适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller 1.1 版本 用户指南

注、小心和警告

注: “注”表示可以帮助您更好地使用计算机的重要信息。

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。

2014 - 12

Rev. A00

目录

1 概览

适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller (CMC) 是用于管理 **PowerEdge FX2/FX2s** 机箱的系统管理硬件和软件解决方案。CMC 具有自己的微处理器和内存，由其所插入的模块化机箱供电。

IT 管理员使用 CMC 可以：

- 查看资源清册。
- 执行配置和监测任务。
- 远程打开和关闭机箱和服务器的电源。
- 启用针对服务器模块中的服务器和组件事件的警报。
- 查看 PCIe 映射信息。
- 为机箱中的 iDRAC 和 I/O 模块提供一对多管理界面。

CMC 为服务器提供多项系统管理功能。电源和温度管理是 CMC 的主要功能，下面列出了这些功能：

- 机柜级别电源和温度实时自动管理。
  - CMC 报告实时功耗，包括用时间戳记录最高点和最低点。
  - CMC 支持设置可选的机柜最大功率限制（系统输入功率上限），一旦超过该限制就会触发警报和采取措施，例如限制服务器功耗和/或防止新服务器开机，以使机柜功率保持在规定的最大功率限制以内。
  - CMC 将监测冷却风扇，同时根据实际环境温度和内部温度测量值自动控制冷却风扇的运行。
  - CMC 提供全面的机柜资源清册和状态或错误报告。
- CMC 提供针对以下设置的集中配置机制：
  - PowerEdge FX2/FX2s 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。
  - 服务器模块上的第一引导设备。
  - 检查 I/O 模块和服务器之间的 I/O 结构一致性。CMC 还可根据需要禁用组件，以保护系统硬件。
  - 用户访问安全。
  - PCIe 插槽。

可以将 CMC 配置为在出现与温度、硬件误配置、电源故障和风扇速度等相关的警告或错误时，发送电子邮件警报或 SNMP 陷阱警报。

主要功能

CMC 功能分为管理功能和安全保护功能。

本发行版中的新增功能

此版本 Dell PowerEdge FX2/FX2s 的 CMC 支持：

- 第 13 代刀片服务器。
- 增强的 WWN/MAC 地址资源清册，其中包括使用 iDRAC IO 标识功能分配给 LOM/精选网络适配器 (SNA) 的 WWN/MAC 地址。
- 查看作为 WWN/MAC 地址资源清册一部分的 NIC 分区的状态（独立于操作系统）。
- 为服务器配置文件和自定义 DUP 存储库使用远程 NFS/CIFS 目录中的目录。
- 使用外部库（CIFS/NFS 目录）更新存储库和配置文件的选项。
- 查看和使用存储在外部库中的已捕获配置文件的选项。
- 使用 iDRAC IO 标识功能的增强 WWN/MAC 地址资源清册。
- 对 CMC 固件映像执行签名检查。
- 使用 DUP 更新 CMC

管理功能

CMC 提供以下管理功能：

- IPv4 和 IPv6 的动态域名系统 (DDNS) 注册。
- 本地用户、Active Directory 和 LDAP 的登录管理与配置。
- 使用 SNMP、Web 界面、集成式 KVM、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机箱日志。
- 针对各种机箱组件的固件更新 - 允许更新 CMC、服务器上 iDRAC 和机箱基础结构的固件。
- 使用 Lifecycle Controller，在机箱中的多个服务器上进行 BIOS、网络控制器等服务器组件的固件更新。
- Dell OpenManage 软件集成 - 使您能够从 Dell OpenManage Server Administrator 或 OpenManage Essentials (OME) 1.2 启动 CMC Web 界面。
- CMC 警报 - 通过远程系统日志电子邮件或 SNMP 陷阱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。
- 多节点底座适配。PowerEdge FM120x4 是多节点底座。
- 机箱功率限制监测。
- iDRAC IO 标识功能支持增强的 WWN/MAC 地址资源清册。
- 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。
- 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。
- 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。
- 多机箱管理，可从主机箱查看最多 19 个其他机箱。

注: 在 IPv6 网络上不支持多机箱管理。

安全保护功能

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：
  - 使用标准架构或扩展架构（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。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。
- CMC 已签名映像 - 用于使用数字签名保护固件映像以防范未检测到的修改。

机箱概览

这里显示了机箱的背面板视图，并在表格中列出了 CMC 中的可用部件和设备。

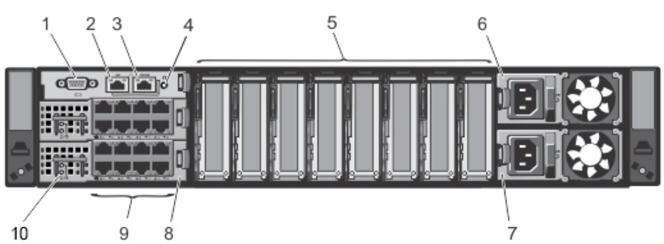
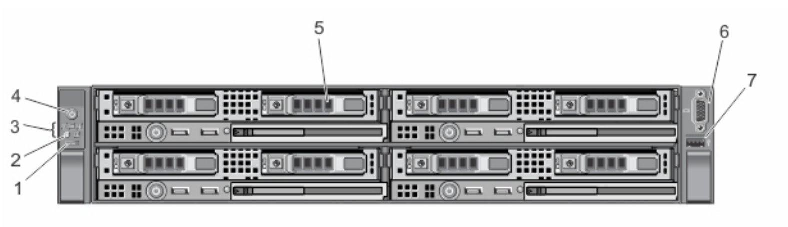


图 1:

项目	指示灯、按钮或连接器
1	串行连接器
2	以太网连接器 Gb1

项目	指示灯、按钮或连接器
3	以太网连接器 STK/Gb2（堆栈）
4	系统识别按钮
5	薄型 PCIe 扩展槽
6	电源设备 (PSU1)
7	电源设备 (PSU2)
8	I/O 模块（2 个）
9	I/O 模块端口
10	I/O 模块指示灯

这里显示了机箱的前面板视图，并在表格中列出了 CMC 中的可用部件和设备。



项目	指示灯、按钮或连接器
1	KVM 选择按钮
2	系统识别按钮
3	诊断指示灯
4	机柜通电指示灯、电源按钮
5	底座
6	视频连接器
7	USB 连接器

支持的远程访问连接

下表列出了支持的远程访问连接。

表. 1: 支持的远程访问连接

<table>
<tr><th>连接</th><th>功能</th></tr>
<tr><td>CMC 网络接口端口</td><td>

- Gb 端口：CMC Web 界面的专用网络接口。CMC 包含两个 RJ-45 以太网端口：
  - Gb1（上行链路端口）
  - Gb2（堆叠或缆线集合端口）。STK/Gb2 端口也可用于 CMC NIC 故障转移。

    注: 确保 CMC 设置从默认的**堆栈**更改为**冗余**以实现 NIC 故障转移。

    小心: 如果 CMC 设置没有从默认的堆栈更改为冗余来实施 NIC 故障转移，则将 STK/Gb2 端口连接到管理网络会出现无法预测的结果。在默认的堆栈模式下，将 Gb1 和 STK/Gb2 端口连接到相同的网络（广播域）会引发广播风暴。如果将 CMC 设置更改为冗余模式，但堆叠模式中的机箱间采用菊花链式连接，还会引发广播风暴。确保布线模式符合针对预期用途的 CMC 设置。
- 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。

</td></tr>
<tr><td>串行端口</td><td>

- 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。

</td></tr>
</table>

支持的平台

CMC 支持 **PowerEdge FX2** 和 **FX2s** 机箱型号。支持的平台包括 PowerEdge FC630 和 PowerEdge FM120x4。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的信息，请参阅 **dell.com/support/manuals** 上的 *Dell Chassis Management Controller (CMC) Version 1.1 for Dell PowerEdge FX2/FX2s Release Notes*（适用于 Dell PowerEdge FX2/FX2s 的 Dell Chassis Management Controller (CMC) 版本 1.1 发行说明）。

支持的 Web 浏览器

有关支持的 Web 浏览器的最新信息，请参阅 **dell.com/support/manuals** 上的 *Dell Chassis Management Controller (CMC) Version 1.1 for Dell PowerEdge FX2/FX2s Release Notes*（适用于 Dell PowerEdge FX2/FX2s 的 Dell Chassis Management Controller (CMC) 版本 1.1 发行说明）。

管理许可证

基于所购买的许可证（CMC Express 或 CMC Enterprise）提供 CMC 功能。界面中只提供已获得许可的功能，以允许您配置或使用 CMC。例如 CMC Web 界面、RACADM、WS-MAN 等。始终可通过 CMC Web 界面和 RACADM 访问 CMC 许可证管理和固件更新功能。

许可证类型

提供的许可证类型包括：

- 30 天评估和扩展 - 许可证在 30 天到期后可延长 30 天。评估许可证按持续时间计时，计时器在为系统通电时开始计时。
- 永久 - 许可证绑定到服务标签，而且是永久性的。

获取许可证

使用以下任何方法都可获取许可证：

- 电子邮件 - 从技术支持中心请求后，许可证会附加到发送的电子邮件中。
- 自助服务门户 - CMC 中提供了自助服务门户的链接。单击该链接可打开互联网上的许可自助服务门户，通过该门户可购买许可证。有关更多信息，请参阅自助服务门户页面的联机帮助。
- 销售点 - 订购系统时即可获得许可证。

许可证操作

在执行许可证管理任务之前，请确保获得许可证。有关更多信息，请参阅获取许可证部分以及 support.dell.com 上提供的“概览和功能指南”。

注: 如果您购买的系统已预先安装所有许可证，请无需进行许可证管理。

对于一对一许可证管理，您可以使用 CMC、RACADM 和 WS-MAN 执行以下许可操作；对于一对多许可证管理，您可以使用 Dell License Manager 执行以下许可操作：

- 查看 - 查看当前许可证信息。
- 导入 - 获取许可证后，将许可证存储在本地存储位置，并使用支持的界面之一将其导入 CMC。如果许可证通过验证检查，则会导入。

  注: 对于新功能，可能需要重新启动 CMC 才能启用功能。
- 导出 - 将已安装的许可证导出至外部存储设备进行备份，或者在更换维修部件后重新安装许可证。导出许可证的文件名和格式为 <EntitlementID>.xml。
- 删除 - 如果组件丢失，删除分配给组件的许可证。将许可证删除后，它不会存储在 CMC 中，并且基本产品功能会启用。
- 更换 - 更换许可证以扩展评估许可证，更改许可证类型（如使用购买的许可证更改评估许可证），或者延长过期的许可证。
- 您可以使用升级的评估许可证或购买的许可证更换评估许可证。
- 可以使用更新的许可证或升级的许可证来更换购买的许可证。有关更多信息，请参阅位于 HTTPS://WWW.DELL.COM/SUPPORT/LICENSING/US/EN/19 的 Dell 软件许可证管理门户。
- 了解详情 - 了解已安装许可证或可供服务器上已安装组件使用的许可证的详细信息。

注: 为了让 Learn More（了解详情）选项显示正确的页面，请确保在 Security Settings“安全设置”中已将 *.dell.com 添加到 Trusted Sites（受信任的站点）列表中。有关更多信息，请参阅“Internet Explorer 帮助”文档。

注: 如果您尝试在 PowerEdge FC630 上安装 PowerEdge FM120x4 许可证，则许可证安装会失败。有关许可的更多信息，请参阅 *Integrated Dell Remote Access Controller (iDRAC) User's Guide*（Integrated Dell Remote Access Controller (iDRAC) 用户指南）。

CMC 中的可授权功能

此表中列出了基于您的许可证启用的 CMC 功能列表。

功能	Express	Enterprise
CMC 网络	是	是
CMC 串行端口	是	是
RACADM（SSH、本地和远程）	是	是
WS-MAN	是	是
SNMP	是	是
Telnet	是	是
SSH	是	是
基于 Web 的界面	是	是
电子邮件警报	是	是
CMC 设置备份	否	是
CMC 设置恢复	是	是
远程系统日志	否	是
目录服务	否	是
单一登录支持	否	是
双重验证	否	是
PK 验证	否	是
远程文件共享	否	是
机柜级功率上限	否	是
多机箱管理	否	是

FlexAddress 启用	否	是
一对多服务器固件更新	否	是
iDRAC 的一对多配置	否	是

许可证组件的状态或条件以及可用操作

下表提供了基于许可证状态或条件的可用许可证操作列表。

表 1. 基于状态和条件的许可证操作

许可证/组件状态或条件	导入	导出	删除	替换	了解更多
非管理员登录	否	是	否	否	是
活动许可证	是	是	是	是	是
过期许可证	否	是	是	是	是
许可证已安装但组件丢失	否	是	是	否	是

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，请仔细阅读 Web 浏览器的说明文件。要查看本地化版本，请将浏览器设置为所需的语言。

支持的管理控制台应用程序

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

如何使用本用户指南

本用户指南中的内容指导您使用以下工具执行任务：

- Web 界面：本指南只提供任务相关信息。有关字段和选项的信息，请参阅可通过 Web 界面打开的*适用于 Dell PowerEdge FX2/FX2s 的 CMC 联机帮助*。
- RACADM 命令：本指南提供您必须使用的 RACADM 命令或对象。有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

您可能需要的其他说明文件

可从 Dell 支持网站访问说明文件。除了本参考指南之外，还可以从 **dell.com/support/manuals** 访问以下指南。

- *CMC FX2/FX2s 联机帮助*提供有关使用 Web 界面的信息。要访问联机帮助，请在 CMC Web 界面上单击**帮助**。
- *Chassis Management Controller Version 1.1 for Dell PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 Dell PowerEdge FX2/FX2s 的 Chassis Management Controller 版本 1.1 RACADM 命令行参考指南）提供有关使用 FX2/FX2s 相关 RACADM 功能的信息。
- *Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2/FX2s Version 1.1 Release Notes*（适用于 Dell PowerEdge FX2/FX2s 的 Dell Chassis Management Controller (CMC) 版本 1.1 发行说明）提供系统或说明文件的最新更新，或者是面向有经验的用户或技术人员的高级技术参考资料。
- *Integrated Dell Remote Access Controller 7 (iDRAC) User's Guide*（Integrated Dell Remote Access Controller 7 (iDRAC7) 用户指南）提供有关在管理系统中安装、配置和维护 iDRAC7 的信息。
- *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 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。
- Dell 系统管理应用程序说明文件提供了关于安装和使用系统管理软件的信息。

以下系统说明文件提供关于安装 CMC PowerEdege FX2/FX2s 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。
- 系统随附的设置单张说明文件提供有关初始系统设置和配置的信息。
- 服务器模块的*用户手册*提供有关服务器模块功能的信息，并介绍如何排除服务器模块故障，以及如何安装或更换服务器模块的组件。此说明文件在 dell.com/poweredgemanuals 上在线提供。
- 机架解决方案附带的机架说明文件介绍了如何将系统安装到机架中（如果需要）。
- 有关本说明文件中所用缩写或缩略词的全称，请参阅 dell.com/support/manuals 上的 Glossary（词汇表）。
- 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。
- 系统随附的所有介质都提供了用于配置和管理系统的说明文件和工具，包括与随系统购买的操作系统、系统管理软件、系统更新以及系统组件相关的说明文件和工具。有关系统的更多信息，请扫描系统的快速资源定位器 (QRL) 以及系统随附的系统设置单张说明文件。从移动平台下载 QRL 应用，以便在您的移动设备上启用该应用。

系统有时附带更新，用于说明对系统、软件和/或说明文件所做的更改。请务必先阅读这些更新，因为这些更新通常会取代其他说明文件中的信息。

从 Dell 支持站点访问说明文件

您可以通过以下方式之一访问所需的说明文件：

- 使用以下链接：
  - 所有企业系统管理说明文件 - **dell.com/softwaresecuritymanuals**
  - 企业系统管理说明文件 - **dell.com/openmanagemanuals**
  - 远程企业系统管理说明文件 - **dell.com/esmmanuals**
  - OpenManage Connections Enterprise 系统管理说明文件 - **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - 适用性工具说明文件 - **dell.com/serviceabilitytools**
  - 客户端系统管理说明文件 - **dell.com/clientsystemsmanagement**
  - OpenManage Connections Client 系统管理说明文件 - **dell.com/connectionsclientsystemsmanagement**

- 从 Dell 支持网站：

  a. 转至 **dell.com/support/home**。
  b. 在 **General support**（一般支持）部分下，单击 **Software & Security**（软件与安全）。
  c. 在 **Software & Security**（软件与安全）组框中，通过以下项单击所需的链接：
     – **Enterprise Systems Management**（企业系统管理）
     – **Remote Enterprise Systems Management**（远程企业系统管理）
     – **Serviceability Tools**（适用性工具）
     – **Client Systems Management**（客户端系统管理）
     – **Connections Client Systems Management**（Connections Client 系统管理）
  d. 要查看说明文件，请单击所需的产品版本。
- 使用搜索引擎：

  – 在搜索框中键入说明文件的名称和版本。

2

安装和设置 CMC

本节介绍如何安装 CMC 硬件、建立对 CMC 的访问、配置您的管理环境以使用 CMC 并引导您完成配置 CMC 的任务：

- 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。

安装 CMC 硬件

CMC 已在机箱上预安装，因此无需安装。

设置机箱一览表

使用以下任务可准确设置机箱：

1. CMC 与使用浏览器的管理站必须位于同一网络，即管理网络。将以太网网络电缆从标记为 **GB1** 的端口连接至管理网络。

   管理网络：CMC 和 iDRAC（位于每个服务器上）以及交换机 I/O 模块的网络管理端口连接到 PowerEdge FX2/FX2s 机箱中的公用内部网络。这可以让管理网络与服务器数据网络相隔离。

   应用程序网络：通过与 I/O 模块 (IOM) 的网络连接实现对受管服务器的访问。这使应用程序网络能够与管理网络相互隔离。隔离此流量对于实现机箱管理的不间断访问十分重要。

   注: 建议将机箱管理与数据网络相隔离。由于数据网络上可能存在流量，因此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 已启动并运行，CMC 也会将其显示为脱机，这又会导致其他意料之外的行为。如果以物理方式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。

2. STK/Gb2 端口也可用于 CMC NIC 故障转移。请确保该 CMC 设置从默认的**堆栈**更改为**冗余**以实现 NIC 故障转移。有关更多信息，请参阅配置管理端口 2。

   小心: 如果 CMC 设置没有从默认的堆栈更改为冗余来实施 NIC 故障转移，则将 STK/Gb2 端口连接到管理网络会出现无法预测的结果。在默认的堆栈模式下，将 Gb1 和 STK/Gb2 端口连接到相同的网络（广播域）会引发广播风暴。如果将 CMC 设置更改为冗余模式，但堆叠模式中的机箱间采用菊花链式连接，还会引发广播风暴。确保布线模式符合针对预期用途的 CMC 设置。

3. 在机箱中安装 I/O 模块，并将网络电缆连接到 I/O 模块。
4. 在机箱中插入服务器。
5. 将机箱与电源相连。
6. 要打开机箱电源，请按电源按钮，或者在完成任务 6 后使用以下界面。使用 Web 界面，转至**机箱概览 → 电源 → 控制 → 电源控制选项 → 打开系统电源**。单击**应用**。

也可以使用命令行界面打开机箱电源，使用 `racadm chassisaction powerup` 命令可完成此操作。

注: 不要打开服务器电源。

7. 默认 CMC 网络配置为“静态”，且 CMC IP 地址为 192.168.0.120。要将网络配置更改为 DHCP，请将串行电缆连接到 CMC 上的串行端口。有关串行连接的更多信息，请参阅从管理站使用远程访问软件部分中的串行接口/协议设置。

   建立串行连接后登录，然后使用命令 `racadm setniccfg —d` 将网络配置更改为 DHCP。CMC 大约需要 30 到 60 秒来从 DHCP 服务器获取 IP 地址。

