件映像的签名，固件更新过程将停止。然后将记录一条警告事件，并显示相应的错误消息。

签名验证可在固件版本 3.1 及更高版本上执行。对于降级到 3.1 版之前的 M1000e CMC 版本的固件，应先将固件升级到大于或等于 3.1 且小于 5.0 版的 M1000e CMC 版本。进行此更新后，降级到较早的未签名的 M1000e CMC 版本的固件也可执行签名验证。CMC 5.0 版和更高版本发行的映像中附有签名，此外还附有 3.10、3.20、3.21、4.0、4.10、4.11、4.30、4.31、4.45 和 4.5 版的签名文件。因此，CMC 固件更新仅支持这些固件版本。对于除此以外的任何版本，应先更新到其中的任何一个版本，然后再更新至所需版本。

查看当前安装的固件版本

可以使用 CMC Web 界面或 RACADM 查看当前安装的固件版本。

使用 CMC Web 界面查看当前安装的固件版本

在 CMC Web 界面，转至以下任一页查看当前固件版本：

- **机箱概述** > **更新**
- **机箱概述** > **机箱控制器** > **更新**
- **机箱概述** > **服务器概述** > **更新**
- **机箱概述** > **I/O 模块概述** > **更新**
- **机箱概述** > **iKVM** > **更新**

固件更新页显示列出的每个组件的当前固件版本，并允许将固件更新到最新版本。

如果机箱中包含 iDRAC 处于恢复模式的早期服务器，或者 CMC 检测到 iDRAC 中有损坏的固件，则早期的 iDRAC 也将列在“固件更新”页中。

使用 RACADM 查看当前安装的固件版本

要使用 RACADM 查看当前安装的固件版本，请使用 **getkvminfo** 子命令。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

更新 CMC 固件

您可以使用 Web 界面或 RACADM 来更新 CMC 固件。默认情况下，固件更新会保留当前的 CMC 设置。在更新过程中，您可以将 CMC 配置设置重设为出厂默认设置。

注: 要更新 CMC 的固件，必须具备机箱配置管理员权限。

如果使用 Web 用户界面会话更新系统组件固件，则空闲超时设置必须设置为足够大的值，以便适应文件传输时间。有时，固件文件传输时间可能长达 30 分钟。要设置空闲超时值，请参阅配置服务。

在 CMC 固件更新期间，机箱中部分或所有风扇装置通常以 100% 速率旋转。

如果机箱中安装了冗余 CMC，建议通过一个操作同时将两个 CMC 更新到相同的固件版本。如果这两个 CMC 的固件版本不同并发生故障转移，可能会出现意外结果。

注: CMC 固件更新或回滚仅支持固件版本 3.10、3.20、3.21、4.0、4.10、4.11、4.30、4.31、4.45、4.5、5.0 和更高版本。对于这些版本之外的任何版本，首先更新至上述任一版本，然后更新至所需版本。

成功上传固件后，活动 CMC 将重设并且暂时不可用。如果存在备用 CMC，则备用和活动角色会交换。备用 CMC 会成为活动 CMC。如果仅对活动 CMC 应用更新，则重设完成后，活动 CMC 将不运行更新的映像，只有备用 CMC 运行该映像。一般来说，强烈建议活动和备用 CMC 保持相同的固件版本。

当备用 CMC 更新完毕后，交换 CMC 的角色，以使刚更新的 CMC 成为活动 CMC，而使用较早固件的 CMC 则成为备用 CMC。有关交换角色的信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）*中的 `cmcchangeover` 命令部分。在第二个 CMC 中更新固件之前，运行此命令可帮助您验证更新是否成功以及新固件是否正常工作。当两个 CMC 都更新后，您可以使用 `cmcchangeover` 命令将 CMC 恢复到以前的角色。CMC 固件版本 2.x 会更新主 CMC 和冗余 CMC，而无需运行 `cmcchangeover` 命令。

为避免在重设期间断开任何用户的连接，请通知所有可以登录 CMC 的已授权用户并在会话页面上检查是否存在活动会话。要打开**会话**页面，请选择树中的**机箱**，单击**网络**选项卡，然后单击**会话**子选项卡。

在 CMC 中更新固件过程的最后阶段，浏览器会话以及与 CMC 的连接将暂时丢失，因为 CMC 未连接至网络。CMC 将报告机箱整体运行状况为“严重”，因为临时网络已丢失。在几分钟后 CMC 重新启动时，登录到 CMC。然后，CMC 会报告机箱整体运行状况为“运行正常”以及 CMC 网络链路已接通。重设 CMC 后，新的固件版本显示在**固件更新**页上。

当从 CMC 传输文件或向 CMC 传输文件时，文件传输图标将在传输期间旋转。如果该图标不显示动画，请确保将浏览器配置为允许动画。有关说明，请参阅允许在 Internet Explorer 中播放动画。

如果在使用 Internet Explorer 从 CMC 下载文件时遇到问题，请启用请勿将加密页面保存到磁盘选项。有关说明，请参阅使用 Internet Explorer 从 CMC 下载文件。

注: 如果您在当前版本的 CMC 中已将插槽名称长度配置为超过 15 个字符，降级 CMC 固件将截断插槽名称长度为 15 个字符。

相关链接

下载 CMC 固件

查看当前安装的固件版本

使用 Web 界面更新 CMC 固件

要使用 CMC Web 界面更新 CMC 固件，请执行以下操作：

1 转至以下任一页：
- **机箱概览 > 更新**
- **机箱概览 > 机箱控制器 > 更新**
- **机箱概览 > I/O 模块概览 > 更新**
- **机箱概览 > iKVM > 更新**

此时将显示**固件更新**页面。

2 在 **CMC 固件**部分，选中**更新目标**列中要更新固件的一个或多个 CMC（如果存在待机 CMC）选择所需的组件，然后单击**应用 CMC 更新**。

3 在**固件映像**字段中，输入管理站或共享网络上固件映像文件的路径，或单击**浏览**导航到文件位置。默认 CMC 固件映像名称为 `firmimg.cmc`。

4 单击**开始固件更新**，然后单击**是**继续。在**固件更新过程**部分提供固件更新状态信息。当上载映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新进程开始时，将自动刷新页面并显示固件更新计时器。

注: 在直流 PSU 支持的机箱中，如果您尝试更新直流 PSU 不支持的固件版本，则会显示错误消息。

5 附加说明：
- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- 要取消该过程，请单击**取消文件传输和更新**。该选项仅在文件传输过程中可用。
- **更新状态**字段显示固件更新状态。

注: CMC 的更新可能需要几分钟时间。

6 对于待机 CMC，当完成更新时，**更新状态**字段将显示**完成**。对于活动 CMC，在固件更新过程的最后阶段，浏览器会话和与 CMC 的连接将在活动 CMC 断开网络连接时暂时丢失。您必须在几分钟后等活动 CMC 重新启动后再次登录。重设 CMC 后，新固件将显示在**固件更新**页上。

注: 固件更新后，清除 Web 浏览器高速缓存。有关如何清除浏览器高速缓存的说明，请参阅 Web 浏览器的联机帮助。

使用 RACADM 更新 CMC 固件

要使用 RACADM 更新 CMC 固件，请使用 `fwupdate` 子命令。有关 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

注: 运行固件更新命令的方式是一次只打开一个远程 RACADM 会话。

更新 iKVM 固件

成功上载固件后，iKVM 将重设并且暂时不可用。

相关链接

下载 CMC 固件

查看当前安装的固件版本

使用 CMC Web 界面更新 iKVM 固件

要使用 CMC Web 界面更新 iKVM 固件，请执行以下操作：

1 转至以下任一页：
- **机箱概览** > **更新**
- **机箱概览** > **机箱控制器** > **更新**
- **机箱概览** > **iKVM** > **更新**

此时将显示 **Firmware Update**（固件更新）页面。

2 在 **iKVM 固件**部分，选中**更新目标**列中要更新固件的 **iKVM** 对应的复选框，然后单击**应用 iKVM 更新**。

3 在**固件映像**字段中，输入管理站或共享网络上固件映像文件的路径，或单击**浏览**导航到文件位置。默认 iKVM 固件映像名称为 iKVM.bin。

4 单击**开始固件更新**，然后单击**是**继续。

在**固件更新过程**部分提供固件更新状态信息。当上载映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新进程开始时，将自动刷新页面并显示固件更新计时器。

5 要遵循的其他说明：
- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- 要取消该过程，请单击**取消文件传输和更新**。该选项仅在文件传输过程中可用。
- **更新状态**字段显示固件更新状态。

注: iKVM 更新过程最多需要两分钟。

更新完成后，iKVM 将重设且新固件将显示在**固件更新**页上。

使用 RACADM 更新 iKVM 固件

要使用 RACADM 更新 iKVM 固件，请使用 `fwupdate` 子命令。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

更新 IOM 基础结构设备固件

通过执行此更新，会更新 IOM 设备组件的固件，但不会更新 IOM 设备自身的固件；组件是 IOM 设备和 CMC 之间的接口电路。组件的更新映像驻留在 CMC 文件系统中，如果组件和 CMC 上组件映像的当前版本不匹配，组件仅显示为 CMC Web 界面上的可更新设备。

在更新 IOM 基础结构设备固件之前，确保 CMC 固件获得更新。

注:

如果 CMC 检测到 IOMINF 固件对于 CMC 文件系统中包含的映像已经过时，则 CMC 允许更新 IOM 基础结构设备固件 (IOMINF)。如果 IOMINF 固件是最新的，CMC 会阻止 IOMINF 更新。最新的 IOMINF 设备未列为可更新设备。

相关链接

下载 CMC 固件

查看当前安装的固件版本

使用 CMC Web 界面更新 IOM 软件

使用 CMC Web 界面更新 IOM 协处理器

要在 CMC Web 界面中更新 IOM 基础结构设备固件，请执行以下操作：

1 转至**机箱概览** > **I/O 模块概览** > **更新**。

随即将显示 **IOM 固件更新**页面。

或者，请转至以下任一页：

- **机箱概览** > **更新** > **IOM 协处理器**
- **机箱概览** > **CMC 固件** > **应用 CMC 更新** > **IOM 协处理器**
- **机箱概览** > **iKVM 固件** > **应用 iKVM 更新** > **IOM 协处理器**

随即显示**固件更新**页面，该页面提供了用于访问 **IOM 固件更新**页面的链接。

2 在 **IOM 固件更新**页面的 **IOM 固件**部分，选中**更新**列中要更新固件的 IOM 对应的复选框，并单击**应用固件更新**。

在**更新状态**部分提供固件更新状态信息。当上载映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新进程开始时，将自动刷新页面并显示固件更新计时器。

注：

- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- 当更新 IOMINF 固件时，不会显示文件传输计时器。
- 如果 IOM 协处理器已有最新固件版本，**更新**列将不会显示复选框。

更新完成后，会暂时失去与 IOM 设备的连接，因为该设备会进行重设并在**固件更新**页面显示新固件。

使用 RACADM 更新 IOM 固件

要使用 RACADM 更新 IOM 基础结构设备固件，请使用 fwupdate 子命令。有关 PowerEdge 命令的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

使用 Web 界面更新服务器 iDRAC 固件

要使用 CMC Web 界面更新服务器中的 iDRAC 固件，请执行以下操作：

1 转至以下任一页：

- **机箱概览** > **更新**
- **机箱概览** > **机箱控制器** > **更新**
- **机箱概览** > **I/O 模块概览** > **更新**
- **机箱概览** > **iKVM** > **更新**

此时将显示 **Firmware Update**（固件更新）页面。

您还可以通过**机箱概览** > **服务器概览** > **更新**来更新服务器 iDRAC 固件。有关更多信息，请参阅更新服务器组件固件。

2 要更新 iDRAC 固件，请在 **iDRAC Enterprise 固件**部分，选中**更新目标**列中要更新固件的 iKVM 对应的复选框，单击**应用 iDRAC Enterprise 更新**，然后转至步骤 4。

3 要更新 iDRAC 固件，请在 **iDRAC Enterprise 固件**部分，单击要更新固件的服务器对应的**更新**链接。

此时将显示**服务器组件更新**页。若要继续，请参阅更新服务器组件固件部分。

4 在**固件映像**字段中，输入管理站或共享网络上固件映像文件的路径，或单击**浏览**导航到文件位置。默认 iDRAC 固件映像名称为 firming.imc。

5 单击**开始固件更新**，然后单击**是**继续。

在**固件更新过程**部分提供固件更新状态信息。当上载映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新进程开始时，将自动刷新页面并显示固件更新计时器。

6 要遵循的其他说明：

- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- 要取消该过程，请单击**取消文件传输和更新**。该选项仅在文件传输过程中可用。
- **更新状态**字段显示固件更新状态。

注: 更新 iDRAC 固件最多需要十分钟。

更新完成后，iKVM 将重设且新固件将显示在**固件更新**页上。

使用 RACADM 更新服务器 iDRAC 固件

要使用 RACADM 更新 iDRAC 固件，请使用 fwupdate 子命令。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide for iDRAC and CMC*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

更新服务器组件固件

CMC 中的一对多更新功能可让您跨多个服务器更新服务器组件固件。您可使用本地系统或网络共享上可用的 Dell Update Package 来更新服务器组件。可利用服务器上的 Lifecycle Controller 功能来启用该操作。

注: 要更新组件固件，必须为服务器启用 CSIOR 选项。要启用 CSIOR：

- 第 11 代服务器 - 在重新启动服务器后，从 CTRL-E 设置中，选择**系统服务**，启用 **CSIOR** 并保存更改。
- 第 12 代服务器及更新的服务器 - 在重新启动服务器后，从 F2 设置中，选择 **iDRAC 设置** > **Lifecycle Controller**，启用 **CSIOR** 并保存更改。

从文件更新方法使您能够使用本地系统中存储的 DUP 文件更新服务器组件固件。您可以选择单独的服务器组件以使用所需的 DUP 文件更新固件。您可以通过使用 SD 卡存储超过 48 MB 内存大小的 DUP 文件来一次更新大量组件。

注:

- 在选择各个服务器组件进行更新时，确保所选组件之间不存在相关性。否则，如果选择和其他组件有相关性的一些组件进行更新可能导致服务器突然停止工作。
- 确保以建议的顺序更新服务器组件。否则，组件固件更新过程可能失败。有关更新服务器组件固件的更多信息，请参阅在 PowerEdge 服务器上执行更新的建议工作流程。

一键更新所有刀片或**从网络共享更新**方法可让您使用存储在网络共享上的 DUP 文件来更新服务器组件固件。您可使用基于 Dell Repository Manager (DRM) 的更新功能来访问存储在网络共享上的 DUP 文件并以单次操作更新服务器组件。您可使用 Dell Repository Manager 设置固件 DUP 和二进制映像的自定义远程存储库并在网络共享上将其共享。

注: 一键更新所有刀片的方法有以下优势：

- 可让您只需最少的点击数即可更新所有刀片服务器上的所有组件。
- 所有更新内容都打包在一个目录中。这可避免单独上载每个组件的固件。
- 在更新服务器组件时更快、更一致。
- 可让您保留标准映像，其中包含可用于以单次操作更新多个服务器所需的服务器组件更新版本。
- 您可从 Dell Server Update Utility (SUU) 下载 DVD 复制更新目录，或者在 Dell Repository Manager (DRM) 中创建所需的更新版本并进行自定义。您无需最新版本的 Dell Repository Manager 即可创建该目录，但 DRM 1.8 版提供有根据导出的 M1000e 资源清册创建存储库（更新目录）的选项。有关保存机箱资源清册报告的更多信息，请参阅使用 CMC Web 界面保存机箱资源清册报告。有关使用 DRM 创建存储库的信息，请参阅 **dell.com/support/manuals** 上的 *Dell Repository Manager Data Center Version 1.8 User's Guide*（Dell Repository Manager Data Center 1.8 版用户指南）以及 *Dell Repository Manager Business Client Version 1.8 User's Guide*（Dell Repository Manager Business Client 1.8 版用户指南）。

Lifecycle Controller 通过 iDRAC 提供模块更新支持。建议在更新服务器组件固件模块之前先更新 CMC 固件。更新 CMC 固件之后，可以在 CMC Web 界面中的**机箱概览 > 服务器概览 > 更新 > 服务器组件更新**页面上更新服务器组件固件。此外，还建议选中服务器的所有组件模块一起更新。这样可使 Lifecycle Controller 使用其优化算法更新固件，减少重新引导的次数。

注: iDRAC 固件必须是 3.2 版或更高版本才支持此功能。

如果 Lifecycle Controller 服务在服务器上禁用，此时**组件/设备固件资源清册**部分将显示 *Lifecycle Controller 可能未启用*。

相关链接

启用 Lifecycle Controller
筛选进行固件更新的组件
查看固件资源清册
Lifecycle Controller 作业操作
更新 IOM 基础结构设备固件

服务器组件更新顺序

对于单个组件的更新，必须按以下顺序为服务器组件更新固件版本：

- iDRAC
- Lifecycle Controller
- 诊断程序（可选）
- 操作系统驱动程序包（可选）
- BIOS
- NIC
- RAID
- 其他组件

注: 当一次性更新所有服务器组件的固件版本时，由 Lifecycle Controller 处理更新顺序。

服务器组件更新支持的固件版本

以下部分提供了 CMC 固件更新和服务器组件更新支持的组件版本。

下表列出了 CMC 固件从 6.0 版更新到 6.1 版（但服务器组件不更新到下一版本）时服务器组件支持的固件版本。

注: 对于下表中所列的所有服务器，使用 N-1 版本的 iDRAC、BIOS 和 Lifecycle Controller 进行从 6.0 版到 6.1 版的 CMC 固件更新成功。

表. 10: CMC 固件更新支持的服务器组件固件版本（从 6.0 版更新至 6.1 版）

平台	服务器组件	当前组件版本（N-1 版本）
M610	iDRAC	3.50 A00
	Lifecycle Controller	1.6.0.73
	诊断程序	5158A3
	BIOS	6.4.0
	NIC	19.2.0

平台	服务器组件	当前组件版本（N-1 版本）
M610x	iDRAC	3.50 A00
	Lifecycle Controller	1.6.0.73
	诊断程序	5158A3
	BIOS	6.4.0
	NIC	19.2.0
M710	iDRAC	3.50 A00
	Lifecycle Controller	1.6.0.73
	诊断程序	5158A3
	BIOS	6.4.0
	NIC	19.2.0
M910	iDRAC	3.50 A00
	Lifecycle Controller	1.6.0.73
	诊断程序	5158A3
	BIOS	2.10.0
M915	iDRAC	3.50 A00
	Lifecycle Controller	1.6.0.73
	诊断程序	5158A3
	BIOS	3.2.2
M710HD	iDRAC	3.50 A00
	Lifecycle Controller	1.6.0.73
	诊断程序	5158A3
	BIOS	8.0.0
M420	iDRAC	2.52.52.52
	Lifecycle Controller	2.52.52.52
	诊断程序	4231A0
	BIOS	2.4.2
	NIC	19.2.0
M520	iDRAC	2.52.52.52

平台	服务器组件	当前组件版本（N-1 版本）
	Lifecycle Controller	2.52.52.52
	诊断程序	4231A0
	BIOS	2.4.2
	NIC	19.2.0
M620	iDRAC	2.52.52.52
	Lifecycle Controller	2.52.52.52
	诊断程序	4231A0
	BIOS	2.5.4
M820	iDRAC	2.52.52.52
	Lifecycle Controller	2.52.52.52
	诊断程序	4231A0
	BIOS	2.6.1
M630	iDRAC	2.52.52.52
	Lifecycle Controller	2.52.52.52
	诊断程序	4239.44
	BIOS	2.6.0
M830	iDRAC	2.52.52.52
	Lifecycle Controller	2.52.52.52
	诊断程序	4239.44
	BIOS	2.5.4
M640	iDRAC	3.15.15.15
	Lifecycle Controller	3.15.15.15
	诊断程序	4301A13
	BIOS	1.3.7

下表列出了以下场景下服务器组件支持的固件版本：现有 CMC 固件版本为 6.0 并且服务器组件从 N-1 版本更新至 N 版本。

注: 对于下表中所列的所有第 11 代、第 12 代、第 13 代和第 14 代服务器，在 CMC 固件版本为 5.0 或更高版本时，服务器组件固件从 N-1 版本成功更新至 N 版本。

表. 11: 服务器组件更新至 N 版本时支持的服务器组件版本

平台	服务器组件	上一组件版本（N-1 版本）	更新后的组件版本（N 版本）
M610	iDRAC	3.50 A00	3.85 A00
	Lifecycle Controller	1.6.0.73	1.7.5.4
	诊断程序	5158A3	5162A0
	BIOS	6.4.0	6.5.0
	NIC	19.2.0	20.00.00.13
M610x	iDRAC	3.50 A00	3.85 A00
	Lifecycle Controller	1.6.0.73	1.7.5.4
	诊断程序	5158A3	5162A0
	BIOS	6.4.0	6.5.0
	NIC	19.2.0	20.00.00.13
M710	iDRAC	3.50 A00	3.85 A00
	Lifecycle Controller	1.6.0.73	1.7.5.4
	诊断程序	5158A3	5162A0
	BIOS	6.4.0	6.5.0
M910	iDRAC	3.50 A00	3.85 A00
	Lifecycle Controller	1.6.0.73	1.7.5.4
	诊断程序	5158A3	5162A0
	BIOS	2.10.0	2.11.0
M915	iDRAC	3.50 A00	3.85 A00
	Lifecycle Controller	1.6.0.73	1.7.5.4
	诊断程序	5158A3	5162A0
	BIOS	3.2.2	3.3.1
M710HD	iDRAC	3.50 A00	3.85 A00
	Lifecycle Controller	1.6.0.73	1.7.5.4
	诊断程序	5158A3	5162A0
	BIOS	8.0.0	8.2.0

平台	服务器组件	上一组件版本（N-1 版本）	更新后的组件版本（N 版本）
	NIC	7.8.15	20.6.18
M420	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	诊断程序	4231A0	4247A1
	BIOS	2.4.2	2.6.1
	NIC	19.2.0	20.00.00.13
M520	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	诊断程序	4231A0	4247A1
	BIOS	2.4.2	2.6.1
	NIC	19.2.0	20.00.00.13
M620	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	诊断程序	4231A0	4247A1
	BIOS	2.5.4	2.6.1
M820	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	诊断程序	4231A0	4247A1
	BIOS	2.6.1	2.6.1
M630	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	诊断程序	4239.44	4239A36
	BIOS	2.6.0	2.7.1
M830	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	诊断程序	4239.44	4239A36
	BIOS	2.5.4	2.7.1
M640	iDRAC	3.15.15.15	3.21.21.21

平台	服务器组件	上一组件版本（N-1 版本）	更新后的组件版本（N 版本）
	Lifecycle Controller	3.15.15.15	3.21.21.21
	诊断程序	4301A13	4301A13
	BIOS	1.3.7	1.4.8

启用 Lifecycle Controller

您可以在服务器引导过程中启用 Lifecycle Controller 服务：

- 对于 iDRAC 服务器，当引导控制台上提示消息 `Press <CTRL-E> for Remote Access Setup within 5 sec.`，按下 <CTRL-E>。然后，在设置屏幕上，启用**系统服务**。
- 对于 iDRAC 服务器，在引导控制台上选择 F2 以进行系统设置。在设置屏幕上，选择 **iDRAC 设置**，然后选择**系统服务**。
  “取消系统服务”可用于取消挂起的所有计划作业并将其从队列中移除。

有关 Lifecycle Controller 和服务器组件以及设备固件管理的更多信息，请参阅：

- *Lifecycle Controller Remote Services User's Guide*（Lifecycle Controller 远程服务用户指南）。
- **delltechcenter.com/page/Lifecycle+Controller**。

服务器组件更新页可以更新系统上的各种固件组件。要使用此页面上的各种功能，您必须拥有以下权限：

- 对于 CMC：**服务器管理员**权限。
- 对于 iDRAC：**配置 iDRAC** 权限和**登录到 iDRAC** 权限。

如果权限不足，则只能查看服务器上组件和设备的固件资源清册。您无法为服务器上任何类型的 Lifecycle Controller 操作选择任何组件或设备。

使用 CMC Web 界面选择服务器组件固件更新类型

要选择服务器组件更新类型：

1 在系统树中，转至**服务器概述**，然后单击**更新** > **服务器组件更新**。
此时将显示**服务器组件更新**页。
2 在**选择更新类型**部分中，选择所需的更新方式：
- **从文件更新**
- **从网络共享更新**

升级服务器组件固件

您可使用文件方法或网络共享方法更新服务器组件固件。

您可以在一个或多个服务器上为所选的组件或设备安装下一个版本的固件映像。固件映像可在回滚操作的 Lifecycle Controller 中获得。

注: 对于 iDRAC 和操作系统驱动程序包固件更新，确保已启用扩展存储功能。

建议在初始化服务器组件固件更新之前清除作业队列。服务器上所有作业的列表可从“Lifecycle Controller 作业”页上获得。此页面允许删除单个或多个作业或清除服务器上的所有作业。请参阅“管理远程系统上的 Lifecycle Controller 作业”的“故障排除”部分。

BIOS 更新特定于服务器的型号。选择逻辑基于此行为。有时，即使选定了服务器上的单一网络接口控制器 (NIC) 设备进行固件更新，更新也可能应用到服务器上所有的 NIC 设备。此行为是 Lifecycle Controller 功能中固有的，尤其是编程采用 Dell Update Package (DUP) 时。目前支持大小小于 48MB 的 Dell Update Package (DUP)。

如果更新文件映像较大，作业状态将指示下载失败。如果在一个服务器上进行多个服务器组件更新，则所有固件更新文件的组合大小也可超过 48MB。在该情况下，其中一个组件更新会因为其更新文件被截断而失败。

要更新服务器上的多个组件，建议先一起更新 Lifecycle Controller 和 32 位诊断程序组件。然后可一起更新其他组件。

下表列出了**固件更新**功能所支持的组件。

注: 通过带外方法或使用 LC Web 界面应用多个固件更新时，这些更新将以最有效率的可能方式排序，以减少对系统进行不必要的重新启动。

表. 12: 固件更新 — 支持的组件

组件名称	支持固件回滚？（“是”或“否”）	带外 — 系统需要重新启动？	带内 — 系统需要重新启动？	Lifecycle Controller GUI — 需要重新启动？
诊断程序	否	否	否	否
操作系统驱动程序包	否	否	否	否
Lifecycle Controller	否	否	否	是
BIOS	是	是	是	是
RAID 控制器	是	是	是	是
背板	是	是	是	是
机柜	是	是	否	是
NIC	是	是	是	是
iDRAC	是	**否	*否	*否
电源设备	是	是	是	是
CPLD	否	是	是	是
FC 卡	是	是	是	是
PCIe SSD	是	是	是	是

* 表示虽然不需要重新启动系统，但必须重新启动 iDRAC 才能应用更新。iDRAC 通信和监测功能可能暂时中断。

** 当从 1.30.30 或更高版本更新 iDRAC 时，无需重新启动系统。但是，在使用带外接口应用早于 1.30.30 的 iDRAC 固件版本时，需要重新启动系统。

通常，所有 Lifecycle Controller 更新都计划立即执行。不过，系统服务可延迟一段时间再执行更新。在这种情况下，会由于通过 CMC 托管的远程共享不再可用而导致更新失败。

所有 LC 组件更新将立即生效。但是，在某些情况下，系统服务会推迟生效的时间。在该情况下，由于 CMC 托管的远程共享不再可用，更新会失败。

使用 CMC Web 界面从文件升级服务器组件固件

要使用**从文件更新**方法将服务器组件固件版本升级至下一个版本，请执行以下操作：

1 在 CMC Web 界面的系统树中，转至**服务器概览**，然后单击**更新** > **服务器组件更新**。

此时将显示**服务器组件更新**页。

2 在**选择更新类型**部分中，选择**从文件更新**。有关更多信息，请参阅选择服务器组件更新类型

3 在**组件/设备更新筛选器**部分，筛选组件或设备（可选）。有关更多信息，请参阅使用 CMC Web 界面筛选进行固件更新的组件。

4 在**更新**列中，选中要将固件更新到下一版本的组件或设备对应的复选框。使用 CRTL 快捷键选择要在所有适用服务器上进行更新的组件或设备类型。按住 CRTL 键以黄色突出显示所有组件。按住 CRTL 键的同时，通过启用**更新**列中关联的复选框选择所需的组件或设备。

此时将显示另外一个表，该表列出所选类型的组件或设备以及固件映像文件的选择器。对于每种类型的组件，会为固件映像文件显示一个选择器。

网络接口控制器 (NIC) 和 RAID 控制器等很少的设备包含许多类型和型号。更新选择逻辑会基于初始选定的设备自动筛选相关的设备类型或型号。此自动筛选行为的主要原因是只能为该类别指定一个固件映像文件。

注: 如果扩展存储功能已安装并已启用，则单一 DUP 或组合 DUP 的更新大小限制可忽略。有关启用扩展存储的信息，请参阅配置 CMC 扩展存储卡。

5 为所选的组件或设备指定固件映像文件。此文件是 Microsoft Windows Dell Update Package (DUP) 文件。

6 选择以下选项之一：

- **立即重新引导** - 立即重新引导。此时将立即应用固件更新
- **下次重新引导时** - 稍后手动重新引导服务器。即下次重新引导后应用固件更新。

注: 该步骤对 Lifecycle Controller 和 32 位 Diagnostics 固件更新无效。这些设备不要求服务器重新引导。

7 单击**更新**。系统会对所选的组件或设备更新固件版本。

使用网络共享一键更新服务器组件

通过使用 Dell Repository Manager 与 Dell PowerEdge M1000e 模块化机箱的集成从网络共享更新服务器或服务器组件，由于使用自定义的捆绑固件，因而简化了更新，便于更快速、更轻松地部署。从网络共享更新可灵活地使用 CIFS 或 NFS 的一个目录同时更新所有第 12 代服务器组件。

通过这种方法，您可以使用 Dell Repository Manager 以及经由 CMC Web 界面导出的机箱资源清册文件快速、轻松地为相连系统构建自定义存储库。DRM 可用于创建完全自定义且仅包含特定系统配置的更新软件包的存储库。您也可以构建仅包含过时设备更新的存储库，或是构建包含所有设备更新的基线存储库。您还可以根据所需的更新模式创建 Linux 或 Windows 的更新捆绑包。通过 DRM，您可以将存储库保存至 CIFS 或 NFS 共享。使用 CMC Web 界面可配置共享的凭据和位置详细信息。通过 CMC Web 界面可为一台服务器或多台服务器进行服务器组件更新。

使用网络共享更新模式的前提条件

要使用“网络共享”模式更新服务器组件固件，必须满足以下前提条件：

- 服务器必须为第 12 代或更高版本，并且必须具备 iDRAC Enterprise 许可证。
- CMC 版本必须为 4.5 版或更高版本。
- 服务器上必须启用 Lifecycle Controller。
- iDRAC 1.50.50 版或更高版本在第 12 代服务器上必须可用。

- 系统上必须安装 Dell Repository Manager 1.8 版或更高版本。
- 必须具备 CMC 管理员权限。

使用 CMC Web 界面从网络共享升级服务器组件固件

使用**从网络共享更新**模式，将服务器组件固件版本升级至下个版本：

1 在 CMC Web 界面的系统树中，转至**服务器概览**，然后单击**更新** > **服务器组件更新**。
此时将显示**服务器组件更新**页。
2 在**选择更新类型**部分中，选择**从网络共享更新**。有关更多信息，请参阅选择服务器组件更新类型。
3 单击**保存资源清册**以导出包含组件和固件详细信息的机箱资源清册文件。
Inventory.xml 文件将保存在外部系统上。Dell Repository Manager 使用 *inventory.xml* 文件创建自定义的更新捆绑。此存储库存储在由 CMC 配置的 CIFS 或 NFS 共享中。有关使用 Dell Repository Manager 创建存储库的信息，请参阅 **dell.com/support/manuals** 上的 *Dell Repository Manager Data Center Version 1.8 User's Guide*（Dell Repository Manager Data Center 1.8 版用户指南）和 *Dell Repository Manager Business Client Version 1.8 User's Guide*（Dell Repository Manager Business Client 1.8 版用户指南）。
4 如果未连接“网络共享”，请为机箱配置“网络共享”。有关更多信息，请参阅使用 CMC Web 界面配置网络共享。
5 单击**检查更新**以查看网络共享中可用的固件更新。
组件/设备固件资源清册部分显示跨所有服务器的机箱中的组件和设备的当前固件版本，以及网络共享中可用 DUP 的固件版本。
6 在**组件/设备固件资源清册**部分中，选择**选择/全部取消**旁的复选框来选择所有支持的服务器。也可选择要更新服务器组件固件的服务器旁的复选框。您不能为服务器选择单个组件。
7 选择以下任一选项可指定在计划更新后是否需要重新引导系统：
   - 立即重新引导 - 计划更新之后就会重新引导服务器，立即将更新应用到服务器组件。
   - 在下次重新引导时 - 计划了更新，但仅在下次重新引导服务器之后应用。
8 单击**更新**计划所选服务器可用组件的固件更新。
将根据所包含更新类型显示一条消息，并要求您确认是否要继续。
9 单击**确定**继续，并为所选服务器完成固件更新的计划。

注: “作业状态”列显示服务器上计划的操作的作业状态。作业状态会动态更新。

筛选进行固件更新的组件

可同时检索所有服务器上所有组件和设备的信息。为了管理这些数量庞大的信息，Lifecycle Controller 提供了各种筛选机制。这些筛选器可以：

- 选择一个或多个组件或设备类别以便于查看。
- 对服务器的组件和设备的固件版本进行比较。
- 自动筛选所选组件和设备，从而基于类型或型号缩小特定组件或设备类别的范围。

注: 自动筛选功能在使用 Dell Update Package (DUP) 时非常重要。DUP 的更新编程可基于组件或设备的类型或型号。自动筛选行为旨在将进行初始选择后的后续选择决策减至最少。

示例

以下是应用筛选机制的一些示例：

- 如果选定 BIOS 筛选器，则只显示所有服务器的 BIOS 资源清册。如果服务器组包含许多服务器型号，并且选定一台服务器用于 BIOS 更新，自动筛选逻辑会自动删除不匹配选定服务器型号的所有其他服务器。这将确保选择的 BIOS 固件更新映像 (DUP) 与正确型号的服务器兼容。
有时，BIOS 固件更新映像可能会与多个服务器型号兼容。这类优化在此兼容性将来不再兼容的情况下忽略。

- 自动筛选对于网络接口控制器 (NIC) 和 RAID 控制器的固件更新非常重要。这些设备类别有不同的类型和型号。类似地，只有在对单一 DUP 进行编程以更新指定类别设备的多个类型或型号时，固件更新映像 (DUP) 才以优化的形式提供。

使用 CMC Web 界面筛选进行固件更新的组件

要筛选设备，请执行以下操作：

1 在系统树中，转至**服务器概述**，然后单击**更新** > **服务器组件更新**。
此时将显示**服务器组件更新**页。
2 在**选择更新类型**部分中，选择**从文件更新**。
3 在**组件/设备更新筛选器**部分，选择以下一项或多项：
- BIOS
- iDRAC
- Lifecycle Controller
- 32 位诊断程序
- 操作系统驱动程序包
- 网络 I/F 控制器
- RAID 控制器

固件资源清册部分只显示机箱中存在的所有服务器的相关组件或设备。该筛选器是通过筛选器；这意味着只允许与该筛选器关联的组件或设备并排除所有其他内容。

筛选的组件和设备组在资源清册部分中显示后，选择进行更新的组件或设备时，可进行进一步筛选。例如，如果选定 BIOS 筛选器，则资源清册部分仅显示所有服务器及其 BIOS 组件。如果选定其中一台服务器上的 BIOS 组件，则资源清册会进一步筛选以显示匹配选定服务器型号名称的服务器。

如果没有选定任何筛选器并在资源清册部分选择了要更新的组件或设备，将自动启用与该选择关联的筛选器。对于所选组件，如果资源清册部分显示的所有服务器在型号、类型或者其他标识形式方面相匹配，则可以进行进一步筛选。例如，如果选定其中一台服务器上的 BIOS 组件进行更新，则筛选器自动设置为 BIOS，并且资源清册部分会显示匹配选定服务器型号名称的服务器。

使用 RACADM 筛选进行固件更新的组件

要使用 RACADM 筛选进行固件更新的组件，请使用 getversion 命令：

```
racadm getversion -l [-m <module>] [-f <filter>]
```

有关更多信息，请参阅 **dell.com/support/manuals** 上的 Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

查看固件资源清册

您可以查看机箱中当前存在的所有服务器的所有组件和设备的固件版本摘要及其状态。

使用 CMC Web 界面查看固件资源清册

要查看固件资源清册，请执行以下操作：

1 在系统树中，转至**服务器概览**，然后单击**更新** > **服务器组件更新**。
此时将显示**服务器组件更新**页。
2 查看**组件/设备固件资源清册**部分中的固件资源清册详细信息。表提供：

- 当前不支持 Lifecycle Controller 服务的服务器列出为**不支持**。所提供的超链接可以导航到替代页，在此可以直接只更新 iDRAC 固件。此页仅支持 iDRAC 固件更新，而不支持对服务器上的任何其他组件和设备进行更新。iDRAC 固件更新不依赖 Lifecycle Controller 服务。
- 如果服务器列为**尚未就绪**，这表示在检索固件资源清册时，服务器上的 iDRAC 仍然在初始化。请稍待片刻，让 iDRAC 充分运行，然后刷新页面以重新检索固件资源清册。
- 如果组件和设备的资源清册没有反映服务器上物理安装的内容，您必须在服务器引导过程中调用 Lifecycle Controller。这可以帮助刷新内部组件和设备信息并允许验证当前安装的组件和设备。出现以下条件时会发生此情况：
  - 更新服务器 iDRAC 固件以将 Lifecycle Controller 功能新引入至服务器管理。
  - 新设备被插入服务器。

  要自动执行此操作，iDRAC 配置公用程序（适用于 iDRAC）或 iDRAC 设置公用程序（适用于 iDRAC）提供了可通过引导控制台访问的选项：

  - 对于 iDRAC 服务器，当引导控制台上提示消息 `Press <CTRL-E> for Remote Access Setup within 5 sec.`，按下 `<CTRL-E>`。然后，在设置屏幕上，启用**在重新启动后收集系统资源清册**。
  - 对于 iDRAC 服务器，在引导控制台上选择 F2 以进行系统设置。在设置屏幕上，选择“iDRAC 设置”，然后选择“系统服务 (USC)”。在设置屏幕上，启用**在重新启动后收集系统资源清册**。
- 执行各种 Lifecycle Controller 操作（例如，“更新”、“回滚”、“重新安装”和“作业删除”）的选项均可用。一次只能执行一种类型的操作。不支持的组件和设备可能会作为资源清册的一部分列出，但不允许 Lifecycle Controller 操作。

下表显示服务器上的组件和设备信息：

表. 13: ：组件和设备信息

字段	说明
插槽	显示机箱中服务器占用的插槽。插槽编号是顺序 ID，从 1 到 16（用于机箱中的 16 个可用插槽），它有助于识别机箱中服务器的位置。如果占用插槽的服务器少于 16 台，则仅显示插有服务器的插槽。
名称	显示每个插槽中的服务器名称。
型号	显示服务器的型号。
组件/设备	显示服务器上的组件或设备的说明。如果列宽过窄，鼠标悬停工具会提供说明视图。显示为以下示例中所示的说明： `QLogic 577xx/578xx 10 Gb Ethernet BCM12345 - 22:X1:X2:X3:BB:0A` **注: FC 16 卡的 WWN 详细信息不显示在固件资源清册部分中。**
当前版本	显示服务器上组件或设备的当前版本。
回滚版本	显示服务器上组件或设备的回滚版本。
作业状态	显示服务器上计划的任何操作的作业状态。作业状态会持续动态更新。如果作业完成并检测到状态“已完成”，则任何组件或设备的固件版本更改时，该服务器上的组件和设备的固件版本会自动刷新。当前状态旁还会提供信息图标，提供当前作业状态的附加信息。此信息可通过单击或悬停在图标上进行查看。
更新	选择服务器上进行固件更新的组件或设备。

使用 RACADM 查看固件资源清册

要使用 RACADM 查看固件资源清册，请使用 getversion 命令：

```
racadm getversion -l [-m <module>] [-f <filter>]
```

有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

使用 CMC Web 界面保存机箱资源清册报告

要保存机箱资源清册报告：

1 在系统树中，转至**服务器概览**，然后单击**更新** > **服务器组件更新**。
此时将显示**服务器组件更新**页。

2 单击**保存资源清册**。
Inventory.xml 文件即会保存在外部系统上。

注: Dell Repository Manager 应用程序使用 *Inventory.xml* 文件作为输入来创建存储库。您必须在单个服务器上启用 CSIOR，并在每次机箱硬件和软件配置发生更改时保存机箱资源清册报告。

使用 CMC Web 界面配置网络共享

要配置或编辑网络共享位置或凭据：

1 在 CMC Web 界面的系统树中，转至**服务器概览**，然后单击**网络共享**。
此时将显示**编辑网络共享**页面。

2 在**网络共享设置**部分中，根据需要配置以下设置：
- 协议
- IP 地址或主机名
- 共享名称
- 更新文件夹
- 文件名（可选）

  注: 仅当默认目录文件名为 catalog.xml 时，文件名为可选。如果目录文件名更改，则必须在该字段输入新名称。
- 配置文件文件夹
- 域名
- 用户名
- 密码
- SMB 版本

注: 仅当协议 类型为 CIFS 时，SMB 版本选项才可用。

注: 如果正在使用借助域注册的 CIFS，并且使用带有 CIFS 本地用户凭据的 IP 访问 CIFS，则必须在域名字段中输入主机名或主机 IP。

有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

3 单击**测试目录**以验证目录是否可读及可写。

4 单击**测试网络连接**来检查是否可访问网络共享位置。
应用 SMB 版本时，将卸载现有的网络共享，并且单击**测试网络连接**或导航到其他 GUI 页面时再次安装。

5 单击**应用**将更改应用到网络共享属性。

注:

单击**上一步**将返回到先前的网络共享设置。

Lifecycle Controller 作业操作

您可以执行 Lifecycle Controller 操作，例如：

- 重新安装
- 回滚
- 更新
- 删除作业

一次只能执行一种类型的操作。不支持的组件和设备可能会作为资源清册的一部分列出，但不允许 Lifecycle Controller 操作。

要执行 Lifecycle Controller 操作，您必须具有：

- 对于 CMC：服务器管理员权限。
- 对于 iDRAC：配置 iDRAC 权限和登录 iDRAC 权限。

Lifecycle Controller 操作在服务器上计划后，可能需要 10 到 15 分钟才能完成。该过程涉及服务器的几次重新引导，在此期间将执行固件安装，还包括固件验证阶段。您可以使用服务器控制台查看此过程的进度。如果服务器上有多个组件或设备需要更新，您可以将所有更新整合为一个计划的操作，从而将所需的重新引导次数减至最少。

有时，如果正在通过另一个会话或环境提交操作进行计划，则会尝试其他操作。在这种情况下，将显示确认弹出消息表明该情况，并且操作不得提交。等待正在进行的操作完成，然后再次提交该操作。

不要在已提交操作进行计划之后离开页面。如果尝试离开，将会显示确认弹出消息以便取消计划的导航。否则，操作将被中断。中断，尤其是“更新”操作期间的中断可能会导致上载的固件映像文件在正确完成之前终止。提交操作进行计划之后，请确保弹出确认消息表明操作已成功计划。

相关链接

重新安装服务器组件固件
回滚服务器组件固件
升级服务器组件固件
删除计划的服务器组件固件作业

重新安装服务器组件固件

您可以在一个或多个服务器上为所选的组件或设备重新安装当前已安装固件的固件映像。固件映像可在 Lifecycle Controller 中获得。

使用 Web 界面重新安装服务器组件固件

要重新安装服务器组件固件，请执行以下操作：

1. 在系统树中，转至**服务器概览**，然后**单击** > **更新** > **服务器组件更新**。
   此时将显示**服务器组件更新**页。
2. 筛选组件或设备（可选）。
3. 在**当前版本**列中，选择您要重新安装固件的组件或设备对应的复选框。
4. 选择以下选项之一：
   - **立即重新引导** - 立即重新引导。
   - **下次重新引导时** - 稍后手动重新引导服务器。
5. 单击**重新安装**。为所选组件或设备重新安装固件版本。

回滚服务器组件固件

您可以在一个或多个服务器上为所选的组件或设备安装以前已安装的固件的固件映像。固件映像可在回滚操作的 Lifecycle Controller 中获得。可用性受 Lifecycle Controller 的版本兼容性逻辑影响。它还假定 Lifecycle Controller 为以前的更新提供便利。

使用 CMC Web 界面回滚服务器组件固件

要将服务器组件固件版本回滚到较早的版本，请执行以下操作：

1 在 CMC Web 界面，展开系统树，转至**服务器概览**，然后单击**更新** > **服务器组件更新**。
随即将显示**服务器组件更新**页面，在**选择更新类型**部分中，选择**从文件更新**。
2 筛选组件或设备（可选）。
3 在**回滚版本**列中，选择您要回滚固件的组件或设备对应的复选框。
4 选择以下选项之一：
- **立即重新引导** - 立即重新引导。
- **下次重新引导时** - 稍后手动重新引导服务器。

5 单击**回滚**。为所选组件或设备重新安装以前安装的固件版本。

删除计划的服务器组件固件作业

您可以删除为一个或多个服务器上所选组件和/或设备计划的作业。

使用 Web 界面删除计划的服务器组件固件作业

要删除计划的服务器组件固件作业，请执行以下操作：

1 在 CMC Web 界面的系统树中，转至**服务器概览**，然后单击**更新** > **服务器组件更新**。
此时将显示**服务器组件更新**页。
2 在**选择更新类型**部分中，选择**从文件更新**。有关更多信息，请参阅选择服务器组件更新类型

注: 您不能对用于服务器组件更新的从网络共享更新模式执行作业删除操作。

3 在**组件/设备更新筛选器**部分，筛选组件或设备（可选）。有关更多信息，请参阅使用 CMC Web 界面筛选进行固件更新的组件。
4 在**作业状态**列中，作业状态旁显示的复选框指示正在进行生命周期控制器作业，并且当前处于指示的状态中。您可选择该作业进行删除操作。
5 单击**作业删除**。
将删除所选组件或设备的作业。

使用 CMC 恢复 iDRAC 固件

iDRAC 固件通常使用 iDRAC 界面更新，如 iDRAC Web 界面、SM-CLP 命令行界面或从 **support.dell.com** 下载的特定操作系统更新软件包。有关更多信息，请参阅 iDRAC User’s Guide（iDRAC 用户指南）。

较早几代的服务器可能包含使用最新 iDRAC 固件更新进程恢复的损坏固件。CMC 检测到损坏的 iDRAC 固件时，将在**固件更新**页上列出服务器。请执行所述的步骤更新固件。

5

查看机箱信息和监测机箱与组件运行状况

您可以查看信息并监测以下各项的运行状况：

- 活动和待机 CMC
- 所有服务器和单个服务器
- 存储阵列
- 所有 IO 模块 (IOM) 和单个 IOM
- 风扇
- iKVM
- 电源设备 (PSU)
- 温度传感器
- LCD 部件

主题：

查看机箱组件摘要

在登录 CMC Web 界面后，可以使用**机箱运行状况**页查看机箱及其组件的运行状况。该页会显示机箱及其组件的实时图形视图。该视图是动态更新的，而且组件子图形覆盖标记和文本提示自动更新以反映当前的状态。

图 6: Web 界面中的机箱图形示例

要查看机箱的运行状况，请转至**机箱概览** > **属性** > **运行状况**。它会显示机箱、活动和待机 CMC、服务器模块、IO 模块 (IOM)、风扇、iKVM、电源设备 (PSU)、温度传感器和 LCD 部件的整体运行状况。单击每个组件即可显示该组件的详情。此外，还会显示 CMC 硬件日志中的最新事件。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

如果将您的机箱配置为组主机箱，则会在登录后显示**组运行状况**页。该页显示机箱级信息和警报。所有活动的重要和不重要的警报都会显示出来。

机箱图形

机箱以正面视图、背面视图和顶部视图呈现（分别为上图和下图）。服务器和 LCD 在正面视图中显示，其余组件在背面视图中显示。选中组件显示为蓝色，并且单击所需组件的图像可进行相应控制。机箱中存在组件时，该组件类型的图标在组件安装位置（插槽）的图形中显示。空位置显示为炭灰色背景。组件图标可指示组件的状态。其他组件显示直观表示物理组件的图标。当安装双倍大小组件时，服务器和 IOM 的图标跨越多个插槽。将光标悬停在组件上方将显示工具提示，其中包含有关该组件的附加信息。

表. 14: 第 13 代系统中的服务器图标状态

图标	说明
	服务器开机且工作正常。
	服务器关闭。

图标	说明
	服务器报告非严重错误。
	服务器报告严重错误。
	无服务器。

表. 15: 第 14 代系统中的服务器图标状态

图标	说明
	服务器开机且工作正常。
	服务器关闭。
	服务器报告非严重错误。

图标	说明
	服务器报告严重错误。
	无服务器。

注: 默认情况下，机箱关闭时，如果您插入 14 代 PowerEdge 服务器，将显示 Dell 的第 13 代 PowerEdge 系统的服务器状态图标。

所选组件信息

所选组件的信息在三个独立的部分中显示：

- “运行状况”、“性能”和“属性” - 显示硬件日志所示的活动严重和非严重事件以及随时间变化的性能数据。
- 属性 - 显示不会随时间变化或很少发生更改的组件属性。
- 快速链接 — 提供链接以导航至常用页面以及常用操作。只有适用于所选组件的链接才会在此部分显示。

注: 在多机箱管理 (MCM) 中，所有与服务器关联的 Quick Links（快速链接）均不会显示。

表. 16: 机箱运行状况页 — 组件属性

组件	运行状况和性能属性	属性	快速链接
LCD 部件	• LCD 运行状况 • 机箱运行状况	无	无
活动和待机 CMC	• 冗余模式 • MAC 地址 • IPv4 • IPv6	• 固件 • 待机固件 • 上次更新时间 • 硬件	• CMC 状态 • 网络 • 固件更新
所有服务器和单个服务器	• 电源状态 • 功耗 • 运行状况 • 分配的功率 • 温度	• 名称 • 型号 • Service Tag • 主机名 • iDRAC • CPLD • BIOS • 操作系统 • CPU 信息	• 服务器状态 • 启动远程控制台 • 启动 iDRAC GUI • 启动 OMSA GUI • 关闭服务器 • 远程文件共享 • 部署 iDRAC 网络 • 服务器组件更新

组件	运行状况和性能属性	属性	快速链接
		• 总系统内存	
iKVM	OSCAR 控制台	• 名称 • 部件号 • 固件 • 硬件	• iKVM 状态 • 固件更新
电源设备	电源状态	容量	• 电源设备状况 • 功耗 • 系统预算
风扇	• 速度	• 严重阈值下限 • 严重阈值上限	• 风扇状况
IOM 插槽	• 电源状态 • Role（角色）	• 型号 • Service Tag	IOM 状态

查看服务器型号名称和服务标签

通过以下步骤可及时获得每台服务器的型号名称和服务标签：

1 展开系统树中的“服务器”。展开的“服务器”列表中显示所有服务器 (1 - 16)。没有服务器的插槽名称会变灰。

2 将光标放在服务器的插槽名称或插槽编号上，工具提示会提示服务器的型号名称和服务标签（如果可用）。

查看机箱摘要

您可以查看机箱中已安装组件的摘要。

要查看机箱摘要信息，请在 CMC Web 界面中，转至**机箱概述** > **属性** > **摘要**。

此时将显示**机箱摘要**页。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看机箱控制器信息和状态

要查看机箱控制器信息和状态，请在 CMC Web 界面中，转至**机箱概述** > **机箱控制器** > **属性** > **状态**。

此时将显示**机箱控制器状态**页。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看所有服务器的信息和运行状况

若要查看所有服务器的运行状况，请执行以下任一操作：

1 转至**机箱概述** > **属性** > **运行状况**。

机箱运行状况页显示机箱中安装的所有服务器的图形概述。服务器运行状况由服务器子图形的覆盖标记指示。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

2 转至**机箱概述** > **服务器概述** > **属性** > **状态**。

服务器状态页提供机箱中服务器的概述。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看单个服务器的运行状况和信息

若要查看单个服务器的运行状况，请执行以下任一操作：

1 转至**机箱概述** > **属性** > **运行状况**。

机箱运行状况页显示机箱中安装的所有服务器的图形概述。服务器运行状况由服务器子图形的覆盖标记指示。将光标移动到单个服务器子图形的上方。所显示的相应文本提示或屏幕提示提供该服务器的附加信息。单击服务器子图形可在右侧查看 IOM 信息。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

2 在系统树中转至**机箱概述**并展开**服务器概述**。展开的列表中显示所有服务器 (1 - 16)。单击想要查看的服务器（插槽）。

Server Status（服务器状态）页（与 **Servers Status**（服务器状态）页不同）提供机箱中服务器的运行状况和指向 iDRAC Web 界面的启动位置，该界面即用于管理服务器的固件。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 若要使用 iDRAC Web 界面，您必须具有 iDRAC 用户名和密码。有关 iDRAC 和使用 iDRAC Web 界面的更多信息，请参阅 *Integrated Dell Remote Access Controller User's Guide*（Integrated Dell Remote Access Controller 用户指南）。

查看存储阵列状态

要查看存储服务器的运行状况，请执行以下任一操作：

1 转至**机箱概述** > **属性** > **运行状况**。

机箱运行状况页显示机箱中安装的所有服务器的图形概述。服务器运行状况由服务器子图形的覆盖标记指示。将光标移动到单个服务器子图形的上方。所显示的相应文本提示或屏幕提示提供该服务器的附加信息。单击服务器子图形可在右侧查看 IOM 信息。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

2 在系统树中，转至**机箱概述**并展开**服务器概述**。展开的列表中显示所有插槽 (1-16)。单击存储阵列插入的插槽。

“存储阵列状态”页提供存储阵列的运行状况和属性。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看所有 IOM 的信息和运行状况

要在 CMC Web 界面中查看 IOM 的运行状况，请执行以下任一操作：

1 转至**机箱概述** > **属性** > **运行状况**。

此时将显示**机箱运行状况**页。**机箱图形**的下半部分展示了机箱的后视图并包含 IOM 的运行状况。IOM 运行状况由 IOM 子图形的覆盖标记表示。将光标移到单个 IOM 子图形的上方。文本提示提供有关该 IOM 的附加信息。单击 IOM 子图形可在右侧查看 IOM 信息。

2 转至**机箱概述** > **I/O 模块概述** > **属性** > **状态**。

I/O 模块状态页提供与机箱关联的所有 IOM 的概述。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看单个 IOM 的信息和运行状况

若要查看单个 IOM 的运行状况，请在 CMC Web 界面中，执行以下任一操作：

1 转至**机箱概览** > **属性** > **运行状况**。

此时将显示**机箱运行状况**页。机箱图形的下半部分展示了机箱的后视图并包含 IOM 的运行状况。IOM 运行状况由 IOM 子图形的覆盖标记表示。将光标移到单个 IOM 子图形的上方。文本提示提供有关该 IOM 的附加信息。单击 IOM 子图形可在右侧查看 IOM 信息。

2 在系统树中转至**机箱概述**并展开 **I/O 模块概述**。展开的列表中显示所有 IOM (1 - 6)。单击想要查看的 IOM（插槽）。

此时将显示特定于该 IOM 插槽的 **I/O 模块状态**页（与整体 **I/O 模块状态**页不同）。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 更新或关机后再开机 IOM/IOA 后，请确保 IOM/IOA 的操作系统也会正确引导。否则，IOM 状态显示为“脱机”。

查看风扇的信息和运行状况

控制风扇速度的 CMC 将根据系统范围内的事件自动提高或降低风扇速度。当发生以下事件时，CMC 生成警报并提高风扇速度：

- 超过 CMC 环境温度阈值。
- 一个风扇发生故障。
- 从机箱中卸下了一个风扇。

注: 在服务器上的 CMC 或 iDRAC 固件更新期间，机箱中的部分或全部风扇装置会 100% 旋转。这是正常现象。

要在 CMC Web 界面中查看风扇的运行状况，请执行以下任一操作：

1 转至**机箱概述** > **属性** > **运行状况**。

此时将显示**机箱运行状况**页。机箱图形的下半部分提供机箱的后视图并包含风扇的运行状况。风扇运行状况由风扇子图形的覆盖标记表示。将光标移到风扇子图形的上方。文本提示提供有关该风扇的附加信息。单击风扇子图形可在右侧查看风扇信息。

2 转至**机箱概述** > **风扇** > **属性**。

风扇状态页提供机箱中风扇的状态和速度测量值（以每分钟转数或 RPM 为单位）。可以有一个或多个风扇。

注: 在 CMC 和风扇装置间发生通信故障时，CMC 将无法获取或显示风扇装置的运行状况。

有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看 iKVM 信息和运行状况

Dell M1000e 服务器机箱的本地访问 KVM 模块称为 Avocent 集成 KVM 交换机模块，即 iKVM。

要查看与机箱关联的 iKVM 的运行状况，请执行以下任一操作：

1 转至**机箱概述** > **属性** > **运行状况**。

此时将显示**机箱运行状况**页。机箱图形的下半部分提供了机箱的后视图并包含 iKVM 的运行状况。iKVM 运行状况由 iKVM 子图形的覆盖标记表示。将光标移到 iKVM 子图形上将显示相应的文本提示或屏幕提示。文本提示提供有关该 iKVM 的附加信息。单击 iKVM 子图形可在右侧查看 iKVM 信息。

2 转至**机箱概述** > **iKVM** > **属性**。

iKVM 状态页显示与机箱关联的 iKVM 的状态和读数。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看 PSU 信息和运行状况

要查看与机箱关联的电源设备 (PSU) 的运行状况，请执行以下任一操作：

1 转至**机箱概** > **属性** > **运行状况**。

此时将显示**机箱运行状况**页。机箱图形的下半部分提供了机箱的后视图并包含所有 PSU 的运行状况。PSU 运行状况由 PSU 子图形的覆盖标记表示。将光标移到单个 PSU 子图形上将显示相应的文本提示或屏幕提示。文本提示提供有关该 PSU 的附加信息。单击 PSU 子图形可在右侧查看 PSU 信息。

2 转至**机箱概述** > **电源**。

电源设备状态页显示与机箱关联的 PSU 的状态和读数。它提供整体电源运行状况、系统电源状况和电源设备冗余状态。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看温度传感器的信息和运行状况

要查看温度传感器的运行状况，请执行以下操作：

转至**机箱概览** > **温度传感器**。

温度传感器状态页显示整个机箱（机箱和服务器）上温度探测器的状态和读数。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 无法编辑温度探测器值。任何超过阈值的更改都会生成警报，从而造成风扇速度发生变化。例如，如果 CMC 环境温度探测器超出阈值，机箱上风扇的速度将提高。

注: 系统无法读取平面板或控制面板温度传感器，您可能已经更改控制面板。

查看 LCD 信息和运行状况

要查看 LCD 的运行状况，请执行以下操作：

1 在 CMC Web 界面的系统树中，转至**机箱概述**，然后单击**属性** > **运行状况**。
此时将显示**机箱运行状况**页。机箱图形的上半部分显示机箱的前视图。LCD 运行状况由 LCD 子图形的覆盖标记表示。

2 移动光标到 LCD 子图形上。相应的文本提示或屏幕提示会提供有关 LCD 的附加信息。

3 单击 LCD 子图形可在右侧查看 LCD 信息。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

6

配置 CMC

通过 CMC 可配置 CMC 属性、设置用户，并且设置警报以执行远程管理任务。

在开始配置 CMC 之前，您必须首先配置 CMC 网络属性设置，以便能够远程管理 CMC 。 该初始配置分配 TCP/IP 联网参数，以便能够访问 CMC。有关更多信息，请参阅设置对 CMC 的初始访问。

可以使用 Web 界面或 RACADM 来配置 CMC。

注: 当首次配置 CMC 时，您必须以 root 用户登录，以在远程系统上执行 RACADM 命令。可创建另一个用户，使之具有配置 CMC 的权限。

在设置 CMC 并执行基本配置之后，您可以执行以下操作：

- 如有必要，修改网络设置。
- 配置访问 CMC 的界面。
- 配置 LED 显示。
- 如有必要，设置机箱组。
- 配置服务器、IOM、或 iKVM。
- 配置 VLAN 设置。
- 获取所需证书。
- 添加和配置具有权限的 CMC 用户。
- 配置并启用电子邮件警报和 SNMP 陷阱。
- 如有必要，设置功率上限策略。