   要查看 DHCP 分配的 CMC IP 地址，请使用以下方法之一：

   - 要使用与 CMC 之间的串行连接查看 CMC IP 地址，请执行以下步骤：
     1. 将串行零调制解调器电缆的一端连接到机箱背面的串行连接器。
     2. 将电缆的另一端连接到管理系统的串行端口。
     3. 在建立连接后，使用默认根帐户凭据登录 CMC。
     4. 运行 `racadm getniccfg` 命令。
        在显示的输出中，搜索**当前 IP 地址**。
   - 要通过使用 KVM 连接服务器来查看 CMC IP 地址，请执行以下步骤：
     1. 使用 KVM 连接到机箱中的某个服务器。

        注: 有关如何通过 KVM 连接到服务器的更多详情，请参阅使用 KVM 访问服务器。
     2. 打开服务器电源。
     3. 确保服务器设置为在统一可扩展固件接口 (UEFI) 模式下引导。
     4. 按 F2 访问“系统设置”页面。
     5. 在**系统设置**页面中，单击 **iDRAC 设置 → 系统摘要**。

        CMC IP 地址显示在 **Chassis Management Controller** 部分中。

        有关 iDRAC GUI 中的 **iDRAC 设置**页面的更多信息，请参阅 *Dell Integrated Dell Remote Access Controller (iDRAC) User’s Guide*（Dell Integrated Dell Remote Access Controller (iDRAC) 用户指南）。
8. 使用 Web 浏览器通过键入默认根帐户凭据连接到 CMC IP 地址。
9. 根据需要配置 iDRAC 网络设置。默认情况下，iDRAC LAN 已启用并配置了静态 IP。要使用**企业版许可证**确定默认静态 IP 地址，请转至**服务器概览 → 设置 → iDRAC**。也可以使用 **Express 许可证**确定静态 IP 地址。转至 **服务器概览 → 服务器插槽 → 设置 → iDRAC**。
10. 在 CMC Web 界面中为 IO 模块提供外部管理 IP 地址（如果适用）。可以通过依次单击 **I/O 模块概览**和**设置**来获取 IP 地址。
11. 通过 Web 界面使用默认根帐户凭据连接到每个 iDRAC，以完成所有必需配置。
12. 打开服务器电源并安装操作系统。

注: 默认的本地帐户凭据为 root（用户名）和 calvin（用户密码）。

从管理站使用远程访问软件

您可从管理站使用多种远程访问软件访问 CMC。下面列出了您的操作系统提供的 Dell 远程访问软件。

接口/协议	说明
串行	CMC 支持串行文本控制台，可使用任意终端仿真软件启动该控制台。下面例举了几个可用于连接到 CMC 的终端仿真软件。 • Linux Minicom • Hilgraeve 针对 Windows 的超级终端 将串行零调制解调器电缆（两端均存在）的一端连接到机箱背面的串行连接器。将电缆的另一端连接到管理站串行端口。有关连接电缆的更多信息，请参见机箱概览部分的机箱背面板。 使用以下参数配置终端仿真软件： • 波特率：115200 • 端口：COM1 • 数据：8 位 • 奇偶校验：无 • 停止位：1 位 • 硬件流控制：是 • 软件流控制：否
远程 RACADM CLI	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，该选项需要 CMC IP、用户名和密码。 要从管理站使用远程 RACADM，请使用系统随附的 Dell Systems Management Tools and Documentation DVD 安装远程 RACADM。有关远程 RACADM 的更多信息
Web 界面	使用图形用户界面提供对 CMC 的远程访问。Web 界面内置于 CMC 固件中，可在管理站上使用受支持的 Web 浏览器通过 NIC 接口访问该界面。有关受支持 Web 浏览器的列表，请参阅 **dell.com/support/manuals** 上的 Dell System Software Support Matrix（Dell 系统软件支持值表）中的**支持的浏览器**部分。
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。 **注:** Telnet 并非安全协议，并且默认为禁用。Telnet 以明文形式传输所有数据，包括密码。
SNMP	简单网络管理协议 (SNMP) 是用于管理网络设备的一组协议定义。CMC 提供对 SNMP 的访问，允许您使用 SNMP 工具来查询 CMC 中的系统管理信息。可以从 CMC Web 界面下载 CMC MIB 文件：转到**机箱概览 → 网络 → 服务 → SNMP**。有关 CMC MIB 的更多信息，请参阅 *Dell OpenManage SNMP Reference Guide*（Dell OpenManage SNMP 参考指南）。

以下示例显示如何使用 `net-snmp snmpget` 命令从 CMC 获取机箱服务标签。

```
snmpget -v 1 -c <CMC community name>
<CMC IP address>.
1.3.6.1.4.1.674.10892.2.1.1.6.0
```

WS-MAN

WSMAN 服务基于 Web 管理服务 (WSMAN) 协议执行一对多系统管理任务。您可以通过 WS-MAN 客户端（如 WinRM 客户端 (Windows) 或 OpenWSMAN 客户端 (Linux)）来使用 LC 远程服务功能。也可以使用 Power Shell 和 Python 编写 WS-MAN 界面脚本。

WSMAN 是用于系统管理的基于简单对象访问协议 (SOAP) 的协议。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 WS-MAN 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。

注: 用于实现传输安全性的 SSL 端口与 CMC HTTPS 端口相同。

有关更多信息，请参阅：

- MOF 和配置文件 - **delltechcenter.com/page/DCIM.Library**
- DTMF 网站 **-** dmtf.org/standards/profiles/
- WS-MAN 发行说明文件。
- **www.wbemsolutions.com/ws_management.html**
- DMTF WS-Management 规范：**www.dmtf.org/standards/wbem/wsman**

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。

使用其他系统管理工具启动 CMC

您还可以从 Dell Server Administrator 或 Dell OpenManage Essentials 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 主页的左侧窗格中，单击**系统 → 主系统机箱 → Remote Access Controller**。有关更多信息，请参阅 **dell.com/support/manuals** 上的 *Dell Server Administrator User's Guide*（Dell Server Administrator 用户指南）。

远程 RACADM 安装

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 **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）。您也可以从 **support.dell.com** 下载最新版本的 Dell DRAC 工具。

在 Windows 管理站上安装远程 RACADM

如果使用的是 DVD，请运行 **<*path*>\SYSMGMT\ManagementStation\windows\DRAC\<*.msi file name*>**

如果已从 **support.dell.com** 下载软件，请执行以下操作：

1. 解压缩下载的文件，然后执行所提供的 **.msi** 文件。
   根据下载的版本，文件将命名为 DRAC.msi、RACTools.msi 或 RACTools64Bit.msi。
2. 接受许可协议，然后单击**下一步**。
3. 选择要安装的位置，然后单击**下一步**。
4. 单击**安装**。
   此时会显示安装窗口。
5. 单击**完成**。

打开管理命令提示符，键入 `racadm` 并按 **Enter**。如果查看 RACADM 帮助说明，会显示软件已正确安装。

在 Linux 管理站上安装远程 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 *ell 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，通过 `–noexec mount` 选项自动装载 DVD。该选项不允许从 DVD 运行任何可执行程序。您需要手动装载 DVD-ROM，然后运行命令。
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 FX2/FX2s RACADM Command Line Reference Guide*（适用于 Dell PowerEdge FX2/FX2s 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 管理站卸载远程 RACADM

1. 以 `root` 用户身份登录到要卸载管理站功能的系统。
2. 运行以下 rpm 查询命令以确定安装的 DRAC 工具版本：
   `rpm -qa | grep mgmtst-racadm`
3. 验证要卸载的软件包版本，通过使用 rpm `-e rpm -qa | grep mgmtst-racadm` 命令卸载该功能。

配置 Web 浏览器

您可以通过 Web 浏览器配置和管理机箱中安装的 CMC、服务器和模块。请参阅 **dell.com/support/manuals** 上的 *Dell Systems Software Support Matrix*（Dell 系统软件支持值表）中的“支持的浏览器”部分。

CMC 与使用浏览器的管理站必须位于相同的网络中，称之为*管理网络*。根据安全性要求，管理网络可以是隔离且高度安全的网络。

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

一些浏览器功能会干扰连接或影响性能，特别是在管理网络没有到 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也不例外。

注: 为解决安全性问题，Microsoft Internet Explorer 严格监测有关其 Cookie 管理的时间。为此，运行 Internet Explorer 的计算机上的时间必须与 CMC 上的时间同步。

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。

Microsoft Phishing Filter

如果在管理系统上的 Internet Explorer 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 等另一个界面时会发生这种延迟。要禁用 Phishing Filter，请执行以下操作：

1. 启动 Internet Explorer。
2. 单击工具 → **Phishing Filter**，然后单击 **Phishing Filter** 设置。
3. 选择**禁用 Phishing Filter** 项选，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，您可能会遇到**不将加密的页保存到磁盘**选项未启用的问题。

要启用**不将加密的页保存到磁盘**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. 在**安全**部分，选中**不将加密的页保存到磁盘**选项。

允许在 Internet Explorer 中播放动画

在 Web 界面之间传输文件时，文件传输图标将旋转以显示传输活动。在使用 Internet Explorer 时，您需要配置浏览器才能播放动画。

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. 转到**多媒体**部分，然后选中**播放网页中的动画**选项。

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

您可以设置机箱在数据中心的位置，以及用于在网络上标识机箱的机箱名称（默认名称为 **cmc-“服务标签”**）。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 界面设置机箱位置和机箱名称，请执行以下操作：

1. 在左侧窗格中，转至**机箱概览**，然后单击**设置**。
2. 在**常规机箱设置**页面中，键入位置属性和机箱名称。有关设置机箱属性的更多信息，请参阅 *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，请参阅 **setsysinfo** 和 **setchassisname** 命令。

例如：`racadm setsysinfo -c chassisname` 或 `racadm setsysinfo -c chassislocation`

有关更多信息，请参阅 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 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

要设置 CMC 上的日期和时间，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **设置** → **日期/时间**。
2. 要将日期和时间与网络时间协议 (NTP) 服务器同步，请在**日期/时间**页上，选择**启用 NTP** 并最多指定三台 NTP 服务器。要手动设置日期和时间，请清除**启用 NTP** 选项，然后编辑**日期和时间**字段。
3. 从下拉菜单中选择**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 **dell.com/support/manuals** 上的 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 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。

例如：`racadm setractime -l 20140207111030`。

使用 `racadm getractime` 命令读取日期和时间。

配置 LED 以识别机箱上的组件

可以让组件（机箱、服务器和 I/O 模块）的 LED 闪烁以识别机箱上的组件。

注: 要修改这些设置，您必须具有 CMC 上的**调试管理员**权限。

使用 CMC Web 界面配置 LED 闪烁

要为一个、多个或所有组件 LED 启用闪烁，请执行以下操作：

- 在左侧窗格中，转至下列任意页面：
  - **机箱概览 → 故障排除**。
  - **机箱概览 → 机箱控制器 → 故障排除**。
  - **机箱概览 → 服务器概览 → 故障排除**。

    注: 只能在此页上选择服务器。

要启用组件 LED 闪烁，请选中相应的组件，然后单击**闪烁**。要禁用组件 LED 闪烁，请取消选中服务器，然后单击**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>`* 指定您要配置其 LED 的模块。配置选项包括：

- `server-`*n*（其中 *n* = 1-4 [PowerEdge FM120x4]）和 `server-`*nx*（其中 *n* = 1–4，*x* = a 至 b [PowerEdge FC630]）。
- `switch-1`
- `cmc-active`

而 *`<ledState>`* 指定 LED 是否应该闪烁。配置选项包括：

- 0 - 不闪烁（默认）
- 1 - 闪烁

配置 CMC 属性

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

配置前面板

可以使用前面板页面配置：

- 电源按钮
- KVM

配置电源按钮

要配置机箱电源按钮，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **前面板** → **设置**。
2. 在**前面板配置**页面的**电源按钮配置**部分下，选择**禁用机箱电源按钮**选项，然后单击**应用**。
   机箱电源按钮即被禁用。

使用 KVM 访问服务器

要从 Web 界面将服务器映射到 KVM，请执行以下操作：

1. 将显示器连接到视频连接器，将键盘连接到位于机箱正面的 USB 连接器。
2. 在左侧窗格中，单击**机箱概览** → **前面板** → **设置**。
3. 在**前面板配置**页面中的 **KVM 配置**部分下，选择**启用 KVM 映射**选项。
4. 在**前面板配置**页面中的 **KVM 配置**部分下，从**已映射 KVM** 选项的下拉列表中选择所需的服务器。
5. 单击**应用**。

要使用 racadm 将服务器映射到 KVM，请使用 `racadm config -g cfgKVMInfo -o cfgKvmMapping` *`[server slot #]`* 命令。

要使用 racadm 查看当前的 KVM 映射，请使用 `racadm getconfig -g cfgKVMInfo`。

配置服务器上的机箱管理模式

此功能可用于管理和监测机箱共享组件和机箱节点（如机架式服务器）。启用此功能时，可以通过以下组件管理和监测机箱风扇、电源设备、温度传感器以及更新和配置 CMC 固件：

- iDRAC
- 刀片服务器操作系统
- Lifecycle Controller

使用 CMC Web 界面配置服务器上的机箱管理

要启用服务器上的机箱管理模式：

1. 在左侧窗格中，单击**机箱概览** → **设置** → **常规**。
2. 在**常规机箱设置**页面中，从**服务器上的机箱管理模式**下拉菜单中选择以下模式之一：
   - **无** - 此模式不允许通过 iDRAC、OS 或 Lifecycle Controller 监测或管理机箱组件。
   - **监测** - 此模式允许通过 iDRAC、OS 或 Lifecycle Controller 监测机箱组件，但无法执行任何固件更新。
   - **管理和监测** - 此模式允许通过 iDRAC、OS 或 Lifecycle Controller 监测机箱组件和使用 DUP 更新 CMC 固件。

使用 RACADM 配置服务器上的机箱管理模式

要使用 RACADM 启用服务器上的机箱管理，请使用以下命令：

- 要禁用服务器上的机箱管理模式，请使用以下命令：

  ```
  racadm config –g cfgRacTuning – cfgRacTuneChassisMgmtAtServer 0
  ```

- 要将服务器上的机箱管理模式更改为监测，请使用以下命令：

  ```
  racadm config –g cfgRacTuning – cfgRacTuneChassisMgmtAtServer 1
  ```

- 要将服务器上的机箱管理模式更改为管理和监测，请使用以下命令：

  ```
  racadm config –g cfgRacTuning – cfgRacTuneChassisMgmtAtServer 2
  ```

3

登录 CMC

您可以作为 CMC 本地用户、Microsoft Active Directory 用户或 LDAP 用户登录 CMC。也可以使用单点登录或智能卡登录。

配置通过 SSH 的公共密钥验证

最多可以配置 6 个公共密钥，通过 SSH 接口与服务用户名一起使用。添加或删除公共密钥之前，务必使用 `view` 命令查看已设置了哪些密钥，这样就不会无意中覆盖或删除密钥。服务用户名是特殊用户帐户，可在通过 SSH 访问 CMC 时使用。在设置和正确使用 SSH 上的 PKA 时，无需输入用户名或密码即可登录到 CMC。这对于设置执行各种功能的自动化脚本非常有用。

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，确保现有密钥没有位于添加新密钥的索引处。CMC 在添加新密钥之前不检查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 PowerEdge FX2/FX2s Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller 命令行参考指南）。

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 Key Generator 为运行 Windows 的客户端创建基本密钥，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 或 SSH-2 DSA。
2. 输入密钥的位数。RSA 密钥大小应介于 768 和 4096 位之间，而建议的 DSA 密钥大小为 1024 位。

注:

- 如果您添加的密钥小于 768 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会失败。
- 对于大于 2048 位的 DSA 密钥，使用以下 racadm 命令。CMC 接受的 RSA 密钥的最大密钥强度为 4096 位，但建议的密钥强度为 1024 位。

```
racadm -r 192.168.8.14 -u <default root account username> -p <default
root account password> sshpkauth -i svcacct -k 1 -p 0xfff -f
dsa_2048.pub
```

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 1024 –C testing
```

其中，

–t 必须为 dsa 或 rsa。

–b 选项指定介于 768 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。

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，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 `The XML page cannot be displayed` 错误，则必须禁用代理才能继续。

要访问 CMC Web 界面，请执行以下操作：

1. 打开您的系统支持的 Web 浏览器。

   有关支持的 Web 浏览器的最新信息，请参阅 **dell.com/support/manuals** 上的 *Dell Systems Software Support Matrix*（Dell 系统软件支持值表）。
2. 在**地址**字段中键入下面的 URL，然后按 <Enter>：
   - 要使用 IPv4 地址访问 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>`
   - 要使用 IPv6 地址访问 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>`，其中 *<CMC IP address>* 是 CMC 的 IP 地址，*<port number>* 是 HTTPS 端口号。

此时将显示 **CMC 登录**页面。

注: 使用 IPv6 时，必须用方括号 ([ ]) 将 CMC IP 地址括起来。

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

要登录 CMC，您必须拥有包含**登录 CMC** 权限的 CMC 帐户。默认根帐户是 CMC 附带的默认管理帐户。

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。

注: 如果启用了证书验证，则应提供系统的 FQDN。如果在启用证书验证的同时提供域控制器的 IP 地址，则登录会失败。

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。

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>

     注: CMC 用户名只能包含字母数字字符和某些特殊字符。不支持 @ 符号和以下特殊字符：
     – 正斜杠 (/)
     – 反斜杠 (/)
     – 分号 (;)
     – 后引号 (`)
     – 双引号 (“)
   - Active Directory 用户名：<domain>\<user name>、<domain>/<user name> 或 <user>@<domain>。
   - LDAP 用户名：<user name>

   注: 此字段区分大小写。
2. 在**密码**字段中，键入用户密码。

   注: 对于 Active Directory 用户，**用户名**字段区分大小写。
3. 在**域**字段中，从下拉菜单中选择所需域。
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段。默认值为 **Web 服务空闲超时**。
5. 单击**确定**。

   您便以所需的用户权限登录 CMC。

   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。

使用智能卡登录 CMC

要使用此功能，必须具有企业版许可证。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。

使用智能卡以 Active Directory 用户身份登录之前，请确保：

- 将受信任的证书颁发机构 (CA) 证书（证书颁发机构签发的 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。

要使用智能卡以 Active Directory 用户身份登录 CMC，请执行以下操作：

1. 使用链接 `https://<cmcname.domain-name>` 登录 CMC。
   此时将显示 **CMC 登录**页面，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 网页，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 对话框。
3. 键入 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。否则，需要使用相应的用户名和密码进行登录。

   您已使用 Active Directory 凭据登录到 CMC。

使用单点登录来登录 CMC

在启用单点登录 (SSO) 时，您可以登录到 CMC 而无需提供域用户验证凭据，如用户名和密码。要使用此功能，您必须有企业版许可证。

注: 您不能使用 IP 地址登录 SSO。Kerberos 会根据完全限定域名 (FQDN) 验证您的凭据。

在使用 SSO 登录到 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。

要使用 SSO 登录 CMC，请执行以骤操作：

1. 使用网络帐户登录客户端系统。
2. 通过 `https://<cmcname.domain-name>` 访问 CMC Web 界面
   例如，cmc-6G2WXF1.cmcad.lab，其中 cmc-6G2WXF1 是 cmcname，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，浏览器将重定向到正常的 CMC 登录页。

注: 如果您不再登录 Active Directory 域并在使用 Internet Explorer 以外的浏览器，则登录将失败，并且浏览器仅显示空白页。

使用串行、Telnet 或 SSH 控制台登录 CMC

可以通过串行、Telnet 或 SSH 连接登录 CMC。

配置完管理站终端仿真软件后，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。

使用公共密钥验证登录 CMC

您可以通过 SSH 登录 CMC 而无需输入密码。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，因此该命令行选项的行为与远程 RACADM 类似。

在通过 SSH 登录 CMC 之前，确保上载了公共密钥。要使用此功能，您必须具有企业版许可证。

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，如果在创建公共密钥或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，运行 Windows 和 Linux 的客户端系统都提供相应方法来自动实现此方法。在运行 Windows 的客户端系统上，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。对于运行 Linux 的客户端系统，您可以使用 ssh 代理。有关如何设置和使用上述任一应用程序的信息，请参阅相应的产品说明文件。

多个 CMC 会话

此表列出了使用各种界面可建立的多个 CMC 会话的情况。

表. 2: 多个 CMC 会话

界面	会话数
CMC Web 界面	4
RACADM	4
Telnet	4

界面	会话数
SSH	4

4

更新固件

可以为以下各项更新固件：

- CMC
- 机箱基础结构
- I/O 模块
- PERC
- 扩展器和 HDD

您可以更新以下服务器组件的固件：

- BIOS
- FM120x4 上的 iDRAC7（第 12 代服务器）
- FC630 上的 iDRAC8（第 13 代服务器）
- Lifecycle Controller
- 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

已签名的 CMC 固件映像

CMC 固件包含签名。CMC 固件执行签名验证步骤以确保所上载的固件的真实性。仅当 CMC 验证固件映像是来自服务提供商的有效映像并且未被篡改时，固件更新过程才会成功。如果 CMC 无法验证所上载固件映像的签名，则固件更新过程会停止。此时会记录警告事件，并显示相应的错误消息。

当您尝试升级 CMC 固件版本时，CMC 固件更新过程会验证所选版本的固件映像是否包含来自服务提供商的签名。如果未找到签名或映像验证失败，则固件更新会停止。此时会记录警告事件，并显示相应的错误消息。

尝试将固件降级至较早版本时，CMC 固件更新过程会验证较早版本的固件映像是否包含来自服务提供商的签名。如果当前 CMC 固件无法识别较早版本所计算出的签名，则固件降级会停止。CMC 固件将记录警告事件，并显示相应的错误消息。

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。

建议在更新机箱的固件时，遵循以下更新顺序：

- 刀片组件固件

- CMC 固件
- 机箱基础结构固件

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：

- **机箱概览 → 更新**
- **机箱概览 → 机箱控制器 → 更新**
- **机箱概览 → 服务器概览 → 服务器组件更新**

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，或者如果 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

可以使用 `racadm getversion` 命令查看当前安装的固件版本。有关其他 RACADM 命令的更多信息，请参阅 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

更新 CMC 固件

可以使用 Web 界面或 RACADM 更新 CMC 固件。默认情况下，固件更新会保留当前的 CMC 设置。

注: 要更新 CMC 的固件，必须具备机箱配置管理员权限。

注: 如果固件映像文件不包含验证签名或包含无效或损坏的验证签名，则无法更新 CMC 固件。

注: 如果当前 CMC 固件无法识别较早版本所计算出的签名，则无法将 CMC 固件降级至该较早版本。

如果使用 Web 用户界面会话更新系统组件固件，则空闲超时（**0、60-10800**）设置必须设置为较大的值，以满足文件传输时间要求。在某些情况下，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，机箱中部分或全部风扇装置通常会全速旋转。

为避免重设期间断开其他用户的连接，请通知可能登录到 CMC 的授权用户，并查看**会话**页中的活动会话。要打开**会话**页，请单击左侧窗格中的**机箱概览**，单击**网络**，然后单击**会话**。

当从 CMC 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，请确保浏览器配置为允许动画。有关在浏览器中允许播放动画的更多信息，请参阅允许在 Internet Explorer 中播放动画。

使用 Web 界面更新 CMC 固件

要使用 CMC Web 界面更新 CMC 固件：

1. 在左侧窗格中，转至下列任意页面：
   - **机箱概览 → 更新**
   - **机箱概览 → 机箱控制器 → 更新**
2. 在**固件更新**页面的 **CMC 固件**部分，在**更新目标**列下为要更新的 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，输入固件映像文件在管理站或共享网络中的路径，或者单击**浏览**以浏览到该文件位置。CMC 固件映像文件的默认名称是 `fx2_cmc.bin`。
4. 单击**开始固件更新**，然后单击**是**。**固件更新进度**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器。文件传输时间因连接速度而异。当内部更新过程开始时，页面将自动刷新并显示固件更新计时器。有关各种固件状态的更多信息，请参阅联机帮助。
5. 对于 CMC，在固件更新过程的最后阶段，浏览器会话以及与 CMC 的连接暂时断开，因为 CMC 未连接至网络。您必须等待几分钟，在 CMC 重新启动后登录。在 CMC 重设后，新固件版本将显示在**固件更新**页面上。

   注: 固件更新后，从 Web 浏览器高速缓存中删除文件。有关清除浏览器高速缓存的说明，请参阅 Web 浏览器的联机帮助。

附加说明：

- 在文件传输期间，不要单击**刷新**图标或者导致到其他页面。
- 要取消该进程，请选择**取消文件传输和更新**选项。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: 更新过程可能需要几分钟时间。

使用 RACADM 更新 CMC 固件

要使用 RACADM 更新 CMC 固件，请使用 `fwupdate` 子命令。

例如：`racadm fwupdate` *`<options>`* *`<firmware image>`*。

有关 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller RACADM 命令行参考指南）。

使用 DUP 更新 CMC

可以使用 Dell Update Package (DUP) 通过以下组件更新 CMC 的固件版本：

- iDRAC
- 刀片服务器操作系统
- Lifecycle Controller

有关通过 iDRAC 更新 CMC 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）。

在使用 DUP 更新 CMC 之前，请确保：

- 在本地系统或网络共享上提供了 DUP 形式的 CMC 固件包。
- **服务器上的机箱管理模式**设置为**管理和监测**。

  有关更多信息，请参阅配置服务器上的机箱管理模式
- 要通过 OS 或 Lifecycle Controller 进行更新，必须启用 iDRAC 选项**启用通过 OS/USC 更新共享组件**。有关如何启用此选项的更多信息，请参阅 *Integrated Dell Remote Access Controller User's Guide*（Integrated Dell Remote Access Controller 用户指南）。

注: 使用 DUP 更新 CMC 时，在机箱下次通电开机时应用 CMC 映像中包含的 IOM 协处理器更新。

更新机箱基础结构固件

机箱基础结构更新操作可更新主板组件。

注: 在更新机箱基础结构固件之前，请先关闭机箱中的所有服务器（如果需要）。

使用 CMC Web 界面更新机箱基础结构固件

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**。
2. 在**固件更新**页上**机箱基础结构固件**部分的**更新目标**列中，选择该选项，然后单击**应用机箱基础结构固件**。
3. 在**固件更新**页上，单击**浏览**，然后选择适当的机箱基础结构固件。
4. 单击**开始固件更新**，然后单击**是**。

   固件更新进度部分提供固件更新状态信息。在上载映像文件时，页面上将显示状态指示灯。文件传输时间取决于连接速度。当内部更新过程开始时，页面会自动刷新，并显示固件更新计时器。

要遵循的附加说明：

- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- **更新状态**字段显示固件更新状态。

更新完成时，与 CMC 之间的连接会中断，因为整个机箱被重设。刷新 Web 界面以再次登录。转至**机箱概览** → **机箱控制器**。
更新完成后，将显示更新后的主板固件版本。

。

使用 RACADM 更新机箱基础结构固件

要使用 RACADM 更新机箱基础结构固件，请使用 `fwupdate` 子命令。

例如：`racadm fwupdate <options> <firmware image>`。

有关使用 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller RACADM 命令行参考指南）。

注: 要更新机箱基础结构固件，请确保服务器已关机。

更新服务器 iDRAC 固件

您可以更新 iDRAC7 或 iDRAC8 的固件。要使用此功能：

- 您必须具有企业版许可证。
- iDRAC7 固件版本必须为 1.57.57 或更高版本。
- iDRAC8 固件版本必须为 2.05.05 或更高版本。

更新固件后，iDRAC（服务器上）将重设并暂时不可用。

使用 Web 界面更新服务器 iDRAC 固件

要更新服务器中的 iDRAC 固件：

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**。

   此时将显示**固件更新**页面。

   注:
   也可以使用**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 iDRAC7 或 iDRAC8 固件，请在 **iDRAC<revision number> Enterprise 固件**部分，单击要更新其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**页面。要继续，请参阅更新服务器组件固件。

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。

Lifecycle Controller 服务在每台服务器上都提供，并且因 iDRAC 变得更简便。您可以使用 Lifecycle Controller 服务管理服务器上的组件和设备的固件。Lifecycle Controller 使用优化算法来更新固件，可有效减少重新启动次数。

Lifecycle Controller 为 iDRAC6 和更新的服务器提供模块更新支持。iDRAC 固件必须为版本 2.3 或更高，才能使用 Lifecycle Controller 更新固件。

Dell Update Package (DUP) 用于使用 Lifecycle Controller 执行固件更新。操作系统驱动程序包组件 DUP 超出此限制，并且必须使用扩展存储功能单独更新。

注: 使用基于 Lifecycle Controller 的更新功能之前，必须更新服务器固件版本。在更新服务器组件固件模块之前，还必须更新 CMC 固件。

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

- 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。
- 第 13 代服务器 - 在重新引导服务器后，当出现提示时，按 F10 键可访问 Lifecycle Controller。通过选择**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**。

使用**从文件更新**方法可以使用存储在本地系统上的 DUP 文件更新服务器组件固件。可以选择各个服务器组件以使用所需的 DUP 文件更新固件。通过使用 SD 卡存储超过 48 MB 内存大小的 DUP 文件来一次性更新大量组件。

注: 请注意下列事项：

- 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依赖性。否则，如果选择和其他组件有依赖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。

  始终采用以下顺序更新服务器组件固件模块：

  - iDRAC
  - Lifecycle Controller
  - BIOS

一键更新所有刀片或**从网络共享更新**方法允许使用存储在网络共享上的 DUP 文件更新服务器组件固件。您可以使用基于 Dell Repository Manager (DRM) 的更新功能访问存储在网络共享上的 DUP 文件，并通过单个操作更新服务器组件。您可以使用 Dell Repository Manager 设置固件 DUP 和二进制映像的自定义远程存储库，并在网络共享上共享该存储库。或者，使用 Dell Repository Manager (DRM) 检查最新的可用固件更新。Dell Repository Manager (DRM) 可确保 Dell 系统拥有最新的 BIOS、驱动程序、固件和软件。您可以基于品牌和型号或服务标签在支持站点 (**support.dell.com**) 上搜索受支持平台的最新可用更新。您可以从搜索结果中下载更新或构建存储库。有关使用 DRM 搜索最新固件更新的更多信息，请参阅 Dell 技术中心内的 http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE_PAPERS/20438118/DOWNLOAD。有关保存资源清册文件（DRM 用作创建存储库的输入）的信息，请参阅使用 CMC Web 界面保存机箱资源清册报告。

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。
- 更快、更一致的服务器组件更新方法。
- 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 复制更新内容的目录，或者在 Dell Repository Manager (DRM) 中创建并自定义所需的更新版本。您无需最新版本的 Dell Repository Manager 即可创建该目录。然而，Dell Repository Manager 版本 1.8 提供了选项来根据从机箱中的服务器导出的资源清册创建存储库（更新内容的目录）。有关使用 Dell Repository Manger 创建存储库的信息，请参阅位于 **dell.com/support/manuals** 的 *Dell Repository Manager Data Center Version 1.8 User's Guide*（Dell Repository Manager Data Center 版本 1.8 用户指南）和 *Dell Repository Manager Business Client Version 1.8 User's Guide*（Dell Repository Manager Business Client 版本 1.8 用户指南）。

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 界面中依次选择**机箱概览 → 服务器概览 → 更新 → 服务器组件更新**，来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 使用优化算法更新固件，从而减少重新引导的次数。

要使用 CMC Web 界面更新服务器组件固件，请单击**机箱概览 → 服务器概览 → 更新 → 服务器组件更新**。

如果服务器不支持 Lifecycle Controller 服务，则**组件/设备固件资源清册**部分显示**不支持**。对于最新一代的服务器，请安装 Lifecycle Controller 固件并更新 iDRAC 固件，以在服务器上启用 Lifecycle Controller 服务。对于旧版服务器，此升级不可行。

通常，Lifecycle Controller 固件通过在服务器操作系统上执行的相应安装包进行安装。对于支持的服务器，可以使用文件扩展名为 .usc 的特殊修复或安装包。该文件使您可以通过本机 iDRAC Web 浏览器界面上提供的固件更新工具安装 Lifecycle Controller 固件。

您还可以通过在服务器操作系统上执行的相应安装软件包安装 Lifecycle Controller 固件。有关更多信息，请参阅 *Dell Lifecycle Controller User's Guide*（Dell Lifecycle Controller 用户指南）。

如果服务器上禁用了 Lifecycle Controller 服务，**组件/设备固件资源清册**部分将显示：