主题：

相关链接

登录 CMC
查看和修改 CMC 网络 LAN 设置
配置 CMC 网络和登录安全设置
为 CMC 配置虚拟 LAN 标签属性
配置服务
配置 LED 以识别机箱上的组件
设置机箱组
配置服务器
管理输入输出结构
配置和使用 iKVM
获取证书
配置用户帐户和权限
配置 CMC 以发送警报
管理和监测电源
使用配置文件通过 RACADM 配置多个 CMC

查看和修改 CMC 网络 LAN 设置

LAN 设置（如团体字符串和 SMTP 服务器 IP 地址）将影响 CMC 和机箱的外部设置。

如果您的机箱具有两个 CMC（活动和待机），且它们均连接至网络，则在出现故障转移时待机 CMC 自动承继活动 CMC 的网络设置。

启动时启用 IPv6，则会每 4 秒发送三个路由器请求。如果外部网络交换机运行生成树协议 (SPT)，则外部交换机端口可在发送 IPv6 路由器请求时阻塞 12 秒以上。在此情况下，当 IPv6 连接受限时，IPv6 路由器无偿发送路由器广告时会等待一段时间。

注: 更改 CMC 网络设置可能会断开当前网络连接。

注: 必须具备机箱配置管理员权限才可以设置 CMC 网络设置。

使用 CMC Web 界面查看和修改 CMC 网络 LAN 设置

要使用 CMC Web 界面查看和修改 CMC 网络 LAN 设置，请执行以下操作：

1 在系统树中，转至**机箱概述**并单击**网络** > **网络**。**网络配置**页显示当前的网络设置。
2 根据需要修改常规、IPv4 或 IPv6 设置。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用更改**，每个部分即应用这些设置。

使用 RACADM 查看 CMC 网络 LAN 设置

使用命令 `getconfig -g cfgcurrentlannetworking` 查看 IPv4 设置。
使用命令 `getconfig -g cfgCurrentIPv6LanNetworking` 查看 IPv6 设置。

要查看机箱的 IPv4 和 IPv6 寻址信息，请使用 `getsysinfo` 子命令。

有关子命令和对象的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

启用 CMC 网络接口

若要为 IPv4 和 IPv6 启用/禁用 CMC 网络接口，请键入：

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicEnable 0
```

注: 如果禁用 CMC 网络接口，禁用操作将执行以下操作：

- 禁用对带外机箱管理（包括 iDRAC 和 IOM 管理）的网络接口访问。
- 防止下行链路状态检测。
- 如仅禁用 CMC 网络访问，应同时禁用 CMC IPv4 和 CMC IPv6。

注: 默认情况下启用 CMC NIC。

要启用/禁用 CMC IPv4 寻址，请键入：

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
1
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
0
```

注: 默认情况下启用 CMC IPv4 寻址。

要启用/禁用 CMC IPv6 寻址，请键入：

```
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
1
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
0
```

注: 默认情况下禁用 CMC IPv6 寻址。

默认情况下，对于 IPv4，CMC 自动从动态主机配置协议 (DHCP) 服务器请求并获取 CMC IP 地址。您可以禁用 DHCP 功能并指定静态 CMC IP 地址、网关和子网掩码。

对于 IPv4 网络，要禁用 DHCP 并指定静态 CMC IP 地址、网关和子网掩码，请键入：

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgNicIpAddress <static IP address>
racadm config -g cfgLanNetworking -o cfgNicGateway <static gateway>
racadm config -g cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

默认情况下，对于 IPv6，CMC 自动从 IPv6 自动配置机制请求并获取 CMC IP 地址。

对于 IPv6 网络，要禁用自动配置功能并指定静态 CMC IPv6 地址、网关和前缀长度，请键入：

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6AutoConfig 0
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Address <IPv6 address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6PrefixLength 64
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Gateway <IPv6 address>
```

为 CMC 网络接口地址启用或禁用 DHCP

当启用时，CMC 的 NIC 地址 DHCP 功能将自动从动态主机配置协议 (DHCP) 服务器请求和获取 IP 地址。默认启用此功能。

您可以禁用 NIC 地址 DHCP 功能并指定静态 IP 地址、子网掩码和网关。有关更多信息，请参阅设置对 CMC 的初始访问。

对 DNS IP 地址启用或禁用 DHCP

默认情况下，禁用 CMC 的 DNS 地址 DHCP 功能。当启用时，该功能将从 DHCP 服务器获取主要和次要 DNS 服务器地址。使用该功能，可以不用配置静态 DNS 服务器 IP 地址。

要禁用 DNS 地址 DHCP 功能并指定静态主要和备用 DNS 服务器地址，请键入：

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

要禁用 IPv6 的 DNS 地址 DHCP 功能并指定静态首选和备用 DNS 服务器地址，请键入：

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServersFromDHCP6 0
```

设置静态 DNS IP 地址

注: 静态 DNS IP 地址设置在禁用 DNS 地址的 DCHP 功能时才有效。

对于 IPv4，要设置主要和次要 DNS IP 服务器地址，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP-address> racadm config -g
cfgLanNetworking -o cfgDNSServer2 <IPv4-address>
```

对于 IPv6，要设置主要和次要 DNS IP 服务器地址，请键入：

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1 <IPv6-address> racadm config -g
cfgIPv6LanNetworking -o cfgIPv6DNSServer2 <IPv6-address>
```

配置 IPv4 和 IPv6 的 DNS 设置

- **CMC 注册** - 若要在 DNS 服务器上注册 CMC，请键入：

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

  注: 有些 DNS 服务器只注册 31 个或更少字符的名称。确保指定的名称在 DNS 要求的范围内。

  注: 只有通过将 cfgDNSRegisterRac 设置为 1 在 DNS 服务器上注册 CMC，以下设置才有效。

- **CMC Name（CMC 名称）**— 默认情况下，DNS 服务器上的 CMC 名称是 cmc-<*服务标签*>。要更改 DNS 服务器上的 CMC 名称，请键入：

  ```
  racadm config -g cfgLanNetworking -o cfgDNSRacName <name>
  ```

  其中，<name> 为最多 63 个字母数字字符和连字符的字符串。例如：cmc-1、d-345。

  注: 如果未指定 DNS 域名，则最大字符数为 63。如果指定了域名，则 CMC 名称中的字符数加上 DNS 域名中的字符数必须小于或等于 63 个字符。

- **DNS Domain Name（DNS 域名）**— 默认 DNS 域名是单个空字符。要设置 DNS 域名，请键入：

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSDomainName <name>
  ```

  其中，<name> 为最多 254 个字母数字字符和连字符的字符串。例如，p45、a-tz-1、r-id-001。

配置 IPv4 和 IPv6 的自动协商、双工模式和网络速度

当启用时，自动协商功能确定 CMC 是否通过与最近的路由器或交换机通信来自动设置双工模式和网络速度。默认启用自动协商功能。

可以通过键入以下命令禁用自动协商并指定双工模式和网络速度：

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

其中：

`<duplex mode>` 为 0（半双工）或 1（全双工，默认值）

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

其中：

`<speed>` 是 10 或 100（默认值）。

设置 IPv4 和 IPv6 的最大传输单元

最大传输单元 (MTU) 属性允许您设置能够通过该接口传输的最大数据包限制。要设置 MTU，请键入：

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

其中 `<mtu>` 是 576 - 1500（包含起始值；默认值为 1500）之间的值。

注: IPv6 要求的最小 MTU 是 1280。如果启用了 IPv6 并且 `cfgNetTuningMtu` 设置为更小的值，则 CMC 会使用 1280 的 MTU。

配置 CMC 网络和登录安全设置

CMC 中的 IP 地址阻止和用户阻止功能使您能够防止由于尝试猜测密码带来的安全问题。此功能使您能够阻止一系列的 IP 地址和可以访问 CMC 的用户。CMC 中默认启用 IP 地址阻止功能。您可以使用 CMC Web 界面或 RACADM 设置 IP 范围属性。要使用 IP 地址阻止和用户阻止功能，请使用 CMC Web 界面或 RACADM 启用选项。配置登录锁定策略设置，使您能够设置特定用户的登录尝试失败或 IP 地址的数量。在超出此限制后，被阻止的用户只能在惩罚时间之后登录。

注: IP 地址阻止功能仅适用于 IPV4 地址。

使用 CMC Web 界面配置 IP 范围属性

注: 要执行以下任务，必须具备机箱配置管理员权限。

要使用 CMC Web 界面配置 IP 范围属性，请执行以下操作：

1. 在系统树中，转至**机箱概览**，单击**网络** > **网络**。随即将显示**网络配置**页面。
2. 在“IPv4 设置”部分，单击**高级设置**。
   将显示**安全登录**页面。
   此外，要访问“安全登录”页面，请在系统树中，转至**机箱概览**，单击**安全** > **登录**。
3. 要启用 IP 范围检查功能，请在 **IP 范围**部分，选中**启用 IP 范围**选项。
   将激活 **IP 范围地址**和 **IP 范围掩码**字段。
4. 在 **IP 范围地址**和 **IP 范围掩码**字段中，输入您希望禁止访问 CMC 的 IP 地址的范围和 IP 范围掩码。
   有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
5. 单击**应用**保存设置。

使用 RACADM 配置 IP 范围属性

您可以使用 RACADM 配置 CMC 的以下 IP 范围属性：

- IP 范围检查功能
- 您希望禁止访问 CMC 的 IP 地址范围
- 您希望禁止访问 CMC 的 IP 范围掩码

IP 筛选功能会比较接入登录的 IP 地址与指定的 IP 地址范围。仅当以下两项相同时才允许接入 IP 地址登录：

- **cfgRacTuneIpRangeMask** 与传入 IP 地址进行按位与
- **cfgRacTuneIpRangeMask** 按位并有 **cfgRacTuneIpRangeAddr**

- 要启用 IP 范围检查功能，请使用 `cfgRacTuning` 组中的以下属性：
  ```
  cfgRacTuneIpRangeEnable <0/1>
  ```
- 要指定您希望禁止访问 CMC 的 IP 地址范围，请使用 `cfgRacTuning` 组中的以下属性：
  ```
  cfgRacTuneIpRangeAddr
  ```
- 要指定您希望禁止访问 CMC 的 IP 范围掩码，请使用 `cfgRacTuning` 组中的以下属性：
  ```
  cfgRacTuneIpRangeMask
  ```

为 CMC 配置虚拟 LAN 标签属性

VLAN 用于允许多个虚拟 LAN 共同存在于同一物理网络电缆上，并允许出于安全性和负载管理的目的而分离网络流量。启用 VLAN 功能时，将给每个网络信息包分配 VLAN 标签。

使用 Web 界面为 CMC 配置虚拟 LAN 标签属性

要使用 CMC Web 界面为 CMC 配置 VLAN，请执行以下操作：

1 转至以下任一页：
   - 在系统树中，转至**机箱概览**，单击**网络** > **VLAN**。
   - 在系统树中，转至**机箱概览** > **服务器概览**并单击**网络** > **VLAN**。

   此时将显示 **VLAN 标签设置**页。VLAN 标签是机箱属性。即使拆下了组件，机箱仍然有这些标签。
2 在 **CMC** 部分，为 CMC 启用 VLAN，设置优先级并分配 ID。有关这些字段的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用**。将保存 VLAN 标签设置。

   您还可以从**机箱概览** > **服务器** > **设置** > **VLAN** 子选项卡访问此页。

使用 RACADM 为 CMC 配置虚拟 LAN 标签属性

1 启用外部机箱管理网络的 VLAN 功能：
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
   ```
2 为外部机箱管理网络指定 VLAN ID：
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN ID>
   ```

   `<VLAN ID>` 的有效值是 1-4000 和 4021-4094。默认值是 1。

例如：

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

3 然后，为外部机箱管理网络指定 VLAN 优先级：

```
racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN priority>
```

<VLAN priority> 的有效值是 0-7。默认值是 0。

例如：

```
racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
```

也可用一个命令指定 VLAN ID 和 VLAN 优先级：

```
racadm setniccfg -v <VLAN id> <VLAN priority>
```

例如：

```
racadm setniccfg -v 1 7
```

4 若要移除 CMC VLAN，请禁用外部机箱管理网络的 VLAN 功能：

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

也可用以下命令移除 CMC VLAN：

```
racadm setniccfg -v
```

联邦信息处理标准

美国联邦政府的机构和承包商使用联邦信息处理标准 (FIPS)，计算机安全性标准，该标准与具有通信接口的所有应用程序相关。140-2 共有四种级别 — 1 级、2 级、3 级和 4 级。FIPS 140 - 2 系列规定所有通信接口必须具有以下安全性属性：

- 验证
- 机密性
- 消息完整性
- 不可否认性
- 可用性
- 访问控制

如果任何属性依赖于加密算法，这些算法必须获得 FIPS 的批准。

默认情况下，FIPS 模式处于禁用状态。FIPS 已启用时，OpenSSL FIPS 的最小密钥大小为 SSH-2 RSA 2048 位。

注: 当在机箱中启用 FIPS 模式时，不支持 PSU 固件更新。

有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

下列功能/应用程序支持 FIPS。

- Web GUI
- RACADM
- WSMan
- SSH v2
- SMTP
- Kerberos
- NTP 客户端
- NFS

注: SNMP 不符合 FIPS 规范。在 FIPS 模式下，除消息摘要算法版本 5 (MD5) 验证以外的所有 SNMP 功能都有效。

使用 CMC Web 界面启用 FIPS 模式

要启用 FIPS：

1 在左侧窗格中，单击**机箱概览**。
此时会显示**机箱运行状况**。
2 在菜单栏上，单击**打印机**。
将显示**网络配置**页面。
3 在**联邦信息处理标准 (FIPS)** 部分中，从 **FIPS 模式**下拉菜单中，选择**已启用**。
此时会显示一条消息：启用 FIPS 会将 CMC 重设为默认设置。
4 单击**确定**继续。

使用 RACADM 启用 FIPS 模式

要启用 FIPS 模式，请运行以下命令：

```
racadm config –g cfgRacTuning –o cfgRacTuneFipsModeEnable 1
```

。

禁用 FIPS 模式

要禁用 FIPS 模式，将 CMC 重设为默认出厂设置。

配置服务

您可以在 CMC 上配置和启用以下服务：

- CMC 串行控制台 - 支持使用串行控制台访问 CMC。
- Web 服务器 - 支持访问 CMC Web 界面。如果您禁用该选项，请使用本地 RACADM 重新启用 Web 服务器，因为禁用 Web 服务器时会同时禁用远程 RACADM。
- SSH - 支持通过固件 RACADM 访问 CMC。
- Telnet - 支持通过固件 RACADM 访问 CMC
- RACADM - 支持使用 RACADM 访问 CMC。
- SNMP - 支持 CMC 发送事件的 SNMP 陷阱。
- 远程系统日志 - 支持 CMC 将事件记录到远程服务器。

注: 在修改 SSH、Telnet、HTTP 或 HTTPS 的 CMC 服务端口号时，请避免使用 OS 服务常用的端口（如端口 111）。请参阅 http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml 上的互联网编号分配机构 (IANA) 保留端口。

CMC 包含 Web 服务器，它配置为使用行业标准 SSL 安全协议通过 Internet 接受和传输来自客户端的加密数据，或者向客户端传输数据。Web 服务器包括 Dell™ 自签名的 SSL 数字证书（服务器 ID）并且负责接受和响应来自客户端的安全 HTTP 请求。该服务是用于与 CMC 通信的 Web 界面和远程 RACADM CLI 工具必需的服务。

如果 Web 服务器重设，请等待至少一分钟以使服务再次可用。Web 服务器重设通常是由以下某个事件所导致的：

- 通过 CMC Web 用户界面或 RACADM 更改了网络配置或网络安全性属性。
- 通过 Web 用户界面或 RACADM 更改了 Web 服务器端口配置。

- CMC 重设。
- 上载了新的 SSL 服务器证书。

注：要修改服务设置，必须具备机箱配置管理员权限。

远程系统日志是 CMC 的附加日志目标。配置远程系统日志之后，CMC 生成的每个新日志条目都会转发至目标。

注：由于在所转发日志条目的网络传输过程中采用 UDP，因此不能保证日志条目成功发送，CMC 也不会收到关于日志条目是否已经被成功接收的反馈。

使用 CMC Web 界面配置服务

要使用 CMC Web 界面配置 CMC 服务，请执行以下操作：

1 在系统树中，转至**机箱概述**，然后单击**网络** > **服务**。此时将显示**服务**页。

2 根据需要配置以下服务：
   - CMC 串行控制台
   - Web 服务器
   - SSH
   - Telnet
   - 远程 RACADM
   - SNMP
   - 远程系统日志

   有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

3 单击**应用**，然后更新所有默认超时和最大超时限制。

使用 RACADM 配置服务

要启用和配置各种服务，请使用以下 RACADM 对象：

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

有关这些对象的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

如果服务器上的固件不支持某项功能，则在配置与该功能相关的属性时将显示错误。例如，使用 RACADM 在不受支持的 iDRAC 启用远程系统日志时将显示一条错误信息。

同样，使用 RACADM getconfig 命令显示 iDRAC 属性时，对于服务器上不支持的功能，属性值显示为 N/A（不适用）。

例如：

```
$ racadm getconfig -g cfgSessionManagement -m server-1 # cfgSsnMgtWebServerMaxSessions=N/A #
cfgSsnMgtWebServerActiveSessions=N/A # cfgSsnMgtWebServerTimeout=N/A #
cfgSsnMgtSSHMaxSessions=N/A # cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSHTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A # cfgSsnMgtTelnetTimeout=N/A
```

配置 CMC 扩展的存储卡

可以启用或修复可选的可移动闪存介质，以用于扩展的非易失性存储。某些 CMC 功能依赖于扩展的非易失性存储进行操作。

要使用 CMC Web 界面启用或修复可选的可移动闪存介质：

1 在系统树中，转到**机箱概览**，然后单击**机箱控制器** > **闪存介质**。 随即显示“可移动闪存介质”页面。
2 从下拉菜单中，根据需要选择以下选项之一：
   - 使用闪存介质存储机箱数据
   - 修复活动控制器介质
   - 开始在介质之间复制数据
   - 停止在介质之间复制数据
   - 停止使用闪存介质存储机箱数据

   有关这些选项的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用**以应用所选的选项。
   如果机箱中存在两个 CMC，则两个 CMC 必须都包含闪存介质。除非安装了 Dell 认证的介质并在此页面已启用，否则依赖于闪存介质的 CMC 功能（除了 Flexaddress 以外）不会正常运行。

设置机箱组

CMC 可以从一个主要机箱监测多个机箱。启用机箱组时，主要机箱中的 CMC 会生成主要机箱的状态和机箱组内所有成员机箱状态的图形显示。
机箱组功能为：

- **机箱组**页面会显示描绘每个机箱正面和反面的图像，主机箱一组，每个成员机箱一组。
- 有关主机箱和组成员的运行状况通过红色或黄色覆盖标记识别，并在有问题的组件上标识 X 或！符号。单击机箱图像或**详情**按钮时，机箱图像下会显示详情。
- 快速启动链接可用于打开成员机箱或服务器的 Web 页面。
- 刀片服务器和输入/输出资源清册对于组可用。
- 提供可选选项，以在新成员添加到组时令新成员的属性与主机箱属性同步。

机箱组最多可包含八个成员。此外，主机箱或成员只能加入一个组。不能将作为一个组的组成部分（主机箱或成员）的机箱加入到另一个组中。可以从一个组中删除机箱，并在稍后将其添加到不同组。

要使用 CMC Web 界面设置机箱组：

1 以机箱管理员权限登录到计划作为主机箱的机箱。
2 单击**设置** > **组管理**。此时会显示**机箱组**页。
3 在 **机箱组**页中的**角色**下，选择**主机箱**。此时将显示用于添加组名称的字段。
4 在**组名称**字段中输入组名称，然后单击**应用**。

   注: 适用于域名的相同规则也适用于组名称。

   创建机箱组后，GUI 会自动切换到**机箱组**页。 系统树按组名称指示组，并且主机箱和未归类的成员机箱会在系统树中显示。

   注: 确保主机箱的版本始终为最新版本。

相关链接

将成员添加到机箱组
从主机箱中移除成员
解散机箱组
在成员机箱中禁用单个成员
启动成员机箱或服务器的 Web 页面
传播主机箱属性至成员机箱

将成员添加到机箱组

设置机箱组后，可以将成员添加到该组：

1 以机箱管理员权限登录到主机箱。
2 在树中选择主机箱。
3 单击**设置** > **组管理**。
4 在**组管理**下的**主机名/IP 地址**字段中输入成员的 IP 地址或 DNS 名称。

注: 要使 MCM 正常工作，必须在所有组成员和主机箱中使用默认的 HTTPS 端口 (443)。

5 在成员机箱的**用户名**字段中输入具备机箱管理员权限的用户名。
6 在**密码**字段中输入相应的密码。
7 单击**应用**。
8 重复步骤 4 到步骤 8 添加最多 8 个成员。新成员的机箱名称显示在**成员**对话框中。

选择树中的组可显示新成员的状态。单击机箱图像或详情按钮可提供详情。

注: 为成员输入的凭据会加密传递到成员机箱，以在成员与主机箱之间建立信任关系。凭据不会在任一机箱中保留，并且永远不会在建立初始信任关系后再次进行交换。

有关传播主机箱属性到成员机箱的信息，请参阅 传播主机箱属性到成员机箱

从主机箱中移除成员

可以从主机箱移除组中的成员。要移除成员，请执行以下操作：

1 以机箱管理员权限登录到主机箱。
2 在树中选择主机箱。
3 单击**设置** > **组管理**。
4 从**移除成员**列表中，选择一个或多个要删除的成员名称，然后单击**应用**。

主机箱随后会与已从组中移除的一个或多个成员机箱（如果选择多个）进行通信。成员名称即被移除。如果因为网络问题导致主机箱与成员机箱之间无法通信，则成员机箱可能无法收到该消息。在这种情况下，从成员机箱禁用该成员即可完成移除。

相关链接

在成员机箱中禁用单个成员

解散机箱组

要从主机箱解散机箱组，请执行以下操作：

1 以管理员权限登录到主机箱。
2 在树中选择主机箱。
3 单击**设置** > **组管理**。
4 在**机箱组**页中的**角色**下，选择**无**，然后单击**应用**。

主机箱随后会与已从组中删除的所有成员通信。最后，主机箱会终止其角色。现在，它可以分配为另一个组的成员或主机箱。

如果因为网络问题导致主机箱与成员机箱之间无法联系，则成员机箱可能无法收到该消息。在这种情况下，从成员机箱禁用该成员即可完成移除。

在成员机箱中禁用单个成员

有时，无法通过主机箱从组中移除成员。如果与该成员的网络连接丢失，则可能会发生此情况。要在成员机箱上从组中移除成员：

1 以机箱管理员权限登录到成员机箱。
2 单击**设置** > **组管理**。
3 选择**无**，然后单击**应用**。

启动成员机箱或服务器的 Web 页面

指向成员机箱的 Web 页面、服务器的远程控制台或服务器 iDRAC 的 Web 页面的链接可通过主机箱的组页面获得。您可使用登录主机箱的相同用户名和密码来登录成员设备。如果成员设备有相同的登录凭据，则无需额外登录。否则，用户将被引导至成员设备的登录页。

要导航到成员设备，请执行以下操作：

1 登录到主机箱。
2 在树中选择**组：名称**。
3 如果成员 CMC 是所需的目标，请为所需机箱选择**启动 CMC**。当主机箱和成员机箱均已启用或已禁用 FIPS 时，如果您尝试使用 **Launch CMC（启动 CMC）**登录到成员机箱，则系统会将您导向 **Chassis Group Health（机箱组运行状况）**页面。否则，您会转至成员机箱的 **Login（登录）**页面。

   如果机箱中的服务器是所需目标：

   a 选择目标机箱的图像。
   b 在 **Health and Alerts（运行状况和警报）**窗格下显示的机箱图像中，选择服务器。
   c 在标记为 **Quick Links（快速链接）**的框中，选择目标设备。此时会显示带有目标页面或登录屏幕的新窗口。

   注: 在 MCM 中，不会显示与服务器关联的所有 Quick Links（快速链接）。

传播主机箱属性至成员机箱

您可以将来自主机箱的属性应用至组中的成员机箱。要同步成员与主机箱属性，请执行以下操作：

1 以管理员权限登录到主机箱。
2 在树中选择主机箱。
3 单击**设置** > **组管理**。
4 在**机箱属性传播**部分，选择以下传播类型之一：
   - 动态变化传播 — 选择此选项以自动传播所选机箱属性设置。每当主机箱属性被更改时，该属性更改即被传播至所有当前的组成员。
   - 手动传播 — 选择此选项以手动传播组机箱主机箱属性至其成员。主机箱属性设置仅在主机箱管理员单击**传播**时，才传播至组的其他成员。
5 在**传播属性**部分，选择将要被传播至成员机箱的主机箱配置属性的类别。

   请仅选择那些您希望在机箱组的所有成员上采取同样配置的设置类别。例如，选择**日志和警报属性**类，以启用组中的所有机箱共享主机箱的日志和警报设置。
6 单击**保存**。

   如果选择**动态变化传播**，成员机箱将采用主机箱的属性。如果选择**手动传播**，当您希望传播所选设置至成员机箱时，请单击**传播**。有关将主机箱属性传播至成员机箱的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

多机箱管理组的服务器资源清册

机箱组运行状况页显示所有成员机箱，并允许您使用标准浏览器下载功能将服务器资源清册报告保存到文件中。该报告包含以下对象的数据：

- 当前在所有组机箱（包括主机箱）中的所有服务器。
- 空插槽和扩展插槽（包括全高和双宽服务器）。

保存服务器资源清册报告

要使用 CMC Web 界面保存服务器资源清册报告：

1 在系统树中，选择**组**。
随即会显示**机箱组运行状况**页面。
2 单击**保存资源清册报告**。
会显示**文件下载**对话框，提示您打开或保存文件。
3 单击**保存**并指定服务器资源清册报告的路径和文件名。

注: 机箱组的主机箱、成员机箱和关联机箱中的服务器必须处于打开状态，才能获得最准确的服务器资源清册报告。

导出的数据

服务器资源清册报告包含在机箱组主机箱的正常轮询期间（每 30 秒一次）由各个机箱组成员最近返回的数据。

要获得最准确的服务器资源清册报告：

- 机箱组主机箱和所有机箱组成员机箱必须处于**机箱电源状态开启**状态。
- 相关机箱中的所有服务器都必须为电源开启状态。

如果机箱组成员机箱的子集为以下状态，则资源清册报告中可能会缺少相关机箱和服务器的资源清册数据：

- **机箱电源状态关闭**
- 关机

注: 如果在机箱电源关闭时插入服务器，则在机箱再次通电前不会在 Web 界面中的任何位置显示型号。

下表列出每个服务器要报告的具体数据字段以及字段的具体要求：

数据字段	示例
机箱名称	数据中心主机箱
机箱 IP 地址	192.168.0.1
插槽位置	1
插槽名称	SLOT-01
主机名	合并 Web 服务器 **注: 需要在服务器上运行的服务器管理员代理；否则显示为空。**

操作系统	Microsoft Windows Server 2012 标准 x64 版本 **注: 需要在服务器上运行的服务器管理员代理；否则显示为空。**
型号	PowerEdgeM630
Service Tag	1PB8VF2
总系统内存	4.0 GB **注: 需要 CMC 5.0（或更高版本）。**
CPU 数量	2 **注: 需要 CMC 5.0（或更高版本）。**
CPU 信息	Intel (R) Xeon (R) CPU E5 - 2690 v3@2.60 GHz

数据格式

资源清册报告以 .CSV 文件格式生成，这样便可将其导入各种工具，例如 Microsoft Excel。可通过在 MS Excel 中选择**数据** > **自文本**将资源清册报告 .CSV 文件导入模板。在将资源清册报告导入至 MS Excel 之后，如果显示一条消息提示需要附加信息，则请选择逗号分隔以将文件导入至 MS Excel。

机箱组资源清册和固件版本

机箱组固件版本页面显示机箱组资源清册与机箱中服务器和服务器组件的固件版本。您还可以在该页面上整理资源清册信息并筛选固件版本视图。将基于服务器或以下任何机箱服务器组件显示视图：

- BIOS
- iDRAC
- CPLD
- USC
- 诊断程序
- 操作系统驱动程序
- RAID
- NIC

注: 每次添加或卸下组中的机箱后，显示的机箱组、成员机箱、服务器和服务器组件资源清册信息都会更新。

查看机箱组资源清册

要使用 CMC Web 界面查看机箱组，请在系统树中选择**组**。单击**属性** > **固件版本**。**机箱组固件版本**页面将显示组中的所有机箱。

使用 Web 界面查看所选机箱的资源清册

要使用 CMC Web 界面查看所选机箱的资源清册，请执行以下操作：

1 在系统树中，选择**组**。单击**属性** > **固件版本**。

机箱组固件版本页面将显示组中的所有机箱。

2 在**选择机箱**部分，选择您要查看其资源清册的成员机箱。

固件视图筛选器部分将显示所选机箱的服务器资源清册和所有服务器组件的固件版本。

使用 Web 界面查看所选服务器组件的固件版本

要使用 CMC Web 界面查看所选服务器组件的固件版本，请执行以下操作：

1 在系统树中，选择**组**。单击**属性** > **固件版本**。

机箱组固件版本页面将显示组中的所有机箱。

2 在**选择机箱**部分，选择您要查看其资源清册的成员机箱。

3 在**固件视图筛选器**部分，选择**组件**。

4 在**组件**列表中，选择您要查看其固件版本的所需组件：BIOS、iDRAC、CPLD、USC、诊断程序、操作系统驱动程序、RAID 设备（最多 2 个）和 NIC 设备（最多 6 个）。

将显示所选成员机箱中所有服务器的所选组件的固件版本。

注: 在以下情况下，服务器的 USC、诊断程序、操作系统驱动程序、RAID 设备和 NIC 设备的固件版本不显示：

- 服务器属于第 10 代 PowerEdge 服务器。这些服务器不支持 Lifecycle Controller。
- 服务器属于第 11 代 PowerEdge 服务器，但是 iDRAC 固件不支持 Lifecycle Controller。
- 成员机箱的 CMC 固件版本低于 4.45。在这种情况下，该机箱中所有服务器的组件都不显示，即使服务器支持 Lifecycle Controller 也是如此。

获取证书

下表列出了基于登录类型的证书类型。

表. 17: 登录和证书类型

登录类型	证书类型	获取方法
使用 Active Directory 的单点登录	可信 CA 证书	生成 CSR 并从证书颁发机构获取签名。
以 Active Directory 用户身份进行智能卡登录	• 用户证书 • 可信 CA 证书	• 用户证书 - 使用智能卡供应商提供的卡管理软件将智能卡用户证书导出为基于 64 位编码的文件。 • 可信 CA 证书 - 此证书由 CA 颁发。
Active Directory 用户登录	可信 CA 证书	此证书由 CA 颁发。
本地用户登录	SSL 证书	生成 CSR 并从可信 CA 获取签名。 **注: CMC 出厂时带有默认的自签名 SSL 服务器证书。CMC Web 服务器和虚拟控制台使用此证书。**

相关链接

安全套接字层服务器证书

安全套接字层服务器证书

CMC 包含一个 Web 服务器，该服务器配置为使用业界 标准安全套接字层 (SSL) 安全保护协议在 Internet 上传输加密数据。基于公共密钥和私人密钥加密技术构建的 SSL 是一项普遍认可的技术，用于在客户端和服务器之间提供经过验证和加密的通信，以防止网络上的窃听现象。

SSL 允许启用 SSL 的系统执行以下任务：

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

此加密过程可提供高级别数据保护。CMC 采用 128 位 SSL 加密标准，这是北美常用的 Internet 浏览器最安全的加密形式。

CMC Web 服务器包括 Dell 自签字的 SSL 数字认证 (Server ID)。要确保 Internet 上的高安全性，请向 CMC 提交生成新证书签名的请求 (CSR) 来替换 Web 服务器 SSL 证书。

在引导时如果发生以下情况，将生成新的自签名证书：

- 自定义证书不存在
- 自签名证书不存在
- 自签名证书已损坏
- 自签名证书已过期（在 30 天窗口期内）

自签名证书显示通用名称 <cmcname.domain-name>，其中 cmcname 是 CMC 的主机名，domain-name 是域名。如果域名不可用，它仅显示部分限定域名 (PQDN)，这是 CMC 的主机名。

证书签名请求

证书签名请求 (CSR) 是对证书颁发机构（在 Web 界面中称为 CA）发出的安全服务器证书数字请求。安全服务器证书确保远程系统的身份并确保与远程系统交换的信息无法由他人查看或更改。要确保 CMC 的安全性，强烈建议生成 CSR、将 CSR 提交给证书机构并上传证书颁发机构返回的证书。

证书颁发机构是 IT 行业公认的业务实体，可满足高标准的可靠性审查、识别和其他重要安全标准。例如，Thwate 和 VeriSign 均为 CA。证书颁发机构接收 CSR 之后将审查并验证 CSR 包含的信息。如果申请人符合证书颁发机构的安全性标准，证书颁发机构会向申请人签发证书，该证书可唯一识别申请人通过网络或 Internet 开展交易。

证书颁发机构批准 CSR 并发送证书后，必须将证书上传到 CMC 固件。存储在 CMC 固件中的 CSR 信息必须与证书中包含的信息匹配。

注: 要为 CMC 配置 SSL 设置，必须具备机箱配置管理员权限。

注: 您上载的任何服务器证书必须为当期（未过期）并且由证书颁发机构签发。

相关链接

生成新的证书签名请求
上载服务器证书
查看服务器证书

生成新的证书签名请求

要确保安全性，强烈建议您获取安全服务器证书并将其上载到 CMC。安全服务器证书可以确保远程系统的身份，且他人无法查看或更改与远程系统交换的信息。没有安全服务器证书，CMC 容易受到未经授权的用户访问。

要为 CMC 获取安全服务器证书，您必须将证书签名请求 (CSR) 提交给您选择的证书颁发机构。CSR 是数字请求，用于请求包含您的组织信息以及唯一识别码且经过签字的安全服务器证书。

在生成 (CSR) 后，系统会提示您将副本保存到管理站或共享网络上，而用于生成 CSR 的唯一信息存储在 CMC 上。该信息用于以后验证您从证书颁发机构接收的服务器证书。收到证书颁发机构的服务器证书后，必须将其上载到 CMC。

注: 为了使 CMC 能够接受由证书颁发机构返回的服务器证书，新证书中包含的验证信息必须与生成 CSR 时存储在 CMC 上的信息匹配。

小心: 生成新的 CSR 后，它会覆盖 CMC 上任何以前的 CSR。如果在证书颁发机构为其颁发服务器证书之前覆盖未完成的 CSR，则 CMC 将无法接受服务器证书，因为它用于验证该证书的信息已经丢失。生成 CSR 时请务必小心，以免覆盖任何未完成的 CSR。

使用 Web 界面生成新的证书签名请求

要使用 CMC Web 界面生成 CSR，请执行以下操作：

1. 在系统树中，转至**机箱概述**，然后单击**网络** > **SSL**。此时将显示 **SSL 主菜单**。
2. 选择 **生成新的证书签名请求（CSR）**并单击**下一步**。此时将显示**生成证书签名请求（CSR）** 页。
3. 为每个 CSR 属性值键入一个值。
4. 单击**生成**。此时将显示**文件下载**对话框。
5. 将 csr.txt 文件保存到管理站或共享网络。（您也可以在此时打开文件并稍后保存。）您必须稍后将该文件提交到证书颁发机构。

使用 RACADM 生成 CSR

要生成 CSR，请使用 `cfgRacSecurityData` 组中的对象指定值，并使用 `sslcsrgen` 命令生成 CSR。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

上载服务器证书

生成 CSR 后，您可以将签名的 SSL 服务器证书上载到 CMC 固件。CMC 会在证书上载后重设。CMC 仅接受 X509，基于 64 编码的 Web 服务器证书。

小心: 在证书上载过程中，CMC 不可用。

注: 如果上载证书并且尝试立即查看该证书，将显示一条错误消息，指示无法执行所请求的操作。发生该问题的原因在于 Web 服务器正在使用新证书重新启动。在 Web 服务器重新启动后，证书上载成功，您便可以查看该新证书了。上载证书后，可能会延迟一分钟左右后才能查看上载的证书。

注: 自签名证书（使用 CSR 功能生成）只能上载一次。如再次尝试上载此证书将失败，因为在第一次上载证书后将删除私钥。

使用 CMC Web 界面上载服务器证书

要使用 CMC Web 界面上载服务器证书，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**网络** > **SSL**。此时将显示 **SSL 主菜单**。
2 选择**根据生成的 CSR 上载服务器证书**选项，然后单击**下一步**。
3 单击**选择文件**并指定证书文件。
4 单击**应用**。如果证书无效，则会显示一条错误消息。

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

使用 RACADM 上载服务器证书

要上载 SSL 服务器证书，请使用 `sslcertupload` 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

上载 Web 服务器密钥和证书

您可以上载 Web 服务器密钥和 Web 服务器密钥的服务器证书。服务器证书由证书颁发机构 (CA) 颁发。

Web 服务器证书是 SSL 加密过程使用的重要组件。它会向启用 SSL 的客户端验证自身，并允许客户端向服务器验证自身，从而支持两个系统建立加密连接。

注: 要上载 Web 服务器密钥和服务器证书，您必须具有机箱配置管理员权限。

使用 CMC Web 界面上载 Web 服务器密钥和证书

要使用 CMC Web 界面上载 Web 服务器密钥和证书，请执行以下操作：

1 在系统树中，转至**机箱概览**并单击**网络** > **SSL**。此时将显示 **SSL 主菜单**。
2 选择**上载 Web 密钥和证书**选项，然后单击**下一步**。
3 通过单击**选择文件**来指定私钥文件和证书文件。
4 上载两个文件后单击**应用**。如果 Web 服务器密钥和证书不匹配，则会显示一条错误消息。

注: 只有 X509，基于 64 位编码的证书才能被 CMC 接受。不会接受使用 DER 等其他编码方式的证书。上载新的证书，取代您通过 CMC 接收的默认证书。

成功上载证书后，CMC 将重设并暂时不可用。要在重设时避免与其他用户断开连接，通知可能登录到 CMC 的授权用户，并通过查看**网络**选项卡下的**会话**页检查活动的会话。

使用 RACADM 上载 Web 服务器密钥和证书

要将客户端的 SSL 密钥上载到 iDRAC，请键入以下命令：

```
racadm sslkeyupload -t <type> -f <filename>
```

有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

查看服务器证书

您可以查看当前在 CMC 中使用的 SSL 服务器证书。

使用 Web 界面查看服务器证书

在 CMC Web 界面中，转至**机箱概览** > **网络** > **SSL**。选择**查看服务器证书**并单击**下一步**。**查看服务器证书**页面将显示当前正在使用的 SSL 服务器证书。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 服务器证书将通用名称显示为机架名称加域名（如果有）。如果没有域名，则仅显示机架名称。

使用 RACADM 查看服务器证书

要查看 SSL 服务器证书，请使用 `sslcertview` 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

机箱配置配置文件

利用机箱配置配置文件功能，可以使用存储在网络共享或本地管理站中的机箱配置配置文件来配置机箱，也可以还原机箱配置。

要在 CMC Web 界面中访问**机箱配置配置文件**，请在系统树中转至**机箱概览**，然后单击 **设置** > **配置文件**。随即会显示**机箱配置配置文件**页面。

您可以使用机箱配置配置文件功能执行以下任务：

- 使用本地管理站上的机箱配置配置文件来配置机箱，以执行初始配置。
- 将当前机箱配置设置保存至网络共享中的 XML 文件或本地管理站。
- 还原机箱配置。
- 将本地管理站上的机箱配置文件（XML 文件）导入网络共享。
- 将网络共享中的机箱配置文件（XML 文件）导出至本地管理站。
- 应用、编辑、删除或导出网络共享中存储的配置文件副本。

保存机箱配置

您可以将当前机箱配置保存至网络共享或本地管理站中的 XML 文件。机箱配置包含所有可通过 CMC Web 界面和 RACADM 命令修改的机箱属性。您也可以使用保存的 XML 文件来在同一机箱上还原配置或配置其他机箱。

注: 服务器和 iDRAC 设置不能通过机箱设置进行保存或还原。

要保存当前机箱配置，请执行以下任务：

1 转至**机箱配置配置文件**页面。在**保存并备份** > **保存当前配置**部分的**配置文件名称**字段中，输入配置文件的名称。

注: 在保存当前机箱配置时，支持标准 ASCII 扩展字符集。但不支持下列特殊字符：
“、.、*、>、<、\、/、:、和 |

2 从**配置文件类型**选项中选择下面的一种配置文件类型：

- **替换** - 包含整个 CMC 配置的属性，但用户密码和服务标签等只写属性除外。此类配置文件用作备份配置文件，用于还原包括标识信息（例如 IP 地址）在内的完整机箱配置。
- **克隆** - 包含所有**替换**类型的配置文件属性。出于安全原因，不包含 MAC 地址、IP 地址等标识属性。此类配置文件用于克隆新机箱。

3 从**配置文件位置**下拉菜单中选择下面的一个位置用于存储配置文件：
- **本地** - 将配置文件保存至本地管理站。
- **网络共享** - 将配置文件保存在某个共享位置。

4 单击**保存**以将配置文件保存至选定位置。

操作完成后，会显示 `Operation Successful` 消息：

注: 要查看已保存至 XML 文件的设置，请在存储的配置文件部分选择保存的配置文件，然后单击查看配置文件列中的查看。

还原机箱配置配置文件

通过导入本地管理站或保存机箱配置所在的网络共享中的备份文件（.xml 或 .bak），可以还原机箱配置。机箱配置包含通过 CMC Web 界面、RACADM 命令和设置可用的所有属性。

要还原机箱配置，请执行以下任务：

1 转至**机箱配置配置文件**页面。在**还原配置** > **还原机箱配置**部分，单击**浏览**选择备份文件，以导入所保存的机箱配置。

2 单击**还原配置**，将加密的备份文件 (.bak) 或存储的 .xml 配置文件上载至 CMC。

成功执行还原操作后，CMC Web 界面将返回登录页面。

注: 如果较早版本 CMC 的备份文件 (.bak) 加载到启用了 FIPS 的最新版本 CMC 上，请重新配置所有 16 个 CMC 本地用户密码。但是，第一个用户的密码重设为 “calvin"。

注: 从 CMC 导入机箱配置文件时，其不支持 FIPS 功能，导入到启用了 FIPS 的 CMC 时，FIPS 在 CMC 中保持启用状态。

注: 如果在机箱配置配置文件中更改 FIPS 模式，则 `DefaultCredentialMitigation` 将被已启用。

查看存储的机箱配置配置文件

要查看存储在网络共享中的机箱配置配置文件，请转至**机箱配置配置文件**页面。在**机箱配置配置文件** > **存储的配置文件**部分，选择相应的配置文件并单击**查看配置文件**列中的**查看**。随即会显示**查看设置**页面。有关所显示设置的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

导入机箱配置配置文件

您可以将存储在网络共享中的机箱配置导入本地管理站。

要将存储在远程文件共享中的配置文件导入 CMC，请执行以下任务：

1 转至**机箱配置配置文件** 页面。在**机箱配置配置文件** > **存储的配置文件**部分，单击**导入配置文件**。

随即会显示**导入配置文件**部分。

2 单击**浏览**从所需的位置访问该配置文件，然后单击**导入配置文件**。

注: 您可以使用 RACADM 导入机箱配置配置文件。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge FX2/FX2s 命令行参考指南）。

应用机箱配置配置文件

如果机箱配置配置文件存储在网络共享中并且可用，则可对机箱应用该机箱配置。要启动机箱配置操作，可以对机箱应用存储的配置文件。

要对机箱应用配置文件，请执行以下任务：

1 转至**机箱配置配置文件**页面。在**存储的配置文件**部分，选择要应用的存储配置文件。

2 单击**应用配置文件**。

随后会显示一条警告消息，指示应用新的配置文件会覆盖当前设置并重新引导所选服务器。系统会提示您确认是否继续该操作。

3 单击**确定**，对机箱应用该配置文件。

导出机箱配置配置文件

您可以将保存在网络共享中的机箱配置配置文件导出至管理站上的指定路径。

要导出存储的配置文件，请执行以下任务：

1 转至**机箱配置配置文件**页面。在**机箱配置配置文件** > **存储的配置文件** 部分中，选择所需的配置文件，然后单击**导出配置文件副本**。

随即会显示**文件下载**消息，询问您打开还是保存文件。

2 单击**保存**或**打开**以导出配置文件至所需的位置。

编辑机箱配置配置文件

您可以编辑机箱的机箱配置配置文件名称。

要编辑机箱配置配置文件名称，请执行以下任务：

1 转至**机箱配置配置文件**页面。在**机箱配置配置文件** > **存储的配置文件**部分中，选择所需的配置文件，然后单击**编辑配置文件**。

随后将显示**编辑配置文件**窗口。

2 在**配置文件名称**字段输入所需的配置文件名称，然后单击**编辑配置文件**。

随后将显示 `Operation Successful` 消息。

3 单击**确定**。

删除机箱配置配置文件

您可以删除存储在网络共享中的机箱配置配置文件。

要删除机箱配置配置文件，请执行以下任务：

1 转至**机箱配置配置文件**页面。在**机箱配置配置文件** > **存储的配置文件**部分，选择所需的配置文件，然后单击**删除配置文件**。

随即显示一条警告消息，指示删除配置文件操作将永久删除选定的配置文件。

2 单击**确定**以删除所选的配置文件。

使用机箱配置配置文件通过 RACADM 配置多个 CMC

通过使用机箱配置配置文件，可以将机箱配置配置文件作为 XML 文件导出，并将其导入另一个机箱。

使用 RACADM get 命令执行导出操作和使用 set 命令执行导入操作。您可以将机箱配置文件（XML 文件）从 CMC 导出到网络共享或本地管理站，以及将机箱配置文件（XML 文件）从网络共享或从本地管理站导入。

注: 默认情况下，导出作为克隆类型来完成。您可以使用 ——clone 来获取 XML 文件形式的克隆类型配置文件。

针对网络共享的导入和导出操作可通过本地 RACADM 和远程 RACADM 完成。针对本地管理站的导入和导出操作只能通过远程 RACADM 界面完成。

导出机箱配置配置文件

您可以使用 get 命令，将机箱配置配置文件导出至网络共享。

1 要使用 get 命令来将机箱配置配置文件作为 clone.xml 文件导出至 CIFS 网络共享，请键入以下命令：

```
racadm get –f clone.xml –t xml –l //xx.xx.xx.xx/PATH –u USERNAME –p PASSWORDCMC
```

2 要使用 get 命令来将机箱配置配置文件作为 clone.xml 文件导出至 NFS 网络共享，请键入以下命令：

```
racadm get –f clone.xml –t xml –l xx.xx.xx.xx:/PATH
```

您可以通过远程 RACADM 界面将机箱配置配置文件导出至网络共享。

1 要将机箱配置配置文件作为 clone.xml 文件导出至 CIFS 网络共享，请键入以下命令：

```
racadm –r xx.xx.xx.xx –u USERNAMECMC –p PASSWORDCMC get –f clone.xml –t xml –l //xx.xx.xx.xx/
PATH –u USERNAME –p PASSWORD
```

2 要将机箱配置配置文件作为 clone.xml 文件导出至 NFS 网络共享，请键入以下命令：

```
racadm –r xx.xx.xx.xx –u USERNAMECMC –p PASSWORDCMC get –f clone.xml –t xml –l xx.xx.xx.xx:/
PATH
```

您可以通过远程 RACADM 界面将机箱配置配置文件导出至本地管理站。

1 要将机箱配置配置文件作为 clone.xml 文件导出，请键入以下命令:

```
racadm –r xx.xx.xx.xx –u USERNAMECMC –p PASSWORDCMC get –f clone.xml –t xml
```

导入机箱配置配置文件

您可以使用 set 命令，将机箱配置配置文件从网络共享导入另一个机箱。

1 要从 CIFS 网络共享导入机箱配置配置文件，请键入以下命令：

```
racadm set –f clone.xml –t xml –l //xx.xx.xx.xx/PATH –u USERNAME –p PASSWORDCMC
```

2 要从 NFS 网络共享导入机箱配置配置文件，请键入以下命令：

```
racadm set –f clone.xml –t xml –l xx.xx.xx.xx:/PATH
```

您可以通过远程 RACADM 界面从网络共享导入机箱配置配置文件。

1 要从 CIFS 网络共享导入机箱配置配置文件，请键入以下命令：

```
racadm –r xx.xx.xx.xx –u USERNAMECMC –p PASSWORDCMC  set –f clone.xml –t xml –l //
xx.xx.xx.xx/PATH –u USERNAME –p PASSWORD
```

2 要从 NFS 网络共享导入机箱配置配置文件，请键入以下命令：

```
racadm –r xx.xx.xx.xx –u USERNAMECMC –p PASSWORDCMC set –f clone.xml –t xml –l xx.xx.xx.xx:/
PATH
```

您可以通过远程 RACADM 界面从本地管理站导入机箱配置配置文件。

1 要将机箱配置配置文件作为 clone.xml 文件导出，请键入以下命令:

```
racadm –r xx.xx.xx.xx –u USERNAMECMC –p PASSWORDCMC set –f clone.xml –t xml
```

分析规则

您可以手动编辑所导出的机箱配置配置文件的 XML 文件属性。

XML 文件包含以下属性：

- System Configuration，这是父节点。
- component，这是主要的子节点。
- **属性**，其中包含名称和值。您可以编辑这些字段。例如，您可以编辑 `Asset Tag` 值，如下所示：

```
<Attribute Name="ChassisInfo.1#AssetTag">xxxxxx</Attribute>
```

xml 文件示例如下：

```
<SystemConfiguration Model="PowerEdge M1000e
"ServiceTag="NOBLE13"
TimeStamp="Tue Apr  7 14:17:48 2015" ExportMode="2">
<!--Export type is Replace-->
<!--Exported configuration may contain commented attributes. Attributes may be commented due to
dependency,
destructive nature, preserving server identity or for security reasons.-->
<Component FQDD="CMC.Integrated.1">
<Attribute Name="ChassisInfo.1#AssetTag">00000</Attribute>
<Attribute Name="ChassisLocation.1#DataCenterName"></Attribute>
<Attribute Name="ChassisLocation.1#AisleName"></Attribute>
<Attribute Name="ChassisLocation.1#RackName"></Attribute>
....
</Component>
</SystemConfiguration>
```

使用配置文件通过 RACADM 配置多个 CMC

您可以使用配置文件来通过 RACADM 配置一个或多个具有相同属性的 CMC 。

使用组 ID 和对象 ID 查询特定 CMC 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 CMC，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 CMC 信息（如静态 IP 地址），在将文件导出到其他 CMC 之前必须修改这些信息。

1 使用 RACADM 查询包含所需配置的目标 CMC。

   注: 生成的配置文件为 myfile.cfg。您可以重命名该文件。.cfg 文件不包含用户密码。在将 .cfg 文件上载到新 CMC 后，您必须重新添加所有密码。

2 打开连接至 CMC 的远程 RACADM 会话，登录，并键入：

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

   注: 仅远程 RACADM 界面支持使用 `getconfig -f` 将 CMC 配置重定向至文件。

3 使用简单文本编辑器（可选）修改配置文件。配置文件中的任何特殊格式字符都可能损坏 RACADM 数据库。

4 使用新创建的配置文件修改目标 CMC。在命令提示符处，键入：

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

5 重设已配置的目标 RAC。在命令提示符处键入：

```
racadm reset
```

`getconfig -f myfile.cfg` 子命令（步骤 1）为活动 CMC 请求 CMC 配置并生成 myfile.cfg 文件。如果需要，可以将文件重命名或将其保存到另一个位置。

可以使用 getconfig 命令来执行以下操作：

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

`config` 子命令将信息载入其他 CMC。Server Administrator 使用 `config` 命令同步用户和密码数据库。

相关链接

创建 CMC 配置文件

创建 CMC 配置文件

CMC 配置文件 **<文件名>.cfg** 与 `racadm config -f <filename>.cfg` 命令配合使用以创建简单文本文件。该命令允许您构建配置文件（类似于 .ini 文件）并从该文件中配置 CMC。

用户可以使用任意文件名，并且文件不一定要使用 .cfg 扩展名（尽管本小节中的指定值采用了此扩展名）。

注: 有关 `getconfig` 子命令的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）*。

RACADM 会在 .cfg 文件首次加载到 CMC 上时对其进行解析，以验证是否存在有效的组和对象名称，并且是否符合简单语法规则。系统将使用检测到的错误所在的行号标记该错误，并且显示一条说明问题原因的消息。系统将解析整个文件以检查其正确性并显示所有错误。如果在 .cfg 文件中发现错误，写命令将不会传输到 CMC。必须先更正所有错误才能使配置生效。

要在创建配置文件之前检查错误，请使用 `-c` 选项和 `config` 子命令。使用 `-c` 选项时，`config` 仅验证语法而不会写入 CMC。

创建 .cfg 文件时，请遵循以下原则：

- 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。
  解析器将从 CMC 读入该组的所有索引。配置 CMC 时，该组内的任何对象都会被修改。如果修改的对象代表新的索引，则系统将在配置过程中在 CMC 上创建该索引。
- 无法在 .cfg 文件中指定所需的索引。
  可以创建和删除索引。经过一段时间后，组中可能会出现使用和未使用的索引碎片。如果索引存在，它将被修改。如果索引不存在，则使用第一个可用的索引。

  此方法允许用户在不需要在所有管理的 CMC 之间实现精确索引匹配时灵活添加索引条目。新用户将被添加至第一个可用的索引。在一个 CMC 上正确解析和运行的 .cfg 文件可能无法在另一个 CMC 上正确运行，如果所有索引都已满，您必须添加新用户。
- 使用 `racresetcfg` 子命令可以为两个 CMC 配置相同的属性。
  使用 `racresetcfg` 子命令可将 CMC 重设为原始默认值，然后运行 `racadm config -f <filename>.cfg` 命令。确保 .cfg 文件中包含所有所需的对象、用户、索引和其他参数。有关对象和组的完整列表，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）*。

  小心: 使用 `racresetcfg` 子命令可将数据库和 CMC 网络接口设置重设为原始默认设置并删除所有用户和用户配置。尽管根用户可用，其他用户的设置也会重设为默认设置。
- 如果您键入 `racadm getconfig -f <filename> .cfg`，则命令将针对当前的 CMC 配置构建 .cfg 文件。此配置文件可以用作示例，作为您的唯一 .cfg 文件的起点。

相关链接

分析规则

分析规则

- 以井号 (#) 开始的行将视为注释。
  注释行必须从第一列开始。所有其他列中的“#”字符均只被视为 # 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。您可能想要生成 .cfg（从 `racadm getconfig -f <filename> .cfg` 命令），然后对另一个 CMC 执行 `racadm config -f <filename> .cfg` 命令，无需添加转义字符。

  例如：

```
#
# This is a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString= <Modem init # not
a comment>
```

- 所有的组条目必须位于左方括号和右方括号（[和]）之内。
  指示组名称的起始 [字符必须在第一列中。此组名称必须在该组中的任何对象之前指定。没有关联组名称的对象将导致错误。配置数据分为三组，如 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）*的“数据库属性”一章中所定义。以下示例显示了组名称、对象以及对象的属性值：

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object name}
{object value}
```

- 所有参数都指定为“对象=值”对，在对象、= 或值之间不留空格。值后包含的空格将忽略。值字符串内的空格保持不变。“=”右侧的任何字符（例如，第二个 =、#、[、] 和等）保留原样。这些字符都是有效的调制解调器对话脚本字符。

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object value}
```

- .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 <filename>.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 <groupname>  -o <anchored object> -i <index 1-16> <unique anchor name>`

- 无法从 .cfg 文件中删除索引组的行。如果使用文本编辑器删除该行，则 RACADM 会在解析配置文件时停止并警告错误。
  用户必须使用以下命令手动移除索引对象：

```
racadm config -g <groupname>  -o <objectname> -i <index 1-16> ""
```

  注: NULL 字符串（两个 " 字符表示）指示 CMC 删除指定组的索引。

  要查看索引组的内容，请运行以下命令：

```
racadm getconfig -g <groupname> -i <index 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= <USER_NAME>
```

- 使用远程 RACADM 将配置组捕获到文件中时，如果组内的关键属性没有设置，则配置组不会保存为配置文件的一部分。要复制其他 CMC 上的这些配置组，请先设置关键属性，然后再执行 `getconfig -f` 命令。或者，运行 `getconfig -f` 命令后，将缺失的属性手动输入配置文件中。这对于所有 racadm 索引组均是如此。
  这是表现出此行为的索引组及其相应的关键属性列表：

  - cfgUserAdmin - cfgUserAdminUserName
  - cfgEmailAlert - cfgEmailAlertAddress
  - cfgTraps - cfgTrapsAlertDestIPAddr

- cfgStandardSchema - cfgSSADRoleGroupName
- cfgServerInfo - cfgServerBmcMacAddress

修改 CMC IP 地址

在配置文件中修改 CMC IP 地址时，移除所有不必要的 `<variable> = <value>` 条目。只有实际变量组标签带有 [和] 的保持不变，包括与 IP 地址更改有关的两个 `<variable> = <value>` 条目。

示例：

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=192.168.2.110
cfgNicGateway=192.168.2.1
```

此文件更新如下：

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=192.168.1.143
# comment, the rest of this line is ignored
cfgNicGateway=192.168.1.1
```

命令 `racadm config -f <myfile>.cfg` 分析文件并通过行号标识任何错误。正确的文件会更新适当的条目。此外，您可以使用与上一示例相同的 `getconfig` 命令确认更新。

使用该文件下载公司范围内的更改或使用命令 `racadm getconfig -f <myfile> .cfg` 通过网络配置新系统。

注: ***Anchor*** **是保留字，不应在 .cfg 文件中使用。**

查看和终止 CMC 会话

您可以查看当前登录到 iDRAC 的用户数以及终止用户会话。

注: 要终止会话，必须具备机箱配置管理员权限。

使用 Web 界面查看和终止 CMC 会话

要使用 Web 界面查看或终止会话，请执行以下操作：

1 在系统树中，转至**机箱概述**并单击**网络 > 会话**。

会话页会显示会话 ID、用户名、IP 地址以及会话类型。有关这些属性的更多信息，请参阅 *CMC Online Help*（iDRAC7 联机帮助）。

2 要终止会话，请对会话单击**终止**。

使用 RACADM 查看和终止 CMC 会话

您必须具有管理员权限才能使用 RACADM 终止 CMC 会话。

要查看当前用户会话，请使用 `getssninfo` 命令。

要终止用户会话，请使用 `closessn` 命令。

有关这些命令的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

为风扇配置增强散热模式

增强散热模式 (ECM) 功能使用第三代 M1000e 风扇提供额外的散热支持。只有在九个风扇插槽都插入了新的第三代 M1000e 风扇后方可使用增强散热模式 (ECM)。新的第三代 M1000e 风扇具有以下特性：

- 启用 ECM 功能时，与前几代 M1000e 风扇相比，可为安装的刀片服务器提供卓越的散热效果。
- 禁用 ECM 功能时，可在相同的功耗下提供与前几代 M1000e 风扇同等的散热效果。

建议将 ECM 模式用于：

- 具有较高散热设计功耗 (TDP) 处理器的刀片服务器配置。
- 性能至关重要的工作负载。
- 在入口温度超过 30°C [86°F] 的环境中部署的系统。

,

注: 在增强散热模式 (ECM) 下，与目前这代 M1000e 机箱风扇相比新一代风扇具有出众的散热效果。并非始终需要该增强散热效果，其代价是声响更大（系统的声响最高会增加 40%）以及系统风扇功耗更高。您可根据机箱需要的散热程度来启用或禁用 ECM 功能。

默认情况下，会禁用机箱上的 ECM 功能。ECM 的启用和禁用操作记录在 CMC 日志中。在 CMC 故障转移以及机箱交流电源关闭再打开后，会保留 ECM 模式状态。

您可以使用 CMC Web 界面或 RACADM CLI 界面启用或禁用 ECM 功能。

使用 Web 界面为风扇配置增强散热模式

要使用 CMC Web 界面为风扇配置增强散热模式 (ECM)：

1 在系统树中，转至**机箱概览**，然后单击**风扇** > **设置**。

显示**高级风扇配置**页面。

注: 如果禁用了 ECM，并且机箱中的所有风扇不支持 ECM，则不会显示用于访问高级风扇配置页面的设置选项卡。

2 在**风扇配置**部分，从**增强散热模式**下拉菜单选择**启用**或**禁用**。

有关字段描述的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注:

增强散热模式选项仅在以下情况下可供选择：

- 机箱中所有风扇都支持 ECM 功能。在这种情况下，您可以启用或禁用 ECM 模式。
- 已经启用 ECM，并且风扇配置更改为“混合模式”或者所有风扇不支持 ECM 模式。在这种情况下，可禁用 ECM 模式，但是在机箱中的所有风扇都支持 ECM 后才可再次启用该模式。

注: 在以下情况下，增强散热模式和应用选项会显示为灰色：

- 已经禁用 ECM 模式，并且风扇配置由不支持的风扇及支持的风扇组成。信息部分显示一条信息，列出不兼容 ECM 功能的风扇。
- 已经禁用 ECM 模式，并且启用了**最大节能模式**(MPCM)。信息部分显示一条消息，说明启用 MPCM 时不支持 ECM。

有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

如果禁用了 ECM 功能，则在机箱中的所有风扇支持 ECM 后方可再次启用功能。

3 单击**应用**。

在成功启用或禁用 ECM 选项之后，会显示操作成功消息。在以下情况下，不会启用 ECM 模式：

- 无法获得所支持风扇所需的额外功率。
- 机箱中有任何风扇不支持 ECM。
- MPCM 已启用。

显示带有 ECM 未启用原因的警报消息。

注: 如果在启用了 ECM 时尝试启用 MPCM，ECM 模式会更改为已启用，但是处于不支持状态。

使用 RACADM 为风扇配置增强散热模式

要为风扇启用并配置“增强散热模式”，可使用 **cfgThermal** 组下的以下 RACADM 对象：