```
Lifecycle Controller may not be enabled.
```

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
- BIOS
- 诊断程序（可选）
- OS 驱动程序包（可选）
- RAID
- NIC
- CPLD
- 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。

启用 Lifecycle Controller

在打开服务器电源时，您可以启用 Lifecycle Controller 服务：

- 对于 iDRAC 服务器，在引导控制台中，按 <F2> 键访问**系统设置**。
- 在**系统设置主菜单**页上，转到 **iDRAC 设置 → Lifecycle Controller**，单击**已启用**。转到**系统设置主菜单**页，并单击**完成**以保存设置。
- “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 和支持的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 Quick Start Guide*（Lifecycle Controller 远程服务快速入门指南）或 **delltechcenter.com/page/Lifecycle+Controller**。
- **服务器组件更新**页可以更新服务器上的各种固件组件。要使用此页面上的特性和功能，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 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**页面。
2. 在**选择更新类型**部分，选择所需的更新方式：
   - **从文件更新**
   - **从网络共享更新**

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相关信息。为了管理这些数量庞大的信息，Lifecycle Controller 提供了各种筛选机制。

注: 要使用此功能，必须具有企业版许可证。

服务器组件更新页面中的**组件/设备更新筛选器**部分允许基于组件筛选信息，并且仅适用于**按文件更新**模式。

这些筛选器支持：

- 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。
- 基于类型或型号缩小特定组件或设备类别的范围，从而自动筛选所选组件和设备。

  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。

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，则自动筛选逻辑会自动删除不匹配所选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) 与正确的服务器型号兼容。

  有时，BIOS 固件更新映像可能会与多个服务器型号兼容。此类优化将被忽略，以防此兼容性在将来不再有效。
- 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。这些设备类别包含不同的类型和型号。同样，固件更新映像 (DUP) 可能以优化形式提供，即单个 DUP 设计为可以更新指定类别的多种设备类型或型号。

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。

注: 要使用此功能，必须具有企业版许可证。

使用 CMC Web 界面查看固件资源清册

要查看固件资源清册：

1. 在左侧窗格中，单击**服务器概览**，然后单击**更新**。
2. 在**服务器组件更新**页面的**组件/设备固件资源清册**部分，查看固件资源清册详情。在此页面中，可以查看以下信息：
   - 如果服务器列为**尚未就绪**，则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。
   - 所提供的超链接可以导航到备用页面，在此可以直接只更新 iDRAC 固件。此页面仅支持 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 固件更新不依赖于 Lifecycle Controller 服务。
   - 如果组件和设备的资源清册没有反映服务器上实际安装的内容，则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。符合以下条件时会出现这种情况：
     - 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。

     为自动执行此操作，iDRAC 设置公用程序提供可通过引导控制台访问的选项：

     1. 在引导控制台中，按 <F2> 键访问**系统设置**。
     2. 在**系统设置主菜单**页面中，单击 **iDRAC 设置 → 重新启动时收集系统资源清册**，选择**已启用**，返回**系统设置主菜单**页面，然后单击**完成**保存设置。
   - 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. 3: 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。对于机箱中的 4 个可用插槽，插槽编号是顺序 ID： • 1、1a、1b、1c、1d • 2、2a、2b、2c、2d • 3、3a、3b、3c、3d • 4、4a、4b、4c、4d 此编号方案有助于识别服务器在机箱中的位置。如果占用插槽的服务器少于 4 个，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	显示服务器上组件或设备的说明。如果列宽过窄，鼠标悬停触发工具会提供说明视图。
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。

字段	说明
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为“已完成”，则服务器上的任何组件或设备的固件版本发生更改时，会自动刷新组件和设备的固件版本。当前状态旁还会显示信息图标，提供关于当前作业状态的附加信息。可通过单击或将鼠标悬停在图标上来查看此信息。
更新	单击可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 PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 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**保存资源清册报告**。
   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机箱中存在的所有刀片的更新存储库。稍后可以将此存储库导出到网络共享。固件更新的**从网络共享更新**模式使用此网络共享更新所有服务器的组件。您必须在各服务器上启用 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的位置或凭据：

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**部分。
2. 在**网络共享设置**部分，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**为选填项。如果目录文件名称更改，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

有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 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。
5. 单击**应用**将更改应用到网络共享属性。

   注:

   单击**后退**以返回到**服务器组件更新**页面。

Lifecycle Controller 作业操作

注: 要使用此功能，必须具有企业版许可证。

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 权限和登录到 iDRAC。

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，当某项操作正提交并计划通过另一个会话或上下文完成时，会尝试进行另一项操作。在这种情况下，将显示确认消息，指出这种情况并且禁止提交该操作。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，将显示确认消息，允许取消离开页面的尝试。否则，操作将被中断。中断（尤其是在更新操作中）可能会导致固件映像文件上载操作在正确完成之前终止。提交操作进行计划之后，请确保确认表明操作已成功计划的确认消息。

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. 在左侧窗格中，单击**服务器概览 → 更新**。
2. 在**服务器组件更新**页面中，单击**选择更新类型**部分中的相应类型。

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选项。
4. 选择以下选项之一：
   - **立即重新引导** - 立即重新启动服务器。
   - **下一次重新引导时** - 稍后手动重新启动服务器。
5. 单击**重新安装**。将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。

注: 要使用此功能，必须具有企业版许可证。

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. 在左侧窗格中，单击**服务器概览→ 更新**。
2. 在**服务器组件更新**页面中，单击**选择更新类型**部分中的相应类型。
3. 在**回滚版本**列中，选择您要为其回滚固件的组件或设备对应的选项。
4. 选择以下选项之一：
   - **立即重新引导** - 立即重新启动服务器。
   - **下一次重新引导时** - 稍后手动重新启动服务器。
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。

升级服务器组件固件

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。在 Lifecycle Controller 中提供了固件映像，以用于回滚操作。要使用此功能，必须具有企业版许可证。

注: 对于 iDRAC 和操作系统驱动程序包固件更新，请确保已启用**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。在 **Lifecycle Controller 作业**页面上提供了服务器上所有作业的列表。此页面允许删除单个或多个作业，或者清除服务器上的所有作业。

BIOS 更新特定于服务器的型号。有时，即使选择更新服务器上的单个网络接口控制器 (NIC) 设备的固件，更新也可能应用到该服务器上的所有 NIC 设备。这是 Lifecycle Controller 功能的固有行为，尤其是编程采用 Dell Update Package (DUP) 时。目前支持小于 85 MB 的 Dell Update Package (DUP)。

如果更新文件映像的体积过大，则作业状态会指示下载失败。如果在服务器上尝试更新多个服务器组件，则所有固件更新文件的总大小也可能超过 85 MB。在这种情况下，更新文件被截断的某个组件更新会失败。要更新服务器上的多个组件，建议首先一起更新 Lifecycle Controller 和 32 位诊断程序组件。这些操作不需要重新引导服务器，而且完成速度相对较快。完成后可以一起更新其他组件。

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。

使用 CMC Web 界面从文件升级服务器组件固件

使用“从文件更新”方法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**从文件更新**。有关更多信息，请参阅选择服务器组件固件更新类型。
3. 在**组件/设备更新筛选器**部分中，筛选组件或设备（可选）。有关更多信息，请参阅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 键快捷方式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 键以黄色高亮显示所有组件。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。这是一个 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。立即应用固件更新。
   - **下一次重新引导时** - 稍后手动重新引导服务器。在下一次重新引导后应用固件更新。

   注: 此步骤对 Lifecycle Controller 和 32 位诊断程序固件更新无效。这些设备不需要重新引导服务器。
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

使用 Dell Repository Manager 和 Dell PowerEdge FX2/FX2s 模块化机箱集成从网络共享更新服务器组件时，通过使用自定义捆绑固件来简化更新，因此可以更快、更轻松地完成部署。从网络共享更新提供了使用来自 CIFS 或 NFS 的单个目录同时更新所有第 12 代服务器组件的灵活性。

这种方法提供了一种快速而简便的方式，可使用 Dell Repository Manager 以及通过 CMC Web 界面导出的机箱资源清册文件为您拥有的已连接系统构建自定义存储库。DRM 允许您创建完全自定义的存储库，其中仅包含针对特定系统配置的更新软件包。您也可以构建仅包含过时设备的更新的存储库，或包含所有设备的更新的基准存储库。您也可以根据所需的更新模式，创建用于 Linux 或 Windows 的更新捆绑包。DRM 允许将存储库保存到 CIFS 或 NFS 共享。使用 CMC Web 界面可以配置共享的凭据和位置详细信息。使用 CMC Web 界面还可以执行单个服务器或多个服务器的服务器组件更新。

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，需要满足以下前提条件：

- 服务器必须具有 iDRAC 企业版许可证。
- 必须在服务器上启用 Lifecycle Controller。
- 必须在系统上安装 Dell Repository Manager 1.8 或更高版本。
- 您必须具有 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，选择**从网络共享更新**。有关更多信息，请参阅"选择服务器组件固件更新类型"。
3. 如果网络共享未连接，则为机箱配置网络共享。要配置或编辑网络共享详细信息，请在"网络共享属性"表中单击**编辑**。有关更多信息，请参阅"使用 CMC Web 界面配置网络共享"。
4. 单击**保存资源清册报告**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 文件即会保存在外部系统上。Dell Repository Manager 使用 *inventory.xml* 文件创建自定义更新捆绑包。此存储库存储在由 CMC 配置的 CIFS 或 NFS 共享中。有关使用 Dell Repository Manger 创建存储库的信息，请参阅位于 **dell.com/support/manuals** 的 *Dell Repository Manager Data Center Version 1.8 User's Guide*（Dell Repository Manager Data Center 版本 1.8 用户指南）和 *Dell Repository Manager Business Client Version 1.8 User's Guide*（Dell Repository Manager Business Client 版本 1.8 用户指南）。
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。

   注: 单击某个插槽的**折叠**可折叠该特定插槽的组件和设备固件详细信息。或者，要再次查看所有详细信息，请单击**展开**。
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。

删除计划的服务器组件固件作业

注: 要使用此功能，必须具有企业版许可证。

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. 在左侧窗格中，单击**服务器概览**，然后单击**更新**。
2. 在**服务器组件更新**页面中，筛选组件或设备（可选）。
3. 在**作业状态**列中，如果作业状态旁边显示复选框，则表示 Lifecycle Controller 作业正在进行并且当前处于所指示的状态。可选择该作业进行作业删除操作。
4. 单击**删除作业**。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 界面进行更新，例如 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 *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide*（Dell Integrated Dell Remote Access Controller (iDRAC) 用户指南）。

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：

- CMC
- 所有服务器和单个服务器
- IO 模块
- 风扇
- 电源设备 (PSU)
- 温度传感器
- PCIe 设备

查看机箱和组件摘要

在登录 CMC Web 界面后，**机箱运行状况**页面会显示机箱及其组件的运行状况。该页面会显示机箱及其组件的图形视图。该视图动态更新，而且组件子图形覆盖标记和文本提示会自动更改以反映当前状态。

要查看机箱运行状况，请单击**机箱概览**。系统会显示机箱、CMC、服务器模块、IO 模块 (IOM)、风扇、电源设备装置 (PSU) 和 PCIe 设备的整体运行状况。单击每个组件可显示该组件的详细信息。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 *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide*（Dell Integrated Dell Remote Access Controller (iDRAC) 用户指南）。

如果将您的机箱配置为组主机箱，则在登录后显示**组运行状况**页面。该页面显示机箱级信息和警报。将显示所有活动、严重和非严重警报。

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 KVM 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。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。

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 - 提供导航至常用页面以及常用操作的链接。只有适用于所选组件的链接才会在此部分显示。

下表列出了 Web 界面中的**机箱运行状况**页面上显示的组件属性和信息。

组件	运行状况和性能属性	属性	快速链接
CMC	• 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 • 服务标签 • 主机名 • iDRAC • CPLD • BIOS • 操作系统 • CPU 信息 • 总系统内存	• 服务器状态 • 启动远程控制台 • 启动 iDRAC GUI • 关闭服务器 • 正常关机 • 远程文件共享 • 部署 iDRAC 网络 • 服务器组件更新 **注:** 仅当服务器电源状态为“打开”时，才会显示“关闭服务器”和“正常关机”的快速链接。如果服务器电源状态为“关闭”，则会显示“打开服务器”的快速链接。
电源设备	电源状态	容量	• 电源设备状况 • 功耗 • 系统预算
PCIe 设备	• 已安装 • 已分配	• 型号 • 映射 • 厂商 ID • 设备 ID • 插槽类型 • 模块类型 • 结构 • 电源状态	• PCIe 状况 • PCIe 设置
风扇	• 速度 • PWM（最大值的百分比） • 风扇补偿	• 警告阈值 • 严重阈值	• 风扇状况 • 风扇配置
IOM 插槽	• 电源状态 • 角色	• 型号 • 服务标签	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. 在左侧窗格中的**服务器概览**树节点下，所有服务器（SLOT-01 至 SLOT-04）将显示在服务器列表中。如果插槽中不存在服务器，则图形中相应的图像将以灰色显示。
2. 将光标悬停在服务器的插槽名称或插槽编号上，工具提示会显示服务器的型号名称和服务标签（如果可用）。

查看机箱摘要

要查看机箱摘要信息，请在左侧窗格中单击**机箱概览** → **属性** → **摘要**。

此时将显示**机箱摘要**页面。有关此页面的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

查看机箱控制器信息和状态

要查看机箱控制器的信息和状态，请在 CMC Web 界面中单击**机箱概览** → **机箱控制器**。

此时将显示**机箱控制器状态**页面。有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

查看所有服务器的信息和运行状况

要查看所有服务器的运行状况，请执行以下任一操作：

- 单击**机箱概览**。**机箱运行状况**页面显示机箱中安装的所有服务器的图形概览。服务器运行状况由服务器子图形的覆盖标记指示。有关机箱运行状况的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。
- 单击**机箱概览** → **服务器概览**。**服务器状态**页面提供机箱中的服务器概览。有关更多信息，请参阅*联机帮助*。

查看 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. 单击**机箱概览**。

   此时会显示**机箱运行状况**页面。左侧窗格中的图形显示机箱的背面视图、正面视图和顶部视图，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。将光标移到各个 IOM 子图形上方，文本提示将提供有关该 IOM 的附加信息。单击 IOM 子图形可在右侧窗格中查看 IOM 信息。
2. 转到**机箱概览** → **I/O 模块概览**。

   I/O 模块状态页面提供与机箱关联的 IOM 的概览。有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

查看风扇的信息和运行状况

CMC 可根据系统事件来增减风扇速度，从而控制机箱风扇的速度。可以使用三种模式运行风扇，如低、中和高（风扇补偿）。有关配置风扇的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

要通过使用 RACADM 命令设置风扇的属性，请在 CLI 界面键入以下命令：

```
racadm fanoffset [-s <off|low|medium|high>]
```

注: CMC 监测机箱中的温度传感器，并根据需要自动调节风扇速度。使用此命令进行覆盖时，CMC 将始终以所选速度运行风扇，即使机箱不需要风扇以该速度运行。但是，可以通过 racadm `fanoffset` 命令进行覆盖以维持最低风扇速度。

有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller RACADM 命令行参考指南）。

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。
- 风扇停止转动。
- 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全速旋转。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. 转到**机箱概览**。

   此时会显示**机箱运行状况**页面。机箱图形的右上部分提供机箱的左上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上方，文本提示将提供有关风扇的附加信息。单击风扇子图形可在右侧窗格中查看风扇信息。
2. 转到**机箱概览** → **风扇**。

   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 (RPM) 为单位）和阈值。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。

   注: 当两个风扇都不在插槽中或者一个风扇低速旋转时，将显示以下消息：

   ```
   Fan <number> is less than the lower critical threshold.
   ```

   有关更多信息，请参阅*联机帮助*。

配置风扇

风扇偏移 - 此功能允许增加输送给 PCIe 卡插槽的风量。例如，在使用比平时需要更大冷却量的大功率或自定义 PCIe 卡时，就需要用到风扇偏移。风扇偏移功能包含“关”、“低”、“中”和“高”选项。这些设置分别对应于最高速度的 20%、50% 和 100% 风扇速度偏移量（增加）。每个选项还有最低速度设置，其中 35% 对应于“低”，65% 对应于“中”，100% 对应于“高”。

例如，将风扇偏移设置为“中”，风扇的转速将比最高速度增加 50%。这一增加值是指高出系统已经基于安装的硬件配置冷却而设置的速度。

在启用“风扇偏移”的任一选项时，功耗都会增加。设置“低”偏移时，系统响声会加大，设置“中”偏移时，系统响声会明显加大，设置“高”偏移时，系统响声会显著加大。未启用“风扇偏移”选项时，风扇速度将降低到系统冷却安装的硬件配置所需的默认速度。

要设置偏移功能，请转到**机箱概览** → **风扇** → **设置**。在**高级风扇配置**页上，从与**风扇偏移**对应的**值**下拉菜单中进行适当选择。

有关“风扇偏移”功能的更多信息，请参阅*联机帮助*。

要通过使用 RACADM 命令设置这些功能，请使用以下命令：

```
racadm fanoffset [-s <off|low|medium|high>]
```

查看前面板属性

要查看前面板属性，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **前面板**。
2. 在**属性**页上，您可以查看以下信息：
    - **电源按钮属性**
    - **KVM 属性**
    - **前面板指示灯**

查看 KVM 信息和运行状况

要查看与机箱关联的 KVM 的运行状况，请执行以下任一操作：

单击**机箱概览** → **前面板**。

在**状态**页面的 **KVM 属性**部分，可以查看与机箱关联的 KVM 的状态和属性。有关更多信息，请参阅*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：

在左侧窗格中，单击**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*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 环境温度探测器超过阈值，机箱的风扇速度会提高。

6

配置 CMC

使用 Chassis Management Controller 可以配置属性、设置用户和警报，以执行远程管理任务。

在开始配置 CMC 之前，必须首先配置 CMC 网络设置，以允许从远程管理 CMC。该初始配置分配 TCP/IP 联网参数，以允许访问 CMC。

可以使用 Web 界面配置 CMC，或设置对 CMC RACADM 的初始访问。

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，可以执行以下操作：

- 根据需要修改网络设置。
- 配置访问 CMC 的界面。
- 根据需要设置机箱组。
- 配置服务器、I/O 模块或前面板。
- 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。
- 根据需要设置功率上限策略。

注: 在两种 CMC 界面（GUI 和 CLI）的属性字符串中，不能使用以下字符：

- &#
- < 和 >
- ;（分号）

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。默认禁用此功能。

可以启用 DHCP 以自动从 DHCP 服务器获取 IP 地址。

启用 CMC 网络接口

若要为 IPv4 和 IPv6 启用或禁用 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：

- 禁用网络接口访问带外机箱管理，包括 iDRAC 和 IOM 管理。
- 禁止下行链路状态检测。

  要仅禁用 CMC 网络访问，请同时禁用 CMC IPv4 和 CMC IPv6。

注: 默认情况下启用 CMC NIC。

要启用或禁用 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。

要启用或禁用 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。

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，DHCP 已禁用。要启用 DHCP 并使用网络上的 DHCP 服务器分配 iDRAC 或 CMC IPv4 地址、子网掩码和网关，请键入：

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

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>
```

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。

要启用 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 cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

要启用 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 1
```

设置静态 DNS IP 地址

注: 只有在禁用 DNS 地址 DCHP 功能的情况下，静态 DNS IP 地址设置才有效。

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>
```

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。

如果在启动时启用 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 (STP)，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，IPv6 连接会在一段时间内受限，直到 IPv6 路由器无偿发送路由器广告。

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. 在左侧窗格中，单击**机箱概览**，然后单击**网络**。**网络配置**页面将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*联机帮助*。
3. 单击各个部分的**应用更改**以应用这些设置。

使用 RACADM 查看和修改 CMC 网络 LAN 设置

要查看 IPv4 设置，请使用对象 `cfgCurrentLanNetworking` 与以下子命令：

- `getniccfg`
- `getconfig`

要查看 IPv6 设置，请使用 `cfgIpv6LanNetworking` 与 `getconfig` 子命令。

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 PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller RACADM 命令行参考指南）。

配置 DNS 设置（IPv4 和 IPv6）

- **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 名称** - 默认情况下，DNS 服务器上的 CMC 名称为 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*> 是由最多 63 个字母数字字符和连字符组成的字符串。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少于或等于 63 个字符。
- **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*> 是由最多 254 个字母数字字符和连字符组成的字符串。例如：p45、a-tz-1、r-id-001。

配置自动协商、双工模式和网络速度（IPv4 和 IPv6）

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）

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

其中：

<*speed*> 是 10 或 100（默认值）。

配置管理端口 2

CMC 上的第二个网络端口可用于以菊花链式连接 CMC 以减少电缆数量，或者作为故障转移网络操作的冗余端口。**管理端口 2** 可以连接到架顶式 (TOR) 交换机或另一个交换机。不需要将两个 CMC NIC 端口连接到同一子网。

在连接 CMC 以实现管理网络端口冗余之前，必须先针对此操作实际配置 CMC。在部署时，CMC 必须使用标准单一网络连接，在部署后可以添加第二个冗余连接。

注: 当管理端口 2 设置为冗余但已进行堆叠电缆连接，则下游 CMC（距离 TOR 交换机更远）将无法拥有网络链路。

注: 当管理端口 2 设置为堆叠但已将电缆连接到冗余（至 TOR 交换机的两个连接），则路由环路可能导致网络风暴。

要指定冗余操作，请使用 `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 1` 命令。

要指定堆叠操作，请使用 `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 0` 命令。

默认情况下，管理端口 2 设置为堆叠。

使用 CMC Web 界面配置管理端口 2

要使用 CMC Web 界面配置管理端口：

1. 在左侧窗格中，单击**机箱概览** → **网络**，然后单击**网络**选项卡。
2. 在**网络配置**页面中的**常规设置**部分，在**管理端口 2** 旁边选择**冗余**或**堆叠**。
3. 单击**应用更改**。
   - 当管理端口 2 设置为冗余但已将电缆连接到堆叠中，则下游 CMC（距离架顶式交换机更远）无法拥有网络链路。
   - 当管理端口 2 设置为堆叠但已将电缆连接到冗余（至 TOR 交换机的两个连接），则路由环路可能导致网络风暴。

使用 RACADM 配置管理端口 2

要指定冗余操作，请使用 `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 1` 命令。

要指定堆叠操作，请使用 `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 0` 命令。

默认情况下，管理端口 2 设置为堆叠。

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。禁用 Web 服务器也会禁用远程 RACADM。
- SSH - 支持通过固件 RACADM 访问 CMC。
- Telnet - 支持通过固件 RACADM 访问 CMC
- 远程 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。要使用此功能，必须具有企业版许可证。

注: 在修改 SSH、Telnet、HTTP 或 HTTPS 的 CMC 服务端口号时，应避免使用操作系统服务的常用端口（如端口 111）。请参阅位于 http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml 的 Internet 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 接受来自客户端的加密数据，或者向客户端传输加密数据。Web 服务器包含 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。Web 界面和远程 RACADM CLI 工具需要该服务与 CMC 进行通信。

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，您必须具有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相应的目标。

注: 由于在转发日志条目时使用 UDP 进行网络传输，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被成功接收的反馈。

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 PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 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 界面启用或修复可移动闪存介质，请执行以下操作：

1. 在左侧窗格中，转至**机箱概览**，然后单击**机箱控制器 → 闪存介质**。
2. 在**可移动闪存介质**页面中，根据需要从下拉菜单中选择以下选项之一：
   - **修复活动控制器介质**
   - **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 for Dell PowerEdge FX2/FX2s 联机帮助*。
3. 单击**应用**以应用所选的选项。

设置机箱组

CMC 可以从一个主机箱监测多个机箱。启用机箱组时，主机箱中的 CMC 会生成主机箱和机箱组中所有成员机箱的状态的图形显示。要使用此功能，必须具有企业版许可证。

机箱组功能为：

- 显示描绘每个机箱正面和背面的图像，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。
- 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 19 个成员。此外，主机箱或成员只能加入一个组。不能将作为某个组的主机箱或成员的机箱加入到另一个组中。可以从组中删除机箱，然后再将其添加到不同组。

要使用 CMC Web 界面设置机箱组：

1. 以机箱管理员权限登录到主机箱。
2. 单击**设置 → 组管理**。
3. 在**机箱组**页面中的**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**字段中键入组名称，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**页面。左侧窗格按组名称和主机箱指示组，并且未填充的成员机箱会在左侧窗格中显示。

   注: 创建机箱组后，树结构中的**机箱概览**项被替换为主机箱的名称。

将成员添加到机箱组

设置机箱组后，通过以下步骤将成员添加到机箱组：

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: 要让 MCM 正常工作，必须在所有组成员和主机箱上使用默认 HTTPS 端口 (443)。

5. 在**用户名**字段中，输入具有该成员机箱的机箱管理员权限的用户名。
6. 在**密码**字段中键入相应的密码。
7. 另外，可选择**同步新成员与主机箱属性**以将主机箱属性推送至成员。有关将成员添加到机箱组的更多信息，请参阅同步新成员与主机箱属性。
8. 单击**应用**。
9. 完成步骤 4 至步骤 8 中的任务可添加最多 8 个成员。新成员的机箱名称显示在**成员**对话框中。

   注: 为成员输入的凭据会以安全方式传递到成员机箱，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，并且在建立初始信任关系后永远不会再次进行交换。

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. 在左侧窗格中，选择主机箱。
3. 单击**设置 → 组管理**。
4. 从**移除成员**列表中，选择要删除的成员的名称，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。

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. 在左侧窗格中选择主机箱。
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移除的所有成员通信。现在，可以将该主机箱分配为新组的主机箱或成员。

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

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. 在左侧窗格中，单击**机箱概览 → 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

可通过主机箱组页面访问成员机箱的 Web 页面、服务器远程控制台或 iDRAC 服务器的 Web 页面。如果成员设备的登录凭据与主机箱相同，则可以使用相同的凭据来访问成员设备。

注: 在多机箱管理中不支持单点登录和智能卡登录。从主机箱通过单点登录启动成员要求在主机箱和成员之间共用用户名/密码。只有 Active Directory、本地和 LDAP 用户支持使用公共用户名/密码。

要导航到成员设备：

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**。

   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**运行状况**部分所显示的机箱图像中，选择服务器。
   c. 在标记为**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。

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：

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**，在想要传播所选设置至成员机箱时，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*联机帮助*。

同步新成员与主机箱属性

您可将来自主机箱的属性应用至组中新添加的成员机箱。要同步新成员与主机箱属性，请执行以下操作：

1. 以管理员权限登录到主机箱。
2. 在树结构中选择主机箱。
3. 单击**设置** → **组管理**。
4. 向组中添加新成员时，请在**机箱组**页中选择**同步新成员与主机箱属性**。
5. 单击**应用**。成员会接收主机箱的属性。