```
cfgThermalEnhancedCoolingMode
```

例如，要启用 ECM 模式，可使用：

```
racadm config –g cfgThermal –o cfgThermalEnhancedCoolingMode 1
```

如果出现错误，则会显示一条错误消息。“增强散热模式”选项的默认值为已禁用 (0)。在发出 **racresetcfg** 命令时，该值设置为已禁用 (0)。

要查看当前的 ECM 模式，可使用：

```
racadm getconfig –g cfgThermal
```

要查看 ECM 模式的当前状态，可使用：

```
racadm getfanreqinfo
[Enhanced Cooling Mode]
Enhanced Cooling Mode(ECM) Status  = Disabled
```

有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

7

配置服务器

您可以在服务器上执行以下操作：

- 配置插槽名称
- 配置 iDRAC 网络设置
- 配置 iDRAC VLAN 标签设置
- 设置第一引导设备
- 配置服务器 FlexAddress
- 配置远程文件共享
- 使用服务器克隆配置 BIOS 设置

主题：

配置插槽名称

插槽名称用于标识单个服务器。选择插槽名称时，以下规则适用：

- 名称仅能包含**最多 24** 个非扩展的 ASCII 字符（ASCII 代码 32 到 126）。此外，名称中还允许使用标准字符及特殊字符。
- 插槽名称必须在机箱内唯一。不能有两个插槽具有相同的名称。
- 字符串不区分大小写。`Server-1`, `server-1`, and `SERVER-1` 是相同的名称。
- 插槽名称不得使用以下字符串开头：
  - `Switch-`
  - `Fan-`
  - `PS-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- 可以使用字符串 `Server-1` 到 `Server-16`，但仅供相应的插槽使用。例如，`Server-3` 是插槽 3 的有效名称，但不是插槽 4 的有效名称。请注意，`Server-03` 可以是任何插槽的有效名称。

注: 要更改插槽名称，您必须具备机箱配置管理员权限。

Web 界面中的插槽名称设置仅保存在 CMC 中。如果从机箱中卸下服务器，则服务器的插槽名称设置将不再保留。

插槽名称设置不会扩展到可选的 iKVM。插槽名称信息通过 iKVM FRU 提供。

CMC Web 界面中的插槽名称设置始终覆盖 iDRAC 界面中对显示名称所做的任何更改。

要使用 CMC Web 界面编辑插槽名称，请执行以下操作：

1 在系统树中，转至**机箱概览** > **服务器概览**，然后单击**设置** > **插槽名称**。此时将显示**插槽名称**页。
2 在**插槽名称**字段中，编辑插槽名称。对您要重命名的每个插槽重复此步骤。
3 要使用服务器的主机名作为插槽名称，请选择**使用主机名作为插槽名称**选项。利用此选项可将静态插槽名称替换为服务器的主机名（或系统名称）（如可用）。

注: 要使用使用主机名作为插槽名称，必须在服务器上安装 OMSA 代理程序。有关 OMSA 代理程序的详细信息，请参阅 *Dell OpenManage Server Administrator User's Guide*（Dell OpenManage Server Administrator 用户指南）。

4 要使用 iDRAC DNS 名称作为插槽名称，请选择**使用 iDRAC DNS 名称作为插槽名称**选项。利用此选项可将静态插槽名称替换为相应的 iDRAC DNS 名称（如可用）。如果 iDRAC DNS 名称不可用，将显示默认插槽名称或编辑过的插槽名称。

注: 要选择使用 iDRAC DNS 名称作为插槽名称选项，必须具备机箱配置管理员权限。

5 单击**应用**保存设置。
6 要将默认插槽名称（**SLOT-01** 到 **SLOT-16**，依服务器的插槽位置而定）还原到服务器，请单击**还原默认值**。

配置 iDRAC 网络设置

您可以配置安装或新插入的服务器的 iDRAC 网络配置设置。用户可配置一个或多个安装的 iDRAC 设备。用户也可为今后要安装的服务器配置默认的 iDRAC 网络配置设置和根密码；这些默认设置是 iDRAC 快速部署设置。

有关 iDRAC 的更多信息，请参阅 **dell.com/support/manuals** 上的 *iDRAC User's Guide*（iDRAC 用户指南）。

相关链接

配置 iDRAC QuickDeploy 网络设置
修改单个服务器 iDRAC 的 iDRAC 网络设置
使用 RACADM 修改 iDRAC 网络设置

配置 iDRAC QuickDeploy 网络设置

使用“QuickDeploy 设置”可为新插入的服务器配置网络设置。在启用 QuickDeploy 后，QuickDeploy 设置会在安装服务器时应用于该服务器。

要使用 CMC Web 界面启用和设置 iDRAC QuickDeploy 设置，请执行以下操作：

1 在系统树中，转至**服务器概览**，然后单击**设置** > **iDRAC**。此时将显示**部署 iDRAC** 页面。
2 在 **QuickDeploy 设置**部分，指定下表所述设置。

表. 18: QuickDeploy 设置

设置	说明
启用 QuickDeploy	启用/禁用将此页上配置的 iDRAC 设置自动应用到新插入服务器的**快速部署**功能；必须在本地 LCD 面板上确认自动配置。 **注: 如果选中插入服务器时设置 iDRAC Root 密码框，则包括 root 用户密码。**

设置	说明
	默认情况下，此选项被禁用。
插入服务器时的操作	从列表中选择以下选项之一： • **无操作** — 插入服务器时不执行任何操作。 • **仅限 QuickDeploy** — 选择此选项以在将新服务器插入机箱中时应用 iDRAC 网络设置。指定的自动部署设置用于配置新的 iDRAC，如果选择了"更改 Root 密码"，则还包括配置 root 用户密码。 • **仅限服务器配置文件** — 选择此选项以在将新服务器插入机箱时应用分配的服务器配置文件。 • **Quick Deploy 和服务器配置文件** — 选择此选项以在将新服务器插入机箱时，首先应用 iDRAC 网络设置，然后应用分配的服务器配置文件。
插入服务器时设置 iDRAC Root 密码	指定插入服务器时服务器的 iDRAC root 密码是否必须改为 **iDRAC Root 密码**字段中提供的值。
iDRAC Root 密码	选中**插入服务器时设置 iDRAC Root 密码**和 **启用 QuickDeploy** 选项后，此密码值会在服务器插入机箱时分配到服务器的 iDRAC root 用户密码。此密码包括 1 至 20 个可打印（含空格）字符。
确认 iDRAC root 密码	验证输入 **iDRAC Root 密码**字段的密码。
启用 iDRAC LAN	启用或禁用 iDRAC LAN 信道。默认情况下，此选项被禁用。
启用 iDRAC IPv4	启用或禁用 iDRAC 上的 IPv4。默认情况下，此选项被启用。
启用 LAN 上 iDRAC IPMI	为机箱中存在的每个 iDRAC 启用/禁用 IPMI over LAN 信道。默认情况下，此选项被禁用。
启用 iDRAC DHCP	为机箱中存在的每个 iDRAC 启用或禁用 DHCP。如果此选项被启用，则字段 **QuickDeploy IP**、**QuickDeploy 子网掩码**和 **QuickDeploy 网关**都被禁用，并且无法修改，因为系统使用 DHCP 自动为每个 iDRAC 分配这些设置。默认情况下，此选项被禁用。
保留的 QuickDeploy IP 地址	可让您选择要为机箱中的 iDRAC 保留的静态 IPv4 地址的数量。从**起始 iDRAC IPv4 地址（插槽 1）**开始的 IPv4 地址会被视为保留的地址，并且假定其不会用于相同网络中的其他地方。对于插入了没有保留静态 IPv4 地址的插槽中的服务器而言，无法使用 QuickDeploy 功能。以下为各类服务器可保留的最大静态 IP 地址数目： • 四分之一高服务器为 32 个 IP 地址。 • 半高服务器为 16 个 IP 地址。 • 全高服务器为 8 个 IP 地址。 **注: 请注意下列事项：** • 少于服务器类型所需最小值的 IP 地址数目值将显示为灰色。 • 如果选择少于所保留 IP 地址数目默认值的选项，将会显示一条错误消息，警告如果减少 IP 地址数目会阻碍快速地将配置文件部署至更高容量的服务器。 • 将把警告消息记录在 CMC 硬件日志 (SEL) 中，并生成 SNMP 警报。 • 如果在启用了 QuickDeploy 功能后，更高容量的服务器插入较低的位置，则不会在 LCD 面板上显示快速部署提示。要在 LCD 面板上再次看到更高容量服务器的快速部署选项，可将 IP 地址值更改为默认值并重置更高容量服务器。 **注:**
起始 iDRAC IPv4 地址（插槽 1）	指定机柜插槽 1 中服务器 iDRAC 的静态 IP 地址。从插槽 1 的静态 IP 地址开始，针对每个插槽，每个后续 iDRAC 的 IP 地址增加 1。如果 IP 地址加插槽编号大于子网掩码，会显示一个错误消息。 **注: 子网掩码和网关不像 IP 地址那样增加。**

设置	说明
	例如，如果起始 IP 地址为 192.168.0.250 并且子网掩码为 255.255.0.0，则插槽 15 的 QuickDeploy IP 地址为 192.168.0.265。如果您尝试设置起始 IP 地址、保留 IP 地址和子网掩码值字段，使得组合可能生成子网之外的 IP 地址，则在您单击**保存 QuickDeploy 设置**或**使用 QuickDeploy 设置自动填充**时，会显示错误消息 QuickDeploy IP address range is not fully within QuickDeploy Subnet（QuickDeploy IP 地址范围未完全处于 QuickDeploy 子网中）。例如，如果起始 IP 为 192.168.1.245，保留 IP 地址为 16 并且子网掩码为 255.255.255.0，为 11 以外的插槽生成的 IP 地址将均在子网以外。因此，尝试为 QuickDeploy 设置进行该组合的设置会生成错误消息。
iDRAC IPv4 子网掩码	指定被分配到所有新插入服务器的 QuickDeploy 子网掩码。
iDRAC IPv4 网关	指定被分配到机箱中所有 iDRAC 的 QuickDeploy 默认网关。
启用 iDRAC IPv6	为机箱中支持 IPv6 的每个 iDRAC 启用 IPv6 寻址。
启用 iDRAC IPv6 自动配置	使 iDRAC 能够从 DHCPv6 服务器获取 IPv6 设置（地址和前缀长度），还启用无状态地址自动配置。默认情况下，此选项被启用。
iDRAC IPv6 网关	指定要分配给 iDRAC 的默认 IPv6 网关。默认值是“::”。
iDRAC IPv6 前缀长度	指定要为 iDRAC 上的 IPv6 地址分配的前缀长度。默认值是 64。
使用 CMC DNS 设置	在刀片服务器插入机箱中时，启用已传播至 iDRAC 的 CMC DNS 服务器设置（IPv4 和 IPv6）。

3 单击**保存 QuickDeploy 设置**以保存设置。如果您对 iDRAC 网络设置进行了更改，请单击**应用 iDRAC 网络设置**将设置部署到 iDRAC。

QuickDeploy 功能仅在启用并且服务器插入机箱中时执行。如果启用**插入服务器时设置 iDRAC Root 密码**和**启用 QuickDeploy**，则在 LCD 界面中会提示用户允许或不允许更改密码。如果网络配置设置不同于当前的 iDRAC 设置，则提示用户接受或不接受更改。

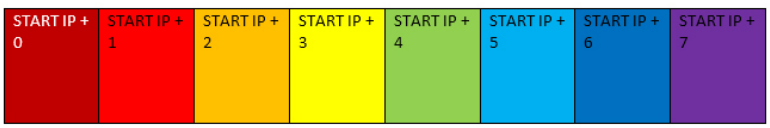
注: 如果存在 LAN 或 IPMI over LAN 差异，则提示用户接受 QuickDeploy IP 地址设置。如果差异是 DHCP 设置，则提示用户接受 DHCP QuickDeploy 设置。

要将 QuickDeploy 设置复制到 **iDRAC 网络设置**部分，请单击**使用 QuickDeploy 设置自动填充**。QuickDeploy 网络配置设置将复制到 **iDRAC 网络配置设置**表中的相应字段。

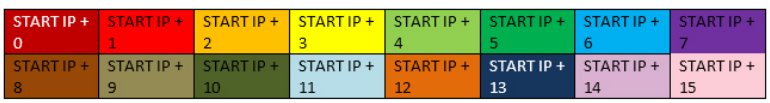
注: 对 QuickDeploy 字段的更改立即生效，但对一个或多个 iDRAC 服务器网络配置设置的更改可能需要几分钟才能从 CMC 传送到 iDRAC。单击刷新太快时，可能只显示一个或多个 iDRAC 服务器的部分正确数据。

服务器的 QuickDeploy IP 地址分配

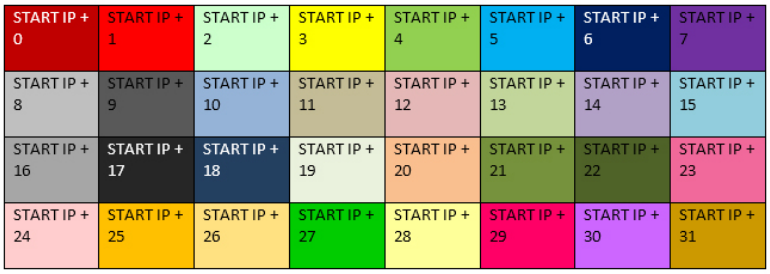
此图显示了 M1000e 机箱中有 8 个全高服务器的情况下对服务器的 QuickDeploy IP 地址分配：



下图显示了 M1000e 机箱中有 16 个半高服务器的情况下对服务器的 QuickDeploy IP 地址分配：



下图显示了 M1000e 机箱中有 32 个四分之一高服务器的情况下对服务器的 QuickDeploy IP 地址分配：



使用 RACADM 配置保留的 QuickDeploy IP 地址

要使用 RACADM 修改为机箱上服务器分配的静态 IP 地址的数量，可使用以下命令：

```
racadm deploy –q -n <num>
```

其中 <num> 是 IP 地址数目，8、16 或 32。

要通过 RACADM 查看为机箱中的服务器保留的 IP 地址数和**使用 CMC DNS 设置**的当前设置，请使用以下命令：

```
racadm deploy –q
```

要通过 RACADM 修改**使用 CMC DNS 设置**选项以便为机箱中的服务器启用快速部署，请使用以下命令：

```
racadm deploy -q -e <enable/disable>
```

有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

修改单个服务器 iDRAC 的 iDRAC 网络设置

使用此表，您可以为每台已安装的服务器配置 iDRAC 网络配置设置。每个字段显示的初始值是从 iDRAC 读取的当前值。

要使用 CMC Web 界面修改 iDRAC 网络设置，请执行以下操作：

1. 在系统树中，转至**服务器概述**，然后单击**设置** > **iDRAC**。此时将显示**部署 iDRAC** 页。**iDRAC 网络设置**部分列出所有安装的服务器的 iDRAC IPv4 和 IPv6 网络配置设置。
2. 根据需要修改服务器的 iDRAC 网络设置。

   注: 您必须选择启用 LAN 选项指定 IPv4 或 IPv6 设置。有关这些字段的信息，请参阅 CMC Online Help（CMC 联机帮助）。
3. 要将设置部署到 iDRAC，请单击**应用 iDRAC 网络设置**。如果您对快速部署设置进行了更改，也会保存这些设置。

   iDRAC 网络设置表反映未来的网络配置设置；为安装服务器显示的值不一定与当前安装的 iDRAC 网络配置设置相同。更改后单击**刷新**更新 **iDRAC 部署**页和每个安装的 iDRAC 网络配置设置。

   注: 对“快速部署”字段的更改立即生效，但对一个或多个 iDRAC 服务器网络配置设置的更改可能需要几分钟才能从 CMC 传送到 iDRAC。单击刷新太快时，可能只显示一台或多台 iDRAC 服务器的部分正确数据。

使用 RACADM 修改 iDRAC 网络设置

RACADM `config` 或 `getconfig` 命令支持以下配置组的 `-m <module>` 选项：

- `cfgLanNetworking`

- `cfgIpv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

有关属性默认值和范围的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

配置 iDRAC VLAN 标签设置

VLAN 用于允许多个虚拟 LAN 共同存在于同一物理网络电缆上，并允许出于安全性或负载管理的目的而分离网络通信流。启用 VLAN 功能时，系统将给每个网络信息包分配 VLAN 标签。VLAN 标签是机箱属性。即使拆下了组件，机箱仍然有这些标签。

注: 仅当 iDRAC 处于专用模式时，使用 CMC 的 VLAN ID 配置才会应用到 iDRAC。如果 iDRAC 处于共享的 LOM 模式，则在 iDRAC 中所做的 VLAN ID 更改不会显示在 CMC GUI 中。

使用 Web 界面配置 iDRAC VLAN 标签设置

要使用 CMC Web 界面配置服务器的 VLAN，请执行以下操作：

1 转至以下任一页：
   - 在系统树中，转至**机箱概览**，单击**网络** > **VLAN**。
   - 在系统树中，转至 **机箱概览** > **服务器概览**，并单击**网络** > **VLAN**。此时将显示 **VLAN 标签设置**页面。
2 在 **iDRAC** 部分，为服务器启用 VLAN，设置优先级并输入 ID。有关这些字段的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用**保存设置。

使用 RACADM 配置 iDRAC VLAN 标签设置

- 用以下命令指定特定服务器的 VLAN ID 和优先级：

  ```
  racadm setniccfg -m server-<n> -v <VLAN id> <VLAN priority>
  ```

  `<n>` 的有效值是 1-16。

  `<VLAN>` 的有效值是 1-4000 和 4021-4094。默认值是 1。

  `<VLAN priority>` 的有效值是 0-7。默认值是 0。

  例如：

  ```
  racadm setniccfg -m server-1 -v 1 7
  ```

  例如：

- 若要删除服务器 VLAN，请禁用指定服务器网络的 VLAN 功能：

  ```
  racadm setniccfg -m server-<n> -v
  ```

  `<n>` 的有效值是 1-16。

  例如：

  ```
  racadm setniccfg -m server-1 -v
  ```

设置第一引导设备

可以为每台服务器指定 CMC 第一引导设备。该设备可能不是服务器的实际第一引导设备，甚至不代表该服务器中的设备，相反它代表会被 CMC 发送到服务器的设备，以及用作该服务器的第一引导设备。

可以设置默认引导设备和设置一次性引导设备，以便引导映像来执行任务，如运行诊断程序或重新安装操作系统。

您可以仅为下一次引导或所有后续重新引导设置第一引导设备。根据此选择，您可以设置服务器的第一引导设备。系统将在下一次以及后续重新引导时从所选设备引导始终作为 BIOS 引导顺序中的第一个引导设备，直到从 CMC Web 界面或从 BIOS 引导顺序再次进行更改。

注: CMC Web 界面中的第一引导设备设置会覆盖系统 BIOS 引导设置。

所指定的引导设备必须存在且包含可引导的介质。

可以将以下设备设置为第一引导设备。

表. 19: ：引导设备

引导设备	说明
PXE	从网络接口卡上的预引导执行环境 (PXE) 协议引导。
硬盘驱动器	从服务器的硬盘驱动器引导。
本地 CD/DVD	从服务器上的 CD/DVD 驱动器引导。
虚拟软盘	从虚拟软盘驱动器引导。软盘驱动器（或软盘映像）位于管理网络中另一台计算机上，并且使用 iDRAC GUI 控制台 Viewer 连接。
虚拟 CD/DVD	从虚拟 CD/DVD 驱动器或 CD/DVD ISO 映像引导。光盘驱动器或 ISO 映像文件位于管理网络中另一台计算机或另一个磁盘上，并且使用 iDRAC GUI 控制台查看器连接。
iSCSI	从 Internet 小型计算机系统接口 (iSCSI) 设备引导。 **注: 此选项直到 Dell 第 11 代 PowerEdge 服务器才受支持。**
本地 SD 卡	从本地 SD（安全数字）卡引导 - 仅适用于支持 iDRAC 系统的服务器。
软盘	从本地软盘驱动器中的软盘引导。
RFS	从远程文件共享 (RFS) 映像引导。映像文件使用 iDRAC GUI 控制台查看器连接。
UEFI 设备路径	从统一可扩展固件接口 (UEFI) 服务器上的设备路径引导。

相关链接

使用 CMC Web 界面为多个服务器设置第一引导设备
使用 CMC Web 界面为单个服务器设置第一引导设备
使用 RACADM 设置第一引导设备

使用 CMC Web 界面为多个服务器设置第一引导设备

注: 要设置服务器的第一引导设备，必须具备服务器管理员权限或机箱配置管理员权限和 iDRAC 登录权限。

要使用 CMC Web 界面为多个服务器设置第一引导设备，请执行以下操作：

1 在系统树中，转至**服务器概述**，然后单击 **设置** > **第一引导设备**。此时将显示服务器的列表。
2 在**第一引导设备**列中，从下拉菜单中选择要用于每个服务器的引导设备。
3 如果要服务器每次引导时都从选定的设备引导，请清除该服务器对应的**引导一次**选项。如果要服务器仅在下一个引导周期从选定的设备引导，请选中该服务器对应的**引导一次**选项。
4 单击**应用**保存设置。

使用 CMC Web 界面为单个服务器设置第一引导设备

要为服务器设置第一引导设备，必须具备**服务器管理员**权限或**机箱配置管理员**权限和 **iDRAC 登录**权限。

要使用 CMC Web 界面为单个服务器设置第一引导设备，请执行以下操作：

1 在系统中，转至**服务器概述**，然后单击要设置第一引导设备的服务器。
2 转至**设置** > **第一引导设备**。此时将显示**第一引导设备**页。
3 在**第一引导设备**下拉菜单中，选择要用于每个服务器的引导设备。
4 如果希望服务器每次引导时都从选定的设备引导，请清除该服务器对应的**引导一次**选项。如果要服务器仅在下一引导周期从选定的设备引导，请选中该服务器对应的**引导一次**选项。
5 单击**应用**保存设置。

使用 RACADM 设置第一引导设备

要设置第一引导设备，请使用 `cfgServerFirstBootDevice` 对象。

要启用为设备引导一次，请使用 `cfgServerBootOnce` 对象。

有关这些对象的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

配置服务器 FlexAddress

有关为服务器配置 FlexAddress 的信息，请参阅为服务器级插槽配置 FlexAddress。

配置远程文件共享

远程虚拟介质文件共享功能通过 CMC 将网络上共享驱动器中的文件映射到一个或多个服务器，以部署或更新操作系统。连接后，可以像访问本地服务器文件那样访问远程文件。支持两种类型的介质：软盘驱动器和 CD/DVD 驱动器。

要执行远程文件共享操作（连接、断开连接或部署），您必须具有**机箱配置管理员**或**服务器管理员**权限。

要使用 CMC Web 界面配置远程文件共享：

1 在系统树中，转至**服务器概览**，然后单击**设置** > **远程文件共享**。
此时会显示**部署远程文件共享**页面。

> **注: 如果任何存在于插槽中的服务器是第 12 代或更高，且没有正确的许可证，则会显示一条消息，指示所需的许可证缺失或已过期。您需要获取适当的许可证并重试，或者联系您的服务提供商以了解更多详情。**

2 指定所需设置。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**连接**以连接到远程文件共享。要连接远程文件共享，您必须提供路径、用户名和密码。操作成功后将允许访问介质。

单击**断开连接**可断开之前连接的远程文件共享。

单击**部署**可部署介质设备。

注: 保存所有工作文件，然后再选择部署选项以部署介质设备，因为此操作会引起服务器重启。

此操作涉及以下步骤：

- 连接远程文件共享。
- 将文件选择为服务器的第一引导设备。
- 重新启动服务器。
- 如果服务器已关机，则接通服务器电源。

使用服务器配置复制功能配置配置文件设置

服务器配置复制功能允许您将指定服务器的所有配置文件设置应用于一个或多个服务器。可以复制的配置文件设置是那些可以修改并且可以跨服务器复制的配置文件设置。将显示并且可以复制服务器的以下三个配置文件组：

- BIOS - 该组仅包含服务器的 BIOS 设置。这些配置文件是从 CMC 4.3 之前的版本生成的。
- BIOS 和引导 - 该组包含服务器的 BIOS 和引导设置。这些配置文件是从以下版本生成的：
  - CMC 版本 4.3
  - CMC 版本 4.45 和第 11 代服务器
  - CMC 版本 4.45 和第 12 代服务器（具有 1.1 版之前版本的 Lifecycle Controller 2）
- 所有设置 - 此版本包含服务器以及该服务器上组件的所有设置。这些配置文件是从以下版本生成的：
  - CMC 版本 4.45 和第 12 代服务器（具有 iDRAC 和 Lifecycle Controller 2 版本 1.1 或更高版本）。
  - CMC 版本 5.0 和第 13 代服务器（具有 iDRAC 和 Lifecycle Controller 2.00.00.00 或更高版本）

服务器配置复制功能支持 iDRAC 和更新的服务器。较早几代 RAC 服务器将在主页上列出，但会显示为灰色，并且不能使用此功能。

要使用服务器配置复制功能，请执行以下操作：

- iDRAC 必须至少具有要求的最低版本。iDRAC 服务器最低需要版本 3.2 和 1.00.00。
- 服务器必须接通电源。

服务器版本和配置文件兼容性：

- iDRAC 及 Lifecycle Controller 2 版本 1.1 和更高的版本可以接受任何版本的配置文件。
- iDRAC 版本 3.2 和 1.0 仅接受“BIOS”或“BIOS 和引导”配置文件。
- 保存服务器上的 iDRAC with Lifecycle Controller 2 版本 1.1 或更高版本的配置文件将生成“所有设置”配置文件。保存从服务器上的 iDRAC 版本 3.2 和 iDRAC 及 Lifecycle Controller 2 版本 1.0 将生成 “BIOS 和引导”配置文件。

可执行以下操作：

- 查看服务器上或来自所保存配置文件的配置文件设置。
- 保存来自服务器的配置文件。
- 将配置文件应用于其他服务器。
- 从 Management Station 或远程文件共享导入存储的配置文件。
- 编辑配置文件的名称和说明。
- 将存储的配置文件导出到 Management Station 或远程文件共享。
- 删除已存储的配置文件。
- 使用**快速部署**选项将所选配置文件部署到目标设备。
- 显示最近的服务器配置文件任务的日志活动。

相关链接

访问服务器配置文件页面
添加或保存配置文件
应用配置文件
查看配置文件设置
查看配置文件日志
完成状态、日志查看和故障排除

访问服务器配置文件页面

您可以使用**服务器配置文件**页面添加和管理服务器配置文件，并将其应用于一个或多个服务器。

要使用 CMC Web 界面访问**服务器配置文件**页面，请在系统树中，转至**机箱概览** > **服务器概览**。单击**设置** > **配置文件**。系统将显示**服务器配置文件**页面。

相关链接

添加或保存配置文件
应用配置文件
查看配置文件设置
查看配置文件日志
完成状态、日志查看和故障排除

添加或保存配置文件

复制服务器属性之前，首先将属性捕捉到存储的配置文件中。创建存储的配置文件，并为每个配置文件提供名称和说明（可选）。在 CMC 非易失性扩展存储介质上最多可保存 16 个存储的配置文件。

注: 如果远程共享可用，则可以使用 CMC 扩展存储和远程共享存储多达 100 个配置文件。有关更多信息，请参阅使用 CMC Web 界面配置网络共享。

卸下或禁用非易失性扩展存储介质会阻止对存储的配置文件进行访问，并禁用服务器配置功能。

要添加或保存配置文件：

1 转至**服务器配置文件**页面。在**服务器配置文件**部分，选择您要从其设置生成配置文件的服务器，然后单击**保存配置文件**。
随即将显示**保存配置文件**部分。

2 选择**扩展存储**或**网络共享**作为配置文件的保存位置。

注: 只有在挂载了网络共享并且网络共享可访问的情况下，才会启用网络共享选项，并在存储的配置文件部分显示其详细信息。如未连接网络共享，应为机箱配置网络共享。要配置网络共享，请在存储的配置文件部分中单击编辑 。有关更多信息，请参阅使用 CMC Web 界面配置网络共享。

3 在**配置文件名称**和**说明**字段中，请输入配置文件名称和说明（可选），然后单击**保存配置文件**。

注: 保存服务器配置文件时支持标准 ASCII 扩展字符集。但不支持以下特殊字符：
)、 “、.、*、>、<、\、/、:、|。#。? 和 ,

CMC 与 Lifecycle Controller 通信以获取可用的服务器配置文件设置，并将其存储为指定的配置文件。

进度指示器表示“保存”操作正在进行中。完成该操作后，会显示一条“操作成功”的消息。

注: 收集设置的进程在后台运行。因此，新配置文件可能需要过一段时间才能显示。如果不显示新配置文件，请检查配置文件日志中是否存在错误。

相关链接

访问服务器配置文件页面

应用配置文件

仅当服务器配置文件存储在 CMC 上的非易失性介质上或存储在远程共享中时，才能执行服务器克隆。要启动服务器配置操作，可将存储的配置文件应用于一台或多台服务器。

注: 如果服务器不支持 Lifecycle Controller 或机箱的电源已关闭，则不能将配置文件应用于服务器。

要将配置文件应用到一个或多个服务器，请执行以下操作：

1 转至**服务器配置文件**页面。在**保存和应用配置文件**部分，选择您要应用所选配置文件的一个或多个服务器。
选择配置文件下拉菜单此时被启用。

注: 选择配置文件 下拉菜单中将显示所有可用的配置文件（按类型排序），包括位于远程共享和 SD 卡上的配置文件。

2 从**选择配置文件**下拉菜单中，选择您要应用的配置文件。
应用配置文件选项此时被启用。

3 单击**应用配置文件**。
会显示警告消息指示将应用新的服务器配置文件覆盖当前设置并重新引导所选服务器。系统会提示您确认是否要继续该操作。

注: 要在服务器上执行服务器配置操作，必须为服务器启用 CSIOR 选项。如果已禁用 CSIOR 选项，会显示警告消息指示服务器未启用 CSIOR。要完成服务器配置复制操作，请确保在服务器上启用 CSIOR 选项。

4 单击**确定**以应用配置文件到选定的服务器。
服务器将应用所选配置文件，并且可能立即重新引导（如果需要）。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

相关链接

访问服务器配置文件页面

导入配置文件

您可以将存储在管理站上的服务器配置文件导入到 CMC。
要将远程文件共享上的存储配置文件导入到 CMC，请执行以下操作：

1 在**服务器配置文件**页面上的**存储的配置文件**部分，单击**导入配置文件**。
将显示**导入服务器配置文件**部分。

2 单击**浏览**从所需的位置访问该配置文件，然后单击**导入配置文件**。
有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

导出配置文件

您可以将存储在 CMC 非易失性介质（SD 卡）上的服务器配置文件导出至管理工作站上的指定路径。
要导出存储的配置文件：

1 转至**服务器配置文件**页面。在**存储的配置文件**部分中，选择所需的配置文件，然后单击**导出配置文件副本**。
随即会显示**文件下载**消息，询问您打开还是保存文件。

2 单击**保存**或**打开**以导出配置文件至所需的位置。

注：如果源配置文件位于 SD 卡上，导出配置文件时会显示一条警告消息，其说明将丢失。按确定以继续导出配置文件。

此时将显示一条消息，提示您选择文件的目标：

- 本地或网络共享（如果源文件位于 SD 卡上）。

注：仅当网络共享已安装且可访问时，网络共享选项启用并在存储的配置文件部分中显示详细信息。如果网络共享未连接，则配置机箱的网络共享。要配置网络共享，请单击存储的配置文件部分中的编辑。有关更多信息，请参阅使用 CMC Web 界面配置网络共享。

- 本地或 SD 卡（如果源文件位于网络共享上）。

有关更多信息，请参阅*联机帮助*。

3 根据显示的选项，选择**本地**、**扩展存储**或**网络共享**作为目标位置。
   - 如果选择**本地**，将显示一个对话框，使您可以将配置文件保存到本地目录。
   - 如果选择**扩展存储**或**网络共享**，则显示**保存配置文件**对话框。
4 单击**保存配置文件**将配置文件保存到选定的位置。

注：CMC Web 界面捕获正常服务器配置文件（服务器的快照），该配置文件可用于目标系统上的复制。但是，RAID 和标识属性等配置不会传播到新服务器。有关 RAID 配置的备用导出模式和标识属性的详细信息，请参阅 DellTechCenter.com 上的白皮书 *Server Cloning with Server Configuration Profiles*（使用服务器配置文件克隆服务器）。

编辑配置文件

您可以编辑存储在 CMC 非易失性介质（SD 卡）上的服务器配置文件的说明或存储在远程共享上的服务器配置文件的名称。

要编辑存储配置文件：

1 转至**服务器配置文件**页面。在**存储的配置文件**部分，选择所需的配置文件，然后单击**编辑配置文件**。
   随即将显示**编辑服务器配置文件 — <配置文件名称>** 部分。
2 按照要求编辑服务器配置文件的名称和说明，然后单击**保存配置文件**。
   有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

删除配置文件

您可以删除存储在 CMC 非易失性介质（SD 卡）或网络共享中的服务器配置文件。

要删除存储的配置文件：

1 在**服务器配置文件**页面上的**存储的配置文件**部分，选择所需的配置文件，然后单击**删除配置文件**。
   随即显示一条警告消息，指示删除配置文件操作将永久删除选定的配置文件。
2 单击**确定**以删除所选的配置文件。
   有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看配置文件设置

要查看选定服务器的**配置文件设置**，请转至**服务器配置文件**页面。在**服务器配置文件**部分，单击所需服务器的**服务器配置文件**列中的**查看**。将显示**查看设置**页面。

有关所显示设置的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注：只有启用重新启动时收集系统资源清册 (CSIOR) 选项，CMC 服务器克隆应用程序才会检索并显示特定服务器的设置。

要在下列服务器上启用 CSIOR，请执行以下操作：

- 第 11 代服务器 - 在重新引导服务器后，从 **Ctrl-E** 设置中，选择**系统服务**，启用 **CSIOR** 并保存更改。
- 第 12 代服务器 - 在重新引导服务器后，从 **F2** 设置中，选择 **iDRAC 设置** > **Lifecycle Controller**，启用 **CSIOR** 并保存更改。
- 第 13 代服务器 - 在重新引导服务器后，当出现提示时，按 **F10** 键以访问 Lifecycle Controller。选择**硬件配置** > **硬件资源清册**转至**硬件资源清册**页面。在**硬件资源清册**页面上，单击**重新启动时收集系统资源清册**。

相关链接

访问服务器配置文件页面

查看存储的配置文件设置

要查看存储在 CMC 非易失性介质（SD 卡）或远程共享上的服务器配置文件的设置，请转至**服务器配置文件**页面。在**存储的配置文件**部分，在所需配置文件的**查看配置文件**列中单击**查看**。随即会显示**查看设置**页面。有关所显示设置的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

查看配置文件日志

要查看配置文件日志，请在**服务器配置文件**页面中，查看**最近配置文件日志**部分。该部分将列出最近 10 个服务器配置操作直接生成的配置文件日志条目。每个日志条目均显示有服务器配置操作的严重性、提交时间和日期，以及配置日志消息描述。日志条目还可以从 RAC 日志中查看。要查看其他可用条目，请单击**转至配置文件日志**。随即将显示**配置文件日志**页面。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 有关 Dell PowerEdge M 4110 服务器中操作和关联日志报告的信息，请参阅 EqualLogic 说明文件。

完成状态、日志查看和故障排除

要检查应用的服务器配置文件的完成状态，请执行以下操作：

1 在**服务器配置文件**页面中，记下**最近配置文件日志**部分中已提交作业的作业 ID (JID)。
2 在系统树中，转至**服务器概览**并单击**故障排除** > **Lifecycle Controller 作业**。在**作业**表中查看相同的 JID。
3 单击**查看日志**链接，可查看特定服务器的 iDRAC Lifecycle Controller 的 Lclogview 结果。
显示的完成或失败的结果与特定服务器的 iDRAC Lifecycle Controller 日志中显示的信息相似。

配置文件的 Quick Deploy

使用快速部署功能可将存储的配置文件分配给服务器插槽。插入该插槽中的任何支持服务器克隆的服务器均将使用分配的配置文件进行配置。只有在**部署 iDRAC** 页面中的**插入服务器时的操作**选项设置为 **服务器配置文件**选项或**快速部署和服务器配置文件**选项时，方可执行快速部署操作。选择这些选项中的一个，便可在新服务器插入机箱中时应用分配的服务器配置文件。要转至**部署 iDRAC** 页面，请选择 **服务器概览** > **设置** > **iDRAC**。可以部署的配置文件存储在 SD 卡或远程共享中。要设置配置文件以进行快速部署，则必须有**机箱管理员**权限。

注:

将服务器配置文件分配给插槽

在**服务器配置文件**页面上可以将服务器配置文件分配给插槽。要将配置文件分配给机箱插槽，请执行以下操作：

1 在**服务器配置文件**页面中，单击**用于 QuickDeploy 的配置文件**部分。

在**分配配置文件**列中包含的选择框中，将显示插槽的当前配置文件分配。

注: 只有在“部署 iDRAC”页面中的“插入服务器时的操作”选项设置为 服务器配置文件选项或快速部署和服务器配置文件选项时，方可执行快速部署操作。选择这些选项中的一个，便可在新服务器插入机箱中时应用分配的服务器配置文件。

2 从下拉菜单中，选择要分配给所需插槽的配置文件。您可选择一个配置文件以应用于多个插槽。

3 单击**分配配置文件**。

配置文件将被分配给选定的插槽

注:

- 没有分配任何配置文件的插槽将在选择框中以“未选择配置文件”来指示。
- 要从一个或多个插槽移除配置文件分配，请选择插槽，然后单击**移除分配**，随即会显示一条消息，警告您从一个或多个插槽移除配置文件的操作也将移除插入该插槽中的任何服务器的配置文件中的配置设置（如启用了**快速部署配置文件**功能）。单击**确定**将移除配置文件分配。
- 要移除插糟的所有配置文件分配，在下拉菜单中，选中**未选择配置文件**。

注: 当使用快速部署配置文件功能为服务器部署配置文件时，应用的过程和结果将记录在配置文件日志中。

注:

- 如果分配的配置文件位于网络共享中，并且在服务器插入该插槽时此网络共享不可访问，LCD 将显示一条消息，指示所分配的配置文件对于插槽 <X> 不可用。
- 只有在挂载了网络共享并且网络共享可访问的情况下，才会启用**网络共享**选项，并在**存储的配置文件**部分显示其详细信息。如未连接网络共享，应为机箱配置网络共享。要配置网络共享，请在**存储的配置文件**部分中单击**编辑** 。有关更多信息，请参阅使用 CMC Web 界面配置网络共享。

引导标识配置文件

要访问 CMC Web 界面中的**引导标识配置文件**页面，请在系统树中转至**机箱概览** > **服务器概览**。单击**设置** > **配置文件**。随即会显示**服务器配置文件**页面。在**服务器配置文件**页面中，单击**引导标识配置文件**。

引导标识配置文件包含 NIC 或 FC 设置，在从 SAN 目标设备和唯一的虚拟 MAC 和 WWN 引导服务器时需要用到引导标识配置文件。由于此类文件可用于通过 CIFS 或 NFS 共享的多个机箱，所以您可以远程将机箱中故障服务器的标识快速移动至相同或不同机箱中的备用服务器，这样便可以使用故障服务器的操作系统和应用程序进行引导。这项功能的主要优点在于使用了唯一的且在所有机箱之间共享的虚拟 MAC 地址池。

在服务器停止工作时，借助这项功能可以联机管理服务器操作，无需物理干预。您可以使用引导标识配置文件功能来执行以下任务：

- 初始设置
  - 创建虚拟 MAC 地址范围。要创建 MAC 地址，您必须具有机箱配置管理员和服务器管理员权限。
  - 保存引导标识配置文件模板，编辑各服务器使用的 SAN 引导参数并将这些参数包含进来，即可对网络共享中的引导标识配置文件进行自定义。
  - 在应用引导标识配置文件前，先对使用初始配置的服务器进行准备。
  - 对每台服务器应用引导标识配置文件，并从 SAN 进行引导。
- 配置一台或多台备用待机服务器以实现快速恢复。
  - 在应用引导标识配置文件前，先对使用初始配置的待机服务器进行准备。
- 通过执行以下任务，可在新服务器中使用故障服务器的工作负载：
  - 清除故障服务器的引导标识，以避免服务器恢复时复制 MAC 地址。
  - 将故障服务器的引导标识应用于备用待机服务器。

- 使用新引导标识设置引导服务器以实现快速恢复工作负载。

保存引导标识配置文件

您可以将引导标识配置文件保存到 CMC 网络共享。可存储的配置文件数取决于 MAC 地址的可用性。有关更多信息，请参阅 *Configuring Network Share Using CMC Web Interface*（使用 CMC Web 界面配置网络共享）。

对于 Emulex 光纤信道 (FC) 卡，Option ROM 中的**启用/禁用从 SAN 引导**属性默认为禁用。请启用 Option ROM 中的此属性，并将引导标识配置文件应用于要从 SAN 引导的服务器。

要保存配置文件，请执行以下任务：

1 转至**服务器配置文件**页面。在**引导标识配置文件**部分，选择具有所需设置（此设置用于生成配置文件）的服务器，并从 **FQDD** 下拉菜单中选择 FQDD。

2 单击**保存标识**。随即会显示**保存标识**部分。

注: 只有在启用了网络共享选项且该选项可访问时，才会保存引导标识，详细信息显示在存储的配置文件部分。如果网络共享未连接，请为机箱配置网络共享。要配置网络共享，单击存储的配置文件部分中的编辑。有关更多信息，请参阅 *Configuring Network Share Using CMC Web Interface*（使用 CMC Web 界面配置网络共享）。

3 在**基本配置文件名称**和**配置文件数**字段中，输入配置文件名称和要保存的配置文件数。

注: 保存引导标识配置文件时，支持标准 ASCII 扩展字符集。但不支持以下特殊字符：

)、 “、.、*、>、<、\、/、:、|、#、? 和 ,

4 从**虚拟 MAC 地址**下拉列表中选择基本配置文件的 MAC 地址，然后单击**保存配置文件**。

创建的模板数基于您指定的配置文件数。CMC 将与 Lifecycle Controller 通信，以获取可用的服务器配置文件设置，并将其作为已命名的配置文件存储。命名文件的格式为 - <base profile name>_<profile number>_<MAC address>。 例如：FC630_01_0E0000000000。

进度指示器指示保存操作正在进行。操作完成后，会显示**操作成功**消息。

注: 收集设置的过程在后台进行。因此，新配置文件可能需要过一段时间才能显示。如果不显示新配置文件，请检查配置文件日志中是否存在错误。

应用引导标识配置文件

如果引导标识配置文件作为网络共享中的存储配置文件提供，您可以应用引导标识配置文件设置。要启动引导标识配置操作，您可以将存储的配置文件应用到一个服务器。

注: 如果服务器不支持 Lifecycle Controller 或机箱的电源已关闭，则不能将配置文件应用于服务器。

要对服务器应用配置文件，请执行以下任务：

1 转至 **Server Profiles（服务器配置文件）**页面。在 **Boot Identity Profiles（引导标识配置文件）**部分，选择要在其中应用所选配置文件的服务器。

选择配置文件下拉菜单此时被启用。

注: 选择配置文件下拉菜单中显示了网络共享中所有可用的配置文件，这些配置文件按类型排序。

2 从**选择配置文件**下拉菜单中，选择您要应用的配置文件。

应用标识选项将处于启用状态。

3 单击**应用标识**。

屏幕上会显示一条警告消息，指示应用新标识会覆盖当前设置并重新引导所选服务器。系统会提示您确认是否继续执行此操作。

注: 要在服务器上执行服务器配置复制操作，必须为服务器启用 CSIOR 选项。如果已禁用 CSIOR 选项，会显示警告消息指示服务器未启用 CSIOR。要完成服务器配置复制操作，请在服务器上启用 CSIOR 选项。

4 单击**确定**以对选定的服务器应用该引导标识配置文件。

所选的配置文件应用到服务器，并且服务器立即重新引导。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 您一次只可以将引导标识配置文件应用到服务器中的一个 NIC FQDD 分区。要为另一台服务器中的 NIC FQDD 分区应用相同的引导标识配置文件，您必须从第一次应用了它的服务器上予以清除。

清除引导标识配置文件

在对备用服务器应用新的引导标识配置文件前，可以使用 CMC Web 界面中的**清除标识**选项，来清除所选服务器的现有引导标识配置。

要清除引导标识配置文件：

1 转至**服务器配置文件**页面。在**引导标识配置文件**部分，选择要清除引导标识配置文件的服务器。

注: 只有选定了服务器且对所选服务器应用了引导标识配置文件时，此选项才处于启用状态。

2 单击**清除标识**。

3 单击**确定**，清除所选服务器的引导标识配置文件。

清除操作将禁用 IO 标识和服务器的持久性策略。完成清除操作后，服务器电源关闭。

查看存储的引导标识配置文件

要查看存储在网络共享中的引导标识配置文件，请转至**服务器配置文件**页面。在**引导标识配置文件** > **存储的配置文件**部分，选择相应的配置文件并在**查看配置文件**列中单击**查看**。随即会显示**查看设置**页面。有关所显示设置的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

导入引导标识配置文件

您可以将存储在管理站上的引导标识配置文件导入网络共享。

要将存储的配置文件从管理站导入到网络共享，请执行以下任务：

1 转至**服务器配置文件**页面。在**引导标识配置文件** > **存储的配置文件**部分，单击**导入配置文件**。

随即会显示**导入配置文件**部分。

2 单击**浏览**从所需的位置访问该配置文件，然后单击**导入配置文件**。

有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

导出引导标识配置文件

您可以将保存在网络共享上的引导标识配置文件导出至管理站上的指定路径。

要导出存储的配置文件，请执行以下任务：

1 转至**服务器配置文件**页面。在**引导标识配置文件存储的配置文件**部分，选择所需的配置文件，然后单击**导出配置文件**。

随即会显示**文件下载**消息，询问您打开还是保存文件。

2 单击**保存**或**打开**以导出配置文件至所需的位置。

删除引导标识配置文件

您可以删除存储在网络共享中的引导标识配置文件。
要删除存储的配置文件，请执行以下任务：

1 转至**服务器配置文件**页面。在**引导标识配置文件** > **存储的配置文件**部分中，选择所需的配置文件，然后单击**删除配置文件**。
随即显示一条警告消息，指示删除配置文件操作将永久删除选定的配置文件。
2 单击**确定**以删除所选的配置文件。
有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

管理虚拟 MAC 地址池

通过使用**管理虚拟 MAC 地址池**，可以创建、添加、移除和停用 MAC 地址。在虚拟 MAC 地址池中只能使用单播 MAC 地址。CMC 中允许的 MAC 地址范围如下。

- 02:00:00:00:00:00 - F2:FF:FF:FF:FF:FF
- 06:00:00:00:00:00 - F6:FF:FF:FF:FF:FF
- 0A:00:00:00:00:00 - FA:FF:FF:FF:FF:FF
- 0E:00:00:00:00:00 - FE:FF:FF:FF:FF:FF

要通过 CMC Web 界面查看**管理虚拟 MAC 地址**选项，请在系统树中转至**机箱概览** > **服务器概览**。单击**设置** > **配置文件** > **引导标识配置文件**。随即将显示**管理虚拟 MAC 地址池**部分。

注: 虚拟 MAC 地址在网络共享中的 vmacdb.xml 文件中进行管理。系统会添加隐藏的锁定文件 (..vmacdb.lock) 然后从网络共享中移除此文件，以实现多个机箱引导标识操作序列化。

创建 MAC 池

您可以使用 CMC Web 界面中的**管理虚拟 MAC 地址池**选项，在网络中创建 MAC 池。

注: 只有在网络共享中的 MAC 地址数据库 (vmacdb.xml) 不可用时，才会显示创建 MAC 池部分。在这种情况下，添加 MAC 地址和移除 MAC 地址选项将被禁用。

要创建 MAC 池：

1 转至**服务器配置文件**页面。在**引导标识配置文件** > **管理虚拟 MAC 地址池** 部分。
2 在**起始 MAC 地址**字段中输入 MAC 地址池的起始 MAC 地址。
3 在 **MAC 地址数**字段中输入 MAC 地址数。
4 单击**创建 MAC 池**以创建 MAC 地址池。
在网络共享中创建 MAC 地址数据库后，**管理虚拟 MAC 地址池**将显示该网络共享中存储的 MAC 地址的列表和状态。在此部分可添加 MAC 地址，或从网络共享中移除 MAC 地址。

添加 MAC 地址

您可以使用 CMC Web 界面中的**添加 MAC 地址**选项，将 MAC 地址范围添加至网络共享。

注: 不能添加已存在于 MAC 地址池中的 MAC 地址。将显示一个错误，表示新添加的 MAC 地址已存在于池中。

要将 MAC 地址添加至网络共享：

1 转至 **服务器配置文件** 页面。在**引导标识配置文件** > **管理虚拟 MAC 地址池**部分，单击 **添加 MAC 地址**。
2 在**起始 MAC 地址**字段中输入 MAC 地址池的起始 MAC 地址。
3 在 **MAC 地址数**字段中输入要添加的 MAC 地址数。
有效值为 1 到 3000。
4 单击**确定**以添加 MAC 地址。
有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

移除 MAC 地址

您可以使用 CMC Web 界面中的**移除 MAC 地址**选项，从网络共享中移除 MAC 地址范围。

注: 不能移除节点上的活动 MAC 地址或被分配给某个配置文件的 MAC 地址。

要从网络共享中移除 MAC 地址：

1 转至**服务器配置文件**页面。在**引导标识配置文件** > **管理虚拟 MAC 地址池**部分，单击**移除 MAC 地址**。
2 在**起始 MAC 地址**字段中输入 MAC 地址池的起始 MAC 地址。
3 在 **MAC 地址数**字段中输入要移除的 MAC 地址数。
4 单击**确定**移除 MAC 地址。

停用 MAC 地址

您可以使用 CMC Web 界面中的**停用 MAC 地址**选项，来停用活动的 MAC 地址。

注: 只有在服务器未响应清除标识操作，或者任何服务器都未使用该 MAC 地址时，才能使用停用 MAC 地址选项。

要从网络共享中移除 MAC 地址：

1 转至**服务器配置文件**页面。在**引导标识配置文件** > **管理虚拟 MAC 地址池**部分，选择要停用的活动 MAC 地址。
2 单击**停用 MAC 地址**。

使用单点登录启动 iDRAC

CMC 提供对机箱个别组件（例如服务器）的有限管理。为了全面管理这些单独组件，CMC 为服务器管理控制器 (iDRAC) 基于 web 的界面提供一个启动点。

用户不需要再次登录即可启动 iDRAC Web 界面，因为此功能采用单点登录。单点登录策略如下：

- 拥有服务器管理权限的 CMC 用户会自动使用单点登录登录到 iDRAC。在 iDRAC 站点上，此用户会自动授予管理员权限。即便该用户在 iDRAC 上没有帐户或该帐户没有管理员权限，这也同样适用。
- **没有**服务器管理权限但在 iDRAC 上具有相同帐户的 CMC 用户会使用单点登录自动登录到 iDRAC。在 iDRAC 站点上，此用户将授予为 iDRAC 帐户创建的权限。
- 没有服务器管理权限但在 iDRAC 上具有相同帐户的 CMC 用户无法使用单点登录自动登录到 iDRAC。单击 **Launch iDRAC GUI（启动 iDRAC GUI）**后，此用户导航至 iDRAC 登录页面。

注: 此上下文中，术语“相同帐户”意味着用户拥有 iDRAC 和 CMC 的相同登录名称以及匹配密码。拥有相同登录名称而没有匹配密码的用户被认为其拥有相同帐户。

注: 可能提示用户登录到 iDRAC（请参阅上面的第三单点登录策略公告）。

注: **如果禁用 iDRAC 网络 LAN（LAN 启用 = 否），单点登录不可用。**

如果您单击 **Launch iDRAC GUI（启动 iDRAC GUI）**，可能会显示错误页面：

- 从机箱中卸下了服务器
- iDRAC IP 地址更改
- iDRAC 网络连接出现问题

在 MCM 中，从成员机箱启动 iDRAC Web 界面时，主机箱和成员机箱的用户凭据必须相同。否则，当前成员机箱的会话会终止，并且将会显示成员机箱的登录页面。

相关链接

从服务器状态页启动 iDRAC

从服务器状态页启动 iDRAC

从服务器状态页启动 iDRAC

要从**服务器状态**页启动 iDRAC 管理控制台，请执行以下操作：

1 在系统树中，单击**服务器概览**。此时将显示**服务器状态**页。

2 对您要启动 iDRAC Web 界面的服务器，单击**启动 iDRAC**。

注: **可以通过 IP 地址或 DNS 名称配置 iDRAC 启动。默认方法是使用 IP 地址启动。**

从服务器状态页启动 iDRAC

要为单个服务器启动 iDRAC 管理控制台，请执行以下操作：

1 在系统树中，展开**服务器概述**。所有服务器 (1 – 16) 都显示在扩展**服务器**列表中。

2 单击要启动 iDRAC Web 界面的服务器。此时将显示**服务器状态**页。

3 单击**启动 iDRAC GUI**。此时将显示 iDRAC Web 界面。

从 CMC Web 界面启动远程控制台

您可以在服务器上直接启动键盘-视频-鼠标 (KVM) 会话。远程控制台功能仅在满足以下所有条件时可用：

- 机箱已开机。
- 支持 iDRAC 的服务器。
- 服务器上的 LAN 界面已启用。
- iDRAC 版本为 2.20 或以上。
- 主机系统安装有 JRE（Java Runtime Environment）6 Update 16 或更高版本。
- 主机系统上的浏览器支持弹出窗口（禁用弹出窗口阻止程序）。

还可以从 iDRAC Web 界面启动远程控制台。有关详情，请参阅 *iDRAC User's Guide*（iDRAC 用户指南）。

相关链接

从机箱运行状况页启动远程控制台

从服务器状态页启动远程控制台

从服务器状态页启动远程控制台

从机箱运行状况页启动远程控制台

要从 CMC Web 界面启动远程控制台，请执行以下任一操作：

1 在系统树中，转至**机箱概述**，然后单击**属性** > **运行状况**。此时将显示**机箱运行状况**页。
2 单击机箱图形中的指定服务器。
3 在**快速链接**部分，单击**启动远程控制台**链接以启动远程控制台。

从服务器状态页启动远程控制台

若要为一个服务器启动远程控制台，请执行以下操作：

1 在系统树中，展开**服务器概览**。
展开的服务器列表中将显示所有服务器（1 - 16 个）。
2 单击您要启动远程控制台的服务器。
随即会显示 **Server Status**（服务器状态）页面。
3 单击**启动远程控制台**。

从服务器状态页启动远程控制台

要从**服务器状态**页启动远程控制台，请执行以下操作：

1 在系统树中，转至**服务器概览**，然后单击**属性** > **状态**。
系统将显示**服务器状态**页面。
2 单击**启动远程控制台**，为所需的服务器启动远程控制台。

8

配置 CMC 以发送警报

您可以为管理系统上发生的某些事件设置警报和操作。当系统组件的状态超过预定义的条件时会发生事件。如果事件与事件筛选器匹配，并且您已将此筛选器配置为生成警报（电子邮件警报或 SNMP 陷阱），则系统会将警报发送给一个或多个配置的目标。

要配置 CMC 来发送警报，请执行以下操作：

1 启用全局机箱事件警报。
2 （可选）您可以选择必须生成警报的事件。
3 配置电子邮件警报或 SNMP 陷阱设置。
4 启用增强的机箱日志。

主题：

相关链接

启用或禁用警报
配置警报目标

启用或禁用警报

要将警报发送到配置的目标，您必须启用全局警报选项。该属性将覆盖单个警报设置。

确保将 SNMP 或电子邮件警报目标配置为接收警报。

使用 CMC Web 界面启用或禁用警报

要启用或禁用生成警报，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**警报** > **机箱事件**。
此时将显示**机箱事件**页。
2 在**机箱事件筛选器配置**部分，选择**启用机箱事件警报**选项以启用警报生成。清除此选项即可禁用警报生成。
3 在**机箱事件列表**部分中，执行以下任一操作：
   - 选择必须生成警报的单个事件。
   - 在列标题上选择**启用警报**选项为所有事件生成警报。否则，请清除此选项。
4 单击**应用**保存设置。

使用 RACADM 启用或禁用警报

要启用或禁用生成警报，请使用 `cfgAlertingEnable` RACAM 对象。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（Chassis Management Controller for Dell PowerEdge M1000e RACADM 命令行参考指南）。

配置警报目标

管理站使用简单网络管理协议 (SNMP) 接收 CMC 发来的数据。

您可以配置 IPv4 和 IPv6 警报目标、电子邮件设置和 SMTP 服务器设置，并测试这些设置。

在配置电子邮件警报或 SNMP 陷阱设置之前，请确保您具有**机箱配置管理员**权限。

相关链接

配置 SNMP 陷阱警报目标
配置电子邮件警报设置

配置 SNMP 陷阱警报目标

您可以配置 IPv6 或 IPv4 地址以接收 SNMP 陷阱。

使用 CMC Web 界面配置 SNMP 陷阱警报目标

要使用 CMC Web 界面配置 IPv4 或 IPv6 警报目标设置，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**警报** > **陷阱设置**。
此时将显示**机箱事件警报目标**页。

2 输入以下信息：
- 在**目标**字段中，输入有效的 IP 地址。使用四点 IPv4 格式、标准 IPv6 地址表示法或 FQDN。例如：**123.123.123.123**、**2001:db8:85a3::8a2e:370:7334** 或 **dell.com**。
  选择一种与您的联网技术或基础结构一致的格式。测试陷阱功能无法根据当前网络配置检测不正确的选择（例如，在仅支持 IPv4 的环境中使用 IPv6 目标）。
- 在**团体字符串**字段中，输入目标管理站所属的有效团体字符串。
  该团体字符串与**机箱** > **网络** > **服务**页上的团体字符串不同。SNMP 陷阱团体字符串是 CMC 用于出站陷阱到管理站的团体字符串。**机箱** > **网络** > **服务**页上的团体字符串是管理站用于查询 CMC 上 SNMP 守护程序的团体字符串。

  注: CMC 将默认的 SNMP 团体字符串用于公用。为了确保更高的安全性，建议更改默认团体字符串并设置非空值。
- 在**启用**下，选中目标 IP 对应的复选框以使该 IP 地址接收陷阱。最多可以指定 4 个 IP 地址。

3 单击**应用**保存设置。

4 要测试 IP 地址是否接收 SNMP 陷阱，请单击**测试 SNMP 陷阱**列中的**发送**。
IP 警报目标即配置完成。

使用 RACADM 配置 SNMP 陷阱警报目标

要使用 RACADM 配置 IP 警报目标，请执行以下操作：

1 打开到 CMC 的串行/Telnet/SSH 文本控制台并登录。

注: 仅可同时对 SNMP 和电子邮件警报设置一个筛选器掩码。如果已选定筛选器掩码，则可以跳过步骤 2。

2 启用警报生成：

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3 指定必须生成警报的事件：

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

其中 `<mask value>` 是 0x0 和 0xffffffff 之间的十六进制值。

要获得掩码值，请使用十六进制模式的科学计算器，并使用 <OR> 键加上各个掩码（1、2、4 等）的第二个值。

例如，要为电池探测器警告 (0x2)、电源设备故障 (0x1000) 和 KVM 故障 (0x80000) 启用陷阱警报，键入 2 <OR> 1000 <OR> 200000 并按下 <=> 键。

结果十六进制值为 81002，用于 RACADM 命令的掩码值为 0x81002。

表. 20: 事件陷阱筛选器掩码

事件	筛选器掩码值
风扇探测器故障	0x1
电池探测器警告	0x2
温度探测器警告	0x8
温度探测器故障	0x10
已降级冗余	0x40
冗余丢失	0x80
电源设备警告	0x800
电源设备故障	0x1000
电源设备不存在	0x2000
硬件日志故障	0x4000
硬件日志警告	0x8000
服务器不存在	0x10000
服务器故障	0x20000
KVM 不存在	0x40000
KVM 故障	0x80000
IOM 不存在	0x100000
IOM 故障	0x200000
固件版本不匹配	0x400000
机箱电源阈值错误	0x1000000

事件	筛选器掩码值
SDCARD 不存在	0x2000000
SDCARD 错误	0x4000000
机箱组错误	0x8000000
服务器套管不存在	0x10000000
结构不匹配	0x20000000

4 启用陷阱警告：

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

其中 <index> 值为 1-4。CMC 使用索引编号来区别最多四个用于陷阱警报的可配置目标。可以将目标指定为格式正确的数字地址（IPv6 或 IPv4）或完全限定域名 (FQDN)。

5 指定接收陷阱警报的目标 IP 地址：

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
```

其中 <IP address> 是有效目标，<index> 是在步骤 4 中指定的索引值。

6 指定团体名称：

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i <index>
```

其中 <community name> 是机箱所属的 SNMP 团体，<index> 是在步骤 4 和 5 中指定的索引值。

注: CMC 将默认的 SNMP 团体字符串用于公用。为了确保更高的安全性，建议更改默认团体字符串并设置非空值。

最多可以配置四个接收陷阱警报的目标。要添加更多目标，请重复步骤 2 - 6。

注: 步骤 2 - 6 中的命令会覆盖为指定索引 (1-4) 配置的任何现有设置。要确定某索引以前是否配置过值，请键入：`racadm getconfig -g cfgTraps -i <index>`。如果已配置该索引，则会出现 cfgTrapsAlertDestIPAddr 和 cfgTrapsCommunityName 对象的值。

7 要测试警报目标的事件陷阱，请键入：

```
racadm testtrap -i <index>
```

其中 <index> 是代表想要测试的警报目标的值 1-4。

如果不确定索引编号，请键入：

```
racadm getconfig -g cfgTraps -i <index>
```

配置电子邮件警报设置

当 CMC 检测到机箱事件时（如环境警告或组件故障），可以将它配置为向一个或多个电子邮件地址发送电子邮件警报。

必须配置 SMTP 电子邮件服务器才能接受来自 CMC IP 地址的中继电子邮件，该功能在大多数邮件服务器上通常由于安全问题而被关闭。有关以安全方式执行此操作的说明，请参阅随 SMTP 服务器一起提供的说明文件。

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

注: 电子邮件警报支持 IPv4 和 IPv6 地址。使用 IPv6 时必须指定 DRAC DNS 域名。

如果网络中存在不时释放并更新 IP 地址租用的 SMTP 服务器，并且每次更新后得到的地址不同，则可能会因为指定的 SMTP 服务器 IP 地址发生变化而导致该属性设置在一段时间内无法工作。这种情况下，请使用 DNS 名称。

使用 CMC Web 界面配置电子邮件警报设置

要使用 Web 界面配置电子邮件警报设置，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**警报** > **电子邮件警报设置**。

2 指定 SMTP 电子邮件服务器设置和电子邮件地址以接收警报。有关这些字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

3 单击**应用**保存设置。

4 单击**测试电子邮件**下的**发送**，将测试电子邮件发送到指定的电子邮件警报目标。

使用 RACADM 配置电子邮件警报设置

要使用 RACADM 向电子邮件警报目标发送测试电子邮件，请执行以下操作：

1 打开到 CMC 的串行/Telnet/SSH 文本控制台并登录。

2 启用警报生成：

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

注: 仅可同时对 SNMP 和电子邮件警报设置一个筛选器掩码。如果已经设置了筛选器掩码，则可以跳过步骤 3。

3 指定必须生成警报的事件：

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

其中 `<mask value>` 是介于 0x0 和 0xffffffff 之间的十六进制值，并且必须带有前导 0x 字符。表事件陷阱筛选器掩码为每种事件类型提供筛选器掩码。有关计算想要启用的筛选器掩码十六进制值的说明，请参阅使用 RACADM 配置 SNMP 陷阱警报目标的步骤 3。

4 启用电子邮件警报生成：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
```

其中 `<index>` 值为 1-4。CMC 使用索引编号来区别最多四个可配置目标电子邮件地址。

5 指定接收电子邮件警报的目标电子邮件地址：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i <index>
```

其中 `<email address>` 是有效电子邮件地址，`<index>` 是在步骤 4 中指定的索引值。

6 指定接收电子邮件警报的个人名称：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i <index>
```

其中 `<email name>` 是接收电子邮件警报的个人或组的名称，`<index>` 是在步骤 4 和步骤 5 中指定的索引值。电子邮件名称最多可包含 32 个字母数字字符、连字符、下划线和句点。空格无效。

7 设置 SMTP 主机：

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
```

其中 `host.domain` 是 FQDN。

您最多可以配置四个接收电子邮件警报的目标电子邮件地址。要添加更多电子邮件地址，请重复步骤 2 至步骤 6。

注: 步骤 2-6 中的命令会覆盖为指定索引 (1-4) 配置的任何现有设置。要确定某索引以前是否配置过值，请键入：`racadm getconfig -g cfgEmailAlert -i <index>`。如果已配置该索引，则会出现 cfgEmailAlertAddress 和 cfgEmailAlertEmailName 对象的值。

有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

9

配置用户帐户和权限

您可以设置具有特定权限（*基于角色的授权*）的用户帐户以使用 CMC 管理系统和维护系统安全。默认情况下，使用本地管理员帐户配置 CMC。此默认用户名为 *root* 并且密码为 *calvin*。作为管理员，您可以设置用户帐户从而允许其他用户访问 CMC。

您最多可以设置 16 个本地用户或用户目录服务（例如 Microsoft Active Directory 或 LDAP）以设置附加用户帐户。使用目录服务可提供一个集中的位置来管理授权的用户帐户。

CMC 支持基于角色访问具有一组相关权限的用户。角色可为管理员、操作员、只读用户或无角色。角色定义可用的最大权限。

主题：

相关链接

用户的类型
配置本地用户
配置 Active Directory 用户
配置通用 LDAP 用户
修改根用户管理员帐户设置

用户的类型

用户有两种类型：

- CMC 用户和机箱用户
- iDRAC 用户或服务器用户（自 iDRAC 驻留在服务器上后）

CMC 和 iDRAC 用户可以是本地用户或 Directory 服务用户。

除 CMC 用户拥有**服务器管理员**权限，授予 CMC 用户的权限都不会自动转移给服务器上的同一用户，因为服务器用户是由 CMC 用户单独创建的。换句话说，CMC Active Directory 用户和 iDRAC Active Directory 用户位于 Active Directory 树中两个不同的分支。要创建本地服务器用户，配置用户必须直接登录到服务器。配置用户不能从 CMC 创建服务器用户，反之亦然。该规则是为了保护服务器的安全性和完整性。

表. 21: 用户类型

权限	说明
CMC 登录用户	用户可登录到 CMC 并查看所有 CMC 数据，但不能增加或修改数据或者执行命令。

权限	说明
	用户可能具备其他权限而不具备 CMC 登录用户登录权限。当需要暂时禁止用户登录时，该功能非常有用。当用户的 CMC 登录用户权限恢复后，用户仍可保留所有之前被授予的其他权限。
机箱配置管理员	用户可添加或更改的数据有： • 标识机箱的数据，例如机箱名称和机箱位置。 • 专门分配给机箱的数据，例如 IP 模式（静态或 DHCP）、静态 IP 地址、静态网关以及静态子网掩码。 • 为机箱提供服务的数据，例如日期和时间、固件更新以及 CMC 重设。 • 与机箱相关的数据，例如插槽名称和插槽优先级。尽管这些属性适用于服务器，但是严格地说，它们是与插槽相关的机箱属性而不是服务器本身的属性。因此，不管插槽中有无服务器，都可以添加或更改插槽名称和插槽优先级。 将服务器移至不同机箱中时，它将继承新机箱中所占用插槽的插槽名称和所分配的插槽优先级。之前的插槽名称和优先级将保留在之前的机箱中。 **注: 具有机箱配置管理员权限的 CMC 用户可配置电源设置。但是，需要机箱控制管理员权限才能执行机箱电源操作，包括开机、关机和重启。**
用户配置管理员	用户可以： • 添加新用户。 • 更改用户密码。 • 更改用户权限。 • 启用或禁用用户的登录权限，但保留用户的名称和在数据库中的其他权限。
清除日志管理员	用户可清除硬件日志和 CMC 日志。
机箱控制管理员（电源命令）	具有**机箱电源管理员**权限的 CMC 用户可执行所有电源相关的操作。他们可以控制机箱电源操作，包括开机、关机和重启。 **注: 要配置电源设置，需要机箱配置管理员权限。**
服务器管理员	这是一种全面的权限，赋予 CMC 用户在机箱中的所有服务器上执行任何操作的所有权利。 当具有**服务器管理员**权限的用户发起要在服务器上执行的操作时，CMC 固件将此命令发送给目标服务器，而不会检查此用户在该服务器上的权限。换言之，**服务器管理员**权限可覆盖服务器上缺少的任何管理员权限。 如果没有**服务器管理员**权限，只有在满足以下所有条件时，机箱上创建的用户才能在服务器上执行命令： • 此服务器上存在相同的用户名。 • 此服务器上相同的用户名的密码必须相同。 • 此用户必须具备执行命令的权限。 当不具有**服务器管理员**权限的 CMC 用户发起要在服务器上执行的操作时，CMC 将使用此用户的登录名和密码向目标服务器发送一条命令。如果该服务器上不存在此用户，或者密码不匹配，则用户被拒绝执行此操作。 如果目标服务器上存在此用户且密码匹配，则服务器将使用此用户针对服务器被授予的权限进行响应。根据来自服务器的权限响应，CMC 固件决定此用户是否有权执行操作。 下面列出了服务器管理员针对服务器被授予的权限和可执行的操作。仅当机箱用户不具备机箱上的服务器管理权限时，这些权限才适用。 服务器配置管理员： • 设置 IP 地址 • 设置网关 • 设置子网掩码

权限	说明
	• 设置第一引导设备 配置用户： • 设置 iDRAC 根密码 • iDRAC 重设 服务器控制管理员： • 打开电源 • 关闭电源 • 打开电源后再关闭电源 • 正常关机 • 服务器重新引导
测试警报用户	用户可发送测试警报消息。
调试命令管理员	用户可执行系统诊断命令。
结构 A 管理员	用户可设置和配置位于 I/O 插槽的插槽 A1 或 A2 的结构 A IOM。
结构 B 管理员	用户可设置和配置位于 I/O 插槽的插槽 B1 或 B2 的结构 B IOM。
结构 C 管理员	用户可设置和配置位于 I/O 插槽的插槽 C1 或 C2 的结构 C IOM。

CMC 用户组提供具有预分配用户权限的一系列用户组。

注: 如果选择“管理员”、“高级用户”或“来宾用户”，然后从预定义设置中添加或删除权限，则 CMC 组会自动更改为自定义。

表. 22: CMC 组权限

用户组	权限分配
管理员	• CMC 登录用户 • 机箱配置管理员 • 用户配置管理员 • 清除日志管理员 • 服务器管理员 • 测试警报用户 • 调试命令管理员 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员
高级用户	• 登录 • 清除日志管理员 • 机箱控制管理员（电源命令） • 服务器管理员 • 测试警报用户 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员

用户组	权限分配
来宾用户	登录
Custom（自定义）	选择以下权限的任意组合： • CMC 登录用户 • 机箱配置管理员 • 用户配置管理员 • 清除日志管理员 • 机箱控制管理员（电源命令） • 服务器管理员 • 测试警报用户 • 调试命令管理员 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员
无	没有分配权限

表. 23: CMC 管理员、高级用户和来宾用户的权限比较

权限集	管理员权限	高级用户权限	来宾用户权限
CMC 登录用户	是	是	是
机箱配置管理员	是	否	否
用户配置管理员	是	否	否
清除日志管理员	是	是	否
机箱控制管理员（电源命令）	是	是	否
服务器管理员	是	是	否
测试警报用户	是	是	否
调试命令管理员	是	否	否
结构 A 管理员	是	是	否
结构 B 管理员	是	是	否
结构 C 管理员	是	是	否

修改根用户管理员帐户设置

为了确保安全，强烈建议您更改 root（用户 1）帐户的默认密码。root 帐户是 CMC 随附的默认管理帐户。
要使用 CMC Web 界面更改 root 帐户的默认密码，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**用户验证** > **本地用户**。
此时将显示 **Users**（用户）页面。
2 在**用户 ID** 列中，单击用户 ID 1。

注: 用户 ID 1 是 CMC 默认随附的根用户帐户。该帐户无法更改。

此时将显示**用户配置**页。
3 选中**更改密码**复选框。
4 在**密码**和**确认密码**字段中键入新密码。

5 单击**应用**。
随即会更改用户 ID 1 的密码。

配置本地用户

您可以使用指定的访问权限在 CMC 上配置多达 16 个本地用户。在创建 CMC 本地用户之前，请验证是否存在任何当前用户。您可以使用这些用户的权限设置用户名、密码和角色。这些用户名和密码可通过任何 CMC 的加密界面（即 Web 界面、RACADM 或 WS-MAN）进行更改。

使用 CMC Web 界面配置本地用户

要添加和配置本地 CMC 用户，请执行以下操作：

注: 您必须具有配置用户权限才能创建 CMC 用户。

1 在系统树中，转至**机箱概览**，然后单击**用户验证** > **本地用户**。
此时将显示**用户**页面。
2 在**用户 ID** 列中，单击用户 ID 编号。

注: 用户 ID 1 是 CMC 默认随附的根用户帐户。该帐户无法更改。

此时将显示**用户配置**页。
3 启用用户 ID 并指定用户的用户名、密码和访问权限。
有关选项的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
4 单击**应用**。
将创建具有所需权限的用户。

使用 RACADM 配置本地用户

注: 必须以用户 root 登录才能在远程 Linux 系统上执行 RACADM 命令。

最多可以在 CMC 属性数据库中配置 16 个用户。手动启用 CMC 用户前，请验证当前用户是否存在。

如果配置新 CMC 或使用了 racadm `racresetcfg` 命令，则当前唯一用户为 `root`，密码为 `calvin`。`racresetcfg` 子目录将所有配置参数重设为最初的默认值。任何之前的更改将丢失。

注: 可以随时启用和禁用用户，并且禁用用户不会从数据库中删除该用户。

若要验证用户是否存在，则打开到 CMC 的 Telnet/SSH 文本控制台，登录，然后为 1-16 的每个索引键入以下命令一次：

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

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

多个参数和对象 ID 会与其当前值一起列出。其中两个重要的对象是：

```
# cfgUserAdminIndex=XX
cfgUserAdminUserName=
```

如果 `cfgUserAdminUserName` 对象没有值，则可以使用 `cfgUserAdminIndex` 对象指示的索引编号。如果“=”后显示了名称，该索引即会被此用户名使用。

使用 racadm `config` 子命令手动启用或禁用用户时，**必须**使用 `-i` 选项指定索引。

命令对象中的“#”字符表示这是一个只读对象。同样，如果您使用 `racadm config -f racadm.cfg` 命令来指定任意数量要写入的组或对象，则无法指定索引。新用户将添加到第一个可用的索引。这种行为允许使用与主 CMC 相同的设置配置第二个 CMC，具备更大的灵活性。

使用 RACADM 添加 CMC 用户

要将新用户添加到 CMC 配置，请执行以下操作：

1 设置用户名。
2 设置密码。
3 设置用户权限。有关用户权限的信息，请参阅用户类型。
4 启用用户。

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

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

注: 有关特定用户权限的有效位掩码值的列表，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。默认权限值为 0，这表明用户没有启用权限。

为验证是否成功地为用户添加了正确的权限，请使用以下命令：

```
racadm getconfig –g cfgUserAdmin –i 2
```

有关 RACADM 命令的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

禁用 CMC 用户

使用 RACADM 时，必须以手动方式逐个对用户进行禁用。不能使用配置文件删除用户。
要删除 CMC 用户，命令语法如下：

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index>"" racadm config -g
cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

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

启用具有权限的 CMC 用户

启用具有特定管理权限的用户（基于角色的授权）：

1 使用命令语法找到可用的用户索引：

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

2 使用新用户名和密码键入以下命令。

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

注: 有关特定用户权限的有效位掩码值列表，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。默认权限值为 0，即表示用户没有启用任何权限。

配置 Active Directory 用户

如果您的公司使用 Microsoft Active Directory 软件，则可以配置该软件以提供访问 CMC 的权限，从而允许添加和控制目录服务中现有用户的 CMC 用户权限。这是获得许可的功能。

注: 在 Microsoft Windows 2000 和 Windows Server 2003 操作系统上支持使用 Active Directory 识别 CMC 用户。Windows 2008 支持基于 IPv6 和 IPv4 的 Active Directory。

您可以通过 Active Directory 配置用户验证以登录到 CMC。您还可以提供基于角色的权限，从而使管理员可以为每位用户配置特定的权限。

支持的 Active Directory 验证机制

您可以通过两种方法使用 Active Directory 定义 CMC 用户访问权限：

- *标准架构*解决方案，仅使用 Microsoft 的默认 Active Directory 组对象。
- *扩展架构*解决方案，拥有 Dell 提供的自定义 Active Directory 对象。所有访问控制对象都在 Active Directory 中维护。它为在具有各种权限级别的不同 CMC 上配置用户访问权限提供了最大的灵活性。

相关链接

标准架构 Active Directory 概览

扩展架构 Active Directory 概述

标准架构 Active Directory 概览

如下图所示，为 Active Directory 集成使用标准架构需要在 Active Directory 和 CMC 上都进行配置。

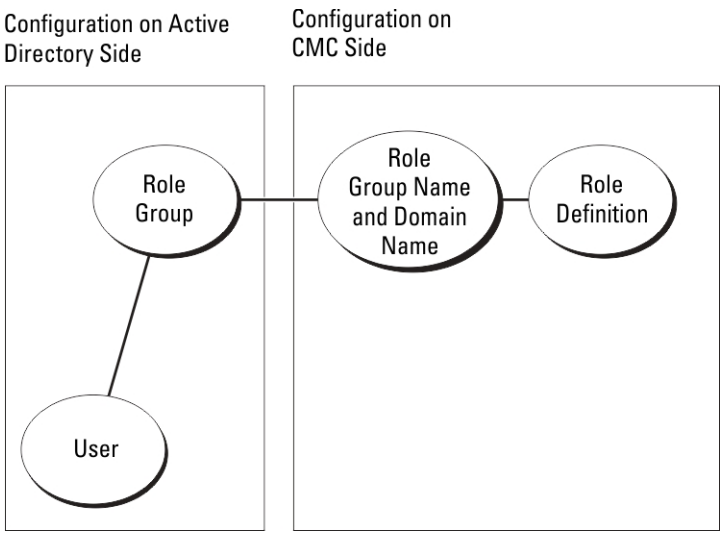


图 7: 使用 Active Directory 标准架构的 CMC 配置

在 Active Directory 中，标准组对象用作角色组。具有 CMC 访问权限的用户属于角色组的成员。要为此用户分配访问特定 CMC 卡的权限，需要在特定 CMC 卡上配置角色组名称及其域名。角色及权限级别在每个 CMC 卡（而不是 Active Directory 中）上进行定义。在每个 CMC 中，您最多可以配置五个角色组。下表显示了默认角色组的权限。

表. 24: 默认角色组权限

角色组	默认权限级别	授予的权限	位掩码
1	无	• CMC 登录用户 • 机箱配置管理员 • 用户配置管理员 • 清除日志管理员 • 机箱控制管理员（电源命令） • 服务器管理员 • 测试警报用户 • 调试命令管理员 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员	0x00000fff
2	无	• CMC 登录用户 • 清除日志管理员 • 机箱控制管理员（电源命令） • 服务器管理员 • 测试警报用户 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员	0x00000ed9
3	无	CMC 登录用户	0x00000001
4	无	没有分配权限	0x00000000
5	无	没有分配权限	0x00000000

注: **“位掩码”值只有在用 RACADM 设置标准架构时才使用。**

注: **有关用户权限的更多信息，请参阅用户类型。**

配置标准架构 Active Directory

要配置 CMC 以进行 Active Directory 登录访问，请执行以下操作：

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 使用 CMC Web 界面或 RACADM：

a 创建组或选择现有组。

b 配置角色权限。

3 将 Active Directory 用户作为 Active Directory 组的成员进行添加，使其能够访问 CMC。

使用 CMC Web 界面配置具有标准架构的 Active Directory

注: **有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。**

1 在系统树中，转至**机箱概述**，然后单击**用户验证** > **目录服务**。此时将显示**目录服务**页。

2 选择 **Microsoft Active Directory（标准架构）**。要为标准架构配置的设置显示在同一页上。

3 指定以下各项：

- 启用 Active Directory，输入根域名称和超时值。
- 如果要用定向调用搜索域控制器和全局编录，请选择**搜索 AD 服务器以搜索（可选）**选项，然后指定域控制器和全局编录详情。

4 单击**应用**保存设置。

注: **您必须先应用设置才能继续。如果您不应用这些设置，则导航至下一页时会丢失这些设置。**

5 在**标准架构设置**部分，单击**角色组**。此时将显示**配置角色组**页。

6 为角色组指定组名、域和权限。

7 单击**应用**保存角色组设置，然后单击**退回到配置**页。

8 如果您启用了证书验证，则必须将域目录林根证书颁发机构签发的证书上载到 CMC。在**管理证书**部分，键入证书的文件路径，或浏览到证书文件。单击**上载**将文件上载到 CMC。

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

域控制器的 SSL 证书必须是由根证书颁发机构签发的证书。访问 CMC 的管理站必须有根证书颁发机构签发的证书。

9 如果您已经在 **Kerberos Keytab** 部分启用单点登录 (SSO)，请单击**浏览**，指定 keytab 文件，然后单击**上载**。上载完成后，会显示一条消息，指示上载成功或失败。

10 单击**应用**。CMC Web 服务器将在单击**应用**后自动重新启动。

11 注销，然后登录 CMC 以完成 CMC Active Directory 配置。

12 在系统树中选择**机箱**，然后导航到**网络**选项卡。此时将显示**网络配置**页。

13 如果在**网络设置**下选择了**使用 DHCP（用于 CMC 网络接口 IP 地址）**，则选择**使用 DHCP 获取 DNS 服务器地址**。

要手动输入 DNS 服务器 IP 地址，请取消选中**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。

14 单击**应用更改**。

CMC 标准架构 Active Directory 功能配置完成。

使用 RACADM 配置具有标准架构的 Active Directory

要使用 RACADM 配置具有标准架构的 CMC Active Directory，请执行以下操作：

1 打开到 CMC 的串行/Telnet/SSH 文本控制台，并键入：

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g cfgActiveDirectory -o
cfgADType 2 racadm config -g cfgActiveDirectory -o cfgADRootDomain <fully qualified root
domain name> racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName <common
name of the role group> racadm config -g cfgStandardSchema -i <index>-o
cfgSSADRoleGroupDomain <fully qualified domain name> racadm config -g cfgStandardSchema -i
<index> -o cfgSSADRoleGroupPrivilege <Bit mask number for specific user permissions> racadm
sslcertupload -t 0x2 -f <ADS root CA certificate> racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```

注: 有关位掩码数值，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的数据库属性章节。

2 使用以下任一选项指定 DNS 服务器：

- 如果 CMC 上已启用 DHCP 并且您希望使用 DHCP 服务器自动获取的 DNS 地址，则键入以下命令：

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

- 如果 CMC 上已禁用 DHCP，或想要手工输入 DNS IP 地址，则键入以下命令：

  ```
  racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm config -g
  cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address> racadm config -g
  cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP address>
  ```

扩展架构 Active Directory 概述

使用扩展架构解决方案需要 Active Directory 架构扩展。

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。数据库中存储的类的一个示例就是用户类。某些示例用户类属性可包括用户的名字、姓氏、电话号码等。

您可以通过添加自己独特的*属性*和*类*来扩展 Active Directory 数据库以满足特定需求。Dell 使用 Active Directory 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。

添加到现有 Active Directory 架构的每个*属性*或*类*都必须使用唯一的 ID 定义。为了在整个行业内维护唯一的 ID，Microsoft 将维护 Active Directory 对象标识符 (OID) 的数据库，以便公司添加架构扩展时，可以保证这些扩展唯一并且不会彼此冲突。要在 Microsoft 的 Active Directory 中扩展架构，对于添加到目录服务中的属性和类，Dell 将收到唯一的 OID、唯一的扩展名和唯一链接的属性 ID。

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

架构扩展概览

Dell 已扩展架构以包括*关联*、*设备*和*权限*属性。*关联*属性用于将用户或组与一组特定的权限一起链接到一个或多个 RAC 设备。此模型为网络上有各种用户、RAC 权限和 RAC 设备组合的管理员提供了最大的灵活性，而无需繁琐操作。

当要与 Active Directory 集成以进行验证和授权的网络上有两个 CMC 时，为其中每个 CMC 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”对象都可以链接到所需的任意多个用户、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 CMC 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。此外，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。

下图显示为提供验证和授权所需连接的关联对象。

注: RAC 权限对象适用于 DRAC 4、DRAC 5 和 CMC。

您可以根据需要创建任意多个关联对象。但是，您必须创建至少一个关联对象，并且网络上要与 Active Directory 集成的每个 RAC (CMC) 都必须具有一个 RAC 设备对象。

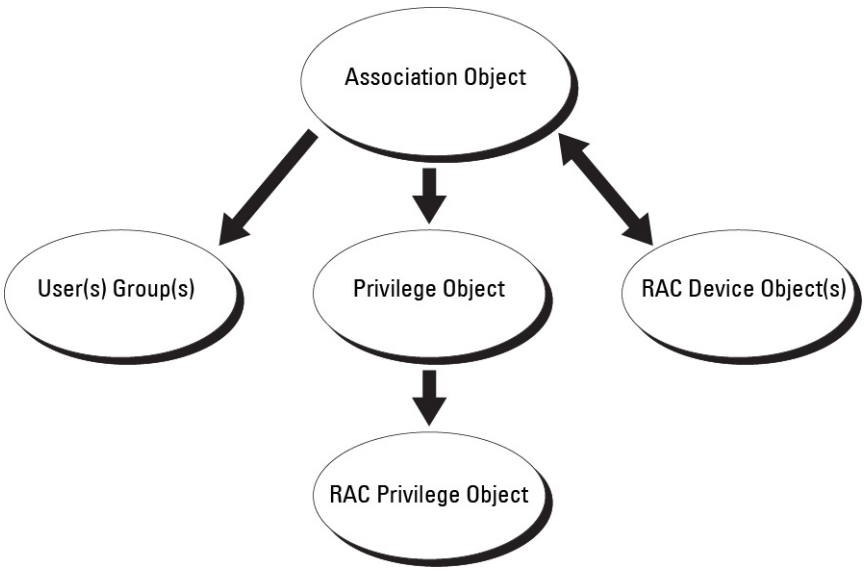


图 8: Active Directory 对象的典型设置

关联对象允许任意多的用户和/或组以及 RAC 设备对象。但是，每个关联对象仅包括一个权限对象。关联对象可连接在 RAC (CMC) 上拥有*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 CMC（RAC1 和 RAC2）和三个现有 Active Directory 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 CMC 的管理员权限并授予用户 3 对 RAC2 卡的登录权限。下图显示了如何在此情况下设置 Active Directory 对象。

添加来自不同域的通用组时，将创建具有通用范围的关联对象。Dell Schema Extender 公用程序创建的默认关联对象是域本地组，并且不能与来自其他域的通用组一起使用。

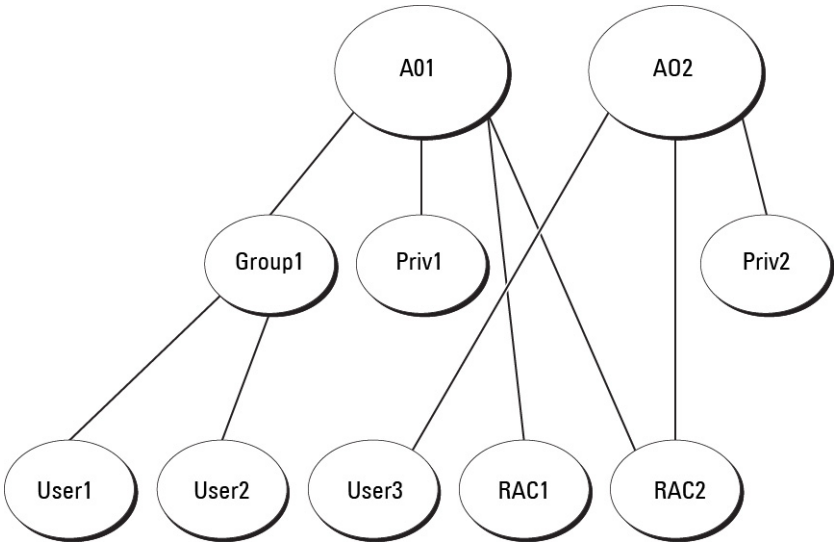


图 9: 在一个域中设置 Active Directory 对象

要为单域情况配置对象，请执行以下操作：

1 创建两个关联对象。
2 创建两个“RAC 设备”对象（RAC1 和 RAC2）以代表两个 CMC。
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 仅具有登录权限。
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 (A01) 的成员，权限 1 作为 A01 的权限对象，而 RAC1 和 RAC2 作为 A01 中的 RAC 设备。
6 将用户 3 添加为关联对象 2 (A02) 的成员，权限 2 作为 A02 的权限对象，而 RAC2 作为 A02 中的 RAC 设备。

下图提供多个域中 Active Directory 对象的示例。在这种情况下，已有两个 CMC（RAC1 和 RAC2）和三个现有 Active Directory 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 CMC 的管理员权限，配置用户 3 具有对 RAC2 卡的登录权限。

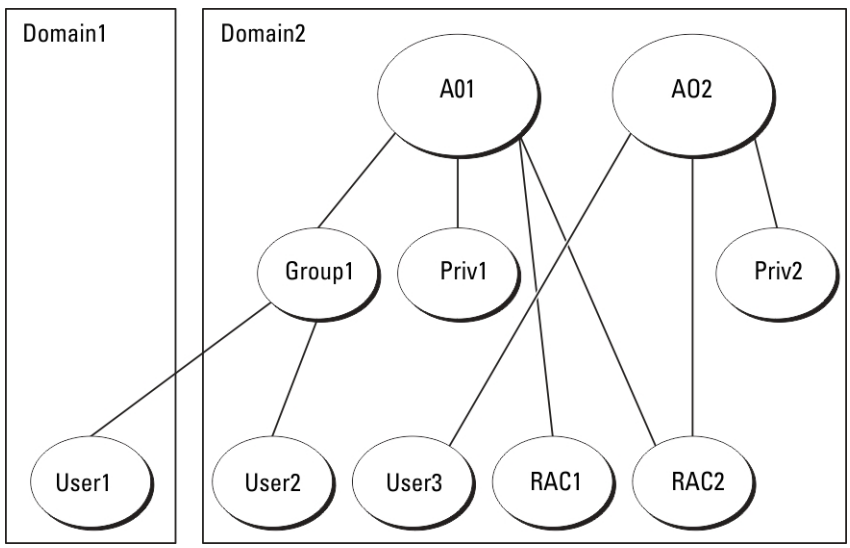


图 10: 在多个域中设置 Active Directory 对象

要为多域情况配置对象，请执行以下操作：

1 确保域目录林功能处于本机或 Windows 2003 模式。
2 在任意域中创建两个“关联”对象：A01（通用范围）和 A02。图“在多个域中设置 Active Directory 对象”显示域 2 中的对象。
3 创建两个“RAC 设备”对象（RAC1 和 RAC2）以代表两个 CMC。
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 仅具有登录权限。
5 将用户 1 和用户 2 分组到组 1。组 1 的组范围必须是通用。
6 将组 1 添加为关联对象 1 (A01) 的成员，权限 1 作为 A01 的权限对象，而 RAC1 和 RAC2 作为 A01 中的 RAC 设备。
7 将用户 3 添加为关联对象 2 (A02) 的成员，权限 2 作为 A02 的权限对象，而 RAC2 作为 A02 中的 RAC 设备。

配置扩展架构 Active Directory

要配置 Active Directory 以访问 CMC，请执行以下操作：

1 扩展 Active Directory 架构。
2 扩展 Active Directory 用户和计算机管理单元。
3 将 CMC 用户及其权限添加到 Active Directory。
4 在各个域控制器上启用 SSL。
5 使用 CMC Web 界面或 RACADM 配置 CMC Active Directory 属性。

相关链接

扩展 Active Directory 架构
安装用于 Microsoft Active Directory 用户和计算机管理单元的 Dell 扩展
将 CMC 用户和权限添加到 Active Directory
使用 CMC Web 界面配置具有扩展架构的 Active Directory
使用 RACADM 配置具有扩展架构的 Active Directory

扩展 Active Directory 架构

通过扩展您的 Active Directory 架构，可向 Active Directory 架构添加 Dell 组织单元、架构类和属性，以及示例权限与关联对象。在您扩展架构之前，确保您对域目录林的架构主机灵活单主机操作 (FSMO) 角色拥有者具有架构管理员权限。

可使用以下任一方法扩展架构：

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

如果使用 LDIF 脚本文件，则不会将 Dell 组织单元添加到架构中。

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

- DVDdrive:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management\LDIF_Files
- <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools\Remote_Management\Schema Extender

要使用 LDIF 文件，请参阅 LDIF_Files 目录中自述文件中的说明。

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

使用 Dell Schema Extender

△ **小心: Dell Schema Extender 使用 SchemaExtenderOem.ini 文件。要确保 Dell Schema Extender 公用程序正常工作，请勿修改此文件的名称。**

1 在**欢迎**屏幕中单击**下一步**。

2 阅读并了解警告，然后单击**下一步**。

3 选择**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**下一步**运行 Dell Schema Extender。

5 单击**完成**。

架构即得到扩展。要验证架构扩展，请使用 MMC 和 Active Directory 架构管理单元验证类和属性是否存在。有关类和属性的更多信息，请参阅类和属性。有关使用 MMC 和 Active Directory 架构管理单元的更多信息，请参阅 Microsoft 说明文件。

类和属性

表. 25: 添加到 Active Directory 架构中类的类定义

类名称	分配的对象标识号 (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表. 26: dellRacDevice 类

OID	1.2.840.113556.1.8000.1280.1.7.1.1
说明	代表 Dell RAC 设备。在 Active Directory 中必须将 RAC 配置为 delliDRACDevice。这种配置使 CMC 可将轻量级目录访问协议 (LDAP) 查询发送到 Active Directory。
类的类型	结构类
超类	dellProduct
属性	dellSchemaVersion dellRacType

表. 27: delliDRACAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.7.1.2
说明	代表 Dell 关联对象。关联对象用于提供用户与设备之间的连接。
类的类型	结构类
超类	组
属性	dellProductMembers

OID	1.2.840.113556.1.8000.1280.1.7.1.2
	dellPrivilegeMember

表. 28: dellRAC4Privileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.3
说明	定义 CMC 设备的权限（授权权限）。
类的类型	辅助类
超类	无
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

表. 29: dellPrivileges 类

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

表. 30: 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. 31: 添加到 Active Directory 架构的属性的列表

分配的 OID/语法对象标识符	单值
属性：`dellPrivilegeMember`	FALSE

分配的 OID/语法对象标识符	单值
说明：属于此属性的 dellPrivilege 对象的列表。 **OID**：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)	
属性：dellProductMembers **说明**：属于此角色的 dellRacDevices 对象的列表。此属性是指向 dellAssociationMembers 反向链接的正向链接。 **链接 ID**：12070 **OID**：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
属性：dellIsCardConfigAdmin **说明**：如果用户具有设备的卡配置权限，则为 TRUE。 **OID**：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
属性：dellIsLoginUser **说明**：如果用户具有设备的登录权限，则为 TRUE。 **OID**：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
属性：dellIsUserConfigAdmin **说明**：如果用户具有设备的用户配置管理员权限，则为 TRUE。 **OID**：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
属性：dellIsLogClearAdmin **说明**：如果用户具有设备的清除日志管理员权限，则为 TRUE。 **OID**：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
属性：dellIsServerResetUser **说明**：如果用户具有设备的服务器重设权限，则为 TRUE。 **OID**：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
属性：dellIsTestAlertUser **说明**：如果用户具有设备的测试警报用户权限，则为 TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.10	TRUE

分配的 OID/语法对象标识符	单值
布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性： dellIsDebugCommandAdmin **说明：**如果用户具有设备的调试命令管理员权限，则为 TRUE。 **OID：**1.2.840.113556.1.8000.1280.1.1.2.11	TRUE
布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性： dellSchemaVersion **说明：**当前架构版本用于更新架构。 **OID：**1.2.840.113556.1.8000.1280.1.1.2.12	TRUE
忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
属性： dellRacType **说明：**此属性是 dellRacDevice 对象的当前 Rac 类型和指向 dellAssociationObjectMembers 正向链接的反向链接。 **OID：**1.2.840.113556.1.8000.1280.1.1.2.13	TRUE
忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
属性： dellAssociationMembers **属性：**属于此产品的 dellAssociationObjectMembers 的列表。此属性是指向 dellProductMembers 链接属性的反向链接。 **链接 ID：**12071 **OID：**1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
属性： dellPermissionsMask1 **OID：**1.2.840.113556.1.8000.1280.1.6.2.1 整数 (LDAPTYPE_INTEGER)	
属性： dellPermissionsMask2 **OID：**1.2.840.113556.1.8000.1280.1.6.2.2 整数 (LDAPTYPE_INTEGER)	

安装用于 Microsoft Active Directory 用户和计算机管理单元的 Dell 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 (CMC) 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，您可以通过在安装程序过程中选择 **Active Directory 用户和计算机管理单元**选项扩展管理单元。有关安装系统管理软件的其他说明，请参阅 *Dell OpenManage Software Quick Installation Guide*（Dell OpenManage 软件快速安装指南）。对于 64 位 Windows 操作系统，管理单元安装程序位于：**<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64**

有关 Active Directory 用户和计算机管理单元的更多信息，请参阅 Microsoft 说明文件。

将 CMC 用户和权限添加到 Active Directory

使用 Dell 扩展的 Active Directory 用户和计算机管理单元，您可以通过创建 RAC 设备、关联和权限对象添加 CMC 用户和权限。要添加每个对象，请执行以下操作：

- 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

相关链接

将对象添加到关联对象
创建 RAC 设备对象
创建权限对象
创建关联对象

创建 RAC 设备对象

要创建 RAC 设备对象，请执行以下操作：

1 在 **MMC 控制台根目录**窗口中，右键单击一个容器。
2 选择**新建** > **Dell 远程管理对象**。
将显示**新建对象**窗口。
3 输入新对象的名称。该名称必须与您在“使用 CMC Web 界面配置具有扩展架构的 Active Directory”中输入的 CMC 名称相同。
4 选择 **RAC 设备对象**，然后单击**确定**。

创建权限对象

要创建权限对象，请执行以下操作：

注: 您必须在相关关联对象的同一个域中创建权限对象。

1 在**控制台根目录 (MMC)** 窗口中，右键单击一个容器。
2 选择**新建** > **Dell 远程管理对象**。
将显示**新建对象**窗口。
3 为新对象输入名称。
4 选择**权限对象**，然后单击**确定**。
5 右键单击已创建的权限对象并选择**属性**。
6 单击 **RAC 权限**选项卡并为用户或组分配权限。
有关 CMC 用户权限的更多信息，请参阅用户类型。

创建关联对象

关联对象从组派生而来，必须包含组类型。关联范围指定关联对象的安全组类型。创建关联对象时，必须选择适用于要添加的对象类型的关联范围。例如：如果选择“通用”，则关联对象只有在 Active Directory 域以本机模式或更高模式运行时才可用。

要创建关联对象，请执行以下操作：

1 在 **MMC 控制台根目录**窗口中，右键单击一个容器。
2 选择**新建** > **Dell 远程管理对象**。
系统会显示**新建对象**窗口。

3 输入新对象的名称并选择**关联对象**。
4 选择**关联对象**的范围，然后单击**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。如果系统在 Microsoft Windows 2000 或更高版本模式下运行，请使用“通用组”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。

相关链接

添加用户或用户组
添加权限
添加 RAC 设备或 RAC 设备组

添加用户或用户组

要添加用户或用户组，请执行以下操作：

1 右键单击**关联对象**并选择**属性**。
2 选择**用户**选项卡并单击**添加**。
3 输入用户或用户组名称并单击**确定**。

添加权限

要添加权限，请执行以下操作：

1 选择**权限对象**选项卡，然后单击**添加**。
2 输入权限对象名称并单击**确定**。
单击**权限对象**选项卡以向关联对象添加权限对象，该关联对象定义了针对 RAC 设备验证时用户或用户组的权限。一个关联对象只能添加一个权限对象。

添加 RAC 设备或 RAC 设备组

要添加 RAC 设备或 RAC 设备组，请执行以下操作：

1 选择**产品**选项卡并单击**添加**。
2 输入 RAC 设备或 RAC 设备组名称并单击**确定**。
3 在**属性**窗口中，依次单击**应用**、**确定**。
单击**产品**选项卡将一个或多个 RAC 设备添加到关联设备。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。

使用 CMC Web 界面配置具有扩展架构的 Active Directory

要使用 CMC Web 界面配置具有扩展架构的 Active Directory，请执行以下操作：

注: 有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

1 在系统树中，转至**机箱概览**，然后单击**用户验证** > **目录服务**。
2 选择 **Microsoft Active Directory（扩展架构）**。
要配置的扩展架构设置将显示在同一个页面上。
3 指定以下各项：
- 启用 Active Directory，提供根域名和超时值。

- 如果要用定向调用搜索域控制器和全局编录，请选择**搜索 AD 服务器以搜索（可选）**选项，然后指定域控制器和全局编录详情。

  注: 将 IP 地址设置为 0.0.0.0 时，将禁止 CMC 搜索服务器。

  注: 可以指定逗号分隔的一组域控制器或全局编录服务器。CMC 允许指定多达三个 IP 地址或主机名。

  注: 如果未针对所有域和应用程序正确配置域控制器或全局编录服务器，可能导致在现有应用程序/域运行过程中产生无法预料的结果。

4 单击**应用**保存设置。

注: 您必须先应用设置才能继续。如果您不应用这些设置，则导航至下一页时会丢失这些设置。

5 在**扩展架构设置**部分，输入 CMC 设备名称和域名。

6 如果您启用了证书验证，则必须将域目录林根证书颁发机构签发的证书上载到 CMC。在**管理证书**部分，键入证书的文件路径，或浏览到证书文件。单击**上载**将文件上载到 CMC。

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

域控制器的 SSL 证书必须是由根证书颁发机构签发的证书。访问 CMC 的管理站必须有根证书颁发机构签发的证书。

小心: 默认需要 SSL 证书验证。禁用此证书会带来风险。

7 如果您已启用单一登录 (SSO)，请在 Kerberos Keytab 部分中，单击**浏览**，指定 keytab 文件并单击**上载**。

上载完成后，将显示一条消息说明上载成功或失败。

8 单击**应用**。

CMC Web 服务器将自动重新启动。

9 登录 CMC Web 界面。

10 在系统树中，选择**机箱**，单击**网络**选项卡，然后单击**网络**子选项卡。

将显示**网络配置**页面。

11 如果启用对 CMC 网络接口 IP 地址**使用 DHCP**，请进行以下任一操作：

- 选择**使用 DHCP 获取 DNS 服务器地址**选项，使 DHCP 服务器能够自动获取 DNS 服务器地址。
- 不选中**使用 DHCP 获取 DNS 服务器地址**选项时，可以手动配置 DNS 服务器 IP 地址。在提供的字段中输入主要和备用 DNS 服务器 IP 地址。

12 单击**应用更改**。

具有扩展架构的 Active Directory 设置已配置完成。

使用 RACADM 配置具有扩展架构的 Active Directory

要使用 RACADM 配置具有扩展架构的 CMC Active Directory，请执行以下操作：

1 打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o
cfgADRacDomain <fully qualified CMC domain name>
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified root domain name>
racadm config -g cfgActiveDirectory -o
cfgADRacName <CMC common name>
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate> -r
racadm sslcertdownload -t 0x1 -f <CMC SSL certificate>
```

注: 只能通过远程 RACADM 使用此命令。有关远程 RACADM 的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

可选项：如果想指定 LDAP 或全局编录服务器，而不是使用由 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**指定服务器**选项：

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

注：当使用指定服务器选项时，证书颁发机构签发证书中的主机名与指定服务器的名称不匹配。如果您是 CMC 管理员，这样尤为有用，因为可以让您输入主机名和 IP 地址。

启用**指定服务器**选项后，可使用服务器的 IP 地址或完全限定域名 (FQDN) 指定 LDAP 服务器和全局编录。FQDN 包含服务器的主机名和域名。

要指定 LDAP 服务器，键入：

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController <AD domain controller IP address>
```

要指定全局编录服务器，键入：

```
racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog <AD global catalog IP address>
```

注：将 IP 地址设置为 0.0.0.0 时，将禁止 CMC 搜索服务器。

注：可以用逗号分隔来指定一组 LDAP 或全局编录服务器。CMC 允许指定多达三个 IP 地址或主机名。

注：如果未针对所有域和应用程序正确配置一个 LDAP 或多个 LDAP，可能导致在现有应用程序/域运行过程中产生无法预料的结果。

2 使用以下任一选项指定 DNS 服务器：

- 如果 CMC 上已启用 DHCP 并且您希望使用 DHCP 服务器自动获取的 DNS 地址，则键入以下命令：

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

- 如果 CMC 上已禁用 DHCP，或如果已启用 DHCP 但想要手工指定 DNS IP 地址，则键入以下命令：

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSServersFromDHCP 0
  racadm config -g cfgLanNetworking -o
  cfgDNSServer1 <primary DNS IP address>
  racadm config -g cfgLanNetworking -o
  cfgDNSServer2 <secondary DNS IP address>
  ```

扩展架构功能配置完成。

配置通用 LDAP 用户

CMC 提供通用解决方案来支持基于轻量级目录访问协议 (LDAP) 的验证。此功能不需要在目录服务上进行任何架构扩展。

CMC 管理员现在可在 CMC 中集成 LDAP 服务器用户登录。此集成要求同时在 LDAP 和 CMC 服务器上配置。在 LDAP 服务器上，标准组对象用作角色组。具有 CMC 权限的用户将成为该角色组的成员。权限仍存储在 CMC 中用于验证，工作方式与具有 Active Directory 支持的标准架构设置类似。

若要支持 LDAP 用户访问特定的 CMC 卡，则必须在特定的 CMC 卡上配置角色组名称及其域名。每个 CMC 可配置最多 5 个角色组。用户可选择添加到目录服务内的多个组。如果用户是多个组的成员，则其获得所有所属组的权限。

有关角色组权限级别和默认角色组设置的信息，请参阅用户的类型。

下图说明如何配置 CMC 及通用 LDAP。

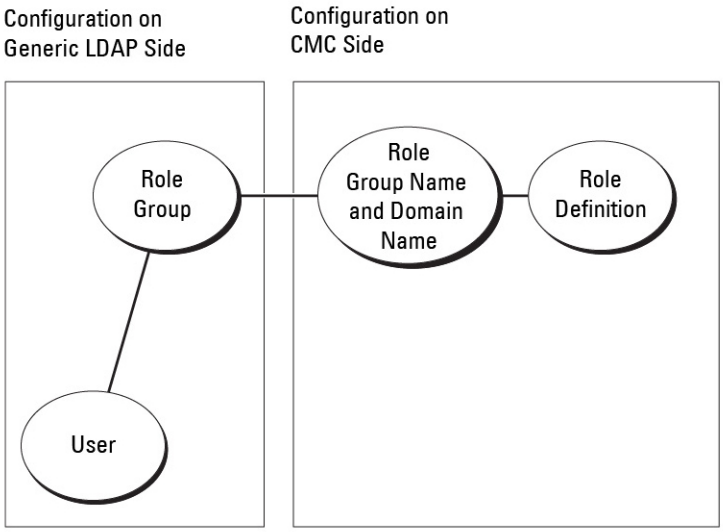


图 11: 配置 CMC 及通用 LDAP

配置通用 LDAP 目录以访问 CMC

CMC 的通用 LDAP 实施在授予用户访问权限时分两阶段 - 先是用户验证，后是用户授权。

LDAP 用户验证

有些目录服务器要求在特定 LDAP 服务器上进行任何搜索前完成绑定。
要验证用户，请执行以下操作：

1 可选绑定到目录服务。默认为匿名绑定。

注: 基于 Windows 的目录服务器不允许匿名登录。因此，输入绑定 DN 名称和密码。

2 根据用户登录搜索用户。默认属性是 `uid`。
如果找到一个以上的对象，则返回错误。

3 解除绑定并以用户的 DN 和密码进行绑定。
如果绑定失败，则登录失败。

如果这些步骤成功完成，则用户通过验证。

LDAP 用户的授权

要对用户授权，请执行以下操作：

1 在各配置的组中，从 `member or uniqueMember` 属性中搜索用户的域名。

2 该用户将拥有所属每个组的叠加权限。

使用 CMC 基于 Web 的界面配置通用 LDAP 目录服务

要配置通用 LDAP 目录服务，请执行以下操作：

注: 您必须拥有机箱配置管理员权限。

1 在系统树中，转至**机箱概览**，然后单击**用户验证** > **目录服务**。
2 选择**通用 LDAP**。
为标准架构配置的设置将显示在同一页面上。
3 指定以下各项：

注: 有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

- 常见设置
- 使用 LDAP 的服务器：
  - 静态服务器 - 指定 FQDN 或 IP 地址和 LDAP 端口号。
  - DNS 服务器 - 指定 DNS 服务器以通过搜索 DNS 内的 SRV 记录来检索 LDAP 服务器列表。
    为 SRV 记录执行以下 DNS 查询：
    ```
    _[Service Name]._tcp.[Search Domain]
    ```
    其中 <*Search Domain*> 是查询中使用的根级别域而 <*Service Name*> 是查询中使用的服务名称。

    例如：
    ```
    _ldap._tcp.dell.com
    ```
    其中 `ldap` 是服务名称而 `dell.com` 是搜索域。

4 单击**应用**保存设置。

注: 您必须先应用设置才能继续。如果您不应用这些设置，则导航至下一页时会丢失这些设置。

5 在**组设置**部分，单击**角色组**。此时将显示**配置 LDAP 角色组**页。
6 为角色组指定组域名和权限。
7 单击**应用**保存角色组设置，单击**退回到配置页**，然后选择**通用 LDAP**。
8 如果您已选中**启用证书验证**选项，则请在**管理证书**部分指定 CA 证书，以便在 SSL 握手过程中验证 LDAP 服务器证书，然后单击**上载**。
证书会上载到 CMC 并显示详情。
9 单击**应用**。
通用 LDAP 目录服务配置完成。

使用 RACADM 配置通用 LDAP 目录服务

要配置 LDAP 目录服务，请使用 `cfgLdap` 和 `cfgLdapRoleGroup` RACADM 组中的对象。

配置 LDAP 登录有多个选项。大多数情况下部分选项可使用其默认设置。

注: 强烈建议使用 racadm `testfeature -f LDAP` 命令在第一次设置时测试 LDAP 设置。此功能支持 IPv4 和 IPv6。

所需属性更改包括启用 LDAP 登录、设置服务器 FQDN 或 IP 以及配置 LDAP 服务器的基础 DN。

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=company,dc=com`

可对 CMC 进行配置，使其查询 DNS 服务器上的 SRV 记录（可选）。如果 `cfgLDAPSRVLookupEnable` 属性启用，则忽略 `cfgLDAPServer` 属性。以下查询可用于为 SRV 记录搜索 DNS 服务器：

```
_ldap._tcp.domainname.com
```

`ldap` 在上述查询中为 `cfgLDAPSRVLookupServiceName` 属性。

`cfgLDAPSRVLookupDomainName` 配置为 **domainname.com**。

有关 RACADM 对象的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

10

配置 CMC 进行单点登录或智能卡登录

此部分为 Active Directory 用户提供配置 CMC 进行智能卡登录和单点登录 (SSO) 的信息。

从 CMC 2.10 版开始，CMC 提供基于 Kerberos 的 Active Directory 验证来支持智能卡登录和 SSO 登录。

SSO 使用 kerberos 作为验证方法，使已经登录到域的用户可以自动登录或单一登录到 Exchange 等随后的应用程序。对于单一登录，CMC 使用客户端系统的凭据。您使用有效的 Active Directory 帐户登录之后操作系统就会高速缓存这些凭据。

双重验证则提供了更高级别的安全性，要求用户具有密码或 PIN 以及含有私人密钥和数字证书的实物卡。Kerberos 使用此双重验证机制使系统可以证明其真实性。

注: 选择登录方法不会设置与诸如 SSH 等其他登录界面相关的策略属性。您还必须设置其他登录界面的其他策略属性。如果您要禁用所有其他登录界面，请导航至服务页并禁用所有（或某些）登录界面。

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista、Windows 7 和 Windows Server 2008 可以使用 Kerberos 作为 SSO 和智能卡登录的验证机制。

有关 Kerberos 的信息，请参阅 Microsoft 网站。

主题：

相关链接

系统要求
单点登录或智能卡登录的前提条件
为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

系统要求

要使用 Kerberos 验证方法，网络必须包括：

- DNS 服务器
- Microsoft Active Directory 服务器

  注: 如果您在 Windows 2003 上使用 Active Directory，请确保客户端系统上安装了最新的 Service Pack 和增补软件。如果您在 Windows 2008 上使用 Active Directory，请确保安装了 SP1 和以下热补丁：

  用于 KTPASS 公用程序的 **Windows6.0-KB951191-x86.msu**。如果没有此增补软件，该公用程序会生成错误 Keytab 文件。

  Windows6.0-KB957072-x86.msu，用作在 LDAP 绑定过程中使用 GSS_API 和 SSL 事务处理。
- Kerberos Key Distribution Center（与 Active Directory Server 软件一起打包）。
- DHCP 服务器（推荐）。
- DNS 服务器反向区域必须有 Active Directory 服务器和 CMC 的条目。

客户端系统

- 对于只通过智能卡的登录，客户端系统必须具有 Microsoft Visual C++ 2005 Redistributable。有关更多信息，请参阅 **www.microsoft.com/downloads/details.aspx?FamilyID= 32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- 对于单点登录或智能卡登录，客户端系统必须是 Active Directory 域和 Kerberos 领域的一部分。

CMC

- CMC 必须有固件版本 2.10 或更高版本。
- 每个 CMC 都必须有 Active Directory 帐户。
- CMC 必须是 Active Directory 域和 Kerberos 领域的一部分。

单点登录或智能卡登录的前提条件

配置 SSO 或智能卡登录的前提条件包括：

- 为 Active Directory (ksetup) 设置 kerberos 领域和密钥分发中心。
- 强健的 NTP 和 DNS 基础结构以避免时钟漂移和反向查询出现问题。
- 使用包含授权成员的 Active Directory 标准架构角色组配置 CMC。
- 对于智能卡，为每个 CMC 创建 Active Directory 用户，配置为使用 Kerberos DES 加密，而不是预验证。
- 配置浏览器实现 SSO 或智能卡登录。
- 使用 Ktpass 在密钥分发中心注册 CMC 用户（这也会将密钥上载到 CMC）。

相关链接

配置标准架构 Active Directory
配置扩展架构 Active Directory
配置浏览器以使用 SSO 登录
生成 Kerberos Keytab 文件
配置浏览器以使用智能卡登录

生成 Kerberos Keytab 文件

要支持 SSO 和智能卡登录验证，CMC 支持 Windows Kerberos 网络。ktpass 工具（Microsoft 在服务器安装 CD/DVD 中提供）用于创建与用户帐户的服务主体名称 (SPN) 绑定并将信任信息导出到 MIT-style Kerberos keytab 文件。有关 ktpass 公用程序的更多信息，请参阅 Microsoft 网站。

生成 keytab 文件之前，您必须创建一个 Active Directory 用户帐户与 ktpass 命令的 **-mapuser** 选项一起使用。您必须拥有与上载生成的 keytab 文件使用的 CMC DNS 名称相同的名称。

使用 ktpass 工具生成 keytab 文件：

1 在希望将 CMC 映射到 Active Directory 中用户帐户的域控制器（Active Directory 服务器）上运行 *ktpass* 公用程序。

2 使用以下 `ktpass` 命令创建 Kerberos keytab 文件：

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

注: RFC 要求 `cmcname.domainname.com` 必须小写，而 `@REALM_NAME` 必须大写。此外，CMC 支持 Kerberos 验证的 DES-CBC-MD5 类型的加密。

所生成的 keytab 文件必须上载到 CMC。

注: keytab 包含加密密钥，必须妥善保管。有关 *ktpass* 公用程序的更多信息，请参阅 Microsoft 网站。

配置 CMC 以使用 Active Directory 架构

有关配置 CMC 以使用 Active Directory 标准架构的信息，请参阅配置标准架构 Active Directory。
有关配置 CMC 以使用扩展架构 Active Directory 的信息，请参阅扩展架构 Active Directory 概述。

配置浏览器以使用 SSO 登录

Internet Explorer 版本 6.0 和更高版本及 Firefox 版本 3.0 和更高版本支持单点登录 (SSO)。

注: 仅当 CMC 结合 Kerberos 验证使用单点登录时，以下说明才适用。

Internet Explorer

配置 Internet Explorer 进行单点登录：

1 在 Internet Explorer 中，选择**工具** > **Internet 选项**。
2 在**安全**选项卡上的**选择要查看或更改安全设置的区域**下面，选择**本地 Intranet**。
3 单击**站点**。
此时将显示**本地 Intranet** 对话框。
4 单击**高级**。
此时将显示**本地 Intranet 高级设置**对话框。
5 在**将该网站添加到区域**中，键入 CMC 的名称和它所属的域，然后单击**添加**。

注: 您可以使用通配符 (*) 指定该域中的所有设备或用户。

Mozilla Firefox

1 在 Firefox 的地址栏中键入 about:config。

注: 如果浏览器显示这样可能会失去质保警告，请单击我保证会小心。

2 在**筛选器**文本框中，键入 negotiate。
浏览器将显示首选项名称的列表，这些名称必须包含单词 negotiate。
3 在该列表中，双击 **network.negotiate-auth.trusted-uris**。
4 在**输入字符串值**对话框中，键入 CMC 的域名并单击**确定**。

配置浏览器以使用智能卡登录

Mozilla Firefox - CMC 2.10 不支持通过 Firefox 浏览器进行智能卡登录。

Internet Explorer - 确保将 Internet Browser 配置为下载 Active-X 插件。

为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

您可以使用 CMC Web 界面或 RACADM 配置 CMC SSO 或智能卡登录。

相关链接

单点登录或智能卡登录的前提条件
上载 Keytab 文件

使用 Web 界面为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

要配置 CMC 的 Active Directory SSO 登录或智能卡登录，请执行以下操作：

注: 有关各选项的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

1 在配置 Active Directory 设置用户帐户时，请执行以下附加步骤：
- 上载 Keytab 文件。
- 要启用 SSO，请选择**启用单点登录**选项。
- 要启用智能卡登录，请选择**启用智能卡登录**选项。

注: 如果选择了此选项，所有命令行带外接口，包括 Secure Shell (SSH)、Telnet、串行和远程 RACADM 都保持不变。

2 单击**应用**。
将保存设置。
您可以使用 RACADM 命令测试使用 Kerberos 验证的 Active Directory：

```
testfeature -f adkrb -u <user>@<domain>
```

其中 `<user>` 是有效的 Active Directory 用户帐户。

命令成功表示 CMC 能够获得 Kerberos 凭据和访问用户的 Active Directory 帐户。如果命令不成功，请解决错误并再次运行该命令。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

上载 Keytab 文件

Kerberos Keytab 文件用作 CMC 对于 Kerberos Data Center (KDC) 的用户名和密码凭据，KDC 又允许访问 Active Directory。Kerberos 领域中的每个 CMC 都必须在 Active Directory 注册，而且必须有唯一的 Keytab 文件。