在同步之后，机箱内几个系统的以下配置服务属性会受到影响：

表. 4: 配置服务属性

属性	导航
SNMP 配置	在左侧窗格中，单击**机箱概览** → **网络** → **服务** → **SNMP**。
机箱远程日志记录	在左侧窗格中，单击**机箱概览** → **网络** → **服务** → **远程系统日志**。
使用 LDAP 和 Active Directory 服务的用户验证	在左侧窗格中，单击**机箱概览** → **用户验证** → **目录服务**。
机箱警报	在左侧窗格中，单击**机箱概览**，然后单击**警报**。

MCM 组的刀片资源清册

组是包含 0 到 19 个机箱组成员的主机箱。**机箱组运行状况**页面显示所有成员机箱，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。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。

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，请执行以下操作：

1. 在左侧窗格中，选择**组**。
2. 在**机箱组运行状况**页面中，单击**保存资源清册报告**。将显示**文件下载**对话框，提示您打开或保存文件。
3. 单击**保存**并指定服务器模块资源清册报告的路径和文件名。

   注: 机箱组主机箱和机箱组成员机箱以及关联机箱中的服务器模块必须接通电源，才能获得最准确的服务器模块资源清册报告。

使用 RACADM 配置多个 CMC

使用 RACADM 可以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. 打开到 CMC 的 Telnet/SSH 文本控制台，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 子命令为 CMC 请求 CMC 配置并生成 **myfile.cfg** 文件。如果需要，可以重命名该文件或将其保存到另一个位置。

   可以运行 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。

分析规则

- 以井号 (#) 开始的行将视为注释。
  注释行必须在第一列中开始。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。您可能要从 racadm getconfig -f <filename>.cfg 命令生成 .cfg，然后对另一个 CMC 执行 racadm config -f <filename> .cfg 命令，而不添加转义字符。

  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。
  表示组名的起始 [字符必须从第一列开始。此组名称必须在该组中的任何对象之前指定。没有关联组名称的对象将导致错误。配置数据将组织成组，如 *RACADM Command Line Reference Guide for iDRAC and CMC*（适用于 iDRAC 和 CMC 的 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。值后的空格将忽略。值字符串内的空格保持不变。"="右侧的所有字符（例如第二个 =、#、[和] 等）都将保留原样。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 会在分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，对象定位器必须是 [ ] 对后的第一个对象。以下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未设置，则配置组不会保存为配置文件的一部分。如果需要将这些配置组克隆到其他 CMC，则在执行 `getconfig -f` 命令之前必须设置关键属性。或者，可以在运行 `getconfig -f` 命令之后手动将缺失的属性输入到配置文件中。对于所有 RACADM 索引组均如此。

  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=10.35.10.110 cfgNicGateway=10.35.10.1
```

此文件更新如下：

```
# # Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.9.143 # comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

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。

使用此文件下载公司范围的更改或使用命令 `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。

7

配置服务器

可以配置服务器的以下设置：

- 插槽名称
- iDRAC 网络设置
- DRAC VLAN 标签设置
- 第一引导设备
- 服务器 FlexAddress
- 远程文件共享
- 使用服务器克隆的 BIOS 设置

配置插槽名称

插槽名称用于标识单个服务器。当选择插槽名称时，将应用以下规则：

- 名称最多可包含 15 个非扩展 ASCII 字符（ASCII 代码为 32 至 126）。名称中允许标准字符和特殊字符。
- 插槽名称必须在机箱内唯一。各插槽不能具有相同的名称。
- 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-
  - DRAC-
  - MC-
  - Chassis
  - Housing-Left
  - Housing-Right
  - Housing-Center
- 可以使用字符串 `Server-1` 到 `Server-4`，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。但是，`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。

CMC Web 界面中的插槽名称设置始终覆盖在 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. 在左侧窗格中，转至**机箱概览 → 服务器概览 → 设置 → 插槽名称**。
2. 在**插槽名称**页面的**插槽名称**字段中编辑插槽名称。
3. 要将服务器的主机名用作插槽名称，请选择**插槽名称使用主机名**选项。如果服务器的主机名（或系统名称）可用，此选项将用该名称覆盖静态插槽名称。这要求 OMSA 代理安装在服务器上。有关 OMSA 代理的更多信息，请参阅 dell.com/support/manuals 上的 *Dell OpenManage Server Administrator User's Guide*（Dell OpenManage Server Administrator 用户指南）。
4. 要保存设置，请单击**应用**。

要还原服务器的默认插槽名称（SLOT-01 至 SLOT-4，基于服务器的插槽位置），请单击**还原默认值**。

配置 iDRAC 网络设置

要使用此功能，必须具有企业版许可证。您可以配置服务器的 iDRAC 网络配置设置。可以使用快速部署设置来配置以后要安装的服务器的默认 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）。

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。

要启用并设置 iDRAC QuickDeploy 设置，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览 → 设置 → iDRAC**。
2. 在**部署 iDRAC** 页面的 **QuickDeploy 设置**部分中，指定在下表中提到的设置。有关这些字段的更多信息，请参阅*联机帮助*。

表. 5: QuickDeploy 设置

设置	说明
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 的网络设置。指定的自动部署设置用于配置新的 iDRAC，如果已选择**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。 • **快速部署和服务器配置文件** - 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	选择此选项可在插入服务器时，更改 iDRAC 根密码以符合在 **iDRAC 根密码**字段中提供的值。
iDRAC Root 密码	选中**插入服务器时设置 iDRAC 根密码**和**启用 QuickDeploy** 选项后，此密码值会在服务器插入机

设置	说明
	箱时分配给服务器的 iDRAC 根用户密码。此密码可包含 1 到 20 个可打印（含空格）字符。
确认 iDRAC root 密码	允许您重新输入在**密码**字段中提供的密码。
启用 iDRAC LAN	启用或禁用 iDRAC LAN 信道。默认情况下，清除此选项。
启用 iDRAC IPv4	启用或禁用 iDRAC 上的 IPv4。默认情况下，选中此选项。
启用 LAN 上 iDRAC IPMI	为机箱中存在的每个 iDRAC 启用或禁用 IPMI over LAN 信道。默认情况下，选中此选项。
启用 iDRAC IPv4 DHCP	为机箱中存在的每个 iDRAC 启用或禁用 DHCP。如果启用此选项，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。要选择此选项，必须选择**启用 iDRAC IPv4** 选项。系统为 快速部署 IP 地址选项提供的两个值为 4 和 2。
保留的 QuickDeploy IP 地址	选择要为机箱中的 iDRAC 保留的 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 Quick Deploy 功能。
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。 例如，如果起始 IP 地址是 `192.168.0.250` 并且子网掩码是 `255.255.0.0`，则插槽 4c 的 QuickDeploy IP 地址是 `192.168.0.265`。如果子网掩码是 `255.255.255.0`，则将在单击**保存 QuickDeploy 设置**或**使用 QuickDeploy 设置自动填充**时显示 `QuickDeploy IP address range is not fully within QuickDeploy Subnet` 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	指定分配给机箱中所有 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。

设置	说明
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。

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时执行。

   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 传播到 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

以下表格显示了根据 FX2/FX2s 机箱中存在的底座为服务器分配 QuickDeploy IP 地址的方式：

- 机箱中的两个全宽底座：

START IP + 0 (SLOT1)
START IP + 2 (SLOT3)

- 机箱中的四个半宽底座：

  注: 要让 QuickDeploy 为底部底座分配 IP 地址，底部底座 iDRAC 的**保留的 QuickDeploy IP 地址**字段必须设置为 4。

START IP + 0 (SLOT1)	START IP + 1(SLOT2)
START IP + 2 (SLOT3)	START IP + 3 (SLOT4)

- 机箱中的八个四分之一宽底座：

START IP + 0 (SLOT1a)	START IP + 4 (SLOT1b)	START IP + 1 (SLOT1c)	START IP + 5 (SLOT1d)
START IP + 2 (SLOT3a)	START IP + 6 (SLOT3b)	START IP + 3 (SLOT3c)	START IP + 7 (SLOT3d)

- 机箱中的四个 FM120x4 底座：

STARTIP+0 (SLOT1a)	STARTIP+4 (SLOT1b)	STARTIP+8 (SLOT1c)	STARTIP+12 (SLOT1d)	STARTIP+1 (SLOT2a)	STARTIP+5 (SLOT2b)	STARTIP+9 (SLOT2c)	STARTIP+13 (SLOT2d)
STARTIP+2 (SLOT3a)	STARTIP+6 (SLOT3b)	STARTIP+10 (SLOT3c)	STARTIP+14 (SLOT3d)	STARTIP+3 (SLOT4a)	STARTIP+7 (SLOT4b)	STARTIP+11 (SLOT4c)	STARTIP+15 (SLOT4d)

- 顶部行仅包含四分之一宽底座，底部行仅包含半宽底座：

START IP + 0 (SLOT1a)	START IP + 4(SLOT1b)	START IP + 1(SLOT1c)	START IP + 5(SLOT1d)
START IP + 2 (SLOT3)		START IP + 3 (SLOT4)	

- 顶部行仅包含全宽底座，底部行仅包含半宽底座：

START IP + 0 (SLOT1)	
START IP+ 2 (SLOT3)	START IP + 3 (SLOT4)

- 顶部行包含全宽底座，底部行仅包含四分之一宽底座：

START IP + 0 (SLOT1)			
START IP + 2 (SLOT3a)	START IP+ 6 (SLOT3b)	START IP + 3(SLOT3c)	START IP + 7(SLOT3d)

修改单个服务器 iDRAC 的 iDRAC 网络设置

使用此功能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。要使用此功能，必须具有企业版许可证。

要修改 iDRAC 网络设置，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**，然后单击**设置**。在**部署 iDRAC** 页面的 **iDRAC 网络设置**部分，列出了所有已安装服务器的 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: 必须选择**启用 LAN** 选项以指定 IPv4 或 IPv6 设置。有关这些字段的信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。
3. 要将设置部署到 iDRAC，请单击**应用 iDRAC 网络设置**。对于 **QuickDeploy 设置**做出的所有更改也会保存。

   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 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，请参阅位于 dell.com/support/manuals 的 *Dell Integrated Dell Remote Access Controller (iDRAC) RACADM Command Line Reference Guide*（Dell Integrated Dell Remote Access Controller (iDRAC) RACADM 命令行参考指南）和 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 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流量。启用 VLAN 功能时，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，机箱仍然保留这些标签。

使用 Web 界面配置 iDRAC VLAN 标签设置

要为服务器配置 VLAN，请执行以下操作：

1. 转至以下任一页：
   - 在左侧窗格中，单击**机箱概览** → **网络** → **VLAN**。
   - 在左侧窗格中，单击**机箱概览** → **服务器概览**，然后单击**设置** → **VLAN**。
2. 在 **VLAN 标签设置**页面的 **iDRAC** 部分，为服务器启用 VLAN，设置优先级并输入 ID。有关各字段的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 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*> 的有效值为 1–4。

  <*VLAN*> 的有效值为 1-4000 和 4021-4094。默认值为 1。

  <*VLAN priority*> 的有效值为 0-7。默认值为 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*> 的有效值为 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。它代表 CMC 发送到服务器的设备，并用作它针对该服务器的第一引导设备。可以将此设备设置为默认第一引导设备或一次性引导设备，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。

您可以设置第一引导设备仅用于下次引导或用于所有后续重新引导。您可以设置服务器的第一引导设备。系统在下次和后续重新引导时会从所选设备引导，并保持作为 BIOS 引导顺序中的第一引导设备，直到从 CMC Web 界面或从 BIOS 引导顺序再次更改为止。

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。

您指定的引导设备必须存在并且包含可引导介质。

您可以将以下设备设置为第一引导设备。但是，要将设备设置为默认第一引导设备，请选择**默认**。

如果服务器上运行的固件版本与第一引导设备中的可用版本相同，为了不覆盖服务器固件版本，请选择**无**。

可以将以下设备设置为第一引导设备。

表. 6: 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	使用硬盘驱动器引导。
本地 CD/DVD	从服务器上的 CD 或 DVD 驱动器引导。
BIOS 设置	在 BIOS 设置过程中引导。
虚拟软盘	从虚拟软盘引导。
虚拟 CD/DVD	从虚拟 CD 或 DVD 驱动器引导。
本地 SD 卡	从本地 SD（安全数字）卡引导。
远程文件共享	从远程文件共享引导。
BIOS 引导管理器	使用 BIOS 引导管理器引导。
Lifecycle Controller	使用 Lifecycle Controller 引导。
本地软盘	从本地软盘驱动器中的软盘引导。

使用 CMC Web 界面为多个服务器设置第一引导设备

注: 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，以及 **iDRAC 登录**权限。

要为多个服务器设置第一引导设备，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览 → 设置 → 第一引导设备**。此时将显示服务器列表。
2. 在**第一引导设备**列中，从各服务器所对应的下拉菜单中选择要用于该服务器的引导设备。
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

注: 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。

要为单个服务器设置第一引导设备，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**，然后单击要为其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**页面。
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 PowerEdge FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2s 的 Chassis Management Controller RACADM 命令行参考指南）。

配置底座网络上行链路

只能在包含内部网络交换机的 PowerEdge FM120x4 底座上配置底座网络上行链路。

要配置底座网络上行链路，请转至**机箱概览 → 服务器概览 → 设置 → 底座网络上行链路**。

为底座网络上行链路配置属性选择下列值之一：

- 标准（聚合式）：在此上行链路配置中，在单个主干组中配置全部四个 IOM 上行链路端口，而所有 LOM 都映射至该组。默认选中此选项。
- 网络适配器隔离（增强安全性）：类似于标准的上行链路配置，但不允许本地节点之间的路由。
- 隔离网络：在此上行链路配置中，每个节点的 LOM1 映射至 IOM A1，而 LOM2 映射至 IOM A2。

部署远程文件共享

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。要使用此功能，必须具有企业版许可证。

要配置远程文件共享，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览 → 设置 → 远程文件共享**。
2. 在**部署远程文件共享**页面中，在各字段中键入相应的数据。有关字段说明的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。
3. 单击**连接**连接到远程文件共享。要连接远程文件共享，必须提供路径、用户名和密码。操作成功后将允许访问该介质。

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: 在单击部署按钮之前务必保存所有工作文件，因为此操作会使服务器重新启动。

单击**部署**后会执行以下任务：

- 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。

配置服务器 FlexAddress

有关为服务器配置 FlexAddress 的信息，请参阅使用 CMC Web 界面为机箱级结构和插槽配置 FlexAddress。要使用此功能，必须具有企业版许可证。

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 - 此组仅包含服务器的 BIOS 设置。
- BIOS 和引导 - 此组包含服务器的 BIOS 和引导设置。
- 所有设置 - 此版本包含服务器以及服务器上的组件的所有设置。这些配置文件是从以下版本生成的：
  - 包含 iDRAC7 1.57.57 或更高版本以及 Lifecycle Controller 2 版本 1.1 或更高版本的第 12 代服务器
  - 包含 iDRAC8 2.05.05 以及 Lifecycle Controller 2.00.00.00 或更高版本的第 13 代服务器。

服务器克隆功能支持 iDRAC7 和 iDRAC8 服务器。先前几代 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：

- iDRAC 必须具有所需的最低版本。iDRAC7 服务器需要版本 1.57.57。iDRAC8 服务器需要版本 2.05.05。
- 服务器必须接通电源。

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。
- 从管理站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管理站或远程文件共享。
- 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。

访问配置文件页面

可以使用**配置文件**页面添加和管理配置文件，以及将其应用于一个或多个服务器。

要使用 CMC Web 界面访问**配置文件**页面，请在左侧窗格中单击**机箱概览 → 服务器概览 → 设置 → 配置文件**。此时将显示**配置文件**页面。

管理存储的配置文件

您可以编辑、查看或删除 BIOS 配置文件。要管理 CMC 的存储配置文件，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览 → 服务器概览 → 设置 → 配置文件**。
2. 在**配置文件**页面的**应用配置文件**部分，单击**管理配置文件**。此时将显示**管理 BIOS 配置文件**页面。

- 要编辑配置文件，请单击**编辑**。
- 要查看 BIOS 设置，请单击**查看**。
- 要删除配置文件，请单击**删除**。有关字段说明的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

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，还可以添加说明。您可以在 CMC 非易失性扩展存储介质上最多保存 16 个存储的配置文件。

注: 如果远程共享可用，则使用 CMC 扩展存储和远程共享最多可存储 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。

非易失性扩展存储介质的删除或禁用会阻止对存储的配置文件的访问，并禁用服务器克隆功能。

要添加配置文件：

1. 转至**服务器配置文件**页面。在**服务器配置文件**部分，单击**应用和保存配置文件**。
2. 选择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**。此时将显示**保存配置文件**部分。
3. 选择**扩展存储**或**网络共享**作为保存配置文件的位置。

   注: 仅当网络共享已装载并且可访问时才会启用“网络共享”选项，并在“存储的配置文件”部分显示详细信息。如果网络共享未连接，则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。
4. 在**配置文件名称**和**说明**字段中，输入配置文件的名称和说明（可选），然后单击**保存配置文件**。

   注:

   保存服务器配置文件时，配置文件名称不支持的字符列表包括井号 (#)、逗号 (,) 和问号 (?)。

   支持标准 ASCII 扩展字符集。不支持以下特殊字符：

)、“、.、*、>、<、\、/、:、和 |

   CMC 与 LC 通信以获取可用的服务器配置文件设置，并将它们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。

应用配置文件

仅当服务器配置文件存储在 CMC 上的非易失性介质或远程共享上时，才能执行服务器克隆。要启动服务器克隆操作，可以将存储的配置文件应用到一个或多个服务器。

应用配置文件表中会显示每个服务器的操作状态、插槽编号、插槽名称以及型号名称。

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到该服务器。

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**下拉菜单显示所有可用的配置文件并按类型排序，包括位于存储库和 SD 卡上的配置文件。
2. 从**选择配置文件**下拉菜单中，选择要应用的配置文件。

   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克隆操作，必须为服务器启用 CSIOR 选项。如果已禁用 CSIOR 选项，会显示警告消息以指示服务器未启用 CSIOR。要完成刀片克隆操作，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。

   所选配置文件被应用至服务器，如果需要，可以立即重新引导服务器。有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

导入配置文件

可以将存储在管理站上的服务器配置文件导入 CMC。

要从 CMC 导入存储的配置文件：

1. 在**服务器配置文件**页面中的**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*联机帮助*。

导出配置文件

您可以将存储的服务器配置文件导出到管理站上的指定路径。

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，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，则会显示一条警告消息，指示如果导出配置文件，则说明会丢失。按**确定**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：

- 如果源文件位于 SD 卡上，则是本地或网络共享。

  注: 仅当网络共享已装载并且可访问时才会启用**网络共享**选项，并在**存储的配置文件**部分显示详细信息。如果网络共享未连接，则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。

- 如果源文件位于网络共享，则是本地或 SD 卡。

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，允许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**，将显示**保存配置文件**对话框。
4. 单击**保存配置文件**以将配置文件保存至所选位置。

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名称和说明。
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**。
   随即显示**编辑 BIOS 配置文件 — <配置文件名>** 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**编辑配置文件**。

   注: 您只能为存储在 SD 卡上的配置文件编辑配置文件说明。

   有关更多信息，请参阅*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*联机帮助*。

注: 只有**重新启动时收集系统资源清册 (CSIOR)** 选项启用时，CMC 服务器配置复制功能才会检索并显示特定服务器的设置。

要启用 CSIOR，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。

要在下列服务器上启用 CSIOR，请执行以下操作：

1. 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。
2. 第 13 代服务器 - 在重新引导服务器后，当出现提示时，按 F10 键访问 Lifecycle Controller。通过选择**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**。

查看存储的配置文件设置

要查看存储的服务器配置文件的配置文件设置，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**查看配置文件**列中的**查看**。此时将显示**查看设置**页面。有关所显示设置的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 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。该部分列出服务器克隆操作直接生成的最近 10 个配置文件日志条目。每条日志记录均显示服务器配置复制操作的严重性、提交时间和日期，以及复制日志消息描述。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**浏览配置文件日志**。**配置文件日志**页面随即显示。有关更多信息，请参阅*联机帮助*。