您可以上载在关联 Active Directory 服务器上生成的 Kerberos Keytab。您可以通过执行 **ktpass.exe** 公用程序从 Active Directory 服务器生成 Kerberos Keytab。此 keytab 会在 Active Directory 服务器和 CMC 之间建立真正的关系。

要上载 Keytab 文件，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**用户验证** > **目录服务**。
2 选择 **Microsoft Active Directory（标准架构）**。
3 在 **Kerberos Keytab** 部分，单击**浏览**，选择 keytab 文件，然后单击**上载**。
上载完成后，会显示一条消息，指出是否成功上载 keytab 文件。

使用 RACADM 为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

除了配置 Active Directory 时执行的步骤以外，还可运行以下命令启用 SSO：

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

除了配置 Active Directory 时执行的步骤以外，还可使用以下对象启用智能卡登录：

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

配置 CMC 以使用命令行控制台

本部分提供有关 CMC 命令行控制台（或串行/Telnet/Secure Shell 控制台）功能的信息，并且说明了如何设置系统以通过控制台执行系统管理操作。有关通过命令行控制台在 CMC 中使用 RACADM 命令的信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

主题：

相关链接

使用串行、Telnet 或 SSH 控制台登录 CMC

CMC 命令行控制台功能

CMC 支持以下串行、Telnet 和 SSH 控制台功能：

- 一个串行客户端连接和最多四个并发 Telnet 客户端连接。
- 最多四个并发 Secure Shell (SSH) 客户端连接。
- RACADM 命令支持。
- 内置 connect 命令连接到服务器和 I/O 模块的串行控制台；也可用作 `racadm connect`。
- 命令行编辑和历史。
- 在所有控制台界面上的会话超时控制。

CMC 命令行命令

当连接到 CMC 命令行时，可以输入这些命令：

表. 32: CMC 命令行命令

命令	说明
`racadm`	RACADM 命令以关键字 `racadm` 开头，后接一个子命令。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line*

命令	说明
	Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。
`connect`	连接到服务器或 I/O 模块的串行控制台。有关更多信息，请参阅使用 Connect 命令连接到服务器或 I/O 模块。 **注: 您还可以使用 racadm `connect` 命令。**
`exit`、`logout` 和 `quit`	所有这些命令都执行相同操作：结束当前会话并返回一个登录提示符。

将 Telnet 控制台与 CMC 配合使用

一次最多可以将四个 Telnet 会话与 CMC 配合使用。

如果管理站在运行 Microsoft Windows XP 或 Microsoft Windows Server 2003，则可能会在 CMC Telnet 会话中遇到字符问题。此问题会以冻结登录的方式发生，在这种情况下，回车键无响应并且不显示密码提示。

要解决此问题，从 **support.microsoft.com** 下载热修复程序 824810。有关更多信息，也可参阅 Microsoft 知识库文章 824810。

在命令行界面中，您可以使用 racadm 命令 `racadm getconfig -g cfgSessionManagement` 管理会话超时。有关更多信息，请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

将 SSH 与 CMC 配合使用

SSH 是一个命令行会话，包含与 Telnet 会话相同的功能，但还具有会话协商和用于提高安全性的加密功能。CMC 支持 SSH 版本 2 和密码验证。CMC 上默认已启用 SSH。

注: CMC 不支持 SSH 版本 1。

在 CMC 登录过程中出现错误时，SSH 客户端会发出错误消息。此消息文本取决于客户端，不受 CMC 控制。查看 RACLog 消息以确定故障原因。

注: `OpenSSH` 必须从 Windows 上的 VT100 或 ANSI 终端仿真程序运行。您也可以使用 Putty.exe 运行 `OpenSSH`。通过 Windows 命令提示符运行 `OpenSSH` 不会提供完整的功能（即，有些键不响应并且不显示任何图形）。对于运行 Linux 的系统，运行 SSH 客户端服务可以使用任何 Shell 连接 CMC。

支持一次同时运行四个 SSH 会话。会话超时由 `cfgSsnMgtSshIdleTimeout` 属性控制。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）*中的“数据库属性”一章、Web 界面上的 **Services Management（服务管理）**页面或者参阅配置服务。

CMC 还支持通过 SSH 的公共密钥验证 (PKA)。此验证方法不再需要嵌入或提示用户 ID/密码，从而提高了 SSH 脚本编写的自动化程度。有关更多信息，请参阅配置通过 SSH 的公共密钥验证。

SSH 默认已启用。如果禁用了 SSH，可使用任何其他支持的界面启用。

要配置 SSH，请参阅配置服务。

相关链接

配置服务

支持的 SSH 加密方案

要使用 SSH 协议与 CMC 通信，它支持下表中列出的多种加密方案。

表. 33: 加密方案

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

配置通过 SSH 的公共密钥验证

最多可以配置 6 个公共密钥，可通过 SSH 接口将这些公共密钥与服务用户名结合使用。添加或删除公共密钥之前，务必使用查看命令查看已设置了什么密钥，这样就不会无意覆盖或删除密钥。服务用户名是在通过 SSH 访问 CMC 时可以使用的特殊用户帐户。在设置和正确使用通过 SSH 的 PKA 时，无需输入用户名或密码即可登录到 CMC。这对于设置自动脚本来执行各种功能非常有用。

注: 不支持使用任何 GUI 管理此功能；您只能使用 RACADM。

添加新公共密钥时，确保现有密钥不位于添加新密钥的索引处。CMC 不检查在添加新密钥之前是否删除了以前的密钥。添加了新密钥后，只要启用了 SSH 接口，新密钥就自动生效。

使用公共密钥的公共密钥注释部分时，请记住 CMC 仅使用前 16 个字符。在使用 RACADM `getssninfo` 命令时，CMC 使用公共密钥注释区分 SSH 用户，因为所有 PKA 用户均使用服务用户名登录。

例如，如果设置了两个公共密钥，一个公共密钥的注释是 PC1，另一个的注释是 PC2：

```
racadm getssninfo
Type       User   IP Address   Login
Date/Time
SSH        PC1    x.x.x.x      06/16/2009
09:00:00
SSH        PC2    x.x.x.x      06/16/2009
09:00:00
```

有关 `sshpkauth` 的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

相关链接

生成在 Windows 系统中使用的公共密钥
生成在 Linux 系统中使用的公共密钥
CMC 的 RACADM 语法注释
查看公共密钥
添加公共密钥
删除公共密钥

生成在 Windows 系统中使用的公共密钥

在添加帐户之前，通过 SSH 访问 CMC 的系统需要公共密钥。有两种方法可生成公共/私人密钥对：对于运行 Windows 的客户端使用 PuTTY Key Generator 应用程序，对于运行 Linux 的客户端使用 ssh-keygen CLI。

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

要使用 PuTTY 密钥生成器为运行 Windows 客户端的系统创建基本密钥，请执行以下操作：

1 启动应用程序，根据要生成的密钥类型（不支持 SSH-1）选择 SSH-2 RSA。

2 输入密钥的位数。请确保 RSA 密钥大小介于 1024 和 4096 之间。

注:

- 如果您添加的密钥小于 1024 或大于 4096 位，CMC 可能不会显示消息，但在您尝试使用这些密钥登录时，这些密钥会失效。
- CMC 接受的 RSA 密钥的强度最多为 4096，但建议的密钥强度为 1024 位。

3 单击**生成**，按指示在窗口中移动鼠标。

创建密钥后，您可以修改密钥注释字段。

还可以输入密码短语，来保证密钥的安全。确保将私人密钥保存起来。

4 使用公共密钥时，有两个选项：
- 将公共密钥保存到文件中以便稍后上载。
- 使用文本选项添加帐户时，从**供粘贴的公共密钥**窗口中复制和粘贴文本。

生成在 Linux 系统中使用的公共密钥

适用于 Linux 客户端的 ssh-keygen 应用程序是不带图形用户界面的命令行工具。打开终端窗口，然后在 Shell 提示符处键入：

```
ssh-keygen –t rsa –b 2048 –C testing
```

其中，

`–t` 必须是 rsa。

`–b` 指定介于 2048 和 4096 之间的加密位数。

`–c` 允许修改公共密钥注释，该选项是可选的。

`<passphrase>` 是可选的。命令完成后，使用公共文件传递到 RACADM 以便上载文件。

CMC 的 RACADM 语法注释

在使用 `racadm sshpkauth` 命令时确保：

- 对于 –i 选项，参数必须为 svcacct。-i 的所有其他参数都会在 CMC 中失败。svcacct 是 CMC 中通过 SSH 的公共密钥验证的特殊帐户。
- 若要登录到 CMC，用户必须为服务。其他类别的用户可使用 sshpkauth 命令访问输入的公共密钥。

查看公共密钥

要查看已经添加到 CMC 的公共密钥，请键入：

```
racadm sshpkauth –i svcacct –k all –v
```

要一次仅查看一个密钥，请将 all 替换为 1-6 中的一个数字。例如，要查看密钥 2，请键入：

```
racadm sshpkauth –i svcacct –k 2 –v
```

添加公共密钥

要使用文件上载 -f 选项将公共密钥添加至 CMC，请键入：

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –f <public key file>
```

注: 只有远程 RACADM 才允许使用文件上载选项。有关更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

要使用文本上载选项添加公共密钥，请键入：

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –t “<public key text>”
```

删除公共密钥

要删除公共密钥，请键入：

```
racadm sshpkauth –i svcacct –k 1 –d
```

要删除所有公共密钥，请键入：

```
racadm sshpkauth –i svcacct –k all –d
```

启用前面板至 iKVM 的连接

有关使用 iKVM 前面板端口的信息和说明，请参阅启用或禁用从前面板到 iKVM 的访问

配置终端仿真软件

CMC 支持在运行以下一种终端仿真软件的管理台上使用串行文本控制台：

- Linux Minicom。
- Hilgraeve's HyperTerminal Private Edition（版本 6.3）。

执行以下小节中的步骤以配置所需类型的终端软件。

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。其他 Minicom 版本的配置步骤可能略有不同，但需要相同的基本设置。要配置 Minicom 的其他版本，请参阅必需的 Minicom 设置部分中的信息。

配置 Minicom 版本 2.0

注: 为了获得最佳效果，将 cfgSerialConsoleColumns 属性设置为与列数匹配。请注意，提示符会占用两个字符。例如，对于 80 列的终端窗口：

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80。
```

1 如果没有 Minicom 配置文件，请转至下一步。如果您有 Minicom 配置文件，请键入 `minicom<Minicom config file name>` 并跳到步骤 12。

2 在 Linux 命令提示符处，键入 `minicom -s`。

3 选择**串行端口设置**并按 <Enter> 键。

4 按 <a> 并选择相应的串行设备（例如，`/dev/ttyS0`）。

5 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 **115200 8N1**。

6 按 <f>，然后将**硬件流量控制**设置为**是**，将**软件流量控制**设计为**否**。要退出**串行端口设置**菜单，请按 <Enter>。

7 选择**调制解调器和拨号**并按 <Enter>。

8 在**调制解调器拨号和参数设置**菜单中，按 <Backspace> 清除**初始化**、**重设**、**连接**和**挂断**设置以使它们保留为空白，然后按 <Enter> 保存每个空白值。

9 清除完所有指定字段后，按 <Enter> 退出**调制解调器拨号和参数设置**菜单。

10 选择**从 Minicom 退出**并按 <Enter>。

11 在命令解释程序提示符下，键入 `minicom <Minicom config file name>`。

12 按 <Ctrl> 加 <a>、<x> 或 <Enter> 键退出 Minicom。

确保 **Minicom** 窗口显示登录提示。如果显示登录提示，说明连接成功。您就可以立即登录和访问 CMC 命令行界面了。

必需的 Minicom 设置

请参阅下表来配置任何版本的 Minicom。

表. 34: 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）	115200 8N1
硬件流量控制	是
软件流量控制	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。

使用 Connect 命令连接到服务器或输入输出模块

CMC 可建立一个连接，以重定向服务器或 I/O 模块的串行控制台。

对于服务器，串行控制台重定向可以使用以下方法完成：

- `racadm connect` 命令。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）*。
- iDRAC Web 界面串行控制台重定向功能。

- iDRAC Serial Over LAN (SOL) 功能。

在串行、Telnet、SSH 控制台中，CMC 支持通过 connect 命令建立到服务器或 IOM 模块的串行连接。服务器串行控制台中包含 BIOS 引导和设置屏幕以及操作系统串行控制台。对于 I/O 模块，交换机串行控制台可用。

小心: 从 CMC 串行控制台执行操作时，`connect -b` 选项将保持连接状态，直到 CMC 重设。此连接具有潜在的安全风险。

注: `connect` 命令可提供 `–b`（二进制）选项。`–b` 选项可传递原始二进制数据，并且 `cfgSerialConsoleQuitKey` 将不会使用。此外，当使用 CMC 串行控制台连接到一个服务器时，DTR 信号中的过渡（例如，如果卸下串行电缆以连接到调试器）不会导致注销。

注: 如果某个 IOM 不支持控制台重定向，此 `connect` 命令将会显示空白的控制台。在这种情况下，要返回到 CMC 控制台，请键入转义序列。默认控制台转义序列是 <CTRL><\>。

管理系统上最多有六个 IOM。要连接到 IOM，请执行以下命令：

```
connect switch-n
```

其中 `n` 为 IOM 标签 A1、A2、B1、B2、C1 和 C2。

（请参阅图 13-1 获得在机箱中安放 IOM 的图示说明。）当在 connect 命令中引用 IOM 时，IOM 将按照下表所示映射到交换机。

表. 35: 将 I/O 模块映射到交换机

I/O 模块标签	Switch（交换机）
A1	交换机 a1 或交换机 1
A2	交换机 a2 或交换机 2
B1	交换机 b1 或交换机 3
B2	交换机 b2 或交换机 4
C1	交换机 c1 或交换机 5
C2	交换机 c2 或交换机 6

注: 每个机箱每次只能有一个 IOM 连接。

注: 不能从串行控制台连接到直通设备。

要连接到受管服务器串行控制台，请使用命令 `connect server-<n><x>`，其中 *n* 是 1-8，而 *x* 是 a、b、c 或 d。您还可以使用 `racadm connect server-n` 命令。使用 `-b` 选项连接服务器时，假定为二进制通信并且转义字符已禁用。如果 iDRAC 不可用，您会看到 `No route to host` 错误消息。

`connect server-n` 命令使用户能够访问服务器的串行端口。建立此连接后，用户能够通过 CMC 串行端口查看服务器控制台重定向，该端口既包括 BIOS 串行控制台，也包括操作系统串行控制台。

注: 要查看 BIOS 引导屏幕，必须在服务器的 BIOS 设置中启用串行重定向。此外，必须将终端仿真程序窗口设置为 80x25。否则屏幕上会出现乱码。

注: 在 BIOS 设置屏幕中，并非所有键都起作用，因此需提供针对 CTRL+ALT+DEL 的相应转义序列和其他转义序列。。初始重定向屏幕显示所需的转义序列。

相关链接

为串行控制台重定向配置管理服务器 BIOS
配置 Windows 进行串行控制台重定向
配置 Linux 在引导期间进行服务器串行控制台重定向
配置 Linux 在引导后进行服务器串行控制台重定向

为串行控制台重定向配置管理服务器 BIOS

需要使用 iKVM 连接到管理服务器（请参阅使用 iKVM 管理服务器）或通过 iDRAC Web 界面建立远程控制台会话（请参阅 **dell.com/support/manuals** 上提供的 *iDRAC User's Guide*（iDRAC 用户指南））。

默认情况下，BIOS 中的串行通信为 OFF（关）。要将主机文本控制台数据重定向到 Serial over LAN，必须启用通过 COM1 进行控制台重定向。要更改 BIOS 设置，请执行以下操作：

1 引导管理务器。
2 在开机自检过程中，按 <F2> 进入 BIOS 设置公用程序。
3 向下滚动到**串行通信**并按 <Enter>。在弹出对话框中，串行通信列表显示以下选项：
   - 关
   - 开，不进行控制台重定向
   - 开，通过 COM1 进行控制台重定向

   可使用箭头键在这些选项之间导航。
4 确保启用了 **开，通过 COM1 进行控制台重定向**。
5 启用**引导后重定向**，默认值为**禁用**。选择此选项可在后续重新引导后进行 BIOS 控制台重定向。
6 保存更改并退出。
   管理服务器重新引导。

配置 Windows 进行串行控制台重定向

对于运行 Microsoft Windows Server（Windows Server 2003 以上版本）的服务器，不必进行任何配置。Windows 会接收来自 BIOS 的信息，并启用特别管理控制台 (SAC) 的一号控制台 COM1。

配置 Linux 在引导期间进行服务器串行控制台重定向

以下步骤特定于 Linux GRand Unified Bootloader (GRUB)。使用不同的引导加载程序需要类似的更改。

注: 在配置客户端 VT100 仿真窗口时，将显示重定向控制台的窗口或应用程序设置为 25 行 x 80 列以确保文本正确显示；否则，有些文本屏幕可能会出现乱码。

按照以下说明编辑 /etc/grub.conf 文件：

1 找到文件的常规设置部分并添加以下两行新命令：
```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```
2 在内核行上追加两个选项：
```
kernel console=ttyS1,57600
```
3 如果 /etc/grub.conf 包含 `splashimage` 指令，应将其注释掉。
   以下示例显示了此过程中说明的更改。
```
# 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 initrd /boot/initrd-2.4.9-e.3.img
```

按照以下原则编辑 /etc/grub.conf 文件：

- 禁用 GRUB 的图形界面并使用基于文本的界面。否则，GRUB 屏幕不会在控制台重定向中显示。要禁用图形界面，请注释掉以 `splashimage` 开头的行。
- 要使用多个 GRUB 选项来通过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
  ```

  此示例显示 `console=ttyS1,57600` 仅添加到第一个选项。

配置 Linux 在引导后进行服务器串行控制台重定向

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
```

下例显示了带有新行的文件。

```
# # 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
```

以下示例显示带有新增行的示例文件。

```
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
```

12

使用 FlexAddress 和 FlexAdress Plus 卡

此部分提供有关 FlexAddress 和 FlexAddress Plus 卡、以及如何配置和使用这些卡的信息。

主题：

相关链接

关于 FlexAddress
关于 FlexAddress Plus
FlexAddress 和 FlexAddress Plus 比较

关于 FlexAddress

如果更换服务器，给定服务器插槽的插槽 FlexAddress 将保持不变。如果将服务器插入新的插槽或机箱，则使用服务器分配的 WWN/MAC，除非该机箱已为新插槽启用 FlexAddress 功能。如果卸下服务器，它将还原为服务器分配的地址。无需重新配置各结构的部署框架、DHCP 服务器和路由器即可识别该新服务器。

在生产过程中，每个服务器模块都被分配了唯一的 WWN 和/或 MAC ID。在使用 FlexAddress 之前，如果需要使用另一个模块替换某个服务器模块，则 WWN/MAC ID 将会更改，并且需要重新配置以太网管理工具和 SAN 资源以标识新的服务器模块。

FlexAddress 允许 CMC 将 WWN/MAC ID 分配给特定的插槽并覆盖出厂 ID。因此，如果更换了服务器模块，则基于插槽的 WWN/MAC ID 保留不变。使用此功能便不需要为新服务器模块重新配置以太网网络管理工具和 SAN 资源。

此外，*覆盖*操作仅在将服务器模块插入支持 FlexAddress 的机箱时发生；对服务器模块没有进行永久性更改。如果服务器模块移到不支持 FlexAddress 的机箱，则使用出厂分配的 WWN/MAC ID。

FlexAddress 功能卡包含一个 MAC 地址范围。安装 FlexAddress 之前，可以通过将 SD 卡插入 USB 内存读卡器并查看文件 **pwwn_mac.xml** 来确定 FlexAddress 功能卡上包含的 MAC 地址范围。SD 卡上的该明文 XML 文件包含一个 XML 标签 *mac_start*，它

代表用于该唯一 MAC 地址范围的第一个起始十六进制 MAC 地址。而 *mac_count* 标签是 SD 卡可以分配的 MAC 地址总数。已分配的总 MAC 范围可以根据以下公式计算：

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

其中 208 是 *mac_count*，公式为：

```
<mac_start> + <mac_count>  - 1 = <mac_end>
```

例如：

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

注: 将 SD 卡插入 USB 内存读卡器之前先锁定 SD 卡，防止意外修改其中的任何内容。将 SD 卡插入 CMC 前，您*必须解除锁定*。

关于 FlexAddress Plus

FlexAddress Plus 是 2.0 版功能卡中的新增功能。它是 FlexAddress 功能卡 1.0 版的升级。FlexAddress Plus 的 MAC 地址多于 FlexAddress 功能。两个功能都允许机箱分配全局名称/介质访问控制 (WWN/MAC) 地址到光纤通道和以太网设备。机箱分配的 WWN/MAC 地址全局唯一且特定于服务器插槽。

FlexAddress 和 FlexAddress Plus 比较

FlexAddress 有 208 个地址分配到 16 个服务器插槽，因此每个插槽分配有 13 个 MAC 地址。

FlexAddress Plus 有 2928 个地址分配到 16 个服务器插槽，因此每个插槽分配有 183 个 MAC 地址。

下表显示了两种功能下分别提供的 MAC 地址。

表. 36: 在 FlexAddress 和 FlexAddress Plus 中预配置的 MAC 地址

	结构 A	结构 B	结构 C	iDRAC 管理	MAC 总数
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

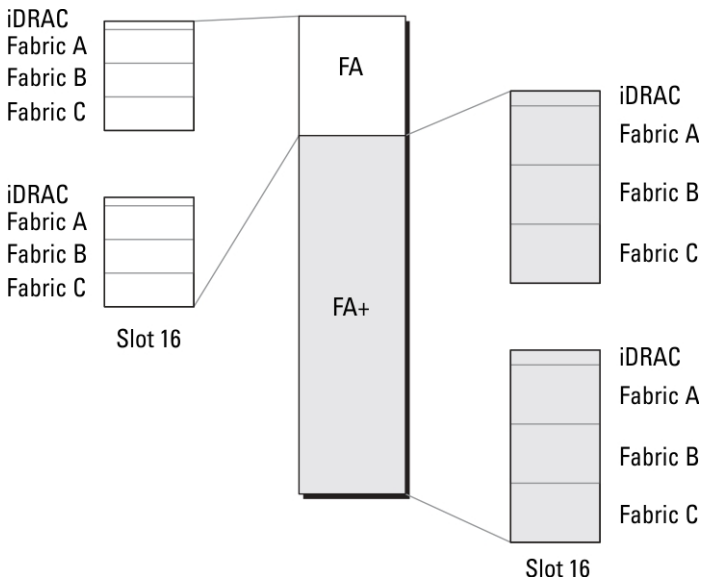


图 12: FlexAdress (FA) 和 FlexPlusAddress (FA+) 功能对比

激活 FlexAddress

安全数字 (SD) 卡上提供了 FlexAddress，必须将该卡插入 CMC 才能激活此功能。要激活 FlexAddress 功能，可能需要软件更新；如果不激活 FlexAddress，就不需要这些更新。下表中列出的更新包括服务器模块 BIOS、I/O 夹层 BIOS 或固件，以及 CMC 固件。必须应用这些更新才能启用 FlexAddress。如果没有应用这些更新，则 FlexAddress 功能可能无法按照预期方式工作。

表. 37: 激活 FlexAddress 的最低软件版本。

组件	最低要求版本
以太网夹层卡 - Broadcom M5708t，5709，5710	• 引导代码固件 4.4.1 或更高版本 • iSCSI 引导固件 2.7.11 或更高版本 • PXE 固件 4.4.3 或更高版本
FC 夹层卡 - QLogic QME2472，FC8	BIOS 2.04 或更高版本
FC 夹层卡 - Emulex LPe1105-M4，FC8	BIOS 3.03a3 和固件 2.72A2 或更高版本
服务器模块 BIOS	• PowerEdge M600 - BIOS 2.02 或更高版本 • PowerEdge M605 - BIOS 2.03 或更高版本 • PowerEdge M805 • PowerEdge M905 • PowerEdge M610 • PowerEdge M710 • PowerEdge M710hd
PowerEdgeM600/M605 主板上的 LAN (LOM)	• 引导代码固件 4.4.1 或更高版本 • iSCSI 引导固件 2.7.11 或更高版本
iDRAC	• 对于 PowerEdge xx0x 系统，为版本 1.50 或更高版本 • 对于 PowerEdge xx1x 系统，为版本 2.10 或更高版本

组件	最低要求版本
CMC	版本 1.10 或更高版本

注: 2008 年 6 月以后订购的任何系统都拥有正确的固件版本。

为了保证正确部署 FlexAddress 功能，请按以下顺序更新 BIOS 和固件：

1 更新所有夹层卡固件和 BIOS。
2 更新服务器模块 BIOS。
3 更新服务器模块上的 iDRAC 固件。
4 更新机箱中的所有 CMC 固件；如果存在冗余 CMC，则保证两个 CMC 的固件都得到更新。
5 将 SD 卡插入被动模块中以获得冗余 CMC 模块系统，或插入单个 CMC 模块中以获得非冗余系统。

注: 如果未安装支持 FlexAddress 的 CMC 固件（版本 1.10 或更高版本），则无法激活此功能。

有关 SD 卡的安装说明，请参阅 *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*（Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范）说明文件。

注: SD 卡含有 FlexAddress 功能。SD 卡上含有的数据经过加密，不能以任何方式复制或修改，因为会禁止系统功能并导致系统出现故障。

注: 一张 SD 卡只能用于一个机箱。如果有多个机箱，则必须购买额外的 SD 卡。

FlexAddress 功能将在安装有 SD 功能卡的 CMC 重新启动后自动激活；激活后会将此功能绑定到当前机箱。如果在冗余 CMC 中已安装 SD 卡，则直到冗余 CMC 激活时才会激活 FlexAddress 功能。有关如何激活冗余 CMC 的信息，请参阅 *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*（Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范）说明文件。

在 CMC 重新启动时，验证激活过程。有关更多信息，请参阅验证 FlexAddress 激活。

激活 FlexAddress Plus

FlexAddress Plus 在 FlexAddress Plus 安全数字 (SD) 卡上随 FlexAddress 功能一起提供。

注: 标有 FlexAddress 的 SD 卡仅包含 FlexAddress，标有 FlexAddress Plus 的卡包含 FlexAddress 和 FlexAddress Plus。必须将卡插入 CMC 才能激活此功能。

某些服务器（如 PowerEdge M710HD）需要的 MAC 地址数可能超过 FA 可以提供给 CMC 的地址数，具体取决于其配置方式。对于这些服务器来说，升级到 FA+ 可得到 WWN/MAC 配置的全面优化。请联系 Dell 获得 FlexAddress Plus 功能的支持。

若要激活 FlexAddress Plus 功能，则要求更新以下软件：服务器 BIOS、服务器 iDRAC 和 CMC 固件。如果不应用这些更新，则只有 FlexAddress 功能可用。有关这些组件需要的最低版本的信息，请参阅 **dell.com/support/manuals** 上的 *Readme*（自述文件）。

验证 FlexAddress 激活

使用以下 RACADM 命令验证 SD 功能卡及其状态：

```
racadm featurecard -s
```

表. 38: 通过 featurecard -s 命令返回状态消息

状态消息	操作
No feature card inserted.	检查 CMC 以验证 SD 卡是否已正确插入。在冗余 CMC 配置中，确保安装了 SD 功能卡的 CMC 是活动 CMC，而不是待机 CMC。
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis.（插入的功能卡有效并包含以下功能 FlexAddress：功能卡绑定到此机箱。）	无需任何操作。
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to another chassis, svctag = ABC1234, SD card SN = 01122334455（插入的功能卡有效并包含以下功能 FlexAddress：功能卡绑定到另一个机箱，svctag = ABC1234，SD 卡 SN = 01122334455）	移除 SD 卡；找到当前机箱的 SD 卡并进行安装。
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is not bound to any chassis.（插入的功能卡有效并包含以下功能 FlexAddress：功能卡未绑定到任何机箱。）	功能卡可以移到另一个机箱或在当前机箱上重新激活。要在当前机箱上重新激活，请输入 `racadm racreset`，直到安装了功能卡的 CMC 模块变为活动为止。

使用以下 RACADM 命令显示机箱上所有激活的功能：

```
racadm feature -s
```

该命令返回以下状态消息：

```
Feature = FlexAddress
Date Activated = 8 April 2008 - 10:39:40
Feature installed from SD-card SN = 01122334455
```

如果机箱中没有活动的功能，则此命令将返回消息：

```
racadm feature -s
No features active on the chassis
```

Dell 功能卡可包含多个的功能。一旦 Dell 功能卡上的所有功能都已在一个机箱上激活，则 Dell 功能卡上所有其他功能都不能在其他机箱上激活。在此情况下，racadm feature -s 命令会显示受到影响的功能的以下消息：

```
ERROR: One or more features on the SD card are active on another chassis
```

有关 **feature** 和 **featurecard** 命令的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

停用 FlexAddress

使用 RACADM 命令可以停用 FlexAddress 功能，并将 SD 卡还原到安装前的状态。Web 界面中没有停用功能。停用功能将把 SD 卡还原到原始状态，以便可以在另一个机箱上安装并激活。在本段落中，FlexAddress 一词指 FlexAddress 和 FlexAddressPlus。

注: SD 卡必须实际安装在 CMC 中，并且在执行停用命令之前必须关闭机箱电源。

如果在未安装卡时执行停用命令，或者对安装在不同机箱上的卡执行该命令，则会停用该功能且不会对该卡进行任何更改。

要停用 FlexAddress 功能并还原 SD 卡，请执行以下操作：

```
racadm feature -d -c flexaddress
```

如果成功停用，该命令将返回以下状态消息：

```
feature FlexAddress is deactivated on the chassis successfully.
```

如果在执行命令前未关闭机箱电源，则该命令会失败并出现以下错误消息：

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

有关该命令的详情，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 **feature** 命令部分。

配置 FlexAddress

FlexAddress 是一种可选升级，它允许服务器模块使用由机箱提供的 WWN/MAC ID 替换工厂分配的 WWN/MAC ID。

注: 在此部分，FlexAddress 一词还指 FlexAddress Plus。

您必须购买和安装 FlexAddress 升级才可以配置 FlexAddress。如果尚未购买和安装升级，Web 界面上会显示以下文本：

```
Optional feature not installed. See the Dell Chassis Management Controller Users Guide for
information on the chassis-based WWN and MAC address administration feature. To purchase this
feature, please contact Dell at www.dell.com.
```

如果随机箱购买了 FlexAddress，则系统开机时，该功能已安装并且已激活。如果单独购买 FlexAddress，则必须按照 **dell.com/support/manuals** 上 *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*（Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范）说明文件中的说明安装 SD 功能卡。

开始配置前必须关闭服务器。可以基于每个结构启用或禁用 FlexAddress。此外，还可以基于每个插槽启用或禁用该功能。在基于每个结构启用该功能后，可以选择要启用的插槽。例如，如果已启用结构 A，则启用的任何插槽将仅在结构 A 上启用 FlexAddress。所有其他结构都使用服务器上工厂分配的 WWN/MAC。

选定的插槽会为所有已启用的结构启用 FlexAddress。例如，如果启用结构 A 和 B，要在结构 A 的插槽 1 上启用 FlexAddress，而不在结构 B 的插槽 1 上启用 FlexAddress，这是不可能的。

注: 确保在更改结构级别（A、B、C 或 DRAC）FlexAddress 之前刀片服务器已关机。

相关链接

LAN 唤醒和 FlexAddress
为机箱级结构和插槽配置 FlexAddress
为服务器级插槽配置 FlexAddress
用于 Linux 的其他 FlexAddress 配置

LAN 唤醒和 FlexAddress

首次部署 FlexAddress 功能时，必须在服务器模块上完成电源关闭和电源打开顺序，FlexAddress 才会生效。以太网设备上的 FlexAddress 由服务器模块的 BIOS 编程。为了使服务器模块的 BIOS 能够对地址进行编程，它必须处于运行状态，这需要打开服务器模块的电源。当电源关闭和电源打开顺序完成后，机箱分配的 MAC ID 可用于 LAN 唤醒 (WOL) 功能。

为机箱级结构和插槽配置 FlexAddress

在机箱级别，可以启用或禁用结构和插槽的 FlexAddress 功能。FlexAddress 在每个结构的基础上启用，然后选择参与该功能的插槽。必须启用结构和插槽才能成功配置 FlexAddress。

使用 CMC Web 界面为机箱级结构和插槽配置 FlexAddress

要使用 CMC Web 界面启用或禁用结构和插槽以便使用 FlexAddress 功能，请执行以下操作：

1 在系统树中，转至**服务器概览**，然后单击**设置** > **FlexAddress**。
此时将显示**部署 FlexAddress** 页。

2 在**为机箱分配的 WWN/MAC 选择结构**部分，选择要启用 FlexAddress 的结构类型。要将其禁用，清除此选项即可。

注: 如果没有选择结构，则不会为选择的插槽启用 FlexAddress。

此时将显示**为机箱分配的 WWN/MAC 选择插槽**页。

3 为要启用 FlexAddress 的插槽选择**启用**选项。要将其禁用，清除此选项即可。

注: 如果插槽中有服务器，请先将其关闭，然后再在该插槽上启用 FlexAddress 功能。

注: 如果没有选择插槽，则不会为选择的结构启用 FlexAddress。

4 单击**应用**保存更改。
有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

使用 RACADM 为机箱级结构和插槽配置 FlexAddress

要启用或禁用结构，请使用以下 RACADM 命令：

```
racadm setflexaddr [-f <fabricName> <state>]
```

其中，*<fabricName>* = A、B、C or iDRAC，*<state>* = 0 or 1

0 表示禁用，1 表示启用。

要启用或禁用插槽，请使用以下 RACADM 命令：

```
racadm setflexaddr [-i <slot#> <state>]
```

其中， *<slot#>* = 1 or 16， *<state>* = 0 or 1

0 表示禁用，1 表示启用。

有关 **setflexaddr** 命令的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

为服务器级插槽配置 FlexAddress

在服务器级别，可以启用或禁用单个插槽的 FlexAddress 功能。

使用 CMC Web 界面为服务器级插槽配置 FlexAddress

要使用 CMC Web 界面启用或禁用单个插槽以使用 FlexAddress 功能，请执行以下操作：

1 在系统树中，展开**服务器概述**。
展开的**服务器**列表中出现的所有服务器 (1-16)。

2 单击想要查看的服务器。

此时将显示**服务器状态**页。

3 单击**设置**选项卡和 **FlexAddress** 子选项卡。

此时将显示 **FlexAddress** 页。

4 从**已启用 FlexAddress** 下拉菜单中，选择**是**启用 FlexAddress，或选择**否**禁用 FlexAddress。

5 单击**应用**保存更改。

有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

使用 RACADM 为服务器级插槽配置 FlexAddress

要使用 RACADM 为服务器级插槽配置 FlexAddress，请执行以下操作：

```
racadm setflexaddr [-i <slot#> <state>] [-f <fabricName> <state>]
```

其中，`<slot#> = 1 到 16`

`<fabricName> = A、B、C`

`<state> = 0 或 1`

0 表示禁用，1 表示启用。

用于 Linux 的其他 FlexAddress 配置

当在基于 Linux 操作系统上将服务器分配的 MAC ID 更改到机箱分配的 MAC ID 时，可能需要其他配置步骤：

- SUSE Linux Enterprise Server 9 和 10：您可能需要在 Linux 系统上运行 Yet Another Setup Tool (YAST) 来配置网络设备，然后重新启动网络服务。
- Red Hat Enterprise Linux 4 和 Red Hat Enterprise Linux 5：运行 Kudzu，该公用程序用于检测和配置系统上的新硬件或更改的硬件。Kudzu 显示“硬件发现菜单”，卸下硬件和添加新硬件时，它会检测 MAC 地址变化。

查看 WWN 或 MAC 地址信息

您可以查看每个服务器插槽或机箱中所有服务器的网络适配器虚拟地址资源清册。虚拟地址资源清册包含以下各项：

- 结构配置

  注：
  - 结构 A 显示所安装输入/输出结构的类型。如果启用结构 A，未填充的插槽会显示结构 A 的机箱分配 MAC 地址。
  - iDRAC 管理控制器不是结构，但其 FlexAddress 被视作结构。
  - 组件的复选标记表示 FlexAddress 或 FlexAddressPlus 启用了该结构。
- 正在 NIC 适配器端口上使用的协议。例如，LAN、iSCSI、FCoE 等。
- 机箱中插槽的光纤信道全局名称 (WWN) 配置和介质访问控制 (MAC) 地址。
- MAC 地址分配类型和当前的活动地址类型 — 服务器分配、FlexAddress 或 I/O 标识 MAC。黑色复选标记表示活动地址类型，可以是服务器分配、机箱分配或远程分配。
- 支持分区的设备的 NIC 分区之状态。

您可以使用 Web 界面或 RACADM CLI 查看 WWN/MAC 地址资源清册。根据界面，您可以筛选 MAC 地址并了解用于该功能或分区的 WWN/MAC 地址。如果适配器已启用 NPAR，您可以查看哪些分区已启用或已禁用。

使用 Web 界面，您可以使用 **FlexAddress** 页面（单击 **Server Overview（服务器概览）** > **Slot <x>（插槽 <x>）** > **Setup（设置）** > **FlexAddress**）查看特定插槽的 WWN/MAC 地址信息。您可以使用 **WWN/MAC Summary（WWN/MAC 摘要）**页面（单击 **Server**

Overview（服务器概览） > **Properties（属性）** > **WWN/MAC**）查看所有插槽的 WWN/MAC 地址信息。从这两个页面，您可以在基本模式或高级模式下查看 WWN/MAC 地址信息：

- **基本模式** — 在此模式中，您可以查看服务器插槽、结构、协议、WWN/MAC 地址和分区状态。仅 WWN/MAC 地址字段中显示活动 MAC 地址。您可使用任何或所有显示的字段进行筛选。
- **高级模式** - 在此模式下，您可以查看基本模式下显示的所有字段以及所有 MAC 类型（服务器分配、Flex Address 和 IO 标识）。您可使用任何或所有显示的字段进行筛选。

在基本模式和高级模式下，WWN/MAC 地址信息均折叠显示。单击插槽的 或单击 **Expand/Collapse All（全部展开/折叠）**查看特定插槽或所有插槽的信息。

您还可以将机箱中所有服务器的 WWN/MAC 地址信息导出到本地文件夹。

有关各字段的信息，请参阅*联机帮助*。

使用 Web 界面查看基本 WWN 或 MAC 地址信息

要查看机箱中每个服务器插槽或所有服务器的 WWN/MAC 地址信息，在基本模式下：

1 单击**服务器概览** > **属性** > **WWN/MAC**。

此时 **WWN/MAC 摘要**页面将显示 WWN/MAC 地址信息。

或者，单击 **Server Overview（服务器概览）** > **Slot <x>（插槽 <x>）** > **Setup（设置）** > **FlexAddress** 查看特定服务器插槽的 WWN/MAC 地址信息。此时将显示 **FlexAddress** 页。

2 在 **WWN/MAC 地址**表中，单击**导出**以本地保存 WWN/MAC 地址。

3 单击插槽的 或单击 **Expand/Collapse All（全部展开/折叠）**以展开或折叠为 WWN/MAC 地址表中特定插槽或所有插槽列出的属性。

4 从**视图**下拉菜单中，选择**基本**以查看树形视图中的 WWN/MAC 地址属性。

5 从**服务器插槽**下拉菜单中，选择**所有服务器**或特定插槽以分别查看所有服务器或仅特定插槽中服务器的 WWN/MAC 地址属性。

6 从**结构**下拉菜单中，选择结构类型之一以查看与服务器关联的所有或特定类型的管理或 I/O 结构的详细信息。

7 从**协议**下拉菜单中，选择**所有协议**或其中一个列出的网络协议，以查看所有 MAC 地址或与选定协议相关联的 MAC 地址。

8 在 **WWN/MAC 地址**字段中，输入 MAC 地址以仅查看与特定 MAC 地址关联的插槽。或者，部分输入 MAC 地址条目以查看关联的插槽。例如，输入 4A 以查看 MAC 地址中包含 4A 的插槽。

9 从**分区状态**下拉菜单中，选择分区状态以显示具有所选分区状态的服务器。

如果特定分区被禁用，显示此分区的行将呈灰色显示。

有关各字段的信息，请参阅*联机帮助*。

使用 Web 界面查看高级 WWN 或 MAC 地址信息

要查看机箱中每个服务器插槽或所有服务器的 WWN/MAC 地址信息，在高级模式下：

1 单击**服务器概览** > **属性** > **WWN/MAC**。

此时 **WWN/MAC 摘要**页面将显示 WWN/MAC 地址信息。

2 从**视图**下拉菜单中，选择**高级**以查看详细视图中的 WWN/MAC 地址属性。

WWN/MAC Addresses（WWN/MAC 地址）表中显示服务器插槽、结构、协议、WWN/MAC 地址、分区状态和当前活动的 MAC 地址分配类型 — 服务器分给、FlexAddress 或 I/O 标识 MAC。黑色复选标记表示活动地址类型，可以是服务器分配、机箱分配或远程分配。MAC。如果服务器未启用 FlexAddress 或 I/O 标识，则 **FlexAddress (Chassis-Assigned)（FlexAddress （机箱分配））**或 **I/O Identity (Remote-Assigned)（I/O 标识（远程分配））**的状态显示为 **Not Enabled（未启用）**，但黑色复选标记标识服务器分配。

3 在 **WWN/MAC 地址**表中，单击**导出**以本地保存 WWN/MAC 地址。

4 单击插槽的 + 或单击 **Expand/Collapse All（全部展开/折叠）**以展开或折叠为 WWN/MAC 地址表中特定插槽或所有插槽列出的属性。

5 从**服务器插槽**下拉菜单中，选择**所有服务器**或特定插槽以分别查看所有服务器或仅特定插槽中服务器的 WWN/MAC 地址属性。

6 从**结构**下拉菜单中，选择结构类型之一以查看与服务器关联的所有或特定类型的管理或 I/O 结构的详细信息。

7 从**协议**下拉菜单中，选择**所有协议**或其中一个列出的网络协议，以查看所有 MAC 地址或与选定协议相关联的 MAC 地址。

8 在 **WWN/MAC 地址**字段中，输入 MAC 地址以仅查看与特定 MAC 地址关联的插槽。或者，部分输入 MAC 地址条目以查看关联的插槽。例如，输入 4A 以查看 MAC 地址中包含 4A 的插槽。

9 从**分区状态**下拉菜单中，选择分区状态以显示具有所选分区状态的服务器。
如果特定分区已禁用，则状态显示为**已禁用**，并且显示该分区的行为灰色。

有关各字段的信息，请参阅*联机帮助*。

使用 RACADM 查看 WWN 或 MAC 地址信息

要使用 RACADM 查看所有服务器或特定服务器的 WWN/MAC 地址信息，请使用 getflexaddr 和 getmacaddress 子命令。

要显示整个机箱的 FlexAddress，请使用以下 RACADM 命令：

```
racadm getflexaddr
```

要显示特定插槽的 FlexAddress 状态，请使用以下 RACADM 命令：

```
racadm getflexaddr [-i <slot#>]
```

其中，*<slot#>* 的值为 1-16。

要显示 NDC 或 LOM MAC 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress
```

要显示机箱的 MAC 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -m chassis
```

要显示所有服务器的 iSCSI MAC 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -t iscsi
```

要显示特定服务器的 iSCSI MAC 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

要显示用户定义的 MAC 和 WWN 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

要显示所有 LOM 或夹层卡的控制台分配 MAC/WWN 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -c all
```

要显示机箱分配的 WWN/MAC 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -c flexaddress
```

要显示所有 LOM 或夹层卡的 MAC/WWN 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -c factory
```

要显示所有 iDRAC/LOM/夹层卡的以太网和 iSCSI MAC/WWN 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -a
```

有关 getflexaddr 和 getmacaddress 子命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

查看全球通用名称或介质访问控制 ID

WWN/MAC Summary（WWN/MAC 摘要）页面可用于查看机箱中插槽的全球通用名称 (WWN) 配置和介质访问控制 (MAC) 地址。

结构配置

结构配置部分显示为结构 A、结构 B 和结构 C 安装的输入/输出结构类型。绿色复选标记表示已为 FlexAddress 启用结构。FlexAddress 功能用于将机箱分配的插槽永久 WWN/MAC 地址部署到机箱内的各种结构和插槽。该功能以结构和插槽为单位启用。

注: 有关 FlexAddress 功能的更多信息，请参阅关于 FlexAddress。

WWN 或 MAC 地址

WWN/MAC 地址部分显示分配到所有服务器的 WWN/MAC 信息，即便那些服务器插槽当前为空。

- **Location（位置）**显示输入/输出模块占用的插槽位置。通过组名（A、B 或 C）和插槽编号（1 或 2）的组合识别 6 个插槽：插槽名称 A1、A2、B1、B2、C1 或 C2。iDRAC 是服务器的集成管理控制器。
- **结构**显示 I/O 结构的类型。
- **服务器分配**显示服务器分配的嵌入控制器硬件中的 WWN/MAC 地址。
- **机箱分配**显示机箱分配的用于特定插槽的 WWN/MAC 地址。

Server-Assigned（服务器分配）或 **Chassis-Assigned（机箱分配）**列中的绿色复选标记指示活动地址的类型。在机箱上激活 FlexAddress 时，将分配机箱分配的地址，并代表插槽永久地址。选中此 ChassisaAssigned 地址时，即便一台服务器已替换另一台服务器也会使用那些地址。

命令消息

下表列出 RACADM 命令和常见 FlexAddress 情况的输出。

表. 39: FlexAddress 命令和输出

情况	命令	输出

活动 CMC 模块中的 SD 卡绑定到另一个服务标签。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: The feature card is bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`

活动 CMC 模块中的 SD 卡绑定到相同的服务标签。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: The feature card is bound to this chassis`

情况	命令	输出

活动 CMC 模块中的 SD 卡未绑定到相同的服务标签。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: The feature card is not bound to any chassis`

出于某种原因（未插入 SD 卡/SD 卡损坏/功能停用后/SD 卡绑定到不同机箱），机箱上的 FlexAddress 功能未处于活动状态。	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		`ERROR: Flexaddress feature is not active on the chassis`

来宾用户尝试在插槽或结构上设置 FlexAddress。	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		`ERROR: Insufficient user privileges to perform operation`

在机箱接通电源的情况下停用 FlexAddress 功能。	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
来宾用户尝试停用机箱上的功能。	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`
服务器模块接通电源时更改插槽/结构 FlexAddress 设置。	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`

FlexAddress DELL 软件许可协议

本协议是您（用户）与 Dell Products L.P 或 Dell Global B.V. ("Dell") 之间的法律协议。本协议涵盖了 Dell 产品附带的所有软件（统称“软件”），除此之外不存在您与软件制造商或所有者之间的任何单独许可协议。本协议并不代表销售软件或任何其他知识产权。所有与软件有关的所有权和知识产权均归软件的制造商或所有者所有。未在本协议中明确授予您的所有权利均由软件的制造商或所有者保留。一旦您打开或拆开本软件包装上的密封，安装或下载本软件，或者使用产品中预装或嵌入的软件，即表示您同意受本协议条款的约束。如果您不同意这些条款，请立即退回所有软件物品（包括磁盘、书面材料和包装），并且删除任何预装或嵌入的软件。

一份软件一次仅可在一台计算机上使用。如果您拥有多份软件许可证，则可以随时使用与许可证份数相同的多个软件。“使用”是指将本软件载入计算机上的临时存储器或永久性存储设备。如果在网络服务器上安装本软件以便将其分配给其他计算机，并且获分配本软件的每台计算机均具有单独的许可证，则不能将这种安装称为“使用”。您必须保证安装在网络服务器上的软件的使用人数不超过您拥有的许可证份数。如果网络服务器上安装的软件的用户数超过许可证数，则必须购买更多的软件许可证，使许可证份数与用户数相等，然后才能允许其他用户使用软件。如果您是 Dell 的商业客户或 Dell 会员，您特此授权 Dell 或 Dell 选定的代理商在正常工作时间内就您对本软件的使用情况进行核查，并且同意在核查期间与 Dell 合作并合理地提供与本软件使用相关的所有记录。核查行为仅限于验证您是否遵循本协议中的条款。

本软件受美国版权法和国际条约的保护。您可以复制一份软件以用于备份或存档；也可以将软件传送至某个硬盘，条件是将原始软件仅用于备份或存档目的。您不得出租或租用本软件，也不得复制本软件附带的书面材料，但是可以作为 Dell 产品销售或转让的一部分永久性地转让本软件及其附带的所有材料，条件是您不保留任何复制件，并且受转让者同意遵守本协议中的条款。任何转让必须包括最新的更新文件和所有先前的版本。不得对软件进行反向工程、反编译或分解。如果计算机附带的软件包装内含有光盘、3.5 英寸和/或 5.25 英寸磁盘，则仅可将适当的磁盘用于您的计算机。不得在另一台计算机或另一个网络上使用这些磁盘，也不得出借、出租、租赁或将它们转让给另一个用户（除非符合本协议的规定）。

有限担保

从您收到这些软件磁盘之日起九十 (90) 天内，Dell 保证这些软件磁盘在正常使用的情况下不会出现材料和工艺方面的缺陷。此担保仅适用于您本人，并且不能转让。任何暗示性担保均限制在从您收到本软件之日起九十 (90) 天之内。某些辖区不允许对暗示性担保的持续时间进行限制，因此上述限制可能不适用于您。Dell 及其供应商的全部责任以及您获得的唯一补偿是：(a) 退回购买本软件所付的款项，或者 (b) 更换不符合此担保要求的任何磁盘，但是您必须将磁盘与退回授权号一起发送至 Dell 并承担相关费用和风险。此有限担保不适用于因意外、滥用、误用或由非 Dell 授权人员维修或修改磁盘所导致的损坏。对于任何更换过的磁盘，其担保期为原始担保期的剩余时间或者三十 (30) 天，以较长的时间为准。

Dell 并不保证本软件的功能可以满足您的要求，也不保证本软件的操作不会中断或不出现错误。您自己负责选择本软件来满足您的特定用途，并且对本软件的使用及其产生的后果负责。

对于软件及其附带的所有书面材料，DELL 代表本公司及其供应商否认其他所有的明示或暗示担保，包括但不限于适销性和对某一特定用途适用性的暗示担保。本有限担保赋予您特定的法律权利；您可能还具有其他权利，视管辖区域的不同而有所差异。

无论在什么情况下，Dell 或其供应商对于因使用本软件或不能使用本软件所造成的任何损失（包括但不限于商业利润损失、业务中断、业务信息丢失或其他经济损失）概不负责，即使已得到可能出现此类损失的通知。由于某些辖区不允许对必然性或偶然性损失的责任进行排除或限制，因此上述限制可能不适用于您。

开放源代码软件

本 CD 的一部分可能包含开放式源代码软件，您可以按照在分发开放式源代码软件时所依据的特殊许可证的条款和条件使用该软件。

本开放源代码软件的发布旨在希望其将是有用的，但本软件按原样提供，无任何明示或暗示的担保，包括但不限于适销性或对于特定目的适用性的暗示担保。无论任何情况，Dell、版权所有者或其他责任者均不会对任何直接的、间接的、偶然的、特殊的、典型的或伴生的损失（包括但不限于替代产品或服务的采购、用途、数据和利润的损失，或业务中断）负责，无论如何引起、基于何种责任的推理、是否有合同、严格的义务或任何由于使用本软件所引发的民事侵权行为（包括疏忽或其他原因），即使已得到可能会有此类损失的提示。

美国政府限制权利

48 C.F.R. 2.101 中的条款规定软件和文档均属于"商品"，它由 48 C.F.R. 12.212 中所用的术语"商业计算机软件"和"商业计算机软件说明文件"组成。与 48 C.F.R. 12.212 和 48 C.F.R. 227.7202-1 到 227.7202-4 一致，所有获得本软件和文档的美国政府最终用户仅具有如前所述的权利。

签约商/制造商是 Dell Products, L.P.，One Dell Way, Round Rock, Texas 78682。

一般信息

本许可在终止前持续有效。本许可会依据上述条件终止，或者如果您违反了本许可规定的任何条款，则本许可会被终止。许可终止后，您同意销毁本软件和随附材料，以及所有副本。本协议受德克萨斯州法律的管辖。本协议中的各项规定均具有可分割性。如果某一规定被认为无法实施，它并不会影响本协议中其他规定、条款或条件的有效性。本协议对本软件的继承者和受让者均有效。在法律允许的最大范围内，Dell 和您均同意放弃就本软件或本协议提起任何诉讼的权利。此放弃行为在某些辖区内可能无效，因此它可能不适用于您。您确认已阅读了本协议，并且理解和同意遵守其中的条款。另外，您还承认本协议是您与 Dell 之间就软件所签署的完整的、唯一的协议声明。

13

管理输入输出结构

机箱最多可以有六个 I/O 模块 (IOM)，其中每个 IOM 是直通或交换机模块。这些 IOM 分为 A、B、C 三组。每组有两个插槽 — 插槽 1 和插槽 2。

插槽在机箱背面自左至右使用字母标记：A1 | B1 | C1| C2 | B2 | A2。每台服务器都有两个用于连接 IOM 的夹层插卡 (MC) 插槽。MC 和相应的 IOM 必须具备相同的结构。

机箱 IO 分成三个独立的数据路径：A、B 和 C。这些路径称为结构，支持以太网、光纤通道或 InfiniBand。这些独立的结构路径分为 2 个 IO 组：组 1 和组 2。每个服务器 IO 适配器（夹层卡或 LOM）可以有两个或四个端口，具体取决于功能。这些端口平均分配到 IOM 组 1 和组 2，以实现冗余性。当您部署以太网、iSCSI 或光纤通道网络时，可以跨组 1 和组 2 分配冗余链接，以实现最大可用性。独立 IOM 通过结构标识符和组号来标识。

示例：A1 表示组 1 中的结构 A。C2 表示组 2 中的结构 C。

机箱支持三种结构或协议类型。组中的 IOM 和夹层卡都必须具有相同或兼容的结构类型。

- 组 A IOMS 始终连接到服务器的机载以太网适配器；组 A 的结构类型始终是以太网。
- 在组 B 中，IOM 插槽永久连接到每个服务器模块的第一个 MC 插槽。
- 在组 C 中，IOM 插槽永久连接到每个服务器模块的第二个 MC 插槽。

注: 在 CMC CLI 中，IOM 按照惯例称为 switch-n：A1=switch-1、A2=switch-2、B1=switch-3、B2=switch-4、C1=switch-5 和 C2= switch-6。

主题：

相关链接

结构管理概述
无效配置
刷新开机场景
监测 IOM 运行状况
为 IOM 配置网络设置
管理 IOM 的 VLAN
管理 IOM 的电源控制操作
启用或禁用 IOM 的 LED 闪烁
将 IOM 重设为出厂默认设置

结构管理概述

结构管理有助于避免由于安装了与机箱既定结构类型不兼容结构类型的 IOM 或 MC，从而造成有关电气、配置或连接问题。无效硬件配置将会给机箱或其组件带来电气或功能问题。结构管理防止接通电源时的无效配置。

下图显示机箱中 IOM 的位置。每个 IOM 的位置由其组编号（A、B 或 C）表示。这些独立的结构路径分为 2 个 IO 组：组 1 和组 2。在机箱上，IOM 插槽名称标记为 A1、A2、B1、B2、C1 或 C2。

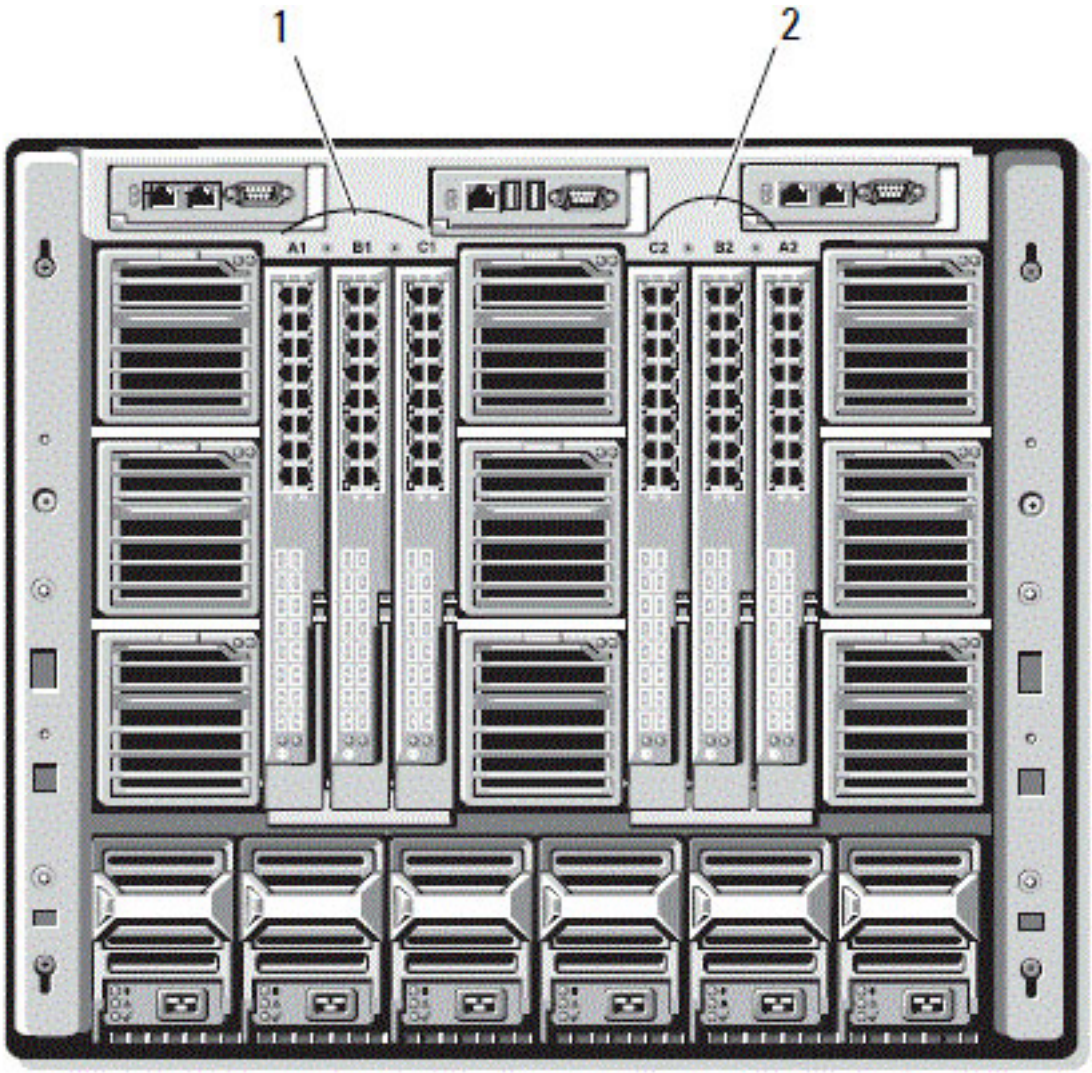


图 13: 机箱后视图，显示 IOM 的位置

表. 40: 机箱后部的 IOM 的位置

1	组 1（插槽 A1、B1、C1）	2	组 2（插槽 A2、B2、C2）

CMC 将在硬件日志和 CMC 日志中为无效硬件配置创建条目。

例如：

- 已连接到光纤信道 IOM 的以太网 MC 是无效配置。然而，连接到以太网交换机和安装在相同 IOM 组中以太网直通 IOM 的以太网 MC 是有效连接。
- 如果所有服务器上的第一个 MC 也是光纤信道，则插槽 B1 和 B2 中的光纤信道直通 IOM 和光纤信道交换机 IOM 是有效配置。在这种情况下，CMC 会启动 IOM 和服务器。不过，某些光纤信道冗余软件可能不支持此配置；并非全部有效的配置都是必要的支持配置。

  只有当机箱开机时，才能对服务器 IOM 和 MC 执行结构验证。当机箱处于电源待机状态时，服务器模块上的 iDRAC 仍处于关机状态，因此它无法报告服务器的 MC 结构类型。在服务器上的 iDRAC 开机之前，CMC 用户界面中可能不会报告 MC 结构类型。另外，如果机箱开机，则在插入服务器或 IOM（可选）时进行结构认证。如果检测到不匹配结构，则允许服务器或 IOM 开机且状态 LED 闪烁琥珀色。

无效配置

有三种无效配置类型：

- 无效 MC 或 LOM 配置，新安装的服务器结构类型与现有的 IOM 结构不同。也就是说，单个服务器的 LOM 或 MC 不受其相应 IOM 的支持。在这种情况下，机箱中的其他所有服务器都保持运行，但是 MC 卡不匹配的服务器无法开机。服务器上的电源按钮将闪烁琥珀色以警示结构不匹配。
- 无效 IOM-MC 配置，新安装的 IOM 结构类型和驻留的 MC 结构类型不匹配或不兼容。不匹配的 IOM 将保持关机状态。CMC 向 CMC 和硬件日志添加条目，注明无效配置并指定 IOM 名称。CMC 导致有问题的 IOM 的错误 LED 指示灯闪烁。如果将 CMC 配置为发送警报，则它将针对该事件发送电子邮件和 SNMP 警报。
- 无效 IOM-IOM 配置，新安装的 IOM 与组中已安装的 IOM 具有不同或不兼容的结构类型。CMC 将新安装的 IOM 保持在关机状态，从而导致 IOM 的错误 LED 指示灯闪烁，并在 CMC 和硬件日志中创建关于不匹配的日志条目。

刷新开机场景

当机箱插入并开机时，I/O 模块的优先级高于服务器。每个组中的第一个 IOM 允许比其他 IOM 先开机。此时不会执行它们的结构类型验证。如果一个组的第一个插槽上没有 IOM，该组第二个插槽上的模块将开机。如果两个插槽上都有 IOM，第二个插槽中的模块将与第一个插槽中的模块比较一致性。

IOM 开机之后，服务器开机，然后 CMC 将验证服务器的结构一致性。

如果直通模块和交换机的结构等同，则允许将它们在相同的组中。甚至当交换机和直通模块由不同的供应商制造时，也可存在于相同的组中。

监测 IOM 运行状况

有关监测 IOM 运行状况的信息，请参阅查看所有 IOM 的信息和运行状况以及查看单个 IOM 的信息和运行状况。

使用 Web 界面查看输入输出模块上行链路和下行链路状态

您可以使用 CMC Web 界面查看 Dell PowerEdge M I/O 聚合器的上行链路和下行链路状态信息：

1 转至**机箱概览**，展开系统树中的 **I/O 模块概览**。
展开的列表中将显示所有 IOM（1 - 6 个）。

2 单击您要查看的 IOM（插槽）。
随即会显示特定于 IOM 插槽的 **I/O Module Status（I/O 模块状态）**页面。随即会显示 **I/O Module Uplink Status（I/O 模块上行链路状态）**和 **I/O Module Downlink Status（I/O 模块下行链路状态）**表格。这些表显示关于下行链路端口 (1-32) 和上行链路端口 (33-56) 的信息。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 确保 I/O 聚合器配置有效，以便端口链路状态能够接通。此页面显示 I/O 聚合器的状态。如果状态为未接通，它表示 I/O 聚合器的服务器端口可能由于配置无效而无法接通。

使用 Web 界面查看输入输出模块 FCoE 会话信息

您可以使用 CMC Web 界面查看 Dell PowerEdge M I/O 聚合器的 FCoE 会话信息：

1 在系统树中，转至**机箱概览**并展开 **I/O 模块概览**。
展开的列表中将显示所有 IOM（1 - 6 个）。

2 单击您要查看的 IOM（插槽），然后单击 **Properties（属性）** > **FCoE**。
随即会显示特定于 IOM 插槽的 **FCoE I/O 模块**页面。

3 在**选择端口**下拉列表中，选择所选 IOM 的所需端口号并单击**显示会话**。
FCoE 会话信息部分将显示交换机的 FCoE 会话信息。

注: 仅当 I/O 聚合器上有正在运行的活动 FCoE 会话时，该部分才会显示 FCoE 信息。

查看 Dell PowerEdge M 输入输出聚合器的堆栈信息

您可以使用 racadm getioinfo 命令查看 Dell PowerEdge M I/O 聚合器的以下堆栈信息：

- 堆栈 ID - 这是堆栈主机的 MAC 地址，表示与该模块关联的堆栈。
- 堆栈单元 - 这是一个整数，表示 I/O 聚合器在堆栈中的位置。
- 机箱 ID - 该 ID 帮助描述堆栈的物理拓扑并指示特定交换机的位置。
- 堆栈角色 — 识别堆栈中此模块的功能。有效值为主要、成员和待机。

使用 racadm getioinfo 命令及 -s 选项，可查看机箱中存在的交换机的 I/O 聚合器相关堆栈信息以及同时位于本地机箱和外部机箱中的堆栈单元。
使用以下命令可查看仅位于本地机箱中的交换机的堆栈信息：

```
racadm getioinfo -s
```

使用以下命令可查看本地堆栈单元的堆栈信息以及外部机箱中的单元：

```
racadm getniccfg [-m <module>]
```

请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 racadm getioinfo 命令部分。

为 IOM 配置网络设置

您可以为用于管理为 IOM 的接口指定网络设置。对于以太网交换机，配置带外管理端口（IP 地址）。不能使用此接口配置带内管理端口（即 VLAN1）。

在为 IOM 配置网络设置之前，确保将 IOM 电源打开。

要配置网络设置，您必须具有：

- 结构 A 的管理员权限，以配置组 A 中的 IOM。
- 结构 B 的管理员权限，以配置组 B 中的 IOM。
- 结构 C 的管理员权限，以配置组 C 中的 IOM。

注: 对于以太网交换机，带内 (VLAN1) 和带外管理 IP 地址不能相同或位于相同的网络；这将导致无法设置带外 IP 地址。请参阅默认带内管理 IP 地址的 IOM 说明文件。

注: 不要为以太网直通和 Infiniband 交换机配置输入/输出模块网络设置。

使用 CMC Web 界面为 IOM 配置网络设置

注: 仅在 PowerEdge M I/O 聚合器 IOM 上支持此功能。不支持包括 MXL 10/40GbE 在内的其他 IOM。

要使用 CMC Web 界面为 IOM 配置网络设置，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置**，或者展开 **I/O 模块概览**，选择 IOM，然后单击**设置**。
部署 I/O 模块页显示开机的 IOMs。
2 对于所需的 IOMs，启用 DHCP，输入 IP 地址、子网掩码和网关地址。

3 对于可管理的 IOM，输入根用户密码、SNMP RO 团体字符串和系统日志服务器 IP 地址。有关这些字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 从 CMC 设置的 IOM IP 地址不会保存到交换机的永久启动配置中。要永久保存 IP 地址配置，您必须输入 `connect switch-n command` 或 `racadm connect switch -n` RACADM 命令，或使用到 IOM GUI 的直接界面将该地址保存到启动配置文件中。

注: SNMP 团体字符串可包含任何可打印字符，ASCII 值范围为 33-125。

4 单击**应用**。

IOM 的网络设置已配置完成。

注: 对于可管理的 IOM，您可以将 VLAN、网络属性和 IO 端口重设为默认配置。

使用 RACADM 为 IOM 配置网络设置

要使用 RACADM 为 IOM 配置网络设置，应设置日期和时间。请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 deploy 命令部分。

您可以使用 RACADM deploy 为 IOM 设置用户名、密码和 SNMP 字符串：

```
racadm deploy -m switch-<n> -u root -p <password>
racadm deploy -m switch-<n> -v SNMPv2 <snmpCommunityString> ro
racadm deploy -a [server|switch] -u root -p <password>
```

将 IOM 重设为出厂默认设置

您可以使用**部署 I/O 模块**页将 IOM 重设为出厂默认设置。

注: 仅在 PowerEdge M I/O 聚合器 IOM 上支持此功能。不支持包括 MXL 10/40GbE 在内的其他 IOM。

要使用 CMC Web 界面将所选 IOM 重设为出厂默认设置，请执行以下操作：

1 在系统树中，转至 **I/O 模块概述**，然后单击**设置**，或者在系统树中展开 **I/O 模块概述**，选择 IOM，然后单击**设置**。

部署 I/O 模块页显示开机的 IOM。

2 对于所需的 IOM，单击**重设**。

随即将显示一条警告消息。

3 单击**确定**继续。

相关链接

结构管理概述
无效配置
刷新开机场景
监测 IOM 运行状况
为 IOM 配置网络设置
管理 IOM 的 VLAN
管理 IOM 的电源控制操作
启用或禁用 IOM 的 LED 闪烁

使用 CMC Web 界面更新 IOM 软件

您可以通过从指定位置选择所需的软件映像来更新 IOM 软件。您也可以回滚到较早的软件版本。

注: 仅在 PowerEdge M I/O 聚合器 IOM 上支持此功能。不支持包括 MXL 10/40GbE 在内的其他 IOM。

要在 CMC Web 界面中更新 IOM 基础结构设备软件，请执行以下操作：

1 转至**机箱概览** > **I/O 模块概览** > **更新**。

此时将显示 **IOM 固件更新**页面。

或者，请转至以下任一页：

- **机箱概览** > **更新**
- **机箱概览** > **机箱控制器** > **更新**
- **机箱概览** > **iKVM** > **更新**

随即显示**固件更新**页面，该页面提供了用于访问 **IOM 固件更新**页面的链接。

2 在 **IOM 固件更新**页面的 **IOM 固件**部分，选中**更新**列中要更新软件的 IOM 对应的复选框，并单击**应用固件更新**。

另外，要回滚到软件的早期版本，请选择**回滚**列中的复选框。

3 使用**浏览**选项，选择用于软件更新的软件映像。在 **IOM 软件位置**字段中显示软件映像的名称。

在**更新状态**部分提供软件更新或回滚状态信息。当上载映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新进程开始时，将自动刷新页面并显示固件更新计时器。

注: 在文件传输过程中，请勿单击刷新图标或导航到另一页。

注: 当更新 IOMINF 固件时，不会显示文件传输计时器。

更新或回滚完成后，与 IOM 设备的连接会短暂丧失，因为该设备会进行重设并且在 **IOM 固件和软件**页上显示新固件。

注: FTOS 或 IOM 软件版本以格式 X-Y(A-B) 显示。例如，8-3(1-4)。如果 FTOS 映像的回滚版本为使用旧版本字符串格式 8-3-1-4 的旧映像，则“当前版本”会显示为 8-3(1-4)。

IOA GUI

您可以从 CMC 启动 IOA GUI，来管理 IOA 配置。要从 CMC 启动 IOA GUI，必须将 IOM 设置为 IOA，并且您必须具备结构 A、结构 B 或结构 C 管理员权限。

您可以从**机箱概览**、**I/O 模块概览**以及 **I/O 模块状态**页面启动 IOA GUI。

注: 在首次登录 IOA 应用程序时，系统会提示您自定义密码。

从“机箱概览”页面启动 IOA GUI

转至**机箱概览** > **快速链接** > **启动 I/O 模块 GUI**。随即会显示 IOA 登录页面。

从“ I/O 模块概览”页面启动 IOA GUI

在目录树中，转至 **I/O 模块概览**。在 **I/O 模块状态**页面中，单击**启动 I/O 模块 GUI**。随即会显示 IOA 登录页面。

从“ I/O 模块状态”页面启动 IOA GUI

在目录树中的 **I/O 模块概览**下，单击 I/O 聚合器。在 **I/O 模块状态**页面中，单击**启动 I/O 模块 GUI**。

输入输出聚合器模块

您可以在 CMC RACADM、**机箱运行状况**、**I/O 模块状态**以及 **I/O 模块概览**页面查看 IOM 和 Flex 模块的详细信息。

通过读取与 IOA 初始协商期间柔性模块的信息，CMC 报告有关 IOA 中的 Flex 模块的信息。通过在初始协商期间发送 XML 命令即可读取。CMC 将可更换模块的信息保存在共享内存中。最多可以由两个柔性模块：

- FlexIO 模块 1
- FlexIO 模块 2

支持命令版本 4 的所有 IOM 软件都支持的 Flex IO 模块信息 XML 命令。只有命令修订版是 4 或更高版本时，CMC 才会发送柔性模块信息。任何读取柔性模块信息的故障都存储在机箱日志中。

Flex 模块信息可能具有以下五个值：

- 4x10G Base-T FlexIO 模块 = 0
- 4x10G SFP+ FlexIO 模块 = 1
- 2x40G QSFP+ FlexIO 模块 = 2
- 4xFC FlexIO 模块 = 3
- 未安装 Flex 模块 = 4

任何大于 4 的值都被视为无效。CMC 显示为“无效/未知”的柔性模块。

IOM 模式如下：

- 独立
- 堆叠
- PMux
- 完全交换

在**机箱运行状况**、**I/O 模块状态**和 **I/O 模块概览**页面选择 IOM 时，可以工具提示的形式查看 IOM 模式。

将有静态 IP 的 IOA 的模式从堆栈更改为独立时，确保 IOA 的网络更改为 DHCP。否则，在所有 IOA 上复制静态 IP。

IOM 处于堆栈模式下时，堆栈 ID 与初始开机期间在 MAC 中刻录的主 IOM 相同。当 IOM 模式更改时，堆栈 ID 也不会更改。例如，在初始开机期间，如果交换机 1 是主交换机，则堆栈中的 MAC 地址与 MAC 地址中刻录的交换机 1 相同。之后，当交换机 3 是主交换机时,交换机 1 MAC 地址保留为堆栈 ID。

racadm 命令 `getmacaddress` 可显示在 MAC 地址 + 2 中刻录的 I/F MAC。

管理 IOM 的 VLAN

出于安全和其他原因考虑，可以使用 IOM 的虚拟 LAN (VLAN) 将用户分到不同的网段。通过使用 VLAN，可以为 32 个端口的交换机用户隔离网络。您可以将交换机上的所选端口与所选 VLAN 关联起来，并将这些端口视作单独的交换机。

CMC Web 界面可用于配置 IOM 上的带内管理端口。

I/O 聚合器的模式从堆栈更改为独立后，移除启动配置并重新加载 I/O 聚合器。您不需要在重新加载 I/O 聚合器时保存系统配置。

相关链接

使用 CMC Web 界面配置 IOM 的 VLAN 设置
使用 CMC Web 界面查看 IOM 的 VLAN 设置
使用 CMC Web 界面查看 IOM 的当前 VLAN 设置
使用 CMC Web 界面为 IOM 添加标记的 VLAN
使用 CMC Web 界面删除 IOM 的 VLAN
使用 CMC Web 界面更新 IOM 的未标记 VLAN
使用 CMC Web 界面重设 IOM 的 VLAN

使用 Web 界面配置 IOM 的管理 VLAN

您可以通过 VLAN 管理带内 IO 聚合器。此 VLAN 必须在使用前进行部署。CMC 支持带内管理 VLAN 部署。该交换机的带内管理 VLAN 要求应用以下设置的基本配置：

- Enable（启用）
- VLAN ID
- Priority（优先级）

注:

要在 **VLAN 设置**页面上配置管理 VLAN，必须具有**机箱配置**权限。要配置 IOM VLAN，除了具有特定结构 A、B 或 C 的**管理员**权限外，还必须具有此权限。

要使用 CMC Web 界面配置 IOM 的管理 VLAN，请执行以下操作：

1 在系统树中，转至**机箱概览**，单击**网络** > **VLAN**。
随即会显示 **VLAN 标签设置**页面。
2 在 **I/O 模块**部分，为 IOM 启用 VLAN，设置优先级并输入 ID。有关这些字段的更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用**保存设置。

使用 RACADM 配置 IOM 的管理 VLAN

要使用 RACADM 配置 IOM 的管理 VLAN，请使用 `racadm setniccfg –m switch-n -v` 命令。

- 用以下命令指定特定 IOM 的 VLAN ID 和优先级：

```
racadm setniccfg -m switch -<n> -v <VLAN id> <VLAN priority>
```

`<n>` 的有效值是 1 - 6。

`<VLAN>` 的有效值是 1-4000 和 4021-4094。默认值是 1。

`<VLAN priority>` 的有效值是 0-7。默认值是 0。

例如：

```
racadm setniccfg -m switch -1 -v 1 7
```

例如：

- 要移除 IOM VLAN，请禁用指定 IOM 网络的 VLAN 功能：

```
racadm setniccfg -m switch-<n> -v
```

`<n>` 的有效值是 1 - 6。

例如：

```
racadm setniccfg -m switch-1 -v
```

使用 CMC Web 界面配置 IOM 的 VLAN 设置

注：您只能配置 PowerEdge M I/O Aggregator IOM 的 VLAN 设置。包括 MXL 10/40GbE 的其他 IOM 不受支持。

要使用 CMC Web 界面配置 IOM 的 VLAN 设置，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置** > **VLAN Manager**。
VLAN Manager 页面将显示打开电源的 IOM 和可用端口。

2 在**步骤 1：选择 I/O 模块**部分，从下拉列表中选择配置类型，然后选择所需的 IOM。
有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

3 在**步骤 2：指定端口范围**部分，选择要分配给所选 IOM 的结构端口范围。
有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

4 选择**全选**或**取消全选**选项分别将更改应用到所有 IOM 或不应用到任何 IOM。
或

选中特定插槽对应的复选框以选择所需的 IOM。

5 在**步骤 3：编辑 VLAN** 部分，输入 IOM 的 VLAN ID。提供 1-4094 范围内的 VLAN ID。VLAN ID 可以采用范围或逗号分隔的形式输入。例如：1,5,10,100-200。

6 根据需要，从下拉菜单中选择以下选项：
- 添加标记的 VLAN
- 删除 VLAN
- 更新未标记的 VLAN
- 重设为所有 VLAN
- 显示 VLAN

7 单击**保存**以保存对 **LAN Manager** 页所做的新设置。
有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注：“所有端口的摘要 VLAN”部分显示有关机箱中和分配的 VLAN 中存在的 IOM 的信息。单击保存将当前 VLAN 设置的摘要保存为 csv 文件。

注：“CMC 管理的 VLAN”部分显示分配给 IOM 的所有 VLAN 的摘要。

8 单击**应用**。
IOM 的网络设置已配置完成。

使用 CMC Web 界面查看 IOM 的 VLAN 设置

要使用 CMC Web 界面查看 IOM 的 VLAN 设置，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置** > **VLAN Manager**。
此时将显示 **VLAN Manager** 页。

所有端口的摘要 VLAN 部分显示有关 IOM 的当前 VLAN 设置的信息。

2 单击**保存**将 VLAN 设置保存到文件。

使用 CMC Web 界面查看 IOM 的当前 VLAN 设置

要使用 CMC Web 界面查看 IOM 的当前 VLAN 设置，请执行以下操作：

1 在系统树中，转至 **I/O 模块概述**，然后单击**设置** > **VLAN Manager**。
此时将显示 **VLAN Manager** 页。
2 在**编辑 VLAN** 部分，从下拉列表中选择**显示 VLAN**，然后单击**应用**。
此时将显示操作成功消息。分配给 IOM 的当前 VLAN 设置显示在“VLAN 分配摘要”字段中。

使用 CMC Web 界面为 IOM 添加标记的 VLAN

要使用 CMC Web 界面为 IOM 添加标记的 VLAN，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置** > **VLAN Manager**。
此时将显示 VLAN Manager 页。
2 在**步骤 1：选择 I/O 模块**部分，选择所需的 IOM。
3 在**步骤 2：指定端口范围**部分，选择要分配给所选 IOM 的结构端口范围。
有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
4 选择**全选**或**取消全选**选项分别将更改应用到所有 IOM 或不应用到任何 IOM。
或

选中特定插槽对应的复选框以选择所需的 IOM。
5 在**步骤 3：编辑 VLAN** 部分，在下拉列表中选择**添加标记的 VLAN** 并单击**应用**。
标记的 VLAN 即分配给所选的 IOM。

此时将显示操作成功消息。分配给 IOM 的当前 VLAN 设置显示在 **VLAN 分配摘要**字段。

使用 CMC Web 界面删除 IOM 的 VLAN

要使用 CMC Web 界面删除 IOM 的 VLAN，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置** > **VLAN Manager**。
此时将显示 VLAN Manager 页。
2 在**步骤 1：选择 I/O 模块**部分，选择所需的 IOM。
3 在**步骤 3：编辑 VLAN** 部分，在下拉列表中选择**移除 VLAN** 并单击**应用**。
分配给所选 IOM 的 VLAN 即被删除。

此时将显示操作成功消息。分配给 IOM 的当前 VLAN 设置显示在 **VLAN 分配摘要**字段中。

使用 CMC Web 界面更新 IOM 的未标记 VLAN

要使用 CMC Web 界面更新 IOM 的未标记 VLAN，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置** > **VLAN Manager**。
此时将显示 **VLAN Manager** 页。
2 在**步骤 1：选择 I/O 模块**部分，选择所需的 IOM。

3 在**步骤 2：指定端口范围**部分，选择要分配给所选 IOM 的结构端口的范围。
有关各字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
4 选择**全选/取消全选**选项分别将更改应用到所有 IOM 或不应用到任何 IOM。
或

选中特定插槽对应的复选框以选择所需的 IOM。
5 在**步骤 3：编辑 VLAN** 部分，在下拉列表中选择**更新未标记的 VLAN**，然后单击**应用**。
此时将显示一条警告消息，指出现有未标记 VLAN 的配置将被新分配的未标记的 VLAN 配置所覆盖。
6 单击**确定**确认。
未标记的 VLAN 用新分配的未标记 VLAN 配置更新。

此时将显示操作成功消息。分配给 IOM 的当前 VLAN 设置显示在 VLAN 分配摘要字段中。

使用 CMC Web 界面重设 IOM 的 VLAN

要使用 CMC Web 界面将 IOM 的 VLAN 重设为默认配置，请执行以下操作：

1 在系统树中，转至 **I/O 模块概览**，然后单击**设置** > **VLAN Manager**。
此时将显示 **VLAN Manager** 页。
2 在**步骤 1：选择 I/O 模块**部分，选择所需的 IOM。
3 在**步骤 3：编辑 VLAN** 部分，从下拉列表中选择**重设 VLAN** 并单击**应用**。
此时将显示一条警告消息，指示现有 VLAN 的配置将使用默认配置覆盖。
4 单击 **OK**（确定）以确认。
即根据默认配置将 VLAN 分配给所选 IOM。

此时将显示操作成功消息。分配给 IOM 的当前 VLAN 设置显示在 **VLAN 分配摘要**字段中。

注: 虚拟链路主干聚合(VLT)模式的 IOA 中不支持重设为所有 VLAN 选项。

管理 IOM 的电源控制操作

有关为 IOM 设置电源控制操作的信息，请参阅对 IOM 执行电源控制操作。

启用或禁用 IOM 的 LED 闪烁

有关启用 IOM 的 LED 闪烁的信息，请参阅配置 LED 以标识机箱上的组件。

14

配置和使用 iKVM

Dell M1000e 服务器机箱的本地访问 KVM 模块称为“Avocent 集成 KVM 交换机模块”，或 iKVM。iKVM 是一种插入机箱中的模拟键盘、视频和鼠标交换机。它是机箱的可选热插拔模块，提供至机箱中的服务器和活动 CMC 命令行的本地键盘、鼠标和视频访问。

主题：

相关链接

iKVM 用户界面
iKVM 关键功能
物理连接接口

iKVM 用户界面

iKVM 使用屏上配置和报告 (OSCAR) 图形用户界面，可通过热键激活。OSCAR 允许用户选择要通过本地键盘、显示器和鼠标访问的其中一个服务器或 Dell CMC 命令行。每个机箱只允许使用一个 iKVM 会话。

相关链接

使用 OSCAR

iKVM 关键功能

- 安全性 - 使用屏幕保护程序密码保护系统。在经过用户定义的一段时间后，屏幕保护程序模式启动，访问被拒绝，直到输入正确密码重新激活 OSCAR 为止。
- 扫描 - 可在 OSCAR 处于扫描模式时选择一组服务器，这些服务器以所选次序显示。
- 服务器标识 - CMC 为机箱中所有服务器分配唯一的插槽名称。虽然您可通过分层连接使用 OSCAR 界面为服务器分配名称，但是 CMC 分配的名称具有优先权，使用 OSCAR 为服务器分配的任何新名称都将被改写。

  要使用 CMC Web 界面更改插槽名称，请参阅配置插槽名称。要使用 RACADM 更改插槽名称，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 **setslotname** 部分。
- 视频 - iKVM 视频连接支持从 640 x 480（60 赫兹）到 1280 x 1024（60 赫兹）的视频显示分辨率。
- 即插即用 - iKVM 支持显示数据信道 (DDC) 即插即用功能，可自动进行视频显示器配置，并符合 VESA DDC2B 标准。
- 快速可升级 - 您可以使用 CMC Web 界面或 RACADM `fwupdate` 命令更新 iKVM 固件。

相关链接

使用 OSCAR
使用 iKVM 管理服务器
从 CMC 管理 iKVM
更新 iKVM 固件

物理连接接口

您可以从机箱前面板、模拟控制台接口 (ACI) 和机箱后面板通过 iKVM 连接到服务器或 CMC CLI 控制台。

注: 机箱正面控制面板上的端口专门为 iKVM 设计，为可选组件。如果没有 iKVM 模块，则无法使用前控制面板端口。

iKVM 连接优先次序

一次只能有一个 iKVM 连接。iKVM 向每种类型连接分配优先次序，以便在存在多个连接时，只有一个连接可用，其他连接均被禁用。

iKVM 连接的优先次序为：

1 前面板
2 ACI
3 后面板

例如，如果前面板和 ACI 中有 iKVM 连接，则前面板连接保持活动，而 ACI 连接被禁用。如果有 ACI 和后面板连接，则 ACI 连接具有优先权。

通过 ACI 连接分层

iKVM 允许与服务器和 iKVM 的 CMC 命令行控制台建立分层连接，既可以通过远程控制台交换机端口在本地实现，也可以通过 Dell RCS 软件远程实现。iKVM 支持从以下产品进行 ACI 连接：

- 180AS、2160AS、2161DS、2161DS-2 或 4161DS Dell 远程控制台交换机
- Avocent AutoView 交换系统
- Avocent DSR 交换系统
- Avocent AMX 交换系统

注: 2161DS 不支持 Dell CMC 控制台连接。

注: iKVM 还支持至 Dell 180ES 和 2160ES 的 ACI 连接，但不是无缝分层。此连接需要一个 USB 到 PS2 SIP。

使用 OSCAR

此部分提供启动、配置和使用 OSCAR 界面的信息。

相关链接

启动 OSCAR
导航基础知识
配置 OSCAR

启动 OSCAR

要启动 OSCAR，请执行以下操作：

1 按下 <Print Screen>。
此时将显示**主菜单**对话框。
如果分配了密码，在单击 <Print Screen> 后显示**密码**对话框。

2 键入密码，然后单击**确定**。
此时将显示**主菜单**对话框。

注: 有四个选项可以调用 OSCAR。可通过选择“主菜单”对话框“调用 OSCAR”部分中的各框，启用一个、多个或全部这些键顺序。

相关链接

设置控制台安全性
导航基础知识

导航基础知识

表. 41: ：OSCAR 键盘和鼠标导航

键或键顺序	结果
• <Print Screen>-<Print Screen> • <Shift>-<Shift> • <Alt>-<Alt> • <Ctrl>-<Ctrl>	任何这些键顺序都可以打开 OSCAR，取决于用户的 **调用 OSCAR** 设置。可通过选择**主菜单**对话框的**调用 OSCAR** 部分中的相应框，然后单击**确定**，启用两个、三个或全部这些键顺序。
<F1> 键	打开当前对话框的**帮助**屏幕。
<Esc> 键	不保存更改而关闭当前对话框，并返回到上一个对话框。 在**主菜单**对话框中，按下 <Esc> 将关闭 OSCAR 界面并返回到所选服务器。 在消息框中，它将关闭弹出框并返回到当前对话框。
<Alt>	当与下划线字母或其他指定字符配合使用时，将打开对话框，选择或勾选选项，并执行操作。
<Alt>+<X>	关闭当前对话框并返回到上一个对话框。
<Alt>+<O>	选择**确定**按钮，然后返回到上一个对话框。
<Enter> 键	完成**主菜单**对话框中的切换操作，并退出 OSCAR。
单击，<Enter>	在文本框中，选择要编辑的文本并启用左箭头键和右箭头键移动光标。再次按下 <Enter> 退出编辑模式。
<Print Screen>，<Backspace>	如果没有其他按键操作，则切换回上一个选择。
<Print Screen>，<Alt>+<0>	立刻断开用户与服务器的连接；不选择服务器。状态标志显示可用。（此操作只适用于键盘而非小键盘上的 =<0>。）
<Print Screen>，<Pause>	如果采用了密码保护，立刻打开屏幕保护程序模式并阻止对该特定控制台的访问。
上/下箭头键	在列表的行间移动光标。

键或键顺序	结果
右/左箭头键	编辑文本框时，在列间移动光标。
<Home>/<End>	移动光标至列表的顶部 (Home) 或底部 (End)。
<Delete>	删除文本框中的字符。
数字键	从键盘或小键盘键入数字。
<Caps Lock>	已禁用。要更改大小写，请使用 <Shift> 键。

配置 OSCAR

可以使用**设置**对话框配置 OSCAR 设置。

访问“设置”对话框

要访问**设置**对话框，请执行以下操作：

1 按 <Print Screen> 启动 OSCAR 界面。
此时将显示**主菜单**对话框。
2 单击**设置**。
此时将显示**设置**对话框。

表. 42: “设置”对话框 — 功能

功能	用途
菜单	按插槽编号以数字顺序或按名称以字母顺序更改服务器排列。
安全性	• 设置限制对服务器访问的密码。 • 启用屏幕保护程序并设置屏幕保护程序出现之前的非活动时间，然后设置屏幕保护模式。
标志	更改状态标志的显示、时间、颜色或位置。
语言	更改所有 OSCAR 屏幕的语言。
广播	设置通过键盘和鼠标操作同时控制多个服务器。
扫描	为多达 16 个服务器设置自定义扫描样式。

相关链接

更改显示行为
为 OSCAR 分配键序列
设置 OSCAR 的屏幕延迟时间
设置状态标志显示

更改显示行为

使用**菜单**对话框更改服务器的显示次序并设置 OSCAR 的屏幕延迟时间。
要更改显示行为，请执行以下操作：

1 按下 <Print Screen> 启动 OSCAR。
此时将显示**主菜单**对话框。
2 单击**设置**，然后单击**菜单**。

此时将显示**菜单**对话框。

3 要选择服务器的默认显示次序，请执行以下任一操作：
   - 选择**名称**，按名称的字母顺序显示服务器。
   - 选择**插槽**，按插槽编号的数字顺序显示服务器。

4 单击**确定**。

为 OSCAR 分配键序列

要为 OSCAR 激活分配一个或多个键序列，请从**调用 OSCAR** 菜单选择键序列，然后单击**确定**。调用 OSCAR 的默认键是 <Print Screen>。

设置 OSCAR 的屏幕延迟时间

要设置 OSCAR 的屏幕延迟时间，请在按 <Print Screen> 键后，输入延迟 OSCAR 显示的秒数（0 到 9）并单击**确定**。

输入 <0> 无延迟启动 OSCAR。

设置 OSCAR 延迟显示时间允许用户完成一次软切换。

相关链接

软切换

设置状态标志显示

状态标志会显示在桌面上，说明所选服务器的名称或所选插槽的状态。使用“标志”对话框配置标志以按服务器显示或更改桌面上标志的颜色、不透明度、显示时间和位置。

表. 43: 标志显示

标志	说明
	按名称划分的标志类型。
	表示用户已从所有系统断开连接的标志
	表示广播模式已启用的标志

要设置状态标志的显示，请执行以下操作：

1 按下 <Print Screen> 启动 OSCAR。
   此时将显示**主菜单**对话框。
2 单击**设置**，然后单击**标志**。
   此时将显示**标志**对话框。
3 选择**已显示**使标志始终显示，或选择**已显示**和**已计时**使标志在交换后只显示 5 秒钟。

   注: 如果选择已计时，则标志不会显示。

4 在**显示颜色**部分，选择标志颜色。选项有黑色、红色、蓝色和紫色。
5 在**显示模式**中，选择**不透明**用于不透明颜色标志，或选择**透明**可通过标志看到桌面。
6 要在桌面上安排状态标志的位置，请单击**设置位置**：

此时将显示**设置位置**标志。

7 左键单击标题栏将其拖到桌面上的所需位置，然后右键单击返回**标志**对话框。

8 单击**确定**并再次单击**确定**保存设置。

要不保存更改而退出，请单击  。

使用 iKVM 管理服务器

iKVM 是一种可支持多达 16 个服务器的模拟交换机模块。iKVM 交换机使用 OSCAR 用户界面选择和配置服务器。此外，iKVM 还包括一个系统输入，可与 CMC 建立 CMC 命令行控制台连接。

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

相关链接

外围设备兼容性与支持
查看并选择服务器

外围设备兼容性与支持

iKVM 与以下外围设备兼容：

- 采用 QWERTY、QWERTZ、AZERTY 和日式 109 布局的标准 PC USB 键盘。
- 配备 DDC 支持的 VGA 显示器。
- 标准 USB 指针设备。
- 连接到 iKVM 上本地 USB 端口的自供电 USB 1.1 集线器。
- 连接到 Dell M1000e 机箱前面板控制台的电源供电 USB 2.0 集线器。

注: 可以在 iKVM 本地 USB 端口上使用多个键盘和鼠标。iKVM 将汇集输入信号。如果存在来自多个 USB 键盘或鼠标的同时输入信号，则可能产生不可预测的结果。

注: USB 连接专用于支持的键盘、鼠标和 USB 集线器。iKVM 不支持来自其他 USB 外围设备的数据传输。

查看并选择服务器

启动 OSCAR 时，会显示**主菜单**对话框。使用**主菜单**对话框通过 iKVM 查看、配置和管理服务器。可以按名称或插槽查看服务器。插槽编号是服务器所占用的机箱插槽编号。**插槽**列指示安装服务器的插槽编号。

注: Dell CMC 命令行占用插槽 17。选择此插槽显示 CMC 命令行，在此可执行 RACADM 命令或连接到服务器或 I/O 模块的串行控制台。

注: 服务器名称和插槽编号由 CMC 分配。

相关链接

软切换
查看服务器状态
选择服务器

查看服务器状态

Main（主）对话框的右侧边栏指示机箱中服务器的状态。下表介绍了设备状态符号。

表. 44: OSCAR 界面状态符号

符号	说明
	服务器联机。
	服务器脱机或不在机箱中。
	服务器不可用。
	服务器正被由字母表示的用户信道访问： • A=后面板、 • B=前面板。

选择服务器

使用**主菜单**对话框选择服务器。选择服务器时，iKVM 将重新配置键盘和鼠标，使之符合该服务器的正确设置。

- 要选择服务器，请执行以下任一操作：
  - 双击服务器名称或插槽编号。
  - 如果服务器列表的显示次序是按插槽排列（即，“插槽”按钮按下），则键入插槽编号并按下 <Enter>。
  - 如果服务器列表的显示次序是按名称排列（即，“名称”按钮按下），则键入服务器名称的前几个字符，将其建立为唯一名称，然后按两次 <Enter>。
- 要选择上一个服务器，请按下 <Print Screen>，然后按下 <Backspace>。此组合键在上一个和当前连接之间进行切换。
- 要断开用户与服务器的连接，请执行以下任一操作：
  - 按下 <Print Screen> 访问 OSCAR，然后单击“断开连接”。
  - 按下 <Print Screen>，然后按下 <Alt><0>。这将使用户处于可用状态，而未选择任何服务器。桌面上如果有活动的状态标志，则显示为“可用”。请参阅**设置状态标志显示**。

软切换

软切换是使用热键序列在服务器之间进行切换。按 <Print Screen> 可软切换至服务器，然后键入该服务器名称或编号的前几个字符。如果以前设置了**延迟时间**（从按下 <Print Screen> 后到“主菜单”对话框显示前所间隔的秒数），并在该时间结束前按下了键序列，则 OSCAR 界面不会显示。

相关链接

配置软切换

软切换到服务器

配置软切换

要将 OSCAR 配置为软切换，请执行以下操作：

1 按 <Print Screen> 启动 OSCAR 界面。

此时将显示**主菜单**对话框。

2 单击**设置**，然后单击**菜单**。

此时将显示**菜单**对话框。

3 为显示/排序键选择**名称**或**插槽**。

4 在**屏幕延迟时间**字段中键入所需延迟秒数。

5 单击**确定**。

软切换到服务器

要软切换到服务器，请执行以下操作：

- 要选择服务器，请按下 <Print Screen>。如果服务器列表的显示次序为您选择的按插槽排列（即，“插槽”按钮被按下），则键入插槽编号并按下 <Enter>。

  或

  如果服务器列表的显示次序为您选择的按名称排列（即，“名称”按钮被按下），则键入服务器名称的前几个字符，将其建立为唯一名称，然后按下 <Enter>。
- 要切换回到上一个服务器，按下 <Print Screen>，然后按下 <Backspace>。

视频连接

iKVM 在机箱的前面板和后面板上有视频连接。前面板连接信号优先于后面板连接信号。当显示器连接到前面板时，视频连接不会传递到后面板，会显示一条后面板 KVM 和 ACI 连接均已禁用的 OSCAR 消息。如果显示器被禁用（即，被从前面板上卸下或被 CMC 命令禁用），则 ACI 连接成为活动的，而后面板 KVM 仍被禁用。

相关链接

iKVM 连接优先次序

从前面板启用或禁用对 iKVM 的访问

抢占警告

通常，一个通过 iKVM 连接到服务器控制台的用户与另一个通过 iDRAC Web 界面控制台重定向功能连接到同一服务器控制台的用户，均具有对该控制台的访问权并可以同时键入信息。

为防止这种情况，在开始 iDRAC Web 界面控制台重定向之前，远程用户可以禁用 iDRAC Web 界面中的本地控制台。本地 iKVM 用户会看到一条 OSCAR 消息，告知他们该连接在一段特定时间内将被抢占使用。本地用户应在 iKVM 到服务器的连接终止之前使用该控制台完成工作。

未向 iKVM 用户提供任何抢占功能。

注: 如果某个远程 iDRAC 用户已禁用某个特定服务器的本地视频，则该服务器的视频、键盘和鼠标对 iKVM 不可用。服务器状态在 OSCAR 菜单中以一个黄点标记，表示它已被锁定或无法在本地使用，请参阅查看服务器状态。

相关链接

查看服务器状态

设置控制台安全性

OSCAR 允许在 iKVM 控制台上配置安全性设置。可以设置屏幕保护程序模式，如果在指定延迟时间内始终未使用控制台，则启用该模式。一旦启用，控制台将保持锁定状态，直到按下任一键或移动鼠标。输入屏幕保护程序密码可继续操作。

在**安全性**对话框中，可使用密码锁定控制台，设置或更改密码，或启用屏幕保护程序。

注: 如果丢失或忘记了 iKVM 密码，可使用 CMC Web 界面或 RACADM 将其重设为 iKVM 出厂默认值。

相关链接

访问安全性对话框
设置密码
为控制台提供密码保护
设置自动注销
从控制台删除密码保护
启用无密码保护的屏幕保护程序模式
退出屏幕保护程序模式
清除丢失或忘记的密码

访问安全性对话框

要访问**安全性**对话框，请执行以下操作：

1 按下 <Print Screen>。
此时将显示**主菜单**对话框。
2 单击**设置**，然后单击**安全性**。
此时将显示**安全性**对话框。

设置密码

要设置密码，请执行以下操作：

1 单击并按下 <Enter> 或双击**新建**字段。
2 键入新密码，然后按下 <Enter>。密码区分大小写并要求为 5-12 个字符。密码必须至少包含一个字母和一个数字。合法字符为：A-Z、a-z、0-9、空格和连字符。
3 在**重复**字段中，再次键入该密码，然后按下 <Enter>。
4 单击**确定**并关闭此对话框。

为控制台提供密码保护

要为控制台提供密码保护，请执行以下操作：

1 如设置密码所述设置密码。
2 选择**启用屏幕保护程序**框。
3 键入延迟密码保护和屏幕保护程序激活的**非活动时间**的分钟数（从 1 到 99）。
4 对于**模式**：如果显示器符合 ENERGY STAR 标准，选择**节能**；否则，选择**屏幕**。
- 如果模式设置为**节能**，则设备将使显示器置于睡眠模式。这通常以显示器关机和琥珀色指示灯取代绿色电源 LED 表示。
- 如果模式设置为**屏幕**，则在测试过程中 OSCAR 标志会在屏幕上跳动。测试开始之前，警告弹出框会显示以下消息："节能模式可能会损坏非 ENERGY STAR 类型的显示器。不过在开始测试后，可通过鼠标或键盘干预立刻放弃测试。"

小心: 对非 Energy Star 类型的显示器使用“节能”模式可能导致显示器损坏。

5 可选项：要启动屏幕保护程序测试，请单击**测试**。此时将显示**屏幕保护程序测试**对话框。单击**确定**开始测试。
测试需要 10 秒钟。测试完成后将返回到**安全性**对话框。

设置自动注销

您可以将 OSCAR 设置为不活动超过一定时间后自动从服务器注销。

1 在**主菜单**对话框中，单击**设置**，然后单击**安全性**。
2 在**非活动时间**字段中，输入希望在自动断开连接前要与服务器保持连接的时间长度。
3 单击**确定**。

从控制台删除密码保护

要从控制台删除密码保护功能，请执行以下操作：

1 在**主菜单**对话框中，单击**设置**，然后单击**安全性**。
2 在**安全性**对话框中，单击并按下 <Enter>，或双击**新建**字段。
3 让**新**字段保持空白，按下 <Enter>。
4 单击并按下 <Enter>，或双击**重复**字段。
5 让**重复**字段保持空白，按下 <Enter>。
6 单击**确定**。

启用无密码保护的屏幕保护程序模式

注: 如果控制台有密码保护，必须先删除密码保护。在启用无密码保护的屏幕保护模式之前，请先删除密码。

要启用无密码保护的屏幕保护程序模式，请执行以下操作：

1 选择**启用屏幕保护程序**。
2 键入将屏幕保护程序延迟激活的分钟数（1 到 99）。
3 如果显示器符合 ENERGY STAR 标准，选择**节能**；否则，选择**屏幕**。

小心: 对非 Energy Star 类型的显示器使用“节能”模式可能导致显示器损坏。

4 可选：要启动屏幕保护程序测试，请单击**测试**。此时将显示**屏幕保护程序测试**对话框。单击**确定**开始测试。此测试需要 10 秒。在测试完成后，会显示**安全性**对话框。

注: 启用屏幕保护程序模式将断开用户与服务器的连接。这意味着没有选择任何服务器。状态标志显示可用。

退出屏幕保护程序模式

要退出屏幕保护程序模式并返回到**主菜单**对话框，请按下任意键或移动鼠标。
要关闭屏幕保护程序，请在**安全性**对话框中，清除**启用屏幕保护程序**框，然后单击**确定**。

要立刻打开屏幕保护程序，请按下 <Print Screen>，然后按下 <Pause>。

清除丢失或忘记的密码

当丢失或忘记了 iKVM 密码时，可将其重设为 iKVM 出厂默认值，然后更改密码。可使用 CMC Web 界面或 RACADM 重设密码。
要使用 CMC Web 界面重设丢失或忘记的 iKVM 密码，请在系统树中，转至**机箱概览** > **iKVM**，单击**设置**选项卡，然后单击**恢复默认值**。

您可以使用 OSCAR 更改默认密码。有关更多信息，请参阅设置密码。

要使用 RACADM 重设丢失或忘记的密码，请打开一个至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm racresetcfg -m kvm
```

注: 如果“前面板启用”和“Dell CMC 控制台启用”设置与默认值不同，请使用 `racresetcfg` 命令重设这些设置。

有关 `racresetcfg` 子命令的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

更改语言

使用**语言**对话框更改 OSCAR 文本以任何支持的语言显示。所有 OSCAR 屏幕上的文本会立刻更改为所选语言。
要更改 OSCAR 语言，请执行以下操作：

1 按下 <Print Screen>。
此时将显示**主菜单**对话框。
2 单击**设置**，然后单击**语言**。
此时会显示**语言**对话框。
3 选择所需的语言并单击**确定**。

显示版本信息

使用**版本**对话框显示 iKVM 固件和硬件版本，并标识语言和键盘配置。
要显示版本信息，请执行以下操作：

1 按下 <Print Screen>。
此时将显示**主菜单**对话框。
2 单击**命令**，然后单击**显示版本**。
此时将显示**版本**对话框。**版本**对话框的上半部分列出子系统版本。
3 单击  或按下 <Esc> 关闭**版本**对话框。

扫描系统

在扫描模式下，iKVM 自动逐个插槽（逐个服务器）进行扫描。通过指定要扫描的服务器和每个服务器的显示秒数，可扫描多达 16 个服务器。

相关链接

将服务器添加到扫描列表
从扫描列表删除服务器
启动扫描模式
取消扫描模式

将服务器添加到扫描列表

要将服务器添加到扫描列表中，请执行以下操作：

1 按下 <Print Screen>。

此时将显示**主菜单**对话框。

2 单击**设置**，然后单击**扫描**。
此时将显示**扫描**对话框，其中列出机箱中的所有服务器。

3 请执行以下功能之一：
- 选择您要扫描的服务器
- 双击该服务器名称或插槽。
- 按 <Alt> 和要扫描的服务器数量。您最多可以选择 16 个服务器。

4 在**时间**字段中，输入希望 iKVM 在扫描移动到序列中下个服务器之前将等待的秒数（3 到 99）。

5 单击**添加**，然后单击**确定**。

从扫描列表删除服务器

要从扫描列表中删除服务器，请执行以下操作：

1 在**扫描**对话框中，执行以下任一操作：
- 选择要删除的服务器。
- 双击该服务器名称或插槽。
- 单击**清除**从**扫描**列表中删除所有服务器。

2 单击**添加**，然后单击**确定**。

启动扫描模式

要启动扫描模式，请执行以下操作：

1 按下 <Print Screen>。
此时将显示**主菜单**对话框。

2 单击**命令**。
此时将显示**命令**对话框。

3 选择**扫描启用**选项。

4 单击**确定**。
此时将显示一条鼠标和键盘均已重设的消息。

5 单击  关闭该消息框。

取消扫描模式

要取消扫描模式，请执行以下操作：

1 如果 OSCAR 打开并且显示有**主菜单**，则选择列表中的服务器。
或

如果 OSCAR 未打开，移动鼠标或按下键盘上的任一键。
此时将显示**主菜单**对话框；选择列表中的服务器。

2 单击**命令**。
此时将显示**命令**对话框。

3 清除**扫描启用**选项并单击**确定**。

广播至服务器

您可以同时控制系统中的多个服务器，确保全部所选服务器都接收相同的输入。您可以选择自行广播击键操作和/或鼠标移动：

- 广播击键操作：当使用击键操作时，接收一个要给予相同解释的击键操作广播的所有服务器的键盘状态必须相同。具体说，所有键盘上的 <Caps Lock> 和 <Num Lock> 模式必须相同。当 iKVM 尝试向所选服务器同时发送击键操作时，某些服务器可能会禁止并进而延迟传输。
- 广播鼠标移动：要使鼠标准确工作，所有服务器必须具有相同的鼠标驱动程序、桌面（如一致放置的图标）和视频分辨率。鼠标在所有屏幕上也必须完全处于相同位置。由于这些条件很难实现，所以向多个服务器广播鼠标移动可能会导致不可预测的结果。

注: 一次可广播多达 16 个服务器。

要广播至服务器，请执行以下操作：

1 按下 <Print Screen>。
此时将显示**主菜单**对话框。
2 单击**设置**，然后单击**广播**。
此时将显示**广播**对话框。
3 通过选择方框启用要接收广播命令的服务器的鼠标和/或键盘。
或
按上下箭头键使鼠标移动到一个目标服务器。然后按下 <Alt> <K> 选择键盘框和/或按下 <Alt> <M> 选择鼠标框。对其他服务器重复这一操作。
4 单击**确定**保存设置并返回到**设置**对话框。
5 单击 或按下 <Escape> 返回到**主菜单**对话框。
6 单击**命令**。
此时将显示**命令**对话框。
7 单击**广播启用**框激活广播。
此时将显示**广播警告**对话框。
8 单击**确定**启用广播。要取消并返回**命令**对话框，请单击 或按 <Esc>
9 如果已启用广播，键入要从管理站广播的信息和/或执行要从管理站广播的鼠标运动。只有列表中的服务器可以访问。

从 CMC 管理 iKVM

可以执行以下操作：

- 查看 iKVM 状态和属性
- 更新 iKVM 固件
- 从前面板启用或禁用对 iKVM 的访问
- 从 Dell CMC 控制台启用或禁用对 iKVM 的访问

相关链接

更新 iKVM 固件
从前面板启用或禁用对 iKVM 的访问
查看 iKVM 信息和运行状况
从 Dell CMC 控制台启用对 iKVM 的访问

从前面板启用或禁用对 iKVM 的访问

可使用 Web 界面或 RACADM 从前面板启用或禁用对 iKVM 的访问。

使用 Web 界面从前面板启用或禁用对 iKVM 的访问

要使用 Web 界面从前面板启用或禁用对 iKVM 的访问功能，请执行以下操作：

1 在系统树中，转至**机箱概述** > **iKVM**，然后单击**设置**选项卡。
此时将显示 **iKVM 配置**页。
2 要启用此功能，请选中**前面板 USB/视频已启用**选项。要禁用此功能，请清除**前面板 USB/视频已启用**选项。
3 单击**应用**保存设置。

使用 RACADM 从前面板启用或禁用对 iKVM 的访问

要使用 RACADM 从前面板启用或禁用对 iKVM 的访问功能，打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <value>
```

其中，<value> 是 1（启用）或 0（禁用）。有关