完成状态和故障排除

要检查应用的 BIOS 配置文件的完成状态，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览 → 服务器概览 → 设置 → 配置文件**。
2. 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)。
3. 在左侧窗格中，单击**服务器概览 → 故障排除 → Lifecycle Controller 作业**。搜索**作业**表中的相同 JID。
   有关使用 CMC 执行 Lifecycle Controller 作业的更多信息，请参阅 Lifecycle Controller 作业操作。

配置文件的快速部署

使用快速部署功能可以将存储的配置文件分配给服务器插槽。插槽中插入的任何支持服务器配置复制的服务器都可以使用分配给该插槽的配置文件进行配置。仅当"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**或**快速部署和服务器配置文件**时，才能执行快速部署操作。选中此选项后，允许在机箱中插入新服务器时应用所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都包含在 SD 卡中。

注: 要设置用于快速部署的配置文件，您必须拥有**机箱管理员**权限。

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**用于快速部署的配置文件**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: 仅当**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**或**快速部署和服务器配置文件**时，才能执行快速部署操作。选中此选项后，允许在机箱中插入新服务器时应用所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。可选择若干配置文件以应用于多个插槽。
3. 单击**分配配置文件**。
   配置文件将应用于选定的插槽。

注: 插入 FM120x4 底座时，分配给该服务器插槽的存储的配置文件将应用至全部四个服务器。

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。
- 要移除为一个或多个插槽分配的配置文件，请选择插槽，然后单击**移除分配**。如果启用了**快速部署配置文件**功能，此时将显示一条消息，警告您移除一个或多个插槽的配置文件将从插槽中插入的所有服务器中移除配置文件中的 XML 配置设置。单击**确定**以移除配置文件分配。
- 要移除插槽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:

仅当网络共享已装载并且可访问时才会启用**网络共享**选项，并在**存储的配置文件**部分显示详细信息。如果网络共享未连接，则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。

使用单点登录启动 iDRAC

CMC 针对单个机箱组件（例如服务器）提供有限的管理。为了全面管理这些单个组件，CMC 提供基于 Web 的服务器管理控制器 (iDRAC) 界面启动点。

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 用户会使用单点登录自动登录到 iDRAC。在 iDRAC 站点上，会自动授予此用户管理员权限。即便同一位用户没有在 iDRAC 上的帐户，或如果该帐户没有管理员权限，这也同样适用。
- CMC 用户如果**没有**服务器管理权限但拥有在 iDRAC 上的相同帐户，可使用单点登录自动登录到 iDRAC。在 iDRAC 站点上，授予此用户为 iDRAC 帐户创建的权限。
- CMC 用户如果没有服务器管理权限或在 iDRAC 上的相同帐户，则**不会**使用单点登录自动登录到 iDRAC。单击 **启动 iDRAC GUI** 可将此用户导航至 iDRAC 登录页。

  注: 在此情况下，术语“相同帐户”的含义是用户拥有 CMC 和 iDRAC 的相同登录名称以及匹配密码。用户拥有相同登录名称而没有匹配密码，也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。

如果从机箱卸下服务器，iDRAC IP 地址会更改，或 iDRAC 网络连接遇到问题，单击“启动 iDRAC GUI”可能会显示一个错误页。

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. 在左侧窗格中，展开**服务器概览**。在展开的**服务器概览**列表中，将显示所有四个服务器。
2. 单击要为其启动 iDRAC Web 界面的服务器。
3. 在**服务器状态**页面中，单击**启动 iDRAC GUI**。

   此时将显示 iDRAC Web 界面。有关字段说明的信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

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. 在左侧窗格中，单击**服务器概览**。
2. 在**服务器状态**页中，为要启动 iDRAC Web 界面的服务器单击**启动 iDRAC**。

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. 在左侧窗格中，展开**服务器概览**。在展开的服务器列表中，将显示所有四个服务器。
2. 单击您要启动远程控制台的服务器。
3. 在**服务器状态**页面中，单击**启动远程控制台**。

注: 仅当服务器安装了企业版许可证时，才会启用**启动远程控制台**按钮或链接。

8 配置 CMC 以发送警报

您可以为机箱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触发事件。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消息（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，例如电子邮件地址、IP 地址或外部服务器。

要配置 CMC 来发送警报，请执行以下操作：

1. 启用**机箱事件警报**选项。
2. 还可以根据类别或严重程度筛选警报。
3. 配置电子邮件警报或 SNMP 陷阱设置。
4. 启用机箱事件警报向已配置的目标发送电子邮件警报或 SNMP 陷阱。

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：

1. 在左侧窗格中，单击**机箱概览 → 警报**。
2. 在**机箱事件**页面的**机箱警报启用**部分，选择**启用机箱事件警报**选项以启用警报，或者清除该选项以禁用警报。
3. 要保存设置，请单击**应用**。

使用 RACADM 启用或禁用警报

要启用或禁用生成警报，请使用 **cfgIpmiLanAlertEnable** RACADM 对象。有关更多信息，请参阅 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

筛选警报

可以基于类别和严重性筛选警报。

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。

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，选中与目标 IP 对应的复选框以使该 IP 地址接收陷阱。您最多可以指定 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. 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)。
4. 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 3 中指定的索引值。

5. 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 2–5。

> **注:** 步骤 2–5 中的命令会覆盖为指定索引 (1-4) 配置的所有现有设置。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。

6. 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 CMC 域名，以便从 CMC 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：

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
   ```
3. 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。
4. 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>` 是有效的电子邮件地址，`<index>` 是在步骤 4 中指定的索引值。
5. 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。
6. 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 5。

   注: 步骤 2-5 中的命令会覆盖为指定索引 (1-4) 配置的所有现有设置。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** 上提供的 *RACADM Command Line Reference Guide for iDRAC and CMC*（适用于 iDRAC 和 CMC 的 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，CMC 配置了默认 root 帐户。作为管理员，您可以设置用户帐户，以允许其他用户访问 CMC。

您最多可以设置 16 个本地用户，或使用目录服务（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。角色包括管理员、操作员、只读用户或无角色。角色定义可用的最大权限。

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**权限外，授予 CMC 用户的权限不会自动转移到服务器上的同一用户，因为服务器用户的创建是与 CMC 用户无关的。换言之，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. 7: 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。 用户可能具备其他权限而不具备 CMC 登录用户权限。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，用户仍将保留所有之前授予的其他权限。
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而非服务器本身相关的机箱属性。因此，不管服务器是否存在于插槽中，都可以添加或更改插槽名称和插槽优先级。

权限	说明
	当服务器移到不同的机箱中时，它会在新机箱中继承分配给它所占据的插槽的名称和优先级。以前的插槽名称和优先级与以前的机箱保持一致。 **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，要执行机箱电源操作，包括打开电源、关闭电源以及打开后再关闭电源，则需要**机箱控制管理员**权限。
用户配置管理员	用户可以： • 添加新用户。 • 更改用户的密码。 • 更改用户的权限。 • 启用或禁用某个用户的登录权限，但保留该用户在数据库中的名称和其他权限。
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）	拥有**机箱电源管理员**权限的 CMC 用户可以执行所有与电源相关的操作。他们可以控制机箱电源操作，包括打开电源、关闭电源以及打开后再关闭电源。 **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 CMC **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。 当不具备**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 会将一条命令发送给具有此用户的登录名和密码的目标服务器。如果该服务器上不存在此用户，或者密码不匹配，则拒绝此用户执行操作。 如果目标服务器上有此用户且密码匹配，则该服务器将应答此用户在该服务器上具有的权限。根据服务器的权限响应，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在服务器上被授予的权限和可以进行的操作。只有在机箱用户未具备机箱上的服务器管理权限时，才应用这些权限。 服务器配置管理员： • 设置 IP 地址 • 设置网关

权限	说明
	• 设置子网掩码 • 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	用户可设置和配置结构 A 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. 8: 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
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
来宾用户	登录
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

用户组	权限分配
	• 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
无	没有分配权限

表. 9: 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

修改根用户管理员帐户设置

为了增强安全性，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。要更改 root 帐户的默认密码，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**用户验证**。
2. 在**用户**页面的**用户 ID** 列中，单击 **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。
3. 在**用户配置**页面中，选择**更改密码**选项。
4. 在**密码**字段中键入新密码，然后在**确认密码**中键入相同的密码。
5. 单击**应用**。即会更改用户 ID **1** 的密码。

配置本地用户

您可以在 CMC 中配置多达 16 个具有特定访问权限的本地用户。在创建 CMC 本地用户之前，请验证是否存在当前用户。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 安全界面（如 Web 界面、RACADM 和 WS-MAN）进行更改。

使用 CMC Web 界面配置本地用户

注: 您必须具有**配置用户**权限才能创建 CMC 用户。

要添加和配置本地 CMC 用户，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**用户验证**。
2. 在**本地用户**页面的**用户 ID** 列中，单击某个用户 ID 号。此时将显示**用户配置**页面。

   注: 用户 ID 1 是 CMC 默认随附的根用户帐户。该帐户无法更改。

3. 启用用户 ID 并指定用户名、密码和该用户的访问权限。有关选项的更多信息，请参阅*联机帮助*。
4. 单击**应用**。即会创建具有相应权限的用户。

使用 RACADM 配置本地用户

注: 必须以 `root` 用户登录才能在远程 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，则当前唯一的用户帐户为默认的 root 帐户。`racresetcfg` 子命令将所有配置参数重设为默认值。之前的所有更改将丢失。

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。

要验证某个用户是否存在，请打开到 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“#”字符表示它是一个只读对象。同样，如果您使用 `racadm config -f racadm.cfg` 命令来指定要写入的任意数量的组/对象，则无法指定索引。新用户会添加到第一个可用的索引。这种行为允许使用与主 CMC 相同的设置来配置另一个 CMC，具备更大的灵活性。

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: 在以下操作系统上，您可以使用 Active Directory 识别 CMC 用户。

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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。

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。

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. 10: 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	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	0x00000ed9
3	无	CMC 登录用户	0x00000001

角色组	默认权限级别	授予的权限	位掩码
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。

扩展架构 Active Directory 概览

使用扩展架构解决方案需要 Active Directory 架构扩展。

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。

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。

配置通用 LDAP 目录以访问 CMC

CMC 的通用 LDAP 实现在授予用户访问权限时分两阶段 - 先是用户验证，然后是用户授权。

使用 CMC Web 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: 您必须具有**机箱配置管理员**权限。

1. 在左侧窗格中，单击**机箱概览** → **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*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**。
6. 在**配置 LDAP 角色组**页面中，指定角色组的组域名和权限。
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. 如果您选择了**启用 SSL 证书验证**选项，则在**管理证书**部分，指定 CA 证书以在 SSL 握手期间验证 LDAP 服务器证书，然后单击**上载**。证书便上载到 CMC 并会显示详细信息。
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。以下查询可用于搜索 DNS 中的 SRV 记录：

`_ldap._tcp.domainname.com`

`ldap` 在上述查询中为 `cfgLDAPSRVLookupServiceName` 属性。

`cfgLDAPSRVLookupDomainName` 配置为 **domainname.com**。

有关 RACADM 命令的更多信息，请参阅 **dell.com/support/manuals** 上的 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell 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。

SSO 使用 Kerberos 作为验证方法，使已经登录的用户可以自动或单点登录到 Exchange 等后续应用程序。对于单点登录，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，操作系统就会缓存这些凭据。

双重验证提供了更高级别的安全性，要求用户具有密码或 PIN 以及含有私钥或数字证书的实物卡。Kerberos 使用此双重验证机制来让系统可以证明用户的真实性。

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**页面并禁用所有（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。

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: 如果您使用 Windows 2003 上的 Active Directory，应确保客户端系统上安装了最新的 Service Pack 和增补软件。如果您使用 Windows 2008 上的 Active Directory，应确保安装了 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

- 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 (KDC)。
- 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）。

生成 Kerberos Keytab 文件

为了支持 SSO 和智能卡登录验证，CMC 支持 Windows Kerberos 网络。ktpass 工具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，以便与 ktpass 命令的 **-mapuser** 选项一起使用。您必须使用与上载生成的 keytab 文件的 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 中的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.domain_name.com@REALM_NAME.COM -mapuser
   dracname -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 概览。

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

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**。
4. 在**代理服务器**部分，选择**为 LAN 使用代理服务器（这些设置不会应用于拨号或 VPN 连接）**选项，然后单击**高级**。
5. 在**例外**部分，将管理网络上的 CMC 和 iDRAC 地址添加到分号分隔的列表。可以在条目中使用 DNS 名称和通配符。

Mozilla Firefox

要在 Mozilla Firefox 版本 19.0 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），或者单击**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**手动代理配置**。
6. 在**不使用代理**字段中，将管理网络上 CMC 和 iDRAC 的地址输入到逗号分隔的列表中。可以在条目中使用 DNS 名称和通配符。

配置浏览器以使用智能卡登录

Internet Explorer - 确保将 Internet 浏览器配置为下载 Active-X 插件。

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 -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`

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 for Dell PowerEdge FX2/FX2s 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: 如果选择了这两个选项，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，则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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell 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. 在左侧窗格中，单击**机箱概览 → 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 -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，并介绍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 PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller RACADM 命令行参考指南）。

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 命令用于连接到服务器和 I/O 模块的串行控制台；也可使用 `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 命令行界面命令

当连接到 CMC 命令行时，可以输入这些命令：

表. 11: 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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。
`connect`	连接到服务器或 IO 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 `connect` RACADM 命令。
`exit`、`logout` 和 `quit`	所有这些命令都执行相同操作，即结束当前会话并返回登录命令行界面。

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。

要修复此问题，请从 **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。

将 SSH 与 CMC 配合使用

SSH 是一种命令行会话，包含与 Telnet 会话相同的功能，但还包含会话协商和加密功能以增强安全性。CMC 支持具有密码验证功能的 SSH 版本 2。CMC 上默认启用 SSH。

注: CMC 不支持 SSH 版本 1。

如果在 CMC 登录过程中出现错误，SSH 客户端就会发出错误消息。此消息文本取决于客户端，不受 CMC 控制。查看 RACLog 消息可确定故障原因。

注: 在 Windows 上，必须从 VT100 或 ANSI 终端仿真程序运行 `OpenSSH`。也可使用 Putty.exe 运行 `OpenSSH`。在 Windows 命令提示符处运行 `OpenSSH` 不能提供完整的功能（即有些键不响应并且不显示图形）。对于运行 Linux 的服务器，运行 SSH 客户端服务以使用任何 Shell 连接到 CMC。

同时支持四个并发 SSH 会话。通过 `cfgSsnMgtSshIdleTimeout` 属性控制会话超时。有关 RACADM 命令的更多信息，请参阅 dell.com/support/Manuals 上的 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

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输入 ID/密码，从而提高了 SSH 脚本编写的自动化程度。

SSH 默认为启用。如果禁用了 SSH，可使用任何其他支持的界面启用。

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. 12: 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

方案类型	方案
	• 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，通过 SSH 接口与服务用户名一起使用。添加或删除公共密钥之前，务必使用 `view` 命令查看已设置了哪些密钥，这样就不会无意中覆盖或删除密钥。服务用户名是特殊用户帐户，可在通过 SSH 访问 CMC 时使用。在设置和正确使用 SSH 上的 PKA 时，无需输入用户名或密码即可登录到 CMC。这对于设置执行各种功能的自动化脚本非常有用。

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，确保现有密钥没有位于添加新密钥的索引处。CMC 在添加新密钥之前不检查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 PowerEdge FX2/FX2s Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Chassis Management Controller 命令行参考指南）。

配置终端仿真软件

CMC 支持串行文本控制台，可使用任意终端仿真软件启动该控制台。下面例举了可用于连接到 CMC 的终端仿真软件。

1. Linux Minicom
2. Hilgraveve 针对 Windows 的超级终端

将串行零调制解调器电缆（两端均存在）的一端连接到机箱背面的串行连接器。将电缆的另一端连接到管理站串行端口。有关连接电缆的更多信息，请参见机箱概览部分的机箱背面板。

使用以下参数配置终端仿真软件：

- **波特率**：115200
- **端口**：COM1
- **数据**：8 位
- **奇偶校验**：无

- **停止位**：1 位
- **硬件流控制**：是
- **软件流控制**：否

使用 Connect 命令连接到服务器或 I/O 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：

- CMC 命令行界面 (CLI) 或 RACADM `connect` 命令。有关运行 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 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 `connect` 命令以建立到服务器或 I/O 模块的串行连接。服务器串行控制台既包含 BIOS 引导和设置屏幕，也包含操作系统串行控制台。对于 I/O 模块，可使用交换机串行控制台。在机箱上有单个 IOM。

小心: 从 CMC 串行控制台运行时，`connect -b` 选项将保持连接状态，直到 CMC 重设为止。此连接具有潜在的安全风险。

注: `connect` 命令提供了 `-b`（二进制）选项。此 `-b` 选项传递原始二进制数据，而不使用 `cfgSerialConsoleQuitKey`。此外，当使用 CMC 串行控制台连接到服务器时，DTR 信号中的过渡（例如，如果卸下串行电缆而连接调试器）不会导致退出应用程序。

注: 如果 IOM 不支持控制台重定向，则 `connect` 命令会显示闲置的控制台。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为 <Ctrl><\>。

要连接到 IOM，请执行以下命令：

`connect switch-`*`n`*

其中 `n` 为 IOM 标签 A1。

在 connect 命令中引用 IOM 时，IOM 将按照下表所示映射到交换机。

表. 13: 将 I/O 模块映射到交换机

I/O 模块标签	交换机
A1	交换机 a1 或交换机 1
A2	交换机 a2 或交换机 2

注: 每个机箱同一时间只能有一个 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的串行控制台，请运行 `connect server-`*`n`* 命令，其中 *n* 为 1–4（PowerEdge FM120x4）和 *n* 为 1–8 (PowerEdge FC630)。也可以使用 `racadm connect server-n` 命令。使用 `-b` 选项连接到服务器时，假定为二进制通信且转义字符被禁用。如果 iDRAC 不可用，则会显示 `No route to host`（没有至主机的路由）错误消息。

命令 `connect server-n` 允许用户访问服务器的串行端口。建立此连接后，用户能够看到服务器通过 CMC 串行端口的控制台重定向，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，页面上的字符将无法正常显示。

注: 在 BIOS 设置页面中，并非所有键都起作用。因此需提供针对 <Ctrl>+<Alt>+<Delete> 和其他键的相应键盘快捷键。初始重定向屏幕显示所需的键盘快捷键。

为串行控制台重定向配置管理服务器 BIOS

您可以使用远程控制台会话通过 iDRAC7 Web 界面连接到管理系统（请参阅位于 **dell.com/support/manuals** 的 *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide* [Dell Integrated Dell Remote Access Controller (iDRAC) 用户指南]）。

默认情况下，BIOS 中的串行通信为关闭。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. 打开管理服务器电源。
2. 在开机自检过程中，按 <F2> 键进入 BIOS 设置公用程序。
3. 转至**串行通信**，然后按 <Enter> 键。在对话框中，串行通信列表将显示以下选项：
   - 关
   - **开，控制台重定向不启用**
   - **开，通过 COM1 进行控制台重定向**

   要在这些选项之间导航，请按相应的箭头键。

   注: 确保选中了**开，通过 COM1 进行控制台重定向**选项。
4. 启用**引导后重定向**，默认值为 **禁用**。选择此选项后，可在后续的重新引导后进行 BIOS 控制台重定向。
5. 保存更改并退出。

   管理系统重新启动。

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键入以下两个新行：

   ```
   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 FlexAddress Plus 卡

本节提供有关 FlexAddress 以及如何使用 FlexAddress Plus 卡配置 FlexAddress 的信息。

注: FlexAddress 是一项许可功能。此功能的许可证包括在企业版许可证中。

关于 FlexAddress

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 保持不变。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、SAN 资源、DHCP 服务器和各种结构的路由器。

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。在没有 FlexAddress 的情况下，如果需要使用另一个服务器模块替换某个服务器，则 WWN/MAC ID 将会更改，并且需要重新配置以太网网络管理工具和 SAN 资源以识别新的服务器模块。

如果将服务器插入新的插槽或机箱，则会使用服务器分配的 WWN/MAC，除非该机箱为新插槽启用了 FlexAddress 功能。如果卸下服务器，它将还原为服务器分配的地址。

此外，*覆盖*操作仅在将服务器模块插入启用了 FlexAddress 的机箱时发生；对服务器模块未进行永久性更改。如果服务器模块移至不支持 FlexAddress 的机箱，则使用出厂分配的 WWN/MAC ID。

CMC FX2/FX2S 机箱附带 FlexAddress Plus SD 卡，该卡支持 FlexAddress、FlexAddress Plus 和扩展存储功能。

注: FlexAddress Plus SD 卡上包含的数据经过加密，不得以任何方式进行复制或修改，否则会妨碍系统功能并导致系统无法正常运行。

注: 每个 FlexAddress Plus SD 卡仅限用于一个机箱。不能在另一个机箱上使用同一个 FlexAddress Plus SD 卡。

关于 FlexAddress Plus

每个 FlexAddress Plus 功能卡包含唯一的 MAC/WWN 池，允许机箱为光纤信道和以太网设备分配全球名称/介质访问控制 (WWN/MAC) 地址。机箱分配的 WWN/MAC 地址全局唯一且特定于服务器插槽。

在安装 FlexAddress 之前，可以通过将 SD 卡插入 USB 内存卡读卡器并查看 **pwwn_mac.xml** 文件来确定 FlexAddress 功能卡中包含的 MAC 地址范围。这个位于 SD 卡上的明文 XML 文件包含 XML 标记 `mac_start`，该标记是用于此唯一 MAC 地址范围的第一个起始十六进制 MAC 地址。`mac_count` 标记是 SD 卡分配的 MAC 地址的总数。要确定分配的总 MAC 范围，请使用以下公式：

```
<mac_start> + <mac_count> - 1 = <mac_end>
```

例如：

```
(starting_mac)00:18:8B:FF:DC:FA + (mac_count)0xCF – 1 =
(ending_mac)00:18:8B:FF:DD:C8
```

注: 将 SD 卡插入 USB 内存读卡器之前先锁定 SD 卡，以防止意外修改其中的任何内容。将 SD 卡插入 CMC 之前，*必须解除锁定*。

验证 FlexAddress 激活

要查看 FlexAddress 功能的激活状态，请运行以下 RACADM 命令：

```
racadm featurecard -s
```

```
       Feature Name = FlexAddress Date/time Activated = 05 Oct 2013 - 11:50:49
Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = FlexAddressPlus Date/time Activated = 05 Oct 2013 -
11:50:49 Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = ExtendedStorage Current Status = redundant, active Date/
time Activated = 05 Oct 2013 - 11:50:58 Feature installed from SD-card serial
number = CN0H871T1374036T00MXA00
```

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

```
racadm feature -s No features active on the chassis
```

要查看 SD 卡信息：

```
$ racadm featurecard -s Active CMC: The feature card inserted is valid, serial
number CN0H871T1374036T00MXA00 The feature card contains the following
feature(s) FlexAddress: bound FlexAddressPlus: bound ExtendedStorage: bound
```

表. 14: featurecard -s 命令返回的状态消息

状态消息	操作
`No feature card inserted.`	检查 CMC 以验证 SD 卡是否正确插入。
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.`	无需任何操作。
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.`	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: not bound.`	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。

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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell 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。停用功能会将 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。在此语境中，FlexAddress 一词指 FlexAddress 和 FlexAddressPlus。

注: SD 卡必须实际安装在 CMC 中，并且在运行停用命令之前必须关闭机箱电源。

如果在未安装卡时运行停用命令，或者对安装在不同机箱上的卡运行该命令，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.
```

如果在运行命令前未关闭机箱电源，则该命令将显示以下错误消息：

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

注: 要再次激活 FlexAddress 功能，请重新引导 CMC。

有关该命令的详情，请参阅 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）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: 通过使用 `racresetcfg` 子命令，您可以将 CMC 的 Flex Address 重设为其出厂默认设置，即“禁用”。RACADM 语法为：

```
racadm racresetcfg -c flex
```

有关 FlexAddress 相关的 RACADM 命令和其他出厂默认属性相关数据的更多信息，请参阅 **dell.com/support/manuals** 上的 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

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。

注: 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。基于每个结构启用 FlexAddress，然后选择参与该功能的插槽。必须同时启用结构和插槽才能成功配置 FlexAddress。

查看全局名称/介质访问控制 (WWN/MAC) ID

WWN/MAC 摘要页面可用于查看机箱中插槽的 WWN 配置和 MAC 地址。

命令消息

下表列出 RACADM 命令和常见 FlexAddress 情况的输出。

表. 15: FlexAddress 命令和输出

情况	命令	输出

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: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`

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: bound`

CMC 模块中的 SD 卡绑定到任何服务标签。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress:not bound`

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），机箱上没有 FlexAddress 功能。	`$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/结构上设置 FlexAddress。	`$racadm setflexaddr [-f` *<fabricName> <slotState>*`]`	`ERROR: Insufficient user privileges to perform operation`

情况	命令	输出
	`$racadm setflexaddr [-i <slot#> <slotstate>]`	
在机箱接通电源的情况下停用 FlexAddress 功能。	`$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`
未安装 CMC 企业版许可证的情况下更改插槽或结构的 Flexaddress 设置。	`$racadm setflexaddr -i<slotnum> <status>` `$racadm setflexaddr -f<FabricName> <status>`	`ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details.` **注:** 要解决此问题，您必须具有 **FlexAddress Enablement** 许可证。

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。

查看 WWN/MAC 地址信息

您可以查看机箱中每个服务器插槽或所有服务器的网络适配器的 WWW/MAC 地址资源清册。资源清册中包含以下信息：

- 结构配置

  注:

  – 结构 A 显示已安装的输入/输出结构的类型。如果启用了结构 A，则未填充的插槽会显示机箱为结构 A 分配的 MAC 地址。

  – iDRAC 管理控制器被视为管理结构的一部分，并与结构的其余部分一起显示。

  – 组件旁的复选标记表示启用了结构的 FlexAddress 或 FlexAddressPlus。
- 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）。绿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。根据使用的界面，您可以筛选 MAC 地址，并了解该功能或分区正在使用的 WWN/MAC 地址。如果适配器启用了 NPAR，则可以查看哪些分区已启用或已禁用。

使用 Web 界面中的 **FlexAddress** 页面（单击**服务器概览 → 插槽 <x> → 设置 → FlexAddress**）可以查看特定插槽的 WWN/MAC 地址信息。您可以使用 **WWN/MAC 摘要**页面（单击**服务器概览 → 属性 → WWN/MAC**）查看所有插槽和服务器的 WWN/MAC 地址信息。使用这两个页面都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** - 在此模式下，可以查看服务器插槽、结构、协议、WWN/MAC 地址和分区状态。在 WWN/MAC 地址字段中仅显示活动 MAC 地址。可以使用显示的任意字段或所有字段进行筛选。
- **高级模式** - 在此模式下，可以查看在基本模式中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）。可以使用显示的任意字段或所有字段进行筛选。

在基本模式和高级模式下，WWN/MAC 地址信息均以折叠表单形式显示。单击某个插槽旁边的 + 或单击**全部展开/折叠**以查看特定插槽或所有插槽的信息。

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 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

使用 Web 界面查看基本 WWN/MAC 地址信息

要在基本模式下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：

1. 单击**服务器概览 → 属性 → WWN/MAC**

   WWN/MAC 摘要页面显示 WWN/MAC 地址信息。

   或者，单击**服务器概览 → 插槽 <x> → 设置 → FlexAddress** 以查看特定服务器插槽的 WWN/MAC 地址信息。此时将显示 **FlexAddress** 页面。
2. 在 **WWN/MAC 地址**表中，单击**导出**以在本地保存 WWN/MAC 地址。
3. 单击某个插槽的 + 或单击**全部展开/折叠**以展开或折叠在 WWN/MAC 地址表中为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**，以在树视图中查看 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特定插槽中的服务器的 WWN/MAC 地址属性。
6. 从**结构**下拉菜单中选择某个结构类型，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**或某个列出的网络协议，以查看所有 MAC 或与所选协议关联的 MAC。
8. 在 **WWN/MAC 地址**字段中，要筛选与特定 MAC 地址关联的插槽，请输入准确的 MAC 地址。或者，输入部分 MAC 地址条目以查看关联的插槽。例如，输入 `4A` 以查看其 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，则显示该分区的行呈灰色。

有关各字段的信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

使用 Web 界面查看高级 WWN/MAC 地址信息

要在高级模式下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：

1. 单击**服务器概览 → 属性 → WWN/MAC**

   WWN/MAC 摘要页面显示 WWN/MAC 地址信息。
2. 从**视图**下拉菜单中选择**高级**，以在详细视图中查看 WWN/MAC 地址属性。

   在 **WWN/MAC 地址**表中显示服务器插槽、结构、协议、WWN/MAC 地址、MAC 地址分配类型（服务器分配、FlexAddress 或 I/O 标识 MAC）以及分区状态。绿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的 MAC 地址。如果服务器未启用 FlexAddress 或 I/O 标识，则 **FlexAddress（机箱分配）**或 **I/O 标识（远程分配）**的状态显示为**未启用**。
3. 在 **WWN/MAC 地址**表中，单击**导出**以在本地保存 WWN/MAC 地址。
4. 单击某个插槽的 + 或单击**全部展开/折叠**以展开或折叠在 WWN/MAC 地址表中为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特定插槽中的服务器的 WWN/MAC 地址属性。
6. 从**结构**下拉菜单中选择某个结构类型，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**或某个列出的网络协议，以查看所有 MAC 或与所选协议关联的 MAC。
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，输入部分 MAC 地址条目以查看关联的插槽。例如，输入 `4A` 以查看其 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，则状态显示为**已禁用**，并且显示该分区的行呈灰色。

有关各字段的信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

使用 RACADM 查看 WWN/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 至 4。

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，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 或夹层卡的以太网和 iSCSI MAC 地址，请使用以下 RACADM 命令：

```
racadm getmacaddress -a
```

要显示所有 LOM 或夹层卡的控制台分配 MAC/WWN，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
```

有关 **getflexaddr** 和 **getmacaddress** 子命令的更多信息，请参阅 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

13

管理结构

机箱支持两种结构类型：结构 A1 和结构 A2，供两个 I/O 模块使用，并且始终连接到服务器的机载以太网适配器。

注: 在 PowerEdge FX2s 机箱中，结构 B 和 C 是到 PCIe 扩展卡的 PCIe 连接。

支持以下 IO 模块：

- 1 GbE 直通
- 10 GbE 直通
- I/O 聚合器（在 PowerEdge FX2/FX2s 中提供）

两种结构都仅支持以太网。根据容量，每个服务器 IO 适配器 (LOM) 可以有两个或四个端口。夹层卡插槽插入 PCIe 扩展卡，而 PCIe 扩展卡连接到 PCIe 卡（而不是 IO 模块）。

注: 在 CMC CLI 中，IOM 按照惯例称为 switch。

监测 IOM 运行状况

有关监测 IOM 运行状况的信息，请参阅查看 IOM 的信息和运行状况。

为 IOM 配置网络设置

可以为用于管理 IOM 的接口指定网络设置。对于以太网交换机，可以配置带外的管理端口（IP 地址）。不能使用此界面配置带内管理端口（即 VLAN1）。

在为 IOM 配置网络设置之前，确保将 IOM 电源打开。

要为组 A 中的 IOM 配置网络设置，必须具有结构 A 管理员权限。

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；否则会导致无法设置带外 IP 地址。有关默认带内管理 IP 地址，请参阅 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

要为 I/O 模块配置网络设置，请执行以下操作：

1. 在左侧窗格中依次单击**机箱概览**、**I/O 模块概览**和**设置**。或者，要配置可用 I/O 模块 **A1** 和 **A2** 的网络设置，请单击 **A1 千兆位以太网**或 **A2 千兆位以太网**，然后单击**设置**。

在**配置 I/O 模块网络设置**页面中，键入相应的数据，然后单击"应用"。

2. 如果允许，请键入 IOM 的根密码、SNMP RO 团体字符串和系统日志服务器 IP 地址。有关字段说明的更多信息，请参阅*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，必须运行 `connect switch` 命令或 `racadm connect switch` RACADM 命令，或者使用到 IOM GUI 的直接界面将该地址保存到启动配置文件中。

3. 单击**应用**。

   IOM 的网络设置已配置完成。

   注: 如果允许，可以将 VLAN、网络属性和 IO 端口重设为默认配置值。

使用 RACADM 为 IOM 配置网络设置

要使用 RACADM 为 IOM 配置网络设置，请设置日期和时间。请参阅 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell 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 命令为 IOM 设置用户名、密码和 SNMP 字符串：

```
racadm deploy -m switch -u <username> -p <password>

racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro

racadm deploy -a [server|switch] -u <username> -p <password>
```

使用 Web 界面查看 I/O 模块的上行链路和下行链路状态

注: 此功能仅在 PowerEdge FX2/FX2s 中提供。

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。要完成此任务，请执行以下操作：

1. 转到**机箱概览** → **I/O 模块概览**。

   展开的列表中将显示所有 IOM (1–2)。

2. 单击您要查看的 IOM（插槽）。

   此时将显示该 IOM 插槽特定的 I/O 模块状态页面，并显示 I/O 模块上行链路状态和 I/O 模块下行链路状态表格。这些表格将显示关于下行链路端口 (1–8) 和上行链路端口 (9-12) 的信息。有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

使用 Web 界面查看 I/O 模块 FCoE 会话信息

可以使用 CMC Web 界面查看 Dell PowerEdge M I/O 聚合器的 FCoE 会话信息。要完成此任务，请执行以下操作：

1. 转到**机箱概览** → **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）。单击**属性** → **FCoE**。

   随即会显示特定于该 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 所需的端口号，然后单击"显示会话"。所选选项会检索交换机的 FCoE 会话信息，并以表格的形式呈现给用户。

FCoE 会话信息部分将显示交换机的 FCoE 会话信息。

注: 当交换机正在使用协议时，I/O 聚合器还会显示活动 FCoE 会话。

将 IOM 重设为出厂默认设置

可以使用**部署 I/O 模块**页面将 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 模块概览**，然后单击**设置**，或者在系统树中展开 **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 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。

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: 此功能仅在 **Dell PowerEdge I/O 聚合器**上受支持。

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**。

   此时会显示“IOM 固件更新”页面。或者，转至以下任一页面

   - **机箱概览** → **更新**。
   - **机箱概览** → **机箱控制器** → **更新**。

   随即显示固件更新页，该页提供用以访问 IOM 固件和软件页的链接。
2. 在“IOM 固件更新”页面中的“固件”部分，选中“更新”列中您要更新其软件的 IOM 对应的复选框，然后单击**应用固件更新**。或者，要回滚至该软件的较早版本，请选中“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。

   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)。

14

使用 VLAN Manager

可以通过使用 **VLAN Manager** 选项指定或查看 IOM 上的 VLAN 设置。

注: 此功能仅在 Dell PowerEdge I/O 聚合器上受支持。

将 VLAN 分配至 IOM

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，可以在 32 端口交换机上为各用户分隔网络。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。

要将 VLAN 分配至 IOM，请转至**机箱概览 → I/O 模块概览 → 设置 → VLAN Manager**。

在 **VLAN 分配**部分中，选择 I/O 模块，然后选择配置类型。同时指定端口范围和插槽。

通过从下拉菜单的列表中进行选择来更改或编辑 VLAN。

使用 CMC Web 界面配置 IOM 的 VLAN 设置

要使用 CMC Web 界面配置 IOM 的 VLAN 设置，请执行以下操作：

1. 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**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。
3. 在**指定端口范围**部分，选择要分配给所选 IOM 的结构端口范围。
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**编辑 VLAN** 部分，输入 IOM 的 VLAN ID。输入范围 1-4094 内的 VLAN ID。VLAN ID 可以采用范围或逗号分隔的形式输入。
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。

   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. 转至 **I/O 模块概览**，然后单击**设置 → VLAN Manager**。

   此时会显示 **VLAN Manager** 页面。"汇总所有端口的 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. 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**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 界面移除 IOM 的 VLAN

要使用 CMC Web 界面移除 IOM 的 VLAN，请执行以下操作：

1. 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**选择 I/O 模块**部分，选择所需的 IOM。
3. 在**编辑 VLAN** 部分，在下拉列表中选择**删除 VLAN** 并单击**应用**。

   分配给所选 IOM 的 VLAN 即被移除。

   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：

注: 未标记的 VLAN 无法设置为已标记的 VLAN ID。

1. 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**选择 I/O 模块**部分，选择所需的 IOM。

3. 在**指定端口范围**部分，选择要分配给所选 IOM 的结构端口范围。
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**编辑 VLAN** 部分，从下拉列表中选择**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. 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**选择 I/O 模块**部分，选择所需的 IOM。
3. 在**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**确定**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。

15 管理和监测电源

PowerEdge FX2/FX2s 机箱是能效最高的服务器机柜。其设计中包含高效率的电源设备和风扇，优化的布局使气流在系统内畅行无阻，并且机柜中处处包含优化能效的组件。优化的硬件设计配合内置于 Chassis Management Controller (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服务器环境的能效。

PowerEdge FX2/FX2s 中的电源管理与 PowerEdge VRTX 不同。电源管理技术的一项重大更改是采用了闭环系统节流 (CLST) 来维持所需的机箱功率上限。使用此技术的目的是提供更好的控制，同时允许机箱充分利用可用的 PSU。

PowerEdge FX2/FX2s 的电源管理功能可帮助管理员配置机柜以减少功耗，调节功率以满足环境的特定需要。

PowerEdge FX2/FX2s 机柜使用交流电源，并在活动电源设备装置 (PSU) 之间分配负载。该系统最多可提供 3371 瓦的交流电源，分配给服务器模块和相关的机柜基础结构。但是，该容量因您选择的电源冗余策略而异。

PowerEdge FX2/FX2s 机柜可配置三种冗余策略中的任何一种，冗余策略会影响 PSU 行为，并决定如何向管理员报告机箱冗余状态。

您也可以通过 **OpenManage Power Center (OMPC)** 控制电源管理。当 OMPC 从外部控制电源时，CMC 可继续维护：

- 冗余策略
- 远程电源日志记录

于是 OMPC 管理：

- 服务器电源
- 系统输入功率容量

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）。

冗余策略

冗余策略是一组可配置的属性，决定 CMC 如何管理机箱供电。可配置以下冗余策略：

- 电网冗余

- 无冗余
- 仅冗余警报

电网冗余策略

电网冗余策略的目的是使机柜系统能够在可以容忍交流电源故障的模式下运行。这些故障可能源自交流电网、布线、输送或 PSU 自身。在为系统配置电网冗余时，将 PSU 1 和 2 连接到不同的电网。

在此模式下，当电网或单个 PSU 发生故障时，CMC 可确保功耗保持不变，从而使系统继续无降级运行。服务器开机受限于单个 PSU 的可用功率。只要无法维持冗余（例如某个 PSU 被卸下或发生故障），就会触发警报，机箱运行状况变为**严重**。

无冗余策略

在此模式下，两个 PSU 的所有电力均可供使用，但不能保证 PSU 或电源故障不会影响系统运行。机箱的冗余状态始终为**无冗余**。

仅冗余警报策略

仅冗余警报策略允许服务器开机以使用两个 PSU 的容量，同时根据实际状况发出冗余丢失警报。如果某个 PSU 被卸下或发生故障，或者实际功耗超出单个 PSU 的容量，则会发出冗余丢失警报。这是默认策略。