```
config
```

子命令的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e RACADM 的 Chassis Management Controller 命令行参考指南）。

从 Dell CMC 控制台启用对 iKVM 的访问

要使用 CMC Web 界面从 iKVM 启用对 CMC CLI 的访问，请在系统树中，转至**机箱概述** > **iKVM**，然后单击**设置**选项卡。选择**允许从 iKVM 访问 CMC CLI** 选项，并单击**应用**保存设置。

要使用 RACADM 从 iKVM 启用对 CMC CLI 的访问，打开一个至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

相关链接

使用串行、Telnet 或 SSH 控制台登录 CMC

15

管理和监测电源

Dell PowerEdge M1000e 服务器机柜是最具有电源效率的模块化服务器机柜。它设计独特，包括高效率的电源设备和风扇，拥有优化的布局使气流在系统内畅通无阻，并且机柜中处处包含电源优化的组件。最优化的硬件设计配合内置到机箱管理控制器 (CMC)、电源设备和 iDRAC 中的先进电源管理功能，使您能够进一步提高电源效率并全面控制电源环境。

M1000e 的电源管理功能可帮助管理员配置机柜减少功耗，调整功率以满足环境的特定需要。

PowerEdge M1000e 模块化机柜消耗功率，并在所有当前使用中的内部电源设备装置 (PSU) 上进行负载分配。系统最多能够提供 16685 瓦 输入功率分配给服务器模块和关联的机柜基础结构。

PowerEdge M1000e 机柜可针对影响 PSU 行为的三种冗余策略之一进行配置，并且可以决定如何向管理员报告机箱冗余状态。

您还可以通过 **Dell OpenManage Power Center** 控制电源管理。如果 **Dell OpenManage Power Center** 在外部控制电源，CMC 会继续保留：

- 冗余策略
- 远程电源日志记录
- 服务器性能优先于电源冗余
- 动态电源设备接入 (DPSE)
- 110 V 交流操作 - 这仅支持交流 PSU。

Dell OpenManage Power Center 则可管理：

- 服务器电源
- 服务器优先级
- 系统输入功率容量
- 最大节能模式

注: 实际电源传输基于配置和工作负载。

可以使用 CMC Web 界面或 RACADM 管理和配置 CMC 电源控制：

- 查看电源分配情况、功耗以及机箱、服务器和 PSU 的状态。
- 配置机箱的电源预算和冗余策略。
- 执行机箱电源控制操作（开机、关机、系统重设、关机后再开机）。

主题：

- 查看电源预算状态
- 冗余状态和总体电源运行状况
- 配置电源预算和冗余
- 执行电源控制操作

相关链接

冗余策略
动态电源设备接入
默认冗余配置
硬件模块电源预算
查看功耗状态
查看电源预算状态
冗余状态和总体电源运行状况
配置电源预算和冗余
执行电源控制操作

冗余策略

冗余策略是一组可配置的属性，它可以确定 CMC 如何管理到机箱的电源。以下冗余策略可配置带或不带动态 PSU 接入：

- 电网冗余
- 电源设备冗余
- 无冗余

电网冗余策略

电网冗余策略的目的是使模块化机柜系统能够在可承受电源故障的模式下运行。这些故障可能因输入电网、布线和传输或 PSU 本身而引起。

在为电网冗余配置系统时，PSU 按电网划分：插槽 1、2 和 3 中的 PSU 在第一个电网，而插槽 4、5 和 6 中的 PSU 在第二个电网。CMC 管理电源，这样即使有一个电网出现故障，系统仍可继续正常运行而不受影响。电网冗余也可承受单个 PSU 的故障。

注: 电网冗余使得即使一个电网出现故障服务器也能无缝运行。因此，两个电网的容量基本相等时，最大功率应该满足维持电网冗余的需要。

注: 电网冗余仅在负载要求不超过供电能力最低的电网容量时可实现。

电网冗余级别

要配置电网冗余，必须在每个电网中至少配置一个 PSU。也可进行其他配置，让每个组合在每个电网中至少有一个 PSU。但是，为了提供最大可用功率，各电网中 PSU 的总功率应尽可能相当。维持电网冗余时的功率上限是两个电网中供电能力较低的电网的可用功率。下图说明了每个电网 2 个 PSU 和电网 1 上的供电故障。

如果配置了**冗余丢失**事件警报，则 CMC 无法维持电网冗余时给管理员发送电子邮件或 SNMP 警报。

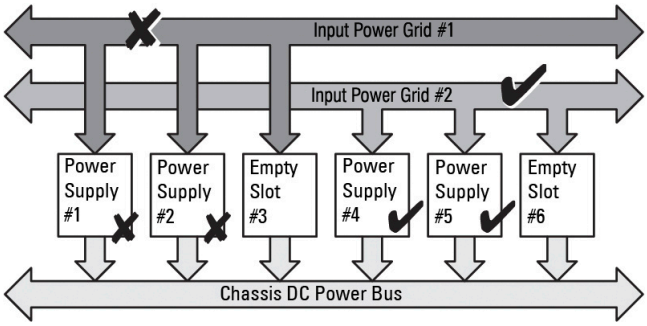


图 14: 每个电网 2 个 PSU 和电网 1 上的供电故障

如果此配置中的一个 PSU 出现故障，发生故障的电网中的其余 PSU 将被标记为“联机”。在这种情况下，如果冗余电网中的 PSU 不是处于故障状态，则会帮助系统正常工作而不会发生中断。如果一个 PSU 出现故障，机箱运行状况将被标记为“不严重”。如果电网较小而无法支持整个机箱的电源分配，电网冗余状态将报告为**无冗余**，机箱运行状况显示为**严重**。

电源设备冗余策略

电源设备冗余策略在冗余电源电网不可用时发挥作用，但您可能希望防止因单个 PSU 出现故障而导致模块化机柜中的服务器停机。供电能力最高的 PSU 将为此目的而联机保留。这样就形成了电源设备冗余池。下图说明电源冗余模式。

超出功率和冗余所需的 PSU 仍可用并会在出现故障时添加到池。

与电网冗余不同的是，选择电源设备冗余后，CMC 不要求 PSU 装置存在于任何特定 PSU 插槽位置。

注: 动态电源设备接入 (DPSE) 允许将 PSU 置于待机状态。该待机状态表示 PSU 未接受供电的实际状态。启用 DPSE 时，可将额外的 PSU 置于待机模式，以提高效率和节约用电。

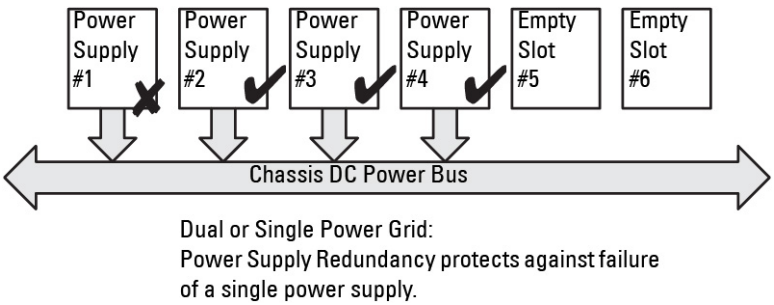


图 15: 电源设备冗余：合计 4 个 PSU，其中 1 个 PSU 故障

注: 建议机柜关机时，修改模块化机柜冗余策略。

无冗余策略

无冗余模式是 3 PSU 配置的出厂默认设置，表示机箱没有配置任何电源冗余。在这种配置下，机箱的总体冗余状态始终表示无冗余。下图说明无冗余模式是 3 PSU 配置的出厂默认设置。

配置**无冗余**时，CMC 不要求 PSU 设备在任何特定的 PSU 插槽位置中显示。

注: 如果在无冗余模式中禁用 DPSE，则机箱中的所有 PSU 均列为联机。在 DPSE 启用时，机箱中所有当前使用中的 PSU 均列为联机，而附加 PSU 可能转入待机模式以提高系统功效。

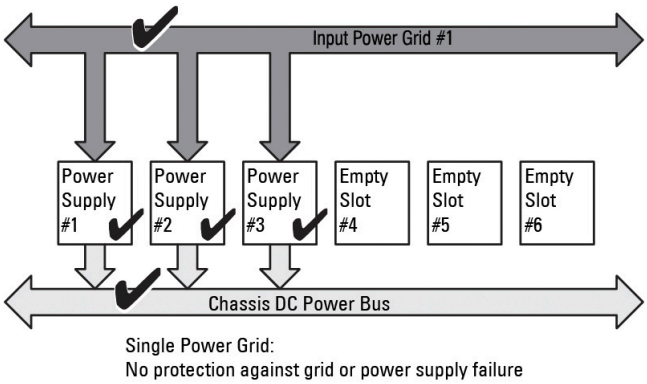


图 16: 机箱中 3 个 PSU 且无冗余

出现 PSU 故障时，系统会根据需要使其他 PSU 退出待机模式，以便支持机箱的电源分配。如果有 4 个 PSU 而只需要 3 个，则在 1 个 PSU 出现故障时第 4 个 PSU 会联机。一个机箱可让所有 6 个 PSU 均联机。

启用 DPSE 时，额外的 PSU 置于待机模式以提高效率和节约用电。有关更多信息，请参阅默认冗余配置。

扩展电源性能

与使用 3000 W AC PSU 的网格冗余性配置中的冗余电源相比，扩展电源性能 (EPP) 模式支持在六个电源设备的配置 (PSU) 中为 M1000e 机箱分配 30% 的额外电源。但是，如果发生 AC 网格故障或 PSU 故障，分配给服务器的电源将自动降低，以避免服务器关机。可分配最高 2700 W 电源，以支持具有高端配置的机箱。

默认情况下，在六个 3000 W AC 电源设备的配置上已启用 EPP 功能。您可以使用 Web 界面和命令行界面查看当前设置以及禁用和启用此功能。

EPP 功能仅在以下情况中允许功率分配：

- 为电网冗余配置功率。
- 具有 6 个 3000W AC 类型的 PSU。
- 系统输入功率上限值高于 13300W AC (45381 BTU/h)。

使用 EPP 模式获取的电源可用于提高服务器性能。与六个 2700 W AC PSU 配置相比，采用增强的冷却模式以启用和激活风扇的六个 3000W AC PSU 提供的额外功率是 723 W。与六个 2700 W AC PSU 配置相比，标准风扇配置模式中提供的额外功率为 1023 W。

可用的 EPP 额外功率为 2700W，此功率可用于提高服务器性能。

仅在禁用了以下电源功能后，方可启用 EPP 模式：

- 最大节能模式 (MPCM)
- 动态电源设备接入 (DPSE)
- 基于服务器的电源管理 (SBPM)
- 服务器性能优先于电源冗余 (SPOPR)

在已启用 MPCM、DPSE、SBPM 或 SPOPR 模式之一的情况下尝试启用 EPP 时，将导致显示一条消息。此消息可以在启用扩展电源性能模式之前提示您禁用这四个功能。扩展电源性能模式已启用时，DPSE、SBPM 或 SPOPR 这三种功能中的任意一种都无法启用。系统将提示您禁用扩展电源性能功能，然后才可以启用这三种功能中的任意一种。

当机箱配有 3000 W AC PSU 时，将固件降级到低于 CMC 4.5 的固件版本将被当前固件阻止。这是因为低于 CMC 4.5 的 CMC 固件版本不支持 3000 W AC PSU。

采用扩展电源性能的默认电源配置

当启用或禁用了 EPP 模式后，机箱上的默认电源配置：

- 在采用电网冗余策略的六个 3000 W 交流 PSU 配置上：
  EPP 已启用 – DPSE 已禁用、SPOPR 已禁用、MPCM 已禁用、SBPM 已禁用
- 在 3000 W 交流 PSU 配置上运行命令 `racadm racresetcfg`，将电源配置重置为以下值：
  EPP 已禁用 – DPSE 已禁用、SPOPR 已禁用、MPCM 已禁用、SBPM 已禁用
- 在少于六个 3000 W 交流 PSU 的配置上：
  EPP 已禁用 – DPSE 已禁用、SPOPR 已禁用、MPCM 已禁用、SBPM 已禁用
- 在 2700 W 交流 PSU 配置上：
  EPP 已禁用 – DPSE 已禁用、SPOPR 已启用、MPCM 已禁用、SBPM 已禁用
- 在 2700 W 交流 PSU 配置上使用 racadm racresetcfg，将电源配置重置为以下值：
  EPP 已禁用 – DPSE 已禁用、SPOPR 已禁用、MPCM 已禁用、SBPM 已禁用
- 在启用 Fresh Air 的机箱配置上，3000W PSU 显示为 2800W，并且不支持 EPP。

动态电源设备接入

默认情况下禁用动态电源设备接入 (DPSE) 模式。DPSE 可通过优化 PSU 向机箱供电的功效而节电。这样还可延长 PSU 的使用寿命、减少热量产生。

CMC 可监测机柜全部电源分配，并且可将 PSU 移至待机状态。将 PSU 移至待机状态有以下作用：

- 通过较少的 PSU 为机箱提供全部电源分配。
- 提高联机 PSU 在高利用率下的运行效率。
- 提高待机 PSU 的运行效率和持久性。

若要其余 PSU 在最大效率下工作：

- 带有 DPSE 的**无冗余**模式具有很高的电源效率，且有最佳数目的 PSU 处于联机状态。不需要的 PSU 置于待机模式。
- 启用 DPSE 的 **PSU 冗余**模式也具有电源效率。至少两个电源设备处于联机状态，其中一个 PSU 为配置提供电力，另一个在出现 PSU 故障时提供冗余。“PSU 冗余”模式可以在任何一个 PSU 出现故障时提供保护，但在交流电网断电时不提供保护。
- 启用 DPSE 的**电网冗余**模式（至少有两个电源设备处于活动状态，每个电网中有一个），在部分负载模块化机柜配置的效率和最大可用性之间实现出色的平衡。
- 禁用 DPSE 会使得效率最低，因为全部六个电源设备都活动并且共享负载，导致每个电源设备的利用率降低。

可针对所有三个电源设备冗余配置启用 DPSE - **无冗余**、**电源设备冗余**和**电网冗余**。

- 在启用 DPSE 的**无冗余**配置中，M1000e 最多可让五个电源设备装置处于**待机**状态。在六 PSU 配置中，有些 PSU 装置处于**待机**模式并保持不使用状态，以便提高电源效率。卸下此配置中的联机 PSU 或它们出现故障时，会导致处于**待机**状态的 PSU 变为**联机**；不过，待机 PSU 需要至多 2 秒钟才能变为活动状态，所以部分服务器模块在**无冗余**配置中的过渡期间可能断电。

  注: 在三 PSU 配置中，服务器负载可能阻止任何 PSU 过渡到“待机”。
- 在**电源设备冗余**配置中，除了机柜开机所需的 PSU 之外，机柜始终保持一个附加的 PSU 处于开启状态并标记为**联机**。电源利用情况受监测，根据总体系统负载，最多四个 PSU 可转到“待机”状态。在六 PSU 配置中，最少两个电源设备装置始终保持开启。

  因为采用 **电源设备冗余**配置的机柜始终启用一个额外的 PSU，所以当一个联机 PSU 出现故障时，机柜仍能正常工作，并且仍能为安装的服务器模块提供充足的电力。当联机 PSU 出现故障时，待机 PSU 将变为联机状态。多个 PSU 同时出现故障可能导致某些服务器模块断电，同时待机 PSU 开机。

- 在**电网冗余**配置中，所有电源设备在机箱开机时都会接入。电源利用情况受监测，如果系统配置和电源利用情况允许，可以将 PSU 移至**待机**状态。电网中的 PSU **联机**状态会镜像其他电网中的情况。因此，机柜可以承受整个电网断电而不会中断给机柜供电。

  电网冗余配置中功率要求的增加会造成 PSU 从**待机**状态接入。这可以保持双电网冗余所需的镜像配置。

注: 启用了 DPSE 时，在三种电源冗余策略模式中，当电源需求增加时，待机 PSU 都会转为联机以收回电源。

默认冗余配置

机箱的默认冗余配置取决于它所含的 PSU 的数量，如下表所示。

表. 45: 默认冗余配置

PSU 配置	默认冗余策略	默认动态 PSU 接入设置
6 PSU	网格冗余	已禁用
3 PSU	无冗余	已禁用

电网冗余

在六 PSU 电网冗余模式中，所有六个 PSU 都处于活动状态。左侧的三个 PSU 必须连接至一个输入电网，同时右侧的三个 PSU 连接到另一个电网。

小心: 为了避免系统故障并使电网冗余有效工作，必须有正确连接到不同电网的均衡 PSU 组。

如果一个电网出现故障，连接至正常运行的电网的 PSU 将接替供电任务，而不会中断服务器或基础结构。

小心: 在电网冗余模式中，必须具有均衡的 PSU 组（每个电网至少有一个 PSU）。如果此条件不能满足，则不能实现电网冗余。

电源设备冗余

启用电源设备冗余时，机箱中的一个 PSU 保持为备用状态，确保任何一个 PSU 的故障不会造成服务器或机箱断电。电源设备冗余模式最多需要四个 PSU。启用 DPSE 后，如果存在额外的 PSU，会使用该 PSU 提高系统的电源效率。冗余丢失后，如果发生故障，可能会导致机箱中的服务器断电。

无冗余

超出机箱供电必需部分的电源即使在故障时仍可用于继续为机箱供电。

小心: 为机箱需求启用 DPSE 后，“无冗余”模式使用优化的 PSU。单个 PSU 故障可导致服务器在此模式下断电和丢失数据。

硬件模块电源预算

CMC 提供电源预算服务，它能够为机箱配置电源预算、冗余和动态电源。

电源管理服务能够优化功耗并根据需要将电源重新分配到不同的模块。

下图显示包含六个 PSU 配置的机箱。PSU 的编号从机柜左侧开始分别为 1-6。

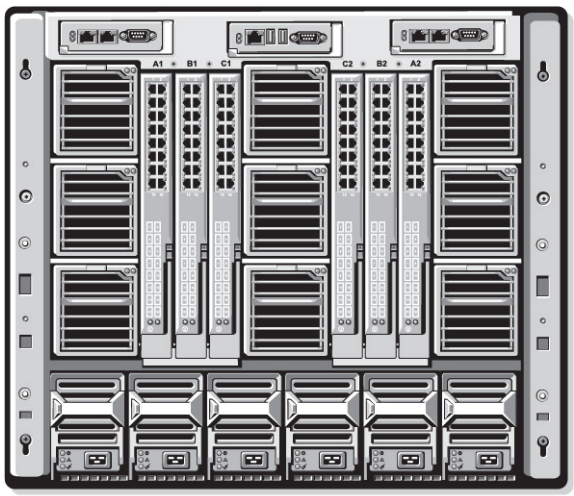


图 17: 配备六个 PSU 的机箱

CMC 为机柜保持电源预算，为所有安装的服务器和组件保留所需功率。

CMC 将功率分配给机箱中的 CMC 基础结构和服务器。CMC 基础结构由机箱中的组件组成，例如风扇、I/O 模块和 iKVM（如果存在）。机箱最多可配备 16 个服务器，这些服务器通过 iDRAC 与机箱通信。有关更多信息，请参阅 **support.dell.com/manuals** 上的 *iDRAC User's Guide*（iDRAC 用户指南）。

服务器开机之前，iDRAC 为 CMC 提供其功率范围需求。功率范围包含可以使服务器运行的最大功率需求和最小功率需求。iDRAC 的初始估计值以其对服务器中组件的初步了解为根据。在工作开始后发现其他组件时，iDRAC 可增加或降低其初始功率要求。

机柜中的服务器开机时，iDRAC 软件重新估计功率需求，并请求随后对功率范围做出调整。

CMC 准许服务器请求的功率，并且从可用预算中减去分配的功率。一旦准许服务器的一个功率请求，服务器的 iDRAC 软件就对实际功耗进行连续监控。iDRAC 功率范围会根据实际功率需求而随时间发生变化。只有服务器完全消耗分配的功率时，iDRAC 才会请求升高功率。

在重负载下，可降低服务器处理器的性能以确保功耗低于用户配置的*系统输入功率上限*。

PowerEdge M1000e 机柜可以为大部分服务器配置的峰值性能提供充足的电能，但许多可用的服务器配置并不会消耗机柜所能提供的最大功率。为了帮助数据中心为它们的机柜提供电源，M1000e 允许您指定*系统输入电源上限*以确保总体机箱交流电源消耗量保持在给定阈值之下。CMC 首先确保提供足够的电能以运行风扇、IO 模块、iKVM（如果存在）和 CMC 自身。此电源分配称作 *分配给机箱基础结构的输入电源*。机柜中的服务器在机箱基础结构后开机。任何将*系统输入功率上限*设置为低于实际功耗的尝试都会失败。

如果需要总体电源预算始终低于*系统输入功率上限*的值，CMC 会为服务器分配一个小于其最大请求功率的值。服务器根据其*服务器优先级*设置获得分配的电力，拥有优先级 1 的服务器获得最大电力，拥有优先级 2 的在拥有优先级 1 的服务器之后获得电力，以此类推。优先级较低的服务器获得的电力可能少于拥有优先级 1 的服务器，这取决于*系统输入最大电源容量*和用户配置的*系统输入功率上限*设置。

如果发生诸如在机箱中增加服务器等配置变化，可能需要提高*系统输入电源上限*。在热条件变化并且需要风扇以更快速度运转时，都会造成它们消耗更多电力，模块化机柜中的电力需求也会随之增加。插入 I/O 模块和 iKVM 也会增加模块化机柜的电力需求。即便是为了保持管理控制器运行而关闭服务器时，也会消耗相当少量的电力。

只有在电力充足时才能打开模块化机柜中的更多服务器。可随时将 *系统输入功率上限*提高到最大 16685W 的值，以允许带动额外的服务器。

模块化机柜中减少功率分配的变动为：

- 服务器电源关闭

- 服务器
- I/O 模块
- iKVM 拆卸
- 机箱过渡到断电状态

机箱打开或关闭时均可重新配置*系统输入电源上限*。

服务器插槽电源优先级设置

CMC 允许您为机柜中十六个服务器插槽的每一个插槽设置电源优先级。优先级设置从 1（最高）到 9（最低）。这些设置被分配给机箱中的插槽，并且插槽的优先级将被插入该插槽中的任何服务器继承。CMC 使用插槽优先级将电源优先预算给机柜中最高优先级服务器。

根据默认服务器插槽优先级设置，电源将平均分配给所有插槽。更改插槽优先级允许管理员区分为哪些服务器优先分配电源。如果更重要的服务器模块保持它们的默认插槽优先级为 1，并且不太重要的服务器模块更改为更低的优先级值 2 或以上，优先级为 1 的服务器模块将首先开机。然后这些更高优先级服务器将获得最大电源分配，而可能不会为更低优先级服务器分配足够电源以便它们以最高性能运行，甚至根本不开机，这取决于设置的系统输入功率上限有多低以及服务器电源要求。

如果管理员在更高优先级服务器之前为低优先级服务器模块手动开机，低优先级服务器模块将首先成为让其功率分配下降到最小调节值的模块，以满足更高优先级的服务器。所以在可供分配的功率耗尽后，CMC 会从较低或同等优先级服务器中收回功率分配直到其达到最低功耗水平。

注: I/O 模块、风扇和 iKVM（如果存在）具有最高优先级。CMC 仅收回低优先级设备的电源以满足优先级更高的模块或服务器的电源需求。

为服务器分配优先级

服务器优先级确定当需要额外电源时，CMC 将从哪台服务器开始节电。

注: 为服务器分配的优先级取决于插槽而不是服务器本身。如果将服务器移动到新插槽，则必须为新插槽位置重新配置优先级。

注: 要执行电源管理操作，必须具有机箱配置管理员权限。

使用 CMC Web 界面为服务器分配优先级

要使用 CMC Web 界面分配优先级，请执行以下操作：

1 在系统树中，转至**服务器概览**，然后单击**电源** > **优先级**。
服务器优先级页会列出机箱中的所有服务器。
2 为一台、多台或全部服务器选择优先级（1-9，1 代表最高优先级）。默认值为 1。可以为多台服务器分配相同的优先级。
3 单击 **Apply**（应用）保存所做的更改。

使用 RACADM 为服务器分配优先级

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <slot number> <priority level>
```

其中 *<slot number>* (1-16) 指代服务器位置，而*<priority level>*为 1-9 之间的值。

例如，要为插槽 5 中的服务器设置为优先级 1，请键入以下命令：

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

查看功耗状态

CMC 为整个系统提供实际输入功耗。

使用 CMC Web 界面查看功耗状态

要使用 CMC Web 界面查看功耗状态，请在系统树中，转至**机箱概述**并单击**电源** > **电源监测**。“电源监测”页显示电源运行状态、系统电源状态、实时电源统计数据和实时能量统计数据。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

注: 您还可以在系统树 > 状态选项卡中的“电源设备”下查看电源冗余状态。

使用 RACADM 查看功耗状态

要使用 RACADM 查看功耗状态，请执行以下操作：

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm getpminfo
```

查看电源预算状态

可使用 CMC Web 界面或 RACADM 查看电源预算状态。

使用 CMC Web 界面查看电源预算状态

要使用 CMC Web 界面查看电源预算状态，请在系统树中，转至**机箱概述**，然后单击**电源** > **预算状态**。**电源预算状态**页显示系统电源策略配置、电源预算详情、为服务器模块分配的预算以及机箱电源设备详情。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

使用 RACADM 查看电源预算状态

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm getpbinfo
```

有关 **getpbinfo** 的更多信息（包括输出详情），请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 **getpbinfo** 命令部分。

冗余状态和总体电源运行状况

冗余状态是确定总体电源运行状况的一个因素。例如，如果电源冗余策略设置为电网冗余，并且冗余状态指示系统正在运行并且有冗余，则总体电源运行状况通常是**正常**。如果机箱上安装的 PSU 由于某种原因出现故障，则机箱的总体电源运行状况显示为**非严重**。不过，如果在设置电网冗余下运行状况无法满足，冗余状态为**否**，总体电源运行状况为**严重**。这是因为系统无法按照配置的冗余策略运行。

注: 将冗余策略更改为电网冗余或将电网冗余更改为冗余策略时，CMC 不会预先检查这些条件。因此，配置冗余策略可能会直接导致冗余丢失或重新获得条件。

相关链接

在降级或无冗余策略情况下的 PSU 故障
在降级或无冗余策略的情况下拆除 PSU
新的服务器接入策略
系统事件日志中的电源和冗余策略更改

在降级或无冗余策略情况下的 PSU 故障

当发生电源不足事件（如 PSU 故障）时，CMC 将减少为服务器供电。减少服务器的电源后，CMC 会重新评估机箱的电源需求。如果电源要求仍未满足，则 CMC 会关闭优先级较低的服务器。

当电源需求维持在功率预算内时，更高优先级服务器的功率逐步恢复。要设置冗余策略，请参阅配置功率预算和冗余。

注: 当机箱超过功率预算时，CMC 会显示消息：由于没有足够的电源无法开启模块-x。

在降级或无冗余策略的情况下拆除 PSU

当您卸下 PSU 或拔下 PSU 交流电缆时，CMC 可能会启动节电功能。CMC 会降低优先级较低服务器的供电，直到机箱中剩余的 PSU 能够支持电源分配。如果卸下多个 PSU，CMC 将在拆卸第二个 PSU 时重新评估电源需求以确定固件响应。如果仍然不满足电源需求，CMC 可能会关闭优先级较低的服务器。

限制

- CMC 不支持对较低优先级的服务器进行*自动*断电，从而为较高优先级的服务器提供足够的电源；但是，它支持执行用户初始化的断电。
- 对 PSU 冗余策略的更改受限于机箱中的 PSU 数量。可以选择默认冗余配置中列出的三种 PSU 冗余配置设置的任意一种。

新的服务器接入策略

如果开启的新服务器所需功率超过了机箱可利用的功率，CMC 可能会降低低优先级服务器的功率，以便为新服务器腾出更多的电力。以下条件下会发生这种情况：

- 管理员配置了机箱功率限制，低于服务器所有功率分配所需的电力。
- 无法满足机箱中所有服务器最坏情况下的电源需求。

如果通过减少为较低优先级服务器分配的电力依旧无法腾出足够的电力，则新服务器可能无法开机。

运行机箱和所有服务器（包括新添加的服务器）所需的最高持续电源即为最坏情况下的电源需求。如果可以提供该电源量，则不会为任何服务器分配低于最坏情况下所需的电源，并且允许新服务器开机。

下表提供在先前描述的情形下新服务器开机时 CMC 所采取的措施。

表. 46: 尝试打开服务器电源时的 CMC 响应

是否满足最差情况下的电源需求	CMC 响应	打开服务器电源
是	不需要节能	允许
否	执行节能：	允许
	• 能够提供新服务器所需的电源	不允许

是否满足最差情况下的电源需求	CMC 响应	打开服务器电源
	• 不能提供新服务器所需的电源	

如果一个 PSU 出现故障，会导致非严重运行状况，并生成 PSU 故障事件。拆下 PSU 时，会生成 PSU 拆下事件。

如果任一事件导致冗余丢失，根据电源分配，将生成*冗余丢失*事件。

如果随后的电源容量或用户电源容量大于服务器分配容量，服务器的性能会降低，在最坏情况下，服务器可能会断电。在这两种条件下都以相反优先级的顺序进行，也就是优先级较低的服务器先断电。

下表提供应用各种 PSU 冗余配置后固件对 PSU 断电或卸载的响应。

表. 47: PSU 故障或卸下对机箱的影响

PSU 配置	动态 PSU 接入	固件响应
网格冗余	Disabled（已禁用）	CMC 警告您失去电网冗余。
电源设备冗余	Disabled（已禁用）	CMC 警告您失去电源设备冗余。
无冗余	Disabled（已禁用）	如果需要，可以减少为低优先级服务器分配的电源。
网格冗余	Enabled（已启用）	CMC 警告您失去电网冗余。将打开待机模式的 PSU（如果有）以补偿 PSU 故障或卸载造成的电源预算损失。
电源设备冗余	Enabled（已启用）	CMC 警告您失去电源设备冗余。将开启待机模式的 PSU（如果有）以补偿 PSU 故障或卸下造成的电源预算损失。
无冗余	Enabled（已启用）	如果需要，可以减少为低优先级服务器分配的电源。

系统事件日志中的电源和冗余策略更改

将电源状态和电源冗余策略的更改记录为事件。在系统事件日志 (SEL) 中记录条目的有关电源的事件包括电源插入和拆卸、电源输入插入和拆卸以及电源输出确认和未确认。

下表列出与电源更改有关的 SEL 条目：

表. 48: 电源更改的 SEL 事件

电源事件	系统事件日志 (SEL) 条目
插入	Power supply <*number*> is present.（电源设备 <number> 已存在。）
卸下	Power supply <*number*> is absent.（电源设备 <number> 缺失。）
Grid or Power Supply Redundancy lost（电网或电源设备冗余丢失）	Power supply redundancy is lost.（电源设备冗余丢失。）
Grid or Power Supply Redundancy regained（电网或电源设备冗余已重新获得）	The power supplies are redundant.（电源设备冗余。）
Input power received（输入功率已接收）	The input power for power supply <*number*> has been restored.（电源设备 <number> 的输入功率已还原。）

电源事件	系统事件日志 (SEL) 条目
Input power lost（输入功率丢失）	The input power for power supply <*number*> has been lost.（电源设备 <number> 的输入功率已丢失。）
产生直流输出	Power supply <*number*> is operating normally.（电源设备 <number> 运行正常。）
直流输出丢失	Power supply <*number*> failed.（电源设备 <number> 故障。）
Input over-voltage（输入电压过高）	An over voltage fault detected on power supply <*number*>.（在电源设备 <number> 上检测到电压过高故障。）
Input under-voltage（输入电压过低）	An under voltage fault detected on power supply <*number*>.（在电源设备 <number> 上检测到电压过低故障。）
Input over-current（输入电流过高）	An over current fault detected on power supply <*number*>.（在电源设备 <number> 上检测到电流过高故障。）
Input under-current（输入电流过低）	An undercurrent fault detected on power supply <*number*>.（在电源设备 <number> 上检测到电流过低故障。）
DC output under-voltage（直流输出电压过低）	An output under voltage fault detected on power supply <*number*>（在电源设备 <number> 上检测到输出电压过低故障。）
DC output over-current（直流输出电流过高）	An output over current fault detected on power supply <*number*>.（在电源设备 <number> 上检测到输出电流过高故障。）
DC output under-current（直流输出电流过低）	An output under current fault detected on power supply <*number*>.（在电源设备 <number> 上检测到输出电流过低故障。）
Communication failure（通信故障）	Cannot communicate with power supply <*number*>.（无法与电源设备 <number> 通信。）
Communication restored（通信已还原）	Communication has been restored to power supply <*number*>.（与电源设备 <number> 的通信已还原。）
Failure to communicate status data（无法传送状态数据）	Cannot obtain status information from power supply <*number*>.（无法从电源设备 <number> 获取状态信息。）
Status data communication restored（状态数据通信已还原）	Power supply <number> status information successfully obtained.（已成功获取电源设备 <number> 的状态信息。）
Over/Under-temperature（温度过高/过低）	The temperature for power supply <*number*> is outside of range.（电源设备 <number> 的温度超出允许范围。）
Fan or Airflow error/warning（风扇或气流错误/警告）	Fan failure detected on power supply <*number*>.（在电源设备 <number> 上检测到风扇故障。）
Fan speed overridden（风扇速度超限）	Fan failure detected on power supply <*number*>.（在电源设备 <number> 上检测到风扇故障。）
Manufacturing fault（制造故障）	Power supply <*number*> failed.（电源设备 <number> 故障。）
Microprocessor busy（微处理器正忙）	Power supply <*number*> failed.（电源设备 <number> 故障。）
FRU error（FRU 错误）	Power supply <*number*> failed.（电源设备 <number> 故障。）
Unacknowledged 110V operation detected（检测到未认可的 110V 工作状态）	Power supply low input voltage (110) was asserted.（电源设备输入低压 (110) 已确认。）
110V operation acknowledged（110V 工作状态认可）	Power supply low input voltage (110) was de-asserted.（电源输入低压 (110) 已解除确认。）

与电源冗余状态变化相关并记录在 SEL 中的事件包括：冗余丢失以及冗余重新获得，这适用于配置为**电网冗余**电源策略或**电源设备冗余**电源策略的模块化机柜。下表列出有关电源冗余策略更改的 SEL 条目。

表. 49: 电源冗余策略更改的 SEL 事件

电源策略事件	系统事件日志 (SEL) 条目
冗余丢失	Redundancy lost was asserted（冗余丢失已确认）
冗余恢复	Redundancy lost was de-asserted（冗余丢失已解除确认）

配置电源预算和冗余

您可以配置整个机箱（机箱、服务器、I/O 模块、iKVM、CMC 和电源设备）的电源预算、冗余和动态电源，整个机箱使用六个电源设备 (PSU)。电源管理服务可优化电源，并根据需要为不同模块重新分配电源。

您可以配置以下各项：

- 系统输入功率上限
- 冗余策略
- 扩展电源性能
- 服务器性能优先于电源冗余
- 动态电源设备接入
- 禁用机箱电源按钮
- 允许 110 V 交流操作
- 最大节能模式
- 远程电源日志记录
- 远程电源日志记录间隔
- 基于服务器的电源管理
- 禁用交流电源恢复

相关链接

节能和功率预算
最大节能模式
减少服务器功率以维持功率预算
PSU 在 110V 交流电源下工作
服务器性能优先于电源冗余
远程日志记录
外部电源管理
使用 CMC Web 界面配置电源预算和冗余
使用 RACADM 配置电源预算和冗余

节能和功率预算

当达到用户配置的最大功率限制时，CMC 会节能。当电源需求超出用户配置的“系统输入功率上限”时，CMC 将按照优先级从低到高的顺序减少为服务器供电，以便为机箱中高优先级的服务器和其他模块腾出电源。

如果机箱中所有或多个插槽配置了相同的优先级，CMC 将按照插槽编号递增的顺序减少为服务器提供的功率。例如，如果插槽 1 和 2 中的服务器具有相同的优先级，则插槽 1 中的服务器将先于插槽 2 中的服务器减少供电。

注: 可以通过指定每台服务器从 1 到 9 的编号，为机箱中每台服务器分配一个优先级。所有服务器的默认优先级为 1。数字越低，优先级越高。

电源预算限制为三个 PSU 中最弱的 PSU 设置的最大值。如果尝试设置交流电源预算值超过*系统输入功率上限*值，CMC 会显示故障消息。电源预算限制为 16685 瓦。

最大节能模式

CMC 在以下情况下进入最大节能模式：

- 启用了最大节能模式
- 由 UPS 设备发出的自动命令行脚本启用最大节能模式。

在最大节能模式下，所有服务器都在最低电源水平下工作且所有后续服务器电源分配请求都会被拒绝。在此模式下，已开机服务器的性能可能下降。额外的服务器无论优先级如何都不能开机。

在清除最大节能模式后，系统恢复到最佳性能。

注: 如果机箱启用了最大节能模式 (MPCM)，来自刀片服务器的所有电源请求均将被拒。如果 iDRAC 中在执行任何操作，或者刀片服务器要求主机启动电源循环，则刀片服务器未开启电源。

减少服务器功率以维持功率预算

为了将系统功耗保持在用户配置的*系统输入功率上限*内而需要额外功率时，CMC 将减少分配给较低优先级服务器的功率。例如，当接入新服务器时，CMC 可能会减少低优先级服务器的功率，以便为新服务器提供更多功率。如果减少分配给较低优先级服务器的功率之后，功率量仍然不足，CMC 会降低服务器的性能，直到能够为新服务器供电而释放出足够的功率为止。

CMC 在两种情况下会减少分配给服务器的功率：

- 总体功耗超过可配置的*系统输入功率上限*。
- 在非冗余配置中出现电源故障。

PSU 在 110V 交流电源下工作

部分 PSU 可在 110V 交流输入下工作。此输入可超出分支电路的允许限制。如果任何 PSU 连接到 110V 交流电源，则用户需要设置 CMC 才能让机柜正常工作。如果未设置且检测到 110V 的 PSU，则所有后续服务器电源分配请求都会被拒绝。在此情况下，额外的服务器无论优先级如何都不能开机。您可通过 Web 接口或 RACADM 设置 CMC 使用 110V 的 PSU。

在以下情况下，电源设备条目会记录到 SEL 日志中：

- 检测到或卸下 110V 电源设备时。
- 启用或禁用 110V 交流输入操作时。

当机箱在 110V 模式下工作且用户未启用 110V 时，整体电源运行状况至少为不严重状态。不严重状态下 Web 界面主页上显示“警告”图标。

不支持 110V 和 220V 的混合操作。如果 CMC 检测到使用两种电压，则会选择一个电压，然后关闭连接到另一个电压的电源设备并将其标记为故障。

服务器性能优先于电源冗余

当启用时，此选项倾向于保证服务器性能和服务器开机，而非维持电源冗余。如果禁用此选项，则系统倾向于电源冗余而非服务器性能。禁用此选项时，如果机箱中的电源未提供足够的功率用于冗余以及最大性能，则要保留冗余，某些服务器不能：

- 为最大性能提供足够的功率。
- 开机

远程日志记录

功耗可报告至远程系统日志服务器。可记录一段收集时间内的机箱总功耗、最小值、最大值和平均功耗。有关启用此功能和配置收集/记录间隔的更多信息，请参阅执行电源控制操作部分。

外部电源管理

可选择地由 **Dell OpenManage Power Center** 控制 CMC 电源管理。有关更多信息，请参阅 *Dell OpenManage Power Center User's Guide*（Dell OpenManage Power Center 用户指南）。

如果启用了外部电源管理，则 **Dell OpenManage Power Center** 可管理：

- 支持的 M1000e 服务器的服务器电源
- 支持的 M1000e 服务器的服务器优先级
- 系统输入功率容量
- 最大节能模式

CMC 可继续维护或管理：

- 冗余策略
- 远程电源日志记录
- 服务器性能优先于电源冗余
- 动态电源设备接入
- 第 11 代及更早期服务器的服务器电源

Dell OpenManage Power Center 在为机箱基础结构以及上一代刀片服务器分配电源后，将根据可用的预算为支持的 M1000e 服务器以及机箱中较高版本的刀片服务器管理优先级和电源。远程电源日志记录不受外部电源管理的影响。

启用“基于服务器的电源管理模式”之后，机箱将准备好进行 **Dell OpenManage Power Center** 管理。所有支持的 M1000e 服务器及更高版本的服务器优先级均被设为 1（高）。**Dell OpenManage Power Center** 直接管理服务器电源和优先级。由于 **Dell OpenManage Power Center** 控制兼容的服务器电源分配，所以 CMC 不再控制最大节能模式，因而此选择被禁用。

在启用“最大节能模式”时，CMC 将把“系统输入功率容量”设为机箱可处理的最大值。CMC 不允许功率超出最高容量。但是 **Dell OpenManage Power Center** 可处理所有其他功率容量限制。

在禁用 **Dell OpenManage Power Center** 电源管理时，CMC 会在启用外部管理之前恢复服务器优先级设置。

注: 在禁用 Dell OpenManage Power Center 管理时，CMC 不会恢复最大机箱电源的先前设置。请参阅 CMC 日志了解先前的设置以便手动恢复该值。

使用 CMC Web 界面配置电源预算和冗余

注: 要执行电源管理操作，必须具有机箱配置管理员权限。

要使用 Web 界面配置电源预算，请执行以下操作：

1 在系统树中，转至**服务器概览**，然后单击**电源** > **配置**。

此时将显示**预算/冗余配置**页。

2 根据需要选择以下任一或所有属性。有关每个字段的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

- 启用基于服务器的电源管理
- 系统输入功率上限
- 冗余策略
- 启用扩展电源性能
- 启用“服务器性能优于电源冗余”
- 启用动态电源设备接入
- 禁用机箱电源按钮
- 允许 110 V 交流操作
- 启用最大节电模式
- 启用远程电源日志记录
- 远程电源日志记录间隔

3 单击**应用**保存更改。

使用 RACADM 配置电源预算和冗余

注: 要执行电源管理操作，必须具有机箱配置管理员权限。

要启用和设置冗余策略，请执行以下操作：

1 打开到 CMC 的串行/Telnet/SSH 文本控制台并登录。

2 根据需要设置属性：

- 要选择冗余策略，请键入：

```
racadm config -g cfgChassisPower -o
cfgChassisRedundancyPolicy <value>
```

其中，*<value>* 是 0（无冗余），1（电网冗余），2（电源设备冗余）。默认值为 0。

例如，以下命令将启用“电网冗余”模式：

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

- 要启用或禁用“扩展电源性能”模式，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable <value>
```

其中，<value> 为 0（禁用），1（启用）。对于 3000W PSU，默认值为 1

- 要设置系统输入功率上限值，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
```

其中 *<value>* 是 2715-16685 之间的数字，表示以瓦为单位的最大电源限制。默认值为 16685。
例如，以下命令将系统输入功率上限设置为 5400 瓦：

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

。

- 要启用或禁用动态 PSU 接入，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <value>
```

其中，*<value>* 为 0（禁用），1（启用）。默认值为 0。
例如，以下命令禁用动态 PSU 接入：

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
```

。

- 要启用最大节能模式，请键入：
  ```
  racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
  ```
- 若要恢复正常操作，请键入：
  ```
  racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
  ```
- 启用 110V 交流 PSU：
  ```
  racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
  ```
- 启用“服务器性能优于电源冗余”：
  ```
  racadm config -g cfgChassisPower -o cfgChassisPerformanceOverRedundancy 1
  ```
- 禁用“服务器性能优于电源冗余”：
  ```
  racadm config -g cfgChassisPower -o cfgChassisPerformanceOverRedundancy 0
  ```
- 要启用电源远程日志记录功能，请键入以下命令：
  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
  ```
- 要指定所需的日志记录间隔，请键入以下命令：
  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval n
  ```

  其中 n 为 1 至 1440 分钟。
- 要确定是否已启用电源远程日志记录功能，请键入以下命令：
  ```
  racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
  ```
- 要确定电源远程日志记录间隔，请键入以下命令：
  ```
  racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
  ```

  电源远程日志记录功能取决于先前配置的远程系统日志主机。必须启用记录到一个或多个远程系统日志主机，否则将记录功耗。这可以通过 Web 界面或 RACADM CLI 启用。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的**远程系统日志配置**说明。
- 要使用 **Dell OpenManage Power Center** 启用远程电源管理，请键入：
  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 1
  ```
- 要恢复 CMC 电源管理，请键入：
  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 0
  ```

有关机箱电源的 RACADM 命令的信息，请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 **config**、**getconfig**、**getpbinfo** 和 **cfgChassisPower** 部分。

执行电源控制操作

可以对机箱、服务器和 IOM 执行以下电源控制操作。

注: 电源控制操作将影响整个机箱。

相关链接

对机箱执行电源控制操作
对服务器执行电源控制操作
对 IOM 执行电源控制操作

对机箱执行电源控制操作

CMC 能够对整个机箱（机箱、服务器、IOM、iKVM 和 PSU）远程执行几项电源管理操作（如按顺序关机）。

注: 要执行电源管理操作，必须具有机箱配置管理员权限。

使用 Web 界面对机箱执行电源控制操作

要使用 CMC Web 界面对机箱执行电源控制操作，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**电源** > **控制**。
此时将显示**机箱电源控制**页。
2 选择以下任一电源控制操作：
- 打开系统电源
- 关闭系统电源
- 关闭系统电源后再开启（冷引导）
- 重设 CMC（热引导）
- 非正常关机

有关每个选项的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用**。
此时将显示要求确认的对话框。
4 单击**确定**执行电源管理操作（例如，执行系统重设）。

使用 RACADM 对机箱执行电源控制操作

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm chassisaction -m chassis <action>
```

其中<*action*>为 `powerup`、`powerdown`、`powercycle`、`nongraceshutdown` 或 `reset`。

交流电源恢复

如果系统的交流电源设备中断，交流电源中断之前机箱被还原到先前的电源状态。恢复到先前的电源状态是默认行为。以下因素可能会导致中断：

- 电源中断
- 电源电缆从电源设备 (PSU) 拔出
- 配电装置 (PDU) 停机

如果选择 **Budget/Redundancy Configuration（预算/冗余配置）** > **Disable AC Power Recovery（禁用交流电恢复）**选项，交流电恢复后机箱保持关机状态。

如果刀片服务器没有配置为自动通电，则可能必须手动启动。

对服务器执行电源控制操作

可以一次对机箱中的多个服务器或对机箱中的单个服务器远程执行电源管理操作。

注: 要执行电源管理操作，必须具有机箱配置管理员权限。

使用 CMC Web 界面对多个服务器执行电源控制操作

要使用 CMC Web 界面对多个服务器执行电源控制操作，请执行以下操作：

1 在系统树中，转至**服务器概述**，然后单击**电源** > **控制**。
此时将显示**电源控制**页。
2 在**操作**列中，从下拉菜单中为所需服务器选择以下任一电源控制操作：
- 无操作
- 打开服务器
- 关闭服务器
- 正常关机
- 重设服务器（热引导）
- 关闭服务器电源后再开启（冷引导）

有关各选项的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
3 单击**应用**。
此时将显示要求确认的对话框。
4 单击**确定**执行电源管理操作（例如，执行服务器重设）。

使用 CMC Web 界面对服务器执行电源控制操作

要使用 CMC Web 界面对单个服务器执行电源控制操作，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**服务器概览**。
2 单击要执行电源控制操作的服务器，然后单击**电源**选项卡。
此时将显示**服务器电源管理**页。
3 选择以下任一电源控制操作：
- 打开服务器
- 关闭服务器
- 重设服务器（热引导）
- 关闭服务器电源后再开启（冷引导）

有关各选项的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
4 单击**应用**。
此时将显示要求确认的对话框。
5 单击**确定**执行电源管理操作（例如，使服务器重设）。

使用 RACADM 对服务器执行电源控制操作

要使用 RACADM 对服务器执行电源控制操作，打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm serveraction -m <module> <action>
```

其中 <*module*> 根据机箱中的插槽号（server-1 到 server-16）指定服务器，而 <*action*> 表示想要执行的操作：`powerup`（开机）、`powerdown`（关机）、`powercycle`（关机后再开机）、`graceshutdown`（有序关机）或 `hardreset`（硬重设）。

对 IOM 执行电源控制操作

可以对单个 IOM 远程执行重设或关机后再开机操作。

注: 要执行电源管理操作，必须具有机箱配置管理员权限。

使用 CMC Web 界面对 IOM 执行电源控制操作

要使用 CMC Web 界面对 IOM 执行电源控制操作，请执行以下操作：

1 在系统树中，转至**机箱概述** > **I/O 模块概述**，然后单击**电源**。
此时将显示**电源控制**页。
2 对于列表中的 IOM，请从下拉菜单中选择要执行的操作（重设或打开电源再关闭电源）。
3 单击**应用**。
此时将显示要求确认的对话框。
4 单击**确定**执行电源管理操作（例如，使 IOM 关机后再开机）。

使用 RACADM 对 IOM 执行电源控制操作

要使用 RACADM 对 IOM 执行电源控制操作，请打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm chassisaction -m switch-<n><action>
```

其中 <*n*> 是数字 1-6，并指定 IOM（A1、A2、B1、B2、C1、C2），<action> 表示您要执行的操作：powercycle（关机后再开机）或 reset（重设）。

16

故障排除和恢复

本节介绍如何使用 CMC Web 界面执行与远程系统问题恢复和故障排除有关的任务。

- 查看机箱信息。
- 查看事件日志。
- 收集配置信息、错误状态和错误日志。
- 使用诊断控制台。
- 管理远程系统上的电源。
- 管理远程系统上的 Lifecycle Controller 作业。
- 重设组件。
- 网络时间协议 (NTP) 故障排除。
- 网络故障排除。
- 警报故障排除。
- 重设忘记的管理员密码。
- 保存并还原机箱配置设置和证书。
- 查看错误代码和日志。

主题：

使用 RACDUMP 收集配置信息、机箱状态和日志

`racdump` 子命令是获得全面机箱状态、配置状态信息和历史事件日志的单一命令。

`racdump` 子命令显示以下信息：

- 常规系统/RAC 信息
- CMC 信息
- 机箱信息

- 会话信息
- 传感器信息
- 固件版次信息

支持的接口

- CLI RACADM
- 远程 RACADM
- Telnet RACADM

Racdump 包含以下子系统并聚合以下 RACADM 命令。有关 racdump 的更多信息，请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

表. 50: 子系统的 RACADM 命令

子系统	RACADM 命令
常规系统/RAC 信息	`getsysinfo`
会话信息	`getssinfo`
传感器信息	`getsensorinfo`
交换机信息（IO 模块）	`getioinfo`
夹层卡信息（子卡）	`getdcinfo`
所有模块信息	`getmodinfo`
电源预算信息	`getpbinfo`
KVM 信息	`getkvminfo`
NIC 信息（CMC 模块）	`getniccfg`
冗余信息	`getredundancymode`
跟踪日志信息	`gettracelog`
RAC 事件日志	`gettraclog`
系统事件日志	`getsel`

下载 SNMP 管理信息库文件

CMC SNMP 管理信息库 (MIB) 文件定义机箱类型、事件和指示灯。CMC 使您能够使用 Web 界面下载 MIB 文件。

要使用 CMC Web 界面下载 CMC 的 SNMP 管理信息库 (MIB) 文件，请执行以下操作：

1 在系统树中，转至**机箱概述**，然后单击**网络** > **服务** > **SNMP**。
此时将显示 **SNMP 配置**部分。

2 单击**保存**将 CMC MIB 文件下载至本地系统。
有关 SNMP MIB 文件的更多信息，请参阅 **dell.com/support/manuals** 上的 *Dell OpenManage Server Administrator SNMP Reference Guide*（Dell OpenManage Server Administrator SNMP 参考指南）。

远程系统故障排除首先需要执行的步骤

以下是在管理系统高级别故障排除时常见的一些问题：

- 系统开机还是关机？
- 如果是开机，操作系统是运作正常、崩溃，还是冻结？
- 如果是关机，电源是意外关闭的吗？

电源故障排除

以下信息可帮助您对电源设备和电源相关问题进行故障排除：

- **问题：**将**电源冗余策略**配置成了**电网冗余**，并引发电源设备冗余丢失事件。
  - **解决方案 A：**此配置要求 1 侧（左边 3 个插槽）至少有 1 个电源且 2 侧（右边 3 个插槽）至少有 1 个电源存在于模块化机柜中并可正常运行。另外，每侧的容量必须足以支持机箱的合计功率分配以维持**电网冗余**。（为了获得完整的电网冗余，确保提供由 6 个电源设备组成的完整 PSU 配置。）
  - **解决方案 B：**确保所有电源设备正确连接到两个交流电网；1 侧的电源设备需要连接到一个交流电网；2 侧的电源设备需要连接到另一个交流电网；且两个交流电网都必须能正常运行。在交流电网之一无法正常工作时，**电网冗余**会丢失。
- **问题：**PSU 状态显示为**失败（无交流）**，即使已连接交流电缆并且配电装置的交流输出良好。
  - **解决方案 A：**检查并更换交流电缆。检查并确认为电源设备供电的配电装置是否按预期方式工作。如果故障依然存在，请致电 Dell 客户服务更换电源设备。
  - **解决方案 B：**确认 PSU 连接的电压是否与其他 PSU 相同。如果 CMC 检测到在不同电压下工作的 PSU，则此 PSU 会被关闭并标记为“故障”。
- **问题：**动态电源设备接入已启用，但**待机**状态中没有显示任何电源。
  - **解决方案 A：**剩余功率不足。一个或多个电源设备仅会在机柜内的剩余功率超过至少一个电源设备的容量时进入待机状态。
  - **解决方案 B：**机柜内的电源设备装置不完全支持动态电源设备接入。要确认是否属于此情况，请用 Web 界面关闭**动态电源设备接入**，然后再次打开。如果不能完全支持动态电源设备接入，则会显示一条消息。
- **问题：**将新服务器插入供电充足的机柜，但服务器无法开机。
  - **解决方案 A：**确保系统输入功率上限设置的配置不是过低，允许其他额外服务器开机。
  - **解决方案 B：**检查是否在 110V 下工作。如果任何电源设备连接到 110V 分支电路，则在允许服务器开机前必须认可这是有效的配置。有关详情，请参阅电源配置设置。
  - **解决方案 C：**检查最大节能设置。如果设置了此项，则允许服务器开机。有关详情，请参阅电源配置设置。
  - **解决方案 D：**确保与新插入服务器相关的插槽的服务器插槽电源优先级不低于任何其他服务器插槽电源优先级。
- **问题：**可用电源不断变化，即便没有更改模块化机柜配置也是如此。
  - **解决方案：**CMC 1.2 和更高版本拥有动态风扇电源管理功能，如果机柜在接近峰值用户配置的功率上限操作，则会暂时减少服务器的分配；这将导致通过降低服务器性能为风扇分配电源，以保证输入电源消耗低于 **系统输入功率上限**。这是一种正常行为。
- **问题：**报告 2000 W 作为 **峰值性能盈余**。
  - **解决方案：**机柜在当前配置中提供 2000 W 剩余电源，并且**系统输入功率上限**可安全地降低报告的此数值，而不会影响服务器性能。
- **问题：**服务器的子集在交流电网故障后损失电源，甚至当机箱在带有六个电源的**电网冗余**配置中运行时也是如此。
  - **解决方案：**发生交流电网故障时，如果电源设备未正确连接到冗余交流电网，则会发生这种问题。**电网冗余**策略需要左侧的三个电源设备连接到一个交流电网，右侧的三个电源设备连接到另一个交流电网。如果未正确连接两个 PSU，例如将 PSU3 和 PSU4 连接到错误的交流电网，交流电网故障会造成最低优先级服务器断电。
- **问题：**最低优先权服务器在 PSU 故障后损失电源。
  - **解决方案：**如果机柜电源策略配置为**无冗余**，则这是预期行为。为了防止未来的电源设备故障导致服务器断电，请确保机箱至少有四个电源设备且配置为**电源设备冗余**策略，以防止产生影响服务器操作的 PSU 故障。
- **问题：**数据中心的室温提高时，总体服务器性能下降。

- **解决方案：**如果**系统输入功率上限**配置的值导致风扇的电源需求增加而将服务器的电源分配降低，则会发生这种问题。用户可将**系统输入功率上限**增加到更高的值，允许为风扇分配额外电源而不会影响服务器性能。

警报故障排除

使用 CMC 日志和跟踪日志排除 CMC 警报故障。每次成功或失败的电子邮件和/或 SNMP 陷阱传输尝试都将记录到 CMC 日志中。描述特定错误的附加信息将记录到跟踪日志中。但是，由于 SNMP 并不确认陷阱的传输，因此请使用网络分析器或 Microsoft 的 snmputil 等工具跟踪管理系统中的信息包。

相关链接

配置 CMC 以发送警报

查看事件日志

可以查看硬件和 CMC 日志，了解受管系统出现的系统级严重事件的信息。

相关链接

查看硬件日志
查看 CMC 日志和增强的机箱日志

查看硬件日志

CMC 生成发生在机箱上的事件的硬件日志。可以使用 Web 界面和远程 RACADM 查看硬件日志。

注: 要清除硬件日志，必须具备清除日志管理员权限。

注: 可以配置 CMC 在发生特定事件时发送电子邮件或 SNMP 陷阱。有关配置 CMC 以发送警报的信息，请参阅配置 CMC 以发送警报。

硬件日志条目示例

```
critical System Software event: redundancy lost
Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted
Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted
Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted
Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

相关链接

查看事件日志

使用 CMC Web 界面查看硬件日志

您可以查看、保存和清除硬件日志。可以单击列标题基于“严重性”、“日期/时间”或“说明”对日志条目排序。

要使用 CMC Web 界面查看硬件日志，请在系统树中，转至**机箱概述**并单击**日志** > **硬件日志**。此时将显示**硬件日志**页。要将硬件日志的副本保存到管理站或网络，请单击**保存日志**，然后指定日志文本文件的位置。

注: 因为日志保存为文本文件，所以不会在用户接口中出现图形来指示严重性。在文本文件中，严重性以“正常”、“通知”、“未知”、“警告”和“严重”等词语表示。日期和时间条目以升序显示。如果在日期/时间列中出现 <SYSTEM BOOT>，这表示在任何模块关闭或启动时发生事件，此时时间或日期不可用。

若要清除硬件日志，请单击**清除日志**。

注: CMC 会创建一个新的日志条目表示日志已清除。

使用 RACADM 查看硬件日志

要使用 RACADM 查看硬件日志，请打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm getsel
```

要清除硬件日志，请键入：

```
racadm clrsel
```

查看 CMC 日志和增强的机箱日志

在启用**启用增强的日志记录和事件**选项时，CMC 会生成机箱相关的事件日志和增强的机箱日志记录。要在**机箱日志**页面中查看增强的机箱日志记录，请在**常规设置**页面中选择**启用增强的日志记录和事件**选项。要使用 RACADM 启用或禁用该功能，请使用 cfgRacTuneEnhancedLog 对象。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

注: 要清除 CMC 日志，您必须具有清除日志管理员权限。

相关链接

查看事件日志

使用 Web 界面查看 CMC 日志

您可以查看、保存和清除 CMC 日志。可以单击列标题基于“来源”、“日期/时间”或“说明”对日志条目排序。

要使用 CMC Web 界面查看 CMC 日志，请在系统树中，转至**机箱概览**并单击**日志** > **CMC 日志**。此时将显示 **CMC 日志**页。

要将 CMC 日志的副本保存到管理站或网络，请单击**保存日志**，然后指定保存日志文件的位置。

使用 RACADM 查看 CMC 日志

要使用 RACADM 查看 CMC 日志信息，请打开一个至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm getraclog
```

可以使用 `racadm chassislog view` 命令查看增强的机箱日志

要清除 CMC 日志，请键入：

```
racadm clrraclog
```

使用 Web 界面查看增强的机箱日志

要查看增强的机箱日志记录，必须启用**常规设置**页面中的**启用增强的日志记录和事件**选项。

您可以使用**机箱日志**页面查看所有机箱活动、筛选日志、清除日志或保存日志。

要将 CMC 日志的副本保存到管理工作站或网络上，请单击**保存日志**，然后指定保存日志文件的位置。

1. 要使用 CMC Web 界面查看增强的机箱日志，请在系统树中转至**机箱概述**，然后单击**日志** > **CMC 日志**。随即将显示**机箱日志**页面。
2. 在“日志筛选”部分，从各自的下拉菜单中选择**日志类型**或**状态级别**，或在**关键字搜索**和**日期范围**字段中输入关键字或日期，然后单击**应用**。

机箱日志表显示根据选定的筛选器排序的日志。

3 要将机箱日志的副本保存到管理站或网络上，请单击**保存日志**，然后指定保存日志文件的位置。
如要清除硬件日志中的当前条目，请单击**清除日志**。

有关其他字段和使用 Web 界面的更多信息，请参阅 CMC Online Help（CMC 联机帮助）。

使用诊断控制台

如果您是一位高级 CMC 用户或技术支持提供指导的用户，可以使用 CLI 命令诊断与机箱硬件相关的问题。

注: 要修改这些设置，必须具备调试命令管理员权限。

要使用 CMC Web 界面访问诊断控制台，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**故障排除** > **诊断**。
随即会显示**诊断控制台**页面。

2 在**命令**文本框中，输入命令并单击**提交**。
有关命令的信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

系统会显示诊断结果页。

重设组件

您可以重设活动 CMC，在不重新引导操作系统的情况下重设 iDRAC，或者虚拟重置服务器，使其产生如同被卸下并重新插入的效果。如果机箱有一个待机 CMC，重设活动 CMC 会造成故障转移并且待机 CMC 变为活动状态。

注: 要重设组件，必须具备调试命令管理员权限。

要使用 CMC Web 界面重设组件，请执行以下操作：

1 在系统树中，转至**机箱概览**，然后单击**故障排除** > **重设组件**。
此时将显示**重设组件**页。

2 要重设活动的 CMC，请在 **CMC 状态**部分单击**重设/故障转移 CMC**。如果待机 CMC 存在并且机箱完全冗余，则故障转移出现会使待机 CMC 变为活动的 CMC。

3 要在不重新引导操作系统的情况下只重设 iDRAC，在**重设服务器**部分，对于那些需要重设 iDRAC 的服务器，单击**重设**下拉菜单中的 **iDRAC 重设**，然后单击**应用选择**。该操作在不重新引导操作系统的情况下为服务器重设 iDRAC。
有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

要使用 RACADM 只重设 iDRAC 而不重新引导操作系统，请参阅 *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

注: 当 iDRAC 重设后，服务器风扇被设定为 100%。

注: 建议在尝试虚拟重置服务器前，先尝试重设 iDRAC。

4 要虚拟重置服务器，在**重设服务器**部分，针对需要重置的服务器在**重设**下拉框中单击**虚拟重置**，然后单击**应用选择**。
有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

此操作使服务器产生如同卸下并重新插入的效果。

保存或还原机箱配置

要使用 CMC Web 界面保存或还原机箱配置的备份，请在系统树中，转至**机箱概览**，然后单击**设置** > **机箱备份**。

将显示**机箱备份**页面。

要保存机箱配置，请单击 **Save（保存）**。覆盖默认文件路径（可选）并单击 **OK（确定）**以保存文件。

注: 默认备份文件名包含机箱的服务标签。此备份文件可在稍后使用，仅用于还原此机箱的设置和证书。

要恢复机箱配置，请单击**选择文件**，指定备份文件，然后单击**恢复**。

注:

- CMC 不会在还原配置时重设，不过，CMC 服务可能需要一些时间才能有效实施任何更改或新增的配置。成功完成后，所有当前会话都会关闭。
- FlexAddress 信息、服务器配置文件和扩展存储不使用机箱配置保存或还原。

网络时间协议错误故障排除

配置 CMC 已将时钟与网络上的远程时间服务器同步后，可能需要 2-3 分钟才会显示日期和时间。如果这段时间后仍没改变，可能需要进行排除故障。出于以下原因，CMC 可能无法同步其时钟：

- NTP 服务器 1、NTP 服务器 2 和 NTP 服务器 3 设置有问题。
- 可能不小心输入了无效的主机名或 IP 地址。
- 网络连接问题，妨碍 CMC 与任一配置的 NTP 服务器进行通信。
- DNS 问题，妨碍解析任意 NTP 服务器主机名。

要对 NTP 相关的问题进行故障排除，请检查 CMC 跟踪日志。此日志包含有关 NTP 故障的错误消息。如果 CMC 无法与任何配置的远程 NTP 服务器同步，则 CMC 时间与本地系统时钟同步并且跟踪日志包含类似如下的条目：

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

您还可以键入以下 racadm 命令检查 ntpd 状态：

```
racadm getractime –n
```

如果配置的服务器之一没有显示“*”，设置可能未正确配置。此命令的输出包含详细的 NTP 统计信息，它可能对于调试问题很有用。

如果您尝试配置基于 Windows 的 NTP 服务器，则它有助于增加 `MaxDist` 参数（为 `ntpd`）。更改此参数之前，请了解所有含义，因为默认设置必须足够大才可配合多数 NTP 服务器。

要修改参数，请键入以下命令：

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

在进行更改后，禁用 NTP，等待 5-10 秒，然后再次启用 NTP：

注: NTP 可能还要再等待 3 分钟才能再次同步。

要禁用 NTP，请键入：

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

要启用 NTP，请键入：

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

如果 NTP 服务器正确配置且此条目存在于追踪日志中，则此项确认 CMC 不能与任何已配置的 NTP 服务器同步。

如果未配置 NTP 服务器 IP 地址，可能会看到与以下内容类似的跟踪日志条目：

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8
19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

如果 NTP 服务器设置配置了一个无效的主机名，可能看到如下所示的跟踪日志条目：

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21 14:34:27 cmc
ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

有关如何使用 CMC Web 界面输入 `gettracelog` 命令查看跟踪日志的信息，请参阅使用诊断控制台。

LED 颜色和闪烁样式说明

机箱上的 LED 提供以下组件状态：

- LED 呈绿色稳定亮起表示组件已打开电源。如果 LED 呈绿色闪烁，则表示属于严重的例行程序的事件（如固件上传），在此期间该装置无法工作。它不表示故障。
- 组件上闪烁的琥珀色 LED 表示该模块发生故障。
- 呈蓝色闪烁的 LED 可由用户配置并可用于标识。有关配置的更多信息，请参阅下载 SNMP 管理信息库 (MIB) 文件。

表. 51: LED 颜色和闪烁样式

组件	LED 颜色，闪烁样式	状态
CMC	绿色，稳定发光	开机
	绿色，闪烁	正在上载固件
	绿色，暗色	关机
	蓝色，稳定发光	活动的
	蓝色，闪烁	用户启用的模块标识符
	琥珀色，稳定发光	未使用
	琥珀色，闪烁	故障
	蓝色，暗色	待机
iKVM	绿色，稳定发光	开机
	绿色，闪烁	正在上载固件
	绿色，暗色	关机
	琥珀色，稳定发光	未使用
	琥珀色，闪烁	故障
	琥珀色，暗色	无故障
服务器	绿色，稳定发光	开机
	绿色，闪烁	正在上载固件
	绿色，暗色	关机
	蓝色，稳定发光	正常
	蓝色，闪烁	用户启用的模块标识符
	琥珀色，稳定发光	未使用
	琥珀色，闪烁	故障
	蓝色，暗色	无故障
IOM（常规）	绿色，稳定发光	开机
	绿色，闪烁	正在上载固件

组件	LED 颜色，闪烁样式	状态
	绿色，暗色	关机
	蓝色，稳定发光	正常/堆栈主装置
	蓝色，闪烁	用户启用的模块标识符
	琥珀色，稳定发光	未使用
	琥珀色，闪烁	故障
	蓝色，暗色	无故障/堆栈从属装置
IOM（直通）	绿色，稳定发光	开机
	绿色，闪烁	未使用
	绿色，暗色	关机
	蓝色，稳定发光	正常
	蓝色，闪烁	用户启用的模块标识符
	琥珀色，稳定发光	未使用
	琥珀色，闪烁	故障
	蓝色，暗色	无故障
风扇	绿色，稳定发光	风扇正在运行
	绿色，闪烁	未使用
	绿色，暗色	关机
	琥珀色，稳定发光	无法识别风扇类型、更新 CMC 固件
	琥珀色，闪烁	风扇出现故障；转速计超出范围
	琥珀色，暗色	未使用
PSU	（椭圆）绿色，稳定发光	交流正常
	（椭圆）绿色，闪烁	未使用
	（椭圆）绿色，暗色	交流不正常
	琥珀色，稳定发光	未使用
	琥珀色，闪烁	故障
	琥珀色，暗色	无故障
	（圆形）绿色，稳定发光	直流正常
	（圆形）绿色，暗色	直流不正常

无响应 CMC 的故障排除

如果使用任意界面（Web 界面、Telnet、SSH、远程 RACADM 或串行）都无法登录到 CMC，则可以通过观察 CMC 上的 LED、使用 DB-9 串行端口获取恢复信息或恢复 CMC 固件映像来验证 CMC 功能。

注: 无法使用串行控制台登录待机 CMC。

观察 LED 隔离问题

正对安装在机箱中的 CMC 前方，可以看到插卡的左侧有两个 LED：

- 顶部 LED - 顶部的绿色 LED 指示电源。如果该 LED 未发光：
  - 验证至少有一个交流电源设备。
  - 验证 CMC 卡是否正确就位。可以释放或拉动排出器手柄，卸下 CMC，重新安装 CMC 以确保插板已插入到位且闩锁正确关闭。
- 底部 LED - 底部 LED 有多种颜色。当 CMC 活动且正在运行时，如果没有问题，则底部 LED 是蓝色。如果是琥珀色，则表示检测到故障。故障可能由以下三种事件中的任意一种引发：
  - 核心故障。这种情况下，必须更换 CMC 板。
  - 自检故障。这种情况下，必须更换 CMC 板。
  - 映像损坏。这种情况下，可以通过上载 CMC 固件映像恢复 CMC。

注: 正常进行 CMC 引导或重设时，需要花费一分钟时间才能完全引导操作系统并进入允许登录状态。蓝色 LED 在活动 CMC 上启用。在冗余、两个 CMC 配置中，待机 CMC 仅启用顶部绿色的 LED。

从 DB-9 串行端口获取恢复信息

如果底部 LED 是琥珀色，则可以从位于 CMC 前方的 DB-9 串行端口获取恢复信息。

要获取恢复信息，请执行以下操作：

1 在 CMC 和客户端计算机之间安装 NULL 调制解调器电缆。

2 打开选择的终端仿真器（如 HyperTerminal 或 Minicom）。设置：8 位、无奇偶校验、无流控制和波特率 115200。

核心内存故障每隔 5 秒钟显示一次错误消息。

3 按 <Enter>。

如果出现恢复提示，则可以获得附加信息。该提示指示 CMC 插槽编号和故障类型。

要显示一些命令的故障原因和语法，请键入 `recover`，然后按 <Enter>。

示例提示：

```
recover1[self test] CMC 1 self test failure
```

```
recover2[Bad FW images] CMC2 has corrupted images
```

- 如果提示出现自检故障，CMC 中没有可维修的组件。CMC 损坏且必须退回 Dell。
- 如果提示指示**固件映像损坏**，请按照恢复固件映像中的步骤解决此问题。

恢复固件映像

当 CMC 无法正常引导至操作时，它将进入恢复模式。在恢复模式下，提供少量命令子集以便通过上载固件更新文件 firmimg.cmc 对 Flash 设备重新编程。该文件与正常固件更新所使用的固件映像文件相同。恢复进程将显示其当前活动并在完成后引导至 CMC 操作系统。

当在 recovery 提示符下键入 recover 然后按下 <Enter> 时，将显示恢复原因和可用子命令。下面是一个恢复序列示例：

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1 recover ping
192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

注: 将网络电缆连接到最左侧的 RJ45。

注: 在恢复模式下，因为没有活动网络堆栈，所以无法正常 ping CMC。`recover ping <TFTP server IP>` 命令可以对 TFTP 服务器执行 ping 命令以检验 LAN 连接。在一些系统上可能需要使用 `recover reset` 命令（在 `setniccfg` 命令后）。