PSU 故障

任何类型的 PSU 故障始终发出警报，而不考虑所选择的冗余策略。

默认冗余配置

仅冗余警报是机箱和两个 PSU 的默认冗余配置。

多节点底座适应

PowerEdge FM120x4 是多节点、半宽底座，可容纳四个服务器以及关联的 iDRAC（包含独立处理器）。其设计旨在提供最佳能效，并且处理器不能卸下。PowerEdge FM120 中的处理器共享公用电源基础结构，例如，整个底座共享单个电源以及温度传感器。

机箱功率限制监测

OpenManage Power Center (OMPC) 可用于监测和控制数据中心内的计算机功耗。PowerEdge FX2/FX2s 允许配置机箱功率上限以及指导功率上限设置的限值，从而支持 OMPC。功率限额的上限和下限由 CMC 设置，并且无法配置。

注: 下限是运行给定当前配置的机箱所需的最低功率。上限则反映当前冗余策略下可用的最大功率。

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

在左侧窗格中，单击**机箱概览 → 电源 → 电源监测**。“电源监测”页面将显示电源运行状况、系统电源状态、实时电源统计信息和实时能耗统计信息。有关更多信息，请参阅*联机帮助*。

注: 您也可以在“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
```

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，请在左侧窗格中转至**机箱概览**，然后单击**电源 → 预算状态**。**电源预算状态**页面显示系统电源策略配置（包含属性**系统输入功率上限**和**冗余策略**）、电源预算详细信息（包含属性**系统输入最大功率容量**、**输入冗余保留**和**可用于服务器开机的电源**）和机箱电源设备（包含电源设备装置详情）。有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell 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，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时，总体电源运行状况通常是**正常**。但是，如果不符合以电网冗余模式运行的条件，则冗余状态为**否**，而且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。

PSU 出现故障后的电源管理。

当 PSU 发生故障或被卸下时，为服务器提供的电力会下降。在极端情况下，可能会关闭服务器以尝试维持运转。配置和维护电网冗余可避免单个 PSU 故障对服务器产生任何影响。

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. 16: 电源更改的 SEL 事件

电源事件	系统事件日志 (SEL) 条目
插入	电源设备存在。
卸下	电源设备缺失。
接受交流输入	电源设备的电源输入已恢复。
交流输入丢失	电源设备的电源输入丢失。
产生直流输出	电源设备工作正常。
直流输出丢失	电源设备发生故障。

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**仅冗余警报**电源策略的机柜。下表列出有关电源冗余策略更改的 SEL 条目。

电源策略事件	系统事件日志 (SEL) 条目
冗余丢失	电源设备冗余丢失。
重获冗余	电源设备处于冗余状态。

配置电源预算和冗余

可以配置整个机箱（机箱、服务器、I/O 模块、CMC、PCIe 和机箱基础结构）的电源预算、冗余和动态电源。电源管理服务可优化功耗，并根据需求将电源重新分配给不同的模块。

您可以配置以下各项：

- 系统输入功率上限
- 冗余策略
- 禁用机箱电源按钮
- 最大节能模式
- 远程电源日志记录
- 远程电源日志记录间隔

节能和电源预算

如果功耗超过“系统输入功率上限”，则 PSU 提供给服务器的电力会缩减，以维持标称水平。

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。

要配置电源预算，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览 → → 电源 → 配置**。
2. 在**预算/冗余配置**页面中，根据需要选择以下任一或所有属性。有关字段说明的信息，请参阅*联机帮助*。
   - **冗余策略**
   - **禁用机箱电源按钮**

- **最大节能模式**

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：

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）或 3（仅冗余警报）。默认值为 3。

     例如，以下命令将冗余策略设置为 1：

     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```
   - 要设置电源预算值，请键入：

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
     ```

     其中 *<value>* 为“当前运行时机箱负荷”和 3371 之间的数字，表示最大功率上限（瓦）。默认值为 3371。

     例如，以下命令将最大电源预算设置为 3371 瓦：

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 3371
     ```
   - 要查看上限和下限，请键入：

     ```
     racadm getconfig -g cfgchassispower -o cfgchassispowercap <lower,upper>
     bound
     ```

     其中 *<lower, upper>* 是下限和上限。

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 3000
     ```
   - 若要启用最大功耗模式，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
     ```
   - 要启用电源远程日志记录功能，请输入以下命令：

     ```
     racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
     ```
   - 要指定所需的日志记录间隔，请输入以下命令：

     ```
     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，请输入以下命令：

     ```
     racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
     ```
   - 要确定电源远程日志记录间隔，请输入以下命令：

     ```
     racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
     ```

     电源远程日志记录功能依赖于之前是否已在远程系统日志主机上配置此功能。必须启用登录到一台或多台远程系统日志主机，否则将记录功耗。可通过 Web GUI 或 RACADM CLI 完成此操作。有关更多信息，请参阅远程系统日志配置说明。

- 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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell 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。

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 和 PSU）远程执行几项电源管理操作（如有序关机）。

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. 在左侧窗格中，单击**机箱概览 → 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。
   有关各个选项的信息，请参阅*联机帮助*。
   - **打开系统电源**
   - **关闭系统电源**
   - **关闭系统电源后重启（冷引导）**
   - **重设 CMC（热引导）**
   - **非正常关机**
3. 单击**应用**。
   将显示一个对话框，要求您进行确认。
4. 单击**确定**执行电源管理操作（例如，使系统重设）。

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（开机）、powerdown（关机）、powercycle（关机后再开机）、nongraceshutdown（非正常关机）或 reset（重设）。

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. 在左侧窗格中，单击**服务器概览 → 电源**。
   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**

- 正常关机
- 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 for Dell PowerEdge FX2/FX2s 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，重设服务器）。

对 IOM 执行电源控制操作

您可以远程重设或开启 IOM。

注: 要执行电源管理操作，必须具有**机箱控制管理员**权限。

使用 CMC Web 界面对 IOM 执行电源控制操作

要对 I/O 模块执行电源控制操作，请执行以下步骤：

1. 在左侧窗格中，单击**机箱概览** → **I/O 模块概览** → **电源**。
2. 在**电源控制**页上，对于 IOM，从下拉菜单中选择希望执行的操作（关机后再开机）。
3. 单击**应用**。

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 <action>
```

其中 <*action*> 表示要执行的操作：power cycle。

有关 RACADM 命令的信息，请参阅 dell.com/support/manuals 上的 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

配置底座电源按钮

可以将底座电源按钮配置为禁用，以便在按下底座电源按钮时不会有效果。要配置底座电源按钮，请转至**机箱概览** → **服务器概览** → **电源** → **控制**。

在**属性**部分下，选中复选框以禁用，或清除复选框以启用。

注: 此设置仅适用于机箱中的多节点底座。其他底座不受影响。

16 查看 PCIe 插槽

PowerEdge FX2/FX2s 机箱可选择包含八个 PCIe 插槽，其中每个 PCIe 插槽分配至特定的底座。默认情况下，所有 PCIe 插槽均已映射。PCIe 插槽无法重新映射至服务器或取消到服务器的映射。

PCIe 插槽	PowerEdge FC630 的映射
PCIe 插槽 1	4
PCIe 插槽 2	4
PCIe 插槽 3	2
PCIe 插槽 4	2
PCIe 插槽 5	3
PCIe 插槽 6	3
PCIe 插槽 7	1
PCIe 插槽 8	1

注: 仅 PowerEdge FX2s 支持 PCIe 管理，而 PowerEdge FX2 不支持。

有关管理 PCIe 插槽的更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

注: 无代理监测功能不适用于机箱 PCIe 插槽中的 PCIe PERC 和网卡。无代理监测是面向 Dell 第 12 代服务器的系统管理解决方案。它是完全的带外功能，不依赖于任何操作系统代理。利用无代理监测，可以使用 iDRAC 监测连接到服务器的存储设备（PERC、硬盘、机柜等）和网络设备，而不需要在管理系统或管理站上安装任何代理。有关无代理监测的更多信息，请参阅 Dell TechCenter 中的 *Agent-free inventory and monitoring for storage and network devices in Dell PowerEdge 12G Servers*（无代理资源清册和监测 Dell PowerEdge 12G 服务器中的存储和网络设备）白皮书。

使用 CMC Web 界面查看 PCIe 插槽属性

- 要查看全部八个 PCIe 插槽的信息，请在左侧窗格中单击**机箱概览** → **PCIe 概览**。单击 + 查看所需插槽的全部属性。
- 要查看一个 PCIe 插槽的信息，请单击**机箱概览** → **PCIe 插槽 <number>** → **属性** → **状态**。

使用 RACADM 查看 PCIe 插槽属性

您可以使用 RACADM 命令查看分配给服务器的 PCIe 插槽。这里提供了一些命令。有关 RACADM 命令的更多信息，请参阅 dell.com/support/Manuals 上的 *Dell Chassis Management Controller for PowerEdge FX2/*

FX2s RACADM Command Line Reference Guide（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

注: 只有在 BIOS 完成 `POST` 后，才会显示关联底座中的 PCIe 卡名称。在此之前，设备名称将显示为未知。

- 要查看当前分配给服务器的 PCIe 设备，请运行以下命令：

  ```
  racadm getpciecfg -a
  ```

- 要使用 FQDD 查看 PCIe 设备的属性，请运行以下命令：

  ```
  racadm getpciecfg [-c <FQDD>]
  ```

  例如，要查看 PCIe 设备 1 的属性，请运行以下命令：

  ```
  racadm getpciecfg -c pcie.chassisslot.1
  ```

注: 如果关联底座中不存在夹层卡，则 PCIe 卡将不会加电。

17

故障排除和恢复

本部分介绍如何使用 CMC Web 界面执行与远程系统问题恢复和故障排除相关的任务。

- 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。
- 网络问题故障排除。
- 警报问题故障排除。
- 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。

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` 包含以下子系统并汇集了以下 RACADM 命令。有关 `racdump` 的更多信息，请参阅 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*（适用于 PowerEdge FX2/FX2s 的 Dell Chassis Management Controller RACADM 命令行参考指南）。

子系统	RACADM 命令
常规系统/RAC 信息	`getsysinfo`
会话信息	`getssninfo`
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`
NIC 信息（CMC 模块）	`getniccfg`
跟踪日志信息	`gettracelog`
RAC 事件日志	`getraclog`
系统事件日志	`getsel`

下载 SNMP 管理信息库 (MIB) 文件

CMC SNMP MIB 文件定义机箱类型、事件和指示灯。使用 CMC 可以通过 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. 在左侧窗格中，单击**机箱概览** → **网络** → **服务** → **SNMP**。
2. 在 **SNMP 配置**部分中，单击**保存**将 CMC MIB 文件下载到本地系统。

   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

以下问题常用于管理系统中的高级别排除故障：

- 系统开机还是关机？
- 如果是开机，操作系统是正常运行、无响应还是停止运行？
- 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：**此配置要求机柜中 1 侧（左插槽）的电源设备和 2 侧（右插槽）的电源设备存在并且运行正常。此外，每个电源设备的容量必须足够支持机箱的总电源分配，以维持**电网冗余**。
  - **解决方案 B：**检查所有电源设备是否正确连接到两个交流电网：1 侧的电源设备必须连接到一个交流电网；2 侧的电源设备必须连接到另一个交流电网；并且两个交流电网都能正常工作。如果其中一个交流电网无法正常工作，则**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：**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：**检查系统输入功率上限设置 - 它的配置可能太低，导致不允许任何附加服务器开机。
- **问题：**可用电源不断变化，即便没有更改机柜配置。
  - **解决方案：**CMC 具有动态风扇电源管理功能，如果机柜在接近用户配置的功率上限峰值下运行时，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来为风扇分配电源，以保证输入功率低于**系统输入功率上限**。这是一种正常行为。
- **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。

查看事件日志

可以查看硬件和机箱日志，了解管理系统上发生的系统级严重事件的信息。

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 在发生指定事件时发送电子邮件或 SNMP 陷阱。

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
```

查看机箱日志

CMC 生成与机箱相关事件的日志。

注: 要清除机箱日志，您必须具有**清除日志管理员**权限。

使用诊断控制台

如果您是一位高级用户或在技术支持指导下的用户，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，您必须具有**调试命令管理员**权限。

要访问诊断控制台，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览 → 故障排除 → 诊断**。
   此时将显示**诊断控制台**页。
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*联机帮助*。

   此时将显示诊断结果页面。

重设组件

您可以重设 CMC，或者虚拟重设服务器，使其产生如同被卸下并重新插入的效果。

注: 要重设组件，必须具备**调试命令管理员**权限。

注: 虚拟重置不适用于 PowerEdge FM120x4 的单个节点。

要使用 CMC Web 界面重设组件，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览 → 故障排除 → 重设组件**。
   此时将显示**重设组件**页。
2. 要重设 CMC，请在 **CMC 状态**部分单击**重设 CMC**。将重新引导可用的 CMC。

有关更多信息，请参阅 *CMC for Dell PowerEdge FX2/FX2s 联机帮助*。

保存或还原机箱配置

这是一项许可功能。要使用 CMC Web 界面保存或还原机箱配置备份，请执行以下操作：

注: Flexaddress 信息、服务器配置文件和扩展存储不会与机箱配置一起保存或还原。建议使用远程文件共享或保存至本地工作站的副本将重要的服务器配置文件与机箱分开保存。有关执行这些操作的更多详情，请参阅添加或保存配置文件。

1. 在左侧窗格中，单击**机箱概览 → 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**保存**。覆盖默认文件路径（可选），然后单击**确定**保存文件。默认备份文件名包含机箱的服务标签。以后使用此备份文件只能还原此机箱的设置和证书。
2. 要还原机箱配置，在“还原”部分单击**浏览**，指定备份文件，然后单击**还原**。

   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。

网络时间协议 (NTP) 错误故障排除

配置 CMC 将其时钟和网络上的远程时间服务器同步后，可能需要 2-3 分钟日期和时间才会发生改变。如果这段时间后仍没有改变，可能需要排除故障。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。

要解决与 NTP 相关的问题，请检查 CMC 跟踪日志中的信息。该日志包含与 NTP 相关的故障的错误消息。如果 CMC 未能与任何配置的远程 NTP 服务器同步，则 CMC 时间与本地系统时钟同步，并且跟踪日志包含与下面类似的条目：

```
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
```

如果配置的一台服务器没有显示"*"，可能设置未正确配置。该命令的输出包含详细的 NTP 统计数据，在解决问题时，这些统计数据可能很有用。

如果您尝试配置基于 Windows 的 NTP 服务器，增大 `ntpd` 的 `MaxDist` 参数可能很有帮助。在更改此参数之前，请了解所有影响，因为默认设置必须足够大，才可配合多数 NTP 服务器运行。

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 指示以下组件状态：

- 组件上闪烁的琥珀色 LED 表示该模块发生故障。
- 蓝色、闪烁 LED 可由用户配置并可用于识别。有关配置的更多信息，请参阅 CMC_Stmp_配置 LED 以识别机箱上的组件。

表. 17: LED 颜色和闪烁样式

组件	LED 颜色，闪烁样式	状态
CMC		已开启
		正在上载固件
		已关闭电源
	蓝色，稳定发光	活动
	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
服务器		已打开电源
		正在上载固件
		已关闭电源
	蓝色，稳定发光	在 KVM 上选择了服务器
	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	已打开电源
	绿色，闪烁	正在上载固件
	绿色，暗色	已关闭电源
	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	已打开电源
	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

组件	LED 颜色，闪烁样式	状态
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	已关闭电源
	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
PCI	蓝色，暗色	已打开电源
	蓝色，闪烁	PCI 识别正在进行中。
	琥珀色，闪烁	故障

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。

观察 LED 以隔离问题

CMC 包含 LED，通过改变颜色来表示：

颜色	说明
蓝色	正常运行
蓝色，闪烁	ID（0.5 秒开，0.5 秒关）
琥珀色	机箱故障摘要
琥珀色，闪烁	机箱故障与并发 ID

从 DB-9 串行端口获取恢复信息

如果 CMC LED 呈琥珀色，则可以从位于 CMC 正面的 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 系统和客户端系统之间安装零调制解调器电缆。
2. 打开您选择的终端仿真器（如 HyperTerminal 或 Minicom）。看到系统提示时输入以下规格：8 位、无奇偶校验、无流控制、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> 键。

   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 self test failure
   ```

   ```
   recover1[Bad FW images] CMC 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。
   - 如果提示指出 **Bad FW Images（固件映像损坏）**，请完成恢复固件映像中的任务。

恢复固件映像

当 CMC 无法正常运行引导时，将进入恢复模式。在恢复模式下，提供小型命令子集以便通过上载固件更新文件 fx2_cmc.bin 对闪存设备重新编程。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。可使用 CMC Web 界面或 RACADM 访问跟踪日志。请参阅 *RACADM Command Line Reference Guide for iDRAC and CMC*（适用于 iDRAC 和 CMC 的 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。

一般故障排除

在操作（例如保存服务器配置文件）完成后显示成功消息，但有时该操作可能未生效。

要解决此问题，请检查 SSH、Telnet、HTTP 或 HTTPS 的任何 CMC 服务端口是否使用了操作系统服务的常用端口（如 111）。如果 CMC 服务端口使用了该端口，则将设置更改为非保留端口。有关保留端口的更多信息，请参阅 http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml。

18

常见问题

本部分列出了关于以下方面的常见问题：

- RACADM
- 管理和恢复远程系统
- Active Directory
- IOM

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)
```

这条消息什么意思？

只有在 CMC 完成重设后，才能发出另一条命令。

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` 子命令可显示正确的语法和用法信息。例如，如果在清除机箱日志时出现错误，可以运行以下子命令。

```
racadm chassislog help clear
```

与 CMC 相关的错误消息 - CMC 无法执行操作的问题。显示以下错误消息

```
racadm command failed.
```

要查看有关机箱的信息，请键入以下命令。

```
racadm gettracelog
```

在使用固件 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。

在使用 `$ logout` 和 `$ quit` 命令时，将显示错误消息：`Not Found`。

管理和恢复远程系统

访问 CMC Web 界面时，显示一个安全警告，指出 SSL 证书的主机名与显示的 CMC 的主机名不匹配。

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. 在左侧窗格中，单击**机箱概览**。
2. 单击**网络**。
   随即会出现**网络配置**页面。
3. 选中**在 DNS 上注册 CMC** 选项。
4. 在 **DNS CMC 名称**字段中输入 CMC 名称。
5. 单击**应用更改**。

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？

CMC Web 服务器重设后，可能需要等待一分钟，远程 RACADM 服务和 Web 界面才会可用。

CMC Web 服务器会在发生以下情况后重设：

- 使用 CMC Web 用户界面更改网络配置或网络安全性属性。
- 更改 cfgRacTuneHttpsPort 属性（包括通过 config -f <配置文件> 进行更改时）。
- 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。

我的 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。要解决此安全问题，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。

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。

如果使用 Microsoft Certificate Services 生成 RAC 证书，则在创建证书时，可能使用了“用户证书”选项而不是“Web 证书”。

要进行恢复，请生成 CSR，从 Microsoft Certificate Services 创建新的 Web 证书并通过运行以下 RACADM 命令进行上载：

```
racadm sslcsrgen [-g] [-f {filename}]
```

```
racadm sslcertupload -t 1 -f {web_sslcert}
```

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 地址是否正确设置。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。

事件和错误消息

将 CMC 固件从最新 CMC 版本降级至较早版本后，机箱日志为何会在一些日志中显示以下消息？

```
USR8513 - MessageID missing from message registry.
```

您看到的是在当前固件中引入的新消息，旧固件无法解读。有关该消息 ID 的更多信息，请参阅 **www.dell.com/openmanagemanuals** 上的“OpenManage 软件”下的 *Event and Error Messages Reference Guide*（事件和错误消息参考指南）。