排除网络故障

内部 CMC 跟踪日志可用于调试 CMC 警报和网络。您可以使用 CMC Web 界面或 RACADM 访问跟踪日志。请参阅 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）中的 `gettracelog` 命令部分。

跟踪日志跟踪以下信息：

- DHCP - 跟踪发送到 DHCP 服务器和从 DHCP 服务器接收的数据包。
- DDNS - 跟踪动态 DNS 更新请求和响应。
- 对网络接口所做的配置更改。

跟踪日志还可能包含 CMC 固件特定的错误代码，与内部 CMC 固件有关，而不是管理系统的操作系统。

重设管理员密码

小心: 多数维修只能由经认证的维修技术人员进行。您只能根据产品说明文件中的授权，或者在联机或电话服务和支持团队的指导下进行故障排除和简单维修。任何未经 Dell 授权的服务所导致的损坏均不在保修范围之列。请阅读并遵循产品附带的安全说明。

要执行管理操作，用户必须具有**管理员**权限。CMC 软件具有用户帐户密码保护安全功能，如果忘记了管理员帐户密码，该帐户会被禁用。如果忘记了管理员帐户密码，可以使用 CMC 板上的 PASSWORD_RSET 跳线进行恢复。

CMC 板使用两针密码重设连接器，如下图所示。如果跳线安装在重设连接器中，默认的管理员帐户和密码已启用并设置为默认值 `username: root` 和 `password: calvin`。如果删除帐户或改变密码，管理员帐户也会重设。

注: 开始之前，请确保 CMC 模块处于被动状态。

要执行管理操作，用户必须具有**管理员**权限。如果忘记了管理员帐户密码，可以使用 CMC 板上的 PASSWORD_RST 跳线重设。

PASSWORD_RST 跳线使用两针接头，如下图所示。

安装 PASSWORD_RST 跳线时，启用默认管理员帐户和密码且设置为以下默认值：

```
username: root

password: calvin
```

如果删除管理员帐户或改变密码，管理员帐户也会临时重设。

注: 在安装 PASSWORD_RST 跳线后，则采用默认串行控制台配置（而不是配置属性值），具体如下：

```
cfgSerialBaudRate=115200

cfgSerialConsoleEnable=1

cfgSerialConsoleQuitKey=^\

cfgSerialConsoleIdleTimeout=0

cfgSerialConsoleNoAuth=0

cfgSerialConsoleCommand=""
```

```
cfgSerialConsoleColumns=0
```

1 按下手柄上的 CMC 释放闩锁，然后将手柄从模块前面板移走。将 CMC 模块滑出机柜。

注: 静电放电 (ESD) 事件可损坏 CMC。在某些情况下，ESD 会在您身体上或在物体上积累，然后释放到 CMC 中。为防止静电释放造成损坏，您必须采取预防措施以便在使用和接触机箱外部 CMC 时先释放身上的静电。

2 从密码重设连接器中取出跳线插头，并插入两针跳线以启用默认管理员帐户。要找到 CMC 板上的密码跳线，请参阅下图。

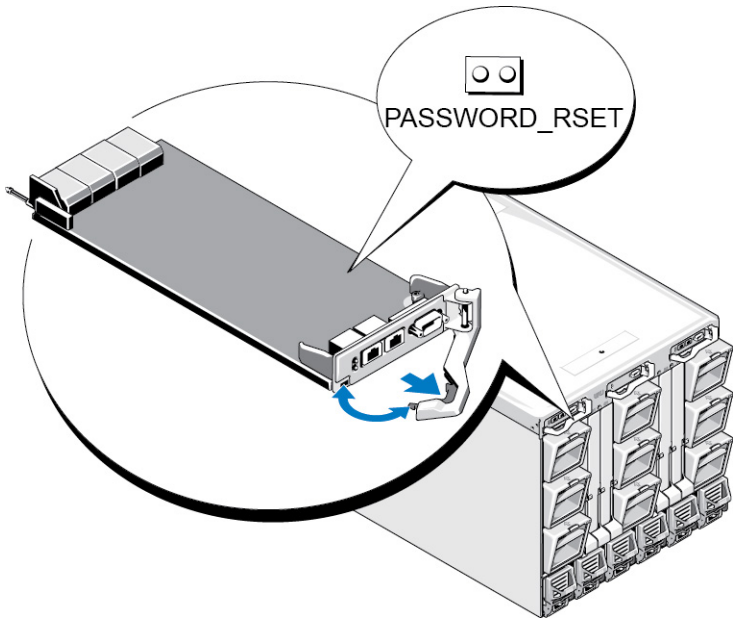


图 18: 密码重设跳线位置

表. 52: CMC 密码跳线设置

PASSWORD_RSET	（默认设置）	已禁用密码重设功能。
		已启用密码重设功能。

3 将 CMC 模块滑入机柜。将任何断开的电缆重新连接起来。

注: 确保 CMC 模块成为活动 CMC，并在剩余步骤完成前保持为活动的 CMC。

4 如果跳线的 CMC 模块是唯一的 CMC，则等待其完成重启。如果机箱中有一个冗余 CMC，则启动切换以使跳线的 CMC 处于活动状态。在 Web 界面的系统树中，转至 **Chassis Overview（机箱概览）**并单击 **Power （电源）** > **Control（控制）**，然后选择 **Reset CMC (warm boot)（重设 CMC（热引导））**并单击 **Apply（应用）**。

CMC 自动故障转移到冗余模块，该模块现在就变为活动模块。

5 使用默认管理员用户名 (root) 和密码 (calvin) 登录到活动 CMC，并恢复任何所需的用户帐户设置。现有帐户和密码未禁用，仍处于活动状态。

6 执行所需的管理操作，包括创建新管理员密码。

7 取出 2 针 PASSWORD_RST 跳线并重新插上跳线插头。

a 按下手柄上的 CMC 释放闩锁，然后将手柄从模块前面板移走。将 CMC 模块滑出机柜。

b 取出 2 针跳线并重新插上跳线插头。

c 将 CMC 模块滑入机柜。将任何断开的电缆重新连接起来。重复步骤 4 以确保未跳线的 CMC 模块成为活动 CMC。

17

使用 LCD 面板界面

可以使用机箱中的 LCD 面板执行配置和诊断，并获取关于机箱及其组件的状态信息。

下图说明了 LCD 面板。LCD 屏幕显示菜单、图标、图片和消息。

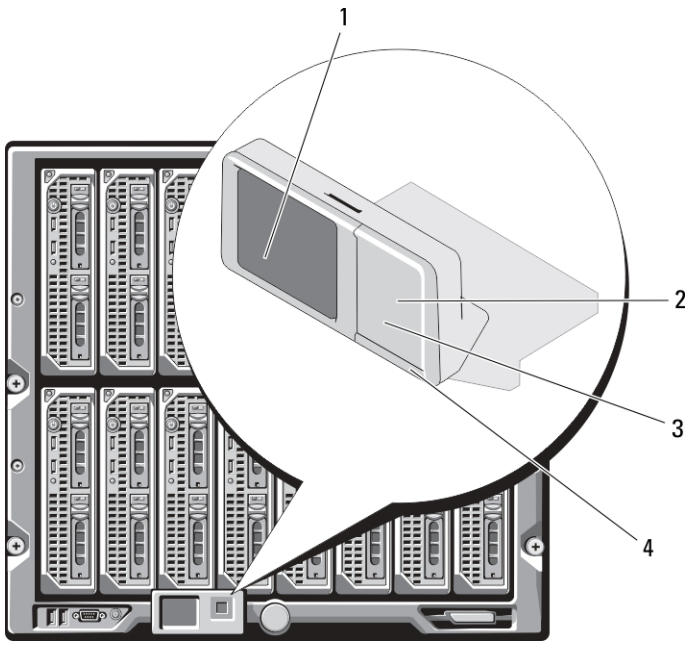


图 19: LCD 显示屏

表. 53: LCD 显示屏 — 组件

1	LCD 屏幕	2	选择（“选中”）按钮
3	滚动按钮（4 个）	4	状态标志 LED

主题：

相关链接

LCD 导航
诊断程序
LCD 硬件故障排除
前面板 LCD 消息
LCD 错误消息
LCD 模块与服务器状态信息

LCD 导航

LCD 面板的右侧包含五个按钮：四个箭头按钮（向上、向下、向左和向右）以及一个中央按钮。

- *要在屏幕之间移动，请使用向右（下一屏）和向左（上一屏）箭头按钮。使用面板过程中的任意时刻，都可以返回到上一屏。*
- *要在屏幕上的选项间滚动，请使用向下和向上箭头按钮。*
- *要选择并保存屏幕上的某个项目并移动到下一屏，请使用中央按钮。*

可以使用上、下、左和右箭头按钮更改屏幕上所选的菜单项或图标。所选项目以浅蓝色背景或边框显示。

当 LCD 屏幕上显示的消息长度超过屏幕长度，使用左和右箭头按钮向左右滚动文本。

下表说明的图标用于在 LCD 屏幕之间导航。

表. 54: LCD 面板导航图标

普通图标	高亮显示图标	图标名称和说明
		**后退** - 高亮显示并按下中央按钮可返回至上一个屏幕。
		**接受/是** - 高亮显示并按下中央按钮可接受更改并返回至上一个屏幕。
		**跳过/下一步** - 高亮显示并按下中央按钮可跳过任何更改并转到下一个屏幕。
		**否** - 高亮显示并按下中央按钮表示对问题回答“否”，并转到下一屏幕。
		**旋转** - 高亮显示并按下中央按钮可在机箱的前后图形视图之间切换。 **注: 琥珀色背景表示相对视图包含错误。**
		**组件标识** - 组件上闪烁的蓝色 LED。 **注: 当启用“组件标识”时，此图标四周将出现不断闪烁的蓝色矩形框。**

LCD 面板上的状态指示 LED 提供机箱及其组件的整体运行状况提示。

- 稳定蓝色表示运行状况良好。
- 不停闪烁的琥珀色表示至少一个组件处于故障状态。
- 不停闪烁的蓝色为 ID 信号，用于识别一组机箱中的某个机箱。

相关链接

主菜单
LCD 设置菜单
语言设置屏幕
默认屏幕
服务器状态图形显示屏幕
模块状态图形显示屏幕
机柜菜单屏幕
模块状态屏幕
机柜状态屏幕
IP 摘要屏幕

主菜单

从**主菜单**中，可导航至以下屏幕：

- **LCD 设置菜单** - 选择要使用的语言和没人使用 LCD 时显示的 LCD 屏幕。
- **服务器** - 显示服务器的状态信息。
- **机柜** - 显示机箱的状态信息。

使用上箭头和下箭头按钮高亮度显示一个项目。

按下中央按钮激活所做的选择。

LCD 设置菜单

LCD 设置菜单显示可配置项目的菜单：

- **语言设置** - 选择要用于 LCD 屏幕文字和消息的语言。
- **默认屏幕** - 选择 LCD 面板上没有任何活动时显示的屏幕。

使用上下箭头按钮高亮度显示菜单中的某个项目，或者如果想返回**主菜单**可高亮度显示**后退**图标。

按下中央按钮激活所做的选择。

语言设置屏幕

语言设置屏幕可用于选择 LCD 面板消息的语言。当前活动语言以浅蓝色背景高亮显示。

1 使用上、下、左和右箭头按钮高亮显示所需语言。
2 按中央按钮。
接受图标出现并被高亮度显示。
3 按中央按钮确认更改。
会显示 **LCD 设置**菜单。

默认屏幕

默认屏幕可用于更改面板上无任何活动时 LCD 面板显示的屏幕。出厂默认屏幕为**主菜单**。可选择显示以下屏幕：

- **主菜单**
- **服务器状态**（机箱的前视图）
- **模块状态**（机箱的后视图）
- **自定义**（带机箱名称的 Dell 徽标）

当前活动默认屏幕以浅蓝色高亮显示。

1 使用上和下箭头按钮高亮显示要设置为默认状况的屏幕。
2 按中央按钮。
将高亮显示**接受**图标。
3 再次按中央按钮确认更改。
将显示**默认屏幕**。

服务器状态图形显示屏幕

服务器状态图形显示屏幕显示机箱中安装的每个服务器的图标并表示每个服务器的常规运行状况。服务器运行状况由服务器图标的颜色表示：

- 灰色 - 服务器关闭，无错误
- 绿色 - 服务器开启，无错误
- 黄色 - 服务器有一个或多个非严重错误
- 红色 - 服务器有一个或多个严重错误
- 黑色 - 服务器不存在

服务器图标四周闪烁的浅蓝色矩形表示该服务器被高亮度显示。

要查看**模块状态图形显示**屏幕，请高亮显示旋转图标，然后按中央按钮。

要查看服务器的状态屏幕，请使用箭头按钮高亮显示所需的服务器，然后按中央按钮。此时将显示**服务器状态**屏幕。

要返回主菜单，请使用箭头按钮高亮显示**后退**图标，然后按中央按钮。

模块状态图形显示屏幕

模块状态图形显示屏幕显示机箱后部安装的所有模块并提供每个模块的摘要运行状况信息。模块运行状况由每个模块图标的颜色按如下表示：

- 灰色 - 模块关闭或待机，无错误
- 绿色 - 模块开启，无错误
- 黄色 - 模块有一个或多个非严重错误
- 红色 - 服务器有一个或多个严重错误
- 黑色 - 模块不存在

模块图标四周闪烁的浅蓝色矩形表示该模块被高亮显示。

要查看**服务器状态图形**屏幕，请高亮显示旋转图标，然后按下中央按钮。

要查看模块的状态屏幕，请使用上、下、左、右箭头按钮高亮显示所需的模块，并按下中央按钮。此时将显示**模块状态**屏幕。

要返回**主菜单**，请使用箭头按钮高亮显示“后退”图标，然后按下中央按钮。此时将显示**主菜单**。

机柜菜单屏幕

从此屏幕可导航至以下屏幕：

- **“模块状态”屏幕**
- **“机柜状态”屏幕**
- **“IP 摘要”屏幕**
- **主菜单**

使用导航按钮高亮显示所需的项目（高亮显示**后退**图标返回**主菜单**），然后按下中央按钮。此时将显示所选的屏幕。

模块状态屏幕

模块状态屏幕显示有关模块的信息和错误消息。有关出现在该屏幕上的消息，请参阅 LCD 模块和服务器状态信息和 LCD 错误消息。

使用上下箭头键滚动消息。使用左右箭头键滚动在屏幕之外的消息。

高亮度显示**后退**图标并按下中央按钮返回**模块状态图形显示**屏幕。

机柜状态屏幕

机柜状态屏幕显示有关机柜的信息和错误消息。有关出现在该屏幕上的消息，请参阅 LCD 错误消息。请使用上下箭头键滚动消息。

使用左右箭头键滚动在屏幕之外的消息。

高亮度显示**后退**图标并按下中央按钮返回**机柜状态**屏幕。

IP 摘要屏幕

IP 摘要屏幕显示每个已安装服务器的 CMC 和 iDRAC 的 IP 信息。

使用上下箭头按钮在列表中滚动。使用左右箭头按钮滚动超过屏幕长度的所选消息。

使用上下箭头按钮选择**后退**图标并按下中央按钮返回**机柜**菜单。

诊断程序

LCD 面板有助于诊断机箱中任何服务器或模块的问题。如果机箱或机箱中任何服务器或其他模块发生问题或故障，则 LCD 面板状态指示灯以琥珀色闪烁。在“主菜单”上，琥珀色图标会显示在导致服务器或模块发生故障的菜单项目（服务器或机柜）旁边。

通过跟踪 LCD 菜单系统中的琥珀色图标，可以显示状态屏幕和发生问题项目的错误消息。

通过卸下导致问题的模块或服务器或通过清除该模块或服务器的硬件日志，可以删除 LCD 面板上的错误消息。对于服务器错误，使用 iDRAC Web 界面或命令行界面清除服务器的系统事件日志 (SEL)。对于机箱错误，使用 CMC Web 界面或命令行界面清除硬件日志。

LCD 硬件故障排除

如果使用 CMC 时遇到与 LCD 相关的问题，可以使用下列硬件故障排除项确定是否是 LCD 硬件或连接出现问题。

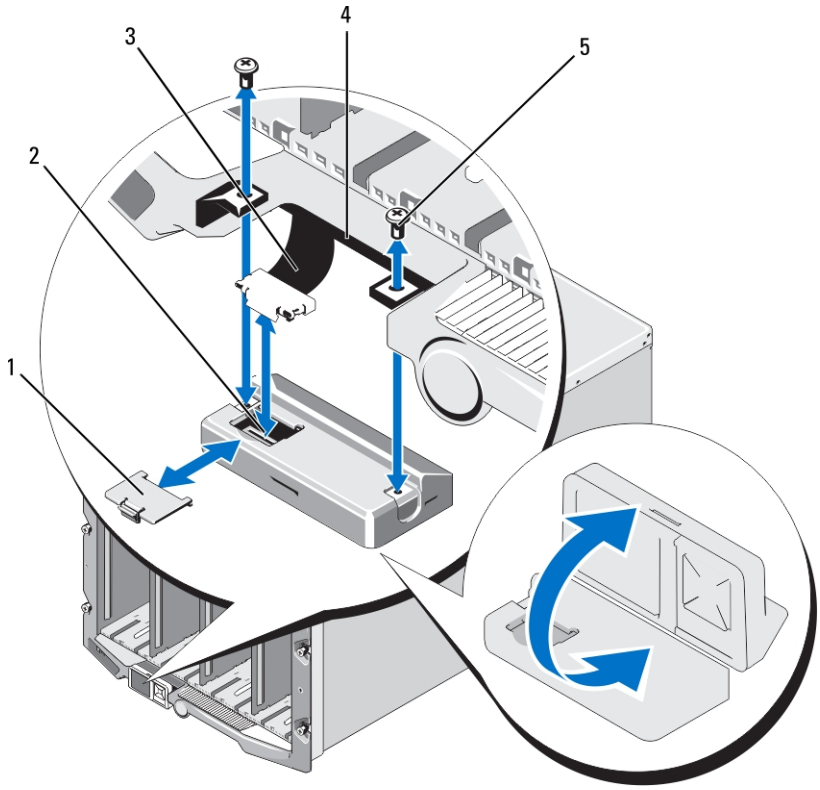


图 20: 卸下和安装 LCD 模块

表. 55: LCD 模块 — 组件

1	电缆护盖	2	LCD 模块
3	带状电缆	4	铰接部件（2 个）
5	螺钉（2 个）		

表. 56: LCD 硬件故障排除项

症状	问题	恢复操作
屏幕显示 `CMC Not Responding` 警报消息且 LED 指示灯呈琥珀色闪烁。	丢失从 CMC 到 LCD 前面板的通信。	检查 CMC 是否正在引导；然后使用 GUI 或 RACADM 命令重设 CMC。
屏幕显示 `CMC Not Responding` 警报消息且 LED 指示灯呈琥珀色常亮或熄灭。	在 CMC 故障转移或重新引导期间 LCD 模块通信阻塞。	使用 GUI 或 RACADM 命令查看硬件日志。查找一条含有如下内容的消息：`Can not communicate with LCD controller.`

		重新布置 LCD 模块排线。
屏幕文本混乱。	有缺陷的 LCD 屏幕。	更换 LCD 模块。
LED 指示灯和 LCD 关闭。	LCD 电缆连接不正确或发生故障；或者 LCD 模块发生故障。	使用 GUI 或 RACADM 命令查看硬件日志。查找具有以下内容的消息： • `The LCD module cable is not connected, or is improperly connected.` • `The control panel cable is not connected, or is improperly connected.` 重装设电缆。
LCD 屏幕显示消息 `No CMC Found.`	机箱中没有 CMC。	将 CMC 插入机箱，或者如果机箱中有 CMC，则重装设现有 CMC。

前面板 LCD 消息

本节包括前面板 LCD 上显示错误和状态信息两个小节。

LCD 上的*错误消息*具有与从 CLI 或 Web 界面查看的系统事件日志 (SEL) 类似的格式。

错误部分中的表格列出各种 LCD 屏幕上显示的错误和警告消息以及可能的原因。尖括号 (< >) 中的文本表示该段文本可能会不一样。

LCD 上的*状态信息*包括关于机箱中各模块的说明性信息。此节中的表格说明了对每个组件显示的信息。

LCD 错误消息

表. 57: CMC 状态屏幕

严重性	消息	原因
严重	CMC <编号> 电池故障。	CMC CMOS 电池缺失或无电压。
严重	CMC <编号> LAN 心跳丢失。	CMC NIC 连接已拆除或未连接。
警告	A firmware or software incompatibility detected between iDRAC in slot <number> and CMC.（检测到插槽 <number> 中的 iDRAC 和 CMC 之间出现固件或软件的不兼容。）	两个设备间的固件不匹配，不支持一个或多个功能。
警告	A firmware or software incompatibility detected between system BIOS in slot <number> and CMC.（检测到插槽 <number> 中的系统 BIOS 和 CMC 之间出现固件或软件的不兼容。）	两个设备间的固件不匹配，不支持一个或多个功能。
警告	A firmware or software incompatibility detected between CMC 1 and CMC 2.（检测到 CMC 1 和 CMC 2 之间出现固件或软件不兼容。）	两个设备间的固件不匹配，不支持一个或多个功能。

表. 58: 机柜/机箱状态屏幕

严重性	消息	原因
严重	风扇 <编号> 已卸下。	此风扇是确保机柜/机箱正常冷却的必要组件。
警告	电源设备冗余下降。	一个或多个 PSU 发生故障或被卸下且系统不再支持完全 PSU 冗余。
严重	Power supply redundancy is lost.（电源设备冗余丢失。）	一个或多个 PSU 发生故障或被卸下且系统不再冗余。
严重	电源设备并非冗余。维持正常运行的资源不足。	一个或多个 PSU 发生故障或被卸下且系统缺乏足够电源维持正常运行。这可导致服务器断电。
警告	控制面板环境温度高于警告阈值上限。	机箱/机柜进气温度超出警告阈值。
严重	控制面板环境温度高于警告阈值上限。	机箱/机柜进气温度超出警告阈值。
严重	CMC 冗余丢失。	CMC 不再有冗余。如果待机 CMC 卸下，则发生此情况。
严重	All event logging is disabled.（所有事件日志记录已禁用。）	机箱/机柜无法将事件存储到日志。这通常表明控制面板或控制面板电缆出现问题。
警告	Log is full.（日志已满。）	机箱检测到 CEL（硬件日志）中只剩一个条目的空间。
警告	Log is almost full.（日志几乎写满。）	机箱事件日志已达到满负荷的 75%。

表. 59: 风扇状态屏幕

严重性	消息	原因
严重	风扇 <编号> 工作时 RPM 低于严重阈值下限。	指定风扇的速度不足以为系统提供充分冷却。
严重	风扇 <编号> 工作时 RPM 高于严重阈值上限。	指定风扇的速度过高，原因通常是扇叶破损。

表. 60: IOM 状态屏幕

严重性	消息	原因
警告	I/O 模块 <编号> 上检测到结构不匹配。	I/O 模块结构与服务器或冗余 I/O 模块的结构不匹配。
警告	在 I/O 模块 <编号> 上检测到链接调节故障。	无法设置 I/O 模块正确使用一个或多个服务器上的 NIC。
严重	在 I/O 模块 <编号> 上检测到故障。	I/O 模块发生故障。如果 I/O 模块热过载，也会导致相同错误。

表. 61: iKVM 状态屏幕

严重性	消息	原因
警告	控制台对本地 KVM 不可用。	轻微故障，如固件损坏等。
严重	本地 KVM 无法检测到任何主机。	USB 主机枚举故障。
严重	屏幕上显示 OSCAR 无法通过本地 KVM 使用。	OSCAR 故障。

严重性	消息	原因
不可恢复	本地 KVM 存在故障并关机。	串行 RIP 故障或 USB 主机芯片故障。

表. 62: PSU 状态屏幕

严重性	消息	原因
严重	Power supply <number> failed.（电源设备 <number> 故障。）	PSU 发生故障。
严重	The power input for power supply <number> is lost.（电源设备 <number> 的电源输入丢失。）	交流电源丢失或交流电源线拔掉。
警告	Power supply <number> is operating at 110 volts, and could cause a circuit breaker fault.（电源设备 <number> 在 110 伏特下工作，可能造成断路器故障。）	电源设备插入 110V 电源。

表. 63: 服务器状态屏幕

严重性	消息	原因
警告	系统板环境温度低于警告阈值下限。	服务器温度降低。
严重	系统板环境温度低于严重阈值下限。	服务器温度降低。
警告	系统板环境温度高于警告阈值上限。	服务器温度升高。
严重	系统板环境温度高于严重阈值上限。	服务器温度过高。
严重	系统板电流闩锁的电流超过允许的范围	电流超过故障阈值。
严重	系统板电池故障。	CMOS 电池缺失或无电压。
警告	存储电池电量低。	ROMB 电池电量不足。
严重	存储电池发生故障。	CMOS 电池缺失或无电压。
严重	CPU <编号> <电压传感器名称> 电压超出允许的范围。	
严重	系统板 <电压传感器名称> 电压超出允许的范围。	
严重	夹层卡 <编号> <电压传感器名称> 电压超过允许的范围。	
严重	存储 <电压传感器名称> 电压超过允许的范围。	
严重	CPU <number> has an internal error (IERR).（CPU <number> 出现内部错误 (IERR)。）	CPU 故障。
严重	CPU <number> has a thermal trip (over-temperature) event.（CPU <number> 出现热断路 [温度过高] 事件。）	CPU 过热。
严重	CPU <number> configuration is unsupported.（CPU <number> 配置不受支持。）	处理器类型不正确或位置错误。
严重	CPU <number> is absent.（CPU <number> 缺失。）	所需 CPU 缺少或不存在。
严重	夹层卡 B<插槽号> 状态：已确认夹层卡 B<插槽号> 的附加卡传感器安装错误。	为 IO 结构安装的夹层卡不正确。

严重性	消息	原因
严重	夹层卡 C<插槽号> 状态：已确认夹层卡 C<插槽号> 的附加卡传感器安装错误。	为 IO 结构安装的夹层卡不正确。
严重	Drive <number> is removed.（驱动器 <number> 已卸下。）	存储驱动器被卸下。
严重	驱动器 <编号> 上检测到故障。	存储驱动器发生故障。
严重	系统板故障保护电压超出允许的范围。	在系统板电压未处于正常水平时生成此事件。
严重	The watchdog timer expired.（监护程序计时器超时。）	iDRAC 监护程序计时器失效且未设置任何操作。
严重	监护程序计时器重设系统。	iDRAC 监护程序检测到系统已崩溃（由于没有从主机收到响应，因此计时器过期），并且操作设置为重新引导。
严重	监护程序计时器关闭系统。	iDRAC 监护程序检测到系统已崩溃（由于没有从主机收到响应，因此计时器过期），并且操作设置为关机。
严重	The watchdog timer power cycled the system.（监护程序计时器关闭系统电源然后打开。）	iDRAC 监护程序检测到系统已崩溃（由于没有从主机收到响应，因此计时器过期），并且操作设置为打开电源再关闭电源。
严重	Log is full.（日志已满。）	SEL 设备检测到 SEL 只剩下一个条目的空间。
警告	在位置 <位置> 处的内存设备上检测到永久可纠正的内存错误。	
警告	在位置 <位置> 处的内存设备上增加了永久可纠正内存错误率。	可纠正 ECC 错误达到严重程度。
严重	在位置 <位置> 处的内存设备上检测到多位内存错误。	已检测到不可校正的 ECC 错误。
严重	在总线 <编号> 设备 <编号> 功能 <编号> 处的组件上检测到 I/O 信道检查 NMI。	I/O 信道中生成严重中断。
严重	在插槽 <编号> 处的组件上检测到 I/O 信道检查 NMI。	I/O 信道中生成严重中断。
严重	在总线 <编号> 设备 <编号> 功能 <编号> 处的组件上检测到 PCI 奇偶校验错误。	在 PCI 总线上检测到奇偶校验错误。
严重	A PCI parity error was detected on a component at slot <number>.（插槽 <number> 的组件上检测到 PCI 奇偶校验错误。）	在 PCI 总线上检测到奇偶校验错误。
严重	在总线 <编号> 设备 <编号> 功能 <编号> 处的组件上检测到 PCI 系统错误。	设备检测到 PCI 错误。
严重	A PCI system error was detected on a component at slot <number>.（插槽 <number> 的组件上检测到 PCI 系统错误。）	设备检测到 PCI 错误。
严重	在位置 <位置> 处的内存设备上已禁用永久可纠正内存错误日志记录。	当内存设备有太多 SBE 记录时，将禁用单位错误日志记录。
严重	All event logging is disabled.（所有事件日志记录已禁用。）	
不可恢复	检测到 CPU 协议错误。	处理器协议已进入一种不可恢复的状态。

严重性	消息	原因
不可恢复	CPU bus parity error detected.（检测到 CPU 总线奇偶校验错误。）	处理器总线 PERR 已进入一种不可恢复的状态。
不可恢复	检测到 CPU <编号> 初始化错误。	处理器初始化已进入一种不可恢复的状态。
不可恢复	检测到 CPU 机器检查。	处理器机器检查已进入一种不可恢复的状态。
严重	Memory redundancy is lost.（内存冗余丢失。）	
严重	在总线 <编号> 设备 <编号> 功能 <编号> 处的组件上检测到总线严重错误。	在 PCIe 总线上检测到严重错误。
严重	在总线 <编号> 设备 <编号> 功能 <编号> 处的组件上检测到软件 NMI。	检测到芯片错误。
严重	在总线 <编号> 设备 <编号> 功能 <编号> 处的组件上无法对虚拟 MAC 地址进行编程。	可为此设备进行弹性地址编程。
严重	Device option ROM on mezzanine card <number> failed to support Link Tuning or FlexAddress.（夹层卡 <number> 上的设备选项 ROM 无法支持链接调节或 FlexAddress。）	选项 ROM 不支持弹性地址或链接调节。
严重	无法从 iDRAC 获取链接调节或 FlexAddress 数据。	

注: 有关其他服务器相关的 LCD 消息方面的信息，请参阅 Server User Guide（服务器用户指南）。

LCD 模块与服务器状态信息

本节中的表格说明了前面板 LCD 上显示的机箱中每种类型组件的状态项目。

表. 64: CMC 状态

项目	说明
示例：CMC1、CMC2	名称或位置。
无错误	如果没有错误，则显示“无错误”消息，否则列出错误消息。先列出严重错误，再列出警告。
固件版本	仅在活动 CMC 上显示。对于待机 CMC 显示“待机”。
IP4 <已启用, 已禁用>	仅在活动的 CMC 上显示当前 IPv4 启用状态。
IP4 地址：<地址, 获取中>	仅在 IPv4 只于活动 CMC 上启用时显示。
IP6 <已启用, 已禁用>	在活动的 CMC 上仅显示当前 IPv6 启用状态。
IP6 本地地址：<地址>	仅在 IPv6 只于活动 CMC 上启用时显示。
IP6 全局地址：<地址>	仅在 IPv6 只于活动 CMC 上启用时显示。
MAC：<地址>	显示 CMC 的 MAC 地址。

表. 65: 机箱或机柜状态

项目	说明
用户定义的名称	示例：Dell 机架系统。您可以通过 CMC 命令行界面 (CLI) 或 Web 界面设置该选项。
错误消息	如果没有错误，则显示“无错误”消息，否则列出错误消息。先列出严重错误，再列出警告。
型号	示例：PowerEdgeM1000e。
功耗	当前功耗（瓦）。
峰值功率	峰值功耗（瓦）。
最小功耗	最小功耗（瓦）。
环境温度	当前环境温度（摄氏度）。
Service Tag	工厂分配的服务标签。
CMC 冗余模式	非冗余或冗余。
PSU 冗余模式	非冗余、交流冗余或直流冗余。

表. 66: 风扇状态

项目	说明
名称/位置。	示例：Fan1、Fan2 等。
错误消息	如果没有错误，则显示"无错误"；否则列出错误信息，先列出严重错误，再列出警告。
RPM	当前风扇速度 (RPM)。

表. 67: PSU 状态

项目	说明
名称/位置。	示例：PSU1、PSU2 等。
错误消息	如果没有错误，则显示“无错误”消息，否则列出错误消息。先列出严重错误，再列出警告。
状态	脱机、联机或待机。
最大功率	PSU 可为系统提供的最大功率。

表. 68: IOM 状态

项目	说明
名称/位置。	例如，IOM A1、IOM B1 等等。
错误消息	如果没有错误，则显示“无错误”消息，否则列出错误消息。先列出严重错误，再列出警告。有关更多信息，请参阅 LCD 错误消息。
状态	关或开。
型号	IOM 型号。
结构类型	网络类型。
IP 地址	只有当 IOM 打开时才显示。对于直通类型 IOM，此值为零。

项目	说明
Service Tag	工厂分配的服务标签。

表. 69: iKVM 状态

项目	说明
名称	iKVM。
无错误	如果没有错误，则显示“无错误”消息，否则列出错误消息。先列出严重错误，再列出警告。有关更多信息，请参阅 LCD 错误消息。
状态	关或开。
型号/制造	iKVM 型号的说明。
Service Tag	工厂分配的服务标签。
部件号	制造商部件号。
固件版本	iKVM 固件版本。
硬件版本	iKVM 硬件版本。

注: 此信息动态更新

表. 70: 服务器状态

项目	说明
示例：Server 1、Server 2 等。	名称/位置。
无错误	如果没有错误，则显示“无错误”消息，否则列出错误消息。先列出严重错误，再列出警告。有关更多信息，请参阅 LCD 错误消息。
插槽名称	机箱插槽名称。例如 SLOT-01。 **注: 可通过 CMC CLI 或 Web 界面设置此表。**
名称	服务器名称，用户可通过 Dell OpenManage 进行设置。只有 iDRAC 完成引导并且服务器支持此功能时才显示该名称，否则显示 iDRAC 引导消息。
型号	如果 iDRAC 完成引导则显示。
Service Tag	如果 iDRAC 完成引导则显示。
BIOS Version	服务器 BIOS 固件版本。
最后一个开机自检代码	显示最后一个服务器 BIOS 开机自检代码消息字符串。
iDRAC 固件版本	如果 iDRAC 完成引导则显示。 **注: iDRAC 版本 1.01 显示为 1.1。不存在 iDRAC 版本 1.10。**
IP4 <已启用, 已禁用>	显示当前 IPv4 启用状态。
IP4 地址：<地址, 获取中>	仅当 IPv4 启用时显示。
IP6 <已启用, 已禁用>	仅当 iDRAC 支持 IPv6 时显示。显示当前 IPv6 启用状态。
IP6 本地地址：<地址>	仅当 iDRAC 支持 IPv6 且已启用 IPv6 时显示。

项目	说明
IP6 全局地址：<地址>	仅当 iDRAC 支持 IPv6 且已启用 IPv6 时显示。
在结构上启用了 Flex 地址	仅当已安装该功能时显示。列出为此服务器启用的结构（即 A、B 和 C）。

此表中的信息动态更新。如果服务器不支持此功能，则不会出现以下信息，否则服务器管理员使用以下选项：

- 选项“无” = LCD 上没有必须显示的字符串。
- 选项“默认值” = 无效果。
- 选项“自定义” = 允许为此服务器输入字符串名称。

仅当 iDRAC 完成引导后才显示此信息。有关此功能的更多信息，请参阅 **dell.com/support/manuals** 上的 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide*（适用于 Dell PowerEdge M1000e 的 Chassis Management Controller RACADM 命令行参考指南）。

18

常见问题

本部分列出了下列常见问题：

- RACADM
- 管理和恢复远程系统
- Active Directory
- FlexAddress 和 FlexAddressPlus
- iKVM
- IOM

主题：

RACADM

在执行 CMC 重设（使用 RACADM racreset 子命令）后，如果输入命令，则显示以下消息：

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

该消息表示仅当 CMC 完成重设后才能发出另一个命令。

使用 RACADM 子命令有时会显示以下一条或多条错误：

- 本地错误消息 - 诸如语法、印刷错误和错误名称等问题。例如：`ERROR: <message>`

使用 RACADM `help` 子命令显示正确的语法和用法信息。

与 CMC 有关的错误消息 - CMC 无法执行操作的问题。可能还会显示“racadm 命令失败”。

键入 `racadm gettracelog` 获取调试信息。

在使用远程 RACADM 时，提示符更改为 ">"，"$" 提示符不再显示。

如果在命令中使用不匹配的双引号 (") 或不匹配的单引号 (’)，则 CLI 会更改为 ">" 提示符并将所有命令排队。

要返回到“$”提示符，请键入 <Ctrl> - d。

此时显示一条错误消息：“未找到”，同时使用 `$ logout` 和 `$ quit` 命令。

在 CMC RACADM 界面中不支持 logout 和 quit 命令。

管理和恢复远程系统

访问 CMC Web 界面时，会显示安全警告，指示 SSL 证书的主机名与显示的 CMC 主机名不匹配。

CMC 包括一个默认的 CMC 服务器证书以确保 Web 界面和远程 RACADM 功能的网络安全。如果使用该证书，Web 浏览器就会显示一个安全警告，因为默认的证书颁发给与 CMC 的主机名（例如，IP 地址）不匹配的 CMC 默认证书。

要解决此安全问题，应上载一个颁发给 CMC IP 地址的 CMC 服务器证书。生成用于颁发证书的证书签名请求 (CSR) 时，应确保 CSR 的常用名 (CN) 与 CMC 的 IP 地址（例如，192.168.0.120）或注册的 DNS CMC 名称匹配。

要确保 CSR 与注册的 DNS CMC 名称匹配，请执行以下操作：

1 在 CMC Web 界面上，转至系统树，单击**机箱概览**。
2 单击**网络**选项卡，然后单击**网络**。
随即会出现**网络配置**页面。
3 在 **DNS** 选项上选择**注册 CMC**。
4 在 **DNS CMC 名称**字段中输入 CMC 名称。
5 单击**应用更改**。
有关生成 CSR 和颁发证书的更多信息，请参阅获取证书。

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 CMC Web 服务器之后，远程 RACADM 服务和 Web 界面可能要过一段时间才能恢复使用。CMC Web 服务器在发生以下事件后会重设：

- 使用 CMC Web 界面更改网络配置或网络安全属性。
- 更改 **cfgRacTuneHttpsPort** 属性（包括通过 `config -f <config file>` 命令进行更改）。
- 使用 `racresetcfg` 或还原机箱配置备份。
- CMC 重设。
- 上载了新的 SSL 服务器证书。

DNS 服务器没有注册我的 CMC。

有些 DNS 服务器最多只能注册含有 31 个字符的名称。

访问 CMC Web 界面时，显示一个安全警告，指出该 SSL 证书是由一家不可信的证书颁发机构颁发的。

CMC 包括一个默认的 CMC 服务器证书以确保 Web 界面和远程 RACADM 功能的网络安全。该证书不是由可信证书颁发机构颁发的。要解决这个安全问题，请上载一个由可信证书颁发机构（例如 Thawte 或 Verisign）颁发的 CMC 服务器证书。有关证书的更多信息，请参阅获取证书。

为何出于未知原因显示以下消息？

Remote Access: SNMP Authentication Failure

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

使用 RACADM 更改 CMC 团体名称。要查看 CMC 团体名称，请使用以下命令：

```
racadm getconfig -g cfgOobSnmp
```

要设置 CMC 团体名称，请使用以下命令：

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
```

要防止生成 SNMP 验证陷阱，请输入代理接受的团体名称。因为 CMC 只允许使用一个团体名称，所以请为 IT Assistant 发现设置输入相同的 get 和 set 团体名称。

Active Directory

Active Directory 是否支持跨多个树进行 CMC 登录？

CMC 的 Active Directory 查询算法支持单个目录林中的多个树。

使用 Active Directory 登录到 CMC 的操作是否可以在混合模式下进行（也就是说，目录林中的域控制器运行着不同的操作系统，比如 Microsoft Windows 2000 或 Windows Server 2003）？

是。在混合模式中，CMC 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。

配合使用 CMC 和 Active Directory 是否支持多个域环境？

是。域目录林功能级别必须处在本机 (Native) 或 Windows 2003 模式。此外，关联对象、RAC 用户对象和 RAC 设备对象（包括关联对象）的组都必须是通用组。

这些 Dell 扩展的对象（Dell 关联对象、Dell RAC 设备和 Dell 权限对象）是否可以位于不同的域？

关联对象和权限对象必须位于相同的域。Dell 扩展的 Active Directory 用户和计算机管理单元只允许您在相同的域中创建这两个对象。其他对象可以位于不同的域。

域控制器 SSL 配置是否有任何限制？

是。目录林中用于 Active Directory 服务器的所有 SSL 证书都必须由相同的根证书颁发机构签发，因为 CMC 只允许上载一个可信证书颁发机构签发的 SSL 证书。

只有在新 RAC 证书创建并上载后，Web 界面才会启动。

如果 Microsoft Certificate Services 用于生成 RAC 证书，则在创建证书时，可能使用了“用户证书”选项而非使用 Web 证书。

要进行恢复，请生成 CSR，从 Microsoft Certificate Services 创建新的 Web 证书并使用以下 RACADM 命令进行上载：

```
racadm sslcsrgen [-g] [-f {filename}]

racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress 和 FlexAddressPlus

如果取出功能卡，会发生什么情况？

取出功能卡后没有明显变化。功能卡可以取出和存储，或者原样不动。

如果取出某个机箱中使用的功能卡，并将它放入另一个机箱中，会发生什么情况？

Web 界面显示以下错误消息：

```
This feature card was activated with a different chassis. It must be removed before accessing
the FlexAddress feature.

Current Chassis Service Tag = XXXXXXXX

Feature Card Chassis Service Tag = YYYYYYYY

An entry is added to the CMC log that states:

cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'
```

如果卸下功能卡并安装非 FlexAddress 卡，会发生什么情况？

不应激活或修改该卡。该卡被 CMC 忽略。在这种情况下，**$racadm featurecard -s** 命令会返回以下消息：

```
No feature card inserted

ERROR: can't open file
```

如果对机箱服务标签重新编程，并且有功能卡绑定到该机箱，会发生什么情况？

- 如果该机箱或任何其它机箱上的活动 CMC 中存在原始功能卡，Web 界面将显示以下错误：
  - `This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.`
  - `Current Chassis Service Tag = XXXXXXXX`
  - `Feature Card Chassis Service Tag = YYYYYYYY`
  - 原始功能卡不能再在该机箱或任何其它机箱上取消激活，除非 Dell 服务人员重新将原始机箱服务标签设置回机箱中，并且具有原始功能卡的 CMC 在该机箱中设为活动。
- FlexAddress 功能在原来绑定的机箱上仍处于活动状态。该机箱*绑定*功能将更新以反映新服务标签。

如果将两个功能卡安装在冗余 CMC 系统中，是否会显示错误消息？

否，不显示任何错误消息。活动 CMC 中的功能卡处于活动状态并且安装在机箱中。CMC 会忽略第二个功能卡。

SD 卡上是否具有写保护锁？

是。将 SD 卡安装到 CMC 模块之前，需要验证写保护锁是否处于“解除锁定”位置。如果 SD 卡受写保护，就不能激活 FlexAddress 功能。在这种情况下，**$racadm feature -s** 命令会返回以下消息：

```
No features active on the chassis. ERROR: read only file system
```

如果活动的 CMC 模块中没有 SD 卡，会发生什么情况？

$racadm featurecard -s 命令会返回以下消息：

```
No feature card inserted.
```

如果服务器 BIOS 从版本 1.xx 更新到版本 2.xx，FlexAddress 功能会发生什么情况？

服务器模块需要在使用 FlexAddress 之前关闭电源。服务器 BIOS 更新完成后，服务器模块会在服务器关闭电源再打开电源之后获得机箱分配的地址。

如果具有单个 CMC 的机箱将固件版本降级到 1.10 之前的版本会发生什么情况？

- 会从机箱删除 FlexAddress 功能和配置。

- 用于激活此机箱上的功能的功能卡不变，而且仍然绑定到该机箱。随后将此机箱的 CMC 固件升级到版本 1.10 或更高版本时，通过重新插入原始功能卡（如有必要），重设 CMC（如果在固件升级完成之后插入功能卡）和重新配置功能来重新激活 FlexAddress 功能。

如果在带有冗余 CMC 的机箱中将 CMC 设备更换为固件版本早于 1.10 的 CMC 设备，会发生什么情况？

在带有冗余 CMC 的机箱中，如果将 CMC 设备更换为固件版本早于 1.10 的 CMC 设备，必须执行以下过程确保当前 FlexAddress 功能和配置不会被删除。

- 确保活动 CMC 固件始终为版本 1.10 或更高。
- 卸下待机 CMC 并在其位置上插入新的 CMC。
- 从活动 CMC 中，将待机 CMC 固件升级到 1.10 或更高版本。

注: 如果待机 CMC 固件未更新到 1.10 或更高版本，并且发生故障转移，则 FlexAddress 功能未配置。此功能必须再次重新激活并重新配置。

如果在 FlexAddress 上执行了停用命令时 SD 卡不在机箱中，则如何恢复使用 SD 卡？

问题在于，如果停用 FlexAddress 时 SD 卡不在 CMC 中，就不能使用该 SD 卡在另一个机箱上安装 FlexAddress。要恢复使用该卡，请将卡插回其绑定到的机箱的 CMC 中，重新安装 FlexAddress，然后再停用 FlexAddress。

已正确安装 SD 卡并且已安装所有固件或软件更新。FlexAddress 处于活动状态，但服务器部署屏幕为什么不显示进行部署的选项？出了什么问题？

这是浏览器缓冲问题；请关闭浏览器并重新启动。

如果我需要使用 RACADM 命令 racresetcfg 重设我的机箱配置，FlexAddress 会发生什么情况？

FlexAddress 功能仍然处于激活状态，随时可以使用。默认情况下会选择所有结构和插槽。

注: 在发出 RACADM 命令 `racresetcfg` 之前，强烈建议关闭机箱电源。

在仅禁用 FlexAddressPlus 功能（让 FlexAddress 仍然处于激活状态）之后，为何仍然活动的 CMC 上的 racadm setflexaddr 命令会失败？

如果 CMC 后来变为活动状态，而 FlexAddressPlus 功能卡仍然在其卡插槽中，则 FlexAddressPlus 功能将被再次激活，而且插槽或结构 flexaddress 配置更改可恢复。

iKVM

连接到前面板的显示器上显示“用户已被 CMC 控制禁用”消息。为什么？

前面板连接已被 CMC 禁用。可以使用 CMC Web 界面或 RACADM 启用前面板。

要使用 CMC Web 界面启用前面板，请转至 **iKVM** > **设置**选项卡，选中**前面板 USB/视频已启用**选项，然后单击**应用**保存设置。

要使用 RACADM 启用前面板，打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1
```

后面板访问不起作用。为什么？

前面板设置已被 CMC 启用，且有一个显示器当前正连接到前面板。

每次只允许有一个连接。前面板连接优先于 ACI 和后面板。有关连接优先次序的更多信息，请参阅“iKVM 连接优先次序”。

连接到后面板的显示器上显示“用户已被禁用，因为另一台设备当前已分层”消息。为什么？

网络电缆已连接到 iKVM ACI 端口连接器和次 KVM 设备。

每次只允许有一个连接。ACI 分层连接优先于后面板显示器连接。优先次序为前面板、ACI，然后是后面板。

iKVM 的琥珀色 LED 指示灯正在闪烁。为什么？

有三种可能原因：

- **iKVM 出现了问题**，需要重新编程。要修复此问题，请遵照 iKVM 固件更新说明操作。
- **iKVM 正在重新编程 CMC 控制台界面。**在这种情况下，CMC 控制台暂时不可用并由 OSCAR 界面中的一个黄点表示。此过程最多需要 15 分钟。
- **iKVM 固件检测到一个硬件错误。**有关附加信息，请查看 iKVM 状态。

KVM 通过 ACI 端口分层到外部 KVM 交换机，但是 ACI 连接的所有条目都不可用。

所有状态都在 OSCAR 界面中显示一个黄点。

前面板连接已启用并已连接一个显示器。因为前面板优先于所有其他 iKVM 连接，所以 ACI 和后面板连接器均被禁用。

要启用 ACI 端口连接，必须先禁用前面板访问或卸下连接到前面板的显示器。外部 KVM 交换机 OSCAR 条目将被激活并可访问。

要使用 Web 界面禁用前面板，请转至 **iKVM** > **设置**选项卡，清除**前面板 USB/视频已启用**选项，然后单击“应用”。

要使用 RACADM 禁用前面板，打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0

在 OSCAR 菜单中，Dell CMC 连接显示红色 X，无法连接到 CMC。为什么？

有两种可能原因：

- **Dell CMC 控制台已被禁用。**在这种情况下，可使用 CMC Web 界面或 RACADM 启用它。
- **CMC 不可用，因为它正在初始化、正在切换到待机 CMC 或正在重新编程。**在这种情况下，只需等待 CMC 完成初始化即可。

一个服务器的插槽名称在 OSCAR 中显示为 "正在初始化"，我无法选择它。为什么？

服务器正在初始化或该服务器上的 iDRAC 初始化失败。

首先，等待 60 秒钟。如果服务器仍在进行初始化，则初始化一完成就会显示插槽名称，然后您可以选择服务器。

如果经过 60 秒钟后，OSCAR 仍表示插槽正在初始化，则应卸下服务器，然后将服务器重新插入机箱。此操作允许 iDRAC 重新初始化。

IOM

在配置更改后，有时 CMC 将 IP 地址显示为 0.0.0.0。

单击**刷新**图标了解交换机上的 IP 地址是否设置正确。如果 IP/掩码/网关设置有误，交换机不会设置 IP 地址并在所有字段中返回 0.0.0.0。

常见错误有：

- 将带外 IP 地址设置为与带内管理 IP 地址相同或位于相同的网络。
- 输入无效的子网掩码。
- 将默认网关设置为没有直接连接到该交换机的网络地址。

有关 IOM 网络设置的更多信息，请参阅 **dell.com/support/manuals** 上的 *Dell PowerConnect M6220 Switch Important Information*（Dell PowerConnect M6220 交换机重要信息）说明文件和 *Dell PowerConnect 6220 Series Port Aggregator White Paper*（Dell PowerConnect 6220 系列端口聚合器白皮书）。

单一登录

虽然已将 CMC 设置为允许单一登录 (SSO)，但浏览器显示空白页。

目前只有 Mozilla Firefox 和 Internet Explorer 浏览器支持 SSO。请检查浏览器设置是否正确。有关更多信息，请参阅配置浏览器以使用 SSO 登录部分。

如果浏览器配置正确，必须确保两个浏览器允许您不输入名称和密码直接登录。使用完全限定域名 (FQDN) 登录 CMC。例如，在浏览器地址栏中输入 **myCMC.Domain.ext/**。浏览器会将您重定向到 **https**（安全模式）并允许您登录到 CMC。**http** 和 **https** 对浏览器来说都有效。如果您将该 URL 保存为书签，则不需要在示例网址中的斜线后输入任何文本。如果您仍然无法使用 SSO 登录，请参阅为 Active Directory 用户配置 CMC SSO 或智能卡登录部分。

19

使用案例场景

本节帮助您导航至本指南中特定的章节来执行特定用户的案例场景。

主题：

机箱基本配置和固件更新

此场景将引导您执行以下任务：

- 使用基本配置启动机箱。
- 验证 CMC 是否正在检测硬件并且无错误。
- 更新 CMC、IOM 和服务器组件的固件。

1 CMC 已预先安装在机箱中，因此无需安装。可以安装第二个 CMC 作为活动 CMC 的备用。
有关安装第二个 CMC 的信息，请参阅了解冗余 CMC 环境部分。

2 按照设置机箱一览表中提供的步骤设置机箱。

3 使用 LCD 面板或 Dell CMC 串行控制台配置 CMC 管理 IP 地址和初始 CMC 网络。
有关信息，请参阅配置初始 CMC 网络部分。

4 配置日志和警报以针对管理系统上发生的某些事件生成日志和设置警报。
有关信息，请参阅配置 CMC 以发送警报部分。

5 使用 CMC Web 界面配置服务器的 IP 地址和网络设置。
有关信息，请参阅配置服务器。

6 使用 Web 界面配置 IOM 的 IP 地址和网络设置。
有关更多信息，请参阅为 IOM 配置网络设置部分。

7 打开服务器电源。

8 检查硬件日志、CMC 日志和电子邮件或 SNMP 陷阱警报中是否存在无效的硬件配置。
有关更多信息，请参阅查看事件日志部分。

9 要诊断与硬件相关的问题，请访问**诊断控制台**。
有关使用**诊断控制台**的更多信息，请参阅使用诊断控制台部分。

10 有关硬件配置问题中的错误信息，请参阅 **dell.com/support/manuals** 上的 *Dell Event Message Reference Guide*（Dell 事件消息参考指南）或 *Server Administrator Messages Reference Guide*（服务器管理员消息参考指南）。

11 更新 CMC、IOM 和服务器组件的固件。
有关信息，请参阅更新固件部分。

备份 CMC 配置和服务器配置。

1 要备份机箱配置，请参阅保存或还原机箱配置部分。
2 要保存服务器的配置，请使用 CMC 的**服务器克隆**功能。
有关信息，请参阅使用服务器克隆配置配置文件设置。
3 使用 CMC Web 界面将服务器的现有配置保存至外部存储卡。
有关信息，请参阅添加或保存配置文件部分。
4 使用 CMC Web 界面，将外部存储卡上保存的配置应用于所需的服务器。
有关更多信息，请参阅应用配置文件部分。

更新管理控制台固件而无需服务器停机

您可以更新 CMC、iDRAC 和 Lifecycle Controller 管理控制台的固件而无需服务器停机：

1 当主要和待机 CMC 都存在时，您可以更新 CMC 固件而无需服务器或 IOM 停机。
2 要更新主要 CMC 上的固件，请参阅更新固件部分。
更新主要 CMC 上的固件时，待机 CMC 会承担主要 CMC 的角色，因此，IOM 和服务器不会停机。

注: 固件更新过程仅会影响 IOM 和 iDRAC 服务器的管理控制台，对服务器和 IOM 之间的外部连接没有影响。

3 要更新 iDRAC 或 Lifecycle Controller 固件而不关闭机箱，请使用 Lifecycle Controller 服务执行更新。有关使用 Lifecycle Controller 更新服务器组件固件的信息，请参阅升级服务器组件固件部分。

注: 更新 Mezzanine 卡、NDC 控制器和 BIOS 等任何其他组件时，服务器需要停机。

扩展电源性能场景 - 使用 Web 界面

场景 1：已对 3000W PSU 启用 EPP：

- Web 界面中的以下选项显示为灰色并且不可供选择：
  - 基于服务器的电源管理 (SBPM)。
  - 冗余策略：电源设备冗余和无冗余。
  - 服务器性能优先于电源冗余 (SPOPR)。
  - 动态电源设备接入 (DPSE)。
  - 允许 110 VAC 运行。
- 如果将系统输入功率上限值更改为小于或等于 13300 W，会显示以下消息：

```
System Input Power Cap cannot be set to less than or equal to 13300 W (45381 BTU/h) while Extended Power Performance is enabled.
```

- 选中该复选框启用最大节能模式 (MPCM) 时将显示以下消息：

```
Enabling Max Power Conservation Mode will deactivate Extended Power Performance. Max Power Conservation Mode option will force servers into a low power, limited performance mode and disable server power up. Press OK to continue.
```

场景 2：已对 3000W PSU 禁用 EPP：

- Web 界面中的以下选项显示为灰色并且不可供选择：
  - 服务器性能优先于电源冗余 (SPOPR)。
  - 允许 110 VAC 运行。

- 选中该复选框启用基于服务器的电源管理 (SBPM) 时将显示以下消息：

  ```
  Checking the Server Based Power Management Mode option will set your power cap to max value, server priorities to default priority, and disables Max Power Conservation Mode. Are you sure you want to continue?
  ```

- 选中该复选框启用最大节能模式 (MPCM) 时将显示以下消息：

  ```
  Enabling Max Power Conservation Mode option will force servers into a low power, limited performance mode and disable server power up. Press OK to continue.
  ```

场景 3：在以下情况下 EPP 选项变为灰色且不可供选择：

- 已对 3000W PSU 禁用 EPP，并且启用了以下任一电源设置：
  - 基于服务器的电源管理 (SBPM)
  - 冗余策略：电源设备冗余或无冗余
  - 最大节能模式 (MPCM)。
  - 动态电源设备接入 (DPSE)。
  - 系统输入功率上限值设置为小于或等于 13300W 或 (45381 BTU/h）。
- 机箱未安装六个 3000W PSU 或所有 PSU 都不支持 EPP，EPP 选项变为灰色且不可供选择。

扩展电源性能场景 - 使用 RACADM

场景 1：使用 racadm getconfig/config set 命令管理 EPP 功能控制（启用/禁用）

- 要在 3000W 交流 PSU 配置上启用 EPP 功能，可使用：

  ```
  racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
  ```

- To disable EPP feature on a 3000W AC PSU configuration, use:

  ```
  To disable EPP feature on a 3000W AC PSU configuration, use:
  ```

- 要在 3000W 交流 PSU 配置上检查是否已启用 EPP 功能，可使用：

  ```
  racadm getconfig -g cfgChassisPower -o cfgChassisEPPEnable
  ```

场景 2：使用 `racadm getpbinfo` 查看 EPP 功能状态：

```
racadm getpbinfo
Extended Power Performance(EPP) Status = Enabled (inactive)
Available Power in EPP Pool            = 3167 W (10806 BTU/h)
Used Power in EPP Pool                 = 0 W (0 BTU/h)
EPP Percent - Available                = 100.0
```

场景 3：查看 CMC 日志中记录的 EPP 功能控制操作：

```
racadm getraclog
Jul 31 14:16:11 CMC-4C2WXF1 Log Cleared
Jul 31 14:15:49 CMC-4C2WXF1 Extended Power Performance is Enabled
Jul 31 14:15:49 CMC-4C2WXF1 Extended Power Performance is Disabled
```

场景 4：在启用了 EPP 时，更改与 EPP 不兼容的电源配置属性：

- 在 3000W 交流 PSU 上启用基于服务器的电源管理 (SBMP)

  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 1
  This feature is not supported while Extended Power Performance is enabled.
  ```

- 在 3000W 交流 PSU 上启用动态电源设备接入

  ```
  racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 1
  This feature is not supported while Extended Power Performance is enabled.
  ```

- 将电源冗余策略从电网冗余策略更改为 3000W 交流 PSU 上的 PSU 冗余策略

  ```
  racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 2
  This feature is not supported while Extended Power Performance is enabled.
  ```

- 将电源冗余策略从电网冗余策略更改为 3000W 交流 PSU 上的无冗余策略

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 0
This feature is not supported while Extended Power Performance is enabled.
```

- 将系统输入功率上限值更改为小于或等于 13300 W

```
racadm config –g cfgChassisPower -o  cfgChassisPowerCap 12500
System Input Power Cap cannot be set to less than or equal to  13300W (45381  BTU/h)
while Extended Power Performance is enabled.
```

- 在 3000W 交流 PSU 上启用 110V（交流）

```
racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
This feature is not supported on 3000W power supplies.
```

- 在 3000W 交流 PSU 上启用最大节能模式

注: 将 RACADM CLI 结合现有界面使用，可在 3000W 交流 PSU 配置上启用最大节能模式 (MPCM)。如果启用了 EPP，启用 MPCM 时无需更改 RACADM CLI 界面。

场景 5：当设置了其他电源配置设置时，尝试从已禁用的开始状态下启用 EPP。

- 在系统输入功率上限较低时在 3000W 交流 PSU 上启用 EPP

```
 racadm config -g cfgchassispower -o cfgChassisEPPEnable
 This feature is not supported while System Input Power Cap is set  to less than or equal to
13300 W (45381 BTU/h).
```

- 在启用了 DPSE 后在 3000W 交流 PSU 上启用 EPP

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported while Dynamic Power Supply Engagement is enabled.
```

- 在启用了 SBPM 后在 3000W 交流 PSU 上启用 EPP

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported while Server Based Power Management is enabled.
```

- 在启用了 MPCM 后在 3000W 交流 PSU 上启用 EPP

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported while Max Power Conservation Mode is enabled.
```

- 在设置了 PSU 冗余策略后在 3000W 交流 PSU 上启用 EPP

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported until Redundancy Policy is set to Grid Redundancy.
```

- 在设置了无冗余策略后在 3000W 交流 PSU 上启用 EPP

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported until Redundancy Policy is set to Grid Redundancy.
```

场景 6：在 3000W 交流 PSU 上启用了 EPP 后固件降级

```
racadm fwupdate -g -u -a 192.168.0.100 -d firmimg.cmc -m cmc-active -m cmc-standby
Cannot update local CMC firmware: The uploaded firmware image does not support the installed
power supplies.
```